特集論文

サイバー攻撃から生産ラインを守る新たなネットワーク脅威対策技術

木村敏之*
Toshiyuki Kimura

New Network Threat Countermeasure Technology to Protect Production Lines from Cyber Attacks

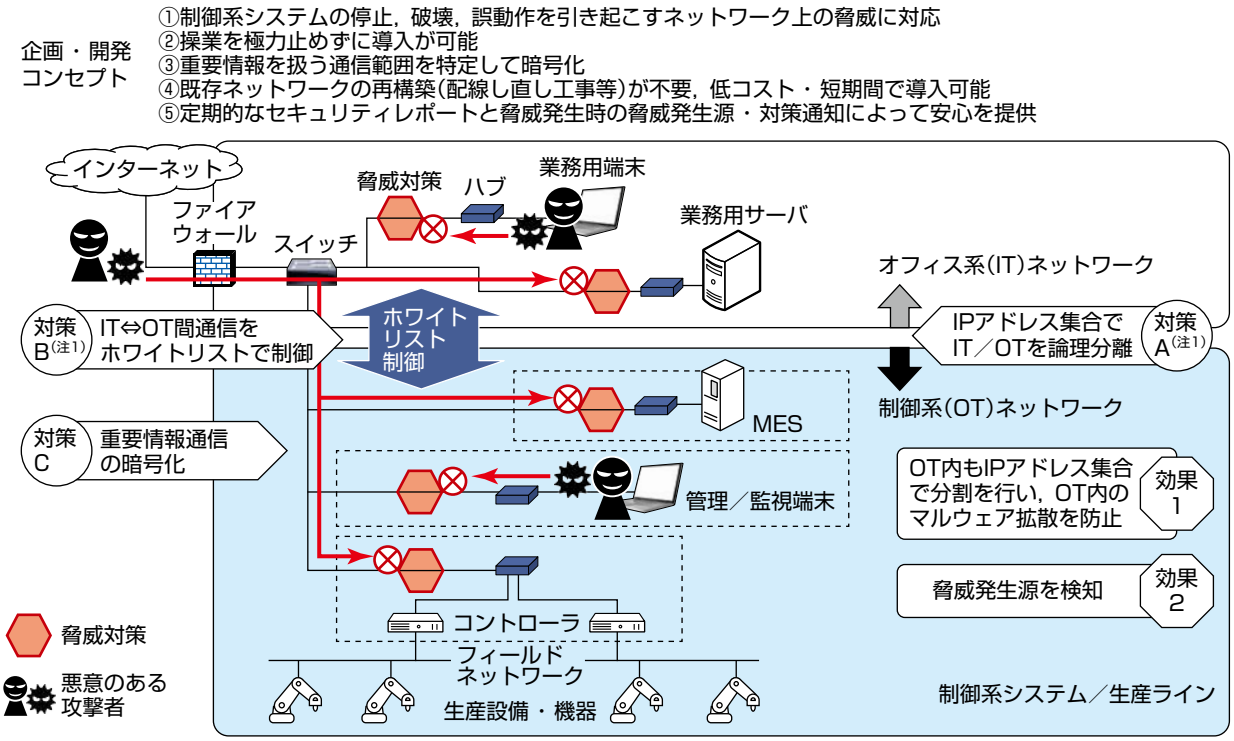
要　旨

三菱電機では，暗号化通信を行うネットワーク製品とネットワークインテグレーション技術によって，1990年代からネットワークセキュリティ事業を展開している。

近年，企業ネットワークを標的にしたサイバー攻撃などのネットワーク脅威は年々増加しており，被害も増大傾向にある。さらに攻撃の対象は，制御系ネットワーク(以下“OT(Operational Technology)ネットワーク”という。)にも拡大している。一方，IoT(Internet of Things)化の急激な進展によって，ネットワーク接続に対応した生産設備・機器(以下“OT機器”という。)が増加・多様化し，生産ラインにネットワークを導入して生産と経営の情報を共有した生産性向上の取組みが拡大している。

そのため，ネットワーク脅威から生産ラインを守ることは喫緊の課題になっており，オフィス系ネットワーク(以下“IT(Information Technology)ネットワーク”という。)とOT機器を対象にしたOTネットワークが混在する環境に対して，既存ネットワーク構成へ大きな影響を与えずに，低コスト・短期間で導入可能なネットワーク脅威対策が求められている。

今回，これらの課題に対して，IT-OT間のネットワーク通信を維持しつつ論理的な分離を可能にして，脅威の感染拡大を防止する“新たなネットワーク脅威対策技術”を開発した。この技術は，既存ネットワーク構成への影響を抑えられる特長があり，特にITとOTのネットワークが混在する環境に対して，操業を極力止めずに，低コストで容易な導入を可能にする。



(注1)　本稿では対策A・Bについて述べる。
IP：Internet Protocol，MES：Manufacturing Execution System(製造実行システム)

サイバー攻撃から生産ラインを守る“新たなネットワーク脅威対策技術”の概念図

本稿で述べる“新たなネットワーク脅威対策技術”は，既存ネットワーク構成を変更せずにIT-OT間通信を論理的に分離してセキュリティ脅威の感染拡大防止を行う。また，複数のIP(Internet Protocol)アドレスをグループ化して分離したネットワーク間の通信許可／不許可のルールを簡単設定，不正通信発生時の発生元通知と定期的なセキュリティレポート，重要情報を扱う通信範囲を特定した暗号化(情報漏洩(ろうえい)，改ざん，なりすましの防止)という特長がある。

*インフォメーションシステム統括事業部

1. まえがき

製造業では，ネットワークに接続する生産ラインのOT機器が年々増加・多様化しており，これらのOT機器も活用した生産性向上などを進めるためには，脅威への不安はあるもののITネットワークと接続せざるを得ない状況が強まっている。一方，ITネットワークを経由したサイバー攻撃(例：破壊，データの搾取や改ざん)も年々増加しており，これらの脅威からOT機器を守ることも求められている。

OTネットワークは無停止又は長期間の稼働が求められる場合が多く，OS更新(OSの最新状態化)やパッチ適用(プログラムを不具合修正版に更新)が行いにくいなどの制約がある。また，ITネットワークから独立した環境下では，USBメモリなどの記憶媒体を用いた情報授受を行う場合があり，OT機器が記憶媒体を介してマルウェア感染し，さらに，それを踏み台とした不正アクセスが行われるなどの脅威がある。

これらへの対策としては，必要な通信だけを行える状態で，ITとOTのネットワークを分離することが確実かつ有効であり，物理的分離と論理的分離の２種類の方式が考えられる。構成の明快さからの最善策は，物理的にネットワークを分離してDMZ(DeMilitarized Zone：非武装地帯)を設ける方式であり，新設ネットワークではこの方式が望ましい。しかし，既存ネットワークに適用する場合は，配線し直しとそれに伴う操業停止，IPアドレス振り直しによるネットワーク再構築などの課題がある。

本稿では，ITとOTのネットワークが混在する環境で起こり得るこれらの課題を解決するために開発した，低コスト・短期間で容易な導入を可能にする“新たなネットワーク脅威対策技術”について述べる。

2. OTネットワークの特徴と脅威対策の課題

2.1 近年のOTネットワークでの脅威と課題

従来，製造業の生産ラインや社会インフラのシステムでは，OT機器などを接続したOTネットワークは，業務用端末などのIT機器を接続したITネットワークから独立した構成になっていた。しかし，OT機器のIoT化によってITとOTのネットワークが混在した構成が増加するに伴い，サイバー攻撃がOTネットワークに対しても行われるようになってきた。最近の攻撃は，件数増加だけでなく悪質化・巧妙化しており(**図１**)，早期の対策が重要視されている。

また，攻撃を受け，OTネットワークが悪意のある攻撃者に乗っ取られると，生産活動停止だけでなく，テレビ放送中断や停電など，重要な社会インフラの停止に至る場合もあり(**表１**)，その被害は我々の生活にも影響する。そのため，OTネットワークへの脅威対策は，より重要度が増している。

2.2 OTネットワーク特有の事情

OTネットワークは，無停止又は長期間の稼働が求められるため，OT機器に対するOS更新やパッチ適用が行いにくく，サポート切れの古いOSのまま使用されている場合もある。また，パソコンのように表示装置を持たないOT機器もあり，人の目による監視が行き届きにくく，サイバー攻撃を受けていることに気づきにくいという特有の事情がある。

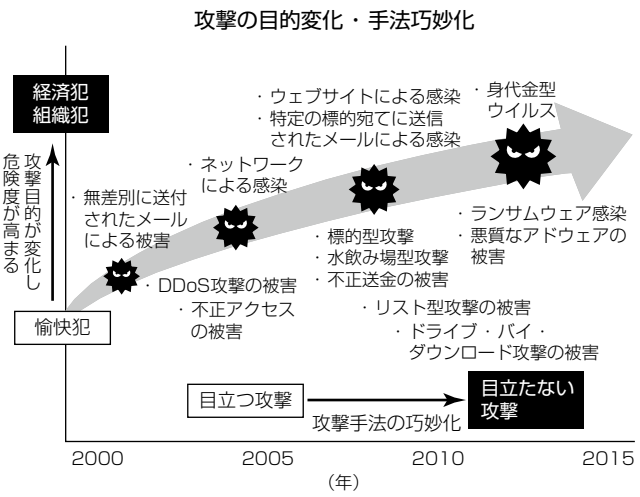


図１．サイバー攻撃の変化[1]

表１．OTネットワークへのサイバー攻撃事例[2]

時期	業界／分野	事例・影響・被害
2014年12月	製造(鉄鋼)	ドイツ国内の製鉄所への標的型攻撃。 溶鉱炉が正常にシャットダウンできず，装置及び製鉄システム(操業)に大きな損害を与える事件が発生した。
2015年４月	放送	フランス国内の国際放送局へのサイバー攻撃。 大規模なサイバー攻撃を受け，番組の放送ができない状況に陥った。
2016年12月	電力	ウクライナ国内の電力施設でのマルウェア感染。 首都キエフ北部とその周辺地域で停電が発生した。手動運用に切り替え，30分以内に電力供給が再開され，約１時間15分後に完全に復電した。
2017年６月	製造(自動車)	日本国内の自動車の生産システムでのランサムウェア感染。 自動車の生産工場で，工場設備に付帯するパソコンがWannaCryに感染しているのが発見され，約１日間生産ラインを停止し，1,000台が生産できなかった。他工場への影響はなく，同工場も翌日には操業を再開した。
2018年８月	製造(半導体)	台湾の世界的半導体チップメーカーでのランサムウェア感染。 重要なコンピュータがWannaCryの亜種に感染し，複数の工場で生産ラインが停止した。影響の大きかった工場では生産再開に約３日かかった。

表２．ネットワーク脅威対策の課題

課題A	コスト負担増	・配線し直し ・配線し直し工事中の操業停止 ・IPアドレス振り直しに伴うネットワーク再構築
課題B	導入に時間が必要	

2.3　OTネットワーク脅威対策の課題

ITとOTのネットワークが混在する場合のネットワーク脅威対策は，ITとOTのネットワークにそれぞれ分離して，両ネットワーク間通信を局所化することである。分離の方法には，物理分離及び論理分離の２種類あり，どちらの方法も大きく二つの課題が存在する。

一つ目の課題はコストである。物理分離を行う場合，稼働中の既存ネットワークに対して，新たにネットワークを配線し直すためのコストが発生する。論理分離を行う場合は，VLAN(Virtual LAN)を構築する場合が多く，ネットワークに接続するOT機器に対して設定変更作業(IPアドレスの振り直しなど)が必要になり，OT機器の数量に応じた設定変更作業コストが発生する。

二つ目の課題は導入期間である。生産ラインや社会インフラのシステムは，無停止又は長期間の稼働が基本であり，ネットワーク脅威対策のためとはいえ，停止期間は極力短くする必要がある。よって，既存ネットワークを大きく変更せずに，そのまま活用しつつ，費用対効果が高く，短期間で導入可能な脅威対策が必要とされている。

表２に二つの課題を示す。

3．ネットワーク脅威対策技術の企画・開発

当社では，1985年に10BASE-5(最大伝送速度10Mbpsに対応したコンピュータネットワーク規格)に対応したネットワーク(LAN)接続装置として“MELNETシリーズ”を販売開始し，その後のLAN高速化，LAN間接続，インターネット，セキュリティ脅威などに対応してきた。さらに，当社の暗号化アルゴリズムである“MISTY”を活用した暗号化ルータを開発し，1995年に“MELWALLシリーズ”として販売開始した。

両シリーズで培った技術を活用して開発した暗号化通信を行う製品とネットワークインテグレーション技術を組み合わせて，1996年にネットワークセキュリティ事業を立ち上げ，顧客ニーズを先読みした製品の開発と販売を継続し，現在に至っている。また，30年余りのこの事業を通して，米国国立標準技術研究所(NIST)が示す[3]セキュリティプロセスの５機能(特定，防止，検知，対応，復旧)に対して，関連する技術を当社で持つに至った。

今回は，**表２**に示す課題A・Bの解決を目的にして，当社保有技術を活用した“新たなネットワーク脅威対策技術”を企画・開発した。

4．容易に導入可能な脅威対策

4.1　新たなネットワーク脅威対策技術の概要

今回開発した技術は次の二つである。

(1)　ネットワークの論理分離(IPアドレス集合)技術
(2)　ホワイトリスト生成技術

なお，この開発に当たっては，**表２**の課題A・Bの解決とともに，他社製品との差別化をより明確化するため，次の二点の実現もターゲットにした。

(1)　既存ネットワークのセグメント内で接続されるOT機器のIPアドレスを意識せずに後付け(追加)可能
(2)　段階的・部分的な導入を可能にし，操業への影響を局所化することが可能

4.2　ネットワーク論理分離(IPアドレス集合)技術

この技術は，**表２**の課題Aへの対応策になる。

接続端末(ネットワークに接続されるIT機器とOT機器)のIPアドレスを変更せずにITとOTのネットワークを論理分離するため，独立行政法人 情報処理推進機構のガイド[2]で示されている“重要資産を共通のセキュリティレベルを持つゾーンに分離”“侵攻拡散を防止するためにネットワークを複数のセグメントに分割して運用”などのセキュリティ対策も考慮して，従来のディストリビューション層ではなくアクセス層で行うことを可能にした。

ネットワーク論理分離(IPアドレス集合)の方式は，次のとおりである。**図２**にネットワーク分離方式の比較を示す。

(1)　接続端末のIPアドレスを検出する
(2)　検出された接続端末のIPアドレスをキーにしてグループ分けを行う
(3)　同一グループ内の接続端末は相互通信が可能，異なるグループの接続端末間はあらかじめ許可された通信以外は通さない(ホワイトリストで制御)

4.3　ホワイトリスト生成技術

この技術は，**表２**の課題Bへの対応策になる。

ホワイトリストとは受入れ対象を選別して受入れ又は拒絶する仕組みの一つで，受入れ対象リスト(例：通信許可するOT機器のIPアドレス一覧)を設定し，その設定にないものは拒絶することを可能にするリストである。ホワイトリストを生成するためには，個々の接続端末に対して接続条件などを考慮した複雑な設定作業が必要になる。

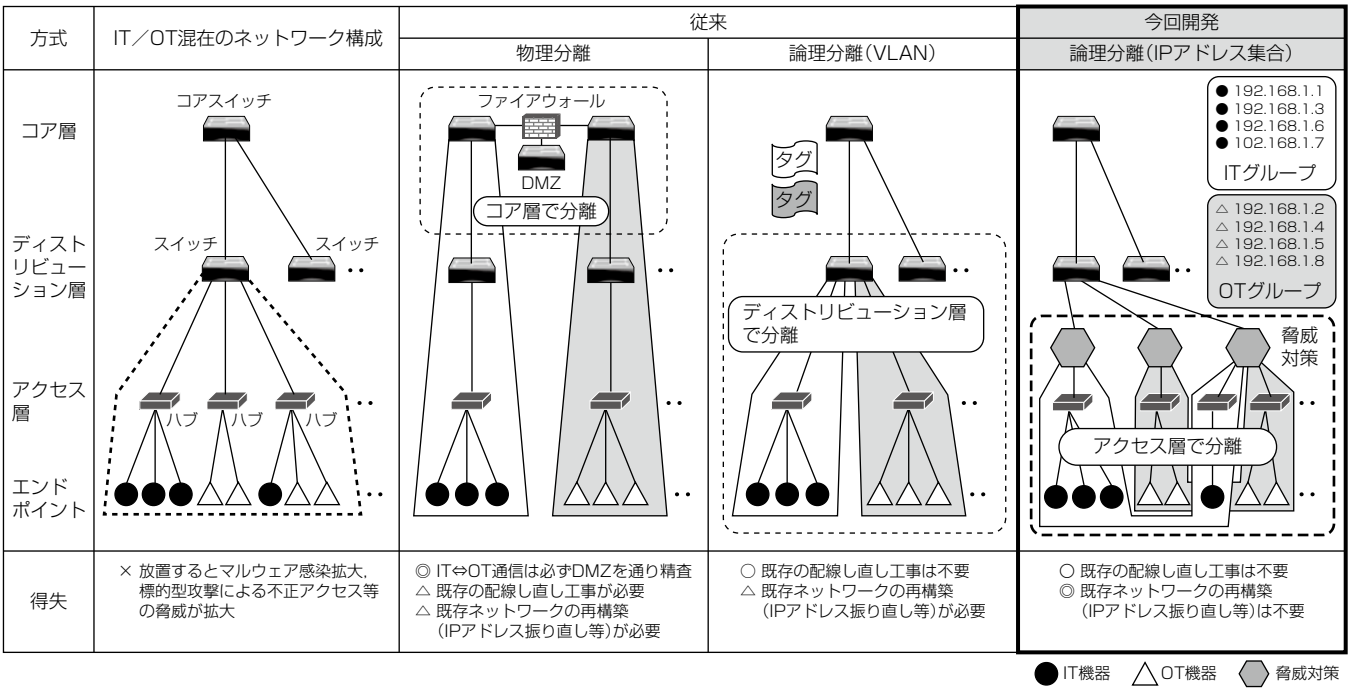


図２．ネットワーク分離方式の比較

表３．特願2020-003790の要点

背景	安全が確認された通信だけを許可するホワイトリスト方式によるトラフィック制御は，有効である反面，個々の端末に対して，ネットワーク接続条件や端末条件を考慮した複雑な設定が必要であるため，ホワイトリスト生成及び管理は運用面で負担になる。
特長	この発明では，ネットワークに接続された複数の端末について，接続端末の一覧を自動生成し，その一覧からネットワーク管理者が接続端末のグループ分けを行うことを可能にし，そのグループ単位でホワイトリストを生成する。また，生成時には，同一グループ間通信は自動的に“許可”，異グループ間通信は通信ログに基づいてネットワーク管理者が“通信可否”の設定を行うことを可能にした。
効果	次のような場合で，ネットワーク管理者の負荷軽減が可能になる。 ・通信可否が明確ではない異グループ間通信だけネットワーク管理者が通信可否を設定可能 ・ネットワークが変更された場合でも，変更の影響を受けるグループだけ再設定

従来は，その設定作業をネットワーク管理者が実施しており，その業務負担が課題になっていた。

今回，ネットワークに接続される接続端末の一覧を自動生成するとともに，接続端末間の通信がIT－OT間通信のセキュリティポリシーに合うか否かをネットワーク管理者が確認した上で，通信の不許可／許可の設定を可能にする新たな方法を開発し，特許出願（特願2020－003790）を行った（**表３**）。

この開発によって，セキュリティポリシーとホワイトリスト生成結果を一括して管理可能になり，設定誤りなどの抑制，導入に伴う手順・作業の簡便化（時間短縮）の効果が見込める。

4.4 製 品 計 画

2020年度内に，今回開発したネットワーク論理分離（IPアドレス集合），ホワイトリスト生成，及び重要情報通信の暗号化技術を搭載した新たなネットワークセキュリティ製品の販売開始を計画している。

5. む す び

生産ラインを持つ企業などに存在するITとOTのネットワークが混在する環境に対し，導入容易な論理分離を可能にして，ITネットワークを経由したOTネットワークへのサイバー攻撃やOTネットワーク内でのマルウェア感染を防止する，“新たなネットワーク脅威対策技術”について述べた。

今後も時代の動きを先取りし，より安全で導入しやすい技術・製品に進化させ，社会に貢献していく。

参 考 文 献

(1) 相川　航：サイバーセキュリティ政策の最新動向，総務省（2019）
https://www.soumu.go.jp/main_content/000603219.pdf
(2) 情報処理推進機構（IPA）セキュリティセンター：制御システムのセキュリティリスク分析ガイド第２版（2020）
https://www.ipa.go.jp/files/000080712.pdf
(3) NIST：Framework for Improving Critical Infrastructure Cybersecurity Version 1.1（2018）
https://doi.org/10.6028/NIST.CSWP.04162018