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 38 回会合 議事概要

１ 日時

令和６年 10 月８日（火）14 時 00 分～16 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）

大杉　謙一　中央大学 大学院法務研究科 教授
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
原田　　智　公益財団法人　京都産業 21　DX 推進監　兼　CISO
松本　　勉　国立研究開発法人 産業技術総合研究所 フェロー
　　横浜国立大学 上席特別教授

（オンライン）

木村　昭彦　電気事業連合会　理事・事務局長
奈良　由美子　放送大学　教養学部　教授
伊勢　勝巳　東日本旅客鉄道株式会社　代表取締役副社長 イノベーション戦略本部長
横浜　信一　日本電信電話株式会社 グループＣＩＳＯ

【事務局】

飯田　　陽一　内閣審議官（センター長代理）
木村　　公彦　内閣審議官
安藤　　敦史　内閣審議官
関口　　祐司　内閣審議官
中溝　　和孝　内閣審議官
田村　　亮平　内閣参事官
水廣　　佳典　内閣参事官
杉本　　貴之　内閣参事官
積田　　北辰　内閣参事官
間仁田　裕美　内閣参事官
山田　　隆裕　企画官
松本　　崇　企画官

【オブザーバー】

（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・組織グループ

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

飯田センター長代理、小松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、内閣サイバーセキュリティセンター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。「官民連携演習等」、「企業経営層向け意見交換会」について、それぞれ資料４、資料５に基づき内閣サイバーセキュリティセンターから報告が行われた。「サイバーインフラ事業者に求められる役割等の検討会の設置」について、資料６に基づき、事務局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。）

（横浜委員）

○　各省の取組の多くが、基本取組の底上げに終始している感があるが、外部の脅威環境は、国家を背景とした重要インフラに対する攻撃に移行してきている。それに対する対応というのは、本日ご紹介頂いた限りでは見えなかった。

国家を背景とする攻撃集団ということを考えると、警察庁、防衛省、自衛隊等も関

係省庁になると思うので、それらの取組の紹介もお願いしたい。民間においては、顔と名前が一致するような接点作りをすることが、有事となったときに重要になってくるのではないか。NISC の方向性の一つとしてご考慮頂ければと思う。

（中溝審議官）

○　警察・防衛については、サイバー安全保障有識者会議で実際に議論を行っているところ。当該会議において、様々な関係省庁の役割も含めて議論が行われており、専門調査会においても、議論の状況をお知らせしていきたい。

（松本委員）

○　こういう部門が攻撃をされた、障害が起きたという場合、他の部門にどう影響が及ぶか、他社にはどう影響が及ぶか、ということが、即応においては重要である。広い意味でのリスク分析になるが、どの程度把握されているのかが気になった。国家を背景とする攻撃が来ているというときに、例えば、電力が攻撃されたとすると、通信、流通が危なくなる、というような依存関係がある。依存関係は NISC が調査していたと思うが、マクロなものではなく、もっとミクロに、この企業がこうやられるとこう影響する、という把握に力を入れていくべきではないか。個別の A 社が担っている業務において、どこの電気が止まると困るのか、ということを把握した方が良いのではないか。

（横浜委員）

○　参考までに、東京 2020 大会の際、病院で何か起きても対応できるよう NTT がソフトウェア、システムを提供している病院はどこなのか社内でリストアップした。自社がどこに依存されているのかのリストアップだが、かなり大変だった。９週間の期間限定であれば乗り切れるが、万博の半年間と言われると組織がもたないと思う。外国からのサイバー攻撃はいつ来るか分からないので、同程度の粒度で依存関係を把握し続けるのはかなり大変である。もっと粗いものであれば、地震や台風が起きたときの指定公共機関制度があり、政府の指揮の下に対策を行うものである。自然災害対策はわが国が培ってきた仕組みなので、指定公共機関制度をサイバー対策にも活かすのが現実的ではないか。

（飯田センター長代理）

○　ご指摘の件、概念的には松本委員がおっしゃる通りだと思うが、事業者のコストや負担などを考えると、優先順位付けが必要なのではないかと思っている。

（松本委員）

○　その通りだと思うが、どのような意図で先の発言をしたかというと、わが国の重フラの中でどこが一番弱いのか、ここを攻撃されると一番被害が出るのではないか、というような点を、誰か把握できているのかというと心許ない。NISC が行うべきことではないかと思う。重要インフラ事業者や関連事業者が、可能性としてこういう

ことが起こりうるということを、リアクティブに先例から学ぶことばかりなので、クリエイティブに考えていく必要もあるのではないか。そのためにも、依存関係をきちんと捉えておくことが必要である。コスト云々の話に行く前に、このような課題にどう取り組むべきかを議論することが必要である。

（飯田センター長代理）

○　経済安全保障においても、どこにチョークポイントがあるのかというのは重要な議論である。松本委員の思うような粒度の細かいところまで出来ているかというと心許ないだろうが、想定できていなかったということにならないように、様々なシチュエーションを考慮していきたいが、一律に全部調査するということではないと思っている。

（原田委員）

○　３点発言をしたい。

１点目、資料２－１の重要インフラを取り巻く情勢で、3.1.3.のキューヘンの事案については単に個人情報漏えいの問題とされているが、サプライチェーンの問題、つまり、この事案が発生した部分だけ別ネットワークということはないと思われるため、重要インフラを担う親会社の九州電力と接続されたネットワークで、情報が漏えいした事案として捉えるべきではないか。

２点目、厚労省の報告については、医療機関に対して着実なセキュリティ向上の取組をされていることは分かるが、マイナンバーカードと保険証の一体化が始まろうとする中、何かあるとメディアに大きく取り上げられるため、かなり密度を上げて取組みを進めて頂いた方がよいのではないか。

最後、3 点目のサイバーインフラ事業者検討会については、安全なソフトウェアの提供は非常に重要だが、作った後に脆弱性が発見されても、不確定等の理由を付けて報告しないのではないかという懸念がある。利用者への適切な情報提供は任意なのか、義務なのか。現実的に義務は難しいとしても、せめて努力義務にはされたい。

（松本企画官）

○　１点目について、被害にあったネットワークの構成等の詳細は公表資料には記載がなく、配布資料のような記載としている。

（山田企画官）

○　３点目について、まさにおっしゃるとおりの問題意識を持っている。ライフサイクル全体でどのように対処するかということを考えている。責務、要求事項はガイドラインに書いていきたい。それらをどう仕組みにしていくかは、その後の検討になる。

（原田委員）

○　日本の事業者はビジネスもあるので積極的に取り組んでくれるが、海外事業者は、

隠しているわけではないと思うが、積極的とは言えない。情報が提供されず分からないまま右往左往させられるのは辛い。

（大杉委員）

○　ソフトウェア供給事業者がどこまで情報を出すかということについて、義務を課すには法律が必要。サイバーセキュリティは、ネットワークの外部性があるため、一箇所が弱いとそこが狙われる。しかし、企業の利潤獲得からすると、あまり情報を出したくない。会社は法令を遵守した上で利益を最大化するが、その間に中間領域があって、それがまさに責務である。重要インフラ事業者である以上は、NISC などが作っているガイドラインに書かれた対策事項を守るべきだろう。自分は、プリンシプルと呼んでいるが、会社の利益よりもプリンシプルを優先すべきである。

（松本委員）

○　IoT 製品に対するセキュリティ適合性評価制度について、統一基準、政府系、自治体系にとどまらず、業界全体としてこの制度を積極的に広げていき、業界標準となるように取組んでいただきたい。

（４）閉会

事務局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