生産現場の理解に基づく OTセキュリティ対策の重要性

三菱電機株式会社　OTセキュリティ事業推進部
大久保　佑

2024/7/26

工場セキュリティガイドライン啓発・連続セミナ第11回

自己紹介

Interop2022,2023,2024 OTセキュリティ教育に関する発表

小学校向けセキュリティ教育

某鉄道会社向けOTセキュリティ教育

三菱電機株式会社
OTセキュリティ事業推進部　コンサルティンググループ

大久保　佑

家族構成　：　妻1　娘1

趣味　　：　ゴルフ　お酒

職歴　　：　空港向け航空管制システム開発
OTセキュリティ製品企画開発
IPA産業サイバーセキュリティセンター(ICSCoE)研修
OTセキュリティサービス企画
└工場模擬環境とサイバー攻撃シミュレータ構築
OTセキュリティコンサルティング

資格　　：　産業サイバーセキュリティエキスパート
情報処理安全確保支援士(セキュリティスペシャリスト)

1-1 イントロダクション

近年、情報システムに対するサイバー攻撃の脅威は増し続けています。企業にとってセキュリティ事故はビジネスに多大な損害を与えるため、**ITセキュリティ対策**は経営課題として重要です。

一方、これまで独立した環境下で運用されてきた工場も生産性向上や品質向上を目的としたDX化が進み、外部とつながることで**OTセキュリティ対策**の重要性も拡大しています。

DXを活用した
生産ラインのデジタル化・
自動化を導入した
「つながる工場」化の加速

これに伴い、
OTセキュリティ対策の重要性が拡大

▼

**OT向けセキュリティ規制や
ガイドラインの強化**

製造分野のDX化により「つながる工場」化が進み、ITセキュリティ対策だけでなく、

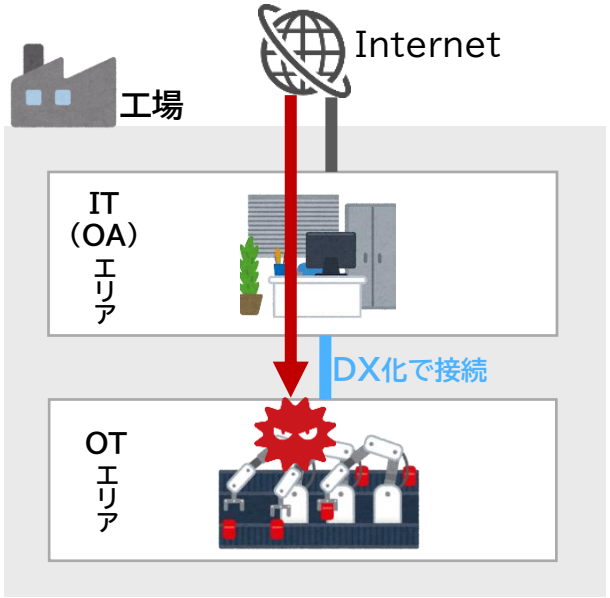
OTセキュリティ対策の重要性が拡大

1-2 OTセキュリティの必要性

よく挙がるOTセキュリティの疑問

製造部門：ITエリアだけを対策すれば十分では？

情報システム部門



以前

ITエリアとOTエリアが完全に分離

外部とつながるITエリアのみ対策をすれば基本的には十分

近年（DXの進展）

OTエリアはITエリアや外部にも接続

ITエリアを通り越し、OTエリアにもサイバー攻撃の脅威が拡大

以前は完全分離であったITエリアとOTエリアがDX化によりつながり
OTエリアにもサイバー攻撃への備えが必要

1-3 生産現場の理解に基づくOTセキュリティ対策を進めるためには

① IT部門/OT部門の認識合わせ

② 製造現場ごとのリスクアセスメント

③ OTの特性を考慮した対策導入（事例紹介）

生産現場の理解に基づくOTセキュリティ対策を進めるためには

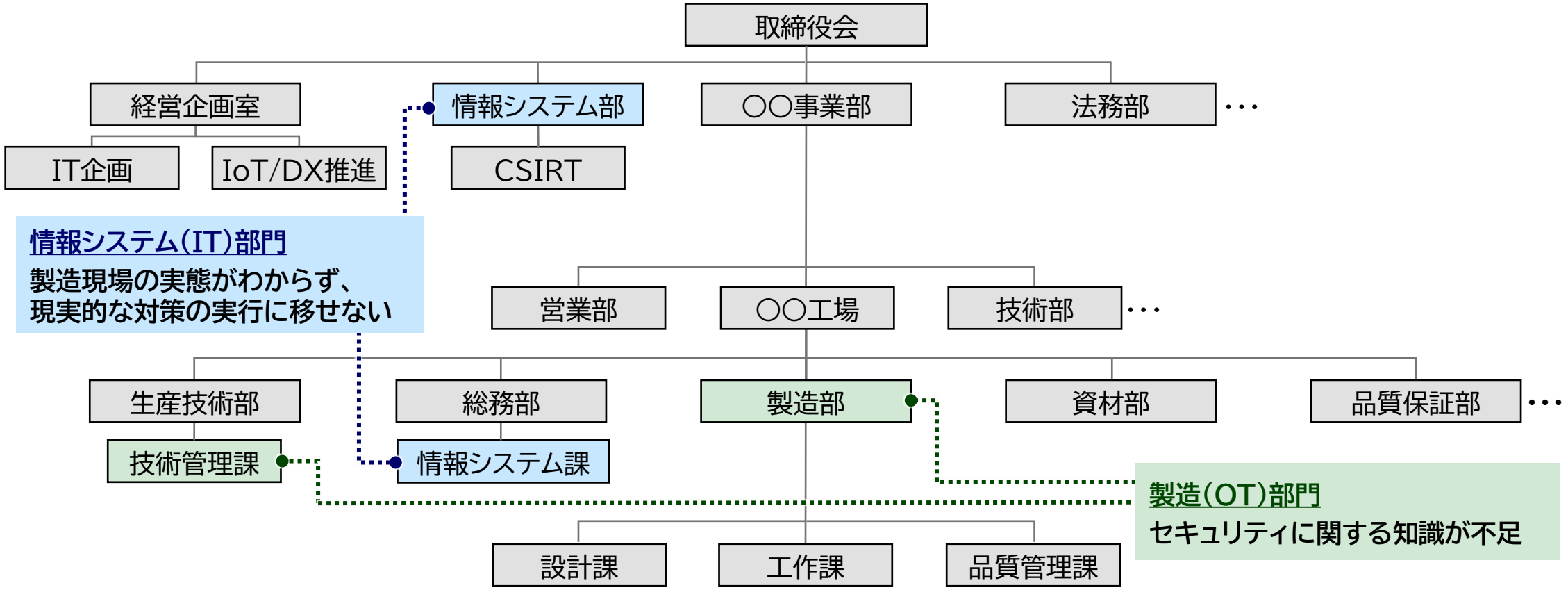
MITSUBISHI ELECTRIC
Changes for the Better

① IT部門/OT部門の認識合わせ

② 製造現場ごとのリスクアセスメント

③ OTの特性を考慮した対策導入（事例紹介）

2-2 OTセキュリティ推進における体制面の課題



Q OTセキュリティ対策を主導する部門は明確ですか？
（専任組織、経営層との連携、部門連携、ガバナンスなど）

2-3 IT（セキュリティ）とOT（セキュリティ）の違い

	IT（情報システム部門）	OT（製造部門）
主な目的	情報の管理や利活用	生産性や品質の向上
利用技術	Windows/Linux、Ethernetなど	PLC、産業用ネットワークなど
保護対象	個人や企業の機密情報	生産情報、モノ（設備、製品）、サービス（連続稼働）
セキュリティの考え方	情報漏洩の防止を重視	情報漏洩の防止、生産・品質の維持の両方を重視
稼働時間	通常業務時間内	24時間365日
システム更新	3～5年	10年～20年

扱う技術や考え方が違うため、お互い理解することが重要

ITセキュリティ ＝ 個人や企業のデータなどの**情報保護対策**

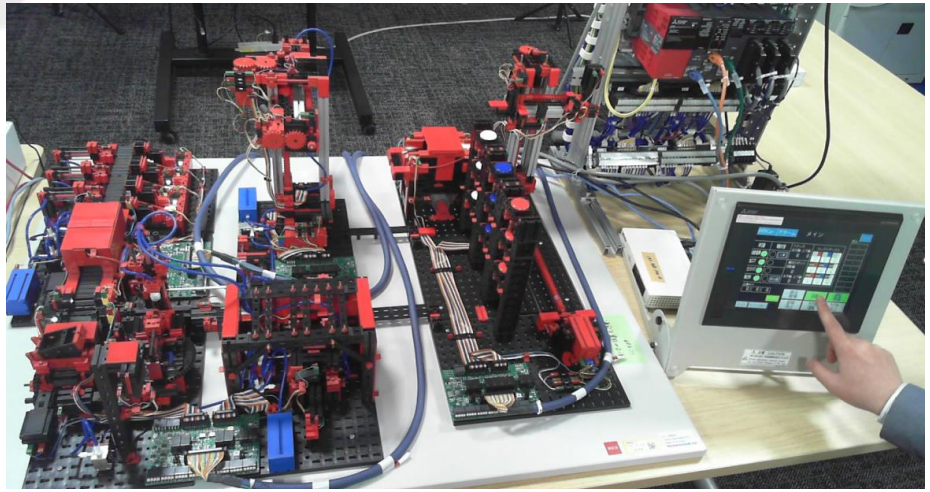
OTセキュリティ ＝ 生産やサービスの**可用性も意図した保護対策**

2-4　当社の取り組み　―　横浜ラボ（工場模擬環境）　―

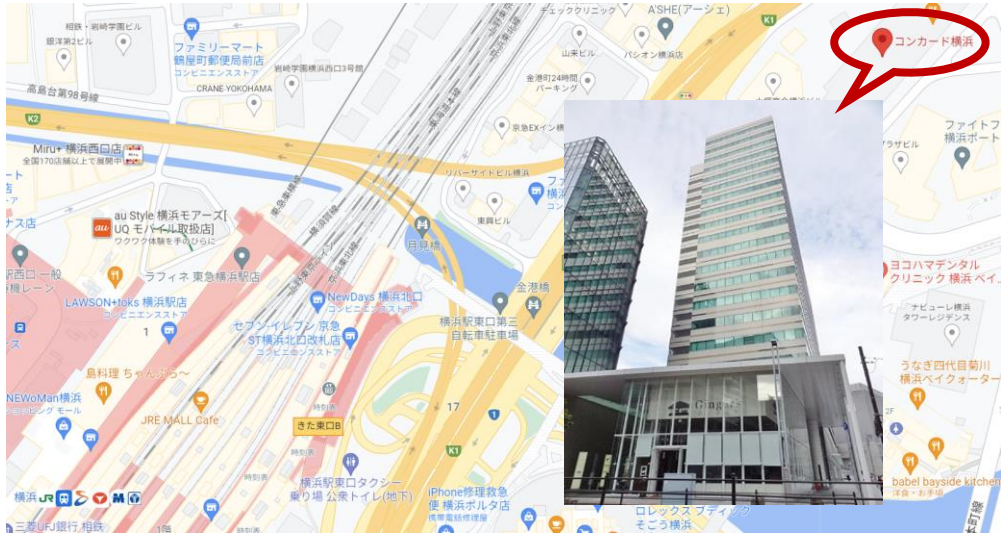
＜目的＞

① お客様にサイバー攻撃による被害と対策のデモをご覧いただき、工場におけるサイバーセキュリティの重要性を体感していただく

② セキュリティ製品を模擬工場ネットワークで検証する

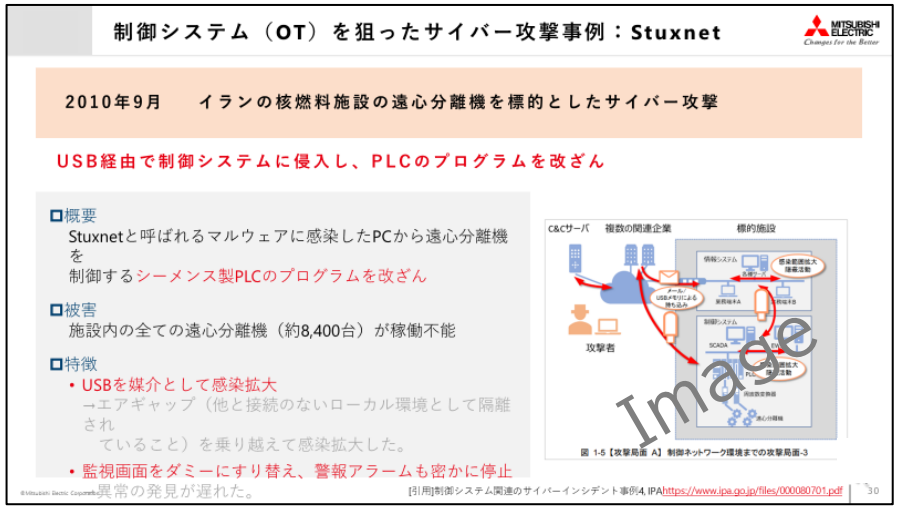


＜場所＞コンカード横浜（横浜駅から徒歩8分）

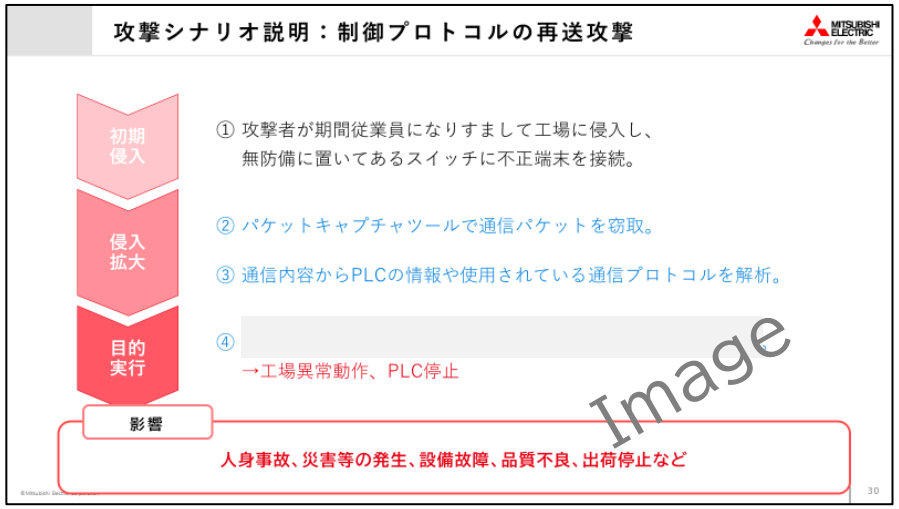


2-5 デモの流れ

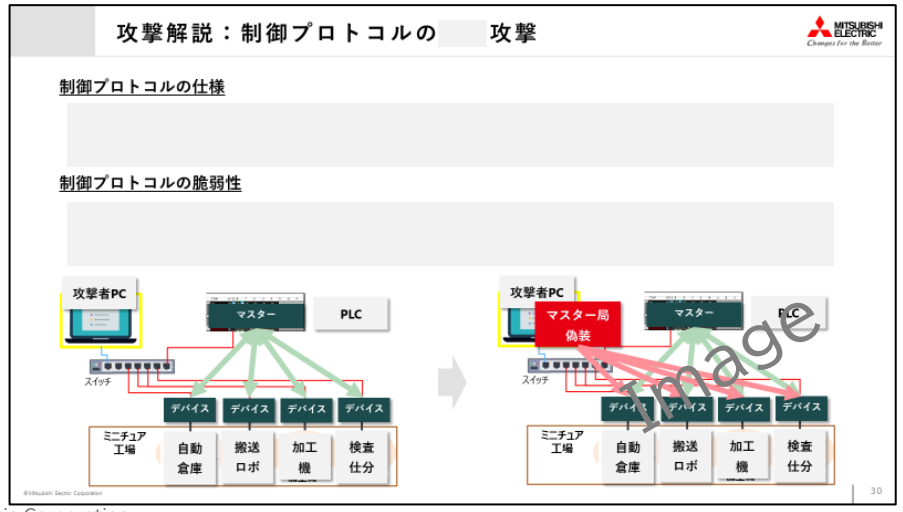
①背景や事例紹介、模擬環境説明



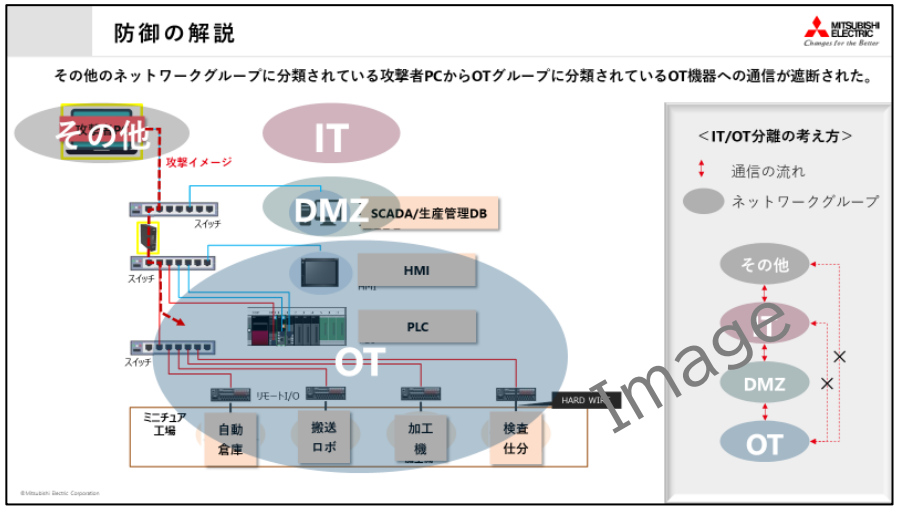
②攻撃シナリオ説明・攻撃実演



③攻撃解説・ディスカッション



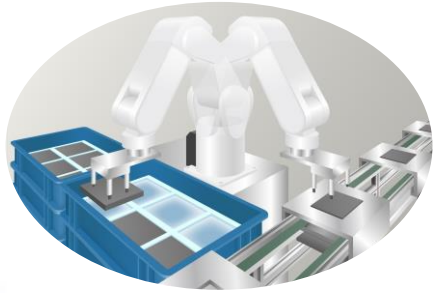
④対策解説



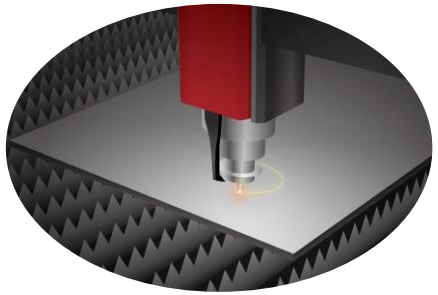
工場模擬環境のイメージ

①ピッキング

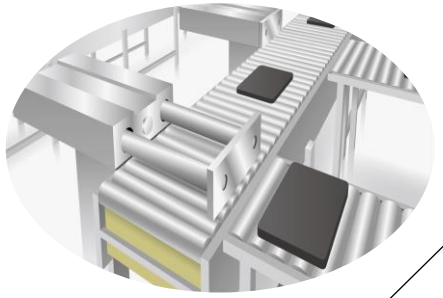
②搬送



③加工



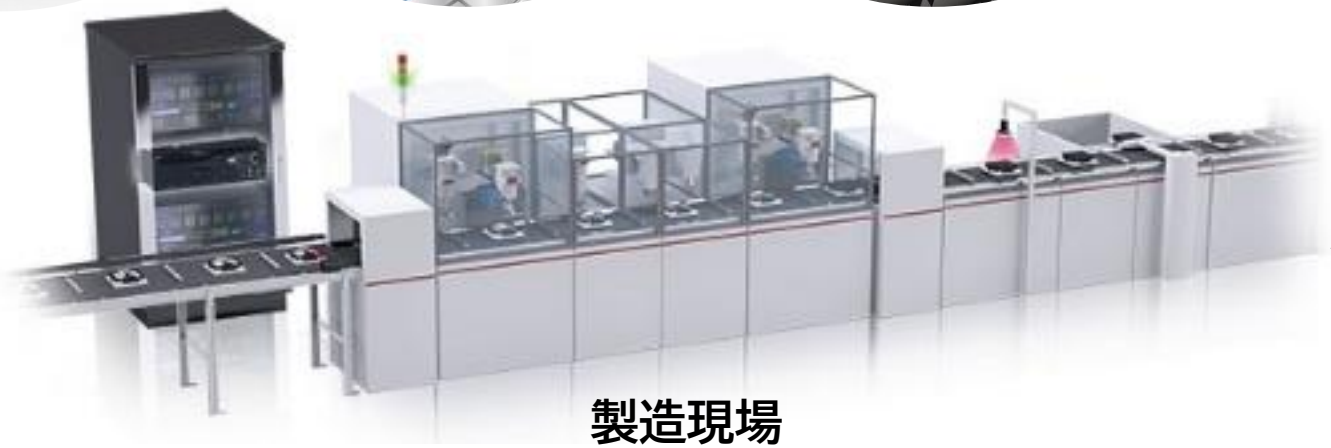
④仕分け



事務所

・遠隔監視
・生産計画/実績集計
・設計

※USB利用有り



製造現場

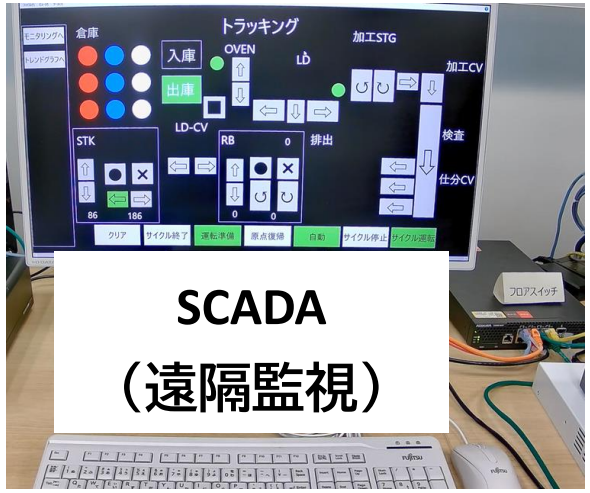
現場事務所

・生産量調整
・品質検査

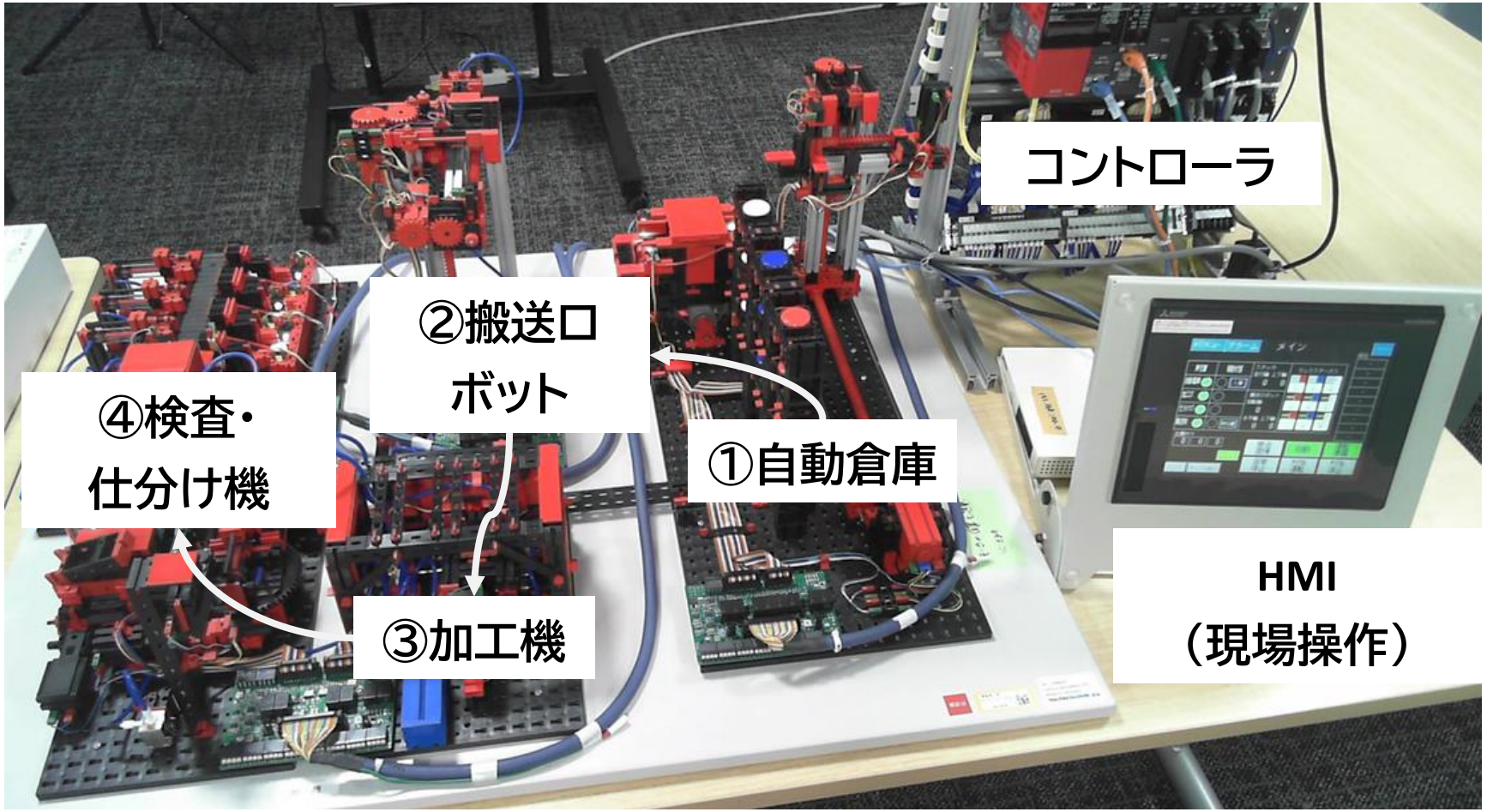
※USB利用有り

2-7 工場模擬環境の実機全体像

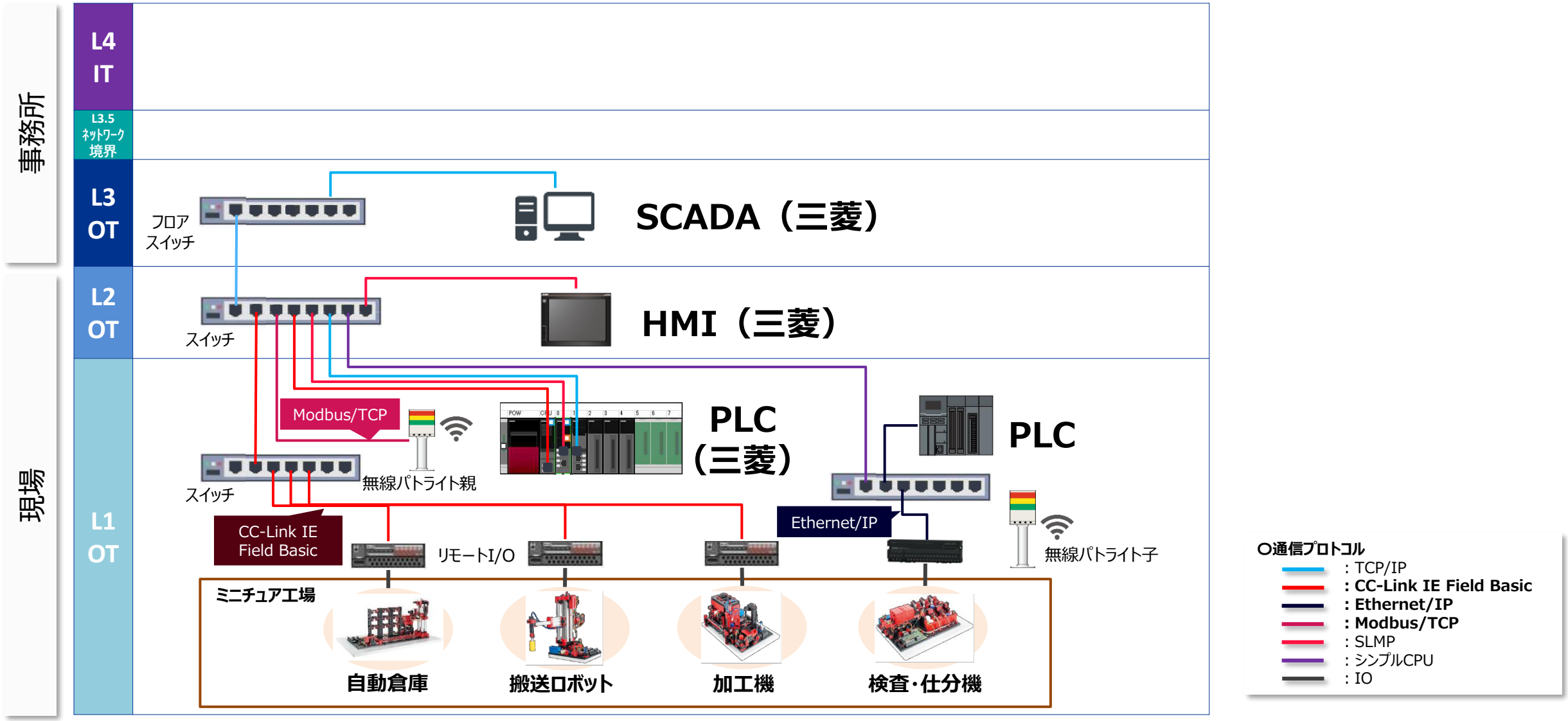
事務所



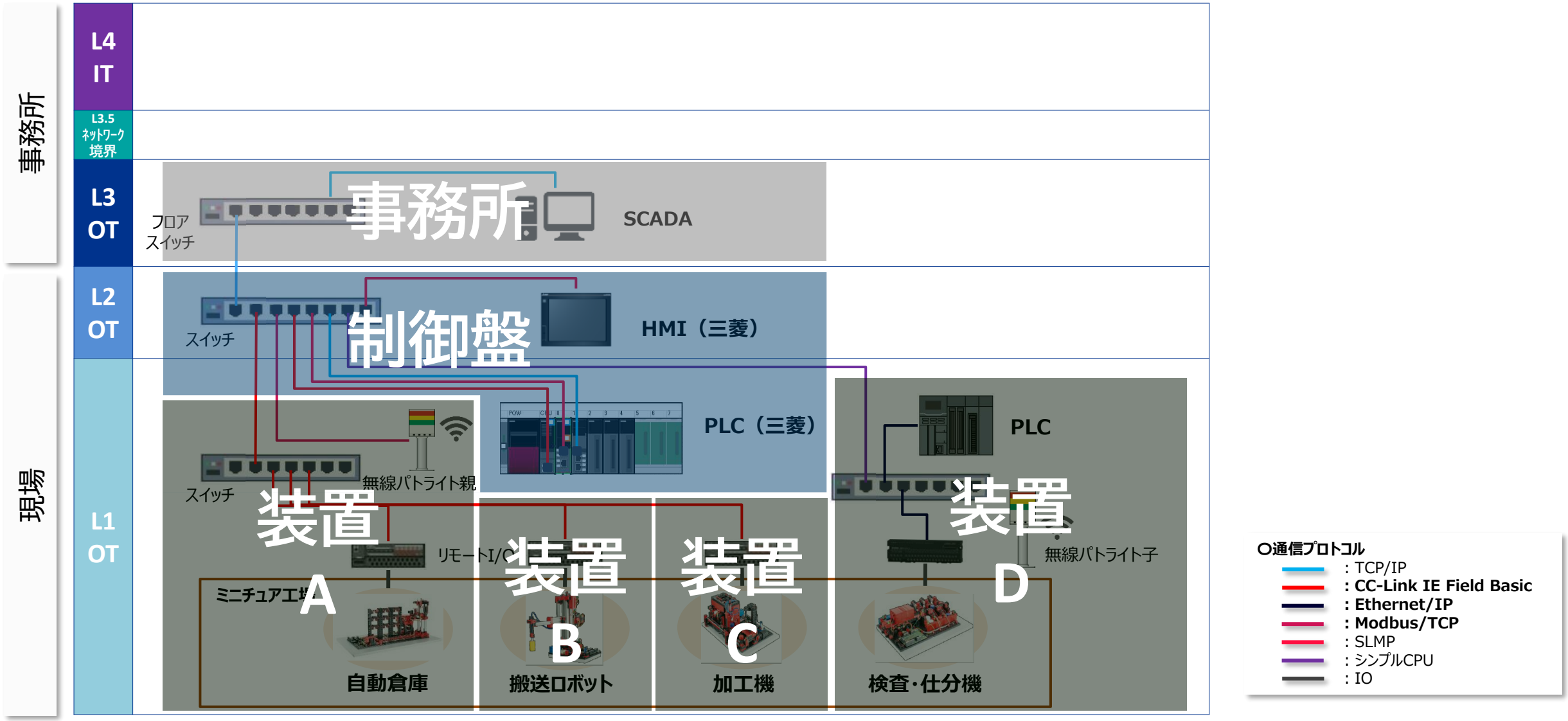
現場



2-8 工場模擬環境のネットワーク構成

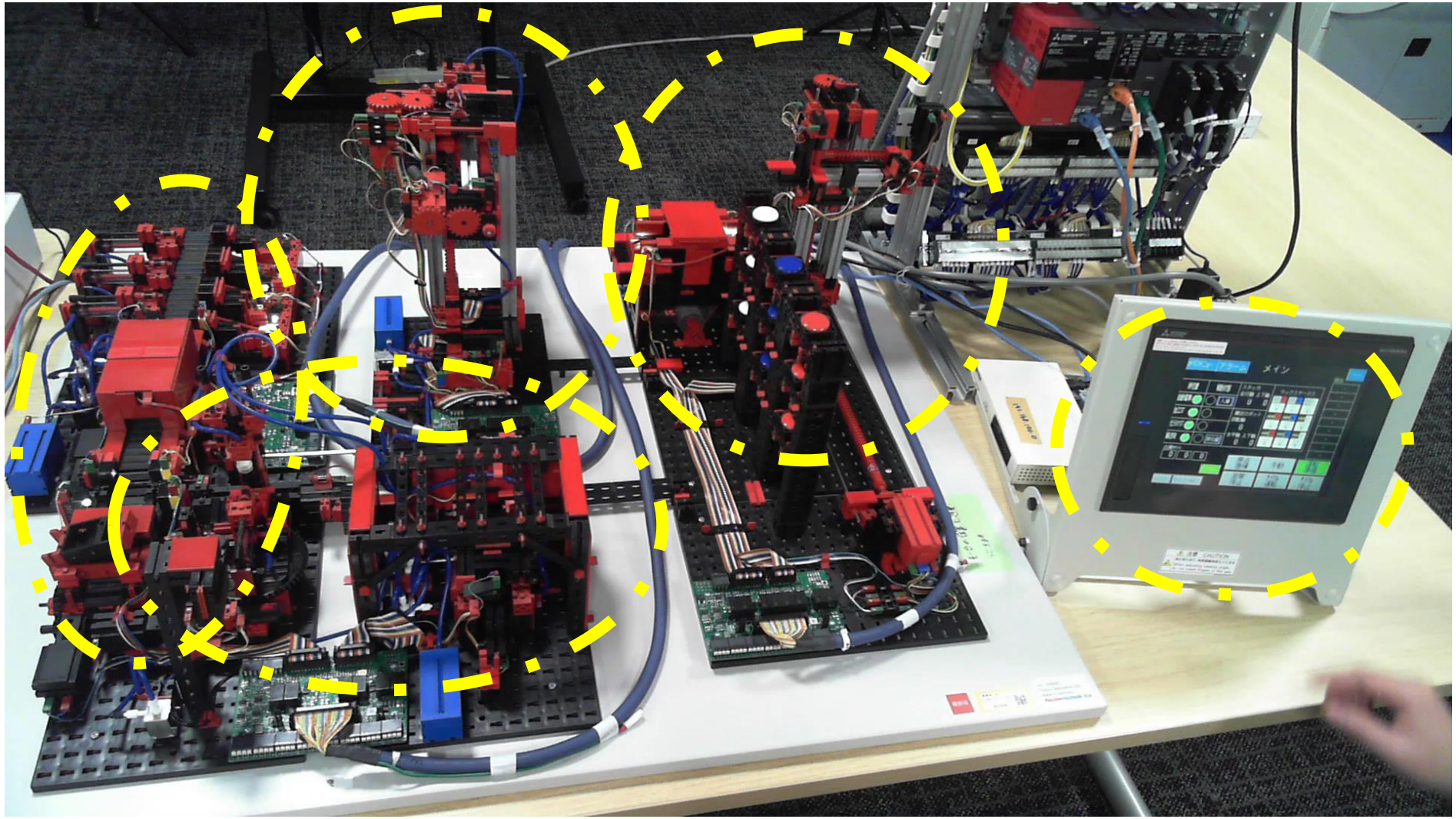


2-9 工場模擬環境のネットワーク構成



正常時の動作確認

※時間短縮のため1.5倍速で再生しています。



検査仕分け機ではワークの色を判定し、色ごとに自動で仕分けます。

2-11 攻撃シナリオ紹介

情報セキュリティの3要素（AIC）の観点で
製造業における発生してほしくない事業被害を設定

各事業被害を引き起こす攻撃シナリオを
攻撃者視点で開発

AICの観点	サイバー攻撃による事業被害（例）	No.	攻撃シナリオ プリセット	発生させる事象
可用性（Availability）	製造設備の異常動作・長期停止	1-1	制御システムへの負荷攻撃	PLC停止
		1-2	制御プロトコルのファジング	PLC停止
		1-3	制御プロトコルの再送攻撃	フィールド機器の異常動作
		1-4	SCADAの表示異常	遠隔監視不可⇒現場確認のため生産停止
		1-5	パトランプの誤作動	パトランプ作動⇒現場確認のため生産停止
完全性（Integrity）	情報改ざんによる不良品の製造・出荷	2-1	HMIからの操作パケット改ざん	PLCの設定値変更⇒不良品製造・出荷
機密性（Confidentiality）	製造機密の情報漏洩	3-1	エンジツールの悪用	PLC内の情報の漏洩
		3-2	パスワード解析	SCADAサーバ内の情報の漏洩

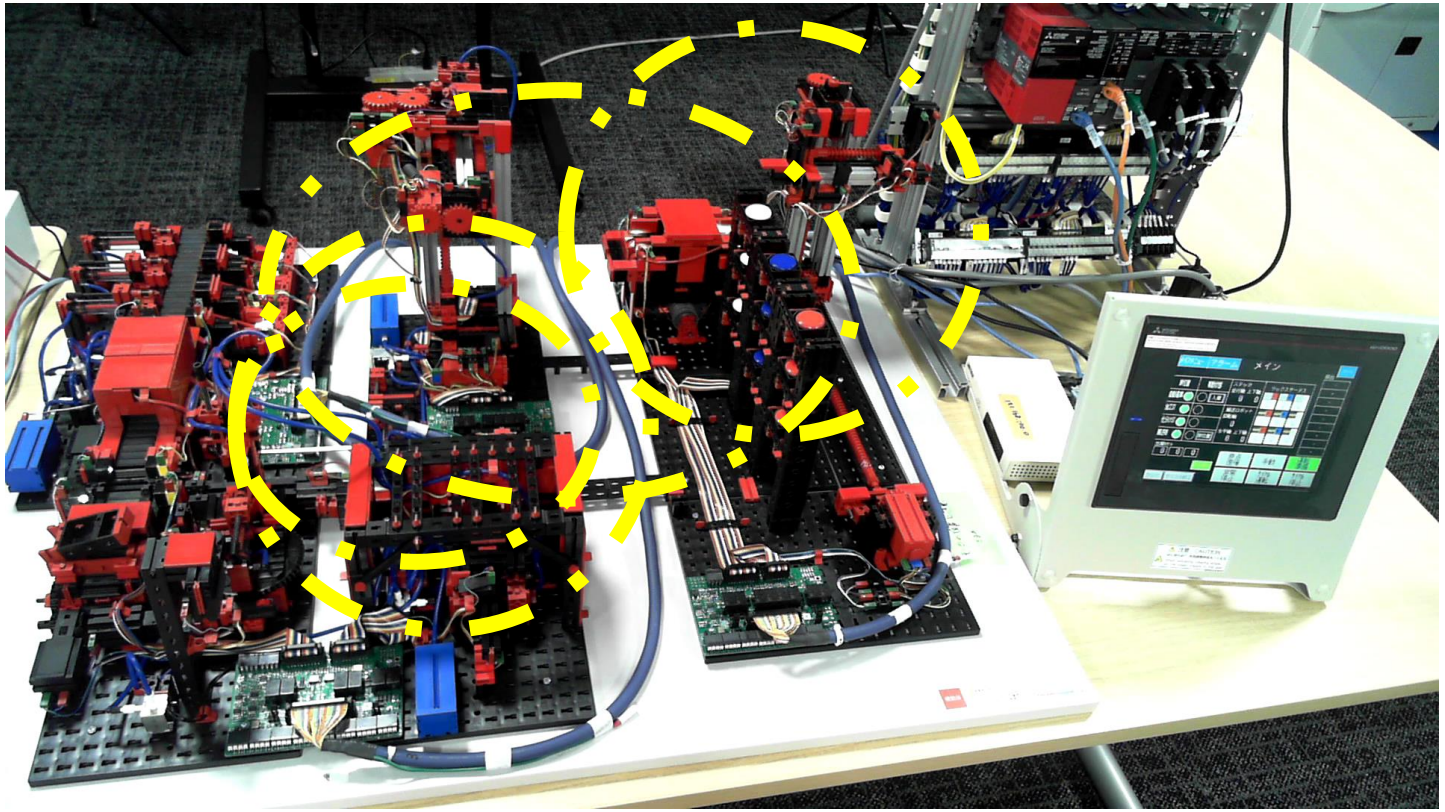
攻撃デモ動画

攻撃者の様子

パケット キャプチャ → ペイロード 解析 → 攻撃

攻撃を終了します。

現場の様子



アームが旋回し倉庫に追突

デモ見学者の声

- セキュリティ対策の必要性を実感した。**セキュリティ製品の導入を検討する。**
- **工場における具体的な脆弱ポイントを知れた。**
- **次回は社内の若手をつれてくるのでセキュリティ教育をしてほしい。** →24年度より研修サービススタート
- **PLC等のOT機器へのサイバー攻撃の仕組みや具体的な攻撃手法を理解できた。**
- **工場のお客様に紹介したい。**
- 実機があることでOTセキュリティについて学びやすかった。

実機へのサイバー攻撃を体験することで、OTの仕組みや攻撃手法/脆弱ポイントの理解が深まり、
OTセキュリティについて認識合わせができる

生産現場の理解に基づくOTセキュリティ対策を進めるためには

① IT部門/OT部門の認識合わせ

② 製造現場ごとのリスクアセスメント

③ OTの特性を考慮した対策導入（事例紹介）

3-2 リスクアセスメントの重要性

経済産業省発行の工場セキュリティガイドラインでは、OTセキュリティを検討するうえで実施する内容を妥当なものとするために、まず始めに必要な情報を収集・整理し、セキュリティリスクを分析したうえで対策方針を策定する手引きが記載されています。

①工場セキュリティガイドライン（経産省）

■以下のサイクルを継続的に回すことが重要

A. 現状把握
- 自社工場システム内の業務を整理
- 保護すべき対象を抽出し、想定される脅威を特定

B. 対策計画
- 対策すべき脅威を決定し対策方針を策定
- 対策に対応したセキュリティ製品/サービスを抽出

C. 対策の導入・運用・保守
- 抽出されたセキュリティ製品/サービスの導入
- セキュリティ製品/サービスの継続的な運用・保守
  （定期的な監視や、挙がったアラートへの対処等）

■本ガイドライン策定のワーキングに当社も参画

https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems guideline.html

3-3 ITとOTのリスクアセスメントの違い

OTのアセスメント

現状システム構成の把握

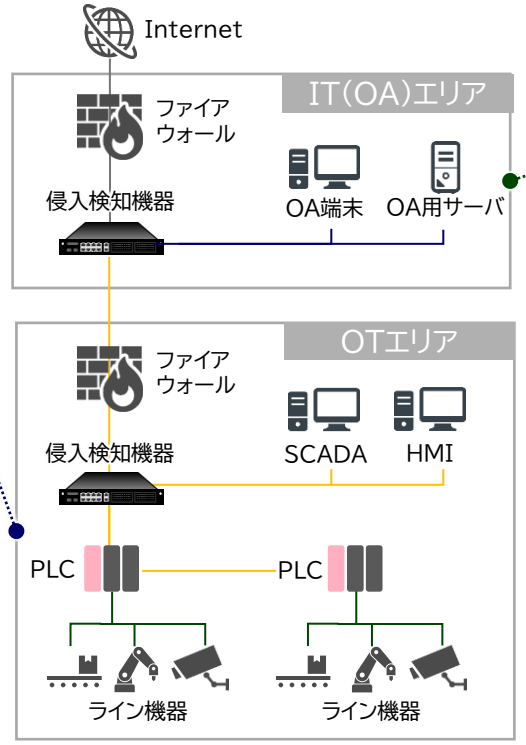
OTの機器やネットワークは様々、
把握が難しい

業務プロセスの把握

OT特有の業務プロセスがあり、
各業務の対策優先度付けが困難

セキュリティリスク分析と対策検討

情報保護＋可用性維持の対策が必要



ITのアセスメント

現状システム構成の把握

ITの機器やネットワークは差異が少なく
把握が容易

業務プロセスの把握

業務プロセスが一般化されており、
対策優先度付けが容易

セキュリティリスク分析と対策検討

情報保護の対策が必要

Q OTを考慮した適切なアセスメントはできていますか？

3-4 リスクアセスメントの種類と当社が提供する3つのサービス

リスクアセスメントの方式

ベースラインアプローチ

分析対象に対しする評価項目を設け、確保すべきレベル（ベースライン）を予め設定し、達成度を分析

リスクアプローチ

分析対象のシステムに対して、「重要度」（あるいは被害レベル）「脅威」「脆弱性」の観点でリスクを分析

評価方法

机上評価

ヒアリングや観察等机上で実施

【簡易アセスメント】

- チェックリストに基づく机上評価
- チェック項目が達成されている状態がベースライン
- 組織面・運用面・技術面に対する課題・対応策（案）の導出

【詳細アセスメント】

- 構成図等のドキュメントに基づく机上評価
- 脅威を起点として、設備・ネットワークに対するリスクを分析するリスクベースのアプローチ
- 分析対象固有のリスクの評価・対応策（案）の導出

実証的評価

パッシブ

ネットワークを流れるパケットを実環境から受動的に取得

【実証的アセスメント】

- 実環境に実機を接続する実証的評価
- ベースラインアプローチとリスクアプローチの考えを組み合わせた方式
  - 取得パケットの分析結果（識別されたOT資産や通信）が、把握できている状態（不明なものがない状態）がベースライン
  - 分析の結果、高リスク（把握していない未知）なOT資産や通信が識別される可能性がある点でリスクベース
- 分析対象の未把握のOT資産や通信、通信経路（攻撃面の可能性）の識別

アクティブ

OTデバイスの反応を実環境から能動的に取得

脆弱性スキャン	ペネトレーションテスト

- 実環境に実機を接続し、アクティブなスキャンや疑似サイバー攻撃を試みる実証的評価

（実環境を対象にアクティブにスキャンするため）稼働停止を伴う可能性あり非推奨

生産現場起点のアセスメント

現場に行き、現場を見て、現場の方と会話をし、アセスメントを実施

当社が現場にこだわる理由

- 生産現場は多種多様で、必要な対策は現場ごとに異なる
  - 企業合併、拠点の見直しによる生産の多様化
  - 導入時期の違いによる多様化
  - 装置メーカーや導入業者の違いによる多様化
- 現場の方にリスク・対策を知っていただく必要性
  - 現場によってまちまちなセキュリティ意識
  - 現場への協力要請
  - セキュリティ対策は、「運用・規則」、「組織・体制」が伴う

生産現場の理解に基づくOTセキュリティ対策を進めるためには

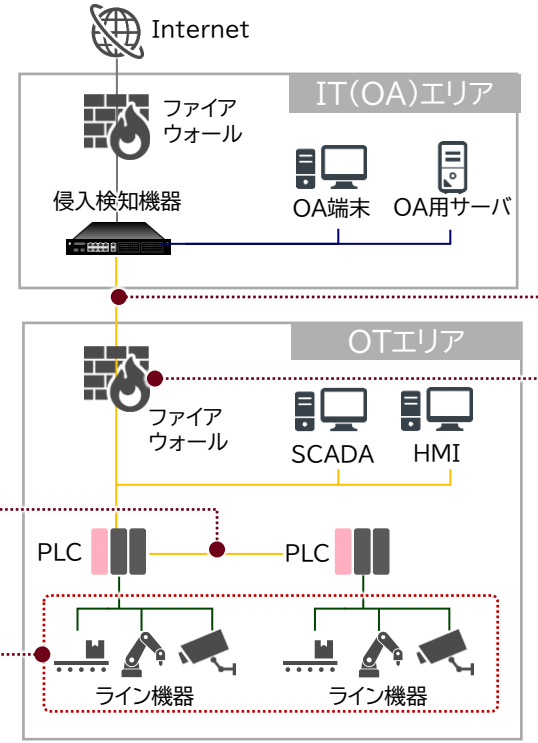
① IT部門/OT部門の認識合わせ

② 製造現場ごとのリスクアセスメント

③ OTの特性を考慮した対策導入（事例紹介）

4-2 OTセキュリティ推進における技術面の課題

OTを理解せず、
ITの知見だけでは限界あり



ネットワーク境界への対策導入の例

OTのシステム構成が把握できず、
ITとOTの境界把握や分離が困難

OT通信の中身を理解することなく、
セキュリティ機器の設定は困難

生産ラインへの対策導入の例

ITの知識のみでは生産設備のネットワークを
正しくセグメンテーションできない

セキュリティ対策ソフトは
PLCや自動化機器に導入できない

Q OTの特性を考慮して対策適用はできていますか？
（ITの常套手段は通用しない、OT向けに正しく導入・設定できたか）

4-3 対策導入の課題と実施事例(1/2)

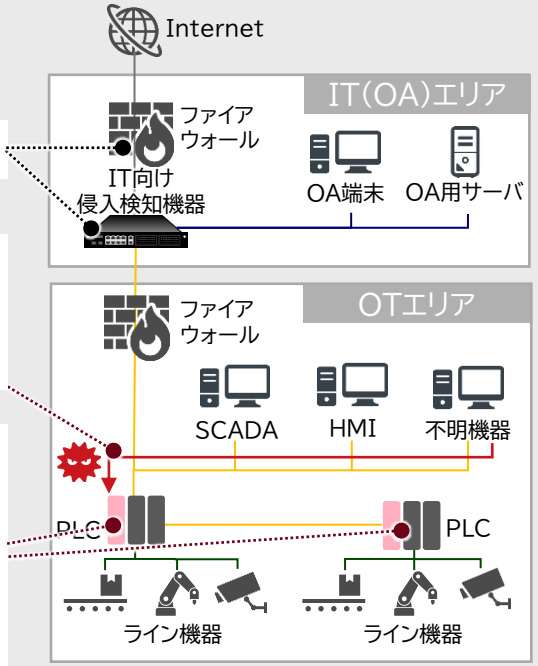
Before

DXのために工場が外部とつながり、
OTエリアのセキュリティの問題が顕在化(下図a、b)

ITセキュリティ対策は実施済み

a. 不審な機器や通信が見抜けず、サイバー攻撃に気付けない

b. サイバー攻撃を受けた時の影響範囲特定が困難なため、全ての解析作業の完了まで全生産ラインを復旧できない



After

これら問題に対して、**生産ラインへ極力影響を与えることなく**
下記A、Bの対策を実施した

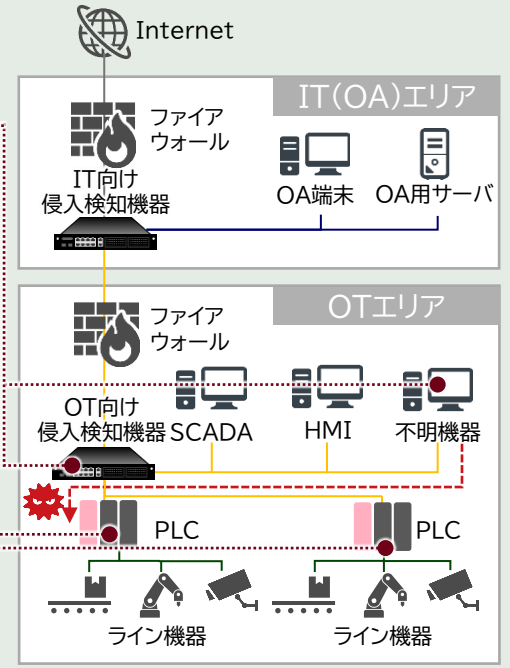
A. OT内の通信や機器を監視し、不審な通信や機器を検知

ITの知見のみで対策すると・・・
→OT内の機器の挙動や通信の内容が理解できず、頻繁に誤検知が挙がる

次頁で詳しく説明

B. サイバー攻撃の影響がない生産ラインを迅速に復旧できるよう、OTネットワークをセグメンテーションして監視

ITの知見のみで対策すると・・・
→適切なセグメンテーションができずインシデント時に迅速に復旧できない



ITの知見だけでなく、OTの知見も合わせることにより
生産ラインへ極力影響を与えることなくセキュリティ対策を講じることが重要

4-4 対策導入の課題と実施事例(2/2)

Before(直面する課題)

A. OT内の通信や機器を監視し、不審な通信や機器を検知

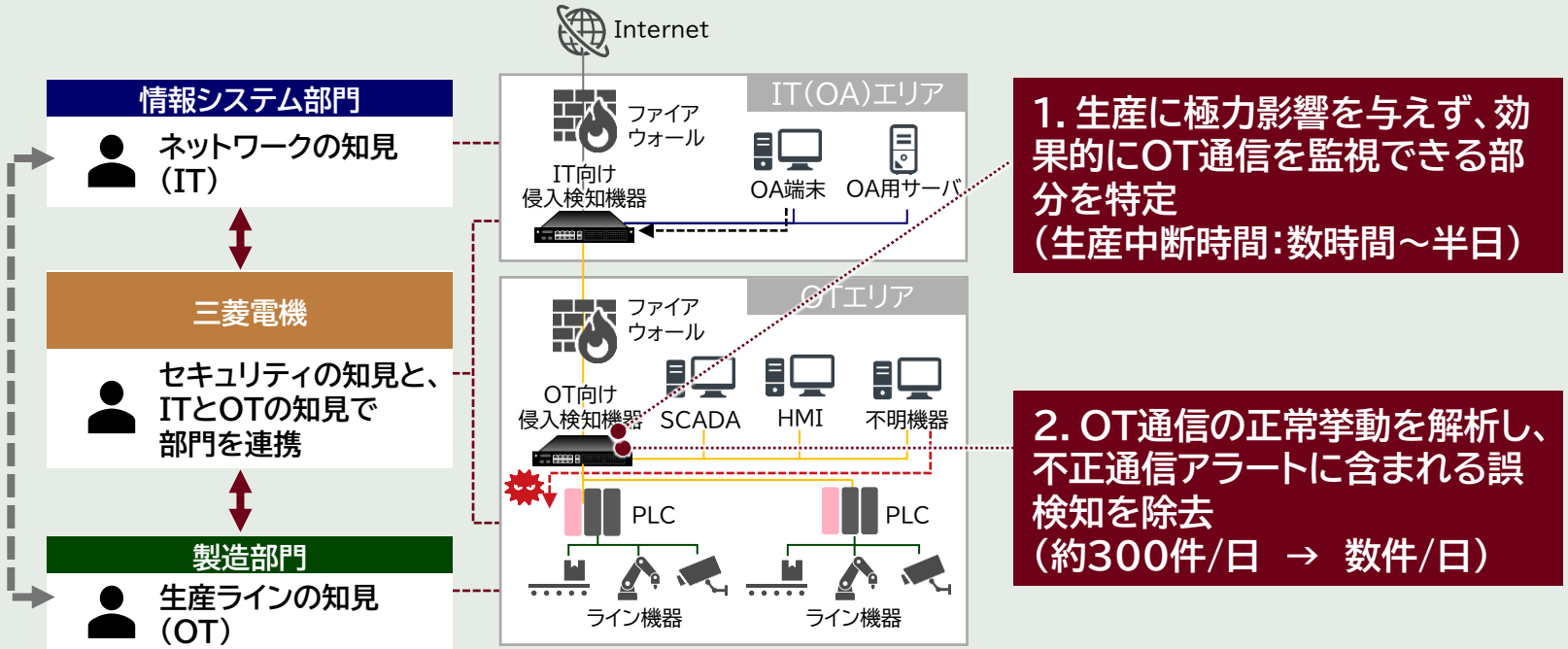
→ OT向け侵入検知機器を導入 

① OTネットワークの全容を把握して設置位置を決めたい
② OT通信プロトコルを理解してチューニングしたい

しかし・・・

①②実施のため部門間連携を試みるが、考え方と技術が違うため会話が困難

After(課題の解決)



1. 生産に極力影響を与えず、効果的にOT通信を監視できる部分を特定
(生産中断時間:数時間～半日)

2. OT通信の正常挙動を解析し、不正通信アラートに含まれる誤検知を除去
(約300件/日 → 数件/日)

OTセキュリティ対策のために情報システム部門、製造部門を取りまとめ、三位一体の知見を合わせて推進・対応していくことで効果的な対策導入を実現可能

4-5 当社での導入事例

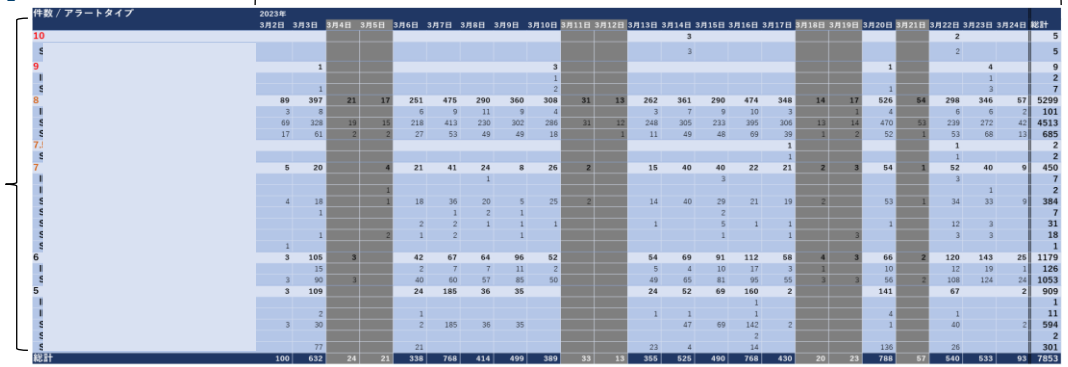
社内工場にIDS(侵入検知機器)を導入してアラートを分析し、2工場について比較しました。

- 一日あたり300件を超えるアラートが発生する工場もある
- 工場によってアラートの種類や検知件数は異なる

社内工場A

日別のアラート検知件数

検知したアラート

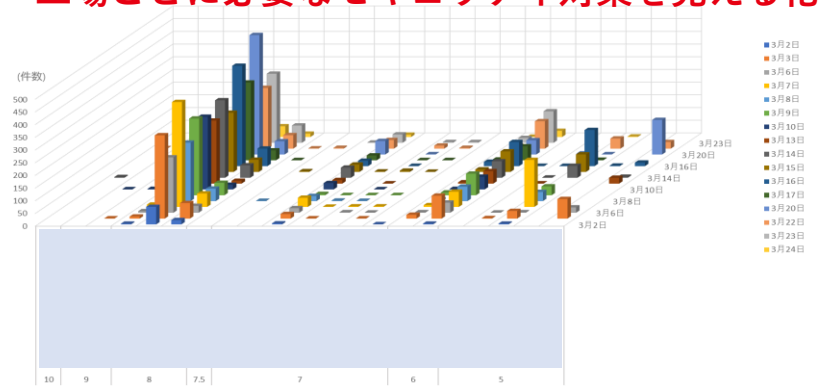


社内工場B

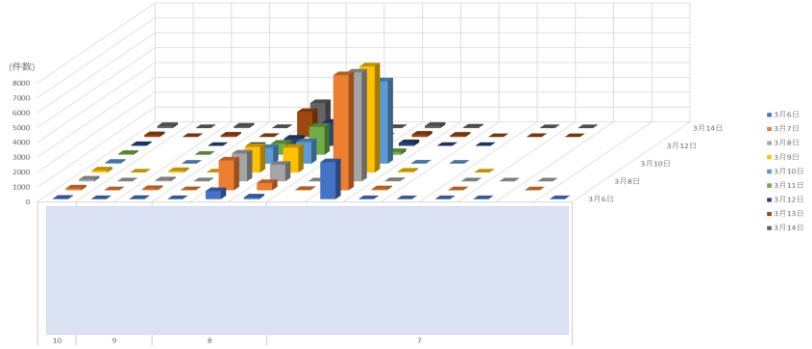
件数 / アラートタイプ	2023年 3月6日	3月7日	3月8日	3月9日	3月10日	3月11日	3月12日	3月13日	3月14日	総計
10	31	128	128	143	61	57	59	128	146	881
[illegible]	31	128	128	143	61	57	59	128	146	881
9	16	91	82	108	1	1	1	107	111	518
[illegible]	3	5	7	6				7	5	33
[illegible]	13	86	75	102	1	1	1	100	106	485
8	668	2509	3007	3417	2511	2626	2054	3126	3448	23366
[illegible]	5	11	10	13	5	4	4	9	11	72
[illegible]	546	2009	1876	1726	1051	749	487	1691	1689	11824
[illegible]	117	489	1121	1678	1455	1873	1563	1426	1748	11470
7	2496	7853	7371	7231	5553	189	194	308	213	31408
[illegible]		28	7	22	4		1	43	13	118
[illegible]	2486	7747	7327	7141	5539	189	190	162	156	30937
[illegible]	5	70	27	62	8		2	96	42	312
[illegible]	1				2		1	1		5
[illegible]	1	7	7	6				5	1	27
[illegible]	2		2					1	1	6
[illegible]		1	1							2
[illegible]	1									1
総計	3211	10581	10588	10899	8126	2873	2308	3669	3918	56173

グラフ化

→工場ごとに必要なセキュリティ対策を見える化



グラフ化



アラートのチューニングと適切な監視運用体制が必要

5-1　さいごに　- 三菱電機の取り組み -

2023年5月 当社IR資料を一部編集

顧客の課題

・現場のIoT化/DXを進めたいがセキュリティが不安
・ITのセキュリティ対策はできているが、OTは不十分/対応方法が不明

当社ソリューション

リスクアセスメントからセキュリティ機器導入、運用・保守までを
ワンストップで提供

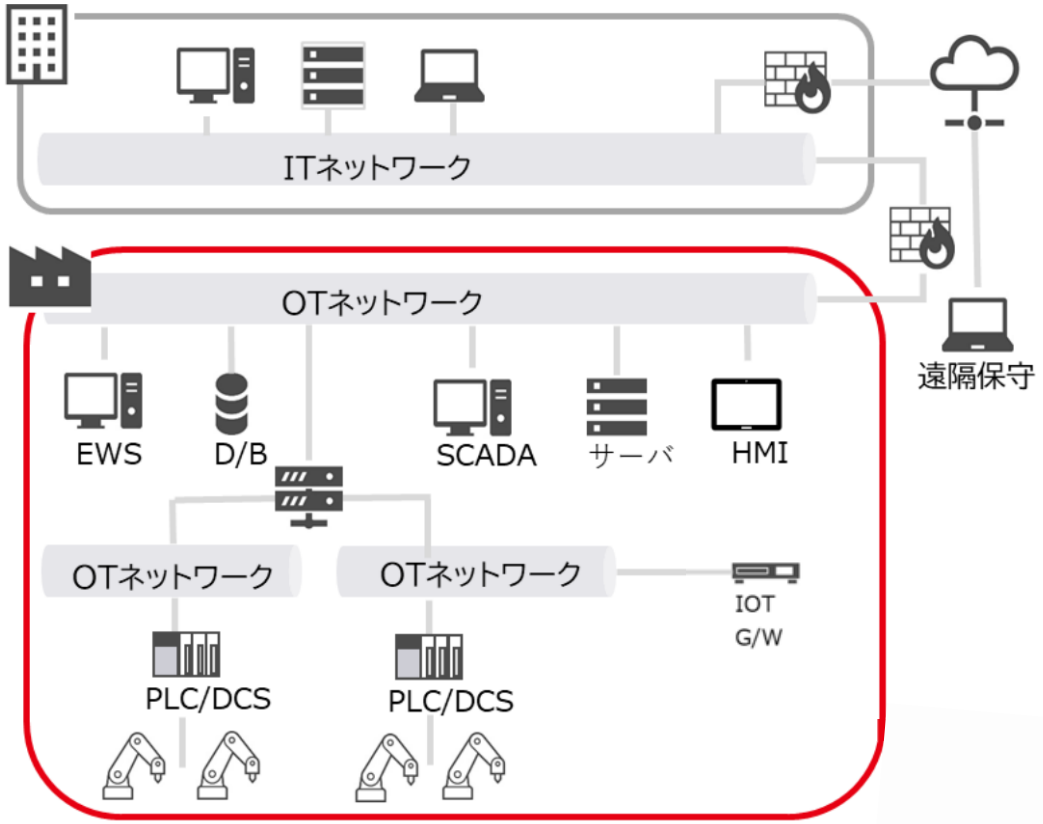
◆ OTとITのデータを組合せて監視・分析強化、OT資産を自動管理
◆ 生産を止めずにセキュリティ対策強化

当社が持つ強み
- OTのリスクアセスメント技術
- セキュアな制御機器、OTネットワークの監視・防御技術
- ITで実績のある24hr/365日のセキュリティ監視サービス

＋

セキュリティベンダの知見
- ファイアウォール
- リモートアクセス　など

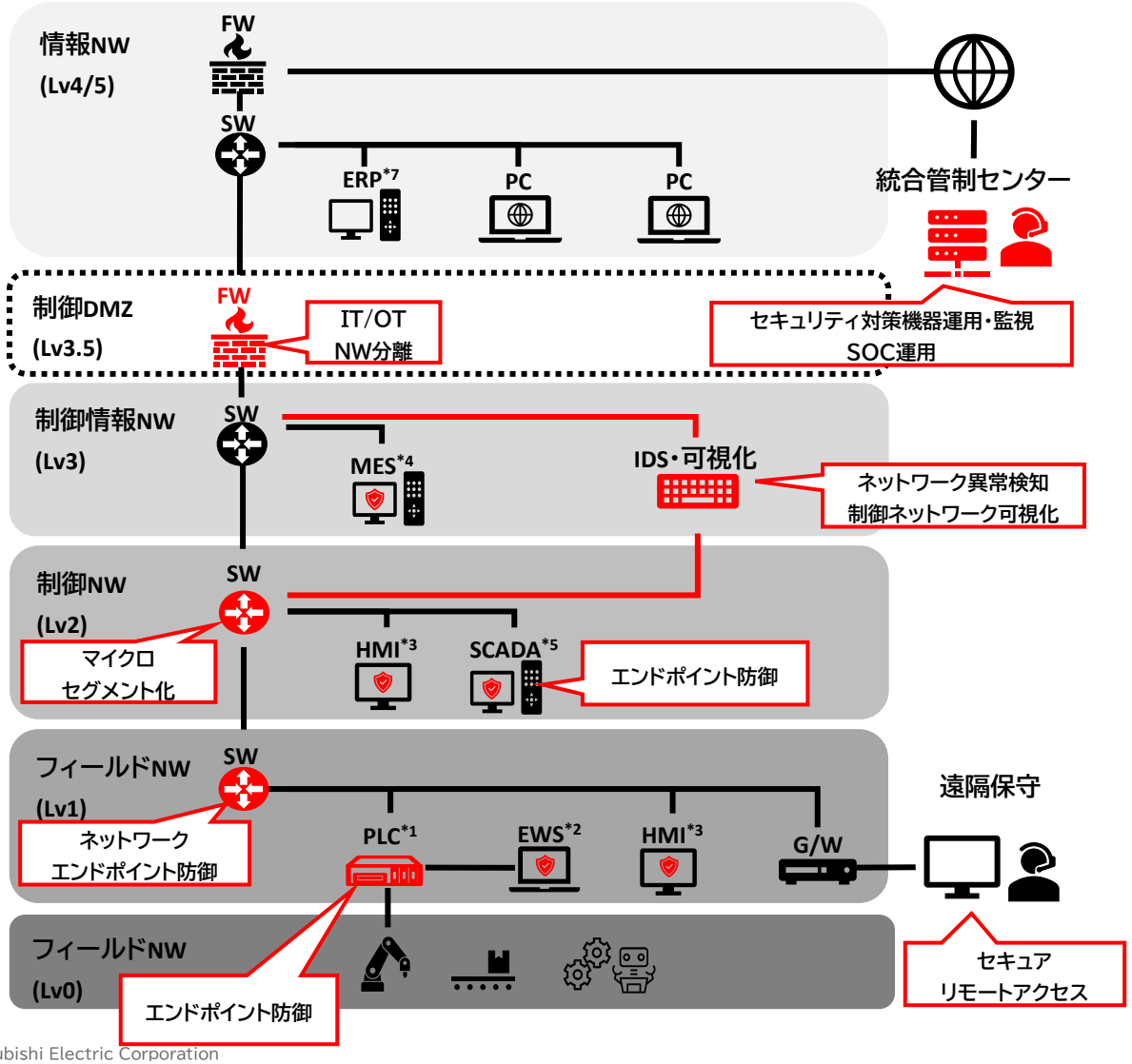
DISPEL　txOne networks　NOZOMI NETWORKS　FORTINET



三菱電機では、パートナー企業様と共にOT資産をセキュアに管理するソリューションをワンストップで提供

5-2 さいごに - 三菱電機の取り組み -

各項目に複数の提案アイテムを保有することで、お客様毎に適した要件(システム環境、機能、組合せ、価格等)にご対応致します。
OTシステムのサイバーセキュリティ対策は三菱電機にお任せください。



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 ■ ネットワーク異常検知・ 制御ネットワーク可視化 ■ 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 ■ セキュリティ対策機器運用・監視 ■ SOC(Security Operation Center) ■ 運用支援(FSIRT)
人材育成	■OTセキュリティ研修

※ 代表的な製品・サービスを記載。今後も新たな製品・サービスをリリース予定

*1: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
*2: EWS (Engineering Workstation): PLCのプログラム開発やシステムおよび機器の構成・保守・診断を行うコンピュータ
*3:HMI (Human Machine Interface): 監視や制御の状態を確認したり、制御したりするための表示装置
*4: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
*5: 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
*6 WMS (Warehouse Management System) :工 場内の入出庫管理など倉庫で行われる業務を管理するシステム
*7: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

6 まとめ

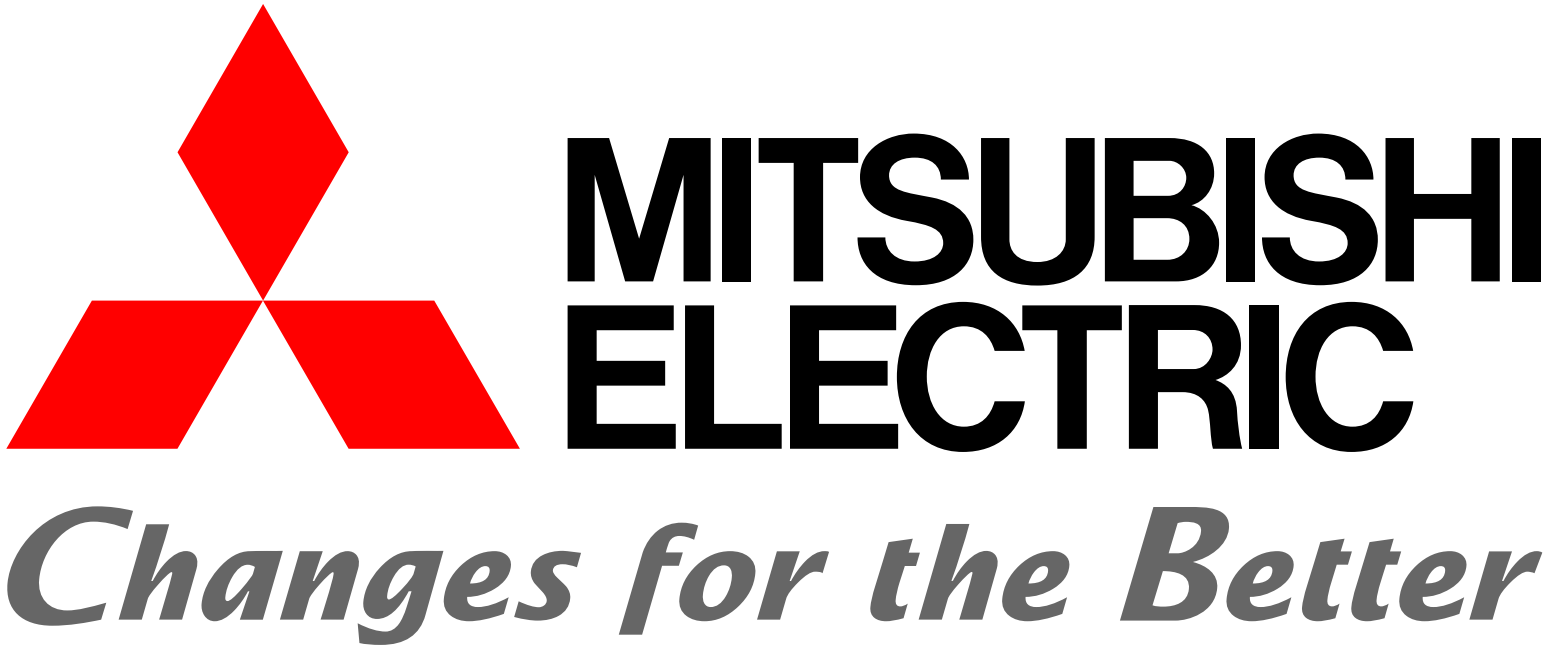
1 製造業DXに伴い
サイバー攻撃のリスクが高まり、
OTセキュリティが重要に

2 ITとOTの知見を用いて
関連部門との密な連携が不可欠

3 アセスメント→対策導入→運用の
一連の流れが重要

4 セキュリティ対策導入にあたっては
OT特有のポイントが存在

**OTセキュリティでお困りの際は、
ITとOTの知見、製造業としての知見も持ち、
トータルでソリューション提供が可能な三菱電機へご相談ください。**


MITSUBISHI
ELECTRIC
Changes for the Better