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８回会合　議事概要

１　日時

平成 28 年 9 月 30 日（金）15 時～17 時

２　場所

経済産業省別館３階　３１２号会議室

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）
伊澤　雅和　委員　（一般社団法人日本ケーブルテレビ連盟）
稲垣　隆一　委員　（稲垣隆一法律事務所）
大高　利夫　委員　（神奈川県藤沢市）
大林　厚臣　委員　（慶應義塾大学　大学院経営管理研究科）
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）
門野　健治　委員　（株式会社みずほフィナンシャルグループ）
真田　博規　委員　（住友生命保険相互会社）
神保　謙　　委員　（慶應義塾大学　総合政策学部）
鈴木　栄一　委員　（一般社団法人日本損害保険協会）
中尾　康二　委員　（KDDI 株式会社 兼 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）
西村　敏信　委員　（公益財団法人金融情報システムセンター）
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）
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　（国立大学法人名古屋工業大学　大学院工学研究科）
渡辺　睦　　委員　（石油連盟）

（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
山内　智生　内閣参事官
阿蘇　隆之　内閣参事官
狩俣　篤志　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
伊貝　耕　　内閣企画官

（オブザーバー）

金融庁総務企画局政策課
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情報政策室
総務省地域力創造グループ地域情報政策室
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・食品安全部水道課水道計画指導室
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情報セキュリティ対策室
原子力規制庁長官官房総務課情報システム室
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

４　議事概要

(1) 開会（挨拶）

中島センター長から挨拶。

〇中島センター長　７月の人事異動で内閣サイバーセキュリティセンター長を拝命。今後ともよろしくお願いしたい。

近年、民間企業や政府機関に対するサイバー攻撃は、ますます巧妙化、深刻化して

いると言われており、我々もそう認識している。

私は、2000年ころに関係職務に従事しており、改めて振り返えると、確かにサイバー攻撃の態様が変化し巧妙化してきている。当時は愉快犯が多かったが、それが国家レベルの話になってきており、そういう意味で、社会基盤としての情報通信技術が急速に広がっていることで、インパクトが非常に大きくなっているということが言えると思う。また同時に、当時と比べ、防御技術が非常に進化してきているが、それを適用できるところとできないところという格差も広がってきており、その脆弱性、弱いところを突いてくるという動きもあるということで、総体として、脅威がそのまま直線的に増大しているというイメージではなく、様々な意味でそのパラダイム自身が変わってきているのではないかと考えている。

現在、サイバー攻撃への対処は、国の安全保障上、危機管理上も重要性を増してきており、またビジネスに与えるインパクトも大きなものになってきていると思う。

先般、リオでオリンピック・パラリンピックの大会が開かれたが、御案内のとおり、サイバー攻撃への対処が、大会運営上のセキュリティに関する大きな課題となった。結果的に、競技の進行に大きな支障となる事案は発生しなかったが、我々もリエゾンを送り、その背後にある関係者による事前準備や期間中の対策について拝見した。このような大規模なイベントに際しては、イベントそのものの安全、また大会を支えるサービス、これが滞りなく提供されることが目標になるが、その際、特に情報通信技術の応用を中核とした新たなサービスが急速に展開されていることを考慮しなければならない。例えばロンドンからリオ、次に東京だが、その脆弱性への備えを想像力を持って講じていく必要があり、言い換えれば、未来社会の脅威への対応という側面があるのではないかと思う。そういう意味で、東京オリンピック・パラリンピックへの対応というのは、将来に向けた非常に重要な一里塚になると考えているが、視線をさらに先に伸ばすと、ICT技術、情報通信技術の急速な発展、それからその応用により、重要インフラを取り巻く環境、社会的なパラメーターと言ってもいいかと思うが、そういうものが今後大きく変化していくということは必然であり、また新たな脅威が予測されるということになる。これに的確に対応する必要がある状況の中、まさに本日参加いただいている各分野の皆様、関係の各省庁、有識者の先生方から継続的に貴重なご意見を伺いながら、それぞれがこの分野における平等な１プレイヤーとして、ともに取組を深化させてまいりたいと考えている。

このような背景を踏まえ、本年３月にまとめられた「重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ」に従い、各省庁において、見直しに向けた検討、様々な取組を進めていただいているところであるが、本日は、その状況について、簡単に報告をいただく予定としている。本日は、そのような状況も踏まえ、行動計画見直しのための骨子案についてご議論願いたい。

今回の見直しに当たっては、これまでいただいたご意見を踏まえ、先導的な取組の

推進、情報共有体制の強化、リスクマネジメントを踏まえた対処態勢の整備といった３点を重点項目として取りまとめたところ。委員の皆様方には、ぜひとも活発なご議論をお願いいたしたい。

渡辺会長から挨拶。

○渡辺会長　第７回会合では、行動計画の見直しに関し、検討体制、スケジュール、進め方について、議論、確認をいただいた。

今回は、前回の議論を踏まえたものとして骨子案が提示されており、後半の討議でご議論いただくこととしている。

センター長からの挨拶にもあったとおり、サイバー攻撃はますます巧妙化している。これは、重要インフラ事業者、また所管省庁においても、個別、単独で乗り切ることができる状態ではなくなったということ。米国でも大きなIT企業による５億件の個人情報漏えいがあった。国内においても、身の代金型、要求型のサイバー攻撃など、多様化、複雑化してきている状況もあり、国内企業の被害は、件数ベースで前同期比９倍ぐらいになっているという報道もある。このような環境は、サイバー攻撃が重要インフラ事業者のサービス障害に直結しつつあるという状況が、既にそこにきているということを表しているのだと思う。

そのような意味では、本日ご参加いただいている皆様方も含めて、滞りなく社会あるいは国民から求められるサービスを提供していくため、どのようなフレームワークで協力し、どのような取組で進めなければいけないのか、その役割と責任分担はどうなるのかということを、引き続き、より具体的に進めていかなければいけないタイミングに来たと思っている。

(2) 報告事項

【関係省庁の取組状況について】

○金融庁　金融庁では、金融分野のサイバーセキュリティ強化に関し、金融機関の取組が実効性あるものとなるよう、金融機関との個別の対応を通じたセキュリティ管理体制の実態把握を引き続き進めているところ。

また、金融庁として初めての金融業界横断的な演習を、今年度に実施する予定としているところ。来月実施予定のこの演習は、民間コンサル等が提供する演習を利用しにくい中小金融機関にも多数参加していただく予定であるが、参加金融機関において、サイバー攻撃に対する現時点での対応態勢や手順の有効性を確認していただき、改善に結びつける機会となることを狙ったもの。この演習を通じて、金融業界全体のセキュリティレベルの底上げを図っていきたいと考えている。

○厚生労働省　医療分野について、現在、安全ガイドラインの改定を行っているところ。水道分野については、今後もサイバーセキュリティ対策を行っていくということで、

ガイドラインの作成を検討していくということになっている。

○経済産業省　重要インフラに関しては、電力分野について、これまでガイドラインの中で規定していた内容を、今般９月に、電気事業法に基づく安全基準に組み込み、電気事業法に関する電力会社に対するサイバーセキュリティ対策をしっかりと実装するという取組を進めたところ。重要インフラの防衛力を高めることは重要な課題だと思っており、これに向けて取り組んでまいる所存。さらに、このような取組を他分野にも広げていきたい。

○国土交通省　２点報告する。事務局の移行として、本年７月15日付で、航空分野の事務局を当省航空局から定期航空協会に、鉄道分野の事務局を当省鉄道局から一般社団法人日本鉄道電気技術協会に移行していただいている。これにより、鉄道分野及び航空分野それぞれのセプターについて、準民間の集まりという形になったところ。また、航空分野において、スカイマークが新たにセプターに参加することとなった。航空分野の事業者が１社増。

次は参考であるが、皆様御案内のJTB個人情報漏えい事案を踏まえ、観光業界における情報共有会議というものについて観光庁を中心に取り組んでおり、このような重要インフラでない分野においても、情報共有の大切さということで取組を行っているところ。

○警察庁　資料３に沿って説明。

○総務省　資料２に沿って説明。

【2020 年東京オリンピック・パラリンピック競技大会に向けたリスクアセスメントの取組について】

○伊貝企画官　資料４に沿って説明。

【JPCERT/CCからの情報提供】

○有村委員　資料５に沿って説明。

質疑応答は次のとおり。

○野口委員　２点について伺いたい。１点は、オリパラに向けたリスクマネジメントの件。拝見したところ大変良くできており、分かりやすくまとまっていると思うが、リスク特定の概念について質問させていただきたい。細かいことのようであるが、大事な部分だと思っている。資料４参考資料の「機能保証のためのリスクアセスメント・ガイドライン」本文18頁には、リスクの特定について「業務の阻害につながる事象の結果、その事象を生じ得る事象及びリスク源を特定」と書いてあるが、その解釈について少し説明が必要だと思っている。資料には、今回のリスク特定は、順番に、何が起こるか、何がリスクか、しっかりと考えた後で、リスクを分析するものであるというステップが明示されており、この考え方は全く問題ない。しかしながら、この資料のように、リスクとリスク源を同時にまとめてここに書いてしまうと、こういう情報

漏えいはUSBによるものだと、経験的に思い込んでしまう怖さがある。リスクとリスク源というのは、ややもするとペアであると誤解されてしまうので、むしろリスク分析の中では、こういうリスクを生み出すリスク源にはこれこれといった様々なものがある、という多様性をしっかり押さえて込んでおくことが重要であるということを、少し丁寧に教えていただきたいと要望する。

２点目は、先ほど（「JPCERT/CCからの情報提供」において）話があったインシデントという言葉。原子力分野では、重大な事故をアクシデント、小さなものをインシデントと使う傾向があるが、基本的にインシデントという言葉は、事の重大さの影響とは無関係であると理解している。本来、インシデントというのは、何かが起きているという状況のみを意味する。そういうわけで、インシデントマネジメントにおいては、必ず最初に、インシデントがどの程度重要かということを見極める行為が記載される。ところが日本は、危機管理という教え方をするので、起きている事象が小さい事象なのか、危機なのかということは、あたかも分かっているというところからマネジメントをスタートするという誤った傾向がある。マネジメントにおいては、その状況がどの程度重要かということを見極める技術が重要なのだ、ということをしっかりと教えるためにも、インシデントというものの意味合いをしっかりと共有するべきではないかと思う。これは意見として。

○伊貝企画官　オリパラ関連のリスクアセスメントの手順については、本日は通り一遍の説明となったが、ご指摘のリスク源とリスクの違いやその間のステップについては、丁寧に説明をしてきている。また、今後、問合せの対応等々があろうかと思うので、その際にも丁寧に説明してまいりたい。

○中尾委員　私としては、提示されたオリパラのリスクアセスメントのフレームは、一般的なリスクアセスメントと同じで、特別なリスクアセスメントには見えない。インシデントやインパクトアセスメントという、様々な言葉の明確な整備が必要かもしれないが、どういう観点から「オリパラに向けた」という形容詞が使われているのか、どこが変わっているのか、考えをご説明いただきたい。

○伊貝企画官　資料４の３頁左側で若干説明しているが、リスク評価の対象となる資産を洗い出す段階が最も重要な部分だと考えている。やや具体的過ぎる例となるが、例えば、鉄道事業においては、会場近くの路線などの直接オリパラに影響するサービスと、そうではないサービスがあり、最初にそれらを振り分けるということを手順において記載している。それ以降のいわゆるリスク評価のステップに関しては、国際標準などを基に作成しているので、標準的な手続に近いと思っている。サービスの洗い出しのほかには、オリパラの期間はやや特異にリスクが高まることなどを踏まえた脅威の置き方もオリパラ特有の部分かと思われる。また、リスク評価の指標についても、例えば、長くて２か月ぐらいの期間を評価するに当たり、数年に１回のリスクと１年に１回のリスクに差はないであろうなどということも考慮していただくこととして

いる。これらを総合的に捉え「オリパラに向けた」としているところ。

○中尾委員　資産というより、サービスをどう特定していき、その起こりやすさをどの程度の頻度でオリパラ用に考えていくかという部分が、インパクト分析を行う際に大きく違うという理解でよろしいか。

○伊貝企画官　貴意のとおり。

○稲垣委員　各省庁の取組状況の報告を受け、大変頼もしく思った。また、NISCの資料に「機能保証のための」という概念が使われおり、先ほどセンター長がおっしゃったパラダイムの変化を明確に反映するものとして、非常に前進したという印象。

その上で質問したいが、各省庁の今回の報告で際立っていたのは、情報共有と連携という言葉であるが、それぞれがこれを行おうとするときの制度的な基盤、法、人材、能力などについて不安はなかったか、やりにくいところはなかったか、あるいは、十分やりやすくなっているか、ということを伺いたい。それぞれの省庁がこれを実行する際、自らではなく、対象とする事業者を動かすことになる。事業法で進めるにしても、監査、報告徴収、指導など、共通の様々な枠組みを使うことになると思うが、本当に十分に円滑な情報収集ができるのかということについて、私が関わっている分野について考えてみても、私自身は不安を覚えている。金もない、人もいない、報告を受けても分析ができない。情報を出す側の立場に立つと、最も苦労するのは、出していいのかどうかを判断する法的な基準がないこと。出す側は、人から情報をもらってくる。その情報には、必ず守秘契約や目的拘束がついてくる。個人情報などは、行政目的であれば明確に許容されるが、例えばそれぞれの省庁がサイバーセキュリティ対策を急ぐんだ、オリパラだ、だから情報共有をするんだ、情報を出してくれ、と言ったときに、現実には協力するという動きがあるが、事業者側は、例えば弁護士に聞いても了解を得られるのだろうか。サイバーセキュリティ基本法には、法務分野における協力も入っている。法テラスという概念に入っているのだが、私としては、非常にやりにくそうだという印象を受けている。予算をとって様々な取組を行うことは頼もしいが、各省庁は不安を抱えてはいないのか。

もう一つの質問は、情報共有で得た情報の使い道について。何に役立てるのかについてのコンセンサスがとれているのか。例えば、オリパラやナショナルセキュリティ、機能保証という抽象的なものはあるのだと思う。しかし、もっと具体的に言うと、警察庁の報告を拝見し本当に頑張ってくれていると感じているが、例えば、実際に事案が起きて対処し、改善のための情報提供、指導をしているという一方、不正アクセスや新種のマルウェアを把握したとき、これに対策してほしいと言うだけでは足りない。それを活かすのは、その対策ができるベンダー、そのベンダーが採用する技術、機器、システム、その製造や規格に活かすことだと考える。そこまでやらないと、言いっ放し、受けっ放しで、ぶん投げて終わりということになり、一生懸命努力したにも関わらず、情報を活かすことができない。やはり、そうした目的のコンセンサスが必要な

のだと思う。NISCに出すというコンセンサスでは駄目。日本のセキュアな環境づくり、技術、さらに安倍戦略との関係で言えば、それを国際戦略の中で売れる日本にするということ。日本は安全だ、あるいは日本のものを買えばそういう情報付きで良いものが手に入る、そのようなことがサイバーセキュリティの課題としてあると思う。この、現実に活かすために情報を収集して連携していくという目標の共通性は存在するか。

○中島センター長　先生ご指摘のとおり、このようなコンセンサスがとれていないというのは、日本だけの状況ではなく、米国やEUについても同様であると思う。ご案内のとおり、米国ではどこまで匿名化するかの議論を行っているところであり、EUではどのように義務づけするかの議論を行っている。我々としても、そのようなことについて、今まさに議論をしているところ。背景にある大きな物の考え方を申し上げれば、これまでは、サイバー攻撃なるものがある種、散発的にストラテジックに行われてきており、その情報を上手く手繰っていくことで対応してきたが、現在は、それらを総体としてどう捉えるかというように、大きく哲学が変わってきているように感じている。その中で、例えば個人情報保護の観点も含め、サイバーセキュリティに関する情報をカテゴライズしながら、日本だけでなくグローバルに考えていかなければならないだろうと考えている。個人的には、ある種、限定的なものにならざるを得ないと思っているが、我々としては、要素をどのように抽出し、その使い道も含め、制度設計をまずどうしていくかということを、今まさに、議論しているところ。今後とも、ぜひご指導のほどをお願いしたい。

○渡辺会長　稲垣委員指摘の内容については、行動計画見直しの重点に情報共有体制の強化という項目もあり、重要なポイントであるので、後半の討議においても議論することとしたい。

(3) 討議事項

【行動計画見直しの骨子案について】

事務局から資料６－１に沿って説明。質疑応答は次のとおり。

○野口委員　大きな意見としては、見直しのポイント、方向性に賛成。大変よくポイントをつかんでいると思う。その上で、２点考慮していただきたいことがある。

１点目は、企業でいう一般社員、国でいう国民に対する位置づけの問題。情報セキュリティを見る仕組みとして、経営者というものを強く打ち出したことは大変すばらしいと思うが、もう一つ、まだ手がつけられていないものがあり、それが一般社員と国民。会社の一般社員は、情報システムについて、あれやるな、これやるなと言われる中で、嫌々ながら協力しているというイメージがある。国民に関しては、資料に記載のとおり、国民というものは不安を払拭される位置づけである、という形となっている。政府としては、情報システム社会においては、情報機器を使う全ての人間がセキュリティの主役である、というメッセージをそろそろ出さなければいけないのでは

ないか。国民が何かの踏み台に使われるということ、社員のちょっとした気の緩みや乱暴な使い方が、せっかくの制度を壊すということもある。経営者と情報システムの人間が一生懸命やっていることに、社員は協力するということではなく、社員自体が主役であり、国民一人一人の注意が国のセキュリティを守るために大事なことなのだ、というメッセージは、そろそろ打ち出していくべきなのではないか。

２点目は、資料２頁目の重要インフラ事業者の先導的取組の推進について。この考え方は、モデルをつくることにもなり、企業の体力や現状の先進性を踏まえれば、このようなレベル分けをして進めていくということには賛成。ただ、情報システムというものの性格を考えれば、機能の観点から見ると、取組を行う事業者だけが頑張ったとしても、それにつながる別の組織が弱ければ、結局機能として使いものにならないということが考えられる。事業者のモデルケースとしては良いが、これに追加して、例えば重要インフラ事業者でないところでも、重要インフラのこの機能に関するこの事項だけは先端的にやるべきだと、機能を追求するためには大手だけがやっても駄目なんだというメッセージは、どこかに入れておく必要がある。大手ではないから、あるいは、重要なインフラ機能につながっている部分が少ないから、うちはこのレベルで良いと思われることがないよう、会社の役割・規模の観点と、機能として重要なものに関わっているかの観点、２つの観点で網掛けを行うべきであると考える。ご配慮いただければ幸い。

○渡辺会長　１番目は、エンドユーザーも参加主体であるという意識醸成をするべきとの意見、２番目は、例えば金融で言えば、主要都市銀行のみならず地銀や信金も関係する決済機能などのように、機能別に考えていくべきという意見、という理解でよいか。

○野口委員　それに加え、例えば、銀行に機器を納入するレベルでもやらなければならないことがある。機能として、重要なインフラ機能を維持するために、自分がどう関係しているのかを考え、そこだけは必ず強くする、というメッセージがどこかに必要なのではないかと思う。

○柳島参事官　サイバーセキュリティ基本法においては、いわゆる重要社会基盤事業者や国だけではなく、その他を含めてみんなで頑張ろうということが、理念として既に書かれている。しかしながら、企業の一般社員もしくは国民一人一人が、自分が主役であるとの思いに至るまでには、まだ時間がかかるのではないかと考えるところでもある。行動計画の中で記載することについては多少議論があるかと思うが、我々としては、そのような取組についても実施していきたいと考えているところ。

また、先導的な企業だけではなく、機能としてその他へ広げていくということは、我々も検討を行っており、今回、重要インフラ事業者以外についても、まずは情報共有の仲間に入ろうということを掲げている。将来的には、そのような事業者も取組を進め、情報を受けるだけではなく、障害対応、リスク評価、情報提供、発信も行う、

となることが望ましいが、今回は、まずは仲間になってもらうためのハードルをなるべく下げたいとの思いがある。

○稲垣委員　NISC設立以前になるが、セキュリティ文化に関する分科会において、OECDがセキュリティカルチャーという概念を打ち出し、その中で、今、野口委員がおっしゃったことが全部言われており、注目された。サイバーセキュリティ基本法を作る際には、それが当然の前提になっていることから、不明確だとの指摘があるのであれば、明確になるように記述するべきだと思う。

次に、我々にとって最も大事なサイバーセキュリティという概念を、今回、少し整理してもらいたい。整理する対象としては、IT障害、重要インフラ防護、サイバーセキュリティという概念。サイバーセキュリティの概念における中核は機能保証。機能保証、IT障害、重要インフラ防護、この概念が、この会議の発展段階の中で変わってきている。日本全体においても同様。今、内閣がセキュリティをどのように考えているのかと言えば、重要インフラに限らず、強い日本、すばらしい日本、安心して人々が暮らせる日本、そして世界的に評価される日本、この要素としてのセキュリティという捉え方なのだと思う。外交などを見てもそのように思われる。これを踏まえれば、我々が取り組む対象は、重要インフラの機能保証ではないか。これまでは、IT障害から重要インフラを守るということが取組の対象であり、機能保証は反射的な目的であった。その後、参加者が増え、役割、経営の機能、社会的要請が強くなり、徐々に機能保証の概念が入ってきた。担い手についても、技術者だけではなく役員も入ってくる。そして、オールジャパンでやろうということで、法律も整備されたという発展があり、つまり、ニーズ、担い手の範囲、セキュリティの目的が変わってきている。このような計画の発展段階を踏まえれば、機能保証こそが我々の取組の対象であり、ここで改めて、IT障害から重要インフラを守ることの反射的な効果として、あるいはそれから得られる効果として機能を守るという、反射的効果論なんてものを捨てる、パラダイムは変わったんだ、という態度を鮮明にすべきではないか。そうでなければ、内閣全体の方針と合わないのではないか。安倍総理が、日本のセキュリティは大丈夫だと言って一生懸命売り込んでいるのに。今までの流れとの整合性もあるが、基本的考え方において、少し整理が必要だろうと思う。骨子の目的の項において整理いただきたい。

次に、行動計画見直しの重点において、制度基盤の強化を明言いただきたい。具体的な修文例としては、資料６－２のⅠ章「１．行動計画見直しの重点」の最後について、「基本的骨格を維持し」の後に「骨格を維持するとともに、有効かつ柔軟な制度的裏付けを与えることとし、」を挿入するなど。大変なことだとは認識しているが、制度基盤の強化がない限り、情報共有を役立つようにはできないと思う。情報共有を行う中で、情報提供の主体が、例えば知財侵害、特許権侵害、著作権法違反といったトラブルを抱えるようであってはならない。情報共有を含めた情報収集活動により集

められた情報は、物理環境について言えば、製品のベンダー、SIer、これを支える部材メーカー、これをコンサルティングするところ、あるいは認証基準などといった周辺事業者において役に立つのだと考える。制度基盤がしっかりしていないと、必ず衝突が起きる。例えば、警察には、現実に起きた事件に関する捜査情報が細かなものから大きなものまで大量に集まっている。事業者が集める間接的な伝聞情報ではなく、動機も含め、事実をしっかりと調べられている宝の宝庫。このようなものは、オープンデータにし、セキュリティ規格や技術基準に活かせるようでなければならないと思う。しかし、現状では、警察庁が情報をオープンにしようとしても、刑訴法の規制により検事長の了解がない限りは出せない。確定記録法によって事件が確定すれば出せるが、３年後にオープンになっても意味がない。このような状況であり、制度基盤があるようにも見えるが十分に機能していないし、制度基盤自体がない場合も多い。警察の例で言えば、NISCに設置された研究ラボに対しては情報を出せるような法制度とし、技術的な研究ができるようにするなどの方法もあろうかと思う。これに限らず、各領域で様々な検討事項があると思うので、制度基盤の強化に取り組むという目標をしっかりと定め、明確に宣言して進んでもらいたい。ただし、時間がかかる話でもあるので、強硬に推し進めるのではなく、発展段階を見ながら柔軟に進めてほしい。

次は､取組主体の拡大について｡IT障害への対応だけではなく機能保証だとすれば、セキュリティの目的は、日本を外に評価してもらう、あるいは国民から評価してもらうということだと考える。そうだとするならば、重要インフラ事業者を支えるベンダー、機器事業者、加工事業者、コンサルタント、会計士、コンプライアンスの観点からは弁護士など、このような対象にも十分に機能してもらわなければならないことから、取組の主体を広げていくことを検討していただきたいと思う。

次に、資料６－２のⅡ章「１．第３次行動計画期間の目標（理想とする将来像）と評価」について。この中では、望ましい形として、国の役割が書かれていないと感じている。これまでの経緯を踏まえると簡単にできることではないかもしれないが、将来像の最初に○を一つ追加し、「関係主体が連携して、十分な制度的基盤に支えられて重要インフラの機能保証に取り組んでいる」という理想的な姿をこの中に含めていただきたい。

○渡辺会長　サービス、セキュリティの基本的な考え方の概念の再整理ということ、制度基盤の強化、整備を今後検討していくことを明言するということ、重要インフラ事業者という今回の取組の対象者をもう少し広げていかなければいけないということ、行動計画の目標と評価における将来像に、政府としての理想とする姿を加えるべきではないか、というご意見について、事務局からコメントをいただきたい。

○柳島参事官　機能保証をしっかりと目的にしていくことについては、まさに我々も考えているところ。書き方については、もう少し工夫していきたい。

制度基盤の強化については、資料６－１の５枚目、表の①「安全基準等の整備及び

浸透」の「見直しの方向性（案）」欄に「情報セキュリティへの取組を業法における保安規制に位置づける等、制度的な枠組みの検討・整備」と記載している。ご指摘のとおり、この部分は時間がかかる取組になると想定していることもあり、無用な反発を誘引することがないよう配慮する意図も含めて、１枚目に打ち出すことを控えたという事情がある。

取組主体の拡大については、同資料２枚目の右欄（緑色の部分）をさらに拡充していくべきではないかということだと思うが、ご指摘を踏まえ、資料の書き方を工夫したい。

将来像については、現行の行動計画の記載内容を引用しているものであるが、ご指摘を踏まえ、今回の見直しにおいて、将来像をどう書き替えていくかという検討をする中で行っていきたい。引き続き、ご意見などをお願いしたい。

○稲垣委員　制度的基盤については、先ほど経産省から、電力分野における電事法の保安基準にガイドラインの内容を盛り込んだと報告があった。これは本当に先進的な取組で、制度的基盤を明確にしたという意味で、非常に大きな一歩だと思う。他省庁においても、同様に取組を進めていただくのと同時に、経産省においても、これにとどまることなくさらに進んでいただきたいと思う。保安規程というのは、物と人を害しないこと、電磁的影響を与えないこと、電力の流通を著しく阻害しないことが目的。現在、内閣で始められている電力改革においても、取引情報に関するものは含まれていない。これは、電事法自体が自由化に対応した法改正がなされていないという意味。電力の流通に関する保安規程のみという現状は、例えば、機器に対する審査機関や審査事業者もなく、セキュリティの領域が狭すぎると感じている。もし、このような領域を含めて考えるようになれば、取組の主体も担い手も広がっていくこととなる。他の分野にもおそらく同様の状況であり、事業法における事業とそのあり方が変化していると思う。ぜひ業法を見直して、情報セキュリティと制御セキュリティの両方に対応することを含め、しっかりと溝を埋めていってほしい。

○中尾委員　第３次行動計画の見直しのポイントは、基本的に良い押さえ方をされていると思うが、「行動計画に基づく施策群により、自主的な取組が浸透しつつあるが、PDCAのうちＣＡに課題」というところに違和感がある。リスクアセスメントにおいてはＰが重要であり、そのＰが適切であるにも関わらずＣとＡに問題があるという状況は、やや特異なものと思われる。ＣＡに問題があるということについて、具体的に説明を伺いたい。

次に、情報共有について。具体的な情報共有は様々な形で進んでいるとの認識ではあるが、例えば、総務省が指導しているICT-ISACでは、メンバーステートの中だけではなく、アメリカやヨーロッパとどのような情報を共有するべきかという議論を具体的に始めている。情報共有の推進や強化は良い取組だと思うが、自分たちは今どのような情報を持ち、又は収集可能であり、それがお互いにどのように役立ち、どのよう

に使えるのか、それがあるとしたらそれをどのような仕組みで交換するのか、共有するのかという、具体論をしないと全く進まない。骨子の段階なので、この程度の記載内容ということかもしれないが、次期計画本文の段階ではもう少し具体的な話が必要になってくるのではないかと強く感じる。情報共有には難しい部分もあり、先ほど中島センター長もおっしゃったとおり、情報の核となるところを匿名化しなくては共有できないという問題も含め、様々な検討事項がある。次のステップに関することかもしれないが、もう少し具体的な事項を書き込んでほしい。

○渡辺会長　PDCAのＣＡが課題である、その心は、という質問。情報共有の具体的な部分をできるだけ書き込むべきという意見について、事務局からコメントをいただきたい。

○栁島参事官　毎年度、安全基準等の浸透状況調査を行い、その結果を年度末に報告させていただいているところであるが、例えば、レーダーチャートで見ても、PDCAと項目が並んでいるところ、左側のＣＡの部分が潰れてしまっている状況。数字で言えばＣＡを行えている事業者数は半数以下という結果を踏まえ、「ＣＡに課題」と記載したもの。ご指摘のとおり、リスクアセスメントにおいてＰが重要との思いは我々にもあるが、資料上は紙面の都合もあり、その部分を大きく省略して記載したところ。

情報共有の具体論については、現行動計画に基づき、各省庁及び事業者との情報共有の手続きについて詳細な項目を定めており、適宜改定も行っている。また、共有するべき情報の内容を明確にするための事例集を作成し、各関係主体に提供している。今回提示した骨子については、骨格段階であることからこのような記載内容としているところ。

○大林委員　今後の見直しも含めてという意味で、今後の変化の趨勢も含め２点申し上げたい。

情報システムのトラブルで、直接に人命や身体の安全が脅かされることは少ないだろうという時代が長かった。しかし、様々な場面でIT化が進むにつれ、今後は、従来は考えられなかったようなリスク、例えば直接身体の安全が脅かされるリスクが考えられるようになるのではないかと思う。交通系を例とすれば、従来、トラブルで乗り物が動かなくなるということが大きなリスクだと考えられていた。しかし、緊急停止が運転手の判断ではなくシステムで行われることがある昨今、緊急停止ができなくなることが、直接に、乗員や乗客の生命、あるいは事故に巻き込まれる可能性がある人の生命を左右するということを考慮する必要が生じている。動かないことではなく、止まらないことによる危険。病院業務なども、IT化が進めば、生命維持が情報システムに依存する割合が増大し、従来は手作業で対応できたトラブルも、それが生命や安全に直接影響を及ぼす割合が高まることになる。広い意味では、サービスが止まるという表現の中に含まれることだと思うが、従来に増して、直接的に人命や身体の安全に関わる危険が増えていることにも注意するべきだと考える。

次に、技術の進歩について。マイナンバーとも似た現象であるが、例えばフィナンシャルテクノロジーに関して、ブロックチェーンという技術がある。これは、セキュリティのレベルを向上する技術だとされているが、暗号などのセキュリティが何かの理由で脅かされれば、経済活動において非常に広範な影響を受ける可能性がある。総体的に安全だとは思うが、ボトルネックになり得る新しいものが生まれてくる。このような変化は、従来の事業者や分野という範囲での対応にとどまらない、より横断的な対応が必要になる新しいタイプのものだと思う。書きぶりに関する具体的なアイデアがなく申しわけないが、このような状況に考慮していただきたい。

○渡辺会長　事務局には、このような点についても考慮をお願いする。

○細川委員　言葉の確認をしたい。資料６－２のⅠ章「2.1.2 安全基準等の継続的改善」に「重要インフラ防護能力の維持・向上に資する取組として、情報セキュリティに関する取組を業法における保安規制に位置づける」とあるが、化学分野に業法はない。先ほど稲垣先生からもお話しがあったとおり、厳密に業法に限るということではなく、制度的基盤に位置づけていけ、という理解で取り組んでいきたいと思うが、その理解でよろしいか。

次に、行動計画の期限について。先の話で恐縮であるが、これまでの行動計画は３年を目途に見直しを行ってきたところ、新しい行動計画が完成する来年の春から３年とすれば、まだオリパラに届かないところで切れることとなる。計画の内容は、回を追うごとにオリパラの色合いが濃くなってきており、骨子案の中にも、オリパラ大会終了後という言葉も入ってきている。今回の改定について、オリパラを含めたところを見越しているのか、現時点の考えを伺いたい。

○柳島参事官　「2.1.2 安全基準等の継続的改善」については、パラグラフが２つあり、１つ目には「業法における」と、２つ目には「安全基準等の体系を確認した上で、必要な制度的枠組みの検討を行い」と表現したところ。後者については、業法がない分野を念頭に置いて記載した部分である。

行動計画の見直し時期については、通常であれば３年としているが、過去には延長した例もあり、３年でなければならないとの規定はない。しかしながら、長く放置すれば内容が陳腐化する可能性もあり、現在のところ、おおむね３年と考えているが、見直し時期については、今後も引き続きご意見をいただきたい。

(4) その他

事務局より今後の予定について説明

○柳島参事官　本日の議事概要は、事務局にて案文を作成後、各委員の皆様方にご確認いただいた上で公表する予定。

行動計画見直しに関する今後のスケジュールとしては、年内を目途に専門調査会で公表する案の了解をいただきたいと考えている。それまでの間、引き続き皆様方から

ご意見を頂戴し、案文を練っていきたい。第９回の会合については12月中の実施を考えているが、詳細については、別途連絡させていただく。

(5) 閉会

○渡辺会長　これにて第８回「重要インフラ専門調査会」を閉会する。

本日はありがとうございました。