参考資料１

重要インフラサイバーセキュリティ研究会（第３回）議事概要

１　日時

令和８年３月４日(水)14:00～16:00

２　場所

赤坂グリーンクロス４階　会議室

３　出席者

【構成員】

江崎　浩	東京大学大学院情報理工学系研究科教授
大日向　隆之	一般社団法人金融 ISAC 理事 株式会社三菱総合研究所客員研究員
柿崎　淑郎	東海大学情報通信学部准教授
北尾　辰也	国土交通省最高情報セキュリティアドバイザー
小松　文子	ノートルダム清心女子大学情報デザイン学部教授
小山　覚	NTT ドコモビジネス株式会社情報セキュリティ部部長
長島　公之	公益社団法人日本医師会常任理事
西本　逸郎	株式会社ラック技術顧問
山岡　裕明	八雲法律事務所弁護士
渡辺　研司	名古屋工業大学大学院工学研究科社会工学専攻教授

【オブザーバ】

高見　穣	独立行政法人情報処理推進機構セキュリティセンター グループリーダー

４　議事概要

【議事】

（１）重要インフラ統一基準等の検討について

・事務局から、資料１に基づき、これまでの研究会における議論について説明。

・事務局から、資料２に基づき、分野別ヒアリング実施結果について説明。

・事務局から、資料３から資料６に基づき、重要インフラ統一基準等の検討、重要インフラ統一基準（素案）、行動計画の改定、今後のスケジュールについてそれぞれ説明。

【主な発言】

〇構成員

・重要インフラ統一基準の策定に当たり、２点申し上げる。１点目として、CISO の設置が重要と考える。CISO の設置については、安全基準等策定指針において明記され、金融庁「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」では、「基本的な対応事項」として位置付けられている。米国ニューヨーク州金融サービス局サイバーセキュリティ規制では、CISO の設置が義務化されており、韓国の電気通信事業法でも同様に義務化されている。このように、グローバルに見ても、重要インフラ分野において CISO の設置が推奨を超えて義務化されつつある。

・２点目として、サイバー保険について言及することも一案。近時のランサムウェア攻撃事案でも示されているように、サイバー攻撃により極めて大きな財務的インパクトが発生し得る。その結果、仮にシステムが復旧したとしても、重要インフラサービスの提供に影響が及ぶリスクがある。よって、ファイナンス部門におけるサイバーリスクに対するソリューション、特に財務的観点からの対策についても、重要インフラ分野において重要視すべきではないか。

〇構成員

・サイバー保険については、レジリエンスに関する具体的な要素の一つとして位置付けることが一案。想定外の事象が実際には発生し得るものであり、復旧を見据えてどのように保険をかけておくかという観点は重要。

〇構成員

・重要インフラ事業者におけるキャッシュフローをどのように確保するかという論点と、発生した損失をどのように補填するかという論点は分けて整理すべき。特にキャッシュフローの確保は、重要インフラ分野において極めて重要な要素であり、政府間の融資といった手段も含め、広く検討すべきではないか。

〇構成員

・ファイナンスは、企業が事業体として存続するために必要な資源を手当てするという観点から重要であり、その選択肢の一つとして保険もあり得る。

〇構成員

・ゼロトラストの導入の有無を問わず、レジリエンスの観点から、セグメンテーションによる分離は非常に重要。また、「専用 OS だから」「閉域網だから」に加えて、「独自技術仕様だから安全」と認識している例が見受

けられるものの、オープンな通信プロトコルではないという理由のみで安全性が担保されるわけではない。重要インフラ統一基準では、これらの点について言及すべき。

○構成員

・閉域網に配置されたネットワーク機器が必ずしも安全ではない理由の一つは、脆弱性に対するパッチ適用が困難である点にある。実際、10 年、20 年と脆弱性を抱えたままネットワーク機器が稼働し続けているケースも存在する。特にミッションクリティカルなネットワーク機器ほど停止が難しく、パッチ適用が容易ではない。このような状況が結果として悪循環を生んでいると認識している。そこで、通信事業者に限らず、重要インフラ分野におけるネットワーク事業者全般に対し、明確なメッセージを発信することが重要。そこで、重要インフラ統一基準には、ネットワーク機器の更改や、パッチ適用の対策が実効的に進むような記載を取り入れてはどうか。

○構成員

・リスクマネジメント、あるいはリスクベースの考え方においては、どの文脈で誰を主体として想定するのかについて留意する必要があるのではないか。重要インフラ事業者等ごとにリスクを捉える場合のほか、例えば、重要インフラ所管省庁において、所管する分野の基幹インフラ事業者のサービス提供が停止することをリスクとして捉えるという場合もあってよいように思う。

○構成員

・重要インフラ事業者等には、規模やセキュリティに関するスキルセットが多様な事業者が含まれている。このような状況で安全基準等を最低限の水準に合わせてしまうと、基準のレベルが過度に低くなるおそれがある。

○構成員

・情報共有については、レイヤーを３段階で考えることが重要。すなわち、同盟国を中心とした国際的な共有、業界内での共有、事業者内部での共有という３つの段階で実施する必要がある。

○構成員

・情報共有については、例えば、同一地域内における分野を超えた情報共有といった、地域内の観点も重要である。

○構成員

・セキュリティ対策に必要な資源の確保について、重要インフラ事業者等

に対しては、投資対効果の観点にとどまらず、社会的使命であり、あるいは最大許容停止時間である MTPD を達成するために必要な投資であるといったメッセージを発信しなければ、経営層の意思決定には結び付かないのではないか。また、資源の確保の最終的な責任者を誰とするのかという点も重要。

・検知の体制について、AI の活用は、攻撃への対処におけるスピード感が高まる中で、深刻化するセキュリティ人材不足の解消につながる取組であると考えている。今後 AI、ひいては AI エージェントを踏まえた対策についても議論していく必要がある。

・近時発生したサイバー攻撃の事案も踏まえると、今後の議論では、被害の影響が他分野等に波及するような、単一障害点になっているサービス（例：大手小売業の物流）をどのように位置付けるかについても議論していく必要がある。

〇構成員

・重要インフラ統一基準において対象となる分野・事業者を特定するに当たり、一定の基準を示す必要があるのではないか。例えば、人口カバー率が一定割合以上である事業者や、代替性が低い事業者等といった特定の基準を示すことが考えられる。

〇構成員

・今後、重要インフラ所管省庁は、重要インフラ統一基準等を踏まえ、各分野の特性やリスクを考慮した上で、各分野の安全基準等を整備していくことになる。国家サイバー統括室におかれては、重要インフラ所管省庁に対し、その役割の重要性を十分に認識した上で取り組んでもらえるよう、適切に推進いただきたい。

・重要インフラ統一基準では、リスクアセスメントの重要性を強調すべき。企業が、従来の手法にとどまってリスクを適切に特定できず、新しい脅威に対応できずに失敗している例がある。また、ネットワーク制御の観点、特に、必要最小限の通信のみを許可するという考え方が重要。さらに、バックアップについては、サイバー攻撃によって破壊されない形式でバックアップを確保することが重要。

〇構成員

・リスクアセスメントについては、あらかじめ想定・定義されたリスクのみを対象として対応すればよい、という理解になりがちである。しかし、確定しているリスクだけを追いかけるのではなく、水平スキャン等を通じて、潜在的・隠れたリスクが存在しないかを発見する行為が重要であ

る。

〇構成員

・CISO の設置は重要であるところ、担当者レベルのサイバーセキュリティ人材と同様に、CISO の役割を担うことができる人材も不足している。そこで、人材育成では、担当者レベルのみならず、CISO 等のサイバーセキュリティのリーダーとして組織を牽引する人材も育成するという観点も必要ではないか。

〇構成員

・医療分野は特殊であり、小規模な医療機関をはじめ、ほとんどの医療機関では、十分なセキュリティ対策を実施できていない。現場の混乱を避けるためにも、このような医療分野の特殊性、現場の実情等を踏まえた施策を検討いただきたい。また、政府側からの支援も併せて検討いただきたい。他方で、例えば、オンライン資格確認、電子処方箋、電子カルテ共有サービス等を運営する社会保険診療報酬支払基金については、社会的影響が大きいため、対策を徹底する必要があると考える。

〇構成員

・重要インフラ統一基準を通じた政府機関における施策の PDCA サイクルにおいては、上位からの指示・下位からのレポートの実効性、あるいはチェックの実効性を確保するため、評価の基準が必要。

・重要インフラに関連する制度や文書が多数存在しており、重要インフラ事業者等側から見て、各事業者等が何を遵守し、あるいは実施すべきなのかが分かりにくくなっているのではないか。今後の行動計画の改定では、各事業者等において内容の理解が進むよう、記載等を工夫いただきたい。

〇構成員

・重要インフラ事業者の実情や、取組と要求事項とのギャップを正確に把握するためには、場合により、国家サイバー統括室が、直接重要インフラ事業者に対して調査やヒアリングを実施するなどし、情報を収集する必要があるのではないか。

〇構成員

・官民連携においては、政府機関と重要インフラ事業者・業界団体等が方向性を共有し、議論を重ねながら協働して進めていくことが重要。

〇構成員

・今後の重要インフラ所管省庁等も含めた議論では、方向性がずれないよう、そもそもサイバーセキュリティは誰のためにあり、何を実施すべき

かという点について認識を共有する必要がある。大きな方針としては、エンドユーザーへのサービスのクオリティを確保するということから議論をスタートさせるべきではないか。

○構成員

・重要インフラ統一基準において、セキュリティが企業の経営層の課題であることを明記してはどうか。

（2）その他

【主な発言】

○構成員

・今後の議論かと思うが、重要インフラ対策において、クラウドサービス、あるいはデータセンターをどのように位置付けていくかは重要ではないか。

【今後の予定】

・事務局から、次回の研究会の開催予定について説明。