第5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：令和2年6月30日（火）　11時55分～13時

場所：経済産業省本館17F国際会議室

2. 出席者

委員　　：村井委員（座長）、阿部様（泉澤委員代理）、大林委員、篠原委員、中西委員、船橋委員(Web会議での出席)、渡辺委員

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、外務省、文部科学省、厚生労働省、農林水産省、国土交通省、防衛装備庁

経済産業省：松本経済産業副大臣、商務情報政策局　西山局長、奥家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　第5回産業サイバーセキュリティ研究会事務局説明資料

4. 議事内容

冒頭、松本経済産業副大臣から以下のとおり挨拶。

- 本研究会では、2018年5月にアクションプランをとりまとめ、2019年4月にこれを加速するための3つの指針を示してきた。前回第4回会合では、新型コロナウィルス感染症に対応するため、デジタル化が急加速していく転換点にあることを踏まえ、すぐ取り組むべきセキュリティ対策の実施を呼び掛ける「産業界へのメッセージ」を公表した。
- 本日は、高いレベルのサイバー攻撃の脅威が常態化するいわば“Cyber New Normal”ともいえる時代に対応するための1～3年程度の期間に取り組むべき課題について、さらに、その先、電力など様々な社会機能がソフトウェアで実現されていく時代における“IT基盤インフラ”のあり方について、この2つの観点からご議論いただきたい。
- 議論に先立ち、経済産業省から一つ提案したい。経済産業省では6月12日に昨今のサイバー攻撃事案などの状況をまとめた報告書を公表し、サイバー攻撃が日々高度化しており、サプライチェーン全体に広がっているという実態を明らかにした。もはや、単独企業の努力だけでは高度化、多様化するサイバー攻撃に適切に対応することが難しくなってきている。そこで、本日の研究会において、産業界が一丸となって大企業と中小企業が共にサイバーセキュリティ対策に取り組んでいくサイバーセキュリティ強化運動を推進するためのコンソーシアムの立ち上げを事務局から提案する。
- 日本の産学の最前線で引っ張る皆様方からは、本日事務局からお示しした案に捉われることなく、大所高所から率直かつ踏み込んだご意見を頂ければ幸い。

次に、村井座長から以下のとおり挨拶。

- 私たちは歴史的変化を経験している。インターネット、サイバー空間が社会のプラットフォームとなっている。色々な機能が縦割にサイロ化していたものが、今後は全ての産業分野や、世界全体で横に繋がるようになる。
- さらに、職場や家庭といった生活エリアでサイバー空間の役割が広がっている。そして今、サイバーセキュリティの問題が大きな変化を迎えている。是非、皆様とのご議論でこの問題に対するアイデアを集めていければと思う。

事務局から、資料3についての説明。

続いて、以下の自由討議を行った。委員からのコメントの概要は下記の通り。

新型コロナウィルス対策に伴う急速なテレワーク等デジタル化の拡大による対応の必要性

- 国民は、今回、デジタルがライフラインであるということを強く意識した。政府が率先してサイバーセキュリティに取り組む必要がある。
- 骨太の方針でもNew Normalが言及されている。EUはコロナ後の戦略としてグリーンとデジタルを掲げていて、その際にサイバーセキュリティを本格的に強化することを明言している。日本では、サイバーセキュリティがまだ遅れていることを痛感している。
- 今後、テレワークが定着、深化していくことは間違いない。働き方の変化に合わせて、セキュリティ対策も考え方、発想を変えていかなければいけない。シン・テレワークシステムはこの変化に即した非常にスピード感がある素晴らしい取組み。
- テレワークの導入において、今まで準備をしてきた企業と、そうでない企業で明らかに大きな差が生じている。これまで日本はインシデントが起きた後の対応が主だったが、今後は官民ともトップダウンで先手を打っていく必要がある。

中小企業を含むサプライチェーン全体のセキュリティ確保について

- 産業全体での取組、例えばコンソーシアムのようなものと、業界ごと、地域ごとのようなリスクを共有しやすいモノの間の取組を並行して進め、いわば縦糸と横糸を組み合わせたようなきめ細やかな取組をしていくことが必要。
- 海外拠点からの攻撃、侵入などの問題が出てくる中で、やはり最後は現場での防御力が大切。
- 製造業のみならず、グローバルにサプライチェーンを繋いでいく過程で、異なるシステムを工夫しながら繋いできたが、そこが狙われている。サプライチェーン全体でのセキュリティ対策が必要。コンソーシアムを是非進めて欲しい。
- 中小企業のテレワークが急速に進んでいる。一方で、半数の中小企業がテレワークセキュリティ対策に不安を感じているとの調査もあり、セキュリティ対策関係情報を分かりやすく発信するなど、中小企業も安心してテレワークを始めとしたIT投資に踏み切ることが出来るように、環境整備が急務である。
- 中小企業の支援を行うサイバーセキュリティお助け隊は、1,000社以上が参加して大きな成果をあげているので、経済産業省はしっかりとPRしていくべき。
- お助け隊実証事業のように、民間企業同士の連携によりセキュリティを地域・中小企業に浸透させる取組みも拡大している。今後も、セキュリティ対策がリスクマネージメントの一環として中小企業に自然と定着していくことを期待。

工場を含む制御系のセキュリティ対策について

- 工場においてデジタル化・IoT機器の導入が急速に進む中で、IoT制御系システムのセキュリティ対策が出来ていないので、急いで進める必要がある。体制と人材をしっかり強化して国際社会をリードできるようにしていくべき。
- 家庭や企業でロボットやIoT、等の使用が増えてきているが、使用者が知らないメーカー・製造元であることが増えている。こういったIoTデバイスを誰がどこでチェックをするのか、そういう仕組みは今のところないが、やらなければいけないことだと思う。
- 「産業IoT」という言葉だと病院や大学など、自分たちは関係ないと考える人が出るなど、領域を狭めかねないので注意して欲しい。

基盤インフラの検討の方向性

- 基盤インフラの基礎となるオープンシステムなどは、グローバルコミュニティで開発されている。オープンシステムやオープンソフトウェアを使っているときに、日本の企業が単に使う側に回るのではなくて、優秀な技術者が積極的にグローバルにコミュニティに参加できるようバックアップしていく必要がある。
- 長期的な基盤インフラの構築には、公共性という価値観を設定すべき。データの共有は公益性を生じさせることになり、しっかり国が主導権をもって議論を深めて欲しい。

国際社会で日本の強みを活かす取組について

- 国際情勢が厳しさを増す中、サイバーセキュリティにどれだけ強いかということが、世界における対抗力にもなっていく。日本は安全保障の観点からもサイバーセキュリティ強化の意識を明確に持つべき。
- DFFTのコンセプトの下、日本が世界に対してサイバーセキュリティにおいて貢献できることを主張していかないといけない。
- 今、必要なのはグローバルな情報力と、機動力・スピード、フレキシブルな対応力。今まで以上にスピード感が求めら
- 経済安全保障の面では、各省庁の縦割を廃した対応が必要。また、政府と企業が深い信頼関係とパートナシップを組み、非常に機微な部分を共有しなければいけない。
- 日本の大企業の技術やサービスのクオリティの高さなどは海外も注目しており、日本的なセキュリティの取組に対する期待もあると思う。

その他

- セキュリティ対策について多くの企業が不安を感じているが、大きな要因は人材不足。企業におけるセキュリティ人材の育成も課題。企業では社内のセキュリティ対策を企画構築できるようなセキュリティマネージメント人材が求められている。

村井座長から、自由討議のまとめとして以下のとおり御発言。

- 地方の中小企業、一次産業や医療等、多くの分野がオンライン化を進めている状況に対応できるよう、サプライチェーン・サイバーセキュリティ・コンソーシアムに、国が知見の共有等をサポートすべき。

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