

SEMI E169-0414 GUIDE FOR EQUIPMENT INFORMATION SYSTEM SECURITY

装置情報システムセキュリティのためのガイド

Notice: This translation is a REFERENCE COPY ONLY. If differences should exist between the English version and a translation in any other language, the English version is the official and authoritative version.

免責事項: この SEMI スタンダードは、投票により作成された英語版が正式なものであり、日本語版は日本の利用者各位の便宜のために作成したものです。万が一英語と日本語とに差異がある場合には英語版記載内容が優先されます。

SEMI スタンダード日本語翻訳版をご利用にあたっての注釈を本文の末尾に記載しております(「すべきである」「しなければならない」について等)。

本スタンダードは、the Information & Control Global Technical Committee で技術的に承認されている。現版は 2014 年 1 月 24 日、global Audits and Reviews Subcommittee にて発行が承認された。2014 年 4 月に www.semiviews.org および www.semi.org で入手可能となる。

1 目的

1.1 コンピュータウィルスによる情報の破壊や情報漏洩による機密性の侵害、サービス拒否による情報可用性の制限などのインシデントが至る所で頻繁に報告されている。そのような状況で、半導体製造装置の情報システムもまた、これらの脅威にさらされている。

1.2 従って、セキュリティ対策は半導体製造装置の不可避な要件となっている。

1.3 半導体製造装置のセキュリティに関して以下のような要求がある。

- マルウェア(ウィルス)防御、ただし装置の性能を損なわないこと。
- レシビの機密性保護、ただし装置の運転効率が低下させないこと。
- トラブルシューティングのために装置の操作ログファイルを利用可能にすること、ただしその機密情報が漏洩されないようにすること。
- ユーザが装置の設計情報を利用できるようにすること、ただしその機密情報が漏洩されないようにすること。

1.4 セキュリティ対策は、個々の装置ユーザの半導体製造ラインの管理計画に合わせて仕立てられる。しかしながら、顧客毎の違いがあるので、個々の装置のユーザとサプライヤの間で装置情報システムのためのセキュリティポリシーの交渉は非効率的である。さらに、そこで取り決められたことが確実に機能し、持続性を持つかどうかは不透明である。半導体製造装置における情報セキュリティのためのガイドラインが必要とされる。

1.5 このスタンダードの目的は、装置情報システムのセキュリティのための共通の基盤を確立することである。これにより、情報セキュリティの概念や対策を示唆し、それらをユーザおよび半導体製造装置のサプライヤ間で共有できるようにする。

1.6 このスタンダードは以下を期待される:

- コスト、納期、および信頼性を最適化するために、適切なセキュリティ対策を装置に適用するガイドラインを提供する。
- 装置の役割や責任についての知識を提供することによって、ユーザのセキュリティシステムの設計をより簡単に、より堅牢にする。
- 業界内のニーズと、セキュリティの評価方法を表現し、その一貫した理解を得るための共通言語を提供する。
- ポータブルで、相互運用可能な実装を提供するオープンスタンダード開発を促進する。

2 範囲

2.1 領域

2.1.1 このスタンダードは、半導体製造装置運用に関する領域をカバーする。

注: SEMI による書面での了承なき場合は、本書の全部もしくは一部の転載を禁じる。

©Semiconductor Equipment and Materials International (<http://www.semi.org/>)

©SEMI ジャパン 〒102-0074 東京都千代田区九段南 4-7-15

2.1.2 その領域は;

- 装置と対話するエンティティ(人, プロセス, システム)
- 装置運用に関するデータ・オブジェクト
- 装置内に組み込まれた情報システム部品

2.1.3 装置のドメインへの外部エンティティ(例えば工場や会社)は, 装置の情報セキュリティに関連している場合にのみ言及される。

2.2 テーマ

2.2.1 このスタンダードは, 装置の操作に関連した情報セキュリティのためのガイドラインの作成に以下の項目に言及する。

- 情報セキュリティの目標(機密性, 完全性, 可用性)
- 保護されるべき資産(装置情報資産)
- 装置情報システムによってサポートされるべき役割
- 重要なセキュリティ要件(例えば, マルウェア対策, ネットワーク上の不正なアクセス防止, ローカル操作, ハードウェア, コンポーネントの処分等)

注意: このスタンダードおよび安全ガイドラインはその使用に関連した全ての安全上の問題を取り扱うことを意図していない。この文書の使用者は, その責任において, 適切な安全および健康上実施すべき事項を決定し, また使用前に法規制やその他の制限への適用性を判断するものである。

3 制限

3.1 時間経過による変化

3.1.1 このスタンダードは, 現在, SEMI スタンダード委員たちによって認識されたセキュリティ上の問題をカバーするために書かれている。脅威, リスク, またはセキュリティ技術は, 時間とともに進化し続けている。したがって, このスタンダードは進化する環境に追いつくために定期的に見直され, 更新されなければならない。

4 参照スタンダードおよび文書

4.1 SEMI スタンダードおよび安全ガイドライン

SEMI E5 — SEMI Equipment Communication Standard 2 Message Content (SECS-II)

SEMI E30 — Generic Model for Communication and Control of Manufacturing Equipment (GEM)

SEMI E37 — High-Speed SECS Message Service (HSMS)

SEMI E40 — Standard for Processing Management

SEMI E87 — Specification for Carrier Management

SEMI E90 — Specification for Substrate Tracking

SEMI E94 — Specification for Control Job Management

SEMI E116 — Specification for Equipment Performance Tracking

SEMI E120 — Specification for the Common Equipment Model (CEM)

SEMI E125 — Specification for Equipment Self Description (EQSD)

SEMI E132 — Specification for Equipment Client Authentication and Authorization

SEMI E134 — Specification for Data Collection Management

SEMI E139 — Specification for Recipe and Parameter Management (RaP)

SEMI E147 — Guide for Equipment Data Acquisition (EDA)

SEMI E148 — Specification for Time Synchronization and Definition of the TS-Clock Object

SEMI E157 — Specification for Module Process Tracking

4.2 ISMI Documents

ISMI Technology Transfer #04104567C-ENG — Semiconductor Equipment Security Guidelines – Virus Protection

ISMI Technology Transfer #07114888A-ENG — Semiconductor Equipment Security Guidelines – Intellectual Property Protection

4.3 NIST Documents¹

NIST IR 7298 Revision 1 — Glossary of Key Information Security Terms

NIST Special Publication 800-27 Revision A — Engineering Principles for Information Technology Security

NIST Special Publication 800-30 — Risk Management Guide for Information Technology Systems

4.4 その他の文書

Equipment Engineering Capabilities (EEC) Guidelines (Phase 2.5), ISMI & JEITA/Selete
CIM Joint Guidance for 300 mm Semiconductor Factories, Release Five, ISMT and J300E

注意: 別途指示のない場合、引用された全ての文書は最新版を指す。

5 用語

5.1 略語および頭字語

- 5.1.1 *DOS* – Denial Of Service (サービスの否認)
- 5.1.2 *ECT* – Equipment Controller Terminal (装置コントローラ端末)
- 5.1.3 *EDA* – Equipment Data Acquisition (装置データ収集)
- 5.1.4 *EES* – Equipment Engineering System (装置エンジニアリングシステム)
- 5.1.5 *EIS* – Equipment Information System (装置情報システム)
- 5.1.6 *EP-ITS* – Engineering Principles for Information Technology Security (NIST document) (情報セキュリティのための技術原則; NIST 発行のドキュメント)
- 5.1.7 *FTP* – File Transfer Protocol (ファイル転送プロトコル)
- 5.1.8 *IP* – Intellectual Property. Example: IP Protection. (知的財産)
- 5.1.9 *IP* – Internet Protocol. Example: IP address. (インターネットプロトコル)
- 5.1.10 *ISMI* — International SEMATECH Manufacturing Initiative
- 5.1.11 *MES* – Manufacturing Execution System (生産実行システム)
- 5.1.12 *NIST* — National Institute of Standards and Technology (米国商務省の標準化研究機関)
- 5.1.13 *OS* – Operating System (オペレーティングシステム)
- 5.1.14 *SQL* – Structured Query Language (データベースの情報操作言語)

5.2 定義

- 5.2.1 *アクセス制御 (access control)* – 認証と承認を検証する機構を使って、情報資産へのアクセスを制限すること。
- 5.2.2 *アプリケーション (application)* – ユーザに対して特定の機能を直接実行し、システム制御、監視、または管理者権限にアクセスすることなく実行することができるソフトウェアプログラム。
- 5.2.3 *アタック、または攻撃 (attack)* – システムサービス、リソース、または情報に不正にアクセスする試み、またはシステムの完全性を危うくしようとする試み。
- 5.2.4 *監査 (audit)* – システム制御の妥当性を判断し、確立された方針や運用手順の遵守を確実にするために、記録や活動の独立したレビューと検査をすること。

¹ National Institute of Standards and Technology, 100 Bureau Drive, Stop 3460, Gaithersburg, MD 20899-3460, USA; Telephone: 301.975.6478, <http://www.nist.gov>

- 5.2.5 真正性 (authenticity) – 本物であり、検証可能で、かつ信頼できるという特性; 送信、メッセージ、またはメッセージの発信者の正当性の確かさ。
- 5.2.6 認証 (authentication) – 情報システム内のリソースへのアクセスを許可するための前提条件としてエンティティの ID を検証すること。
- 5.2.7 権限 (authority) – 特定の情報へのアクセスが許可されているという特性。
- 5.2.8 承認 (authorization) – 権限を確認するためにエンティティのアクセス特権を検証すること。
- 5.2.9 サービスの否認 (denial of service ; DOS) – ネットワーク、システム、またはアプリケーションの正当な使用を妨げ、または妨害するために資源を使い尽くす攻撃。
- 5.2.10 エンティティ (entity) – 情報やシステム状態を操作する能動要素 (人またはコンピュータプロセス)。
- 5.2.11 ファイアウォール (firewall) – 特定のセキュリティポリシーに従ってネットワークまたはシステム間のアクセスを制限するハードウェアとソフトウェアの能力。
- 5.2.12 ハーデニング (hardening) – システムのセキュリティ上の弱点を軽減するためにシステムを構成すると。
- 5.2.13 インシデント (incident) – 情報資産や装置の操作に害を与える問題の発生。
- 5.2.14 情報資産 (information asset) – 情報システムに上の価値のある情報と資源。
- 5.2.15 情報ポート (information port) – 装置情報システムと工場システムの間の情報の交換ポイント。
- 5.2.16 ログ (log) – 装置の操作または活動の記録。
- 5.2.17 マルウェア (malware) – ウィルスやスパイウェアなど、コンピュータシステムに妨害や損傷を加えるため、または機密情報を開示させるために特別に設計された悪意のあるソフトウェアを表現する包括的な用語。
- 5.2.18 なりすまし (masquerading) – 無許可のエージェントが、他のエージェントの認証を要求すること。
- 5.2.19 ミッションクリティカルシステム (mission critical system) – インシデントにより停止することを許されない、年間を通じて利用可能であることが必要なシステム。
- 5.2.20 特権 (privilege) – 個人、プログラム、またはプロセスに付与された権利。
- 5.2.21 代理サーバー (proxy server) – 他のサーバーにそれらの要求を転送することによって、クライアントの要求にサービスを提供するサーバー。
- 5.2.22 リスク (risk) – 情報資産に害を与えるインシデントの可能性。
- 5.2.23 スパイウェア (spyware) – ハードドライブや、メモリから密かにデータを送信することにより、別のコンピュータの活動に関する秘密の情報を得るために作られたソフトウェア。
- 5.2.24 サードレイヤ (third layer) – OSI モデルのレイヤ 3。データストリーム内の各 IP パケットを認証し、暗号化することによりインターネットプロトコル (IP) 通信を保護するプロトコルのセットである IP セキュリティ (IPsec) がこの層に応用できる。
- 5.2.25 改ざん (tampering) – システムの変更、その意図された行動の変更、または、データの変更が生じる故意のイベント。
- 5.2.26 脅威 (threat) – 情報資産に害を及ぼす可能性がある物事。
- 5.2.27 脆弱性 (vulnerability) – 情報資産を危険にさらすため、または害を及ぼすために利用できる弱点。
- 5.2.28 ウィルス (virus (computer virus)) – 自体をコピーして、一般的にシステムを破壊、またはデータを破壊する有害な効果をもつプログラム。
- 5.2.29 ゼロデイ攻撃 (zero-day attack) – 脆弱性の存在が広く公表される前に、脆弱性 (セキュリティホール) を利用して攻撃すること。

6 EIS セキュリティのポリシー

6.1 情報セキュリティの達成すべき目標

6.1.1 情報セキュリティの目的は、情報資産の機密性、完全性、可用性を保証することである。

- 機密性 (Confidentiality) は、機密情報を漏洩しないように、アクセスを制限し、情報資産を保護することである。
- 完全性 (Integrity) は、不正改変または破壊に対して情報を保護し、情報資産の健全性を維持することである。

- 可用性(Availability)は、正当なユーザが情報をタイムリーに利用できることを保証する能力である。

6.2 セキュリティシステムの目的

6.2.1 セキュリティシステムの目的は、「攻撃」に対して情報資産を保護し、情報セキュリティの目標を達成することである。攻撃は、表 1 にリストされたクラスに分類することができる。セキュリティ対策を検討するために、この「攻撃のクラス」を参考にすることができる。

表 1 攻撃の分類

攻撃のクラス	攻撃の例
受動的監視 (Passive Monitoring)	ネットワークに流れる情報の監視 装置コントローラ端末 (ECT) の観察
能動的ネットワーク攻撃 (Active Network Attack)	ネットワークを介する侵入、またはマルウェアの注入 サービスの否認 (DOS)
内部者による侵害 (Exploitation by Insiders)	正規ユーザによる意図的なセキュリティ規定違反
物理的アクセス、または近接者による攻撃 (Attack by Physical Access or Proximity)	外部デバイスの接続によるウィルス感染、または情報漏洩 装置コントロール端末 (ECT) からの侵入 内蔵記憶デバイスを取り外し、持ち去る
悪意のあるプログラム (Malicious Code)	コンピュータウィルスの活性化

6.2.2 特定のタイプの攻撃は常に知られているわけではない。既知の種類の攻撃に対する防御は最低限の要件だが、知られていないけれども、しかし以前のパターンによって予測できる攻撃に対する防御も必要とされる。

6.2.3 EIS は、常にシステム内のセキュリティにギャップがありうることを考慮しながら、攻撃から情報を防御するために備える必要がある。例えば、システムは、ゼロデイ攻撃など、予期しない攻撃を防御するためにタイムリーに更新される必要がある。

6.3 情報セキュリティの管理側面

6.3.1 コストと性能のトレードオフ

6.3.1.1 リスクを低減する対策がセキュリティを維持するために適用されるが、リスクを低下させるプロセスがコストを増大し、意図された機能のためにシステム性能を低下させる等の悪影響を及ぼす傾向がある。セキュリティ性能向上と、コストの増加、およびシステム性能低下の間のトレードオフを考慮しながら、最適にバランスをとらなければならない。コストには、初期コストに加えてセキュリティシステムのランニングコストが含まれるべきだろう。

6.3.2 扱いの容易さ

6.3.2.1 セキュリティ機能の維持や操作が容易ではない場合には、セキュリティ対策の有効性が低下する。セキュリティ対策は維持し、操作しやすいように設計されるべきである。さらに、継続的な教育と、システム管理者やユーザのトレーニングへの投資が必要となる。

6.3.3 階層化されたセキュリティ

6.3.3.1 セキュリティ設計者は、ユーザ(企業など、工場など)のシステム階層に装置を統合することが重要である。ユーザのシステムが装置の上に覆いかぶさることにより、装置の攻撃をより困難にさせる。セキュリティシステムはこの階層的構造により強化される。例えば、アプリケーションゲートウェイ、侵入検知システム、パケットフィルタリング、パスワード制御、ユーザトレーニング、およびその他の措置をそれぞれの階層に適用することができる。セキュリティ性能、セキュリティのコスト、製造のパフォーマンスのバランスを取りながら、それぞれの階層の役割と責任の最適配分を決定することが必要である。

6.3.4 複合されたセキュリティ

6.3.4.1 階層化されたセキュリティに加えて、様々なセキュリティ対策を組み合わせることが必要不可欠である。例えば、セキュリティ対策としてひとつの種類のみ各層に適用した場合、防御が一度だけ破壊されるだけで、容易に

システム内部に深く浸透することができてしまう。それぞれ階層に様々なセキュリティ対策を組み合わせることが重要だ。

6.3.5 復元力

6.3.5.1 インシデントが発生した場合に、情報システムの受ける損傷をできるだけ小さくし、問題からの復元を容易にできるようにすべきである。この要件を満たすために、システムは、インシデントに対処するための明確に定義された方策が必要とされる。例えば、危険を排除するためにラインから問題のシステムを除去することが戦略の一部かもしれない。回復のスピードを重視しながら、インシデントから回復するための手順を定義することが必要とされる。

6.3.5.2 情報システムのセキュリティ状態が、インシデントを示すために管理されるべきである。例えば、システムは、「緊急応答」、「回復」、または「通常運転」の状態変化で管理されるかもしれない。

6.3.6 時間とともに低下する信頼性

6.3.6.1 技術の進化と環境の進化のため、情報セキュリティ対策の信頼性は時間の経過に従って低下する。情報セキュリティ対策は定期的に評価され、再検討されるべきである。新たなリスクが識別されたときに、使用する技術を更新し、または新技術を導入することが必要である。

6.3.6.2 そのセキュリティ対策が容易に更新できるように情報システムは設計されるべきである。

6.3.7 改善プロセスの実施

6.3.7.1 システムの設計では見込まれていなかった問題が繰り返し発生し、悪影響を情報セキュリティに与える可能性がある。問題の再発を防止するために、見込まれていなかった問題や、露呈したシステムの脆弱性の経験を活かし、過去から学び、継続的にセキュリティの向上を実現することが必要である。

6.4 方法セキュリティの技術側面

6.4.1 リスクの構図

6.4.1.1 リスクは、情報セキュリティの「脆弱性」を「脅威」が「攻撃」するによって、「インシデント」が発生し、「情報資産」が損傷される可能性である。

6.4.1.2 情報セキュリティへの既知の脅威には、「不正アクセス」、「なりすまし」、「不正利用」、「不正実行」、「マルウェア実行」、および「サービス否認(DOS)」が含まれる。その結果、「誤動作」、「性能劣化」、「故障」、または「情報資産の損傷と破壊」が、これらの攻撃によって引き起こされ得る。リスクを低くするためには、その「脅威」、「脆弱性」、「攻撃」、および「インシデント」が及ぼす可能性のある損傷を理解する必要がある。図 1 は、「脅威」、「攻撃」、「リスク」、「インシデント」などの関係を示している。

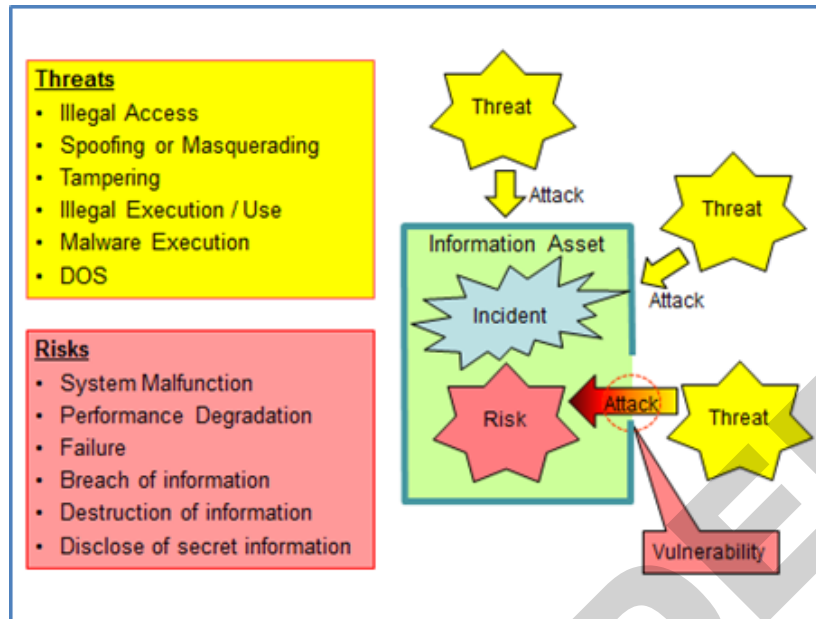


図 1
リスクの構図

6.4.2 認証と承認によるアクセス制御

6.4.2.1 侵入や不正使用などの攻撃を防止するために、認証と承認による情報資産へのアクセス制御が必要とされる。

6.4.2.2 認証は、システムにアクセスしようとするエンティティの真正性を検証するプロセスである。システムにアクセスするエンティティは、その真正性を証明する必要がある。多くの場合、ユーザ識別(ユーザ ID)およびパスワードがその真正性を証明するために使用される。

6.4.2.3 承認は、情報資産の特定の部分に対するアクセス権限に基づいて、エンティティのアクセス制御をするプロセスである。エンティティは、その指定された権限の範囲内の情報資産へのアクセスを許可されるが、その権限の外にある情報へのアクセスを許可されない。

6.4.2.4 セキュリティシステムは、情報システム全体にわたってアクセス制御の機能をサポートする必要がある。統合された認証プロセスを確立するために、セキュリティシステムは、ドメイン内のすべてのエンティティの認証をサポートする認証サーバーを実装することがある。

6.4.3 最小な特権の付与

6.4.3.1 エンティティに与えられた権限は、そのエンティティの役割を実行するために必要であり、最小な特権に制限される必要がある。不必要に広い特権範囲の付与は、不正アクセスのリスクを増大させる。システムのユーザおよび管理者は、その役割に応じた個別のアクセス権を与えられるべきである。いわゆる「スーパーユーザ」と呼ばれるユーザの権限を許可すると、不正アクセスのリスクを増大させる。

6.4.4 公衆アクセスからの分離

6.4.4.1 EIS は、装置の制御専用に使われるミッションクリティカルなシステムとして特徴づけられる。EIS は公衆アクセスから分離される必要がある。EIS の環境ドメイン(工場)は、EIS への公衆アクセスを分離する措置を実施すべきである。さらに、公衆ドメインからのアクセスを分離するために、EIS は外部のドメインとの会話を制限する措置を採用すべきである。

6.4.5 ネットワーク境界での情報フローの制御

6.4.5.1 ネットワークの境界上のアクセスと情報の流れの制御は、重要なセキュリティ要件である。アクセスおよび情報フロー制御のために、以下の属性を考慮すべきである。

- 外部とのインターフェース

- 情報フローメカニズム（プッシュ、またはプル）
- 必要なポート、プロトコル、ネットワークサービス
- 情報交換の仕様

6.4.5.2 EIS に流れ込む情報と同様に、EIS から出てゆく情報についても制御されるべきであることに注意が必要だ。EIS は、工場内の他のシステムに害を与えるための「踏み台」として使用されるかもしれない。

6.4.6 監査メカニズムの要求

6.4.6.1 不正アクセスを識別し、インシデントを調査するために、監査メカニズムのサポートが必要とされる。EIS は、この監査活動のために、定期的なログの調査を支援する機能を提供することが求められる。

6.5 EIS ライフサイクル全体にわたるセキュリティ

6.5.1 セキュリティは、情報システムのライフサイクルの段階に応じて異なる様相を示す。システムライフサイクルのフェーズが、リスク管理の枠組みを示すために定義されるべきである。

6.5.2 NIST は、その文書 (NIST Special Publication 800-30) で、これらのフェーズの定義を提供しており、それを EIS に適用することもできる。表 2 は、NIST の文書から引用したフェーズの定義を示している。

表 2 情報システムのライフサイクル中のフェーズ

フェーズ	説明	リスク管理について
Phase 1 – Initiation (初期)	IT システムの必要性が表現され、IT システムの目的および範囲が文書化される。	ここで特定されたリスクは、セキュリティ要件、システム要件、および運用（戦略）などのセキュリティ概念を開発フェーズに示すために使用される。
Phase 2 – Development or Acquisition (開発と取り込み)	IT システムが、設計、購入、プログラム、開発、または他の方法で構成される。	このフェーズ中に識別されたリスクは、開発中のシステムの構造、および設計のトレードオフを導くシステムのセキュリティ分析をサポートするために使用される。
Phase 3 – Implementation (実装)	システムのセキュリティ機能が設定され、有効化され、テスト、および検証される。	リスク管理プロセスが、モデル化された運用環境内の中で、その要求に対するシステム実装の評価をサポートする。特定されたリスクに関する決定は、システムの動作前に行わなければならない。
Phase 4 – Operation or Maintenance (運用、または保守)	システムは、その機能を実行する。システムは、一般に、ハードウェアとソフトウェアの追加、および、組織のプロセス、ポリシー、および手順への変更によって継続的に修正される。	定期的なシステム再認可（または再認定）のために、またはその運用や生産環境の主要な変更（例えば、新たなシステム・インターフェース）が加えられたときに、リスク管理活動が実行される。
Phase 5 – Disposal (廃棄)	この段階には、情報、ハードウェア、およびソフトウェアの除去が含まれる。それは、情報の移動、アーカイブ、廃棄、または破壊などで、ハードウェアおよびソフトウェア的に情報を除去することがある。	残っているデータが適切に処理され、またそのシステムの移行が安全かつ体系的な方法で行われ、ハードウェアとソフトウェアが適切に廃棄または置換されることを保証されるように、リスク管理活動がシステム要素に対して実施される。

7 装置情報資産 (Equipment Information Asset)

7.1 装置情報資産 (Equipment Information Asset) は、脅威に対して保護されるべき対象の全体である。その情報資産には、装置情報システム (EIS) と、それが管理する装置情報 (Equipment Information) が含まれている。装置情報資産の例が図 2 に示されている。

注 1: この章の図と説明は、情報資産の実装を求めるものではなく、情報資産の概念を導入することを意図している。