産業サイバーセキュリティ研究会 WG1
半導体産業サブワーキンググループ(第3回会合)
議事要旨

1. 日時・場所

日時:令和7年6月19日(木)10時30分～12時30分

場所:新東京ビル7階セミナールームH(ハイブリッド)

2. 出席者

委員　　:江崎委員(座長、オンライン)、飯嶋委員、高橋委員、高原委員、中川委員(オンライン)、
長野委員(オンライン)、浜島委員(オンライン)、東委員(オンライン)、三井委員、渡部委員、
秋山委員(オンライン)

オブザーバ:独立行政法人情報処理推進機構

事務局　　:経済産業省

3. 配付資料

資料1　議事次第・配布資料一覧

資料2　委員等名簿

資料3　ローム様講演資料　工場セキュリティ リスクコントロール戦略

資料4　日本電子様講演資料　SEMI E187スタンダード　概要と実施例の紹介

資料5　事務局説明資料

資料6　半導体デバイス工場におけるOTセキュリティガイドライン概要資料

資料7　半導体デバイス工場におけるOTセキュリティガイドライン(案)

資料8　半導体デバイス工場におけるOTセキュリティガイドライン(案)英訳版

資料9　半導体産業におけるセキュリティ対策基準について

4. 議事内容

冒頭、経済産業省商務情報政策局 見次室長から挨拶があり、次に、ローム井上様より資料 3、日本電子金田様より資料 4 の説明があった。続けて事務局より資料 5～9 の説明を行った後、自由討議が行われたところ、概要は以下の通り。

＜ローム様講演について＞

○渡部委員

・　資料３（P24）にリモートメンテナンス経路の標準化とあるが、リモートメンテナンスの定義は何か。
⇒（ローム井上様）インフラや MES に対してリモートでメンテナンスする場合と、装置自体に P2P で接続する場合の二つがあり、これらをリモートメンテナンスとしている。なお、装置は最下層にあるためネットワークから切り離した状況でつなげている。オフラインにした上で、装置だけをインターネットにつなげてリモートメンテナンスを行っている。

○高橋委員

・　セキュリティ対策について、一般的に通信を暗号化することが求められている環境において、IPS と暗号化通信の相性の悪さがあると思う。また、IPS は誤検知も多いが、何か運用の工夫をされているか。

⇒（ローム井上様）暗号化について、受ける側と送る側の双方で対応する必要があるが、まだそこまで対応できていない。誤検知が多いことについては、ツールを入れた時に最初は誤検知がよく出るが、潰していくことでほぼ出なくなっていく。最初にパケットを解析し、ホワイトリスト化することで対応している。

○ニコン鈴木様

・ 脆弱性対策の一つとしてペネストレーションテストを OT の工場内に対しても行っているか。また、その結果を装置メーカーに開示した実績または今後の予定はあるか。

⇒（ローム井上様）ペネトレーションテストは MES を対象に行っている。稼働中のシステムにペネトレーションテストを実施する際には、強度を弱くしている。なお、今期は仮想環境を作って、そこで強度の強いペネストレーションテストを行うことも考えている。ペネトレーションテストの結果についてはある程度開示は可能であるが、装置に対してペネストレーションテストを行うことは現状考えていない。

＜日本電子様講演について＞

○長野委員

・ E187 対応について、どの程度古い製品群に対して実施したか。

⇒（日本電子金田様）

2025 年 1 月 1 日から E187 対応を求められたため、それ以降に納入する装置に対して対応した。既納装置への適用は E187 には記載されていないが、E188 では機器ユーザーと機器サプライヤが合意した期間は機器サプライヤが脆弱性を評価してリスクに対処することになっている。将来的には E188 の対応も求められると考えられる。

＜半導体デバイス工場における OT セキュリティガイドライン（案）について＞

○SEAJ 渡部様

・ 業界団体で説明会を開催し OT セキュリティガイドラインの周知をしていく必要があると考えているが、非常にボリュームがあるため、どのように説明していくべきか相談したい。

⇒（事務局）説明方法の工夫としては、概要資料を用いて説明する、複数の業界団体に対してまとめて説明会を実施する、説明を録画し配布するなどが考えられる。

○日本電子金田様

・ 英語版の OT セキュリティガイドラインの対象読者はどのような方々であるか。

⇒（事務局）本ガイドラインのパブリックコメントについては、SMCC や米国 SIA 等に声掛けをし、グローバルにご意見をいただくことを目的に英語化した。

○江崎座長

・ 現在、日本はサイバーセキュリティ対策に対して受け身になっているため、グローバル企業と対等に議論を進めていくことを目指していく必要がある。グローバルな会合（SEMICON、SMCC 等）で議論を行うためにも英語版は有効である。

○日本電子金田様

・ 英訳版ガイドラインについて、1.1 の最初二つのパラグラフ及び 1.2 の想定読者については、記載内容が日本に偏りすぎているため修正した方がよいと感じた。

○長野委員

・ 資料 6 に出てくるリファレンスアーキテクチャ―のクラウド AI 分析サービスとの記載について、生成 AI など取扱いが難しいものもある。AI と書かない方がよいのではないか。

⇒（事務局）ガイドラインを作成するにあたり、デバイスメーカーへのヒアリングの中でクラウド AI 分析

サービスを導入しているとのことで記載した経緯があるが、生成 AI の活用との誤解を招く可能性があるため、御指摘のとおり修正させていただく。

＜半導体産業におけるセキュリティ対策基準について＞

○ニコン高橋委員

・　セキュリティ対策基準のタイムラインはどのように考えているか。

⇒（事務局）IT 基準は検討中のサプライチェーン強化に向けたセキュリティ対策評価制度から抽出しているが、同評価制度の正式な運用開始は来年の秋頃になる予定である。そのため、セキュリティ対策基準もそれに整合したタイムラインになるが、プレリリースのような形で先行的にご参照いただくことも考えられる。なお、具体的な投資促進施策との紐づけについては、今後決めていく予定である。

○SCREEN 林様

・　セキュリティ対策基準について、投資関連施策との紐づけとはどのようなイメージで考えているか。

⇒（事務局）安全保障の補助金など特定の半導体企業の皆様に対して様々な支援策を用意させていただいているが、その中でセキュリティ対策基準に準拠していただくことを考えている。

○日本電子小泉様

・　項目内容によっては行うことが難しいものもあるという印象を受けた。例えば、4-4 の「不要サービスを無効化すること」という項目は、OT 資産全てに対して不要かどうかを判断して無効化するのはかなり難しいと考えている。チェックリストは対応した項目数のみで評価するのか。

⇒（事務局）評価基準（案）は IT と OT に分けている。本社や情報システムなどのエンタープライズ IT に対しては IT 評価基準を使い、工場については OT 評価基準を使って評価する形になる。そのため、OT 資産に対して不要サービスを無効化することまでを求めることは想定していない。

以上