サイバーセキュリティ戦略本部　重要インフラ専門調査会
第 31 回会合　議事概要

１　日時

令和４年 12 月 22 日（木）16 時 00 分～18 時 00 分

２　場所

Web 会議

３　出席者（五十音順・敬称略）

（委員）

大杉　謙一　　中央大学　大学院法務研究科　教授
小松　文子　　長崎県立大学　情報システム学部　教授
佐々木秀明　　電気事業連合会　理事・事務局長
高橋　正和　　株式会社 Preferred Networks　執行役員　最高セキュリティ責任者
武田　雅哉　　青森県　ＩＴ専門監
長島　公之　　公益社団法人日本医師会　常任理事
奈良由美子　　放送大学　教養学部　教授
野口　和彦　　横浜国立大学　客員教授
前川　　篤　　株式会社シグマクシス　シニアフェロー、大阪大学　招聘教授、京都大学　特任教授
松本　　勉　　横浜国立大学　大学院環境情報研究院　教授
横浜　信一　　日本電信電話株式会社　執行役員　セキュリティ・アンド・トラスト室長　ＣＩＳＯ
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

（事務局）

髙橋　憲一　　内閣サイバーセキュリティセンター長
吉川　徹志　　内閣審議官
内藤　茂雄　　内閣審議官
上村　昌博　　内閣審議官
小柳　誠二　　内閣審議官
中溝　和孝　　内閣参事官
紺野　博行　　内閣参事官
中越　一彰　　内閣参事官
松本　　崇　　企画官
中尾　康二　　サイバーセキュリティ参与

（オブザーバー）

内閣官房（事態室）
金融庁総合政策局リスク分析総括課
総務省サイバーセキュリティ統括官室
総務省自治行政局デジタル基盤推進室
外務省大臣官房情報通信課
厚生労働省政策統括官付サイバーセキュリティ担当参事官室
経済産業省商務情報政策局サイバーセキュリティ課
原子力規制庁長官官房
国土交通省総合政策局情報政策課サイバーセキュリティ対策室
防衛省整備計画局情報通信課 AI・サイバーセキュリティ推進室

４　議事概要

（１）開会

渡辺会長から開会に際しての挨拶が行われた。

（２）報告事項

「重要インフラを取り巻く情勢」について、資料２に基づき、事務局から報告が行われた。「関係省庁の取組状況」について、資料３に基づき、金融庁、総務省、厚生労働省、経済産業省及び国土交通省から報告が行われた。

（本議題に関する主なやりとりは次のとおり。）

（長島委員）

○ 先般、大阪府内の病院でランサムウェアによる被害で診療停止に至る事態が発生した。外部委託先への侵入に起因するものとみられており、資料２で示すインシデントから得られた教訓が、残念ながら生かされていなかった。

○ 医療分野では「知識」「人材」「財源」が不足しており、サイバーセキュリティの確保がなかなか進んでいないのが実情。そこで、日本医師会では、６月から「サイバーセキュリティ支援制度」を開始した。緊急相談窓口の設置や被害発生時の初期対応支援金の提供を実施している。

（前川委員）

○ 医療機関にランサムウェア攻撃をした犯人は検挙されているのか。犯人検挙は攻撃抑制の観点から重要と考える。

（厚生労働省）

○ 基本的にインシデントが発生したら即座に警察と連携し調査にあたっている。

（横浜委員）
○ NISCや各省庁の取組を国内外に積極的に情報発信すべき。
（紺野参事官）
○ 効果的な広報活動に関して今後の検討としたい。

（野口委員）
○ インシデントの再発防止に向けた取組だけでなく、インシデントとして顕在化していないリスクも含めたマネジメントに関する取組があるとよい。
（総務省）
○ 資料３－２で示すC&Cサーバ検知技術の実証のように、平時から予防する取組についても実施していきたい。
○ 事故検証においては、同様事象の再発防止だけでなく、その他の可能性を考慮した対応策を検討している。

（高橋委員）
○ サイバー犯罪をなくす努力も大切だが、実際に犯罪はなくならないので、継続的な対策が必要という現実を伝えるべき。
○ 日本ネットワークセキュリティ協会にてサイバーインシデントの緊急対応が可能なベンダー企業一覧を提供しているので、活用願いたい。
○ 事業者間ローミングにより通信量が増大し、システム障害に繋がることを懸念。ローミングの対象を緊急通報とするなど、社会として守るべき重要インフラサービスを明確にしたほうがよい。

（武田委員）
○ 病院の情報システムは独自にカスタマイズされ、セキュリティパッチを適用できない場合があると聞いている。システムの標準化が重要だと考える。
（厚生労働省）
○ 課題として認識しており、ガイドライン等を通じた対策など今後の検討としたい。

（３）討議事項

「安全基準等策定指針・手引書の改定骨子（案）」について、資料４に基づき事務局から説明が行われ、討議がなされた。
（本議題に関する主なやりとりは以下のとおり。）

（野口委員）

○ ベースラインといった要求事項は機能として規定すべき。仕様として規定すると変化の激しいサイバー空間の脅威に対応するために都度変更を加える必要が生じる。

○ 中小規模の事業者に対する要求事項を現実的なものにすることについて、要求事項は提供するサービスの重要度によって設定されるべきであり、事業者の規模で変わるものではない。要求される機能を満たすための手段は組織特性に応じて選択できるようにすればよい。

（佐々木委員）

○ 先進事項である「取締役に相当する者の中からCISOを任命するのが望ましい」について、業務執行権限が執行役員に委ねられている事業者も存在するため、「経営層の中から任命する」といった表現が現実的ではないか。

（大杉委員）

○ 事業者の規模によって投資可能額が変わるため、小規模事業者等は業界団体やサプライチェーン等の支援が必要となるケースも想定される。指針においては、基本的な考え方だけでなく、現場で対策を導入・実施する際の実践的な要領にも言及すべき。

○ CISOが取締役であるか否かは本質でなく、取締役会に相当する場で選任することに加え、有事に経営層に対して直談判できる人物であることが肝要。

（前川委員）

○ 安全基準等策定指針（骨子案）３ページの組織方針における「サイバーセキュリティに関する事項も考慮する」という表現は実行性に乏しいので、再考すべき。

（松本委員）

○ 主な御意見にあるレッドチームの設置について、分野横断的演習での実施にとどまらず、定常的に実施すべき事項ではないか。

（横浜委員）

○ こちらは私から出した意見だが、本来の意図は定常的な実施。しかし、実際には法制上難しい部分もあると思われ、まずは演習から取り組めばよいと考える。

（佐々木委員）

○　サプライチェーン・リスクの管理にあたり、直接取引する供給者を対象とするのであれば問題ないが、その先の二次、三次供給者まで管理するのは事業者にとって困難なケースもあり、配慮いただきたい。

（高橋委員）

○　サプライチェーンの定義やスコープについて議論毎に明示すべき。

○　BCPの一部としてIT-BCPを策定することについて、IT-BCP以外にもサイバーセキュリティBCPというものもあり、自然災害用とサイバーインシデント用では内容が異なるため、読み手が混同しないような説明を盛り込めるとよい。

（松本委員）

○　ベースラインを機能規定とすべき意見に同意する一方、その場合、最低限実施すべき対策事項を示すのが困難となる懸念もある。

（大杉委員）

○　法令に基づく立入検査で実効性が確保されているとの御意見について、国の立ち入り検査だけでは安全の確保を断定できない側面もあり、指針本文においては誤解を招かないような表現とすべき。

（小松委員）

○　骨子案を拝見するに、関連文書の優れた箇所を引用し繋ぎ合わせたものと思う。各文書の想定する目標は異なるため、目標が曖昧にならないように各文書を組み合わせる必要がある。例えば、NISTサイバーセキュリティフレームワークやCISAサイバーセキュリティパフォーマンス目標は、具体的な対策を最終的な目標として設定するものだが、ISO27000やISO31000は、フレームワークを構築、運用するものである。

（高橋委員）

○　マチュリティモデルの知見を盛り込むべき。

○　東京2020オリンピック・パラリンピック競技大会を成功例として活用することについて、東京大会はプロジェクトであり、プロジェクトにおける対策と事業における対策の相違点に留意すべき。

（奈良委員）

○　ベースラインの定義を明らかにすべき。また、読み手がベースラインと先進

事項を確実に区別できるよう表記方法に関しても工夫できるとよい。

（前川委員）

○　手引書改定骨子案概要で示されるリスクマネジメントのプロセス図について、各プロセスを実行する主体を記載すべき。組織に適用する際、誰が何をすべきか理解できるものがよい。

（野口委員）

○　当該プロセス図は、リスクマネジメントの各機能の関係を示したもの。ご指摘の組織適用時の図は別途用意できるとよいのではないか。また、それぞれの図が示す内容に関して、読み手に分かり易い説明を記載する必要がある。

（４）閉会

髙橋センター長から閉会に際しての挨拶が行われた。

次回の専門調査会の開催予定について、事務局から連絡があった。

以上