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

近年，特定の企業，組織を狙った「標的型攻撃」などのサイバー攻撃が増加し，社会を支えるインフラシステムでも被害が発生している。そうした状況の中，社会インフラを守るためのサイバー攻撃対策の重要性が増している。
日立は，サイバー攻撃を早期に検知するための技術として，リアルタイムで不正侵入を検出する「日立アノマリ検知装置（Hitachi Anomaly Detector)」を製品化し，また，不正侵入検知後の一次対処と事業継続判断を支援する「統合監視ソリューション」の実証適用を進めている。さらに，セキュリティ監視のグローバル対応に取り組んでいる。本稿では，サイバー攻撃を早期に検知して，被害を未然に防ぐためのセキュリティ統合監視ソリューションを紹介する。

飯田 恒雄 | Iida Tsuneo
原田 宏美 | Harada Hiromi
野末 大樹 | Nozue Daiki
大森 雅司 | Ohmori Masashi
Guillaume Daleux

1. はじめに

サイバー攻撃による被害を未然に防ぐためには，不正な侵入を早期に検知することが重要である。例えば，WannaCryのようなワーム型マルウェアが拡散を始めるときの通信や，標的型攻撃における攻撃者の一連の潜伏行動時などに発生する通信を監視することで不正侵入を検知できる。

このような不正侵入検知技術の一つとして，日立は社会インフラなどの制御システム向けにリアルタイムで不正侵入を検出する技術を確立し，「日立アノマリ検知装置（Hitachi Anomaly Detector)」として製品化した。2章で日立アノマリ検知装置を紹介する。

また，安全稼働が最優先の社会インフラシステムでは，各種不正検知技術により不正侵入などのインシデントを検知した後には，一次対処と事業継続判断が重要となる。これを支援する「統合監視ソリューション」と適用事例について，3章で紹介する。

さらに，社会インフラシステムなどのグローバル化が進む中では，セキュリティ監視についてのグローバル対応も重要となる。グローバルセキュリティ監視の取り組みについて，4章で述べる。

2. 日立アノマリ検知装置（Hitachi Anomaly Detector）

2.1 開発背景

従来，社会を支える重要インフラなどの制御システムは，閉鎖ネットワークのためセキュリティ脅威は少ないと考えられていたが，IoT（Internet of Things）時代を迎えて脅威が増大している。内閣府が推進しNEDO（国

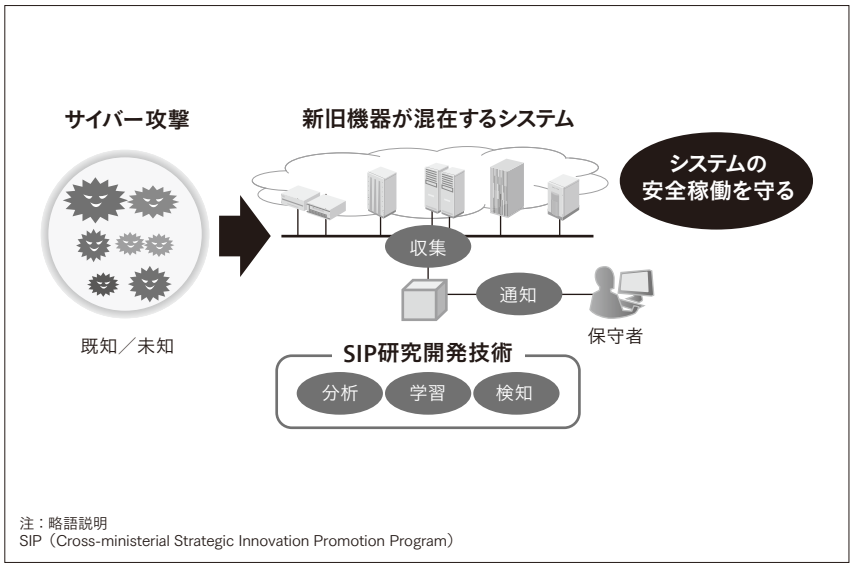


図1｜全体の開発技術イメージ
制御システムの動作監視技術として，容易に接続可能な構成で提供している。

立研究開発法人新エネルギー・産業技術総合開発機構）が管理法人を務める「戦略的イノベーション創造プログラム（SIP）」でも，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向けた研究開発が推進され，日立はその技術成果を搭載して「日立アノマリ検知装置」をリリースした[1)]（**図1**参照）。

2.2 セキュリティ対策に向けた課題

近年，特定の企業，組織を狙った「標的型攻撃」が増加し，安全と考えられてきた制御システムでも被害が増加している。そこで，制御システムに向けたサイバー攻撃への対策を進める必要があるが，制御システムには情報システムとは異なる課題が存在し，情報システム向けの従来のセキュリティ技術では対応することが困難である。

制御システム固有の課題としては，（1）サービスを止めずに対策を行う必要があり，影響評価を含め，システム内部への製品の導入が難しい，（2）ソフトウェアの追加が難しいOS（Operating System）の古い機器，リソースが少ない機器を含めた対策が要求される，（3）独自プロトコルの利用を加味したセキュリティ技術の適用が必要となる，といった点が挙げられる。これらを考慮した対策が早急に求められている。

2.3 製品の特徴

制御システム固有の課題を解決して，制御システムにも適用可能となる不正検知製品を開発するため，技術開発および導入構成の検討を進めた。通常の運用に影響を与えず，サービスを止めずに容易な導入を可能とすることを実現するため，既存ネットワークに対してネットワークタップもしくはスイッチのポートミラーリングで導入する構成とし，外部からネットワークを監視する方式とした（**図2**参照）。これにより，（1）サービスを止めずに対策を行うことが可能となり，（2）既設の機器へソフトウェアを導入することなく適用することができ，（3）通信プロトコルに依存しない不正検知方式を実現した。

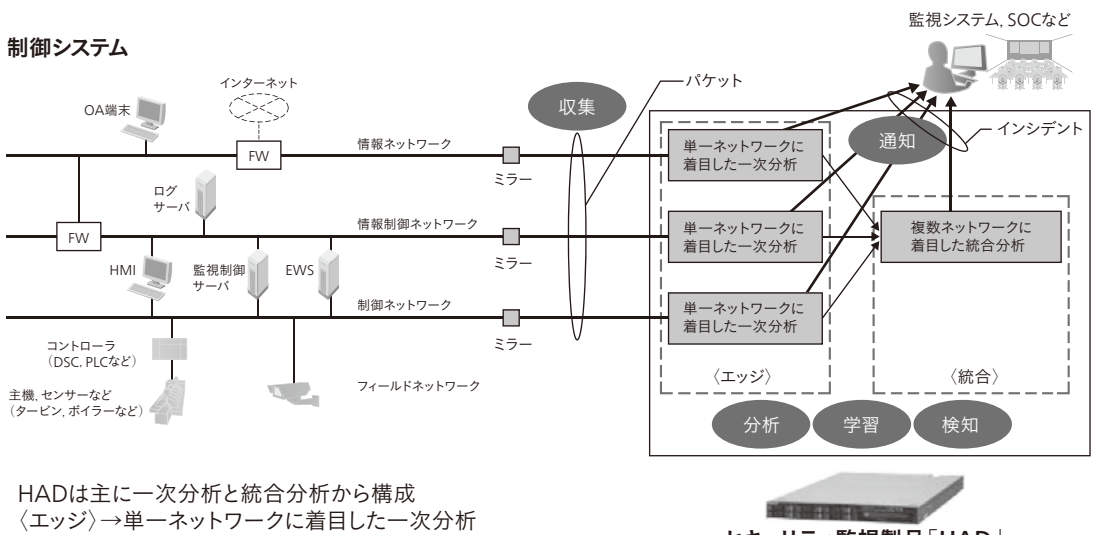
また，この構成を前提とするため，ネットワークからの情報でセキュリティ対策をする必要があり，高度なサイバー攻撃，未知の脅威をネットワークに流れるデータの振る舞いからリアルタイムに検知する技術が求められる。正常なシステム業務の通信とリアルタイムの通信を比較することにより，通常と異なる通信の振る舞いを捉え，サイバー攻撃の探索行為や踏み台による攻撃などを把握する多層的な検知アルゴリズムを開発した。多層的な検知アルゴリズムはきめ細かいリアルタイム検出が可能であり，高度なサイバー攻撃や未知の脅威も検知できる。

さらに，正常なシステム業務をネットワークに流れる通信から自動的に学習するため，システムの正常データなどを事前登録する必要がなく，製品の導入が容易となっている。常に学習が可能なので，保守作業の手動による編集から通常業務のモデルを変更することもサポートしている。

現在は各ネットワークに接続するエッジ構成のみに対応しているが，エッジを統合して各ネットワークをまたがる不審な振る舞いも検知する機能の研究開発も進めている。

図2｜システム全体の論理構成

制御ネットワークのミラーポートに接続し，データ収集，分析／学習，検知を行う。



注：略語説明
OA（Office Automation），FW（Fire Wall），HMI（Human Machine Interface），EWS（Engineering Work Station），DSC（Diameter Signaling Controller），
PLC（Programmable Logic Controller），SOC（Security Operation Center：セキュリティ監視・運用組織），HAD（Hitachi Anomaly Detector）

3. 統合監視ソリューションの適用事例

3.1 制御システムのセキュリティを常時監視

近年，社会インフラシステムへのサイバー攻撃のリスクが高まるとともに，その攻撃手法も高度化・複雑化している。制御システム［OT（Operational Technology）システム］にも情報システム（ITシステム）と同様なセキュリティ対策を施す必要があるが，OTシステムの場合はシステム停止が容易でないことから，システム改修を伴うセキュリティ対策を頻繁に施すことが困難である。そのため，昨今ではシステムを常時監視し，対策の有効性を検証しながら日々進化するサイバー攻撃に対応することが求められている。

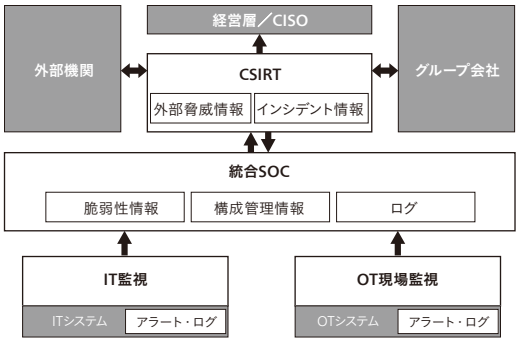
日立は，長年培ってきたOTシステムに関する技術やノウハウとITシステムに関する監視サービスの適用実績を基に，制御システム向けのセキュリティ監視ソリューションを開発した[2)]。

3.2 インシデントを早期検知・一次対処して事業継続判断を支援

従来，セキュリティ監視はSOC（Security Operation Center）がシステム全体を集中監視する形で行われてきた。しかし，OTシステムでは稼働確保のためにプラントやラインといった現場での判断も必要である。また，近年のITとOTの連携によりセキュリティ攻撃もITからOTへ波及している。そこで，セキュリティ監視を現場と統合に分けて行う方式を提案している（**図3**参照）。現場と統合は連携しており，現場ではインシデントを検知するとその内容，影響範囲と稼働への影響を考慮して一次対処を行う。統合では現場からの情報やITシステムの状況，さらには外部機関の情報を収集し，統合的に分析して根本対処の指示を行う方針である。

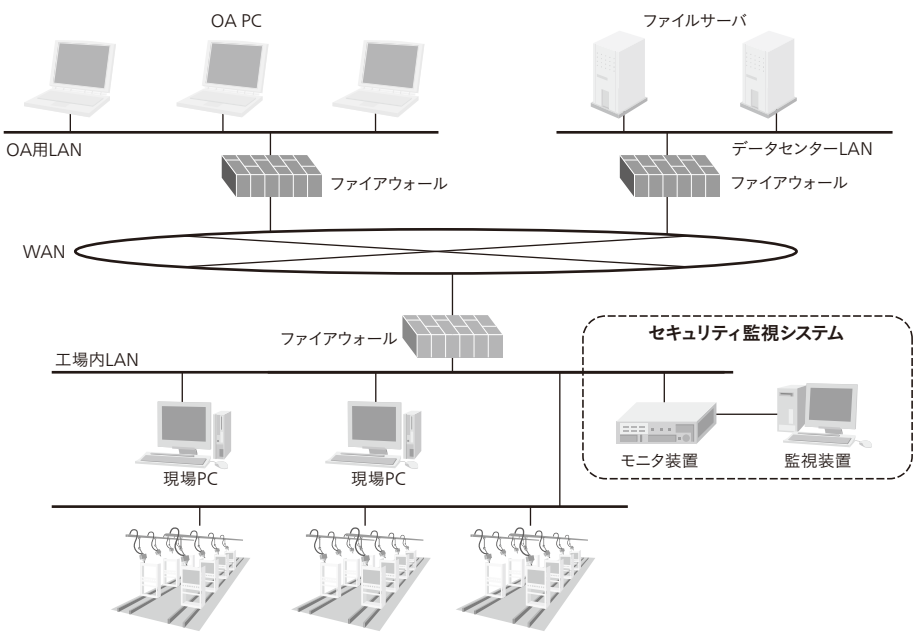
図3｜セキュリティ統合監視

日立が提案するセキュリティ統合監視方式を示す。



注：略語説明
CSIRT（Computer Security Incident Response Team：インシデント対応組織），
CISO（Chief Information Security Officer：最高情報セキュリティ責任者），
OT（Operational Technology）

図4｜工場実証システム構成
制御セキュリティ監視実証のシステム構成を示す。



注：略語説明
WAN（Wide Area Network），LAN（Local Area Network）

3.3
社内のIT×OT環境を利用した実証

現在，社内工場を対象に制御セキュリティ監視の実証を進めている。**図4**に実証システム構成を示す。セキュリティ監視システムは，工場内LAN（Local Area Network）を監視するためのモニタ装置と，モニタ装置のログを監視･分析する監視装置から成る。これにより，例えば工場内LANに不正なPCを接続したなどといったインシデントを検知し，現場の保守担当者に通知できる。

またITからOTへの侵入などさまざまな攻撃パターンに対応するために，ITとOTのログ相関分析や，外部からのセキュリティ脆（ぜい）弱性情報をシステム構成情報と照合して脆弱性管理などを行うセキュリティ統合監視の実証も現在進めているところである。

4. グローバルセキュリティ監視の取り組み

4.1
脅威のグローバル化

企業経営のグローバル化が進む中，ビジネスの基盤を支えるITは重要なキーとなっており，海外拠点を相互に接続した環境下で，24時間世界中の至る所で業務が行われている。一方で情報セキュリティに視点を移すと，ITの管理が各拠点に分散していることや利用者のITリテラシーの違いにより，各拠点単位でセキュリティレベルに違いが出てしまいがちである。このような状態を放置しておくと，セキュリティレベルの低い海外拠点を攻撃起点として瞬時に被害がグローバルに拡大してしまう傾向にあり，グローバルレベルでセキュリティ監視・情報の連携を行うことは企業のビジネス継続の観点でも重要な対応と言える。

日立システムズグループ（株式会社日立システムズおよびHitachi Systems Security Inc.）は，世界4拠点で，4つの言語（英語，フランス語，スペイン語，日本語）をサポートしたSOCサービスを45か国の顧客へ提供している[3]（**図5**参照）。

4.2
地域ごとのセキュリティレベルを リアルタイムに把握・是正

日立システムズが提供するSOCサービスを別の言葉に例えるなら，「顧客にとってのITのセキュリティドクター」である。SOC事業者の責務は，顧客のセキュリティを安全なレベルに維持するために監視を通して是正を支援することである。

セキュリティリスクを最適なレベルで維持するには，

図5｜日立システムズグループで展開しているSOCのグローバル拠点

グローバル4拠点において，「One SOC-One Process」をキャッチフレーズに，4極で同じSOC運用基盤を用い，業務プロセスを効率的に回す運用を実現している。

各地域の現状のセキュリティリスクを認知し対応者へ情報の連携がなされた後，確実に対処することが必要である。日立システムズのセキュリティ監視では，地域・部門ごとのIT資産別にセキュリティリスクを管理でき，視覚的かつ定量的に管理者が問題を認識するビューを用意している。また，セキュリティリスクは世間の情勢やシステムの状態とともに変化するものであり，日々忙しい管理者が常に状態を監視するのは現実的でない。このサービスでは一定のリスクレベルを超えたIT資産に対して，管理者へ問題点と推奨策をリアルタイムに発報する仕組みを提供している。

4.3 「人」，「プロセス」，「技術」の融合

クオリティの高いサービスをグローバルに提供するには，4つの拠点SOCが「技術」，「人」を効果的に運用するための「プロセス」が密接に絡み合った運用モデルでなければならない。日立システムズでは「人」，「プロセス」，「技術」を効率的かつ有機的に連携する手段として，Hitachi Systems Securityが開発した共通のオペレーション基盤「ArkAngel」を用いてサービスを提供している。「ArkAngel」は，セキュリティアナリストの専門知識を最大限に活用できるナレッジベースの基盤であり，大量のセキュリティイベントを相関的に分析する機能を中心に，サービス提供に必要な機能を兼ね備えている。この基盤を，経験と専門知識を有したセキュリティアナリストが世界中から集まったナレッジをベースに同じプロセスで運用することで，クオリティを落とさずにサービスを提供している（**図6**参照）。

今後もグローバルに事業展開する日立の強みを生かし，サービス内容を強化していく予定である。

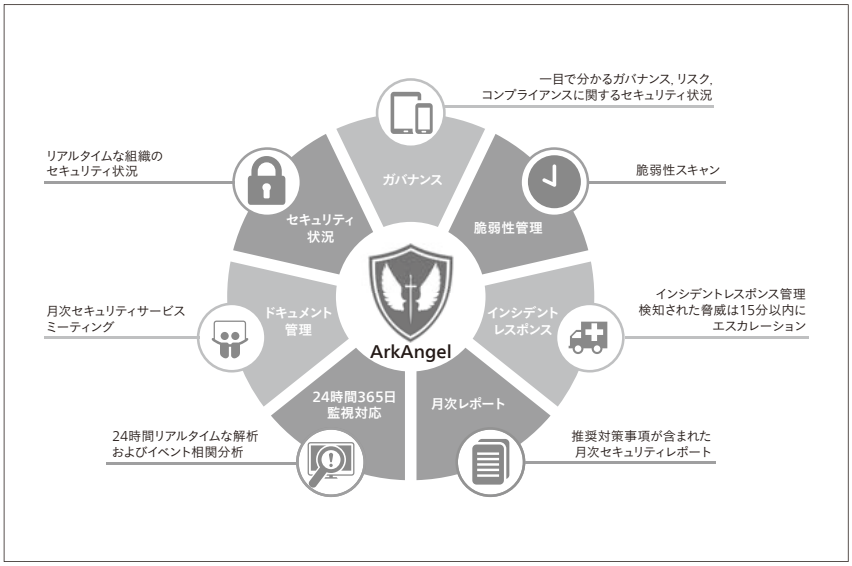


図6｜SOC運用基盤ArkAngelの概要

セキュリティアナリストがSOC運用を効率的に実施できるように設計された，Hitachi Systems Securityが開発した独自のSOC運用基盤である。

5. おわりに

本稿では，社会インフラを守るためのソリューションとして，制御システム向けのリアルタイム不正侵入検知技術，不正侵入検知後の一次対処と事業継続判断を支援する「統合監視ソリューション」，およびグローバルセキュリティ監視の取り組みについて紹介した。

日立は今後も最新技術の開発を進め，安全・安心な社会インフラの実現に向けたソリューションを提供していく。

謝辞

本稿の2章で紹介した「日立アノマリ検知装置」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）の研究開発の成果を活用し，日立製作所が開発したソフトウェア製品である。

参考文献など

1）国立研究開発法人新エネルギー・産業技術総合開発機構，日立製作所 ニュースリリース：サイバー攻撃の脅威を早期に検知する新規アルゴリズムを開発，「Hitachi Anomaly Detector」として製品化へ（2017.10），
http://www.nedo.go.jp/news/press/AA5_100845.html,
http://www.hitachi.co.jp/New/cnews/month/2017/10/1002.html

2）制御システム向けセキュリティ監視ソリューションホームページ，
http://www.hitachi.co.jp/products/it/security/solution/integrated/monitoring/index.html

3）株式会社日立システムズ ニュースリリース，カナダのグループ企業であるアバブセキュリティ社の社名を日立システムズセキュリティに変更（2017.7），
https://www.hitachi-systems.com/news/2017/20170710.html

執筆者紹介

飯田 恒雄
日立製作所 サービス＆プラットフォームビジネスユニット
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
サイバーセキュリティ技術本部
セキュリティイノベーション推進センタ 所属
現在，セキュリティの技術統括事業に従事
技術士（情報工学部門）
情報処理学会会員

原田 宏美
日立製作所 サービス＆プラットフォームビジネスユニット
サービスプラットフォーム事業本部 IoT・クラウドサービス事業部
エンジニアリングサービス第1本部
エッジコンピューティング部 所属
現在，セキュリティソリューション開発に従事

野末 大樹
日立製作所 サービス＆プラットフォームビジネスユニット
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
マネジメント本部 セキュリティ企画部 所属
現在，セキュリティ統合監視事業に従事
日本物理学会会員

大森 雅司
株式会社日立システムズ ネットワークセキュリティサービス事業部
ネットワークセキュリティオペレーション本部 第一部 所属
現在，セキュリティ事業における企画・検討に従事
公認内部監査人
公認情報システム監査人
公認情報セキュリティマネージャー
CISSP

Guillaume Daleux
Hitachi Systems Security Inc., Operation Division,
Managed Security Services Department 所属
現在，顧客システムのセキュリティの設計，最適化の支援およびサービスのグローバル展開事業に従事