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1回会合)
議事要旨

1. 日時・場所

日時:令和6年11月26日(火)13時00分～14時45分

場所:新東京ビル7階セミナールームS(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、高原委員、中川委員(オンライン)、長野委員、浜島委員、東委員、藤井委員、三井委員、渡部委員、中西様(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 本サブワーキンググループの議事運営について(案)

資料4 事務局説明資料

資料5 JEITA半導体部会様講演資料

資料6 SEMI様講演資料

4. 議事内容

冒頭、経済産業省商務情報政策局 武尾サイバーセキュリティ課長および金指情報産業課長から挨拶があり、次に、事務局より資料4の説明があった。続けて三井委員より資料5、浜島委員および東京エレクトロン萩尾様より資料6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。

＜守るべき対象について＞

- 材料メーカーやコンポーネントメーカーも検討の対象に含めても良いのではないか。
- OTガイドラインは、継続的な半導体デバイス生産活動を守るために作成する認識であるが、先端半導体デバイスの技術情報や顧客から開示された半導体設計情報はどう守るのか。
  ⇒(事務局)資料4の21・22ページに記載があるが、知財や情報の流出については、ITセキュリティ対策基準の作成で対応したいと考えており、OTガイドラインの検討から始め、後半にかけてITセキュリティ対策基準の中身を検討していく。
- サプライチェーンのセキュリティ対策評価制度SWGの成果を本SWGに展開できる。他にも、ビル、工場、自動車等のSWGがあり工場ガイドラインは組み込み工場に焦点を当てた汎用的なもの、自動車業界においても工場ガイドラインベースに検討を深めブラッシュアップしたものを作成している。検討において他業界の取組みを参考にする必要があれば、他のSWGからエキスパートを呼んで話をしてもらいたい。
- 国内にはレガシー半導体を手掛ける企業も多く、これらの製造や設計に関するノウハウも価値がある。
  ⇒(事務局)レガシー半導体の重要性も認識しており、先端に議論を閉じるという意図では全くない。ノウハウについては、メーカー内に閉じた製造ノウハウだけでなく、顧客とのすり合わせ等も含め様々なノウハ

ウがあると認識。サイバーセキュリティの観点から、先端半導体とレガシー半導体との違いも含めて、様々なご意見をいただきたい。

- 国際標準に準拠することは極めて重要であり検討を行うにあたり整合性を確保していただきたい。
- 委員の各企業がやるべきことを実行することが重要であり、国は支援を行うものの、業界が主体的に取組まないとグローバルでマーケットを失ってしまうとの認識を持つ必要がある。
- 検討の進め方に関して、資料 6 に記載の SMCC プログラムカレンダーに作業部会のスケジュールを整合させてはどうか。これにより、日本で検討した内容をグローバルに発信し、グローバルの検討内容を国内に展開することが可能になる。OT ガイドラインは来年の夏頃に公表との説明があったが、これを SEMICON West で発信するなど、良いトラクション（牽引力）が作れると思う。
- サイバー攻撃の事例リストに日本企業が入っていない理由はあるのか。
  ⇒（事務局）掲載している事例は公表されている情報をまとめたものであるが、公表されていない国内企業が攻撃された事案が複数あり、決して日本企業が狙われていないということではない。
- 情報を守るため自社で情報のラベリングをしっかりと行っている。このベースがないと、守るべきものが何か優先順位が付けられないので、情報管理のガイドラインなども今回の検討に必要と思う。

＜ガイドラインについて＞

- SEMI E187、NIST CSF 等に書いてあることは当たり前のことが多く、どこまで実装するかが重要となる。OT ガイドラインでは、E187 より少し広い範囲をターゲットにして、グローバルな半導体企業がここまで実装すれば良いというものにすると使いやすいものになると思う。例えば、CSF のティアと対応して実装のレベルまで意識を合わせられると監査等の次のステップにおいても意義がある。
- E187 は初歩的なレベルであるが、台湾においても守られていない企業があり、次のステップが大事である。日本から E187 の実装を前提に次はインプルメンタブルなステップを示すことで、日本が国際的な標準化のリーダーシップの中に入っていく構造にすることが重要であり、本 SWG はその良い機会である。
- 半導体工場ではかなりのロボットオペレーションが導入されており、ソフトウェアロボットとハードウェアロボットの両方が工場に入ってくると、それに対するプロテクション、調達条件を調達側が持っておくというのは重要なことになる。調達の際にこれら条件を要求しやすくするため、国として基準を作っており、政府調達の条件とすることが考えられ、このような枠組みを適用するのが一番効率的である。
- 一番重要なのは、企業のオペレーション上のクリティカルな点を把握して対策の優先度を上げていく議論である。他の SWG と違う点があるはずで、そこを明確化するのが非常に重要である。
- 討議を聞いていると E187 を含め対応がある程度進んでいるという認識を持った。サイバーセキュリティ対策に関しては E187 をベースするのが一番わかりやすいと思うが、各社の E187 への準拠状況を評価したうえで、半年間のフィージブルな目標を設定するのが良いと思う。E187 自体は非常にベーシックな内容であるが、結構な数の日本企業が対応できていないと認識している。
- NIST の CMMC 等の認証取得を考えているが、米国基準の認証取得となるため、日本国内で認知されるかという課題はある。国際的な基準の中に日本の意見をうまく入れ込み、日本で同様の認証を取得すると NIST の基準にも合致している状態になると非常にありがたい。
- 様々な業界のやる気のないベンダーからファイアウォールがあるから大丈夫だと聞くが、あくまで補助手段であり攻撃による内部への侵入を減らすことが目的で、インシデントやアタックの可能性を低くするだけのもので、導入するとサイバー攻撃から守れる、他の対策は不要と誤解されないよう十分気を付ける必要がある。デジタル庁等でもセキュリティ対策としてはゼロトラストのコンセプトをベースに置いている。

＜検討スコープについて＞

- 脆弱性が破られた際の PSIRT、CSIRT 等の対処も検討の対象になるか。
- 台湾が企業に要求している対策にはコーポレートガバナンスまで含まれており、インシデントレスポンスの体制もチェックリストに入っている。しかしながら、大企業と中小企業で体制や人的リソースが違うので、業界として中小企業をどのようにサポートするも重要な論点になる。サプライチェーンの中でこれがビジネスとして動けばエコシステムとして回っていく認識である。
- 攻撃アクターにより講じるセキュリティ対策のレベルが変わってくる。いわゆるランサムウェアによる攻撃がターゲットではなく、半導体において国家レベルの支援を受けているアクターを想定する場合、ガイドラインのレベルが変わってくる。E187 では足りずアディショナルな対策を検討する必要があるのではないか。
- ガイドラインを活用する際に、どの製品を選べばよいかという課題がある。この領域についてはこのソリューションを使うとガイドラインの要求事項を充足できるといった情報があると助かる。例えば、工場セキュリティの SOC サービス事業者を性能品質の問題で過去に 2 回変えており、要求事項を満たすソリューションの一覧があると非常にありがたい。
- 国のガイドラインにおいて特定のプロダクトを推奨することはできないが、方法論を実装するプロダクト、ソリューションとの記述はできる。公正取引の観点に注意しながら書く必要はあるが、プラティカルな情報をガイドラインに添付していくことは、業界として実際にやっていることであり、適合していないのではないかという場合に修正箇所をフィードバックすることで対応できる。買う側がベンダーに対して実装すべき要件を言うことも可能であり、業界としてどうしていくかが重要である。

＜人材育成について＞

- 世界的に半導体人材が足りないと言われている中で、セキュリティ人材にも不足感はあるか。また、人材育成に対する具体的な取り組みがあれば教えて頂きたい。米国では、退役軍人がサイバーセキュリティの分野で活躍している話も聞くところ、欧米企業ではセキュリティ人材は揃っているのか。
- どこの国でも半導体人材が不足している中、サイバーセキュリティ人材がどこまで不足しているかなど掘り下げた情報は持っていない。しかし、米国では退役軍人をリソースとして活用することが期待されており、どのように引っ張るかというプログラムもあると聞くところ、一定規模の人材プールはあると思う。
- 米国では退役軍人等様々なサイバーセキュリティ人材がいるが、日本人に比べて給料が 3-4 倍と高額なため、雇用することは非現実的である。日本では、聞いている限り人材がそろっている会社はゼロである。したがって、人材をいかに育成するかが一番重要であり、今いるサイバーセキュリティ人材をいかに取られないということを意識する必要がある。
- 一つの解決策として給料を上げるとの話はでてくると思う。高専を活用する取組みは九州の方で既に始まっている。人材への投資をしっかり行うべきと経営者に対してメッセージすることも重要である。
- ⇒（事務局）人材育成については WG2 で検討しており連携しながら IT・OT 人材、製品セキュリティ人材について検討できればと考えている。OT セキュリティについては紹介させていただいた IPA の中核人材育成プログラム等あり、この場を活用して色々な取組みを実施する必要があると認識している。
- 今までの経験からしてもすぐに育たないので、例えば IT やネットワークを多少理解している人材をいかに OT セキュリティに引っ張り込むかが重要である。
- SOC レベルのテクニカルな部分を判断できる専門家が必要であるところ、難しいとは思うが、企業間でデータを共有することが許容されれば、共同 SOC のような取組みも考えられる。ハイレベルの専門家でも、集約し企業が共同で利用すれば効率化できると思う。
- SOC はアウトソースでサービスを買える状態にあり、AI を使って振る舞い検知を行うプロダクトを提供す

る企業もある。半導体業界としてサービス事業者を選定し情報を共有するとよい。

- 全てアウトソーシングできるかというとそうではなく、企業内でログデータ等を判断できるエンジニアが必要となる。このようなエンジニアを育成する際に、IPA の ICSCoE が実施している取組みが活用できる。電力業界やクリティカルインフラストラクチャー業界で活躍するエースを育成しており、プログラムに参加することでセキュリティ業界との人脈も構築できハイエンドな知識を得られる。新しいものを作るのではなく、既存のカリキュラムに半導体業界として戦略的に人材を投入して育成するのが良い。
- 育成や採用の責任者として退職者の再就職先を聞く機会が多いが、製造系企業でセキュリティ責任者になるケースが増えている。セキュリティの知見や経験を蓄積し事業会社に転職してセキュリティの分野で活躍するといった好循環が生まれていると感じる。また、セキュリティの専門知識と経験を持っていることに加え、自社のビジネスや業務を理解していること、この両方がないと活躍できない。セキュリティ人材については全体の母数が足りないのが事実であり、国も含めて推進する必要がある。

以上