産業分野の事例
日立計装システムにおける制御セキュリティの対応

金子 茂則 Kaneko Shigenori
森田 和信 Morita Kazunobu
須永 朋之 Sunaga Tomoyuki
村上 仁志 Murakami Hitoshi
村上 牧子 Murakami Makiko
花島 勝美 Hanashima Katsumi

産業分野においては，工場の生産ライン・生産管理システムは，一般に更新サイクルが長く，今なお古い機器を使っていることが多い。従来は，外部との接続をしないことでシステムを守っていたが，ビッグデータ活用やIoTの適用により外部との接続が避けられないものとなり，セキュリティに関する脅威にさらされるように変わりつつある。

このような状況の下，日立は，生産ライン・生産管理システムとの親和性を重視したセキュリティ対策を3つのホワイトリストに分けたコンセプトに基づき，ひな型化により生産現場の負担を軽減したセキュリティ強化の方法を提案している。

1. はじめに

産業分野においては，プラントや工場における生産性を上げるために，新規設備の建設や既設設備の延命・稼働率向上の一つの手段として，運転データのビッグデータ解析，設備や装置の状態をデータとして収集するためのIoT（Internet of Things）の適用などが進められつつある。

運転データのビッグデータ解析のために設備側のデータをクラウドサーバへ送る，IoT化のために無線やキャリア回線を使用するなど，制御システムが外部システムとつながることが必然となっている。

このような中，サイバーセキュリティ基本法が公布され，重要インフラ13分野が規定されており，産業分野の生産設備のサイバーセキュリティ対策が重要視されてきている。しかし，現場では，設備稼働や生産性確保の対応が優先されており，上流コンサルティングから入り，システムに対する脅威分析をしたうえで，セキュリティ装置の設置とパラメータ設定を行うという通常の対応は，作業負担増となるため，積極的に推進することが困難な状況にある。

日立では，生産設備としての，生産ライン・生産管理システムを構成する計装システムにおいて，セキュリティ対策のひな型を定義することが重要であると考えている。このひな型に基づいて，システムを提案・提供することにより，現場側の負担を増やさずにセキュリティ対策ができるソリューションの提供をめざし，その取り組みを強化している。

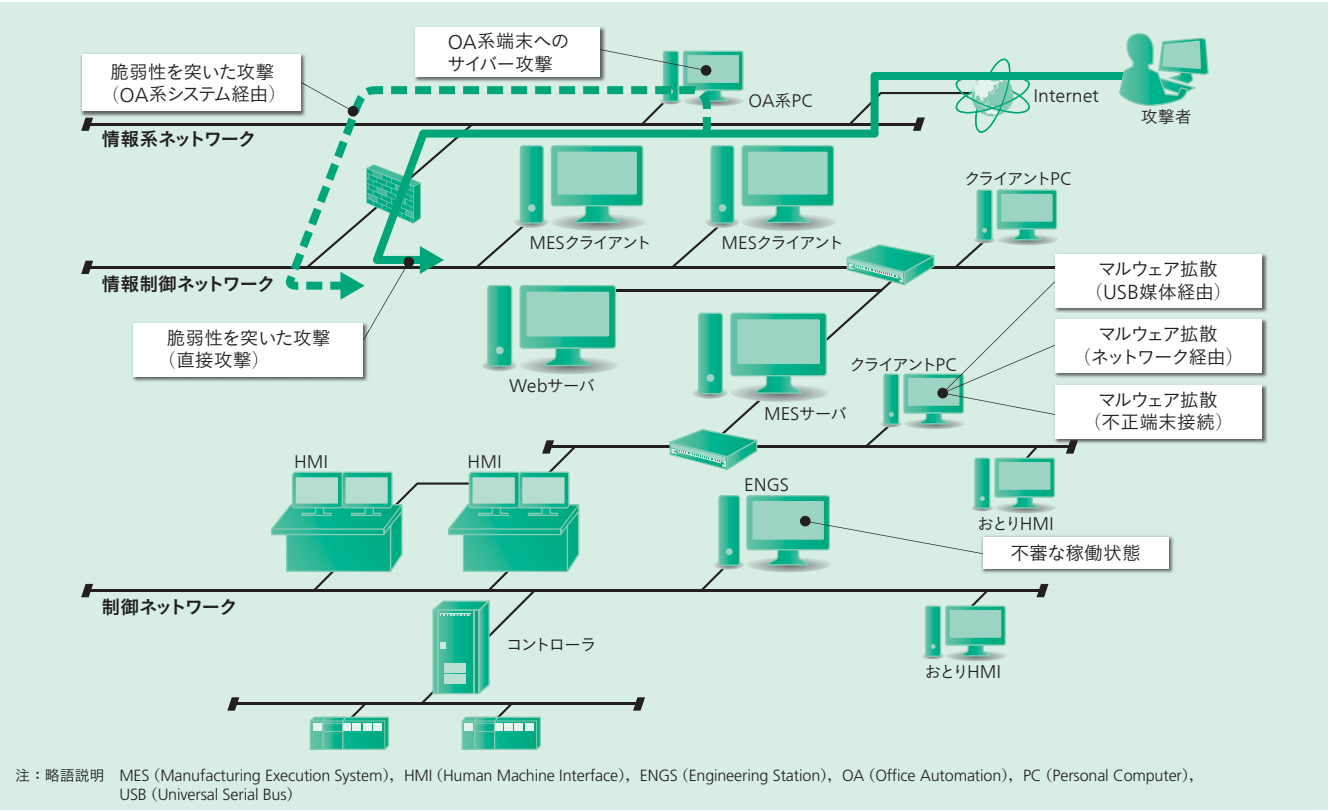
ここでは，このソリューションについて述べる。

2. 生産ライン・生産管理システムの特徴と課題

生産ライン・生産管理システムにおける計装システムのシステム構成は，基本的には，MES（Manufacturing Execution System）を構成するクライアントとサーバ，DCS（Distributed Control System）を構成するHMI（Human Machine Interface）とENGS（Engineering Station），コントローラ，これらをつなぐネットワークとなっている。

現在，このシステムにおいて，オフラインシステムだから安全であるという従来の考えが大きく崩れてきている。ビッグデータ対応や，IoT化の結果として，制御システムが外部システムとつながること以外にも，ネットワークによる遠隔監視やOA（Office Automation）系システムとの接続，可搬記録媒体［USB（Universal Serial Bus）メモリ］の活用などにより，ファイアウォールを介して接続されてはいても，遠隔監視やOA系システムを経由したサイバー攻撃や直接の攻撃を受けるリスク，マルウェアに感染するリスクが高くなっている（図1参照）。

これらのリスクに対応するセキュリティ対策のひな型を考えるため，システムの特徴と課題を整理した。結果として，ひな型において，以下の3点が重要であると判断した。



注：略語説明　MES（Manufacturing Execution System），HMI（Human Machine Interface），ENGS（Engineering Station），OA（Office Automation），PC（Personal Computer），USB（Universal Serial Bus）

図1｜生産ライン・生産管理システム概要とセキュリティに関する脅威

標準的な生産ライン・生産管理システムを定義し，ひな型とすることにより脅威分析およびセキュリティ対策をひな型化する。予算やシステムに合わせた，対策レベルの選択と段階的システム強化を可能としている。

(1) システムの寿命が長いこと

ITシステムを構成するハードウェアやソフトウェアの維持保守期間は5～7年であることに対し，生産ライン・生産管理システムでは10～20年と長期にわたり使用する。

このため，ソフトウェア，特にOS（Operating System）のサポート期間が切れ，セキュリティパッチの提供がされない状態となっても使い続けるという課題がある。

(2) システムを停止できないこと

情報セキュリティにおいては，機密性・完全性・可用性の3要素の対応が重要とされるが，その中でもシステムを停止できないという可用性が優先される場合が多い。

このため，セキュリティパッチやセキュリティ対策ツールによる頻繁な更新（再起動が必要）が行えないという課題がある。

(3) レスポンス遅延がクリティカルな場合があること

レスポンス遅延が許されないタイムクリティカルなシステムがある。

このようなシステムの場合，セキュリティパッチの適用やツールの導入が，レスポンス遅延の致命傷につながる可能性がある。また，システムのレスポンスに与える影響を見極めることが必須であり，システム稼働後のプログラムの追加が難しいという課題がある。

3. 生産ライン・生産管理システムのセキュリティ要件と対策コンセプト

前章で整理した特徴と課題から導き出される要件を以下に述べる。

3.1 セキュリティ要件

(1) オフラインシステムであること

要件の1番目は，これまでのセキュリティ対策の延長の発想で，外のシステムとは接続されないオフライン状態のネットワーク環境で運用するオフラインシステムへ対応できることである。外部との接続が必須となってきているものの，オフライン環境にあるシステムは，まだ多数存在する。この場合，シグネチャーやパターンファイルをリアルタイムでアップデートできないため導入時の環境でセキュアな状態を維持する必要がある。

(2) システム寿命が長いこと

要件の2番目は，OSへ導入するツールは，レガシーOSで動作する必要があることである。さらに，長期利用のため，サポート期間が切れたOS上でも動作する必要がある。

(3) システムを停止できないという可用性が優先されること

要件の3番目は，システムの停止・再起動をさせないことである。システムの停止が，事業そのものの継続性に直結するため，ソフトウェアのアップデートなどによるシス

テムの停止・再起動を最小限にとどめる必要がある。

(4) タイムクリティカルなシステムであること

要件の4番目は，レスポンス遅延が発生しないことである。セキュリティ対策の適用で，レスポンス遅延が発生するとクリティカルな問題に発展する可能性が非常に高い。

3.2　対策コンセプト

生産ライン・生産管理システムが停止せず，事業を継続することを目的として上項で述べた要件を満たすため，マルウェア感染を前提としながらも，感染のリスク低減と感染時の早期検知による周辺への拡散防止を多段防御の仕組みで実現することが効果的である。

日立では，以下に述べる3つのホワイトリストのコンセプトを提案している。

(1) アプリケーションのホワイトリスト化

(2) ネットワークに接続する機器のホワイトリスト化

(3) 制御系ネットワークの通信のホワイトリスト化

4.　生産ライン・制御システムのセキュリティ対策提案

(1) アプリケーションのホワイトリスト化

日立が適応を確認した市場流通ホワイトリスト型セキュリティ製品を適用し，動作するアプリケーションを限定することで，ひな型に沿ったシステムと親和性のある対応を可能とした（図2参照）。

(2) ネットワークに接続する機器のホワイトリスト化

ネットワークに接続してもよい機器を限定することで，ネットワークをホワイトリスト化する（図3参照）。

日立では，不正接続検知装置「NX NetMonitor」を製品化している。ネットワークに外付け，後付けでの設置が可能なため，新設・既設を問わず，システムと親和性のある設置ができる（図4参照）。

(3) 制御系ネットワークの通信のホワイトリスト化

制御系ネットワークでは，生産ライン・生産管理のシステムが物理的に存在するため，通信する相手も事前に決定することができ，許可されていない通信を検知することができる。この特性を利用して，通信のホワイトリスト化を実現している（図5参照）。

許可されていない通信の検知は，日立が製品化している「HighR-Switch」（図6参照）や，セキュリティ専業ベンダーが提供している製品を適用することによって実現している。これらの製品とシステムとの親和性を確保するため，

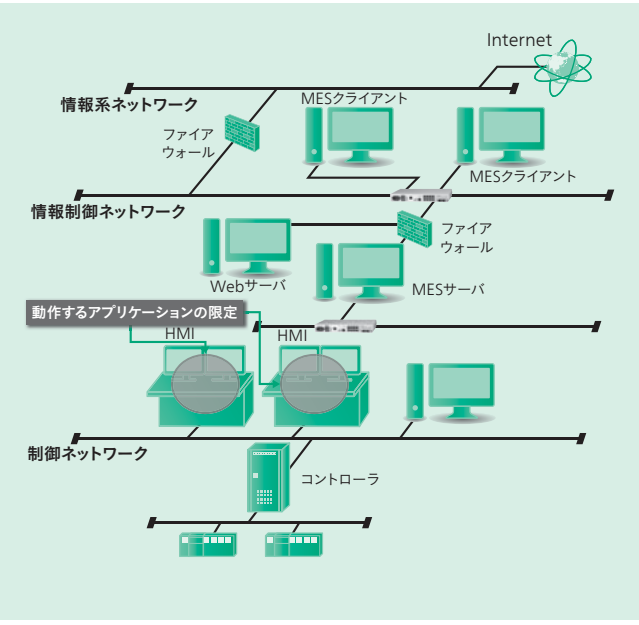


図2｜アプリケーションのホワイトリスト化
HMIで動作するアプリケーションを限定することで，システムを守る。

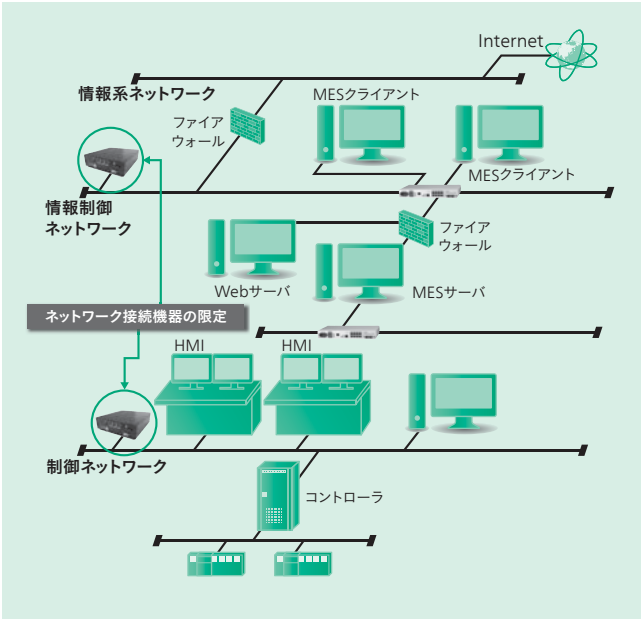


図3｜ネットワークに接続する機器のホワイトリスト化
ネットワークに接続できる機器を限定することで，システムを守る。

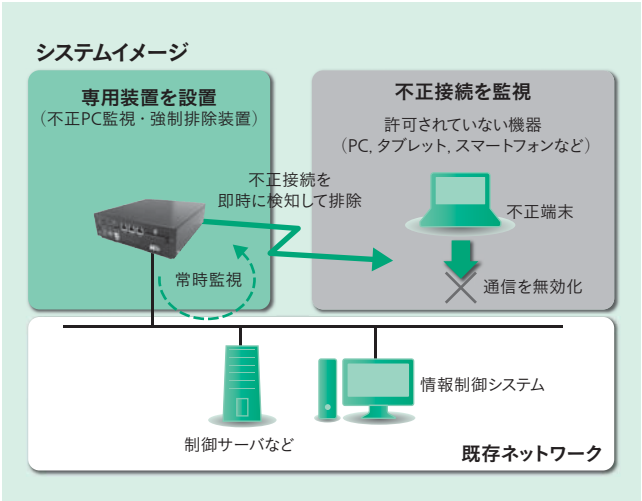


図4｜不正接続検知装置「NX NetMonitor」
未登録の機器がネットワークに接続しようとするのを検知し，自動的に排除することで，サイバー攻撃の脅威を防ぐ。

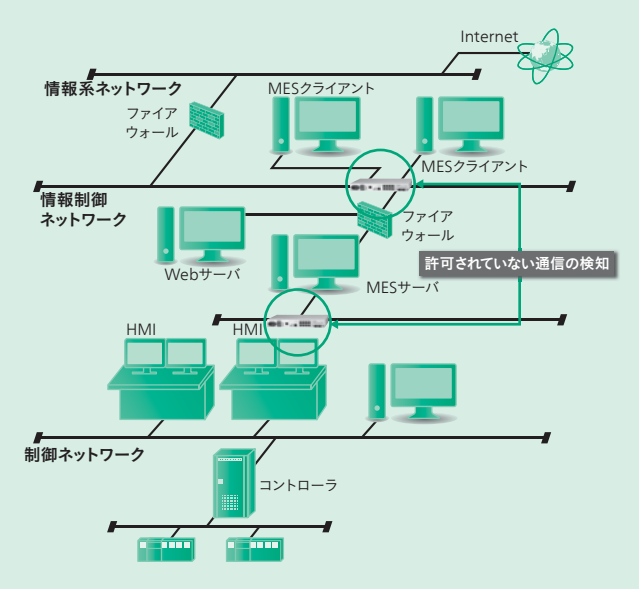


図5｜制御系ネットワークの通信のホワイトリスト化
許可されていない通信を検知する仕組みをネットワークに付加して，システムを守る。

図6｜「HighR-Switch」
耐環境性の強化により現場設備への設置を可能とした。一般的なネットワーク機能に加え，未登録の通信を検知し，自動的に排除する。

新設・既設のシステムを考慮した組み合わせで評価・検証することで，日立提案のひな型における型を定義し，現場での容易な導入が可能となるものと考える。

5. おわりに

ここでは，生産ライン・生産管理システムの特質に応じながら，現場側を考慮し，導入をしやすくする，ひな型に基づくセキュリティ対策の事例について述べた。

今後，日立は，自社国産技術を大切にしつつ，顧客のシステムを守るため，トータルソリューションとして，日立総合計装システム「EX-N01」や，日立デジタル統合監視制御システム「HIDIC-AZ/SP G2」への適用も含め，適切なセキュリティ対策商材の組み合わせで，セキュリティエコシステムの提供に取り組んでいく考えである。

参考文献

1） 遅野井，外：現場データ利活用を実現する情報制御プラットフォーム，日立評論，98，3，201～205（2016.3）
2） 大久保，外：セキュリティ堅牢性を備えたシステムを構成するプラント監視制御システム，計装，Vol.58，No.12，p.34～37（2015.12）

執筆者紹介

金子 茂則
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
制御プラットフォーム統括本部 制御プラットフォーム開発本部 所属
現在，制御システムのコンポーネント開発に従事
情報処理学会会員，計測自動制御学会会員，
プロジェクトマネジメント学会会員

森田 和信
日立製作所 産業・流通ビジネスユニット
産業ソリューション事業部 産業製造ソリューション本部 所属
現在，産業製造ソリューション事業の取りまとめに従事

須永 朋之
日立製作所 産業・流通ビジネスユニット
産業ソリューション事業部 産業製造ソリューション本部
産業システムエンジニアリング部 所属
現在，産業向け計装システムの取りまとめに従事

村上 仁志
株式会社日立ハイテクソリューションズ 計装システム統括本部
計装システム営業本部 計装技術部 所属
現在，産業向け計装システムの事業企画に従事

村上 牧子
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
制御プラットフォーム統括本部 制御プラットフォーム開発本部
制御プラットフォーム開発部 所属
現在，産業向け計装システムのミドルソフトウェア開発に従事

花島 勝美
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
制御プラットフォーム統括本部 制御プラットフォーム開発本部 所属
現在，産業向け計装システムのミドルソフトウェア開発の取りまとめに従事