第2回　産業サイバーセキュリティ研究会 議事要旨

1. 日時・場所

日時：平成30年5月30日（水） 8時00分～9時00分

場所：経済産業省　本館　17階国際会議室

2. 出席者

委員　　：村井委員（座長）、宮下様（石原委員代理）、鵜浦委員、遠藤委員、岩野様（小林委員代理）、
中西委員、船橋委員、阿部様（宮永委員代理）、渡辺委員

オブザーバ：内閣サイバーセキュリティセンター　中島センター長、三角内閣審議官、警察庁長官官房　植田審議官、
金融庁総務企画局　油布参事官(金融庁　佐々木総括審議官代理)、総務省　谷脇政策統括官、
外務省総合外交政策局　大鷹審議官、文部科学省大臣官房　藤野審議官、
厚生労働省大臣官房　大橋審議官、農林水産省大臣官房　山本審議官、
国土交通省大臣官房　大野審議官、防衛省防衛装備庁長官官房　藤井審議官

経済産業省：西銘経済産業副大臣、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、製造産業局　多田局長、
通商政策局　福永サイバー国際経済政策統括調整官

3. 議事概要

冒頭、西銘経済産業副大臣から以下のとおり挨拶。

1. 第1回研究会では、日本の産業界が直面するサイバー脅威と、目指すべき産業サイバーセキュリティの方向性について議論いただいた。私たちはこの研究会のもとで3つのWGを設置し、御意見を具体化するための検討を進めてきた。
2. 本日は、各WGの検討を踏まえてまとめた産業サイバーセキュリティ強化に向けたアクションプランについて、御議論をいただきたい。このアクションプランは、1）サプライチェーンサイバーセキュリティ強化、2）サイバーセキュリティ経営強化、3）サイバーセキュリティ人材育成・活躍促進、4）セキュリティビジネスエコシステム創造の4つのパッケージで構成。
3. 皆様にはアクションプランを具体的に進めていくにあたり、どのようなことに注意していくのか、今後さらに取り組んでいくべき点などについて忌憚の無い御意見をいただきたい。

次に、座長から以下のとおり挨拶。

1. 本産業サイバーセキュリティ研究会におけるサイバースペースと実空間が重なり合うという視点に立つと、サイバースペースは初めからボーダの無いつながり方をしているという意味で、サプライチェーンは川上から川下まで全てつながる。また、産業という意味では、産業を超えて新しい産業が生まれたり、産業がつながって新しい連結ができたり、これもサイバー空間のなせる技である。このような視点でサイバーセキュリティを議論していくというのは、とても重要なことであり、世界の中で非常に高く評価されている分野ではないかと考える。
2. 本研究会は、産業面、国際関係、そしてサイバーセキュリティに関する人材ということについても大変大きな役割を担っていると考える。
3. 出席されている委員の皆様方の活発な議論を期待している。

事務局から、産業サイバーセキュリティ強化へ向けたアクションプラン（資料3）及び国内外のサイバーセキュリティを巡る情勢（資料4）について説明。

各委員からの意見は以下のとおり。

（1） サプライチェーンサイバーセキュリティ対策について

- サイバー・フィジカル・セキュリティ対策フレームワークは、フィジカル空間の中でのサプライチェーン、フィジカル空間とサイバー空間のつながり、サイバー空間の中でのつながりと網羅されており、よくまとまっている。海外でも展開をお願いしたい。ただ、実際のユーザ企業に対する対策につなげるためには、具体的で実践的なガイドライン、事例集があるとより有効。
- セキュリティレベルを上げるほど、利便性やアクセス性が欠けるなど、マイナスの影響もあり、数人で経営するサプライヤーには大きな負担にもなる。そういったサプライヤーに対して、どこまでの情報についてセキュリティをかけるか、が議論になる。
- 製品を作るときの高機能部品、高機能装置などを購入して使う場合に、その中身がセキュリティ上、変なものを組み込まれていないかを気にせざるを得ない。いま、国内だけで全てを調達して組み立てることは、なかなかできず、部品や機器を世界から買ってこざるを得ない。そのようなものに対して、どのようなプロテクトをしていくか光を当てていく必要がある。
- 非常に速いスピードで、進化し、物量が増えているIoT機器に対して、どのような認可、認証の方法でセキュリティを確保するのかという問題である。早急な対応策が必要。

（2） 経営・サイバー保険について

- 経営に対してセキュリティの重要性を認識してもらうために非常に苦労しているという話をよく聞く。コーポレートガバナンスシステムの中で、サイバーセキュリティ対策を位置付けることは非常に有効な手段。
- セキュリティは結局守り、攻めに行かないので企業もどの程度お金を払って良いのかわからない。インシデントが起きると途端に大変だということになるが、それまではセキュリティ対策が出来て当たり前の体制で、地味な活動をしないといけない。セキュリティ対策のレベルを保つためには、年間最低限1,000万とか1,500万とか基準を業界で作る必要がある。
- セキュリティ対策のレベルが分からないと保険というものが効いてこない。「どこまで対応をしているので、どこまでの保険はある」というような仕組みを考える必要がある。
- 日本では、中小企業の数が約90％程度あり、日本経済を支えている。日本全体で考えると中小企業のサイバーセキュリティ対策は非常に重要な意味を持つ。中小企業のネットワークがIoT時代にどのようなネットワークに接続される可能性があるかを検討したうえで、中小企業が持つネットワークの内容に応じて、サイバーセキュリティ対策の適切性を検証し、セキュリティガードレベルのランキングをすることができることが望ましい。これができると、セキュリティガードレベルに応じた保険対応が可能となり、中小企業のセキュリティ意識、対策が進むと考えられる。

（3） 中小企業のセキュリティ対策について

- 中小企業が、サプライチェーンとして繋がっていく中で、どのようにやっていくのか、まだ模索状態にある。「お助け隊」を是非具体化していただきたい。
- 今年4月に発表した企業IT動向調査結果では、経営者のサイバーセキュリティに対する認識は、全体平均36%で昨年よりは上がっているが、まだ十分ではない。特に売上高が100億円未満の企業だと2割程度。

- セキュリティ費用については、中小企業のリスクに見合う、身の丈にあったセキュリティ対策が必要。
- 「サイバーセキュリティお助け隊」の構想が盛り込まれているが、特に地方での体制の充実をお願いしたい。
- コーポレートガバナンスコードに基づくガイドラインで個別企業に対するプレッシャーをかけていくというのは結構なことだが、中小企業にとってはとんでもないプレッシャーになる。上場企業と中小企業との取組のウェイト付けをやってあげる必要がある。中小企業も取り組みやすいプロセス論を用意すべき。
- 「お助け隊」自身がある種ネットワーク化しないといけない。心配しているのは分散した「お助け隊」ができあがること。ピラミッド的に連携体制ができている「お助け隊」でないと実現が難しい。
- 中小企業のセキュリティ対策は非常に大事。中小企業の体力から言って専門家は雇えない、雇えても1、2人。横のコミュニティでお互い切磋琢磨して行かないと、企業の中でもアイソレイトされた状態になってしまう。

(4) 人材について

- 産業サイバーセキュリティセンターでは、経営戦略層のところはCISOを対象にした2日間プログラムを年4回位やっているが、レベルや議論の深さなどが正直言ってまだ足りない。今後の戦略マネジメント層の育成をどうするかが大きな課題。
- 若年層の教育強化を考える必要がある。理科学的な能力は一般に18歳がピークといわれており、能力を高めるには、この時期までの教育が重要。
- インフラ、NW機器やソフトウェア等、サイバーアタックに対する脆弱性を理解する上では、実機実習が必須。初心者による最低限の理解レベル習得でも2週間程度、機器を占有して使用する必要があり、もう少し高度の方を育てようとすると6ケ月間の占有が最低限必要となる。実習機器の整備が、質、量、両方の観点から必要。
- 高専レベルとか、もっと中学生レベルから、全員ではなくポテンシャルを持った人を早く作っていく手法が必要。人材育成にとって一番大事なのは、これが自分の10年後、20年後にどれだけ役に立つ、価値のある事かを明確に示すこと。ホワイトハッカーがスタープレーヤーであることを早く明確化する必要がある。

(5) 安全保障について

- 安全保障を口実としてセキュリティ対策のルールメイキングに取り組むといった保護主義的な動きがあり、また囲い込みのリスクもある。地政学をしっかりと押さえていくべき。
- ウクライナに対するサイバーアタックについて、ハイブリッドウォーであったという分析が出された辺りから、オールオブソサエティーアプローチという概念が安全保障では出てきた。サイバー攻撃にはオールオブガバメント、政府一丸だけでは足りなくて、社会一丸となって対応すべき。
- サイバーに費やす人と金が日本より一桁、二桁大きい国がある現実を踏まえて、どういう付き合い方をすればよいか、国と産業界が一体となって真正面から取り組む必要がある。

(6) 日本としての取組について

- 日本の優位性のためにも、セキュアブートのような形で、全ての機器や端末を全部チェックするというような技術、体制が必要。受身ではなく、むしろ逆に攻勢に出るといった考え方が必要。
- 日本はサーバーセキュリティに対するソフトエウェア開発が遅れている。日本のサーバーセキュリティ能力を上げる上では、脆弱性の検証を、AIで行う方法の開発が重要。

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