

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 33 回会合 議事概要

1 日時

令和 5 年 6 月 2 日（金）10 時 00 分～12 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
越智 俊城	株式会社三菱 UFJ 銀行 取締役常務執行役員 CIO
小松 文子	ノートルダム清心女子大学 特別招聘教授
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
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
原田 智	公益財団法人 京都産業 21 DX 推進監 兼 CISO
前川 篤	株式会社シグマックス 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）

高橋 憲一	内閣サイバーセキュリティセンター長
林 学	内閣審議官
吉川 徹志	内閣審議官
遠藤 顕史	内閣審議官
上村 昌博	内閣審議官
内藤 茂雄	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

(オブザーバー)

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

「重要インフラの安全基準等の継続的改善状況等に関する調査」、「重要インフラの安全基準等の浸透状況等に関する調査」、「重要インフラを取り巻く情勢」、「重要インフラにおけるセプターの活動状況」、「重要インフラにおける補完調査」について、資料2～6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7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）

- サイバー攻撃による被害が甚大であったという情報だけでなく、適切な対策により被害を抑制できた好事例を積極的に発信いただきたい。
- 日本医師会と警察庁サイバー警察局は、サイバー事案への対処に関する連携を実現するため、今年4月に覚書を締結した。加えて、都道府県医師会と都道府県警察の連携も深めているところである。
- 日本医師会では、会員向けのサイバーセキュリティ支援制度を今年6月から

拡充し、今般改定されたガイドラインに沿って対応を進めている。

(野口委員)

- 資料2の継続的改善状況等に関する調査について、重要インフラ分野間における相互依存を考慮すると、分野別に隔てられた取組がいつまで有効なのかという中長期的な懸念を抱いている。
- 資料3の浸透状況等に関する調査について、リスクアセスメントの実施やコンテンツジェンシープランの策定、脆弱性診断の実施等の水準が低い原因を深掘りすべき。これらの取組を実施していることを前提にその有効性を検証するのが望ましい姿であり、従来の方法を継続するだけでは対策が間に合わない懸念がある。

(紺野参事官)

- 各省庁と連携を図りながら分析、改善を検討したい。

(前川委員)

- ランサムウェア事案について、犯人検挙に関する情報を公表することにより抑止力に繋がるものとする。
- ウクライナ侵攻問題のような有事のサイバーセキュリティに関する考察も一度、まとめていただくよう検討されたい。

(警察庁)

- 警察として外国捜査機関等と連携するなどしてランサムウェア事案の捜査に取り組んでおり、引き続き対応を進めていく。

(松本企画官)

- ウクライナ侵攻問題等のまとめにつき、ご指摘を踏まえ今後の検討としたい。

(奈良委員)

- 資料3の浸透状況等に関する調査について、人材の十分な配置に関する実施水準が分野共通的に低くなっている。これらへの対応について伺いたい。

(紺野参事官)

- 各省庁が人材育成等に取り組んでいるところ、NISCとしても総合調整の観点から取組を推進したい。

(原田委員)

- 資料6の補完調査について、事例3にあるような組織的な攻撃が自治体に対しても活発になっている。国と自治体が一体となって対策を講じるとともに、自治体への情報提供、支援を引き続きお願いしたい。

(紺野参事官)

- 安全基準等策定指針の公表や分野横断的演習の実施等を通じて引き続き連携を図りたい。

(長島委員)

- 厚労省や日本医師会の調査によると、小規模事業者のセキュリティ対策が遅れがちである。事業者の規模別に分析し、きめ細やかな対応を推進されたい。

(紺野参事官)

- 事業者の規模による影響も加味した上で適切な対応を検討したい。

(横浜委員)

- 前川委員が言及された安全保障環境も踏まえた検討は、今後ますます必要になると考える。国家安全保障戦略に基づく重要インフラ防護のための官民連携に関する議論を積み上げていくべき。

(紺野参事官)

- 本調査会における議論事項に対する提案と受け止め、今後の検討としたい。

(高橋センター長)

- 国家安全保障戦略においてサイバーセキュリティの強化や官民連携が位置づけられており、また、経済安全保障においても基幹インフラのサプライチェーンやセキュリティクリアランスの問題が議論されている。これらの様々な意見を踏まえながら、重要インフラ及び他の基幹インフラの防護のための官民連携の取組や人材育成を併せて、サイバーセキュリティ戦略本部に諮って推進していきたい。

(松本委員)

- 資料7-5の国土交通省の取組にあるように、バックアップがうまく機能せずにサービス停止に陥る事例がいくつか見受けられるが、詳細な事例分析、効果的な注意喚起によって同様の事態を防止すべき。

(紺野参事官)

- 今後の事例分析、情報共有における検討としたい。

(3) 討議事項

「重要インフラにおける取組の進捗状況(年次報告)(案)」及び「重要インフラのサイバーセキュリティに係る安全基準等策定指針(案)等に対する意見募集の結果について(案)」について、資料8、9に基づき事務局から説明が行われ、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

高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