「装置情報システム・セキュリティ」ガイドの開発

東京エレクトロン株式会社　坂本 見恒

ウィルス感染や不正アクセスなどの手口で、貴重な情報が漏洩または破損する情報セキュリティ侵害の出来事が、世界中で頻繁に報告されています。半導体の製造ラインにおいても、ウィルス感染、情報の漏洩、情報の破壊などがすでに経験されています。半導体製造装置は、まさしくこれらの脅威に対する防御策をとることを必要とされています。

「想定外」のサイバー攻撃

半導体製造装置の情報システムについては、従来、例えば装置コントローラのように、限られた専門的な用途に使われ、直接インターネットなどのオープンなネットワーク環境に接続されないという想定から、情報セキュリティが強調されることはありませんでした。一方で、情報システムへの攻撃の目的が、単なる遊びレベルのものから、業務を妨害することを意図するものにまで発展してきています。Stuxnetがプラント深部の機器制御ネットワークにまで侵入し、攻撃を加え、核燃料濃縮施設の操業を妨害したことは、現在専らの話題となっています。半導体製造ラインも、このような攻撃のターゲットにならないとも限らないのではないでしょうか？

アンチウィルス・ソフトウェアの問題

今日、一般の情報システムでは、アンチウィルス・ソフトウェアの適用は当然必要なものとなっています。半導体製造装置の上の情報システムもその例外ではないと言えます。しかしながら、アンチウィルス・ソフトウェアを装置情報システムにインストールして機能させると、装置本来の機能性能が低下してしまうという問題があります。また、アンチウィルス・ソフトウェアはパターンファイル更新することが必要で、このパターンの更新のためにさらに装置の性能が低下し、ひいては装置の運用を一時休止しなければならないということになります。これらの問題を回避しつつ、ウィルスの攻撃を防御できるようにしなければなりません。

プロセス情報の漏洩防止

プロセス情報は、レシピや装置設定などのプロセス仕様とプロセス結果の情報を含み、半導体デバイスの製造方法にかかわる重要な知的財産です。もし、あるデバイス・メーカーのプロセス情報が、競合するデバイス・メーカーに漏洩されてしまったら？ そのデバイス・メーカーは、ビジネスで損失を被ることになります。半導体製造装置は、この知的財産を暴露しないように防御する機能を提供することを求められています。特に、現実の製造ラインで、レシピの漏洩をどう防ぐかについてさまざまな議論がされています。

トラブルシューティングのためにログファイルを！

半導体製造装置の運用に関するログファイルは、プロセス、装置の運用と挙動、製造中の製品などに関連した多様な、しかも知的財産と思われる情報が混合して記録されています。したがって、ログファイルに記録された情報は漏洩しないように守られなければなりません。

一方で、ログファイルの本来の目的のひとつは、トラブルシューティングのための情報を提供することです。トラブルシューティング時に、ログファイルにアクセスし、ファイルを取得し、分析するようなことができなければなりません。もし、ログが必要とされている時に、必要な人に利用可能でなければ、メンテナンスの時間が長引き、装置の生産性の指標のひとつであるMTTR（Mean Time To Repair）が悪影響を受けることになるでしょう。であるにもかかわらず、最近、情報セキュリティの観点からログへのアクセスが禁止され、情報取得が困難になりそうな現実の状況があります。今後、装置生産性の向上がますます求められており、トラブルシューティングでのログ情報利用の必要性がますます高まるでしょう。この問題を解決するために、機密保持と情報利用の両方を保障するような新しい枠組みが示されて、その枠組みが共通に認識されることが望まれます。そして、装置はその枠組みに組み込まれた機能をサポートするようになるべきでしょう。

装置情報セキュリティ・ガイドが必要！

現在の半導体製造装置のセキュリティ防御策は、装置ユーザーとサプライヤの間のローカルな交渉ベースで検討されています。このローカルな交渉ベースのやり方では、当然のことながら、コスト、品質、およびその実施において非能率であると考えられます。さらに、個別に検討された防御策が信頼できて、持続可能であるかどうかは、その防衛策を考える枠組みの強弱によって変わってきてしまいます。半導体製造装置と、それが運用される環境を踏まえて、情報セキュリティの概念と、実施において適用されている防御方法を捉え、装置における情報セキュリティを考える枠組みを提供するガイドが必要とされています。

SEMI Draft Doc. #5422 EISS

装置情報システム・セキュリティガイド（Guide for Equipment Information System Security）が、現在SEMIスタンダード化の投票（Ballot #5422）に掛けられています。（2013年2月末時点）

SpecificationではなくGuideスタンダード

このバロットは、半導体製造装置の情報システムのセキュリティを検討するための、枠組みとなるガイドを示すために努力しています。ここで、あえて「努力」と言っているのは、セキュリティという問題が相互に関連する多くの側面をもち、また時間とともに進化変遷していくものであり、一面的には捉えがたいという意味を込めています。また、このガイドは、ITのセキュリティ技術に言及するのではなく、むしろその運営面の考え方にハイライトしています。このスタンダードを、Specification（仕様）とするのではなく、Guide（ガイド）とした理由には、これらの考えが含まれています。

スタンダードの構成と展開

このスタンダードの展開として、まずは「情報セキュリティは何か？」という認識合わせをするために、情報セキュリティ・ポリシーに言及するところから始まります。次に、防御すべき対象である装置情報イメージを共有するために、装置情報資産のモデル（Equipment Information Asset）を提案します。続いて、ファクトリ・システムに統合されることを前提として、その中での装置の情報システムのセキュリティに関する役割を提案します。最後に、実際的な装置のセキュリティ機能の要求と、その対応の理解を共有するために、情報セキュリティの実施について言及するという展開になります。

情報セキュリティのゴール

セキュリティが達成すべき課題は、情報漏洩を防止するための機密性（Confidentiality）、情報の意図しない改変、破壊から守り、完全性を確保すること（Integrity）、情報の利用可能性を確保すること（Availability）としています。これらをまとめて、「CIA」と言うこともあります。装置コントローラのような、特にリアルタイムで情報を処理するものではAvailabilityが優先されるべきだという議論もあり、その場合、「AICと言うべきでないか？」などと言われることもあります。このような、セキュリティ・ポリシーの議論については、米国商務省のスタンダード研究機関であるNISTから発行されているペーパーなどを参考にして、一般的な情報セキュリティの考え方からまとめました。

装置情報システムの役割

装置のセキュリティは、ファクトリ・システムの一部に組み込まれ、その階層の中で役割を果たすという構図を前提としています。装置情報システムの役割は、以下のように提案しています。

- マルウェア防御
- 未使用のサービスとプログラムの停止
- アクセス制御
- 情報の分類と分離
- 監査のための情報の提供

「ホワイト・リスト」によるマルウェア対策

特に、マルウェア（ウィルスなど）の防御については、ホワイト・リスト方式の対策を採用することを提案しています。

ホワイト・リスト方式のマルウェア防御では、記憶領域をスキャンしてパターンと照合してマルウェアを発見、退治するのではなく、許可のないプログラムの実行を禁止することにより、マルウェアの働きを封じ込めるという考え方を取っています。

ホワイト・リスト方式は、コンピュータ能力の消費が非常に少なく、そのため、リアルタイムに情報を処理する装置コントローラのようなシステムに適しています。

アクセス・コントロール

装置にアクセスするすべてのエンティティからのアクセスを制限し、制御することを考えなければなりません。エンティティとは、通信を介してアクセスする外部のプログラム、装置コントロール・ターミナルを介してアクセスするオペレータ、外付けデバイス（USBなどの機器）などのことです。情報セキュリティのゴールであるCIA（AIC）を保つために、堅牢なアクセス・コントロールが適用される必要があります。

アクセスの対象となる装置情報資産を分類、分離して、それぞれのアクセスを制御するための手法として、役割ベースのアクセス制御（Role Based Access Control）を紹介しています。

セキュリティ対策と、コストのトレードオフ

マルウェア防御やアクセス・コントロールなど、多様な対策が装置に求められます。ただし、一方でセキュリティだけが本来の装置の目的ではないことを忘れてはならないのです。コストとのトレードオフ、または装置の性能とのトレードオフのバランスを適切なレベルに落とす必要があります。

装置の情報システム・セキュリティは、ファクトリ・システムの階層の中に組み込まれることを前提として、役割を明確化し、抑えどころを知ることが肝心であると考えられます。

Guide for EISSの行方

このバロット #5422のために、2011年12月にタスクフォースが設立され、2012年を通してバロット開発と検討が進められました。そして、現在2013年のサイクル2でバロット投票に掛けられています。

情報セキュリティは全容を捉えることが困難な、非常に多様な側面をもつ課題です。そのため、「このバロットでどこまでそれをカバーできているのか？」という問いにすぐに答えることはできません。しかしながら、目に見えるドキュメントという形でガイドを持ち、セキュリティ対策を議論していただければ、その価値を感じていただけるのではないかと考えています。

SEMIスタンダード規約では、「ガイドを元にして新たな技術スタンダードが開発されること」を、ガイド・スタンダードのひとつの目的としています。このスタンダードが、より詳細で実用的な技術仕様を規定するために参照されることを期待します。

ともあれ、この原稿を書いている現在、バロット投票が進められています。状況によっては、4月の委員会でスタンダードとして成立するかもしれません。しかしながら、今回のバロットが最終的なガイドになるとも考えられていません。脅威の進化、それに応じた防御技術の進化に伴い、このガイド自身も進化していかなければなりません。今後もスタンダード委員会の皆様の関心と協力をいただき、このガイドについての新たな課題、または問題点などについて、議論が続けられることを期待しています。