特集論文

インダストリアルIoTネットワークセキュリティーサービス“CyberMinder IoT”の最新状況と展望

川邉喜彦*
Yoshihiko Kawabe
増田岳人*
Takehito Masuda

*三菱電機インフォメーションネットワーク㈱

Current Status and Future Prospects of "CyberMinder IoT": Industrial IoT Network Security Service

要　旨

近年，ランサムウエアが猛威を振るうようになり，大企業やそのサプライチェーンでも生産停止を余儀なくされる被害が発生している。このためDX(デジタルトランスフォーメーション)化が進む製造現場でセキュリティー対策の必要性がますます高まっている。

三菱電機インフォメーションネットワーク㈱(MIND)では，大企業から中小規模の製造現場(工場)に対処できるサイバーセキュリティー対策ソリューションとして，インダストリアルIoTネットワークセキュリティーサービス“CyberMinder IoT”を提供している。また，このサービスの提供を通して，日々進化するサイバー攻撃に合わせて最新の攻撃手法を分析し，提供するサービス内容のアップデートを図っている。

1. ま え が き

近年，技術の革新によって安価で高性能な汎用コンピューターが普及したことで，製造現場の産業用制御システムでは，様々な製造装置が汎用ネットワークに接続されるIoT(Internet of Things)化が進んだ。製造装置から生産データなどを収集し，生産ラインの稼働状況や品質データを蓄積することが可能になり，生産プロセスの効率化や品質向上，故障の予兆検知など，デジタル技術を活用した工場DXが進んでいる。一方で，これまで産業用制御システムは外部から独立していることでセキュリティーが保たれていたが，IoT化が進んだことによってセキュリティー侵害のリスクが増加し，実際に侵害を受けて生産が停止するなどの被害が発生している。

MINDでは，IoT化が進む産業用制御システムで，製造装置だけの対策ではなく，製造装置が接続されるネットワークにセキュリティー対策を実装することが有効であると考えている。製造現場向けのセキュリティー対策サービスとして，四つのソリューションから成るインダストリアルIoTネットワークセキュリティーサービス“CyberMinder IoT”を提供しているが，サイバー攻撃を取り巻く環境は日々変化しており最新の動向を常に注視しておく必要がある。

本稿では，攻撃者の視点でサイバー攻撃の手法をまとめたフレームワークであるMITRE ATT&CK(注1) for ICS(Adversarial Tactics, Techniques, and Common Knowledge for Industrial Control System)の分析結果と，CyberMinder IoTの最新状況と展望について述べる。

(注1)　MITRE，ATT&CKは，The MITRE Corp.の登録商標である。

2. MITRE ATT&CK for ICSの分析(1)

MITRE ATT&CKは米国の非営利団体であるThe MITRE Corp.が発行している，CVE(注2)(Common Vulnerabilities and Exposures)を基に，脆弱(ぜいじゃく)性を悪用した攻撃を戦術とテクニックの観点で分類したナレッジベースであり，サイバー攻撃でのフローと手法を体系化したフレームワークである。半期ごとに新たな攻撃や戦術，テクニックのデータが更新され続けているため，現在ではセキュリティーを強化する際のデファクトスタンダードになりつつある。また，MITRE ATT&CKでは，標的とするシステムによって異なる攻撃手法に応じて戦術やテクニックを展開している。

MINDでは，CyberMinder IoTの最新の攻撃への対応状況を評価するため，産業用制御システムに対応するMITRE ATT&CK for ICSについて注目し分析した。

MITRE ATT&CKでサイバー攻撃を防御する側に向けて提供されている対策を緩和策と呼ぶ。MITRE ATT&CK for ICSでは分析を実施した時点で51項目の緩和策が定義されていた(2024年1月時点で52項目)。そこで各緩和策を，製造装置の設計や設定の見直しによって緩和が可能なもの，何らかの対策の導入によって緩和が可能なもの，組織や運用に

よって緩和が可能なもの，に整理した(**表１**)。一つの緩和策に対して複数箇所で対応が必要なケースもあり，緩和策の総数と**表１**の項目数は一致しない。

表１－緩和策の分類表

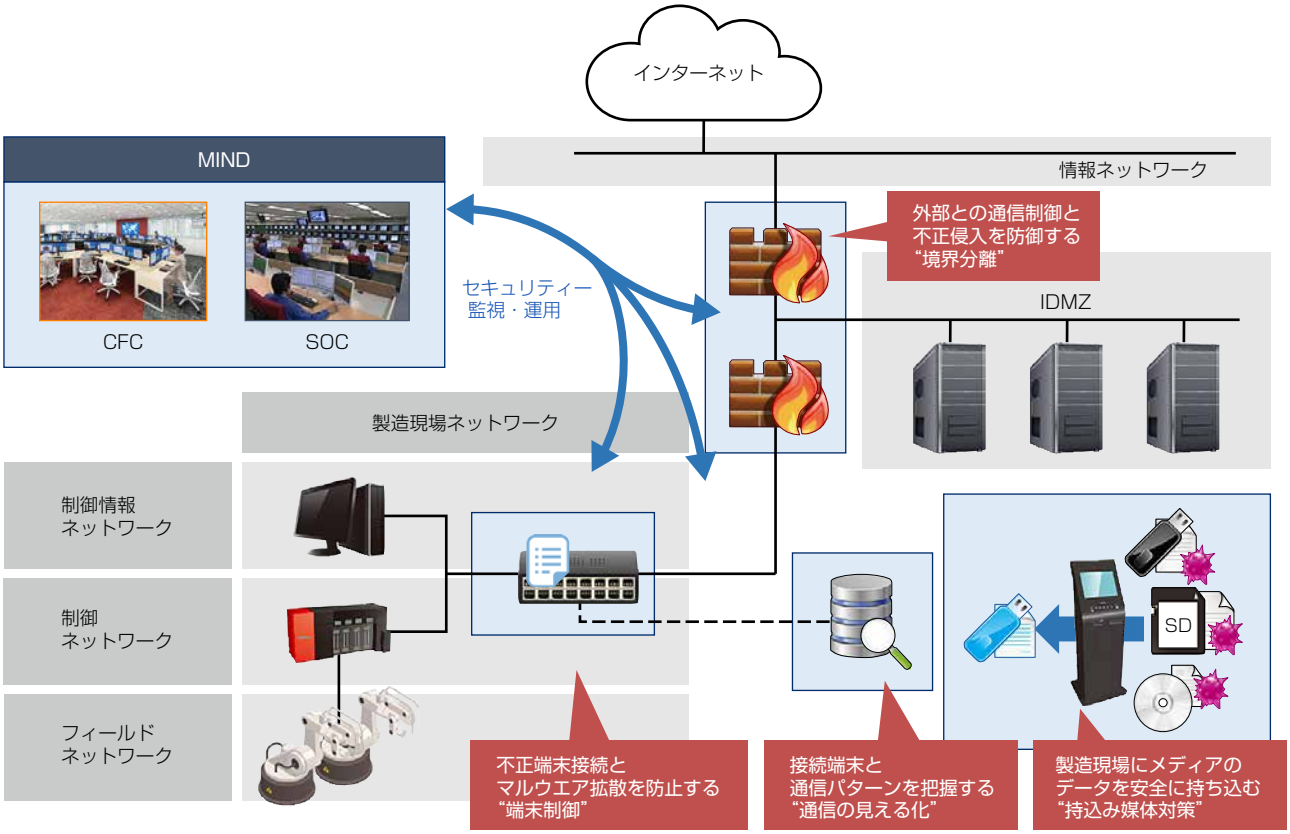
内容	対策箇所	項目数
装置の設計や設定によって緩和が可能 （例：アカウント使用ポリシー）	装置	27
何らかの施策の導入によって緩和が可能 （例：ウイルス／マルウエア対策）	装置	5
	インフラ	20
適切に運用を行うことによって緩和が可能 （例：サプライチェーン管理）	装置	4
	組織	3
	インフラ	3

分類の結果，対策箇所が装置に関するものが36項目，ネットワークなどインフラに関するものが23項目，組織に関するものが３項目になった。**３章**以降では，インフラに関する緩和策に対応したMINDのソリューションについて述べる。

（注２）　CVEは，The MITRE Corp.の登録商標である。

3. インダストリアルIoTネットワークセキュリティーサービス“CyberMinder IoT”

CyberMinder IoTのサービス構成を**図１**に示す。



CFC：サイバーフュージョンセンター，SOC：セキュリティーオペレーションセンター，IDMZ：Industrial DeMilitarized Zone

図１－CyberMinder IoTサービス構成

MITRE ATT＆CK for ICSで示された攻撃と緩和策に対して，CyberMinder IoTは“境界分離”“通信の見える化”“端末制御”“持込み媒体対策”の四つのソリューションで顧客の製造現場でのセキュリティー対策に貢献している。各ソリューションでは，それらを実現するためのセキュリティー対策製品の設計・構築・導入，及び導入後の運用サービスを

提供しており，セキュリティーインシデントを検知した場合には，SOCから顧客へ通報する。また，これまで顧客の対応領域としていたインシデントに対する調査や復旧などのCSIRT(Computer Security Incident Response Team)領域をサイバーフュージョンセンターで支援している。

3.1　外部との通信制御と不正侵入を防止する“境界分離”

日常的にインターネットと通信を行う端末(情報系端末)は，インターネット上の悪意のあるウェブサイトを経由しマルウエアなどに感染するリスクが少なからず存在する。一方，製造装置は一般的にライフサイクルが長く，脆弱性を含むサポートが終了した古いOSを利用しているケースや，製造装置メーカーがサポートしないといった理由から，アンチウイルスのような端末(エンドポイント)上でセキュリティー対策を行うEPP(Endpoint Protection Platform)製品の導入など，情報系端末では一般的なセキュリティー対策が実施できないケースが多い。そのため，情報系端末と製造装置が同一ネットワーク上に混在している場合には，情報系端末を経由して製造装置が攻撃を受ける可能性がある。

このような課題に対して“境界分離”ソリューションでは，顧客のネットワークをインターネットなど外部と通信を行う情報系ネットワークと生産に関わる製造現場ネットワークに論理的に分離し，ファイアウォールで情報系端末からの通信を必要最低限に制御することで製造現場ネットワークを保護する。

また，ファイアウォールの代わりにUTM(Unified Threat Management：統合脅威管理)を導入し，IDS(Intrusion Detection System：侵入検知システム)／IPS(Intrusion Prevention System：侵入防御システム)機能やアンチウイルス機能を有効にすることでDPI(Deep Packet Inspection)によるシグネチャベースの脅威検査を実施し，EPP製品が導入できない装置に対して仮想セキュリティーパッチを適用して不正侵入を防止する。

3.2　接続端末と通信パターンを把握する“通信の見える化”

情報系ネットワークの端末は情報システム部門で管理されているが，製造現場ネットワークは管轄外であることが多く，サポートが終了した古いOSを利用した端末が未対策のまま放置されているなど，端末(資産)が管理できていない状況にあるケースが多い。

このような課題に対して“通信の見える化”ソリューションでは，製造現場のネットワークで収集したパケットを解析することによって，ネットワークに接続されている端末を一覧化し，顧客の資産を“見える化”する。“見える化”した端末のOSの種類やバージョンの情報，それらに含まれる脆弱性を一覧化することで顧客はセキュリティー対策の現状を把握し，必要な対策を講じることが可能になる。

また，DPIによるシグネチャベースの脅威検査や機械学習による通常とは異なる通信パターンの検出(振る舞い検知)を組み合わせることで異常な通信を“見える化”し，マルウエアの拡散や攻撃者の活動を検出する。

3.3　不正端末接続とマルウエア拡散を防止する“端末制御”

通信の見える化では製造現場ネットワーク内の不正端末の接続やマルウエアの感染拡大を検知するが，検知した端末をネットワークから切り離したり通信を遮断したりする機能はない。“端末制御”ソリューションでは端末認証機能やホワイトリストによる通信制御によって，不正端末の接続やマルウエア感染の拡散を防止する。

端末認証はスイッチに接続された端末のMACアドレス(Media Access Control Address)をチェックし，事前登録した正規のMACアドレスか検査する。登録されていないMACアドレスの端末が接続された場合は，スイッチの該当ポートをシャットダウンして，不正端末の接続とマルウエアの拡散を防止する。

また，ホワイトリストスイッチでは，製造現場ネットワークに流れる正しい通信パターンをホワイトリストとして学習し，登録したホワイトリスト以外の通信パターンが発生した場合に当該パケットを遮断して，不正な通信を制限する。なお，提供するホワイトリストスイッチは，通過する通信を基に自動的にホワイトリストを生成できるので，導入環境の通信パターンを把握できていない場合でも導入が容易である。

3.4　製造現場にメディアのデータを安全に持ち込む“持込み媒体対策”

製造現場では，製造装置の保守メンテナンスの際に利用されるUSBメモリーなどの可搬媒体によって，製造装置が直接マルウエアなどに感染するリスクが存在する。“持込み媒体対策”ソリューションでは可搬媒体をウイルスチェックすることで製造現場へのマルウエアの侵入を防止する。

“持込み媒体対策”ソリューションで実施するウイルスチェックでは，世界各地のメーカーが提供するアンチウイルスエンジンを最大30種類搭載でき，持ち込むデータを複数のウイルスエンジンで一度にスキャンする。また，データ無害化機能も搭載しておりMicrosoft(注3) WordやExcel(注3)，PDF(Portable Document Format)などに埋め込まれたマクロを自動的に削除することも可能である。

また，可搬媒体のウイルスチェックは専用のキオスク端末で実施し，検査結果はログとして保管でき，レシートに印字して出力することも可能である。製造現場への入構の手続きと併せて実施することで，いつ・だれが・どのようなファイルを持ち込んだか追跡できる。

（注３） Microsoft，Excelは，Microsoft Corp.の登録商標である。

4. CyberMinder IoTのMITRE ATT＆CK for ICSへの対応状況と展望

３章で述べたCyberMinder IoTのソリューションは，**２章**で分析したMITRE ATT＆CK for ICSのインフラで対応すべき23項目のうち20項目の緩和策に対応している(**表２**)。残る３項目の緩和策は，特定の攻撃手法を防止するActive Directory(注4)の設定(緩和策ID：M0915)や，セキュリティー対策を考慮したネットワーク設計(緩和策ID：M0810，M0812)であるが，これらについてもMINDのネットワーク構築サービスなど他のサービスを利用することでインフラで対応すべき23項目全ての緩和策に対応可能である。

表２-緩和策への対応一覧(対応済み緩和策だけ抜粋)

ID	緩和策名	境界分離	通信の見える化	端末防御	持込み媒体対策
M0801	Access Management	○	-	-	-
M0915	Active Directory Configuration	-	-	-	-
M0949	Antivirus/Antimalware	○	○	○	○
M0800	Authorization Enforcement	○	-	-	-
M0803	Data Loss Prevention	○	○	-	-
M0942	Disable or Remove Feature or Program	-	-	-	○
M0950	Exploit Protection	○	○	○	○
M0937	Filter Network Traffic	○	○	○	-
M0804	Human User Authentication	○	-	-	-
M0935	Limit Access to Resource Over Network	○	-	-	-
M0934	Limit Hardware Installation	-	○	-	-
M0806	Minimize Wireless Signal Propagation	-	○	-	-
M0932	Multi-factor Authentication	○	-	-	-
M0807	Network Allowlists	○	○	○	-
M0931	Network Intrusion Prevention	○	-	-	-
M0930	Network Segmentation	○	-	-	-
M0810	Out-of-Band Communications Channel	-	-	-	-
M0920	SSL/TLS Inspection	○	○	○	-
M0812	Safety Instrumented Systems	-	-	-	-
M0814	Static Network Configuration	○	○	○	-
M0919	Threat Intelligence Program	○	○	○	-
M0951	Update Software	-	○	-	-
M0916	Vulnerability Scanning	-	○	-	-

SSL：Secure Socket Layer，TLS：Transport Layer Security

なお，CyberMinder IoTでは，**表１**で示したインフラ以外の装置，組織としての対策箇所についても顧客の対応を支援するため，アセスメントやコンサルティングのサービスとして提供する計画である。また，システムの正規な機能を悪用した攻撃など，緩和策では対応できない攻撃戦術を受けても，それを検知する仕組みや被害を最小限にするための方策について研究を継続する。

（注４） Active Directoryは，Microsoft Corp.の登録商標である。

5. む　す　び

今後工場DXはより一層進んで，様々な製造装置がネットワークに接続されることが想定される。サイバー攻撃を受ければより広範囲の生産に大きな影響を及ぼす可能性があり，セキュリティー対策の重要性は増大している。一方でセキュリティーを取り巻く環境は日々変化している。インダストリアルIoTネットワークセキュリティーサービス“CyberMinder IoT”では，最新の技術動向を踏まえて，顧客のニーズや顧客が直面する脅威に合わせて更なるソリューションの拡充を進めていく。

参 考 文 献

(1) The MITRE Corp.：MITRE ATT＆CK ICS Matrix
https://attack.mitre.org/matrices/ics/