第8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6年4月5日（金） 9時00分～10時54分

場所：経済産業省本館17階国際会議室・Web会議

2. 出席者

委員　　：村井委員（座長）、田崎様（泉澤委員代理）、遠藤委員、大林委員、澤田委員、齋藤様（寺田委員代理）、東原委員、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、内閣官房サイバー安全保障体制整備準備室、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、防衛装備庁

経済産業省：上月経済産業副大臣、商務情報政策局 野原局長、
大臣官房 上村サイバーセキュリティ・情報化審議官、
商務情報政策局 武尾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8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、上月経済産業副大臣から以下のとおり挨拶。

- 昨今のデジタル化の進展や世界的な地政学リスクの高まり、サイバー攻撃の深刻化・巧妙化等により、サイバーリスクは高まっている。欧米等では、産業界におけるサイバーセキュリティ対策の強化に向けた制度整備の動きが活発化しており、我が国においても、対策を強化していくことが求められている状況である。
- 企業の経営層の方々にもサイバーセキュリティ対策を将来の事業活動の成長に必要な投資と位置付けていただき、リーダーシップを発揮しながら、積極的な取組を行っていただくことが不可欠と考えている。
- 経済産業省は、我が国の産業界に対するサイバー攻撃を抑制・防御し、事業活動への影響を最小限にしていくために、国が行うべき政策を企画・実行する役割を担っている。政府は一昨年末に国家安全保障戦略を閣議決定し、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるとの目標を掲げている。経済産業省としても、産業界に向けた取組を通じて、このサイバー安全保障の目標にも貢献をしていきたいと考えている。
- これまで推進してきた各種ガイドライン等の整備に加え、今後は政府調達等への要件化などを通じて、サイバーセキュリティ対策の実効性強化を図っていく。今回の研究会では企業の規模や業種等に応じ、適切なセキュリティ対策レベルを評価し可視化する仕組の検討、国産製品の開発・普及促進や高度人材の育成確保に向けた包括的な政策対応の検討、官民の状況把握力・対処能力向上のため独立行政法人情報処理推進機構（IPA）の機能強化といった取組を提案している。その上で、産業界全体のサイバーセキュリティ対策の強化に向け、政府のみが政策を推進するだけでなく、産業界においてもその政策の方向性に沿って、積極的な取組を実施していただくことが必要不可欠である。
- 今回の研究会では、組織幹部のリーダーシップの下で、サイバーセキュリティに対する投資を中長期的な企業価値向上に結実することやサプライチェーン全体での対策強化に向けた意識を徹底することなど産業界の各主体に積極

的に取り組んでいただきたい事項を整理した産業界へのメッセージを発出したいと考えている。本日産業界から参加されている経営層の方々には、産業界を代表する立場として、本メッセージを広く展開いただき、各組織において積極的な取組を奨励いただけると大変有難い。

次に、村井座長から以下のとおり挨拶。

- 2022 年 4 月の前回研究会の開催以降、相当な状況変化があり、産業界のリーダーがサイバーセキュリティについて議論することの重要性が高まっている。
- 変化の一つはコロナ・パンデミックであり、DXの追い風となった。全ての分野が DX に取り組んだ結果として、産業界の全てが繋がっていくという状況になった。そこからサイバーセキュリティに対する真剣さが格段に変わった。結果として、サプライチェーン、役所で言えば、各省庁の各分野に連鎖的にサイバー攻撃が影響を与えるようになった。
- 国際情勢についてもこの 2～3 年で大きく変化した。安全保障と国際情勢の不安定さの基盤そのものにデジタルインフラがある、すなわちサイバーセキュリティは安全保障分野全般の中心的な役割を果たしている。
- 我が国は自然災害から逃れることはできない。これに対するレジリエンスの観点から、世界の中で大きな責任と役割を日本は有していると思う。サイバーセキュリティは、国民の命や国土を守るといったことに直結してくるため、産業界のリーダーの方々が集まり、この経済産業省という場所でサイバーセキュリティについて議論を行うことは、大変重要であると認識している。是非委員の方々の意見を共有する形で、本日の研究会において良い議論ができるようお願いしたい。

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。

<u>サプライチェーン全体での対策強化に向けた対応の在り方</u>

- 取引先のサイバーセキュリティ取組状況については、チェックリスト等での自己評価となっているため実態の確認が難しく、取引先から見れば、複数の企業から様々なチェックリストへの対応が強いられることにより取引先の工数が増加していると考えられる。「サプライチェーン強化に向けたセキュリティ・アーキテクチャの検討」の中で、ガイドラインを一元管理して対策基準を明確化にしつつ、業種横断的なセキュリティ対策レベルを自己評価に加え、第三者認証を取り入れる評価の仕組みについて、是非実現に向けて早期に取り掛かることを期待する。
- セキュリティ対策には際限がないため、どのような取組が実効性があるのかを検討していただきたい。民間の好事例などがあれば、サプライチェーン対策の好事例の横展開も行いながら、サプライチェーン全体の取組を進めていく必要がある。
- 「サプライチェーン強化に向けたセキュリティ・アーキテクチャの検討」について、第三者認証を前提としていることから、認証基準や審査機関、監査人の育成等が必要であり、相当時間がかかると思うので、早期の取組をお願いしたい。
- 経済安全保障推進法との関係性をよりクリアに整理した方が良い。さらに、これまでサイバーセキュリティ経営ガイドライン等を詳しく整備され、社内にかなり展開しやすくなっているが、その他に ISO/IEC 27001 や Common Criteria など、様々な基準がある中で、それぞれの関係をより明確にされると良い。他組織と連携する際にも求めるレベルが明確になればインセンティブにもなると考える。
- 企業としての取組について、何か起きてからではなく、重要な経営課題として日常的に備えをしておき、起きてしまった際には速やかに内外のステークホルダーに情報共有を行って、これからどうやって改善していくのかという雰

囲気を醸成していくことが重要である。また、そのような企業がステークホルダーから評価され、企業価値の向上につながるという社会全体としての仕組みが必要である。

- 認証制度などの方向性が決まった段階で、ロードマップを作成し民間に示していただきたい。前提条件を明確化し、それが変わったらステアリングコミッティ等でロードマップを変えていけるような枠組みを整備されたい。
- 発注側の企業から取引先に対して、どこまでセキュリティ対策を求められるかの境界線が曖昧である。2022 年 10 月に経済産業省と公正取引委員会によって「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」が発表され、取引先への対策の要請に係る独占禁止法・下請法の考え方が示されたが、より具体的なサプライチェーン全体のサイバーセキュリティ向上に向けた取引先との関係構築に関するガイドライン等を提供いただけないか。

<u>中小企業対策の在り方</u>

- 中小企業のセキュリティについて、サイバーセキュリティ対策を実施していると認識している経営者が多いが、実際には一般的な対策に留まっており、脆弱性診断などの専門的な対策は多く行われていない。経営者は費用対効果が分からず対策が進んでいない状況。
- 中小企業の対策について、お助け隊サービスの導入について、中小企業全体からみれば極めて限られており、十分ではない。これまで認知向上を行ってきた点は理解するが、現状このような数値に留まっているのは、知らずに導入に至らない以外にも理由があるのではないかと考えており、導入が停滞している理由について調査いただきたい。
- SECURITY ACTION の自己宣言もまだまだ普及推進の余地がある。SECURITY ACTION の一つ星はマンパワーや予算などが限られている企業にも取り組みやすい制度となっているので、更なる普及推進を期待したい。補助金の要件にすることで宣言数が増えていると聞いているが、補助金等のインセンティブを地方自治体にも広げつつ、これらの取組は自社の体制を見直す機会となるため、中小企業の意識改革やレベルの底上げにつながればと考える。
- 中小企業のサイバーセキュリティ強化は重要な施策であり、積極的に取り組むためのインセンティブがあると良い。例えば、英国には認証を取得した企業に対して、特定領域の仕事に対して入札許可を与える制度（Cyber Essentials 制度）がある。
- セキュア・バイ・デザイン、セキュア・バイ・デフォルトの重要性を認識する一方で、中小企業にこれらの取組をお願いすると、その対価をどう求めるか、どのようなアドバンテージやインセンティブがあるのかという声もいただくので、ご考慮いただきたい。
- 日本産業界のレジリエンスを高める上ではサプライチェーンのサイバーセキュリティ強化が重要である。IPA においてサプライチェーン・サイバーセキュリティ・コンソーシアム(SC3)を設立いただいており、大変感謝している。SC3 は民間企業を束ねるプラットフォームとして非常に重要であり、今後もこの組織を経済産業省にサポートいただきたい。

国際連携の在り方

- 「サプライチェーン強化に向けたセキュリティ・アーキテクチャの検討」の第三者認証について、ISO9001を制定した際のように、各社のトータル・クオリティ・マネジメントは日本が先行していたものの、ルールメイキングで欧州が先に進めてしまったという教訓もあるところ、このまま進めると欧州勢に市場を席巻されるおそれがある。また、日本の認証についても、欧米等との相互認証を前提に検討を進めていただきたい。
- IoT適合性評価制度については、米国のサイバートラストマーク、欧州のサイバーレジリエンス法との相互認証の早期実現が重要である。それぞれの制度に対応するのは非常に煩雑であり、我が国の制度に基づいて統一いただけると有難い。仮に対応が進まなければ、製品の競争力にも影響する。

- SBOM も非常に重要である。海外企業と取引するに当たり、今後は SBOM が要求されるようになるのではないかと考える。相互運用性の確保の観点から国際標準化に持っていくところまで経済産業省にリードしていただきたい。
- 今後は AI 内に別の AI が組み込まれているケースも増えることが予想される。その場合、トレーサビリティが必要となり得るため、SBOM と同様の取組が必要となる。この点、民間側も一緒に協力させていただきたい。
- サイバーセキュリティの政策の知名度を上げていく意味でも、ガイドライン等については、英語版の公表をお願いしたい。英語版が少ないと、NIST や ENISA 等、海外の顧客に知らしめることができないため、グローバル企業では国内のガイドラインを採用しにくいのではと思っている。
- ガイドライン等の英語版の整備については、サイバー空間は世界に繋がっており、世界に日本を認識していただくためにも、単純なことだが、重要なことと考える。

セキュリティ産業振興の在り方

- セキュリティエコノミーの確立に向けては、ベンダーだけでなく、医療機器メーカーや小さな物流機器メーカー等の企業や業界団体にアピールできるような政策パッケージがあるとよい。セキュリティ分野において市場を拡大させることは難しいため、経済産業省が進めるOuranos Ecosystem(ウラノス・エコシステム)をはじめとした、欧米におけるGaia－XやCatena-X、IDSに匹敵するデータ流通の仕組みがあるとデータ連携の市場が活発化するのではないか。

<u>人材育成の在り方</u>

- 英米の事例では国防の優先度が高いところもあるかと思うが、国が主導して大学や民間を巻き込みながら、サイバーセキュリティの専門学位のプログラム等が整備され、助成金や奨学金等によって優秀な人材を確保していると聞いている。司令塔という話もあったが、各省庁や民間で実施する取組を体系的・戦略的に整理した上でどこをどう拡充するかをより戦略的に検討されたい。また、人材には限りがあるため、同盟国や有志国を中心とした国際連携も重要になる。経済安全保障の観点も含めた国際協力に携わることのできる人材も必要になってくると思われるため、そのような観点のプログラムがあるとよい。
- 人材育成に関しては IPA でも取り組んでいるが、人材自体はそれほど多く育たない。限られたリソース（人材）を有効活用することが重要であり、政府内で横串を刺して人材活用について検討してはどうか。英国では、民間と国家サイバーセキュリティセンター(NCSC)の間に人材交流が行われている。官民が共に仕事をすることで、危機感を共有することができている。民間人材の育成にも繋がるため、既存の枠組を用いつつ、日本でも同様の取組を検討いただきたい。
- 米国でも、官民人材協力がなされているが、セキュリティクリアランス等の非常に厳しい基準があり、官民のリボルビングドアとなっていて、官に行くと給料が下がるが、民間に戻った時に給料が上がる。また、官での経験が評価され、官として働くことの使命感を感じると聞いたことがある。そういった仕組を我が国でどのように実現するのかを検討することも重要ではないか。
- 英国では、Active Cyber Defenseの一環として、政府が国民にセキュリティ関連サービスを無償提供していると伺った。かかるサービスによって企業・個人のリテラシーが向上し、人材が不足していても、ある程度のセキュリティが担保できているようである。これは人材不足を前提としてサービスを提供することで、国家全体のリテラシーを向上させるという考え方に立っている。人材が不足する中でサービス等を如何に活用し、レジリエンスを高めるか、これまでの議論も踏まえて検討することが必要である。
- AIが台頭し、国民全体に一気に広まった点に怖さがある。我が国のレジリエンスはどうあるべきか、議論する必要が出てきたのではないか。国家のレジリエンスは対応者の能力に依存するのではないか。その観点から、いかに多くの国民・現場の方々にリテラシー教育を施すことができるかが重要ではないか。
- すべての若い人に資格取得を求めたり、専門高等学校や高専によるコンテストを開催するなど、裾野の広がりになる

ような仕組みの検討も重要ではないか。

- セキュリティ技術では、設計からプログラミング、テストまで基礎能力を求められる。また、セキュリティに関する技術を習得しようと考える学生向けの仕組があると早い段階から人材育成ができるのではないかと考えており、プラスセキュリティ人材の育成の施策についても検討いただきたい。
- 中小企業では、人材を確保できていないため、専門人材育成と併せて、プラスセキュリティ人材の育成を進めることが重要ではないか。
- 中核人材育成プログラム、情報処理安全確保支援士制度等により、専門人材の育成環境は整ってきているように思われるが、育成したくてもそもそも人材が不足しているというのが実態である。最近では経営者によるサイバーセキュリティの認識も高まっており、予算は付くようになっているが、人材までは提供できず、予算があっても使い切れない状況であるという声を伺っている。多くのセキュリティ専門人材がセキュリティベンダーに偏っており、ユーザー企業で専門的なセキュリティ要員を確保することが非常に難しくなっている。IPA の中核人材育成プログラムは良い取組だが、人材不足の中で 1 年間の研修に送り出すのはハードルが高いため、より短期、例えば 2 ヶ月程度の研修プログラムを期待する。
- セキュリティに強い人材は能力が高く、セキュリティ部門に配属されない人が多い。また、セキュリティに強い人材は海外にとられる傾向がある。セキュリティ部門の処遇の改善が必要ではないか。
- エッセンシャルワーカーでの置き換えに至るまでAIはまだ充実していない。ホワイトカラーのリスキルが進まないと我が国のホワイトカラーのリソース配分が歪なままになる。終身雇用を前提とせず、例えば第二の義務教育にするなど、リスキルして再就職するといった考え方を取り入れないと、ミスマッチは解消されないのではないか。
- サイバーセキュリティ分野においても英語が不可欠になってきている。技術の進歩により英語が話せなくても障害がなくなるかもしれないが、今まで以上に海外とのつながりが多くなる。国際連携等に係るスキルを若手に引き継がせようとするが、英語ができない点に難があり、例えば、起業家等も自分のビジネスモデルを英語で説明できず、ドメスティックなところに留まっている人が多い。短期的にはサイバーセキュリティの話をしているが、長期的には英語というインフラを大事に扱っていただきたい。

官民の対処能力向上に向けた取組の在り方

- 政府体制について、各省庁がそれぞれ施策を実施するという時代ではなくなってきている。政府内の司令塔を明確にした上で、ガバナンスを強化・各省庁連携していただきたい。
- 警察官全員がサイバー攻撃の初級スキルを習得していると聞いた。警視庁ではこのような取組を行っているが、横の連携があまりなされていないようにみえる。いずれかの組織が司令塔となってサイバーセキュリティ対策を実施していただければよい。
- 政府内における司令塔の一本化を急いでいただきたい。
- デジタル環境はライフラインになりつつあり、国民の生命に関わる。レジリエンス力をもって回復していくという観点で、官民で力を合わせる体制が必要。
- 国家のレジリエンスを高める上で、有事を意識しなければならない状況にある。とりわけ、半導体などの重要領域において、有事の際にサプライチェーン全体でどのように対応するのか、事前に考えておくことが重要。
- 日本の場合、カスタマイズや業界標準が多くあるため、セキュリティホールができやすいのではないか。そのため、IPA にレッドチームの設置を検討いただきたい。疑似的な攻撃を行って対策状況に関する情報を集め、当該事業者・官公庁に対策ができていないことを認識させるなど、性悪説に基づく活動の推進も重要。
- 専門組織同士でのサイバー被害情報共有は重要だが、サイバー被害情報は攻撃を受けている最中の企業にとって

は、インシデントの公表前に特定された被害情報が拡散されれば、準備が整う前に問合せが殺到して大きな混乱が生じ、結果的にステークホルダーからの信頼を失いかねない。ユーザー企業による情報提供を推進するには、情報提供による共助のメリットを感じられるだけでなく、自社を特定・拡散されないという安心して情報提供できる仕組みの構築に加え、経営者等が安全性を正しく理解できる啓発が必要である。また、共有を受ける専門ベンダー側については、セキュリティの専門性はもちろんセキュリティ面のスキルに加え、情報倫理、危機管理のスキルが必要になると思われる。

その他の御意見

- Before Covid と After Covid が異なるように、Before DX と After DX や Before AI と After AI も異なる。この変化をプラスにできれば、例えば AI をうまく使ったセキュリティの仕組や人材不足に対する補完なども検討できるのではないかと思う。その辺りの検証と国際的な調整等、情勢が非常に変わってきているので、今までと同じ方法ではなく、新しい産業サイバーセキュリティの世界ができるということにも取り組まねばならないと考える。
- 全体像から捉えることが重要。経済産業省は DX 推進の中で「デジタルライフライン」という言葉を使用している。多岐にわたる産業、国土全般にわたる、国民の生命にもかかわる重要なインフラと理解される良い言葉だと思う。官民で連携を進めることが必要。また、包括的な視点に加えて、領域単位での視点に立ち、領域間での接続にも留意する必要がある。AI と選挙といったように、あるテーマに焦点を当てて議論することも必要。

次回開催日程については事務局より別途案内する旨言及があった。

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:03-3501-1511(内線)3964