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2回会合)
議事要旨

1. 日時・場所

日時:令和7年3月31日(月)13時00分～15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)、飯嶋委員、高橋委員(オンライン)、高原委員、中川委員(オンライン)、長野委員、浜島委員(オンライン)、東委員(オンライン)、藤井委員、三井委員、渡部委員(オンライン)、蓬莱様(秋山委員代理・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　SEAJ講演資料　SEAJサイバーセキュリティ活動状況

資料4　IPA講演資料①　J-CSIP半導体業界SIGについて

資料5　IPA講演資料②　ICSCoEの事業説明

資料6　事務局説明資料

資料7　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について

参考資料1　半導体デバイス工場におけるOTガイドライン(案)概要資料【関係者限り】

参考資料2　半導体デバイス工場におけるOTガイドライン(案)【関係者限り】

4. 議事内容

冒頭、経済産業省商務情報政策局 見次サイバーセキュリティ制度企画室長から挨拶があり、次に、渡部委員より資料 3、IPA 松田様より資料 4、IPA 釜谷様より資料 5 の説明があった。続けて事務局より資料 6～7 並びに参考資料 1～2 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。

＜具体的対策例について＞

- JEITA 半導体部会では BCP のタスクフォースを立ち上げ、半導体工場がどのような被災をしたか、それに対してどのような対策をしたかという対策事例集を取りまとめている。サイバーセキュリティにおいても対策事例を取りまとめていただくことは多くの企業にとって非常に有意義な活動になると考えている。
- 新しい事例があった時に、どのように周知し、産業界での情報共有チャネルをどのように作っていくかが非常に重要である。クリティカルな情報を外に出すと攻撃の対象となる場合があるため、選ばれた人たちの中で共有する必要があるが、他業界での勉強会の情報を共有するという方法も考えられる。
- OT ガイドラインの 4 章に FSIRT についての記載があり、工場向けのガイドラインであるためと思うが、装置に対しては PSIRT での対応が必要になる。FSIRT と PSIRT の連携について記載すると良いのではないか。工場の担当者、FSIRT の担当者と装置メーカーの PSIRT 担当者を結びつける枠組みを整理いただきたい。

⇒（事務局）本ガイドラインに CSIRT、PSIRT、FSIRT の図があるが、企業全体のガバナンス構造の中での各 SIRT の考え方の例を記載している。御指摘の点を、拡充する方向で検討したい。

＜サプライチェーン対策評価制度について＞

・ NIST CSF では Tier でマチュリティを整理しているが、OT ガイドラインでは Tier のようなマチュリティの考え方を導入する予定はあるか。
⇒（事務局）現段階では成熟度の考え方は取り入れていないが、将来的には考慮し得ると考えている。

・ OT ガイドラインをサプライヤー全体に広げていくことに対して、どのようなイメージを持っているか。
⇒（事務局）サプライチェーン対策評価制度を活用することを考えており、半導体業界でも実証を行い、コストや実現可能性を検討したいと考えているが、この制度は検討中の段階であるので、必要な項目があればご意見をいただきブラッシュアップしていきたいと考えている。なお、この基準を作成するにあたって、自工会・部工会のガイドラインを参考にしており、そのチェックリストから厳選した 25 項目が★3、44 項目が★4 として設定されているとイメージいただきたい。

・ 自工会ではヨーロッパのサプライチェーンとの連携まで検討が進んでいる。実施している取組や苦労していることなどを情報共有する場を作っていくことが非常に重要であると考えている。この SWG を活用して自工会との情報共有の場を作ることを検討してもよいのではないか。

・ 各企業がどの★まで達成しているかを取りまとめた非公開なデータベースなどは検討されているか。
⇒（事務局）自己適合宣言ではあるが、登録制にすることも検討している。発注者が調達要件に記載したり、契約サプライヤーに対して★のレベルを求めたりする仕組みを想定している。

・ 登録制については IPA が担う方向で議論が進んでいる。加えて、評価結果データに対する信憑性をグローバルに担保する枠組みについても議論されている。

・ 評価制度について、お客様からのプレッシャーがあれば企業は★を取得すると思うが、要求されるから取得するという形ではより高いレベルのセキュリティ対策を突き詰めていくイメージが沸かない。それに対してサイバー保険は、セキュリティ対策を実施すると保険料が下がるメリットが企業にあるため、各社が積極的にセキュリティ対策を行う要因になると思う。サイバー保険と連携しこの制度を普及させる施策はあるか。
⇒（事務局）どのように普及させるかという点が一番の課題である。保険もアイディアとして出ており、保険業界の方にも委員に入っていただいている。★を取得していると保険料の見積もり額が低くなる等の可能性はあるが、個々の具体的な仕組みは制度ができた後に議論して考えていきたいと思っている。

・ 評価制度については、有償で★を取得することをイメージしているか。
⇒（事務局）★3 は自己適合宣言ではあるが、登録料はかかることになると思う。また、★4 については、第三者が有償で評価し認証を取得することを検討しているが、できるだけ安価にしたいと考えている。基準自体は HP に掲載し自由に使えるが、客観性を担保するための登録制度や第三者認証は有償の予定である。

・ サプライチェーン対策評価制度は企業を評価するものであり、製造装置や IoT を評価するものではないという認識で合っているか。
⇒（事務局）認識の通りである。IoT 製品に対する制度として別に JC-STAR 制度がある。

＜グローバルとの整合について＞

・ OT ガイドラインを遵守することで、グローバルのお客様から見た際にどのような価値や意味を持たせることができるかが重要である。NIST CSF や CMMC2.0 を次のステップアップのターゲットとしていただけると説明がしやすい。OT ガイドラインの位置づけや認識を高めるための取組は考えているか。
⇒（事務局）本ガイドラインは、NIST CSF2.0 半導体製造プロファイルと整合性を取って作成している。

・ SEMI SMCC としても、グローバルな基準と日本の基準について、どこが共通項目であり、どこが日本独自

なものであるか、経済産業省とコミュニケーションしていきたいと考えている。各国と同様、国内においても SMCC との連携が進められており、検討した内容をグローバルな基準としてどのように取り込んでいくかにフォーカスしたいと考えている。

⇒（事務局）SMCC との協力的な関係を構築することは重要であると考えており、本 SWG には SEMI 様も参加いただいているが、一案として、SMCC と本 SWG が共同で会合等を開催することも考えられる。いずれにせよ、SMCC とのコミュニケーションは継続していきたい。12 月に開催される SEMICON JAPAN も大きなマイルストーンになると考えている。

＜レガシー装置への対応について＞

・ 半導体業界ではレガシー装置が多いため、それを解消するような支援があるとよいと思う。例えば、フロント PC の交換やレガシー装置の更新に当たり、支援をいただけると非常に助かると考えている。

⇒(事務局) レガシー装置をどのようにアップデートしていくかは、一つの大きな課題であると考えている。単に政府からの支援で解決する問題ではなく、技術的面での課題解決も重要であると考えている。この場でも議論しながら、必要な研究開発への支援も含めて検討していきたい。

・ 政策を検討するにあたり、ICSCoE の人材を活用してはどうか。電力業界の取組では、最初から意識的に ICSCoE の人材に入ってもらった結果、多くの新たな施策が彼らから提案された。非常に参考になると思う。

⇒（事務局）ICSCoE は一年間の育成プログラムであるが、卒業研究のテーマとして、レガシーOS の効果的なアップデート方法について研究してもらうといったアイディアも考えられる。

＜普及に向けた取組について＞

・ OT ガイドラインの普及に向けた取組として、経営層の認識を高めるという点も重要な要素と考えている。JEITA 主催の経営者が参加する会議等の場で、経済産業省から半導体産業 SWG についてご講演いただくなど、業界団体をうまくご活用頂きたい。

＜クリアランスとの関係について＞

・ このサイバーセキュリティ対策の取組は重要経済安全保護法やセキュリティクリアランス新法との関連付け等は考えてられているか。

⇒（事務局）内閣官房にて能動的サイバー防御の導入に向けて議論しており、官民で情報を共有するための枠組みが設立される予定である。電力やガスインフラ事業者などの基幹インフラ事業者がメインであるが、それ以外の関係する事業者も参加することができ、一定程度機密性が高いものについてはクリアランス制度を所得している人に限り共有することなどが考えられる。

以上