資料7

txOne networks *The Leader of OT Zero Trust*

九州半導体人材育成等コンソーシアム第7回会合

半導体産業サイバーセキュリティ取り組み

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10月17日

TXOne Networksについて

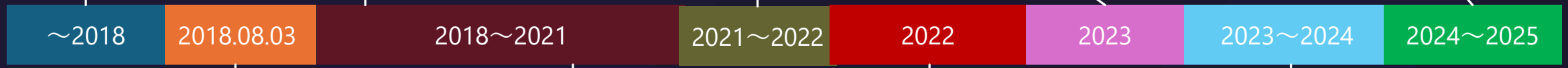
トレンドマイクロとMoxaが**OT特化のセキュリティソリューション**
を共同開発することを目的に2019年に設立。

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+）

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

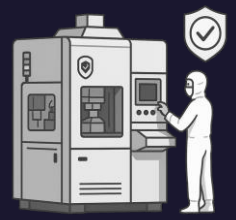
Fab内部システムの保護

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

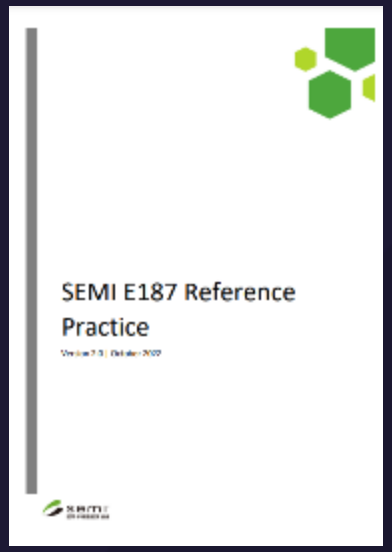
SEMI台湾 Cybersecurity Committee

SEMI台湾で開発・発行した規格、ガイドブック

ファブ装置のセキュリティ規格
SEMI E187発行

2022年1月

SEMI E187
Reference Practice発行

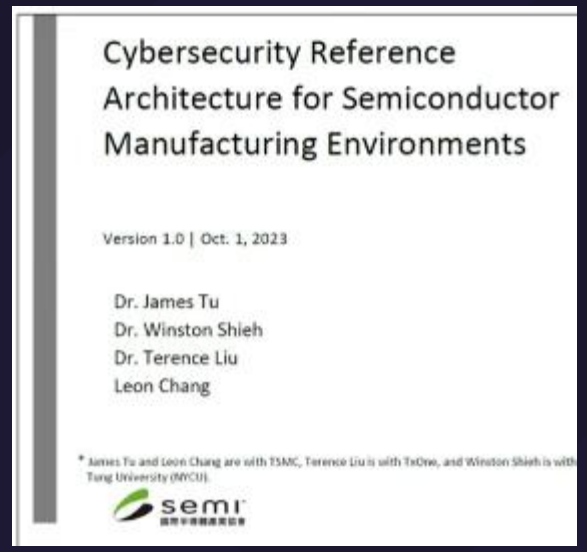


2022年10月

SEMI Semiconductor
Cybersecurity
Risk Rating Service

2023年1月

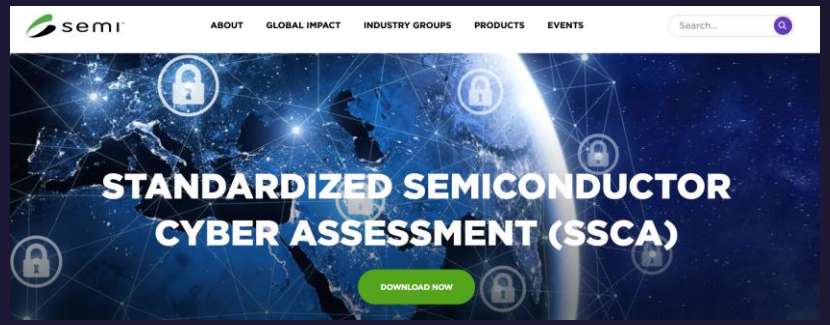
Cybersecurity Reference
Architecture for
Semiconductor
Manufacturing Environments



2023年10月

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

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

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

Keep the Operation Running