txOne networks

The Leader of OT Zero Trust

半導体産業セキュリティ対策事例

TXOne Networks Japan合同会社

業務執行役員 マーケティング本部長　今野 尊之

2025年12月10日

半導体産業におけるサイバーセキュリティの進化・発展

半導体製造工場は、重要な国家インフラとして位置付けられ、その複雑さと自動化はますます高度化

業界の教訓:
ファブエリアのみならず、装置メーカーを含めたサプライチェーン全体のセキュリティレベル向上が急務

半導体業界連携の強化:
SEMIを中心とした業界コミュニティの形成が進み、TSMCが議長を務める台湾半導体サイバーセキュリティ委員会が発足

SEMICON WESTにおいて、TSMCがグローバルビジョンを提示:
SEMIと連携し、サプライヤーを含めた半導体エコシステム全体でサイバーセキュリティ強化の推進を宣言

経産省 産業サイバーセキュリティ研究会 WG1 半導体SWG発足:
半導体関連産業（デバイスメーカー、装置メーカー、素材メーカーなど）が参画し、サイバーセキュリティのあり方、守るべき対象、具体的な対策等を議論する場として発足

TSMCのランサムウェア被害:
WannaCryの亜種が台湾のTSMC工場の生産を妨げ、操業を停止させた。80%の復旧に3日かかり、損失は2018年第3四半期時点で約8,400万ドルに達した。感染はサプライヤーの侵害されたツールに起因することが判明した。

Fabにおける資産導入時の対策強化 (Inside-out Approach):
1. 運用環境のセキュリティ確保
2. 導入装置・機器の検査
3. サプライチェーンのサイバーセキュリティ強化

SEMI E187 発行:
SEMI E187（ファブ設備のサイバーセキュリティ仕様）は、半導体装置のセキュリティ要件を定め、世界中のファブにおける主要な調達基準として発行

半導体製造サイバーセキュリティコンソーシアム（SMCC）発足
サプライチェーンのサイバーレジリエンスの向上、フレームワークの統一、サイバーレジリエンス法（CRA）を含む国際的な規制動向への対応を目的としたグローバルな連携体として設立。

基本コンセプト：Inside-out Approach (3 STEP)

① Fab内部システムの保護
② サプライチェーンからの脅威を保護（導入装置・機器の検査）
③ サプライチェーン全体のセキュリティ強化

1

Fab内部システムの保護

内部システム保護、セグメンテーション、エンドポイントセキュリティ

2

サプライチェーンからの脅威を保護

すべての導入機器および可搬型デバイスの厳格な検査

3

サプライチェーン全体のセキュリティ強化

サプライヤーに対し、セキュリティアンケート、脆弱性スキャンの実施を徹底。

Inside → Outside

txOne networks

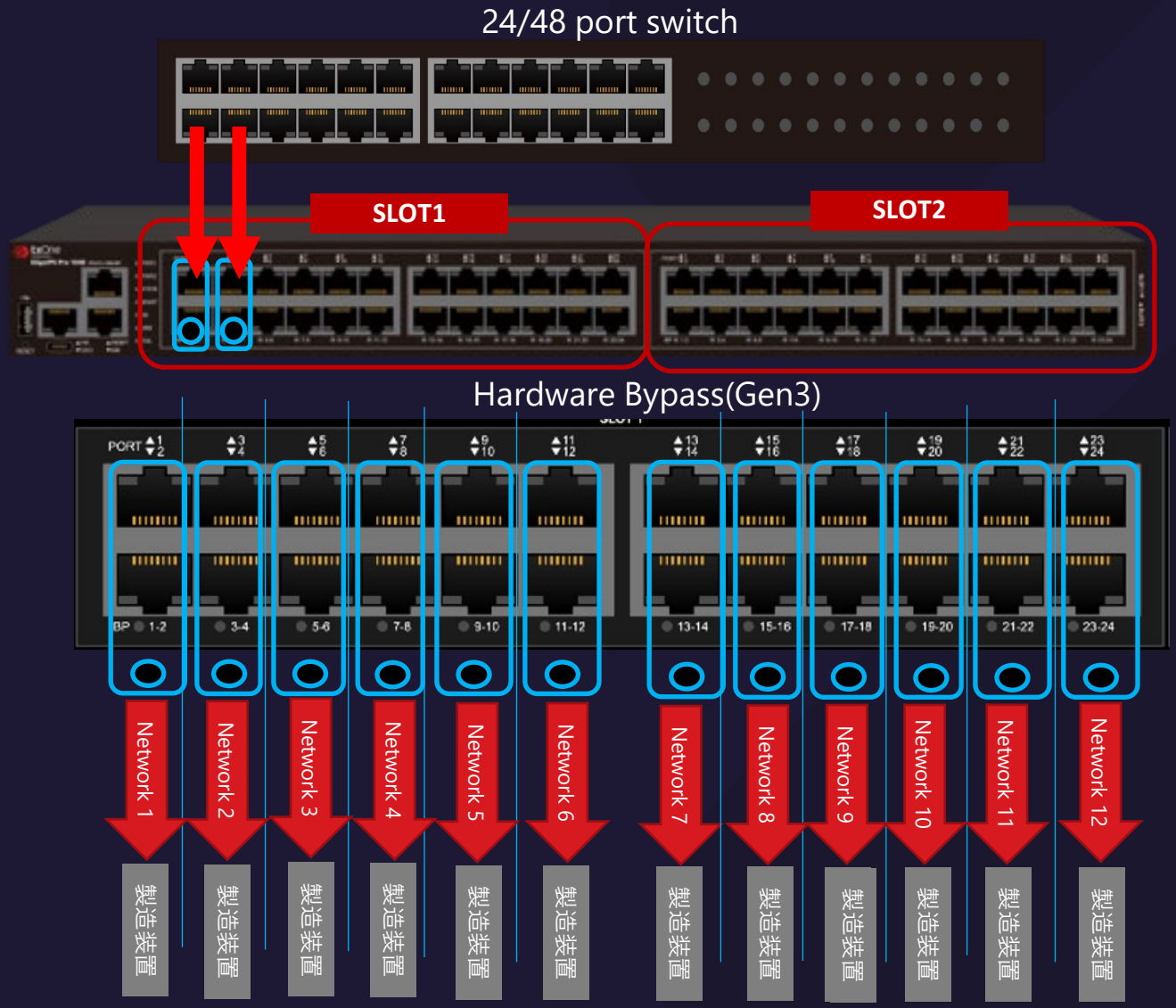
① Fab内部システムの保護

ネットワークソリューションの事例

数千台規模かつ連続稼働が求められる資産を集約的に保護

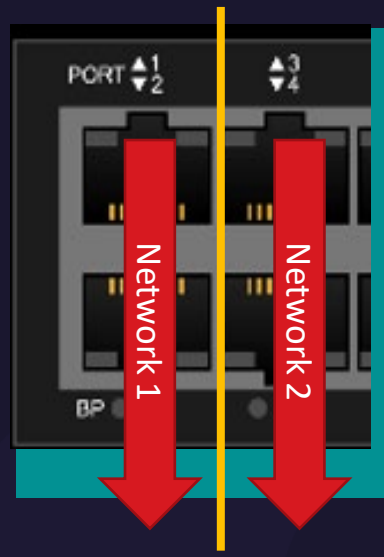
生産管理システム
MES
ERP
EAP
SPC
FDC/APC
FAB DC ZONE
24Ports Edge Switch
24Ports Edge Switch
24Ports Edge Switch
24Ports Edge Switch
データ分析システム
EDA
MCS
(OHT/AGV)
搬送制御システム
EdgeIPS Pro
マイクロセグメンテーション
マイクロセグメンテーション
マイクロセグメンテーション
マイクロセグメンテーション
SECS/GEM
SECS/GEM
SECS/GEM
SECS/GEM
Tool #1
Tool #2
Tool #n
Tool #11
Tool #22
Tool #2n
Tool #31
Tool #32
Tool #3n
Tool #41
Tool #42
Tool #4n
ウイルス対策
脆弱性対策（仮想パッチ）
ウイルス対策
脆弱性対策（仮想パッチ）
ウイルス対策
脆弱性対策（仮想パッチ）
ウイルス対策
脆弱性対策（仮想パッチ）
Photo
Etch
(Diff)
(Thin)

ポート単位で異なるセキュリティポリシーを適用可能



半導体製造工場に求められるネットワークセキュリティ要件

- 高可用性
- 高スループット・低遅延
- フェイルセーフ機能
- レガシーシステムの保護
- ネットワーク可視性（SEMIトラフィック：SECS/GEM, Interface-A)
- マルウェア・脆弱性対策
- 標準的なAPIサポート



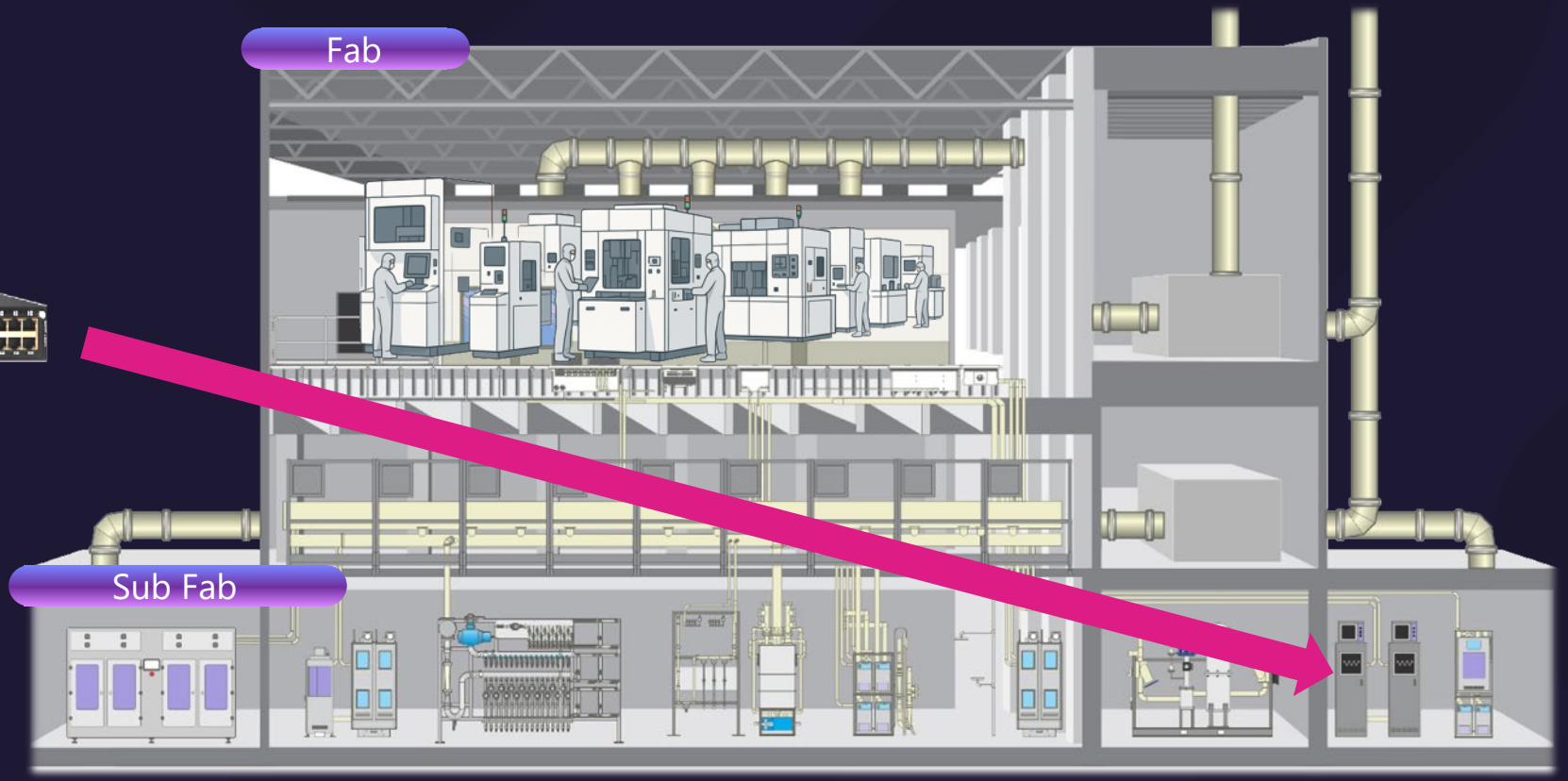
Isolated（分離）

- 各ポートペアに対し、1台の製造装置を接続し、物理的に分離
- 各ポートペアごとに独立したポリシー設定やHWバイパスの有効/無効の設定が可能
- 仮想パッチによる脆弱性保護

ネットワークソリューション展開例 ①　（Sub Fabへ設置）

- OT向けIPSをSub Fabに直接設置することで、サーバールームを必要とせず、スペース効率の高い展開が可能
- Fabクリーンルームに入退出する手間と工数を削減（クリーンスーツ着用、エアシャワー通過、持込制限など）
- 特にスペースに制約のある工場環境において、配線等が集約されているSub Fabで効率的な設置・運用が可能

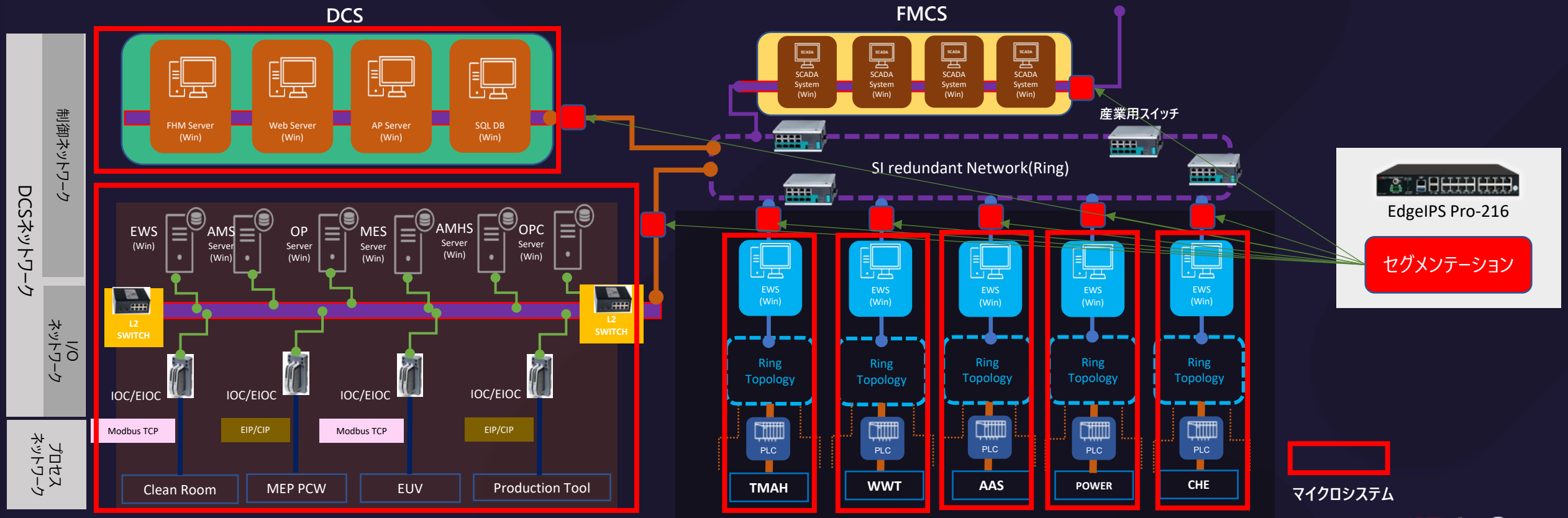
EdgeIPS Pro



Sub Fab：Fabの生産活動を支える各種インフラ装置（真空ポンプ、除外装置、化学薬品供給システム等）が設置されるエリア

ネットワークソリューション展開例 ②　（FMCSのセキュリティ）

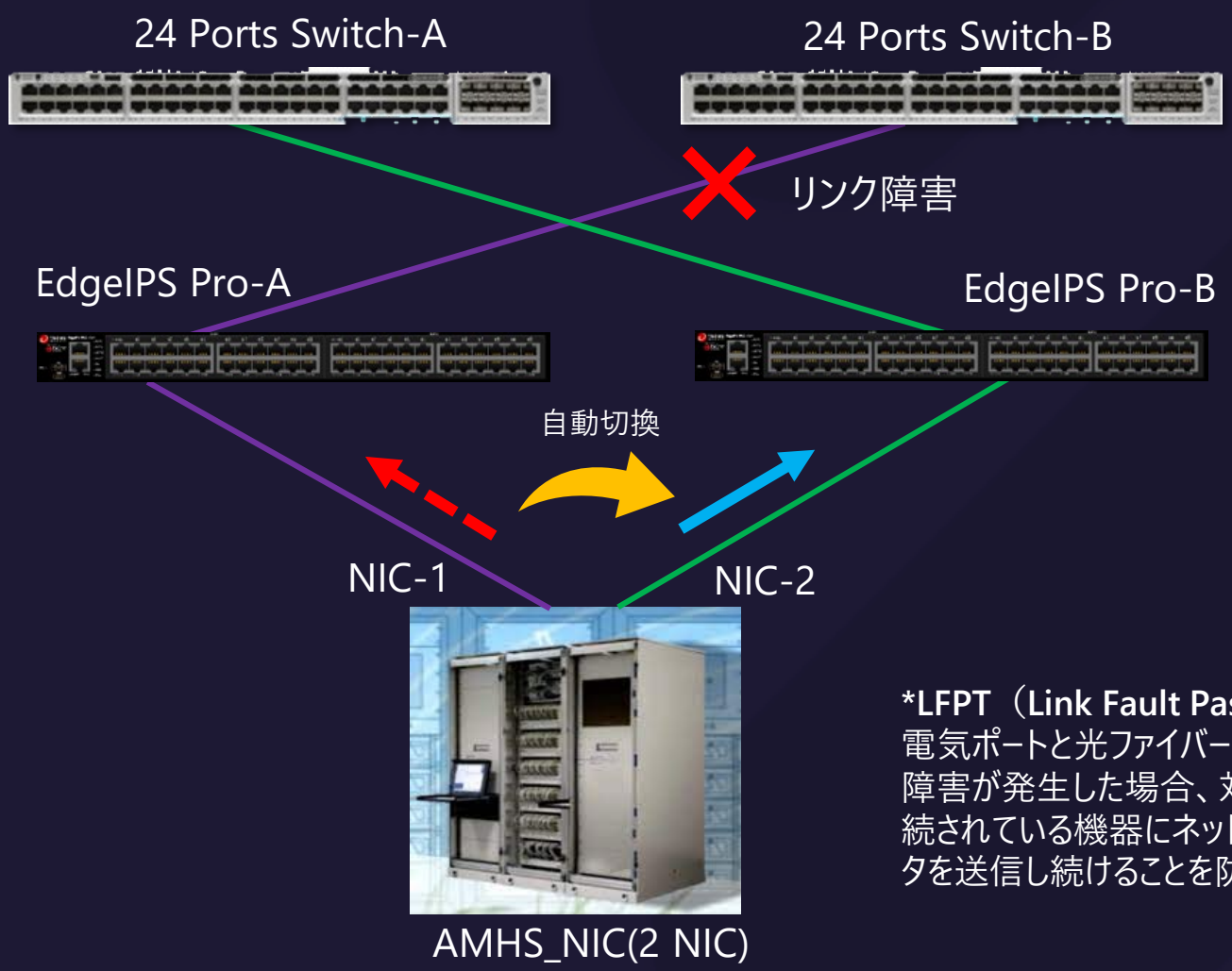
- 分散制御システム（DCS）ネットワークは、独自ネットワークとマイクロネットワークで構成される複合ネットワークに分割される。
- マイクロネットワークは信頼性の高い通信経路を確保するために、リングトポロジーに接続するノードネットワークで構成されている。
- このネットワーク構成において、産業用IPSを各入力トラフィックノードに設置し、FMCS内のマイクロシステムをセグメンテーションすると同時に、DCSネットワークを独立した制御ゾーンとして分割することにより、責任分界点を明確にし、障害発生時の対応を効率化します。



FMCS (Facility Monitoring and Control System)：電力、給排水、空調等の生産設備を一元的に監視･制御するシステム

ネットワークソリューション展開例 ③ （AMHSのセキュリティ）

AMHS（Automated Material Handling System）自動搬送システム



- 半導体製造は連続稼働が求められ、AMHSの停止は即ライン停止・歩留まり悪化につながるため、システムの冗長性は必須要件となる。
- セキュリティを確保しつつ、ネットワークの冗長化を実現するために、EdgeIPSはデュアルウェイLFPT*をサポート
- ネットワークインターフェースの片側が故障した場合、システムは迅速にもう片側のインターフェースに切り替え、最小限の障害で超低遅延のネットワーク接続を実現します。

***LFPT（Link Fault Pass Through）**
電気ポートと光ファイバーポートの接続状態を同時に監視し、いずれか一方の電気ポートに障害が発生した場合、対向側の電気ポートを自動的にシャットダウンします。これにより、接続されている機器にネットワーク異常を即座に通知でき、通信が途絶えた経路に対してデータを送信し続けることを防ぎます。

① Fab内部システムの保護

エンドポイント保護の事例

半導体製造工場のエンドポイント保護の課題

マルウェア対策

FAB環境においてマルウェア感染を阻止できず、Conficker(Downad)のような古いウイルスも依然として蔓延

＜主な感染源＞
- VMイメージ
- 新規導入資産
- USBメモリ
- メンテナンス作業者
- IT部門からの感染拡大

レガシーシステム

依然として多数のレガシーシステムが現役で稼働しており、脆弱な状態

- 更新やパッチ適用が受けられない
- 低スペックのコンピュータが多い
- 回復力と復旧能力が限定的
- 監視とログ記録の機能が不十分

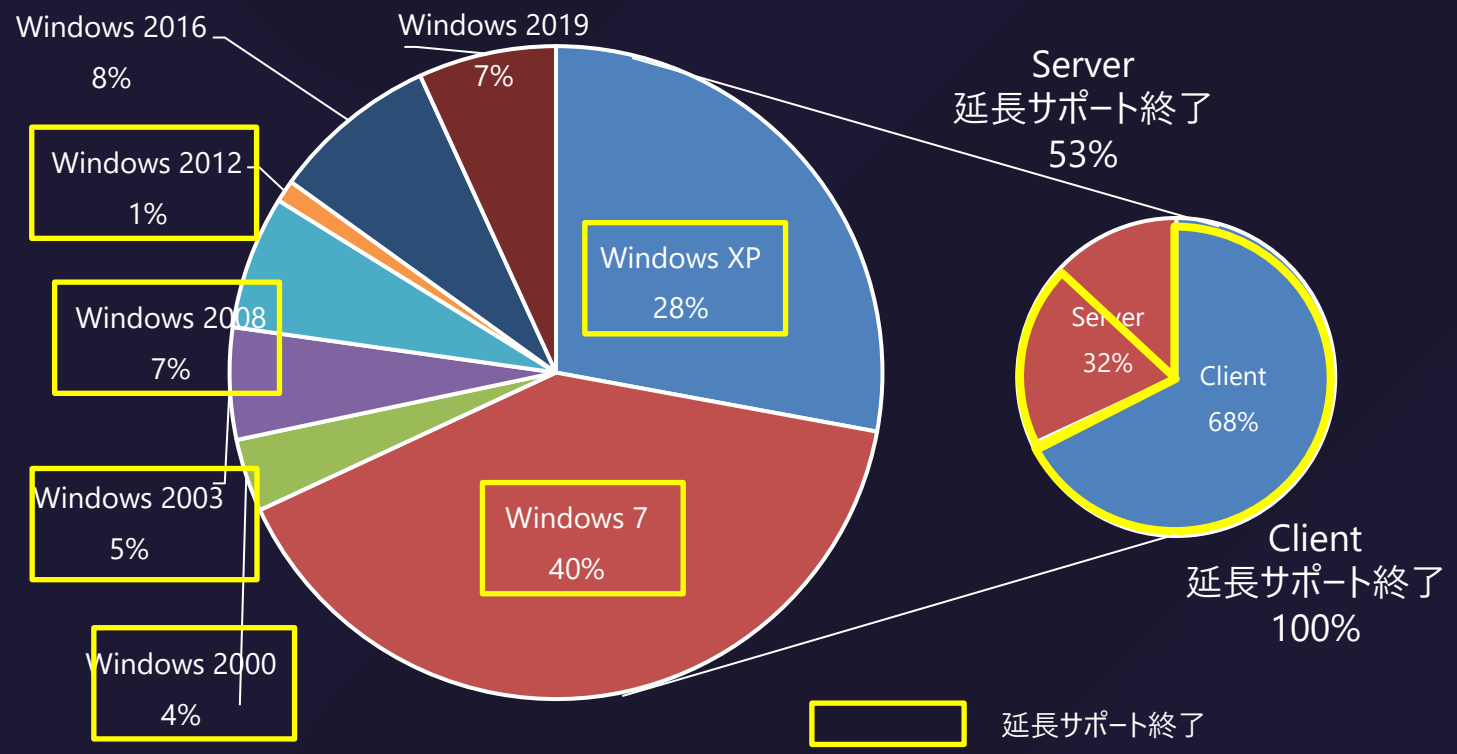
運用・管理の負荷

複数ベンダーのエンドポイント保護ソリューションの運用・管理のエフォート

- 新システムとレガシーシステムが混在する環境への対応
- 異なる環境や資産へ画一的なポリシー適用が困難
- セキュリティインシデント対応における全体的な視点が欠如

現役で稼働するレガシーOS

半導体製造工場で稼働するデバイスの約8割が延長サポート終了OSで稼働

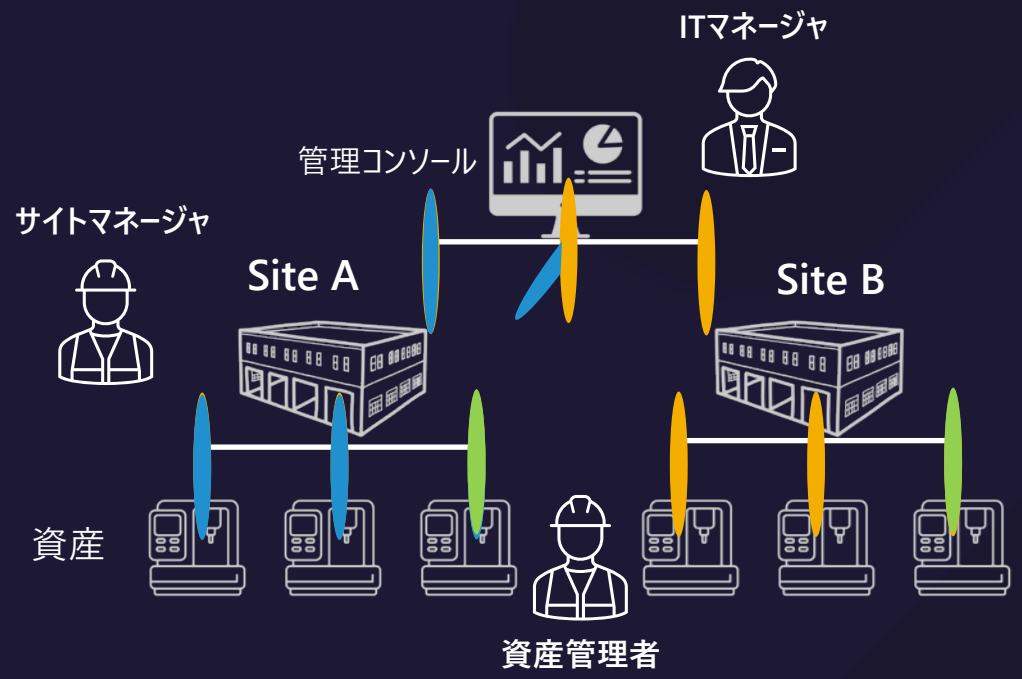


半導体製造A社：Windows端末 約5万台（TXOne調べ）

半導体製造工場のエンドポイント保護で学んだこと

- OT環境のエンドポイント保護として「ホワイトリスト型」を採用するケースがあるが、半導体製造工場のように近代的なツールでは、頻繁な更新や変更を必要とするため、ホワイトリストの維持・管理の負荷が課題となる。
- レガシーシステムと最新のシステムが混在した環境において、ホワイトリスト型、アンチウイルス、EDRなど、環境に適合したソリューションを検討・採用する必要がある。
- 各サイト間、資産の環境や要件が異なるため、画一的なポリシー展開が困難
- ウエハ製造工程において、IT向けアンチウイルス製品からOT向けエンドポイント対策製品に変更したことによりウエハの処理効率を2倍に改善。
  - ✓ IT向けアンチウイルス製品の平均CPU使用率10%前後に対し、OT向けエンドポイント対策製品の平均CPU使用率は1%未満

セキュリティポリシーと定義ファイル更新のレイヤー管理



現場からの要望

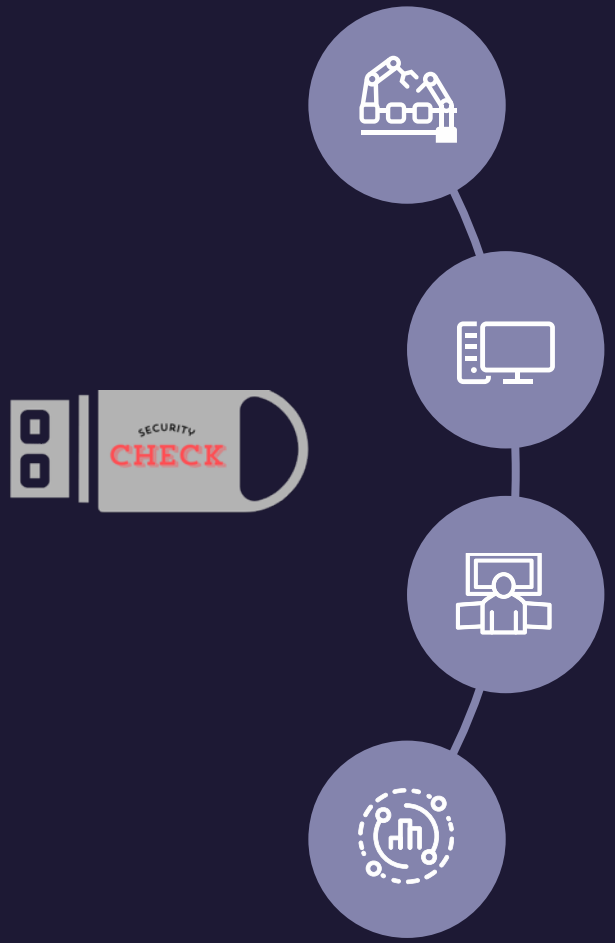
- ポリシーを大規模に一斉展開したい
- サイト間のポリシー適用に柔軟性を持たせたい
- 資産レベルでポリシー適用に柔軟性を持たせたい

1. ITマネージャー：グローバルポリシーを展開し、デフォルトですべての資産と拠点に適用
2. サイトマネージャ：各サイトの要件に合わせてグローバルポリシーを調整
3. 資産管理者：必要に応じてローカルポリシーを設定変更する権利を保持

② サプライチェーンからの脅威を保護

装置・機器導入時の検査の事例

導入装置・機器の検査ポイント



マルウェア検査

- 新たに導入する装置・機器にマルウェアが潜んでいないか検査

資産管理の向上

- OSバージョン、脆弱性、パッチと更新プログラム、有効なサービス、潜在的な攻撃対象領域等の情報を収集
- これらの情報をCMDB（構成管理データベース）にアップロードし、今後の追跡に活用

内部システム

- 多くの装置は内部に複数のサブシステムを有しており、すべてを検査する必要がある

People, Process, and Technology

- 装置の導入プロセスとして確立することが重要

対策事例：製造装置の納品前セキュリティ検査（SEMI E187対応）

装置納品時にマルウェアフリーを証明する必要がある。

Before

1. 装置に一時的にAVソフトをインストール
2. 装置をマルウェアスキャン
3. マルウェアスキャン結果をスクリーンショットで保存
4. 装置のAVソフトをアンインストール
5. システムの完全性検査と性能調整を実施

After

- インストール不要のセキュリティ検査ツールでマルウェアスキャン
- スキャン結果を自動でレポート出力
- 装置のAVソフトのインストール/アンインストール作業が不要
- スキャン実施後のシステム完全性検査や性能調整が不要

可搬型記憶装置のセキュリティ検査

1 可搬型記憶装置をマルウェア検査

2 管理コンソールに検査結果を集約

3 検査ログをSIEMに送信

マルウェア検査専用機

- 外付けハードディスク
- USBメモリ
- SDカード

ラベルプリンター

2 マルウェアフリーのラベルを印刷し、可搬型記憶装置に貼り付け

3 工場環境での利用を許可

③ サプライチェーン全体のセキュリティ強化

TSMCの調達要件にセキュリティ規格(SEMI E 187）を適用

TSMC Strengthens "Specification for Cybersecurity of Semiconductor Equipment", Realizing Mutual Industry Benefits

TSMC has Upgraded the Security of its Factories by Requiring New Equipment to Comply with the Standards through Procurement Contracts, Strengthening the Cybersecurity Defense of its Supply Chain

2023/09/14

Leon Chang　Jill Wang

TSMC is dedicated to fulfilling the commitments of its "Information Security Declaration". In response to the Company's development toward smart manufacturing, TSMC has initiated and promoted the global security standard "Specification for Cybersecurity of Fab Equipment" (SEMI E187) to enhance the cybersecurity of the semiconductor supply chain. In 2023, it was included as a tool procurement specification and verification mechanism, and established to ensure that suppliers comply with the standard before the introduction of any new equipment. Additionally, to accelerate the integration and networking efficiency of the entire factory system, TSMC has collaborated with the Semiconductor Equipment and Materials International Organization (SEMI) to define the "Cybersecurity Reference Architecture for Semiconductor Manufacturing Environment". This was first released at the SEMICON Taiwan international semiconductor exhibition in September and will be launched online in October. The architecture optimizes the cybersecurity management of semiconductor fabs and ensures production quality.

“

In the face of global challenges to information security in the semiconductor industry, TSMC continues to collaborate with supply chain partners to strengthen defense and resilience, safeguarding the overall security of the industry chain.

- Dr. James Tu, *Head of Corporate Information Security at TSMC and the Inaugural Chairman of SEMI Cybersecurity Committee*

“半導体工場のセキュリティをさらに強化するため、ファブ装置のサイバーセキュリティ仕様 SEMI E187が**TSMCの調達契約要件の1つとして正式に採用**され、新規装置の導入前に、コンピュータ運用システム、ネットワークセキュリティ、エンドポイントデバイス保護、セキュリティ監視と情報セキュリティ監査の4分野において、規格への準拠を検証するメカニズムを確立”

サプライヤーと緊密に連携し、サプライチェーン全体のセキュリティレベル向上に取り組み、また、その実績を他産業へ展開することも視野に入れいている。

出所: TSMC Strengthens “Specification for Cybersecurity of Semiconductor Equipment”, Realizing Mutual Industry Benefitsより抜粋

TSMCは主要サプライヤーに対して「10の重要管理項目」を徹底

2024年7月に「サプライチェーン情報セキュリティ管理の実践強化」をテーマとして、初のサプライチェーン・セキュリティ・ワークショップを開催（486社、800名が参加）

①	外部ネットワーク保護	企業の外部ネットワークまたはサービスには、堅牢なセキュリティ対策（ファイアウォール、IPS、クラウドセキュリティ）を装備しなければならない
②	リモートアクセス管理	承認スキームを確立し、会社の内部ネットワークにリモートアクセスする従業員はセキュリティ制御（会社支給PCの使用、多要素認証、VPNなど）を遵守する
③	Eメール保護	メールはレピュテーション評価、スパムフィルタリング、ウイルススキャンを適用し、送信者情報を偽装したメールは送信ドメイン認証等によりブロックする
④	不正プログラム保護	会社のコンピューターとサーバーにはEPP（エンドポイント保護プラットフォーム）を導入し、定期的に更新する
⑤	アカウント・パスワード管理	アカウントとパスワードの管理を強化する。生体認証の利用が望ましい
⑥	インターネットアクセス制御	インターネットアクセス制御には、悪意のあるウェブサイトや実行可能ファイルの検査を含めるべきであり、ブラウザにおけるサンドボックス技術の利用が推奨される
⑦	セキュリティ更新・管理	セキュリティ更新プログラムの適用ポリシーを策定し、オフィスPC、データセンターのみならず、VPNやアプリケーションサービス等の外部ネットワークサービスにも適用する
⑧	特権アカウント管理	高権限/ハイリスクアカウントは、多要素認証を強制するか、特定のコンピューターもしくはローカルネットワークセグメントでの操作のみを許可する
⑨	可搬型記憶装置の制御	USBメモリや書込み可能CD-ROMなどのコンピュータ入出力インターフェースを制御する
⑩	コンピュータ機器のセキュリティ制御	会社支給PCの使用のみ認め、EPPを導入し、ユーザーの管理者権限の使用を制限する。また、USBポートを無効化し、セキュリティ更新プログラムの適用を確認する

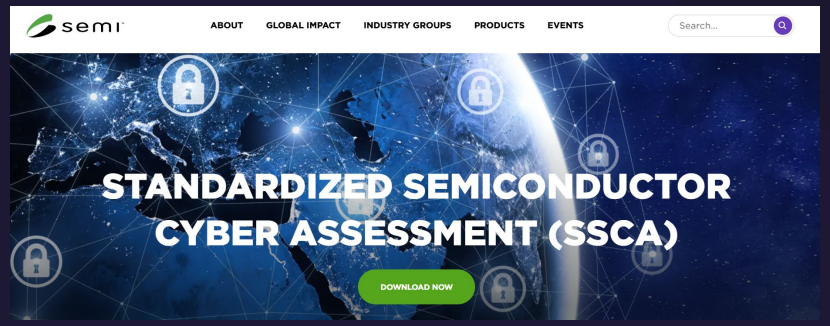
Adoption Rate

出所：TSMC Website: https://esg.tsmc.com/en-US/articles/318

txOne networks

SSCA (Standardized Semiconductor Cyber Assessment)

半導体業界向けに設計されたサイバーセキュリティ・アセスメントのフレームワーク



- SMCC WG3(Supply Chain Cybersecurity)の成果物として2025年8月に発行
- 半導体産業サプライチェーン全体を対象
- 21カテゴリ、168の評価項目で構成
- 自動車業界向けセキュリティ評価制度（TISAX）を参照

＜主な目的＞

- サプライヤと製品を評価するための業界標準のアセスメント項目を確立
- アセスメント対応コスト削減、コラボレーションと情報共有の強化

出所：SMCC Website　https://www.semi.org/en/industry-groups/semiconductor-cybersecurity/ssca

半導体産業のサイバーセキュリティ対策を総合的に支援

エージェントレス
セキュリティ検査ツール

Portable Inspector

ポータブルメディアの
マルウェア検査

Safe Port

レガシーOSにも対応した
エンドポイント保護

Stellar

半導体産業の厳格なネットワーク
要件に対応した産業用IPS

Edge IPS

エージェントレス
セキュリティ検査ツール

Portable Inspector

ポータブルメディアの
マルウェア検査

Safe Port

セキュリティ検査　エンドポイント保護　ネットワーク防御　セキュリティ検査

装置サプライヤ　オンボーディング　ステージング　プロダクション　メンテナンス

装置メーカー　ファブ・ファシリティエリア

製品セキュリティとしてのCRA対応例

Stellar

EdgeIPS

txOne networks

OEM
ライセンス
提供

装置にEdgeIPS/Stellarをバンドル

装置ベンダー

ライセンス
再許諾

工場（顧客）

ハードウェア (5年保証)

保守用品販売

ハードウェア

ソフトウェアライセンス
(パーペチュアル)

EdgeOne
管理ノードライセンス

ソフトウェア

*EdgeIPSの場合

txOne networks

Keep the Operation Running

TXOne Networksについて

トレンドマイクロとMoxaが**OT特化の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。

世界の4,200社（内、大手企業350社）がTXOne Networksの製品を採用

- 半導体製造
  - 半導体製造装置　TOP10の 8社
  - 半導体製造　TOP10の 6社
  - パッケージング　TOP10の 5社
- 医薬品業界　TOP10の 5社
- 自動車業界　TOP10の 5社
- 航空業界　TOP10の 5社

CEO：Dr. Terence Liu
Chairman：大三川 彰彦
日本法人代表：近藤 禎夫
従業員数：400名+（30か国）
総資金調達額: 約1億5570万ドル（シリーズB+）