第1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29年12月27日(水) 8時00分～9時30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)、石原委員、鵜浦委員、遠藤委員、小林委員、中西委員、船橋委員、
宮永委員、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:世耕経済産業大臣、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、大臣から以下のとおり挨拶。

1. サイバー攻撃の起点は急激に拡大し、攻撃の手法も日に日に高度化しており、サイバーを通じてどこからどのような攻撃が来るのか、今や、把握することすら容易ではなくなっているのが実情。
2. 国境のないサイバー空間におけるセキュリティの状況の大きな変化は、日本だけが直面している問題ではない。米国でも、欧州でも、中国でも、この問題を深刻に捉え、新たな取組に着手し始めている。
3. 皆さんには、こうした世界的な大きな流れの中で、日本の産業が更に発展していくために、日本のサイバーセキュリティがどうあるべきか、高い目線から、議論をいただきたい。

次に、座長から以下のとおり挨拶。

1. IoT等によって、グローバル空間の中でデータを流通・利用したり、処理する技術が、AI/ビッグデータ処理という形で発展している。産業の中でこれら全てがつながっていくので、データフォーマットなどの共通化が必要であり、イノベーションにつながっていく。
2. 経済産業省の重要な使命は、世界に対する国際標準をどのようにして展開していくかにある。そのことは、どのようにして安心できる・信頼できる技術を展開していくかという世界へのメッセージになる。日本が各産業分野で、あるいは各行政分野で共通のサイバーセキュリティに対するメッセージをしっかり持っていることは大変重要。
3. 産業界のリーダ達で議論するのは貴重。本研究会は、各省庁のオブザーバの皆様にも参加していただいて議論いただく貴重な機会と認識している。

事務局から、産業分野におけるサイバーセキュリティ政策(資料5)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・経営者の意識について

- サイバーセキュリティに関する関心が年々高まっているが経営会議でサイバーセキュリティについて議論しているような意識が高い企業が三分の一程度ある一方で、多くはIT部門任せで、約1割は関心がない。
- サイバーセキュリティ対策について何をいつまでにどこまでやれば良いのか、アドバイスをどこへ求めればよいかわからないという声が多い。サイバーセキュリティ経営ガイドラインが浸透する中で、ポリシーを設定している企業は多いが、体制、設備投資まで踏み込んでいるのは少数。まして、サプライチェーンまではやれていない。多くの企業が悩んでいる実態にある。
- サイバーセキュリティは費用対効果が馴染み難い。政府にはベストプラクティスを全国的・全世界的に収集して示してほしい。
- サイバーセキュリティの取組は、縦横斜めで様々な形で“共有”しなければならない。サプライチェーン全体、業界横断、他の国との連携等が必要であり、一企業、一国のような閉じた取り組みでは不十分。
- 全省庁の関連産業が縦割りにならずに共通の基盤を作ることが重要。
- サイバーセキュリティは「産業を持続させるもの」という認識が必要。安心できるサプライチェーンがあることが日本の長期的なメリットとなる。
- 企業のCIO、CISOが各々の責任・ミッションに応じた対応をしっかり進めていくことが重要。

（2） 情報共有の必要性について

- サイバー攻撃の脅威が増す中、全部を守ることは難しいのが実態。初めに被害にあった人が、迅速に情報を共有して次の人が被害を受けないことが大事。情報共有は社会全体の仕組みの問題なので、是非国が主導権をもって進めてほしい。
- サイバーセキュリティの情報をしっかり共有する流れを作るべき。共有すべきインシデント情報を経営情報と混同し、共有が進まないケースがあるため、共有する項目を明確にして情報共有を促進すべき。
- サイバー攻撃の被害者を批判的に扱うのではなく、被害を受けた情報をいち早くオープンにすることが正しいという価値観をメディアも含めて高めていくことが必要。
- 重要インフラに対するサイバー攻撃は社会活動自体を機能停止させるものであり、特に重要な分野などを整理して、官民それぞれのレイヤで情報共有体制の強化を図るべき。

（3） 中小企業について

- 政府が策定した新しい経済政策に関するパッケージは、中小企業のIT導入を促進するとともに、情報セキュリティ対策に目を向けていくための絶好のチャンスであり、効果的な啓蒙活動に取り組んでいってもらいたい。
- 中小企業のサイバーセキュリティ対策促進のため、3点の見える化が必要。①優秀なベンダ・サービスの見える化、②費用の見える化、③専門家の見える化。
- 企業がサイバーセキュリティのサービスを使い易くする仕組み作り、保険割引などによるインセンティブの付与を進めてほしい。

（4）人材について

- 人材不足は大きな課題。セキュリティを扱える人材は、IT人材の中でも最優秀層であり、すぐに育成できるものではなく、専門人材をユーザ企業単独で確保することは困難。IPAが運営しているICSCoEに人材を派遣し、専門人材を育てているが、それでも人数的に不足している。
- ホワイトハッカーは企業で囲い込むのではなく、社会で共有するようなことを考えていかなければならない。学生が花形の職業としてチャレンジしていくことにもつながる。
- セキュリティに関して、コンサルなど専門企業に支援を仰ぐことになるが、その際にどのような能力のある人なのかがわからないと適切なセキュリティ対策を講じられない。人材の評価モデルを整備してほしい。
- 経営トップを支え、経営と現場をつなぐ人材が必要だが、こうした人材を養成していく取組が課題。長期的な取組の一例として、九州大学が新入生に対してサイバーセキュリティ教育を必修として取り入れている。学校教育の中にサイバーセキュリティの取組を組み入れていくのも一案。
- 小中学校のレベルでも極めて高い技術を持つものが出てきている。こうした若者が更に能力を磨くことが出来る、憧れとなるような高校ぐらいからの専門課程を作るべき。

（5）安全保障について

- サイバー空間の優越が、経済だけでなく、社会・文化の安定、安全保障上も重要な課題であることを明確にするべき。経済、技術、インテリジェンス、戦略という極めて高次なところでサイバーセキュリティは関連する。サイバーセキュリティが新たな地政学のファクターとなる中、国家が企業のサイバーセキュリティを侵害する主役となりつつある。その場合、企業単独でサイバーセキュリティを確保するのは極めて難しい。「敵」は国家であるか、非国家であるかの識別能力の向上を含め、国家に対し国家として取り組むことが何かを明確にして全政府的に取組を進めるべき。

（6）その他

- サイバーセキュリティが重要であることが認識されていても、各省庁がバラバラだと、実際の予算措置の際にプライオリタイゼーションが変わってしまう。デジタル省のような形とか、そのような形でなくても政府内で予算措置のプライオリタイゼーションがしっかりとぶれないような取組をすべき。米国2兆円、日本数百億円で桁が1桁異なっているわけで、日本はよりプライオリタイゼーションをしっかりさせることが必要。

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