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 35 回会合　議事概要

１　日時

令和５年 12 月 20 日（水）14 時 00 分～16 時 00 分

２　場所

ハイブリッド開催（中央合同庁舎８号館８階特別中会議室、Web 会議）

３　出席者（敬称略）

【委員】（五十音順）

（対面）

小松　文子	ノートルダム清心女子大学 特別招聘教授
野口　和彦	横浜国立大学　客員教授
原田　　智	公益財団法人 京都産業 21　DX 推進監　兼　CISO
松本　　勉	横浜国立大学　大学院環境情報研究院　教授
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

（オンライン）

大杉　謙一	中央大学　大学院法務研究科　教授
越智　俊城	株式会社三菱 UFJ 銀行　取締役常務執行役員　CIO
佐々木秀明	電気事業連合会　理事・事務局長
神保　　謙	慶應義塾大学　総合政策学部　教授
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
長島　公之	公益社団法人日本医師会　常任理事
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

【事務局】

鈴木　敦夫	内閣サイバーセキュリティセンター長
林　　学	内閣審議官
中溝　和孝	内閣審議官
門松　　貴	内閣審議官
遠藤　顕史	内閣審議官
上村　昌博	内閣審議官
豊嶋　基暢	内閣審議官
垣見　直彦	内閣参事官
紺野　博行	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】
（対面）
国土交通省港湾局海岸･防災課危機管理室
（オンライン）
内閣官房（事態室）
警察庁サイバー警察局サイバー企画課
金融庁総合政策局リスク分析総括課
デジタル庁戦略・企画グループ
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サイバーセキュリティ対策チーム
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
防衛省整備計画局サイバー整備課

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。）

（野口委員）
○　インシデント調査について、発生した個別事象の原因を分析するのでは不十分である。事前に実施していたリスク分析や対応体制整備を振り返り、インシデントを防げなかった要因を検証の上、対策を講ずるべきと考える。
○　サイバーセキュリティはコストでなく投資であることを従来以上に明確化すべきである。分野や事業者によってはサイバーセキュリティの重要性の認識

に関して根本的な問題があるように見受けられる。

○　重要インフラに係る脅威環境や防護取組の情報共有について、情報共有そのものが目的化している懸念がある。デジタルやAI等の進展にセキュリティが遅れないようにするため、共有された情報をどのように活用するか更に踏み込んで議論すべきである。

（長島委員）

○　医療機関におけるサイバーセキュリティ対策について、診療報酬の問題等に起因してサイバーセキュリティに係る財源を確保できず、投資を困難にさせている現状がある。

○　クラウド化の進展やマイナンバーカードを用いた保険資格確認等によって多くの病院や薬局が外部のネットワークに繋がざるをえなくなった。医師会の対応として、昨年から開始した会員向けサイバーセキュリティ支援制度を順次拡充しているが、依然として国からの支援も必要な状況であると考える。

（厚生労働省）

○　厚生労働省としてどのような取組が可能か、引き続き検討してまいりたい。

（経済産業省）

○　サイバーセキュリティお助け隊サービス等のセキュリティ支援施策について、厚生労働省と連携の上、取り組んでまいりたい。

（松本委員）

○　重要インフラにおける情報共有件数について、情報共有をして実際に役立った事例や効果等を把握しているか。共有された情報を活用することで攻撃への対策を先回りして講ずることが可能と考える。

（松本企画官）

○　インシデント等の情報は、重要インフラ事業者等から所管省庁を通じてNISCに報告されるが、その際、実施したインシデント対応等に係る助言等のフィードバックを適宜実施している。また、報告されたインシデントや関係機関からの情報等をもとに必要に応じて注意喚起を発出している。

（原田委員）

○　インフラ関係のシステム障害においてベンダーによる原因報告が不正確な場合、正確な情報を共有していれば防げたはずが、二次被害、三次被害へと拡大してしまう懸念がある。ベンダーとしてシステムに関するテストを重ねたにもかかわらず発生したのであれば、なおさら原因を正確な情報に整理して広く共有するよう徹底いただきたい。

○　港湾を重要インフラ分野として位置づけるための検討においては、自治体が管理する地方港湾への対策も考慮に入れていただきたい。

（国土交通省）

○　重要インフラの対象となる港湾については、行政以外の専門家の意見も踏まえつつ今後検討してまいりたい。

（小松委員）

○　病院内のシステムをはじめ、複数のベンダーによるアプリケーションで構成される環境下においては、ネットワーク構成や技術的情報の把握はもちろんのこと、責任の所在を明らかにしておくべきと考える。

（厚生労働省）

○　複数のベンダーで責任分界点を定めることは重要な観点であり、十分に留意して取組を進めてまいりたい。

（横浜委員）

○　今後のキーワードとして、重要インフラ事業者の取組としてはスレットハンティングの実施を打ち出すことが考えられる。自組織が抱える脅威を積極的に収集し、外部から共有された情報と繋ぎ合わせることで、具体的な対策等の行動に結びつくと考える。

（神保委員）

○　能動的サイバー防御について、日本国内における定義の幅がかなり広いように見受けられる。攻撃の各段階に能動性をどのように当てはめるか、事態の深刻度に応じて能動性をどのように変化させるか等、議論の幅が大きい。本調査会において重要インフラ防護に係る能動的サイバー防御の概念に対してどのようなアプローチがふさわしいのかを整理することは、将来の議論において重要な観点であると考える。

（３）討議事項

「その他」について、資料４に基づき事務局等から説明が行われ、討議がなされた。（本討議事項に関する質疑応答は非公開。）

（４）閉会

事務局から閉会に際しての挨拶が行われた。

以上