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 30 回会合　議事概要

１　日時

令和４年９月 20 日（火）14 時 00 分～16 時 00 分

２　場所

Web 会議

３　出席者（五十音順・敬称略）

（委員）

内川　　淳　　株式会社三井住友銀行　取締役　兼　専務執行役員
大杉　謙一　　中央大学　大学院法務研究科　教授
小松　文子　　長崎県立大学　情報システム学部　教授
佐々木秀明　　電気事業連合会　理事・事務局長
神保　謙　　慶應義塾大学　総合政策学部　教授
武田　雅哉　　青森県　ＩＴ専門監
奈良由美子　　放送大学　教養学部　教授
野口　和彦　　横浜国立大学　客員教授
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
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

（事務局）

下田　隆文　内閣審議官
内藤　茂雄　内閣審議官
上村　昌博　内閣審議官
小柳　誠二　内閣審議官
中溝　和孝　内閣参事官
紺野　博行　内閣参事官
中越　一彰　内閣参事官
松本　　崇　企画官
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（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
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
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

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

「分野横断的演習の実施」、「重要インフラを取り巻く情勢」、「情報共有の手引書」について、資料２から資料４までに基づき、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。）

（小松委員）

○ 半田病院のランサムウェア被害について政府から注意喚起を発していたにも関わらず、インシデントが発生してしまった。この事実に対する教訓があった方がよいと思う。被害者の方に注意喚起が届いていなかったのか、又は注意喚起が届いていたが対応できなかったのか、その点はいかがか。

（松本企画官）

○ 医療機関における事例について、今後、補完調査等で深掘りするなどして、御指摘の点についても情報を追加、共有できるよう検討してまいりたい。

（厚労省）

○ 半田病院の報告書では、脆弱性情報について、医療機関に届いているにも関わらず、医療機関及びベンダー双方が自らが対応する必要があると認識しておらず、双方の責任に帰するものであったと指摘されている。

○ このような事態を招かないためにも、現在、ベンダーと医療機関等の合意形成を促進する取組を検討しているところである。

（野口委員）

○ サイバー攻撃だけでなく、様々な要因による不完全性への対処という観点が、新しい行動計画におけるポイントの１つである。「重要インフラを取り巻く情勢」で取り上げられた事例は、サイバー攻撃にやや特化している印象を抱いた。国際的な緊張感が増大している情勢下において攻撃に備えることは重要だが、管理ミスや機器の故障等のトラブルの原因を考えることは非常に重要であるし、加えて、大規模災害時における情報通信等の重要インフラの可用性についても重要であると考えるが、今回は取り上げるべき事例はなかったという理解か。

（松本企画官）

○ 今後の情勢分析における検討としたい。

「関係省庁の取組状況」について、資料５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。

（本議題に関する主なやりとりは次のとおり。）

（前川委員）

○ KDDIの通信障害の原因は作業者個人のミスなのか、プロセス自体の問題なのか。また、誤設定を検知した際に正常な状態に戻すプロセスが存在していたか。

（総務省）

○ 作業員が古い手順書を参照し、誤ったプロセスで作業を進めた。その後すぐに気が付いて正しい設定に戻そうとしたが、その過程で輻輳が生じた。再発防止として、正しい手順書を参照することや、問題発生時に被害を抑制しながら復旧させることについて検討を進めている。

（野口委員）

○ KDDIの通信障害はリスクアセスメントの観点において、自らのシステムを運用する際のリスクを事前にどの程度のレベルまで把握、分析できていたのか。

（総務省）

○ リスク評価は一定程度実施されていたと思われる。リスクを低減させることも含め、再発防止策の検討としたい。

（松本委員）

○ クレジットカードの不正利用について、2013年頃から被害額が増えているが、店頭での対面販売とネットショッピングのいずれが多いか。

（経産省）

○ ECサイトにおける不正利用が増加しており、これを含めた再発防止策を検討している。

（３）討議事項

「安全基準等策定指針・手引書の改定」について、資料６に基づき事務局から説明が行われ、討議がなされた。

（本議題に関する主なやりとりは以下のとおり。）

（前川委員）

○ 組織統治の一部としてサイバーセキュリティを実施することが今回の指針改定におけるポイントである。経営会議等でサイバーセキュリティに関する取組の決定を行うこと、また、サステナビリティにおけるエコシステムのように、サイバーセキュリティも取り組んだ企業が社会から評価されるような仕組み作りを行うことが重要な検討事項であると考える。

（紺野参事官）

○ サイバーセキュリティ確保にあたり、コストに目がいきがちな現状を課題として認識しており、指針改定にあたっての検討としたい。

（松本委員）

○ 現行の指針の構成としてPDCAが採用されているが、PDCAだと実際の危ない状況に対して十分な機動力をもって対処できないケースが増えているとの認識である。

（紺野参事官）

○ 現行の指針は過去のISOをベースに作成しており、PDCAに沿った構成となっている。御指摘の点を踏まえて柔軟な対応を検討したい。

（野口委員）

○ 継続改善の意思表明としてのPDCAであることを明確化した方がよい。また、民間だけでなく国のPDCAも明らかにすべき。サイバーセキュリティに関しては定期的ではなく随時見直さなければ、対応が間に合わないのではないか。

○ 任務保証をどの程度まで担保するかは、民主主義国家として事業者が決定することだが、重要インフラに関しては社会がそのレベルを要求、決定する要素もある。任務保証の説明について今一度検討する必要があるのではないか。特に、大規模災害時のサービスの可用性についてどの程度のレベルで設定するかは国として重要な指針である。

○ 17スライドのセキュリティガバナンスのイメージ例は、サイバーセキュリテ

ィの回し方を示しており、ガバナンスのイメージ図にはなっていない。企業が事業計画とサイバーセキュリティをどう関連させるかについての枠組みがなければガバナンスとはいえない。ただし、イメージ化は非常に難しい課題であるため、時間をかけて議論したい。

（紺野参事官）

○　行政のPDCAについて、行動計画で示されている評価・検証を確実に行い、各項目の実施状況等について確認、改善してまいりたい。

○　任務保証について、大規模災害時の可用性をどの程度のレベルで設定すべきかを含め、今後の検討としたい。

○　ガバナンスのイメージ図について、読み手に正確に伝わる内容となるよう、今後の検討としたい。

（奈良委員）

○　指針改定案の構成として、組織の状態の確定や、モニタリング及びレビュー、リスクアセスメント及びリスク対応、コミュニケーションといった要素を内包し、具体的且つ構造的にまとめられており評価できる。特に、リスクコミュニケーションについて、リスクアセスメントの全プロセスに関わる構造としているのは適切であると考える。

○　平時と障害発生時に分けて項目を設定した点も評価できる。これまでのアンケート調査によると、DoとCheckの部分が低調であり、当該部分の実効性を確保する意味で、指針の内容が充実するのは大変良いものと捉えている。また、セキュリティを組織的、物理的、技術的、人的の４つに分けている点も現場実態に沿った適切な整理であると考える。

○　16、17スライドのガバナンスのイメージ図は、事業者にとって実施が難しい印象を受けた。各事業者の既存の仕組みを応用、流用可能なガバナンスを考え、そこにサイバーセキュリティを取り込んでいきたい。

（紺野参事官）

○　ガバナンスのイメージ図について、事業者にとっての分かり易さや、各分野における組織の違いを考慮して、今後の検討としたい。

（佐々木委員）

○　サプライチェーンリスク対応について、事業者は指針だけでなく経済安全保障推進法への対応も求められるところであり、両施策の方向性がずれることのないよう検討を進めていただきたい。また、サプライチェーンリスク対応の重要性は理解する一方、自由な企業活動や経済的な効率性が必要以上に阻害されないよう、配慮をお願いしたい。

○　サプライチェーンリスクの整理にあたり、調達リスクやソフトウェアの不正使用リスク等様々なものが挙げられているが、指針においてはいずれのリスクを想定したものなのか明示していただきたい。

（紺野参事官）

○　経済安全保障推進法に関して、国家安全保障局を中心に具体的な決定がなされていくものと承知しているが、引き続き当該議論を注視してまいりたい。

○　自由な企業活動や経済活動の効率性を確保する点、具体的なリスクを明示する点について、本調査会やセプター等を通じて事業者の意見を聞きながら、今後の検討としたい。

（大杉委員）

○　15スライドの「CISOを取締役会から設置する」旨の記載について、取締役から１人CISOをあてがう、取締役会においてCISOを任命する、の２通りの解釈ができる。日本の大企業においてもCISOが取締役であるケースはごく一部であり、前者を強く推奨することは現実的ではないので、取締役会が経営幹部としてCISOを選任するという趣旨が明確に伝わるようにすべき。

○　セキュリティに詳しくない人物に形式的にCISOの肩書きを与えるのではなく、CISOは、セキュリティ部門と信頼関係を築いて忌憚なくコミュニケーションでき、経営層にも直言できるような立場が望ましい。そうした立ち位置、職務を経営層や取締役会が理解した上で任命すべき。

○　前川委員が指摘されたサステナビリティの取組事例は、ESGやSDGｓに該当するかと思うが、サイバーセキュリティはSDGsの「産業と技術革新の基盤をつくろう」という目標に繋がるものであり、そうした観点から議論を進めることも可能であろうと推察する。

（紺野参事官）

○　CISOの記載に関しては、分かり易い表現となるよう、今後の検討としたい。

○　SDGｓの観点についても効果的に取り込んでいけるよう、今後の検討としたい。

（小松委員）

○　企業統治の一部としてサイバーセキュリティを実施するということは、エンタープライズリスクマネジメントの中にサイバーセキュリティを組み入れることと理解している。その際、他のリスクと並行して評価することになり、これにはリスクの定量化が必要。サイバーセキュリティはリスクの定量化が難しく、IPAの制御システムにおけるリスクアセスメントでは発生頻度というよりは発生可能性を考慮する試みを行っている。発生頻度に囚われない現実的なリスクアセスメント手法を盛り込んでいただけるとよい。

（紺野参事官）

○　IPAの手法を含めて確認の上、今後の検討としたい。

（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