txOne networks *The Leader of OT Zero Trust*

工場セキュリティガイドライン啓発・連続セミナ 第2回

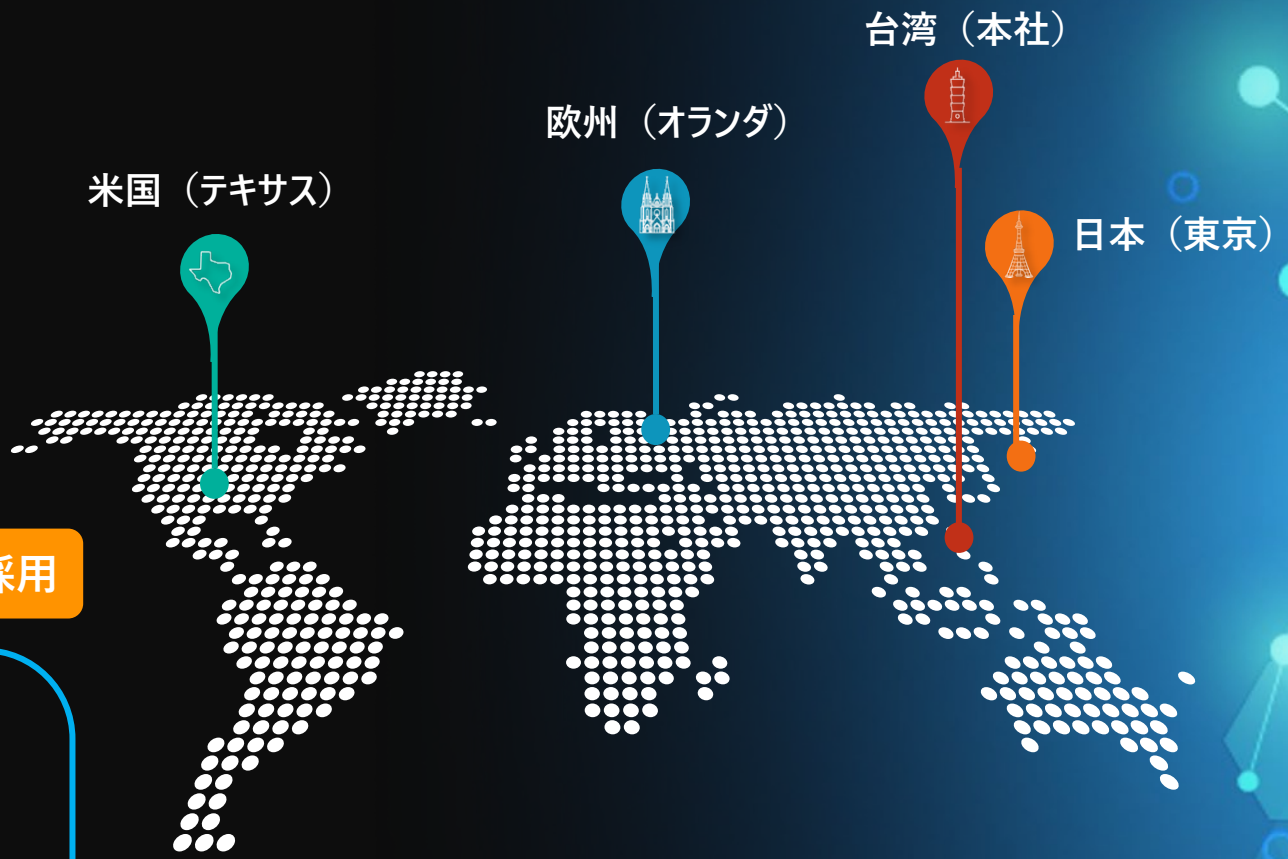
高まるファブのサイバー対策需要、SEMI初のセキュリティ規格と今後の展開

TXOne Networks Japan合同会社
業務執行役員 今野 尊之
takayuki_imano@txone.com

Keep the Operation Running ~オペレーションの継続~

txOne networks

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：280名＋（2023年2月現在）

世界の350社を超える大手企業がTXOne Networksの製品を採用

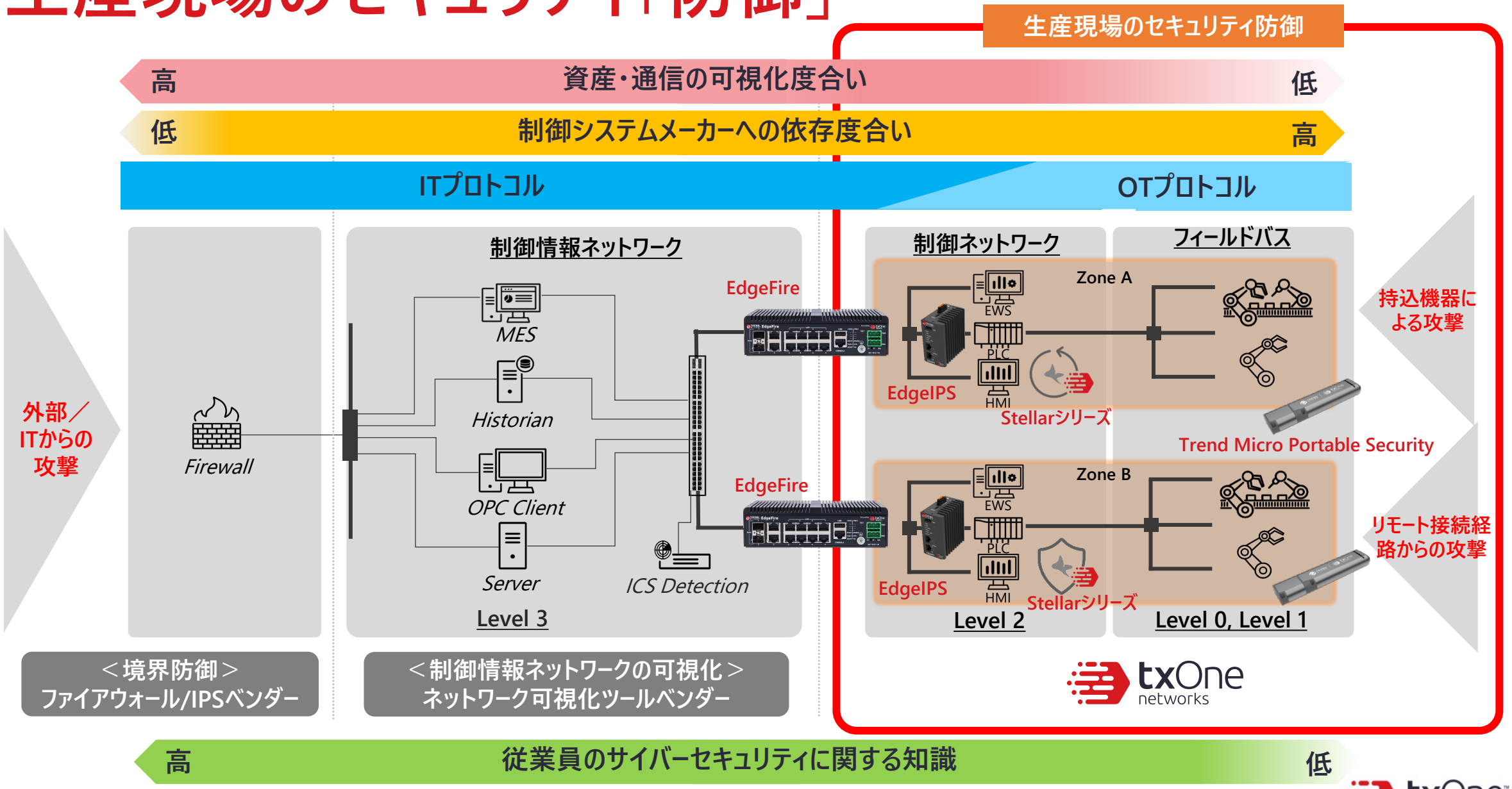
- **半導体製造**
  - 半導体製造装置　TOP10の 5社
  - 半導体製造　TOP10の 5社
  - パッケージング　TOP10の 4社
- **医薬品業界**　TOP10の 5社
- **自動車業界**　TOP10の 5社
- **航空業界**　TOP10の 4社

TXOne Networksが提供する価値

OT環境のサイバーセキュリティの課題を克服し
産業用機器の運用を継続する。

~Keep the Operation Running~

生産現場のセキュリティ「防御」



txOne networks

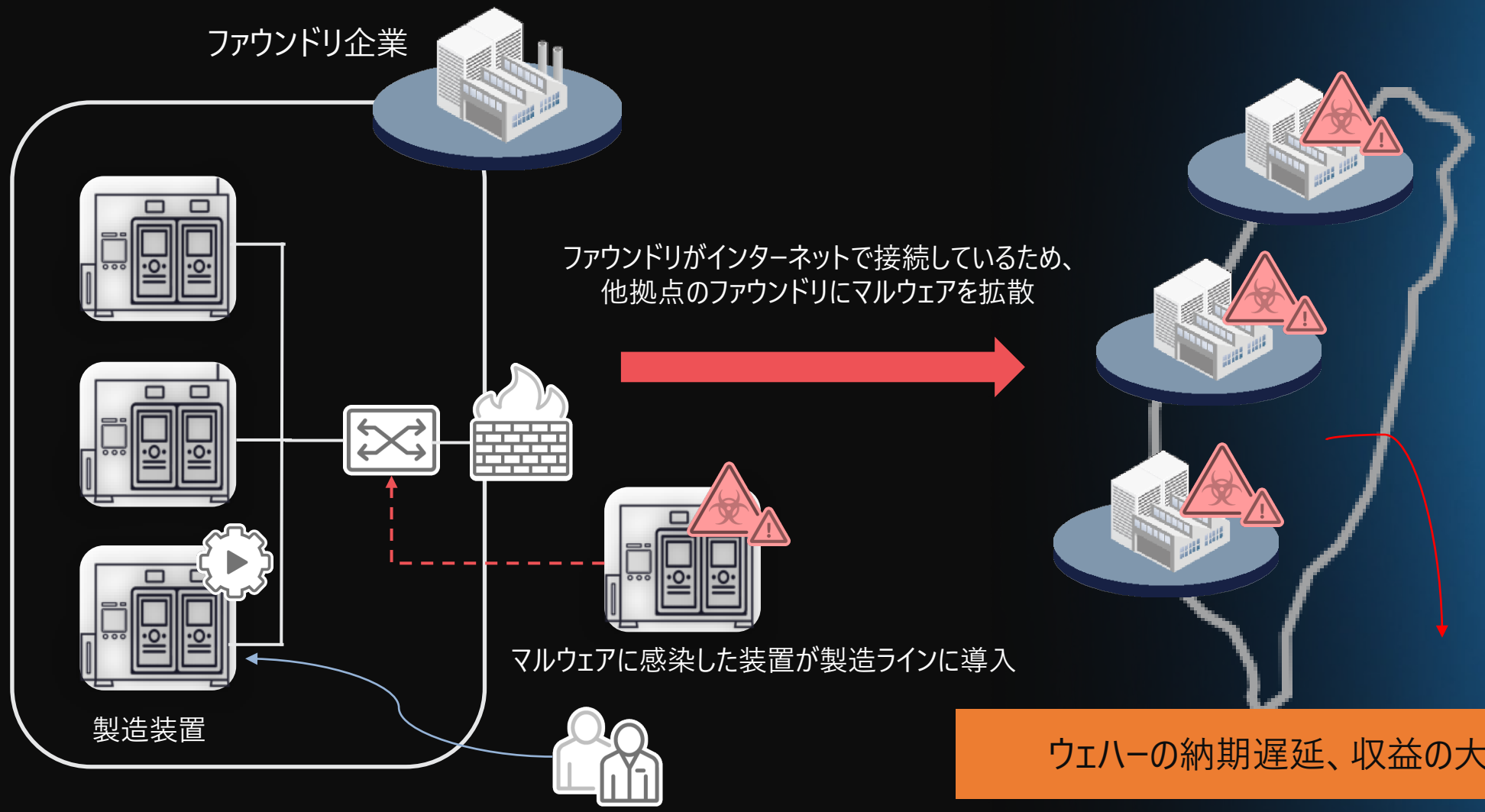
txOne networks

半導体企業におけるインシデント事例

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 	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 	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 	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 	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

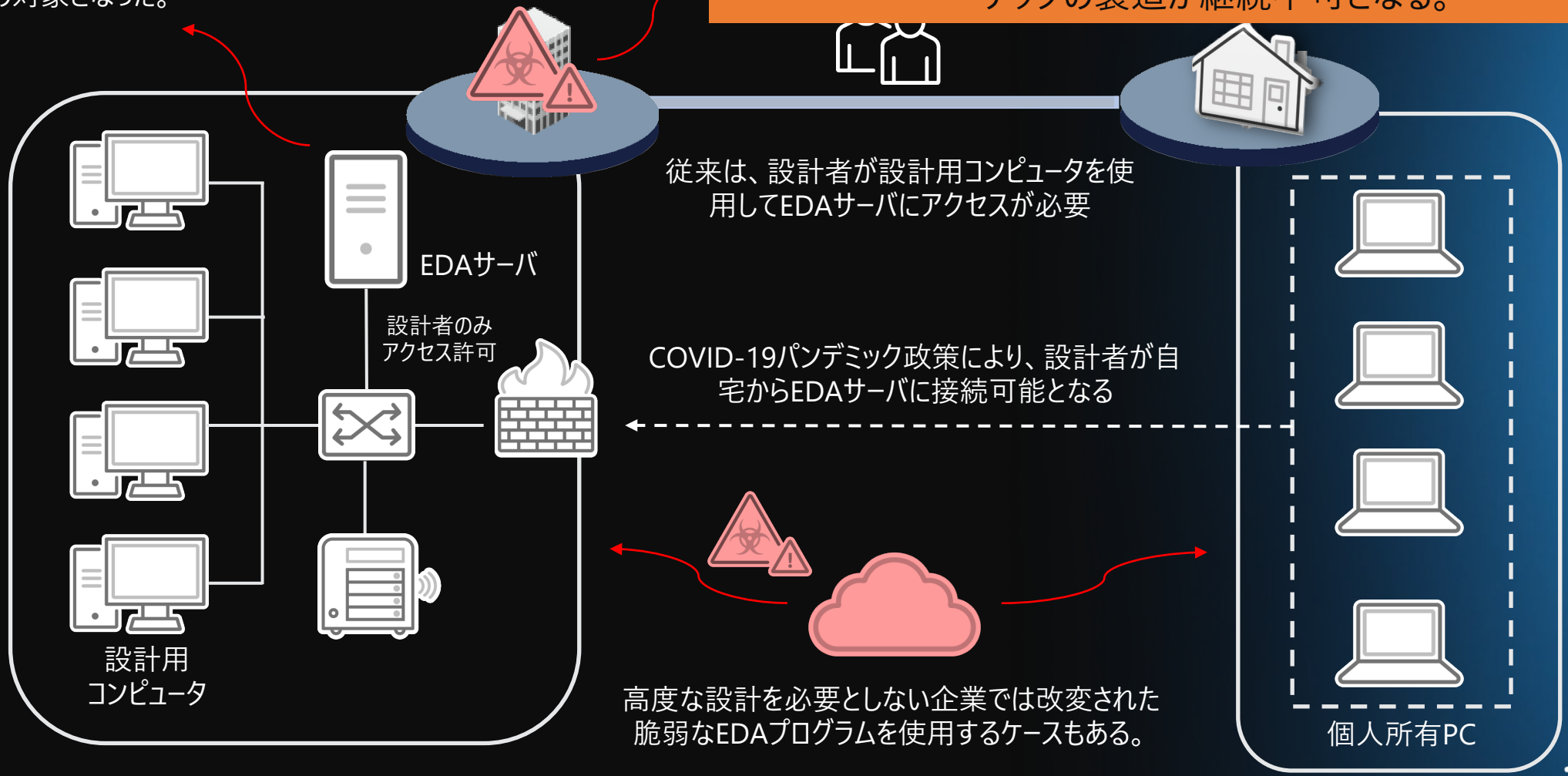


半導体企業の想定インシデント・シナリオ

2021年に一部のEDA製品がLog4jの脆弱性の対象となった。

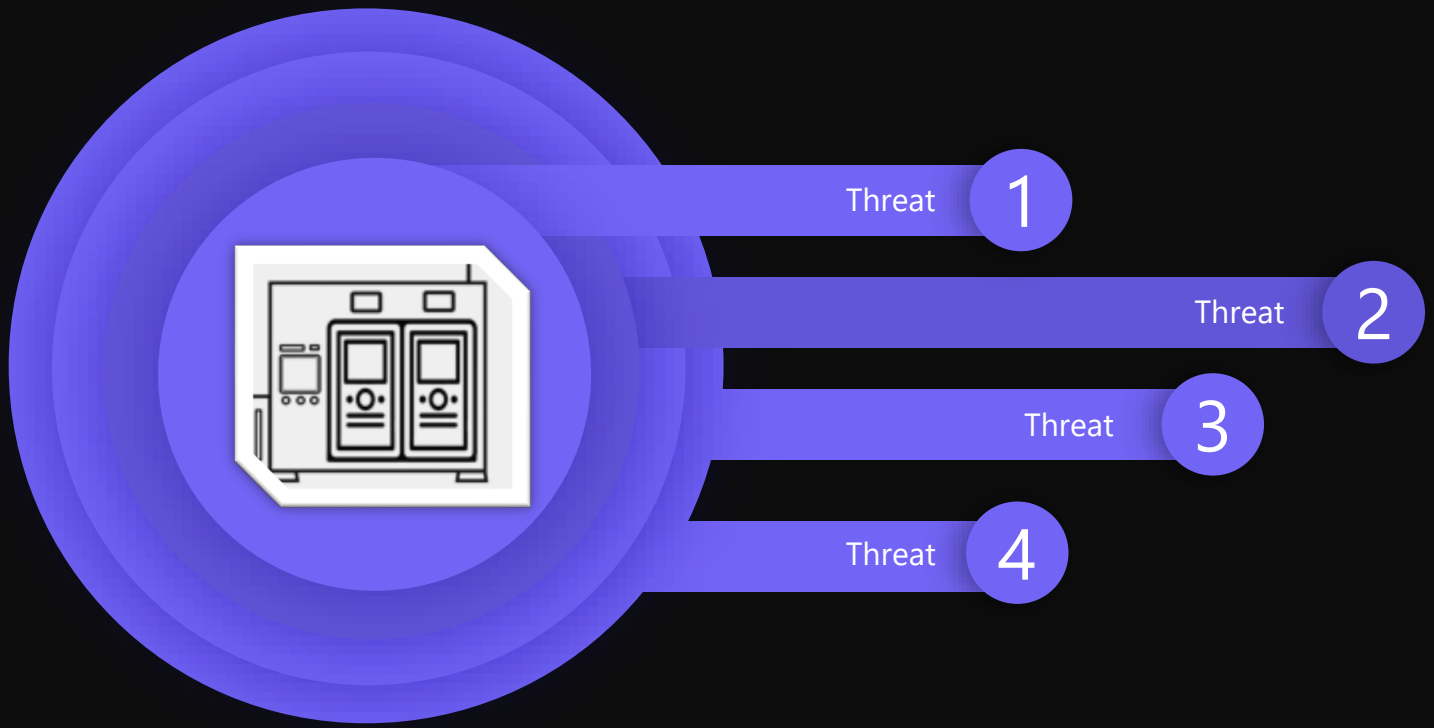
ファブレス半導体企業

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）

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り、攻撃者の攻撃ベクトルを増加させる。

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

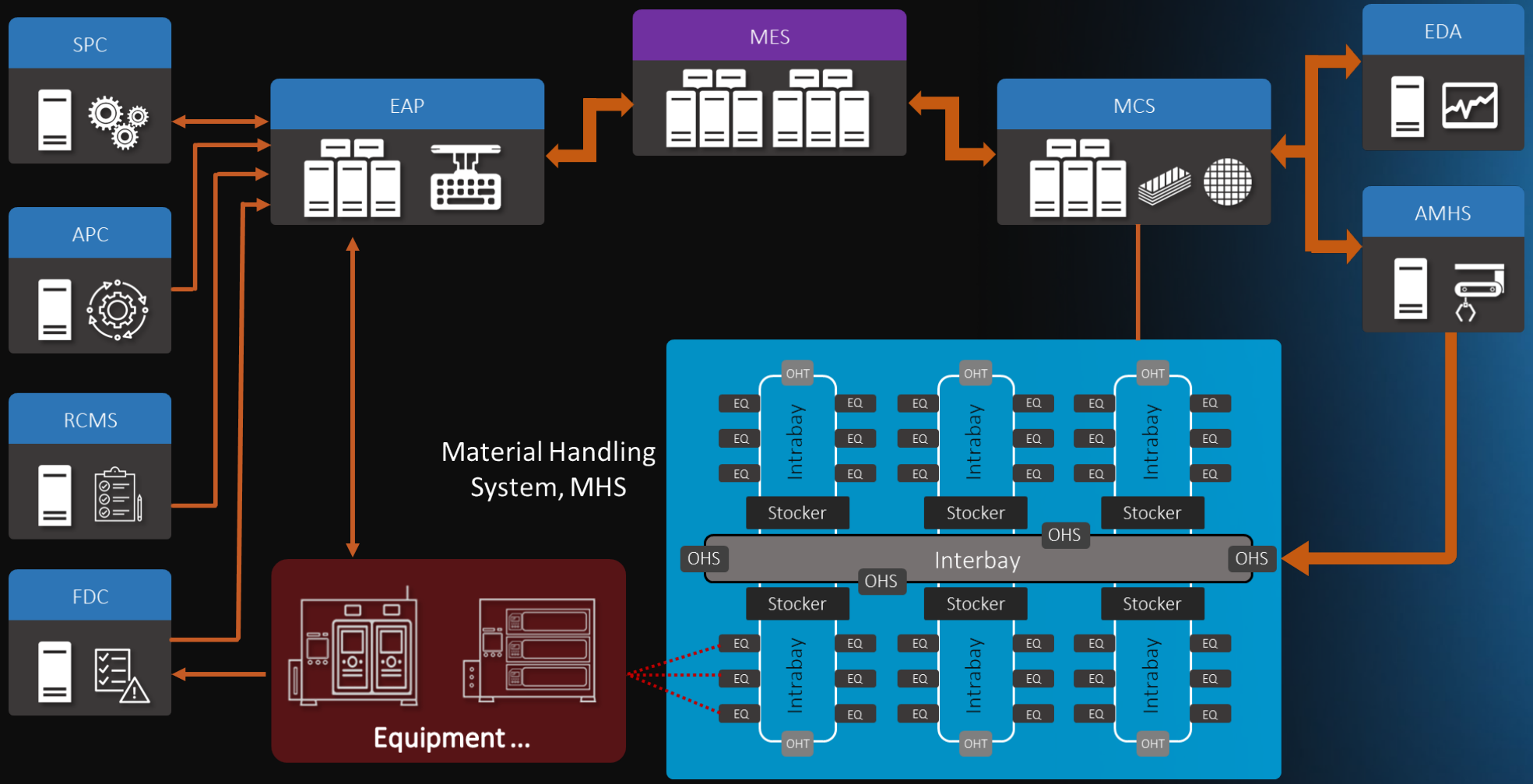
不適切なネットワークセグメンテーションにより、マルウェアの蔓延・拡散が容易となる。

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。

膨大な数の資産が稼働するファウンドリ環境

- 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必要



txOne networks

SEMI E187
（ファブ装置のサイバーセキュリティ仕様）

SEMI E187とは？

- Specification for Cybersecurity of Fab Equipment（ファブ装置のサイバーセキュリティ仕様）

- ファブ装置へのサイバー攻撃の急増を受け、SEMI台湾地区 Information & Control 技術委員会、Fab & Equipment Information 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月に出版。

- 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の目的と対象

- 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包括的に定義。

- 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等を対象として想定。

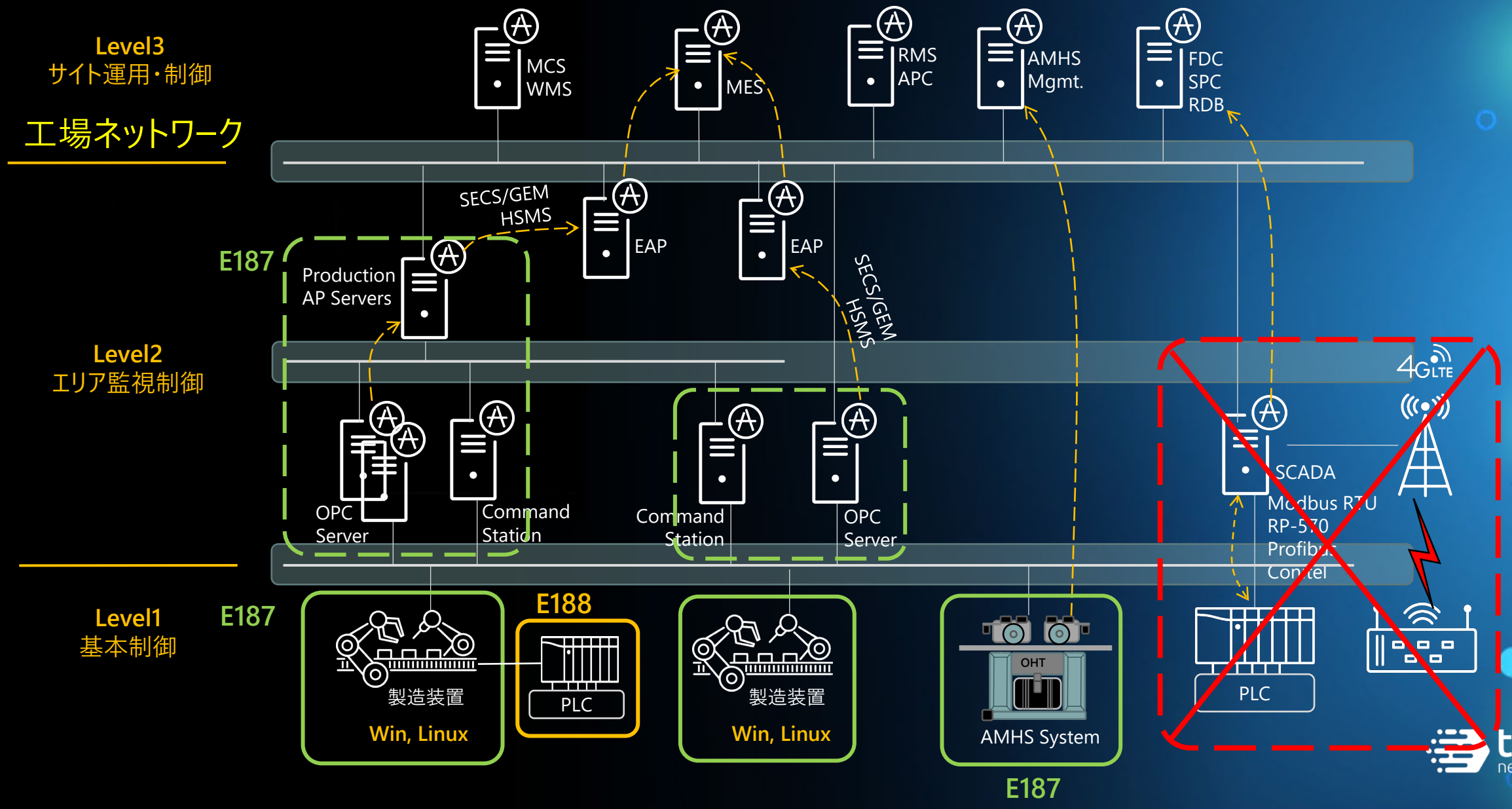
- 装置サプライヤーは装置の設計段階で本規格の要求事項を考慮すると同時に、設備所有者がセキュリティポリシーを策定する際のセキュリティベースラインとして活用することも期待。

E187 / E188 の位置づけ

アイテム	E187	E188
テーマ	ファブ装置のサイバーセキュリティ仕様	マルウェアフリーで装置を導入する為の仕様
フェーズ	製造装置を導入するフェーズ	製造装置の導入、運用、保守のフェーズ
スコープ	装置サプライヤ向け • 生産設備 • マテハン自動化システム (AMHS) • Windows, Linux OS搭載装置 • SCADA、PLCは対象外	装置サプライヤ向け • 生産設備 • マテハン自動化システム (AMHS) • SCADAは対象外、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	• 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E188の対象設備



SEMI E187 要求事項のスコープ

①オペレーティングシステム

②ネットワークセキュリティ

③エンドポイント保護

④セキュリティモニタリング

SEMI E187の各要求事項

①オペレーティングシステム

1. 装置搭載OSに関する要求
2. パッチ適用手順の技術文書作成

②ネットワークセキュリティ

3. 安全な通信転送プロトコルのサポート
4. ネットワーク構成の技術文書作成

③エンドポイント保護

5. 脆弱性の軽減
6. マルウェアスキャン実行
7. アンチマルウェア対策
8. システムハードニング
9. 認証機構の適用
10. アクセス権の設定

④セキュリティモニタリング

11. セキュリティイベントログ
12. ログタイプ

オペレーティングシステムに対する要求事項

①オペレーティングシステム

1. 装置搭載OSに関する要求
2. パッチ適用手順の技術文書作成

■装置サプライヤーはOSベンダーによってサポートされていない
OSを搭載した装置を出荷してはならない。

Equipment supplier **shall not ship** equipment with OS that are not supported by the OS vendor

＜考慮すべき事項＞

サポート終了したOSの使用を継続する場合

クライアントOS	Latest update or service pack	メインストリームサポート	延長サポート
Windows XP	Service Pack 3	2009/4/14	2014/4/8
Windows Vista	Service Pack 2	2012/4/10	2017/4/11
Windows 7	Service Pack 1	2015/1/13	2020/1/14

https://docs.microsoft.com/en-us/lifecycle/

オペレーティングシステムに対する要求事項

①オペレーティングシステム

1. 装置搭載OSに関する要求
2. パッチ適用手順の技術文書作成

■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こと。

Equipment suppliers **shall provide** the procedure to apply the patches or the security updates

＜考慮すべき事項＞

- タイムリーなパッチ適用が困難な場合
- サポート終了したOSの使用を継続する場合

システムパッチアップデートレポート

1.0 目的
....
2.0 スコープ
....
3.0 責任と役割
....
4.0 プロセス
　4.1 .....
　4.2 ....

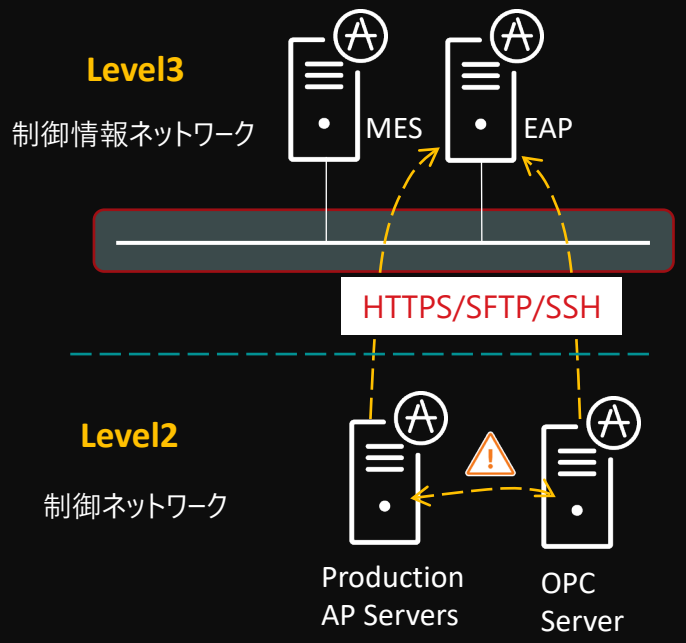
システムパッチパッケージ情報

Item	Result
パッケージ情報 . Name, version	
1. ソフトウェア互換性テスト	
2. ソフトウェアパッケージ依存性	
3. パフォーマンスへの影響分析	
4. サイドエフェクト調査	
5. 機能テスト	

ネットワークセキュリティに関する要求事項

②ネットワークセキュリティ

3. 安全な通信転送プロトコルのサポート
4. ネットワーク構成の技術文書作成



■ウェブサービス、ファイル転送、ターミナルサービス（telnet）のアプリケーションを提供する機器は、HTTPS、SFTP、SSHなどの安全な伝送プロトコルをサポートすること。

Equipment that provides applications of web service, file transfer, and terminal service (telnet) **shall support secure** transmission protocols, like HTTPS, SFTP and SSH.

＜考慮すべき事項＞

- デバイス同士の通信（東西通信）のセキュリティ

ネットワークセキュリティに関する要求事項

②ネットワークセキュリティ

3. 安全な通信転送プロトコルのサポート
4. ネットワーク構成の技術文書作成

装置サプライヤーは、ネットワーク構成に関する文書を提供すること。
- ネットワークプロトコル／ポートの使用状況
- ネットワーク構成やポート変更の保守手順

Equipment supplier **shall provide** documentation for network configurations
- Network protocols/ports usage
- Instructions for changing the network configuration if supported

＜考慮すべき事項＞

- 既知の攻撃で多用されているポートやプロトコルの制限
  （例：WannaCryが使用するSMB、445番ポートなど）

ネットワークプロトコル・ポート使用状況レポート

対象	ポート	目的
装置名		
Protocol / Port 使用リスト		
.Modbus TCP	502	
.SMB	445	
.HTTPS	443	

エンドポイント保護の要求事項

③エンドポイント保護

5. 脆弱性の軽減
6. マルウェアスキャン実行
7. アンチマルウェア対策
8. システムハードニング
9. 認証機構の適用
10. アクセス権の設定

■装置出荷前に脆弱性スキャンを実施し、スキャン報告書を提出すること。

Equipment supplier **shall perform** vulnerability scan prior to equipment shipment and deliver a scanning report

＜考慮すべき事項＞

- 確認された重要かつ緊急度の高い脆弱性に即時にパッチ適用ができない場合

SCAP認証を受けたOpenSCAP等のスキャンツールの使用を推奨

Critical & High

脆弱性調査報告書

アイテム	結果
検索ツール情報	
実施日	
検索対象ホスト情報	
脆弱性調査結果 . CVE識別子 . NVD深刻度 . 脆弱性詳細	

エンドポイント保護の要求事項

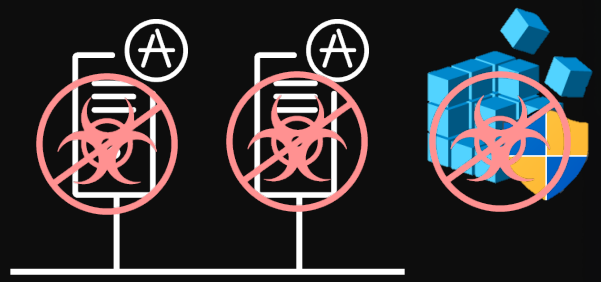
③エンドポイント保護

5. 脆弱性の軽減
6. マルウェアスキャン実行
7. アンチマルウェア対策
8. システムハードニング
9. 認証機構の適用
10. アクセス権の設定

■装置サプライヤーは、装置出荷前にマルウェアスキャンを実施し、スキャンレポートを提供すること。

Equipment supplier **shall perform** malware scan prior to equipment shipment and deliver a scanning report

オペレーティングシステム



OSのマルウェア検索
（レジストリ検索も推奨）

マルウェア検索レポート

アイテム	結果
システム情報 . デバイス名 . OS情報	
ウイルス対策ソフト . 検索エンジンver . 検索日時	
検索結果	
検査日時	
検査者	サイン

エンドポイント保護の要求事項

③エンドポイント保護

5. 脆弱性の軽減
6. マルウェアスキャン実行
7. アンチマルウェア対策
8. システムハードニング
9. 認証機構の適用
10. アクセス権の設定

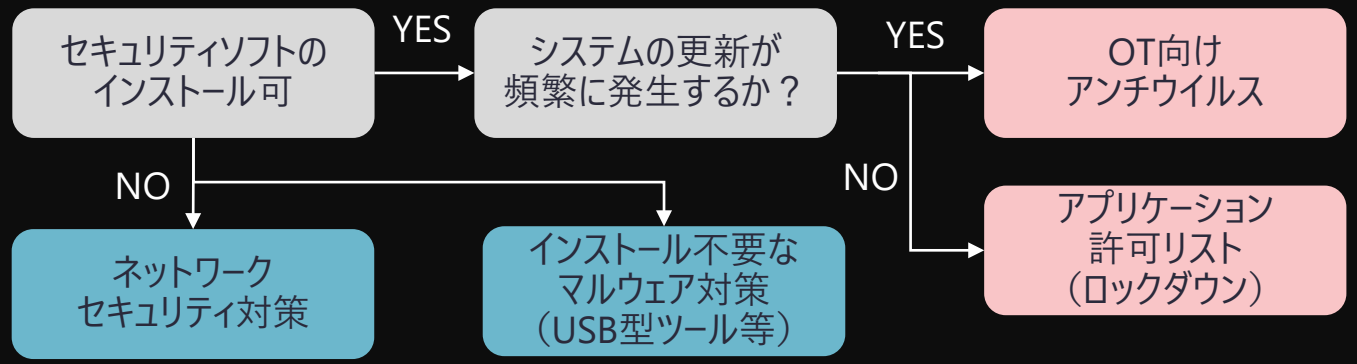
■装置サプライヤーはファブ装置と互換性の取れたマルウェア対策ソリューションの文書を提供すること。

- マルウェア対策ソリューション（OT向けアンチウイルス）
- アプリケーション許可リスト（ロックダウン）

Equipment supplier **shall provide** documentation of the **compatible** anti-malware solutions for the fab equipment.

- Anti-Malware Solutions
- Application allow list control mechanisms

- 通信環境、装置のHWスペック、装置パフォーマンスへの影響等を考慮



アンチマルウェアソフトの互換性リスト

アンチマルウェアソリューション名

アイテム	結果
調査日	
テストケース概要	
テストケース レポート詳細	

エンドポイント保護の要求事項

③エンドポイント保護

5. 脆弱性の軽減
6. マルウェアスキャン実行
7. アンチマルウェア対策
8. システムハードニング
9. 認証機構の適用
10. アクセス権の設定

■装置サプライヤーは、以下を含むセキュリティハードニングに関する文書を提供すること。

- USB や DVD±RW などの I/Oインターフェースの有効化・無効化の手順
- OSの未使用ユーティリティやサービスを無効にする手順
- I/Oインターフェース、ユーティリティサービスを無効にするためのハードニング手法

Equipment suppliers **shall provide** documents regarding **security hardening** including

- Enable/disable I/O interfaces such as USB or DVD±RW.
- Disable unused OS utilities and services.

エンドポイント保護の要求事項

③エンドポイント保護

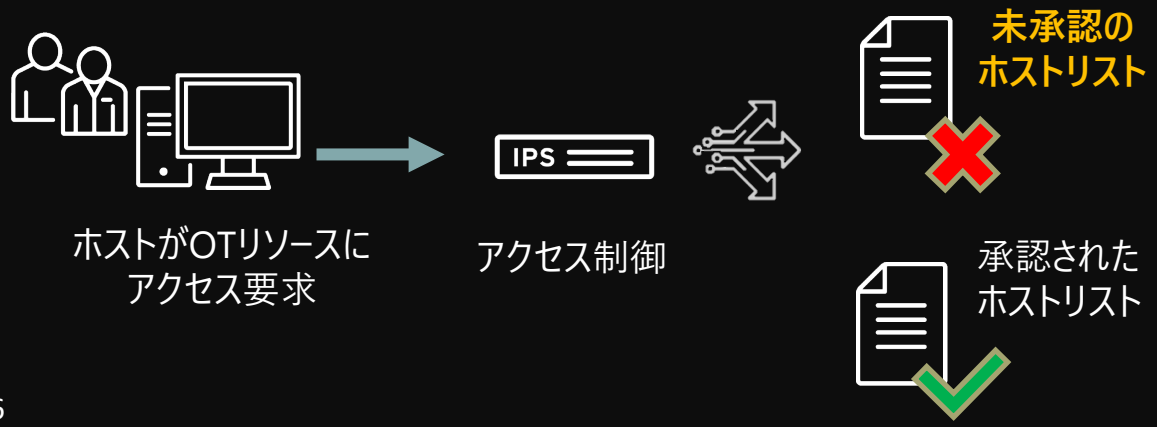
5. 脆弱性の軽減
6. マルウェアスキャン実行
7. アンチマルウェア対策
8. システムハードニング
9. 認証機構の適用
10. アクセス権の設定

■以下のシステムに対する接続に認証機構を適用すること。

- オペレーティングシステム
- 装置のアクセス制御

Authentication mechanism(s) **shall be used** for
- Operating system
- Equipment access control

- ユーザ認証と承認済ホストの許可を組み合わせ、よりセキュアに



エンドポイント保護の要求事項

③エンドポイント保護

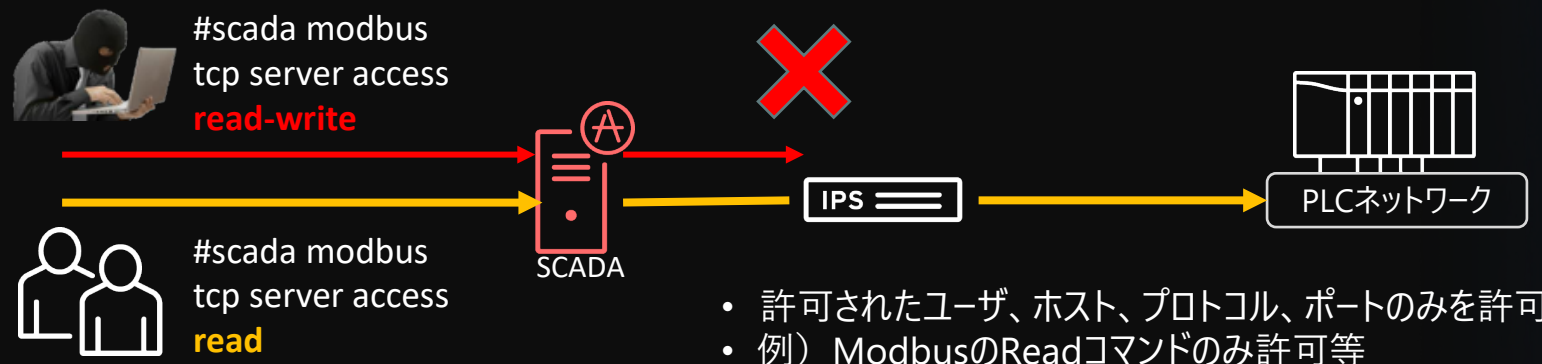
5. 脆弱性の軽減
6. マルウェアスキャン実行
7. アンチマルウェア対策
8. システムハードニング
9. 認証機構の適用
10. アクセス権の設定

■装置サプライヤーは以下をサポートするアクセス権/特権の認可ソリューションを提供する

- 職務権限の分離
- 最小権限ポリシー

Equipment suppliers **shall provide** access rights/privileges authorization solutions to support

- Segregation of duties
- Least privilege policy



- 許可されたユーザ、ホスト、プロトコル、ポートのみを許可
- 例）ModbusのReadコマンドのみ許可等

職務権限の分離と最小権限ポリシー

セキュリティモニタリングの要求事項

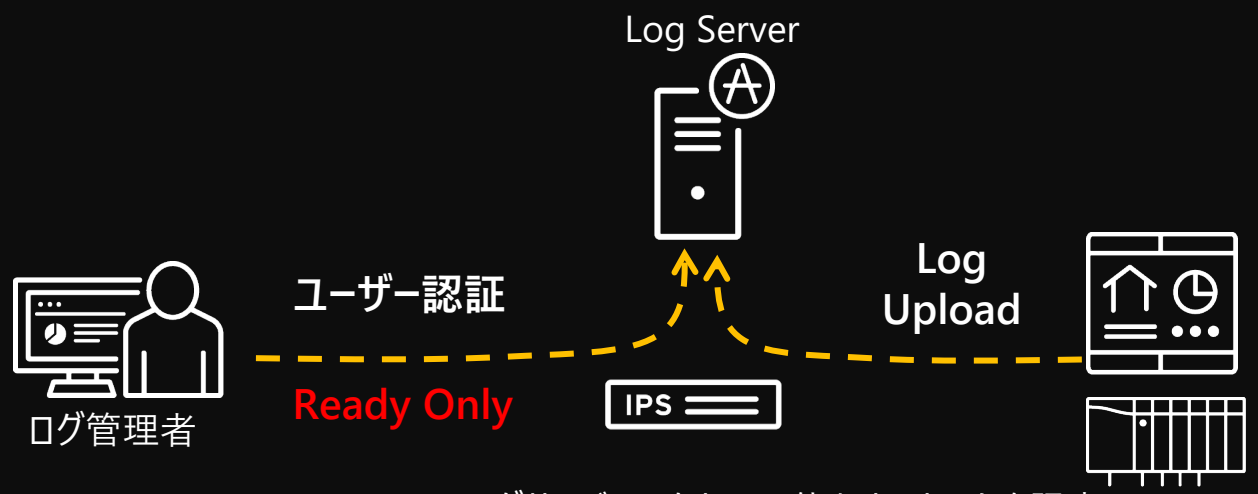
■ファブ装置は以下のセキュリティイベントログを記録/出力できること。

- システム
- アプリケーション

Fab equipment shall be capable of recording and exporting security event logs, including
- System
- Application

④セキュリティモニタリング

11. セキュリティイベントログ
12. ログタイプ



ユーザー認証

Ready Only

システム

Time stamp: 2021/06/29 15:36
Source : 23.5.6.8
Account : domain ¥ user
Role : Administrator
Activity : Console logon

許可されていないアクセス

アプリケーション

Time stamp: 2021/06/29 15:46
Source : 172.16.3.5
Protocol : Modbus TCP
Function call : 15
Command : xxxxxx

- ログサーバにアクセス可能なホスト・人を限定
- ログをアップロードできる装置を限定

セキュリティモニタリングの要求事項

④セキュリティモニタリング

11. セキュリティイベントログ
12. ログタイプ

■イベントログは以下内容を含むこと。
- アクセスコントロール
- 設定変更
- システムエラー

Event logs **shall include** following types,
- Access control
- Configuration changes
- System errors

アクセスコントロール

Time stamp: 2021/06/29 15:36
Source : 23.5.6.8
Account : domain ¥ user
Role : Administrator
Activity : Console logon

設定変更

Time stamp: 2021/06/29 15:46
Source : 172.16.3.5
Protocol : Modbus TCP
Command :
scada modbus tcp server access
permit 198.51.100.200

システムエラー

Time stamp: 2021/06/29 15:46
Source : SChannel
Event ID : 36871
Error state : 10013
Description :
A fatal error occurred while creating a TLS client credential

SEMI TAIWAN 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）

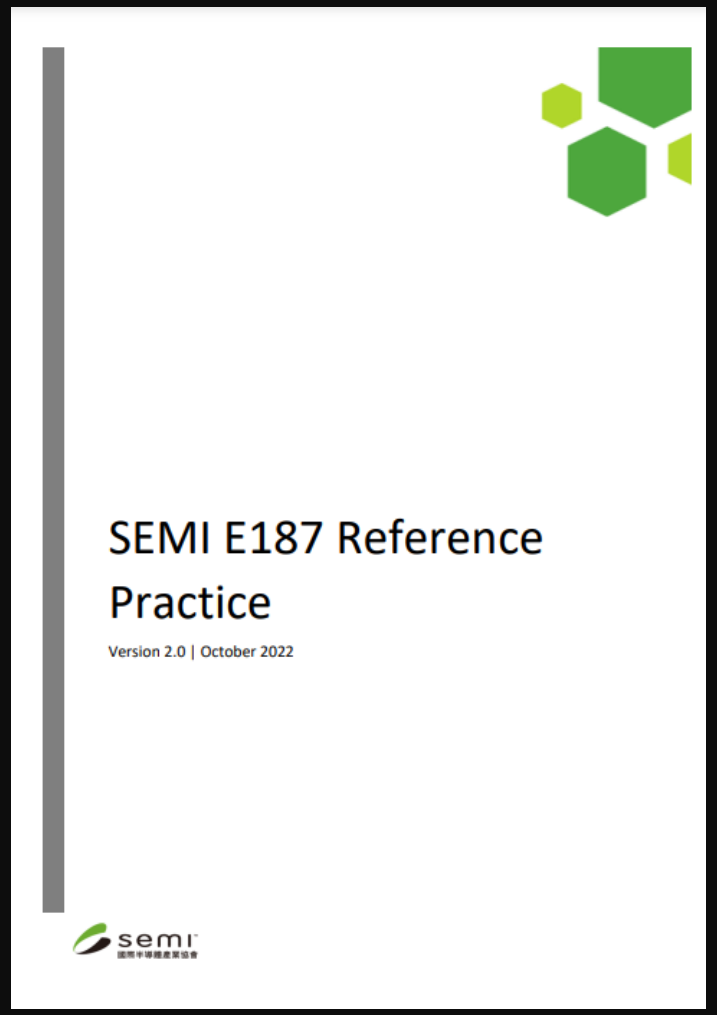
FOCUS 03

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

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

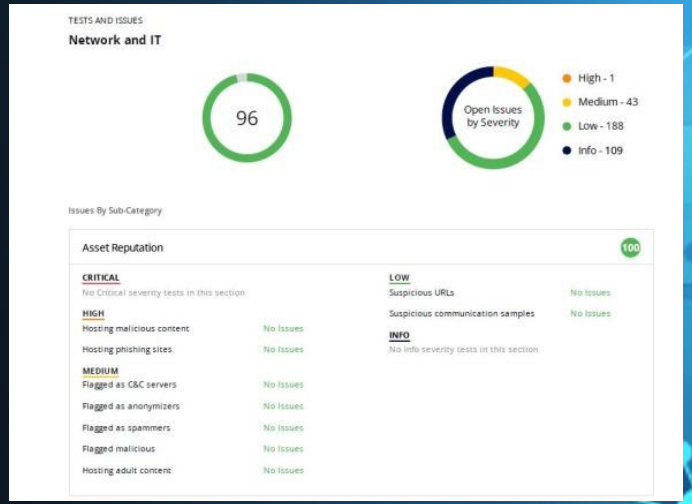
- Windows XP, Windows Vista and Windows 7 indicated in Table 1 are examples of end-of-support operating systems. When Microsoft stopped issuing updates and patches, these operating systems rapidly became orders of magnitude more vulnerable to security threats. Equipment vendors should not ship equipment 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.

半導体情報セキュリティリスク評価サービス（台湾SEMI）

- SEMI Taiwanが2022年11月5日より「半導体情報セキュリティリスク評価サービス」の提供を開始
- 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アンケートにより、リスクスコアリングとリスク状況を把握可能
- 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

半導体情報セキュリティリスク評価サービス（台湾SEMI）

メニュー	オプションA：Entry Level	オプションB：Experts Level
内容	• サービス開始後 7 日間の継続的な監視 • サービス期間中のリスク評価記録の照会 • リスク評価レポート (情報セキュリティ状況スコアおよび同業他社との比較を含む) • 問題の発見と改善提案 • SEMI情報セキュリティ評価	• サービス開始後 30 日間の継続的な監視 • サービス期間中のリスク評価記録の照会 • リスク評価評価レポート (情報セキュリティ状況スコアおよび同業他社との比較を含む) • 問題の発見と改善提案 • SEMI 情報セキュリティ評価 • 中長期の評価結果の記録
価格	SEMI非会員：約127,000円 (28,875台湾ドル) SEMI会員：約99,000円 (22,575台湾ドル)	SEMI非会員：約383,000円 (87,150台湾ドル) SEMI会員：約297,000円 (67,515台湾ドル)
その他	• 12/5~12/19までSEMI会員向けに本サービスの無償トライアルサービスを提供（申込は12/1まで） • 本評価サービス利用後、評価スコアを向上させるために、CHT Security（中華電信のセキュリティ子会社）のセキュリティコンサルティングサービスを利用することが可能。	

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

サプライチェーンリスクにどう向き合うべきか？

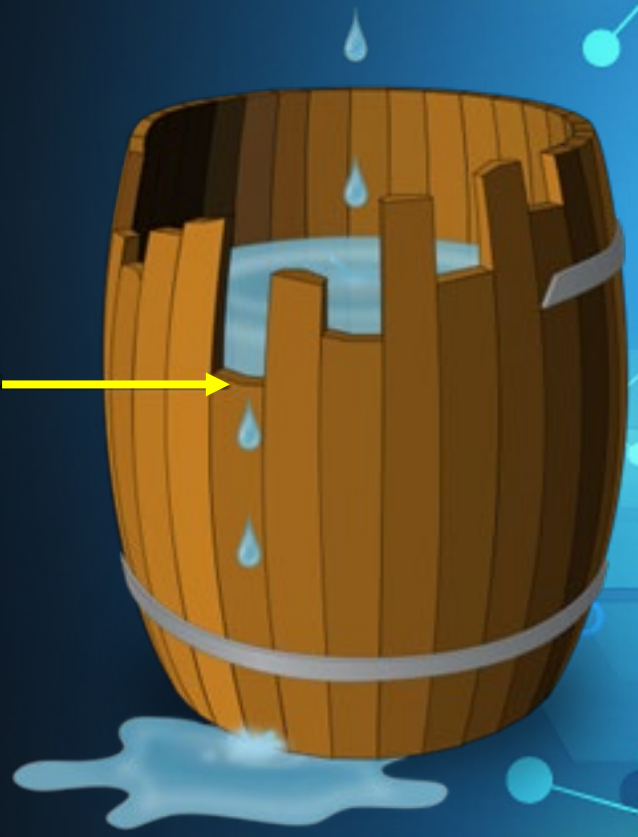
「セキュリティの樽」
貯められる水の量は最も短い板に依存する。

- 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

順位	組織	前年順位
1位	ランサムウェアによる被害	1位
2位	サプライチェーンの弱点を悪用した攻撃	3位
3位	標的型攻撃による機密情報の窃取	2位

出典：IPA 情報セキュリティ10大脅威 2023

最もセキュリティレベルが低い企業



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（特に脆弱性対策）

OTセキュリティ推進のトリガ

サイバー攻撃被害によりビジネスにダメージを受ける

該当企業は対応を進めるが、
他社は対岸の火事。。。

Industry Leading Company

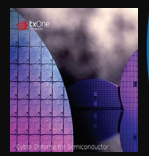
各産業のリーディング企業がサプライチェーン企業を巻き込んで推進

一部の産業ではガバナンスを効かせた取り組みが進みつつあるも、限定的

セキュリティ規格やガイドラインによって対応が求められる

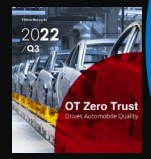
推進者の予算確保や経営層の説得がしやすい

各産業の実態に即した実践的な規格やガイドラインの策定・推進（啓蒙・評価制度等）が重要



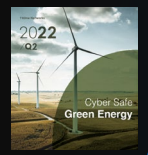
SEMICONDUCTOR

SEMI
E 187/188



AUTO

JAMA/JAPIA/Auto-ISAC
ISO21434/Security Guideline



UTILITY

JE-ISAC
Security Guideline

Other Verticals

txOne networks

まとめ

- SEMI E187は「ファブ装置のサイバーセキュリティ仕様」として、4つの主要分野（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）の基本的なセキュリティ要件を定義

- SEMI E187は、半導体装置メーカーが自社の情報を保護する上で有効なだけでなく、サプライチェーン全体が協力して、業界全体として情報セキュリティの強化を図ることを目指す。

- リファレンス・プラクティスの開発を通じた、規格の普及啓蒙活動の他、サプライチェーンに対する情報セキュリティ評価サービスの提供など、グローバルレベルで半導体産業のセキュリティレベルを底上げする活動が推進されている。

Keep the Operation Running