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5回)
議事要旨

1. 日時・場所

日時：令和6年12月24日（火） 13時00分～15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 Librus 株式会社 鎌田様からの情報提供

資料4 総務省サイバーセキュリティ統括官室 西村様からの情報提供

資料5 事務局資料（これまでの議論を踏まえた仮説）

4. 議事内容

冒頭、事務局より挨拶の後、Librus 株式会社 鎌田様より資料 3 について、総務省サイバーセキュリティ統括官室 西村様より資料 4 について情報提供があった。続けて事務局より資料 5 について説明があった後、自由討議が行われたところ、概要は以下の通り。

＜資料 3 について＞

■ 人材について

・ 高度人材のうち、どの分野のどのような人材が不足しているか。

⇒ ・ セキュリティ診断やデジタルフォレンジックに係る人材は不足している。さらに今後は、より上流のセキュリティコンサルタントも重要な位置づけになると考えられる。

・ セキュリティに限らず、御社で必要とされている人材はどのような方か。

⇒ ・ 上流工程の対応ができる人材が必要である。開発を簡易にするツールが浸透してきており、オフショア開発という選択肢が増える中で、顧客のハンドリングやプロジェクトマネジメントができる人材を増やしていきたいと考えている。

・ 経営的に見て、事業を伸ばすために経理やマーケティングで人材は必要ないか。

⇒ ・ 上場を目指すならば身内としての Chief Financial Officer(CFO)が必要である。

・ Chief Marketing Officer(CMO)のような企業のブランディングや広告運用など、対外的に顧客誘導ができる人材がいれば成長につながると考えている。

■　企業のニーズについて

・　診断のニーズは季節性がある。年度末の 1 月～3 月になると需要が増える。需要が高い時期に人員を配備すると、過剰人員となるおそれがある。どのように対応されているか。

⇒ ・　3 月末を含む四半期末に案件が増える傾向があるが、これは予算消化の意味合いもあると思われる。

・　例えば、生成AIに近いツールを導入した企業から、セキュリティ対策に関する相談をいただくことがある。セキュリティエンジニアがシステム開発や SOC 等の季節性のないものと担当を兼ねることで需要の差を緩和している。

・　セキュリティエンジニアがシステム開発を行うことで、保守現場を想像できるようになり、結果的にセキュリティ診断レポートの質が向上することが見込まれる。レポートの質の向上によって、顧客との質問の手間を軽減でき、結果として、セキュリティ品質を向上させることにもつながり得る。

・　本検討会でも、需要の不足が指摘されている。例えば、月額 5 千円でもセキュリティ製品が浸透していかない中小企業市場において、需要喚起の策はあるか。

⇒ ・　中小企業では、セキュリティ対策がコストセンターの活動になっているという認識がある。サプライチェーンの文脈でセキュリティの取組を拡大させていくことが非常に重要である。大手自動車メーカの部品メーカへの攻撃や暗号通貨に係るウォレットの運営事業者への攻撃も観測されているなか、サプライチェーン全体が被害を受けている。経済産業省でも「サプライチェーン強化に向けたセキュリティ対策評価制度」の検討が別途なされているが、サプライチェーン全体で大手企業起点での需要喚起が重要と考えられる。

・　中小企業の経営者としては、資金調達、融資なども重要な関心事項である。EC 事業者においてクレジットカードが使えなくなったことによって、事業をたたむケースがみられている。サイバーセキュリティに取り組むこと自体が企業の持続可能性、ブランド、安心感につながるような施策を構想できれば、中小企業もより積極的に取り組めるのではないか。

■　日本における競争環境/企業の対策状況について

・　資料 3「サイバーセキュリティ産業 振興にかかる御提言」(P.3)には、ベンダー（サービス）の As Is が記載されており、日本にとって悪くない内容との認識であるが、これはベンダー（サービス）にとってビジネスの土壌があるものと理解してよいか。

⇒ ・　我々としてはビジネスがしやすいと考えている。サイバーセキュリティの分野でなければ、これほど大手企業を含めた顧客に恵まれなかったのではないか。日本では大手 SIer が顧客を持っており、SIer には提供できない価値を提供することで、当社は市場に参入している。売り上げを立てられないという声を外資ベンダーから聞くが、SIer が顧客を深く握っていて参入が難しくなっている側面があるのではないか。

・　日本のセキュリティベンダーを買収する動きもあるが、成長産業であるセキュリティベンダーを売りたいと思っている企業は少ない。

・　国内でサービスを提供する土壌はあるものと再認識し、これも切り口の一つであると理解した。

・　日本の企業ではセキュリティの防御能力がある程度高い一方で、レジリエンスは低いという発言があった。具体的にはどのような脅威への対処が欠けているのか。

⇒ ・　二重脅迫を含むランサムウェアの脅威が大きい。日本企業のサイバー防御が優れている理由は、コンプライアンスベースアプローチに基づくところが大きい。網羅的な脆弱性対応等を行っているため、レベルが高い。他方で、脅威ベースの対策も今後は必要となる。従来のコンプライアンスアプローチには限界があり、全ての脆弱性に対処するのは困難である。リスクシナリオを作り、個々のリスク脅威に対する対策を行うことが重要となる。

＜資料 4 について＞

・　高度人材のうち、どの分野のどのような人材が不足しているか。

⇒ ・　CYNEX アライアンスで高度な解析者の育成を目指している。CYDER では、事案発生時に初期対応ができる人材の不足を背景として能力の底上げを目指している。高度なものから初歩段階の育成まで全体的にセキュリティ人材が不足している。サイバー攻撃が質、量ともに拡大しているなか、それに応じて求められる人材の要件も変わってくるものと考えられる。

・　CYNEX アライアンスは重要な取組である。また、海外との連携強化は重要であり、国家間の競争力につながると認識している。総務省として、セキュリティクリアランスに基づく情報取扱の制限についてどのように考えているか。

⇒ ・　セキュリティクリアランスは非常に重要と認識しつつも、扱いが難しい。国を跨ぐ公知情報の共有には、意識啓発や注意喚起は重要である。他方で、公知になっていない情報に対して対処の方針を決めるフェーズだと扱いが難しくなる。少なくとも、CYNEXでは一定の公知性が認められれば、アライアンス内で積極的に情報共有している。脆弱性情報等の扱いを決めるフェーズでは、特別な扱いは継続する。CYNEXでは関係者間で情報を共有できるコミュニティを目指しており、情報共有の必要性は論点としてある。国全体の状況の進展を踏まえながら議論としては継続している状況である。

・　国産製品のテスト実施等の実績はどの程度あるか。また、費用等は必要か。

⇒ ・　NICT が保有している技術を踏まえて検証を行う。申し込みをいただいて、製品を持ち込んでいただく企業の制限はない。CYNEX アライアンス参画者に対して、考え方に沿って環境を提供している。

＜資料 5 について＞

■　「セキュリティビジネスにおける仮説③」（P. 5）について

・　仮説はやや唐突感があるが、エコシステムの形成が重要である点は従前の通りである。

・　「後押しすべき主体」に示された①～③について、様々な課題がある中で重要なものを示しているという点を追記されたい。

・　「後押しすべき主体」にベンダーを含める必要があるのではないか。後押しする主体は重要であり、指摘は、後押しすべき主体の記載にこれまでの議論内容が含めきれていないのではないか、という趣旨と理解した。

■　「これまでの議論を踏まえたセキュリティビジネス振興に向けた考え方」（P. 6）について

・　競争力不足という現状に対して、リソースや場の不足が課題とされているが、なぜリソースや場が不足しているかを深掘りした分析が必要である。エコシステムの構築については資料 4「データ負けのスパイラル」(P.2)を参考としつつ、なぜ好循環のループが築けていないのか、なぜ悪循環のループとなっているかを理解しやすい絵があるとよい。

・　「現状」と「目指す姿」が書かれているが、「主な課題」と「政策対応」の論理性がやや弱い印象がある。網羅性の観点で深掘りが必要と感じる。

・　最終的に目指す姿と KPI を設定した点は非常に高く評価できる。KPI は、政府調達の数や海外での市場規模も考えられる。

・　「政策対応」に「ベンダー間協働のための枠組み構築」とある。JNSA にも多くのセキュリティベンダー会員がいるとこ

ろ、このような取組はできていなかったので、今後検討したい。企業の表彰についても JNSA との連携も想定される。

■ 「必要な施策検討の方向性」(P.7)について

・ 全ての問題はヒトとカネに行きつく。示されたものは既存のものが多く、これらを続けても大きな効果は見込めないのではないか。課題とのつながりを明確化されたい。

・ 「これまでの議論を踏まえたセキュリティビジネス振興に向けた考え方」(P.6)の「政策対応」と関係すると考えられるが、その関係性がクリアでないため、それらを明確化されたい。KPI や KPI の時間軸を明確にするとストーリーとして分かりやすくなる。

・ 時間軸の要素を追加いただきたい。どのような将来に向けて何をしようとしているかを明確化すべき。具体的に目標を達成するために、ヒトとカネを動かさねばならない。時間軸を定めて、短中期でマイルストーンを書き込むことで具体性が出る。

・ ポイントは記載いただいた通りであり、違和感はない。これらがどういった切り口で悪循環ループから好循環ループへの変化に寄与するかが分かりやすく記載されているとよい。

・ 3 つの方向性が示されている。①は技術に係るもの、②は売り手の環境整備に係るもの、③は人材育成に係るものである。3 つの趣旨が一見してわかるようになっているとよい。

・ 国産化の議論の前段として、人材育成の担い手である企業、大学、産学の共同事業体を組み合わせて徹底的に人材を育てる枠組みの構築が必要である。「必要な施策検討の方向性」に、人材育成産業の育成も追加いただきたい。

・ 人材育成の観点で、初等教育からの働きかけがないと裾野が広がらないのではないか。裾野が広いと高い山ができるが、今のままでは弱いのではないかと感じる。

・ 本検討会はセキュリティビジネスの振興がメインターゲットで、人材育成は経産省全体で取りまとめられるとよい。

・ 国際標準を含む標準化戦略も必要ではないか。

・ SIer の影響が大きい点は日本特有の事情と考えられ、SIer に扱ってもらうことが製品の販売拡大に繋がる。また、人海戦術を必要とするサービスはレバレッジが効かないため、それが効くようなサービスも必要である。SIer に扱ってもらうためにはユーザーニーズに働きかけていく必要があり、初期としては、調達等でユーザーニーズを作り出す必要があるのではないか。好循環の状況に乗るためには、初期段階だけでもユーザーニーズを喚起すべき。

・ 事業者のセキュリティに係る調達力が弱い可能性がある。ベンダーの提案に頼らざるを得ず、事業者に主体性がない。事業者の弱さが、新しい製品の導入につながらない根本原因ではないか。

・ 「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引 Ver. 1.0」の「SBOM に関するツール」には、国産サービスとして唯一「yamory」が示されている。「yamory」ホームページ上では、同手引書で紹介されたツールであるとの記載があり、2024 年には関連する特許出願もあったことからビジネス的な好循環を生み出して

いると伺える。これは手引書へのツールとしての掲出が事業成長に有益である証左といえるのではないか。他方、取り上げられていない国産ツールもあり、適切な情報吸い上げと更新による啓蒙が必要。このようなツールを広く掲載して紹介することが重要ではないか。

以上