戦略的イノベーション創造プログラム（SIP）

【日本電信電話】

1－1　サーバ機器の改変を常時検知して重要インフラを保護

真贋判定技術

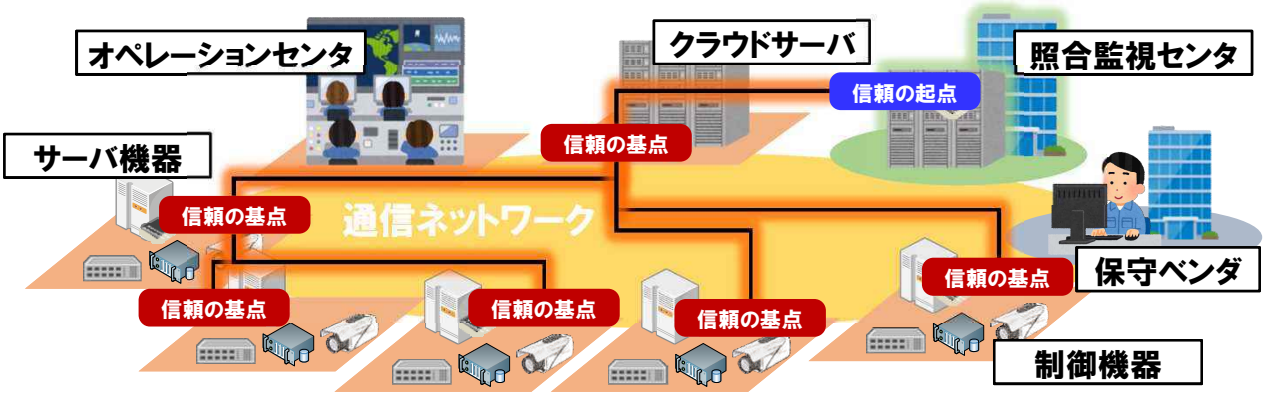
システムの不正な改変を常時検知して、バックドア通信などの異常な動作を阻止します

特長

① **システムの不正な改変の常時監視と記録保護**
システムの改変事実を常時検知して、改変に起因する異常な動作を阻止します（リアルタイム監視・防御技術）。
本技術の動作検査、及び監視記録の破壊対策等により安全確実な監視が可能です（セキュアレコーディング技術）。

② **効率的かつ確実かつ簡単な導入・運用**
本機能に必要な設定は機器間で安全に共有でき、かつ多くの機器で構成されるシステムにも効率的に導入できます（セキュアコンフィグレーションシェアリング技術）。
機器のソフトウェア構成等に応じて、本機能に必要な設定を自動調整できます（自動コンフィグレーション技術）。

導入イメージと差異化ポイント（高いサイバー攻撃耐性を備えた“きめ細かな完全性証明技術”を実現）



安全確実な改ざん検知

世界標準の最新セキュリティチップ（TPM2.0）と暗号技術を駆使して、監視記録の不正な改変などを検知し、安全確実な監視機能を実現

大規模システム全体の監視

数百～数千台レベル、1台あたり数十万の大量ファイルからなるサーバ機器に対応し、設備全体の真贋を判定可能にする「信頼の連鎖」を実現

ライフサイクル全体を監視

サーバ機器の起動から運用に至るまで、リアルタイムにソフトウェアの完全性を監視

実用化・事業化に向けた計画

	2017年度	2018年度	2019年度	2020年度～
研究成果普及	事業者提案	技術検証	試験導入 ⇒ 商用導入	
	先行導入実績をフィードバックしつつ導入拡大		重要インフラ分野展開（個別SI型）	
さらなる展開施策		OA系等の重要インフラ分野以外にも展開		既存製品連携によるソリューション化
			設備共用型による導入を実現	認証制度／照合監視センタサービス

戦略的イノベーション創造プログラム（SIP）

【日本電信電話】

1－1　サーバ機器の改変を常時検知して重要インフラを保護

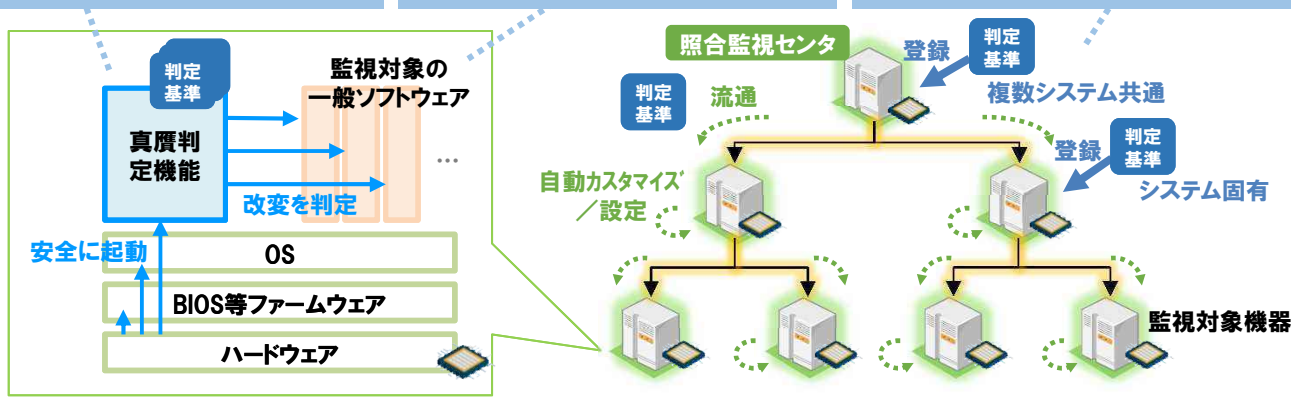
本研究開発テーマの背景

機器の配送、導入、保守を契機とした人為的改変や高度なマルウェアなどによって、バックドアを持つ不正な機器が重要インフラに混入するリスクが高まっています。特に、日本国内では東京2020オリンピック・パラリンピック競技大会に向けてそのような脅威がさらに高まると予測されており、2020年には、ファイアウォールを導入するような従来の追加型セキュリティ対策だけでなく、重要インフラ設備自体のセキュリティ強度を根本から高める新技術が必要な時代が到来すると考えられます。

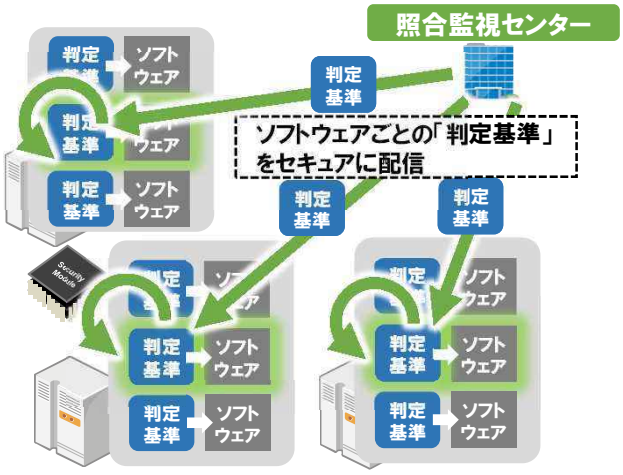
本技術の動作概要

3つの特長

真贋判定機能を安全に起動　**判定基準と比較して改変を判定**　**判定基準の安全な取得・自動設定**



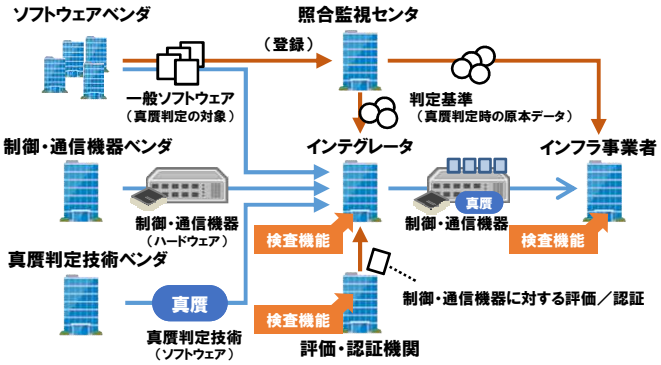
大規模システムの安全なアップデートが可能です



ソフトウェアごとの「ルール」に基づく自動設定

信頼の連鎖によって判定基準を共有し、機器ごとの差異には判定基準の自動設定で対応できます。

サプライチェーン上での検査機能を提供します



制御通信・機器の導入プロセスにおける検査

上記のような制御・通信機器のサプライチェーンにおいて、「インテグレータ」「インフラ事業者」「評価・認証機関」のそれぞれが、真贋判定技術が正しく導入され、かつ制御・通信機器の改変がないことを検査できます。

既存技術との比較

	本技術	A社製品	B者製品	C社製品
監視記録の保護	○	×	×	×
大規模システムへの導入のしやすさ	○	△	×	-
リアルタイム監視	○	△	△	×
改変ファイルの実行阻止	○	×	×	×

戦略的イノベーション創造プログラム（SIP）　【富士通】

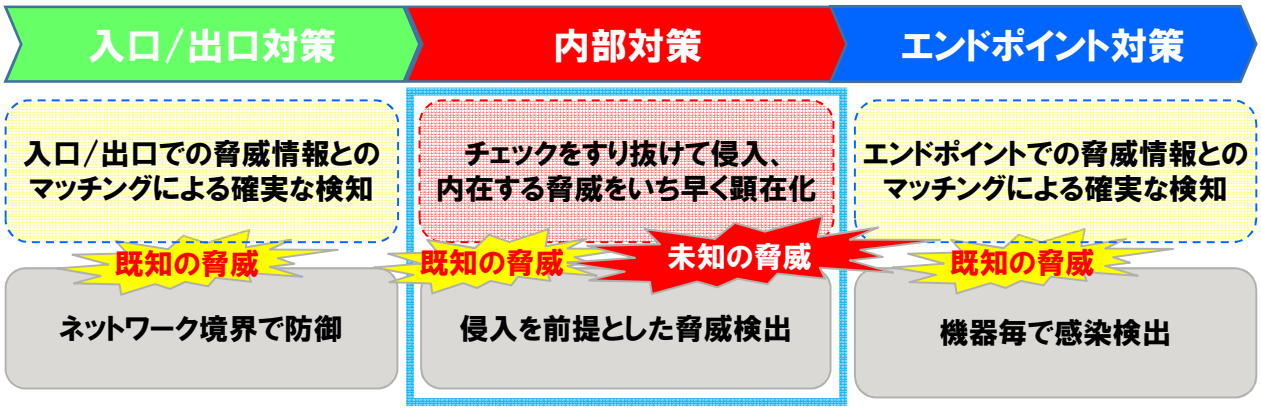
1－2　内在する脅威の早期顕在化にて業務影響を最小化

動作監視解析技術

既存のセキュリティ対策をすり抜けた内在する脅威をいち早く顕在化させ、脅威を監視・分析する高スキル業務を支援

■ 入口/出口脅威対策等を補完（多層で防御）する内部対策技術

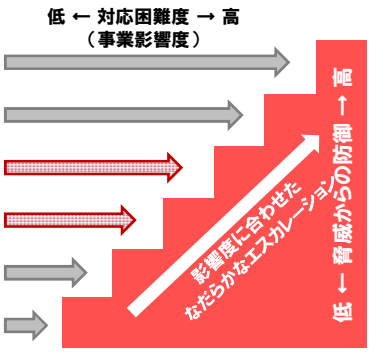
入口/出口対策、エンドポイント対策をすり抜けた内在する脅威の顕在化スピードをアップさせ、脅威レベルがエスカレーションされる前に捕獲する多層対策技術



■ 脅威を監視・分析する高スキル業務を支援

内在する未知の脅威の増加に伴い、Level-2/3の高スキル業務も増加
Level-1技術者にてLevel-2/3の業務ができるようシステムにて支援

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



■ 既存技術との違い

大規模ネットワークにおいて事前学習を必要としない数理モデルを適用

技術要素	既存技術	本研究テーマ技術
検知手法	過去挙動との差分	他機器挙動との差分
検知モデル	機械学習（事前学習要）	数理モデル（事前学習不要）
適合ネットワーク	小規模～大規模	大規模
監視対象通信	ネットワーク毎の監視	旧機器～仮想化混在に対応

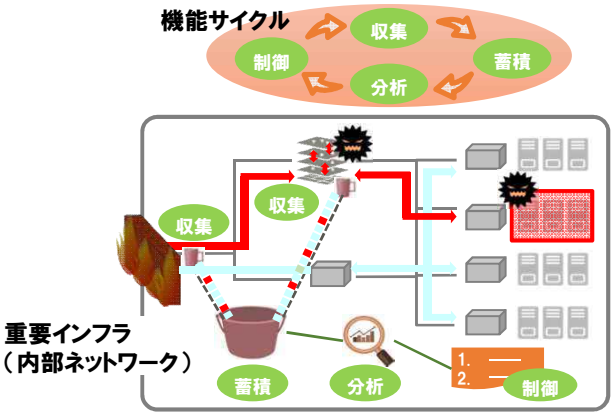
戦略的イノベーション創造プログラム（SIP）　【富士通】

1－2　内在する脅威の早期顕在化にて業務影響を最小化

動作監視解析技術

既存のセキュリティ対策をすり抜けた内在する脅威をいち早く顕在化させ、脅威を監視・分析する高スキル業務を支援

内部対策の機能サイクルと配備



技術ポイント

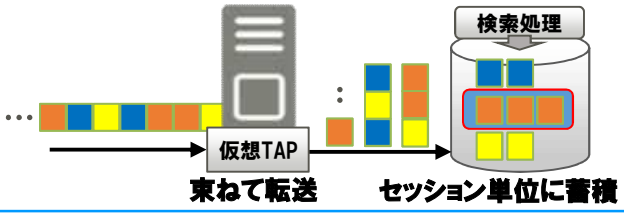
物理/仮想が混在する大規模ネットワークにおいて収集、蓄積、分析、制御の4機能サイクルを実現

① 仮想ネットワークから10Gbpsの高速でキャプチャするTAP収集技術
② 100Gbps対応高速・大容量蓄積技術
③ 事前学習を必要としない数理モデルによる分析技術
④ 脅威対策の高スキル業務を支援する制御技術

仮想ネットワークから通信を高速キャプチャ・蓄積する技術

収集　蓄積

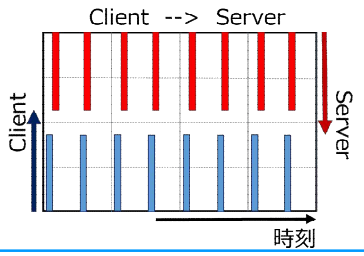
- 仮想スイッチへのアドオン技術により、高速パケットをキャプチャ、複数のパケットを束ねて転送することで仮想スイッチの輻輳回避
- セッション単位でのディスク書込み・読込みにより高速アクセスを実現



正常通信の中に紛れた不審な通信を検出する解析技術

分析

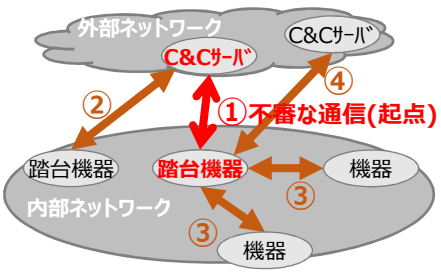
- 通信の規則性に着目（右図）、送受信相手の種類や取次状況を指標化、正常通信との識別性能を向上
- 独自の閾値調整手法（特許出願中）により、即時性の向上と精度低下の抑制を両立
- 既存セキュリティ技術で見過ごされていた、不審な通信の特定に成功（NEDO、富士通、NII　2019年11月29日プレス発表）



システムにて影響調査範囲を自動抽出

制御

- 不審な通信と相関関係にある通信をシステムにて分析・可視化することで脅威拡散被害の調査範囲を抽出し、オペレータの調査稼働を軽減



①検知した不審な通信（1次脅威）
②C&Cサーバとの通信（2次脅威）
③踏台機器との通信（2次脅威）
④SBY C&Cサーバとの通信（2次脅威）

製品展開予定

製品化予定：収集／蓄積技術 2019年度、分析／制御技術 2020年度

問合せ先：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

戦略的イノベーション創造プログラム（SIP）

【日立製作所】

1－3　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

動作監視解析技術

可用性が重視される制御システムにおいて気づきが難しい不正な動作を早期に検知します

特長　微細な挙動変化を監視、システムの免疫力を強化

① 正常業務に紛れた不正な動作を検知します

既存の技術で検知しにくい不正な動作であっても、制御システムで発生した小さな変化をとらえ、検知します（統合健全性判定技術）。

② 制御システムの特性に適した監視を行います

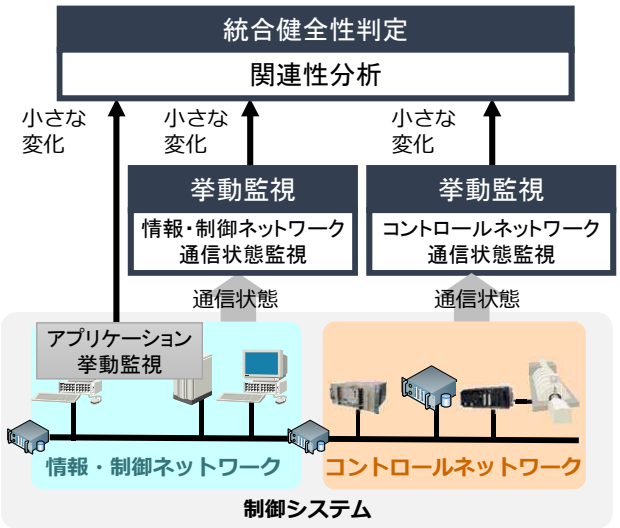
通信状態から制御システムの特性を学習、モデル化し監視することで小さな変化を検知します（挙動監視技術）。可用性が重視されるシステムに対しても、影響を最小限に導入可能です。

現在の重要インフラシステムでの課題

近年未知のウイルスが次々と生み出されるとともに、侵入方法も巧妙化しているため、侵入防御・攻撃防御技術だけで、すべての侵入を防ぐことは難しくなっています。また、外部ネットワークに直接つながっていない制御システムにおいても、侵入・攻撃リスクは高まっています。そのため、万一侵入された場合に備え、制御システムに適した侵入・攻撃検知技術が必要とされています。

課題を解決する技術

統合健全性判定技術



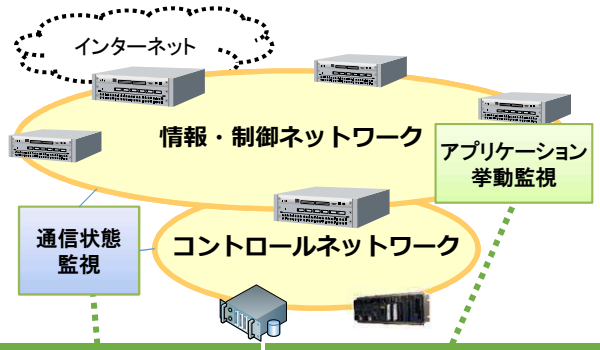
小さな変化を使って不正な動作を統合判定

小さな変化の関連性を分析することで、単一の変化だけでは見逃してしまう不正な動作を浮き彫りにしたり、過度な不正判定を抑制したりします。

挙動監視技術

制御システムに適応

制御システムの特性に応じて正常状態を学習しモデル化します。適用先に応じて通信状態監視・アプリケーション挙動監視を選択可能です。



通信状態監視

通信状態をリアルタイムに監視し、モデルと比較して、小さな変化を検知します。

アプリケーション挙動監視

通信状態に現れない機器内の活動をとらえ、小さな変化を検知します。

実施状況/スケジュール

重要インフラ事業者と協働した検証を2017年度末に実施しており、先行して研究開発が完了した技術に関して2017年度に製品化済みです。（製品：Hitachi Anomaly Detector）
製品化後も引き続き連携した活動を実施しており、現在実施中の研究成果も今後製品化予定です。

【日立製作所】

戦略的イノベーション創造プログラム（SIP）

1－3　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

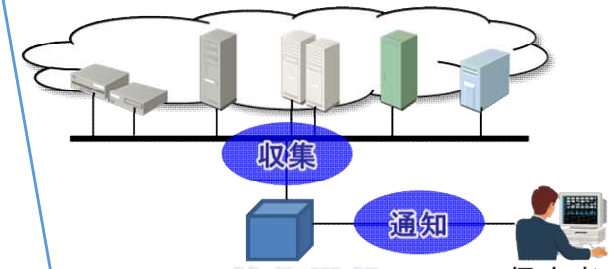
先行して研究開発が完了した技術を製品化　－ Hitachi Anomaly Detector －

SIPサイバー先行研究開発技術　多層監査膜

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

日立が長年積み上げてきた制御システムに対するノウハウを生かし、多角的な視点で業務をホワイト化

新旧機器が混在するシステム



セキュリティ監視製品
Hitachi Anomaly Detector

<特長> 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

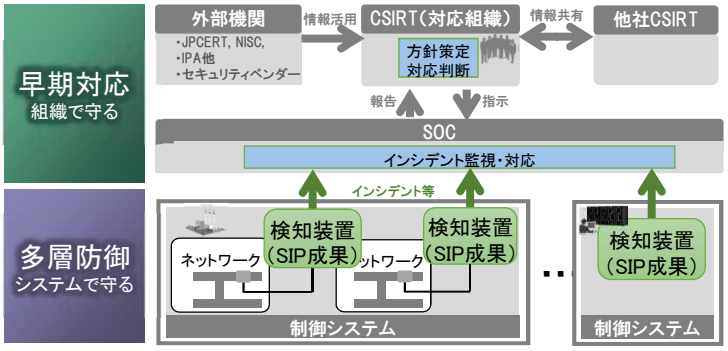
システムの安全稼働を守る

研究開発技術の適用方法

フェーズごとのガイドライン

- 設計
- 構築(確認)
- 構築(事前準備)
- 構築(導入)
- 運用

セキュリティシステム設計／構築方法や組織体制、運用設計等のポイントを解説

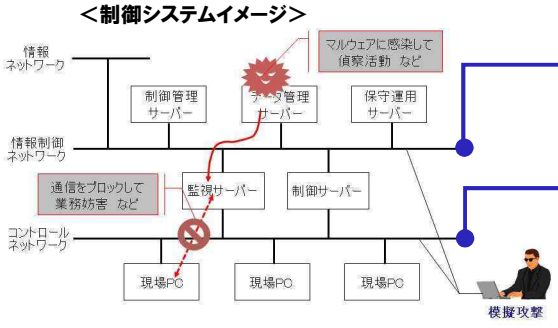


・現場の制御システムに検知装置を配置し、微細な変化を漏らさずインシデントとして検出
・SOC2) で各種インシデントを監視、統合的に判断して早期対応

展示概要

○検知装置で検知したインシデントの表示や運用方法を体感してください。

＜制御システムイメージ＞



＜検知装置構成例＞

① 模擬攻撃を実施

② 検知された模擬攻撃が運用画面に表示され、運用者視点でのオペレーションを実施

1) OT：Operational Technology
2) SOC：Security Operation Center

戦略的イノベーション創造プログラム（SIP）【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】

1－4 異常検知時においても安全な運用継続を可能とするシステム防御技術

動作監視防御技術

検知しづらい高度な攻撃から制御システム全体を保護して安全な運転を継続します

特長

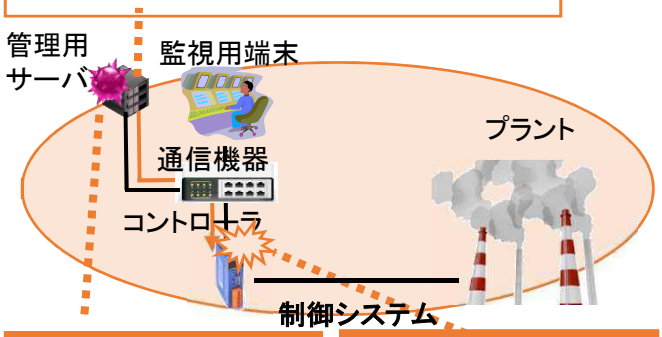
① 制御システムの異常箇所を迅速に特定
プラントの運転状態に応じて防御条件を適切に変更し、監視用端末（上位）、通信機器（中位）、コントローラ（下位）の3つのレベルで、制御システムへの命令・指示を階層的に監視。
既存技術にはない下位レベルの監視を含めた各階層の機器の特徴を活かした検査機能を利用して制御システムに対する攻撃箇所を迅速に特定し保護します（階層検査機能）。

② 異常検知時も安全な運用を継続
協調用端末により、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。
コントローラを攻撃による停止・誤動作から保護しつつ運用を継続します（協調機能）。

検知しづらい高度な攻撃に備える必要があります

正規のコマンドによる攻撃

正規のコマンドにより、防御条件をすり抜ける攻撃を仕掛けられる可能性があります。



検知困難な攻撃

高度化されたサイバー攻撃は、単一の防御条件では防ぎきれない可能性があります。

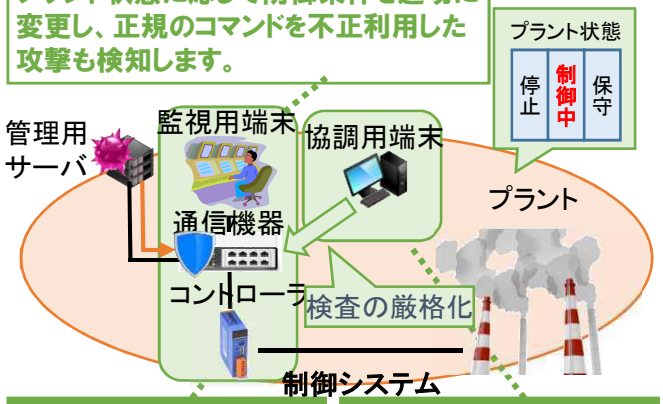
コントローラを狙うリスク

プラントの安全を維持する機器を狙ったサイバー攻撃により、大事故になる可能性があります。

高度な攻撃から制御システム全体を保護します

運転状態に応じた防御

プラント状態に応じて防御条件を適切に変更し、正規のコマンドを不正利用した攻撃も検知します。



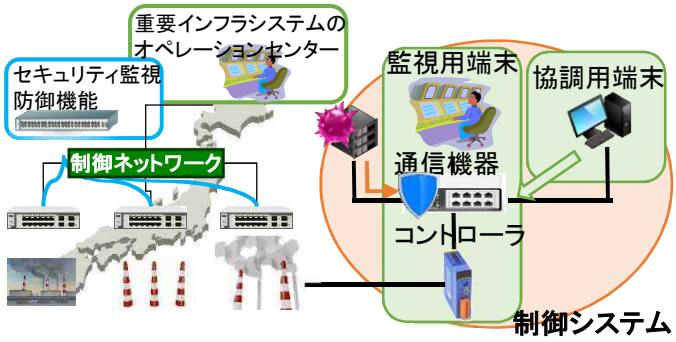
上～下まで全階層で防御

防御網を多段に設置する階層防御により、高度化された攻撃であってもすり抜けを阻止します。

現場から遠ざける防御

プラント全体を安全に稼働するため、可能な限り上位で攻撃を食い止めることができます。

社会実装に取り組みます



進捗

重要インフラ事業者と協働の技術開発を実施し、技術評価、導入・運用手順を成果目標にします。

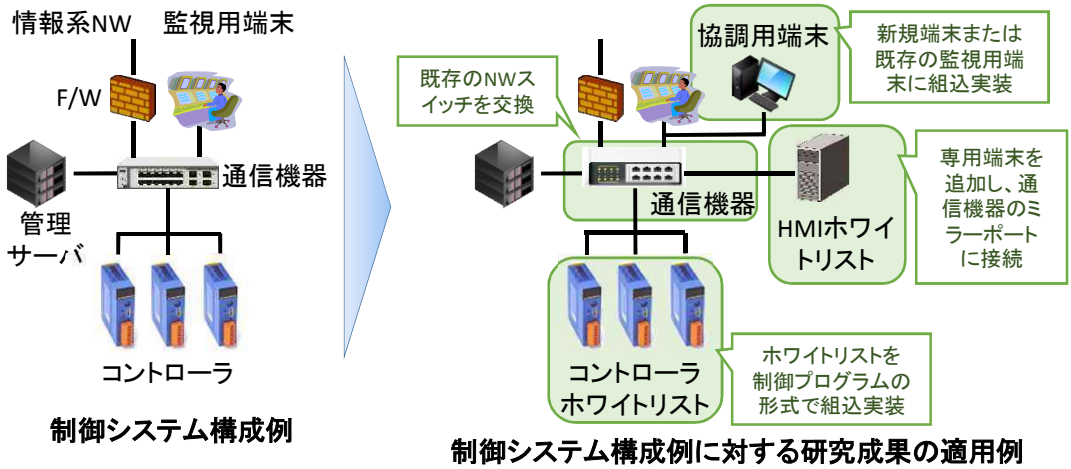
【社会実装へ向けて】
・先行して導入可能な技術から重要インフラ事業者様へ導入し、ご活用いただいています。

【研究技術について】
・協調ホワイトリスト防御機能を開発し、試験用模擬プラントに実装しました。
・複数種類の試験用模擬プラントを利用した検証を実施しました。

戦略的イノベーション創造プログラム（SIP）【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】

1－4 異常検知時においても安全な運用継続を可能とするシステム防御技術

導入イメージ

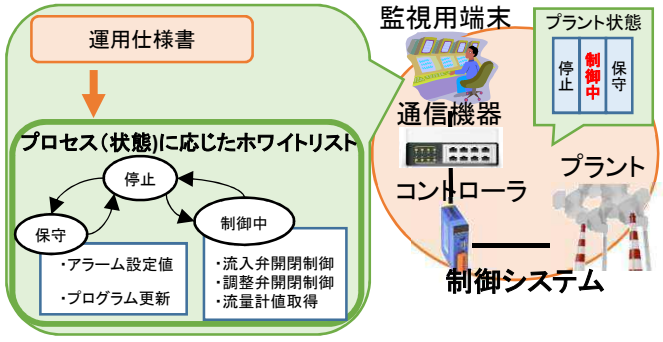


研究開発成果の導入

・3種類のホワイトリストセキュリティ機能およびホワイトリスト協調機能を導入することで、検知しづらい高度な攻撃から制御システムを守ります

・導入にあたっては、対象の制御システムに応じて必要な要素を個々に導入することも可能となります

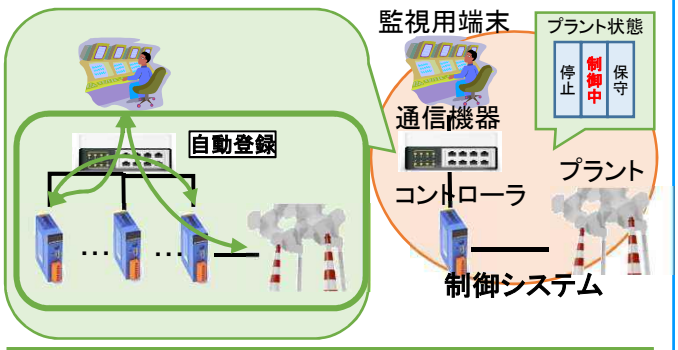
（上位）通常発生しない命令を検知・防御します



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。

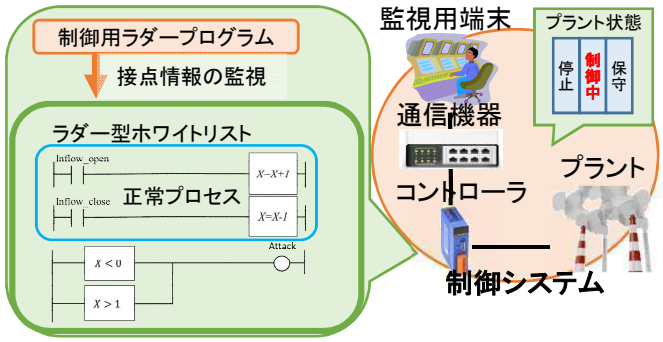
（中位）煩雑な管理なく攻撃を検知・防御します



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。

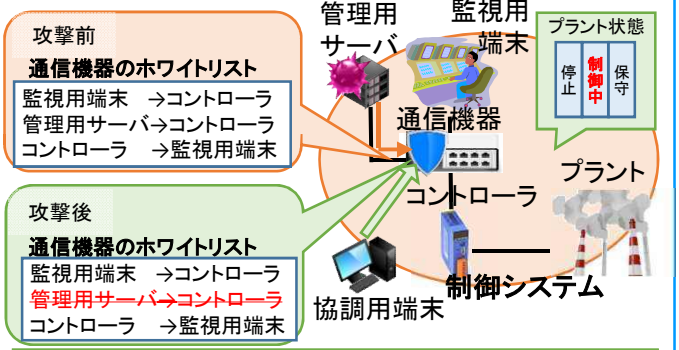
（下位）プラントの動作状態を監視・防御します



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。

2－1　モニタリング機器の追加でIoTセキュリティ監視を提供

IoT向け対策技術

多様なIoT機器に自動適応して動作を監視・解析し、セキュリティ異常を検知します。

特長

① **未知なものを含む多様なIoT機器に対応したIoTシステムの動作監視・解析**
新たなIoT機器や、用途が多様化したとしても、自動的に適応して動作を監視・解析します（IoT機器特徴学習技術）。
IoT機器自体に特別な機能を備える必要がありません（IoT機器挙動監視技術）。

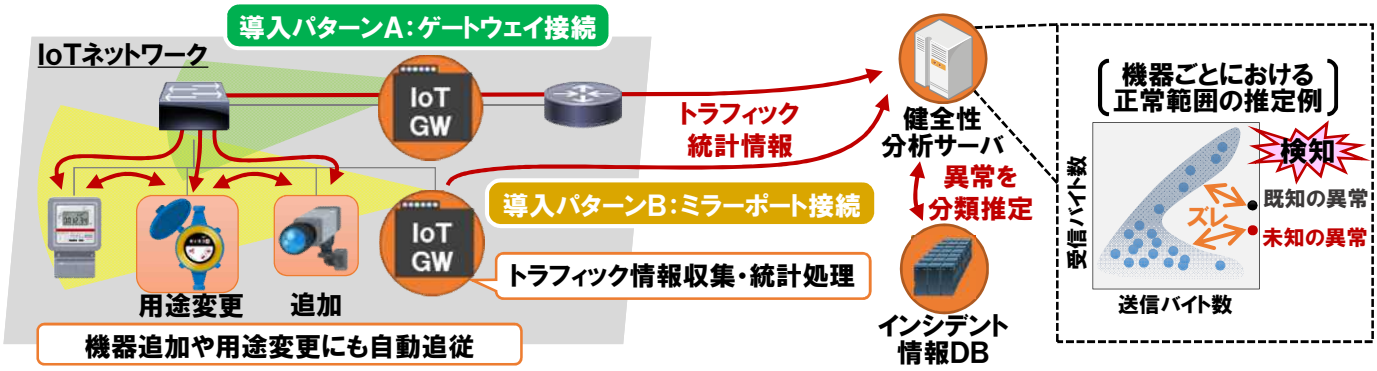
② **膨大なIoT機器により構成されたIoTシステムの動作監視・解析**
膨大なIoT機器を接続方法によらず自動検出し、効率的に導入できます（監視対象自動設定技術）。
複数IoTシステムからの結果を安全に集約・解析して異常を分類推定します（IoTシステム統合解析技術）。

③ **重要インフラ事業者向けセキュリティ監視サービスの導入・運用**
事業者毎の利用形態や既存管理システムに合わせ、2020時代に適した柔軟なIoTセキュリティ監視サービスを提供します（IoTセキュリティ監視サービス）。

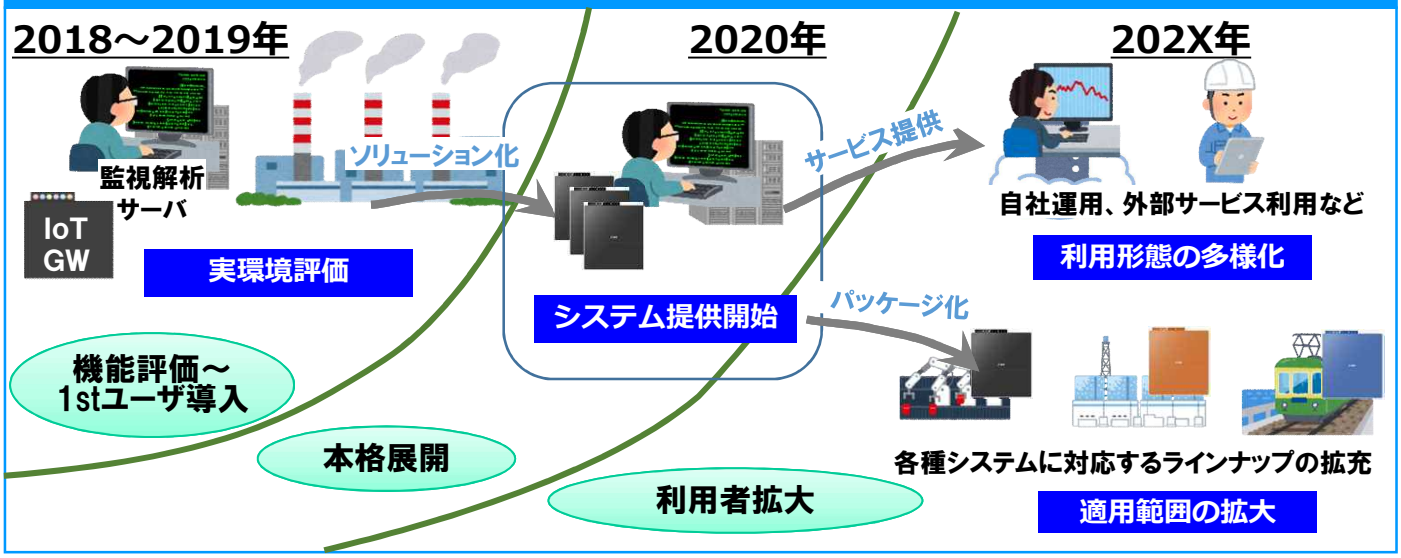
急速なIoT化に伴い脅威が拡大しているため、IoTが招くセキュリティ事故に備える必要があります。

IoT機器改造やシステム構成変更を伴わず導入可能で、多様なIoT機器の新たな脅威にも即時対応可能です。

お客様環境に応じて、健全性分析サーバおよびインシデント情報DBはMSSとしても提供可能です。
IoT GWをお客様環境に設置して頂くことは必須となります。



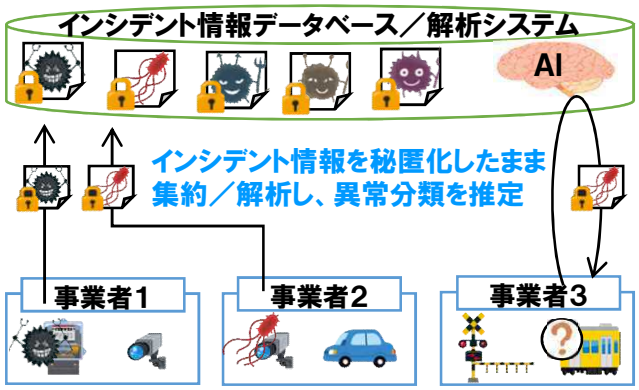
IoT GWを用いたセキュリティ技術の社会実装、ビジネス展開



戦略的イノベーション創造プログラム（SIP）　【三菱電機、日本電信電話】

2－1　モニタリング機器の追加でIoTセキュリティ監視を提供

インシデント情報を安全に集約して分類を推定します



大量なIoT機器からリアルタイムに情報を収集します

攻撃検知には、大量のIoT機器から行われる通信の
一つ一つを、漏れなく統計情報化する必要があります。

対象システム例：　映像監視の場合
カメラ256台 x 4種類の通信フロー ＝ 1024通信フロー

		要件	本技術
統計情報収集	①フロー数 ②項目数	①1024フロー以上 ②9項目以上 （5tuples+通信量）	①5000 ②17項目 （+フラグ情報）
通信転送性能		1Gbpsワイヤレート	

異常検知と異常分類の推定を併せもつ技術を開発（既存技術との比較）

AIを活用したホワイトリスト方式の拡張によって、ホワイトリストの自動生成と異常分類の推定を実現

	ブラックリスト方式	ホワイトリスト方式	本技術（ホワイトリスト方式拡張）
既知の攻撃による異常検知	○	○	○（自動）
未知の攻撃による異常検知	×	○	○（自動）
異常分類の推定	○	×	○

［ブラックリスト方式］

- 既知の異常を定義
  ⇒ 異常分類の推定が可能
- 定義されていない未知の
  攻撃は対処不可

［ホワイトリスト方式］

- 正常動作を定義
- 異常検知は可能だが
  異常分類の推定は不可

［本技術］

- 正常動作を自動定義
- 異常分類の推定も可
- IoT機器の追加および
  変更に自動追従

導入構成

① SI提供（オンプレミス）

- 自社にてセキュリティ運用が可能な
  事業者様向けにオンプレミスで
  フルセットを提供

② パッケージ提供＋サービス提供

- IoT GW設置のみでユーザは特別な
  知識を必要としない遠隔セキュリティ
  監視サービスとして提供
- 高精度な異常分類推定が可能な
  インシデント情報DBサービスを
  付加価値として提供

戦略的イノベーション創造プログラム（SIP）

【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】

2－2　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

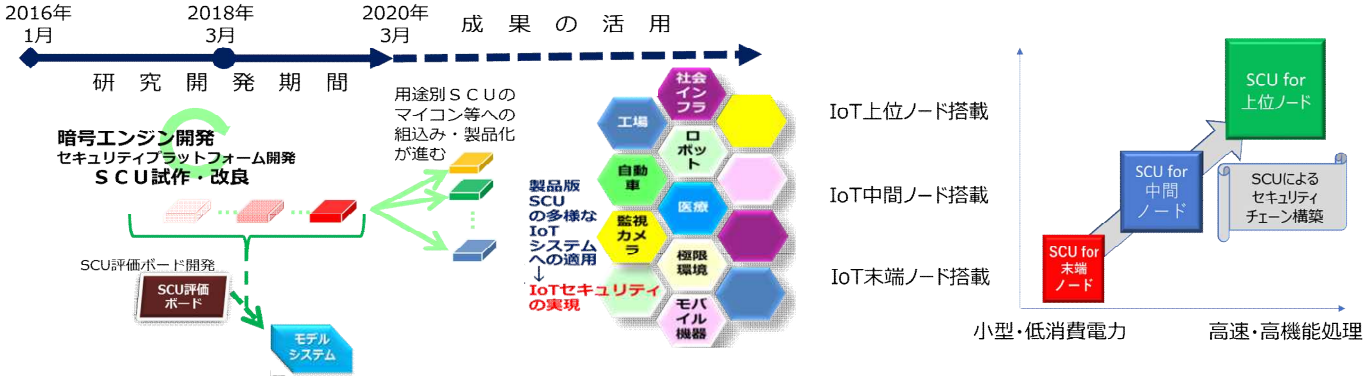
IoT向け対策技術

どこでも公開鍵暗号を！ Secure Cryptographic Unit

SCUのユーザメリットと普及に向けた方針

開発技術	ユーザメリット	普及に向けた方針
SCU	● すべての末端IoT機器に公開鍵暗号を耐タンパー性を確保して搭載可能 ● 末端ノードから中間ノード、上位サーバーまでスケーラブルな展開が容易 ● 既存のTPM製品等より、小型・低消費電力・高速化の点で有利。	● 認知度を高め、IoT市場での普及を加速するため、標準化モデル、ユースケースを研究 ● 先進ユーザ企業と連携し先導的な成功事例を蓄積 ● 多彩な分野／用途にアプリ展開。ガイド文書の充実。 →幅広い分野別ユースケースに対応したSCUモデル展開へ

研究成果による将来展望（イメージ）



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）

戦略的イノベーション創造プログラム（SIP）

【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】

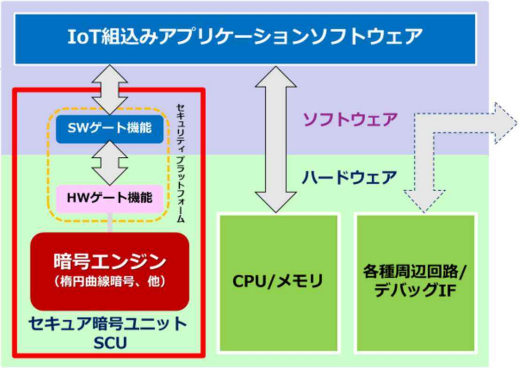
2－2　IoTのセキュリティを実現する超低電力公開鍵暗号実装技術

IoT向け対策技術

どこでも公開鍵暗号を！ Secure Cryptographic Unit

セキュア暗号ユニット（SCU）

・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。
・暗号エンジンとセキュリティプラットフォームから構成され、全ての繋がる機器に「最先端の公開鍵暗号機能」を内蔵させIoTのセキュリティを実現する。



セキュア暗号ユニット（SCU）の特長

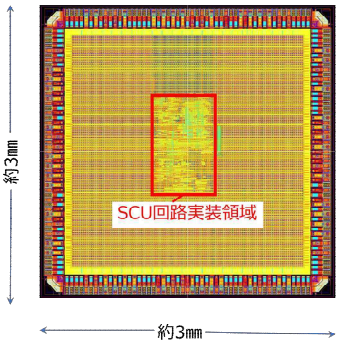
IoTシステムを構成する“末端ノード、中間ノード、上位ノードまでをスケーラブルに最先端の暗号技術・セキュリティ技術で守る。

1．IoT末端ノード向けに小型で超低電力の最先端の公開鍵暗号エンジンを搭載。
2．「信頼の起点」となる耐タンパー性の確保とライフサイクル管理の構築が可能。
3．ローエンドMCU (Micro Controller Unit) から高性能SOC (System On Chip)まで、スケーラブルに展開が可能。

ポイント1：「SCUプロトタイプチップ KM10 シリーズ」

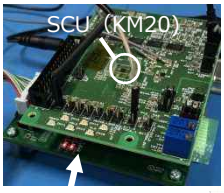
本研究では、プロトタイプチップを試作し、現実のIoTシステムにおけるSCUの応用を模したモデルシステムを開発している。

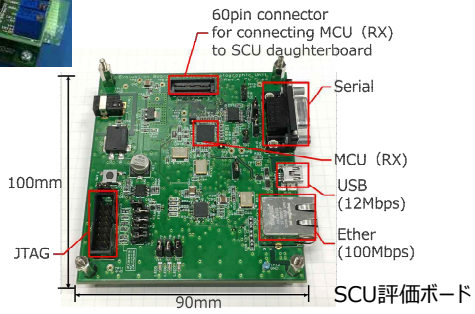
＜SCU“KM10シリーズ”の主な仕様＞
・暗号エンジン：ECC（楕円曲線暗号;256ビット素体), AES, SHA-256, ChaCha20-Poly1305, 物理乱数生成器
・セキュリティ制御：HWゲート、SWゲート



ポイント2：「SCU評価ボード」

SCU評価ボードは、SCUを搭載するIoT機器や応用システムの開発向けに提供される開発ツールで、SCUのセキュリティプラットフォームを利用してアプリ開発・評価を行うことが可能。





戦略的イノベーション創造プログラム（SIP）

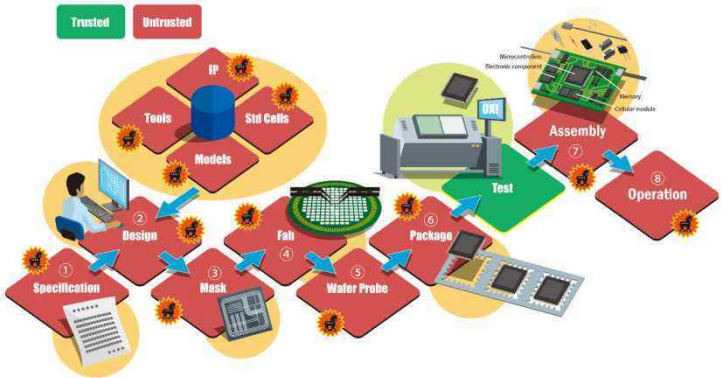
【電子商取引安全技術研究組合
ルネサスエレクトロニクス株式会社】

2－2 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

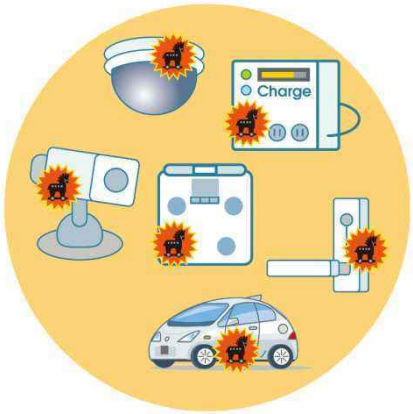
IoT向け対策技術

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（HT）の脅威



信頼できないサプライチェーンにおいてICチップ、基板、接続線路などに意図的な電気的改変が行われる



安価に実装できるHTの出現により民生品にも脅威が拡大

攻撃タイミング・想定される攻撃・前提・コスト

	攻撃タイミング	想定される攻撃	攻撃の前提	攻撃コスト	攻撃者
システムLSIの設計製造工程	①要求仕様	ベンダによる悪意ある製品	サプライチェーンへの介入・ICへの物理アクセスによる攻撃の実行	コスト大	Bespoke, Professional
	②システムLSI設計	悪意ある設計者による設計			
	③マスク製造	製造過程におけるマスクの改ざん・すり替え			
	④チップ製造	下請けベンダの介入による設計改ざん			
	⑤チップ検査	下請けによる配線・回路改ざん			
	⑥パッケージ				
組込機器の製造工程	⑦制御部の組込	電子部品の挿入	機器への物理アクセスによる攻撃の実行	「コスト大」よりは大幅に少ないコスト	Bespoke, Professional, Hobbyist
	⑦機器の組み立て				
出荷後	⑧機器の運用	電子部品の挿入・マルウェアの書き込み・装置の挿入		上記に比べ少ないコスト	Bespoke, Professional, Hobbyist

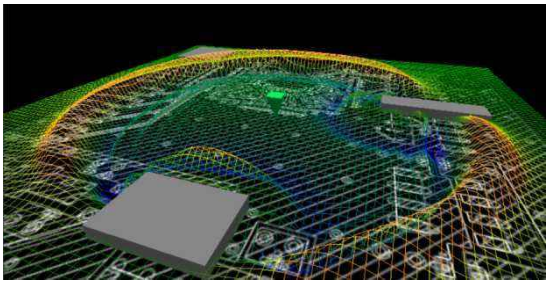
課題1： マイコンなどの制御部品にハードウェアトロイが仕掛けられないようにする仕組の構築（ 制御部品の設計製造工程におけるトロイの検出、発動の抑止）

課題2： マイコンなどの制御部品にはハードウェアトロイはないという前提で、安全な制御部品を利用してハードウェアトロイが仕掛けられないようにする仕組みの構築（ 組込機器の製造工程におけるトロイの検出、発動の抑止）

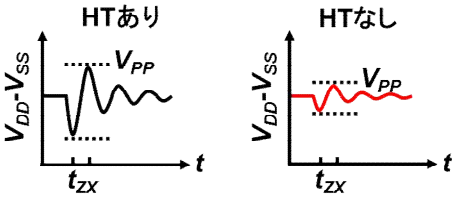
課題3： ライフサイクルにおいてトロイが発動した場合の対処法に関する検討

課題2の解決技術を展示

IC及びその周辺に仕掛けられたHTを検出する技術の開発

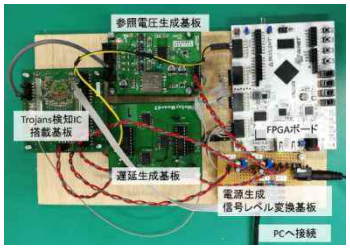


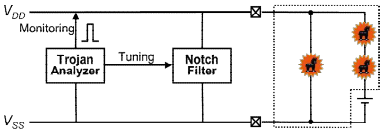
真正性が保証されているICから周囲IC及び電気素子をセンシング



センサーから発せられるインパルスを用いた回路応答からHTの有無を検出

HT検出試験環境





戦略的イノベーション創造プログラム（SIP）

【パナソニック】

2－3 「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

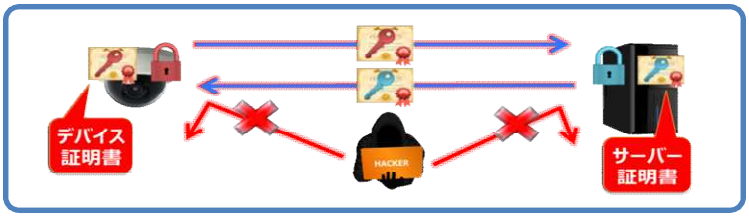
IoT向け対策技術

IoT機器内で生成した推測リスクの少ないシードから 暗号・認証鍵を生成することで、安全な暗号・認証機能を実現

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



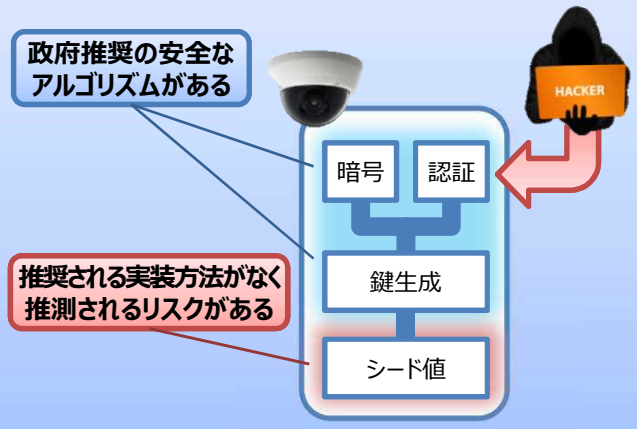
エンドポイント間での PKI認証が必須

② シード生成 ： 推測リスクの少ないシードから安全な鍵を生成

従来の課題　Before	導入による効果　After
ゆらぎの少ないシードや設計者秘密は、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シードを生成
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	機器の内部でシード、鍵を生成し、漏えいリスクを低減

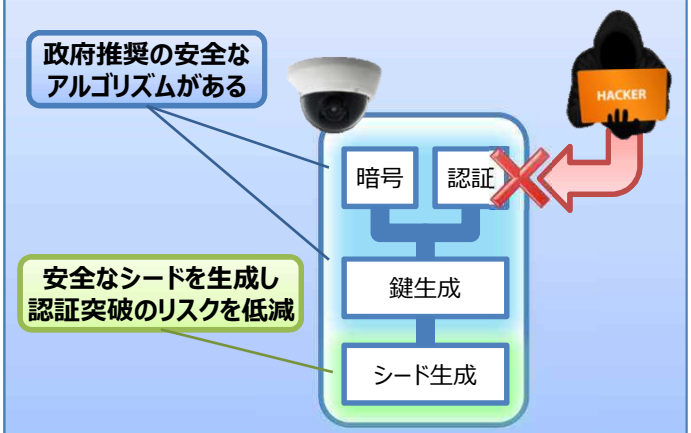
Before

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シードから 鍵を生成し、安全な暗号・認証機能を実現



	ノイズ源 方式	ノイズ源 概要	メリット	デメリット
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

戦略的イノベーション創造プログラム（SIP）

【パナソニック】

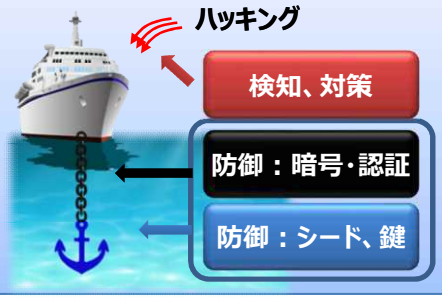
2－3 「防御」、「検知」、「対策」でエンドポイントを守る トータルサイバーセキュリティ

IoT向け対策技術

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

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

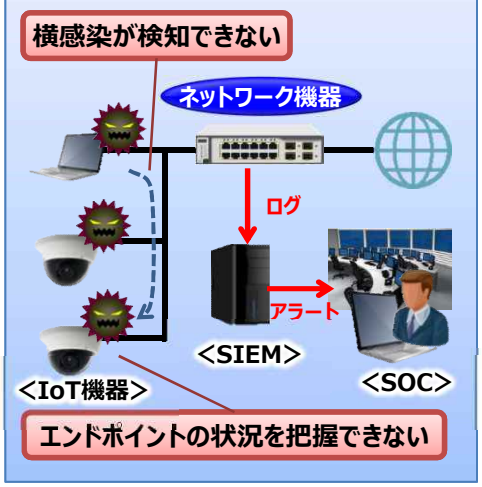


	ITセキュリティ	IoTセキュリティ
対 策	Windows Update ウィルスの隔離 等	サイバー攻撃対策
検 知	アンチウィルスソフト 等	
防 御	標準暗号通信 PKI認証	標準暗号通信 PKI認証

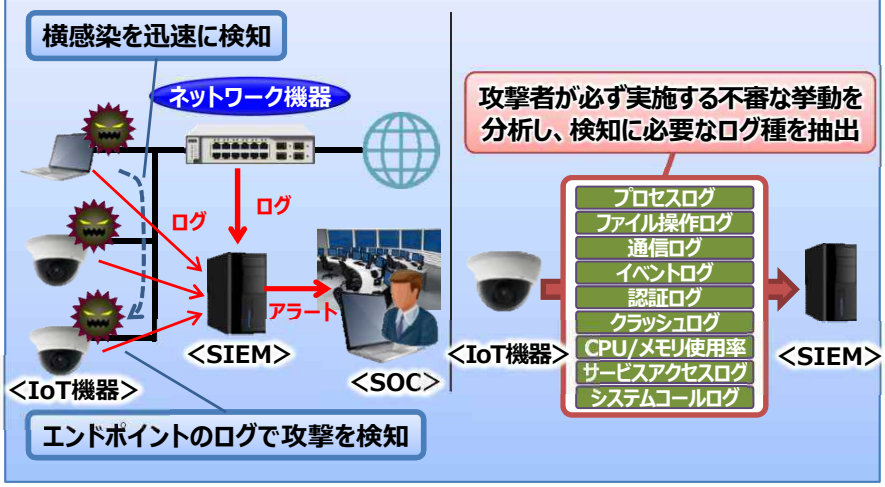
② サイバー攻撃対策：IoT機器のログを使って迅速に検知、対策

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

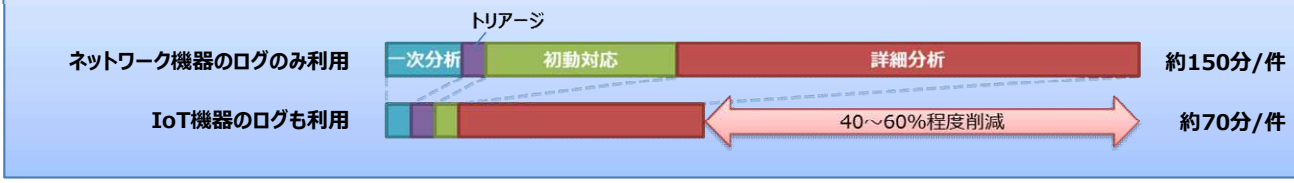
Before：ネットワーク機器のログを利用



After：IoT機器のログも利用



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



戦略的イノベーション創造プログラム（SIP）　【産業技術総合研究所】

3-1　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

社会実装技術

従来になく有効で、かつ、速やかに社会実装可能な適合性確認のあり方と仕組みの検討

特長
① 自然言語処理技術で複数セキュリティ規程を比較し、適合性確認の省力化と定量化
② セキュリティ バイ デザインによる開発とゴール指向分析によるテンプレートの活用で確実な適合性確認

関連技術分野：要求分析、セキュリティ＆セーフティ分析
連携先業種：　重要インフラ関連事業

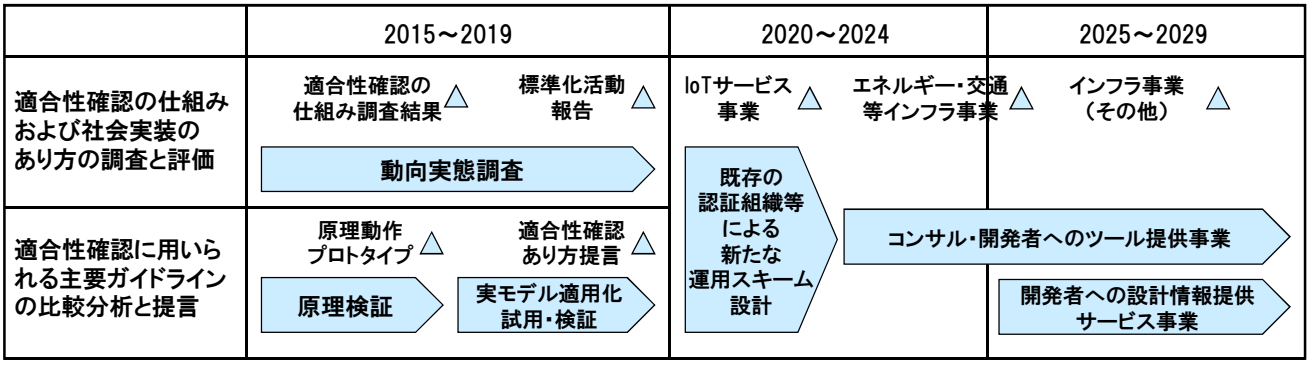
研究のねらい

スマートグリッドシステム等のエネルギーインフラの導入で先行する諸外国の取組み状況を調査し、調査により得られた基礎データをもとに、我が国の重要インフラ事業者及び重要インフラシステムを取り巻く環境・リスクを考慮して、セキュリティ評価制度の検討を進める。これらの研究を通じて、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。

研究内容

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技術に関して、欧米の動向及び実態を調査し、(a1) 真贋性判定技術とSP800-53の対応関係を分析してフィードバックを行った。
2. 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、自然言語処理技術活用することによって、大きな省力化と定量化を実現した。これは、ある規程に適合した製品を別の規程にも適合させたい場合に、活用できる手法である。欧米と日本の規格を比較することで、以下の3を導いた。
3. 1及び2の結果に基づいて、(a2) 動作監視・解析技術を題材にケーススタディを行った。復旧対応を監視製品/サービスの要件にすべきであり、このような要件を政府統一基準でも盛り込むべきであると結論した。
4. 3の監視製品/サービスに対する復旧対応の要件化の国際標準化活動を検討した。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るべきと結論した。
5. 適合性確認を確実にするために、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プロセス支援ツールの基本原理を構築し、検証した。
6. 適合性確認のために、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ための基本原理を構築し、ツールの試作・評価した。

スケジュール



① 自然言語処理技術を活用し複数セキュリティ規程を分析する手法

従来、人手で分析したものはあったが、ITを使うことによって、大きな省力化と定量化を実現できた。これは、ある規程に適合した製品を別の規程にも適合させたい場合に、活用できる手法である。また、規程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、規程を作る側にも参考情報になる。

図 SP800-53の自己相関分析

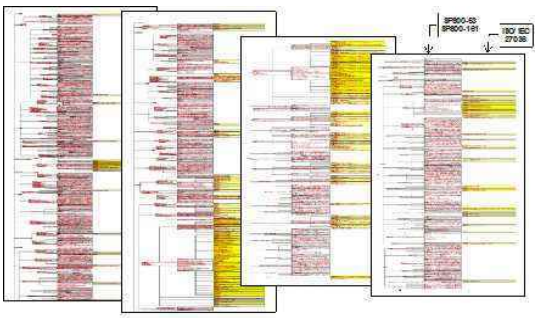
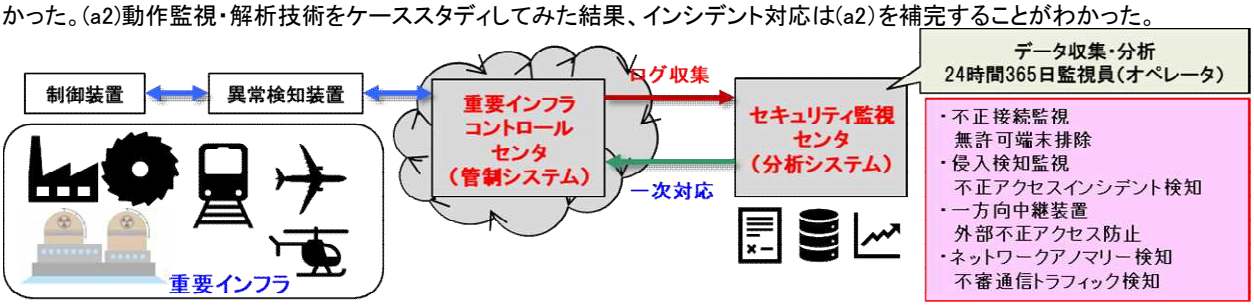


図 SP800-161とISO/IEC 27046の突合分析

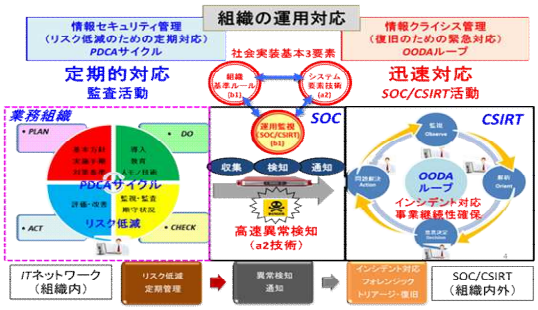
② ①の活用とケーススタディ

政府統一基準とSP 800-53を①を活用して分析した結果、政府統一基準には、インシデント対応の要求事項が必要であることがわかった。(a2)動作監視・解析技術をケーススタディしてみた結果、インシデント対応は(a2)を補完することがわかった。



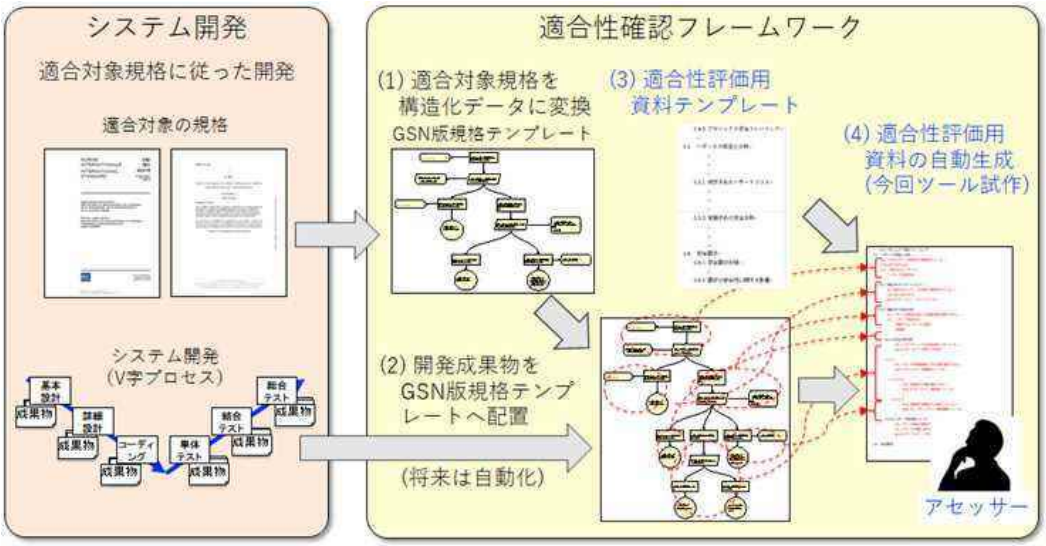
a2 技術の基本機能
NIST SP800-53 管理策
①IR-5：インシデントモニタリング監視・自動データ収集/分析/...
②IR-6：インシデント報告・自動報告/...

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検知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



③ セキュリティに関する規程への適合性確認の方法

規程からセキュリティ バイ デザインの開発手法を使って製品等を開発して、開発過程において規程に準拠していることの証拠を生成し、また、ゴール指向分析を基にした規程を満たすための必要事項の構造を示すテンプレートを準備することで、上記の証拠と規格テンプレートの比較によって、製品等が規程に適合していることを判断可能にするための手法を開発した。この手法は、具体的な製品が規程に適合しているかを企業内で確認するために活用できる。



戦略的イノベーション創造プログラム（SIP）

【日立製作所】

3－2 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

社会実装技術

脅威情報を機械処理可能な定型フォーマットとし、迅速な配信を実現。
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。

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。

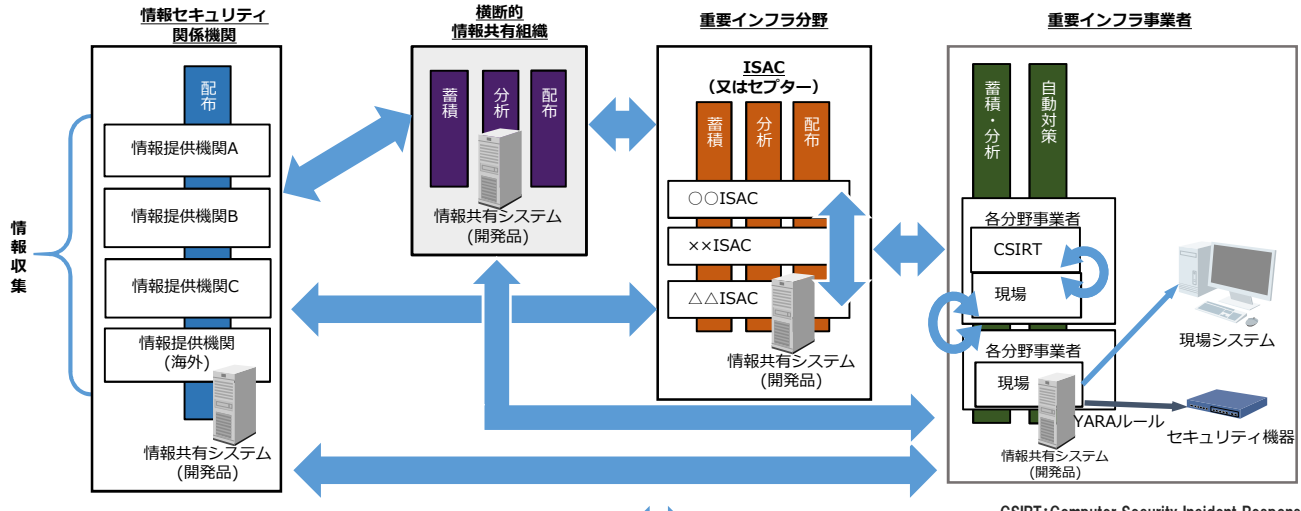
④ 導入ガイドの提供
組織の実情に応じた情報共有の構築を助ける補助ツールとしてデザインガイドを用意。

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

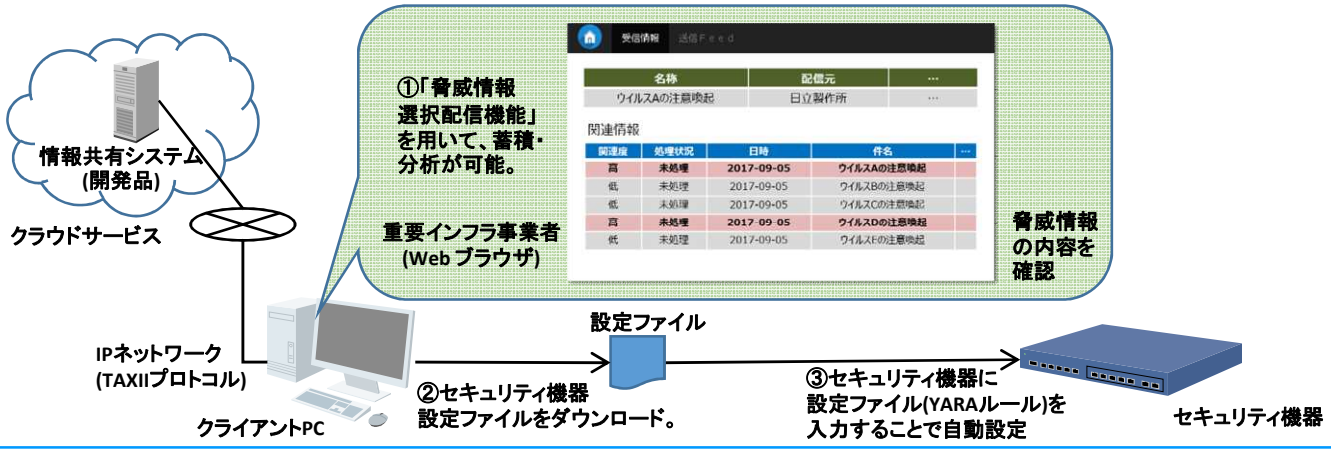
◆情報共有システムを連携して利用する仕掛けを構築することで、脅威情報の入手から配信と対策までをスピードUP。



（※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。

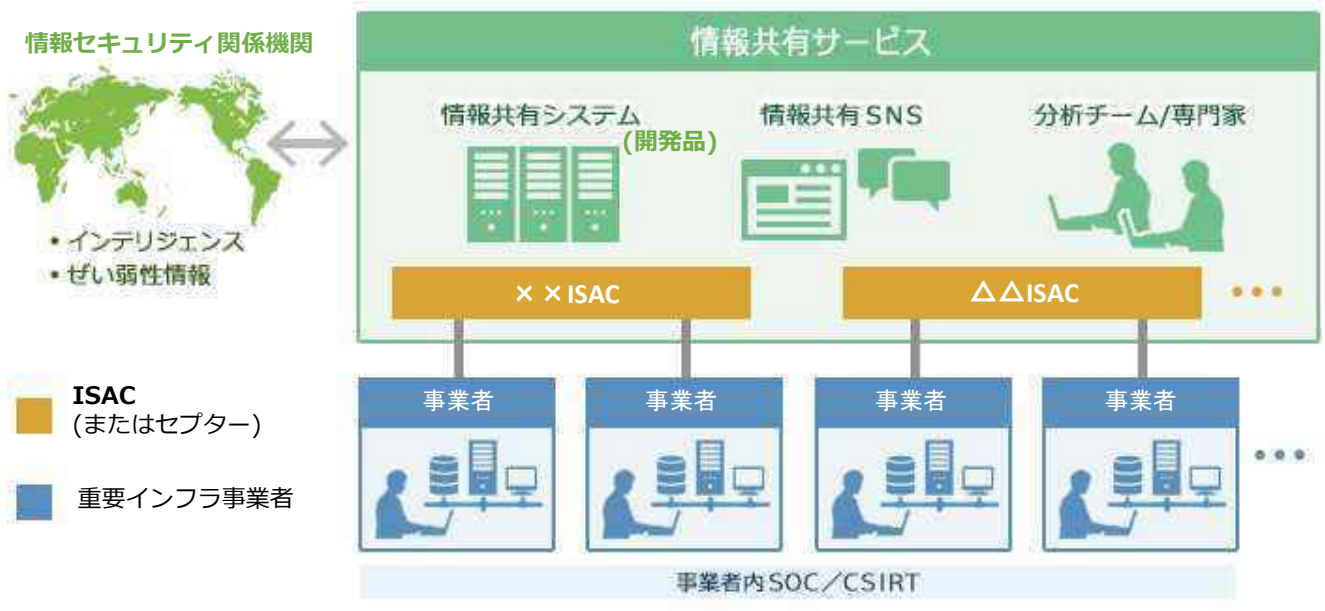
製品イメージ

◆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わ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。



スケジュール

◆2017年度に情報共有システムを開発し、重要インフラ事業者等において評価検証を実施。
2018年度に、2017年度の評価検証結果を織り込んだものを実用化し、社会実装する。

◆2020年4月以降は、本格的な普及展開を図る。

2017年度	2018年度	2019年度	2020年度
評価検証	継続開発	実用化	新規機能の運用

3-3 重要インフラでの実践力を養うセキュリティ人材育成

社会実装技術

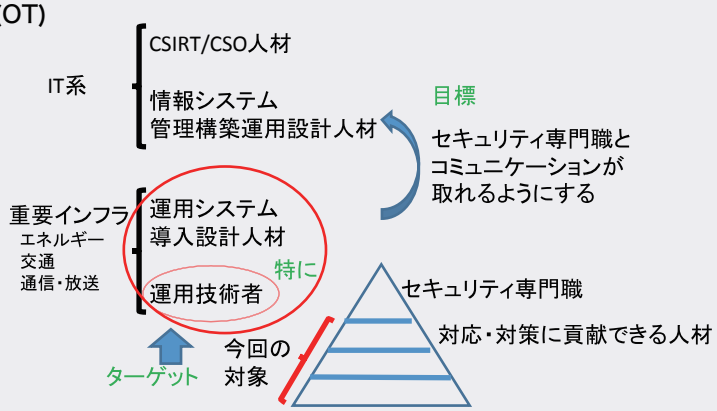
セキュリティ人材育成の研究開発

ターゲット人材

重要インフラ等のオペレーションに従事する技術者(OT)

育成目標

・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
・セキュリティとは何かを理解できる
・定常的にセキュリティを意識できる
・対応・対策に貢献できる
→セキュリティ専門家とコミュニケーションできる



開発内容

① カリキュラムの研究開発
指導内容の精査
② 講義・演習教材の研究開発
指導のための抗議演習教材の開発及び
指導要領の整備
③ E-Learning System機能の研究開発
柔軟な受講を可能とする教材の整備
④ セキュリティ関連コミュニティ機能の研究開発
指導者コミュニティの支援機能の提供
教材更新のメカニズムの確立

（1）新規性

目標: 運用技術者(OT)がセキュリティ担当者(IT)の説明を理解し、インシデント発生時に報告できるようにすること
指導要領としての指導方法の提供を行っている。

何を教えるか! → どうやって教えるか!

（2）実用性

教材を広く配布(意見集約と改善)
多くの指導者が人材育成に従事可能 (指導要領)
個々の環境に合わせたカスタマイズ (カスタマイズマニュアル)
指導者コミュニティの形成
教材更新のための情報共有と更新プロセスの確立

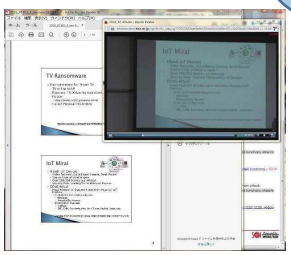

テキスト


講義

演習

1. カリキュラム研究開発
2. 演習・講義教材研究開発
気付きから、
基礎知識、対応、対策、報告まで
指導要領

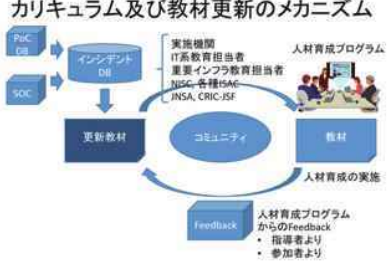

インシデント体験演習
(ランサムウェア)


e-learning

3. e-learning system
柔軟な学習環境
進捗把握

4. コミュニティ
最新情報の交換
自己学習環境
教材更新

カリキュラム及び教材更新のメカニズム



3-3 重要インフラでの実践力を養うセキュリティ人材育成

成果

（1）現在の達成度

教材の配布を開始しており、具体的な人材育成の試行が進められている。

これらからの意見を集約し、教材の更新を進行中

テキスト教材 40程度の組織に配布

配布先での人材育成が進んでいる

体験型演習 情報セキュリティ大学院大学、慶應大にて演習コースを提供

（2）達成見込み

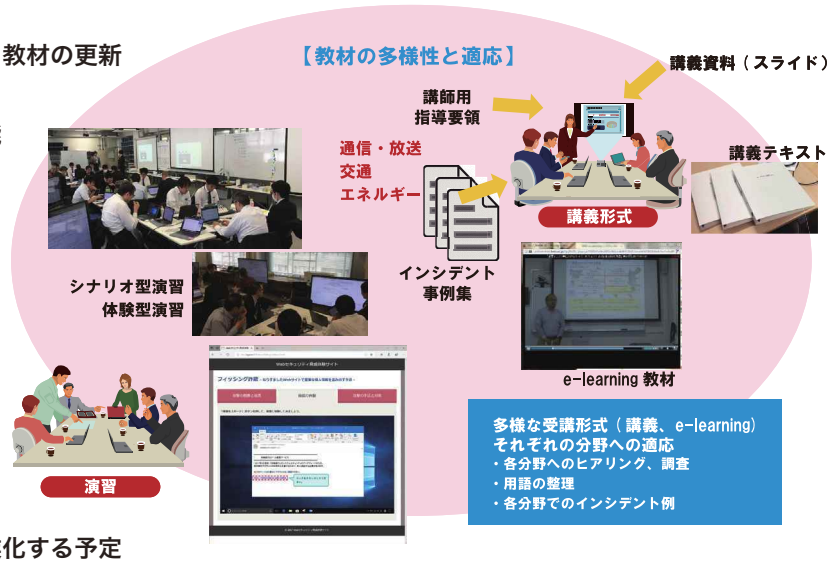
開発した教材を基礎として、定常的な更新を進める体制を整備

指導者コミュニティの形成

コミュニティにおける情報の共有と教材の更新

実施組織における事業化

指導者コミュニティの核として機能



研究テーマの実用化・事業化

（1）　取組状況

教材を用いた教育プログラムを事業化する予定

また、教材を活用する組織の指導者コミュニティを形成するとともに、このコミュニティにおいて教材活用、情報交換、教材更新を持続的に維持する体制を確立する。

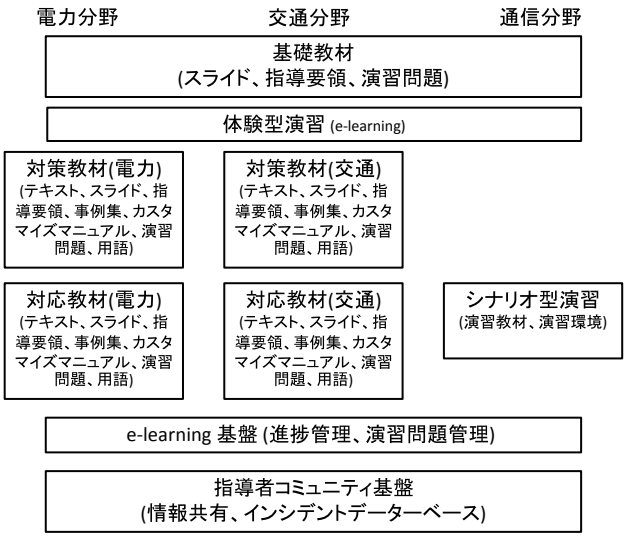
特に、教材更新については、実施機関だけでなく、NISCなどの政府機関、ISACなどの各分野の業界組織、JNSAやCRIC-CSFなどの業界連携組織などと連携し、継続的な更新を行える体制を確立する。

（2）　事業化に向けた課題

人材育成の対象がさまざまであり、これらを効果的に行う教育プログラムの組み上げが必要であるが、本研究開発で形成されたコミュニティを基盤として広く展開することが可能であると考える。

（3）　対処方針と今後の計画

平成31年/令和元年度に試行を行いながら、令和2年度より実施機関での事業を開始する。



3－4 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

社会実装技術

想定外が不可避のサイバーインシデントに対応できるレジリエンスの高い組織的連携を実現するための演習システムの提案

サイバーインシデント対応に求められる組織連携とは

- スーパーマンを求めるよりも、組織としての対応
- 守り切れない前提で、想定外への対応能力を向上させる
- 部分的には陥落しても、全滅を防ぐ、多重多様な安全対策
- 事業継続の破綻は、関連するAND条件すべてが原因になる（関係者が多い）
- 緊急時にできることは、通信遮断と自動システムに頼らない手動操作
  - 気づけたら、安全は確保できるように計装は構成されているはず
  - 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？
  - 通信遮断して事業継続できるなら、早期遮断が可能
- 操業系のリスク管理、および現場事故対応はOT
  通信系の監視、ツール管理はITが中心になって協力

⇒求められる連携をイメージできる演習（疑似体験）を繰り返す

レジリエンス向上が重要

安全の観点での検討
- Safety-Ⅰ 事故を起こさない能力
- Safety-Ⅱ 想定外な事故でも抑え込める能力
  レジリエンス

サイバー攻撃は、安全破綻のひとつの原因
- サイバー攻撃の手口は想定しきれない
  （脆弱性も攻撃者の発明品）
- 危険源がサイバー攻撃であっても、
  起こる事故は、制御対象で決まる

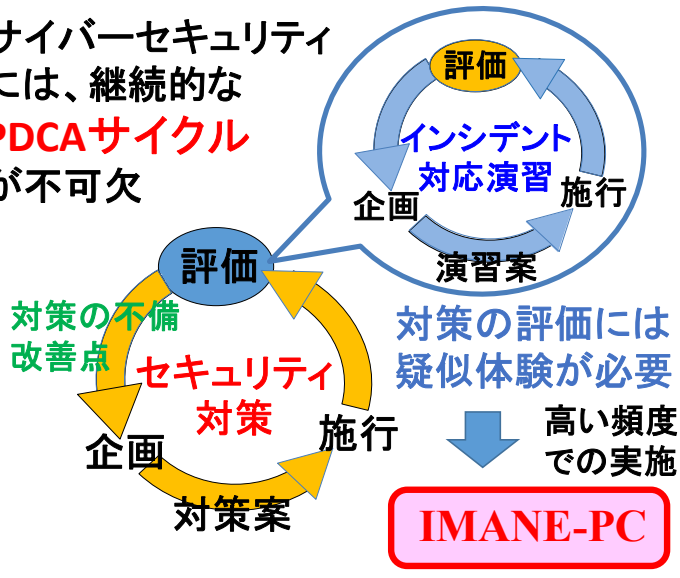
↓

予想外の攻撃にも気づける可能性のある人を配置し、
気づきを適切に対策につなげられる組織体制をつくる

↓

予想外への気づきには、想像力が重要で、
複数のシナリオでの疑似体験（演習）が有効

サイバーセキュリティには、継続的な**PDCAサイクル**が不可欠



対策の評価には疑似体験が必要

高い頻度での実施

IMANE-PC

組織連携を理解するための演習IMANE(Incident MANagement Exercise)シリーズを開発

EX-1: IMANE-DEMO　私は関係したくないという人を引き込むための演習
EX-2: IMANE-CARD　演習のための予習を必要とせず、その場で問題意識を共有するための演習
EX-3: IMANE-PC　コンピュータを利用して、組織連携を疑似体験する演習

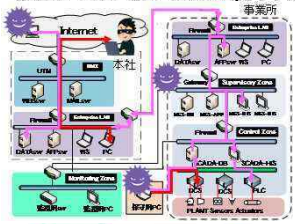
T-1: IMANE-DRAW　インシデント演習用シナリオを編集し、CARD,PC用データを合成するツール
T-2: IMANE-DB　IMANE-PCの実施用データと実施結果のデータを蓄積・検索するデータベース

3―4 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

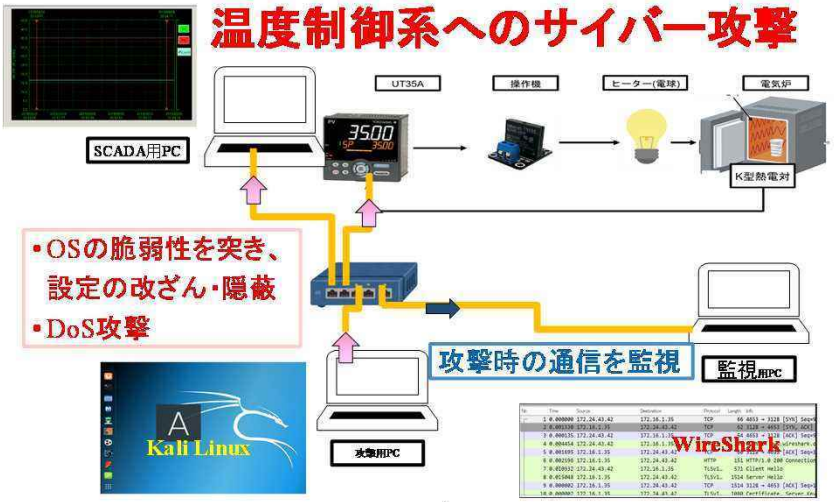
開発した演習システム IMANE (Incident MANagement Exercise)

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



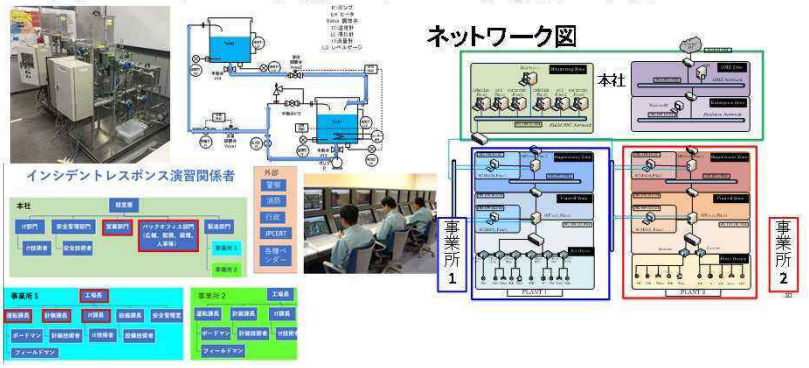
PC3台とコントローラ1台とランプ,HUBだけで実施できる。

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

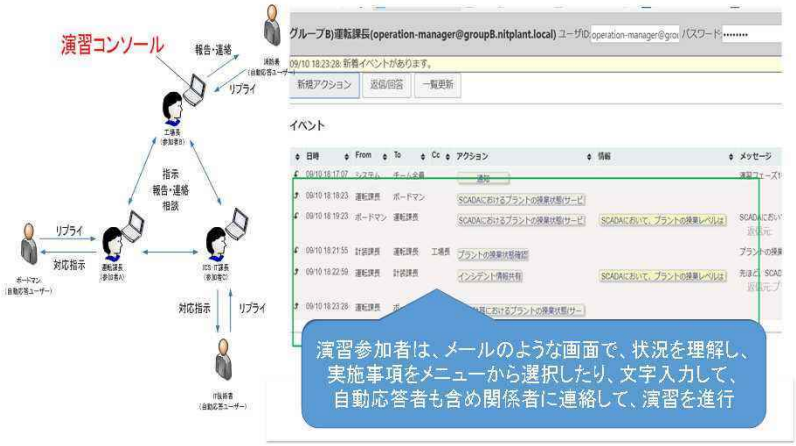
(事業所のシナリオで参加者が役割を理解しているときには不要)

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。