サイバー・フィジカル・セキュリティ
対策検討ガイドブック

セキュリティ製品導入のための手引き

2023年2月

内　閣　府

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・セキュリティ社会実装WG

本資料は、内閣府が進める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」（研究推進法人：NEDO）によって作成されました。

目　次

図表目次

はじめに

1 目的

内閣府が進めたSIP 第2期では、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「サイバー・フィジカル・セキュリティ対策基盤」を研究開発しました。目的は、実稼働するサプライチェーンに組み込み実用化することで、サイバー脅威に対するIoT社会の強靭化を図ることです。現実の世界である「フィジカル」空間の膨大かつ多様なデータをコンピュータで作られた仮想空間である「サイバー」空間に収集し、蓄積・分析・融合・フィードバックを行うことで価値創造及び課題解決に寄与する「サイバー・フィジカル・システム」が対象となります。

本ガイドブックでは、IoTやOTに関するサイバー・フィジカル・セキュリティに関わる具体的事例の分析を通じて、企業や組織にとって身近な課題への気付きをうながし、SIP第2期で研究開発したサイバー・フィジカル・セキュリティ技術に関心を持っていただくことを目的としています。

IoTとは、Internet of Thingsの略称であり、本ガイドブックでは「固有にIPアドレスを持ち、単体または別の機器を用いてネットワークに通信で繋がっている機器」をIoT機器と定義しています。IoT機器の代表例として、スマート家電、自動運転車、産業用ロボット等が挙げられ、「IoTセキュリティガイドライン（2016年7月）」[1]では、IoT機器の特有の性質と想定されるリスクとして以下の特徴が挙げられています。

- （インターネット等のネットワークに接続していない機器に比べ）脅威が物理的に影響を与える範囲・度合いが大きい
- （IoT機器として利用される製品は10年以上と）ライフサイクルが長い場合が多く、セキュリティ対策が時代遅れとなる可能性がある
- （パソコン等のように画面がなく可視化されにくいことから）IoT機器に対する監視が行き届きにくい
- （IoT 機器側とネットワーク側の環境や特性の相互理解が不十分であり）所要の安全や性能を満たせないことがある
- センサー等IoT 機器は小規模化や省エネ化のため、搭載機能や性能が限定される
- （これまで外部につながっていなかったモノがネットワークに接続され）機器やシステムの開発者が想定していなかった影響がでる

1 「IoTセキュリティガイドライン」はIoT推進コンソーシアム、総務省、経済産業省の3者の連名で公表されている。

OT とは、Operational Technology の略称であり、本ガイドブックでは「工場やプラント等の機械設備や生産工程を制御する運用制御技術」と定義しています。OT 機器の代表例として PLC（機械自動制御装置）、SCADA（監視制御システム）、DCS（分散制御システム）が挙げられます。

以下は、OT で多くみられる特有の性質になります。

- 10 年以上利用している機器が多い
- 古いバージョンの Windows が利用されており、定期パッチも適用されていない
- 暗号化されていないパスワードが使用されている
- アンチ・ウイルスソフトの定義ファイルが常に最新の状態になるよう自動更新されていない
- リモートアクセスからの攻撃を検知することができないデバイスが存在している
- IoT や OT デバイスがインターネットに直接接続している
- OT ネットワークの監視を実施していない
- OT 専任のセキュリティ担当者がいない

経営層の方々には、本ガイドブックによって、自社のサイバー・フィジカル・セキュリティ対策の必要性を理解いただくことを期待しています。また、責任者（及び担当者）の方々には、サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）[2]と併せて、本ガイドブックに基づいて「どのような活動を進めていくべきか」具体的に検討していただくことを想定しています。

2　2019 年 4 月、経済産業省は「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）を策定した。このフレームワークは、サイバー空間とフィジカル空間を高度に融合させた「Society 5.0」や様々なつながりによって新たな付加価値を創出する「Connected Industries」における新たなサプライチェーン全体のセキュリティ確保を目的として、産業に求められるセキュリティ対策の全体像を整理したもの。

2 本ガイドブックの対象読者

本ガイドブックは企業や各種団体の経営者と導入運営の責任者や担当者を対象に、企業規模は限定せず、幅広く読んでいただくことを想定しています。

IoT 社会では複数の IoT 機器やシステムによってサイバー空間とフィジカル空間が双方向に通信を行い、高度な機能を実現するため、様々な企業がサービス提供に関わっています。そのため、所属する企業・組織についてサイバー・フィジカル・セキュリティ対策の必要がないか、確認する必要があります。例えば、図表 1 の例に該当するシステムがある場合は対策が必要です。

図表 1　サイバー・フィジカル・セキュリティの対象となるシステムの例（製造業の場合）

#	データの動き	サイバー・フィジカル・セキュリティの対象となるシステムの例
1	フィジカル ⇒サイバー	IoT デバイスから制御システムへのインプットがある
2	サイバー ⇒フィジカル	制御システムからロボットやドローンへのアウトプットがある
3	サイバー ⇔サイバー	IoT デバイス、ロボット、ドローン、及びその関連システムに対して以下の対応がある ● 遠隔保守 ● 遠隔からのソフトウェア更新

（出典）IPA「スマート工場のセキュリティリスク分析調査 調査報告書」を参考に作成

例えば、スマート工場では、産業向けデバイス製造企業から製造された IoT デバイスを多数設置し、電子部品製造企業が製造したセンサーや、通信モジュール製造企業が製造した通信モジュールを通じて作業の進捗状況のデータを収集します。収集されたデータは通信･ネットワーク企業の無線・有線通信サービスを通じて、IoT プラットフォーム企業のデータ分析サーバーに集約され、作業工程の進捗を最適化するために調査・分析が行われます。アプリケーション企業は各産業・用途別 に個別のアプリケーションを開発・提供し、工場勤務者は最適化されたデータに基づいた画面を参照して作業工程の改善を図り、工場内のロボットやアクチュエータの動作制御を実施します。

このように、IoT 機器 1 つとっても、デバイス製造企業、電子部品製造企業、通信モジュール製造企業、通信・ネットワーク企業、IoT プラットフォーム企業、アプリケーション企業、工場勤務者等多数の関係者が関与しており、上記事例に限らず幅広い業界の方々が対象読者となり得ます。

3 本ガイドブックの全体構成

本ガイドブックは、本編4章と付録により構成されています（図表2）。付録には、本ガイドブックで紹介している各技術説明を掲載しています。

図表2　本ガイドブックの全体構成

構成	対象読者	概要
第1章 IoTやOTシステムの危険性	経営層	● IoTやOTのサイバー・フィジカル・セキュリティに関する危険性等、経営層が把握しておくべき事項や自らの責任で実践しなければならない事項について説明しています。
第2章 IoTやOTに関するサイバー・セキュリティ対策の現状	セキュリティ責任者（担当者）	● 自社の置かれている状況を把握するために、IoTやOTのサイバー・フィジカル・セキュリティに関する脅威や省庁や業界団体における対応状況について説明しています。
第3章 SIP技術を用いたサイバー・フィジカル・セキュリティの対策例		● IoTやOTに関する主要なサイバー・セキュリティの脅威に対応する解決策について、「サイバー・フィジカル・セキュリティ対策基盤」の各ソリューションを題材に具体例を説明しています。
第4章 対策の企画・導入の進め方		● サイバー・フィジカル・セキュリティ・対策フレームワークのセキュリティ・リスクマネジメントの流れを参考に、検討の流れを説明しています。 ● 現状のサイバー・フィジカル・セキュリティ対策の十分性を確認するためのチェック項目例を用意しています。

第1章
IoTやOTシステムの危険性

☑ ポイント①
サイバー・セキュリティ対策が十分でないIoT機器やOTシステムにより、経営が危険にさらされています。

☑ ポイント②
サイバー・セキュリティ対策の不備により、企業や経営者は法的責任に問われる可能性があります。

☑ ポイント③
IoT機器やOTシステムに対するサイバー・セキュリティ対策を検討するため、経営者は担当者の設定やその担当者への指示を行う必要があります。

1.1. 近年のサイバー攻撃の傾向

従来、完全にクローズドなネットワーク環境（閉域網）を確立しているためサイバー攻撃の恐れはないとされていた重要インフラやその制御機器は、様々な機器のネットワークへの接続やリモートメンテナンスの発生により、閉域網での運用が困難になってきています。

IoT 機器等への攻撃増加は閉域網への攻撃増加にも影響しています。さらに、閉域網に設置された機器は安全と考えられていたことから、OS 等にセキュリティパッチ等定期的なアップデートが適用されていない、あるいは古いアプリケーションが継続利用されているといった状況があります。

自社ネットワークや接続されている機器に対して必要と考えられる対策が講じられている場合でも、導入機器の製造や運用におけるサプライチェーン上で対策が不十分な企業が存在する場合は、その企業から脆弱性を持つ部品やソフトウェアが混入する可能性があります。

比較的セキュリティ対策が進んでいると言われている自動車業界であってもセキュリティ事案が発生しており、従来の対策だけでは不十分であることを示唆しています。サイバー攻撃を受けた企業には、一般的にサイバー攻撃の被害として想起される個人情報や企業の重要情報等の情報流出のみならず、一定期間の業務停止もしくは一部の業務制限が発生してしまう可能性があります。

被害発生時の社会的なインパクトが大きい重要インフラ分野においても、サプライチェーンを起因とした攻撃が発生しています（図表 3）。

図表 3　近年の重要インフラ分野へのサイバー攻撃事例

#	発生年	事例	事例の概要
1	2021 年	外部委託先の ランサムウェア被害	**【サプライチェーン起因】** 外部委託先がランサムウェアに感染したことで、重要インフラ事業者の情報が漏えいした可能性が発覚
2	2021 年	ネットワークを経由した マルウェア感染	**【サプライチェーン起因】** 子会社のサーバーがマルウェア感染し、グループ間ネットワークを経由して重要インフラ事業者のサーバーが感染
3	2021 年	VPN ルーターの脆弱性を悪用したランサムウェア感染	**【サプライチェーン起因】** 委託先事業者が設置した VPN ルーターの脆弱性を悪用して侵入された後、ランサムウェアにより暗号化
4	2020 年	連携サービス間の脆弱性を突いたサービスの不正利用	**【サプライチェーン起因】** 利用者から身に覚えのないサービスの利用履歴があるとの問合せを重要インフラ事業者が短期間に複数受領。原因は、サービスを連携する他事業者の仕様変更により生じた連携サービス間の脆弱性の悪用と判明

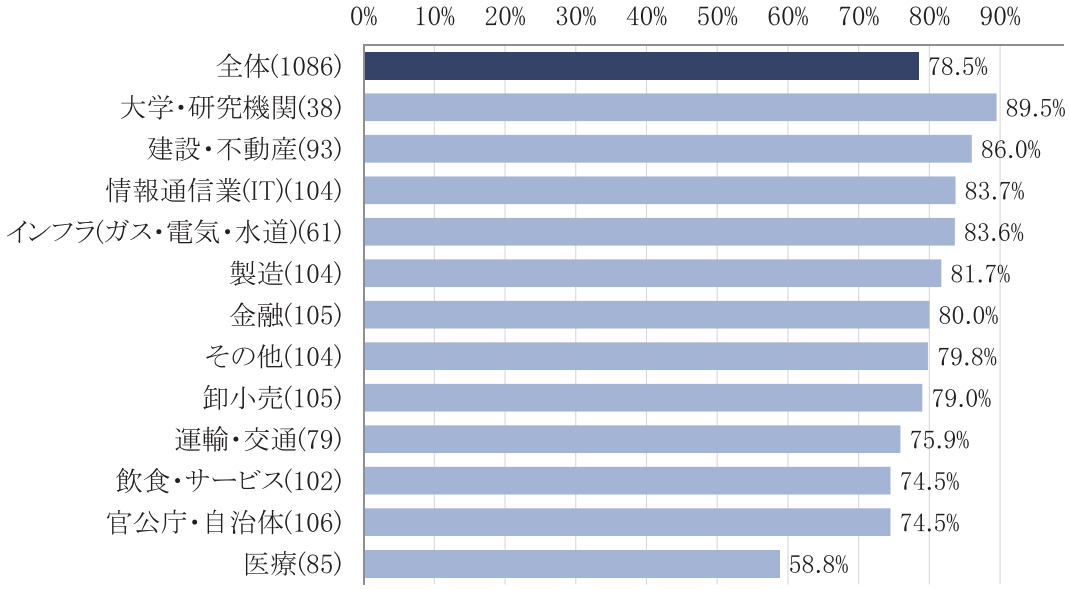
（出典）内閣官房 内閣サイバーセキュリティセンター（NISC）「2020 年度 重要インフラにおける補完調査について」(2021 年 5 月)、「2021 年度 重要インフラにおける 補完調査について」(2022 年 5 月）

1.2. 攻撃における被害の拡大

近年のサイバー攻撃はあらゆる業種、あらゆる規模の企業を狙っており、その被害は拡大しています。例えば、2022 年、大手食品･飲料メーカーでは、使用していた SSL-VPN（Secure Socket Layer-Virtual Private Network）[3] 機器の脆弱性を利用した不正侵入により、社内サーバーがランサムウェアに感染し、EC（電子商取引）サイトが停止する事態に発展しました。警察や個人情報保護委員会への相談や届け出、外部の専門家による原因究明の調査等、様々な対応が行われ、EDR（Endpoint Detection and Response）[4] や MDR（Managed Detection and Response）[5] といったセキュリティ対策が導入されました。

トレンドマイクロの「法人組織のセキュリティ動向調査 2020 年版」（対象：自組織のインシデント状況を把握しているリスク管理・IT システム・情報セキュリティ担当者　計 1,086 人（民間企業：980 人、官公庁自治体：106 人））によれば、（何かしらのセキュリティ・インシデントを経験した）セキュリティ・インシデントの発生率は全体で見ると約 8 割を占めました（図表 4）。また、損失額だけではなく調査費用、改善策の導入、損害賠償等の事後対応を含め 1 社あたりの年間平均被害額は約 1 億 4,800 万円という結果が出ています。

図表 4　セキュリティ・インシデント発生率（業種別）



（出典）トレンドマイクロ「法人組織のセキュリティ動向調査 2020 年版」（2020 年 10 月）

3　インターネット上に仮想の専用線を設定して特定の人のみが利用できる専用ネットワーク（VPN）を SSL（Secure Sockets Layer）技術を使用して利用すること
4　コンピュータシステムのエンドポイント（端末や機器）においてを継続的に監視して対応する技術
5　EDR 製品をマネージドサービスで提供したものを MDR と呼ぶことが多い

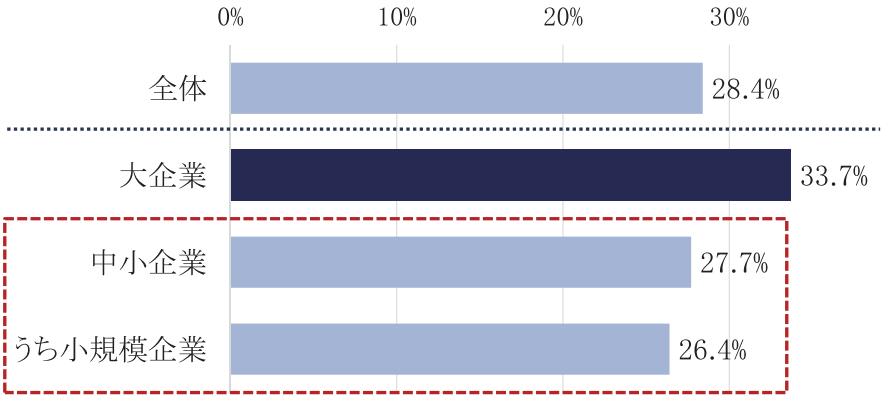
被害を受けた場合には、個人情報保護委員会への申告（個人情報流出の場合）や所轄警察署への被害申告が必要となります。さらに、不正アクセスを受けた企業や団体は、フォレンジック等原因特定や被害範囲特定を行うための調査が必要となります。EC（電子商取引）サイトへの不正アクセスを受けた中小企業が、外部に委託した場合の費用は 100 ～ 500 万円程度で、200 ～ 249 万円が最も多くなっています。

被害発生時の対応を経営者一人で行うことは不可能であるため、上記のような報告、プレスリリース、報道対応調査や対策チーム等を設置・運営するための人的コスト、及び新しいセキュリティソリューションの導入や社員に対する教育徹底等再発防止策の導入に多額のコストがかかります。

直接的な被害への対応によってコストが発生するだけでなく、通常業務が行えなくなることや風評被害による機会損失は売上減少に直結することから、経営管理事項として喫緊の課題となります。適切なソリューションを導入することができれば、IoT や OT への不正アクセスからの防御、もしくは早期検知や一次対処により被害を最小限に留めることができます。近年は、リスク回避や軽減の手段として、サイバー保険への加入も増加しています。

2022 年 3 月に帝国データバンクにて実施された「サイバー攻撃に対する実態アンケート」では、アンケート回答日を起点として 1 カ月以内に攻撃を受けた企業は 28.4%、中小企業においても 27.7% 存在し、サプライチェーンの事業活動に支障が出た例もあったとの結果が出ています（図表 5）。

図表 5　1 か月以内にサイバー攻撃を受けた割合（規模別）



（出典）帝国データバンク「サイバー攻撃に対する実態アンケート」（2022 年 3 月）

さらに、IoT や OT へのサイバー攻撃を受けた業種によっては、社会全体への被害が発生する可能性もあります。例えば、医療、化学、インフラ業界だった場合、死亡事故や環境汚染等の発生も考えられます。 2022 年 10 月には、「高度救命救急センター」クラスの医療機関が「ランサムウェア」とみられるサイバー攻撃を受けたことで患者の個人情報や治療内容を記録した電子カルテが機能しなくなり、一般外来業務を受けられない状況となりました。旧式だったソフトウェアの脆弱性を突かれたことが要因として挙げられています。高度救命救急センターが停止になることにより救急患者の受入れもできなくなる等、医療業界へのサイバー攻撃は患者の生命を奪う深刻なものとなりかねない状況となっています。

Gartner によれば、被害に遭う人命の価値を除いても、損害賠償、訴訟費用、保険費用、規制上の罰金、評判の低下等で発生するコストは莫大なものになり、2023 年には、サイバー・フィジカル・システムへの攻撃による財務的な影響は 500 億ドルを超えると予想されています[6]。

以上のように、サイバー・フィジカル・システムへの攻撃は企業経営に甚大な損害を与える可能性があります。また、対応状況によっては、会社が十分な安全管理措置を取っていない、善管注意義務を怠っているとして、企業や経営層が被害者から訴えられる可能性も考えられます。訴訟になった場合、報道や SNS 等に取り上げられることで、訴訟内容や最終的な判決に関わらず、企業の信用やブランド価値の低下につながります。

このような企業経営上の被害を防ぐために、まずは責任者や担当者の任命や対策検討の指示が必要となります。経団連から公表されている取締役向けの「サイバーリスクハンドブック」に記載されている 5 つの原則の中には「十分な人員と予算を投じて、全社的なサイバーリスク管理の枠組みを確立すべきである。」と記載されていることから[7]、経営者は経営責任を果たすために、全社的なリスク管理の問題として組織的に取り組むことが求められています。

近年のサイバー攻撃の傾向や被害については、「2.1 節　サイバー・フィジカル・システムの急速な増加」でも詳しく述べていますので、是非ご参照ください。

6　Gartner, 'Predicts 2020: Security and Risk Management Programs'（2020 年 9 月）
https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75--of-ceos-will-be-personally-liabl
7　一般社団法人日本経済団体連合会「サイバーリスクハンドブック　取締役向けハンドブック 日本版」
https://www.keidanren.or.jp/policy/cybersecurity/CyberRiskHandbook.html

第2章
IoTやOTに関するサイバー・セキュリティ対策の現状

☑ ポイント①
サイバー・フィジカル・システムの急速な普及によってサイバー・セキュリティの脅威が増大しています。

☑ ポイント②
IoT機器やネットワーク機器等の様々な機器が攻撃の踏み台として活用されているため、注意が必要となっています。
（「閉域網だから安心」にはなりません）

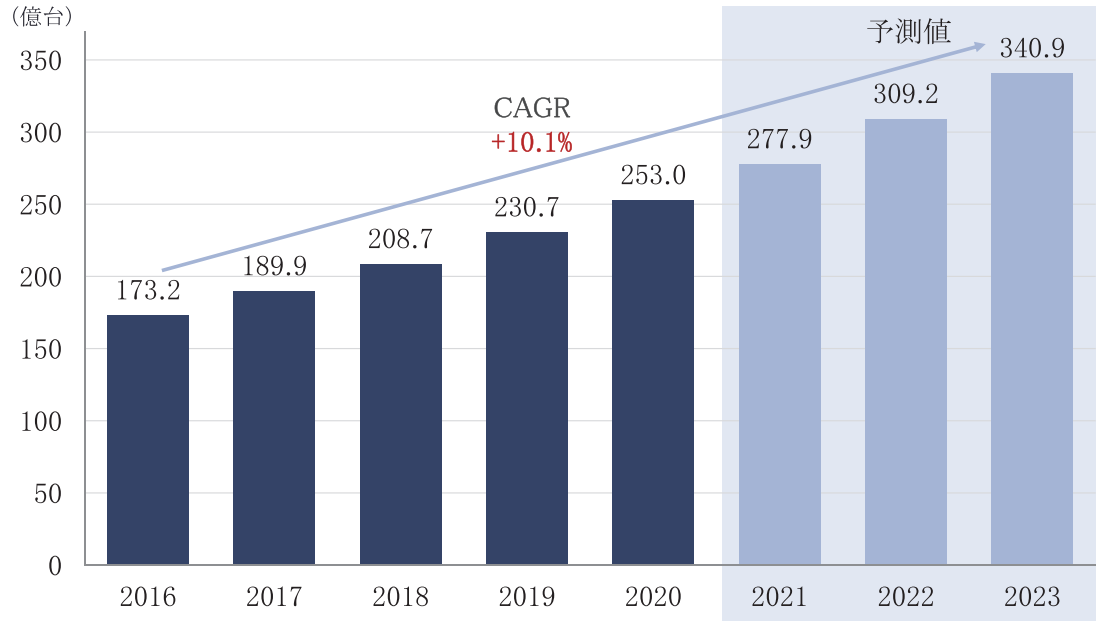
☑ ポイント③
『サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）』が公表されただけでなく、様々な規格やガイドラインに反映されてきています。

2.1. サイバー・フィジカル・システムの急速な普及

AI、IoT 技術の進展に伴い、現実世界をセンサーで把握し、AI で付加価値を加えてフィードバックする「サイバー・フィジカル・システム（CPS）」[8] と呼ばれる機器やサービスが増えてきています。

総務省が 2021 年 7 月に発表した調査レポート「令和 3 年版情報通信白書　IoT デバイスの急速な普及」では、世界の IoT デバイス数の推移及び予測について、2016 年の実績は 173.2 億台、その後、2016 年～ 2023 年の年間平均成長率（CAGR）が 10.1％で成長し、2023 年には 340.9 億台に達すると予想されています（図表 6）。

図表 6　世界の IoT デバイス数の推移及び予測



（出典）総務省「令和 3 年版情報通信白書　IoT デバイスの急速な普及」（2021 年 7 月）

この動きを受け、我が国では、第 5 期科学技術基本計画（2016 年 1 月 22 日閣議決定）にて、「情報社会（Society 4.0）」に続く、目指すべき未来社会の姿として、「超スマート社会（Society 5.0）」[9] が提唱されました（図表 7）。「Society 5.0」が実現された社会では、フィジカル空間のセンサーからの膨大な情報がサイバー空間に集積されます。サイバー・フィジカル・シス

8　CPS とは、IoT の技術革新により、実世界（フィジカル空間）にある多様なデータをセンサーネットワーク等で収集し、サイバー空間で大規模データ処理等を駆使して分析／知識化を行い、そこで創出した情報や価値によって、産業活性化や社会問題を図っていくという相互連関を指す。

9　「Society 5.0」の詳細については、「サイバー・フィジカル・セキュリティ対策 フレームワーク ver1.0」「はじめに」を参照。

テムでは、フィジカル空間から得られた情報を基に AI 等を用いて判断の高度化やテーラーメイド化を行うことで、フィジカル空間においては多様なニーズにきめ細かに対応した製品やサービスを提供することが可能となります。

図表７　「Society 5.0 のしくみ」

（出典）内閣府「Society 5.0 のしくみ」

2.2. サイバー・フィジカル・システムの急速な普及に伴う課題

「Society 5.0」では新たな価値が提供される一方、以下のような問題が生じることから、適切な対策を行うことが重要な課題となります。

① 様々なデータの企業間流通量増加による情報漏えいの可能性増大

サイバー空間とフィジカル空間は相互に作用し合うため、近年のサイバー攻撃の対象拡大に伴ってフィジカル空間に及ぼす影響は増大しています。サイバー空間とフィジカル空間の高度な融合に伴って発生する新たなサービスや機器が、サイバー攻撃の新たな対象として顕在化していることを認識する必要があります。

＜対策例＞

▶ 3.5 節 不適正な組織・事業者の接続への対策
付録 ソリューション④：信頼できる取引ネットワーク構築サービス

② サイバー攻撃からフィジカル空間の機器を操作することによる物理的被害の発生

DVR（デジタルビデオレコーダー、いわゆる WEB に接続されているカメラ等から得られる映像の記録装置）の脆弱性やバックドアを突いて不正アクセスすることにより、工場内の映像を盗み見られたり改ざんされたりする事象が発生しています。

＜対策例＞

▶ 3.1 節 悪意ある人物による機器に対する直接攻撃への対策
付録 ソリューション①：既存機器のインターフェース部に外付け可能な通信暗号化コネクタシステム

▶ 3.2 節 サプライチェーンフェーズでの悪意のあるソフトウェア混入への対策
付録 ソリューション②：IoT 機器向けの改ざん検知ソフトウェア（サービス）

▶ 3.3 節 リモートメンテナンスの脆弱性への対策
付録 ソリューション③：IoT や OT システムにおけるセキュリティ異常対処支援サービス

▶ 3.4 節 自社で脆弱性を検討できないことによる放置リスクへの対策
付録 ソリューション③：IoT や OT システムにおけるセキュリティ異常対処支援サービス

③ サプライチェーン上の脆弱性を突いた攻撃によるサプライチェーン全体の被害発生

サイバー・セキュリティ対策が未整備の関係企業のネットワーク機器の脆弱性を突いて不正アクセスを行い、関係企業と攻撃対象企業の電子的なやりとりを通じて攻撃対象企業の PC やサーバーをランサムウェアに感染させることにより、業務に必要な情報を暗

号化して業務停止に追い込まれる被害が発生しています。

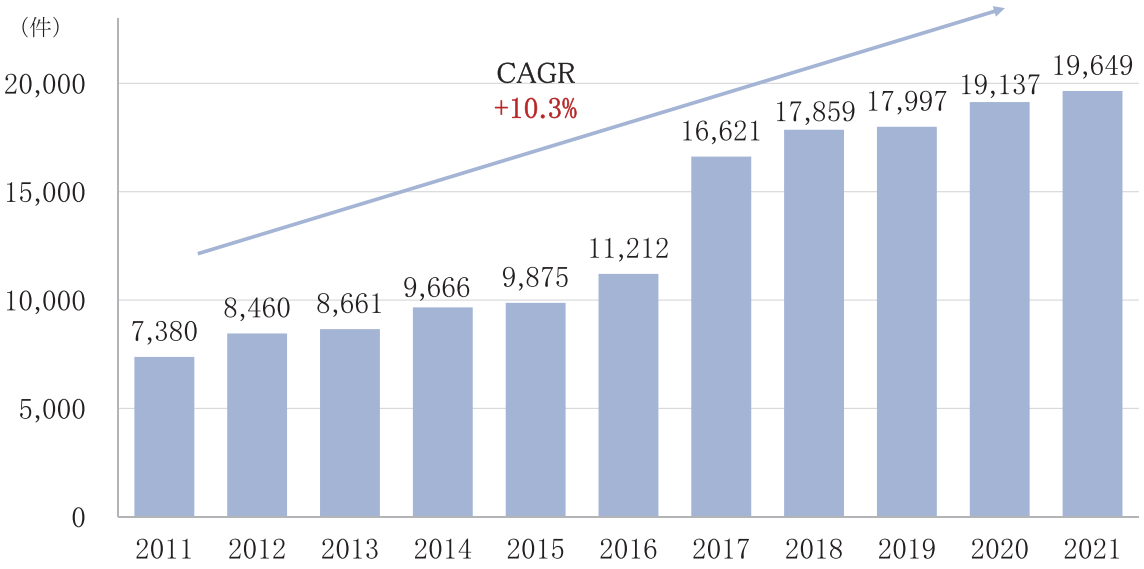
＜対策例＞

- ▶ 3.2 節　サプライチェーンフェーズでの悪意のあるソフトウェア混入への対策
  付録 ソリューション②：IoT 機器向けの改ざん検知ソフトウェア（サービス）
- ▶ 3.6 節　サプライチェーン上で流通するデータ改ざんへの対策
  付録 ソリューション⑤：サプライチェーン・トラスト・ソリューション

IoT や ICS への攻撃数増加の実態

IBM Security の調査（2022 年）では、産業での IT 活用が促進され、IoT や OT 機器等攻撃ポイントの増加によりサイバー攻撃リスクが高まっているとされています[10](図表8)。また、同レポートにおいて、産業用制御システム（ICS）に対する攻撃数は、2018 年から 2019 年にかけて 20 倍超になり、2019 年の OT 機器への攻撃数も 2016 年～ 2018 年の過去 3 年間分の攻撃合計数を大幅に上回っていると報告されています[11]。

図表 8　年別の IoT 及び OT の脆弱性の新規発見件数



（出典）IBM Security「X-Force Threat Intelligence Index 2022」（2022 年 2 月）

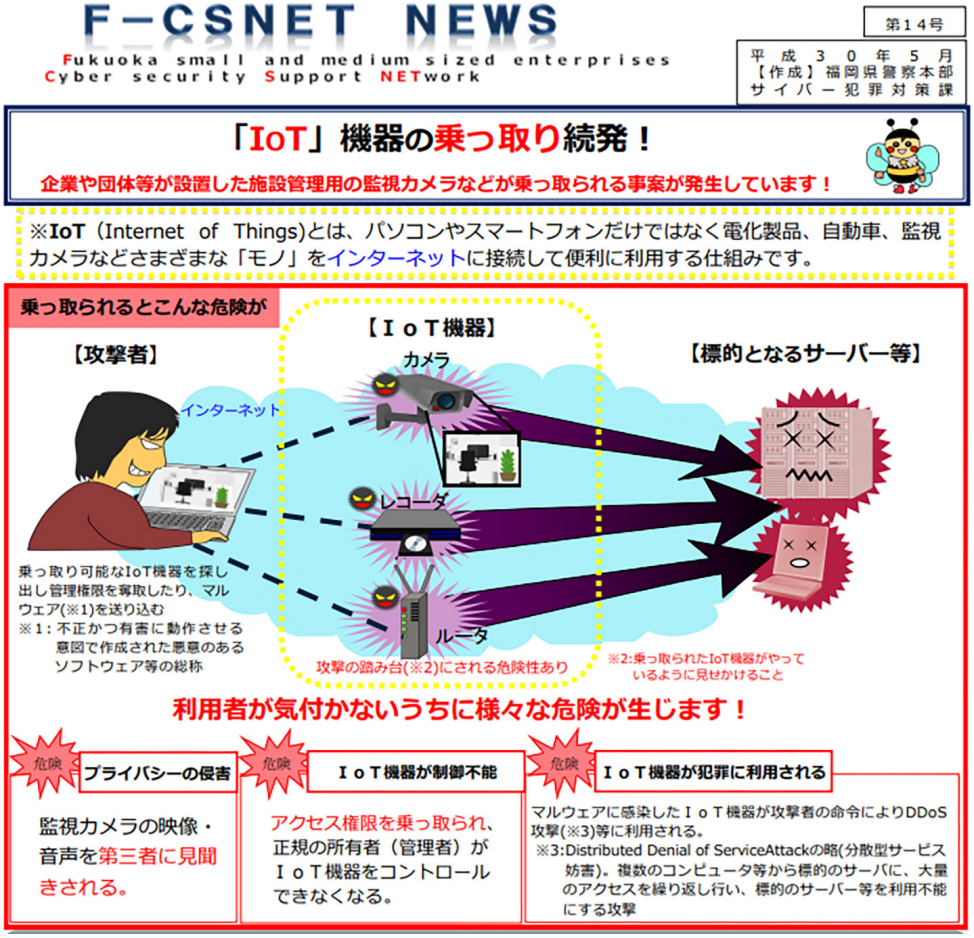
身近なところでは、IoT 機器の乗っ取り増加について、福岡県警察本部サイバー犯罪対策課等複数の県警にて「企業や団体等が設置した『施設管理用』の監視カメラが乗っ取られる

10　IBM Security,'X-Force　Threat Intelligence Index 2022'（2022 年 2 月）
https://www.ibm.com/downloads/cas/ADLMYLAZ　同レポートにおいては、OT と ICS はほぼ同義的に利用されている。但し、正確には、OT（Operational Technology）はシステムの制御・運用技術と定義されており、特に OT によって製造業の工場や研究所では産業制御システム（Industrial Control System）を動かしている。

11　同上

事案が発生している」として注意喚起されています[12]（図表 9）。また、警視庁においてもプライバシー保護に関連して動画での注意喚起がなされています

図表 9　IoT 機器の乗っ取り増加に関する注意喚起



（出典）福岡県警察本部サイバー犯罪対策「F-CSNET NEWS」（2018 年 5 月）

サプライチェーン攻撃の実態

グローバル化やサプライチェーンの多様化により、オフィスのみならず、工場、医療現場、農作業現場等様々な場所で IoT 機器が活用されています。そのため、対策が行き届いていない脆弱な組織の機器を踏み台として機器の内部に侵入し、ターゲットとなる組織のシステムを攻撃する「サプライチェーンの弱点を悪用した攻撃」も注目されています。IPA より 2022 年 1 月 27 日に公表された「情報セキュリティ 10 大脅威 2022」[13] においても「サプライチェー

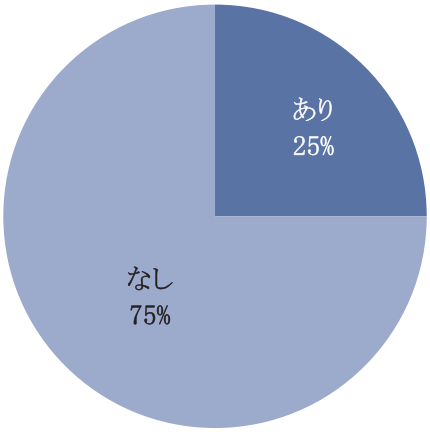
12　福岡県警察本部サイバー犯罪対策課「F-CSNET NEWS」（2018 年 5 月）
https://www.chuokai-fukuoka.or.jp/filedb/201805/F-csnet14.pdf、警視庁「IoT 機器乗っ取り編」（2021 年 6 月）
https://www.keishicho.metro.tokyo.lg.jp/about_mpd/joho/movie/cyber/cs_anime/personal/303.html
その他、ISP 事業者では、顧客（会員）に対して乗っ取りの増加を注意喚起した上で、実施すべき事項を分かり易く伝えている。

13　情報セキュリティ 10 大脅威 2022（https://www.ipa.go.jp/security/vuln/10threats2022.html）

ンの弱点を悪用した攻撃」は第３位にランクインしており、2021 年の４位からさらに順位を上げています。

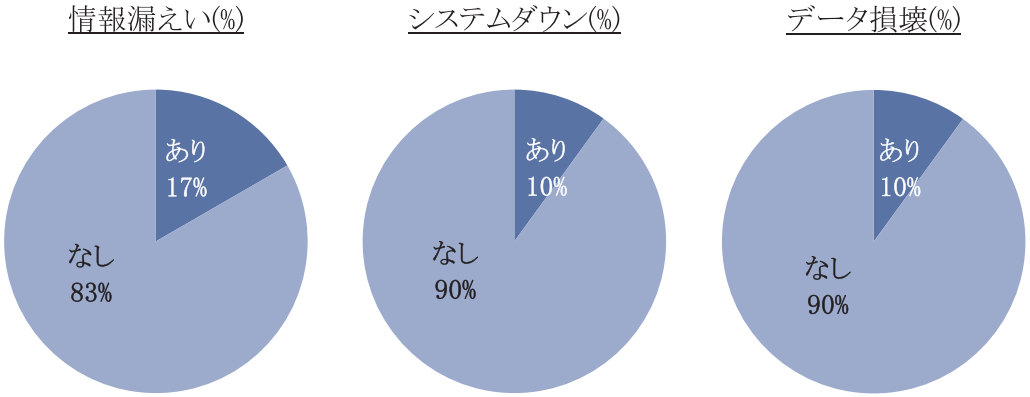
2019 年５月、大阪商工会議所が大企業・中堅企業 118 社に対して実施した「サプライチェーンにおける取引先のサイバー・セキュリティ対策等に関する調査」では、「取引先（中小企業）のサイバー攻撃被害による影響が自社に及んだ経験」を有する企業は４社に１社（25％）の割合で存在し（図表 10）、「情報漏えい」（17％）、システムダウン（10％）、データ損壊（10％）等の実害も発生していました（図表 11）。

図表 10　取引先のサイバー攻撃の影響が自社に及んだ経験の有無



（出典）大阪商工会議所「サプライチェーンにおける取引先のサイバー・セキュリティ対策等に関する調査」（2019 年５月）

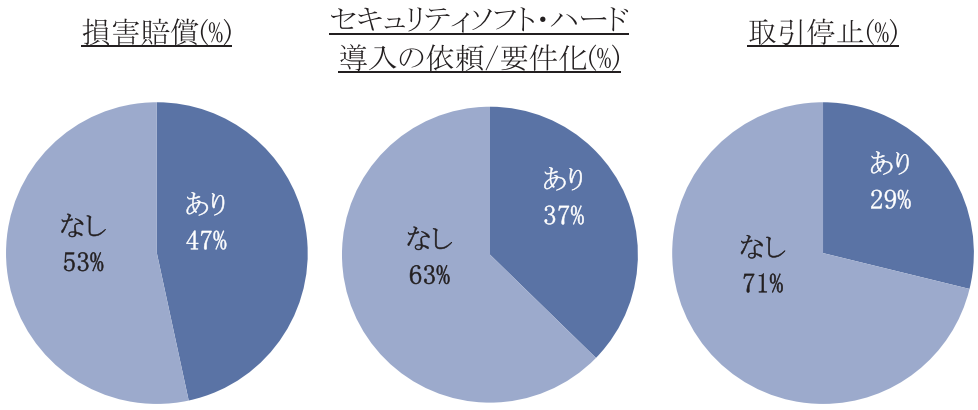
図表 11　取引先のサイバー攻撃の影響が自社に及んだ事案の被害内容



（出典）大阪商工会議所「サプライチェーンにおける取引先のサイバー・セキュリティ対策等に関する調査」（2019 年５月）

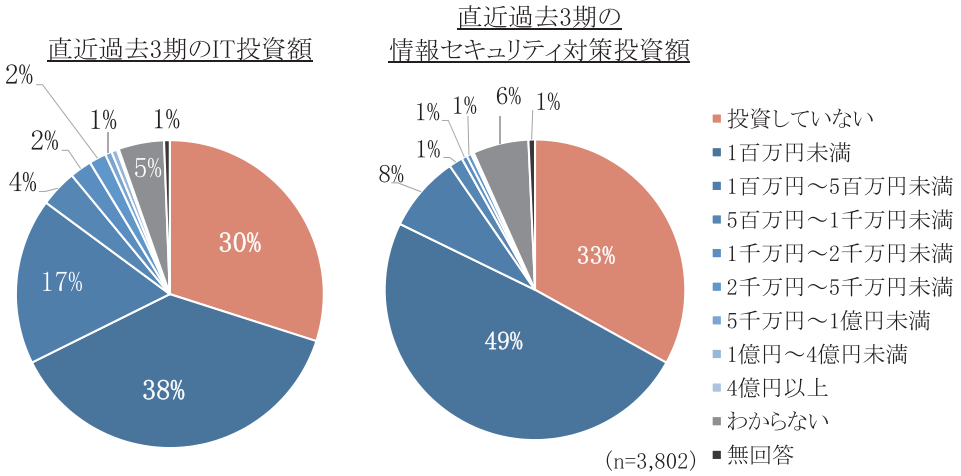
「取引先がサイバー攻撃を受け、その被害が自社にも及んだ場合取り得る対処」の回答として「損害賠償請求」（47%）、「取引停止」（29%）があったことから、中小企業がサイバー攻撃を受けて何らかの障害が発生した場合、自社の業務停止に留まらず、加害者として大企業から多額の損害賠償を請求される可能性もあると考えられます（図表 12）。

図表 12　取引先のサイバー攻撃の影響が自社に及んだ事案にて取り得る対処



（出典）大阪商工会議所「サプライチェーンにおける取引先のサイバー・セキュリティ対策等に関する調査」（2019 年 5 月）

図表 13　直近過去 3 期の IT 投資額と情報セキュリティ対策投資



（出典）IPA「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」（2022 年 5 月）

一方で、IPA の「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」（2022 年 5 月）[14] によれば、中小企業における直近過去 3 期の IT 投資額と情報セキュリティ

14　IPA「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」（2022 年 5 月）
https://www.ipa.go.jp/security/fy2021/reports/sme/index.html

対策投資額について、ともに約３割が「投資していない」と回答しています。IPA は「依然として中小企業における対策実施に関する課題は多く、更なる対策の必要性の訴求や、対策の実践に向けた支援の必要性が明らかになった」としています（図表 13）。

また、サイバー空間とフィジカル空間が高度に融合したシステムでは、サプライチェーンの拡大によりサイバー攻撃の起点が増加するとともに、サイバー攻撃による被害がフィジカル空間に及ぼす影響も増大し、これまでとは異なる新たなリスクも伴います。例えば、製品製造のサプライチェーンでは、製造時に不正な部品やソフトウェアが混入する、運用後にはソフトウェアアップデート時にマルウェア等の不正ソフトウェアが仕込まれるといった可能性があります。また、企業間等の情報の授受において内容の改ざんや、なりすまし、情報漏えい等も考えられます。そのため、自社のみを対象としたウイルス対策ソフト、ふるまい検知や EDR の導入といった対策でこのような脅威に対して安全性を担保することは困難です。

さらに、様々な機器やソフトウェアを外部調達して製品製造している場合は、調達した機器内のソフトウェアを含め「クリーン[15]」なソフトウェアのみで構成されているかの保証や、規定された手順に則った「正しい」作業によって製造され、潜在的な欠陥や誤設定がないことの証跡をサプライチェーン間で融通し合い、運用時においても常に「クリーン」な状況であるかを監視するといった取り組みが必要です。

15　出荷前に不正に埋め込まれたマルウェア等によって汚染されていない状態

2.3. サイバー・フィジカル・セキュリティ対策に関する規格・ガイドライン

2022 年 5 月、国会では経済安全保障推進法が衆参両院の本会議にて可決、成立しました。この法律には「基幹インフラ役務の安定的な提供の確保に関する制度」という章があり、対象とする分野[16]に対して「基幹インフラ役務の安定的な提供の確保は安全保障上重要である」としています。このことから、基幹インフラの重要設備が我が国の外部から行われる役務の安定的な提供を妨害する行為の手段として使用されることを防止するため、重要設備の導入や維持管理等の委託について事前審査が求められることとなります。事前審査では、サイバー攻撃によるシステム障害や情報流出のリスクにおいても審査される可能性があります。

また、翌 6 月に定められた「経済財政運営と改革の基本方針 2022」では、「経済安全保障の強化」として「国際情勢の変化等を踏まえたサイバー・セキュリティの確保に向けた官民連携や分析能力の強化について、技術開発の推進や制度整備を含めた所要の措置を講ずるべく検討を進める」とされています。

このような動きを受け、企業・各種団体にも求められる対策・対応すべき事項が増えてきており、各産業界においても規格やガイドラインを最新化する流れにあります。

また、経済産業省は様々な産業に求められるセキュリティ対策の全体像をまとめたフレームワークとして『サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）』を 2019 年 4 月 18 日に策定しました。従来のセキュリティ対策がサイバー空間におけるセキュリティを想定していたことに対し、サイバー・フィジカル・セキュリティ対策フレームワークでは「Society 5.0」や「Connected Industries」の中で表現されている、サイバー空間ならびにフィジカル空間におけるサプライチェーン全体のセキュリティの確保を目的としています。また、重要インフラの 14 分野では分野ごとにサイバー・フィジカル・セキュリティに対する規格やガイドラインの概要が用意されています（図表 14）。

さらに、重要インフラ以外の業界や業種についても、多くの領域で規格やガイドラインが作成されています（図表 15）。具体的な規制がない、もしくは普及していない業界に属する企業であっても、常時リスクに晒されていることを前提に手立てを考える必要があります。

16 挙げられているのは電機、ガス、石油、水道、鉄道、貨物自動車運送、外航貨物、航空、空港、電気通信、放送、郵便、金融、クレジットカードの 14 分野。法律で対象事業の外縁を示したうえで、政令にて絞り込む予定である。

図表 14　重要インフラにおけるサイバー・フィジカル・セキュリティに対する規格やガイドライン

分野		安全基準等の名称
情報通信	電気通信	● 事業用電気通信設備規則 ● 情報通信ネットワーク安全・信頼性基準 ● 電気通信分野における情報セキュリティ確保に係る安全基準（第 4.1 版）
	放送	● 放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン ● 放送設備サイバー攻撃対策ガイドライン
	ケーブルテレビ	● ケーブルテレビの情報セキュリティ確保に係る「安全基準等」策定ガイドライン＜初版＞
金融	銀行等 生命保険 損害保険 証券	● 金融機関等におけるセキュリティポリシー策定のための手引書 ● 金融機関等コンピュータシステムの安全対策基準・解説書 ● 金融機関等におけるコンティンジェンシープラン策定のための手引書
航空		● 航空分野における情報セキュリティ確保に係る安全ガイドライン（第 5 版）
空港		● 空港分野における情報セキュリティ確保に係る安全ガイドライン（第 2 版）
鉄道		● 鉄道分野における情報セキュリティ確保に係る安全ガイドライン（第 4 版）
電力		● 電気事業法施行規則第 50 条第 2 項の解釈適用に当たっての考え方 ● 電気設備の技術基準の解釈 ● 電力制御システムセキュリティガイドライン・スマートメーターシステムセキュリティガイドライン
ガス		● 都市ガス製造・供給に係る監視・制御系システムのセキュリティ対策要領及び同解説
政府・行政サービス		● 地方公共団体における情報セキュリティポリシーに関するガイドライン
医療		● 医療情報システムの安全管理に関するガイドライン（第 5 版）
水道		● 水道分野における情報セキュリティガイドライン（第 4 版）
物流		● 物流分野における情報セキュリティ確保に係る安全ガイドライン（第 4 版）
化学		● 石油化学分野における情報セキュリティ確保に係る安全基準
クレジット		● クレジット CEPTOAR における情報セキュリティガイドライン
石油		● 石油分野における情報セキュリティ確保に係る安全ガイドライン

（出典）内閣サイバーセキュリティセンター「重要インフラ分野における安全基準等の継続的改善状況等に関する調査について［2019 年度］」（2020 年 7 月）

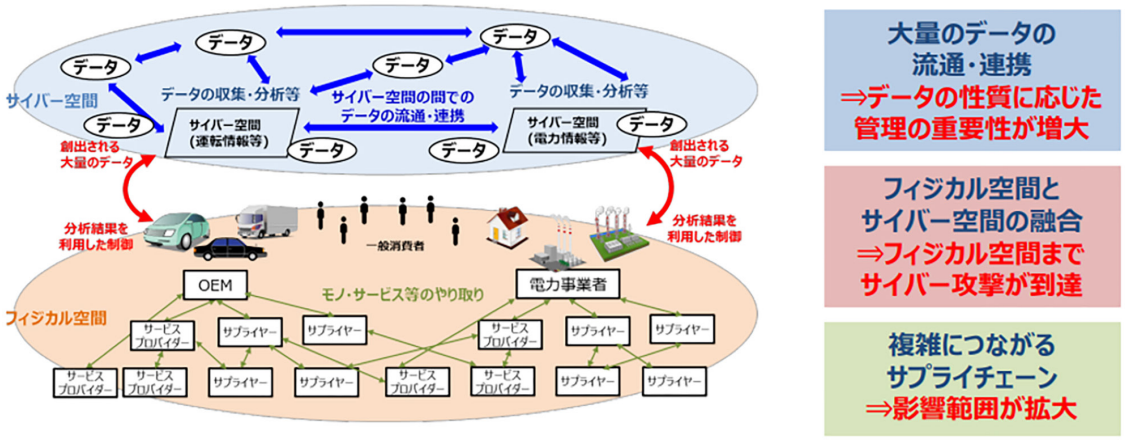
図表 15　その他業種別のサイバー・フィジカル・セキュリティに対する規格やガイドライン

分野	作成者	名称
電気通信会社	総務省	5G セキュリティガイドライン第 1 版
	ICT-ISAC	ローカル 5G セキュリティガイドライン
交通	-	鉄道 / 航空の安全・安定輸送に資するサイバーセキュリティ対策の手引き（非公開）
	jama、JAPIA	自工会 / 部工会・サイバーセキュリティガイドライン
	国土交通省	情報セキュリティ対策のチェックリスト（鉄道、バス、バスターミナル、タクシー、宿泊施設、フェリー・旅客船、空港・空港ビル）
医療	総務省 経済産業省	医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン
原子力・核物質	原子力規制庁	原子力施設情報システムセキュリティ対策ガイドライン（非公開）
建設	日本建設業連合会	建設現場における情報セキュリティガイドライン
土木工事	国土交通省	土木工事等の情報共有システム活用ガイドライン
電気工事	経済産業省	自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン
林業	森林 GIS フォーラム	森林クラウドシステムに関わる情報セキュリティガイドライン
印刷	日本印刷産業 連合会	印刷産業における個人情報保護ガイドライン
農業	農林水産省	農業分野におけるオープンＡＰＩ整備に関するガイドライン ver1.0
	農林水産省	農業機械の自動走行に関する安全性確保ガイドライン
	総務省	解説文書
漁業	金融庁、水産省	漁協系統信用事業における総合的な監督指針
製造産業	経産省	工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン
	-	サイバーセキュリティ対策、鉄鋼業向けガイドライン（非公開）
	JPCERT/CC	工場における産業用 IoT 導入のためのセキュリティファーストステップ
スマートシティ	総務省	スマートシティセキュリティガイドライン（第 2.0 版）
港湾	国際海事機関	海事サイバーリスク管理に関する MSC-FAL.1/Circ.3 ガイドライン
	日本海事協会	解説文書
	国際港湾協会	港湾及び港湾施設のためのサイバーセキュリティガイドライン

2.4. サイバー・フィジカル・セキュリティ対策フレームワーク

経済産業省が策定した「サイバー・フィジカル・セキュリティ対策フレームワーク」では、従来のサプライチェーンの活動範囲から拡張された付加価値を創造する活動のセキュリティ上のリスク源を洗い出した後に、対応方針を示すため、以下の３つの「層」（下から順に１層：企業間のつながり、２層：フィジカル空間とサイバー空間のつながり、３層：サイバー空間におけるつながり）でサイバー・フィジカル・システムを整理しています（図表 16）。

図表 16　Society 5.0 の社会におけるモノ・データ等のつながりのイメージ



（出典）経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク」（2019 年 4 月）

サイバー・フィジカル・システムにおいては、3 層の層毎に信頼性確保に向けた基点の確保によって、サプライチェーンにおけるプロセス全体の信頼性を確保することが重要となります。各層毎の信頼性を確保するための基点と対策について図表 17 に示されています。

図表 17　層毎に必要となるセキュリティ対策

層	概要
第 3 層－ サイバー空間に おけるつながり	データそのものが「信頼の基点」となる ⇒データの流通・管理や適切な編集・加工を行うための セキュリティ対策等
第 2 層－ フィジカル空間と サイバー空間の つながり	要求される情報の正確性に応じて適切な正確さで情報が変換されること、つまり転写機能の正確性が「信頼の基点」となる ⇒転写という機能の信頼性を確保するための措置
第 1 層－ フィジカル空間 （現実社会）における つながり	企業（組織）のマネジメントが「信頼の基点」となる ⇒信頼性の確認された企業（組織）間のつながりを サプライチェーンのセキュリティ確保につなげる しくみ

図表 14 や図表 15 に挙げている規格やガイドラインには、セキュリティ対策立案に対する要件や実施の考え方に関するものが多く見られますが、それを実現するための具体的な対応については詳細には記載されていません。また、第 1 章で記載しているように、IoT や OT 向けとなると、従来のサイバー・セキュリティ対策を拡張した考え方が必要となるため、具体的なセキュリティ対策については、担当者の力量に依存してしまい、上記に挙げた規格やガイドラインへの対応検討が十分に行えない可能性が考えられます。IoT や OT が導入されている場合には、第 3 章に記載しているソリューションについて導入検討を行う必要があります。

第３章
SIP技術を用いたサイバー・フィジカル・セキュリティの対策例

☑ ポイント①
戦略的イノベーション創造プログラム（SIP）第2期では、サイバー・フィジカル・システムのセキュリティ対策として、サプライチェーン全体を対象とした「サイバー・フィジカル・セキュリティ対策基盤」を開発しました。

☑ ポイント②
代表的なサイバー・フィジカル・システムリスクに対して、サイバー・フィジカル・セキュリティ対策基盤の各ソリューションがどのような対策なのか、各節で解説しています。

戦略的イノベーション創造プログラム（SIP）第2期では、サプライチェーン全体を対象としたサイバー・フィジカル・セキュリティ対策基盤を開発しました。サイバー空間とフィジカル空間の双方に跨るIoT社会でのサプライチェーンの各構成要素に信頼の基点としてセキュリティ確保（信頼の創出）とその確認（信頼の証明）を繰り返し行い、信頼のチェーンを構築して維持することで、IoTシステムのサプライチェーン全体のセキュリティ確保の実現を企図しています。

図表18では、サイバー・フィジカル・セキュリティ対策フレームワークに記載されている「想定されるセキュリティ・インシデント」を基に「一般的な想定リスク」を縦列に記載しました。製造時や導入時だけでなく運用時も含めた製品やサービスのライフサイクル全般で発生しうるリスクについて挙げ、それらの想定リスクに対してサイバー・フィジカル・セキュリティ対策基盤を構成する5つのソリューション（①～⑤）がどのように対応するかを横軸で示しました。それぞれのソリューションを用いた想定リスクへの具体的対応について、3.1節から3.6節で説明します（図表19）。なお、①～⑤の個々のソリューションについては付録も併せてご参照下さい。

図表 18　想定リスクと対応するソリューション

一般的な想定リスク	サイバー・フィジカル・セキュリティ対策基盤				
	①既存機器のインターフェース部に外付け可能な通信暗号化コネクタシステム	②ＩｏＴ機器向けの改ざん検知ソフトウェア（サービス）	③ＩｏＴやＯＴシステムにおけるセキュリティ異常対処支援サービス	④信頼できる取引ネットワーク構築サービス	⑤サプライチェーントラストソリューション
リスク A） 機器自体の差し替えや不正機器のネットワークへの接続	○	○			○
リスク B） ネットワーク上の通信傍受	○			○	
リスク C） 不正ソフトウェアの混入	○	○	○[17]		
リスク D） 脆弱性を発端とする攻撃		○[18]	○	○[19]	○[20]
リスク E） 不正アクセスによる情報漏えいや改ざん	○	○	○	○	○
リスク F） 内部による不正行為					○

「一般的な想定リスク」はサイバー・フィジカル・セキュリティ対策フレームワークにおける３層の層ごとに想定されるリスクを集約した内容となっています。これらの想定リスクについて対応することにより、各層ごとに想定されるリスクへの対応が可能となります。

17　不正ソフトウェアの混入により、不正な通信を検知した場合、検知ならびに一次対処を支援
18　不正通信があり、異常情報があった場合には検知可能
19　ランサムウェアがデータを暗号化しようとした場合に、権限管理にて阻止可能
20　攻撃や不正が起きてしまった場合、行為違反を記録し、責任の範囲と実施内容の説明が可能

図表 19　第 3 章で取り扱うシナリオと対象とする業界の対応

#	シナリオ	業界
3.1	悪意ある人物による機器に対する 直接攻撃への対策	医療分野
3.2	サプライチェーンフェーズでの 悪意のあるソフトウェア混入への対策	医療分野
3.3	リモートメンテナンスの脆弱性への 対策	医療分野
3.4	自社で脆弱性を検討できないことによる 放置リスクへの対策	製造業
3.5	不適切な組織・事業者の接続への対策	自治体
3.6	サプライチェーン上で流通する データ改ざんへの対策	医療分野

医療機関について

コラム

医療機関においては、サイバー・フィジカル・セキュリティへの対策として、医療機関向けの『医療情報システムの安全管理に関するガイドライン』ならびに医療情報提供者向けの『医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン』があります。

ガイドラインに基づきシステムにおける監査が定期的に実施されているため、医療分野は一定のサイバー・フィジカル・セキュリティ対策が既に施されており、ウイルス対策ソフトやふるまい検知ソフトの導入等による院内システムのセキュリティ強化が図られています。一方、急速な情報化に伴う医療機関の業務環境の変化やサイバー攻撃手法の多様化により、セキュリティ対策が十分に追いついていないケースが見受けられ、国内でもサイバー攻撃が相次いで発生しています。

2022 年 5 月、日本経済新聞は、各地域の医療の中心となる大規模病院「地域医療支援病院」約 600 カ所のうち病床数の多い 100 カ所に対して、イスラエルのセキュリティ企業 KELA と共同で闇サイトの関連情報を調査しました[21]。その結果、3 病院で攻撃可能なマルウェアが闇サイトで販売されていたこと、3 分の 2 の病院では職員のパスワードが漏洩していることが判明し、気付かないうちに多くのサイバー攻撃を受けていることが露呈しました。

昨今、医療機関がサイバー攻撃の的になっている要因の一つとして、システムトラブルが人命に関わること、病歴や治療歴等に加えてワクチン接種でさらに多くの個人情報が集まっていること、新型コロナウイルス感染拡大により治療体制が切迫していることから身代金の支払いに応じる可能性が高いと攻撃者に想定され、「攻撃対象の価値（影響度）」が一気に高まったことが考えられます。また、多くの医療機関で脆弱性のある古い機器類や OS 等が放置されていることから、「攻撃の容易性」も要因に繋がっていると考えられます。本章では医療分野において具体的に想定されるリスクを題材に、サイバー・フィジカル・セキュリティ対策基盤を活用することにより、どのような対策を講じることができるかについて具体的に説明します。

21　日本経済新聞「大規模病院にサイバー攻撃 遅れる医療防衛 3 分の 2 で情報漏れも 日経調査」（2022 年 5 月 29 日）

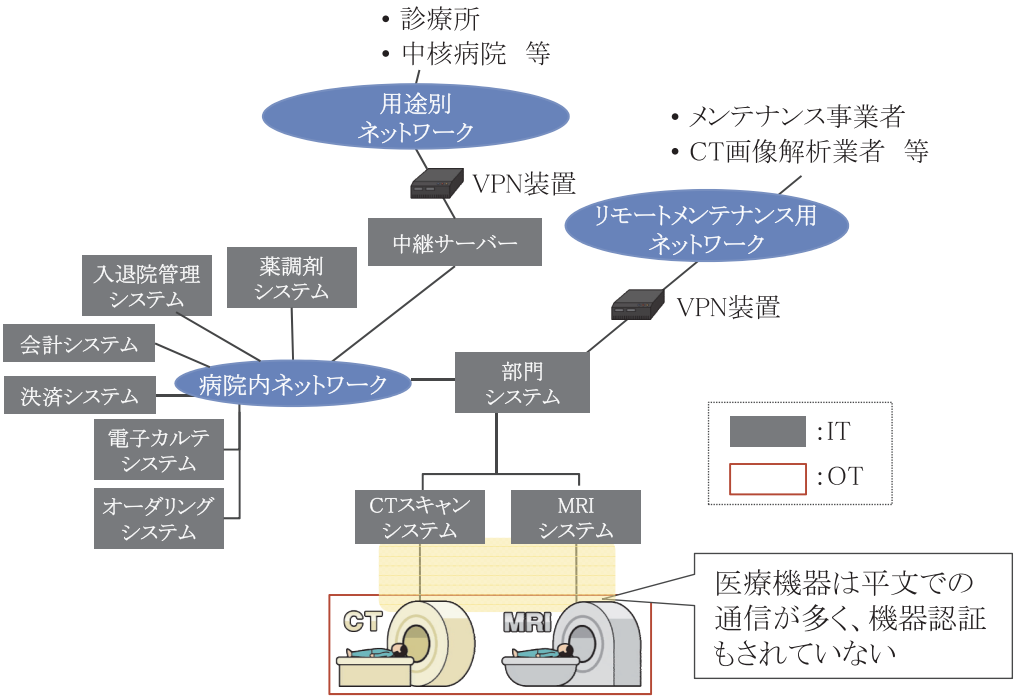
3.1. 悪意ある人物による機器に対する直接攻撃への対策

「コラム：医療機関について」のとおり、近年医療機関を狙ったサイバー攻撃の事案が発生しており、対策が急務であることから、本節では近年特に対策が求められている「リスク A）機器自体の差し替えや不正機器のネットワークへの接続」と「リスク B）ネットワーク上の通信傍受」を事例として取り上げ、サイバー・フィジカル・セキュリティ対策基盤の「既存機器のインターフェース部に外付け可能な通信暗号化コネクタシステム」（付録①）を活用することにより、どのように対策を行うことができるかについて具体的に説明します。

3.1.1. 現状

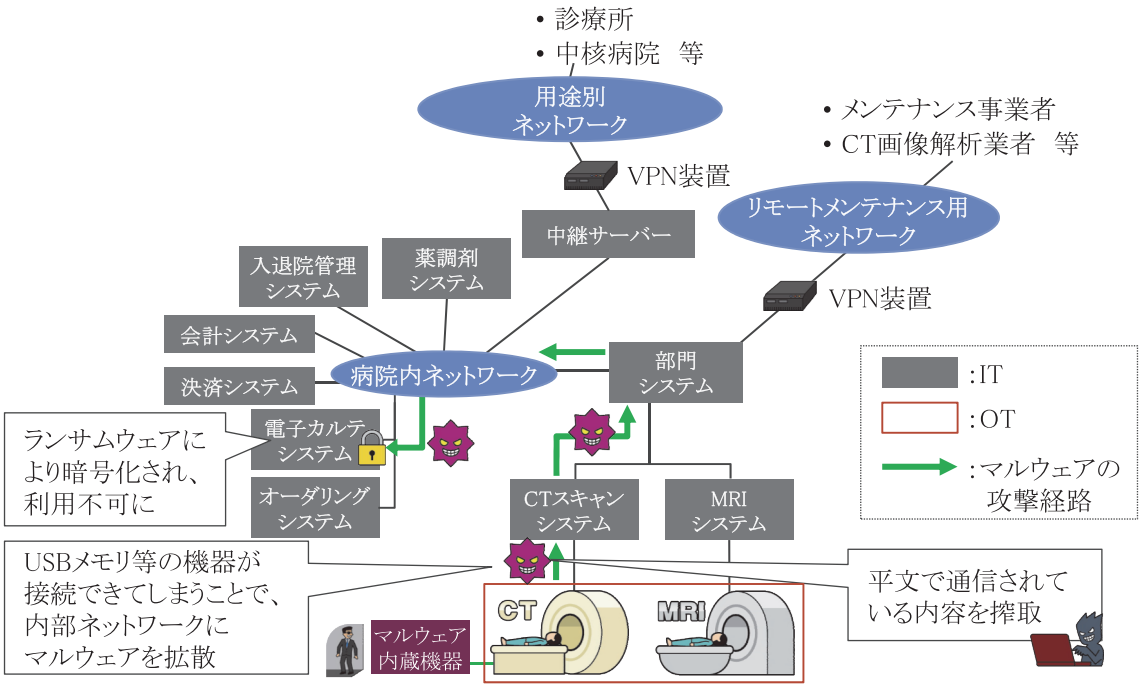
医療機関では、メンテナンス事業者や清掃員等多くのステークホルダーが医療現場に出入りしており、悪意を持つ人物も侵入が比較的容易な職場環境になっています。医療機器やそこから出ている LAN ケーブルや無線ルーターに何らかの操作をしたとしても、外部委託先のメンテナンス作業として捉えられてしまう恐れがあります。また、医療従事者の方は多忙なため、IoT 機器のネットワーク機器への新たな接続やネットワーク機器（無線ルーター）の交換について、すぐには気づかない可能性があります。一般的には機器認証によって正式ではない機器が接続できない対策や、通信を暗号化することで万が一通信内容を傍受されたとしても内容を確認できない対策が施されています（図表 20）。

図表 20　医療機関のシステム例



しかし、IoT 機器はリソースの制約から、一般的なパソコンに実装されている TPM（Trusted Platform Module[22]）が実装されていないことが多いため機器認証や通信の暗号化が進んでいません。昨今、IoT 機器の医療現場への導入が進みつつあるため、対策を怠っている場合は危険な状況になっている恐れがあります。医療機器の保守端末や IoT 機器を含む医療機器から攻撃者の侵入を許してしまうと、通信内容の改ざんやネットワークに侵入されることによって電子カルテ等の医療情報にアクセスされてしまいます（図表 21）。

図表 21　IoT 機器を含む医療機器への攻撃の例



また、OT である医療機器（CT や MRI 等）への攻撃は医療機器や関連システムの不具合を発生させ、医療サービスの制限や停止につながります。情報流出や医療サービスの制限や停止は顧客からの信頼を低下させ、顧客流出につながり、経営基盤が揺らいでしまう可能性もあります。

22　コンピュータのマザーボード等に装着されるセキュリティ関連の処理機能を実装した半導体チップ。国際的な業界団体である Trusted Computing Group（TCG）により標準仕様化され、暗号処理機能、暗号鍵の保護機能、プラットフォームの正当性検証機能等、セキュリティ機能を持つ。

3.1.2. 解決策の方向性

悪意ある人物による IoT 機器に対する直接攻撃には強固なパスワードの設定や機器固有の識別子による接続機器の制限等が重要となります。また、情報改ざんや抜き取りの防止には通信の暗号化が有効です。万が一侵入されてしまった場合に向けてはネットワークのセグメント分けやアクセス権限管理の強化等の対策をあらかじめ行っておくことにより被害拡大を食い止めることができます。

ところが、医療機関内のネットワークは閉域網前提であることから、暗号化について考慮されておらず、医療機器は高額であることから一定期間使い続ける傾向があります。セキュリティ対策が施されていない機器や、運用期間中に高度化することが考慮されていない機器が多いため、利用期間中にセキュリティ対策を高度化することは難しいです。また、リアルタイム性が求められる領域は、暗号化による遅延を許容しづらく、導入後にセキュリティ高度化の対応をしようとした場合は高額になる傾向があります。

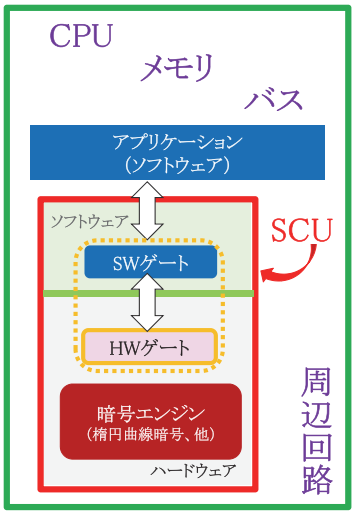
そのため、悪意ある人物による機器への直接攻撃のリスクを顕現させるためには、暗号化通信に対応できていない機器とネットワーク機器の通信を後付けで簡便に暗号化できるソリューションが必要です。また、このソリューションにはリアルタイム性を損なわない暗号化及び復号の速度が求められます。そして、接続機器の入れ替えや機器の新規追加にも対応できていることが重要なポイントです。

3.1.3. 具体的な対応：既存機器のインターフェース部に外付け可能な通信暗号化コネクタシステム（付録①）

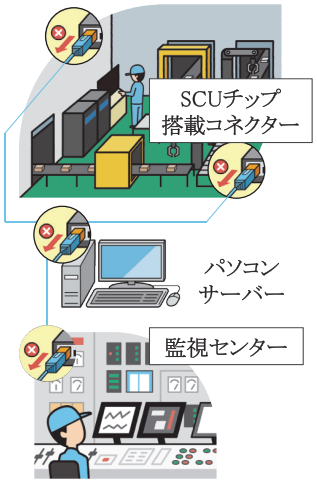
悪意ある人物による機器への直接攻撃については、上述のように、通信の暗号化や何らかの方法を用いた接続機器の制限が重要です。様々な攻撃手段が開発されていることから、運用中の機器についてもセキュリティレベルを上げる必要があるため、後付けで同様の対策を講じる必要があります。

今回ご紹介する「既存機器のインターフェース部に外付け可能な通信暗号化コネクタシステム」は LAN ケーブルのモジュラーをコネクタシステムに交換するだけで（図表 22）、機器間の通信を暗号することや接続先システムの機器認証が保証され、末端デバイスにおけるネットワーク対策を高いレベルに引き上げます。

図表 22　コネクタシステムによる対応イメージ



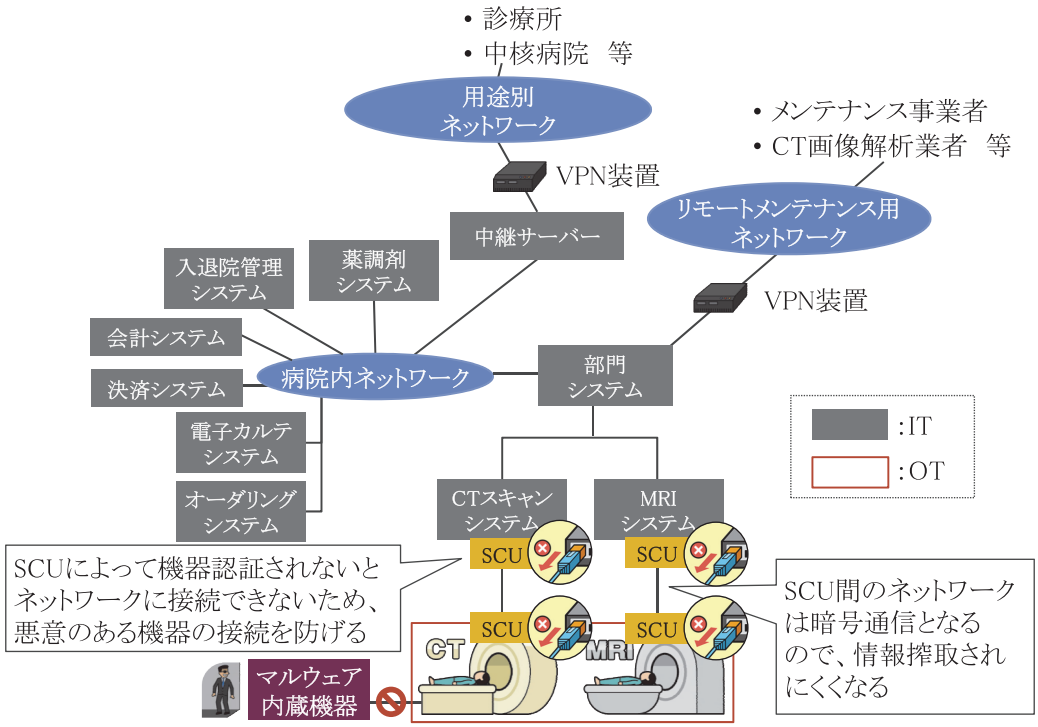
SCU搭載チップの一般的構成



また、コネクタシステムが LAN ポートから物理的に外せない機構になっていることから、マルウェアやバックドアのある不正な端末への差し替えや新しい機器の接続を試みようとしても、機器からコネクタシステムを抜いて別の機器へ差し替えることが出来なくなっています。

さらに、コネクタシステムに組み込まれているSCUチップにより接続先システム同士の相互認証を行っているため、新しい機器がネットワーク機器に接続されたとしても機器認証を突破することはできません。そのため、不正な機器経由によるマルウェア等悪意のあるソフトウェアのインストールやバックドアによる侵入・乗っ取りを防止することができ、TPM相当の状況を作り上げることができます（図表23）。

図表23　悪意ある人物による機器への直接攻撃に対して想定される対策



既存機器のインターフェース部に外付け可能な通信暗号化コネクタシステムに関する問い合わせ先

株式会社 SCU
Email : c01.contact@scu.co.jp

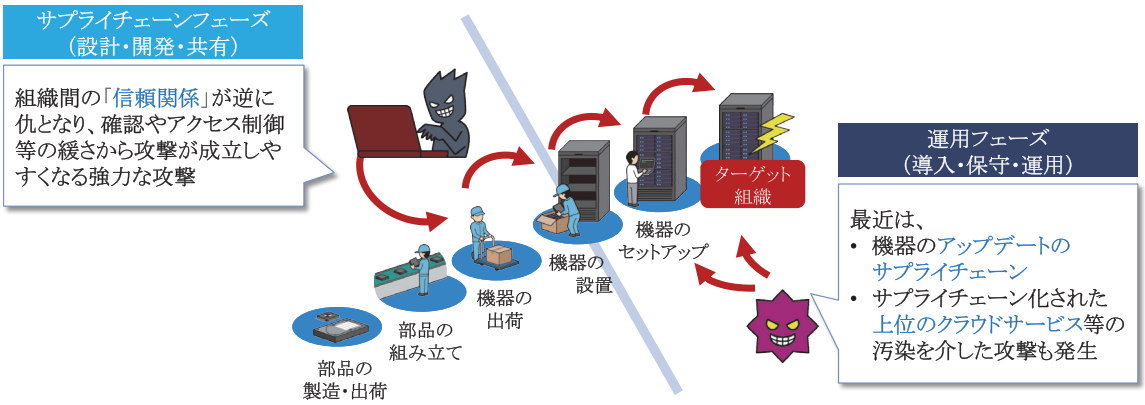
3.2. サプライチェーンフェーズでの悪意のあるソフトウェア混入への対策

本節では近年特に対策が求められているサプライチェーンフェーズでの「(図表 18) リスク C) 不正ソフトウェア混入」を事例として取り上げ、サイバー・フィジカル・セキュリティ対策基盤の「IoT 機器向けの改ざん検知ソフトウェア（サービス)」(付録②) を活用することにより、どのように対策を行うことができるかについて具体的に説明します。

3.2.1. 現状

汎用のハードやソフトウェアを利用した機器開発、プラットフォームを活用したクラウドサービスの開発の割合が多くなり、機器調達時の「不正ソフトウェアの混入」や運用開始後の「アップデート作業及び稼働中ソフトウェアにおける改ざん 」のリスクが増大しています (図表 24)。機器等の調達やサービス利用において製造、物流や業務委託等の商流に関わってきます。

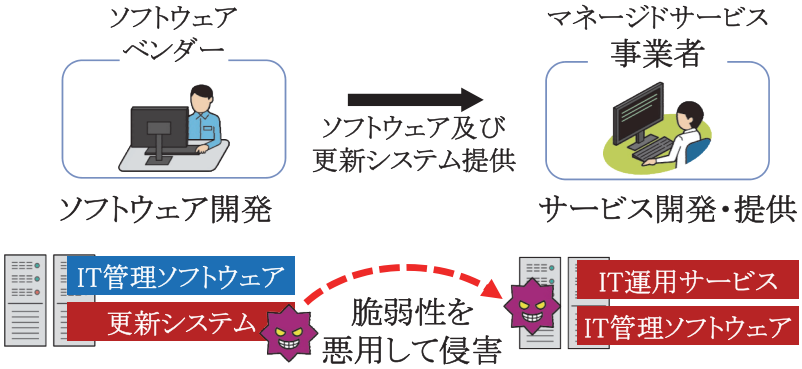
図表 24　サプライチェーン攻撃概念図



そのため、サプライチェーンに属する企業の中で、セキュリティ対策が十分に行き届いていない企業がある場合は、その企業に対して攻撃することで標的となる企業へ被害をつなげていくサプライチェーン攻撃が可能です（図表 25）。この攻撃手法は増加傾向にあり、大きな脅威として認識されています。

例えば、トップレベルでサイバー対策が講じられていたと想定されるネットワーク監視ツール提供企業が、自動更新時にバックドアのマルウェアが配布されるよう攻撃者に仕込まれたことにより、米国政府機関を含む多くの顧客に影響が発生しました。

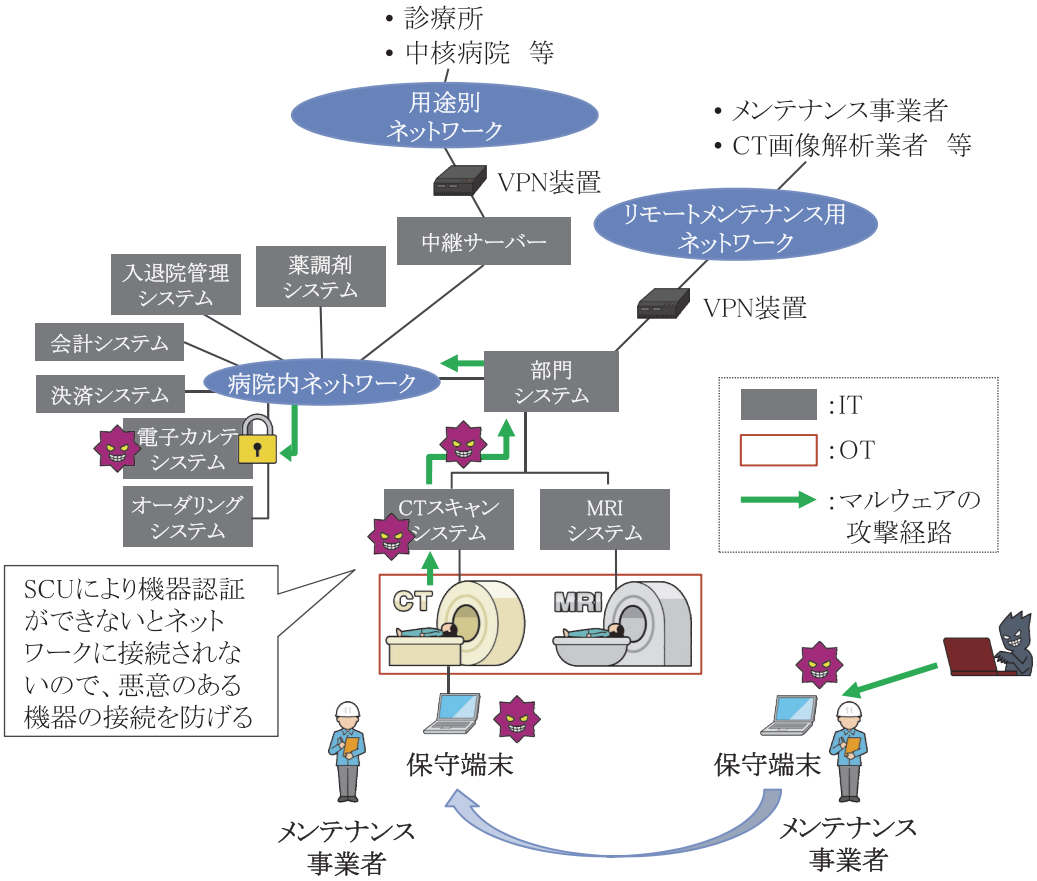
図表 25　ソフトウェアサプライチェーンを脅かす攻撃例



医療現場においても、悪意あるソフトウェアが医療機器に混入されることにより、医療機器が汚染される可能性があります。

また、導入後、メンテナンス事業者によるソフトウェア更新の際、接続された PC を媒体として医療機器が汚染されることも考えられます（図表 26）。汚染された機器を発端として、ランサムウェアによるシステム停止や情報流出が発生してしまう恐れもあります。

図表 26　メンテナンスサービスを介したサプライチェーン攻撃例



特に、近年では運用中における「アップデート作業及び稼働中ソフトウェアの改ざん」のリスクも増大しており、調達及び製造のフェーズよりも狙われる状況で実害が多く出ています。具体的には汎用 OS の脆弱性を突いた攻撃により、ソフトウェア開発企業のソフトウェアに不正アクセスが行われ、アップデート用のシステムにランサムウェアが仕掛けられた事例が発生しています。

さらに、デジタルトランスフォーメーション（DX）の流れの中、デジタル記録の増加と統合されたシステムへの移行が多くなっており、これまで以上に多くのサービスプロバイダーとサプライヤーが重要情報にアクセスするようになることから、攻撃対象領域や脆弱性の露出が拡大の一途をたどっています。

そのため、近年米国ではこうしたサプライチェーン上のリスクに対処すべく、IoT 製品の安全性を表示するためのラベル表示に関する試験的制度の開始やヘルスケア分野における SBOM（Software Bill Of Materials、コラム参照）の実証実験等が行われています。また、経済産業省においても 2022 年度下期に実証実験（PoC）を実施することでコストや効果を計測する予定です。

SBOM (Software Bill Of Materials)

SBOM（Software Bill Of Materials: ソフトウェア部品表）とは、ソフトウェア製品に含まれる全てのソフトウェアコンポーネント（ライブラリ、モジュール等）、ライセンス、そのパッケージの依存関係等を包括的に一覧化したものを指します。

ソフトウェアのプロダクト自体の複雑度が上がっていくに従い、どのような「部品」を利用しているか把握することが次第に困難になっていきます。SBOM によって、ソフトウェアの全体像を可視化することができ、セキュリティ等様々なリスクが明確化されます。近年、ソフトウェアの脆弱性を突いたサプライチェーン攻撃が増加しつつあることを背景に、2021 年 5 月に米国バイデン大統領によって取り上げられ（「国家のサイバーセキュリティの向上に関する大統領令（Executive Order on Improving the Nation's Cyber Security）」）、注目を集めるようになりました。

3.2.2. 解決策の方向性

意図した設計通りにソフトウェアが組み込まれているか、調達及び製造のフェーズから、機器内のソフトウェア構成をモニタリングし続けることにより、万が一悪意のあるソフトウェアの混入が行われ、ソフトウェアが改ざんされた場合にも即時に検知できることが重要となります。

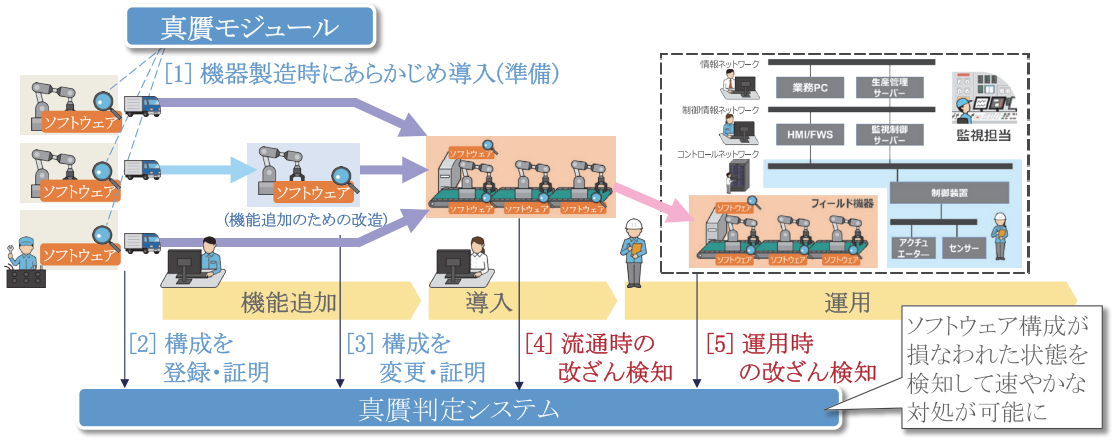
しかし、小型の IoT 機器はリソースや性能が制限されることから、稼働時にソフトウェアを常時モニタリングするソフトウェアを常駐させることが難しく、構成の確認に関して手が付けられない状況になっています。

そのため、納品時やソフトウェア更新後に、構成情報の正当性を確認する必要があります。

3.2.3. 具体的な対応：IoT 機器向けの改ざん検知ソフトウェア（サービス）（付録②）

対象の機器の性能が限られていても、インストールかつ常駐するソフトウェア改ざん検知ソフトウェアによってクリーンな機器であることが証明できるため、汚染された機器の受け入れリスクが低減されます（図表 27）。

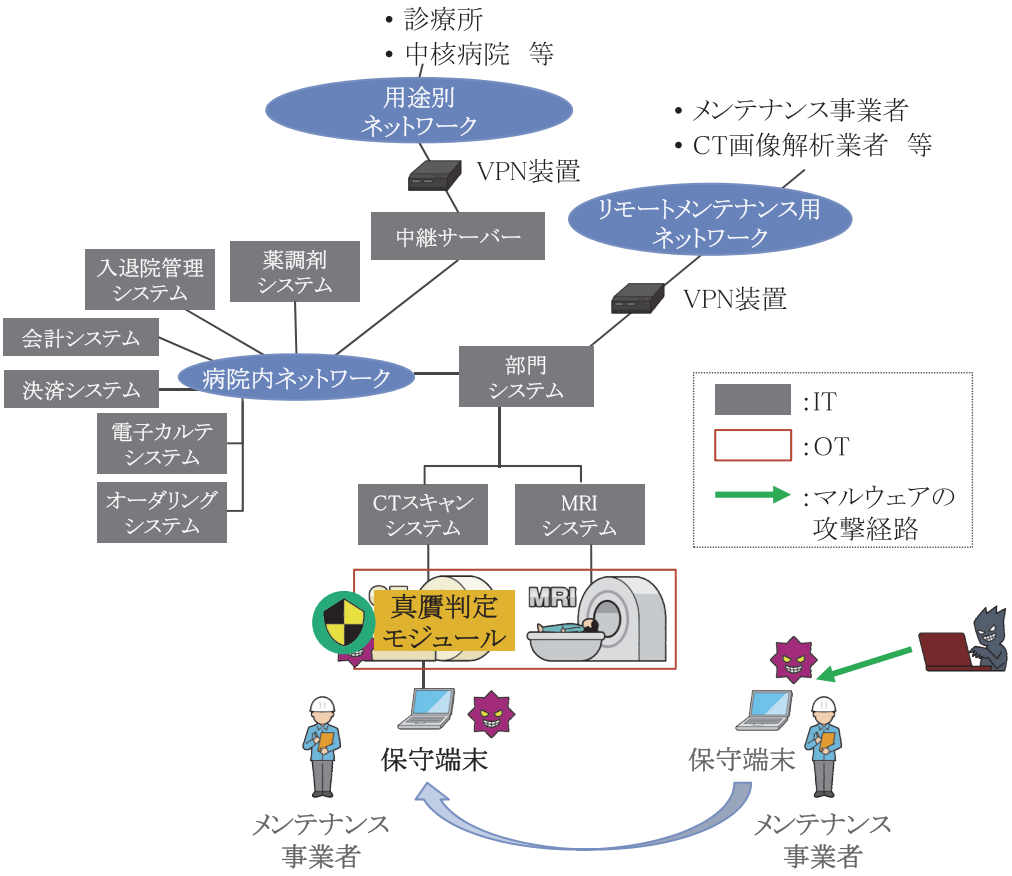
図表 27　IoT 機器向けの改ざん検知ソフトウェア（サービス）の対応イメージ



「製品の構成の正しさ」を常時確認・証明するには、保護対象となる IoT 機器の製造時に「真贋判定モジュール」を搭載する必要があります。この「真贋判定モジュール」は、製造時のサプライチェーンと運用時のサプライチェーンの全体を通じて機器内のソフトウェア構成を常時監視し、ソフトウェア構成が損なわれた場合に通知します。そのため、開発工程におい

てIoT機器に不正な構成要素（マルウェア等）が混入する脅威だけでなく、運用中に遠隔制御やメンテナンスサービス等を介して汚染される脅威についても対処が可能となり、機器の全ライフサイクルにおいてソフトウェア構成の改変リスクに対応できます（図表28）。

図表28　メンテナンスサービスを介したサプライチェーン攻撃に対して想定される対策



機器納入時は、検査において判定機能を実行することで機器全体を漏れなく検査できます。また、運用後もメモリ上の稼働中ソフトウェアを常時検査することで本来の動作に影響を与えず、稼働中の機器のソフトウェア構成を守ることができます。

なお、「真贋判定モジュール」はCPUやメモリ等のリソース制限等によって、従来対策が困難であった「中～低レベルの機器（センサー、カメラ、OA機器等の多様なIoT機器）」に搭載できるように開発されています。

IoT機器向けの改ざん検知ソフトウェア（技術）に関する問い合わせ先

日本電信電話株式会社　社会情報研究所
Email：solab@ml.ntt.com

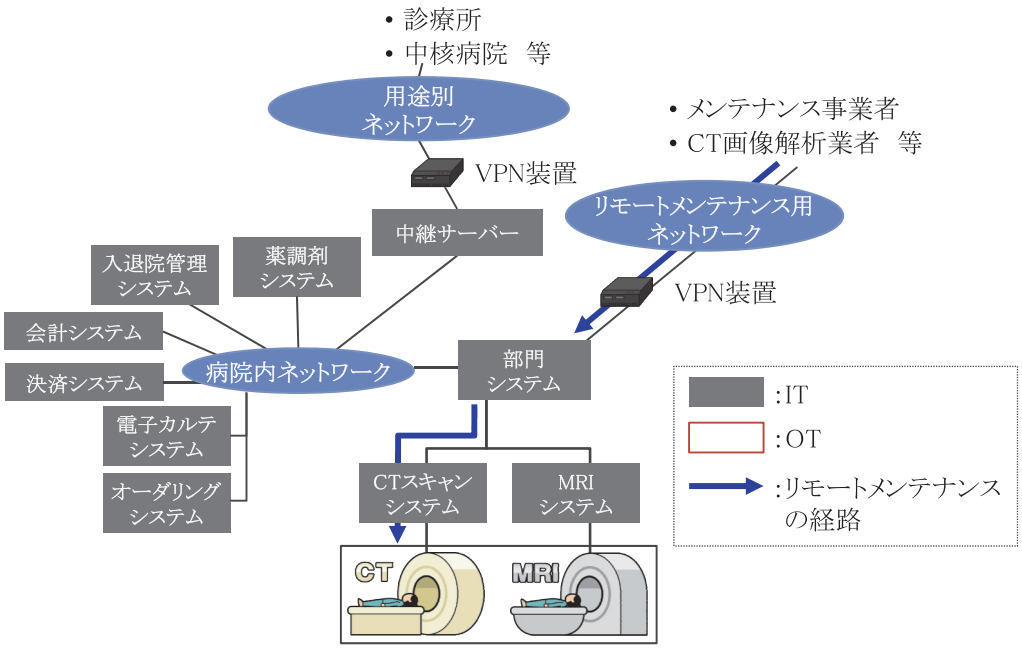
3.3. リモートメンテナンスの脆弱性への対策

前述のとおり、近年医療機関を狙ったサイバー攻撃の事案が発生しており、対策が急務であることから、本節では近年特に対策が求められている（図表 18）「リスク D）脆弱性を発端とする攻撃」を事例として取り上げ、サイバー・フィジカル・セキュリティ対策基盤の「IoT や OT システムにおけるセキュリティ異常対処支援サービス」（付録③参照）を活用することにより、脆弱性が突かれた攻撃を電文のモニタリングによって把握し、即時対処の支援を行います。

3.3.1. 現状

通常、医療機関には電子カルテシステムやオーダリングシステム等の院内ネットワークに接続しているシステムだけでなく、リモートメンテナンス等を行うための外部ネットワークと接続するためのシステムがあり、それぞれに適切なセキュリティ対策を施す必要があります。一般的に外部システムと接続する際には VPN と呼ばれる仮想の専用回線を用いることにより、リモートメンテナンス業者等特定の認証された人のみしかネットワークに接続できないよう対策が施されています。例えば、CT スキャン機器について機能追加がある場合、リモートメンテナンス業者は、図表 29 に記載のリモートメンテナンス用ネットワークから VPN 装置を介して CT スキャンシステム経由で CT スキャン機器のソフトウェアをメンテナンスします。厚生労働省から出ている医療情報連携ネットワーク支援 Navi にて近年増加していると解説されている「外部からの攻撃」にも「保守端末を経由した攻撃」が挙げられており、注意が必要です。

図表 29　医療機関のリモートメンテナンス



しかし、医療機関の情報化に伴う業務環境の変化に対して十分なセキュリティ対策が取られていないことや、攻撃者の手法の進化により、医療機関で把握されていないリモートメンテナンス用の VPN 等を介して侵入され、ランサムウェア攻撃を仕掛けられて情報の窃取や業務停止に追い込まれる等の事例が国内外で発生しています。

医療機関のセキュリティ体制に着目すると、ネットワークやシステムの脆弱性に対して、多くの大手病院においてはセキュリティベンダーへの監視の委託や MSS（マネージド・セキュリティ・サービス）等による不正通信等の 24 時間 365 日のシステム監視を実施しています。しかし、中小規模の病院では予算等の都合上こうした業務委託を行っていない場合や監視サービスに入っていないことが多く、万が一不正通信があった場合にも気づけない状況です。また、医療機関内にはシステム担当者が在籍しているものの、主な業務は業務用 PC の不具合等に関する対応であり、定期的にセキュリティを監視できる環境ではないのが現状です。

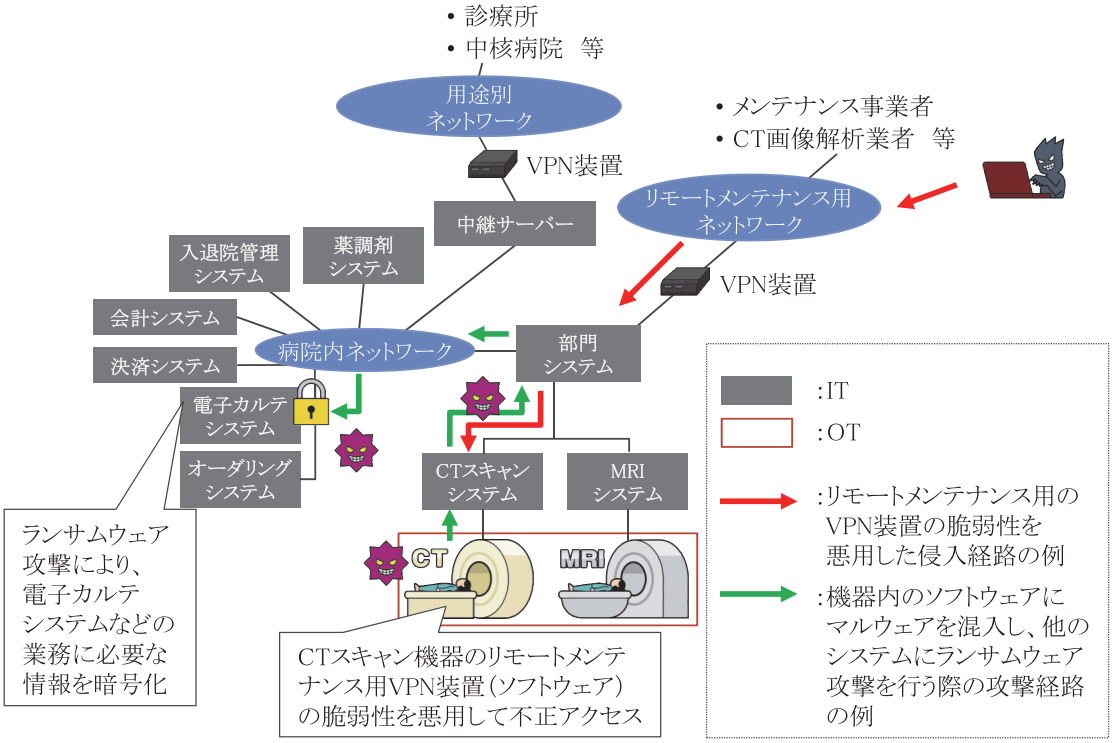
実際、厚生労働省が実施した「『病院における医療情報システムのバックアップデータ及びリモートゲートウェイ装置に係る調査』の結果について」[23] によると、「VPN 機器へのアクセス記録は定期的に検査しているか」というアンケートの問いに対して、VPN 機器が存在すると回答した医療機関のうち、約 6 割の医療機関が「いいえ」と回答しており、現状多くの VPN 機器へのアクセス記録は定期的に検査されていません。

例えば、先程の CT スキャン機器のリモートメンテンス用 VPN 装置について適切なセキュリティ対策が施されていなかった場合、VPN 機器の脆弱性を悪用した攻撃者に不正侵入され、院内システムにバックドアやデータの改ざんや不正取得、ランサムウェア攻撃等が仕掛けられてしまいます。この中でもマルウェアと呼ばれる不正なソフトウェアを介して他の院内システムに侵入し、電子カルテシステム等業務に必要な情報を暗号化してしまうランサムウェア攻撃は被害が甚大となる可能性があります（図表 30）。

暗号化されてしまうことで、診察・検査・治療が出来なくなるため、新規患者の受け入れが困難になる等、業務停止に追い込まれる可能性もあります。また、電子カルテシステムの情報等が暗号化されてしまうと、新規患者のみでなく、入院患者の治療にも大きな影響を及ぼします。

23 厚生労働省「『病院における医療情報システムのバックアップデータ及びリモートゲートウェイ装置に係る調査』の結果について」（2022 年 3 月） https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html

図表 30　リモートメンテナンス用 VPN 装置の脆弱性を悪用した攻撃の例



さらに、患者の診察情報等の機微情報を攻撃者に窃取され外部に流出してしまうことや、システムが復旧できるまで長期間に亘り診療が行えなくなることから、医療機関としての信頼を失墜させてしまう可能性もあります。特に医療機関は個人のプライバシーに深く関わる情報を多く保持しており、外部に流出してしまった場合は、患者から多額の損害賠償を請求される可能性も出てきます。他の業界でも、個人情報の流出により、多額の損害賠償が生じた事例があり、注意が必要です。

このように、医療機関はリモートメンテナンス用 VPN 機器の脆弱性リスクによって大きな被害を受ける可能性があり、病院長の責任を問われるような事態にもなりかねないことから、十分なセキュリティ対策を行う必要があります。

3.3.2. 解決策の方向性

医療情報システムのリモートメンテナンス用のネットワークに関する機器（VPN 等）に脆弱性がある場合、以下の図表 31 のような対策が想定されます。

図表 31　リモートメンテナンス用のネットワークに関する機器（VPN 等）に脆弱性がある場合に想定される対策

最新の脆弱性情報の確認及び対策	• 脆弱性がないか、最新情報を定期的に確認する • 発見された脆弱性について対応を行う
異常検知/一次対処	• 不正通信の検知及び一次対処により被害拡大を抑制する
改ざん検知	• ランサムウェア等悪意のあるソフトウェアをインストールされそうになった場合、PC上で機能することでインストールを阻止する
権限管理	• ランサムウェアがサーバーのデータを暗号化しようとした場合、権限管理により阻止する
証跡保管	• 攻撃や不正が起きてしまった場合、行為違反が記録されることで事象が判明し、責任の範囲と実施内容を説明できる

上記の図のように医療システムや機器類の情報を基に、攻撃シミュレーションを行うことができれば、脆弱性、及び想定される攻撃手法や攻撃ルート想定が可能となり、機器内のソフトウェアへの適切なアップデートの実施、ファイアウォールの設置、アクセス権限管理の強化等の対策を行うことができます。また、最新の脆弱性情報を定期的に確認することができれば、新たに発生したリスクへの対策が可能となります。

ところが、脆弱性が判明しても、電子カルテシステムを含むサーバー系で稼働している基幹システムの場合、Windows のアップデートを適用することにより正常動作しなくなる可能性があることから、どうしても適用せざるを得ない場合以外は実施していないといった実態があります（クラウドの電子カルテソリューション等を利用している等、サーバーや PC にソフトウェアを導入していない場合は状況が異なります）。中には、現在も Windows のアップデートができず、未だに Windows2000 を利用しているというケースも存在しています。

さらに、医療機器はリアルタイム性が重視されるため、膨大なデータを通信している場合、暗号通信が難しいケースもあり、データ漏えいや改ざんの対策が必要です。また、OS 等動作環境により、対策可能なソリューションが制限される可能性も考えられます。

このように様々な制約があり、十分な対策を講じることが難しい場合は可能な範囲から対策を講じることが重要です。まず、いち早く不正通信等の異常検知ができるよう、ネットワークを常時監視することが必要となります。また、万が一、サイバー攻撃を受けた際には、被害拡大防止のため、即時に通信を遮断する等の対応も必要となります。そのためには、一次対処に向けた支援サービスを導入することも考えられます。

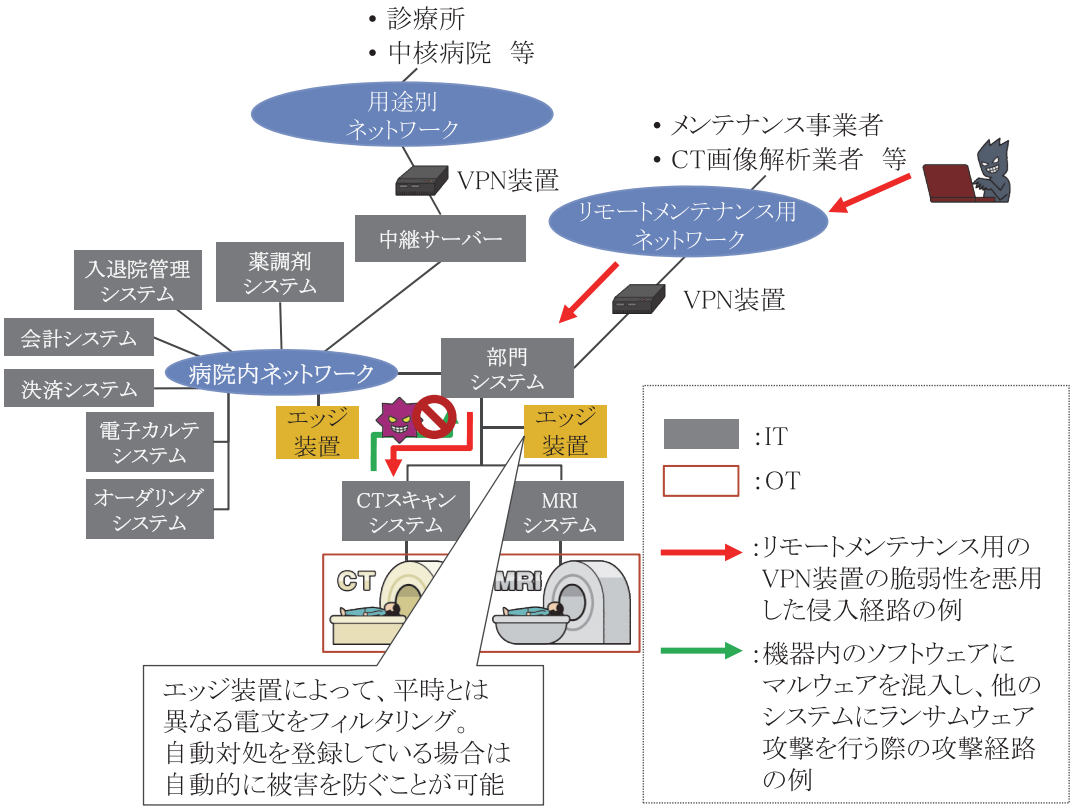
脆弱性に対するリスクを軽減させるためには、想定外の通信異常に気付き、その異常に対して対処できることが必要となります。具体的には、ソフトウェアの脆弱性の事前把握や、脆弱性を発端とする攻撃の早期発見から一次対処までのリードタイムの短縮が必要となります。また、一次対処までの時間を短縮するためには、影響範囲の特定やその影響に対する施策の絞り込みを効率的に実施できるかが重要なポイントとなります。

3.3.3. 具体的な対応：IoT や OT システムにおける セキュリティ異常対処支援サービス（付録③）

リモートメンテナンス用のネットワークに関連する機器の脆弱性に対しては、前述のように、機器のソフトウェアアップデートが難しいことや、取り得るセキュリティ対策にも制限があることから、異常を早期発見し、被害拡大に繋がらないよう速やかに一次対処を行える体制を整えることが重要です。

そのため、今回紹介する「IoT や OT システムにおけるセキュリティ異常対処支援サービス」では機器間の通信トラフィックを AI によって監視することで、ネットワーク上の異常を高精度に検知します（図表 32）。世の中には手順・形式等の取り決めを規定した様々な通信プロトコルが存在しますが、本サービスは多様な通信仕様に自動適応して監視することができるため、医療系専用プロトコルにも対応可能です。検知した内容を基に、事前に設定している業務の情報や可用性等のシステムの特性を踏まえて影響評価を行い、業務への影響が少ない対処を監視オペレーターに推奨することで、早期に適切な一次対処を行えるよう支援します。また、事前設定により、一次対処を自動化しておくことも可能です。

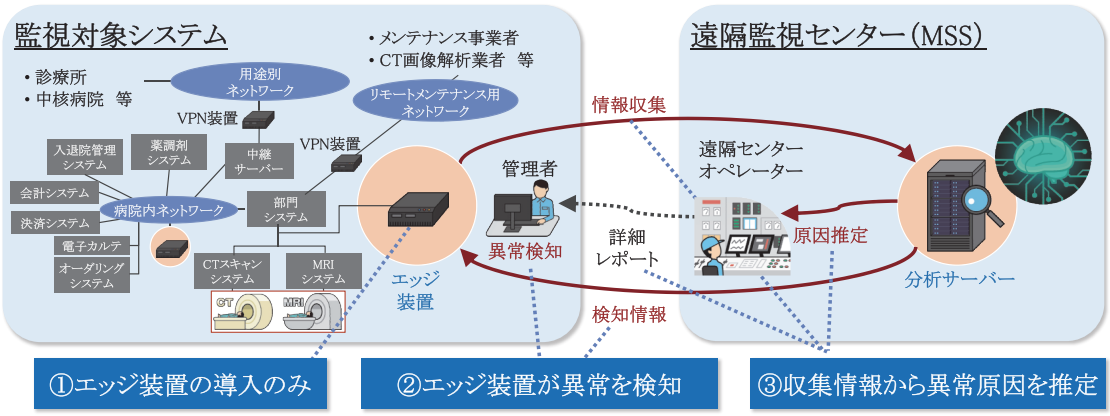
図表 32　リモートメンテナンス用の VPN 装置の脆弱性への対策例



図表 33 に記載のように、エッジ装置によって医療系専用プロトコルの通信状況を監視し、通信容量の急激な増加等通常とは異なるパターンが異常として検知します。そして、分析サーバーによって原因が推定されることで、検知後速やかに一次対処策として通信遮断が行われます。

「IoT や OT システムにおけるセキュリティ異常対処支援サービス」にて常時監視されることで、異常検知からの一次対処が行いやすくなるため、リモートメンテナンス業者が CT スキャン機器等の機能追加や仕様変更を行う際にも安心して作業することができます。

図表 33　セキュリティ異常対処支援サービスで導入するエッジ装置や分析サーバー



既存のセキュリティ監視技術と異なる、本サービスの強みとしては以下 3 点が挙げられます。

1 点目「既存システムに影響を与えない導入」では、後述する「エッジ装置」をシステム構成の変更なく既存の監視対象のシステムに設置することで、容易に通信の監視を行うことができます。

2 点目「一次対策案の支援」は、業務の情報やシステムの可用性等のシステム特性情報をインプットとして用いることで、業務影響を考慮した一次対処案を提示できることが大きな特徴です。従来技術では業務への影響が考慮されていない一次対処案を推奨するものが多く、異常検知後に現場主体で業務への影響判断を行うことになるため一次対処までに時間を要していました。本サービスは一次対処までの時間を短縮することが可能となるため、被害拡大防止に貢献します。

3 点目「AI を活用した自動監視」では、監視対象となるシステム群にエッジ装置を設置するだけで、監視対象システムの「正常」とされる基準を自動的に把握して学習モデルが作られ、

自動監視へ移行します。そのため、システム構築時だけでなく、既に稼働している設備にも容易に後付けで導入することができます。

前述のとおり「IoT や OT システムにおけるセキュリティ異常対処支援サービス」を活用することで、異常を早期発見し、速やかに一次対処を行うことが可能となるため、ランサムウェア攻撃によるデータの暗号化や情報漏えい被害を防ぐことができます。

IoT や OT システムにおけるセキュリティ異常対処支援技術に関する
問い合わせ先

日本電信電話株式会社 社会情報研究所
Email : solab@ml.ntt.com

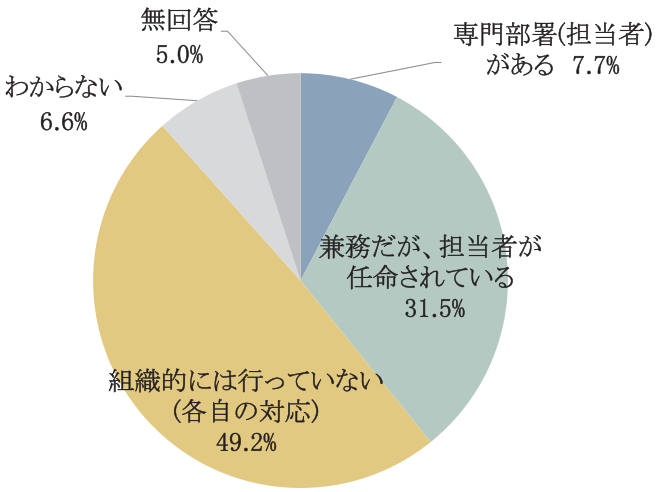
3.4. 自社で脆弱性を検討できないことによる放置リスクへの対策

本節では近年特に対策が求められている「(図表 18) リスク D) 自社で脆弱性を検討できないことによる放置リスク」を事例として取り上げ、サイバー・フィジカル・セキュリティ対策基盤の「IoT や OT システムにおけるセキュリティ異常対処支援サービス」(付録③) を活用することにより、どのように対策を行うことができるかについて具体的に説明していきます。

3.4.1. 現状

自社の体制で OT システムのリスク診断を出来ていない企業が多く存在しています。リスク診断には一定のスキルを持つ技術者が必要となりますが、中小企業にはそのような人材が少なく、新規に雇うことも難しい状況です。IPA の調査によると、5 割弱の中小企業が情報セキュリティの対策を組織的に行っていません（図表 34)。

図表 34　情報セキュリティの組織体制

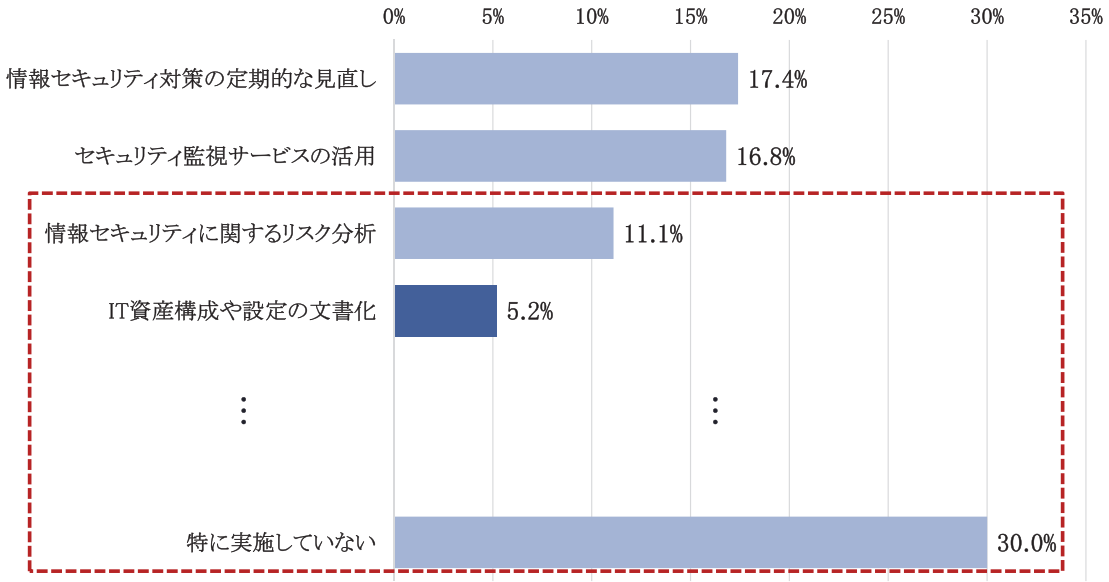


（出典）IPA「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」(2022 年 3 月)

IPA の同調査では、被害防止のための組織面･運用面での対策について「情報セキュリティに関するリスク分析」が 11.1% と自社でのリスク分析は低水準に留まっています。外部委託の状況・内容においても「セキュリティ検査・監査サービス」が 4.5% と低く、リスクが放置されています（図表 35）。

また、IT 資産構成や設定の文書化もされていないことから、OT についても同様の傾向にあると考えられ、リスク分析を行う手前の現状把握ができていない中小企業が多く存在するものと想定されます。自社の代表的な OT である製造設備が閉鎖網であることから､サイバー攻撃を受けないと判断しているケースが多くあります。2015 年に発生した日本年金機構の個人情報漏洩事案は閉域網にもかかわらず、職員によるルール逸脱行為が起因となって発生しました。そのため、閉鎖網であってもサイバー攻撃を受ける可能性があるという前提に立ち、確認していくことが必要です。

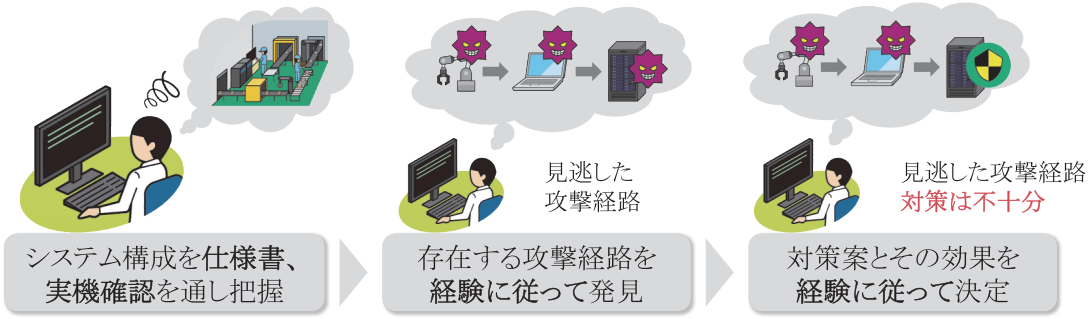
図表 35　中小企業における被害防止のための組織面・運用面での対策（複数回答）



（出典）IPA「2021 年度 中小企業における情報セキュリティ対策に関する実態調査」（2022 年 3 月）を参考に作成

脆弱性リスクを放置している場合は、情報流出だけでなく、システム停止や誤作動による被害（改ざん含む）等が発生する恐れがあります（図表 36）。また、当初は攻撃を受けた被害者の立場であるものの、被害がサプライチェーン上の会社に拡大することで加害者側の立場に立ってしまう場合もあります。サプライチェーン上で被害を拡大させてしまった場合は、サプライチェーンから外され契約を切られる可能性があることから、製造や運用に関わっている企業は対応が必要になるものと想定されます。

図表 36　自社でリスク分析できないためにリスクを放置



3.4.2. 解決策の方向性

脆弱性リスクを放置しないためには、定期的にリスク分析を行い、そこで判明したリスクについて対策を検討できる体制を構築する必要があります。ただし、中小企業ではリスク分析や対策検討を行うための人材を雇い入れることが難しい状況も想定され、その場合は外部の脆弱性診断サービスの活用が有効と考えられます。有償で様々なレベルのものが存在しており、政府でも「サイバーセキュリティお助け隊サービス[24]」等による支援体制を整備しています。

しかし、業務系ネットワークと生産管理ネットワークは分離されており、生産管理は閉域網との意識から、ネットワークにおけるセキュリティ対策の必要性がないと認識され、脆弱性を把握したとしてもアクションを取ろうとしていない場合が多く存在しています。閉鎖網であってもサイバー攻撃を受ける可能性があること念頭に検討することが重要です。

また、OT の場合は事業継続性を大事にすることから、Windows アップデートを適用するとシステムが正常稼働しなくなる、システムを停止できないといった事情によって、OS や制御系システムのアップデートがされておらず、脆弱性が放置されているケースがあります。既存のサイバー・セキュリティ対策ソリューションは、OS が一定のレベルにアップデートされていることが前提となるため、その状況に合わせて、必要となる対策を講じる必要があります。

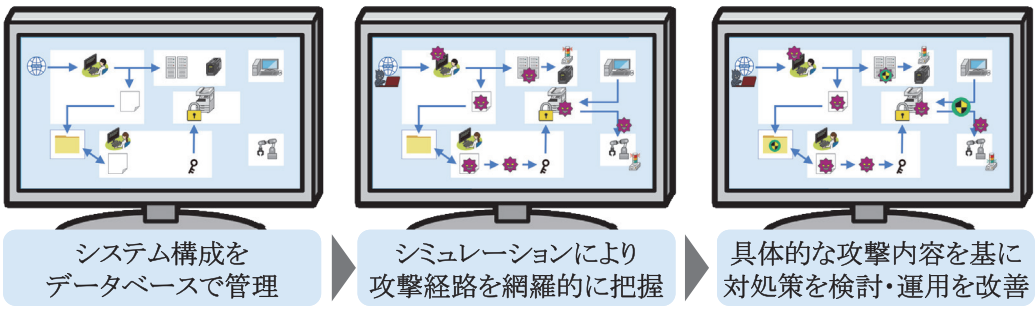
24　https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html

さらに、ネットワークを常時監視することで、サイバー攻撃を受けた際に不正通信等の異常検知を即時に検知し、被害拡大防止のため、即時に通信遮断等の一次対処を遠隔に実施するための支援サービスを導入するといった対応が必要になります。

3.4.3. 具体的な対応：IoT や OT システムにおけるセキュリティ異常対処支援サービス（付録③）

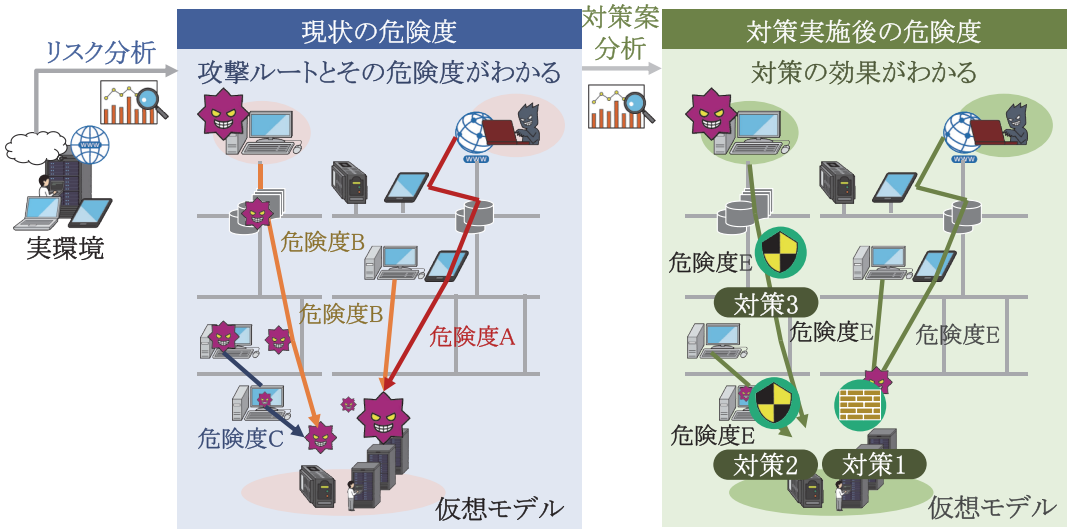
リスク診断が難しいという問題に対しては、高スキルを持たない要員でもリスク診断できるツールを活用して自社にて実施するか、安価な外部サービスを活用してサプライチェーン配下の企業がリスク診断サービスを定期的に実施し、改善活動に取り組んでいくか、どちらかの対応が必要となります。そのため、今回、紹介する「IoT や OT システムにおけるセキュリティ異常対処支援サービス」の一機能であるリスク診断機能は、設備情報を登録することにより攻撃シミュレーションが行われ、脆弱性が洗い出されます（図表 37）。

図表 37　リスク分析ができることによって対策検討が可能



従来の支援ツールよりも自動化される範囲が広いことから、熟練者でなく、ある一定程度の知識を持った要員であれば、分析レポート作成や分析が可能です。また、外部の診断サービスを提供する事業者がこの技術を活用することで、現状よりもコストを低減できると想定されます。安価になることで他サービスや機器提供に付帯して診断サービスが提供されていくことも考えられます（図表 38）。

図表 38　リスク診断のイメージ



攻撃被害

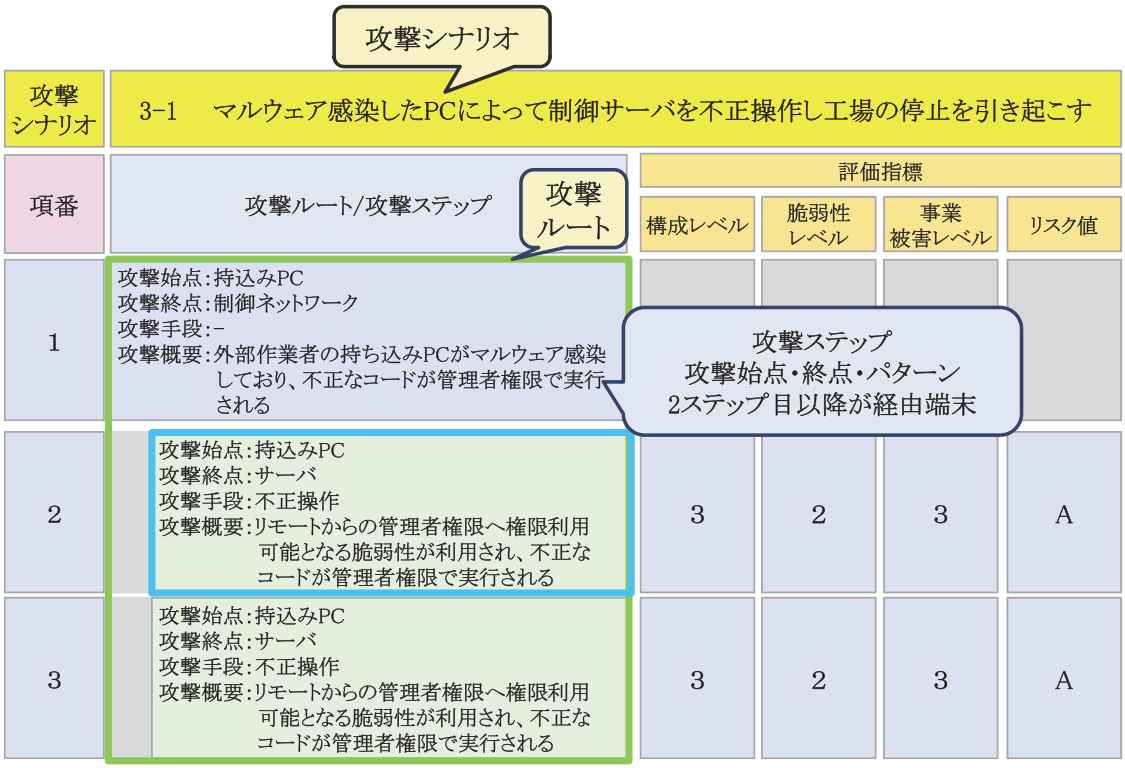
侵入口/攻撃目標	不正操作	ﾃﾞｰﾀ改ざん	ﾃﾞｰﾀ搾取	機能停止
①Internet/ﾌｧｲﾙｻｰﾊﾞｰ	A	A	A	A
②社内端末/ﾌｧｲﾙｻｰﾊﾞｰ	B	B	B	B
③遠隔端末/ﾌｧｲﾙｻｰﾊﾞｰ	B	B	C	B
④操作端末/ﾌｧｲﾙｻｰﾊﾞｰ	C	D	D	C

攻撃被害

	不正操作	ﾃﾞｰﾀ改ざん	ﾃﾞｰﾀ搾取	機能停止
対策1	E	E	E	E
	E	E	E	E
	E	E	E	E
対策2	E	E	E	E
			対策3	

診断対象の企業が製造業の場合は、本ソリューションの初期設定としてIPA公表のガイドラインの遵守状況についてレポートとして出力可能となっています。本ソリューションによって対策が十分ではない箇所を特定でき、効率的に対策を講じることもできます。このため、事前のサイバー・フィジカル・セキュリティ対策を実施しやすくなることで、サイバー攻撃リスクを低減することができます（図表39）。

図表39　ガイドラインに沿った分析レポートの出力



IoTやOTシステムにおけるセキュリティ異常対処支援技術に関する
問い合わせ先

日本電信電話株式会社　社会情報研究所
Email：solab@ml.ntt.com

3.5. 不適正な組織・事業者の接続への対策

本節では近年特に対策が求められている「（図表 18）リスク E）不正アクセスによる情報漏えいや改ざん」を事例として取り上げ、サイバー・フィジカル・セキュリティ対策基盤の「信頼できる取引ネットワーク構築サービス」（付録④）を活用することにより、どのように対策を行うことができるかについて具体的に説明していきます。

3.5.1. 現状

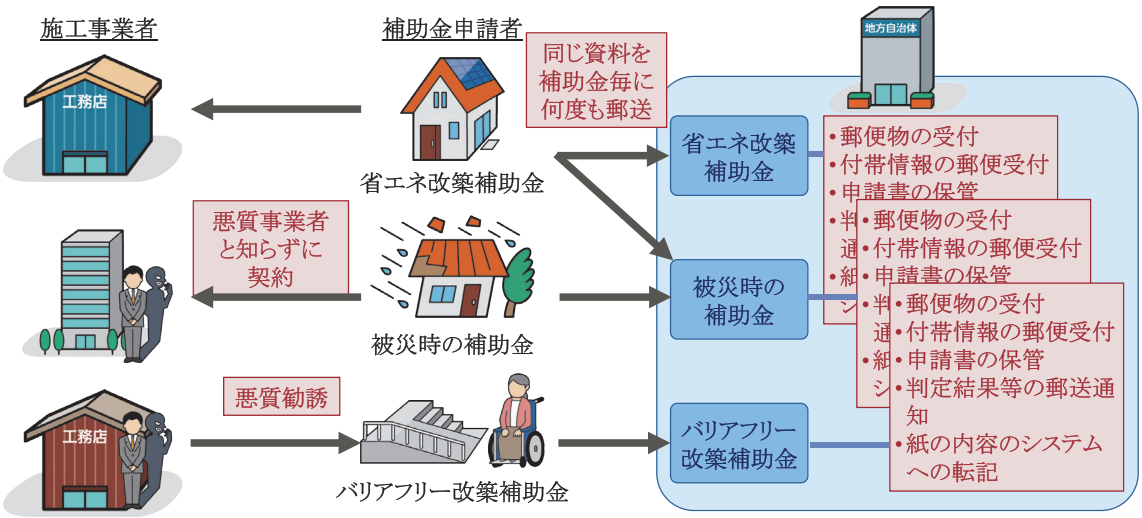
行政において、行政機関の効率化だけでなく利用者の利便性向上を念頭にデジタル化が推進されてきており、その一環として窓口業務である申請手続や交付手続のオンライン化が進められています。しかし、未だオンライン化されていない窓口業務があることや、地域の事業者や町内会等の外部関係者と協調しながら進めていく自治体業務についてはオンライン化されていない業務が多く残っています。

外部関係者と協調しながら進める自治体業務では、外部組織の健全性や資格を検証するための情報や経営状態を示す情報等、秘守義務を伴う情報や取り扱う情報毎に異なった情報管理ルールが定められているものがあります。そのため、情報アクセス権限の複雑な制御やシステムを分離しなければならないケースがほとんどであり、オンライン化による情報共有が進んでいない状況にあります。

例えば、住宅補助金事業では、補助金申請の受付はオンライン化されていても、申請書、申請書に付帯する工期や費用、図面、工事内容等の申請に付帯する詳細情報、工事完了後の報告等、本人確認情報や秘守義務の伴う情報は、郵送や面談によって流通しています。さらに申請においては、複数の施工事業者が工事を行う場合や、施工事業者による代行申請も可能である等、申請者毎に、情報を共有する関係者が異なります。そのため、管理ルールが複雑になり、オンライン化が進まず、紙で管理されているのが現状です。紙の運用であるため、郵便の受け取り、面談、保管場所の管理等、職員の負担を強いています。また、複数の関連した申請を行う場合、補助金毎に別々に申請する必要があることから、同じ情報を何度も郵送・面談により提出する必要があり、申請者にも負担を強いているのが現状です。

さらに、住宅工事は悪徳事業が比較的多い業界であり、申請時に事業実績や経営状態等、施工事業者の検証ができれば、被害を少なくすることができるため、税金の有効活用に寄与すると考えられます。しかし、申請毎にデータが別々に紙で管理されているため、実績データに基づく施工事業者の健全性検証も困難な状況です（図表 40）。

図表 40　申請内容によって異なる受付体制



このように、利用資格者の検証や細やかなアクセス制御の実現は非常に難しいため、現状では比較的立ち上げることが容易な個々の案件毎にシステムが整備されています。そのため、共通化すべき機能があるにもかかわらず、個別対応を行い、対応費用が大きくなります。また、新しい試みを実施する際にシステムの立ち上げ待ちといった状況も発生します。

3.5.2. 解決策の方向性

個々の案件毎にシステムが作られるという問題については、単にシステムを共通化すれば良いというわけではなく、データ連携可能とすることが重要であり、個別最適に陥らずに全体最適を図る必要があります（図表 41）。また、見知らぬ接続相手とサイバー空間上で相対するには、相手先の信用性や安全性を検証できる機能を構築することで、接続先や流通する情報の真正性を確保できる接続検証が必要となります。そのため、接続検証には、現状のフィジカル空間とサイバー空間で個々に行われている検証をサイバー空間において連続性を確保しつつ、公平性を確保する必要があります。

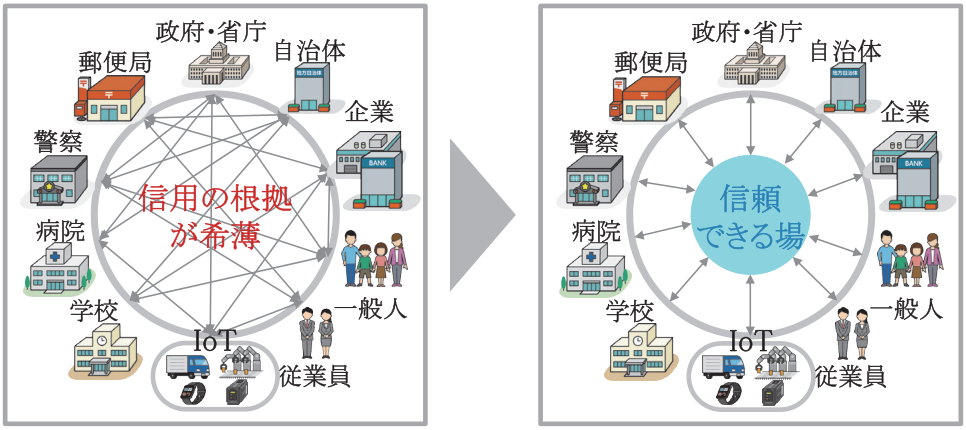
図表 41　共通化されるべき機能群

#	データ	概要
1	ログイン情報	申請者を特定する ID やパスワード
2	申請に付帯する情報	申請者の適正を示す情報（組織や事業者の存在や申請資格）
3	情報へのアクセス許諾に必要な情報	情報に対しアクセスする組織・事業者の健全性を示す情報

情報へのアクセス許諾に必要な情報については、情報毎に存在する法令や条例等の遵守すべきルールに則りシステマティックに制御する仕組みが必要です。また、対象事業が増えた場合には、既に存在するデータへのアクセス許諾の追加等が必要で、以下の要件を満たす複数目的で活用可能なシステムが求められます。例えば、図表 42 のように、政府･省庁、自治体、企業、一般人等、様々な人や組織等を制御しなければなりません。

1）接続時に厳格な利用者の資格（権限）確認を実施
2）様々な利用目的に沿って、情報へのアクセス権限を動的に制御

図表 42　求められる動的なアクセス権限の制御



【現在】
- 送られてきたメールやデータは正しいのか？
- 相手は信頼できる人か

【今後】
- 安全、かつシンプルな繋がり（人/組織/クラウド間等）を実現

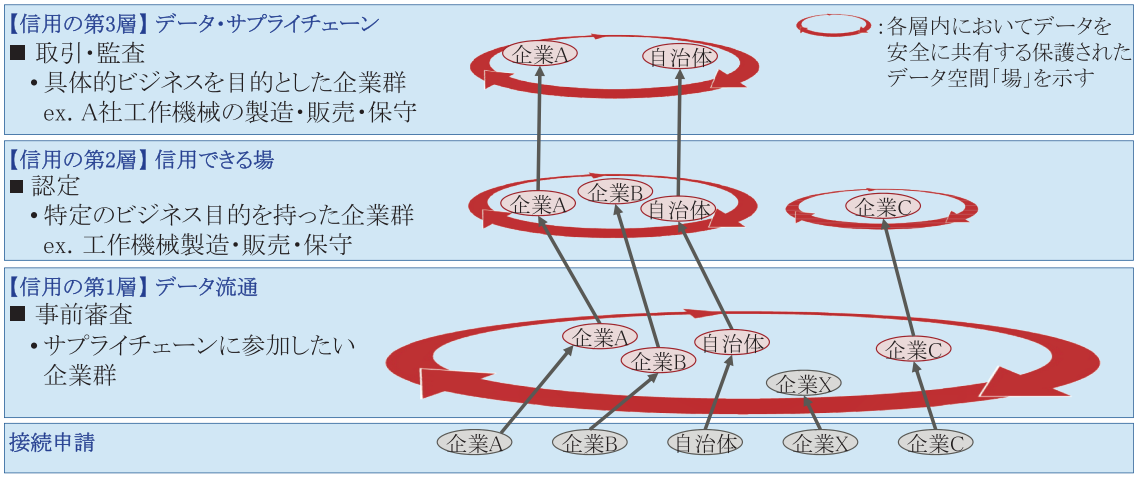
「地方公共団体における情報セキュリティポリシーに関するガイドライン」において、アクセス制御や制限等の要件が示されているものの、「様々な利用目的に沿って、情報へのアクセス権限を動的に制御」に対する要件は十分ではありません。今後の業務効率化を踏まえると、「アクセス権限の動的な制御」は考慮すべき要件と考えられます。

3.5.3. 具体的な対応:信頼できる取引ネットワーク構築サービス(付録④)

「信頼できる取引ネットワーク構築サービス」を用いることで、接続先が提供する属性情報の検証によって、利用資格のない接続申請者を排除しつつ、接続先が持つ資格(権限)に応じてアクセス権限を付与するサービスを様々な目的横断で構築することができます。「信頼できる取引ネットワーク構築サービス」では、誰でも接続可能なオープンなネットワーク環境において、接続先の検証を行い、問題ないと判断のついた組織間で安全なデータ流通が保証される仕組みを実現しています。

具体的には、「事前審査」、「認定」、「取引・監査」の3つの層に流通させる情報を分け、段階的に接続先の組織を選別することで安全なデータ流通を実現しています(図表44)。第1層(事前審査)では、サプライチェーン企業群の企業情報や与信情報等の組織の機能や状態を示す情報を流通させることで、接続検証を行います。第2層では、第1層の企業群のうち特定の目的を持った企業群の提供プランや提供範囲等の組織のサービス能力を示す情報を流通させ、接続検証を行います。最後の第3層(取引)では、取引・監査として第2層の企業群のうち具体的な取引を目的とした企業群の利用申請情報や利用資格保有情報等の組織実行能力を示す情報を流通させ、接続検証を行います。各層で流通させる情報は、各層に設ける保護されたデータ空間「場」に保持され、改ざんや漏洩、不正アクセスから守られます。これを信用の3層モデルと呼んでいます(図表43)。

図表43 信用の3層モデル



図表44のように信頼できるネットワークを構築することにより接続先の真正性が保証され、申請内容の確認範囲を狭められることで、行政やその他ステークホルダーにおける確認稼働の削減を期待できることや、無資格者への情報流出や不正申請を防ぐことができます。

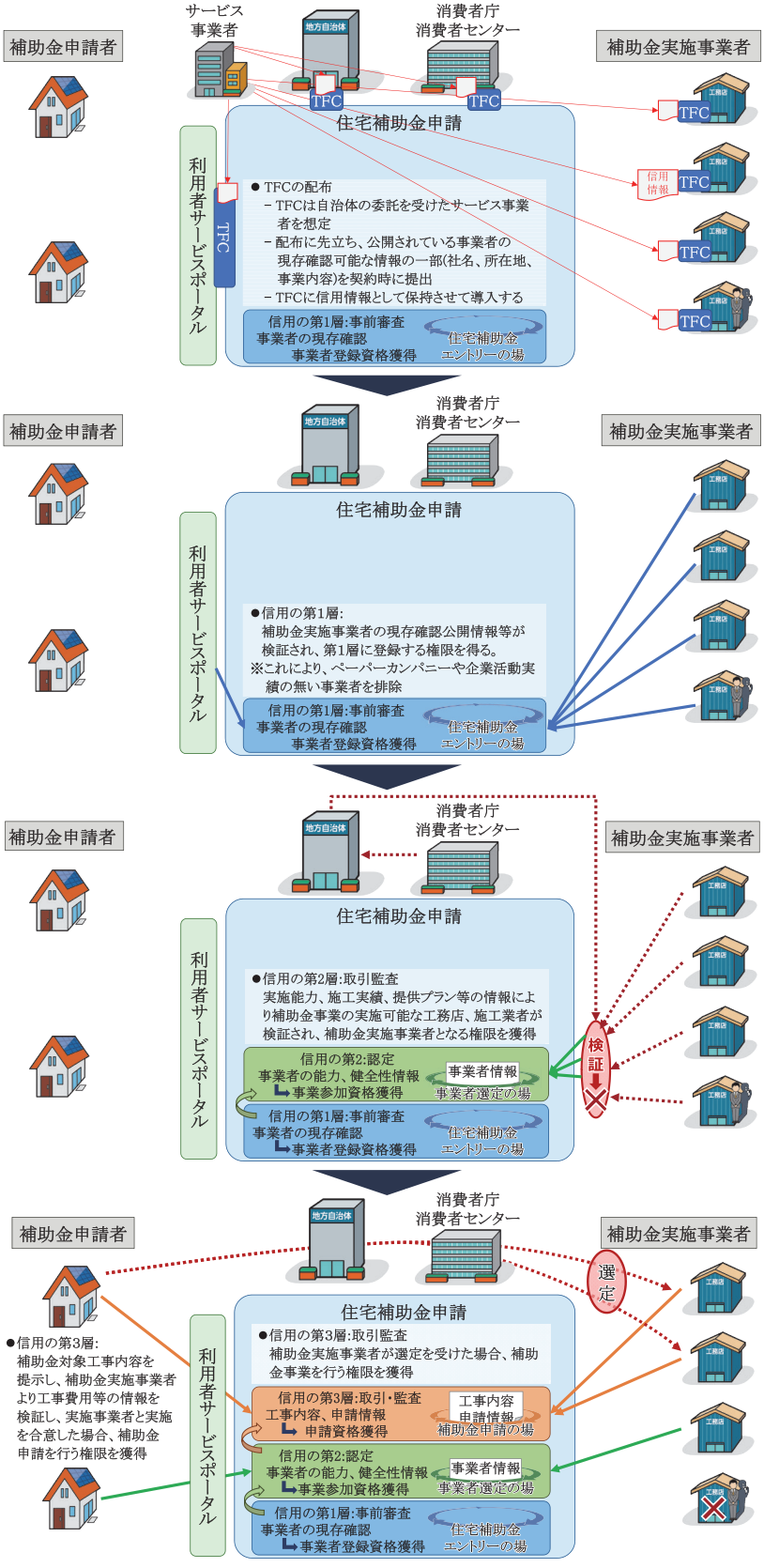
図表 44　信頼できる取引ネットワーク構築の流れ

①導入
地方自治体から委託を受けたサービス事業者が補助金実施事業者に現存確認可能な信用情報を書き込んだうえでTFCソフトウェアを配布する。
➢ 事業者は信用の第1層「住宅補助金事業エントリーの場」に自動的に参加

②信用の第1層
[事業者登録資格獲得]
信用の第1層に参加した事業者は、他事業者より健全性検証ができるよう自身の身元や活動内容が確認できる信用情報を追加登録
➢ 信用情報が提供できないペーパーカンパニーのような事業者は、この段階で除外

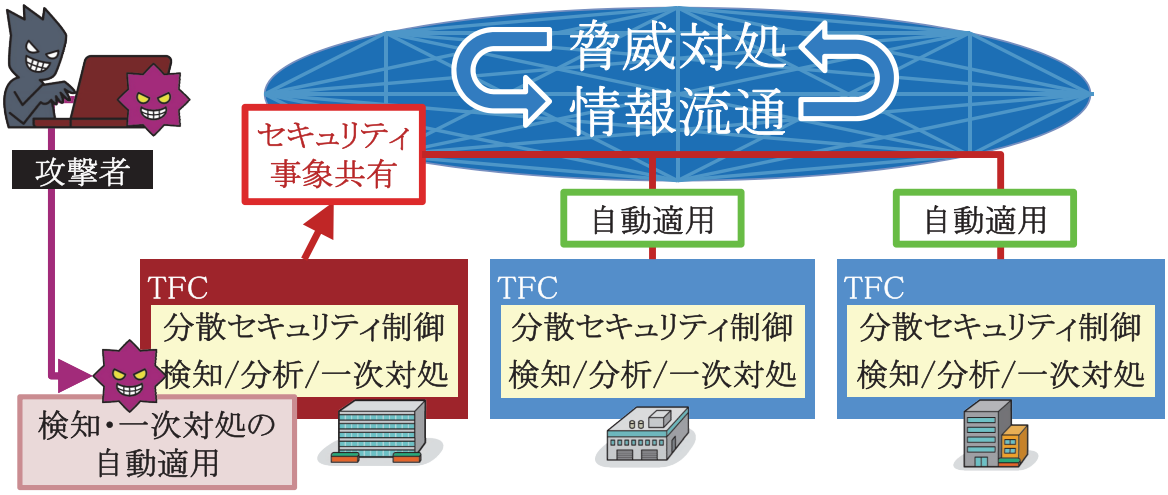
③信用の第2層
[事業参加資格獲得]
信用の第2層「事業者選定の場」を作り、実施能力・施工実績・提供プランなどの信用情報により補助金事業の実施可否を参加事業者によって検証し、事業者を絞り込む
➢選定された事業者が補助金事業への参加資格を獲得

④信用の第3層
[事業申請資格獲得]
信用の第3層として「補助金申請の場」を作り、事業者の活動実績に関する信用情報を補助金申請者が検証し、補助金事業にふさわしい事業者を選定
➢資格を獲得選定された事業者が補助金事業を実施する資格を獲得



3層モデルをオープンなネットワークで安心して実行するには、接続用ソフトウェア（TFC（Trustworthy Field Constructor）[25]、付録④参照）によって構成するネットワーク全体をセキュリティ脅威から守ることが必要です。接続先の持つフィジカル空間の固有情報をTFCによって接続検証することで、フィジカル空間とサイバー空間で検証された組織の一意性を保証します（図表45）。

図表45　TFCによる信頼できる取引ネットワーク構築サービスへの接続



また、接続先のセキュリティ事象を常に監視していることから、脅威検知時の自動対策適用や、その脅威情報を他接続先へ展開できるため、セキュリティ攻撃への対策も徹底されます。

信頼できる取引ネットワーク構築サービスに関する問い合わせ先

富士通株式会社
キャリア＆メディア事業本部 NTTソリューション事業部
Email：contact-sip2-b2@cs.jp.fujitsu.com

25　SIPで技術開発したソフトウェアゲートウェイ

3.6. サプライチェーン上で流通するデータ改ざんへの対策

本節では近年特に対策が求められている「(図表 18) リスク F) 内部による不正行為」を事例として取り上げ、サイバー・フィジカル・セキュリティ対策基盤の「サプライチェーン・トラスト・ソリューション」(付録⑤) を活用することにより、どのように対策を行うことができるかについて具体的に説明していきます。

3.6.1. 現状

企業の対策が不十分な結果、医療機器の製造データや検査データが改ざんされてしまうことで、本来は製品検査に合格しない不適合な医療機器が出荷され医療機関に納品されてしまう恐れがあります。その結果、設計時点で意図したとおりに医療機器が動作しなくなる恐れがあります。現在は、登録時の虚偽登録や、データの改ざんに気づくことが難しい状況になっています。このような内部不正は様々な業種で発生しています (図表 46)。

図表 46　国内における内部不正事例一覧

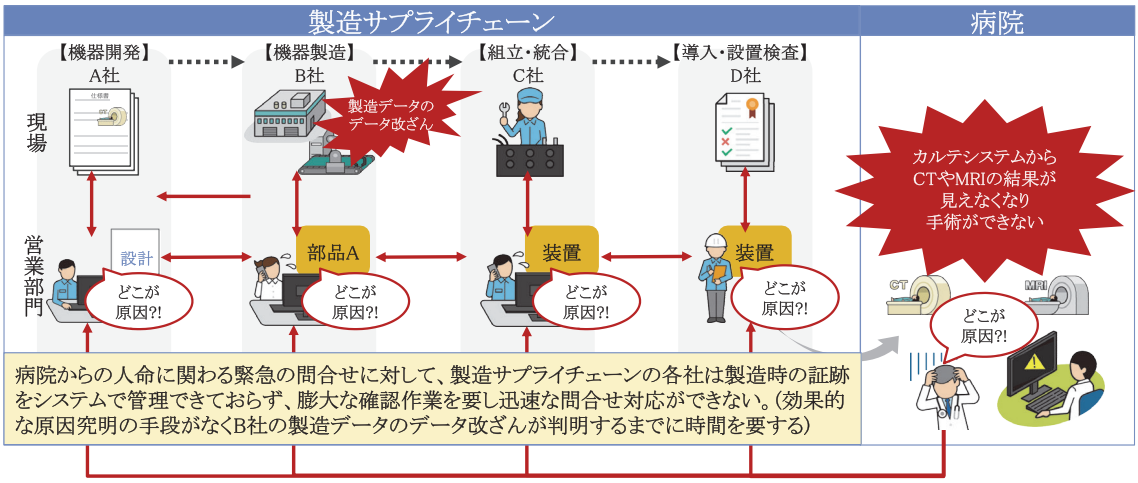
#	事例	時期	分野	原因	品質への影響	被害、信頼への影響
1	建設工事に関する国家資格の不正取得	2021/8	建設	規程違反	不明	• 施工品質への信頼棄損。全物件で第三者機関に施工品質の検証を依頼
2	鉄道向け空調機器、空気圧縮機の検査不正	2021/6	産業用機器	規程違反	不明	• 規程に沿った検査実施、製品の安全性への信頼棄損
3	医療事故検証結果報告書への虚偽記載	2019/10	医療機関	規程違反	不明	• 報告書への信頼棄損 • 原因究明と再発防止に向けた取組みの阻害
4	医師によるカルテ改ざん	2020/9	医療機関	規程違反	不明	• カルテ情報への信頼棄損による不正受給の疑い
5	新幹線車両台車枠の仕様外製品の納入	2018/2	車両製造	規程不備	あり	• 新幹線車両台車枠に亀裂 • 製品、サービスの安全性への信頼棄損
6	アルミ・銅製品の品質データ改ざん	2017/10	鉄鋼	規程違反	なし	• 規程に沿った検査実施、製品の安全性への信頼棄損
7	産業ゴム製品の検査不正	2017/3	産業用部品	規程違反	あり	• 規程に沿った検査実施、製品の安全性への信頼棄損

医療機器に不具合や不備があると、結果的に医療活動に支障が出てしまいます。具体的には、対策が不十分な結果、機器不良による医療活動の制限、医療情報の改変による人命への被害発生が想定されます。

上記のような事態が発生した場合、ベンダーはリコールによる損害やブランドの毀損、損害賠償にも発展する恐れがあり、医療機関も信用失墜等にもつながってしまいます。

現代では、サプライチェーン全体でのアカウンタビリティ（説明責任）を果たし、製品やサービスの価値（製品・サービスの差別化・競争力強化）を評価することが重要となってきています。しかし、サプライチェーン全体でアカウンタビリティを果たすには膨大な工数が必要となることから対応が進んでいない状況です（図表 47）。

図表 47　問題発生時の確認作業イメージ



3.6.2. 解決策の方向性

タイムスタンプの利用及び計測器や計測方法の信頼性を高めることによって、データがある時点で存在し、そこから改変されていないという信頼性は担保できます。一般的に「仕様通りに実施していたか」の証跡を取得した上で、サプライチェーン上の企業間で横断的にその証跡を情報流通させるには共通言語が必要です。

ただし、サプライチェーン上の企業によって規程類の解釈や証跡として残している情報が異なっており、実際には共通化が難しい状況です。また、サプライチェーン上の企業間で、上記を共通化することや証跡を適切に保管して共有することが難しい状況も対策が進まない1つの要因となっています。

その証跡に医療機器の製造設計データ等の機微情報が含まれるためサプライチェーン上でデータの参照権限について細やかな制御ができていなければならず、サプライチェーン上の各企業においてデータのトラストを担保し、サプライチェーンに属する企業間で共有することのできるシステム基盤が必要になります。このシステム基盤を構築するには様々なソフトウェアを組み合わせて構築する必要があり、対応費用が高価になってしまう状況です。

また、データ駆動型社会において、流通するデータの信頼性確保が不可欠です。データが信頼できない場合は、サイバー・フィジカル・システムの制御そのものの信頼性が担保できないためです。

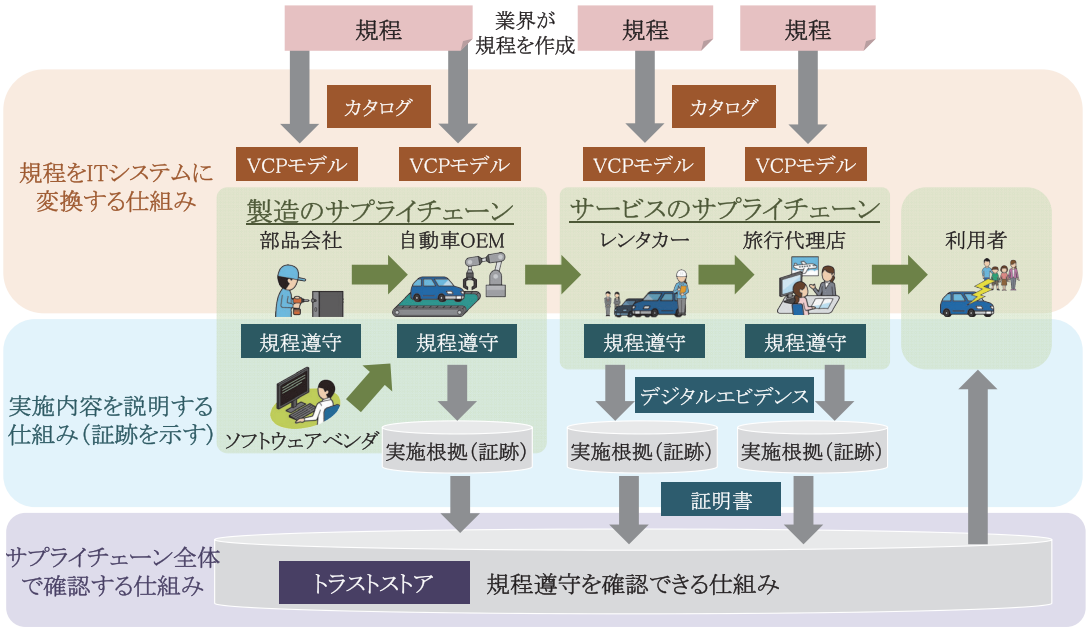
そのため、上記を解決する製品・サービスがサプライチェーン全体で適切な規程に従って、製造・運用されたことを、容易にかつ効率的に確認できる仕組みを利用することが望まれています。

3.6.3. 具体的な対応：サプライチェーン・トラスト・ソリューション（付録⑤）

権限を逸脱した行為や規程違反を防ぎ、製品やサービスを提供するためには、サプライチェーン全体で適切な規程に従い生成、運用された製品であることを、容易かつ効率的に確認できる仕組みが必要となります。

規程内容について記述方法である VCP（Value Creation Process）モデルによって、「規程に従い生成されたこと」、「確認方法」、「エビデンス」を関連付けて、「信頼性の裏付け（デジタルエビデンス）」として証跡化することができます。その証跡をトラストストアから辿れるようにすることで、サプライチェーン内に適切に共有することができるようになります。製品・サービス等がサプライチェーン全体で適切な規程に従って生成、運用されていることを、容易にかつ効率的に確認し合えるようになります（図表 48）。

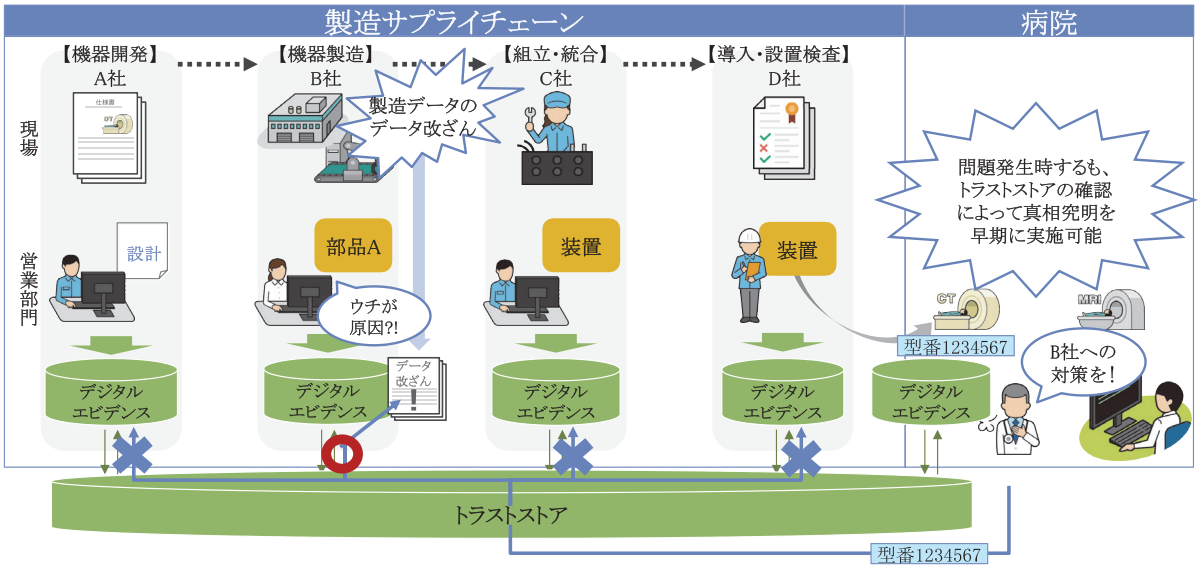
図表 48　サプライチェーン・トラスト・ソリューションの対応イメージ



上記機能が含まれているサプライチェーン・トラスト・ソリューションを活用することで、製品・サービスが、サプライチェーン全体で適切な規程に従い生成、運用されたことを容易にかつ効率的に確認できるようになります。現場やデータベース上で改ざん余地を低減させ、サプライチェーン全体で規程に従って適切に機器が製造されたことを客観的なデータを用いて対外的に証明できるようになります。

また、トラストストアによって製造データや検査データの証明書を共有することが容易になるため、問題が発生した場合はサプライチェーンの情報を遡ってデータを確認できることによって、原因究明を行いやすくなることや監査機関等への情報提供も簡便に対応できるようになります（図表 49）。

図表 49　サプライチェーン・トラスト・ソリューション導入後の問題発生時の確認作業イメージ



VCP（Value Creation Process）モデル

VCP モデルは、「規程に従い生成されたこと」、「確認方法」、「エビデンス」を関連付けて記述できる機械可読なプロセスモデル記法です。記述できる内容に「規程に従い生成されたこと」が含まれていることから、記録されている規程順守状況を容易に検索できます。

本技術は、サイバー・フィジカル・セキュリティ対策フレームワークに対応させるため、SIP のプロジェクトにて開発した技術になります。業界団体等で業界として求められる規程を反映させた「共通 VCP モデル」を用意することで、サプライチェーンに属する企業間のルール解釈のバラツキを解消し、順守状況の相互運用性を高めることが期待できます。

サプライチェーントラストソリューションに関する問い合わせ先

株式会社日立製作所
　サービスプラットフォーム事業本部 マネージドサービス事業部
　SIP2_B3_info1@ml.itg.hitachi.co.jp

第４章
対策の企画・導入の進め方

☑ ポイント①
サイバー・フィジカル・セキュリティ・対策フレームワークのセキュリティ・リスクマネジメントの流れを参考に、検討の流れを説明しています。

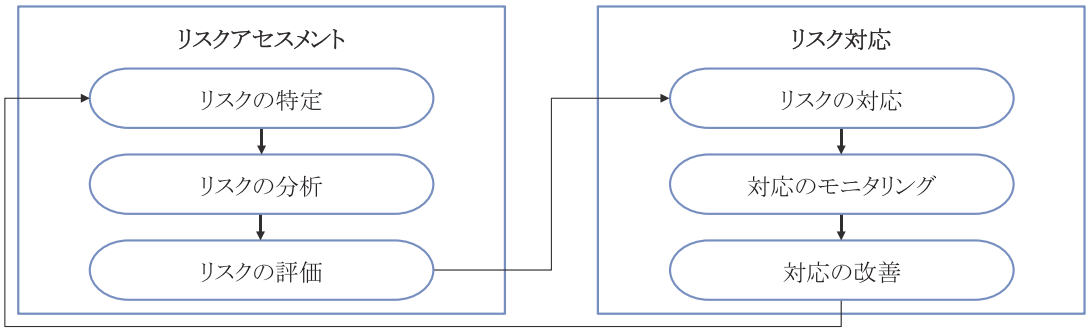
☑ ポイント②
現状のサイバー・フィジカル・セキュリティの対策について十分性を確認するためのチェック項目例を用意しているので、確認してみてください。

第3章ではサイバー・フィジカル・セキュリティの代表的なリスクに対して、必要となる対策を具体的な業界を用いて解説を行いました。本章では、SIPのサイバー・フィジカル・セキュリティ対策基盤が提供する5つのソリューション（以下、「SIPソリューション」という。）の導入を前提に、実際にソリューションを導入する際の流れ及び運用の流れについて説明します。

サイバー・フィジカル・セキュリティに対する対策検討の流れは、リスク分析の対象となる領域を特定した後に、その構成要素を整理していく中でセキュリティ・リスクについての洗い出しを行います。その後、各セキュリティ・リスクが事業に対してどの程度の被害を発生させるのか、被害の大きさとその発生可能性を評価することで、対応策の検討すべき領域や必要となる対策が決定されます。導入すべきソリューションの選定については、複数のソリューションによって比較検討が必要となりますが、本書では第2章で紹介をしているSIPソリューションの導入を前提に、実際にソリューションを導入する際の流れ及び運用の流れについて説明します。

なお、サイバー・フィジカル・セキュリティ・対策フレームワークのセキュリティ・リスクマネジメントの流れを参考に、図表50の流れで解説します。また本フェーズでは、ソリューション①「インシデント検知」を活用した場合とそうでない場合に分けて検討の流れについて記載を行い、具体的な事例として病院を例に記載しています。

図表50　セキュリティ・リスクマネジメントの流れ



4.1. リスクアセスメント

インシデント検知が必要となる状況では、脆弱性が組み込まれているOSS（オープンソースソフトウェア）等の部品でシステムが構成されていることや、完全な閉域網ではないこと等を把握した上で、何らかのセキュリティ・インシデントが発生した場合に業務継続性が著しく損なわれることや、情報漏えい等の発生等による社会的使命が損なわれることがないかの確認が重要となります。

リスクアセスメントでは安全上の問題を引き起こす可能性のある箇所、該当する機器を明確化した上で、リスク分析及び評価を進めることが重要となります。よって、本ステップでは、意思決定プロセス、資産（機器）やシステム構成の明確化を含めた「リスクの特定」から必要となるリスク対策を決定するリスク分析・評価までの流れを解説します。

説明した内容が読者の方々の所属する団体やサプライチェーンにおいて、サイバー・セキュリティの被害が発生しうる状況であるか、具体的に確認していただくため、チェック項目例を以下に示します。一つでもチェックが付かない項目がある場合は、サイバー・フィジカル・セキュリティ対策基盤に関連するリスクがあることから、具体的にリスクアセスメントを実施することをお勧めします。

図表 51　SIP ソリューションの必要性に対するチェック項目

No	チェック項目	SIP ソリューション	フェーズ
1	ルーター等のネットワーク機器は、客観的かつ透明な評価ができる機器を利用しているか。特に、施設内のネットワーク機器において、不適切な経路が作られないように設定しているか	①既存機器のインターフェース部に外付け可能な通信暗号化コネクタシステム ＜対応するリスク＞ ● 機器自体の差し替えや不正機器のネットワークへの接続 ● ネットワーク上の通信傍受	予防
2	ネットワーク上の通信の改ざん等による障害発生を防止するため、安全な暗号プロトコル（WPA2-AES、WPA2-TKIP 等）により通信を秘匿化しているか		
3	許可されていない機器、媒体、プログラムを社内ネットワークに接続されないように対策しているか		検知
4	IoT 機器のソフトウェアアップデートを確実に適用する方法を検討し、運用しているか	② IoT 機器向けの改ざん検知ソフトウェア（サービス） ＜対応するリスク＞ 不正ソフトウェアの混入	予防
5	セキュリティ対策の最善策、特に、ソフトウェアサプライチェーン対策のための情報収集を行い、サイバー・セキュリティ対策の必要性を検討しているか		
6	外部より、機器のプログラムを追加・変更（改ざん）されないよう、適切な措置をとっているか。もしくは、上記が発生した際、即時に検知できるようにしているか		
7	脆弱性対策を実施し、既知の脆弱性の有無を確認しているか	③ IoT や OT システムにおけるセキュリティ異常対処支援サービス ＜対応するリスク＞ 脆弱性を発端とする攻撃	分析
8	OS や各種ソフトウェア等に修正プログラムを適用しているか		
9	機器やシステムに異常が発生した際の業務への影響度合いを分析しているか		
10	ソフトウェアの脆弱性対策として常に最新のバージョンにアップデートしているか、実施していない場合は別の対策を実施しているか		予防
11	各種機器やシステムのセキュリティ設定に不備はないか（初期設定の利用開始時の変更や定期的な変更）		
12	第三者による不正アクセスや機器間の不正な通信を識別するために通信の監視をしているか		
13	USB、外部媒体に接続する際に不正アクセスや機器間の不正な通信を検知できるようにしているか		検知

No	チェック項目	SIP ソリューション	フェーズ
14	クローズドなネットワークでも、不正なアクセスや機器間の不正な通信を識別できるようにしているか		検知
15	パッチ等の修正手段が提供されていない脆弱性が明らかになった場合、提供されるまでの間、攻撃による影響を低減するための対策や体制が整備されているか		対応
16	不正な通信が検知された場合、迅速に影響調査をして遮断を検討できる体制が整備されているか		
17	コンピューターウイルス対策ソフトやパーソナルファイアーウォールの導入等により、不正アクセスやマルウェア感染等を回避できるような対策を行っているか	④信頼できる取引ネットワーク構築サービス ＜対応するリスク＞ 不正アクセスによる情報漏えいや改ざん	予防
18	不正なアクセスや挙動の記録が残るログの不当な削除／改ざん／追加等を禁止する措置をしているか		
19	サーバー上のファイルやディレクトリが第三者に不正に改ざんされないようにアクセス制御をしているか		
20	機微情報システムへのアクセスにおける利用者の識別･認証を厳格に行っているか。また、関係組織とネットワークを通じて情報をやり取りする場合、通信元と通信先の正当性を相互に認証しているか		
21	各種ログを記録及び保存し、定期的に点検及び分析しているか		検知
22	監査に利用可能ログを記録及び保存して、定期的に点検及び分析しているか。ログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した情報が特定できるように記録しているか		
23	可搬媒体の授受及び保存状況を確実に記録し、可搬媒体の所在について把握し、情報の持ち出しを禁止できるようにしているか	⑤サプライチェーントラストソリューション ＜対応するリスク＞ 内部による不正行為	予防
24	監査に利用可能なログの時刻情報は、内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で作業事実の記録として問題のない範囲の精度を保っているか		
25	機微情報が参照可能な場所においては、来訪者の記録･識別、入退制限等の入退管理を定めているか		

図表 51 は、「医療情報システムの安全管理に関するガイドライン　第 5.2 版」[26] に別添されている「医療機関のサイバー・セキュリティ対策チェックリスト」を参考に作成しています。1 つでも該当しない項目がある場合は、セキュリティ・リスクに晒されている可能性があるため、対策有無について検討する必要があります。

どのような対応が求められるかをイメージしていただけるよう、参考として、図表 51 のチェック項目について一般的に想定される対応を例示します。（数が多いため、基本的な内容や、特に認識が必要なポイントが含まれる項目を例示します。）

＜一般的に想定される対応（例示）＞

A）　チェック項目 No.7：脆弱性検査を実施し、既知の脆弱性の有無を点検しているか
チェック項目 No.8：OS や各種ソフトウェア等修正プログラムを適用しているか

- 部門で管理しているものも含めて以下の資産を把握し、管理情報（名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報等）の一覧が作成されている。
  - ‥　保有している機器類（サーバー、PC、IoT 機器、OT 機器等）
  - ‥　機器類の OS やソフトウェア、ミドルウェア
  - ‥　リモートメンテナンス等を含めたネットワーク
- 把握した機器、及び OS やソフトウェアについて、脆弱性診断ツールや脆弱性対策情報データベース（JVN iPedia 等）等を使用して脆弱性を確認し、確認日や確認結果を記録している。
- ファイアウォールが適用されている。
- 脆弱性防御ソリューション等を導入し、攻撃をブロックしている。
- 修正プログラムの適用が必要な脆弱性を把握し、修正プログラムの公開予定を確認している。
- 脆弱性が発見された場合、システム構成及び各システム間の情報の流れや、外部との情報の流れを基に、サイバー攻撃を受けた際の業務とシステムへの影響範囲や影響度及び被害額等を算定している。
- 上記の算定結果をもとにサイバー・フィジカル・セキュリティの対策が検討されている。

26 「医療情報システムの安全管理に関するガイドライン　第 5.2 版」（2022 年 3 月）
https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html 「医療情報システムの安全管理に関するガイドライン」は、平成 17 年 3 月 31 日「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」の別添として、個人情報保護に資する情報システムの運用管理、個人情報保護法への適切な対応等について示しました。近年のサイバー攻撃の手法の多様化・巧妙化、情報セキュリティに関するガイドラインの整備、地域医療連携や医療介護連携等の推進、クラウドサービス等の普及等に伴い、医療機関等を対象とするセキュリティ・リスクが顕在化していることへの対応として、情報セキュリティの観点から医療機関等が遵守すべき事項等の規程を設ける等所要の改定を行い、「医療情報システムの安全管理に関するガイドライン 第 5.2 版」を策定している。

B）　チェック項目 No.9：機器やシステムに異常が発生した際の業務への影響度合いを分析しているか

- 最新の脆弱性情報確認と、A）で管理している資産への影響確認を常に行っている。
- 修正プログラムやパッチが公表された場合は、速やかに適用している。

C）　チェック項目 No.10：ソフトウェアの脆弱性対策として常に最新のバージョンにデートしているか、実施していない場合は別の対策を実施しているか

- A）の分析を実施し、何らかの理由により必要なパッチが即時に適用できない場合については緊急度についても把握し、結果を記録している。
  - ※　例えば、JVN iPedia の CVSS 計算ツールを使えば、各組織での対象製品の利用範囲や攻撃を受けた場合の被害の大きさ等を考慮し、利用者自身が脆弱性への対応を判断するための CVSS 環境値を計算することが可能である。CVSS 環境値が 7.0 以上は緊急にパッチ、4.0 以上は月次パッチ、それ以外は定期保守でパッチ等、パッチ対策の緊急度の見極めに活用することができる。詳細については、IPA の「古いソフトウェア製品を利用しているウェブサイトへの注意喚起」[27] を参照。

D）　チェック項目 No.12：第三者による不正アクセスや機器間の不正な通信を識別するために通信の監視をしているか

- 通信のログを採取している。
- 通信のログを基に、不正検知ツール等を使用して、異常な通信がないかを常時または定期的に確認している。
- 通信に異常が発生している可能性がある場合、連絡が必要な先へ通知が行えるよう対策を講じている。

E）　チェック項目 No.13：USB、外部媒体に接続する際に不正アクセスや機器間の不正な通信を検知できるようにしているか

- 外部媒体へ接続時及び接続後、外部からの不正通信、外部への通信、及び自組織内の機器間の不正通信が発生した場合、速やかに検知し、連絡が必要な先へ通知が行えるよう対策を講じている。

F）　チェック項目 No.14：クローズドなネットワークでも、不正なアクセスや機器間の不正な通信を識別できるようにしているか

27　https://www.ipa.go.jp/security/vuln/documents/2009/200903_update.html

- インターネットへの接続を行っていないクローズドな環境であっても、リモートメンテナンスや IoT 機器等を通じたサイバー攻撃の可能性を踏まえ、外部からの不正通信、外部への通信、及び自組織内の機器間の不正通信が発生した場合、速やかに検知し、連絡が必要な先へ通知が行えるよう対策を講じている。

G） チェック項目 No.15:パッチ等の修正手段が提供されていない脆弱性が明らかになった場合、提供されるまでの間、攻撃による影響を低減するための対策や体制が整備されているか

- ファイアウォールを活用する。
- 脆弱性防御ソリューション等を導入し、攻撃をブロックしている。
- 通信やシステムの利用状況を監視出来るようになっている。
- 攻撃発生時の影響可能性、対策実施状況、及び業務の優先度等を勘案し、追加でできる対策を検討している。
  - ‥ 不正検知や防御の対策が出来ていない場合には、対策ができるまで業務を縮小するといった対応も考えられている。
    （BCP（Business Continuity Plan・事業継続計画）が用意されている。）

H） チェック項目 No.16：不正な通信が検知された場合、迅速に影響調査をして遮断を検討できる体制が整備されているか

- 不正通信を検知した場合、不正通信遮断サービス等により、直ちに不正通信の発信元の特定・遮断を行えるよう対策を講じている。
  - ‥ 何等かの事情により自動で遮断することができない場合は、被害拡大防止のため、速やかに判断･対応を行える体制（判断を行う権限者の複数設定、緊急連絡先の複数設定、検討方法等）を整備する。
- 不正通信を遮断した後、影響確認、影響が発生した場合の対応、及び監視強化等を行い得る体制が整っている。

認識したリスクについてはリスク分析・評価としては、一般的に考えられる事業被害のレベルを参考に、事業被害レベルを設定します。対応すべき領域の特定として、洗い出した攻撃シナリオから特定された脅威について、リスク評価基準を設定する必要があります。定義した事業被害レベルとその発生の可能性を加味した内容を踏まえ、領域を特定します。

対応が必要となるリスクが特定されると、必要となる対策要件が決定されます。想定リスクとそれに対する対策要件についての詳細についてはサイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の添付 B [28] を参照下さい。

28 サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の添付 B
https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf

4.2. リスク対応

この節では 4.1 にて洗い出されたリスクに対して、どのように対応していくかについて説明していきます。一般的にリスクへの対応方法として、回避、低減、移転のいずれかの対応を取りますが、ここでは洗い出されたリスクに対して、対策を講じることにより、発生しやすさや被害の深刻度を低減する「リスクの低減」という対策を行います。

＜事前準備のための４つのステップ＞

ステップ１：　対象システムの把握
ステップ２：　設置が必要な機器の設置場所・設置構成の検討
ステップ３：　事前検証
ステップ４：　ソリューション導入に向けた手順検討及び安全性検証

ステップ１：対象システムの把握

まずは「対象システムの把握」を行います。具体的にはシステム構成図、ネットワーク構成図、IP アドレス一覧を基にセキュリティ対策を行う対象システムの把握を行います。その際、部門ごとに独自でシステムを導入し、利用している場合があり、それらのシステムが、基幹システムに連携されている場合もあるため、関係者にヒアリングやアンケートを行い、上記のようなシステム有無の確認や、情報システム担当にて把握していないリモートメンテナンスの回線の有無等を把握し、対象となり得る対象となり得る資産（機器）やサービスを洗い出します。（EXCEL ファイルや画像のメールでの送信・授受についても確認する必要があります。）

＜POINT＞

■ Windows アップデートの実施状況について事前に確認しましょう。

⇒ システムが正常稼動しなくなる可能性等を考慮して、Windows アップデートを実施していない、或いは実施しているが限定的といった場合は、事前にソリューション担当者へご相談ください。

■ 基幹システム以外の部門システムや EUC（End User Computing）と呼ばれるシステム等、把握されていないシステムが存在していないか事前に確認しましょう。

⇒ 把握されていないシステムがネットワークに接続されていて、脆弱性への対応がされていなかった場合、重大な問題に繋がる可能性もあるため、導入前には必ず確認をお願いします。

■ ソリューション導入及び運用に対応する人材を確保しましょう。

⇒ 人材の確保が困難な場合は、常駐 SE による対応や遠隔保守について検討が必要となります。

■ 役割分担、及び意思決定権者と意思決定プロセスの明確化を行いましょう。

⇒ 誰がいつ何をどのように実施すべきかが明確になっていない場合は作業遅延や漏れが発生する可能性があります。また、意思決定に時間を要する場合は、ソリューション導入やインシデント発生時の対処遅延が生じ、重大な問題に繋がる可能性が発生する可能性があります。

ステップ 2：機器の設置場所・設置構成の検討

次に機器（センサー等）の設置場所･設置構成について検討を行います。具体的にはステップ 1 にて把握した対象システムの情報を基に、対象システムごとに、ソリューション導入の際に設置が必要な機器をどこに設置すべきかについて検討します。具体的な流れとしては、まず設置が必要な機器に関する情報（ソリューション毎に用意されるマニュアル等）を参照し、システム構成図・ネットワーク構成図を基に設置場所ならびに設置するスペース等の検討を行います。設置場所が適切か確認する機能が搭載されている機器の場合は、その機能を活用いただくことで効果的に設置することが可能となります。

また、本サービスの設計・構築を OT ベンダーに委託される場合には、OT ベンダーにてシステム構成図やネットワーク構成図を基に最適な設置場所の検討が行われます。なお既存システムへの影響も鑑み、設置場所の検討結果ならびに既存システムへの影響有無については、検討時に自社と OT ベンダー間にて認識合わせを行っておく必要があります。また設置場所の検討にあたっては、1）電源の場所、2）監視センターの場所ならびに異常検知時のオペレーターへの伝達方法についても併せて確認を行う必要があります。

＜ POINT ＞

■　機器の設置場所や電源を確保しましょう。

⇒　場所がない、電源が確保できないといったことにより、想定したスケジュールでソリューションが導入できなくなる可能性があります。

■　監視センターの場所や、異常検知時のオペレーターへの伝達方法について事前に検討を行いましょう。

⇒　基本的に外部接続ができないといった業界や、伝達方法に問題があると思われる場合は事前にソリューション担当者へご相談ください。

ステップ３：事前検証

必要な機器の設置場所や設置構成の検討が完了したら、次に「事前検証」を実施します。

本番環境への影響を考慮し、非本番環境が用意されている場合は、事前に本番システムと同等の非本番環境を準備し、事前検証を行うことが望ましいですが、非本番環境が用意されていない場合には、既存のネットワークに影響が出ないように調査を行い、本番環境にて設置が必要な機器の設置場所や監視ポイントの洗い出しを行います。

エッジ装置の場合、通常ミラーポートと呼ばれる、ネットワーク上に流れる通信（パケット）を採取することができる箇所（ポート）に接続しますが、ミラーポートのスイッチがオフになっている場合は事前にミラーポートの設定変更を行う必要があります。設定変更を行うことにより本番環境の通信が影響がでることもあるため、ミラーポートの設定変更にあたっては夜間や休日等、本番環境が動いていない時間帯に設定変更を行う必要があります。

ステップ４：ソリューション導入に向けた手順検討及び安全性検証

「事前検証」実施後、本番システムに設置が必要な機器を導入する際に、既存システムに影響を与えずに安全に導入するための手順を検討します。非本番環境が用意されている場合には、非本番環境にてその手順を実際に実行することで、手順の安全性を検証することが重要となります。非本番環境が用意されていない場合には、実際の実行は行わず、手順の検討のみを行います。

2）導入

続いてソリューション導入に向けた作業として、以下４つのステップを実施していきます。

＜導入のための３つのステップ＞

ステップ５：　導入機器の準備

ステップ６：　関連部署における影響範囲の把握

ステップ７：　導入作業の実施

ステップ５：導入機器の準備

「事前検証」の項目で触れたように、エッジ装置を接続する場合は、その接続先であるミラーポートの設定がオフだった場合には事前にミラーポートの設定を変更しておく必要があります。

設置が必要な機器を導入する場合には、詳細についてマニュアルやソリューション担当にご確認ください。

ステップ６：関連部署における影響範囲の把握

導入作業の目的や作業内容を、関係する部署に対して周知し、何かあった場合の原因の可能性を共有します。導入作業のシステム担当者は、作業直前には導入作業に必要な機器やマニュアル等が揃っていることの確認や、当日の運用状態のチェックを行うことで、導入作業における障害発生リスクを可能な限り低減します。

ステップ７：導入作業の実施

事前に導入準備ならびに関係部署への周知を行った上で、設置が必要な機器の導入作業に入ります。具体的にはマニュアルと事前の検討結果に基づき、機器の設置ならびに対象システムへ機器を導入できる状態にするため、機器へのソフトウェアのインストールを実施し、構成の設定を行います。

3）運用　導入時対応や運用時に導入先企業にて発生する業務を記載

最後にソリューション運用時の作業として、以下を実施します。

ステップ８：正常起動の確認

導入した機器とソリューション等が正常に起動していること、導入した機器やソリューションが既存のネットワーク・ハードウェア・ソフトウェア等に影響を与えず、正常に稼動していることを確認します。可能であれば、本格稼動の前に異常検知と一次対処実行についてもシミュレーションを行い、有事に備えておくことが望ましいです。

既存の監視システムにて異常の検知ならびに一次対処の勧奨メッセージを受信するケースや、MSS（マネージド・セキュリティ・サービス）と呼ばれる監視代行を行うベンダー（見守りサービスを提供するベンダー）と契約しているケースもありますので、それらのサービスにて本サービスから出力されたログを検知し、深刻な場合に病院の担当者に伝達されるかについても確認します。

第５章
まとめ

従来、インターネットから独立していた業務システムは、IoT 機器等の影響によって、サイバー・フィジカル・システムとなり、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ます。IoT 機器を含む様々な機器は、中小企業を含むサプライチェーンによって製造及び運用されていることから、サプライチェーンの各構成要素についてセキュリティを確保する必要があります。

このような認識の中、2018 年に開始された内閣府の推進している戦略的イノベーション創造プログラム（SIP）第 2 期に「IoT 社会に対応したサイバー・フィジカル・セキュリティ」が課題として設定され、第 3 章や付録で説明しているサイバー・フィジカル・セキュリティ対策基盤を研究開発しました。

本ガイドブックは、サイバー・フィジカル・システムへのサイバー攻撃の脅威を経営層や現場の方々に改めて認識していただき、対応が迫られている状況であることを理解いただき、実際に対策を具体的に検討いただくために纏めました。

サイバー・フィジカル・セキュリティ対策基盤の各ソリューションにご興味がある場合は、第 3 章の対応している節の最後及び付録の冒頭（次頁）に連絡先を記載しておりますので、ご連絡ください。

さまざまな企業や業界もしくはサプライチェーン等の単位でリスクアセスメントやリスク対応の検討が進むことで、我が国のセキュリティ対策レベルが向上していくことを期待しています。そうした活動のなかで、本ガイドブックをご活用いただければ幸いです。

付録
ソリューションの技術説明

本付録では本文中に紹介しました各ソリューションの詳細について説明します（図表 52）。

図表 52　問い合わせ先一覧

ソリューション（技術）名	該当ページ	連絡先
ソリューション①：既存機器のインターフェース部に外付け可能な通信暗号化コネクタシステム	pp.87-90	株式会社 SCU c01.contact@scu.co.jp
ソリューション②：IoT 機器向けの改ざん検知ソフトウェア（技術）	pp.91-93	日本電信電話株式会社 社会情報研究所 solab@ml.ntt.com
ソリューション③：IoT や OT システムにおけるセキュリティ異常対処支援技術	pp.94-98	
ソリューション④：信頼できる取引ネットワーク構築サービス	pp.99-102	富士通株式会社 キャリア＆メディア事業本部 NTT ソリューション事業部 contact-sip2-b2@cs.jp.fujitsu.com
ソリューション⑤：サプライチェーン・トラスト・ソリューション	pp.103-105	株式会社日立製作所 サービスプラットフォーム事業本部 マネージドサービス事業部 SIP2_B3_info1@ml.itg.hitachi.co.jp

ソリューション①：既存機器のインターフェース部に外付け可能な通信暗号化コネクタシステム

放置されているリスク

近年オフィスのみならず、工場、医療現場、農作業現場等様々な場所でIoT機器が活用されるようになりましたが、一方でIoT機器の消費電力、CPU能力やメモリ等の都合上、十分なセキュリティ対策を行う事が難しく、結果的にネットワーク通信によるデータの盗み見やデータの改ざんリスクに晒されています。

解決策の方向性

ネットワーク通信傍受によるデータの盗み見や改ざんのリスクを解決するためには、「IoT機器、末端ノード」及び「ネットワーク上でやりとりされている情報（通信）」を守るためのセキュリティ対策が必要となります。具体的には「IoT機器そのものをすり替えられた場合に、そのすり替えをすぐに検知できる技術」、「IoT機器やIoT機器とパソコンを繋ぐネットワークに不正なソフト・マルウェアが混入されてしまったら、その異常を検知して通信を停止し、感染拡大を防ぐ技術」、「ネットワークでやりとりされるデータを暗号化する技術」等、これらの技術が具備されたIoT機器、ネットワークを利用することが必要不可欠となります。

解決策の具体例

上記SCUの組込及びコネクタシステムの2つの展開について、順に説明します。

＜SCU＞

研究開発成果であるSCU（Secure Cryptographic Unit（セキュア暗号ユニット））と呼ばれる微少な消費電力で利用することができるセキュリティチップを活用することで、IoT機器ならびにIoT機器とパソコンを繋ぐネットワークのセキュリティ対策を行うことが可能となります。具体的には、SCUをIoT機器ならびに接続先のPC端末やネットワーク機器に組み込むことにより、IoT機器とPC端末の間のネットワークを専用回線化し、ネットワーク間で通信されるデータを暗号化することができます。

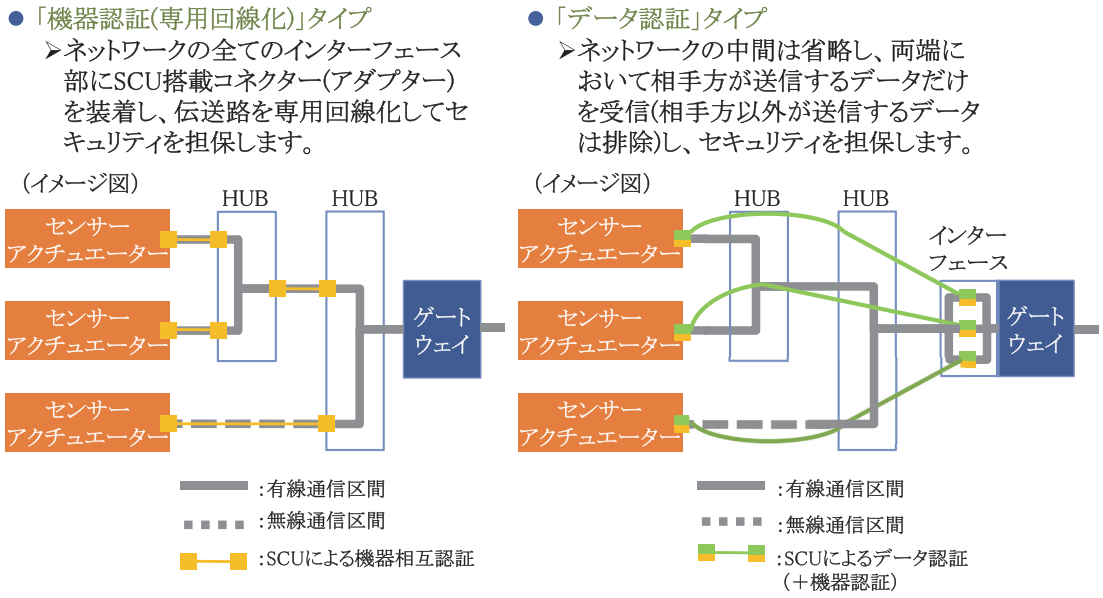
＜コネクタシステム＞

まず、機器への内蔵が難しい場合には、このSCUを各種機器に後付け可能なコネクタシステムも用意されており、有線の場合はLANの差込口への機器追加や、無線の場合はUSB等への所定機器を取付けによって対応することができます。

内蔵が難しい場合でも、SCU搭載のコネクタをネットワークの全てのインターフェース部

分（この事例の場合はIoT機器とネットワークの接触面及びパソコンとネットワークの接触面）に装着し、ネットワークを専用回線化することによっても対策を行うことが可能となります。具体的には以下に図表53に掲載しているとおり、SCU搭載のコネクタをネットワークの全てのインターフェース部分（たとえばIoT機器とネットワークの接触面及びパソコンとネットワークの接触面）に装着し、ネットワークを専用回線化することによってセキュリティ対策を行うことが可能となります。つまり、SCU搭載のコネクタを装着し、IoT機器とPCの認証手続きを行うことで、SCU組込機器と同等の効果を得ることができます。

図表53　SCU搭載コネクタシステムのイメージ図



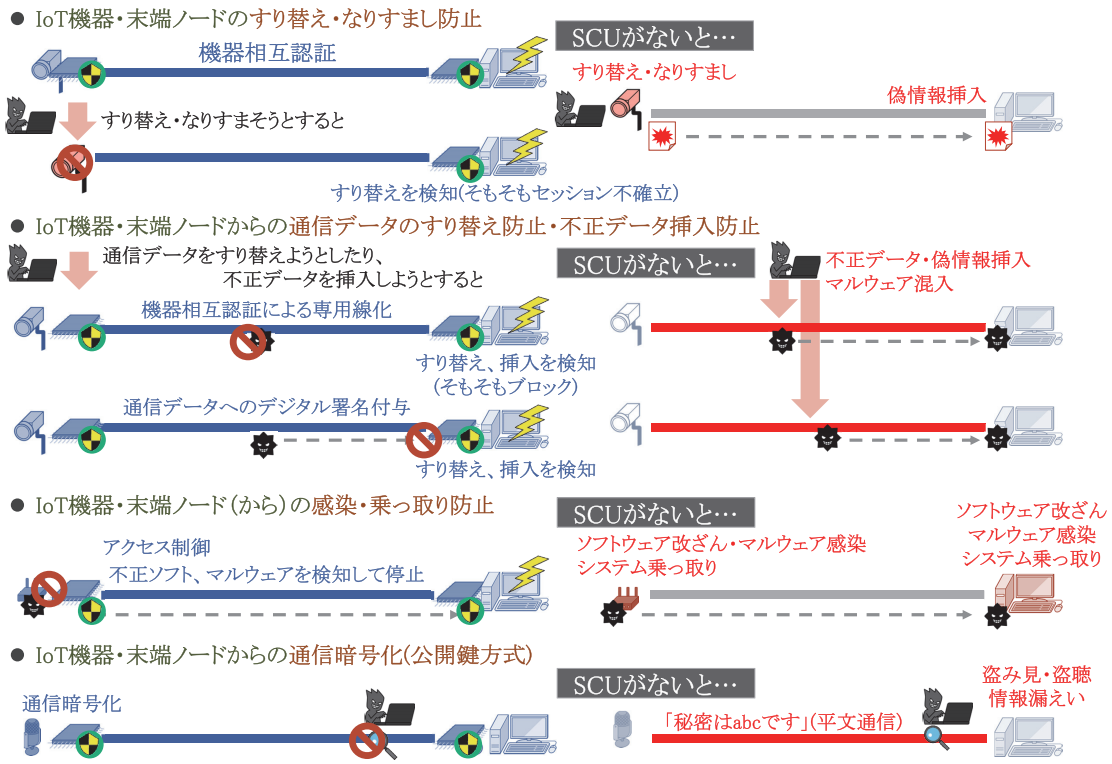
提供価値 / 導入効果

＜ SCU ＞

SCUの機器への組み込みもしくはSCUを組み込んだ機器の導入により、「IoT機器とゲートウェイ間の通信の安全性確保」が期待できます。

具体的には図表54に掲載していますが、IoT機器と通信先のPC端末等にSCUを組込むことにより、IoT機器と通信先のPC端末間で通信されるデータをSCUの機能を用いて暗号化することができるため、仮に外部から不正な通信があった場合も情報を盗み見されてしまったり、データそのものを改ざんされてしまったりするリスクを軽減することができます。また、SCUによる通信を開始時には、IoT機器と接続先のPC端末とで機器の登録を行い、以後通信時には毎回機器認証を行うため、想定リスクA）で懸念されている機器の差し替えや不正機器の接続が仮に発生した場合でも、通信時の機器認証により、異常が検知された場合に通信を停止することが可能となります。

図表 54　SCU の効能



＜コネクタシステム＞

IoT 機器等ネットワークに接続されている末端ノードのなりすましや IoT 機器とゲートウェイ間の通信の盗み見の対応策として利用できるのが、SCU 搭載のコネクタシステムです。コネクタシステムを活用することにより、1）IoT 機器とゲートウェイ間の通信の安全性確保ならびに 2）レガシーシステムのセキュリティレベルの向上が期待できます。

まず、1 点目の「IoT 機器とゲートウェイ間の通信の安全性確保」ですが、前述の SCU 組込機器を活用した場合と同様に、IoT 機器と通信先の PC 端末との間のネットワークにコネクタシステムを装着することにより、IoT 機器と通信先の PC 端末間で通信されるデータを SCU の機能を用いて暗号化することができます。もし、仮に外部から不正な通信があった場合も、情報を盗み見されてしまったりデータそのものを改ざんされてしまったりするリスクを軽減することができます。SCU による通信を開始時には、IoT 機器と接続先の PC 端末とで機器の登録を行い、以後通信時には毎回機器認証を行うため、想定リスク A）で懸念されている機器の差し替えや不正機器の接続が仮に発生した場合でも、通信時の機器認証により、異常を検知し、通信を停止することが可能となります。

また、2点目の「レガシーシステムのセキュリティレベルの向上」では、既存のIoTのIoT機器ならびにPC端末を入れ替えることなくセキュリティ対策を行うことができるため、業務継続の観点からシステムを止めることが難しいインフラ業界、医療業界等の重要なインフラ業界にも活用することができます。そして、大規模なシステム刷新が不要であるため、中小企業でも活用が可能となります。

競合優位性

＜SCU＞

SCUの優れている点は、微少な消費電力でIoT機器及びネットワークのセキュリティ対策を行えることです。また世界最小の楕円曲線暗号エンジンを利用していることから、非常に小さなIoT機器へも組み込むことが可能です。

＜コネクタシステム＞

コネクタシステムの優れている点は、SCUの特長として挙げた点の他に、既存の機器の入れ替えが不要である点が挙げられます。前述の事例はSCUそのものをIoT機器ならびに通信先のPC端末への組込みが必要ですが、コネクタシステムの場合には既存のIoT機器ならびにPC端末を入れ替えることなく、ネットワークのインターフェース部分にSCU搭載のコネクタを搭載するだけで機器の認証ならびに通信の暗号化を行うことができるのが特長です。この技術により、既存の機器のセキュリティ性能をTPM並みに高め、使い続けることができます。

既存機器のインターフェース部に外付け可能な通信暗号化コネクタシステムに関する問い合わせ先

株式会社SCU
Email：c01.contact@scu.co.jp

ソリューション②：IoT 機器向けの改ざん検知ソフトウェア（サービス）

放置されているリスク

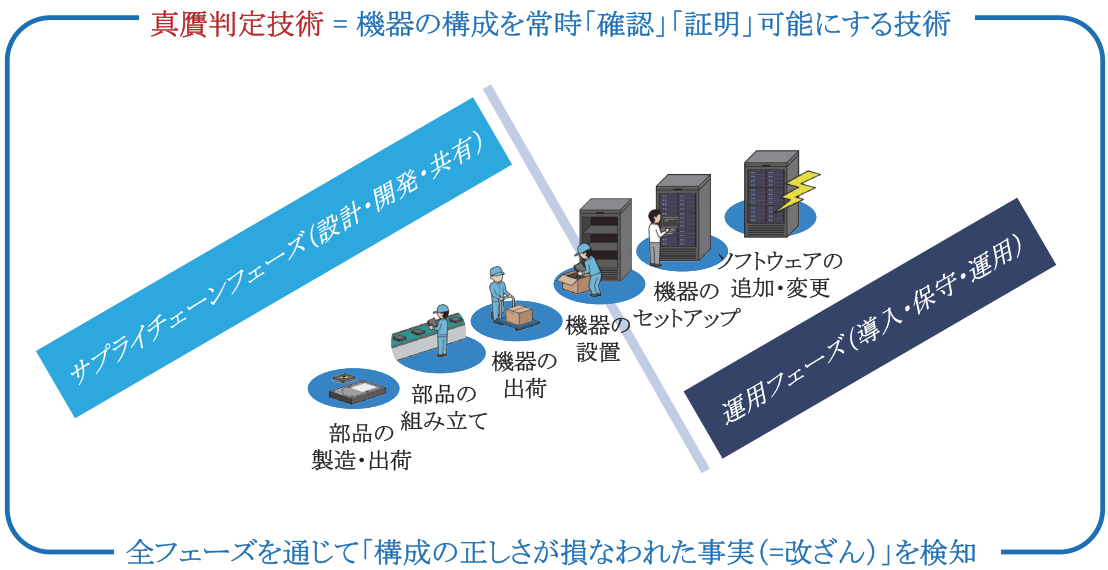
近年サプライチェーン攻撃と呼ばれる、1）サイバー・フィジカル・セキュリティ対策が十分でない組織に侵入し、その組織を介してターゲット組織を攻撃する、2）サプライチェーン上で製品やサービスを汚染して、これをターゲット組織に利用させて攻撃する、といったサプライチェーン攻撃手法が増加しています。

また、一般的に IoT 機器はサイズ、CPU やメモリ等のリソースの制限等により、十分なセキュリティ対策を講じるのが難しいといった課題があります。

解決の方向性

サプライチェーン攻撃への対応としては、部品の出荷や組み立て及び機器の出荷・設置・セットアップに至るまでの製品の製造工程から、製品の運用工程に亘って、「製品の構成の正しさ」を常時確認する必要があります。改ざんされた場合は、検知した内容をもとに、対処する必要があります（図表 55）。

図表 55　真贋判定技術

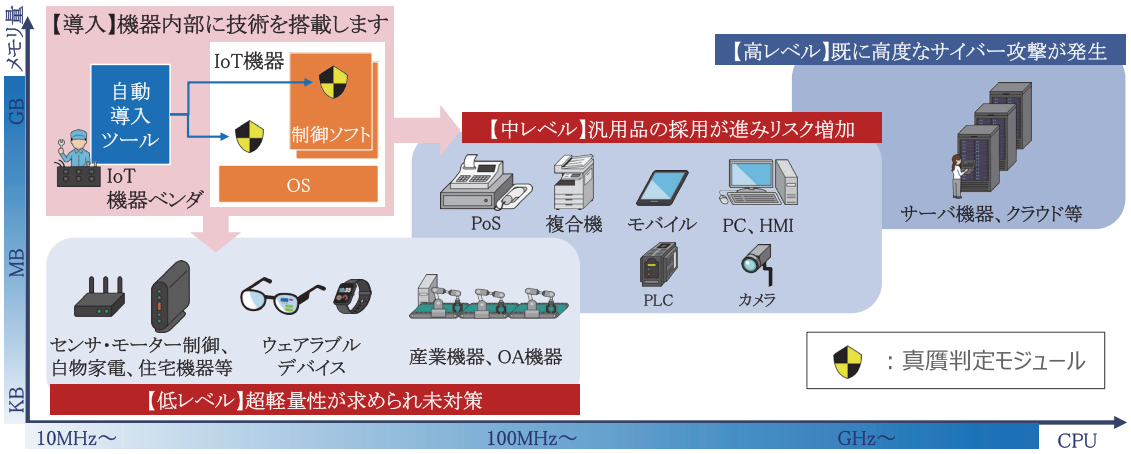


具体的な解決策の例

「製品の構成の正しさ」を常時確認するとともに、その内容を証明可能とするには、保護対象となるIoT機器の製造時にIoT機器向けの改ざん検知ソフトウェアである「真贋判定モジュール」を搭載する必要があります。この「真贋判定モジュール」は、サプライチェーン（設計・開発・供給）フェーズと運用フェーズの全体を通じて機器内のソフトウェア構成を常時監視し、ソフトウェア構成が損なわれた場合にその旨を通知します。例えば、開発工程においてIoT機器に不正な構成要素（マルウェア等）が混入する脅威、及び運用中に、遠隔制御や保守作業等を介して汚染される脅威へ対処が可能となります。

なお、「真贋判定モジュール」はCPUやメモリ等のリソース制限等によって、従来対策が困難であった「中～低レベルの機器（センサー、カメラ、OA機器等の多様なIoT機器）」に搭載できるように開発されているため、様々な機器に搭載することで出来ます（図表56）。

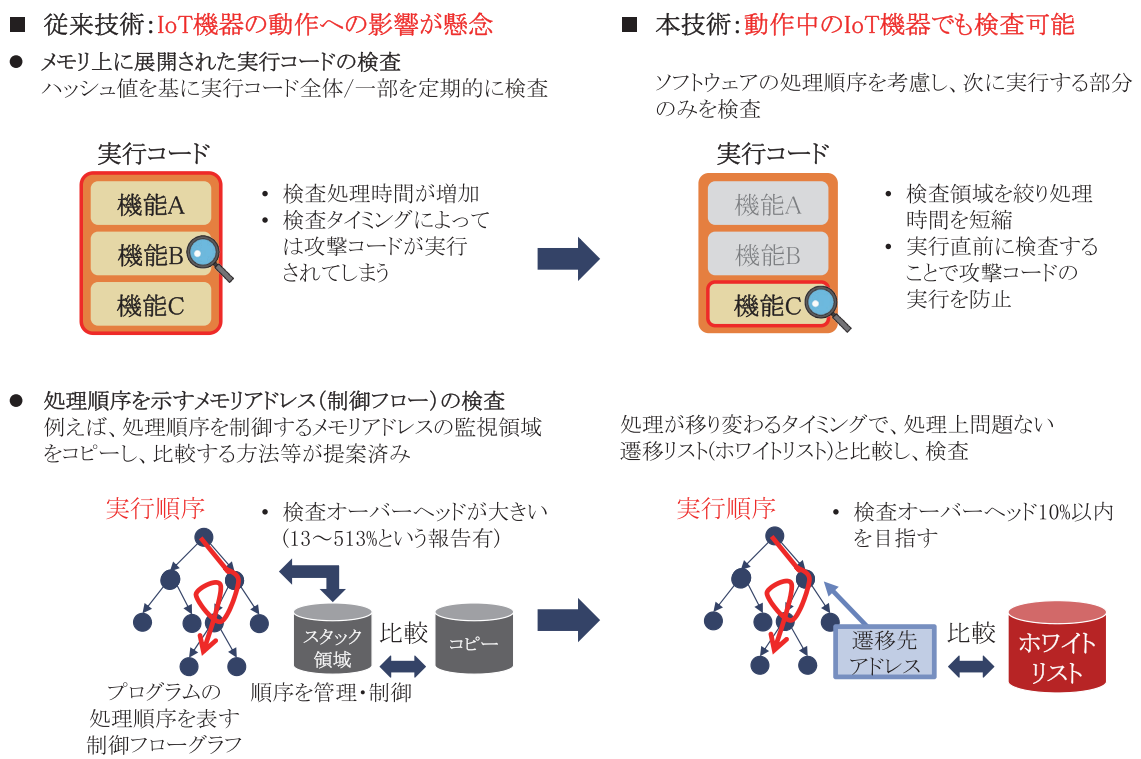
図表56　真贋判定モジュールを搭載可能なIoT機器



顧客候補への提供価値 / 導入効果

IoT機器に搭載する「真贋判定モジュール」が、IoT機器の製造、調達、及び運用等からなるサプライチェーンの全フェーズにおいてソフトウェアの改ざんを確認します。この確認結果を各フェーズにおいて記録蓄積しておくによって、その記録情報（改ざんが検知されなかったことの記録情報）は、結果的にIoT機器のセキュリティ（構成）を証明する効果をもたらします。また、この記録情報は、IoT機器において改ざんが万が一検知された際に、その原因（どこで改ざんが発生したか）を突き止めることにも役立ちます。さらに、IoT機器にインストールされたソフトウェアが稼働している状態であっても改ざんを確認できることから、より漏れのない確認（証明）も可能になります（図表57）。

図表 57　稼働中機器におけるリアルタイム判定



競合優位性

従来ソフトウェア監視技術は、ソフトウェアの動作を考慮した設計がなされていなかったため、機器の動作に影響が生じる可能性があり、稼働中の機器の常時監視は困難でした。本ソリューションでは、処理の実行順序を基に効率的に検査を実施することにより、機器動作への影響を最小限に留めることが可能となったため、稼働中の機器の常時監視が可能となっています。また、前述のとおり、リソース制限のある小規模な機器についても搭載出来るように開発されていることから、様々な機器に対応可能です。

また、IoT 機器向けの改ざん検知ソフトウェアによる機器構成の確認は、更新のためのソフトウェアとは別ルートにて入手した判定基準に基づいて真贋判定を行なうため、更新のためのソフトウェアが改ざんされていた場合でも、サプライチェーン上で確実に異常検知することが可能となります。

IoT 機器向けの改ざん検知ソフトウェア（技術）に関する問い合わせ先

日本電信電話株式会社　社会情報研究所
Email : solab@ml.ntt.com

ソリューション③：IoT や OT システムにおける セキュリティ異常対処支援サービス

放置されているリスク

IoT 機器では、OSS 等や他社ソリューション等の共通部品を利用した開発が主流になってきており、利用されている共通部品に脆弱性が存在しているリスクが増大しています。また、モノ（製品）の利用・運用フェーズにおいて、脆弱性対応の漏れや対応遅延等のリスクもあります。

解決策の方向性

上記リスクを軽減させるためには、想定外のセキュリティの異常に気付くことができ、その異常に対して、対処ができることが必要となります。

具体的には、ソフトウェアの脆弱性の早期発見や、脆弱性を発端とする攻撃の早期発見から一次対処までのリードタイムの短縮が必要となります。また、一次対処までの時間を短縮するためには、影響範囲の特定やその影響に対する施策の絞り込みを効率的に実施できるかが重要なポイントとなります。

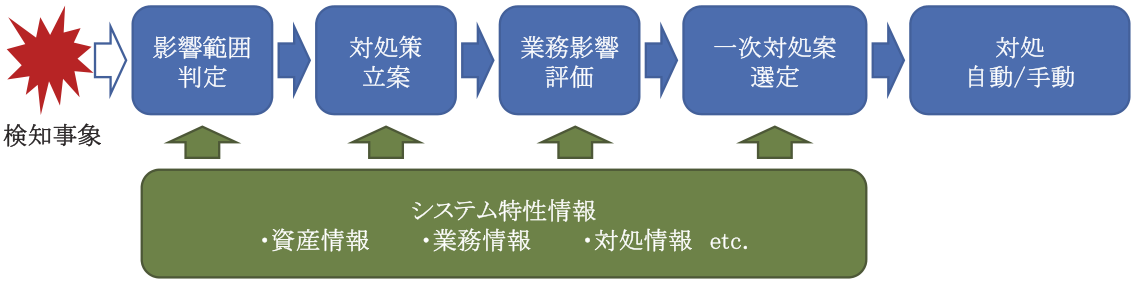
解決策の具体例

想定外の異常に気づき、対処するためには、事前のリスク分析と運用時の監視が必要となります。ここでは具体的にソリューションを用いてセキュリティ対策を実施する方法として、「1）リスク分析による事前の対処及び異常検知」、「2）業務影響を考慮した対策」、及び上記 1)、2）を実現するためのソリューションの技術的なしくみの 3 つのパートに分けて説明していきます。

「1）リスク分析による事前の対処及び異常検知」では、事前のリスク分析として、設備情報を本ソリューションへ登録することで攻撃シミュレーションを実施します。想定される攻撃手法が洗い出され事前に認識できることから、必要となるセキュリティ対策を検討することが可能となります。また、万が一、事前に施したセキュリティ対策をすり抜けてしまった場合においても、本ソリューションの異常検知機能によって、運用時に発生するサイバー攻撃を高精度に検知することが可能となります。さらに検知した異常に対して、既知の攻撃に対しては一次対処を自動で行い、システムによって推定された異常の原因について監視オペレーターへ伝えられるため、監視オペレーターはその異常に気付くことができ、適切な対応を行えるようなります。これらのリスク分析機能、異常検知機能及び自動一次対処機能により、脆弱性への対応の効率化が可能です。

次は「2）業務影響を考慮した対策」についてです。従来の一次対処機能では、ルールに則り一次対処を行っていく技術が多く、業務への影響が考慮されずに実行されてしまうため、中途半端な対応になっていました。実際の対処を実行するにあたっては「どのような業務影響かあるのか」といった一次対処を行うにあたっての業務影響の考慮ができないためです。そこで本ソリューションでは、業務の情報やシステムの可用性等の「システム特性情報」を自動一次対処機能のインプットとして用いることで、業務影響を考慮した一次対処を自動化することを可能としました（図表 58）。

図表 58　一次対処の自動化のしくみ



最後に上記の対策を実現する「ソリューションのしくみ」について「異常検知」と「自動監視」の 2 つの機能に分けて説明します。まず異常検知のしくみですが、システム構成としては監視対象設備に設置される「エッジ装置」と、監視側の設備として設置される「分析サーバー」によって構成されます。

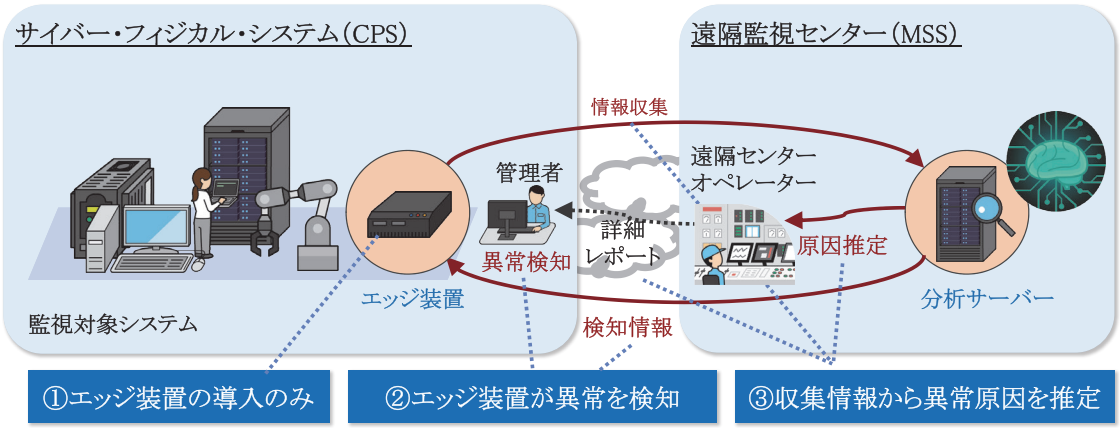
監視対象設備にエッジ装置が導入されると IoT 機器をはじめとしたサイバー・フィジカル・システム[29]の自動検出を行った後に自動監視が開始されます。そして、自動監視は、図表 59 に記載のようにエッジ装置によって収集された情報を用いて分析サーバーが生成した学習モデルを用いて異常を検知します。その後、異常検知した際には、エッジ装置が収集した情報を基に分析サーバーによって原因を自動推定し、監視オペレーター（管理者）向けに情報提供が行われます。この情報によって、監視オペレーターは異常の原因について知ることができ、サイバー攻撃に対して自動もしくは手動にて速やかに対処することが可能となります。このような流れで異常検知及び自動監視が行われます。

なお、本ソリューションの特長として、エッジ装置と分析サーバーの導入のみで、異常検知が可能となり、既存のシステム構成の変更は不要である点が挙げられます。また、2 つ目として異常検知はエッジ装置と分析サーバーによって実施されているため、閉域網でも対応可能です。

29　実世界（フィジカル空間）にある多様なデータをセンサーネットワーク等で収集し、サイバー空間で大規模データ処理技術等を駆使して分析／知識化を行い、そこで創出した情報／価値によって、産業の活性化や社会問題の解決を図っていく取組みのこと

上記ソリューションの内容を攻撃者の目線でまとめてみますと、仮に攻撃者が外部からの不正アクセスを試みた場合、まずはエッジ装置ならびに分析サーバーにより、不正な通信が検知され、監視システムのオペレーターに不正な通信があった事が伝えられます。次に上記の不正通信に対して、業務影響等を考慮された上で、一次対処策が選定され、不正通信に対処するための対処策（不正な通信の遮断等）が本ソリューションにより自動もしくはオペレーターにより手動にて実行されます。これらの一連の対応により、仮に攻撃者が不正通信を試みようとしても、すぐに通信を検知され、通信遮断等の対処が行われるため、システムへの侵入が困難となります。

図表 59　導入するエッジ装置や分析サーバー



提供価値 / 導入効果

本ソリューションにて「リスク分析」を実施することで、現在のリスクの把握、対策すべきポイントの見極め、効果的な対策の検討が可能となります。また「異常検知」を実施することで AI を用いた平常時の通信の特徴分析による異常検知ならびにシステム担当者への連絡、業務影響や事業継続性を考慮した自動一次対処を実現できます。

まず「現在のリスクの把握」では、実際のシステム構成を仮想環境上に登録することで、攻撃シミュレーションを行うことでき、セキュリティ担当者は現在のリスクをレポート形式で把握することが可能となります。システム構成の登録のみで、様々な攻撃手口を踏まえたシミュレーションが可能となることから、専門知識を有していなくても網羅的にリスクを洗い出すことができます。

次の「対策すべきポイントの見極め」では、攻撃シミュレーションによって得られるレポートに、各攻撃における各システムのリスクを認識できるため、現在のシステム環境におけるリスク対応すべき内容を絞り込めます。

最後に「効果的な対策の検討」では、本ソリューションを用いることにより、現在の各システムの危険度を認識することができるだけでなく、仮想空間上で対策実施後のリスクを攻撃ごとにシミュレーションすることが可能となりますので、対策実施後の効果を確認することができ、より効果的な対策を打つことが可能となります。

続いて本ソリューションにて「異常検知・自動一次対処」を行うことで得られる効果について説明します。

まず1つ目の「AIを用いた平常時の通信の特徴分析による異常検知」は、IoT機器等の通信が一時的に急激に増加するバースト性という特徴も加味し誤検知を防ぎ、多様な通信に対してAIによる平常時の通信の特徴分析を行うことにより、不正通信の見逃しリスクも軽減することが可能になります。ただし、製造時に混入された不正ソフトウェアがあらかじめ設定された攻撃のタイミングまでまったく動作しない場合は、事前の検知が難しいため、ソリューション②：IoT機器向けの改ざん検知ソフトウェア（サービス）での対応が必要となります。

2つ目の「業務影響や事業継続性を考慮した自動一次対処」では、前述のとおり、本業務の情報やシステムの可用性等の「システム特性情報」を一次対処の検討に用いる業務への影響評価により、業務影響の少ない対処を選定することが可能となる点が挙げられます。

3つ目の「運用オペレーターへの通知」は、異常の発生や発生原因の運用担当者への通知です。収集情報から推定した異常原因が通知されることによって、事後に発生する詳細レポートの作成稼動を大幅に削減することが可能になります。

このような特長を持つ異常検知・自動一次対処技術を用いることにより、より正確に不正通信を検知し、異常に対処することが可能となります。

競合優位性

続いて本ソリューションの競合優位性について説明します。本ソリューションは従来の監視技術・リスク分析技術に比べ、1）プロトコルの多様性に自動適応できる点、2）大規模なシステムでの対応が可能である点、3）実際にあった攻撃事例に近い手口の分析が可能である点、4）システム特性を考慮した自動一次対処が可能である点の4つの特長があります。

まず1点目の「プロトコルの多様性に自動適応できる点」は、FA（ファクトリーオートメーション）分野及びBA（ビルディングオートメーション）分野で用いられる主要な通信プロトコルへの適用が可能であり、現在BA/FA分野においては世界の80%以上の通信プロトコルへの適用可能となっています。また、独自で用いられている通信プロトコルへの適用も可能となっており、より多くの企業で実装を行う事が可能となっております。

また2点目の「大規模なシステムでの対応が可能である点」は、従来の監視技術ではIoT機器の通信を監視する台数として千台程度が限度だったのに対し、本ソリューションでは1万台規模の環境でも通信の監視が可能となっており、より多くの環境で利用することが可能となっております。

さらに3点目の「実際にあった攻撃事例に近い手口の分析が可能である点」については、従来の攻撃シミュレーション技術では脆弱性を起因としたネットワークを用いたサーバー等への攻撃を攻撃手法として分析していたのに対し、本ソリューションでは、上記攻撃に加え、フィッシングメール詐欺等の標的型攻撃やUSB等による外部持込による攻撃も攻撃手法として分析を行うことが可能となり、より現実に近い形での攻撃シミュレーションが可能となっています。

最後の4点目の「システム特性を考慮した自動一次対処が可能である点」では、前述のとおり、従来のルールベースのみの自動一次対処ではなく、業務影響やシステムへの影響も考慮した形で自動一次対処を実施することにより、より安全に一次対処を実施する事が可能となるという特長があります。

IoTやOTシステムにおけるセキュリティ異常対処支援技術に関する
問い合わせ先

日本電信電話株式会社 社会情報研究所
Email : solab@ml.ntt.com

ソリューション④：信頼できる取引ネットワーク構築サービス

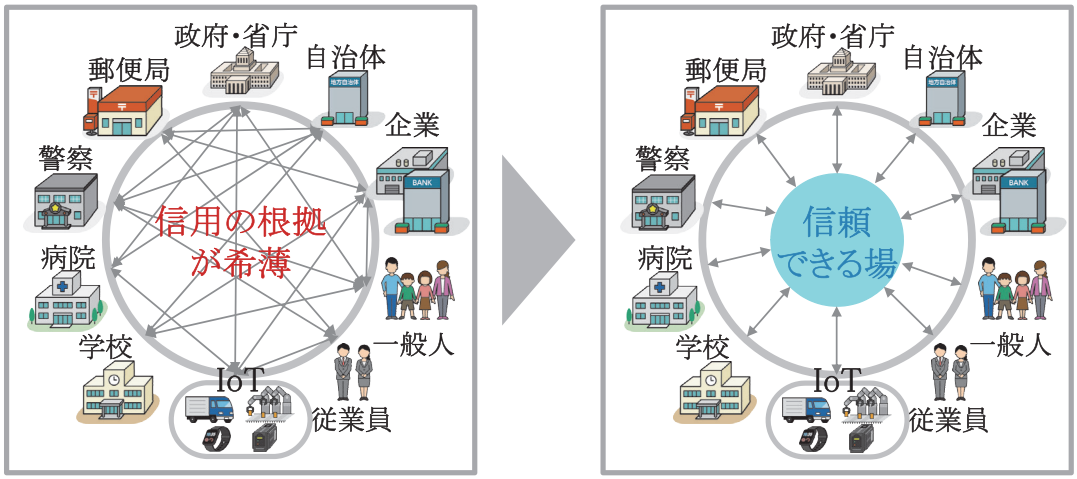
放置されているリスク

サイバー空間上で安全に取引を行うには、取引先の信頼性や安全性を検証することが重要となります。しかし、新規の取引先については信用の根拠が希薄であるため、取引先の信頼性を担保することが難しい場合が往々にして存在しています。一例として、「送られてきたメールやデータは正しいのか」、「相手は信頼できる人か」といったように曖昧な信用をもとに取引を行うケースが挙げられ、取引先の信用に対する明確な裏付けがないことが課題となっています。

解決の方向性

安心して見知らぬ取引先と取引するためには、相手先の信用性や安全性を検証できる機能を構築することで、接続先や流通する情報の真正性を確保できる接続検証が必要となります。その際に、接続検証を行う組織を特定組織に集中させることによって、フィジカル空間とサイバー空間の検証の連続性を確保する方法もありますが、権限が集中した組織による意思決定の公平性確保が困難かつ管理コストが高くなるという課題があります。そこで、フィジカル空間とサイバー空間の検証の連続性を確保しつつ、公平性を確保する接続検証技術が必要となります（図表 60）。

図表 60　信頼できる場のイメージ



【現在】
- 送られてきたメールやデータは正しいのか？
- 相手は信頼できる人か

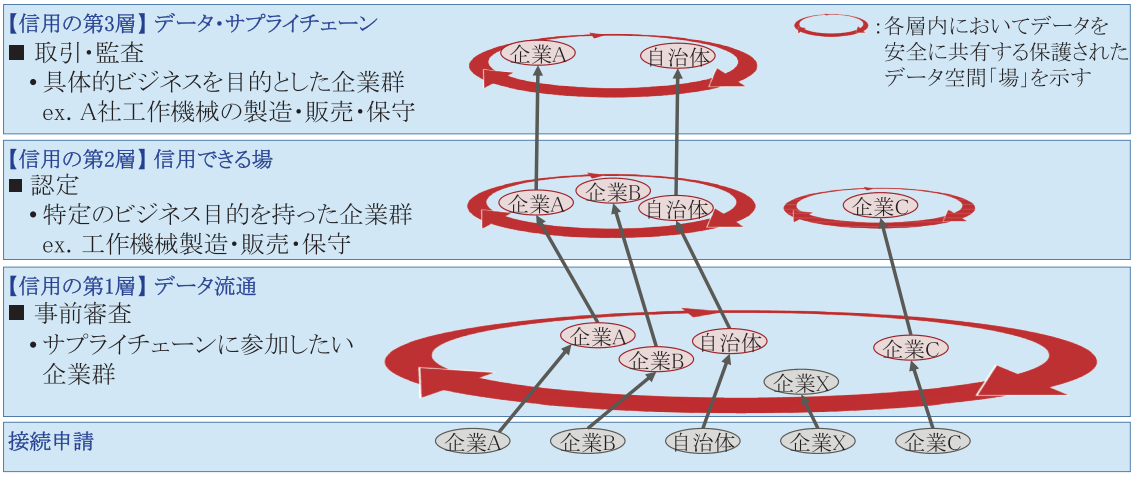
【今後】
- 安全、かつシンプルな繋がり（人/組織/クラウド間等）を実現

具体的な解決策の例

「信頼できる取引ネットワーク構築サービス」では、誰でも接続可能なオープンなネットワーク環境において、接続先の検証を行い、問題ないと判断のついた組織間で安全なデータ流通が保証される仕組みを実現しています。よって、見知らぬ取引先と安心して取引できるようになります。具体的には、「事前審査」、「認定」、「取引・監査」の３つの層で流通させる情報を分けることで、段階的に組織を選別し、安全なデータ流通を実現しています。これを信用の３層モデルと呼んでいます（図表 61）。

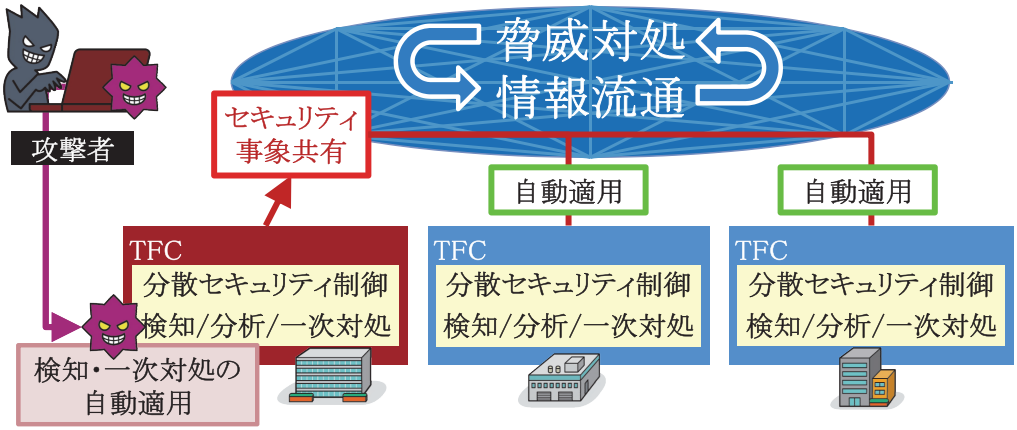
第１層（事前審査）ではサプライチェーン企業群の企業情報や与信情報等の組織の機能や状態を示す情報を流通させることで、接続検証を行います。第２層では、第１層の企業群のうち特定の目的を持った企業群の提供プランや提供範囲等の組織のサービス能力を示す情報を流通させ、接続検証を行います。最後の第３層（取引）では、取引・監査として第２層の企業群のうち具体的な取引を目的とした企業群の利用申請情報や利用資格保有情報等の組織実行能力を示す情報を流通させ、接続検証を行います。各層で流通させる情報は、各層に設ける保護されたデータ空間「場」に保持され、改ざんや漏洩、不正アクセスから守られます。

図表 61　信用の３層モデル（再掲）



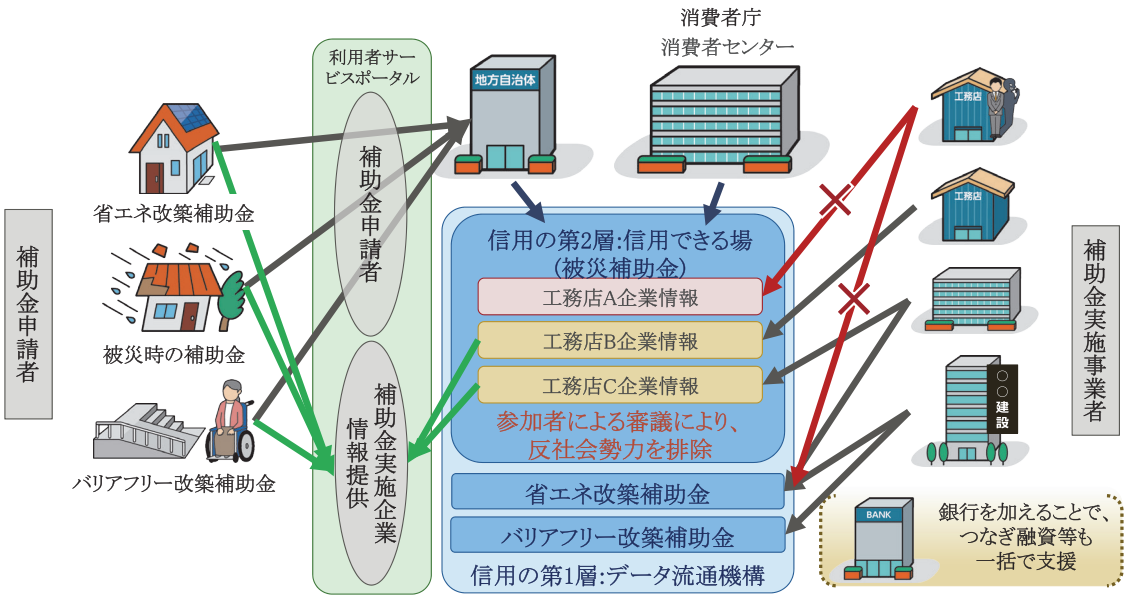
信用の３層モデルをオープンなネットワークで安心して実行するには、「信頼できる取引ネットワーク構築サービス」のために開発した接続用ソフトウェア（TFC）を導入し、ネットワーク全体をセキュリティの脅威から守ることが必要です。TFC によって、接続先が持つフィジカル空間にある組織固有情報をサイバー空間で検証することにより、フィジカル空間とサイバー空間で検証された組織の一意性を保証します。セキュリティの脅威への対処や危険度も TFC 間で共有することで、脅威対策がネットワーク上に拡散され、各接続先に自動適用されることで、ネットワーク全体の安全性を維持できるようになります（図表 62）。

図表 62　TFC による信頼できる取引ネットワーク構築サービスへの接続（再掲）



例えば、自治体が事業会社からの申請を審査する際に、不適正事業者や反社会勢力を排除する必要があります。「信頼できる取引ネットワーク構築サービス」を用いると、偽った資格で申請を行うことができず、接続先を一意で把握できるため、資格要件に満たない事業者を排除することができます。また、何らかの問題を起こした事業者は、そのネットワーク間でその情報が共有されるため、ネットワーク参加者の適正化が図られることになります（図表 63）。

図表 63　地方自治体への導入イメージ



提供価値 / 導入効果

企業や団体は、「信頼できる取引ネットワーク構築サービス」のために開発した接続用ソフトウェア（TFC）の導入によりデータ流通を支えるネットワーク全体の安全性を維持することができます。複数の信頼の場に接続する場合についても 1 つの TFC によって、複数のサプライチェーンに属している中小企業においても複数の信頼の場に簡単に接続することができます。

不正な組織との接続防止やセキュリティ脅威情報を自動展開することによりネットワーク全体の被害拡大防止を期待できるため、「信頼の場」で流通されるデータについて信頼性が向上され、情報流通を安心して行えるため必要となる情報を共有することができます。

競合優位性

「信頼できる取引ネットワーク構築サービス」は特定の検証を特定の組織に集中させず、関係者に対等に分散させることで、合意形成の公平性が担保されている点とセキュリティ対策を個々の企業任せではなく、接続用ソフトウェア（TFC）によりセキュリティ対策がネットワーク上で拡散され各接続先に自動適用される点にあります。

また、動的な検証により接続が管理されているため、資格がないと判断された場合は、即時に権限のはく奪が行われ、適切な範囲での情報が守られることになります。そのため、複雑な権限管理（段階的等）や権限付与が状況によって変わってしまう不特定多数から接続されるシステムに対して、安全な接続やデータ共有を提供することができます。

信頼できる取引ネットワーク構築サービスに関する問い合わせ先

富士通株式会社
キャリア＆メディア事業本部 NTT ソリューション事業部
Email : contact-sip2-b2@cs.jp.fujitsu.com

ソリューション⑤：サプライチェーン・トラスト・ソリューション

放置されているリスク

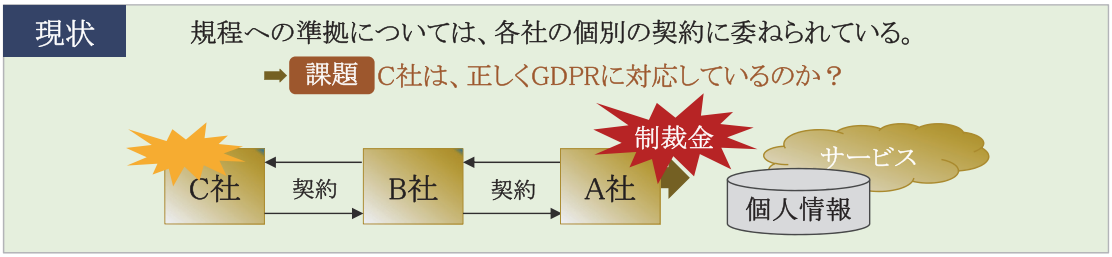
近年、さまざまな不正や虚偽報告等の事例（独自判断、規程外作業、改ざん、人の資格不正）が頻発しています。SDGs や ESG の観点からもサプライチェーン全体での取り組みについて対策が求められています。

しかし、現状では、大部分の企業は個社における規程遵守の取り組みに終始しています。各企業で規程類等のルール解釈にバラつきがあることから、サプライチェーン全体で証跡を適切に保管して共有することが難しい状況になっています（図表 64）。

解決の方向性

権限を逸脱した行為や規程違反を防ぎ、製品やサービスを提供するためには、サプライチェーン全体で適切な規程に従い生成、運用された製品であることを、容易かつ効率的に確認できる仕組みが必要となります。具体的には、「適切な人や機器が適切な規程に従って製品を製造していることを証明するしくみ」が必要となります。

図表 64　サプライチェーン上での課題



サプライチェーン全体で取り組みを推進するためには、規程内容をサプライチェーン内で共有して、その規程に従って実施したことを示すデータを証跡として保管、そして、その証跡をサプライチェーン内で相互確認できる、この 3 点が必要となります。

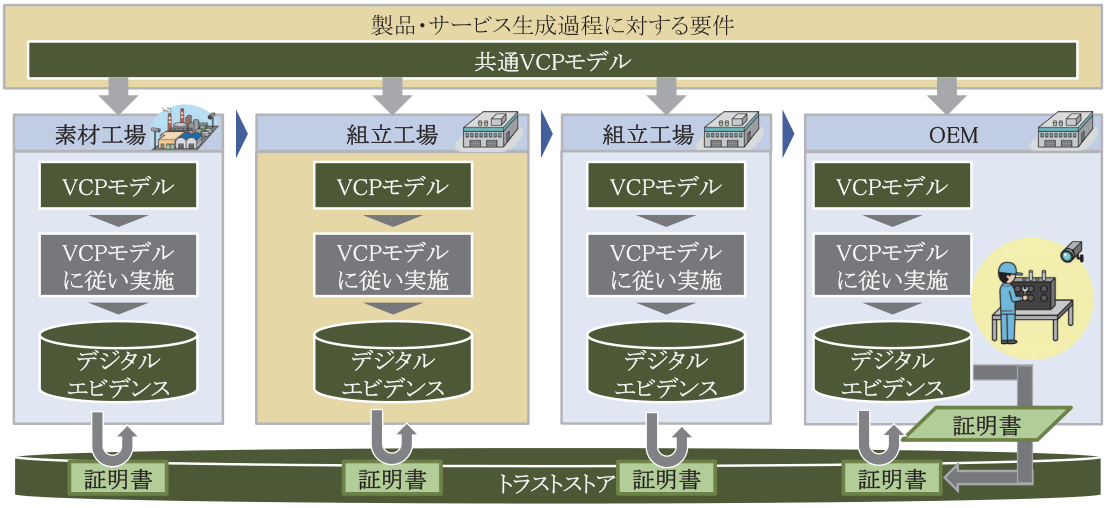
具体的な解決策の例

サプライチェーン・トラスト・ソリューションの技術では上記 3 点をソリューションとして提供します。規程内容をサプライチェーン内で共有するため、「規程に従い生成されたこと」、「確認方法」、「エビデンス」を関連付けて記述可能な VCP 表記法を用いて生産工程等の工程を記述します。この VCP 表記法で記述した内容と工程のデータを組み合わせて検証することで規程に従って実施したことを示すデータを「信頼性の裏付け（デジタルエビデン

ス)」として保存します。そして、この証跡を顧客や上位サプライヤー等にも示すことが可能となります。

デジタルエビデンスとして規程に従って実施したことをデータとして保管され、トラストストアによりサプライチェーンを辿ってデジタルエビデンスを照会できるようになっていることから、サプライチェーン全体で規程に従って生成、運用されたことを確認できます（図表 65)。

図表 65　サプライチェーン・トラスト・ソリューション全体像



顧客への提要価値 / 導入効果

サプライチェーン・トラスト・ソリューションを用いることにより、サプライチェーン全体で規程に従って適切な生産活動等を実施することで客観的なデータを対外的に示すことができるようになります。また、規程等のルール順守だけでなく、SDGs や ESG 等の新たな社会価値や環境価値への取り組みに関するサプライチェーン全体での取組についても、データを用いて訴求できるようになります。

例えば、「衛生管理や安全管理等目には見えにくい提供価値の見える化」では、現状の課題として、安全、安心、快適な環境の提供に向けて「衛生管理」や「安全管理」のサービスを正しく実施しているものの、その価値を利用者に認識してもらうことが難しいという問題があります。衛生管理サービスを提供している企業ならびにそのサービスを利用している企業（(例）清掃会社とビル会社等）は規程等のルール順守が疑わしい安価なサービスとの違いをテナントや利用者に伝えることに苦慮しています。

トラストストア等を用いると、根拠となる安価なサービスとの違いを示すデータを第三者であるテナントや利用者に示すことが可能になることから、テナントや利用者に訴求しづらい「衛生管理」や「安全管理」等のサービス価値も認識してもらいやすくなります。第三者であるレストランの利用客が店舗の換気状態を調べるにあたって、テナント先であるレストランの店舗はトラストストアを通じて、テナント先の「換気」状態を、ビルオーナーは実施している「設備管理」状態を、建設業者は施工を行った「空調設備」の施工状態を、それぞれデジタルエビデンスとして提供することで、レストランの利用者は安心して食事を行うことが可能となるというメリットが挙げられます。

競合優位性

各工程のデータは、VCP モデルと比較の上、適合性検証が行われ、検証を行う際に使用した各工程のデータと検証結果はデジタルエビデンスというデータで保存されることになります。トラストストアというデジタルエビデンス管理技術と連携されることで容易に関連性の高い作業工程の検証結果・根拠を検索できるようになります。そのため、万が一問題が発生した場合は、下流工程から上流工程へと紐づけられるため、サプライチェーン全体で根拠となる証跡の確認によって原因となった作業工程を容易に確認することができます。

また、このトラストストアの情報は、サプライチェーンを構成する企業以外への情報開示が容易であるため、第三者の方が容易に根拠となる証跡の確認ならびにそれらの確認を通じて信頼を醸成することができるようになります。

サプライチェーントラストソリューションに関する問い合わせ先

株式会社日立製作所
サービスプラットフォーム事業本部 マネージドサービス事業部
SIP2_B3_info1@ml.itg.hitachi.co.jp

● 略語表

略語	英語表記	日本語表記
AES	Advanced Encryption Standard	先進的暗号化標準
AI	Artificial Intelligence	人工知能
CT	Computed Tomography	コンピュータ断層撮影
CPS	Cyber-Physical System	サイバー・フィジカル・システム
CPU	Central Processing Unit	中央処理装置
CVSS	Common Vulnerability Scoring System	共通脆弱性評価システム
DVR	Digital video recorder	デジタルビデオレコーダー
DX	Digital Transformation	デジタルトランスフォーメーション
EDR	Endpoint Detection and Response	エンドポイント検出応答
ICS	Industrial Control system	産業用制御システム
IoT	Internet of Things	モノのインターネット
IT	Information Technology	情報技術
IPA	Information-technology Promotion Agency, Japan	情報処理推進機構
LAN	Local Area Network	ローカルエリアネットワーク
MDR	Managed Detection and Response	検知と対応のマネージドサービス
MSS	Managed Security Service	マネージド・セキュリティ・サービス
MRI	Magnetic Resonance Imaging	磁気共鳴画像診断
OA	Office Automation	オフィスの自動化
OS	Operating System	オペレーティングシステム
OSS	Open Source Software	オープンソースソフトウェア
OT	Operational Technology	制御・運用技術
PC	Personal Computer	パソコン
SBOM	Software Bill Of Materials	ソフトウェア部品表
SIP	Cross-ministerial Strategic Innovation Promotion Program	戦略的イノベーション創造プログラム
TFC	Trustworthy Field Constructor	ティー・エフ・シー
TPM	Trusted Platform Module	トラステッド・プラットフォーム・モジュール
USB	Universal Serial Bus	ユニバーサル・シリアル・バス
VCP	Value Creation Process	バリュー・クリエイション・プロセス
VPN	Virtual Private Network	仮想専用線
WAF	Web Application Firewall	Web アプリケーションファイアウォール

免責事項

本ガイドブックには法的拘束力はなく、ある行為等が、本ガイドブックに記載された事項に準拠しなかったことをもって、本ガイドブックに基づき法令上の罰則等が課されるものではありません（ただし、その行為等が他の法令等に抵触する場合には、当然、当該法令等に基づき罰則等が課される場合があるので留意が必要です。）。

本ガイドブックは、個別のサイバー・セキュリティ対策に関する助言を構成するものではありません。本ガイドブックは、実行されたサイバー・セキュリティ対策の導入効果等を証明するものではなく、当該効果等について責任を負うものではありません。個別のサイバー・セキュリティ対策の検討を行う者は、その責任の下で検討を行うものとします。内閣府は、本ガイドラインに記載された情報の利用等、又は、本ガイドブックの変更、廃止等に起因し、又は関連して発生する全ての損害、損失又は費用について、いかなる者に対しても何らの責任を負うものではありません。

ソリューション（技術）内容についての問い合わせ先

ソリューション（技術）名	連絡先
ソリューション①: 既存機器のインターフェース部に外付け可能な 通信暗号化コネクタシステム	株式会社 SCU c01.contact@scu.co.jp
ソリューション②: IoT 機器向けの改ざん検知ソフトウェア（技術）	日本電信電話株式会社 社会情報研究所 solab@ml.ntt.com
ソリューション③: IoT や OT システムにおけるセキュリティ 異常対処支援技術	
ソリューション④: 信頼できる取引ネットワーク構築サービス	富士通株式会社 キャリア＆メディア事業本部 NTT ソリューション事業部 contact-sip2-b2@cs.jp.fujitsu.com
ソリューション⑤: サプライチェーン・トラスト・ソリューション	株式会社日立製作所 サービスプラットフォーム事業本部 マネージドサービス事業部 SIP2_B3_info1@ml.itg.hitachi.co.jp

その他ガイドブックに関する一般的な問い合わせ先

NEDO　IoT 推進部

Tel : 044-520-5211　　E-mail : cyber-sec2@nedo.go.jp

QR コードから NEDO の WEB ページ（https://www.nedo.go.jp/activities/ZZJP2_100123.html）
を参照いただくと、本資料およびガイドブックエグゼクティブサマリーをダウンロードできます。