txOne networks *The Leader of OT Zero Trust*

工場を守るCybersecurity Day in KYUSHU

半導体工場に求められるセキュリティ対策

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

今野 尊之（いまの たかゆき）takayuki_imano@txone.com

TXOne Networks Japan 合同会社
業務執行役員 ビジネス戦略担当 兼 マーケティング本部長

SEMICON JAPAN 2023 サイバーセキュリティフォーラム

- 2001年トレンドマイクロ株式会社入社。通信事業との協業によるセキュリティサービス開発、IoTセキュリティビジネス開発、自動車向けセキュリティビジネス開発、IoT/OTセキュリティマーケティング等、主にビジネス開発およびマーケティング業務に従事。
- 2021年7月にトレンドマイクロ株式会社において、TXOne Networks Japan設立準備室の責任者に着任。日本法人の設立準備に従事し、2022年6月よりTXOne Networks Japanに転籍。

TXOne Networksについて

トレンドマイクロと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。

CEO：Dr. Terence Liu
従業員数：400名+（30か国）
総資金調達額: 約1億470万ドル（シリーズB）

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

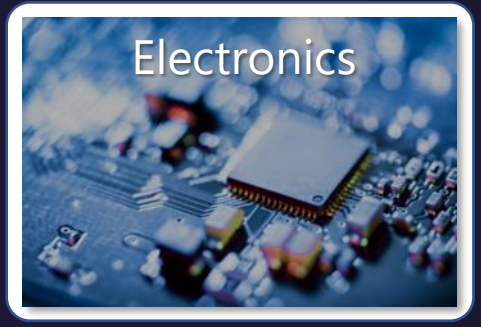
- 半導体製造
  - 半導体製造装置　TOP10の 8社
  - 半導体製造　TOP10の 6社
  - パッケージング　TOP10の 5社
- 医薬品業界　TOP10の 5社
- 自動車業界　TOP10の 5社
- 航空業界　TOP10の 5社

ICS Cybersecurity関連のAwardで製品戦略、製品の先進性が評価

TXOne Networksの注力産業

EXCELLING

EXPANDING



DEVELOPING

IT/OTサイバーセキュリティプラットフォームのリーダー

- Westlands Advisoryが発表した「産業用サイバーセキュリティの展望 2023-2030」において、「IT/OTサイバーセキュリティプラットフォーム」のリーダーとして評価されました。
- 以下のセキュリティ機能の戦略方向性、機能的特徴を基準に選考・評価
  - 資産の可視化
  - ネットワーク保護
  - ネットワークセグメンテーション
  - 脆弱性管理
  - エンドポイントプロテクション
  - セキュアアクセス
  - ネイティブソリューションの提供
  - 一元管理型のプラットフォームに統合
  - 他のプットフォームとの連携

txOne networks

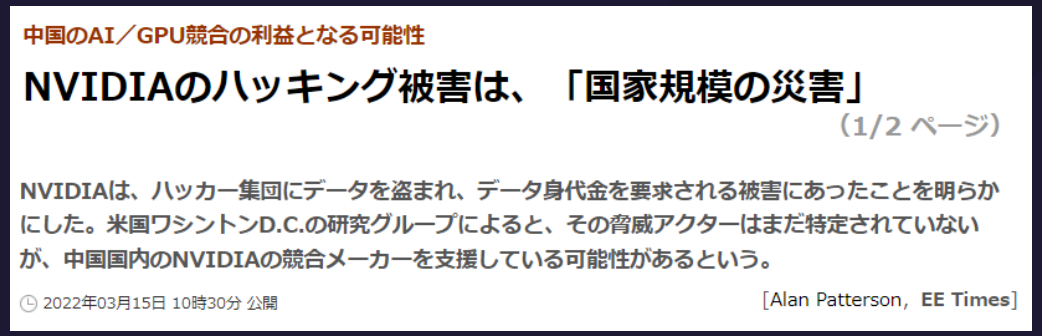
半導体業界セキュリティ動向

半導体製造企業におけるインシデント事例

企業	発生時期	概要	影響
半導体ファウンドリ（台湾）	2018年8月	半導体工場がウイルス（ランサムウェア）に感染。ランサムウェアに感染したツール（装置）を工場ネットワークに接続したことが原因	• 3日間に渡り生産活動が停止 • 最大190億円の損害
半導体向け研磨剤メーカー（日本）	2022年2月	日本法人および台湾子会社のサーバへ不正アクセスを確認。ホームページおよびネットワークを含めた社内システムを停止し、一部の生産と出荷を見合わせ	• 生産・出荷の一時停止 • ホームページの一時閉鎖 • 決算手続の遅延により決算発表時期を延期
シリコンウエハー製造メーカー（日本）	2022年3月	生産管理などの機密情報を扱う社内サーバへ不正アクセスを確認	• 社内システムをネットワークから切り離す措置を実施した影響により製造・出荷を一時停止
パワー半導体製造メーカー（ドイツ）	2022年8月	ランサムウェアの攻撃を受け、特定のデータが暗号化され、情報が流出した疑い	• 調査、復旧作業の影響により製造が一時停止

半導体製造企業におけるインシデント事例

2022年3月 NVIDIAがハッカー集団にデータを盗まれ、身代金を要求される被害を受けた。



中国のAI／GPU競合の利益となる可能性

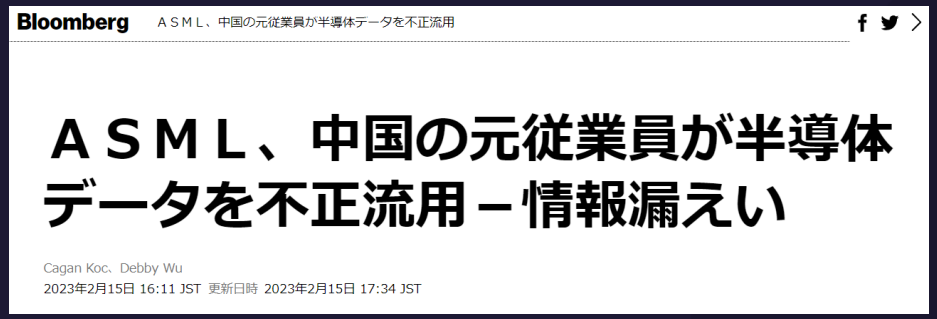
NVIDIAのハッキング被害は、「国家規模の災害」

（1/2 ページ）

NVIDIAは、ハッカー集団にデータを盗まれ、データ身代金を要求される被害にあったことを明らかにした。米国ワシントンD.C.の研究グループによると、その脅威アクターはまだ特定されていないが、中国国内のNVIDIAの競合メーカーを支援している可能性があるという。

2022年03月15日 10時30分 公開　[Alan Patterson, EE Times]

2023年2月 オランダの半導体製造装置メーカー、ASMLが元従業員が技術情報を不正流用し、結果的に輸出規制に違反した可能性があると明らかにした。



Bloomberg　ＡＳＭＬ、中国の元従業員が半導体データを不正流用

ＡＳＭＬ、中国の元従業員が半導体データを不正流用－情報漏えい

Cagan Koc、Debby Wu
2023年2月15日 16:11 JST 更新日時 2023年2月15日 17:34 JST

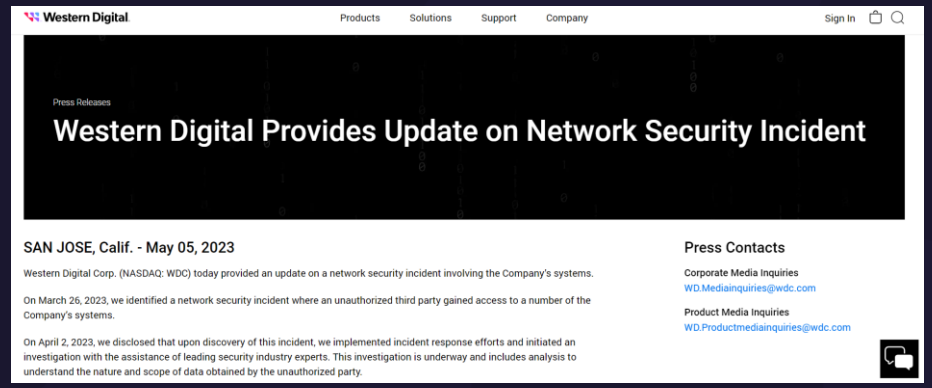
2023年2月 米国の半導体製造装置メーカー、MKSインスツルメンツは、ランサムウェア攻撃によるサプライチェーン業務の中断を受け、四半期収益に20％（約2億ドル）の打撃を受ける見込みであることを発表。

DIVE BRIEF

MKS Instruments says February ransomware attack will clip $200M from revenue

Published March 2, 2023

2023年4月 大手ストレージ企業のウエスタンデジタルがハッキングの被害を受け、クラウドサービスが一時的にダウン。ハッカーは「顧客情報を含むデータを盗み出した」と主張しており、最低1000万ドル以上の身代金を要求していると報じられた。



Western Digital　Products　Solutions　Support　Company　Sign In

Press Releases

Western Digital Provides Update on Network Security Incident

SAN JOSE, Calif. - May 05, 2023

Western Digital Corp. (NASDAQ: WDC) today provided an update on a network security incident involving the Company's systems.

On March 26, 2023, we identified a network security incident where an unauthorized third party gained access to a number of the Company's systems.

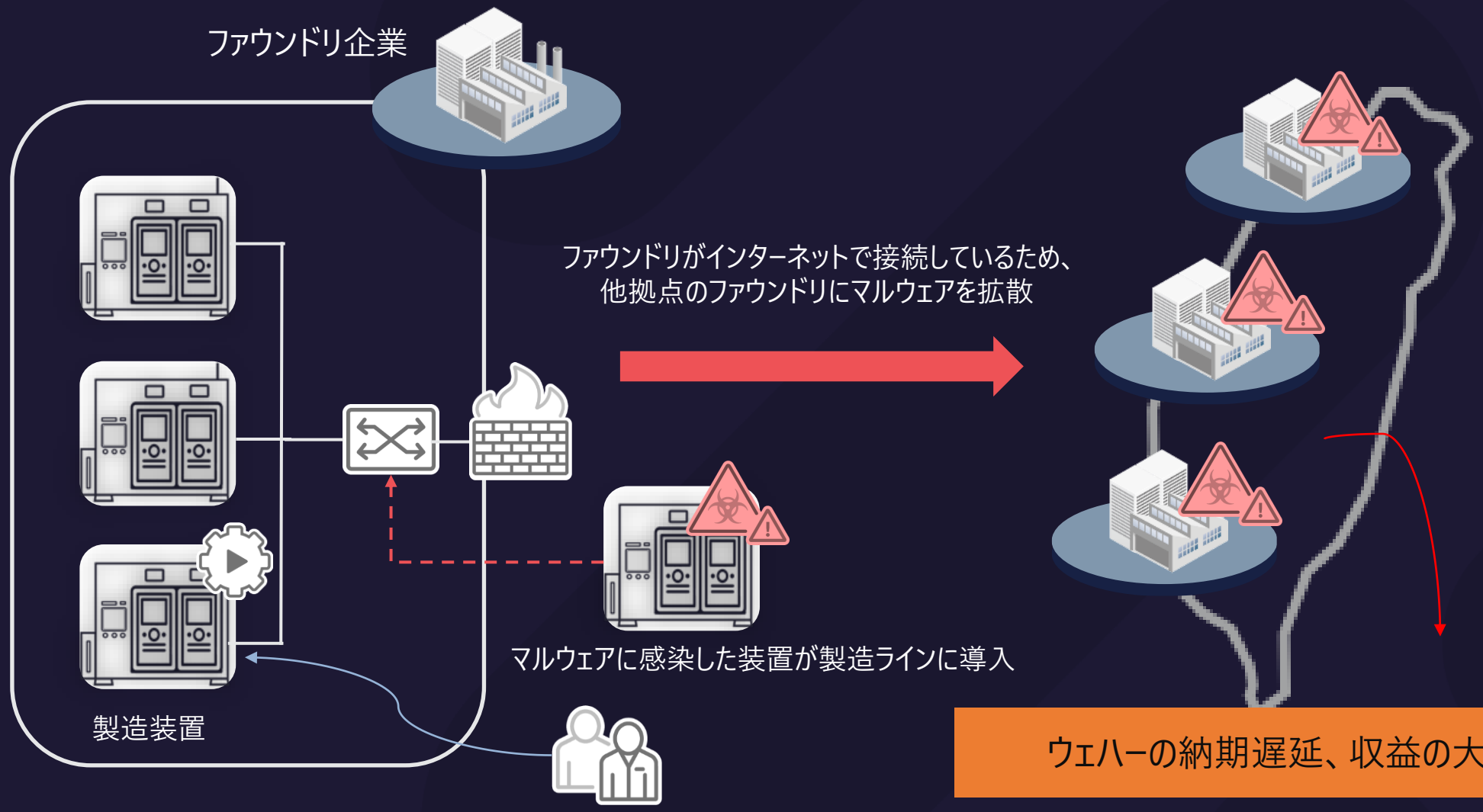
On April 2, 2023, we disclosed that upon discovery of this incident, we implemented incident response efforts and initiated an investigation with the assistance of leading security industry experts. This investigation is underway and includes analysis to understand the nature and scope of data obtained by the unauthorized party.

Press Contacts

Corporate Media Inquiries
WD.Mediainquiries@wdc.com

Product Media Inquiries
WD.Productmediainquiries@wdc.com

半導体企業の想定インシデント・シナリオ

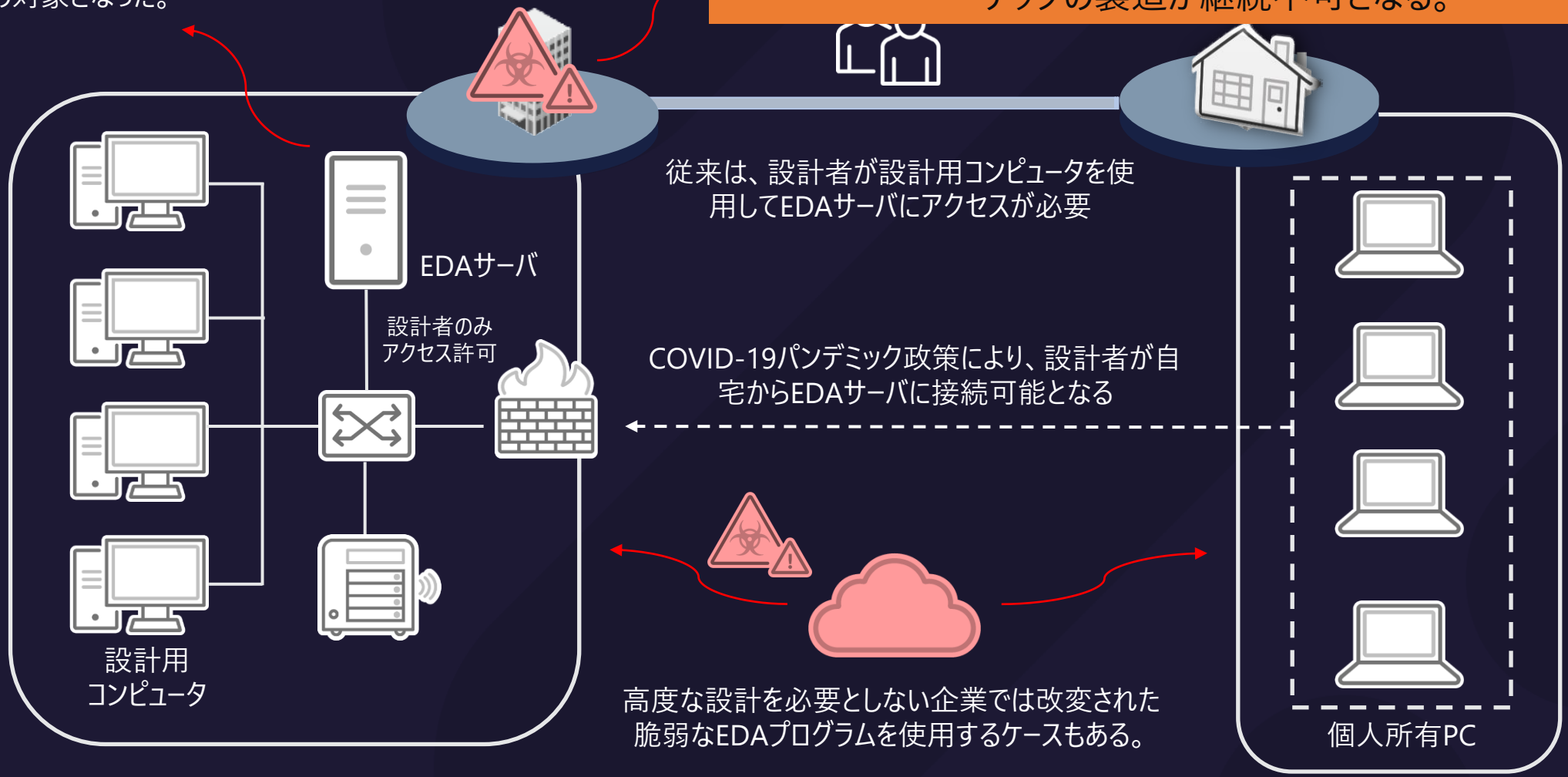


半導体企業の想定インシデント・シナリオ

2021年に一部のEDA製品がLog4jの脆弱性の対象となった。

ファブレス半導体企業

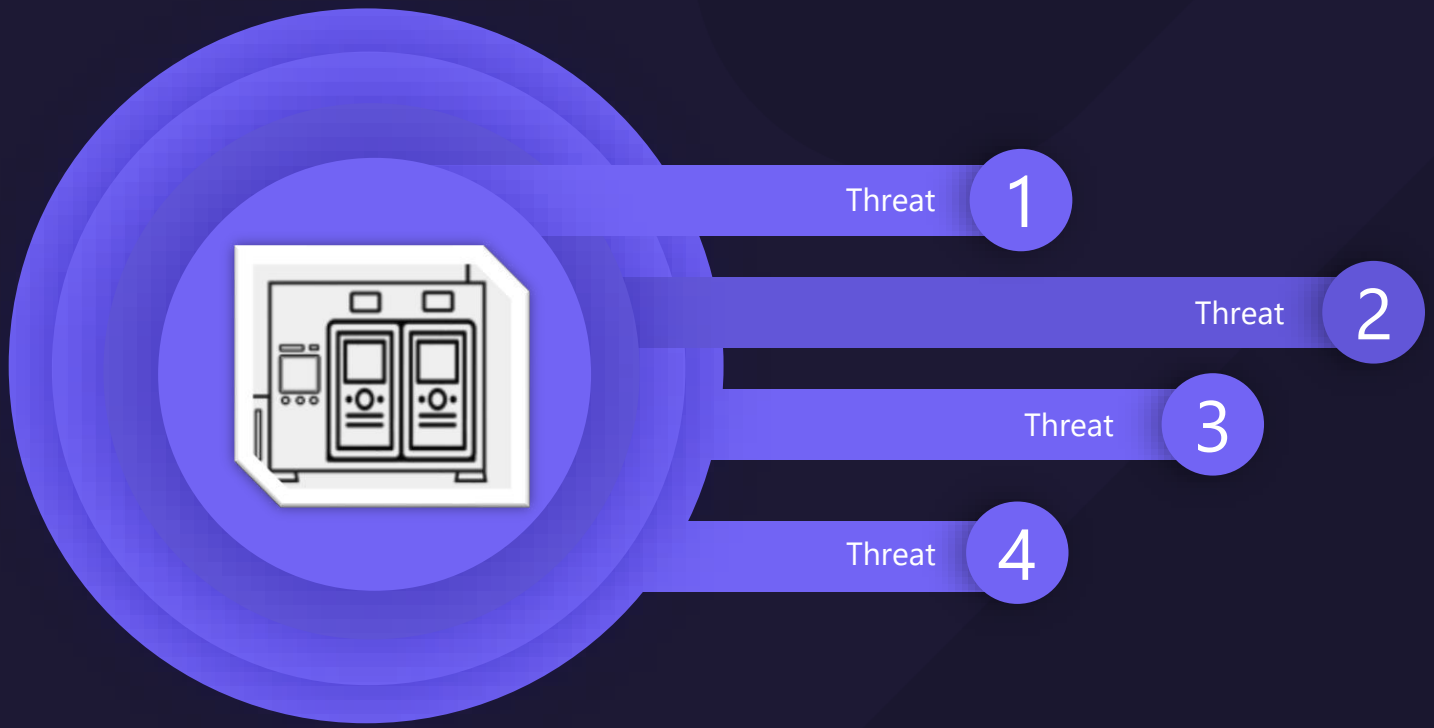
設計工程の作業が遅延し、中流・下流工程に影響を与えた結果、チップの製造が継続不可となる。



*EDA(Electronic Design Automation：電子設計自動化）

txOne networks

半導体関連企業のセキュリティ対策の課題



重要資産の価格高騰

資産の価格高騰により、費用対効果に優れた資産のシェアリングやアウトソースの導入によって、攻撃者の攻撃ベクトルが増加。

重要資産の精密な設計

資産所有者が任意に変更を加えることができないため、一般的なセキュリティ対策を適用することが困難。

工場のフラットなネットワーク環境

不適切なネットワークセグメンテーションにより、マルウェアの蔓延・拡散が容易となる。

膨大な資産

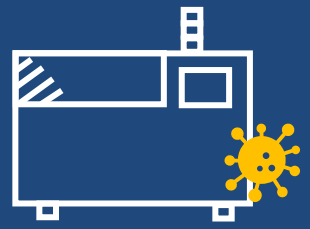
1工場で数百台の装置や数万台のコンピュータが稼働しており、メンテナンス負荷軽減のためにも中央集約的なログイベントや脆弱性の管理が求められる。

半導体業界におけるセキュリティリスク

内部関係者によるリスク

マルウェアが含まれるUSBを製造装置に接続することによる製造装置へのマルウェア感染

サプライチェーンリスク



生産現場に装置を納入する際に装置内に潜んでいたマルウェアがネットワーク接続時に拡散

外部脅威

リモート開発やメンテナンス用のVPN機器の脆弱性をついて侵入される

txOne networks

資産のライフサイクルにおける感染要因

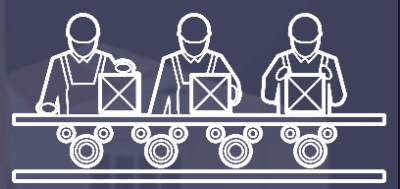
サプライチェーン・セキュリティ
（安全な設計・導入）

オペレーショナル・セキュリティ
（安全な運用）

サプライヤが資産を納入

オンボーディング

ステージング



生産活動

メンテナンス

47%

新規に導入した資産に最初から脆弱性・悪意のあるファイルが含まれていた

6%

OT環境のすべてのWindows端末にセキュリティ対策を行っている企業

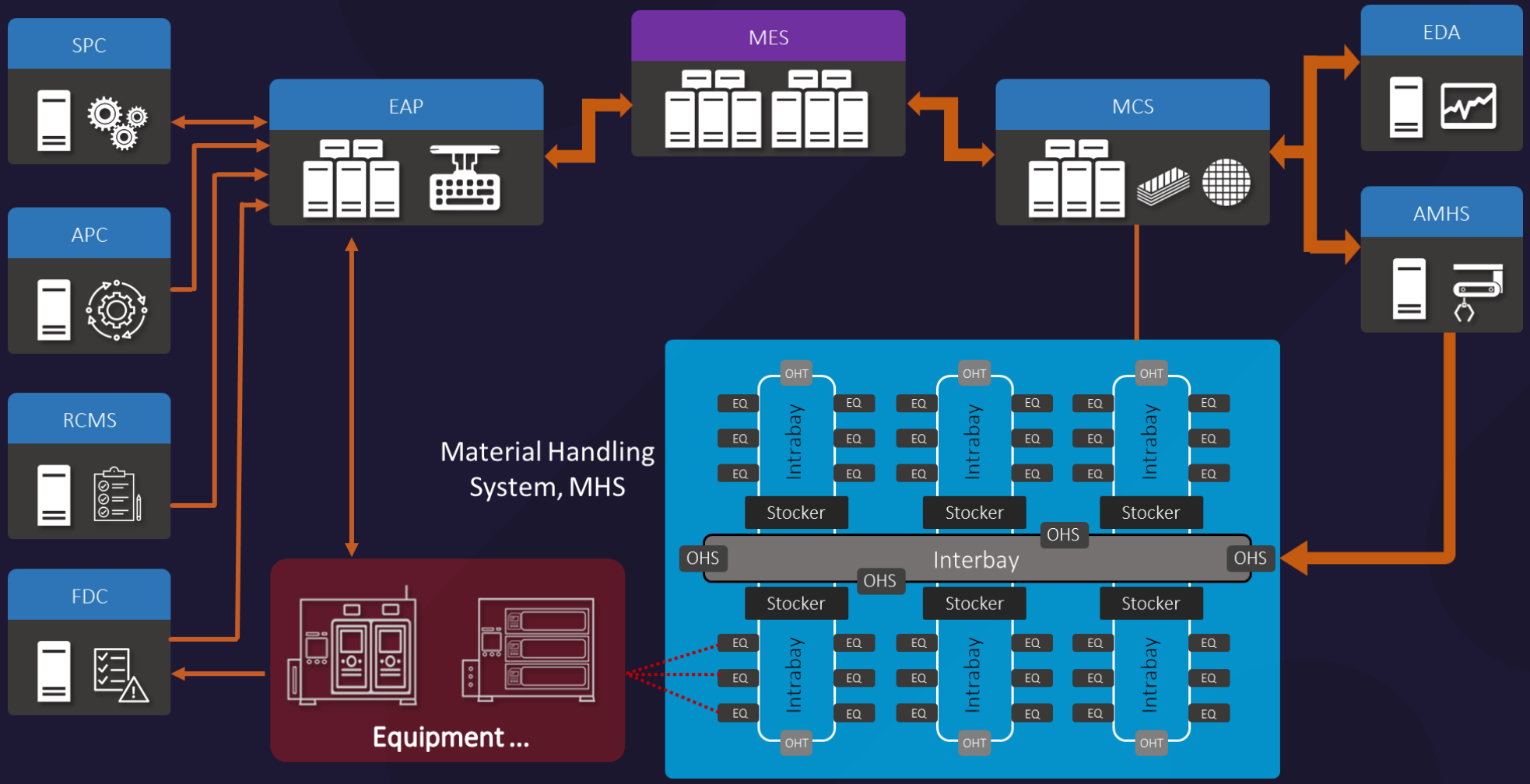
94%

ITセキュリティのインシデントがOT環境にも影響を及ぼした

Source: TXOne Networks 2022年 ICS/OTサイバーセキュリティ実態調査

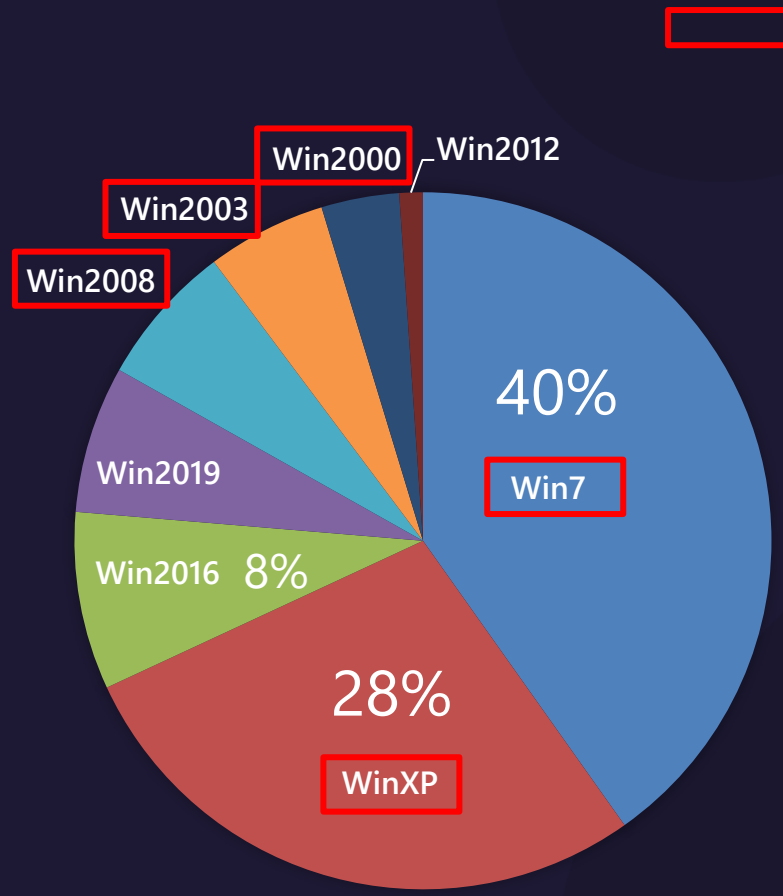
膨大な数の資産が稼働するファウンドリ

- ファウンドリには平均8,000~15,000台のコンピューティングパワーを持つ端末が稼働
- 膨大な数の端末のログイベントおよび脆弱性を集中管理する仕組みが求められる

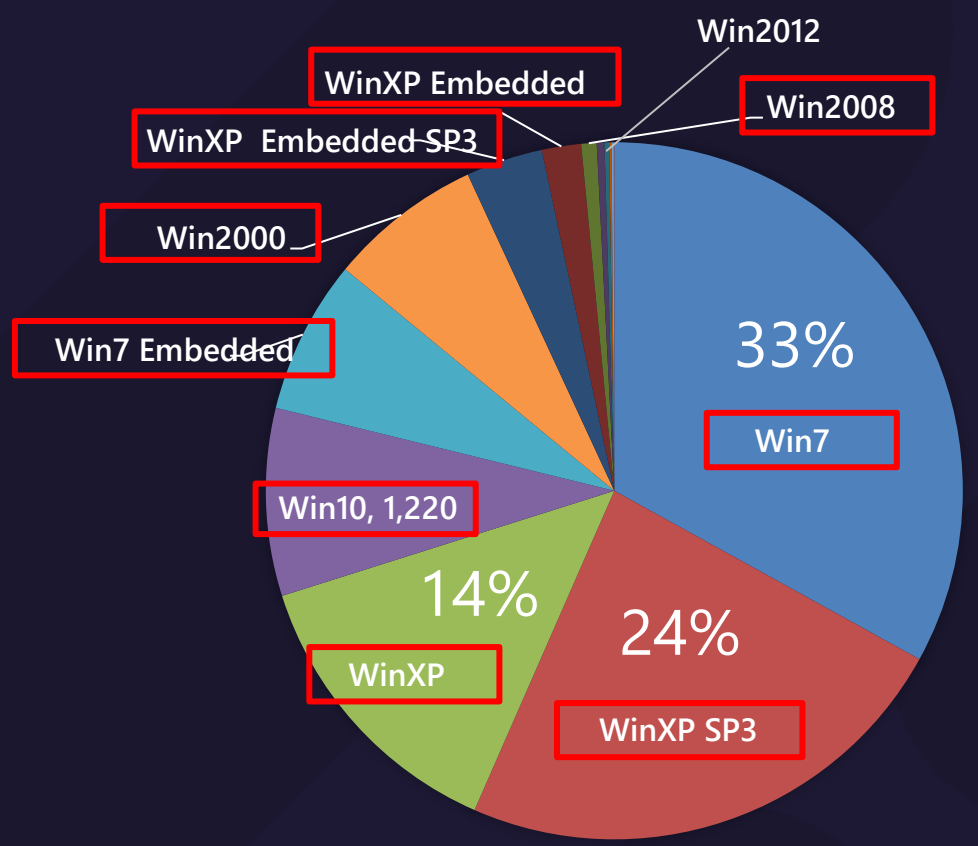


グローバル大手半導体製造工場で稼働する端末

- 全端末台数の約8~9割が既にOSメーカの延長サポートが終了したOSで稼働



A社 TOTAL：約50,000台



B社 TOTAL：約14,000台

txOne networks

SEMI台湾におけるサイバーセキュリティの取組

SEMI台湾 Cybersecurity Committee

グループリーダー
Dr. Terence Liu
CEO, TXOne Networks

SEMI TAIWAN
Cybersecurity
Committee

FOCUS 01

SEMI規格のプロモーション
レファレンスアーキテクチャの検討

FOCUS 02

サイバーセキュリティ啓蒙
（四半期毎、随時開催のイベント開催）

FOCUS 03

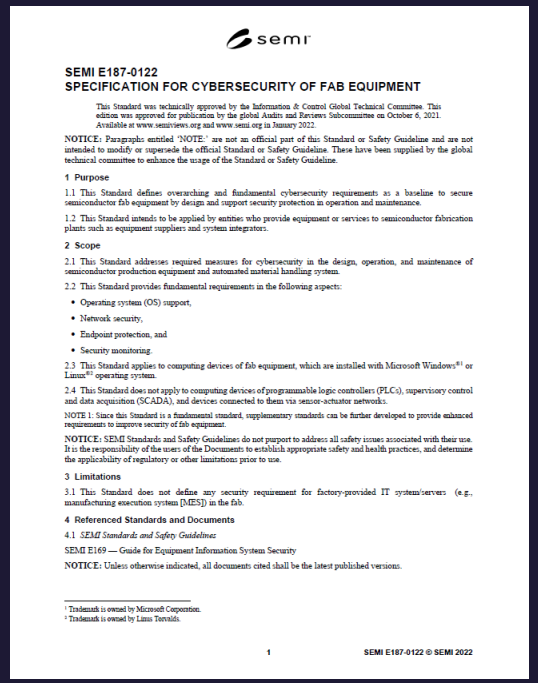
サプライチェーンサイバーセキュリティ
の評価方法の検討

FOCUS 04

NIST CSFをベースとしたサプライチェーン
サイバーセキュリティリスクアセスメントの検討

規格の発行から普及・啓蒙、実装まで支援

ファブ装置のセキュリティ規格
SEMI E-187発行



SEMI E187-0122
SPECIFICATION FOR CYBERSECURITY OF FAB EQUIPMENT

This Standard was technically approved by the Information & Control Global Technical Committee. This edition was approved for publication by the global Audits and Reviews Subcommittee on October 6, 2021. Available at www.semiviews.org and www.semi.org in January 2022.

NOTICE: Paragraphs entitled 'NOTE:' are not an official part of this Standard or Safety Guideline and are not intended to modify or supersede the official Standard or Safety Guideline. These have been supplied by the global technical committee to enhance the usage of the Standard or Safety Guideline.

1 Purpose

1.1 This Standard defines overarching and fundamental cybersecurity requirements as a baseline to secure semiconductor fab equipment by design and support security protection in operation and maintenance.

1.2 This Standard intends to be applied by entities who provide equipment or services to semiconductor fabrication plants such as equipment suppliers and system integrators.

2 Scope

2.1 This Standard addresses required measures for cybersecurity in the design, operation, and maintenance of semiconductor production equipment and automated material handling system.

2.2 This Standard provides fundamental requirements in the following aspects:

- Operating system (OS) support,
- Network security,
- Endpoint protection, and
- Security monitoring.

2.3 This Standard applies to computing devices of fab equipment, which are installed with Microsoft Windows®[1] or Linux®[2] operating system.

2.4 This Standard does not apply to computing devices of programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA), and devices connected to them via sensor-actuator networks.

NOTE 1: Since this Standard is a fundamental standard, supplementary standards can be further developed to provide enhanced requirements to improve security of fab equipment.

NOTICE: SEMI Standards and Safety Guidelines do not purport to address all safety issues associated with their use. It is the responsibility of the users of the Documents to establish appropriate safety and health practices, and determine the applicability of regulatory or other limitations prior to use.

3 Limitations

3.1 This Standard does not define any security requirement for factory-provided IT system/servers (e.g., manufacturing execution system [MES]) in the fab.

4 Referenced Standards and Documents

4.1 *SEMI Standards and Safety Guidelines*

SEMI E169 — Guide for Equipment Information System Security

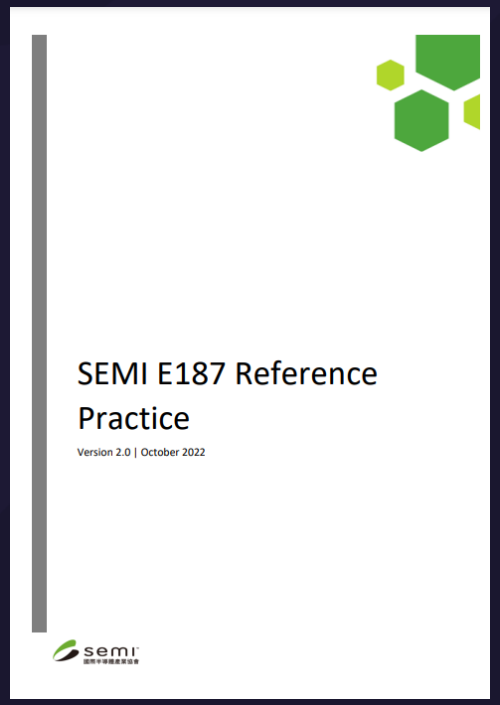
NOTICE: Unless otherwise indicated, all documents cited shall be the latest published versions.

[1] Trademark is owned by Microsoft Corporation.
[2] Trademark is owned by Linus Torvalds.

1 SEMI E187-0122 © SEMI 2022

2022年1月

SEMI E-187
Reference Practice発行

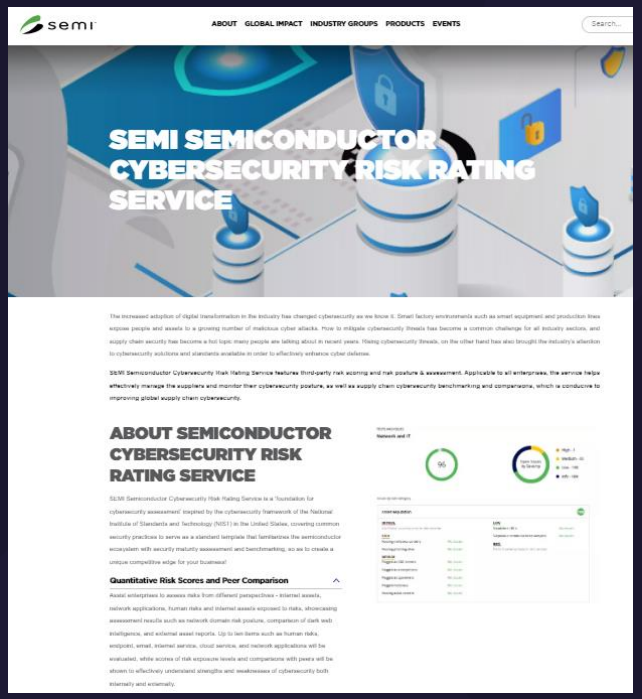


SEMI E187 Reference Practice

Version 2.0 | October 2022

2022年10月

SEMI Semiconductor
Cybersecurity Risk Rating Service



2023年1月

txOne networks

半導体業界向けセキュリティ規格
SEMI E187/E188

SEMI E-187/188

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)** **2022年1月発行**	• SEMIスタンダード台湾地区のTask Forceによって開発 • Fab装置の共通の最低限のセキュリティ要件を定義 • 製造装置の4つの主要コンポーネント(オペレーティング・システム、ネットワークセキュリティ、エンドポイント保護、セキュリティモニタリング)にフォーカス
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)** **2022年2月発行**	• SEMI スタンダード北米地区のTask Forceによって開発 • 初期の装置導入時、フィールドサービスの修理、パッチ適用、メンテナンスなどの継続的な活動を通じて、工場内へのマルウェアの感染から守ることにフォーカス

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

E187 / E188の位置づけ

	E187	E188
テーマ	新規の装置開発に必要な基本的なサイバーセキュリティ	資産のライフサイクルにおけるマルウェアフリーの実現
目的	装置の脆弱性や脅威を半導体製造現場に持ち込まれることを防ぐ	
フェーズ	製造装置を開発・導入するフェーズ	製造装置の導入、運用、保守のフェーズ
主な対象	装置サプライヤ	
スコープ	工場ネットワークに接続されるコンピューティング機器 • Windows, Linux OS搭載装置 • PLC、センサー、SCADA、MESは対象外	装置導入後の資産のライフサイクルにおける、マルウェアフリーの実装プロセス • 既存の機器（コンピュータ、コントローラ、PLCなど）のあらゆる演算装置 • MES、MCS、ホストシステムなどは除く
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 • セキュリティパッチ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	• 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

※E188と重複する実施事項

SEMI E187とは？

- ファブ装置へのサイバー攻撃の急増を受け、SEMI台湾地区のSecurityタスクフォースにおいて、3年にわたり開発され、3回の電子投票を経て2022年1月に発行。
- 半導体製造装置を設計上安全にし，運用・保守上のセキュリティ保護を支援するための基本的なサイバーセキュリティの要件を定義。
- 半導体製造工場に装置やサービスを提供する装置サプライヤー、システムインテグレータを対象として想定。
- 装置のサプライチェーン全体におけるグローバルなサイバーセキュリティ・コンプライアンスの確立を目指す。

SEMI E187のスコープ

SEMI E187の要求事項

① オペレーティング・システム(OS)のセキュリティ

- オペレーティングシステムのEOL*ステータスを追跡する。
- 装置サプライヤーはEOLを迎えたOSを搭載した装置を出荷してはならない。
- 装置サプライヤーはパッチやセキュリティアップデートの適用手順を文書で提供する。

*EOL: End of Life

② ネットワークのセキュリティ

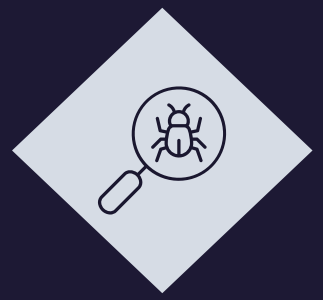
- セキュアな通信ネットワークプロトコル（HTTPS, SSH, SFTP）やサービスに対応する。
- ネットワークプロトコル、ポートの使用状況の文書を提供する。
- ネットワーク構成やポート変更の保守手順の文書を提供する。

SEMI E187の要求事項

③ エンドポイントのセキュリティ

- 装置出荷前に脆弱性スキャンを行い、日時を含むスキャンログを作成する。
- 装置出荷前にマルウェアスキャンを行い、装置がマルウェアフリーであることを証明するレポートを作成する。
- 悪意のあるファイルやスクリプトからシステムを保護可能な、アンチマルウェアソリューションとファブ装置の互換性を評価する。
- セキュリティハードニングに関する文書を提供する。
- OSとアプリケーションのユーザー認証手法を実装する。
- OSとアプリケーションに対してロールベースでアクセス権を管理する機能を実装する。

SEMI E187の要求事項



④ セキュリティモニタリング

- システムおよびアプリケーションのセキュリティ・イベント・ログを記録し、アーカイブする。
- システム・イベント・ログには、少なくともアクセス制御、設定変更、システムエラーの記録を含める。
- セキュリティ・イベント・ログを安全に保管する。
- セキュリティ・イベント・ログを監視および確認するためのツールを用いる。
- セキュリティ・イベント・ログを機械読み取り可能な形式で正規化する。

SEMI E187の要求事項への対応例

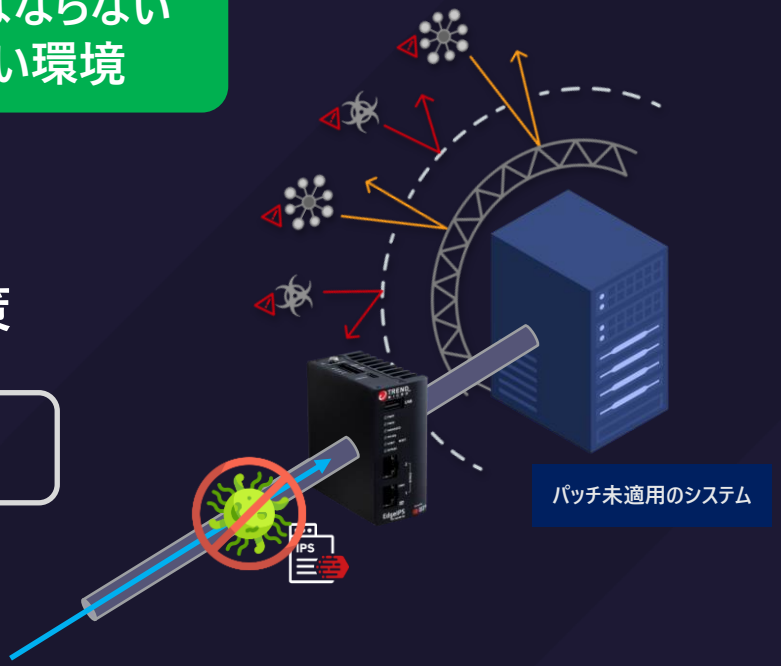
① オペレーティング・システム(OS)のセキュリティ

- オペレーティングシステムのEOLステータスを追跡する。
- 装置サプライヤーはEOLを迎えたOSを搭載した装置を出荷してはならない。
- 装置サプライヤーはパッチやセキュリティアップデートの適用手順を文書で提供する。

- EOLを迎えたOSを使い続けなければならない
- タイムリーなパッチアップデートが難しい環境

“仮想パッチ”による脆弱性対策

パッチ適用が難しい/時間がかかる環境
に対するリスク軽減



Edgeシリーズの仮想パッチで保護

SEMI E187の要求事項への対応例

③ エンドポイントのセキュリティ

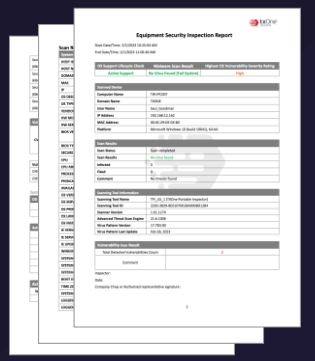
- 装置出荷前に脆弱性スキャンを行い、日時を含むスキャンログを作成する。
- 装置出荷前にマルウェアスキャンを行い、装置がマルウェアフリーであることを証明する日付入りのスキャンレポートを作成する。

- **装置出荷前のマルウェアフリー検査の実施**
- **マルウェアフリーのエビデンスレポートの生成**

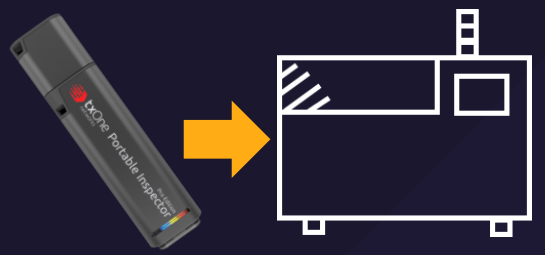
- **“エージェントレス”のマルウェア検査**
- **資産情報の収集・管理**

Element One

PDF形式の「マルウェアフリーレポート」を生成



- 詳細なシステム情報
- スキャナーの構成
- インストールされているアプリケーションのリスト
- インストールされているWindows Update
- 脆弱性スキャンと未適用のパッチ情報
- アクティブなポート、サービス



Portable Inspector

SEMI E187の要求事項への対応例

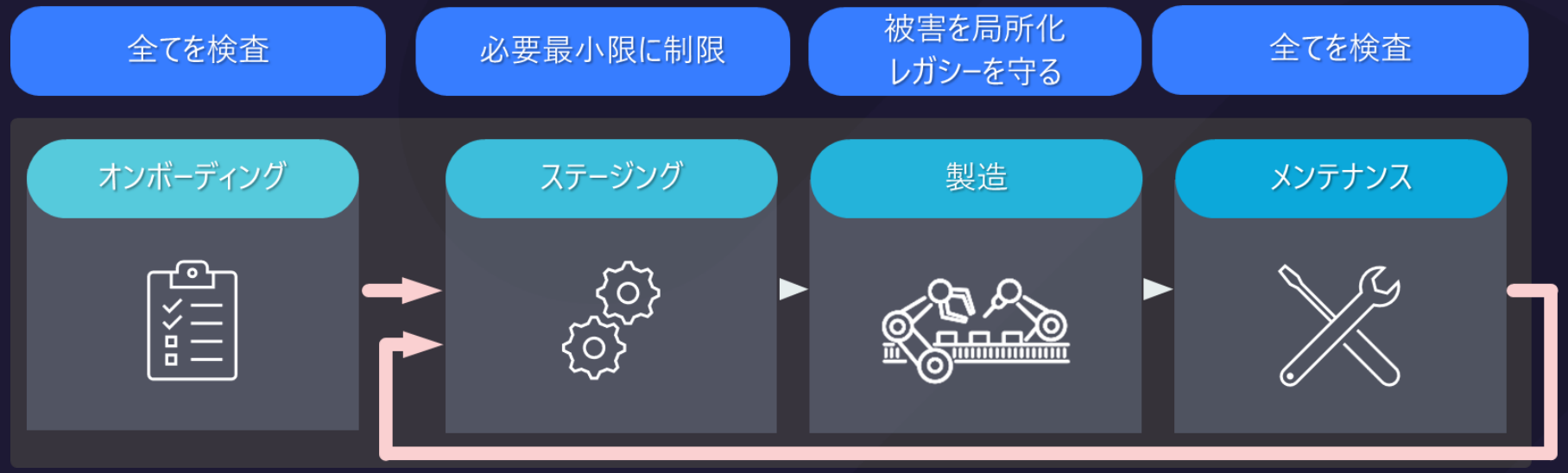
③ エンドポイントのセキュリティ

- 悪意のあるファイルやスクリプトからシステムを保護可能な、アンチマルウェアソリューションとファブ装置の互換性を評価する。

装置のパフォーマンスへの影響を考慮し、互換性を評価

- **装置の用途や環境に合わせた保護手段を選択可能**
- **多用な環境を1つのエージェントで柔軟に保護**

SEMI E187に適合したTXOne Networksのソリューション



導入機器経由の
マルウェア感染

USB型セキュリティツールによる
出荷前検査

Portable Inspector

パッチ適用が困難
マシンリソースが不十分

- ロックダウンによる保護
- OT環境に適したアンチウイルス

Stellar

フラットなネットワーク
による感染拡大
レガシーOSの保護

- マイクロセグメンテーション
- 仮想パッチ
- アクセス制御

Edgeシリーズ

作業用PCやUSBメモリに
よるマルウェア感染

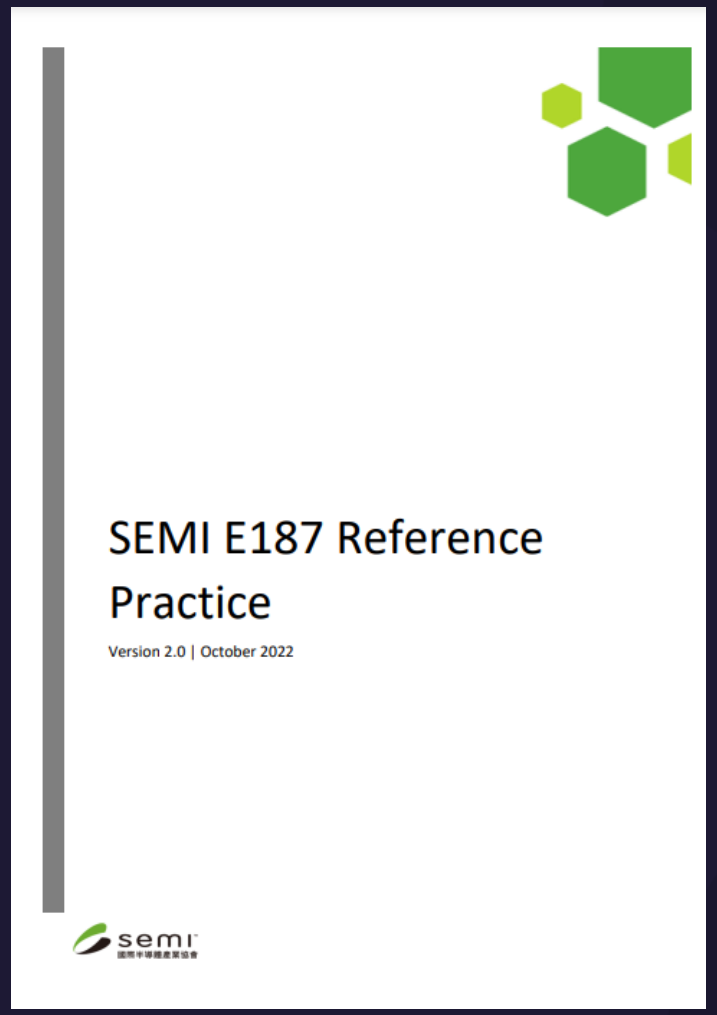
USB型セキュリティツールによる
作業前検査

Portable Inspector
Safe Port

E187/E188に関するよくある質問

	質問	回答
1	E187がWindowsやLinux OSがを対象としているの理由は？	実際に半導体製造企業で発生したインシデントがWindowsシステムの脆弱性に起因しており、同様のインシデントの再発を防ぐことと、生産設備で使用されているコンピュータの多くがWindowsやLinuxであるため、E187はOSに着目しています。
2	PLCはなぜE187では適用外となり、E188では適用対象となっているのか？	PLCの多くはOSを搭載しないリアルタイムシステムのため、OSに着目したE187は対象外としています。一方、E188はPLCを対象としていますが、PLCに対してマルウェアスキャンを実行可能な商用ツールが存在しない場合は、ユーザとの合意のもと、マルウェアフリーを証明する代替手段を提供することを要求しています。
3	SCADAはなぜE187の適用外となっているのでしょうか？	半導体工場のSCADAの多くは、FAB施設の管理システムであるFMCS(Facility Management Control System)に属しており、半導体メーカー自身がセキュリティソリューションを導入し、適切に管理しているため、装置サプライヤを対象としたE187の適用外となっています。
4	E187とE188はどのように使い分けるのでしょうか？	E187とE188は補完関係にあり、装置の環境やユーザからの要件を踏まえ、両規格を併用することで半導体製造ラインをよりセキュアにすることができます。
5	E187/E188は実際に装置メーカーの調達要件となっているのでしょうか？	実際の調達要件について、弊社では把握できておりませんが、半導体関連企業様からのE187/E188に関するご相談やお問い合わせは増えてきております。
6	TXOne NetworksはE187/E188の策定にどのように関わっているのでしょうか？	当社CEOテレンス・リュウがSEMI台湾 Cybersecurity Committeeのグループリーダーを務め、規格の策定や普及・啓蒙活動に貢献しています。

SEMI E187 Reference Practice (2022年10月発行)



- Taiwan Semiconductor Cybersecurity Committeeのリファレンス・アーキテクチャ・ワーキンググループがSEMI E187の実際の展開を支援するために作成。
- E187の各要求事項の解説とセキュリティ対策実装に関するQ＆Aおよび実践例を紹介

3.1.1 FAQ:

- ***Which operating systems are applicable in the scope of this standard?***
  This Standard applies to computing devices of fab equipment, which are installed with Microsoft Windows® or Linux® operating system.
- ***How does the equipment supplier know if the operating system is end of life?***
  It is recommended that the equipment provider periodically tracks the product roadmap information of the operating system vendors such as Microsoft ®, Red Hat ®, Ubuntu ®.

3.1.2 Practice and Example

- Windows XP, Windows Vista and Windows 7 indicated in Table 1 are examples of end-of-support operating systems. When Microsoft stopped issuing updates and patches, these operating systems rapidly became orders of magnitude more vulnerable to security threats. Equipment vendors should not ship equipment with end-of-support operating systems. If an EOL operating system is needed to use on the fab equipment, both the user and supplier may agree on alternative methods to identify and fix vulnerabilities. However, negotiating such an agreement is out of the scope of SEMI E187.

DLサイト：https://forms.office.com/Pages/ResponsePage.aspx?id=3QuozL10F0-Obe7NC6xaAujCICXu0vFEnfhFAXAhCNJUNzdWMDA5Rjc3U1ZUSktTUk1US1gySVVLVy4u

半導体情報セキュリティリスク評価サービス（SEMI台湾）

- 半導体サプライヤーのサイバーセキュリティ対策状況を評価し、評価結果を元にした改善や取引信頼性の向上に活用。特に中小企業のサイバーセキュリティ対策状況の改善が期待される。
- NIST CSFをベースとした3rd Party製（Panorays社）のサプライチェーンリスク評価ツールと包括的なチェックリストにより、リスク状況をリスクスコアリングとして把握可能
- エントリーレベル（オプションA）とエキスパートレベル（オプションB）の2つの有償サービスを提供

「半導体情報セキュリティリスク評価サービス」で実現できること

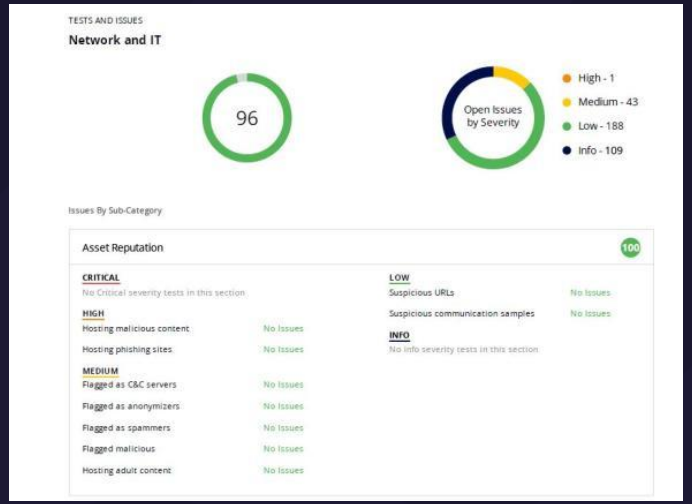
① リスクスコアを定量化し、同業他社とセキュリティ対策状況を比較

② 総合的なリスク評価スコアと半導体業界の知見を元にしたセキュリティ評価

③ リスク低減の提案結果を元に、改善後の評価結果を確認

④ 継続的なリスク評価により、リスク状況の変化を把握

⑤ リスク評価結果を取引先に共有し、取引の信頼性の構築に活用



SEMI Taiwan HP: https://www.semi.org/en/products-services/semitwn-semiconductor-cybersecurity-service/assessment-fundamentum

TSMC Webサイトのアナウンスメント（2023年9月14日）

Dr. James Tu (fourth from the left), Head of Corporate Information Security, shares cybersecurity challenges and solutions at the 2023 SEMICON Taiwan Semiconductor Cybersecurity Global Summit. (Photo source: SEMI)

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*

TSMC Strengthens "Specification for Cybers ecurity of Semiconductor Equipment", Realiz ing Mutual Industry Benefits

TSMCは「半導体装置のサイバーセキュリティ規格」を強化し、業界相互の産業利益を追求する。

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

TSMCのアナウンスメント要約

1. 半導体工場のセキュリティをさらに強化するために、2023年より、半導体装置のセキュリティ規格（SEMI E-187）が、TSMCの**調達契約要件**のひとつとして、正式に盛り込まれた。
2. サプライヤーが新しい装置をTSMCに導入する際に、SEMI E187の準拠を検証する仕組みが確立された。
3. 2023年、SEMI台湾は台湾デジタル産業局(MODA)と協力し、半導体装置メーカーに対して、セキュリティ・チェックリストの適用を支援。その中で、**Gallant Precision Machining**（台湾）と**Contrel Technology**（台湾）は、SEMI E-187の要件を満たしていることを、認証機関によって証明された世界初のサプライヤーとなった。

TSMCのアナウンスメント要約

4. TSMCとSEMI台湾が協力し、**「半導体工場サイバーセキュリティ・リファレンス・アーキテクチャー」**を作成。**2023年10月**にSEMI台湾より公開。
5. 2023年に**「SEMI半導体サイバーセキュリティ・リスク評価サービス」**をリリースし、企業がサイバーセキュリティの脆弱性を迅速に特定し、保護対策の有効性を監視できるよう支援する。年内に**1,000社以上**がこのサービスを採用する見込み。

認証機関によるE-187適合性証明書

SEMI E187認証機関であるビューローベリタスがGallant Precision Machining社とContrel Technology社に対し、**世界初のSEMI E187適合性証明書(VoC)**を発行。（2023年8月）

Certificate No: S112082801 Page 1 / 2

BUREAU VERITAS

Verification of Conformity

Applicant: Gallant Precision Machining Co., Ltd
Brand Name: GPM
Equipment: [redacted]
Test Model: [redacted]
Test Report No.: CYT-[redacted]

We, **Bureau Veritas Consumer Products Services (H.K.) Ltd., Taoyuan Branch**, declare that the equipment above has been tested in our facility and found compliance with the requirement limits of applicable standards. The test record, data evaluation and Equipment Under Test (EUT) configurations represented herein are true and accurate under the standards herein specified.

The pass requirements of SEMI E187-0122 are as follows:

Computer Operation System Security Requirement (2/2)
Network Security Requirement (2/2)
Endpoint Protection Requirement (6/6)
Security Monitor Requirement (2/2)

Shang Jyh Lin

Shang Jyh Lin / Expert
Aug. 28, 2023

Certificate No: S112082401 Page 1 / 2

BUREAU VERITAS

Verification of Conformity

Applicant: Contrel Technology Co., Ltd.
Brand Name: Contrel
Equipment: [redacted]
Test Model: [redacted]
Test Report No.: CYT-[redacted]

We, **Bureau Veritas Consumer Products Services (H.K.) Ltd., Taoyuan Branch**, declare that the equipment above has been tested in our facility and found compliance with the requirement limits of applicable standards. The test record, data evaluation and Equipment Under Test (EUT) configurations represented herein are true and accurate under the standards herein specified.

The pass requirements of SEMI E187-0122 are as follows:

Computer Operation System Security Requirement (2/2)
Network Security Requirement (2/2)
Endpoint Protection Requirement (6/6)
Security Monitor Requirement (2/2)

Shang Jyh Lin

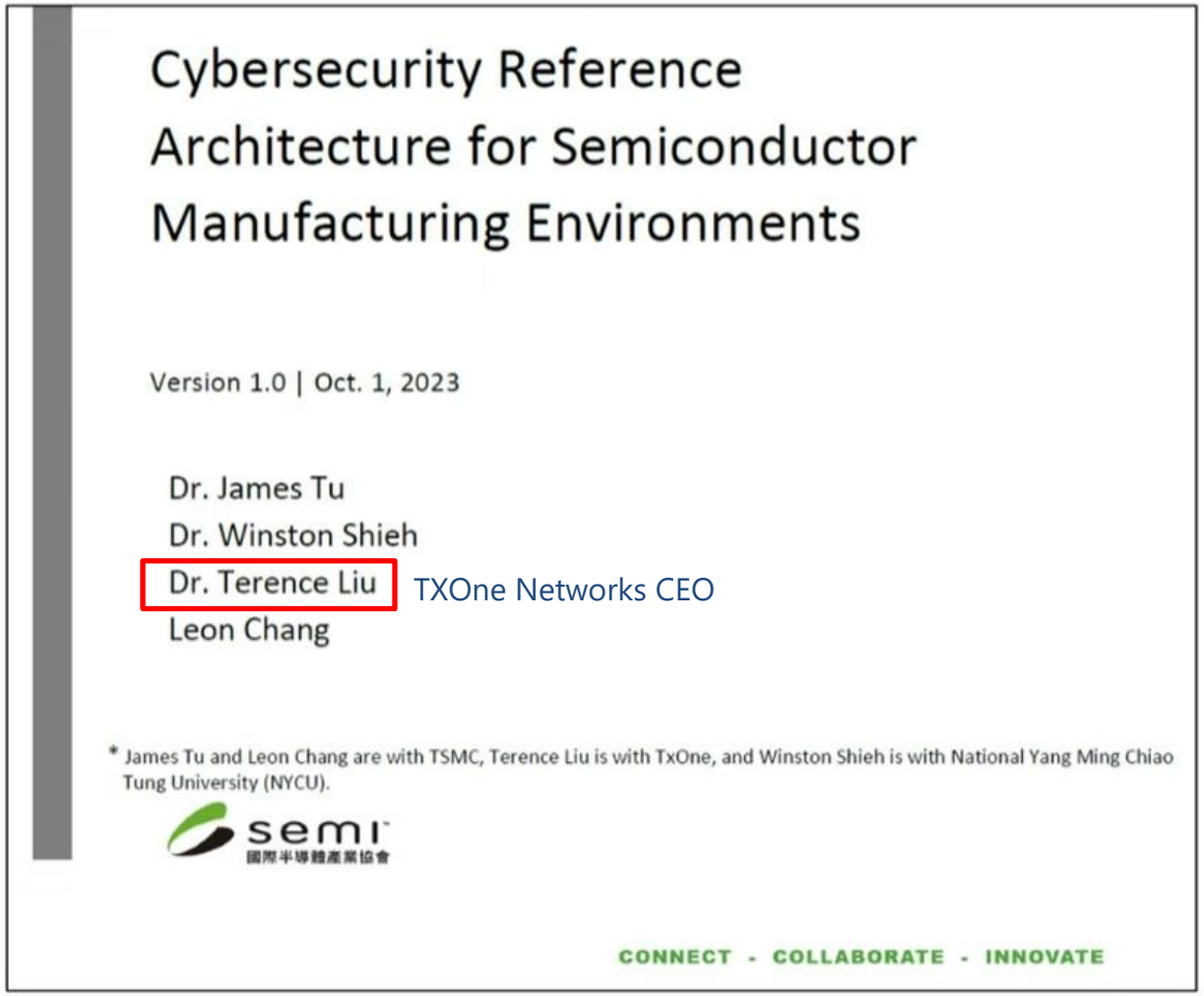
Shang Jyh Lin / Expert
Aug. 24, 2023

台湾当局によるE187普及促進活動

台湾デジタル発展省デジタル開発部が、ビューローベリタスが発行した世界初のSEMI E187適合証明書(VoC)を取得したGallant Precision Machining社とContrel Technology社を表彰。

出典:台湾デジタル発展省公式Webサイト
https://moda.gov.tw/ADI/news/latest-news/6465

Fabサイバーセキュリティ・リファレンス・アーキテクチャー



Cybersecurity Reference Architecture for Semiconductor Manufacturing Environments

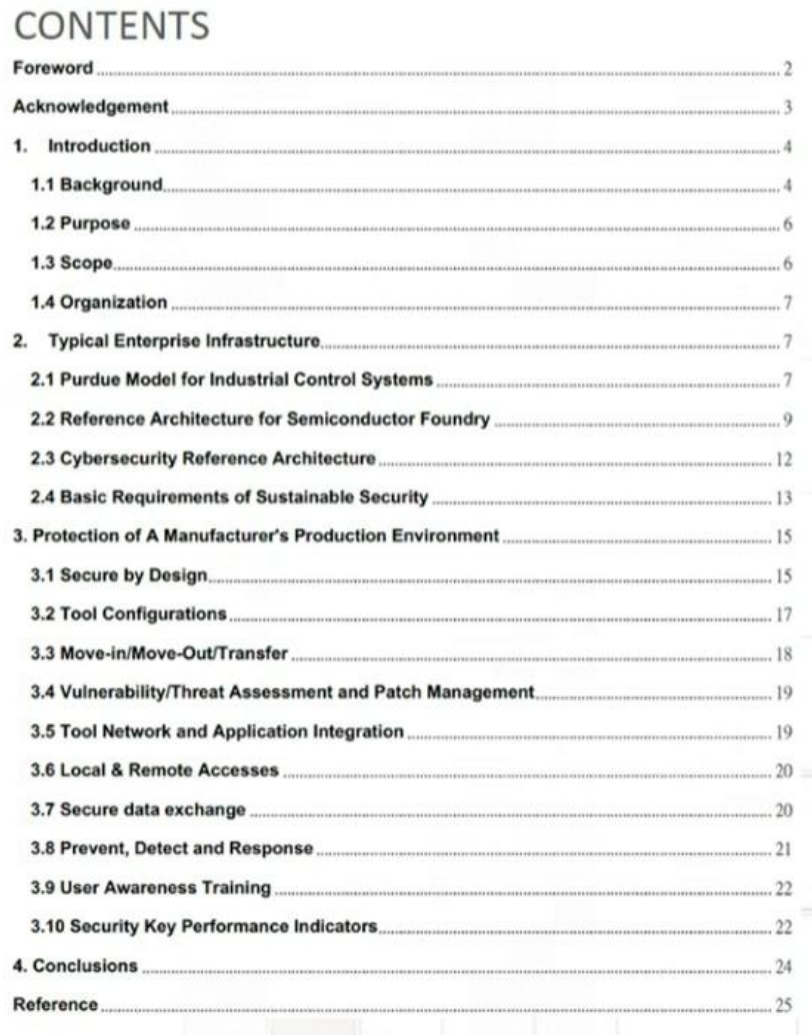
Version 1.0 | Oct. 1, 2023

Dr. James Tu
Dr. Winston Shieh
Dr. Terence Liu TXOne Networks CEO
Leon Chang

* James Tu and Leon Chang are with TSMC, Terence Liu is with TxOne, and Winston Shieh is with National Yang Ming Chiao Tung University (NYCU).

semi 國際半導體產業協會

CONNECT - COLLABORATE - INNOVATE

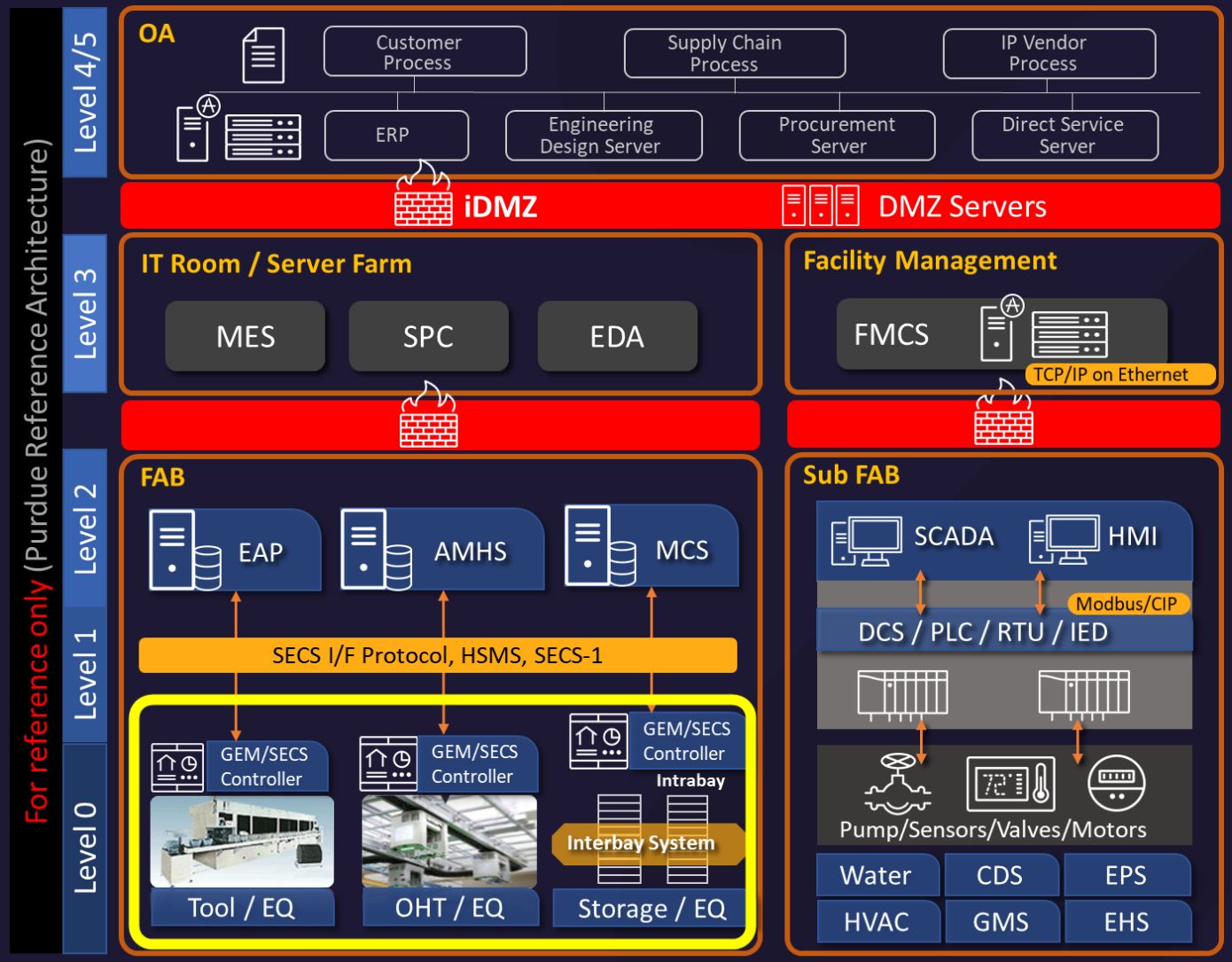


CONTENTS

参考URL：https://www.txone.com/blog/unveiling-semi-innovative-cybersecurity-architecture/

txOne networks

Fabサイバーセキュリティ・リファレンス・アーキテクチャー



SEMI E187

IEC 62443 で規定されている階層的かつ段階的なアプローチに基づいて、ツール開発、配備プロセス、生産管理のセキュリティ要件を定義することを目的として作成。

Basic Requirements of Sustainable Security

1) 安全性を考慮したツール設計・設定
2) ツールの導入/移設時の対応
3) 脆弱性評価とパッチマネジメント
4) ローカル/リモートアクセスの制御ポリシー
5) 安全な工場ネットワークとアプリケーションの統合
6) 安全なデータ交換
7) 脅威の予防、検出、対応
8) Fabセキュリティ管理
9) 多層防御のためのKPI

txOne networks

Fabのネットワークセグメンテーションとエンドポイント対策

txOne networks

国内半導体企業のセキュリティ取組状況

Semiconductor Cybersecurity Executive Conference

Date：2023年12月15日 15:00~17:00
参加者：国内半導体製造企業、半導体装置製造企業（12社）

Time	Subject	Speakers
	Greeting Message	**Yoshio Kondo** Head of TXOne Networks Japan
15:00-15:05	Opening remark, Introduction of participants	**Takayuki Imano** TXOne Networks Japan Marketing Director
15:05-15:20	Opening Message	**Terence Liu** TXOne Networks CEO
15:20-15:40	Keynote : The Practice on Semiconductor's Cybersecurity	**Dr. James Tu** Director. Head of Corporate Information Security at TSMC
15:40-16:00	Keynote : Trends in government related factory systems cybersecurity promotion.	**Professor Hiroshi Esaki** TOKYO University
16:00-16:45	Q&A and round table discussion	All
16:45-16:50	Closing	**Akihiko Omikawa** TXOne Networks Chairman
16:50-17:00	Group Photo & Adjournment	All

事前アンケート Roundtable Session

Q1:ゲストスピーカーへの質問および意見交換を希望するテーマ
Q2:参加企業の方々と情報交換、意見交換を希望するトピック
Q3:半導体サイバーセキュリティ規格 SEMI E-187の自社における適用状況

Topic1: レガシーOSやレガシーシステムのセキュリティ対策
Topic2: SEMI E-187の適用状況
Topic3: 半導体製造工場のセキュリティ対策の取組
Topic4: TSMCのセキュリティポリシー及び現在の取組状況
Topic5: グローバルオペレーション
Topic6: その他

Roundtable Sessionで取り上げたいテーマ

Topic1:レガシーOSやレガシーシステムのセキュリティ対策

1-1 標的型脅威に対するOTのセキュリティ対策　（特に組込みOSとレガシーOSについて）
1-2 レガシーOSのセキュリティ対策
1-3 レガシー工場のセキュリティ対応状況

Topic2: SEMI E-187の適用状況

2-1 SEMI E187で対応できないサイバーセキュリティ対策
2-2 E187とE188の将来計画、あるべき姿
2-3 既存装置に対するE-187適用の考え方
2-4 装置ベンダーへのガイドラインの展開方法

Topic3:半導体製造工場のセキュリティ対策の取組

3-1 セキュリティ保守・運用（SOC）は、対応・復旧を含めてどのように行うのか
3-2 リモートメンテナンスにおける、機器ベンダー側からのアクセス制御の考え方
3-3 既存設備にガイドラインを適用する際のセキュリティポリシー
3-4 FSIRT はOT と IT の両方を管理するのか、それとも別々に管理するのか
3-5 セキュリティへの投資対効果を評価する指標

Roundtable Sessionで取り上げたいテーマ

Topic4: TSMCのセキュリティポリシー及び現在の取組状況

4-1 投資計画に占めるOTセキュリティ対策の割合
4-2 工場のセキュリティ運用（自社／パートナー）の進め方
4-3 セキュリティ対策の方針・運用・管理方法
4-4 TSMC社内のセキュリティ対策方針・運用・管理方法の実態

Topic5:グローバルオペレーション

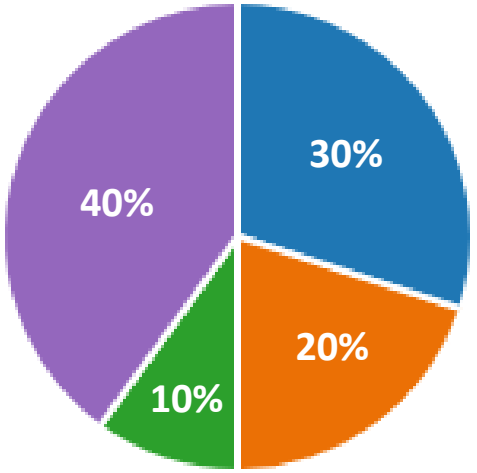
5-1 グローバルに展開する工場のセキュリティガバナンスと運用
5-2 中国工場へのリモートメンテナンスを行う場合、データの越境問題の解決方法
5-3 日本と海外、それぞれの地域におけるベンダー採用・調達の方針

Topic6: その他

6-1 エンドユーザーとサプライヤーの責任境界
6-2 E188において有償SCAPの使用を推奨しているが、コスト負担はどうしているか

SEMI E-187の自社における適用状況

- 取引先の調達要件において、E-187を元にしたセキュリティ対策が求められており、既にセキュリティ対策に着手している。
- 取引先の調達要件において、E-187を元にしたセキュリティ対策が求められているが、情報収集段階にあり、セキュリティ対策は未着手
- 取引先の調達要件において、セキュリティ対策は求められていない
- E-187について知らない
- その他



＜その他＞

- 当社としては対応していないがセキュリティサービスの検討時にE187を意識している。
- 新設工場のため、これから取り組む予定。
- サプライヤの調達要件において、セキュリティ対策は要求されているが、E-187の記載はない。
- E-187は適用されていないが、サプライヤーへの調達要求事項において、セキュリティ対策が求められるようになってきている。

スマート工場EXPO 2024（東京ビッグサイト）に出展します

[会　　期] 2024年1月24日（水）～26日（金）10:00～17:00
[出展場所]　東京ビッグサイト西館 Hall2 ブースNo. W61-16
[来場登録]　ご登録はこちら

Keep the Operation Running