つながる工場を守る！
OT セキュリティ最前線

東京エレクトロン デバイス株式会社
EC BU クラウドIoTカンパニー
IIoTソリューション部
吉川　義洋

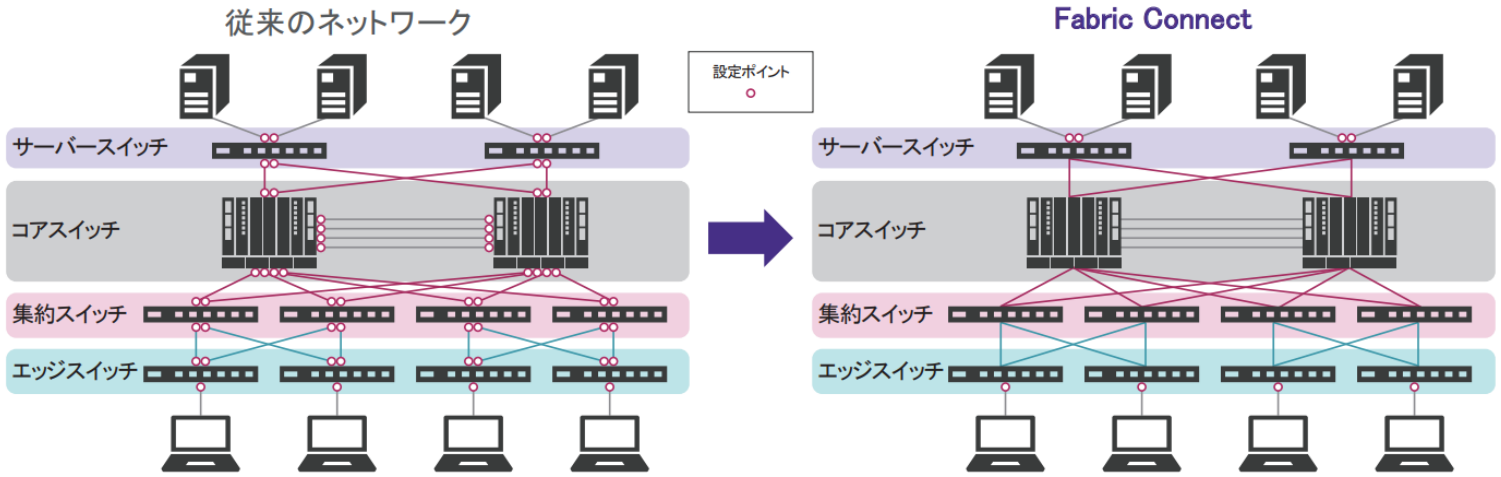
Copyright © Tokyo Electron Device LTD. All Rights Reserved.

Extreme製品特長

特徴

- 高性能かつ低消費電力のAP
- 3rdパーティー製品を含めた有線・無線の統合管理が可能
- 全機能を網羅したシンプルな管理系ライセンス、プール型で自動割り当て、使い回しが可能
- Fabric Connectの技術による柔軟で拡張性のある堅牢なネットワーク構築を実現

Fabric Connect



Fabric Connectとは

ネットワーク末端のスイッチに新たな設定を追加するだけで、
最適な経路と冗長性を確保し、
設定作業の簡略化や人的ミスを削減が可能

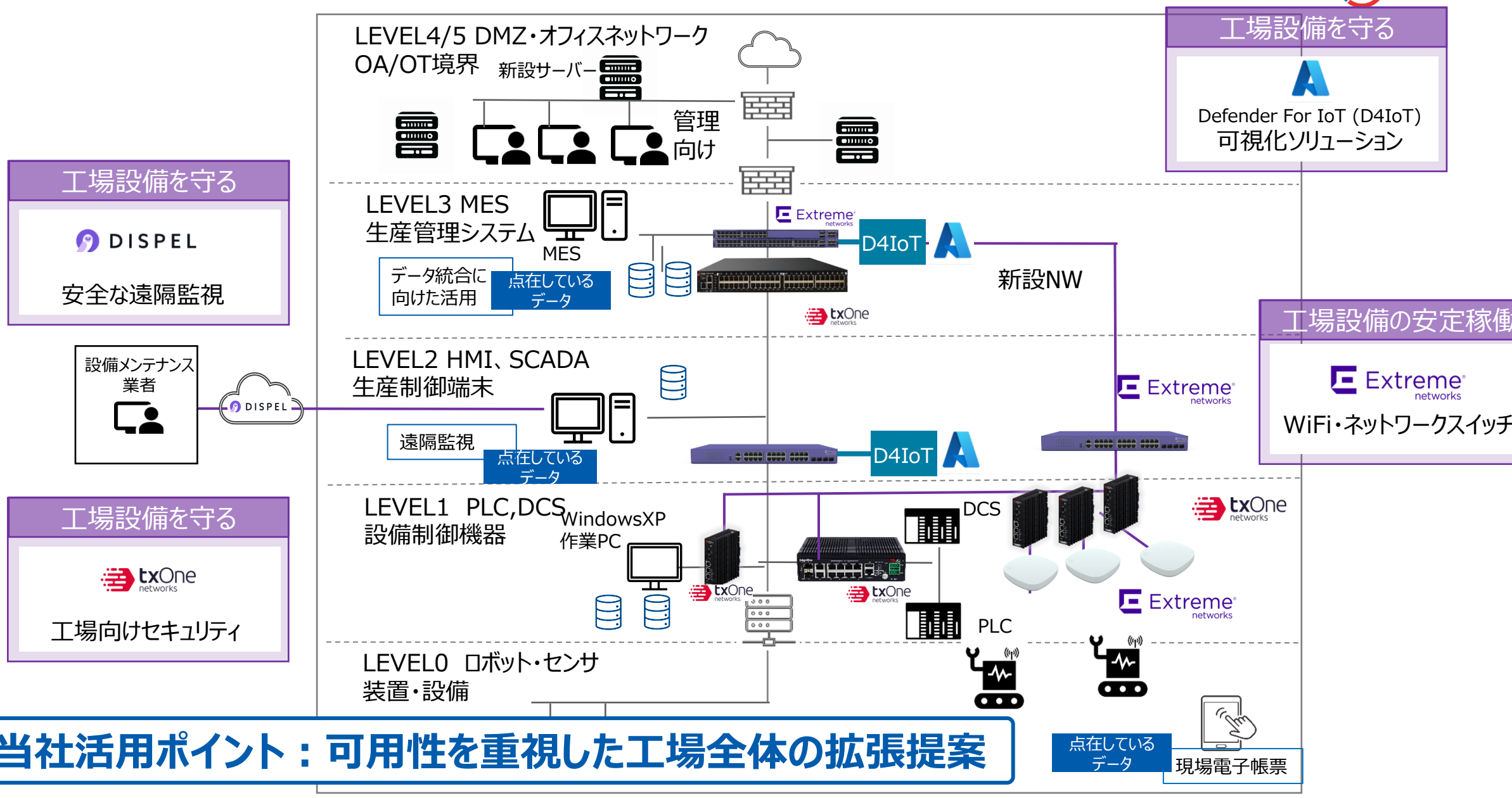
複雑な設定なしに、最適な道でデータを
超高速・安定的に送ることが可能

製造業におけるFabric Connectのメリット

- 一部のNWに障害が発生した際も、他の道を探し、効率的に切り替わるため、生産ラインを止めずに稼働を続けられる
- 生産ラインの変更や、新しい機械を導入する際も、複雑な設定変更なく利用できるため、柔軟に対応ができる

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

DXを推進するための環境整備ソリューション



当社活用ポイント：可用性を重視した工場全体の拡張提案

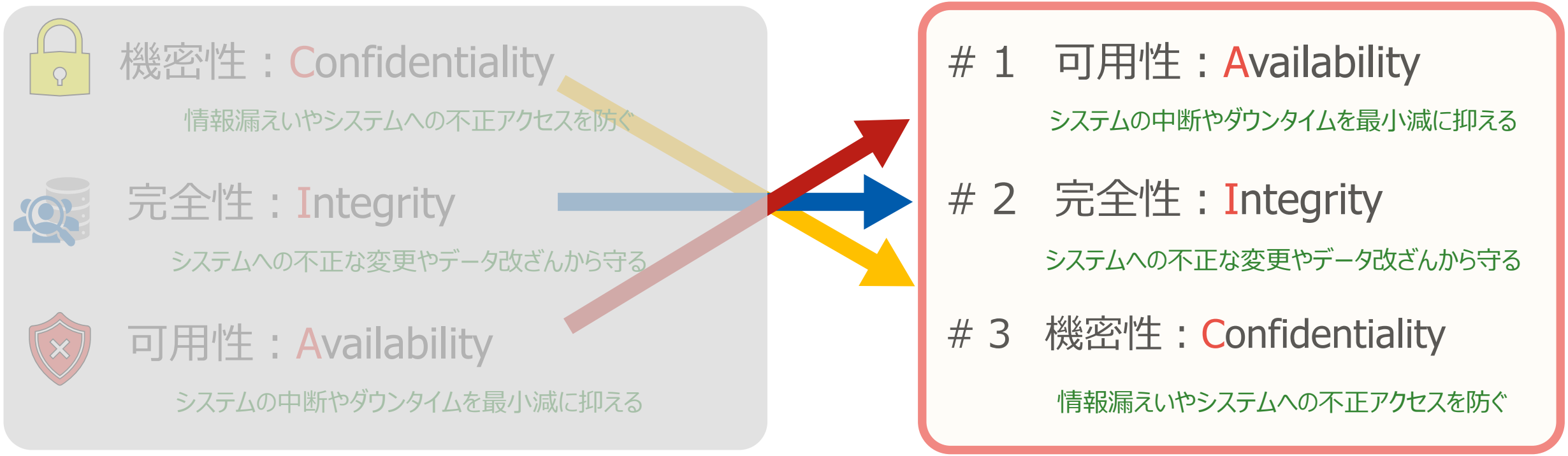
Copyright © Tokyo Electron Device LTD. All Rights Reserved.

東京エレクトロン デバイス

情報セキュリティの3要素の優先度　CIA→AIC

● ITセキュリティとOTセキュリティの違い　：OTでは可用性が最も重要

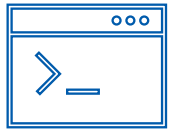
製造ラインやインフラ設備などでは連続稼働（可用性）が最も重要視される。攻撃者視点では、産業用制御システムや物理的な機器自体が対象となり、結果としてシステム停止や最悪の場合は人命に関わるリスクが生じる。システム停止攻撃としては、DDoS（Distributed Denial Service：分散型サービス拒否）攻撃が代表例だが、ランサムウェア攻撃やゼロデイ脆弱性の悪用については、IT・OTの区別なく共通の脅威となり得る。DX化によるITとOTの融合により、OTネットワークへのリスクが増加され、攻撃対象領域（アタックサーフェイス：Attack Surface）が拡大する。



Copyright © Tokyo Electron Device LTD. All Rights Reserved.

工場特有の課題

技術的課題

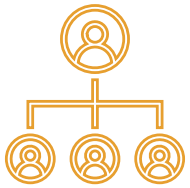


- システムはリアルタイム処理が要求されるため、装置のCPUやメモリに負荷をかけられない
- レガシーOS端末にセキュリティソフトをインストールできない（サポート終了、スペック不足等）
- セキュリティソフトの展開時にシステムや端末の再起動が発生し、生産活動に影響がでる
- ネットワークが適切にセグメンテーションされていない、ネットワーク構成の変更が難しい
- リモートメンテナンスやリモート制御等の外部からの通信のセキュリティ対策が不十分

運用的課題

- ネットワーク構成や資産を把握できていない（クローズド環境も大きく影響）
- 外部業者によるシステムメンテナス時に接続される作業用PCのチェック・管理が不十分
- 計画停止時以外はシステムを停止できない、オンラインアップデートできない
- システムは10~20年の長期利用を前提としており、搭載OSのサポート切れが発生する
- システムにセキュリティソフトウェアをインストールするとメーカーの動作保証外となる

人・組織的課題



- ITシステムは情報システム部門、OTシステムは製造・設備部門の責任範囲となっている
- サイバーセキュリティの専門スキルを有した人材がいない
- 経営層にセキュリティ対策の重要性が理解されず、予算負担部門も不明（コスト意識）
- DXの推進により、幅広い部門がシステム開発・運用を行うためステークホルダが増える

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

まずは現状把握・健康診断から　（セキュリティソリューション導入のステップ）

01 課題ヒアリング

現状とプラン：運用の懸念やシステム変更/拡張の予定　※対象エリア・利用者・資産管理

インシデントなど外的要因：直近のインシデント　サプライチェーン　システムの老朽化　※保護対象

02 現状分析

資産の可視化：保護対象の整理（システム・デバイス・データ）

リスクアセスメント：保護対象の重要度の設定（発生確率×損害額での優先度）

03 対策立案

対策内容の検討：優先度の高い内容から、ネットワーク・デバイス・データのセキュリティ対策/運用を検討

対策時期の検討：対策実施の時期、準備（机上調査＋PoCによる事前の実機検証）

04 実行導入

影響とリカバリー：可用性影響とサプライチェーン考慮、導入直後のシステムトラブルへのリカバリー対応

新規アラート検知：必ず発生する新規アラートへの対応、初期チューニングと対応承認フローの整理

05 運用・保守支援

運用：定期アップデートおよびアラート対応の整理（内部対応・外部委託）

保守：業者保守支援によるインシデント配慮、ヒトとモノのチェック（VPN・持込PC作業・USB利用）

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

まずは現状把握・健康診断から　/　法規制（経済産業省ガイドライン）

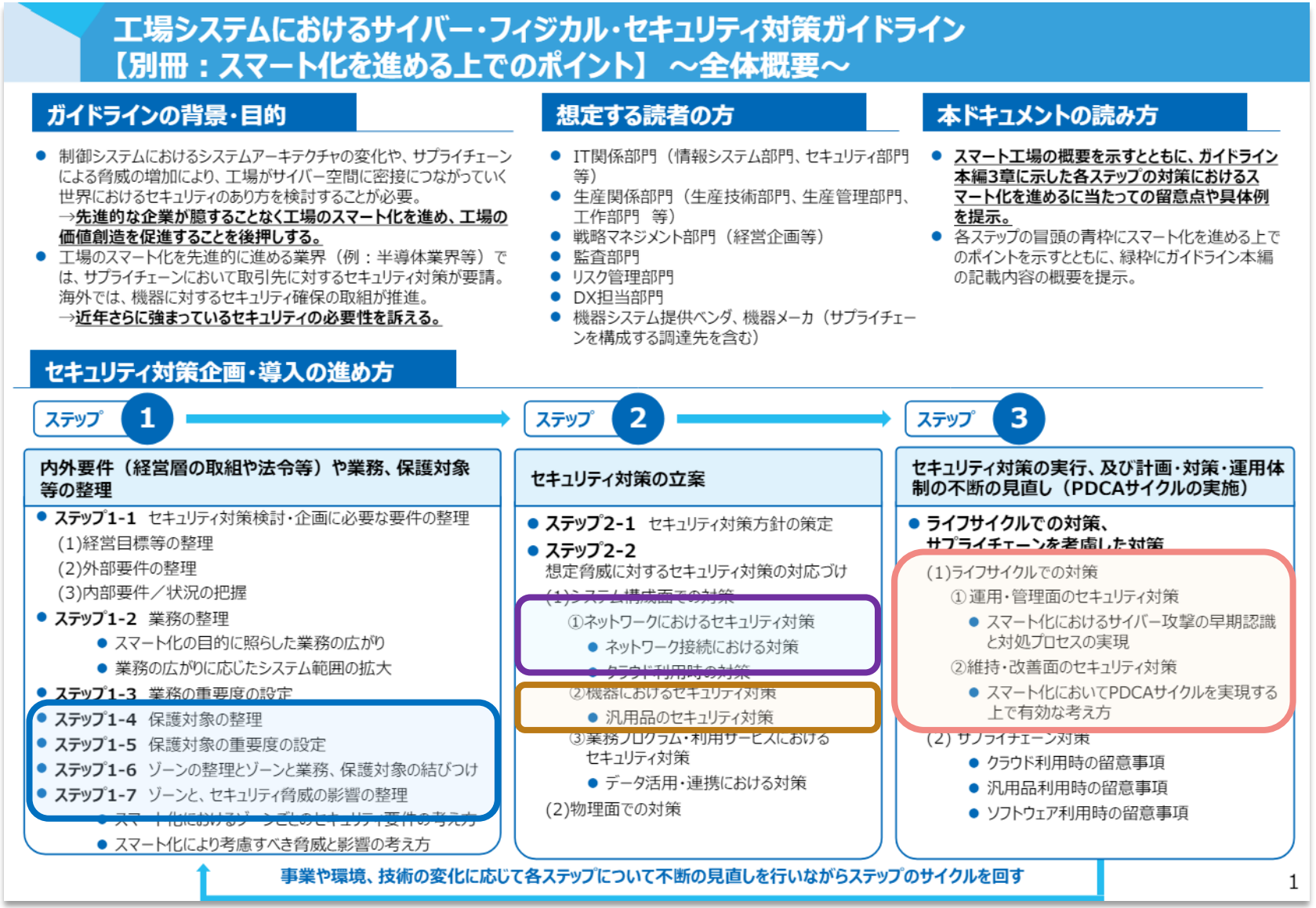
2022年11月：Ver1.0 発行
2024年04月：別冊発行

現状分析（資産・データ可視化）
資産情報（台帳作成）
通信の可視化、リスク優先度判定

ネットワーク対策：産業用IPS、FW
リスクの可視化：産業用IDS、NDR

デバイス対策：産業用AV/許可リスト型

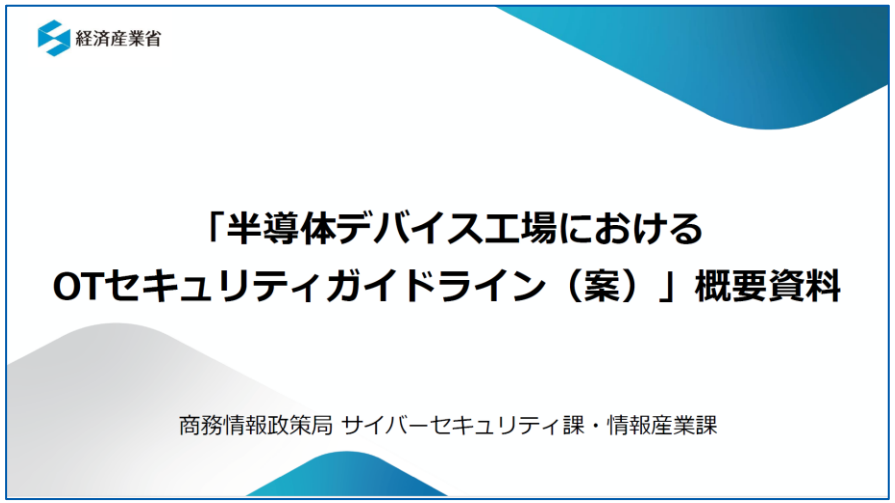
運用、維持改善：PDCAサイクルの実施



引用元：経済産業省　https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_appendix.pdf

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

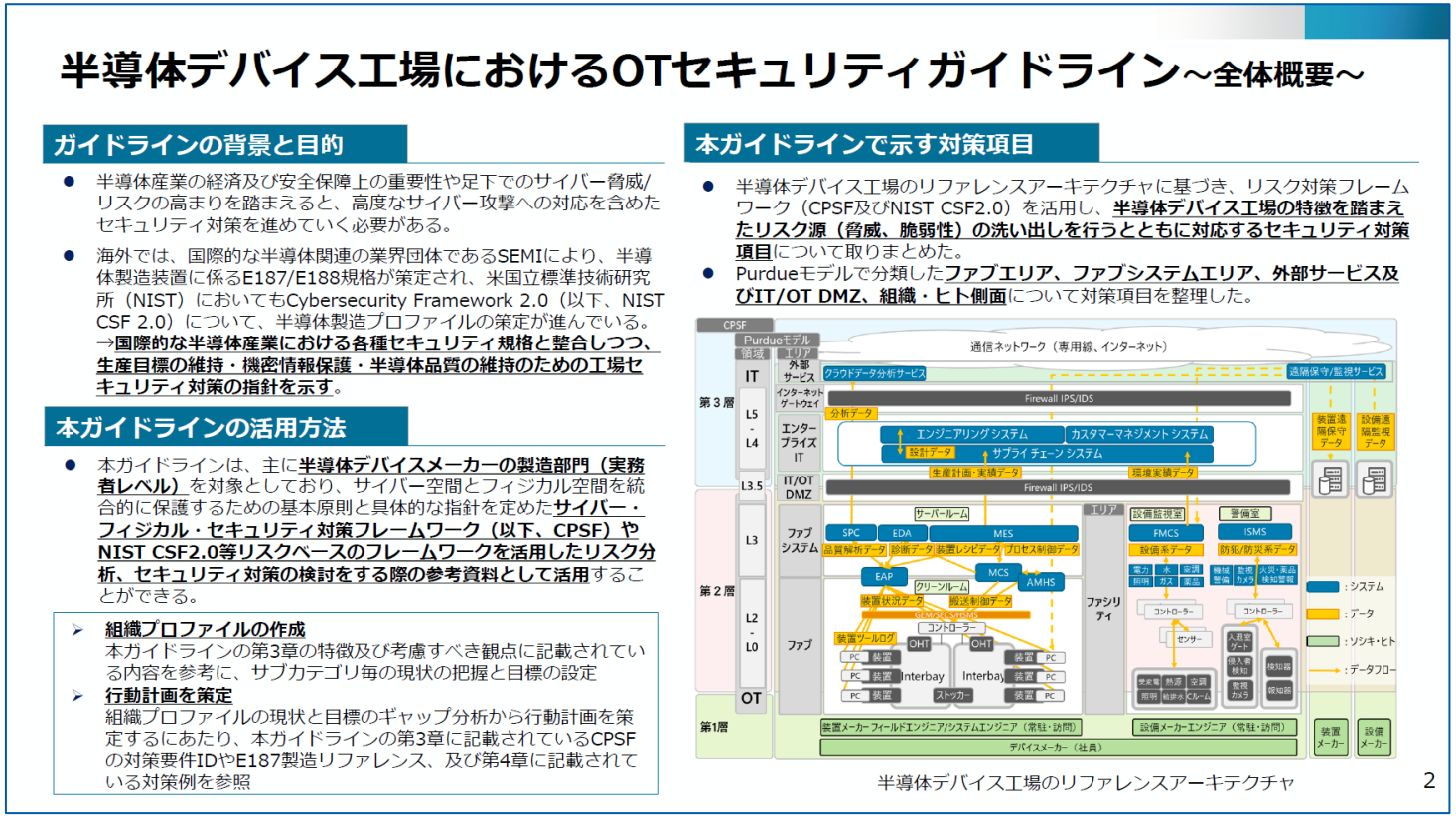
経済産業省：半導体デバイス工場におけるOTセキュリティガイドライン



2025年6月27日：60日間のパブリックコメント開始

- 最も高度な攻撃を想定した対策レベルの指針
- リスクベースのサイバーセキュリティフレームワーク
- NIST CSF2.0、SEMI E187/E188との整合
- 半導体工場の特徴を踏まえたリスクへの対策項目
- Purdueモデルで分類したエリアについての対策
- 組織・ヒト側面についての対策

2022年に公表した「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」は、一般的な工場向けとなっており、**工場の規模が大きく、汎用OSを用いた製造装置の台数が多いなどの特徴を有する半導体工場にはなじまない実態**があり、2024年11月から半導体工場のあり方について議論、国際的な半導体産業における規格に準拠したガンドライン（案）を取りまとめ、**国内外の利害関係者からの意見をいただくパブリックコメントを実施**。



引用元：経済産業省　https://www.meti.go.jp/press/2025/06/20250627009/20250627009.html

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

法規制（経産省ガイドライン、CRA、SEMI/半導体など）

● 半導体セキュリティ規格　：　SEMI規格（Semiconductor Equipment and Materials International　E187/E188）

半導体製造に関して、産業の発展を目指す団体「SEMI（2000社以上が所属）」による、半導体製造装置とその材料の標準化を目的としたガイドライン。各分野ごとにアルファベットで識別（E/装置、M/材料、C/薬液やガスなど）され、2022年にセキュリティ規格としてE187/E188が発行。E187は、Fab装置のサイバーセキュリティ仕様として台湾地区のタスクフォースにて開発され、E188は、マルウェアフリー装置組込みの為の仕様として北米地区のタスクフォースにて開発された。E187が装置開発・導入フェーズのWindows/LinuxOS搭載装置にフォーカスされる。E188では導入・運用・保守フェーズでのマルウェアスキャンや脆弱性チェックを要求している。罰則は無いが、準拠を前提としてビジネスが展開されている。

SEMI初となるサイバーセキュリティ規格を出版

SEMI本部, International Standards, EHS & Sustainability, Senior Director ,James Amano

近年、企業に対するサイバー攻撃が急増しており、半導体業界に影響を及ぼしています。
例えば、2018年にランサムウェアに感染した装置を調査するために、大手ファウンドリーが一時操業の停止を余儀なくされました。
将来起こりうるサイバー攻撃から工場設備を守るために、SEMIは2つの主要なSEMIスタンダード標準化活動を開始し、業界全体の努力の元に次の2つの新しい規格が発表されました。

SEMI E187 - Specification for Cybersecurity of Fab Equipment(ファブ装置のサイバーセキュリティ仕様)
SEMI E188 - Specification for Malware Free Equipment Integration(マルウェアフリー装置組み込みの為の仕様)

	SEMI E187 ファブ装置のサイバーセキュリティ仕様	SEMI E188 マルウエアフリー装置組込みの為の仕様
発効	2022年1月初版(台湾)	2022年2月初版(北米)
対象者	**半導体製造装置サプライヤー** システムインテグレーター	**半導体製造装置サプライヤー** HW&SWコンポーネントサプライヤー **半導体製造装置ユーザー**
目的	半導体製造装置を設計により保護し、運用・保守においてセキュリティ保護をサポートするためのベースラインとして、包括的かつ基本的なサイバーセキュリティの要件を規定	製造設備へのマルウェア伝播を軽減するため、製造装置の納入、設置、サポート活動において求められる情報セキュリティ対策について規定
スコープ	生産設備・マテハン自動化システム・SCADA、PLC は対象外	生産設備・マテハン自動化システム・PLCを含む
推奨実施事項	装置搭載のオペレーティングシステムに関する要求 安全な通信転送プロトコルのサポート ネットワーク構成の技術文書作成 脆弱性の軽減、スキャンの実行 マルウェアスキャンの実行（マルウェアフリー） システムハードニング パッチまたはセキュリティ更新を適用する手順の技術文書の作成 アクセス制御の適用 セキュリティイベントログの管理	＊E188と重複事項 安全な通信転送プロトコルのサポート ネットワーク構成の技術文書作成 脆弱性の軽減、スキャンの実行 マルウェアスキャンの実行（マルウェアフリー） システムハードニング
参照規格	E187 4 Referenced Standards and Documentsより SEMI E169 (Guide for Equipment Information System Security ：機器情報システムセキュリティガイド) E187 11 Related Documentsより IEC規格 IEC 62443-1-1、62443-2-4、及び62443-3-3	E188 12 Related Documentsより SEMI E169 NIST SP800-83 (Guide to Malware Incident　Prevention and Handling： マルウェアによるインシデントの防止と対応のためのガイド)

引用元：SEMI　https://www.semi.org/jp/standards-watch-2022-March/SEMI-publishes-first-cybersecurity-standards

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

法規制（経産省ガイドライン、CRA、SEMI/半導体など）：サプライチェーン

サプライチェーン・サイバーセキュリティ・リスク

「セキュリティの樽」
貯められる水の量は<u>最も短い板に依存</u>する。

- **貯められる水の量**
  ＝サプライチェーン全体のセキュリティレベル
- **板の長さ**
  ＝各企業のセキュリティレベル

サプライチェーンに関わる組織全体の
セキュリティレベルを高めることが重要

12

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

TXOne Networks社 会社概要

情報セキュリティのリーディングカンパニーである“トレンドマイクロ”とOTネットワーク製品のリーディングカンパニーである“Moxa“が産業制御システムを保護するサイバーセキュリティ・ソリューションを共同開発することを目的に2019年に設立したOTセキュリティ専業ベンダーです。

会社名	TXOne Networks Inc.
代表取締役社長 (CEO)	Dr. Terence Liu
本社所在地	台湾（台北）
設立	2019年6月
社員数	400名＋ ※2024年4月

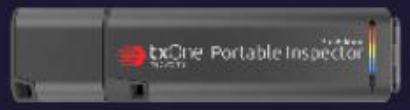
世界の350社を超える大手企業がTXOne Networksの製品を採用
（半導体製造、半導体装置製造、製薬、自動車製造、航空会社など）

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

TXOne Networks社ソリューション

セキュリティ検査

Elementシリーズ



Potable Inspector

ElementOne

Safe Port

インストール不要マルウェア検査
持込メディアのサニタイズ

OTエンドポイント保護

Stellarシリーズ

OT環境に最適化された
エンドポイント保護ソフトウェア

OTネットワーク防御

Edgeシリーズ

EdgeIPS
EdgeFire

EdgeIPS Pro

生産ラインの安定稼働を
支援する産業向けIPS

CPS保護プラットフォーム

SageOne

TXOne製品の統合管理
プラットフォーム

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

東京エレクトロン デバイス

製造工場の課題と対策

レガシーアセット

- **レガシー装置**

多くのレガシーシステムは、セキュリティソリューションのインストールや、更新によるパッチを当てることができない
（サイバー攻撃へ脆弱さ↗）

➢ **レガシー端末にソフトウェアインストール可能エンドポイント対応　Stellarシリーズ**

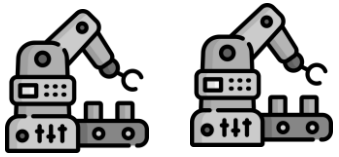

独自性高い
製造ライン

- **独自性の高い製造ライン**

製造ラインの独自性は、セキュリティソリューションのポリシールールのメンテナンスの難易度を上げている
（セキュリティポリシー設定の難易度↗）

➢ **レガシー端末にソフトウェアインストール不可の場合ネットワーク保護（IPS）**

-仮想パッチによるレガシーシステム保護
-オートルールラーニングによる通信リスト化・管理・制御
-セグメンテーション機能によるウイルス蔓延防止


フラットなネットワーク

- **フラットなネットワーク**

フラットなネットワーク構造のため、ウイルス発生時はネットワーク全体にウイルスが拡散するリスクを抱えている
（有事の際の可用性↘）

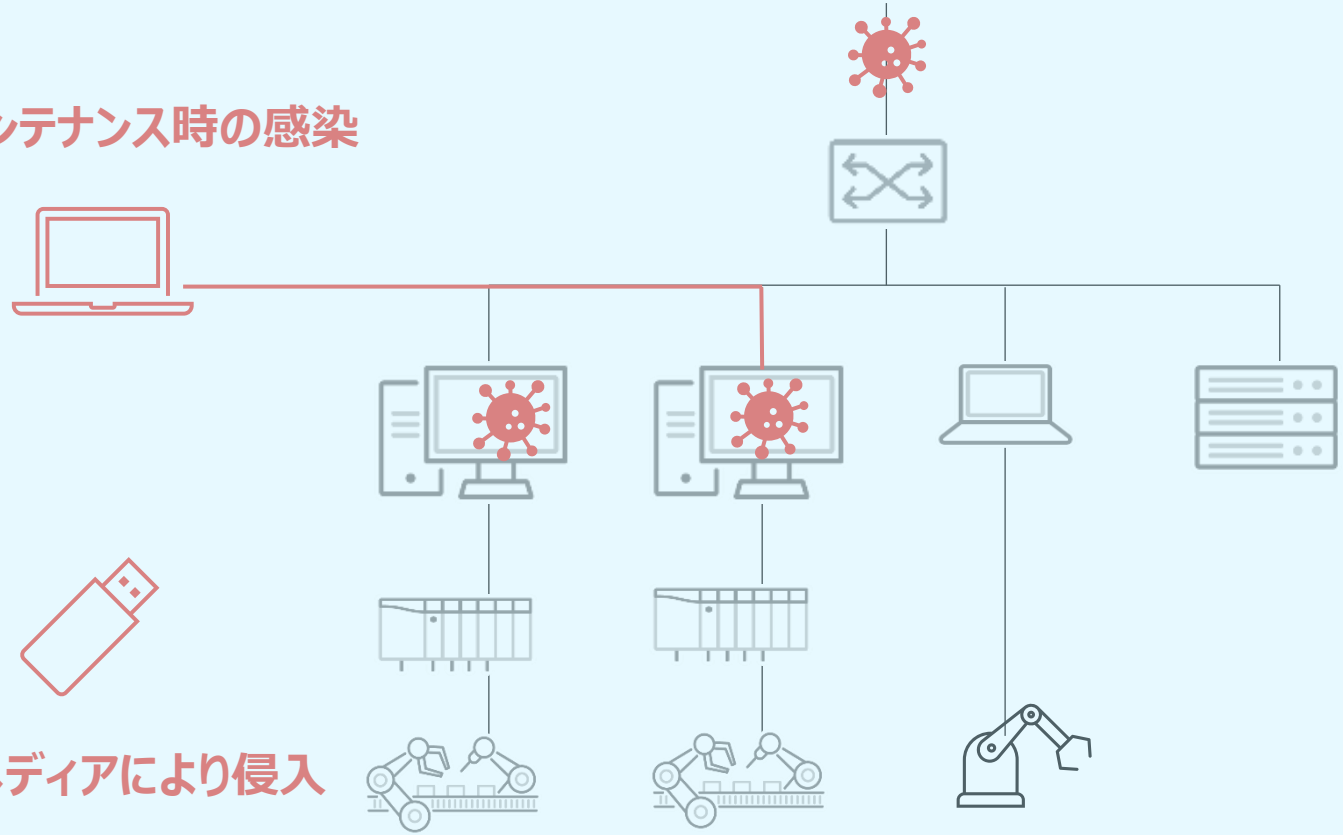
➢ **セキュリティ検査・インシデント対応マルウェア検査・駆除　Elementシリーズ**

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

工場でのインシデント事例

インターネット・イントラネット経由したセキュリティ事故
IT側からの横感染

OTメンテナンス時の感染

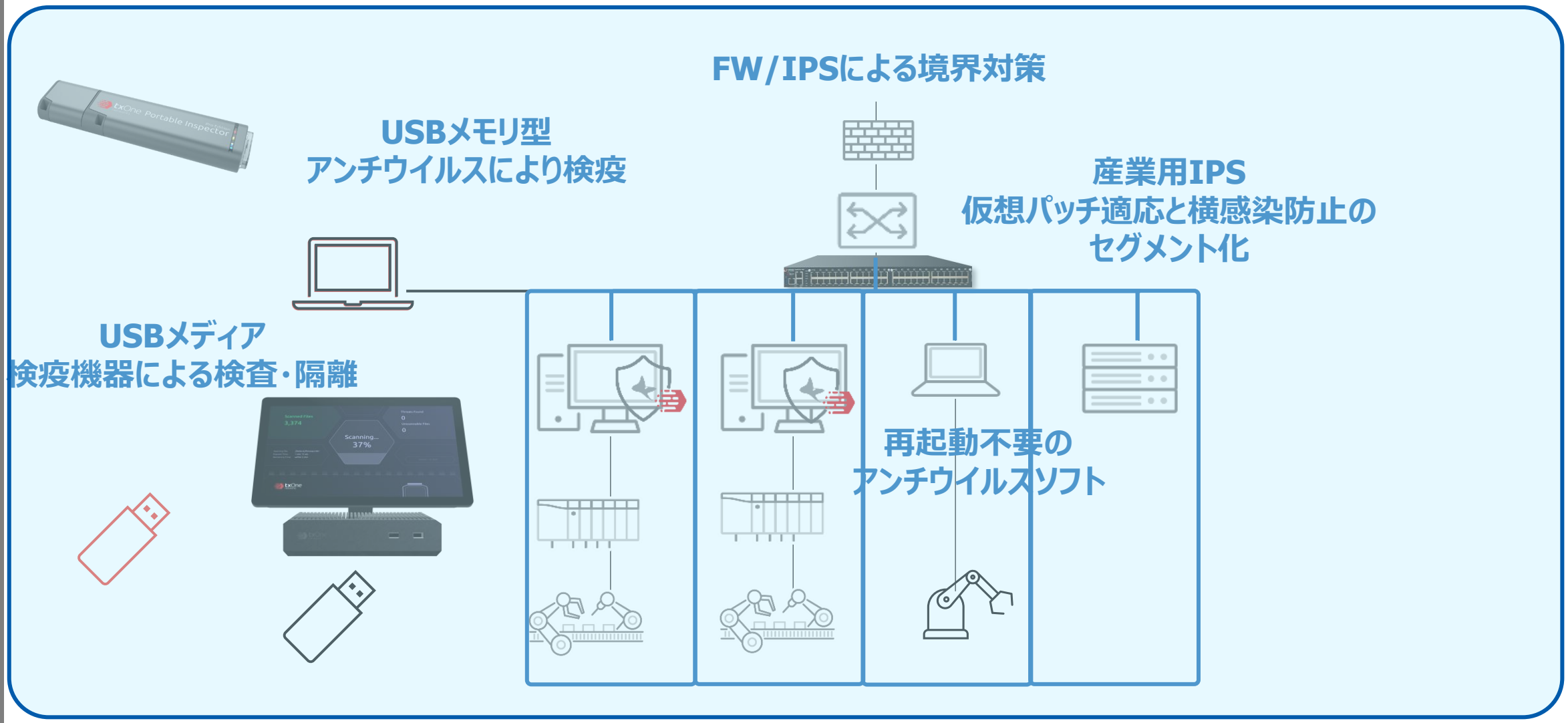


USBメディアにより侵入

制御端末へのアンチウイルスソフトのインストールや、パッチの更新などのサイバーセキュリティ対策が取りにくい

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

工場でよくあるセキュリティ事故の対応例



制御端末へのアンチウイルスソフトのインストールや、パッチの更新などのサイバーセキュリティ対策が取りにくい

Copyright © Tokyo Electron Device LTD. All Rights Reserved.

当社活用の利点

01 業界動向と工場セキュリティ

半導体関連・各種業界への提案

半導体業界に求められる要件を理解した
サービス・セキュリティ製品の提供

02 OT向けオリジナルサービス

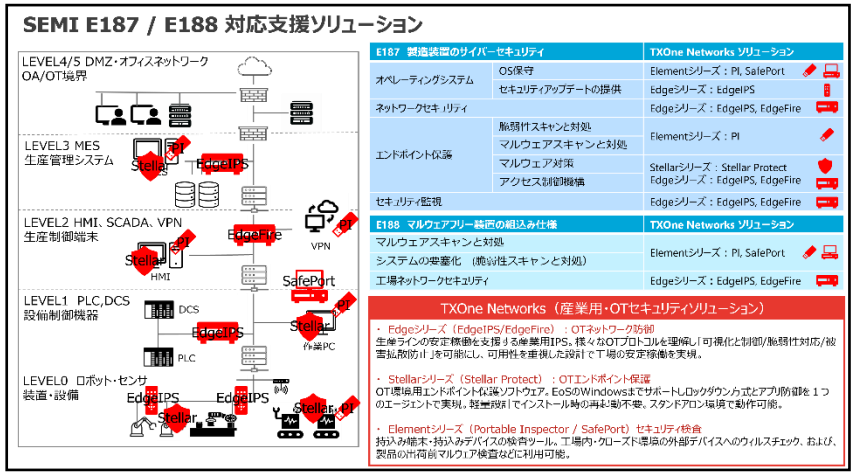
導入実績に基づくサービス展開

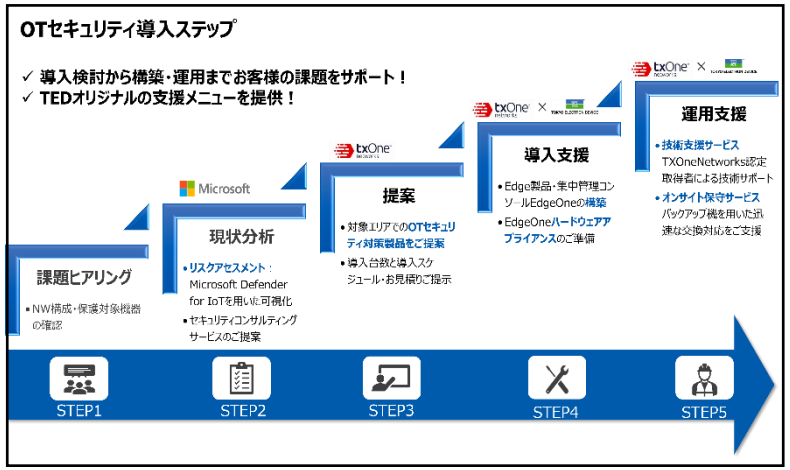
半導体工場を含むEdge製品の国内導入
販売実績3000台以上
導入実績に基づく、当社オリジナルの導入・保守
サービスの提供

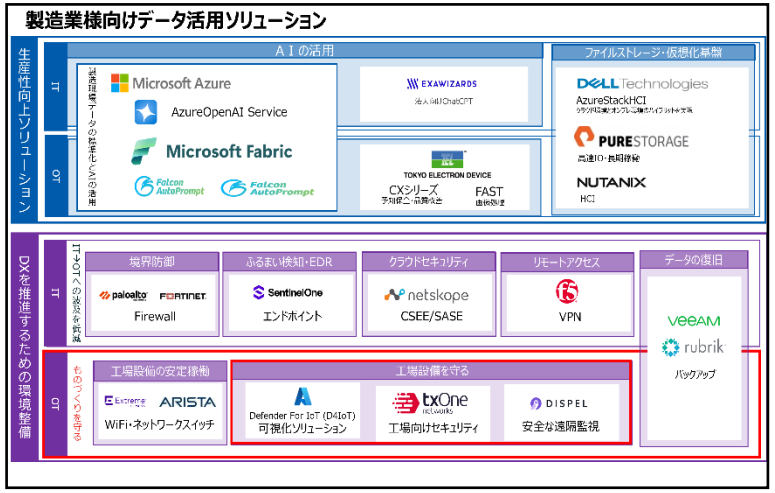
03 製造業向けDX支援

デバイス保護からクラウドサービスまで

レガシー機器対応から生成AI活用まで
製造業DXにおける推進支援



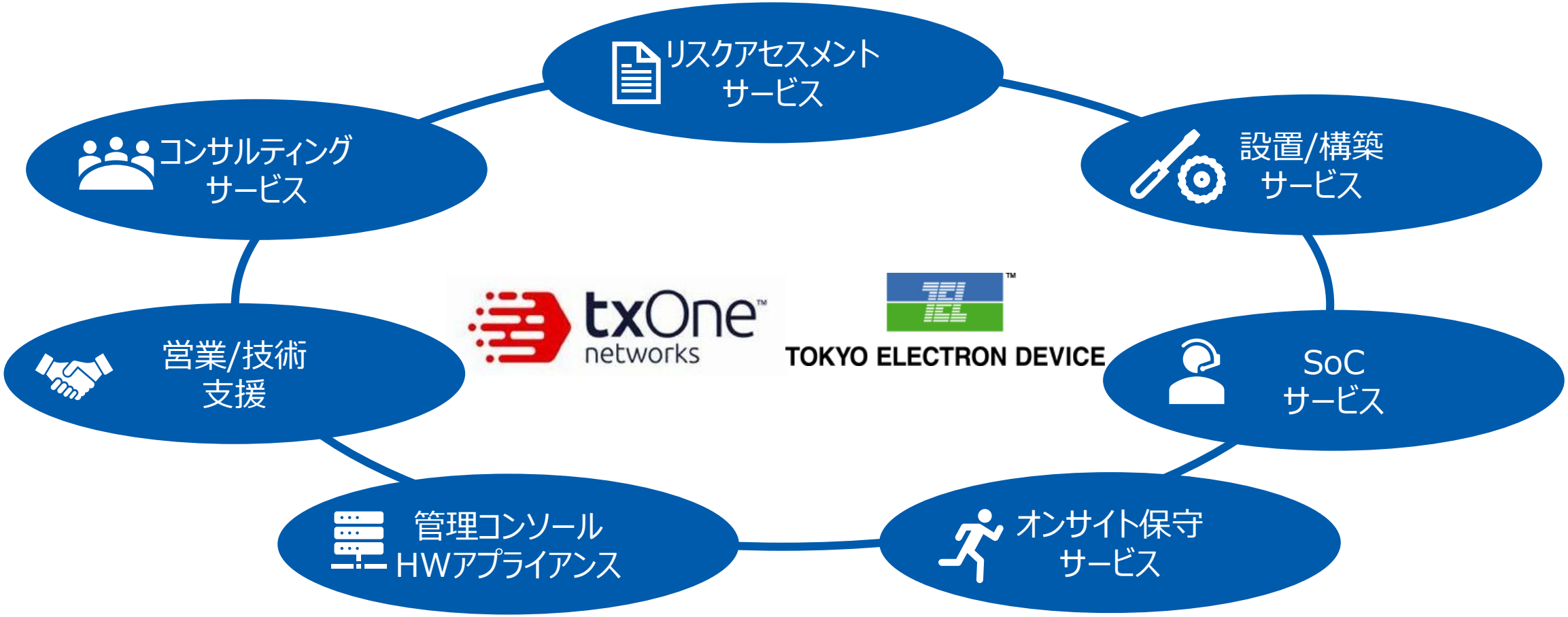




Copyright © Tokyo Electron Device LTD. All Rights Reserved.

東京エレクトロンデバイス　OTトータルソリューション

- 東京エレクトロンデバイスは、OTセキュリティのトータルソリューションプロバイダーを目指し、TXOne Networks製品をフルサポートし安心してご採用頂き、早期導入頂けるよう、各種サービスを提供致します。



Copyright © Tokyo Electron Device LTD. All Rights Reserved.