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8回会合)
議事要旨

1. 日時・場所

日時：令和6年4月3日（水）　13時00分～14時50分

場所：Web開催

2. 出席者

WG3委員　　:國領委員（座長）、東委員、石井委員、稲垣委員、鵜飼委員、鴨田委員、栗原委員、教学委員、篠田委員、関委員、手塚委員、中野委員、花見委員、林委員、古田委員、三輪委員

オブザーバー　　: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、独立行政法人情報処理推進機構

事務局　　:経済産業省 上村サイバーセキュリティ・情報化審議官、武尾サイバーセキュリティ課長

3. 配付資料

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

●サプライチェーン全体での対策強化について

- 本日示された取組は評価している。中小企業では資金繰りが厳しいことも多い中で、例えば、サイバーセキュリティお助け隊サービス（以下。お助け隊サービスという）を利用した場合に金利が安くなるなどの金融面での促進策、登録セキスペにも見返りがあるなどの取組は現状講じられているか。
- 福岡や熊本では、製造現場の国内回帰が進んでいる。工場内セキュリティに対する意識が高まっているなか、上流企業が海外企業と契約している場合にサプライチェーンの末端の中小企業における対応が厳しくなっているため、そこの支援が課題となっている。自治体による企業誘致が活発する中で、高度 IT 企業などの誘致を検討している団体もいるため、グローバルサプライチェーンセキュリティの中でかかる団体と連携していくことが重要。
- サプライチェーンのなかでセキュリティが脆弱であると取引関係に影響が生じ得る環境につき、取引企業などと協力関係を築き、サプライチェーン全体で取組を見える化できると、より広がっていくと思う。
- 政府としてサイバーセキュリティ保険の利用を推奨しているか。米国ではサイバーセキュリティ保険の利用率が 20%程度伸びたが、一方で日本ではそれほどの成長となっていない(5～8%に留まる)。保険を含めサイバーセキュリティ対策をしている事が条件になることから米国では普及した様子。サイバーセキュリティ対策と同様、セットとして検討すべき。
- 中小企業の支援を含めて手厚い土台を築いてきたと評価するが、ガイドラインを卒業してルール(事実上のルールを含む)に移行してもいいのではないかと思う。
- 可能であれば各種取組の目標を定めたい。例えば、中小企業の何割程度が検証済みのサービスを利用するか、お助け隊サービスを利用するかなど。それらを可視化できれば、国際的にもかなり高い水準に到達できるのではないか。

- 需要喚起という意味で、ガイドラインからの卒業を考える時期にも来ている。かねてよりサプライチェーンへ呼びかけをしてきたが、Tier2 までは声が届くが、Tier3 以降は声が届かずなかなか動いていただけない実態がある。中小企業だけでなく、セキュリティに弱い企業が含まれるため、中堅企業も支援の対象としてルールについて検討いただきたいと思う。
- ガイドラインからルールへの移行という点について、サービスや製品を導入するには需要側でコスト負担をしなければならないという風土が必要である。情報提供、広報を含めて検討いただきたい。
- 現状でも下請法や独占禁止法、不正競争防止法などあると思うが、例えば、セキュリティに関するルールというよりも開発や調達に際しての見積りチェックについて、細かいところに目配りする必要がある。発注者側にコストを負担させることを前提として、見積に組込んでいることを証拠で立証するための立法やルールが必要であろう。

●サイバーセキュリティお助け隊サービスについて
- 早期から関与し様々な課題を感じてきたところ、今般２類を新設した点は高く評価する。
- 中小企業の意識も高まっているところ、自身も継続的に取り組みたいと考えている。また、日本におけるサイバーセキュリティ事業や産業振興とお助け隊サービスをうまく結びつけられないかと考えている。また、経済安全保障上の課題とセキュリティ対策がセットになるとよい。うまく政策がリンクされることを期待する。
- 2000 社程度の実績がある点も言及があったが、日本の中小企業全体からみるとわずかとなっている。審査期間が長い、価格上限付近に多くのサービスが張り付いてしまっているなどの経済的な課題もあるなかで、上限については２類で価格を上げるという説明があったが、価格や補助率の向上が必要と思う。
- ２類は１類の拡充とされているが、２類への参画にあたって「１類サービス登録から２年」や「１類サービスを１年以上にわたり 10 社以上提供している実績があること」といった 3/15 付の IPA 発表の条件は市場に投入されるサービスのハードルになる可能性があるため、撤廃されるべきと考える。
- ２類の新設について賛成するが、どのように需要を喚起するかが重要。自社の顧客には 100 名以下の企業もいるが、取引先から求められるため受動的に対策を実施しているという声もあり、能動的な取組が深く浸透しているわけではない。
- インシデント対応時の回復措置も必要と考える。初期化してクリーンインストールという方法が一般的だが、ある程度の規模になるとその対応では事業継続性に懸念がある。
- 外部で講演した際に、まだまだ認知されていないことを実感した。中小企業の相談先には税理士等など多いことから、そこを経由して認知拡大を図ることも一案である。

●IoT 適合性評価制度について
- 政府調達での利用などについて報道があったが、日本ではもともと重要生活機器連携セキュリティ協議会などによる認証の取組があったところ、今回の取組はそれらを包含するようなものと理解できるか。また、第三者評価として経産省/IPA がどこまで踏み込んで継続的に取り組むかを注視している。
- 情報セキュリティサービス審査登録制度とともに、基準づくりに加え、評価制度を明確にする点で重要と考える。今後、技術の進展などに応じて基準を見直すとともに、評価についても見直すという取組を、透明性と説明責任を果たしつつ進めることを期待する。もう一つ重要な視点として、規制とインセンティブのバランスがある。よりよい制度とするために明確化を図られたい。さらに、国際基準との関係で日本の制度がガラパゴスとならないようにお願いしたい。

・ 認証で製品上市が遅れる、認定取得コストを考慮して取りやめになるというリスクにも目配せしつつ、海外制度との相互運用は可能な範囲で推進するような取組を期待する。
・ 産官学でエコシステムを構築する際、デジタル田園都市国家構想に係る取組では、IoT 機器を導入する自治体が増えているところ、そこでの活用は検討されたい。
・ 星 1 及び星 2 について自己適合宣言で問題ないか疑問がある。当社で実施する機器検証に持ち込まれる製品には使用するポートがすべて開いているなど、検証を行う以前のレベル感のものもある。顧客は IoT セキュリティガイドラインに関する認識が薄く、製品がすぐにリリースされているところもあり、現実にはもう少し厳しくする必要があるのではないか。

●情報セキュリティサービス審査登録制度について
・ 既に多くの事業者が参加しているが、制度の基準が低く、使う側からしてかかる制度を活用して問題ないかという点の回答になっていない場合がある。安心を求めるユーザーの目線から、より高い段階の認定があってもいいと思う。

●需要側、供給側それぞれへの取組について
・ 今までの取組は不良品を排除するものと認識した上で、需要者はセキュリティ要件が揃った製品を求めていると認識すべき。国のエコシステムを作っていくためのプロジェクトと考えた場合に、これまでの取組から範囲を大きく広げていくべき。
・ 欠けている視点として、責任の視点があると思う。需要者側のニーズをどう把握し、最適化するのか、の目配りが必要である。研究開発、人材育成、体制づくりなどがなければ、取組はアドホックなものとならざるを得ない。
・ 顧客と投資家を分けて考えると、顧客観点では、責任の確実な履行、問題が起きた際の填補、訴訟による責任の明確化などに関するスピード感のある取組が必要となる。問題が起きた際の填補という意味では保険があるが、応急的に復旧させるための(電力のエネルギーの価格上昇などにならった)基金が有効ではないかと考える。さらに、責任財産に対して簡単な手続きを実現するなど、目を配っていただきたい。
・ 投資家の観点では、企業のセキュリティに関する取組について、会計制度の中で平準化して対外的に開示できる仕組が必要である。国際会計基準などもあるが、独自の仕分けをしてもよいと思う。
・ これまで日本では集団訴訟制度がなく、訴訟が相対的に少なかったが、意識を高めることが必要。実績の認知を高められる仕組の構築もお願いしたい。
・ 事務局説明は供給側の支援が中心となっており、その点は充実してきていると感じる。次は、それらをどのように市場へ導入していくか、利用していくかを考えなければエコシステム化につながらないと考える。
・ 中小企業の取組が焦点になっていたと思うので、導入のインセンティブ、例えば税制上の加速償却や金融面のインセンティブなど、様々な後押しがあるとよい。

●セキュリティ産業振興について
・ 国産ベンチャー製品の海外に対する売込みを行っているが、門前払いになるケースがある。例えば、英語サポートがなく怖くて使えないという意見に加え、Gartner や Forrester といった知名度のある調査レポート日本企業のセキュリティ投資の振興を図る観点から、政府機関そのものがより活発に投資をするということに加えて、経営者の啓発を進める必要がある。これまではホラーストーリー中心の説明となっていたが、最近ではコンプライアンス遵守のためにセキュリティが必要と説明を行うことで、民間企業において投資がなされるケースがあると伺っている。その観点で、現在検討している IoT 適合性評価制度には意義があると考

えている。

- 日本の企業は制度対応に時間を要する傾向がある。海外製品のみが認定をとり、日本製品がとれないという形になり得る点を懸念しているため、普及にあたっては注意いただきたい。
- 製品・サービス市場の見える化について意識的に発信するとよい。条件を満たしている会社の製品やサービスを国や自治体が積極的に使うことも重要である。セキュリティ品質面の要素も入札の要件に入ると、より一層取組が進むと考える。
- 国産製品の普及を図るにあたっては、人材面として、登録セキスペなどの有資格者を増やすというのも一案だが、サービス提供の効率性を高めることも有効と考える。それらを促すような研究助成などを検討されるとサービス化が進むのではないか。

●人材育成について

- 中小企業の現状を踏まえると、ファイナンシングの観点から、給与面も考慮してどのように人を集められるか、セキュリティを高めることができるかという施策を検討できるとよい。
- 文部科学省のデジタル活用高等人材育成事業のカリキュラムも設定されているところ、こういう取組の位置付けが明確になることで並行して検討が可能になる。
- 総務省でもNational Cyber Training Centerがあるが、セキュリティキャンプなどと同じような人たちが参加しており、やや重複感がある。総務省では自治体向けにCYDERを実施しているが、映像コンテンツが有効とのことであり、民間向けに展開するとよいだろう。
- 数字の大幅な上昇を実現するには学校の巻込みが必要である。本議論と直接関係ない可能性があるが、全てのデジタル人材予算が消化されていないと伺ったことがある。理由があるはずであるため確認されてはいかがか。

●その他

- 昨今、経済安全保障の論点が重要となる中、それをサイバーセキュリティの観点でどのように考えるかを今後議論されたい。
- 提示された方向性は問題ないが、述べた観点を踏まえつつ今後の検討を進めていただきたい。
- 欧州GDPRではインシデント発生後72時間以内、米国証券取引委員会(SEC)では4日以内の報告が求められているところ、日本では同種の取組が出遅れている。例えば、サイバーセキュリティ経営ガイドラインの今回の改定の中で、善管注意義務違反や懈怠による訴訟のリスクを追記したが、同様にインシデント報告についても一定期間内に所管組織に報告を求める旨を追記してはどうか。
- AI関連の研究助成について、米国では中小企業関連の資金を用いてAI Cyber Challenge(※1)を実施しており、取組の参考になる。
  (※1)AI Cyber Challenge (https://aicyberchallenge.com/)
- 海外のカンファレンスに展示しようと思ったが、費用がかかりすぎるため、あきらめた社長の話を伺った。その社長によると、JETROの支援などでジャパンビレッジがあると助かるとのことであった。

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