内閣官房におけるサプライチェーンのセキュリティ確保の取り組みとSIPへの期待

内閣官房内閣サイバーセキュリティセンター
副センター長・内閣審議官

山内 智生 氏

NISC National center of Incident readiness and Strategy for Cybersecurity

内閣官房におけるサプライチェーンのセキュリティ確保の取組とＳＩＰへの期待

令和元年10月31日

内閣官房　内閣サイバーセキュリティセンター（NISC）
副センター長・内閣審議官　山内 智生

サイバーセキュリティ政策の推進体制

内閣　内閣総理大臣

高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）

高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進

緊密連携

サイバーセキュリティ戦略本部（2015.1.9 サイバーセキュリティ基本法により設置）

本部長　内閣官房長官
副本部長　サイバーセキュリティ戦略本部に関する事務を担当する国務大臣
本部員　国家公安委員会委員長
総務大臣
外務大臣
経済産業大臣
防衛大臣
情報通信技術（ＩＴ）政策担当大臣
東京オリンピック競技大会・パラリンピック競技大会担当大臣※
有識者（８名；10名以下）
※平成27年７月22日付け内閣総理大臣決定により本部員に指定

閣僚が参画

- 遠藤　信博　日本電気株式会社代表取締役会長
- 小野寺　正　ＫＤＤＩ株式会社相談役
- 後藤　厚宏　情報セキュリティ大学院大学学長
- 中谷　和弘　東京大学大学院法学政治学研究科教授
- 野原佐和子　株式会社イプシ・マーケティング研究所代表取締役社長
- 前田　雅英　日本大学大学院法務研究科教授
- 宮澤　栄一　株式会社デジタルハーツホールディングス取締役会長
- 村井　純　慶應義塾大学環境情報学部教授

重要インフラ専門調査会
研究開発戦略専門調査会
普及啓発・人材育成専門調査会
サイバーセキュリティ対策推進会議（CISO等連絡会議）

緊密連携

国家安全保障会議（NSC）

我が国の安全保障に関する重要事項を審議

（事務局）

内閣官房　内閣サイバーセキュリティセンター（2015.1.9 内閣官房組織令により設置）

内閣サイバーセキュリティセンター長
（内閣官房副長官補(事態対処・危機管理)が兼務）
副センター長（内閣審議官）
上席サイバーセキュリティ分析官
サイバーセキュリティ参与

政府関係機関・情報セキュリティ横断監視・即応調整チーム（ＧＳＯＣ）
情報セキュリティ緊急支援チーム（CYMAT）

協力

＜重要インフラ所管省庁＞
金融庁（金融機関）
総務省（地方公共団体、情報通信）
厚生労働省（医療、水道）
経済産業省（電力、ガス、化学、クレジット、石油）
国土交通省（鉄道、航空、物流、空港）

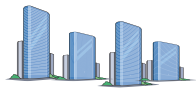
＜その他関係省庁＞
文部科学省（セキュリティ教育）等

協力

閣僚本部員５省庁

- 警察庁（サイバー犯罪・攻撃の取締り）
- 総務省（通信・ネットワーク政策）
- 外務省（外交・安全保障）
- 経済産業省（情報政策）
- 防衛省（国の防衛）


重要インフラ事業者等


政府機関（各府省庁）

企業


個人

サイバーセキュリティ戦略の概要

平成30年７月27日
閣 議 決 定

◆ 新たなサイバーセキュリティ戦略(2018年７月)は、サイバーセキュリティ基本法に基づく２回目の「サイバーセキュリティに関する基本的な計画」。2020年以降の目指す姿も念頭に、我が国の基本的な立場等と今後３年間（2018年～2021年）の諸施策の目標及び実施方針を国内外に示すもの
◆ サイバーセキュリティ2018は、同戦略に基づく初めての年次計画であり、各府省庁はこれに基づき、施策を着実に実施

＜新戦略(2018年戦略)（平成30年7月27日閣議決定）の全体構成＞

1 策定の趣旨・背景

- サイバー空間がもたらす人類が経験したことのないパラダイムシフト（Society5.0）
- サイバー空間と実空間の一体化の進展に伴う脅威の深刻化、2020年東京大会を見据えた新たな戦略の必要性

2 サイバー空間に係る認識

- 人工知能（AI）、IoTなど科学的知見・技術革新やサービス利用が社会に定着し、人々に豊かさをもたらしている。
- 技術・サービスを制御できなくなるおそれは常に内在。IoT、重要インフラ、サプライチェーンを狙った攻撃等により、国家の関与が疑われる事案も含め、多大な経済的・社会的損失が生ずる可能性は指数関数的に拡大

3 本戦略の目的

- 基本的な立場の堅持（基本法の目的、基本的な理念（自由、公正かつ安全なサイバー空間）及び基本原則）
- 目指すサイバーセキュリティの基本的な在り方：持続的な発展のためのサイバーセキュリティ（サイバーセキュリティエコシステム）の推進。３つの観点（①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働）からの取組を推進

4 目的達成のための施策

経済社会の活力の向上及び持続的発展
～新たな価値創出を支えるサイバーセキュリティの推進～

- 新たな価値創出を支えるサイバーセキュリティの推進
- 多様なつながりから価値を生み出すサプライチェーンの実現
- 安全なIoTシステムの構築

国民が安全で安心して暮らせる社会の実現
～国民・社会を守る任務を保証～

- 国民・社会を守るための取組
- 官民一体となった重要インフラの防護
- 政府機関等におけるセキュリティ強化・充実
- 大学等における安全・安心な教育・研究環境の確保
- 2020年東京大会とその後を見据えた取組
- 従来の枠を超えた情報共有・連携体制の構築
- 大規模サイバー攻撃事態等への対処態勢の強化

国際社会の平和・安定及び我が国の安全保障への寄与
～自由、公正かつ安全なサイバー空間の堅持～

- 自由、公正かつ安全なサイバー空間の堅持
- 我が国の防御力・抑止力・状況把握力の強化
- 国際協力・連携

横断的施策

- 人材育成・確保
- 研究開発の推進
- 全員参加による協働

5 推進体制

内閣サイバーセキュリティセンターを中心に関係機関の一層の能力強化を図るとともに、同センターが調整・連携の主導的役割を担う。

現状認識と将来像（サイバー空間と実空間の一体化に伴う脅威の深刻化）

中長期

策定の趣旨・背景

【（2015年戦略策定時）連接融合情報社会の到来】
～実空間のヒト・モノがネットワークに**連接**され、
実空間とサイバー空間の**融合**が高度に深化～

一体化

【サイバー空間と実空間の一体化、活動空間の拡張】

サイバー空間に係る認識

・AI、IoT 、Fintech 、ロボティクス、３Dプリンター 、AR/VR など、**サイバー空間における知見や技術・サービスが社会に定着し**、経済社会活動・国民生活の既存構造に変革をもたらす**イノベーションを牽引する一方で、不確実さは常に内在**

サイバー空間がもたらす恩恵

・サイバー空間における技術・サービスが**制御され、様々な分野で当然に利用されており、人々に豊かさをもたらしている**。
・深層学習による**AIの進化**により、既に幅広い産業に応用され始めている。
・**IoT機器で得られるデータ**を利活用した新たなビジネスやサービスが創出されつつある。

サイバー空間における脅威の深刻化

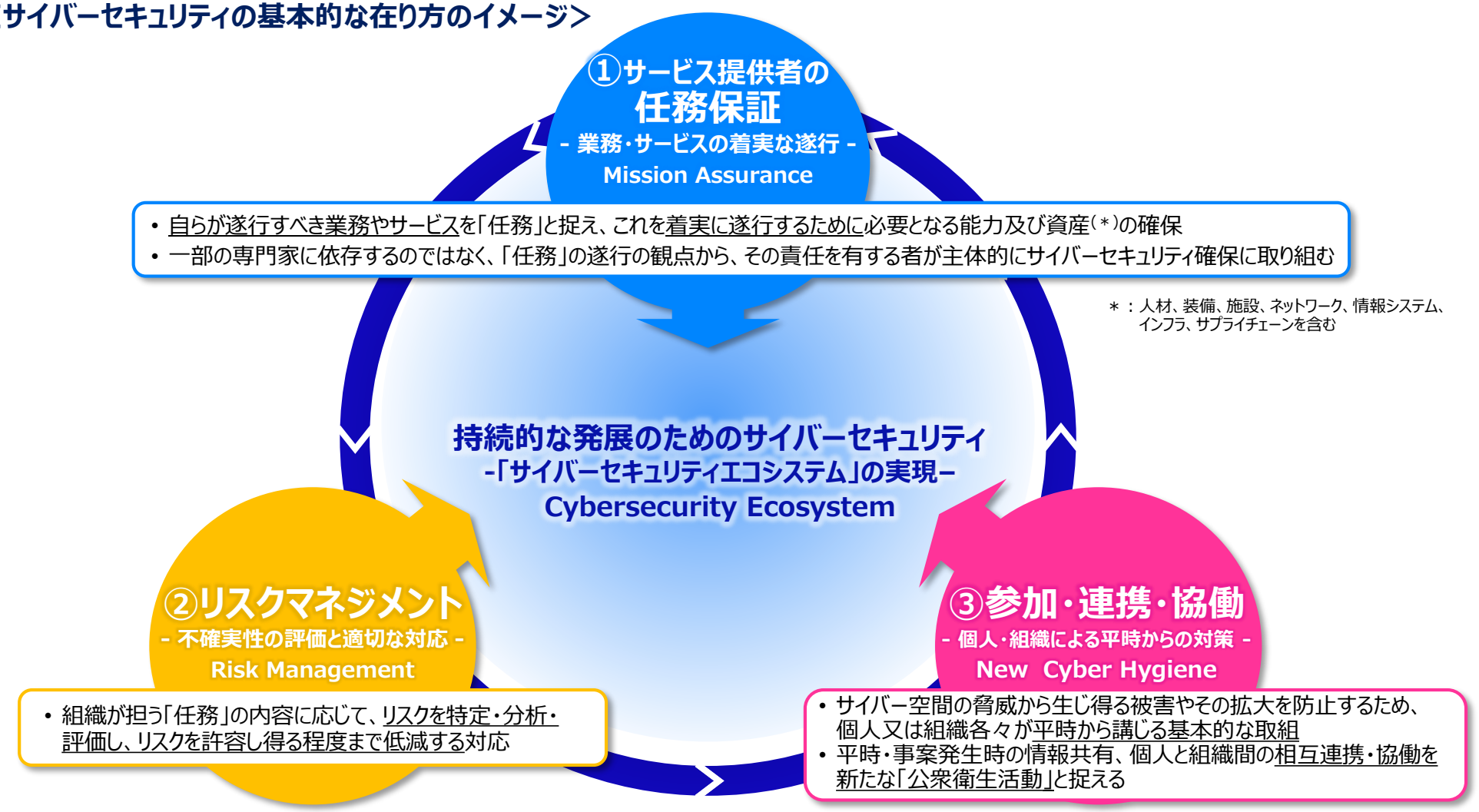
・サイバー空間における技術・サービスを**制御できなくなるおそれは常に内在しており、多大な経済的・社会的な損失が生じ得る。**
・重要インフラサービスの障害やIoT機器の意図しない作動により、様々な**業務・機能・サービス障害が生じた場合、社会に大きな影響が生じ、国家安全保障上の問題**に発展する可能性
・サイバーセキュリティ対策の不備が、**金銭的な損害を直接引き起こし**、拡大することが予想される。

目指す姿（持続的な発展のためのサイバーセキュリティ　–「サイバーセキュリティエコシステム」の実現- ）

○　新しい価値やサービスが次々と創出されて人々に豊かさをもたらす社会（Society5.0※）の実現に寄与するため、実空間との一体化が進展しているサイバー空間の持続的な発展を目指す（「サイバーセキュリティエコシステム」の実現）。

○　このため、これまでの基本的な立場を堅持しつつ、３つの観点（①サービス提供者の任務保証、②リスクマネジメント、③参加・連携・協働）から、官民のサイバーセキュリティに関する取組を推進していく。

＜サイバーセキュリティの基本的な在り方のイメージ＞



IT調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ等について

■ サプライチェーン・リスクとは

- 情報通信機器等の開発や製造過程において、情報の窃取・破壊や、情報システムの停止等の悪意のある機能が組み込まれる懸念。
- さらに、納入後においても、情報システムの特徴として、事後的な運用・保守作業により、製造業者等が修正プログラムを適用する等、調達機関が意図しない、不正な変更が行われる可能性。

■ サプライチェーン・リスク対策の重要性

- 「サイバーセキュリティ戦略」において、サプライチェーン・リスク対策の重要性について言及。
- 「政府統一基準群」において、サプライチェーン・リスク対策に係る考え方を記載。

～ 政府機関等の対策基準策定のためのガイドラインの解説（遵守事項5.1.2(1)(a)”「不正な変更が加えられない」について”に係る解説）から抜粋 ～

「開発・製造過程において悪意ある機能が組み込まれる懸念が払拭できない機器等、及びサプライチェーン・リスクに係る懸念が払拭できない企業の機器等を調達しないことが求められる。」

■ 「サプライチェーン・リスク対策」のより具体的な方策として全省庁による「申合せ」を決定。

（平成３０年１２月１０日　サイバーセキュリティ対策推進会議（第16回）各府省情報化統括責任者連絡会議（第81回）合同会議）

１．適用対象：重要性の観点から５類型を提示。

２．適用時期：平成31年度予算に基づき平成31年４月１日以降に調達手続（公告等）が開始されるもの。

３．調達手続の流れ：

- 「総合評価落札方式」や「企画競争」等を用い、RFIやRFPといった事前の情報取得や、審査の過程において、必要な情報を入手し評価することにより、サプライチェーン・リスク対策を実施。
- 必要に応じて、情報通信技術（ＩＴ）総合戦略室及び内閣サイバーセキュリティセンターから、講ずべき必要な措置について助言を実施。

① **国家安全保障及び治安関係**の業務を行うシステム
② **機密性の高い情報を取り扱う**システム並びに情報の漏洩及び情報の改ざんによる**社会的・経済的混乱を招くおそれのある情報を取り扱う**システム
③ **番号制度関係の業務を行う**システム等、**個人情報を極めて大量に取り扱う**業務を行うシステム
④ 機能停止等の場合、**各省庁における業務遂行に著しい影響を及ぼす**基幹業務システム、LAN等の基盤システム
⑤ **運営経費が極めて大きい**システム

（参考）IT調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ

■ 「サイバーセキュリティ戦略」等における、サプライチェーン・リスク対策関連記述。（一部）

【サイバーセキュリティ戦略（平成30年7月27日閣議決定）】

4. 目的達成のための施策

4.2 国民が安全で安心して暮らせる社会の実現

4.2.3 政府機関等におけるセキュリティ強化・充実

（略）

複雑化・巧妙化しているサイバー攻撃に対しては、引き続き攻撃を前提とした多層防御や、サプライチェーンリスクへの対応を強化するとともに、新たな技術を活用し、従来の攻撃側優位の状況を改善するための取組を進めることが求められる。

（略）

【政府機関等の対策基準策定のためのガイドライン（平成30年度版）（平成30年7月25日）】

5.1.2 機器等の調達に係る規定の整備

遵守事項

(1) 機器等の調達に係る規定の整備

(a) 統括情報セキュリティ責任者は、機器等の選定基準を整備すること。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を機関等が確認できることを加えること。

（解説） 遵守事項5.1.2(1)(a)「不正な変更が加えられない」について

機関等は、機器等の開発や製造過程において、情報の窃取・破壊や情報システムの停止等の悪意ある機能が組み込まれるサプライチェーン・リスクの懸念が払拭できない機器等を調達しないようにする必要がある。このサプライチェーン・リスクに対応する方法として、機関等が、国内外の情報セキュリティに関する情報を収集し、こうした知見をもとにサプライチェーン・リスクを当該調達に関する要件の一つとして取り上げることにより、開発・製造過程において悪意ある機能が組み込まれる懸念が払拭できない機器等、及びサプライチェーン・リスクに係る懸念が払拭できない企業の機器等を調達しないことが求められる。

このような対応をする手段の一つとして、政府調達において、相対の交渉が可能な契約であれば、調達に係る契約の相手方に対して、サプライチェーン・リスクに係る十分な知見をもとに、機器等に関し必要な要件を備えるべく、交渉を通じて個別に求めることが考えられる。

なお、上記の場合においても、関係する国内法令（会計法、予算決算及び会計令、国の物品等又は特定役務の調達手続の特例を定める政令・省令等）及び関係する国際協定（政府調達に関する協定を改正する議定書等）を遵守する必要がある。

「サイバーセキュリティ研究・技術開発取組方針」（概要）

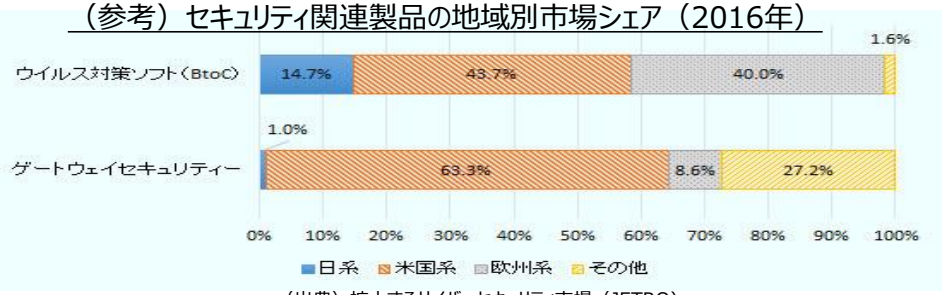
令和元年5月23日
サイバーセキュリティ戦略本部報告

「サイバーセキュリティ戦略」（平成30年（2018年）7月閣議決定）に基づき、戦略期間中の実践的な研究・技術開発に関する取組の具体化を図るという目的のもと、研究開発戦略専門調査会において**「サイバーセキュリティ研究・技術開発取組方針」を策定**。

取り組むべき課題

(1)**サプライチェーンリスク**の増大
(2)**サイバーセキュリティ自給率**の低迷
(3)研究・技術開発に資する**データの活用**
(4)先端技術開発に伴う**新たなリスク**の出現
(5)**産学官連携**強化の必要
(6)**国際標準化**の必要

（参考）セキュリティ関連製品の地域別市場シェア（2016年）



（出典）拡大するサイバーセキュリティ市場（JETRO）
https://www.jetro.go.jp/biz/areareports/2018/1fb2ecd606c590e5.html

今後の取組強化の方向性

①サプライチェーンリスクへ対応するための オールジャパンの技術検証体制の整備

・ICT機器・サービスの信頼性・有効性を検証するためのオールジャパンの体制整備
・ハードウェア・ソフトウェア両面の検証技術の研究開発・実用化（5Gセキュリティ、チップ脆弱性検知、エッジからクラウドに至るまでのハードウェアセキュリティ）

②国内産業の育成・発展に向けた支援策の推進

・「Proven in Japan」の推進に向けた、日本発のサイバーセキュリティ製品・サービスの創出・活用及び信頼性を検証するための包括的検証基盤の構築
・中小企業のニーズに対応したビジネス創出のための支援（サイバーセキュリティお助け隊、コラボレーション・プラットフォーム）

③攻撃把握・分析・共有基盤の強化

・サイバー攻撃を迅速に把握するための観測技術の高度化や、AI等の活用による分析・解析技術の効率化・自動化（NICTER、STARDUST等）
・サイバー攻撃の把握・分析データを共有する基盤（CURE）構築

④暗号等の基礎研究の促進

・耐量子計算機暗号や量子暗号等の安全なセキュリティ技術、IoTデバイスにて活用可能な暗号技術の研究・開発
・暗号技術、暗号・セキュリティ製品やモジュール認証等の国際標準化促進

⑤産学官連携の研究・技術開発のコミュニティ形成

・産学官によるコミュニティの形成及び諸外国との連携に向けた検討

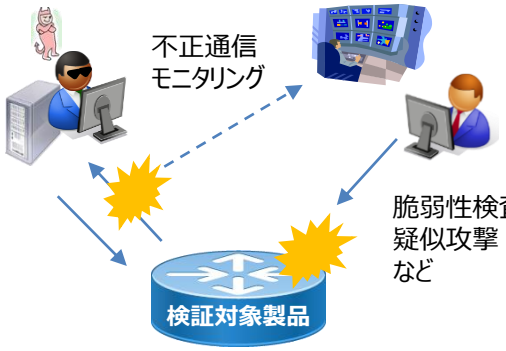
・上記の取組強化の方向性に沿って、関係省庁が連携して、具体的・実践的な研究開発を推進
・個別の研究・技術開発の成果の創出に留まらず、**社会実装までのプロセスを念頭に置きつつ推進**するとともに、**国民社会におけるサイバーセキュリティに関する意識向上**に向けた取組も併せて実施
・研究開発戦略専門調査会において**定期的に評価**を行い、**必要に応じて方針の見直しを実施**

サプライチェーンリスクへ対応するためのオールジャパンの技術検証体制の整備

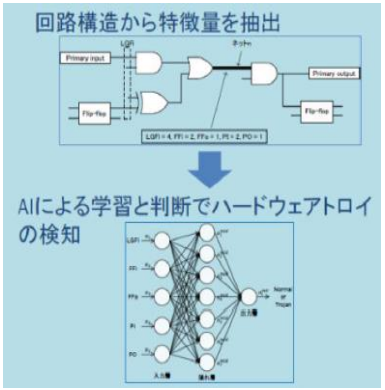
- Society5.0の進展、サイバー攻撃の複雑化・巧妙化に伴い、サプライチェーンリスクの問題が顕在化。諸外国においても、対応強化のための取組が進められている。
- 我が国においても、ICT機器の信頼性を検証するための技術開発と推進体制の構築を進め、サプライチェーンリスクに対応するための技術検証体制の整備を推進することが必要。

（１）検証技術の開発

脆弱性、不正機能のチェック

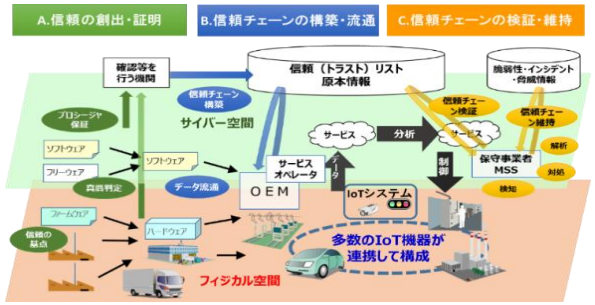


ハードウェアトロイの検出



信頼性・安全性確保のための基盤構築

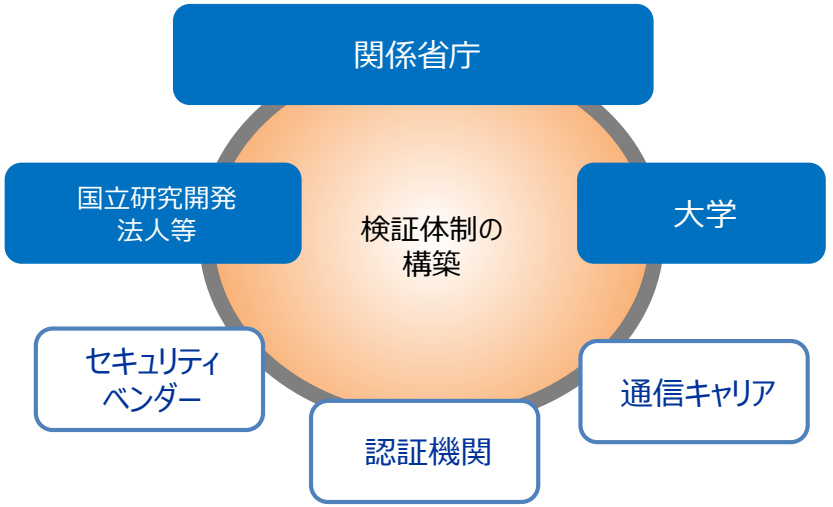
サプライチェーン全体を守るための『サイバー・フィジカル・セキュリティ対策基盤』の開発



（２）推進体制の整備

推進体制の整備

オールジャパンの官民連携体制の構築



検証結果の活用方策の推進

政府機関や重要インフラ事業者等のシステムで活用するための措置を推進

SIPへの期待

①社会実装

既に実証評価ＷＧにおける検討をはじめとして、取組が進められていると認識。どの課題も、社会実装を見据えた取組を早い段階から行い、最終的に、国民が実感するインパクトある成果を社会に還元すべく、一丸となった取組を期待。

②関係府省による社会実装へのサポート

参画事業者による社会実装への取組に対しては、関係府省が一丸となってサポートをしていくことが重要。

③新たな知識の共有と人材育成

社会実装を見据えた取組とともに知的財産の適切な確保等が前提としても、研究開発から生まれる新たな知識は、人類の財産として積極的に学会等で発表し国際社会における我が国研究開発コミュニティの存在感を示していただくことを期待。

これにより、次世代を担う人材育成確保を含めて、大型プロジェクトの波及効果を次につなげることに期待。