産業サイバーセキュリティ研究会
ワーキンググループ3(サイバーセキュリティビジネス化)(第7回)
議事要旨

1. 日時・場所

日時:令和4年4月6日(水) 13時00分～15時00分

場所:Web開催

2. 出席者

委員 : 國領委員(座長)、東委員、石井委員、稲垣委員、鵜飼委員、栗原委員、教学委員、篠田委員、手塚委員、中野委員、子川委員、花見委員、林委員、古田委員、本城委員、宮澤委員、三輪委員

オブザーバ: 内閣官房 内閣サイバーセキュリティセンター、警察庁、金融庁、総務省、厚生労働省、文部科学省、独立行政法人情報処理推進機構、一般財団法人日本情報経済社会推進協会

経済産業省: 大臣官房 江口サイバーセキュリティ・情報化審議官、商務情報政策局 奥田サイバーセキュリティ課長、佐藤サイバーセキュリティ戦略専門官、塚本課長補佐、原課長補佐、原田課長補佐、和平課長補佐

3. 配布資料

資料1 議事次第・配付資料一覧

資料2 委員等名簿

資料3 事務局説明資料

4. 議事内容

事務局から、現下の状況を踏まえて、本日はオンライン(Web)開催との発言があった。

開会にあたり江口サイバーセキュリティ・情報化審議官から挨拶があった。

國領座長が、議事進行を行った。事務局から、資料の確認と委員について、東京海上日動火災保険株式会社井口様から教学様へ、ソフトバンク株式会社北山様から中野様へ、富士通株式会社森様から子川様へ交代との発言があった。

次に、本日の議題に入り、事務局より資料3の説明があった。続いて自由討議を行い、各委員より以下の意見があがった。

(1) 論点① 供給サイドの取組の方向性(安心して製品・サービスを利用できる基盤の構築)

- WG3 は「ビジネス」に関して議論する場になるので、検証サービスや検証された製品・サービスに対してどれだけの費用を捻出する価値があるのか、その価値の把握方法として検証有無による価格差など、資金の流れや資金を捻出する意思という観点で調査を進めるべきである。そのうえで、どこの、誰に、どれだけの資金を流す必要があるのかを考えなければビジネスにならない。自発的なサービス利用を促進したいのであれば、費用がどれだけかかるのかという意思決定に対する

情報を提供しなければならず、中小企業であっても価値が分かれば費用をかけるであろう。検証サービスの規模感は提供側の責任の大きさに比例する。現状、検証サービスの供給側には資金が流れていないため規模を拡大させる設計ができていないと考えられる。これらの問題意識を持って取り組むべき。WG3 には企業経営者の方々が委員と参画していらっしゃるが、事業展開の知見をお持ちのはずなので、ご意見を頂戴しつつ進めてはどうか。

- 機器のリリース後に脆弱性が見つかる場合が多発している。機器の検証がワンタイムで終わってしまうことはリスクが残るのではないか。有効期限の設定もしくは定期的・継続的に検証を行うビジネスモデルの検討が必要であり、SBOM 等を使って安全・安心であることの追跡ができるとなお使いやすい。ただし、このモデルではお金の流れや価格体系も従来と異なるはずである。
- 検証サービスを展開している側の意見として、検証ビジネスの市場規模はまだ小さく、相場観も定まっていないため、価格は固定せずに市場価格に任せたほうがよい。検証しても脆弱性が完全に無くなったと断言できないのが検証ビジネスであり、安全性を保証できるのか、といった議論に進んでしまう傾向にあるため、ベストエフォートで提供するビジネスモデルが適切である。
- セキュリティの本質的な性質上、バージョンアップ・アップデートが必ず必要になる。完成品を検証するという手法に加えて、製造プロセスを認証していく方法も考えられる。マイナーチェンジに関しては良く取られている手法である。機器のマイナーチェンジの度に検証を行うやり方では、ユーザが検証することから離れてしまうのではないかと危惧している。

- 本議論では安全保障の観点も必要であり、特に外国人の在籍状況や外国籍企業が提供する検証サービスを供給サイドで把握しておいたほうがよい。一方で、検証技術を保有した人材は少ないため、国家レベルで検証人材の把握や共有、育成が必要である。
- 経済安全保障の観点も踏まえて整理してみてはどうか。他国の取組では、検証結果を調達基準に設定し、その基準を満たした調達リストには、結果的に自国の製品が並ぶことで自国の製品が育つといった流れになっている。また、「攻撃型を含めたハイレベルな検証サービス」においても、安全保障の観点から必要な検証ができる土壌を作り、検証結果の管理方法や検証事業者のクリアランスが必要になると思うので用意していただきたい。
- 半導体集積のような経済安全保障上重要な拠点へのサイバー攻撃に対しては、自治体と経済産業省との連携が必要となってくる。

- 損害保険業界から、どのように支援できるのかを考えている。検証サービスの供給側と検証を受けるベンダ側の責任分界を明確にすることは難しいと感じている。特に検証サービスの供給側がすべて責任を負うということは考えにくい。サイバー保険を展開するなかでの事例では、セキュリティ製品を提供する側が過失を問われる場合があるものの、どこまで責任があったのかを立証することは難しいことがある。今後、セキュリティ製品を検証する側に責任が寄っていくということは、検証事業者のリスクが大きくなることを意味する。専門的業務賠償責任保険という専門職への保険は存在するものの、専門職のリスクを測ることは損害との因果関係を見極めることになり、成熟途上であることから難易度が非常に高いと感じている。このような制度が日本全体で必要になるのであれば、日本政府で大きな保険制度を作り運用していくことも必要ではないか。

- セキュリティ製品の機能有効性検証について、製品ベンダにとって検証することのモチベーションやメリットを定量的に示せるとよい。定量的に示すことが難しくても、検証することの重要性を伝える取組やユーザ企業が検証済み製品を認めることで成り立つ制度をお願いしたい。また、ユーザ企業ではセキュリティエンジニアが少なく、セキュリティ対策を通信事業者やインテグレータにアウトソースする場合が多い。通信事業者やインテグレータといったサービスプロバイダー側の観点における評価があるとよい。
- 赤検証や緑検証について、コモディティ化していない領域や新しい分野においては、時間をかけてまで検証したいと思わせる何等かのインセンティブが必要なのではないか。このような検証を受けようとするベンダが出てくるかどうかはインセンティブに係っている。
- サイバーセキュリティを考える上では明確な基準を定めることが重要である。例えば、最低限実施すべき検証を行っていればリスク値がわかる、となれば保険も適用できるのではないかと思うものの、そのような最低ラインの実施基準を準備できるのか、準備できた場合に損害保険業界の協力を得られるのか、など引き続き検討が必要である。

（2）論点② 需要サイドの取組の方向性（隠れたニーズの掘り起こし）
- 隠れたニーズの掘り起こしは実施しなくてよいのではないか。検証サービスを必要とする人に提供することが重要である。

- 検証ビジネス市場を育てていかないといけないと認識している。現時点では検証済み製品の国際認証から入っていくことが現実的であると考えられるため、今後の検証事業では国際相互認証についても取り組んでいく必要がある。お墨付きを得たものが他国でも売れる、日本独自のものではないといった取組が必要。
- 検証事業の国際相互認証は、脱炭素に関する議論に似ている。取り組みを行っていたとしても、国際的なルールに則っていない日本企業が低い評価となってしまうことがあり、国際的なサプライチェーンから外されることも起こっている。検証事業においても、同じような負のスパイラルに陥らないように注意が必要である。資料には海外のセキュリティラベリング制度が記載されているが、このような制度を日本でも構築できると良く、検証しないと取引できない、サプライチェーンにはいれない、製品が売れないといった状況になり、結果として検証ビジネスのニーズの掘り起こしにつながる。日本だけが厳しい基準を示すのではなく、国際的な動向に合わせ、各国とスピード感を合わせていけるとよい。
- 検証のためのフレームワークや基準が重要であり、その基準が国際標準として認められるのかが重要な論点となるが、既存の取組で整理できる部分があるのではないか。既存の取組では、基準や標準が示され、機器の供給側は基準に基づき製造し、それらの機器を第三者機関が基準と照らし合わせて検証するといったフレームワークが定められ運用されている。このような取組のどこを強化していくのか、ギャップや補完関係のなかで我が国がやるべきところを明確にした上で我が国が先行するといった戦略が必要ではないか。
- 事務局資料の P.60、検証基盤における「製品ベンダ X」、「製品ベンダ Y」は何であるべきかを考

える必要がある。ビジネスを回す場合にはお金の回し方を考えなければならず、そのためにはベンダ X、Y や製品について何かターゲットを具体的に決めたほうがビジネスモデルのイメージが沸くのではないか。経済安全保障の観点からも製品ベンダ Y を何にすべきか、という検討が必要である。

- 官と民の役割分担について、デジタル庁のトラストサービスでも同様の議論となるが、トラストアンカー（例：国、民間）をどこが担うのかが焦点となっている。基準が同じでもトラストアンカーが違えば制度が異なってくる。特に国際的な繋がりを考えると国がアンカーにならないと認め合うことが難しくなり、業界ごとに考える必要がある。パブリックセキュリティとプライベートセキュリティで場合分けを行う必要があるのではないか。パブリックでは国、プライベートでは業界ごとという整理。
- Proven in Japan に関する取組みは、国際的な相互認証等によってグローバルと繋がること、安全性の最新性を担保していくことの 2 点が重要である。最新性の担保は、単一の製品で最新性が証明されていることが、システム全体の安全性にどのように寄与しているかを表現するところに課題がある。また、データセキュリティ（データの暗号化や無意味化、データ交換）の部分で、言語の観点や法制度の観点を理解したうえで正当性を表現できる仕組みを日本で検討し、それらをグローバルに展開していくと、海外で取り入れやすくなるのではないか。
- ビジネス化の促進については、Small Business Innovation Research（SBIR）的な取り組みができればと思う。公共調達や交付金を有効に活用し需要を作り出してはどうか。グローバルシティアライアンスの中でグローバルポリシーロードマップの策定においても、サイバーレジリエンスが取り込まれていたり、スーパーシティ構想では「空飛ぶ車」について議論されていたりする。この様な新しい分野とセキュリティビジネスが連携していくことも重要。
- 日本が世界に合わせるか、日本がリードするかという論点は重要。日本がリードするためには例えば検証事業者においては、検証後に脆弱性が明らかになった場合の責任を何等か負うといったところまで踏み込むべきなのではないか。
- 需要サイドへのニーズ喚起の観点で、IoT 製品等にセキュリティバイデザインを適用していくことは非常にハードルが高いと感じる。本議論の他にも、産業サイバーセキュリティ研究会 WG1 の下に設置された「『第 2 層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース」では、「IoT セキュリティ・セーフティ・フレームワーク」のユースケースを作成している。どんな事業者に対してどんなリスクがあるかを整理した資料があるので、需要サイドの意識を高めるための資料として有効なのではないか。
- 実環境における試行検証では、ユーザ企業が試行検証のすべてを実施することは難しく、インテグレータや通信事業者が重要になってくる。インテグレータや通信事業者にとってのインセンティブもあるとよい。国によるサポートやモチベーション施策があると、日本発の尖ったテクノロジーが日本の産業になっていくと考えられる。

（3）論点③　需要と供給のマッチング

- 中小企業に対してセキュリティ対策の必要性の警鐘を鳴らす必要がある。日本の企業はセキュリティインシデントを恥だと思ってしまい、発生したことを隠してしまう傾向にある。インシデントが発

生した最初の報道はあるものの、インシデント対応の結果が共有されてないがために注意喚起が不十分であると感じる。実名でなくでもよいので、どんな損失を被ったのかを明確に示すべきである。また、国から公平な立場で事実のみを伝えるサイトがあってもよいのではないか。伝える術があればニーズの掘り起こしは必要ないのではないか。

- 各所管する産業におけるインシデントは所管省庁への届け出を義務付けるといった案はどうか。啓蒙は感覚で発信するのではなく、被害の実態を把握して発信すべきであり、このような制度があればインシデントの件数や実態把握、セキュリティ対策の啓蒙、セキュリティビジネスの需要喚起が流れるのではないか。被害に遭った企業の情報公開によって需要が喚起されると考えられるので報告義務等について検討すべきではないか。
- 米国の重要インフラでも報告については法律で義務付けられている。米国においても被害や身代金の支払いを隠す傾向にあり、それを把握する目的で制度化を行った。日本の企業においても、特に重要インフラや政府行政機関は報告の義務化に進むべきであり、検討いただきたい。
- 担当者が少ない中小企業では、即座に対応することが難しい可能性があるため、もし制度設計する場合は報告期限について長めに設定頂けば幸いである。
- 報告については免責と結び付けて考えて頂ければありがたい。

- 論点②にも関連し、サプライチェーンのなかでも直接取引の無い企業に対してはセキュリティ対策の重要性が伝わらないのが現状である。また、サプライチェーンのなかにはリソースが足りず、セキュリティ対策のやり方が分からない企業も多い。そういった企業がどのように取り組んでいけるかについて、SC3 やサイバーセキュリティお助け隊サービスを活用し、トライアルをしているところ。サプライチェーンの委託元から委託先へと、インシデント事例などを踏まえながらセキュリティ対策の必要性を訴えていきたい。
- サイバーセキュリティお助け隊の今後の展開についてもお伺いしたい。実際にサービス提供企業へ連絡するユーザ企業は少ないのが現状である。サービスを買わされるイメージであるため、コンシュルジュの様な相談サービスがあるとよい。また、インシデント発生後の報告窓口もわかりにくいことは政府の継続課題である。これら 2 点をわかりやすく企業へ伝えるべき。エコシステムについては、利用者の声をフィードバックできる仕組みがあるとよい。
- 損害保険会社ではインシデントが発生時に再発防止策に向けてセキュリティベンダ等を紹介することがある。損害保険会社は中立的な立場であることから、IPA で取り組んでいるビジネスマッチングにも貢献できればと考えている。

- 経済産業省が公表した「サイバーセキュリティ経営ガイドライン」は広く浸透している。本文書にはサプライチェーンに関する記載もあり、その中には委託元が委託先の管理監督をすべしと示してある。これらをもっと活用してはどうか。
- 啓蒙に携わることも多いが、なかなか自分事として捉えていただけないことが多い。企業の実態を把握して不足する点を具体的に示すなど、アセスメントの実施やベストプラクティスの提示が必要である。
- 中小企業へ啓蒙する際には、「いくら」と金額を伝えることが重要である。サイバー攻撃により、い

くら損害がでたのか、身代金についてもいくら要求されたのか、などを伝えたほうがよい。

- 需給という視点に加えて、事業者を支える基盤といったもう一つの層をつくり、金融事業者、損害保険事業者、人材育成、能力の供給などについても着眼して取り組んでいけるとよい。

お問合せ先
商務情報政策局 サイバーセキュリティ課
電話:03-3501-1253

以上