SIP 戦略的イノベーション創造プログラム
Cross-ministerial Strategic Innovation Promotion Program

戦略的イノベーション創造プログラム（SIP）
重要インフラ等におけるサイバーセキュリティの確保

研究開発成果集

2020年3月

内閣府
国立研究開発法人 新エネルギー・産業技術総合開発機構

巻頭のご挨拶

ＳＩＰ「重要インフラ等におけるサイバーセキュリティの確保」
～世界で最も安心・安全な社会基盤の確立を目指して～

戦略的イノベーション創造プログラム（ＳＩＰ）は、総合科学技術・イノベーション会議（ＣＳＴＩ）が司令塔機能を発揮して、府省の枠や旧来の分野を超えたマネジメントにより、経済再生・成長の実現、あるいは社会的課題の解決を行うために、2014年度に創設した国家プロジェクトです。当初は農業、自動走行等の10課題でスタートしましたが、増大するサイバー攻撃の脅威に対応するため、2015年度に本プロジェクト「重要インフラ等におけるサイバーセキュリティの確保」が追加されました。

サイバー攻撃は年々巧妙化しており、何時どのような攻撃が発生するのか全く油断出来ない状況です。特に2020年に東京オリンピック・パラリンピック競技大会を迎える我が国においては、国民生活の根幹を支える重要インフラのサイバーセキュリティ確保は急務です。また、我が国では、企業のサイバーセキュリティ対策に組み入れられている製品の多くは海外事業者に依存していますが、重要インフラのサイバーセキュリティ対策では、その重要性を鑑み、国産技術のレベルを高めて活用していく必要があります。

このような状況の中、本プロジェクトでは、2020年までの実用化を必達事項として、特に通信・放送、エネルギー、交通といった我が国の重要インフラを確実に防護することを目標に、重要インフラシステムの設備内部の耐性を高めるコア技術の開発と、それを使いこなすための社会実装技術の開発をあわせて進めました。また、研究開発当初から重要インフラ事業者との協働検討体制を通して事業者のニーズを研究開発に反映できたこともあり、本プロジェクトの開発技術の重要インフラ事業への導入が既に始まっています。

今回、５年間のプロジェクトの仕上げの一つとして本プロジェクトの研究開発テーマの概要・取組を成果集としてまとめました。本プロジェクトの成果を確認いただくとともに、プロジェクト終了後も広くご活用いただきたく思います。

2020年3月

内閣府　プログラムディレクター
情報セキュリティ大学院大学　学長
後藤　厚宏

目次

1. 研究開発の狙い

背景：サイバー攻撃のターゲットは重要インフラへ

◆ サイバーセキュリティ戦略（2018.7.27閣議決定）
「国民・社会を守る任務を保証」⇒**官民一体となった重要インフラの防護の推進**

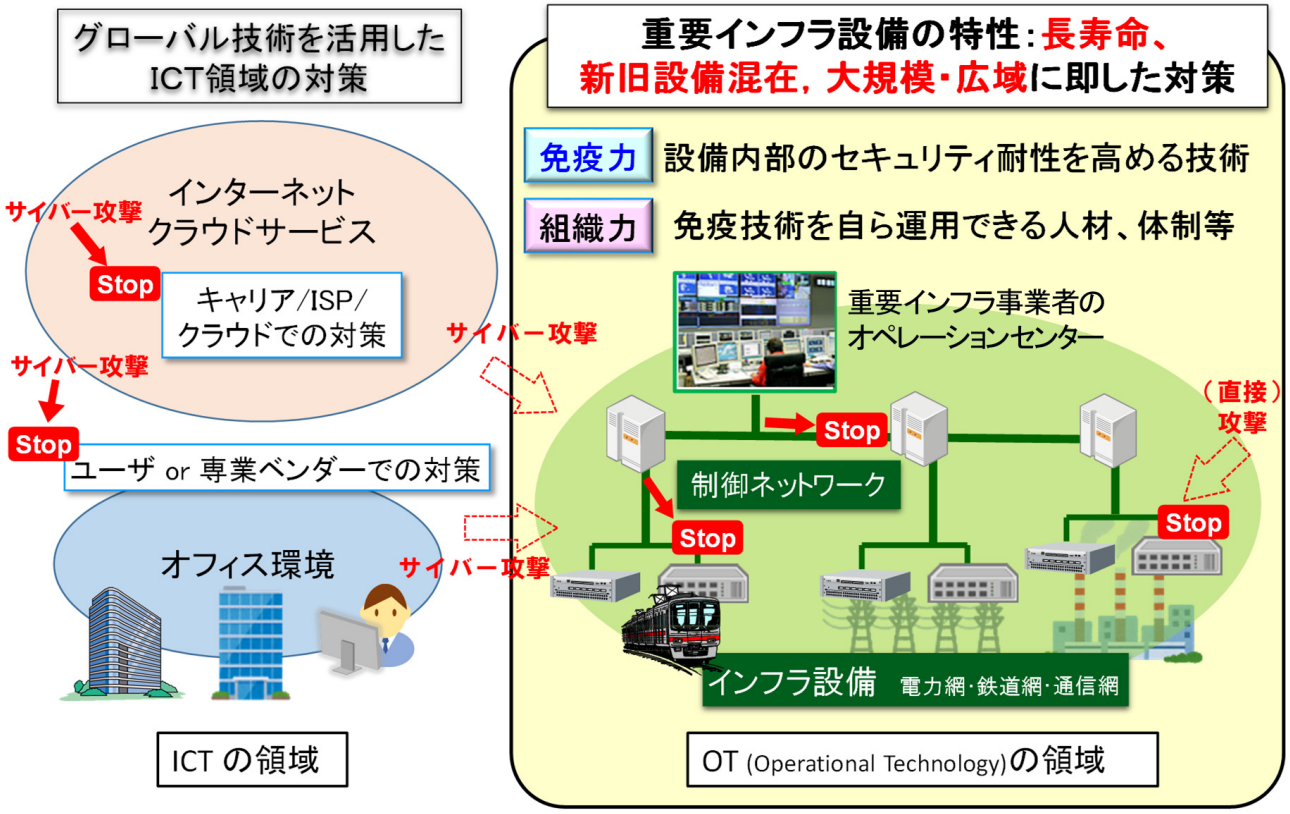
重要インフラのサイバーセキュリティ確保

国内インフラの強靭さは投資を呼び込む要件＆インフラ輸出競争力の源泉 ⇒ サイバー攻撃の脅威は現実に

2020年東京オリンピック・パラリンピック競技大会
⇒最大リスクは「日本のレピュテーション」の失墜

重要インフラの特性（長寿命、新旧設備混在、大規模・広域等）に適合したセキュリティ確保技術は世界的に未解決
⇒技術と運用の自給が必須

本プロジェクトの対象領域



研究開発の狙い

◆国内インフラ産業の安定運用、インフラ輸出、およびIoT時代に対応できる重要インフラ向け国産セキュリティ技術（拡大版）を開発し、産業活性化に貢献

◆計画段階からコア技術の社会実装を加速する取組として、重要インフラの通信・放送、エネルギー、交通の3分野で協働検討体制を構築

◆オリパラ前に首都圏近郊主要インフラに先行的に社会実装し、オリパラ2020の安全な開催に貢献

コア技術

「システムの免疫力」の向上
- 真贋判定技術
- 動作監視解析防御技術
- IoT向け暗号実装技術

社会実装技術

「組織対応能力」向上
- 情報共有基盤
- セキュリティ人材育成
- 適合性確認

研究開発テーマ

1. 制御ネットワークシステムのセキュリティ強化　コア技術

- サーバー機器の改変を常時検知して重要インフラを保護 （NTT）
- 内在する脅威の早期顕在化にて業務影響を最小化 （富士通）
- 侵入・攻撃の早期検知による制御システムのセキュリティ耐性強化 （日立製作所）
- 異常検知時においても安全に運用継続を可能とするシステム防御技術 （アラクサラ、CSSC）

2. IoTシステムの普及拡大に先行したセキュリティ対策技術　コア技術

- モニタリング機器の追加でIoTセキュリティ監視を提供 （NTT、三菱電機）
- IoTのセキュリティを実現する超低電力公開鍵暗号実装技術 （ECSEC、ルネサス）
- 「防御」「検知」「対策」でエンドポイントを守るトータルサイバーセキュリティ （パナソニック）

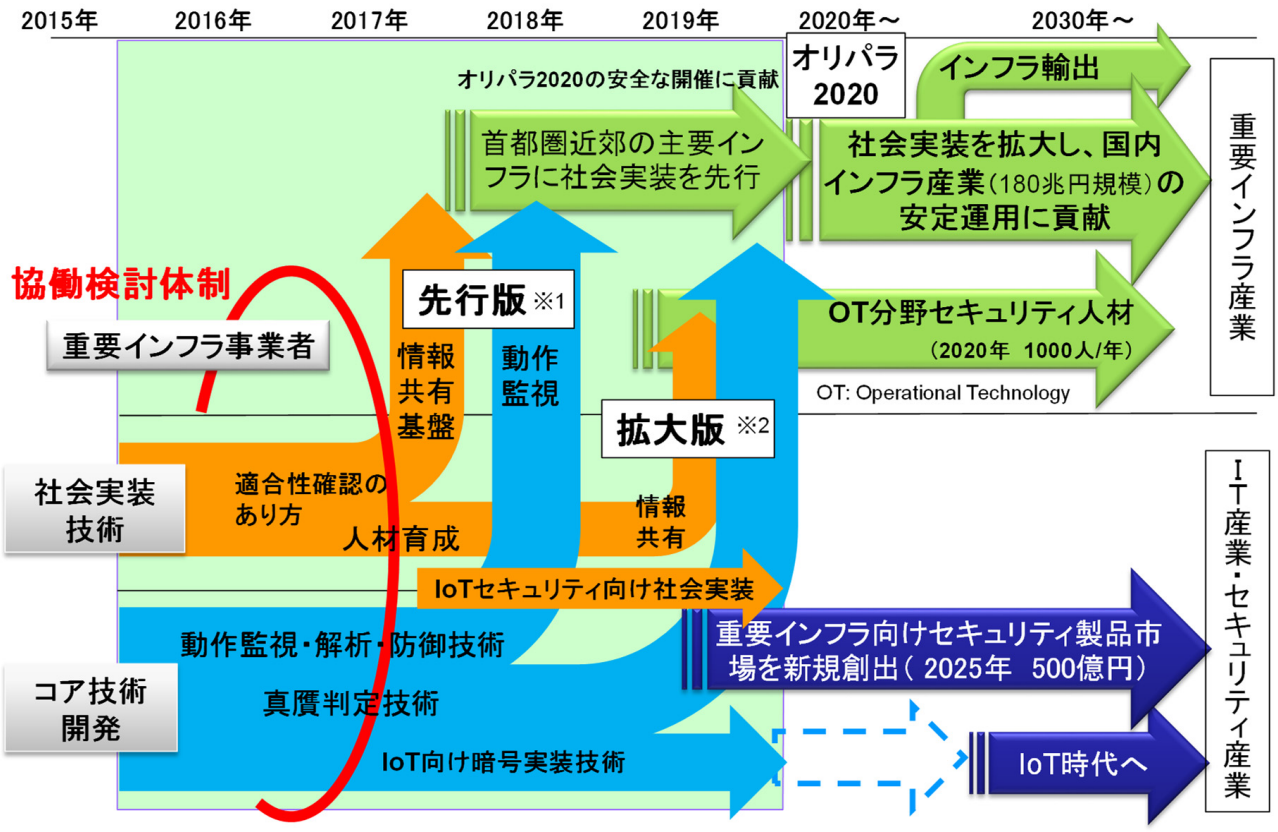
3. 重要インフラのセキュリティを確保する組織力強化と仕組みづくり　社会実装技術

- 研究開発技術の社会実装を促す適合性確認のあり方の研究開発 （産総研）
- 緊急度の高い脅威情報を迅速に配信し、重要インフラ事業者を防御 （日立製作所）
- 重要インフラでの実践力を養うセキュリティ人材育成 （慶應義塾大学）
- 組織のインシデント対応能力向上をめざす人材育成プログラム （名古屋工業大学）

4. SIP自動走行システムとの課題間連携

- ダイナミックマップの流通に向けたデータセキュリティマネジメントの実現 （富士通）

展開計画（プロジェクト期間：2015～2019年度）



※1 先行版：早期の社会実装を優先し機能を絞り込んだ版　※2 拡大版：本格的な社会実装に必要な機能を備えた版

2. 研究開発テーマ概要

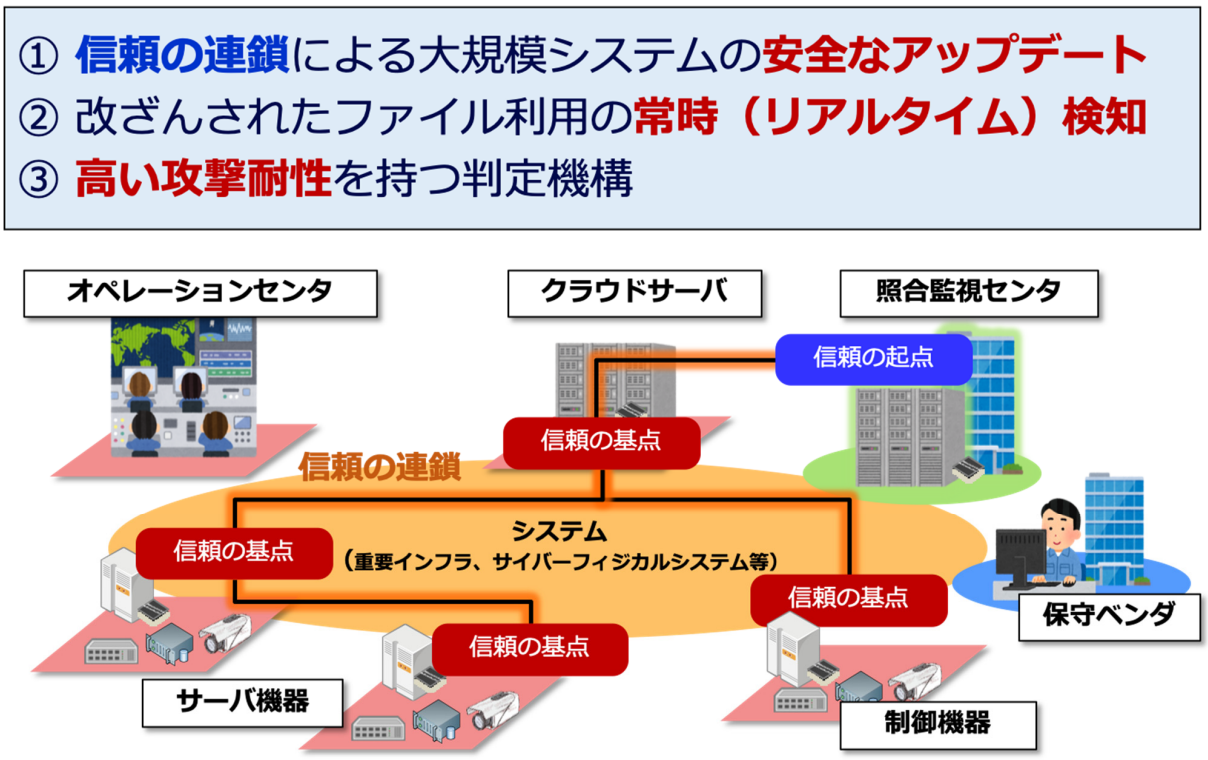
2．1　サーバー機器の改変を常時検知して重要インフラを保護

【研究開発の概要】

重要インフラ等のサービスを支える設備やネットワークは、個別製品や要素技術のみならず個々の機能を組み合わせて一つの統合体として機能していることから、システム全体でのセキュリティ確認が重要となる。本研究開発におけるセキュリティ確認とは真正性確認すなわち「制御・通信機器自体がなりすまされておらず正しいものであることの確認」、及び完全性確認すなわち「制御・通信機器で動作しているソフトウェア等が改ざんされていないことの確認」である。本研究開発は、システム全体に対するセキュリティ確認について、情報・制御ネットワークにおける信頼の基点を設定・駆使するアプローチにより研究開発に取り組み、重要インフラを構成するサーバ機器のシステム出荷・導入時に加えて運用時においても当該機器のセキュリティ確認（真正性確認・完全性確認）を効果的かつ効率的に行うことを可能にする技術の確立を目指した。

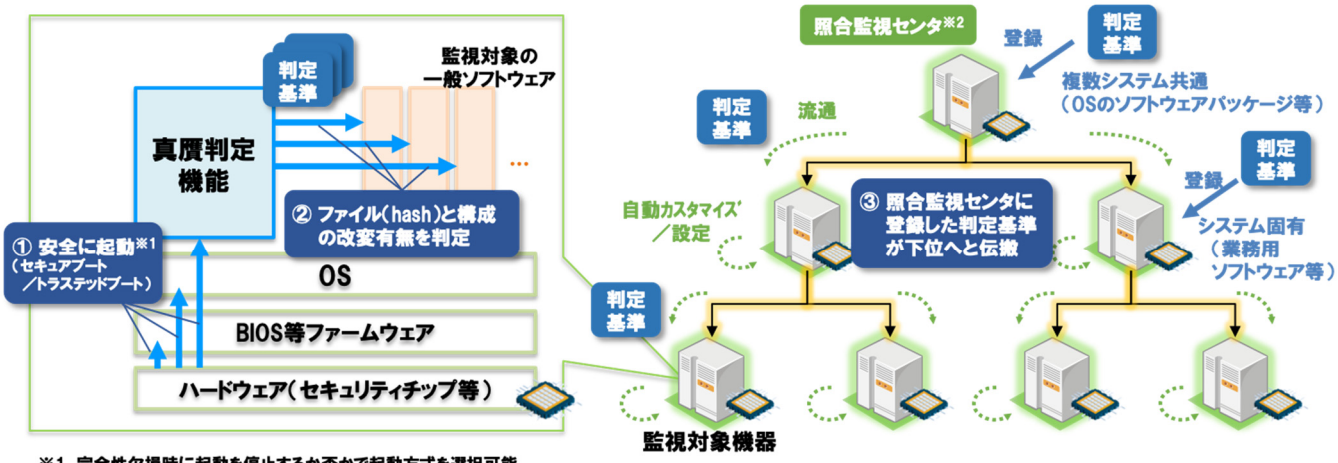
本研究開発では、このような認識の下で、重要インフラシステムを構成するサーバ機器の真贋（機器内のソフトウェアの完全性）を厳密に判定可能な技術である「真贋判定技術」を確立した。真贋判定技術では、独自機構である「信頼の連鎖」を活用して、重要インフラシステムのように多数のサーバ機器によって構成される大規模システムであっても、各サーバ機器の起動から運用を含むライフサイクル全体にわたって完全性の厳密かつ効率的な確認を可能にする。真贋判定技術では、各サーバ機器内部に「信頼の基点」を設け、「信頼の基点」がつながり合うことによって「信頼の連鎖」を形成する。各サーバ機器の「信頼の基点」は耐タンパー性を備えた本技術の基本要素であり、本技術がサイバー攻撃に対して高い耐性を備えるための必須要素となっている。

【「信頼の基点」及び「信頼の連鎖」を中核とする真贋判定システムの全体像】



【本技術の動作概要】

① 電源投入から真贋判定機能までを**安全に起動**
② 監視対象ソフトウェアの**ファイルと構成の改変有無を判定**
③ ソフトウェアのインストール/更新等を契機に**判定基準を上位機器から安全に取得**し、機器ごとに異なる判定基準は**機器内で自動調整**して設定

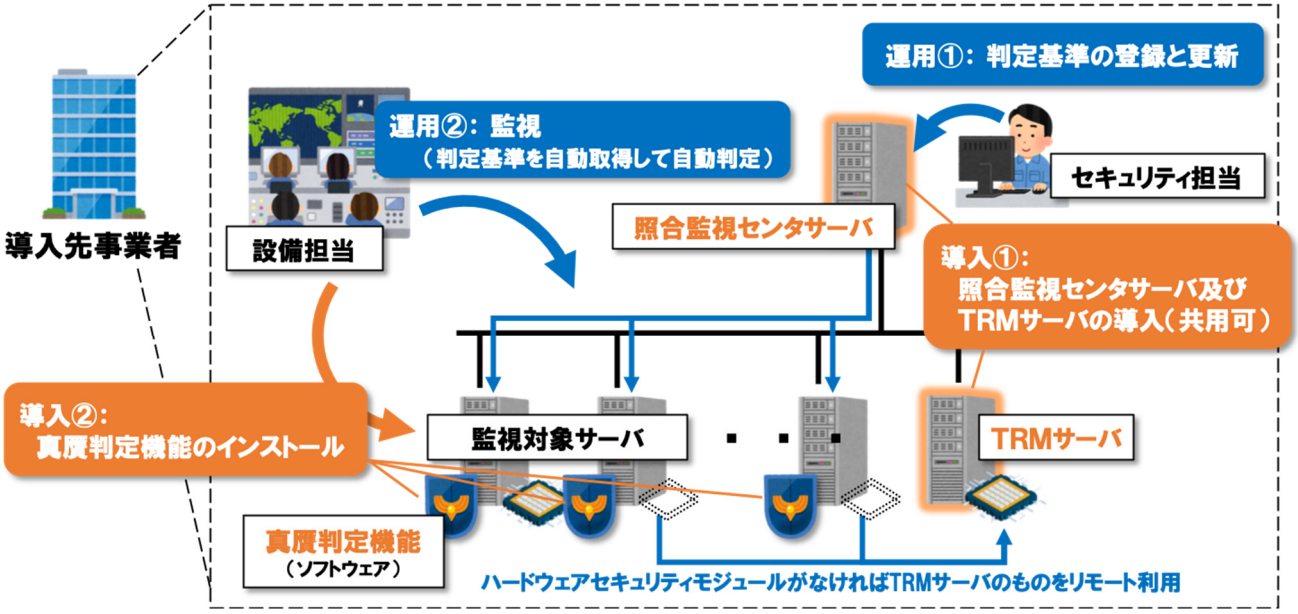


※1 完全性欠損時に起動を停止するか否かで起動方式を選択可能

※2 スケーラビリティを確保した真贋判定を実現するため、複数システム共通の判定基準の登録・配布元となり信頼の連鎖の起点となる機器

【本技術の導入例】

導入時： **ボルトオン型技術に近い導入**が可能
① **照合監視センタサーバ**及び**TRMサーバ**を新規導入（監視対象サーバから共用）
② 監視対象サーバに**真贋判定機能**を導入 （セキュリティモジュールは任意）
運用時： 判定基準の登録・更新業務の分離によって**高い安全性と自動判定**を実現



2.2　内在する脅威の早期顕在化にて業務影響を最小化

本研究開発テーマでは「個々の制御・通信機器及び制御ネットワークとしての動作を監視し、バックドアの有無などを解析するために、制御・通信機器のログ分析を機器内で行う機能、もしくはネットワーク経由で処理を集約する設備で行う機能」及び「将来にわたり高速大容量化するネットワークトラフィックに追従できる先進的なリアルタイムのログ収集機能、および将来の重要インフラ等において普及が予想される革新的な監視機能、および制御機能」を実現する為に必要な研究開発に取り組んだ。

過去の事例に基づく脅威検知パターンとの照合では、既知の攻撃手口とその亜種しか検知することができない。また、個々の装置に着目した挙動監視によるアノマリ検知では、通信装置の通信挙動には末端機器の通信が含まれるため、その装置自身が行う不審な挙動を特定することができない。そこで、ほとんどの通信装置の挙動は正常であり、バックドアが埋め込まれた通信機器はある時点ではごく一部であるという仮説に基づき、他の通信装置の挙動との乖離の有無を判断することで不審通信（バックドア通信）を行う機器を特定する技術を確立した。

重要インフラにおける高速・大容量の通信情報基盤には、新旧多種多様な情報機器・通信機器にて構成されている状況に加え、汎用技術の導入により、システムの仮想化・ネットワークの仮想化が急速に進んでいる。このような状況を踏まえ運用稼動中の機器を改変することなく、最小限の監視機器の導入にて通信パケットをモニター・分析する手法が求められることから、以下に挙げる４つの技術項目の研究開発を行った。

（1）システムならびにネットワークの仮想化に対応した高性能な**通信パケット収集技術**による仮想空間における通信の可視化技術

（2）大容量通信パケットの蓄積、検索を低コスト、高スケーラビリティにて実現する上での汎用サーバーを並列利用する**高速パケット蓄積・検索技術**

（3）通信の規則性や送受信の関係性に着目し、通信データ全体を正常とみなし、それらの特徴量と乖離を判断する群挙動モデル**解析技術**により、正常通信の中に紛れた不審な通信を抽出する技術

（4）セキュリティ脅威検出時においても重要インフラサービス・業務の安定継続は最重要事項として位置付け、緊急度と業務重要度に対する対処リコメンド**制御技術**

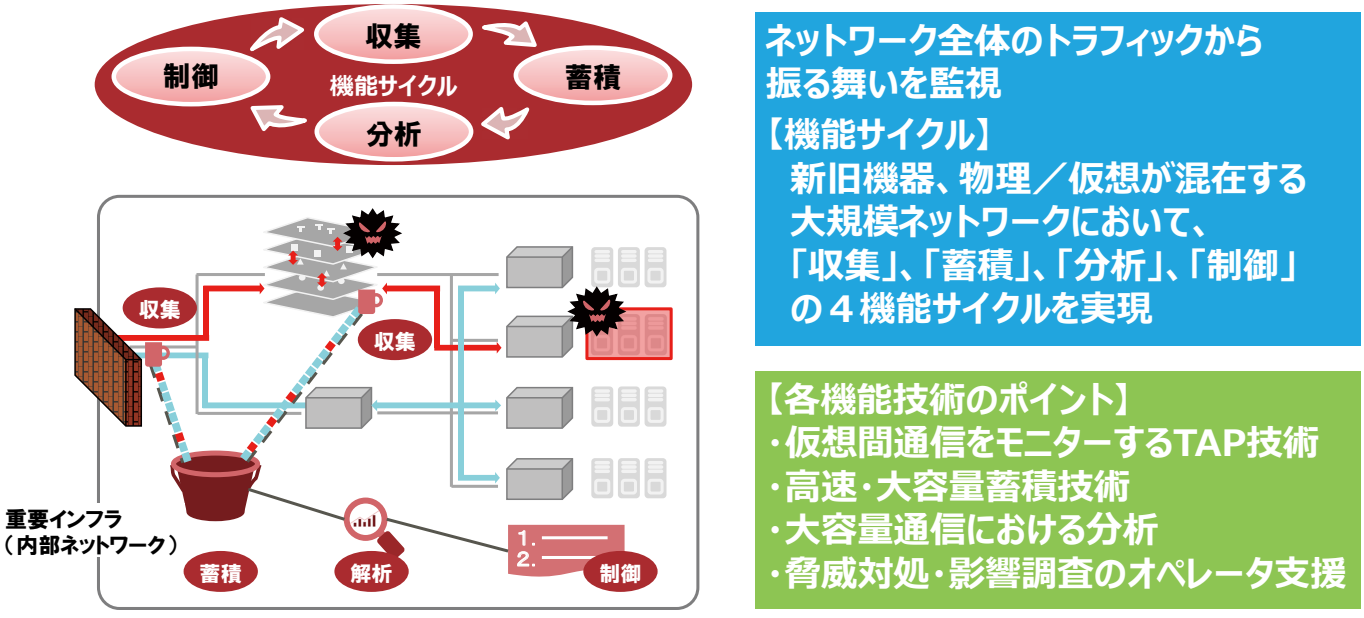


図2-2-1　機能サイクル

これら4つの技術により、物理／仮想ネットワーク形態に依存することなく、高速・大容量通信ネットワークの通信パケットを漏らさず監視・分析することで、ネットワーク内に潜在している脅威がエスカレーションされる前に顕在化させ、業務影響の最小化を図った。

開発した技術の優位性を表2-2-1に示す。

導入事業者にとってのメリットは、（1）高性能な仮想化モニターによって、仮想ネットワークの高速大容量通信を逃さずモニター可能とできるとともに、物理仮想が混在したネットワークも一元管理可能としている。また、（2）安価でスケーラブルな高速・大容量蓄積によって、安価な構築と、ネットワークの規模拡大に応じた設備投資が可能となっている。更に、（3）大量通信を俯瞰的に解析する群挙動モデル解析によって、短時間で全体の俯瞰的な検知が可能となっている。これに加え、（4）緊急度と業務重要度に対応する対処リコメンドによって、オペレータの稼動軽減を実現している。

表 2-2-1 技術的優位性

技術的な優位性	ユーザーメリット
（1）高性能な仮想化モニター	■従来技術と比較して7倍の性能により仮想ネットワークの高速大容量通信を逃さずモニター可能 ■物理環境と仮想環境の通信パケットを同時に収集できるため、物理仮想が混在したネットワークの一元管理可能
（2）安価でスケーラブルな高速・大容量蓄積	■汎用サーバーを使用することで専用機と比較して安価に構築可能 ■汎用サーバー並列によるスケールアウト型構成によりネットワークの規模拡大に応じた設備投資が可能
（3）大容量の正常通信の中に紛れた不審な通信を検出する解析	■個々に機器を解析する手法と比較して、事前学習を必要とせず、短時間でネットワーク全体の俯瞰的な検知が可能 ■通信の規則性に着目した解析手法のため暗号化通信にも対応
（4）緊急度と業務重要度に基づく対処リコメンド及び脅威の影響調査範囲の可視化	■従来技術は検知に留まり対処は運用者に依存 ➢レベル付けと対処提示でオペレータの作業を軽減 ➢検知した不審な通信の相関関係から、脅威拡散通信の候補抽出、他通信機器におけるバックドアの可能性がある被疑通信の抽出、可視化により早期に脅威を顕在化

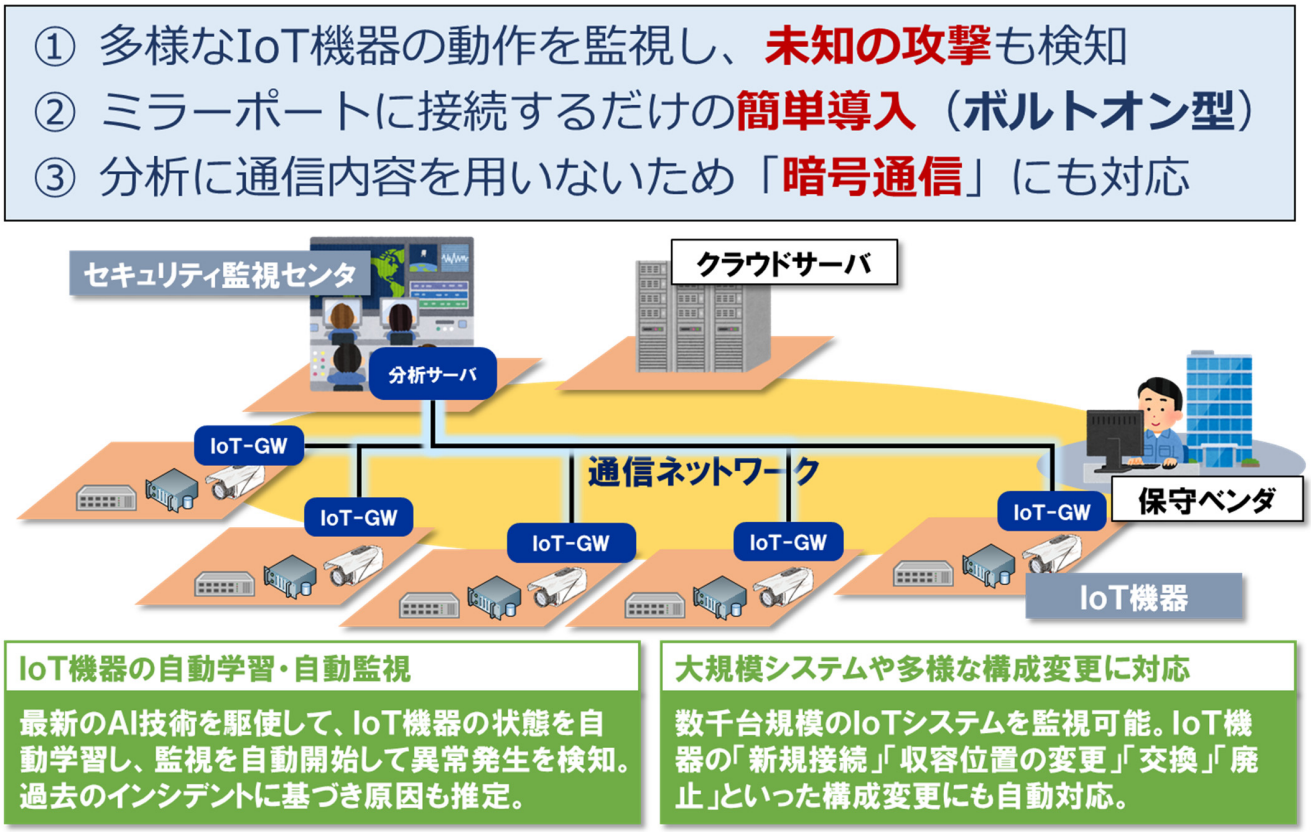
2.3　モニタリング機器の追加でIoTセキュリティ監視を提供

【研究開発の概要】

本研究開発では、IoTネットワークを監視するゲートウェイ装置（IoT-GW）と最先端のAI技術によって、多種多様なIoT機器に自動適応し、不正な動作を検知する技術の確立を目指した。

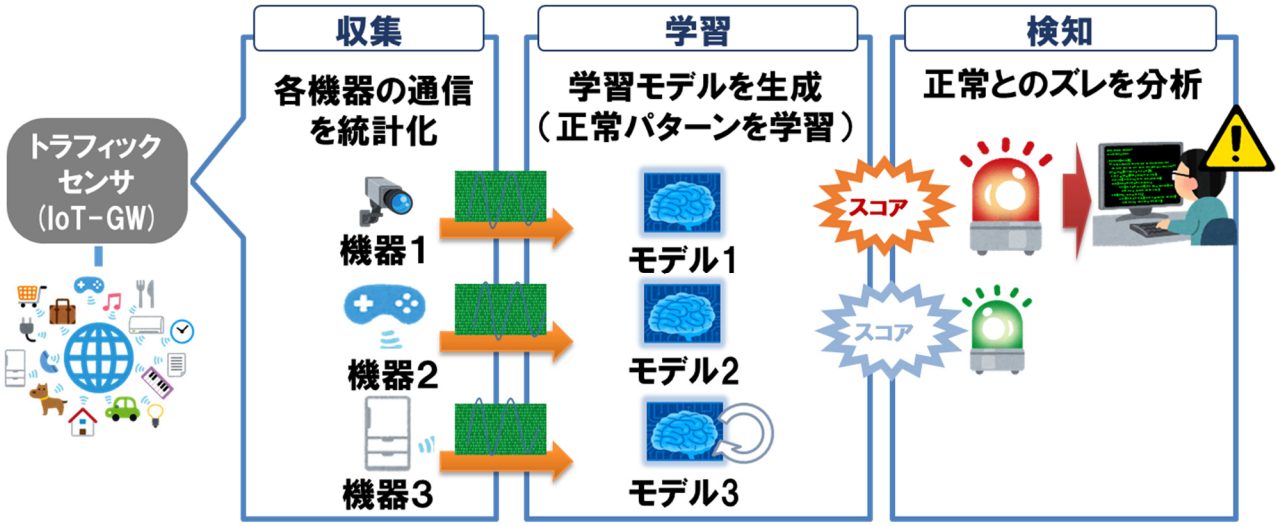
本研究開発において確立した技術は、既存のIoTシステムへの導入容易性を重視したIoTシステム向けの監視技術である。本技術が監視可能な機器は、通信トラフィックのバリエーションが限定的な機器であり、多くのIoT機器がこの特徴にあてはまる。また、定型業務端末についても発生する通信トラフィックの観点から同様の特徴を持つ場合、十分に監視が可能である。IoTシステムにおいて構成変更や規模変動が発生する場合、IoT機器の自動追従機能（学習等）及び分析サーバのスケールアウト機能によって監視を適切に継続することができる。

本技術は、IoTシステムの外部接続点において監視を行うゲートウェイ監視モードに加えて、IoTシステム内の随所で監視を行うミラー監視モードを備えている。監視ポイントの選定にあたっては、監視ポイント増設自動判定機能を活用して自動的に監視可否を判定することができる。本技術のユーザ事業者は、当該機能を活用しながら、漏れのない監視を優先する場合には監視対象機器付近での監視を行い、導入・運用コスト優先の場合には多くの通信トラフィックを観測しやすい監視ポイントを選択するなど、セキュリティとコストのバランスを考慮した多様な設計に対応可能である。



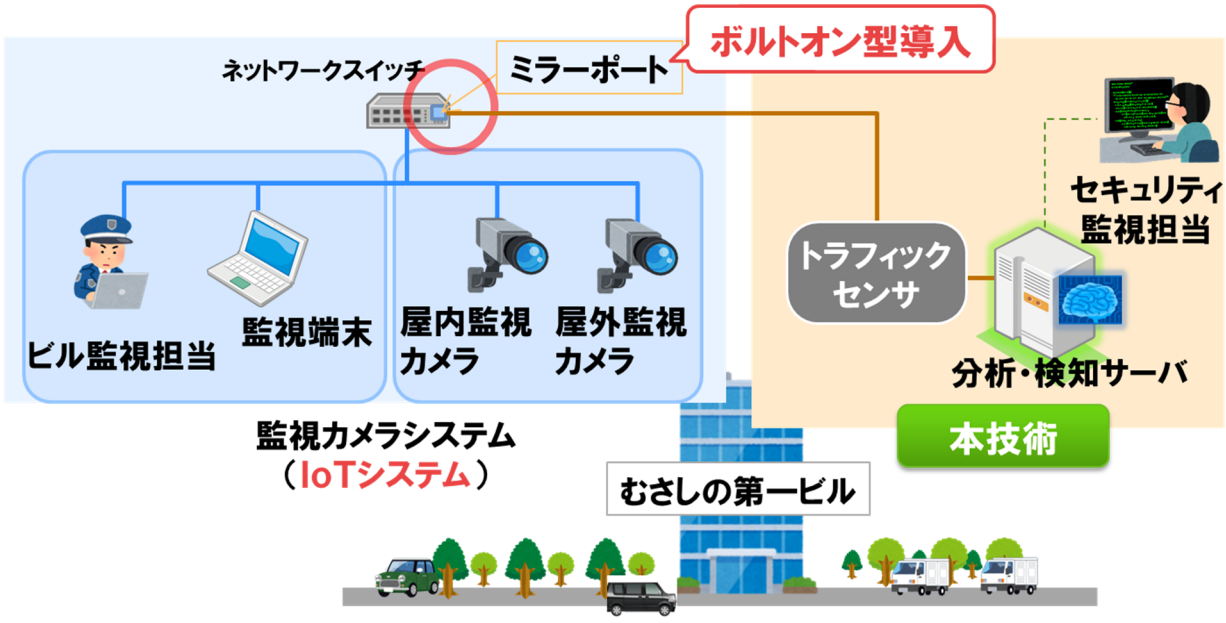
【本技術の動作概要】

- トラフィックセンサ（IoT-GW）が**対象機器の情報を収集**
- 対象機器ごとに**正常パターンを学習**
- 対象機器の**正常とのズレを分析**（**未知の異常も検知**）



【本技術の導入例】

ネットワークスイッチの**ミラーポートに接続**するのみで良く
既存のＩｏＴシステムへの導入が容易です。



2．4　侵入・攻撃の早期検知による制御システムのセキュリティ耐性強化

近年の巧妙化されたサイバー攻撃から重要インフラを守るためには、重要インフラシステムに適したセキュリティ技術が必要である。さらに、セキュリティ技術の研究開発に加えてセキュリティ運用・組織の確立も重要である。そのため本テーマでは、セキュリティ技術、運用・組織について研究開発した。

セキュリティ技術においては、制御ネットワーク向け動作監視・解析技術の確立を目指した。新旧機器が混在するシステムに影響することなく導入可能な、最先端の微細な変化を捕らえる統合健全性判定技術により、正常業務に紛れた不正動作を検知することを目的とし、「重要インフラにおける制御システムの分野固有知識と、分野間にまたがる共有知を統合できる革新的な解析モデルを構築し、継続的に進化可能な動作監視・解析技術」を実現するために必要な研究開発に取り組んだ。

重要インフラのサイバーセキュリティを確保するために、コントロールネットワークまでを含めたシステム全体の健全性を確認できる必要がある。このため、標的型攻撃などサイバー攻撃による健全性の劣化を検知する手段が必要である。標的型攻撃では、情報・制御ネットワークの制御・通信機器へ徐々に侵入し、最終的にコントロールネットワークの制御・通信機器に破壊的な異常を発生させることが想定される。標的型攻撃などによる健全性の劣化を破壊的な異常が発生する前に検知するためには、情報・制御ネットワークからコントロールネットワークにわたり、幅広く変化を検知し、解析する必要がある。

情報・制御ネットワークと、コントロールネットワークの変化を検知するには、以下の課題がある。

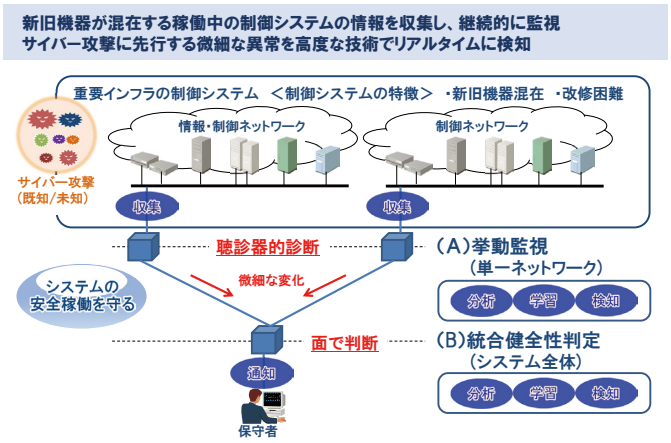
（1）コントロールネットワークを含むシステム健全性確認のためのセキュリティ侵害起因による障害検知の困難性

（2）正規ツールを悪用した標的型攻撃などによる異常検知の困難性

（3）コントロールネットワークにおける異常検知のための正常モデル生成の困難性

上記の課題を解決するために、（1）コントロールネットワークを含むシステムの健全性確認技術、（2）正規ツールを悪用した標的型攻撃などによる異常の検知技術、（3）コントロールネットワークの異常を検知するための正常モデル自動生成技術を研究開発した。

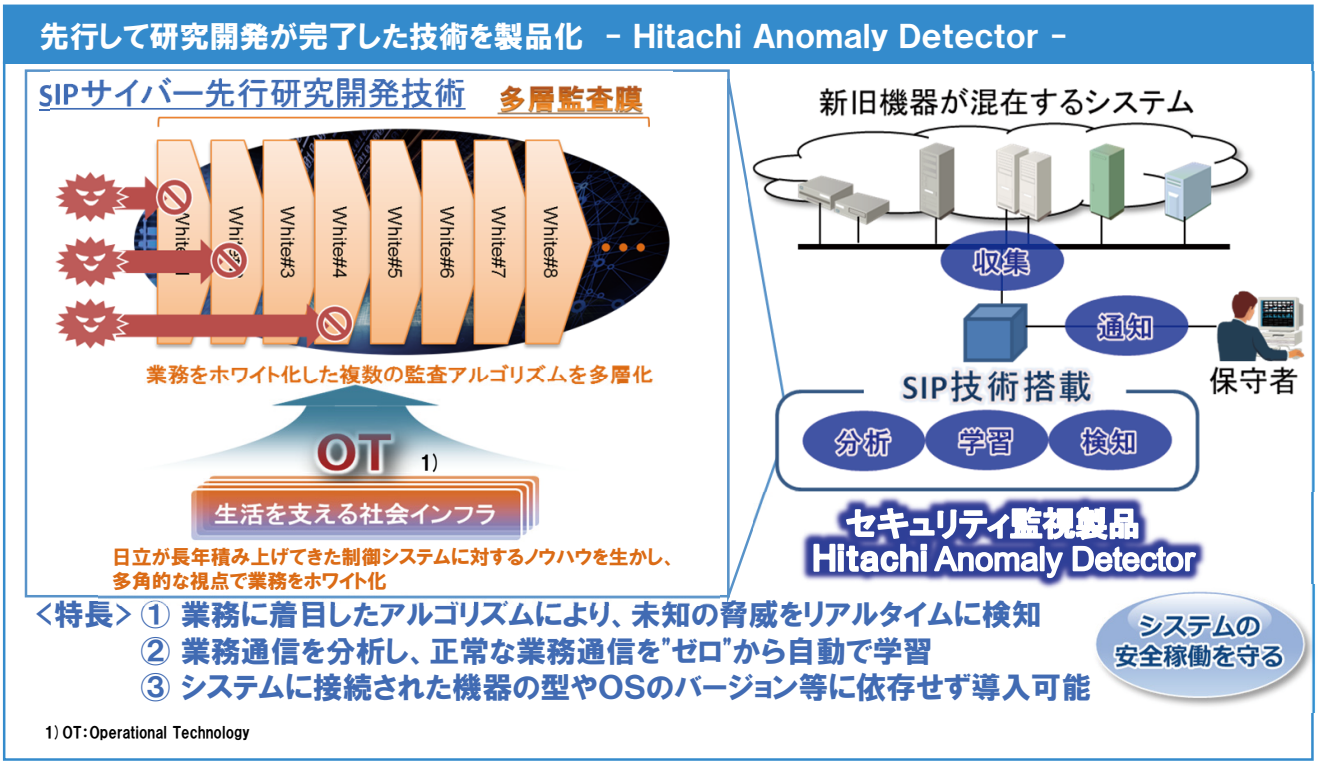
その研究の成果として、制御システムの特徴をとらえたアノマリ型の監視アルゴリズムをコア技術とする、システムを面で捉えたリアルタイム検知技術を完成させた。これは異常の発生箇所の具体化、検知要因の高度分析・具体化等によって、巧妙化が進む制御システムの攻撃を早期に検知することで制御システムのセキュリティを強化するものである。



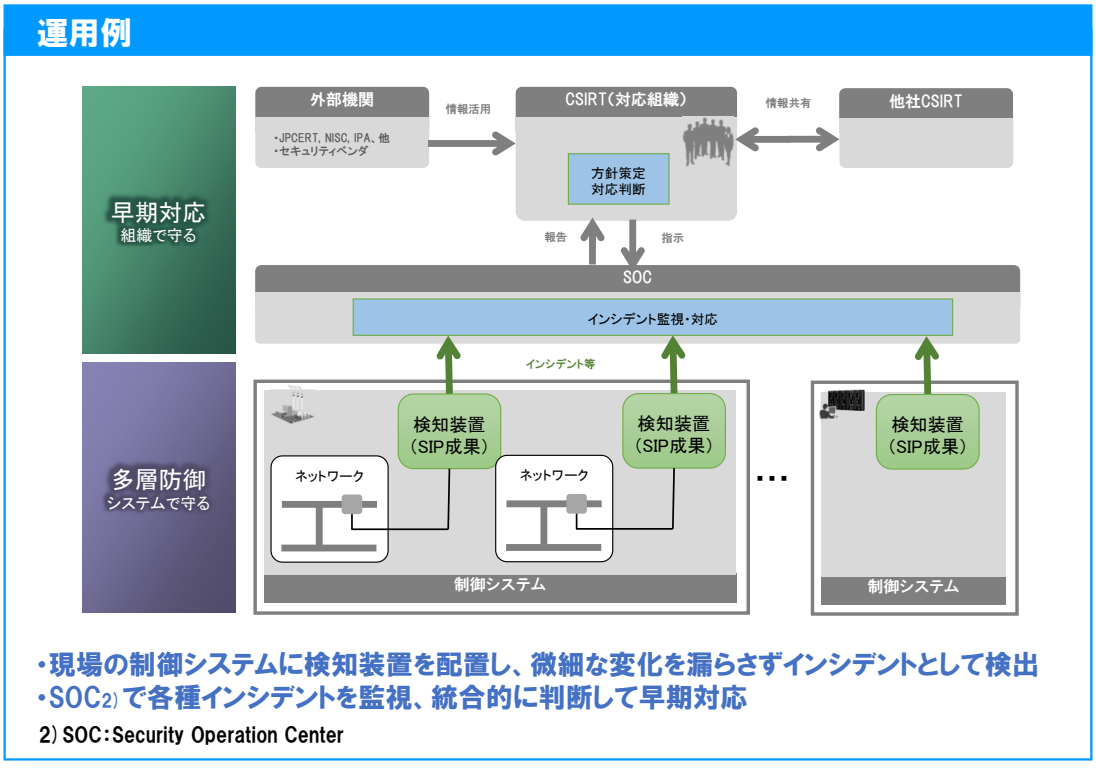
さらに、重要インフラ事業者によるセキュリティ対策のスムーズな導入に向け、事業者が特に考慮すべき事項や具体的な実現手法をガイドラインとしてまとめた。セキュリティ対策の導入においては、「設計」「構築」「運用」のライフサイクル全般を通した検討が必要となる。また、重要インフラシステムは可用性重視でサービスを止められないため、元のシステムに特別な加工を施すことなく追加する形（ボルトオン）でのセキュリティ対策適用が必要であるという特徴を持つ。本ガイドラインでは、このような特徴を持つ重

要インフラシステムに対して、「設計」「構築」「運用」の各フェーズにおいて、重要インフラ事業者が特に注意を払う必要がある点を重要ポイントとして抽出し、各ポイントの解説や実現例を記述した。

コア技術であるアノマリ監視アルゴリズムは、先行してHitachi Anomaly Detectorとして製品リリースされている。この製品は（a2）③技術の特長を活かしており、その特長は、新旧システムが混在するシステムに対し、（1）業務に着目したアルゴリズムにより、未知の脅威をリアルタイムに検知、（2）業務通信を分析し、正常な業務通信を"ゼロ"から自動で学習、（3）システムに接続された機器の型やOSのバージョン等に依存せず導入可能、である。



以下にHitachi Anomaly DetectorのCSIRT（対応組織）のSOC（Security Operation Center）での運用例を示す。



2.5　ダイナミックマップの流通に向けたデータセキュリティマネジメントの実現

本研究開発テーマでは、多種多様なダイナミックマップ情報（地図情報・地理情報）を保持する情報提供者と、そのダイナミックマップ情報を活用し付加価値サービスを提供するサービス提供者の間で、安心・安全にダイナミックマップ情報の受け渡しを実現する「ダイナミックマップ情報を取り扱う情報インフラ」（以降、ダイナミックマッププラットフォームと呼ぶ）のセキュリティ確保に必要な研究開発に取り組んだ。

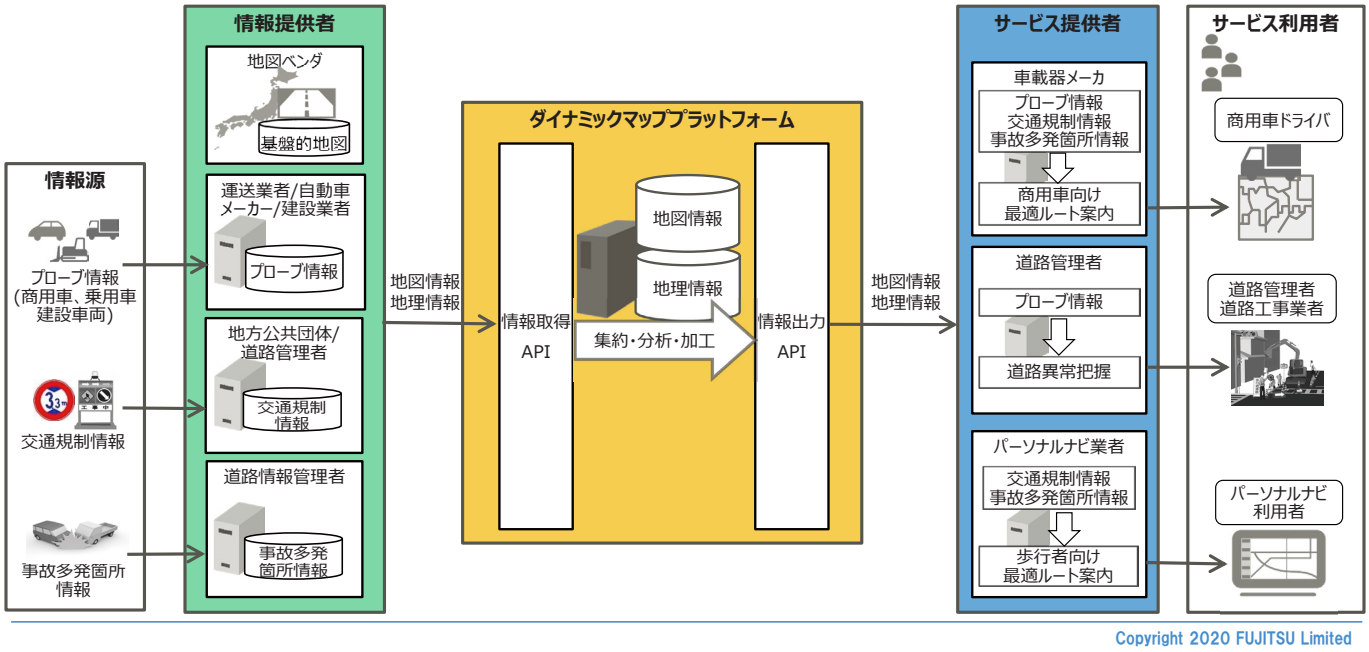


図2-5-1　ダイナミックマッププラットフォームの全体像

（1）ダイナミックマッププラットフォームのセキュリティ確保に必要なセキュリティ要求事項の策定

SIP／自動走行システムにて研究開発に取り組むダイナミックマップサービスプラットフォームをモデルとし、インフラ面と業務面から網羅的にセキュリティを検討し、ダイナミックマッププラットフォームに必要なセキュリティ要求事項（12カテゴリ、59要求事項、167項目）を策定した。さらに、セキュリティ要求事項に含まれない更なるセキュリティ強化に必要な仕組み、制度、運用等についてセキュリティ強化提言としてまとめ、今後の検討課題を抽出した。

（2）データのセキュリティ（機密性・完全性・真正性）を確保する技術の開発

ダイナミックマッププラットフォームで取り扱うデータには自動車の位置情報や車載カメラの画像などがあり高いセキュリティレベルが求められるため、データのセキュリティを確保することが重要課題である。

そこで、セキュリティ要求事項の実用に向けて重要課題であるデータのセキュリティを確保する仕組みを検討、情報提供者、サービス提供者、ダイナミックマッププラットフォームが連携することでデータのセキュリティを確保する技術（データセキュリティマネージメント）を開発した。

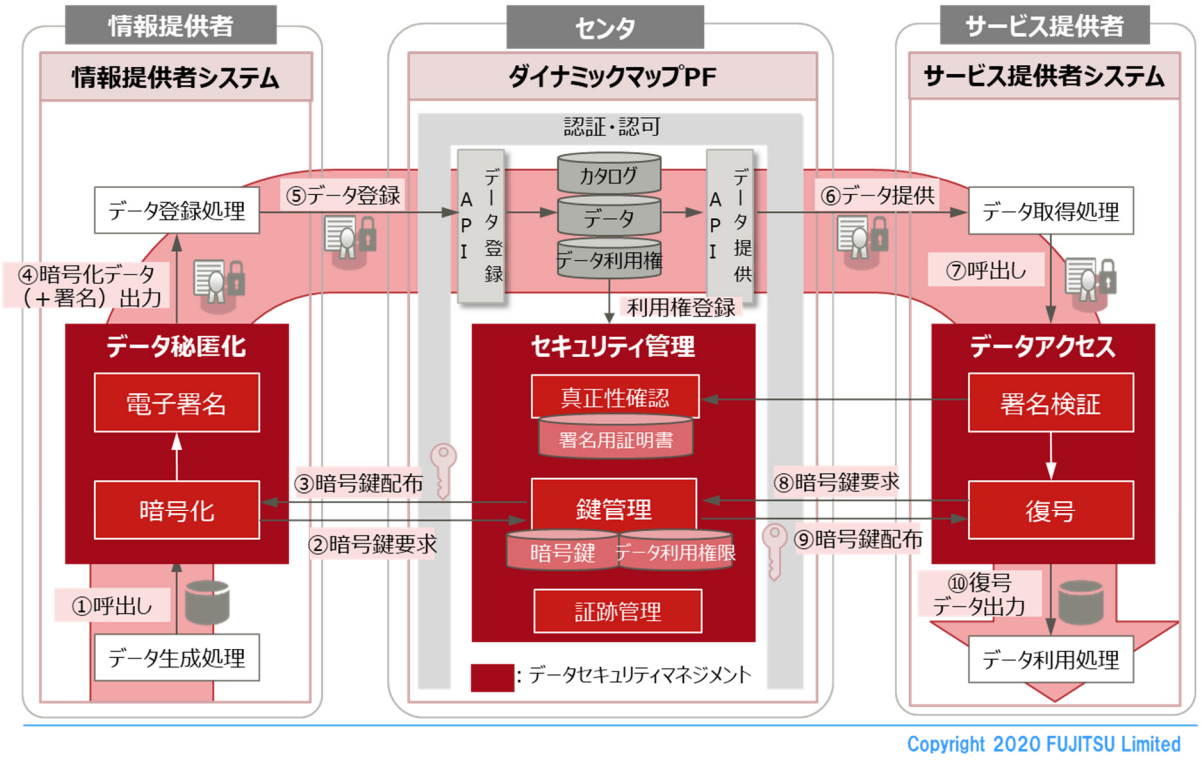


図 2-5-2　データセキュリティマネジメントの全体像

なお、本研究開発テーマはSIP／自動走行システム第1期と連携して取り組み研究成果を共有することで、SIP／自動走行システム第1期で調査・検討したダイナミックマップサービスプラットフォームのセキュリティ強化とセキュリティ・バイ・デザインを実現している。

2．6　異常検知時においても安全に運用継続を可能とするシステム防御技術

特徴

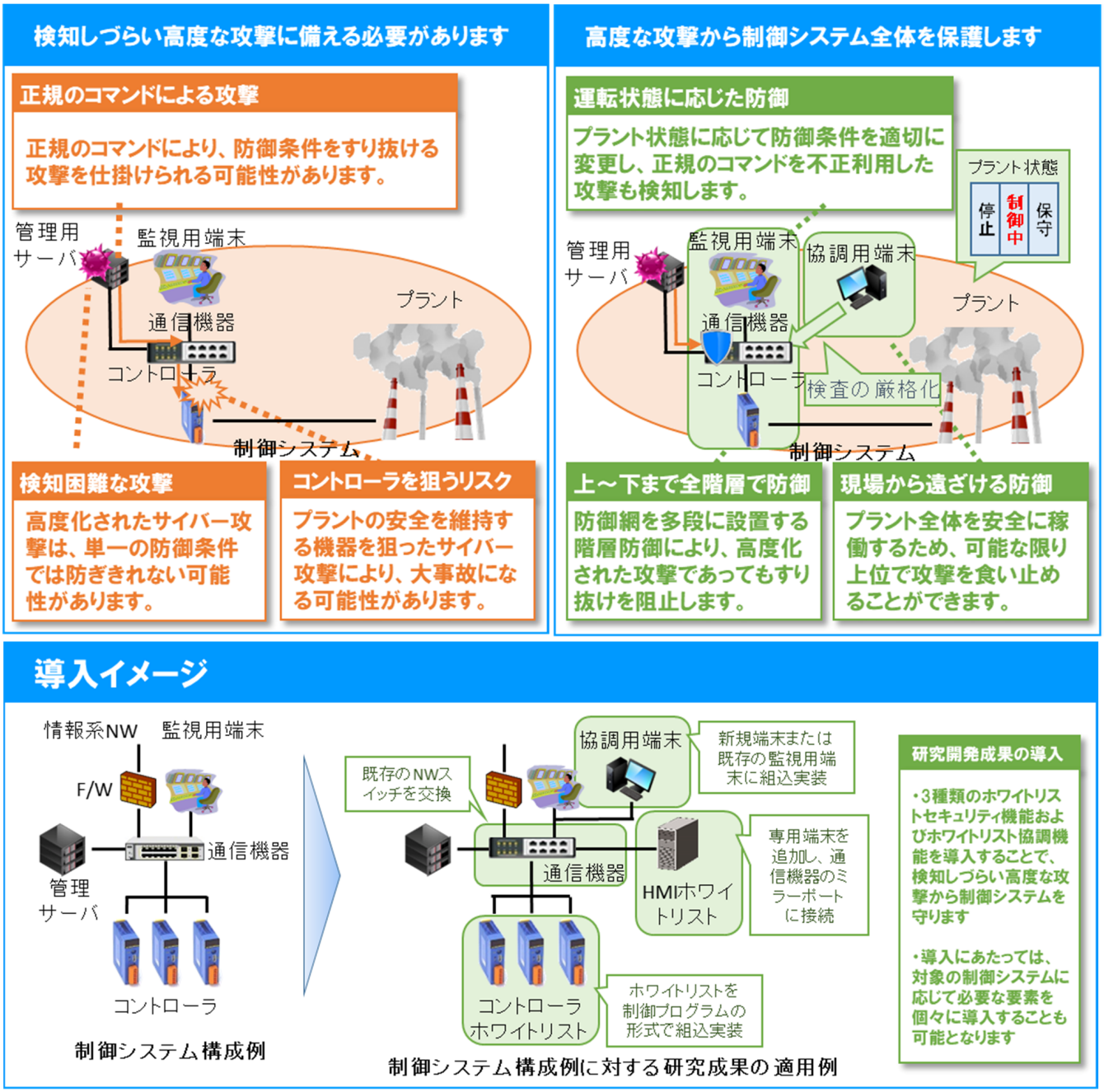
（1）制御システムの異常箇所を迅速に特定

プラントの運転状態に応じてライフサイクルを適切に変更し、監視用端末（上位）、通信機器（中位）、コントローラ（下位）の3つのレベルで、制御システムへの命令・指示を階層的に監視する。

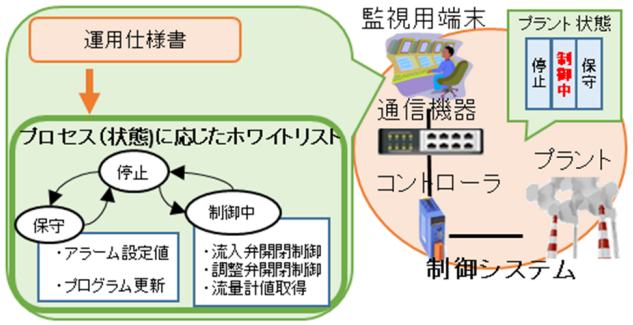
既存技術にはない下位レベルの監視を含めた各階層の機器の特徴を活かした検査機能を利用して、制御システムに対する攻撃箇所を迅速に特定し保護を行う。（階層検査機能）

（2）異常検知時も安全な運用を継続

協調機能により、攻撃を検知した機器の通信・処理を運用継続可能な範囲で制限しつつ運用を継続する。（協調機能）



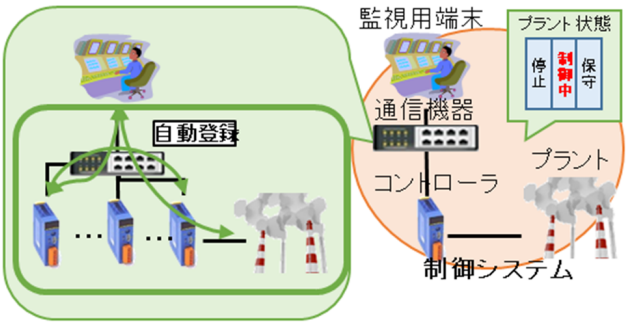
（上位）通常発生しない命令を検知・防御します



プラント状態に応じた防御

運用仕様書からプラント状態ごとに利用される命令をホワイトリストに定義し、ある状態では利用されるはずのない命令を攻撃として検知・防御します。

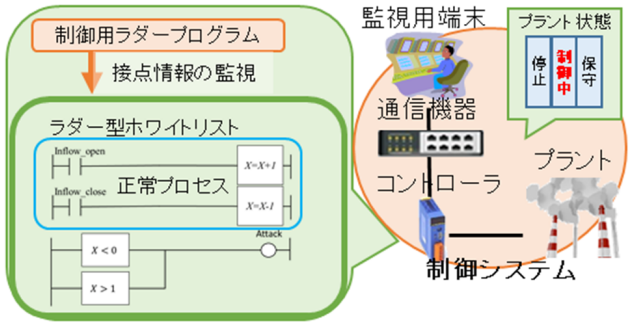
（中位）煩雑な管理なく攻撃を検知・防御します



制御プロトコルにも対応した学習機能を用いて防御

プラント状態ごとに利用される通信を自動学習によりホワイトリストに定義し、ある状態では利用されるはずのない通信を攻撃として検知・防御します。

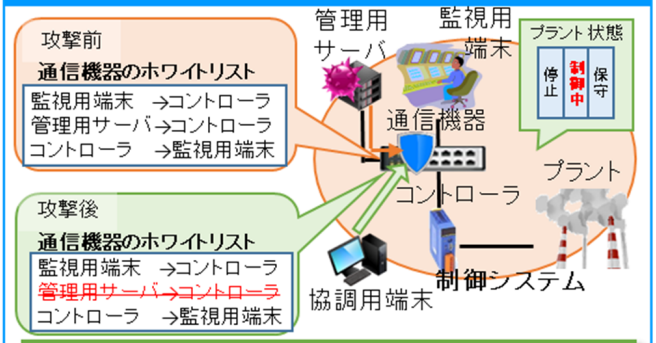
（下位）プラントの動作状態を監視・防御します



プラントの動作状態を監視し、動作が逸脱するものに対して防御

プラントの動作状態(I/Oの正常プロセス)を表現するラダープログラムが接点情報を監視することで、あらかじめ決められた動作を逸脱する場合を攻撃として検知・防御します。

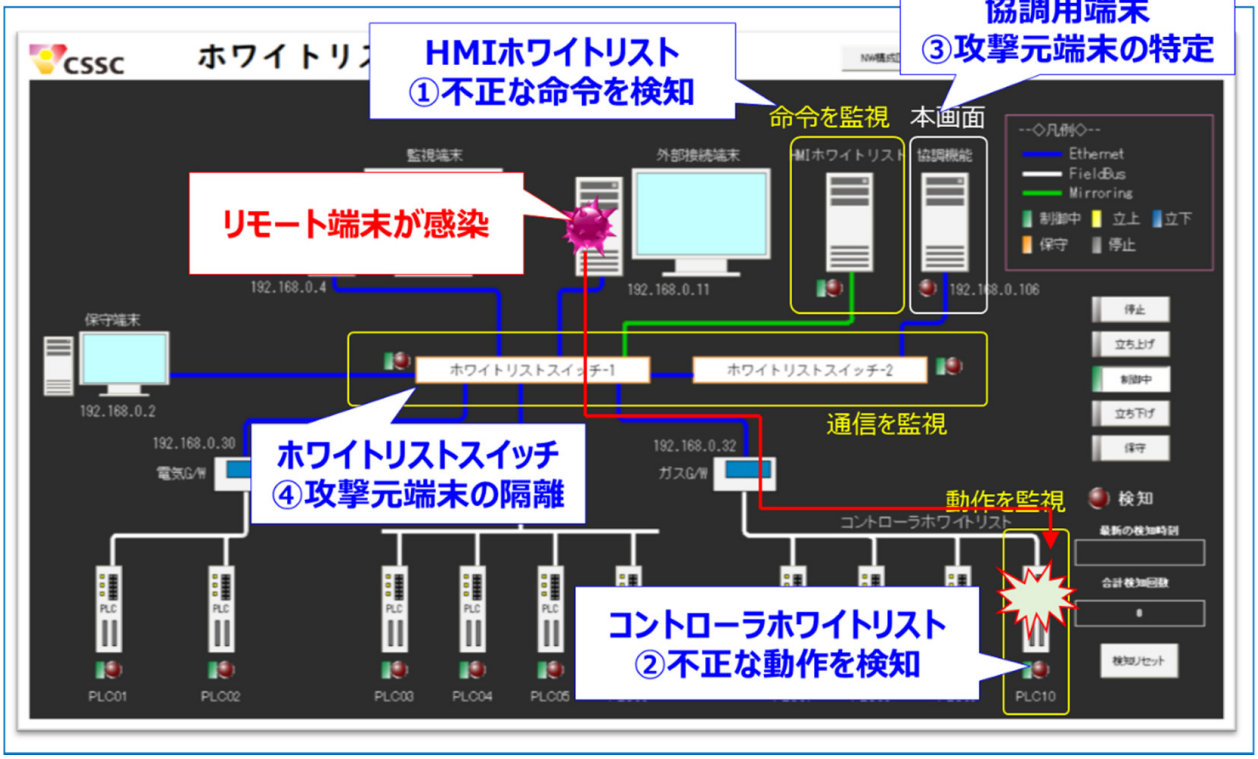
状況に応じた防御機能を適用し攻撃を防御します



攻撃をより上位で防御するため、上位の防御機能を厳格化して保護

プラント全体を安全に稼働するため、上位ですり抜けてきた攻撃を下位で検知できた場合、上位の防御機能の条件を見直して検知・防御します。

協調機能の動作例



2.7　IoTのセキュリティを実現する超低電力公開鍵暗号実装技術

公開鍵暗号をIoTの末端ノードでも自在に活用できる状況を創出

セキュア暗号ユニットSCU

入りマイコン（チップ）

SCU導入・活用方法

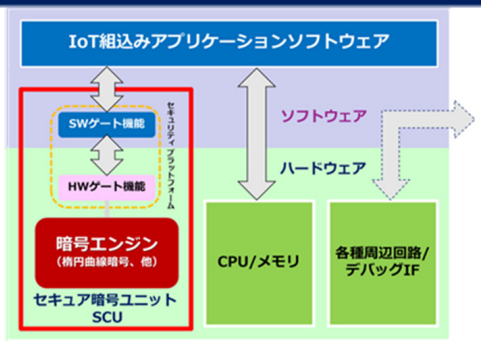
公開鍵暗号応用方式

IoT向けPKI

どこでも 公開鍵 暗号

A	共通鍵暗号しか使えない場合に比べ、格上のセキュリティを達成可
B	多数の末端ノードの鍵管理・セキュリティ管理コストを圧倒的に削減可
C	大規模IoTの利便性とセキュリティの両立に大きく貢献

セキュア暗号ユニットＳＣＵ入りマイコンを開発



本プロジェクトで唯一重要インフラ向けにこだわらず、IoTネットワーク向けの開発と位置づけ、2020年代のIoT社会全体のセキュリティ確保のための研究開発をめざした。

セキュリティプラットフォーム技術
ルネサスエレクトロニクス

セキュア暗号ユニット（SCU）のSWゲート/HWゲートの設計仕様開発と設計試作、SCU暗号エンジン部分への外部からのセキュアなアクセス制御を実現。

デジタル回路設計・暗号実装
横浜国立大学、東京大学、電子商取引安全技術研究組合

セキュア暗号ユニット（SCU）の暗号エンジン部分の設計仕様開発とデジタル回路設計及び試作、楕円曲線暗号（ECDSA)の超効率的なハードウェア実装を通じて、「軽く、速い」公開鍵暗号エンジンを実現。

アナログ回路設計・構造
神戸大学、産業技術総合研究所、電子商取引安全技術研究組合

セキュア暗号ユニットを搭載するシステムLSI全体のアナログ実装技術の新規開発、2.5次元実装等を通じて、システムLSIの性能向上とセキュリティの双方を実現。

耐タンパー技術
東北大学、横浜国立大学、神戸大学、奈良先端科学技術大学院大学、電子商取引安全技術研究組合

セキュア暗号ユニット（SCU）の耐タンパー性を確保する技術の開発と実装、評価。「強い」公開鍵暗号エンジンの実現。

HWトロージャン対抗技術
電気通信大学、奈良先端科学技術大学院大学、神戸大学、横浜国立大学、電子商取引安全技術研究組合

組込み機器へのHWトロージャン攻撃の事例整理と各製品レイヤーでの攻撃技術の分析、ポイントを絞った対抗技術の開発。

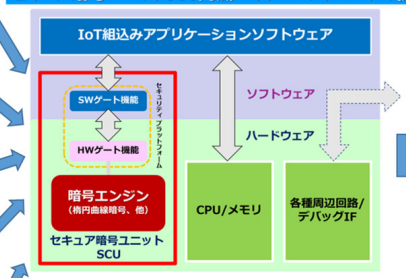
研究開発成果をセキュア暗号ユニット（SCU）として結実

各研究機関の共同研究の成果を結集して、システムLSIチップに搭載されるセキュア暗号ユニット（SCU）に集約。将来SCU部分をシステムLSIの設計IPとして、チップベンダに供給することを目指す。
（アナログ構造、耐タンパー技術、HWトロージャン対抗技術等はSCU以外の分野にも応用可能。）

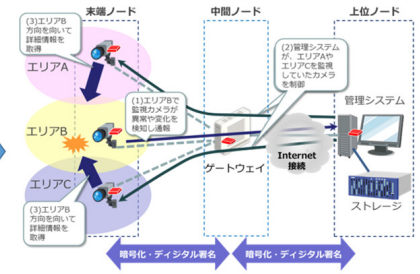
モデルシステムとして監視カメラシステムを構築
電子商取引安全技術研究組合

セキュア暗号ユニット（SCU）を搭載したシステムLSIチップのIoTシステムへのアプリケーション実証例の一つとして監視カメラシステムを構築し、検証。但し、SCUの応用範囲は、広く産業用機器制御、交通・医療機器、ロボット等IoT全般。

セキュア暗号ユニットSCU内蔵マイクロコントローラの例



セキュア暗号ユニット適用例：監視カメラシステム



実用化へ

社会実装に向けて

【導入分析】　セコム
自動車や医療機器のような、１つのシステムがマルチベンダの部品やモジュールによって構成され、さらに他システムと相互接続されることが見込まれるものや、人命等の重要資産にクリティカルに影響する分野で、広く社会アプリケーションで活用する可能性を検討し、可能なアプリケーション・システムのモデルを複数提案する。

【知財戦略ほか】　電子商取引安全技術研究組合
SIP終了後も研究開発成果を一体として知財運用するため、プロジェクト参加者の一つである電子商取引安全技術研究組合を会社化し、事業後継法人としてSCUの知財運用と普及に努める。
既に、本研究開発期間の中途から、IoTユーザより中間成果を利用したいとの引合いがあり、SCUは、今後IoTシステムのセキュリティを向上させるコア技術として、広く産業用機器制御、交通・医療機器、ロボット等、IoT全般での利用が期待される。

研究開発スケジュールと活用の展望

以下に各研究開発実施項目別の研究成果要約を掲げる。

（1）IoTシステムを構成する機器のためのSCUの開発

① 暗号モジュール試作開発

IoT向け半導体チップに搭載するIPユニットとしてSCU（セキュア暗号ユニット）の試作開発を行い、実施計画に掲げた所期の性能目標を達成した。

② 耐タンパー技術開発

半導体チップに対する外部からの侵襲性・非侵襲性攻撃技術の研究を行い、それらの攻撃の一部に対する対策技術を開発し①のSCU試作開発に反映させた。

③ セキュリティプラットフォーム開発

セキュリティプラットフォームを構成するハードウェアゲートとソフトウェアゲートの開発を行い、①のSCU試作開発に反映させた。

モデルシステムに必要となる暗号エンジンの内、ECCエンジン以外の部分の開発を行い、①のSCU試作開発に反映させた。

SCUユーザのためのガイダンス文書等を作成した。

④ 実用化戦略研究

SCUを社会実装するための知財戦略、SCUを広く普及させるための国際標準化戦略とインターオペラビリティ戦略の研究を行い、成案を得た。

（2）SCUを活用したモデルシステムの構築

① SCUを活用したモデルシステムの構築

SCUボードを搭載した監視カメラシステムを構築し、成りすましや映像データの改ざんなどの影響とSCUの効果をアプリケーションレベルで検証した。

② SCUの導入分析および実施モデル提案

SCUの効果が最大化されるような社会実装を検討するために、SCUの導入分析および運用モデルの提案を行った。

③ ハードウェアトロージャンに対抗する技術の開発

ハードウェアトロージャンを検出する手法の基礎検討を行い、半導体チップを用いた検出機構について基本的なデモンストレーションとシミュレーションを構築し、その有効性を示した。

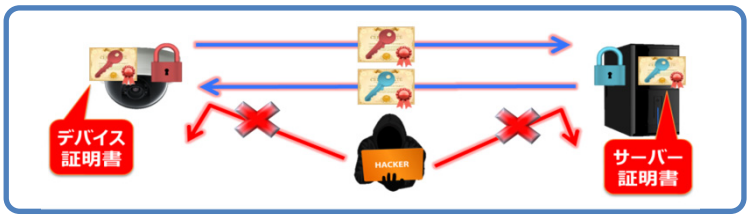
2.8 「防御」、「検知」、「対策」でエンドポイントを守るトータルサイバーセキュリティ

IoT向けセキュリティ対策技術として、IoT機器が持っている標準機能を使って推測困難な乱数を生成する技術を実現した。生成された乱数は計算量的に推測が困難な複雑度を保有しており、定型動作の多いIoT機器では不確定になりやすい乱数の生成時間も実用的な時間で実現している。また、専用のハードウェアを必要としないので、コストをかけずに実装することができる。本技術により、推測リスクの少ない乱数で暗号・認証鍵を生成することができ、IoT機器の安全な暗号・認証機能を実現することができる。

①「防御」技術：暗号・認証

セキュリティが脆弱なIoT機器は攻撃対象

- 中間者攻撃
- 総当り攻撃



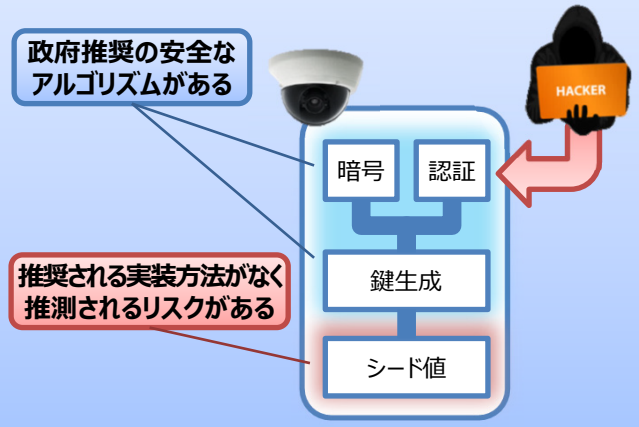
エンドポイント間でのPKI認証が必須

② 乱数生成 ： 推測リスクの少ない乱数から安全な鍵を生成

従来の課題　Before	導入による効果　After
ゆらぎの少ない乱数や設計者秘密は、鍵を推測されるリスクがある	IoT機器が持っている機能で推測困難な乱数を生成
機器の外部で生成した鍵は、漏えい時に漏えい元の特定が困難	機器の内部で乱数、鍵を生成し、漏えいリスクを低減

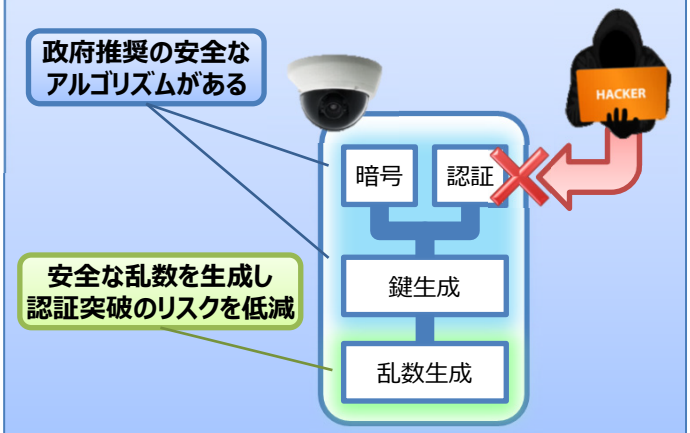
Before

シード値から暗号・認証鍵を推測され暗号・認証を突破されるリスクがある



After

IoT機器内で生成した推測困難な乱数から鍵を生成し、安全な暗号・認証機能を実現

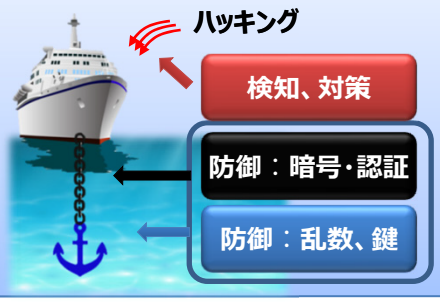


	ノイズ源		メリット	デメリット
	方式	概要		
従来の手法	機器固有ID等	MACアドレス等を利用	・生成速度が速い ・コストアップがない	・設計者秘密から推測されるリスクあり
	/dev/random	割り込みを利用 (ブロッキング型)	・推測が難しい ・コストアップがない	・割込みが少なく生成速度が遅い
	/dev/urandom	割り込みを利用 (ノンブロッキング型)	・生成速度が速い ・コストアップがない	・推測されるリスクあり
	物理乱数生成器	専用ハードウェアを利用	・生成速度が速い ・推測が難しい	・専用ハードウェアのコストアップが発生
研究成果手法	HW/SWのゆらぎ	オシレータ、実行パイプライン、分岐予測ユニット、スケジューラ、キャッシュ等のゆらぎ利用	・生成速度が速い ・推測が難しい ・コストアップがない	・安全性の評価が必要

また、暗号・認証機能で防げないサイバー攻撃に対しては、攻撃を検知し、対策する必要がある。従来ITで活用されている攻撃検知の仕組みはIoT機器からログを収集しないため、ネットワーク機器を経由しないIoT機器間の横感染の検知やIoT機器への攻撃に対する状況把握が難しく、インシデント発生時の検知漏れや対応時間が課題となっているが、IoT機器からログを収集する機能を実現し、ネットワーク通信に加え、IoT機器のログを監視することでサイバー攻撃を早期に発見し、被害拡大を低減することができる。

① 求められるセキュリティ

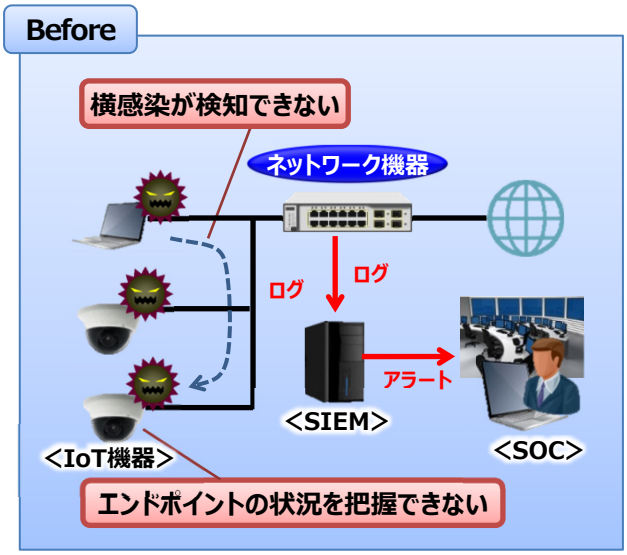
ライフサイクルが長く、人が介在しないIoTでは、「防御」に加え、「検知」と「対策」も重要

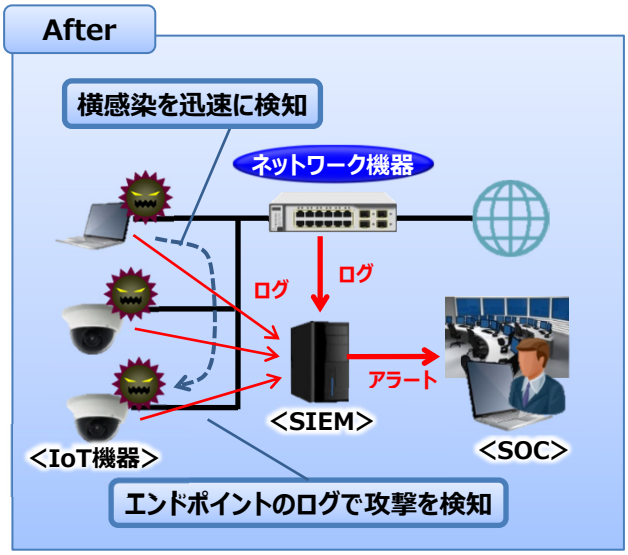


	ITセキュリティ	IoTセキュリティ
対 策	Windows Update ウィルスの隔離 等	サイバー攻撃対策
検 知	アンチウィルスソフト 等	
防 御	標準暗号通信 PKI認証	標準暗号通信 PKI認証

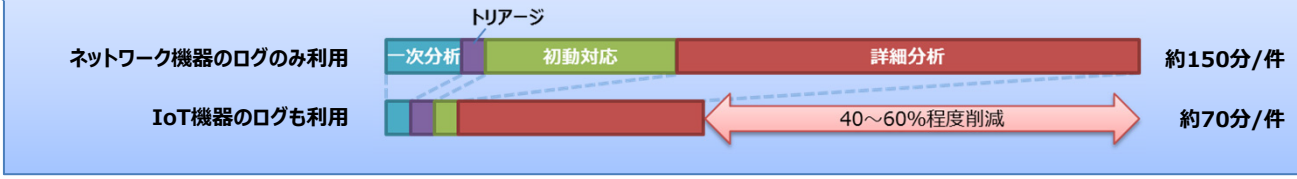
② サイバー攻撃対策：IoT機器のログを使って迅速に検知、対策

従来の課題　Before	導入による効果　After
ネットワーク内部の横感染が検知できない	IoT機器のログで、横感染を迅速に検知
IoT機器のログがなく、分析に時間がかかる	IoT機器のログを利用してインシデント対応工数を効率化
IoT機器からログ出力しても形式が多様で活用が難しい	ITと同じ形式でログ出力し、既存のSOCを活用





IoT機器から収集したログを利用することでインシデント時のSOC対応工数を削減



2．9　研究開発技術の社会実装を促す適合性確認のあり方の研究開発

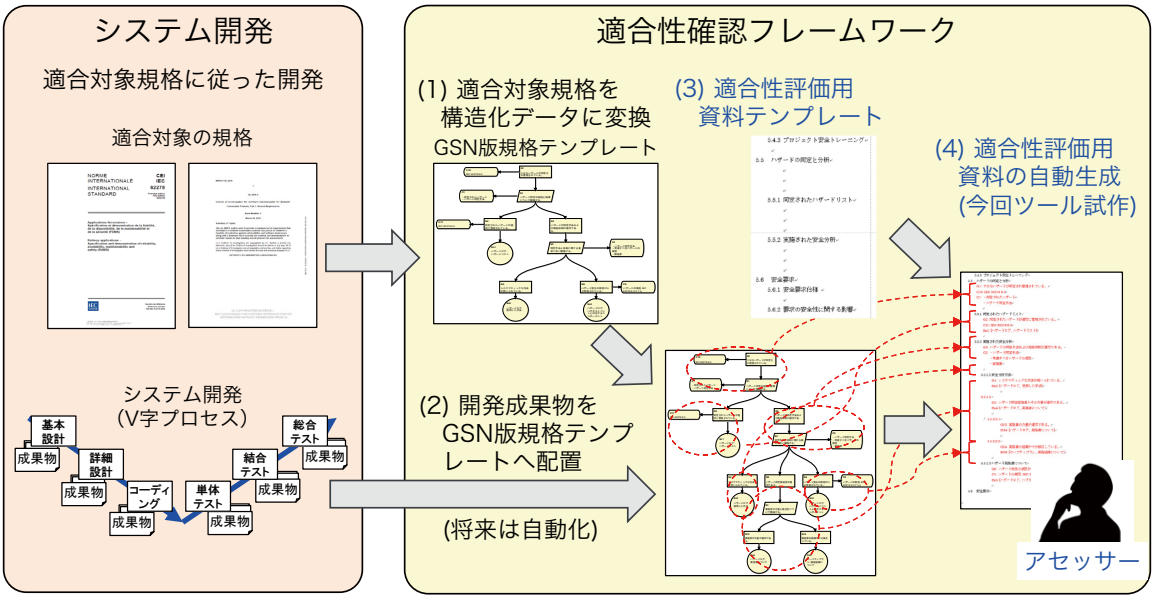
研究の位置付け：
- 開発技術の社会実装に向けた検討→他テーマの研究開発をサポート
- 以下2テーマを実施、現状の適合性確認の比較分析と将来のあり方について提示

1. 重要インフラ等におけるサイバーセキュリティの確保の社会実装に資する、従来になく有効かつ速やかな適合性確認の仕組みの調査、評価
2. 適合性確認に必要となる各種ツールの研究、関連ガイドライン・基準の比較分析、評価

成果（例）：
- ITツール（自然言語処理）によるセキュリティ規程の比較分析の有効性を確認
  - 共通部分、相違部分を効率的に視覚化
  - 規程の改訂や策定に活用可能（例：足りない部分を追加する、等）
  - 効率的な適合性確認に活用可能（例：規程Aに適合した技術を規程Ｂに適合させる場合に両者の相違部分のみを検討する、等）
- 他テーマ開発技術と既存のセキュリティ規程の対応関係をケーススタディとして分析、結果をプロジェクト全体にフィードバック
- 政府統一基準と米国基準の比較、ケーススタディの結果から、政府統一基準への提言を導出
- 適合性確認をミスなく確実に行うための手法の開発
  - セキュリティ バイ デザインの開発手法とゴール指向分析の考えに基づく要求分析手法
  - セキュリティ機能とセーフティ機能の相互の影響を分析する手法
- 標準化の現状調査、ケーススタディによる提案方針の検討

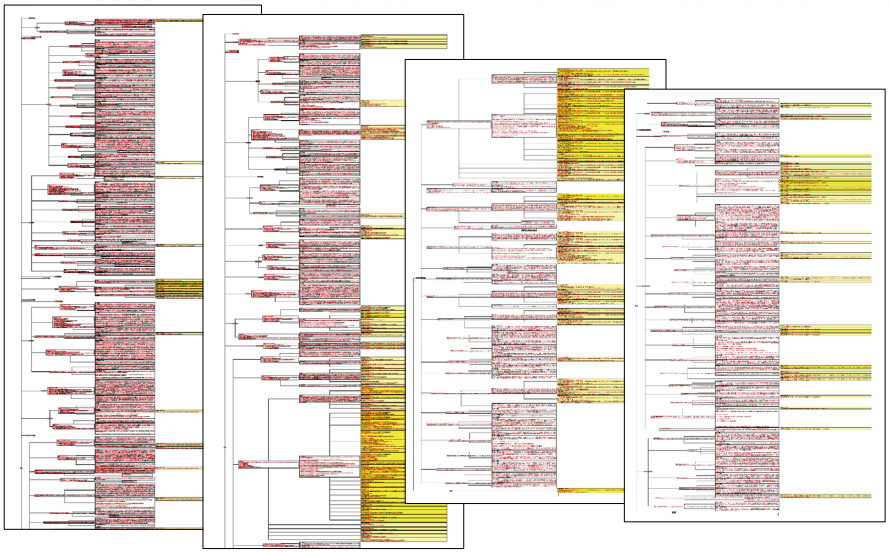
主要成果1:セキュリティに関する規程への適合性確認方法

- セキュリティ バイ デザインの開発手法を使った製品開発過程で、規程準拠確認のための証拠を生成
- ゴール指向分析を基に、規程の要求事項の構造テンプレートを準備
- 証拠とテンプレートの比較によって、製品の規程適合を判断
- 企業内でも活用可能



主要成果2:自然言語処理技術を用いた規程の比較分析手法

- 適合性確認に用いられる主要ガイドラインの比較分析を、自然言語処理技術を活用して、大きく省力化（定量的評価実施）
- ひとつの規程に適合した製品を別の規程にも適合させる場合の効率化に適用可能
- 欧米と日本の規格に手法を適用し、主要成果3の提言も導出



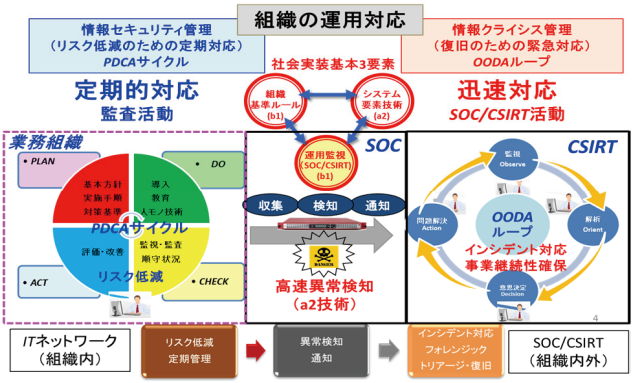
SP800-161とISO/IEC 27036の突合分析

主要成果3:重要インフラ事業への成果普及に向けたケーススタディ

- (a1)真贋性判定技術とSP800-53の対応関係を分析し、プロジェクト内で連携、分析結果を活用
- (a2)動作監視・解析技術に、政府統一基準とSP800-53の比較分析結果（主要成果2）を適用し、政府統一基準で「復旧対応を監視製品/サービスの要件にすべき」との提言を作成
  - 復旧対応を迅速にするためには、CSIRT/SOCを設置し、運用監視し、異常検知通知に対して迅速にOODAループを回し、インシデントの監視と解析、対応方針の意思決定、問題解決を実行することが必要

(a2) 技術の基本機能
NIST SP800-53 管理策
①IR-5：インシデントモニタリング監視・自動データ収集/分析/…
②IR-6：インシデント報告・自動報告/…

(a1)技術と(a2)技術の特長と先進性
・正常なシステム状態を自動学習
・事前登録不要で異常状態を自動検知
・多層防御検知アルゴリズムで対応
（偵察・マルウエア拡散・IT/OT攻撃）
・従来型がリスクコア合計検知方式の反応が遅いのに対し、
(a2)型は個別微細変化検知方式で検知反応が早い



2．10　緊急度の高い脅威情報を迅速に配信し、重要インフラ事業者を防御

本研究開発では、機械処理可能な定型フォーマットを利用することにより、脅威情報の迅速な配信を実現し、重要インフラ事業者のより早い防御を可能とする情報共有システムを開発した。

特長

①　定型フォーマットによる迅速な配信

機械が判断可能な最新の国際標準仕様である定型フォーマット（STIX※1/TAXII※2）を採用し、システムが受信した情報を事業者へ迅速に配信可能。

②　脅威の関連情報や重要度がわかる

システムで蓄積した脅威情報を、関連性分析機能で簡易解析し、関連情報や重要度を見やすく表示。

③　セキュリティ対策の自動化を支援

脅威情報をセキュリティ機器の設定形式である「YARA※3ルール」で出力することで対策の省力化が可能。

④　導入ガイドの提供

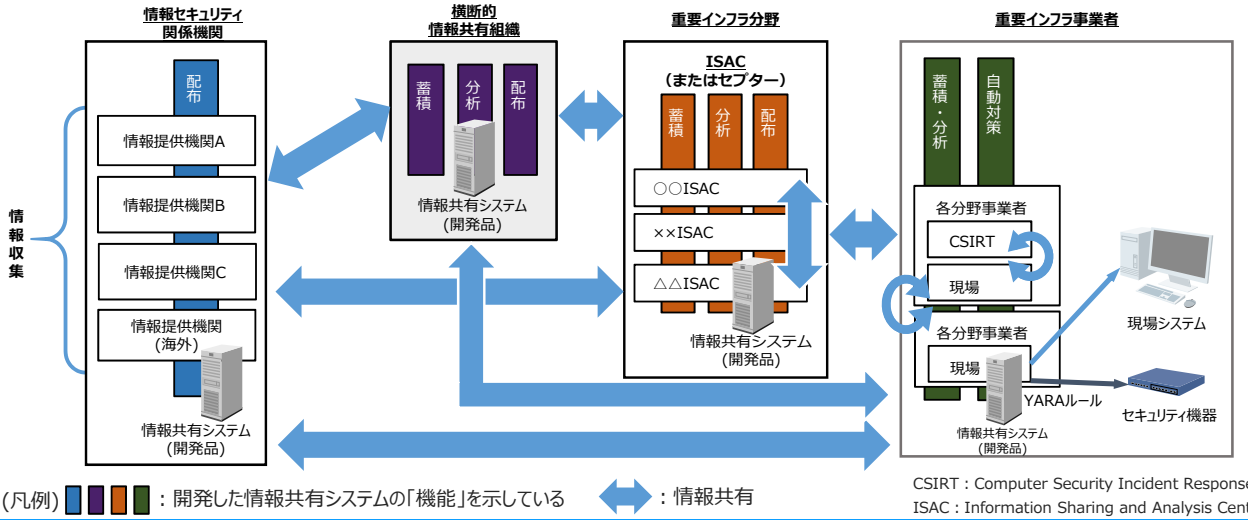
組織の実情に応じた情報共有の構築を助ける補助ツールとしてデザインガイドを用意。

背景と目的

課題	対応
課題① 現状、メールで受信する脅威情報を、人が判断して、転送しているため、時間がかかる。	①定型フォーマットによる迅速な配信により、機械が判断するため、迅速な転送が可能となり、重要インフラ事業者は、早く対策できる。
課題② サイバー攻撃の情報を収集し、事前対策に役立てたいが、情報が多過ぎて、取捨選択に人手が必要。	②脅威の関連情報や重要度がわかることで、自組織に必要な情報の取捨選択が容易となる。
課題③ セキュリティ機器への対策設定に、手間がかかる。	③セキュリティ対策の自動化支援により機器対策の設定の人手と手間が省ける。
課題④ どのように情報共有を始めればよいかわからない。	④組織の実情にあわせた情報共有を補助ツールであるデザインガイドに沿って構築。

適用イメージ

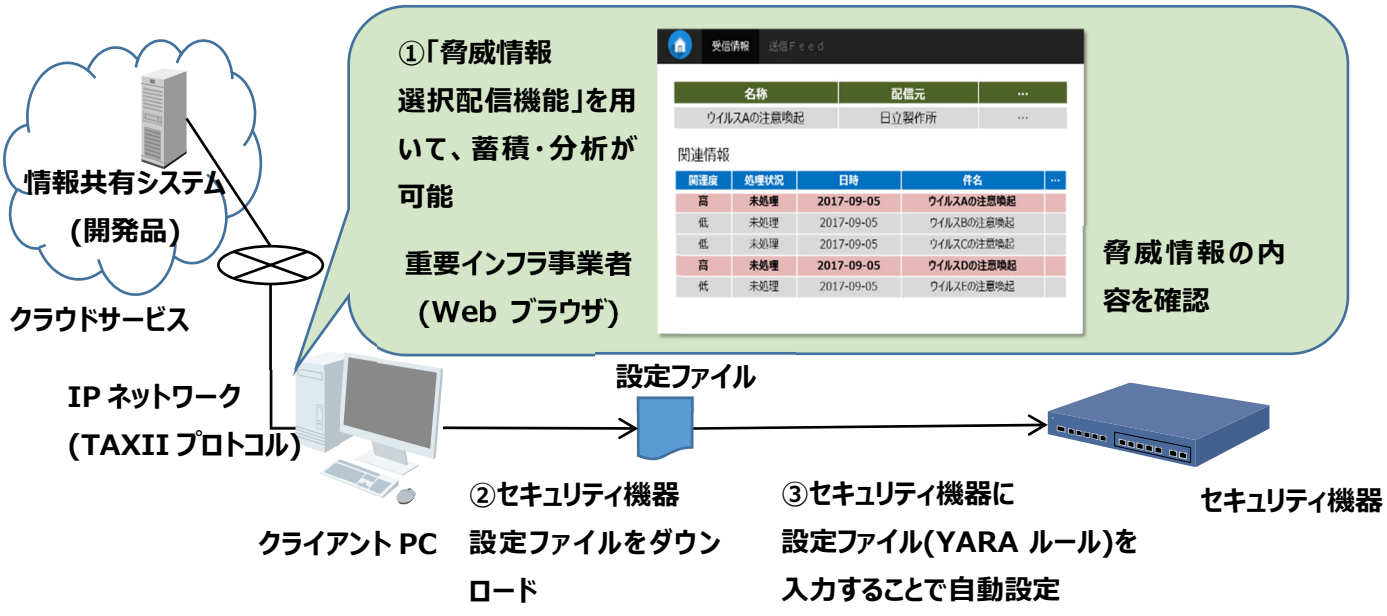
◆情報共有システムを連携して利用する仕掛けを構築することで、脅威情報の入手から配信と対策までをスピードUP。



（※1）Structured Threat Information eXpression（脅威情報構造化記述形式）の略称で、サイバー攻撃情報を表すためのフォーマット仕様。
（※2）Trusted Automated eXchange of Indicator Information（検知指標情報自動交換手順）の略称で、サイバー脅威情報を送受信するプロトコル。
（※3）システムのセキュリティ対策で使われるマルウェア解析・検知用ソフトウェアで、用いられる条件フォーマットセットを示す。

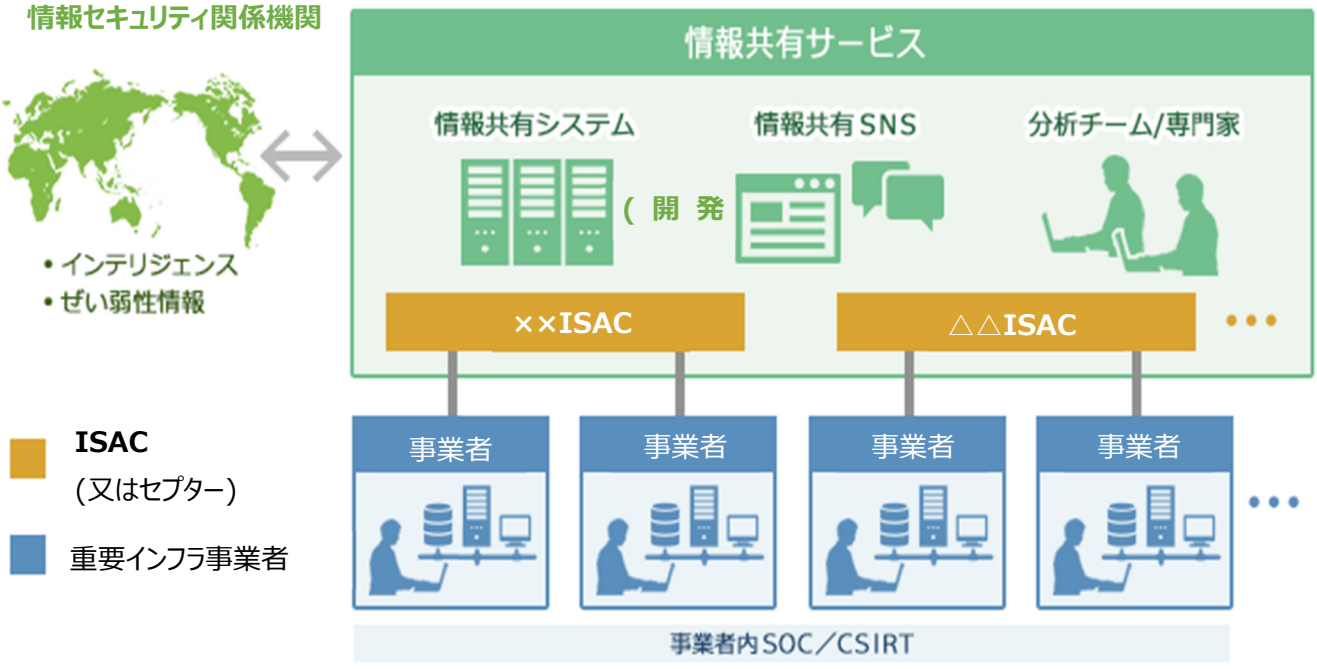
製品イメージ

◆複数のユーザーが、どこからでも情報共有システムを使えるよう、クラウド環境で提供



導入イメージ

◆情報共有システムをコアとして、国内外の情報セキュリティ関係機関から配信される情報を、STIX・TAXII で収集・蓄積し、情報の重要度をランク付け。関連情報を直感的に分かるように仕分けし、グルーピングを施すサービスとして提供。



2．11　重要インフラでの実践力を養うセキュリティ人材育成

【研究開発の目的】

重要インフラ等のオペレーションに従事する技術者に対してセキュリティに関連する知識及びスキルを習得させ、業務においてセキュリティを意識した活動を可能とする人材の育成を目指すため、そのカリキュラムの研究開発を行う。また、その実施のための講義・演習教材の研究開発、それを支援するためのe-learning環境の研究開発、セキュリティ関連コミュニティ機能の研究開発を実施する。

【研究開発の内容】

重要インフラ等のオペレーションに従事する技術者(OT) をターゲット人材とし、業務においてセキュリティを意識した活動を可能とする人材の育成を目標として、（1）セキュリティとは何かを理解できる、（2）定常的にセキュリティを意識できる、（3）対応・対策に貢献できセキュリティ専門家とコミュニケーションできるようになることを目的とする。

これを実現するため、（1）カリキュラムの研究開発、（2）講義・演習教材の研究開発、（3）E-Learning System機能の研究開発、（4）セキュリティ関連コミュニティ機能の研究開発 を実施した。

【研究開発の成果】

開発したカリキュラム及びそれに基づく講義・演習教材として以下の教材を作成した。

1. テキスト・スライドを核とした指導教材

共通の基礎編、電力分野/交通分野を対象とした対策編、対応編についてテキスト、スライドとともに、指導のための参考になる指導要領で構成されている。また、各組織で現場の環境に合わせたカスタマイズをするためのカスタマイズマニュアル、理解度を確認するための演習課題例、IT分野とOT分野で異なる用語等がありこうした差異を吸収するための用語集、具体的な事例によって身近なことであることを理解するための事例集で構成されている。

2. 演習教材

2.1. インシデント体験演習教材

現場で発生するインシデントを体験することにより、インシデントの発生状況を理解するための体験演習教材をe-learning型で開発を行った。現在、ランサムウェア、フィッシング、SQLインジェクション、バックドア、SDカード、ウェブカメラのシナリオが準備されているが、こうしたシナリオを充実するとともに、シナリオを開発するためのマニュアルを整備している。

2.2. シナリオ型演習教材

実際のインシデントが発生した際に、どのように振る舞うべきかを学ぶためのシナリオ型の演習教材の開発を行った。本教材は、通信分野用にカスタマイズされており、実際に通信分野で運用を行っているA社のためのカスタマイズを行い、評価を行っている。また、他の組織でも利用できるようにするための汎用化とカスタマイズ手順マニュアルの整備を行った。

以上の教材を活用するために、ビデオオンデマンド型のe-learningシステムを開発した。本システムは、単にオンデマンドビデオ型の教材を視聴する機能を提供するだけでなく、受講者の視聴状況、課題の出題及び提出、提出状況の管理を行う状況を備えている。また、開発した教材に基づいたコンテンツの作成を行い利用できるようにしている。

さらに、刻々と変化する状況に対応するために教材の更新を進めるためのコミュニティによる教材の更新プロセスの確立を行った。

【実用化事例】

テキスト・スライドを核とした指導教材は、すでに延べ40以上の組織への配布を完了している。また、これらの教材を用いた講座も実施しており、教材等への意見のフィードバックを得るとともに、教材の更新を行っている。インシデント体験演習教材については、15以上の組織で利用されており1万名以上がセキュリティインシデントの体験からセキュリティに対する心構えを学んでいる。

また、本事業で開発された教材を用いて実際に行われた人材育成コース事業が実施されており、実施組織の事業及び配布先の組織において実施された教育プログラムを通して、数百名の人材育成が行われている。こうした事業によってOTの指導者層を含め、組織内においてリーダーを担う人材の育成が実施されている。参加者は、漠然として理解していたセキュリティインシデントに対して具体的なイメージを持ち、心構えを持って現場での対応に携わる準備が整ったとしている。

【本技術の適用範囲・導入条件】

本事業で開発されたカリキュラム及び教材には指導要領を含む指導のための補助的資料が含まれており、導入するだけで人材育成を開始できるように配慮されている。一方、各組織の現場に合わせたカスタマイズを可能とするためのカスタマイズマニュアルを整備しており、個別の環境に合わせた教材とすることも可能となっている。但し、各社の状況に合わせて適用させることが必要であり、今後も支援体制を整えていくとともに、こうした人材育成コースを経た指導者らによるコミュニティでの相互扶助を推進することが必要である。

【今後の展開】

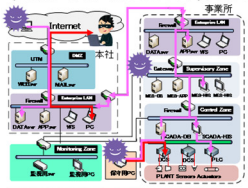
開発された教材を用いて、エクステンションコースなどを通して、人材育成事業を展開していくとともに、刻々と変化する状況に対応させるため、教材を常に更新していく体制を整備していく。教材の更新は、事業を実施した大学が中核となって行うが、本教材を活用している各組織の担当者や教育コース参加者、NISCなどの政府機関、ISACなどの各分野の業界組織、JNSAやCRIC-CSFなどの業界連携組織などと連携し、定常的に更新を行える体制を展開していく。

2．12　組織のインシデント対応能力向上をめざす人材育成プログラム

開発した演習システム IMANE (Incident MANagement Exercise)

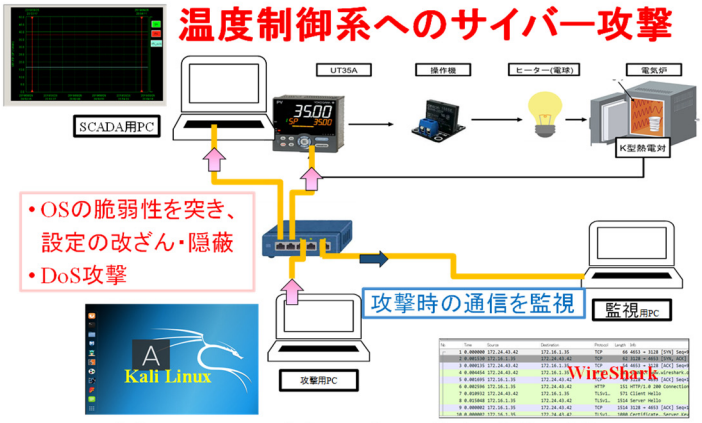
IMANE-DEMO

- 制御系を構築することでその構造を理解
- 構築した制御系をKali Linuxで自分で攻撃
- 攻撃されている状況での通信を監視し、検知できるとした場合の防御について考える



制御ネットワークに侵入できればSCADA, Local Controllerを操作するだけでなく、気づけない攻撃が実現できることおよび通信監視で攻撃が見えることを理解する

温度制御系へのサイバー攻撃



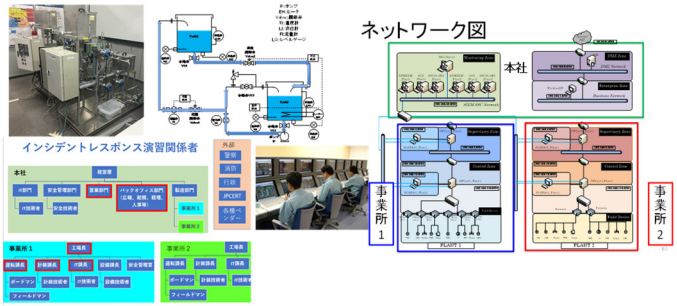
PC3台とコントローラ1台とランプ,HUBだけで実施できる。

IMANE-CARD

① 演習対象のインシデント対応体制の確認

(事業所のシナリオで参加者が役割を理解しているときには不要)

- 守るべきプラントと組織とネットワーク構造の確認



② 演習対象のインシデント対応の流れの確認

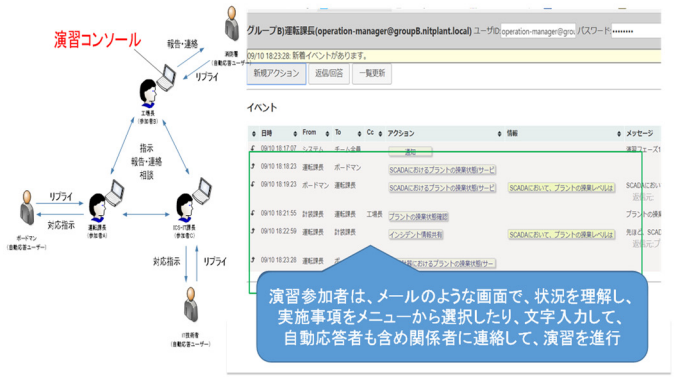
(事業所のシナリオで参加者が役割を理解しているときには不要)

どんな状況で、どんな連携が必要かをカードを並べながら議論する。

カードを正しく配置できるかではなく、カード内容を確認しながら、配置することで、インシデント発生時の状況のイメージを膨らませ、対応を検討する。

IMANE-PC

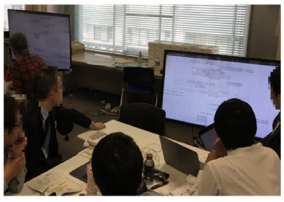
① コンピュータを利用した演習実施



演習実施風景

（直後に振り返り）

（キーボード入力だけで、会話のない静かな演習時）



ヒューマンインターフェイスはシンプルだが、だからこそ、様々な事業所やシナリオに対応しやすく、演習実施頻度を向上させやすい。そして、直後に、具体的な行動をもとにした振り返りが可能となっている。

IMANE サポートツール

IMANE-DRAW	インシデント演習用シナリオを編集し、CARD,PC用データを合成するツール
IMANE-DB	IMANE-PCの実施用データと実施結果のデータを蓄積・検索するデータベース

提案する演習のねらいと特徴

ここで提案している演習は、従来の取り決めた手順を基に、確実な施行をめざす演習とは趣を異にする。

- 対応手順を記憶するのでは、想定外のサイバー攻撃には到底立ち向かうことはできない。
- 従来の安全対策で検討されてきた危険源と悪意に基づくサイバー攻撃がいかに異なるかを理解し、想定外の手口であっても、変化しない共通の特性に着目して、臨機応変に対応できる組織の構築をめざす。
- サイバー攻撃が物理的変化を起こすのは、計装（コントローラ・センサ）を介してしかないということから、コントローラへの危険な指示は監視すべきであることを、演習を通じて気づかせる。
- 想定外が不可避のサイバー攻撃対策には、スーパーマンを求めるよりも、組織としての対応が重要である。
- 異なったシナリオでの組織連携によるインシデント対応を経験し、実行結果を議論するということを繰り返すことで、インシデント対応で共通に求められる組織連携のイメージを獲得させる。
- シナリオを共有し、身近なシナリオにカスタマイズするシナリオ作成環境を整備する。
- 演習結果や振り返りでの議論を共有でき、演習の普及と演習の向上をはかる環境を提供する。

演習のシナリオ作成および振り返りにおける留意点の例

提案した演習では、特にシナリオ作成と振り返りが重要である。重要インフラのサイバーインシデント対応演習のシナリオ作成と振り返りのファシリテーションで重要になる観点を以下に示す。

- 東京オリンピックを標的にするようなサイバー攻撃は、多箇所で同時多重に行われる危険性が高く、物理的変化を検知してからでは遅いという危機感が必要である。
- 安全対策は、多重多層に取られており、全停電させても安全は確保できるはずではあり、SCADAがブラックアウトするというような現象が生じても、大事故が起こるわけではない。
- 多重多層の安全対策も、異常が検知されて初めて稼働するので、隠ぺい工作が行われれば、機能できない。サイバー攻撃では隠ぺいが可能であり、気づけない可能性こそが危険である。
- サイバーテロが隠ぺいを含めた高度な事故の仕掛けを設置するとすれば、コントローラの情報収集が必要で、その後のサイバー兵器の設置までには、制御ネットワークでの通信が発生しているはずである。
- サイバー攻撃と特定するには時間がかかり、その間に感染や侵入は広がってしまう危険性が高い。
- 疑わしい通信検知の段階で対応するには、通信が遮断された状態での自動システムをあてにしない操業が必要。
- いつ、どこを遮断したら、被害を局在化し、早期復旧が図れるか？通信遮断をするためにどんな検知が必要か、遮断後の対応操作は？という議論を、通信系の監視、遮断後の解析はITが中心、通信遮断後の操業対応はOTが中心で協議すべき。
- サイバー攻撃が物理的変化を起こせば、センサ以外にも、現場の表示計器など、サイバー攻撃では隠ぺいしきれない検知手段があるはずである。現場パトロールや他部署でインシデントが検知される可能性を考慮すべきである。
- 重要インフラの場合、サービスの継続が重要であるので、安全が確保できても、サービス停止の範囲が広く、復旧までに時間がかかると、重大インシデントとなる。サービス停止の危険源は、事業所内にとどまらず、サプライチェーン全体に存在し、管理の弱いところが狙われる。
- サイバー攻撃は多重に仕掛けられている可能性があり、もし、機能が復旧できたとしても、危険源がまだ潜んでいる可能性がある。復旧も完全復旧だけでない段階的な判断が必要かもしれない。
- 異常が隠ぺいされ、正常でないサービスあるいは製品が外部に提供されてしまうと、現場は安全でも、重大事故となり、経済的にもコンプライアンスとしても大きな被害になることを意識すべきである。
- 特に、保守・保全の管理は重要。検査も所定の機能が実現できていることのチェックでは不十分で、所定の機能以外のことが発生しないこともチェック対象となるが、部品の回路として入り込む危険性まで考慮すると、守り切れないという前提での対策も必要。

3. 研究開発テーマ詳細

3．1　サーバー機器の改変を常時検知して重要インフラを保護

（a1）制御・通信機器のセキュリティ確認技術
委託先：日本電信電話株式会社
再委託先（共同実施先）：エヌティティエレクトロニクス株式会社、株式会社ＦＦＲＩ

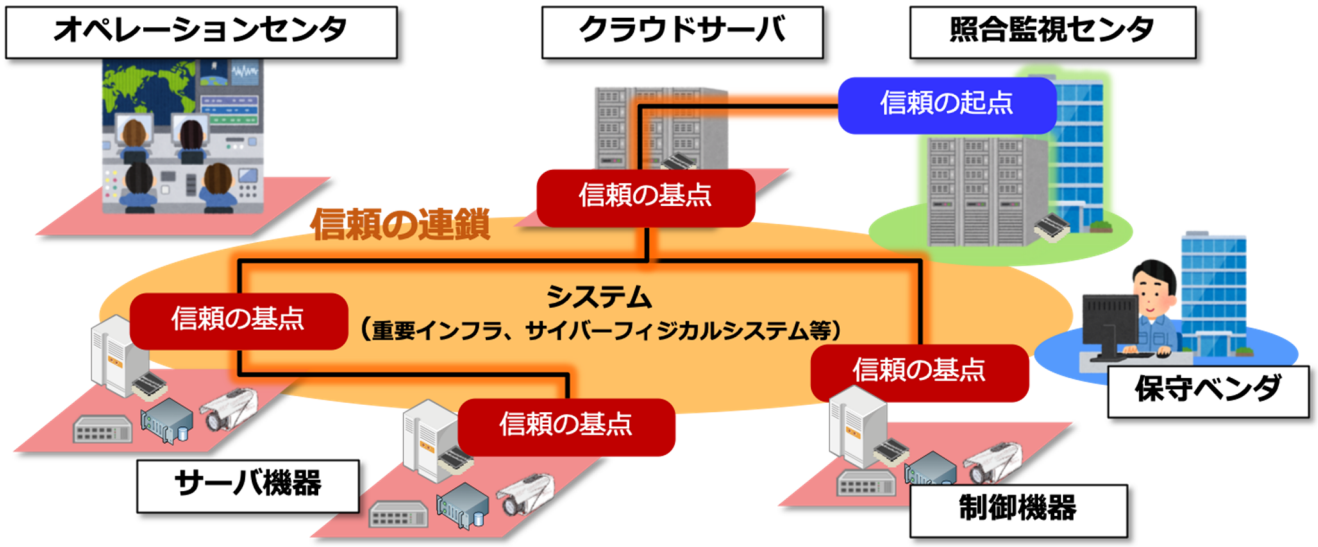
【研究開発の目的・内容】

重要インフラ等のサービスを支える設備やネットワークは、個別製品や要素技術のみならず個々の機能を組み合わせて一つの統合体として機能していることから、システム全体でのセキュリティ確認が重要となる。本研究開発におけるセキュリティ確認とは真正性確認すなわち「制御・通信機器自体がなりすまされておらず正しいものであることの確認」、及び完全性確認すなわち「制御・通信機器で動作しているソフトウェア等が改ざんされていないことの確認」である。

本研究開発は、システム全体に対するセキュリティ確認について、情報・制御ネットワークにおける信頼の基点を設定・駆使するアプローチにより研究開発に取り組み、重要インフラを構成するサーバ機器のシステム出荷・導入時に加えて運用時においても当該機器のセキュリティ確認（真正性確認・完全性確認）を効果的かつ効率的に行うことを可能にする技術（真贋判定技術）の確立を目的とするものである。

本研究開発事業では、このような認識の下、重要インフラシステムを構成するサーバ機器の真贋（機器内のソフトウェアの完全性）を厳密に判定可能な技術である「真贋判定技術」を確立した。真贋判定技術では、独自機構である「信頼の連鎖」を活用して、重要インフラシステムのように多数のサーバ機器によって構成される大規模システムであっても、各サーバ機器の起動から運用を含むライフサイクル全体にわたって完全性の厳密かつ効率的な確認を可能にする。

真贋判定技術では、各サーバ機器内部に「信頼の基点」を設け、「信頼の基点」がつながり合うことによって「信頼の連鎖」を形成する。各サーバ機器の「信頼の基点」は耐タンパー性を備えた本技術の基本要素であり、本技術がサイバー攻撃に対して高い耐性を備えるための必須要素である。

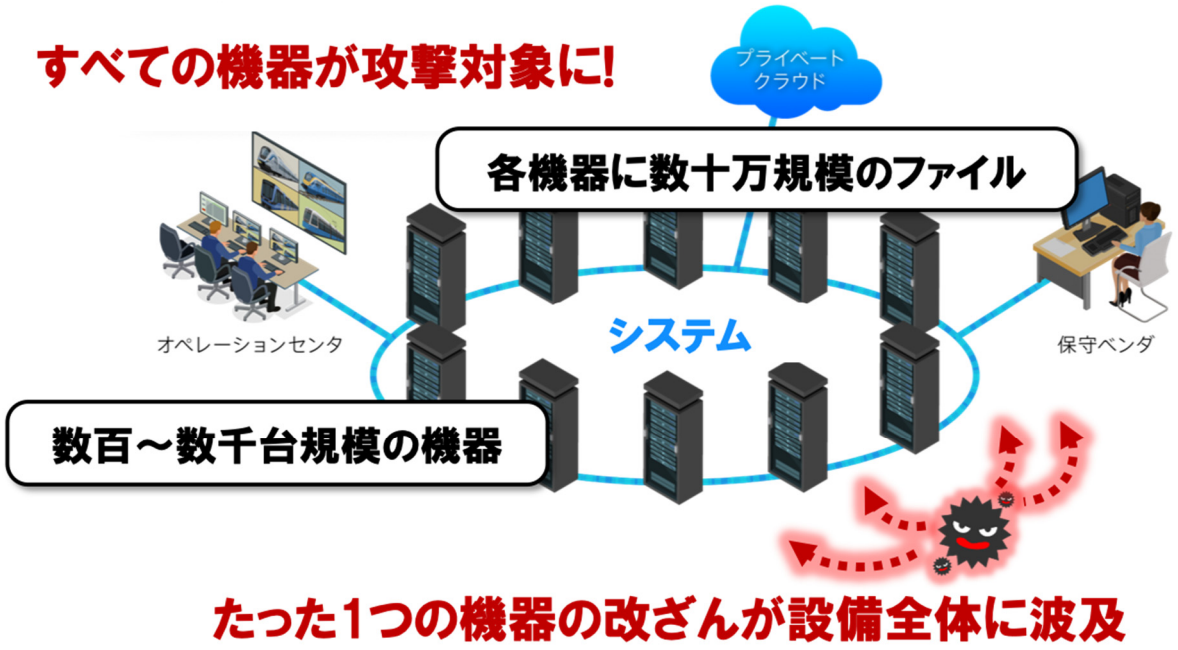


【研究開発の成果】

背景

重要インフラシステムは数百から数千台規模のサーバ機器によって構成され、各サーバ機器には少なくとも数十万規模のファイル（ソフトウェア、データ等）が存在している。このような膨大なサーバ機器及び

ファイルがすべて攻撃の対象となるとともに、一つの改ざんがシステム全体の改ざんへと波及し得る。また、汎用ハード及び汎用ソフトウェアの採用が進み、サイバー攻撃に必要となる事前情報も得やすいことから改ざんの脅威が現実化している。

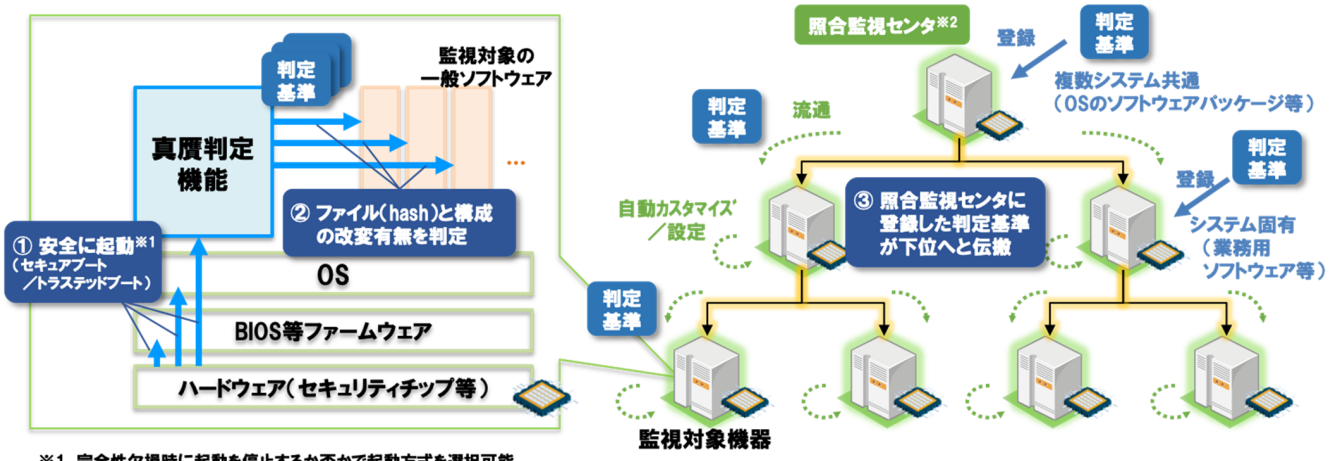


重要インフラ設備を構成する機器の複雑化・高度化が進み、その導入のサプライチェーンにはさまざまなプレイヤが関わる。各プレイヤの作業環境が汚染されることによってマルウェア感染する可能性、作業担当者による内部不正の可能性など、さまざまな改ざん要因が考えられ、これらを完全に回避することは困難である。重要インフラ設備の構成機器に対する改ざんの発生は、社会に対して回復困難な事態をもたらす可能性がある。2020年東京オリンピック・パラリンピック競技大会開催時に向けても、国内重要インフラにおけるこのようなリスクはさらに高まるおそれがありその対策は喫緊の課題であることから、改ざんの発生を前提としつつ、その事実の迅速な検知と対処が重要になっている。

真贋判定技術の動作概要

真贋判定を行うためには、事前に監視対象（真贋判定の対象）となるサーバ機器に「真贋判定機能（ソフトウェア）」を導入する。監視対象となるサーバ機器の電源投入から真贋判定機能が起動までは、セキュアブート・トラストテッドブートを利用して完全性が保たれていることを確認した上で行われる。その後、真贋判定機能が、OS上で動作するソフトウェアや用いられるデータの完全性を常時監視する。

監視にあたっては、各ソフトウェアを構成するファイル及びファイル構成の完全性を確認する。また、完全性の確認に用いる基準（判定基準）は「信頼の連鎖」を通じて共有され、「照合監視センタ」が基準共有の起点となる。また、各監視対象機器に適合させる自動調整を含め、すべての処理が「信頼の連鎖」及び「信頼の基点」を利用して安全に行われる。簡易対象のファルについて完全性が損なわれていることが検知された場合、真贋判定機能は監視担当者に対して改ざん事実の通知を行うとともに、必要に応じて当該ファイルの利用を即時停止することができる。



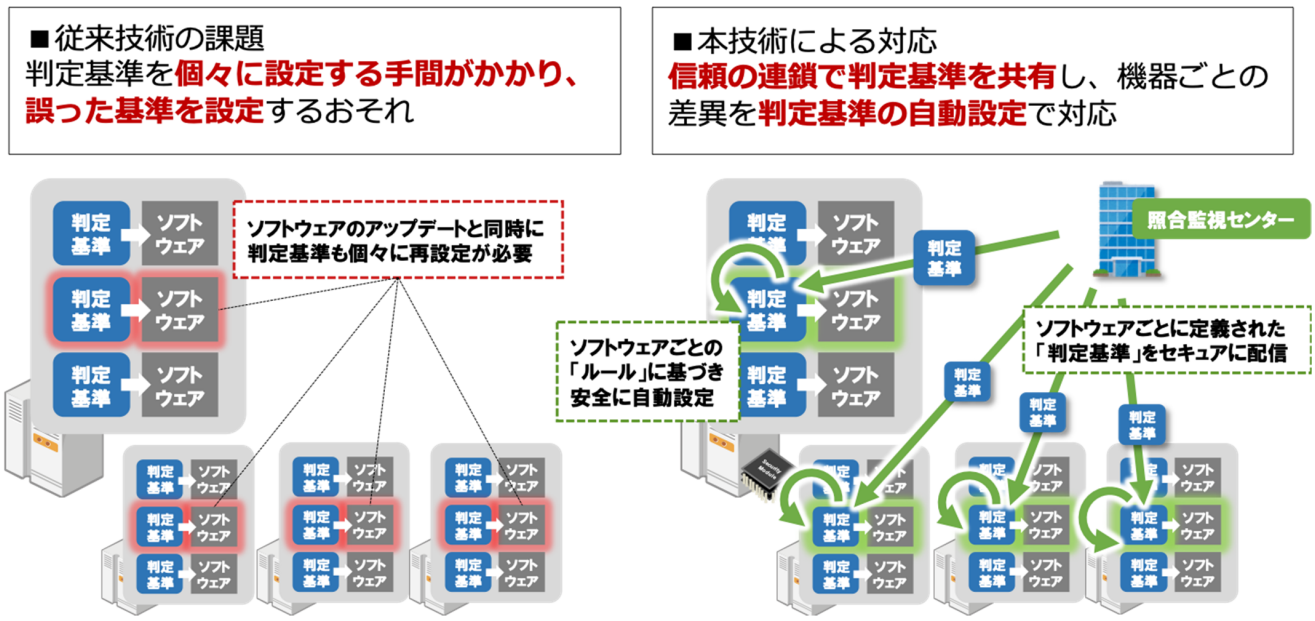
※1 完全性欠損時に起動を停止するか否かで起動方式を選択可能

※2 スケーラビリティを確保した真贋判定を実現するため、複数システム共通の判定基準の登録・配布元となり信頼の連鎖の起点となる機器

特長①：大規模システムにおける安全なアップデートの実現

真贋判定技術では、判定基準の安全かつ効率的な共有と適用を「信頼の連鎖」と「自動設定」によって行い、大規模システムの安全なアップデートを実現している。監視対象となるサーバ機器において判定基準を個々に設定する場合、サーバ機器の増大とともに作業コストも増大し、作業の煩雑化によって誤った判定基準を設定するおそれもある。

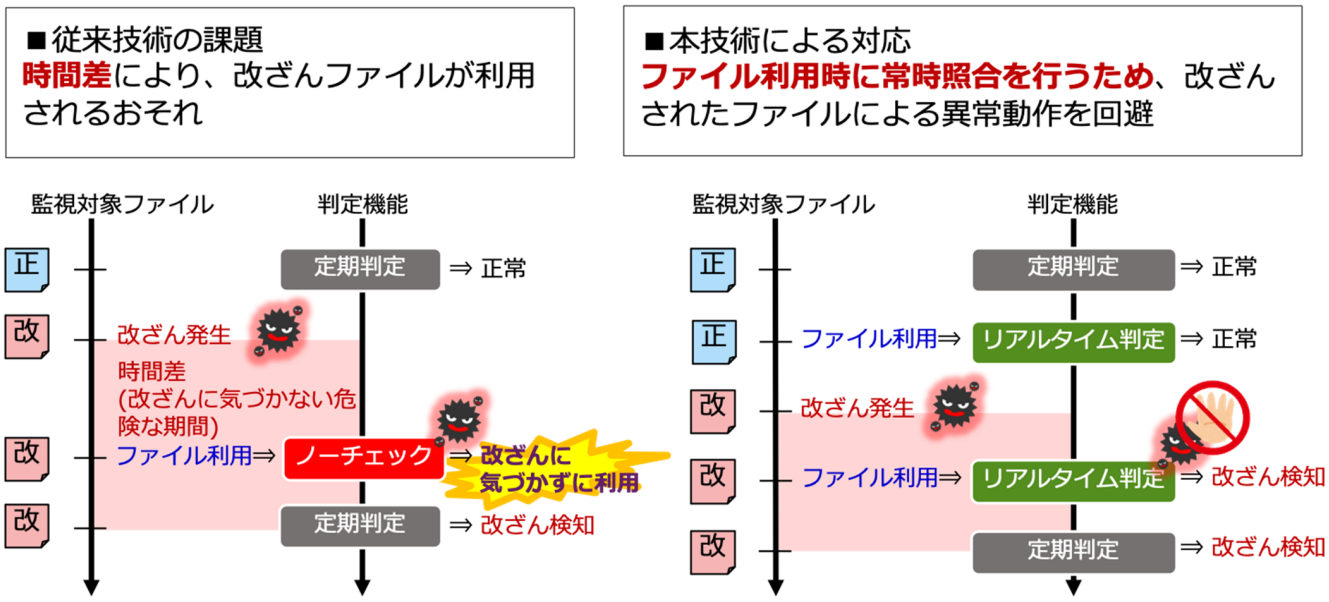
真贋判定技術では、「信頼の連鎖」を通じて判定基準を安全に共有し、監視対象となるサーバ機器に適合するよう判定基準の自動調整を行うため、大規模システムにおいても安全性を犠牲にすることなく効率的に完全性を確認することができる。特に、脆弱性の修正等、ソフトウェアのアップデートに対する機会と重要性が増す中、大規模システムの安全なアップデートの実現は本技術が保守運用業務に対してもたらす大きなメリットである。



特長②：完全性の常時検知

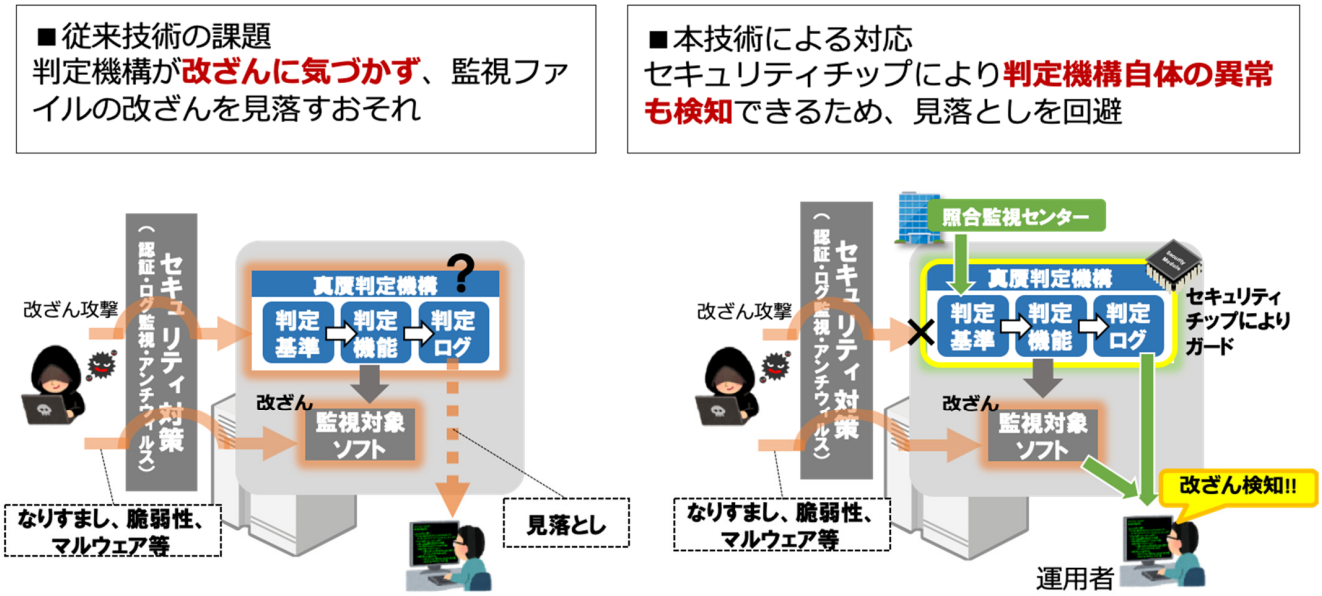
従来、完全性の判定は定期実行によって行われる場合が多い。この場合、改ざんの発生タイミングと定期実行タイミングの時間差が、改ざんされたファイルが利用されうる期間となり、改ざんの影響発生を阻止することができない。

真贋判定技術では、監視対象ファイルの利用契機において完全性の確認を常に行い、完全性が損なわれている場合には当該ファイルの利用を停止する。効率的な判定機構を実現することによって、本来機能に対する影響（リソース利用率）は一般的なサーバ機器において十分に許容できるレベルを実現している。



特長③：高い攻撃耐性を備えた強固な判定機構

高度なサイバー攻撃では、セキュリティ機能自体を無効化した上で、攻撃動作を行う可能性がある。完全性の確認においても、完全性を判定する機構自体、判定に用いる基準、判定の結果のいずれかの要素が改ざんされれば、改ざんに気づくことが不可能になる。そこで、真贋判定技術では、監視対象サーバ機器においてOS管理者権限がたとえ奪取されることも想定した判定機構を備えている。真贋判定機能自体が改ざんされた場合には、その事実を確実に検知することができる。



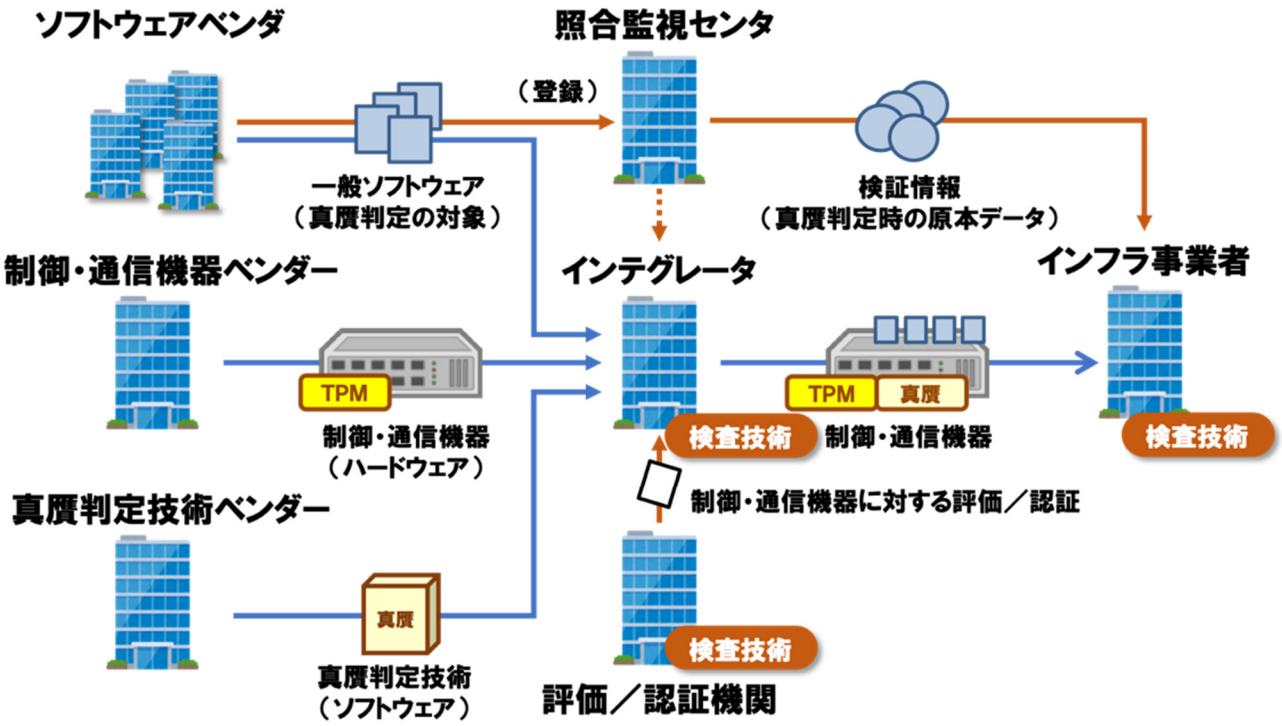
特長④：機能検査技術

重要インフラ設備を構成する機器導入のサプライチェーンにはさまざまなプレイヤが関わる。そこで、真贋判定技術を機器ベンダーが製造する機器（ハードウェア）に対して導入することによって、その後は当該機器に導入されるソフトウェアの完全性を判定することが可能になり、不正なソフトウェアの混入を検知・阻止することができる。

しかしながら、そのためには真贋判定技術が機器に正しく導入され動作可能であることが求められることから、本研究開発では、簡易な操作によって検査を自動実行可能であり、真贋判定技術を機器に導入するプレイヤ（インテグレータ）が「真贋判定技術を正しく導入できたこと」を容易に検査することを可能にする機能検査技術を確立した。さらに、当該機器を調達して重要インフラ設備に導入するプレイヤ（インフラ事業者）が、本実施項目の検査技術によって「調達した機器に搭載された真贋判定技術の正しさ」を検査することも可能とした。

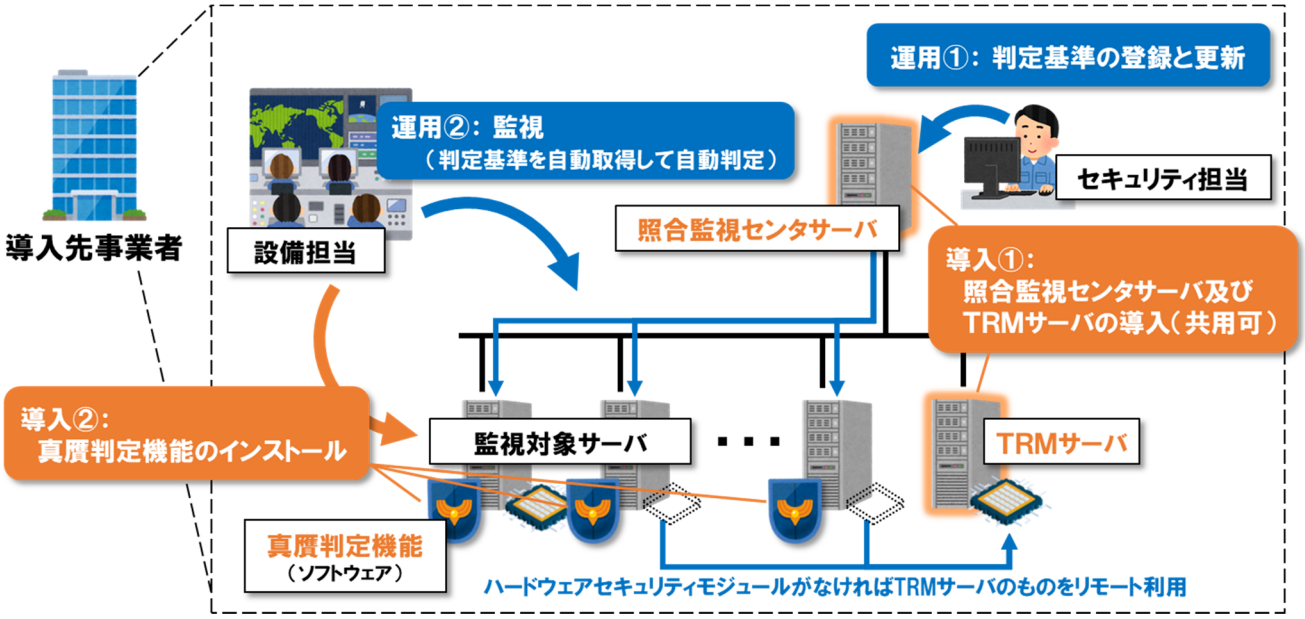
将来的には、真贋判定技術の導入を認証する制度が社会実装された場合に、当該認証制度に基づき第三者評価を行うプレイヤ（評価／認証機関）が、本実施項目の検査技術を使用して「真贋判定技術が正しく機器に導入され、かつ動作可能であること」を検査することもできる。

このように、本実施項目による検査技術は、サプライチェーン上の各プレイヤが活用することによって、機器のサプライチェーンにおける改ざんリスクの低減に寄与することが可能となる。



【実用化事例】

以下の構成図は、真贋判定技術の典型的な導入例である。判定基準を登録・配付する「照合監視センタサーバ」を導入した上で、真贋判定の対象とするサーバ機器に「真贋判定機能」をインストールする。

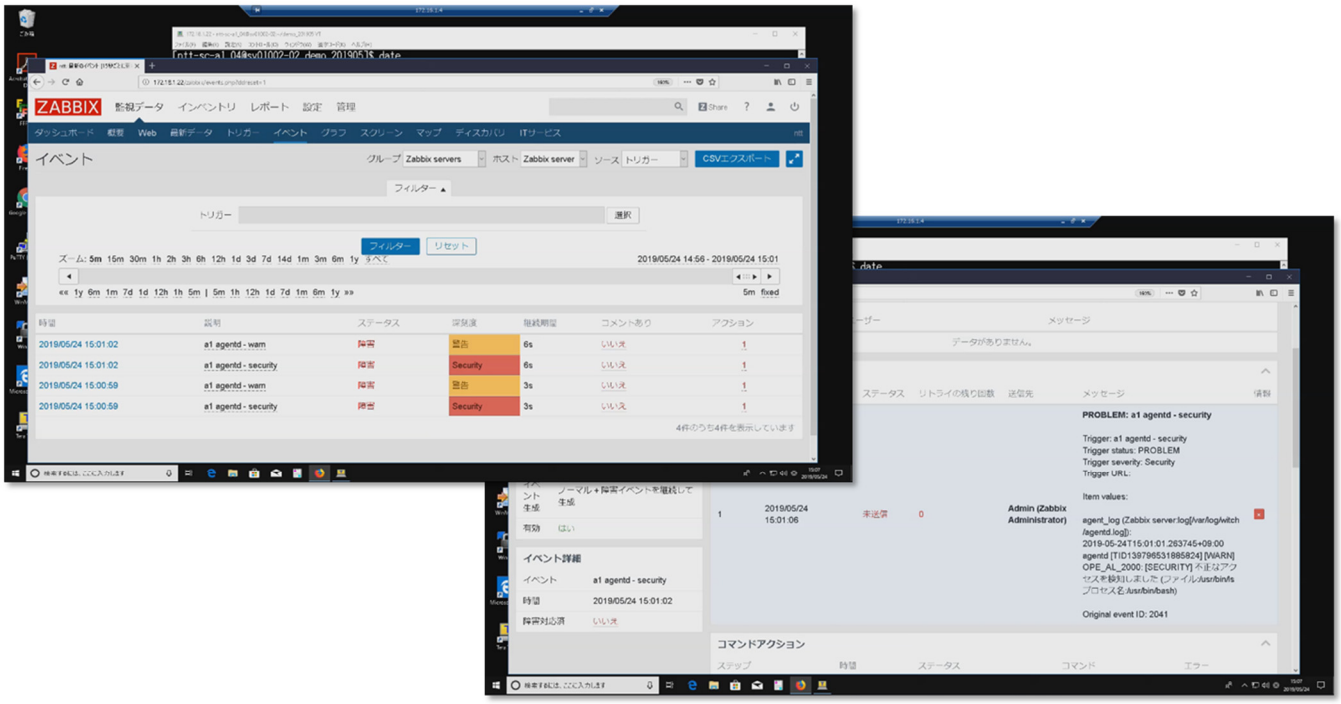


真贋判定技術では、強固なサイバー攻撃耐性を備えるためハードウェセキュリティモジュールを活用して「信頼の基点」を構成する。そのため、真贋判定の対象機器にハードウェアセキュリティモジュールが搭載されていることが望ましい。

ハードウェアハードウェアセキュリティモジュールを搭載していないサーバ機器においても真贋判定技術による監視を行うことは可能である。このような場合に対応するため、真贋判定技術は「TRMサーバ」と呼ぶ機能を備えている。TRMサーバはハードウェアセキュリティモジュールを搭載するサーバ機器であり、

ハードウェアハードウェアセキュリティモジュールを搭載していないサーバ機器に対して「信頼の基点」をネットワーク経由により遠隔利用可能にし、上記の導入条件を緩和することができる。

なお、真贋判定技術による監視結果は専用のログ出力の他に、一般的な監視ソフトウェアに集約して取り扱うことが可能な形式でも出力可能である。以下の図は、このようにして監視結果を集約して監視を行う画面の例である。



【本技術の適用範囲・導入条件】

真贋判定技術の適用範囲は、主に重要インフラ設備や一般的な情報システムを構成するサーバ機器である。現在、利用可能な実装では、OSとしてRedHat Linux、ハードウェアセキュリティモジュールとしてTPM2.0が条件となる。監視対象とするサーバ機器にハードウェアセキュリティモジュールが搭載されていない場合でも、前述した構成によって導入可能である。

【今後の展開】

本技術は、導入可能なソフトウェア実装が既に完成しており、重要インフラ設備において技術実証を完了した上で、2018年度には商用導入も達成している。今後、2020年度には重要インフラ分野におけるさらなる導入拡大、及び法人システムにおけるサーバ機器に対する導入拡大を図っていく計画である。

【お問い合わせ先】

日本電信電話株式会社　NTTセキュアプラットフォーム研究所
E-mail: scpflab@hco.ntt.co.jp

3．2　内在する脅威の早期顕在化にて業務影響を最小化

（a2）制御・通信機器および制御ネットワークの動作監視・解析技術

①情報・制御ネットワーク構成機器のログ・トラフィック分析による健全性確認技術

委託先：富士通株式会社

再委託先（共同実施先）：大学共同利用機関法人国立情報学研究所

【研究開発の目的】

攻撃手口の巧妙化と共に重要なインフラに対する様々なサイバー攻撃が発生する中で、図3-2-1に示す通り、これまでのネットワーク境界での通信監視による脅威情報とのマッチングによる入口／出口対策や情報機器上でのエンドポイント対策では防ぎきれず、すり抜けて組織のネットワークに侵入することを前提として、組織の内部ネットワークで活動する脅威を検知して、推奨される対処の提示、影響調査範囲の抽出により、業務影響の最小化を目指した。

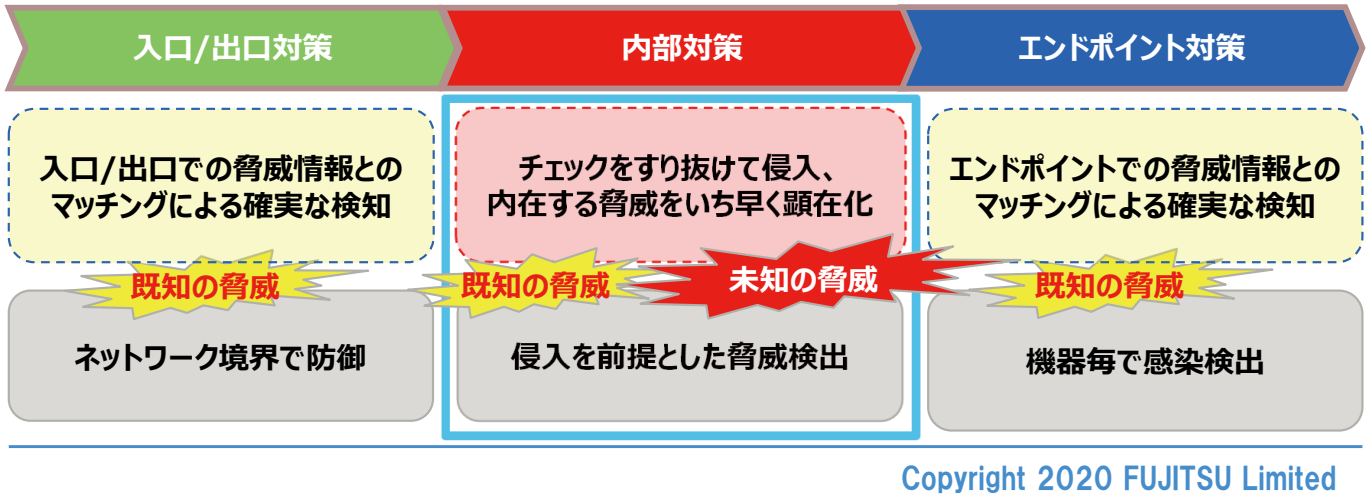


図 3-2-1　侵入を前提とした内部対策

潜在脅威に対する監視・対処は図3-2-2に示す階層のレベル2～3に対応するSOC（Security Operation Center）およびCSIRT（Computer Security Incident Response Team）の活動である。セキュリティ人材不足や業務輻輳が課題となっている本階層に対して、潜在脅威の抽出・推奨対策の提示・影響調査範囲の抽出業務をシステムにて支援することで社会的課題解決を図っている。

脅威検知レベル（定義）		対策判断者	対策の観点
Level-5	業務サービスの異常検知	事業責任者 経営者	事業継続 （BCP）
Level-4	業務システム全体の健全性阻害の検知	リスク委員会 （CISO）	システムの健全化
Level-3	内部ネットワークにおける異常拡散（侵入深化）の検知（ex. C&Cの対策）	CSIRT	システムの安定化
Level-2	外部ネットワークとの異常通信（C&Cサーバー通信）の検知（ex. C&Cの存在、情報漏洩）	セキュリティエキスパート（SOC）	影響範囲の特定
Level-1	内部ネットワークにおける通信変化を検知 （ex. C&C通信の可能性と対象領域）	ネットワークオペレータ（NOC）	被害の特定・除去
Level-0	外部ネットワークからのセキュリティ脅威の通知 （ex.アタック発生）	ツール（機器）	被害の特定・除去

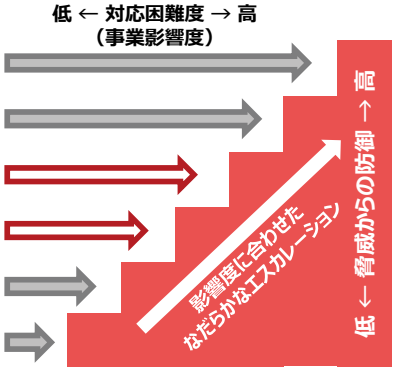


図 3-2-2　脅威検知階層レベル

【研究開発の内容】

高速・大容量、新旧多種多様な情報機器・通信機器、情報機器／通信機器の仮想化の進展を特徴とする重要インフラの通信情報基盤において、最小限の監視機器の導入にて通信パケットをモニター・分析する手法が不可欠であり、これを「収集」、「蓄積」、「分析」、「制御」の４つの技術で実現している。

- システムならびにネットワークの仮想化に対応した高性能な**通信パケット収集技術**による仮想空間における通信の可視化技術
- 大容量通信パケットの蓄積、検索を低コスト、高スケーラビリティにて実現する上での汎用サーバーを並列利用する**高速パケット蓄積・検索技術**

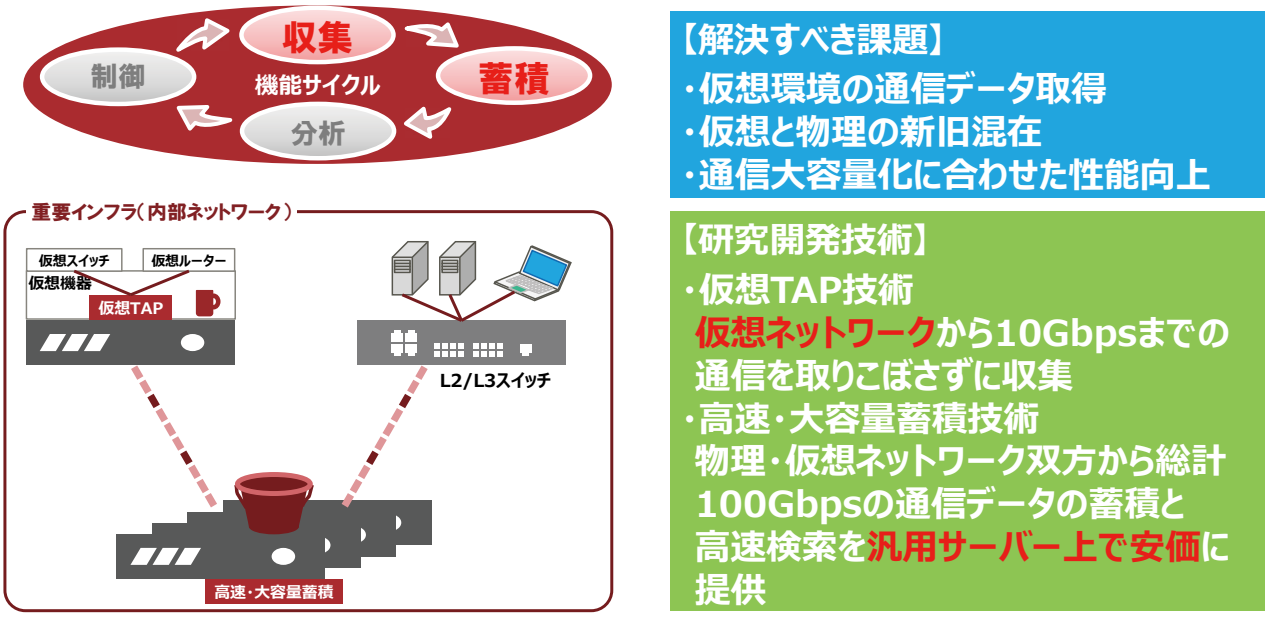


図 3-2-3　収集・蓄積技術

新旧機器、仮想／物理が混在する大規模ネットワークにおいて、ネットワーク環境に依存しないセキュリティ対策を実現するため、異なるネットワーク環境の各監視ポイントからの通信パケットをTAP形式にて収集し、蓄積サーバーへの転送することで、一極集約での蓄積が可能となり、各監視ポイントでのトラフィック蓄積・分析と比較して安価でかつネットワーク全体での俯瞰的な分析を実現した。

セキュリティインシデント発生時の適切な事後対応として、「原因の特定」、「被害範囲(漏洩情報) の特定」、「再発防止の徹底」が求められるが、セキュリティ装置やフォレンジック製品のログだけではこれらの事後対応に必要となるマルウェアの検体、C&Cサーバーのコマンド内容、窃取されたデータの把握・特定には多大な時間が必要となる。本技術により蓄積された大量の通信データから不審な通信のパケット内容を確認することで事後対応の時間短縮化を実現した。このような原因・被害範囲の特定などの証跡としてパケットデータの蓄積は重要であるが、専用蓄積装置では高性能CPUや記憶媒体としてSSD (Solid State Drive) を適用して高速化を実現しており、大容量の通信トラフィック蓄積では設備コストが非常に高価となる課題に対して、取りこぼしなく、通信トラフィックの拡大に合わせたスケーラブル性のある高速・大容量蓄積を汎用サーバーの性能を最大限活用することで、安価に実現している。

- 通信の規則性や送受信の関係性に着目し、通信データ全体を正常とみなし、それらの特徴量と乖離を判断する群挙動モデル**解析技術**により、正常通信の中に紛れた不審な通信を抽出する技術
- セキュリティ脅威検出時においても重要インフラサービス・業務の安定継続は最重要事項として位置付け、緊急度と業務重要度に対する対処リコメンド**制御技術**

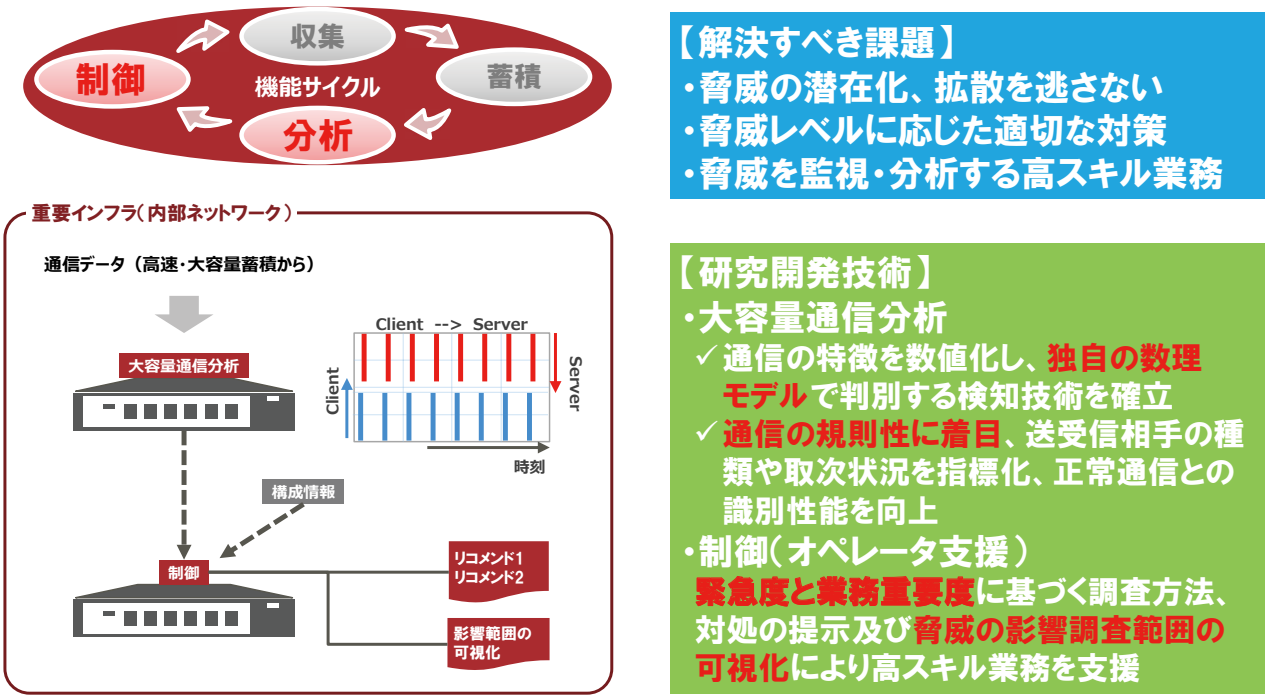


図 3-2-4　分析・制御技術

攻撃シナリオやAI技術を活用した最新の脅威検知技術は、長期にわたる通信を攻撃手口と関連付けて解析することで、これらの見逃しを削減している。しかしながら、さまざまな形態で利用される高速・大容量の通信基盤においては、関連付けのための中間データが膨大となり、これらの技術をそのまま適用することが困難であることからデータ量を抑制できる独自の数理モデルでの検知技術を確立した。検知した通信が不審通信であった場合　脅威拡散状況を調査する上では、蓄積された大量の通信データから通信の相関関係ならびに通信の特徴情報から影響範囲の絞り込みが容易となり、事後対応の時間短縮化を図ることができる。

【研究開発の成果】

本技術による成果は、（1）高性能な仮想化モニターによって、仮想ネットワークの10Gbpsまでの通信を取りこぼさず収集することが可能である。また、（2）安価でスケーラブルな高速・大容量蓄積によって、物理仮想ネットワーク双方から総計100Gbpsの通信パケットを14日分の蓄積が可能となっている。更に、（3）大量通信を俯瞰的に解析する群挙動モデル解析によって、20Gbps高速大容量の通信環境において不審な通信の検知に成功した。これに加え、（4）緊急度と業務重要度に対応する対処リコメンドと脅威の影響調査範囲可視化によって、内在する脅威の早期顕在化を実現し、オペレータ稼働の一部軽減が可能となった。

表 3-2-1　研究開発の成果

研究開発技術	成果
仮想通信パケット収集	10Gbpsまでの通信を取りこぼさず収集
高速・大容量通信パケット蓄積	物理仮想ネットワーク双方から総計100Gbpsの通信パケットを14日分蓄積
大容量通信分析	20Gbps高速大容量の通信環境において不審な通信を検知
対処リコメンド（オペレータ稼働軽減）	内在する脅威の早期顕在化によりオペレータ稼働の一部軽減

【実用化事例】

ICT技術革新とともに付加サービスとして、運転状況通知や予約サービス等の多種多様なサービスをインターネット経由で利用者への提供が不可欠となっている。このニーズに対応するために重要インフラ事業者の業務用ネットワークは限定的にインターネットに接続されており、完全な閉域環境とは成りえず、利用者への提供サービス拡充とともにセキュリティ対策の高度化、多層化が重要となってくることから製品提供形態での実用化を進めている。

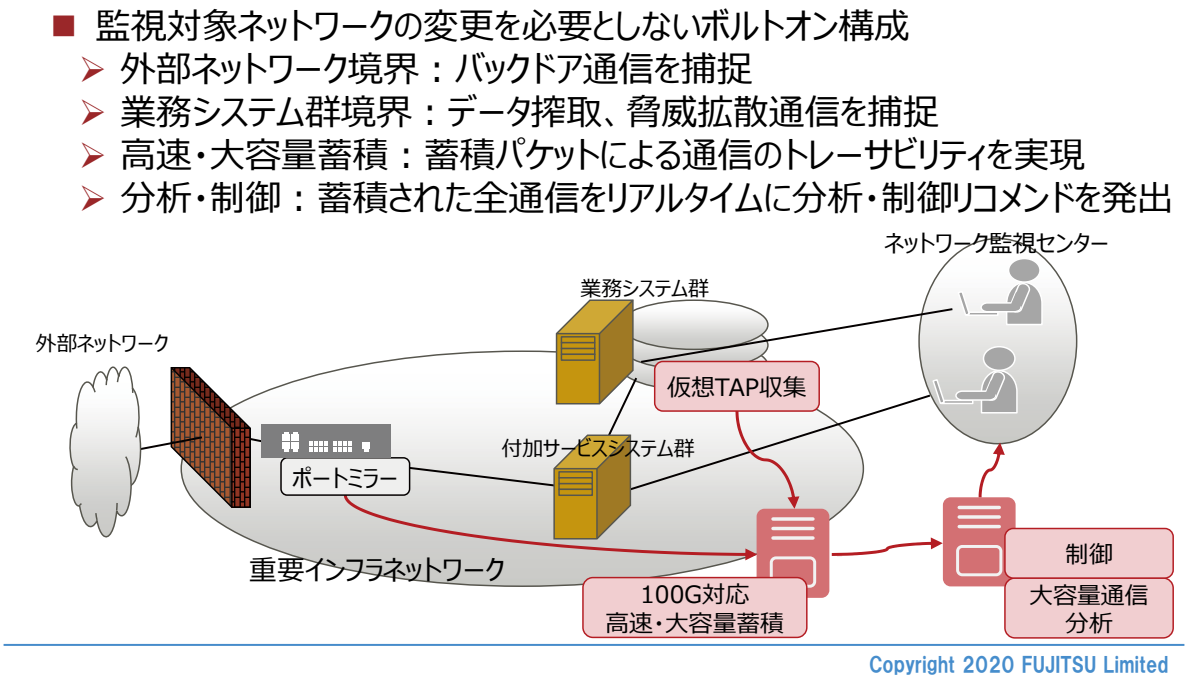


図 3-2-5　適用イメージ

【本技術の適用範囲・導入条件】

- 汎用サーバーをプラットフォームとするソフトウェアで構成
- インターネットあるいは外部ネットワークとの境界を監視収集ポイントに設定すること
- セグメント毎に監視収集ポイントを設定することでインシデントの事後対応時間が短縮可能
- 収集したパケットをネットワーク上で蓄積サーバーに転送する上で、転送通信量に沿ったネットワーク帯域設計が必要

【今後の展開】

- 「収集」、「蓄積」技術：製品化済「分析」、「制御」技術：2020年度製品化予定
- 通信事業者、電力事業者等の重要インフラ事業者向けに「収集」、「蓄積」、「分析」、「制御」の技術セットで製品展開
- 「収集」、「蓄積」、「分析」、「制御」技術をドッカー・コンテナ技術で、様々な製品に折込んだ形での商材化により、一般企業向けに展開

【お問い合わせ先】

富士通株式会社　ネットワークソリューション事業本部
044-280-9861　fj-ci-procontact@dl.jp.fujitsu.com

3.3　モニタリング機器の追加でIoTセキュリティ監視を提供

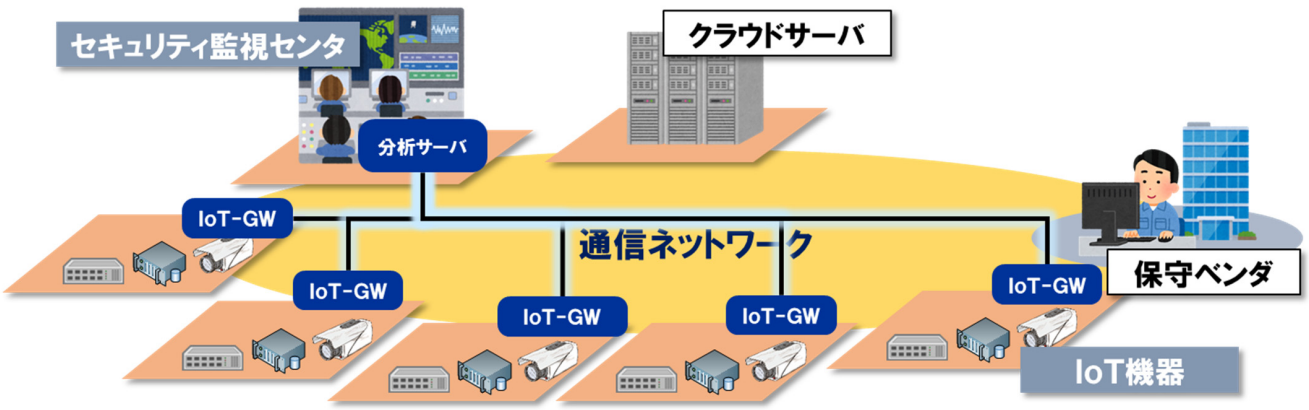
（a2）　制御・通信機器および制御ネットワークの動作監視・解析技術
　②　IoT機器のログ・トラフィック分析による健全性確認技術
　委託先：三菱電機株式会社、日本電信電話株式会社
　再委託先（共同実施先）：学校法人金沢工業大学
（b5-2）IoTセキュリティ社会実装技術（IoT機器向けゲートウェイの社会実装に関する研究開発）
　委託先：三菱電機株式会社、日本電信電話株式会社

【研究開発の目的・内容】

重要インフラ等のユーザ事業者の設備においては、長期間にわたり運用されている古い機器やセキュリティ対策を施すことが困難な弱い機器が存在する。特に、重要インフラ設備においても導入が進むIoT機器ではこのような特性が顕著であることから、本研究開発では、IoTネットワークを監視するゲートウェイ装置（IoT-GW）と最先端のAI技術によって、多種多様なIoT機器に自動適応し、不正な動作を検知する技術の確立を目指した。

本研究開発において確立した技術は、既存のIoTシステムへの導入容易性を重視したIoTシステム向けの監視技術である。本技術が監視可能な機器は、通信トラフィックのバリエーションが限定的な機器であり、多くのIoT機器がこの特徴にあてはまる。また、定型業務端末についても発生する通信トラフィックの観点から同様の特徴を持つ場合、十分に監視が可能である。IoTシステムにおいて構成変更や規模変動が発生する場合、IoT機器の自動追従機能（学習等）及び分析サーバのスケールアウト機能によって、監視を適切に継続することができる。

本技術は、IoTシステムの外部接続点において監視を行うゲートウェイ監視モードに加えて、IoTシステム内の随所で監視を行うミラー監視モードを備えている。監視ポイントの選定にあたっては、監視ポイント増設自動判定機能を活用して自動的に監視可否を判定することができる。本技術のユーザ事業者は、当該機能を活用しながら、漏れのない監視を優先する場合には監視対象機器付近での監視を行い、導入・運用コスト優先の場合には多くの通信トラフィックを観測しやすい監視ポイントを選択するなど、セキュリティとコストのバランスを考慮した多様な設計に対応可能である。

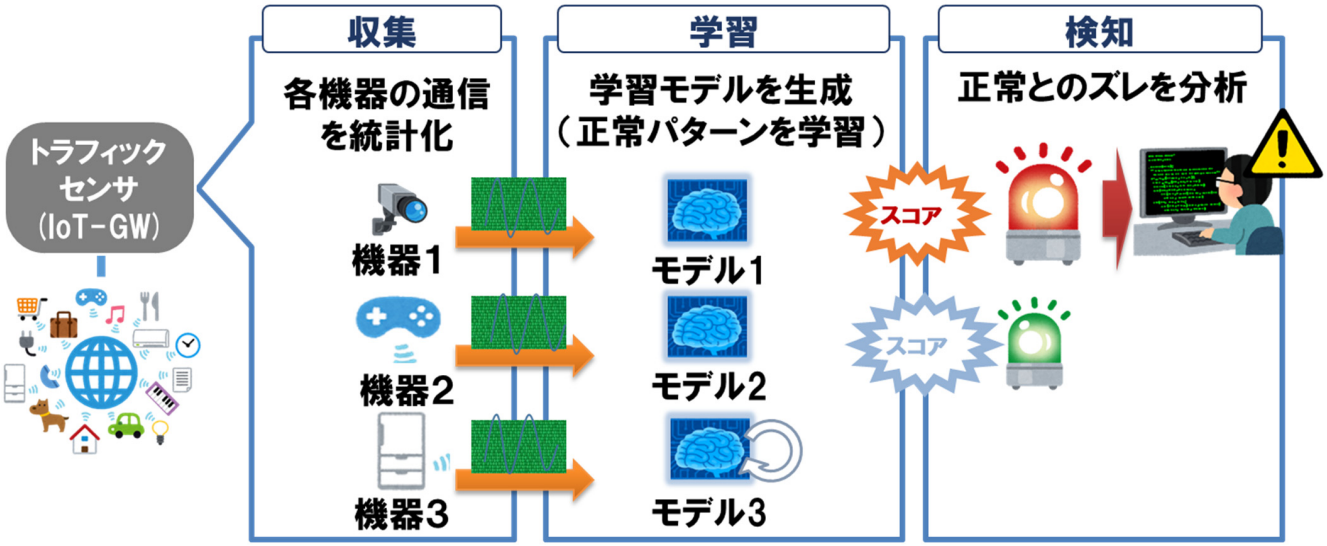


【研究開発の成果】

本技術の主な特長（技術的優位性）は以下のとおりである。

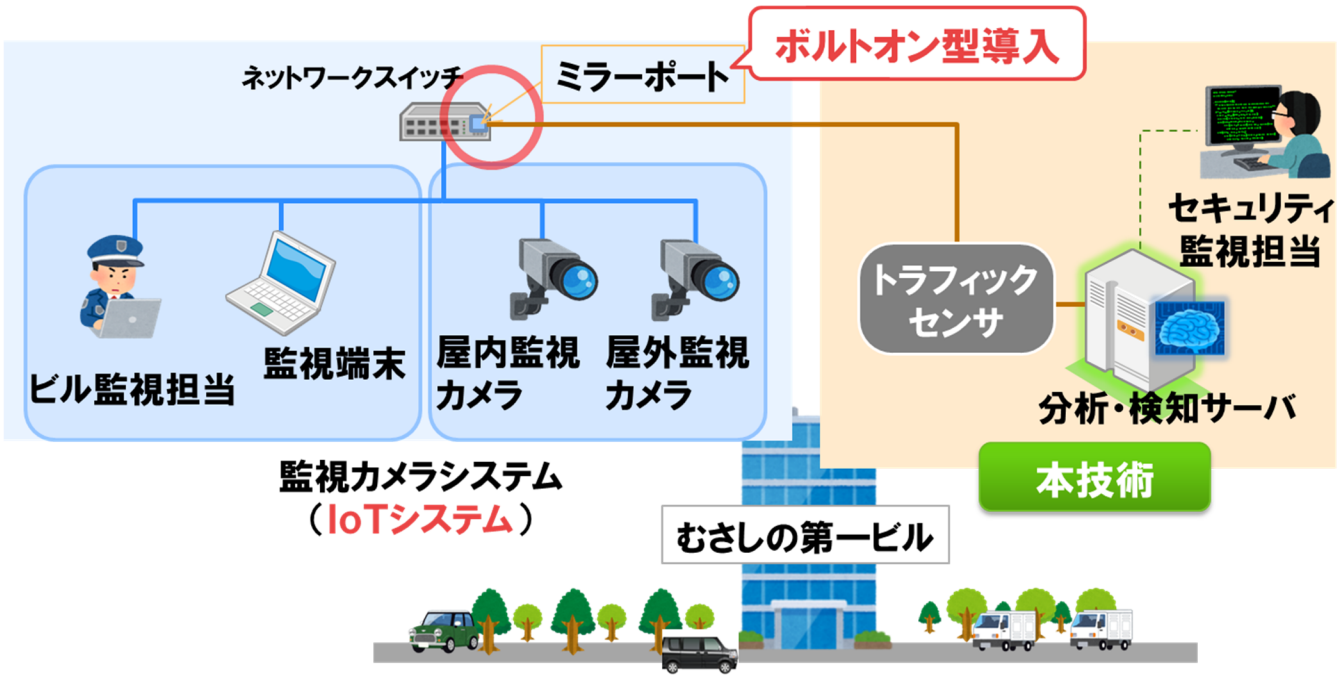
① 未知のサイバー攻撃等により発生するセキュリティ異常を高精度に検知可能
② 多様なIoT機器の新たな利用に対しても自動的に適応可能であり、かつ機微な情報を扱うIoTシステムにおいて暗号通信が用いられる場合にも対応可能
③ ゲートウェア監視モード及びミラー監視モードの両モードに対応することによって、既存のIoTシステムの構成に応じて影響を最小限に抑えた上での柔軟な導入が可能

本研究開発において確立した分析技術では、最新の深層学習に基づく理論を応用した学習方式によって、IoT機器の正常状態を表す学習モデルをあらかじめ生成し、当該学習モデルと観測データ（通信トラフィック等）との差異に基づいてセキュリティ異常を検出するアプローチを採用している。本方式はセキュリティ異常やその原因となるサイバー攻撃に関する事前知識を必要としないことから、上記の①のとおり未知のサイバー攻撃等により発生するセキュリティ異常を高精度に検知可能となる特長を有する。



一般的に、IoT機器に関するより詳細な情報を用いて学習を行うと、状態学習の精度は向上する。しかしながら、これは特定IoT機器や特定設備への依存性を増大させることにつながり、結果的に技術の適用性が低下するおそれがある。このような問題に対して、本実施項目では、IoT機器の通信トラフィックに関する新たな特徴量抽出技術を創出した。当該方式を中核として、上記の②に記載のとおり、本技術は多様なIoT機器に自動的適応可能な画期的な特長を有している。さらに、当該技術は対象となるIoT機器が暗号通信を行う場合であっても復号することなく特徴量を抽出可能であるため、機微な情報を取り扱うユーザ事業者の設備においても導入障壁が発生しづらいという実用的な優位性を備えている。

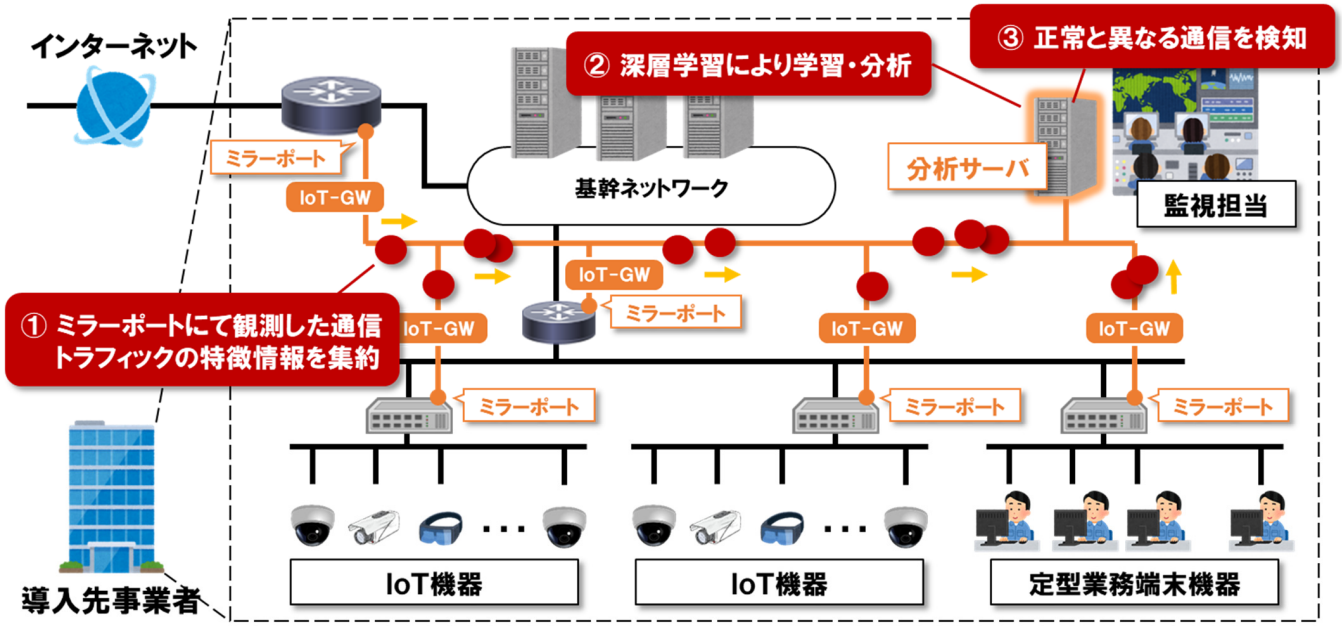
さらに、本研究開発では、ミラーポート接続による導入が可能な技術を確立した。既存のIoTシステムに対しては、本技術による監視システムを追加的に導入することが可能であり、上記の③に記載のとおり導入対象設備に対する影響を最小限に抑えることができる特長を有している。



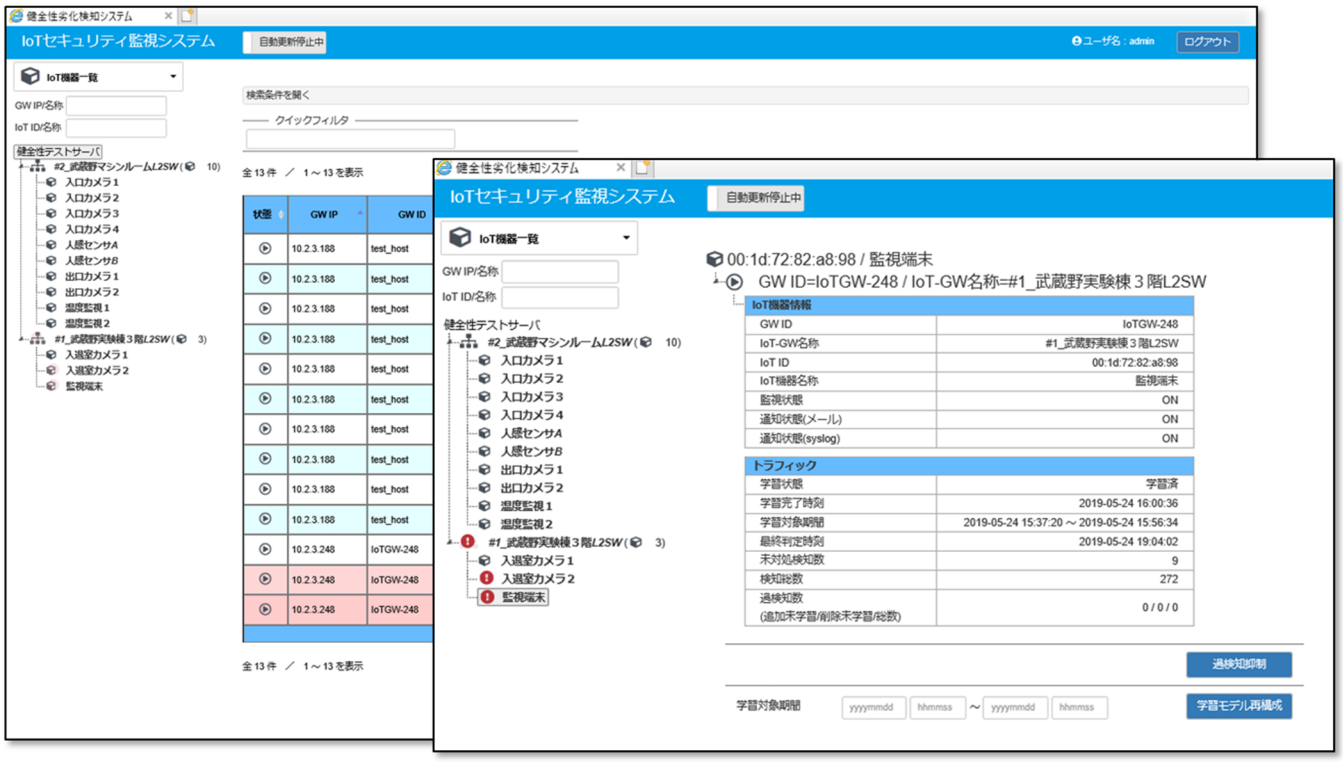
【実用化事例】

以下の構成図は、本技術の典型的な導入例である。通信トラフィックを収集するIoT-GWを、IoTネットワークを構成するネットワーク装置のミラーポートに接続するとともに、IoT-GWから通信トラフィックの特徴情報を集約して深層学習による分析を行う分析サーバを導入する。

IoT-GWの設置位置は、監視対象となるIoTに近いネットワーク、あるいはインターネットのような外部ネットワークとの接続点に近い箇所など、セキュリティとコストのバランスを考慮して設計する必要がある。なお、IoT-GWは接続位置に応じて監視性能の過不足を評価する機能を備えているため、このような監視ポイント設計の際に有効である。



以下の画面は、本技術が標準で備えている監視画面である。深層学習による学習管理、及びセキュリティ異常の検知結果の確認等のオペレーションを、できる限り特別な知識を求めず行えるように設計されている。



【本技術の適用範囲・導入条件】

本技術の適用範囲は、主に通信バリエーションが固定的な機器によって構成されるシステムである。そのような特性を備えたシステムとして典型的にはIoTシステムが考えられるが、さらに定型的な業務を行う端末についても同様の特性を備えていることが多いことから監視可能である。なお、分析サーバの現実装では、OSとしてRedHat Linuxを搭載したサーバ機器を利用している。

【今後の展開】

本技術は、導入可能なソフトウェア実装が既に完成しており、2018年度以降は重要インフラ設備において技術実証を行って有効性を確認している。今後、2020年度以降は重要インフラ分野における導入を達成するとともに、さらに工場分野等の多様な分野にも導入拡大を図っていく計画である。

【お問い合わせ先】

分析技術関連：
日本電信電話株式会社 NTTセキュアプラットフォーム研究所
E-mail: scpflab@hco.ntt.co.jp
IoT-GW関連：
三菱電機株式会社 コミュニケーション・ネットワーク製作所
E-mail: xs5n02@nh.MitsubishiElectric.co.jp

3.4　侵入・攻撃の早期検知による制御システムのセキュリティ耐性強化

（a2）制御・通信機器および制御ネットワークの動作監視・解析技術
③制御・通信機器のログ・トラフィック分析による健全性確認技術
委託先：株式会社日立製作所
（b3）評価検証プラットフォーム技術
委託先：株式会社日立製作所、エヌ・ティ・ティ・コミュニケーションズ株式会社
再委託先（共同実施先）：エヌ・ティ・ティ・アドバンステクノロジ株式会社

【研究開発の目的】

近年の巧妙化されたサイバー攻撃から重要インフラを守るためには、重要インフラシステムに適したセキュリティ技術が必要である。さらに、セキュリティ技術の研究開発に加えてセキュリティ運用・組織の確立も重要である。そのためテーマ（a2）③ではセキュリティ技術、テーマ（b3）では主に運用・組織について研究開発した。

テーマ（a2）③では「重要インフラにおける制御システムの分野固有知識と、分野間にまたがる共有知を統合できる革新的な解析モデルを構築し、継続的に進化可能な動作監視・解析技術」を実現するために必要な研究開発に取り組んだ。

重要インフラのサイバーセキュリティを確保するために、コントロールネットワークまでを含めたシステム全体の健全性を確認できる必要がある。このため、標的型攻撃などサイバー攻撃による健全性の劣化を検知する手段が必要である。標的型攻撃では、情報・制御ネットワークの制御・通信機器へ徐々に侵入し、最終的にコントロールネットワークの制御・通信機器に破壊的な異常を発生させることが想定される。標的型攻撃などによる健全性の劣化を破壊的な異常が発生する前に検知するためには、情報・制御ネットワークからコントロールネットワークにわたり、幅広く変化を検知し、解析する必要があるが解析手法は確立されていなかった。

情報・制御ネットワークと、コントロールネットワークの変化を検知するには、以下の課題がある。

（1）コントロールネットワークを含むシステム健全性確認のためのセキュリティ侵害起因による障害検知の困難性
従来から故障等の障害によるコントロールネットワークの異常を検知する故障予知技術は存在したが、セキュリティ侵害に起因する障害の検知技術は実用化されていなかった。

（2）正規ツールを悪用した標的型攻撃などによる異常検知の困難性
近年の標的型攻撃では、攻撃を検知されないようにするため、OS標準コマンドを利用するなど、正規ツールや業務ツールを悪用した事例が増えている。このようなツールの利用はウイルス対策ソフトの検知対象ではないため、対応困難である。

（3）コントロールネットワークにおける異常検知のための正常モデル生成の困難性
従来、標的型攻撃等に起因する異常を検知するには、正常動作時のモデル（正常モデル）と監視状態との微細な変化を検知するアノマリ検知が有用である。しかしながら、コントロールネットワークではシステム毎にプロトコルや業務フローが異なるなど汎用的な正常モデルを生成することが困難である。

上記の課題を解決するために、（1）コントロールネットワークを含むシステムの健全性確認技術、（2）正規ツールを悪用した標的型攻撃などによる異常の検知技術、（3）コントロールネットワークの異常を検知するための正常モデル自動生成技術を研究開発した。

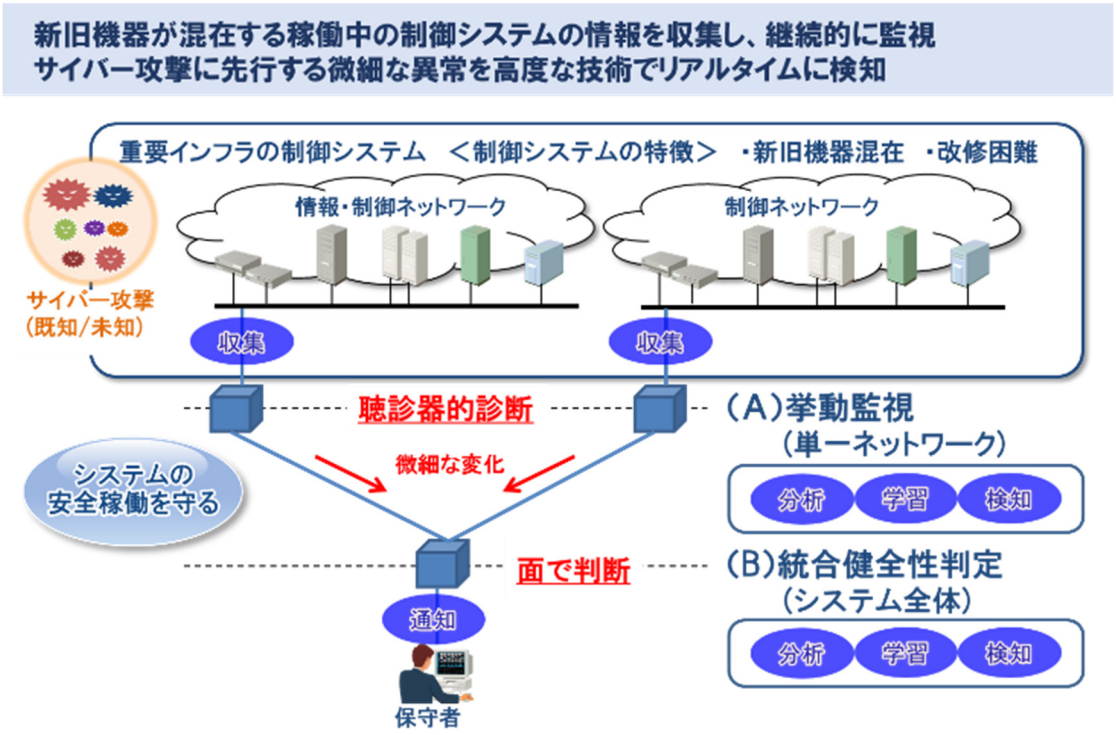
テーマ（b3）では鉄道、電力、水道、ガスといった社会インフラを支える重要インフラシステム（制御システム）は、ネットワークや装置への汎用技術の取り込みや、情報システムとの接続の増加に伴い、情報システムと同様のセキュリティ対策が求められてきている。重要インフラシステムで何らかの障害が発生した場合、死亡事故や環境汚染といった大きな影響を及ぼす恐れがあるため、セキュリティ対策は不可欠なも

のとして確実に実施する必要がある。一方、制御システムのセキュリティ対策に関連する規格・ガイドラインには、セキュリティ対策を実現するための具体的な方法を示しているものは少ない。このため、セキュリティ対策は設計者のノウハウに依存した結果となってしまう恐れがある。

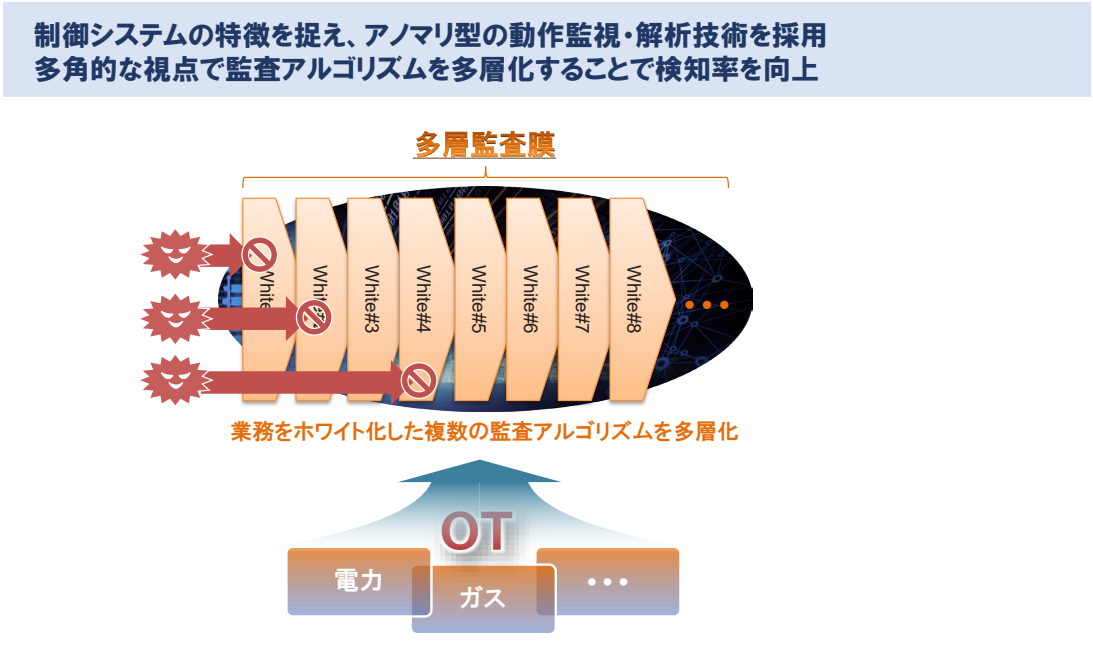
これを受け本研究では、制御システムにセキュリティ対策を適用する際の具体的な実現手法を示し、事業者のスムーズなセキュリティ対策導入を支援することを目的とした。

【研究開発の内容】

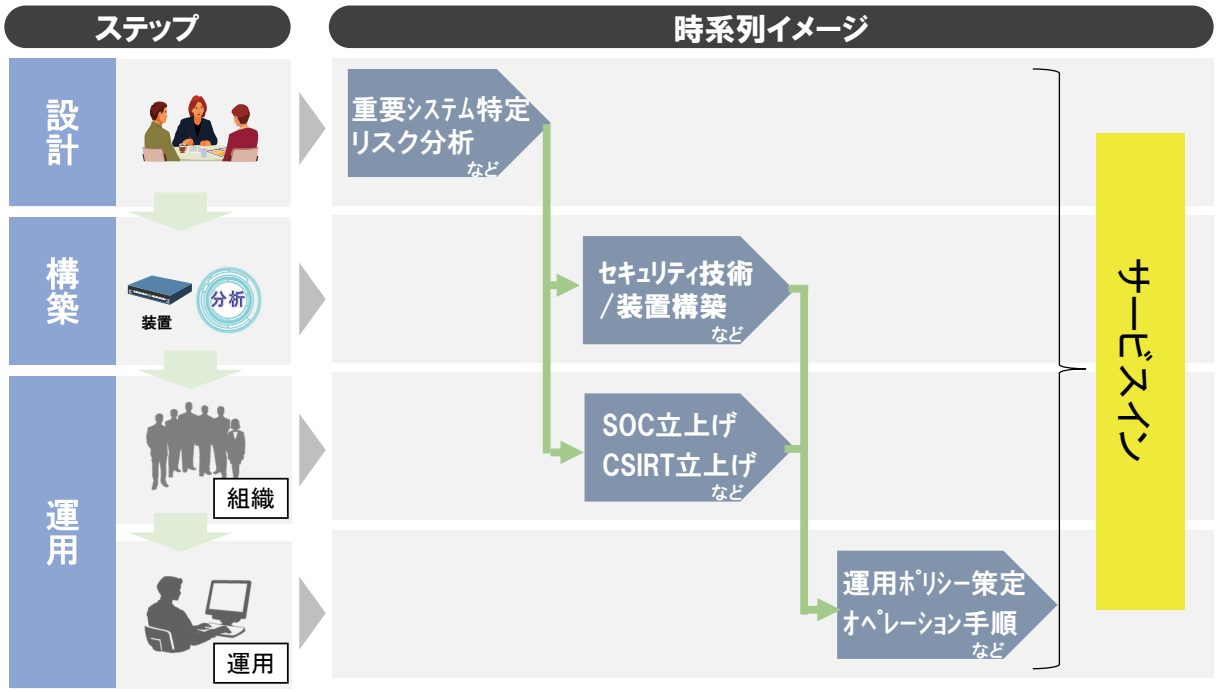
テーマ（a2）③で研究した検知技術の技術概要を以下に示す。



テーマ（a2）③の研究のコア技術は、多層監査膜を特徴とする。業務をホワイト化した複数の監査アルゴリズムを多層化している。技術的な特徴には、制御システムの特徴を捉え、アノマリ型の動作監視・解析技術を採用と、多角的な視点で監査アルゴリズムを多層化することによる検知率向上がある。



テーマ（b3）では重要インフラ事業者によるセキュリティ対策のスムーズな導入に向け、事業者が特に考慮すべき事項や具体的な実現手法をガイドラインとしてまとめた。セキュリティ対策の導入においては、「設計」「構築」「運用」のライフサイクル全般を通した検討が必要となる。また、重要インフラシステムは可用性重視でサービスを止められないため、元のシステムに特別な加工を施すことなく追加する形（ボルトオン）でのセキュリティ対策適用が必要であるという特徴を持つ。このような特性を持つ重要インフラシステムに対して、セキュリティ対策を確実・安全に導入するには、情報システムと同様の手順だけでは不十分な場合がある。



本ガイドラインでは、「設計」「構築」「運用」の各フェーズにおいて、重要インフラ事業者が特に注意を払う必要がある点を重要ポイントとして抽出し、各ポイントの解説や実現例を記述した。以下の図に重要ポイントの一例を示す。

重要ポイント ：セキュリティ対策を実施する箇所の決定

下記の観点から、セキュリティ対策実施箇所を決定する

リスクの大きさ	重要業務に関連する箇所や、脆弱性が高い箇所を優先的に監視/検知対象とする。 例えば、誰でも触れる場所にある機器（脆弱性が高い）を優先する。
効果	監視/検知対象を複数個所で監視/検知可能な場合、効果の大きい方を選択する。 例えば、特定の通信より多数の通信を監視できる箇所を優先する。
既存システムへの影響	万が一、監視/検知システムが既存システムに悪影響を及ぼす可能性を考慮する。 例えば、悪影響発生時に切り離し可能な部分を選定して設置する。
物理的制約	予め物理的制約も考慮して、導入機器を選定する。 例えば、設置スペースを考慮して導入機器の大きさを確認してから決定する。

【研究開発の成果】

テーマ（a2）③ではシステムを面で捉えたリアルタイム検知技術を完成させ、異常の発生箇所の具体化、検知要因の高度分析・具体化等によって、巧妙化が進む制御システムの攻撃を早期フェーズで検知を実現した。

本技術の技術的な優位性を以下の表に示す。

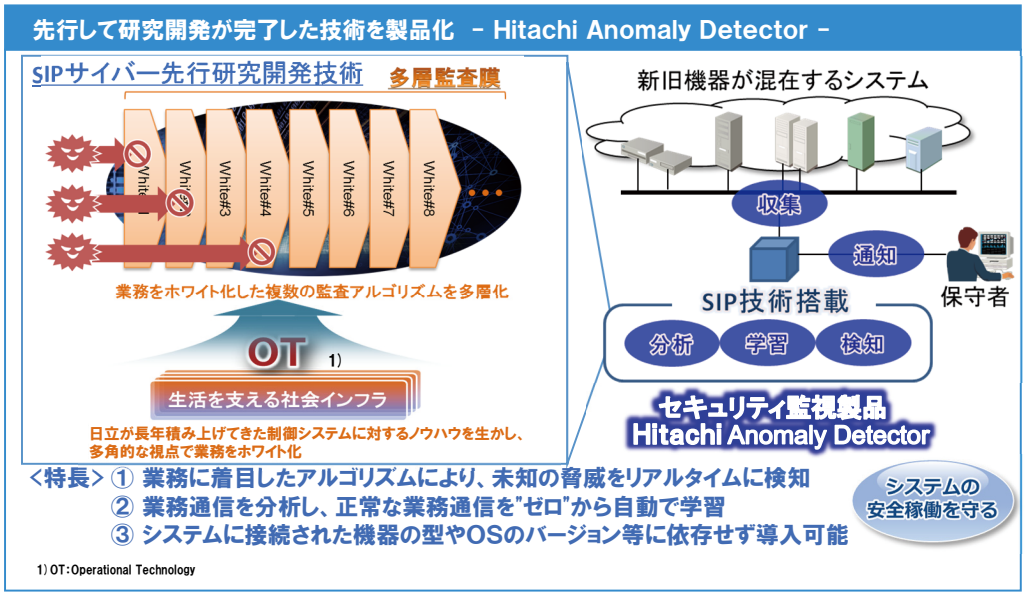
主要な技術的優位性	ユーザメリット
① 微細な変化のリアルタイム検知	■ 既知の脅威に加え、これまで検知が難しかった未知の脅威を早期かつリアルタイムに検知する技術 ■ リアルタイム検知技術自体の可用性を向上する技術
② 制御システムの学習	■ 制御システムの業務通信を多角的な視点で学習し、サイバー攻撃の検知に使用するモデルを生成する技術 ■ 制御システムの構成変更に追随するための制御システムの業務通信の追加学習機能
③ 統合分析	■ システムを面で捉えることで、サイバー攻撃やオペレーションミス等のサービスに影響を与える事象に対する検知率を向上する技術 ■ 業務通信以外の情報を加えて統合的に分析することで、サービスに影響を与える事象やその予兆を検知する技術
④ 導入構成	■ 新旧機器（OSのバージョンが古いもの、リソースの小さい機器など）が混在したシステムに対してもシステムに影響なく導入可能な構成

テーマ（b3）では重要インフラシステム（制御システム）は事業規模が大きく、事業を構成する業務やシステムも多種多様であるため、事業全体のリスクを網羅的に把握するのが困難である。さらには、重要インフラ事業は多数の事業と連携するため、他事業との依存関係を考慮したリスクの把握が必要であるが、他事業との複雑な依存関係の把握も困難である。また、これまでの各世代で導入された既存システムが入り混じっており、加えて機能の性質上可用性重視でサービスを止められないため、元のシステムに特別な加工を施すことなく追加する形（ボルトオン）でのセキュリティ対策適用が必須である。

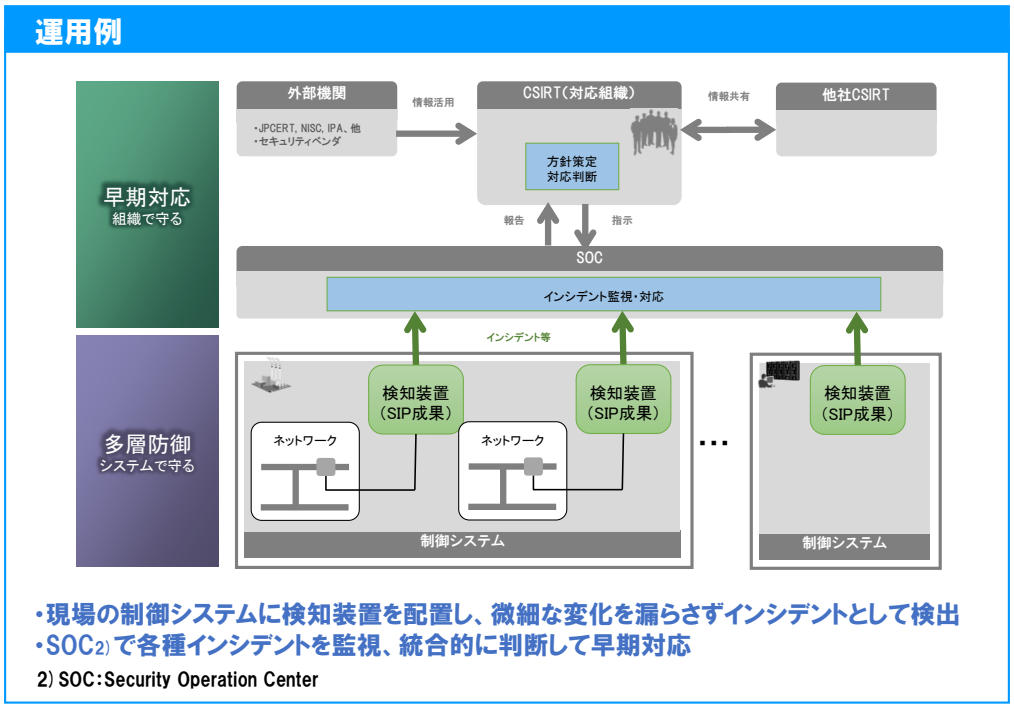
本研究では、上記の特徴を踏まえたセキュリティ対策導入の手法を確立した。

【実用化事例】

コア技術であるアノマリ監視アルゴリズムは、先行してHitachi Anomaly Detectorとして製品リリースされている。この製品は（a2）③技術の特長を活かしており、その特長は、新旧システムが混在するシステムに対し、（ⅰ）業務に着目したアルゴリズムにより、未知の脅威をリアルタイムに検知、（ⅱ）業務通信を分析し、正常な業務通信を"ゼロ"から自動で学習、（ⅲ）システムに接続された機器の型やOSのバージョン等に依存せず導入可能、である。



以下にHitachi Anomaly Detector – のCSIRT（対応組織）のSOC（Security Operation Center）での運用例を示す。



【本技術の適用範囲・導入条件】

本研究で開発した技術は、重要インフラシステム（制御システム）を対象としている。システムを検知技術で守るとともに、運用をガイドラインで守り、体制を含めてすべての面でのセキュリティ耐性強化を促進するものである。

【今後の展開】

研究開発した技術を製品にフィードバックし、今後とも社会インフラのセキュリティ強化に貢献してゆく。

【お問い合わせ先】

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　セキュリティ事業統括本部
電話番号：03-5471-2324

3.5　ダイナミックマップの流通に向けたデータセキュリティマネジメントの実現

（a2）制御・通信機器および制御ネットワークの動作監視・解析技術
④ダイナミックマッププラットフォームのインフラとなるクラウドシステムの健全性確認技術
委託先：富士通株式会社

【研究開発の目的】

本研究開発テーマでは、多種多様なダイナミックマップ情報（地図情報・地理情報）を保持する情報提供者と、そのダイナミックマップ情報を活用し付加価値サービスを提供するサービス提供者の間で、安心・安全にダイナミックマップ情報の受け渡しを実現する「ダイナミックマップ情報を取り扱う情報インフラ」（以降、ダイナミックマッププラットフォームと呼ぶ）のセキュリティ確保に必要な研究開発に取り組んだ。

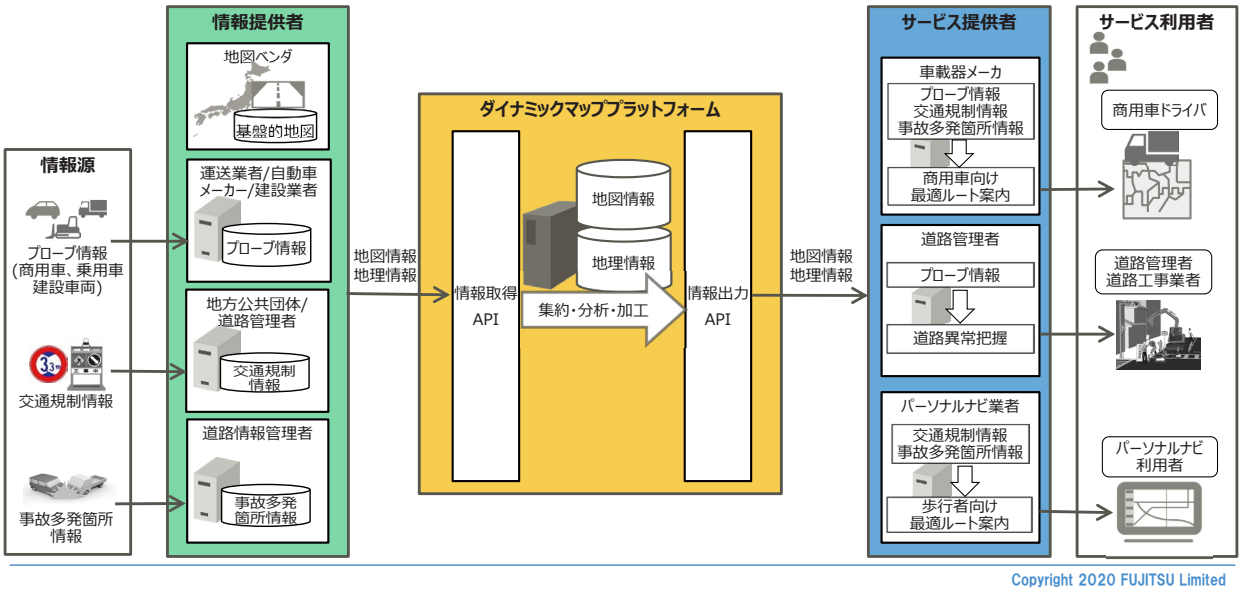


図3-5-1　ダイナミックマッププラットフォームの全体像

【研究開発の内容】

（1）ダイナミックマッププラットフォームのセキュリティ確保に必要なセキュリティ要求事項の策定

SIP／自動走行システムにて研究開発に取り組むダイナミックマップサービスプラットフォームをモデルとし、インフラ面と業務面から網羅的にセキュリティを検討し、ダイナミックマッププラットフォームに必要なセキュリティ要求事項（12カテゴリ、59要求事項、167項目）を策定した。さらに、セキュリティ要求事項に含まれない更なるセキュリティ強化に必要な仕組み、制度、運用等についてセキュリティ強化提言としてまとめ、今後の検討課題を抽出した。

（2）データのセキュリティ（機密性・完全性・真正性）を確保する技術の開発

ダイナミックマッププラットフォームで取り扱うデータには自動車の位置情報や車載カメラの画像などがあり高いセキュリティレベルが求められるためデータのセキュリティを確保することが重要課題である。

そこで、セキュリティ要求事項の実用に向けて重要課題であるデータのセキュリティを確保する仕組みを検討、情報提供者、サービス提供者、ダイナミックマッププラットフォームが連携することでデータのセキュリティを確保する技術（データセキュリティマネージメント）を開発した。

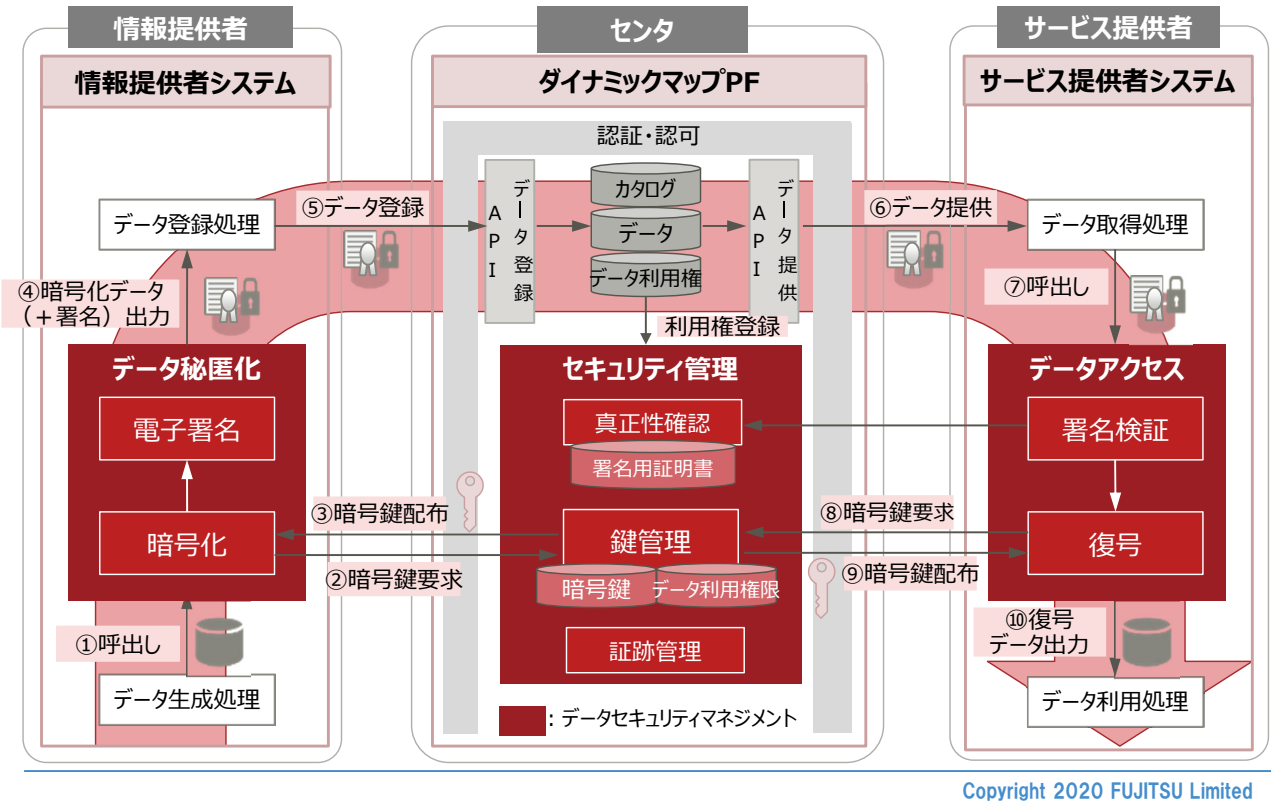


図3-5-2　データセキュリティマネジメントの全体像

【研究開発の成果】

- ダイナミックマップ情報(地図情報・地理情報) の安全な流通が可能となり、自動走行システムの高度化、およびダイナミックマップ情報を活用した新たなサービス創出が期待できる。
- SIP／自動走行システムと連携して取り組み、研究成果を共有することで、SIP／自動走行システムで研究開発に取り組むダイナミックマップサービスプラットフォームのセキュリティ強化とセキュリティ・バイ・デザインを実現できた。
- 情報提供者、サービス提供者のセキュリティレベルによらずデータ流通のセキュリティ強化が実現できるため、防災・減災分野、インフラ維持管理分野、農業分野など様々なデータプラットフォームのセキュリティ強化に応用でき、超スマート社会（Society5.0）の実現が加速される。

【本技術の適用範囲・導入条件】

- ダイナミックマップ、防災・減災分野、インフラ維持管理分野、農業分野など様々なデータプラットフォームに適用可能
- 仮説、机上による検証であるため、実装にあたっては妥当性の確認を再度実施する必要がある。

【今後の展開】

- SIP／自動走行システムのダイナミックマップサービスプラットフォームが事業化される際にセキュリティ機能として実装を予定している。

【お問い合わせ先】

富士通株式会社　Mobilityシステム事業本部
fj-mob-sip-sec@dl.jp.fujitsu.com

3.6　異常検知時においても安全に運用継続を可能とするシステム防御技術

（a3）制御・通信機器およびシステムの防御技術
委託先：アラクサラネットワークス株式会社、技術研究組合制御システムセキュリティセンター
再委託先（共同実施先）：三菱電機株式会社、国立大学法人電気通信大学

【研究開発の目的】

昨今制御システムへの高度なサイバー攻撃により被害が発生しており、我が国の重要インフラをサイバー攻撃から保護することは重要となっている。

本研究開発では、サイバー攻撃から制御機器を防御しつつ、安全に運転を継続できる可能性を有するホワイトリスト機能を用いて、プラントの安全・安心な運転を継続させ、我が国の重要インフラを保護することを目的として、ライフサイクル（プラントの運転状況など）を組み込んだ協調ホワイトリスト防御による制御システムの階層防御機能を開発している。本技術は、監視端末（Human Machine Interface: HMI）、ネットワークスイッチ、コントローラに対して実装し、それぞれにおいて「命令」「通信」「動作」のレベルで検知防御を行う。制御システムの命令の流れは、監視端末→ネットワークスイッチ→コントローラの順であり、この3ヶ所が制御システムをサイバー攻撃から守る上で重要となる。

制御システムは、決まった端末、機器において予め決められた動作を繰り返し行うものであり、制御のリアルタイム性が重要視される。情報システムで広く用いられるブラックリスト型マルウェア対策は、リアルタイム性確保困難、マルウェア定義ファイルの更新困難の観点から、制御システムに適しているとは言えない。これに対して、ホワイトリスト型マルウェア対策は、制御システムが予め決められた動作のみを行うという特徴から、親和性が高く有望であると考えられている。しかし、既存のホワイトリスト型対策は、Stuxnetのような高度なサイバー攻撃には不十分であると考えられる。

そこで、本研究開発では、ライフサイクル（プラントの運転状況など）に基づき異なる制御機器（HMI、スイッチ、コントローラ）にホワイトリストを導入し、異なるレイヤを監視することで、階層防御を実現し、検知機能を高精度化する。ライフサイクルによりホワイトリストに時系列情報や因果関係を持たせ精緻なサイバー攻撃の検出を実現することができる。同機能でサイバー攻撃を受ける範囲を局所化に貢献し、通常運転から縮退運転への速やかな移行、さらには通常運転状態への回復を加速することを目的とする。

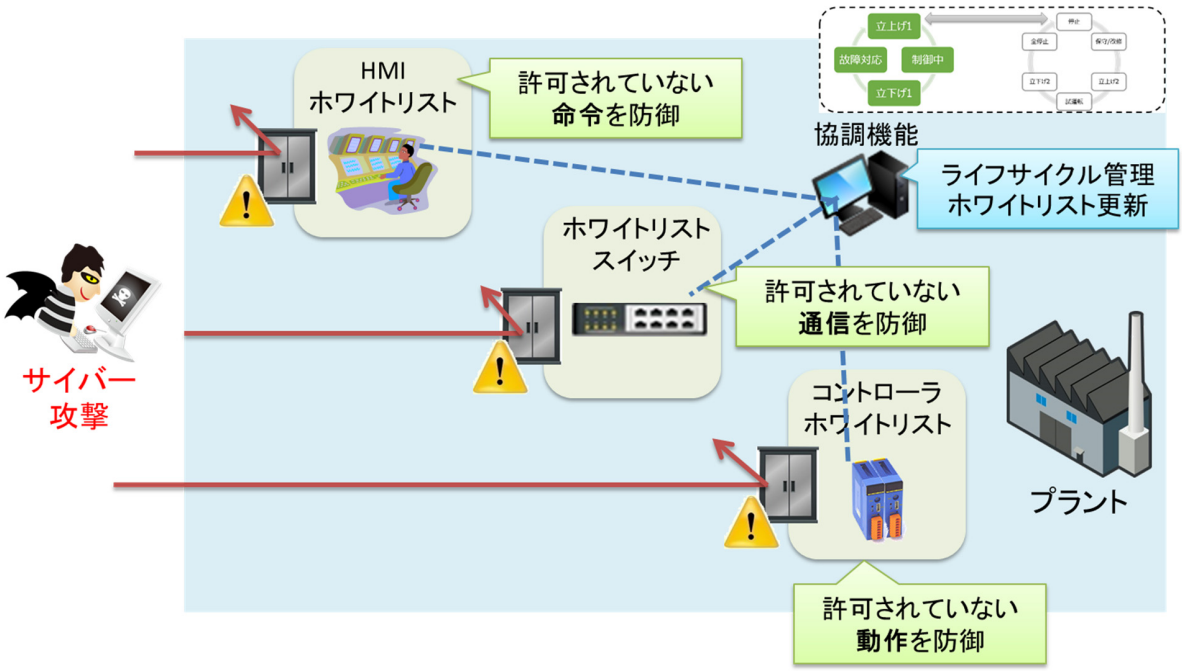
【研究開発の内容】

現状のホワイトリストの問題の解決の方向性として、我々は以下の方向性に基づき、本研究開発を実施している。

- 制御システムにおけるライフサイクル（プラントの運転状況等）ごとの特定の動作に着目し、ライフサイクルごとに定められた動作以外を許可しないホワイトリスト技術を確立する
- 制御システムの主要なコンポーネントである監視端末、ネットワークスイッチ、コントローラに対して実用的なホワイトリスト技術を開発する
- 監視端末ホワイトリスト、ネットワークスイッチホワイトリスト（ホワイトリストスイッチ）、コントローラホワイトリストは協調機能により連動し、サイバー攻撃検知時には連携して防御を行う
- 各機器にホワイトリスト機能を追加した場合でも、制御システムへの影響を最小限にする実装方式とする

コンセプト

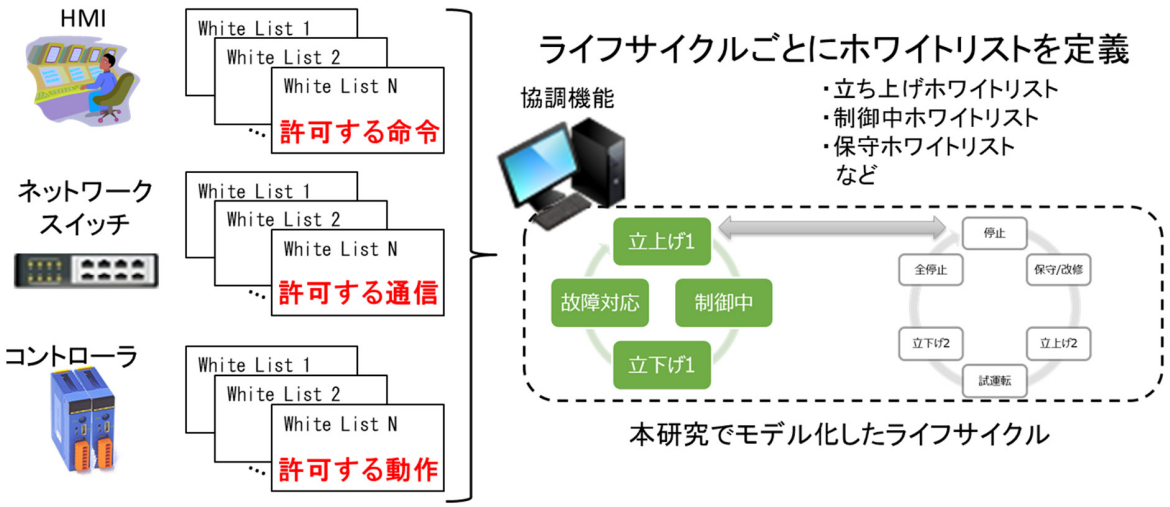
重要インフラの制御システムへのサイバー攻撃を3層のホワイトリストを
ライフサイクル（プラントの運転状況等）に基づき協調動作させて防御



研究開発内容

●監視端末（HMI）、ネットワークスイッチ、コントローラの各機器に異なる性質のホワイトリスト機能を実装

●協調機能により、ライフサイクル（プラントの運転状態など）に応じてホワイトリストを切り替えて運用



【研究開発の成果】

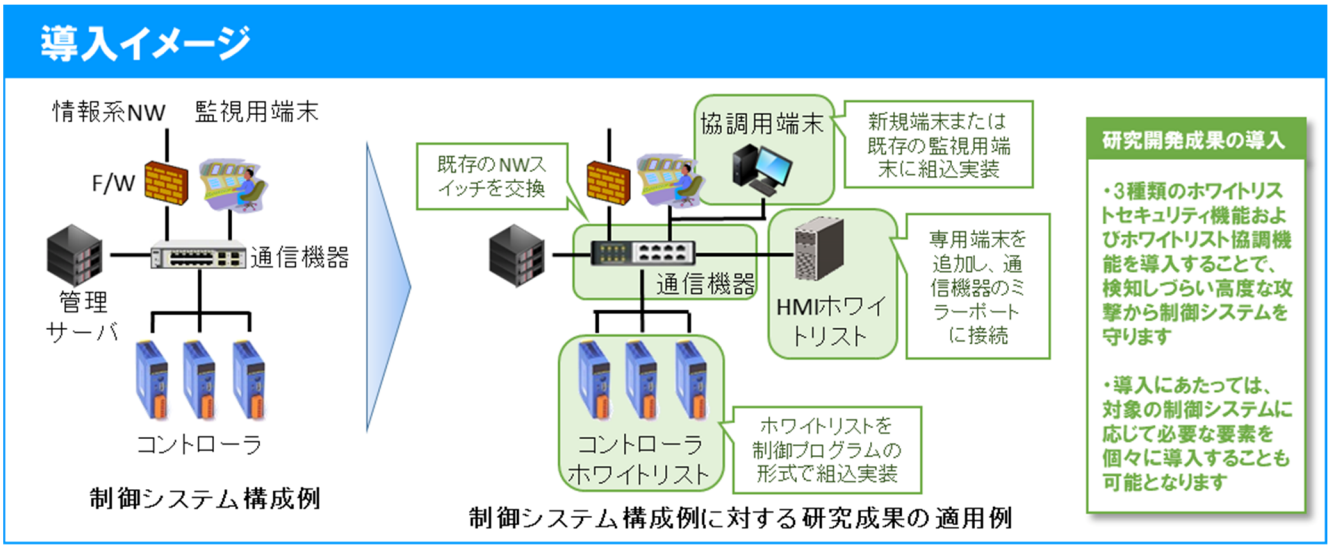
- ライフサイクル（プラントの運転状況など）に応じてホワイトリストを切り替えることで、精緻な攻撃検出を実現した
- 監視端末（HMI）、ネットワークスイッチ、コントローラにホワイトリストを導入し、異なるレイヤを監視することで、階層防御を実現し、検知機能を高精度化した

【実用化事例】

• 開発成果の一部（通信機器のホワイトリスト機能）を電力事業者1社のシステムに導入した

【本技術の適用範囲・導入条件】

• ライフサイクル対応のホワイトリストを搭載した監視端末（HMI）、通信機器、コントローラ（PLC）、協調機能搭載端末



一般的な制御システムを構成するコンポーネント(HMI、通信機器、コントローラ) に実装可能。工場やビル、プラントにて幅広く利用できる。各機能単体でも適用可能。

○監視端末ホワイトリスト

専用端末を追加して導入する。通信機器のミラーポートから監視端末が送信した命令を監視する。

○通信機器ホワイトリスト

既存のネットワークスイッチを、本研究成果を適用した製品に置き換えて導入する。

○コントローラホワイトリスト

コントローラホワイトリストを制御プログラム（ラダー言語）の形式でプログラマブルコントローラに組み込んで導入する。コントローラに対する専用ハードウェアの追加は必要なく、ソフトウェアのみで実装可能。

○ホワイトリスト協調機能

他のホワイトリスト機能と組み合わせ、ライフサイクルの切り替えや検知情報の管理・表示を行う。新規端末に実装して導入する。また、既存の監視端末を改修して組み込むこともできる。

【今後の展開】

2020年度以降、各ホワイトリスト機能の機能向上の研究を継続しつつ、各機能単体およびホワイトリスト協調機能により連携した協調ホワイトリスト防御システムの事業化を目指す。

【お問い合わせ先】

技術研究組合制御システムセキュリティセンター　東北多賀城本部（TTHQ）
TEL:022-353-6751　FAX:050-3153-0000　E-mail:cssc-sec@css-center.or.jp

3.7　IoTのセキュリティを実現する超低電力公開鍵暗号実装技術

（a4-1）IoT向けセキュリティ確認技術（IoT向けのセキュリティ確認技術の研究開発）
委託先：電子商取引安全技術研究組合、ルネサスエレクトロニクス株式会社
再委託先（共同実施先）：国立大学法人奈良先端科学技術大学院大学、セコム株式会社、
国立大学法人神戸大学、国立大学法人東京大学、国立大学法人横浜国立大学、国立大学法人電気通信大学、
国立大学法人東北大学、国立研究開発法人産業技術総合研究所、学校法人東北学院東北学院大学

【研究開発の目的】

IoT（Internet of Things）は、あらゆるモノがネットワークにつながることによって、新しい価値を創造する情報社会を意味する概念である。IoTシステムのセキュリティを確保するためには、本質的には、暗号技術を利用した構成機器間の相互認証が必須の条件となる。

しかし、実際のIoTシステムにおいて、暗号による機器間相互認証を行えている事例はまだ少ない（2014年7月HP社調査によれば、IoTシステム構成機器の内、暗号機能を使用していない比率は70%とされる）。

その理由は、

- IoTシステムが普及して日が浅いこと
- 末端の機器がリソースに乏しいこと
- 攻撃を受けた例がまだ少ないこと

などである。

だが、今後、IoTシステムへの攻撃事案は飛躍的に増加することが見込まれる。とりわけ、次の二つの事例については、注意が必要である。

- 重要な資産を保護し、セキュリティを必要とするIoTシステム（例:警備、医療、自動車、ロボット・・）が攻撃される。
- IoTシステムが、重要な資産を保護し特にセキュリティを必要とする重要インフラ等のシステムに接続していて、IoTシステムの末端機器から侵入を受け、重要インフラ等が攻撃される。

本研究開発においては、これらの事例にとくに着目しつつ、IoTシステムにおける構成機器間相互認証のためのキーデバイスとなる、耐タンパー性を具備するセキュア暗号モジュールを開発し、それを活用したモデルシステムを構築することを目的とする。

【研究開発の内容】

多数のモノがネットワークに繋がることにより新しい機能を創造することを目指すIoTが図1のようなシステムとして構築されつつある。大いなる潜在力を秘めたIoTが適切に機能し、運用され、維持されていくためには、IoTを構成するシステムに対する脅威を踏まえ、適切なセキュリティが達成される状況を作り出さなければならない。図1の右の部分にセキュリティ上の脅威の主なものを列挙している。

これらの脅威に対処するためには、多様な観点からの措置が必要となるが、最も基盤的に必要な技術的目標は、IoTシステムのスコープ内の全ての構成機器間での、暗号による相互認証とデータ保護を実現することである。

このためには、公開鍵暗号技術の導入が必須となる。例えばディジタル署名技術は、IoT機器が外部から受信したソフトウェアがその機器内で使用が正当なもので否かをIoT機器自身が判断するために役立ち、また、あるデータが、特定のIoT機器で生成・処理・送信されたデータであるかを、それを受け取ったどの機器においても検証できるなど、システムのインテグリティ向上の効率よい実現に寄与する公開鍵暗号技術である。この他にも、データの守秘性、共通鍵暗号技術における鍵の共有など、公開鍵暗号技術はIoTシステムのセキュリティを充実するために基本となる諸々の機能を達成できる。

ただし、IoTシステムにおいて、公開鍵暗号技術が、計算能力や消費電力の点で制約の多い末端ノードに至るまで、特別な工夫をしなくてもごく当たり前に利用可能であるようにしなければならない。IoTシステムに公開鍵暗号技術を導入する利点を図2にまとめる。

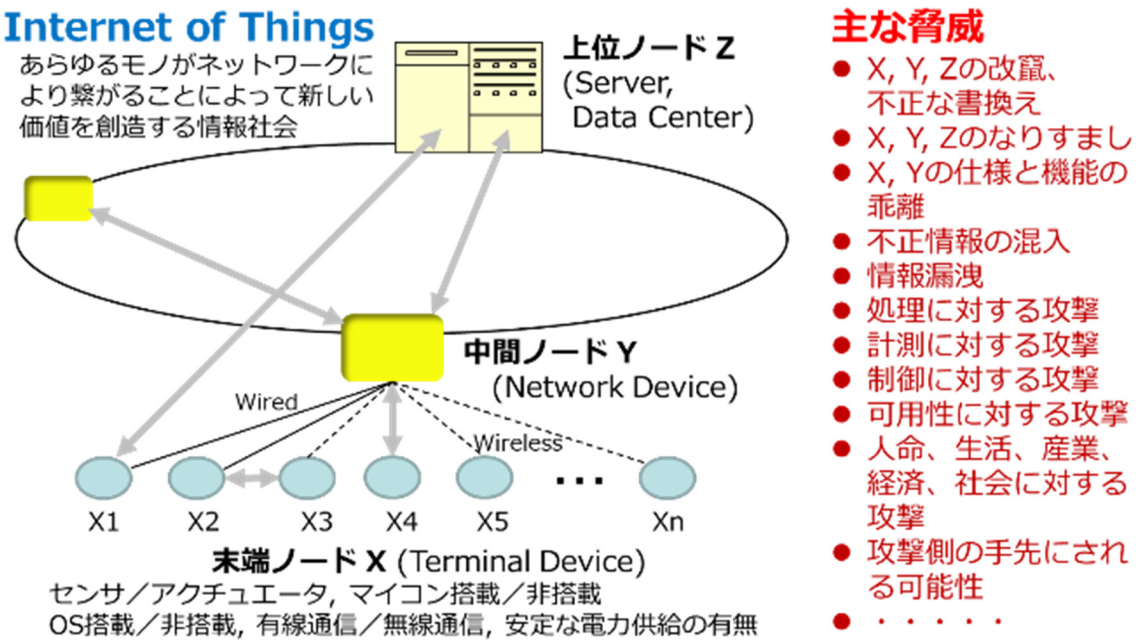


図1.　IoTのモデルとセキュリティ上の脅威

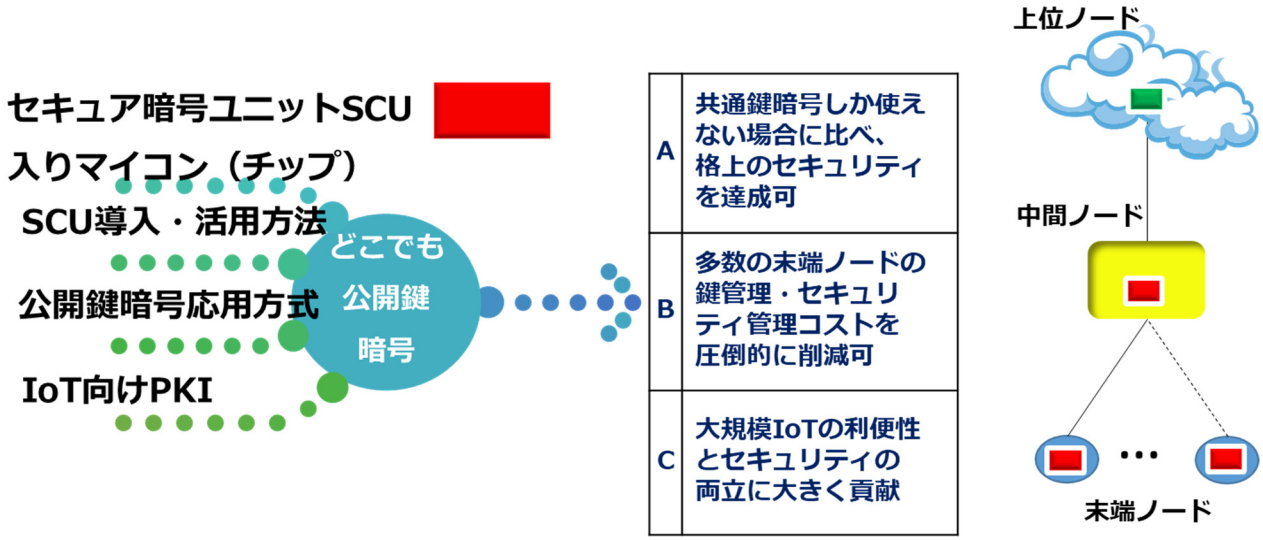


図2.公開鍵暗号をIoTの末端ノードでも簡単に利用できる状況を創出

公開鍵暗号技術の末端ノードまでの浸透という大きな目標を具体的に達成するには、今後のIoTでの大幅な利用が期待される公開鍵暗号技術である楕円曲線暗号技術を、末端ノードを構成するローエンドのマイクロコントローラチップに内蔵できることが必須であり、これは難易度の高い課題であった。また暗号の鍵やアルゴリズム自体を攻撃から守る耐タンパー機能の充実をそのような末端ノードにおいて図ることも大きな課題であった。

これらの課題に対し、本研究開発ではセキュア暗号ユニット（Secure Cryptographic Unit; SCU）のコンセプトを練り上げ、優れた実装方式を含むSCU構築技術の研究開発を進め、同技術を確立した。開発したSCUの概要を図3にまとめる。

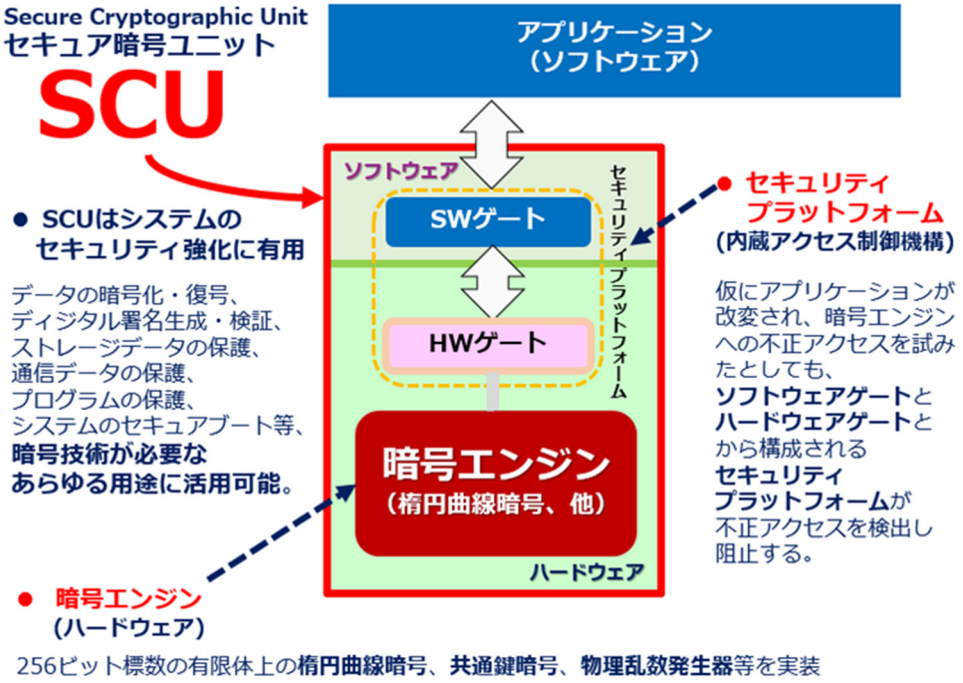


図３. SCUの概要

【研究開発の成果】

	実施項目	成果
①	IoTシステムを構成する機器のためのSCUの開発	
①-1	暗号モジュール試作開発	IoT向け半導体チップに搭載するIPユニットとしてSCU（セキュア暗号ユニット）の試作開発を行い、実施計画に掲げた所期の性能目標を達成した。
①-2	耐タンパー技術開発	半導体チップに対する外部からの侵襲性・非侵襲性攻撃技術の研究を行い、それらの攻撃の一部に対する対策技術を開発し①-1のSCU試作開発に反映させた。
①-3	セキュリティプラットフォーム開発	セキュリティプラットフォームを構成するハードウェアゲートとソフトウェアゲートの開発を行い、①-1のSCU試作開発に反映させた。モデルシステムに必要となる暗号エンジンの内、ECCエンジン以外の部分の開発を行い、①-1のSCU試作開発に反映させた。SCUユーザのためのガイダンス文書等を作成した。
①-4	実用化戦略研究	SCUを社会実装するための知財戦略、SCUを広く普及させるための国際標準化戦略とインターオペラビリティ戦略の研究を行い、成案を得た。
②	SCUを活用したモデルシステムの構築	
②-1	SCUを活用したモデルシステムの構築	SCUボードを搭載した監視カメラシステムを構築し、成りすましや映像データの改竄などの影響とSCUの効果をアプリケーションレベルで検証した。
②-2	SCUの導入分析および実施モデル提案	SCU の効果が最大化されるような社会実装を検討するために、SCUの導入分析および運用モデルの提案を行った。
③	ハードウェアトロージャンに対抗する技術の開発	ハードウェアトロージャンを検出する手法の基礎検討を行い、半導体チップを用いた検出機構について基本的なデモンストレーションとシミュレーションを構築し、その有効性を示した。

SCUは、IoT機器をサイバー攻撃から守るICチップ内に組込む“軽い、速い、強い”モジュール

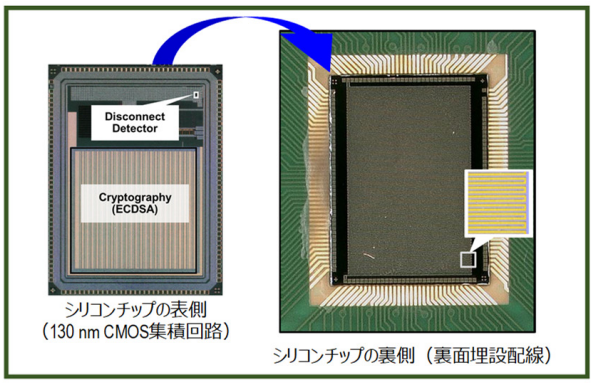
ECDSA（楕円曲線暗号）の処理において、世界最小、世界最少消費電力、世界最速の個別記録を複数試作品でそれぞれ達成。

末端ノード用	中間ノード用
小面積・低電力化を達成 0.09mW 13kgate	高速処理化を達成 10,000回/sec

項目	No	内容	達成度	成果
SCUの開発	1	SCUの試作開発	○	SCU評価ボード（KMシリーズ）
	2	耐タンパー技術開発	○	評価報告の完成 デモンストレーションの提示
	3	セキュアプラットフォームの開発	○	ST・ガイドラインの完成
	4	実用化戦略研究	○	実用化戦略提案（実装顧客の開拓）
モデルシステムの開発	1	モデルシステム構築	○	モデルシステムの完成
	2	セキュア暗号モジュールの導入分析および実施モデル提案	○	報告書の完成
対HWトロージャン技術開発	1	攻撃事例整理	○	報告書の完成
	2	対策技術研究	○	評価報告の完成 デモンストレーションの提示

※成果につきましてはNEDOの成果報告をご参照ください。

SCU評価ボード



耐タンパー技術評価チップ

【本技術の適用範囲・導入条件】

本技術は半導体チップの部分となるIP（知財）であり、アプリケーションにおいてセキュリティ機能を必要とする半導体チップに広く適用される。なかでもIoT機器向けの半導体製品に親和性が高い。

導入条件については、NEDO成果報告書サイトに下記の文書が公開されるので、参照されたい。

- SCU_ST（セキュリティ設計仕様書）
- SCUガイダンス_IoT機器におけるSCU搭載チップの利用ガイダンス
- SCUガイダンス_SCU_IP利用者向けガイダンス
- SCUガイダンス_鍵マネジメントに関するガイダンス

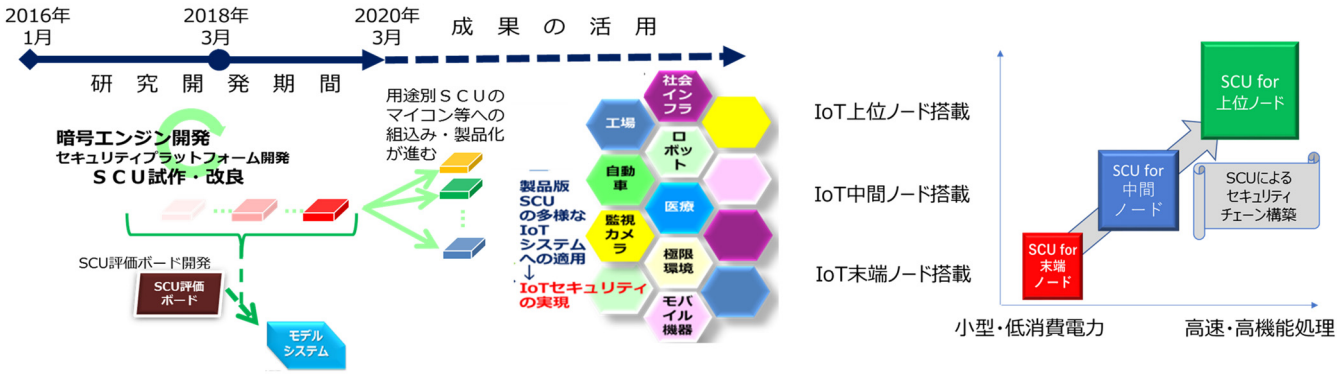
公開時期:2020年４月以降

URL: https://www.nedo.go.jp/activities/ZZJP_100109.html

【今後の展開】

2020年度、大手民間企業２社が各々SCUを搭載した半導体製品の試作を行い、試作品の評価を経て、本研究で開発された技術を活用してアプリケーション事業展開に進む見込みである。

電子商取引安全技術研究組合は、2022年４月より、技術研究組合法の適用を受けて企業化し、SCU技術の知財管理・運用ビジネス、及び、SCU搭載半導体チップのターンキービジネスを行う予定である。



SCUの普及イメージ（IoT用途別の広がりとIoTノード別の進化）

【お問い合わせ先】

電子商取引安全技術研究組合

Tel：03-5259-8077　Fax：03-5259-8070　URL：https://www.ecsec.org

3.8 「防御」、「検知」、「対策」でエンドポイントを守るトータルサイバーセキュリティ

（a4-2）IoT向けセキュリティ確認技術（IoT機器向け評価検証プラットフォーム技術の研究開発）
委託先：パナソニック株式会社
（b5-1）IoTセキュリティ社会実装（IoTセキュリティ社会実装技術の研究開発）
委託先：パナソニック株式会社
再委託先（共同実施先）：PwCコンサルティング合同会社

【研究開発の目的】

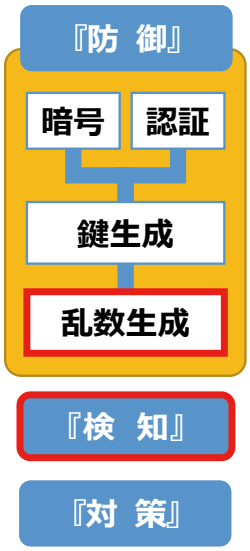
IoT技術を活用することにより生産性やサービスの利便性が飛躍的に向上するため、IoT機器の普及が急速に進んでいる。一方で、IoT機器を標的とした攻撃も急増し、IoT機器を踏み台とした大規模な攻撃も発生している。IoT機器への攻撃は生命・財産に影響を及ぼす可能性もあるため、安全な社会インフラを実現するとともに、国内産業のグローバルな競争力を強化するためには、IoT機器に対するサイバー攻撃の対策は喫緊の課題である。

このような背景のなか、IoT機器に対するセキュリティの設計指針となるガイドラインは策定されているが、具体的な実装方法が分からないことがIoTベンダーのお困りごととなっている。サイバー攻撃を防ぐためには、スペックの低いIoT機器でもITと同様の暗号・認証機能を実装し、暗号・認証機能で防げない攻撃に対しては早期に発見して対策する必要がある。また、攻撃者はセキュリティ対策が十分でないIoT機器を狙ってシステムへの侵入を試みるため、IoT機器のセキュリティ対策を全体的に底上げする必要がある。そこで、幅広いIoT機器で活用できるセキュリティ技術を開発するとともに、開発したセキュリティ技術を社会普及させるために、実装方法のガイドラインを作成する。

【研究開発の内容】

攻撃者はIoT機器の認証機能やソフトウェアの脆弱性を攻撃してIoT機器に侵入し、データの不正取得、改ざんなどを行うため、セキュリティ対策としては、なりすましによる不正侵入も含めてこれらの攻撃を防ぐことができる公開鍵暗号方式を用いたPKI（Public Key Infrastructure）による暗号・認証機能や、被害が拡大する前に早期にサイバー攻撃を検知する攻撃検知機能が有効である。PKIによる暗号・認証機能は、安全な通信を実現する暗号・認証機能だけでなく、暗号・認証鍵を生成する鍵生成機能、安全な鍵の生成

に必要な乱数生成機能から構成される。ここで、暗号・認証機能、鍵生成機能には政府推奨暗号等の安全性が確認されたアルゴリズムが公開されているが、乱数生成機能の具体的な実装方法は示されていない。乱数が推測されると暗号・認証機能が強固であってもサイバー攻撃は可能となるため、IoT機器に如何に安全な乱数生成機能を実装するかが課題となっている。



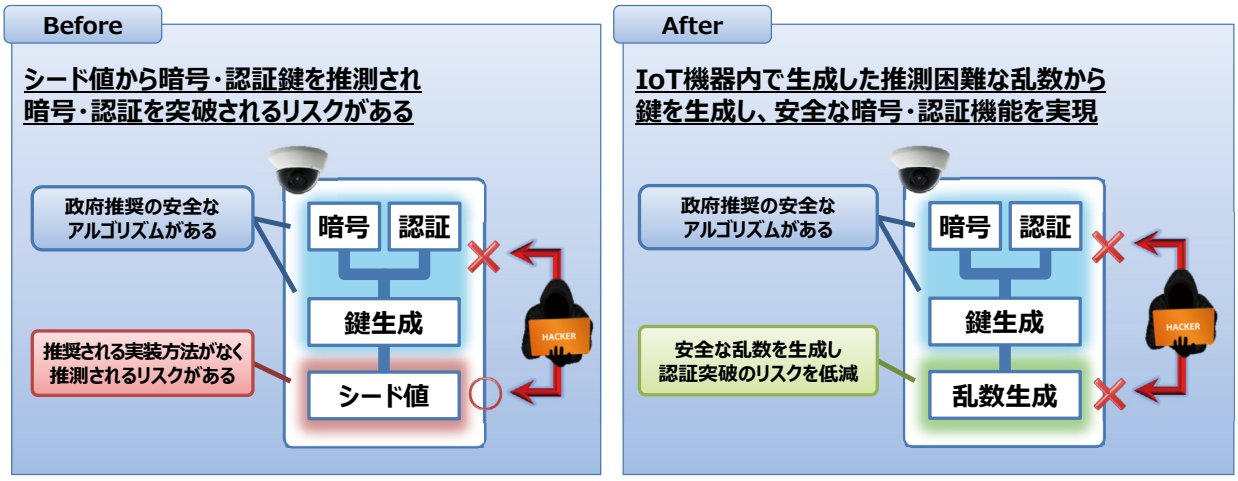
また、攻撃検知機能としてITセキュリティではPC（Personal Computer）や、各種セキュリティ機能を統合したUTM（Unified Threat Management）などのネットワーク機器からログを収集し、収集したログを一元管理・分析するSIEM（Security Information and Event Management）でサイバー攻撃を検知する仕組みが実現されている。しかし、IoT機器からのログは収集されていないため、ネットワーク機器を経由しないIoT機器間の横感染の検知やIoT機器への攻撃に対する状況把握が難しく、インシデント発生時の検知漏れや対応時間を要することが課題となっている。

そこで、安全な暗号・認証機能を実現するためにIoT機器の中で推測困難な乱数を生成する乱数生成技術、及びネットワーク機器の監視に加えてIoT機器のログも監視して攻撃を早期に検知する攻撃検知技術について開発を行った。

【研究開発の成果】

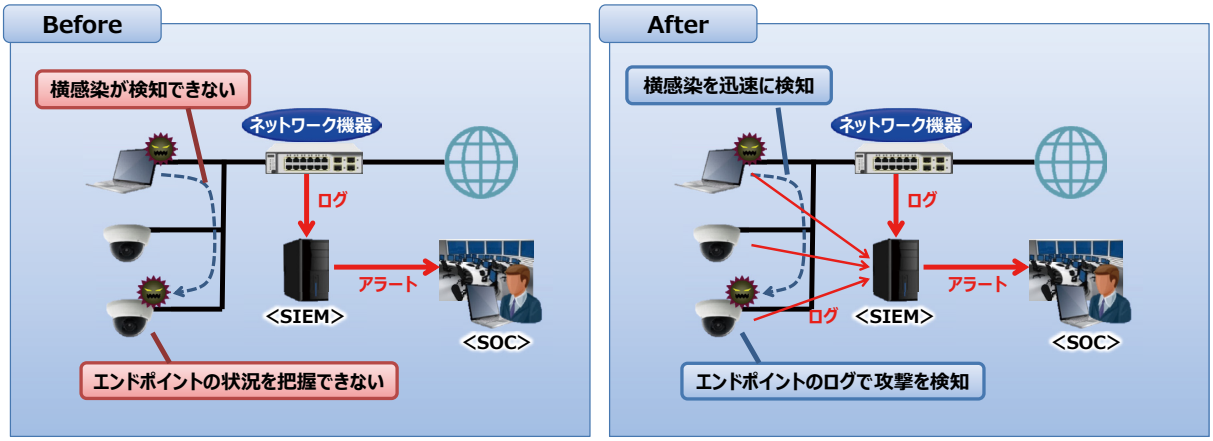
■乱数生成技術の開発

幅広いIoT機器で活用できる乱数生成技術を実現するために、一般的なIoT機器に搭載されているOSやCPUの中に乱数生成に利用できるノイズ源がないか調査・検証を行い、IoT機器が持っている標準機能を使って推測困難な乱数を生成する技術を実現した。生成された乱数は計算量的に推測が困難な複雑度を保有しており、定型動作の多いIoT機器では不確定になりやすい乱数の生成時間も実用的な時間で実現している。また、専用のハードウェアを必要としないので、コストをかけずに実装することができる。本技術を適用することで、推測リスクの少ない乱数でIoT機器の安全な暗号・認証機能を実現することができる。



■攻撃検知技術の開発

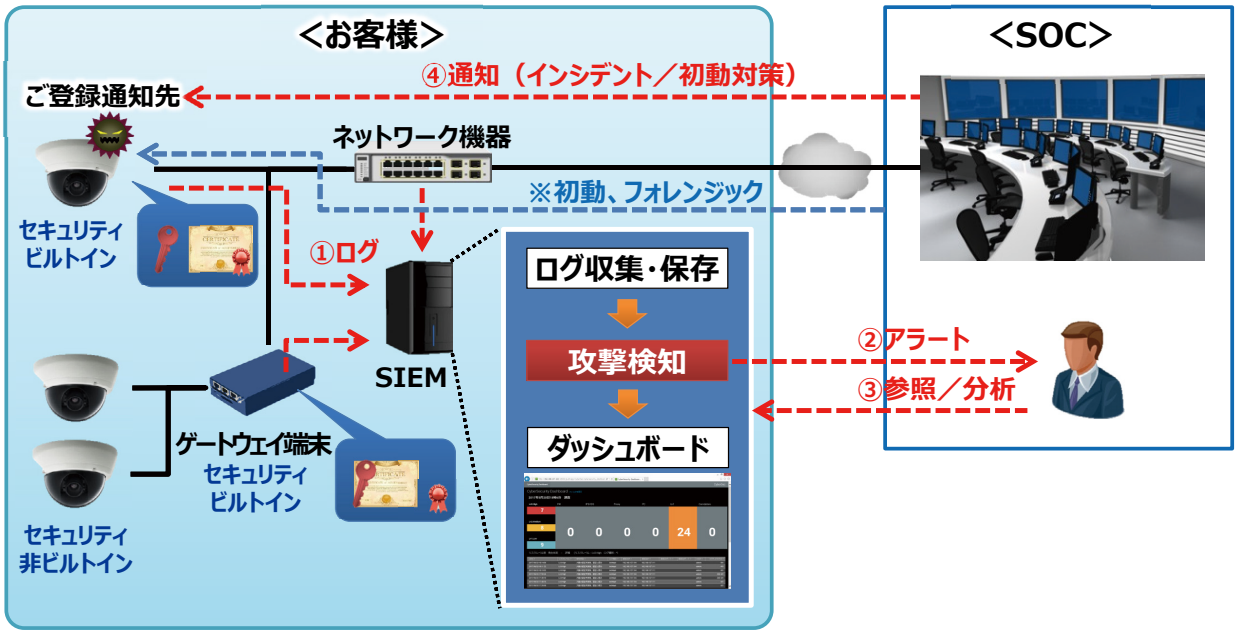
PCに加え、CPUやメモリのスペックが低いIoT機器からログを収集するために、IoT機器に対する攻撃者の不審な挙動、攻撃シナリオの分析を行い、攻撃シナリオから検知に必要なログ種の絞り込みを行った。検知に必要なログを出力する機能をIoT機器に実装し、絞り込んだログによる検知アルゴリズムをSIEMに実装することで、IoT機器向けの攻撃検知技術を実現した。ネットワーク機器に加えIoT機器からもログを収集することで、インシデント対応時間を50％程度削減している。また、IoT機器もITと同様の形式でログを出力するので、既存のSOC（Security Operation Center）を活用してIoT機器のインシデントに対応することも可能となっている。



SIEM（Security Information and Event Management）：ネットワーク機器やデバイスから得たセキュリティ情報を収集、脅威となる事象を分析・通知する装置
SOC（Security Operation Center）：セキュリティ・オペレーション・センターの略。各種機器のログ等を分析、脅威の調査や対策提言を行う組織

【実用化事例】

本技術を適用したサイバー攻撃検知サービスの提供を2019年10月に開始した。IoT機器に乱数生成機能とログ出力機能を実装し、SIEMに攻撃検知アルゴリズムを実装することで、IoT機器の安全な通信と攻撃検知を実現している。また、乱数生成機能とログ出力機能をゲートウェイ端末に実装することで、既設のIoT機器にも適用可能である。



【本技術の適用範囲・導入条件】

本技術は汎用的なCPU、OSを搭載したIoT機器や、OSを搭載していないIoT機器に適用可能である。但し、一部のCPU、OSの機能では動作しない場合があるため、詳細についてはお問い合わせ下さい。

【今後の展開】

本技術を適用したサイバー攻撃検知サービスの販売拡大を推進していく。

【お問い合わせ先】

パナソニック株式会社　コネクティッドソリューションズ社　イノベーションセンター
info_sip_cybersecurity@ml.jp.panasonic.com

3．9　研究開発技術の社会実装を促す適合性確認のあり方の研究開発

（b1）研究開発技術の社会実装を促す適合性確認のあり方の研究開発
委託先：国立研究開発法人産業技術総合研究所
再委託先（共同実施先）：学校法人湘南工科大学

【研究開発の目的】

重要インフラ等におけるサイバーセキュリティの確保に関して、従来になく有効で、かつ、速やかに社会実装が可能な適合性確認の仕組みを調査、評価することを本研究開発の目的とする。

【研究開発の内容】

実施項目1「ＳＩＰ／重要インフラ等におけるサイバーセキュリティの確保」に関する適合性確認の仕組みおよび社会実装のあり方の調査と評価

（1）「ＳＩＰ／重要インフラ等におけるサイバーセキュリティの確保」の技術に関する動向実態調査
（2）「ＳＩＰ／重要インフラ等におけるサイバーセキュリティの確保」の技術に関する適合性確認の仕組みと社会実装のあり方の調査と評価
（3）「ＳＩＰ／重要インフラ等におけるサイバーセキュリティの確保」の技術に関する国際標準化活動

実施項目2　適合性確認に必要となる各種ツールの研究、新旧混在系を含むセキュリティ強化策の研究、関連ガイドライン・基準の比較分析、評価

（4）適合性確認の仕組みに必要となるツールの研究（要求分析プロセス支援ツール）
（5）適合性確認の仕組みに必要となるツールの研究（セキュリティ・セーフティ可視化支援ツール）
（6）適合性確認に用いられる主要ガイドラインの比較分析と提言

【研究開発の成果】

（1）「ＳＩＰ／重要インフラ等におけるサイバーセキュリティの確保」の技術に関する動向実態調査

欧米ではセキュリティのマネジメントフレームワークと最先端脅威の分析技術の開発が進んでおり、日本はそのキャッチアップが急務である。日本での制度・基準の設計にあたり、次の3点が重要である。

第一に、日米欧の基準の対応関係を明確化し、相互運用性を向上することが重要である。サイバーセキュリティは本質的にボーダレスであり、今後の国際商取引のさらなる活発化に鑑みると、欧米基準とのギャップを低減し、欧米の各基準へもスムーズに適合できる基準と仕組みづくりが重要である。

第二に、公的強制と自主規制の最適なバランスが重要である。日米欧とも、基準と適合性確認の仕組みは、法律に基づく強制基準、業界の自主規制基準、事業者毎の内部基準の3階層で構成され、政府、業界、事業者の三者が連携し、役割分担し推進されている。2019年6月施行のEUサイバーセキュリティ法では、認証フレームワークに3段階の認証を設けている。第三者評価と自主評価による認証の使い分けは、上記バランスを考慮した結果であろう。

第三に、セキュリティとセーフティの相互影響を考慮した、セキュリティ規格とセーフティ規格の関連付けが重要である。サイバーフィジカル時代には、セキュリティとセーフティを両立する、製造や適合性確認が必要となる。

サイバーセキュリティの脅威は、多様化・高度化し、攻撃対象が拡大している。攻撃対象は、ITシステムだけでなく、IoTや制御システムなどあらゆるものが攻撃対象になり、実際に世界中で数多くの攻撃が行われている。車、ATM、送電、その他制御システムについても、脆弱性や具体的な攻撃法が提示されている。また、セキュリティを製品に作り込むことも重要ではあるが、新たな脅威に対して完全に予防するのは限界があるので、早期発見・対処がトレンドになっている。

（2）「ＳＩＰ／重要インフラ等におけるサイバーセキュリティの確保」の技術に関する適合性確認の仕組みと社会実装のあり方の調査と評価

制度面における適合性確認の仕組みの設計において重要なポイントは、①で述べた。EUのサイバーセキュリティ認証フレームワークのような、第三者評価と自主評価による認証のレベル分けは、今後のひとつのあり方であろう。また、SIP開発技術と規格との関係については、 1）（a1）真贋性判定技術とSP800-53の対応関係分析、 2）②の政府統一基準とSP800-53を参考に（a2）動作監視・

解析技術の適合性確認のケーススタディを実施した。

重要インフラシステムのサイバーセキュリティには、基準に基づく組織的防御と要素技術に基づくシステム防御に加え、運用保守体制に基づく復旧対応が必要である。異常が検知されても、復旧対応が迅速に行われないと、社会に混乱を来たす。監視製品/サービスには復旧対応を要件にすべきであり、政府統一基準にも盛り込むべきであると結論した。

（3）「SIP／重要インフラ等におけるサイバーセキュリティの確保」の技術に関する国際標準化活動

法的強制のある認証機関及び私的認証機関について、国際間相互認証のための方法を検討した。各産業界の標準は、各国の規制に従うものの、業界毎・分野別に国際標準化の検討を進めることが望ましい。重要インフラ等におけるサイバーセキュリティの確保でも、海外との整合は重要であり、規格の国際標準化が強く求められ、官民一体の交渉と調整が必要である。②の監視製品/サービスに対する復旧対応の要件化については、適用する重要インフラセクターの標準化委員会でインフラ特有の必要事項を標準化する一方、重要インフラ共通で利用される技術部分については、セキュリティを対象とする委員会で標準化すべきと結論した。

（4）適合性確認の仕組みに必要となるツールの研究（要求分析プロセス支援ツール）

自然言語処理のトピックモデル分析を使い、システムの規格への準拠性確認や規格間の関係を評価する、要求分析プロセス支援ツールを適用試行し、確認を完了した。本ツールにより、単一規格内の自己相関分析及び複数規格間の突合分析を可視化することが可能となる。また、ツールの利用により、規格間の整合性を確認し易くなり、自組織のガイドラインの見直しや更新を効率良く行うことが期待できる（規格間の整合性確認は、手作業の5%程度の期間で実施可能）。

ツールによる自動化で誰が実施しても同等の結果が得られるが、規程間で記述方法が異なる場合に事前処理が必要となる課題もある。有意な結果を得るには、まだ、分析対象のセキュリティ全般の知識を有する技術者による実施が必要である。

（5）適合性確認の仕組みに必要となるツールの研究（セキュリティ・セーフティ可視化支援ツール）

セキュリティとセーフティの双方の観点からの適合性確認を行うツールの基本原理を構築し、適用性の検証を行った。本ツールは、製品開発で今後より一般化するであろうセキュリティ バイ デザインを前提とした（24ページ主要成果1参照）。

（6）適合性確認に用いられる主要ガイドラインの比較分析と提言

（4）のツールを使って、サプライチェーンに係るセキュリティ要件を対象とした米国のSP800-161とISO/IEC 27036とを、政府のセキュリティ要件を対象とした我が国の政府統一基準と米国のSP800-53とを、それぞれ比較分析した。SP800-161とISO/IEC 27036との比較では、異なるプロセスモデルに基づくものの、相補的関係にあり、併用が可能かつ有用であることが確認できた。本成果は、SIPプロジェクト内で紹介して、他の研究課題で活用された。また、政府統一基準とSP800-53との比較では、緊急時対応計画・プライバシー等について、SP800-53の方がより詳細に規定している。これらの要件は運用時には対応が必須であることから、本研究開発の成果として、政府統一基準に関連する要件を早急に追加することを提言する。

この手法は、ある基準に適合した製品を別の基準にも適合させたい場合に、広く活用できる手法である。また、基準の比較分析結果自体も、重要インフラの開発企業だけでなく、基準を作る側にも参考情報になる。

【実用化事例】

なし（研究開発をサポートする技術であり、本研究開発で試行した）。

【本技術の適用範囲・導入条件】

調査及び分析手法の研究なので、適用範囲の制限はない。導入条件も特にない。自然言語処理技術は、（4）のツールである必要はなく、市販の自然言語処理技術も仕様によっては適用可能である。

【今後の展開】

重要インフラ事業者からの要求に応じて、普及展開を共同研究として実施する。

【お問い合わせ先】

国立研究開発法人 産業技術総合研究所　サイバーフィジカルセキュリティ研究センター
cpsec-inquiry-ml@aist.go.jp

3．10　緊急度の高い脅威情報を迅速に配信し、重要インフラ事業者を防御

（b2）情報共有プラットフォーム技術

委託先：株式会社日立製作所

再委託先（共同実施先）：株式会社日立システムズ

【研究開発の目的】

近年、重要インフラシステムに対するサイバー攻撃が増加、高度化しており、実被害が発生するようになってきた。

国内では、2015年6月に年金機構においてマルウェア感染による大規模な情報漏えい事故が発生している。本事件では、同一のマルウェアに多数の組織が感染し、被害を拡大させたが、その原因の一つに、他組織での被害の状況や原因などの脅威の情報が共有されなかったために対策が後手に回ったことが挙げられる。

このように、高度化しその影響が広範にわたる重要インフラへのサイバー攻撃の脅威へ対抗するためには、個々の重要インフラ事業者が単独でセキュリティ対策を講じている現状では対処しきれない状況になってきている。

このような状況に対し、2015年9月に閣議決定された「サイバーセキュリティ戦略」においても重要インフラを防御するため、「効果的かつ迅速な情報共有の実現」が項目として掲げられている。

このように、関連する重要インフラ事業者等の間で脅威やインシデント等の情報を共有し、他組織で発生した事象や兆候をいち早く共有することで第二・第三の被害を未然に防止すること、さらには、対策技術も共有して事前対処性にも優れた耐性の強いシステム運用を実現することが期待されている。

本研究では、異なる重要インフラ分野の事業者間で円滑に、脅威情報やインシデント等の情報共有を行うためのあり方の検討、および情報共有プラットフォーム技術を研究開発し、我が国のサイバーセキュリティ対策の促進に貢献する。

【研究開発の内容】

目的を達成するために、以下の研究を実施した。

（1）情報共有ツールの開発：国際的な標準フォーマットであるSTIX*1/TAXII*2を採用したツールを開発。該ツールを核としたプラットフォームを構築し、運用実験を実施し、その結果を反映した。運用実験のイメージを図10-1に示す。

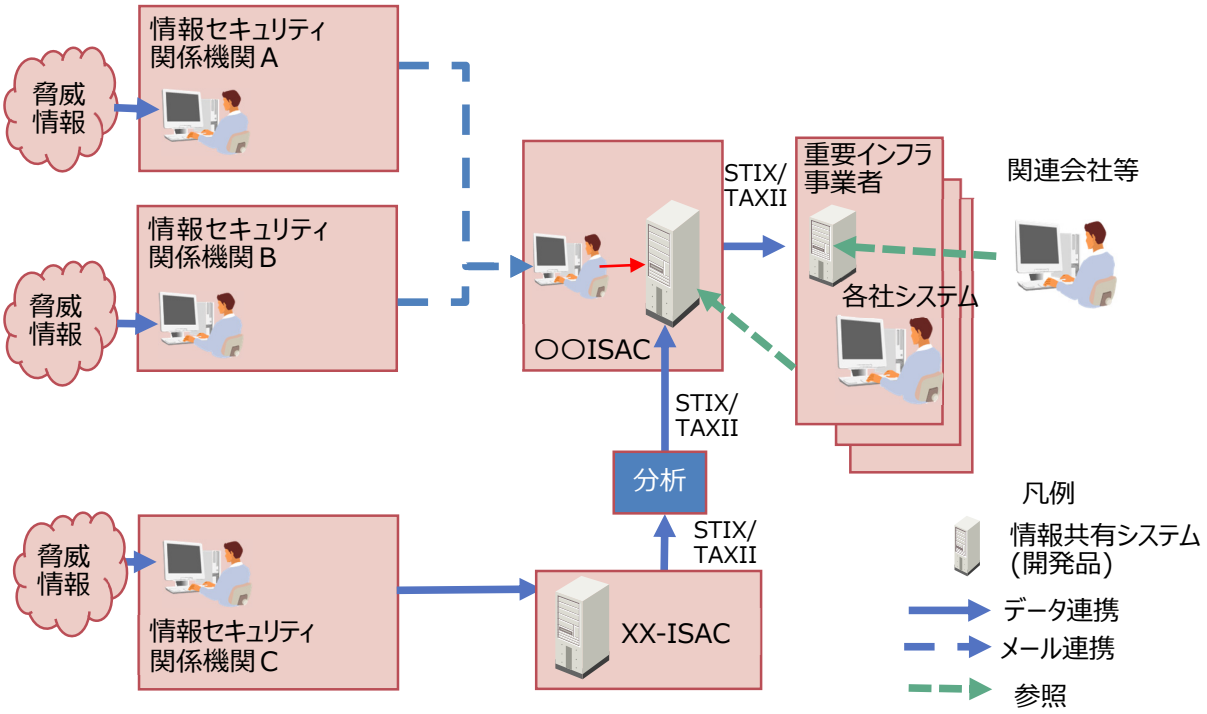


図10-1　運用実験

開発したプラットフォームは、以下の特徴を有する。

- 情報を機械処理可能な標準フォーマットとすることで、事業者/ISAC[*3]間で機械的に情報処理が可能。
- 情報の標準フォーマットとして、機械処理可能な最新の国際標準であるSTIX/TAXIIを採用し、海外との情報共有も容易に可能とする。

（2）社会実装に向けた関係組織の支援：情報共有機能の立ち上げを支援するドキュメントとして、情報共有デザインガイドを作成。情報共有デザインガイドは、構築編と運用編の2部構成とし、組織内での仕掛けの構築と実運用の設計や、利用者のコミュニティでの活動等での普及活動で利用可能としている。

【研究開発の成果】

- 社会実装として、開発した情報共有ツールを活用したプラットフォームに、検証結果を反映し、情報分析等の付帯サービスを組合わせた商用サービス「SHIELD 情報共有サービス」の販売を開始した。
- 国内外の情報共有に関する調査を実施し、社会実装に利する情報共有デザインガイドを作成し公開した。

【実用化事例】

開発した情報共有ツールを活用したプラットフォームに、検証結果を反映し、情報分析等の付帯サービスを組み合わせた商用サービス「SHIELD 情報共有サービス」の販売を開始した。

この「SHIELD情報共有サービス」を以下に示す。

（1）概要

本研究開発を通じて、世界中から報告されるセキュリティ情報を異なる組織間で迅速かつ安全に共有するための情報共有基盤を開発した。株式会社日立システムズより、この基盤を実装した「SHIELD 情報共有サービス」を重要インフラ事業者やサイバーセキュリティ関連組織向けに提供開始した。

（2）本研究開発の成果

今回開発した情報共有基盤は、外部の情報機関からの提供や他の企業・組織が共有したサイバーセキュリティ情報を蓄積し、利用者が必要な時に必要な情報を検索・周知するための基盤。本基盤は、国際標準規格であるSTIX・TAXIIを採用しているため、国内外の脅威情報および対策方法について、STIX・TAXIIを採用する他の情報機関から受信し、注意喚起として一斉自動配信する機能を備えている。

（3）SHIELD 情報共有サービス

重要インフラなどにおけるサイバーセキュリティの確保を支援する。

「SHIELD 情報共有サービス」は、情報発信機関・ISAC・事業者の各組織の連携により、サイバー攻撃に対し全体のレジリエンスを向上させ、業種横断でサイバー攻撃に備えることができる。

① 概要・特長

セキュリティ脅威情報やインシデントの情報共有システムをクラウド環境で提供。

〇情報共有システム

- 定型フォーマット（STIX/TAXII）にて脅威情報を受信し、利用者に配信することが可能。
- 脅威情報を蓄積し、関連性分析機能で簡易解析を行える。
- 脅威情報からセキュリティ機器の設定形式に変換（YARA*4ルール）することが可能。

〇組織内SNS*5

利用者間で脅威の傾向や攻撃兆候の議論、組織内での作業指示などのディスカッションを行うことができる。

〇サービス提供イメージ

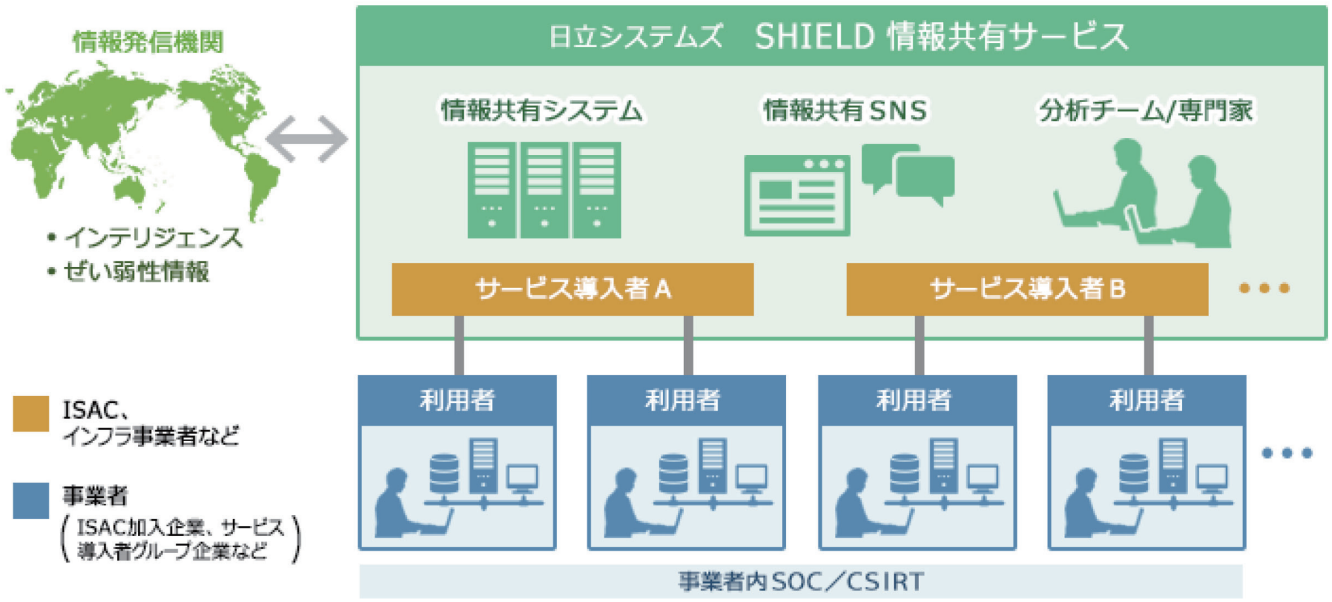


図10-2　SHIELD 情報共有サービス　提供イメージ

② 機能詳細

「SHIELD情報共有サービス」は、以下の機能を有する。

- 脅威情報の蓄積・検索

脅威情報を蓄積することにより、特定のメッセージを検索することが可能。また、過去の脅威情報を確認することにより、対策判断の時間を短縮することができる。

- 脅威情報のアグリゲーション

大量の脅威情報に埋もれないように、重複情報や過去の類似脅威情報を確認することができる。脅威情報の閲覧時に重複や類似の情報が確認できるため、対策判断の時間短縮にもつながる。

- ファイルの添付、ダウンロード機能

脅威情報の新規作成時にMicrosoft Word、Excelファイルなどを添付することが可能。また、情報提供機関が添付したファイルもダウンロードして参照することができる。

- 脅威情報のエクスポート

脅威情報の一覧をCSV形式でエクスポートすることができる。また、脅威情報の詳細をJSONおよびCSV形式でエクスポートすることが可能で、その情報を他システムへ提供することにより、対策管理の工数低減が可能。

- 機器設定支援

脅威情報からセキュリティ機器の設定形式に変換（YARAルール）することができる。YARAルールに

対応したセキュリティ機器であれば、対策の適用が容易になる。

③　関連サービス

セキュリティソリューション「SHIELD」は、株式会社日立システムズが提供する、セキュリティ導入時のコンサルテーションからポリシー作成、システム構築、運用まで、専門家による豊富なノウハウでお応えするワンストップソリューション。

＊1：Structured Threat Information eXpression (trademark of The MITRE Corporation)
＊2：Trusted Automated eXchange of Indicator Information (trademark of The MITRE Corporation)
＊3：Information Sharing and Analysis Center (アイザック)
業界ごとにサイバーセキュリティに関する情報を共有し、サイバー攻撃への対策および安全性向上のために協働活動を行う民間組織。
＊4：マルウェア解析・検知ツール。YARAルールという文字列と条件/条件演算子/正規表現などを用いてマルウェアを検出する。
＊5：Social Networking Service

【本技術の適用範囲・導入条件】

サイバー攻撃の巧妙化や先進化、そして組織化が進んでおり、企業が単独で対策するには限界がある。「SHIELD 情報共有サービス」は、情報発信機関・ISAC・事業者の各組織の連携により、サイバー攻撃に対し全体のレジリエンスを向上させ、業種横断でサイバー攻撃に備えることができる。

対象の企業/団体さま
・政府系脅威情報配信機関のお客さま
・各種ISACのお客さま
・重要インフラ事業者のお客さま

【今後の展開】

本研究開発の成果を活用し、株式会社日立システムズは、同社のサイバーセキュリティソリューション「SHIELD」のラインアップの一つに「SHIELD 情報共有サービス」を追加し、提供を開始した。今後継続し展開する。
https://www.hitachi-systems.com/solution/s0308/threat_share/index.html

【お問い合わせ先】

株式会社日立製作所 セキュリティに関するお問い合わせフォーム
https://www8.hitachi.co.jp/inquiry/it/security/form.jsp?q=toi04/

株式会社日立システムズ SHIELD 情報共有サービス 資料請求・お問い合わせ
https://www.hitachi-systems.com/form/contactus

3．11　重要インフラでの実践力を養うセキュリティ人材育成

（b4-1）セキュリティ人材育成（セキュリティ人材育成）
委託先：学校法人慶應義塾
再委託先（共同実施先）：情報セキュリティ大学院大学

【研究開発の目的】

重要インフラ等のオペレーションに従事する技術者に対してセキュリティに関連する知識及びスキルを習得させ、業務においてセキュリティを意識した活動を可能とする人材の育成を目指すため、そのカリキュラムの研究開発を行った。また、その実施のための講義・演習教材の研究開発、それを支援するためのe-learning環境の研究開発、セキュリティ関連コミュニティ機能の研究開発を実施した。

【研究開発の内容】

重要インフラ等のオペレーションに従事する技術者(OT) をターゲット人材とし、業務においてセキュリティを意識した活動を可能とする人材の育成を目標として、
（1）セキュリティとは何かを理解できる
（2）定常的にセキュリティを意識できる
（3）対応・対策に貢献できセキュリティ専門家とコミュニケーションできる
ようになることを目的とする。

これを実現するため、以下の開発項目を実施した（図1）。

（1）カリキュラムの研究開発
重要インフラ等のオペレーションに従事する技術者に対してセキュリティに関連する知識及びスキルを習得させ、業務においてセキュリティを意識した活動を可能とする人材の育成を目指すため、そのカリキュラムの研究開発を行った。

（2）講義・演習教材の研究開発
開発項目（1）において開発されたカリキュラムに基づいてテキスト、スライド、演習教材及び指導要領の開発を行った。

（3）E-Learning System機能の研究開発
参加者の状況に合わせて柔軟に受講が可能となるようにe-learningシステムを開発するとともに、実施項目（1）（2）で開発したカリキュラム・教材に基づいたコンテンツを作成した。

（4）セキュリティ関連コミュニティ機能の研究開発
開発したカリキュラム・教材に基づく人材育成コースに参加し修了した後も、最新の情報を得たり、それに伴ったスキルを獲得したりできる環境を活用するとともに、インシデント時の連携支援機能、キャリアパス関連情報共有等の機能を追加し、具体的なセキュリティ関連活動において有効に作用する機能の開発を進め、セキュリティの知識を持つ人材、特にセキュリティ教育を行うことができる人材の発掘、評価、育成、活用ができるコミュニティの構築のための基礎整備を行った。特に、定常的な教材更新のためインシデントデータベース基盤を元に、そこでの情報の整理、教材化のための議論ができる環境の整備を行った。

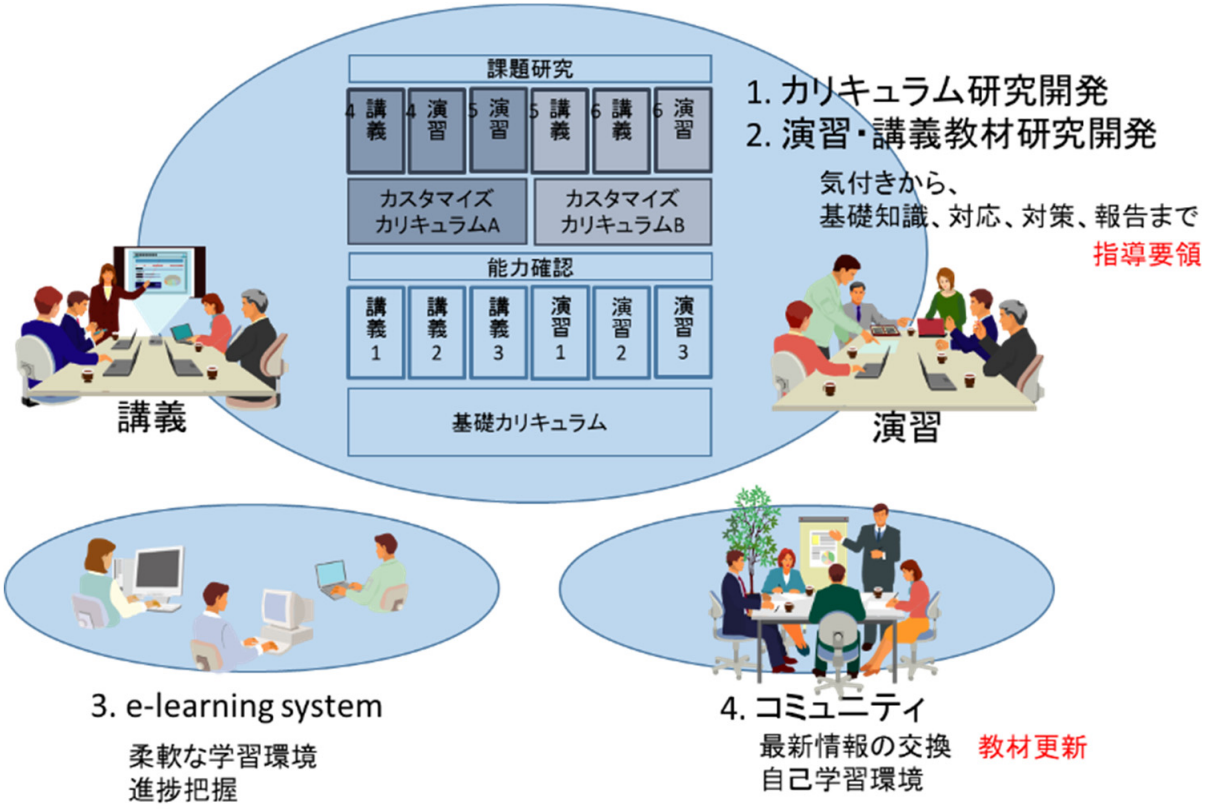


図 1：研究開発概要

【研究開発の成果】

開発したカリキュラム及びそれに基づく講義・演習教材として以下の教材を作成した。

1.テキスト・スライドを核とした指導教材

共通の基礎編、電力分野/交通分野を対象とした対策編、対応編についてテキスト、スライドとともに、指導のための参考になる指導要領で構成されている。また、各組織で現場の環境に合わせたカスタマイズをするためのカスタマイズマニュアル、理解度を確認するための演習課題例、IT分野とOT分野で異なる用語等がありこうした差異を吸収するための用語集、具体的な事例によって身近なことであることを理解するための事例集で構成されている。

図 2：テキスト・スライド教材

2. 演習教材

2.1. インシデント体験演習教材

現場で発生するインシデントを体験することにより、インシデントの発生状況を理解するための体験演習教材をe-learning型で開発を行った。現在、ランサムウェア、フィッシング、SQLインジェクション、バックドア、SDカード、ウェブカメラのシナリオが準備されているが、こうしたシナリオを充実するとともに、シナリオを開発するためのマニュアルを整備している。

図3：インシデント体験演習教材（ランサムウェア）

2.2. シナリオ型演習教材

実際のインシデントが発生した際に、どのように振る舞うべきかを学ぶためのシナリオ型の演習教材の開発を行った。本教材は、通信分野用にカスタマイズされており、実際に通信分野で運用を行っているA社のためのカスタマイズを行い、評価を行っている。また、他の組織でも利用できるようにするための汎用化とカスタマイズ手順マニュアルの整備を行った。

以上の教材を活用するために、ビデオオンデマンド型のe-learningシステムを開発した。本システムは、単にオンデマンドビデオ型の教材を視聴する機能を提供するだけでなく、受講者の視聴状況、課題の出題及び提出、提出状況の管理を行う状況を備えている。また、開発した教材に基づいたコンテンツの作成を行い利用できるようにしている（図4）。

さらに、刻々と変化する状況に対応するために教材の更新を進めるためのコミュニティによる教材の更新プロセスの確立を行った（図5）。ここでは、実際に発生したインシデントなどの具体的な例を分析し、その度合いに応じて教材を更新していくように設計されている。そのため、発生したインシデントのレベルに応じて、教材の更新方針を決定するマニュアルの整備を行っている。

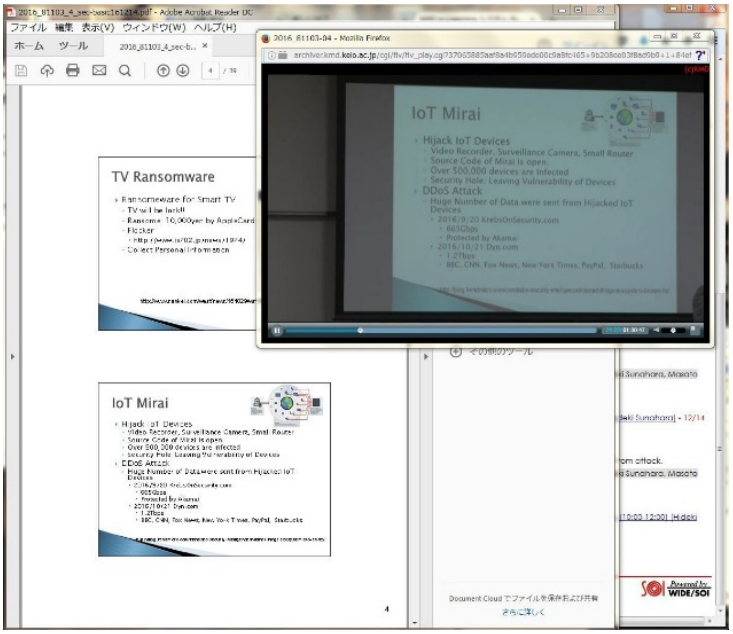


図４: e-learningシステム

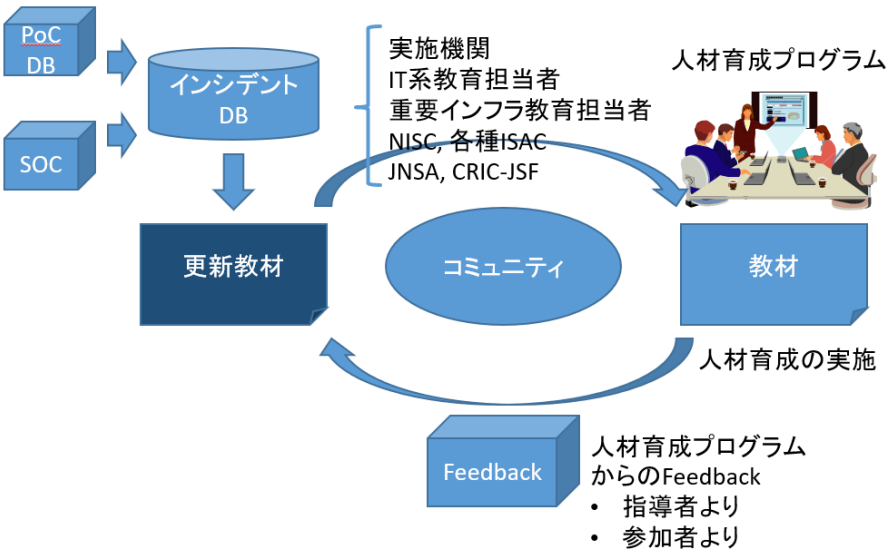


図５: カリキュラム及び教材の更新メカニズム

【実用化事例】

テキスト・スライドを核とした指導教材は、すでに延べ40以上の組織への配布を完了している。また、これらの教材を用いた講座も実施しており、教材等への意見のフィードバックを得るとともに、教材の更新を行っている。インシデント体験演習教材については、15以上の組織で利用されており一万名以上がセキュリティインシデントの体験からセキュリティに対する心構えを学んでいる。

また、本事業で開発された教材を用いて実際に行われた人材育成コース事業が実施されており、実施組織の事業及び配布先の組織において実施された教育プログラムを通して、数百名の人材育成が行われている。一例として、実施組織において2019/2に実際されたenPiT-Pro Security/ProSec インシデントハンドリングコースにおいても開発教材を用いた講義を含めた人材育成コースを実施している。こうした事業によってOTの指導者層を含め、組織内においてリーダーを担う人材の育成が実施されている。参加者は、漠然として理解していたセキュリティインシデントに対して具体的なイメージを持ち、心構えを持って現場での対応に携わる準備が整ったとしている。

図6：enPiT-Pro Security/ProSec
インシデントハンドリングコースでの講義の様子

【本技術の適用範囲・導入条件】

本事業で開発されたカリキュラム及び教材には指導要領を含む指導のための補助的資料が含まれており、導入するだけで人材育成を開始できるように配慮されている。一方、各組織の現場に合わせたカスタマイズを可能とするためのカスタマイズマニュアルを整備しており、個別の環境に合わせた教材とすることも可能となっている。但し、各社の状況に合わせて適用させることが必要であり、今後も支援体制を整えていくとともに、こうした人材育成コースを経た指導者らによるコミュニティでの相互扶助を推進することが必要である。

【今後の展開】

開発された教材を用いて、エクステンションコースなどを通して、人材育成事業を展開していくとともに、刻々と変化する状況に対応させるため、教材を常に更新していく体制を整備していく。教材の更新は、事業を実施した大学が中核となって行うが、本教材を活用している各組織の担当者や教育コース参加者、NISCなどの政府機関、ISACなどの各分野の業界組織、JNSAやCRIC-CSFなどの業界連携組織などと連携し、定常的に更新を行える体制を展開していく。

【お問い合わせ先】

慶應義塾大学サイバーセキュリティ研究センター
E-Mail: sip-b4-text@kmd.keio.ac.jp

3．12　組織のインシデント対応能力向上をめざす人材育成プログラム

（b4-2）セキュリティ人材育成（セキュリティ人材育成の研究開発）
委託先：国立大学法人名古屋工業大学

【研究開発の目的】

制御システムもサイバー攻撃の対象になり、経済的だけでなく、物理的にも甚大な被害が発生する危険性が高まってきたという認識のもと、研究グループは、サイバー攻撃が、物理的な変化を引き起こすには、コントローラを操作するしかないという観点で、制御を専門としていた立場から、サイバー攻撃による物理的な事故を防ぐセキュリティ対策を中心に考えてきた。サイバー攻撃には、想定外が不可避で、臨機応変な対応が必要である。

サイバーインシデント対応に関する演習としては、内閣府サイバーセキュリティセンター（NISC）が大規模な分野横断型演習を、重要インフラを対象に2006年から毎年実施している。これは非常に有用で重要なものであるが、演習実施日には正解の行動をとることが求められるので、関係者はその準備に長期間を要し、1年1事業所での実施に限られるという面がある。

サイバー攻撃から守るためには、関係する多くの部局において、インシデントを想定した演習を実施することが望まれるが、この形態の演習では、展開が難しい。また、想定外がつきもののサイバー攻撃に対する準備としては、一つのシナリオでの対応を学ぶだけでは十分ではない。臨機応変な対応を実現するためには、組織のメンバーが繰り返し、異なるインシデントシナリオで、対応における組織連携の在り方を学んでいれば、想定外の攻撃にも、組織の誰かが気づき、その気づきを早期対応につなげられる組織連携体制ができると期待できる。このようなレジリエンシーが高い組織を実現できて、広く早く普及できる演習形態を開発するのが、今回の目的である。

【研究開発の内容】

演習システムを開発する際に想定した要求性能は以下のようにまとめられる。

- サイバーインシデント発生時に適切な対応をするために必要な組織連携を学習できる。
- サイバー攻撃のリスクを、演習の場で疑似体験を通じて学習できる演習で、準備を要求せず、1日でも複数のシナリオを体験できる形態で、演習の早期普及を可能にする。
- 演習実施用データ、実施結果のデータのフォーマットを揃え、蓄積＆共有できるようにする。既存のデータを参考にできれば、演習シナリオのバリエーションを広げやすくなり、実施結果のベストプラクティス等と比較することで、セキュリティ向上対策を議論しやすくなる。

【研究開発の成果】

演習の形態として、IMANE-PC,IMANE-CARD,IMANE-DEMOの3つ、演習を支えるツールとしてIMANE-DRAW,IMANE-DBの2つを開発した。演習の実施形態、振り返り画面などは、2．研究開発テーマ概要（12）に示したので、ここでは、その実現形態について解説する。

- IMANE-PC：コンピュータゲーム形式で、インシデント対応を疑似体験する演習
  このコンピュータシステムは、JAVAとJAVASCRIPTで構築されており、tomcatが稼働するシステムであれば、WindowsでもMacintosh、Linuxでもサーバーとして利用できる。また、受講生が利用するクライアントにもGoogle Chromeが利用できるものであれば、利用できる。IMANE-PCのサーバーを社内クラウドに設置し、社内のどこでも、演習を実施できる体制をとった企業も存在する。
- IMANE-CARD：カードを並べながら、インシデント対応のシナリオを検討する演習
- IMANE-DEMO：制御系がサイバー攻撃に襲われる状況を体験する演習
- IMANE-DB：IMANE-PCのシナリオデータと実施結果データを蓄積し、検索するデータベースソフト
- IMANE-DRAW：IMANE-PCのシナリオを作成編集するソフト
  draw.ioというフリーソフトとpythonの組み合わせで実現している。インシデント対応の登場人物をシーケンス図の各レーンに設定し、情報連携の流れをフローチャートとして描くと、シナリオのjsonファイルが合成される。

【実用化事例】

名古屋工業大学での研究室主催のワークショップ、IPAの産業サイバーセキュリティ人材育成センターの中核人材育成プログラム（ICSCoE）、名古屋市と名古屋工業大学主催のロボット・IoT・サイバーセキュリティ専門人材育成講座、千葉県産業振興センター主催の安全とセキュリティのための組織レジリエンス構築講座、愛知県警主催サイバーセキュリティ協議会、化学企業、石油企業、電力会社、富士通、富士通ラーニングメディアの社内研修など、多くの機会で演習を実施してきている。

IMANE-DEMOの受講生からは、以下のような意見を得ることができている。

- サイバー攻撃を目の当たりにすることで、自分のプラントにも危険性があることを実感できる。
- 攻撃に気づくための通信検知システムの重要性に気づく。
- 攻撃のデモを目の当たりして、自分のプラントを守るためのセキュリティ対策を知りたくなる。
- サイバー攻撃には想定外がつきものなので、知ることよりも考える姿勢が重要ことを理解できた。
- 簡単な装置で実現できるので、各事業所で実現できる。ぜひ、導入したい。

また、IMANE-CARD、IMANE-PCに関しては、以下のような意見を得ている。

- カスタマイズして事業所のシステムに近づけても、差異が残り、自分は違うからという受講生の反応につながるので、へたに近づけるより、アナロジーを感じることができるという対象で、インシデントシナリオを展開した方が有用
- 演習での体験から、サイバー攻撃でSCADAが利用できなくなっても、従来の安全対策で、安全は確保できることは理解できた。
- 攻撃に気づかせない攻撃も想定する必要があることを理解できた。
- OT技術者が、サイバー攻撃を意識しないと、攻撃の被害が拡大し、早期復旧を妨げる行動をしてしまう危険性があることが理解できた。
- IT技術者がフォレンジックしようとしても、情報が全く保持されていない、あるいは抹消してしまう状況がありうることが理解できた。
- 今のままではサイバー攻撃を疑えたとしても、遮断の対応をとれないが、OT技術者が、通信がなく、コントローラが利用できない状況での対応をしっかり取ることができれば、疑わしい時点で早期の対応がとりうることが理解できた。
- インシデント対応演習を展開して、関係者の意識向上につなげたい。

【本技術の適用範囲・導入条件】

重要インフラのサイバーセキュリティを対象に開発したインシデント対応演習であるが、組織連携による対応が必要な問題における疑似体験を通じた演習課題には、適用できると考えられる。制御セキュリティだけでなく、情報セキュリティの問題も考えられるし、自然災害などに対する対応にも適用できると期待できる。IMANE-PCは、GIT-HUBにMITライセンスで無料公開して、普及促進を期待する。IMANE-DEMOに関しては、業種に適したシステムの開発が望まれるが、名古屋工業大学で複数のシステムを開発し、無償貸与するとともに、企業等での開発に協力する。

【今後の展開】

IMANEシリーズの開発は今後も進めるが、IMANE-PCのシステムは、GIT-HUBで公開することで、ユーザー会を構成し、ユーザーでの維持管理を志向する。このユーザー会の中心には、このSIPのプロジェクトをきっかけに設立した名古屋工業大学発のベンチャー企業を位置づけ、企業としては、演習のシナリオ開発支援、演習実施支援などをサービスとして、収入を得るとともに、IMANEシリーズの発展を支える。

当面の公開は、IMANE-PCのシステムだけにとどまるが、IMANE-DRAW, IMANE-DBについても、さらにユーザー評価を進めたうえで、公開する予定である。

【お問い合わせ先】

名古屋工業大学 橋本芳宏
inquiry@manage.nitech.ac.jp

SIPホームページ（内閣府）
https://www8.cao.go.jp/cstp/gaiyo/sip/

SIP「重要インフラ等におけるサイバーセキュリティの確保」
ホームページ（NEDO）
https://www.nedo.go.jp/activities/ZZJP_100109.html

発行日：2020年3月26日
発行者：国立研究開発法人　新エネルギー・産業技術総合開発機構（NEDO）

〒212-8554 神奈川県川崎市幸区大宮町1310 ミューザ川崎セントラルタワー
Tel 044-520-5100
http://www.nedo.go.jp

内閣府　NEDO