第6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3年4月2日(金) 15時30分～16時45分

場所:Web会議

2. 出席者

委員 :村井委員(座長)、阿部様(泉澤委員代理)、遠藤委員、大林委員、篠原委員、中西委員、船橋委員、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: 梶山経済産業大臣、商務情報政策局 平井局長、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6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、梶山経済産業大臣から以下のとおり挨拶。

- 前回第5回研究会では、大企業と中小企業がともにセキュリティ対策を進めるためのコンソーシアムの立ち上げについて御議論をいただいたが、昨年11月、本研究会に御列席の皆様のイニシアティブにより、「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」が設立された。本研究会の議論をベースに、官民が連携した取組が大きく展開されており、改めて皆様に感謝申し上げる。
- 一方、サイバー攻撃の高度化・激化は更に進んでいる。経済産業省では昨年12月に経営者の皆様に向けた注意喚起を公表し、いわゆるランサムウェア攻撃や、海外拠点経由での攻撃の増加などに警鐘を鳴らした。しかし、昨年12月末には、米政府機関を含む多数の組織が被害を受けた事案が発覚するなど、その後も高度なサイバー攻撃が次々と明らかになっており、サイバー攻撃によって経済活動の基盤そのものが突き崩されるのではないかという不安を感じざるを得ない。
- 本日は、産業界のセキュリティ対策の強化の視点に加えて、攻撃者優位といわれる状況を打開するための、サイバー攻撃に対する国としての対処能力の強化の視点も踏まえ幅広く御議論いただきたい。大所高所から率直かつ踏み込んだ御意見をいただければありがたい。

次に、村井座長から以下のとおり挨拶。

- 2021年は、国会でデジタル関連法案が審議されている中で、全ての分野がデジタルテクノロジーを使った産業分野になると認識することになり、大変重要な意味がある年になる。
- また、デジタル社会は、大企業・中小企業などあらゆる規模の企業の活力を、東京一極集中ではなく全国で結びつけて発展させる原動力になっていく。その意味でも産業界でのサイバーセキュリティが大変重要になる。
- もちろんサイバー空間は我が国だけではなくグローバルな空間なので、国際的な協調・連携も大変活発に動き始めている。グローバル社会の中で日本が、どのような責任を果たすのかも重要。
- 最後に、デジタル社会の推進は、全国民が恩恵を受けることから、国土、社会、生活に産業のサイバーセキュリティが

どのような責任や役割を果たすかが大変重要。ここでの議論が大変重要なので、是非活発な議論をお願いしたい。

事務局から、資料3についての説明があった。

各委員の主な意見は以下のとおり。

サプライチェーン全体でのサイバーセキュリティ確保に向けた対応

- 中小企業を巻き込んだサプライチェーンの取組が随分進んだ一方で、大学などの学術機関もサプライチェーン上重要であり、産官「学」が連携した施策として進めていただきたい。
- 業界によっては、ISACのような企業間連携があって、情報交換ができているところもあるが、他の多くの業界では、そういった仕組みが無い。行政で主導して企業間連携を進めていただきたい。産業界でも協力する。
- サプライチェーン・サイバーセキュリティ・コンソーシアムについて、民間主導で進めるものの、産業政策上の課題とも密接に絡むので、今後とも政府による強力なバックアップが必要。
- 民間化が進むお助け隊サービスについて、お助け隊同士で連携して攻撃への対処にあたるという考え方もある。

中小企業のサイバーセキュリティ

- セキュリティに対する意識は全体として向上していると言えるが、例えば大企業と中小企業、あるいは、業種によって、経営者の間の意識格差がある。国からサイバーセキュリティは経営問題であるというメッセージを出して、格差を解消していく必要がある。
- 中小企業において、新型コロナウィルス感染症の感染拡大を機にテレワークを導入するなど、デジタルの効果に気付いた経営者が多くいるが、それに伴いテレワークのセキュリティ対策が課題となっている。
- 人材や情報、予算の不足という中小企業の課題に対応するものとしてサイバーセキュリティお助け隊サービスに期待。今後、新たに策定された基準を満たしたサービスが公開されることになっているが、例えば、お助け隊サービスの利用を補助金等の審査の加点要素とするなど、お助け隊サービス普及のための支援の検討をお願いしたい。

国の対処能力

- 水道施設への攻撃や組織的な計画的攻撃など、この1年間非常に大きなインシデントがあった。一企業が対応できるような状況にはないと思われるので、改めて民間のコレクティブディフェンス体制と行政からの情報共有を進め、民間のチームの間で手分けをして解決するような方法論を検討し、体制の強化を図るべき。
- 2020年は、サイバー攻撃に関し、従来とスケールが変わった、まさに新しい大変危険な状態の中に突入し、危機感を覚えている。そろそろ専守防衛という考え方では、通じなくなっている。大変抵抗感が強いかもしれないが、これからは、日本も多少の攻撃能力を持つことも想定した法律的な議論を含めて、全体を考えていくべきではないか。
- 国としての対応能力という観点では、経済産業省だけの問題ではないが、海外当局と連携して犯人を逮捕、検挙する能力を持つことが、牽制につながる。
- 事故調について、従来のITシステムへの攻撃に関する分析ではWindowsのOSのような汎用品が分析の対象だが、OTの世界ではシステム一つ一つが全部違うので、分析を含めて対応が難しい。ICSCoEで相当人材が育ってきているので、特にインフラに対するサイバーインシデントに対応する人材をいかに有効に使うかも考えていくべき。
- 政府内のサイバーセキュリティの所掌は、デジ庁やNISCにも非常に限られた権限しか与えられていない。日本では法律や所掌の境界で危機が生じることが多いので、全社会に対してのサイバーセキュリティの司令塔が必要。サイバーセキュリティなくして、ナショナル・サイバー・パワーの構築はない、という認識をもっと強める必要がある。

- 現在の重要インフラ14分野の対策を進めるだけでも苦労したのに、新たなデジタル化の波が押し寄せており、あらゆる産業でサイバーセキュリティが必要になっている。単純な組織論ではなく、国全体のセキュリティをどのように確保していくのかについて、法律的な議論も含めて着手しなければならないのはないか。
- 各省庁で力を集約して対策を強化するべき。

<u>デジタル化の進展に伴う重要インフラの変容と省庁横断的な対応の必要性</u>

- スマートシティやPPPのような事業が増えてくると、もし何かが起こったときに、補償制度が懸念になる。例えば地震保険のように、ある一定の範囲まで民間の保険会社が担保して、それ以上の補償が難しいものについては、国が何らかの形で担保するなどしないと、PPPやスマートシティも進まなくなっていくのではないかと懸念。
- リスクをゼロにできない中で、それを補完する社会の仕組みとして、保険的なアプローチが必要なのではないか。
  大規模技術を社会実装するときに、システムの相互依存のところにリスクが生じるとされるが、現在、サイバー・フィジカルの融合が急速に深まってきている中で、相互依存が大規模な形で進行してきている。これからは、医療機器も含めた制御に関する部分へのサイバー攻撃を通じた人命へのリスクが常態化する。
- 社会・産業の基盤となるインフラに対するサイバー攻撃に対する防御については、防御レベルや攻撃への対処に関するガイドラインを策定し、国と事業者の役割分担を明確にするなど、系統立てて対応する必要があるのではないか。
- 重要インフラは、それぞれが相互依存関係にあるので、その全体像を一度絵に描いてみた上で、どこから着手するかを検討するべきではないか。また、業界間の連携、ISAC of ISACのようなものを作る必要があるのではないか。
- スマートシティなど、色々なデータを持ち寄って全体で価値を作るものは、サイバー攻撃で一か所を叩かれると、その全体最適ができなくなる難しさがある。省庁横断的な対応が必要であり、日本が苦手な部分。どのような守り方をしていったら良いのかを、考えるべきではないか。

<u>その他の御意見</u>

- 今後の社会インフラは仮想化基盤上のソフトウェアで構成されていくようになる。その際、海外技術や海外製品の利用だけではなく、必要な国産技術を保持することが重要。現在、SIP等の国プロで開発している技術を含めた国産技術の積極的な活用についても、検討をお願いしたい。
- 多岐にわたる重要な施策が進捗しているが、受け取る側が消化不良になることを危惧。政策の棚卸をするタイミングでもあるのではないか。
- これからクラウドがますます普及する中で、クラウドの安全性が保たれているかどうかを検証する検証事業者の国内での育成が必要。
- 政府の活動における民間人材の活用やLike-mindedとの人的交流を含めた関係強化には、セキュリティクリアランスが必要ではないか。アクセスするデータの分類自体も変えて、分類に応じてセキュリティクリアランスを設定するなど、少しデータの定義のところまで踏み込むべき。

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