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 39 回会合 議事概要

１ 日時

令和７年６月２日（月）14 時 00 分～16 時 00 分

２ 場所

ハイブリッド開催（赤坂グリーンクロス 26 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
白井　大輔　株式会社三井住友フィナンシャルグループ グループＣＩＳＯ　サイバーセキュリティ統括部長
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
高橋　正和　株式会社 Preferred Networks セキュリティアーキテクト兼シニアアドバイザー
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
横浜　信一　日本電信電話株式会社 グループＣＩＳＯ

【事務局】

鈴木　　敦夫　内閣官房副長官補（内閣サイバーセキュリティセンター長）
木村　　公彦　審議官
安藤　　敦史　審議官
関口　　祐司　審議官
中溝　　和孝　審議官
田村　　亮平　参事官
杉本　　貴之　参事官
積田　　北辰　参事官

間仁田　裕美　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
総務省サイバーセキュリティ統括官室
総務省自治行政局住民制度課サイバーセキュリティ対策室
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、小松会長より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、それぞれ資料２から資料６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。「サイバーインフラ事業者に求められる役割等に関するガイドライン（案）の概要」、「サイバー対処能力強化法及び同整備法」について、それぞれ資料８、資料９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。

（本議題に関する主なやりとりは次のとおり。）

（原田委員）

○　資料４－３について、国民の皆様が一番印象に残っているインシデントは、昨年末の航空各社のシステムに対するＤＤｏＳ攻撃かと思うが、現状、ＤＤｏＳ攻撃に対する特効薬はほぼ存在しないと思っている。お盆の時期に同様の攻撃を受ける可能性は高くないと考えているが、国民の皆様の中には、お盆の時期にまた攻撃があるのではないかと心配をされている方もいらっしゃるのではないかと思っている。

国民に対して、NISC が国のセキュリティ対策のリーダーシップを取っているというメッセージを発信することも含め、関連情報の提供など、何か取組をされた方がよいと思うがいかがか。

（間仁田参事官）

○　今回の年末年始のサイバー攻撃に関しては、2025 年２月４日に重要インフラに対して注意喚起をさせていただいている。おっしゃるとおり、今後もこういったＤＤｏＳ攻撃があるということも想定されるため、NISC としてはリーダーシップを取って、メッセージをこれからも出していきたいと思う。

（積田参事官）

○　補足すると、外部に対する発信についてはケース・バイ・ケースで考えなくてはいけないと思っている。今回の重要インフラ事業者に対する注意喚起は対外的に公表しているが、そういったやり方が常によいかどうかはケース・バイ・ケースと考えている。例えばハクティビストによる攻撃は、これだけの被害が発生しているという発信をすることで、攻撃を逆に助長してしまうというような面もあるため、攻撃者の目的に加担するような形での情報発信は避けなければならない。そういった点を踏まえ、常にケース・バイ・ケースで考えていきながら対応していきたい。

（松本委員）

○　金融庁の資料で耐量子計算機暗号（ＰＱＣ）への移行対応について報告されているが、他のセクターに先んじて金融機関側からこのような報告をされたのは、どのような背景があるのか。

（金融庁）

○　ＰＱＣへの移行には長期間を要すること、システム投資や人的リソースの確保が必要といった点や、移行対応について、どのような留意点が存在するか、参考となる情報を整理し、発信していくべきとの業界からの要望を受け、金融業界とそれ以外の専門家にも参画いただき、検討会を開催し、その報告書をとりまとめのうえ公表しているので、今回報告をさせていただいた。

（白井委員）

○　金融庁から説明があったとおり、ＰＱＣへの移行対応には非常に多額のコストと

時間がかかるため、金融業界としては、経営側の課題と捉え、一歩一歩、金融庁と進めているというような状況。当然金融分野への対応として行っているが、メーカーや通信インフラ等も含め、他の産業へも対応は行っていかなければいけないというのが、金融庁が置かれた状況だと理解している。そういう意味では、金融界がまとめたものを今回の法案の成立を受け、NISC でリーダーシップを取っていただき、ＰＱＣのワーキングを立ち上げていただくことが、今後のためになると考えているため、検討をお願いしたい。

（中溝審議官）

○　参考資料３に、先日開催されたサイバーセキュリティ戦略本部で、喫緊に取り組むべき事項として決定した内容を掲載している。6 ページ目にて、「量子技術については、」から「次期サイバーセキュリティ戦略に盛り込む」のくだりで、多岐にわたる課題に対応するため関係省庁による検討体制を立ち上げ、政府機関等におけるＰＱＣへの移行の方向性について、次期サイバーセキュリティ戦略に盛り込むことが決定している。諸外国の状況も踏まえて、ＰＱＣへの対応を政府全体で検討を進めていく。移行の方向性を盛り込む次期サイバーセキュリティ戦略は年内に策定する方向で進めていくが、ご指摘の意向も盛り込むということで検討を進めてまいりたい。

（松本委員）

○　座長を務める暗号技術検討会で個人的にもＰＱＣへの対応は早くしないと困ってしまうと申しあげてきた。ようやくこのような状況となって喜ばしいが、諸外国からはかなり遅れをとっている状況であることから、巻き返していかないといけないと感じている。

（白井委員）

○　ＰＱＣに関して、ＱＫＤという量子暗号通信が通信インフラ全体に関わってくると言われており、時期やスケジュール等色々あると思うが、同じ枠組みの中で検討していただけるとありがたい。

（横浜委員）

○　先程のＤＤｏＳの議論や新しい法案にも関連するが、弊社も同時期にＤＤｏＳ攻撃を受けており、復旧に 10 時間以上かかった。その理由として、非常に攻撃が執拗かつ高度だったため、まずほとんどのアクセスをブロックし、問題のないと思われる接続を少しずつ追加して、穴をあけていくという対策を取った。結果、本件の最終的な復旧には約 10 日以上かかることとなった。

この話は、ＮＴＴグループ内で共有しており、類似の攻撃が発生した場合を想定して、予めホワイトリストを作っておいたらどうかという議論を行っている。実現は容易ではないが、極めて大規模なＤＤｏＳ攻撃が発生した際には、全て止めるのではなく、

重要インフラとしてここだけは絶対に停止してはいけないというリストを予め用意しておき、乱暴ではあるが、必要な通信は担保しそれ以外は止めるという方法もあるのではと考えている。

こういった話は、今回成立した新法案の官民情報連携の中で共有することで、インシデントの経験を他の企業でも活用できると考えている。今回成立した法案の、特に官民連携情報共有には期待しており、今後発生する実例をうまく活用できればと思っている。

（３）討議事項

「重要インフラ事業者等におけるサイバーセキュリティに関する取組等（案）」について、資料 10 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