MITSUBISHI ELECTRIC
Changes for the Better
Automating the World

CRA対応に向けた
弊社機器製品のご提案

三菱電機株式会社

2025年12月

アジェンダ

1 セキュリティに関する概況

2 IEC 62443

3 欧州サイバーレジリエンス法(CRA)

4 OTセキュリティのご提案

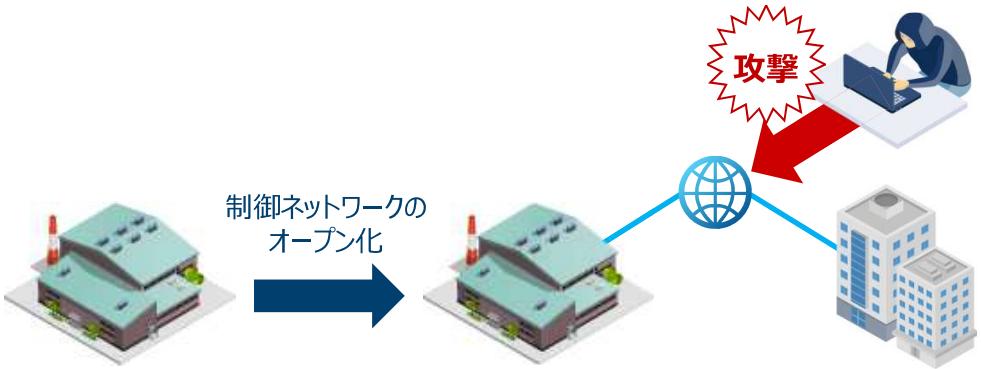
MITSUBISHI ELECTRIC
Changes for the Better
Automating the World

1-1 概況

制御システムに対するサイバー攻撃の脅威が増加

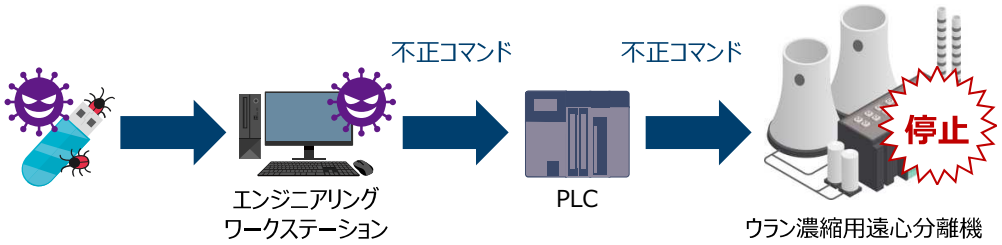
制御システムの変化

制御システムにおけるIoTの導入、制御ネットワークのオープン化により、工場やプラントがサイバー攻撃の対象として狙われやすくなりました。



制御システムが攻撃された事例

2010年にイラン核燃料施設のシステムがウィルス感染し、ウラン濃縮用遠心分離機8,400台が稼働不能になりました。
ウィルス(Stuxnet)がPLCに不正なコマンドを送信し、遠心分離機がダウンしました。

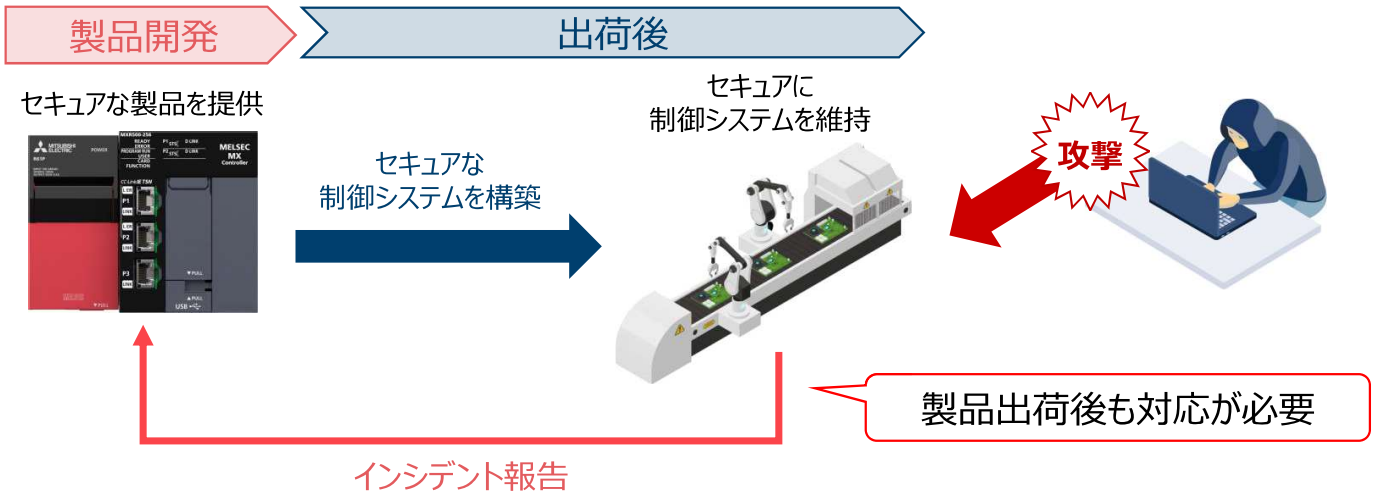


▼出典元

1-1 概況

制御機器や制御システムのライフサイクル全体でセキュリティ対策が必要

サイバーセキュリティ攻撃は日々進化しています。
そのため、セキュアな製品を開発するだけでなく、出荷後も攻撃に対する対策を実施する必要があります。



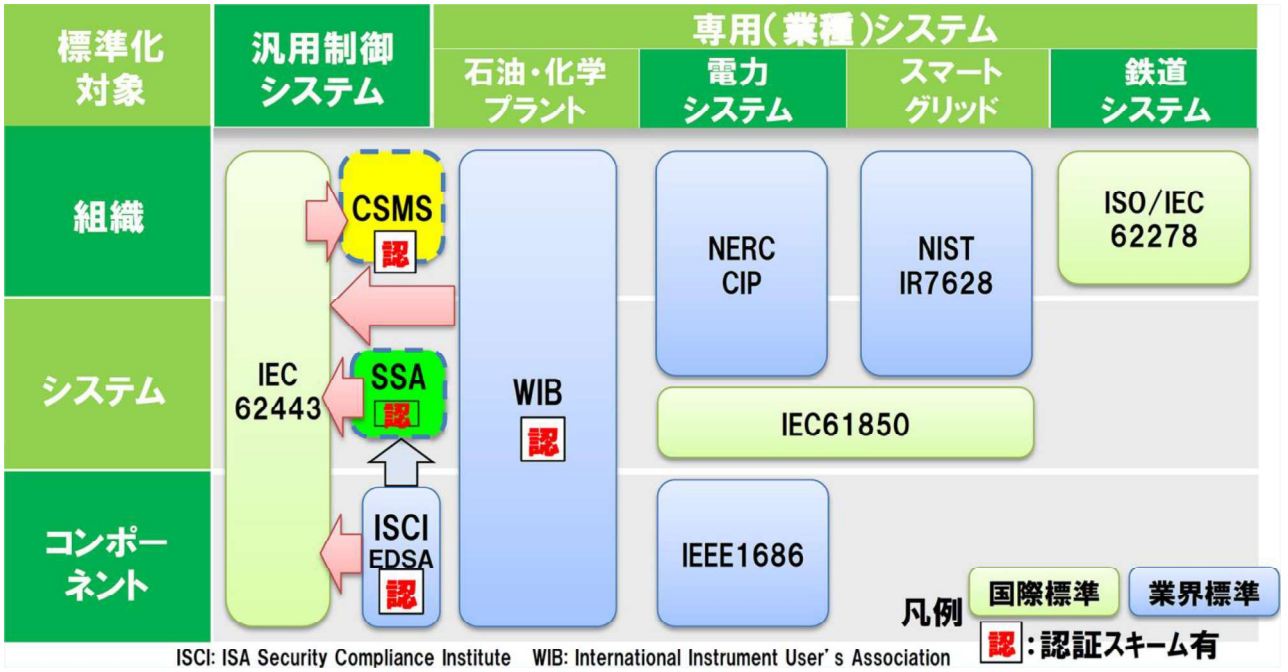
MITSUBISHI ELECTRIC Changes for the Better | Automating the World

1-2 セキュリティに関する規格

各業種に適したセキュリティ規格が存在

ライフサイクル全体で、組織・システム・コンポーネントを対象に標準化したセキュリティ規格が存在します。
弊社では、汎用制御システムの規格であるIEC 62443*に対して取り組んでいます。

＊：産業用オートメーション・制御システム(IACS)のサイバーセキュリティに関する国際規格



▼出典元

1 セキュリティに関する概況

2 IEC 62443

3 欧州サイバーレジリエンス法(CRA)

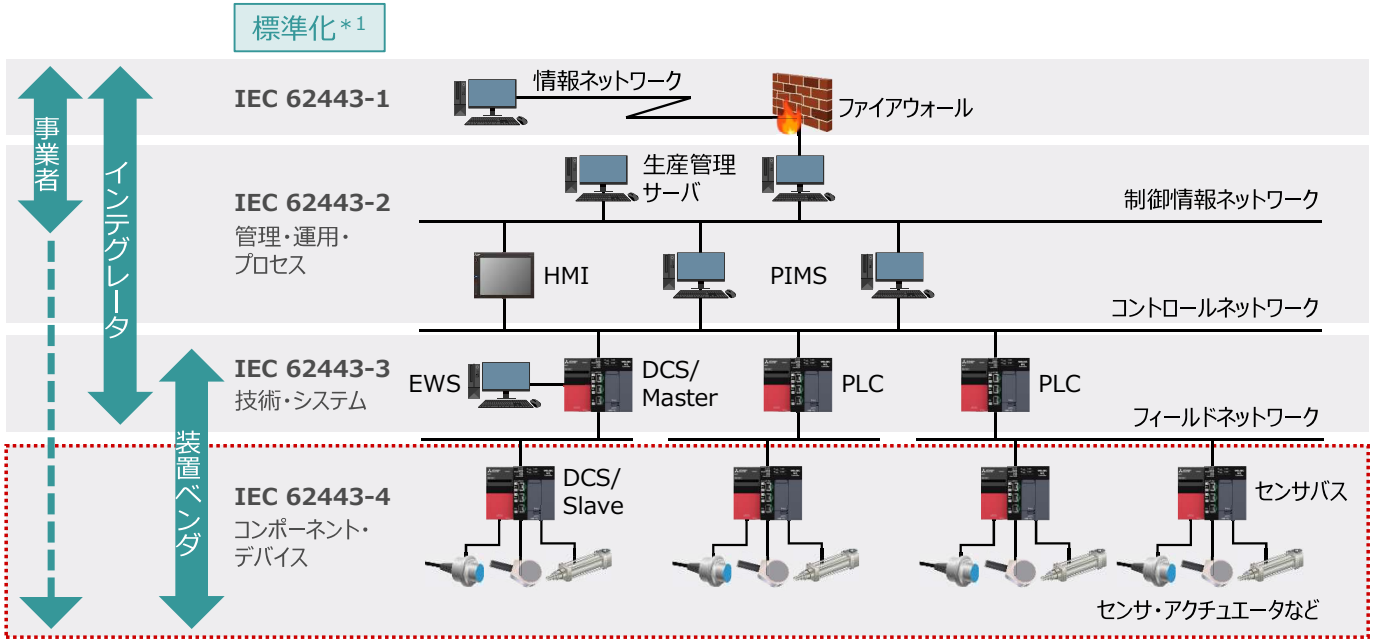
4 OTセキュリティのご提案

MITSUBISHI ELECTRIC Changes for the Better | Automating the World

2-1 IEC 62443の全体像

弊社の関連規格はIEC 62443-4

弊社が関連している規格はIEC 62443-4です。
IEC 62443シリーズのうち、主に産業機器のセキュリティ要件を定めた規格です。



<評価事業>

- **CSMS認証*2（予定）**
- **EDSA認証*3**
- **Wurldtech Ach*4**

*1：IEC 62443-1のCyber securityの標準化作業は、IEC/TC65/WG10が担当(日本国内事務局はJEMIMAが対応)

*2：Cyber Security Management System：ISMSを制御システム関連組織向けに特化した要求事項を規定(認証スキーム開始予定)

*3：EDSA：Embedded Device Security Assurance：制御機器(コンポーネント)の認証プログラム →IEC 62443-4に提案されている

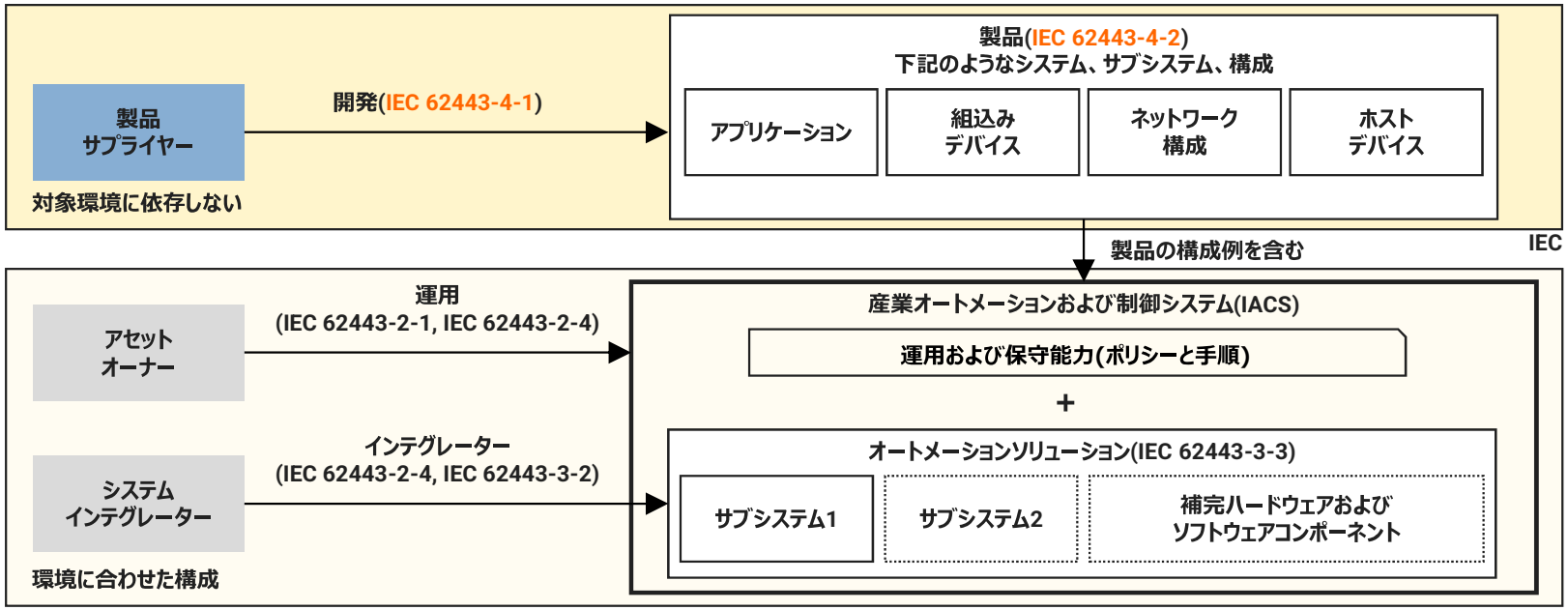
*4：ネットワーク接続装置(コントローラなど)の認証(ペネトレーション、ファジングテスト)調達要件に指定されている(EDSA要件としても引用)

▼出典元

2-2 IEC 62443-4シリーズの概要

IEC 62443-4-1とIEC 62443-4-2の関係性

製品の開発プロセス(IEC 62443-4-1)とセキュリティ機能(IEC 62443-4-2)の要件を定めています。
IEC 62443-4における役割として、製品サプライヤーは製品のセキュア開発とサポートを担うことなります。
アセットオーナーやシステムインテグレーターは弊社のような製品サプライヤーとは異なり、IEC62443-2やIEC62443-3といった規格の要件に準じた対応が必要です。



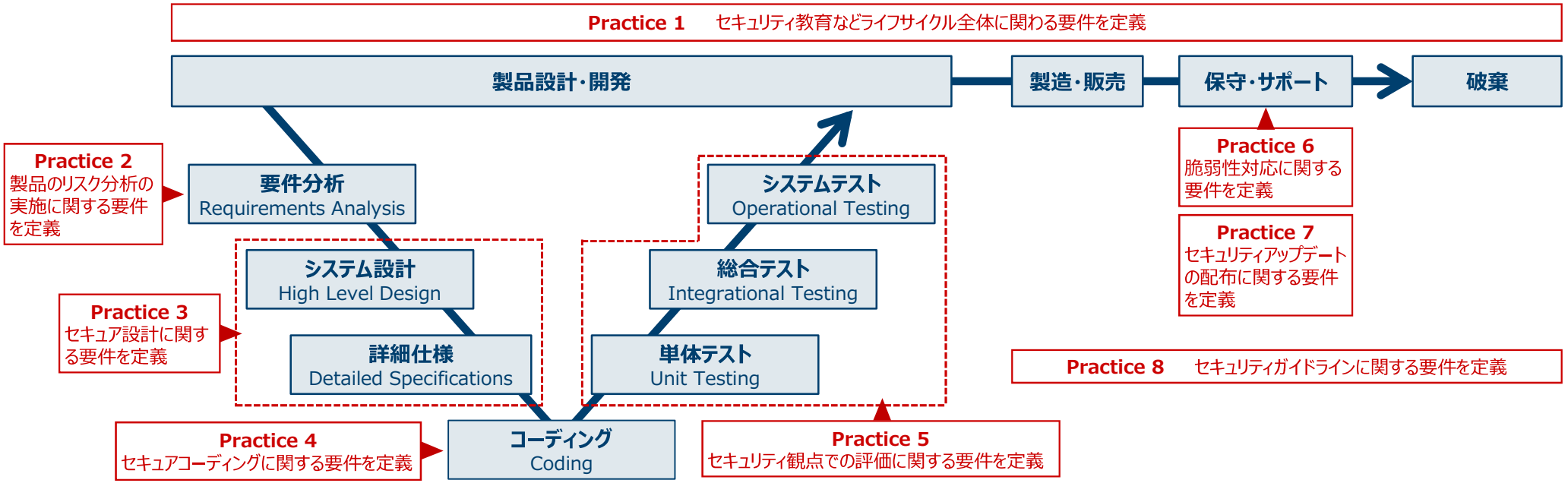
IEC 62443-4-2に準拠した製品は、IEC 62443-3-3で求められるセキュリティ機能の多くを製品レベルで備えています。
そのため、適切にシステム設計・設定・運用を行うことで、IEC 62443-3-3準拠のシステムを簡単に構築できます。

▼出典元

2-3 IEC 62443-4-1の概要

開発のV字プロセスに対応した定義

各開発プロセスに関連するIEC 62443-4-1には8つの実践分野(Practice)があります。
IEC 62443-4-1を適用するためには、各プロセスでPracticeを満たす必要があります。



MITSUBISHI ELECTRIC Changes for the Better | Automating the World

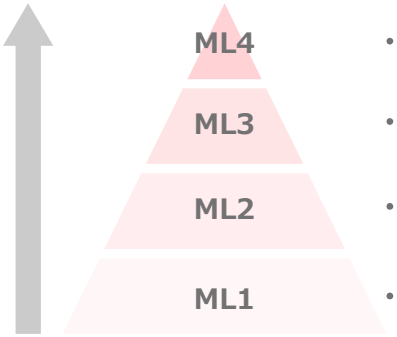
2-4 IEC 62443-4-1の弊社取組み

弊社はIEC 62443-4-1の認証取得済み (‘21/5)

弊社(名古屋製作所/メカトロニクス製作所)の認証情報は、弊社FAサイトに掲載しています。

現在、弊社はMaturity Level 3(ML3)を取得しています。
このML3は、成熟度モデルとして定義されており、IEC 62443-4-1の開発プロセスに従って開発していることが認証されました。

Maturity Level(成熟度レベル)概要



弊社はIEC62443-4-1で規定された開発プロセスを実践しています。
これを基に製造業者が要求されるCRAの開発プロセスに対応する予定です。

▼出典元


Certificate

Cyber Security Management

CS Management (TÜV Rheinland)
IEC 62443-4-1:2018 (Edition 1.0) - Product Supplier
CSM 111, Maturity Level 3: Defined - Practiced

Certificate No.	968/CSM 111.03/24
Certified Company & Location	Mitsubishi Electric Corporation 1-14 Yada-Minami 5-chome Higashi-ku Nagoya 461-8670 Japan
Scope of Certification	Product Supplier, related to IEC 62443-4-1:2018 (Edition 1.0) Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements The company has successfully demonstrated during an audit process that a Security Development Lifecycle Management System is established and practiced in accordance with the applicable requirements of the standard, according Maturity Level 3: Defined - Practiced The local scope of certification is limited to the departments located in 1-14 Yada-Minami 5-chome, Higashi-ku, Nagoya 461-8670, Japan: Nagoya Works Industrial Mechatronics Systems Works Purpose of the audit is to obtain evidence of compliance with the organizational requirements related to the Management of Cyber Security according to the Scope of Certification, covering the lifecycle of security related components and systems. This CSM Certification refers to the listed company location and their involved departments, which comply with the organizational CSM requirements for the listed Scope of Certification. This certificate does not imply approval or certification for specific security related developments of products.
Validity	This certificate is valid until 2027-05-04

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Cologne, 2024-05-15
Dipl.-Ing. (FH) Sergei Biberdorf

TÜV Rheinland Industrie Service GmbH
Automation and Functional Safety
Am Grauen Stein
51105 Cologne - Germany

Certification Body Safety & Security for Automation & Grid
Further information referring to the scope of certification, see https://www.tuvasi.com. The issue of this certificate is based upon an evaluation in accordance with the Certification Program CERT SDLA V2.0 2020:2020 in its actual version, whose results are documented in Report No. 968/CSM 111.03/24 dated 2024-05-15. Issued by the certification body accredited by DAkkS according to DIN EN ISO/IEC 17065. The accreditation is only valid for the scope listed in the annex to the accreditation certificate D-ZE-11052-02-00.

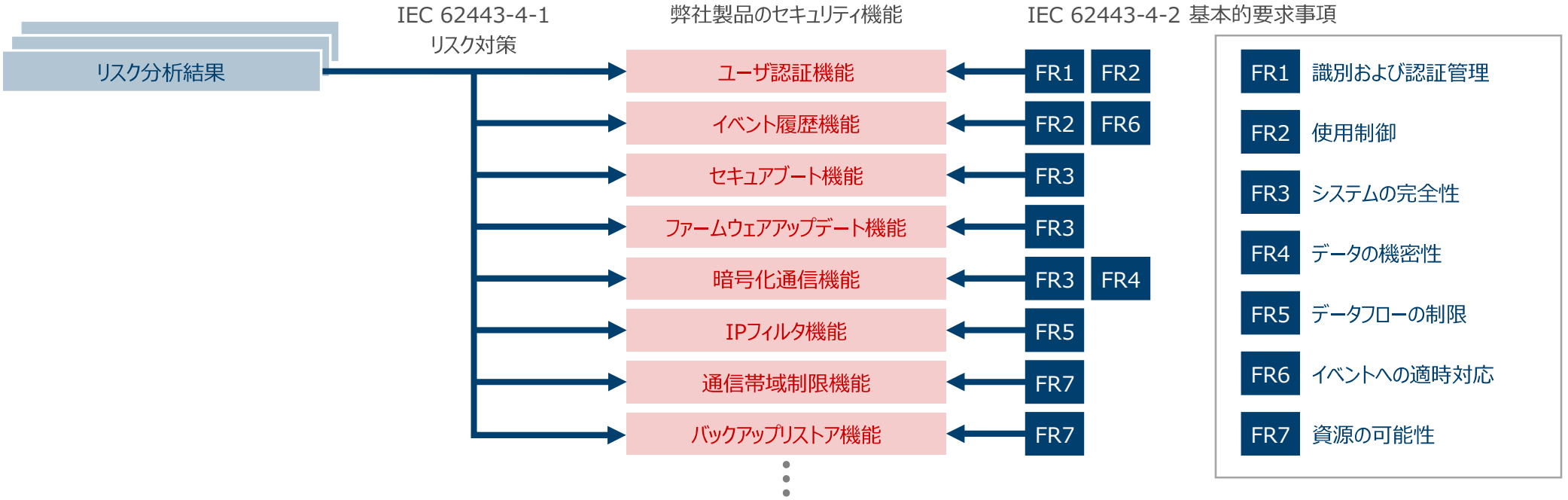
www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

2-5 IEC 62443-4-2の概要

製品に必要なセキュリティ機能を定義

IEC 62443-4-1の開発プロセスに沿って、IEC 62443-4-2に対応したセキュリティ機能を開発する必要があります。
IEC 62443-4-2は、7つの基本的要求事項(Functional Requirement)を定義しています。
実装するセキュリティ機能は、要求事項を満たす必要があります。



MITSUBISHI ELECTRIC Changes for the Better | Automating the World

2-6 IEC 62443-4-2の製品での取組み

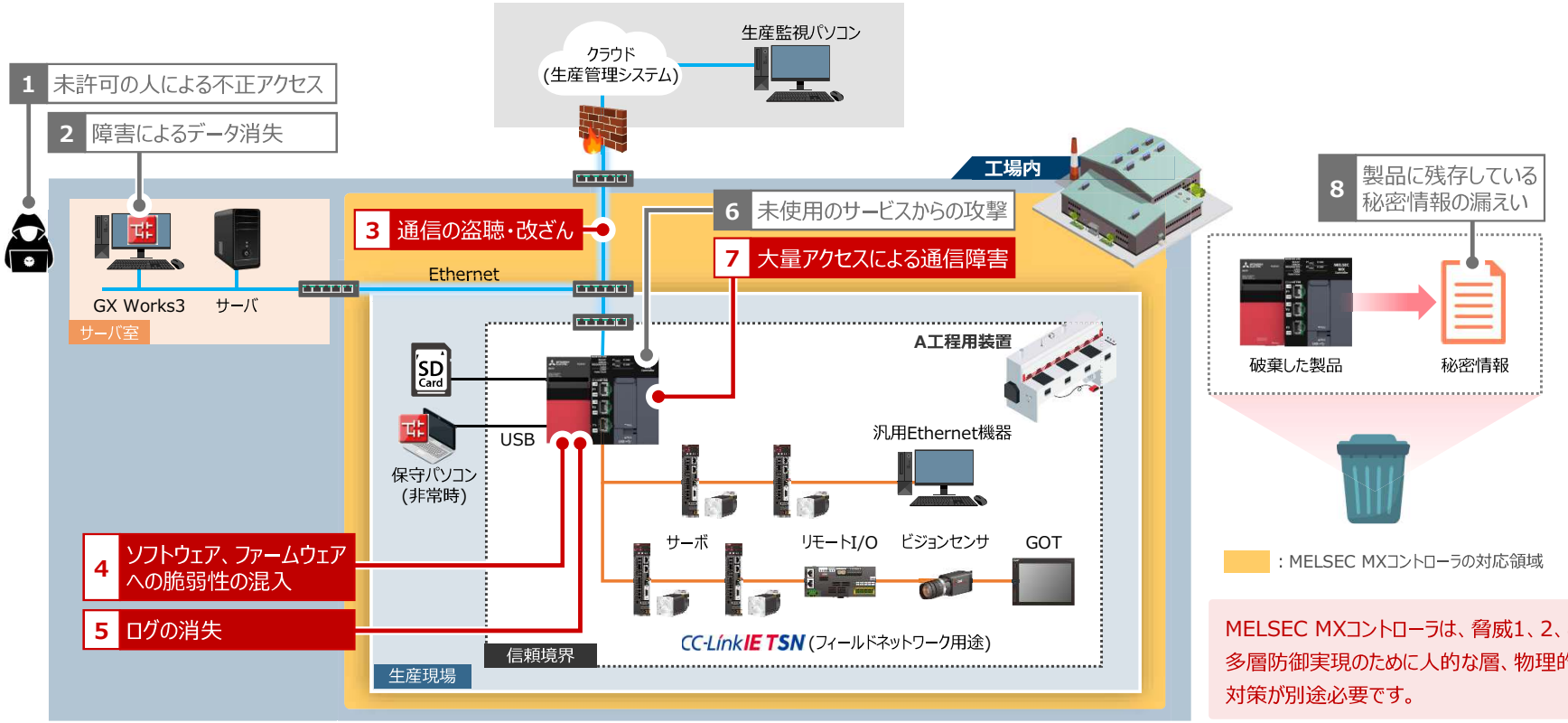
弊社のセキュリティ機能

MELSEC MXコントローラは国内PLCメーカで先行してIEC62443-4-2に適合しています。
具体的には、下記の代表的なセキュリティ機能を搭載しており、IEC62443-4-2の要件を満たしています。

セキュリティ機能名	機能説明	関連する脅威	IEC 62443-4-2要件との対応概要
ユーザ認証	ユーザごとに設定された操作権限を基に、デバイス/ラベル、ファイルへのアクセスを制御する。	未許可の人・機器による不正アクセス	識別および認証管理 使用制御
イベント履歴	コントローラ内で発生したイベントをログ保存する。	ログの消失	使用制御 イベントへの適時対応
セキュアブート	コントローラが起動する際に、信頼できるファームウェアかを確認(公開鍵暗号方式による署名検証)する。	ソフトウェア、ファームウェアへの脆弱性の混入	システム完全性
ファイル改ざんチェック	コントローラが起動する際に、お客様が作成したプログラム、設定したパラメータが改ざんされていないかを確認(共通鍵暗号方式による検証)する。		
ファームウェアアップデート	最新かつ正規のファームウェアに更新する。		
暗号化通信	外部機器との通信を暗号化することで第三者による盗聴を防止する。 暗号証明書を有する機器との通信のみ行う。	通信の盗聴および改ざん	データの機密性
IPフィルタ	許可したIPアドレスの機器とのみ通信を許可する。 または、禁止したIPアドレスの機器との通信を禁止することも可能である。	大量アクセスによる通信障害	制限されたデータフロー
通信帯域制限	指定のポートをクローズできる。 また、設定帯域を超えた送受信が発生した場合、通信元または通信先のパケットを遮断する。		資源の可用性
バックアップ/リストア	コントローラ内のユーザプログラム/パラメータ/デバイス/ラベルをバックアップ(保存)する。 バックアップファイルを任意のタイミングでコントローラにリストア(書戻し)可能である。	障害によるデータ消失	

2-7 弊社製品に対する脅威

弊社MELSEC MXコントローラの利用環境における脅威は下記です。(リスクアセスメントや公知の攻撃事例の知見を基にした場合)



MELSEC MXコントローラは、脅威1、2、8に対する機能も有していますが、多層防御実現のために人的な層、物理的な層、ネットワーク層のセキュリティ対策が別途必要です。

次ページからMXコントローラ単体機能で脅威3、4、5、7に対応するための機能をご紹介します。

2-7-1 ソフトウェア、ファームウェアへの脆弱性の混入

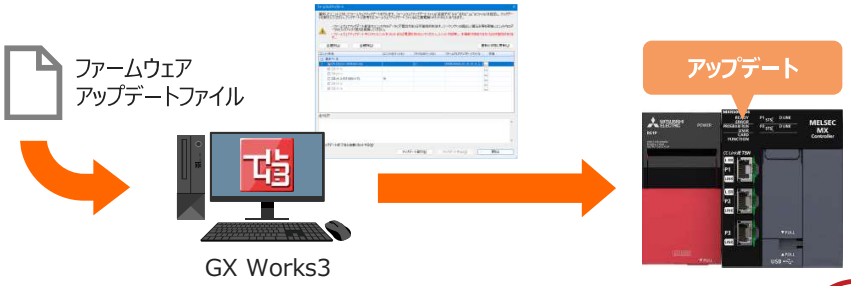
MELSEC MXコントローラは、ソフトウェアとファームウェアの脆弱性を狙う脅威に対処するセキュリティ機能に対応しています。

脅威

日々進化するサイバー攻撃の脅威に
対応できるか心配だ・・・

ファームウェアアップデート機能で対応できます！

ファームウェアアップデートを行うことで、最新のパッチをMXコントローラに反映してセキュリティを強固にできます。



CRA 附属書I-2「脆弱性処理要件」(2)(7) 対応

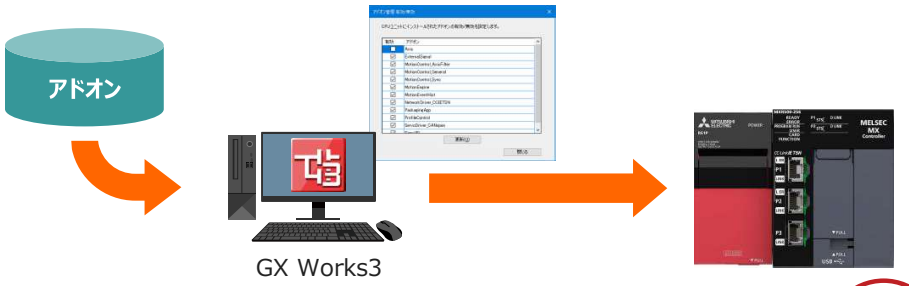
＊ 規約の対応を保証するものではありません。

脅威

不正ソフトウェアが混入したときに
コントローラが意図しない動作をしないか心配だ…

アドオン機能で対応できます！

MXコントローラに機能を追加・拡張するためのプログラム(アドオン)をインストールできます。インストールしたアドオンの有効/無効を設定できるため、認知しているアドオンのみを実行できます。また、セーフモードにも対応しています。



CRA 附属書I-1「セキュリティ特性要件」(3)(d) 対応

＊ 規約の対応を保証するものではありません。

2-7-2 ログの消失

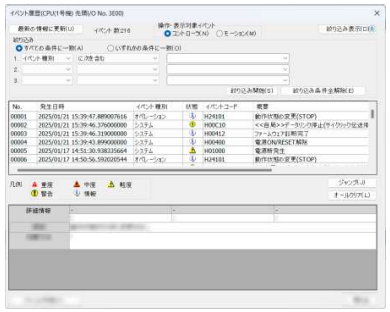
MELSEC MXコントローラは、設備/装置で発生した不具合の原因究明や不正アクセス/操作を検出するセキュリティ機能に対応しています。

脅威

不正アクセスでログを操作されないか心配だ・・・

イベント履歴機能とユーザ認証機能で対応できます！

イベント履歴機能　：イベント履歴として保存された操作やエラーなどの情報を、発生履歴を時系列で確認できます。
ユーザ認証機能　　：MXコントローラへのアクセスを制限し、不正アクセスを防止できます。
また、両機能を組み合わせてイベント履歴の操作を管理者権限とすることができます。



CRA 附属書I-1「セキュリティ特性要件」(3)(b、j)　対応

＊ 規約の対応を保証するものではありません。

MITSUBISHI ELECTRIC Changes for the Better | Automating the World

2-7-3 通信の盗聴および改ざん

MELSEC MXコントローラは、ネットワークを流れる通信データに対して第三者からの不正アクセスによる盗聴や改ざんなどを防止するセキュリティ機能に対応しています。

脅威

通信データの盗聴や改ざんが心配だ・・・

暗号化通信機能で対応できます！

信頼境界をまたがる相手機器との通信時、通信データを暗号化できます。暗号化通信を行うには、電子証明書による公開鍵の受渡しが必要です。

1. プロトコルをTLS/DTLSに設定
2. コントローラの証明書作成
3. コントローラの証明書読み出し
4. 相手機器への証明書登録

CRA 附属書I-1「セキュリティ特性要件」(3)(c) 対応

＊ 規約の対応を保証するものではありません。

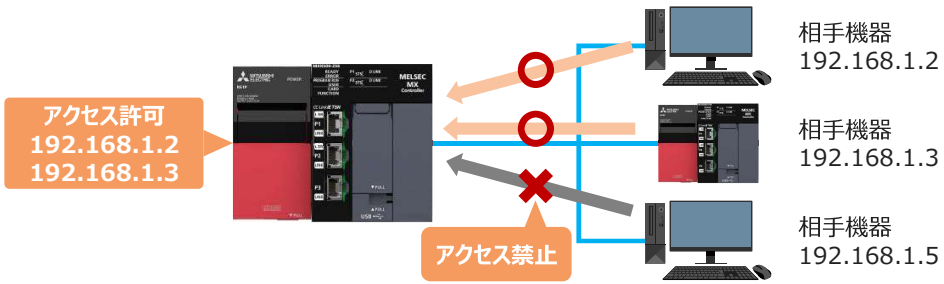
2-7-4 大量アクセスによる通信障害

MELSEC MXコントローラは、ネットワーク内通信トラフィックの増大による通信障害を回避するセキュリティ機能に対応しています。

脅威 アクセスが集中してデータ通信が正常に行われるか心配だ・・・

IPフィルタ機能で対応できます！

アクセス元のIPアドレスを識別して、特定のIPアドレスによるアクセスを防止します。



脅威 ネットワークの通信帯域が不正アクセスによるパケットで埋め尽くされないか心配だ・・・

DoS攻撃に対する帯域制限機能で対応できます！

外部機器からの不正アクセス(プログラムやデータの破壊など)を防止します。
他の対策と組み合わせることで、セキュリティはさらに強固になります。

CRA 附属書I-1「セキュリティ特性要件」(3)(f、g) 対応

＊ 規約の対応を保証するものではありません。

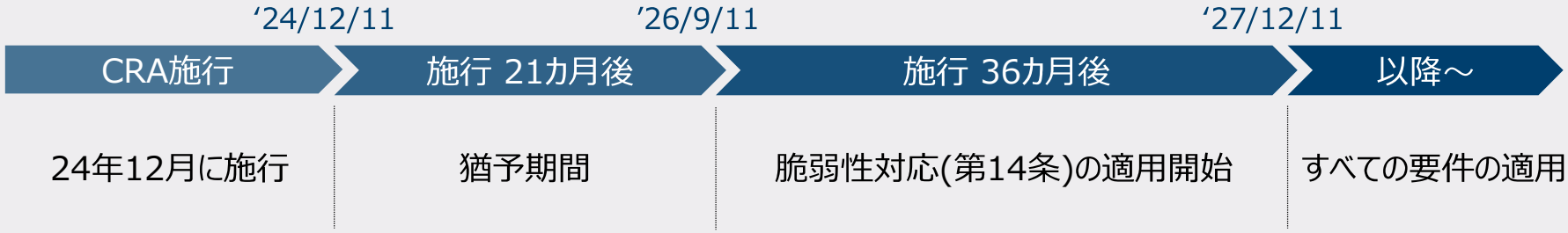
3-1 欧州サイバーレジリエンス法(CRA)について

2027年12月までに全条項対応

すべての装置メーカーがデジタル製品にセキュリティ対策が必要

2024年12月にEUサイバーレジリエンス法(CRA)が施行され、欧州に上市するデジタル製品のセキュリティ対応が義務付けられました。
2026年9月には脆弱性対応の報告義務があり、2027年12月にはすべての条項(開発やセキュリティ機能など)を実装する必要があります。
CEマーキング制度の一部として運用されるため、従来の安全基準に加えてサイバーセキュリティ基準を満たす必要があります。

CRAの今後のスケジュール



CRA適用後、**違反した場合は、罰金**が科せられます。
罰金は、最大1,500万ユーロまたは全世界売上高の2.5%のいずれか高い方が適用されます。

3-2 CRAの要件概要

セキュリティ特性要件と脆弱性処理要件の対応が求められる

デジタル製品(デジタル要素を備えた製品)に対する製造者の義務として、欧州CRA第13条の下記を満たす必要があります。

- 附属書Iの１「セキュリティ特性要件」を満たし、適切に設置・維持され、目的どおりに使用されていること
- 附属書Iの２「脆弱性処理要件」を満たすこと

セキュリティ特性要件

リスクアセスメントを実施してサイバーセキュリティ要件を遵守するための要件です。

脆弱性処理要件

SBOM(ソフトウェア部品表)の作成、無料更新プログラムの提供など脆弱性処理に関する要件です。

弊社は、IEC 62443のセキュリティ要求事項やプロセスの活用により、各FA製品のCRA法への対応を進めております。

全てのデジタル製品に求められるセキュリティ特性要件（附属書I）

附属書Iの１「セキュリティ特性要件」

（１）リスクに基づいて適切なサイバーセキュリティを確保するよう設計・開発・生産されていること。
（２）悪用可能な脆弱性が含まれないこと。
（３）リスクベースアセスメントに基づいて、以下を満たすこと。
(a) 製品を元の状態にリセット可能である等、安全な構成となっていること。
(b) 適切な制御メカニズムにより不正アクセスからの保護が確保されていること。
(c) 最先端の暗号化などにより個人データ・その他のデータの機密性を保護すること。
(d) データやプログラムなどの完全性を許可されていない操作から保護し、破損についても報告すること。
(e) 必要なデータに限定して処理を行うこと。（データの最小化）
(f) DoS攻撃からの回復・緩和などの重要な可用性の機能を保護すること。
(g) 他の機器やネットワークからのサービスの可用性について自身への悪影響を最小化すること。
(h) 外部インターフェース等の攻撃対象領域を制限して設計・開発・製造されていること。
(i) インシデントの影響を軽減するように設計・開発・製造されているころ。
(j) アクセス、データ修正、サービス、機能などの内部活動を記録・監視し、セキュリティ情報を提供すること。
(k) 自動更新やユーザーへのアップデート通知などによりセキュリティアップデートによる脆弱性対応を確実に行えること。

附属書Iの２「脆弱性処理要件」　・・・製造業者が満たすべき要件

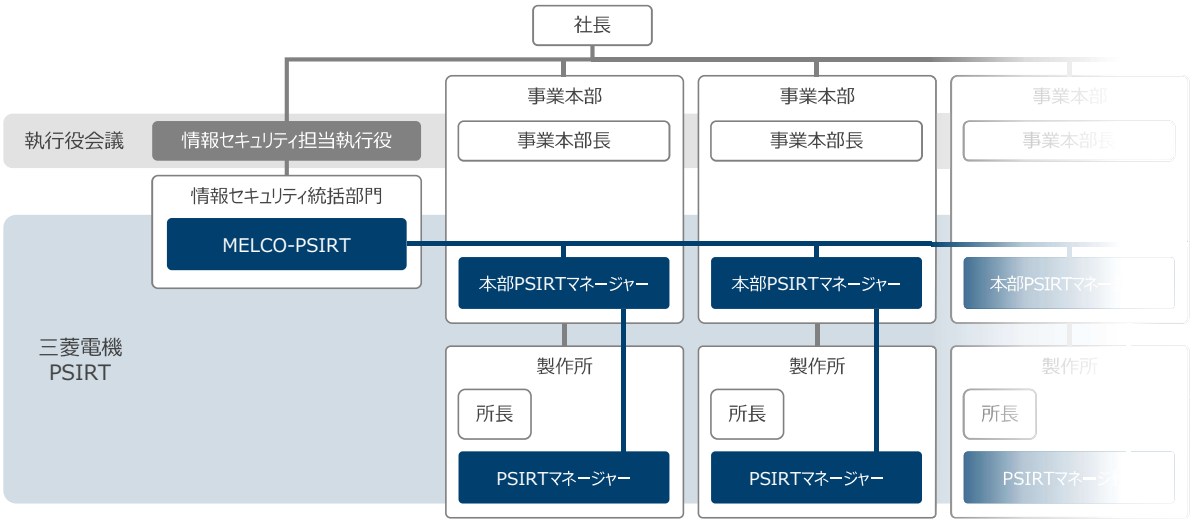
（１）製品に含まれる脆弱性とコンポーネントを特定し、文書化すること。そのために、機械読み取り可能な形式で一般的に使用されるSBOM作成（少なくとも最上位レベルの依存関係含む）を行うこと。
（２）セキュリティアップデートの提供など、遅滞なく脆弱性に対処・緩和すること。
（３）効果的かつ定期的なテストとレビューを行うこと。
（４）脆弱性情報の公開及び修正を行うこと。
（５）脆弱性開示ポリシーを導入し、実施すること。
（６）製品やサードパーティコンポーネントの潜在的な脆弱性に関する情報共有を行い、連絡先を提供すること。
（７）悪用可能な脆弱性が適時に修正・緩和されるように安全にアップデートを配布するメカニズムを提供すること。
（８）セキュリティパッチや更新プログラムが遅滞なく無料で配布され、ユーザーへの助言メッセージも添付すること。

▼出典元

3-3 CRAの弊社取り組み

IEC 62443の対応をベースにCRA準拠

弊社は脆弱性情報をPSIRT体制を構築し、全社で製品・サービスのセキュリティ品質に取り組んでいます。
CRAでは製造者による迅速な脆弱性報告義務が要件として要求されているため、本体制で迅速に対応します。



▼出典元

上図のように、弊社は実施済みのIEC 62443-4-1対応をベースに、CRAにも対応する方針です。

3-4 弊社機器のCRA対応(現時点の構想案)

機種	シリーズ	CRA適合方針(*)
コントローラ	MELSEC MXコントローラ(MX-Rモデル)	○
コントローラ	MELSEC MXコントローラ(MX-Fモデル)	○
コントローラ	MELSEC iQ-Rシリーズ	○
コントローラ	MELSEC iQ-Fシリーズ	○

＊ 27/10月までに適合(予定)

本資料に掲載のない機種は"対象外"または"対応検討中"となります。

3-4 弊社機器のCRA対応(現時点の構想案)

機種	シリーズ	CRA適合方針(*)
モーションユニット	MELSEC iQ-R/iQ-Fシリーズ	○
サーボアンプ	MR-J5シリーズ	○
サーボアンプ	MR-J4シリーズ	○
サーボモータ	HG/HKシリーズ	○

＊ 27/10月までに適合(予定)

本資料に掲載のない機種は"対象外"または"対応検討中"となります。

MITSUBISHI ELECTRIC Changes for the Better | Automating the World

3-4 弊社機器のCRA対応(現時点の構想案)

機種	シリーズ	CRA適合方針(*)
表示器	GOT3000シリーズ	○
表示器	GOT2000シリーズ	○

＊ 27/10月までに適合(予定)

本資料に掲載のない機種は"対象外"または"対応検討中"となります。

MITSUBISHI ELECTRIC Changes for the Better | Automating the World

3-4 弊社機器のCRA対応(現時点の構想案)

機種	シリーズ	CRA適合方針(*)
インバータ	FREQROL-A800シリーズ	○
インバータ	FREQROL-E800シリーズ	○
インバータ	FREQROL-F800シリーズ	○
インバータ	FREQROL-D800シリーズ	○

＊ 27/10月までに適合(予定)

本資料に掲載のない機種は"対象外"または"対応検討中"となります。

MITSUBISHI ELECTRIC Changes for the Better | Automating the World

3-4 弊社機器のCRA対応(現時点の構想案)

機種	シリーズ	CRA適合方針(*)
ロボット	MELFA FRシリーズ(Dタイプ)	○
ロボット	MELFA FRシリーズ(Rタイプ)	○
ロボット	MELFA CRシリーズ(Dタイプ)	○
テンションコントローラ	全シリーズ(ケーブル/メモリカセットは対象外)	○

＊ 27/10月までに適合(予定)

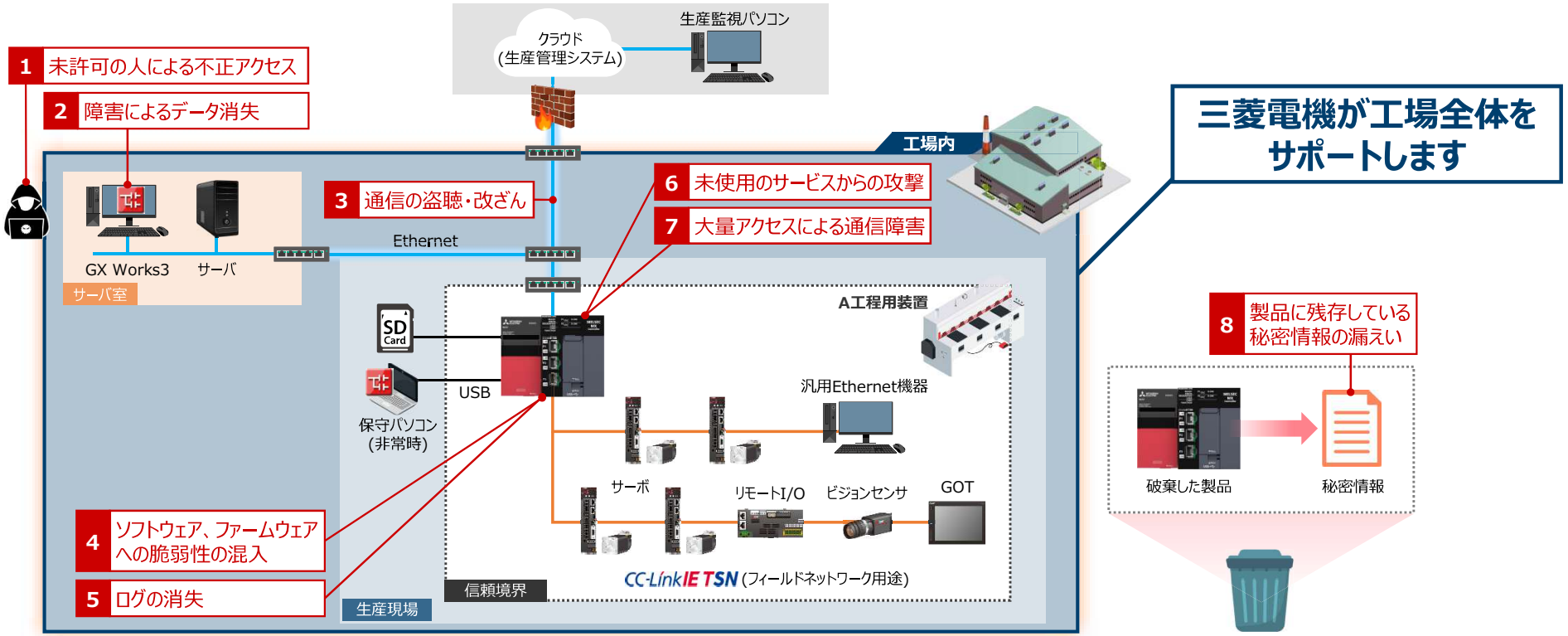
本資料に掲載のない機種は"対象外"または"対応検討中"となります。

MITSUBISHI ELECTRIC Changes for the Better | Automating the World

4-1 三菱電機のOTセキュリティ

弊社製品は幅広いサイバーセキュリティに対応

コンサルティングが必要なお客様に、三菱電機がOTセキュリティソリューションを提案いたします。



4 OTセキュリティのご提案

三菱電機のOTセキュリティソリューションは、OTセキュリティ対策に必要な「課題抽出・対策立案」→「対策導入」→「運用」のサイクルをワンストップで提供いたします。総合電機メーカならではの豊富なノウハウを活用し、サービスをご提供します。

製造現場のセキュリティ対策は三菱電機が解決します。

OTセキュリティ対策をワンストップでご提供

お客様のセキュリティレベルに応じた課題抽出をはじめ、OTの特性を考慮した対策導入、24時間365日の監視体制によるシステム管理・運用までワンストップでご提供します。

OTとIT両分野での豊富な経験を活かしたセキュリティ対策

製造業をはじめとした制御機器/システム事業で長年培ったOTの知見と、金融業界をはじめとする各分野向けで培ってきたITセキュリティ技術を融合し、製造現場ならではの可能性と安全性を重視したセキュリティ対策をご提案します。

ソリューション	
課題抽出・対策立案	■ アセスメント・脆弱性診断 ■ コンサルティング
対策導入	■ IT/OT分離 ■ マイクロセグメント化 ■ エンドポイント防御(脆弱性対策、マルウェア対策) ■ ネットワークエンドポイント防御
運用	■ セキュアリモートアクセス ■ ネットワーク異常検知・ 制御ネットワーク可視化 ■ セキュリティ対策機器運用・監視 ■ SOC(Security Operation Center) ■ 運用支援(FSIRT)

STEP 1
現状調査・課題抽出

当社のエンジニアが、セキュリティ検査ツールを活用し、お客様のシステムを詳細に診断・調査いたします。
その過程で、潜在的な脆弱性などの課題を抽出します。

STEP 2
提案・導入～セキュリティ対策と可視化～

お客様のセキュリティに対する課題に対して最適な対策をご提案いたします。さらにSCADAと連携してサイバー攻撃を可視化できます。

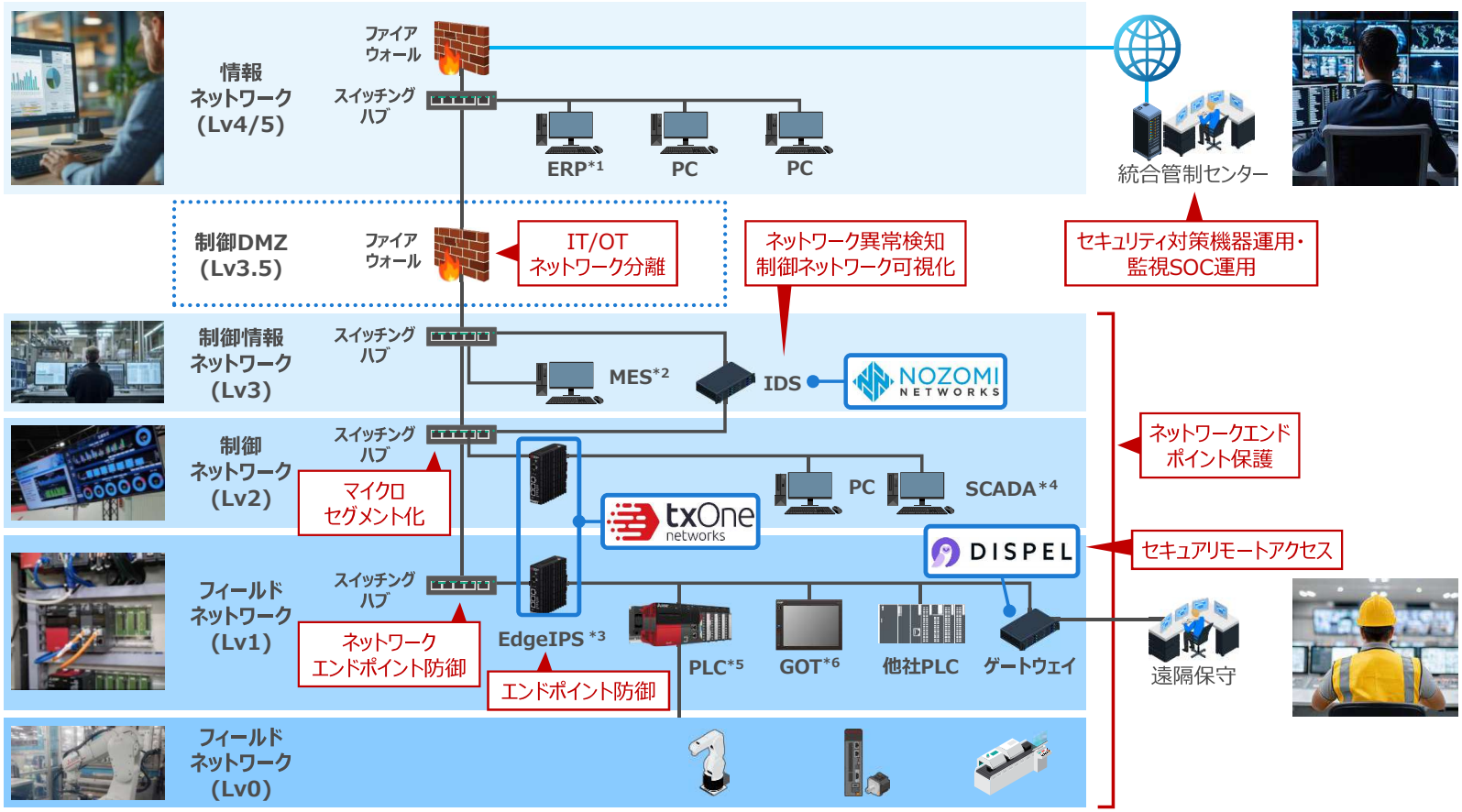
STEP 3
保守・運用

システムの定期的な点検や診断を通じて、最新のセキュリティ対策を行います。また、発見した潜在的リスクは必要に応じてシステムのアップデートや設定の最適化を実施いたします。

4 OTセキュリティのご提案

MITSUBISHI ELECTRIC Changes for the Better | Automating the World

OTセキュリティに関する課題をお客様ごとに調査し、最適なOTセキュリティ機器の選定から導入、サイバー攻撃の可視化、導入後の保守運用まで、安定稼働に向けたサポートを提供いたします。製造DXを実現するOTネットワーク構築やプログラムバックアップシステムもお任せください。



*1：ERP (Enterprise Resources Planning)
会社全体の資源を管理するための統合型システム

*2：MES (Manufacturing Execution System)
製造プロセスの状態把握や管理、作業者への指示や支援を行う情報システム

*3：IPS (Intrusion Detection System)
不正アクセスやサイバー攻撃を自動的に検知・遮断するセキュリティシステム

*4：SCADA (Supervisory Control And Data Acquisition)
工場内の情報を監視・集約し、設備を管理するシステム

*5：PLC (Programmable Logic Controller)
外部の機器を自動的にコントロールできる制御装置

*6：GOT (Graphic Operation Terminal)
モニタ画面上でハードウェア的な表示・操作を行うことができるタッチパネル付の表示器

4 OTセキュリティのご提案

三菱電機のOTセキュリティソリューションは、業界で強いパートナーと協業し、高いレベルのサービスを提供しています。
主に、可視化・異常検知ツールの「Nozomi」、脅威から機器を保護する「txOne」、セキュアなリモートアクセスの「DISPEL」があります。

ソリューション1 可視化・異常検知

NOZOMI NETWORKS

- 工場ネットワーク内の資産をリアルタイムで監視します。
- 既知の脆弱性、サポート切れのOS使用状況、安全ではない構成、脆弱なパスワード利用などを継続的に可視化します。
- 不正アクセスや異常な通信をリアルタイムで検知して通知します。

ソリューション2 脅威から保護

txOne networks

- 工場ネットワークにつながる資産とセキュリティを強化して安定運用を支援します。
- IPSで不正アクセスを防ぎ、ネットワークセグメンテーションで感染を局所的に遮断。
- 仮想パッチで古い機器を最新の脅威から保護します。

ソリューション3 リモートアクセス

DISPEL

- 工場ネットワークにつながる装置へのセキュアなリモートアクセスサービスを提供します。
- 大規模な製造現場では複数の装置メーカーから納入された装置が混在しているケースがありますが、安全かつ簡単に実現します。
- 「いつ・誰が・どこに」のアクセス制御やログ・録画によるトレーサビリティ確保の技術を保有。世界標準セキュリティ規格に準拠し、リモートアクセス環境をグローバルに提供します。

4 OTセキュリティのご提案

三菱電機はこれまでシーケンサや産業用ロボットなど、製造現場を支えるFA機器を製造してきました。また鉄道や金融のシステムも手掛け、セキュリティソリューションを提供してきました。専門企業との協業で対応力を強化し、お客様に最適なOTセキュリティソリューションを提供いたします。

OT 製造現場を熟知

三菱電機は長年にわたり国内トップシェアを誇るシーケンサなどの制御機器、駆動機器、省エネ支援機器、配電制御機器から産業メカトロニクスまで、多岐にわたるFA製品を開発、製造し、お客様のものづくり力の進化に貢献してきました。

IT 情報システムを熟知

三菱電機は信頼性や安全性が求められる、鉄道や上下水道などの公共インフラシステムや金融システムの構築を手掛け、お客様の生活に貢献してきました。また、同分野へのセキュリティ対策も手掛け、ノウハウを蓄積してきました。

攻撃 専門企業と協業

セキュリティ対策で必要となる、可視化、異常検知、遮断、リモートアクセスに関わる製品やサービスは、同分野で世界的に強いパートナー企業との協業を進め、お客様への価値提供向上に取り組んでいます。

三菱電機は、グローバルNo.1のOTセキュリティソリューションプロバイダーを目指します

4 OTセキュリティのご提案

三菱電機は、FA機器製品のセキュリティ強化にも取り組んでいます。
最新機器のIEC62443-4-2対応や、購入後に実施いただけるFWバージョンアップ機能、脆弱性の情報公開などの対策に取り組んでいます。

IEC62443-4-2への対応

IEC62443-4-2は産業用オートメーション/制御システムのセキュリティ要件を定めた規格で、MXコントローラ MX-R/Fが適合しています。
表示器 GOT3000も将来対応予定です。

MELSEC MXコントローラ

MX-Rモデル

MX-Fモデル

IEC62443-4-2適合

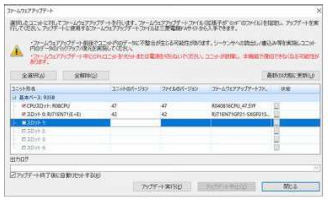
IEC62443-4-2適合（2025/11）

GOT3000

将来対応予定

FWバージョンアップ

MXコントローラ MX-R/F、MELSEC iQ-R/iQ-FのCPUユニットやインテリジェント機能ユニットは、最新のFWにバージョンアップして使用できます。
バージョンアップすることで最新機能をご使用いただけます。



GX Works3

脆弱性対策

三菱電機は製品・サービスの情報セキュリティに対して全社で取り組んでいます。お客様に提供している製品・サービスの脆弱性に関する情報を広く収集し、発見された脆弱性の対応を迅速に行います。また、脆弱性の情報・対策を広くお客様に公開しています。

三菱電機PSIRT　検索

三菱電機は既存のFA機器に対する対策も、しっかり取り組んでいます。

4 OTセキュリティのご提案

MITSUBISHI ELECTRIC Changes for the Better | Automating the World

OTセキュリティの導入を検討されている方は、ぜひ「OTセキュリティラボ横浜」をご視察ください。実際の制御機器を備えた模擬工場を構築し、DoS攻撃や異常操作などを仕掛けて異常を発生させるデモにより、攻撃、被害、回復のシナリオを体感いただけます。

横浜ダイヤビルディング

〒221-0056
神奈川県横浜市神奈川区金港町1-7

JR・東急東横線・京浜急行線・相鉄線・市営地下鉄「横浜駅」(きた東口)
徒歩3分

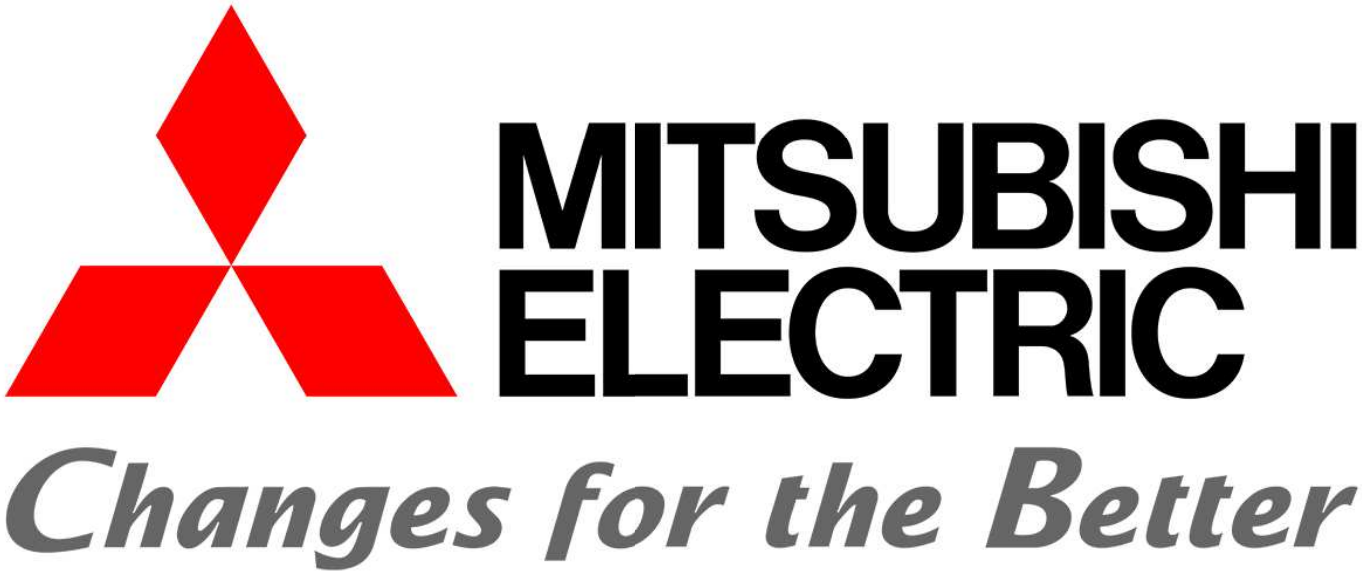
デモの流れ

1. 背景や事例紹介、模擬環境説明
2. 攻撃シナリオ説明・攻撃実演
3. 攻撃に関するディスカッション
4. 対策の提案・説明

対策

＊：USB利用あり

**OTセキュリティは部門間にまたがる課題のため、
情報システム(IT)ご担当者様と、制御システム(OT)ご担当者様が一緒に見学されることをお勧めしています。
また、新規予算獲得判断も必要となるため、決裁権をお持ちの方にも見学をお勧めしています。
ラボを通じて関係者の課題を理解し合う契機にしていただけましたら幸いです。**



弊社MELSEC MXコントローラの利用環境における脅威と、対処するためのセキュリティ機能を下記に示します。
(リスクアセスメントや公知の攻撃事例の知見を基にした場合)

No.	脅威	対処方針	MELSEC MXコントローラが対応しているセキュリティ機能	
1	未許可の人による不正アクセス	• 適切な権限設定 • 利用者の識別	ユーザ認証機能	OPC UAサーバとOPC UAクライアントの接続時に、ログイン操作によるユーザ認証を設けます。
2	障害によるデータ喪失	• 保存情報の自動バックアップ • 計画的なバックアップ • バックアップデータによるシステム復旧	コントローラのバックアップ/リストア機能	コントローラのプログラムファイルやパラメータファイル、デバイス/ラベルデータなどをバックアップします。 バックアップしたデータは、必要に応じてリストアできます。
3	通信の盗聴・改ざん	通信の認証・暗号化	暗号化通信機能	信頼境界をまたがる相手機器と通信するとき、通信データを暗号化します。
4	ソフトウェア、ファームウェアへの脆弱性の混入	• 不正ソフトウェアの実行制限 • 正規ソフトウェアの保護	ファームウェアアップデート機能	コントローラおよびMELSEC iQ-Rシリーズのユニットのファームウェアを更新します。
			アドオン機能	コントローラにアドオンソフトウェアパッケージをインストールしてコントローラの機能を拡張します。
5	ログの消失	• ログへのアクセスを制限 • ログの保存サイズ超過によるログ消失防止 • 定期的なログの確認	イベント履歴機能	各ユニットで発生したエラー、実行された操作、ネットワーク上のエラーなどのイベント情報を表示します。
6	未使用のサービスからの攻撃	通信ポートの使用有無設定	デフォルトオープンポートの使用有無設定機能	コントローラのデフォルトオープンしているポート番号のオープン/クローズを設定できます。
7	大量アクセスによる通信障害	• パケットのブロック • 帯域制限	IPフィルタ機能	アクセス元のIPアドレスを識別し、不正なIPアドレス指定によるアクセスを防止します。
			DoS攻撃に対する帯域制限機能	コントローラが使用するEthernet用ポートのネットワーク帯域を制限します。
8	製品に残存している秘密情報の情報漏えい	利用終了時に秘密情報を削除	コントローラの全情報初期化	対象ファイルの管理情報を消去し、対象デバイス/ラベルなどのデータが格納されているエリアを0で上書きします。

IEC 62443-4-2の各FR(基本的要求事項)の概要を下記に示します。
各FRには複数の要求事項があります。(7FR、全57要件)

FR1	識別および認証管理 Identification and authentication control	システムまたは資産へのアクセスを許可する前に、すべてのユーザ(人間、ソフトウェアプロセスおよびデバイス)を識別し、認証する。
FR2	使用制御 Use control	認証されたユーザ(人間、ソフトウェアプロセスまたはデバイス)に割り当てられた特権を行使して、コンポーネントに対して要求されたアクションを実行し、こららの特権の使用を監視する。
FR3	システム完全性 System integrity	不正な操作または変更から保護するために、コンポーネントの完全性を確実にする。
FR4	データの機密性 Data confidentiality	不正開示を防止するために、通信チャネル上およびリポジトリに保存されているデータ内の情報の機密性を確実にする。
FR5	制限されたデータフロー Restricted data flow	不要なデータの流れを制限するために、ゾーンおよびコンジットを介して制御システムをセグメント化する。
FR6	イベントへの適時対応 Timely response to events	インシデントが発見されたときに、関係当局への通知、必要な違反の証拠の報告および是正処置のタイムリーな実行によって、セキュリティ違反に対応する。
FR7	資源の可用性 Resource availability	必須サービスの低下または不能に対するコンポーネントの可用性を確保する。

製品が目指すセキュリティレベル(SL)によって、対象となる要件が異なります。
また、対象となる製品のシステム、サブシステム、構成*によって要件が変更される場合があります。

＊：組込みデバイス、ネットワークデバイス、ホストデバイス、アプリケーションデバイス

出典先リンク集

IPA 「制御システム関連のサイバーインシデント 事例4」	https://www.ipa.go.jp/security/controlsystem/ug65p900000197wa-att/000080701.pdf
CSSC 「IEC 62443の概要と認証について」	https://www.css-center.or.jp/ja/info/documents/2013/20131120_ET2013.pdf
CSSC 「制御システムセキュリティの脅威と対策の動向および CSSCの研究概要について」	https://www.css-center.or.jp/pdf/about_CSSC.pdf
LDRA 「Applying IEC62443-4-1 to Industrial Automation Control Systems」	https://ldra.com/wp-content/uploads/ldra/Applying_IEC_62443_4_1_Technical_Overview_v2_0.pdf
三菱電機 「製品セキュリティへの取り組み 」	https://www.mitsubishielectric.co.jp/fa/about-us/security/index.html
Maturity Level 3(ML3)の認証取得	https://fs-products.tuvasi.com/files/certificates/certificates_asi/2024/CSM/968_CSM_111_03_24/968_CSM_111_03_24_en_el.pdf
経済産業省 「EUサイバーレジリエンス法(草案概要)」	https://www.jisa.or.jp/Portals/0/resource/news/1340/901.pdf
三菱電機 「製品セキュリティー対応体制」	https://www.mitsubishielectric.co.jp/psirt/framework/index.html

2020年6月に自動車メーカ A社がランサムウェアによる攻撃を受けて国内外9工場の操業停止、復旧まで数日を要しました。
2022年4月には電気機器メーカ B社が同様の攻撃を受けました。対策が完了する1カ月半の間、暗号化された情報を復旧できませんでした。

自動車メーカ A社

ランサムウェアによる被害

A社内ネットワークでのみ動作する専用ランサムウェア攻撃を受けました。
社内ネットワークが1日稼働停止し、国内外の工場が生産停止となり、完全復旧に数日を要しました。

被害発生日	2020年6月
目的	非公表　身代金目的か
方法	ランサムウェア
対象	ネットワーク情報管理サーバ
被害内容	国内外9工場の操業停止、復旧まで数日要す
被害金額	非公表

電気機器メーカ B社

ランサムウェアによる被害

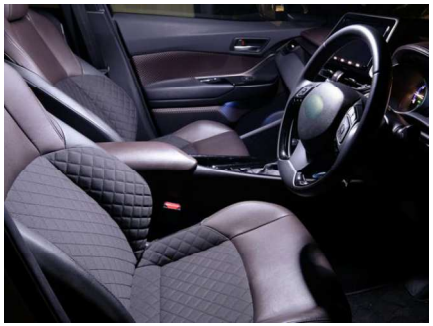
リモートアクセス機器の脆弱性へのランサムウェア攻撃を受け、製造・販売システムを停止しました。
対策の完了までに1カ月半を要し、暗号化された従業員の個人情報の復元を断念しました。

被害発生日	2022年4月
目的	非公表
方法	ランサムウェア
対象	サーバ
被害内容	製造・販売システムの停止、従業員個人情報の暗号化
被害金額	非公表

2022年3月に自動車メーカ C社がランサムウェアによる被害を受けました。自社工場停止による供給遅延で取引先完成車メーカが停止し、サプライチェーン全体が大混乱する事態となりました。2025年9月には飲料メーカ D社が同攻撃を受け、出荷を全面停止しました。

自動車部品メーカ C社

ランサムウェアによる被害



子会社が利用していたリモート接続機器の脆弱性から、C社のネットワークに侵入するサプライチェーン攻撃を受けました。C社の取引先は取引用システムが利用できず、1日の稼働停止となりました。

被害発生日	2022年3月
目的	非公表　身代金目的か
方法	ランサムウェア
対象	サーバやパソコン
被害内容	自社工場停止、さらに取引先完成車メーカの複数工場が稼働停止
被害金額	非公表

飲料メーカ D社

ランサムウェアによる被害

サイバー攻撃を受け、システム障害が発生。酒類・飲料・食品の国内の受注と出荷が全面停止しました。

被害発生日	2025年9月
目的	非公表　身代金目的か
方法	ランサムウェア
対象	非公表　サーバか？
被害内容	情報漏洩、酒類・飲料・食品の国内の受注と出荷が全面停止
被害金額	非公表

ランサムウェア以外の攻撃としては、2021年12月に製薬メーカ E社で不正アクセスによる個人情報漏洩被害が発生し、22万人の個人情報が流出しました。2024年4月には製薬メーカ F社でも同攻撃による個人情報漏洩被害が発生し、70万人の個人情報が流出しました。

製薬メーカ E社

サーバ不正アクセスによる個人情報漏洩被害

複数拠点のサーバが不正アクセスを受け、個人株主や採用応募者など個人情報が流出したおそれがあると発表しました。

被害発生日	2021年12月
目的	不明
方法	不正アクセス
対象	複数拠点のサーバ
被害内容	個人株主や採用応募者の個人情報22万件の流出
被害金額	不明

製薬メーカ F社

サーバ不正アクセスによる個人情報漏洩被害

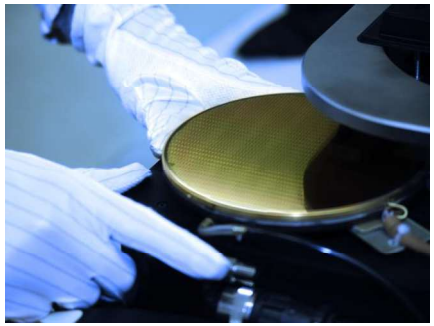
不正アクセスにより、F社の日本法人から日本国内の個人情報が漏洩しました。攻撃者はセキュリティポリシーに反した海外コンサルタントの個人PCからIDを不正利用し、F社のデータベースに侵入しました。

被害発生日	2024年4月
目的	不明
方法	不正アクセス
対象	サーバ
被害内容	日本国内の医療従事者70万人以上の個人情報が漏洩
被害金額	不明

従業員による不正被害も発生しました。2014年3月に半導体メーカ G社が提携先社員による内部不正により、データをUSBメモリに複製する原始的な手段で、技術情報を競合他社に漏洩する事故がありました。降格への不満や転職条件を有利にする目的だったと報じられています。

半導体メーカ G社

提携先社員による内部不正



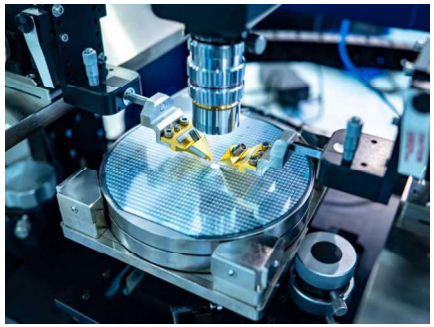
G社と業務提携していたH社の元技術者が、G社の研究データを不正に持ち出してI社に提供していました。
不正行為は約2年間続けられ、G社はI社に対して損害賠償を求めて起訴し、最終的に和解が成立しました。

被害発生日	2014年3月
目的	降格への不満、転職条件を有利にするため
方法	USBメモリへのコピー
対象	技術情報を管理するサーバ
被害内容	技術情報の漏洩
被害金額	損害賠償約1090億円、和解金約330億円

製造DXが進展して製造現場をネットワークに接続する時代になったたため、製造現場(OT)での被害事例も増加しています。
2018年8月に台湾半導体メーカ、2019年3月にはノルウェー アルミニウム製造メーカがランサムウェアの被害に遭い、OT機器にも拡大しました。

台湾半導体メーカ

ランサムウェアによる被害



ランサムウェアの被害を受けて多くのコンピュータと製造装置に影響を及ぼしました。ウィルスに感染した機器をOTネットワークに接続したため、感染が拡大しました。

被害発生日	2018年8月
目的	不明
方法	ランサムウェア 「WannaCry」
対象	パソコン、製造装置
被害内容	3日間生産停止
被害金額	営業利益ベースで190億円

引用：(IPA)「制御システム関連のサイバーインシデント事例」シリーズ 2018年 半導体製造企業のランサムウェアによる操業停止

ノルウェー アルミニウム製造メーカ

標的型攻撃＋ランサムウェアによる操業停止

取引先とのメールを悪用して悪意のあるサイトに誘導してIT機器がランサムウェアに感染しました。感染は、OT機器にも拡大しました。

被害発生日	2019年3月
目的	不明
方法	ランサムウェア 「LockerGoga」
対象	パソコン、製造装置
被害内容	数か月の生産減、手作業による生産
被害金額	2019年Q1とQ2の合計65～77億円

引用：(IPA)「制御システム関連のサイバーインシデント事例」シリーズ 2019年　ランサムウェアによる事業減速

補足資料

Nozomi Guardianは、産業用ネットワークのセキュリティと可視化・異常検知を実現するソリューションです。リアルタイムで脅威を検知して迅速に対応できます。異常なトラフィックを把握して業務の継続性を維持し、サイバー攻撃に対する防御を強化します。

特長

制御システムネットワークを一元的に管理

- OT環境をモニタリングして環境内の資産を可視化
- 通信状態や接続構成などを総合的に管理

異常通信を検出してセキュリティ運用を支援

- 通信環境を分析してサイバー攻撃や予兆を検知
- 異常通信の情報を記録して有事の分析をサポート

最新の脅威情報を用いて脆弱性・リスクを把握

- 最新の脅威情報を随時配信
- 変化する脅威の状況を常に把握

製品ラインアップ

機種名	NSG-M 1000	NSG-M 750	NS1 250	NS1 100	NS1R
外観					
最大ノード数	40,000	10,000	5,000	1,000	500
最大ネットワークエレメント	600,000	200,000	90,000	20,000	10,000
最大スループット	1Gbps	1Gbps	500Mbps	500Mbps	250Mbps
搭載インタフェース	7×1000BASE-T 4×SFP 拡張1slot	7×1000BASE-T 4×SFP 拡張1slot	7×1000BASE-T 拡張1slot	7×1000BASE-T 拡張1slot	1×1000BASE-T 2×SFP
ストレージ容量	256GB	256GB	128GB	128GB	64GB

システム概要

ネットワーク、構成機器(資産)の可視化

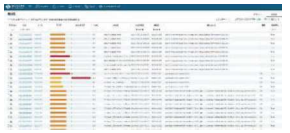
- 制御システムネットワークに接続されている機器を検出し、ネットワークマップ上に表示
- 機器の区分(PC/PLCなど)や使用されているプロトコルを判定

ネットワーク異常検知

- 環境下で発生したセキュリティ上の異常な振る舞いをアラートとして発報
- 異常通信として定義された振る舞いや、定常時の通信から外れた未知の挙動を検知

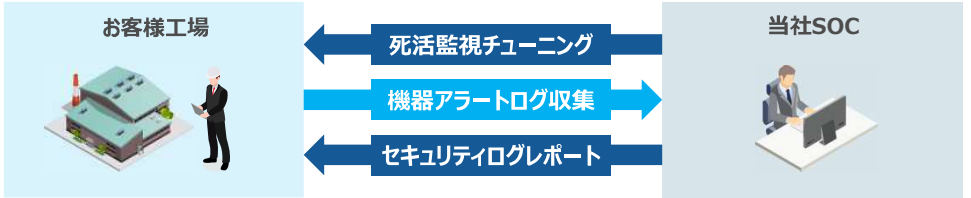
脆弱性・リスク管理

- セキュリティパッチやファームウェアのバージョンを把握し、公開されている脆弱性情報と照らし合わせて、リスク値を表示



セキュリティ運用支援

- 機器導入後は統合管理センター(SOC)で24時間365日体制で機器のセキュリティ監視・死活監視
- 緊急性の高いイベントを検知時、お客様に直接通知



補足資料

Nozomi Arc Embeddedは、三菱電機とNozomi Networksの共同開発製品です。当社PLCにエンドポイントセキュリティセンサ「Nozomi Arc」を搭載した、PLC常駐型のセンサです。フィールドネットワークの可視化・異常検知を可能にします。

特長

PLC組込み セキュリティセンサー

- Nozomi Networks社と三菱電機の共同開発品
- PLCにエンドポイントセキュリティセンサーを搭載可能

可視化/検知できる範囲を拡大

- PLCの製品情報と稼働情報を見える化
- PLCの通信状態を常時監視
- USBなどの通信を検知

Nozomi Guardianと連動し、可視化・異常検知

- 最新の脅威情報を随時配信
- 変化する脅威の状況を常に把握

製品紹介

iQ-R C言語インテリジェント機能ユニット RD55UP12-Vに、Nozomi Arc Embeddedが搭載可能です。
データを収集・分析するエンドポイントセンサとして、収集したデータをNozomi Guardianに送信します。

MELSEC iQ-Rシリーズ

インストール

Arc Embedded

MELSEC iQ-R
C言語インテリジェント機能ユニット
RD55UP12-V

OTネットワーク

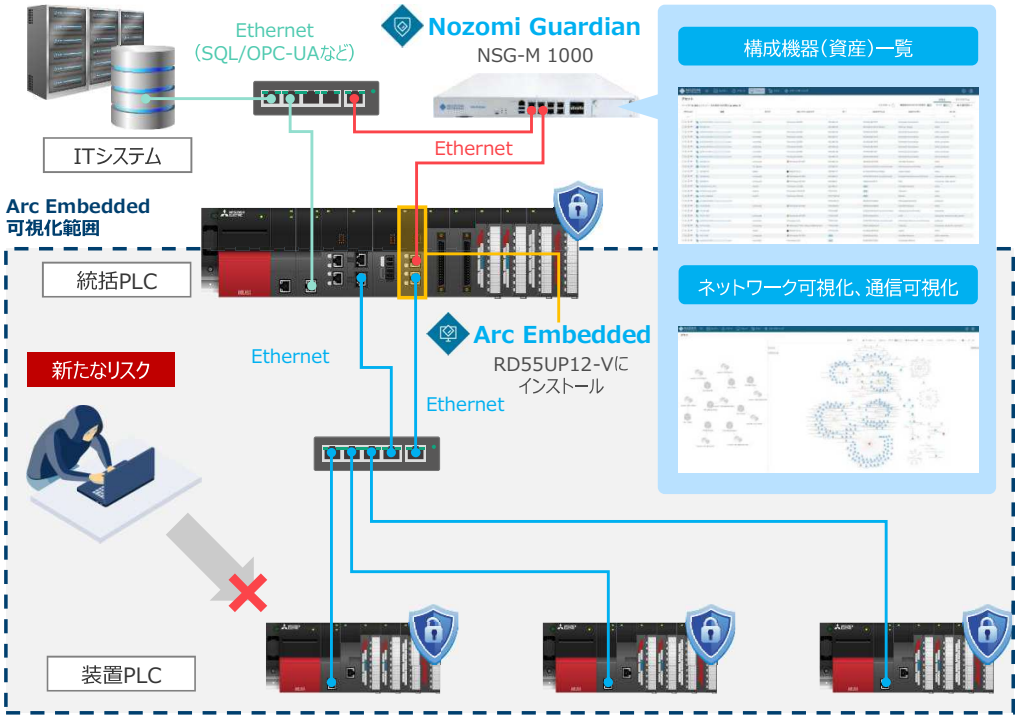
情報ネットワーク(Lv4/5)
制御DMZ(Lv3.5)
制御情報ネットワーク(Lv3)
制御ネットワーク(Lv2)
フィールドネットワーク(Lv1)
フィールドネットワーク(Lv0)

Nozomi Guardian 可視化範囲

Arc Embedded 可視化範囲

システム概要

DXの進展により、データ収集を目的に装置PLCもネットワークに接続されるようになり、新たなリスクが生じています。統括PLCのiQ-RにNozomi Arc Embeddedを搭載することで、統括PLCと装置PLCの通信を監視することができます。



補足資料

TXOne Networks EdgeIPSは、産業用ネットワークのセキュリティを強化する侵入防止システムです。リアルタイムでサイバー攻撃を検知し、迅速に防御策を講じることができます。OT環境に特化しており、業務の安全性を高めて運用の継続性を確保します。

特長

ネットワークセグメンテーション

- IPアドレスなどの情報から通信を許可・拒否(遮断)
- 生産ラインをマイクロセグメント化してマルウェア感染の拡大を防止

仮想パッチ

- 既知の脆弱性をネットワークで遮断し、古い設備(エンドポイント)を防御

運用セキュリティ支援

- 統合監視装置EdgeOneを用いたEdgrIPSの集中管理で運用の手間を削減

製品ラインアップ

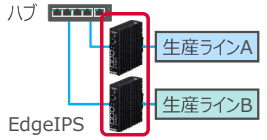
機能	EdgeIPS 103	EdgeIPS Pro 216	EdgeIPS Pro 1048/2096	EdgeIPS Pro 2008/2016F	EdgeFire
スループット	850Mbps＋	2Gbps＋	10Gbps/20Gbps	20Gbps	200Mbps＋
ネットワークセグメンテーション	1	8	12/24/48/96	4/8	2 WAN/8 LAN
ハードウェアバイパス*	設定可能	設定可能	設定可能	設定可能	-
ストリーミングベースアンチウイルス	-	✓	✓	✓	-
ポートペア間の横感染防止	-	✓	✓	✓	✓

*：電源喪失時にEdgeIPSを介した通信を継続する機能

機能概要

ネットワークセグメンテーション

- EdgeIPSを設置するだけで、ネットワーク再設計不要で通信を論理的に分断



セグメント化でラインAとラインBの所属が同一から個々のセグメントに変化

仮想パッチ

- 攻撃パターンを基に古い設備宛ての通信を検定し、ネットワーク攻撃を遮断

定期的に更新される攻撃パターン情報により、新たな攻撃にも対応

運用セキュリティ支援

- Webブラウザから製造現場に設置したEdgeIPSを一覧で表示し、設定変更や状態監視、ソフトウェアのアップデートなどが可能

SOCサービス

- 機器導入後は統合管理センター(SOC)で24時間365日体制で機器のセキュリティ監視・死活監視
- 緊急性の高いイベントを検知時、お客様に直接通知

補足資料

DISPELは、セキュアなリモートアクセスを提供するソリューションです。機密データを保護できるため、お客様は安全に企業のネットワークに接続してリモート作業を行うことができます。アクセスを厳格に管理することで、サイバー攻撃のリスクを低減して安全な業務を実現します。

特長

柔軟で一元的な運用管理

- すべての設定管理はクラウド上で一元化
- 管理者によるリモートアクセスの承認

高度なセキュリティ

- MTD*1技術やVDI*2によるセキュアなリモートアクセス環境をSaaS型で提供

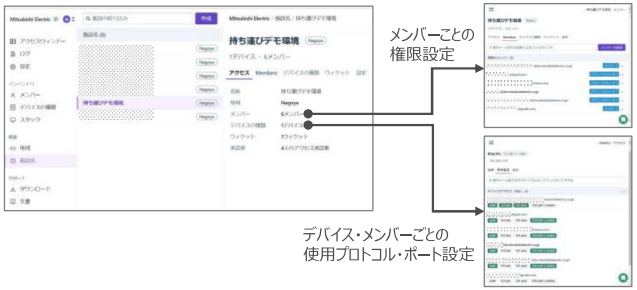
各種ガイドライン準拠

- 国政基準ガイドラインに準拠(NIST CSF*3IEC62443*4)

*1：MTD (Moving Target Defense) 攻撃者に標的を見失わせるように、コンピュータのIPアドレスを頻繁に変更する技術
*2：VDI (Virtual Infrastructure) 仮想デスクトップ
*3：米国国立標準技術研究所によって公開されている、組織のサイバーセキュリティリスクを軽減するための一連のガイドライン
*4：産業用オートメーション、制御機器、開発プロセスを対象とした規格

直感的な操作を実現した管理画面

- 拠点、工場、ラインなどの各施設にアクセスを許可するメンバー(利用者)、デバイス(設備)、Wicketを登録
- 各メンバーに対象施設に対する管理者権限や一般ユーザ権限を設定
- 各デバイスおよびメンバーが使用できるプロトコル(TCP、UDP、ICMPなど)・ポート番号を制限



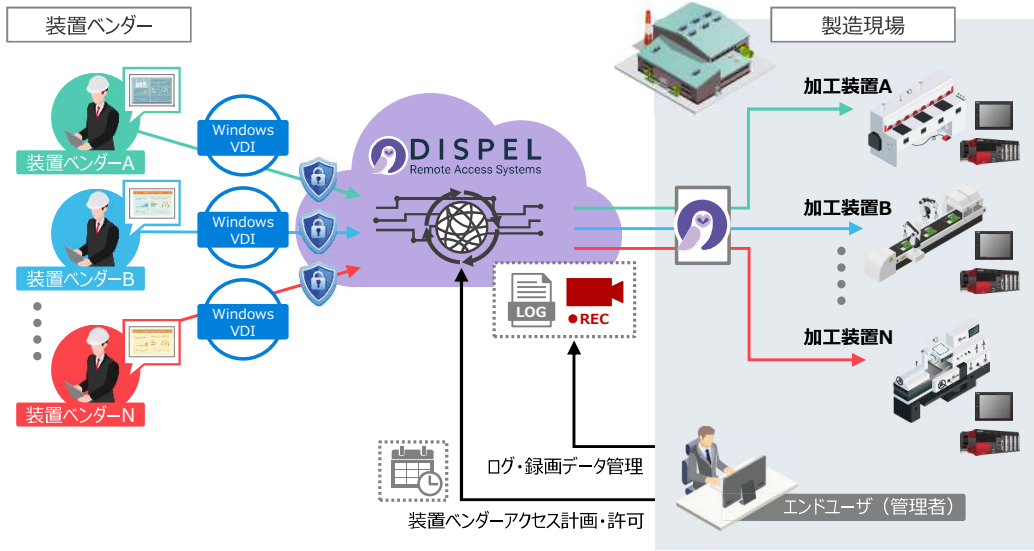
システム概要

SaaS型リモートアクセス

- VDI環境により、メンテナンス作業用のPC管理業務から解放
- 管理者は利用者のVDI環境内におけるすべての操作を確認できる
- 通信経路を接続するたび、ランダムに変更して確立

強化されたセキュリティ機能

- クライアントPCに直接接続する必要がないため、ウイルス感染リスクを低減
- 接続経路が頻繁に変更されるため、ハッカーに標的を絞らせない
- インバウンドボードの開放が不要のため、外部ネットワークの侵入口が見えない



補足資料

SOC(Security Operation Center)サービスは、専門技術者がOT環境を24時間365日監視し、サイバー攻撃を正確かつ迅速に分析するサービスです。多種多様な通信が流れるOT環境を専門技術者が監視し、素早く正確に攻撃を検知し、影響を最小限に抑えることが可能です。

特長

24時間365日対応

- OT環境に導入した対策ソリューションも監視対象とすることで、可用性が重視される製造現場でのインシデントにいち早く対応できます。

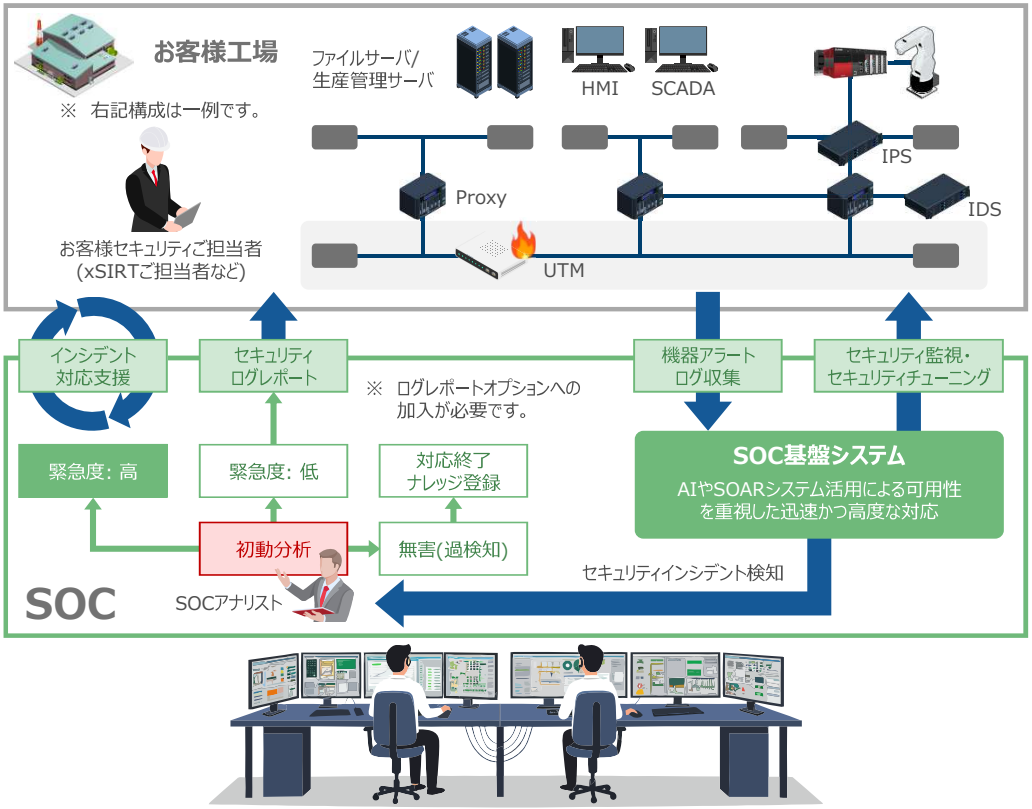
高度な監視技術

- 当社研究所で開発した技術を活用し、独自の検知技術により高度なセキュリティ監視を実現します。

先進的な分析技術

- 自動化、AI活用など迅速で高度なインシデント分析を実現します。

システム概要



サービスの内容

セキュリティ監視

- 各種対策ソリューションで導入したセンサ類によりインシデントを検知します。
- 当社独自ルールに基づくSIEM分析により、複雑で高度な攻撃を検知します。

インシデント対応

- 一次対応としてSOCアナリストによる検知・分析を実施します。
- 高度な攻撃に対しては二次対応としてシニアアナリストによる詳細分析を行い、影響を判断します。
- セキュリティログレポート

セキュリティログレポート

- 発生したインシデントの傾向や世間の情勢から攻撃の予兆などを分析し、月次でレポートとして報告します。

セキュリティチューニング

- 各種対策ソリューション(IDS/IPSなど)導入時に、過検知・誤検知などの不要なアラームを削減し、迅速なインシデント検知を目的としたチューニングを実施します。
- 構成変更や誤検知などがあった際にも継続してチューニングを実施し、セキュリティ対策を強化します。