産業サイバーセキュリティ研究会 WG3
「産業界のセキュリティ対策強化とセキュリティ産業の振興の好循環（仮題）」に向けての検討会(第3回)
議事要旨

1. 日時・場所

日時：令和6年10月29日（火） 10時00分～12時00分

場所：オンライン開催

2. 出席者

委員　　：國領委員（座長）、稲垣委員、鵜飼委員、鴨田委員、下村委員、関委員、花見委員、丸山委員

オブザーバ:総務省

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 事務局説明資料（これまでの議論の整理）

資料4 鵜飼委員からの情報提供

資料5 花見委員からの情報提供

資料6 下村委員からの情報提供

資料7 経済産業省イノベーション創出新事業推進課からの情報提供

4. 議事内容

冒頭、事務局より挨拶と資料3の説明があった。次に、鵜飼委員より資料4について、花見委員より資料5について、下村委員より資料6について、経済産業省イノベーション創出新事業推進課より資料7についての説明があった後、続けて自由討議が行われたところ、概要は以下の通り。

■本検討会の方向性や目的等について（意見・質問）

- 資料6において指摘があったが、議論としては国内のセキュリティ産業振興と安全保障は分けて行うべきである。最終的にはセキュリティ製品の国産化の話で、この 2 つを合流させていくことが望ましい。例えば、100 社のスタートアップ企業のうち安全保障に係る企業は 3 社から 4 社程度とすると、まずはスタートアップ企業の裾野を広げるべきである。スタートアップ企業が 10 社程度の場合に全ての企業がトップガンになるわけではないので、安全保障につながる企業が出てくる可能性は少ない。その意味ではスタートアップ企業の支援は重要である。既存の枠組みの中にサイバーセキュリティの枠を設け、積極的な呼込みを行い、最終的には出口戦略として海外進出や上場等に進むことが望ましい。
- 個々の技術や企業、企業群の支援を議論しているのではなく、スタートアップや学生等を含めた日本全体で競争力を強化するところで分かれ道に来ている。議論の視点を明確にした上で、施策を考え、そこで挙げられる課題に取り組むべきである。あるべき姿と現状の整理が必要であり、議論を混乱させてはいけない。
- 資料5で示されたセキュリティ製品やサービスの提供実績についての意見に共感する。また、立場は異なるが各委員のコメントにも共感する。本検討会として、どの主体に対してどのような目標を課すかを明確にすべきである。

■セキュリティ製品やサービスを選定する際の実績主義について（意見・質問）

- 実績主義により、企業の参入が難しいという指摘があったが、以前より同様の指摘がされている。かつて情報通信研究機構(NICT)のテストベッドにおいても同じ問題意識があったと記憶している。実績主義を突破し、スタートアップ企業の商材を迅速に展開させるために、不足している点や手当すべき点は何か。
- 個人的な意見であるが、実績主義は致し方ないと考えている。その前提で申し上げると、サイバーセキュリティ分野においては検証事業者や要員が乏しいため、腹を据えて育成すべきではないか。また、競合他社に運営が委託されており、活用する企業に不安感があるため、制御システムセキュリティセンター(CSSC)に構築した OT 向け検証環境は活用されていないと感じる。
- マーケティングやラベリングの部分で、検証を行った後のスタートアップ企業の面倒をみていくべきである。そのスタートアップ企業の製品等が官公庁に採用され、実績として数えられるという流れが必要である。
- 過去のビジネスの経験から申し上げると、米国企業は国防等の政府調達での実績を売りにしていた。米国ではユーザー企業が強く、そのユーザー企業に製品を試験してもらうことで、試験導入への道につながっている。日本ではその部分が弱い。
- ユーザー企業の人材がネックになっているかについては、大手の金融機関は新しい製品の導入に関心があるが、地方銀行等ではその関心はない。ユーザー企業のレベルに対応していると考えられる。
- 実績主義について、ユーザー企業の問題が大きい。米国企業の CISO と会話した際、新製品の導入が自らのキャリアの評価につながる環境があると伺った。多くの日本の企業では、セキュリティ担当は「あて職」で、担当期間中に失敗できないという思いもあり、積極的に新しい技術や製品を導入する意欲がない。新技術の導入を推奨するという政策は、新技術や英品を導入してみようという意欲がある方にとってはメリットがあるが、そうでない方には効果的ではない。米国のような労働環境になれば、よいのだろうが、労働環境の変化は短期的には難しいようにおもう。

■実績主義と SIer 依存について（意見・質問）

- 実績主義がユーザー企業の SIer 依存にもつながっているのではないか。
- SIer はユーザー企業の御用聞きの側面がある。顧客が製品の導入実績を重視する場合、SIer はそれを越えて提案することは困難である。また、一旦使い慣れてくると、使い慣れたものを使いたいというエンジニアの考え方もある。そのような背景がユーザー企業の実績重視につながっていると理解している。当社もそれだけではなく、とがったスタートアップ企業や製品等に対しては VC 投資や育成も長期的に行い始めているところである。
- スタートアップには実績が問われる点はご指摘の通りである。顧客及び SIer の双方に該当することである。とがったユーザー企業を作ることも大変と理解している。当社は、他のスタートアップ企業の屍の山の中を偶然生き残った。2017 年ごろからニーズが立ち上がり、ユーザー企業にとって他の選択肢が十分になかったため、弊社製品が売上実績を残した。

■セキュリティ人材について（意見・質問）

- セキュリティ人材の不足についてコメントしたい。弊社でも育成を手掛けているが、供給先が限られている。Security Operation Center も労働集約的な現場が多く、大手企業でまとまったセキュリティ供給を受けなければと規模が大きくならない。一部のトップスキルの方が動いているという感じ。スキル面で上位層と下位層で別れてレイヤー化されており、受け皿が小さい。中小企業において自社での運用や運用委託をするなかで、ホワイトハッカーの活用などは限定されている。
- 海外人材の活用について、優秀な人材もいるが、日本語の壁も厚い。レポートを提出したい際に、「てにをは」を直され、本質的な内容に目が向かないところもある。

・ 本来、スタートアップ企業は死屍累々であり、成功は前提にない。失敗を許容する資金の流れや文化の醸成、人材の育成が必要である。製品検証や製品購入に係る規模の大きいファンドは必要であるが、その目的を明確化させる必要がある。育成を目的にした組織はほとんどなく、あったとしても教育機関の位置づけである。産業界と距離があるため、ぜひそのような観点での取組を行っていただきたい。文部科学省も含めて議論すべきではないか。
・ 東北大学などいくつかの大学では大学発ベンチャー等に係る取組を推進されているが、学生の時点からビジネス化も含むセキュリティ人材の育成が重要であろう。市場を拡大する際に入り口、つまりセキュリティを学ぶ学生を増やすことが重要である。ぜひ文部科学省にも取組をご説明いただきたい。
・ ユーザー企業のセキュリティに係る人材パスは論点の一つとして考えられる。CIO という考え方も日本に定着するまでに時間を要したため、セキュリティ人材についても時間を要する可能性があるが、引き続き議論は進めていくべきである。

■政府の支援策について（意見・質問）
・ 需要と供給の議論は避けられない。需要面は非常に重要であるが、ユーザー企業のニーズ喚起は不足している。

■政府調達について（意見・質問）
・ スタートアップ企業からすると、製品等を購入いただくことが一番の支援となる。北米では、官がスタートアップ企業の有望な技術を購入しており、その実績をもとにスタートアップ企業が海外展開を行うという、よいエコシステムが回っている。ただし、WTO のルールからみると微妙な面もあり、当該ルールを遵守としている日本では難しいという理解である。
・ 気概のある企業の技術を官に購入していただき、優遇していただくことが効果的である。他方、ISMAP は海外の大手クラウドベンダーを優遇する仕組みに見え、スタートアップが参入し辛くなっているおそれがある。エコシステムが作られにくく、改めて議論が必要である。
・ 政府調達での活用を想定した際に、育成という目的のため、「より最適化されたもの」を求める一般の調達とは区別された調達の形態を検討されたい。

■法改正等について（意見・質問）
・ 資料6(P.7)の「日本のサイバーセキュリティ産業の課題」にて、「脆弱性検査ツールの開発など、攻撃手法の研究を意図的に避けている」との記載があった。法的な問題の可能性があるということで、攻撃手法の研究を避けているという認識である。ルール改正を期待したい。
・ グローバルサプライチェーンに目を向けた際に、データ保護規制がログの収集や分析等を妨げるケースがある。これらの規制がクラウドベースでのサービス、グローバル SOC を分断しており、当社も現実解の中で対応をしている。ログ内に個人情報が含まれる場合の懸念を指摘されているため、海外展開を想定する場合には当該ポイントの対応も必要である。

■失敗を許容する仕組みや集団的なリスクを引き受ける仕組みの構築について（意見・質問）
・ 法規制対応等がある中で保守的に振る舞うことを是認すべきではない。責任を果たす中でリスクをとることに舵を切っていくべきである。スタートアップ企業を支援する際には、失敗と責任を引き受けてくれる構造を作っていくことが求められるのではないか。責任の議論は重要であるが、失敗したとしてもある程度問題ないとした上で、リスクをとってチャレンジさせることにシフトさせるべきである。
・ 近代法においては合意した関係者間に限って責任関係が生じるが、サプライチェーンにはそれ以外の関係性も連鎖する。サプライチェーンは合意をしていない人の連鎖であり、企業間のつながりは、一直線ではなく三次元的であ

る。責任論は二者間で閉じないため、集団的なリスクの引受けなどを担う共同体が必要ではないか。Asisの話となってしまうため個別企業の話に閉じずに、ぜひ大風呂敷を広げていただきたい。

以上