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 24 回会合　議事概要

１　日時

令和３年１月 26 日（火）16 時 00 分～17 時 00 分

２　場所

Web 会議

３　出席者（五十音順・敬称略）

（委員）

有村　浩一　一般社団法人ＪＰＣＥＲＴコーディネーションセンター　常務理事
安藤　広和　一般社団法人日本ガス協会　技術ユニット長
稲垣　隆一　稲垣隆一法律事務所　弁護士
植田　広樹　日本電信電話株式会社　技術企画部門　セキュリティ戦略担当　統括部長
大友　洋一　電気事業連合会　情報通信部長
大林　厚臣　慶應義塾大学大学院　経営管理研究科　教授
小野　森彦　石油連盟　総務部長
鐘築　泰則　住友生命保険相互会社　情報システム部　システムリスク管理室長
川合　一匡　成田国際空港株式会社　経営企画部門　ＩＴ推進部　次長
河野　敬一　一般社団法人日本クレジット協会　業務企画部部長
小松　文子　長崎県立大学　情報システム学部　教授
志済　聡子　中外製薬株式会社　執行役員　デジタル・ＩＴ統括部門長
神保　　謙　慶應義塾大学　総合政策学部　教授
鈴木　栄一　一般社団法人日本損害保険協会　ＩＴ推進部長
田中　明良　日本放送協会　情報システム局　ＣＳＩＲＴ部長
田中　一三　日本通運株式会社　ＩＴ推進部
手塚　　悟　慶應義塾大学　環境情報学部　教授
戸田　裕之　公益財団法人金融情報システムセンター　監査安全部長
永井　　久　野村ホールディングス株式会社　ＩＴ統括部長
長島　公之　公益社団法人日本医師会　常任理事
中山　広樹　株式会社三井住友銀行　システムセキュリティ統括部　システムリスク管理グループ　グループ長
塗師　敏男　横浜市　総務局　しごと改革室　ＩＣＴ担当部長
野口　和彦　国立大学法人横浜国立大学　客員教授
福島　雅哉　日本航空株式会社　セキュリティ戦略グループ長
堀内　浩規　一般社団法人日本ケーブルテレビ連盟　理事　兼　通信制度部長
細川　　猛　石油化学工業協会　総務部　担当部長
松田　栄之　エヌ・ティ・ティ・データ先端技術株式会社　セキュリティコンサルティング事業部　コンサルティングサービス担当

盛合　志帆　国立研究開発法人情報通信研究機構　経営企画部　統括　兼　サイバーセキュリティ研究所　上席研究員
山北　正宣　東日本旅客鉄道株式会社　技術イノベーション推進本部　システムマネジメント部門　次長
渡辺　研司　名古屋工業大学　大学院工学研究科　教授

（事務局）

髙橋　憲一　内閣サイバーセキュリティセンター長
松本　裕之　内閣審議官
山内　智生　内閣審議官
江口　純一　内閣審議官
吉川　徹志　内閣参事官
堀　真之助　内閣参事官
結城　則尚　内閣参事官
中尾　康二　サイバーセキュリティ参与

（オブザーバー）

内閣官房副長官補（事態対処・危機管理担当）付
内閣官房情報通信技術（IT）総合戦略室
内閣官房東京オリンピック・パラリンピック推進本部事務局
警察庁警備局警備企画課
金融庁総合政策局総合政策課
総務省サイバーセキュリティ統括官室
外務省大臣官房情報通信課
文部科学省大臣官房政策課
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
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

４　議事概要

（１）開会（挨拶）

髙橋センター長及び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

「関係省庁の取組状況」について、資料２に基づき総務省及び経済産業省から報告が行われた。また、「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３及び資料４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。）

（稲垣委員）

○　ぜい弱な状態にあるIoT機器を見つけ出し、管理者に注意喚起を行うという総務省の取組は素晴らしいが、事前に調査対象から何らかの同意を得ているのか。

（総務省）

○　今回の調査は、一般に公開されているインターネット上の管理画面を調査するものであり、調査対象から事前の同意を得るということは特段行っていないが、御指摘の点も踏まえ、今回の結果をどのように活用していくか検討していきたい。

（稲垣委員）

○　このような取組は引き続き進めていくべきであるが、法的な問題が今後出てくることも考えられるため、万全を期して進めるようにしていただきたい。

○　次に、ランサムウェア対策に関し、経済産業省に伺いたい。ランサムウェアの被害に遭った企業が加害者に対して資金提供することは、犯罪行為に対する協力とみなされ、制裁を受ける構造になっている。これ自体は特に問題ないと思うが、ランサムウェアの被害を受けた企業が身代金を支払わずとも事業を継続できるよう支援していくべきではないか。

（経済産業省）

○　IPAにJ-CRATという組織を設けており、重要インフラ等で被害が発生した場合には、必要に応じてチームを現場に派遣し、被害企業と協力して初動対応に当たるとともに、技術的な支援を行うこととしている。

○　また、ランサムウェアによる被害に遭わないようにする、仮に被害に遭ったとしてもビジネスを継続できるようにする等も重要であるため、注意喚起の実施やガイドラインの公表により、事業者が適切な対策を行えるよう支援している。

（野口委員）

○　リスクマネジメントの世界では環境が変化するとリスクも変化すると教えているが、新型コロナウイルス感染症の拡大によってもたらされた社会や企業運営の変化がサイバーセキュリティにどのような影響を与えたかについて何か分析されているのか伺いたい。

○　また、サイバーセキュリティの世界で先手を打つためには、今後どのような変化が起こるかという予測を共有した上で対策を考えていくことが非常に重要となる。資料にはそのような観点を含めていただけるとありがたい。

（結城参事官）

○　先端技術を有する産業が狙われるなど、サイバーの脅威は高まっており、その手法も巧妙化していることから、これらに対してどのような対策を行っていくのかということを行動計画では検討していく必要があると考えている。

○　世界各国においてサイバーセキュリティ対策が始まったのは2000年頃であり、そこから20年が経過したが、この20年で起きたこととこれから先20年で起こることは同じではないと考えている。かつては事業者一律で対策を考えていたが、同じ物理事象でも事業者が置かれている状況によってリスクは変わってくるということを踏まえると、共通脅威の高まりにどのように対処していくかということとともに、事業者の特質を踏まえてどのように対応していくべきかということも検討していく必要があると考えている。

（３）その他

「次期重要インフラ行動計画の検討」について、資料５に基づき事務局から説明が行われた。また、「政府のデジタル改革を巡る動向」について、資料６に基づき内閣官房情報通信技術（IT）総合戦略室から説明が行われた

（本件に関する主なやりとりは次のとおり。）

（稲垣委員）

○　次期行動計画においては、どこにどういう人材を供給し、その人材を誰が育てていくのかという、人材育成のグランドデザインを検討することも盛り込んでいただきたい。人材育成の重要性については企業側の認知も進んでおり、経営課題だと認識されていると考えている。

（結城参事官）

○　人材育成は、経営層、実務者層等のそれぞれの階層において求められる能力を明確にした上で、必要な教育を進めていくべきだと考えている。また、サイバーセキュリティは経営の課題の一つだという観点から、企業経営にまで踏み込んで人材育成の在り方を記載する必要があると思う。

○　なお､人材育成については､ＮＩＳＣ内で専門に検討を行う体制があるため、そのチームと連携して進めていくこととする。

（野口委員）

○　将来展開をどう見るかによって行動計画の内容は大きく変わってくるため、検討の視点は「事業の特質及び現状を踏まえた」ものだけではなく、「現状と将来展開を踏まえた」ものであることも大事だと思う。

○　現在の行動計画が優れていたのは、経営というものにメスを入れたというところだと考えている。サイバーセキュリティは現場のものというこれまでの考

え方から、経営も含めたセキュリティ体制の構築という内容を入れたことは、非常によかったと思う。その一方で、経営側でも使いづらく、現場側も使いづらい中途半端なものになってしまったことはないだろうかと若干心配をしている。行動計画をより具体的なものしていくためには、総合的な計画と同時に、マネジメントという視点と現場の技術という視点の両方が重要である。

○　また、セキュリティはシステムありきで考えられているが、セキュリティ対策というのは、どういうシステムを構築するかというシステム導入の計画の段階から始まるものである。次期行動計画は、このタイムスケジュールを踏まえて総合的に考えていく必要があるのではないかと思う。

○　サイバーセキュリティというのは、サイバーに関する知識だけではなく、それを使う社会や事業者の組織マネジメントの知識、人間の特性に対する知識等が必要となる。次期行動計画では、そういう実務の専門家を集めて検討をやっていただきたい。

（結城参事官）

○　次期行動計画の検討に当たっては、政府側からの視点だけではなく、事業者側の視点も入れてレビューを行い、何をどう変えたらいいのかということは明らかにしていきたい。

○　また、マネジメントについては、上からトップダウンでやるものと下から積み上げるものの両方を理解して調和させることが重要であると考えており、今回の目標の一つとしている。このためには、それぞれの事業者のプロファイルを明確にした上で、その特性を踏まえてリスクを認識し、リスクコンシャスで資源を有効に配分していくということが前提となる。一律のリスクではなく、事業者が自らのリスクは何かと同定するところから始められるようにしたいと考えている。

（大林委員）

○　行動計画では、システムを重要インフラ防護の対象としているが、データドリブンのシステムもあることから、重要インフラサービスを維持するためには、重要なデータのセキュリティをどう確保していくかについても考えていく必要があるのではないか。

（結城参事官）

○　現在の行動計画が防護の対象としている資産はシステムであるが、この資産の中にデータも加えていきたいと考えている。また、昨今のトラブルは、不適切な資産管理に起因するものが多数見受けられることから、重要インフラの範囲や定義についても検討を行っていくことを提案したい考えている。

（４）閉会

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