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 26 回会合　議事概要

１　日時

令和３年 10 月 25 日（月）16 時 00 分～18 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
稲垣　隆一　稲垣隆一法律事務所　弁護士
植村　元洋　野村ホールディングス株式会社　グループ・ＩＴ統括部長
臼井　　節　一般社団法人日本ガス協会　技術部長
大杉　謙一　中央大学　大学院法務研究科　教授
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
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
亀田　浩樹　株式会社三菱ＵＦＪ銀行　取締役常務執行役員　ＣＩＯ
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
木村　正人　日本電信電話株式会社　技術企画部門　セキュリティ・アンド・トラスト室　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
佐藤　政広　石油連盟　企画総務部部長
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
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
田中　明良　日本放送協会　情報システム局　ＣＳＩＲＴ部長
手塚　　悟　慶應義塾大学　環境情報学部　教授
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
西原　靖幸　株式会社三菱UFJ銀行 システム企画部 サイバーセキュリティ推進室 サイバーセキュリティグループ 次長
塗師　敏男　横浜市　最高情報セキュリティ責任者補佐監
野口　和彦　横浜国立大学　客員教授
細川　　猛　石油化学工業協会　総務部　担当部長
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

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
松本　　勉　横浜国立大学　大学院環境情報研究院　教授
宮本　一厳　日本通運株式会社　ＩＴ推進部専任部長
盛合　志帆　国立研究開発法人情報通信研究機構　サイバーセキュリティ研究所　研究所長
師岡　　悟　公益社団法人日本水道協会　工務部　規格課長
山内　勝浩　公益財団法人金融情報システムセンター　監査安全部長
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
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　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
下田　隆文　内閣審議官
吉川　徹志　内閣審議官
江口　純一　内閣審議官
中溝　和孝　内閣参事官
堀　真之助　内閣参事官
結城　則尚　内閣参事官

（オブザーバー）

内閣官房（事態室）
警察庁警備局警備企画課
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
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（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

「重要インフラを取り巻く情勢」「分野横断的演習の実施」「関係省庁の取組状況」について、資料２、３及び４に基づき事務局から報告が行われた。

（３）討議事項

「重要インフラ行動計画の改定」について、資料５に基づき松本委員から説明がなされ、討議が行われた。

（本議題に関する主なやりとりは次のとおり。）

（野口委員）

○　【提言１】について、これまでは「経営層への働きかけ」としていたが、サイバーセキュリティの専門的・技術的な問題点と、経営者が抱えている事業運営の問題点を融合させるといった大きなマネジメントイノベーションととらえて頂きたい。

○　【提言２】について、これまでサイバーセキュリティはサイバー攻撃など事前に予測することは不可能だという甘えがあった。しかし、実際には外からの攻撃以外にも管理すれば対策できる事例が多い。ただし、起きていない可能性を見つける技術的な問題がある。それらは、アタックゼロという視点のリスク分析の仕方、設計や技術的な問題に対するリスクの洗い出し、マネジメントが起因する問題の洗い出しなど、全てリスク分析方法が異なる。そういった難しいことにチャレンジしようとする提言だとお考えいただきたい。

（前川委員）

○　政策部会は、最初は12の論点の議論から始まった。環境が劇的に変化する中で、行動計画で何を変えたいのか、どこを強化するのかということを考えたときに12の論点だけでは曖昧になると懸念されたため提言を提出することとなった。

○　【提案１】の「経営層への働きかけ」から、組織統治の一部として対応することを入れることは画期的である。サイバーセキュリティ基本法は、重要インフラ事業者はサービス提供に関して責務を持っている。

（長島委員）

○　医療の分野では、セキュリティの専門家を確保できないという事業所が大部分であるため、厚生労働省において、医療情報システムの安全管理に関するガイドラインの中にチェックリストとフローチャートが新たに作成された。今回、「行動計画の改定に向けた議論が行われる中で、障害対応体制の強化に

向けて参考になる取組であるため紹介する。

（山北委員）

○ サプライチェーンに関して、細かい内容は次期行動計画の中には書かれるのか。

（結城参事官）

○　サプライチェーンに関しては、何が必要か整理し枠組みからはいっていくことを考えている。事業者が決めるものと国が決めるべきところがあるので、委員会と相談しながら進めていきたい。

（横浜委員）

○　効果的な対策とは、時代にあった、あるいは時代を先取りした対策、包括的な視点にたった対策である。

（神保委員）

○　論点の１つである「関係主体の責任及び権限」についてサイバーセキュリティ戦略を見てみると、場合によっては一つの事象に対応すべき担当省庁の数が6-8個と多い。

○　事業者の任務保証で完結しない国民の安全と直結するような横断的な攻撃が増えている。分野横断的演習については事態別に関係省庁を含めたインシデントレスポンスのフローを作る段階になってきたのではないか。

（結城参事官）

○　国としてどうするのかはサイバーセキュリティ基本法で明示的に決められているが、より大きい括りが必要と考えている

（高橋委員）

○　現場の立場からするとセキュリティ対策がそもそも難しいことであるということが謳われていない点が懸念点である。実施すれば対策ができるということ前提になっている論調に見えるが、セキュリティ対策の難しさを経営層に謳う一文を入れるべきである。

○　セキュリティ対策を実施する人がしっかりと評価されるようになるとよいと考える。

（野口委員）

○　高橋委員のご指摘はその通り。サイバーセキュリティの主語を大雑把にするのではなく、実施すべきことを経営として判断することが大事だと考える。大規模なシステムになるほど対応が難しいため、難しさを経営が理解したうえで対応することを記述する。

（稲垣委員）

○　サイバーセキュリティの定義をサイバーセキュリティ基本法から引用しており、技術的なサイバーセキュリティの脅威に対応するのではなく、あらゆる脅威に対応して情報システムや事業の任務を保証するという取組を出発点とすることが大事だと考える。今まではシステム防護のみだった。

○　経営課題として捉えるというレベルからは決別し、統治の責任について具体的に何ができなければならないのかといった目標を立てられるような行動計画にするべきである。

○　「企業統治」を謳う以上は「論点６：関係者の責任と取組」の中に企業統治に係る関係者を考慮するべきである。

○　お金の流れについては金融機関、証券会社、監査法人の監査事務、会計システムなどの関係者がいる。取締役だけではなく企業会計や株式評価の指標にも関連部署に入ってもらうべきである。

○　具体的な行動について、国の責任として書き込むべき。事業者に対して実施することを謳うだけでは、環境も作らずに結局できないことに陥る懸念がある。

○　経営層と直接やり取りをしているか。経営者はセキュリティを経営課題と認知しているが、具体的な内容を求めている。

（結城参事官）

○　実践するためには、重要インフラサービスの継続的な供給という性質から「継続的な改善」といった方策が求められる。

○　現場レベルでは把握しているものの、経営層にエスカレーションができず結果的に企業の大損失に繋がったという類似事案が目立っているため、風通しをよくする施策はすぐにできるのではないか。

○　2014年度に公布、施行された「サイバーセキュリティ基本法」と「第４次行動計画」は関連性が明確ではなく、行動計画の位置づけについて全く認知されていない。まずはできるところから実施し、実施しながら改善していくことが一つの方策である。

○　経営層についてのご指摘については、政策部会に経営層にも参加していただき、すでに議論を実施している。

（長島委員）

○　デジタル庁の設置について、サイバーセキュリティに関して今後どのような役割を果たし、どのようにすべきと考えているか。

（結城参事官）

○　デジタル庁とNISCは車の両輪として定期的な打合せや顔合わせ等を実施しており、論点５に項目として出している。

○　昨年末の閣議決定におけるIT基本法の改正で、少なくとも５年以内に地方自治体の抜本的な改革を行うとされており、さらには準公共として医療と防災が検討されていることについて、デジタル庁と一緒に進んでいく。

（大林委員）

○　情報セキュリティ分野は、会社全体を動かすほどの障害が発生する頻度は稀であるため、経営者に専門知識が足りず、組織内外の連携ができないといった問題がある。例えば、地震防災では、メディアなどを通じて予備知識が備わっている経営者や政治家が多いため、比較的この課題を解決している。情報セキュリティについても、世間一般に成功例、失敗例、リスク、影響などを広報していくのがよい。世論が動き出せば、経営者も動かざるを得ないと考える。

（横浜委員）

○　米国では監督と執行が分離しているが、日本ではそうではない会社が多いため、日本の現実に即した対応が重要である。必ずしも取締役だけではなく、経営会議メンバーも考慮したものにするとよいと考える。

（小松委員）

○　経営層の働きかけについて、経産省が発行した「サイバーセキュリティ経営ガイドライン」を確認し、具体的に足りないところについて考慮しているのか。

（結城参事官）

○　次期行動計画では、「サイバーセキュリティ経営ガイドライン」を踏まえている。本ガイドラインの内容は、経営層に対する希望レベルであったが、次期行動計画は実際に経営層を巻き込んで作り上げている。

○　実装ベースになった場合には「サイバーセキュリティ経営ガイドライン」は

使用できる。今回はトップからのメッセージという点が新しいところである。

（４）閉会

次回の専門調査会の開催の調整について、事務局から連絡があった。

以上