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

株式会社　日立製作所
セキュリティ事業統括本部
主管技師
飯田（いいだ）　恒雄（つねお）

株式会社　日立製作所
IoT・クラウドサービス事業部
主任技師
山崎（やまさき）　伊織（いおり）

1. はじめに

近年、電力・交通・情報通信といった重要インフラ等においてサイバー攻撃による事故事例が発生している。重要インフラ等へのサイバー攻撃は、情報の窃取や破壊にとどまらず、社会的に重大な影響を引き起こす恐れがあるため、サイバー攻撃から重要インフラ等を守ることが大きな社会課題となっている。

重要インフラ等では、情報システムと制御システムの2つの系統のシステムから構成されている場合が多いが、通常、情報システムでは機密性が重視されるのに対して、制御システムではシステム停止が許容されないなど安定性が重視されるといった違いがある。このことから、セキュリティ対策についても、情報システムに対する従来のセキュリティ対策をそのまま制御システムに適用することが難しいという課題があった。

本研究において、このような制御システムに適した新しいセキュリティ技術について研究開発を行った。さらに、安全が重視される重要インフラシステムの特徴を踏まえ、既存システムに影響を与えずに安全に新しいセキュリティ技術を適用するための制御システム向けセキュリティ運用・組織の確立についても研究開発を行った。

本稿では、2章で制御システム向けの新しいセキュリティ技術を紹介し、3章で制御システム向けセキュリティ運用・組織の確立について解説する。さらに、4章でこれらの実用化事例についても紹介する。

2. 制御システム向け動作監視・解析技術

従来、重要インフラ等における制御システムは、閉鎖ネットワークのためにサイバー攻撃を受けにくいと考えられていたが、IoT（Internet of Things）の進展により、ネットワークなどを経由してサイバー攻撃を受ける脅威が増大してきている。

そこで、そのようなサイバー攻撃から制御システムを守るために、制御システムにおけるネットワークの動作を監視・解析し、サイバー攻撃などにより引き起こされるネットワークの異常を検出する技術について研究開発を行った。

通常、制御システムにおけるネットワークは、情報系ネットワークの他に、制御情報系ネットワーク、制御系ネットワークなどの構成となっていることが多い。

標的型攻撃では、電子メールやその他の手段で情報系ネットワークから侵入した後、制御情報系ネットワークの制御・通信機器へ徐々に侵入し、最終的に制御系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ている。そこで、このような破壊的な異常が発生する前に、ネットワークに順次侵入してくる攻撃の予兆を早期に検知することが重要となる。

ネットワークへの侵入を検知するには、制御情報系ネットワークから制御系ネットワークにわたって幅広くネットワークを監視しておき、サイバー攻撃によるネットワークの異常を検出・解析することで可能になる。

制御システムの制御情報系ネットワークと制御系ネットワークにおけるサイバー攻撃による異常を検知する解析手法は、以下の課題があり、これまで確立されていなかった。

(1) サイバー攻撃起因による障害の検知困難性

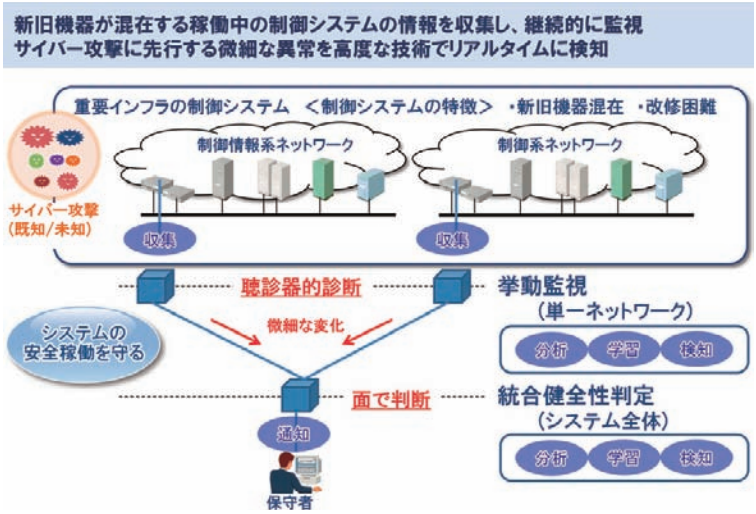
従来から故障などの障害による制御系ネットワークの異常を検知する故障予知技術は存在したが、サイバー攻撃に起因する障害の検知技術は実用化されていなかった。

(2) 正規ツールを悪用した攻撃の検知困難性

近年の標的型攻撃では、ウイルス対策ソフトに検知されないようにするため、ウイルスとして動作するのではなく、OS標準コマンドなどを使った正規ツールや業務ツールを悪用した事例も増えている。このような正規ツールを悪用した攻撃はウイルス対策ソフトでは検知困難である。

(3) 制御系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

標的型攻撃などに起因する異常を検知するには、正常



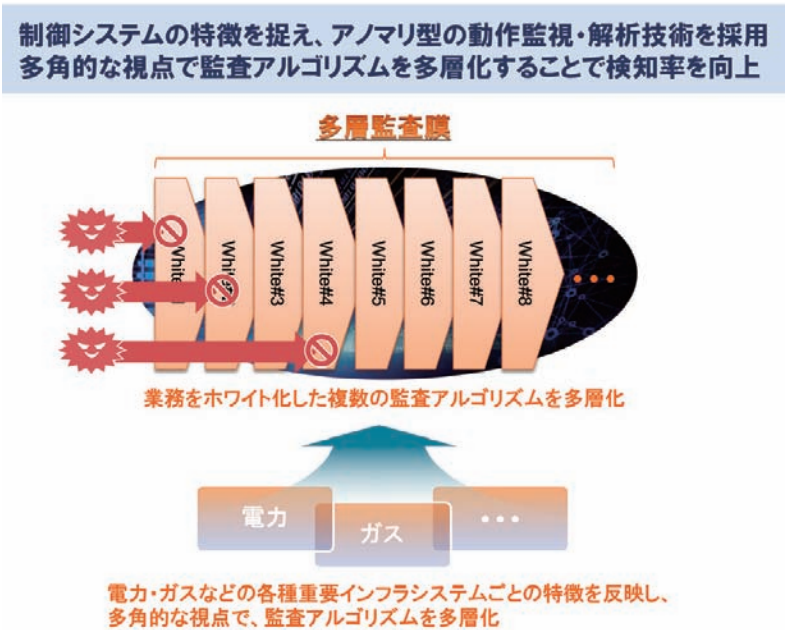
■図1.　検知技術の技術概要

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、制御系ネットワークではシステムごと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) 制御系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) 制御系ネットワークの微細変化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。

今回研究開発した検知技術の技術概要を図1に示す。

今回研究開発した検知技術では、制御システムの特徴に合わせて、通常業務でのネットワークの動きを正常モデルとして定義（ホワイト化）しておき、それとは異なるネットワークの変化を検出するアノマリ型の動作監視・解析技術を採用した。さらに、アノマリ型の監査アルゴリズムを多角的な視点で複数種類用意し、複数の監査アルゴリズムを多層化することで検知率を向上させる多層監査膜方式とした。



■図2.　検知率向上のための多重監査膜

検知率向上のための多重監査膜の技術概要を図2に示す。

今回の研究開発において、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・具体化などによって、巧妙化が進む制御システムへの攻撃を早期に検知する技術を実現した。

今回研究開発したセキュリティ技術は、①微細な変化をリアルタイム検知する技術を有し、②制御システムの業務通信を多角的な視点で学習する機能を持ち、③システムを面で捉えて総合的に分析することができるという特長がある。さらに、新旧機器が混在しているという制御システムの特徴に合わせて、システムに影響なく導入可能な構成とした。

本検知技術の技術的優位性を表に示す。

■表．検知技術の技術的優位性

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

3. 制御システム向けセキュリティ運用・組織の確立について

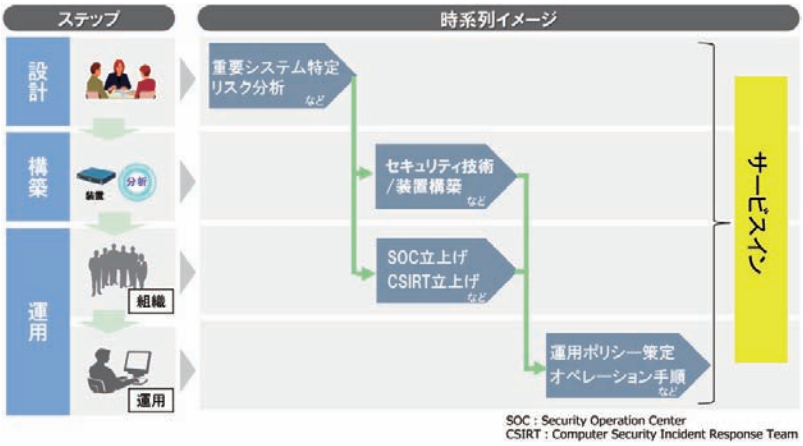
重要インフラシステムをサイバー攻撃から守るためには、2章で述べたような制御システム向けの新しいセキュリティ技術の開発に加えて、その新しいセキュリティ技術をどのように重要インフラシステムに適用・運用していくかということも重要である。

重要インフラシステムへのセキュリティ対策の適用・運用には、まずリスク分析を行って対策すべき箇所を検討し、その適用箇所に対してセキュリティ対策を導入して運用していくことになる。

そこで本研究では、はじめに、重要インフラシステムのリスク分析を行うための「制御システム向け事業レベルでのリスク分析手法」を研究開発した[1]。

重要インフラシステムは事業規模が大きく、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。また、制御システムと情報システムとでは保護対象や想定脅威が異なるため、制御システムの特徴を考慮した分析が必要である。このような課題を受け、本研究において、事業レベルでのリスク分析手法として、事業全体のリスクを効率的に抽出し、それらを俯瞰した上で優先的に対策すべき業務／システムを把握する手法を研究した。本手法では、入力、出力、人、システム、装置、規格・計画の構成要素を活用し、汎用的な事業モデルを定義することで、事業全体を把握可能であることを示した。また、制御システムで考慮すべきH&SEB（Health, Safety, Environment and Business）の観点で事業上のリスクを解析的に抽出し、重大なリスクに関係の深い業務／システムを特定可能であることを示した。

次に、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研究した。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



■図3．制御システム向けセキュリティ運用・組織の確立

別な加工を施すことなく追加する形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である。

本研究において、上記の特徴を踏まえた制御システム向けのセキュリティ対策導入の手法を確立した。**図3**に制御システム向けセキュリティ運用・組織の確立に向けた各ステップと検討項目の時系列イメージを示す。

今回研究開発を行った、重要インフラ事業者が特に考慮すべき事項や具体的な実現手法については、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）のホームページにて「セキュリティ対策適用ガイドライン」として公開している[2]。

4. 実用化事例

制御システム向け動作監視・解析技術として研究開発した、多重検査膜方式のアノマリ監視アルゴリズムを基にして、Hitachi Anomaly Detectorとして（株）日立製作所より製品化を行った[3]。この製品の特長は、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のバージョンなどに依存せず導入可能という点が挙げられる。

Hitachi Anomaly Detectorの概要を**図4**に示す

5. おわりに

今回、重要インフラ等をサイバー攻撃から守るために、制御システムに適した新しいセキュリティ技術について研究開発を行い、さらに、安全が重視される重要インフラシステムの特徴を踏まえ、既存システムに影響を与えずに安全に新しいセキュリティ技術を適用するための制御システム向けセキュリティ運用・組織の確立についても研究開発を行った。また、今回研究開発した成果を基に製品化を行い、安全に利用できるように準備した。

謝辞

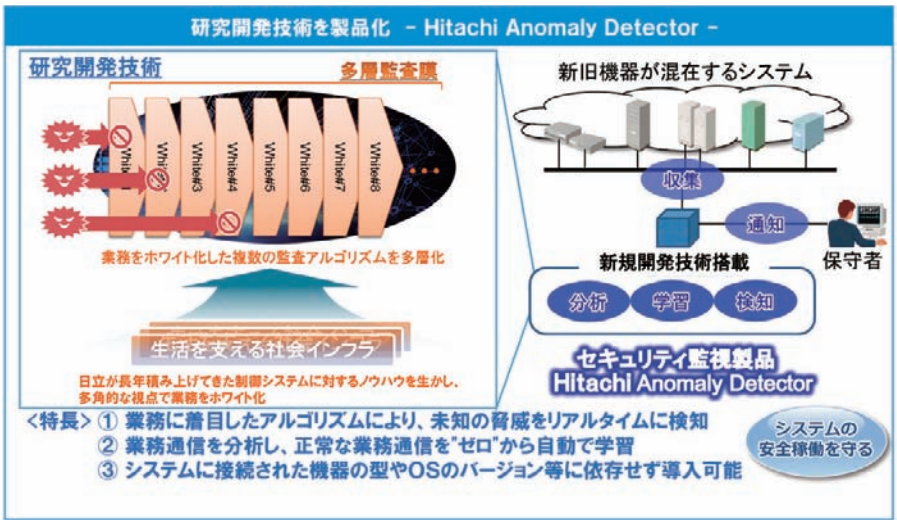
本研究は、内閣府が進める戦略的イノベーション創造プログラム（SIP）「重要インフラ等におけるサイバーセキュリティの確保」（管理法人：NEDO）によって実施されました。

参考文献

[1] 熊谷洋子，松原佑生子，内山宏樹，鍛忠司，藤田淳也，中野利彦「制御システム向け事業レベルでのリスク分析手法の提案」，情報処理学会論文誌「デジタルトランスフォーメーションを加速するコンピュータセキュリティ技術」特集 Vol.60 No.9, pp.1518-1527（2019）

[2] 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／（b3）評価検証プラットフォーム技術，「セキュリティ対策適用ガイドライン」，https://www.nedo.go.jp/content/100904079.pdf

[3] 飯田恒雄，原田宏美，野末大樹，大森雅司，Guillaume Daleux「社会インフラの安全・安心を支えるセキュリティ統合監視ソリューション」，日立評論2018年No.3号



■図4. Hitachi Anomaly Detector