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 36 回会合　議事概要

１　日時

令和６年２月 22 日（木）10 時 00 分～12 時 00 分

２　場所

ハイブリッド開催（内閣府庁舎別館９階会議室、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
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
奈良由美子	放送大学　教養学部　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
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
岡　　素彦	内閣審議官
上村　昌博	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

【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）

内閣府（防災）

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

文部科学省大臣官房政策課サイバーセキュリティ・情報化推進室

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

鈴木センター長、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」、「分野横断的演習の実施結果」について、資料２、３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４に基づき、総務省、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）

○　資料２の最近のインシデントから得られた教訓について、リスクアセスメントに係る説明として「リスクの洗い出し（特定）」という表現は曖昧であり、不十分なリスクアセスメントにとどまる懸念がある。難しいとは思うが、可能な限り、事業者に刺さるような表現を検討願いたい。

○　資料３について、分野横断的演習の実施結果を評価するにあたり、演習当日

の成果を踏まえて自組織における障害対応体制の改善に向けた評価･検証を行うといったフォローアップの部分まで含めるべきと考える。

○　資料４－１について、我が国のサイバーセキュリティにおいて災害時の通信、電気の確保がきわめて重要な観点であると考えるが、総務省としての取組をうかがいたい。

（松本企画官）

○　資料２に関しては、適切な表現についてご相談させていただきたい。

（紺野参事官）

○　分野横断的演習は、「事前準備」、「演習当日」、「事後改善」の３部構成である。演習後のフォローアップ体制として、各事業者による自組織の障害対応体制の改善に向けた評価･検証のほか、事業者同士の意見交換会、事後アンケート等を実施している。

（総務省）

○　災害時、ICTインフラを途絶させず、可用性を確保することが重要と認識しており、関係部署や事業者等と連携の上、対応を進めている。

（奈良委員）

○　資料３の分野横断的演習当日におけるステークホルダーへの広報について、対象とするステークホルダーの範囲や属性、連携する情報の内容等は、事務局側が指定しているのか。

○　分野横断的演習への対面参加の利点としてネットワーク形成が挙げられる。演習の成果として、このようなネットワーク形成の効果を整理、公表すべきと考える。

○　今後の分野横断的演習の在り方として、演習の内容や参加者の職位をレベル別に分けて開催することも有効だと考える。

（紺野参事官）

○　ステークホルダーへの広報について、事務局として対象等の指定は行っておらず、各事業者が自社の取引先等を踏まえてそれぞれ決定している。

○　社会情勢を踏まえ昨年度からハイブリッド形式での演習を開始した。対外的な説明にあたり、ネットワークの場としての成果も考慮に含めてまいりたい。

○　レベル別の演習について、所管省庁が各分野に対して実施している演習において一定程度カバーすることが想定される。他方、分野に特化しないニーズも考慮すべきであり、政府としての関わり方を検討してまいりたい。

（松本委員）

○　資料３の演習シナリオについて、自組織のシステム障害の影響を受けるサプ

ライチェーンの範囲はどの程度までを想定しているか。

○　今後の演習シナリオとして、まだ認知されていない新しい攻撃手法を用いられた際の対処について取り上げることも有効だと考える。

（紺野参事官）

○　事務局が作成した基本シナリオを各事業者が自社の状況に読み替えてアレンジしており、サプライチェーンの範囲も各事業者がそれぞれの実態に合わせて設定している。

○　演習参加者が多岐にわたるため、シナリオ作成にあたってはトレンドも考慮しつつ普遍的なものを選んでいる。対策が確立していない未知の攻撃に関する要素をどのように盛り込めるか、今後検討してまいりたい。

（前川委員）

○　資料２の最近のインシデントから得られた教訓について、リスクアセスメントは人材の知識や技術的能力に左右されるところが大きい。したがい、知識や技術を伝承する高度な教育が重要であり、本資料に掲載されているような教訓を広く共有することが必要と考える。

（松本企画官）

○　ご指摘の知識や技術の伝承について、追記することを検討したい。また、最近のインシデントから得られた教訓は公開資料であるところ、掲載する情報の適切な粒度について、今後も検討、改善を続けてまいりたい。

（横浜委員）

○　海外の重要インフラ防護政策における大きなトレンドとして、ミニマムベースラインを設定すること、サプライヤーに責任を持たせること、の２点が挙げられる。重要インフラのサイバーセキュリティに係る骨太の方針として、これらの考えをNISCから打ち出してはいかがか。

○　重要インフラ事業者における必要最低限のサイバーセキュリティ要件として、台湾有事を想定したスレットハンティングを実施すべきと考える。政府がシナリオを提供し、それに耐えうる態勢を構築できているか事業者が検証することを義務付けるのがよいと考える。

（中溝審議官）

○　ご示唆いただいたトレンドについて、欧米を中心にそのような動きがあることを承知している。現在、日本としても国家安全保障戦略を踏まえた重要インフラのレジリエンス強化に係る協議を進めており、いただいた観点も含めて検討してまいりたい。

（原田委員）

○　資料２の最近のインシデントから得られた教訓のうち廃止済ドメインの悪用については、一定期間再利用されないよう保障するデポジット制のような管理制度を政府主導で検討されてはどうか。

○　資料４－２について、IoT製品自体のセキュリティのみならず、近年はIoT製品がクラウド上にあげた情報に他の情報が結びつけられるため、そのセキュリティも重要となっている。これは分野共通的な課題であり、NISCを中心に全省庁が取り組むべきと考える。

（紺野参事官）

○　「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」における分野共通的な対策としてIoT製品のラベリング制度に言及する等、検討を進めてまいりたい。

（３）討議事項

「港湾分野における重要インフラとしての取組」について、資料５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

事務局から閉会に際しての挨拶が行われた。

以上