産業サイバーセキュリティ研究会 WG1
サプライチェーン強化に向けたセキュリティ対策評価制度に関する
サブワーキンググループ(第2回会合)
議事要旨

1. 日時・場所

日時:令和6年9月9日(月) 10時00分～12時00分

場所:オンライン会議

2. 出席者

委員　　:渡辺委員(座長)、江崎委員、教学委員、下村委員、高橋委員、武井委員、古田委員、丸山委員、森委員、和田委員、曽根原様(三井委員代理)

オブザーバ:内閣府、警察庁、金融庁、デジタル庁、総務省、外務省、厚生労働省、農林水産省、国土交通省、防衛省、防衛装備庁、独立行政法人情報処理推進機構

事務局　　:経済産業省、内閣官房内閣サイバーセキュリティセンター

3. 配付資料

資料1 議事次第・配布資料一覧

資料2 委員名簿

資料3 サプライチェーン対策評価制度の基本構想(案)について

資料4 日本自動車工業会 自工会／部工会サイバーセキュリティガイドラインについて

資料5 みずほフィナンシャルグループ 金融分野におけるサイバーセキュリティの評価の枠組み

4. 議事内容

冒頭、経済産業省商務情報政策局 武尾サイバーセキュリティ課長より冒頭あった。次に、事務局より資料3の説明があり、古田委員より資料 4、森委員より資料 5 の説明を行った後、続けて自由討議が行われたところ、概要は以下の通り。

＜資料 4 について＞

■質問

- チェックシートの要求事項において、個別の製品として例えば EDR などを指定する要求事項を設けているか。
- 取組の中で第三者評価は活用しているか。

■回答

- 個別の製品を指定するといった要求事項は設けていないが、よろず相談会を開催し、そちらで対策方法について情報共有を行っている。業界団体としての立場上、特定製品の紹介はできないが、例えば費用をかけずに対策ができたといった事例を共有している。
- 第三者評価は行っていない。ガイドラインの浸透フェーズにあり、まずはよろず相談会で地道な取組を行っている。評価の部分で悩みを抱えているが、業界全体で第三者評価に取り組むには至っていない。

＜資料 5 について＞

■質問

- P.3 について「サプライチェーン構成企業のサイバーセキュリティ管理態勢が把握・確認できるように、上記評価結果を対外的に明示する枠組みを整備することが必要」とあるが、サイバーセキュリティ管理態勢の把握に ISMS 認証も使え得ると認識している。ISMS 認証をどのように評価しているか。また、ISMS 認証に問題はあるか。
- P.3 について、第三者評価の評価主体は誰か。
- 金融業界について、監督省庁からの要求事項と現場で運用している実習ルールを統合する流れがあった。「金融分野におけるサイバーセキュリティに関するガイドライン」を策定している金融庁と「金融機関等コンピュータシステムの安全対策基準」を策定している金融情報システムセンター(FISC)の動きはご存知か。

■回答

- 情報セキュリティ管理態勢を可視化できるため ISMS 認証制度を求めることも 1 つの手と考えられる。ただし、ISMS 認証との今回の制度との関係性の整理が必要とも考える。
- 第三者評価の評価主体としては、たとえばコンサルティングファームやセキュリティの専門部隊を持っている企業といった専門事業者が挙げられる。
- 金融庁が策定している「金融分野におけるサイバーセキュリティに関するガイドライン」(案)は様々なフレームワークを参考に策定されていると伺っている。ただし、金融情報システムセンター(FISC)の動きとの関係性については把握していない。

＜資料 3 について＞

■対象事業者のイメージについて

- P.6 では、ネットワークの接続有無にフォーカスされすぎていると感じた。USB メモリ等のメディア経由やメール経由でマルウェア侵入を許容するリスクは依然として残っている。記載方法については留意いただきたい。
- P.7 のビジネスの観点で追加すべきかとの質問を事務局からいただいたため、一案を申し上げたい。今回の対策評価制度では、財務面や経営者のプロファイルはスコープ外と認識している。一方で、財務状況が悪化すると M&A 等を通じて好ましくない企業から買収されるリスクがあり、情報や技術者の流出のおそれがある。本評価制度で財務面等を考慮する必要はないにしても、契約面から財務上及ぼす影響について本検討会からのコメントを出す必要があるのではないか。
- P.7 をみると、もともと発注者が取引先を評価する制度なのか、又は期待値なのかなどがわかりにくいため、政府と発注者、評価主体の関係性を明確に定義した方がよい。
- 発注者が受注者の委託先まで把握できない現状がある。サプライチェーン全体をみたときにどう捉えるのか。
- P.7 に示された★5 のビジネス観点において、口座番号が例示されているが、「『個人情報の保護に関する法律についてのガイドライン』に関するＱ＆Ａ」には、銀行口座番号のみの漏えいは直ちに「不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等」に該当するものではなく、銀行口座番号とインターネットバンキングのパスワードの組合せが漏えいした場合に該当すると考えられる、と記載されている。P.7 の記載は個人情報保護法や関連ガイドライン等に則った定義を行うとよい。
- P.7 について、目標とする★3 の取得企業数を確認したい。例えば、自動車工業会のガイドラインに対応している企業は自動的に★3 レベルにあるとすれば、★3 の取得企業数が増えることになる。取得企業数をそのような形で増やすことにより、上場企業が取引を行う上での最低条件とする世界観を目指してはいかがか。それ以上は★4 以上で求めることとして、例えば、★3 取得企業数は 100 万社等の具体的な数字として提示するのはどうか。
- ビジネスの観点で、国家安全保障や海外有事の観点は考慮しない認識か。

■対策の適用範囲について

- P.8 について、組織管理はプロジェクトに依存するため、組織内対策で括られるのかに疑問がある。
- P.8 に示された★4 と 5 の組織的対策は同一にみえるが、果たして★4 と 5 の組織的対策は同一でよいのか。同一とした理由がよく分からない。

■対策の基本的な考え方について

- 資料の順番について、P.10 を冒頭に位置付けた上で、★3～5 の流れがあると分かりやすくなる。順番を再考いただきたい。

■各段階でベンチマークとする制度・ガイドラインについて

- P.9 について、既存のガイドラインとのマッピングをお願いしたい。本評価制度の認証と他の認証との関係性が理解できなければ、事業者の負担が増えるだけである。要求事項だけではなく、既存の認証制度との相互認証についても整理いただきたい。
- 自動車工業会で既に行っている自己評価と、本制度との関係性を整理されたい。サプライヤーにとって二重の対応が必要となるため、本制度の位置づけを明確にした上でメッセージとして出すべきである。自動車工業会の取組との違いは第三者認証の部分であり、客観性が担保されている点であると認識している。
- 前回の検討会と同様のお願いとなってしまうが、国土交通省から公開されているガイドラインを踏まえて対策を行っているところ、任務保証の考えのもとで必要な事項についてまとめられている当該ガイドラインを遵守した場合、どのレベル(★3～5)に該当するのか、整合性の確保をお願いしたい。
- 航空会社は、様々な事業者(例:通信、海外ベンダ)と協力していることもあり、他制度との関係性を整理いただけるとありがたい。
- P.12 にあるような既存の制度をベンチマークにして検討をお願いしたい。
- 本評価制度は後発の制度であるため、先行するガイドラインや認証の仕組みを踏まえつつ、相互認証を進めるべきである。
- ベストプラクティスの提示は、非常に有効だと考える。具体的な解法の事例集は有効である。

■対策項目について

- 中小企業の担当者は、何をすればよいかわからず、踏み込んだことをしない可能性がある。具体的な内容を記載しては如何か。また、本制度と IPA の「中小企業の情報セキュリティ対策ガイドライン」との連携も考えていきたい。本制度で全てを解決することは難しい可能性がある。
- P.9 において、例えば★3 では UTM の導入、★4 では EDR 導入を行うものと理解した。しかし、★3 でも EDR 導入を求めるレベル感でもよいのではないか。また、対策要件の中で特定の製品を推奨する方が理解しやすい。機能だけでは企業ではわかりにくいため、例示が必要である。アタックサーフェスマネジメントの導入方法についても盛り込むべきではないか。
- ★3 は基本的な対策と考えると、対応・復旧プロセスで求める内容もわかりやすく丁寧に示していくべきではないか。例えば、実際にセキュリティインシデントが発生した際に、感染拡大を回避する観点から自らシステムを停止する場合等があると考えられる。

以上