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1回) 議事要旨

1. 日時・場所

日時:平成30年4月4日(水) 10時00分～12時00分

場所:経済産業省 本館2階西3共用会議室

2. 出席者

委員 :國領委員(座長)、東委員、飯島委員、石井委員、石原委員、稲垣委員、鵜飼委員、鴨田委員、栗原委員、手塚委員、花見委員、古田委員、宮澤委員、三輪委員、本島委員、山内委員

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、総務省、外務省、防衛装備庁、独立行政法人情報処理推進機構、一般社団法人日本情報経済社会推進協会、一般社団法人JPCERTコーディネーションセンター

経済産業省:商務情報政策局 寺澤局長、前田大臣官房審議官、伊東大臣官房審議官、奥家サイバーセキュリティ課長、土屋サイバーセキュリティ課企画官

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 本会議の運営について(案)

資料4 サイバーセキュリティビジネスの現状と今後の取組の方向性

4. 議事内容

冒頭、寺澤局長から以下の通り挨拶。

- IoTが進む中、サイバー攻撃のリスクが広がると同時に、攻撃のインパクトも大きくなり、サイバーセキュリティの重要性が益々高まっている。
- 上記観点から昨年12月27日に産業サイバーセキュリティ研究会を開催し、産業界を代表する方々と関係省庁の幹部の方々に集まっていただき、大臣出席の下で会合を実施した。これだけのメンバーが集まるのは例がなく、サイバーセキュリティに関する産業界・関係省庁の関心の高さの表れといえる。
- 研究会では、サイバーセキュリティの重要性を発信し、具体論を議論する場として3つのWGを立ち上げた。WG1では、産業界、サプライチェーン全体で必要なセキュリティ対策を示す、サイバー・フィジカル・セキュリティ対策フレームワークを検討する。WG2では経営者の意識喚起、人材育成、国際連携について議論をする。
- WG3では、サイバーセキュリティビジネス化をテーマに議論をするが、サイバーセキュリティ対策を進めるためにはサイバーセキュリティビジネスが重要である。非常に難しいテーマであるが、建設的な議論ができるようWG3は非公開とさせていただいた。皆様から率直なご意見をいただき、活発な議論ができればと思っている。

事務局から本WGおよびサイバーセキュリティビジネスの現状と今後の取組の方向性について説明の後、課題および今後検討が必要な事項について、自由討議を行った。委員からの意見は以下の通り。

（1） 現状の問題意識について

- for security と with security は両方大事だが、世の中でセキュリティというと for security しか大事だと思ってもらえない。サプライチェーンの末端になるほど with security に関して非常に関心が薄く、そこが問題だと思う。メイドインジャパンにはセキュリティが入っていて安心だという with security を世の中へ広めていくことが重要ではないか。
- 金融の世界においては、従来の金融システムを for security でどう守るかという世界から、Fintech の技術にどのように投資をし、顧客へシステムを活用したサービスを提供できるかといった with security の世界に変わってきている。
- セキュリティにおいて for と with の関係が示されているが、今までは守りと攻めということで考えてきた。守りはコストになるので経営者判断としては難しい話だが、一方で攻めについては、デジタルエコノミーをいかに活性化していくかという中でセキュリティが重要な武器になると考えている。
- サイバー保険市場は、北米と比べて一桁以上少ない状況である。まずはセキュリティ対策を行ってから、保険に加入するというのがあるべき姿だが、上手く回っていない。また、実際の事故情報が少ないことも、保険が普及しない要因となっている。このような問題点を整理していかないと、サイバー保険の普及が進んでいかないのではないか。
- 日本は、ユーザに対するサイバーセキュリティの情報発信が少ない。見せ方や情報発信の仕方一つで、企業のセキュリティ分野への関心も高まり、セキュリティ産業成長のきっかけになるのではないか。
- セキュリティ製品やサービスを契約する際に、インシデントが発生した際に誰が責任を負うかといった点について合意形成がしっかりされていないため、トラブルが発生することがある。中小企業では特に、実際にインシデントがあった時に、どのように対応すれば良いか分からないといった企業が多いため、契約時の合意形成をしっかり実施するべきである。
- International Cybersecurity Center of Excellence を英国、米国、日本の主要大学で立ち上げている。英国の場合は GCHQ が大学のサイバーセキュリティについて認可しており、米国は NSA、DHS が同様に認可している。それに対して日本にはそのような仕組みがないことは課題である。

（2）今後の検討課題について

- セキュリティは製品やサービス単体で売り込むのではなく、日本独特の産業・企業構造を前提に、どのようにセキュリティをシステムに組み込んでいくかを考える必要がある。
- 導入実績の有無が障壁となる課題はベンチャー企業に限った話ではなく、高度な技術を売りにするとお客様から PoC の実施を要求されることが多い。技術自体を売り込むのではなく、経営課題や社会課題を解決するためにこの技術が必要だというアプローチが重要。例えば自動運転などの社会課題を解決するものに対して、セキュリティをどう組込んでいくかという視点を入れて考えるべき。
- 製品・サービスだけではなく、人、ルール、プロセス等もセットで日本のイノベーションを輸出していくことを業界横断で検討すべき。こうした仕組みがあれば、日本のセキュリティ産業が強くなっていくのではないか。
- サイバーセキュリティの観点で、日本の中の、誰の、何を、何から、守るのか等しっかり整理して、検討していく必要ある。今後、日本国内で知財や知的な財産を守り、育てていかなければ、日本はサイバーセキュリティの領域から排除されてしまう。知財戦略や知財を生み出す人間を育てることが重要である。
- サイバーセキュリティは全産業に寄与する課題であるため、各省庁横断で取組んでいくことが重要である。国家全体の価値序列をきちんと定め、それに従って、法による支えとともに、法規制と運用を序列づける取組みを、関係省庁と協力して具体的に行っていくことが大切ではないか。

・ 企業が海外展開する際に GDPR の関係等、海外の法制度を意識する必要があるため、海外の法律において気を付ける点が整理されているとよい。
・ 日本の強みである分野（例えば、センサー等）の技術を活用したインフラ基盤の構築にセキュリティサービスを組み込んでいくと良い。こうした事例を発信することも重要で、例えば業界共通のインフラ構築に関連した日本版の大きなセキュリティビジネスを外へ発信できるとよい。
・ サイバーセキュリティは評価の高い製品・サービスを導入すればよいというものではなく、それらをどう活用できるかといった組織的な対応力が重要となる。このため、事業者側のサイバーセキュリティに関する組織力をレーディングする仕組みがあればよいのではないか。また、レーティングが上手くできれば保険業界でも評価指標に使えると思う。さらに、レーティングによって、企業の競争力が強化されることも期待できる。その結果として日本のインフラも強くなるのではないか。
・ データの視点で考えると”ナショナルセキュリティのデータ”、”重要インフラのデータ”、”プライバシーのデータ”などが混在してネットワーク上を流通している。これらをしっかりと定義づけてどう守るかについても議論した方がよい。
・ 信頼性のあるシステム・サービスを日本としてどうやって世界に発信していくかを考えないといけない。システム・サービス・ツールに分けて考えると、ツールを提供する上での重要なことはいかに量を出すかということだが、日本の製品群は独立して作られているため量として小さく、日本の弱みでもある。それに対してシステム・サービスは量ではなく、いかに信頼性があるかが重要となる。そういった考え方を整理して、日本としての戦略を考えるべきである。
・ 自動運転や車はもはや自動車産業ではなく、モビリティサービスという考えにもなっている。モビリティサービスにおいては自動車だけがセキュアであればいいというものではなく、他のサービスも含めて考える必要がある。
・ フィジカル側の時間感覚とサイバー側の時間感覚が全然違うことに留意する人用がある中で、都市開発に今注目している。都市の寿命は大体 50 年と長く、開発コストも数千億という規模になる。都市開発は官民両方の資金が入り、今後、データ利活用による都市マネジメントが広がっていくことを考えると、サイバーセキュリティも新たな論点となりいいチャンスだと思う。日本はもともとフィジカルが強いのでインフラ輸出においてもサイバー側の産業と組み合わせて輸出するなど、日本としてどういう戦略を持って都市開発戦略を立てるのかも検討するべきではないか。
・ セキュリティ製品・サービスの品質評価については 3 つの視点が重要になると思う。1 つ目は機能性について。悪意あるものは何かを見つけることはセキュリティ上非常に重要である。攻撃者は、現存するセキュリティ対策をかい潜り、常に攻撃手法を進化させてくるので、進化する未知の悪意あるもの（攻撃）への検知力確保は永遠の課題である。2 つ目はパフォーマンス。検知するのにどのくらい時間かかるのかという点である。今ある情報が明日には陳腐化している情報ということにもなり得るので、いかに早く新鮮なデータを提供するかがセキュリティ上重要である。自動車を例にとると、「セーフティ」の観点から検知時間が例えばマイクロ秒単位で行えるかと行った要件が出てくる。3 つ目はユーザビリティ。単に可視化することも大事だが、制御業務と不可分な運用等に結びつくような使い勝手も重要である。
・ 競争領域と非競争領域をどのように区別するかという議論が必要。共通部分はみんなで使えるようにすればよい。非競争領域については現在でも JICA の支援策等の部分的な制度はあるが全体としては不十分だと思う。まずはリストアップしてきちんと整理したほうがよい。
・ テストベッドの共有化、人（研究者）を守る環境を作っていくところも具体的に検討してほしい。

（3）ベンチャー企業の検討軸について

- 日本のベンチャー企業が北米に比べて苦戦している要因は、マーケットインが上手くいっていないからではないか。アメリカは成長させたい産業や会社があれば、政府がその製品を買って鍛えた上で、導入事例を出し、ベンチャー企業のマーケットインを進めている。今後、日本のベンチャー企業が成長するためには、北米モデルのように政府がベンチャー企業のマーケットインを支援する仕組みが必要ではないか。
- 今後、新しいサービスを世界に発信していくためには、技術のキャッチアップも重要だが、日本人の独自性や個性を出していくことが必要ではないか。もう一つは連携が必要。オールジャパンで連携して日本の製品やサービスを世界へ発信していけるとよい。
- 日本の企業もコーポレートベンチャーキャピタリストとして海外の企業へ投資しているが、日本のベンチャー企業への投資は活発ではない。日本のベンチャー企業への関心をより高めるには、どうすれば良いかという観点からも議論する必要があるのではないか。
- Fintech におけるベンチャー企業の関係性という意味では、今までのような金融システムの体制ではできなくなってくることもある。一方でこれから新しく出てくる Fintech サービスにおいては、金融機関だけでは作れないので、様々な業種・業態の出資構造による新しい会社で進めていくことも考えられる。しかし、リリースの話になると、金融機関系だとセキュリティベンチャー企業と組んでサービスを構築したことを公表しづらい問題が出てくる。どうしても、リリースが裏を返せば、攻撃対象をさらすようなものともなる為のリスク管理的な発想が生まれてしまう。
- ベンチャー企業の導入実績の課題を解消するのはなかなか難しいと思っている。この課題をどのようにベンチャー企業に乗り越えさせるか、スタートアップをサポートする仕組みが重要ではないか。
- ベンチャー企業の育成という観点では、実環境でテストできるとよい。製品を作ってもお客様の環境に持っていくと上手く動かないこともあるため、実環境でテストできることはベンチャー企業にとっては重要である。
- ベンチャー企業の育成という観点では、セキュリティ企業を継続する上でも 3 つの視点がある。1 つ目はセキュリティインテリジェンスとしてのデータ。IoT/制御分野でも何が悪意あるものかは検体を集めて分析しないとわからない。検体がないとベンチャー企業でいいアイディアがあったとしても実装にはつながらない可能性があり、いかに多くの検体を集め、そこから必要なデータを得られるかがポイントになる。2 つ目は解析基盤。最近だと AI/ML やビッグデータ解析を行うクラウドを使うというケースもある。こういった基盤をある程度共通化してベンチャー企業にも使えるようにするといいのではないか。3 つ目は人。人材育成を行っていくことは重要である。脆弱性診断のように、「データや解析基盤に強く依存しなくても尖れる人材を活用したセキュリティビジネス」は無いかという視点からの検討は考えられないか。

以上

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