第7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4年4月11日(月) 14時10分～15時30分

場所:経済産業省本館17F国際会議室・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、梶田様(大林委員代理)、篠原委員、東原委員、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、デジタル庁、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、防衛省

経済産業省:萩生田経済産業大臣、商務情報政策局 野原局長、
大臣官房 江口サイバーセキュリティ・情報化審議官、
商務情報政策局 奥田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7回産業サイバーセキュリティ研究会 事務局説明資料

資料4 サイバーセキュリティ対策についての産業界へのメッセージ(案)

4. 議事内容

冒頭、萩生田経済産業大臣から以下のとおり挨拶。

- 昨今の情勢からサイバー攻撃事案のリスクは高まっており、さまざまな業種の日本企業を対象として、ランサムウェアを含めたサイバー攻撃が確認されている。また、Emotetと呼ばれるマルウェアを用いたサイバー攻撃による被害も増加傾向にある。こうしたサイバー攻撃の手法は、年々高度化し、特にサプライチェーンの中でのセキュリティが脆弱な部分が狙われるようになってきている一方で、その影響は、攻撃を直接受ける企業に留まらず、サプライチェーンを通じて複数の企業に広がるリスクが高まっている。こうした脅威に対抗していくためには、中小企業や地域の企業、海外拠点も含め、サプライチェーン全体でセキュリティのレベルを高めていくことが必要不可欠。
- これまで、経済産業省では、本研究会に参加いただいている皆様のイニシアチブによって設立されたサプライチェーン・サイバーセキュリティ・コンソーシアムとも密接に連携し、セキュリティの取り組みを中小企業や地域へと展開するための活動を進めてきた。コンソーシアムや本研究会での議論も踏まえて、中小企業に必要な対策を安価かつワンパッケージにまとめた「サイバーセキュリティお助け隊サービス」についても、さらに普及を加速していく。
- 本日、サイバーセキュリティ対策の重要性について、本研究会から産業界に対してメッセージを発出いただくとともに、サイバーセキュリティのセキュリティ強化に向けた方策や、猛威を振るうサイバー攻撃の脅威に屈しない強靭な対処体制の在り方など、幅広くご議論いただきたい。
- 委員の皆様からは、事務局からお示しした案にとらわれることなく、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幸い。本研究会の議論を契機として、産業分野におけるサイバーセキュリティの確保に向けた取り組みが大きく展開されていくことを期待。

次に、村井座長から以下のとおり挨拶。

- 大臣からお話しがあったように、いくつかの大きな背景における変化が急激に進んでいるのではないかと思っている。1つは、デジタル田園都市国家構想。すべての国民がデジタル社会の中で生きていくという体制になると、サイバーセキュリティに関する守備範囲の問題、coverageが産業や地域的な分野でも100%に近くなるということに対応したい。中小企業の話もあるが、従来の産業、企業規模にとらわれない新しい体制が必要なるのではないか。
- 人材に関しても、サプライチェーンとの連携で多様な人材が新しい力を持つことが必要になるのではないか。昨今のウクライナ侵攻、それに伴うEmotetやその他のサイバー攻撃の事象を見ると、ひとつ大きな特徴がある。SNSや流れているデータの分析、衛星画像の解析、こういったものをAI的な手法で分析して、それに対応する力が求められるような状況が多く起こってきています。従いまして、従来の検知やインシデントに対する対応に加えて予知のようなことができるようになっている。こういった技術の変化に対応したサイバーセキュリティの体制、産業構造、あるいは政府の体制も必要なのではないかと思います。
- 本日は、各界のリーダ、責任者の集まり。是非、こういったことを考慮した議論になることを期待。

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。

<u>ロシアのウクライナ侵攻などを受けた国際情勢の緊張の高まりに関して</u>

- 例えば電力グリッドの破壊のような大規模サイバー攻撃が起こっていないことから、ロシアのサイバー攻撃はたいしたことはないのではないかという見方も出ているが、NATOからも発信があったように、ものすごいサイバー攻撃に対し、ウクライナが善戦していると言われている。避難民を輸送するための鉄道網に対するサイバーアタックの防御など、アメリカも相当ウクライナに対して協力しているとのこと。
- ウクライナでは、過去の侵略のときに企業のBCPが確立されていて、セキュリティを含めて仕事ができる体制のプロセスができており、避難した企業の業務回復も早かった。
- 休戦、平和協定に向けて、経済制裁がデスカレーションし、混乱が収束する方向にあっても、その間もサイバーだけは休戦はない。サイバー攻撃は常在戦場であり、同時に無差別攻撃的な色彩が非常に強い。グローバルサプライチェーンの中で一番弱いところが狙われるため、日本のSMEのような弱いところを踏み台にされて攻撃されるというようなことにもなりかねない、グローバルに全てに関わってくるところが大きな注意点である。また、市民も企業も関係なく個々のプレイヤーが参戦するという時代になってしまった。アノニマス始め、攻撃者側も入り乱れて、しかも無差別攻撃的も活動が行われる中で、標的型攻撃が行われている。
- ウクライナ側は、自分の国を自分で守ると意識と能力を極めて明確に示し、国民一丸となって対処している、そこに世界も協力するという展開になっている。自分たちで自分の国を守るという意思と能力を明確に示さないと、世界が味方をしてくれないということも教訓である。サイバー戦、情報戦、認知戦においては、＜世界は自ら助くる者を助く＞という戦い方が重要になってきている。総力戦のグローバル化とでもいおうか。メタバースにおける国家安全保障を強化しなければならない。国民もそこでは当事者意識を持って参画することが求められる。“国民総当事者”社会で乗り切って行かなくてはならない。
- ロシアのウクライナ侵攻で、破壊型攻撃の被害が非常に多かったと言われている。アジア地域でも経済安全保障に関する緊張の高まり、国際関係の動向に注意を払わざる得ない状況にあり、日本でも、同程度の攻撃を受けても被害を最小に抑えるようなセキュリティ対策が必要。我々のシステム、インフラのセキュリティ対策は、同様の攻撃を受けた場合にも大丈夫かどうか、それのチェックと対応が必要ではないか。

- ロシアからの攻撃で非常に特徴的なのは、いわゆる偽情報やフェイクニュースの使用。これらの影響を最小限に留めるためには、日頃から正確な情報収集に加えて、情報の真贋を見極められる点では、独立した機関の準備というようなものが必要。信頼できる情報の発生源の確保、特に正確な脅威情報などをしっかりと発信できる機関が必要なのではないか。
- ネットワークインフラ、そのものがダメージを受けるような場合があるので、その場合は、オルタナティブな情報共有インフラを準備しておくことが必要。
- サイバーセキュリティは、いまや国家安全保障のど真ん中であり、国家を守るもの。国家安全保障で国を守るといったときに、防衛は国が行うこと。しかし、サイバーセキュリティに関しては、まだ民間任せの傾向が非常に強い。これでは国家安全保障の戦いに勝てない。中小企業はコストがかかって大変というが、そこをなんとかしないと国家としての安全保障はできないという時代に入っている。Security is only as strong as its weakest link.と言う言葉があるが、一番弱いところを相手に衝かれると、他をどれほど強くしても全体がられてしまう。

<u>サプライチェーン全体、中小企業でのサイバーセキュリティ確保に向けた対応</u>

- 我が社の、我が組織の重要な部分はインターネットにつながっていないのでサイバー攻撃の心配はないなど、状況を過小評価する声は未だにある。自分たちの持っているアセットが、サイバー空間にどのようにつながっているかという認識、ここを正しく認識することができなければ、その後の対応がないので、この認識をもっとしっかりやる必要がある。
- 多くの中小企業では、セキュリティの専門部署や担当者を置けていないのが実情であり、被害に遭っているものの、それを意識していない（気が付いていない）という状況にあるのではないか。このため、「対策の重要性」を強調するだけでは、なかなか実際の対応は進まない。多くの中小企業はコロナ禍に加え、昨年来からの資源価格の高騰や円安基調、それに続く人手不足や人件費増に苦しんでおり、生産性の向上が欠かせない。雇用の7割を占める中小企業の生産性を引き上げることが、日本全体の生産性を高め、経済を成長させることに直結する。このために、中小企業にとって「デジタル化は生き残りを賭けた重要な経営課題」であると同時に、「サイバーセキュリティ対策も必須」であることを改めて発信すべき。
- サプライチェーン全体での「デジタル化」と「サイバーセキュリティ対策」を進めていくことも重要である。これは中小企業だけでなく、競争力強化を目指す大企業にとっても、取引先の生産性向上や利用継続という観点から有益ではないか。
- 現在、政府は、大企業と中小企業の新たな共存共栄関係を構築するための「パートナーシップ構築宣言」の推進を働きかけており、経済界も普及に力を入れている。宣言のひな型には、大企業による中小企業へのデジタル化推進と、そのための人材育成の支援が盛り込まれている。先月末には、新たにサイバーセキュリティ対策の助言・支援が追加された。政府におかれては、SC3などを通じて発注元に対し、①「パートナーシップ構築宣言」を策定する際は、サプライチェーン全体でのサイバーセキュリティ対策を盛り込むこと、②サイバーチェーン全体で「サイバーセキュリティお助け隊サービス」を活用すること、の2点を推奨し、取組事例の収集と横展開をお願いしたい。
- 中小企業にとってなかなか具体的なセキュリティ対策を取ることは難しい。SECURITY ACTIONはまだ自己認証なので、サプライチェーンの中で使うには、信頼度で十分と言えないところがあるのではないか。プライバシーマーク制度は広く普及していることを参考に、ISMSの認証をもう少し取りやすくするなどの工夫があるとよい。
- 中小企業に認識を高めてもらうためには、より積極的にSC3などを通して働きかけをしないといけない。サプライチェーンという観点では、企業でいえば中小企業かもしれないが、地方も同じ。地方に対するセキュリティ意識を高めることも同等にやっていかなければいけない。
- お助け隊は認知度が低い。これまでの取組をしっかりレビューして、認知度向上に向けて対策を行うことが必要。

国の対処能力

- 事故調査体制について。重要インフラで発生する事故は、社会に対する影響が非常に大きく、安全確保の上で非常に重要な領域。インシデントの発生後、実際に事故が発生したプラントやシステムにおいて、徹底的に原因究明を行い事故の原因を確定することが極めて重要。一方でOTシステムが内包する特殊性があり、解析の大きな障害になることが予想されるため、このあたりを意識した徹底的な調査が必要であり、そのための用意が必要。
- 今年度、サイバー事故調のパイロット実証事業が行われると伺っているが、特殊な領域であるため、ICSCoEでは、OTシステムの専門家たちを集めて積極的に協力をしている。特に各社が導入しているシステムの違いをどのように吸収するのか、調査員が知り得たノウハウとその保存方法、OT独特の課題と解決の方向性なども明確にしていくことが重要。また、事故調の体制に情報を提供していただく企業に事故調の必要性を納得していただくための方法論も検討していかなければならない。
- リモートワークが進み、家庭のWi-Fiなど様々なところが攻撃の侵入ルートとなる懸念がある。侵入を完全には防ぐことはできないという前提で、インシデント発生時に活動するサイバー事故調は重要。ICSCoEは非常に優れた機能を持っているので、coverageを広げて、重要インフラ分野をカバーするかたちで、サイバー事故調を前倒しして強化していただきたい。
- インシデントの被害情報を共有することは、発生防止、あるいは、攻撃阻止の圧力といった場面で極めて重要であり、有効。一方で公表率の低い原因が、被害組織であるにも関わらず、発表することによって不当な非難や、風評被害を受ける可能性があること、そのために被害情報の取り扱い体制の確立、公表はしないが共有するなど、攻撃の特徴や統計情報等を、組織名を非公開、非公表した上で共有する仕組み、さらには社会風土の改革、被害組織のさらなる被害を防ぐ努力も必要なのではないか。
- サイバー攻撃を受けた際の報告や相談窓口の一元化があるとよい。情報を提供した組織、企業が何らかのメリットが得られるような仕組みなどに関しても知恵を出す必要がある。
- サイバー攻撃が発生した後も、国レベルで集まって、報告や情報共有がしやすいような体制を整えていただき、産官学で共有できるような体制をとっていただきたい。
- 国レベル、国際レベルで予兆、検知体制を確立すべきではないか。その情報を共有しながら、中小企業を含め情報を共有して防御することが、日本を強靭なサイバーセキュリティの国にするという意味では非常に重要で、それをしっかりやっているということを見せること自体が、攻撃防御のひとつになるのではないか。
- 産業界の意識改革だけでは対応できない部分も数多くある。事故調や公表のあり方の検討もあるが、それだけではなくて、サイバー被害の未然防止、事故発生時の被害最小化につながるようなことについても力を発揮していただきたい。例えば、攻めのサイバーセキュリティ強化ということであれば、国としてセキュリティ対策レベルの検証機能を設けて、希望者に対して疑似サイバー攻撃を仕掛けて、十分な対策ができているかどうかを確認するというようなことも大事なのではないか。

人材育成

- 情報共有も人材育成に役立つということで、経営層が経験した事例を、若手を集めた勉強会で管理職が講師になって共有するという取組をしている。皆で情報を理解し、対応に取り組んでいくことが必要。いち企業や団体だけでは足りないので、省庁縦割りを排除し、日本全体で人材育成ができるような知恵を出し合い、官民で協力して人材育成に努めたい。
- AI的な分析、データに対する分析能力などがサイバー攻撃の予知・未然防止に繋がっていくと思うが、そのような力を持った人材がサイバーセキュリティの分野で必要。

- いろいろな海外の国々の企業も含めたバリューチェーンが作られて、価値を創造していく形になるわけで、特に我々含めてASEANの方々のサイバーセキュリティレベルを上げていく努力も非常に重要。ICSCoEでは、日本の企業の人材育成を行っており、そのときにASEANを含めて、一緒に訓練を行う仕組みも持っているが、ASEANの人材育成に繋がるようなことについても、政府の協力的な支援をいただきたい。

<u>その他のサイバーセキュリティ対策検討の方向性</u>

- サイバーに休戦なし、常時いつでも起こっていることで、インシデント発生から、報告を受け、リカバリーを行う時間軸に対する考え方、今までのサイバーセキュリティの考え方を変えて、それを前提に体制を作らなければいけないのではないか。
- サイバーセキュリティに関しては、地方、省庁、国際、安全保障といった、組織や分野の縦割りを越えて連携・協調して取り組む必要がある。
- ランサムウェアやEmotetの脅威に関して、注意喚起のメッセージを出すが、我々が見る中で正確な数値情報、統計情報が少ないと感じており、結果として各組織で危機感までには繋がっていないのではないかと思う。政府機関や公的機関でも、正確な数値情報、統計情報を出して納得性の啓蒙を行う必要がある。
- サイバー攻撃で被害を受けた場合のレリジエンス、回復、被害を最小にするといった観点が重要。攻撃を100%防ぐことは難しく、防御を破られた場合に、被害をミニマムにして早期回復させることが重要であり、そういった指針やシステムをどうしていくかという議論が必要。
- サイバーセキュリティ経営ガイドラインにおいて、復旧や再発防止策など、事故が起こった場合の対処方法について強調してはどうか。復旧を図ることも心構えとして大事。
- 攻撃をしにくい、されにくいシステム、インフラをどのように考えていくか、抑止力の観点からの議論も必要。わが国のリアルの世界での防衛の議論があるが、同じようにサイバーの世界でも同じ議論をやっていく時期に来ているのではないか。
- 制御系に関するサイバーセキュリティの認識をもっと高めていく必要がある。例えば、コロナ禍をきっかけに研究機関でリモート実験できるようにしようという動きがある。研究機関では、サイバー攻撃に対して考えていなかったという話がほとんど。病院の医療機器も外部につながっているという観点では、病院の医師は気が付いていなくとも、外部につながっているという状況。そのような観点からも、さまざまな部門でセキュリティ意識は、まだまだ十分ではないと思っている。
- 今回のウクライナ情勢をきっかけに、サイバーセキュリティが戦時であれ平時であれ、それを問わずに国力の重要要素であるという考え方が広がっていく。サイバーセキュリティに関する自立性を高めていく必要がある。予兆検知体制もその一つ。セキュリティ製品の国産率が非常に低い、サイバーセキュリティに関するインテリジェンスについても外国に依存する部分が多いということについて考える必要がある。インテリジェンス・セキュリティ製品の国産化は、簡単ではないが大事な取り組み。
- Proven in Japanだけでなく、予兆に気づくSignaled by Japanや事故調査が終わったとき、あるいは途中に、検証、フィードバックにいれるReviewed by Japan、このようなものの合わせ技が必要。
- Proven in Japanは非常に重要で、これをどのように日本を標準にして民主主義国のサイバーセキュリティ向上に資するようにするか、これは日本にとっても非常にチャンスであると思う。ある意味では投資の分野であるので、日本の強み、世界に売れるところへ持っていかないといけない。
- トータルシステムとしてシステムアーキテクチャ論を考えていかなければならない。デジタル田園都市国家構想を含めた議論が深まっていくと思うが、全体のアーキテクチャ論と並行してデバイスやシステムのセキュリティを考えていく必要がある。もう少し言えば、DFFTは日本が中心となって世界に展開をかけていく上で、with trustをどのように実現し

ていくのかもアーキテクチャ論であり、日本の国家レベルでの全体のアーキテクチャについての議論を起こしていってもらいたい。

- サプライチェーンの一番弱いところ以上の守りはできない中で、東南アジアとのいろいろなサプライチェーンがあり、グローバルにつながっている空間故に、一番弱いところを日本が守ることが、日本の国民を守ることになる。
- 厚労省と連携した医療機関に向けた対策は非常に有益なので、是非、このような場を使って、意識向上を図っていただきたい。

資料4「サイバーセキュリティ対策についての産業界へのメッセージ(案)」について、会合後に公表する旨、委員に了承を得た。

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