特集論文

国際標準規格IEC 62443の分析に基づくインダストリアルIoTネットワークセキュリティサービス“CyberMinder IoT”

川邉喜彦*
伊藤　隆**
山中忠和**

Industrial IoT Network Security Service "CyberMinder IoT" Based on Analysis of International Standards IEC 62443

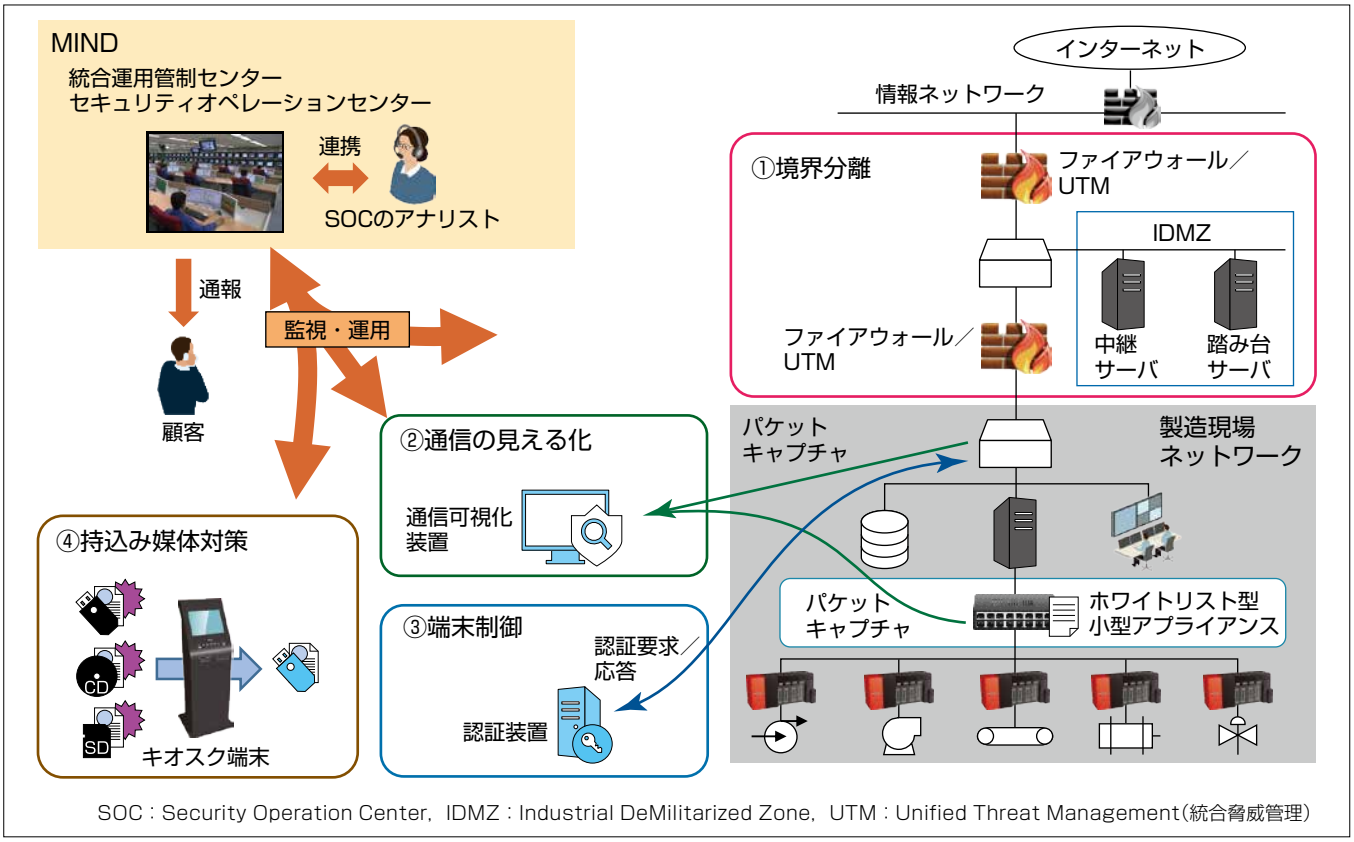
Yoshihiko Kawabe, Takashi Ito, Tadakazu Yamanaka

要　旨

IoT(Internet of Things)やデータ分析技術の進歩によって，インダストリー4.0やスマート工場などに代表される情報通信技術をモノづくりの現場でも活用する動きが進んでいる。それによって製造現場のネットワークはインターネットなどの外部ネットワークと接続され，サイバー攻撃の標的となるリスクが増加している。

これらの脅威に対抗するために，三菱電機インフォメーションネットワーク㈱(MIND)では，三菱電機の情報技術総合研究所と連携して国際電気標準会議(International Electrotechnical Commission：IEC)の定める制御システムセキュリティの標準規格IEC 62443の分析と実際の現場で想定される脅威の分析に基づいて，次の四つの製造現場向けサイバーセキュリティ対策ソリューションからなるインダストリアルIoTネットワークセキュリティサービス“CyberMinder IoT”の提供を開始した。

(1) 製造現場ネットワークと外部ネットワークの境界で通信制御と不正侵入を防止する“境界分離”
(2) 製造現場ネットワークに接続されている端末と流れる通信パターンを可視化する“通信の見える化”
(3) 製造現場ネットワークへの不正端末の接続防止と，侵入したマルウェアがネットワーク内の他の装置へ拡散することを防止する“端末制御”
(4) 保守作業などで持ち込むUSB(Universal Serial Bus)メモリなどの可搬媒体のウイルスチェックを実施する“持込み媒体対策”



SOC：Security Operation Center，IDMZ：Industrial DeMilitarized Zone，UTM：Unified Threat Management(統合脅威管理)

インダストリアルIoTネットワークセキュリティサービス“CyberMinder IoT”のサービス構成

インダストリアルIoTネットワークセキュリティサービスは，①境界分離，②通信の見える化，③端末制御，④持込み媒体対策の四つのソリューションで構成され，各ソリューションで導入するセキュリティ製品の設計・構築・導入及び導入後の監視・運用までをMINDがワンストップで提供する。

*三菱電機インフォメーションネットワーク㈱
**三菱電機㈱ 情報技術総合研究所

1. まえがき

近年，技術の革新によって安価で高性能なコンピュータが普及したことによって，これまでアナログで動作していた様々な装置がデジタル化されネットワークに接続されている。製造現場でもこれまでの手作業からロボットなどの機械利用が進み，それらをネットワークでつないだ製造工程のオートメーション化が進んでいる。さらに，昨今のAI(Artificial Intelligence)技術の進化によって，オートメーション化された装置からネットワーク経由で生産情報などが収集され，故障の予兆検知や作業工数の削減など生産性向上に利用されている。

これまでの製造現場ネットワークは各製造装置メーカーの独自プロトコルによって構成されており，外部からネットワークを経由した侵入が容易ではなかったが，Windows(注1)やEthernet(注2)に代表される汎用OSやプロトコルの利用が進んだ結果，情報系ネットワークとの境界が曖昧になり，インターネットなどの外部ネットワークから侵入されるリスクが増加している。

一方，製造装置や付随するセンサ類は，その装置が稼働するために必要なコンピュータリソースしか実装しておらず，一般的なコンピュータでは今では当たり前となったアンチウイルスソフトウェアなどのセキュリティ対策製品の導入が難しい現状にある。加えて製造装置のライフサイクルは一般的なコンピュータなどの３～５年に比べて10年以上と長く，搭載OSのサポート切れによって，脆弱(ぜいじゃく)性が発見されてもセキュリティパッチの適用など十分なサポートが受けられないという課題がある。

MINDではそのような製造装置自身のセキュリティの課題の解決策として，製造装置が接続されるネットワーク側でセキュリティ対策を実装することが有効であると考えており，インダストリアルIoTネットワークセキュリティサービス“CyberMinder IoT”を開発した。

本稿では，サービス開発に際して行った国際標準規格IEC 62443の分析と脅威の分析，及びそれに基づいて開発したCyberMinder IoTについて述べる。

(注１)　Windowsは，Microsoft Corp.の登録商標である。
(注２)　Ethernetは，富士ゼロックス㈱の登録商標である。

2. 国際標準規格IEC 62443の分析

2.1　IEC 62443の全体構成

IEC 62443は汎用制御システムを対象としたセキュリティ規格であり，**表１**の規格群で構成される。IEC 62443-2シリーズは主に事業者向け，IEC 62443-3シリーズはインテグレータ向け，IEC 62443-4シリーズは装置ベンダー向けのセキュリティ要件などを規定している。MINDはシステムに対してサービス提供を行うインテグレータであるため，主としてIEC 62443-3シリーズを参照する必要があり，この中でも制御システムが持つべき要件を“システムセキュリティ要件”として整理したIEC 62443-3-3に着目する。

2.2　IEC 62443-3-3のシステムセキュリティ要件

IEC 62443-3-3はシステムセキュリティ要件を七つの“基礎的要求事項(Foundational Requirement：FR)”に分類して規定している(**表２**)。各要件にはセキュリティレベル(１～４)が設定されており，システム全体に求められるセキュリティレベルに応じて，満たすべき要件を抽出して活用できる仕組みとなっている。

表２．IEC 62443-3-3のシステムセキュリティ要件

基礎的要求事項	要件数
FR1 識別及び認証管理	24
FR2 使用制御	24
FR3 システム完全性	19
FR4 データ機密性	6
FR5 制限されたデータフロー	11
FR6 イベントへの適時対応	3
FR7 資源の可用性	13

表１．IEC 62443の全体構成

区分	IEC	名称	版(発行年月)
一般	62443-1-1	Terminology, concepts and models	1.0(2009-07)
	62443-1-2	Master glossary of terms and abbreviations	策定中
	62443-1-3	System security compliance metrics	策定中
	62443-1-4	IACS security life-cycle and use-cases	策定中
ポリシー及び手順	62443-2-1	Establishing IACS security program	1.0(2010-11)
	62443-2-2	IACS protection levels	策定中
	62443-2-3	Patch management in the IACS environment	1.0(2015-06)
	62443-2-4	Security program requirements for IACS service providers	1.1(2017-08)
システム	62443-3-1	Security technologies for IACS	1.0(2009-07)
	62443-3-2	Security risk assessment and system design	策定中
	62443-3-3	System security requirements and security levels	1.0(2013-08)
コンポーネント	62443-4-1	Secure product development lifecycle requirements	1.0(2018-01)
	62443-4-2	Technical security requirements for IACS components	1.0(2019-02)

IACS：Industrial Automation and Control System

3. 脅威の分析

MINDでは製造現場向けのネットワークセキュリティサービスを検討するに際し，実際に発生した事案から製造現場で現実に起こりうる脅威を分析した。

3.1 外部ネットワークからの侵入

製造現場では既に情報通信技術(Information and Communication Technology：ICT)の活用が進んでおり，製造現場ネットワークと情報系ネットワークを接続しているケースが多く，インターネットから情報系ネットワークを経由してマルウェアが侵入するリスクがある。

3.2 持込み媒体からの感染

製造装置メーカーの作業員が保守作業のために外部からデータを持ち込む，又は作業ログなどのデータを持ち出すケースがあり，その際に利用するUSBメモリなどの可搬媒体がマルウェアの感染経路となるリスクがある。

3.3 保守用回線からの侵入

製造装置メーカーごとにユーザーが管理していない保守用のリモート回線を敷設し，メーカーの保守拠点などからリモートアクセスをするケースがあり，異なるセキュリティレベルのネットワークからマルウェアなどが侵入するリスクがある。

3.4 不正端末接続からの侵入

保守・運用作業の一環として汎用OSが搭載された端末を製造現場ネットワークに接続するケースがあり，そこからマルウェアなどが侵入するリスクがある。また，保守用に用意されたスイッチの空きポートに無許可の端末が接続できるケースもあり，そこから悪意のある攻撃者がネットワークへ侵入するリスクがある。

3.5 感染端末の拡散

ネットワークがフラット(単一セグメント)で構成されているケースが多く，万が一マルウェアなどが侵入した場合にほかの装置や製造ラインへ感染拡大するリスクがある。

4. CyberMinder IoT

先に述べたIEC 62443と脅威の分析に基づいて開発したインダストリアルIoTネットワークセキュリティサービスCyberMinder IoTでは，次の四つのソリューションで対策を実現している(**図1**)。また，各ソリューションでセキュリティインシデントを検知した場合には，MINDの統合運用管制センターから顧客へ通報する。

4.1 境界分離

情報系ネットワークと製造現場ネットワークの境界にファイアウォールを導入して許可された通信だけを透過する。さらに，中継サーバや踏み台サーバを配置したIDMZを設け，双方のネットワーク間での直接通信を避ける構成とすることで多層防御を実現し，外部ネットワークからの侵入リスクを低減する。また，ファイアウォールの代わりにUTMを導入し，侵入検知システム(Intrusion Detection System：IDS)／侵入防御システム(Intrusion Prevention System：IPS)やアンチウイルス機能で，DPI(Deep Packet Inspection)によるシグネチャベースの脅威検査を実施し，マルウェアなどの侵入を防止する。

また，IDMZに装置メーカーごとの保守用回線を集約し，保守用リモートアクセスをファイアウォールで制御することで，外部ネットワークからの不正アクセスやマルウェアなどの侵入を防止する。

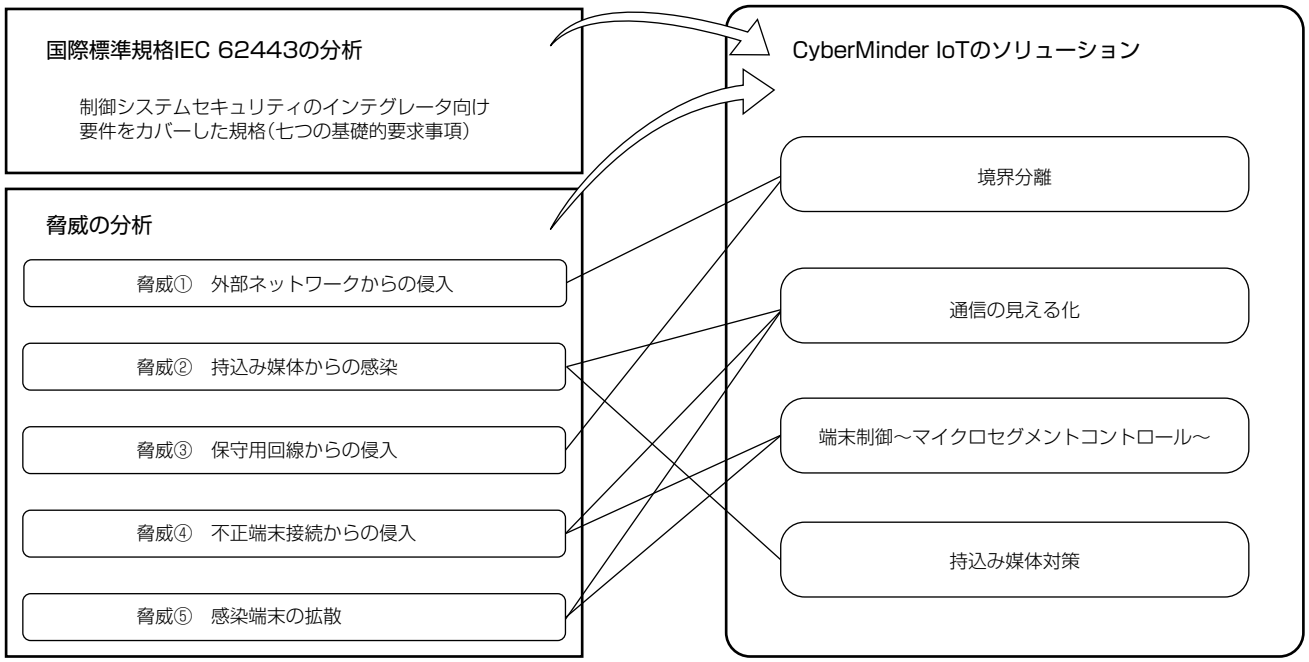


図1．サービス開発のアプローチ及び脅威とソリューションの対応

4.2 通信の見える化

製造現場ネットワーク内のスイッチからパケットをミラーリングして通信可視化装置へ取り込み，リアルタイムにネットワークの構造と流れるトラフィック及び端末の情報を収集し，端末に内在する既知の脆弱性情報をリスト化する。さらに，収集したパケットをDPIによるシグネチャベースの脅威検査と，機械学習による通常とは異なる通信パターンの抽出によってゼロデイ攻撃や標的型攻撃を検出し，ネットワーク内の不正端末の接続や感染端末の拡散に対して早期検出することで影響を局所化する。

4.3 端末制御

スイッチに接続された端末のMAC(Media Access Control)アドレスを認証装置へ照会し，認証装置に事前登録した正規のMACアドレスであるか検査する。登録されていないMACアドレスを持った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アラートを発報する。

また，今後は感染端末の拡散を防止する対策として，末端のネットワークハブをホワイトリスト型小型アプライアンスに置き換え，端末ごとの通信制御を実現する。ホワイトリスト型小型アプライアンスは通過する通信を自動的にホワイトリストとして学習し，学習した通信パターン以外の通信が発生した場合に当該パケットを遮断することで，万が一不正な端末やマルウェアに感染した端末がネットワークに接続された場合でも，他の装置への攻撃やマルウェア自体の拡散を防止する。

4.4 持込み媒体対策

外部から持ち込むUSBメモリなど可搬媒体をウイルスチェックするキオスク端末を提供する。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種類搭載することが可能で，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してマルウェアの持込みを防止する。

また，データ無害化機能も搭載しておりMicrosoft WordやExcel(注3)，Adobe PDF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になっている。

(注3) Excelは，Microsoft Corp.の登録商標である。

5. むすび

今後，製造現場のネットワークはより一層のIoT化が進み，標準Ethernetの拡張であるTSN(Time-Sensitive Networking)や第五世代移動通信システム(Fifth Generation： 5G)，自営LTE(Long Term Evolution)などの新しい技術によって様々な装置がネットワークに接続される“つながる工場”へと進化すると想定されるが，それによって小さなセキュリティインシデントであっても広範囲に拡散していくことで生産に大きな影響を及ぼす可能性があり，セキュリティ対策の重要性は増大している。

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，サービスの更なる拡充を進めていく。

参考文献

(1) IEC：System security requirements and security levels，IEC 62443-3-3 (2018)