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 11 回会合　議事概要

１　日　時

平成 29 年 6 月 27 日（火）10 時～12 時

２　場　所

金融庁 13 階　共用第一特別会議室

３　出席者（五十音順・敬称略）

阿部　克之　委員　（電気事業連合会）
有村　浩一　委員　（一般社団法人ＪＰＣＥＲＴコーディネーションセンター）
大高　利夫　委員　（神奈川県藤沢市）
大平　充洋　委員　（一般社団法人日本クレジット協会）
荻島　　敦　委員　（日本通運株式会社）
金子　　功　委員　（一般社団法人日本ガス協会）
真田　博規　委員　（住友生命保険相互会社）
鈴木　栄一　委員　（一般社団法人日本損害保険協会）
鈴木　　悟　委員　（株式会社三井住友銀行）
手塚　　悟　委員　（慶応義塾大学　大学院政策・メディア研究科）
西村　佳久　委員　（東日本旅客鉄道株式会社）
野口　和彦　委員　（国立大学法人横浜国立大学　リスク共生社会創造センター　兼　大学院　環境情報研究院）
橋本伊知郎　委員　（野村ホールディングス株式会社）
原田　　充　委員　（日本航空株式会社）
平田　真一　委員　（日本電信電話株式会社）
細川　　猛　委員　（石油化学工業協会）
増子　明洋　委員　（日本放送協会）
松田　栄之　委員　（ＮＴＴデータ先端技術株式会社）
盛合　志帆　委員　（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）
若林　武夫　委員　（公益社団法人日本水道協会）
渡辺　研司　会長　（名古屋工業大学　大学院工学研究科）
渡辺　　睦　委員　（石油連盟）
和田　昌昭　委員　（公益財団法人金融情報システムセンター）

（「重要インフラ専門調査会の設置について（平成 17 年 9 月 15 日情報セキュリティ政策会議決定）」４．による出席）

中島　一郎　（早稲田大学研究戦略センター）
（重要インフラサービス障害に係る対処態勢検討ＷＧ主査）

（事務局）
中島　明彦　内閣サイバーセキュリティセンター長
永井　達也　内閣審議官
三角　育生　内閣審議官
中尾　康二　サイバーセキュリティ補佐官
山内　智生　内閣参事官
栁島　智　　内閣参事官
林　　泰三　内閣参事官
瓜生　和久　内閣参事官
阿蘇　隆之　内閣参事官

（オブザーバー）
日本銀行金融機構局
一般社団法人日本民営鉄道協会運輸調整部
金融庁総務企画局政策課サイバーセキュリティ対策企画調整室
総務省情報流通行政局情報流通振興課情報セキュリティ対策室
総務省自治行政局地域政策課地域情報政策室
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
厚生労働省医政局研究開発振興課医療技術情報推進室
厚生労働省医薬・生活衛生局生活衛生・食品安全部水道課
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原子力災害対策・核物質防護課核セキュリティ・核物質防護室
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
警察庁警備局警備企画課サイバー攻撃対策官
警察庁長官官房総務課
警察庁情報通信局情報技術解析課
外務省大臣官房情報通信課
防衛省整備計画局情報通信課サイバーセキュリティ政策室

４　議事概要

(1) 開会（挨拶）

渡辺会長から挨拶。

○渡辺会長　本日も、お忙しい中参集いただき、感謝申し上げたい。

４月のサイバーセキュリティ戦略本部においては、皆様に御協力いただき当専門調査会で検討してきた第４次行動計画が決定され、重要インフラにおけるサイバーセキュリティの取組が、新たなステージに入ったと考えている。本日は、その手始めとして、行動計画に沿った安全基準等策定指針の見直しについて、特に、重要インフラサービス障害に係る対処態勢検討WGの検討結果について、本日参加いただいている中島主査から説明をうかがった上で、議論いただきたい。ポイントは、コンティンジェンシープラン及び事業継続計画の策定を含めた対処態勢の整備、ＩＴのみならずＯＴ（オペレーションテクノロジー）も視野に入れた対策等を考慮していくことの２点。

このWGには、私も含め本日参加いただいている委員、総勢６名が参加しており、本日は、中島主査にお越しいただき、議論の結果について報告いただくこととしている。対処態勢整備に係るサイバー攻撃リスクの特性が主要な議題であったが、サービスに異常が発生したときの対処については、分野ごとに考え方や価値観が異なり、まとまりをつけることが難しい状況ではあったものの、ひとまず中間報告という形で提示できる状態になってきたと考えている。成果物の適用対象等々についても、活発な議論があったので、本日はその結果を報告いただくことになる。

この他、報告事項の後には、重要インフラにおける昨年度の取組状況と今後の取組についてまとめた、重要インフラにおける取り組みの進捗状況等（年次報告）について、承認いただきたいと思っている。

本日も、闊達な議論をお願いしたい。

○渡辺会長　繰り返しになるが、本日は、重要インフラサービス障害に係る対処態勢検討WGで主査を務めていただいた中島主査に参集いただいている。

これは、「重要インフラ専門調査会の設置について」の第４項に「専門調査会の会長は、必要があると認めるときは、当該専門調査会の委員以外の者に対し、当該専門調査会の会議に出席して意見を述べることを求めることができる」とあり、この条項に基づき、私が、会長としてお呼びさせていただいたこととなる。

○柳島参事官　委員の変更について報告する。銀行分野において門野様から鈴木様に、金融分野において西村様から和田様に変更になっている。また、中尾委員については、４月１日よりサイバーセキュリティ補佐官に就任され、委員の立場から補佐官の立場に変わり、引き続き、議論に参加いただくこととなった。

(2) 報告事項

警察庁より資料２について、林参事官より資料３について報告。質疑応答は次のとおり。

○野口委員　東京オリパラ競技大会は、情報セキュリティを強化する１つの大きなターゲットになっていると承知しており、そういう意味で、状況を踏まえつつ訓練等が行われていることは理解している。しかし、それぞれのアプローチにより、順次詰めて

いくという方法で、本当にオリパラというものに必要な訓練が全てできるのだろうかという心配をしている。

オリパラの場合、警察庁から説明があったように、例えば、東京スタジアムで水が出なくなるだけでトイレが使えなくなり、非常に大きな支障が出るし、山手線が止まるだけでかなり大ごととなる。このような大会においては、１つの要素が機能しなくなるだけで、非常に大きな障害となることがある。

このように、オリパラに向けての訓練ということとＮＩＳＣの情報セキュリティというものの視点での訓練とをどこで合わせるかという問題があり、ＮＩＳＣの立場で訓練を行うことに問題はないと考えているが、ＮＩＳＣで行っている訓練があたかも東京オリパラに必要な訓練のかなりの部分を満足していると捉えられてしまうことが、非常に怖くて心配している。オリパラを見据えた場合、オリパラにおける必要な訓練とＮＩＳＣの行っている訓練がどのような関係にあり、その必要十分条件は何なのかを、一度どこかで調整していただきたい。

○警察庁　ご指摘の点には同意。警察では、年間数百程度の訓練を10年以上継続しており、そこで得た知見をＮＩＳＣとも共有している。今回の訓練においても、50人程度の参加者に対し、同時にＮＩＳＣを含めて50人程度に見学をしてもらっている。抜けがないようにという点はご指摘のとおりではあるが、最初から全てを見通して網羅するというのは難しい面もあるので、現在は、できるところから数多く実施して情報を共有し、お互いに穴を見つけて埋めていくというアプローチをとっているところ。

○永井審議官　ご指摘の電車が停止するという事象は、サイバー攻撃だけではなく、テロや自然災害、その他の物理的な障害によっても発生し得ると理解。内閣危機管理監が長となったオリパラのセキュリティ幹事会の中で、サイバーも含め、さまざまなリスク要因により事象が発生したときに、どう対応するのかということについて検討しており、全体の総合調整訓練等もあわせて行っているということを補足させていただきたい。

○野口委員　官の視点では、セキュリティという、つまり被害を生じさせないという観点を中心に取り組む傾向がある。しかし、オリンピックの運営という意味で言えば、被害が出ないということだけではなく、一般の観客が気持ちよく楽しくなるよう運営する、参加者も満足をもって大会を終わるということが求められ、セキュリティの視点とは少し異なるのではないかと思う。

繰り返しになるが、ＮＩＳＣの視点で行っていることは、今の感覚で十分だと思っている。一方で、オリパラというものの必要十分の考え方と、いわゆるセキュリティ、サイバーセキュリティという考え方との取り合いについては、整理を行うべき。ここですべてをカバーしなければならないと言っているわけではなく、ここで行っていることはこういうことで、ここが抜けているということを整理しておかなければ、そこでつまずく可能性があると感じているという意味とご理解いただきたい。

○渡辺会長　イベントやエンターテイメント的な部分との接点を見ながら、それぞれの訓練の位置付けを認識しながら実施するべきとの指摘と理解。そのような意識で調整をお願いしたい。

○手塚委員　サイバーだけではなく、さまざまな視点で検討しているという話をうかがい、非常に心強く思ったところ。そのような中、シナリオがどのくらい蓄積されているかという点を定量的な形で示すことが有効だと考える。今後、網羅性を検証する際に重要になると思うので、シナリオ項目などを整理していただきたい。

分野横断的演習について。資料３の最後のページを見て、2006年からはじまり10年間の努力のたまものであると感じている。数値的には参加人数が順次増加していることが確認できる一方で、どのようなところを最終的な目標とするのかについては、今後、検討が必要なのではないか。このようなものは、避難訓練と似たようなところがあるので、全国規模で９月１日に避難訓練の日を決めて実施するというところにつなげるのか、もしくは、何らかの分野で設定して実施することとするのか、そのような大きな考え方を検討いただければと思う。

○林参事官　シナリオについては、今年度の演習に関し、現在、具体的にどのような内容にするべきかについて、事務局で検討を開始させていただいているところ。今後、分野横断的演習の検討会の場などを通じ、有識者の意見等々をうかがいながら、できる限り実践的かつプラクティカルなものにしてまいりたいと考えている。

分野横断的演習の最終的な到達点、目標に関し、参加人数については、昨年度の演習で既に2,084名となっており、数字としてはマキシマムに近い水準に到達しつつあると考えている。会場には一定のキャパシティーの上限があること、我々としては、演習のあるべき姿という視点から、必ずしも数字のみを追求しているわけではないことから、2017年度においては、量的な部分もさることながら、質の面を含め、演習の実質的内容、密度の充実について注力していきたいと考えている。

(3) 決定事項

栁島参事官より資料４について説明。質疑応答は次のとおり。

○盛合委員　資料４－１の３ページ目の表１に、重要インフラ事業者等との情報共有件数が記載されており、2016 年度は、前年に比べ２倍近くになったと示されている。さきほどの説明では、情報共有件数の増加と脅威の高まりとは無関係との説明がなされたが、そうであるならば、この数字を何の指標と考えるべきなのか、あるいは、ここから何を読み取るべきかについて教えていただきたい。

○栁島参事官　我々としても共有された情報の内容を確認しているが、特別なインシデントが起こったことで共有件数が増えているというよりは、重要インフラ事業者の皆様方に、報告をするという意識が少しずつ広がってきているのではないかと感じているところ。先ほどの説明と重複するが、ヒヤリハットは法令等で義務付けられた報告

事項ではないが、そういったものについても報告されていることを見ても、取り組まなければいけない、共有することに意味があるという認識が広がってきているのではないかと期待している。若干季節変動があることについては、例えば、たまたまその時期にＣ＆Ｃサーバーが見つかり、関連する通信を行っている機器の関係者に対しても注意喚起がなされたということもあるようだとも聞いている。個別の具体的な部分については不明な点もあるが、そのようなこともあり、季節変動が起こっていると考えられるのではないかと感じている。

○渡辺会長　危機が高まっていないという意味ではなく、必ずしも直結してはいないという意味であるとの理解でよいか。

○柳島参事官　我々は、脅威が高まっている、攻撃の手法が高度化しているという表現を使うことが多々ある。最近の事例であるワナクライは、海外でかなりの被害が出たケースであった一方で、日本においては、被害が非常に大きかったという状況でもなかったという例を見ても、どういったことが脅威の高まりなのかということを数字で示すことはなかなか難しい。資料の表にある数字だけを見ると、年度ごとに脅威が高まっていると見えてしまう側面もあるが、重要インフラ事業者の対応のレベルが上がっているという面もあり、必ずしも数と脅威の高まりは連動していないのではないかと考えている。

○中尾補佐官　今の質問は、非常に重要だと思う。情報を共有した、情報が上がってきた、ＮＩＳＣから情報を出したということ、情報を共有しなければならないもしくは情報を出さなければいけないという、ある意味ではアライアンスができてきたということは、非常によいことだと思う。一方で、最も重要なのは、その情報を受けた側や出す側が、その情報を分析してどのように活用できているかという点だと考える。その点は、どこかのタイミングで、もう少し深いサーベイをしておかないと、本質が抜けてしまうのではないかと感じている。ヒヤリハットも含めて何件という数字にも意味はあるが、その効果という部分が重要なのだと思う。

加えて、先週、国際連携の一環として、T-CEPTOARを担当しているICT-ISACが、米国政府機関や米国のISACとの意見交換を行った。情報連携に関連して、自動的な情報のフィードをするAISに関することも含め、かなり密で活発な意見交換となった。年次報告において、今後もセプターやセプターカウンシルの活動をしっかりと支援していくと記載しているところであるが、30程度ある米国のISACのほとんどにおいては、ISACの中でいかに情報を共有し、それを分析して活用するかということが、非常に重要なポイントとなっており、その中で、どのような対応をとることが良いのかというベストプラクティスをまとめ、それを関係の研究機関や分析機関と共有し連携しているという状況であった。日本のセプターという組織において、演習を行う、情報を共有するという動きが活発になっていることは、良いことだと感じている。一方で、この意見交換を通じ、米国のISACがベストであるという意味ではないものの、日本の

セプターと米国のISACとの間に温度差を感じた。このとき、National Council of ISACsというミーティングにも参加したが、彼らは一つ一つのISACに対してヒアリングをしながら情報共有を行っていた。

重要インフラの取組の中で、今後、セプターやセプターカウンシルの位置付けもう少し強めていくというメッセージも考えていくべきなのではないだろうかと考えている。もしかしたら、ISAC化ということもあるかもしれないと思い、今後の参考までに申し上げる。

○三角審議官　情報を共有しただけでは意味がないというのはご指摘のとおり。現在、戦略本部で、サイバーセキュリティ戦略の中間レビューという位置付けで、取組の全体を見直し、その中で情報連携を進めていこうとしており、重要インフラにとどまらず、もう少し全体をみていこうと考えている。このコンセプトは、受けた側の行動につながらなければ意味が無いということ。その中で、行動につながる情報は何なのか、そのために必要な仕組みは何なのかということを検討しているところであり、全体を見据えながら考えていきたいと思っている。

○有村委員　私も、中尾補佐官、三角審議官の発言のとおりと考えている。JPCERTは、セプターカウンシル事務局の全面的な支援を行っているが、その中で、セプターカウンシルあるいは日本のISACのそれぞれに、企業と同様に、体力差があるように感じている。それをある程度解消させるためには、例えばインディケーター情報を渡したときにそれが活用できるか否かという点が、具体的な論点になると思う。情報を受け取り、アナリストがそれを解きほぐして自社内に展開しインプリしていくことができる組織もあれば、その手法を否定はしないものの、来た情報をそのままベンダーに任せるしかないという組織もある。そのような点を踏まえれば、アナリストを抱えるなど分析力を持つ組織は、そのような情報共有の仕組みやコミュニティを形成するという方法もあるが、それをできない組織に対しては、自動化を進め、即応的に流し込めるようにするなどの方法が考えられる。例えば、先ほど触れられたAISやSTIX/TAXIIなど。また、内閣府のSIPの中でも、そのようなものをどのように使うことができるか、そのためのフォーマットをどうするべきかと、ICT-ISACを中心に電力ISAC、金融ISACを交えながら、JPCERTやIPAも入って議論しているところ。

政策として反映させていく、さらにそれをもう一歩強目に押し出していくことについては大切なことであるので、議論し、形にしていただきたいと思うが、一方で、議論の最中ではあるが、現実的な部分として、このような具体的な取組を継続しているところではあるということを紹介させていただきたいと思う。

○渡辺会長　いただいた意見は、本年度以降の方向性に関するものと理解するが、本議題は、昨年度の取組の報告に関するものであるので、整理をさせていただき、これを今後の議論に関する重要な論点と位置付け、必ず次の議論にこの論点を展開するということで事務局に引き取っていただくこととしたい。ついては、資料の内容について

了解をいただければ、昨年度の活動報告として資料４－１を決定することとしたいがいかがか。

○一同　異議なし

○渡辺会長　それでは、資料４－１について決定する。

(4) 討議事項

瓜生参事官より資料５について、中島主査より資料６について説明。討議概要は次のとおり。

○渡辺会長　さきほど説明があったとおり、本日の議論を踏まえ、改定原案に反映し、また討議を進めていくこととしているので、可能な限り多くの意見をいただきたいと思っている。

○松田委員　資料５について。ＯＴを含めるという点で非常に良い取組だと感じているが、ＩＴの機密情報や個人情報の保護という機密性を重要視する考え方、ＯＴの可用性に重点を置き、人命や安全面を重要視する考え方、２つの異なるカルチャーをどのようにまとめていこうとしているのかについて教えていただきたい。

○瓜生参事官　ご指摘のとおり、ＯＴは、可用性に重点を置き、さらに、HSE、Health、Safety、Environment とよく言われるが、健康、安全及び環境を重視するという特徴があると認識している。制御システムのマネジメントシステムである CSMS は ISMS をベースとしつつ、そのような点を考慮して作られていることから、CSMS 的なものをうまく取り入れる形で構成していければと思っている。

○野口委員　資料５の２ページについて。ＰＤＣＡの考え方が今回の改定のキーとなると考えているが、この中で、ＰＤＣＡというものをオープンなＰＤＣＡにしていただきたいというのが意見。現在、汎用的に使われているＰＤＣＡであるが、このＰＤＣＡにも、最初に計画したことでクローズしてしまう傾向があるという弱点がある。訓練などでよく見受けられることだが、訓練を実施し、その中で問題が確認されればその問題を改善するというＰＤＣＡが回り始めると、よくなっているようにも見えるが、実はある問題を固定しその問題の深堀りをしているだけとなり、新しい観点を取り入れることのないループになってしまうことがある。言い方を変えると、訓練の改善は、訓練を実施した結果のみでしかチェックされないという問題点等も出てきている。このような意味で、プラン「Ｐ」やチェック「Ｃ」の部分など、どの場所に外部からインプットを追加するかということにこだわりはないが、世の中の状況変化や未経験のリスクに対するマネジメントの結果の参考など、ＰＤＣＡのサイクルに外からの新たなインプットを入れて改善するという仕組みを、ぜひ見せていただきたい。

加えて、同じページの図について。はじめは、ＮＩＳＣの視点という新たな情報が入っており良いと思ったが、改めて考えてみると、この図では、民間の事業者がＮＩＳＣという行政の指示によりＰＤＣＡを回すという形に見え、少し問題があるかもし

れない。今後のことを考えれば、ＮＩＳＣの指示を待つのではなく、事業者自らが社会状況の変化や技術動向を見るという、ＮＩＳＣとは違う方法からの情報を入れるという要素が図の中に必要なのではないか。

さらに、ＰＤＣＡとしては、本来３つのＰＤＣＡが必要だと考えている。資料に記載されているものは「対策系のＰＤＣＡ」であるが、この上位には、その組織の「マネジメントシステムのＰＤＣＡ」というものがあり、さらに社外に視点を移せば、民間のＰＤＣＡを見つめる「行政のＰＤＣＡ」がある。この３つがぐるぐるっと回っていかなければ、社会全体としての改善はうまく機能しない。「対策系のＰＤＣＡ」で回していると、ややもすると現場の問題だと捉えられてしまうことがある。これを経営陣に持ち込むためには、少なくとも「マネジメントシステムのＰＤＣＡ」があることを示さなければならない。また、行政においても、さまざまな規制の在り方を考える際に「行政のＰＤＣＡ」がある。このような構図が必要なのではないかと思っているというのが、ＰＤＣＡに関する意見。

もう一点は、資料５、５ページの２番目の項目について。ここで「利害関係者」という用語を用いているが、「関係者」とするべきだと思う。「ステークホルダー」と「インタレステッド・パーティ」の使い分けで右往左往している状況もあるが、これはもともと、英語を置きかえる中、あたかも２つが並列しているように誤解され、日本語も２つに分かれているだけ。特に情報分野の場合には、「利害関係者」より「関係者」という広い意味合いを持つ表現の方が、状況と合致するのではないか。

○瓜生参事官　２点のポイントがあると考えている。

１つ目は、経営層の関わり方。経営層が広い視点からそれぞれの取組を俯瞰した上でマネジメントしていくことが重要だと考えており、ＰＤＣＡで言えば「Ｐ」に該当するが、指針本編の『「リーダーシップ」の観点』という項目で言及することを検討している。２つ目は、リスクアセスメントの仕方。資料の中で「リスクアセスメント・ガイドライン」という文書にも触れているが、さまざまなリスクに対してどう対応するのかをしっかりと考えてからＰＤＣＡを回していくという動きが必要だと考えており、このようなリスクアセスメントの重要性を伝えていければと思っている。

ＰＤＣＡの本来的な在り方については、まさに経営層の取組が重要であると考えている。「対策のＰＤＣＡ」と「マネジメントシステムのＰＤＣＡ」とは、経営層の関わり方により効果的な形で回すことができるのではないかと期待している。また「行政のＰＤＣＡ」については、現状として至らない点もあるかと思うが、我々としても、事業者側のニーズをよくうかがいながら、事業者が必要としている対策を進めていけるよう、十分にコミュニケーションをとっていきたいと思う。

○渡辺会長　資料５の４ページに新旧対照表があるが、これまで１つの項目としてまとまっていた「Ｃ」と「Ａ」の項目をきちんと分離したこと、また「6.1.1(1)組織及びその状況の理解」や「6.1.1(2)利害関係者のニーズ及び期待の理解」の部分で、「これは

１回行うだけではなく絶えず見直すことが必要である」旨を明記することで、野口委員の懸念が解消される部分もあると思う。ぜひ記載をお願いしたい。

○平田委員　資料５の３ページ、指針改定のポイントについて。今回は、ＯＴを意識した改定だと承知しているが、ポイントの記載事項からは、人材育成や CSIRT に注目しているように見受けられる。事業継続計画やコンティンジェンシープランについてもＯＴを意識した検討を行っていることを踏まえれば、もう少し幅広く項目を加えた方がよいのではないか。

資料５の５ページ、２番目の項目について。「利害関係者のニーズ及び期待の理解」については、ステークホルダーの関係性や依存性などの整理が大切だと考えている。事業者側としても、どこまでどのような範囲で整理したらいいのか悩む部分だと思う。この点について、指針対策編等で具体的な事例を示すなど、考慮いただきたい。

○瓜生参事官　指摘を踏まえ、次回提出する改定原案の中でしっかりと書き込んでいきたい。

○増子委員　指針手引書が統合されるとされている「重要インフラにおける情報セキュリティ確保に係るリスクアセスメント・ガイドライン」とこれまで６回中２回行われた「オリパラ向けリスクアセスメント・ガイドライン」との関係性を教えてほしい。

○柳島参事官　現在、皆様方にお願いしているリスクアセスメントのガイドラインについては、既に公表しているとおり。これは、オリパラをしっかりと実施して問題なく終わらせるという観点から、派生するリスクをピックアップしていただいているところ。これから作成する「重要インフラにおける情報セキュリティ確保に係るリスクアセスメント・ガイドライン」については、その観点だけにとどまらず、事業をしっかりと実施するという観点で、もう少し幅広な目標設定等をしていかなければならなくなると考えており、このような観点で、これまでの手引書にある項目なども反映させつつ、充実させていこうと考えている。

○大高委員　本日の議論の大きなポイントとしては、情報共有とリスクアセスメントに関しＯＴが加わったという点だと感じている。特に、第４次行動計画でＯＴが対象に加わったという点は大きな進展だと思う。

資料６、別紙１の２ページについて。サイバー攻撃リスクの特性の３番目に、「また、インターネットに接続していないクローズド環境で運用される」とあるが、ＯＴの分野では非常に多い環境だと思う。これにより、ＯＴ分野の方は、独自ネットワークしか使っていないので安心だと、リスクを意識していないケースが多いと感じている。そのような意味で、リスクアセスメントの基本であるリスク源あるいはリスクというものをしっかりと認識する姿勢、新たな脅威が次々と発生している現状も踏まえ、そのようなものを拾い出して共有するなど、新たな被害があるということを流通することにより、自分の組織にもそのような被害が起こる可能性があるという認識を持つ、という姿勢の必要性をどこかに盛り込めないか。

○渡辺会長　「クローズドだから安心」ではないということを、より能動的に意識するための指摘であると理解。対応及び対策の考慮事項の欄に、「何とかだから大丈夫ではなく、環境が絶えず変わることも踏まえ、能動的に発見し続ける」という主旨を具体的に記述するよう、事務局にお願いする。

○中尾補佐官　資料６について。サイバー攻撃の特性は挙げれば切りがないと思うが、よくまとまっている。これまでWGを３回行い、今後何回かで右の欄が埋まっていくことと推測するが、その際、右欄のまとめをどのように進める考えか。本資料では、サイバー攻撃の特性をある切り口で表現しているが、対策や対応がかなりオーバーラップするのではないかとの懸念がある。

○瓜生参事官　今後の進め方としては、「対応及び対策の考慮事項」の欄についても具体的な記述を行った上で、指針本編の改正原案と合わせて提示し、次回の専門調査会の場で議論いただくことを想定している。対策の内容が重複するという点については、同じ懸念を抱いているところではあるが、おそらく、重複を恐れずに、今回提示した特性の整理に合わせる形で進めることになろうかと考えている。

○中尾補佐官　例えば、「攻撃手口の高度化」については、検知を困難にさせたり、アンチウィルスの検知を外したりと、さまざまな手法が使われると思う。このように、ひとつのサイバー攻撃の特性とその対策は、おそらくOne to Oneの関係にはならないだろうと考える。「このような特性を加味してこのような対応や対策を考えてほしい」というような１つの提言が出されるイメージだとわかりやすいと思うので、検討いただきたい。

○渡辺会長　WGに参加いただいた金融分野の和田委員からコメントをいただきたい。

○和田委員　金融分野は、資料６の例で言えば例１に該当するもの。今回のWGはＯＴの特性を踏まえるとの観点が大きかったことから、例１に該当する事例を紹介しつつ、例２の考え方などを勉強させていただいたという位置付けとなった。指針改定においては、ＯＴの観点をうまく取り入れることができ、非常に有効な指針になるであろうと感じている。

○渡辺会長　金融分野では、既にコンティンジェンシープランの策定の取り決めが形になっており、冒頭にプレゼンしていただいた。WGにおいては、いわゆる製造業だけを制御と言うのではなく、ある意味では金融もひとつの制御システムだという話をしたり、分野は違えどもＯＴとして触れる部分は、ここでしっかりと標準化していくというような議論もあったと記憶している。

○手塚委員　資料６のサイバー攻撃リスクの特性について。ＩＴとＯＴに分類することは、ひとつの考え方としてあると思うが、ネットワーク、システム、業務という縦方向でのサイバー攻撃に対する対処の仕方について、どのように考えているのか教えてほしい。

○瓜生参事官　ネットワーク、システム、業務という攻撃の対象によって、攻撃リスク

の特性が変わってくるのではないかという主旨か。

○手塚委員　攻撃には、ネットワーク型、システム型、標的型など、いろいろなパターンがあると思う。これに対し、受ける側は、それらを整理して対応方法を考えなければならないと考えるが、整理学の観点からいかがか。

○瓜生参事官　今回のとりまとめは、コンティンジェンシープランや事業継続計画の作成に当たって必要となるサイバー攻撃リスクの特性の視点と考えている。事象が発生した際には、コンティンジェンシープランに基づいて、業務分野がどうなっているか、ネットワークがどうなっているかと、それぞれの箇所での対応を行うことになる。これを踏まえ、それぞれの箇所の対策や対応を検討するに当たり、このような特性を考慮したときに、自分がどのような状態になるのかを考え、改めて、それぞれの部署がコンティンジェンシープランを作り直していくという形を想定しており、そのような使い方がなされることを期待している。

○手塚委員　考え方は理解。ぜひ、そのような関係性を整理しながら考えてほしい。

○平田委員　WG に参加していたので、少し補足したい。WG で、特性を踏まえた対策についてどのような方向性とするべきかという議論があったが、その中では、ネットワーク、システム、業務のそれぞれがどのような状態になっているのかをしっかりと把握することが重要であるという意見があったので、この点は反映されるものと考えている。

○渡辺会長　WG に参加いただいた電力分野の阿部委員からコメントをいただきたい。WG では、能動的に送電をとめなければいけないという事態があるかもしれないという議論もあったと記憶している。

○阿部委員　電力分野としては、サイバー攻撃に限ったものではなく、長年かけて安全面の体制を整えてきたと認識している。サイバーについて言えば、一昔前の状況として、さきほど指摘があったような、制御と情報システムは分離しているから大丈夫だという考えも一部にはあったと思う。現在は、電力自由化の進展もあり外部接続の要因も増えているとの認識のもとリスクアセスメントを行っている。今回、改めてサイバー攻撃リスクの特性を整理することとなったが、これにより、今まで気付かなかった脅威を認識することができ、有用性を感じている。これは、電力分野だけではない他分野の考えも参考にしていくことで、リスクの捉え方やこれから整理する考慮事項を検討する上で、有効な気付きにつながるのではないかと考えている。WG は今後も継続すると思うので、これまで認識されてきた脅威に加え、そのような点も考慮事項に反映できればと考えている。

○渡辺会長　電力 ISAC も立ち上がりつつあると承知しているが、そのような論点が全面に入ってくるという理解でよろしいか。

○阿部委員　電力 ISAC については、旧一般電気事業者 10 社をベースとしながら、新電力事業者も加わっているので、さまざまな知見の融合がなされていくだろうと考え

ている。電力の安定供給の面から、送配電網なども扱っている事業者と発電事業を主とする新電力など、事業者によって運転設備の範囲や特性などに違いがあるので、情報共有の範囲は整理しながらも、お互いの気付きという部分は大事にしていきたいと考えている。

○中尾補佐官　資料５に関連してＰＤＣＡについて。ISMS に長年携わってきて、ＰＤＣＡは非常に重要なプロセスモデルだと感じており、そこにＯＴを含めて整理する取組は非常に重要だと思う。しかしながら、ご案内のとおり、ＰＤＣＡは基本的にマネジメントのためのプロセスモデルであり、その中で、具体的な対策を検討するに当たり、対策の中でも小さなＰＤＣＡが回っているもの。一方、ＯＴについては、ＰＤＣＡに加え、もう一つのモデルがよく議論されている。ご案内かと思うが、まずは状況をモニター「観測（Observe)」し、その後、Estimate of situation と言って、現状を「認識（Orient)」する。把握した結果として具体的にどのような方向性で対応するかを検討して「決定（Decide)」し、実際の「行動（Act)」につなげる。この Act には、今後の対策（Productive plan）を含んでいる。特に、ＯＴのように可用性（Availability）を重視する分野では、このようなプロセスモデルが考えられていると認識している。CSMS は、そこまで具体的に踏み込んでいない印象があるが、ＰＤＣＡのプロセスモデルと関連したこのような考え方は、重要インフラの中に浸透している状況か。

○野口委員　ご指摘のとおり、情報セキュリティの問題はいろいろなものの進展が早い。ＰＤＣＡは、１年間をかけてゆっくり行うことが多く、動的な活動であるものの、技術の変化と比較するとスタティックなイメージがあるが、計画はこうだったがモニタリングで状況を把握したらすぐにぐるぐると回すという、かなりスピーディーなＰＤＣＡが必要であるという点は、情報セキュリティならではの観点であり、入れておかなければならないものであると強く思う。

本日、各委員から提示された意見について、思い至った点をお伝えしたい。

攻撃リスクの特性とその対策の一対一の対応問題について。WG の中では、対策を考えてリスク特性と線でつなぐことを試みたが、その中である課題に対する対策は他のものにも有効だということを確認している。これをどのように処理するかについては、現在、事務局が悩みながら取り組んでいる状況である。しかし、問題点に対して対策を示すという方法で対策を蓄積していくと、対策の塊になってしまう可能性がある。情報セキュリティの可用性までを含めた場合には、それぞれの問題と対策を一対一で対応させるのではなく、対応の集合、総合的な対策が、本当にこのシステムにとって実現可能か、有効かを確認するステップを１回入れておく必要がある。さもないと、問題を発見するたびにひとつずつ加わって、対策のお化けになってしまう。このような視点からも、この特性と対策の対応関係は、改めて整理が必要であると感じた次第。

ネットワークの問題について。今まで、このような問題を考える際には、原因系を

発生させる箇所の問題として捉える傾向があるが、ネットワークでつながっている場合、その考え方の延長線上で考えることが本当に適切なのだろうか。例えば、ネットワークを通信会社の持っている１つのシステムとして捉えることが適切なのかということについては、しっかり考えなければならないと思う。ネットワークには、個々の問題のポイントの集合体では論じることができない問題があるように感じているので、手塚委員の指摘のとおり、少し別の切り口で入れておかなければならないと感じた。私も賛同するので、そのような面について少し深めてほしい。

○瓜生参事官　対応したい。

○若林委員　資料６について。サイバー攻撃リスクの特性については、非常によくまとまっている。システムの評価、リスク評価、システム構築などにおいても、これらの特性を踏まえることは重要だと思うが、これをそのようなものにも活用していく考えはあるか。

○瓜生参事官　ぜひ利用していただきたいと考えている。

○三角審議官　この資料は、コンティンジェンシープランを作成する際に活用いただくことを念頭に作成したものではあるが、ＯＴも含め考慮が必要な特性を列挙しており、コンティンジェンシープランに基づく対応の準備として、システムであらかじめ考慮されていることで、実際の対応が容易になると考える。今後、本資料の使い方を具体化する際、そのような点についても考え方を明らかにすることは望ましいと思う。

○渡辺会長　攻撃特性を踏まえた対策は、コンティンジェンシープランも含め対症療法的なものだけでは限界があり、グランドデザインとして、システム更新のタイミングでこのような要素を入れることが重要。そのような意味で、コンティンジェンシープラン策定のためというだけではなく、システム設計・開発などにも活用するという主旨をどこかに加えてほしい。

○大高委員　資料６について。サイバーセキュリティという用語が使われる状況になってから非常に気になっていた部分であるが、重要インフラ事業者としては、可用性を担保するため、物理的な部分への配慮が重要な要素のひとつであると考えている。例えば、通信の線を切られるという事象は、対象とするのか否か。当たり前の前提と捉えられていることだとしても、そのような視点については、どこかに残しておく必要があると思う。その前提の中で、サイバーセキュリティという大きな脅威に対して取り組んでいくということを、姿勢としてどこかに記載してほしいと感じている。

○瓜生参事官　今回のとりまとめは、これまでのコンティンジェンシープランや事業継続計画は、自然災害やパンデミックなど、これまで想定された物理対策のような観点で作られている中、現時点では欠けていると思われるサイバー攻撃リスクの特性をさらに追加していただくという趣旨を込めて進めてきた。ご指摘のとおり、そういう物理的対策だけでなくサイバーも含め、重要インフラ事業者として全体をどうするかということを検討し、改めてコンティンジェンシープラン等を作成することなどに資す

るものとして、指針の文書を作成する考え。ご指摘の点については、指針本編の前文に記載する方向で検討させていただきたい。

○大高委員　オリパラのリスクアセスメントを行う中では、サイバーもあるが、特に物理的な対応という部分が目に付きやすい。そのような場面で、ＮＩＳＣはどちらを捉えているのかと疑問視されることがないよう、基本的なところは押さえた上で、ということを踏まえるようお願いしたい。

○有村委員　私も WG に参加していたので、個人的な意見も含め補足をしたい。

資料６別紙１の例２のモデルは、いわゆる基本プロセス制御システムが正常に運転しているところから、何らかの原因で逸脱を始め、アラームが発生し、運転員が動かし始め、コントロールできないと、SIS、緊急安全装置が働く。それがさらに外れた場合には、重大インシデントあるいはシビアアクシデントにつながっていくという、いわゆる制御モデルの時間推移をベースとしている。これは、従来からあるシステムエンジニアリングあるいは信頼性工学に基づいたハードウェア故障をベースにした発想で作られたハザードシナリオなので、サイバーの要因というのは入っていない。本取組の基本的考え方は、ＩＴとＯＴの接点を考えるのであれば、この時間推移のモデル部分にサイバーの要素を上手に、納得あるように入れる必要があるのではないかという問題意識がベースになっていると思っている。そのような意味では、旧来のいわゆるハザードシナリオの中には物理的な部分が既に入っており、その中に、誤操作や誤作動を発生させる要因として、サイバー攻撃がプラスアルファで加わったとき、ハザードシナリオが最悪な状態に到達するのか否か、そのようなことを考えてほしいということが、ＩＴからＯＴへのメッセージだと感じている。

このように、ＯＴのこれまで考えていたハザードシナリオの中に、さらにＩＴのリスクや攻撃を加えた場合に、それが破綻しないということが確認できればよいと考えれば、先ほどのサイバー攻撃リスクの特性はシステム設計などに活用できるのではとのご意見も、重要インフラ事業者側による応用として考えられることから、積極的な活用を期待したい。

○渡辺会長　今後、事務局において、本日いただいたインプットを検討して安全基準等策定指針の改定原案を作成し、次回の専門調査会において提示させていただくこととしたい。そこで改めて、皆様に具体的な討議をお願いしたい。

本日の議論はここまでとするが、加えてコメントがある場合には、７月３日までに事務局まで提示願いたい。

(5) その他

瓜生参事官より「重要インフラサービス障害等に係る深刻度判定基準（素案)」（資料非公表）について説明。

○瓜生参事官　本件について内部で議論を重ねているところであるが、実態がわからな

い中での内部の議論に限界を感じており、今後、徐々にではあるが、各重要インフラ分野の方々から、基本的なシステムの構成やコンティンジェンシープランによる対処を行う際の発動の目安のような実態などについて、少し勉強させていただきたいと考えている。ついては、重要インフラ所管省庁、専門調査会の委員の方々にご協力いただき、お時間をとっていただければと思っているので、よろしくお願いしたい。

今後は、その結果も踏まえ、秋ごろを目処にＮＩＳＣ素案を提示させていただき、皆様方の議論をお願いしたいと考えている。

○柳島参事官　今後の予定について。本日の議事概要については、事務局にて作成後、委員の皆様に確認いただいた上で公表させていただく。次回、第12回会合の開催については、本日議論いただいた結果を踏まえて作成した、安全基準等策定指針の改定原案を提示して議論いただきたいと考えている。時期としては秋頃と考えているが、詳細については、別途連絡をさせていただきたい。

(6) 閉会

中島センター長から挨拶。

○中島センター長　本日は、遅れての参加となり大変申し訳なく感じているところ、委員の皆様におかれては、お忙しい中参集いただき感謝申し上げたい。

ご案内のとおり、４月18日のサイバーセキュリティ戦略本部において、「重要インフラの情報セキュリティ対策に係る第４次行動計画」を決定した。まさに、この場で議論いただいたものであるが、重要インフラサービスを安全かつ持続的に提供できるということを主眼に、経営層に積極的に関与していただき、機能保証という考え方に立ち、各種の取組を推進していくということが明確にされたところ。

少し感想めいた話となるが、従来、サイバーセキュリティは、情報システムを中核とする概念として捉えられ、比較的、閉じた議論となっていたかと思う。しかしながら、サービス全体の観点から考えることは、非常に重要な視点であると考えており、先ほどサイバーと物理という話もあったが、重要インフラに限らず、例えばオリンピックについても、究極として、我々が何をやらなければならないのかという観点から、改めて、あらゆる分野でサイバーを見直すという議論が、サイバーセキュリティセンターで行われている。例えば、研究開発や人材育成などの全てを、そのような観点で、ある種、抽象度をひとつ上げて、ないしは目的のチェーンの階層を１つ上の段階から考えようと議論しているところ。

背景を考えると、例えば、ICT技術自身が社会制度や我々の行動を変えていく中で、これまでの情報システムの捉え方のまま、既存のモデルを導入するだけでは、既にもたなくなっているのではないかと感じている。これからIoTが拡散していく、自分の子供の行動形態が我々の時代と大きく異なることからもわかるように、社会が急速に変わっていく中で、これをどのように考えていくのか。ビジネス的に見れば、ひとつの

チャンスなのだろうと思うが、これは、同時にチャレンジでもあると考える。攻撃側についても、これまでおよそ考えられなかったような攻撃も出てくる。先ほどの議論にもあったが、新たな課題として、ＩＴとＯＴとの関係、物理とサイバーとの関係といった、少々面倒な課題も出てくる。ただこれは、知的に非常にチャレンジングな状況なので、喜びを感じながら取り組まれている方も多いのではないかとも思うが、そのような意味で、重要インフラにおける取組は、パラダイムが変わり、新たなステージに入ったのではないかと考えているところ。このようなことを、この場で私も勉強させていただいており、委員の皆様のこれまでの議論に本当に感謝申し上げたい。

本日、第４次行動計画の策定に伴う安全基準等策定指針の改定方針、重要インフラサービス障害に係る対処態勢の検討状況について議論いただいたところであるが、本日の議論を踏まえ、年度内を目処に指針の改定に取り組んでまいりたいと考えている。また、深刻度判断基準は、今後さまざまな知見をいただきながら、策定作業を進めていきたいと考えているので、引き続きよろしくお願いしたい。

○渡辺会長　最後になるが、ご多忙の中、WGの主査を務め、本日参加いただいた中島主査に改めて感謝申し上げたい。これにて、第11回「重要インフラ専門調査会」を閉会する。

以　上