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5回会合)
議事要旨

1. 日時・場所

日時:令和8年1月20日(火)10時00分～12時00分

場所:新東京ビル7階 セミナールームA(ハイブリッド)

2. 出席者

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

オブザーバ:独立行政法人情報処理推進機構、JPCERT/CC

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　NECファシリティーズ社講演資料

資料4　事務局説明資料

参考資料1　IT項目要求事項・要求項目(案)

参考資料2　OT項目要求事項・要求項目(案)

参考資料3　中核人材育成プログラム説明資料

4. 議事内容

冒頭、経済産業省商務情報政策局 橋本企画官から挨拶があり、次に、NEC ファシリティーズ様より資料 3 の説明があった。続けて事務局より資料 4 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。

＜NEC ファシリティーズ社講演について＞

・　監視システムへのパッチ適用は困難とのことだが、具体的なソリューションはあるか。
　⇒現状、明快な解決策はなく、年末年始などの生産停止期間を利用してパッチ適用する等の運用でカバーしている。抜本的には、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等で示される FMCS などに変更していくことが必要である。

・　体制図にあった CSIRT、FSIRT、PSIRT は、具体的にどのように連携しているのか。
　⇒CSIRT、PSIRT、FSIRT の順で整備を進めており、現在は三者を統合してセキュリティ部門として統制を図ろうとしている段階である。まだ試行錯誤の状況だが、連携・統制の必要性を感じて日々対応している。

・　エアギャップ環境において、USB メモリの持ち込みに関してどのようなルール作りを行っているか。
　⇒顧客のガイドラインに則るのが基本である。自社では暗号化されたメモリのみ使用可能とし、原則として書き込みを禁止している。将来的には、セキュリティゲートウェイやデータダイオード等を活用し、USB メモリを使用しないデータ連携方法を検討している。

・　HMI の表示が偽装された場合、その表示が正しいか否かを確認する術はあるか。
　⇒現場に赴き、装置のアナログメーターやより起点に近い計装システムから直接情報を確認している。PLC

の偽装も想定し、さらに下位のセンサーから情報を取ることも考えられる。理想は、常時監視・自己診断する仕組みを導入することである。

⇒システムデータだけでなくカメラ映像を併用したり、人が異なるタイミングで巡回確認したりと、複数の手段を組み合わせることで不正検知の確度を上げている。

・ 貴社の R&D ラボで、物理的な設備を使ったサイバー攻撃からの復旧訓練は実施しているか。また、他社への貸し出しは行っているか。

⇒現時点では復旧訓練の実施には至っていないが、設備的には可能であり、サービスメニューとして検討している。業界のテストベッドや共同訓練施設として貢献できる可能性も考えている。

＜半導体装置メーカーに対するセキュリティ要求事項について＞

・ ガイドラインを策定するにあたり、欧州のサイバーレジリエンス法（CRA）との関係性はどのように整理されるのか。CRA と SEMI 規格とに加えて本要求項目が新たに上乗せされる形になった結果、現場が混乱することを懸念している。

⇒本要求事項は認証を伴うものではなく、あくまで参照する文書である。CRA や SEMI E187 に該当する箇所を明記し、関係性を分かりやすく記述することが重要である。

⇒CRA の方がハードルの高いものであり、本要求事項を遵守しても CRA 対応を保証するものではない、という関係性を明確に記述する必要があると考える。

・ 本ガイドラインと、JC-STAR のような製品ラベリング制度との関連性はどうなるのか。国内統一基準としてラベリング制度があると、メーカーは対応しやすいのではないかと思う。

⇒（事務局）既存の SCS 評価制度や JC-STAR を活用することは可能と考えている。ただし、半導体特化の認証制度については、業界のニーズを慎重に見極めたい。JC-STAR の類型に半導体装置を追加し、SEMI 規格や CRA との相互認証を目指すことも仕組み上は可能だが、費用対効果の検討が必要である。

・ 装置そのものへのセキュリティ要求項目（SEMI E187 等）は必要と考えるが、組織全体に求めるセキュリティ要求項目については、デバイスメーカーと装置メーカーでは事情が異なるため、一律の基準（SCS 評価制度★4 等）とすることには慎重であるべきかと思う。

⇒近年の顧客（例: TSMC）は、製品だけでなく、それを提供する企業組織のセキュリティ対策の成熟度も評価対象としているため、組織全体への要求は避けられない状況にある。サプライチェーンのレジリエンス確保が必須であり、その上で★4 というレベル設定が適切かどうかが次の論点となる。

・ 半導体以外の製品と共用する生産ラインを持つ装置メーカーにとって、組織全体に一律で SCS 評価制度★4 レベルを求めるのは社内合意が難しいかと思うので、適用範囲に関する明確な指針があると動きやすい。

⇒（事務局）（受発注者間の★取得にかかる協議を踏まえ、）最終的には各社の経営判断となる。

⇒ガイドラインを基準としつつも、自社の状況に応じて「なぜこの項目を適用しないのか」をバイヤーに対して明確に説明できる枠組みが重要であるかと思う。これにより、共通の基準のもとで対話が可能になり、一律適用が困難な場合でも柔軟な対応ができると考えられる。

・ 「セキュリティ要求事項」は装置メーカーにとってどのような位置づけであるか。投資促進施策との紐付けなど、対応へのインセンティブはあるのか。

⇒（事務局）装置メーカー向けの要求事項も、将来的にはデバイスメーカー向けと同様に、投資促進施策と紐付けることを検討している。

＜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のファシリティエリアに関する検討について＞

・ ファシリティエリアのガイドラインの論点として、「エネルギー供給システムが統合され IT 領域と接続され

る中で、PLC を中心としたネットワークのセグメンテーションや、境界におけるセキュリティソリューションの考え方」と「エネルギー供給形態（自社運用、管理の委託、外部からの供給）の多様化を踏まえた、責任分解点や境界制御の考え方」の 2 点を加えてほしい。

⇒（事務局）貴重なご意見として、ガイドラインのたたき台作成の際に参考にさせていただく。

・ 「セキュリティ要求事項」と「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の改版」は別のドキュメントという理解でよいか。

⇒（事務局）別物である。ただし、要求事項の OT 項目がガイドラインを引用するなど、関連性はある。装置メーカー向けの要求事項は、次回以降の SWG で取りまとめ、ガイドラインとは別の文書として確定する予定である。

以上