第１４回 工場セキュリティ啓発・連続セミナ 講演資料

半導体製造装置で実施したセキュリティ対策

2025.2.28

日本電子株式会社
ＳＥ技術本部　金田 源太

本テーマの紹介

SEMI規格 E187-0122
(ファブ装置のサイバーセキュリティ仕様)

半導体工場に装置を納入する際にSEMI E187への適合が求められます。

SEMI E187に適合するにはOSの脆弱性対策、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関する12個の要件に適合しなければなりません。

本講演ではE187に適合した半導体製造装置で実施したセキュリティ対策について紹介します。

SEMI: 国際半導体製造装置材料協会 (Semiconductor Equipment and Materials International)
ファブ: 半導体工場

Contents

内容

1. 会社紹介、自己紹介
2. 装置のセキュリティ対策を始めたきっかけ
3. SEMI E187の特徴、スコープ、構成
4. セキュリティ対策完了までのプロセス
5. 審査過程
6. オンサイト試験
7. まとめ

会社紹介

img src: https://www.jeol.co.jp/corporate/

日本電子株式会社 JEOL

本社所在地	東京都昭島市武蔵野3丁目1番2号
事業内容	理科学計測機器、半導体関連機器、産業機器、医用機器の製造 ・ 販売・ サービス
設立年	1949年
従業員数	3,435人
URL	https://www.jeol.co.jp/

製品紹介

img src: https://www.jeol.co.jp/products/

自己紹介

金田 源太

日本電子株式会社
SE技術本部 PL技術開発部
部長

1998年 日本電子入社、半導体機器技術本部 設計部に配属、
　　電子ビーム描画装置の電気設計に従事
2003年 テクニカルサービス部に配属、技術サポートに従事
2007年 技術開発部に配属、電子ビーム描画装置の開発に従事
2011年 設計部に配属、電子ビーム描画装置の電気設計に従事
2019年 技術開発部に配属、電子ビーム描画装置の開発に従事

SEMI S2、EMC、機械指令、NFPA 79、その他規格対応に従事
SEMI委員会（社内技術委員会）委員長（2015年～）⇒ E187に取り組んだ

対策開始から審査開始までの14か月

装置のセキュリティ対策を始めたきっかけ

2022年1月 SEMI E187-0122発行

SEMI初となるサイバーセキュリティガイドラインが出版された
https://www.semi.org/jp/standards-watch-2022-March/SEMI-publishes-first-cybersecurity-standards

当時はサイバーセキュリティ対策に積極的ではなかったため見過ごした。

2023年4月21日 台湾の半導体メーカーがサプライヤに説明会を実施

- **SEMI E187適合が購入仕様に追加された**
- **2024年12月に猶予期間が終了し、例外は許可されない**
- **適合を検証するためのチェックリストを提供する**
- 追加料金は認められない
- 新規に開発されたすべての装置および既存のツールの新規出荷に適用される
- インストール済みのツールには適用されない

2025年1月1日までにSEMI E187に適合する
ことが目標（20か月しかない）

SEMI E187の特徴とスコープ

特徴

- 半導体製造装置向け包括的かつ基本的なサイバーセキュリティ要件
- 半導体製造工場に装置やサービスを提供するベンダーが実施するスタンダード（サプライチェーンのスタンダード）
- 主に装置を出荷する前に行う要件

適用範囲

- 半導体製造装置及び自動マテリアルハンドリングシステム
- Windows®またはLinux®がインストールされているファブ装置のコンピューティングデバイス
- プログラマブルコントローラ(PLC)、監視制御およびデータ取得(SCADA) には適用されない

SEMI E187の構成

適合・不適合・NAでチェックシートに回答する

基本要求事項 4項	要件 12件	概要
オペレーティングシステム (OS)のサポート	2件	OSのサポート期間内であること パッチを適用する手順があること
ネットワークセキュリティ	2件	安全な転送プロトコルの使用 ネットワーク構成の文書を提供
エンドポイント保護	6件	脆弱性スキャンとマルウェアスキャン マルウェア対策ソリューション指定 入出力インターフェースの無効化 未使用ユーティリティとサービスの無効化 認証と認可の使用、権限の制限
セキュリティ監視	2件	セキュリティイベントログの記録

認証機関のサービス

自力では要件への対応方法がわからない。

img src: https://www.bureauveritas.jp/electronics-wireless/newsroom/231027

適合証明書（VoC：Verification of Conformity）は必須ではないが認証機関のサービスを利用するのが最適だと考えて審査を依頼した。

対策完了までのプロセス（タイムライン）

スタンダード解釈と対応方針策定 — 2023/4 ☆
- ガイドラインの翻訳と対策方針の検討

セキュリティ製品検討 — 2023/10～
- 市販のセキュリティ製品の採用を検討

準備期間 14か月

認証機関の事前審査
- 事前トレーニング、審査基準の説明（録画） — 2024/6 ☆
- 資料のアセスメント — 2024/8～10

事前審査対応 — 2024/6～10
- 事前審査での指摘事項への対応

認証機関の立会い審査
- 立会い審査（口頭試験、実機試験） — 2024/11/1
- 適合証明書発行 — 2024/11/27

実施期間 5か月

審査開始から適合証明書発行までの5か月

認証機関の事前審査
事前審査対応
立会い審査

審査過程（１）

SEMI E187-0122の要件（1, 2）コンピュータオペレーティングシステムのサポート

1. 装置サプライヤは、OSベンダのサポートが切れたOSを含む装置を出荷してはならない
2. 装置サプライヤは、パッチまたはセキュリティアップデートを適用する手順を提供する必要がある

審査前の解釈

- OSの変更は動作確認が大変なので困る、パッチの適用は客先環境では難しい
- IPS（不正侵入防止システム）を導入するなどハード側で対策を行う方がよい

セキュリティ製品検討

- OT用IPSを使えばOSにパッチを適用しないでもセキュリティ対策できる
- OSサポート終了後もOSの脆弱性に対処できる

認証機関の事前審査

- IPSを使った脆弱性対策は有効だが要件1、2とは別の話
- 要件2は「アップデート手順」を作ることであり適合するにはエビデンスが必要

事前審査指摘への対応

- Windows®10からWindows®11へアップデートを実施
- 各PCのOSバージョンとサポート終了時期（EOL）のリスト、EOLの証拠を文書化
- パッチ評価手順と動作確認プロセスを文書化

OT用IPSの例

審査過程（２）

SEMI E187-0122の要件（3, 4）ネットワークセキュリティ要件

3. HTTP、FTP、telnet の転送プロトコルを提供する機器は、HTTPS、SFTP、SSH などの安全な転送プロトコルをサポートしなければならない
4. 通信プロトコル/ポートの使用法を含むネットワーク構成の文書を提供しなければならない。ネットワーク構成を変更するための保守手順を提供しなければならない。

審査前の解釈

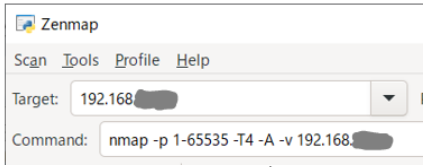
- 工場と装置の通信だけが要件の対象なので装置内は実施不要（要件3, 4とも）
- 工場と装置の通信にはHTTP、FTP、またはTelnet機能がないのでNA

認証機関の事前審査

- 要件3、4は装置内部にも適用しなければならない
- エビデンスが必要、Wireshark などのツールを使用して通信プロトコルを検証する
- 通信 プロトコル/ポートの使用状況をNmap などのポートスキャンツールを使用して確認する

事前審査指摘への対応

- HTTPSに対応し、転送プロトコルのリストを文書化
- ポート番号、通信プロトコル、使用目的のリストを文書に記載
- Nmap結果を文書に記載
- Wiresharkの結果を認証機関に送付



Nmapの例

審査過程（３）

SEMI E187-0122の要件（5, 6）エンドポイント保護要件

5. 機器の出荷前に脆弱性スキャンを実施し、重大な脆弱性がないことを示したスキャンレポートを納入しなければならない。
6. 装置の出荷前にマルウェアスキャンを実施し、スキャンツールの名前とバージョン、スキャン範囲、スキャン日を含むスキャンレポートを納入しなければならない。

審査前の解釈

- 市販のスキャンツールでマルウェアと脆弱性スキャンを行う

セキュリティ製品検討

- 脆弱性スキャンとマルウェアスキャンを行えるスキャンツールがある

スキャンツールの例

認証機関の事前審査

- 市販のスキャンツール使用可（スキャンツールがないOSはSBOMで審査する）
- スキャン ツールの名前、バージョン、スキャン範囲などの情報が必要

事前審査指摘への対応

- スキャンツールを使用して脆弱性スキャンとマルウェアスキャンを実施した
- スキャンツールが自動作成するレポートをエビデンスとして使用

審査過程（４）

SEMI E187-0122の要件（7）エンドポイント保護要件

7. 装置サプライヤは、製造装置に対応するマルウェア対策ソリューションを指定する文書を提供しなければならない。

審査前の解釈

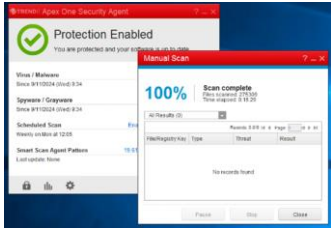
- 互換性のあるマルウェア対策ソリューションの推奨設定を指定して文書化する

認証機関の事前審査

- 文書内で指定したマルウェア対策ソリューションがデバイスとの互換性があるエビデンスが必要

事前審査指摘への対応

- マルウェア対策ソリューションの設定とスキャン結果のスクリーンショットを文書に追加



マルウェア対策ソリューションの例

審査過程（５）

SEMI E187-0122の要件（8）エンドポイント保護要件

8. 以下を含むセキュリティ強化に関する文書を提供しなければならない。
   - USBやDVD Rewritable (DVD±RW)などの入出力インターフェースの無効化
   - 未使用のオペレーティングシステムのユーティリティとサービスの無効化

審査前の解釈

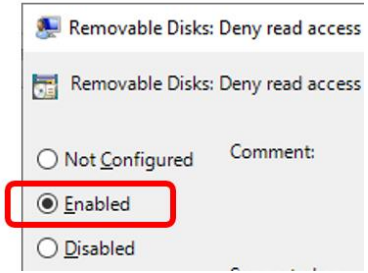
- I/O無効化の手順を文書化する（ローカルグループポリシーを使用）
- ユーティリティとサービスの無効化の手順を文書化（コントロールパネル、管理ツールを使用)

認証機関の事前審査

- 各ユーティリティとサービスを使用する具体的な目的を説明する必要がある
- 「Windows® 既定のサービス」では使用理由として不十分

事前審査指摘への対応

- ユーティリティとサービスを可能な限り無効化して動作確認した
- ユーティリティとサービスのリストのスクリーンショットを文書に追加
- ユーティリティとサービスの具体的な使用目的を文書に追加



USB 無効化手順の例

※ アップデートすると自動で有効になるサービスがある。注意が必要。

審査過程（６）

SEMI E187-0122の要件（9, 10）エンドポイント保護要件

9. オペレーティングシステムおよび装置のアクセス制御に認証メカニズム(Authentication)が使用されなければならない。
10. 職務の分離の原則と最小権限の原則をサポートするため、アクセス権認可ソリューションを提供しなければならない。

審査前の解釈

- エンドポイント保護なので工場と接続されているPCのみに適用すればよい

認証機関の事前審査

- すべてのPCに要件を適用する必要がある
- オペレーター、メンテナンス員、プロセスエンジニアなど役割ごとのユーザーIDとパスワードが必要

事前審査指摘への対応

- 役割ごとにユーザーIDとパスワードを準備してユーザーリストを文書化した
- ユーザーごとの権限について上記文書に記載した
- ユーザーアカウントのスクリーンショットを上記文書に記載した

審査過程（７）

SEMI E187-0122の要件（11, 12）セキュリティモニタ要件

11. Fab装置は、システムセキュリティイベントログおよびアプリケーションセキュリティイベントログを記録およびエクスポートできなければならない。
12. アクセス制限、設定変更、システムエラーはイベントログとして残す必要があり、イベントログには、イベントタイプ、イベントの説明、ユーザーアカウント、タイムスタンプを構成しなければならない。

審査前の解釈

- Windows® のイベント ログを利用する

認証機関の事前審査

- Windows® システムのログだけではなくアプリケーションセキュリティ イベント ログも必要
- アクセス制御、設定変更、システムエラーのログが記録されるエビデンスが必要

事前審査指摘への対応

- 自社製アプリケーションにセキュリティイベントログ機能を追加
- 認証の失敗、パッチの適用、システムエラーのログのスクリーンショットを上記文書に記載した

SEMI E187オンサイト試験

認証機関のオンサイト審査

- **口頭試験**（日本電子の理解度確認）
  事前に提出した資料に関しての質問を口頭で答えられるか試験

- **実機試験**（事前に提出した資料と実機が同じ状態か確認）
  12要件からランダムに選んでその場で実施状況を確認した
  - ✓ OSのバージョン確認
  - ✓ パッチ適用の手順確認とイベントログに記録されることを確認
  - ✓ 脆弱性スキャンの実施
  - ✓ 入出力デバイス無効化設定の確認
  - ✓ 有効になっているサービスの用途に関する質疑応答
  - ✓ ユーザーリストの確認と認証メカニズムの確認

セキュリティ対策完了　適合証明書発行

Verification of Conformity

Applicant: JEOL Ltd.

Brand Name: JEOL

Equipment: MBBW PLATFORM

Test Model: DS-IB30PL

Certificate #: CYT-BKJ-2024-(00)SEME107-I

We, Bureau Veritas Japan Co., Ltd., declare that the equipment above has been verified and tested in the on-site facility and found compliance with the requirements listed at 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 (10)
Network Security Requirement (22)
Endpoint Protection Requirement (6/8)
Security Monitor Requirement (22)

The following models are applicable under the scope of this certificate:

- DS-IB30PL
- DS-Z30029PL
- DS-Z30029PLK
- DS-Z30019PL
- DS-Z30019PLS

Clause and Reference ID:	Results/Remarks	Verdict
[E187.00-RQ-00001-00] 7.2 Support for Operating System	All equipment's OS are still within the support period.	Pass
[E187.00-RQ-00003-00] 7.2 Support for Operating System	The equipment suppliers have provided a detailed procedure for applying patches and security updates. This procedure includes the evaluation of software compatibility, software package dependencies, potential performance impacts, and any side effects associated with implementing the patches or updates.	Pass
[E187.00-RQ-00008-00] 8.2 Network Transmission Security	Non-secure transmission protocols are not utilized.	Pass
[E187.00-RQ-00004-00] 8.3 Network Configuration Management	The equipment supplier has provided comprehensive documentation detailing network configurations, including the usage of network protocols and ports. Additionally, maintenance instructions for modifying network configurations, such as changing network port assignments, are included where supported.	Pass
[E187.00-RQ-00005-00] 9.2 Vulnerability Mitigation	The equipment supplier has conducted a vulnerability scan prior to shipment and delivered a comprehensive scanning report. The report includes the name and version of the scanning tool, the scanning scope of coverage, and the scanning date. The evidence provided confirms that there are no critical severity vulnerabilities, as assessed according to a common industrial vulnerability scoring standard.	Pass
[E187.00-RQ-00006-00] 9.5 Malware Scanning	The equipment supplier has performed a malware scan prior to shipment and provided a detailed scanning report. The report includes the name and version of the scanning tool, the scanning scope of coverage, and the scanning date, ensuring that the equipment is free from malware before delivery.	Pass
[E187.00-RQ-00007-00] 9.4 Anti-Malware Protection	The equipment supplier has provided documentation specifying the compatible anti-malware solutions for the fab equipment.	Pass
[E187.00-RQ-00008-00] 9.4 Anti-Malware Protection	The equipment supplier has provided documentation regarding security hardening measures, including instructions to enable/disable input/output interfaces and to disable unused operating system utilities and services.	Pass
[E187.00-RQ-00009-00] 9.5 Access Control Mechanism	Authentication mechanisms have been implemented for both operating system and equipment access control, ensuring secure and authorized access.	Pass
[E187.00-RQ-00010-00] 9.5 Access Control Mechanism	The equipment supplier has provided access rights and privileges authorization solutions to support the segregation of duties and the implementation of the least privilege policy.	Pass
[E187.00-RQ-00011-00] 10.2 Log Requirement	The fab equipment is capable of recording and exporting both system and application security event logs.	Pass

[E187.00-RQ-00013-00] 10.2 Log Requirement	The event logs recorded by the fab equipment include access control, configuration changes, and system errors. Each log entry contains details such as event type, event description, user account, and timestamp, ensuring comprehensive traceability.	Pass

まとめ

SEMI E187対応について
新規開発時の対策

SEMI E187対応について

- スタンダードが何を要求しているのか理解して対策する

  要求しているモノはサポート期間、手順、機能、検査結果などさまざま

- スタンダードの要求を別の方法で満たす対策では適合ではない

  手順が要求されているのに機能を追加してはダメ（規格への適合として）

- 適合するにはエビデンスが必要

  「手順がある」＋「合格基準がある」＋「実行されている」＋「結果がある」＝「エビデンス」

- 適合証明書を取得する

  自社で行った解釈には誤りが多かった

  エビデンスが準備できていれば口頭審査と実機審査を受けるだけ

新規開発時の対策

製品開発の方針は根本から変わる

- 出荷後の製品をアップデートする前提で設計する
- 最初からE187対応設計を行う必要がある
  OSのサポート期間、転送プロトコル選定、認証、認可、権限の制限、イベントログ

E187-0122は基本的な対策が要求されるスタンダードでした。
バージョンアップが検討されていますがE187-0122で行った対策の重要性は変わりません。

半導体製造装置で実施したセキュリティ対策

ご清聴ありがとうございました