平成３０年度成果報告書

戦略的イノベーション創造プログラム(SIP)第２期
IoT 社会に対応したサイバー・フィジカル・セキュリティ

『サイバー・フィジカル・セキュリティ対策基盤』に関わる動向調査報告書

平成３１年３月

国立研究開発法人新エネルギー・産業技術総合開発機構

(委託先)　日本電気株式会社

要約 （和文）

IoT は、Society 5.0 の基盤技術であり、社会インフラ、産業システム、生活環境、自然環境等のフィジカル空間に埋め込まれた IoT 機器が、多様なネットワークを介してクラウド等のサイバー空間と連結され、AI に代表される高度な知識処理やビッグデータとしての分析・解析処理と連携することにより、様々な付加価値やサービスを創出し、フィジカル空間である経済社会に多大な恩恵をもたらすと期待されている。

一方、サイバー攻撃の対象は急激に拡大し、攻撃の手法も著しく高度化している。また、製品やサービスを製造し流通する過程で不正なプログラムの組込みや改造が行われるサプライチェーンリスクの問題も顕在化しつつあり、グローバルなサプライチェーンにおいてサイバーセキュリティ対策の強化が求められている。

このため、戦略的イノベーション創造プログラム（SIP）第二期において、課題名『IoT 社会に対応したサイバー・フィジカル・セキュリティ』として、セキュアな Society 5.0 の実現に向け、様々な IoT 機器を守り、社会全体の安全・安心を確立するため、IoT システム・サービス及び中小企業を含む大規模サプライチェーン全体を守ることに活用できる『サイバー・フィジカル・セキュリティ対策基盤』の研究開発と実証を進めている。

本事業はその中で、研究開発の出口戦略実現に向け、「サイバー・フィジカル・セキュリティ対策基盤」に関し、下記 3 点につき調査を行った。

①IoT 機器とクラウド等のセキュリティに関する動向調査

サプライチェーンセキュリティに関連する標準規格文書・国際標準化動向等の調査、海外の事業者に関するアンケート調査・ヒアリング調査を実施した。

調査結果を基に、各事業者が自ら対応するセキュリティ対応範囲と事業者間の責任分界点、監査・認定機関の位置付けと実際に監査・認定を行う際に用いられる手段、社会実装時に課題となると考えられる点と SIP 研究開発項目との対比についての考察を行った。

②IoT ネットワークのセキュリティに関する動向調査

今後　サプライチェーンに起因するセキュリティの脅威が増加すると想定されるため、下記の調査を実施した。

- 国　：９ヵ国のセキュリティに関する政策動向
- 業界団体　：3GPP と GSMA の認定制度
- ベンダー　：主要 4 ベンダーのセキュリティマネジメント/プロセス等
- キャリア　：主要国の 4 キャリアの受入試験/運用対策等
- OSS コミュニティ：SDN/NFV 関連の 3 コミュニティの体制面/プロセス等

③技術動向調査

下記三つの観点より調査を実施した。

- ソフトウェア検査技術調査
  脆弱性検出/品質確保のための検査技術として、静的/動的解析の課題と研究状況
- ハードウェア検査技術調査
  バックドア（不正）を検出するための技術/ツールの内容と研究状況
- ホワイトハッカー活用調査
  人手による脆弱性調査を活用している領域として、米国でホワイトハッカーを活用している事例

上記の調査結果を踏まえ　今後取り組むべき内容の考察を行った。

最後に、②、③の調査結果を分析し、課題を抽出した。そして、その課題に対して、情報共有の仕組み作り、検査技術の研究・開発、認証制度・評価機関の設置の観点で、ネットワークセキュリティの確保の方向性の考察を行った。

要約 （英文）

IoT is the fundamental technology of Society 5.0, where IoT devices embedded in a physical space, such as social infrastructures, industrial systems, living environments, and natural environments, are expected to create various added values and services, and to bring significant benefits to the economy and society, which are also physical space, through connection with cyberspace, such as clouds via various networks, collaboration with advanced knowledge processing (represented by AI), and analysis processing as big data.

On the other hand, the scope of the targets of cyberattacks is rapidly expanding, and attack techniques are becoming more advanced. In particular, as a result of the spread and expansion of IoT which create new value within industrial society and family life, the threat of cyberattacks can be found in all industrial activities, not only in cyberspace, but also in physical space.

To comply the above social needs the Cross-Ministerial Strategic Innovation Promotion Program (SIP) Phaes-2 has launched the research and development program under the project " Cyber Physical Security for IoT Society" to provide IoT systems and services to protect various IoT devices and to achieve safe and secure society, and "Platform for Cyber Physical Security Measures" which will assure the security of large scale supply chain including small-to-medium sized enterprises in realizing secure Society 5.0.

In defining the outcome of this research and development program, this project has made the survey in the following three key aspects;

① Survey on security aspects for IoT devices and cloud services

The team ran surveys on standards documents and international standardization activities related to supply chain security, gave questionnaire and interviews to communication service providers (CSP). Based on the survey results the team has made further studies on the definition of the scope of CSP's security measures and responsibility boundaries between multiple CSPs, positioning of and method used by certification bodies and accreditation bodies, and the real life implementation issues when compared with the SIP R&D items.

② Survey on IoT network security

Due to possible increase of supply chain security vulnerabilities following targets have been surveyed.

- Countries : Government legislations, rules, policies, guidelines on security matters in 9 countries
- Industrial Organizations : Security certification processes issued by 3GPP and GSMA
- Vendors : Security management and processes by 4 major network infrastructure vendors
- Network Operators : Acceptance test and operational processes on security aspects by flagship operators in 4 countries
- OSS Community : Organizational structure and processes in 3 SDN/NFV related communities

③ Survey on technical aspects]

The team has surveyed the following three technical areas.

- Technologies on software evaluation

  R&D status and issues on static analytics/dynamic analytics which are to be used for detecting vulnerabilities and quality improvements

- Technologies on hardware evaluation
  R&D status of technologies and tools for backdoor detection although the team understands it is still at immature stage
- Use of White Hacker
  Cases found in U.S.A. using white hackers for areas where man-intervened actions are needed for vulnerability detection

The team has performed studies on the directions of actions to be taken in the near future based on the survey results.

Last but not the least, the team has analyzed the survey results from ② and ③ and extracted some of the key issues. Studies were made for the resolution to those issues in respect of assuring network security by creating the framework for sharing information, research and development on the inspection technologies, and establishing appropriate certification bodies and accreditation systems.

まえがき

戦略的イノベーション創造プログラム（SIP）第二期は、課題名『IoT 社会に対応したサイバー・フィジカル・セキュリティ』として、セキュアな Society 5.0 の実現に向け、様々な IoT 機器を守り、社会全体の安全・安心を確立するため、IoT システム・サービス及び中小企業を含む大規模サプライチェーン全体を守ることに活用できる『サイバー・フィジカル・セキュリティ対策基盤』の研究開発と実証を進めている。

本報告書は、『サイバー・フィジカル・セキュリティ対策基盤』に関連する研究開発動向や政策動向として、IoT のセキュリティ確保のための活動状況、各国制度動向、セキュリティ検査技術動向の調査結果を報告するものである。

目 次

図 目 次

表 目 次

用語一覧

本報告書では、以下の通り組織や施策等の略語を統一する。

（アルファベット順）

用語	概要
3GPP	モバイルネットワークシステムの仕様検討・作成を実施している業界団体（Third Generation Partnership Project）
AFL	Google の研究者が打ち出したファジングツールで、遺伝的アルゴリズムを用いたデータの自動生成・ファジング実行を行う（American Fuzzy Lop）
BSA	ソフトウェアの知的財産保護や不正使用対策を推進している団体（The Software Alliance）
CSIRT	コンピュータインシデント対応組織（Computer Security Incident Response Team）
CVE	ソフトウェア脆弱性の識別番号（Common Vulnerabilities and Exposures）
CVSS	共通脆弱性評価システム （Common Vulnerability Scoring System）
CWE	脆弱性の種類を分類するための識別番号（共通脆弱性タイプ：Common Weakness Enumeration）
DAST	動的セキュリティ解析技術（Dynamic Application Security Testing）
DDoS	分散 DoS 攻撃（Distributed Denial of Control）
DFSEC	ノキアにて採用しているセキュリティに関する開発～評価に適用する一連のスキーム（Design for Security）
DHS	アメリカ国土安全保障省（Department of Homeland Security）
DLL	様々なプログラムから利用される汎用性の高い機能を収録した、部品化されたプログラム。実行ファイルが起動する際に自動的に連結されメモリ上に展開される。（Dynamic Link Library）
DoC	攻撃による影響の一種で、制御妨害（Denial of Control）
DrDoS	反射型 DDoS 攻撃（Distributed Reflection Denial of Service Attack）
ELF	ファイル形式の 1 つ。Linux ディストリビューションの多くで標準バイナリ形式として採用。（Executable and Linking Format）
EPC	4G 等で使用されるモバイルコアネットワーク（Evolved Packet Core）
FedRAMP	米国政府機関のクラウド調達基準（Federal Risk and Authorization Management Program）
GAFA	Google、Apple、Facebook, Inc.、Amazon.com の 4 企業をまとめた呼称。これらの米企業は、IT の発達によってそれぞれの分野で市場を席巻しており、まとめて GAFA と呼ばれる。
GDPR	2018 年に制定された、欧州における新たな個人情報保護の枠組みである一般データ保護規則 （General Data Protection Regulation）
GPL	ソフトウェアの利用許諾条件などを定めたライセンスの一つ。主にフリーソフトウェアの開発・配布のために用いられるもの。（GNU General Public License）
GSMA	元々GSM 方式を採用していた企業・団体にて結成された業界団体（GSM Association）
IAST	静的・動的解析のハイブリッドという位置づけのセキュリティ解析技術（Interactive Application Security Testing）

用語	概要
ICS	産業制御システム（Industrial Control System）
ICS-CERT	DHS 内の産業制御システムのインシデント対応を行う CSIRT 組織
IDS	外部との通信を監視し、攻撃や侵入の試みなど不正なアクセスを検知するシステム（侵入検知システム: Intrusion Detection System）
IEC	電気・電子技術に関する規格を策定する国際的な標準化団体の一つ（国際電気標準会議：International Electrotechnical Commission）
IMSI	携帯電話加入者に発行される、国際的な加入者識別番号（International Mobile Subscriber Identity）
ISO	産業分野の国際標準を定める国際機関の一つ（国際標準化機構：International Organization for Standardization）
JIS	工業標準化法に基づいて、工業製品の仕様などについて定められる日本の国家標準（日本工業規格：Japan Industrial Standards）
LoV	攻撃による影響の一種で、監視機能喪失（Loss of View）
MITRE	米国連邦政府がファンディングする非営利研究開発機関
MoC	攻撃による影響の一種で、制御不正操作（Manipulation of Control）
MSAN	さまざまなメタル回線を収容できる装置（Multi-Service Access Node）
NCCIC	米国 DHS 内の国家サイバーセキュリティ通信統合センター（National Cybersecurity and Communications Integration Center）
NDAA	特定のメーカーを指定して調達を禁ずる規制を含む、国防授権法（National Defense Authorization Act 2019）
NESAS	3GPP/GSMA にて規定しているネットワーク機器の認証スキーム（Network Equipment Security Assurance Scheme)"
NIST	工業技術などに関する規格の標準化を支援しているアメリカ合衆国の政府機関（アメリカ国立標準技術研究所：National Institute of Standards and Technology）
NIST CSF	NIST サイバーセキュリティフレームワーク（NIST Cybersecurity Framework）
NIS 指令	2016 年 8 月に制定された、EU では初となるサイバーセキュリティに関する指令（The Directive on Security of Network and Information Systems）
NITRD	米国ネットワーク IT 研究開発プログラム（Network Information Research and Development）
NTIA	米国商務省電気通信情報局（National Telecommunications and Information Administration）
NVD	米国政府による脆弱性情報管理のための標準化されたデータベース（National Vulnerability Database）
OSS	ソースコードを広く一般に公開し、誰でも自由に扱ってよいとする考え方。また、そのような考えに基づいて公開されたソフトウェアのこと。（Open Source Software）
PLC	自動機械の制御に使用される制御装置（Programmable Logic Controller）
RAN	無線アクセス網（Radio Access Network）
RASP	アンチウイルス等と同じ思想で、事後的にセキュリティ対策を行う技術（Runtime Application Self-Protection）
rootkit	コンピュータシステムへのアクセスを確保したあとで第三者（通常は侵入者）によって使用されるソフトウェアツールのセット
SAST	静的セキュリティ解析技術（Static Application Security Testing）
SBOM	ソフトウェアの構成要素リスト（Software Bill Of Materials）

用語	概要
SCAS	ネットワーク機器毎に実現すべきセキュリティ要件とその評価の規定（Security Assurance Specification）
SECAG	GSMA にて NESAS 策定に向けた活動を行っているグループ（SECurity Assurance Group）
SECAM	3GPP で規定したセキュリティアシュアランスと評価のフレームワーク（SECurity Assurance Methodology）
WCLSCAN	インターネット脅威監視システム
XML	文書やデータの意味や構造を記述するためのマークアップ言語の一つ（Extensible Markup Lang）

1．はじめに

IoT は、Society 5.0 の基盤技術であり、社会インフラ、産業システム、生活環境、自然環境等のフィジカル空間に埋め込まれた IoT 機器が、多様なネットワークを介してクラウド等のサイバー空間と連結され、AI に代表される高度な知識処理やビッグデータとしての分析・解析処理と連携することにより、様々な付加価値やサービスを創出し、フィジカル空間である経済社会に多大な恩恵をもたらすと期待されている。

一方、サイバー攻撃の対象は急激に拡大し、攻撃の手法も著しく高度化している。特に、産業社会や家庭生活に新たな価値創造をもたらす IoT の普及・拡大に伴い、サイバー攻撃の脅威は、サイバー空間だけでなくフィジカル空間を合わせた、あらゆる産業活動に潜むようになっている。

また、製品やサービスを製造し流通する過程で不正なプログラムの組込みや改造が行われるサプライチェーンリスクの問題も顕在化しつつあり、グローバルなサプライチェーンにおいてサイバーセキュリティ対策の強化が求められている。今後は一定の水準のセキュリティ要件を満たさない事業者、製品、サービスがグローバルな調達要件からはじき出される恐れがあり、輸出の大部分を占める製造業の参入機会を確保することが重要な課題となる。

このため、戦略的イノベーション創造プログラム（SIP）第二期において、課題名「IoT 社会に対応したサイバー・フィジカル・セキュリティ」として、セキュアな Society 5.0 の実現に向け、様々な IoT 機器を守り、社会全体の安全・安心を確立するため、IoT システム・サービス及び中小企業を含む大規模サプライチェーン全体を守ることに活用できる「サイバー・フィジカル・セキュリティ対策基盤」の研究開発と実証を進めている。

本事業はその中で、研究開発の出口戦略実現に向け、「サイバー・フィジカル・セキュリティ対策基盤」に関連する研究開発動向や政策動向等の調査を実施した。

2. 事業概要

第 5 期科学技術基本計画（2016 年 1 月 22 日閣議決定）で、「Society 5.0」は、サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステム（以下「サイバー・フィジカル高度融合システム」という。）により、IoT や AI 等の先端技術を用いてすべての人とモノがつながり、様々な知識や情報が共有され、新たな価値観が生まれる社会として、目指す姿が示されている。

また、2017 年 3 月に経済産業省から「Connected Industries」が発表され、ネットワーク化の進展は、従来とは異なる、より柔軟で動的なサプライチェーンの構成を可能とし、新たな付加価値を生み出す機会を増大させるものとして、目指す姿が示されている。

一方で、「Society 5.0」や「Connected Industries」により、ネットワーク化が進むことで、サイバーセキュリティの観点では、攻撃の対象点が増加し、防御すべき範囲が拡大することになる。また、その脅威はサイバー空間のみならず、フィジカル空間に対しても深刻な影響を及ぼしうる。このような状況の中、グローバルなサプライチェーンに関連したセキュリティにおける対策が必要となっている。具体的な動向の事例を以下に記載する。

- 技術面

製品やサービスを製造し流通する過程で不正なプログラムの組込みや改造が行われるサプライチェーンリスクの問題が顕在化しつつある。

※事例
－スマートフォンのファームウェアに、ユーザーの個人情報等を国外に送信する機能が埋め込まれる。
－通信機器に仕掛けたバックドア（裏口）を使ってウイルスを侵入させ、情報を窃取したり、基幹インフラを攻撃できる。

- 制度面

各国で、制度面での対策検討が進められており、今後は一定の水準を満たしていなければ取引ができなくなる等、セキュリティ要件を満たさない事業者、製品、サービスは、グローバルなサプライチェーンにおいて淘汰されるといった影響も懸念される。

※事例
－米国では、国防総省の調達に NIST SP800-171 への遵守が求められる。
－米国では、サイバーセキュリティのリスク評価の枠組みを示した「サイバーセキュリティフレームワーク（NIST Cybersecurity Framework）」の中で、サイバーサプライチェーンリスクの評価を明確に位置付ける方針を示しており、対応が求められる可能性がある。
－EU では、2017 年 9 月に発表した政策パッケージの中で、「サイバーセキュリティ認証フレームワーク（The EU cybersecurity certification framework）」を今後整備していく旨を表明しており、各機器の特性や認証方法も考慮に入れた上で、今後、サプライチェーンまで含めたサイバーセキュリティ対策が求められる可能性がある。

上記の事例を踏まえ、今後、技術的にグローバルでサプライチェーン全体のセキュリティを確保し、運用される多様な IoT システム・サービスのセキュリティ維持を実現することで、社会全体の安全・安心を確立し、また制度面で国際ハーモナイゼーションを確保し、グローバルに企業が活動できる環境整備を行う必要がある。

そのために、本調査で、サプライチェーンに関連するセキュリティの技術や国の政策等の海外動向調査を実施し、今後取り組むべき方向性の提言を行う。

3. 報告書の構成

「サイバー・フィジカル・セキュリティ対策基盤」におけるセキュリティ対策の対象となる構成要素は、IoT 機器、IoT ネットワーク、クラウド等である。セキュリティ対策は、各構成要素（IoT 機器、IoT ネットワーク、クラウド等）すべてにおいて実施することが重要である。サイバー攻撃は、構成要素の中にセキュリティの脆弱なポイントを一か所見つけるだけで、そこが起点となり、他の構成要素への攻撃が可能となる。そのため、本事業では、IoT 機器－IoT ネットワークークラウド等の End to End を対象として、以下の三つの点で調査を実施した。

① 「サイバー・フィジカル・セキュリティ対策基盤」における IoT 機器とクラウド等のセキュリティに関する動向調査
② 「サイバー・フィジカル・セキュリティ対策基盤」における IoT ネットワークのセキュリティに関する動向調査
③ 「サイバー・フィジカル・セキュリティ対策基盤」における技術動向調査

本報告書では、4 章において、IoT 機器とクラウド等のセキュリティに関する動向調査結果をまとめ、5 章において IoT ネットワークのセキュリティに関する動向調査、6 章において技術動向調査についてまとめる。また、7 章において、ネットワークセキュリティ確保の方向性をまとめる。

4. IoT 機器とクラウド等のセキュリティに関する動向調査

4.1 はじめに

IoT の進展に伴い、セキュリティの脅威が高まっている。国内においては、政府は、Society5.0、Connected Industries を推進する中で、攻撃の対象点が増加し、防御範囲が拡大し、サイバー空間のみならず、フィジカル空間に対しても脅威が高まっている。グローバルには、スマートフォンのファームウェアへの個人情報等の国外送信機能の埋め込み等の技術面でのサプライチェーンリスクが顕在化しており、制度面では米国防総省の調達に NIST SP800-171 への遵守が要件化される等の動きがある。

このような背景から、本調査では、海外のサプライチェーンに関連する基準や企業の取り組み実態について調査し、今後の取り組み課題について提言をまとめる。

4.2 調査方法

本調査は図 4-1 に示すプロセスにより実施した。最初に、サプライチェーンセキュリティに関連する標準規格文書・国際標準化動向等の調査、海外の事業者に関するアンケート調査・ヒアリング調査を実施した。その調査結果を基に、各事業者が自ら対応するセキュリティ対応範囲と事象者間の責任分界点、監査・認定機関の位置付けと実際に監査・認定を行う際に用いられる手段、社会実装時に課題となると考えられる点と SIP 研究開発項目との対比についての考察を行った。

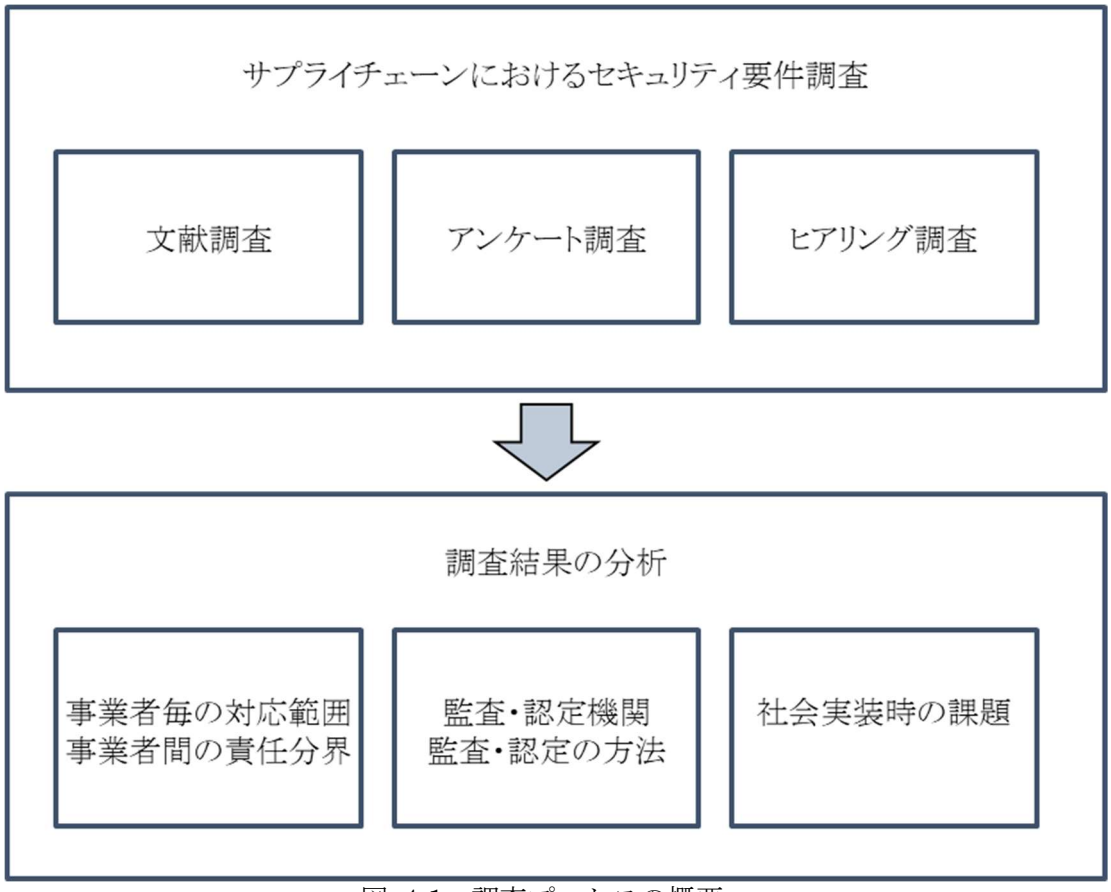


図 4-1 調査プロセスの概要

4.3　サプライチェーンにおけるセキュリティ要件

4.3.1　全体概要

サプライチェーンにおけるセキュリティ要件の分析を行うため、図 4-2 に示す標準規格類を対象に調査を行った。各規格について、策定背景と目的、基本コンセプトと位置付け、想定されるステークホルダー、管理目標と対策要件の概要の観点から整理を実施した。

最初に、分野共通の汎用規格文書を調査することで、サプライチェーンに求められる標準的セキュリティ要件を抽出した。特に IoT システムに関連する要件を対象とした規格を重点的に取り上げている。次に、特定の産業分野（自動車・電気通信・電力）を対象とする規格の調査を実施し、分野別に固有の取り組みや特徴的な点について要点をまとめた。

また、海外の事業者を対象に、アンケート調査及びヒアリング調査を実施し、サプライチェーンセキュリティ対策の実施状況、対策を実装する上での課題について実態を整理した。

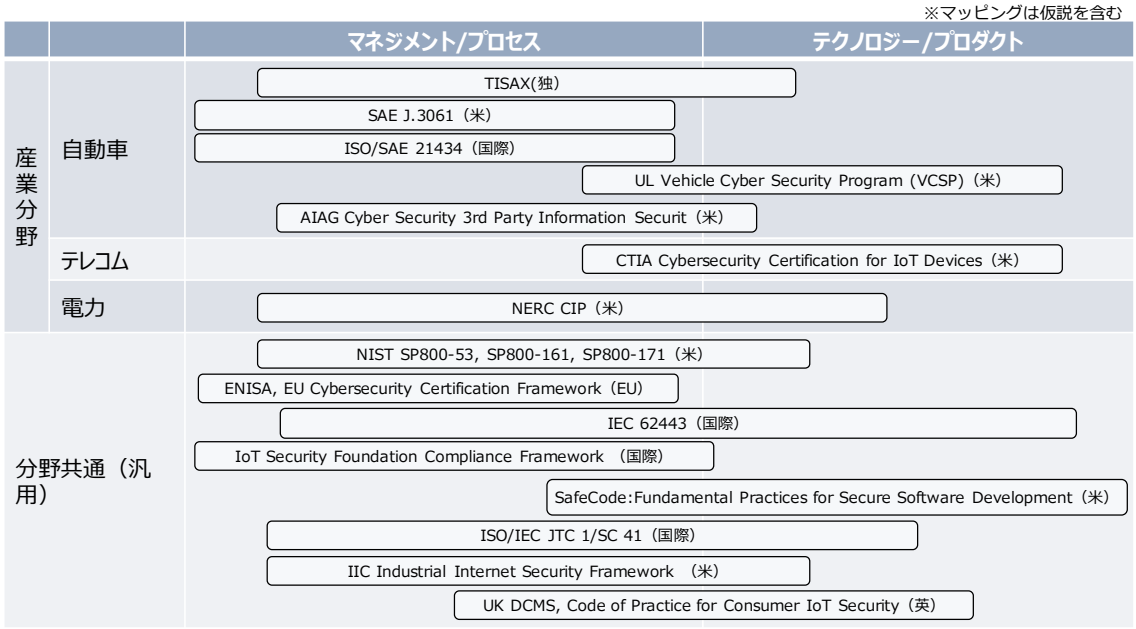


図 4-2　調査対象規格

4.3.2　文献調査

4.3.2.1 分野共通(汎用)規格

4.3.2.1.1 NIST SP 800-53 Rev. 4

NIST SP 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations に関する調査結果を以下に示す。

- 背景・目的

  米国連邦政府機関の情報システムに対するセキュリティ管理策及びプライバシー保護管理策を示す基準。FIPS Publication 200 が米国連邦政府機関の情報システムの情報システムに対する最低限の要求事項を定めていることに対し、本基準は FIPS Publication 200 に準拠するために実施すべき管理策を選択・特定するために対策カタログ及びガイダンスを提供する。

NIST SP800-37 の定めるリスク管理フレームワークにおける「セキュリティ管理策の選択」に該当する基準と位置付けられる。セキュリティ管理策は 18 の管理領域から構成され、これらは NIST Cybersecurity Framework とも対応がとられている。米国連邦政府機関の情報システムを管理する職員は、担当するシステムのリスク分析を行った上で必要なセキュリティ管理策を本基準から選択・適用することが求められる。

複数の改訂が繰り返されており、正式に発効されている最新版（2019 年 2 月時点）は第 4 版にあたる。2019 年夏に第 5 版が発行される予定となっている。

- 基本コンセプト
  - ✓ <u>対策実施優先順位のガイダンス</u>
    各管理策には 4 段階の対策優先順位が設定されている。自組織でセルフアセスメントを実施した結果として、未適合の管理策が複数存在した場合には、より優先度の高い管理策から順に取り組んでいくことが推奨される。

  - ✓ <u>影響度に応じたベースライン管理策と追加の拡張管理策</u>
    情報システムのセキュリティ侵害時の影響度に応じて採用すべきセキュリティ対策のベースラインについてガイダンスが示されている。ベースラインは「LOW（低位）」、「MOD（中位）」、「HIGH（高位）」の 3 段階から選択することになり、各ベースラインで採用が推奨される管理策の一覧がガイダンスとして提供されている。特に中位、高位の管理策には追加の拡張管理策が提供され、より詳細なセキュリティ対策を実践するため方法が示されている。

- 想定されるステークホルダー

  NIST SP 800-53 Rev. 4 の想定するステークホルダーとその特徴は以下の通りである。
  - ✓ 米国連邦政府機関の所有する情報システム管理者向けに、セキュリティ管理策を選択するためのカタログ及びガイダンスを提供するものであり、何らかの拘束力を持った指針ではない。
  - ✓ 実際にサプライチェーンへセキュリティ対策を適用する基準に関しては、別基準（SP 800-161, SP 800-171 等）を参照することとなる。
  - ✓ Revision 5 に向けた改訂議論の中では対象を連邦政府以外の政府機関のシステムまで拡大することが検討されている。また、NIST Cybersecurity Framework が v1.1 へ改訂され、管理領域に SC（サプライチェーンリスク管理）を追加したこと等を踏まえた整合性をとるための修正も行われる見込みである。

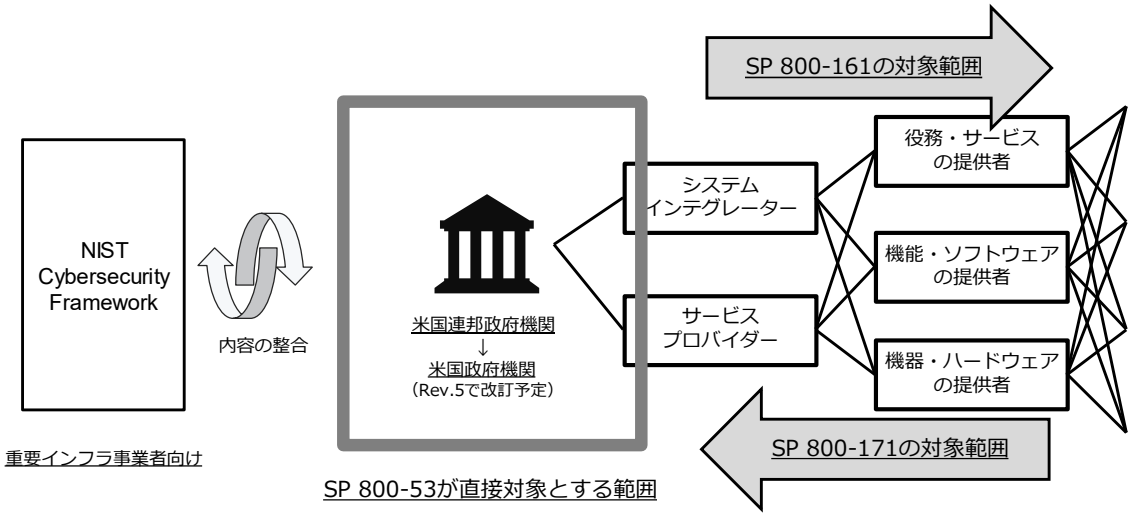


図 4-3　NIST SP 800-53 Rev. 4 の想定するステークホルダー

- 管理目標と対策要件の概要

NIST SP 800-53 Rev. 4 の管理目標と対策要件の概要である。

✓ 政府情報システムへのセキュリティ対策及びプライバシー保護対策を目標とし、18 の管理領域、256 の詳細管理策がリスト化されている。詳細管理策には複数の拡張管理策が対応付けられ、影響度に応じた選択が可能である。

✓ マネジメントに重きを置く ISO/IEC 27001 と比較して、具体度の高い技術対策やインシデントへの対応、復旧といった事後対策への言及が多くみられる。

No.	管理策の概要
1	アクセス管理に関する対策(25) ●アカウント管理（最小権限と職務の分離） ●リモート、無線、モバイルアクセス管理 ○セッションの管理、ロック　など
2	セキュリティ教育に関する対策(5) ●意識向上のための教育 ●役割毎のトレーニングの実施 ○教育、訓練実施履歴の記録　など
3	監査と説明責任に関する対策(16) ●監査イベントの記録、分析、報告 ○否認の防止、監査の効率化 ○組織横断型監査の実施　など
4	セキュリティ評価・認可に関する対策(9) ●セキュリティ評価基準の策定 ●外部システムとの相互接続管理 ○内部接続、Redチームによる侵入試験　など
5	システム構成管理に関する対策(11) ●システム基本構成の管理、最小機能原則 ●構成変更の管理と変更権限の制限 ○セキュリティ影響分析、使用制限　など
6	コンティンジェンシープランに関する対策(13) ●コンティンジェンシープランの策定 ●代替拠点設置、通信の冗長化、バックアップ ○訓練・演習の実施、セーフモード機能　など

No.	管理策の概要
7	IDと認証の管理に関する対策(25) ●IDと認証コードの管理（職員、デバイス） ●組織外ユーザの識別と認証 ○認証結果の秘匿、情報サービスの認証　など
8	インシデント対応に関する対策(10) ●インシデント対応計画の策定 ●インシデントの監視・管理・報告 ○インシデント対応訓練・演習　など
9	システムの保守に関する対策(16) ●システム保守手順の作成 ○保守の管理、保守の適時実施 ○保守ツールの利用　など
10	記録媒体の保護に関する対策(8) ●記録媒体利用権限の管理 ●記録媒体の使用、保存、配送、破棄の手順 ○記録媒体へのラベリング　など
11	物理・環境のセキュリティに関する対策(20) ●施設の入退館管理、セキュリティ区画管理 ●防火・防水管理、電源管理と非常電源 ○装置利用制限、代替施設、資産の追跡　など
12	セキュリティ計画に関する対策(9) ●システムのセキュリティ対応計画 ○セキュリティを考慮した行動規範の作成 ○セキュリティ計画の集中管理　など

No.	管理策の概要
13	職員のセキュリティに関する対策(8) ●職務に応じたリスクと権限の管理 ●雇用・解雇規約上のセキュリティ要件 ○異動時の対策事項、懲戒事項　など
14	リスク評価に関する対策(6) ●セキュリティ要求の分類とリスク評価実施 ●情報資産の脆弱性棚卸し ○ベンチマーク調査　など
15	システムとサービスの調達に関する対策(16) ●システム開発ライフサイクルと調達プロセス ●セキュア開発原則、サプライチェーン保護 ●セキュリティ試験、外部サービス評価　など
16	システムとネットワークに関する対策(44) ●システム機能分割とセキュリティ機能の分離 ●ネットワーク分割と境界防御、DoS対策 ●通信の暗号化と鍵管理、DNS保護　など
17	システムと情報の完全性に関する対策(17) ●データ処理の欠損修復、改ざん防止 ●プログラム・ファイルの保護、改ざん検知 ○エラー処理、出力のフィルタリング　など
18	情報セキュリティプログラム(16) ○計画策定と責任者の明確化、リソースの確保 ○システムの一覧化と効果測定規則の決定 ○インサイダー脅威対策、関連団体協力　など

図 4-4　NIST SP 800-53 Rev.4 対策要件の構成
（●は最優先で対策を行うべき対策、○はそれ以下の優先度の対策）

- 改訂に向けた動向の要点

NIST SP 800-53 は Rev. 5 への改訂が予定されており、以下のような追加・変更が行われる見込みである。

✓ Revision 5 は 2019 年夏に発効予定であり、適用対象の拡大と対策主体の整理等が実施される予定である。

✓ 新規管理領域も追加される予定であり、プライバシー保護を目的とした管理策が強化されようとしている。

規格の体系・位置づけの整理

- 対象機関の拡大：従来は「米国連邦政府機関」向けの規格とされていたが、連邦政府機関以外の政府機関を対象に含む規格へ変更。
- 対象システムの拡大：従来は「情報システム」向けの規格とされていたが、制御システムやIoTシステムを対象として明示する予定。
- 対策実施主体の整理：想定される対策実施主体が分かりやすい形に要求事項の記載が改められる予定。組織管理者による対策が求められる対策か、システム管理者による対策か、等。
- 関連規格との整合：主に「NIST Cybersecurity Framework」がver.1.1に改訂されたことを踏まえた整合性の調整を行う。CSFでは新規管理領域としてサプライチェーンマネジメントが追加された。

新規管理領域の追加

- 追加される予定の管理領域は「Individual Participation(IP)」「Privacy Authorization (PA)」の2領域である。
  IPは6件、PAは4件の管理策が追加される予定である。
- 個人参加の原則：IPの領域では、個人情報保護の重要観点である個人参加の原則に関する管理策が記述される。個人情報管理ポリシーを策定したうえで、合意に基づく個人情報の取得・利用、データの正確性に関する異議申し立て、情報の削除請求への対応などを実施することが規定される。
- プライバシーの保証：PAの領域では、プライバシー管理規程を策定したうえで、個人情報の取り扱いを適正な手続きに則って行うことが規定される。具体的管理策としては、収集する情報の種類、利用範囲等の明示、目的外利用の禁止、外部機関と情報を共有する場合の制約事項などが記載される予定である。

図 4-5　NIST SP 800-53 Rev.5 ドラフト版における改訂要点

4.3.2.1.2 NIST SP 800-161

NIST SP 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations に関する調査結果を以下に示す。

- 背景・目的

  米国連邦政府の ICT システム利用の拡大に伴い、拡大したサプライチェーンリスクの管理策を強化する必要性から策定された基準。従来用いられていたサプライチェーンリスク管理策 NIST IR 7622 を引き継ぎ、拡張する形で整備された。2016 年に米国行政管理予算局からの通達において、サプライチェーンリスク管理要件として位置付けられた。

  ICT システムの構築・運用において、外部のサービス、機能の利用や、システムを構成する製品・部品の提供を担うプレイヤーの多様化によってサプライチェーンの複雑化・多様化が進んだ。効率性や互換性の向上といったポジティブな進展が見られる一方で、供給フロー全体のプロセスを詳細に把握することは困難になった。供給品質の問題に加え、悪意を持った介入により ICT システムに被害が生じる事例が発生し始めた。

  これらの脅威に対して総合的な対策を行う目的で実施すべき管理策が本基準に示されている。

- 基本コンセプト
  - ✓ **リスクベースのサプライチェーンセキュリティ対策**

    サプライチェーンセキュリティ対策を行う上で、リスクベースの考え方を採用している。階層化されたサプライチェーンにおいては、直接契約関係にない間接的サプライヤーとの関わりが発生するため、すべてのサプライヤーの管理を行うことはできない。組織に対する脅威・組織の抱える脆弱性からセキュリティ事象の発生確率・影響の大きさを評価し、リスクベースのサプライチェーンセキュリティ対策を志向する。

  - ✓ **リスク管理体系の階層化**

    組織全体を通じた統合的リスク管理を実施するため、リスク管理レベルの階層化を行うアプローチを採用している。
    組織階層間のリスクを戦略的に統合管理することで、管理目標の達成を目指す。

- 想定されるステークホルダー

  NIST SP 800-161 の想定するステークホルダーとその特徴は以下の通りである。
  - ✓ 原則、米国連邦政府機関の所有する ICT システム管理者及びそのサプライヤーを対象とする。
  - ✓ 組織的リスクマネジメントの考え方に基づいた遵守事項及びサプライヤーへ要求すべき事項が整理されている。
  - ✓ サプライヤーとしては、システムインテグレーター・サービスプロバイダーの他、ソフトウェア・ハードウェア・システム運用業務の提供等を行う事業者を対象とする。
  - ✓ サプライチェーンには、サプライヤーへのサプライヤー（2 次以上のサプライヤー）を含む構図となる。

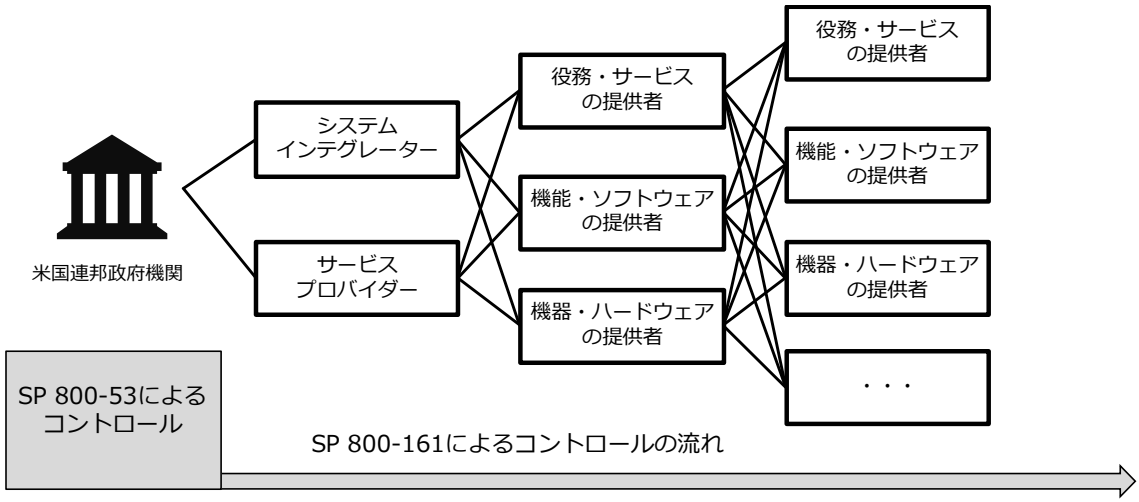


図 4-6　NIST SP 800-161 の想定するステークホルダー

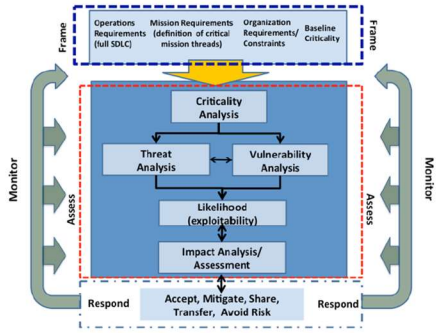
- 管理目標と対策要件の概要

  NIST SP 800-161 の管理目標の概要は以下の通りである。

  ✓ 以下のフレームワークに基づき、サプライチェーンセキュリティリスク管理を行うことを目標としている。
    - NIST SP 800-39 に定義されるリスクマネジメントプロセス
    - NIST SP 800-53 rev.4 に定義される ICT セキュリティ管理策

  ✓ 具体的なリスクマネジメントプロセスとして、NIST SP 800-39 を拡張したモデルを採用している。

リスクマネジメントプロセスの概要



リスクマネジメントプロセスのフローチャート

（出所）NIST COMPUTER SECURITY RESOURCE CENTER
https://csrc.nist.gov/publications/detail/sp/800-161/final

【特徴的なポイント】
- リスク対策の枠組みに従い、リスクの評価・リスク対応・リスクの監視が行われる。
- リスク対策の枠組みは、サプライチェーンの構造を考慮した上で決定することとされている。具体的には、ICTシステムに関するサプライチェーンリスクマネジメントポリシーの策定や、ICTサプライチェーンのリスク評価手法の確立等が求められている。
- リスクの評価、リスク対応、リスクの監視においてもサプライチェーンを念頭においた実施事項が定められている。具体的には、サプライヤーへ最低限要求すべき水準の設定や、リスク監視の対象にサプライヤーを含めることなどが記述されている。
- リスクの評価、リスク対応、リスクの監視は相互に関連し合っているため、各プロセスの実施結果に応じて他のプロセスの実施内容を見直すことが求められている。

図 4-7　NIST SP 800-161 リスクマネジメントプロセス

NIST SP 800-161 の対策要件の概要は以下の通りである。

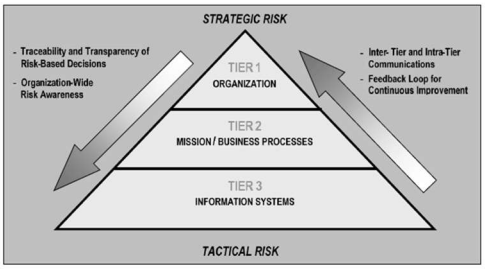
✓ 組織のリスクを統合的に管理するため、階層化されたリスクマネジメント体系が示されている。

✓ 詳細管理策については、NIST SP 800-53 rev.4 の管理策へ付加的管理策を追加する形で記述されている。

✓ オーバーレイの考え方に基づき、以下のプロセスで詳細管理策体系が構成される。
  - NIST SP 800-53 rev.4 に定義される ICT セキュリティ管理策からサプライチェーンに関連するものを抽出
  - 抽出した管理策へサプライチェーンの観点から付加的対策を追加、また独自の新規管理策を追加

- 組織階層（Tier1-3）別に管理策を分類・整理

階層化されたリスクマネジメント体系の概要

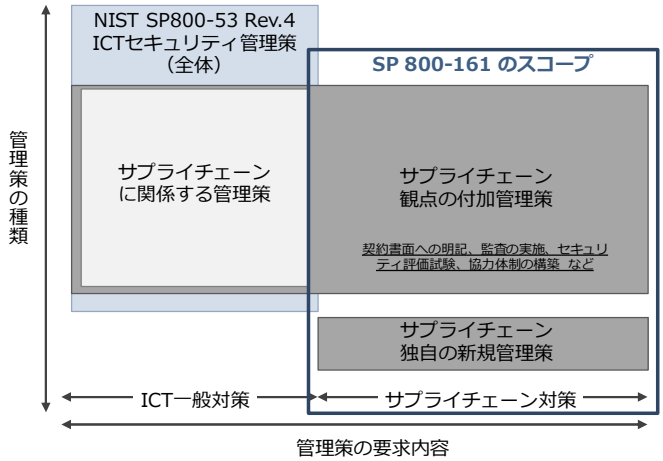


組織的リスクマネジメント階層の概要図

（出所）NIST COMPUTER SECURITY RESOURCE CENTER
https://csrc.nist.gov/publications/detail/sp/800-161/final

【特徴的なポイント】
- リスク管理階層は、Tier1「組織」, Tier2「ミッション/業務プロセス」, Tier3「情報システム」の3階層から成る。
- 各階層ではそれぞれのレベルに応じてサプライヤー管理策、サプライヤーへの要求水準を定義する。
- Tier1「組織」では、全体サプライチェーンリスク管理計画を策定し、組織共通対策水準をTier2/Tier3へ適用することを促す。
- Tier2「ミッション/業務プロセス」では、Tier1の策定する共通対策水準を受け、業務ミッションの重要度に応じた優先順位毎の対策水準を策定しTier3へ提供する。また、業務上の実態や改善要望のフィードバックをTier1へ返す。
- Tier3「情報システム」では、Tier1/Tier2の方針を踏まえた各システム固有のセキュリティ対策計画を策定・運用する。また、業務上の実態や改善要望のフィードバックをTier2/Tier1へ返す。
- 各Tierで実施される対策の透明性と追跡性を担保する。

図 4-8　NIST SP 800-161 階層化されたリスマネジメント体系



- SP 800-53 Rev.4から18の管理領域から228件の管理策を抽出し、追加のサプライチェーン対策を付加している。
  - 各管理に付加される対策は、契約や監査等の組織的対策とセキュリティ検証等の技術的対策がTier毎に記述されている。
- SP 800-53 Rev.4に存在しないサプライチェーン独自の新規管理策を6件追加。
  - 新規管理領域としてPV(来歴管理)が追加され、サプライヤーへ適用するポリシーの策定や遵守状況の追跡等の４件の管理策が記述されている。
  - ICT一般管理領域へ追加された新規管理策には保守の監視[MA-7]、調達の耐タンパ性に関する要求[SA-18(3)]の２件がある。

図 4-9　NIST SP 800-161 詳細管理策の構成

4.3.2.1.3 NIST SP 800-171 Rev. 1

NIST SP 800-171 Revision 1: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations に関する調査結果を以下に示す。

- 背景・目的

米国連邦政府機関において外部 ICT サービス依存や外部機関との情報共有が進み、連邦政府に関係する重要情報が連邦政府外に送信・保管されることが増えたことが本基準策定の背景とされている。

連邦政府の重要情報の機密性を適切に保護することは、連邦政府や政府外組織がその役割を果たすために必須であるという考えから、政府外組織が連邦政府との間で遵守すべき規律を政府調達要件として明確化する目的で策定されたのが本基準である。米国防衛省の調達要件において、すべてのサプライヤー向けに 2017 年末までに本基準を遵守する要求が発令された。今後は重要インフラ産業等に対象が拡大していくものと見られている。

- 基本コンセプト
  - ✓ <u>情報の機密性を保護すべき対象（CUI の保護）</u>
    本基準が保護の対象とする情報は「CUI（管理された非格付け情報: Controlled Unclassified Information）」とされている。連邦政府が具体的に指定する極秘情報や機密情報には分類されないが、機密性を保護すべき政府情報を意味する。プライバシーに関する情報や営業秘密、法執行による捜査情報等の例示があるが、これらに限定されるものではない。各省庁は CUI とみなす情報を指定し、NARA (National Archives and Records Administration) が管理する CUI 登録台帳へ記述する。

  - ✓ <u>調達要件としての位置付け</u>
    本基準で定義されるセキュリティ対策要件は、CUI を扱う政府機関外のすべての組織が遵守すべき要件と位置付けられており、政府機関の情報システム構築・運用を行う事業者だけでなく、システムの機能・部品等を提供する事業者からシステムコンサルティングを行う事象者まで幅広く対象となる。
    これらの政府外期間に対して本基準を調達要件として利用し、契約等の合意を得やすくする狙いがある。連邦政府調達規則 FAR 52.204-21 では、NIST SP 800-171 は CUI を扱う情報システムすべてを対象とする基準である旨が示されているが、適用開始は各省の裁量に委ねられている。2019 年 2 月現在は、防衛省のみが必須調達要件としての適用を開始している（DFARS 252.204-7012)。

- 想定されるステークホルダー
  NIST SP 800-171 の想定するステークホルダーとその特徴は以下の通りである。
  - ✓ 直接的な対象者は米国連邦政府機関から CUI に関係する ICT 関連業務を受託する者である。
  - ✓ サプライヤー側からの能動的な遵守表明を求める点に特徴がある。連邦政府からの要求は調達要件等の形で実施する。
  - ✓ ただし、受託者は自身の受託範囲において CUI の機密性を保護することが求められるため、二次請け以降の関係者においても本基準の定めるセキュリティ要件に準ずる内容の対策実施が求められると考えられる。

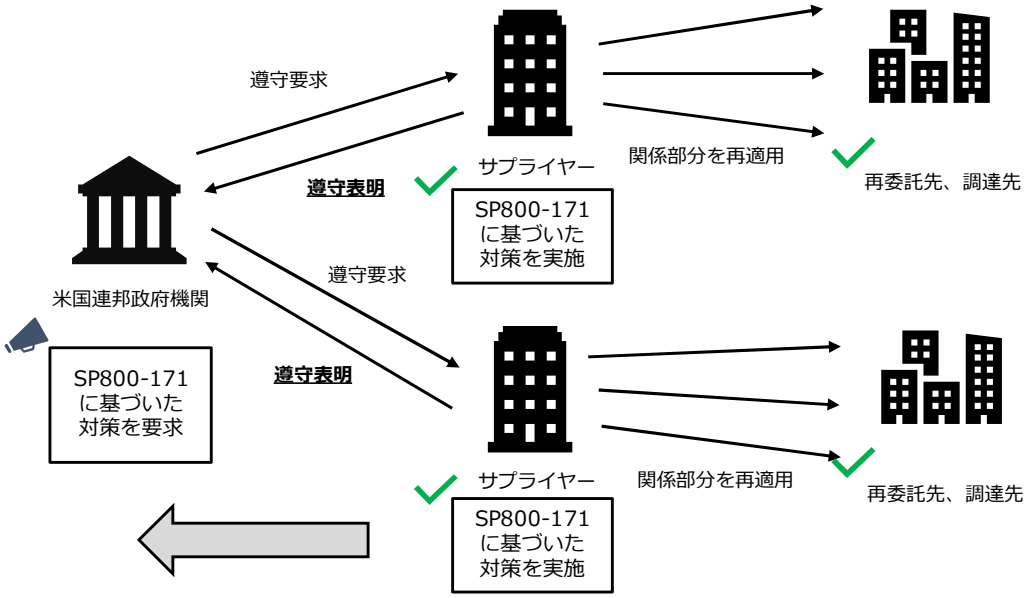


図 4-10　NIST SP 800-171 の想定するステークホルダー

- 管理目標と対策要件の概要
  NIST SP 800-171 の管理目標と対策要件の概要は以下の通りである。
  - ✓ CUI の適切な保護を目標とし、14 の領域でセキュリティ対策を行うことが要求されている。
  - ✓ 詳細対策要件は 192 件が示され、NIST SP 800-53, ISO /IEC 27001 との対応関係も示されている。ただし、NIST SP 800-53 との対応は全項目で示されているが、ISO/IEC 27001 との対応は一部の項目で「直接の対応がない」とされている。

No.	セキュリティ対策要件
1	アクセス制御
2	意識向上と訓練
3	監査と責任追跡性(説明責任)
4	構成管理
5	識別と認証
6	インシデント対応
7	メンテナンス

No.	セキュリティ対策要件
8	メディア保護
9	人的セキュリティ
10	物理的保護
11	リスクアセスメント
12	セキュリティアセスメント
13	システムと通信の保護
14	システムと情報の完全性

図 4-11　NIST SP 800-171 対策要件の構成

4.3.2.1.4 IEC 62443

IEC 62443 (IEC 62443-1, IEC 62443-2, IEC 62443-3, IEC 62443-4) に関する調査結果を以下に示す。

- 背景・目的
  IEC（国際電気標準会議: International Electrotechnical Commission）によって策定された制御システムのサイバーセキュリティ対策基準を定めた国際規格。制御システムの自動化や遠隔操縦が普及したことから、外部の脅威からシステムを保護するためのセキュリティ対策の必要性が高まったことが策定の背景とされている。
  本規格では、すべての制御システム関係者（構築・運用・保守等）を組織的に実施すべきセキュリティ対策の内容を標準化することを目的としている。
  また、2019 年 2 月に UNECE（国際連合欧州経済委員会: United Nations Economic Commission for Europe）が本規格を共通規制フレームワークへ統合する方針を承認している。

- 基本コンセプト
  - ✓ 体系化された対策基準群
    IEC 62443 シリーズは、「General（共通規則）」、「Policy & Procedures（ポリシーと手順）」、「System（システム）」、「Component/Product（部品・製品）」という四つの管理領域に体系化されている。それぞれの管理領域において実施すべきセキュリティ対策の標準化が行われている。

  - ✓ ゾーン別セキュリティレベル設定の考え方
    本規格では、制御システムの稼働する設備において、要求されるセキュリティレベルを分類し、等しいセキュリティレベルで防護すべきゾーン（区域）を設定する。その上で各区画の要求レベルに合ったセキュリティ対策を行うべきという考えが基本となっている。またゾーンの境界点となる領域をコンジット（管）と呼び、境界防御を徹底することで、低レベルゾーンから高レベルゾーンへの侵入を防ぐことが重要な対策と位置付けられている。

- 想定されるステークホルダー
  IEC 62443 の想定するステークホルダーとその特徴は以下の通りである。
  - ✓ 制御システムを利用する事業会社（IEC 62443-2)、システムインテグレーター（IEC 62443-3)、部品・製品等のサプライヤー（IEC 62443-4）が対象である。
  - ✓ 各プレイヤーにそれぞれの役割を割り当てることで、責任範囲を明確にしている。
  - ✓ サプライチェーンの上流に位置する組織が下流側の組織を統制する形の管理体系を想定している。

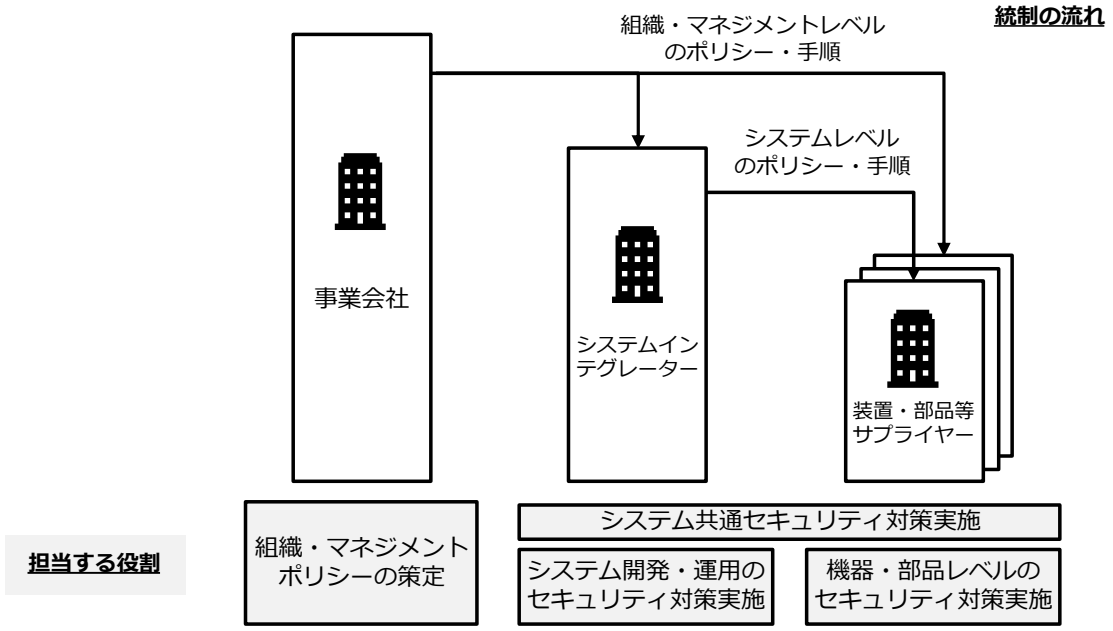


図 4-12　IEC 62443 の想定するステークホルダー

- 管理目標と対策要件の概要
  IEC 62443 の管理目標の概要は以下の通りである。
  - ✓ 制御システムにおけるセキュリティ対策を管理領域ごとの役割をマネジメントすることで実装することを目標とする。
  - ✓ セキュリティ対策を実装する管理領域は四つに分類される。
    - 共通規則: すべての関係組織に適用される規則。制御システムセキュリティマネジメントのコンセプトを示す。
    - ポリシーと手順: 主に事業会社、システムインテグレーターを対象とするマネジメント面の要求事項。
    - システム: 主にシステムインテグレーター、装置・部品等のサプライヤーを対象とするシステム的な対策要求事項。
    - 部品・製品: 主に装置・部品等のサプライヤーを対象とする製品品質担保に関する要求事項。
  - ✓ 各基準に対応する第三者認証制度を用意し、事業者間の相互確認負荷を軽減することを狙う活動が存在する。

管理領域	基準名	概要	対応する認証制度
共通規則	IEC 62443-1-1	IEC 62443シリーズ全体のコンセプト、モデル、用語等の定義。	－
	IEC 62443-1-2, 3	(未発行) 用語のより詳細な解説、セキュリティ対策の効果測定ガイド。	
ポリシーと手順	IEC 62443-2-1	制御システム向けセキュリティマネジメントシステム確立のための要求事項。ISMSと対応づけられており、PDCAサイクルを基本とする。	CSMS認証 (制御システム版ISMS認証)
	IEC 62443-2-2, 3	（未発行）セキュリティマネジメントを実装するための具体的対策集。	
	IEC 62443-2-4	事業会社からシステムインテグレーター等への対策要求事項を規定したもの。調達要件等への活用が想定されている。	
システム	IEC 62443-3-1	標準的セキュリティ対策技術を制御システムへ適用するための技術解説。	－
	IEC 62443-3-2	（未発行）IEC 62443のコンセプトであるゾーンとコンジットについての具体的対策要求事項。	
	IEC 62443-3-3	制御システムに対するシステムレベルでのセキュリティ対策要件集。	
部品・製品	IEC 62443-4-1	制御システムへ組み込まれる製品・部品等のセキュア開発に関する要求事項。	EDSA認証 （米ISASecureによる認証）
	IEC 62443-4-2	（未発行）製品・部品等に組み込まれるべきセキュリティ機能の要求。	

図 4-13　IEC 62443 の管理領域と対応する基準の一覧

IEC 62443 の対策要件の概要は以下の通りである。

- ✓ 発行済の基準で具体的な管理策を示すものは IEC 62443-2-1（組織マネジメント領域）、IEC 62443-3-3（システム対策要件領域）、IEC 62443-4-1（製品のセキュア開発領域）である。
- ✓ それぞれの管理領域に応じた詳細対策要件が規定されている。

No.	IEC 62443-2-1（組織）
サイバーセキュリティマネジメントシステム	
1	一般要求
2	リスク分析
3	リスクへの対処
4	監視と改善
詳細対策事項	※各領域でのポリシー策定基準が中心
1	事業継続計画
2	要員のセキュリティ
3	物理・環境のセキュリティ
4	ネットワーク分割
5	アクセス制御（アカウント管理）
6	アクセス制御（認証）
7	アクセス制御（認可）
8	システム開発・保守プロセスの管理
9	情報資産と文書の管理
10	インシデント対応の計画・実施

No.	IEC 62443-3-3（システム）
1	IDと認証に関する対策(11) ・一意のID付与、多要素認証の実施 ・ID、認証コード、鍵情報等の情報管理 ・パスワード強度、認可有効期間の設定　など
2	システム利用管理に関する対策(12) ・職務の分離と承認権限・特権制御の管理 ・無線・リモート接続・モバイル端末の制限 ・監査機能と監査ログの実装　など
3	システムの完全性確保に関する対策(9) ・通信の暗号化と改ざん防止対策 ・入出力値の検証、エラーチェックと通知 ・セッション管理　など
4	データの機密性確保に関する対策(3) ・データへのアクセス制限と持出の管理 ・利用を終了した情報の削除 ・十分な強度での暗号化　など
5	データフローの制限に関する対策(4) ・ネットワークの分割（物理・論理） ・ネットワーク境界防御 ・個人間の私的通信の禁止機能　など
6	応答性確保に関する対策(2) ・監視ログの収集可能性とアクセス性の担保 ・セキュリティ侵害の検出と通知　など ※通知まで時間は規格の要求外
7	リソースの可用性確保に関する対策(8) ・サービス不能攻撃への対策 ・バックアップ・復旧機能、非常電源の用意 ・構成情報の管理と不要機能の廃止　など

No.	IEC 62443-4-1（製品開発）
1	セキュリティマネジメントに関する対策(13) ・開発スコープ、開発プロセスの管理と改善 ・開発環境、開発データのセキュリティ管理 ・外部委託、サードパーティ製品の管理　など
2	セキュリティ要件の定義に関する対策(5) ・製品の周辺環境と脅威の分析 ・製品のセキュリティ要求分析とレビューなど
3	セキュリティバイデザインに関する対策(4) ・設計段階からのセキュリティ要件定義 ・ベストプラクティスの利用、多層防御　など
4	セキュアな実装に関する対策(2) ・セキュリティの実装レビュー ・セキュアコーディング規則　など
5	セキュリティのテストと検証に関する対策(5) ・脆弱性検査、ペネトレーションテスト ・試験実施者の独立性確保　など
6	セキュリティ関連課題の管理に関する対策(6) ・セキュリティ関連課題の特定、周知、管理 ・セキュリティ関連課題の定期レビュー　など
7	セキュリティアップデートに関する対策(5) ・セキュリティアップデート基準の文書化 ・アップデート配信計画と適時実施　など
8	セキュリティガイドラインに関する対策(5) ・製品の多層防御、堅牢化のガイドライン ・運用、廃棄、ID管理のガイドライン　など

図 4-14　IEC 62443 の対策要件の構成

4.3.2.1.5 ENISA, EU Cybersecurity Certification Framework

ENISA（欧州ネットワーク・情報セキュリティ機関: European Network and Information Security Agency）の発行する EU Cybersecurity Certification Framework に関する調査結果を以下に示す。

- 背景・目的

  EU デジタル単一市場のセキュリティ確保、プライバシー保護を目的とした認証フレームワーク。ENISA によって提言がまとめられ、欧州委員会にて本フレームワークの導入を目指していく方向性が承認されている。

  ICT サービス、IoT 機器に公的認証を与えることでサプライチェーンの品質保証及び事

業者間の相互確認負荷低減効果を生むことを狙いとしている。法的拘束力をもって遵守を促すものではなくフレームワークの採用は事業者の自由意志に委ねることを原則としている。

対策要件として具体的な技術要件・評価手法については本フレームワークで規定をせず、各領域の基準に沿った対策を行うことを励行するに留めている。

- 基本コンセプト
  - ✓ **認証制度そのものを規定するフレームワーク**

    ENISA 自体は直接的な認証を行わないスキームを採用している。本フレームワークでは、サイバーセキュリティ認証を機能させるための制度面として、認証機関の要件、審査方法、監督実施といった認証制度自体の要件を規定する。認証制度を実際に運用するための認証機関の設置、審査の実施、事業者の監督等は EU 加盟各国の裁量で行うことを前提とする。ただし、域内外のビジネス障壁とならないよう可能な限り多くの国際基準と同期をとることを志向するとされている。

  - ✓ **技術対策要件の自由**

    本フレームワークには認証への適合性審査に用いるための具体的な技術要件・検証要件を指定しない。例えば特定用途向け IoT 機器は当該用途機器のコモンクライテリアに則った対策の実施状況を審査することが基本であり、統一的な基準を採用する必要はない。ENISA による IoT 機器の技術的対策要件としては、本フレームワークとは別に「Baseline Security Recommendations for IoT」が 2017 年に公表されている。

- 想定されるステークホルダー

  EU Cybersecurity Certification Framework の想定するステークホルダーとその特徴は以下の通りである。
  - ✓ ENISA は認証制度の基準を統一する役割を果たし、直接の審査・認証は実施しない。
  - ✓ EU 加盟各国の認証機関は機器・サービスの認証実施に用いる基準を独自に選択可能である。
  - ✓ 実際に認証に用いられる基準が域内外で不一致を起こすことを防ぐため、国際標準の採用が推奨される。

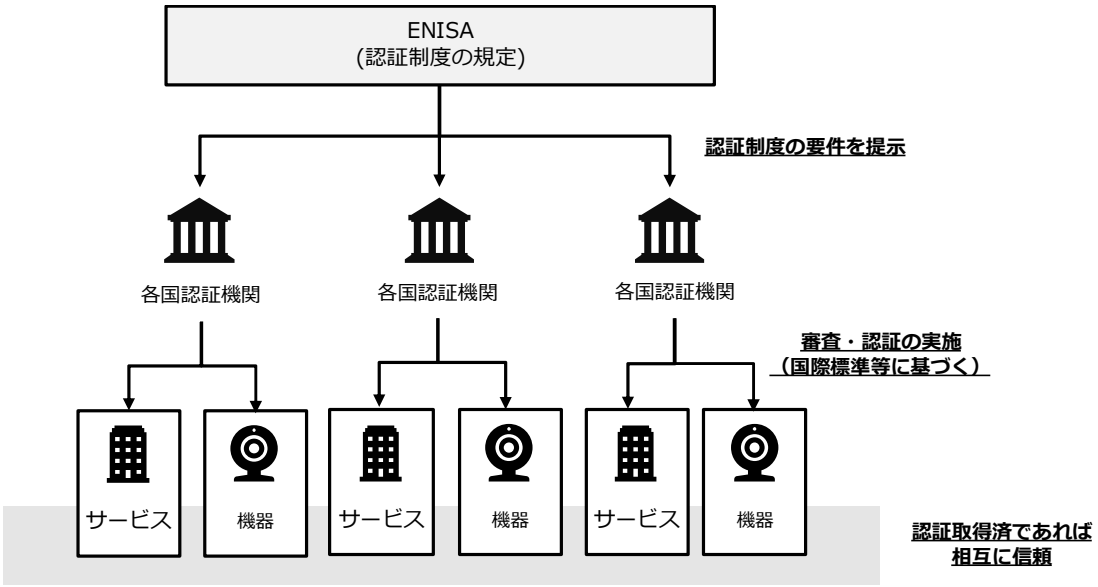


図 4-15　EU Cybersecurity Certification Framework の想定するステークホルダー

- 管理目標と対策要件の概要
  EU Cybersecurity Certification Framework ではセキュリティ対策要件への直接的な言及はなく、各認証機関の裁量で対象に合致する基準を選定可能。

  ✓ ここでは、ENISA が発行する IoT システム向け推奨対策基準である「Baseline Security Recommendations for IoT」の内容を例示する。

No.	推奨セキュリティ対策	対策例
1	セキュリティ・バイ・デザイン	IoTシステムライフサイクル全体を考慮、異なるセキュリティポリシーの統合、人体へ危害を加えない、節電のためにセキュリティ軽視しない、コンポーネントのカプセル化、ペネトレーションテスト、コードレビュー
2	プライバシー・バイ・デザイン	設計・開発時点からプライバシー保護を基本原則とする、全てのアプリケーションのリリース前にプライバシー情報の重要度を評価する（リリースする地域の法規制・文化、利用目的、利用文脈・ビジネス文脈）
3	情報資産管理	資産管理手順の策定、主要なシステム・ネットワークの設定管理、IoTサービスに関連するデバイスの特定（ゲートウェイ機器、エンドポイントデバイス、ホームネットワーク、ローミング、サービスプラットフォーム）
4	リスクと脅威の特定・評価	多層防御の考え方に基づき深刻なリスクを特定する（End-To-Endでリスクを評価しサプライチェーンリスクをスコープに含める、サードパーティベンダのコンポーネント評価は最新の情報に基づく）、IoTデバイスを利用する環境と目的を特定する
5	ハードウェアのセキュリティ	ハードウェアを基準とする不変のトラストを構築、セキュリティ機能によるデバイス保護・完全性確保（デバイスIDを認証する機能、暗号鍵の保護、重要なコードへのアクセス制限）
6	トラストと完全性の管理	デバイスの起動でトラストを確立する、署名による改ざんの検証・実行監視による改ざん防止、ソフトウェアインストールの制限、システムのリストア機能、トラストとトラストの関係性を表現・管理するための機能
7	初期設定のセキュリティ・プライバシー強化	初期設定状態においてセキュリティを有効にする（セキュリティ保護機能の有効化、不要な機能・安全でない機能の無効化）、デバイスに設定する全ての初期パスワードを十分な強度のものとする
8	データの保護とコンプライアンス	同意に基づく個人情報の取得と利用、個人情報利用目的の遵守、収集・利用する個人情報を最小限にする、GDPRへの準拠、異議申立てへの対処
9	システムの安全性と信頼性	予想外の動作を起こすことを前提とした安全設計、故障・動作異常時の自己診断・自己回復機能、スタンドアローンでの動作保証（通信途絶、サーバダウン時の動作継続）
10	ソフトウェア・ファームウェアのセキュリティアップデート	ソフトウェア・ファームウェア等を安全に遠隔アップデートする機能（安全なアップデートサーバ、機密情報を含まないデータ、通信の暗号化、改ざん検証）、自動アップデート機能、ファームウェアの下位互換性
11	認証	システムレベルの脅威モデルに基づく認証設計、初期設定時に初期パスワード・ユーザー名の変更を強制する（強度不足の変更は許可しない）、2要素以上の認証を検討する、認証情報データの暗号化、失敗回数の制限、安全なアカウント回復・パスワードリセット機能
12	認可	最小権限の原則による動作権限設定、ファームウェアを特権ユーザーのみアクセス可能な領域に保存する
13	アクセス制御（物理・環境）	アクセス制御によりデータの完全性・機密性を保護する、利用文脈を考慮したセキュリティとプライバシーの保護、オフラインでの改ざんの防止と検知、不要な接続ポートの閉塞
14	暗号化	通信の暗号化（十分な強度の暗号化アルゴリズムの使用、脆弱なプロトコルの無効化）、暗号鍵を安全に管理する、軽量暗号の利用
15	コミュニケーションのセキュリティ・トラスト	通信データ・保存データのトラストを保証する、最新の情報に基づいた通信セキュリティ確保、資格情報の漏えい防止、データ交換の信頼性を保証する（保存する毎に署名）、許可された相手とのみ通信、接続は意図的に行う（意図しない不正接続を許可しない）、不要な通信ポートの無効化、トラフィック量の制限
16	インターフェース・ネットワークのセキュリティ	ネットワークセグメントの分割、デバイス侵害時の被害を局所化するためのプロトコル設計、各デバイスで異なる秘密鍵を使用する、不要な通信ポートを公開しない、DoS対策・負荷分散、エラー表示の情報制限
17	入出力の制御	入力データの検証（不正な値が入力されないことを保証する）、出力のフィルタリング
18	ログの出力	システムログの記録（ユーザー認証ログ、アクセス管理設定ログ、セキュリティログなど）
19	監視と監査	デバイス動作の監視・検証（マルウェア検査、整合性監視など）、監査とレビュー（ペネトレーションテスト）
20	サポートの終了	IoT製品のサポート終了戦略の策定、サポート終了期日およびセキュリティアップデート・セキュリティパッチの提供機関を開示する、製品ライフサイクル内での効果測定と既知の脆弱性対策パッチの提供
21	実績のあるソリューション	よく知られていて利用実績が豊富なコンポーネントを選択し、独自の改変を行うことは避ける（通信プロトコル、暗号化アルゴリズムなど）
22	脆弱性とインシデントの管理	セキュリティインシデントの分析・処理を行うための手順を策定する、脆弱性開示の手順を調整する、脆弱性に関する情報共有のコミュニティに参加する、脆弱性レポート公表の仕組みを用意する（バグバウンティ）
23	人的セキュリティと教育・訓練	要員のセキュリティ・プライバシー意識の啓発、研修・訓練の計画と実施、全ての従業員のセキュリティに関する役割と責任を明確にする
24	サードパーティとの関係性	社外とのデータ処理における契約遵守、消費者との同意がある場合にのみ個人情報を第三者と共有する（製品の動作に必須であり、サービス運用に利用が制限されている場合を除く）、サプライチェーンリスク管理ポリシーを明確にした上で関係者に要件を伝達する。

図 4-16　Baseline Security Recommendations for IoT 対策要件の構成

4.3.2.1.6 IoT Security Foundation, IoT Security Compliance Framework

IoT Security Foundation の発行する IoT Security Compliance Framework に関する調査結果を以下に示す。

- 背景・目的

  国際 NPO である IoT Security Foundation が作成した IoT システムのセキュリティ対策、プライバシー保護のためのベストプラクティス集。同団体には、intel・ARM・IBM・Huawei・SAMSUNG 等の民間企業や、国際規格認証組織の UL 等も加盟している。

  チェックリスト形式でセキュリティ対策の実施要件を確認可能な形式となっているが、具体的な認証制度等を運用することは想定されていない。特徴としてはセキュリティ目標に応じて対策項目を選択的にチェックするフローを用いていることにある。

  コンプライアンスフレームワークの名の通り、セキュリティ対策だけでなくプライバシー保護のための要求（クラウドとネットワーク、サプライチェーン保護、安全な設定）が充実している。

- 基本コンセプト

  ✓ **純粋に対策要件へのベストプラクティスを提供することに限定した取り組み**

  本フレームワークはベストプラクティスを浸透させることを目的としており、NPO である IoT Security Foundation としては認証等の実施はしない立場をとっている。また、IoT セキュリティ対策に絶対的なものはなく、現在・今後ともに本対策の実施が十分性を保証するものではないことを注記した上で非常に具体性の高い対策の数々を列挙している。

  ✓ **対象・レベル別チェックの考え方**

  本フレームワークに様々なベストプラクティスが提供されているが、すべての対策の実施をチェックするのではなく業種・要求セキュリティレベルに準じた対策の実装とチェックを推奨している。現時点で発行されているフレームワーク (Release 1.0) はコンシューマー向け IoT 機器（カテゴリーA）を対象とするものと位置付けられている。要求セキュリティレベルは、要求される機密性・可用性・完全性から 5 段階にレベル分けするためのリスクアセスメントプロセスが示されている。今後のリリースでは、企業向け、産業向け、医療向け、自動車向け、公的機関向け、重要インフラ向けに対象を拡大していく予定とされている。

- 想定されるステークホルダー

  IoT Security Compliance Framework の想定するステークホルダーとその特徴は以下の通りである。

  ✓ IoT Security Foundation の役割はフレームワークの整理と提供に限定され、認証等は行わない。
  ✓ 各事業者はフレームワーク内のガイドに従いリスクアセスメントを実施、対策レベルを決定する。
  ✓ 決定した対策レベルに対応した対策を実装し、チェックリストを用いたアセスメントを各事業者が自ら行う。

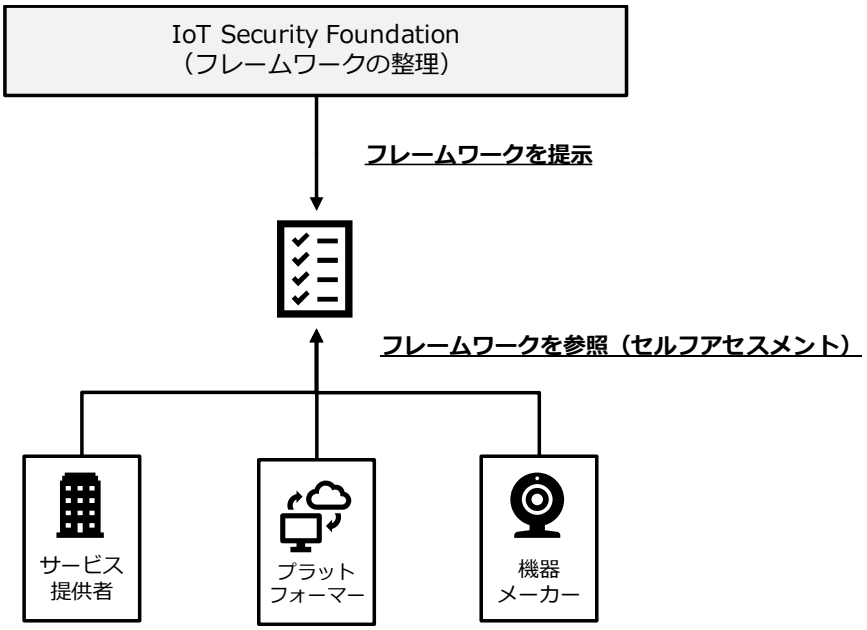


図 4-17　IoT Security Compliance Framework の想定するステークホルダー

- 管理目標と対策要件の概要

  IoT Security Compliance Framework の管理目標と対策要件の概要は以下の通りである。

  - ✓ IoT システムの達成すべきコンプライアンス目標として「マネジメント統制」、「セキュアエンジニアリング」、「目的に適合した暗号化」、「セキュアネットワーク・アプリケーション」、「セキュア開発プロセスとサプライチェーン保護」、「顧客の安全性とセキュリティ」が示されている。
  - ✓ トラストのサプライチェーンを重要視しており、IoT 機器を構成する各要素（ハードウェア、ソフトウェア等）それぞれのセキュリティアセスメント結果の証跡が、監査可能な統合的に管理されることを目標としている。

コンプライアンスクラスの分類

セキュリティが侵害された場合に、利用者・組織へ与える影響の大きさを評価し、３段階に分類する。
Release 1.0はコンシューマー向けIoT機器を対象しているが、個人情報を扱うIoT機器はClass　3以上に分類される。

クラス	機密性	完全性	可用性
Class 0	Basic	Basic	Basic
Class 1	Basic	Medium	Medium
Class 2	Medium	Medium	High
Class 3	High	Medium	High
Class 4	High	High	High

対策カテゴリ分類のためのキーワード

各セキュリティ対策を実装することが期待される領域を示すためにキーワードによる分類を行っている。システム面とビジネス面の2階層にそれぞれ3つのキーワードを対応させている。

第1キーワード	説明	第2キーワード	説明
システム	製品／デバイスおよびサービスの技術的要素	ソフトウェア	デバイスやサービスのソフトウェアへの直接的対策事項
		ハードウェア	デバイスやサービスの電気的ハードウェアへの直接的対策事項
		物理	デバイスの機械的側面における直接的対策事項
ビジネス	製品／デバイスおよびサービスへのビジネス的要求事項 ※運用機能には直接関係しないもの	プロセス	デバイスやサービスのセキュリティ特性に間接的に影響する行動フローに関する対策事項
		ポリシー	説明書やガイドラインにおいてセキュリティ特性に間接的に影響する要素への対策
		責任	デバイスやサービスのセキュリティ特性に間接的に影響する役割と責任に関する対策事項

図 4-18　IoT Security Compliance Framework の管理目標設定方法

No.	対策トピック	対策例
1	ビジネスセキュリティプロセス・ポリシーと責任	経営層による対策の主導、リスクアセスメント実施、セキュリティ侵害時の広報対応、脆弱性情報管理の各種対応と脆弱性公表ガイドラインへの対応（必須）、サードパーティとの連絡口の用意（Class 1以上必須）、標準規格への準拠、セキュリティアップデートの透明性（Class 2以上必須）、ISO 30111を参考としたポリシー（オプション）
2	デバイスのハードウェア・物理セキュリティ	USB等の接続ポートを原則閉塞する、認証情報や鍵を安全な領域に配置、CPU監視と異常検知時のリセット（必須）、セキュアブート機能実装とデフォルト有効化、デバッグ機能利用の制限(Class 1以上必須)、テスト用機能の削除、真にランダムな変数の生成（Class 2以上必須）、耐タンパ性のための物理的保護（Class 3以上必須）
3	デバイスのソフトウェア	認可されていないソフトウェアの制限、遠隔アップデート時の署名と実行前検証、改ざん検知機能の実装と停止禁止、トラスト署名ルートを耐タンパメモリに保存、脆弱なバージョンからの保護、デバッグ機能削除（必須）、アップデート時の通信暗号化、デバッグ機能をトラスト圏外へ提示しない、セキュアコーディング基準（Class 2以上必須）、機微情報の流出対策機能とサイドチャネル攻撃耐性（Class3以上必須）
4	デバイスのOS	セキュリティアップデート機能、不要アカウントの無効化、不要サービスの停止、必要最小限のアクセス権限・実行権限（必須）、パスワードをデバイスローカル環境に保存し特権ユーザー以外のアクセスを禁止する、認可外プロセスからのカーネルアクセス禁止、OSのすべてのセキュリティ機能を有効化（Class 1以上必須）、トラストレベルの異なるアプリケーションを分離、マイクロカーネル設計（Class 2以上必須）
5	デバイスのインターフェイス（有線・無線）	認可されない変更を検知した際の警告、通信途絶時に可能な範囲で動作継続（必須）、認可されない通信の拒否、ネットワーク設定のレビュー、既知の脆弱性があるプロトコルを利用しない、不要ポートの閉塞、機器固有のパスワードを設定する、初期ペアリング時の認証強度とパスワード変更の強制、推奨暗号リストの参照、暗号強度不足のプロトコルを無効化する、アプリケーション層のプロトコルをTLSで保護する（Class 1以上必須）
6	認証と認可	初期セットアップ時に全ユーザーログイン用初期パスワードの変更を強制する、時刻同期の正確性確保、遠隔制御による安全な状態への復旧（必須）、耐タンパ性のあるデバイスの固有ID、全てのデバイスに別個の初期パスワード設定する、空白ユーザー名・パスワードの禁止、パスワードの一部にユーザー名を含ませない機能、総当たり攻撃耐性、ゲストアカウント原則禁止、NIST SP800-63b等の標準規格への準拠（Class 1以上必須）
7	ハードウェアにおける暗号化と鍵の管理	鍵のコピー防止、危殆化した暗号アルゴリズムを利用しない、推奨暗号リストの利用、安全で耐タンパ性のある領域への保存（Class 1以上必須）、鍵の生成から配布・更新のプロセスを準備、デバイス固有かつ復号不可能な秘密鍵、NIST SP800-57相当の十分な鍵長（Class 2以上必須）
8	Webユーザーインターフェース	パブリックとプライベートでの認可を区別、入力値の正当性検証、URLエンコーディング等を用いてデータをラップする（必須）、認証強度の確保、管理画面ログインに強力な認証を用いる、初期パスワードをデバイス固有に設定、セッションタイムアウト、パスワードの平文保存禁止とsalt付与、入力パスワードをデフォルト非表示にする、OWASP等のガイドラインを参照、脆弱性試験実施、ファジングテスト（Class 1以上必須）
9	モバイルアプリケーション	伝送データの正当性検証、入出力値の正当性検証・ホワイトリスト化（必須）、初期パスワード変更必須、NIST SP800-63b等の標準規格への準拠、ファイルやデータベースへのアクセス制限と耐タンパー性、外部通信時のTLS利用、入力パスワードをデフォルト非表示にする、管理者用インターフェースへアクセス可能な権限を制限する（Class 1以上必須）
10	プライバシー保護	必要最小限の個人情報収集、閲覧権限のある個人にのみアクセスを許可、特に外部への開示時など可能な限り多くの場合に個人情報を匿名化する、個人情報の修正・削除を行うための機能、GDPRなど当該地域における規制への適合、ユーザーの意思決定負荷低減、承諾なくユーザーの音声・映像を記録しない（必須）、データの保存時と通信時の個人情報暗号化、個人情報保護ポリシーの開示、収集する情報と保存場所の明示、個人情報破棄要請手段の提供（Class 1以上必須）
11	クラウドとネットワークの要素	クラウドからデバイスのレジストリを参照・編集する権限を制限、クラウド内に保存された製品に関連するデータベースを暗号化する・アクセス制限する、仮想化技術を用いた多層防御、クラウドへの安全なリモートアクセス（必須）、Webサーバ設定の堅牢化、TLS関連の諸対策実施、既知の脆弱性を排除、不要ポート閉塞、安全なパスワード、アクセス制御（Class 1以上必須）クラウド上のOS等を最新バージョンに保つ、DDoS攻撃対策（Class 2以上必須）
12	セキュアなサプライチェーンと製造	デバイスの製造工程における耐タンパ性、デバイスのシリアルナンバーの一意性、強化プライバシーID [ISO 20008/20009]（Class 1以上必須）、製造時に使用するテスト用ソフトウェアを出荷前に削除、最終的な設定ファイル・ソースコードは暗号化して保存、セキュアブートを有効とした状態で全ての試験を行う、製造施設が信頼できない場合に調達の安全を管理するための方法、製品に関係する全てのライブラリで脆弱性対応を公言（オプション）
13	設定	デバイスと関連Webサービスの設定における耐タンパ性、デバイス設定のセキュリティ更新は即時配信する（Class 1以上必須）
14	デバイス所有権の移譲	譲渡時に元の所有者の個人情報を削除する機能を提供、ユーザーが利用を停止する際は個人情報を削除する、復旧不可能な方法での廃棄手段、セキュアな方法でデバイスを登録する、デバイスの一意性は利用者属性へ依存せずに保証する（Class 1以上必須）、デバイスIDから利用者情報を復元できないことを保証する（Class 2以上必須）

図 4-19　IoT Security Compliance Framework の推奨対策トピックと対策例

4.3.2.1.7 ISO/IEC JTC 1 / SC 41

ISO/IEC JTC 1 / SC 41 に関する調査結果を以下に示す。

- 背景・目的

  ISO/IEC JTC 1 / SC 41 は、ISO（国際標準化機構: International Organization for Standardization）及び IEC（国際電気標準会議: International Electrotechnical Commission）の合同技術委員会 JTC (Joint Technical Committee) のうち、情報技術を担当する JTC 1 内に設置された分科委員会である。2017 年から本格的な活動を開始している。

  SC41 で議論される標準規格の対象領域は IoT 及びその関連技術と定義されている。具体的な関連技術としては、センサーネットワーク、ウェアラブルデバイスが挙げられている。SC41 配下には三つの WG（アーキテクチャ、相互接続性、アプリケーション）、複数の SG（ウェアラブル、トラスト、Industorial IoT、エッジコンピューティング、リアルタイム IoT、ユースケース策定等）が設置されている。日本国内では情報処理学会情報企画調査会内に「SC 41 専門委員会」及び「スマートシティズ小委員会」が設置されており、SC41 に関連した活動を行っている。

- 基本コンセプト

  ✓ **IoT とその周辺システムの統合を推進するための標準化活動**

  本委員会では、IoT システムとその周辺領域を議論の対象とする。ネットワークやデータを主な着目点としつつ、分散型のスマートデバイスのアーキテクチャやアプリケーション、M2M（デバイス間: Machine to Machine）のインターフェースに関する標準化が検討される。Industorial IoT もスコープとして含まれており、スマートシティが具体的なユースケースの例として挙げられている。

  ✓ **相互運用性とトラストの考え方**

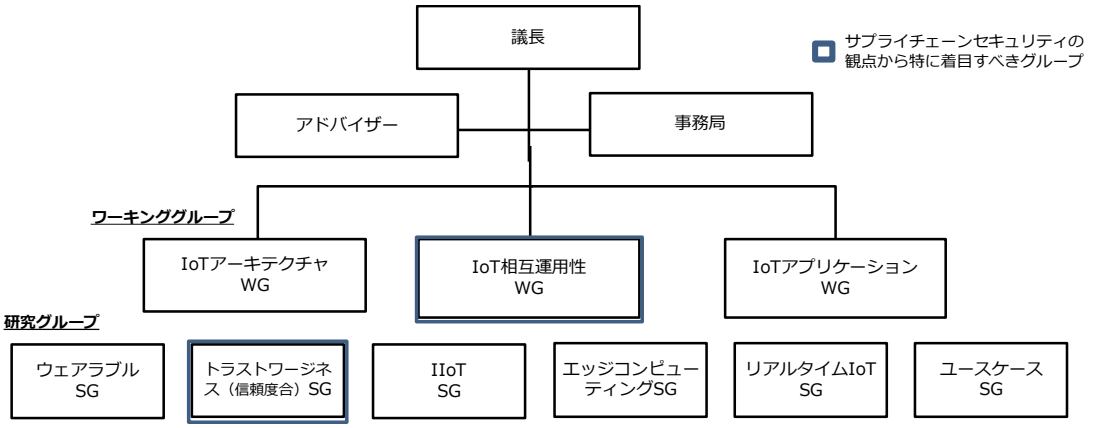
  独立したワーキンググループとして IoT の相互運用性を議論する WG 4 が設けら

れている。相互運用性に関連するトピックとして、接続可能性・準拠性・試験実施といった用語に言及されている。また、WG 4 とは独立した研究グループのテーマとして「Trustworthiness」が挙げられている。IoT システム・サービスのサプライチェーン内で信頼形成の実施と維持を行うための方法論を標準化するための議論が行われている。

- 委員会の特徴と全体構成

ISO/IEC JTC 1 / SC 41 の特徴と全体構成は以下の通り。

✓ IoT システムとその周辺領域までを対象とした議論を行うため、以下のような論点までスコープに含めた議論を行っている。
- エッジデバイスとのアーキテクチャ、アプリケーションの仕様
- システム間の相互運用性のためのインターフェース、信頼の形成と保証に関する基準



「SC 41 Business Plan and Dashboard 2017」をもとに三菱総合研究所作成
出所） https://www.iec.ch/public/miscfiles/sbp/jtc1-sc41.pdf

図 4-20　ISO/IEC JTC 1 / SC 41 の全体構成

- 規格開発状況

ISO/IEC JTC 1 / SC 41 において、作成中の標準規格と出版済の標準規格の状況は以下の通りである。

✓ センサーネットワーク関連の標準規格の作成が特に進捗している。ISO/IEC 29182 シリーズで定義される SNRA (Sensor Network Reference Architecture) モデルに基づき、スマートグリッド用センサー、水中センサー等の用途別センサーの標準が規格化されている。

✓ 相互運用性についての標準規格は ISO/IEC 21823、トラストに関連する標準規格は ISO/IEC 30147, 30149 として、それぞれの規格開発が進行している。2019 年 2 月末時点で出版済の規格は ISO/IEC 21823-1（相互運用性のフレームワーク）のみである。

- ISO/IEC 21823 Internet of things (IoT) -Interoperability for iot systems-
  IoT システム間の相互運用性を標準化する規格群。発行済の ISO/IEC 21823-1 (Part 1: Framework) では、IoT の相互運用性の面 (facet) のモデルを導入しており、「伝送」、「構文」、「意味（セマンティック）」、「動作」、「ポリシー」の相互運用性を確保することを目標としている。加えて、考慮すべき具体的要求事項として「IoT システムの特性（ネットワーク通信等）」、「IoT コンポーネントの特性（デバイスのネットワーク接続性、一意性等）「レガシーサポート」等とともに「セキュリティ」、「コンプライアンス」の項目を挙げている。「セキュリティ」の項目内では、機密性と完全性と並列に個人情報保護

対策の実装を要求している。

- ISO/IEC 30147 Internet of Things (IoT) -Methodology for implementing and maintaining trustworthiness of IoT systems and services-, ISO/IEC 30149 Internet of Things (IoT) -Trustworthiness framework-

  IoT システム間の Trustworthiness（信頼度合）を標準化する規格群。Trustworthiness は、システムが外部脅威にさらされたとしても安全、セキュリティ、プライバシー等を想定通りに保護し続ける動作をすることに対してステークホルダーが持つ自信の程度を表す概念とされている。両規格ともにドラフト作成中の段階であるが、ISO/IEC 30147 に関しては、日本から「IoT セキュリティガイドライン（IoT 推進コンソーシアム・総務省・経済産業省）」、「安全な IoT システムのためのセキュリティに関する一般的枠組」に基づいた内容が提案されており、両ガイドラインに記載された IoT システム向けのセキュリティ対策が Trustworthiness を実装・維持するための方策のベースとなる方向性で議論が進められているものと考えられる。

4.3.2.1.8 SAFECode:Fundamental Practices for Secure Software Development

SAFECode:Fundamental Practices for Secure Software Development に関する調査結果を以下に示す。

- 背景・目的

  ソフトウェアアシュアランスは、ソフトウェアが意図した通り機能し、設計や実装の欠陥が存在しないことを保証するための開発と実装の手法とプロセスを提供するものである。SAFECode が公開する Fundamental Practices for Secure Software Development によりその基本的なベストプラクティスが示されている。2008 年、2011 年に続き、2018 年に改訂版が発行されている。2018 年版では、Secure Development Lifecycle (SDL) を成功させるために重要なベストプラクティスを加えている。

  Juniper、Symantec、Microsoft、NOKIA、SAP、Adobe、EMC 等の会員企業における実践を通じたベストプラクティスを提供するものである。SAFECode では、産業界におけるセキュリティ対策が、理論的なベストプラクティスから効果的に実装可能であることを検証されたベストプラクティスに移行することを目指している。

- 基本コンセプト
  - ✓ <u>Secure Development Lifecycle (SDL) 成功のためのベストプラクティス</u>

    要求の特定、第三者コンポーネント（オープンソース、既製品（Commercial Off-the-Shelf:COTS）の管理、脆弱性対処と開示等、Development Lifecycle (SDL) の成功のためのベストプラクティスを提供する

  - ✓ <u>ライフサイクルを通じたセキュリティ管理策</u>

    開発プロセスや脅威の環境変化に応じてセキュリティ管理策を継続的に改善するアプローチを示している。上位の視点からは、①脅威、リスクの特定、②脅威・リスクに対処するセキュリティ要求の特定、③実装チームに対するセキュリティ要求の伝達、④セキュリティ要求が実装されているかの妥当性確認、⑤ポリシーや規制に準拠しているかの監査、というプロセスが重要となる。

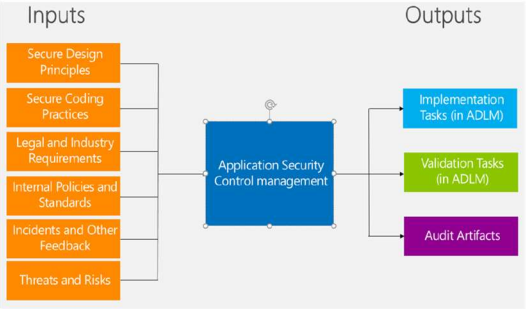
- 想定されるステークホルダー

  SafeCode:Fundamental Practices for Secure Software Development は、ソフトウェアディベロッパーを対象とするベストプラクティスである。SAFECode 会員を始めとし、広く一般的な企業において活用が可能な規格となっている。

- 管理目標と対策要件の概要

  SafeCode: Fundamental Practices for Secure Software Development の管理目標の概要は以下の通りである。

  - ✓ システムライフサイクルを通じたセキュリティ管理策の管理・改善の考え方に基づくベストプラクティスを示すことを目標としている。
  - ✓ ソフトウェアアシュアランスの考えに基づき、意図的、非意図的な脆弱性を解消し、ソフトウェアが意図した通り機能することを保証するための方策を提示する。ソフトウェアアシュアランスは、セキュリティ、認証、完全性を保証する上で中核的な領域を担うものであり、SAFECode では、ソフトウェアアシュアランスを実現するためのガイドとして、Secure Software Development, Software Integrity Controls, Software Integrity Framework 等の文書を提供する。



Application Security Control Managementは、セキュアソフトウェア開発プロセスを管理・改善するためのアプローチで、セキュア設計原則、セキュアコーディングプラクティス、法的・産業的な要求、内部ポリシー、標準、インシデント等のフィードバック、脅威・リスクなどをインプットとして、ソフトウェアの実装、検証、妥当性確認、監査などのアウトプットを生み出すプロセスとして捉えるものである。

構成要素	概要
設計	セキュア設計の原則、脅威モデリング、暗号戦略、IDアクセス管理、ログ管理と監査などの指針を示す。
セキュアコーディング	OWASP, CERT等コーディング標準、APIの利用制限、コード解析、データ保護、エラー対処などに関する指針を示す。
第三者コンポーネント使用時のリスク管理	オープンソース、COTS等を活用した開発の対策指針について、"Managing Security Risks Inherent in the Use of Third-party Components"等を参照する。
テストと妥当性確認	静的・動的解析、ファジングなど自動テスト、マニュアルテストの指針を示す。MITRE CAPEC等を参照する。
セキュリティ管理	影響度、リスク許容プロセスの対策指針を示す。
脆弱性の対応と開示	脆弱性対応ポリシー、役割と責任、第三者コンポーネントの管理と管理、脆弱性の修正と回避策等について締めす。
セキュア開発プラクティスの実装の計画	組織文化、組織スキルレベル、製品開発モデルとライフサイクル、ステークホルダー管理等について示す。

図 4-21　SAFECode のコンセプト

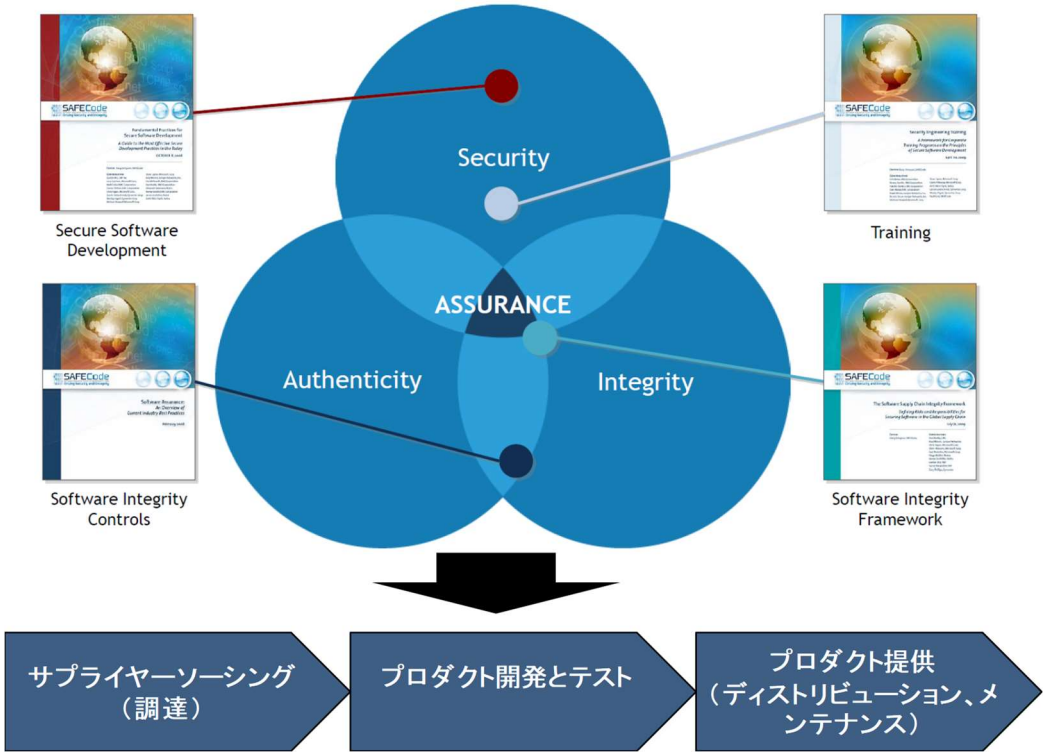


図 4-22　SAFECode におけるソフトウェアアシュアランス

SafeCode:Fundamental Practices for Secure Software Development の推奨対策集の構成と概要は以下の通りである。

- ✓ ソフトウェアアシュアランスとセキュアなソフトウェア開発力の向上のためのガイドラインを、“Fundamental Practices for Secure Software Development, 2nd ed”において示している。
- ✓ 開発プロセスにおける設計、プログラミング、テスト工程に焦点を絞り、実践すべき事項、関連する脆弱性（CWE: Common Weakness Enumeration）、実践すべき事項が行われているかを検証する手法をまとめている。
- ✓ リソース欄では、情報源、ツール等をまとめ、ソフトウェアアシュアランスの包括的なインデックスを提供している。

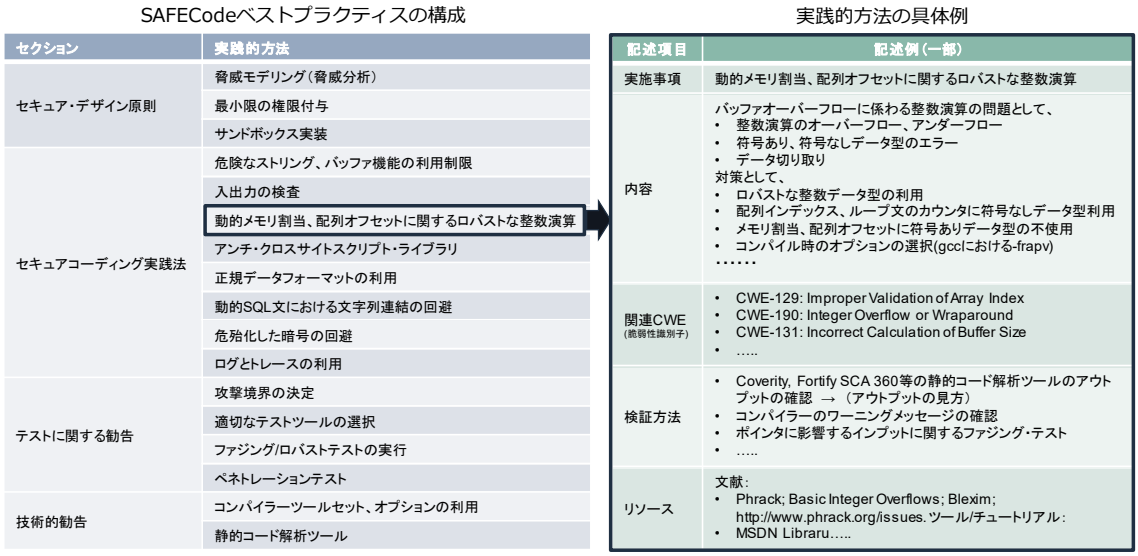


図 4-23　SAFECode ベストプラクティスの構成と具体例[1]

4.3.2.1.9 IIC, Industrial Internet Security Framework

IIC Industrial Internet Security Framework に関する調査結果を以下に示す。

- 背景・目的

  IIC, Industrial Internet Security Framework (IISF) は、Industrial Internet Consortium (IIC) が公開した、IIoT（産業用 IoT: Industrial Internet of Things）システムのセキュリティ問題に対処する共通フレームワークである。

  IIC は、相互接続機器の開発や導入、普及、インテリジェント分析等 IIoT 利用を加速することを目的として 2014 年に設立された、世界的な官民連携のオープンな会員組織である。創設メンバーには、AT&T や Cisco Systems、General Electric (GE)、IBM、Intel 等が名を連ね、現在では、世界 24 ヵ国から 160 社の企業を集めるまでに拡大した。現在、IIC は、技術標準化団体「Object Management Group (OMG)」の管理下に置かれている。

  IISF の策定に至った背景としては、IIoT と消費者向け IoT とではセキュリティ要件が異なるため、IIoT の要件に焦点を当てた検討が必要であった。IIoT のセキュリティでは、発電システム等の重要インフラへのリスクを低減する必要があるため、消費者向け IoT よりも高い堅牢性が求められる。さらに、IIoT セキュリティは、導入期間が数十年間に及ぶため、高可用性システムを長期に渡って維持するとともに、操作上の安全も維持しなければならない。これらの点も、消費者向け IoT とは異なるものであり、IISF は、このようなニーズへの対応方法について、関連性のある既存の安全基準や業界標準を特定し、開発業者を指導していく上での手順となる。

- 基本コンセプト
  - ✓ <u>五つの信用性 (Trustworthiness)</u>

    IISF は、信頼性を実現するために安全性、信頼性、強靭性、セキュリティ、プライバシーの五つの要素を適切に扱うことで、攻撃等の脅威に対抗することができる、としている。

[1] ISO: SAFECode Software Assurance Forum for Excellence in Code
https://www.iso.org/organization/7387391.html

- 想定されるステークホルダー
  IISF は産業界の異なるセキュリティ要件を包括的に捉えたものであり、クラウドから通信経路、プロトコル、組み込み機器から管理・運用、プライバシーや安全のための規格まで、IoT を構成する様々な要素のみならず、サプライチェーンまでも網羅している。これらの要素に関連する事業者は広く対象となる。

- 管理目標と対策要件の概要
  IISF の管理目標の概要は以下の通りである。
  - ✓ 図 4-24 に示す五つの信用性（Trustworthiness）目標を達成する。

No.	セキュリティ対策要件	要 件 詳 細	参　照
1	サイバーセキュリティ	重要な機能を実行するための保護対策維持	NIST SP1500-201
2	プライバシー	個人情報の処理から生じるリスク軽減	同 上
3	安全性	物理的な損傷や人々の健康被害で許容できないリスクから壊滅的な影響の防止	同 上
4	信頼性	サービスの継続を提供する能力	同 上
5	強靭性	状況の変化に適応し、攻撃、事故から迅速に回復する能力	同 上

図 4-24　信用性目標の定義

  - ✓ 図 4-25 に IIoT システムへの統合対策を規定する 12 のフレームワークを示す。

No.	セキュリティ対策要件	要 件 詳 細
1	概要	文書の目的や適用範囲、想定利用者、IICの他の文書との関連を解説
2	モチベーション	IIoT、IT/OTの融合に伴う安全対策の重要性を解説
3	堅牢なシステムのための考え方	対象となるシステムの特徴を理解することで、弱点とその対策が明らかになり、堅牢なシステムのための五つの要素の関連を解説
4	IT（Information Technology）と OT(Operation Technology) の融合に伴う安全対策の重要性	ITとOTとの融合に伴い、システムの特徴が変化する。今までとは異なる状況に合わせるための基礎的な考え方を解説
5	リスクマネージメント	ビジネス上のリスクの扱いを解説
6	ライフサイクルや信頼性等の複雑な構成と構成要素	ライフサイクルや信頼など、IIoTの複雑な構成を解説
7	通信・データの保護などの構成と構成要素	通信・データの保護など、IIoTの複雑な構成を解説
8	エンドポイント保護	エンドポイント保護を、ハードやCPU、仮想環境などの技術、ライフサイクルやサプライチェーンの影響を加味した包括的に解説
9	通信や接続性の保護	ITネットワークと制御ネットワーク、各種プロトコルや無線通信規格などを踏まえて代表的な対策を解説
10	セキュリティ監視や分析	セキュリティ状態の監視プロセス、予知や検知などのIRのためのプロセスなどの解説
11	セキュリティ環境の構成と変更・管理	セキュリティ環境の構成と変更・管理を解説
12	将来を見据えて	継続して本文書の更新を進めていく基となるのはテストベッドであることを解説

図 4-25　IISF のフレームワーク

4.3.2.1.10 UK DCMS, Code of Practice for Consumer IoT Security

UK DCMS, Code of Practice for Consumer IoT Security に関する調査結果を以下に示す。

- 背景・目的

UK DCMS, Code of Practice for Consumer IoT Security は、英国政府機関の一つである Department for Digital, Culture, Media & Sport (DCMS) が、消費者向け IoT 製品のセキュリティ確保のため、2018 年に作成したガイドラインである。作成は、国家サイバーセキュリティセンターの協力の下で行われ、産業界、消費者団体、学界とも連携がなされた。

英国による家庭用 IoT 機器製品の普及を受け、個人情報保護や DDoS 攻撃への加担を防ぐこと等を目的としたセキュリティ対策ガイドラインを策定する必要性が認識されていた。本ガイドラインでは、意識啓発による対策に留まらず、各事業者が IoT 製品の設計段階からセキュリティ対策を実装することで IoT サプライチェーン全体のセキュリティを担保することを目的としている。

英国政府は、IoT 製造元または IoT サービス業者が製品またはサービスの提供時に、ガイドラインをベンダーやプロバイダーに提示することを推奨している。ガイドラインに対応しているか、ガイドラインを採用していないかにより、ガイドラインを採用していない業者は、適切なベンダーやプロバイダーではないと見なすべきとしている。ハイテク企業である HP Inc., Centrica Hive Ltd 及び Green Energy Options (geo) Ltd.は、本ガイドラインに同意する最初の企業であり、政府は他の製造業者や小売業者にもこれに従うことを推奨している。

- 基本コンセプト
  - ✓ <u>安全な IoT を実現するためのガイドライン</u>
    IoT のセキュリティにおけるベストプラクティスを、成果に焦点を当てて 13 項目のガイドラインに集約している。

- 想定されるステークホルダー
  IoT 製品の開発からサービスの提供、販売までに関わる事業者が対象となる。
  - ✓ **デバイスメーカー:** 組み立てが完了したインターネット接続型の最終製品を製造する企業。完成品には様々な他社製品が含まれる場合がある。
  - ✓ **IoT サービス提供者:** IoT ソリューションの一部として、ネットワークやクラウドストレージ、データ移管等のサービスを提供する企業。インターネット接続型デバイスの提供はサービスに含まれることがある。
  - ✓ **モバイルアプリケーション開発業者:** モバイルデバイスで動作するアプリケーションの開発業者、提供を行う企業。こうしたアプリケーションは、デバイスとの通信手段として、IoT ソリューションに含まれることが多い。
  - ✓ **小売業者**: インターネット接続型の製品や関連サービスを消費者に提供する業者を指す。

- 管理目標と対策要件の概要
  UK DCMS, Code of Practice for Consumer IoT Security の管理目標の概要は以下の通りである。
  - ✓ 合計 13 項目の基本対策項目が示され、特に重要な 3 項目は優先度高に位置付けられている。

No.	セキュリティ対策要件	要 件 詳 細
1	デフォルト（初期）パスワードを設定しない(優先度：高)	多くのIoTデバイスは、普遍的なデフォルトのユーザー名とパスワードで販売されている。利用者は使用前にパスワードを変更する必要がある。
2	脆弱性に関する情報の公開方針を導入する(優先度：高)	インターネットに接続された機器やサービスを提供する事業者は、脆弱性の開示方針の一部として公開窓口を提供しなければならない。これにより、セキュリティ研究者などが問題をタイムリーに報告することができる。
3	ソフトウエアを定期的に更新する(優先度：高)	インターネットに接続された機器に常駐するソフトウェアは安全に更新可能にしなければいけない。更新はデバイスの機能に影響を与えず、タイムリーに配信されるべきである。
4	認証情報とセキュリティ上重要な情報を安全に保存する	資格情報はすべてIoTサービスとデバイス内に安全に保存する必要がある。資格情報はハードコードし、デバイスソフトウェアでは取得できないようにする。
5	安全に通信する	オープンで検証済みのインターネットセキュリティ標準を使用することを推奨する。
6	攻撃対象になる場所を最小限に抑える	機密性の高いデータは、通信時にリモート管理や制御を含めて暗号化する必要がある。すべての鍵は安全に管理されるべきである。
7	ソフトウエアの整合性を確認する	セキュアブートメカニズム（コンピューターの起動時にあらかじめデジタル署名のあるソフトウェアしか実行できないようにする技術）を使用してIoTデバイスソフトウェアを検証する必要がある。許可されていない変更を検出すると、デバイスはオペレータに問題を警告する。問題の通知は、アラートの配信に必要となる以上の広域なネットワークには接続しない。
8	個人データの保護の徹底	デバイスまたはサービスの一方または両方で個人データを処理する場合、一般保護規則（GDPR）やデータ保護法（2018年）など、該当するデータ保護法に従って処理しなければならない。デバイスメーカとIoTサービスプロバイダは、それぞれのデバイスやサービスにおいて消費者のデータをだれが、どのように、何の目的で使用するかという明確かつ透明性の高い情報を消費者に提供する必要がある。これは、関与する可能性のある第三者にも適用される（広告主も含む）。消費者の同意に基づいて個人データを処理する場合、その個人のデータは正当かつ合理的に取得し、消費者はいつでもその情報の使用を停止できるものとする。
9	回復力のある運用を実現	IoTサービスは、ネットワーク接続が切断された場合でも運用を継続し、電力が回復した場合には速やかに回復する。IoTデバイスは、迅速にネットワーク運用に戻るべきである。
10	テレメトリデータ	セキュリティの異常について、使用状況と測定データを監視する必要がある。
11	データの所有権と削除	IoTデバイスは所有権を変更する可能性があり、リサイクルまたは処分される可能性がある。消費者（GDPR（EU一般データ保護規則）またはCCPA（カリフォルニア消費者プライバシー法）の規制の対象となる統制を維持し、サービス、デバイス、およびアプリケーションからデータを削除できるようにするメカニズムを提供する必要がある。
12	簡単な機器の設置とメンテナンス	IoT機器の設置とメンテナンスは、セキュリティを考慮した最も効率のよい技法、手法とする
13	データ入力の検証	ユーザーインターフェイスを介して、API（プログラムからソフトウェアを操作するためのインターフェイス）またはサービス内のネットワーク間で転送される入力されたデータを検証する。

図 4-26　消費者保護のためのセキュリティ対策要件集

4.3.2.2 自動車分野向け規格

4.3.2.2.1 TISAX

TISAX (Trusted Information Security Assessment Exchange) に関する調査結果を以下に示す。

- 背景・目的

  TISAX は、VDA（ドイツ自動車工業会: Verbands der Automobilindustrie）において自動車メーカーとサプライヤー間のサプライチェーンにおける情報セキュリティの評価・審査の標準化と結果の共有を制度化したもの。供給関係の信頼性を高めるために評価情報を透明化することを目的とする。

  VDA の情報セキュリティワーキンググループでは、ドイツ自動車産業が約 82 万人を

雇用し 400 万台を超える自動車を輸出し情報セキュリティの重要性が高まっていると認識していた。これを受け、個々のサプライヤーへの多重監査を避けるために ISO/IEC 27001, 27002 をベースとした TISAX を 2016 年に開発した。

企業間の情報セキュリティ認識について共通の標準を確立する狙いがある。2016 年 5 月から 2017 年にかけて試行され、2017 年初より VDA からの委託により ENX (European Network Exchange) が運用を開始した。2019 年 2 月現在はバージョン 2.0.2（2018 年 9 月 18 日リリース）に基づいた運用が行われている。

- 基本コンセプト
  - ✓ <u>国際標準に基づいた評価基準</u>

    ISA（情報セキュリティ評価: Information Security Assessment）基準は、ISO/IEC 27001 (ISMS) の管理策を基本としている。加えて、データの保護に関する基準として、BDSG（ドイツ連邦データ保護法: Bundesdatenschutzgesets）の第 3 条 9 項「特殊タイプ」と第 11 条「受注処理」の要綱を参照している。

    他の基準への準拠、認証の取得による試験の免除は原則行われない。ただし、ISO/IEC 27001 を取得している場合等は自己評価のプロセスを省力化できる。

  - ✓ <u>評価対象項目、評価手法、評価結果のレベル分け</u>

    評価対象項目は 4 カテゴリ×2 レベル、評価手法は 3 レベルに段階分けされている。また、評価結果を 6 レベルの成熟度に基づいた認定が行われる。評価結果の成熟度レベル認定の有効期間は最大で 3 年間である。

項目	区分数	内　容
評価対象項目	4カテゴリ	情報セキュリティ、サードパーティーへの対応、データの保護、試作品の保護
評価対象項目のレベル	2レベル	高い保護、非常に高い保護
評価方法	3レベル	レベル1(AL1、自己評価のみ)、2(AL2)、3(AL3、自己評価の他に証拠文書等の検証・インタビュー確認・オンサイト検査も実施)
評価結果	6レベル	0(不完全な)、1(実施されている)、2(管理された)、3(確立された)、4(予測可能な)、5(最適化している)

図 4-27　TISAX による評価

- 想定されるステークホルダー

TISAX で想定するステークホルダー関係はプロダクトに関係する情報を提供する者 (Active) と受領する者 (Passive) として表される。共有プロセスは以下の通りである。

- ✓ プロセスは「登録」、「審査」、「共有」の 3 ステップで構成される。
- ✓ 「審査」の結果は、ポータルサイトにて提供者と受領者の間で共有される。

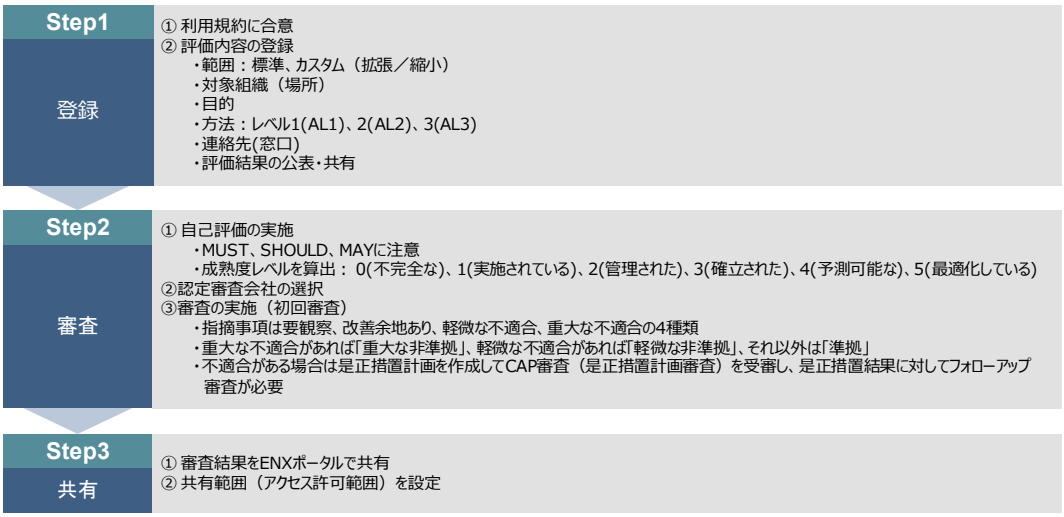


図 4-28　TISAX の登録から共有までのプロセス

- 管理目標と対策要件の概要

  TISAX の評価項目となる対策要件、及び ISO/IEC 27001, 27002 との対応関係は以下の通りである。

  ✓ マネジメント基準は ISO/IEC 27001 (ISMS) に集約している。

  ✓ 具体的対策要件基準は ISO/IEC 27002 に基づいて定めている。

No.	評価カテゴリ	評価項目名	項目数	ISO/IEC 27001, 27002の管理策	
				区分	対応する要求事項
1	情報セキュリティ	1 ISMS	3	27001	4(組織の状況) 5.1(リーダーシップ及びコミットメント) 6.1.2(情報セキュリティリスクアセスメント) 8.1(運用の計画及び管理) 8.2(情報セキュリティリスクアセスメント) 9.1(監視，測定，分析及び評価) 10.1(不適合及び是正処置) 10.2(継続的改善)
2		5 情報セキュリティ方針	1	27002	5.1.1(情報セキュリティのための方針群) 5.1.2(情報セキュリティのための方針群のレビュー)
3		6 情報セキュリティの組織	4		6.1.1(情報セキュリティの役割及び責任) 6.1.5(プロジェクトマネジメントにおける情報セキュリティ) 6.2.1(モバイル機器の方針) 6.2.2(テレワーキング)
4		7 人的資源のセキュリティ	2		7.1.2(雇用条件) 7.2.1(経営陣の責任) 7.2.2(情報セキュリティの意識向上，教育及び訓練) 7.3.1(雇用の終了又は変更に関する責任)
5		8 資産管理	4		8.1.1(資産目録) 8.1.2(資産の管理責任) 8.1.3(資産利用の許容範囲) 8.1.4(資産の返却) 8.2.1(情報の分類) 8.2.2(情報のラベル付け) 8.2.3(資産の取扱い) 8.3.1(取外し可能な媒体の管理) 8.3.2(媒体の処分) 8.3.3(物理的媒体の輸送)
6		9 アクセス制御	6		9.1.2(ネットワーク及びネットワークサービスへのアクセス) 9.2.1(利用者登録及び登録削除) 9.2.2(利用者アクセスの提供) 9.2.3(特権的アクセス権の管理) 9.2.4(利用者の秘密認証情報の管理) 9.2.5(利用者アクセス権のレビュー) 9.3.1(秘密認証情報の利用) 9.4.3(パスワード管理システム) 9.4.1(情報へのアクセス制限) 9.4.2(セキュリティに配慮したログオン手順)
7		10 暗号	1		10.1.1(暗号による管理策の利用方針)
8		11 物理的・環境的なセキュリティ	4		11.1.1(物理的セキュリティ境界) 11.1.2(物理的入退管理策) 11.1.4(外部及び環境の脅威からの保護) 11.1.6(受渡場所) 11.2.5(資産の移動) 11.2.6(構外にある装置及び資産のセキュリティ) 11.2.7(装置のセキュリティを保った処分又は再利用)
9		12 運用のセキュリティ	9		12.1.2(変更管理) 12.1.4(開発環境，試験環境及び運用環境の分離) 12.2.1(マルウェアに対する管理策) 12.3.1(情報のバックアップ) 12.4.1(イベントログ取得) 12.4.2(ログ情報の保護) 12.4.3(実務管理者及び運用担当者の作業ログ) 12.6.1(技術的ぜい弱性の管理) 12.6.2(ソフトウェアのインストールの制限) 12.7.1(情報システムの監査に対する管理策) 18.2.3(技術的順守のレビュー)
10		13 通信のセキュリティ	5		13.1.1(ネットワーク管理策) 13.1.2(ネットワークサービスのセキュリティ) 13.1.3(ネットワークの分離) 13.2.1(情報転送の方針及び手順) 13.2.3(電子的メッセージ通信) 13.2.4(秘密保持契約又は守秘義務契約)
11		14 システムの調達・開発・保守運用	4		14.1.1(情報セキュリティ要求事項の分析及び仕様化) 14.1.2(公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮) 14.1.3(アプリケーションサービスのトランザクションの保護) 14.2.1(セキュリティに配慮した開発のための方針) 14.2.2(システムの変更管理手順) 14.2.3(オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー) 14.2.4(パッケージソフトウェアの変更に対する制限) 14.2.5(セキュリティに配慮したシステム構築の原則) 14.2.6(セキュリティに配慮した開発環境) 14.2.7(外部委託による開発) 14.2.8(システムセキュリティの試験) 14.2.9(システムの受入れ試験) 14.3.1(試験データの保護)
12		15 供給者との関係	2		15.1.1(供給者関係のための情報セキュリティの方針) 15.1.2(供給者との合意におけるセキュリティの取扱い) 15.1.3(ICTサプライチェーン) 15.2.1(供給者のサービス提供の監視及びレビュー)
13		16 情報セキュリティ事故管理	2		16.1.1(責任及び手順) 16.1.2(情報セキュリティ事象の報告) 16.1.3(情報セキュリティ弱点の報告) 16.1.4 (情報セキュリティ事象の評価及び決定) 16.1.5(情報セキュリティインシデントへの対応) 16.1.6(情報セキュリティインシデントからの学習) 16.1.7(証拠の収集)
14		17 事業継続マネジメントにおける情報セキュリティ	1		17.1.1(情報セキュリティ継続の計画) 17.1.2(情報セキュリティ継続の実施) 17.1.3(情報セキュリティ継続の検証，レビュー及び評価) 17.2.1(情報処理施設の可用性)
15		18 コンプライアンス	4		18.1.1(適用法令及び契約上の要求事項の特定) 18.1.2(知的財産権) 18.1.3(記録の保護) 18.1.5(暗号化機能に対する規制) 18.1.4(プライバシー及び個人を特定できる情報（PII）の保護) 18.2.1(情報セキュリティの独立したレビュー) 18.2.2(情報セキュリティのための方針群及び標準の順守) 18.2.3(技術的順守のレビュー)
16	サードパーティーへの対応	23 サードパーティーへの対応	4		7.2.1(経営陣の責任) 7.2.2(情報セキュリティの意識向上，教育及び訓練) 9.2.1(利用者登録及び登録削除) 9.2.2(利用者アクセスの提供) 9.2.4(利用者の秘密認証情報の管理) 9.2.5(利用者アクセス権のレビュー) 11.1.1(物理的セキュリティ境界) 11.1.2(物理的入退管理策) 13.1.3(ネットワークの分離)
17	データの保護	24 データの保護	4		※ドイツ連邦データ保護法(BDSG)の第3条9項「特殊タイプ」と第11条「受注処理」に対応している
18	試作品の保護	25 試作品の保護 ※ 25.3「試作品の扱い」はTISAX独自 試作品保護のための最低限の物理的・環境的セキュリティ要件の決定、 試作品利用者の制限、試作品利用環境の監視、など	22		7.2.1(経営陣の責任) 7.2.2(情報セキュリティの意識向上，教育及び訓練) 8.2.2(情報のラベル付け) 11.1.1(物理的セキュリティ境界) 11.1.2(物理的入退管理策) 11.1.3(オフィス，部屋及び施設のセキュリティ) 11.1.5(セキュリティを保つべき領域での作業) 13.2.4(秘密保持契約又は守秘義務契約) 15.1.1(供給者関係のための情報セキュリティの方針) 15.1.2(供給者との合意におけるセキュリティの取扱い) 15.1.3(ICTサプライチェーン)

図 4-29　TISAX 評価項目と ISO/IEC 27001, 27002 の関係

4.3.2.2.2 SAE J.3061

SAE J.3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems に関する調査結果を以下に示す。

- 背景・目的

  SAE J.3061 は、SAE（米国自動車技術者協会: Society of Automotive Engineers）が、2016 年 1 月に公開した世界初の自動車産業向けのサイバーセキュリティガイドブックである。SAE は、1905 年に設立されたモビリティ専門家の米国の非営利団体であり、2016 年現在、約 110 ヵ国 14.5 万人以上の会員がいる。

  サイバーセキュリティは自動車業界にとって比較的新しいが重要な分野であり、自動車が他者に悪用される可能性を最小限に抑えつつ、新たな機能・サービスを実装する統合的システム設計のためのベストプラクティスを提供する目的で作成された。

  本ガイドブックに基づく認証取得制度はないが、NHTSA（米国運輸省道路交通安全局: National Highway Traffic Safety Administration）により参照が推奨されている。

- 基本コンセプト

  ✓ <u>自動車のサイバーセキュリティ構築のためのプロセス・フレームワーク</u>

  自動車製品の企画（コンセプト設計）、製品開発、生産、運用・サービス、廃棄までのライフサイクル全体で、サイバーセキュリティを構築するためのプロセス・フレームワークを定義している。また、ベストプラクティスとして自動車のサイバーセキュリティに関する基本理念・原則、設計・検証のためのツールや方法論といった各種情報を提供している。

  ✓ <u>機能安全規格との整合性に関する留意</u>

  自動車の機能安全要件との整合性に留意しており、特に ISO 26262 Road vehicles -Functional safety-、と矛盾なく整合するように、各フェーズでの対策内容を同期・調整している。逆に ISO 26262-2 の改訂に向けたドラフト版や SAE J. 3138:2018 において本規格が参照され整合が図られている。

- 想定されるステークホルダー

  SAE J.3061 では、直接的には自動車プロダクトの最終責任を持つ自動車メーカー（OEM）を対象とする。ただし、セキュリティ対策要求事項は自動車製品のライフサイクルすべてに言及されるため、ハードウェアやソフトウェアを供給するサプライヤーも自身の責任範囲においての準拠が求められる。

- 管理目標と対策要件の概要

  SAE J.3061 で規定される自動車のサイバーセキュリティを構築するフレームワークとプロセスの概要は以下の通りである。

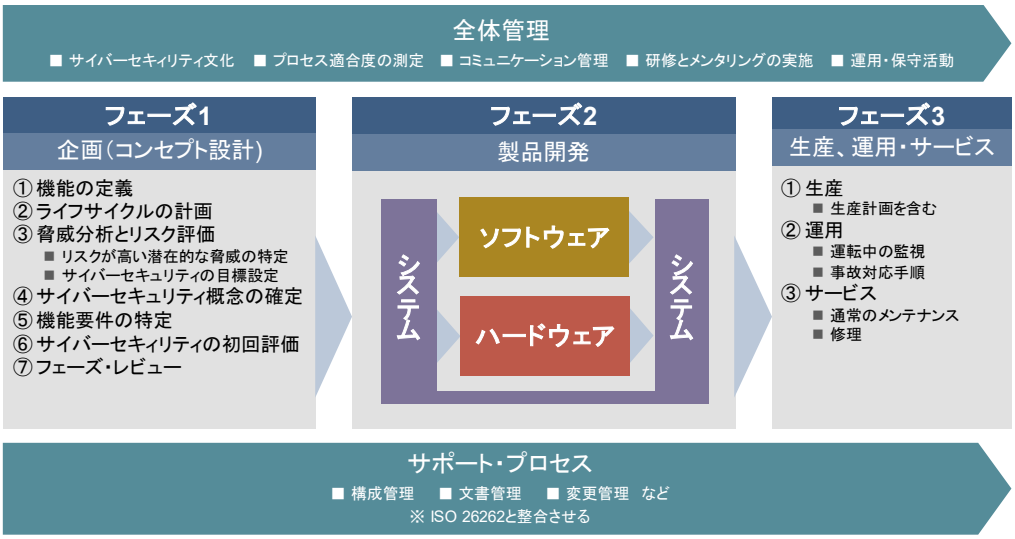


図 4-30　フレームワークの概要

さらに、フェーズ 2 の製品開発では、ウォーターフォール型の V 字開発モデルを想定して、システム・ハードウェア・ソフトウェアの 3 段階レベルで分類し、企画・要件定義・設計・実装・テスト・確認・評価の各プロセスにおける要求事項を定義している。

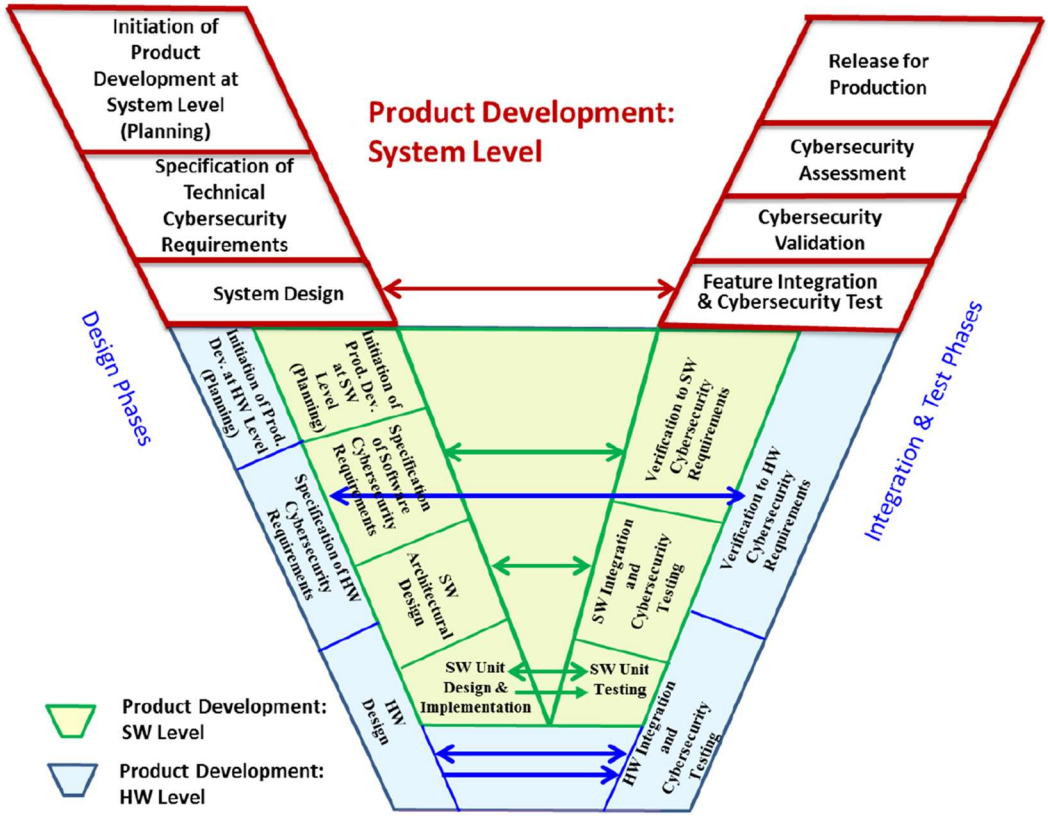


図 4-31　フェーズ 2「製品開発」のプロセス[2]

また、対策ガイドの構成と参照する関連規格は以下の通りである。

[2] SAE International, J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, Page 26 of 128 Figure 5, 2019/2/26

番号	内　容	番号	内 容
第1章	適用範囲	付録A	サイバーセキュリティ解析手法の説明
第2章	参照情報	付録B	作業成果物テンプレート例
第3章	定義および略語	付録C	解析手法の使用例
第4章	システム安全性とシステム・サイバーセキュリティの関係	付録D	セキュリティとプライバシーの制御に関する説明と実装
第5章	自動車システムにおけるサイバーセキュリティのガイド指針	付録E	脆弱性データベースと脆弱性分類体系
第6章	サイバーセキュリティのプロセス概要	付録F	車両レベルでの考慮事項
第7章	サイバーセキュリティの全体的な管理	付録G	自動車業界に役立つ可能性がある現在のサイバーセキュリティ基準とガイドライン
第8章	プロセス実装	付録H	自動車に関するプロジェクトの状況
第9章	注意事項	付録I	自動車業界で使用される可能性のあるセキュリティ試験ツール

図 4-32　対策ガイドの構成

No.	参照規格	
1	ISO/IEC/IEEE 29119 : 2013	Software and Systems Engineering – Software Testing
2	ISO/IEC 12207 : 2008	Systems and Software Engineering – Software Life Cycle Processes
3	ISO/IEC 15408 : 2008（R2014）	Information Technology – Security Techniques – Evaluation Criteria for IT Security
4	ISO/IEC 15408 : 2009（R2015）	
5	ISO TS 16949 : 2009	Quality Management Systems – Particular Requirements for the Application of ISO 9001:2008 for Automotive Production and Relevant Service Part Organizations
6	ISO 26262 : 2011	Road vehicles – Functional safety
7	ISO/IEC 27001 : 2013	Information Technology – Security Techniques – Information Security Management System - Requirements
8	ISO/IEC 27002 : 2013	Information Technology – Security Techniques – Code of Practice for Information Security Controls
9	AIAG QS 9000 : 3ED 98	Quality System Requirements

図 4-33　ガイド内で参照される関連規格

4.3.2.2.3 ISO/SAE 21434

ISO/SAE 21434: Road Vehicles - Cybersecurity Engineering に関する調査結果を以下に示す。

- 背景・目的

  自動車業界の車載電気・電子システムの機能安全に係る標準規格としては「ISO 26262: Road vehicles - Functional safety」が従来策定されていたが、サイバーセキュリティへの対応は不十分であると考えられていた。2016 年 9 月に ISO と SAE は PSDO（協力協定: Partnership Standards Development Organization）を締結し、SAE J.3061 を ISO に組み込む方針を合意した。

  ISO / TC 22 / SC 32 / WG 11 で四つの PG に分かれ、ISO と SAE の双方からメンバーが参加して規格内容を検討している。2020 年 5 月の出版が予定されている。

- 基本コンセプト

  ✓ <u>SAE J.3061 をベースとした規格体系</u>

  ISO 26262 での対応が不十分と考えられる自動車におけるサイバーセキュリティ対策を SAE J.3061 をベースとした内容で整備することを検討しており、本編 10 章と付録で構成される予定（約 200 ページ前後の予定）。

  ✓ <u>自動車のライフサイクル全体のサイバーセキュリティ活動を規定</u>

  自動車の企画（コンセプト設計）、製品開発、生産、運用・サービス、廃棄まで、

ライフサイクル全体のサイバーセキュリティに関する活動を規定。

- 想定されるステークホルダー
  SAE J.3061 と同様に、ISO/SAE 21434 も直接的には自動車プロダクトの最終責任を持つ自動車メーカー（OEM）を対象とし、サプライヤーも自身の責任範囲においての準拠が求められる。ただし、ISO/SAE 21434 は国際規格に位置付けられるため、本規格を基にした第三者認証の検討等、より公的な権威のある形で普及する可能性がある。

- 管理目標と対策要件の概要
  ISO/SAE 21434 の規格構成は SAE J.3061 の基本構成を踏襲する形で整理されることが予定されている。マネジメント規格として、全体管理体系とリスク管理を定義した上で、企画や開発等のプロセス毎に具体的な管理策を定める。

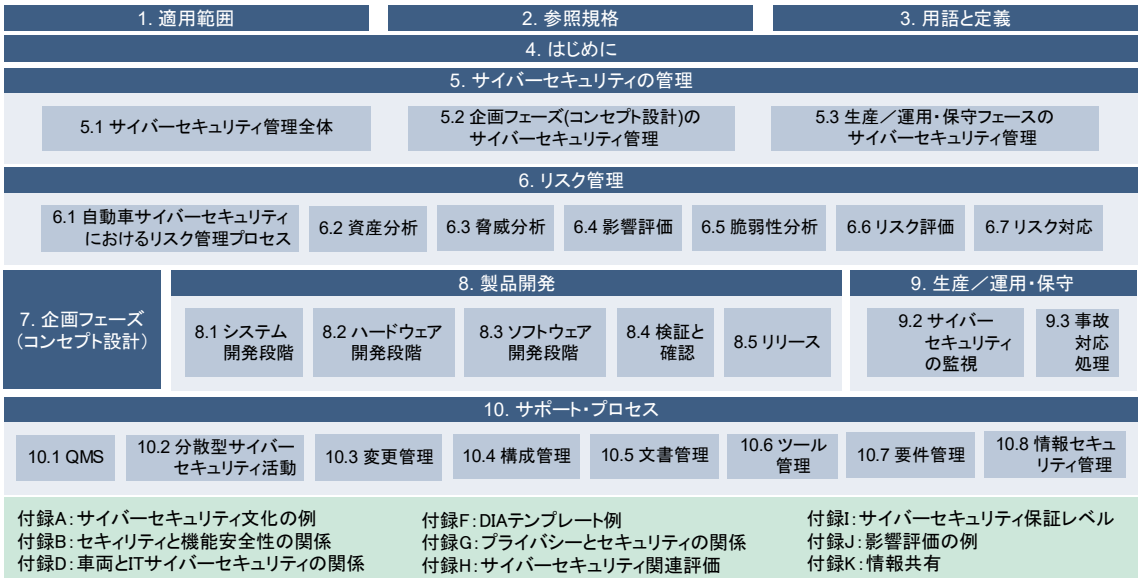


図 4-34　ISO/SAE 21434 の規格構成

各管理策の詳細な内容は現在議論の最中である。議論はライフサイクルのプロセス毎にわかれて行う形が基本となっているが、サポートプロセスの範囲の議論を行う PG4 において、相互依存がキーワードとなっていることは注目すべきポイントである。

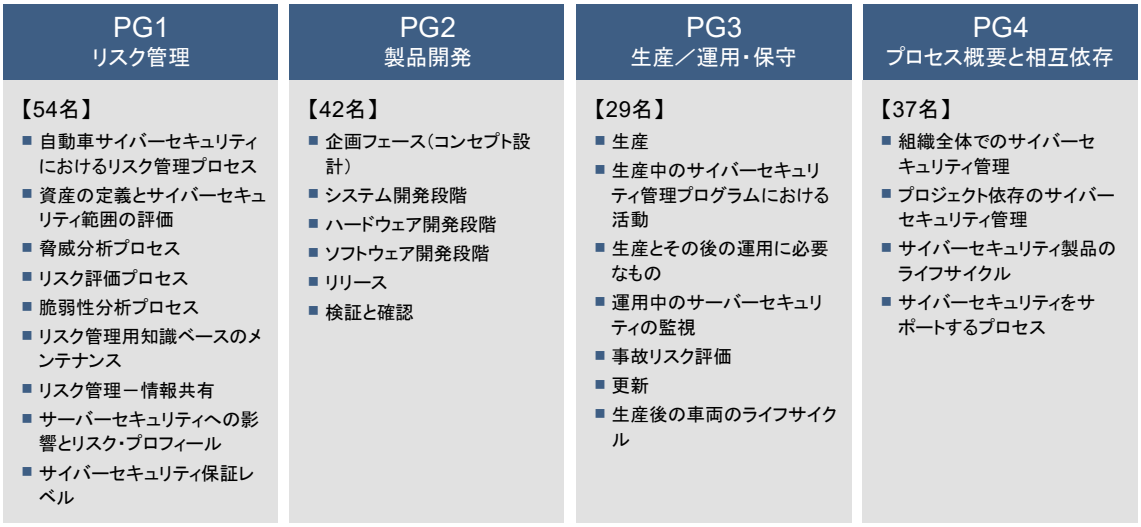


図 4-35　検討 PG の構成

4.3.2.2.4 AIAG Cyber Security 3rd Party Information Security

AIAG Cyber Security 3rd Party Information Security に関する調査結果を以下に示す。

- 背景・目的

  AIAG（全米自動車産業協会: Automotive Industry Action Group）は 1982 年に米国の 3 大自動車メーカー (General Motors、Ford、Chrysler) によって設立された協会である。現在は日本メーカーを含む約 800 社が参画している。

  AIAG の発行する規格は北米で事実上の自動車品質基準となっており、多くの自動車業界標準が策定、公表されている。

  AIAG は複雑化した自動車サプライチェーンでの情報共有に対応すべく、GM、Ford、FCA、ホンダと共同で、サプライヤー向けのサイバーセキュリティガイドラインを 2018 年 2 月に発表した。自動車産業においてサプライヤーが従うべき最小限の要件を示し、機密情報保護等を推進するものである。トヨタ、日産、Caterpillar、Bosch、Continental、Magna の各社とも提携している。

- 基本コンセプト

  ✓ <u>サプライヤーの情報管理に限定した最小限の規格</u>

  本規格では、自動車部品（プロダクト）そのものは対象外とし、情報セキュリティ管理要件を 9 カテゴリ 19 項目に整理している。

  ✓ <u>政府規格、国際標準規格をベースとした規格体系</u>

  NIST SP 800-53、NIST SP 800-171、ISO 27002 に対応した規格体系を構成している。3 規格の内容を基本とし、自動車メーカーのデータを作成、収集、処理、管理、アクセス、保存するサプライヤーのための安全な最小限の情報交換ガイドラインとして整理されている。

- 想定されるステークホルダー

  AIAG Cyber Security 3rd Party Information Security の主たる対象は自動車産業におけるサプライヤー事業者である。自動車メーカーの保有する情報のセキュリティを適切に管理するためにサプライヤーが本基準への準拠を示し、自動車メーカーが確認し、受け入れる形が標準的である。

- 管理目標と対策要件の概要

  AIAG Cyber Security 3rd Party Information Security の管理目標は九つの領域に分類される。ISO/IEC 27000 シリーズと同様に、情報セキュリティプログラムの枠組みを提示した上で、具体的な管理要件をそれぞれ定めている。

  また、NIST SP 800-171 と同様に、ステークホルダーをまたがって共有される重要な情報資産を保護することを目的としているため、具体的な製品へのセキュリティ要求事項ではなく、情報資産の管理のために必要となる対策要件が列挙されている。

  本規格の管理策は、NIST SP 800-53、NIST SP 800-171 との対応は示されているが、必ずしもすべての対策要件が合致するものではない。一方で、ISO/IEC 27002 の管理策に対してはすべての管理策がマッピングされている。

	管理要件	NIST 800-53	NIST 800-171	ISO 27002
1	➢ 情報セキュリティプログラム	○	△	○
2	➢ パスワード制御 ➢ 論理的アクセス制御 ➢ ネットワークと論理性 ➢ 暗号化 ➢ ネットワーク制御 ➢ 無線制御	○	○	○
3	➢ 物理的セキュリティ	○	○	○
4	➢ マルウェア対策設定	○	○	○
5	➢ 事故対応	○	○	○
6	➢ データの区分と保持 ➢ メディアの再利用と廃棄	○	×	○
7	➢ 外部監査とコンプライアンス	○	○	○
8	➢ コミュニケーション	×	×	○
9	➢ 変更・リリース管理 ➢ 構成管理 ➢ 可用性管理 ➢ 問題管理	○	△ （可用性管理が△）	○

図 4-36　AIAG Cyber Security 3rd Party Information Security の規格構成

4.3.2.2.5 UL VCSP

UL Vehicle Cybersecurity Program に関する調査結果を以下に示す。

- 背景・目的

  UL は 1894 年に電気製品の検査・試験のために設立された米国最古の安全規格開発機関である。現在は電気製品の他、産業機器や機械類全般、自動車部品、化学物質等、広範囲に及ぶ製品の検査・試験を実施している。試験・検査に合格した場合には UL 認証マークの表示を認可する。また、マーク発行リスト（UL リスト）を管理し利用者等に提供する。UL 認証は世界中で利用されており、現在は 104 ヵ国へ事業展開し、日本を含む世界 40 ヵ国以上に事業所や関連企業がある。

  UL は 2016 年 4 月に「Cyber Security Assurance Program, CAP」の一環として、ネットワーク接続可能製品のソフトウェア脆弱性へ対応するために UL 2900 シリーズを立ち上げた。UL 2900-1 は一般要求事項であり、ANSI（米国国家規格協会: American National Standards Institute）及び SCC（カナダ規格審議会: Standards Council of Canada）にも承認されている。

  自動車メーカーに対しても、脅威分析、リスク評価、脆弱性テスト及びセキュリティ保護対策の検証を通じてサイバーセキュリティリスクを最小限に抑えることを目的として、UL 2900-1 に基づいた Vehicle Cyber Security Program (VCSP) という UL 認証プログラムを提供している。

- 基本コンセプト

  ✓ <u>UL 2900-1 をベースとして自動車部品の脅威と脆弱性を評価</u>

  本規格では、ANSI 及び SCC にも承認されている UL 規格である UL2900-1 をベースとした検証を行うことを基本としている。蓄積されたノウハウを活用し、各種ツール・試験手法を駆使した効率的な評価・テストを行う。

  ✓ <u>自動車部品への脅威と脆弱性を評価</u>

  自動車部品への脅威と脆弱性に基づいた脆弱性評価プロセスを採用している。開発者によるリスク管理プロセス、部品・ソフトウェアにおける脆弱性対策やマル

ウェア対策、アーキテクチャや設計に起因するリスクの評価等を行う。ハードウェア、ソフトウェアともに機能要件の評価は対象外となる。

- 想定されるステークホルダー

UL VCSP は、自動車プロダクトのセキュリティ評価・検証を目的とするため、直接の対象は自動車メーカーとなる。ただし、ベンダー調達製品のリスク管理についても要求事項に含まれており、自動車メーカーはサプライヤーから調達した製品のリスクを管理することも要求される。

- 管理目標と対策要件の概要

UL VCSP では、アクセス制御やユーザー認証といった標準的な検証に加え、自動車ソフトウェアのセキュリティ要件に対する詳細な検証が行われる。既知の脆弱性に対する対策の試験、マルウェア対策試験等はツールを活用したシステマティックな評価を可能な限り行う。

区分	内　容	区分	内 容
序文		付録A	A1 ソフトウェアの弱点の情報源
序論	1 範囲 2 参照規格 3 用語集 4 製品、製品設計および製品利用の文書 5 製品設計の文書 6 製品利用の文書 7 リスク統制 8 アクセス制御、ユーザ認証およびユーザ権限 9 遠隔からの通信 10 機密データ 11 製品管理	付録B	B1 機密データと個人情報を保管する安全な仕組みのための要件
		付録C	C1 セキュリティ機能要件
リスク管理	12 ベンダー調達製品のリスク管理プロセス		
ソフトウェア及びそれ以外の脆弱性	13 既知の脆弱性に対するテスト 14 マルウェアに対するテスト 15 不正形式入力に対するテスト 16 構造化された侵入テスト		
ソフトウェアの弱点	17 ソフトウェアの弱点分析 18 静的ソースコード分析 19 静的バイナリ/バイトコード分析		

図 4-37　UL VSCP の要求事項構成

4.3.2.2.6 自動車分野におけるサイバーセキュリティの脅威と規格の対応

- 車の進化とサイバーセキュリティ

飛躍的な進化を続ける自動車産業は、自動運転を始めとして次世代技術への転換期を迎えている。車は IoT の一部となり、サイバーセキュリティの重要性は高まってきている。最近の車では IT サービスの利用が増加しており、クラウド経由で地図情報等と常時接続したり、スマートフォンと連携して様々な情報を利用している。

自動車の付加価値はこれまで自動車を製造する段階で設置される車載器によって決まっていたが、現在は各種の情報機器とそのデータによって絶えず変化している。いわゆる「つながる車（コネクテッドカー）」による新しい社会となった。車の電子化が進められ、つながることによって、利便性や快適性等の新しい価値を生み出すと同時に、新たに生じるサイバーセキュリティリスクへの対応が重要となってきた。

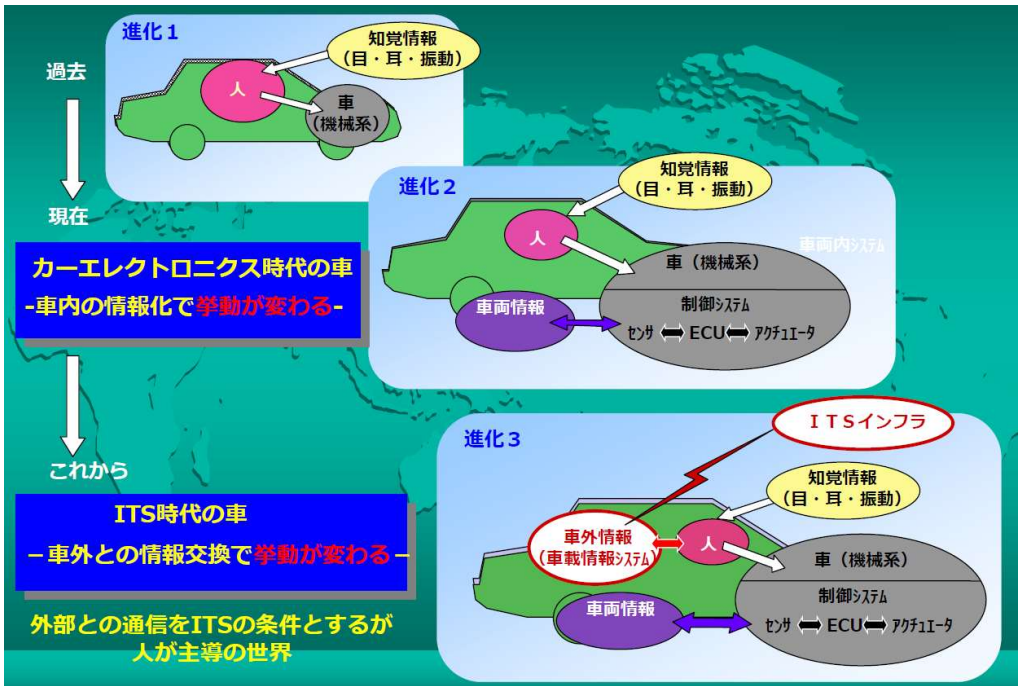


図 4-38　車の進化[3]

これまではメカニカルな鍵をコピーされて車両が盗難に遭ったり（車両盗難）、ドアの施錠機構を壊されて車内の金品を盗まれたり（社内物品盗難）、という物理的攻撃が主なものであり、イモビライザーの普及、車内侵入センサーの開発・法制化といった対応が取られてきた。

1970 年代以降は電子制御（コンピュータ制御）の普及により機器間でのデータ（情報）の通信が活発化し、情報の多様化・多量化へと変化してきた。車両内には通信線と電源線が張りめぐらされ、1 台の総延長は 3km を超えるといわれている。現在の車で使用されているコードは 1 台に 100 万行を超えることもある（ちなみにスペースシャトルは約 40 万行、F-35 戦闘機は約 2,500 万行、Windows XP は約 4,000 万行である）。これらのプログラムは利便性（ドライバーアシスタンス）やエンターテイメント、安全、車両管理等の便益をもたらしている。コネクテッドカーでは、行先、車内で過ごした時間、通話先、走行スピード、走行距離、各種警告ログ等、1 台で 1 日あたり 30 テラバイト程度のデータが生成されると推測されている。

自動車へのサイバー攻撃については、2010 年より研究や事故の報告が挙がり始めた。

- ✓ 2010 年: ワシントン大学の研究者により、自動車の CAN（車載 LAN: Controller Area Network）を悪用して様々な自動車の制御を乗っ取ることが可能であると発表された。
- ✓ 2010 年: 米国で遠隔イモビライザーを不正に起動することで自動車 100 台以上のエンジンがかからなくなり、警告ホーンが鳴り続けた。また、イモビライザーを解除する「イモビカッター」を悪用した自動車窃盗が発生した。
- ✓ 2011 年: CAN 以外の経路からの攻撃や脅威についても指摘され、無線通信プロトコル（Wi-Fi、Bluetooth）や IVI（In-Vehicle Information）で使用される CD や USB 等のメディア利用による脅威の可能性が示された。また、PKES（スマートキー: Passive Keyless Entry and Start）の脆弱性として、第三者が車のドア開錠やエンジンスタートできることも指摘された。
- ✓ 2014 年: Ford Escape や Toyota Prius に対して、車両内の CAN メッセージを不

[3] インターネット ITS 協議会: 2020 年の自動車社会とセキュリティ
https://www.ipa.go.jp/files/000037537.pdf、p.6 車の進化、2019/2/27

正に偽造して送信することにより脅威が実現することが報告された。

- ✓ 2015 年: Fiat Chrysler Jeep Cherokee に対するハッキング事例（制御自体の乗っ取り）が公表され、7 車種 140 万台に及ぶリコールが発生した。もし 1 台のリコールで 400 ドルかかると 140 万台では約 5 億 6,000 万ドルとなり、ブランドのダメージや訴訟を考慮すればその 2 倍、約 11 億ドルを超えるコストが 1 回のサイバー事故により発生する可能性がある。
- ✓ 2015 年以降: 超音波センサー、LIDAR (Light Detection and Ranging、Laser Imaging Dertection and rangong) やカメラ等のセンサー類を誤認識させた攻撃事例が報告されている。
- ✓ 2016 年: 自動車メーカーの提供するスマートフォン用アプリケーションの脆弱性を利用して、第三者が電気自動車のファンを遠隔で操作できることが示された。
- ✓ 2017 年: 車載情報端末である IVI の脆弱性が侵入口として狙われており、シェルスクリプトの実行等が報告されている。
- ✓ 2018 年: 以下の図 4-39 に示す。

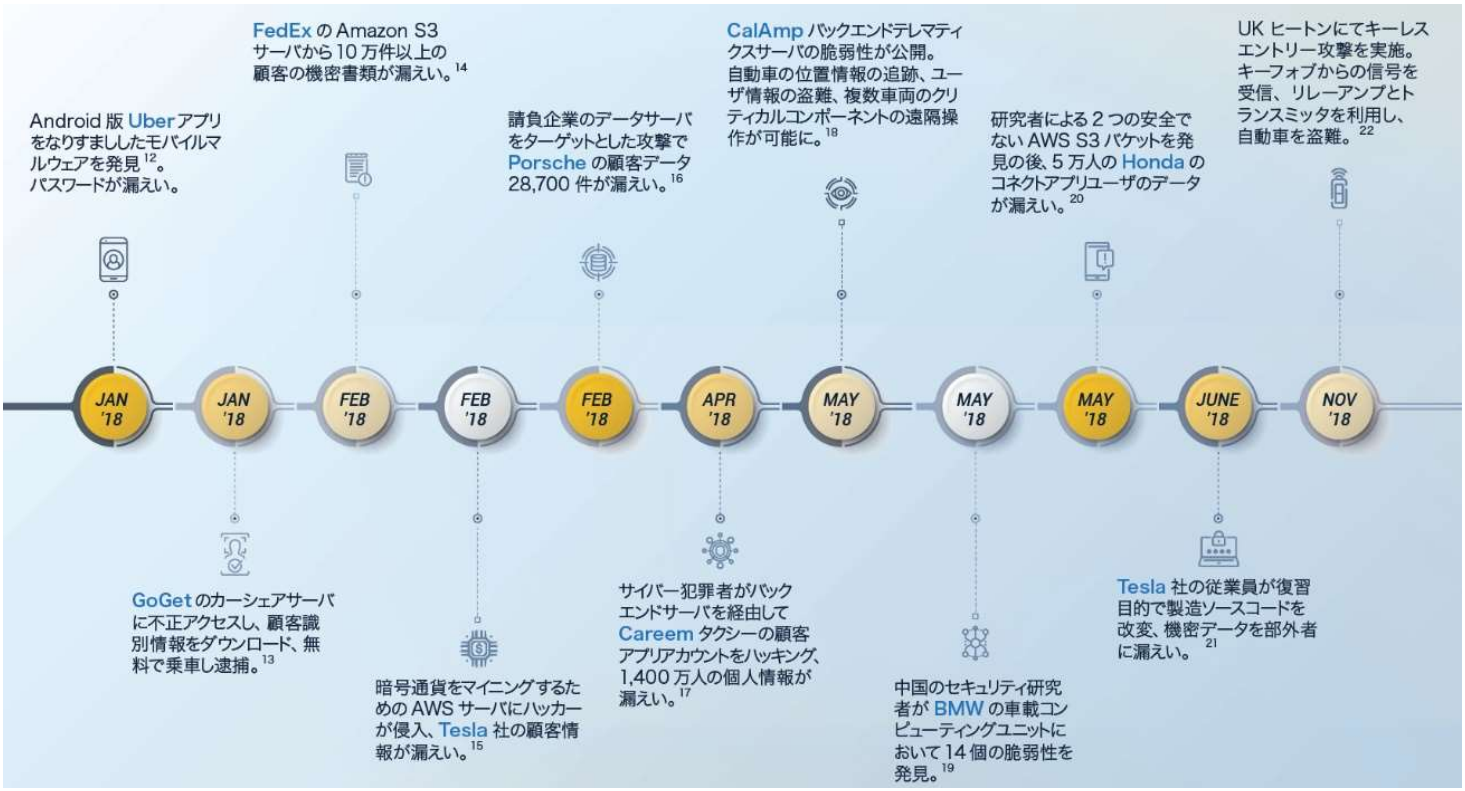


図 4-39　2018 年に発生した主な自動車サイバー事故[4]

2018 年に発生した事故は大きく 2 種類に分けられる。一つ目はモバイルアプリや Web ポータルといった自動車サービスに接続していた以前の車所有者が、サービスへのアクセス、データ閲覧、車の遠隔操作等をできてしまうもの、もう一つは利用者が自分のモバイルデバイスを情報システムと同期させているカーシェアやレンタカーサービスを通じてデータやプライバシーを侵害してしまうものである。

[4] Upstream: UPSTREAM SECURITY GLOBAL AUTOMOTIVE CYBERSECURITY REPORT 2019 スマートモビリティに対するサイバー攻撃トレンドの研究
https://www.upstream.auto/upstream-security-global-automotive-cybersecurity-report-2019/、p.8
2018 年に発生した主なサイバーインシデント、2019/2/27

自動車サイバーセキュリティを考える場合、その脅威や防御を多層構造として捉らえて検討する場合が多く、以下の 4 レベルは典型的なものである。

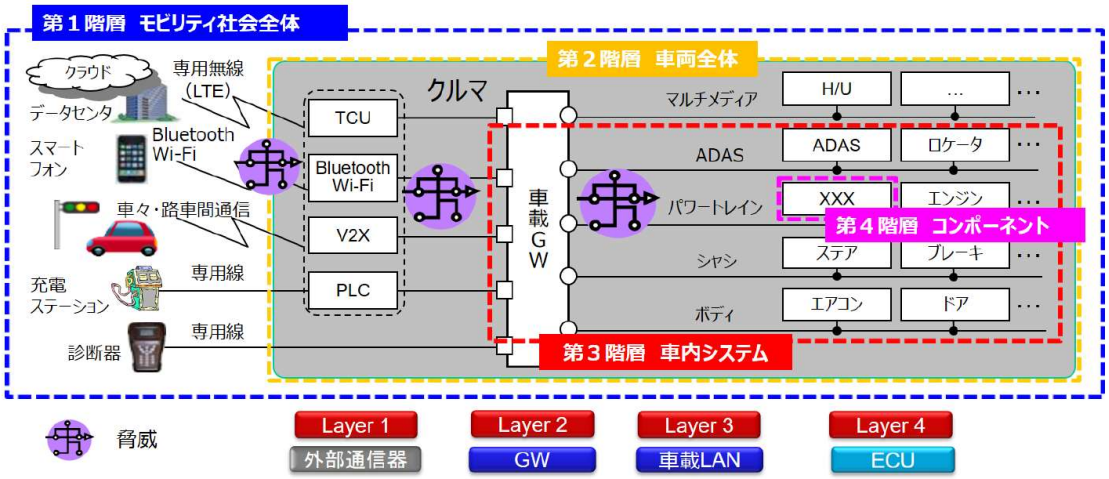


図 4-40　自動車サイバーセキュリティにおける脅威と防御の構造[5]

- ✓ 第 1 階層: クラウド等の社外通信システムを含むモビリティ社会全体であり、WiFi や Bluetooth 等の様々な無線通信手段の他、診断器や充電器等の物理的な接続もある。車車間通信や路車間通信も含まれる。安全な通信のための暗号化技術だけでなく、「正しい」情報を識別するためのサーバー認証やパケットフィルタリング等も必要となる。
- ✓ 第 2 階層: 物理的な車両全体であり、従来の制御系システム（＝「安全」・「品質」の確保）に加え、サイバーセキュリティの対象として情報系システムの脅威が高まっている。膨大なデータの統合・解析・監視・管理が必要となってきている。ネットワーク管理とともに ECU（制御用コンピュータ: Electronic Control Unit。1 台あたり数十個以上搭載されている）の認証やメッセージ認証、通信路（CAN、CAN-FD、Ethernet）暗号化等の技術が適用され、ファイアウォールやゲートウェイを備えている。
- ✓ 第 3 層: 車載ゲートウェイ以下の車内ネットワークであり、車の各種機能群を CAN で接続し、車載制御プロトコルを使用してデータ交換しており、IT 技術を駆使して機能の完全性・安全性を確保する必要がある。
- ✓ 第 4 層: ECU 等のコンポーネントであり、ハードウェアとソフトウェアからなる。ソフトウェアにおける不具合（バグ）が人命に関わる事故に至る可能性もあり、確実なプログラム更新が必要である。プログラム認証やデバイス認証、コンテンツ暗号化、鍵の機密性確保、セキュアブート等の技術が必要となる。

● サイバーセキュリティの脅威と規格・基準の普及

最近の自動車へのサイバー攻撃は、具体的にはどのような手法が取られているであろうか。図 4-41 は直近 10 年間、約 200 件のサイバー攻撃の方法をまとめている。

サイバー攻撃の 21.4%はサーバー攻撃であり、幅広い事故を網羅している。テレマティクスのサーバー、スマートモビリティアプリケーションサービス、自動車メーカー（OEM、Original Equipment Manufacturer）の Web サイトのような Web サーバーを含み、自動車、顧客、プログラムコード、運転者のデータを幅広くカバーしている。これらの攻撃はリモートで実施されており、車の近くで起こっているわけではない。

[5] 一般財団法人日本自動車研究所: 自動車セキュリティにおける課題と取組み http://www.jari.or.jp/Portals/0/resource/JRJ_q/JRJ20181101_q.pdf、p.2 図 2 セキュリティ防御の階層構造、2019/2/27

キーレスエントリーはサイバー犯罪者の注目を集めており、18.8%を占めている。ドアやイグニッションスイッチにキーを使用することなく車に侵入することができる。最近では2017年7月、スマートキーの信号を増幅したリレー攻撃でBMWが盗難に遭い、注目を集めている。2018年10月、セキュリティ研究者がTesla Model Sに対してキーレスジャミング（車のドアをロックする信号をブロック）を実施し、話題となった。

また、OBD（On-Board Diagnostics）ポートの悪用は10.5%あり、自動車本体と物理的に接続する攻撃である。自動車をマルウェアで感染させたり、悪意のあるCANメッセージをCANバスに送信する等がある。

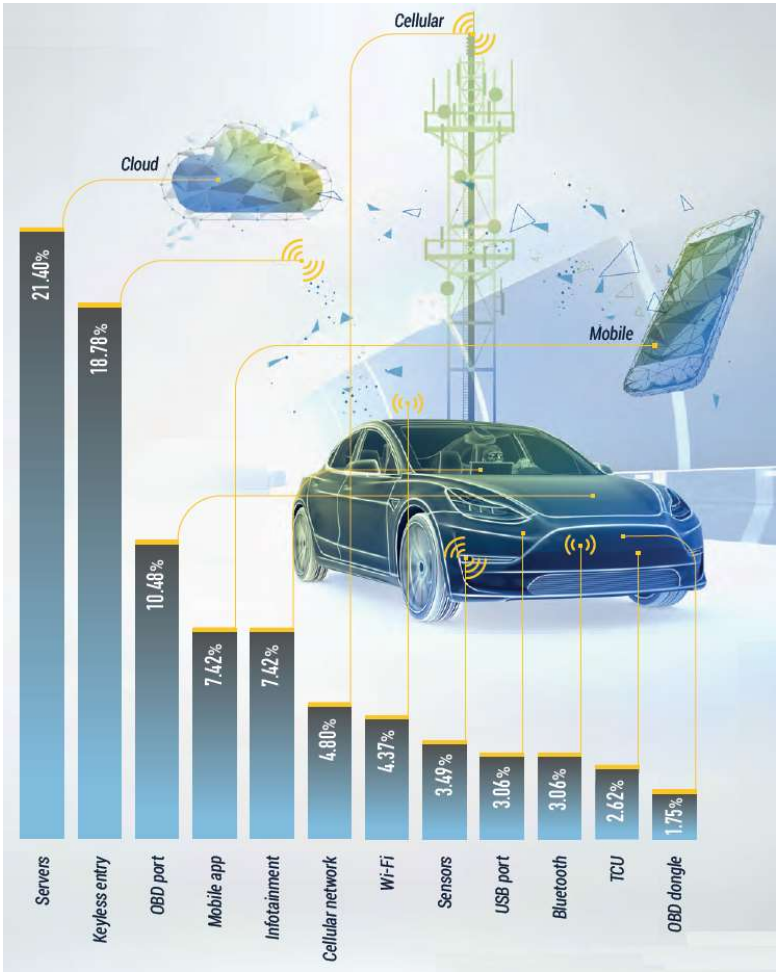


図 4-41　自動車へのサイバー攻撃[6]

これらのサイバー攻撃の対象（誰が影響を誰が受けているか）を調査すると、モビリティ社会のすべてのステークホルダーであり、サイバーセキュリティの脆弱性による危険にさらされている。具体的には、自動車メーカー（OEM）、サプライヤー企業、カーシェア会社、ライドシェア会社、フリート関連、鉄道会社、レンタカー会社、自動車販売店、緊急サービス、政府関連会社、保険会社、バイクシェアリング会社、公共交通等である。自動車の場合、製造から運用までステークホルダーが多岐にわたるため、サイバー攻撃が発生すると各ステークホルダーに被害が発生する。自動車メーカー（OEM）やサプライヤー企業は脆弱性

[6] Upstream: UPSTREAM SECURITY GLOBAL AUTOMOTIVE CYBERSECURITY REPORT 2019 スマートモビリティに対するサイバー攻撃トレンドの研究
https://www.upstream.auto/upstream-security-global-automotive-cybersecurity-report-2019/、p.11 スマートモビリティへの攻撃手法、2019/2/27

を回収するためにリコールしなければならない可能性があり、膨大なリコールコスト負担だけでなく信用失墜等のリスクがある。サイバー攻撃の影響は財務的なリスクだけでなく、人命に対する脅威でもあり、1 回のサイバー事故で運転手とその乗客だけでなく、歩行者や居合わせた人、他の運転手等の命を奪う可能性がある。

図 4-42 はサイバー攻撃による盗難、データ漏洩、詐欺等自動車へのハッキングの影響のインパクトを調査した結果である。最も大きな影響は制御システムの制御不能であり(27.6%)、自動車の安全性、つまりは人命を脅かし、壊滅的な影響を与える恐れがある。サイバー攻撃により事故が発生した場合、攻撃の際の証拠や履歴を十分に取っておかないと事故原因の分析ができず、その原因が運転手の操作誤りなのか、部品の故障なのか、サイバー攻撃の影響なのか判断がつかない可能性がある。自動車の運転者や所有者だけでなく、自動車保険会社にも関係するリスクである。

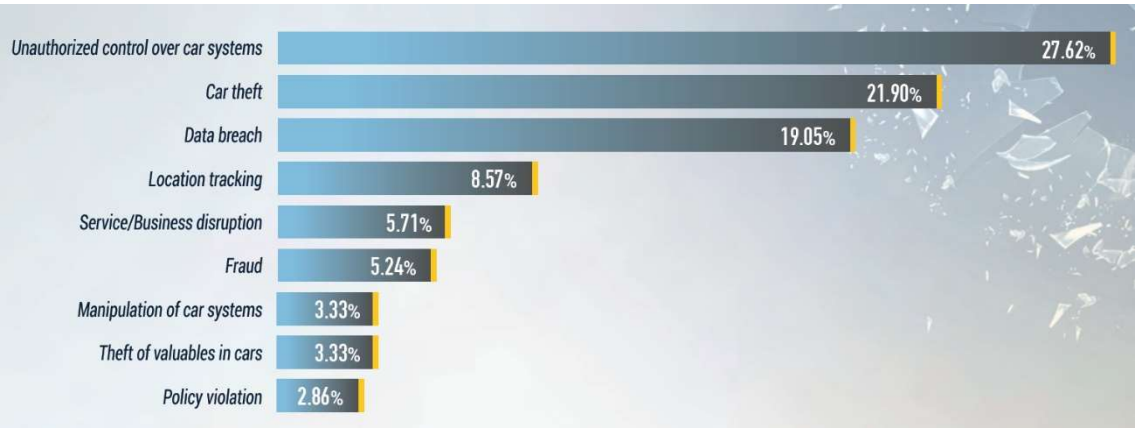


図 4-42　自動車業界への影響が大きなサイバー攻撃[7]

自動車へのサイバー攻撃への対策としては、自動車業界全体で、サプライチェーン全体を含む形での対応が必要であり、以下のようなものが検討されている。

- ✓ セキュリティ対策方針の策定: 市場・業界動向を把握し、規格・基準を踏まえて、既存の各種の会社ポリシーと整合するようにセキュリティ対策方針を策定し、最適な自動車のライフサイクル（企画・開発・製造から運用・廃棄まで）を実現する。
- ✓ 技術開発と情報共有: 人命の安全のための制御系システムと整合させた、財産・プライバシー保護にも対応する情報セキュリティ（情報系システム）の実装について、プロセスとプロダクトの両面から、各種の規格・基準を利用しながら IT 技術の車載適用を実現する。「車の進化とサイバーセキュリティ」で示した脅威と防御の 4 レベルそれぞれでの対応（多層セキュリティ基盤）が必要であり、境界セキュリティの向上、ウイルス対策ソリューション、クラウドセキュリティ、内部セグメンテーション技術等が重要なテーマとなっている。自動車のセキュリティを保つためには、安全と同様、サプライチェーン全体を可視化して管理を行うことが必要である。さらには運用フェーズも含め、自動車業界全体で情報共有できる体制の構築が望まれ、未知の脅威や脆弱性の発生に対して迅速な対策や被害拡散防止を図ることが検討されている。
- ✓ セキュリティ人材育成: 自動車のサイバーセキュリティ技術者は、制御システム（＝安全）と情報セキュリティの両方に精通する必要があり、圧倒的に不足している。例えば北米では学生教育と自動車脆弱性検査の両方を目的として、

[7] Upstream: UPSTREAM SECURITY GLOBAL AUTOMOTIVE CYBERSECURITY REPORT 2019 スマートモビリティに対するサイバー攻撃トレンドの研究 https://www.upstream.auto/upstream-security-global-automotive-cybersecurity-report-2019/、p.21 自動車業界における最もインパクトの大きいサイバー攻撃、2019/2/27

CyberAuto Challenge[8]が開催されている。また優秀な White Hat Hacker の協力の下、脆弱性分析・評価を行う仕組みの検討が必要かもしれない。

「車の進化とサイバーセキュリティ」で説明したように、自動車へのサイバー攻撃は 2010 年より研究や事故の報告が挙がり始めている。調査会社モルドール・インテリジェンスによると、自動車サイバーセキュリティの市場規模は、2017 年は 7,848 万ドルであったが、2023 年には 5 億 8,614 万ドルまで拡大すると予測されている（年平均成長率は約 50%）。

このように急速に拡大するサイバーセキュリティリスクの状況に対して、特に米国や英国で各種の法案が政府主導で検討される中、自動車業界においても自動車メーカー（OEM）主導で自主的なガイドラインを策定する動きが起こった。政府の規制が追いついてくる前に、業界や企業は自社のブランドと利益のために相応の投資を行ったのである。各種の規格・基準の対象は様々で、自動車業界の複雑なサプライチェーンや自動車のライフサイクルを考慮して、主として欧米から 2016 年以降多くが提案・公表された。これらはサイバー攻撃への対策としてその有効性が期待されている。

2016 年 9 月、NHTSA（米国運輸省道路交通安全局: National Highway Traffic Safety Administration）は自動運転車の開発指針「Federal Automated Vehicle Policy」を発表しているが、自動運転車の設計・開発に関する 15 項目の安全評価基準の中にはサイバーセキュリティ、データ保護、プライバシー保護等が含まれている。同年 10 月、NHTSA は自動車のサイバーセキュリティガイドラインとして「Cybersecurity Best Practices for Modern Vehicles」を引き続き発表した。これは、設計段階から自動車のサイバーセキュリティについて検討したり、機密データを保護したり、攻撃からの復旧方法を内蔵させること等を呼びかけている。

以降、様々な規格・基準が公開された。4.3.2.2　(1)～(5) で説明している、本研究で調査した自動車分野の TISAX、SAE J3061、ISO/SAE 21434、UL VCSP、AIAG Cyber Security の五つについて、その利用目的を図 4-43 に、適用対象と適用方法を図 4-44 に示す。サプライチェーンを含めた自動車業界全体の情報マネジメントとしては、ドイツを中心としたヨーロッパで普及している TISAX と、北米を中心に普及している AIAG Cyber Security が挙げられる。

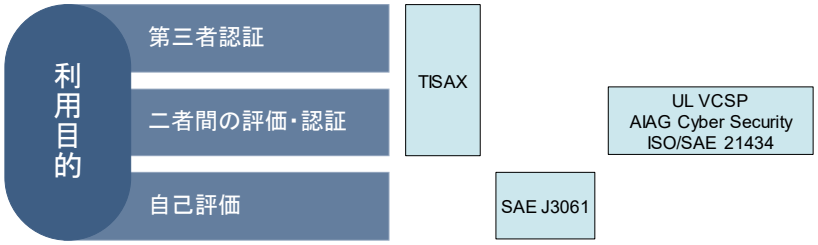


図 4-43　本研究で調査した自動車分野 5 規格・基準の利用目的

[8] SAE International: SAE CyberAuto Challenge™
http://www.sae.org/events/cyberauto/

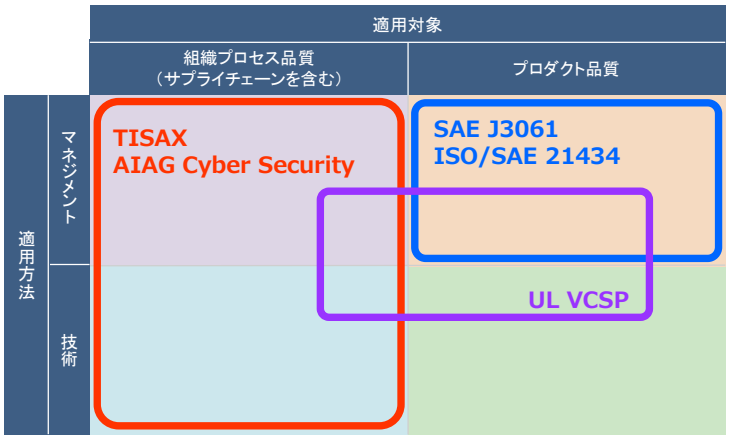


図 4-44　本研究で調査した自動車分野 5 規格・基準の適用対象と適用方法

現在は自動車メーカー（OEM）を対象にしたサイバーセキュリティ対策の義務化、法制度化が検討されており、自動車の開発段階（企画・開発）から製造・運用・廃棄までライフサイクル全体でセキュリティ診断・解析・評価が行われるようになるであろう。新たな脅威は常に進化を続けており、設計者・開発者とは異なる第三者による評価・診断が必要になるかもしれない。

4.3.2.3 電気通信分野向け規格

4.3.2.3.1 CTIA Cybersecurity Certification for IoT Devices

CTIA Cybersecurity Certification for IoT Devices に関する調査結果を以下に示す。

- 背景・目的

  CTIA Cybersecurity Certification for IoT Devices は、米国を中心として 1984 年に設立された、携帯電話等の移動体通信や無線通信等、300 以上の事業者が参画する国際的な業界団体 CTIA（Cellular Telecommunications & Internet Association）が策定した認証規格である。

  米国や EU 等で遠隔医療やコネクテッドカー等の IoT 機器の急成長によってセキュリティ問題が注目され、米国や英国等では各種の法案が検討される中、CTIA は AT&T、Sprint、Verizon、T-Mobile 等の通信事業者と共同で、NTIA（米国電気通信情報局: National Telecommunications and Information Administration）及び NIST（米国標準技術局: National Institute of Standards and Technology）のセキュリティ勧告に基づいて、業界主導で IoT 機器のサイバーセキュリティ認証プログラムを作成しリリースした（2018 年 10 月）。

  LTE または Wi-Fi を介してインターネットに接続する IoT 機器について、サイバーセキュリティ評価の要求事項、テスト等各種の認証取得プロセスを示し、CTIA に認定されたテスト施設でテストを実施して合格基準を満たせば認証が取得できるプログラムであり、レベル 1 から 3 までの 3 段階での認定を行う。

- 基本コンセプト

  ✓ <u>機器別・レベル別の評価と再認証の規定</u>

  評価対象 IoT 機器の特定のハードウェア／ソフトウェアのバージョン・モデル単位で個々に認証を付与する。機器のバージョンアップを行う場合は再度の認証が要求される。レベル別の評価テスト項目、認証費用は以下の通り（テスト費用は

各テスト施設に依存する）。
- レベル 1: 評価テスト項目は 6 種類、認証費用は 500 米ドル、
- レベル 2: 評価テスト項目は 13 種類、認証費用は 750 米ドル
- レベル 3: 評価テスト項目は 17 種類、認証費用は 1,000 米ドル
- バージョンアップ: 認証費用は 500 米ドル

✓ <u>評価基準の標準互換性</u>
評価テスト項目は他の標準規格を参照し、互換性が考慮されている。サプライチェーンセキュリティ対策に関しても同様である。参照される規格は、NIST SP 800 シリーズを中心に、CCS、ISO/IEC、RFC、FIPS、ISA 等との対応が言及される。

- 想定されるステークホルダー

CTIA Cybersecurity Certification for IoT Devices は、電気通信用途に供する消費者向け IoT デバイスの製造者（セットメーカー）を対象として想定した規格である。

- 認証体系と対策要件の概要

CTIA Cybersecurity Certification for IoT Devices の認証制度を体系化する文書の一覧は以下の通りである。

No.	文書名	内容	制定（Version 1.0）	最新版
1	IoT Cybersecurity Certification Program Management Document	認証の要求事項、認証のためのテスト等各種プロセス	2018年10月	同左
2	CTIA Cybersecurity Certification Test Plan for IoT Devices	レベル1から3までの各レベルにおけるテスト項目内容、テスト手順と合格基準	2018年8月	2018年10月（Version 1.0.1）
3	Policies and Procedures for CTIA Authorized Test Laboratories	CTIA認定テスト施設の要求事項、対応する認証制度、テスト実施方法 ※ テスト施設数は104（2019/2/19現在）	2012年1月	2019年2月（Version 1.8）

図 4-45　CTIA Cybersecurity Certification for IoT Devices の文書構成

✓ No.1 において認証制度の体系が定義される。No.2 の文書で規定される評価テスト項目と手順に従い、No.3 の文書で規定される CTIA 認定テスト施設においてテストを実施し、結果がすべて合格であった場合のみ、認証が認められる。
✓ 他の基準への適合・認証取得による試験の免除・省略は認められない。

CTIA Cybersecurity Certification for IoT Devices の評価テスト基準では、レベル毎に要求されるセキュリティ対策要件が異なる。セキュリティ対策要件の構成及び概要は以下の通りである。

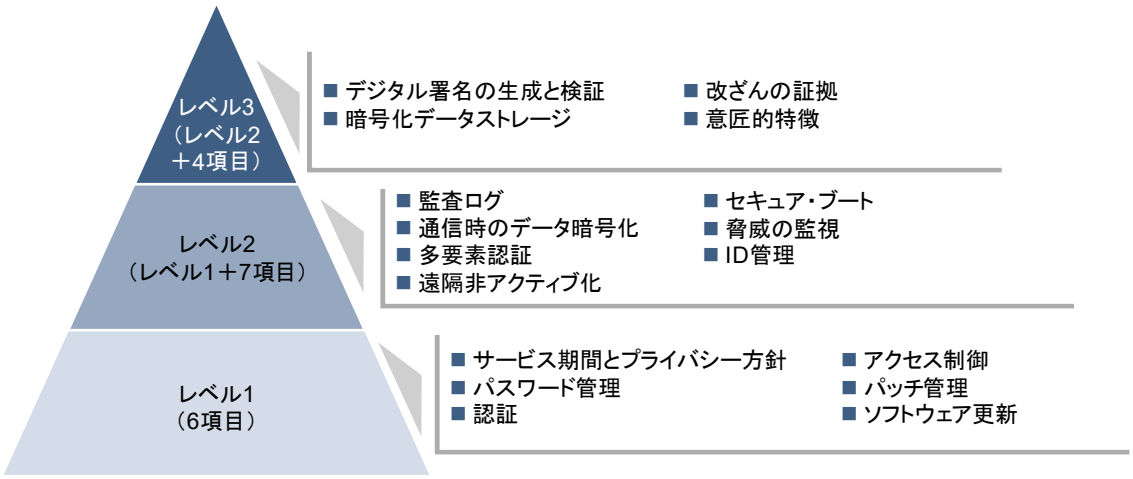


図 4-46　認証レベルと評価テスト項目の対応

No.	評価テスト項目	参照規格		
		レベル1（6項目）	レベル2（13項目）	レベル3（17項目）
1	サービス期間とプライバシー方針	CTIA Consumer Code for Wireless Service NIST SP 800-53 Rev.4	CTIA Consumer Code for Wireless Service NIST SP 800-53 Rev.4	レベル2に同一
2	パスワード管理	NIST SP 800-53 Rev.4 NIST SP 800-63B	ISO/IEC 27001:2013 NIST SP 800-63B	レベル2に同一
3	認証	CCS CSC NIST SP 800-53 Rev.4	CCS CSC ISO/IEC 27001:2013 NIST SP 800-53 Rev.4	レベル2に同一
4	アクセス制御	CCS CSC NIST SP 800-53 Rev.4	レベル1に同一	レベル2に同一
5	パッチ管理	CCS CSC NIST SP 800-53 Rev.4 NIST SP 800-40 Rev.3	CCS CSC NIST SP 800-53 Rev.4 NIST SP 800-40 Rev.3	CCS CSC ISO/IEC 27001:2013 NIST SP 800-53 Rev.4 NIST SP 800-40 Rev.3
6	ソフトウェア更新	CCS CSC NIST SP 800-53 Rev.4	CCS CSC NIST SP 800-53 Rev.4	CCS CSC ISO/IEC 27001:2013 NIST SP 800-53 Rev.4
7	監査ログ		CCS CSC ISA 62443-2-1 : 2009 ISO/IEC 27001:2013 NIST SP 800-53 Rev.4 NIST SP 800-92 RFC 5424 RFC 5425 RFC 6012	CCS CSC ISA 62443-2-1 : 2009 ISO/IEC 27001:2013 NIST SP 800-53 Rev.4 NIST SP 800-92 RFC 5424 RFC 6012
8	通信時のデータ暗号化		CCS CSC NIST CSF v1.1 NIST SP 800-53 Rev.4 NIST SP 800-113 FIPS PUB 197 RFC 5426 RRC 6012	レベル2に同一
9	多要素認証		CCS CSC NIST SP 800-53 Rev.4 NIST SP 800-463B	レベル2に同一
10	遠隔非アクティブ化		CCS CSC NIST CSF v1.1 ISO/IEC 27001:2013 NIST SP 800-53 Rev.4	レベル2に同一
11	セキュア・ブート		CCS CSC NIST SP 800-53 Rev.4 NIST SP 800-147	レベル2に同一
12	脅威の監視		ISO/IEC 27001:2013 NIST SP 800-53 Rev.4	レベル2に同一
13	ID管理		NIST SP 800-63B NIST SP 800 63-3	レベル2に同一
14	デジタル署名の生成と検証			NIST SP 800-25 NIST SP 800-49 NIST SP 800-53 Rev.4 NIST SP 800-89 FIPS PUB 186-4 RFC 5280 RFC 5652 RFC 5751
15	暗号化データストレージ			ISO/IEC 27001:2013 NIST SP 800-53 Rev.4 NIST SP 800-113 FIPS PUB 197
16	改ざんの証拠			NIST SP 800-53
17	意匠的特徴			NIST SP 800-53 NIST SP 800-160

図 4-47　評価テスト項目と各レベルでの参照規格

4.3.2.4 電力分野向け規格

4.3.2.4.1 NERC CIP

NERC CIP (Critical Infrastructure Protection Standards) に関する調査結果を以下に示す。

- 背景・目的

  米国の電力事業者向けのサイバーセキュリティ対策標準。発電・送電インフラの信頼性確保のための自主規制機関である NERC（北米電力信頼度協議会: North American Electric Reliability Corporation）によって策定された。チェックリスト方式で対策要件を構成しており、事業者が行うべき対策を明確にするとともに、対策の実施状況の評価を行いやすい形式となっている。

  本対策標準は米エネルギー省配下の FERC（米国連邦エネルギー規制委員会: Federal Energy Regulatory Commission）によって内容を承認された上で採択されており、電力事業者のサイバーセキュリティ対策の実施状況を評価するための公的基準と位置付けられる。FERC による規制は強制力を持った規制であるため、CIP 基準を満たさず、改善への取り組みが不十分と判断された事業者に対しては罰則が科される。

- 基本コンセプト
  - ✓ **電力系統への影響度に基づいた設備リスク基準**

    NERC CIP ver.5 では電力系統へ各電力関連設備が与える影響度の大きさを 3 段階別（高・中・低）に分類し、リスク評価の尺度として採用している。分類基準は極めて具体的なものであり、発電所の有効電力容量の数値等で判断を行う。

  - ✓ **チェックリスト型対策基準**

    本標準の各対策要件は「適用対象システム」、「具体的要求事項（チェック可能な形式）」、「効果測定・証跡確認のための手段」が整理されており、チェックリストとして利用しやすい形式にまとめられている。FERC によるアセスメントにおいても本対策基準に定められる手順により確認が行われる。

- 想定されるステークホルダー

  NERC CIP の想定するステークホルダーとその特徴は以下の通りである。
  - ✓ 政府関係機関による公的規制を中央集権型統制として実施する形式となっている。
  - ✓ チェックリスト形式の統一基準を用いることで各設備に対して、ある程度機械的にアセスメントを実施できる。
  - ✓ 規制への準拠に強制力があるため、各設備は確実に対応を行う必要がある。

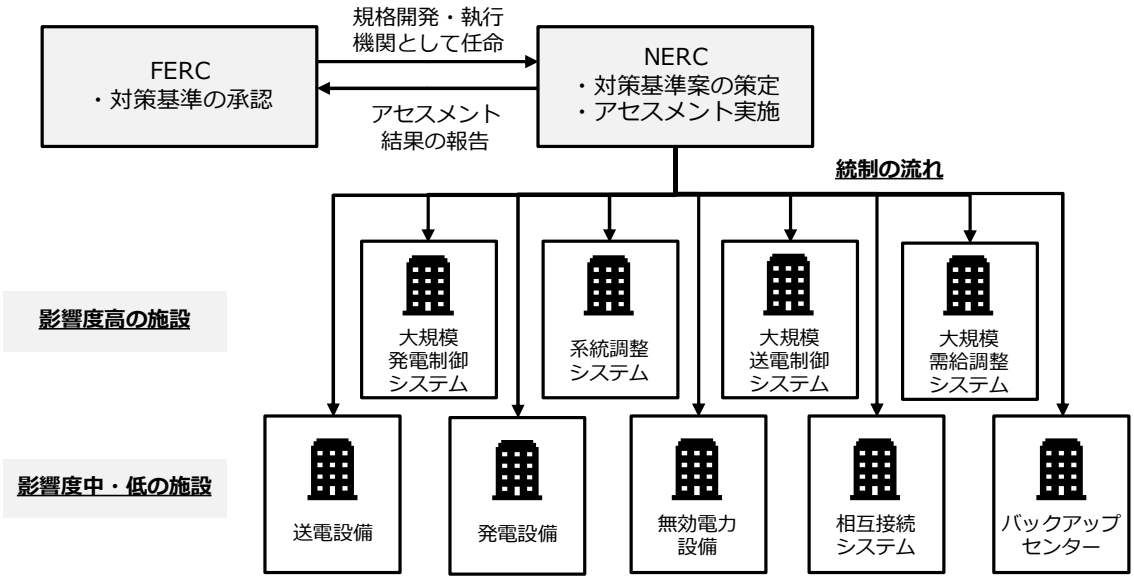


図 4-48　NERC CIP の想定するステークホルダー

- 管理目標と対策要件の概要

  NERC CIP の管理目標と対策要件の概要である。

  ✓ 電力設備の影響度別に実施すべき対策と実施状況の確認方法を明確化する。

  ✓ 電力事業者への対策浸透、規制の実施と違反時の罰則適用を統一的な基準によって遂行する。

  ✓ チェックの明確さを高めるために具体性の高い対策要求が記載されている。

  （例）「四半期に 1 回のセキュリティ研修開催」、「アクセス許可のための犯罪歴評価」、「15 カ月毎のアカウント正当性チェック」、「アクセス違反アカウントの 24 時間以内停止」、「物理セキュリティ境界侵害に対する 15 分以内の警報」、「物理的アクセスログの 90 日間保存」、「新規セキュリティパッチ適用を 35 日以内に評価」「パスワードに要求される文字数、文字種」、「15 カ月に一回以上のインシデント対応計画テスト」等

影響度評価の分類（CIP-002-5.1a）

影響	該当する設備の例
大	・系統信頼性制御センター ・3000MW以上の需給調整制御センター ・送電設備等の集中制御センター ・発電設備等の集中制御センター　など
中	・有効電力容量1500MW以上の発電所 ・無効電力1000MVAR以上の無効電力設備 ・500kV以上規模の送電設備 ・3変電所以上と接続する200kV以上の送電設備 ・相互接続の重要性を指摘された発送電設備 など
小	・大／中に該当しない電力設備

現在適用中の基準（CIP-00X-Y）
（X:基準の通番　Y:バージョン）

要件ID	セキュリティ対策要件（要件の例）
CIP-003-6	セキュリティマネジメントの管理（対策計画の策定・実施）
CIP-004-6	人的セキュリティと訓練の実施（アクセス制限、要員の教育）
CIP-005-5	電気的セキュリティ境界の保護（領域の決定、境界防御）
CIP-006-6	電力設備の物理セキュリティ（物理的アクセス制限、侵害通知）
CIP-007-6	システムセキュリティ管理（堅牢化、パッチ管理、不正検知）
CIP-008-5	インシデント対応計画（対応計画の策定・テスト・更新）
CIP-009-6	電力設備の復旧計画（復旧計画の策定・テスト・更新）
CIP-010-2	設定変更の管理と脆弱性の特定（構成管理、変更管理）
CIP-011-2	情報の保護（情報取扱い手続き、記録媒体の管理）
CIP-014-2	物理セキュリティ（送電設備の保護）

図 4-49　NERC CIP 対策要件の構成

- 特定技術の導入による要求事項免除の規定

  NERC CIP ver.5 では、単方向ゲートウェイ（Unidirectional gateway）を導入することにより 103 の要求事項のうち 37 事項が免除される。High Impact, Middle Impact System のうち、単方向ゲートウェイの導入により電子セキュリティ境界（Electronic

Security Perimeter）の外から双方向ルーティング可能な接続（External Routable Connectivity）を持たないようにすることで、免除される要求事項が規定されている。

Standard	Req	ERC Exempt	Remaining
002 BES Cyber System Categorization	7	-	
003 Security Management Controls	4	-	
004 Personnel & Training	19	16	3 HI only
005 Electronic Security Perimeters	8	6	ESP & dial-up
006 Physical Security	14	10	1 HI, process, mon, alert
007 Systems Security Management	20	5	
008 Incident Reporting & Resp. Planning	9	-	
009 Recovery Plans	10	-	
010 Change Mgmt & Vuln Assessments	10	-	
011 Information Protection	4	-	
Totals:	103	37	

図 4-50　単方向ゲートウェイ導入により免除される要求事項の数

CIP-005-5 Table R1 – Electronic Security Perimeter			
Part	Applicable Systems	Requirements	Measures
1.2	High Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA Medium Impact BES Cyber Systems with External Routable Connectivity and their associated: • PCA	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	An example of evidence may include, but is not limited to, network diagrams showing all external routable communication paths and the identified EAPs.

図 4-51　免除される要求事項の例[9]

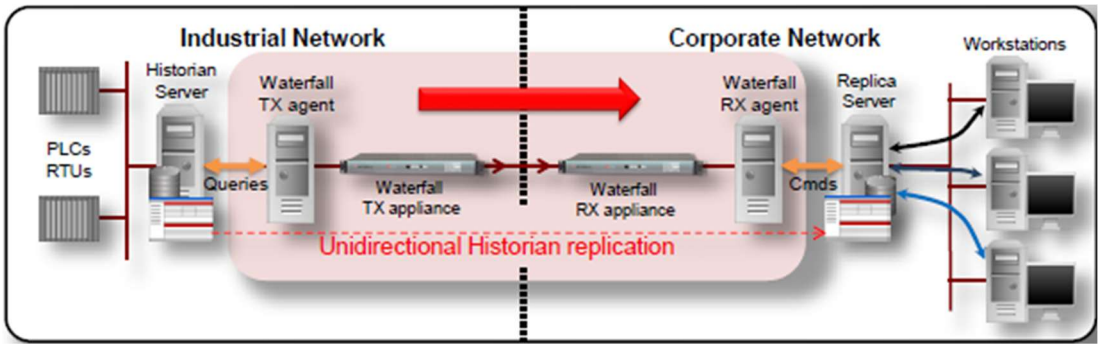


図 4-52　単方向ゲートウェイの利用例[10]

- サプライチェーン管理策の追加に関する動向の概要

  NERC では現在発効中の対策要件だけでなく、将来的な発効を検討している対策要件の情報を開示している。2019 年 2 月現在、既存対策要件の改訂に加え、サプライチェーンリスク管理に関する対策要件の素案を公開中である。

  Supply Chain Risk Management (CIP-014-1) の概要は以下の通りである。

  ✓ 各電力設備の管理者を「責任主体」として捉え、電力サプライチェーンのリスクを統合管理する狙いがある。

[9] NERC: CIP-005-5 - Cyber Security - Electronic Security Perimeter(s)
https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-005-5.pdf
[10] Waterfall 社 HP

- ✓ 系統信頼性の調整事業者、各種配電サービス提供者、発電システムの責任者、送電設備の責任者等が責任主体に該当する。
- ✓ CIP シニアマネージャによる確認が義務付けられるため、監査・認証に近い位置付けとも解釈できる。

要件ID	詳細対策要件
R1	各責任主体は以下に関するサプライチェーンセキュリティマネジメント計画を文書化すること ●電力システムの調達計画におけるサイバーセキュリティリスクの特定と評価 ・特に「ベンダー製品の調達とソフトウェアインストール」、「契約ベンダーの切替え・引継ぎ」のプロセスのリスク） ●電力システムの調達プロセスにおけるサプライチェーンリスク対応 ・ベンダーに求める対応の例 1．調達製品・サービスに関する当該ベンダー固有インシデント情報の通知（責任主体に影響のあるもの） 2．調達製品・サービスに関する当該ベンダー固有インシデントへの対応の調整 3．ベンダーの関係者ではなくなった者からのアクセス発生時のベンダーからの通知 4．調達製品・サービスに関する既知の脆弱性情報の提供 5．提供される全てのソフトウェア・パッチについての完全性と認可の検証 6．ベンダーからのリモートアクセス・ベンダーシステム間リモートアクセスの統制
R2	各責任主体は計画したサプライチェーンセキュリティ計画を実装すること
R3	各責任主体は計画したサプライチェーンセキュリティのレビューを行い、15カ月に一度以上の頻度でCIPシニアマネージャー等の確認をうけること

図 4-53　CIP-014-1 の要件 ID と詳細対策要件

4.3.3　アンケート調査

諸外国におけるサプライチェーンセキュリティ対策の実態と課題の把握を行うため、アンケートによる調査を行った。調査対象は、サプライチェーンセキュリティ対策基準類の策定元や適用先となる欧米諸国とした。調査仮説は、国内の事業者を対象とした類似の調査結果[11]等を参考に検討した。設問の設計にあたっては、対策基準の浸透状況、対策実施の効果と課題が残る点、特定産業分野向け基準の活用状況等に着目する方針とした。

4.3.3.1 アンケート実施計画

本調査におけるアンケートの実施計画と設問項目の概要は以下の通りである。

- 調査対象及び調査方式
  - ✓ 調査対象国: 米国、ドイツ、英国、フランス
  - ✓ 調査対象者: 企業の経営者、法務・監査部門、総務・調達部門、情報システム部門、セキュリティ部門の担当者
  - ✓ 調査対象業種: 情報通信、製造業（日用品）、製造業（機械・化学）、自動車、金融、電力、放送・メディア
  - ✓ 調査対象要件: 自社の情報セキュリティ対策を主導もしくは把握している者
  - ✓ 調査方式: Web アンケート
  - ✓ 調査期間: 2/14～2/28（15 日間）
  - ✓ 回収件数: 104 件（26 件×4 ヵ国）

- 設問項目の概要
  - ✓ 回答者の所属企業の業態等の基本情報
  - ✓ 各社が対策の採用・参考にしている基準
  - ✓ 各社・各業界が深刻と考えているセキュリティ脅威

[11] 情報処理推進機構「IT サプライチェーンの業務委託におけるセキュリティインシデント及びマネジメントに関する調査」(2018 年 3 月)

- ✓ 各社・各業界が深刻と考えているサプライチェーン脅威
- ✓ 各社が実際に取り組んでいる対策とその成熟度
- ✓ 取引先との契約書へ実際に織り込まれている項目
- ✓ 取引先の対策実施状況を重視している度合い
- ✓ 取引先の対策実態を把握している程度
- ✓ 取引先の対策実態把握のために行っている対応
- ✓ サプライチェーン対策を推進する上で課題に感じる点

4.3.3.2 アンケート調査結果

本調査におけるアンケート調査結果は以下の通りである。

- 全体調査結果
  - ✓ アンケート回答者の属性

  アンケート回答者の担当職務、所属企業の業種・業態、規模、委託元／委託先の区分に関する調査結果は以下の通りである。社としてのセキュリティ対策要件の把握を条件としたスクリーニングの結果として経営層による回答比率が高まったものと考えられる。

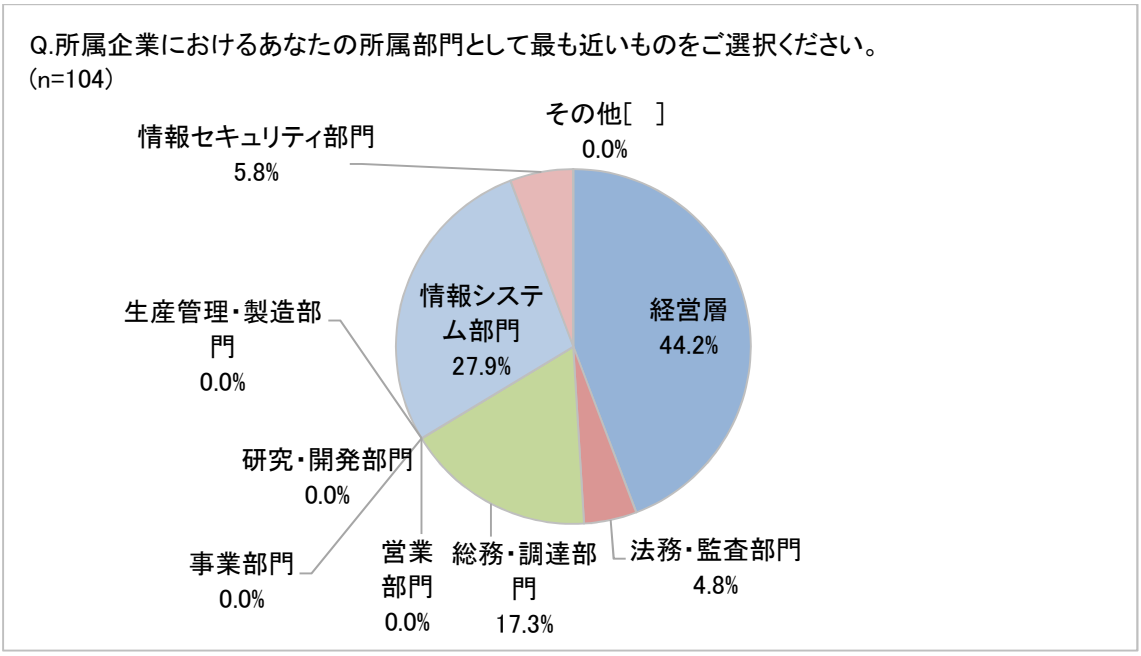


図 4-54 担当職務

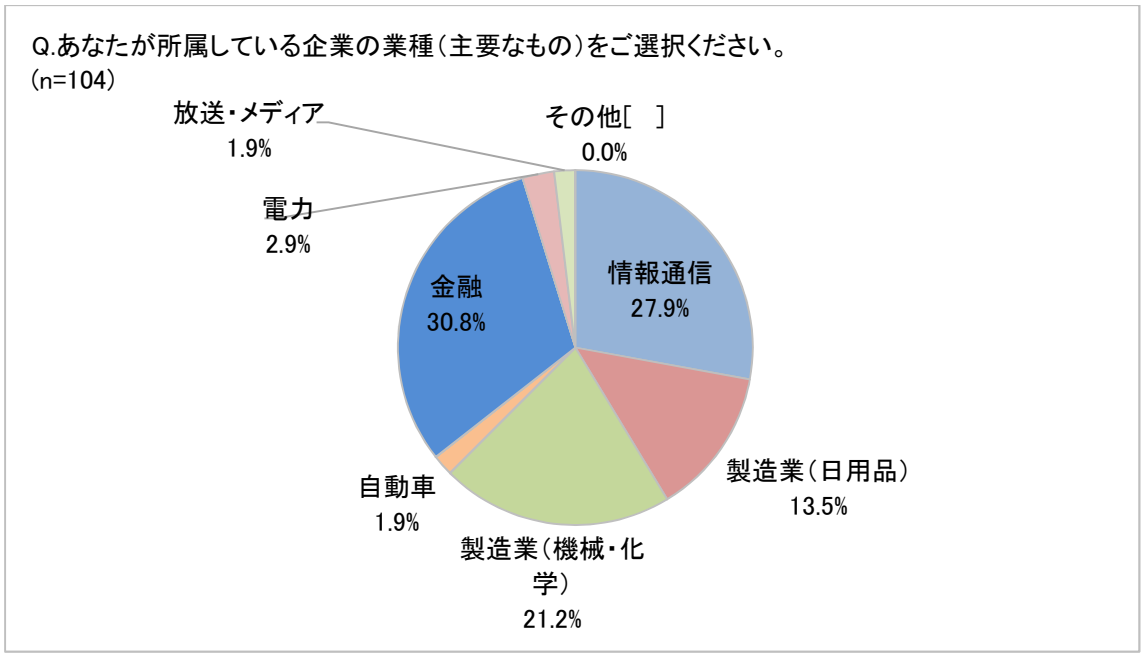


図 4-55　所属企業の業種

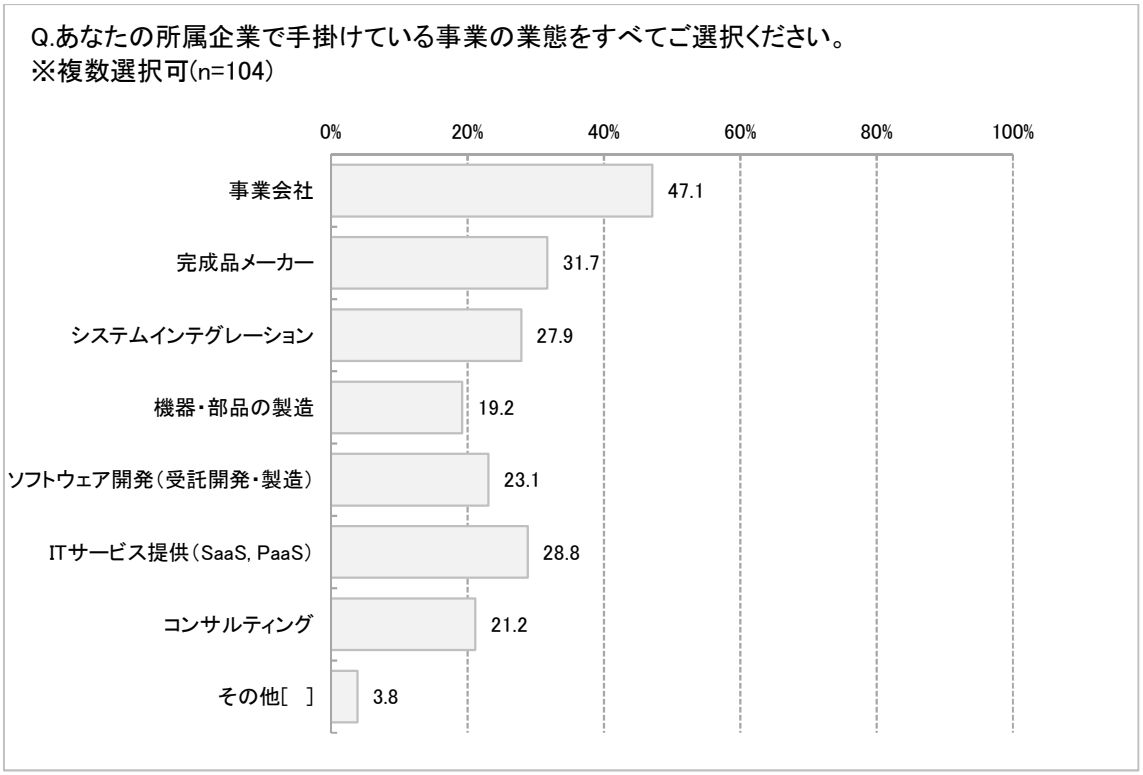


図 4-56　所属企業の業態

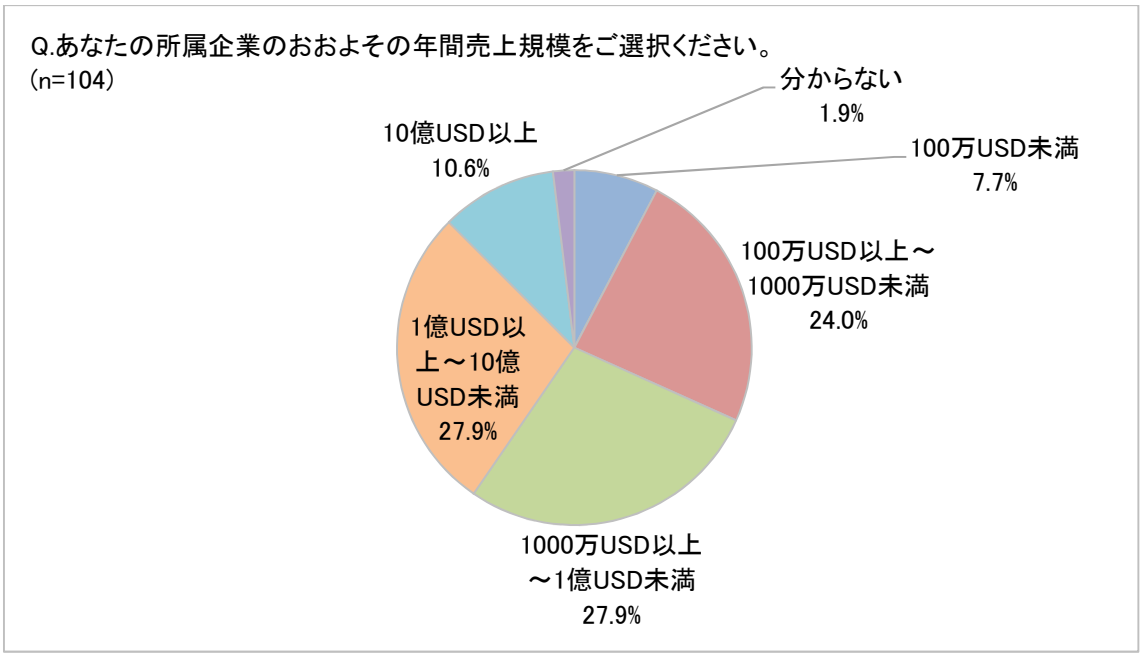


図 4-57　所属企業の事業規模

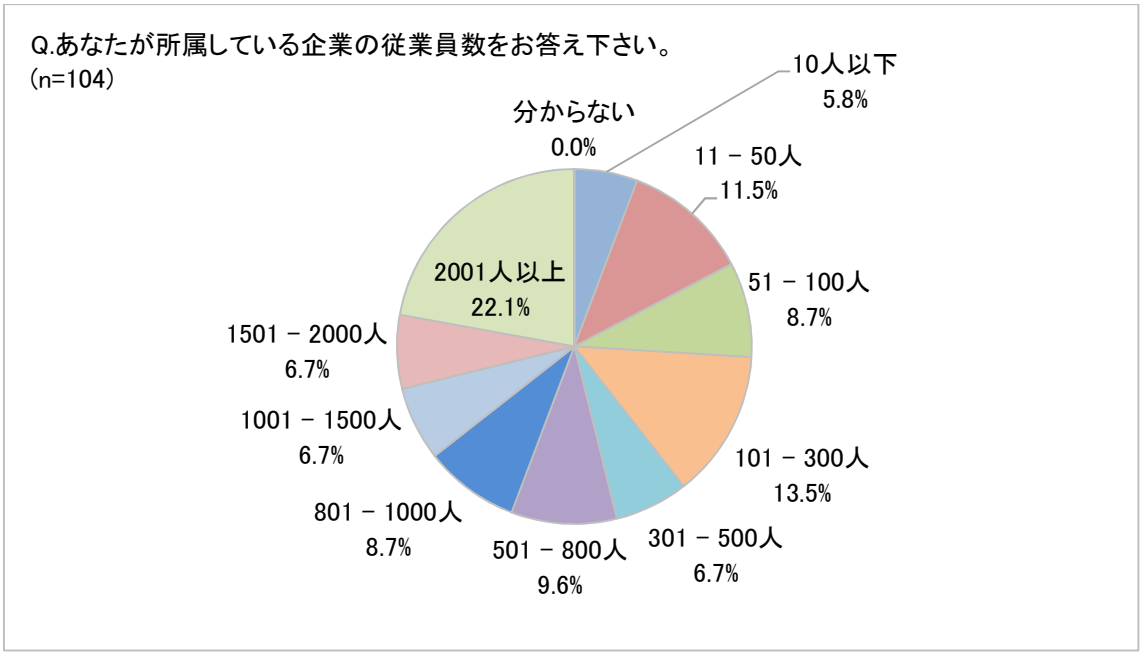


図 4-58　所属企業の従業員数

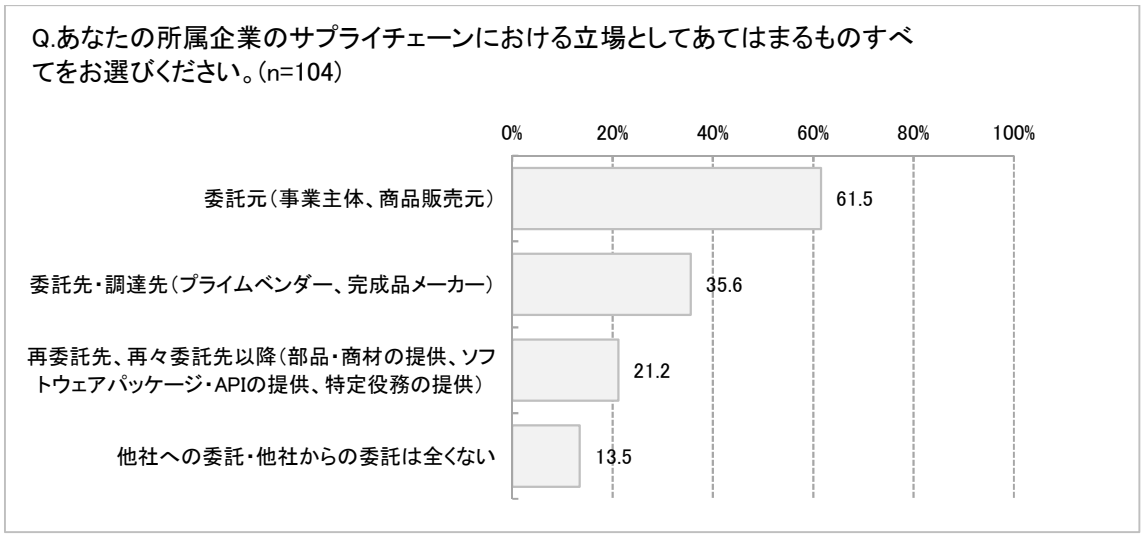


図 4-59　所属企業の委託元／委託先区分

✓ セキュリティ対策標準規格の採用状況

アンケート回答者の所属企業におけるセキュリティ対策標準規格の採用状況に関する調査を行った結果は以下の通りである。

多くの企業において標準規格を採用した対策が実施もしくは検討されている。政府機関等の発行する標準規格と比較して民間団体による対策規格の採用比率が高い傾向が見られた。ただし、選択された規格にはバラつきがあり、分野横断で同一規格が統一的に採用される傾向は見られなかった。

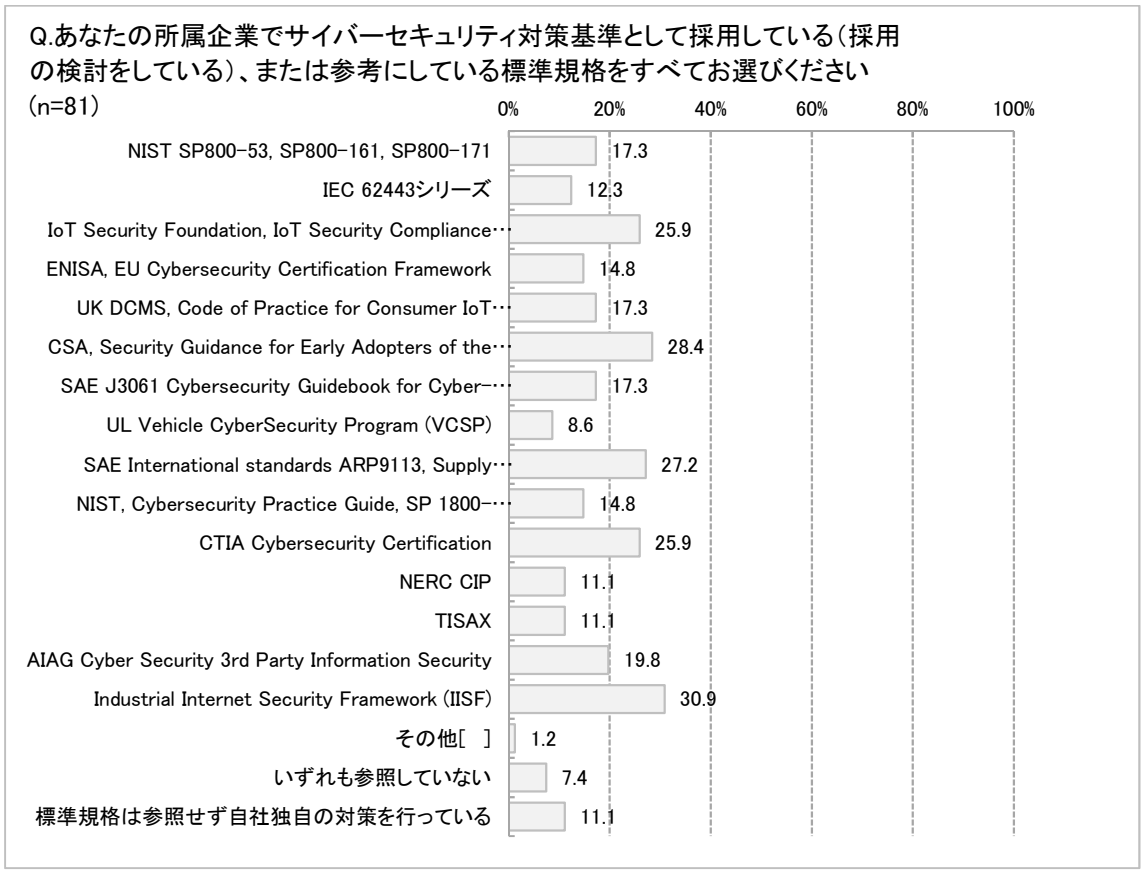


図 4-60　所属企業の参照するセキュリティ対策標準規格

✓ セキュリティ脅威の認識との対策実施状況

アンケート回答者の所属企業におけるセキュリティ脅威認識の度合いと対策の実施状況に関する調査の結果は以下の通りである。

全体的にセキュリティ脅威への意識は高く、特に標的型攻撃、Web サービスへの攻撃を重要視される傾向がみられた。企業への深刻な被害をもたらす標的型攻撃と、攻撃者にとって攻撃を実施しやすい Web サービスへの警戒を高めていると考えられる。

対策実施状況は、経営層主導による対策実施の浸透と、暗号化、マルウェア対策の実装を優先する傾向が見られた。サプライチェーン対策は他の対策と比較して成熟度が低いとの認識が見られたが、一定水準は満たしているものと考える企業が多かった。

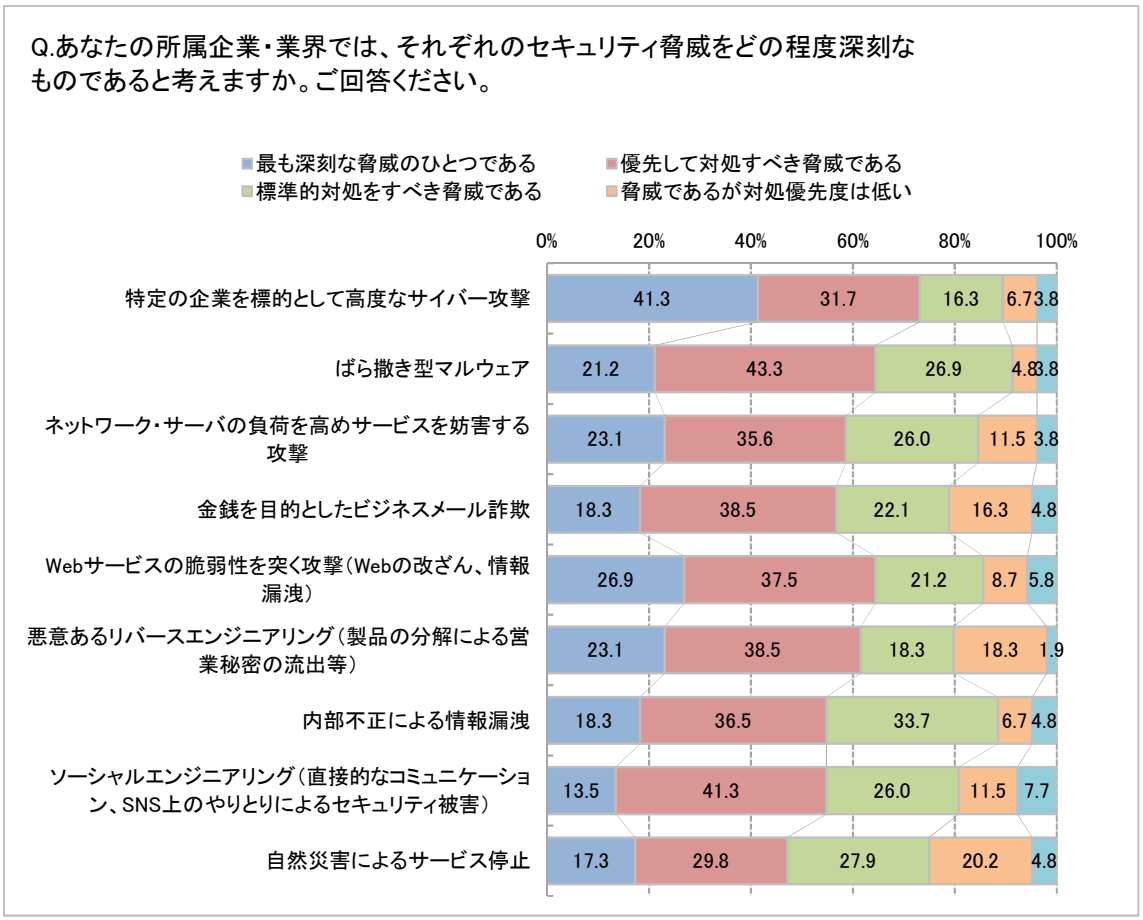


図 4-61　所属企業・業界におけるセキュリティ脅威認識

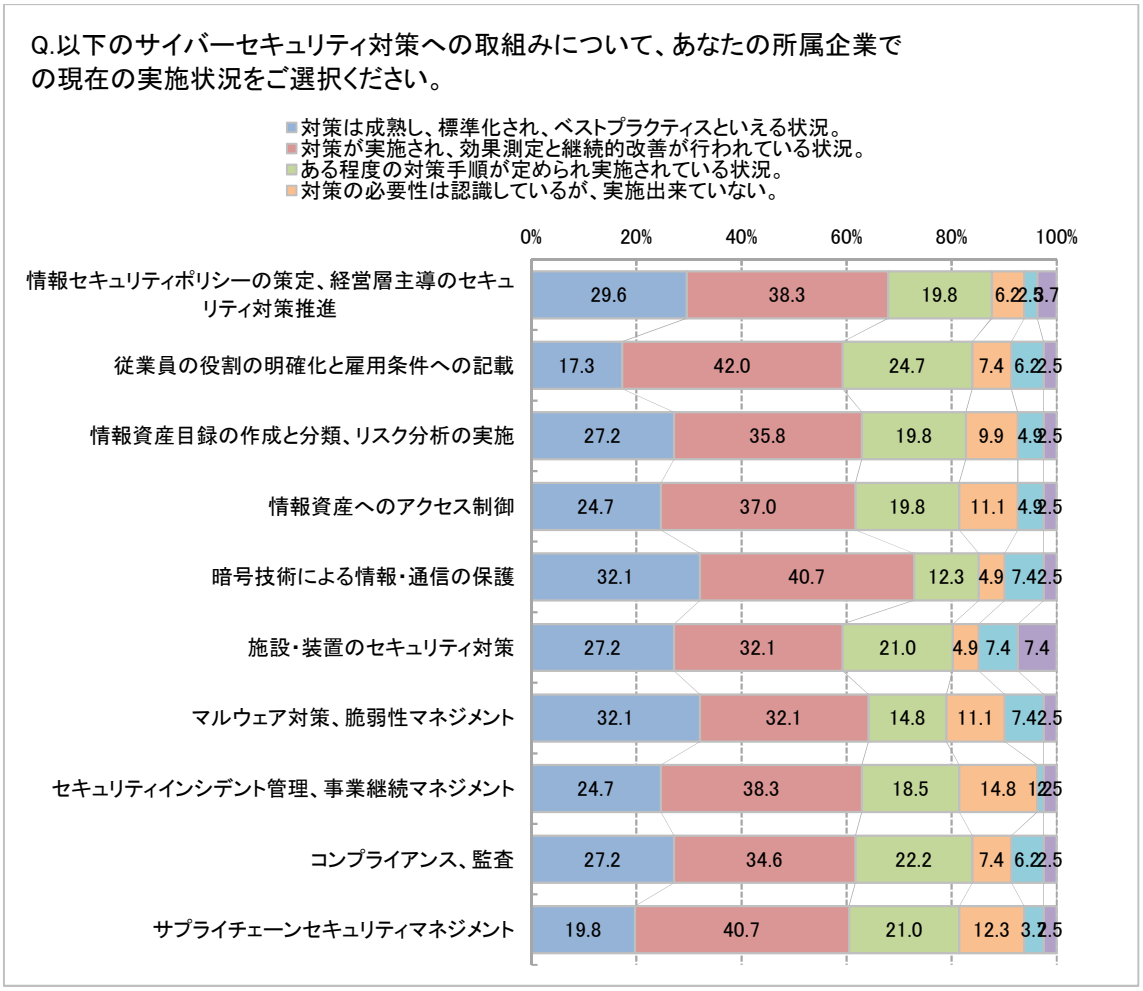


図 4-62　所属企業のサイバーセキュリティ対策への取り組み状況

✓ サプライチェーンセキュリティ脅威の認識状況

アンケート回答者の所属企業におけるサプライチェーンセキュリティ脅威の認識状況と取引先における取り組みを重視する度合い、取引先での対策状況への印象に関する調査の結果は以下の通りである。

サプライチェーンへのセキュリティ脅威としては、委託先を対象とする悪意に基づく脅威を特に深刻と捉えている傾向が見て取れた。委託先での内部犯行のみならず、製造過程でのマルウェア混入、委託先を踏み台とした自社へのサイバー攻撃等、委託先の脆弱性を悪用した攻撃への危機意識が高い。

取引先のセキュリティ対策状況を重視する度合いも相応に高く、7 割程度の企業が大きな評価基準として考えているという結果が得られた。一方で、実際に取引先がどの程度セキュリティ対策を実施できているかに関しては、過半数の企業が、取引先はある程度以上の対策を実施できていると感じているという結果が得られており、セキュリティを相互に重視している関係性がある程度でき上がっているものと考えられる。

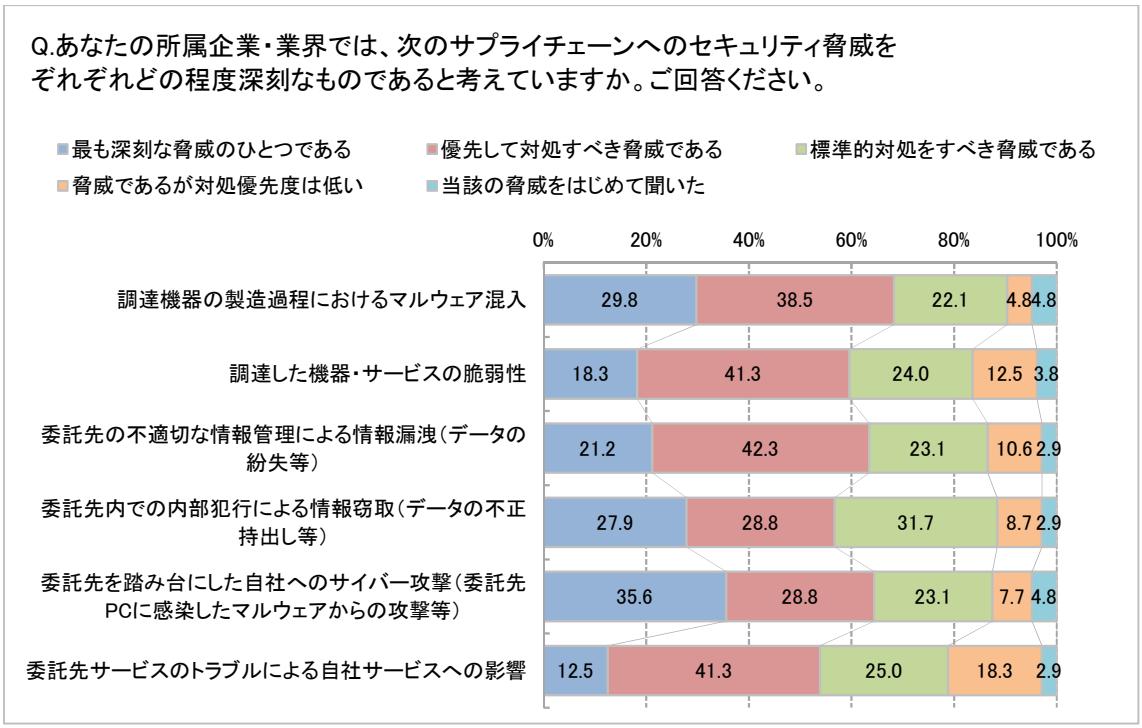


図 4-63　サプライチェーンセキュリティ脅威の認識

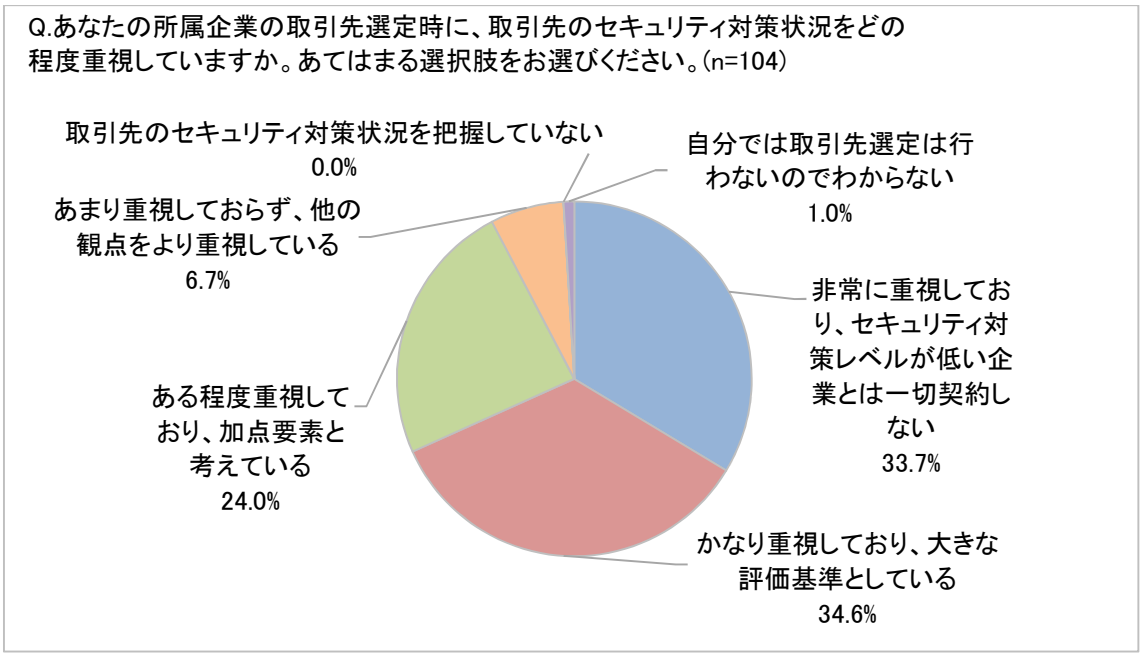


図 4-64　取引先のセキュリティ対策状況を重視する度合い

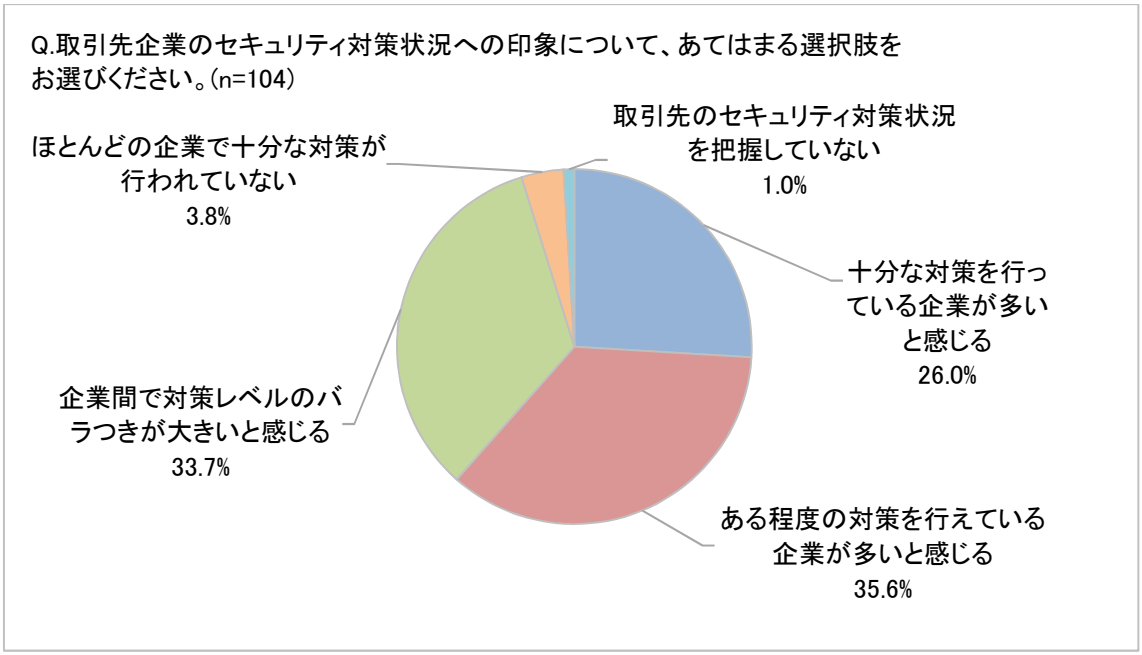


図 4-65　取引先のセキュリティ対策状況への印象

✓ サプライチェーンセキュリティ対策の実施状況

アンケート回答者の所属企業におけるサプライチェーンセキュリティ対策の実施状況についての調査結果は以下の通りである。

取引先との契約においては、秘密保持契約の他に、情報セキュリティ監査の受入・認証適合証明、セキュリティ検査の実施が特に重視されていた。実際に状況を把握するための手段としては、自社または第三者による確認を求め、誓約書提出のみでは不十分とする考えが見られた。自己認証のみならず客観的指標による保証を要求する傾向がみられる。

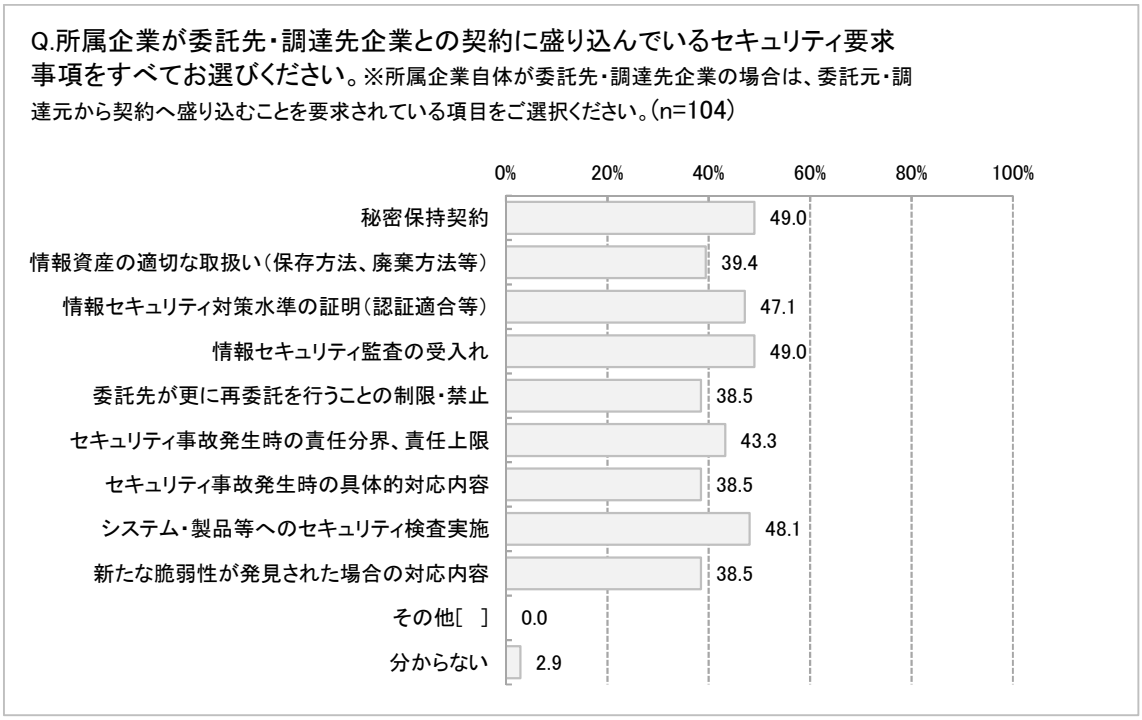


図 4-66　取引先との契約におけるセキュリティ関連事項の記載

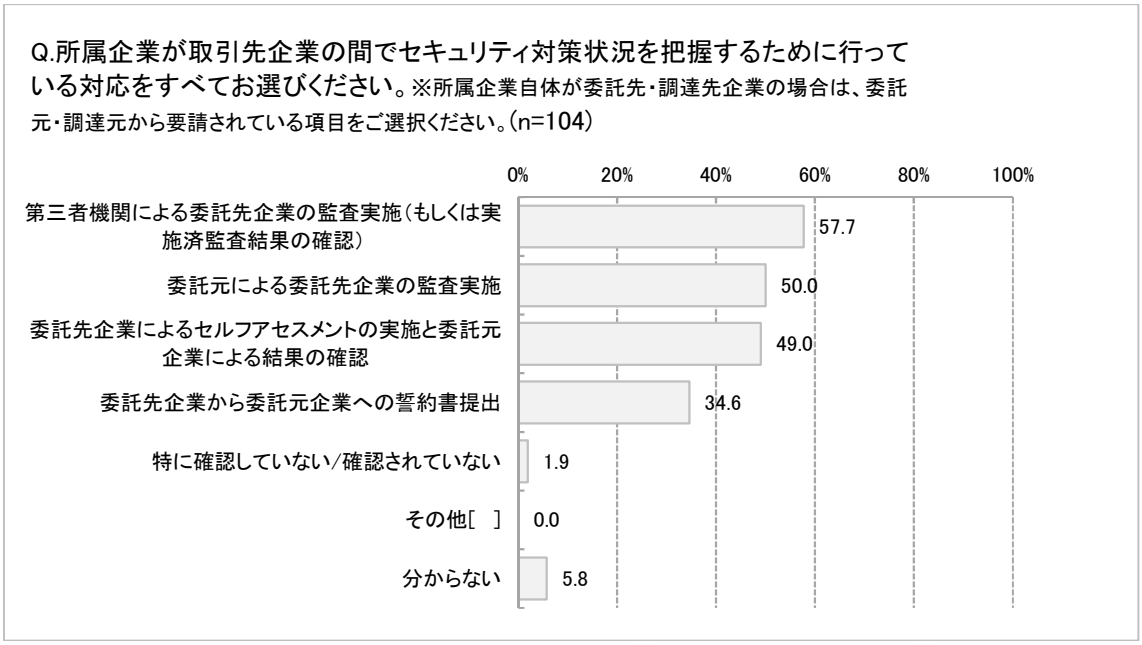


図 4-67　取引先のセキュリティ対策状況把握のための施策

✓ サプライチェーンセキュリティへの課題意識

アンケート回答者の所属企業にいてサプライチェーンセキュリティの課題として捉えられている事項の調査結果は以下の通りである。

最も大きな課題として捉えられているものは、他社のシステムや製品を検証することの難しさであった。その他、セキュリティ事故や契約後に発生するリスクへの対応の契約時取り決めへの課題意識が見られた。対策基準のすり合わせに関しては、最も大きな課題と捉える回答は少なかったが、3 番目に重要と考える回答者が最も多く、地味ではあるが無視できない課題としての位置付けとの意識が読み取れる。

図 4-68　サプライチェーンセキュリティ実装への課題意識

4.3.4　ヒアリング調査

4.3.4.1 ヒアリング実施計画

製造業を中心とした海外の企業に対して、サプライチェーンに係る基準・標準の導入実態や、取り組み状況、課題等について明らかにするため、現地ヒアリングを実施しまとめる。

主な質問項目は以下の通りである。

- サプライチェーン（取引関係）におけるセキュリティの要件をどのように決めているか。
  - ✓ 参照する基準と主な要素
  - ✓ 利用する技術、ツール（マネジメント支援、検査ツール等）
    - 可視化技術、アシュアランスの手法（検査結果等のエビデンスの獲得と論証に基づく説明方法、説明責任の達成）
  - ✓ 独自の基準（可能であれば、主な観点）
- マルチステークホルダー対応
  - ✓ サプライチェーンにおける主なステークホルダーとリスク
  - ✓ リスクの評価法
  - ✓ 契約上の責任分界点の取決め
  - ✓ リスク対策の考え方（責任主体が明確な調達とオープンソース等責任主体が明確ではない場合の違い）
- 認証制度（適合性評価制度）
  - ✓ 認証制度の適用状況
  - ✓ 認証制度の効果と課題
  - ✓ 自己宣言、第三者認証
- 社会実装時の課題
  - ✓ 既存のセキュリティ基準の効果に対してコストが高い、または効果が測定できない。
  - ✓ 必要最小限の対策基準が明確ではない。
  - ✓ その他、サプライチェーンセキュリティを確保する上で解決すべき課題

ヒアリングは、時間的制約のためドイツ研究機関 Fraunhofer Institute のセキュリティ専門組織 Secure Information Technology に委託し実施した。

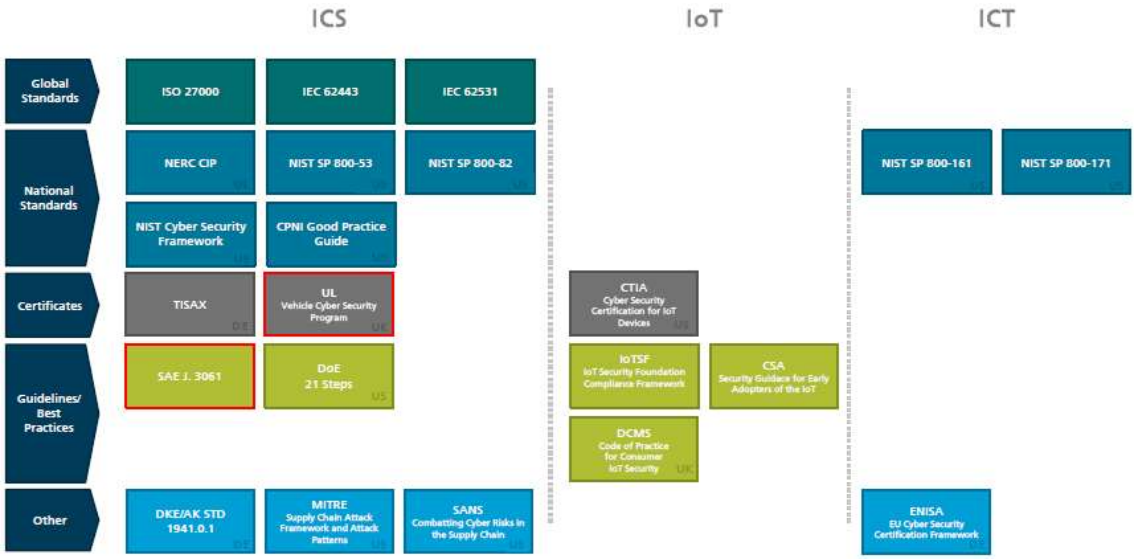


図 4-69　ヒアリングの対象とした主な基準・標準等

4.3.4.2 ヒアリング調査結果

調査委託先が、ヒアリング依頼をかけた結果、2 社から匿名化を条件に回答を得ることができた。回答した 2 社は、大手自動車システムサプライヤーである。

ヒアリングの結果得られた主な知見は以下の通りである。

- 標準等の適用実装時の問題点
  - ✓ 異なる標準間の重複の特定
  - ✓ 技術面以外では、標準のプロセスを受け入れ意識して開発する等の組織の文化を変えることが最も大きな課題であった。

- 調達における認証の要件化
  - ✓ TISAX 認証を取得していないことから調達を回避した。
  - ✓ 自動車業界では、 TISAX 認証企業のみを調達先とする傾向性がある。

- サプライチェーンにおける責任と保証の方法
  - ✓ サプライチェーンにおける責任保証をするための手段として、品質マネジメントプロセスの利用、安全規制への準拠が挙げられる。
  - ✓ インシデントリスク評価に基づき個社ごとにインシデント時の保証と責任について取り決める。
- 運用保守フェーズのセキュリティ確保
  - ✓ ISO 27000 及び IEC 62443 に基づきセキュリティを確保する。

4.3.5　サプライチェーンセキュリティ要件に対する実態と課題のまとめ

4.3.5.1 サプライチェーンセキュリティ要件の実装動向

文献調査においては、分野共通の汎用規格及び個別分野における標準規格の策定背景、セキュリティ対策要求事項の内容を確認するとともに、それぞれの標準規格が対象とするステークホルダー、サプライチェーン内でどの範囲を主に対象と考えたものであるかを整理してきた。各規格の主な利用目的及び主な利用者・利用状況を一覧化した結果は図 4-70、図 4-71 の通りである。
NIST や ISO/IEC のような汎用基準が、個々のリスクアセスメントに基づいた対策要件の実装と評価を重視することに対し、分野別基準は評価方法を標準化することで、客観的信頼性基準を確立することを目指す傾向が見られる。また、評価手法は運用性を高めるための効率化に配慮が行われている。

アンケート結果においては、NIST 基準、IEC 基準を直接参照している事業者は多くなかった。これは各分野の事業者はより直接的に関係する基準を参照する傾向があるものと考えられる。ただし、TISAX や CTIA 基準のように、国際標準や汎用規格を参照し、対策要件として引き継ぐ場合は間接的な準拠を行っているとも考えられる。

汎用規格（分野共通）		政府規格・国際標準規格						民間規格		
		NIST SP 800-53	NIST SP 800-161	NIST SP 800-171	IEC 62443	ENISA, EU Cybersecurity Certification Framework	UK DCMS, Code of Practice for Consumer IoT Security	IoT Security Foundation, IoT Security Compliance Framework	SafeCode, Fundamental Practice for Secure Software Development	IIS, Industrial Internet Security Framework
主な利用目的	第三者認証				○	○				
	二者間の評価・認証			○	○					
	自己評価	○	○		○		○	○	○	○
主な利用者利用状況	当局・認証機関（規制の実施、証書の付与）			○	○	○				
	サービス/製品の責任主体（提供するサービス・製品の品質担保）	○	○	○	○		○	○	○	○
	構成要素・部品等のサプライヤー（構成要素・部品等の品質担保）		○		○		○	○	○	○
	顧客・消費者（提供される製品・サービスの品質確認）									

図 4-70　汎用規格（分野共通）の主な利用の整理

分野別規格		自動車					電力	電気通信
		TISAX	SAE J.3061	ISO/SAE 21434	UL VCSP	AIAG, Cyber Security 3rd Party Information Security	NERC CIP Standards	CTIA, Cybersecurity Certification for IoT Devices
利用目的	第三者認証	○						○
	二者間の評価・認証	○		○	○	○	○	
	自己評価		○					
利用者利用状況	当局・認証機関（規制の実施、証書の付与）	○		○			○	○
	サービス/製品の責任主体（提供するサービス・製品の品質担保）	○	○	○	○		○	○
	構成要素・部品等のサプライヤー（構成要素・部品等の品質担保）	○	○	○		○		
	顧客・消費者（提供される製品・サービスの品質確認）		○					

図 4-71　分野別規格の主な利用の整理

4.3.5.2 サプライチェーンセキュリティ推進上の課題

アンケート調査結果からは、直接の取引先であっても、機密保持の観点や技術的ハードルの観点から相手のセキュリティ対策状況を確認することが容易ではないことが課題となっていることが明らかとなった。監査の実施や認証への準拠確認、契約による責任範囲の明確化といった対応は行われているが、実態の把握度合いが必ずしも十分ではないと考えられているものと解釈できる。また、各社がサプライチェーンセキュリティを推進するにあたって、自社と取引先のどちらがコスト負担を行うべきか、セキュリティ事故発生時の責任をどちらが負うべきかの合意を得ることが難しいことが課題であるとの回答も多く見られた。これらは事業者間の間で客観的な基準による統一見解を得られる場合は、現状必ずしも多くないことが原因の一つとして存在するものと考えられる。

また、再委託先や間接的な取引先といった直接の契約関係を持たない事業者とのセキュリティ保証に関しては、確認のための障壁の大きさへの回答よりも、そもそも関係するサプライチェーンの全体像を把握すること自体ができていないという回答が多く見られるという結果になった。多種多様な事業者の関係性が複雑化し、巨大化するサプライチェーンにおいて、End-To-End での確認を事業者間の手続きを介して行うことのコストの高さが現実に課題として表れているものとみることができる。

4.4 事業者毎の対応範囲、事業者間の責任分界点

4.4.1 主な分野のステークホルダー関係整理

4.4.1.1 自動車分野

4.4.1.1.1 車のライフサイクルにおけるサイバーセキュリティの脅威とステークホルダーの関係

従来、車のライフサイクル管理は、自動車メーカーが車を「企画・開発し製造する」までと、車をお客様に渡した後の「修理・メンテナンス（＝車検対応）や事故対応、中古車販売、廃棄等」に分けていた。自動車メーカーでは社会ニーズや相場に合った車を企画・開発・製造してきており、制御系システムを中心とした物理的な部品の安全性・品質をサプライチェーン全体にわたって保証するため何十年という長い時間をかけて成熟したプロセスを構築してきた。サプライチェーンは自動車メーカー（OEM）をトップとした複雑で大規模なものとなり、自動車メーカー各社がサプライチェーン内のそれぞれの会社に対して保証プロセスが準備されていた。

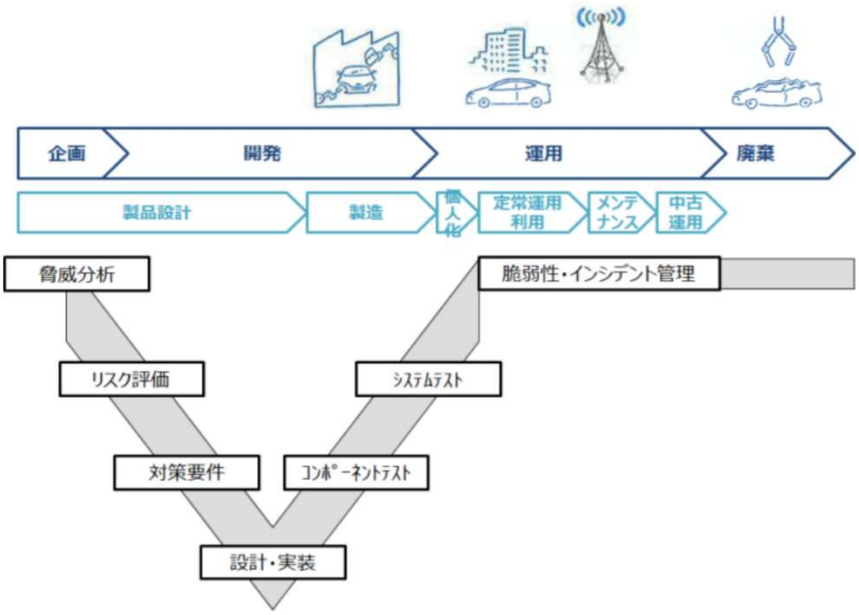


図 4-72　従来の自動車ライフサイクル[12]

サイバーセキュリティを考えた場合、最近は MaaS (Mobility as a Service)、シェアリングや自動運転を実現するための走行データ、事故データの蓄積活用、事故情報の共有と OTA (Over the Air) アップデート等、自動車業界においては新たなステークホルダーが多数参加するビジネスエコシステムへと進化している。これらの多種多様なステークホルダーのサイバーセキュリティ対策は様々であり、従来のサプライチェーンに加えて異業種を含めた、拡張されたサプライチェーンにおけるサイバーセキュリティ対策に対する要求は 2010 年頃より急速に高まっている。サイバー攻撃が深刻な場合はセキュリティ関連のリコールとなるが、リコールによる車の改修率は 100%ではないことや、攻撃方法が日々進化していることを考慮すると、サイバーセキュリティ対策としてはプログラム更新（セキュリティの維持向上）が重要であり、車をお客様に渡した後のライフサイクル管理（プログラムやデータの管理）がより重要になってきている。車は耐用年数が長く、内蔵されているソフトウェア（プログラム）をいかに最適化するかが脅威に対する防御として重要となる。現在、迅速かつ徹底的なプログラム更新維持ができる車両は Tesla 等ごく一部である。そのため車のプログラム更新については無線ネットワークを利用した OTA が注目されており、例えば Uptone[13]等がある。

[12] 経済産業省: 自動走行システムにおけるサイバーセキュリティ対策
http://www.meti.go.jp/committee/kenkyukai/seizou/jido_soukou/pdf/sankou_002.pdf、p.2 自動車のライフサイクル、2019/2/27

[13] ニューヨーク大学の研究者らが始めた自動車向けの OTA 技術研究のプロジェクト・フレームワーク。
Uptane: https://uptane.github.io/

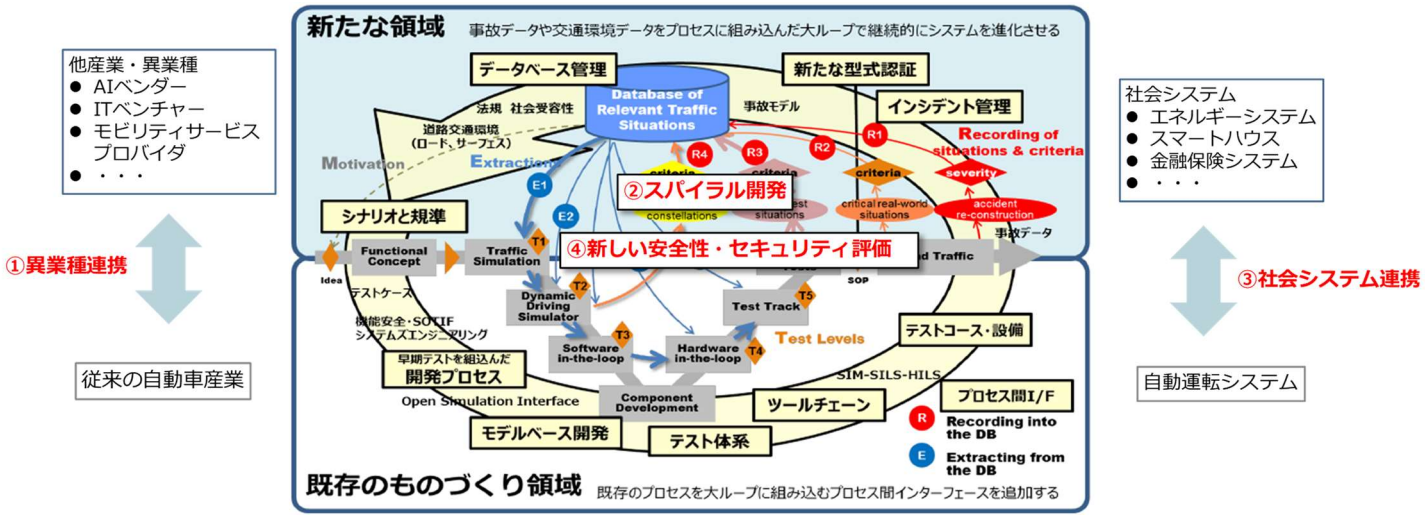


図 4-73　新たな自動車ライフサイクル[14]

今後は、異業種連携、スパイラル開発、システム連携、新しい安全性評価の四つの観点における、運用サービス領域を含むサイバーセキュリティ脅威への対応が求められる。

- ✓ 異業種連携: 自動車業界を超えた異業種のプレイヤーが連携するエコシステムを前提とした開発
- ✓ スパイラル開発: 開発時だけでなく自動車販売後の自動車利用時におけるデータのフィードバックによるスパイラル型開発プロセスへの対応
- ✓ システム連携: エネルギーシステム・金融保険システム等の社会システムと自動運転等自動車システムが連携する進化型のモビリティサービスの開発
- ✓ 新しい安全性・セキュリティ評価: 自動運転等に対応した安全性・セキュリティ評価、アシュアランスと社会的受容性を確保する開発手法

図 4-73 は自動運転に関する新たな自動車ライフサイクルの例である。

4.4.1.1.2 自動車業界の産業構造とサプライチェーンセキュリティ

様々な異業種のステークホルダーも含めた、現在の自動車業界の産業構造（サプライチェーン）は図 4-74 の通りである。日本の場合は固定的な系列関係の傾向が高く、自動車メーカー（OEM）から下位サプライヤーに向かって要求情報が流れるが、欧米では自動車メーカー（OEM）やサプライヤーの独立性が高く、サプライヤーは特定の自動車メーカー（OEM）に大きく依存していない。特に中核となる 1 次サプライヤーが設計開発において付加価値の高い役割を果たすことが多い。

[14] 経済産業省: 自動走行ビジネス検討会「自動走行の実現に向けた取組方針」報告書概要 Version2.0、http://www.meti.go.jp/report/whitepaper/data/pdf/20180330002_03.pdf、p.27 (独)PEGASUS における自動運転の評価プロセス、2019/2/27

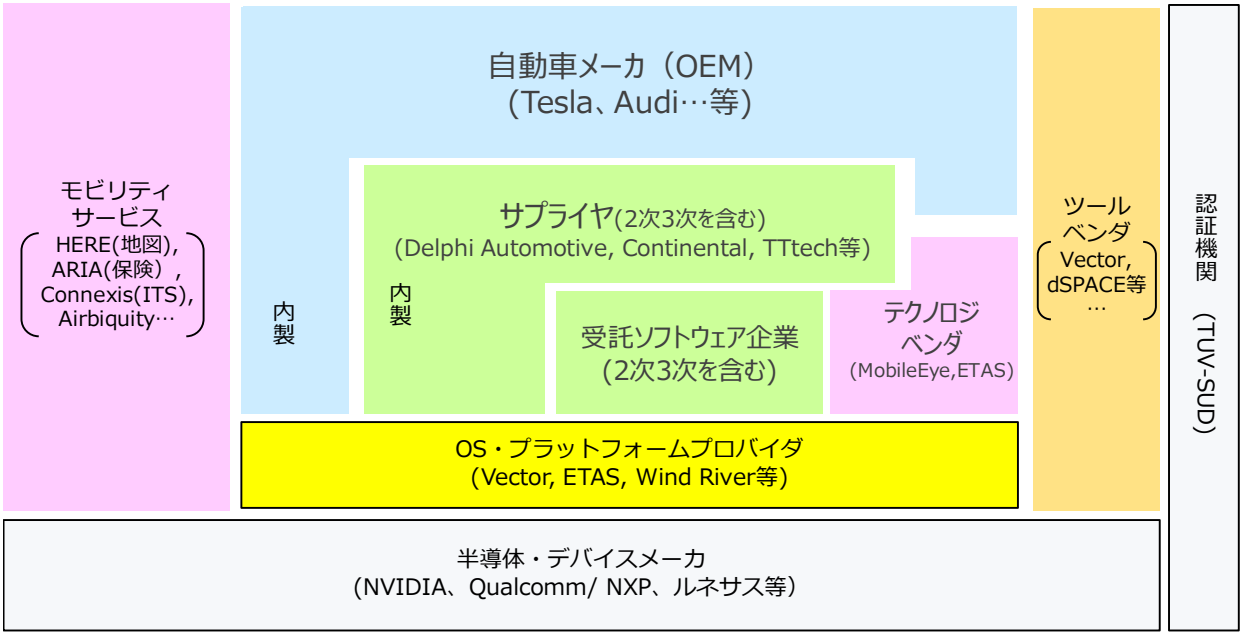


図 4-74　自動車業界の産業構造

図 4-74 に示す自動車業界のサプライチェーンを考慮して、自動車ライフサイクルにおけるサイバーセキュリティリスクを示すと図 4-75 のようになる。従来の制御系における安全性対策は主として「企画・開発・製造」フェーズを中心としたサプライチェーンにおける品質保証であり、ハードウェア、ソフトウェアともウォーターフォール型（V 字型）の開発におけるレビュー・試験・検査が重要な対策であった。情報系を中心としたサイバーセキュリティリスクを考える場合、「企画・開発・製造」フェーズにおける対策だけでは不十分である。車は耐用年数が長く運用以降のライフサイクルが数年以上となるため、ハードウェア・ソフトウェアとも「企画・開発・製造」フェーズとは使用環境が変化していき、特にソフトウェアでは想定していなかった脆弱性が発見・攻撃される可能性がある。そのため、セキュリティ対策としては「運用・廃棄」フェーズも含めなくてはならない。このフェーズでは自動車業界にとっては新たに加わった各種モビリティサービス提供者やプログラム更新（OTA）等のツールベンダーも含めた、従来のサプライチェーンを拡張した関係の中での対策が必要となっている。

サプライチェーンでのサイバーセキュリティ対策としては、「サプライチェーンにおける組織プロセス品質」（各会社間での情報セキュリティ基盤の構築）と「個々のコンポーネントにおけるプロダクト品質」（それぞれの部品やプログラム、製品に関する技術的なセキュリティ機能の担保）の二つに大きく分けられる。自動車業界では、従来の制御系システム（＝安全の確保）については長い時間をかけて成熟したプロセスをサプライチェーン全体で構築してきた。一方サイバーセキュリティについてはまだ不十分な状況であり、新たなステークホルダーが参加している状況において様々なサイバー攻撃が発生する中、コネクテッドカーには複雑化したサプライチェーンが存在しており、サイバーセキュリティリスクの管理経験が異なる多種多様なベンダーで構成されている。そのため、新たなサプライチェーンにおいてセキュリティを 2 社間で個別に担保し、サプライチェーン全体としてセキュリティのトレーサビリティを確保するには時間がかかりすぎてしまい、サイバーセキュリティリスクへの対策が間に合わない。そのため、「4.3.2.2　(6) 自動車分野におけるサイバーセキュリティの脅威と規格の対応」で調査した TISAX や AIAG Cyber Security 等の規格・基準を利用した第三者による「サプライチェーンにおける組織プロセス品質」の担保に期待が寄せられている。

サイバーセキュリティ対策として特に重要であり、従来の安全性対策と異なるのは、「運用・廃棄」フェーズにおけるプログラムやデータに起因する脆弱さである。「4.3.2.2　(6) 自

動車分野におけるサイバーセキュリティの脅威と規格の対応」で様々なサイバー攻撃を紹介したように、この「運用・廃棄」フェーズでは自動車プログラムに対する不正コードの追加や改ざん、マルウェア攻撃の他に、車の所有者や運転者による操作の誤りも考えられる。コネクテッドカーに対しては、一般的な情報システムと同等のセキュリティ対策が必要である。

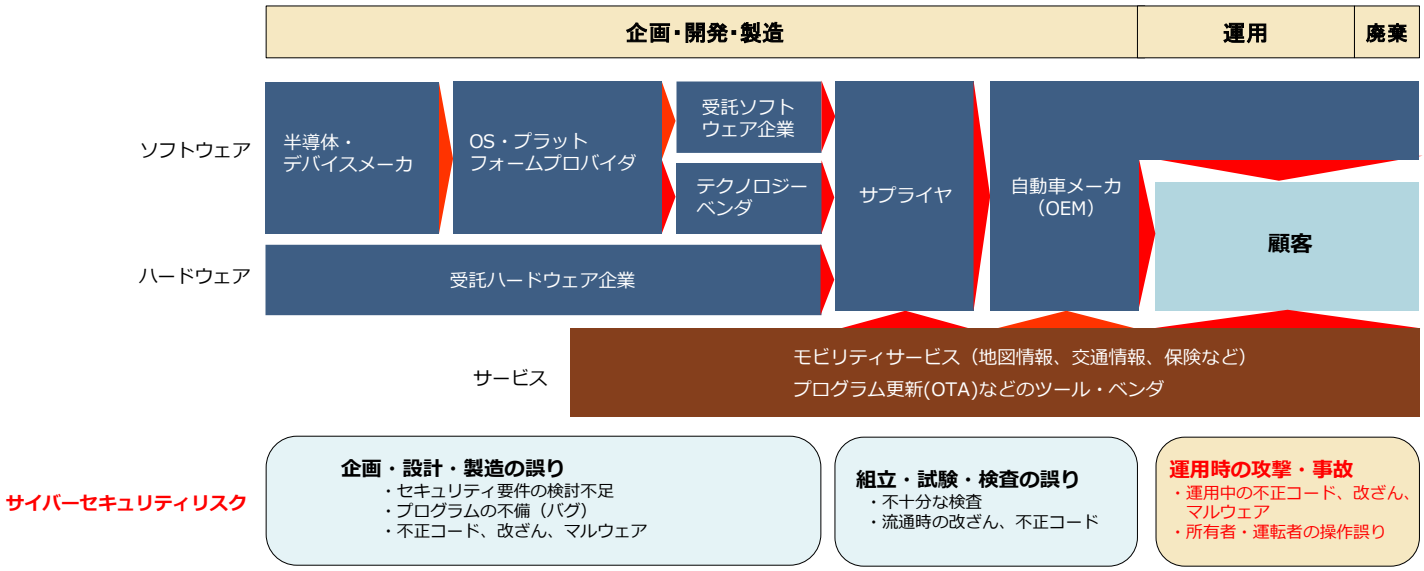


図 4-75　自動車ライフサイクルにおけるサイバーセキュリティリスク

図 4-44 で示したように、規格・基準の対象は「サプライチェーンにおける組織プロセス品質」(TISAX、AIAG Cyber Security) と「個々のコンポーネントにおけるプロダクト品質」(SAE J3061、ISO/SAE 21434) に分けられる。サイバー攻撃方法は日々進化しているため、技術面での対策を直接的に個別に規定することは難しく、現在策定中の ISO/SAE 21434 では技術面については付録として情報提供することを予定している。

4.4.1.2 政府調達分野

政府調達分野におけるサプライチェーンの責任分界の整理を行うとともに、本調査で対象とした標準規格の位置付けの分析を行い、米国及び欧州における政府調達基準の傾向差異を整理した結果を以下に示す。

4.4.1.2.1 政府調達分野のサプライチェーンリスクの整理

米国 MITER 及び防衛省による“Supply Chain Attack Framework and Attack Patterns”の内容に基づき、政府調達分野のサプライチェーンリスクを整理する。当該フレームワークでは、防衛省の重要システムの調達・維持時におけるリスクを評価することを目的に、調達ライフサイクルの一般化、サプライチェーン攻撃パターンの網羅的なカタログ提供を行っている。防衛システム調達における五つのフェーズに対し、六つの攻撃ポイント、四つの攻撃対象に分類している。

図 4-76　防衛調達における五つのフェーズ定義（DoDI 5000.02）

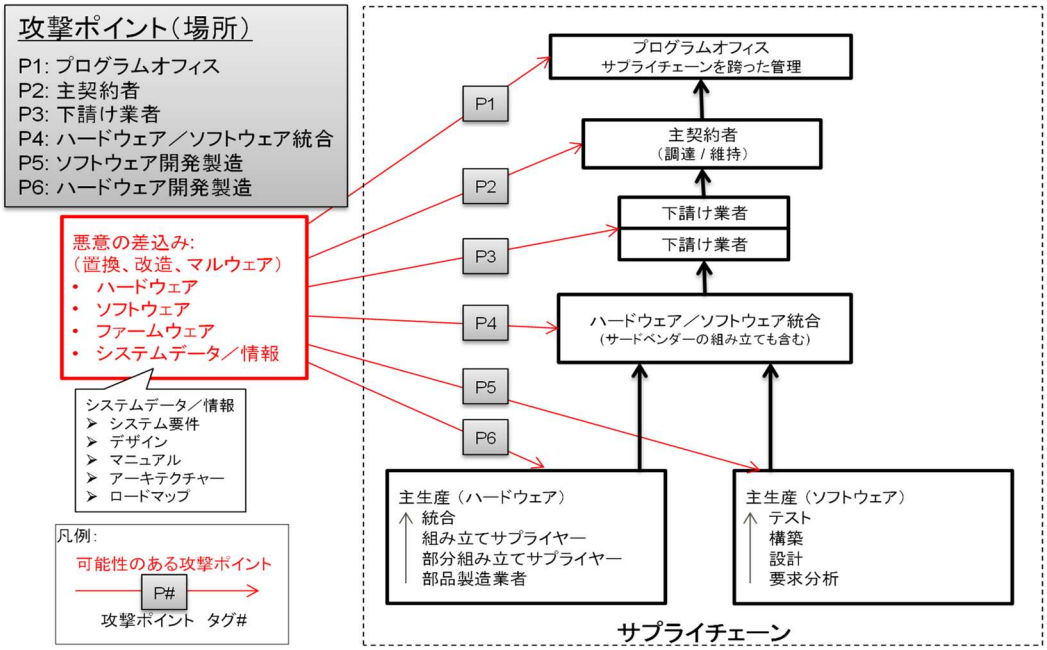


図 4-77　六つの攻撃ポイントと四つの攻撃対象の整理

また、各フェーズ、攻撃対象毎に 41 の詳細攻撃パターンと 20 の対策がカタログ化されている。製造開発プロセスでのハードウェア、ソフトウェアへの悪意ある改変等を特に警戒しており、多くの攻撃パターンが列挙されている。

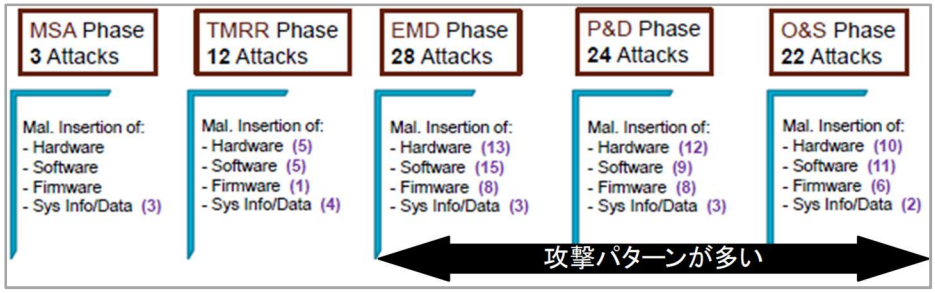


図 4-78　攻撃パターンの分布

4.4.1.2.2　米国政府調達分野における責任分界と保証の考え方

米国においては、政府機関とサプライヤーの二者間の評価、認証の関係性を構築する形態をサプライチェーンにおけるセキュリティアシュアランスの基本形とする傾向が見て取れる。従来から、FIPS Publication 200 では連邦政府機関は所管する情報システムのセキュリティ対策を自らの責任において実施することを求めており、NIST SP 800-53 は対策カタログとして機能している。また、連邦政府機関がサプライヤーのリスクを管理するための対

策は NIST SP 800-161 に準じて行うことが米国行政管理予算局からの通達にて要求されている。

一方で、サプライヤーを主体としたセキュリティアシュアランスの表明を求める動きが特に近年においては強化されている。FAR 52.204-21 では、NIST SP 800-171 によってサプライヤーが保持することとなる情報のセキュリティとプライバシーを管理することを基本方針としており、DFARS 252.204-7012 において防衛省の必須調達要件として運用されている。また、クラウドサービスの調達においては、連邦政府の認定した認証機関によって FedRAMP 認証を取得したサービスのみが調達資格を有する。

これらの要件は ISO/IEC 27001 等の国際標準との対応関係が示されてはいるが、必ずしもすべての対策要件が合致するものではなく、あくまで連邦政府自らが必要と考える対策要件を特定・定義するものであり、責任分界を中央集権的に管理する傾向が見られる。

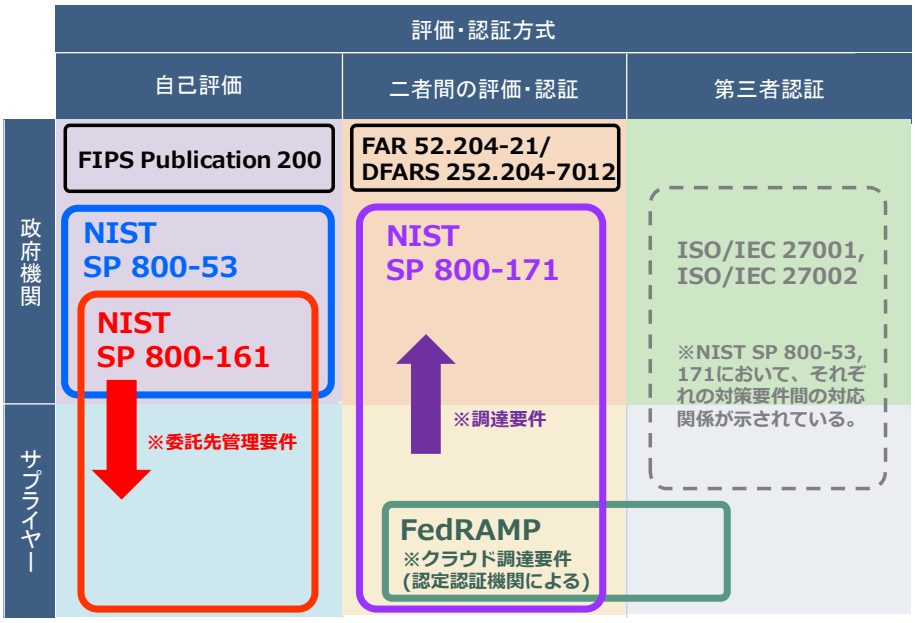


図 4-79　米国における責任分界と保証の整理

4.4.1.2.3 欧州政府調達分野における責任分界と保証の考え方

一方で欧州においては、第三者認証の制度を重視し、広く通じる共有の指針によるアシュアランスを志向する傾向が強い。欧州デジタル単一市場の理念では、EU 域内での情報流通は共通の指針で行われることを目指している。よって各国独自基準による運用が行われることは極力避けたいと考えられているが、各国の事情、産業毎の事情には配慮する仕組みを用意しながらの標準化を目指す意図が読み取れる。

EU Cybersecurity Certification Framework では、認証機関自体の要件を規定することに集中しており、具体的な技術対策要件は各国認定機関に任せる形を取っている。一方で採用される基準は可能な限り国際標準、デファクトスタンダード規格等とすることが励行されており、各国認証機関の責任の下、共通の指針による相互保証が行われることを目標としている。ISO や IEC といった国際標準化活動にも積極的に貢献しており、IoT システムを始めとするコネクテッドシステムのサプライチェーンにおけるトラスト、セキュリティに関しては今後も ISO/IEC JTC 1 / SC 41 において標準化議論が活発に行われるものとみられる。直近では、SAFECode Perspective on Cybersecurity Certification 2018 において、EU Cybersecurity Certification Framework について、ISO/IEC 27034 等に基づいて各国の整合性をとりながら国際相互承認を推進すべき旨が勧告されている。

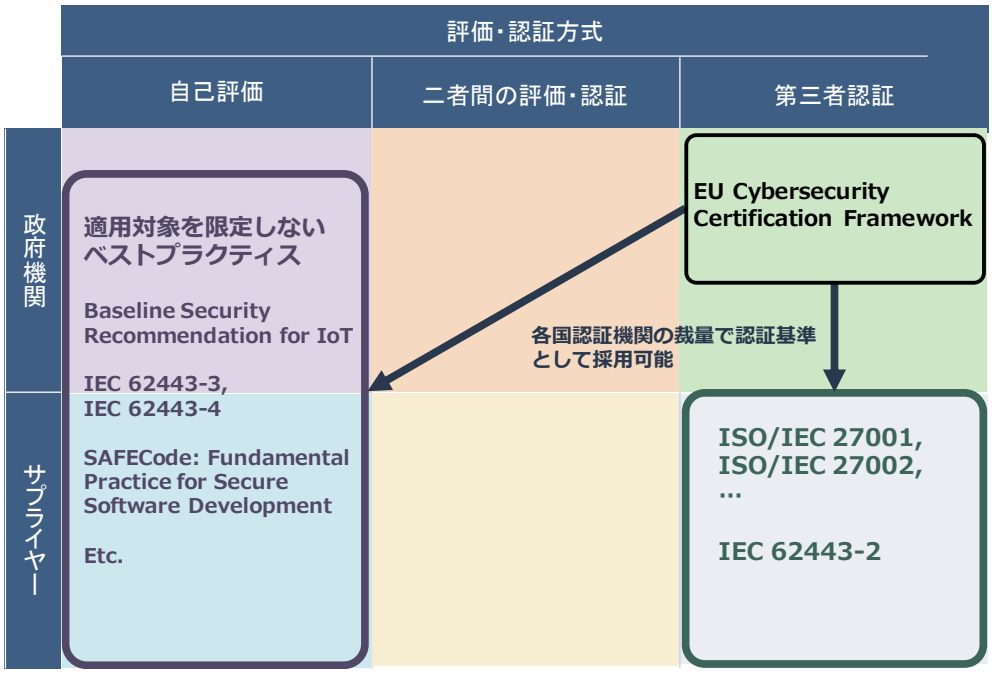


図 4-80　EU における責任分界と保証の整理

4.5　監査・認証制度における課題と取り組みアプローチ

サプライチェーンセキュリティに係る監査・認証を推進するための方法について整理する。

4.5.1　サプライチェーンセキュリティにおける課題

多様なステークホルダーから構成されるサプライチェーン全体でセキュリティを確保するためには、自組織のセキュリティ確保だけでなく、開発委託先、製品提供者等の外部の組織におけるセキュリティが確保されていることについて確信を持てなければならない。

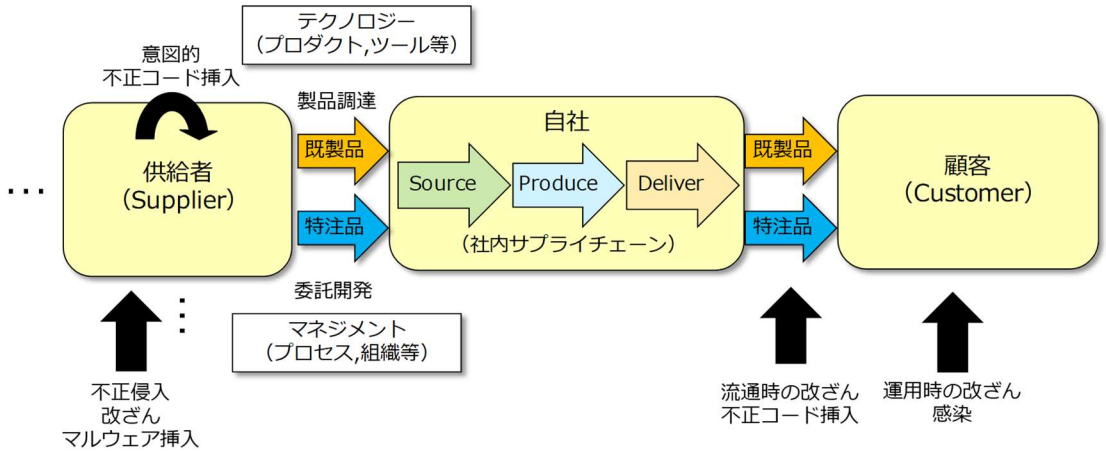


図 4-81　サプライチェーンにおける脅威の構成[15]

自組織で閉じたセキュリティ確保であればセキュリティ対策自体が関心の中心となるが、

[15] SCOR (Supply-Chain Operations Reference) モデルを元に三菱総合研究所作成。

サプライチェーンにおける他組織のセキュリティ確保のためには、他組織がセキュリティ対策を適切に行っていることを保証しなければならない。このようなセキュリティを確保していることを他者に保証する概念が、セキュリティアシュアランスであり、自組織に閉じたセキュリティ確保とサプライチェーンにおけるセキュリティ確保において求められることの本質的な違いである。

アシュアランスの確保に関する典型的な例として、コモンクライテリアにおけるセキュリティ保証要求や、セーフティ分野の認証制度において要件化されるアシュアランスケース[16]を挙げることができる。認証制度は、他者に対して製品、サービス、組織等が一定の基準を満たしていることを可視化し、保証するための典型的なアプローチである。

4.5.2 適合性評価制度と認証制度の国際フレームワークの概要

WTO/TBT 協定により、国の認証制度、規格、適合性評価手続きが国際貿易の障害とならないように、国際規格に整合することが合意され、それにより、国際規格の位置付けが明確になり、国際規格の数が急速に増加した。

従来、国ごとに異なる「基準」、「評価方法」であったものが、適合性評価フレームワークにより国際的に開かれた共通ルールへと進展してきている。

「適合性評価（Conformity_Assessment)」は、製品、プロセス、システム、要員、または機関に関する規定要求事項が満たされていることを実証すること（ISO/IEC 17000:2004)。

「認証（Certification)」とは、製品、プロセス、システム、要員等が、規定の要求事項（法令、規格、技術仕様）を満たしていることを第三者※が証明（attestation,実証されたことを表明）すること（ISO/IEC 17000）。

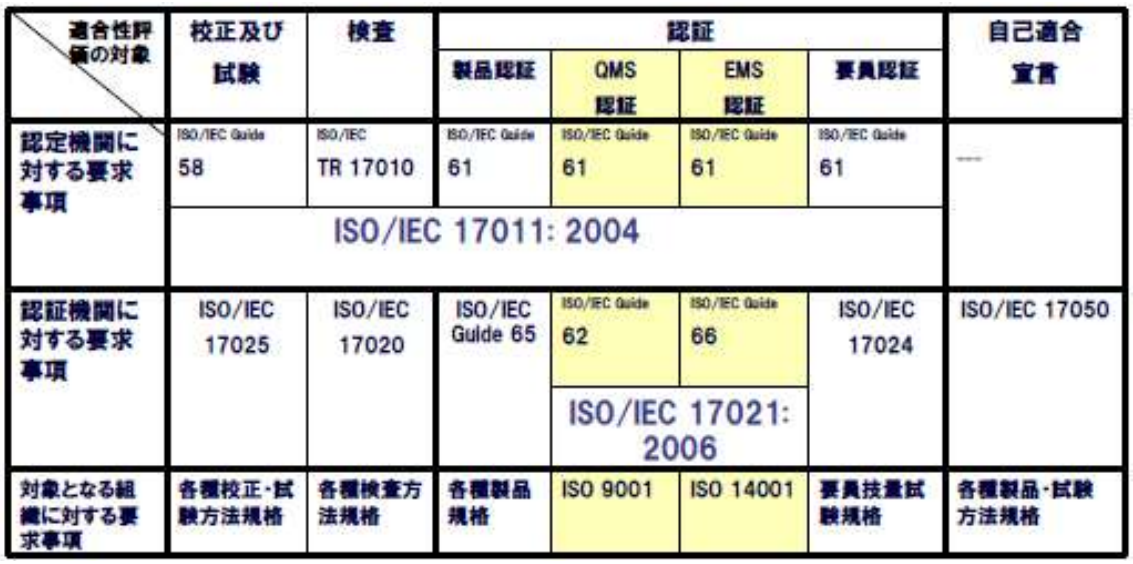


図 4-82 適合性評価の分野と適用される規格及びガイド類[17]

認証は、(1) 認定機関による認証機関の認定（信用の付与）と (2) 認証機関による認証対象（製品、プロセス、システム、要員等）に対する適合性の評価と第三者証明の発行、という 2 段階で行われる。国際相互承認協定により、各国の認証制度による認証結果を認め合うことでワンストップ認証を可能とすることが推進されている。

---

[16] テスト結果等の客観的な根拠をもとに論理的・体系的にシステムの安全性を示し、利用者、ステークホルダーに安全性の保証・確信を与えるための文書類。

[17] 一般財団法人日本規格協会: 適合性評価と認定・認証制度
https://www.jsa.or.jp/datas/media/10000/md_746.pdf

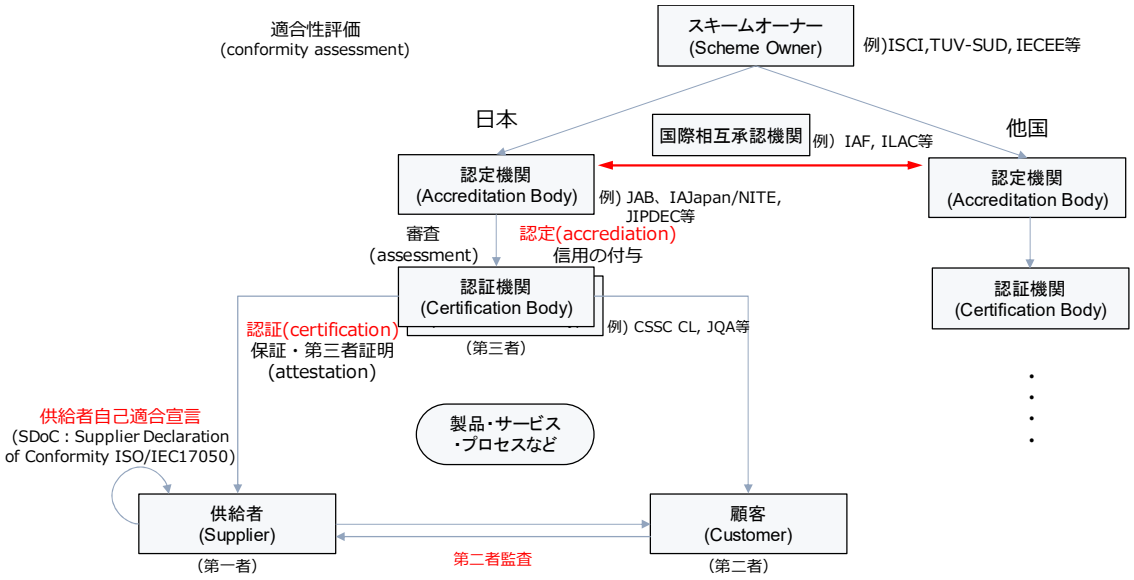


図 4-83　適合性評価の国際的なフレームワークと認証スキーム[18]

4.5.3　認証制度の現状と社会実装に係る参考モデル

主な認証制度・規制について現状を整理したものを以下に示す。

18 三菱総合研究所作成。

区分		規制・認証制度	基準・標準	認定機関	監査・認証機関	概要・特徴	社会実装の参考ポイント
国	強制	129 FERC 61,224	NERC CIP	FERC	NERC	自主規制機関NERCにより具体性の高いチェックリストを規定。サプライチェーンリスク管理の追加を検討中。	リスク評価尺度として電力系統への影響を３段階で分類。データダイオード導入により要求事項免除あり。
	強制	DFARS	NIST SP800-171	DoD	第三者機関	監査と責任追跡性、システムと情報の完全性を含む。	サプライヤーの自己宣言、またはサプライヤーが第三者認証機関に依頼。
	任意	EU Cybersecurity Certification Framework	各国毎に決める。例としてBaseline Security Recommendations for IoT を規定	各国認定機関	各国認証機関	認証機関の要件、審査方法などの認証制度のフレームワークを規定。トラストと完全性の管理、コミュニケーションのトラスト、サードパーティとの関係性など規定。	基準は各国に委ねる。国家間の整合性は既存国際標準による。2019年5月EU Cybersecurity Act発行予定。
民間	任意	TISAX	Information Security Assessment	VDA	ENX	システムの調達・開発・保守運用供給者との関係、ICTサプライチェーンを含む	評価対象4カテゴリ、評価方法3レベル。27001取得で審査を省力化。ドイツではデファクト標準。
	任意	Vehicle Cyber Security Program (VCSP)	UL 2900-1ベース	—	UL	ベンダー調達製品のリスク管理プロセス、静的コード解析を含む	基準は自動車メーカーがカスタマイズ。
	任意	AIAG Cyber Security 3rd Party Information Security	Cyber Security 3rd Party Information Security	—	AIAG	外部監査とコンプライアンス、変更・リリース管理を含む。NIST SP800-53, SP800-171, ISO/IEC27002に対応。	AIAG規格は北米で事実上の自動車品質基準。業界主導で策定。
	任意	CTIA Cybersecurity Certification for IoT Devices	Cybersecurity Certification for IoT Devices	—	CTIA	改ざんの証拠、セキュアブート、ソフトウェア更新などを含む NIST SP800-53, ISO/IEC 27001ベース	評価テスト項目に応じて３レベル

図 4-84　主な認証制度・規制の特徴と社会実装における参考ポイント[19]

[19] 三菱総合研究所

図 4-84 に基づき、主な認証制度・規制の現状及び取り組みをもとに認証制度に関連してサプライチェーンセキュリティを普及促進していく上で参考になる点を整理すると以下の通りである。

社会実装において参考となる観点

- 認証対象に応じたカテゴリ分け、レベル分けにより対策、審査範囲の限定・省力化することで、普及を促進する。
- 業界による自主的な基準の策定、汎用基準からのカスタマイズによる必要最小限の基準に最適化・合理化を図る。
- 他の認証基準、技術要件の適合による重複する要求事項を免除することで、効率的な認証の取得を促進する。

図 4-85　セキュリティ対策基準を普及する上で参考となる例

4.5.4　国際標準･認証基準の選択アプローチ

近年、セキュリティに係る基準・国際標準等が多数策定されている。それぞれ目的に応じて策定されているが、相互に重複するものや、相互参照を行うもの、特定分野にカスタマイズしたもの等関係性が複雑である。

NIST は、サプライチェーンセキュリティに関する主な国際標準やガイドラインの関係を整理し、全体のリスク管理に用いるフレームワークの選定や、事業目的やサプライチェーンにおける役割に応じた対策のための俯瞰マップを整理している。

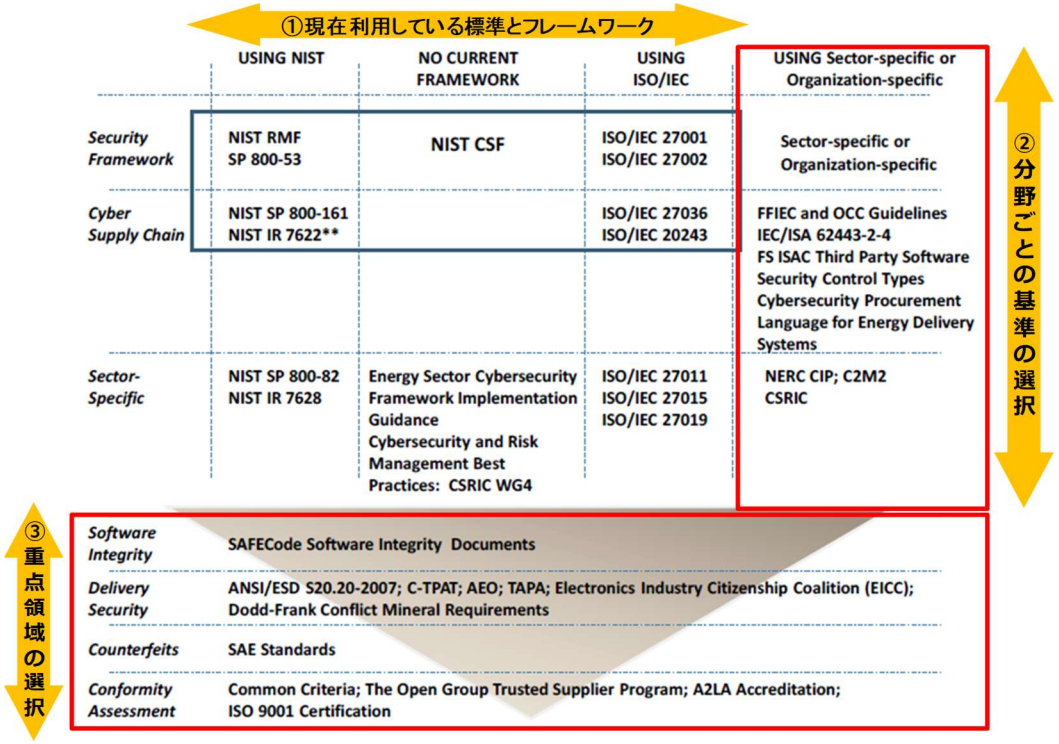


図 4-86　適切なサイバーサプライチェーン標準の選択のためのロードマップ[20]

[20] NIST: Cyber Supply Chain Standards Mapping and Roadmap
https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-SCRM-Standards-Mapping.pdf

このロードマップにおいては、①現在利用している標準とフレームワークをベースとして、②分野ごとの基準を選択し、さらに、③重点領域の選択という流れで、組織や産業の縦割りを越えた分野横断的なベストプラクティスの活用を推進することが示されている。

近年、策定される基準・標準は、先行する基準・標準を参照し、それらを活用しながらそれぞれの目的に合った基準・標準が策定されている点が特徴である。そのような参照関係を可視化、整理することで、適用する基準・標準を選択する際の有効な手がかりとなることが想定される。例えば、英国 DCMS では、以下のようなサイトで、セキュリティ基準・標準またはそれを策定した組織の関係性を可視化、データ化[21]している。

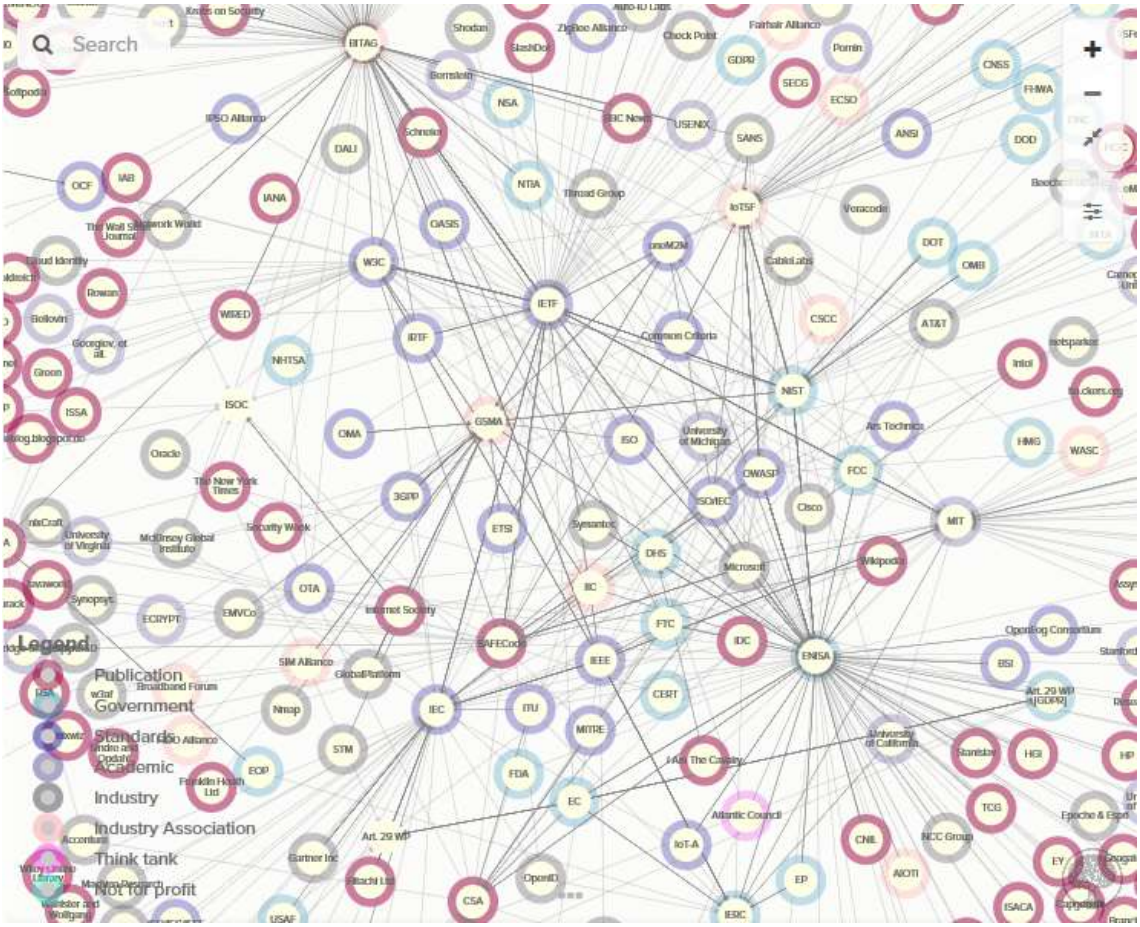


図 4-87　セキュリティ基準・標準を策定した組織の関係[22]

4.5.5　アシュアランスとトレーサビリティの確保

サプライチェーンセキュリティの確保においては、自組織におけるセキュリティの確保だけでなく、取引関係にある他組織が、必要なセキュリティ対策を行っていることを保証すること(アシュアランス)が本質的に重要となる。自組織だけでビジネスが完結していれば、アシュアランスは注目されないが、他組織と協業している場合には必要となる概念がアシュアランスである。

---

[21] https://iotsecuritymapping.uk/wp-content/uploads/2018/10/High-level-relationship-mapping-from-external-references-in-recommendations-and-standards_v1.csv

[22] Copper Horse: Mapping of External References within Guidance and Recommendations https://iotsecuritymapping.uk/by-sector-and-body/

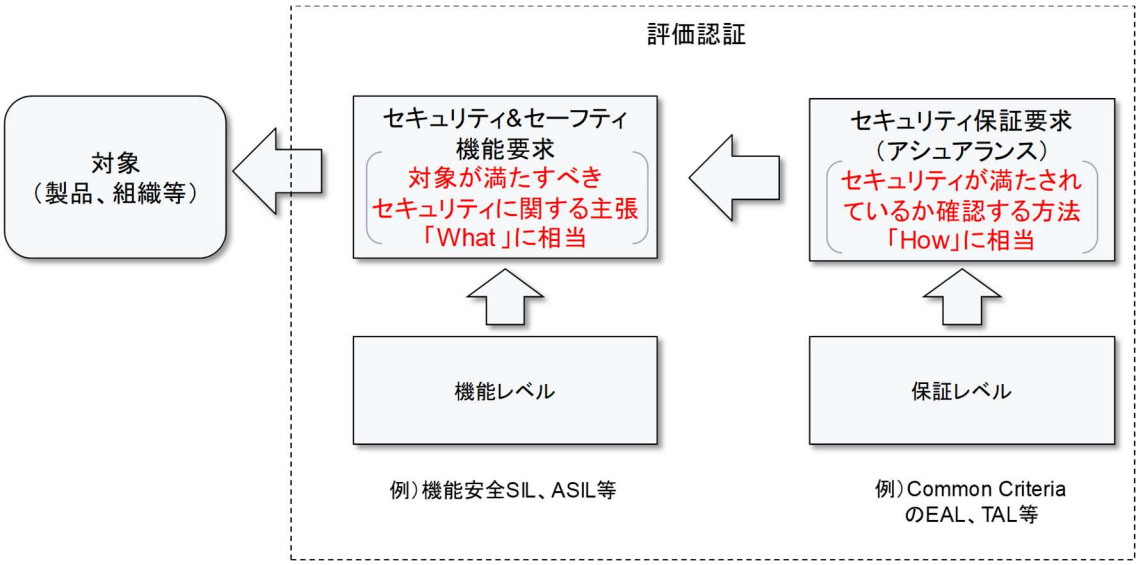


図 4-88　セキュリティ確保とアシュアランスの関係[23]

一方で、アシュアランスのためには、セキュリティ確保に加えてアシュアランスのためのコストが必要となる。また、アシュアランスに求めるレベルにより発生コストも大きく異なる。

コモンクライテリアのセキュリティ保証レベルは、IT 製品やシステムに限定されるが、アシュアランスの概念を明確に定義したものである。コモンクライテリアは、認証取得の負担とコストの問題等で利用しづらい基準と見なされることもあるが、アシュアランスの概念について参考とすることができる。

4.5.5.1 コモンクライテリア評価保証レベル

開発者に求められるセキュリティ機能が、確実に実現されていることを「証明する証拠資料の充足度」を表したものが EAL（評価保証レベル: Evaluation Assurance Level）である。評価保証レベルは、セキュリティ機能自体とは独立に設定される。製品のセキュリティの強度は、「セキュリティ機能要件」により確保され、その機能がどのぐらい確からしいか保証するために、期待される確度とコストを考慮して EAL を設定することになる。

評価保証レベルごとに定義された保証コンポーネントのセットである保証パッケージが指定される。

[23] 三菱総合研究所作成。

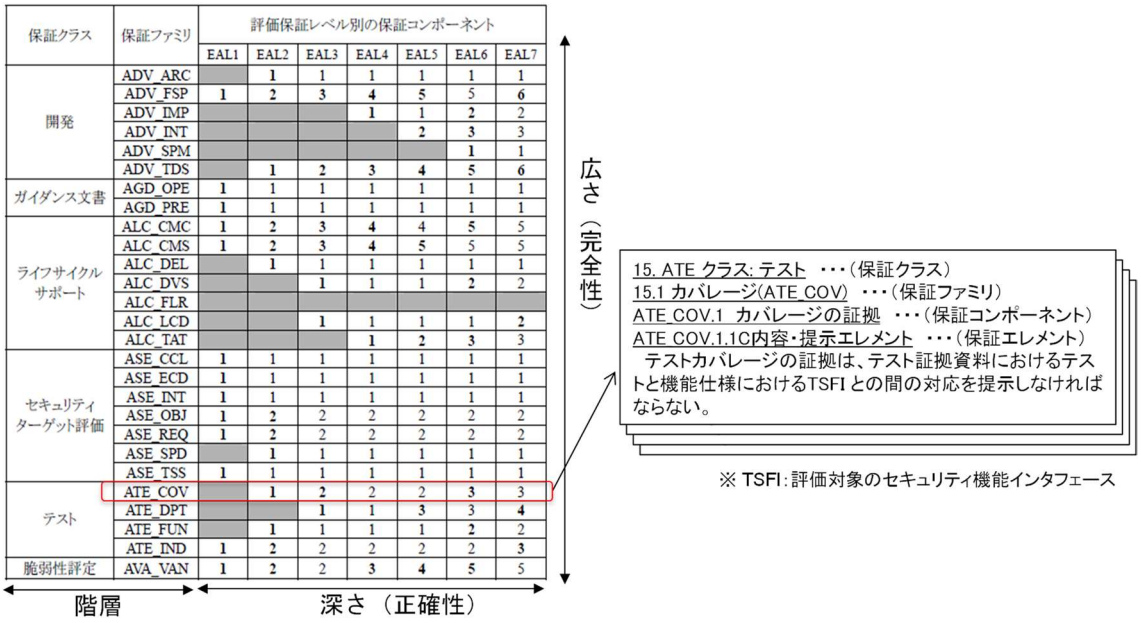


図 4-89　評価保証レベル（EAL）と保証コンポーネントの対応関係[24]

EAL に応じて、セキュリティ保証要件の階層構造のうちコンポーネントの何番まで要求されるかについて規定したものが図 4-89 の左表である。例えば、EAL4 であれば、保証クラス「開発」の保証ファミリ「ADV_ARC」は保証コンポーネント 1、保証ファミリ「ADV_FSP」は保証コンポーネント 4 まで求められることになる。それらをまとめたものが表 4-1 である。

表 4-1　保証コンポーネント（EAL4 に求められる保証要求）[25]

保証クラス	保証コンポーネント
ADV: 開発	ADV_ARC.1 セキュリティアーキテクチャ記述
	ADV_FSP. 4 完全な機能仕様
	ADV_IMP.1 TSF の実装表現
	ADV_TDS.3 基本モジュール設計
AGD: ガイダンス文書	AGD_OPE.1 利用者操作ガイダンス
	AGD_PRE.1 準備手続き
ALC: ライフサイクルサポート	ALC_CMC.4 製造支援、受入れ手続き、及び自動化
	ALC_CMS.4 課題追跡の CM 範囲
	ALC_DEL.1 配付手続き
	ALC_DVS.1 セキュリティ手段の識別
	ALC_LCD.1 開発者によるライフサイクルモデルの定義
	ALC_TAT.1 明確に定義された開発ツール
ASE: セキュリティターゲット評価	ASE_CCL.1 適合主張
	ASE_ECD.1 拡張コンポーネント定義
	ASE_INT.1 ST 概説
	ASE_OBJ.2 セキュリティ対策方針
	ASE_REQ.2 派生したセキュリティ要件

[24] Common Criteria for Information Technology Security Evaluation を基に三菱総合研究所が作成。
[25] CC/CEM バージョン 3.1 リリース 5 （日本語翻訳版）
IPA: セキュリティ評価基準（CC/CEM）
https://www.ipa.go.jp/security/jisec/cc/index.html

保証クラス	保証コンポーネント
	ASE_SPD.1 セキュリティ課題定義
	ASE_TSS.1 TOE 要約仕様
ATE: テスト	ATE_COV.2 カバレージの分析
	ATE_DPT.1 テスト:基本設計
	ATE_FUN.1 機能テスト
	ATE_IND.2 独立テスト - サンプル

評価保証レベルは、一般的な民需用途では、EAL2 から EAL4 まで、軍用や特殊用途は EAL5 以上とされる。コモンクライテリア認証は、CCRA（国際的アレンジメント：Common Criteria Recognition Arrangement）に基づき、一つの国で取得した認証は、協定を結ぶ関係国で有効となる。ただし、この相互承認は EAL4 まで合意される。また、国内の評価機関は、現時点で EAL4 まで評価可能であることから、国内で取得し、国際的に有効な認証とできる EAL は 4 までとなる。

実際には、コストや安全性等を考慮して EAL を設定する必要がある。

表 4-2　評価保証レベル（EAL）の概要 [25]

	評価保証レベル	選択のポイント
一般的な民需用途	EAL1（機能テスト）	セキュリティへの脅威が重大ではない場合に適用され、特定の機能の要件が対処されていることを確認する。 仕様に対する評価者のテスト、ガイダンスの調査など開発者の支援を受けずに最小の費用で評価を実施できる。 EAL1は、評価されていないITに比べ、保証の増加を提供する。
	EAL2（構造テスト）	古くから継承されたシステムの安全性を確保するなど完全な開発資料を提供できないような場合で、低レベルから中レベルの保証されたセキュリティを要する環境で適用できる。開発者からの設計情報と開発者テスト結果の提供レベルで評価を実施する。また、開発環境における構成管理や製品の配付の手続を評価する。 EAL2は、EAL1の保証に加え、開発者テスト、基本的攻撃能力を想定した脆弱性分析、さらに詳細なTOE仕様に基づく評価者のテストを要求する。
	EAL3（方式テスト及びチェック）	中レベルの保証されたセキュリティを必要とし、既存の適切な開発方法を大幅に変更することなく、TOEとその開発の完全な調査を要する状況に適用される。 EAL3は、EAL2の保証に加え、テストの網羅性や開発時のTOE改ざんを防止するメカニズムや手続を要求する。
	EAL4（方式設計、テスト及びレビュー）	既存の商用製品の開発に対し、セキュリティに係るエンジニアリングコストの追加を受け入れられ、中レベルから高レベルの保証されたセキュリティを必要とする場合に適用される。 EAL4は、EAL3の保証に加え、より多くの設計記述、ソースコードなどのセキュリティ機能のすべての実装表現、開発時のTOE改ざんを防止する向上されたメカニズムや手続を要求する。
軍用や特殊用途	EAL5（準形式的設計及びテスト）	EAL5レベルの保証をはじめから達成する意図を持って開発され、高レベルのセキュリティを必要とし、専門的なセキュリティエンジニアリング技法の適用する適切なコストを負担する場合に適用される。 EAL5は、EAL4の保証に加え、準形式的な設計記述、構造化され分析可能なアーキテクチャ、TOE改ざんを防止するさらに向上されたメカニズムや手続を要求する。
	EAL6（準形式検証済み設計及びテスト）	保護する資産の価値が、高い保証のための追加的な開発コストを正当化するようなリスクの高い状況で使用する場合に適用される。 EAL6は、EAL5の保証に加え、さらに広範囲な分析、実装の構造化表現、さらなるアーキテクチャ構造、さらに広範囲な評価者の脆弱性評定、さらに向上された構成管理と開発環境の制御を要求する。
	EAL7（形式的検証済み設計及びテスト）	リスクが非常に高いか、高い資産価値により、さらに高い開発コストが正当化される場合に適用される。 EAL7は、EAL6の保証に加え、数学的検証を伴う形式的表現と対応、広範囲のテストを使用する包括的分析を要求する。

認証に必要な期間は、評価対象の規模や評価保証レベル（EAL）、開発期間によって異なるが、一般に EAL2 の場合で最短でも 4～6 ヶ月が必要とされる。EAL4 の場合、12 ヶ月以上かかる場合もある。認証機関への申請の際に支払う認証申請手数料は、EAL5 で 1,081,500 円であり、認証に必要な費用は、評価機関に支払う評価費用、認証機関に支払う認証申請手数料のほか、ST（セキュリティターゲット：Security Target）作成や、開発プロセスにおいて作成される資料で不十分な場合に、コモンクライテリアで定められた各種証拠資料の準備、評価中に生じる不具合等への対応、テスト環境の準備等の内部工数、あるいはコンサルタントにかかる費用が発生する。

4.5.5.2 トレーサビリティの必要性

アシュアランスを確保する上で、トレーサビリティツールは有効な手段となる。機能安全（セーフティ）の分野では、機能安全に関わる意思決定の説明責任のトレーサビリティを保証することが求められている。

セキュリティ分野では、コモンクライテリアの保証クラス「開発クラス ADV」においてトレーサビリティが要件化されている。図 4-90 に示す通り、セキュリティ課題、機能要件、機能仕様、設計記述、実装表現、実装といった開発成果物についてセキュリティに関連する要素のトレーサビリティを確保することが求められている。

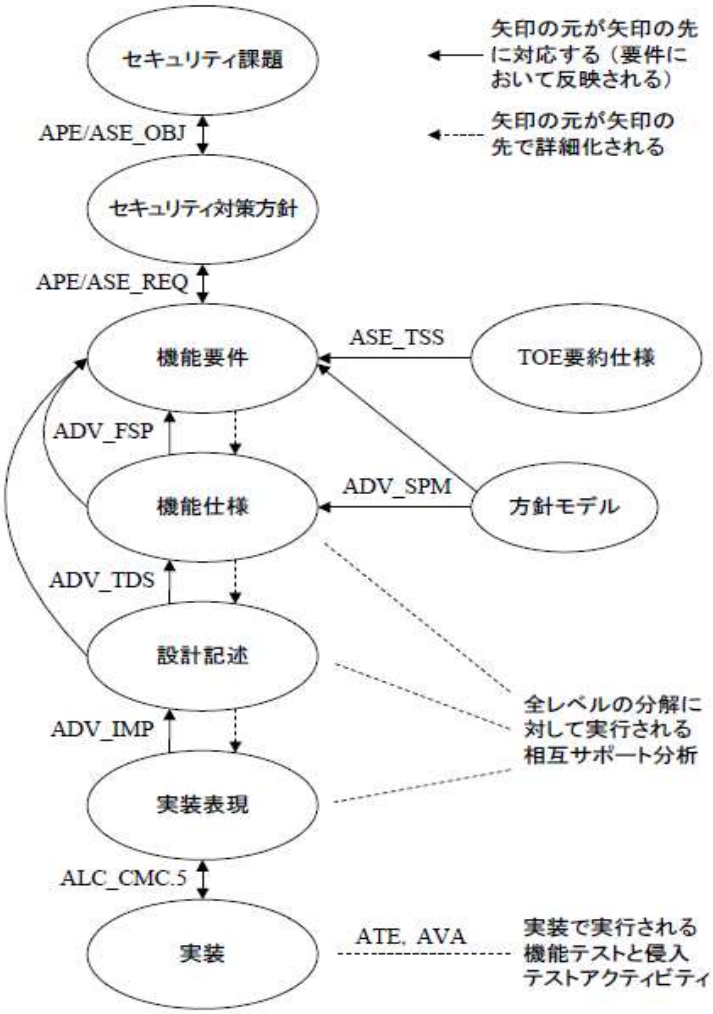


図 4-90　コモンクライテリアにおけるトレーサビリティに関する保証要求 [25]

SIP の研究開発においては、さらに広い概念において、人、モノ、組織、サービス、プロシージャ等についてトレーサビリティの対象やそれらの関係性を具体化・モデル化し、人手ではなく、システマティックに信頼の創出・証明、構築・流通、検証・維持が可能となるような環境を構築することが期待される。

4.6　社会実装における課題と提言

4.6.1　SIP 第 2 期研究開発項目との対応関係

SIP 第 2 期研究開発項目と既存のセキュリティ基準・標準類の要求事項の対応関係を図 4-91 の通り整理し、分析を行った結果は以下の通りである。

4.6.1.1 SIP「(A) 信頼の創出・証明」と既存規格等の関係

SIP の研究項目「(A) 信頼の創出・証明」については、既存の基準・標準の多くのものについて、関連する要求事項が示されていると考えられる。特に IoT セキュリティ対策関連規格において、A1 における機器の信頼基点構築手段としてのデバイス ID 一意性、耐タンパ性の確保、暗号化技術による保護等が最も重視すべき対策の一つとして位置付けられているものと考えることができる。

例として、ENISA, Baseline Security Recommendations for IoT では、デバイス保護の要件としてデバイス ID の認証や暗号化技術が具体的に言及された上で、デバイスの起動時点からこれらの保護が実行・継続されることが求められる（セキュアブート）。これらの信頼基点を根拠に、コミュニケーションのセキュリティとトラストの確保に係る要求が定められており、A2・A3 における真贋性やプロシージャ適格性の検証との対応関係が見て取れる。また、IoT Security Foundation, IoT Security Compliance Framework においては、デバイスのハードウェア、ソフトウェア、認証機構等のそれぞれの対策領域において耐タンパ性確保が個別に要件化されている。これらは必須要件、もしくは Class 1 以上のシステムで必須要件として扱われており、非常に基本的な対策ポイントとして位置付けられている。特にトラストを署名で検証するための認証ルートは必ず耐タンパメモリに保存することが必須要件とされている。また、製造工程における耐タンパ性を確保し、サプライチェーン全体を通じたデバイス保護が要求されている。さらに、参考対策として製造施設の信頼性が十分に検証できない場合の対策を用意しておくことに言及されている。

その他の汎用規格においては、ICT システムとしての一般的な対策要求レベルでの暗号化要件や通信の完全性要件等への言及は見られたが、他システムや他デバイス、他事業者からの検証可能性等に踏み込んだ特徴的記述は見られなかった。

4.6.1.2 SIP「信頼チェーンの構築・流通」、「信頼チェーンの検証・維持」と既存規格の関係

「(B) 信頼チェーンの構築・流通」及び「(C) 信頼チェーンの検証・維持」については、先進的な研究課題であり、既存の標準規格の対策要件との対応関係はあまり見られなかった。国際標準化動向としては ISO/IEC JTC1 / SC 41 における相互運用性、Trustworthiness に関する議論が関連性の高い取り組みである。複数の標準規格のドラフト作成が進行している状況であり、引き続き動向を注視すべきと考えられる。

一方で、個別の論点に関しては現行の規格において対応関係に言及すべき要素も挙げられる。B1 のトラストリストの作成・管理に関する取り組みに関連する事項として、TISAX や CTIA Cybersecurity Certification for IoT Devices の監査済データの共有や信頼機器リストの公表が挙げられる。分野内でのトラストを可視化する試みと考えることが可能であり、目的の類似性を指摘できる。特に TISAX では、監査リストをデータベースとして共有しており、トラストリストをシステム的にシェアする試みと見ることができる。また、ENISA, EU Certification Framework の認証体系では、国別、分野別の認証体系の構築を認めつつ、可能な限り共通的な指針での運用を企図しているため 2019 年 5 月に公表予定の EU Cybersecurity Act の中でどのように位置付けられていくかを確認すべきである。

B2 におけるサイバー攻撃の可視化・極小化、レジリエンシー確保や、C2 におけるインシ

デント分析、不正データ検知等に関連する対策要件に関しては、各規格において一定の言及は見られるものの、自システムへの攻撃への対処・復旧、もしくは直接関係するシステムへの連絡についての記述が中心である。SIP 第 2 期研究開発項目におけるサプライチェーン全体としての対策に関しては、具体的対策要求事項として記述されるケースは現状では見られなかった。

C1 の信頼チェーン検証技術に関しては、一部の規格で同様の主旨の対策要件に関する記述が見られた。ENISA, Baseline Security Recommendations for IoT においては、データ交換の信頼性を保証するための推奨対策としてデータを保存する際は、都度デジタル署名を行うという例への言及がある。この例はブロックチェーン技術等の利用を想定した記述であると思われるが、信頼チェーン検証技術とある程度の関連性を指摘できる。ただし、匿名検証については言及されない。

テーマ区分	説明	詳細テーマ例	汎用			自動車	電力	通信
			US政府系	EU政府系	民間系IoT			
(A)信頼の創出・証明	個々のIoT 機器やサービスのセキュリティを強化し、多様なIoTシステム・サービスやサプライチェーン全体のセキュリティ確保を実現する上で必要な信頼の創出・証明技術の多角的な研究開発	A1 ・機器の信頼基点構築・暗号モジュール ・耐タンパー性確保 ・セキュリティ保証スキーム ・小型IoT機器の暗号実装技術	ICTシステム一般基準レベルの標準的対策を要求	ENISAのIoT規格では、IoT機器のデバイスIDの一意性、耐タンパー性への具体的要求が充実	IoT機器のデバイスIDの一意性、耐タンパー性への具体的要求が充実	ISO/IEC 27001、NIST SP 800-53等を参照する形で標準的対策を要求	ICTシステム一般基準レベルの標準的対策を要求	IoT機器のデバイスIDの一意性、耐タンパー性への具体的要求が充実
		A2 ・真贋性判定	ICTシステム一般基準レベルの標準的対策を要求	デバイスIDを他のデバイスから検証可能であること等を要求	デバイスIDを他のデバイスから検証可能であること等を要求	ICTシステム一般基準レベルの標準的対策を要求	ICTシステム一般基準レベルの標準的対策を要求	ICTシステム一般基準レベルの標準的対策を要求
		A3 ・プロシージャ適格性検証 ・外部イベントからの検証 ・トレーサビリティ確保	ICTシステム一般基準レベルの標準的対策を要求	ノード間通信内容の正当性を都度検証することを要求	ノード間通信内容の正当性を都度検証することを要求	ICTシステム一般基準レベルの標準的対策を要求	ICTシステム一般基準レベルの標準的対策を要求	ICTシステム一般基準レベルの標準的対策を要求
(B)信頼チェーンの構築・流通	多様な社会インフラやサービス、幅広いサプライチェーンのセキュリティを確保するため、IoT システム・サービスや調達・構築に関わるサプライチェーンにおいて「信頼チェーン」を構築し、必要な情報をセキュアに流通させる技術を研究開発する。	B1 ・トラストリストの作成管理 ・サプライチェーンの分野別プロファイル		ENISAがEU Cybersecurity Certification Framework の枠組みを検討中		TISAX規格での監査済データ共有、ULの認定マーク等の取組み		機器の保証レベル認定を公開
		B2 ・トレーサビリティ確保 ・サイバー攻撃の影響範囲可視化 ・サイバー攻撃の影響被害極小化 ・レジリエンシー確保	ICTシステム一般基準レベルの標準的対策を要求	ICTシステム一般基準レベルの標準的対策を要求	ICTシステム一般基準レベルの標準的対策を要求	ICTシステム一般基準レベルの標準的対策を要求	ICTシステム一般基準レベルの標準的対策を要求	ICTシステム一般基準レベルの標準的対策を要求
(C)信頼チェーンの検証・維持	「信頼チェーン」を構築したIoTシステム・サービス及びサプライチェーンにおいて、「信頼チェーン」が安全に運用されていることを検証し、維持することを可能とする技術を研究開発する。加えて、技術成果の社会実装に必要な導入・運用マニュアルや組織・人材開発の取組みも併せて行う。	C1 ・信頼チェーン検証技術 ・匿名信頼検証			ノード間で通信内容の正当性を都度検証することを要求			
		C2 ・サイバーフィジカルインシデント統合解析 ・不正データ検知 ・サイバー攻撃影響評価、対処決定、シミュレーション評価	ICTシステム一般基準レベルの標準的対策を要求	ICTシステム一般基準レベルの標準的対策を要求	ICTシステム一般基準レベルの標準的対策を要求	ICTシステム一般基準レベルの標準的対策を要求	ICTシステム一般基準レベルの標準的対策を要求	ICTシステム一般基準レベルの標準的対策を要求

図 4-91　SIP 第 2 期研究開発項目との対応整理表

4.6.2　SIP 研究開発項目の活用可能性に関する検討と提言

本調査で分析をした社会実装時の課題に対し、SIP 第 2 期研究開発項目の活用可能性を分析した結果を以下に示す。

4.6.2.1 信頼の創出･証明に係る研究開発項目の活用可能性

既存の基準・標準の多くのものについて、SIP「（A）信頼の創出・証明」と対応する要求事項が示されているため、SIP「（A）信頼の創出・証明」の研究成果は、既存の基準・標準の多くのものについて活用されるものと考えられる。

信頼の創出・証明に関連する研究開発項目は、事業者が信頼の創出・証明を実施するために必要となるコストを低減するための活用が有効であると考えられる。

デバイス ID の一意性や耐タンパ性、機器情報の暗号化といった信頼の創出に係る基本的対策要求は現行の対策標準規格において言及される部分が多く存在する。しかし、各対策規格において、信頼の創出を技術的に実現するための要求が比較的具体性を伴って記述される一方、サプライチェーン内の関係者間で信頼の証明を行う手段としては、契約の遵守や監査の実施等の手段に留まる記載が多い。また、アンケート調査の結果から各事業者間でお互いのセキュリティ対策水準を確認することが非常に難しいという事実が課題として明らかになった。信頼の証明及びその検証のプロセスを標準化し、技術的な方策をもって効率化することは、事業者へ大きなコストメリットを提供するとともに、サプライチェーンのセキュリティアシュアランスを強化する余地があるものと考えられる。

4.6.2.2 信頼チェーンの構築･流通に係る研究開発項目の活用可能性

SIP 研究項目（B）に係る対策は、現状としては具体的な対象や体系化がなされておらず、現場では俗人的な対応となっているが、SIP の研究成果が得られれば、体系化されたツールに基づく自動化、効率化も可能となると考えられる。

信頼チェーンの定義・構造の標準化に係る課題に対する技術的な解決策としての活用可能性があると考えられる。自動車分野の TISAX における監査済データベースの共有を通じて信頼可能なサプライヤーを明らかにする試みであると解釈可能であることを分析してきた。しかし、あくまで監査結果合否、認定レベルと簡易な監査レポートを共有する仕組みであり、信頼可能性の定義はシンプルなものである。

B1 にあるようにサプライチェーンの分野別プロファイル等を記述可能にする体系を開発することによって、分野内でトラストリスト作成のための基準を定義し、当該分野におけるサプライチェーンの特徴を考慮した上で、接続許可性・相互運用性等の判断をある程度システマティックに実行可能とすること等が期待できる。

また、こうしたトラストリストに基づく信頼チェーンが事業者間で流通することで、多数のノードが複雑に接続される IoT システムにおいて、B2 にあるようなサイバー攻撃の影響等を効率的に可視化する技術がより活用されることも期待できる。例として、NERC CIP のような動作障害時に関係システムへ与えるインパクトレベルを定義し、これをトラストリストの構造情報として流通するようなことを考える。こうした情報が共有された場合、既存規格の想定する事業者間の直接連絡を行うことなく、個々のノードへのサイバー攻撃の影響が IoT システム全体への影響として可視化・共有され、関係ノードが自律的な判断を行うこと等が可能であればサイバー攻撃への対処効率が大幅に向上するものと考えられる。

4.6.2.3 信頼チェーンの検証・維持に係る研究開発項目の活用性に関する整理

信頼チェーンの検証・維持に関して、信頼の証明と同様にサプライチェーン内で信頼の基準を標準化できるかが重要な論点である。標準化された基準がサプライチェーン内で共有された場合、サプライチェーン内のプロシージャの適格性やインシデント兆候の解析、検知といった検証を通じてサプライチェーンセキュリティの維持に資する活用が期待できる。

アンケート調査の結果では、事業者間でお互いが参照する基準が異なる場合の合意形成の難しさや確認コストの大きさが課題として挙げられた他、機密保持の観点から相手の情報を十分に提供・入手することは難しいという実態が明らかになった。

C1 に係る技術群はこうした課題に対して有効な対策となりえる。例えば複数の対策基準に対応し、相互の対応関係を翻訳可能な信頼検証技術が開発されたような場合、信頼チェーン内での相互評価負荷の削減が期待できる。また、相対する事業者に対して自社の情報を匿名化したまま信頼を検証する技術が導入された場合、機密を保持したままより実効的な評価を相互に実施できるものと考える。

また、C2 に係る技術群は、IoT システム全体として信頼チェーンの正常性を検証・維持することで B2 に係る技術群の効果をより一層高めることが期待できる。既存の各対策基準群では、ほぼすべてにおいてシステムのリスク分析実施が求められる。リスクを評価するためには、脅威情報と脆弱性情報が必要であり、各規格では脅威情報及び脆弱性情報を収集し、また事業者間での共有が要求されるが、IoT システムにおいては、複数のシステムが接続されるほどリスクの全体増の把握とコミュニケーションコストが増大することとなる。匿名検証技術等を活用しつつ、サプライチェーン内でインシデント情報や脆弱性報告情報をデータベース化し、共有することができれば攻撃時の影響評価や不正検知をより高精度に行えるものと考えられる。

4.6.3 今後の動向調査に関する提言

本調査では、サプライチェーンセキュリティに関する基準・標準の要求事項の動向、企業におけるそれらの基準・標準の適用実態調査に基づき、SIP 研究項目との関係性や成果の活用可能性について分析をまとめた。

これらの結果を踏まえて、今後、SIP 研究開発を効果的に進めるためには以下のような動向について調査を行い、SIP 研究開発がより有効なものとなるように反映していくことが期待される。

4.6.3.1 セキュリティアシュアランスに関する標準・技術の動向調査

本調査では、サプライチェーンセキュリティを確保する上で本質的なセキュリティアシュアランスの概念と基礎的な考え方について整理した。近年、EU Security Certification Framework や ISO/IEC 27034-7 Assurauce prediction framework を始めとして、トラストセキュリティを実現する上でセキュリティアシュアランスの確保に基づく取り組みが始まっている。SIP におけるトラストセキュリティの研究を効果的に推進する上で、研究項目に密接に関連し、またサプライチェーンセキュリティの根幹となるセキュリティアシュアランスやその実現手法の一つであるトレーサビリティ確保に関する標準や技術の動向を調査し、その成果を活用して研究開発を促進していくことが期待される。

4.6.3.2 サイバーセキュリティ経済学の動向調査

サプライチェーンセキュリティを強化していく上で、ステークホルダーのインセンティブを高めていくことは重要である。セキュリティ分野には、市場メカニズムが適切に機能し

ない外部不経済や、インセンティブが適切に働かない本質的な問題がある[26]。このような問題を解消し、セキュリティ対策を向上させていく上で、リスクの定量化、可視化に加え、インセンティブの適正化等を含むサイバーセキュリティ経済学の動向を把握することは重要である。また、サイバーセキュリティ経済学に関する特集ジャーナル[27]が企画される等、注目が高まっている分野である。このような最新動向を把握することで SIP 研究成果を社会実装の方法を検討することが重要である。

4.6.3.3 先端応用分野におけるトラストセキュリティの適用可能性に関する調査

フィンテック、ブロックチェーン、AI・ディープラーニング等先端技術を応用した分野が次々と誕生する中で、それらの応用に係わるセキュリティの脅威が高まっている。このような新しい先端応用分野において、SIP の研究テーマであるトラストセキュリティ技術の応用可能性を検討することは、SIP の研究成果の適用範囲を拡大していく上で有効と考えられる。

[26] Center for Strategic and International Studies, Misaligned Incentives in Cybersecurity, 2017
[27] The International Journal of eScience, Future Generation Computer Systems, Special Issue on Economic Aspects of Cybersecurity and Privacy, 2018 Call for Papers, Elsevier

5．IoT ネットワークのセキュリティに関する動向調査

5.1　調査の全体像

ネットワーク技術やインターネットデバイスの進化と普及によって、IoT は産業用やコンシューマー向けに広がりつつある。その中で、モビリティが要求される IoT デバイスをインターネットにつなげるためには、現状では 4G ネットワークが利用されているが、この 4G ネットワークは、スマートフォンに代表される端末を人が使い、インターネット等に接続してデジタルサービスを快適に利用できるように技術仕様が策定され、装置もそれに最適に対応できるよう設計されている。そのため 4G ネットワークにおいて人が介在しない多数の IoT デバイスが通信するような利用ケースにおいては多くの課題が存在する。たとえば、4G ネットワークでは、通信遅延が 50ms 程度、基地局当たりの同時接続が数百台程度、多量の IoT デバイスが同時に大容量の通信をしようとすると通信速度が不足、IoT デバイスに必要なバッテリー容量の確保等、様々な課題がみえている。これらの課題を解決できると期待されているのが 5G ネットワークで、日本では 2020 年に商用サービスが開始されることになっている。

しかし、このような IoT/5G 時代のネットワークは二つの側面でセキュリティのリスクが高くなる。それは、上述したように 5G がより IoT のユースケースへの適用性が高くなることで、ホームネットワークのようなコンシューマーIoT だけでなく、企業や官公庁を含めた重要インフラに関連するアプリケーションがネットワークを利用することが可能になるため、システムへのサイバー攻撃が成功したときの経済的損害は甚大なものになると想定されることと、5G のネットワークを構成する機器で使用されるソフトウェアや部品にオープンソースを活用する等のオープン化が加速することでサプライチェーン上のリスクが増し、不正なソフトウェアの混入やソフトウェアの改ざんによる新たな攻撃の可能性が増すことになる。

電力や金融、水道、鉄道等、Closed な専用の自営ネットワークを組んでいる既存の重要インフラ事業者が、ネットワークを高度化することで、業務の効率化やユーザーへの付加価値の向上を実現するために、通信インフラとして 5G を利用していくことも想定され、また、コネクテッドカーや遠隔医療、ドローンの運航管制等、サイバーとフィジカルが融合した新しい分野での利用も期待されている。このように今後の重要インフラのアプリケーションを支える 5G ネットワークにサイバー攻撃が成功すると、社会インフラや経済活動の広範囲な停止やユーザー情報の漏洩だけでなく、フィジカル世界で重大な事故を招いてしまう危険性もある。

一方、5G ネットワークに対する新たなサイバー攻撃の手法として、FCC（米国連邦通信委員会: Federal Communications Commission）が 2018 年 9 月に発行したレポート[28]にあるように、ネットワーク機器に unwanted functionality と称する不正なプログラムがオープン化等によるサプライチェーン上で混入されるリスクが指摘されている。内部に潜んでいる不正なプログラムは、そこを起点としてサービス停止、盗聴、なりすまし、改ざん等のあらゆるサイバー攻撃が可能になる最大の内部脅威である。

5G ネットワーク機器はソフトウェアで実装される要素が増えており、基地局、コア、ルータ等の機能がサーバー等の汎用機器上のソフトウェアで実装されるようになる。さらに MEC (Multi-Access Edge Computing) と呼ばれる基地局に近いネットワークのエッジ部分で、クラウドのアプリケーションの一部が動作するようになり、そこから 5G ネットワークに内部から攻撃が行われる危険性もでてくる。このように、5G ネットワークは IT のサイバー攻撃の手法が適用されやすくなり、内部に潜んだ不正プログラムのサイバー攻撃の影響は計り知れない。

---

[28] FCC: Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging 5G Wireless Networks v14.0
https://www.fcc.gov/files/csric6wg3sept18report5gdocx-0

4G 以前のネットワークで指摘されていたローミング先からの攻撃や偽基地局による IMSI (International Mobile Subscriber Identity) 詐取等の表面化した課題は、5G ネットワークの技術仕様策定において対策が盛り込まれていく。今後、新たな問題が判明する可能性はあり、サービス開始後の脆弱性の有無は現時点では予想できないが、そのような技術仕様上の脆弱性は技術仕様策定の場にて修正されるものと想定する。

そこで、今回の調査のターゲットは、5G ネットワークのセキュリティ課題として注目されている不正プログラムの混入対策についての各国・産業での議論、法制度化の動向の調査を実施した。不正なプログラムは、その検体があるわけではなく、かつ、通常のロジックを処理される正常のプログラムに紛れて混入されることが想定され、不正なプログラムであることを特定することは技術的に難しい。そこで、日本国における最良な対策を検討するため、機器やシステムの調達を含めた法制度やガイあドライン等の動向や、民間の取り組みについて調査を行った。

図 5-1 に本調査の全体像を示す。

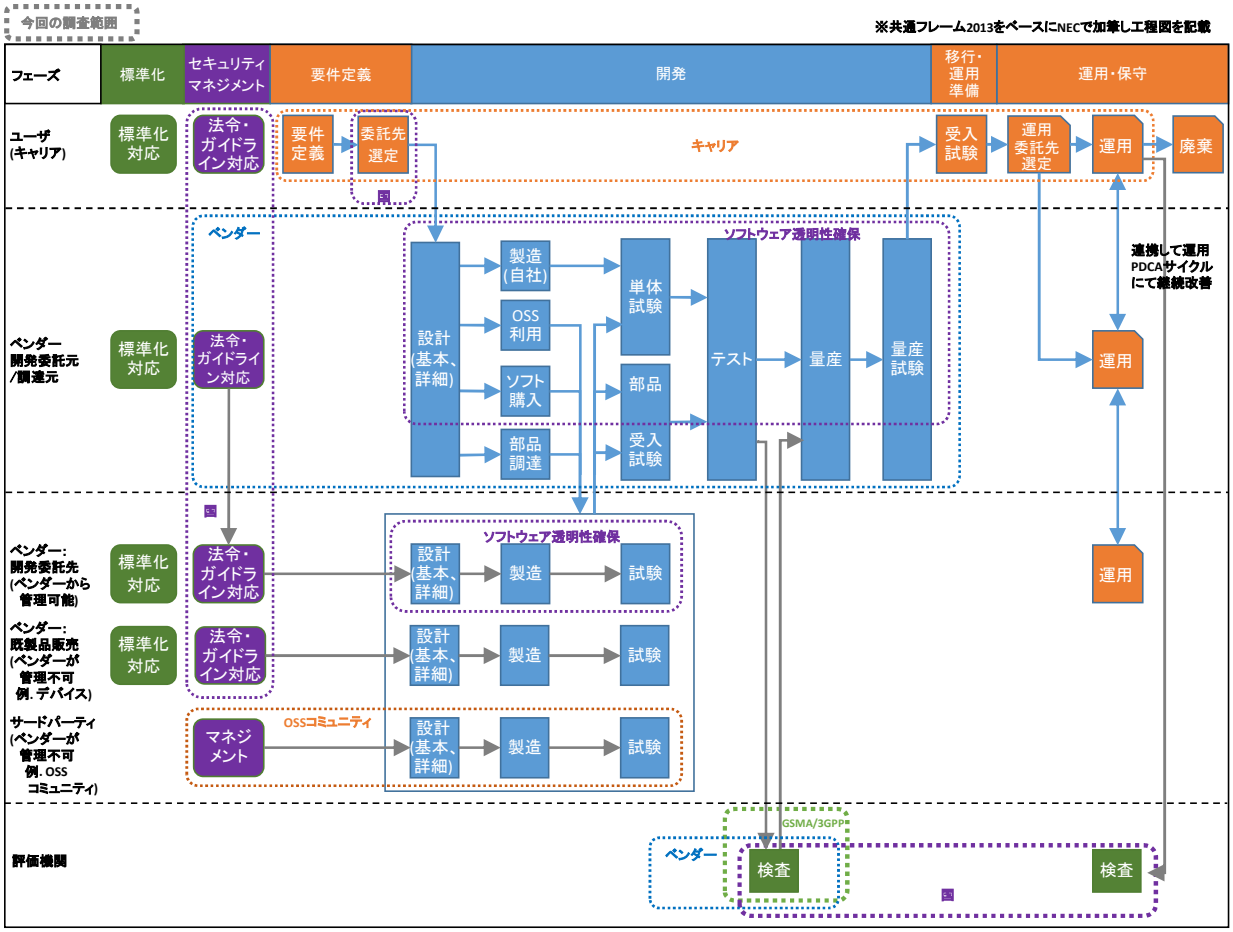


図 5-1　調査の全体像

全体像で用いている共通フレームとは、ソフトウェア、システム、サービスの構想から開発、運用、保守、廃棄に至るまでのライフサイクルを通じて必要な作業項目、役割等を包括的に定めたもので、システム開発を委託する際等に発注側と受注側の間に誤解が生じないように、汎用的な用語や各工程の内容（分類）を標準化するために制定されたものである。共通フレーム 2013 は、ISO/IEC 12207 を翻訳した日本工業規格 JIS X 0160:2012 をベースに制定されている。全体像においては、共通フレームをベースにカスタマイズしたものを用いている。

IoT ネットワークのシステムにおいては、共通フレームにおけるステークホルダー（役割:ロール）としてユーザー（キャリア）、ベンダー、OSS（オープンソースソフトウェア）コ

ミュニティ、評価機関、国を設定している。

キャリアは、各通信会社であり、構築されたネットワークを実際に運用して、ユーザーへの通信サービスの提供と、そのネットワークの運用、保守を行う。IoT ネットワークのベンダーは、ネットワーク機器の部品調達、装置の開発製造を行うベンダーである。OSS コミュニティは、ソフトウェア開発において利用される OSS のコミュニティである。国は、重要インフラの監督やセキュリティに関する法令・ガイドライン、調達基準、認証制度等の制定を行う各国における政府機関である。評価機関は、製造された製品の評価、検証の内容の詳細化やその検証を行う。

このため、IoT ネットワークのセキュリティに関する動向調査では、全体像で示すようなシステムやサービスの構想から開発、運用、保守に至るまでのライフサイクル工程において関連する各国政府、キャリア、ベンダー、OSS コミュニティ、評価機関の動向調査を行った。

表 5-1　調査の対象国

対象	調査内容の概要	調査先
国	政府調達や重要インフラの監督をする立場として、セキュリティに関する法令・ガイドライン、調達基準、認証制度等の動向について調査	米国、オーストラリア、英国、フランス、ドイツ、EU、スウェーデン、インド、中国の 8 ヵ国 1 地域
ベンダー	部品調達、製品開発を行う立場として、セキュリティマネジメント（法令・ガイドライン対応）、調達品や製品のセキュリティプロセス等について調査	主要通信機器ベンダー4 社 Ericsson、Nokia、Huawei、Cisco
OSS コミュニティ	様々なメンバーが参加可能な OSS の利用が進むことから、OSS コミュニティの体制面やセキュリティプロセスについて調査	SDN/NFV 関連の 3 コミュニティ Openstack、OPNFV、ONOS
キャリア	製品を調達する立場として、受入試験や運用対策について調査	主要国のキャリア 4 社 AT&T、DT、Telstra、Orange
評価機関	製品の評価に関する内容、方法、レベル等について調査	GSMA の NESAS インドの認証機関

5.2　各国の政策動向に関する調査

5.2.1　調査目的

IoT ネットワーク（5G）の構成のサプライチェーンにおけるリスクに対して、各国の政策での対策について調査を行い、今後取り組むべき方向性をつけていくための情報を収集した。調査の対象国は、米国、オーストラリア、英国、EU、フランス、ドイツ、スウェーデン、インド、中国とした。

これらの国について、各国の政策（法令・ガイドライン）を把握するため、デスクトップ調査を次の 4 点の観点で行った。

- IoT セキュリティ全般に関する政策、
- 重要インフラに関する政策
- 政府調達に関する政策
- 今後の方向性

5.2.2　各国の政策動向

デスクトップ調査の結果から、各国の政策動向の概要を表 5-2 にまとめた。

表 5-2　各国の政策動向（まとめ）

国	概要
米国	政府データの保護のため政府調達規制を基軸に各政府機関がセキュリティ基準を設定。DoD（Department of Defense）配下の DISA（米国国防情報システム局: Defense Information System Agency）では DISA 発行の基準に基づく認定制度を採用、認定リストが活用されている。2018 年 8 月に米国国防授権法が成立、今後、技術的な基準に加えて特定国/企業の排除が実施される可能性がある。
オーストラリア	現行法令にて、基本的な個人情報保護やデータ侵害・セキュリティ侵害の通知義務、特定商品・サービスの輸出制限等を規定している。システム・ネットワークの政府調達では、EPL（Evaluated Products List）からの選択を義務付けている。国家安全保障上の懸念に基づき特定国/企業に対し、5G 展開に関連しネットワーク技術を提供する契約への入札が禁止された。
英国	セキュリティに関しては GDPR/NIS 指令を国内法に置き換えることで対応。政府調達においては、政府機関による認証プログラム（Cyber Essentials）を規定し活用。
EU	GDPR 及び NIS 指令により欧州全体のサイバーセキュリティを強化中。2017 年にサイバーセキュリティ強化に向けた政策パッケージを公表、ENISA の強化とサイバーセキュリティ認証の枠組み「ICT サイバーセキュリティ認証に関する規則案」を発表した。今後は同政策パッケージに沿ってセキュリティ強化が図られる。
フランス	EU と足並みを揃える形でサイバーセキュリティを強化中。Military programming Act for the years 2019 to 2025 にて ANSSI と電気通信事業者に情報システムの安全のための権限を付与しており、今後 ANSSI を中心に対策が進むと思われる。政府調達において、EU 域外からの入札は WTO 多国間政府調達協定国、または公的機関入札で EU と協定を結んでいる国に制限している。
ドイツ	情報セキュリティ管轄の政府機関 BSI が中心となり、重要インフラ

国	概要
	の保護対策/セキュリティ製品認証/セキュリティ評価機関の認定等を推進する。政府調達に関しては、BSI 提供のガイドラインに基づく認証制度にて、BSI 認定テストセンターによる適合性評価が実施されている。現在策定中の IT Security Act 2.0 にて、組織モニタリングや罰則指令等 BSI の権限は拡大される見込。
スウェーデン	EU と足並みを揃える形でサイバーセキュリティを強化中。安全保障関連の調達に関しては、Protective Security Act (2018:585) に記載されており、この中でセキュリティ保護の調査実施やセキュリティ対策の計画・実施を求めている。国防に関する IT 関連システムに関しては国防省傘下の独立機関 CSEC が認証を行っている。
インド	DoT Guidelines にて DoT ライセンシ（免許を受ける事業者）に対するネットワーク機器・サービス・ソフトウェアの脆弱性やバックドアチェックの確認等の強化義務を規定している。政府調達においては国産製品優遇を推進。今後、通信領域に関し Telegraph Rules による通信機器の試験・認証の導入が予定されており、通信機器のテスト及び認証手順が定められた。
中国	2017 年制定のサイバーセキュリティ法(サイバーセキュリティの義務や個人情報の保護に関する義務を規定）にて、ネットワーク事業者/重要インフラ事業者が遵守すべき義務を記載、国策/国防の観点からサイバー空間の監督を強化している。重要インフラ運用者には安全性評価実施が義務付けられ、必要基幹ネットワーク機器やセキュリティ製品の販売/使用には、国家インターネット安全弁公室が実施する安全審査に合格（認定リストに記載）する必要がある。

5.2.2.1 米国

5.2.2.1.1 国としての全体的な状況(まとめ)

米国の政策動向の概要を表 5-3 に示す。

表 5-3　米国の政策動向（まとめ）

	項目	概要
現状	全体傾向	原則、特定の SW/HW/NW を排除するものではなく、各セクター毎にデータセキュリティ/マネジメントに関し、政府レベル/州レベルで規制/ガイドラインを規定していた。2019 年 8 月に政府機関のシステムの重要な要素として Huawei/ZTE 製の通信機器の使用・調達・契約更新を禁止する米国国防授権法が成立。これまでの技術的な基準にに加えて、特定国/企業の排除等が重要インフラ調達において実施される可能性がある。
	重要インフラの法制度	原則、業界のベストプラクティス及び官民のパートナーシップに基づいて運用している。ただし、通信会社や外資系企業に対しては、適宜規制を適用。通信会社に対するインシデント発生時の通知義務を規定している。政府と各企業の合意に基づき、外資系企業に対して追加のセキュリティ要件を規定することができる。
	政府調達	政府データの保護のため、政府調達に関する規制を基軸に、各政府機関が独自のセキュリティ基準を設定。例えば、DoD では契約時に特定の種類のデータを扱う企業に対して課す要件を規定している。DoD 下の米国国防情報システム局 (DISA) では、調達に際して DISA 発行のセキュリティ技術実装ガイド Security Technical Implementation Guides (STIGs) に基づく認定制度を採用している。
	認証/認定制度	DISA 調達に際して、STIGs に基づき DISA の統一機能認証局 (UCCO) が認定する承認製品リストにて規定される。対象機器は、主に VVoIP (Voice and Video over Internet Protocol)、MCU、Firewall、IPS、LAN スイッチ、メディアゲートウェイ、アクセスコントローラー、ルータ、VPN 等、通信関連の HW/SW。UCCO が承認した米国国内の五つのテストセンターにて行われる。海外生産の機器や外国メーカーを排除する規定はないが、すべての情報をさらして検査を受ける必要がある上、定期的に検査を受ける必要があり、そのハードルは高い。
	体制	DoD (Dept of Difense)、DoC (Dept. of Commerce)、DHS (Dept. of Homeland Security) 等の各政府機関において、それぞれセキュリティ運用が行われる。DoC 配下の NIST において、情報の取り扱い規定等の各種ガイドラインが策定されている。
今後	全体的な傾向	2018 年 9 月発表の国家サイバーセキュリティ戦略に基づき、積極的なセキュリティ対策への移行がなされる見込み。政府調達においては、2019 年に FAR の改定が見込まれており、各機関の規制の統一へ向かうと予想されている。
	重要インフラの法制度	国家サイバーセキュリティ戦略に基づき、5G へ向けたセキュリティ対策及び特定の中国通信機器メーカーの調達に関する大統領令の発効が予想されている。特定のベンダー名の記載に関しては不明であるが、DoC 調達への影響が予想されている。

	項目	概要
	政府調達	関連法案の改正による規制の拡大・強化が予想される。NDAA 法では、米国内政府機関に対して、2019 年 8 月、同法の対象となる製品・サービスを実質的・本質的に利用している機器、システム、サービスの購入/取得/利用が禁止している。2020 年 8 月、同法の対象となる製品・サービスを実質的・本質的に利用している機器、システム、サービスを利用している企業との契約/取引を禁止している。

現在の米国における IoT セキュリティに関する規制や規則は、原則、特定のソフトウェア、ハードウェア、及びネットワークを選び出して排除するものではなく、各セクターによって内容が異なり、主にデータのセキュリティ及びマネジメントについて規定されている。米国では、連邦政府（または政府の関連機関）及び各州において規制が制定されている。例えば、連邦政府では、各政府機関における情報セキュリティの保護に関する規制 FISMA (Federal Information Security Management Act) や各セクターにおける規制 HIPAA (Health Insurance Portability and Accountability Act) Security Rule、GLBA (Graham-Leach-Bliley Act) §501 等を規定している。また、ニューヨーク州、オハイオ州、マサチューセッツ州、及びネバダ州の各州では各管轄下における IoT セキュリティに関する規制を規定している。また、法令に加え、ガイドライン等のセキュリティ対策を推奨する制度も規定されており、連邦政府では、サイバーセキュリティに関するフレームワーク NIST (National Institute of Standards and Technology) Cyber Security Framework v1.1 や各セクターにおける情報セキュリティに関する基準 HSS (Dept. of Health & Human Services) Guidance、Interagency Security Guidelines Establishing Information Security Standards を規定しており、各州においては、フロリダ州が州の各機関におけるサイバーセキュリティに関する基準 FCS (Florida Cybersecurity Standards) を規定している。

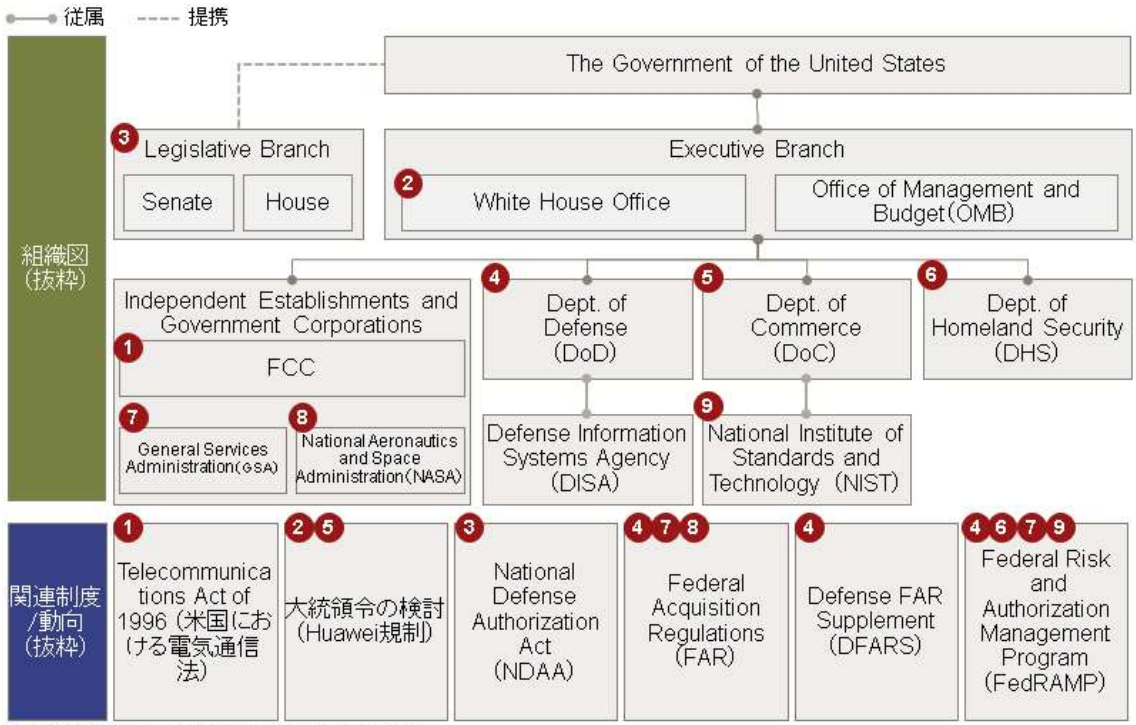
重要インフラについては、通信インフラに関する体系的な規制はなく、原則、通信業界のベストプラクティス及び官民のパートナーシップによって運用されている。ただし、通信会社に対してインシデント発生時の通知義務 47 C.F.R. (Code of Federal Regulations) Part 4、47 C.F.R. § 64.2011 を規定していたり、外資系企業に対して、政府との交渉に基づく契約に従い、追加の要件を課したりできる制度 NSA (Network Security Agreement) も存在する。

政府調達については、政府データの保護を目的とし、政府調達時のプロセスにおいて IT システムの契約会社に課す規制 FAR (Federal Acquisition Regulations) 52.204-21 を基軸に、各政府機関が独自のセキュリティ基準を設定している。例えば、DoD (Dept. of Defense) との契約では、特定の種類のデータを扱う際の要件 DFARS (Defense FAR Supplement) を規定している。さらに、クラウドサービスについては、政府の認証プログラム FedRAMP (Federal Risk and Authorization Management Program) を規定しており、サービスに求められるセキュリティの要件を示している。

今後に向けては、White House が国家のサイバーセキュリティ戦略 National Cybersecurity Strategy を発表し、積極的なセキュリティ対策を行うことを表明したり、政府の関連機関 NHTSA (National Highway Traffic Safety Administration) が自動運転におけるセキュリティや暗号化等に関する規制 (policy paper) の検討を始めたりしている。また、重要インフラについては、特に 5G へ向けた通信インフラのセキュリティの強化及び中国通信機器メーカーによるサイバーセキュリティの脅威への対処が検討されており、国家サイバー戦略に基づいた通信ネットワークセキュリティの保護及び強化や、特定の中国通信機器メーカーの製品を排除する大統領令の検討がなされている。政府調達については、関連制度の改正（FAR の改正及び FedRAMP Reform Act of 2018）により、各政府機関で形式化されていなかった規制が統一化へ向かうことが見込まれている。また、超党派による立法化の動きが見られている他、特定の中国通信機器メーカーの製品の調達・使用を禁じる規制 NDAA（国防授権法: National Defense Authorization Act 2019）の制定も行われてい

る。Huawei 等の中国企業の調達に関して、昨年上下両院にて NDAA 法が可決された。また、Huawei に関する新たな規制が大統領令として検討されている。

図 5-2 は、米国における政府関連組織と関連法制度をまとめたものである。番号により、組織と法制度の関連性を表現している（組織の概要は表 5-4 を、法制度の概要は表 5-5 を参照）。米国においては、DoD（国防総省:Dept of Defence）、DoC（商務省: Dept of Commerce）、DHS（国土安全保障省: Dept. of Homeland Security）等各政府機関や NASA（航空宇宙局: National Aeronautics and Space Administration）等の独立機関において、それぞれセキュリティ運用が行われる。FAR（連邦調達規則: Federal Acquisition Regulations）は、すべての連邦政府機関による調達に伴う規制を網羅したもので、調達を迅速に行えるよう各段階でのガイドラインを提示している。FAR は、DoD/GSA（一般調達庁）/NASA が共同で発行、維持している。また、国防に関する調達は DFARS（国防総省調達規則）に記載されている。NIST（米国国立標準技術研究所: National Institute of Standards and Technology）は、商務省配下の技術部門であり、米国の技術革新や産業競争力強化のための計測学、企画、産業技術の促進をミッションとする。NIST は情報セキュリティを強化し、安全に運用するための様々な規格やガイドラインを策定している。米国における電気通信法である Telecommunications Act of 1996（連邦テレコム法）は、FCC（連邦通信委員会）が所掌している。



各関連制度/動向と関連する省官庁の番号と対応
出所(The United States Government Manualおよび各種資料より抜粋)

図 5-2　米国の政府関連組織と関連法制度

表 5-4　米国における政府関連組織

OMB	米国合衆国行政管理予算局。 予算教書の作成、予算執行、各行政機関の活動を管理。
FCC	連邦通信委員会。 放送通信事業の規制の監督。
DoD	米国合衆国国防総省。 沿岸警備隊、米国公衆衛生局士官部隊、合衆国海洋大気局士官部隊を除く陸軍、海軍、空軍、海兵隊の四つの軍を傘下に収める陸海空軍の各省

	の統括組織。
DoC	米国合衆国商務省。 経済成長、技術競争力、持続的発展を促進するインフラを整備することによって、すべての米国人のために雇用の創出と生活水準の向上を図る。
DHS	米国合衆国国土安全保障省。 公共の安寧の保持を所掌事務とする。テロリズムの防止、国境の警備・管理、出入国管理と税関業務、サイバーセキュリティ、防災・災害対策を行う。
DISA	米国国防情報システム局。 軍事通信、電波監理や通信システムの開発等を担当する国防総省の内局。主要任務は、通信、戦闘支援情報処理、情報保証、統合指揮統制、統合共同運用支援の五つ。
NIST	米国国立標準技術研究所。 技術革新や産業競争力を強化するために、経済保障を強化して生活の質を高めるように計測学、規格、産業技術を促進。

表 5-5　米国における関連法制度

Telecommunications Act of 1996	米国における電気通信法。
大統領令の検討（Huawei 規制）	トランプ政権において、今後数週間以内（2019 年 2 月 4 日時点）に大統領令の発効が予想されており、これにより中国を拠点とする通信機器ベンダーが自社のネットワーク機器を米国の通信キャリアへ販売することが困難になる。
NDAA	国防授権法。 特定のメーカーを指定して調達を禁ずる規制も出てきている。2018 年に成立した同法は、Huawei 及び ZTE をはじめとする特定の中国の通信機器メーカーからの調達を禁じる規定が盛り込まれている。
FAR	連邦調達規則。 米国の政府調達に関する一般的な調達原則を定めたもので、入札招請から契約に至る完全かつオープンな競争手続を規定している（ただし、バイ・アメリカン法の適用は妨げられない。）が、「国家非常事態における製品・サービスの供給源維持及び産業動員基盤確保のために特定の供給源と契約しなければならない場合」や、「供給源の数を制限しない限り、機関がそのニーズを開示することによって国家安全保障が脅かされる場合」は、そのような競争手続に従わなくてよいとしている。
DFARS	国防総省調達規則（補足）は FAR の補足事項を定めたものであるが、「国家安全保障プログラム下のいかなる国防省の契約も、当該契約を実行するために制限情報にアクセスする必要がある場合には、外国政府がコントロールしている機関の所有企業には付与されない」として外国企業を排除する規定を設けている。
FedRAMP	米国政府機関のクラウド調達基準。 クラウドの製品やサービスに対するセキュリティ評価、認証、継続的監視に関する標準的なアプローチを提供している。

5.2.2.1.2 対応状況

a. IoT セキュリティ全般

現在の米国における IoT セキュリティに関する規制や規則は、原則、特定のソフトウェア、ハードウェア、及びネットワークを選び出して排除するものではなく、各セクターによって内容が異なり、主にデータのセキュリティ及びマネジメントについて規定されている[1]。米国では、連邦政府（または政府の関連機関）及び各州単位で規制が制定されており、一部例外は存在するものの（連邦政府における規制よりも、州における規制の方が厳格なケース等）、原則、双方の規制の内容に関して矛盾はない[36]。連邦政府が規定する規制として[34]、例えば、FTC (Federal Trade Commission) Act §5 では、FTC により、不公平または不正な取引慣行に対する実行活動の手引きが具体化されている[3]。また、FISMA では、各政府機関に対して、情報の不正なアクセスや改変等に起因する危害のリスクやその度合いに応じて、情報セキュリティの保護に関する規定を義務付けている[8]。セクター別に見ると、例えば、ヘルスケア分野では、HIPAA Security Rule が制定されており、HHS により医療機関等の対象事業体及びその関連事業体に対して、健康情報の取扱い方に関するセーフガードの適用が義務付けられている[4]。また、金融分野では、GLBA § 501 が制定されており、各金融機関に対して、顧客の非公開情報の安全性及び機密性の保護を義務付けている[6]。

ニューヨーク州、オハイオ州、マサチューセッツ州、及びネバダ州の各州では各管轄下における IoT セキュリティに関する規制は次の通りである。ニューヨーク州では New York Dept. of Financial Services Cybersecurity Regulations、オハイオ州では Ohio SB (Senate Bill) 220 Cybersecurity Safe Harbor、マサチューセッツ州では Massachusetts Standards for the Protection of Personal Information、ネバダ州では Nevada Encryption Law をそれぞれ規定している。Ohio SB 220 Cybersecurity Safe Harbor では、オハイオ州において、各組織が何らかのサイバーセキュリティフレームワーク（後述する FedRAMP 等）に適切に準拠している場合、データ漏洩時の通知義務に関するセーフハーバーを提供している[10]。

上述の規制以外に、自発的なセキュリティ対策を促すフレームワークやガイドラインが規定されている。連邦政府が規定している代表的なフレームワークとして、NIST Cybersecurity Framework v. 1.1 がある。このフレームワークは、2018 年 4 月に改定されており、NIST により、各組織が自発的にサイバーセキュリティ対策を推進することを目的とし、作成されている[2]。米国の政策レベルに求める最低限のセキュリティ管理水準とされており、機能を五つの要素として特定 (Identify)、保護 (Protect)、検知 (Detect)、対応 (Respond)、復旧 (Recover) に分解し、サイバーセキュリティリスクの管理に関する基準を提示している[58]。また、各セクターにおいてもガイドラインが制定されており、例えば、ヘルスケア分野では、HHS により健康情報の保護に関するガイドラインが規定されており[5]、金融分野では、Interagency Security Guidelines Establishing Information Security Standards により、顧客の情報のセキュリティを保護するために管理上・技術上・物理上のセーフガードの基準となるガイドラインを規定している[7]。

b. 重要インフラ

重要インフラについては、特定の種類のデータ（個人の健康情報や顧客所有のネットワーク情報等）に関してサイバーセキュリティの要件を課しているが、通信インフラには体系的な規制があるわけではなく、基本的に通信業界のベストプラクティス（ネットワーク全体の適切な場所にファイアウォールを設置する等が該当[44]）及び広域なコミュニケーションエコシステムの確立を図る官民のパートナーシップ（民間企業が米国政府とリアルタイムにサイバー空間における脅威情報を共有する中央ハブ機関に相当する ISAC (Information Sharing and Analysis Center) 等が該当[45]）により運用されている。例えば、通信会社

は自社の慣行を NIST Cybersecurity Framework に照らし合わせ、NCCIC にリアルタイムにサイバー空間における脅威情報を共有することが奨励されており、大部分の企業は実施しているものの、義務付けられているわけではない [23]。ただし、海外の事業体または個人によって過半数が所有されている通信会社は、米国政府との交渉による NSA に基づいて、追加の要件が課される対象となりうる [25]。NSA では、自発的な業界のベストプラクティス（NIST Cybersecurity Framework 等）を監査が可能な要件にすることができる。例えば、米国政府による承認が必要なサイバーインシデントへの対応計画の策定が求められたり、NIST のフレームワークへの追従が必要になったりする [26]。また、外資系企業（厳密には定義されていないが、投資関連の規制に基づくと、一般的に少なくとも一人の外国投資家が 10%以上の非受動的株式（non-passive interest）を保有する企業が該当 [46]）に対して国内企業以上に厳格な要件を課すことができる。例えば、米国政府は、外資系企業に対して特定の機器ベンダーやサービスプロバイダーとの契約を規制する可能性があるが、国内企業には同じ措置が課されることはないといったことがある [27]。実際に適用された事例として、機密な詳細を開示することなく、米国政府が通信プロバイダーに対して、ネットワークから特定のベンダーのすべての機器の取替（“Rip and Replace”）を課した一方で、このベンダーを長期に渡りネットワーク全体で遍く使用していた国内企業の競合他社に対しては、その排除が義務付けられなかったといった先例がある [47]。

また、通信会社には、2 種類のインシデントが発生した際に、FCC への通知義務が課されている。すなわち、47 C.F.R. Part 4 では、通信ネットワークが停止してしまった際に、FCC へ Network Outage Reporting System を通じて通知することを義務付けており、また、47 C.F.R. § 64.2011 では、データ漏洩が発生した場合に、Data Breach Reporting Portal を介してインシデントを通知することを義務付けている [24]。

c. 政府調達

政府調達については、政府データの保護のために、契約企業に対してサイバーセキュリティに関する要件を課している [16]。FAR 52.204-21 は、幅広な政府案件に適用されている規制であり、政府調達における各プロセスにおいて、IT システムの契約会社に対して、セーフガードの要件を満たすことを義務付けている。一般的に、これらの要件は基本的なものであるため、大部分の政府機関は、この規制に加えて独自のサイバーセキュリティ要件を設定している [17]。その中でも最も洗練されているものとして、DoD との契約における要件が挙げられる。特に、FAR の補足事項として規定されている DFARS 252.204-7012 では、特定の種類のデータ（Covered Defense Information (CDI)）を扱う契約会社に対して、サイバーセキュリティマネジメントの基準を満たす IT システム上で情報を保持することを義務付けている。また、漏洩が発生した場合の特定の通知要件や CDI を保持する外部のクラウドサービスプロバイダーに関する要件も含まれている。さらに、DFARS 252.239-7010 では、クラウドサービスを政府に直接提供している企業に対する追加の要件が含まれており [18]、Cloud Computing Security Requirements Guide に明記されている基準を満たさなければならない。また、政府の契約担当機関からの書面による承認を受けない限り、情報は米国国内で維持・管理しなければならないとされている [38]。加えて、32 C.F.R. § 2002.1 以下では、各政府機関が遵守しなければならないサイバーセキュリティ要件（情報の維持の方法やベンダーの選定に関する規定等）が規定されており [19]、各政府機関の内部において要件が設定されている [39]。各州や地方自治体（警察や消防署も含む）においても、独自のサイバーセキュリティ要件を設定しており、各管轄下において独立に施行されている [21]。また、クラウドサービスに関する政府全体のセキュリティ認証プログラムである FedRAMP が提供されている。FedRAMP では、クラウド製品・クラウドサービスのセキュリティ評価、承認、及び継続的な監視に対する標準化されたアプローチが提供されており、（ⅰ）政府機関が使用するクラウドシステムに適切なセーフガードがあることを保証すること、（ⅱ）二度手間を排除しリスクマネジメントコストを削減すること、（ⅲ）迅速で費用対効果の高い情報システム・サービスの政府調達を可能にすること、が目的とされている

[56]。各プロバイダーは企業の規模や種類（国内企業、国外企業）に依らず、定められた要件を満たさなければならない [51]。

また、米国国防情報システム局 (DISA) は国防省の内局であり軍事用の通信システムの開発を担当している。通信システムから派生してサイバーセキュリティを担っており、分析、アセスメント・調査、企業向けの情報提供、インシデント管理、ネットワーク防御、及び、セキュア設定ガイドのサービスを提供している。特に、ネットワーク機器に対するセキュリティの認定制度を運用しており、DISA が発行したセキュリティ技術実装ガイド Security Technical Implementation Guides (STIGs) にしたがって認定されたネットワーク製品で構成することで、高いレベルのセキュリティを確保できるとしている。DISA の枠組みを使いたい国防省の顧客（重要インフラや国防関連企業等）は DISA の統一機能認証局 (UCCO) が認定しているハードウェアやソフトウェアだけを購入することになる。認定する機器の種類としては、VVoIP、MCU、Firewall、IPS、LAN スイッチ、メディアゲートウェイ、アクセスコントローラー、ルータ、VPN 等、通信関連のハードウェアまたはソフトウェアが中心である。

機器の承認製品リストの認定プロセスは DISA の UCCO の責任で実施される。機器の認定は、UCCO が承認したアリゾナ州の JITC を含め米国国内の五つのテストセンターにて行われる。STIGs に準拠して構成され運用されていること確認して UC APL（統一機能承認製品リスト）への認定が行われる。UC APL 認定プロセスでは、相互運用性のテストと情報保証のテストが行われる。相互運用性のテストでは、ほかのベンダーとの相互運用できることを確認する。情報保証のテストでは、STIGs の要件を満たすことを確認する。STIGs の要件は、ユーザー特権の適切な割り当てと制限、パスワードポリシーやアカウント管理、データファイルの保護、セキュリティ監査とログ記録が含まれる。テストはおおむね 1 ヶ月から 2 ヵ月の期間で行われる。脆弱性やバックドアの検査が認定基準に入っているかは不明であるが、STIGs の評価項目を見る限り、認定テストの主目的は脆弱性の有無よりも、セキュリティの確保のために必要な機能が実装されて正しく動作しているかを確認するものと推察できる。

機器の認定においては、ガイドラインを満たしているかどうかで判断することになっており、海外生産の機器や外国メーカーを排除する規定はない。実際に内外差別的な運用をしているかは確認できない。しかし、すべての情報を国防省にさらしてテストされ、しかも、認可の有効期限が切れないように定期的に検査を受ける必要があるので、知財権を侵害している可能性が高い外国企業が、米国の国防省の内局に機器認定を申請するのは、事実上困難であると思われる。

5.2.2.1.3 今後の方向性

a. IoT セキュリティ全般

今後の IoT セキュリティに関する方向性として、2018 年 9 月、White House は、National Cyber Strategy を通じて国家のサイバーセキュリティ戦略を発表し [29]、下記の四つの柱を軸に戦略を策定した [60]。

- 国民、国土、生活様式の保護: 連邦政府のネットワーク・情報の保全、重要インフラの保全、サイバー犯罪への対処及びインシデントレポートの改善、について
- 米国繁栄の促進: デジタル経済の育成、米国の独創性の育成・保護、優秀なサイバーセキュリティ人材の育成、について
- 強靭さによる平和の保全: 国家の行動規範に基づくサイバー空間の安定性の向上及びサイバースペースにおける非容認行動の抑止、について
- 米国の影響力の拡大: オープン・相互運用可能・信頼性の高い・安全なインターネットの促進及び国際サイバー能力の構築、について

また、今後規定が見込まれているソフトロー等の強制力のない制度は見受けられていない [54]。

b. 重要インフラ

重要インフラについては、各政府機関において、特に、5G へ向けたセキュリティ対策及び中国通信機器メーカーの調達に関する規制が見込まれている。5G は、次世代の通信インフラとして期待されており、各電気通信会社は、世界において 5G をリードするために開発に注力している一方で、5G の世界におけるセキュリティの課題について懸念を示している [28]。White House は、国家のサイバーセキュリティ戦略にあたる National Cyber Strategy を発表し、サイバー空間におけるセキュリティの強化の方向性を提示している [29]。また、連邦政府は、米国の通信ネットワークに脆弱性をもたらす“バックドア”が機器に含まれていることを懸念して、中国の通信機器メーカーである Huawei の通信機器の配備または使用の禁止を検討している。2018 年初頭、White House は、米国の国内企業においても特定の中国通信機器メーカーの機器の使用を禁ずる大統領令を検討しており（上述の NDAA 2019 では、米国政府機関との取引に関する規制であることに留意）、その際は発効までは至らなかったが [30]、今後数週間以内に進展が見込まれている（2019 年 2 月 4 日時点）。発令された場合、中国を拠点とする通信機器ベンダーが自社のネットワーク機器を米国の通信キャリアへ販売することが困難になる。報道によると、大統領令は、米国の通信キャリアが米国の国家安全保障に関してリスクをもたらしうるベンダーの通信ネットワーク設備を購入することを阻止する発令を行うよう DoC に指示するものであるとされている。大統領令では、Huawei や ZTE といった具体名の記載は予期されていないものの、DoC はこれら二つのベンダーに対しても規制を適用する見込みである。これらの大統領令の発効の可能性を伝える相次ぐ報道は、オーストラリア、カナダ、ニュージーランド、及び英国等の同盟国に対して、中国の通信機器メーカーへの厳格な安全保障態勢を敷くように圧力をかける一種の政府のキャンペーンであるとの見方がなされている。大統領令の法的根拠に関しては、International Economic Powers Act で規定されており、国家の緊急事態に対応して米国の商取引を規制する権限を大統領に与える [53]。また、米国議会及び NSA (National Security Agency) も、Huawei を重大な安全保障上の脅威だとみなしており、米国での活動を抑制するための追加措置を講ずる可能性があるとしているものの、現時点では具体的な措置の検討内容は不明である [30]。

c. 政府調達

政府調達については、2019 年に FAR の改定が見込まれている [22]。これまでは、原則、各政府機関において固有の規制が設けられており、形式化されていなかった。そのため、各政府機関との契約ごとに、サイバーセキュリティに関する要件の有無を綿密に検討することが肝要であった。しかし、FAR の改定により、すべての政府機関において契約企業・案件に対するセーフガードの要件が適用される見込みであり [20]、これにより、各機関における規制が統一へ向かうと予想されている [40]。また、NDAA 2019 では、特定のメーカーを指定して調達を禁ずる規制も出てきている。2018 年に成立した同法には、特定の中国の通信機器メーカーからの調達を禁じる規制を 2 段階において適用することが記載されており、1 段階目では、2019 年 8 月以降、米国政府機関が中国通信機器メーカー5 社（Huawei、ZTE、Hytera Communications Corporation、Hangzhou Hikvision Digital Technology Company、Dahua Technology Company（及びその関連会社））の製品及び製品を使用する機器・サービスの調達を禁じ、2 段階目では、2020 年 8 月以降、上記 5 社の製品を使用する企業との契約を禁ずる規定が盛り込まれている [55]。

さらに、IoT デバイスの政府調達に関するセキュリティ要件に関して、超党派で立法化の動きもある。2017 年に Mark Warner 上院議員が Cory Gardner 上院議員とともに同案を発案したが、進展が見られていなかった。しかし、2019 年に、より大きな法律の一部の改

正として再導入される可能性があるとされている [14]。具体的には、政府が調達する IoT デバイスのベンダーに対して、パッチを適用可能な状態にする、業界の標準的なプロトコルに従う、ハードコードされたパスワードを使用しない、既知のセキュリティの脆弱性を含まないようにする等といった要件が盛り込まれる見込みである [37]。また、クラウドサービスの認証プログラムである FedRAMP にも改正の動きが見られる。2018 年 7 月、民主党の Gerry Connolly 下院議員は、FedRAMP の認定プロセスの効率化を目指し、FedRAMP Reform Act of 2018 を議会に提出した。これまで、他の政府機関により導入されたクラウドサービスが FedRAMP の認証を既に取得していても、再利用せず独自でセキュリティの評価を行い、一からシステムの認証申請を行わせる政府機関が多数あった。Connolly 議員は、これらの重複した認証申請プロセスを発生させていること等を問題とし、同法案で、FedRAMP の関連組織の役割の明確化を行う、各政府機関が FedRAMP のガイダンスに準拠するよう徹底させる責任を OMB に対して負わせる、取得した認証については FedRAMP の統括部署 PMO (Project Management Office) に報告する義務を各政府機関に対して課す等といった改正を求めている [59]。

ア) 略称名称一覧(各カテゴリのアルファベット順)

カテゴリ	略称	正式名称
制度	C.F.R.	Code of Federal Regulations
	DFARS	Defense FAR Supplement
	FAR	Federal Acquisition Regulations
	FCS	Florida Cybersecurity Standards
	FedRAMP	Federal Risk and Authorization Management Program
	FISMA	Federal Information Security Management Act
	FTC Act	Federal Trade Commission Act
	GLBA	Graham-Leach-Bliley Act
	HIPAA	Health Insurance Portability and Accountability Act
	NDAA	National Defense Authorization Act
	NSA	Network Security Agreement
	SB	Senate Bill
組織	DHS	Dept. of Homeland Security
	DoC	Dept. of Commerce
	DoD	Dept. of Defense
	DoJ	Dept. of Justice
	DoT	Dept. of Transportation
	FBI	Federal Bureau of Investigation
	FCC	Federal Communications Commission
	FRS	Federal Reserve System
	FTC	Federal Trade Commission
	GSA	General Services Administration
	HHS	Dept. of Health & Human Services
	NARA	National Archives and Records Administration
	NASA	National Aeronautics and Space Administration
	NCCIC	National Cybersecurity and Communications Integration Center
	NHTSA	National Highway Traffic Safety Administration
	NIST	National Institute of Standards and Technology
	NSA	National Security Agency
	OMB	Office of Management and Budget

カテゴリ	略称	正式名称
その他	CDI	Covered Defense Information
	CI	Classified Information
	CISO	Chief Information Security Officer
	CUI	Controlled Unclassified Information
	ISAC	Information Sharing and Analysis Center
	NPRM	Notice of Proposed Rulemaking
	PMO	Project Management Office

イ） 重要インフラの定義

米国における重要インフラは 16 分野とされており、具体的には、Chemical、Commercial Facilities、Communications、Critical Manufacturing、Dams、Defense Industrial Base、Emergency Services、Energy、Financial Services、Food and Agriculture、Government Facilities、Healthcare and Public Health、Information Technology、Nuclear Reactors, Materials, and Waste、Transportation、及び Water and Wastewater である [52]。

5.2.2.1.4 Evidence 及び原典

a. 法律事務所による回答

US

December 26, 2018

---

1 An overview of your jurisdiction's cyber security legislation and regulations, including both legally binding laws or non-binding guidance or principles, as they concern network systems for the "Internet-of-Things" and/or information and communication technology.

[Existing Legislation and Regulations]

Generally speaking, US regulations and guidance do not single out particular networks, hardware, or software for regulation. Rather, rules and regulations are largely sectoral in nature and concern themselves with data security and management. [1] While one state, California (discussed in Section 2(c) below), and possibly several more US states by the end of 2019, regulates IoT devices, the type of statutes and guidance that one sees in the 51 U.S. jurisdictions (50 states + federal government) are generally agnostic about software and hardware.

A. FEDERAL

1. The National Institute for Standards and Technology (NIST) Cybersecurity Framework v. 1.1 (April 16, 2018): Voluntary risk-based framework. When it was

released in 2014, it was designed for critical infrastructure, but was updated in April 2018 to be available to all sectors. [2]

2. **Federal Trade Commission Act § 5:** Provides for FTC enforcement of unfair or deceptive trade practices. Cybersecurity guidance has been fleshed out through enforcement actions against companies. [3] They have issued guidance (see below) for private sector cybersecurity standards.

3. **HIPAA Security Rule:** The Security Rule requires application of safeguards by Covered Entities and Business Associates. [4] The same framework applies, regardless of the size, resources or extent of data the organization has, but the entity has flexibility to implement the requirements proportionate to such considerations. The Dept. of Health and Human Services has also issued cybersecurity guidelines (see link below) that are not mandatory. [5]

4. **Graham-Leach-Bliley Act § 501:** GLBA regulates the financial sector. Section 501 imposes obligations on financial institutions to protect the security and confidentiality of their customers' non-public personal information. [6] Section 501 further requires each federal financial regulatory agency to establish security standards for the financial institutions under their jurisdiction.

5. **Interagency Security Guidelines Establishing Information Security Standards:** These regulations establish standards relating to administrative, technical and physical safeguards to ensure the security, confidentiality, integrity and proper disposal of customer information. [7] These standards include implementing a comprehensive written information security program that includes involving the board of directors, assessing risk, managing and controlling risk and overseeing provider arrangements.

6. **Federal Information Security Management Act (FISMA):** This act requires federal agencies to assume responsibility for providing information security protection commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, modification, disruption, or destruction of information. [8]

B. STATE

2. **Ohio SB220 Cybersecurity Safe Harbor:** This legislation, enacted in September 2018, provides a safe harbor for data breach notification liability if the organization "reasonably conforms" with one of the cybersecurity frameworks identified in the legislation (NIST, NIST 800-171, 800-53, and 800-53a, FedRAMP security assessment framework, etc.). [10]

[Forthcoming Legislation and Regulations and Discussions on Future Trends]

In 2017 Sen. Mark Warner introduced bi-partisan legislation with Sen. Cory Gardner proposing to impose federal government procurement security requirements for IoT devices. The legislation did not move forward. It is likely to be reintroduced in 2019 and potentially might be enacted as an amendment to a larger piece of legislation. [14] In October 2018, so this may be of interest to the client.

References:

NIST: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

FTC:https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security

HIPAA:https://www.ecfr.gov/cgi-bin/text-idx?SID=7987e9b9ca2b0d06a7efca2f0da4b249&node=pt45.1.164&rgn=div5#sp45.1.164.c

HHS Guidance: https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html

GLBA: https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf

Interagency Security Guidelines: 12 C.F.R. Part 30; 12 C.F.R. Part 208; 12 C.F.R. Part 364

FISMA: https://www.govinfo.gov/app/details/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapIII-sec3541

NYDFS: https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf

OH SB220: https://www.legislature.ohio.gov/legislation/legislation-documents?id=GA132-SB-220

FCS: https://www.flrules.org/gateway/ChapterHome.asp?Chapter=74-2

SEC: https://www.sec.gov/rules/final/2013/34-69359.pdf

MA 201 CMR 17.00: https://www.mass.gov/files/documents/2017/10/02/201cmr17.pdf

NV: https://www.leg.state.nv.us/NRS/NRS-603A.html#NRS603ASec210

NHTSA Proposed Rulemaking: https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf

2 Details of your jurisdiction's cyber security-related regulations relevant to procurement of goods in the following sectors

(a) Government (national security, defense, police, fire station, tax, academic research, etc.)

[Existing Legislation and Regulations]

The Federal government places cybersecurity requirements on companies with which it contracts in order to protect certain government data. [16] The Federal Acquisition Regulations ("FAR") are the regulations that apply to Federal procurements. FAR 52.204-21 applies to a broad range of government contracts and requires contractors' IT systems to satisfy certain safeguarding requirements. In general, these requirements

are basic and companies find them fairly easy to implement. In addition to the FAR clause, many agencies have their own cybersecurity requirements. [17] The most sophisticated and onerous of these requirements are contained in contracts with the Department of Defense. Specifically, Defense FAR Supplement (DFARS) 252.204-7012 requires contractors to maintain certain types of data (called Covered Defense Information ("CDI")) on IT systems that satisfy a detailed list of cybersecurity controls. The DFARS clause also contains specific reporting requirements in the event of a breach and requirements for external cloud service providers that host CDI. In addition, DFARS 252.239-7010 contains further requirements that apply to companies that are providing cloud computing services directly to the Government. [18]

In addition to the above, there are also cybersecurity requirements that Government agencies must follow including how they must maintain information and with which vendors they may contract to host Government data. 32 C.F.R. § 2002.1, *et seq.* [19] As discussed below, it is expected that these requirements will soon translate into a new FAR clause that will impose safeguarding requirements on contractors across all government agencies, rather than the agency-specific regime that currently exists. [20]

Importantly, the above requirements apply to unclassified information. Classified information is controlled under a separate regulatory scheme. There are also other requirements in the United States related to the safeguarding of personal identifiable information.

State and local governments (which would include police and fire rescue departments) may have their own cybersecurity requirements. These would be unique to each jurisdiction. [21]

References:

FAR 52.204-21:
https://www.acquisition.gov/sites/default/files/current/far/html/FARTOCP52.html

DFARS 252.204-7012:
https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm

DFARS 252.239-7010:
https://www.acq.osd.mil/dpap/dars/dfars/html/current/252239.htm#252.239-7010

Notice of regulatory agenda indicating that CUI FAR clause is in the rulemaking stage:
https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201810&RIN=9000-AN56

(b) Critical infrastructure (telecommunication, electricity, transport, etc.)

[Existing Legislation and Regulations]

Although the Federal government imposes cybersecurity requirements on certain types of data (like personal health information or customer proprietary network information), cybersecurity for telecommunications infrastructure is largely governed through industry best practices and public/private partnerships aimed at securing the broader communications ecosystem rather than through codified regulations. For example, telecom companies are encouraged to map their company's practices to the NIST Cyber Framework and share cyber threat information in real time through the National Cybersecurity and Communications Integration Center, but are not required to do so (although most companies do participate). [23] There are two types of cybersecurity incidents that telecom infrastructure providers must report:

Outage Reporting. When telecommunications company experiences an outage on its network of a certain number of "user minutes" or more over a specified period, they must report the outage to the FCC through the FCC's Network Outage Reporting Systems, and provide updates over subsequent days (see 47 C.F.R. Part 4). Several states also have their own outage reporting requirements.

Protection of Data. Companies are expected to take reasonable measures to protect the data on their networks and must comply with FTC consent decrees governing the sale of data to third parties. The FCC requires that security incidents involving the unauthorized disclosure of customer proprietary network data be reported through a centralized portal (see 47 C.F.R. § 64.2011). [24]

However, telecom companies that are majority-owned by a foreign entity or person will be subject to a number of additional requirements under the terms of a network security agreement (NSA) negotiated with the US government. [25] These agreements turn many of the voluntary industry best practices described above into requirements that can be audited against (*e.g.*, company would be required to develop a cyber incident response plan that would have to be approved by the US Government and track the NIST framework). [26] NSAs can impose much more rigorous cybersecurity requirements on a foreign-owned entity than what is required of domestically-owned competitors (*e.g.*, US government may get to block the foreign-owned company from engaging with a certain equipment vendor or service provider, but domestic company would not be blocked from same action). [27]

[Forthcoming Legislation and Regulations and Discussions on Future Trends]

The security of US telecommunications networks is front of mind for many government agencies. Some recent trends:

Race to 5G. Telecom companies are engaged in a global race to be the first to successfully deploy 5G, the next generation of communications. This next generation is expected to usher in lightning-fast speeds and near-constant connectivity to support functions like the Internet of Things and connected cars. However, telecommunications companies and the US government alike are concerned about the cybersecurity challenges that will be presented by a 5G world. [28] As such, effective cybersecurity practices will be even more critical to a company's success. The White House issued a high-level document earlier this year on its cybersecurity strategy. [29]

Suspicion of Chinese Providers. In recent months, the Federal government has been very focused on preventing the deployment or use of telecom equipment from Huawei, a Chinese telecom equipment manufacturer, over fears that the equipment contains a "back door" that facilitates surveillance and presents vulnerabilities to US telecom networks. Earlier in 2018, the White House considered an Executive Order that would have expanded the Executive Branch's authority to block even domestic companies from using equipment from certain manufacturers (*i.e.*, Huawei and ZTE), but it was never issued. Congress and the national security agencies continue to see Huawei as a significant security threat and may take further steps to curtail its activity in the United States, but it is unclear what further steps are being contemplated at this time. [30]

References:

Review of recent cyber legislation across the US: http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx

National Cybersecurity and Communications Integration Center: https://www.us-cert.gov/about-us

NIST Cyber Framework: https://www.nist.gov/cyberframework

FCC CSRIC Best Practices: https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data

FCC NORS Reporting: https://www.fcc.gov/network-outage-reporting-system-nors

FCC CPNI breach reporting portal: https://www.cpnireporting.gov/cpni/content/disclaimer.seam

Proposed EO on telecom manufacturers: https://www.washingtonpost.com/world/national-security/trump-eyes-executive-order-expanding-power-to-block-deals-between-us-foreign-telecom-firms/2018/06/29/f6d26a0a-7af3-11e8-aeee-4d04c8ac6158_story.html

Trump White House Cyber Strategy: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

(c) Equipment or services for consumers

[Existing Legislation and Regulations]

In September of 2018, this law does not regulate purchasers or retailers, it is likely to improve security in the supply chain.

References:

https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

b. 法律事務所を通じた Q&A

1. 1. An overview of your jurisdiction's cyber security legislation and regulations, including both legally binding laws or non-binding guidance or principles, as they concern network systems for the "Internet-of-Things" and/or information and communication technology.における[Existing Legislation and Regulations]以下について
   I. FEDERAL の六つの規制は、例示的な記載という理解でよいか（他にも同様な規制が存在するが、文量を鑑みて、代表的なものを選定したという理解でよいか）
   - ✓ Ans : The laws and guidance listed in A under Section 1 are illustrative; additional federal agencies have issued guidance that could have an effect on IoT. [34]

   II. Federal と State における規制の内容について、矛盾はないという理解で良いか
   - ✓ Ans: Correct, but it is not that simple. In the privacy/cyber space, some state laws mirror the federal law (e.g., laws pertaining to unfair and deceptive trade practices – similar to Title V of the FTC Act); some laws are more restrictive (but do not conflict with) than federal law; and, in other circumstances, the federal law has not spoken on the issue. [36] In some contexts, e.g., data breach (which is beyond the scope of this topic), the state laws do conflict with one another, thus requiring a careful review on a state-by-state basis.

2. In 2017 Sen. Mark Warner introduced bi-partisan legislation with Sen. Cory Gardner proposing to impose federal government procurement security requirements for IoT devices. The legislation did not move forward. It is likely to be reintroduced in 2019 and potentially might be enacted as an amendment to a larger piece of legislation.の下線部について、具体的にどのような要件なのか
   - ✓ Ans: The bill would have required vendors of IoT devices purchased by the federal government to ensure their devices are patchable, rely on industry standard protocols, do not use hard-coded passwords, and do not contain any known security vulnerabilities. [37]

- Direct the Office of Management and Budget (OMB) to develop alternative network-level security requirements for devices with limited data processing and software functionality.
- Direct the Department of Homeland Security's National Protection and Programs Directorate to issue guidelines regarding cybersecurity coordinated vulnerability disclosure policies to be required by contractors providing connected devices to the U.S. Government.
- Exempt cybersecurity researchers engaging in good-faith research from liability under the Computer Fraud and Abuse Act and the Digital Millennium Copyright Act when in engaged in research pursuant to adopted coordinated vulnerability disclosure guidelines.
- Require each executive agency to inventory all Internet-connected devices in use by the agency.

3. In addition, DFARS 252.239-7010 contains further requirements that apply to companies that are providing cloud computing services directly to the Government. の下線部について、具体的にどのような要件なのか？
   - ✓ Ans: DFARS 252.239-7010 requires contractors that are using cloud services when providing IT services directly to the Government to use a cloud that meets certain security level requirements which are set forth in the Cloud Computing Security Requirements Guide. Importantly, the clause also states that the information must be mainained within the United States, unless the contractor received written approval from the Government's Contracting Officer to use a different location. [38] The clause also contains limits regarding the use of information and reporting requirements in the event of a cyber breach that impacts (or potentially impacts) the government's information.
4. In addition to the above, there are also cybersecurity requirements that Government agencies must follow including how they must maintain information and with which vendors they may contract to host Government data. 32 C.F.R. § 2002.1, et seq. の下線部について、具体的にどのように情報を維持すべきとされているのか
   - ✓ Ans: Government agencies have internal requirements that include how such information must be marked and stored. They may also only use cloud service providers that have been approved by the Government as satisfying onerous security controls. [39]
5. As discussed below, it is expected that these requirements will soon translate into a new FAR clause that will impose safeguarding requirements on contractors across all government agencies, rather than the agency-specific regime that currently exists.の下線部について、具体的にどの機関を指すのか？
   - ✓ Ans: The Department of Defense has the most sophisticated requirements regarding cybersecurity issues. It is not feasible to list all of the other agencies that have cybersecurity requirements. In general, the requirements have not been formalized in regulation, and are included as contract-specific requirements. In other instances, the requirements vary even within the

agency. Further, we anticipate that the upcoming FAR clause (as discussed in the response and below) will unify the requirements of the different agencies so that in the future, there will not be many different requirements. [40]

6. The Federal government is expected to release a new FAR clause in 2019 that contains safeguarding requirements for contractors that receive, collect, develop, transmit, or otherwise store certain information (defined as Controlled Unclassified Information ("CUI"). CUI is has significant overlap with CDI, which is currently controlled under the Department of Defense's DFARS clauses.の下線部について、

7. Although the Federal government imposes cybersecurity requirements on certain types of data (like personal health information or customer proprietary network information), cybersecurity for telecommunications infrastructure is largely governed through industry best practices and public/private partnerships aimed at securing the broader communications ecosystem rather than through codified regulations.
の下線部について、

I. industry best practices における、"industry"の定義は何か
- ✓ Ans: As used here, "industry" refers to telecommunications providers.
- ✓ Examples of telecom industry best practices include:
  - Setting up firewalls in appropriate spots throughout a network;
  - Having an alarm system in place for facilities that house Domestic Communications Infrastructure; and
  - Requiring users to use strong passwords and change their passwords every 90 days.

(1) Each of the above practices is aimed at eliminating or minimizing cyber vulnerabilities or mitigating the impact of a cyber incident. [44]

II. "public/private partnerships aimed at securing the broader communications ecosystem"とは具体的に何を指すのか
- ✓ Ans: The most prominent Public-Private Partnership is the Communications Information Sharing and Analysis Center (ISAC). It serves as a central hub for private entities to share cyber threat intelligence with the US Government in real time.
- ✓ In doing so, the private sector "partners" with the public sector to ensure that all entities can prevent, detect, respond to, mitigate, and recover from cyber incidents in a timely fashion. [45]

8. NSAs can impose much more rigorous cybersecurity requirements on a foreign-owned entity than what is required of domestically-owned competitors (e.g., US government may get to block the foreign-owned company from engaging with a certain equipment vendor or service provider, but domestic company would not be blocked from same action).の下線部について、

I. “foreign-owned entity”及び“domestically-owned competitors”の定義は何か（二つの境界線はどこか）（例: 外国資本比率 X%以上が“foreign-owned entity”で、X%未満は“domestically-owned”等）

- ✓ Ans: <u>These terms are not specifically defined and should instead be considered relative to the regulations surrounding the Council for Foreign Investment in the United States (CFIUS)</u>.
- ✓ CFIUS is permitted to review “any merger, acquisition, or takeover ... by or with any foreign person which could result in foreign control of any person engaged in interstate commerce in the United States,” with the intent of evaluating whether and to what extent such transactions could impact US national security.
- ✓ “Control” is defined in the CFIUS regs as the “power, direct or indirect, whether or not exercised, through the ownership of a majority or a dominant minority of the total outstanding voting interest in an entity, board representation, proxy voting, a special share, contractual arrangements, formal or informal arrangements to act in concert, or other means, to determine, direct, or decide important matters affecting an entity; in particular, but without limitation, to determine, direct, take, reach, or cause decisions regarding the [matters listed in § 800.204(a)], or any other similarly important matters affecting an entity.” See 31 U.S.C. § 800.204(a).
- ✓ There is no bright line test for when a transaction warrants CFIUS review, but generally speaking, where a foreign person or entity seeks to acquire a non-passive investment of more than 10 percent in a U.S. company – i.e., upon closing, the foreign person or entity would theoretically hold enough voting interest to be able to direct or influence the actions of the company or its board – filing for CFIUS review is recommended.
- ✓ <u>So, as used here, a “foreign-owned” entity would have at least one foreign investor holding a 10 percent or more non-passive interest in the US company. A “domestically-owned” entity would not have any foreign investors.</u> [46]

II. NSA の例（e.g.以下の文）は、実際の事例という理解でよいか？

- ✓ Ans: <u>This is based on an actual case. Without disclosing confidential details, there is precedent in which the US Government required a telecom provider to “rip and replace” from its network all equipment from a certain vendor. In contrast, a domestically-owned competitor used this vendor widely throughout its network for years and has never been required to remove it.</u> [47]

9. Most recent State cybersecurity regulations have focused on the cybersecurity of state agencies, or provide an individual cause of action where personal data is improperly disclosed. However, <u>states have been increasingly focused on election security and preventing unauthorized remote access to telecom networks.</u> For example, California recently adopted a bill that requires connected device manufacturers to install mechanisms on the connected device aimed at preventing unauthorized use or remote access.

   の下線部について、

   As it is early in the year, it is difficult to predict with certainty which additional states also may propose legislation.

10. FedRAMP の認証を取得する難易度は、企業の規模や種類（米国資本企業 or 外国資本企業）に依存しないという理解で良いか

- ✓ Ans: <u>Not necessarily, rather it is whether the entity can meet the controls. The certification is available if the cloud provider is going to hold government data.</u>

[51] In addition to the link above, the following link contains additional information about various components of the program: https://www.fedramp.gov/about/

11. 米国における“Critical Infrastructure”の定義は何か？
    - ✓ Ans: “Critical Infrastructure” is composed of the physical and cyber assets, systems, and networks that are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Put simply, “Critical Infrastructure” provides essential services that underpin American society (e.g., sewer systems; communications networks; power grids; military bases; etc.)
    - ✓ Presidential Policy Directive 21 (PPD-21) identifies the following 16 industry sectors as having Critical Infrastructure:
        1. Chemical
        2. Commercial Facilities
        3. Communications
        4. Critical Manufacturing
        5. Dams
        6. Defense Industrial Base
        7. Emergency Services
        8. Energy
        9. Financial Services
        10. Food and Agriculture
        11. Government Facilities
        12. Healthcare and Public Health
        13. Information Technology
        14. Nuclear Reactors, Materials, and Waste
        15. Transportation
        16. Water and Wastewater
    - ✓ References:
    - ✓ Dept. of Homeland Security, Infrastructure Security Overview: https://www.dhs.gov/cisa/overview
    - ✓ Presidential Policy Directive 21 (PPD-21) - Critical Infrastructure Security and Resilience: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [52]
12. 政府調達または通信インフラ・重要インフラの調達において、違反として摘発された事例や排除された事例はないか？
    - ✓ Ans:Huawei Indictment: In January 2019, the U.S. Department of Justice unsealed a 13-count indictment against Huawei. The indictment charges Huawei and certain Huawei subsidiaries with bank fraud, money laundering, obstruction of justice and violations of U.S. sanctions against Iran, among other things. The indictment specifically alleges that Huawei engaged in a scheme to deceive numerous financial institutions and the U.S. government regarding Huawei’s business activities in Iran by falsely stating that Huawei was not affiliated with an Iranian company, Skycom, which actually was Huawei’s

Iranian affiliate. (U.S. laws generally prohibit banks from processing transactions related to Iran through the United States.) It is too early to determine how the Huawei case ultimately will be resolved, especially since it has become part of the broader trade dispute between China and the United States and involves the jurisdiction of multiple U.S. government agencies. However, the indictment confirms that the U.S. government is willing to use all available measures to restrict the ability of Huawei and other Chinese entities it deems a threat to U.S. national security to sell their products to U.S. carriers.

- ✓ Pending Executive Order on Supply Chain: The Trump Administration is expected to release an Executive Order in the coming weeks that would make it more difficult for Chinese-based telecommunications vendors to sell their network equipment to U.S. carriers. Based on reports, the Executive Order would direct the U.S. Commerce Department to issue an order that would block U.S. carriers from buying telecommunications network equipment from vendors that pose U.S. national security risks. While the Executive Order will not specifically name Huawei or ZTE, the Commerce Department likely would interpret it to apply to those two vendors. The legal basis for the Executive Order purportedly will be the International Economic Powers Act, which is a U.S. law that provides the president with the authority to regulate U.S. commerce in response to a national emergency. The potential release of the Executive Order follows the U.S. government's campaign to pressure allies like Australia, Canada, New Zealand, and the United Kingdom to also adopt a stricter security posture towards Chinese telecom manufacturers. [53] U.S. government agencies and contractors are already barred from buying products from Huawei and ZTE under a recently enacted law.
- ✓ References:
- ✓ The above has been widely reported in the media and is pulled from a variety of publicly available sources.

13. 今後、サイバーセキュリティに関して策定が予定されている Soft law（強制力のないもの）及び連邦政府や各州における推進部門や体制等はないか？
    - ✓ Ans: Many U.S. agencies, including, the Securities and Exchange Commission and the Internal Revenue Service, among others, have issued non-binding guidance on various privacy/cyber related topics. Unless the guidance issues as a result of a public forum or other situation in which the agency has sought comment, we cannot predict which agency will issue guidance and in what form. [54]

c. 法律事務所による回答以外の情報ソース

- NDAA 2019 [55]
  - ✓ https://www.congress.gov/bill/115th-congress/house-bill/5515/text
- FedRAMP [56]
  - ✓ https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf
- 一般社団法人　重要生活機器連携セキュリティ協議会編　(2018 年)　「企業リスクを避ける　押さえておくべき IoT セキュリティ～脅威・規制・技術を読み解く！～」P.40-P.42　株式会社インプレス [57]
- 一般社団法人　重要生活機器連携セキュリティ協議会編　(2018 年)　「企業リスクを避ける　押さえておくべき IoT セキュリティ～脅威・規制・技術を読み解く！～」P.89-P.90　株式会社インプレス [58]
- JETRO/IPA NewYork 2018 年 8 月“米国行政における電子化（デジタルガバメント）

及びクラウド活用の現状 [59]
https://www.ipa.go.jp/files/000068889.pdf
- Text - H.R.6550 - 115th Congress (2017-2018): FedRAMP Authorization Act Congress.gov | Library of Congress [59]
https://www.congress.gov/bill/115th-congress/house-bill/6550/text
- Connolly Introduces FedRAMP Reform Act of 2018 | U.S. House of Representatives
https://connolly.house.gov/news/documentsingle.aspx?DocumentID=1441 [59]
- President Trump Unveils America's First Cybersecurity Strategy in 15 Years | The White House [60]
https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/

5.2.2.2 オーストラリア

5.2.2.2.1 国としての全体的な状況(まとめ)

オーストラリアの政策動向の概要を表 5-6 に示す。

表 5-6　オーストラリアの政策動向（まとめ）

	項目	概要
現状	全体傾向	サイバーセキュリティの脅威となるバグやウイルスを含む可能性のあるハードウェアやソフトウェアを除外する特別な法律はないが、現行法規制の下、政府機関と民間企業の両方に対して、潜在的なサイバーセキュリティの脅威を軽減するフレームワークが提供されている。法律・制度の面では、基本的な個人情報保護やデータ侵害・セキュリティ侵害の通知義務、特定商品・サービスの輸出制限等が規定されている
	重要インフラの法制度	1997 年に法改正により、スパイ、サボタージュ、外国からのオーストラリアの通信ネットワークと設備への干渉について、国家安全保障上のリスクを適切に管理する枠組みが作られ、これに基づき 2018 年 9 月よりキャリアは新たな法的義務を負うとともに、政府には情報収集権限、国家安全保障上のリスクから保護するための指示権が付与された。
	政府調達	政府調達では、システム・ネットワーク構築での調達等において、Evaluated Products List (EPL) という政府による審査済みの製品リストからの選択を義務付けたほか、PSPF (Protective Security Policy Framework) により、セキュリティ脅威軽減のために必要なセキュリティを準備することが指導されている。また、国家安全保障上の懸念に基づき、Huawei 及び ZTE に対し、5G 展開に関連しネットワーク技術を提供する契約への入札が禁止された。
	認証/認定制度	EPL には、政府機関で使用するために ASD (Australian Signals Directorate) によって評価された ICT 製品のリストが記載されており、ISO 15408 が認証されている。
	体制	重要インフラセンター (Critical Infrastructure Centre) にあるテレコミュニケーションセクターセキュリティ (TSS) が、通信事業者のセキュリティに取り組んでいる
今後	全体的な傾向	現時点では、政府調達や重要インフラに関する特に目立った制度制定の動きは見られないが、国家安全保障上の懸念に基づく法律の枠組みの構築が行われる可能性がある。
	重要インフラの法制度	通信領域において、Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 法案（暗号化されたデータへのアクセスを法執行機関に提供するためのもの）が 2018 年に可決されたが、立法が過剰な権限をえる可能性があるとして、修正法案提出等の可能性あり。
	政府調達	現行目立った制度制定の動きはないが、国家安全保障上の懸念に基づく法的枠組み構築の可能性あり。

オーストラリアには、サイバーセキュリティの脅威となるバグやウイルスを含む可能性のあるハードウェアやソフトウェアを除外する特別な法律はないが、現行の法規制の下で

は、政府機関と民間企業の両方に対して、潜在的なサイバーセキュリティの脅威を軽減するフレームワークが提供されている。法律・制度の面では、基本的な個人情報保護として、Privacy Act (Privacy Act 1988 (Cth)) や Spam Act 2003 (Cth) が規定されている。また、データ侵害・セキュリティ侵害の通知義務として、NDB scheme (Notifiable Data Breaches scheme)、ASX listing rules が規定され、特定商品・サービスの輸出制限として、Customs Act (Customs Act 1901 (Cth)) や Customs (Prohibited Exports) Regulations 1958 が規定されている。

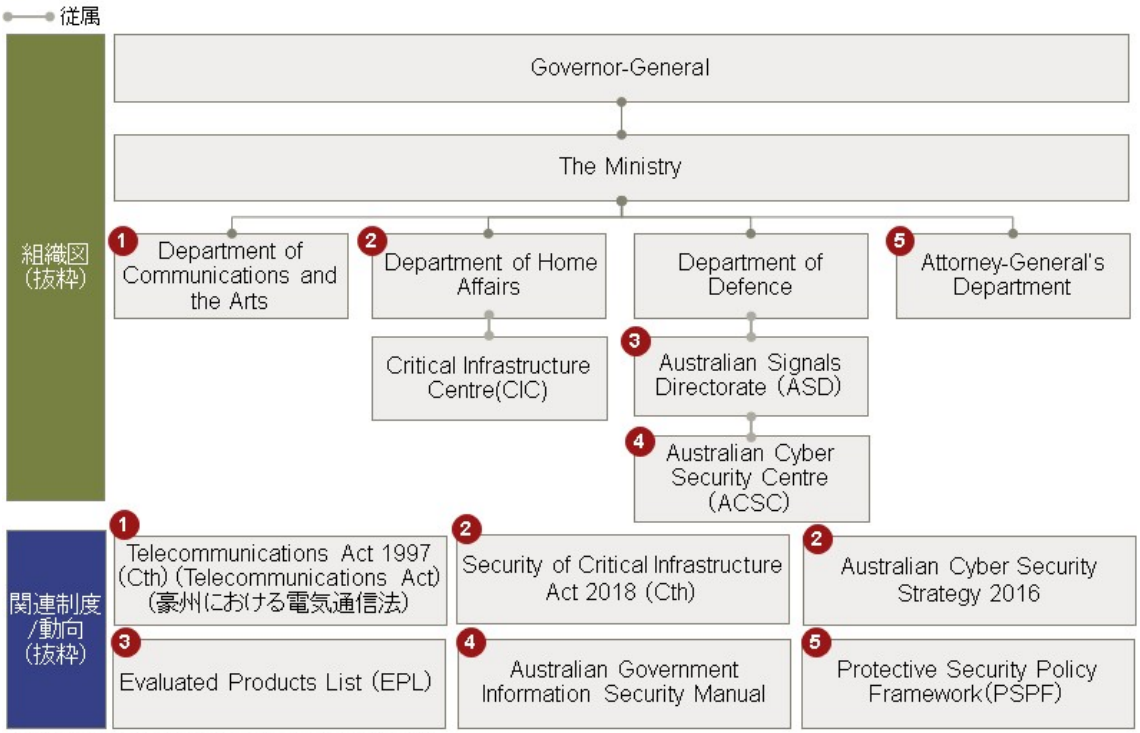
重要インフラについては、政府による情報取得や指導の権利が規定されている Security of Critical Infrastructure Act 2018 (Cth) の他、通信領域においては設備設置や機器輸入、データ保持に関して規定されている Telecommunications Act (Telecommunications Act 1997 (Cth)) や TIA Act (Telecommunications (Interception and Access) Act 1979 (Cth)) がある。

政府調達については、ベンダーは一般的に、契約上定められた規制や政策に従うことになっており、ICT 関連の契約の多くも、契約している政府のレベル（連邦、州、準州）や政府機関によって異なる政策に従うことをベンダーに求めている。また法律・制度以外の部分では、政府機関・民間企業それぞれに対して、サイバーセキュリティ対応やリスク管理に関するガイダンス・フレームワーク（Strategies to Mitigate Cyber Security Incidents、Australian Government Information Security Manual 等）が提供されている。他にも、政府の指針を示すプログラム (Australian Cyber Security Strategy 2016) の発表や、国民からのサイバー犯罪報告を受け付ける窓口 ACORN (Australian Cybercrime Online Reporting Network) の設置等がなされている。特に政府調達では、システム・ネットワーク構築での調達等において、EPL (Evaluated Products List) という政府機関 ASD（オーストラリア通信電子局: Australian Signals Directorate）による審査済みの製品リストからの選択が義務付けられている他、セキュリティ脅威軽減のために必要なセキュリティを準備することが指導されている。

今後に向けて法律・制度の面では、金融機関やその関係者に対して、情報セキュリティポリシーやインシデント管理メカニズム、セキュリティケイパビリティ維持の義務が導入予定となっている (Prudential Standard CPS 234 Information Security (Standard))。重要インフラでは特に通信領域において、重大犯罪の捜査を目的に、政府機関が通信事業者に対して技術支援やその能力の構築を要求できるとする法案が可決されている (Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth))。政府調達においては、国家安全保障上の懸念に基づき、Huawei 及び ZTE に対して、5G 展開に関連してネットワーク技術を提供する契約への入札が禁止されている。特に政府調達の分野では Defence SIGINT (signals intelligence) や Cyber Command といった新たなサイバーユニットが設立されている。SIGINT では通信傍受による諜報活動の妨害、Cyber Command では軍でのサイバー部隊成長に向けた組織構築を行う。CIC（オーストラリア政府の重要インフラセンター: Critical Infrastructure Centre）にある TSS (Telecommunications Sector Security) が、通信事業者のセキュリティに取り組んでいる。1997 年に法改正があり、スパイ、サボタージュ、外国からのオーストラリアの通信ネットワークと設備への干渉についての、国家安全保障上のリスクをより適切に管理する枠組みが作られた。2018 年 9 月からキャリアは新たな法的義務を負うことになり、適切な監督と管理を維持するセキュリティ義務、セキュリティ計画の変更の通知義務を負い、政府は政府に対する情報を収集する権限、国家安全保障上のリスクから保護するための指示権が付与された。サイバーセキュリティのコントロールに関しては、法律や政令、ライセンス許可条件等で細かく規制しているのではなく、通信事業者の実装の自由度は確保されているように思われる。その代わり、政府が通信事業者のセキュリティを把握して、場合によっては、国家安全保障上の理由で指令を出せることが注目するべき点である。この法律によって、政府の判断で国家安全保障上のリスクがあると認定した場合には、特定の国の企業の製品を、有形無形の政治的圧力ではなく、法律の枠組みで合法的に排除することが可能である。

図 5-3 は、オーストラリアにおける政府関連組織と関連法制度をまとめたものである。

番号により、組織と法制度の関連性を表現している（組織の概要は表 5-7 を、法制度の概要は表 5-8 を参照）。Department of Communications and the Arts（通信芸術省）は、通信、放送分野の政策立案のほか、ブロードバンドの普及や地上デジタル放送への移行等、情報通信の普及・振興に関する施策を実施する。2015 年 9 月にターンブル前通信相が首相に就任した際に、芸術分野を所掌事項に含めて、通信省から改称した。オーストラリアにおける電気通信法である、Telecommunications Act を定めている。Department of Home Affairs（内務省）は、連邦警察、航空・海運の安全確保、治安維持、危機管理、多文化問題・移住、税関、国境警備等を所管する新しい省庁として 2017 年 12 月に発足した。サイバー・セキュリティ・ポリシーの策定や重要インフラの保護を行っている。内務省は、Security of Critical Infrastructure Act 2018 (Cth) と Australian Cyber Security Strategy 2016 を定めている。CIC は、内務省配下にあり、オーストラリアの重要インフラへのリスクを識別し、管理するために政府のすべてのレベルを横断し、オーナーとオペレーターと活動している。Department of Defense（防衛省）は、オーストラリアとその国益を防衛する。ASD は、外国の諜報、軍事行動へのサポート、サイバー戦争、及び情報セキュリティに責任がある。ASD はオーストラリアの情報機関の一部であり UKUSA 協定（Five Eyes）中の ASD の役割は、南東アジアで信号情報 SIGINT を監視することである。ASD は、EPL を定めている。ACSC（オーストラリアサイバーセキュリティセンター: Australian Cyber Security Centre）はサイバーセキュリティに関して、政府や省庁間の調整を行う。サイバー脅威を分析・調査・報告し、サイバー犯罪、サイバーテロ、及びサイバー戦争のインシデントに対応する。ACSC は、Australian Government Information Security Manual を定めている。Attorney-General's Department（司法省）は、国の法枠組み、司法枠組みを維持・改善し、国家セキュリティと危機管理を強化するための各種プログラムや政策を実施する。Attorney-General's Department は、PSPF (Protective Security Policy Framework) を定めている。



各関連制度/動向と関連する省官庁の番号と対応
出所(Parliament of Australia, Australian Government "Government departments and agencies", Australian Government "Federal Register of Legislation"および各種資料より抜粋)

図 5-3　オーストラリアの政府関連組織と関連法制度

表 5-7　オーストラリアにおける政府関連組織

Department of Communications and the Arts	通信芸術省。 通信、放送分野の政策立案のほか、ブロードバンドの普及や地上デジタル放送への移行等、情報通信の普及・振興に関する施策を実施。2015 年 9 月にターンブル前通信相が首相に就任した際に、芸術分野を所掌事項に含めて、通信省から改称。
Department of Home Affairs	内務省。 連邦警察、航空・海運の安全確保、治安維持、危機管理、多文化問題・移住、税関、国境警備等を所管する新しい省庁として 2017 年 12 月に発足。 サイバー・セキュリティ・ポリシーの策定や重要インフラの保護を実施行っている。
CIC	重要インフラセンター。 内務省配下にあり、オーストラリアの重要インフラへのリスクを識別し、管理するために政府のすべてのレベルを横断し、オーナーやオペレーターと活動。
Department of Defense	防衛省。 オーストラリアとその国益を防衛。
ASD	オーストラリア通信電子局。 外国の諜報、軍事行動へのサポート、サイバー戦争、及び情報セキュリティに責任がある。ASD はオーストラリアの情報機関の一部であり UKUSA 協定（Five Eyes）中の ASD の役割は、南東アジアで信号情報 SIGINT (signals intelligence) を監視することである。
ACSC	オーストラリアサイバーセキュリティセンター。 サイバーセキュリティに関して、政府や省庁間の調整を行う。サイバー脅威を分析・調査・報告し、サイバー犯罪、サイバーテロ、及びサイバー戦争のインシデントに対応する。
Attorney-General's Department	司法省。 国の法枠組み、司法枠組みを維持・改善し、国家セキュリティと危機管理を強化するための各種プログラムや政策を実施。

表 5-8　オーストラリアにおける関連法制度

Telecommunications Act 1997	オーストラリアにおける電気通信法。
Security of Critical Infrastructure Act 2018（Cth）	重要インフラのセキュリティリスク管理について規定。 内務省長官（Secretary）が重要インフラ所有者から詳細な情報を入手できるとしているほか、国家安全保障上のリスク軽減を目的として、重要インフラ所有者・運営者に対する指導権を内務大臣（Minister）に与えている。
Australian Cyber Security Strategy 2016	オンラインにおける自国の利益推進・保護を目的とした政府のプログラム。
EPL	政府機関で使用するために ASD によって評価された ICT 製品のリスト。 ISO 15408 が認証されており、政府機関に対して、セキュ

	リティ脅威を軽減するために必要なセキュリティの準備、及び EPL 記載製品の使用が指導されている。
Australian Government Information Security Manual	サイバーセキュリティリスク管理のフレームワークを形成する際の参考となるガイダンス・基準を規定。
PSPF	セキュリティ脅威を軽減するために必要なセキュリティの準備、及び EPL 記載製品の使用を規定。

5.2.2.2.2 対応状況

a. IoT セキュリティ全般

オーストラリアには、サイバーセキュリティの脅威となるバグやウイルスを含む可能性のあるハードウェアやソフトウェアを除外する特別な法律はないが、現行の法規制の下では、政府機関と民間企業の両方に対して、潜在的なサイバーセキュリティの脅威を軽減するフレームワークが提供されている[1]。

法律・制度の面では、基本的な個人情報保護について規定したものとして、Privacy Act や Spam Act 2003 (Cth) があり、また EU におけるデータ保護規則である GDPR (General Data Protection Regulation) も一定の条件下で適用されうる。Privacy Act ではすべての政府機関、もしくは年間売上高 300 万オーストラリアドル以上の民間企業に対し、個人情報の保護に関する考え方が組織内に浸透するよう、デザインアプローチに基づいた個人情報保護の考え方の導入を求めている[10]。またデータ侵害やセキュリティ侵害が発生した際の通知義務について、NDB scheme や ASX listing rules で規定されている。NDB scheme は Privacy Act に基づき 2018 年 2 月に導入された制度で、データ漏洩の通知義務について規定している。データ漏洩が発生した、もしくは発生が疑われる組織は、OAIC、被害を受けた個人、場合によってはメディアに対し通知する義務がある[12]。

法律・制度以外の取り組みとして、政府機関・民間企業を対象に、ACSC、Attorney-General's Department、ASIC、APRA、ASD 等様々な機関からサイバーセキュリティへの対応やリスク管理に関するガイダンス・フレームワーク等が数多く提供されている。ACSC からはサイバーセキュリティ及びサイバーインシデントの傾向と展望に関する年次レポートが発行されている他[2]、Strategies to Mitigate Cyber Security Incidents が発表され、システムへの不正侵入を防ぐ方法が紹介されている[3]。また ISM ではサイバーセキュリティリスク管理のフレームワークを形成する際の参考となるガイダンス・基準を定めている[8]。Attorney-General's Department からはガバナンス・セキュリティ分野における政府機関の政策実行を支援する Protective Security Policy Framework (PSPF) が示され、ICT システムに適切なセキュリティが適用されていることを認証するシステムや、サイバー空間における脅威からの保護や堅牢な ICT システムに関するガイダンスが提供されている[9]。ASIC からは Report 429 (Cyber resilience: Health check) が発表され、企業のサイバー攻撃に対する準備や対応に関するベストプラクティスが示されている。また、サイバー攻撃からの復旧プロセス確立に関するガイダンスも提供されている[17]。APRA からもサイバーセキュリティリスク管理に関する実践ガイドが提供され、法的強制力はないもののベストプラクティスとみなすことができる[20]。ASD からは政府や国防軍に対し、サイバー犯罪を軽減し、サイバーセキュリティリスクを管理するための戦略が提供されている[6]。

b. 重要インフラ

重要インフラについては、関連する法律としては Security of Critical Infrastructure Act 2018 (Cth) があり、また特に通信領域においては Telecommunications Act、TIA Act や Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth) がある。Security of Critical Infrastructure Act 2018 (Cth) では重要インフラのセキュリティリスク管理について規定されており、内務省長官 (Secretary) が重要インフラ所有者から詳細な情報を入手できるとしている他、国家安全保障上のリスク軽減を目的として、重要インフラ所有者・運営者に対する指導権を内務大臣 (Minister) に与えている[33]。特に通信領域においては Telecommunications Act に基づき、通信設備の設置が特定種類（低影響設備）に限定されている他、通信機器に関して特定機器のみがオーストラリアでの使用目的の輸入を許可されている[34]。特定機器の選定基準としては、「電話、ファックス等の通信機器は Regulatory Compliance Mark (RCM) や C-Tick、A-Tick 等のオーストラリア規格を遵守したもののみネットワークに接続可能」や「コードレス通信システムはオーストラリアで使えない周波数を使用するため使用不可」等がある[47]。TIA Act では、ASIO (Australian Security Intelligence Organisation) 及び特定の法執行機関が、通信事業者・搬送サービスプロバイダーによる通信データを開示する権限をもつ[14]。Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth) では、特にサービスプロバイダーに対し、通信サービスを介した通信に関する特定の情報を収集し、2 年間安全に保持することを要求する Data Retention Scheme を定めている（保持対象は通信自体ではなく、「メタデータ」）[15]。

c. 政府調達

政府調達については、ベンダーは一般的に、契約上定められた規制や政策に従うことになっている。ICT 関連の契約の多くも、契約している政府のレベル（連邦、州、準州）や政府機関によって異なる政策に従うことをベンダーに求めている。例として、Department of Finance 独自のサイバーセキュリティに関する条項や、南オーストラリア政府がもつ、ICT 調達における政策・基準を示すセキュリティリスク管理に関するガイドライン等がある[25]。また、上述した ISM 及び PSPF が関連している。ISM では、政府のシステム・ネットワークで使用する製品の調達等の同マニュアルに記載の目的においては、EPL からの選択を義務付けている[46]。EPL には、政府機関で使用するために ASD によって評価された ICT 製品のリストが登録されており、登録された製品には国際規格である ISO 15408 が認証されている[29]。認証は Australasian Information Security Evaluation Program (AISEP) に基づいて行われ、AISEP は ASD 内の Australasian Certification Authority によって監督されている。現在 EPL に登録されている製品のカテゴリは 12 あり、“Access Control Devices and Systems”、“Data Protection”、“Host Security Module Products”、“ICs, Smart Cards and Smart Card related Devices and Systems”、“Miscellaneous Products”、“Mobile Products”、“Network and Network Related Devices and Systems”、“Operating System Products”、“Other Devices and Systems”、“PC Security Products”、“Peripheral Switch”、“PKI Products” がこれにあたる。また評価済みの登録製品数は 69 点で、そのうち 45 点を Network and Network Related Devices and Systems が占める（2019 年 2 月 25 日時点）[32][51]。PSPF では政府機関に対して、セキュリティ脅威を軽減するために必要なセキュリティの準備、及び EPL 記載製品の使用が指導されている[30]。

5.2.2.2.3 今後の方向性

a. IoT セキュリティ全般

オーストラリアにおける IoT ネットワークの今後の動きとして、Standard や Consumer Data Right がある。Standard は APRA が 2019 年 7 月から導入予定の基準で、APRA の監督対象企業に対し、情報セキュリティポリシーやインシデント管理メカニズム維持の義務を課す。対象企業は自社の情報資産に対する脅威の規模に見合う情報セキュリティポリシー、堅牢なインシデント管理メカニズムやセキュリティケイパビリティを維持する義務を負う。また企業は自社の情報セキュリティや情報資産に関与する可能性のある第三者についても、Standard に基づく義務を遵守させることが求められる[19]。Consumer Data Right は 2019 年に導入が予定されている、消費者が自身の消費者データにアクセスし、ポータビリティを持たせることができる権利である。この権利の導入にあたっては、データ転送に関するコンプライアンスや技術要件を保証するためのデータ規則や、消費者にデータアクセスを許可した際に発生しうるサイバーセキュリティ関連のリスク管理についてのガイダンス等が提供される可能性がある[24]。

b. 重要インフラ

重要インフラでは特に通信領域において、Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)という改正法案が 2018 年に可決されている。この中で様々な政府機関は通信事業者に対して、技術支援や、技術支援能力の構築を要求できるとされている[21][23]。法案は表向きには重大犯罪捜査を目的として、暗号化されたデータへのアクセスを法執行機関に提供するためのものとなっているが、立法が過剰な権限をえる可能性をはらんでおり、立法がオーストラリアのセキュリティ・暗号化ソリューションに大きな影響を与える可能性があるとして、国内外のテクノロジー企業から批判を受けている。また、この法案は多くの分野において曖昧であり、野党は議会での法案通過と引き換えに、後に大幅な修正を加えた案を提出するとしている[22]。

c. 政府調達

政府調達は政府が特に懸念する領域であり、2018 年 8 月に政府は、国家安全保障上の懸念に基づき、Huawei 及び ZTE に対して、5G 展開に関連してネットワーク技術を提供する契約への入札を禁止している[26]。また、この領域で特に新しい法規制の動きはないが、2018 年に Department of Defence が新たなサイバーユニットを二つ設立している。通信傍受による諜報活動を妨害する Defence SIGINT と、軍におけるサイバー部隊の成長サポートに向けた組織構築をする Cyber Command がこれにあたる[31]。

ア） 略称名称一覧（各カテゴリのアルファベット順）

カテゴリ	略称	正式名称
制度	ACL	Australian Consumer Law
	CCA	Competition and Consumer Act 2010 (Cth)
	Corporations Act	Corporations Act 2001 (Cth)
	Criminal Code	Criminal Code Act 1995
	Customs Act	Customs Act 1901 (Cth)
	GDPR	General Data Protection Regulation
	ISM	Australian Government Information Security Manual
	NDB scheme	Notifiable Data Breaches scheme
	Privacy Act	Privacy Act 1988 (Cth)
	PSPF	Protective Security Policy Framework
	Standard	Prudential Standard CPS 234 Information Security
	Telecommunications Act	Telecommunications Act 1997 (Cth)
	TIA Act	Telecommunications (Interception and Access) Act 1979 (Cth)
組織	ACCC	Australian Competition and Consumer Commission
	ACMA	Australian Communications and Media Authority
	ACSC	Australian Cyber Security Centre
	APRA	Australian Prudential Regulation Authority
	ASD	Australian Signals Directorate
	ASIC	Australian Securities and Investment Commission
	OAIC	Office of the Australian Information Commissioner
	SIGINT	signals Intelligence
その他	ACORN	Australian Cybercrime Online Reporting Network
	DSGL	Defence and Strategic Goods List
	EPL	Evaluated Products List
	RCM	Regulatory Compliance Mark

イ） 重要インフラの定義

オーストラリアにおける critical infrastructure asset の定義は Security of Critical Infrastructure Act 2018 の第 9 条で規定されており、critical electricity asset 、critical port 、critical water asset 、critical gas asset と、内務大臣 (Minister) が critical infrastructure asset として宣言した資産及び規則により規定された資産がこれにあたる[48]。

5.2.2.2.4 Evidence 及び原典

a. 法律事務所による回答

AUSTRALIA

December 26, 2018

1.An overview of your jurisdiction's cyber security legislation and regulations, including both legally binding laws or non-binding guidance or principles, as they concern network systems for the "Internet-of-Things" and/or information and communication technology.

[Existing Legislation and Regulations]

Australia has a complex and fractured legislative and regulatory framework for data protection, information risk and cyber security issues. There are different regimes that apply at the federal level to those that apply at the State or Territory level, requirements that apply to specific sectors（particularly in the telecommunications sector）and also a mix of criminal and other laws.

There is no specific legislation in Australia which excludes hardware or software which may include bugs or viruses which pose cyber security threats, however, the current legislative and regulatory environment provides a framework for both government agencies and private sector organisations to mitigate potential cyber security threats. [1] It has been sought to set out an overview of this framework below to provide context of the Australian environment.

Government cyber security initiatives

The Australian Government has developed a number of initiatives in response to the increased regulatory concern with cyber security related incidents, including the following:

- The Australian Cyber Security Centre（ACSC）[https://www.acsc.gov.au/] which is the Australian Government's primary cyber security body. ACSC releases an annual Threat Report on the trends and changing landscape of cyber security and cyber incidents. [2] The 2017 Threat Report details the security challenges presented by outsourcing arrangements involving third party providers, particularly as these are attractive targets due to the volume of customers and the opportunity for the exploitation of broad access to customer networks. It also regularly publishes Strategies to Mitigate Cyber Security Incidents, identifying a myriad of mechanisms to increase cyber security, including the "essential eight" which make it harder for

adversaries to compromise systems such as application whitelisting, patching applications, application hardening and patching operation systems. [3]

- Australian Cybercrime Online Reporting Network (ACORN) [https://www.acorn.gov.au/] which is a national online system that allows the public to securely report instances of cybercrime. [4] The ACORN provides the public with a simple method to report an incidence of cybercrime. This may include hacking, online scams, online fraud, identity theft and attacks on computer systems. The organization hopes to create further awareness, encourage the sharing of information between government and public sector to reduce and help resolve these incidences.
- CERT Australia is part of the Australian Cyber Security Centre and is the national computer emergency response team that acts as the point of contact in Government for cyber security issues affecting major Australian businesses and owners and operators of Australia's critical infrastructure and systems of national interest. It encourages the establishment of partnerships with businesses (there are currently over 500 such partnerships) before an incident occurs, so that CERT may share information on prevention methods and quickly assist in the event of a cybercrime. [5] CERT also operates the Australian Internet Security Initiative, a public-private partnership, aiming to reduce malicious software and service vulnerabilities.
- Australian Signals Directorate [https://asd.gov.au/about/index.htm] which is the national intelligence, cyber security and offensive operations support for the Australian Government and the Australian Defence Force. Amongst other things, the Australian Signals Directorate provides strategies in mitigating cyber-crime and managing cyber security risks, in particular to deal with, targeted cyber intrusions, ransomware and external adversaries who destroy data; malicious insiders who steal data and the like. [6]
- The Australian Security Intelligence Organisation (ASIO) has power under the Australian Security Intelligence Organisation Act 1979 (Cth) and the Intelligence Services Act 2001 (Cth) to conduct various activities including surveillance.

Australian Cyber Security Strategy 2016

Australia's Cyber Security Strategy was released in April 2016, and sets out the Australian Government's program for advancing and protecting Australia's interests online. [7] The strategy promotes various initiatives and has several key focuses including the following:

- education: creating awareness of the threats of cybercrimes in the community;

- partnerships: a joint effort is required to combat cybercrimes, and as such the government is developing partnerships with businesses and the IT industry to be able to respond effectively to cyber threats;
- developing cyber defences: producing better mechanisms and methods to deal with cyber-attacks, encouraging growth and innovation; and
- global efforts: strengthening international engagement on cybercrime, including the development of a harmonised international legal framework.

The first annual update on the Australian Cyber Security Strategy was released in 2017 which assessed the progress thus far on the strategy against each goal and established next steps against the strategy. The next steps include action items such as guidance for government departments to manage supply chain security risks in ICT equipment/services and various other initiatives. As the government continues to implement the Australian Cyber Security Strategy further legislative and regulatory developments may occur.

Australian Government Information Security Manual

The manual is not legally binding, but sets out guidance and standards for organisations to consider when forming their risk management framework in respect of cyber security. The manual includes guidelines in relation to the authorisation of systems, cyber security incidents, communications infrastructure and the management of ICT equipment (amongst others). [8]

The Protective Security Policy Framework

The Framework is designed to support government entities (including corporate Commonwealth entities and wholly-owned Commonwealth companies) in implementing policy in the areas of security, governance, personnel security, physical security and information security. Detailed guidance is provided on safeguarding from cyber threats and robust ICT systems, along with an accreditation system to certify that appropriate levels of security are being applied to ICT systems. [9]

Privacy and data protection - Office of the Australian Information Commissioner

In Australia, the *Privacy Act 1988* (Cth) (**Privacy Act**), which includes the Australian Privacy Principles (**APPs**), regulates how personal information is handled. Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable whether true or not and whether recorded in material form or not. Practically, the Privacy Act applies to all government agencies and private sector organisations with an annual turnover of at least $3 million AUD. The Privacy Act requires organisations to adopt a privacy by design approach to ensure that privacy is designed into each aspect of an organisation. [10]

The mandatory data breach notification regime was introduced in Australia in February 2018 under the Privacy Act, and imposes a range of obligations on organisations where any eligible data breach has, or is suspected, to have occurred. Under the regime, organisations are obliged to notify the Office of the Australian Information Commissioner (**OAIC**), individuals and, in some cases, the media of certain data breaches. [12] Notification to the media can be a particularly harsh consequence, particularly as media coverage and negative press associated with a cyber-incident can often be more detrimental to an organisation than the incident (especially in terms of lost revenue etc.).

An eligible data breach is a breach where there has been unauthorised access or unauthorised disclosure of personal information (or a loss of personal information) and it is likely to result in serious harm to impacted individuals. There are a number of key criteria to examine when determining if serious harm is likely to result from a breach which should be assessed holistically and take into account: the kinds of information, sensitivity, security measures protecting the information, the nature of the harm (i.e. physical, psychological, emotional, financial or reputational harm) and the kind(s) of person(s) who may obtain the information.

The introduction of the regime has resulted in many organisations requiring detailed contractual obligations with third party suppliers in relation to cyber security and the protection of personal information of their customers/clients. Complimenting this regime, the OAIC has also released several guidance notes relating to the regime which include topics such as the security of personal information, whilst these are not legally binding, they are considered to set industry best practice.

Telecommunications specific requirements

The *Telecommunications Act 1997* (Cth) (**Telecommunications Act**) and *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIA Act**) (which includes the Data Retention Scheme introduced by the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth)) impose a number of specific data retention and data security requirements on carriers, carriage service providers and others.

The ACMA is responsible for regulating telecommunications in accordance with the Telecommunications Act and TIA Act.

Under the TIA Act, the Australian Security and Intelligence Organisation (**ASIO**) and certain domestic law enforcement agencies can authorise the disclosure of telecommunications data by a carrier or carriage service provider, [14] including

telecommunications data collected and retained under the Data Retention Scheme. The access rights and powers are set out in Chapter 4 of the TIA Act.

Section 7 of the TIA Act prohibits interception of a communication over a telecommunication network without a court order, for covert surveillance or without the consent of at least one party to the communication. Wholly private networks that are not in any way connected to or use a public telecommunications network fall outside of this federal law, but must be considered under relevant State and territory laws.

The Data Retention Scheme, which came into force in October 2015, requires service providers to, amongst other things, collect and securely retain certain information about communications made through telecommunications services (but not the communications themselves, i.e. the obligation is to retain "metadata") for a period of 2 years [15] (see Part 5-1A of the TIA Act for the obligations relating to data retention).

Communications Alliance

The Communications Alliance (**CA**) promotes the interests of the Australian communications industry and the protection of consumer interests. Membership to the CA is voluntary, however, industry names such as Google, Optus, Telstra and Vodafone (amongst others) are involved in the CA. The CA sets industry standard codes that intend to define good industry practice along with various guidelines and standards. The codes cover areas such as cyber security practices and information accessibility and include the Internet Industry Codes of Practice - Internet and Mobile Content, iCode and the Telecommunications Consumer Protections (TCP) Code.

Australian Securities and Investment Commission

The Australian Securities and Investment Commission (**ASIC**), the corporate regulator in Australia, released Report 429 (Cyber resilience: Health check) in March 2015. This report discussed a broad range of issues with respect to a corporations' ability to prepare, respond, adapt and recover from a cyber-attack.

Although the report is not legally binding, it can be considered as industry best practice in Australia and serves as a reference point for issues such as how cyber risks should be addressed by entities (taking into account current legal and compliance obligations) and how entities can improve their cyber resilience. [17] In particular, the report:

- recommends that corporations regularly review and update their cyber-risk management practices;
- provides guidance on how to implement "health checks" which ensure the entities respond/recover to cyber-attacks in line with their obligations; and

- emphasises that effective corporate governance should involve active engagement by directors and the board in managing any applicable cyber risk and that directors may need to take cyber risks into account when undertaking their duties.

Additionally, ASIC also sets out eleven 'good practices' as guidance for organisations to establish and maintain cyber resilience processes. The 'good practices' include:

- board engagement and governance;
- cyber risk management and threat assessment;
- collaboration and information sharing;
- asset management and cyber awareness training;
- protective measures and controls;
- detection systems and processes; and
- response and recovery planning.

While boards and directors have been aware of these issues for some time, the fact that ASIC expressly identified these issues in its report and has released further guidance on cyber resilience good practice, highlights that cyber security and information security are very much 'front of mind' issues for Australia's corporate regulators.

A failure to appropriately monitor and manage cyber risks could cause a director to breach their duty to exercise their powers and duties with care and diligence（see section 180）. The potential penalties for breaches of directors of duties include financial penalties and being disqualified from acting as a director or officer of a corporation for a period.

The potential consequences of failing to comply with these continuous disclosure obligations including the imposition of civil penalties by a court.

Australian Prudential Regulation Authority

The Australian Prudential Regulation Authority（**APRA**）, Australia's regulator of the banking, insurance and superannuation financial sectors, released the new Prudential Standard CPS 234 Information Security（the **Standard**）to commence on 1 July 2019. The Standard applies to APRA regulated entities including authorized deposit taking institutions, general insurers, life companies and private health insurers. Under the Standard, APRA regulated entities are obliged to maintain information security policies, robust incident management mechanisms and security capabilities commensurate with the size and extent of threats to its information assets. The Standard specifically requires entities to ensure that any related or third parties who may be involved in the information security or information assets of the entity also comply with the obligations under the Standard. [19]

APRA also has several practice guides relating to cyber security issues to assist regulated institutions manage cyber security risks. The guides include CPG 234 - Management of Security Risk in Information and Information Technology and CPG 235 - Managing Data Risk. The guides themselves are not legally enforceable, but do indicate best practice. [20]

[Forthcoming Legislation and Regulations and Discussions on Future Trends]

The federal parliament recently passed under urgency a very wide ranging omnibus amendment act (*Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth)) which - ostensibly - is to provide law enforcement agencies with access to encrypted data for serious crime investigation. [21] In reality, the legislation may inadvertently have a much broader remit with limited judicial oversight, and this has caused an eruption from local and global technology firms which have stated the legislation has the potential of significantly impacting on security/encryption solutions in Australia. The enacted laws are ambiguous in many areas and the political opposition party has flagged that a condition of its agreement to pass the act in parliament was the right to raise significant amendments after the pending holiday season. [22]

At its heart, the Act allows various agencies to:

- issue a "technical assistance notice", which will require a communications provider to give assistance that is reasonable, proportionate, practicable, and technically feasible;
- issue a "technical capability notice", which will require a communications provider to build new capabilities to assist. The Attorney-General must consult with the communications provider prior to issuing the notice, and must be satisfied that the notice is reasonable, proportionate, practicable and technically feasible; and
- make "technical assistance requests", to give foreign and domestic communications providers and device manufacturers a legal basis to provide voluntary assistance to various Australian intelligence organisations and interception agencies relating to issues of national interest, national security, and law enforcement. [23]

Organisations will need to ensure customer terms and conditions deal carefully with the matter of legal compliance and any commitments made to customers generally.

Consumer Data Right

The introduction of the Consumer Data Right in 2019 will provide consumers with the right to access and move their consumer data. The right will be established sector by sector (with banking, energy and the telecommunications sectors being first cabs off the

rank). The consumer data right will involve detailed data rules to ensure appropriate compliance and technical requirements particularly around the transfer of data.

It is intended that the consumer data right will also include specific privacy safeguards to enhance the security of consumer data right information. It is likely that the introduction of the consumer data right will include specific guidance around cyber security risks and issues that may arise in information security when allowing consumers access to such data. [24]

References:

Existing legislation and regulations

- ASIC - Cyber resilience good practices [https://asic.gov.au/regulatory-resources/digital-transformation/cyber-resilience/cyber-resilience-good-practices/]
- ASIC - REP 429 Cyber Resilience: Health Check, 19 March 2015 [https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-429-cyber-resilience-health-check/]
- APRA - CPG 234 - Management of Security Risk in Information and Information Technology [https://www.apra.gov.au/sites/default/files/Prudential-Practice-Guide-CPG-234-Management-of-Security-Risk-May-2013_1.pdf]
- APRA - CPG 235 - Managing Data Risk [https://www.apra.gov.au/file/7071]
- APRA - Prudential Standard CPS 234 Information Security [https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf]
- Australia's Cyber Security Strategy, April 2016 [https://cybersecuritystrategy.homeaffairs.gov.au/sites/all/themes/cybersecurity/img/PMC-Cyber-Strategy.pdf]
- Australia's Cyber Security Strategy - First Annual Update [https://cybersecuritystrategy.homeaffairs.gov.au/australia%E2%80%99s-cyber-security-strategy]
- Australian Government Information Security Manual [https://acsc.gov.au/publications/ism/Australian_Government_Information_Security_Manual.pdf]
- ACSC - Threat Report, 2017 [https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf]
- Communications Alliance - Industry Codes [http://www.commsalliance.com.au/Documents/all/codes]

- Criminal Code Act 1995 (Cth) [https://www.legislation.gov.au/Details/C2018C00500/Html/Volume_2#_Toc532547391]
- Intelligence Services Act 2001 (Cth) [https://www.legislation.gov.au/Details/C2018C00357]
- OAIC - Guide to securing personal information [https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information]
- Privacy Act 1988（Cth）[https://www.legislation.gov.au/Details/C2018C00456]
- Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) [https://www.legislation.gov.au/Details/C2017A00012]
- The Protective Security Policy Framework [https://www.protectivesecurity.gov.au/Pages/default.aspx]
- Telecommunications Act 1997 (Cth) [https://www.legislation.gov.au/Details/C2018C00495]
- Telecommunications (Interception and Access) Act 1979 (Cth) [https://www.legislation.gov.au/Details/C2018C00503]
- Telecommunications（Interception and Access）Amendment（Data Retention）Act 2015（Cth）[https://www.legislation.gov.au/Details/C2015A00039/Download]

Forthcoming legislation etc.

- Telecommunications and Other Legislation Amendment（Assistance and Access）Act 2018（Cth）[https://www.legislation.gov.au/Details/C2018A00148]
- The Treasury - Consumer Data Right [https://treasury.gov.au/consumer-data-right/]
- News article - Encryption: Tech Sector is reeling [https://www.innovationaus.com/2018/12/Encryption-Tech-sector-is-reeling]

2.Details of your jurisdiction's cyber security-related regulations relevant to procurement of goods in the following sectors

(a) Government (national security, defense, police, fire station, tax, academic research, etc.)

[Existing Legislation and Regulations]

The procurement of goods and services in the government sector is typically governed by specific legislation and policy concerns which vendors are contractually obliged to comply with. For example, many government ICT contracts require vendors to comply with particular government policies which will be dependent on the level of government contracted with (i.e. Federal or State/Territory) or on the relevant government agency. For example:

- the Department of Finance provides its own model cyber security clauses for inclusion in government contracts; and
- the South Australian government has specific guidelines relating to cyber security risk management which provide the specific policies and standards to be complied with in ICT procurement. [25]

This is a particular area of concern for the government and in August 2018, the Australian government prohibited providers Huawei and ZTE from bidding on contracts relating to the 5G rollout to provide network related technology on the basis of national security concerns. [26]

The urgent passing of the new *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) also provides law enforcement agencies with additional powers in relation to the access of encrypted data for serious crime investigation.

Defence Trade Controls

Where technology is being procured for use in defense / national security where those goods are dual use goods (i.e. can be used for both military and civilian purposes), there may be particular customs requirements which apply. In particular, sections 112, 112A and 112B of the Customs Act specify when and how the Commonwealth government can prohibit the export of goods for a military end-use.

Such export only occurs when a person in Australia sends or provides access to DSGL-listed software or technology to another person outside of Australia (ie, information is transmitted electronically). Examples of supply include sending DSGL-listed software or technology via email or fax, or providing someone outside of Australia with a password to access DSGL-listed software or technology stored electronically.

The Defence and Strategic Goods List (**DSGL**) is the list that specifies the goods, software or technology that is regulated when exported, supplied, brokered or published. For more information about the DSGL and Australia's export controls, see the Department of Defence's export controls website [http://www.defence.gov.au/ExportControls/AboutUs.asp].

Evaluated Products List

Where goods are procured for use in government systems/networks, please see the information set out below in relation to the Evaluated Products List. The Evaluated Products List (**EPL**) sets out a list of ICT security products that have been evaluated by the Australian Signals Directorate (ASD) for use in Australian government agencies. Products on the EPL list may be used to build secure systems and networks as

set out in the Australian Government Information Security Manual and have been certified against the ISO 15408. [29]

Additionally, the guidance under the Protective Security Policy Framework relating to the development and maintenance of robust ICT systems under the framework for Commonwealth entities directs entities to ensure that suppliers provide the necessary security to mitigate security threats and to use those products contains on the EPL. [30]

[Forthcoming Legislation and Regulations and Discussions on Future Trends]

As at the current date, there are no forthcoming legislation or regulations regarding the procurement of cyber security goods and services in the government sector.

However, as mentioned above, cyber security has been on the radar of government, particularly in relation to defence. In addition to the government bodies listed above (i.e. CSOS; ASC), most recently, on 29 January 2018, Australia's defence department also established two new cyber units - a defence signals intelligence unit called SIGINT and "Cyber Command" with the intention of creating an organizational structure to support the future growth of Australia's military cyber workforce which was outlined in the 2016 Defence Whitepaper. [31]

References:

- Department of Finance - Model Cyber Security Clauses [https://www.finance.gov.au/blog/2014/09/05/model-cyber-security-clauses/]
- Defence Export Controls [http://www.defence.gov.au/ExportControls/AboutUs.asp]
- Evaluated Products List [https://www.asd.gov.au/infosec/epl/index.php] [32]
- ISMF Guideline 6 - Cyber security in procurement activities [https://digital.sa.gov.au/sites/default/files/content_files/policy/cyber-security-procurement-activities.pdf]
- Procure IT Framework [https://procurepoint.nsw.gov.au/before-you-supply/ict-contract-templates/procure-it-framework]

(b) Critical infrastructure (telecommunication, electricity, transport, etc.)

[Existing Legislation and Regulations]

The management of security risks (including cyber security risks) to critical infrastructure in Australia is managed by the Critical Infrastructure Centre (**CIC**). The CIC focuses on risks of sabotage, espionage and coercion in telecommunications, electricity, gas, water and ports. The *Security of Critical Infrastructure Act 2018* (Cth) commenced in July 2018 and:

- establishes a Register of Critical Infrastructure Assets to assist in the proactive management of risks facing such assets and provides the Secretary of the Department of Home Affairs with the ability to obtain detailed information from the owners of such assets; and
- provides the Minister for Home Affairs with the ability to direct an owner/operator of critical infrastructure to do or not do a specified thing to mitigate against a national security risk. [33]

Government bodies such as the Australian Cyber Security Centre also provide assistance and support relating to cyber threats to the owners/operators of critical infrastructure.

Given the introduction of the *Security of Critical Infrastructure Act 2018*, the procurement of goods and services relating to cyber security / networks will likely be under increased scrutiny. Such procurement will typically be governed by governmental policy concerns which vendors are contractually obliged to comply with and as such the comments above at（a）are applicable.

Telecommunications

The telecommunications sector is heavily regulated, the Telecommunications Act restricts the installation of telecommunications facilities to particular types of facilities (i.e. low impact facilities). Telecommunications equipment is also heavily regulated with only certain equipment being permitted to be imported into Australia for use. [34]

[Forthcoming Legislation and Regulations and Discussions on Future Trends]

As at the current date, there are no forthcoming legislation or regulations regarding the procurement of cyber security goods and services relating to critical infrastructure. However, the use（if any use is made）of the powers established under the Security of Critical Infrastructure Act 2018（Cth）will be an interesting area to watch.

References:

- ACMA - Bringing communications equipment into Australia [https://www.acma.gov.au/theACMA/bringing-communications-equipment-into-australia]
- ACMA - Industry and Infrastructure [https://www.acma.gov.au/Industry/Telco/Infrastructure/Network-facilities/industry-infrastructure-network-facilities-i-acma]
- Critical Infrastructure Centre [https://cicentre.gov.au/infrastructure]
- Security of Critical Infrastructure Act 2018 (Cth) [https://www.legislation.gov.au/Details/C2018A00029]

(c) Equipment or services for consumers

[Existing Legislation and Regulations]

If a product or service fails to meet a guarantee, a consumer has rights against the supplier, and in some cases the manufacturer, who must provide a 'remedy' if the guarantee is not met.

The specific remedy available depends on the guarantee breached, whether the action is brought against the supplier or manufacturer, and the nature of the breach. For example, if it is a minor problem the supplier can choose between providing a repair or offering the consumer a replacement or refund. The problem should be rectified at the cost of the supplier and within a reasonable timeframe.

[Forthcoming Legislation and Regulations and Discussions on Future Trends]

As at the current date, there are no forthcoming legislation or regulations regarding the procurement of equipment or services for consumers in this space.

References:

- Australian Competition and Consumer Commission - Consumer rights and guarantees [https://www.accc.gov.au/consumers/consumer-rights-guarantees]
- Competition and Consumer Act 2010 (Cth) [https://www.legislation.gov.au/Details/C2018C00437]

b. 法律事務所を通じた Q&A

1. The Privacy Act requires organisations to adopt a privacy by design approach to ensure that privacy is designed into each aspect of an organisation.
   の下線部について、具体的にどのようなプライバシーなのか？
   - ✓ Ans: Organisations should design their personal information security measures with the aim to: prevent the misuse, interference, loss or unauthorized accessing, modification or disclosure of personal information; detect privacy breaches promptly; and be ready to respond to potential privacy breaches in a timely and appropriate manner. Importantly, organisations should integrate privacy into their risk management strategies and embed them early, including by choosing the appropriate technology and measures to respond to a changing technological landscape overtime.
2. The GDPR imposes additional requirements in respect of cyber security to which many organisations are also subject.
   の下線部について、GPDR は具体的にどのような追加要件を課しているのか？
   - ✓ Ans: Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context

and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

3. There are different regimes that apply at the federal level to those that apply at the State or Territory level, requirements that apply to specific sectors (particularly in the telecommunications sector) and also a mix of criminal and other laws.

   の下線部について、サイバーセキュリティ関連の規制に関して、州もしくは準州レベルで適用されるものもあると記載されているが、受領したレポートでは基本的に連邦レベルでの規制について述べられているように見える。州／準州レベルの規制ではどのようなものがあるか？

   ✓ Ans: Please see below a brief overview in the sections titled "State and Territory Government cyber security initiatives"; "Privacy and data protection - Office of the Australian Information Commissioner" and "Criminal Laws" regarding State and Territory regulations / government initiatives.

   - State and Territory government cyber security initiatives
     In Australia, State and Territory governments, amongst other things, maintain policies, legislation and plans within their jurisdictions and maintain counter-terrorism and consequence-management capabilities (including, in response to cyber security issues) within their relevant agencies and determine prevention strategies and operational responses to threats, including seeking assistance from other jurisdictions. For example, the New South Wales and Victorian governments have each launched their first Cyber Security Strategies which plans include whole-of government integrated approaches to managing cyber risks and responding to cyber security threats, safeguarding information, assets, services and citizens across their respective states. In addition, Western Australia, Victoria, Queensland, New South Wales and South Australia have each established a Joint Cyber Security Centre in their capital cities with the aim being that those facilities will play a major role in keeping Australians safe from cyber-attacks. [42]

   - Criminal laws
     Most commonly, persons suspected of engaging in cybercrime are charged pursuant to the Criminal Code, given its universal application in all States and Territories in Australia.

4. Products on the EPL list may be used to build secure systems and networks as set out in the Australian Government Information Security Manual and have been certified against the ISO 15408.

   の下線部について、政府のシステム／ネットワークに使用する物品／システムに EPL 記載のものを使うことについて、法的強制力はないという認識で正しいか？

   ✓ Ans: The EPL sets out products which are specified for certain purposes. It is not a legal requirement per se to only use products listed on the EPL given, in certain circumstances, the EPL may not contain an extensive list. However, where a product is used for a purpose listed in the Information Security Manual then it needs to comply with any requirements listed in the Information Security Manual which may include complying with the EPL. [46]

5. In addition to the government bodies listed above (i.e. CSOS; ASC), most recently, on 29 January 2018, Australia's defence department also established two new cyber units - a defence signals intelligence unit called SIGINT and "Cyber Command" with the intention of creating an organizational structure to support the future growth of Australia's military cyber workforce which was outlined in the 2016 Defence Whitepaper.
   の下線部について、SIGINT というのはサイバーユニットの名称という認識で正しいか？（通常、SIGINT とは通信傍受による諜報活動そのものを指すように見受けられる）
   - ✓ Ans: Correct, it is the name of the defence signals intelligence unit (and, yes, it is also commonly a generic name given to signals intelligence).

6. Telecommunications equipment is also heavily regulated with only certain equipment being permitted to be imported into Australia for use.
   の下線部について、オーストラリアへの輸入が許可されている特定の通信機器は、どういった基準で選ばれているのか？
   - ✓ Ans: By way of high level overview, the operation or use of communications equipment that is designed to work in Australia can cause interference with the operation of other equipment or endanger the health or the safety of others. As such, even if an item of communications equipment is suitable for use in another country it may not necessarily be suitable for use in Australia. By way of example:
     - telecommunications equipment such as telephones, modems, answering machines and facsimile machines may only be connected to an Australian telecommunications network if the equipment bears an Australian-compliant mark (e.g. the "RCM" or the "A-Tick") regulatory compliance mark;
     - many cordless telecommunications systems which are suitable in other countries cannot be used in Australia because they use radiofrequencies that are not available for such use in Australia;
     - mobile phone booster amplifiers or 'boosters' which connect to a mobile phone to boost or amplify the signal to that phone are prohibited in Australia (and, it is illegal to sell or supply boosters); and
     - the use of non-standard radio communications equipment (i.e. devices that generally don't bear the C-Tick, A-Tick or the RCM regulatory compliance marks) not designed for the Australian environment may also cause costly interference. [47]

7. オーストラリアにおける“Critical Infrastructure”の定義は何か？
   - ✓ Ans: Critical Infrastructure Asset' is defined in section 9 of Security of Critical Infrastructure Act 2018 to include the following:
     - a 'critical electricity asset', which means:
       - a network, system, or interconnector, for the transmission or distribution of electricity to ultimately service at least 100,000 customers; or
       - an electricity generation station that is critical to ensuring the security and reliability of electricity networks or electricity

systems in a State or Territory, in accordance with any requirements for security and reliability prescribed by rules (Note: rules are made by the Minister for Home Affairs pursuant to section 61);

- a 'critical port', which means land that forms part of any of the following security regulated ports: Broome Port; Port Adelaide; Port of Brisbane; Port of Cairns; Port of Christmas Island; Port of Dampier; Port of Darwin; Port of Eden; Port of Geelong; Port of Gladstone; Port of Hay Point; Port of Hobart; Port of Melbourne; Port of Newcastle; Port of Port Botany; Port of Port Hedland; Port of Rockhampton; Port of Sydney Harbour; Port of Townsville; a security regulated port prescribed by rules;
- a 'critical water asset', which means one or more water or sewerage systems or networks that:
  - are managed by a single water utility; and
  - ultimately deliver services to at least 100,000 water connections or 100,000 sewerage connections;
- a critical gas asset, which means:
  - a gas processing facility that has a capacity of at least 300 terajoules per day or any other capacity prescribed rules;
  - a gas storage facility that has a maximum daily quantity of at least 75 terajoules per day or any other quantity prescribed by rules;
  - a network or system for the distribution of gas to ultimately service at least 100,000 customers or any other number of customers prescribed by rules;
  - a gas transmission pipeline that is critical to ensuring the security and reliability of a gas market, in accordance with rules that may prescribe requirements for security and reliability;
- an asset declared by the Minister for Home Affairs (pursuant to section 51) to be a critical infrastructure asset; or
- an asset prescribed by rules. [48]

Note: Rules (made by the Minister for Home Affairs pursuant to section 61) may prescribe that an asset falling into one of the above categories is not a 'Critical Infrastructure Asset'.

References:

- Security of Critical Infrastructure Act 2018 (Cth) https://www.legislation.gov.au/Details/C2018A00029

8. 政府調達／通信インフラ・重要インフラの調達／コンシューマー向け機器・サービスの調達において、違反として摘発された事例や排除された事例はないか？

✓ Ans: The Australian counsel is not aware of instances of prosecution in connection with procurement or supply chain cyber-attacks within the sectors identified above in Australia (and, this is not to say there will not be instances in the near-future). Cyber-security is an issue receiving a lot of attention from both regulators and the private sector which, in part, is influenced by the negative publicity surrounding major security incidents in Australia. Below is an example of such incidents in the sectors identified above:

(ii) Telecommunications or other critical infrastructure

PageUp / Australia Post / Telstra - May 2018

'PageUp' is an online recruitment services organisation and service as a software provider. It provides a cloud-based human resources software to various major Australian clients including Australia Post (the primary

government-owned postal service business) and Telstra (a major telecommunications company). PageUp identified that its systems had been infected with malware, which could have compromised employee data of its clients. The incident was notified to the OAIC, UK's Information Commissioner's Office, ACSC and CERT Australia.
The ACSC commended PageUp for its level of transparency and response to the incident.
(ii) Equipment or services for consumers
Inbenta / Ticketmaster - June 2018
Ticketmaster UK (an event ticket sales company) identified malicious software on a customer support product hosted by third party Spanish supplier based in the US 'Inbenta Technologies'. This may have compromised customer data in the UK and Australia.
References:

- PageUp: https://www.acsc.gov.au/news/pageup.html
- Inbenta: https://securitybrief.com.au/story/ticketmaster-breached-heres-what-seven-security-experts-had-say

c. 法律事務所による回答以外の情報ソース

- AISEP – Australasian Information Security Evaluation Program
  - ✓ https://acsc.gov.au/infosec/aisep.htm

5.2.2.3 英国

5.2.2.3.1 国としての全体的な状況(まとめ)

英国の政策動向の概要を表 5-9 に示す。

表 5-9 英国の政策動向（まとめ）

	項目	概要
現状	全体傾向	包括的なサイバーセキュリティ法は存在せず、GDPR/PECR、NIS 指令等で対応。Brexit に備え、GDPR/NIS 指令等重要インフラのサイバーセキュリティ要件に関する規制等を国内法に置き換え中。データの保護の方法に関するガイドライン等各省庁・監督機関が対応。データの保護の方法に関する 10 個の技術的アドバイスシートを提供するとともに、政府のセキュリティ機関によるサイバーセキュリティの認証プログラム（Cyber Essentials）を規定している。
	重要インフラの法制度	NIS 指令により、重要インフラ提供企業に対して、サイバー攻撃へのレジリエンスの確保のための適切な手段の確保及び重大インシデントの通知の仕組み確保を義務化、また、高度なサイバーセキュリティに関するガイドラインの提供、暗号化やセキュリティを考慮したシステム設計等、高度なサイバーセキュリティに関するアドバイスを規定している。政府によるセキュリティ認証プログラムの遵守を義務化している。
	政府調達	サイバーセキュリティ及びデータの保護・処理の方法の双方の観点から要件を義務化、政府のセキュリティ機関によるサイバーセキュリティの認証プログラム（Cyber Essentials）を規定。政府調達に関わる企業に対して、遵守を義務付けている。
	認証/認定制度	組織が基礎的なサイバーセキュリティ対策をとっていることを示す Cyber Essentials 認証を実施。基礎レベルの Cyber Essentials は自己診断ベース。Cyber Essentials Plus はこれに加えて、基本的なハッキングやフィッシング攻撃に対する防御等の、オンサイトで脆弱性テストが実施される。国防省のコントラクター向けには Cyber Essentials Plus 取得が強く求められている。
	体制	国家サイバーセキュリティ戦略により新たに設立された GCHQ 配下の国家サイバーセキュリティ・センター（NCSC）を中心に、サイバーセキュリティの国家全体のレベルの底上げを実施中。また、英国の重要な国内インフラの一部に Huawei が関与することにより生じると考えられるリスクの軽減を目的に、Huawei のサイバーセキュリティ評価センターの監視委員会である Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board が設立された。
今後	全体的な傾向	現時点でサイバーセキュリティに関する重要な規制の改正は見受けられていないが、2016 年 11 月に公表された「国家サイバーセキュリティ戦略 2016」に基づき、システムやインフラへの投資や新たなイノベーションセンターの設立等のセキュリティの強化等、規制外の介入の推進・検討が進められている。

	項目	概要
	重要インフラの法制度	重要ネットワークインフラに関する政府の合同委員会における見解に基づくサイバーセキュリティ要件の強化進行中。また、重要インフラのインシデント発生時の緩和計画と危機管理計画を策定中。
	政府調達	大手国際企業からの調達時における最低限のセキュリティ基準の規定が進行中。

現在の英国における IoT セキュリティに関する規制は、EU による規制及び英国の国内法によって規定されており、EU からの離脱（Brexit）に備え、既存の EU の法律を英国の国内法に置き換えている。例えば、GDPR（General Data Protection Regulation）に相当する個人情報のデータ保護に関する規制 DPA 2018（Data Protection Act 2018）や、五つのセクター（エネルギー・輸送機関・医療・上水道・デジタルインフラセクター）における重要インフラの提供企業及び関連するデジタルサービスプロバイダーに対して、サイバー攻撃のレジリエンスの確保及びインシデント発生時の通知義務等を課す規制 NIS Regulations 2018（Network and Information Systems Regulations 2018）がある。他にも、政府のセキュリティ機関 NCSC（国家サイバーセキュリティ・センター: National Cyber Security Centre）により、データの保護の方法に関するガイドライン 10 Steps to Cybersecurity が規定されていたり、企業のセキュリティレベルを担保する認証制度 Cyber Essentials Scheme が提供されていたりする。

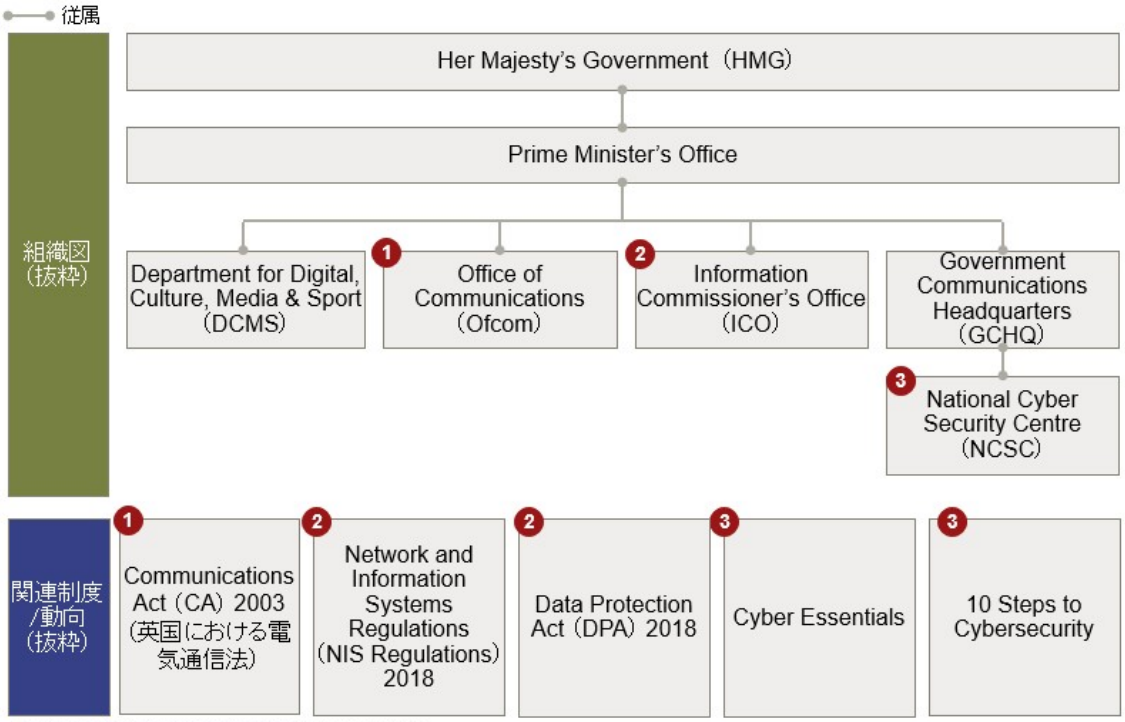
重要インフラについては、重要インフラ事業者に NIS Regulations2018 に加え、Cyber Essentials の遵守を義務付けている。さらに、高度なサイバーセキュリティ対策についてもガイドラインの形で示されており、暗号化やセキュリティを考慮したシステムの設計等を実行することが奨励されている。

政府調達については、企業に対して、サイバーセキュリティ及びデータの保護・処理の方法の双方の観点から義務を課していたり（DPA 2018 及び NIS Regulations 2018）、政府によるセキュリティ認証プログラム Cyber Essentials の遵守を義務付けることにより、政府調達時のセキュリティ基準を提示している。

今後に向けては、政府は国家サイバーセキュリティ戦略 National Cyber Security Strategy for the years 2016-2021（the Strategy）を発表し、サイバーセキュリティの強化の方向性を明らかにしている。具体的には、英国のシステム及びインフラへの投資や、新たなサイバーイノベーションセンターの設立等を行うと表明していたり、NCSC 等のセキュリティ機関による組織へのアドバイスまたはガイダンスの提供や、サイバーセキュリティリスクマネジメントの改善の奨励等を通じた規制外の介入の推進・検討がなされていたりする。ただし、英国における規制の動向として、2018 年にはサイバーセキュリティに影響を与える規制の進展が見受けられてきたが、現在進展中の重要な規制の改正は見受けられていない。政府が発表した Secure by Design: Improving the cyber security of consumer Internet of Things のレポートでは、規制化が可能な選択肢を追求している。これは Code of Practice for Consumer IoT Security における特定の項目の規制化について模索していることを意味する。その意味で、サプライヤーはこれらの項目に目を向けることで、英国における将来の規制の動向のヒントを得ることができる [49]。また、重要インフラについては、政府の合同委員会（Joint Committee Report on CNI）が開催され、政府による規制外の介入・奨励（大手国際企業からの調達時における最低限の基準の規定、NCSC 認定の“kitemark”（消費者のための自発的ラベリングスキーム）の確立、政府による重要ネットワークインフラに一斉に影響を及ぼす単一障害点の特定及び緩和・危機管理計画の策定等）が推奨され、セキュリティ対策のさらなる強化の方向性を示している。さらに、中国の通信機器メーカーである Huawei のサイバーセキュリティに関して評価を行う組織 HCSEC（Huawei Cyber Security Evaluation Centre）が運営されており、今後、Huawei のネットワークの規制に関して進展が見られる可能性がある（2018 年 12 月 26 日時点）。また、中国企業の調達に関して、英国政府は、通信事業者が、中国企業から調達できるネットワーク機器の割合を最

大 50%に制限する条項を、2019 年春までに見直しを進めており、サプライチェーン法令に盛り込む準備している模様である。

図 5-4 は、英国における政府関連組織と関連法制度をまとめたものである。番号により、組織と法制度の関連性を表現している（組織の概要は表 5-10 を、法制度の概要は表 5-11 を参照）。DCMS（デジタル・文化・メディア・スポーツ省: Department for Digital, Culture, Media & Sport）は、デジタル（通信、放送、メディアを含む）、スポーツ、市民社会、芸術、遺産、観光の各分野を所掌する。Ofcom（通信庁: Office of Communications）は、英国における電気通信法である CA (Communications Act) 2003 を定めている。ICO（情報コミッショナーズ・オフィス: Information Commissioner's Office）は、情報コミッショナーズ・オフィス情報に関する権利を守るために設立された独立情報保護監督機関であり、英国内での GDPR に関する取り締まりを行う。ICO は、NIS Regulations と DPA 2018 を定めている。GCHQ（政府通信本部: Government Communications Headquarters）は、偵察衛星や電子機器を用いた国内外の情報収集・暗号解読業務を担当する諜報機関である。NCSC は、サイバーセキュリティに関する知見の共有、英国内におけるサイバー関連リスクの低減、具体的サイバー攻撃事案への対処、英国内におけるサイバー攻撃事案への対処能力向上等、英国のサイバーセキュリティ対策の中心的役割を担う。NCSC は、Cyber Essentials と 10 Steps to Cybersecurity を定めている。



各関連制度/動向と関連する省官庁の番号と対応
出所(Departments, agencies and public bodies - GOV.UKおよび各種資料より抜粋)

図 5-4　英国の政府関連組織と関連法制度

表 5-10　英国における政府関連組織

DCMS	デジタル・文化・メディア・スポーツ省。 デジタル（通信、放送、メディアを含む）、スポーツ、市民社会、芸術、遺産、観光の各分野を所掌する。
Ofcom	通信庁。 通信、放送に関する規制監督を行っている。コンテンツ規制から周波数管理、電気通信及び放送事業に対する経済的規制まで所掌するほか、CA (Communications Act) 2003 の適用における権限をもつ。
ICO	情報コミッショナーズ・オフィス。 情報に関する権利を守るために設立された独立情報保護監督機関であり、英国内での GDPR に関する取り締まりを行う。
GCHQ	政府通信本部。 偵察衛星や電子機器を用いた国内外の情報収集・暗号解読業務を担当する諜報機関。
NCSC	国家サイバーセキュリティ・センター。 サイバーセキュリティに関する知見の共有、英国内におけるサイバー関連リスクの低減、具体的サイバー攻撃事案への対処、英国内におけるサイバー攻撃事案への対処能力向上等、英国のサイバーセキュリティ対策の中心的役割を担う。

表 5-11　英国における関連法制度

CA 2003	英国における電気通信法。
NIS Regulations 2018	リスク軽減のために欠かせないネットワーク・情報セキュリティ保護の仕組みを確立。なお、サービスの継続を担保し、規制の実行の責を負うのは、OES (Operators of Essential Services) であるとされている。そのため、OES のサプライチェーンに属する企業に対しては、法律の遵守が奨励されてはいるものの、法的責任が課されることはない。また、主要な要件として、関連する DSP (Digital Services Providers) に対しては、ネットワーク及び情報システムのセキュリティにおけるリスクを管理するために、適切かつ相応な手段を特定し実行することが義務付けられている。
DPA (Data Protection Act) 2018	個人情報のデータ保護に関する規制。 データの保護・処理の方法の観点から、サプライチェーンに属する企業が従わなければならない規制が規定されている。
Cyber Essentials	サイバー攻撃からの技術的保護のために組織が実施すべき基本的な管理策を規定するスキーム。
10 Steps to Cybersecurity	データの保護の方法に関するガイドライン。 企業のシステムにメディアをインポートする前に、すべてのメディアに対してマルウェアのスキャン及びセキュリティ管理の監視とテストを行うといった、送信中及び保管中のデータ保護に関するアドバイスが含まれている。

5.2.2.3.2 対応状況

a. IoT セキュリティ全般

英国における IoT セキュリティに関する規制は、EU による規制及び英国の国内法によって規定されている [1]。英国は Brexit に備え、既存の EU の法律を国内法に置き換える予定であるが [2]、ここでは英国の国内法における IoT セキュリティの代表的な制度について述べる。DPA 2018 は、EU における個人情報のデータ保護の規制にあたる GDPR を英国の国内法に取り入れた法律であり、Brexit 後も EU と個人データの交換を自由に行えることを目的に策定されている。DPA 2018 では、GDPR の内容に加え、対象を GDPR ではカバーしていない処理（インテリジェンスサービス（MI5、MI6、GCHQ [51]））における個人データ処理や手動管理書類（手書き書類等 [52] の処理等）にも拡大したり、規制の違反時における最高罰金額の引き上げ等を行ったりしている [3]。また、PECR (Privacy and Electronic Communications (EC Directive) Regulations) では、公共電子通信ネットワーク PECN（電話ケーブルまたは携帯電話のネットワーク等 [53]：Public Electronic Communication Network）、及び公共電子通信サービス PECS（電話契約やインターネット接続等 [54]：Public Electronic Communication Service）に対して、ネットワーク及びサービスのセキュリティを保護するために、適切な措置を講ずることが義務付けられている。PECR では、特に PECS に対して、（ⅰ）合法的な目的のために、委任された担当者のみが個人データにアクセスが可能な状態にする、（ⅱ）偶発的または違法なデータのアクセス等の行為から保護する、（ⅲ）個人データの処理に関するセキュリティポリシーの実施を確実に行う、ことが義務付けられている [4]。上記の措置を講じたにも関わらず、個人データの漏洩が発生した際は、ICO に通知し、その漏洩が利用者のプライバシーに影響を与える可能性がある場合、漏洩の影響等に関する通知義務が課されている [5]。また、GDPR と同様に、PECR は域外効果 (extraterritorial effect) があり、外資系企業が PECN・PECS のプロバイダーとして英国内でビジネスを行う場合、活動拠点に依らず義務の対象となりうる [6]。CA 2003 の第 105A 条では、PECN・PECS プロバイダーは、PECN・PECS のセキュリティに対するリスクマネジメントのために、技術的・組織的な対策を適切に講じなければならないと規定されている [7]。また、PECN・PECS の運用に重大な影響を与えるセキュリティの違反が発生した場合、または PECN の安定性が低下した場合、Ofcom への通知義務を課している。Ofcom はその通知を受け取ると、他の加盟国における国の規制機関及び ENISA (European Network and Information Security Agency) へ通知を行う [8]。CA 2003 にも域外効果があり、活動拠点に依らず規制が適用される [9]。NIS Regulations 2018 では、エネルギー・輸送機関・医療・上水道・デジタルインフラセクターにおけるオペレーターOES (Operators of Essential Services)、及びオンラインマーケット・オンライン検索エンジン・クラウドサービス等のデジタルサービスプロバイダーDSP (Digital Services Providers) に対して、サイバー攻撃へのレジリエンスを確保するための適切な手順及び管轄当局に重大なインシデントを通知するための仕組みを取り入れることを義務付けており、違反した場合には、高いペナルティ（最高で罰金 1,700 万ポンド）が課される [10]。

Anti-Terrorism Crime and Security Act 2001 では、国家安全保障の保護または国家安全保障に関連しうる犯罪の防止・検出のために、通信会社に、特定の行動規範に従って通信データを保持することを義務付けており [14]、Official Secrets Act 1989 では、スパイ行為及び特定のカテゴリの公式情報への不正な開示に対する主な法的な保護に関して規定している [15]。他にも、Investigatory Powers Act 2016 では、標的とされた通信の傍受、通信データの一括収集、及び大量の通信の傍受を実行するために、英国の諜報機関及び法執行機関に対して新たな権限を導入しており [16]、Digital Economy Act 2017 では、データの共有に関する主要な三つの条項が規定されている [17]。

また、上記に加え、サイバーセキュリティに関して法的な拘束力がないガイドラインや基準も規定されている [18]。NCSC により規定されている 10 Steps to Cybersecurity では、

企業のシステムにメディアをインポートする前に、すべてのメディアに対してマルウェアのスキャン及びセキュリティ管理の監視とテストを行うといった、送信中及び保管中のデータ保護に関するアドバイスが含まれている [19]。加えて、役員または役員レベルのスタッフ向けのガイダンスとなることを目的とし、各企業が導入を検討すべき 10 個の技術的なアドバイスシートが提供されている。具体的には、(i) リスク管理体制、(ii) セキュリティ設定管理、(iii) ネットワークセキュリティ、(iv) ユーザー権限の管理、(v) ユーザーの教育と啓蒙、(vi) インシデント管理、(vii) マルウェア対策、(viii) モニタリング、(ix) リムーバブルメディア管理、及び(x)在宅・リモート勤務 の 10 個について記載されている [30]。

また、英国政府は、サイバー攻撃からの技術的保護のために組織が実施すべき基本的な管理策を規定するスキームである Cyber Essentials Scheme を導入し、組織が各レベル（Cyber Essentials または、Cyber Essentials Plus）の認証基準を満たしていることを保証するフレームワークを提供している。Cyber Essentials 認証は、セルフアセスメントに基づいて付与される。一方、Cyber Essentials Plus は、より高いレベルの認証であり、組織のサイバーセキュリティのアプローチに対する外部テストが含まれる [20]。なお、国内企業と国内以外の企業間における要件の相違はない。英国外にオフィスを保有する場合、国外オフィスも認証基準を満たす必要があり、認証を取得する際のハードルとなりえる [55]。また、2018 年 1 月時点で Cyber Essentials 約 9,500 件、Cyber Essentials Plus 約 2,500 件の計 12,000 件の認定証が発行されている。2019 年 1 月には、Cyber Essentioals/Cyber Essentials Plus 合わせて約 22,000 件（内訳は不明）の認定証が発行されており、英国内に広まっていることがわかる [56]。この他にも、PCI DSS では、支払いカードデータの処理に関する基準を示しており [21]、ISO 27001 及び ISO 27002 は、英国のセキュリティリスクマネジメントにおける産業の基準となるフレームワークとして一般的に適用されている [22]。

b. 重要インフラ

重要インフラについては、上述した NIS Regulations 2018 が適用されており、五つのセクター（エネルギー・輸送機関・医療・上水道・デジタルインフラセクター）の CNI (Critical Network Infrastructure) のオペレーターは、第三者機関を使用する場合には、適切な措置を講じることが推奨されている [33]。しかし、サプライチェーンの調査、適切なリスクアセスメント、及び管理の実施は CNI のオペレーターの責任とされており（なお、大部分のケースにおいて、OES は CNI のオペレーターに含まれる [57]）、第三者機関の使用の有無を問わず、関連するセキュリティ要件を満たすことが義務付けられている [34]。また、CNI のオペレーターは Cyber Essentials の認証基準を満たすことが義務付けられている。

さらに CNI のオペレーターには、追加で高度なサイバーセキュリティ対策（暗号化やセキュリティを考慮したシステムの設計方法等）を実行することが奨励されている [35]。また、サプライヤーと取引を行う際は、CNI のオペレーターは、そのサプライヤーに対して最低限のセキュリティ要件を設定することが望ましいとされている [36]。

c. 政府調達

政府調達については、上述した NIS Regulations 2018 及び DPA 2018（概要は IoT セキュリティ全般にて記載）を基盤に、サイバーセキュリティ及びデータの保護・処理の方法の双方の観点から、サプライチェーンに属する企業が従うべき規制が規定されている [27]。NIS Regulations 2018 においては、リスク軽減のために必要なネットワーク・情報セキュリティ保護の仕組みの確立とサービスの継続を担保し、規制の実行の責を負うのは、OES であるとされている。そのため、OES のサプライチェーンに属する企業に対しては、法律の遵守が奨励されてはいるものの、法的責任が課されることはない。また、主要な要件として、関連する DSP に対しては、ネットワーク及び情報システムのセキュリティにおけるリスクを管理するために、適切かつ相応な手段を特定し実行することが義務付けられている

[28]。さらに、政府調達の案件に入札するすべての企業は、Cyber Essentials の認証を取得する[29]とともに、DPA 2018 に対応する必要があり、違反すると ICO から罰金が科される可能性がある [31]。

5.2.2.3.3 今後の方向性

a. IoT セキュリティ全般

英国における規制の動向として、2018 年にはサイバーセキュリティに影響を与える規制の進展が見受けられてきたが、現在進展中の重要な規制の改正は見受けられていない [23]。英国政府は、より優れたサイバーリスクマネジメントを推進するために、NCSC を介して組織にアドバイスやガイダンスを提供する等、規制外の介入策を探求している。[24][25]。政府は、2016 年から 2021 年にかけての国家のサイバーセキュリティ戦略にあたる National Cyber Security Strategy for the years 2016-2021 (the Strategy) を発表し、この戦略において英国のシステムのシステムとインフラを保護するために 19 億ポンドの投資を行うほか、新しいサイバーイノベーションセンターの立ち上げや ACD (Active Cyber Defence) の開発・適用を表明している（詳細は下記の通り）[26]。

- 英国のシステムとインフラを保護するために 19 億ポンドを投資する。
- 国際的な行動を追求し影響力を発揮する。
- より積極的に介入し、投資を増やす。
- 国軍がレジリエンスをもち、強力なサイバー防御策を保有する。
- サイバーセキュリティスキルの不足に対処するためのプログラムに投資する権限と影響力をもつ。
- 二つの新しいサイバーイノベーションセンターを立ち上げ、最先端のサイバー製品及びダイナミックな新しいサイバーセキュリティ企業の開発を推進する。
- 英国のネットワーク全体でサイバーセキュリティのレベルを大幅に向上させることを目指し、ACD を開発及び適用するために、業界のケイパビリティを利用する。
- より安全なインターネットを構築し、英国でのサイバー犯罪を減少させることを目指す。

b. 重要インフラ

重要インフラについては、英国政府は、サプライヤーに対するサイバーセキュリティ要件を強化しており、2018 年 6 月の発表では、契約に最低基準を書き入れ、各主要サプライヤーの「信用格付け」に相当するものを作成するとされている [37]。また、最近、英国議会の議員から、サイバーセキュリティ大臣に CNI の保護が要求されている。同様に、英国の CNI の国家安全保障戦略に関する合同委員会による報告 (Joint Committee Report on CNI) では、英国の CNI に対する脅威は増大・発展していることを強調している [38]。この報告では、“CNI のサイバーレジリエンスを強化するためのより包括的かつ効果的なアプローチにより、CNI 事業者の文化とその拡大されたサプライチェーンを変えることが必要である。（後略）”と述べられており [39]、CNI の分野の垣根を超えて継続的な文化の変化や改善が促進されるように、政府に対して規制外の介入及び改善の奨励を緊急に検討するよう推奨している [40]。これらの介入及び奨励は、CNI のオペレーターのサプライチェーンにおけるサイバーリスクマネジメントに関する内容が含まれるべきとされており、CNI 事業者が直面している困難に対処するために、次の事項を求めている[41]。

- 特に、大手国際企業から調達する場合は、ハードウェア・ソフトウェア・サービスに対して最低限のセキュリティ基準を強制し実施すること、国際的なプロバイダーに影響を与えるために、政府が G7 等の国際的なフォーラムにおいて外交的な存在感を示すこ

と、そして、信頼できるサプライヤーには、NCSC 認定の「kitemark」（消費者のための自発的ラベリングスキーム）を確立すること

- CNI の各分野に一斉に影響を与えうる「単一障害点」をもつデータサービスプロバイダー・ハードウェア等が蔓延していることに備え、政府はこれらを特定し、積極的に緩和計画と危機管理計画を準備すること

また、Huawei のサイバーセキュリティ評価センターである HCSEC Oversight Board が、英国政府と Huawei の間の一連の取り決めの下、2010 年 11 月から運営されている。このセンターは、英国の重要インフラの一部に Huawei が関与することにより生じると考えられるリスクの軽減を任務としている。

c. 政府調達

政府調達については、2016 年 12 月に政府によって実施された Cyber Security Regulation and Incentives のレビューの報告書では、GDPR (DPA 2018) が、“強固なサイバーセキュリティを基盤とした、頑強なデータ保護の組織体制を形成するための鍵になる”とされている。なお、重要インフラについては、このレビューのスコープから除外されている [32]。

ア） 略称名称一覧（各カテゴリのアルファベット順）

カテゴリ	略称	正式名称
制度	CA	Communications Act
	DPA	Data Protection Act
	GDPR	General Data Protection Regulation
	NIS Regulations	The Network and Information Systems Regulations
	PECR	Privacy and Electronic Communications (EC Directive) Regulations
	RIPA	Regulation of Investigatory Powers Act
組織	CPNI	Center for the Protection of National Infrastructure
	DCMS	Department for Digital, Culture, Media & Sport
	ENISA	European Network and Information Security Agency
	FCO	Foreign & Commonwealth Office
	GCHQ	Government Communications Headquarters
	HCSEC	Huawei Cyber Security Evaluation Centre
	HMG	Her Majesty’s Government
	HMT	HM Treasury
	ICO	Information Commissioner’s Office
	MoD	Ministry of Defence
	NCSC	National Cyber Security Centre
	Ofcom	Office of Communications
	SFO	Serious Fraud Office
	SIS, MI6	Secret Intelligence Service
	SS, MI5	Security Service
	ACD	Active Cyber Defense
その他	CNI	Critical Network Infrastructure
	DSP	Digital Services Providers

	OES	Operators of Essential Services
	PECN	Public Electronic Communication Network
	PECS	Public Electronic Communication Service

イ） 重要インフラの定義

英国における国家インフラセクターは、Chemicals、Civil Nuclear、Communications、Defence、Emergency Services、Energy、Finance、Food、Government、Health、Space、Transport 、及び Water の 13 分野であるとされており、その中でも、英国政府公式の定義として、重要インフラに認定されているのは、

“障害が発生した場合に、

- 経済的・社会的に深刻な影響を及ぼすことを考慮し、サービスの可用性・完全性・提供に対する深刻な悪影響（完全性の喪失による多大な死傷者・犠牲者の発生が考えられる場合も含む）
- 国家安全保障・国防・行政機能への著しい悪影響

をもたらしえる要素（資産・施設・システム・ネットワーク・プロセス及びそれらを運用する重要な作業者）”とされている [58]。

5.2.2.3.4 Evidence 及び原典

a. 法律事務所による回答

UK

December 26, 2018

---

1 An overview of your jurisdiction's cyber security legislation and regulations, including both legally binding laws or non-binding guidance or principles, as they concern network systems for the "Internet-of-Things" and/or information and communication technology.

[Existing Legislation and Regulations]

The UK has a substantial body of law governing cyber security, comprising of both European Union (EU) legislation and UK specific legislation. [1] An overview of the applicable legislative framework in the UK is set out below.

- **EU legislation**

The EU has legislated on matters that impact cyber security through both EU Regulations and EU Directives. EU Regulations are directly applicable in the Member States, although the UK is transposing them into national law in preparation for the UK exit from the EU (Brexit). EU Directives are not directly applicable in the territory of the Member States. Their objectives must be implemented into the national legislation by each of the Member States by a specific date. However, as all existing EU law will become national law upon Brexit [2], this section sets out both the relevant EU Regulations and EU Directives.

(a) The General Data Protection Regulation

The General Data Protection Regulation (GDPR), Regulation 2016/679 became directly applicable throughout the EU as of May 25, 2018, without requiring implementation by the EU Member States through national law. However, there are more than 30 areas covered by the GDPR where Member States are permitted to legislate differently in their own domestic data protection laws. Member States will also need to amend their existing laws to rectify any conflicts with the GDPR.

The GDPR extends the scope of responsibilities for both data controllers and processors including on cyber security, with new obligations in relation to data security, data breach notification and the requirement to appoint a data protection officer in certain circumstances. The GDPR also enhances the regime for enforcement to include the risk of fines at up to 4% of an organization's worldwide annual turnover.

The GDPR has extraterritorial effect, although there is still some uncertainty as to how and to what extent the GDPR will be enforced outside the EU. The GDPR applies to any organization outside the EU that processes personal data of individuals in the EU in connection with offering goods or services to such individuals or monitoring their behavior.

- **General GDPR Principles relating to processing of personal data**

In terms of general personal data[29] handling obligations, Articles 5(1) (a)-(e) of the GDPR impose broad obligations on controllers by requiring them to ensure that personal data must be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purpose(s);
- Accurate and, where necessary, kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed.

- **GDPR "Security" Principle**

In addition, the GDPR's fundamental "*security principle*", Article 5(1) (f), which is of principal importance for cyber security purposes, provides that personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organizational measures.
The UK regulatory authority, the Information Commissioner's Office ("**ICO**"), considers[30] that this principle requires the following steps to be undertaken:

- consider things like risk analysis, organisational policies, and physical and technical measures;
- take into account additional requirements about the security of your processing – and these also apply to data processors.

[29] Personal data is defined under GDPR as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

[30] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/

- consider the state of the art and costs of implementation when deciding what measures to take – but they must be appropriate both to your circumstances and the risk your processing poses.
- where appropriate, you should look to use measures such as pseudonymisation and encryption.
- your measures must ensure the 'confidentiality, integrity and availability' of your systems and services and the personal data you process within them.
- the measures must also enable you to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.
- you also need to ensure that you have appropriate processes in place to test the effectiveness of your measures, and undertake any required improvements.

- **Other relevant GDPR provisions**
  - **Automated processing (Article 22)**

The GDPR provides for the right for data subjects not to be subject to automated decision making, including profiling. The scope of this right is potentially extremely broad and may throw into question legitimate profiling to detect fraud and cybercrime. This is an area where further guidance is needed on how Article 22 will be applied to specific types of profiling.

- **Notification of personal data breaches (Articles 33 & 34)**

The GDPR also imposes mandatory notification obligations for personal data breaches where such breaches are likely to result in a risk to the rights and freedoms of natural persons. In determining whether such a risk arises, the European Data Protection Board's Guidelines on personal data breach notification[31] are the principal source of guidance.

Where such a report requires to be made it must be submitted to the ICO by the relevant Data Controller within 72 hours of awareness. In most cases, notification will also require to be made to affected data subjects without undue delay.

(b) The Privacy and Electronic Communications (E-Privacy) Directive

The E-Privacy Directive (2002/58/EC), as amended by Citizens' Rights Directive (2009/136/EC), requires telecom operators and Internet service providers to manage risks to their networks and report significant breaches of security or network integrity; it also imposes restrictions on such providers processing of billing and traffic data. Additionally, the revised E-Privacy Directive (2009/136/EC) requires that when a personal data breach[32] occurs, the provider must report the breach to the relevant national authority. The provider must inform affected subscribers directly when the breach is likely to adversely affect personal data or privacy.

However, please note that it is expected that the e-Privacy Directive will be replaced by the e-Privacy Regulation during late 2019 / early 2020 (see below).

(c) The Framework Directive

Under the Directive on a common regulatory framework for electronic communications

[31] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

[32] Defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community"

networks and services (Framework Directive) (2002/21/EC), operators providing public communications networks or electronic communications services must ensure the security of the networks. The competent national regulatory authority must be informed of any breach of security or loss of integrity in the network. That authority will in turn inform the national regulatory authority of the other Member States. To protect network security, the national regulatory authorities have the power to issue binding instructions to undertakings providing communication networks.

(d) The Network and Information Security Directive (also known as the Cybersecurity Directive or NIS Directive)

The Directive on security of network and information systems (2016/1148/EC) (the "**NIS Directive**") requires operators of essential services (OES) (such as energy, health, water supply, transport and digital infrastructure) but also certain digital services providers (DSP) (such as online marketplaces, online search engines and cloud computing services) to adopt appropriate steps to ensure that they are resilient to cyber-attacks and mechanisms to report serious incidents to the national competent authorities.

Member States are required to identify operators of essential services from the above sectors using criteria such as: whether the service is essential for society and the economy; whether it depends on network and information systems; and whether an incident could have significant disruptive effects on its provision.

Increased cooperation across Member States on these matters is encouraged through the development of a strategic cooperation group to exchange information and best practices, manage cross border incidents, develop guidelines and coordinated responses and assist each other in cyber security capacity building.

The NIS Directive was adopted by the European Parliament on July 6, 2016, and entered into force in August 2016. EU member states had until May 2018 to implement the NIS Directive into their national laws and 6 months more to identify operators of essential services.

(e) Directive on European Critical Infrastructures

The Directive on European Critical Infrastructures (2008/114/EC) of December 8, 2008 (on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection) mandates that Member States identify and designate European critical infrastructure located in their territory.

Each critical infrastructure operator must develop a security plan to prevent, mitigate and neutralize the risks of service interruption and infrastructure destruction. This directive also requires operators of critical infrastructures to cooperate with the government, exchange information and comply with inspections and instructions from the government of their Member State.

(f) Export Controls

If security technology relative to cyber security qualifies as “military goods” or as “dual-use goods” (goods that can be of military as well as another type of use), then they also are subject to a number of EU and national rules and regulations.

For example, EU Regulation No. 388/2012 requires a number of categories of dual-use goods (including software and technology) to be subject to controls when they are exported from or in transit through an EU Member State.

One of these categories (category 5: Telecommunications and information security and subcategory 5A002: information security systems, equipment and components) includes encryption technology. The goods in category 5A002 may not be exported (or even transported) through the EU without a licence. At the EU level, there are no import or deployment restrictions on encryption technology.

- **UK legislation**

(g) Data Protection 2018

The Data Protection Act 2018 (DPA 2018) repeals and replaces the old Data Protection Act 2008 and, in preparation for Brexit, incorporates the GDPR (referred to at (a) above) into UK law and it is designed to ensure that the UK will be able to exchange personal data freely with the EU post-Brexit. In addition, unlike the GDPR, the DPA 2018:

- Applies to processing of personal data for intelligence services;
- Extends the GDPR standards to additional types of processing not covered by the GDPR and EU law, such as the processing of unstructured manual files by public authorities; and
- Consolidates data protection enforcement increasing the maximum fines in accordance with the GDPR and also introducing two new criminal offences (re-identification of the de-identified personal data and alternation of personal data to prevent disclosure). [3]

(h) Privacy and Electronic Communications (EC Directive) Regulation 2003

The UK Privacy and Electronic Communications (EC Directive) Regulations (PECR) (2003/2426), as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (SI 2011/2018), implemented the E-Privacy Directive (as amended and referred to at (b) above) into UK law.

The Regulations include a requirement for public electronic communication network (PECN) providers and public electronic communication service (PECS) providers to take appropriate technical and organizational measures to safeguard the security of that network and service. It also imposes restrictions on such providers processing of billing and traffic data.

In particular, PECS must:

- Ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;
- Protect personal data stored or transmitted against:
  - Accidental or unlawful destruction;
  - Accidental loss or alteration; and
  - Unauthorised or unlawful storage, processing, access or disclosure.
- Ensure the implementation of a security policy regarding the processing of personal data. [4]

Measures shall be considered appropriate if, having regard to the state of technological developments, and the cost of implementing them, they are proportionate to the risks against which it would safeguard.

Where, despite taking the above measures, a personal data breach occurs:

- The PECS must notify that breach to the ICO satisfying the requirements contained in the Notification Regulation (611/2013); and
- If the breach is likely to affect the personal data or privacy of a subscriber or user, the provider must inform the relevant subscribers of:

- The nature of the risk;
- The consequences of the breach; and
- The measures taken or proposed to be taken by the provider to address the breach. [5]

The notification to subscribers will not be required where the PECS has demonstrated to the satisfaction of the ICO that it has implemented appropriate technological protection measures which render the data unintelligible to any person who is not authorised to access it, and that those measures have been applied.

Like the GDPR, the PERC also has extra-territorial effects where foreign businesses act as providers of a PECN and/or PECS. PECS providers will also be subject to obligations under the Notification Regulations (regardless of where the business is based) in respect of their activities as a PECS provided within the UK. [6]

(i) Communications Act 2003

The UK Communications Act (CA 2003)[33], in particular articles 105A to 105D, implements European directives that govern the provision of electronic communications networks and services in the UK, including the Framework Directive (referred to at (c) above) and includes requirements related to managing the security and availability of networks and services.

Section 105A of the CA 2003 provides that PECN providers and PECS providers must take technical and organisational measures appropriately to manage risks to the security of the PECN and PECS. [7] These measures include those to prevent or minimise the impact of security incidents on:

- End-users; and
- Interconnection of PECNs.

In addition, PECN providers must take all appropriate steps to protect, so far as possible, the availability of the provider's PECN.

The CA 2003 also imposes reporting obligations on PECN, such that a PECN must notify Ofcom (the UK telecommunications regulator) of:

- A breach of security that has a significant impact on the operation of a PECN or the operation of a PECS; and
- A reduction in the availability of a PECN that has significant impact on the network. [8]

Where Ofcom receives a notification, Ofcom will (when appropriate) notify:

- The national regulatory authorities in another Member States and the European Network and Information Security Agency (ENISA);
- The public or require the PECN provider or the PECS provider to do so.

Again, the CA 2003 also has extraterritorial effect in that it applies regardless where the PECN and/or the PECS providers are based in respect of their activities within the UK. [9]

(j) The Network and Information Systems Regulations 2018 (NIS Regulations)

The Network and Information Systems Regulations 2018 (as amended) implement the

[33] As at December 2018, the official government link to this piece of legislation does not currently show all the amendments. For an updated copy showing all changes, please contact us.

NIS Directive (referred to at (d) above) into UK national law, requiring operators of essential services (such digital infrastructure) and certain providers of digital services (online marketplaces, online search engines and cloud computing services) to adopt appropriate steps to ensure that they are resilient to cyber-attacks and mechanisms to report serious incidents to the national competent authorities. They have potential impact on businesses that rely on IT systems in the following sectors:

- Energy, transport health drinking water supply and distribution, digital infrastructure (OESs); and
- Online marketplaces, online search engines and cloud computing services (DSPs).

The NIS Regulations focus on IT systems of OESs and DSPs and impose security and incident reporting requirements and provide for high penalties (with a maximum fine of £17 million) in the event of non-compliance. [10]

(k) Computer Misuse Act 1990

The Computer Misuse Act 1990, as amended by the Police and Justice Act 2006, criminalizes unauthorized access to computer systems. [11]

(l) Regulation of Investigatory Powers Act 2000 (RIPA)

RIPA establishes the criminal offense of unauthorized interception of an electronic communication across public networks. [12] It also regulates the use of covert techniques by public authorities to ensure that private information is obtained, including by way of interception of communications, with proper authority in a way that is proportionate and compatible with human rights.

(m) Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, often referred to as the Lawful Business Practice Regulations, set out the circumstances in which persons are authorized to intercept electronic communications for specified business purposes without breaching RIPA. [13]

(n) Anti-Terrorism, Crime and Security Act 2001

The Anti-Terrorism, Crime and Security Act 2001 requires communication providers to retain communications data in accordance with specified codes of practice for the purpose of safeguarding national security or preventing or detecting crime that may relate to national security. [14]

(o) Official Secrets Act 1989

The Official Secrets Act 1989 provides the main legal protection in the UK against espionage and the unauthorised disclosure of certain categories of official information. [15]

(p) Investigatory Powers Act 2016

The Investigatory Powers Act 2016 introduced new powers, and restated existing powers, for UK intelligence agencies and law enforcement to carry out targeted interception of communications, bulk collection of communications data, and bulk interception of communications. [16]

(q) Digital Economy Act 2017

The Digital Economy Act 2017 includes three principal provisions affecting data sharing [17] - namely:

- Public Sector Data Sharing obligations: permitting extensive sharing of personal data between public authorities including water, gas and electricity companies, for service delivery functions;
- Introduction of a Direct Marketing Code: requiring the ICO to consult on and publish a statutory Code of Practice. The Code will contain 'good practice' and not just be limited to compliance with the law; and
- Introducing provisions for the ICO to continue to charge fees for certain functions post 25 May 2018.

- **Soft law**

Although they are not legislative or regulatory measures, there are published standards that are generally accepted as recognised cyber security guidance / standards, many of which and have cyber security implications: [18]

(r) *10 Steps to Cybersecurity*: This 10-step guide to cybersecurity, published by the UK Government's National Cyber Security Centre (part of the UK's Government Communications Headquarters (GCHQ)SG), includes advice on topics such as protecting data both in transit and at rest, scanning all media for malware before importing the media into a corporate system and monitoring and testing security controls. [19]

(s) *Cyber Essentials Scheme*: The UK Government has introduced a scheme which sets out the basic controls that organizations should implement for technical protection from cyber attacks. The scheme also provides an assurance framework through which organizations can obtain two levels of certification: Cyber Essentials and Cyber Essentials Plus. The Cyber Essentials certification is awarded on the basis of a verified self-assessment. The Cyber Essential Plus certification entails a higher level of assurance and involves external testing of an organisation's cyber security approach. [20]

(t) *PCI DSS*: Processors of payment card data should meet the Payment Card Industry Data Security Standards (PCI DSS). [21]

(u) *ISO 27001 and ISO 27002*: These standards are generally accepted as an industry standard framework for security risk management in the UK. [22]

[Forthcoming Legislation and Regulations and Discussions on Future Trends]

Forthcoming legislation

In terms of EU legislation, the E-Privacy Directive (referred to at (b) above) will be replaced by the E-Privacy Regulation, which will then be directly applicable in the territory of all Member States. At the time of writing in December 2018, it is

anticipated that the E-Privacy Regulation will be in final form and come into force at some point in 2019. In its current form, the E-Privacy Regulation focusses on:

- Enhancing security and confidentiality of electronic communications, including "over-the-top" communications - content, services or applications that are provided to the end user over the open internet e.g. VOIP.
- Specific regulation of direct marketing, website audience measurement, the transmission of communications across devices and browsers, and cookies set on users' machines.
- Addressing fragmentation of legislation across Europe (as a Regulation this will be directly applicable, unlike the existing Directive which is implemented by national legislatures at a local level).
- Consistent enforcement of e-Privacy rules by independent supervisory authorities already competent to enforce the GDPR.

In terms of UK legislation, as set out above, 2018 has seen a substantial number of legislative developments that have impacted cyber security. Although the fast-moving pace of cyber security may mean that new legislative developments may be tabled in the near future, there does not appear to be any significant legislative developments affecting cyber security in the pipeline. [23]

Strategy and Trends

The UK Government's current strategy is to pursue a number of new non-regulatory interventions to incentivise better cyber risk management [24] , in support of the existing business engagement strategy. These interventions will mostly likely be delivered through the National Cyber Security Centre (the UK authority on cyber security environment), providing advice and guidance to organisations and incentivising them to improve their cyber security risk management. [25]

The UK Government has published a National Cyber Security Strategy for the years 2016-2021 (the Strategy). The Strategy states that the UK Government will:

- Invest £1.9 billion in "*defending the UK systems and infrastructure, deterring adversaries, and developing a whole-society capability*".
- Pursue international action and exert influence by investing in partnerships that shape the global evolution of cyberspace. This will be done both bilaterally and multilaterally including through the EU, NATO and the UN.
- Intervene more actively and use increased investment, while continuing to support market forces to raise cyber security standards across the UK. The UK Government will also have measures to intervene to drive improvements that are win the national interest, particularly in relation to the cyber security of the UK critical national infrastructure (for more details please see section 2(b) below).
- Ensure that the Armed Forces are resilient and have the strong cyber defences they need to secure and defend their networks and platforms.
- Use the authority and influence to invest in programmes to address the shortage of cyber security skills in the UK, from schools to universities and across the workforce.

- Launch two new cyber innovation centres to drive the development of cutting-edge cyber products and dynamic new cyber security companies.
- Draw on its capabilities and those of industry to develop and apply Active Cyber Defence (ACD) measures to significantly enhance the levels of cyber security across UK networks. In pursuing an ACD, the UK will (among other) work with industry, especially Communications Service Providers (CSPs), to make it significantly harder to attack the UK internet services and users, and greatly reduce the prospect of attacks having a sustained impact on the UK. This will include the UK Government undertaking specific actions such as:
    - Working with CSPs to block malware attacks. This will be done by restricting access to specific domains, IP addresses or websites that are known sources of malware. This is known as Domain Name System (DNS) blocking/filtering.
    - Preventing phishing activity that relies on domain 'spoofing' (where an email appears to be from a specific sender, such as a bank or government department, but is actually fraudulent) by deploying an email verification system on government networks as standard and encouraging industry to do likewise.
    - Promoting security best practice though multi-stakeholder internet governance organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN) which incorporates the domain name system, the Internet Engineering Task Force (IETF) and the European Regional Internet Registry (RIPE) and engagement with stakeholders in the UN Internet Governance Forum (IGF).
    - Working with law enforcement channels in order to protect UK citizens from being targeted in cyber-attacks from unprotected infrastructure overseas.
    - Working toward the implementation of controls to secure the routing of internet traffic for government departments to ensure that it cannot be illegitimately re-routed by malicious actors.
    - Investing in programmes in the Ministry of Defence, the National Crime Agency and the Government Communications Head Quarters that will enhance the capabilities of these organisations to respond to, and disrupt, serious state-sponsored and criminal cyber activity targeting UK networks.
- Build a more secure internet, which will reduce cyber-crime in the UK. This will be done by ensuring that hardware and software providers sell online products and services with the security settings activated by default. The Government will also invest in technologies like Trusted Platform Modules and emerging industry standards such as Fast Identity Online, which do not .rely on passwords for user authentication, but use the machine and other devices in the user's possession to authenticate. [26]

References:

Legislation

(a) EU Legislation

- General Data Protection Regulation (EU) 2016/679: *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.*
- Privacy and Electronic Communications Directive 2002/58/EC, as amended by Citizens' Rights Directive 2009/136/EC: *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.*
- Framework Directive 2002/21/EC: *Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications and services (Framework Directive).*
- Directive (EU) 2016/1148 on security of network and information systems *(NIS): Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.*
- Directive on Critical Infrastructures 2008/114/EC: *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.*
- Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, as amended by Regulation (EU) No 388/2012

(b) UK Legislation

- Data Protection Act 2018
- Privacy and Electronic Communications Regulation (PECR) 2003 (SI 2003/2426) (original), as amended by The Privacy and Electronic Communications (Amendment) Regulations 2018 (SI 2018/1189)
- The Network and Information Systems Regulations 2018 (NIS Regulations) (SI 2018/506), as amended by The Network and Information Systems Regulations 2018 (SI 2018/506)
- Communications Act 2003
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000 (RIPA)

- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.
- Anti-Terrorism, Crime and Security Act 2001
- Official Secrets Act 1989
- Investigatory Powers Act 2016
- Digital Economy Act 2017
- Human Rights Act 1998

Government Documents

- Cyber Security Regulation and Incentives Review (December 2016).
- National Cyber Security Strategy 2016 to 2021.

Public bodies' Guidance, Standards

- PCI DSS: Payment Card Industry Data Security Standards.
- ISO 27001 and ISO 27002.
- Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003: https://www.ofcom.org.uk/__data/assets/pdf_file/0021/51474/ofcom-guidance.pdf
- The National Cyber Security Centre guidance: 10 Steps to Cyber Security: https://www.ncsc.gov.uk/guidance/10-steps-cyber-security
- Cyber Essentials, issued by The National Cyber Security Centre: https://www.cyberessentials.ncsc.gov.uk/

2 Details of your jurisdiction's cyber security-related regulations relevant to procurement of goods in the following sectors

(a) Government (national security, defense, police, fire station, tax, academic research, etc.)

[Existing Legislation and Regulations]

A number of pieces of legislation govern the laws a company in a procurement supply chain in the UK must comply with in respect of both cybersecurity and the protection and proper handling of data. The bedrock of legislation in this area is the Network and Information Systems Regulation 2018 and the Data Protection Act 2018. [27]

In addition, the UK Government has in recent years published numerous guidelines on how companies can follow best practice on cyber-security regulations. Some of these are mandatory for suppliers to government, others may simply be advisable to follow while tendering for such work.

(1) **UK Legislation and Guidelines**

The Network and Information Security Directive (also known as the Cybersecurity Directive or NIS Directive) (detailed at paragraph (d) in section 1

of this summary) as implemented into the UK by the Network and Information Systems Regulations 2018 ((j) of Section 1 of this summary)

The NIS applies to two specific groups of organisations:

(i) operators of essential services ("**OES**"), which include Energy, Transport, Health, Water and digital infrastructure; and

(ii) relevant digital service providers ("**RDSPs**").

As it is the responsibility of the OES to implement these laws by ensuring the necessary network and information security protection mechanisms to mitigate risks, thereby protecting the continuance of critical services, it will ultimately not be (as part of this legislation) the legal responsibility of companies supplying along the procurement chain to do so. A company seeking to contract with government along any part of the supply chain would do well to ensure that compliance with the NIS Regulations (wherever relevant) is part of their security regime however.

The NIS relates to 'incidents' that have a significant impact on the continuity of the essential service which that OES provides. This means whilst it is primarily intended to be a cybersecurity law, it does have wider implications for OESs and RDSPs.

The principal requirement is contained in Regulation (NIS Regulations 2018) 12(1), which requires RDSPs to: "identify and take appropriate and proportionate measures to manage the risks posed to the security of network and information systems". [28]_

These measures are further set out in Regulation 12(2), and require RDSPs to:

(i) ensure a level of security appropriate to the risk posed;

(ii) prevent and minimise the impact of incidents affecting digital services; and

(iii) take account of the requirements contained in EU Regulation 2018/151

Included amongst those things envisioned by Regulation 12(2) is that the RDSP must take into account the following elements specified in Article 2 of EU Regulation 2018/151:

(i) the security of systems and facilities;

(ii) incident handling;

(iii) business continuity management;

(iv) monitoring auditing and testing; and

compliance with international standards.

(2) "Cyber Essentials"

In September 2014 the Government mandated new cyber security standards for its suppliers in the form of a set of "Cyber Essentials" which all suppliers must comply with if they are bidding for certain government contracts. [29]

The "Cyber Essentials" are relevant to suppliers bidding for government contracts which involve the handling of sensitive or personal information, as well as the provision of certain technical products and services.

The scheme contains a set of five critical controls, which are: (i) secure your devices and software, (ii) secure your internet connection, (iii) control access to your data and services, (iv) keep your devices and software up to date, and (v) protect from viruses and other malware.

The scheme is run by the National Cyber Security Centre (NCSC).

(3) NCSC's Ten Steps

NCSC, which forms part of GCHQ, published guidance in the form of "10 Steps to Cyber Security" in August 2016. This is intended to be guidance for executive/board level staff, and includes 10 technical advice sheets that companies should consider putting in place.

These 10 steps include advice sheets for: (i) Risk Management Regime, (ii) Secure Configuration, (iii) Network Security, (iv) Managing User Privileges, (v) User Education and Awareness, (vi) Incident Management, (vii) Malware Prevention, (viii) Monitoring, (ix) Removable Media Controls, and (x) Home and Mobile Working. [30]

(4) Data Protection Regulation

All companies which are part of a supply chain to Government (alongside all other data processors in the UK) must comply with the requirements of the GDPR (as set out at (a) in section 1 of this summary), and the Data Protection Act 2018 (as set out at (g) in section 1 of this summary) which implements the provisions of the GDPR into the UK.

This is the main legislative test of cyber hygiene in the UK, and companies can face fines from the regulatory body ICO for non-compliance with the regime. [31]

[Forthcoming Legislation and Regulations and Discussions on Future Trends]

(1) UK Developments

A review was undertaken by the Government during 2016 of Cyber Security Regulation and Incentives.

The review report, published in December 2016, recognizes that the GDPR (as implemented in the UK by the Data Protection Act 2018) would be "*key to ensuring strong organizational data protection regimes supported by strong cyber security*". The report confirmed that for the time being, "*the Government will not seek to pursue further general cybersecurity regulation for the wider economy over and above the GDPR*".

The review focused on initiatives in respect of general education and awareness. These were to be implemented by relevant regulatory organisations such as the National Cyber Security Centre (NCSC).

Critical Infrastructure was ruled out of the remit of this review [32]; for current legislation and future developments in which please see the section below in this report.

(2) EU Developments

On September 13 2017, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy published a Joint Communication to the European Parliament and the Council of the European Union on "*Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*".

Part of this approach was a proposal to introduce a new "Cybersecurity Act", which would give the EU Cybersecurity Agency a permanent mandate, as well as set up an EU certification framework with ENISA in a central role. That framework would define the procedure for the creation of voluntary EU cybersecurity certification schemes. The ultimate aim is to reduce the financial cost for businesses who need to undertake a number of certification processes when conducting business across the EU.

References:

Legislation

The Network and Information Systems Regulations 2018 (NIS Regulations) (SI 2018/506), as amended by The Network and Information Systems Regulations 2018 (SI 2018/506).

General Data Protection Regulation (EU) 2016/679: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural

persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Data Protection Act 2018.

Government Guidance

Cyber Essentials Scheme: Overview, HM Government, April 2014 (on 16 January 2018).

Government mandates new cyber security standard for suppliers, HM Government, September 2014.

Cyber Security Regulation and Incentives Review, December 2016.

NCSC's Ten Steps, August 2016.

The European Commission and the High Representative of the Union for Foreign Affairs and Security Policy published a Joint Communication to the European Parliament and the Council of the European Union on "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", September 2017.

(b) Critical infrastructure (telecommunication, electricity, transport, etc.)

[Existing Legislation and Regulations]

EU Legislation:

As set out at (e) in section 1 of this summary, at EU level, the Directive on European Critical Infrastructures (2008/114/EC) of December 8, 2008 provides that each critical infrastructure operator must develop a security plan to prevent, mitigate and neutralize the risks of service interruption and infrastructure destruction. This obligation arguably includes the Critical Network infrastructure ("**CNI")** operator's obligation to manage cyber risks with their suppliers.

UK Legislation:

The NIS Regulations (referred to at (j) in section 1 of this summary) set an expectation that CNI operators in the five NIS sectors (energy, transport, heath, drinking water and digital infrastructure) will ensure that "*appropriate measures are employed where third party services are used.*" [33] These include "*contractual agreements*" (for example auditing rights and key performance indicators) and specified "security properties" for products and services which on "the essential service depends".

However, it is incumbent on CNI operators to examine their supply chains, undertake an appropriate risk assessment and implement controls accordingly. [34] Indeed, under the NIS Regulations an OES is responsible for ensuring that the relevant security requirements are met regardless of whether the organization or a third party delivers the service. The OES is responsible for driving compliance.

Soft law

From 1 October 2014, like the rest of bidders in a public procurement process in respect of government contracts involving the handling of certain sensitive and personal information, CNI operators must comply with the Cyber Essentials. In addition, CNI operators are expected to implement advanced cyber security measures:

- Encryption - sensitive data can be stored or transmitted in a form that is un-readable without a digital key;
- Integrity checking - system files can be checked against previous records to detect changes and identity attacks;

- Network monitoring - detecting suspicious behavior such as a user accessing many separate parts of a network or transferring lots of data, can be an early warning of an attack;
- Penetration testing - conducting controlled cyber-attacks on systems can test their defences and identify their vulnerabilities.
- Security by design - systems can be designed to perform narrowly defined actions and only accept instructions from verified sources, and networks can be designed to minimize the impact of a single failure.
- Disconnection - the most critical systems can be disconnected from networks or replaced with non-digital systems. [35]

When dealing with suppliers, it is recommended that CNI operators, in particular OES, set and communicate minimum security requirements to the suppliers. [36]

[Forthcoming Legislation and Regulations and Discussions on Future Trends]

The UK Government is stepping up cyber security requirements for its direct suppliers, having announced in June 2018 that it will write minimum standards into its contracts and create the equivalent to a 'credit rating' for each of its prime suppliers. [37]

Despite the above, Members of the UK Parliament (MPs) have recently called for a cyber security minister to defend CNI. This followed a report issued by the Joint Committee on National Security Strategy on UK's CNI (Joint Committee Report on CNI), which highlighted the threat to the UK's CNI is both growing and evolving. [38]

The report acknowledges (at paragraph 73) that "*a more holistic and effective approach to strengthening the cyber resilience of CNI requires changing the culture of the CNI operators and their extended supply chains.* [39] *Embedding the view that cyber risk is another business risk, which must be proactively managed, will be central to this process. It is especially important for those private-sector operators whose commercial interests may not always align with the demands of national security.*"

The Joint Committee Report on CNI recommends the Government to give urgent consideration to non-regulatory incentives and interventions that have the potential to drive cultural change across CNI sectors, establishing an environment in which continual improvement is encouraged. [40] These incentives and interventions should include how to mange cyber risk through and within the extended supply chains of CNI operators.

In order to deal with the difficulty that CNI operators are facing of :

- Mandating and enforcing minimum security standards for hardware, software or services bought 'off the shelf', especially when they are procured from major international companies, it has been recommended that the Government should use its "buying power" and diplomatic presence in multinational forums such as the G7 to influence international providers, and potentially establish NCSC-accredited 'kitemark' (a voluntary labelling scheme for consumers)for trusted suppliers; and
- Facing a widespread use of certain data service providers, software packages, computer processors and hardware, which creates "single points of failure" that could affect operators simultaneously across CNI sectors, it has been recommended

that the Government should proactively identify these potentials points of failure and prepare mitigation and contingency plans. [41]

References:

Legislation

(a) EU Legislation

- Directive on Critical Infrastructures 2008/114/EC: *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*.

(b) *UK Legislation*

- The Network and Information Systems Regulations 2018 (NIS Regulations) (SI 2018/506), as amended by The Network and Information Systems Regulations 2018 (SI 2018/506).

Government Releases

- Cyber Essentials Scheme: Overview, HM Government, April 2014 (on 16 January 2018).
- Government mandates new cyber security standard for suppliers, HM Government, September 2014.

Guidance, reports and other

- Annual Report 2016, A report to the National Security Adviser of the United Kingdom, Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board, May 2016.
- Cyber Security on UK Infrastructure, Houses of Parliament, PostNote, 554, May 2017.
- Guidance Supply chain security collection, by NCSC, January 2018.
- Security of UK Telecommunications, Houses of Parliament, PostNote no. 584, August 2018.
- Guidance on supply chain, by NCSC, April 2018.
- Minimum Cyber Security Standards, June 2018.
- The NCSC highlighted the issue of supply chain security in its 2018 Annual Review, stating that it had become "*acutely conscious of the role the supply chain plays in leaving organisations vulnerable to compromise*"". NCSC, "Annual Review 2018", October 2018, page 11.
- Report on cyber Security of the UK's critical national infrastructure by the Joint Committee on the National Security Strategy, November, 2018.

Press releases

- *"Spectre and Meltdown processor security flaws—explained"*, The Guardian, 4 January 2018.
- "*MPs call for a cyber security minister to defend critical infrastructure*", Computerworld UK, November 19, 2018.

(c) Equipment or services for consumers

[Existing Legislation and Regulations]

The UK has traditionally had strong consumer protection laws, and therefore the Government has taken an active interest in cybersecurity in respect of equipment to be provided to consumers. In particular, the Government has recently produced a report and a code of practice on consumer IoT aimed at different groups along the supply chain. [43]

The Code of Practice for Consumer IoT, October 2018

The Government Department for Digital, Culture, Media & Sport published a Code of Practice for Consumer IoT Security in October 2018. This is described as *"[bringing] together, in thirteen outcome-focused guidelines, what is widely considered good practice in IoT security*", and has been produced in conjunction with the National Cyber Security Centre (NCSC). The code is available in all main world languages.

The codes are marked by different audiences with different guidelines applicable to each, these audiences are: (i) device manufacturer, (ii) IoT Service Providers, (iii) Mobile Application Developers, and (iv) Retailers. It therefore applies at all stages of the product lifecycle, including the supply of IoT devices.

The first three guidelines are those which are stated to be the most important as they will have the most immediate results, with the other guidelines having more of an impact across the supply chain. The most significant guidelines are therefore: (i) no default passwords, (ii) implement a vulnerability disclosure policy, and (iii) keep software updated. [44]

These are only guidelines for best practice without binding effects in law, but in that sense they can be seen as indicative of the sort of trends which may eventually be given more stringent protection in legislation. A number of the recommendations are aligned with the EU's GDPR and the UK's Data Protection Act 2018.

Given that it is unclear how the ICO will enforce this regime in relation to the IoT, in designing, producing and supplying IoT products and services to consumers it would be prudent for an engaged company to take note of these guidelines as best practice when operating in the UK. [45]

The GDPR as introduced into the UK by the Data Protection Act 2018

It is the inherent nature of IoT systems and often consumer devices that they will process consumer data. As such any organization processing this data in respect of IoT devives (alongside all other data processors in the UK) must comply with the requirements of the GDPR (as summarized at (a) in section 1 of this summary), and the Data Protection Act 2018 [46] (as summarized at (g) in section 1 of this summary) which implements the provisions of the GDPR into the UK.

This is the main legislative test of cyber hygiene in the UK, and companies can face fines from the regulatory body ICO for non-compliance with the regime. [47]

[Forthcoming Legislation and Regulations and Discussions on Future Trends]

UK Developments

There has been an increased focus on the risk unsecured IoT devices and applications pose to consumers both as an EU and UK level in recent years, with a general understanding that the current crop of regulation may not be current enough to capture IoT devices. [48]

The Government produced a report this year titled "Secure by Design: Improving the cyber security of consumer Internet of Things". This report explores the regulatory options available and notes that the Government is consulting on how certain provisions of the Code of Practice for Consumer IoT Security outlined above can be given regulatory footing. It notes in this sense that the parts of the Code relating to data protection are already given legal weight by the Data Protection Act 2018.

In that sense a supplier can look to the for Consumer IoT Security to get a sense of where future regulatory developments will lead in the UK. [49]

In addition, the Government is currently in the process of producing a Consumer Green Paper. It is anticipated that this will include provisions in relation to cybersecurity in areas where the UK's consumer protection laws are outdated or not fit for purpose. [50]

EU Developments

ANEC (the European Association for the Co-Ordinartion of Consumer Representation in Standardisation) and the BEUC (The European Consumer Organiation) published a report titled "Cyber security for connected products" in March 2018.

This report highlights the weakness of current legislation: "today, most of the connected devices available in the EU's Single Market are designed and manufactured without the most basic security features embedded in the software". It goes on to put a series of recommendations forward to the European Commission, including a minimum set of security measures to be obligatory for all connected products as a condition for putting them on the market. This would include encryption, software updates and strong authentication methods.

References:

Legislation

General Data Protection Regulation (EU) 2016/679: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Data Protection Act 2018.

Guidance

Code of Practice for Consumer IoT Security, October 2018.

Department for Digital, Culture Media and Sport "Secure by Design" Report, 2018.

ANEC / BEUC Position Paper on Cybersecurity for Connected Products, March 2018.

b. 法律事務所を通じた Q&A

9. The Data Protection Act 2018 (DPA 2018) repeals and replaces the old Data Protection Act 2008 and, in preparation for Brexit, incorporates the GDPR (referred to at (a) above) into UK law and it is designed to ensure that the UK will be able to exchange personal data freely with the EU post-Brexit. In addition, unlike the GDPR, the DPA 2018:

・Applies to processing of personal data for intelligence services;

・Extends the GDPR standards to additional types of processing not covered by the GDPR and EU law, such as the processing of unstructured manual files by public authorities; and

・Consolidates data protection enforcement increasing the maximum fines in accordance with the GDPR and also introducing two new criminal offences (re-identification of the de-identified personal data and alternation of personal data to prevent disclosure).

の下線部について、

I. intelligence services の定義は何か？
   - ✓ Ans: It is defined as the UK's Security Service (also known as MI5), Secret Intelligence Service (also known as MI6) or the Government Communications Headquarters. [51]

II. unstructured manual files by public authorities とは、具体的に何か？
   - ✓ Ans: For example, files containing handwritten notes. [52] （注: manual files とは、いわゆる「マニュアル」のことではなく、データとして自動的に整理されていない状態で（手動で）管理されている手書きの書類等を指す。）

10. The Regulations include a requirement for public electronic communication network (PECN) providers and public electronic communication service (PECS) providers to take appropriate technical and organizational measures to safeguard the security of that network and service. の下線部について、

III. PECN （provider）に含まれる代表的な組織・企業は何か？
   - ✓ Ans : A PECN is defined as an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public. Examples of PECNs include transmitters or transmission plus associated equipment, software and stored data used to convey electronic signals (including sounds, images or data of any description). This could be a wired or a wireless network – for example, any provider of a network of phone cables or a mobile phone network. [53] This would include providers of commercial broadband internet or mobile phone infrastructure. The UK ICO considers that the network ends at the customer's point of connection (eg their master phone socket), so any equipment installed by a customer (eg wi-fi routers) does not form part of a relevant network.

IV. PECS（provider）に含まれる代表的なサービスは何か？
   - ✓ Ans: A PECS is defined as any electronic communications service that is provided so as to be available for use by members of the public. The UK ICO considers this to be any service that members of the public can sign up to in

order to send or receive electronic signals (including sounds, images or data of any description) – for example, a phone contract or internet connection. [54] This does not include a 'content service' that provides or edits the actual content of signals – for example, a broadcast service or an online news service. A service provider of PECS is considered to be someone who provides any service allowing members of the public to send electronic messages. This includes telecoms providers and internet service providers. Some service providers will operate their own network, but those using a network managed by a third party are also covered. In the UK ICO's view, businesses offering wi-fi access to customers as a supplementary service are not service providers. A service provider would generally have a formal and ongoing contract with the customer subscribing to the service. By contrast, a coffee shop or hotel that provides wi-fi will itself be a subscriber to a service, and is simply permitting passing customers to use its connection.

11. Cyber Essentials Scheme: The UK Government has introduced a scheme which sets out the basic controls that organizations should implement for technical protection from cyber attacks. The scheme also provides an assurance framework through which organizations can obtain two levels of certification: Cyber Essentials and Cyber Essentials Plus. The Cyber Essentials certification is awarded on the basis of a verified self-assessment. The Cyber Essential Plus certification entails a higher level of assurance and involves external testing of an organisation's cyber security approach.

の下線部について、

V. 国内企業・外資系企業の違いにより、Cyber Essentials/Cyber Essentials Plus の認証の取得の難易度は異なるのか？

- ✓ Ans: There is no difference in certification requirements or process for UK companies as opposed to non-UK companies. The only hurdle that may exist, in respect of obtaining certification, would be that if the company has offices external to the UK the IT requirements of that office would also have to meet the requirements. [55] There may be issues with company set up etc. but there are no separate certification requirements for non-UK companies.

VI. 現在時点における Cyber Essentials・Cyber Essentials Plus のそれぞれの取得企業数の数はどれだけか？

- ✓ Ans: As of 1 January 2019, there are a total of 22,000 certificates issued (at the time of writing, unfortunately, there is no breakdown available between Cyber Essentials / Cyber Essentials Plus). This is a marked increase from 1 January 2018, at which time a total of 12,000 certificates were issued (comprising 9,500 Cyber Essentials and 2,500 Cyber Essentials Plus). [56]

12. However, it is incumbent on CNI operators to examine their supply chains, undertake an appropriate risk assessment and implement controls accordingly. Indeed, under the NIS Regulations an OES is responsible for ensuring that the relevant security requirements are met regardless of whether the organization or a third party delivers the service. The OES is responsible for driving compliance.

の下線部について、OES（Operators of Essential Services）との違いは何か？

- ✓ Ans: In most instances, an OES would be anticipated to likely also be considered by Government to be a CNI operator. [57]

13. イギリスにおける“Critical Infrastructure”の定義は何か？

✓ In the UK, there are 13 national infrastructure sectors: Chemicals, Civil Nuclear Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water. Several sectors have defined 'sub-sectors'; Emergency Services for example can be split into Police, Ambulance, Fire Services and Coast Guard.

Among these national infrastructure sectors, the UK government's official definition of Critical National Infrastructure is:

'Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

a) Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or

b) Significant impact on national security, national defence, or the functioning of the state.' [58]

References:

- https://www.cpni.gov.uk/critical-national-infrastructure-0

14. イギリスにおける、（ⅰ）政府調達、（ⅱ）通信インフラ・重要インフラの調達、及び（ⅲ）コンシューマー向け機器・サービスにおいて、違反として摘発された事例または排除された事例はないか？

✓ Ans:

The UK Government has, of late, been proactive in stepping in to restrict the ability of companies to be awarded, or considered for, Government contracts where they have exhibited irresponsible behavior.

One such example of this relates to a company called G4S Security. They are the providers of security services and were the successful bidder in relation to a government contract to provide electronic tagging ankle bracelets for offenders. G4S were found to have overcharged the Government by creating phantom offenders and thus inflating the number of orders required. Once this was exposed, the Government were quick to ban G4S from bidding on public contracts. Ultimately, G4S ended up paying the Government £109 million before they were allowed to bid on contracts again.

It is worth noting, however, that G4S have subsequently been awarded a Government contract in relation to the supply of tagging services, despite an ongoing Serious Fraud Office investigation.

Recently, and following upon the collapse of Carillion, who were the UK's second largest construction company, the Government has announced that it will take a tough stance on companies who do not have "robust procedures" in place to ensure the timely payment of subcontractors under government awarded contracts. Carillion were the UK's second largest construction company that recently entered liquidation with debts in the region of £1.5 billion. Amongst other projects, Carillion held a great number of Government contracts and their collapse has left a great number of third party contractors facing non-payment of invoices. The UK Government is taking action and is expected to introduce the Prompt Payment Initiative that is set to ensure that the government only does business with companies who pay their suppliers on time. The initiative is thought to include provision to exclude suppliers who fail to show fair and effective payment of subcontractors. It is therefore thought that a history of

prompt payment of third party invoices will require to be exhibited when tendering for Government awarded contracts.
There is an indication from the UK Government that they will take enforcement action against companies who do not act responsibly when applying for, or acting under, a Government contract.

References:

- https://www.bbc.co.uk/news/uk-26541375
- https://publications.parliament.uk/pa/cm201719/cmselect/cmbeis/807/80709.htm
- https://www.gov.uk/government/news/crack-down-on-suppliers-who-dont-pay-on-time
- https://www.gov.uk/guidance/prompt-payment-policy
- https://www.theguardian.com/business/2017/jul/10/g4s-awarded-25m-government-contract-despite-inquiry
- https://www.telegraph.co.uk/business/2018/11/29/outsourcers-could-banned-bidding-government-contracts-late-payments/

5.2.2.4 EU

5.2.2.4.1 国としての全体的な状況(まとめ)

EU の政策動向の概要を表 5-12 に示す。

表 5-12　EU の政策動向（まとめ）

	項目	概要
現状	全体傾向	EU 一般データ保護規則（GDPR）及びネットワークと情報セキュリティ指令（NIS 指令）導入により、欧州全体のサイバーセキュリティの強化中。NIS 指令は、事故時の情報共有等を規定、加盟国に法制度組込を要求。また、サイバーセキュリティ強化に向けた政策パッケージを 2017 年に公表、ENISA の強化とともに EU におけるサイバーセキュリティの認証の枠組み「ICT サイバーセキュリティ認証に関する規則案」を発表した。
	重要インフラの法制度	NIS 指令により、EU 各国に重要インフラを提供する事業者の特定を求めるとともに、サイバーアタックに対する強靭な体制と、事故時の情報共有の手続きを規定している。
	政府調達	EU の政府機関の調達は、DIRECTIVE 2014/24/EU（公共一般）、DIRECTIVE 2014/25/EU（水/エネルギー/運輸/郵便等の公共事業）、DIRECTIVE 2009/81/EU（防衛・安全保障）で規定されている。公共調達では、価格と品質による審査基準に一本化（最低価格方式廃止）するとともに、水道/電気事業に競争的対話手続きを導入。
	認証/認定制度	EU におけるサイバーセキュリティの認証の仕組み「ICT サイバーセキュリティ認証に関する規則案」は 2018 年 12 月に欧州委員会と議会にて合意された。今後導入に向けた具体的な認証のスキームの検討も開始される。
	体制	欧州ネットワーク・情報セキュリティ機関（ENISA）が EU 域内におけるネットワークと情報セキュリティ改善の責任を負い、各種ガイドラインの発効や認証スキームの作成等を行う。2017 年発表のサイバーセキュリティ強化に向けた政策パッケージでは権限強化に向けて「EU サイバーセキュリティ庁」創設（発展）が提言された。
今後	全体的な傾向	2017 年公表のサイバーセキュリティパッケージの検討が進む。特に、EU サイバーセキュリティの認証の仕組み「ICT サイバーセキュリティ認証に関する規則案」は導入に向け認証のスキームの検討が開始されており、これが導入されれば、欧州のサイバーセキュリティはさらに強化される。
	重要インフラの法制度	2017 年に公表されたサイバーセキュリティのパッケージの検討が進むと考えられる。
	政府調達	サイバーセキュリティの認証スキーム検討は、「ワークプログラムの作成」、「認証スキームの作成」、「認証スキームの適用」の順に進められる。同スキームは ENISA を中心に進められ、まずは対象となる製品/サービス/プロセスに関する一時的なリストから作成する。

「EU サイバーセキュリティ戦略（Cybersecurity Strategy of the European Union）」が 2013 年に公表され、EU のサイバーセキュリティに関する動きは活発化してきている。2015 年 4 月発表の「セキュリティに関する欧州の行動計画（The European Agenda on Security）」にて政策・立法措置等がまとめられ、サイバー犯罪が優先課題と位置付けられた。2016 年 8 月には EU では初となるサイバーセキュリティに関する指令である NIS 指令（ネットワークと情報セキュリティ指令: The Directive on Security of Network and Information Systems）が発効された。また、2018 年に、個人情報保護の枠組みである GDPR（一般データ保護規則: General Data Protection Regulation）が発効され、NIS 指令とともに、欧州各国の法制度の中に組み込まれた。重要インフラについては、そのサイバーセキュリティに関して、NIS 指令にて規定されている。

政府調達については、2014 年に EU の政府機関による調達、EU の公共事業を行う事業体が調達を行う際の規定について指令が発効された。防衛・安全保障に関する調達については上記の指令とは別に指令が定められている。EU の一般予算及びその適用規則を記載した Financial Regulations には、EU が公共調達を行う際に、EU 域外の企業も入札に参加することが可能であるが、WTO（世界貿易機構: World Trade Organization）の政府調達に関する協定（Agreement on Government Procurement）に参加しているか、または入札参加に関して EU と特定の同意を結んでいる必要があると記載されている。

今後に向けては、2017 年に公表されたサイバーセキュリティのパッケージが挙げられる。この中のサイバーセキュリティ法案（Cybersecurity ACT）には、欧州のサイバーセキュリティを所掌する機関である ENISA（欧州ネットワーク・情報セキュリティ機関: European Network and Information Security Agency）の権限強化や欧州全域にまたがるサイバーセキュリティ訓練の実施について記載されている。「ICT サイバーセキュリティ認証に関する規則案」は、ICT に関する機器、サービス、プロセスについて EU 全域での統一的なサイバーセキュリティの認証の仕組みを提案している。同規則案は、2018 年 12 月に EC（欧州委員会: European Commission）と議会によって合意された。現在は実現に向けて審議中であるが、これが実現されれば欧州のサイバーセキュリティはさらに強化されると考えられる。5G のネットワーク調達に関しては、EC の技術コミッショナーが 2018 年 12 月に懸念を示したものの、2019 年 1 月にはトーンダウンしており、調達ルールへの排除規定導入は不明である。

図 5-5 は、EU における政府関連組織と関連法制度をまとめたものである。番号により、組織と法制度の関連性を表現している（組織の概要は表 5-13 を、法制度の概要は表 5-14 を参照）。EU の行政機関は、欧州連合理事会に対して政策立案や法案の発議を行うとともに、行政執行の任務も負い、規則の発令や予算の管理を行う EC と、EC の下で特定の専門領域に関する任務を行うための専門機関により構成される。サイバーセキュリティに関連する専門委員会として、ENISA、Europol（欧州刑事警察機構: European Police Office）、EDA（欧州防衛機関: European Defense Agency）等が挙げられる。ENISA は 2004 年に設立され、EU 域内におけるネットワークと情報セキュリティを改善することに責任を負う。具体的には、サイバーセキュリティに関する情報収集、助言の提出、セキュリティ関連機関の連携促進を任務としている。2010 年からはサイバーセキュリティに関する大規模なインシデントの発生を想定したサイバー演習を隔年で実施している。Europol は加盟国間の情報交換促進並びに捜査支援を行うことを目的とする機関であり、その傘下にサイバー犯罪に対応するために 2013 年に設立された EC3（欧州サイバー犯罪センター: European Cybercrime Center）がある。EDA は、2004 年に設立され、防衛能力の向上等を行っている。また、CERT-EU（Computer Emergency Response Team for the EU Institutions, bodies and agencies）は、2012 年には設立された。主要な EU 機関（EC 等）の IT セキュリティエキスパートで構成され、EU 各機関のコンピュータシステムに対する脅威を管理する。また、EU 加盟国の CERT や専門的な IT セキュリティ企業と連携する。NIS 指令と GDPR は EU により発効されている。また、ENISA の権限等に関しては、Regulation (EC) No 460/2004、Regulation (EU) No 526/2013 に定められている。

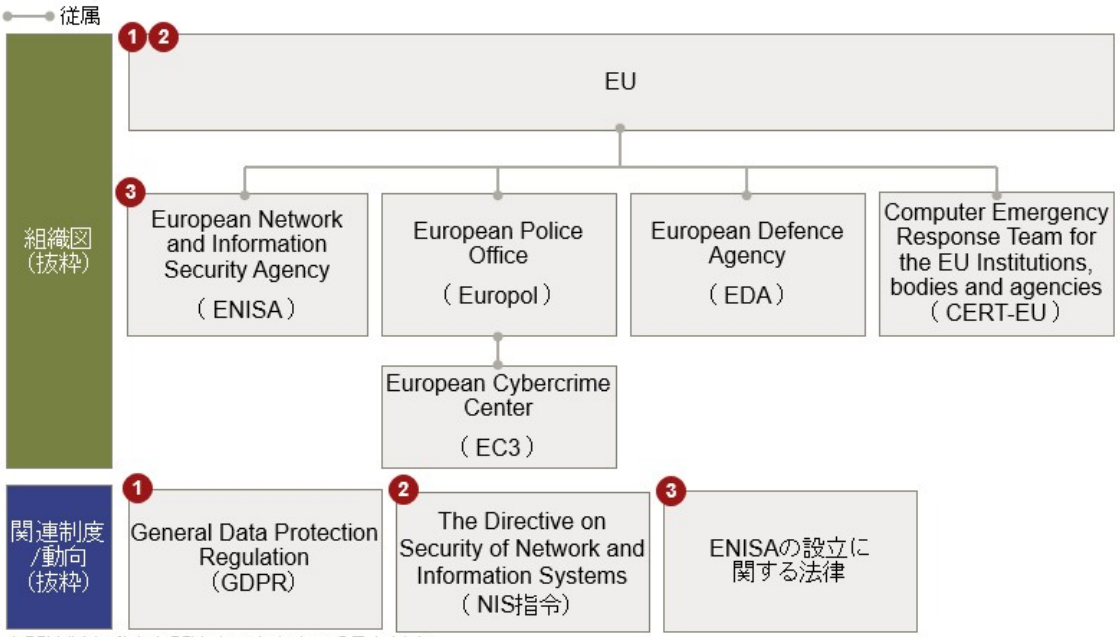


図 5-5　EU の政府関連組織と関連法制度

表 5-13　EU における政府関連組織

ENISA	欧州ネットワーク・情報セキュリティ機関。 ENISA は 2004 年に設立され、EU 域内におけるネットワークと情報セキュリティを改善することに責任を負う機関である。具体的には、サイバーセキュリティに関する情報収集、助言の提出、セキュリティ関連機関の連携促進を任務としている。また、2010 年からはサイバーセキュリティに関する大規模なインシデントの発生を想定したサイバー演習を隔年で実施している。
Europol	欧州刑事警察機構。 警察捜査を行うのではなく、加盟国間での情報交換の促進、加盟国館内での操作支援を行うことを目的とする機関である。
EC3	欧州サイバー犯罪センター。 拡大するサイバー犯罪に対応するために 2013 年に設立された機関である。
EDA	欧州防衛機関。 2004 年に設立され、防衛能力の向上等を行っている。
CERT-EU	EU 機関のための Computer Emergency Response Team。 2012 年には設立された。主要な EU 機関（欧州委員会等）の IT セキュリティエキスパートで構成され、EU 各機関のコンピュータシステムに対する脅威を管理する。また、EU 加盟国の CERT や専門的な IT セキュリティ企業と連携する。

表 5-14　EU における関連法制度

NIS 指令	2016 年 8 月に EU で制定された、サイバーセキュリティに関する指令。 法令番号は DIRECTIVE (EU) 2016/1148 となっている。
GDPR	2018 年に EU で制定された、一般データ保護規則。 法令番号は REGULATION (EU) 2016/679 となっている。
ENISA の設立に関する法律	法令番号は Regulation (EC) No 460/2004、Regulation (EU) No 526/2013 となっている。

5.2.2.4.2 対応状況

a. IoT セキュリティ全般

2013 年に公表された「EU サイバーセキュリティ戦略（Cybersecurity Strategy of the European Union）」では、EU が取り組むべき分野として、「サイバー耐性の構築」、「サイバー犯罪の劇的な減少」、「サイバー防衛政策推進と共通の防衛セキュリティ政策の実現」、「サイバーセキュリティ関連の産業・技術資源の確保」、「EU の中心的な価値の推進する包括的な国際サイバー空間政策の確立」の五つが記されている。2015 年 4 月「セキュリティに関する欧州の行動計画（The European Agenda on Security）」により、政策・立法措置等がまとめられ、その中でサイバー犯罪が優先課題と位置付けられた。そして、2016 年 8 月に EU では初となるサイバーセキュリティに関する指令 NIS 指令が発効された。また、2018 年には GDPR が発効され、個人情報の保護に関する強化が行われた。NIS 指令及び GDPR は欧州各国の法制度に組み込まれている（EU の法令に関しては、表 5-15 を参照）。また、2017 年 11 月に、ENISA は IoT セキュリティに関するガイドライン「Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures」を公表、IoT のセキュリティ要件、資産、脅威、想定される攻撃、セキュリティ対策等に関する情報を提供している。

欧州加盟国間にてセキュリティに関する共通の保護基準と認証ポリシーを標準化する協定 SOG-IS (Senior Official Group Information Systems Security) は発効されているが、現時点で EU レベルでの IT セキュリティ製品に関するセキュリティ認証の枠組みは存在していない。一方で、サイバーセキュリティのパッケージが 2017 年に公表され、EU におけるサイバーセキュリティの認証の仕組みである「ICT サイバーセキュリティ認証に関する規則案」が 2018 年 12 月に EC と議会によって合意されたことから今後導入に向けて作業が進むものと思われる。

表 5-15　EU 法令の分類[34]

日本語	英語	内容
規則	Regulation	・ 加盟国の国内法に優先して、加盟国の政府や企業、個人に直接適用される。 ・ そのため、加盟国の国内立法を必要とせず、加盟国の政府等に対して直接的な法的拘束力を及ぼす。
指令	Directive	・ 加盟国の政府に対して直接的な法的拘束力を及ぼす。 ・ 指令には政策目標と実施期限が定められ、指令が採択されると、各加盟国は、期限内に政策目標を達成するために国内立法等の措置を取ることが求められる。 ・ ただし、どのような措置を取るかは各加盟国に委ねられる。なお、企業や個人には直接適用されない。
決定	Decision	・ 特定の加盟国の政府や企業、個人に対して直接適用されるもので、対象となる加盟国の政府等に対して直接的な法的拘束力を及ぼす
勧告	Recommendation	・ 加盟国の政府や企業、個人等に一定の行為や措置を取ることを期待する旨、欧州委員会が表明するもの。原則として法的拘束力はない。
意見	Opinion	・ 特定のテーマについて欧州委員会の意思を表明するもの。勧告と同様、原則として法的拘束力はない。

b.　重要インフラ

重要インフラのサイバーセキュリティは、NIS 指令にて規定されている。NIS 指令において EU 加盟国は「エネルギー」、「保険衛生」、「水の供給」、「交通」、「デジタルインフラ」といった重要インフラ分野や、「オンラインマーケットプレイス」、「検索エンジン」、「クラウドコンピューティング」といったデジタルサービスの分野において、①提供されるサービスが社会・経済に対して必要不可欠であるか、②提供されるサービスがネットワークや情報システムに依存しているか、③インシデントが発生した際にサービスの供給に破壊的な効果をもたらすかどうか、という基準をもとに重要インフラ事業者及びデジタルサービス事業者を指定し、管理することが義務付けられている。NIS 指令にて規定されている義務と罰則に関して表 5-16 に示す。義務としては、①国家戦略の策定及び管轄官庁の指定、②各事業者の指定、セキュリティ対策及びインシデントの提出、③協力グループと CSIRT ネッ

[34]「EU 法について」国立国会図書館リサーチ・ナビより作成
https://rnavi.ndl.go.jp/politics/entry/eu-law.php

トワークを設置が規定されている。また、規定違反に対しては、罰則を規定し、実施措置を講じなければならない。

表 5-16　NIS 指令にて規定される義務と罰則

国家戦略の策定及び管轄官庁の指定	・ ネットワーク・情報システムの安全に関する国家戦略を策定して欧州委員会に通知する。 ・ 重要インフラ事業者及びデジタルサービス事業者の事業分野を所掌する管轄官庁に指定する。 ・ CSIRT（コンピュータセキュリティインシデント対応チーム: Computer Security Indicent Response Team ）を指定する。
各事業者の指定、セキュリティ対策及びインシデントの提出	・ 重要インフラ事業者及びデジタルサービス事業者の指定を行う。 ・ 上記事業者に指定された場合、セキュリティ対策とインシデント届出の義務が課される。
協力グループと CSIRT ネットワークを設置	・ EU 加盟国間の戦略的協力及び情報共有の支援、促進等を目的として、加盟国、欧州委員会、ENISA の代表者からなる協力グループを形成し、ベストプラクティスの共有、加盟国間の取り組みの共有等を行う。 ・ リスク対策及びインシデント対応の実施組織として EU 加盟国で指定された CSIRT のネットワークを設置する。
罰則	・ EU 加盟国は NIS 指令を組み入れた国内規定への違反があった場合には、適用可能な罰則規定を定め、その実施を確保するための措置を講じなければならない。

c.　政府調達

調達に関しては、表 5-17 にまとめた。2014 年発効の公共調達指令 Directive 2014/24/EC（政府機関による調達）、Directive 2014/25/EC（公益事業を行う事業体による調達）にて規定されている。Directive 2014/24/EC は主に加盟国及び加盟国内の地域もしくは地方の政府機関を対象としており、Directive 2014/25/EC は、「上下水道」、「交通サービス」、「港湾と空港」、「郵便サービス」、「エネルギー」の 5 分野の公益事業を対象としている。両指令において、調達の手続きや落札基準が記載されている。2004 年策定のそれ以前の調達と比較して、手続きを簡素で効率的なものとし発注者/受注者の負担の軽減を図るとともに、透明性と競争性を重視し、発注者にとって VFM (Value For Money) が得られるように見直しがされている。

EU の政府機関に関する調達の規定は、工事については 518.6 万ユーロ、役務については 13.4 万ユーロまたは 75 万ユーロ、物品調達については 20.7 万ユーロ以上の調達に適用さ

れる。また、公益事業に関する調達の規定は、工事については 518.6 万ユーロ、役務については 100 万ユーロ、物品調達については 41.4 万ユーロ以上の調達に適用される。

「防衛・安全保障に関する調達」は、2009 年発効の防衛・安全保障に関する調達指令(DIRECTIVE 2009/81/EC) で規定されている。調達の適用範囲は、「軍事装備（部品、コンポーネント等を含む)」、「機密関連の機器（部品、コンポーネント等を含む)」、「軍事装備、機密関連機器に直接関連する作業、供給及びサービス」、「特定の軍事目的または機密に関連する作業、サービス」と定義されている。また調達の対象となる金額は工事については 515 万ユーロ、物品調達については 41.2 万ユーロとなっている。防衛・安全保障に関する調達に入札する企業は、入札及び契約を行う際に機密情報の保護を目的とした要件を入札者や物品/役務提供者に課される場合がある。

EU の一般予算及びその適用規則を記載した Financial Regulations には、EU が公共調達を行う際に、EU 域外の企業も入札に参加することが可能であるが、WTO の政府調達に関する協定（Agreement on Government Procurement）に参加しているか、または入札参加に関して EU と特定の同意を結んでいる必要があると記載されている。入札企業は、そのサプライチェーンにおいて、欧州域外で、WTO の政府調達協定に加盟していない中国製品も利用することは可能となっているが、入札プロジェクトの仕様によって対応状況は異なるとされている。

表 5-17　EU における政府調達に関わる指令等

調達の対象	指令名	概説
EU 政府機関による調達	2014/24/EU	・ 加盟国政府機関が契約により、物品や役務（サービス）を調達する際のルールが定められた指令である。
公益事業を行う事業体による調達	2014/25/EU	・ 公共事業を行う事業体が、物品や役務（サービス）を調達する際のルールが定められた指令である。
防衛・安全保障に関する調達	2009/81/EC	・ 防衛及び安全保障関に関する物品、役務（サービス）を調達する際のルールが定められた指令である。 ・ 入札及び契約を行う際に機密情報の保護を目的とした要件を入札者や物品/役務提供者に課す場合がある。
Financial Regulation	-	・ EU が物品や役務（サービス）を調達する際の予算に関する取り決めが記載されている。 ・ その他、Financial Regulation においては、調達に入札可能な国が規定されている（Article176、Article177)。

5.2.2.4.3 今後の方向性

EU では、2017 年に「サイバーセキュリティのパッケージ」を公表しており、今後は同パッケージに沿ってサイバーセキュリティの検討が進むと思われる。特に、EU におけるサイバーセキュリティの認証に関して 2018 年 12 月に「ICT サイバーセキュリティ認証に関する規則案」が EC と議会によって合意されており、今後導入に向けて具体的な認証スキームの検討も開始されると思われる。図 5-6 は認証スキーム作成の手続きを示したものである。本規則案が発効された後、「ワークプログラムの作成」、「認証スキームの作成」の順に進められる。本認証スキームは、あくまでも自主的（Voluntary）なものであり、ただちに規制を課すものではない。認証制度に関して産業界では、国際的な標準・認証と、産業界の密接な関与が重要との立場を表明、認証制度に関して懐疑的な見解を示している。しかしながら、本認証スキームが導入されれば、欧州のサイバーセキュリティはさらに強化される可能性があり、同認証が欧州域内で広く普及した場合、欧州域外へも適用範囲が広がる可能性もあり、動向に注視する必要がある。

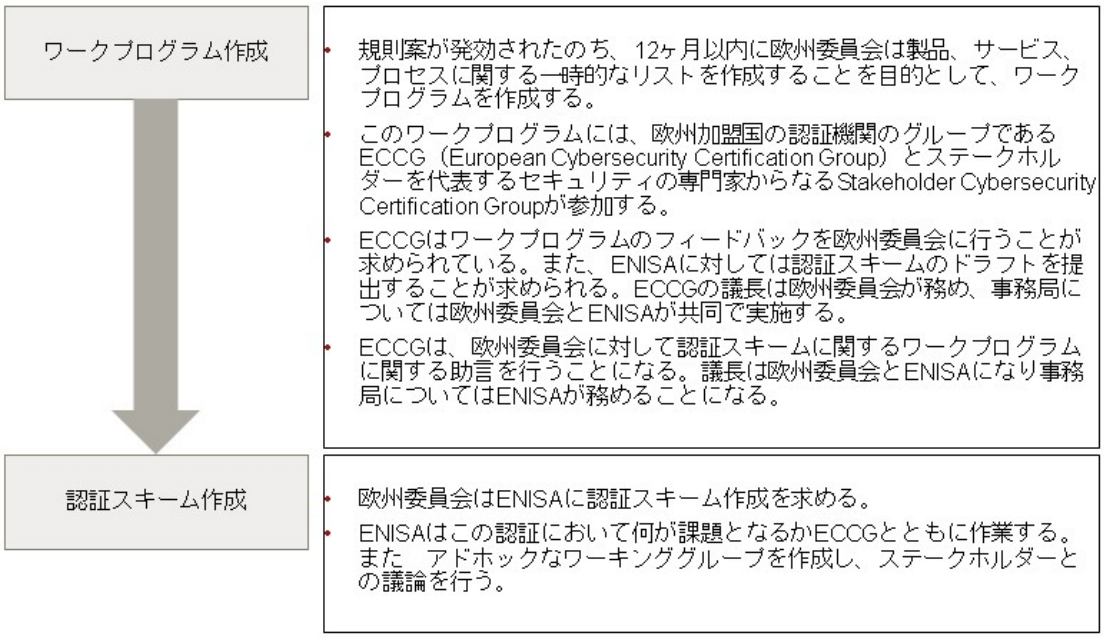


図 5-6 「ICT サイバーセキュリティ認証に関する規則案」の認証のスキームの検討

5.2.2.4.4 Evidence 及び原典

ア） 国としての全体的な状況（まとめ）

- EU サイバーセキュリティ戦略（Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace）
  https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
- ネットワークと情報セキュリティ指令(The Directive on Security of Network and Information Systems (DIRECTIVE (EU) 2016/1148))
  https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN
- セキュリティに関する欧州の行動計画（The European Agenda on Security）
  http://www.europarl.europa.eu/cmsdata/125863/EU%20agenda%20on%20security.pdf

- 一般データ保護規則（GDRP (General Data Protection Regulation) (REGULATION (EU) 2016/679)）
  https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN
- ENISA
  https://www.enisa.europa.eu/
- Europol
  https://www.europol.europa.eu/
- European Cybercrime Center
  https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
- サイバーセキュリティ法案（Cybersecurity ACT）
  https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en
- Europe should be wary of Huawei, EU tech official says
  https://www.reuters.com/article/us-eu-china-huawei/europe-should-be-afraid-of-huawei-eu-tech-official-says-idUSKBN1O611X
- EU Tech Chief Warns Again on Cyber Threat From China
  https://www.bloomberg.com/news/articles/2019-01-25/eu-tech-chief-says-can-no-longer-be-naive-over-china-cyber-risks

イ） 対応状況

- IoT セキュリティ全般
  - 一般データ保護規則（GDRP (General Data Protection Regulation) (REGULATION (EU) 2016/679)）
    https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN
  - Baseline Security Recommendations for IoT
    https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
  - SOG-IS (Senior Official Group Information Systems Security)
    https://www.sogis.eu/

- 重要インフラ
  - ネットワークと情報セキュリティ指令（The Directive on Security of Network and Information Systems (DIRECTIVE (EU) 2016/1148)）
    https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN
  - 「ネットワーク・情報システムの安全に関する指令（NIS 指令）―EU のサイバーセキュリティ対策立法―」
    国立国会図書館 調査及び立法考査局　海外立法情報課 島村 智子
    外国の立法 277 (2018.9)
    http://dl.ndl.go.jp/view/download/digidepo_11152345_po_02770001.pdf?contentNo=1&alternativeNo=

- 政府調達
  - public procurement and repealing Directive 2004/18/EC (DIRECTIVE 2014/24/EU)
    https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0024&from=EN
  - procurement by entities operating in the water, energy, transport and postal

services sectors and repealing Directive 2004/17/EC (DIRECTIVE 2014/25/EU)
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0025&from=EN

- the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC(DIRECTIVE 2009/81/EC)
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0081&from=EN
- 政府調達に関する協定（Agreement on Government Procurement）
https://www.wto.org/english/docs_e/legal_e/rev-gpr-94_01_e.htm
- Financial Regulation 2018
http://ec.europa.eu/budget/library/biblio/publications/2018/financialregulation_en.pdf

ウ） 今後の方向性

- サイバーセキュリティ法案（Cybersecurity ACT）
https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en
- Europe should be wary of Huawei, EU tech official says
https://www.reuters.com/article/us-eu-china-huawei/europe-should-be-afraid-of-huawei-eu-tech-official-says-idUSKBN1O611X
- EU Tech Chief Warns Again on Cyber Threat From China
https://www.bloomberg.com/news/articles/2019-01-25/eu-tech-chief-says-can-no-longer-be-naive-over-china-cyber-risks

5.2.2.5 フランス

5.2.2.5.1 国としての全体的な状況(まとめ)

フランスの政策動向の概要を表 5-18 に示す。

表 5-18　フランスの政策動向（まとめ）

	項目	概要
現状	全体傾向	EU と足並みを揃える形でサイバーセキュリティの強化を行っている。EU における GDPR/NIS 指令もそれぞれ 2018 年 6 月/5 月にフランス国内法に組み込まれた。
	重要インフラの法制度	「The Military Programming Act for the years 2014 to 2019」にて重要インフラ事業者を定義（200 社程度）、各企業の情報システムの安全性に関する措置を定めた。2019 年以降を対象とした国内法「Military programming Act for the years 2019 to 2025」では、ANSSI と電気通信事業者に情報システムの安全に影響する脅威を予防し、明らかにするための権限が付与されている。
	政府調達	2014 年の一連の EU 指令（2014/24/EU, 2014/25/EU）が国内法に組み込まれた。防衛安全分野については、EU 指令(2009/81/EU）が国内法に組み込まれる形で定められている。EU 域外からの入札は、WTO 多国間政府調達協定国、または公的機関入札で EU と協定を結んでいる国が入札に参加可能。
	認証/認定制度	サイバーセキュリティに関し、フランス固有の認証/認定制度は見られない。基本的には EU 制度/体制を踏襲するものと考えられる。
	体制	政府から独立した専門機関がサイバーセキュリティをリードしている。国防安全保障事務局（SGDSN）配下のサイバーセキュリティ専門機関 ANSSI は、情報システムのセキュリティの責任を負い、個人情報当局 CNIL は、データ保護を監督する。ARCEP は、電気通信分野の独立規制機関で、電気通信規制権限を行使する。
今後	全体的な傾向	2018 年 2 月に「サイバーディフェンスにおける戦略レビュー」を公表、サイバーセキュリティに関する危機管理と国家戦略としての目標を明確化した。
	重要インフラの法制度	EU の施策に沿っており、フランスとして現状目立った動きはみられない。
	政府調達	同上。

フランスでは、EU と足並みを揃える形でサイバーセキュリティの強化を行っている。EU における NIS 指令は 2018 年 5 月に、GDPR は 2018 年 6 月にフランス国内法に組み込まれた。フランスのサイバーセキュリティは、SGDSN（首相府防衛・国家安全総局: General Secretariat for Defence and National Security）とその配下の ANSSI（国家情報システムセキュリティ庁: French National Cybersecurity Agency）が主導しており、その中で ANSSI が IT 機器に関する認証「Security VISA」も提供している。

重要インフラについては、The Military Programming Act for the years 2019 to 2025 によって最重要事業者が規定されている。また、ANSSI と電気通信事業者に情報システムに脅威を予防し、明らかにするための権限が付与されている。

政府調達については、2014 年に EU から新たに公表された EU 政府機関よる調達の指令(2014/24/EU)、公益事業体を行う事業体による調達の指令（2014/25/EU）を国内の法律にして導入している。また、防衛・安全保障に関する調達についても、防衛・安全保障に関する調達の指令（2009/81/EU）を国内の法律として導入をしている。また、EU 域外からの入札については、法律 Ordonnance n° 2015-899 の中で WTO (World Trade Organization) の WTO 多国間政府調達協定 (WTO Plurilateral Agreement on Government Procurement) の国、または公的機関の入札に関して EU と協定を結んでいる国が入札に参加可能なことが規定されている。

今後に向けては、フランスのサイバーセキュリティに関しては、EU の NIS 指令や GDPR を国内に導入することで EU と歩調を合わせているように見える。一方で、報道によるとサイバーセキュリティに対応する人材を軍部に配備する計画やそれに伴う国防費の増加が指摘されており、国防の課題として積極的に取り組む流れが見える。現時点では法制度導入への直接的な動きはないが、今後の動きに注視が必要である。

図 5-7 は、フランスにおける政府関連組織と関連法制度をまとめたものである。番号により、組織と法制度の関連性を表現している（組織の概要は表 5-19 を、法制度の概要は表 5-20 を参照）。SGDSN は、国防と安全保障について首相を補佐する機関である。また、ANSSI はフランス国内における情報システムのセキュリティに関して責任を負う国家機関である。ARCEP は、電気通信分野の独立規制機関となっており、ANSSI は ARCEP に対して重要インフラ事業者に対するサイバーアタックがあった際に技術的な情報を求めることが可能となっている。その他にも、ARCEP は「郵便・電子通信法典」を所掌する機関でもある。HFDS はフランスの各省庁において、情報システムのセキュリティや実装を行う際の責任主管となる。最後に、CNIL はフランスにおけるデータ保護監督機関であり、GDPR をもとに個人情報保護違反があった際には制裁金を科すことを行っている。

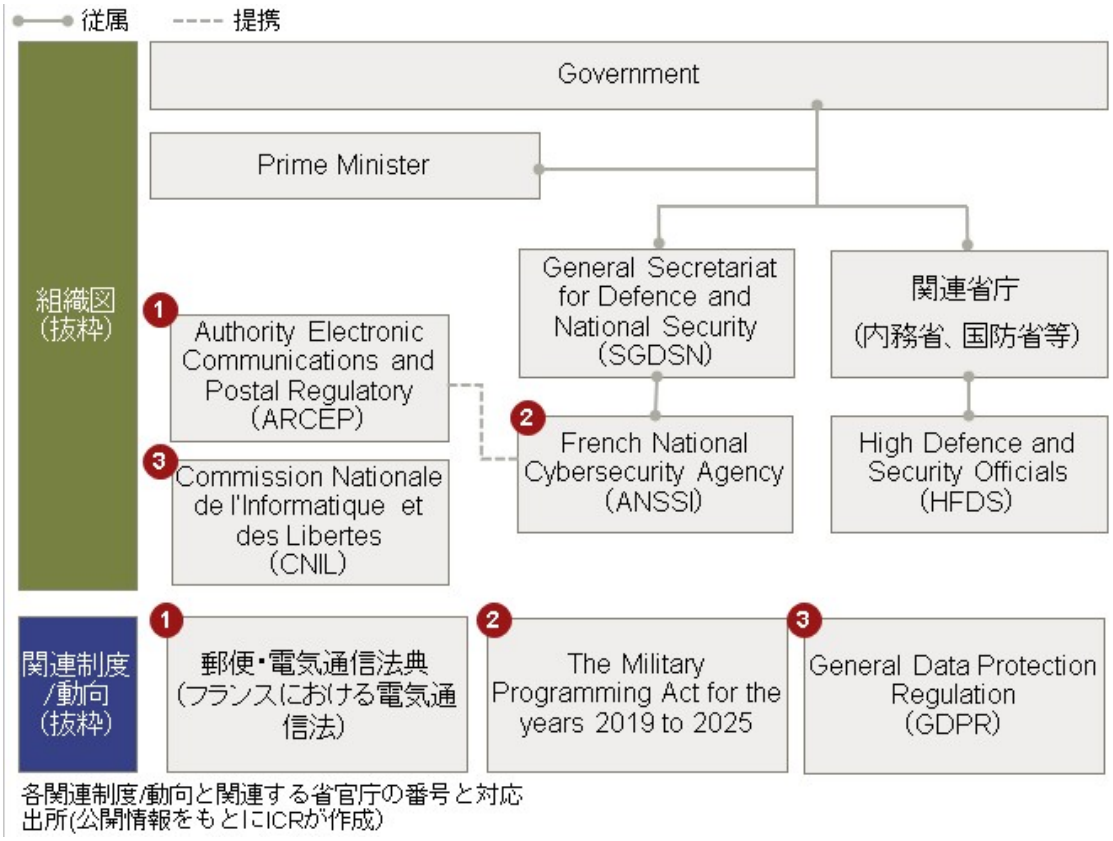


図 5-7　フランスの政府関連組織と関連法制度

表 5-19　フランスにおける政府関連組織

SGDSN	首相府防衛・国家安全総局。 SGDSN は、国防と安全保障について首相を補佐する機関である。
ANSSI	国家情報システムセキュリティ庁。 情報システムのセキュリティに関して責任を負う国家機関である。
ARCEP	電子通信・郵便規制機関。 電気通信分野の独立規制機関である。また、ARCEP は日本の電気通信事業法にあたる「郵便・電気通信法典」を所掌する。
HFDS	フランスの各省庁において、情報システムのセキュリティや実装を行う際の責任主管。
CNIL	国家個人情報保護機関。 CNIL はフランスにおけるデータ保護監督機関である GDPR をもとに個人情報保護違反があった際には制裁金を科すことを行っている。

表 5-20　フランスにおける関連法制度

郵便・電気通信法典	フランスにおける電気通信事業法。
The Military Programming Act for the years 2019 to 2025	重要インフラ事業者を規定。 各企業の情報システムの安全性に関する措置を定められている。ANSSI と電気通信事業者に情報システムの安全に影響する脅威を予防し、明らかにするための権限が付与された。
GDPR	2018 年に EU で制定された、一般データ保護規則。 国内法 LOI n° 2018-493 及び Loi 78-17 du 6 janvier 1978 modifiée として取り入れられた。

5.2.2.5.2 対応状況

a. IoT セキュリティ全般

フランスのサイバーセキュリティに関する取り組みとしては、2007 年に国防軍が国家安全保障戦略として「防衛と国家安全に関する白書（The French White Paper on Defence and National Security)」を公表したことに始まる。この白書ではサイバー攻撃が主要なテーマとして取り上げられており、フランスのサイバーセキュリティ専門の機関である ANSSI の設置が提言されている。ANSSI に関しては、2018 年 1 月時点で、約 500 人程度の局員が在籍しており、1 年間で約 100 程度の資格や認証をそれぞれ発行している。また、2015 年には「国家サイバーセキュリティ戦略（French National Digital Security Strategy)」が公表され、サイバー空間におけるフランスの基本的な利益を確保するために、防衛力を確保することが記されており、また防衛主導でフランス全体のサイバーセキュリティを確保することを表明している。この戦略は、「デジタルセキュリティは政府、サービス事業者及び市民の共同の責務」、「国民の個人情報への侵害は国家の安全上の重大用件」、「仏企業のデジタルセキュリティ製品・サービスは産業界での国際競争力強化の重要要件」という観点から、主要な目的を①国防、②デジタルの信頼性向上、③セキュリティ教育、④デジタル関連企業支援、⑤欧州域内におけるサイバー空間の安定性、の 5 項目にまとめている。

フランスの IoT 全般に関する法律としては、GDPR が 2018 年 6 月 21 日からフランス国

内法に組み入れられており（LOI n° 2018-493 及び Loi 78-17 du 6 janvier 1978 modifiée）、フランス国内のデータ保護に関する機関は CNIL となっている。認証については、ANSSI が IT 関連製品の認証「Security VISA」を政令（Décret n° 2002-535）に基づいて提供しており、認証プロセスには 6～18 カ月程度かかる。具体的には、国際標準ベースのコモンクライテリア（CC）と ANSSI の独自標準（CSPN）という二つの水準での認証が提供されている。CC とはコンピュータセキュリティの国際規格で、IT 製品・情報システムに関する情報セキュリティを評価・認証する基準を定めている。この認証を取得することで製品の競争力が向上するとされている。また CC は国際協定を含むため、他国で同一製品の認証を再度受ける必要がなくなる。CSPN は CC 認証ほど網羅的ではなく、高いセキュリティレベルが求められない製品の認証に重点をおいたものとなっている。また、実際に検証を行う際は ANSSI が認定した第三者機関である「IT Security Evaluation Facility（ITSEF）」が行っている。

ANSSI によって公開されている情報をもとに、認証プロセスについては以下の通りである。

1. メーカーもしくは販売業者が認証を申請する。
2. ANSSI の認定を受けたテストセンター（ITSEF）が、ANSSI が公開しているもしくは一般的に認可されている IT セキュリティ基準（12 項目）に基づいて評価を実施する。なお、この評価はテストセンターの従業員によって行われ、一貫したアプローチ及び方法論が保証されている。
3. 認証の結果をテストセンターが認証報告書（certification report）に記録する。その報告書には、製品の安全に関する説明・評価の詳細・消費者へのアドバイス等が含まれる。なお、証明書及び認証報告書は ANSSI が発行し、申請者の同意の下、公表される。

また、認証にかかる費用負担は申請者が行うとされているが、具体的な金額は今回の調査では不明である。なお、EAL は CC で定められている情報セキュリティの厳格さを評価する指標であり、EAL1（低）から EAL7（高）までの 7 段階が存在する。この認証をクリアした製品は具体名とともに ANSSI の Web サイトで公開されている。具体的な評価機関については公表されていない。

b. 重要インフラ

重要インフラについては、The Military Programming Act for the years 2014 to 2019 によって重要インフラ事業者が定義されており、各企業の情報システムの安全性に関する措置を定められている。重要インフラ事業者は公的部門、民間部門を含めて 200 社程度が選定されているが、具体名についてはセキュリティの観点から非公開となっている。カテゴリについては、「ヘルスケア関連製品」、「水管理」、「食品」、「電力供給」、「天然ガス供給」、「石油炭化水素供給」、「交通」、「オーディオビジュアルと情報」、「電気通信とインターネット」、「金融」、「原子力」、「兵器産業」、「宇宙」となっている。特に、EU では規定されていない「原子力」、「兵器産業」、「宇宙」といった分野が指定されていることが特徴的といえる。また、2019 年以降を対象とする法律 Military programming Act for the years 2019 to 2025 では、ANSSI と電気通信事業者に情報システムの安全に影響する脅威を予防し、明らかにするための権限が付与された。

さらに、EU の NIS 指令を組み込む法律（LOI n° 2018-133）が制定され、オンラインマーケットプレイス、検索エンジン、クラウドコンピューティングサービスに関する事業者にも新しいサイバーセキュリティの義務を組み入れられた。これらの事業者は NIS 指令で規定されているように、セキュリティ対策の制定と ANSSI へ重大インシデントを報告する義務が求められている。ここで技術的な義務として導入が求められているセキュリティ対

策には、①情報システムには業務とセキュリティに必要なものしかインストールしてはならない、②情報システムへファイアウォールの設置する、③情報システムにリモートでアクセスする場合には暗号化と認証の仕組みを取り入れる、といったものがある。その他にもセキュリティ違反を察知するシステムや情報システムのログを取得することが求められている。技術以外では、重要インフラ事業者にネットワークと情報システムのセキュリティポリシーの作成や、情報システムのリスク評価の実施等が義務付けられている。

その他、重要インフラ事業者に関する法律としては Law for a Digital Republic 2016 (LOI n° 2016-1321) がある。電気通信事業者に対するサイバーセキュリティの義務を課したものとなっており、事業者にはネットワークの耐久性、品質、利用可能性、セキュリティと保全が求められ、ネットワークセキュリティまたは保全の違反があった場合には、CNIL 及び ANSSI への報告が求められている。

c. 政府調達

政府調達については、概要を表 5-21 に示す。2014 年に EU から新たに公表された、公共調達指令 Directive 2014/24/EC（政府機関による調達）、Directive 2014/25/EC（公益事業を行う事業体による調達）の二つを導入した法律（Ordonnance n° 2015-899）が適用されている。これは、政府機関、公益事業を行う事業体が契約により、物品や役務（サービス）を調達する際のルールが定められた指令である。政府機関の対象としては、国、公法（public law）に服する機関等が含まれる。政府機関に関する調達の規定は、工事については 518.6 万ユーロ、役務については 13.4 万ユーロまたは 75 万ユーロ、物品調達については 20.7 万ユーロ以上の調達に適用される。また、公益事業に関する調達の規定は、工事については 518.6 万ユーロ、役務については 100 万ユーロ、物品調達については 41.4 万ユーロ以上の調達に適用される。調達に入札可能な国として、WTO (World Trade Organization) の WTO 多国間政府調達協定（WTO Plurilateral Agreement on Government Procurement）の国、または公的機関の入札に関して EU と協定を結んでいる国であることが規定されている。また、防衛・安全保障に関する調達についても、EU の 2009 年発効の防衛・安全保障に関する調達指令（DIRECTIVE 2009/81/EC）を政令（Décret n° 2016-361）として導入を行っている。これは、防衛及び安全保障に関する物品、役務（サービス）を調達する際のルールが定められた政令である。EU の調達のように機密情報に関する記述は見つけることができなかった。調達の適用範囲は、「軍事装備（部品、コンポーネント等を含む）」、「機密関連の機器（部品、コンポーネント等を含む）」、「軍事装備、機密関連機器に直接関連する作業、供給及びサービス」、「特定の軍事目的または機密に関連する作業、サービス」と定義されている。また調達の対象となる金額は工事については 515 万ユーロ、物品調達については 41.2 万ユーロとなっている。防衛・安全保障に関する調達に入札する企業は、入札及び契約を行う際に機密情報の保護を目的とした要件を入札者や物品/役務提供者に課される場合がある。EU 域外からの入札については、法律 Ordonnance n° 2015-899 の中において WTO (World Trade Organization) の WTO 多国間政府調達協定（WTO Plurilateral Agreement on Government Procurement）の国、または公的機関の入札に関して EU と協定を結んでいる国が入札に参加可能なことが規定されている。また、防衛や情報セキュリティを確保するために調達者は入札に特別な条件を課すことが可能となっており、EU の防衛・安全保障に関する調達と同様の考え方が盛り込まれている。

表 5-21　フランスの政府調達に関する指令及び規制

調達の対象	指令名	概説
仏政府機関、公益事業を行う事業体による物品・役務の調達	Ordonnance n° 2015-899	・ 政府機関、公益事業を行う事業体が契約により、物品や役務（サービス）を調達する際のルールが定められた指令である。 ・ 政府機関の対象としては、国、公法（public law）に服する機関等が含まれる。 ・ 調達に入札可能な国として、WTO（World Trade Organization）の WTO 多国間政府調達協定（WTO Plurilateral Agreement on Government Procurement）の国、または公的機関の入札に関して EU と協定を結んでいる国であることが規定されている。
防衛・安全保障に関する調達	Décret n°2016-361	・ 防衛及び安全保障関に関する物品、役務（サービス）を調達する際のルールが定められた政令である。 ・ EU の調達のように機密情報に関する記述は見つけることができなかった。

5.2.2.5.3 今後の方向性

フランスのサイバーセキュリティに関しては、EU の NIS 指令や GDPR を国内に導入することで EU と歩調を合わせているように見える。しかし、2018 年後半からはサイバーセキュリティに関して EU とは異なる動きを見せている独自色を示すようになってきている。

特徴的な事例としては、2018 年 11 月にパリで開催された「インターネットガバナンスフォーラム（IGF）」において、エマニュエル・マクロン大統領が行った演説やほぼ同じ時期に公開された「Paris Call」が挙げられる。同演説や「Paris Call」は、そのままフランス国内法に導入されるわけではないが、要約するとサイバー空間の安全性を確保するためには国として何らかの規制が必要であるというものであり、EU とは異なる動きを見せている。また、参照した Web 記事「France's New Offensive Cyber Doctrine」によれば、2025 年までにサイバー関連の人員を 1,500 人増やし、トータルで 4,000 人確保し、16 億ユーロを投入するとしており、国防としてのサイバーセキュリティ強化に力を入れていることがわかる。

5.2.2.5.4 Evidence 及び原典

ア） 国としての全体的な状況（まとめ）

- 防衛と国家安全に関する白書（The French White Paper on Defence and National Security）
  http://www.mocr.army.cz/images/Bilakniha/ZSD/French%20White%20Paper%20on%20Defence%20and%20National%20Security%202008.pdf
- 国家サイバーセキュリティ戦略（French National Digital Security Strategy）
  https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
- 一般データ保護規則（GDRP（General Data Protection Regulation）（REGULATION（EU）2016/679））
  https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN
- ネットワークと情報セキュリティ指令（The Directive on Security of Network and Information Systems（DIRECTIVE（EU）2016/1148））
  https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN
- Security VISA
  https://www.ssi.gouv.fr/en/security-visa/
  https://www.ssi.gouv.fr/uploads/2018/01/catalogue_qualified_solutions_anssi.pdf
- The Militaly Programming Act for the years 2014 to 2019
  https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&categorieLien=id
- The Military Programming Act for the years 2019 to 2025
  https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037192797&categorieLien=id
- public procurement and repealing Directive 2004/18/EC（DIRECTIVE 2014/24/EU）
  https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0024&from=EN
- procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC(DIRECTIVE 2014/25/EU)
  https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0025&from=EN
- the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC(DIRECTIVE 2009/81/EC)
  https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0081&from=EN
- SGDSN
  http://www.sgdsn.gouv.fr/
- ANSSI
  https://www.ssi.gouv.fr/
- ARCEP
  https://www.arcep.fr/
- CNIL
  https://www.cnil.fr/

イ） 対応状況

- IoT セキュリティ全般
  - LOI n° 2018-493
    https://www.legifrance.gouv.fr/eli/loi/2018/6/20/JUSC1732261L/jo/texte
  - Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
    https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460
  - Décret n°2002-535
    https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000412673&categorieLien=cid
  - IT Security Evaluation Facility (ITSEF)
    https://www.ssi.gouv.fr/en/certification/common-criteria-certification/licensed-itsef/
  - LES PRODUITS CSPN
    https://www.ssi.gouv.fr/administration/produits-certifies/cspn/produits-certifies-cspn/

- 重要インフラ
  - The Militaly Programming Act for the years 2014 to 2019
    https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&categorieLien=id
  - The Military Programming Act for the years 2019 to 2025
    https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037192797&categorieLien=id
  - LOI n° 2018-133
    https://www.legifrance.gouv.fr/eli/loi/2018/2/26/INTX1728622L/jo/texte/
  - Law for a Digital Republic 2016（LOI n° 2016-1321）
    https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746&categorieLien=id

- 政府調達
  - public procurement and repealing Directive 2004/18/EC (DIRECTIVE 2014/24/EU)
    https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0024&from=EN
  - procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC(DIRECTIVE 2014/25/EU)
    https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0025&from=EN
  - Ordonnance n° 2015-899
    https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030920376
  - the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defence and security, and amending Directives 2004/17/EC and 2004/18/EC(DIRECTIVE 2009/81/EC)
    https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0081&from=EN
  - Décret n°2016-361
    https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032296743&categorieLien=id

ウ） 今後の方向性

- インターネットガバナンスフォーラム（IGF）
  https://www.intgovforum.org/multilingual/
- Paris Call
  https://jp.ambafrance.org/article13835
- France's New Offensive Cyber Doctrine
  https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine

5.2.2.6 ドイツ

5.2.2.6.1 国としての全体的な状況(まとめ)

ドイツの政策動向の概要を表 5-22 に示す。

表 5-22　ドイツの政策動向（まとめ）

	項目	概要
現状	全体傾向	情報セキュリティ管轄の政府機関 BSI (Federal Office for Information Security) が中心となり、IoT セキュリティに関する制度を規定している。BSI は、重要インシデント発生時の通知義務を規定する法律や、重要インフラに関するガイドラインを発効するとともに、連邦政府で用いる IT 製品が満たすべき最低基準の規定や、IT 製品の種類に応じた認証制度策定を主導している。通信サービスプロバイダー/NW プロバイダーは BNetzA 作成の Telecommunications Act で規制している。
	重要インフラの法制度	IT Security Act 及び EU の NIS 指令を取り入れた BSI Act にて BSI の権限等に関して規定するとともに、重要インフラの通知義務等を規定している。通信サービスプロバイダー/NW プロバイダーに関しては、電気通信事業法に相当する Telecommunications Act (TKG)、テレメディアに関しては Telemedia Act (TMG) で規定している。また、BSI は重要インフラの各セクターにおける奨励事項を記述した TRITIS を提供している。
	政府調達	政府調達に関しては、BSI Act に基づき政府の情報技術のセキュリティを担保するための最低基準としての Minimum Standards が規定されている。ハードウェア・ソフトウェア・ネットワーク等の技術的要素から、テクノロジーに纏わる組織・人的資源等の観点等様々な視点で規定しており、異なる分野の政府機関の統一した基準となっている。
	認証/認定制度	IT 製品/情報システムの調達に関しては国際規格であるコモンクライテリアに基づく認証制度を導入している。政府調達に関しては、BSI 提供の Technical Guideline に基づく認証制度 Certification to TR にて、BSI 認定のテストセンターによって TR の定義に基づき適合性評価が実施されており、評価が完了すると適合性確認書が授与される。
	体制	IoT セキュリティ及びサイバーセキュリティは、情報セキュリティに関する政府の管轄機関である BSI を中心に推進されており、責任範囲はコンピュータ AP (application program) のセキュリティ/重要インフラの保護対策/セキュリティ製品の認証/セキュリティ評価機関の多岐にわたる。通信ネットワークのセキュリティに関しては、連邦ネットワーク庁である BNetzA が規定する。
今後	全体的な傾向	サイバーセキュリティに関して、高度なイノベーションを志向する機関 (Agency for Innovation in Cyber Security) 設置等強化を継続。新規に IT 製品認証制度 (Accelerated Security Certification) を制定、認証効の効率化を目指している。重要インフラに対しては、不審なオンライン行動を政府機関と自動的に共有するデータバンクの整備の意向が示されている。

	項目	概要
	重要インフラの法制度	重要インフラにおいては、IT Security Act 2.0 が策定中で、この中で組織のモニタリングや罰則指令等 BSI のさらなる権限拡大が検討されている。また BMI の大臣は重要インフラに関してドイツで販売されている IT 製品に対して、BSI の認定証明書を必須とする法律を制定する意向を示している。
	政府調達	サイバーセキュリティに関する懸念から、特定企業への対応方法に関して政治的な議論をなされているが、現時点では技術に基づき選別し、特定の個別企業を排除しない方向で検討されている。政府調達についての新たな制度制定の動きは現在のところ見受けられない。

現状のドイツにおける IoT セキュリティ及びサイバーセキュリティに関する規制は主に、情報セキュリティに関する政府の管轄機関である BSI（連邦情報セキュリティ庁: Federal Office for Information Security）が規定している。BSI の権限等は法律 BSI Act (Act on the Federal Office for Information Technology) に基づいて規定されており、BSI はこの規定に従い、公的機関・企業における情報セキュリティ問題への対処方法や情報技術の使用者へ向けた技術的なサポートに関する規定（BSI-Standards）を定めている他、重要インフラを含む様々なサイバーセキュリティに関する奨励事項（Recommendations）を規定している（ガイドラインと奨励事項は、いずれも原則として法的拘束力を有しない「奨励」的な性質を有するという点では共通している。一方で、法令上の義務が具体化されているガイドラインでは、規定事項の不履行により法令上の違反につながるケースがあるため、事実上強制力が認められる場合もある）。また BSI は、各 IT 製品の種類に応じた認証制度（Certification to CC (Common Criteria) (Zertifizierung nach CC)、IT-Grundschutz Certification、C5 (Cloud Computing Compliance Controls Catalogue) に基づいた認証等）に関しても規定している。

重要インフラについては、重要インフラのオペレーターに対して重大インシデントが発生した場合に BSI へ通知することが義務付けられている他（BSI Act)、特に通信サービスプロバイダー及びネットワークプロバイダーに対しては、Federal Network Agency for Electricity, Gas, Telecommunication, Post and Railway (BNetzA) が通信の機密性の保護や個人データの漏洩の防止等に関する法律 TKG (Telecommunications Act) を規定していたりする。さらに、BSI が重要インフラの各セクター固有のセキュリティ基準 KRITIS sector specific security standard for data centres, server farms and content delivery networks（KRITIS branchenspezifischen Sicherheitsstandard (B3S) für Rechenzentren, Serverfarmen und Content Delivery Netzwerke）等）を規定している。

政府調達については、BMI（連邦内務省: Federal Ministry of the Interior, Building and Community）が、入札手続きの間、外国の諜報機関に機密データの転送を行わないことの宣言を義務付ける法律 No-Spy Regulation (No-Spy-Erlass) を制定している他、BSI が政府機関の IT セキュリティにおいて最低限満たさなければならないとされている基準 (Minimum Standards) を規定しており、異なる分野の政府機関においてサイバー攻撃に対する効果的な保護対策に関して統一した基準が確立されている。さらに BSI は、IT 製品に関する認証制度 Certification to TR (Technical Guidelines) (Zertifizierung nach TR) も規定しており、国家安全保障上セキュリティ対策が重要な分野の製品に関して一定のセキュリティ基準をクリアしていることを担保する。

今後に向けては、サイバーセキュリティ分野における高度なイノベーションを志向する機関 Agency for Innovation in Cyber Security の設置が見込まれており、BMI、及び BMVg (Federal Ministry of Defense) が管轄を行うとしている。また BSI は、IT 製品の認証制度において、評価に要する時間の短縮やセキュリティ文書要件の削減を企図した新しい制度 BSZ (Accelerated Security Certification) の制定を進めている。重要インフラについては、法律の改正により IT Security Act 2.0 (Act to Strengthen the Security of Federal

Information Technology 2.0)、BSI の権限や罰則に関する新たな権利等の制定が検討されている。また政府は、重要インフラにおける不審なオンライン行動を政府機関と自動的に共有するデータバンクの整備の意向を示している。

図 5-8 は、ドイツにおける政府関連組織と関連法制度をまとめたものである。番号により、組織と法制度の関連性を表現している（組織の概要は表 5-23 を、法制度の概要は表 5-24 を参照)。BMI は治安、災害、テロ等から国民の保護を行う責任をもつ。BMVI（連邦交通デジタルインフラ省: Federal Ministry of Transport and Digital Infrastructure）は、2013 年 12 月に発足した。同省は、水路・航空・道路等の運輸インフラのほか、デジタルインフラを所管する。BMWi（連邦経済エネルギー省: Federal Ministry of Economic Affairs and Energy）は、情報通信政策を行っている。German Chancellery（ドイツ首相府）は、デジタルアジェンダ 2014－2017 に責任をもつ。このアジェンダは、IT システムと IT サービスの安全性を改善、ネットワーク社会と経済における信頼性とセキュリティの確保等を目標とし、BMWi、BMI、BMVI が作成した。また、BSI は、情報セキュリティに関する政府の管轄機関であり、BSI の権限等は BSI Act に基づいて規定されている。IoT セキュリティ及びサイバーセキュリティに関する規制を行っている。BNetzA（連邦ネットワーク庁: Federal Network Agency for Electricity, Gas, Telecommunication, Post and Railway）は、電気、ガス、通信、郵便のほか、社会インフラ全般を所掌している。

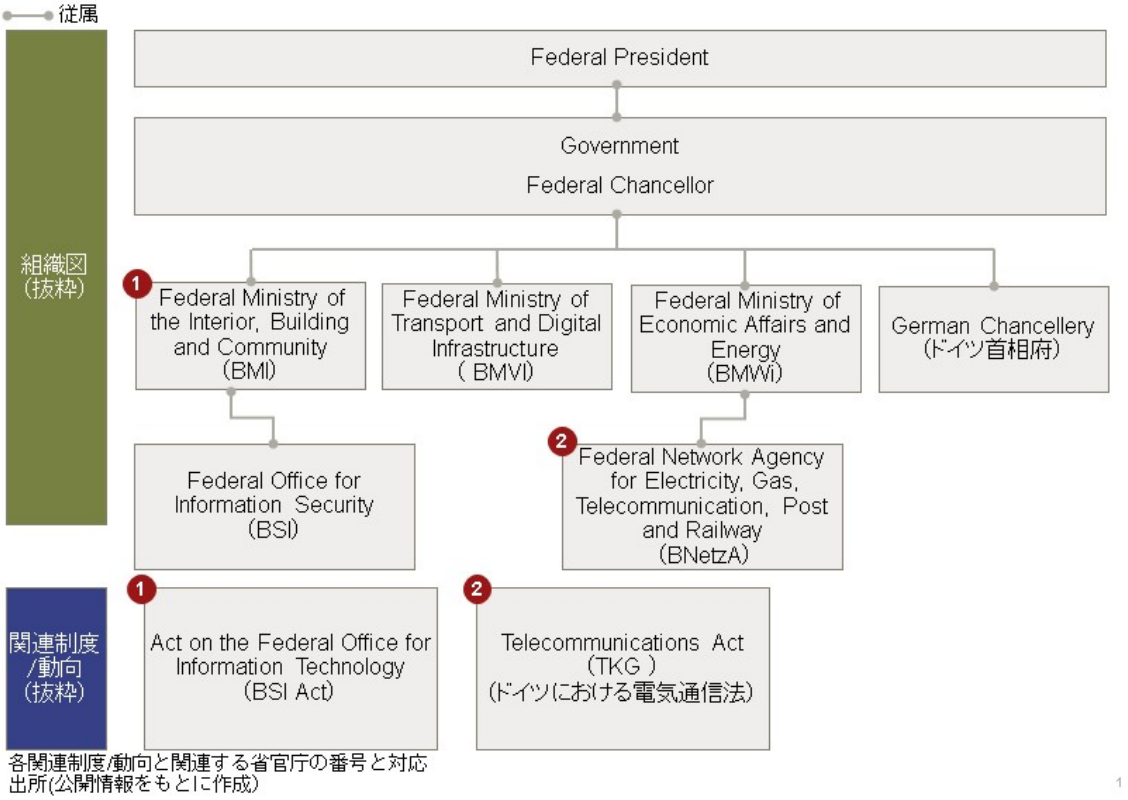


図 5-8　ドイツの政府関連組織と関連法制度

表 5-23　ドイツにおける政府関連組織

BMI	連邦内務省。 治安、災害、テロ等から国民の保護を行う責任をもつ。
BMVI	連邦交通デジタルインフラ省。 2013年12月に発足。同省は、水路・航空・道路等の運輸インフラのほか、デジタルインフラを所管する。
BMWi	連邦経済エネルギー省。 2005 年 11 月に発足。主な役割は、ドイツ経済の持続的成長及び競争機会提供雇用創出、経済競争力の確保ため新技術及び革推進等である。情報通信政策も行っている。
German Chancellery	ドイツ首相府。 デジタルアジェンダに対して責任がある。
BSI	連邦情報セキュリティ庁。 情報セキュリティに関する政府の管轄機関であり、IoT セキュリティ及びサイバーセキュリティに関する規制を行っている。
BNetzA	連邦ネットワーク庁。 2005 年 7 月に発足。電気、ガス、通信、郵便のほか、2006 年 1 月からは鉄道を含む社会インフラ全般を所掌している。

表 5-24　ドイツにおける関連法制度

Act on the Federal Office for Information Technology (BSI Act)	ドイツにおける電気通信法。
TKG	通信の機密性の保護や個人データの漏洩の防止等に関する法律。

5.2.2.6.2 対応状況

a. IoT セキュリティ全般

ドイツにおけるサイバーセキュリティ固有の制度としては主に、重要インフラのオペレーターまたはオンラインサービスに関して、あるいは IoT 及び情報通信技術におけるネットワークシステムの観点から規定されている [1]。また、これらとは別に IoT や情報通信技術のネットワークシステムにおける一般的なサイバーセキュリティに関して、商法やプライバシー法等によっても規定されている [2]。

サイバーセキュリティの観点では、BSI の法的根拠・権限・能力に関して規定している BSI Act がある（BSI Act は IT Security Act 及び EU の NIS 指令を施行し、取り入れた制度に相当）[3]。BSI Act では、政府、民間それぞれに対して次のことがらを規定している [4][5][6]。政府における情報セキュリティ問題に対する、代表的な BSI の権限・能力に関しては、①セキュリティや攻撃に関する情報収集・評価の権限、②通信データの収集・収集・評価・保管・使用・処理する権限、③有害なソフトウェア等に関して組織または一般市民へ警告し、情報を伝達する権限、④セキュリティを担保するための最低基準（Minimum Standards（詳細は後述））を策定し、適切な製品を開発・利用できるようにする権限、⑤政府の IT システムに関して Minimum Standards を規定する義務が規定されている（詳細は、下記を参照）。

- 政府及び関連機関において、情報技術のセキュリティギャップ及び成功した・試みた攻撃に関する情報を収集・評価する権限を有する（Article 4）
- 政府の通信インフラに対する将来的なサイバー攻撃を回避するために、プロトコルデータ及び政府の通信技術のインターフェースから発生するデータを収集・評価・保管・使用・処理する権限を有する（Article 5）
- 情報技術の製品・サービスにおけるセキュリティギャップ及び有害なソフトウェアに関して、影響を受ける組織または一般市民へ警告し、情報を伝達する権限を有する（なお、事前にメーカーに通知し、その後一般へ公開）（Article 7）
- 脆弱性を有する IT の構成要素をもつ不適切な製品が政府のシステムやネットワークで使用されるのを防ぐために、政府の情報技術のセキュリティを担保するための Minimum Standards を策定し、必要に応じて適切な製品を開発・利用できるようにする権限を有する（Article 8）
- 政府の IT セキュリティを強化するために、政府の IT システムに関して Minimum Standards を規定する義務を有する（Article 8 段落 1）

民間企業（特に重要インフラのオペレーター及びデジタルサービスプロバイダー（オンラインマーケット・検索エンジン・クラウドサービス））に適用する IT セキュリティに関する規制については別途、詳細を後述する。

また BSI は、サイバーセキュリティに関する様々な奨励事項（Recommendations）を提供しており、公的機関・企業における情報セキュリティ問題への対処方法や情報技術の使用者へ向けた技術的なサポートを提供している奨励事項である BSI-Standards を規定しており、表 5-25 に示す項目が含まれる[41]。BSI-Standard 100-1 は、ISMS の一般的な要件を規定している。BSI-Standard 100-2 では情報セキュリティマネジメントの設定や実際の運用についての方法論が記載されており、それに基づいたリスクを分析する方法が BSI-Standard 100-3 に記載されている。BSI-Standard 100-4 では、機関及び企業の事業継続マネジメントシステムの開発・確立等に関する体系的な方法論が提示されている。Threats Catalogue には、BSI-Standard 100-2 及び BSI-Standard 100-3 を適用するための基本的な脅威情報が記載されている。

表 5-25　BSI-Standards の規定内容

規定されている項目	規定されている内容
BSI-Standard 100-1 (ISMS)Information Security Management Systems	ISMS の一般的な要件が規定されている。ISMS では、情報セキュリティの確保を目的としたタスク及び活動を管理するために、管理者が使用すべき方法・手段が定められている。
BSI-Standard 100-2 IT-Grundschutz Methodology	情報セキュリティマネジメントの設定や実際の運用についての方法論が記載されており、実用的なセキュリティコンセプトの策定方法、適切なセキュリティ対策の選択方法、及びセキュリティコンセプトを実装する際の重要な点等が規定されている。
BSI-Standard 100-3 Risk Analysis based on IT-Grundschutz	IT-Grundschutz に基づいて、リスクを分析する方法が記載されている。IT-Grundschutz とは BSI が開発した情報セキュリティの基盤を指し、組織のあらゆる種類の情報に対し、適切なレベルのセキュリティを確保することを目的としている。例えば、IT-Grundschutz Standards（BSI-Standards と同義）、IT-Grundschutz Catalogues（IT 環境における脆弱性の検出及び攻撃への対処に関する有用な情報を提供する文書集）、及び認証制度の一つである IT-Grundschutz Certification（後述）が挙げられる [44]。

BSI-Standard 100-4 Business Continuity Management	機関及び企業の BCMS（事業継続マネジメントシステム: Business Continuity Management System）の開発・確立等に関する体系的な方法論が提示されている。
Threats Catalogue – Elementary Threats	IT-Grundschutz methodology (BSI-Standard 100-2) 及び Risk Analysis based on IT-Grundschutz (BSI-Standard 100-3) を適用するための基本的な脅威情報が記載されている。

さらに、BSI はサイバーセキュリティに関する様々な奨励事項を提供しており、例えば Protection of Critical Infrastructures - Basic Security Concept では、自然災害・テロ攻撃・犯罪行為に対する重要インフラの脆弱性を減少させることを目的とし、様々な保護対策に関する基本的なセキュリティコンセプト及び保護に関する奨励事項を規定している [13]。また、Cyber Security Requirements for Network-Connected Medical Devices では、ネットワークに接続する医療機器のメーカーに関するベストプラクティスをまとめており、最新技術に準拠した適切なレベルのサイバーセキュリティの実装及び保守のサポートを目的とした奨励事項を記載していたり [14]、Secure Provision of ISP-Services - Guidance for ISP (Internet Services Providers) (Sichere Bereitstellung von ISP-Dienstleistungen - Handlungsempfehlungen für Internet-Service-Provider (ISP)) では、インターネットサービスプロバイダーに対して、個人データの処理方法等に関する基本的な奨励事項等を提供していたりする [15]。さらに、Secure Webhosting - Guidance for Webhosting Services Providers (Sicheres Webhosting - Handlungsempfehlungen für Webhoster) では、Web ホスティングにおけるセキュリティを向上させるための奨励対策等を記載していたり [16]、Defense against DDoS attacks (Abwehr von DDoS-Angriffen) では、DDoS 攻撃の影響を軽減するための防御策について解説していたりする [17]。

各セクターにおいても間接的にネットワークのサイバーセキュリティに関して追加の要件が規定されており、例えば金融セクターでは、BaFin が BAIT (Supervisory Requirements for IT in Financial Institutions) 及び VAIT (Supervisory Requirements for IT in Insurance Undertakings) という回状 (circular letter) を規定しており、BAIT では金融分野における重要インフラの運用方法や BSI Act に準じた詳細な仕様について記載しており、VAIT では保険業界における要件を規定している [23]。

BSI は、IT 製品やセキュリティに関する基準及び認証制度についても規定を行っており [7]、その一つとして、コモンクライテリア (CC) に基づいた認証制度である Certification to CC（Zertifizierung nach CC）を規定している。CC とはコンピュータセキュリティの国際規格で、IT 製品・情報システムに関する情報セキュリティを評価・認証する基準を定めている。この認証を取得することで製品の競争力が向上するとされている。また CC は国際協定を含むため、他国で同一製品の認証を再度受ける必要がなくなる。認証プロセスについては以下の通りである。

- メーカーもしくは販売業者が認証を申請する。
- BSI の認定を受けたテストセンター（テストセンターのリストは公開されている [45]）が、BSI が公開している、もしくは一般的に認可されている IT セキュリティ基準（12 項目）に基づいて評価を実施する。この評価はテストセンターの従業員によって行われ、一貫したアプローチ及び方法論が保証されている。
- 認証の結果をテストセンターが認証報告書 (certification report) に記録する。その報告書には、製品の安全に関する説明・評価の詳細・消費者へのアドバイス等が含まれる。証明書及び認証報告書は BSI が発行し、申請者の同意の下、公表される。

認証に必要な費用は、テストセンターにおける技術評価に関する費用及び BSI への手数料が含まれており、前者については各テストセンターで金額が異なり、具体的な費用は不明である。後者については製品の種類及び認証レベル (EAL) によって異なり、1,200 ユーロ

から 20,420 ユーロであるとされている。ここで EAL は CC で定められている情報セキュリティの厳格さを評価する指標であり、EAL1（低）から EAL7（高）までの 7 段階が存在する。この制度で認証を受けた製品リストは公開されており、現在までに約 770 製品が認証を受けている [45]。

BSI は IT-Grundschutz（上述）の実装を目的とし、主に ISMS に関する認証制度である IT-Grundschutz Certification を導入しており、この認証を受けると ISO 27001 を取得できる。また、手続きに関する一連の基準は IT-Grundschutz methodology や IT-Grundschutz Catalogues によって定められており、その認証プロセスについては以下の通りである。

- BSI により発行されたライセンスを保持する外部監査機関が監査を実施する。外部監査機関が BSI のライセンスを取得するには、IT セキュリティ分野における最低 2 年間の専門的経験及び IT-Grundschutz に関連するプロジェクトに最低 3 件携わったことを示す証拠を提出した上で、資格制度に関するトレーニングに参加する必要がある。
- 監査機関が監査結果のレポートを BSI の認証部門に提示し、BSI が認証の授与の是非を決定する。

企業や政府機関はこの認証・監査を受けることで、情報セキュリティへの取り組みを外部に示すことができ、競争優位性を得ることができる [42]。

また、BSI はクラウド認証についても規定しており、その一つとして、C5 に基づいた認証を提供している。C5 は BSI が発行するクラウドサービスプロバイダーが満たすべき要件について概説されたカタログであり、17 個のトピック（暗号化やセキュリティポリシー等）に渡って記載されている。記載されている要件は、ISO/IEC 27001（組織内での ISMS の確立・実行・維持・改善に関する要件を規定）等を踏襲しており、必要に応じて BSI が要件を追記している。C5 に基づいた認証に強制力はないものの、認証の取得により、クラウドサービスプロバイダーにとっては顧客とのリレーションの確立に、また顧客にとっては適切なクラウドサービスプロバイダーの選択に資するとされている。認証プロセスについては以下の通りである。

- 公認監査機関（public auditor）が C5 に基づき監査を実施する。元来、大部分のクラウドサービスプロバイダーでは年次監査が義務付けられており、その一環として IT システムの監査が行われていたことを利用し、これを拡張して適用する。
- 基準をクリアした場合、監査を担当した公認監査機関が認証を発行する。

また、クラウドサービスに対する認証制度は他にもあり、代表的なものとして CSA STAR（クラウドサービスプロバイダーのセキュリティ対応に関する透明性の確保に向けた活動を行う Cloud Security Alliance（CSA）が公開しているベストプラクティスに準拠した認証）等が挙げられる他、IT-Grundschutz Certification 等も利用されている [11][12][39][40][42]。

b. 重要インフラ

重要インフラについては、民間企業に適用する IT セキュリティの規制の一環として、BSI Act に基づき、主に重要インフラのオペレーター及びデジタルサービスプロバイダーに対する規制を規定しており、具体的には以下の内容を含んでいる [5][6]。

主に重要インフラのオペレーターに関する規制:

- 重要インフラのオペレーターは、2 年ごとに BSI へ最新の IT セキュリティに準拠していることを通知し、情報技術システムの可用性・完全性・信頼性・機密性へ影響を及ぼすインシデントを回避するために適切な組織的・技術的な措置を講じていることを示

さなければならない（Article 8a 段落 1、 段落 3）
- BSI は、重要インフラのオペレーターが Article 8a 段落 1 の要件に準拠しているかについて監査する権限を有する（Article 8a 段落 4）
- BSI は、重要インフラのオペレーターが Article 8a 段落 1 の要件を遵守していることを証明できるようにするために、セキュリティの監査及び認証に関する詳細事項を決定する権限を有する（Article 8a 段落 5）
- 重要インフラのオペレーターは、もし提供サービスへ影響が生じるような重大な IT インシデントが発生した場合、BSI へ通知する義務を有する（Article 8b）
- もし重要インフラのオペレーターが、通知義務が課されている IT インシデントの影響を受けた場合、BSI は必要に応じて、IT 製品・システムに対応するメーカーに対しても協力を要請する権限を有する（Article 8b）
- BSI は、IT 製品のセキュリティを調査する権限を有する

デジタルサービスプロバイダーに対する規制:
- デジタルサービスプロバイダーは、セキュリティインシデント及び潜在的な悪影響を防止・最小化するために、予防策及びネットワーク・情報システムに影響を与えるセキュリティリスクを抑えるための適切な技術的・組織的な措置を講じなければならない（ただし、中小企業等例外も存在することに留意（Article 8d 段落 4））（Article 8c）
- デジタルサービスプロバイダーが講じる措置は、欧州委員会が策定した規制（Directive (EU) 2016/1148）または BSI Act による BMI に関する規制（Article 10 段落 4）に詳述されている内容に準ずるべきである。
- デジタルサービスプロバイダーは、インシデントが発生した場合、BSI へ速やかに通知する義務を有する。また、デジタルサービスプロバイダーが規定されたセキュリティ要件に準拠していることを担保するために、BSI は調査及び介入を行う権利を有する（Article 8c 及び 8e）。

また、通信サービスプロバイダー及びネットワークオペレーターに関しては、BNetzA が TKG を規定しており、通信サービスプロバイダーは、（ⅰ）通信の機密性の保護、（ⅱ）最新技術を考慮した個人データ漏洩の防止、に関して技術的な措置を講じなければならないとしている（Article 109 (1)）[18]。また、公共通信ネットワークオペレーター及び公的な利用が可能な電気通信プロバイダーは、（ⅰ）外部攻撃・災害によって引き起こされる重大な影響を伴う障害に対する保護、（ⅱ）通信ネットワークサービスのセキュリティに対するリスク管理に関する技術的対策、を講じなければならないとしており、この措置は特に不正アクセスから保護し、最新技術を考慮しなければならないとしている（Article 109 (2)）。さらに TKG では、実施された措置はセキュリティの観点から文書化されなければならないとしている他（Article 109 (4)）[19]、特別なセキュリティインシデント及びデータ漏洩の発生時に、その旨を BSI・BNetzA・BfDI に通知する義務を規定している（Article 109 (5)）[20]。

また、BSI は重要インフラの各分野に関するガイドラインを複数提供しており、例えば、データセンター・サーバーファーム・コンテンツ配信ネットワークに関する業界固有のセキュリティ規格である KRITIS sector specific security standard for data centres, server farms and content delivery networks があり、これらに基づき、重要インフラの各セクターに関するセキュリティの適合性に関して規定している [9][10]。さらに、テレメディアサービスについても、BSI が奨励事項である Protection of telemedia services in accordance with technical state of the art を規定しており、不正使用・妨害・外部攻撃からテレメディアサービスを保護するため、最新技術に準拠してサービスを運用する方法に関して記載している [22]。

なお、重要インフラに関して調達に特化したサイバーセキュリティ関連の制度は規定されていない [30]。

c. 政府調達

政府調達については、BSI が、BSI Act (Article 8) に基づき政府の情報技術のセキュリティを担保するための最低基準とされている Minimum Standards を規定している。Minimum Standards は、BSI の技術的専門知識及び政府機関におけるセキュリティはこの基準を下回ってはならないとの確信に基づいて定義されており、政府の IT セキュリティ要件を規定することにより、異なる分野の政府機関においてサイバー攻撃の効果的な保護対策に関する統一基準を確立することが目的とされている。Minimum Standards は様々なトピックに関して定められており、具体的には、外部クラウドサービス・モバイルデバイスマネジメント・安全な Web ブラウザ等について規定されている。この基準では、ハードウェア・ソフトウェア・ネットワーク等の技術的要素は勿論、テクノロジーに纏わる組織・人的資源等の観点からも要件を指定できるとされている。基準の策定は、有効かつ効率的に策定・モニタリングするために標準化された手順に準拠しており、この手順の一環として、政府との協議を含む複数の審査サイクルが存在し、各政府機関は基準のドラフトにコメントすることで策定に参加できる。具体的には下記のように、三つのフェーズ（機関内策定、外部コンサルテーション、公開後の適用フェーズ）に大別され、さらに細分化すると七つのフェーズ（Pre-α、α、β、RC (Release Candidate)、R (Release)、◿、RfC (Request for Charge)）で構成されるライフサイクルによって策定を行っている。

1. 機関内策定（the in-house development）
   I. Pre-α：最初に、新しい最低基準に関するトピックを特定する。
   II. α：その後、基準の担当部門と該当分野の専門部門がドラフトを作成し、BSI 全体で合意がなされた後、BSI がファーストドラフトを作成する。
2. 外部コンサルテーション（the external consultation procedure）
   III. β：次に外部コンサルテーションフェーズに入り、BSI は政府機関にドラフトを展開するとともに Web サイトに公開する。これにより、対象機関やその他関心のある専門家がドラフトに対してコメントすることが可能になり、専門知識を基準の策定に反映させる機会を設ける。
   IV. RC: βにおけるコメントをドラフトに反映させ、セカンドドラフトを作成し、その内容について BSI 内で最終合意・承認がなされる。
   V. R: その後、その内容について BSI の Web サイトで公開され、実施のために各政府機関に展開される。
3. 公開後の適用フェーズ（the use phase after publication）
   VI. ◿: 公開後もライフサイクルは継続され、BSI は基準の適用状況に関する分析・精査によるサポート・モニタリングを実施する。
   VII. RfC: これにより、項目を修正する必要が生じた場合（技術的な動向が変化した場合等）、公表された基準の見直しを行うことができる。

このように Minimum Standards は、フィードバックや批評が、積極的かつ継続的に行われるプロセスを通じて規定されている。Minimum Standards は連邦政府を対象に策定されているが、連邦政府以外においても適用できるように規定されているため、州政府等にも適用可能である [43]。

さらに BSI は、IT 製品の認証制度も規定しており、TR に準拠した認証である Certification to TR (Zertifizierung nach TR) を提供している。この認証は、国家安全保障上セキュリティの担保が重要とされている分野において使用される IT 製品・システムに適用されており、例えば暗号化メカニズムや公式文書の送信に関するガイドライン等が規定されている。ここで TR の対象は、IT システムの導入・保護に関わるすべての関係者とされており、調達への入札の観点から製品の適合性を評価する際にも適用可能である。この認証を取得することで、製品が他の認証済みの製品と互換性をもち、あらゆる準拠システムに統合可能であることの証明となる他、機密性が高く、特に政府によって使用される製品（電

子 ID、医療システム等）については、政府契約を結ぶための重要な要素となる。また、市場における競合優位性の獲得にもつながることもメリットに含まれる。認証プロセスについては以下の通りである。

- BSI の認定を受けたテストセンター（テストセンターのリストは公開されている [47]）が TR の定義に基づいて適合性評価を実施する。特定の評価分野においては、TR 監査の代わりに、BSI の認可を受けた機関または人物（通常、CC 認証を受けたテストセンターや、BSI 認証を受けた監査機関が該当（テストセンターのリストは公開されている [47]））が適合性監査を行う。
- 評価が正常に完了すると、BSI が適合性確認書（conformity confirmation）及び証明書（certificate）を授与する。

この制度で認証を受けた製品リストは公開されており、現在までに約 270 製品が認証を受けている [8][27][47]。そのほか、BMI が No-Spy Regulation (No-Spy-Erlass) を制定しており、入札手続きの間に、入札者自身及び製品が外国の諜報機関へ機密データの転送を行わないことを宣言しなければならないと規定している [26]。法律事務所の見解によると、BSI はこれまで調達に特化したガイドラインを発行しておらず、さらに、公共の調達手続きの文脈において、公的機関が一般的な技術的ガイドラインをどの程度遵守しなければならないかについては不明であるとされている [28]。

5.2.2.6.3 今後の方向性

a. IoT セキュリティ全般

IoT セキュリティ全般の動きとして、ドイツ政府は、サイバーセキュリティ分野において高度なイノベーションを伴う意欲的な研究開発プロジェクトへの資金供給及び促進を目的として、Agency for Innovation in Cyber Security の設置の決定を行った（2018 年 8 月 29 日の BMI の公式プレスリリース）。この機関は BMVg 及び BMI が管轄を行うとされているが、研究及び新しい基準等のより具体的な情報に関しては現在のところ不明である [25]。

また、現在策定中の認証制度として、BSI は Certification to CC の代わりに製品の安全性を認証する BSZ の制定を進めている。この認証制度では、Certification to CC と比較して認証の柔軟性は低くなるものの、それと引き換えに、評価時間の短縮及び文書要件の削減が実現される。認証プロセスについては以下の通りである [48]。

- BSI の認証を受けたテストセンターが、メーカーが約束したセキュリティ性能の達成に関する評価及び侵入テストを組み合わせた技術評価を実施する。各評価は一貫したアプローチ及び方法論を担保するため、テストセンターの従業員によって行われる。
- 評価に合格すると、認証機関が安全性証明書（safety certificate）及び認証報告書（certification report）を発行し、申請者の同意の下、公表される。

BSZ は現在パイロットフェーズであり、終了後の 2019 年に申請を受け付ける予定である。また、BMI の Horst Seehofer 大臣は、ドイツで販売されている IT 製品に対して、BSI によって発行された認定証明書を必須とする法律の制定の意向を示している [31]。

b. 重要インフラ

重要インフラについては、BSI Act に取り入れられている IT Security Act が IT Security Act 2.0 として、今後数ヶ月以内に立法機関による討議の対象となりうるとされており、以

下の内容を含む可能性がある（ただし、情報源は非公式なものであることに留意）（2019 年 2 月 28 日時点）[24]。

- BMI が重要インフラとして定義している法的規制（Regulation for the determination of critical infrastructures according to the BSI（(KritisVO) BSI-Kritisverordnung) [38]）をさらに多くの産業分野に拡大し、企業が重要インフラのオペレーターとして分類される基準を引き下げる。
- 対象範囲を、メーカーやサプライヤーを含むサプライチェーン全体に拡大する。
- ハードウェア・ソフトウェアプロバイダーに対して IT 製品の欠陥を報告する義務を課す。
- BSI に対して、セキュリティ対策に纏わる違反を行った組織のモニタリング及び罰則の指令に関して、より多くの能力・権限を付与する（BSI は既に一定の罰金を課す権限を与えられていることに留意（BSI Act Article14) [37]）。これにより、BSI はサイバー攻撃から重要インフラを保護するための規定を追加できるようになるとされている [32]。

さらに、大部分の重要インフラのオペレーターは不審なオンライン行動を政府に対して定期的に報告していない現状を受け、政府はそのような行動を察知した場合に自動的に通知する共有データバンクの整備の意向を示している [33]。

c. 政府調達

政府調達に関して新たな制度制定の動きは現在のところ見受けられない [29]。

ア） 略称名称一覧（各カテゴリのアルファベット順）

カテゴリ	略称	正式名称
制度	B3S	sector specific security standard
	BAIT	Supervisory Requirements for IT in Financial Institutions
	BSI Act	Act on the Federal Office for Information Technology
	BSZ	Accelerated Security Certification
	CC	Common Criteria
	IT Security Act	Act to Strengthen the Security of Federal Information Technology
	KritisVO	BSI-Kritisverordnung
	SigV	Signaturverordnung
	TKG	Telecommunications Act
	TR	Technical Guidelines
	VAIT	Supervisory Requirements for IT in Insurance Undertakings
組織	BaFin	Federal Financial Supervisory Authority
	BfDI	Federal commissioner for Data Protection and Freedom of Information
	BMI	Federal Ministry of the Interior, Building and Community
	BMVg	Federal Ministry of Defense
	BMWi	Federal Ministry of Economic Affairs and Energy
	BNetzA	Federal Network Agency for Electricity, Gas, Telecommunication, Post and Railway
	BSI	Federal Office for Information Security
その他	5C	Cloud Computing Compliance Controls Catalogue
	BCMS	Business Continuity Management System
	ISMS	Information Security Management Systems
	ISP	Internet Services Providers
	KRITIS	Kritischer Infrastrukturen
	R	Release
	RC	Release Candidate
	RfC	Request for Charge

イ） 重要インフラの定義

ドイツにおける重要インフラの定義は energy、information technology and telecommunications、transportation and traffic、health、water、nutrition 及び finance and insurance の 7 分野であるとされており、その中でも欠損や機能障害が発生することにより、重大な供給不足や公衆安全への危険をもたらす社会的機能において重要な分野のことを指す [35][38]。

5.2.2.6.4 Evidence 及び原典

a. 法律事務所による回答

Germany

February 28, 2019

1. An overview of your jurisdiction's cyber security legislation and regulations, including both legally binding laws or non-binding guidance or principles, as they concern network systems for the "Internet-of-Things" and/or information and communication technology.

[Existing Legislation and Regulations]

General Remark

Cyber Security specific legislation and regulations (including both legally binding laws or non-binding guidance or principles) are relatively rare under German law. Such cyber security specific legislation and regulations is largely addressing cyber security aspects of operators of critical infrastructures and online services as defined by law on a more general level and are not directly, specifically and expressly addressing network systems for the "Internet-of-Things" and/or information and communication technology. [1] Irrespective thereof general cyber security aspects as those related to for the "Internet-of-Things" and/or information and communication technology network systems might be of relevance under further non-cyber-specific Germen law, e.g. civil and commercial law, privacy laws etc. [2]

The summary to follow exclusively summarizes the (general) cyber security legislation and regulations, including both legally binding laws or non-binding guidance or principles, as they - might in terms of the specifically requested maximum broad understanding, potentially directly or indirectly - apply for network systems for the "Internet-of-Things" and/or information and communication technology with respect to the respective topics to be answered. In addition it lists selected technical guidelines published in Germany and by the Federal Agency for Information Security ("*Bundesamt für Sicherheit in der Informationstechnik*"- hereinafter "**BSI**") in particular in order to meet the request to list and name technical "standards, requirements, equipment testing or certification system provided by the authority (potentially) applicable to IoT products or services for government procurement". Whether or not theses technical standards are indeed relevant to IoT products or services for government procurement and are exhaustively listed needs to be finally assessed by a technical expert having the necessary skills and experience to give a final evaluation in this respect. Non Cyber-

specific legislation and regulations are mentioned and referred to on a high level basis as it is reasonable for the understanding of the overall legal landscape in Germany.

Cyber Security Specific Legislation and Technical Standards

a) With respect to cyber security, the Act re. the Establishment of the Federal Agency for Information Security ("*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik",* hereinafter **"BSI Act"**), which regulates the legal bases, powers and procedures of the BSI), applies. The Act implements and incorporates the regulations of the Act to Strengthen the Security of Federal Information Technology effective as of July 25, 2015 (*"Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)"*, hereinafter **"IT Security Act"**) and the Act on the implementation of Directive 2016/1148 of the European Parliament concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) implemented on 10/05/18. [3]

In summary, the BSI Act regulates the following:
Competences of the BSI for German federal information security matters. This particularly, but not comprehensively, includes

- the right to collect and evaluate information about security gaps and successful or attempted attacks on the security of information technology on a federal level and relating to federal authorities (Article 4 BSI Act),
- the authority to collect, evaluate, store, use and process protocol data as well as data arising at the interfaces of the communication technology of the Federal Government in order to avoid future cyber security attacks on the Federal communication infrastructure (Article 5 BSI Act),
- that the BSI may pass on information and warnings about security gaps in information technology products as well as harmful software to the affected market participants or to the public. The product manufacturer must be informed in advance; thereafter the BSI might address the public (Article 7 BSI Act), and
- the authority to develop minimum standards for ensuring the security of federal information technology and, if necessary, to have suitable products developed and make them available
  (Article 8 BSI Act) to prevent unsuitable products with weak points or manipulated IT components from being used in the federal administration and in government networks.
- In order to strengthen the IT security of the federal administration, the BSI is obliged to develop minimum standards for IT-Systems of the federal administration (Art 8 para 1 BSIG). [4]

Main regulations of interest in the field of IT-Security, especially applying outside the federal administration (i.e. on private operations etc.):

- Operators of critical infrastructures (as defined by law - see below) must regularly (every two years) demonstrate to the BSI that they comply with the state of the art in IT security, which means in particular, to take appropriate

organisational and technical precautionary measures in order to avoid any disruptions to the availability, integrity, authenticity and confidentiality of their information technology systems (Article 8a para 1, para 3 BSI Act).

- BSI may audit operators of critical infrastructures on its compliance with the requirements of Art 8a para 1 BSI Act (as mentioned above; Art. 8a para 4 BSI Act).
- BSI might determine details re. (security) audits and certification allowing the operator of critical infrastructures to prove its compliance with the requirements of Art 8a para 1 BSI Act (as mentioned above; Art. 8a para 5 BSI Act)
- Operators of critical infrastructures must report any significant IT disruption to the BSI if such disruption can affect the availability of critical services (Article 8b BSI Act).
- If a critical infrastructure operator is affected by IT disruptions to be be reported, the BSI may, if necessary, also request the manufacturers of the corresponding IT products and systems to cooperate (Article 8b BSI Act).
- The BSI is allowed to examine IT products for their security. [5]

Special requirements for providers of digital services (i.e. online marketplaces, search engines and cloud computing services in terms of Article 2 para. 11 BSI Act and Art. 4 nos. 5, 17, 18, 19 Directive (EU) 2016/1148) (**"Digital Services Providers"**):

- Article 8c BSI Act requires Digital Services Providers to undertake appropriate and proportionate technical and organizational measures to address security risks that may affect their network and information systems and to take precautionary measures to prevent security incidents and to minimize potential impacts. Exceptions apply according to Article 8d para. 4 BSI Act, e.g. to small businesses.
- The measures to be taken are detailed either by implementing acts adopted by the European Commission in accordance with Directive (EU) 2016/1148 or by regulations of the German Federal Ministry of the Interior (Article 10 Paragraph 4 BSI-Act). In the meantime, the EU Commission has laid down such rules by the Implementing Regulation (EU) 2018/151 as of 30 January 2018 ("Implementing Regulation for Digital Services Providers") specifying the elements to be taken into account by Digital Service Providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has to be reported.
- Significant incidents must be reported to the BSI immediately. In order to ensure that Digital Services Providers comply with the required security standards, Article 8c and 8e authorizes the BSI to take investigative and intervening measures (e.g. to report on technical improvements or to direct the service

provider to take additional measures). [6]

For additional requirements re. telecommunications and telemedia services, see also Section 1 lit. b) and c) below. Besides, the BSI has published hundreds of pages of technical guidelines which (might potentially) apply o. cyber security of networks, security standards and information on certification, attestation and labelling [7], such as:

- **BSI Technical Guidelines:** The BSI Technical Guidelines address all players involved in the installation or safeguarding of (general) IT-systems. They complement the technical test specifications of the BSI and provide criteria and practices for conformity evaluations ensuring the interoperability of IT security components as well as the implementation of defined IT-security requirements. [8]
- **KRITIS sector specific security standard (B3S) for data centres, server farms and content delivery networks**: With the industry specific security standard (B3S) for data centres, server farms and content delivery networks, the BSI has determined the suitability of the first security standard for the KRITIS information technology and telecommunications sector. The B3S "Industry-specific security standard for IT security" is therefore considered suitable for implementing the requirements of Article 8a para. 1 BSIG. [9]
- **KRITIS sector specific security standard (B3S) for food supply:** With the industry-specific security standard (B3S) for food supply the BSI has specified the second security standard for a KRITIS industry sector. [10]
- **Cloud Computing Compliance Controls Catalogue (C5)**: The Cloud Computing Compliance Controls Catalogue (abbreviated "C5") is intended primarily for professional cloud service providers, their auditors and customers of the cloud service providers. It is defined which requirements (also referred to as controls in this context) the cloud providers have to comply with or which minimum requirements the cloud providers shall be obliged to meet. [11]
- **Cloud Certification:** Certificates and attestations demonstrate evidence of the information security standard offered by a cloud provider. The basic idea behind certificates and/or attestations is that a cloud provider submits itself to a set of controls and can be audited by an independent third party verifying compliance with these controls. The audit is carried out on the basis of the audit scheme for the certificate/attestation and the audit result is documented in a defined format. The BSI's Cloud Computing Compliance Controls Catalogue (C5) can be attested via an ISAE 3000 audit which ends in a SOC 2 report in order to demonstrate

proof of compliance with the controls. This attestation, however, is not issued by the BSI, but by a certified public auditor. [12]

See links in Section "References" below for further detail.

Moreover, the BSI has published several more or less specific recommendations re. cyber security of networks, such as:

- **Protection of Critical Infrastructures - Basic Security Concept (*"Schutz Kritischer Infrastrukturen - Basisschutzkonzept - Empfehlungen für Unternehmen"*):** The goal of this document is to reduce the vulnerability of critical infrastructures to natural events and accidents as well as terrorist attacks and criminal acts. The Basic Security Concept focuses on structural, organizational, personal and technical protection measures and includes respective safeguarding recommendations. [13]
- **Cyber Security Requirements for Network-Connected Medical Devices (*"Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte"*):** This paper summarizes best practices for manufacturers of network-connected medical devices. The recommendations accompany regulatory requirements and are intended to support implementation and maintenance at an appropriate level of cyber security according to the current state of the art. [14]
- **Secure Provision of ISP-Services - Guidance for Internet Services Providers (ISP) (*"Sichere Bereitstellung von ISP-Dienstleistungen - Handlungsempfehlungen für Internet-Service-Provider (ISP)"*):** Internet service providers must take appropriate technical precautions and other protective measures in accordance with Article 109 of the German Telecommunications Act (*"Telekommunikationsgesetz"* - hereinafter **"TKG"**; see Article 1 lit. b) below for further detail). In consultation with the BSI, the Federal Network Agency has drawn up a catalogue of security requirements for the operation of telecommunications and data processing systems as well as for the processing of personal data as a basis for the security concept pursuant to Article 109 TKG (hereinafter **"Service Catalogue"**). In order to ensure the provision of the best possible service, various organizational measures must be implemented. The Guidance for Internet Services Providers provides some basic recommendations and a link to further details, in particular to the Service Catalogue. [15]
- **Secure Webhosting - Guidance for Webhosting Services Providers (*"Sicheres Webhosting - Handlungsempfehlungen für Webhoster"*):** This recommendation paper is aimed to web hoster and addresses measures to improve security for web hosting customers. It is focused on the different phases of web hosting including basic security measures. [16]

- **Defense against DDoS attacks (*"Abwehr von DDoS-Angriffen"*):** This recommendation paper explains how to defend against Distributed Denial of Service (DDoS) attacks in order to mitigate consequences of respective attacks also in the event precautionary measures are missing or are deemed ineffective. [17]

See links in Section "References" below for further detail.

b) Telecommunication services providers and network operators are subject to special regulation under the TKG.

Telecommunication services providers have to implement technical measures for (i) the protection of telecommunication secrecy and (ii) to prevent personal data breaches which have to take into account the technical state of the art (Article 109 (1) TKG). [18]

Operators of public telecommunication networks and providers of publicly available telecommunications have to implement technical measures for (i) the protection against interferences with significant effects caused by external attacks and catastrophes and (ii) the control of risks for the security of telecommunication networks and services. The measure shall in particular protect against unauthorized access and have to take into account the state of the art (Article 109 (2) TKG). According to Article 109 (4) TKG the implemented measures have to be documented in a security concept. [19]

Article 109 (5) and Article 109a TKG contains special security incident and data breach notification obligations to the BSI, the German Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway ("*Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*", hereinafter "**Federal Network Agency**") and the Federal Commissioner for Data Protection and Freedom of Information ("*Bundesbeauftragter für Datenschutz und Informationsfreiheit*", hereinafter "**BfDI**"). [20]

c) According to Article 13 para. 7 of the German Telemedia Act (*"Telemediengesetz"*, hereinafter **"TMG"**), providers of telemedia services, meaning - as a rough guide - electronic services neither being telecommunications services nor being broadcasting services such as website operator, shall protect a telemedia service against unauthorized use, disturbances and external attacks. Respective arrangements must comply with technical state of the art, in particular a method of encryption recognized as being secure. [21]

For further specification and in addition to the publications listed above, see the BSI recommendation as to the protection of telemedia services in accordance with technical state of the art (*"Absicherung von Telemediendiensten nach Stand der Technik"*). This includes a recommendation how to operate telemedia services in accordance with

technical state of the art to protect a telemedia service against unauthorized use, disturbances and external attacks. [22]

d) Additional requirements (indirectly) affecting the cyber security of networks may also apply from a sector regulatory perspective, e.g. for financial and insurance institutions. Respective provisions do not constitute specific and detailed (technical) requirements related to cyber security for network systems. They are more driven by general financial regulatory means and, as such, based on an understanding of overall risk oriented supervision by public authorities.

As part of such regulatory requirements, the German Federal Financial Supervisory Authority (*"Bundesanstalt für Finanzdienstleistungsaufsicht"*, hereinafter **"BaFin"**) has published a general, high-level framework of guidelines for the technical and organizational measures of financial institutions in terms of IT management including, inter alia, IT strategies, IT risk management, IT security management (including the appointment of a IT security officer) and user access management. The BaFin circular letter (*"BaFin Rundschreiben"*) 10/2017 as amended September 14, 2018 (*"BAIT"*) now also includes an additional Chapter 9 for the operation of Critical Infrastructures in terms and for further specification of the BSI Act regarding the financial sector.

Further, we include the BaFin circular letter 10/2018 (*"VAIT"*) in the Section "References" below as stipulating respective requirements for insurance companies whereas, in particular, also technical state of the art shall apply (see Section II.4.27 VAIT). [23]

[Forthcoming Legislation and Regulations and Discussions on Future Trends]

a) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (12/09/18).

b) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cyber security certification (**"Cybersecurity Act"**) (04/10/17).

c) An "IT Security Act 2.0" (**"IT Security Act 2.0"**) might become subject to discussions of legislative bodies in the upcoming months. Such IT Security Act 2.0 might particularly contain the following according to unreliable, not official, inconsistent and vague sources:

- extension of the German Federal Ministry of the Interior's legal regulation (*"BSI-Kritisverordnung"* - hereinafter **"KritisVO"**) to further industry sectors and lowering the threshold for companies to be classified as critical infrastructure operators,
- scope might be extended to the entire supply chain including manufacturers and suppliers, and
- an obligation for providers of hard- and software to report deficiencies on IT products. [24]

Please be aware that this is neither a trend nor a guidance and no resilient, specific governmental discussions on such regulation are available to the public yet. Therefore, there are no official news articles or press releases existing as to that. An update of the IT security requirement framework is, for now, just phrased in the German Government's coalition agreement as a (theoretical) political intention. On that ground, one of the governmental parties published a position paper on a possibly new IT Security Act 2.0, as the only publicly available document on that topic (see Section "References" below).

d) According to an official press release of the German Federal Ministry of the Interior dated August 29, 2018, the German government has decided to establish an Agency for Innovation in Cyber Security with the purpose to finance and promote ambitious research and development projects with high innovation in the field of cyber security. More specific information, in particular about researches or new standards developed or published by the Agency for Innovation in Cyber Security is not available to knowledge, up to now. [25]

References:

- BSI Act:
  https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html
- Implementing Regulation for Digital Services Providers:
  https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0151&from=EN
- BSI Technical Guidelines:
  https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html
  https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TechnicalGuidelines_node.html
  https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/traenderungen_node.html

- KRITIS Sector specific security standard (B3S) for data centres, server farms and content delivery networks: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Kritis_IKT-Sicherheitsstandard_anerkannt_20062018.html
- KRITIS Sector specific security standard (B3S) for food supply: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Sicherheitsstandard_Lebensmittelhandel_16052018.html
- Cloud Computing Compliance Controls Catalogue (C5): https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_Catalogue/Compliance_Controls_Catalogue_node.html
- Cloud Certification: https://www.bsi.bund.de/EN/Topics/CloudComputing/CloudCertification/CloudCertification_node.html
- Protection of Criticial Infrastructures - Basic Security Concept (*"Schutz Kritischer Infrastrukturen - Basisschutzkonzept - Empfehlungen für Unternehmen"*) https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/PublikationenKritis/Basisschutzkonzept_Kritis.pdf;jsessionid=5F43692B50A360577B83BCAD7309E73D.1_cid345?__blob=publicationFile
- Cyber Security Requirements for Network-Connected Medical Devices (*"Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte"*):(English Available) https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_132E.pdf?__blob=publicationFile&v=5
- Secure Provision of ISP-Services - Guidance for Internet Services Providers (ISP) (*"Sichere Bereitstellung von ISP-Dienstleistungen - Handlungsempfehlungen für Internet-Service-Provider (ISP)"*): https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_114.pdf?__blob=publicationFile&v=3
- Secure Webhosting - Guidance for Webhosting Services Providers (*"Sicheres Webhosting - Handlungsempfehlungen für Webhoster"*): https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_068.pdf?__blob=publicationFile&v=3
- Defense against DDoS attacks (*"Abwehr von DDoS-Angriffen"*): https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_002.pdf?__blob=publicationFile&v=3
- Telecommunications Act (*"Telekommunikationsgesetz"*): https://www.gesetze-im-internet.de/tkg_2004/

- Telemedia Act (*"Telemediengesetz"*): https://www.gesetze-im-internet.de/tmg/TMG.pdf
- Protection of telemedia services in accordance with technical state of the art (*"Absicherung von Telemediendiensten nach Stand der Technik"*): https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_125.pdf?__blob=publicationFile&v=7
- BAIT: https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.html
- VAIT: https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1810_vait_va.pdf?__blob=publicationFile&v=4
- Regulation proposal: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2018:0630:FIN:EN:PDF
- Proposal on "Cybersecurity Act": https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0477R(01)&from=D
- Position paper of the SPD parliamentary group in the Bundestag on an IT Security Act 2.0: https://blogs.spdfraktion.de/netzpolitik/files/2019/01/IT-Sicherheitsgesetz-2.0_DigitalesImmunsystem.pdf
- Press release of the German Federal Ministry of the Interior dated August 29, 2018 as to establishment of an Agency for Innovation in Cyber Security https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2018/08/cyberagentur.html

2 Details of your jurisdiction's cyber security-related regulations relevant to procurement of goods in the following sectors

(a) Government (national security, defense, police, fire station, tax, academic research, etc.)

[Existing Legislation and Regulations]

aa) No-Spy Regulation by Federal Ministry of the Interior: During tender procedures bidders must make declarations that they and their products will not conduct secret transfers of confidential data to foreign intelligence services. [26]

bb) The BSI may provide technical guidelines to be considered by federal authorities when assessing the suitability of bidders and IT products in the context of procurement tenders (Article 8 para. 2 BSI Act). [27]
According to documents accompanying the legislation procedure (cf. BT-Drs. 16/11967, p. 16), these guideline are intended to provide authorities handling procurement processes with information on how to develop and formulate suitability and performance requirements depending on the purpose of the information technology and appropriate to the involved risks. Any such guideline shall not affect other general and non cyber specific public procurement laws, especially the provisions of the Act against Restraints of Competition (*"Gesetz gegen Wettbewerbsbeschränkungen"*, hereinafter **"GWB"**).
To our knowledge, no special procurement guidelines have been issued by the BSI to date. Further it is unclear to which extent the public authorities shall adhere to the general technical guidelines (see references in Section 1 of this document above) in the context of public procurement procedures. [28] It is also unclear whether or not Article 8 para. 2 BSI Act refers to special suitability requirements of the bidder (*"besondere Eingungsvoraussetzungen des Bieters"*) in terms of the Ordinance on the Award of Public Contracts (*"Verordnung über die Vergabe öffentlicher Aufträge"*, hereinafter **"VgV"**).
In response to a provisional inquiry about that questions and whether or not additional special procurement guidelines have been issued or are currently being worked out, the BSI did not provide any information but stated that this would require a specified written request.

cc) Irrespective of the aforementioned criteria, the issuer of a request for proposal is also free, but not requested by law, to request that the bidders' proposal complies to additional case-specific technical and security requirements. If a bidder does not comply with such requirements, the bidder can be excluded from the further tender procedure. Furthermore, of course, the requirements of the statutory provisions (e.g. the GWB and the VgV) are to be observed, e.g. specific requirements for electronic communications are to be considered (Article 9, 19 and 53 VgV). Please note that these requirements are not cyber or network security specific characteristics, but part of the respective tender conditions.

[Forthcoming Legislation and Regulations and Discussions on Future Trends]
There is no forthcoming regulation or discussions. [29]

References:
https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2014/08/no-spy-erlass.html

http://dip21.bundestag.de/dip21/btd/16/119/1611967.pdf

(b) Critical infrastructure (telecommunication, electricity, transport, etc.)

[Existing Legislation and Regulations]

There is no cyber security-related specific to procurement of goods. General reporting obligations already elaborated in section 1 a) above. [30]

[Forthcoming Legislation and Regulations and Discussions on Future Trends]

Interior Minister Horst Seehofer wants to implement a law that IT products sold in Germany need a certification stamp issued by the bureau of IT security (Bundesamt für Sicherheit in der Informationstechnik). [31]

BSI will also be given more responsibilities in monitoring and fining agencies that violate security measures. This agency will also be able to add more stipulations to protect critical infrastructure from cyber-attacks. [32]

Because most operators of critical infrastructure do not regularly report any suspicious online behavior, the government wants to create a shared databank which would automatically inform the government of any attacks. [33]

Also, See Section 1 c) above.

※こちらは、https://www.tagesschau.de/inland/it-sicherheit-111.htmlを元に記載されたもので、この記事の位置付けは、Section 1のForthcoming Legislation、c)に言及されているIT Security Act 2.0の立法に向けた議論等を記載したものである。また、BSI Act Section 14の下で、既にBSIは一定の罰金を科す権限を与えられている。(https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf?__blob=publicationFile&v=4)。

References:

News Article from tagesschau.de (German National news agency) 2/22/2019
https://www.tagesschau.de/inland/it-sicherheit-111.html

3 The definition of Critical Infrastructure in your jurisdiction and list all the infrastructure falling into the scope of the definition.

According to Article 2 (10) of the BSI Act critical infrastructure shall mean facilities, equipment or parts thereof that are both:

- part of the sectors energy, information technology and telecommunications, transportation and traffic, health, water, nutrition, and the finance and insurance industries and
- are of high importance to the functioning of the community since their failure or

impairment would result in material shortages of supply or dangers to public safety. [35]

a) The critical infrastructure sectors as referred to in the BSI Act are defined in detail by the German Federal Ministry of the Interior by legal regulation (*"BSI-Kritisverordnung"*), as follows:

- Energy: Supply of electricity, gas, motor and heating oil, district heating
- Water: Supply of drinking water, wastewater disposal
- Nutrition: food supply
- Information technology and telecommunications: audio and data communications, data storage and data processing, including cloud services providers
- Health sector: inpatient medical care, the provision of directly life-supporting medical devices, that are consumer goods, the provision of prescription pharmaceuticals and blood and plasma concentrates for use in or on the human body, laboratory diagnostics
- Finance and insurance: cash supply, card-based payment transactions, conventional payment transactions, the clearing and settlement of securities and derivatives transactions, Insurance services.
- Transport and traffic: public provision of services for the transport of persons and goods

b) Whether or not a facility, equipment or part thereof is deemed to be of high importance to the functioning of the community as mentioned in number 2 above, specific thresholds set out in Annexes 1 to 7 of KritisVO apply and result from the calculation methods also stated therein.

References:

https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html (BSI Act, see Article 2 (10))

https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html (KritisVO)

4 In Germany, is there any case or precedent of prosecution or prohibition by the public authorities in connection with (i) the government procurement, (ii) procurement of telecommunication or other critical infrastructure or (iii) equipment or services for consumers? If yes, please provide brief description of each case with relevant sources.

No official statement available, but consider discussions on European Commission level as to exclusion of Chinese telecommunications providers from 5G network development activities due to security concerns as to network components. [36]

References:

https://uk.reuters.com/article/uk-usa-china-huawei-tech-europe/eu-considers-proposals-to-exclude-chinese-firms-from-5g-networks-idUKKCN1PO2MJ

b. 法律事務所による回答以外の情報ソース

- BSI Act [37]:
  - ✓ https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf?__blob=publicationFile&v=4
- KritisVO [38] :
  - ✓ https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/ITSiG/Neuregelungen_KRITIS/B3S/b3s.html
- C5 [39] :
  - ✓ https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_Catalogue/Compliance_Controls_Catalogue_node.html
  - ✓ https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_Catalogue/FAQ/FAQ_Audit_Report_node.html
  - ✓ https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Controls_Catalogue/FAQ/FAQ_Requirements_node.html
- Cloud Certification [40]
  - ✓ https://www.bsi.bund.de/EN/Topics/CloudComputing/CloudCertification/CloudCertification_node.html
- BSI-Standards [41]
  - ✓ https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html
  - ✓ https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile&v=1
- IT-Grundschutz Certification [42]
  - ✓ https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile&v=1
- Minimum Standards [43]
  - ✓ https://www.bsi.bund.de/EN/Topics/Minimum_Standards/Minimum_Standards_node.html
  - ✓ https://www.bsi.bund.de/EN/Topics/Minimum_Standards/FAQ_MST_EN/FAQ_MST_EN_node.html#faq12012696
  - ✓ https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards_Bund/Mindeststandards_Bund_node.html
- IT Grundschutz [44]
  - ✓ https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html
  - ✓ https://www.bsi.bund.de/cln_174/DE/Themen/ITGrundschutz/itgrundschutz_node.html
- Zer¬ti¬fi¬zie¬rung nach CC [45]
  - ✓ https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/ZertifizierteProdukte/Betriebssysteme/Betriebssystem_node.html
  - ✓ https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/zertifizierungnachcc_node.html;jsessionid=B88A0848BE5C85272CD3994E69C96418.2_cid360
  - ✓ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_32_pdf.pdf?__blob=publicationFile&v=2
  - ✓ https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/Antraege/antraege_node.html

- ✓ https://www.security-insider.de/produkte-nach-common-criteria-cc-zertifizieren-a-343441/
- ✓ http://www.gesetze-im-internet.de/bsi-kostv_2005/anlage.html
- ✓ テストセンター：https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Stellen/ITSEC_CC/CC_Liste/CC_Liste_node.html
- ✓ 認証製品：https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/ZertifiziierteProdukte/zertifizierteprodukte_node.html

- Be¬stä¬ti¬gung SigG [46]
  - ✓ https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/BestaetigungnachdemSignaturgesetz/ListebestaetigterProdukte/listebestaetigterprodukte_node.html
  - ✓ https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/BestaetigungnachdemSignaturgesetz/bestaetigungnachdemsignaturgesetz_node.html;jsessionid=3F12356B82F84DAE84E47A6CCF175667.1_cid351
  - ✓ https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/BestaetigungnachdemSignaturgesetz/bestaetigungnachdemsignaturgesetz_node.html;jsessionid=3F12356B82F84DAE84E47A6CCF175667.1_cid351
  - ✓ テストセンター：https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Stellen/ITSEC_CC/CC_Liste/CC_Liste_node.html
  - ✓ 認証製品：https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/BestaetigungnachdemSignaturgesetz/ListebestaetigterProdukte/listebestaetigterprodukte_node.html
- Zer¬ti¬fi¬zie¬rung nach TR [47]
  - ✓ https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachTR/ZertifiziierteProdukte/zertifizierteprodukte_node.html
  - ✓ https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachTR/ZertifiziierteProdukte/zertifizierteprodukte_node.html
  - ✓ https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachTR/Pruefbereiche/Pruefbereiche.html
  - ✓ https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachTR/Pruefstellen/Pruefstellen_Auditoren_node.html
  - ✓ https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html
  - ✓ https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TechnicalGuidelines_node.html
  - ✓ https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/traenderungen_node.html
  - ✓ テストセンター：https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachTR/Pruefstellen/Liste_TR-Pruefstellen/Liste_TR-Pruefstellen_node.html
  - ✓ テストセンター（特定分野）：https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktz

ertifizierung/ZertifizierungnachTR/Pruefstellen/Pruefstellen_Auditoren_node.html

- ✓ 認証製品：https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachTR/ZertifizierteProdukte/zertifizierteprodukte_node.html

- BSZ [48]
  - ✓ https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/Beschleunigte_Sicherheitszertifizierung/BSZ_node.html

5.2.2.7 スウェーデン

5.2.2.7.1 国としての全体的な状況(まとめ)

スウェーデンの政策動向の概要を表 5-26 に示す。

表 5-26　スウェーデンの政策動向（まとめ）

	項目	概要
現状	全体傾向	2016 年に国家サイバーセキュリティ戦略を公表、サイバーセキュリティ強化の動きが見え始めている。基本的には、EU と足並みを揃える形で強化を実施、EU における GDPR/NIS 指令はスウェーデン国内法に組み込まれた。
	重要インフラの法制度	NIS 指令を組み込んだ国内法 Lag（2018:1174）にて重要インフラ提供企業に対するセキュリティ要件やインシデント報告義務を規定している。重要インフラ提供企業にはデジタルサービス事業者も含まれており、サービス時に使用するネットワーク/情報システムのセキュリティ対処を義務付けている。
	政府調達	EU 指令を国内法に組み込み対応している。スウェーデンの安全保障関連の調達に関するプロセス/ルール等は、Protective Security Act（2018:585）に記載されており、この中で政府調達に伴うセキュリティ保護の調査実施やセキュリティ対策の計画・実施を求めている。
	認証/認定制度	スウェーデン国防省傘下の独立機関 CSEC が国防に関する IT 関連システムの認証を行っている。
	体制	法務省配下の SDPA が個人情報保護を主管、国防省配下の SCCA が市民や公共の安全の保護、重要インフラ事業者のセキュリティ保護を主管している。国防省配下で装備調達を主管する SDMA 配下の CSEC が国防に関する IT 関連システムの認証を主管している。
今後	全体的な傾向	EU の GDPR や NIS 指令等、EU の施策に沿ってセキュリティを強化していく。2017 年 12 月にスウェーデン防衛委員会が報告書「Resilience The total defence concept and the development of civil defence 2021-2025」にて、サイバーセキュリティに関する分析を実施、現在及び将来的なサイバー脅威に対処するための法律等が検討されている。
	重要インフラの法制度	EU の施策に沿っており、現状目立った動きはみられない。
	政府調達	同上。

スウェーデンでは、2016 年に国家サイバーセキュリティ戦略（A national cyber security strategy）が公表される等、サイバーセキュリティ強化の動きが見え始めている。EU において、サイバーセキュリティの強化が行われている動きに合わせて 2018 年 5 月には GDPR が、2018 年 8 月には EU の「ネットワークと情報セキュリティ指令（NIS 指令）」が国内の法律として取り入れられている。また、IT 機器やシステム関連の認証機関としては、スウェーデン国防省傘下の独立機関 CSEC が認証を行っている。

重要インフラについては、上述のように 2018 年 8 月に NIS 指令を国内の法律に取り込み、重要インフラ事業者が指定された。デジタルサービス事業者については、法律ではなく条例の形で取り込まれている。また、条例 Förordning（2018:1175）で重要インフラ事業者、

デジタルサービス事業者に指定された企業は、情報セキュリティのリスク管理やインシデントの報告義務、また、これらの義務を怠った場合の罰金も規定されている。

政府調達については、EU が 2014 年に交付した政府機関による調達と公共事業を行う事業体による調達に関する指令が、それぞれ法律 Lag (2016:1145)、法律 Lag (2016:1146) として組み込まれている。軍用製品等の調達である国防・安全保障に関する調達については、別の法律 Lag (2011:1029) が適用されている。

今後に向けては、GDPR や NIS 指令を国内に取り込んでおり、EU と歩調を合わせてサイバーセキュリティ強化に取り組んでいるものと思われる。また、サイバー攻撃に関しては今後の国防に関わる課題として捉えられており、報道によるとサイバーセキュリティ対策を反映して、国防費も拡大傾向にあるという。また、スウエーデン政府のエネルギー・デジタル開発相は、国内の 5G ネットワーク構築にあたり、自国の国家安全保障上の脅威を与える可能性のある、サプライヤーや通信事業者を排除することが望ましいと発言している。

図 5-9 は、スウェーデンにおける政府関連組織と関連法制度をまとめたものである。番号により、組織と法制度の関連性を表現している（組織の概要は表 5-27 を、法制度の概要は表 5-28 を参照）。PTS (Swedish National Post and Telecom Agency) は、スウェーデンの郵便と電気通信に関する独立規制機関であり、「2003 年電気通信法」を所掌する機関でもある。Datainspektionen (Swedish Data Protection Authority) は MoJ（法務省: Ministry of Justice）に属する機関であり、GDPR に基づき、情報システムにおける個人情報の保護を主管している。MSB (Swedish Civil Contingencies Agency) は、MoD（防衛省:Ministry of Defence）に属する機関で市民や公共安全の保護を行い、NIS 指令に基づき重要インフラ事業者のセキュリティ保護を主管している。CSEC (Swedish Certification Body for IT-Security) は ISO/IEC 15408 (Common Criteria) に基づいて、IT 関連システムの製品とシステムのセキュリティに関する認証を主管している。

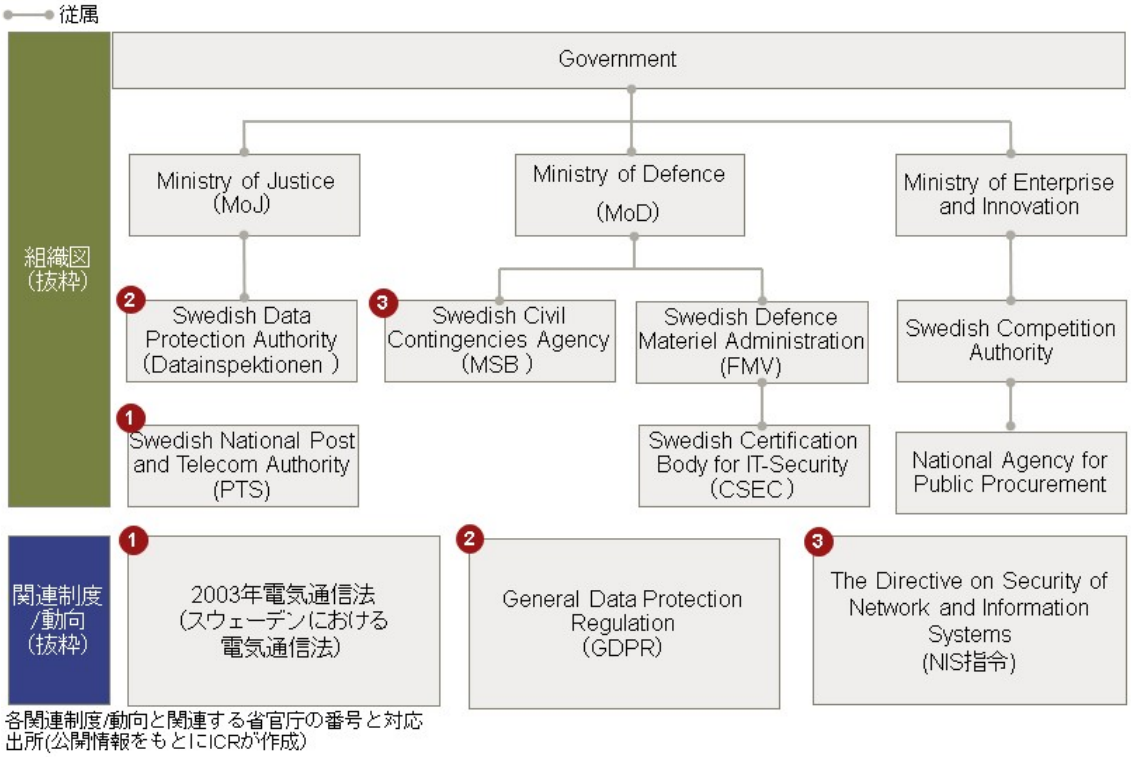


図 5-9　スウェーデンの政府関連組織と関連法制度

表 5-27　スウェーデンにおける政府関連組織

PTS	スウェーデンの郵便と電気通信に関する独立規制機関。「2003 年電子通信法」を所掌する。
MoJ	法務省。
Datainspektionen	情報システムにおける個人情報の保護を主管。
MoD	防衛省。
MSB	国防省に属する機関で、市民や公共安全の保護、また重要インフラ事業者のセキュリティ保護を主管。
FMV	防衛装備品の調達を実施。
CSEC	IT関連製品、システムの認証を実施。
Ministry of Enterprise and Innovation	ICT や電気通信分野に関する政策立案を実施し、国際協議では政府を代表。
Swedish Competition Authority	政府調達を監督。
National Agency for Public Procurement	政府調達を実行。

表 5-28　スウェーデンにおける関連法制度

2003 年電気通信法	スウェーデンにおける電気通信事業法。
NIS 指令	2016 年 8 月に EU で制定されたサイバーセキュリティに関する指令。 国内法 Lag (2018:1174) として取り入れられた。
GDPR	2018 年に EU で制定された、一般データ保護規則。 国内法 Lag (2018:218) として取り入れられた。

5.2.2.7.2 対応状況

a. IoT セキュリティ全般

スウェーデンでは、2016 年に国家サイバーセキュリティ戦略（A national cyber security strategy）が公表される等、サイバーセキュリティ強化の動きが見え始めている。国家サイバーセキュリティ戦略の中では、今後対応すべき 6 本の戦略的優先事項が示された。具体的には「サイバーセキュリティの取り組みにおける体系的かつ包括的な取り組みの確保」、「ネットワーク、製品、システムにおけるセキュリティの強化」、「サイバー攻撃等の IT インシデントの防止、検知、管理能力の強化」、「サイバー犯罪への防御と対抗力の強化」、「知識及び専門性の向上」、「国際協力の強化」である。EU において、サイバーセキュリティの強化が行われている動きに合わせて 2018 年 5 月には GDPR が、2018 年 8 月には NIS 指令が、それぞれ法律 Lag (2018:218)、法律 Lag (2018:1174) として取り入れられている。また、Datainspektionen (Swedish Data Protection Authority) が国内のデータ保護に関する機関として、GDPR に基づき、情報システムにおける個人情報の保護を主管している。

また、スウェーデン国内の IT 関連製品、システムの認証は、スウェーデン国防省参加の機関である FMV (Försvarets materielverk: The Swedish Defence Materiel Administration) 内部にある独立機関 CSEC が担当している。同機関は、標準の CC (Common Certification) のセキュリティ認証を行う。同機関が用いている認証基準としては、ISO/IEC 15408 を利用している (ISO/IEC 15408 は欧米 6 ヵ国 7 機関で構成される CC プロジェクトによって開発された共通基準)。

b. 重要インフラ

重要インフラについては、2018 年 8 月に EU の NIS 指令が組み込まれ法律 Lag (2018:1174) として発効された。同法律は重要インフラ事業者 (Operators of Essential Services) の定義を定めており、重要インフラ事業者は、社会や経済活動を維持するために重要なサービスを提供しており、インシデントの発生が社会に重大な混乱を招くことが予想される企業、としている。より具体的な分野については「エネルギー」、「交通」、「銀行業」、「金融市場インフラ」、「保険医療」、「飲料水の配給」、「デジタルインフラストラクチャー」と定められている。また、上記した分野のみならず、条例 Förordning (2018:1175) で DSP（デジタルサービス事業者: Digital Service Provider）も対象に含めている。MSB の Web サイトではより具体的な条件が示されており、「本社がスウェーデンにある企業」、「年間の売上高が 1,000 ユーロ以上」、「社員数が 50 人以上」が対象企業となっている。

重要インフラ事業者、デジタルサービス事業者に指定された企業は、情報セキュリティについて、図 5-10 に示す義務を求められる。

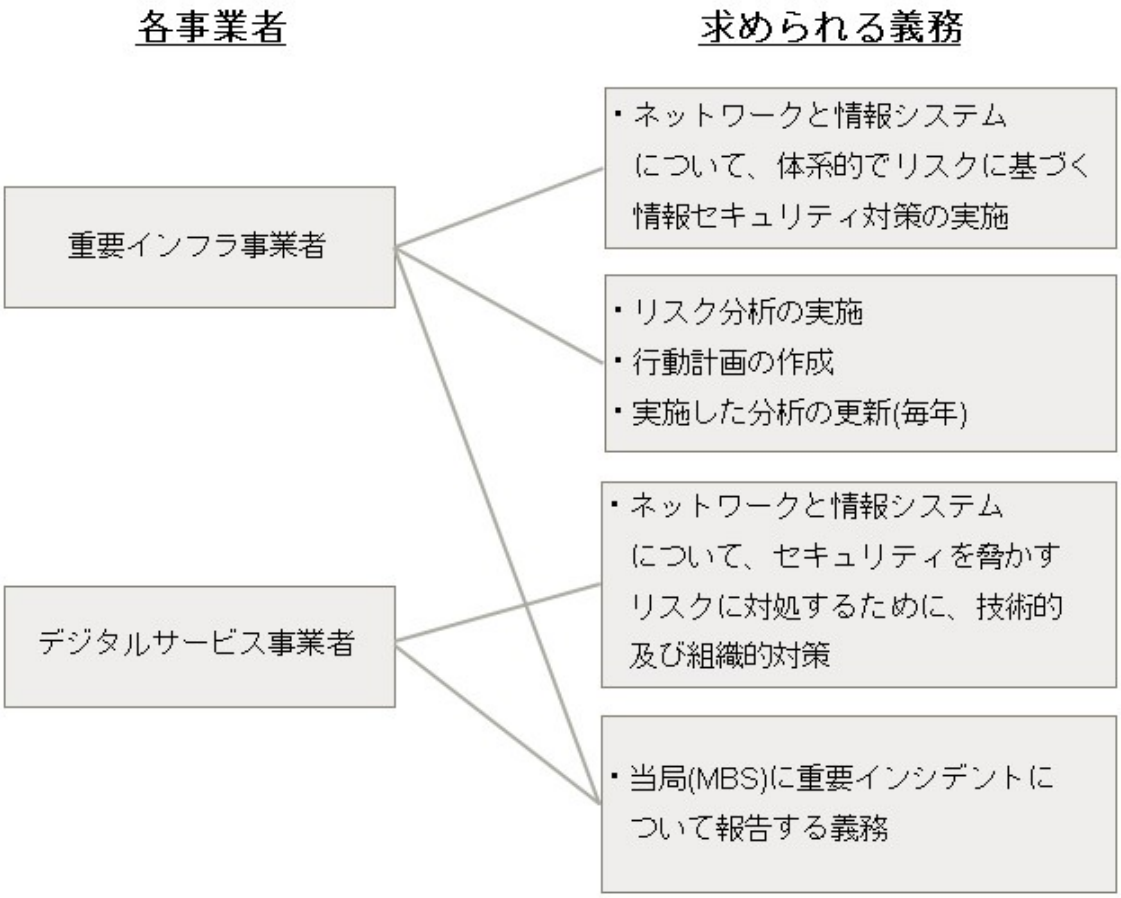


図 5-10　各事業者に求められる義務

重要インフラ事業者は、ネットワークと情報システムについて体系的でリスクに基づく情報セキュリティを実施する必要がある。また、セキュリティについてリスク分析を実施し、行動計画を作成する必要がある。さらに、実施した分析は毎年ドキュメント化し、更新することが求められる。

デジタルサービス事業者は、ネットワーク及び情報システムについてセキュリティを脅かすリスクに対処するために、技術的及び組織的対策を講じなくてはならない。

重要インフラ事業者、デジタルサービス事業者ともに、スウェーデン政府が設定した当局 (MSB) に重要インシデントについて報告する義務がある。表 5-29 に各分野の情報セキュ

リティを監督する省庁を示す。

表 5-29　各分野の情報セキュリティを監督する省庁

分野	監督省庁
エネルギー	Statens energimyndighet（スウェーデンエネルギー庁）
交通	Transportstyrelsen（スウェーデン交通局）
銀行業	Finansinspektionen（スウェーデン金融監督機関）
金融インフラ	Finansinspektionen（スウェーデン金融監督機関）
保険医療	IVO（スウェーデン医療福祉監督局）
飲料水の共有	Livsmedelsverket（スウェーデン食品庁）
デジタルインフラ	PTS（スウェーデン郵便電気通信庁）
デジタルサービス	PTS（スウェーデン郵便電気通信庁）

表 5-29 にある各省庁は規制、特にインシデントの報告とセキュリティ対策が遵守されているかを監視している。また、重要インフラ事業者、またデジタルサービス事業者から報告されるレポートは MSB が受け取る。また、重要インフラ事業者、デジタルサービス事業者がこれらの義務を怠った場合の罰金も規定されている。具体的な罰金の金額については、最低 5,000 クローネから最大で 10 万クローネに設定されている。また、2019 年 2 月末時点で重大インシデント報告に関するシステムは開発中であると MSB の Web サイトに記載されている[35]。

c.　政府調達

政府調達については、概要を表 5-30 に示す。2014 年に EU から新たに公表された、公共調達指令 Directive 2014/24/EC（政府機関による調達）、Directive 2014/25/EC（公益事業を行う事業体による調達）を取り込み法律 Lag (2016:1145)、法律 Lag (2016:1146) を発効して対応している。

スウェーデン政府の調達に関する法律 Lag (2016:1145) では次のようなことが規定されている。具体的には、政府機関の対象としては、国、自治体、郡評議会が対象となる。また、政府による物品・役務の調達は一定額以上の契約に適用される。金額についてはスウェーデン政府が独自に制定したものではなく、政府機関による物品・役務の調達司令 Directive 2014/24/EC が適用される。

公益事業を行う事業体による調達には法律 Lag (2016:1146) が適用される。ここでの公益事業は「上下水道」、「交通サービス」、「港湾と空港」、「郵便サービス」、「エネルギー」が対象分野である。政府による物品・役務の調達は一定額以上の契約に適用される。金額についてはスウェーデン政府が独自に制定したものではなく、政府機関による物品・役務の調達司令 Directive 2014/25/EC が適用される。

防衛・安全保障に関する調達には EU の防衛・安全保障に関する調達の指令 Directive 2009/81/EC を国内に組み込んだ法律 Lag (2011:1029) で規定されている。調達において適用される範囲は「軍事装備（部品、コンポーネント等を含む)」、「機密関連の機器（部品、コンポーネント等を含む)」、「軍事装備、機密関連機器に直接関連する作業、供給及びサービス」、「特定の軍事目的または機密に関連する作業、サービス」と定義されている。金額については上述した、政府機関による調達、また公共事業を行う事業体による調達と同様に、EU の防衛・安全保障に関する調達の指令 Directive 2009/81/EC と同額であるとしている。

スウェーデンの安全保障関連の調達に関するプロセス、ルール等は、2018 年 5 月に発効されたセキュリティ保護法 (2018:585) にまとめられている。具体的には政府調達に伴ってセキュリティ保護の調査を実施すること、またその調査・分析に基づいて、政府等調達者が

[35] https://www.msb.se/sv/Forebyggande/Informationssakerhet/NIS-direktivet/

セキュリティ対策を計画し、実施することが求められている。

表 5-30　スウェーデンの政府調達に関する指令及び規制

調達の対象	指令名	概説
スウェーデン政府機関による調達	Lag 2016:1145	・ 政府機関が契約により、物品や役務（サービス）を調達する際のルールが定められた法律であり、EU 指令（2014/24/EU）が組み込まれている。 ・ 政府機関の対象としては、国、自治体、郡評議会等が含まれている。
公益事業を行う事業体による調達	Lag 2016:1146	・ 公共事業を行う事業体が、物品や役務（サービス）を調達する際のルールが定められた法律である。 ・ 公共事業の種類は「上下水道」、「交通サービス」、「港湾と空港」、「郵便サービス」、「エネルギー」と定義されている。
防衛・安全保障に関する調達	Lag 2011:1029	・ 防衛及び安全保障関に関する物品、役務（サービス）を調達する際のルールが定められた指令である。
防衛・安全保障に関する調達のプロセス、特定のルール等	Protective Security Act（2018:585）	・ 安全保障の活動に関わる事業者は、セキュリティ保護に関する調査を実施することが求められる。分析に基づいて、事業の性質と範囲、機密情報の有無、その他の事情を考慮して、必要なセキュリティ対策を計画し実施することが求められる。 ・ 物品、役務（サービス）、または工事に関する調達を行う政府機関、地方自治体、郡評議会は上記のセキュリティ対策が供給業者によって満たされているか確認する必要がある。

5.2.2.7.3 今後の方向性

上述のように、スウェーデンのサイバーセキュリティに関する法律は、EU の NIS 指令や GDPR をそのまま国内に取り込んでいるものが多い。そのため、今後も EU が示すサイバーセキュリティの政策に同調する形で、強化されていることが予想される。

また、サイバー攻撃に関しては今後の国防に関わる課題として捉えられており、2017 年 12 月にはスウェーデンの防衛委員会が「Resilience The total defence concept and the development of civil defence 2021-2025」という報告書の中で、サイバーセキュリティが今後より重大になることが指摘されており、将来的なサイバー脅威に対処するための法律等

が検討されている。また、報道によれば、サイバーセキュリティ対策を反映して、国防費も拡大傾向にあるという。具体的にはインテリジェンスとサイバー防衛領域に関する予算を10%拡大し 5 億 1,000 万ユーロにする計画があるという。

5.2.2.7.4 Evidence 及び原典

ア） 国としての全体的な状況（まとめ）

- 国家サイバーセキュリティ戦略（A national cyber security strategy）
  A national cyber security strategy
  https://www.government.se/4ac8ff/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213
- 一般データ保護規則（GDRP (General Data Protection Regulation) (REGULATION (EU) 2016/679) ）
  https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN
- ネットワークと情報セキュリティ指令（The Directive on Security of Network and Information Systems (Directive (EU) 2016/1148) ）
  https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN
- Datainspektionen (Swedish Data Protection Authority)
  https://www.datainspektionen.se/
- MSB (Swedish Civil Contingencies Agency)
  https://www.msb.se/
- CSEC (Swedish Certification Body for IT-Security)
  http://www.fmv.se/en/Our-activities/CSEC---The-Swedish-Certification-Body-for-IT-Security/
- PTS (Swedish National Post and Telecom Authority)
  https://pts.se/

イ） 対応状況

- IoT セキュリティ全般
  - Lag (2018:218)
    https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218

- 重要インフラ
  - Lag (2018:1174)
    https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181174-om-informationssakerhet-for_sfs-2018-1174
  - Organisationer som berörs av NIS-regleringen
    https://www.msb.se/sv/Forebyggande/Informationssakerhet/NIS-direktivet/Organisationer-som-berors/
  - Förordning (2018:1175)
    https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-20181175-om-informationssakerhet_sfs-2018-1175

- Lag, förordning och föreskrifter
  https://www.msb.se/sv/Forebyggande/Informationssakerhet/NIS-direktivet/Lag-forordning-och-foreskrifter/
- NIS-direktivet
  https://www.msb.se/sv/Forebyggande/Informationssakerhet/NIS-direktivet/

- 政府調達
  - Directive 2014/24/EU
    https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0024&from=SV
  - Lag (2016:1145)
    https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20161145-om-offentlig-upphandling_sfs-2016-1145
  - Directive 2014/25/EU
    https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014L0025&from=EN25
  - Lag (2016:1146)
    https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20161146-om-upphandling-inom_sfs-2016-1146
  - Directive 2009/81/EC
    https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0081&from=EN
  - Lag (2011:1029)
    https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20111029-om-upphandling-pa-forsvars--och_sfs-2011-1029

ウ） 今後の方向性

- Resilience The total defence concept and the development of civil defence 2021-2025
  https://www.regeringen.se/4afeb9/globalassets/regeringen/dokument/forsvarsdepartementet/forsvarsberedningen/resilience---report-summary---20171220ny.pdf
- Sweden steps up cyber defence measures
  https://www.computerweekly.com/news/450432739/Sweden-steps-up-cyber-defence-measures

5.2.2.8 インド

5.2.2.8.1 国としての全体的な状況(まとめ)

インドの政策動向の概要を表 5-31 に示す。

表 5-31 インドの政策動向（まとめ）

	項目	概要
現状	全体傾向	IoT セキュリティ関連の法規制はまだ初期段階であり、主に IT Act 及びこれに紐づく規則により規制されている。近年、企業における個人情報取扱規制やインシデント発生時の報告義務、サイバーセキュリティ強化や重要インフラ保護担当の政府機関設立等セキュリティ関連の整備が進んでいる。
	重要インフラの法制度	通信及び電力領域にて動きが見られる。通信領域では、2018 年 9 月発行の DoT guidelines にて DoT ライセンシーに対するネットワーク機器・サービス・ソフトウェアの脆弱性やバックドアのチェックの確認等セキュリティ強化義務の規定、及び国内企業に対し優先的な市場アクセスを許可する通知が発行された。電力分野では、セキュリティフレームワーク整備義務の規定及び当局が策定・通知すべき領域等を規定されている。
	政府調達	調達については現状有効な基準は特にないものの、国産製品の優遇が推進されている。 Public Procurement Orders に基づき、MeitY が 2017 年に出した通告では、すべての政府機関に対し、国内で製造されたサイバーセキュリティ製品を優先採用することを奨励している。
	認証/認定制度	政府機関（TEC）が定める、通信機器へのテスト及び認証に関する手順（MT&CTE）が定められている。 事前評価は Indian Accredited Labs によって行われ、その結果に基づき TEC が認証を発行する（2019 年実施予定だが延期されており、開始時期は現時点で不明）。
	体制	2016 年 6 月に通信 IT 省下にあった電子情報技術局（DeitY）を格上げした電子情報技術省（MeitY）及びこの際に新設された通信省（Ministry of Communication）を中心にサイバーセキュリティに関する施策や電気通信分野の施策を推進する。
今後	全体的な傾向	MeitY により公開された Draft IOT Policy に沿って整備が進む。政府機関（TEPC）は国家安全保障顧問（National Security Advisor）に対し、Huawei/ZTE 等の中国企業製品について政府ネットワーク用途で購入することの禁止を求めた。一方、通信業界団体（Cellular Operators Association of India）は、中国企業制限にメリットはないと考えており、通信大臣からも、セキュリティ要件を満たしていれば、自由に機器を購入できるとの発言をしている。
	重要インフラの法制度	通信領域に関し、Telegraph Rules による通信機器の評価・認証が導入される予定である。
	政府調達	Telegraph Rules に従い、通信関連機器の評価及び認証取得を義務付ける制度の導入が予定されている。使用用途の官民を問わず、インド政府によるライセンスの下で確立・維持・機能しているすべての telegraph は、販売前に TEC による事前評価及び認

	項目	概要
		証を受けるとしており、評価及び認証に関する詳細な手順(MT&CTE)を定めている。

現在のインドにおける IoT セキュリティに関する規制や法律はまだ初期段階にあり、重要な制度としては IT Act (Information Technology Act, 2000) とそれに紐づく規則 IT Privacy Rules (Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011)、Cert-In Rules (Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013) 等がある。これらでは、個人情報を収集している企業に対するセキュリティへの取り組みやセキュリティポリシーの保持義務、またサービスプロバイダー等に対するインシデント発生時の報告義務を規定している。

重要インフラについては、通信領域と電力領域に関する動きがあり、通信領域では 2018 年 8 月に DoT (Department of Telecommunications) から国内の通信機器サプライヤー及びメーカーに対する優先的な市場アクセスが通告されている他、DoT のライセンシーに対して、製品・サービスの脆弱性を確認するため、提供元との適切な契約を締結すること等が義務付けられている DoT guidelines (Minimum requirements for security policy for DoT licensees) がある。電力領域に関しては、信頼性ある電力網運用のためのセキュリティフレームワーク整備や、政府機関 NLDC (National Load Despatch Centre) によるインシデント発生の監視等が規定されている IEGC (Indian Electricity Grid Code) や Electricity Regulations (Central Electricity Regulatory Commission (Communication System for inter-State transmission of electricity) Regulations, 2017) 等がある。

政府調達については、インド製のサイバーセキュリティ製品の使用推奨 Public Procurement Order (Public Procurement (Preference to Make in India) Order 2017) や調達に関するガイドライン・方針の発表等がなされている (GFRs (General Financial Rules 2017)、eProcurement Guidelines (Guidelines for Compliance to Quality Requirements of eProcurement Systems) 等がある。

今後に向けては、個人情報の保護措置や悪用防止に関する権限をもつ当局設立を規定した法案 PDP Bill (Personal Data Protection Bill, 2018) が提出されている。他にも IoT 関連の方向性を幅広に示した政策ドラフト (Draft IOT Policy (draft IOT Policy document)) が公開されており、その中で IoT 関連の標準化や規格策定を推進する機関の指定、IoT 基準の進展・導入を行う委員会設立、セキュリティ・プライバシー確保の促進、国内企業の優先的な市場アクセス拡大等が提言されている。また特に通信関連機器については、官民どちらで使用されるものについても、政府指定の MT&CTE という手順に則り評価・認証を受けることが義務付けられる予定である(Telegraph Rules (Indian Telegraph (Amendment) Rules, 2017))。体制として、評価が Indian Accredited Labs で実施され、その結果を受けて DoT 内の TEC (Telecommunication Engineering Centre) が認証を行う。当初の計画では 2019 年 1 月より導入予定であったが、その後延期が発表され、導入時期については不明である。

図 5-11 は、インドにおける政府関連組織と関連法制度をまとめたものである。番号により、組織と法制度の関連性を表現している（組織の概要は表 5-32 を、法制度の概要は表 5-33 を参照)。MoC（通信省: Ministry of Communications）は、通信と郵便を管轄し、インドにおける電気通信法である Indian Telegraph Act, 1885 と、Telegraph Rules を定めている。DoT は、電気通信の免許付与、国際調整、標準化を行い、DoT guidelines をライセンシーに義務付けている。また、DoT は NDCP (National Digital Communications Policy, 2018) を定めている。TEC（テレコム・エンジニアリング・センター: Telecommunication Engineering Centre）は Telegraph Rules の事前評価及び認証を発行する。MeitY（電子情報技術省: Ministry of Electronics and Information Technology）はサイバーセキュリティへ対応を行い、NTP 2012 (National Telecom Policy, 2012) と、Public Procurement Order

(Public Procurement (Preference to Make in India) Order 2017) を定めている。STQC Directorate（試験標準化・試験・品質認証総局: Standardisation Testing and Quality Certification Directorate）は、政府機関が考慮するべきガイドラインや、デジタル署名に関するガイドラインを定め、また eProcurement Guidelines を定めている。その他の組織として、次のものがある。Cert-In（Indian Computer Emergency Response Team）は、サイバーセキュリティの分野において、インシデント情報の収集・分析・普及や、ガイドライン・ホワイトペーパーの発行等を行う国家機関として機能している。NCIIPC（国立重要情報インフラ保護センター: National Critical Information Infrastructure Protection Center）は、重要な情報インフラの保護、サイバー空間における脅威への脆弱性軽減を目的としたアドバイス等の役割をもつ。NCCC（国立サイバー調整センター: National Cyber Coordination Center）は、Web トラフィックを分析しサイバーセキュリティへの脅威を検出、状況を把握することでこれらの脅威の回避に努めている。

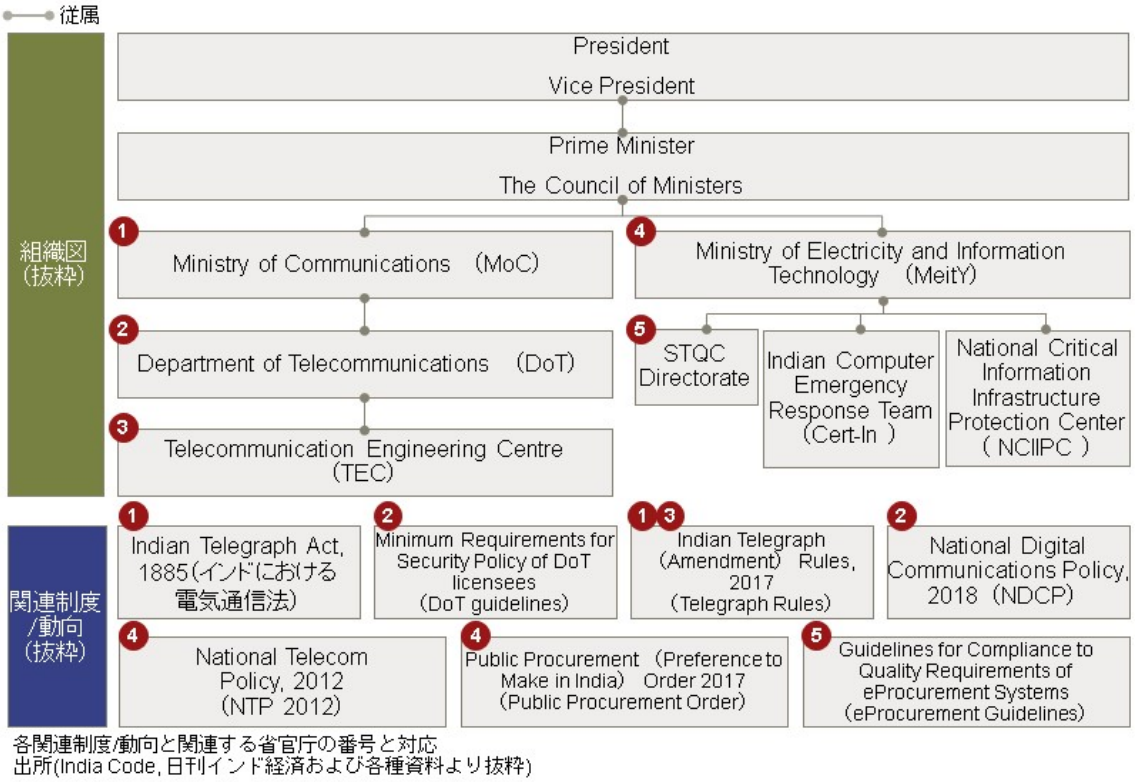


図 5-11　インドの政府関連組織と関連法制度

表 5-32　インドにおける政府関連組織

MoC	通信省。 通信と郵便を管轄する。2016 年 6 月に通信 IT 省傘下の電子情報技術局（DeitY）が電子情報技術省（MeitY）に格上げされたことで新設された。
DoT	電気通信局。 電気通信の免許付与、国際調整、標準化を行う。
TEC	テレコム・エンジニアリング・センター。 Telegraph の事前評価及び認証を発行する。
MeitY	電子情報技術省。 IT 、エレクトロニス、インターネット関連の政策策定、振興、国際連携、標準化を行う。また、サイバーセキュリティへ対応を行う。 2016 年 6 月に通信 IT 省傘下の電子情報技術局（DeitY）

	から格上げされた。
STQC Directorate	試験標準化・試験・品質認証総局。 政府機関が考慮するべきガイドラインや、デジタル署名に関するガイドラインを定めている。
Cert-In	インドにおける Computer Emergency Response Team。 サイバーセキュリティの分野において、インシデント情報の収集・分析・普及や、ガイドライン・ホワイトペーパーの発行等を行う国家機関として機能している。
NCIIPC	国立重要情報インフラ保護センター。 重要インフラ保護の国家中核機関に指定されており、重要な情報インフラの保護、サイバー空間における脅威への脆弱性軽減を目的としたアドバイス等の役割をもつ。
NCCC	国立サイバー調整センター。 Web トラフィックをスキャンしメタデータと順列を用いてサイバーセキュリティへの脅威を検出、状況を把握することでこれらの脅威の回避に努めている

表 5-33　インドにおける関連法制度

Indian Telegraph Act, 1885	インドにおける電気通信法。
DoT guidelines	ライセンシーに義務付けているを規定。 DoT のライセンシーに対し、ネットワークセキュリティ・情報セキュリティの責任者任命や、ネットワーク機器・サービス・ソフトウェアの脆弱性やバックドアがチェックされていることを確認するための製造元・ベンダーとの適切な契約の締結等が義務付けられている。
Telegraph Rules	政府指定の MT&CTE という手順に則り評価・認証を受けることを義務付けている規定。 導入が予定されている通信関連機器のテスト及び認証取得を義務付ける制度であり、使用用途の官民を問わずインド政府によるライセンスの下で確立・維持・機能している telegrapht 及びその telegraph とともに使用される、もしくは使用される可能性のあるすべての telegraph は、インドでの販売前に TEC による事前テスト及び認証を受ける必要があるとしている。
NDCP	デジタル通信システムの主権、安全性及びセキュリティの確保を目的としており、また国際的なベストプラクティスを取り込んだ IoT・M2M 等に関するセキュリティフレームワークの必要性について触れられている。
NTP 2012	現在及び将来のネットワークにおいて安全な接続や途切れない一貫した機能の実現を確保するために、すべての通信製品がテスト・認証される必要があるとしている。
Public Procurement Order	MeitY が 2017 年に出した通告では、サイバーセキュリティは戦略的セクターであるとの理由から、すべての政府機関に対し、国内で製造されたサイバーセキュリティ製品を優先採用することを奨励している。
eProcurement Guidelines	入札文書発行やそのプロセスにおいて、スパイウェアやトロイの木馬等を防止するため政府機関が考慮するべきガイドラインや、デジタル署名に関するガイドラインを定めて

	いる。

5.2.2.8.2 対応状況

a. IoT セキュリティ全般

インドにおける IoT セキュリティに関する規制や法律はまだ初期段階にあり、重要な制度としては IT Act とそれに紐づく規則がある [1]。IT Act では「サイバーセキュリティ」という言葉を、情報、機器、コンピュータ、コンピュータリソース、通信デバイス、及びそれらに保存されている情報を、不正なアクセス、使用、開示、破壊、改変から保護することとして定義している [2]。IT Act に基づき制定された IT Privacy Rules では、個人情報を収集している企業に対し、合理的なセキュリティへの取り組みの実行と、文書化された情報セキュリティポリシーの保持を義務付けている [3]。IT Act の規定に従い設立された Cert-In はサイバーセキュリティの分野において、インシデント情報の収集・分析・普及や、ガイドライン・ホワイトペーパーの発行等を行う国家機関として機能している [4]。またこれも IT Act に基づき定められた Cert-In Rules において、サービスプロバイダー、仲介業者、データセンター、企業に対し、サイバーセキュリティインシデントの発生について Cert-In への通知義務を課している [5]。ここでのサイバーセキュリティインシデントには、IT システム・データへの不正アクセスや、DoS 攻撃・DDoS 攻撃等が含まれる [6]。

また上記の法律・制度以外の取り組みとして、サイバーセキュリティに関していくつかの政府機関が設立されている。2014 年に IT Act に基づき設立された NCIIPC もこれに該当し、重要インフラ保護の国家中核機関に指定されており、重要な情報インフラの保護、サイバー空間における脅威への脆弱性軽減を目的としたアドバイス等の役割をもつ [8]。他にも 2017 年 8 月に設立された NCCC では、Web トラフィックをスキャンしメタデータと順列を用いてサイバーセキュリティへの脅威を検出、状況を把握することでこれらの脅威の回避に努めている [9]。また政府からいくつかの政策が発表されている。一つは NCSP (National Cyber Security Policy, 2013) であり、その目的としてはグローバルなセキュリティ基準の遵守、常に重要インフラを保護するための NCIIPC 運営、強力なサイバーセキュリティ要員を 50 万人生み出しサイバーセキュリティを実践することによる企業利益の提供等がある [10]。Cyber Swachhta Kendra は NCSP の目的に沿って Cert-In が設立した機関で、安全なサイバーエコシステムの構築を想定している [11]。2018 年に政府に承認され、NDCP では、デジタル通信システムの主権、安全性及びセキュリティの確保を目的としており、また国際的なベストプラクティスを取り込んだ IoT・M2M 等に関するセキュリティフレームワークの必要性について触れられている [13]。ここまでで挙げた以外にも、サイバー犯罪・情報セキュリティの関連事項調査を目的とした Cyber & Information Security Division の設置 [14]、サイバー攻撃・サイバーテロへの抵抗を目的とした Cyber Crisis Management Plan 策定 [16]、定期的なサイバーセキュリティ模擬訓練の実施 [17]、NIC によるサイバーリソース保護等の取り組みがある [18]。

b. 重要インフラ

重要インフラについては、まず通信領域において、DoT は 2018 年 8 月に、国内の通信機器サプライヤー及びメーカーに対し、優先的な市場アクセスを許可する通知を発行した [36]。また DoT が 2018 年 9 月に発行した DoT guidelines では DoT のライセンシーに対し、ネットワークセキュリティ・情報セキュリティの責任者任命や、ネットワーク機器・サービス・ソフトウェアの脆弱性やバックドアがチェックされていることを確認するための製造元・ベンダーとの適切な契約の締結等が義務付けられている [37]。

また電力領域においても規制があり、CERC に作られた IEGC では、すべての公益事業

体に対し、信頼性のある電力網運用のため、サイバー空間における資産を確認し、それらを保護するためのサイバーセキュリティフレームワークの整備を規定している [38]。また Electricity Regulations では、CEA が技術的基準、サイバーセキュリティ要件、電力セクター用通信システムのプロトコルを策定・通知するとしている他 [39]、通信インフラの計画・設計・実行は CEA 指定の基準に従うことや、NLDC がサイバーセキュリティ発生を監視、必要に応じて措置を講じること等が規定されている [40]。

c. 政府調達

政府調達については、インドでは政府契約や商品・サービスの調達に関する独自のサイバーセキュリティ規制はないが、主に Ministry of Finance によって発行される GFRs、Manual for Procurement of Consultancy and Other Services 2017、Manual for Procurement of Goods 2017 に従って実施されている [52]。また上述のようにサイバーセキュリティインシデント監視のための機関設立に加え、すべての政府機関に適用される特定の措置も講じている。Public Procurement Order に基づき MeitY が 2017 年に出した通告では、サイバーセキュリティは戦略的セクターであるとの理由から、すべての政府機関に対し、国内で製造されたサイバーセキュリティ製品を優先採用することを奨励している [24]。ここでのサイバーセキュリティ製品の定義は Public Procurement Order によると、情報、設備、コンピュータ機器、コンピュータリソース、通信機器及びこれらに保存された情報を、不正なアクセス、使用、開示、断絶、変更または破壊されることから保護するための製品、器具もしくはソフトウェアとされている [25]。

また上記の法律・制度以外にも、ガイドラインや方針等が発表されている。STQC Directorate から発行された eProcurement Guidelines では、入札文書発行やそのプロセスにおいて、スパイウェアやトロイの木馬等を防止するため政府機関が考慮するべきガイドラインや、デジタル署名に関するガイドラインを定めている [27]。また通信領域においては、NDCP と NTP 2012 で、現在及び将来のネットワークにおいて安全な接続や途切れない一貫した機能の実現を確保するために、すべての通信製品がテスト・認証される必要があるとしている [30]。

5.2.2.8.3 今後の方向性

a. IoT セキュリティ全般

今後の IoT セキュリティに関する方向性として、MeitY から Draft IOT Policy が公開されており、その中で以下のような提案がなされている。

- IoT 標準化やクラウド内外の通信規格策定等を推進する中核機関の指定 [19]
- 世界的に確立され相互運用可能な IoT 基準を進展、導入する国家専門委員会の設立 [20]
- 堅牢なセキュリティとプライバシー確保のため IoT ソリューション進展促進 [21]
- 国内メーカーに対する優先的な市場アクセス拡大[22]

また 2018 年 7 月には、コンシューマー向け機器・サービスに関しては上述の個人情報保護に関する法案（PDP Bill）が提出され、この中では Data Protection Authority の設立が規定され、またその権限として（i）個人の利益保護のための措置を講じること、（ii）個人データの悪用を防止すること、（iii）法案の遵守を保証すること、が規定されている [23]。

b. 重要インフラ

通信領域については、上述の通り Telegraph Rules による通信機器の評価・認証が導入予

定である。

c. 政府調達

政府調達については、特に通信領域において Telegraph Rules に従い、通信関連機器の評価及び認証取得を義務付ける制度の導入が予定されている。この制度においては、使用用途の官民を問わず、インド政府によるライセンスの下で確立・維持・機能している telegraph とともに使用される、もしくは使用される可能性のあるすべての telegraph は、インドでの販売前に TEC による事前評価及び認証を受ける必要があり、また TEC はこの評価及び認証に関する詳細な手順である MT&CTE を定めている [31] [51]。事前評価は Indian Accredited Labs によって行われ、その結果に基づき TEC が認証を発行する [33]。評価・認証制度は当初の計画では 2019 年 1 月より導入される予定だったが、その後延期が発表され、導入時期については不明である [50]。ちなみに telegraph の定義は Indian Telegraph Act, 1885 によると、「有線・電磁放射・電波・ヘルツ波・電気的もしくは磁気的なあらゆる手段による信号・文章・画像・音の送受信に使用されている、もしくは使用される可能性がある装置・機器・資材もしくは器具」とされている [32]。

d. 略称名称一覧（各カテゴリのアルファベット順）

カテゴリ	略称	正式名称
制度	Cert-In Rules	Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013
	DISHA	Digital Information Security in Healthcare Act
	DoT guidelines	minimum requirements for security policy for DoT licensees
	Draft IOT Policy	draft IOT Policy document
	Electricity Regulations	Central Electricity Regulatory Commission (Communication System for inter-State transmission of electricity) Regulations, 2017
	eProcurement Guidelines	Guidelines for Compliance to Quality Requirements of eProcurement Systems
	GFRs	General Financial Rules 2017
	IEGC	Indian Electricity Grid Code
	IT Act	Information Technology Act, 2000
	IT CA Rules	Information Technology (Certifying Authorities) Rules, 2000
	IT Privacy Rules	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
	NCSP	National Cyber Security Policy, 2013
	NDCP	National Digital Communications Policy, 2018
	NTP 2012	National Telecom Policy, 2012
	PDP Bill	Personal Data Protection Bill, 2018
	Public Procurement Order	Public Procurement (Preference to Make in India) Order 2017

カテゴリ	略称	正式名称
	SCM	Smart Cities Mission
	Telegraph Rules	Indian Telegraph (Amendment) Rules, 2017
組織	CEA	Central Electricity Authority
	CERC	Central Electricity Regulatory Commission
	Cert-In	Indian Computer Emergency Response Team
	DoT	Department of Telecommunications
	MeitY	Ministry of Electronics and Information Technology
	NCCC	National Cyber Coordination Center
	NCIIPC	National Critical Information Infrastructure Protection Center
	NIST	National Institute of Standards & Technology
	NLDC	National Load Despatch Centre
	TEC	Telecommunication Engineering Centre
	TEPC	Telecom Equipment and Services Export Promotion Council
その他	AISEP	Australasian Information Security Evaluation Program
	GeMI	Government e-Marketplace

e. 重要インフラの定義

なお、インドにおける critical infrastructure の定義について、法律及びそれに紐づく政策では示されていない [47]が、NCSP やこれに基づいて発行された通知では critical sectors として、finance/banking、defence、energy/power、transportation、telecommunication が挙げられている [48]。また IT Act では critical information infrastructure の定義を、無力化または破壊された際に国家の安全保障、経済、公衆衛生もしくは安全を衰弱させるコンピュータ資産としている [49]。

5.2.2.8.4 Evidence 及び原典

a. 法律事務所による回答

INDIA

December 26, 2018

1.An overview of your jurisdiction's cyber security legislation and regulations, including both legally binding laws or non-binding guidance or principles, as they concern network systems for the "Internet-of-Things" and/or information and communication technology.

[Existing Legislation and Regulations]

The laws pertaining to cyber security in India, are at a nascent stage and the only significant legislation is the Information Technology Act, 2000 ("**IT Act**") and the rules framed thereunder. [1] The IT Act has defined "cyber security" to mean

protecting information, equipment, devices, computer, computer resource, communication device, and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction.[36] [2]

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**IT Privacy Rules**") formulated pursuant to the IT Act, mandate that every corporate entity (or a person on its behalf) collecting personal information, including sensitive personal information shall implement reasonable security practices and procedures and have a comprehensive documented information security policy containing managerial, technical, operational and physical security control measures. [3] Any such corporate entity should implement either IS/ISO/IEC 27001 standard or the codes of best practices for data protection other than IS/ISO/IEC of any industry association or an entity formed by such an association approved and notified by the Government of India.

The Government of India has formed various agencies under the IT Act and has taken various measures for preventing cybercrime in the country.

The Indian Computer Emergency Response Team ("**Cert-In**") formed pursuant to the provisions of the IT Act, serves as the national agency for performing the following functions in the area of cyber security:[37]

(a) collection, analysis and dissemination of information on cyber incidents;

(b) forecast and alerts of cyber security incidents;

(c) emergency measures for handling cyber security incidents;

(d) coordination of cyber incidents response activities;

(e) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, preventation, response and reporting of cyber incidents; and

(f) such other functions relating to cyber security as may be prescribed. [4]

The Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 ("**Cert-In Rules**") framed under the IT Act imposes mandatory notification requirements on service providers, intermediaries, data centres and corporate entities, upon the occurrence of certain "cyber security incidents" within a reasonable time of occurrence or noticing of such incident. [5] "Cyber security incidents" have been defined to mean any real or suspected adverse events, in relation to cyber security, that violate any explicitly or

[36] See Section 2(1)(nb) of the IT Act
[37] See Section 70B (4) of the IT Act

implicitly applicable security policy, resulting in: (a) unauthorised access, denial or disruption of service, (b) unauthorised use of a computer resource for processing or storage of information, and (c) changes to data, information without authorisation.[38]

The occurrence of the following cyber security incidents should be mandatorily reported to the Cert-In under the Cert-In Rules[39]:

(a) Targeted scanning/probing of critical networks/systems;

(b) Compromise of critical systems/information;

(c) Unauthorised access of IT systems/data;

(d) Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to certain external websites etc.;

(e) Malicious code attacks such as spreading of virus/worm/Trojan/Botnets/Spyware;

(f) Attacks on servers such as database Mail and DNS network services such as Routers;

(g) Identity thefts, spoofing and phishing attacks;

(h) Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks;

(i) Attacks on critical infrastructure, SCADA Systems and Wireless networks; and

(j) Attacks on applications such as E-Governance, E-Commerce etc. [6]

The service providers providing services to government departments and agencies (Central, State, Union Territories and Municipal Corporations) under contractual agreement had sought clarification on their role in notifying the security incidents to Cert-In. Cert-In noted that under the standard terms of contract signed between the government departments and the service provider for services, it is the responsibility of primary owners to formally notify the security incidents to government department and agencies, and not the service providers who provide services under contractual agreement, and has therefore clarified that it is only the primary security owner (i.e. Central, State, Union Territories and Municipal Corporations) and not the service providers which are required to report incidents directly to Cert-In.[40] [7]

The National Critical Information Infrastructure Protection Centre ("**NCIIPC**") is an organisation of the Government of India created under Sec 70A of the IT Act,

[38] See Rule 2(h) of the Cert-In Rules
[39] See Rule 12(1)(a) read with the Annexure.to the Cert-In Rules
[40] https://www.dsci.in/sites/default/files/documents/resource_centre/DSCI-Communication.pdf

through a gazette notification on January 16, 2014.[41] NCIIPC is designated as the national nodal agency in respect of critical information infrastructure protection. The formal roles and responsibilities of the NCIIPC include inter alia,

(a) National nodal agency for all measures to protect nation's critical information infrastructure;

(b) Protect and deliver advice that aims to reduce the vulnerabilities of critical information infrastructure, against cyber terrorism, cyber warfare and other threats;

(c) Identification of all critical information infrastructure elements for approval by the appropriate Government for notifying the same; and

(d) Provide strategic leadership and coherence across government to respond to cyber security threats against the identified critical information infrastructure. [8]

The NCIIPC has defined controls for the critical infrastructure sectors to enhance security.[42]

In August 2017, the Government of India announced the National Cyber Coordination Centre ("**NCCC**") to address various kinds of cyber security threats, including threats arising out of misuse of social media. The NCCC scans the country's web traffic to detect cyber security threats using metadata and various permutations to get a situational awareness and fend off such threats in a timely manner.[43] [9]

The Government of India took the first formalized step towards cyber security in 2013, vide the Ministry of Communication and Information Technology, Department of Electronics and Information Technology's National Cyber Security Policy, 2013 ("**NCSP**").[44]

The NCSP is aimed at building a secure and resilient cyberspace for citizens, businesses and the government. Its mission is to protect cyberspace information and infrastructure, build capabilities to prevent and respond to cyber-attacks, and minimise damages through coordinated efforts of institutional structures, people, processes, and technology. The objectives of the policy include creating a secure cyber ecosystem, compliance with global security standards, strengthen the regulatory framework, creating round the clock mechanisms for gathering intelligence and

---

[41] G.S.R. 19(E), dated January 16, 2014 published in the Gazette of India, Extra., Pt. II, Sec 3(i), No. 15, dated January 16, 2014.

[42] https://nciipc.gov.in/

[43] https://timesofindia.indiatimes.com/india/govt-sets-up-cyber-coordination-centre-to-address-cyber-security-threats/articleshow/63614415.cms

[44] Notification on National Cyber Security Policy 2013, dated July 2, 2013 issued by MeitY, Government of India, http://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf

effective response, operation of a National Critical Information Infrastructure Protection Centre for 24×7 protection of critical information infrastructure, research and development for security technologies, create a 500,000 strong cyber security workforce, to provide fiscal benefits to businesses for adopting cyber security practices, to build public private partnerships for cooperative cyber security efforts. [10]

To combat cyber security violations and prevent their increase, Cert-In launched 'Cyber Swachhta Kendra' (Botnet Cleaning and Malware Analysis Centre) a new desktop and mobile security solution for cyber security in India. The 'Cyber Swachhta Kendra' (Botnet Cleaning and Malware Analysis Centre)[45] was set up in accordance with the objectives of the NCSP, which envisages creating a secure cyber eco-system in the country. [11] This centre operates in close coordination and collaboration with internet service providers and product/antivirus companies. It functions to analyze BOTs/malware characteristics, provides information and enables citizens to remove BOTs/malware and to create awareness among citizens to secure their data, computers, mobile phones and devices such as home routers.

In 2015, the Government of India launched the Smart Cities Mission ("**SCM**") with the stated purpose of improving the governance and infrastructural deficiencies that plague Indian cities. Pursuant to the SCM, the Ministry of Housing and Urban Affairs, Government of India released a model framework for cyber security in smart cities on May 20, 2016.[46] It covers the security of smart cities across different layers, namely sensor layer, communication layer, data layer and application layer. The major guidelines include, but are not limited to:

(a) Designing a secure network architecture based on the National Institute of Standards & Technology (NIST) reference IT architecture;

(b) Security solutions that needs to be considered while developing a smart city;

(c) Secure storage and transmission of data between different systems and devices implemented in the smart city;

(d) Security assessment of the services before and after going live;

(e) Compliance with standards such as ISO 27001, ISO 22301, ISO 37120, ISO 3712, ISO 27017, ISO 27018, BSI PAS 180, BSI PAS 182, Protected Extensible Authentication protocol (PEAP) and 3rd generation Partnership Project (3GPP), as applicable;

[45] https://www.cyberswachhtakendra.gov.in/
[46] Cyber Security Requirement for Smart City- Model Framework issued by National Security Council Secretariat, https://smartnet.niua.org/sites/default/files/resources/Cyber_Securitypdf.pdf

(f) Setting up of security monitoring for smart city network, devices and sensors; and

(g) Reporting of security incidents to relevant bodies such as Cert-In and NCIIPC. [12]

The Government of India has also recently approved the National Digital Communications Policy, 2018[47] ("**NDCP**"). The mission of NDCP 2018 is, inter alia, to ensure the sovereignty, safety and security of digital communications systems in India. NDCP also highlights the need for the formulation of security frameworks for IoT/ M2M / future services and network elements incorporating international best practices. [13]

In addition to the above measures, the Government of India has also taken additional steps to prevent cyber crime in India, which include inter alia:[48]

(a) The Ministry of Home Affairs, Government of India has recently set up a Cyber & Information Security Division to look into relevant matters relating to cyber-crime & information security [14];

(b) All the new government websites and applications are to be audited with respect to cyber security prior to their hosting. The auditing of the websites and applications is to be conducted on a regular basis after hosting [15];

(c) Government of India has formulated Cyber Crisis Management Plan for countering cyber attacks and cyber terrorism [16];

(d) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors [17]; and

(e) NIC which provides IT/E-Governance related services to Government Departments protects the cyber resources from possible compromises through a layered security approach in the form of practices, procedures and technologies. [18]

[Forthcoming Legislation and Regulations and Discussions on Future Trends]

The Ministry of Electronics and Information Technology ("**MeitY**") had released a draft IOT Policy document ("**Draft IOT Policy**").[49] The Draft IOT Policy proposes to

[47] National Digital Communications Policy 2018, http://www.dot.gov.in/sites/default/files/Final%20NDCP-2018.pdf?download=1

[48] Saving Cyber Network from Criminal threat, published by Press Information Bureau, Ministry of Home Affairs, Government of India, http://pib.nic.in/newsite/PrintRelease.aspx?relid=177079

[49] Draft Policy on Internet of Things, http://meity.gov.in/writereaddata/files/Revised-Draft-IoT-Policy%20%281%29_0.pdf

appoint relevant nodal organization for driving and formalizing standards relating to technology, process, interoperability and services like:

(a) IoT standardization

(b) Spectrum energy communication protocols standards

(c) Standards for communication within and outside the cloud.

(d) International quality/integrity standards for data creation, data traceability.

(e) Standards for Energy consumption

(f) Device security and Safety standards (for example: Protection to humans from EMF and other health hazards)

(g) Data Privacy, Data Accuracy & Integrity and Security Standards. The privacy law to be made congruent with the evolving IoT paradigm. [19]

The Draft IOT Policy also proposes to create national expert committee for developing and adopting globally established and interoperable IoT standards in the country. [20] The expert committee is proposed to comprise of industry experts/organizations in inter alia, security and privacy technologies.

The Draft IOT Policy further proposes (i) to facilitate the development of IoT solutions with relevant changes in telecom policies for ensuring robust security and privacy [21]; and (ii) that the preferential market access will be extended to domestic manufacturers of IoT solutions. [22] It also recognises that IoT will lead to new systems/products/services where machine will take decision based on certain available data and hence legal frameworks will need to be created for issues that might arise due to IoT related product/systems/services.

On August 24, 2017, the Supreme Court of India, in the landmark case of Justice K.S. Puttaswamy and Anr. v. Union of India and Ors[50], ruled "privacy" as a Fundamental Right essential to life and liberty, and thereby, it has been put under the ambit of Article 21 of the Indian Constitution. In order to have an effective and efficient data protection mechanism in India, a committee was formed which submitted the draft bill on personal data protection to the Ministry of Electronic and Information Technology on July 27, 2018 ("**PDP Bill**")[51].

The PDP Bill provides the basic elements of data protection, which will need to be carefully fine-tuned to achieve the NDCP's objective of ensuring security of data. As per the PDP Bill, "Personal Data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait,

[50] (2017) 10 SCC 1

[51] The Personal Data Protection Bill, 2018, http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information.

The PDP Bill also includes provisions to protect personal data as an essential facet of information privacy, and provides guidelines on the data processing grounds, rights of the data principal, penalties and exemptions, amongst other areas. The PDP Bill provides for the establishment of a Data Protection Authority. The Authority is empowered to: (i) take steps to protect interests of individuals, (ii) prevent misuse of personal data, and (iii) ensure compliance with the Bill. [23]

References:

Links are provided in the form of footnotes for ease of reference.

2.Details of your jurisdiction's cyber security-related regulations relevant to procurement of goods in the following sectors

(a) Government (national security, defense, police, fire station, tax, academic research, etc.)

[Existing Legislation and Regulations]

Government contracts:

There are no separate cyber security regulations governing government contracts and public procurement of goods and services in India. However, the government has, in addition to the setting up of various agencies to monitor and advise on cyber security incidents as stated above, also undertaken specific steps in relation to procurement contracts which are applicable to all government departments and public procurements in India.

Pursuant to the Public Procurement (Preference to Make in India) Order 2017 ("**Public Procurement Order**")[52] issued by the Government of India vide the Department of Industrial Policy and Promotion (DIPP) Notification No. P - 45021/2/2017- B.E. - II dated June 15, 2017 and partially modified order no P- 45021/2/2017- PP(BE- II) issued on May 28, 2018, the MeitY has issued notification dated July 2, 2018 stating that cyber security being a strategic sector, preference would be provided by all procuring government entities to domestically manufactured/produced cyber security products. [24] "Cyber security product" has been defined under the Public Procurement Order as a product or appliance or

[52] Notification dated July 2, 2018 on Public Procurement (Preference to Make in India) Order 2018 for Cyber Security Products, MeitY, Government of India http://meity.gov.in/writereaddata/files/public_procurement-preference_to_make_in_india-order_2018_for_cyber_security_products.pdf

software manufactured/ produced for the purpose of protecting, information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. [25]

In addition to the above, India's national public procurement portal (Government e-Marketplace (GeM)) has tied up with original equipment manufacturers ("**OEM**") of information technology hardware and software to certify their sellers in a move to weed out counterfeits. [26] GeM, the end-to-end online marketplace for central and state governments, has partnered with atleast a hundred OEMs by signing memoranda of understanding with their respective industry associations including Nasscom and Manufacturers Association for Information Technology.[53]

The Guidelines for Compliance to Quality Requirements of eProcurement Systems ("**eProcurement Guidelines**") issued by the STQC Directorate set up under the Department of Information Technology has prescribed guidelines to be considered by government entities while issuing tender documents and for the bid process.[i] The guidelines and recommended practices to be considered by the government entities, to prevent spyware/ Trojan/ BOTS during tender process, includes, inter alia, the manner of securing the system from injection of spyware by:

(a) Hardening of hardware and software of the entire Information Technology infrastructure (which includes computer system, software, router, etc.);

(b) Installing anti spyware, anti-spam and antivirus software;

(c) Installation of software tools to protect the operating system from injection of spyware and continuous upgradation of such software;

(d) The entire infrastructure needs to be secured at the perimeter level by installing firewalls and intrusion prevention system;

(e) After installation of software and protecting by devices as the entire IT infrastructure needs to be audited by the Cert-In which has empanelled auditors for auditing systems from the point of view of cyber security. The system should be audited at least once in a year and as and when the infrastructure (i.e. hardware and software) is augmented by additions of new hardware and software;

(f) People operating these systems should be trained in monitoring and detecting any intrusion in the system and network;

---

[53] Government ties up with OEMs to weed out fakes from public procurement, dated December 11, 2018 https://economictimes.indiatimes.com/news/economy/policy/government-ties-up-with-oems-to-weed-out-fakes-from-public-procurement/articleshow/67045786.cms

(g) The kernel of the operating system in the IT infrastructure should be secured first by hardening the operating system and installation of software which protects it from the injection of spyware or any kind of intrusion; and

(h) The e - procurement system should have audit trail facilities. These audit trails are complex but dependable. The audit trails reports provide useful information about the instructions which take place in the system both at operating system and application software. This information is necessary to analyze nature of intrusion, vulnerabilities exploited and to track the perpetrators. It also helps in taking steps in preventing future intrusion.

The eProcurement Guidelines also prescribes the guidelines pertaining to digital signatures which state inter alia, that:

(a) any e-tendering portal to be used by the government organisation must allow the users of the portal to use any one digital certificate/ digital signature issued by the Certifying Authority;

(b) all digital signature certificates should be PKI based issued by a Certifying Authority licensed by the Controller of Certifying Authorities;

(c) vendors of e - tendering portals, or tendering software, should be specifically instructed to keep in view section 42 (1), and section 85B2(b) of the IT Act while giving a `confirmation of compliance with the IT Act';

(d) to avoid compromise of security (i.e. compromise of private key in this context), users of an e - tendering portal should not obtain `pre - prepared' digital certificates' through the service provider or any other source. The digital certificate should be generated by the concerned user (i.e. the applicant of the digital certificate) himself, preferably on his own computer, and securely stored under a password; and

(e) the Digital Signature (i.e. Private Key) cannot be handed over by the owner of that key to any other person. [27]

The Information Technology (Certifying Authorities) Rules, 2000 ("**IT CA Rules**"), framed under the IT Act, provides for the creation and verification of a digital signature by public key cryptography method and prescribes the use of internationally proven encryption techniques such as PKCS#1 RSA Encryption Standard (2048 bit, 4096 bit), PKCS#5 (Password Based Encryption Standard) etc. for different activities associated with the Certifying Authorities in relation to the issue of digital/electronic signature certificates.[54] [28]

[54] See Rule 6 of the IT CA Rules

IT Act states that where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in the law, such requirement shall be deemed to be satisfied, if such information or matter is authenticated by means of electronic signature affixed in a manner as prescribed. [29] The digital signature can be utilized for sending and receiving digitally signed and encrypted emails/ documents; for carrying out secure web-based transactions; in e-Tendering, e-Procurement; filing e-documents with the Registrar of Companies and e-filing of income tax returns and also in many other applications.

Telecommunication infrastructure:

The NDCP and also the erstwhile (Indian) National Telecom Policy, 2012 ("**NTP 2012**") recognises that testing and certification of all telecom products are necessary to ensure safe-to-connect and seamless functioning in the existing and future networks. [30]

Pursuant to the NTP 2012, and with a cautionary approach in procurement of telecom equipment from telecom manufacturers, the Government of India amended the (Indian) Telegraph Rules, 1951 on September 5, 2017 to provide for mandatory testing and certification of "telegraph".

The Indian Telegraph (Amendment) Rules, 2017, provides that any telegraph which is used or capable of being used with any telegraph established, maintained or worked under the licence granted by the Government of India must undergo prior mandatory testing and certification by the Telecommunication Engineering Centre, DoT, Ministry of Communications ("**TEC**") before sale of such telegraph in India ("**Telegraph Rules**").[55] The TEC has framed a detailed procedure for mandatory testing and certification of telecom equipment ("**MT&CTE**")[56]. [31] The Indian Telegraph Act, 1885 defines "telegraph" as any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images, and sounds or intelligence of any nature by wire, visual or other electro-magnetic emissions, Radio waves or Hertzian waves, galvanic, electric or magnetic means. [32]

The testing is to be carried out by Indian Accredited Labs and based upon their test reports, certificate shall be issued by TEC.[57] [33] The Telegraph Rules mandates DoT to take punitive action under the licence norms and also seize the equipment, if

[55] Indian Telegraph (Amendment) Rules, 2017, http://tec.gov.in/pdf/Whatsnew/eGazetteNotif.pdf
[56] Procedure for Mandatory Testing and Certification of Telecommunication Equipment issued by Department of Telecommunications, Ministry of Communications, Government of India, http://tec.gov.in/pdf/Whatsnew/Final%20MTCTE%202017%20Procedure.pdf
[57] http://www.tec.gov.in/certification-approval-procedure/

a telecom operator fails to adhere to them. The Telegraph Rules bar telecom operators from using untested and uncertified equipment. Some important points of the Telegraph Rules and MT&CTE are as follows:[58]

(a) Every OEM (Indian and foreign) and importer, who wishes to sell or import any telecom equipment in India, must get its telecom equipment mandatorily tested and certified by TEC and mark or affix such equipment with TEC's certification label;

(b) TEC has specified certain essential requirements for various telecom equipment, which would need to be met before TEC grants the certification. On the other hand, the DoT is yet to specify the security requirements for equipment; and

(c) TEC's certification needs to be obtained only once for 1 (one) model of telecom equipment. In this regard, TEC has also clarified that where equipment with different model numbers are not substantially different from each other in respect of communication modules/interface cards, all such models may be considered belonging to the same family and only 1 (one) of such models (with higher configuration) can be tested and certified.

The above measures taken by the Government of India in relation to government contracts and procurement of telecom infrastructure applies to all departments of the government.

[Existing Legislation and Regulations]

Please see the response above in relation to the telecommunication infrastructure.

Telecommunication:

In addition to the above, the Department of Telecommunications, Government of India ("**DoT**") has on August 28, 2018 issued a notification[ii] which grants preferential market access to domestic telecom equipment suppliers and manufacturers. [36]

On September 26, 2018 the DoT issued the minimum requirements for security policy for DoT licensees ("**DoT guidelines**")[59] in furtherance of DoT's licensing conditions issued in May/June 2011 which mandated organisational Policy for Security and Security Management of licensees' telecom assets. The DoT guidelines aim to ensure adequate management directions and support for security arrangements in accordance with service continuity and relevant laws & regulations

[58] Procedure for Mandatory Testing and Certification of Telecommunication Equipment issued by Department of Telecommunications, Ministry of Communications, Government of India, http://tec.gov.in/pdf/Whatsnew/Final%20MTCTE%202017%20Procedure.pdf

[59] Minimum Requirements for Security Policy of DoT licensees dated September 26, 2018, issued by Department of Telecommunications, Ministry of Communications, Government of India, http://www.dot.gov.in/sites/default/files/MBBS.pdf?download=1

and provide direction for establishment, implementation, maintenance and continual improvement in Security and Security Management under its scope including security requirements related to vendors' /suppliers' contracts. It states that the security policy of DoT licensees' will have minimum provisions which shall be applicable for telecom networks, and systems holding customer's data including the endpoints through which such infrastructure and information is accessible. The DoT guidelines require Dot licensees to, inter alia:

(a) Designate a Chief Security Officer(s) for Network Security and Information Security and define his roles and functions;

(b) Auditing their network or get the network audited from security point of view once a year or as and when configuration of network is changed significantly;

(c) Ensure proper and effective use of encryption techniques/devices to protect confidentiality, authenticity and/ or integrity of information;

(d) Identify organizational assets including critical information infrastructure assets and appropriate protection responsibilities;

(e) Protection of telecom assets against intrusion of malware;

(f) Backup policy to protect against loss of data/information;

(g) Ensure that the customer data/information is operated, accessed and remains in the country at all times;

(h) To inspect the hardware, software, design, development, manufacturing facility and supply chain and subject all software to a security/threat check any time during the supplies of equipment as required; and

(i) Have a suitable agreement with hardware/ software manufacturer/ vendors and supplier of services to ensure that the equipment/ services/ software in the network, have been checked thoroughly for risk and vulnerabilities, backdoors etc. The agreement should cover aspects related to security measures like access control, password control and management etc. Clauses addressing the service continuity and service up gradation be included in the agreement, with consequences defined for each party in case of breach, particularly the security breaches. [37]

Electricity:

The Indian Electricity Grid Code ("**IEGC**")[60] is a Regulation made by the Central Electricity Regulatory Commission in exercise of powers of Section 79 and 178 of the Electricity Act, 2003. The IEGC lays down the mandatory rules, standards, guidelines to be followed by various persons and participants in power system to

[60] Central Electricity Regulatory Commission (Indian Electricity Grid Code) Regulations, 2010, dated April 28, 2010, https://powermin.nic.in/sites/default/files/uploads/Indian_Electricity_Grid_Code.pdf

plan, develop, maintain and operate the power system. The IEGC states, inter alia, that all utilities, shall have in place, a cyber security framework to identify the critical cyber assets and protect them so as to support reliable operation of the grid. [38]

The Central Electricity Regulatory Commission (Communication System for inter-State transmission of electricity) Regulations, 2017 ("**Electricity Regulations**") states that the Central Electricity Authority shall formulate and notify technical standards, cyber security requirements in accordance with the Cyber security Policy of the Government of India from time to time, protocol for the communication system for Power Sector within the country including the grid integration with the grid of the neighbouring countries.[61] [39]

The Electricity Regulations also state that the:

(a) Communication infrastructure shall be planned, designed and executed to address the network security needs as per standard specified by Central Electricity Authority and shall be in conformity with the Cyber Security Policy of the Government of India, issued from time to time;

(b) National Load Despatch Centre shall monitor case of cyber security incidences and take necessary action as deemed fit; and

(c) Regional Power Committee is to ensure that third party cyber security audits shall be conducted periodically and appropriate measures shall be implemented to comply with the findings of the audits. The audits will be conducted by Cert-In certified third-party auditors. [40]

[Forthcoming Legislation and Regulations and Discussions on Future Trends]

There are no forthcoming legislations, regulations or discussions in this regard.

References:

Links are provided in the form of footnotes for ease of reference.

(c) Equipment or services for consumers

[Existing Legislation and Regulations]

Please see the response above.

The Government of India has introduced, for good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services, the concept of assigning unique identity numbers termed as "Aadhaar number" to individuals residing in India. [41] The Aadhaar (Targeted Delivery of Financial and Other Subsidies,

[61] See 7.1 of the Central Electricity Regulatory Commission (Communication System for inter-State transmission of electricity) Regulations, 2017, http://www.cercind.gov.in/2017/regulation/134.pdf

Benefits and Services) Act, 2016 provides that every resident individual shall be entitled to obtain an Aadhaar number from Unique Identification Authority of India ("**UIDAI**") appointed by the Indian Government, by submitting his demographic information and biometric information by undergoing the process of enrolment. The enrolment data provided by the individual are strongly encrypted using public key cryptography encryption (PKI-2048 and AES-256) and (2048-bit encryption).

The IT Act has defined various terms, like "computer", "computer system", "computer network", "computer resource", "communication device", "computer source code", etc. and further provides for both civil and criminal penalties for unauthorised access or use of computers, computer systems or computer networks and disclosure of data stored therein (including sensitive personal data) by individuals and corporate entities. [42]

The IT Privacy Rules also mandate that any corporate entity (or any person who on behalf of such entity) collects, receives, possess, stores, deals or handles information, shall provide a privacy policy that discloses its practices regarding the handling of or dealing in personal information including sensitive personal data or information and ensure that the policy is available for view by such providers of information who have provided such information under lawful contract to the corporate entity. [43] Such policy shall be published on the website of the corporate entity (or the person acting on its behalf). The IT Privacy Rules require corporate entities collecting, processing and storing personal information, including sensitive personal information to comply with certain procedures. It distinguishes both "personal information" and "sensitive personal information", as defined below.

Under the IT Privacy Rules, a corporate entity must obtain the consent of the provider of the sensitive personal data or information in writing through letter or fax or any other mode of electronic communication regarding purpose of usage before collection of such information and such information shall be used only for the purpose for which it has been collected. The IT Privacy Rules also mandate the company to require prior permission from the provider of sensitive personal data or information before disclosing such information to any third party. [44] However, such consent will not be required if such disclosure has been agreed to in the contract between the corporate entity and the provider of information or where the disclosure is necessary for compliance of a legal obligation.

The transfer of sensitive personal data or information may be allowed by a corporate entity (or any person on its behalf) to any other corporate entity or person in India or in any other country that ensures the same level of data protection as provided for under the IT Privacy Rules. Such transfer may be allowed only if it is necessary for

the performance of the lawful contract between the corporate entity (or any person, who on behalf of such entity) and provider of information or where such person has consented for data transfer. Prior consent from the provider of information is also not required for sharing such information with the Indian Government agencies mandated under law to obtain information including sensitive personal data or information or if disclosure is made to any third party by an order of the authority or pursuant to the law for the time being in force.

Further, as stated above, the IT Privacy Rules, mandate that every corporate entity (or a person on its behalf) collecting personal information, including sensitive personal information to implement reasonable security practices and procedures and have a comprehensive documented information security policy containing managerial, technical, operational and physical security control measures. Any such corporate entity should implement either IS/ISO/IEC 27001 standard or the codes of best practices for data protection other than IS/ISO/IEC of any industry association or an entity formed by such an association approved and notified by the Government of India.

[Forthcoming Legislation and Regulations and Discussions on Future Trends]

As mentioned above, the PDP Bill has been introduced which aims to protect the autonomy of individuals from data privacy violations by the state and private entities. [45]

The draft of the Digital Information Security in Healthcare Act (DISHA)[62] was also released in the public domain for comments. It aims to provide for electronic health data privacy, confidentiality, security and standardization and provide for a National Health Authority in India which shall be responsible for enforcing privacy and security measures for electronic health data, and to regulate storage and exchange of the same. [46]

References:

Links are provided in the form of footnotes for ease of reference.

b. 法律事務所を通じたQ&A

1. インドにおける"Critical Infrastructure"の定義は何か？
   - ✓ Ans: The term 'critical infrastructure' has not been defined under Indian laws or policies framed thereunder. [47] While the National Cyber Security Policy, 2013 refers to the term 'critical sectors,' but the same has not been defined

[62] Draft of Digital Information Security in Healthcare Act, https://mohfw.gov.in/newshighlights/comments-draft-digital-information-security-health-care-actdisha

thereunder (https://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf). The draft National Cyber Security Policy, 2013 suggests that critical sectors include finance, defence, energy, transportation and telecommunication (https://meity.gov.in/writereaddata/files/ncsp_060411.pdf (page 8)). The notification issued pursuant to the National Cyber Security Policy, 2013 mentions critical sectors to include banking, telecommunications and power [48] (http://pib.nic.in/PressReleaseIframePage.aspx?PRID=1525356).

- ✓ The Information Technology Act defines the term 'critical information infrastructure' to mean the computer resource, the incapacitation or destruction of which, shall have the debilitating impact on national security, economy, public health or safety. [49] Please see Section 70(1) of the Information Technology (Amendment) Act, 2008 (https://meity.gov.in/writereaddata/files/it_amendment_act2008%20%281%29_0.pdf)

2. The Indian Telegraph (Amendment) Rules, 2017, provides that any telegraph which is used or capable of being used with any telegraph established, maintained or worked under the licence granted by the Government of India must undergo prior mandatory testing and certification by the Telecommunication Engineering Centre, DoT, Ministry of Communications ("TEC") before sale of such telegraph in India ("Telegraph Rules"). で述べられている telegraph へのテスト及び認証について、これは構想段階／評価段階ではなく、すでに正式導入されている制度という認識で正しいか？

- ✓ Ans: As per the notification dated September 27, 2018 issued by the Department of Telecommunications, Ministry of Communications, Government of India, the prior mandatory testing and certification of telecom equipment imported or sold in India were to commence from January 1, 2019. However, a subsequent notification dated December 31, 2018, states that proposal to extend the said date of January 1, 2019 is under consideration by the Government of India and the fresh dates shall be separately notified. We note that no fresh date has presently been notified. Accordingly, we understand that at present, mandatory testing and certification of telecom equipment prior to its sale or import in India, is not conducted. [50] Please refer to the following links: http://tec.gov.in/pdf/Whatsnew/TECNotificationSept18.pdf ; http://tec.gov.in/pdf/Whatsnew/TECNotification31Dec18.pdf

3. これは政府調達にのみ適用されるものなのか？あるいは民間での調達にも適用されるのか？

- ✓ Ans: The Telegraph Rules state that any original equipment manufacturer / importer who wishes to **sell or import any telecom equipment in India**, shall have to get mandatory testing and certification done before sale/ import of telecom equipment in India. The requirement for prior mandatory testing and certification is not restricted only to government procurement but extends to any telegraph equipment sold or imported in the Indian market. [51] Please see Rules 529, 531, 532 and 533 of the Indian Telegraph Rules, 1951. Please refer to the following link: http://tec.gov.in/pdf/Whatsnew/eGazetteNotif.pdf

4. 政府調達／通信インフラ・重要インフラの調達／コンシューマー向け機器・サービスの調達において、違反として摘発された事例や排除された事例はないか？

- ✓ Ans: (1) ***Government Procurement***: While there are no separate cyber security regulations governing government contracts and public procurement of goods and services in India, public procurement of goods and services in India are largely governed by the rules and directives stipulated in the General Financial Rules 2017, Manual for Procurement of Consultancy and Other Services 2017 and Manual for Procurement of Goods 2017, issued from time to time by the Ministry of Finance, Government of India ("**General Rules**") [52] (Please refer to the following links: https://doe.gov.in/sites/default/files/GFR2017_0.pdf; https://doe.gov.in/sites/default/files/Manual%20for%20Procurement%20of%20Consultancy%20and%20Other%20Services%202017_0.pdf; https://doe.gov.in/sites/default/files/Manual%20for%20Procurement%20of%20Goods%202017_0_0.pdf). The General Rules also provide for blacklisting and temporary or permanent debarment of suppliers by the procuring government entity in the event of breach of the contract or code of integrity, by the suppliers. The relevant supplier may also be removed from the list of suppliers/ banned if, *inter alia*, (i) the Central Bureau of Investigation/Central Vigilance Commission /Comptroller and Auditor General of India or Vigilance Department of procuring government entity or any other investigating agency recommends such a course in respect of a case under investigation; (ii) due to national security considerations as determined by appropriate agencies of Government of India; or (iii) on any other grounds based on which the Government of India, considers that banning is in public interest.
  There have been instances wherein the procuring government entities have blacklisted suppliers from participation in the procurement process on account of breach of contract or failure to furnish appropriate bank guarantee or due to corruption charges (Please see the following links: http://dot.gov.in/sites/default/files/2018_07_13%20Circulation%20Blacklisted%20Firm.pdf; http://www.pib.nic.in/Pressreleaseshare.aspx?PRID=1539032). However, the local counsel is not aware of any instance wherein any procuring government entity has debarred or blacklisted any supplier on account of breach or threatened breach of cyber-security. [53]

  (2) ***Procurement of Telecommunication and Other Critical Infrastructure***: To update the response provided in December 2018, the Government of India has clarified that at present, there is no proposal before the government considering banning telecom gear and equipment made by Huawei and that mobile companies are free to buy equipment from any equipment maker based on their techno-commercial interests, provided they adhere to all the security requirements as per licence conditions (Please refer to the following news article: https://economictimes.indiatimes.com/industry/telecom/telecom-news/manoj-sinha-says-no-plan-yet-to-ban-huawei-telecom-equipment/articleshow/67391143.cms).
  As stated above, while there have been instances wherein suppliers have been blacklisted on account of breach of contract or failure to furnish appropriate bank guarantee, the local counsel is not aware of any debarment or prosecution by public authorities in India in connection to procurement of telecom equipment or any other critical infrastructure on account of breach or threatened breach of cyber-security. [54]

(3) ***Equipment or Services for Consumers***: Under the Consumer Protection Act, 1986, the Government of India and the State Governments are empowered to file either in their individual capacity or as a representative of interests of the consumers in general, a complaint in relation to any goods sold or delivered or agreed to be sold or delivered or any service provided or agreed to be provided (Please see Section 12(1) (d) of the Consumer Protection Act, 1986). Please refer to the following link: http://ncdrc.nic.in/bare_acts/consumer%20protection%20act-1986.html#_Hlk149662073).

There have been cases where the government has filed complaints to the consumer protection forum on behalf of the consumers. The local counsel has, however, not come across any case of debarment or prosecution by public authorities in India on account of breach or threatened breach of cyber-security in connection to equipment or services for consumers. [55]

c. 法律事務所による回答以外の情報ソース

- Government mulls scrutiny on Huawei, ZTE for commercial 5G rollout after security concerns: Official [56]
  https://economictimes.indiatimes.com/industry/telecom/telecom-news/government-mulls-scrutiny-on-huawei-zte-for-commercial-5g-rollout-after-security-concerns-official/articleshow/67180409.cms

---

[i] Guidelines to compliance to Quality requirements of E-procurement Systems dated August 31, 2011 issued by STQC Directorate, Department of Information Technology, Ministry of Communications and Information Technology, Government of India, http://www.egovstandards.gov.in/sites/default/files/Compliance%20to%20Quality%20Requirements%20of%20e-Procurement%20Systems.pdf

[ii] Notification dated August 29, 2018 on Public Procurement (Preference to Make in India) Order 2018 – Notification of Telecom Products, Services or Works regarding, issued by Department of Telecommunications, Ministry of Communications, Government of India, https://dipp.gov.in/sites/default/files/Telecommunications_29082018.pdf

5.2.2.9 中国

5.2.2.9.1 国としての全体的な状況(まとめ)

中国の政策動向の概要を表 5-34 に示す。

表 5-34　中国の政策動向（まとめ）

	項目	概要
現状	全体傾向	2017 年制定のサイバーセキュリティ法にて、ネットワーク事業者/重要インフラ事業者が遵守すべきサイバーセキュリティの義務や個人情報の保護に関する義務を記載、国策や国防の観点から国家によるサイバー空間の監督を強化している。
	重要インフラの法制度	サイバーセキュリティ法にて、重要インフラ事業者に対して専門部署設置/担当者任命/セキュリティ面からの経歴確認/定期的なサイバーセキュリティ教育/技術訓練と技能評価の実施等、適切なセキュリティ保護確保の責務を規定したほか、個人情報/重要データの中国領土内保管等を定めている。このほか、産業制御システムのサイバー脅威に対応するガイドライン等各種ガイドラインを発行している。
	政府調達	GPL Implementation Regulation において、中国で入手できないケースを除き、製品/サービスを国内から調達することが求められている。また、基幹ネットワーク機器やセキュリティ製品は中国国内の標準に準拠し、認定リストに記載されたものでなければ販売できず、また使用もしてはならないと定めている。
	認証/認定制度	サイバーセキュリティ法、及び「ネットワーク製品及びサービス安全審査弁法」に基づき重要インフラ運用者は毎年安全検査測定評価実施が必要。また、基幹ネットワーク機器やセキュリティ製品の販売/使用には、中国国内の標準に準拠の上、国家インターネット安全弁公室が実施する安全審査に合格（認定リストに記載）する必要がある。
	体制	2011 年に創設の中国サイバースペース管理局（CAC）がサイバーセキュリティに関する政策作成を行う。中央公安部（MPS）はネットワークのセキュリティ保護を担当する。工業情報化部(MIIT) はインターネットベースのビジネスに関する規制を所管、電気通信事業に相当する包括的な法令「電信条例」を所掌する。このほか国家暗号管理局（NCA）は商用の暗号製品の規制を所管する。
今後	全体的な傾向	製造業の強国を目指す“Made in China 2025”に向けて、サイバーセキュリティ法をベースに国防だけでなく経済政策に対象を広げた上で、規制の強化・整備が進展するものと考えらえる。
	重要インフラの法制度	サイバーセキュリティ法をベースに規制の強化･整備が進むものと思われる。
	政府調達	現行の調達制度をベースに強化・整備が進むものと思われる。

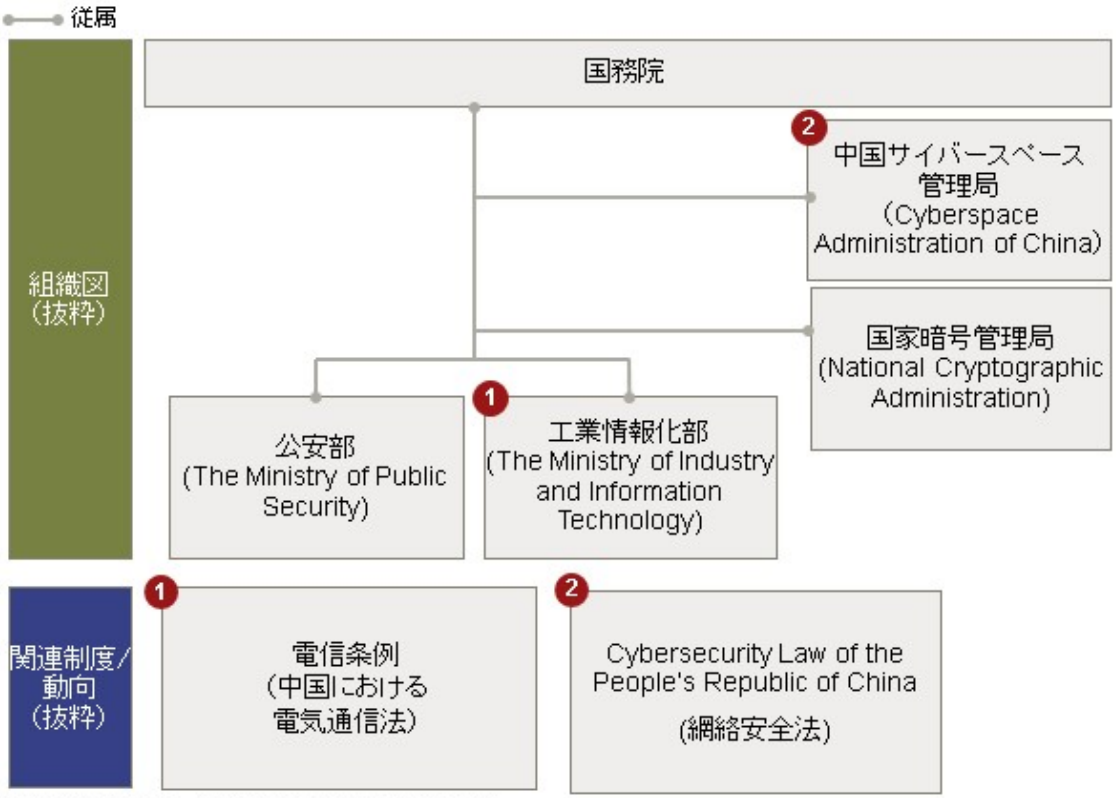
現在の中国におけるサイバーセキュリティの法規制は 2017 年に施行されたサイバーセキュリティ法（Cybersecurity Law of the People's Republic of China :中华人民共和国网络安全法）が中心となっている。この法律では、格付け方式に従って、すべてのネットワーク事業者が遵守すべきサイバーセキュリティに関する義務、重要インフラ事業者が遵守すべ

きサイバーセキュリティの義務、個人情報の保護に関する義務の三つをネットワーク事業者に課す包括的なものとなっている。

政府調達に関する法律については、2003 年に発効された政府調達法（Government Procurement Law: 中华人民共和国政府采购法）と 2000 年に発効された入札法（Tendering and Bidding Law: 中华人民共和国招标投标法）が存在する。前者は中国の政府機関による調達を規定していたものであり、後者は中国の国営企業や民間企業によるインフラ工事に関する調達について、それぞれ定めている。

今後については、中国では IoT やインターネットを活用して、製造業の強国を目指す政策「メイドインチャイナ 2025」で必要不可欠であることから、今後もサイバーセキュリティの拡充が続くと思われる。拡充に際しては、サイバーセキュリティ法に沿って進めていくものと思われる。また、欧米等で中国のネットワーク製品を排除する動きが広がっているが、今回調査した限りにおいては、中国では欧米企業のネットワーク製品を排除するという動きは特に見られない。

図 5-12 は、中国における政府関連組織と関連法制度をまとめたものである。番号により、組織と法制度の関連性を表現している（組織の概要は表 5-35 を、法制度の概要は表 5-36 を参照）。MPS（中国公安部: The Ministry of Public Security）はネットワークのセキュリティ保護を行う機関である。MIIT（工業情報化部: The Ministry of Industry and Information Technology）は、インターネットベースのビジネスに関する規制（ライセンスの発行等）を主な所管している。また、電気通信事業に関する包括的な法令である「電信条例」も所掌となっている。中国サイバースペース管理局は 2011 年に設立された。中国サイバースペース管理局はサイバーセキュリティに関するすべての問題の調整と政策作成に注力することが求められている。また、サイバーセキュリティ法を所掌している。NCA（国家暗号管理局: The National Cryptographic Administration）はネットワーク保護に利用される商用の暗号製品の規制を所管している。



各関連制度/動向と関連する省官庁の番号と対応
出所(公開情報をもとにICRが作成)

図 5-12　中国の政府関連組織と関連法制度

表 5-35　中国における政府関連組織

中国公安部	ネットワークのセキュリティ保護を行う機関。
工業情報化部	主にインターネットベースのビジネスに関する規制（ライセンスの発行等）を所管。
中国サイバースペース管理局	サイバーセキュリティに関する政策を作成。 国務院の所属ではないが、中国のサイバーセキュリティの問題に対して重要な役割を果たす組織であり、サイバーセキュリティに関する課題の調整と政策策定に焦点を当てた機関で、サイバーセキュリティ法を主管する。
国家暗号管理局	ネットワーク保護に利用される商用の暗号製品の規制を所管。

表 5-36　中国における関連法制度

電信条例	中国における電気通信事業法。
サイバーセキュリティ法	すべてのネットワーク事業者が遵守すべき義務、重要インフラ事業者が遵守すべき義務、個人情報の保護に関する義務を規定。

5.2.2.9.2 対応状況

a. IoT セキュリティ全般

中国のサイバーセキュリティに関して正式に発表された規制は、1994 年に公表されたコンピュータ情報システム安全保護条例（Regulations of the People's Republic of China on the Security Protection of Computer Information System (1994): 中华人民共和国计算机信息系统安全保护条例）、2003 年 7 月に意見書が公表された、国家情報化指導組織の情報セキュリティ保障業務に関する意見（国家信息化领导小组关于加强信息安全保障工作的意见）に遡ることができる。

サイバーセキュリティ法は 2017 年に施行されており、ネットワーク事業者が遵守すべきサイバーセキュリティに関する義務、重要インフラ事業者（OCII）が遵守すべきサイバーセキュリティの義務、個人情報の保護に関する義務の三つをネットワーク事業者に課す包括的なものとなっている。サイバーセキュリティ法でのネットワークの定義と、その対象をまとめると表 5-37 のようになる。サイバーセキュリティ法でのネットワークとは、コンピュータ、その他の情報端末等により構成される情報システムである。また、ネットワーク運営者、重要情報インフラ運営者、ネットワーク製品及びサービス提供者は、その内容によりそれぞれ分類される。

表 5-37　中国のサイバーセキュリティ法での定義と対象[63]

項目	内容
サイバーセキュリティ法でのネットワークの定義	コンピュータ、その他の情報端末及び関連設備により構成される情報システムをいい、インターネット、移動通信ネットワーク、VPN 等が含まれる。
ネットワーク運営者（対象）	ネットワークの所有者、管理者及びネットワークサービス提供者をいう。
重要情報インフラ運営者（対象）	ネットワーク運営者のうち、そのネットワーク施設または情報システムの機能が破壊され、もしくは失われ、またはそのデータが漏洩すれば、国の安全、国の経済、人民の生活、公共の利益が著しく損なわれる可能性のあるような重要情報インフラを運営する者は「重要情報インフラの運営者」に該当する。
ネットワーク製品及びサービス提供者（対象)	ネットワーク製品及びサービス提供者には、ネットワークに関連する設備またはソフト等を生産、販売する企業、クラウドコンピューティングサービス、データの処理及び保存サービス、インターネット通信サービス等を提供する事業者がネットワーク製品及びサービス提供者に該当する。

ネットワーク事業者のサイバーセキュリティ義務は、以下の通りとなる。

- ネットワークが干渉、混乱または不正アクセスから解放されていることを保障し、ネットワークデータの漏洩、盗難、改ざんを防止する義務。ネットワークの格付けに基づいて要件が定められており、内部セキュリティ管理システムと運用指示の策定、サイバーセキュリティを危険にさらす活動を防止するための適切な技術的対策、ネットワーク運用とサイバーセキュリティ事案を監視及び記録するための適切な技術的対策の実行、データ分類、バックアップに関する適切な対策の実行、重要なデータの暗号化等が含まれる。
- システムのバグ、コンピュータウイルス、ネットワーク攻撃や侵入等のセキュリティリスクに迅速に対応するサイバーセキュリティ事案への緊急時対応計画を定める義務。

また、サイバーセキュリティ法では、重要インフラ事業者に対する責務を規定している。主な責務は下記の通りである。

- 適切なセキュリティ保護を確保する責務。責務には、セキュリティ管理専門の部署の設置、セキュリティ担当者の任命、当該人物及び主要な立場にある人物のセキュリティ面からの経歴の確認、及び実務者への定期的なサイバーセキュリティ教育、技術訓練と技能評価の実施等が含まれる。また、重要インフラ事業者は、重要なシステムとデータベースの災害復旧及びバックアップ計画を確立すること、サイバーセキュリティ事案に対する緊急計画を作成すること、また、定期的に模擬訓練を実施すること等の義務を負っている。
- 中国国内での運用中に収集及び生成された個人情報及び重要なデータを中国の領土内に保管する責務。そのような情報及びデータを事業目的のために海外に転送しなければならない場合は、関連する措置に従ってセキュリティ評価を実施することとされている。
- サイバーセキュリティ及び潜在的なリスクの調査及び評価を行い、その結果及び改善策を所管インフラストラクチャの安全当局に提出する責務。これらは、独力により、あ

[63]「中国におけるサイバーセキュリティー法規制にかかわる対策マニュアル」（2018 年 2 月、ジェトロ）より作成

るいはサイバーセキュリティサービスプロバイダーを通じて、年に 1 度行う。

また、上記の責務が果たされなかった場合の処罰・罰金を、以下の表 5-38 にまとめる。各区域の公安部門内に設けられたインターネット情報部門が、表中のすべての行為に対して、是正を命じ、警告を与える。また、是正を拒絶し、情状が重大であり、サイバーセキュリティに危害を及ぼす等の結果をもたらした場合には、各対象に「罰金 i」が科される。また、直接責任を負う主管者及びその他の直接責任者に対しては、「罰金 ii」が科される。

表 5-38　中国のサイバーセキュリティ法で制定されている処罰行為等[64]

対象	行為	罰金 i	罰金 ii
ネットワーク運営者	サイバーセキュリティ等級保護義務を履行しないとき	1～10 万元	5,000～5 万元
	サイバーセキュリティ事件緊急対応プランを制定しないとき	同上	同上
	実名制義務を履行しないとき	5～50 万元	1～10 万元
	違法にサイバーセキュリティ認証、検査等の活動を実施したとき、またはシステムのバグ、インターネット攻撃等のサイバーセキュリティ情報を対外的に公布しないとき	1～10 万元	5,000～5 万元
	個人情報を侵害したとき	違法所得の 1～10 倍（違法所得がない場合には 100 万元以下）	1～10 万元
	ユーザー発布情報に対する管理を強化しなかったとき	10～50 万元	同上
	法執行協力義務を履行せず、またはその履行を拒否したとき	5～10 万元	同上
重要情報インフラ運営者	サイバーセキュリティ保護義務を履行しないとき	10～100 万元	1～10 万元
	データ現地化の要求に違反したとき	5～10 万元	同上
	国の安全審査規定に違反したとき	購入金額の 1～10 倍	同上
ネットワーク製品及びサービス提供者	製品及びサービスの安全に関する義務に違反したとき	5～50 万元	1～10 万元

他にも IoT セキュリティ関連では産業用制御システムのサイバーセキュリティに関するガイドライン「The Guidelines on the Emergency Management of Information Security Incidents in the Industrial Control System（工业控制系统信息安全事件应急管理工作指南）(“Industrial Control System Guidelines”) 」が存在する。このガイドラインでは、産業用制御システムのセキュリティを確立し、サイバー脅威を監視するとともに報告することが指導されている。

[64]「中国におけるサイバーセキュリティー法規制にかかわる対策マニュアル」（2018 年 2 月、ジェトロ）より作成

b. 重要インフラ

1994 年に公表されたコンピュータ情報システム安全保護条例（Regulations of the People's Republic of China on the Security Protection of Computer Information System (1994): 中华人民共和国计算机信息系统安全保护条例）に基づき、対象となるネットワークの「格付け方式」がベースとなり、重要インフラ事業者が分類された。

2007 年には情報安全等級保護管理弁法（The Measures on Security Examination for Online Products and Services (2007): 信息安全等级保护管理办法）が発表され、情報システムの新たな格付けに関する詳細な内容を提供している。上記した「格付け」に関しては、以下の表 5-39 のようにまとめることができる。

表 5-39 対象となるネットワークの格付け

格付け	内容
グレード I	このグレードの情報システムを破壊しても、市民、法人、及びその他の団体の合法的な権利と利益には損害が生じるが、国家の安全保障、社会秩序または公共の利益には損害が生じない
グレード II	このグレードの情報システムの破壊は、市民、法人、その他の団体の合法的な権利や利益に重大な損害を与えたり、社会秩序や公共の利益に損害を与えたりするが、国家の安全を損なうことはない。
グレード III	このグレード情報システムを破壊すると、社会秩序や公益に重大な損害を与えたり、国家安全保障に損害を与えたりする。
グレード IV	このグレードの情報システムの破壊は、社会秩序や公共の利益に特に重大な損害を与えるか、国家安全保障に重大な損害を与える。
グレード V	このグレードの情報システムの破壊は、国家安全保障に特に重大な損害を与える。

また、サイバーセキュリティ監査の運用を記載したガイドライン（The National Guidelines for Operation of Cyber Security Inspection: 国家网络安全检查操作指南）では、どのような種類のネットワークを監査の対象とすべきかについて次のように示されている。①重要な事業（表 5-40）を特定し、②その事業を支援する情報システムを特定し、③情報システムに依存している程度、またはインシデントが発生した際に生じる影響に基づいて重要インフラを定めるとしている。ただし、上記の情報システムは、事業により産業用制御システムに読み替える。

表 5-40　中国における重要な事業

産業分野		重要事業
エネルギー	電力	・　発電（火力、水力、原子力等を含む） ・　送電 ・　配電
	石油及び石油化学	・　原油及びガス開発 ・　精製 ・　石油とガスの輸送 ・　石油とガスの貯蔵
	石炭	・　石炭鉱業 ・　石炭化学
金融		・　銀行業務 ・　証券及び先物取引 ・　決済 ・　保険業務
運輸	鉄道	・　旅客サービス ・　貨物サービス ・　輸送生産 ・　駅管理
	航空	・　航空管制 ・　空港管理 ・　航空券予約、離陸及び飛行計画検査 ・　航空会社運営
	高速道路	・　高速道路交通管制 ・　高度道路交通システム（T-union, ETC による課金等）
	水運	・　水運会社運営（旅客及び貨物サービスを含む） ・　港湾管理及び運営 ・　水運管制
水産業		・　給水差し止めと制御 ・　長距離給水制御 ・　都市給水源管理
保健医療		・　病院その他の保健機関の運営 ・　疾病対策 ・　救急センター運営
環境保護		・　環境モニタリングと早期警戒（水、大気、土壌、放射能線等）
製造（原材料、設備、消耗品、電子製品）		・　企業経営と管理 ・　知的生産システム（産業用インターネット、IoT、スマートデバイス等） ・　有害化学物質（放射性化学物質を含む）の製造、加工、貯蔵及び管理 ・　危険度の高い産業施設の運用と管理
都市建設		・　水・熱・ガスの供給管理 ・　都市鉄道 ・　下水道 ・　スマートシティの運用･管理
電気通信及びインターネット		・　音声、データ、インターネットの基盤となるネットワーク及びハブ ・　ドメインの名前解決とトップレベルのドメイ

産業分野	重要事業
	ンネーム登録管理 ・ データセンター／クラウドサービス
ラジオ及びテレビ	・ テレビ放送管理 ・ ラジオ放送管理
政府機関	・ 情報公開 ・ 公共サービス ・ 事務システム

c. 政府調達

政府調達に関する法律については、2003 年に発効された政府調達法が存在する。この法律は、中国の財政部によって管理されている。この法律が発効されるまでは、統一された政府調達の規則が存在せず、政府機関や地方自治体でそれぞれに独自に行われていた模様である。そのため、調達に関する透明性の欠如や汚職、紛争時の解決メカニズムが存在しないことが課題であったが、政府調達法の施行により中国における政府調達に関するルールが定められたといえる。

政府調達法で定められている政府とは、あらゆるレベルでの政府部門、機関、公的部門のことであるとされている。また、これらの主体が調達する際の製品、サービス、工事は中国の財政部が作成したカタログに掲載されている（カタログの詳細は不明）。なお、政府調達法には軍部による調達は含まれておらず、中国の中央軍事委員会が定めるものと記載されている。詳細に関しては不明である。

また、政府調達法では、政府調達で必要とされる製品、サービスが中国で利用できない、調達されたものが中国の国外で利用されるといった場合を除いて、基本的には中国国内から調達することが求められている。

その他、2000 年に発効された入札法では政府調達法では対象とされていない、国有企業による調達、また民間企業によるインフラストラクチャ構築に関する調達が定められている（入札法は国家発展改革委員会（National Development and Reform Commission：中华人民共和国国家发展和改革委员会）が管理している）。

また、その他に政府調達に関連するものとしては、WTO による WTO 政府調達協定がある。WTO 政府調達協定では、協定に加盟する国間での政府や自治体による物品、サービス、工事の国際的なルールを定めるものである。日本の外務省の Web サイトの情報によれば、2018 年 9 月時点で中国は加盟申請国となっている。

5.2.2.9.3 今後の方向性

中国がサイバーセキュリティに関する規制や制度を整備する理由は、サイバースペースの拡大と、それに伴うサイバー脅威という国防上の問題があるかと考えられる。また、近年、中国においては、2025 年までに、IoT やインターネットといった技術を活用して、製造業の強国になることを目指す「メイドインチャイナ 2025」という政策がある。IoT やインターネットを活用した製造には情報セキュリティの確保は必要不可欠であると考えられる。そのため、2017 年に施行されたサイバーセキュリティ法の導入に伴って中国がサイバーセキュリティの拡充を図っていることがわかる。このような法律が制定されたことで、IDC 中国は中国のセキュリティ市場が 2017 年に 230 億元であったものが、2021 年には 657 億元に拡大し、年成長率が 23.4%になると推計しており、産業として中国のサイバーセキュリティ市場が拡大することが指摘されている。そのため、今後もサイバーセキュリティは国防のみならず、中国の新たな経済政策を支えるものとして今後強化していくことが予想され

る。

また、米国、オーストラリア、ニュージーランド、欧州の一部の国等で Huawei 等、サイバーセキュリティの観点から、中国のネットワーク製品を排除する動きが広がっている。これらの国の製品について報復措置として中国から排除することが懸念されるが、今回調査した限りにおいては、中国ではそのような動向は見つけることができなかった。

5.2.2.9.4 Evidence 及び原典

ア） 国としての全体的な状況（まとめ）

- Regulations of the People's Republic of China on the Security Protection of Computer Information System (1994)（中华人民共和国计算机信息系统安全保护条例）
  http://www.mps.gov.cn/n2254314/n2254409/n2254419/n2254429/c3721836/content.html
- Opinions of the National Informatization Leadership Group regarding Strengthening Information Security Safeguard Work（国家信息化领导小组关于加强信息安全保障工作的意见）
  http://www.chinastor.com/a/netsafe/0209362A2017.html
- Cybersecurity Law of the People's Republic of China（中华人民共和国网络安全法）
  http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm
- The Guidelines on the Emergency Management of Information Security Incidents in the Industrial Control System（工业控制系统信息安全事件应急管理工作指南）
  http://www.cac.gov.cn/wxb_pdf/cac2017062002.docx
- 国家互联网信息办公室（中国サイバースペース管理局：Cyberspace Administration of China）
  http://www.cac.gov.cn/
- 中华人民共和国公安部（中国公安部：The Ministry of Public Security）
  http://www.mps.gov.cn/
- 工業和信息化部（工業情報化部: The Ministry of Industry and Information Technology）
  http://www.miit.gov.cn/

イ） 対応状況

- IoT セキュリティ全般
  - ✓ Cybersecurity Law of the People's Republic of China（中华人民共和国网络安全法）
    http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm
  - ✓ The Guidelines on the Emergency Management of Information Security Incidents in the Industrial Control System（工业控制系统信息安全事件应急管理工作指南）
    http://www.cac.gov.cn/wxb_pdf/cac2017062002.docx
  - ✓ 「中国におけるサイバーセキュリティ法規制にかかわる対策マニュアル」(2018 年 2 月、ジェトロ)
    https://www.jetro.go.jp/ext_images/_Reports/02/2018/155b6354c9acea0c/cn-report.pdf

- 重要インフラ
  - ✓ Regulations of the People's Republic of China on the Security Protection of Computer Information System (1994) （中华人民共和国计算机信息系统安全保护条例）
    http://www.mps.gov.cn/n2254314/n2254409/n2254419/n2254429/c3721836/content.html
  - ✓ The Measures on Security Examination for Online Products and Services (2007)（信息安全等级保护管理办法）
    URL については不明

- 政府調達
  - ✓ 中华人民共和国政府采购法（Government Procurement Law）
    http://www.npc.gov.cn/wxzl/wxzl/2002-07/10/content_297298.htm
  - ✓ 中华人民共和国招标投标法（Tendering and Bidding Law）
    http://www.npc.gov.cn/englishnpc/Law/2007-12/11/content_1383557.htm

ウ） 今後の方向性

- 中国制造 2025
  http://www.miit.gov.cn/n973401/n1234620/n1234622/index.html

5.3 業界団体のセキュリティ対策に関する調査

5.3.1 調査目的

IoT ネットワーク（5G）におけるセキュリティを議論するにあたって、そのデジュールスタンダード・デファクトスタンダードとなる業界標準を検討する業界団体の動向の把握が必要である。業界団体の中でも、モバイルネットワーク業界で主要な業界団体である 3GPP にてセキュリティ関連のテストスペック策定、GSMA にてそのスペックの運用スキーム作りが進んでおり、そのスキームの策定状況及びその方向性について調査を実施した。

調査対象は先述の通り、ネットワーク機器向けの主要な業界団体である表 5-41 に示す 2 団体とする。

表 5-41 調査対象の業界団体

業界団体	概要
3GPP	1998 年の設立以来、3G、4G、5G のモバイルネットワークシステムの仕様検討・作成を行ってきた標準化を行う団体。ネットワーク機器ベンダー、通信事業者、各国の政府関係者が参加し、セキュリティの検討も実施している。
GSMA	元々は GSM 方式を採用していた通信事業者やベンダー等、関連企業からなる業界団体であり、1995 年に設立された。ネットワーク機器評価のフレームワークを検討している。

5.3.2　業界団体のセキュリティ対策の取り組み

5.3.2.1 3GPP

3GPP の組織図は図 5-13 の通りである。3GPP におけるセキュリティに関する議論は、PCG（Project Co-ordination Group）配下の三つの検討グループ（TSG: Technical Specification Group）の中でも、サービスとそれを実現するアーキテクチャを規定する SA (Service & system Aspect) の WG (Working Group) 3 にて行われている（以下 SA3 と表現する）。

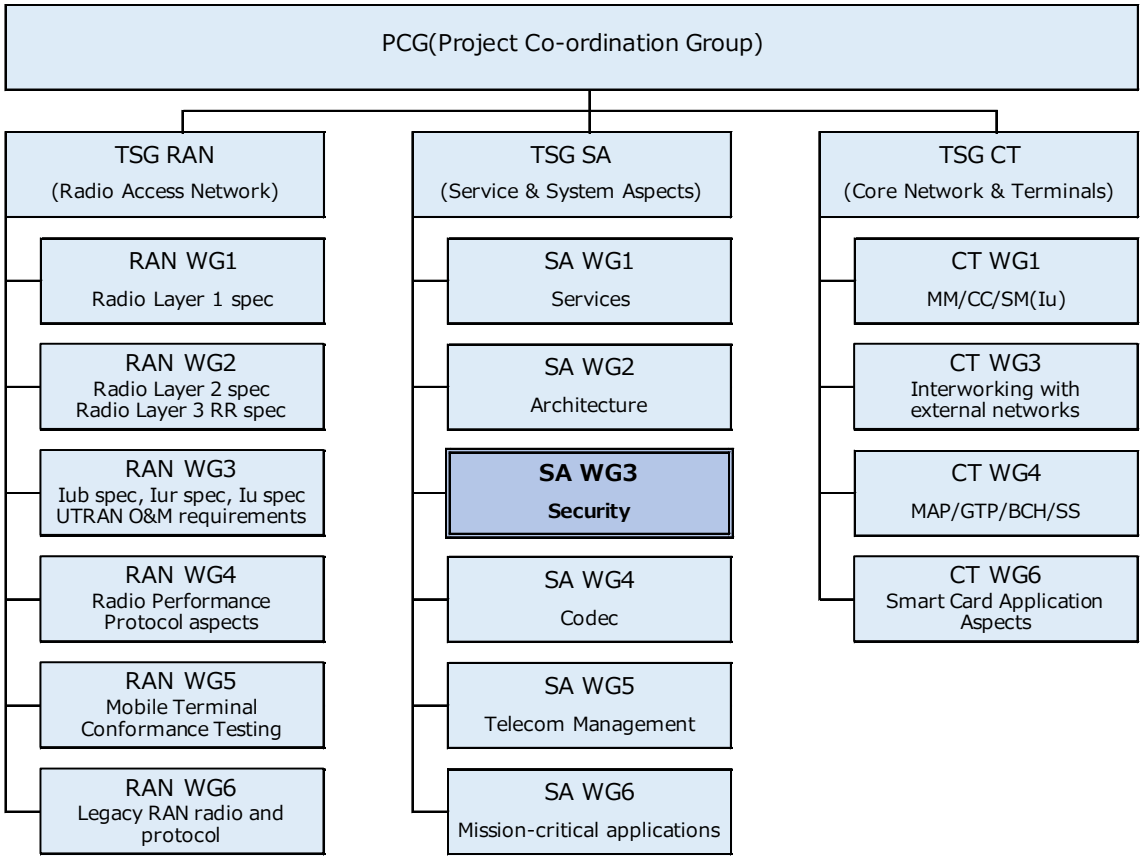


図 5-13　3GPP の組織図[65]

ネットワークが社会インフラストラクチャの重要な機能を担うにつれ、ネットワーク製品において強固なセキュリティの必要性がますます重要になっている。そのような背景を受け、SA3 ではセキュアなネットワークアーキテクチャの提供を目的として、SECAM (SECurity Assurance Methodology) と呼ばれるセキュリティアシュアランスと評価のフレームワークを作成した。これは 3GPP のスコープ範疇のネットワーク機器について、共通かつテスト可能なセキュリティベースラインの提供を目指したものである。ネットワーク機器のセキュリティ脆弱性への各ベンダーの対策をネットワークオペレーターが直接コントロールすることは困難なため、その対策状況をオペレーターが客観的に判断できるよう、ベンダーが準拠すべきセキュリティ対応指針として策定された。SECAM のプロセスを図 5-14 に示す。

[65] 以下の資料を基に NEC が作成
Specification Groups
https://www.3gpp.org/specifications-groups

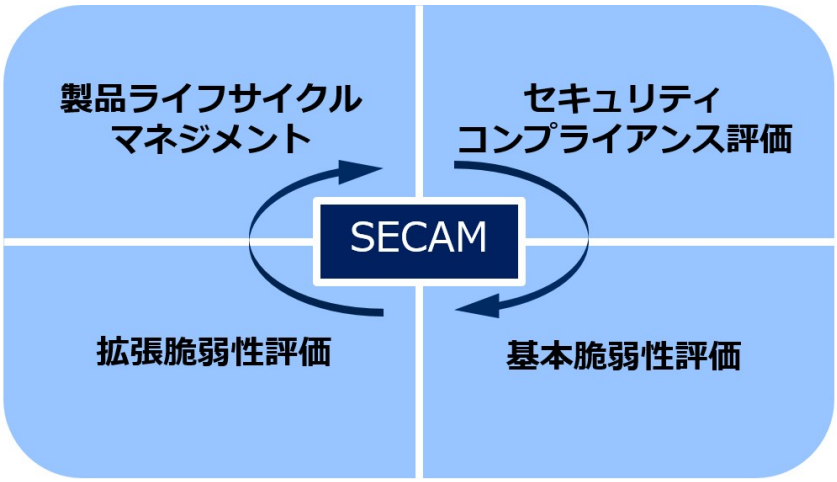


図 5-14　SECAM 概要[iii]

SECAM の評価は以下のタスクをカバーするものである。

(1) ベンダーのネットワーク製品における開発プロセス及びライフサイクルマネジメントプロセスの遵守（製品開発プロセスがベンダーのネットワーク製品開発及びネットワーク製品ライフサイクルマネジメントプロセス保証の要件に準拠しているかの評価）。

(2) セキュリティコンプライアンス評価（要求されたセキュリティ要件がネットワーク製品に正しく実装されているかの評価）。これには基本的な脆弱性評価が含まれる。

SECAM にて定義されたセキュリティアシュアランスプロセスを、3GPP にて規定した各ネットワーク機器クラスにて実現すべきセキュリティ要件とその評価として規定したものが SCAS (Security Assurance Specification) である。2019/2 時点で 3GPP にて SCAS が定義及び検討されているネットワーク機器クラスは表 5-42 の通りである。3G/LTE のネットワーク機器を対象とした TS は Release 15 までに FIX しており、5G 向けについては Release 16 にて議論、FIX 予定となっている。

表 5-42　SCAS 対応ネットワーク機器クラス

3GPP Ref.番号	ネットワーク機器クラス名称	通信世代
TS 33.116	MME	3G/LTE
TS 33.117	全ネットワーク機器	ALL
TS 33.216	Evolved NodeB (eNB)	LTE
TS 33.511	NR Node B	5G
TS 33.512	Access and Mobility management Function (AMF)	5G
TS 33.513	User Plane Function (UPF)	5G
TS 33.514	Unified Data Management (UDM)	5G
TS 33.515	Session Management Function (SMF)	5G
TS 33.516	Authentication Server Function (AUSF)	5G
TS 33.517	Security Edge Protection Proxy (SEPP)	5G
TS 33.518	Network Repository Function (NRF)	5G
TS 33.519	Network Exposure Function (NEF)	5G
TR 33.818	3GPP virtualized network products (※)	5G
TR 33.916	3GPP network products	3G/LTE

(※) TR 33.818 では仮想化製品向けの SECAM も定義されている。

SCAS の一例として、すべてのネットワーク機器を対象としている 3GPP TS 33.117[66]に挙げられているセキュリティ要件を表 5-43 に示す。

表 5-43　TS33.117 におけるセキュリティ要件

大分類	小分類	要件
セキュリティ評価	技術ベースライン	データと情報の保護
		可用性と完全性の保護
		認証と認可のポリシー策定
		セッションの保護
		セキュリティイベントのロギング実装
	OS	汎用 OS 要件
		UNIX 系 OS 特化の要件
	Web サーバー	HTTPS の使用
		Web サーバーのロギング実装
		HTTP ユーザーセッションの保護
		HTTP 入力の検証
	ネットワーク機器	データと情報の保護
		可用性と完全性の保護
堅牢性評価	技術ベースライン	不要もしくは安全でないサービス/プロトコルの無効化
		サービスに対するアクセス制限
		使用しないソフトウェアの削除
		使用しない機能の削除
		未サポートのコンポーネントの削除
		リモートからの特権ユーザーとしてのログインの制限
		ファイルシステムのアクセス権の設定
	OS	汎用 OS 要件
	Web サーバー	Web サーバープロセスへの特権付与の禁止
		未使用の HTTP メソッドの無効化
		未使用のアドオンの無効化
		コンパイラ、インタプリタ、CGI（Common Gateway Interface）経由のシェル機能の削除
		CGI 及びその他スクリプトによるアップロード無効化
		SSI (Server Side Includes) によるシステムコマンド実行の無効化
		Web サーバー設定のアクセス権の設定
		デフォルトコンテンツの削除
		ディレクトリリスティングの無効化
		HTTP ヘッダへの Web サーバー情報の最小化
		エラーページの Web サーバー情報の削除
		不要なファイル種別の関連付けの削除
		ファイルアクセスの制限

[66] 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Catalogue of general security assurance requirements (Release 15)
http://www.3gpp.org/ftp//Specs/archive/33_series/33.117/33117-f20.zip

大分類	小分類	要件
		CGI 及びその他スクリプトの実行ディレクトリの制限
	ネットワーク機器	O&M と制御プレーンの通信の分離
脆弱性評価	ポートスキャン	ー
	脆弱性スキャン	ー
	ファジングテスト	ー

5.3.2.2 GSMA

GSMA (GSM Association) は、元々GSM 方式を採用していた携帯事業者やベンダー等、関連企業からなる業界団体として組織された。GSM における標準化や技術開発、普及を目的として 1995 年に設立され、現在ではモバイルエコシステムに携わる 350 社以上の企業と通信事業者 750 社以上から構成されている。

FASG (Fraud and Security Group)、IDS (Interoperability Data Specifications and Settlement Group)、NG (Networks Group)、SIM (SIM Working Group)、TSG (Terminal Steering Group)、IG (Internet Group)、WAS (Wholesale Agreements and Solutions Group) の七つの Working Group が設定されており、GSMA メンバーを事務局として通信事業者やネットワーク機器ベンダー等からの自由参加により議論を行われている。また、3GPP とも連携しながら標準化、オペレーター間における相互接続ルールの策定等を実施している。

GSMA においてもサイバーセキュリティに関する脅威は各オペレーターにとっても非常に重要な、対処すべき課題だと認識されており、関心が高い議題の一つである。実際、WG にてセキュリティに関する議論は実施されており、既にいくつかのホワイトペーパーが公開されている。

GSMA ではオペレーター間の呼処理に関する領域を対象としたセキュリティ基準を主要な議論対象としている。また、通信ネットワーク内におけるセキュリティに関しては各通信オペレーターが独自で取り組むべき課題というスタンスを取っているが、そのネットワーク内に設置される機器の認証に関しては FASG 主導にて NESAS (Network Equipment Security Assurance Scheme) と呼ぶスキームを定義している。

5.3.3 GSMA の NESAS の分析と方向性

5.3.3.1 NESAS 概要

NESAS は、3GPP SA3 及び GSMA FASG のサブグループである SECAG (SECurity Assurance Group) によって定義された自主的なネットワーク機器の認証スキームである[67]。通信業界における各ステークホルダーのニーズを満たすソリューション提供を目指すもので、ネットワーク機器ベンダーが自社の機器がセキュリティ要件を満たし、製品ライフサイクルプロセスに関する標準ガイドラインに従って開発されていることを証明するべく、製品開発及びライフサイクルプロセスを包括的なセキュリティ監査の対象とするためのスキームである。本スキームの全体概要は図 5-15 の通りである。

[67] GSM Association: Network Equipment Security Assurance Scheme Overview Version 0.3 https://www.gsma.com/aboutus/wp-content/uploads/2017/03/FS.13-NESAS-Overview-Pilot-Release_0.3.pdf

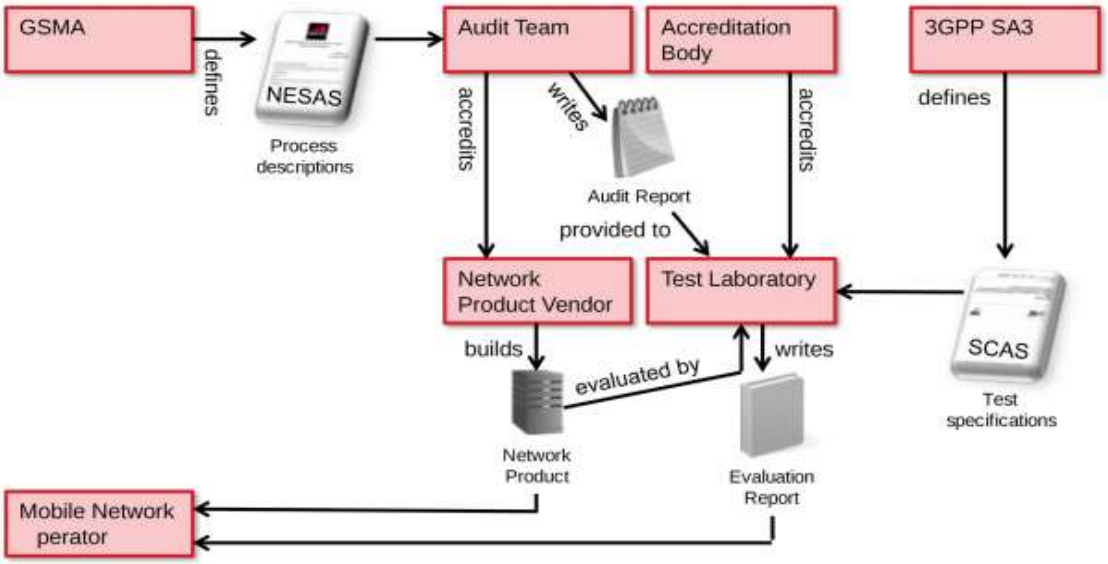


図 5-15　NESAS スキームの全体概要 [67]

このスキームの大まかな流れは以下の通りである。

(1) GSMA がネットワーク機器ベンダーの設計、開発、実装、及び製品保守のプロセスを監査するチーム（監査チーム）を任命

(2) 監査チームはネットワーク機器ベンダーのプロセスを監査し監査レポートを作成

(3) ネットワーク機器ベンダーはネットワーク製品を製造し、ISO 17025 認定を受けているテストラボに評価を依頼

(4) テストラボにて、当該ネットワーク機器に関連する 3GPP SCAS に基づいた評価を実施

(5) テストラボにて監査チームからのプロセス監査レポートとともに試験結果をまとめた評価レポートを作成

(6) ネットワーク機器ベンダーはネットワーク機器とともにその評価レポートを顧客である通信オペレーターに出荷

次にベンダーに対する認定プロセスの詳細を示す。

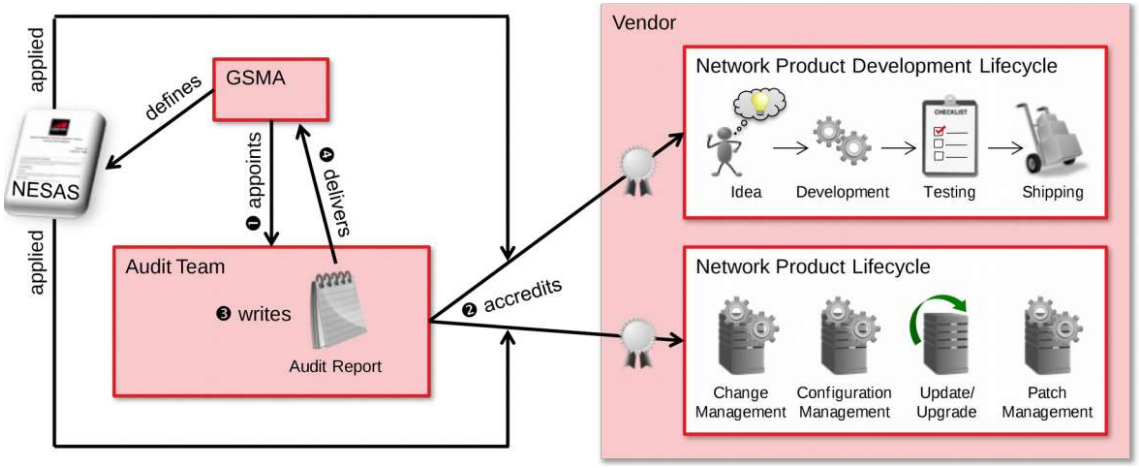


図 5-16　NESAS におけるベンダー認定プロセス [67]

図 5-16 の②において NESAS にて規定している、ベンダー認定に必要となる要件は表 5-44 の通りである。認定の対象となるネットワーク機器が、製品ライフサイクルのどのステージに位置しているかにより、個々の要件の適用要否が異なる（表 5-45）。

表 5-44　ベンダー認定に必要な要件

フェーズ	要件	内容
設計	セキュリティバイデザイン	製品に対する脅威分析プロセスを実施し、潜在的な脅威とその軽減策を特定することにより、セキュリティバイデザインを実現すること。
実装	バージョン管理システム	製品の商用ライフサイクルを通じて、ベンダーはソースコードのコミットの完全性を保証するバージョン管理システムを利用すること。
	変更の追跡	ネットワーク機器のすべての要件と設計変更を確実に実施するための文書化された手順を用意すること。
	ソースコードレビュー	適切なコーディング規約に準拠するようコードレビューを実施すること。可能ならばソースコード解析ツールも用いること。
	ソフトウェアセキュリティテスト	脆弱性や危険な、想定外の動作に起因した問題が存在しないことをセキュリティテストにより確認すること。
	従業員教育	ネットワーク機器の設計、開発、実装、保守に携わる従業員に対して、セキュリティに関する知識や気づきを持ち続けられるよう継続した教育を行うこと。
保守	脆弱性改善プロセス	リリースされたネットワーク製品の脆弱性に対処するためのプロセスの確立をすること。即ち脆弱性を適切に対処し、合意されたスケジュール内にパッチ/ソフトウェアのアップグレードをオペレーターに配布すること。
	脆弱性改善の独立性	ネットワーク製品のソフトウェアについて、機能変更を目的としたアップグレードと、セキュリティの脆弱性解消を目的としたアップグレードとで、分離可能な提供手段を用意とすること。

フェーズ	要件	内容
	情報セキュリティ管理システム	製品ライフサイクル全体を通して、機微情報の漏洩を防ぐ情報セキュリティ管理システムを採用すること。
	自動化ビルドツール	ソースコードのコンパイルには自動ビルドツールを利用し、そのログを保存すること。
	ビルド環境管理	ビルド環境のすべてのデータ（ソースコード、ビルドスクリプト、コンパイルツール、及びコンパイル環境を含む）は、バージョン管理システムから直接取得可能にすること。
	脆弱性情報管理	使用しているサードパーティ製コンポーネントに発見された脆弱性を認識し、ネットワーク製品の運用への影響有無を評価するプロセスを確立すること。
	ソフトウェアの一貫性保持	ネットワーク製品の配送時に改竄がないよう、管理方法を確立し維持すること。ソフトウェアパッケージの真正性を判断するための手段をオペレーターに提供すること。
	ユニークなソフトウェアリリース識別子	リリースするソフトウェアパッケージのバージョンには、一意に区別が可能な識別子を付与すること。
	セキュリティ問題修正に伴う情報伝達	セキュリティ関連の修正に関する情報は、ソフトウェアのリリースの際にオペレーターに伝達すること。
	ドキュメントの正確性	ネットワーク製品またはそのソフトウェアのリリースの際には、セキュリティの観点も含め、ネットワーク製品のすべての機能をオペレーター向け提出資料に反映すること。
	セキュリティ担当者へのコンタクト	セキュリティに関するオペレーターからの質問や問題報告のための窓口を用意すること。

表 5-45　NESAS のベンダー認定要件と製品ライフサイクルとのマッピング

	開発フェーズ（上位）			開発フェーズ(下位)							商用フェーズ			
	開発中	保守	終焉	計画	設計	実装	評価	リリース	製造	配送	初回商用	マイナーリリース	メジャーリリース	EOL
セキュリティバイデザイン	✓				✓						✓	✓	✓	
バージョン管理システム	✓	✓				✓					✓	✓	✓	
変更の追跡	✓	✓		✓	✓	✓					✓	✓	✓	
ソースコードレビュー	✓	✓				✓					✓	✓	✓	
ソフトウェアセキュリティテスト	✓	✓					✓				✓	✓	✓	
従業員教育	✓	✓												
脆弱性改善プロセス	✓	✓								✓				
脆弱性改善の独立性	✓	✓					✓					✓	✓	
情報セキュリティ管理システム	✓	✓												
自動化ビルドツール	✓	✓						✓			✓	✓	✓	
ビルド環境管理	✓	✓						✓						
脆弱性情報管理	✓	✓												
ソフトウェアの一貫性保持	✓	✓						✓	✓	✓	✓	✓	✓	
ユニークなソフトウェアリリース識別子	✓	✓						✓		✓	✓	✓	✓	
セキュリティ問題修正に伴う情報伝達	✓	✓										✓		
ドキュメントの正確性	✓	✓												
セキュリティ担当者へのコンタクト	✓	✓												

認定を受けるベンダーは、予め監査開始前に監査対象となるネットワーク製品に対し、「要件を満たしていることを監査チームに証明するのに十分であると判断した」証拠を記述したドキュメントを提示する。実際の監査時には要件の適用状況の論理的証拠を含む自己評価レポートを監査チームに提供する。

監査チームはこの自己評価レポートをレビューし、ベンダーから提供された根拠が、該当製品の開発に対して要件を適用した、という十分な証拠を提供しているかどうかを評価する。その後、当該ネットワーク製品が各要件の充足について十分な証拠があると考えられる事由の詳細を監査報告書に記し、NESAS 認定委員会に提出する。

なお NESAS では、監査のために提出する論理的証拠の作成がベンダーにとって不必要な負担になることは望ましくないと考えられており、一般的に採用されている業界慣行以上の余計な努力や、要求を満たすのに十分な既存のプロセスに対する大幅な変更は必要ない、とされている。

また監査チームが、要件の性質上、十分に満たされていることの証拠を作成、または評価

することが困難であると判断した場合、ベンダーに別に証拠を提出させるか、テストラボでの評価にて要件の検証を行う必要がある。その場合、監査チームはその問題についての詳細情報と推奨事項を併せて NESAS 認定委員会に通知する。NESAS 認定委員会は、類似問題の再発を避けるために、NESAS 規格の要件を修正するものとする。

5.3.3.2 NESAS の現状

2019 年 2 月現在、NESAS の規定文書の整備は完了しており、SECAG 内にてパイロット運用が進められている。このパイロットでは NESAS で定義している全プロセスを試験的に運用しており、実運用に耐えうるスキームとなっているかの検証と見直しを実施している。

このパイロットにてネットワーク機器ベンダーの監査を行う監査チームとして、ATSEC（独、瑞）、NCC Group（英）の 2 社が GSMA にて選定されており、実運用の際には機器ベンダーはこの 2 社のいずれかを選択して監査を受けることとなる見通し。

公式のリリースは 2019 年 5 月開催予定の GSMA Mobile 360 イベントにて実施される見通しとなっている。

5.3.3.3 NESAS の課題と方向性

現状では各オペレーターにて独自の機器調達スキームを構築・運用しているが、統一基準となることによりネットワーク機器ベンダーは異なるオペレーターに対する納入であっても納入基準を共通化できるため、設計、開発、実装、及び製品保守でのオペレーター固有の対応コストの削減が期待できる。一方、ネットワークオペレーターは NESAS スキームにより機器そのものに対するセキュリティ機能の実装の観点のみならず、機器の設計、開発といったオペレーターに見えづらいプロセスにおいてもセキュリティ基準が一定に担保されたネットワーク機器の納入を要求できる。DT は 2019 年より NESAS スキームをネットワーク機器の調達要件として RFQ に含める方向で検討している。

今後の商用移行においては、いかに多くのベンダーやオペレーターが参加し、NESAS 認証を調達条件として位置付けるかと、認証機関としての中立性をどうやって担保するかがポイントとなる。

5.4　ベンダーのセキュリティ対策に関する調査

5.4.1　調査目的

IoT ネットワークの構築に向けては、そのネットワークエッジやクラウドを構成する機器を提供するベンダーの存在が必要である。IoT 機器とクラウド等の一連の通信は、各ベンダーが提供する基地局からゲートウェイ、ルータ等様々な機器にて実現される。

本調査では IoT ネットワーク向け機器ベンダーのセキュリティ対策に対する取り組みについて現状を把握する。

今回の調査にあたり、5G のネットワーク機器ベンダーとしてマーケットシェアが高い(図 5-17）3 ベンダー、及び汎用ネットワーク機器ベンダーとしてマーケットシェアが高い（図 5-18）1 ベンダーを調査対象とした（表 5-46)。

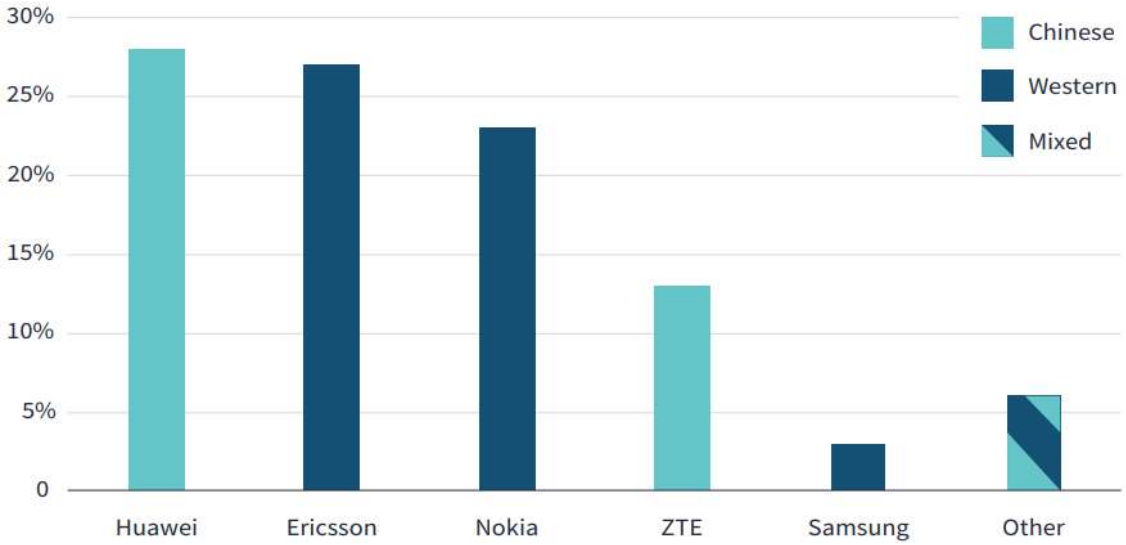


図 5-17　5G ネットワーク機器の企業別世界シェア（2017)[68]

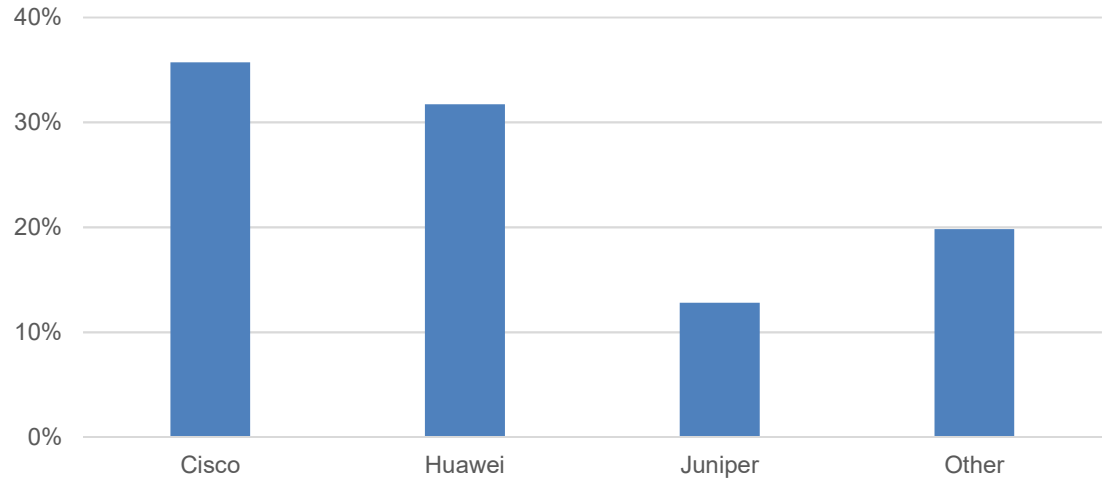


図 5-18　エンタープライズルータの企業別世界シェア（2018/2Q)[69]

[68] CSIS: How 5G Will Shape Innovation and Security
https://csis-prod.s3.amazonaws.com/s3fs-public/publication/181206_Lewis_5GPrimer_WEB.pdf
[69] 以下を基に NEC が作成
Business Wire: IDC's Worldwide Quarterly Ethernet Switch Tracker Shows Solid Growth in Q2 2018 While Router Market Sees Mixed Results

表 5-46　本調査の対象としたベンダー

ベンダー	概要
Ericsson	スウェーデンのストックホルムに本社を置く、通信機器ベンダー。
Nokia	フィンランド・エスポーに本社を置く、通信インフラ施設・無線技術を中心とする開発ベンダー。
Huawei	中華人民共和国深圳市に本社を置く通信機器ベンダー。
Cisco	米国カリフォルニア州サンノゼに本社を置く、世界最大のコンピュータネットワーク機器開発ベンダー。

各社におけるネットワーク機器に対するセキュリティ対策の実状を把握するため、表 5-47 の内容についてデスクトップ調査及びヒアリング調査を実施した。

表 5-47　ネットワーク機器ベンダーに関する調査内容

プロセス	分類	調査事項
セキュリティマネジメント	各国セキュリティガイドライン対応状況	（例えば NIST SP800-171/53 等の）セキュリティガイドラインへの対応状況の実状及び今後の対応計画
部品調達	サプライチェーン対策の実施状況	調達物の受入検査でのセキュリティ観点の試験内容
		開発拠点・調達先・製造拠点について
		開発拠点・調達先・製造拠点の見直しに対する検討状況
製造（組立）	組立、物流時の対策	組立、物流時のセキュリティ対策
検査	GSMA の評価機関の利用状況	NESAS ガイドラインの利用状況、及び未利用ならば利用しない理由
	外部セキュリティ検査	外部機関でのセキュリティ検査の受審有無
	リサーチセンター	HCSEC で実施されている内容、監査内容

※■:全社調査対象 ■:Ericsson、Nokia のみ調査対象 ■:Huawei のみ調査対象

5.4.2　ベンダーのセキュリティ対策の取り組み

5.4.2.1 Ericsson

5.4.2.1.1 サイバーセキュリティに関する基本的な考え方

以下はホワイトペーパー[70]として公開されている Ericsson の 5G セキュリティに対する考え方をまとめたものである。

IoT ネットワークに接続されるデバイスやモバイルアプリケーションにはレジリエンスで、安全、個人のプライバシーを保護できるワイヤレスネットワークアクセスが必要である。

Ericsson の長年にわたるコネクテッドソサエティのビジョンは、モバイルシステムがモ

https://www.businesswire.com/news/home/20180906005826/en/

[70] Ericsson: 5G security - enabling a trustworthy 5G system -
https://www.ericsson.com/en/white-papers/5g-security---enabling-a-trustworthy-5g-system

ノのインターネット（IoT）と急速に拡大するデジタルサービスの両方のバックボーンとして機能することで、近年現実のものとなってきた。そして 5G システムは、モバイルシステムの重要な役割を今よりさらに明確にする多くの新しいユースケースを可能とする。

5G に含まれている最先端の暗号化に加え、5G システムの信頼性は図 5-19 に示す五つの特性、即ちレジリエンス、通信セキュリティ、アイデンティティ管理、プライバシーそしてセキュリティ保証の結果である。

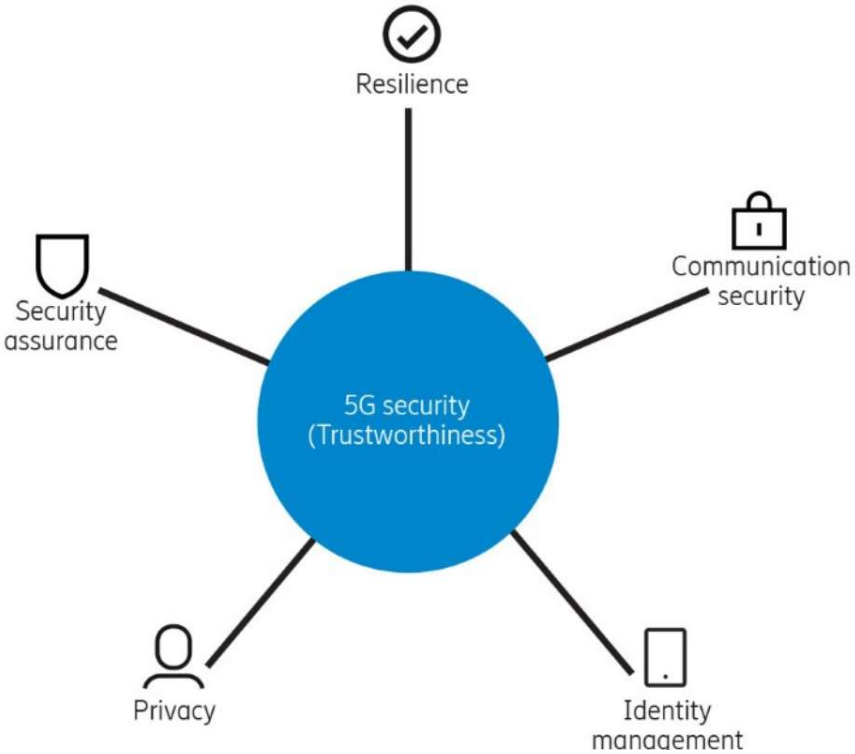


図 5-19　5G システムの信頼性に寄与する五つの要素 [70]

a.　レジリエンス

サイバー攻撃や悪意のない事故に対する 5G システムのレジリエンスは、補完的かつ部分的に重複する様々な機能によってもたらされる。

5G の無線基地局においては、CU（Central Unit）と DU（Distributed Unit）と呼ばれる二つの装置に分割して配置することにより、事故や攻撃に対する更なるレジリエンスをえることができるようになっている。

5G のコアネットワークのアーキテクチャもまたレジリエンスの概念に基づいて設計されている。例えばネットワークスライシングは、ネットワーク機能のグループを他の機能から分離する。これはつまり、パブリックセーフティに関わる通信を完全に独立したモバイルネットワークとして使用できることを意味する。

b.　通信セキュリティ

5G システムは通信デバイスと、システム自身のインフラストラクチャのために安全な通信を提供する。後者は、基地局の CU と DU との間のフロントホール、アクセスノードとコアネットワークとの間のバックホール、及びコアネットワークノード間のネットワークドメインリンク等を含む。セキュリティ設計は 4G システムで使用されているものと同様の

原則に従いながらも、新しいユースケースのニーズを一層満たすように進化している。
また、5G システムの端末は、特定目的向けのキーの分離、ハンドオーバ時のキーのバックワード・フォワードセキュリティ、アイドル状態のモビリティ、安全なアルゴリズムネゴシエーション等、4G システムのセキュリティ機能も継承している。

c. アイデンティティ管理

5G システムは加入者を識別及び認証するための安全な ID 管理機能があり、本当の加入者だけがネットワークサービスにアクセスできることを保証する仕組みを有している。通信オペレーターは 5G AKA（5G Authentication and Key Agreement）プロトコル及び EAP（Extensible Authentication Protocol）フレームワークから認証方法が選択可能である。

d. プライバシー

近年、加入者の識別や追跡、さらには 2G 通話の盗聴にも使用可能な、いわゆる IMSI キャッチャーや偽基地局について多くの事例が言及されている。GDPR（General Data Protection Regulation）やヨーロッパで進行中の ePrivacy Directive 等、懸念の高まりとプライバシーに関する法律に対応するため、加入者のプライバシーに関して予め設計にて含まれた 5G システムにてプライバシーの問題に対処することが最優先事項となっている。
5G システムはまた、IMSI または TMSI キャッチャーの根本原因である偽基地局を検出することができる。

e. セキュリティ保証

電気通信業界では、安全な標準化システムとプロトコルに加えて、安全な実装を保証する必要性が認識されていた。そのため、3GPP と GSMA は NESAS（network equipment security assurance scheme）と呼ばれる通信機器のライフサイクルに最適化されたセキュリティ保証スキームを作成するためのイニシアチブをとった。

5.4.2.1.2 サイバーセキュリティに関する体制

サイバーセキュリティに関わる社員は全世界で 700 人ほどいる。
社内的な脆弱性への対応には、PSIRT（Product Security Incident Response Team）と呼ばれる組織があり、フィンランドを主な拠点として 2004 年から稼働している。社内だけではなく、世の中にどのようなセキュリティの問題があるのか、他の関連する企業や団体と連携しながら運営しており、Ericsson の製品やサービスにてセキュリティインシデントが起こった際に対応している。
また、Ericsson 内部には CSO（Chief Security Officer）やサイバーセキュリティの部隊は配置されているが、組織図として公開しているものはない。

5.4.2.1.3 サイバーセキュリティに関する具体的な検証内容

Ericsson としてはサイバーセキュリティに伴う公開情報として、ソースコード等の開示を行っている。製品のセキュリティ対策としては、開発過程が重要だと考えており、ペネトレーションテスト、マニュアルハッキング、ファジング等を行う自動化ツールを用いて試験

を行っている。
また、国際的なセキュリティ標準である ISO/IEC27001,27002、NIST SP800-171/53 等多数の認証取得も行っている。

5.4.2.2 Nokia

5.4.2.2.1 サイバーセキュリティに関する基本的な考え方

Nokia は、通信ネットワークの中に脆弱性を見つける厄介者（bad actors）に対して、多くの攻撃機会を与えてしまっている現状があると認識している。その背景として、旧来は独自プロトコルをベースとした独立して構築していた通信ネットワークが、現在では標準化されたプロトコルを用いてインターネットとつながるネットワークへと全面移行しているため、善悪の意思に関わらず接続容易性が実現されたことが挙げられる。またネットワーク構築や保守の自動化、仮想化の発展によって開発や展開にかかる時間的なサイクルが短縮化したという環境の変化によるものもセキュリティリスクの一因となっているとの考えである。
Nokia は長年、ミッションクリティカルなネットワーク向け機器を製造してきているベンダーだが、それでも急速に進化する技術環境の中で強固な製品セキュリティを担保することは容易なことではない。この課題に対し、製造プロセスのコントロールだけでは対策として不十分であり、また機器が必須の技術要件を満たしているというだけでもやはり不足であると認識している。
したがって、セキュリティ開発プロセスと一連のセキュリティ技術要件を準備することに加え、さらに実装レベルでフォローアップし、測定し、監視することが必須である。そしてそれは組織の上下を問わず、厳格なセキュリティポリシーとその運用を維持するために社員誰もがコミットしなければならない、との考えを持っている。
来る 5G 時代においては通信ネットワークの複雑化により、例えば NFV MANO（Network Function Virtualization Management and Orchestration）を用いたネットワーク運用の仮想化、自動化が一層進むことが想定される。ノードであるネットワーク機器が MANO からの遠隔制御を受け付けるということは、同時に通信ネットワークに対する侵入リスクも高まることを意味する。そのため、セキュリティ対策はより一層重要になってくるものと認識している。
また Nokia では、2017 年から全社の取組としてすべての事業・すべての製品に対してセキュリティとプライバシーの領域での要求項目を設定すべく計画を進めている。社内では、両領域で業界リーダとして認知されるという目標「2020 ターゲット」を掲げている。
これまで Nokia では通信設備について通信事業者向けのみ手掛けてきたが、2018 年からエンタープライズ向け、とくにクリティカルユース向けのソリューション事業を強化している。このソリューションでは、機器の設置から運用まで参画していることから、通信事業者向けと同様にセキュリティ対策は重視している。
NIST 対応では、Nokia は米国が定めるセキュリティ要件仕様 FIPS（Federal Information Processing Standard）140-2[71]に準拠したセキュリティポリシーを設定し、それを満たす暗号化ソフトウェアモジュールである Nokia Cryptographic Module を提供している。
また、セキュリティ情報関連のイベントモニタリングのため、セキュリティオペレーションセンター（SOC）を設置・運用し、Nokia のシステムを使う顧客に対してアクセスコントロールや認証、暗号化等を行っている。

[71] Nokia: Nokia Cryptographic Module FIPS 140-2 Security Policy
https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2024.pdf

サプライチェーンの面でのセキュリティ対策としては工程毎に以下のようになっている。

a. 調達品でのセキュリティ対策

自社で Supply chain security program を運用している[72]。

b. 製造(組立)時のセキュリティ対策

セキュリティ要件のカタログを作成済であり、自社のセキュリティ基準に基づき、社内外のツールを使ってテストを実施している。

c. 物流のセキュリティ対策

Nokia のグローバル配送センターにおいて、ISO27001 準拠のための外部監査・内部監査を行っている [72]。

さらに、Nokia はネットワークへの侵入を防ぎ管理するため、「探索・分析」「封じ込め・根絶・回復」「事後対応」について、セキュリティ関連事象のタイプや程度に応じて、「Incident Response Teams (IRTs)」、「Major Event Team (MET)」、「Crisis Management Team (CMT)」の 3 種類のチーム組織で対応している。各チームは毎年トレーニングを実施し、その中では外部からの攻撃に対するシミュレーション訓練も実施している。

なお、2018 年末に、世界のセキュリティ関連のトレンドをまとめたホワイトペーパー「Nokia Threat Intelligence Report 2019」を公開した。これは 2012 年から経年にわたって作成・公開してきたものの最新版となっている。

5.4.2.2.2 サイバーセキュリティに関する体制

Nokia は DFSEC (Design for Security) と呼ばれる、製品の設計段階から評価に至る一連のプロセスに対するセキュリティスキームを採用している。DFSEC のアプローチは図 5-20 となる。

[72] Nokia: People & Planet Report 2017
https://www.nokia.com/sites/default/files/nokia_people_and_planet_report_2017.pdf 内 p.107

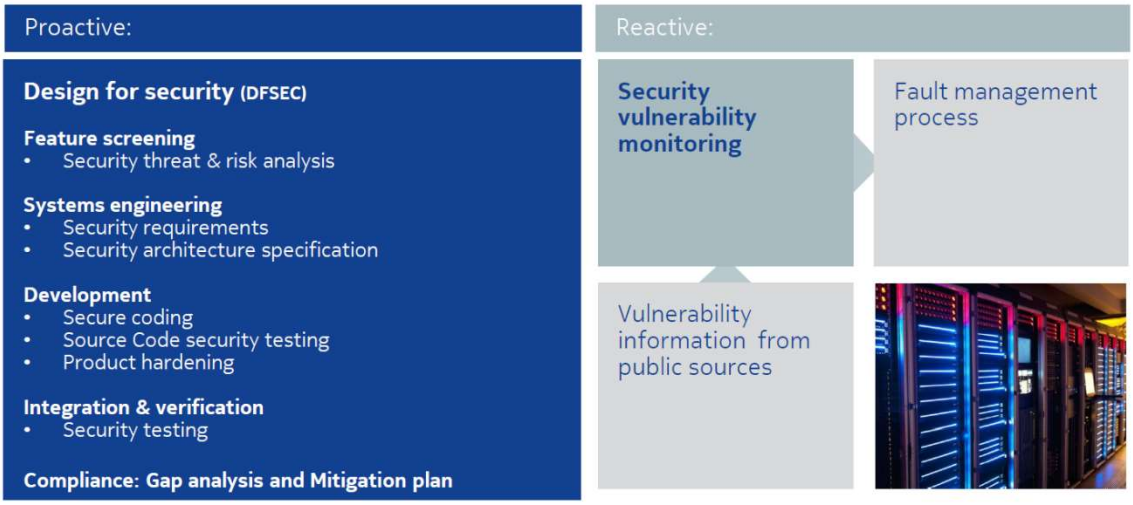


図 5-20　DFSEC のアプローチ[73]

プロアクティブなアプローチとして、製品が自社の事業グループで組み立てられる前にセキュリティやプライバシーが確実に担保されるよう、自社の DFSEC 規格に則ったツールやプロセスが用いられている。

Nokia が必須と位置付けているセキュリティ要件のカタログは、様々な情報インプットが元になって作られている。あらゆる製品開発においてそのカタログを使うことを必須としているが、その要件については優先度と重大性の観点からグループ分けされている。このカタログの運用は Nokia の DFSEC プロセスの中核をなし、3GPP のような業界フォーラム、顧客、規制当局といった外部との関わりから入手できる情報も取り込んでいる。

5.4.2.2.3 サイバーセキュリティに関する具体的な検証内容

Nokia では、開発のできるだけ早い段階でコードにある潜在的なセキュリティ問題について開発者へ自動的にフィードバックを提供することを目指し、ネットワークの脆弱性スキャンや様々なアプリケーションセキュリティテストを自動化することで定期的かつ一貫性を持って検証が行われている。研究開発チームとセキュリティマネジメントチームが必要な時に迅速に介入できるようトレーサビリティを持った初期段階でのインジケーターと、より包括的な製品テストが行われる。製品がコンプライアンスを満たしていない場合、Nokia のセキュリティ管理部門は製品に対して拒否権を発動することができる。

また Nokia は製品に対してセキュリティベースラインを設定し、セキュリティ、プライバシー、相互運用性に対するロードマップを定義する目的で製品の評価を行っている。

評価には様々な社内ツール、市販ツールを使って実施している。開発サイクルを通じた完全性を担保するため、静的・動的なコード分析や強力な暗号化を可能な限り活用している。

一方でこのように厳格な評価にて作り上げたソフトウェアであっても、あとから欠陥が発見される可能性を排除できないことから、Nokia は自社製品に搭載しているソフトウェア(自社製でもサードパーティ製でも)にセキュリティ面で脆弱性が生じる可能性について、公開・非公開の情報ソースを継続的にモニターしている。

脆弱性は各製品の状況に応じた規模でグレード付けされ、自社の研究開発チームがこうした問題を解決するために様々な対策を講じている。コンプライアンスを一元的に監視しながら、DFSEC の原則を順守する責任があるすべての研究開発チームに適用されるものと

[73] Nokia: With growing network performance requirements as 5G unfolds, how rigorous are your ground-up security processes?
https://www.nokia.com/blog/growing-network-performance-requirements-5g-unfolds-how-rigorous-are-your-ground-security-processes/

なっている。

5.4.2.3 Huawei

5.4.2.3.1 サイバーセキュリティに関する基本的な考え方

Huawei のサイバーセキュリティに関する基本的な考え方は、同社 CEO 任正非氏の声明の形で Web サイトに公表されている[74]。この声明によれば、同社にとってサイバーセキュリティは「最重要項目であり、自社の商業的利益をこれに優先させることは決してありません」と明記されている。

また、任正非氏は、関係する国や地域の法律、規制、規格の遵守に基づき、また業界のベストプラクティスを参照することにより、エンドツーエンドのサイバーセキュリティ保証システムを確立し、今後もこれを継続的に最適化していくことを宣言している。このサイバーセキュリティの保証システムは、全社方針、組織体制、ビジネスプロセス、技術、標準的業務の側面を包括するものであるとしており、Huawei は政府、顧客、パートナーと協力し、オープンで透明な姿勢でサイバーセキュリティの課題に積極的に取り組んでいく、としている。

5.4.2.3.2 サイバーセキュリティに関する体制

Huawei がサイバーセキュリティを確保するためのガバナンスは以下の図のようにまとめることができる（図 5-21）。

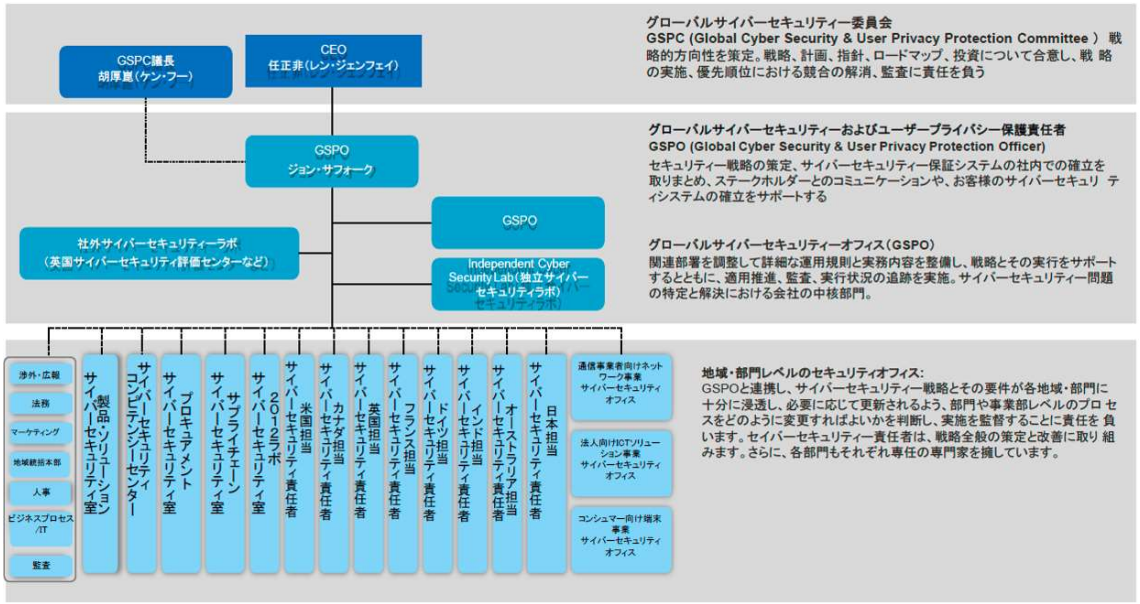


図 5-21　サイバーセキュリティに関するガバナンス体制[75]

グローバルサイバーセキュリティ委員会（以下、GSPC: Global Cyber Security & User Privacy Protection Committee）には CEO の任正非氏、GSPC 議長の胡厚崑氏がおり、サイバーセキュリティに関する戦略、計画、ロードマップといった包括的な戦略を策定し、そ

[74] Huawei: グローバルサイバーセキュリティ保証システムの確立についての声明
https://www.huawei.com/jp/about-huawei/declarations/cyber-security
[75] Huawei 提供資料をもとに ICR が作成

の実施や監査に責任を負うという。

その下にはグローバルサイバーセキュリティ及びユーザープライバシー責任者（以下、GSPO:Global Cyber Security & User Privacy Protection Officer）を設置している。GSPOの役割としては、セキュリティ戦略の策定やステークホルダーとのコミュニケーション、顧客のサイバーセキュリティシステムの確立の支援を行うことになる。また、グローバルサイバーセキュリティーオフィス（GSPO）が設置されており、関連部署の調整等、Huaweiにおけるサイバーセキュリティ問題の特定と解決における中核部門となっている。

さらにHuaweiが展開する地域等に設置されているセキュリティオフィスは、GSPOと連携しHuaweiのサイバーセキュリティ戦略の実施を監視すること等に責任を負っている。

5.4.2.3.3 サイバーセキュリティに関する具体的な検証内容

Huawei内のサイバーセキュリティ管理に関しては以下の通りである（図 5-22）。

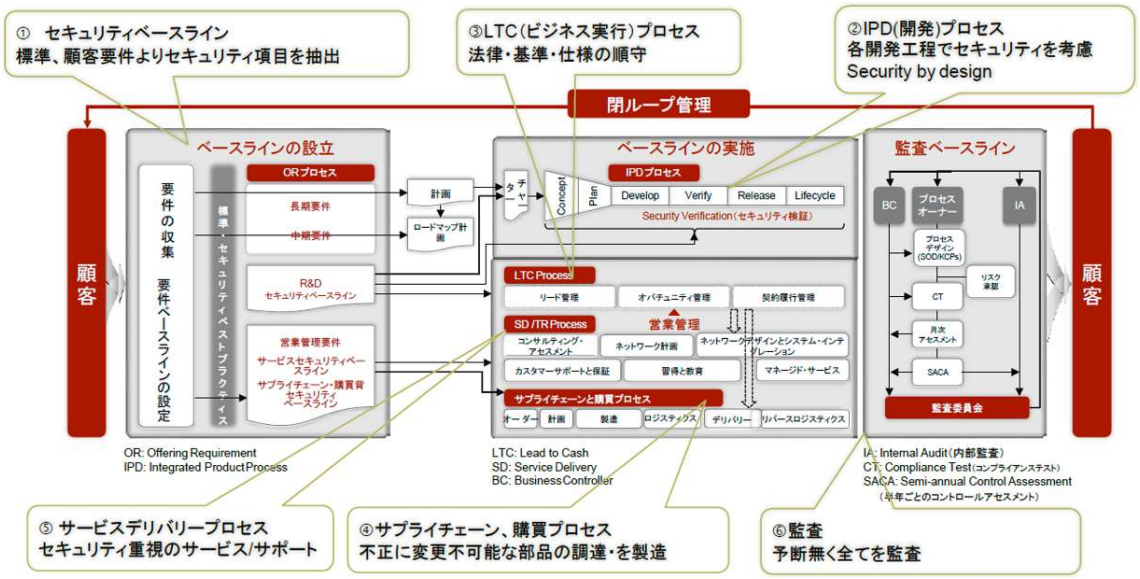


図 5-22　Huawei社内におけるサイバーセキュリティ管理[75]

図 5-22にあるようにセキュリティ管理のプロセスは以下の六つに分かれている。

(1) セキュリティベースライン：標準、顧客要件よりセキュリティ項目を抽出

(2) IPD（開発）プロセス：各開発工程でセキュリティを考慮（IPDについては後述）

(3) LTC（ビジネス実行）プロセス：法律・基準、仕様の順守

(4) サプライチェーン、購買プロセス：不正に変更不可能な部品調達

(5) サービスデリバリープロセス：セキュリティ重視のサービス/サポート

(6) 監査：予断なくすべてを監査

開発プロセスにおけるサイバーセキュリティ管理は図 5-23 に示すようなプロセスで実施されている。

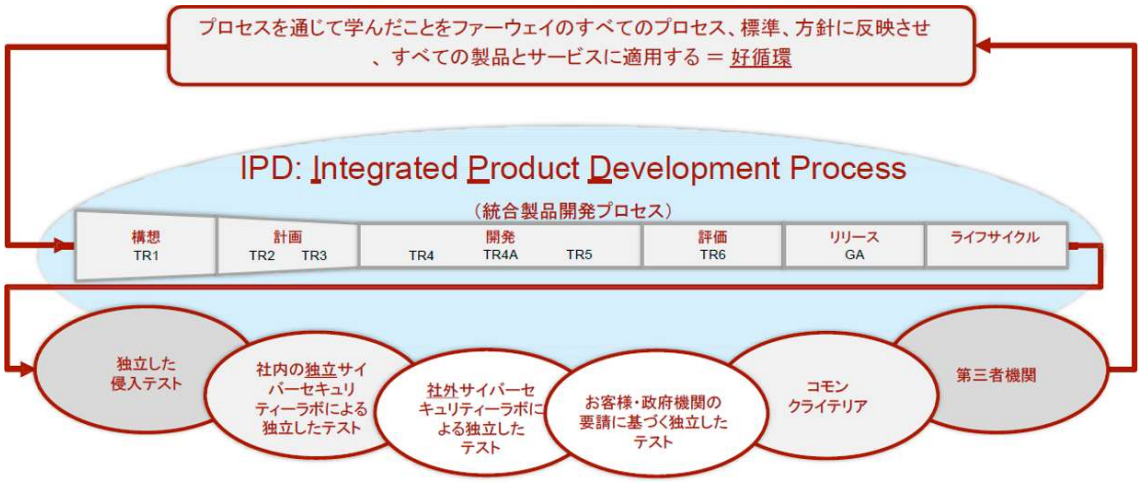


図 5-23　IPD（統合製品開発）プロセスにおけるサイバーセキュリティ管理 [75]

図 5-23 にて示す独立サイバーセキュリティラボや社外サイバーセキュリティラボについて、Huawei がどのような機関で検証を行っているかについて以下に説明する。同社が公開しているホワイトペーパー[76]によれば、Huawei は以下の三つの形態でサイバーセキュリティに関する評価を行っている。

a.　Huawei 社内の独立サイバーセキュリティラボ

製品開発ラインから独立した社内のサイバーセキュリティラボがすべての製品のセキュリティ評価を実施。セキュリティの自己評価には既存の脆弱性と基本的な製品セキュリティに対する審査等がある。

b.　Huawei 社外のサイバーセキュリティラボ

国・地域レベルでセキュリティ評価を実施する。この評価は、現地の政府や顧客から提案されたセキュリティ認証要件を満たすことを目的としている。現在、英国やカナダ、ドイツにある CSEC（サイバーセキュリティ評価センター: Cyber Security Evaluation Centre）がこのような評価を実施中である。

この評価では、商業的ツールや個人が設計したツールを使用してソースコードの品質とセキュリティを解析し、潜在的なコードの弱点を検出している。ソフトウェアについても、幅広いツールと技術を使用してハッキングへの耐性を検証し、最終的にセキュリティ設計の機能について追加の審査を実施する。

c.　第三者評価機関

第三者評価機関とも連携し、Huawei 製品について公平なセキュリティ評価を実施してもらうとともに、場合によっては認証も取得する。この評価は通常顧客及び第三機関の監査人によって実施され、コモンクライテリア（CC）セキュリティ認証モデルによる評価も含むものとなっている。また、Huawei は複数の製品で CC 認証を取得している。

顧客によっては、より安全な環境を整備する努力の一環として製品に独自の社内セキュリティ試験を実施する場合もあれば、北米や欧州の顧客のように第三者機関に依頼して製品を独立してテストする場合もある。

---

[76] サイバー・セキュリティに対するファーウェイの視点と取り組み
http://www.huawei.com/ilink/jp/download/HW_310660

また、Huawei は業界最先端のサイバーセキュリティに対応しており、その対応状況は図 5-24 のようにまとめることができる。実際に、サイバーセキュリティの問題に対応する体制である CERT (Computer Emergency Response Team) は図 5-25 のようになっている。

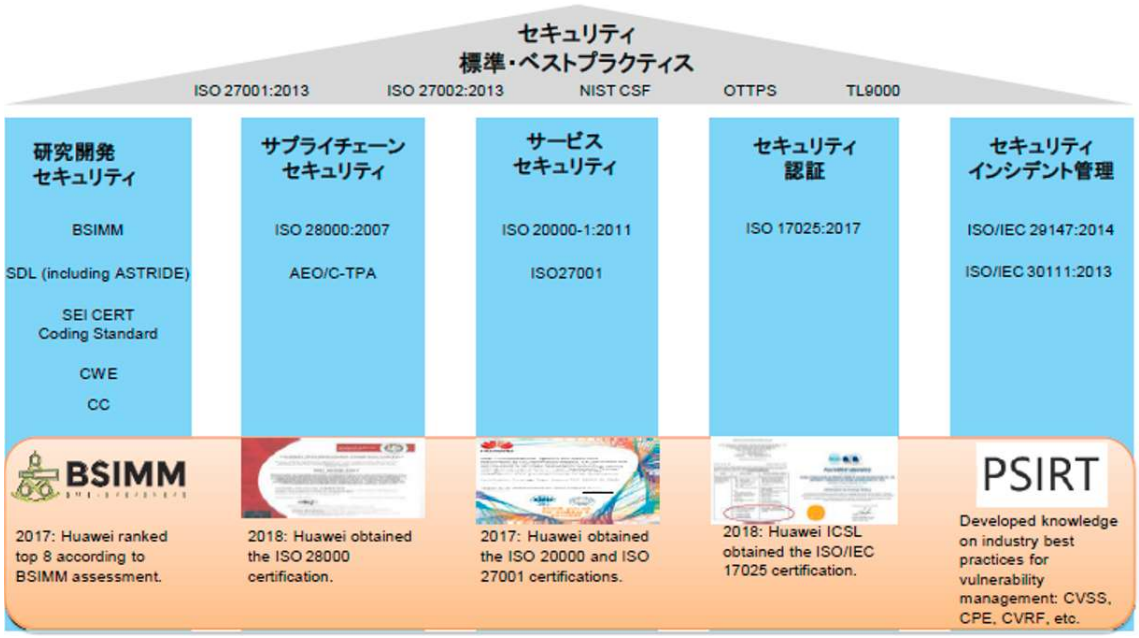


図 5-24　Huawei のサイバーセキュリティ標準への準拠状況 75

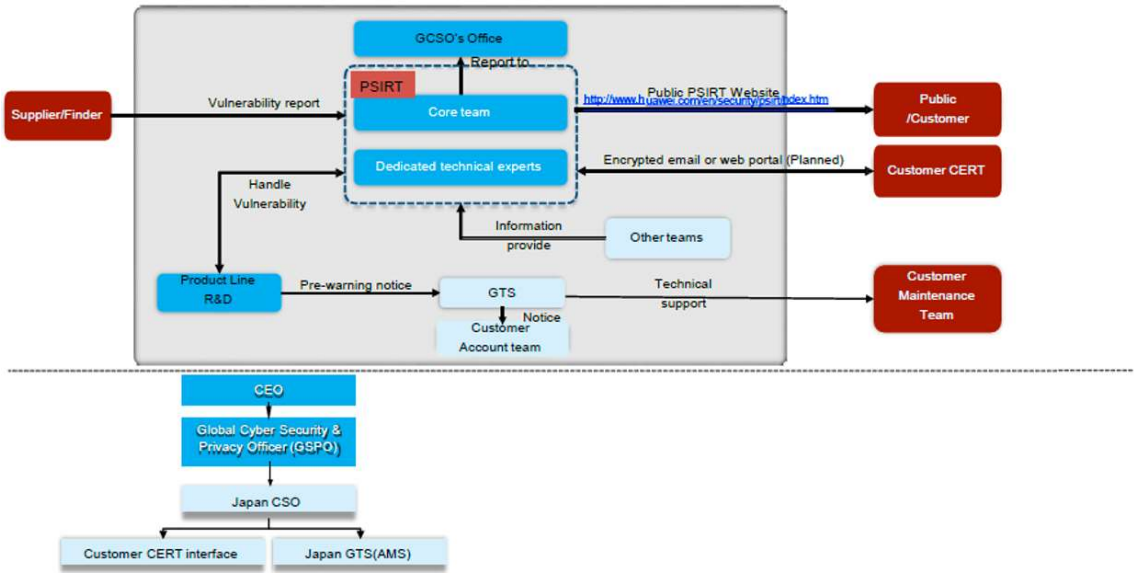


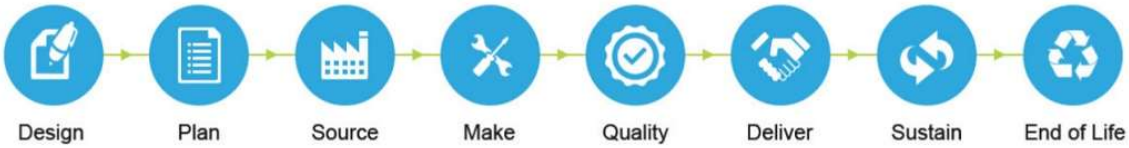
図 5-25　Huawei の CERT 体制 75

5.4.2.4 Cisco

5.4.2.4.1 サイバーセキュリティに関する基本的な考え方

Cisco は「Value Chain Security」と呼ばれるプログラムを実施している。Cisco へのサプライヤーのセキュリティ向上を目的に、ソリューションのライフサイクル全体を通じて、サプライヤーのセキュリティを継続的に評価、監視して、問題があれば改善する機能を設計

し、サプライヤーに対して展開している。ソリューションのライフサイクルである設計、計画、ソース（パートナー選定）、製造、品質、配送、保守、サポート終了の全工程を管理している（図 5-26）。なお、設計と製造においては、サードパーティソフトウェア、オープンソースソフトウェア、OEM 開発等のソフトウェアのセキュア開発に関するプログラムが定義されている。



出所（Value Chain Security | Cisco[77]）

図 5-26　Cisco のソリューションライフサイクル

管理しているリスクの分野は九つあり、プライバシーとデータセキュリティ、インフラセキュリティ、アプリケーションセキュリティ、ロギング・監査容易性、ID 管理、事業継続性・災害復旧、セキュリティ統制、インシデント管理、脆弱性管理である（図 5-27）。一般的な企業のセキュリティの管理策とは異なっており、Cisco に被害が発生しないような対策と、インシデントが発生した場合の Cisco からの管理の容易さと、Cisco の事業に与えるインパクトの最小化に力点が置かれていると推察できる。

図 5-27　管理対象のリスク分類[78]

Cisco では「Trust Anchor Technologies」とよばれる、自社製品に対して、信頼できるシステムで構築されたことを保証する基盤を提供している。 Trust Anchor とセキュアブートによる署名付きイメージの検証を実施することで、Cisco のハードウェアプラットフォームで、Cisco が許可を与えた正しいコードだけが実行されることを保証する。起動時にプラットフォーム上で実行されているすべてのレベルのソフトウェアを検証することで、システムに対する信頼関係を確立する。ブートコードの整合性の検証は、すべての Cisco のプラットフォームベースの「Cisco セキュア開発ライフサイクル」で義務付けられている。

Cisco Trust Anchor Technologies は、製品保証機能と基本的なセキュリティ機能を提供しており、不変のアイデンティティ、安全性の高いストレージ、ランダムビットジェネレータ、そして安全な鍵管理を提供する。

これを実現するトラストチェインについて説明する（図 5-28）。

---

77 https://www.cisco.com/c/en/us/about/trust-center/global-value-chain-security.html

78 Cisco: 3rd Party Cloud Service Provider Security https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-third-party-cloud-security-infographic.pdf

まずはデジタル署名による改ざん検知機能として、ソフトウェアコード等の特定のデータブロックに対して一意のデジタル署名を作成する。シグネチャはチェックサムと同様のハッシュアルゴリズムで作成され、ソフトウェアコードの「ハッシュ値」を計算する。 このハッシュ値は署名鍵を使用して暗号化される。 署名付きソフトウェアコードは実行開始時にチェックされ、署名された段階から変更されていないことを確認する。署名保護チェックが迂回するようなソフトウェアコードまたはシステムの変更を防ぐためにコード保護対策が不十分な場合は、発行した署名を無効にすることができる。

トラストチェインは、このデジタル署名の仕組みをハードウェア、マイクロローダ、BIOS ブートローダ、OS の署名へとつなげていきセキュアなブートプロセスを実現している。改ざん不可能なハードウェアで実装されている領域に信頼のルート（根源）が存在し、信頼の連鎖が開始される。下流のソフトウェアコードが起動される前に上流で、そのソフトウェアコードの検証が行われる。

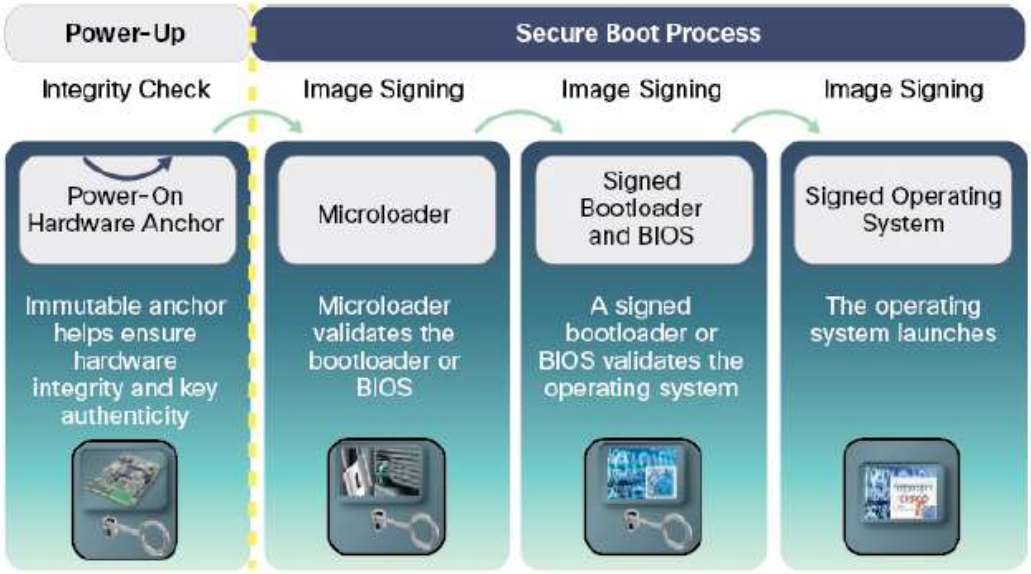


図 5-28　Cisco のトラストチェイン[79]

[79] Cisco: Cisco Trust Anchor Technology
https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/trust-anchor-technologies-ds-45-734230.pdf

5.5　OSS コミュニティのセキュリティ対策に関する調査

5.5.1　調査目的

OSS 開発コミュニティでのセキュリティは、個々のコミュニティ独自に何らかの対策が講じられていると考えられる。

本調査では社内 OSS コミュニティ活動参加者を通じて、OSS コミュニティ活動におけるセキュリティ対策プロセス・体制の実状のヒアリングを実施する。

調査の対象は次世代ネットワーク構築に不可欠な技術である SDN/NFV を実現するための手段を提供する OSS であり、かつ主要ベンダーが参加している表 5-48 の OSS コミュニティとした。

表 5-48　調査対象の OSS コミュニティ

OSS コミュニティ	概要
OpenStack	OpenStack はクラウド基盤を構築するための OSS プロジェクト。SDN 市場におけるデファクトスタンダード。サポート企業は 678 社に上る[80]（プラチナメンバー8 社、ゴールドメンバー19 社、インフラ提供 7 社、スポンサー企業 70 社、サポート 574 社）。
OPNFV	OPNFV（Open Platform for NFV）は The Linux Foundation のエコシステム傘下にて NFV を実現するソフトウェア環境の実現を目指す OSS プロジェクト。
ONOS	ONOS（Open Network Operating System）は SDN を実現するための通信事業者向け OS を開発する OSS プロジェクト。サポート企業は 67 社[81]（パートナー15 社、コラボレーター52 社）。

これらの OSS コミュニティについて、セキュリティ対策を実施するプロセス・体制の実態を把握するため、表 5-49 の内容についてヒアリング調査を実施した。

表 5-49　OSS コミュニティへの調査内容

プロセス	分類	ヒアリング事項
セキュリティマネジメント	開発者や所属組織の審査	開発コミュニティ参入時において開発者やその所属組織に対する審査の有無
		コミュニティの体制
		人の評価、信頼の判断基準
		セキュリティを脅かす不正動作を作成した開発者の評価
		不具合の件数や重大性に応じた開発者の処遇
	サポート企業の戦略	サポート企業がコミュニティに参加するモチベーション
	OSS コミュニティ自体の評価	OSS コミュニティ自体を客観的に評価する制度・期間の有無
開発	開発プロセス	採用している開発プロセス
		開発プロセスにおけるセキュリティチェック機能の運用状況

[80] OpenStack project: Companies Supporting The OpenStack Foundation
https://www.openstack.org/foundation/companies/

[81] the Linux Foundation: Organizations supporting the Open Network Operating System (ONOS®)
https://onosproject.org/members/

プロセス	分類	ヒアリング事項
		セキュリティチェックを実施する要員
		セキュリティチェック要員になるための素養
		セキュリティを脅かす不正動作の混入リスクに対する考え
		セキュリティチェック機能の今後の方向性
運用	ディストリビュータのセキュリティ観点の対策	セキュリティの観点でのチェック内容
		セキュリティを脅かす不正動作の修正作業の分担
		セキュリティを脅かす不正動作の修正基準の有無
	OSS ユーザー側の対策	OSS ユーザーが実施すべき対策

5.5.2 OSS コミュニティのセキュリティ対策の取り組み

以下の章では各 OSS コミュニティのヒアリング結果を記載する。

5.5.2.1 OpenStack

5.5.2.1.1 開発者や所属組織の審査

開発者のコミュニティ参加に対し、その素性の確認や所属組織に対する審査は行われていない。OSS コミュニティにとっては、開発者がいかにコミュニティの利益に貢献しているか（有益な機能を持つソースコードの投稿、質の高いレビューコメント等）がその開発者の評価に使用される観点となる。コミュニティは広く開放されており、提案されたソースコードのみで採用可否が判断される。開発者の評価はプロジェクト活動の貢献度や議論、開発スキル等から総合的に判断され、所属組織や役割はその判断に影響しない。

5.5.2.1.2 開発プロセス

OpenStack の開発体制においては、セキュリティ脆弱性の問題として報告された不具合について、その管理を行う VMT (Vulnerability Management Team) と呼ばれる専門のセキュリティチームが存在する。セキュリティ問題に関する情報の早期漏洩を防ぐため、VMT はごく限られたメンバーで構成されている（2019/2 現在 6 名）。またセキュリティ問題は通常の問題対応の経路とは異なり、VMT とコアレビューアの一部メンバーのみの管理下での開発プロセスにて対応がなされる。各々の問題には VMT コーディネーターがアサインされ、問題修正からステークホルダーへの情報開示に至るまでの一連のプロセスは厳密に管理されている。そのため、ゼロデイ攻撃のような既知の脆弱性を突いた攻撃に対する対策は十分行われていると言える。

開発者が意図した実装になっていない、いわゆるソフトウェアバグであるセキュリティ脆弱性が存在する一方で、OSS コミュニティに特定の思想を持った開発者が参画していた場合、意図的に不正動作を埋め込もうとする可能性がある。OpenStack コミュニティとしてはそのような作為的な不正動作に対して特定の排除プロセスが存在するわけではないが、仮にそのようなケースが生じたとしても、ソースコードのレビューや承認のプロセスでの相互監視の作用により、不正動作を混入させることは非常に困難となっている。

5.5.2.1.3 ディストリビュータのセキュリティ観点の対策

OpenStack パッケージのセキュリティ対策は OpenStack コミュニティにて対応することが原則であるため、Linux ディストリビューションが個別のセキュリティ対策を行うことは考えづらい。ただし、OpenStack サポートメンバーには redhat、SUSE、ubuntu といった著名な Linux ディストリビューションが名を連ねており、OpenStack コミュニティにて積極的にセキュリティ対応を行った上で自ディストリビューションのコンポーネントへの取り込みを行うケースもある。

5.5.2.1.4 サポート企業の戦略

サポート企業の自社製品への取り込みを前提として OpenStack コミュニティに参画するケースが多いと考えられる。また自社のプライベートクラウド基盤として利用している企業が、品質や安定性の向上のために参加しているケースもある。

5.5.2.1.5 ユーザー側の対策

OpenStack のユーザーはコミュニティが発行しているセキュリティ勧告（OSSA: OpenStack Security Advisories)、セキュリティノートを参照し、必要であれば主体的な対策を行う必要がある。

5.5.2.1.6 OSS コミュニティ自体の評価

OpenStack コミュニティの客観的評価としては、CII（The Core Infrastructure Initiative）より 2017 年 6 月にベストプラクティスを達成した認証を受けている。CII はオープンソースプロジェクトがセキュリティ、品質及び安定性のベストプラクティスに適合しているかを評価する Linux Foundation プロジェクトである。

5.5.2.2 OPNFV

5.5.2.2.1 開発者や所属組織の審査

開発者のコミュニティ参加に対し、その素性の確認や所属組織に対する審査は行われていない。コミュニティは広く開放されており、提案されたソースコードのみで採用可否が判断される。開発者の評価はプロジェクト活動の貢献度や議論、開発スキル等から総合的に判断され、所属組織や役割はその判断に影響しない。

5.5.2.2.2 開発プロセス

OPNFV の開発体制においては、開発プロジェクトとは独立したセキュリティプロジェクトが存在し、セキュリティガイドラインの策定とセキュリティスキャンの作成・実施 が行われている。セキュリティスキャンは提案されたコード毎に簡易実行されるものと定期的に時間をかけて実行されるものがあるが、検査項目は OpenSCAP（Open Security Content Automation Protocol）を用いた一般的なものに限られている。そのため、最終的にはソースコードの採否判断を行う各プロジェクトコミッタのチェックに頼っているのが実状であ

る。
セキュリティ脆弱性に関わる問題については、OPNFV コミュニティにて使用しているプロジェクト管理システムの当該脆弱性を含むプロジェクトポータルより、セキュリティレベルに”Embergo”を指定することで OSVM (OPNFV Security Vulnerability Management) プロセスにて管理される。“Embergo”に指定された問題はプロジェクトリーダー、リポーター、対応がアサインされているメンバー、セキュリティプロジェクトメンバー及び当該プロジェクトのグループメンバのみが参照可能となり、問題の特定に至るまでは非公開で対応が進められる。
また、OPNFV コミュニティでは意図的に不正動作を埋め込もうとするような開発者は存在する、という前提に立ったプロジェクト運用がなされている。企業や個人のコミュニティ参加時には貢献者ライセンス合意書（CLA: Contributor License Agreement）を交わすことで、悪意に対する心理的障壁を高めている。

5.5.2.2.3 ディストリビュータのセキュリティ観点の対策

OPNFV はディストリビュータモデルではないため割愛。

5.5.2.2.4 サポート企業の戦略

参加企業の共通的な期待としては NFV の市場活性化や導入加速であり、長期プロセスとなる標準化ではなく OSS によるデファクトスタンダード化を期待している。
オペレーターは自社システムでの活用で構築保守コストの削減を期待している。
システムインテグレーターやベンダー企業の活動の状況としては、相互接続性の向上による開発・試験コストの削減、自社製品に合ったアーキテクチャ・API へデファクトを誘導することで市場優位性確保、あるいは自社製品の売込み（コミュニティ版が未成熟なうちに同等製品を顧客に提案）等が挙げられる。
また、テレコム業界においてフットプリントが小さい、あるいは存在しなかった IT/クラウド/チップのベンダーが参入機会と見做している場合もある。

5.5.2.2.5 ユーザー側の対策

ユーザーの構築するシステム毎にリスク分析を行うとともに、コンポーネントのセキュリティ成熟度に応じた OSS コンポーネントの絞り込みや、代替品の採用等を検討が必要である。

5.5.2.2.6 OSS コミュニティ自体の評価

OPNFV コミュニティ内ではコンポーネント毎の成熟度を確認する制度は存在する。外部の評価機関は把握できていないが、OSS を使用する企業それぞれでコミュニティの評価を実施しているのが実態だと予想される。

5.5.2.3 ONOS

5.5.2.3.1 開発者や所属組織の審査

ONOS においても今回調査対象とした他の OSS コミュニティと同様、開発者のコミュニティ参加に対し、その素性の確認や所属組織に対する審査は行われていない。ソースコードによるコミュニティ貢献は勿論として、メーリングリストや Slack（チームコミュニケーションツール）等のチャネルでの設計議論、他のメンバーへの手助けの状況も開発者の評価に用いられる。

5.5.2.3.2 開発プロセス

マージまでのプロセスにおいては、人によるコードレビュー、静的検査ツールによるチェックが行われている。マージ後においては BlackDuck 社の検査の他、欧州のセキュリティ研究者が毎年研究の一環として評価している。

ONOS におけるセキュリティ脆弱性の不具合については、専用の報告用メーリングリストが用意されており、その報告を受けてセキュリティレスポンスチームによるハンドリングが行われる。セキュリティレスポンスチームは 8 名（2019 年 2 月現在）の TST（Technical Steering Team）と推薦された専門家（2019 年 2 月現在では 2 名の ONF（Open Networking Forum）メンバー）から構成され、解決方法が開示されるまでの間、セキュリティレスポンスチーム内のみの秘密情報として管理される。

また、ONOS コミュニティにおいても OPNFV と同様に企業や個人のコミュニティ参加時には貢献者ライセンス合意書（CLA: Contributor License Agreement）を交わすこととなっている。

5.5.2.3.3 ディストリビュータのセキュリティ観点の対策

コミュニティにおいてはセキュリティ検査を含むシステム試験を実施した上でリリースを行っているが、採用している OSS ライセンス（Apache2 License）上、セキュリティ評価を強要するようなことはできず、その後ディストリビュータとしての再試験等が実施されているかは不明である。

5.5.2.3.4 サポート企業の戦略

各企業でも思惑はざまざまであると考えられる。

ベンダー系企業は、オープン化の流れをサポートしているとのマーケティングメッセージを出す活動の一環と位置付けたり、主要なテレコム系の顧客からの要請に応える形で参加している様子も見られる。また ONOS を自社ソリューションに組み込んでおり必要な機能をアップストリームしやすくするために必要なコミュニティ環境とする意図もあるものと思われる。

CSP ビジネス観点で新興となる、ODM（Original Design Manufacuturing）ベンダーやシステムインテグレーターは、自社サービスメニューの拡充、顧客との PoC 及びマーケティング活動の場としての参加している。

また自社ビジョンにあった方向に向かうようコード寄付等を通じエコシステム形成し、当該ソフトやアーキテクチャをサポートする ODM ベンダーの拡大やドメイン知識を抑えたエンジニアのリクルートのしやすい状況を作り出すため参加している IT 企業もある。

5.5.2.3.5 ユーザー側の対策

ONOS に限った話ではないが、OSS の位置付け上あくまでベストエフォート提供となるため、自社の利用シナリオに沿った受入テストは、セキュリティレベル、品質レベルをコストと秤にかけ、自ら実施する必要がある。

5.5.2.3.6 OSS コミュニティ自体の評価

Bitergia よりプロジェクトの活動状況を可視化するダッシュボードを提供したいとの申し出があり ONF として協力しており、客観的指標の一つとして参照可能となっている。

5.6　キャリアのセキュリティ対策に関する調査

5.6.1　調査目的

IoT ネットワークはキャリアが提供するネットワークを使用して実現される。

キャリアは IoT 機器が使用するネットワークの構築、運用、保守を行うが、ネットワークの構築においては、各ネットワーク機器のベンダーから製品を調達して、ネットワーク構築を行う。IoT のセキュリティを考える場合に、IoT デバイスに対して安全なネットワークの提供が必要であり、ネットワークを提供するキャリアでは、調達するネットワーク機器に対してセキュリティ対策が行われているかの確認が必要である。

本調査ではキャリアのセキュリティ対策の取り組みについての現状を把握するために、実態調査を行う。調査の対象は各国での大手キャリアである以下のキャリアとした。

表 5-50　調査対象のキャリア

キャリア	概要
AT&T	AT&T Inc.（エイ ティ アンド ティ）は、米国の情報通信・メディアコングロマリット。 (https://www.att.com/)
DT	Deutsche Telekom（ドイツテレコム）は、ドイツ・ボンに本社を置く電気通信事業者。 (https://www.telekom.com/en)
Orange	Orange S.A.は、フランスの主要電気通信事業者の一つ。 (https://www.orange.com/en/home)
BT	BT グループ（英: BT Group plc）は、英国・ロンドンに本社を置く大手電気通信事業者。英国における最大手の固定電話事業者及びインターネットプロバイダーであり、世界でも最大規模の通信事業者の一つである。 (https://www.bt.com/)

これらのキャリアについて、セキュリティに対するプロセス・体制の実状を把握するため、以下の内容についてデスクトップ調査を実施した。

表 5-51　調査事項

カテゴリ	項目	調査事項
法令・ガイドライン対応	各国セキュリティガイドラインの対応状況	NIST SP800-171/53 といったセキュリティガイドラインの対応状況
		NIST SP800-171/53 といったセキュリティガイドラインへの対応計画
受入検査	受入検査でのセキュリティ検査	セキュリティの受入検査での対応方法
		受入検査の対応内容の変更計画
運用	運用時のセキュリティ対策	機器の不正動作（バックドア等）に備えた対策の実施
	評価機関によるセキュリティ検査	評価機関でのセキュリティ試験の実施状況
		評価機関を行う対象設備
		評価機関での試験内容

5.6.2 キャリアのセキュリティ対策の取り組み

以下の章では各キャリアでのデスクトップ調査及びヒアリング調査の結果を記載する。

5.6.2.1 AT&T

5.6.2.1.1 デスクトップ調査

a. 各国セキュリティガイドライン対応状況

調査を行ったが、セキュリティガイドラインに対しての対応や今後の対応予定といったことについての情報はない。

b. 受入検査でのセキュリティ検査

AT&T では受け入れる製品に対して脆弱性テストを実施している。脆弱性テストの実施では、アクセスが許可されている特定の担当者が、AT&T が開発したツールと最先端のスキャンツールを使用して、不正アクセスされてしまうような操作がないかを検証している[82]。

c. 運用時のセキュリティ対策

調査を行ったが、運用時におけるセキュリティ対策として IDS やパケットのキャプチャ等の対応を行っているかの情報はない。

d. 第三者試験でのセキュリティ検査

調査を行ったが、第三者試験によるセキュリティ試験を実施しているといった情報はない。

e. GSMA の評価機関

調査を行ったが、GSMA の評価機関のベンダーへの利用促進や、ベンダーからの調達条件に加えるといった情報はない。

[82] AT&T: Network Security
https://about.att.com/csr/home/issue-brief-builder/people/network-security.html

5.6.2.2 DT

5.6.2.2.1 デスクトップ調査

a. 各国セキュリティガイドライン対応状況

調査を行ったが、セキュリティガイドラインへの対応や、今後の対応予定といったことについての情報はない。

b. 受入検査でのセキュリティ検査

現状で実施しているかの情報はない。
ただし、国としては受入検査を変える動きがあり、機器導入の前に独立したラボで認定（検証）を提案している。また、ネットワーク機器ベンダーはソースを第三者機関に提供し、オペレーターが特定の状況下で脆弱性にアクセス可能としている。
法的責任を、オペレーターに加え、ネットワーク機器ベンダーにも課す（広げる）ことも検討されている。

c. 運用時のセキュリティ対策

調査を行ったが、運用時におけるセキュリティ対策として IDS やパケットのキャプチャ等の対応を行っている情報はない。

d. 第三者試験でのセキュリティ検査

第三者試験として BSI[83]が実施する検査があるが、DT が調達時の条件としているか情報なし。

e. GSMA の評価機関

調査を行ったが、GSMA の評価機関のベンダーへの利用促進や、ベンダーからの調達条件に加えるといった情報はない。

5.6.2.3 Orange

5.6.2.3.1 デスクトップ調査

a. 各国セキュリティガイドライン対応状況

調査を行ったが、セキュリティガイドラインへの対応や対応予定といった情報はない。

[83] BSI (Bundesamt für Sicherheit in der Informationstechnik) は、ドイツ連邦政府においてコンピュータと通信のセキュリティ担当部門

b. 受入検査でのセキュリティ検査

調査では、Orange での調達時の条件となっているかは不明だが、仏当局（ANSSI）ではベンダーの技術情報（ソースコード含む）の提示を要求しており、提供された情報から認証等を行っている。

c. 運用時のセキュリティ対策

調査を行ったが、該当する情報はない。

d. 第三者試験でのセキュリティ検査

ANSSI がベンダー、サプライヤーに対して、技術情報（ソースコードを含む）の提示を要求している。調達する製品のマザーボードや、部品配置、暗号化キー、ソースコードといった企業秘密の情報に該当するものを要求し、取得した情報から ANSSI が検査を実施している。

ANSSI は ITSEC 認証やコモンクライテリア認証の認証機関でもあり、ベンダーから提供された技術情報から認証を行う。認証された製品は、ANSSI で認証機器一覧として公開されている。認証に伴う試験、検査等の詳細な情報については情報なし。

e. GSMA の評価機関

調査を行ったが、該当する情報はない。

5.6.2.4 BT

5.6.2.4.1 デスクトップ調査

a. 各国セキュリティガイドライン対応状況

調査を行ったが、セキュリティガイドラインに対しての対応や今後の対応予定といったことについての具体的情報はない。（英国政府のレターを受けて）調達ルールの変更は示唆されてはいるが、具体性のある情報は出されていない。

b. 受入検査でのセキュリティ検査

ベンダー内に評価センターを設置しているとのことだが、詳細は不明。

c. 運用時のセキュリティ対策

対策の一つとして、Red Team 攻撃を行っている。BT のセキュリティ防御に対して「倫理的な攻撃」を行って弱点を特定し、実際のハッカーが BT の防御の不具合を見つける前に同社の防御を強化している。そのプロセスは、「Red-Teaming」と呼ばれ、BT Security の Red Team によって実行されている。また、これに対応する Blue Team も存在し、これらのサイバーセキュリティ戦争ゲームがネットワークの防御に寄与している。「これは大きなオーバーヘッドではあるが、それだけの価値がある。Red Team は問題を見つけ、Blue Team

と協力して修正を行う」とのことで、Red Team は攻撃の演習が完了するまで待つことはしないため、Red Team と Blue Team は「Purple-Teaming」と呼ぶプロセスの中で、継続的な「アジャイル」な方法で絶えず協力しているとのこと[84]。

d. 第三者試験でのセキュリティ検査

調査を行ったが、明確な情報は得られていない。

e. GSMA の評価機関

調査を行ったが、GSMA の評価機関のベンダーへの利用促進や、ベンダーからの調達条件に加えるといった情報はない。

[84] Light Reading: Why BT's Security Chief Is Attacking His Own Network
https://www.lightreading.com/security/security-strategies/why-bts-security-chief-is-attacking-his-own-network/d/d-id/734526

5.7 BSA によるソフトウェア透明性確保に関する民間活動

5.7.1 調査目的

ソフトウェアの既知脆弱性を把握するためには、開発するコードだけではなくリンクされるライブラリを含めたソフトウェア全体構成を把握し、チェックする必要がある。そのため、ソフトウェアの構成要素を把握するソフトウェア透明性確保に関する活動の状況を調査した。

5.7.2 調査対象

ソフトウェアの知的財産保護や不正使用対策を推進している BSA (The Software Alliance) の活動を調査対象とした。また、民間活動ではないが、NTIA（米国商務省電気通信情報局: National Telecommunications and Information Administration）のソフトウェア透明性についての活動も追加調査を行った。

5.7.3 調査方法

デスクトップ調査及びセキュリティ有識者へのヒアリングにより情報収集を行った。

5.7.4 調査結果 (BSA)

5.7.4.1 BSA [85](The Software Alliance)概要

BSA は 1988 年に設立され、ワシントン DC に本部を置き 60 ヵ国以上で活動している。日本での活動は 1992 年に開始した。主な活動は、法制度及び重要政策に関する政府への提言（ポリシーアジェンダ）と不正対策活動（不正対策アジェンダ)。さらに、①知的財産とイノベーションの保護、②グローバル市場の開放、③グローバルクラウドの促進、④プライバシーの保護、⑤サイバーセキュリティ、等の重要政策に取り組んでいる。

2018 年 11 月時点で 38 の企業が加盟、Apple、Microsoft、IBM 等の大手 IT 企業が名前を連ねており、日本企業ではニコンイメージングジャパン（映像事業の国内販社）が加盟している。

5.7.4.2 ソフトウェア透明性への取り組み（Software Component Transparency）

BSA 単独では透明性に向けた大きな取り組みは見受けられなかった。しかし、NTIA が進めているソフトウェア構成透明性 (Software Component Transparency[86]) の議論に参画している模様であった。

そのため、民間活動ではないが、調査対象として NTIA の活動を追加した。

---

[85] BSA: https://bsa.or.jp/

[86] NTIA: NTIA Software Component Transparency
https://www.ntia.doc.gov/SoftwareTransparency

5.7.5　調査結果（NTIA）

5.7.5.1 NTIA[87]概要

NTIA は 1978 年にワシントンに設立された、大統領に対して電気通信・情報関連政策に関して助言を行う行政機関である。他省庁と協力して、電波の周波数割り当て、ブロードバンド、インターネットの利用に関連する政策課題（プライバシー、サイバーセキュリティ、著作権）等も扱っている。

2018 年 6 月、NTIA は、ソフトウェアを構成するモジュール、ライブラリ、オープンソース、商用ソフトウェア等の透明性を高め、セキュリティ向上を目指した施策である Software Component Transparency の開始を発表した。ソフトウェアの開発者やベンダーが、どのようにしてソフトウェアの構成要素に関する有益な情報を提供するか、どのようなツールを用いるか、ソフトウェア購入企業がセキュリティの観点からこのデータをどのように活用するか等について議論を進めている。

公開されている情報は多くはなく、具体的な参加者も明示されていないが、簡単な経緯が公表されている。

2019 年 2 月末の時点で 3 回ミーティングが実施されている。

5.7.5.2 第一回目ミーティング

2018 年 7 月 19 日に第一回目のミーティングが開催され、以下の登壇者による、ソフトウェア透明性に対する見解のプレゼンテーションが実施された。

- Art Manion, Senior Vulnerability Analyst, CERT/CC[iv]
- Bruce Lowenthal, Senior Director, Security Alerts Group, Oracle[88]
- Jim Jacobson, Chief Product Security Officer, Siemens Healthineers[89]
- Chris Wysopal, Chief Technology Officer, Veracode
- Joshua Corman, Chief Security Officer, PTC[90]
- Jennings Aske, VP & CISO, New York Presbyterian[91]

CERT/CC の Manion 氏は、エンドユーザーやベンダーの立場からは、製品全体の脆弱性有無を確認するためには、製品をブレイクダウンして個々のコンポーネントの脆弱性の有無を確認することが有効である旨の見解を表明した。

Oracle の Lowenthal 氏は、ベンダー、コンシューマー、サードパーティ開発者の各観点からソフトウェア透明性に関するメリット・デメリットを考える必要がある旨の見解を表明した。ベンダーやコンシューマーとしては、ソフトウェアが迅速に開発されつつも、悪用可能な脆弱性は確実に対処されるようになることを目指している。一方、サードパーティ開発者としては、煩雑な規制・ルールが導入されることによりサードパーティ製コンポーネントの使用が控えられるようにならないことを目指していると考えられる。また、ソフトウェアの構成要素が透明化されることには、不要な修正も多く発生しかねないというデメリットもあるとしている。

---

87 NTIA: https://www.ntia.doc.gov/

88 1977 年に米国で設立された、データベース管理システムを中心とした企業向けソフトウェア開発・販売会社

89 独 Siemens グループの医療事業会社。2016 年に Siemens Healthcare より名称を変更

90 Parametric Technology Corporation。CAD や PLM（製品ライフサイクル管理: Product Life cycle Management）関連のソフトウェア及びサービスを提供する米国のソフトウェア会社

91 ニューヨーク長老派教会医療センター

Siemens Healthineers の Jacobson 氏[92]によると、メーカーは脆弱性管理のために SBOM（ソフトウェアの構成要素リスト: software bill of materials）を活用しており、リスクの低減や信頼の構築のために消費者にその情報を提供することにも前向きだが、ユースケースや標準的な手法等について詳細を詰める必要があるとしている。また、同氏は 2018 年 3 月にも、顧客の環境を守り信頼したパートナー関係を構築するために、透明性を向上する必要があるとの考えをオープンレターで表明している。

Veracode の Wysopal 氏によると、NVD（NIST が管理している脆弱性情報データベース: Nationality Vulnerability Database）にすべての脆弱性情報が含まれているわけではなく、オープンソースプロジェクトには NVD には掲載されていない多くの脆弱性が含まれている。また、構成要素であるライブラリに脆弱性が存在する場合でも、製品としては脆弱性を示さない場合が多いことを示した。

PTC の Corman 氏[v]は、2018 年 8 月に PTC は、同社製品が動作する環境に影響を与えうる脆弱性をエコシステム全体で協力して発見・修正する取り組みである、Coordinated Vulnerability Disclosure Program を発表した。Corman 氏は本取り組みの発表時に、ソフトウェアが複雑化している状況下ではサイバーセキュリティに対してあらゆる人が責任を持ち、脅威に対応するために協働しなければならないと述べている。

ニューヨーク長老派教会医療センターの Aske 氏は、以前実施されたインタビュー[93]では、ヘルスケア業界でもその他の産業と同様のサイバー脅威に直面しているが、セキュリティの重要性への理解が他産業よりも遅れていると感じていると表明し、ヘルスケア業界においても、NIST サイバーセキュリティフレームワークのような今日のサイバー脅威に対応したフレームワークを適用すべきだとの考えを示した。

また、本ミーティングでは以下の四つのワーキンググループが提案され、活動が進められることとなった。

- Understanding the Problem: ソフトウェアの透明性を実現するためのアイデアと解決すべき問題や、SBOM データをどのようにシェアすべきかについて詳しく調査を実施する。
- Use Cases and State of Practice: 現状調査を通じて、何が有効で何が障害となりうるかを分析する。SBOM データ活用のユースケースを特定する。
- Standards and Formats: ソフトウェア製品を構成するライブラリ、オープンソース、商用ソース等を特定する際の、現状の標準的な方法を調査する。また、この透明性確保を機械化するための、コミュニティや産業界の活動を調査・分析する。
- Healthcare Proof of Concept: ヘルスケア業界と協働し、SBOM データの作成と利用方法を実験し、SBOM データフォーマットとプロセスのプロトタイプを作成する。

5.7.5.3 第二回目ミーティング

2018 年 11 月 6 日に第二回目のミーティングが実施され、各ワーキンググループの方向性が確認された。

Understanding the Problem のワーキンググループからは、関係者の認識を合わせるために、ハイレベルなガイダンスのドラフトが提示された。スコープは SBOM の構造、共有方法、活用方法等の定義を含むとしている。SBOM の提供者や使用者もリストアップし、ユースケースを定義することを目標として掲げている。

---

92 Global Engage: Medical Device Cyber Security: An Open Letter From Jim Jacobson http://www.global-engage.com/life-science/medical-device-cyber-security-an-open-letter-from-jim-jacobson/

93 CareersInfoSecurity: Jennings Aske on Getting Serious About Medical Device Security https://www.careersinfosecurity.asia/interviews/jennings-aske-on-getting-serious-about-medical-device-security-i-3756

Healthcare Proof of Concept のワーキンググループからもコンセプトが提示され、目標は SBOM 活用の成功例を示し、セクター共通の標準的なフォーマットやプロセス作成に寄与することとされている。ユースケースの検証で主要な役割を担う組織として、医療機関からは、ニューヨーク長老派教会医療センターとシダーズ・サイナイ医療センター、ヘルスケア企業からは、Abbott、Bayer、Philips、Siemens が挙げられている。Use Cases and State of Practice や Standards and Formats ワーキンググループと連携してユースケースを作成、検証を進めるとしている。

5.7.5.4 第三回目ミーティング

2019 年 2 月 20 日に第三回目のミーティングが実施され、各ワーキンググループの活動状況の報告があった。

Healthcare Proof of Concept のワーキンググループでは、PoC の流れが説明された。現在、ヘルスケアのユースケースにて SBOM の共有に関する実証を進めている。

- ヘルスケアのユースケース
  - ✓ HDO（医療提供機関: Healthcare Delivery Organization）と医療機器製造業者(MDM: Medical Device Manufacturers）の間で SBOM を共有

- 効果測定ポイント
  - ✓ 調達（Procurement）
  - ✓ 資産管理（Asset Management）
  - ✓ 脆弱性とリスク管理（Vulnerability and Risk Management）

- 現在（2019 年 2 月）の進捗状況
  - ✓ ユースケースの確定
  - ✓ 暫定 SBOM データフォーマットを決定
  - ✓ HDO インベントリ完成
  - ✓ 最終的な PoC の役割と責任を定義

- 今後のステップ
  - ✓ SBOM の共有協定の締結
  - ✓ MDM が SBOM を提供する製品の決定
  - ✓ どの効果測定ポイントを、どの HDO で実行するか決定
  - ✓ HDO での評価
  - ✓ データ収集フォーマットの標準化
  - ✓ 最終報告書の作成

次回のミーティングは 2019 年 4 月 11 日に予定されている。

5.7.5.5 セキュリティ有識者による見解

本議論の目的はソフトウェアの透明性を高め、脆弱性発見を促すことで製品のセキュリティを高めることである。ただ、サイバーセキュリティのコンサルティングや講演活動等を行っているセキュリティ有識者は、「このような新たなルールを策定すると、新たなツール・サービスや認証が必要となるのが常であり、それが規制団体の一つの狙いでもある」との見解を持っている。つまり、本ルール策定により生じるツール・サービス提供ビジネスの取り込みが企図されていると考えられる。さらに、ルール通りに透明性を確保しない企業や、実

施のためのコスト負担ができない企業はサプライチェーンから排除されることとなる。また、決まったルールを他国へも展開（押しつけ）する可能性も考えられる。

[iii] 以下の資料を基に NEC が作成
Dr.ir. Anand R. Prasad, 3GPP TSG SA WG3 Chairman, NEC Corp.: India-European Dialogue on ICT Standards & Emerging Technologies
https://docbox.etsi.org/workshop/indo-european%20dialogue%20on%20ict%20standards%20and%20emerging%20technologies/21_anand_prasad_nec.pdf

[iv] CERT Coordination Center。インターネットセキュリティを扱う米国の研究・開発センター。1988 年に DARPA（Defense Advanced Research Projects Agency: 米国防高等研究計画局）が中心となり米カーネギーメロン大学の Software Engineering Institute 内に設置された、世界で最初の CSIRT (Computer Security Incident Response Team)

[v] PTC: PTC Launches Cybersecurity Initiative to Collaborate with Customers, Partners, and Researchers for More Secure and Resilient IoT Deployments
https://investor.ptc.com/news-releases/news-release-details/ptc-launches-cybersecurity-initiative-collaborate-customers

6. 技術動向調査(検査技術)

6.1 調査目的

検査技術の課題に関する最新動向を調査し、技術開発の方向性等の提言を行うための情報を収集する。

6.2 検査技術に関する調査の全体像

6.2.1 調査スコープ

本調査では、セキュリティ検査の技術動向、ホワイトハッカーの活用状況（バグバウンティ）について調査を行った。

セキュリティ検査の技術動向については、①プログラムに異常がある脆弱性検知の高度化技術、②バックドア等のプログラムは正常だが意図していない不正を検知する技術の二つの技術に絞って調査を行った。具体的には、バックドア等の不正に関しては、事例を調査し、誰が発見したのか、その発見者のバックグラウンドはどのようなものかを調査した。さらに、脆弱性・不正検出のための手法の現状と課題、研究動向、今後の研究課題について調査した。

ホワイトハッカー活用状況については、バグバウンティを提供している会社の採用・報酬・プロジェクト運用方法や、関連制度について調査した。

6.2.2 調査結果の要旨

6.2.2.1 不正検知の事例

不正の事例は、ハードウェアで 2 件（及び疑惑があったが否定されたものが 1 件)、ソフトウェアで 8 件の公開情報が見つかった。このうち大半はセキュリティベンダーの研究者による発見であった。

6.2.2.2 ソフトウェアに対する検査技術動向

ソフトウェアに対する検査技術として、大きく動的解析（ファジング）と静的解析（ソースコード解析）がある。

動的解析（ファジング）においては、「何をインプットデータとして、どの程度行えばセキュリティが担保されるのか」という課題が存在し、その課題に対して何を入力データとすることが効率的・効果的かという研究が主に行われている。

静的解析（ソースコード解析）においては、機械学習、AI 等を活用して、人的にカバーしている部分をいかに自動化するかという研究が行われている。

上記のような研究が行われている一方、静的、動的解析単体の精度を高くしたとしても、問題はついてまわるため、両者を組み合わせてセキュリティを担保していくことが現実的であり、そのようなアプローチで製品を提供している会社も存在する。

6.2.2.3 ハードウェアに対する技術動向

不正なチップの検出において、物理的に違いを見つける方法として画像を比較する等の手法や、電気特性を利用して違いを見つける研究が行われている。その際に真正性の定義は、設計図または真正と思われる実物のチップをベースとして行われている。

設計図を元にファウンドリ（Foundry）が作成したチップを動的に変更するカモフラージュ技術も研究されており、真正性を定義することは現実的にはかなり困難になると想定される。

多数の購買品の中から差分を見つける等の横比較で異物を見つける等の方法を用いることしか一般的な企業では対応できない可能性が出てきている。

6.2.2.4 ホワイトハッカー活用状況

バグバウンティのプラットフォーム提供企業では Synack や HackerOne、Bugcrowd を調査対象とした。各社はペンタゴン（米国防総省）主催のバグバウンティに参画しており、パブリックドメインを HackerOne や Bugcrowd が、より機密性が高いプライベートドメインは Synack が担当している。

Synack では、ハッカーの選考に非常に厳正なプロセスがとられており、バックグラウンドチェックも入念になされているため、クライアントからの信頼が厚い。そのため、ペンタゴンが実施しているプログラムでも機密性の高い領域を任せられており、有名企業からも多くの重要な案件が持ち込まれている。このことがハッカーの人気を呼び、多くの採用申し込みが自然と集まる状況となっている。

また、Synack Red Team のメンバーはフリーランスで働いている人もいれば、Google や Facebook のような GAFA 等の IT 大手企業に勤務しつつ副業として働いている人もいる。上記の通りチャレンジングな案件を多数抱えていることが、エンゲージメントを高める一因となっている。

6.3 ソフトウェア検査技術

6.3.1 ソフトウェアの不正検知事例

ソフトウェアの不正検知事例として 8 件の事例は、4 件（3 社）がセキュリティ会社/研究機関、2 件が政府関与も一定の可能性があるセキュリティ会社/研究機関、1 件がマイクロソフト、1 件が個人（OSS 開発者）による発見であった。

6.3.1.1 事例①: 中国製スマートフォンのバックドアの発見[94]（2014 年、Palo Alto Networks）

6.3.1.1.1 概要

米国のセキュリティベンダーである Palo Alto Networks は 2014 年 12 月、中国大手スマートフォンメーカーである宇竜計算機通信科技が販売している Android 搭載スマートフォン「Coolpad」にバックドアが存在することを発見した。

多くの同社製端末ユーザーから不審な挙動が報告されていたことから、Palo Alto

[94] インターネットコム: 米パロアルト、中国製スマートフォンのクールパッドにバックドアを発見 https://internetcom.jp/allnet/20141219/palo-alto-finds-back-door-in-cool-pad-chinese-made-smartphone.html

Networks の脅威インテリジェンスチームである Unit 42 が調査・分析を行い、バックドアを発見した。このバックドアは「CoolReaper」と呼ばれ、基本的なデータ収集の範疇を越えた動作を行っていた。

ユーザー情報や行動履歴をサーバーに送信し、リモートでインストール・広告の表示等が可能になる機能が確認された。また、Coolpad では Android OS を変更して、アンチウイルスプログラムがバックドアの検出を行うのを困難にしていた。

Coolpad は世界で 6 位、中国では 3 位のシェア（当時）があったため、1,000 万人以上のユーザーが影響を受ける対象となっていた。

6.3.1.1.2 発見者プロファイル: Palo Alto Networks[95]

- 企業概要

2005 年に米国で設立された情報セキュリティ企業である。エンドポイントセキュリティ、クラウドセキュリティ、ファイアウォール等、幅広く製品を提供している。2018 年 7 月期売上高は 22 億 73,00 万米ドルで、2018 年 10 月時点の連結ベースでの従業員数は 5,645 人である。150 ヵ国以上の様々な業界で 54,000 件を超える顧客を擁している。

- リサーチチーム: Unit 42

Unit 42 は Palo Alto Networks の脅威インテリジェンスチームで、熟練したサイバーセキュリティ研究者と業界の専門家で構成されている。最新のサイバー脅威を調査・分析し、インサイトを顧客、パートナー、コミュニティと共有することで、企業、サービスプロバイダー、政府のコンピュータ環境をよりよく守ることに貢献することを目的としている。

Unit 42 では Palo Alto Networks のセキュリティプラットフォームから収集されたデータから、攻撃者の動機と方法に関連するコンテキストを分析する。脅威の分析に必要なデータを定義し、そのデータを社内外から収集、詳細な脅威分析プロセスを実行している。

- 設立背景

現在 CTO（最高技術責任者: Chief Technology Officer）を務める Nir Zuk 氏が共同創業者の一人として創業した。Nir Zuk 氏は、Palo Alto Networks を共同創業する以前は、2004 年に Juniper Networks 社によって買収されることになる NetScreen Technologies 社の CTO を務めていた。NetScreen 社の前は、IPS（不正侵入防御: Intrusion Protection System）のアプライアンスを他に先駆けて開発した OneSecure 社の共同創業者で CTO だった。それ以前は Check Point Software Technologies 社の主要なエンジニアとして勤務していた。

- CEO

2018 年 6 月に Nikesh Arora 氏が会長兼 CEO（最高経営責任者: Chief Executive Officer）に就任。

Palo Alto Networks の会長兼 CEO に就任以前には、ソフトバンク株式会社（現 ソフトバンクグループ株式会社）の代表取締役副社長を務めた。それ以前は Google 社に在籍し、10 年にわたり上級副社長、最高ビジネス責任者、グローバルセールスオペレーションやビジネス開発の責任者、欧州・中東・アフリカ地区の責任者等を歴任。Google 社勤務以前は、T-Mobile International 社の欧州事業であるドイツテレコム AG 社の最高マーケティング責任者や T-Motion PLC 社の創業者兼 CEO を務めた。T-Motion PLC 社は、2002 年に T-Mobile 社と合併した。

現在は、スイスに本社を置く高級品ブランドの Richemont 社や、ベイエリアで貧困問題と戦う非営利団体 Tipping Point の理事会のメンバーも務めている。また過去には Sprint 社、Colgate-Palmolive 社、ヤフー株式会社等の取締会のメンバーを歴任した。

---

[95] パロアルトネットワークス株式会社: 事業概要
https://www.paloaltonetworks.jp/company

ノースイースタン大学の経営学修士、ボストン大学の財政学修士、ベナレス・ヒンドゥー大学の電子工学科学技術学士を取得している。

6.3.1.2 事例②: Android を狙うバックドアの発見[96]（2016 年、Palo Alto Networks）

6.3.1.2.1 概要

Palo Alto Networks の Unit42 の研究者は、Android 向けのトロイの木馬「SpyNote」を発見し、流行の兆しがあると 2016 年 7 月に公表を行った。

複数のバージョンの SpyNote を作成するためのビルダーツールの存在を確認した。このツールを使って開発されるトロイの木馬はバックドアとして機能するための様々な機能を有している。また、一度インストールしてしまうと取り除くことが難しいとのことであった。

6.3.1.3 事例③: 大使館を狙うバックドアの発見[97]（2017 年、ESET）

6.3.1.3.1 概要

2017 年 8 月、ESET は同社の研究者らが有名なサイバースパイグループ「Turla」が利用してきたと見られるステルス性が極めて高いバックドア型マルウェア「Gazer」を発見したと発表した。

政府や外交官を対象とした攻撃が少なくとも 2016 年から行われていることが疑われ続けていた。ESET の研究者らは、これまで正体が不明だったこのバックドアについて、世界で初めて明らかにすることに成功したとしている。研究者らは分析の中で、感染の第一段階では別のバックドアが使われて第二段階で Gazer が使われていること、Gazer がセキュリティソフトウェアによって検出されないように高いレベルのステルス機能を備えていること等を指摘した。また、同研究者によると、Gazer は世界中で多くのコンピュータに侵入しており、大部分の被害は欧州、主に旧ソ連や欧州の南東エリアで発生していた。

6.3.1.3.2 発見者プロファイル: ESET[98]

- 企業概要

1992 年にスロバキアで設立された情報セキュリティ企業である。コンピュータセキュリティの脅威に対抗するための包括的なソフトウェアソリューションの設計・開発・実施等を行っている。

2015 年 4 月時点で従業員数 1,000 人を突破し、2017 年 12 月期の売上高は 4 億 6,100 万ユーロである。200 以上の国・地域でビジネスを展開している。

- 設立背景

1987 年に Peter Pasko 氏と Miroslav Trnka 氏が世界で最初のウイルスの一つを発見、それを検出するプログラムを開発し、1992 年に両氏により ESET が設立された。

---

[96] マイナビニュース: Android を狙うトロイの木馬「SpyNote」、近いうちに流行か
https://news.mynavi.jp/article/20160801-a320/

[97] マイナビニュース: 大使館を狙うバックドア「Gazer」を発見 - ESET
https://news.mynavi.jp/article/20170901-a070/

[98] ESET North America: About us
https://www.eset.com/us/about/

- CEO

Richard Marko 氏が CEO を務めている。大学在学中から ESET で働き始め、現在の主要アンチウイルスソフトの開発にも携わった。2011 年 1 月より現職。

6.3.1.4 事例④: ホワイトハウス・軍戦略センターでのバックドアアカウントの発見[99]（2016 年、SEC Consult）

6.3.1.4.1 概要

2016 年 1 月、SEC Consult によりホワイトハウスと軍事戦略センターで使われている AMX デバイスのファームウェアにバックドアアカウントが発見されたと発表された。

研究者らはソースコードに秘密のユーザーアカウントを作成する機能があることを発見した。この機能で作成したアカウントはデバイスの設定画面には表示されない仕組みになっていたという。

SEC Consult は AMX（米国の会議装置ベンダー）に問題を報告し、AMX が問題を修正したファームウェアを公開したが、再度 SEC Consult が調査を実施したところ、隠れたアカウント名が変わっただけで同じ機能が残っていることが発見された。SEC Consult はなおも働きかけを続け、新しいバージョンではどちらのアカウントも存在しないとリリースノートに掲載されるに至った。AMX はこれらのアカウントはデバッグ目的で使われていたと説明している。

6.3.1.4.2 発見者プロファイル: SEC Consult[100]

- 企業概要

2002 年にオーストリアで設立された、セキュリティコンサルティングサービス会社である。セキュリティコンサルティングやインシデントレスポンス（事故原因の調査・再発防止策の実施）、脆弱性検査等の各種サービスを提供しており、欧州における政府機関や民間企業等への豊富な提供実績・ノウハウを有している。

内部のセキュリティ研究所として Vulnerability Lab を運営しており、ネットワークとアプリケーション領域でのノウハウ蓄積を企図している。さらに、Vulnerability Lab はペネトレーションテストや新技術評価も実施している。

- 設立背景

Clemens Foisner 氏により設立された。

6.3.1.5 事例⑤: 正規ソフトウェアのアップデートにバックドアを仕込んだ「ShadowPad」を発見[101]（2017 年、Kaspersky）

6.3.1.5.1 概要

2017 年 8 月、Kaspersky Lab の GReAT（グローバル調査分析チーム: Global Research

[99] マイナビニュース: ホワイトハウスおよび軍戦略センターでバックドアアカウント発見
https://news.mynavi.jp/article/20160122-a633/
[100] SEC Consult: https://sec-consult.com/en/
[101] 日本経済新聞: カスペルスキー、正規ソフトのアップデートにバックドアを仕込んだ「ShadowPad」を発見
https://www.nikkei.com/article/DGXLRSP454208_Y7A810C1000000/

and Analysis Team）のリサーチャーが、世界数百の大手企業にサーバー管理ツールを提供している NetSarang（韓国）が配信したソフトウェアパッケージに埋め込まれたバックドアを発見したと発表した。

2017 年 7 月、GReAT のリサーチャーが取引先のある金融機関からの依頼で、金融取引処理に関わるシステムにおいて疑わしい DNS リクエストについて調査を行った。その結果、これらのリクエストは NetSarang のサーバー管理ソフトウェアから来ていることが発覚した。このソフトウェアは、金融サービス、教育、通信、製造、エネルギー、運輸業界等、数百もの組織が導入していた。

リサーチャーがさらに詳細に分析したところ、この疑わしい DNS リクエストは NetSarang の正規ソフトウェアのアップデートが改竄され、仕込まれたマルウェアによって実行されていることが判明した。改竄されたアップデートをインストールすると、このマルウェアは複数の特定ドメイン（指令サーバー）に対して 8 時間に 1 回、感染コンピュータのユーザー名、ドメイン名、ホスト名等の基本情報を送信し、攻撃者がそのコンピュータに「興味を持った」場合は指令サーバーが応答、バックドアを有効化して悪意あるコードをダウンロードして実行できるようになる仕組みであった。

NetSarang は Kaspersky Lab からの連絡を受け、直ちに悪意あるコードを削除したソフトウェアのアップデートをリリースした。本バックドアが仕込まれたマルウェア「ShadowPad」は、これまでのサプライチェーン攻撃の中でも最大規模の一つと言われており、素早く検知、解決していなければ、世界中の数百もの組織が攻撃の被害に遭っていた可能性があった。

6.3.1.5.2 発見者プロファイル: Kaspersky Lab[102]

- 企業概要

1997 年に設立されたコンピュータセキュリティ企業で、ロシアに本社を置く。持株会社は英国で設立しており、200 の国・地域で事業を展開、世界 31 ヵ国に 35 の事業所を設けている。世界中に 3,800 人以上の社員を擁しており、その 3 分の 1 が研究・開発業務に従事している。2017 年の全世界での IFRS 収益（国際財務報告基準: International Finincial Reporting Standards）は 6 億 9,800 万米ドルである。

- リサーチチーム: GReAT

GReAT は 2008 年に設立され、全世界に 40 人超の専門家を抱えている。Kaspersky Lab の R&D で研究開発に携わる中核部門として、脅威に関する情報収集、調査研究及びその成果発表等の活動を実施している。また、マルウェアによるインシデント発生時の対応措置も担当している。

- 設立背景

現在の CEO である Eugene Kaspersky 氏により設立された。

Eugene Kaspersky 氏は 1987 年、ソ連国家保安委員会（KGB）技術アカデミーで数学・暗号理論・計算機科学・数理工学等を専攻して卒業した。1989 年に自身が利用していたコンピュータがウイルスに感染した際に、専攻していた暗号学の知識を用いてウイルスを解析し駆除するツールを開発したことが設立に至る基礎となる。1990 年に研究者を集めてアンチウイルスプログラムを作成し、1997 年には同僚と Kaspersky Lab を設立、Eugene Kaspersky 氏は同社のアンチウイルス研究をリードした。

[102] Kaspersky Lab: 会社情報
https://www.kaspersky.co.jp/about/company

- CEO

Eugene Kaspersky 氏が 2007 年に CEO に就任した。

- 米国政府との関係性[vi]

2017 年 9 月、DHS（米国土安全保障省: United States Department of Homeland Security）は、連邦政府機関において Kaspersky Lab の製品の使用を禁じる通達を行った。

米国政府は 2016 年の大統領選挙でロシア政府のハッキングによる介入があったとして調査を行い、安全保障上の問題があるとして、政府調達企業リストから同社を外した。

Kaspersky Lab はこの騒動を受け、透明性を高める取り組みを進めており、2018 年 5 月には同社が使用するツールやソースコードを第三者組織が監査・検証するための施設「Transparency Center」をスイスのチューリッヒに開設した。2020 年までにはアジア、米国にも同施設を開設する予定になっている。

6.3.1.6 事例⑥: Android 端末への不正ファームウェア搭載の発見[103]（2016 年、Kryptowire）

6.3.1.6.1 概要

2016 年 11 月掲載の記事で、政府機関や個人企業にモバイル端末向けセキュリティサービスを提供する Kryptowire は、7 億台の Android スマートフォンにデバイスデータ及び特定可能なユーザーの個人情報を所有者の許可をえることなく送信するファームウェアが搭載されていると指摘した。

バックドアが見つかったのは、中国企業・上海広升信息技術（ADUPS）のファームウェアが搭載されている Android OS 搭載スマートフォンで、米国各地で販売される米メーカーである BLU Products 社の端末が含まれていた。ADUPS 社製のファームウェアにバックドアが含まれており、端末が特定できるデータや、発着信があった電話番号、連絡先のリスト、テキストメッセージ等が定期的に中国のサーバーに送られていた。同ファームウェアにはまた、遠隔操作によりスマートフォン上でコマンドを実行したり、プログラムを書き換えたりする機能が備わっていたとされる。

ADUPS は声明を発表し、問題のファームウェアは迷惑なメッセージや電話を選別する目的で設計されたものだと釈明した。他の顧客向けに開発された自動アップデートが BLU 社の製品にも「意図せずに」インストールされてしまったが、BLU 社側の苦情を受けて既に無効化したと説明した。ADUPS は「テキストメッセージや連絡先、通話記録等、問題の機能に関する情報は第三者には一切公開されておらず、該当する短期間のうちに BLU 製スマートフォンから集められた情報はすべて削除された」と述べている。

6.3.1.6.2 発見者プロファイル: Kryptowire[104]

- 企業概要

2011 年に米国で設立された、セキュリティ解析ツール（主にモバイルアプリケーション、IoT 機器向け）提供会社である。民営・公営セクターの各組織に対し、自動化した高度なソフトウェアテスト技術を提供している。

- 設立背景

DARPA（米国防高等研究計画局: Defense Advanced Research Projects Agency）、DHS

[103] マイナビニュース: 7 億台の Android 端末に中国にデータ送るバックドア
https://news.mynavi.jp/article/20161121-a325/
[104] Kryptowire: About Us
https://www.kryptowire.com/about-us/

を背景に設立された。創業者は Angelos Stavrou 氏で、CEO も務めている。

- CEO

Kryptowire の創業者かつ CEO である Angelos Stavrou 氏は、ジョージメイソン大学の教授も務めている。

NSF（米国立科学財団: National Science Foundation）や DARPA、DHS 等の様々な機関で主要な研究者として務め、現在は NIST（米国国立標準技術研究所: National Institute of Standards and Technology）のモバイルセキュリティチームのアクティブメンバーでもあり、今までに 90 本以上の査読済み記事を執筆している。

現在の研究テーマは、分散システムのセキュリティと信頼性、仮想化のセキュリティ原則等である。

6.3.1.7 事例⑦: サプライチェーン攻撃の発見[105]（2018 年、Microsoft[106]）

6.3.1.7.1 概要

2018 年 7 月、Microsoft は PDF 編集アプリケーションにおいてサプライチェーン攻撃があったことを発見したと発表した。

Microsoft のスタッフが商用の Windows Defender からアラートを受け取り、内容の詳細を分析したことで攻撃が発覚した。攻撃者は正規の PDF 編集アプリケーションプロバイダーのサーバーを複製し、同サーバーにマルウェアを含んだフォントファイルを格納することで、同ファイルを知らずにインストールしたユーザーの PC に暗号通貨マイニングソフトがインストールされるようになっていた。インストールされると、不正の暗号通貨マイニングソフトはユーザーのシステムにフルアクセスを持つことになる恐れがあったが、Windows Defender ではマイニングコードに特有な振る舞いを検知し、アラートの発信に至った。

6.3.1.8 事例⑧: Samsung ギャラクシー端末のバックドアの発見[107]（2014 年、OSS 開発者）

6.3.1.8.1 概要

2014 年 3 月、Android 搭載スマートフォン向けの OSS 開発者が、Samsung Electronics のスマートフォン「Galaxy シリーズ」に、スマートフォンに保存されているファイルの読み込み・書き込み・削除を可能にするプログラムが組み込まれていることを発見したと発表した。今回明らかになったバックドアは、モデムがスマートフォンの記憶領域に直接アクセスできない遠隔地にある場合においても、端末内のデータの閲覧・書き込み・削除を可能にしてしまうものであった。Samsung は、調査の結果セキュリティ上のリスクは存在しないことが判明したと発表した。

---

105 Bleeping Computer: Microsoft Discovers Supply Chain Attack at Unnamed Maker of PDF Software
https://www.bleepingcomputer.com/news/security/microsoft-discovers-supply-chain-attack-at-unnamed-maker-of-pdf-software/

106 1975 年に Bill Gates 氏らにより設立された、米国のソフトウェア開発・販売会社。

107 Gadgets 360: Third-party developers discover a 'backdoor' in Samsung Galaxy devices
https://gadgets.ndtv.com/mobiles/news/third-party-developers-discover-a-backdoor-in-samsung-galaxy-devices-495318

6.3.1.9 その他事例: ソフトウェア PLC の脆弱性発見[108]（2018 年、東大学生）

6.3.1.9.1 概要

2018 年 9 月、IPA 及び JPCERT コーディネーションセンターは、マイクロネットが提供するソフトウェア PLC[109] 「INplc」に複数の脆弱性が存在すると「Japan Vulnerability Notes （JVN） 」で発表した。脆弱性の存在は、東京大学の学生である白木氏の報告により明らかになった。

影響を受けるバージョンでは、DLL 読み込みに関する脆弱性、バッファーオーバーフロー、認証不備、権限昇格の脆弱性が存在し、任意コードや任意の操作の実行、DoS 攻撃等の影響を受ける可能性があったが、最新版にアップデートすることでこれらの脆弱性は解消されるとしている。

6.3.1.10 その他研究機関による不正検知

具体的な事例は見いだせないが、BAE Systems[110]、Thales[111]、UCSB（カリフォルニア大学サンタバーバラ校: University of California, Santa Barbara）[112]の研究所等が有名で、上記のような不正発見事例がある可能性がある。

また、INL（アイダホ国立研究所: Idaho National Laboratory）[113]は DHS の要請で国内外の重要インフラのセキュリティ評価を何百件もこなし、これらシステムは極めて複雑で理解しづらく、完全な防御はほぼ不可能であると判断したとの記事がハーバードビジネスレビューに掲載されている。

6.3.2 ソフトウェア検査技術の研究動向

6.3.2.1 研究動向概要

脆弱性や不正なコードの検出においては、ソースコードが入手できない状況では主にファジングで、入手できる場合は主にソースコード解析により検出が試みられている。

ファジングには、「何をインプットデータとして入力し、どの程度行えば十分セキュリティが担保されるのか」という課題が常に存在し、その課題に対して何を入力データとすることが効率的かという研究が主に行われている。

ソースコード解析には、一見すると問題ないように見えるが動作をすると問題が起きるようなコードに関しては人の目による確認が必要という課題があり、人的部分をツールに置き換えるために自動化の研究が行われている。

---

[108] ScanNetSecurity: ソフトウェア PLC「INplc」に複数の脆弱性（JVN）
https://scan.netsecurity.ne.jp/article/2018/09/10/41367.html

[109] Programmable Logic Controller: 自動機械の制御に使用される制御装置で、ソフトウェア PLC は、PLC に柔軟性を持たせるためにソフトウェア化したもの。

[110] 1999 年に British Aerospace と Marconi Electronic Systems との合併により設立された、英国の国防・情報セキュリティ・航空宇宙関連企業。

[111] フランスの大手電機企業であり、航空宇宙分野、防衛分野、交通システム分野、セキュリティ分野での情報システムと各種サービスを提供。前身は Thomson-CSF で、2000 年に英国の防衛機器メーカー Racal Electronics plc を吸収合併した際に社名を Thales に変更。フランス政府が 25%強を出資。

[112]公立の研究型大学で、カリフォルニア大学システムを構成する 10 校のうちの 1 つ。1944 年に設置。

[113] 1949 年に NRTS（国立原子炉試験場：National Reactor Testing Station）として設立され、名称変更を重ね、2005 年に現在の INL となった。核エネルギー、国家セキュリティ、エネルギー・環境等についての研究を行っている。

一方で、上記を動的解析、静的解析の一つとして捉えると、ソースコードが入手できる状況では、トータルでの効率性の観点から、動的解析により脆弱性・不正のあたりをつけて静的解析で詳細な分析を行うという手法をとるのが一般的である。研究者からも、静的・動的解析単体の精度を上げることは様々な角度から研究されているが、実用性を考えると、両者の組み合わせ製品を出していくことが現実的である、とコメントがあった。

6.3.2.2 ファジング

6.3.2.2.1 ファジングの課題と対応

脆弱性スキャンは、既知の脆弱性のデータを元に検証するため、そのデータベースが、最新か否かが、重要な要素となる。一方、ファジングテストはファズデータを評価検証者が準備を行うケースも少なくなく、有償版でも、「何をインプットデータとして入力し、どの程度行えば十分セキュリティが担保されるのか」という問題が常についてまわることとなる。

このような中で、各社は、効果的なファジングを行うために、その裏付けとして自社のデータベース、知見に基づくアルゴリズムをアピールしている。

攻撃者側の視点から見ても、ハッキングとしての成果と合わせてヘッドカウントをはじめとするコスト、つまりは効率性も昨今は重視されるようになっており、ファジングを行い一つでも脆弱性を見つけることがハッキングの端緒となりうるため、AI や機械学習等も活用しながら自動化し、効率的にファジングを行い、脆弱性を発見するような状況へ移行することが予測されている。そのため、対策側も同様に効率化・高度化が求められることとなる。

また、昨今では Google の研究者が打ち出した AFL (American Fuzzy Lop) をベースにした研究が行われている。さらに、網羅性を向上するためにシンボリック実行を取り入れた研究や、AFL とシンボリック実行を組み合わせた研究も行われている。

6.3.2.2.2 Beyond Security[114] の製品: beStorm

代表的な製品の一つとして Beyond Security の beStorm があり、製品情報として、自社独自のアルゴリズムにより効果的にインプットを行い、アウトプットを得られることをうたっている。

beSTORM は、可能性のあるすべての入力の組み合わせを網羅的に検索して製品の弱点をテストするためにプログラムされた、自動化されたファジングツールである。当然ながら、すべての理論的な入力の組み合わせをプログラムに含めることは事実上不可能なため、beSTORM には優先順位付けアルゴリズムが装備されており、その中で妥当だと思われる検証を行う。

この優先順位付けのアルゴリズムは、Beyond Security の長年の蓄積に基づく知見から生まれたものであり、世界最大級のセキュリティデータベースの一つである SecuriTeam.com に展開されている 15,500 以上のセキュリティ脆弱性もカバーしている。

ソフトウェア開発会社からすると、網羅的に検証をするコストをかけることはできないため、Beyond Security の研究者が、ほとんどの脆弱性をカバーできるように上記のようなアルゴリズムを策定し、検証プロセスを標準化した製品を提供している。

---

[114] 1999 年に米国で設立された、脆弱性検査ソリューション提供企業。
Beyond Security: https://www.beyondsecurity.com/

6.3.2.2.3 Microsoft によるファジングツール公開[115]: Security Risk Detection

2017 年 7 月に新たな脆弱性発見ツール「Microsoft Security Risk Detection」を発表した。このツールの目的は、脆弱性が攻撃者に悪用されないよう、その検出と除去を支援することにある。ファジングを用いる同ツールは、Microsoft Research において 10 年以上前から「Project Springfield」という名称の下で開発が続けられていた。

Microsoft は、「Windows」や「Office」製品の深刻な脆弱性を発見するために、アップデートのリリース前にこのテクノロジーを活用している。同テクノロジーは一部の顧客やパートナー企業のみに提供されていたが、同社は 2016 年に Project Springfield の成果を製品化する意向を明らかにし、「Microsoft Azure」ベースのプレビュー版アプリとして公開していた。

本ツールでは、独自に人工知能（AI）を利用して、仮定したシナリオを提示し、深刻なセキュリティ脆弱性の原因となりうるものを絞り込むことで、脆弱性を特定している。

6.3.2.2.4 その他の製品事例

その他の有名なファジング製品としては、有償なものでは、Synopsys[vii]の Defensics、Wurldtech Security Technologies[116] のアキレス認証に対応した Achilles Test Software/Platform 等がある。

また OSS の無償ツールも多数出ており、論文等でも比較される製品としては、peach、sulley、boofuzz 等の製品がある。なお OSS の 3 製品に関しては標準的な機能の優劣はなく、OSS 特有のライセンス問題（GPL 等）や診断パターンファイルの記述方法が異なるという評価がなされている[117] 。

6.3.2.2.5 American Fuzzy Lop (AFL)[viii]: 遺伝的アルゴリズムを活用したファジングツール（Google）

American Fuzzy Lop (AFL) は、Google のエンジニアである Michal Zalewski 氏らによる、遺伝的アルゴリズムを用いたデータの自動生成、ファジング実行ツールである。AFL は専用のコンパイラでファジング対象ソフトウェアをあらかじめコンパイルする必要があったが、米国のセキュリティベンダーである NCC Group が Linux カーネルと AFL を統合することで、ソースコードがなくても AFL を使用できるようになり、利用の幅が広がった。

- 遺伝的アルゴリズム

生物が自然淘汰や交叉・突然変異を何世代にもわたって繰り返しながら進化していく様子を模したアルゴリズムであり、以下のステップにより構成される。

①初期集団の生成: ランダムなデータを複数用意して、初期世代とする。
②評価・選択: 各データを評価し、一定の規則を用いて選択する。評価の低いデータは淘汰され、その個数だけ評価の高いデータが増殖する。
③交叉: 設定した交叉確率・交叉方法により交叉し、新しいデータを生成する。
④突然変異: 設定した確率・方法により突然変異を行い、新しいデータを生成し、世代数が一つ上がる。

---

[115] ZDNet: MS、AI 利用のクラウドベース脆弱性発見ツール「Security Risk Detection」発表 https://japan.zdnet.com/article/35104705/

[116] 2006 年に設立された、カナダの制御システムセキュリティツールメーカ。2014 年に GE Digital が完全子会社化。

[117] 福山潤、松井俊浩（2018）「ファジングツールの機能評価と診断パターンファイルの特性調査」情報処理学会第 80 回全国大会

あらかじめ設定した世代数に到達する等の終了条件を満たすまで「②評価・選択」から「④突然変異」を繰り返す。

6.3.2.2.6 AFL 事例①: AFL の性能向上技術の研究[118]（複数国の研究者チーム）

シンガポール、オーストラリア、ルーマニアの研究者で構成されるチームは、AFL を改良したアプローチを使用した AFL SMART を発表し、従来の AFL の性能向上を図った。

AFL では入力データのビットを反転させて、プログラムを少しずつ調査しているが、より深部にある不具合を発見する目的で、ファイルの構造を大きく変化させるのには適していなかった。研究チームはこの問題を解決すべく、入力データをチャンクと呼ばれる複数のパーツに分解し、チャンク間の関係性を構造的に整理したマップを作成した。

ファジングツールにおいては、入力データをチャンクレベルで追加、削除、接合が可能であるため、出力結果を踏まえて、より効果的な組み合わせを生成することができる。生成された組み合わせに基づいてプログラムのテストを繰り返し、不具合が発見されやすい入力データを調べることでカバレッジの拡大を図った。

結果としては、従来の AFL に比べ多くの場合で発見できるパス数が増加したが、一部のファイルフォーマットでは発見できたパス数が減少した。さらに効率性を向上するためには、交叉や突然変異の確率・方法を適切に設定することが課題となる。

6.3.2.2.7 AFL 事例②: AFL をベースとしたニューラルファジング（Microsoft）

Microsoft の研究者チームは、AFL をベースに、入力値と実行結果のフィードバックループにディープラーニングを挿入したファジング手法であるニューラルファジングを考案[119]した。同手法を用い、解析を行うプログラムとして四つのファイルフォーマット（ELF、PDF、PNG、XML）を使用して実験を行った（図 6-1）。

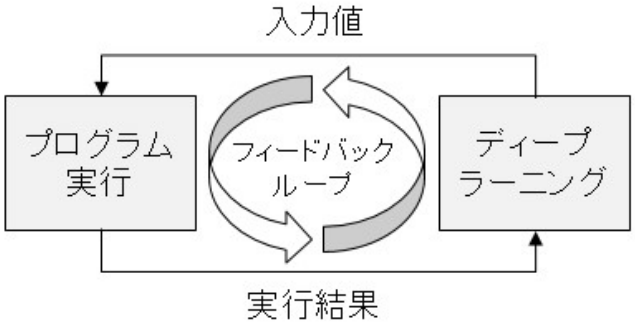


図 6-1　Microsoft ニューラルファジングイメージ図

実験の結果、従来の AFL に比べて、ELF と PNG でコードカバレッジが 10%程度改善し、PDF 以外のすべてのファイルフォーマットでより多くのユニークパスを発見、PNG では最初の 24 時間で 2 倍のユニークコードパスを発見、ELF や XML でより多くのクラッシュを報告といった、様々な点で性能が向上していることが確認された。

本手法は、入力値を自動的に予測可能であるためシンプルで、短時間でより多くのユニー

---

[118] Van-Thuan Pham, Marcel Bohme, Andrew E. Santosa, Alexandru Razva Caciulescu, Abhik roychoudhury (2018). “Smart Greybox Fuzzing”

[119] Patrice Godefroid, Hila Peleg, Rishabh Singh (2017). “Learn&Fuzz: Machine Learning for Input Fuzzing”

クパスを発見できる効率的な手法である。また、あらゆるファジング手法に適用可能なため、汎用的な手法でもある。

6.3.2.2.8 angr: シンボリック実行を活用したファジングツール（UCSB の研究チーム）

UCSB の研究チームにより開発されたバイナリ解析フレームワークで、シンボリック実行をファジングで利用できるようツール化してオープンソース化したものである。論文[120]は 2016 年に採択されている。

論文では、24 時間実行した場合の angr によるシンボリック実行の結果と従来のファジングとの比較結果が掲載されている。結果は、パスが短い位置のバグについては angr の方が多く発見しているが、パスが長くなるとファジングの方が多くのバグを発見しており、合計でもファジングの方が多くのバグを発見している。これはパスが長くなるほどシンボリック実行の計算時間が長くなるためであると考えられている。理論的にはシンボリック実行の方がより深くのパスまで到達できるため、計算時間短縮のため、パス数爆発の解消やソルバの性能向上等により高速化を図ることが課題として挙げられる。

- シンボリック実行

プログラムを解析し、存在する実行パス（実行可能なパス）の抽出及びそのパスを実行するための入力データを決定する技術である。

例えば、図 6-2 のようにプログラムをパスで考え、緑のボックスに到達したいと考えた場合、到達するための論理式は緑のボックスに記述した通りとなる。これらの論理式を満たす x、y、z の値を特定することで、狙ったパスを通していくこととなる。このような充足条件の答えを導くためのアルゴリズムを実装したソフトウェアであるソルバを用いて計算する。

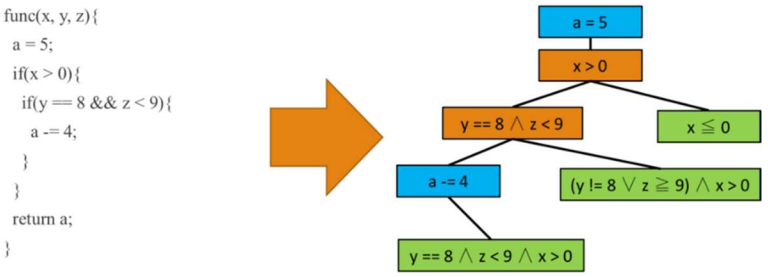


図 6-2　プログラムとパスの関係

シンボリック実行には以下のような課題が存在する。

- パス数の爆発: プログラムが複雑になるにつれ、パス数とそれに伴う計算量が爆発的に増加する。
- ソルバの制約: ソルバの種類によって得手、不得手が存在し、解を出せなかったり時間が多くかかったりする。
- 入力値が一意に定まらない: 条件を満たす入力値の組み合わせが多数存在し、一意に定まらない。

6.3.2.2.9 Driller: AFL とシンボリック実行を組み合わせたファジングツール（UCSB の研究チ

[120] Yan Shoshitaishvili, Ruoyu Wang, Christopher Salls, Nick Stephens, Mario Polino, Audrey Dutcher, John Grosen, Siji Feng, Christophe Hauser, Christopher Kruegel, Giovanni Vigna (2016). "(State of) The Art of War: Offensive Techniques in Binary Analysis", IEEE

ーム)

angr の開発陣により AFL の拡張に関する研究が行われた。論文[121]は NDSS 2016 (The Network and Distributed System Security) に採択されている。

Driller は、ファジングとシンボリック実行を交互に行うことで深い位置にある脆弱性を発見するためのファジングツールである。具体的な手順は以下の通りである（図 6-3)。

①入力値を作成
②ファジングを実施し、通過できないパスが生じた場合に手順③へ
③通過できなかった区間に対してシンボリック実行を実施し、目標とするパスを通るような入力値を特定
④手順③の実行結果から得られた値をファジングの入力へ
⑤手順②から手順④を繰り返す

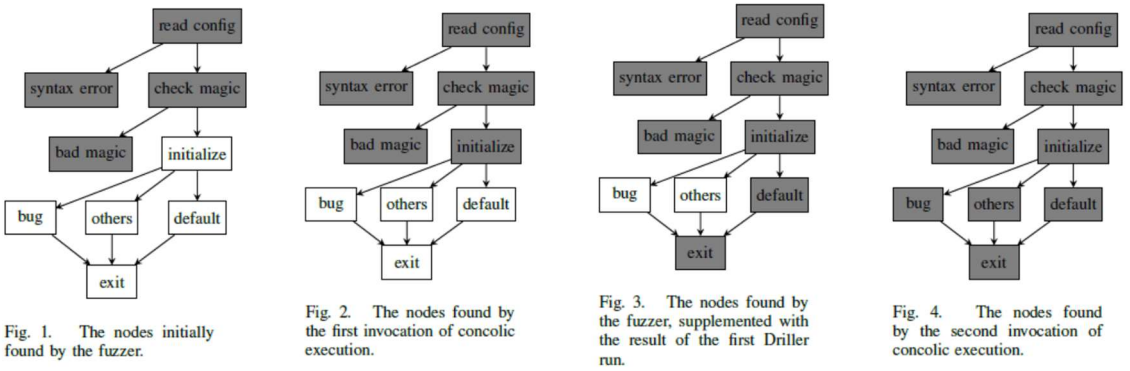


Fig. 1. The nodes initially found by the fuzzer.

Fig. 2. The nodes found by the first invocation of concolic execution.

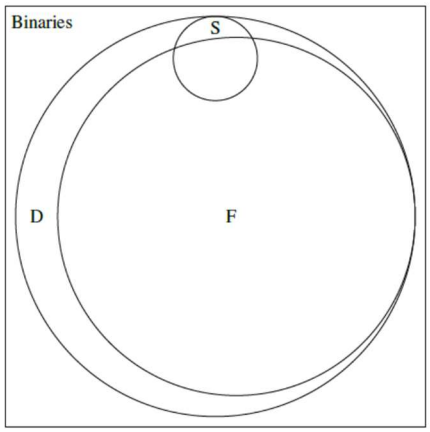
Fig. 3. The nodes found by the fuzzer, supplemented with the result of the first Driller run.

Fig. 4. The nodes found by the second invocation of concolic execution.

図 6-3　Driller の実行イメージ

図 6-4 は、126 の脆弱性が存在するプログラムに対し、Driller と AFL 単体とシンボリック実行単体（カーネギーメロン大学の研究者らが考案した手法[122] がベース）の実行結果を示したものである。Driller は 77 件、AFL 単体は 68 件、シンボリック実行単体は 16 件の脆弱性を発見しているが、Driller が発見した脆弱性は、AFL とシンボリック実行それぞれを単体で実行した場合に発見された脆弱性をすべてカバーしており、性能が向上していることがわかる。

[121] Nick Stephens, John Grosen, Christopher Salls, Audrey Dutcher, Ruoyu Wang, Jacopo Corbetta, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna (2016). “Driller: Augmenting Fuzzing Through Selective Symbolic Execution”, Network and Distributed System Security Symposium ‘16
[122] Sang Kil Cha, Thanassis Avgerinos, Alexandre Rebert and David Brumley (2012). “Unleashing MAYHEM on Binary Code”, 2012 IEEE Symposium on Security and Privacy



Method	Crashes Found
Fuzzing	68
Fuzzing ∩ Driller	68
Fuzzing ∩ Symbolic	13
Symbolic	16
Symbolic ∩ Driller	16
Driller	77

図 6-4　Driller、AFL、シンボリック実行の実行結果

また、ファジングの性能を比較するための標準的な手法が存在せず、論文どうしの比較によるファジングの性能比較は困難な状況であるが、米メリーランド大学の研究者らからは、性能比較の際は、複数回試行し統計的分析を行うこと、既知のバグが含まれたベンチマークプログラムを用いること、最低 24 時間は実行すること等が提案されている[123] 。

6.3.2.2.10 その他の研究動向

- 参考）テスト入力値生成技術の研究動向[124]

学術的には、この 10 年（2006-2016 年）のソフトウェア工学及びソフトウェアテスト分野における主要会議（ICSE, FSE, ASE, ISSTA, ICST）における発表論文の調査に基づくと、テスト入力値生成の目的は大きく「ソフトウェア構造の網羅を目指す」、「バグをピンポイントで検出する」、「入力空間を効果的に狭める」、「その他」の四つに分かれ、そのうち「ソフトウェア構造の網羅を目指す」の研究が盛んである。

目的別に分類を行うと、この 10 年の研究は「ソフトウェア構造の網羅を目指す」が 46%、「バグをピンポイントで検出する」が 24%、「入力空間を効果的に狭める」が 16%、「その他」が 14%となっている。コードの網羅率向上の研究が盛んである背景として、新たな研究アプローチ（DSE[125] や FDRT[126]）が確立されたことにより、実践的に研究を行うことが可能になったことによると推測されている（図 6-5）。

[123] George Klees, Andrew Ruef, Shiyi Wei, Michael Hicks (2018). “Evaluating Fuzz Testing”, ACM Conference on Computer and Communications Security (CCS) 2018

[124] 丹野治門、倉林利行、張暁晶、伊山宗吉、安達悠、岩田真治、切貫弘之（2017）「テスト入力値生成技術の研究動向」

[125] DSE: Dynamic symbolic execution（動的シンボリック実行）

[126] FDRT: Feedback-Directed Random Testing

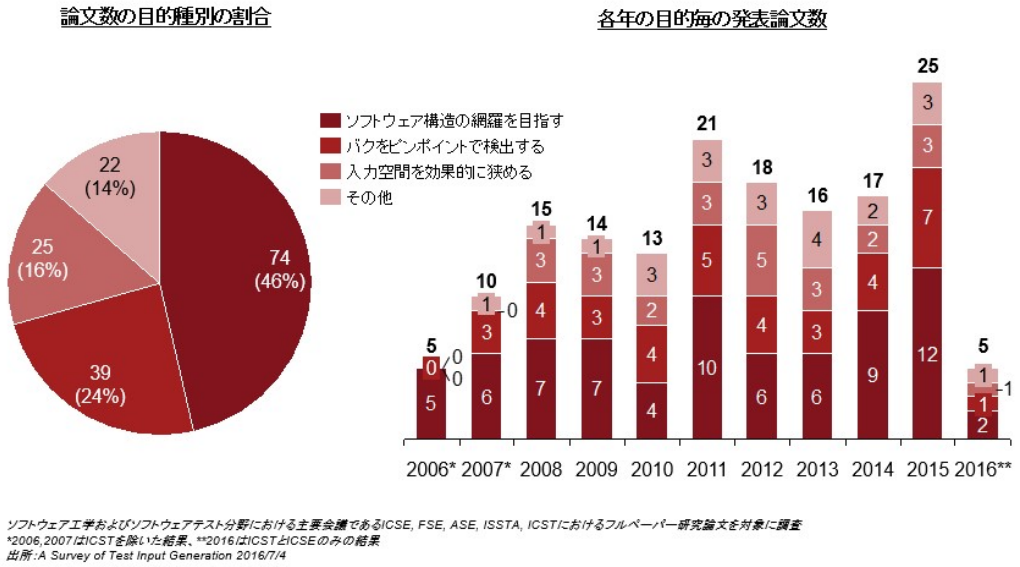


図 6-5　論文数の目的種別の割合、各年の目的毎の発表論文数

なお、上記目的種別の定義は以下の通りである。

「ソフトウェア構造の網羅を目指す」ものには、コード上の網羅率を指標としたコード網羅率の向上を目的とするものと、何らかのモデル上の網羅率を基準としたモデル網羅率の向上を目的とするものがある。

「バグをピンポイントで検出する」は、特定のバグをピンポイントで検出することを目的としている。バグ検出には、大きく分けて機能性バグ検出、性能バグ検出、セキュリティバグ検出、並行バグ検出がある。

「入力空間を効果的に狭める」は、効果を維持しながら、テスト入力値がとりうる入力空間を効果的に絞り込むことを目的とする。

「その他」は、上記に当てはまらなかったもので、改造による影響範囲のテスト、テスト入力値生成の高速化、テスト入力値の匿名化、適合性テスト、テスト入力値の可読性向上という五つがある。

6.3.2.2.11 まとめと今後の展望

ファジングは、必ずしもソースコードを必要とせず、問題を起こしそうなデータを入力し動作状態を確認することで脆弱性を発見できる手法である。ただし、どの程度のパスを検査できたかがわからず、既存の商用ツールでも製品性能の記載はあいまいで、どれだけのパスや脆弱性をカバーできるかを明示できていないのが現状である。

課題としては、何を入力データとすればよいかが不明確であることや、どこまで検査をすれば十分かが不明確であること、プログラム上正しく動作する不正コードをどう検出するか等が挙げられる。

何を入力データとすればよいか、どこまで検査すれば十分かという課題を解決するために、効率性向上や網羅性向上のための研究が行われている。効率性向上の研究では、Google のエンジニアが開発した、遺伝的アルゴリズムを活用した AFL（6.3.2.2.5　項参照）をベースに、複数国の研究者チーム（6.3.2.2.6　項参照）や Microsoft（6.3.2.2.7　項参照）により、拡張のための研究が行われている。網羅性向上のためにはシンボリック実行を活用した研究が進められており、UCSB の研究チームにより、シンボリック実行を活用したファジングツールである angr が発表されている（6.3.2.2.8　項参照）。

遺伝的アルゴリズムに関しては、交叉確率・方法や突然変異確率・方法が性能に影響を与え、これらを適切に設定して効率性を向上させることが今後の研究課題となっている。シン

ボリック実行に関しては、パス数の爆発、適切なソルバ開発、適切な入力値の特定等の課題を解決し、高速化を図ることが研究課題となっている。実務的には、これらの欠点を補い合うために、遺伝的アルゴリズムとシンボリック実行を組み合わせた Driller が考案（6.3.2.2.9 項参照）されており、何をどこまでやればよいかという課題を解決しようとしている。また、不正コードの検出に関しても引き続き課題として残っており、実務的には運用中に発見するしかないのが実情である。

6.3.2.3 ソースコード解析

6.3.2.3.1 ソースコード解析の課題と対応

ソースコード解析における脆弱性の発見難易度は大きく三つに分類できる。

ソースコードを見て一定の知見があれば誰でもわかるようなタイプの脆弱性であればツールでも容易に発見できる。

一方で、一見すると問題はないように見えるが実際に動作をさせると問題が起きる（例: 無限ループが起きてしまう等）コードに関しては、ツールでは必ずしもチェックしきることができないという課題がある。

さらには、プログラムとしては正常に動作するが意図しない通信を行う等の不正なコードに関しては、より発見が困難だという問題がある。

二つ目、三つ目に関しては人的にカバーしているのが現状である。これに対して、いかに人的部分を自動化するかといった研究が行われている。一方、自動化によりすべてのパスを確認し判断できるようになればよいが、それでも膨大な時間がかかるため、現実的な解としては、前述の通り動的解析との組み合わせによって脆弱性・不正検出が行われる。特に、不正な通信を発見する等の、ある特定条件において特定の挙動を示すようなものは仕様のミスなのかどうかも含めて判断がつかないため、実際に動作をさせる必要があると推測される。

6.3.2.3.2 代表的な製品

ソースコード解析の代表的な製品としては、Synopsys の Coverity や GrammaTech[127] の CodeSonar 等が存在する。

各社の製品ページではたいてい、OWASP[128] Top 10 や CWE [129]/SANS[130] Top 25 等の重大な脆弱性に対応していることを示しており、この点において差別化はないように見受けられる。

製品によっては CWE のカバーも詳細化しており、例えば JAVA では、Synopsys の Coverity では 123 種類、GrammaTech の CodeSonar では 96 種類、Parasoft[131] の Jtest では 208 種類をカバーしている。なお、CWE は 2018 年 3 月時点では 1,039 種類が定義されている。

---

[127] 1988 年に米コーネル大学からスピンオフして米国で設立された、ソフトウェア開発ツールベンダー。
[128] The Open Web Application Security Project：Web アプリケーションセキュリティをとりまく課題を解決することを目的とする、国際的なオープンなコミュニティ。
[129] Common Weakness Enumeration：共通脆弱性タイプ一覧。脆弱性のパターンを定義したもの。
[130] SANS (SysAdmin, Audit, Network, Security) Institute：政府や企業・団体間における研究、及びそれらに所属する人々の IT セキュリティ教育を目的として 1989 年に設立された組織。
[131] 1987 年に米国で設立された、自動ソフトウェアテストとアプリケーションセキュリティに特化したソフトウェアベンダ。

6.3.2.3.3 AI 自動化の製品①: Microsoft[132]

Microsoft は、2018 年 5 月に米国シアトルで開催したイベント「Microsoft Build 2018」で、AI を用いてプログラマの開発を支援する「Visual Studio IntelliCode」を発表した。

IntelliCode では既存のソースコードを AI に学習させることで、コンテキストに対応したコード補完、コーディングのパターンやスタイルを遵守するためのガイドの提供、バグ等の問題の発見等の機能を提供する。

6.3.2.3.4 AI 自動化の製品②: マサチューセッツ工科大学(MIT)[133]

MIT の研究者により、機械学習を用いたバグ修正アルゴリズムが開発された。

従来の一般的なバグ修正手法では、修正したいソースコードに対する正解セット（入力値とそれに対する正しい出力値）をいくつか用意し、その正解セットに合致するような修正提案をシステムが探し出すもので、計算時間が長かったり、正解セット以外の入力値に対しては正しい出力値を得られなかったりといった問題が存在した。MIT の研究者により開発された手法では、オープンソースプログラムの修正パッチを学習データとして汎用的な規則を抽出することで、従来手法よりも高い成果が得られた。

6.3.2.3.5 AI 自動化の製品③: DeepCode[134]

DeepCode は、既存のコードを AI に学習させることで、作成中のコードの問題点と修復方法が提示されるようになっている。

企業としての DeepCode はスイスのチューリッヒ工科大学から独立した研究プロジェクトがスピンオフして設立され、プログラミング用ツールとして製品が開発された。製品の DeepCode は公開されている大量のソースコードを読み込むことでルールを学習し、ユーザーに対して、より良いプログラムとなるようにコードを提案する。

6.3.2.3.6 AI 自動化の製品④[135]: 富士通[136]

富士通は 2017 年 11 月より、社内のシステム開発プロジェクトにおいて「ソース診断」を活用している。

ソース診断においては、英数字や記号といった文字列の塊であるソースコードを画像データとして AI で分析し、可読性を診断する。可読性が低い箇所をソース診断によりあたりをつけ、該当箇所を集中的にエンジニアがレビューする体制とすることで、レビュアーの作業効率化と精緻化が見込める。

---

[132] @IT: IntelliCode：AI を利用した効率的なコーディングを実現？
http://www.atmarkit.co.jp/ait/articles/1805/15/news029.html

[133] MIT News: Recognizing correct code
http://news.mit.edu/2016/faster-automatic-bug-repair-code-errors-0129

[134] TechCrunch: DeepCode は AI の力でコードを洗う…未来のフロントエンドはプログラミングの自動化
https://jp.techcrunch.com/2018/04/27/2018-04-26-deepcode-cleans-your-code-with-the-power-of-ai/

[135] 日経 xTECH: ソースコードの不備を AI で見つける富士通、新しい診断ツールの中身
https://tech.nikkeibp.co.jp/it/atcl/column/14/346926/122501258/

[136] 1935 年に設立された、日本の総合エレクトロニクスメーカ・IT ベンダー。

6.3.2.3.7 コード解析関連研究事例①: CFG の共有構造割合を基にしたマルウェア検出(信州大学)

信州大学の研究者により 2013 年の情報処理学会で発表[137] された、CFG（制御フローグラフ: Control Flow Graph）の共有構造割合から Android のマルウェアを検出するための手法である。

本研究では、アプリケーションのメソッドごとに制御フロー解析を行ってグラフを生成しており、その際、アプリケーションの動作に関係のないメソッドについては対応するノードを削除することでグラフを簡略化している。マルウェア検体から生成されたグラフのうち、マルウェアの動作に必要とされるメソッドのグラフを、そのマルウェアの定義ファイルとしている。検査するアプリのグラフと定義ファイルのグラフで一致したノード数と、定義ファイルのグラフのノード数との割合を包含度とし、この値が、別途サンプルファイルの計算から得られた閾値を超えるかどうかで、検査対象のアプリがマルウェアを含んでいるかを判定している。

本研究で提案している手法だけでは検出漏れが生じており、複数の手法を組み合わせる等して精度を向上させることが課題として述べられている。

6.3.2.3.8 コード解析関連研究事例②: CFG の構造の近さを基にしたマルウェア解析の効率化（情報セキュリティ大学院大学）

情報セキュリティ大学院大学の研究者により、2016 年に「マルチメディア、分散、協調とモバイル（DICOMO 2016）シンポジウム」で発表[138] された、CFG を用いてマルウェアの解析を効率化するための手法である。

ソフトウェア中の関数で、悪意のある挙動を示しうる関数を絞り込むことがマルウェア解析では重要となっている。本研究では、検査対象のグラフとマルウェアに含まれる関数のグラフで、両者の編集距離を類似度とし、検査グラフ内の関数を類似度が高い順に並べて示すことで、より詳細な分析が必要な関数の優先順位付けを行う BinGrep を提案している。なお、編集距離は、ノードの追加や削除でグラフを編集する場合のグラフ間の最小の編集数で定義される。

コードの類似度比較のために従来用いられているツールとしては、Google が 2011 年に買収したドイツのセキュリティベンダーである zynamics 社が提供している BinDiff が存在する。BinDiff ではグラフ特徴量のユークリッド距離をベースに、関数の 1 対 1 対応により類似点・相違点を検出している。

本研究では、BinGrep と BinDiff とで、バージョンアップ前後のプログラムで 381 個の関数を対象に性能の比較を行っている。精度の結果は

表 6-1 の通りで、BinGrep 単体では必ずしも精度は向上していない。一方で、BinDiff では不正解であったが BinGrep では正解であったものもあることから、両手法を組み合わせることで精度が向上する可能性があると考えられる。また、実行時間は BinDiff が全部で 3.7 秒であったのに対し、BinGrep は関数一つあたり平均 3.48 秒（全部で約 22 分）と、計算時間が長くなっている。

表 6-1　BinGrep と BinDiff の精度比較結果

	BinDiff		合計
	正解	不正解	

[137] 岩本一樹、和﨑克己（2013）「制御フロー解析により生成されたグラフ比較による Android マルウェア検出方法の提案」、情報処理学会研究報告、Vol. 2013-CSEC-61 No.5、Vol. 2013-IOT-21 No.5

[138] 羽田大樹、後藤厚宏（2016）「制御フローグラフの比較を用いた関数の検索によるマルウェア解析の効率化の提案」、『マルチメディア、分散、協調とモバイル（DICOMO 2016）シンポジウム』

BinGrep	正解	314	29	343
	不正解	31	7	38
合計		345	36	381

6.3.2.3.9 その他の研究[139]

機械学習を用いることで、プログラミング言語で書かれたコードから個人の識別が可能であるという研究結果が発表された。

研究は、米国ドレクセル大学でコンピューターサイエンスの准教授を務める Rachel Greenstadt 氏と、米国ジョージワ・シントン大学でコンピューターサイエンスの准教授を務める Aylin Caliskan 氏によるものである。非常に短いコードの断片や、機械語にコンパイルされたコードからでも個人の識別が可能とされている。

Caliskan 氏らの研究チームは、Google が開催するプログラミングコンテストの Google Code Jam で書かれたコードを基に精度を実験。識別する開発者を 100 人とした場合は 96%の精度で個人を識別でき、識別する開発者数を 600 人に拡大した場合でも 83%の精度で個人を識別できたとしている。同手法はマルウェアの開発者を特定する時等に役立つとしている。

6.3.2.3.10 まとめと今後の展望

ソースコード解析は、自社開発の場合と他社開発の場合とで異なる。自社開発の場合は問題にならないが、他社開発の場合は、ソースコード解析を実施するためには、ソースコードが納入されており、コード解析が契約上禁止されていない必要がある。

ソースコード解析の手法としては、特定のコーディングパターン（ルール）の違反箇所を指摘するコーディングスタンダード解析と、実行パスをシミュレートし、処理フローや渡された値によって発生する問題点を特定するフロー解析とが存在する。

コーディングスタンダード解析は、製品上は IDE（統合開発環境: Integrated Development Environment）に含まれている場合が多く、自社開発の場合はコード実装中に同解析を実施できるが、コードの実行順序やパスに起因するようなフローに関する問題は検出ができないという課題があるため、その課題に対処するためにフロー解析が行われる。また、他社開発コードに対しては主にフロー解析を実施することになる。フロー解析では現状、既存の有償製品では OWASP Top 10 や CWE/SANS Top 25 等の重要な脆弱性はカバーできている。

一方、誤検出があるため最終目視確認が必要なことや、検出漏れもある可能性があることが課題となっている。また、未知な構造の脆弱性・不正をどのようにして検出するかという課題も存在する。

フロー解析の課題に対応するために、ソースコードの特徴を捉えやすくするモデル化の研究や、検査対象コードと脆弱性コードの構造の近さを定義する計算手法を検討する、類似度比較の研究が存在する。類似度比較に関する研究では岩本らの研究（6.3.2.3.7　項参照）や羽田らの研究（6.3.2.3.8　項参照）が存在する。また、岩本らの研究では効率的なモデル化についても手法に組み込まれている。

羽田らの研究では提案手法と既存手法とで精度・計算時間を比較しているが、必ずしも精度が向上したとは言えず、計算時間も長くなっている。類似度比較においては、引き続き、精度向上と高速化が今後の研究課題となっている。また、未知な構造の脆弱性・不正検出に関しては、現実的には動的解析と静的解析を組み合わせた手法が検討されている。

---

[139] GIGAZINE: 機械学習を用いると匿名のソースコードから個人を識別可能であることが判明
https://gigazine.net/news/20180813-machine-learning-identify-code-authors/

6.3.2.4 組み合わせた手法: IAST

6.3.2.4.1 IAST 概要

静的・動的解析のハイブリッドという位置付けで IAST (Interactive Application Security Testing) という概念が存在する。静的解析と動的解析を組み合わせた解析は一般に行われてはいるため、新たな技術というよりは、カテゴリの切り方や見せ方を変えた、一種のマーケティング手法としての意味合いのある概念でもある。

動的解析のファジングに関して言えば、どのような効率化を行っても、必要十分を示すことは相当困難である。ソースコード解析を行えば理論上は完全な解析を行うことができるものの、一見すると問題がないように見えるが実際に動作をさせると問題が生じるコード（無限ループが生じる等）は必ずしもチェックしきることができず、さらに、プログラムとしては正常に動作するが意図しない通信を行う等の不正コードに関してはより発見がしにくいという問題がある。さらには、それが不正か仕様により起きていたのかを判断することはなおさら困難である。

動的解析、静的解析はどこまでいっても単体だけでは問題が残り続ける可能性があるため、脆弱性・不正の発見のためには、動的解析や静的解析の技術をそれぞれで向上させるよりは、動的に動かして怪しい部分を見つけた上で、ソースコードを解析するというハイブリッド型の IAST の活用が現実的と考えられる。

6.3.2.4.2 IAST 製品

例えば Contrast Security[140]の Contrast Assess[141]や、Micro Focus[142]の Fortify On Demand[143]等が存在する。

Contrast Assess はソフトウェアの脆弱性検査を行うセキュリティテストソリューションで、IAST の脆弱性検査機能を提供している。アプリケーションサーバーに検査用のエージェントを組み込み、アプリケーションの挙動を監視しながら脆弱性の検出を行う。また、アプリケーションで利用している OSS 等、サードパーティコンポーネントの種類やバージョンを識別でき、脆弱性情報データベースと組み合わせることで、利用中のコンポーネントの既知の脆弱性を自動的に検出することが可能となっている。

Fortify On Demand は IAST を実践できるクラウドベースの脆弱性検査サービスである。Web アプリにエージェントを導入すれば、クラウド側でセキュリティ検査が実行される。見つかった脆弱性は Web 上のダッシュボードで確認でき、アプリケーションのどこに、どの程度深刻な脆弱性があるかが一目で把握できるようになっている。

---

[140] 2014 年に米国で設立された、サイバー攻撃からアプリケーションを守るセキュリティ技術のプロバイダー。

[141] Contrast Security: Interactive Application Security Testing (IAST) Solution
https://www.contrastsecurity.com/interactive-application-security-testing-iast

[142] 1976 年に英国で設立された、COBOL 言語の開発ツールを中心としたソフトウェア会社。2016 年に Hewlett Packard Enterprise のソフトウェア部門と合併し、世界最大級のソフトウェア会社となった。

[143] Micro Focus: Fortify on Demand
https://www.microfocus.com/ja-jp/products/application-security-testing/overview

6.3.2.5 事後的防御技術: RASP

6.3.2.5.1 RASP 概要

静的・動的解析を行っても結局は事前に検知し防御することは不可能という、アンチウイルス等と同じ思想で、事後的に防ぐ RASP (Runtime Application Self-Protection) という製品も存在しており、今後市場が成長していく可能性があると予測する調査会社も存在する。

6.3.2.5.2 RASP 製品

例えば Contrast Security[144] の Contrast Protect や Micro Focus の Application Defender[145]等が存在する。

Contrast Protect は稼働中の Web アプリケーションへの攻撃をリアルタイムに検知し、自己防御する機能を提供する。アプリケーションサーバーで監視用エージェントを稼働させ、アプリケーションレベルで不正アクセスをブロックすることで、脆弱性を修正する前に自動的にアプリケーションの保護を行うことができる。

Application Defender は、クラウド管理のアプリケーション自己保護サービスで、アプリケーションを監視し、攻撃を可視化することや、アプリケーションの動作を変更してアプリケーションを防御することが可能となっている。

6.3.2.5.3 その他の会社

その他にも、IBM[146]、Veracode[ix]、WhiteHat Security[147] 、Synopsys が取り扱っている。

リサーチ会社である Transparency Market Research の公表している内容によると、2016 年の RASP の市場規模は 2 億 5,000 万米ドルだが、CAGR 32.4%で成長し、2025 年には 31 億 3,000 万米ドルに達する見込みとのことである[x]。

6.4 ハードウェア検査技術

6.4.1 ハードウェアの不正検知事例

ハードウェアの不正検知事例として挙げられる 2 件の事例のうち、1 件は政府からケンブリッジ大学と研究機関が依頼され請け負ったもので、もう 1 件は個人が見つけたものである。さらに、疑惑があったが否定されたものが 1 件あった。

---

144 Contrast Security: Runtime Application Self-Protecting (RASP) Solution
https://www.contrastsecurity.com/runtime-application-self-protection-rasp

145 Micro Focus: Application Defender
https://www.microfocus.com/ja-jp/products/application-defender/overview

146 1911 年に米国で設立された、民間・公的機関を対象にコンピュータ関連製品及びサービスを提供する企業。

147 2001 年に米国で設立されたセキュリティ技術提供企業。静的解析、動的解析、モバイルアプリケーションセキュリティテスト等を提供している。

6.4.1.1 不正検知の実情

バックドアに代表される不正を検知することは、現状ではほぼできておらず、大半の脆弱性・不正は上市後に発見されていると言われる。例えば防衛省の備品や自動車のような重大なモノに関してもチェックが行われていない状況である。

防衛省においては、所持している武器が現場できちんと動作する保証があるとは言えないという認識を持っていると言われている。米国のサプライチェーン対応、NIST SP800-171 の対応や日本版のセキュリティクリアランスが提言されているが、具体化は今後の課題である。

また、自動運転に注力をしている自動車メーカーでも開発段階で網羅的に脆弱性等を排除できているわけではない。「米スパイレントのサミール・ディクシ氏は 2 年前の会議を今でも忘れない。ある自動車メーカーの経営陣との話し合いを終え、部屋を出ると同僚と顔を見合わせた。『あのクルマは絶対に買わない』。ディクシ氏らは自動車メーカーからの依頼を受けて、開発中のクルマを検査した。クルマにはスマートフォンのアプリと連携する機能が付いており、ヘッドライトやエアコン等を操作できる。このシステムに欠陥が見つかり、第三者が遠隔から走行中のクルマの速度を変更できることがわかった。一歩間違えれば重大事故につながる。だが欠陥を報告しても、メーカーはそのままクルマの発売を強行した。発売日が迫っており、システム改修が間に合わないというのが理由だった。ディクシ氏らは悪意あるハッカーが欠陥を発見しないことを願うほかなかった。」（日経ビジネス　2018/9/10 号より抜粋）

なお、上市後に脆弱性を発見しているのは、主に技術力をアピールするためのセキュリティ会社や、バグバウンティ、つまり賞金目的のホワイトハッカー等であることがよく知られている。

以下には、公開されている不正発見の情報として、ハードウェアの不正事例を 2 件（及び疑惑があったが否定されたものが 1 件）、ソフトウェアの事例を 8 件、また研究機関として不正発見に関わる可能性がある組織についても言及する。

6.4.1.2 事例①: 米軍事用チップのバックドアの発見[148]（2012 年、Sergei Skorobogatov 氏・Quo Vadis Labs）

6.4.1.2.1 概要

2012 年、ケンブリッジ大学コンピュータ研究所の Sergei Skorobogatov 上級研究教授は、MI5（英国情報局保安部）や NSA（米国国家安全保障局: National Security Agency）、IARPA（諜報先端研究プロジェクト活動: Intelligence Advanced Research Projects Activity）等からシリコンチップの危険性についての情報を受けて調査を行い、バックドアを発見した。

調査は軍事用に用いられているシリコンチップの暗号解読を行い、チップ内に未知の機能が存在するかどうかを調べることを目的として行われた。調査対象は米国が軍事用途で用いているチップで、高度な暗号化がなされた中国製のものだった。Skorobogatov 教授は Quo Vadis Labs（英国）と協働して調査を実施した結果バックドアを発見した。

発見されたバックドアを用いると、チップを使用不可能にしたり、再プログラムしたりすることが可能な状態であった。このチップは武器関係の多くのシステムで普及しているほか原子力発電所や公共交通機関でも使用されているもので、今回見つかったバックドアを使えば、数百万もの兵器に対して攻撃を仕掛けることが可能なものだった。また、同バックドアはファームウェアではなくチップ自体に埋め込まれていた。

ただし、米国のあるセキュリティコンサルタントは、Skorobogotov 教授が発見した侵入

[148] Nextgov: UK researchers discover backdoor in American military chip
https://www.nextgov.com/cio-briefing/2012/05/uk-researchers-discover-backdoor-american-military-chip/55949/

経路は、メーカーが故意にインストールしたデバッグツールである可能性が高いと主張している。

6.4.1.2.2 発見者プロファイル①: Sergei Skorobogatov[149]氏（ケンブリッジ大学）

- キャリアサマリー

2005 年にケンブリッジ大学のコンピューターサイエンス学科で博士号を取得した。現在はケンブリッジ大学コンピュータ研究所のセキュリティグループの上級研究教授である。

2000 年にケンブリッジ大学での研究を開始する前は、視力検査や矯正で使うための様々な電子デバイスを設計する企業に勤務していた。研究や企業勤務の経験から、エレクトロニクス、化学、コンピューターサイエンス、物理学等の知識を有す。

- 研究

研究分野にはハードウェアセキュリティ、組み込みメモリのセキュリティ、スマートカード、半導体故障解析、フォレンジック分析等を含む。

ハードウェアセキュリティでは攻撃技術や耐タンパープロセッサの研究に取り組んでおり、脆弱性の発見や隠れた機能、バックドア等をシリコンチップから検出することを目指している。

6.4.1.2.3 発見者プロファイル②: Quo Vadis Labs[150]

- 企業概要

コミュニケーション・電子システムにおける脆弱性を発見し、対処するためのソリューションを開発することを企業の目的としている。少数の専門的な科学者、エンジニアのチームで構成されており、暗号解析、高周波システム、半導体、ネットワークセキュリティの専門家等が含まれる。

- 設立背景

ケンブリッジ大学コンピュータ研究所との長期パートナーシップを基にした研究プロジェクトを背景に、2008 年に設立された。

6.4.1.3 事例②: プロセッサのバックドアの発見[151]（2018 年、Christopher Domas 氏）

6.4.1.3.1 概要

GitHub で活動する Christopher Domas 氏が、かつて VIA Technologies（台湾）が開発した C3 プロセッサにバックドア「rosenbridge」が存在することを発見し、2018 年 8 月に開催の「Black hat USA 2018」で報告した。

同氏によると、rosenbridge は CPU が管理するすべてのメモリだけでなく、レジスタファイルと実行ラインにもアクセスできるという、かなり深いレベルに組み込まれたコプロセッサとなっている。

なお、C3 は 2001 年に発表/販売されたプロセッサであり、低価格/低発熱等で広く受け入

149 University of Cambridge: Dr Sergei Skorobogatov
https://www.cl.cam.ac.uk/~sps32/
150 Quo Vadis Labs: http://www.quovadislabs.com/
151 PC Watch: 17 年前の「VIA C3」プロセッサにバックドアが見つかる
https://pc.watch.impress.co.jp/docs/news/1137913.html

れられ、特に組み込み機器での採用実績が多い。

6.4.1.3.2 発見者プロファイル: Christopher Domas[152]氏

- キャリアサマリー

2009 年から 2018 年までの 9 年間、バテル記念研究所（米国）に勤務、サイバーセキュリティリサーチリーダーを務めた。バテル記念研究所は鉄鋼業で巨額の富を築いた Gordon Battelle 氏の遺産を基に 1929 年に設立され、米政府や企業からの受託研究と米英の国立研究所の運営受託を中心に活動し、原子力等のエネルギー、バイオ・先端材料、医療機器、防御システム等幅広い分野の研究を行っている。Domas 氏は、同研究所では x86、ARM、リバースエンジニアリング、脆弱性分析、ファジング、組み込み装置等にフォーカスして研究を行っていた。

2014 年からはオハイオ州立大学の非常勤講師を務め、C 言語、アセンブリー、システムアーキテクチャ等を担当した。

2018 年からは Intel（米国）のプリンシパルセキュリティリサーチャーとして勤務している。

6.4.1.4 参考事例: 中国製スパイチップ疑惑[xi]（2018 年）

Bloomberg Businessweek は、2018 年 10 月、Super Micro Computer（米国）のサーバー用マザーボードに、中国製スパイチップが埋め込まれていたと報道した。マザーボードに埋め込まれたスパイチップは微小で、バックドアの機能があった。スパイチップは Super Micro の中国工場で埋め込まれたといい、中国人民解放軍の関与が疑われており、Amazon や Apple 等、約 30 社の米国企業が被害を受けたという。Apple は 2015 年、Super Micro 製サーバーから「スパイチップ」を発見し、同社との取引を停止したとされる。

ただし、Super Micro、Amazon、Apple いずれも報道内容を否定するコメントを発表している。情報源は、（現在・元）国家安全保障関係者 6 人、Apple の内部関係者 3 人、元 Super Micro 従業員 6 人等とされているが、いずれも匿名の情報提供者であり、情報の真偽を確認するための外部からの検証が不可能な状態となっていた。

Super Micro はサードパーティの調査会社 Nardello & Co.に調査を依頼したが、同年 12 月、Nardello により、Super Micro のマザーボード上に悪質なハードウェアが存在する証拠はないと結論された。一連の騒動に結論が出たかたちだが、その被害は大きく、最初の記事が出た直後には Super Micro の株が 41%あまりも下落した。

6.4.1.5 その他事例: MEMS センサの物理的脆弱性の実証[153]（2017 年、Alibaba[154] ）

2017 年 7 月下旬に開催されたセキュリティカンファレンス「Black Hat 2017」で、中国アリババ集団のセキュリティ部門「アリババセキュリティ」の研究者は、多種多様な機器において、MEMS センサの脆弱性が攻撃されうると発表した。

MEMS（微小電子機械システム: Micro Electro Mechanical Systems）は、機械要素部品、センサ、アクチュエータ、電子回路を一つのシリコン基板、ガラス基板、有機材料等の上に微細加工技術によって集積化したデバイスのことである。

---

[152] Christopher Domas: https://www.linkedin.com/in/christopher-domas-39b3a5102/

[153] 日経 xTECH: ドローンや VR 機器は超音波に弱い、中国アリババの研究者が実証 https://tech.nikkeibp.co.jp/it/atcl/column/15/061500148/082100122/

[154] 1999 年に Jack Ma 氏により設立された中国の大手 IT 企業。電子商取引サイト、検索サイト、電子マネー等のサービスを提供している。

同センサは、ドローンやVRヘッドセット、スマートフォン等に、姿勢検出や位置推定のために搭載されている。超音波を加速度や角速度と誤って検出してしまい、外部から測定結果が操作可能となる物理的な脆弱性が存在しており、そのことは韓国科学技術院やミシガン大学の研究者らにより示されていたが、今回の発表により、実際に多種多様な機器で操作可能であることが示された。

6.4.2 ハードウェア検査技術を使用したサービス

6.4.2.1 ファームウェア解析

監視カメラやスマートスピーカー、重要インフラ・医療現場・工場等で利用されるセンサ等 IoT 機器は様々なシーンで利用されるようになっている。この IoT 機器の脆弱性を診断することは、ソフトウェアを対象とするものに比べサービスが少ない状況にある。

その中にあって、IoT 機器に組み込まれるファームウェアを解析し、セキュリティレポートを生成するサービスが出てきている。

現在サービスとして提供されているものは、クラウド上にサーバーがあり、ファームウェアをアップロードするとセキュリティレポートが生成されダウンロードできる仕組みとなっている。

このファームウェアはソースコードが不要であり、バイナリ形式で行うことが可能である。

6.4.2.1.1 イスラエル VDOO[155]

VDOO は、IoT セキュリティ自動化の先駆者として、組み込みシステムセキュリティとエンドポイントセキュリティの分野で膨大な知識を持つ起業家と、トップのサイバーセキュリティ研究者と開発者によって 2017 年に設立された。

2019 年 4 月より IoT セキュリティ自動診断ソリューション「VDOO Vision」が日本国内で提供開始予定となっている[xii]。

- サービス名: Vision[156]

IoT デバイスを保護するには、各デバイスとその属性に関する独自のノウハウと、サードパーティ製コンポーネントへの可視性が必要である。セキュリティアーキテクチャを改善するための自動分析アプローチとして以下を提供している。

①ファームウェアバイナリファイルのアップロード
Vision がファームウェアからデバイス属性を自動的に抽出。
②自動脅威分析
Vision がデバイス固有の脅威を計算し、その固有のセキュリティ概要を作成。
③セキュリティギャップ分析
Vision が具体的なセキュリティギャップを特定し、段階的な緩和と強化のガイダンスを提供。
④ファームウェアの再分析
Vision は必要なセキュリティ要件が満たされており、デバイスが CertIoT（VDOO の IoT デバイス認証プログラム）に対応していることを確認。

---

155 VDOO: VDOO for Connected Devices Makers
https://www.vdoo.com/iot-security-platform-for-makers/
156 VDOO: Vision™
https://www.vdoo.com/security-architecture-automation/

6.4.2.1.2 米国 refirm labs[157]

2017 年に元 NSA の職員等により設立され、Red Team で磨いた攻撃ノウハウを基礎としてサイバー攻撃に関する豊富な知識と経験を有している。RSA の 2018 年トップ 10 イノベーターファイナリストの一つに選ばれた。

株式会社ソリトンシステムズ[158]は、refirm Labs と提携し、IoT ファームウェア脆弱性調査を 2019 年 1 月より開始し、そのプラットフォーム「Centrifuge（セントリフュージ)」を提供している。そのため、日本でも活用可能となっている。

- ツール名: Certrifuge[159]

ファームウェアのバイナリファイルを Centrifuge プラットフォームにドラッグ&ドロップするだけで、簡単に脆弱性の診断を行うことができる。ソースコードは不要である。

サポート OS は Linux、QNX、Android で、今後は UEFI (Unified Extensible Firmware Interface) や VxWorks 等への対応も予定している。

6.4.2.1.3 まとめ

ファームウェアをアップロードするため情報漏洩・不正利用の懸念があるが、ソースコード不要で実施できることはメリットとなる。

ただし、ファームウェアが暗号化・難読化している場合には、内容をチェックすることができないと想定されるため、開発ベンダーでの利用になると推測される。

6.4.3 ハードウェア検査技術の研究動向

6.4.3.1 研究動向概要

ハードウェア（チップ）における脆弱性は主に各チップメーカーが自社で検証を行っていると推測される。外部が分析し、発見した事例としては、Google のセキュリティ分析チームによる発見が見受けられた。

不正なチップや回路の検出に関しては、真正性をどのように定義するか、真正性が認められたものを基にどのように不正を検出するかという二段階が考えられるが、真正性の定義に関する目立った研究は見受けられなかった。

真正なものを基にした不正チップ・回路の検出に関しては、物理的に違いを見つける方法として回路画像を比較する研究や、半導体の特徴である電気特性を利用した研究が行われている。なお、上記は、設計図を基にしたケースと、正常（と思われる）チップを真正とし、研究されていた。

また、設計図を基にファウンドリ（Foundry）が作成したチップを動的に変更するカモフラージュ技術も研究されているため、真正性を定義することは現実的にはかなり困難になると想定される。多数の購買品の中から差分を見つける等の横比較で異物を見つける等の

---

157 ReFirm Labs: https://www.refirmlabs.com/

158 Soliton Systems: IoT ファームウェアの脆弱性調査を開始 - サプライチェーンのセキュリティ対策の判定にも有効、ソースコード不要 -
https://www.soliton.co.jp/news/2019/003472.html

159 Soliton Systems: IoT 機器で動作するファームウェアの脆弱性を自動解析
https://www.soliton.co.jp/products/category/product/cyber/refirm/

方法を用いることしか一般的な企業では対応できない可能性が出てきている。

6.4.3.2 事例①: プロセッサの脆弱性の発見[160](Google[161])

Google のセキュリティ分析チームである Project Zero は 2018 年 1 月、Intel、AMD、ARM 等の多くの CPU に使われている、性能を最適化するための「投機的実行」機能に欠陥があり、深刻な脆弱性が存在すると発表した。

投機的実行はコンピュータの処理を高速化する手法の一つである。条件分岐命令が含まれる場合に、どちらに分岐するのかを予測（分岐予測）し、予測先の命令を先行してパイプラインに投入して実行し始めてしまうものだが、予測が当たれば分岐先の確定を待つより高速に処理を継続できるが、外れた場合は実行途中の命令を破棄して正しい分岐先の命令の実行をやり直すことになる。外れても確定を待つのと同じであるため、投機的実行をしないよりは全体として高速になる。

Project Zero の研究員である Jann Horn 氏によると、悪意のある攻撃者は CPU の投機的実行を利用することで、本来アクセス権限のないソフトウェアでアクセスできないはずのシステムメモリを読み取ることができ、パスワードや暗号化キー、アプリケーションで開いている機密情報にアクセス可能になるという。

Intel は、2018 年 10 月に、脆弱性に対処するためにハードウェアレベルで修正を施した新プロセッサを発表した。

6.4.3.3 事例②: AI･X 線を用いたスパイチップ検出システム[162](フロリダ州サイバーセキュリティ研究所[163])

フロリダ州サイバーセキュリティ研究所のディレクターである Mark Tehranipoor 氏は、X 線や光学イメージング、AI 等を組み合わせてマザーボード内に埋め込まれたスパイチップを発見するというシステムを開発している。システムは半自動化されており、プリント回路基板やチップの構成要素を元の設計図と比較し、スパイチップのような「本来の設計にはないもの」を発見する。

プロセスは、回路基板の表と裏の超高解像度写真を撮るところから始まる。機械学習及び AI アルゴリズムを用いたシステムが写真上の回路を認識し、構成要素がどのようにつながっているかを識別、続いて X 線マイクロトモグラフィを用いることで回路基板を断層撮影する。Tehranipoor 氏らの研究チームが開発したシステムは、撮影した複数の 2D 画像を取り込み、それらを自動的につなぎ合わせることでレイヤーごとに分析する。断層撮影したデータを元の設計図と比較し、製造工程において何かしらの要素が追加されたり減算されたり変更されたりしていないかを識別するものである。

これらのプロセスはほぼすべて自動化されており、Tehranipoor 氏の研究グループはシステムが人間の手助けを借りずにマザーボードを分析できるようになることを目指している。また、より識別が難しい「ボード上のコンデンサや抵抗の物理的な値が変更されたもの」や「インターコネクトの寸法が微妙に変更されたもの」といったものをシステムで識別できるようになることも目標としている。

---

160 PC Watch: Google、CPU の投機実行機能に脆弱性発見。業界をあげて対策へ
https://pc.watch.impress.co.jp/docs/news/1099687.html

161 1998 年に Larry Page 氏らによって設立された、インターネット関連のサービスと製品に特化した米国のテクノロジー企業。

162 GIGAZINE: AI や X 線を使ってマザーボードに仕込まれたスパイチップを見破るシステム
https://gigazine.net/news/20181010-spotted-secret-chinese-chip/

163 Florida Institute for Cybersecurity Research (FICS Research)。長期的な産官学の連携のもと、サイバーセキュリティ分野の発展のために学際的な研究を行う機関として設立された。

6.4.3.4 事例③: AI・X 線を用いた不正チップ検出[164]（Creative Electron）

2008 年設立の X 線検査装置・ソリューション提供企業である Creative Electron は、正常なチップの画像データを AI に学習させ、X 線で取得した検査対象チップの画像データと照合して不正チップを検出する技術を開発している。

Creative Electron は、設立後、数年は技術開発にフォーカスし、その間にセキュリティ・防衛分野で政府機関とも協働した経験がある。現在は、大規模・小規模・AI 搭載・自動・中古品等、様々な X 線検査装置とソフトウェア、メンテナンスサービス等を、エレクトロニクス製品のあらゆる開発ステージを対象にして大小様々な顧客に提供している。

6.4.3.5 事例④: AI を用いた回路構造からの悪意の回路検出[165]（早稲田大学戸川研究室）

早稲田大学の戸川研究室は、2017 年 6 月、半導体等の電子部品に組み込まれた「悪意の回路（ハードウェアトロイ）」を検知するため、政府と人工知能（AI）を使った検知技術の開発に着手した。既に特定した悪意の回路の特徴を AI に学習させ、未知の回路でも識別できる検知技術の開発を目指しており、2020 年までに検知装置の商用化につなげることを想定している。

戸川研究室は、SoC 設計と設計技術、組込みシステム設計と設計技術、動的再構成可能システム、地理情報処理並びに高度交通システム、通信情報処理等を研究テーマとしている。また、戸川教授は 2018 年 4 月、平成 30 年度 科学技術分野の文部科学大臣表彰 科学技術賞を受賞している。受賞業績は、集積回路の革新的設計技術とそのセキュリティ応用研究。

6.4.3.6 事例⑤: 電磁波を利用したサイドチャネル分析によるハードウェアトロイの検出（IEEE）

天津大学・フロリダ大学の研究者により執筆された論文が 2017 年 10 月に IEEE のジャーナル誌に掲載された[166] 。

従来のハードウェアトロイ検出の研究では、真正性が確認された製造済みのチップをベースにしていたが、本研究では設計データをベースにしている。また、理論上ではどのようなプロセスを経て製造されたチップにでも対応できる手法でもある。

チップ内に流れる電流の量はチップ内のロジック構造の変化と相関関係があり、流れる電流の影響で電磁波が発生する。FPGA や CMOS に流れる電流と発生する電磁波はロジック構造の変化のみに影響を受け、実装の仕方やレイアウトからは影響を受けないが、ハードウェアトロイが混入した場合は回路の構造が変更されていることから電流・電磁波が変化する。本研究では、設計データをベースに発生する電磁波をシミュレーションし、実際のチップから発生する電磁波と比較することでハードウェアトロイの混入を検出する手法を提案している。

---

[164] Creative Electron: Finding hardware hacks using x-rays
https://creativeelectron.com/2018/10/05/finding-hardware-hacks-using-x-rays/

[165] 産経ニュース: 「悪意の回路」をＡＩで検知　政府と早大が研究着手　サイバー攻撃の被害拡大を阻止
https://www.sankei.com/economy/news/170606/ecn1706060001-n1.html

[166] Jiaji He, Yiqiang Zhao, Xiaolong Guo, Yier Jim (2017). “Hardware Trojan Detection Through Chip-Free Electromagnetic Side-Channel Statistical Analysis”, IEEE Transactions on Very Large Scale Integration Systems, Vol. 25, No. 10

6.4.3.7 その他事例①: 真正性の定義が困難になる動的カモフラージュ[167]

ニューヨーク大学の Nikhil Rangarajan 氏の研究チームが動的カモフラージュという手法を開発した。

設計段階で半導体回路の一部をブラックボックス化することで、リバースエンジニアリングが不可能な構造としている。設計通りに製造したチップはそのままでは機能せず、チップメーカーが事後的に回路を切り替えることで初めて意図した機能が発現されるような仕様となっている（図 6-6）。

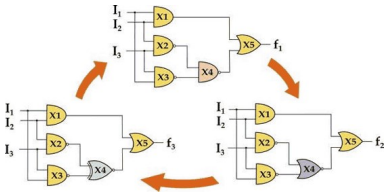


図 6-6　動的カモフラージュイメージ図

6.4.3.8 その他事例②: 物理的な攻撃への対応[168]

物理的な攻撃には大きく以下の四つのパターンが存在する。

①プロービング攻撃:
チップ内部をプロービングしてメモリから機密データを読み出したり、チップ内部の配線に変更を加えてセキュリティ機能を無効化することで信号を取り出したりする攻撃。
②かく乱攻撃:
動作中のチップ上にレーザー光を照射、または電源やクロックラインにパルスを印加することによりチップの動作をかく乱させて、プログラムの流れや処理データを変更させる攻撃。
③サイドチャネル攻撃:
チップ動作時の消費電力や放射電磁波の波形を採取して採取波形の特徴を分析し、多数の波形の統計処理を行うことにより内部の機密情報を抽出する攻撃。
④誤動作攻撃:
未定義コマンドや想定外のパラメーターをチップに与えることで、想定外の振る舞いやレスポンスを行わせて内部情報を抽出する攻撃。

それぞれの攻撃への様々な対抗技術が検討されており、各チップ製造関連企業では対策がとられている。①のプロービング攻撃に対しては、シールド配線層を設けることで回路を直接見えなくし、回路の加工を困難にしていたり、②のかく乱攻撃に対しては、レーザー検知センサを実装したりすることで対処している。③のサイドチャネル攻撃に対しては、ダミー演算やランダム遅延の挿入、ノイズ付加等を通じて内部情報を読み取りにくくしている。また、④の誤動作攻撃に対しても、例えば Infineon 社は対抗できていると発表しているが、詳細な技術内容は非公表となっている。

---

[167] GIGAZINE: 知財窃盗や悪意あるコード混入などを予防するため半導体チップを動的にカモフラージュする技術が考案される
https://gigazine.net/news/20181129-dynamic-camouflaging-approach-on-chip/

[168] 株式会社 ECSEC Laboratory: ハードウェア評価・認証スキームの国内唯一の認定評価機関によるシステム LSI の脆弱性評価
http://www.ecsec.jp/HW3.html

6.4.3.9 まとめと今後の展望

ハードウェアにおいては、脆弱性の検出については主に各チップメーカーが自社で検証していると想定され、不正の検出においても商用化できるほどの手法が見受けられない。

不正検出における現状の課題としては、不正検出手法をどのようにして確立するかと、そもそもの真正なモノをどのように定義するかという 2 種類に大別される。

不正検出手法の確立については、物理的な違いを利用した研究と、電気特性を利用した研究が存在している。物理的な違いを利用した研究としては、AI・X 線を用いて回路構造を比較して不正を検出するフロリダ州サイバーセキュリティ研究所の研究（6.4.3.3　項参照）や、Creative Electron（6.4.3.4　項参照）の研究がある。これらの研究は真正なモノと検査対象との比較を前提としており、設計データは必要としない。また、AI を用いて回路構造から悪意の回路を検出する戸川研究室による研究（6.4.3.5　項参照）もあり、こちらは設計データの存在を前提としている。電気特性を利用した研究としては、通電時に発生する電磁波を分析して不正を検出する IEEE の He 氏らの研究（6.4.3.6　項参照）が存在し、設計データの存在を前提としている。

真正なモノの定義方法については目立った研究は見受けられず、今後の研究課題として残っている。不正検出手法の確立に関しては、真正なモノの定義方法に加え、トレードオフ関係の誤検出と検出漏れをどのようにして少なくするかという精度向上の課題や、自動化・高速化・コストダウンをどのようにして図るかという実用化・商用化のための課題が、今後の研究課題として挙げられる。

また、チップ・マザーボード以外の構成部品（センサ、アンテナ、モジュール等）では脆弱性・不正検出の研究は見受けられない。各メーカーが自社で検査を実施し、取引先は各メーカーへの信頼のもと調達しているため、特段研究が進められていないと想定される。脆弱性・不正検出ツールの製品化もされておらず、実務的には、まずソフトウェア/ファームウェアを主眼としてペネトレーションテスト等でチェックしている。さらに、運用の結果、ハードウェア側の脆弱性・不正が判明することもある。

6.5　ホワイトハッカー活用状況

6.5.1　概要

ペネトレーションテストのサービスを提供している Synack について、主に採用とエンゲージメントの観点から調査し、関係者インタビューを行った。その結果、Synack の厳正な選考プロセスが良質な案件や強いブランド力につながり、採用とエンゲージメントの両面に良い影響をもたらしていることが判明した。

また、Synack と同様のサービスを提供している HackerOne、Bugcrowd についても調査を実施し、ペンタゴンのバグバウンティ（脆弱性報奨金制度）活用事例について整理した。ペンタゴンは Synack や HackerOne、Bugcrowd を活用しているが、機密性の高いプライベートドメインは Synack が受け持ち、HackerOne や Bugcrowd は機密性の低いパブリックドメインを受け持っている。

さらに、バグバウンティ活用状況やハッカーの生態についての調査データによると、ハッカーは若い人が多く、金銭・キャリア目的のために副業としてハッキングを行っていることが多いということがわかった。

バグバウンティのプラットフォームに登録しているホワイトハッカー数は増加を続けており、報告される脆弱性に支払われる報酬も増加の傾向が見て取れるため、今後も活用範囲が広がっていくと考えられる。

6.5.2 Synack[169]について

6.5.2.1 概要

2013 年に米国で設立された、クラウドソーシング脆弱性検査サービス提供企業である。正社員とは別に、Synack Red Team (SRT) と呼ばれるホワイトハッカーチームを有し、契約ハッカーを 1,000 人程度抱える。

ハッカーの選考には非常に厳正なプロセスがとられ、バックグラウンドチェックも入念になされており、クライアントからの Synack への信頼は厚い。ペンタゴンが実施しているプログラムでも機密性の高い領域を任せられており、有名企業からも多くの重要な案件が持ち込まれている。このことがハッカーの人気を呼び、多くの採用申し込みが自然と集まる状況となっている。

また、SRT のメンバーはフリーランスで働いている人もいれば、Google や Facebook のような GAFA 等の IT 大手企業に勤務しつつ副業として働いている人もいるが、上記の通りチャレンジングな案件を多数抱えていることが、SRT へのエンゲージメントを高める一因となっている。

6.5.2.2 採用

SRT はハッカーの間で人気が高く、自然と応募が集まる状況である。応募者は、会社の採用ページで必要事項をフォームに記載して申し込む。また、LinkedIn のプロフィールや HackerOne、Bugcrowd 等の bug-hunting のプロフィールを元にした募集も行っている。

選考は非常に厳正なプロセスで行われる。書類チェックからプロセスが始まり、レジュメに書かれている bug-hunting 実績が本当かどうか等を確認される。なお、学歴や職務経験等は求められないが、脆弱性の発見の実績が問われることとなる。次の面接は録音・録画されており、後ほど再度チェックすることが可能となっている。さらに理論と実践のアセスメントが行われる。アセスメントでは、与えられたテストの中から重大な脆弱性が発見できるか等が確認される。

バックグラウンドのチェックは特に丁寧に行っており、外部に委託して周辺人物へのヒアリング調査を行う等の裏取りも行っている。他社との差別化ポイントとなり、サービス提供時の品質にもつながるため、丁寧に上記調査を行っているが、プロセスに時間がかかってしまうという側面もある。審査を通って採用されている人材は、重大な脆弱性を発見してニュースになったこともあるような有名な人材も多数いる。

採用された後も継続的にモニタリングされており、SNS 等で不審な動きがないかもチェックされている。採用時のバックグラウンドチェックや採用後のモニタリングに関しては、対抗策にもつながってしまうため、詳細な内容をうかがい知ることができない状況である（図 6-7）。

[169] Synack: The Synack Red Team
https://www.synack.com/red-team/

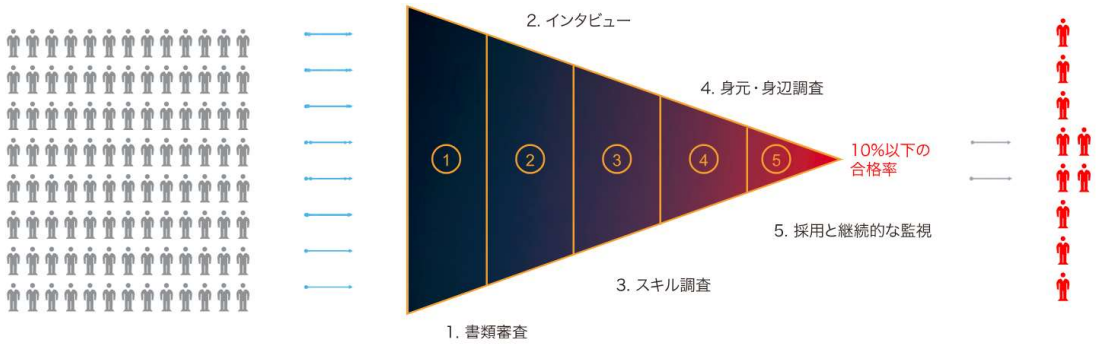


図 6-7　Synack Red Team の選考プロセス

6.5.2.3 報酬

報酬は基本的に成果給として支払われる。固定給はなく、必要経費として 1,000 米ドル/プロジェクトと、脆弱性発見者に対して 100～2,000 米ドル/脆弱性が支払われる。ハッカーにグレードはなく、みな平等に扱われており、支払いレートは成果の度合い（発見した脆弱性の重要度等）のみに応じて決定されている。一方、クライアントへの請求額は固定のため、Synack は一定程度のファイナンスリスクをとっている形式となっているが、チームが使用しているツールの性能向上にも寄与するため、Synack 側にも多くの脆弱性を発見するインセンティブは存在する。

上記の通常の報酬に加え、多数の重要な脆弱性を発見したようなホワイトハッカーにはボーナスが支給され、本社に招かれてパーティにも参加することができる。また、機密性の高い重要プロジェクトに多く関われることもエンゲージメントを高める一因となっている。

一方、報酬体系は基本的には成果給であるため、安定のために固定給の仕事の方が好ましいと思っているハッカーもいる。

6.5.2.4 プロジェクト運用

クライアントの検査対象に応じ、得意分野が適合するハッカーを選定し、50～100 人程度の検査チームを編成する。選考の段階で厳しい審査を経ているため、検査チーム編成の際には厳しい審査はないが、クライアントの要望（例: 特定の国のハッカーのみにする、特定の国のハッカーを除外する等）に応じて編成される。

脆弱性検査の際は、作業を記録・監視するゲートウェイである Launch Point を用いた VPN 経由で行われる。プロジェクトを管理する Synack 社のチームである Mission Ops（社員により構成される、SRT とは別のチーム。プロジェクトを管理する。）により、検査中の作業画面のモニタリングや、脆弱性の確認、アタックの再現等が行われる。

検査ではまず、独自スキャンツールである Hydra を使用し、既知の脆弱性を検出する。ここで検出された脆弱性は報奨金の対象とはならない。発見された脆弱性を基に、SRT はさらに深い脆弱性検査を実施する。また、SRT により発見された脆弱性は、Hydra の性能向上にも活用されている。

SRT が発見した脆弱性は Mission Ops が内容を確認し、本当に脆弱性かどうかをチェックする。脆弱性と認められたものは、脆弱性情報（概要、深刻度・影響度、存在場所、修正方法等）とともにクライアントポータル上に表示される。ここで掲載された脆弱性に対して報奨金が支払われる。

クライアントポータル上ではどのシステムにどれだけの攻撃を仕掛けたがわかるようになっており、脆弱性チェックの網羅性を確認することができるようになっている。適宜検査チームと連絡も取れるようになっており、より詳しく調査してほしい箇所や、もう検査が不要な箇所等の伝達も可能となっている。また、クライアントは、検査チームの指摘を受けて

修正した脆弱性に対する再検査の依頼も可能となっている。

サービスの種類としては、スポットでのサービス提供と、継続的なサービス提供とに大別される。スポットでのサービス提供では、2 週間等の期間を決めて、上述のような内容・フローで脆弱性チェックが実施される。継続的なサービス提供では、より長い期間を決め、その期間中は常に Hydra によるスキャンを実施し、任意のタイミングで特定回数のスポットサービスを提供する内容となっている（例: 1 年間 Hydra でスキャンし、その期間中に 2 回のスポットサービス利用が可能）。

なお、身辺警護等の身の安全に対しての保障は特にない。また、VPN 経由ですべてのトラフィックが会社にモニタリングされていることに不満を感じているハッカーもいる。

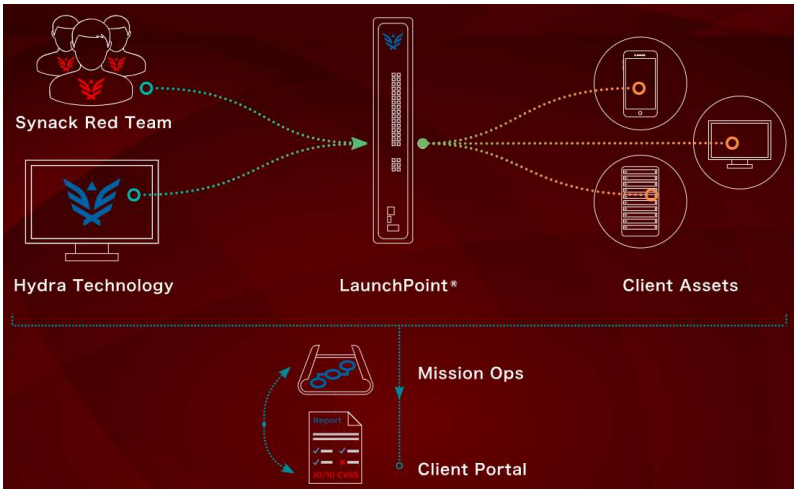


図 6-8　プロジェクト体制イメージ

上記（図 6-8）のプロジェクト運用の一連の流れはビジネスモデル特許（図 6-9）を取得している（Patent No.: US9697362 B2）。

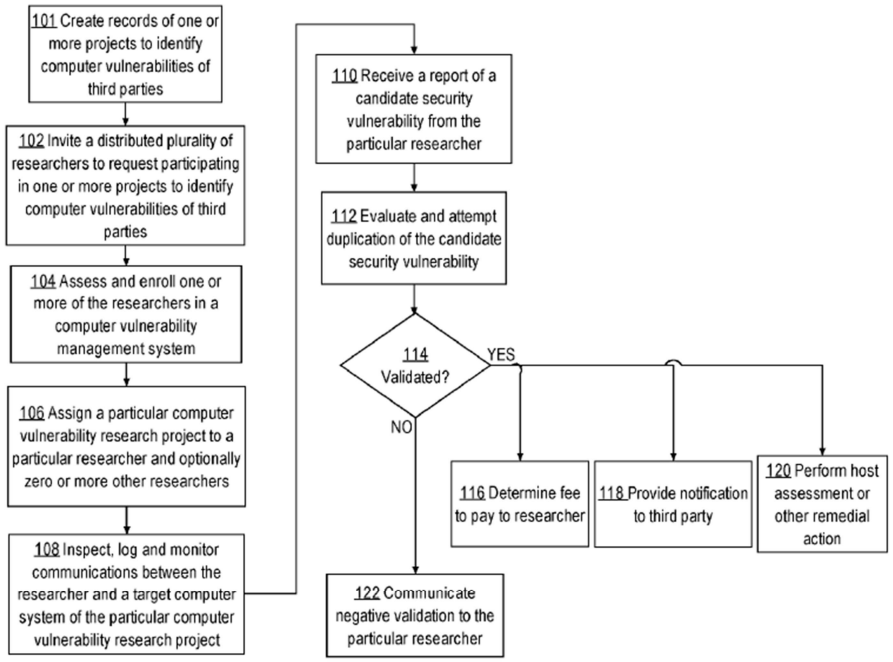


図 6-9　ビジネスモデル特許に掲載のフロー図

6.5.2.5 参考: セキュリティクリアランス制度におけるバックグラウンドチェック

6.5.2.5.1 米国

米国では、機密情報にアクセスする必要がある個人に対してバックグラウンドチェックを行う、セキュリティクリアランス制度[xiii]が実施されている。

連邦職員に対して行われるセキュリティクリアランス審査では、まずは Standard Form 86 (Questionnaire for National Security Positions) という質問票を提出する必要があり、審査を受ける人物の居住実態や家族・友人との関係のほかに、テロとの関係性、過去の犯罪歴、IT システムの不正利用の有無、麻薬使用やアルコール消費の状況、心情・情緒面での健全性、資産状況、海外でのビジネス経験や渡航歴の有無、裁判への関与履歴の有無等に関して回答することが義務付けられている。内容は、スキャンした指紋とともに国務省の Office of Personnel Security and Suitability によりチェックされる。

チェックののちに調査員による対面での面接が実施され、過去・現在の居住場所、通学先、通勤先等を含む事実確認が行われる。調査員は、調査対象者の過去・現在の隣人、上司、同僚、クラスメート等にもヒアリングし、事実確認を行う。

これらの調査が完了すると、National Security Adjudicative Guidelines に照らし合わせ、資格認定の判断を下す。なお、機密情報を扱う民間企業の従業員に対しても同内容のプロセスで審査が実施される。

6.5.2.5.2 日本

日本では、2017 年 5 月の「デジタル・ニッポン 2017」において日本版セキュリティクリアランス制度の導入が提言されたが、実施には至っていない。類似の法律としては、2014 年 12 月に施行（2013 年 12 月に成立）された特定秘密保護法[170] が存在する。

特定秘密保護法では、防衛・外交・スパイ活動防止・テロ防止の項目について、関連省庁の長（大臣等）が指定したものを特定秘密とし、特定秘密を扱う公務員や防衛産業等に従事する社員については秘密を漏らす恐れがないかを「適正評価」で審査する必要があるとしている。

適正評価では、①特定有害活動及びテロリズムとの関係に関する事項、②犯罪及び懲戒の経歴に関する事項、③情報の取扱いに係る非違の経歴に関する事項、④薬物の濫用及び影響に関する事項、⑤精神疾患に関する事項、⑥飲酒についての節度に関する事項、⑦信用状態その他の経済的な状況に関する事項が調査事項として挙げられており、米国のセキュリティクリアランス制度よりも項目が絞られている。家族（配偶者・父母・子・兄弟姉妹、配偶者の父母及び子）及び同居人については、①の調査にあたって、氏名・生年月日・国籍・住所のみを調査する。

評価では、評価対象者の同意のもと、本人またはその上司・同僚等の関係者への質問、評価対象者への資料提出の要求、公務所または公私の団体への照会等を通じて調査を実施する。

---

[170] 内閣官房: 特定秘密保護法関連
https://www.cas.go.jp/jp/tokuteihimitsu/index.html

6.5.3 HackerOne[xiv] について

6.5.3.1 概要

脆弱性情報の公開と、バグ発見者への報奨金プログラムを提供するプラットフォームで、2012 年からサービスを開始し、現在 20 万人以上のハッカーが登録している。企業とセキュリティ研究者を結びつけている。顧客には、米 Yahoo!、Adobe Systems、Dropbox、LinkedIn、Twitter、WordPress 等 250 社を超える企業が名を連ねている。日本企業でも、任天堂、パナソニック等が活用している。

HackerOne が取り組みを始めた 2012 年から 2018 年 6 月までの間に、様々な組織から支払われた賞金の総額は 3,100 万米ドルを超えており、その 3 分の 1 以上となる 1,170 万米ドルが 2017 年 5 月から 2018 年 4 月の 1 年間だけで支払われている。

政府主導の公的なプログラムは前年比で 125%増加している。例えば、米国防総省をはじめ、欧州委員会やシンガポール防衛省も実施している。

6.5.3.2 案件種類

バグバウンティの形態を大きく「public」と「private」に分けると 79%が「private」である。ここで「public」とは広く一般に公開されて誰でも参加できるものを指しており、「private」は招待された人または参加申し込みを経て受け付けられた人のみが参加できるもので、いわゆる非公開案件のことである。

6.5.3.3 報酬

1 万米ドルを超える報奨金が支払われたバグレポートは 116 件あった。深刻（critical）なものに対する報酬の平均額は 2,000 米ドルを超えるまでに増加している。また、25 万米ドルを提示している組織もある。

6.5.4 ペンタゴンの事例[xv]

ペンタゴンは 2016 年 3 月、サイバーセキュリティの脆弱性を発見・修正するために、選定された専門家に米国防総省のインターネットページをハックさせる計画を明らかにした。この計画は“Hack the Pentagon”と呼ばれている。

Hack the Pentagon は連邦政府で初めてのバグバウンティとして、同年の 4 月から 5 月にかけて実施された。それまでは、脆弱性の報告・修正が目的であったとしても、ハッカーが国防総省の Web サイトの脆弱性を探すことさえ違法となりえたが、Hack the Pentagon では合法的に脆弱性を探すことができる。HackerOne が実行のパートナーとして選定され、本プログラムでは 1,400 人のセキュリティリサーチャーが参加し、138 の重大な脆弱性が発見・修正された。

同プログラムの成功を受け、2016 年 10 月にペンタゴンは Hack the Pentagon の延長を決定した。HackerOne と Synack が運営者として選定され、HackerOne がパブリックドメインを担当し、Synack がより機密性が高いプライベートドメインを担当した。

同プログラムは繰り返し実施され、2018 年 10 月には、プログラムの対象をハードウェア・物理システムを含めたあらゆる領域にまで拡張して実施すると発表した。また、運営者に Bugcrowd が加えられた。ここまでのプログラムで 3,000 以上の脆弱性が発見され、33 万米ドル以上がハッカーに支払われている。

6.5.5　Bugcrowd について

6.5.5.1 概要

Bugcrowd は 2012 年に米国で設立された「バグ報奨金制度の代行事業者」であり、強固なプログラム管理と信頼できる一流リサーチャー、統合型プラットフォームを持つ。このプラットフォームにて、脆弱性発見バグ報奨金プログラムを提供し、従来型のテスト試行に比べて 7 倍の重要な脆弱性を発見しているとアナウンス[171]している。

2018 年 3 月までに 700 以上のプログラムを運営し、賞金の総支払額も年々増加している（図 6-10）。

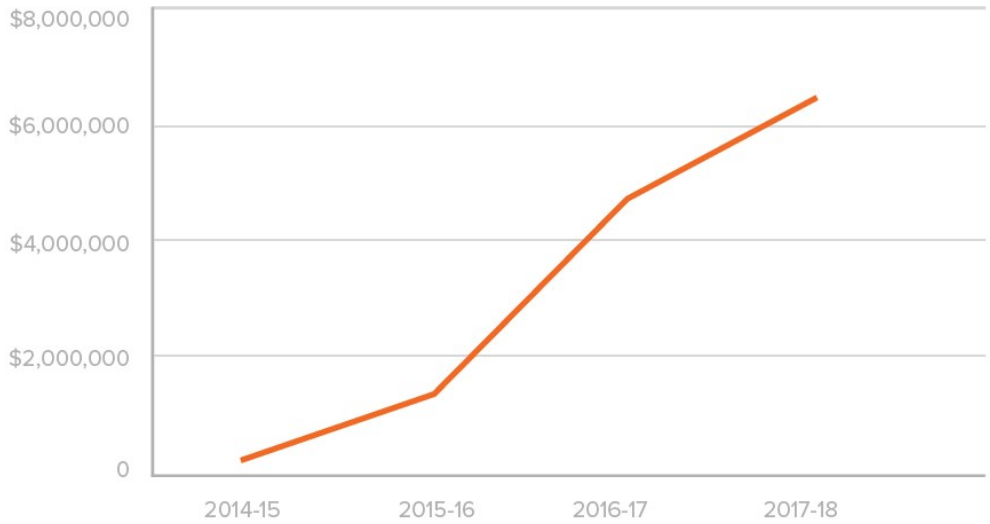


図 6-10　賞金の総支払額推移[172]

登録しているセキュリティ技術者も増加を続けており、2018 年には 8 万人以上とレポートされている[173]。

- 2018 年 3 月 8 万人以上　109 ヵ国
- 2017 年 3 月 53,332 人　国数不明
- 2016 年 3 月 26,782 人　112 ヵ国
- 2015 年 6 月 17,994 人　147 ヵ国

[171] Bugcrowd: The Ultimate Guide to Managed Bug Bounty
https://www.bugcrowd.com/the-ultimate-guide-to-managed-bug-bounty/
[172] Bugcrowd: 2018 State of Bug Bounty Report
https://www.bugcrowd.com/resource/2018-state-of-bug-bounty-report/
[173] 各年の Bugcrowd 発表の State of Bug Bounty Report より。

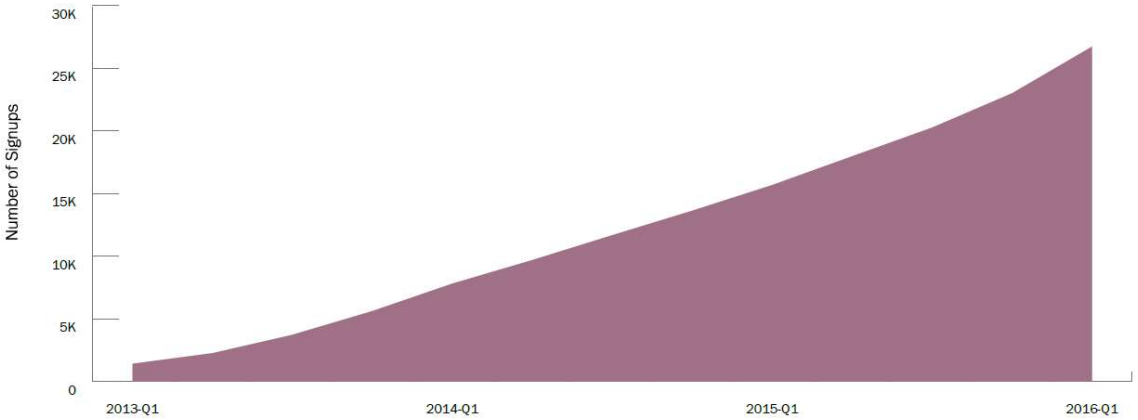


図 6-11　登録しているセキュリティ技術者の推移[174]

国別の人員は、2017 年 3 月現在、米国 14,244 人、インド 11,663 人、英国 2,952 人、オーストラリア 1,588 人の順である（2018 年 3 月資料では、具体的な国別人員構成の記載なし）。

6.5.5.2 脆弱性価格設定モデル[175]

Bugcrowd は、脆弱性と賞金の値付け方法について情報を公開している。
この脆弱性価格設定モデルは、組織の成熟度と脆弱性の優先度（技術的及びビジネスへの影響）という二つの側面に基づいている。

表 6-2 以降に示すように、五つの脆弱性レベルと関連する三つの組織の成熟度レベル（Basic、Progressing、Advanced）により価格が設定される。

[174] Bugcrowd: 2016 State of Bug Bounty
https://www.bugcrowd.com/resource/2016-state-bug-bounty/
[175] Bugcrowd: Defensive Vulnerability Pricing Model
https://www.bugcrowd.com/resource/bugcrowds-defensive-vulnerability-pricing-model/

表 6-2　組織の成熟度ステージ

	Basic	Progressing	Advanced
Philosophy	"Cybersecurity is a necessary evil."	"Cybersecurity must be more integrated into the business."	"Cybersecurity is part of the culture."
People	CISO reports to IT Small security team with minimal skills	CISO reports to COO or other non-IT manager Larger security team with some autonomy from IT	CISO reports to CEO and is active with the board Large, well-organized staff with good work environment
Process	Informal and ad-hoc Subservient to IT	Better coordination with IT, but processes are rare, informal, manual and dependent upon individual contributors	Documented and formal with an eye toward scale and automation
Technology	Elementary security technologies with simple configurations Decentralized security organizations with limited coordination across functions Focus on preventions and regulatory compliance	More advanced use of security technologies and adoption of new tools for incident detections and security analytics	Building enterprise security technology architecture Focus on incident prevention, detection and response Adding elements of identity management and data security to deal with cloud and mobile computing security

Source: Enterprise Strategy Group

表 6-3　組織の成熟度ステージ（和訳）

	Basic	Progressing	Advanced
哲学 Philosophy	➢ サイバーセキュリティは必要な悪である	➢ サイバーセキュリティはビジネスにより統合されている	➢ サイバーセキュリティは文化の一部
人 People	➢ CISO は IT に報告 ➢ 最小限のスキルしか持たない小規模なセキュリティチーム	➢ CISO は COO または他の非 IT マネジャーに報告 ➢ IT からある程度の権利を持つ大規模なセキュリティチーム	➢ CISO は最高経営責任者（CEO）に報告し、取締役会で活動 ➢ 職場環境がよく整頓された大規模なスタッフを持つ
プロセス Process	➢ 非公式でアドホック的 ➢ IT へ従属	➢ IT との連携は改善されているが、プロセスは非公式で、手動で、個々の貢献者に依存	➢ 自動化を見据えた正式な文書化
技術 Technology	➢ 簡単な構成の基本的なセキュリティ技術 ➢ 機能間の調整が制限されている分散型セキュリティ組織 ➢ 予防と法令遵守にフォーカス	➢ セキュリティ技術のより高度な使用とインシデント検出とセキュリティ分析のための新しいツールの採用	➢ エンタープライズセキュリティテクノロジアーキテクチャの構築 ➢ インシデントの防止、検出及び対応にフォーカス ➢ クラウド及びモバイルコンピューティングのセキュリティに対処するための ID 管理及びデータセキュリティの要素の追加

表 6-4　脆弱性レベルの表

Priority	Impact	Vulnerability Types
P1 - Critical	Vulnerabilities that cause a privilege escalation from unprivileged to admin or allow for remote execution, financial theft, etc.	• Remote Code Execution • Vertical Authentication Bypass • XML External Entities Injection with significant impact • SQL Injection with significant impact
P2 - High	Vulnerabilities that affect the security of the platform including the processes it supports	• Lateral authentication bypass • Stored XXS with significant impact • CSRF with significant impact • Direct object reference with significant impact • Internal SSRF
P3 - Medium	Vulnerabilities that affect multiple users and require little or no user interaction to trigger	• Reflective XXS with impact • Direct object reference • URL redirect • CSRF with impact
P4 - Low	Vulnerabilities that affect singular users and require interaction or significant prerequisites to trigger (MitM) to trigger	• SSL misconfigurations with little impact • SPF configuration problems • XSS with limited impact • CSRF with limited impact
P5 - Acceptable Risk	Non-exploitable vulnerabilities in functionality. Vulnerabilities that are by design or are deemed acceptable business risk to the customer	• Debug information • Use of CAPTCHAs • Code obfuscation • Rate limiting, etc.

Impact and vulnerability types by priority

表 6-5　脆弱性レベルの表（和訳）

プライオリティ	影響	脆弱性タイプ
P1 - クリティカル	特権のないユーザーから管理者に権限昇格、リモート実行、金銭盗難等を可能にする脆弱性	・リモートコード実行 ・バーティカルな認証バイパス ・重大な影響を与える XML 外部エンティティインジェクション ・重大な影響を与える SQL インジェクション
P2 - 高	サポートするプロセスを含むプラットフォームのセキュリティに影響を与える脆弱性	・ラテラル認証バイパス ・重大な影響を与えるストアド XXS ・重大な影響を与える CSRF ・重要な影響を与える直接オブジェクト参照 ・内部 SSRF
P3 - 中	複数のユーザーに影響を及ぼし、トリガーするのにユーザー操作がほとんどまたはまったく必要ない脆弱性	・影響のある反射型 XXS ・直接オブジェクト参照 ・URL リダイレクト ・影響のある CSRF
P4 - 低	単一のユーザーに影響を及ぼし、トリガーするのにユーザー操作または MitM 等の重要な前提条件を必要とする脆弱性	・影響がほとんどない SSL の設定ミス ・SPF (Sender Policy Framework) 設定問題 ・影響が限定的な XSS ・影響が限定的な CSRF
P5 - 許容できるリスク	悪用されない脆弱性 設計上のもの、または顧客にとってビジネスリスクが許容できる脆弱性	・デバッグ情報 ・CAPTCHA の使用 ・コードの難読化 ・レート制限等

表 6-6　バグの市場レート（The Market Rate for Bugs）

	Security Maturity Model		
	Basic	Progressing	Advanced
Payout Range	$100 - $1,500	$200 - $5,000	$300 - $15,000
Average Bug Payout	$300	$600	$1,000
P1	$1,500	$5,000	$15,000
P2	$900	$1,800	$2,500
P3	$300	$600	$900
P4	$100	$200	$300

Baseline vulnerability budget

実際に支払われた金額の推移をみると、全体的に増額の傾向にあることがわかる（図 6-12）。

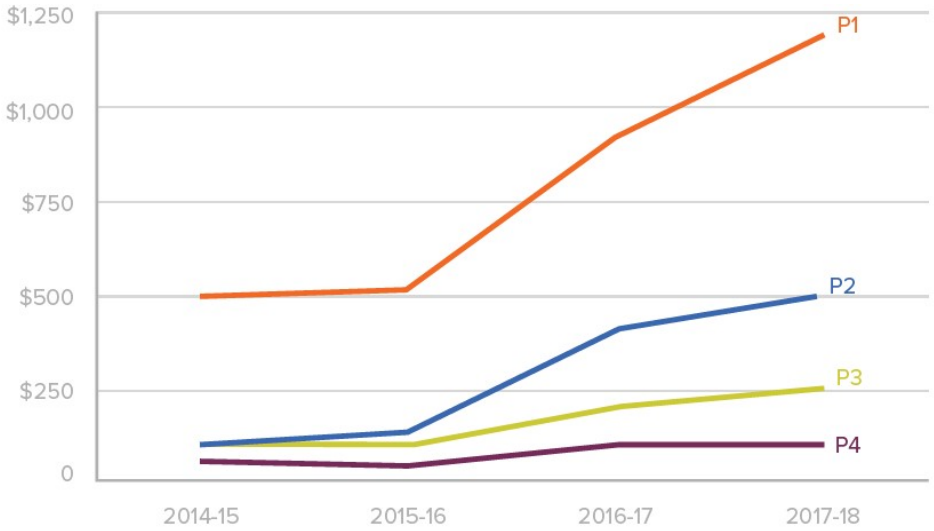


図 6-12　脆弱性プライオリティ 1 件毎の支払額の変遷 [172]

6.5.5.3 活動状況[xvi]

2017 年 4 月 1 日から 2018 年 3 月 31 日までの間のすべての Bugcrowd プラットフォームデータより算出した結果よりまとめた。

- プログラム数は、過去 1 年間で 40%増加。
- プライベートプログラムが 33%増加した。
- 昨年実施したプログラムのうち 79%はプライベートだった。
- この 1 年で、登録セキュリティ技術者は 71%増加した。
- 脆弱性あたりの平均支払額は 781 米ドルで、昨年から 73%の増加。
- P1 脆弱性のうち 75%は 1,200 米ドル超を支払った。

- 昨年支払われた全脆弱性の 13%が Cross-Site Scripting (XSS) Stored に分類された脆弱性に対するものだった。
- プラットフォームを介して提出された脆弱性の総数は、昨年から 21%増加。
- 提出された脆弱性のプライオリティは、P1 7%、P2 13%、P3 31%、P4 26%、P5 16%（6%が「その他」に分類された）。
- クロスサイトスクリプティング（XSS）（プライオリティ P3）は、今年提出された脆弱性で一番多いものであった。

6.5.6 バグバウンティの実態調査 [176]

HackerOne の調査に基づくと、近年バグバウンティはより活用される傾向にある。支払い賞金額も増加し、政府機関等も活用していることがわかる。

6.5.6.1 利用者産業別賞金額

2017 年 5 月～2018 年 4 月の 1 年間に支払われた賞金総額は、約 3,000 万米ドルであり、そのうちの約 7 割がテクノロジー業界企業からの支払いになっている。一方、1 件当たりの平均的な支払い額でみると政府機関が最上位であり、政府は高額を支払って活用していることもわかる（図 6-13）。

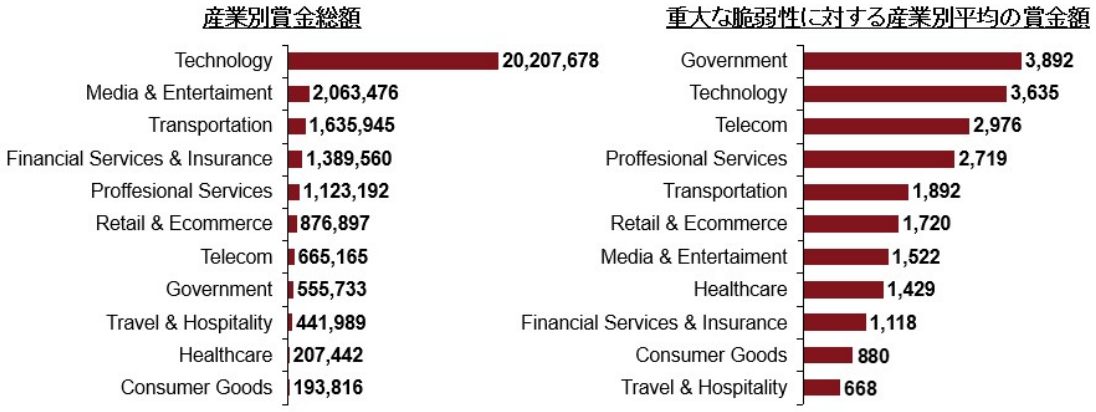


図 6-13 バグバウンティにおける賞金額（2017/5-2018/4、米ドル）

6.5.6.2 ハッキングの理由

ハッカーのハッキング理由の上位は、「金銭・キャリア目的」、「趣味や人のため」といった回答が並び、目立つことを目的にすることはほとんどない（図 6-14）。

176 HackerOne: The Hacker-Powered Security Report 2018
https://www.hackerone.com/sites/default/files/2018-07/The%20Hacker-Powered%20Security%20Report%202018.pdf

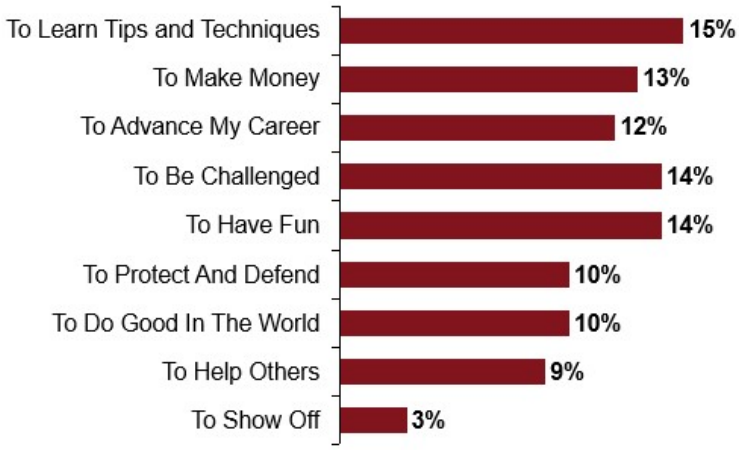


図 6-14　ハッキングを行う理由

6.5.6.3 ハッカー(アンケート回答者)のプロファイル

18-34 歳までが 82%を占め、またハッキングに費やす時間も 10 時間/週が 44%で最も多かった。必ずしも、職業専業として行っているわけではないことがわかる（図 6-15)。

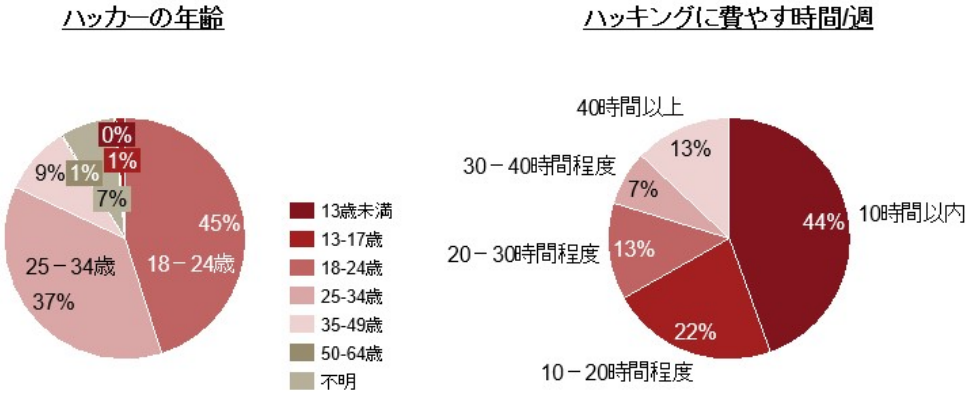


図 6-15　ハッカー（アンケート回答者）のプロファイル

6.5.7　バグバウンティ活用の注意点[177]

バグバウンティでは、登録しているホワイトハッカー（バグハンター）にて脆弱性を調査することになるが、最大の懸念は訴訟リスクとなっている。

訴訟を防ぐため、バグバウンティプログラムにはバグを発見したハッカーを提訴しないという保護措置条項が盛り込まれている場合がほとんどである。過去の問題事例の場合、このような条項が記載されていなかったという話もあり、制度をしっかり整備する必要に迫られている。

[177] StoneWasher's Journa: 社会を支えるバグハンター、最大の悩みは訴訟リスク
https://stonewashersjournal.com/2018/10/15/bughunter-and-legal-issues/2/

6.5.7.1 DJI の件[178]

2017 年、ドローン開発会社の DJI は、自社でバグバウンティプログラムを展開。バグハンターにソフトウェアのバグ発見を依頼した。

その後、あるハンターが重要なバグを発見して DJI に報告した。彼はこれで 3 万米ドルの報奨金が受け取れるはずだったが、DJI のバグバウンティプログラムには、発見したバグの内容を公表しないという条件がつけられていた。その条件だと 3 万米ドルは手に入るが、この案件を自分の功績として公表することができなかった。

最終的に、このハンターは金銭よりも手柄の公表を優先し、プログラムの一環として報告するのではなく独自に発見したバグとして公表することを決定した。3 万米ドルを諦めてでも、自分の技術を証明することに役立てることを選んだ。

6.5.7.2 Keeper の件[179]

2018 年、パスワード管理ソフトである Keeper に脆弱性があるというニュースが発表された。発表時点でその脆弱性は解消されており、そのこともあって発表されたのであるが、Keeper 側はこれを事実無根の内容であるとして、記事の執筆者を名誉毀損で訴えた。

6.6 検査技術強化の方向性

ソフトウェアに対する解析技術として、ソースコード解析及びファジングを調査したところ、より使いやすく・工数のかからない・効率的・検出性能向上を目指した研究・ツール開発が行われている状況であり、今後も継続されていくと想定される。

ハードウェアに対する解析技術としては、まだ研究段階のものが多く、使いやすいツールの製品化が望まれる。また、研究が進められている領域が LSI に対するものが多く、モジュールや製品向けの技術強化も必要となってくると考えられる。

ホワイトハッカー活用に関しては、バグバウンティを実施するプラットフォームが構築されているため、より身近になっていくと考えられる。

---

178 TechCrunch Japan: DJI に脆弱性報告のハッカー、報奨金 3 万ドルを突き返す。実績公表禁じる契約、法的措置ちらつかされ反発
https://jp.techcrunch.com/2017/11/22/engadget-dji-3/

179 スラド: パスワード管理ツールを開発する Keeper Security、脆弱性を伝える記事を掲載したメディアを提訴
https://security.srad.jp/story/17/12/26/0731249/

[vi] PC Watch: 米国土安全保障省がカスペルスキー製品の排除を通達
https://pc.watch.impress.co.jp/docs/news/yajiuma/1080844.html
INTERNET Watch: 米政府のカスペルスキー製品使用禁止の件について、ユージン・カスペルスキー氏が語る
https://internet.watch.impress.co.jp/docs/news/1127229.html
[vii] 1986 年に GE のマイクロエレクトロニクス部隊の研究者が設立した米国のソフトウェア企業。半導体設計からソフトウェア開発までの領域（Silicon to Software）をカバーしており、SoC 設計者やアプリケーションソフトウェアの開発者向けに、EDA（電子設計自動化）ツールと IP（半導体設計資産）を提供。売上は EDA セグメントが 6 割、IP セグメントが 3 割を占めており、セキュリティテスト・管理サービスは IP セグメントの一部を構成している。
[viii] merican fuzzy lop (2.52b)
http://lcamtuf.coredump.cx/afl/
OSDN Magazine: ファジングテスト「American Fuzzy Lop（AFL）」をより汎用的に利用可能にすることを目指す「Project Triforce」
https://mag.osdn.jp/16/06/29/163000
[ix] 2006 年に米国で設立された、アプリケーションセキュリティ企業。静的解析、動的解析、振る舞い分析等を含む様々なセキュリティ分析技術を提供している。2017 年に米国のソフトウェア企業である CA Technologies の傘下となった（CA Technologies は 2018 年に米国の半導体企業である Broadcom の傘下となった）。
[x] Transparency Market Research: Runtime Application Self-Protection Market (Component - Solutions (Web Applications, Mobile Applications, Others) and Services (Professional Services and Managed Services); Deployment – (On-premise and Cloud); Industry Vertical - (BFSI, IT and Telecommunications, Government and Defense, Energy and Utilities, Manufacturing, Healthcare, and Retail) - Global Industry Analysis, Size, Share, Growth, Trends and Forecast 2017 - 2025
https://www.transparencymarketresearch.com/runtime-application-selfprotection-market.html
[xi] ・当初報道記事
GIGAZINE: Apple&Amazon サーバーが中国人民解放軍の実働部隊にデータを盗むチップを仕込まれたと Bloomberg が報道、Apple・Amazon は完全否定
http://gigazine.net/news/20181005-apple-amazon-supermicro-hack/
Bloomberg Businessweek: The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies
https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
Bloomberg Businessweek: The Big Hack: Statements From Amazon, Apple, Supermicro, and the Chinese Government
https://www.bloomberg.com/news/articles/2018-10-04/the-big-hack-amazon-apple-supermicro-and-beijing-respond
・各社報道否定プレスリリース
Apple: Apple に関する Businessweek の誤った報道について
https://www.apple.com/jp/newsroom/2018/10/what-businessweek-got-wrong-about-apple/
Amazon Web Services: Setting the Record Straight on Bloomberg BusinessWeek's Erroneous Article
https://aws.amazon.com/jp/blogs/security/setting-the-record-straight-on-bloomberg-businessweeks-erroneous-article/
Super Micro Computer: Bloomberg による当社に関する報道について
https://www.supermicro.com/newsroom/pressreleases/2018/press181004_Bloomberg_Japanese.htm
[xii] マクニカネットワークス株式会社: VDOO Vision
https://www.macnica.net/vdoo/
マクニカネットワークス株式会社: マクニカネットワークス、IoT デバイスのセキュリティ対策を専門とする VDOO 社と代理店契約を締結
https://www.macnica.net/pressrelease/vdoo_20190305.html/
[xiii] U.S. Department of State: All About Security Clearances
https://www.state.gov/m/ds/clearances/c10978.htm
U.S. Office of Personnel Management: QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS
https://www.opm.gov/Forms/pdf_fill/SF86.pdf
[xiv] 2012 年に米国で設立された、国際的なバグバウンティプラットフォーム提供企業。
HackerOne: ABOUT HACKERONE
https://www.hackerone.com/about
CNET Japan: 脆弱性対応とバグ発見報奨金プラットフォームの HackerOne、2500 万ドルを調達

https://japan.cnet.com/article/35066454/

[xv] 米国防総省、バグ探し懸賞プログラム “Hack the Pentagon” を拡大
https://jp.techcrunch.com/2016/06/20/20160617department-of-defense-expanding-hack-the-pentagon-program/
Department of Defense: DOD partners with HackerOne and Synack on “Hack the Pentagon” Follow-up Security Initiative
https://dod.defense.gov/News/News-Releases/News-Release-View/Article/980731/dod-partners-with-hackerone-and-synack-on-hack-the-pentagon-follow-up-security/
CNN BUSINESS: Why the Pentagon wants people to hack it
https://money.cnn.com/2017/04/11/technology/hack-the-pentagon-synack-bug-bounty/index.html
Department of Defense: Department of Defense Expands ‘Hack the Pentagon’ Crowdsourced Digital Defense Program
https://dod.defense.gov/News/News-Releases/News-Release-View/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/
Nextgov: DOD Invests $34 Million in Hack the Pentagon Expansion
https://www.nextgov.com/cybersecurity/2018/10/dod-invests-34-million-hack-pentagon-expansion/152267/

[xvi] Bugcrowd: 2018 State of Bug Bounty Report
https://www.bugcrowd.com/resource/2018-state-of-bug-bounty-report/
Bugcrowd: The 2017 State of Bug Bounty
https://www.bugcrowd.com/resource/2017-state-of-bug-bounty/
Bugcrowd: 2016 State of Bug Bounty
https://www.bugcrowd.com/resource/2016-state-bug-bounty/
Bugcrowd: THE STATE OF BUG BOUNTY
https://foundershield.com/wp-content/uploads/2018/02/state-of-bug-bounty-08-2015.compressed.pdf

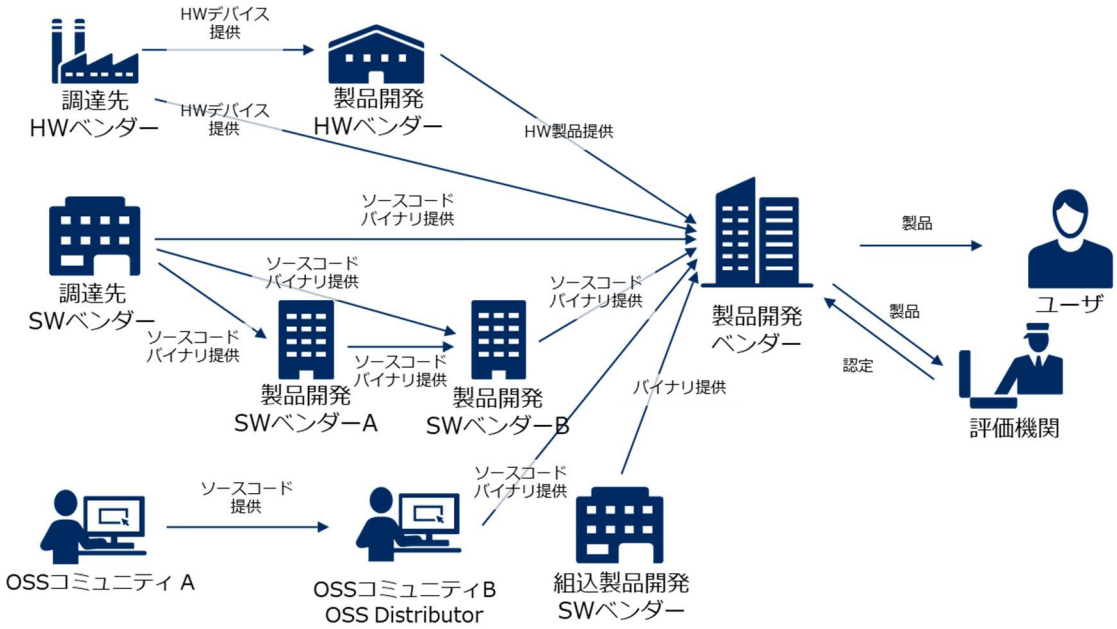
7. ネットワークセキュリティ確保の方向性

7.1 はじめに

5 章では、国、キャリア、ベンダー、OSS コミュニティ、ソフトウェア透明性の活動について調査を行い、各ステークホルダーが、セキュリティ確保の様々な対応を行っていることがわかった。6 章では、解析技術の動向について調査を行った。これらの状況を踏まえ、本章では、ネットワークセキュリティの確保の方向性について検討する。

7.2 機器検査の分析

まず、ネットワーク機器開発の主なステークホルダーの関係を図 7-1 に記載する。



日本電気作成

図 7-1 ステークホルダーの関係

次に各検査対象についてステークホルダーが実施している検査内容について、表 7-1 にまとめる。

表 7-1　各検査対象に対するステークホルダーの現状の対応

日本電気作成

対象	開発・提供主体	製品ベンダーの調達物	検査対象	ステークホルダー						
				調達先HWベンダー	調達先SWベンダー	OSSコミュニティ	OSS Distributor	製品ベンダー	評価機関	ユーザ
HW部品	製品開発ベンダー			－	－	－	－	不明	未実施	未実施
	調達先ベンダー			不明	－	－	－	不明	未実施	未実施
SW部品	製品開発ベンダー	－	ソースコード	－	－	－	－	ツール/人的	未実施	未実施
		－	バイナリ	－	－	－	－	ツール	製品として実施	製品として実施
	調達先ベンダー	ソースコード	ソースコード	－	不明	－	－	不明	未実施	未実施
			バイナリ	－	不明	－	－	不明	製品として実施	製品として実施
		バイナリ	ソースコード	－	不明	－	－	不可	不可	不可
			バイナリ	－	不明	－	－	不明	製品として実施	製品として実施
	OSSコミュニティ/OSS Distributor	ソースコード	ソースコード	－	－	ツール/人的	不明	不明	未実施	未実施
			バイナリ	－	－	不明	不明	不明	製品として実施	製品として実施
		バイナリ	ソースコード	－	－	不明	不明	不可	不可	不可
			バイナリ	－	－	不明	不明	不明	製品として実施	製品として実施
製品	製品開発ベンダー	－	バイナリ	－	－	－	－	ツール ペンテスト	ツール	ツール

この結果を踏まえると課題として以下が挙げられる。

- 試験の重複
  複数のステークホルダーで、重複した試験を実施している可能性がある。
- 製品構成品の把握の不十分さ
  製品ベンダーが調達した製品の構成内容がわからないため、検査が必要な対象の洗い出しが不十分な可能性がある。
- バイナリの品質確認のみ
  製品ベンダー、評価機関、ユーザーが、バイナリのみしか入手できないケースがあり、ソースコードで担保するレベルのセキュリティ品質が確認できない場合がある。

また 6 章の調査結果から課題として以下が挙げられる。

- 検査技術の検知精度向上
  市販品ではすべての脆弱性や不正動作を発見することができない。

これらの課題の対策案として以下が考えられる。

- ハードウェア、ソフトウェアの検査内容の共有
  本情報をステークホルダー間で情報共有することで、重複した検査の削減やバイナリの品質確認状況の把握を行うことができる。
- ソフトウェアの構成品の共有
  本情報をステークホルダー間で情報共有することで、検査対象の把握できる。
- 市販品以上の検査技術の開発
  セキュリティ向上を図ることができる。

上記の対策案を踏まえた各ステークホルダーの対応案を表 7-2 にまとめる。

表 7-2　各検査対象に対するステークホルダーの対応案

日本電気作成

対象	開発・提供主体	製品ベンダーの調達物	検査対象	ステークホルダー						
				調達先HWベンダー	調達先SWベンダー	OSSコミュニティ	OSS Distributor	製品ベンダー	評価機関	ユーザ
HW部品	製品開発ベンダー			–	–	–	–	D	B	
	調達先ベンダー			A	–	–	–			
SW部品	製品開発ベンダー	–	ソースコード	–	–	–	–	D	E ②、③	
		–	バイナリ	–	–	–	–	D	E ②、③	
	調達先ベンダー	ソースコード	ソースコード	–	A	–	–	D	E	
			バイナリ	–	A	–	–	D	E	
		バイナリ	ソースコード	–	A	–	–	対応不可	対応不可	対応不可
			バイナリ	–	A	–	–	D	E	
	OSSコミュニティ/OSS Distributor	ソースコード	ソースコード	–	–	A	A	D	E	
			バイナリ	–	–	A	A	D	E	
		バイナリ	ソースコード	–	–			対応困難	対応困難	対応困難
			バイナリ	–	–			D	E	
製品	製品開発ベンダー	–	バイナリ	–	–	–	–	D	E	

B, C

表中の補足: A. 調達先の検査、B. ハードウェア、ソフトウェアの検査内容の共有、
C. ソフトウェアの構成品の共有、D. 製品ベンダーの検査、
E. 市販品以上の検査技術による検査

7.3　評価機関の分析

セキュリティ評価を実施している政府や業界団体の現状を表 7-3 にまとめる。

表 7-3　セキュリティ評価機関の現状

日本電気作成

カテゴリ	GSMA NESAS	インド 認証制度
基準策定者	民間の業界団体	国
評価者	第三者認証機関	第三者認証機関
対象機器	基地局、コア	基地局、コア
評価内容	・設計～実装までの一連の開発プロセス ・3GPP 策定のテストスペック	・3GPP 策定のテストスペックと同等
評価方法	・開発プロセス監査 ・3GPP 策定のテストスペックの評価	・3GPP 策定のテストスペックの評価
規模	パイロット運用中のため不明	非公開

7.3.1　GSMA NESAS

NESAS の詳細については 5.3.3 に示した通りである。ネットワーク機器ベンダーが受ける NESAS 認定プロセスでは、開発プロセスの適合性とテストスペックに倣った評価結果の観点が採用されている。

テストスペックについては 3GPP SCAS への準拠を前提としている。SCAS にはネットワーク機器に特化した要件とその評価が記述されている。また、汎用的な脆弱性評価として、ポートスキャン、脆弱性スキャン、ファジングテストの実施が規定されているが、ソースコード解析のような静的解析手法については定義がないため、ソースレベルでのセキュリティ検証が課題と考えられる。

開発プロセスについては監査の方法が書類審査となっているが、NESAS でも「表 5-44 ベンダー認定に必要な要件」にある通り定性的な要件定義のため、通過可能なレベルが不明な状況である。そのため、実運用が開始された段階で、再度の確認が必要である。

7.3.2　インドの認証制度

インドでは 5.2.2.8.3　に記載のある通り、テレコムネットワーク機器向けの認定要件として MT&CTE (Mandatory Testing & Certification of Telecommunication Equipment)ルールが規定されている。また、具体的なテストスペックとして ITSAR (Indian Telecom Security Assurance Requirements) のドラフト版が公開済みとなっている。この ITSAR も NESAS と同様に 3GPP SCAS をベースに策定されているが、セキュアなソフトウェア更新手順の確立や、既知のマルウェアの検出といった、開発や運用プロセスの内容も一部規定されている。ただし、MT&CTE に基づく試験・認証制度は未施行（導入時期も未定）のため、実運用が開始された段階での確認が必要である。

7.4　OSS のセキュリティ対策分析

OSS コミュニティに関する調査の結果の概略を表 7-4 にまとめる。今回対象とした OSS コミュニティについては概ね類似した傾向を持っていることが確認できた。

表 7-4　OSS コミュニティ毎のセキュリティ対策状況概略

日本電気作成

カテゴリ		OpenStack	OPNFV	ONOS
セキュリティマネジメント		コミュニティの参加への審査はなし。コミュニティへの貢献度が評価の基準。	コミュニティの参加への審査はなし。コミュニティへの貢献度が評価の基準。	コミュニティの参加への審査はなし。コミュニティへの貢献度が評価の基準。
開発フェーズ	セキュリティチェック体制	セキュリティチェックは機能開発とは分離。2 名以上の異なる企業のコア開発者がコードレビュー。専門チームがセキュリティバグ対応。	セキュリティチェックは機能開発とは分離。セキュリティプロジェクトメンバー、及び各サブプロジェクトメンバーがチェック。	TST (Technical Steering Team) 8 名
	セキュリティ観点のチェック方法	コア開発者のコードレビュー、不特定多数のコードレビュー。	コード提案毎の相互レビューとセキュリティスキャン。	コア開発者によるコードレビュー、静的検査ツール、Black Duck 社検査等。
その他	意図的な不正の可能性についての見解	レビュー中や承認時の相互監視によって開発プロセス内にてセキュリティ問題を混入させることは非常に困難。	起こりうる前提で契約等を整備。参加時に企業・個人レベルで CLA を締結、不正認定時には追放可。	TST（2019 年 2 月時点で 8 名）中心となり、複数開発者が開発しているため、意図的な不正動作の混入可能性は低い。

次に OSS コミュニティにおいてセキュリティのリスクとなりうるポイントとその実状を以下にまとめる。

(1) OSS コミュニティでの開発者の採用

3 コミュニティに関して OSS コミュニティでの開発者の採用にあたっての判断基準は存在しない。ただし、コミュニティに対する貢献の際には、いずれのコミュニティでも CLA（貢献者ライセンス合意書: Contributor License Agreement）への合意を要求しており、開発者及び組織を排除することを可能とする機構は配備されている。

開発者がコミュニティに参加した後も、原則としてコミュニティへの貢献のみにより個人の評価がなされる。

(2) 不正動作の組み込み

意図的に不正動作をコードに組み込まれる可能性については、コミュニティによる差はなくレビュープロセスや承認プロセスにおける多くの目による相互監視により回避されている状況である。OSS コミュニティにとっては、この開発プロセスにて多くの目に晒されることで、自浄作用が働いているといえる。

(3) Linux ディストリビューションでのセキュリティ対策

Linux ディストリビューションでは OSS コミュニティよりコンポーネントとして取り込むパッケージのセキュリティ対策について関与はしない。ディストリビューション毎の自主対応に依存することとなるため、OSS コミュニティとディストリビューションとの連携の有無・強弱に関わらず OSS コミュニティ側での対策が必須である。

(4) ユーザーによる OSS 使用

OSS パッケージをコンポーネントとする Linux ディストリビューションから入手するにせよ、ユーザー自身で OSS パッケージを実装するにせよ、OSS の採否の判断はユーザーに委ねられている。

本調査の対象とした 3 コミュニティの実状を通じて見えてきた結果と課題について、体制及び技術の観点より以下に示す。

まず、体制面から OSS コミュニティのセキュリティリスクを俯瞰すると、異なる企業のメンバーによる確認体制や、開発とは異なるセキュリティチームを設け独立した確認体制をとっていることから、不正動作の意図的な混入は難しいと考えられる。一方で、リソースや資金力等の要因により、このような厳格なセキュリティ体制を組めないコミュニティが存在する可能性もある。

機器ベンダーをはじめとしたユーザーが OSS を利用するにあたり、OSS そのもののセキュリティ成熟度の定量的な評価は Blackduck Open Hub[180]や Bitergia[181]といった統計情報を一般に開示しているサービスが存在する。しかしながら、該当の OSS コミュニティについてセキュリティ観点での運用健全性を把握するには、本調査と同様の観点での確認を行う必要がある。ただし、第三者が今回のようなヒアリング調査を行うことは困難なため、主要なコミュニティについて同様の観点にて調査を行い、その情報を開示するスキーム作りが必要であると考えられる。

次に技術的観点から OSS のセキュリティ対策を考察する。今回調査対象とした 3 コミュニティでは、実施フェーズ毎に人的リソースとツールを使い分けながらセキュリティの観点でのチェックが実施されている。しかし、そのようなセキュリティチェックが行われているにも関わらず、OpenSSL で報告された Heartbleed、POODLE や、bash の shellshock、glibc の GHOST 等、OSS のソフトウェアバグを突いたセキュリティ脆弱性は数多く報告されている。これらのように、OSS 開発のセキュリティチェックで摘出できなかった不具合が存在したことを踏まえ、検査ツールの更なる向上が必要であると考えられる。

180 Black Duck: Open Hub
https://www.openhub.net
181 Bitergia: https://bitergia.com

7.5　ネットワークセキュリティ確保の方向性のまとめ

7.2～7.4 章の分析を踏まえ、ネットワークセキュリティ確保の方向性の案について考察する。

- 情報共有の仕組み作り
  - ソフトウェアの構成品の共有

    BSA/NTIA のソフトウェア透明性に関する活動を継続してウオッチしつつ、ソフトウェアの構成品の情報共有の仕組み作りを行うべきと考えられる。ただし、本情報が攻撃者に渡ると、潜在的な脆弱性情報の提供にもなるため取り扱いには十分な配慮が必要である。

  - ハードウェア、ソフトウェアの検査内容の共有

    上記とともに、ハードウェア、ソフトウェアの構成の検査内容の共有することで、重複した検査の削減についての仕組み作りを行うべきと考えられる。本情報を基に、セキュリティ対策が確認できないハードウェアやソフトウェアについては使用しないという選択も必要と考えられる。ただし本情報が攻撃者に渡ると、潜在的な脆弱性情報の提供にもなるため取り扱いには十分な配慮が必要である。

  - OSS コミュニティのセキュリティ対策状況の把握

    OSS コミュニティのセキュリティに関する体制面やプロセスについて調査を行い、情報共有するスキームの構築が必要と考えられる。

- 検査技術の研究・開発
  - ツールの検知精度の把握

    ツールには、それぞれの検出能力がある。そのためセキュリティ対策がどの程度行われているかを把握するためには、そのツールの特性を把握しておく必要があると考えられる。

  - ツールの検知精度の向上

    市販ツールで検出できない脆弱性について、検出可能なツールを開発することで、セキュリティレベルを高めるとともに、従来のツールの検出レベルをかいくぐる不正動作の埋め込みの検出・抑止を行うことも重要と考えられる。また不正動作については、それを検出する上で、情報収集とともに、実行手段の研究も重要と考えられる。

- 認証制度・評価機関の設置

  認証制度や評価機関の設置することにより、ある一定以上のセキュリティを確保するためには重要な役割を果たすことが期待できる。一方で、その基準を満たせばよいとも言えるので、通常の技術要件であれば、多くのベンダーは対応可能となる。セキュリティ対策にはコストを要するため、認証制度・評価機関の設置の検討にあたっては、対象ユーザー（重要インフラ、コンシューマー等）のリスクレベルに応じた要件の検討が必要と考えられる。

  また実施内容によっては一国で対応するにはコストがかかるため、各国や GSMA と連携した対応が必要と考えられる。ただし、今回の調査で評価機関の設立に否定的な国があるため、十分な検討が必要と考えられる。国内にも、コモンクライテリアの認証機関等あるため、要件によっては活用を行うべきと考えられる。

契約管理番号：１８１０２１２２－０