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1回)
議事要旨

1. 日時・場所

日時：令和6年7月31日（水） 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、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 委員名簿

資料3 事務局説明資料

4. 議事内容

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より本検討会の趣旨に関する冒頭の挨拶があった後、國領座長が議事の進行を行った。次に事務局から資料 3 の説明があり、続けて自由討議が行われたところ、概要は以下のとおり。

＜全体的な討議＞

- 資料 3 の P.29～31 に記載の論点 1～3 に関係する部分で発言したい。調査や仮説の対象が企業、事業単位となっており、企業も大企業と中小企業や供給側と需要側で分けられている。配布資料で示されているものよりも更に一歩進んだ調査は進められているか。進められていないとすれば実施し、議論するべきではないか。
- 支援等の対象は企業とされているが、「サイバーセキュリティ産業」の主体は人であり、能力や権限の有無等が問題となる。大企業を評価する際には、その企業の評価対象が何かを分析することが重要となる。すなわち、実績の有無等を評価する際に、どのような事項を評価しているか。セキュリティ産業として育成すべき要素は何かを明らかにする必要がある。

＜論点１（資料３ P. 29）について＞

- 企業群とあるが、企業の要素まで分解した議論や調査等があれば、今後テコ入れするべき課題がもっと具体化するのではないか。
- 「サイバーセキュリティ産業」の定義がはっきりしていないので、広めにとった方がよいと考える。その上で、注力する領域を理由とともに示すとよい。例えば GDP の向上や安全保障への寄与の観点から領域を絞って取組みを行うこととするべきではないか等。後になって、サイバーセキュリティ産業の内容やその対策についての議論がいろいろと出てくるのは避けるべきである。
- 「サイバーセキュリティ産業」とは、仮説 1～3 で示されたもの全てが対象であると考える。他方で、どこが伸びそうか、

又は重要かを議論するのは難しい。重要なものが生まれるための環境作りについて議論を集中させた方がよい。

- 本検討会のゴールは国として施策を打ち出すことと認識している。民間がやるべきとか研究開発をこのように進めるべきという結論ではなく、国として何ができるのか、こういった研究機関を作る又は補助金を出すといった実際の施策に落とし込むことが重要である。
- 仮説 1～3 で示されたもの全てを「サイバーセキュリティ産業」の対象に含むことは賛成である。

＜論点２（資料３ P. 29）について＞

- 具体的な政策を定めるにあたり、その目標も具体的に設定することが重要である。例えばセキュリティ市場を予測以上に伸ばすことや、セキュリティ投資額を 3 年後までに増やす、攻撃検知数を増やすなどの目標を定めるのが良いと考える。
- 論点 1 にあったセキュリティ産業の定義と論点 2 の世界観が対応しているべきである。政府の政策を起点にしてセキュリティ産業が振興するための構造を構築することが重要と理解している。
- 規制やガイドライン、調達要件等による縛りをきっかけにしつつ、それに適合する製品や企業が普及していく世界観を作っていく。具体的には、技術開発への投資が促進し、製品やサービス等の産業構造が構築され、加えて人材育成や更なる投資が生まれるような仕掛けを通じて、産業がより成長・発展するような世界観を想定するために、産業については幅広に捉えて定義していくとよい。
- 産業のエコシステムを構築する際は、普及の度合いや格付けレベルの底上げを図れるようになるとなおよい。
- 国際標準に我が国の考えを戦略的に載せていくことが重要。国産のサイバーセキュリティ産業の育成に資するものであるため、わが国発の標準が国際標準となる等が記載されるべきではないか。論点 2 には標準化戦略を記載すべきである。
- 製品のセキュリティライフサイクルやボット化の話等もあるが、製品をどう買い替えていただくかも含めて検討するべきで、セキュリティのレベルを上げていくための目線を持つことが重要である。
- UTM すら導入していない企業もあるのが現実であるため、サプライチェーンセキュリティを考慮するとこのような企業の底上げなども必要と考える。

＜論点３（資料３ P. 30）について＞

- 製品の供給側においても、新しいビジネスや製品・サービスがある中で、EDR の先進的な会社としては海外の複数社が挙げられる。ある会社は買収後に供給停止となったし、別の会社も買収後には新しい製品開発が停滞している事例がある。産業を振興させても海外企業に買収され得るというリスク等にどう対応していくかが課題となる。何らかのガイドラインや規制があるとよいのではないか。
- 論点 3 において、政府として支援すべき主体について記載しているが、主体を選ぶべきなのかは疑問である。
- 国産のサイバーセキュリティに関連する製品やサービスが生まれる土壌をどうすれば整備できるかについて検討するべきではないか。
- あえて主体を選ぶのであれば、仮説 2 で示されている「当該事業が技術的・ビジネス的に優位性を持っている、ないしは元来強みを持つ分野においてセキュリティ品質を加えている等、国際競争力を有していると考えられる分野の企業」を支援するべきと考える。
- 対象分野が明確になった際には、その企業をどのように育てるかということを念頭に置いた政策も必要である。
- 企業や業界では単位が大きすぎるため、絞るべきである。また、時間軸を設定して検討するべき。例えば、1 年後と 3 年後、10 年後、20 年後で目標は異なり得る。既に米国に特許がある分野だと 1 年後に国産製品で具体的な成果をあげることは難しい。また、認証を作るとしても、現実的には 3～10 年かかる。どのような時間軸でどのような主体を支援するのかを議論した方がよい。

・ 大学を応援するのではなく、大学のどのような取組み、どのような学生を応援するのかという観点で支援内容を具体化するべきである。
・ 資料 3 を踏まえると、中小企業は支援対象になる認識である。大企業は一握りで、中小企業が 9 割以上である日本において、中小企業を対象にセキュリティを普及させることが重要である。その上で、仮説 1～3 で示されている主体全てを支援できるとよいが、あえて絞るのであれば仮説1で示されている「今後産業界において強化する必要がある分野（セキュリティ対策強化を政策的に促している領域）に必要な製品・サービスを提供する企業」を支援することは重要ではないか。裾野が広いIoT製品や中小企業向けの製品・サービスは応援すべきポイントである。
・ 応援には 2 種類あると考えている。例えばソブリンクラウドのようなものを作って国内で普及させた後に、政府主導で海外への展開を支援するというもの。もう 1 つは、赤青緑の検証等で扱った日本発の製品の海外への展開を支援するもの。海外展開のノウハウを持たないベンチャー企業は多いため、マーケティング面等で支援を行えるとよい。

＜論点４及び５（資料３ P. 31）について＞

・ 日本のベンチャーが海外展開するときに販路開拓が難しいという話を聞く。展示会への出展や英語のマニュアルなど支援してはどうか。
・ ディストリビュータはレッドオーシャンである一方で、そのディストリビュータの活用は重要であると考える。海外で力のあるディストリビュータに認知してもらえれば、製品を販売してもらえるため、そのディストリビュータとベンチャー企業とのマッチングの支援も一案である。
・ ASEAN 諸国は米国 NIST 標準(NIST SP800 シリーズ)への準拠を重視している。海外展開を行う際は標準化とセットであり、我が国の標準が評価され、製品が展開できるようなエコシステムが必要である。
・ 赤青緑の検証事業は、アワードのような取得製品をアピールできる場の整備までを取り組むべきだった。また、製品を省庁に採用してもらうような取組みもできるとよかったが、実現できていない。是非やっていきたい。
・ よいものをつくるだけでなく、販売にもそれと同等の努力を行わねばならない。
・ 国内市場において、ユーザはセキュリティに係る実績から大企業を選択する。一方でサービス提供側の大企業は小さな企業を主たる顧客には選ばない。ここにミスマッチが起きている。
・ 大企業の要素や機能を分解、分析した上で、新しいビジネス領域を検討していくべきではないか。ユーザが製品やサービスを調達する際に、ビジネスの相手が大企業であると手間が少なく済む。但し、大企業に依頼したとしても、実際にビジネスを行う相手はその下請や孫請けの企業となる。なぜそのような仕組みが成り立っているのか。そこを分析し、新しいビジネスの形として提示できるとよいのではないか。そしてそこに中小企業やベンチャーが参画できる仕組みができてくるとよい。実績信託のようなものを作り、大企業がノウハウを提供できるといった新たなビジネス領域を構築するよいのではないか。
・ 機能ではなく、別の領域を議論していることは隔靴掻痒と感じる。
・ 中小企業を中心とした普及を考えたとき、要件がガイドラインで止まっていることに課題を感じている。これが調達要件等になると世界が変わってくると認識している。「IoT 適合性評価制度」は、政府調達等で活用されることが宣言されている。その宣言によって周囲の反応が変わった。単なるガイドラインと大きな差を感じており、一つの理想の姿を実現する際の課題になっていると考えている。
・ 中小企業を対象とした普及の取組みとして、サイバーセキュリティお助け隊サービスやセキュリティサービスの認証等がなされている。これらの取組みはよくできていて、手厚いものになっているが、現行のような任意のものではなく、調達要件などになれば一気に活動の規模が大きくなる契機になると思う。

＜今後に向けた要望等＞

・ 海外政府のセキュリティ政策の動きも、日本政府の競合として理解しておくべきではないか。他国も米国製品に席巻

されているのは同様であり、そこでどうしているか他国の取組みも理解されるとよいかと思う。

・ 先日サイバーセキュリティに特化した投資ファンドが設立されたと聞いている。彼らが、何を課題かと捉えているかを確認したい。

以上