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 12 回会合　議事概要

１　日　時

平成 29 年 10 月 4 日（水）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）
安藤伊佐武　委員　（第一生命保険株式会社）
石川　広己　委員　（公益社団法人日本医師会）
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）
金子　功　　委員　（一般社団法人日本ガス協会）
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）
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）
堀内　浩規　委員　（一般社団法人日本ケーブルテレビ協会）
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）
和田　昌昭　委員　（公益財団法人金融情報システムセンター）
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）

（事務局）
中島　明彦　内閣サイバーセキュリティセンター長

桑原振一郎　内閣審議官
三角　育生　内閣審議官
山内　智生　内閣参事官
越後　和徳　内閣参事官
林　　泰三　内閣参事官
瓜生　和久　内閣参事官
吉田　恭子　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）

中島センター長から挨拶。

○中島センター長　本日も、お忙しい中参集いただき感謝申し上げたい。

本年８月25日に、サイバーセキュリティ戦略本部において、サイバーセキュリティ2017を決定したところ。これは、７月に中間レビューを行ったサイバーセキュリティ戦略を反映して、今年度実施する取組を安定的に遂行するために策定しているもの。重要インフラに係る取組としては、この場で何回も御議論いただいた第４次行動計画に基づいて施策を推進してまいりたいと考えている。この第４次行動計画には、御案内のとおり機能保証やリスクマネジメントといった非常に重要な基本的

概念が書かれおり、今後、これをどのように反映して施策を実施していくかということが課題になると考えている。我々としても、行動計画を実施する主体として、さまざま検討していきたいと思っている。

まだ形にはなっていないが、我々の取組の一部を紹介したい。

１点目は、ＩＴ、ＯＴという部分をこれからはどのように捉えていくべきかというようなことを議論している。セキュリティとセーフティの違いといった基本的な概念の議論を含め、さまざま議論しているところであり、これはまさに、機能保証を踏まえ、今後どのように頭の中のモデルを構築していくかという努力の一環だろうと考えている。

２点目は、過去にこの場でも御紹介させていただいた深刻度判断基準の議論を続けている。まだ基本的なメルクマールの部分でさまざま議論している段階であるが、さまざまなサービスを提供していく上で、マーケットのパブリック・パーセプションをどのようにマネージしていくのかについては非常に重要だと考えており、また、経営層の判断の指標になる非常に重要なツールになると思っているので、ぜひ皆様のお知恵を拝借させていただければと考えている。

３点目は、行動計画の中でも論じられているＰＤＣＡサイクルについて。役人には、前年度に実施したことを踏襲していく傾向がある。過去にどうだったかと必ず上司に問われることの影響かもしれない。そのせいか、ＰＤＣＡについても毎年同じことを行いちょっとずつ改良していけば良いという発想になる傾向があり、私としては、それでは駄目だと常々指摘を行っているところ。私としては、このＰＤＣＡはスパイラルで考えた方が良いと感じている。脅威もサービスの提供関係も変化し続いている中、少しずつ上昇するベクトルが必要なのだと思う。これがなければ、ＰＤＣＡサイクルが役人の思考の中にぴたっとはまってしまう可能性がある。公務員の世界の中だけで考えるのではなく、何か別の刺激を持たなければならないと考えている。

少し脱線したかもしれないが、このような形で、今後とも新たなサービスやビジネスを支える一助となるよう環境整備をしてまいりたいと思っているところ。

重要インフラを標的とするサイバー攻撃の状況として、本年５月のWannaCryの蔓延について少し触れたい。我々としては、このテクノロジー自体は特に高度なものではないという印象があったが、攻撃の機械化によるロングテール現象というのか、脅威環境が変化しており、このような攻撃を抑えるためには、検出だけではなく、ネットワークサイドでの取組が大事になるだろうと感じている。その中で、例えばボット対策をどうするのかということについて、通信セプターの事業者の方々とも御相談をさせていただきながら、総務省、NISCが一体となって取り組んでいきたいと考えている。

本日の専門調査会では、重要インフラにおける情報セキュリティ確保に係る安全

基準等策定指針の原案について報告することとしており、本日の議論を踏まえ、年度内をめどに指針の改定に取り組んでまいりたいと考えているので、ぜひとも活発な御議論をお願いしたい。

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。

前回６月の本調査会において、行動計画に基づいた安全基準等策定指針の改定方針について、さまざま御議論いただき感謝申し上げる。

本日は、前回の議論を踏まえた改定原案を事務局から提示する。この原案においては、重要インフラ防衛能力の維持向上、とりわけ経営層の職責として求められる取組、あるいはコンティンジェンシープラン等の作成を含めた対処態勢の整備、先ほどセンター長からも発言があったＩＴだけでなくＯＴも視野に入れた対策等に資することを目的に、指針本編等の見直しを行っている。

2020年に向けてさまざまな動きがあるが、既にこの分野は事が発生しているので、今、すぐそこにある危機ということで、もっとスピード感を持って取り組んでいかなければならないということを実感しているところ。

そのような意味では、本日の最後の議題としているが、前回、中島先生から御報告があった本調査会が設置している重要インフラサービス障害に係る対処態勢検討ワーキンググループにおいて、深刻度判断基準というものを検討したいと考えている。これは、さまざまな事態が生じたときに、その事態の深刻さがどの程度なのかということを、利害関係者で共通認識を持ってアクションに移していくというもの。安全基準というのは事前の準備段階での基準であるが、もう既に事が起こっているという状況に鑑み、レスポンス、つまり、判断して行動を起こすために、利害関係者が同じ認識を持つための判断基準というものの議論を行うため、ワーキンググループの再開を認めていただきたいと考えている。本件については、本日の最後に皆様に諮りたいと考えているので、その際には、ぜひ御意見をいただきたい。

限られた時間ではあるが、ぜひ積極的な御意見をお願いしたい。

(2) 報告事項

警察庁より資料２について報告。質疑応答は次のとおり。

○稲垣委員　具体的な事業者との接触を含め、社会における非常に有用な取組が進められているという印象を受けた。

先ほど、今後アウトプットの仕方について検討を行うとの説明があった。法的な制約があることは承知しているが、説明があった取組の中で得られたものを含め、法的な観点からセキュリティ対策を考える上で必要となる情報をもう少し出していただくことをぜひ検討願いたい。ISOへの提言なども含め、各企業が何らかの規格を作ろ

うとした時に必要となるのは、事実。そうした事実を情報としていただけることは、非常に有効だと考えている。事実は事件の中で把握されているが、これには刑訴法の制約があり、例えば確定記録を取ろうとしても事件の番号である検番がわからないと検索もできない。これは法務省の問題だが、事件の関係がない人間に検番などはわかるわけがない。警察には情報を外に出すという法制度上の担保はないが、例えば論文、科捜研や科警研の研究報告など、そのような事件とは関係のない形で、具体的な事実を出していただくチャンネルは幾つかあると思う。学会や規格づくりなどに対し、具体的な事実を提供できる工夫をしていただけると、事業者だけでなくそれを支える人々の支えにもなると考える。このような点を踏まえ、ぜひよろしくお願いしたい。

また、サイバーポリスも充実されてきているようなので、できれば、捜査のあり方についても、刑罰権の発動だけを目的とするのではなく、取り調べに当たっても、今後の対策に生かせるような事実も聴取していくような教養を深めていただきたい。そのような実務者を作っていただければ、この取組がさらに有効になると思うので、ぜひ御検討いただきたい。

(3) 討議事項

瓜生参事官より資料３、資料３－１、資料３－２について説明。質疑応答は次のとおり。

○大林委員　資料３－１p.８について。現在、インフラ事業者の経営層の中で、情報セキュリティの重要性についての認識は、かなり広がっているのではないかと思うが、情報セキュリティの具体的な方法については、何をどこまでやるべきなのかがわからないという経営者は比較的多いと感じている。そのギャップにより、事前の対策が不十分であった、あるいはトラブルが発生し、また発生したおそれがあるという時の対応が遅れてしまうということが、経営層に関する問題の大きなポイントなのだと思う。

4.1.2(3)の１段落目で、「経営層は、・・・役割を担う部署及び職員を決定する」とあり、実際、これを文章が意図するように実施していただければ、経営者をしっかりと補佐する形になるだろうと思うが、この文章だけを読んでいると、担当部署だけに任せておけば良いという趣旨にも読めてしまう。普段から担当部署あるいは担当者が経営者に対して、費用対効果も勘案して、この程度のことをここまでやるべきですと十分な助言ができており、いざトラブルが発生したあるいはそのおそれがあるという時に、経営者の判断に対する的確な支援ができるような状態でなければ、経営者の視点からは、どこかに任せたということだけで終わってしまう可能性がある。

また、企業によっての方針もあり、この文書でここまで踏み込んで書くべきかどうかわからないので、推奨とするなど書き方は任せたいが、例えば「役員の職務分掌に情報セキュリティを含める」と記載するなど、役員の職務分掌もひとつのポイントになるのではないかと感じた。

資料３－２p.19について。経営資源を重視するという考え方は非常に重要だと思う。図表 10 を記載していることも、そのような趣旨であり、青色の矢印で因果関係を遡って分析しているという意味であろうと想像している。確かに経営資源も重要ではあるが、最終的に守るべきは国民へのサービスであり、その国民へのサービスを実行するための重要な経営資源の一つとして、基幹的なシステム、重要なシステムがあるということだと思う。この図では、制御システムあるいはそういった重要なシステムが因果関係を遡っていく中での一番最初とされているが、実は、その一つ手前の因果関係で、国民へのサービスがあるのではないか。経営資源としてのシステムが守られていさえすれば良いというように、サービスの視点が漏れてしまう可能性があるのではないかと危惧する。例えば、資源は大丈夫かと確認する際に、情報システムが計画したパフォーマンスを発揮していることで、情報システムは大丈夫だと考える傾向があるが、想定した以上のトラフィックが発生し、それによって容量を超えてしまっているということもある。読み方によっては、それは業務の阻害につながる事象と捉えられるかもしれないが、システムは想定したとおりの働きをしていたとしても、結果的に容量やパフォーマンスが不足してしまうということはあり得る。そのような点も漏れないよう、リスクを考えていく上で、注意してほしい。また、システムが正常に稼働するための経営資源というものもある。電力等を含め、外部に依存しているものも資源として見落としてはいけない要素だと思う。経営資源をシステムと言ってしまうと、実は、その中にさらに資源があるという構造になる。このような点も抜けがないような書き方を工夫願いたい。

加えて、用語について。「業務の阻害につながる事象の結果」とあるが、この「業務」というのは情報システム関連の業務と考えたら良いのか、重要なサービスの提供と考えたら良いのか。ここでは広くとる必要があろうかと思うので、狭く「情報システム関連業務の阻害」と限定しない形とするよう留意してもらいたい。

○瓜生参事官　資料３－１p.８については、経営層が職員に丸投げするということではなく、受けた側も助言をするなどという形で経営層を支援するという、職員の在り方なども含め、経営層と職員がお互いをカバーし合うような形の書きぶりを加えたい。

資料３－２p.19についても、さまざまな外部条件、国民生活や社会生活に対するインパクトを含めた形とするなど、もう少し丁寧に表現することとしたい。

○稲垣委員　名宛て人の中に経営層を明確に位置づけた。そのために、機能保証という概念を鮮明にした。ガイドラインの本文において、今まで抽象的なものだった経営課題として、労働力という人的リソースについて具体的な指摘をしたという点で、経営者にとってわかりやすく響く内容・構造になったことを高く評価したい。

その上で、２点お願いしたい。

１点目は、機能保証の概念について。経営者の役割は、目的に基づいてリスクをとりながら方向性を示していくことなので、大林委員が指摘したとおり、技術的な対策

の話に関して、経営層は何をやったらいいのかわからないというのもうなずけるところ。ISO27000レベルの話は、技術論や具体的なマネジメントの下層の体制論に過ぎなかった。しかし、今回のガイドラインでは、機能保証という概念を使うことにより、経営の取り扱う課題まで持ち上げたという意味がある。また、機能保証という目的を明確にしたという意味がある。機能保証という概念は、本文やリスクアセスメント・ガイドラインの中でいくら強調しても良いと思う。

そのような趣旨では、本文の中で、機能保証の概念の説明が十分ではないように感じる。資料３－１の中で、機能保証が最初に出てくるのはp.１の４行目。ここに、これから実施することについては機能保証の考え方を踏まえるとし、機能保証という用語について脚注で説明している。この部分について、説明内容を資料３－２に記載している概念と一致させること、この説明を脚注とせず本文に記載することの２点について検討してほしい。

資料３－２においては、p.５、p.13にわかりやすい説明が記載されている。機能保証の概念は、機能と保証という２つの概念に分かれる。機能と言った場合、この場での議論では、セキュリティ上の脅威に対する技術的な仕組みの機能というだけではなく、事業の持っている機能を果たす、事業の機能という概念なのだと認識している。だからこそ、資料３－２では、「機能の発揮やサービスの提供を全うするという観点」を強調しているのだと思う。技術論から経営の課題へと発展したからには、ここまで上げないと機能保証という概念の意味が通じない。事業上の機能の発揮やサービスの提供の全うと事業継続を確保するというのが、機能保証の中核的な意味だと考える。

しかし、資料３－１p.１の脚注では、これと異なる内容となっていると感じる。おそらく書き手が異なるのだと思うが、資料３－２との整合性をとるべき。しかも、誤解があるような印象があり、これまで我々がこの場で議論してきた内容と相違がある。脚注においては、防護や機能維持を確約することではない、約束しなくていいのだと。では、どうするのかというと、防護や機能維持のためのプロセスについて責任を持って請け合うのだと。だから、結果は確約しなくて良い。プロセスがあれば良い。責任を持って請け負うことで良いと。事業の結果を確約するのではない、対象はプロセスであり、確約ではなく責任を持って請け負うことで良い、という形でトーンダウンしている。しかも「すなわち」以下を読めば、責任を持って請け負うという概念が「必要な努力を適切に払うことを求める考え方」となっており、だんだんと中身が空虚になってしまっている。これは資料３－２の定義とも異なっている。確かに、これまでさまざま複雑な経緯を経ており、この記述が過去の文書から抜き出されてこのような形になっているのであろうけれども、対処策の具体的な文書として、経営層や社会に対して出す以上は、経営機能の発揮、サービスの維持、事業継続の維持という観点で、機能保証という概念を捉えるのだと腹を決めるべき。この目的を達成するために、経営課題としての情報セキュリティがある。このような位置づけを明確に経営層に伝え

ることにより、何をするべきかが決まるということだと考える。機能保証の概念について、先ほど申し上げた内容で統一してほしい。できれば、脚注に落とさず、本文において、機能保証の考え方はこうだと言い切り、その後のサービス提供の部分につなげてほしい。

２点目は、コミュニケーションについて。資料３－２に関連して、先ほど、社内での情報の提供、支援という話が大林委員からあったが、ISO31000の特徴は、コミュニケーションというプロセスが明確にされたことだと認識している。大林先生の指摘もこのISO31000のコミュニケーションに関するものだと思う。資料３－２　p.2の図表１にはコミュニケーションと記載されているが、実は、本文中にコミュニケーションのプロセスというものが明記されていない。コミュニケーションをリスクアセスメントのそれぞれのプロセスの中に溶け込ませて説明されてしまっている。図表１では、このようなプロセスで実施していくという中にコミュニケーションが入り込んでしまっている。ISO31000を参考に検討しているのであれば、大林委員が指摘されたような現実的なことについて、本文に一つのセクションを設け、コミュニケーションのプロセスとして記述するべきだと思う。言葉としては、さまざまなセクションからの支援、経営的には正確な情報提供という言い方のほうがいいのではないかと思う。例えば、新入社員が社長を支援すると言うよりも、きちんと情報提供すると言う方が良いと思う。法的にも経営の役割の一部は部下に任せることができる。ただし、これには前提があり、正確な情報収集の仕組みがあるということが必要。また、収集された情報が適正であるということを評価するのは役員の責任。その仕組みがない場合には、部下に任せることは組織に対する責務を果たしていないという判断がなされる。これは、多くの内部統制に関する判例でも指摘するところ。法的にも、コミュニケーションは非常に重要なことであると明確にされているので、これに基づく経営層のコミットメントについても、今申し上げたことを参考に検討していただきたい。

○瓜生参事官　１点目については、本年４月に決定された第４次行動計画の記載を単純に引用しているものであり、一度はこの場でも合意いただいた内容である。ただ、ご指摘のとおり、現時点ではそれからもう少し議論が進んでいる状況かと思うので、第４次行動計画とは異なるさらに先に進んだ概念として、もう少し踏み込んだ形に書き替え、資料３－１本文に記載することとしたい。

○野口委員　稲垣委員の指摘のとおり、コミュニケーションに関しては、資料３－２の本文に一つ入れた方が良いと思う。ただし、コミュニケーションには、組織と外部のコミュニケーション、組織内のコミュニケーションという２種類があるので、これらをどのように整理するのかに留意してほしい。

○大林委員　先ほど申し上げたのは、情報セキュリティのリスクマネジメント全般に関するもの。資料３－２は、リスクアセスメントというその中の一業務に関するものなので、先ほど申し上げた内容は、この資料３－２だけでは納まらないものかもしれな

い。ただ、リスクアセスメントの話として言うならば、洗い出しというのか、そのような社内のコミュニケーション、あるいは情報セキュリティの組織体制、そういったものが適切に機能しているかという観点だと思う。もし機能していないのだとすれば、それもリスクになる。強いて、資料３－２に落とし込むとすれば、そのような書き方になるかと思う。

○稲垣委員　資料３－２p.2図表１は、今回の思想を明確に表現しているものだと思う。機能保証の概念を踏まえず、経営課題としても十分な位置づけをしないでリスクアセスメントのプロセスを記述するとしたら、あるいは従前どう書いてきたかというと、この図表１右に記載している「優先サービス」の部分が、データとか情報資産などという記述になっているはず。ここを「優先サービス」と捉えたところが、まさに情報セキュリティを経営課題としたことの表れであり、保証すべき機能を対象としたリスクアセスメントをするのだということの宣言であると感じている。

捉えるべき課題としては、情報資産ももちろんであるが、経営的なもの、外に向かってはサプライチェーンもある。資料３－２にどこまで書き込むのかは別としても、こういったものとのさまざまなチャンネルによるコミュニケーションが射程としては含まれているはず。そういったものが含まれなければ、経営課題に関する完全なリスクマネジメントはできない。

大林委員は、資料３－２はリスクアセスメントに限定したものと表現されたが、あえて限定して考える必要はないと思う。本当に良く作られていると思う。

○瓜生参事官　コミュニケーションには、内と外との２種類があること、重要な課題であることについてはご指摘のとおりと理解。これらについては、野口委員のお知恵も拝借しながら、一連のプロセスの中に強調した形で書き込みたい。

補足で説明をさせていただくと、資料３－１p.15 4.1.4(3)に、「リスクオーナーを支援するための、内部のコミュニケーション及び報告の仕組みを確立する」旨を書き込んでいる。これについては、経営層を意識し、もう少し目立つよう頭の部分で記述することとする。

○渡辺会長　アセスメントのプロセスの中では、横断的なもの、依存関係にあるものなど、横軸を通さないとできないものが出てくる。資料３－１のような書き方も良いが、資料３－２においても、リスクアセスメントのプロセスの中のコミュニケーションとはどのようなものか、アセスメントのアクションの中ではどのようなコミュニケーションが必要なのかということを、ぜひ具体的に書き込んでほしい。

○野口委員　私もこの資料３－１、資料３－２は、非常に力作だと思っている。

１点目は、資料３－１「はじめに」について。p.７「経営層の在り方」の４番目の項目にある「対応を実現するための環境の整備も経営者の責務である」ということは、「はじめに」にも入れておくべき。いい言葉が書いてあるが、「はじめに」に抜けているので、経営層は方針さえ宣言すれば良いと思われないように、という意図。加えて、

両方に抜けている視点として、経営層には対応の効果と影響を検証する責務があるということを記載しなければならない。ただ、ガイドラインはリスクアセスメントまでのものであり、対策の効果に関する部分についてはガイドラインの範疇から外れるという見方もあるので、少し違和感はあるかもしれない。しかしながら、実際、経営者に必要なのは、やれと言ってやりましたという報告を受け、そうかと言うだけではなく、本当にそれは効果があったのかを検証すること。効果と影響と言った意味は、経営としては、情報セキュリティは強化されたが、それが事業全体に障害や悪影響を与えていないかということも検証しなければならない。これも経営者の責務。マネジメントは、複数の機能の総合調整であるので、対応の効果と影響の検証を行うということは、「はじめに」とp.７の両方に、経営者の責務として記述するべきだと思う。

２点目は、ＰＤＣＡについて。最初に中島センター長から発言があったが、非常に大事な指摘をいただいたと思っている。それは、ＰＤＣＡ自体がクローズで回ってしまうと世の中の状況の変化に対応できないという点。この構造は、セキュリティの方針とＰＤＣＡが直接つながっているところにある。方針はなかなか変わらないものと認識されていることから、それに基づいたＰＤＣＡを一旦回し始めると、そこでクローズしてしまう傾向がある。ただ実際は、方針とＰＤＣＡとの間に、マンデートという経営者が要求する要求項目や宣言項目が存在する。これは当然、世の中の変化等に応じて変化するので、ＰＤＣＡも変化するはず。しかしながら、このマンデートを挟まないことが多いので、どうしてもＰＤＣＡはクローズになってしまう。資料３－２p.２図表１左上部、リスクアセスメントの上部に「組織状況の確定」という項目がある。この部分では、世の中とのコミュニケーションを行い、これから先にどういうことが起こり得るのか、世の中の要求がどう変わっているのかという変化を捉え、捉えた変化に対してリスクアセスメントを行うという構造になっている。しかし、この資料３－２では、この部分がぽんと抜けているので、ＰＤＣＡもここが抜けているように見えているのだと思う。

最も簡単に修正するには、資料３－１p.８　4.1.3(1)の１番目の項目の１行目に、「自組織を取り巻く状況や関係主体等のニーズの変化を踏まえ」と「の変化」という言葉を入れると、変化するということを少しは認識させることができるのではないか。では、このニーズの変化をどう捉えるのかというと、外部とのコミュニケーション等によって状況の変化を確定し、それがマンデートとなって出てくるという形なのであるが、これを追記するのも大変なので、１行目を修正することで、これを解説する契機を与えておいていただければいいのではないかと思う。センター長の発言にあったＰＤＣＡをスパイラルに見せるためには、このような工夫が必要だと思う。訓練によく見られるが、前年度の訓練の成果しか反映しないことで、訓練自体がどんどんクローズ化してしまうという現象が生じる。

３点目は、「ＨＳＥの観点」という表現について。資料３－１p.９に「ＨＳＥの観点

も考慮して」とあるが、これは、情報システムだけに限らず事業機能という部分に関わるというものであり、このＨＳＥという観点が入った瞬間に、情報システムの中だけではこの話がクローズできなくなるということを意味するということを意識するべき。情報システムから発生するさまざまな事業の効果を検証するという、経営層も含め、体制自体が非常にダイナミックに変化していることを意味している。しかし、その意味がこれだけで伝わるか、という問題意識がある。また、機能等で考えれば、ＨＳＥだけを特記することには、若干の気持ち悪さがある。さまざまな機能がある中でなぜＨＳＥだけなのかという疑問もあるので、本質的な指摘ではないかもしれないが、文章としては「ＨＳＥ等の観点も考慮して」と「等」を入れることで、少し広める配慮をしてはどうか。ただ、ＨＳＥ等の観点も考慮するということが、情報セキュリティリスク対応にも書いている訓練の対象も、情報システム中心から事業全体に変わってきたのだということは、明記できているという形になる。

４点目は、「リスク源の除去」について。最も象徴的な部分としては、資料３－２p.29「発生頻度及び影響度に応じたリスク対応（例）」のマトリクス。非常に気になるのは、オレンジ色のマスに「リスク源の除去」と書いてあるところ。例えば、化学産業等では、危険な物質を使わないという意味でこのような書き方をすることもある。私が問題だと考えているのは、IoTシステムに関しては、IoTシステム自体がリスク源になるということ。「リスク源の除去」と書くということは、システムをやめるということになるので、この表現は、IoTを含めた情報システムに関してはそぐわない。別の図の中にも、リスク源として「USB等」と書いてある。特に重要なのは、この発想をもうやめなければならないということ。情報システム自体がリスク源である、非常に大きな効果を生み出すものであり、危ない状況を生み出すものであるという認識を持たなければいけない現状において、リスクアセスメント・ガイドラインの中で、この表現を使うことは適切ではない。これは単なる表現だけではなくて、リスクとIoTシステムとをどう捉えるかという基本的な問題。しっかりと基本姿勢を捉えた上で、さまざまな情報アセスメントの成果を取り入れるときに、情報システムのリスクアセスメントとしての言葉の選択を検討してほしい。

○瓜生参事官　１点目について。「対応を実現するための環境の整備も経営層の責務である」ということは、資料３－１「はじめに」に、対応の効果と影響については、資料３－１「はじめに」とp.７の双方に追記したい。

２点目について。資料３－１p.６　4.1.1(1)の「外部環境及び内部環境の理解」の冒頭で、少し抽象的な書き方ではあるが、自分を取り巻く外部環境及び内部環境の変化について整理すると記載している。この考え方は、情報セキュリティ対策の全体と特にリスクアセスメントを検討する上で必要な事項だと思う。全体に対するものとしてはこの4.1.1(1)で、また、アセスメントに対するものとしてp.８　4.1.3(1)に改めて記載する方向で修正したい。

○野口委員　お願いする。加えて、ＰＤＣＡ全体がクローズではないということも、メインのどこかに書くべきだと思う。ＰＤＣＡというものは、前年度の反省だけで成り立っているのではなく、世の中の変化をしっかりと取り入れるのだと、どこかで１文を入れてほしい。

○渡辺会長　これについてもお願いする。

３点目についてはどうか。NISTを意識してＨＳＥを入れ込んだということかと思うが、その心を説明する部分がないことで、もしかしたら誤解もしくはわからないという読者も出てくる可能性があるので、「こういうことが重要で、例えばＨＳＥ等・・・」という形ではどうか。

○瓜生参事官　ＨＳＥと入れた意味を書き下し、さらに「等」と付けて、修正を検討したい。

○渡辺会長　４点目についてはどうか。「リスク源の除去」の書きぶりをどうするのかなど、このマトリクスを使わないということも含めて、提案があれば。

○大林委員　書きぶりについて。ここでは、「回避」を「事業の回避」と定義しているものと認識しているが、これは、リスクの低減の仕方次第かと考える。事業単位で見るのか、より小レベルのリスクで見るのか。ここの「回避」はさまざまな解釈ができると思うので、よりリスクの小さい方法で目的を達成するという意味であれば、書きぶりの観点からは、特定の小レベルのリスク源を回避するという表現も成り立つのではないか。

○瓜生参事官　当方としても大林委員の発言と同じような理解をしていた。システム自体がリスク源であるとの認識は、大きな視点から捉えた認識であると理解。これをさらに細分化して見た場合には、例えば、外とつなぐことができないようUSBの使用を止める、なくすという方法もあると考えている。制御システムの中の小さな部分に視点を移して、さまざまな細かいリスクとなり得るものを消していくなど、小さい単位で回避するという手段もあるのではないか。全体を捉え、情報システム自体が危険と考えれば、確かに除去することはできない。ただ、その情報システム全体の中のある部分を除去するという小さな単位で整理していくことはできるのではないかと思うがいかがか。

○野口委員　言葉について。昔のリスクマネジメントでは、この部分をハザードと言っていた。ハザードというのは、潜在的危険要因という定義をしており、それを何故、リスクソース、リスク源という言葉に変えたかというと、リスク源という言葉には、力という意味しかなく、このリスクの力というものが、情報システムの効果をもたらしたり、被害をもたらすということを表現するため。パワーという意味しかない。だから、もしここでUSBなどの細かいことを示したいのであれば、やはり、リスク源という言葉を使うのは、リスクマネジメントの世界ではふさわしくない。リスク源というのは、そもそもリスクを生み出す情報システム自体のポテンシャルのことを言うの

で、USBなどはそのほんの一部にすぎない。USBがリスク源のひとつであることは間違いないが、USBによってある事象が起きたときに、USBさえ使わなければそのリスクが起きないと思うことが怖い。やはり、このような情報システムを使っているということの本質を捉えたときのリスク対応はどうあるべきか、ということを考えると、ここの言葉はもう少し慎重に考えるべき。情報に経営を巻き込んで大きな流れで捉えようとしている今、まだ昔のリスクアセスメントの言葉を使っているようで、大きな違和感がある。

○稲垣委員　この問題は、ISO31000、資料３－２のガイドライン、そこにおける定義、言葉について、本当は深い議論が必要なのだと思う。その議論が今ここことで行われているわけであるが、資料３－２では、p.33で「リスク源」を定義している。伝わりやすさを踏まえ、これに何らかの説明や具体例を入れるという方向で、野口委員にも御指導いただきながら取りまとめていってはどうか。例えば、裁判所、法廷では日本語を用いるという規定があるが、そのように、わかりやすく、きちんと定義ができる言葉を使っていくということが大事。全ての要素を入れることは難しいかもしれないが、御指導いただきながら調整していただきたい。

○渡辺会長　確かにこれはリスクの本質論に関わることなので、時間に限りがあるこの場では納まらないかもしれない。例示はあった方が良いが、この図に関しては、誤解を招く可能性があるのであれば、違う図にするかなくすなど、関係の有識者の皆様も含め、御指導を受けながら改善していくということで、一旦納めさせていただきたい。

○原田委員　資料３－２p.14 に「業務の最大許容停止時間（MTPD）を推定します」とあり、具体的には資料３－２に添付されている STEP４の記入例の表下部に凡例があり、例えば「影響あり」は「活動目的の阻害につながる影響がある」などとされているのみとされている。これは、各事業者の業務部門が見た場合、自分たちが考えているサービスレベルとしてどれだけ停止したら影響が出るかと考えているものと、別途定められようとしている深刻度のレベルにおいて、どの辺りの影響のことを言っているのかが一致しない可能性があると思う。特に、重要インフラ事業かつ優先サービスであるとなれば、どれだけ止めて良いのかという言葉だけで考えると、全く止めることが許されない、せいぜい瞬時かという話になり、×が並び、MTPD についても数分若しくは０分ということになる。この表の記載がブレないようにするには、凡例の表現として、単に影響があるかどうかとするのではなく、別途定められる深刻度レベルというものが出てくるのであれば、どの深刻度レベルの影響が出るかということが理解できるような表現にしてほしい。

２点目は、資料３－２p.20 について。具体的に影響を洗い出して、どうすれば良いかという対策の例が図表 11 にある。この例には、最終的な対策として「社員教育の実施」と例示されている。これはいわゆる非 IT、情報システムそのものに対する対策ではないと認識しているが、一方で、先ほどと同じく資料３－２に添付されている様式

記入例の中では、特定された経営資源は、情報、データ、情報通信システムというものとなっており、その対策の例も、システムにおける対策に特化されているような印象がある。先日のオリパラに関するリスクアセスメントの情報交換会の中でも、システムにおける対策を中心に書き込みを行った。資料３－２　p.20 で求められている洗い出すべき対象や最終的にとるべき対策の対象が、情報システムに焦点を当てたものなのか、それ以外の会社業務全般を含むものなのか、ブレがないよう明示してほしい。

○瓜生参事官　深刻度については、起こった事象がどのようなものかを評価しようとする試みであり、新たに許容時間を決めるという性質のものではないとご理解願いたい。我々としては、ご指摘のサービスの許容停止時間というものは、各所管省庁が定める業法をベースに、各事業者が検討を行っていると理解している。深刻度判断基準の検討においては、例えば業法で定められた基準を超えるような事態が生じたことが公表された場合に、それが日本全体としてどれだけのインパクトとなるのかを評価できればと考えている。レベルという意味で言えば、例えば政府として対応が必要となるような緊急事態であった場合には高い評価値とするなど、基本的には、既存の制度にある基準値をベースにして、政府全体としてどう対応するか、それを世の中にどういう形で発信するか、ということを検討する想定であり、新たな基準を作るものではないので、事業者の皆様が考えているサービスレベルに関する感覚と大きくブレる形にはならないと思う。その点に関しては心配されているような状況にはならないと考えていただきたい。

○原田委員　事業者のサービスレベルとしてどれだけを目指すのかについては、必ずしも業法で定められている部分とは異なることもあり、ブレが出ることを危惧しての質問であったが、これについては、各事業者の定め次第というところで理解した。

○瓜生参事官　２点目について。機能保証の考え方から言えば、リスクアセスメント自体としては、基本的にはビジネス全体を対象とするものと考えている。先ほど資料３－２の位置付けとして説明させていただいたとおり、資料３－２は、さまざまなビジネスを扱うリスクマネジメントの取組の中に、情報セキュリティシステムの視点を追加して補完する際の参考という位置付け。経営全体のリスクアセスメントの中のシステムの部分を対象とするガイドと認識していただき、活用していただければと思う。

○原田委員　了解。

○石川委員　これまで４年ほど参加しているが、本日ほど、この指針とガイドラインがストンと腑に落ちた経験はない。医療分野としては、ICT 利用に対する関心がどんどん高まっていることを背景として、特に、個人情報保護と情報セキュリティについて取組が遅れているという認識が明らかになりつつあるという現状がある。医療においては、マイナンバーとは異なる医療等 ID を使うことが政府方針になっているが、ここ数年は、我々としても、マイナンバーが医療にどのような影響を及ぼすのかということについて関心を持って注視している。また、医療介護の全体をネットワークでつ

なぐことについて、平成 32 年を目標に一生懸命取り組んでいるところ。ご案内かと思うが、次世代医療基盤法に関連して、いわゆる代理機関に関する検討、ビッグデータの利用に関する検討なども継続して行っている。このように医療分野で情報セキュリティに関する機運が高まっている中、本日の指針とガイドラインは、納得感のある内容となっていると感じた。特に、経営陣と人材育成に関する事項については、医療経営を行っている我々として、しっかりと考えて取り組まなければならないということが、非常によく理解できた。

他方、これら文書を拝見し、医療分野の取組が、今からどうすれば良いのかわからないほど遅れているということを改めて痛感した。例えば個人情報保護について言えば、法改正に当たり、瓜生参事官にも支援をいただきながら、5月 31 日以降、何とか良いところまでは来れたのだと思うものの、国民あるいは医療従事者に、この内容が十分には伝わり切れていない、完全なレベルには到達していないとの印象がある。ガイドラインなども策定されているが、現場では実行段階に至っていないと、切実に感じている。現在、厚生労働省、内閣官房、総務省、経産省の４省に協力をいただき、医療分野のネットワークに関する取組を進めているところではあるが、この情報セキュリティの部分について、医療界に対し、政府から特段の支援をよろしくお願いしたい。

○渡辺会長　生命、医療に関しては、確かに全体の中ではスローな時期もあったが、近年、急進されて意識も上がっているとのこと。センター長含め事務局から、医療分野に対してのコミットメントについてコメントをお願いする。

○三角審議官　御発言に感謝。米国では、個人情報の次のテーマとして、医療機器を補完するシステムとしてのネットワーク化、さらにその高度化についての議論が行われている。今後の医療の状況なども踏まえ、協力して取り組んでいきたいと思っているので、引き続き、よろしくお願いする。

○石川委員　ご発言に感謝。今、遺伝子のゲノムを使った医療が喫緊の課題として迫ってきており、決めなければならないことが山積している。これは、番号制度にも関わっており、例えばゲノムの情報を今後の医療、創薬に使おうという動きがあり、このときにそのような情報の番号をどうするのか。既に今年度から、がんの治療などにもゲノム情報を使うことになっている。このような状況からも、個人情報保護の対策についても、早く欧米の段階までレベルを上げたいと取り組んでいるので、ぜひ御指導をお願いしたい。

○稲垣委員　一言、応援させてほしい。産業政策、日本の国力向上、日本の国際社会におけるプレゼンスの向上という意味で、医療のような人命を救う分野でのセキュリティ対策の確保・向上は、日本が平和国家として、国際的な機能を果たす上で重要な取組だと思う。例えば、遠隔医療に関する取組。これがセキュリティを確保した上で国際的に輸出ができれば、日本の国際競争力を高め、かつ日本の国際的な役割を果たす

ことにもつながるのではないか。病院もない、看護師しかいない、死傷者を戸板で運ぶしかないという状況の国もまだまだ存在している。そのような国に、日本の医療や世界の医療を提供したい。日本がその先陣を切ることになれば、その意味は非常に大きい。ぜひ、今のご発言を大事に取り組んでいただきたい。

○渡辺会長　その点は、しかと受けとめたいと思う。

○有村委員　資料３に記載の指針改定のポイントについて。経営層と機能保証については他の委員からコメントがあったので、ＩＴのみならずＯＴも視野に入れた対策という点、コンティンジェンシープラン等の作成も含めた対処態勢整備という点についてコメントしたい。

資料３p.４の表、資料３－１p.26 の別紙３について。第４版までになかったこのパートについて、ワーキンググループでの議論を経て入れ込むことができたことに対し、その努力に敬意を表したい。

先月、ICS セキュリティカンファレンスという国際会議に出席するなどして、複数の海外 ICS-CERT と話をする機会があった。これらのメンバーの間で、サイバーフィジカルスレッドモデル、簡単に言えば、ＩＴとＯＴとの関係をどう整理するのかということが、ひとつの大きなトピックになっていると聞いた。彼らは、ＩＴとＯＴの両方を視野に入れた場合、ＩＴ vs ＯＴと捉える傾向がある。この中で私からは、資料３－１別紙３にある保安管理体制や業法をセットにしたＩＴコンティンジェンシープランのトランジションの部分、それを考えるに当たって表にあるサイバー攻撃ならではの特性を考慮しなくてはならないという部分、さらにＮＩＳＣが情報セキュリティ確保に係る安全基準等策定指針を改定しこれらを盛り込むこととなっていること、そのようなトップダウンのアプローチをとっているということをプレゼンさせていただいた。セキュリティ政策については、グローバルな視点を持ちつつ取り組んでいくことも必要ではあるが、保安管理体制に関連する部分や制度に関連する部分など、我が国独特の良い概念は切り捨ててはならないと考えており、これは、ＩＴ vs ＯＴなのではなく、ＩＴとＯＴのフュージョンであると説明した。日本的な発想なのかもしれないが、対立構造ではなくフュージョンであるとの主張は、彼らの受けも良く、一定の理解を得たと思う。

ワーキンググループでは、保安管理体制下で運転している制御システムに対するサイバー攻撃にどう対処するかと考え、サイバー攻撃の特性をリスト化した。フュージョンというコンセプトでここまで来ているのは日本が唯一だと思う。そのような意味では、このリストを作成すること自体が、アンビシャスでチャレンジな取組であると言える。リスト化に当たっては、重複せず漏れなくが最も理想的できれいだと思うが、とても難しいとも思う。今後、パブコメや有識者との議論も経て取りまとめが行われることになろうと思うが、重複は恐れず、ただし抜けはないように、という精神で注意して取り組んでいきたいと考えている。そのような目線でこのリストをご覧いただ

き、今後とも御指導いただきたい。

○渡辺会長　サービスの提供という意味では、システム・オブ・システムなどと言うのか、情報システムは一体と見るべきだろうと思う。そのような意味で、サイバー攻撃の特性を７つの項目で整理しているところ。重複については事務局も認識しているが、さまざまな形で、さまざまな見方で、さまざまなポイントを炙り出した方が良いだろうと考えた結果としてのこの７項目。ただ、有村委員の発言のとおり、漏れはあるべきではないと考えているので、ぜひ、改めて御確認いただき、御指摘をいただきたい。

○和田委員　資料３－１p.10 4.1.3(2)(ア)の「人的資源のセキュリティ（外部委託）」において、「委託先との業務委託契約書等には、委託先が自組織と同等レベル以上の情報セキュリティ対策を・・・」とあるが、委託先に求める情報セキュリティ対策の基準が、委託元の自組織のレベルという点に少し違和感がある。委託するということは、コスト削減もあるだろうが、高い技術を求めて委託する場合もある。この部分で言わんとしていることは、リスクアセスメントのリスク評価の結果として導き出された必要なレベルをしっかりと委託先に求めるという趣旨なのではないか。修正をお願いしたい。

また、その部分に続いて、「情報セキュリティ動向の変化に応じて、契約文言の見直し・・・」とあるが、動向に応じて変わるのはリスクアセスメントの方なのではないか。資料３－２でも継続的な見直しとしているように、リスクアセスメントの継続的な見直しを行った結果に応じて、契約文言の見直しを行う、というのがこの部分の趣旨なのではないかと思う。

○瓜生参事官　ご指摘の２点について、丁寧な書きぶりに修正したい。

○盛合委員　資料３－１p.11 4.1.3(2)(エ)の「暗号を活用した情報管理」について。「なお、暗号化機能は、関連する法令及び規制を順守して用いる」とあるが、この文章から、どのような法令や規制を用いるのかについて、読者に丸投げしているような印象を受けた。統一基準的なものなのか、あるいはクレジットカードの PCIDSS などの業界ごとに決まっているようなものなのか、また、主語が「暗号化機能」であることから考えれば輸出規制の話なのだろうか、など迷いを生じさせてしまうのではないか。読者は必ずしも専門家ではないかと思うので、何を想定しているのかが伝わるような書きぶりに修正した方が良いのではないか。また、暗号化技術には、暗号化機能だけではなく認証機能などもある。おそらくこの文章は両方を対象に考えているのだと思うので、この文章の主語としては、「暗号技術は」とするべき。

加えて、細かい点を２点。資料３－１p.36 参考文献の下から３番目について。経済産業省のサイバーセキュリティ経営ガイドライン ver.1.1 は、2016 年の発行ではないか。資料３－２の別紙２「結果を生じ得る事象（脅威）の例」の「ソーシャルエンジニアリング」の項目に「機会を伺って情報システム・・・」とあるが、「伺う」の表記が誤り。

○瓜生参事官　参照するべき法令、規制については、別途一覧表として掲載する予定。今後、どの文書を記載するべきかを含め、盛合委員にご相談させていただきたいと考えているので、よろしくお願いしたい。

○平田委員　資料３－１別紙３の「ＣＰ及びＢＣＰの策定・改定における考慮事項」について。この記載の中に、例示ではあるが、システム的な手段に踏み込んで記載されている部分がある。これが義務であるとの誤解を生むことがないよう、考え方のレベルにとどめるべきだろうと思う。例えば、p.31 では、「ＣＰ及びＢＣＰの発動に備えた平時の対策」において「非常用システムもメインシステムと同様の手口でサイバー攻撃を受ける可能性があるため、・・・異なるシステム構成で構築する、異なる提供者から調達する」と記載されている。本質的には、同じ手口で狙われるので、その手口に対応した上で非常用のシステムを動かすということだと思う。読者には、その手段よりも、その考え方を参照していただいた方が良い。他の部分に、いくつか同様の記載があるので、考慮をお願いしたい。

○大高委員　今回、指針とガイドラインが非常に良いものとなったと思っている。ただ、これを各分野におけるガイドラインにどう反映してもらうのか、その進め方がなかなか難しいかもしれないと感じているところ。各分野におけるガイドラインでは、従前の ISO27000 シリーズの要求事項さえ満たせば良い、という形になっている傾向がある。他方、この指針とガイドラインにおいては、この場の議論により言葉一つ一つを慎重に選び、その裏にある機能保証の考え方などを盛り込んでいる。この意味を、どのようにそれぞれの分野に取り込んでもらうのか。その取組の方向性などを示していただけるとありがたいと思う。

特に今回は、対策編を廃止して指針本編に取り込んだ。これは、今回の内容の変化に対して必要なことだと思うが、現場に下りていけば、具体的な対策が求められる。現場では、その対策だけ守っていれば良いという感覚になりがちであるが、今回の指針における思想や機能保証というものの考え方、経営層の関与についても、かなり深みを増してきている。この考え方を、それぞれの分野のガイドラインにしっかりと記載していただく取組を、ぜひ進めていただきたいと思う。

○渡辺会長　これは、各所管省庁とも相談しながら、どのような形でこれを各分野に展開していくかということを議論し、検討していくのかと思う。

○瓜生参事官　既にある省庁から、これまでのものからどう変わったのかについて、わかりやすく示してほしいという要望もいただいている。今後、新旧対照表のようなものを用意し、具体的に解説するなど、各分野の皆様とも相談しながら取り組んでいきたいと思っている。

○稲垣委員　それは最低限必要なこと。それに加え、このような新しい取組を支える支援業務、コンサルティング事業など、各省庁においてそのようなものに対する特段の予算措置を検討するなど、そのようなところまで踏み込んで、初めて実効性のある取

組になると思う。中身を決め、それを理解できる者がやれば良いという構造ではなく、できるように支援する、そのために何が必要かと考えてほしい。予算を獲得する、このような新しい政策として実行してもらう、ということをこの場から発信する必要があるのではないか。この点についても、ぜひ検討願いたい。

○渡辺会長　時間が限られており、全ての意見を伺えず申し訳なかったが、本日の議論はここまでとしたい。追加の御意見については、10 月 10 日までに事務局へ提示願いたい。追加の御意見も踏まえ、必要な修正を行わせてただき、修正後の文書について次回の専門委員会で報告して討議いただき、その後、パブコメに付すという形で進めたい。

(4) その他

瓜生参事官より資料４について説明。質疑応答は次のとおり。

○大林委員　この深刻度というものは、国民への発信を前提としているものか。もし発信することを前提としているのであれば、自然災害の場合のレベル感との調整が必要だと思う。情報セキュリティについては、国際的な整合性が非常に重要。国民向けなのであれば、自然災害の場合の深刻度とうまくすり合わせる必要がある。それができないようであるならば、あえて同じものとせず、国民向けのものと使い分けるという方法もある。これから検討しようとしているものは、情報セキュリティ関係者の間のみで共有されるものなのか、国民向けのメッセージとして使われるものなのか、今の考えを伺いたい。

○瓜生参事官　今まさにそのような議論をしているところ。我々としては、システムの部分に注目しがちであるが、機能保証の観点からすれば、サービスが停止して国民に影響を与えるというレベルの状況もカバーしなければならない。そのような意味では、例えば、大地震で緊急災害対策本部が立ち上がるというレベルも含めた物差しによって、生じた事象がどれくらいのレベルに相当するのかということを評価することになると考えている。国民に発信することを前提として、自然災害を含めたさまざまな災害に関するこれまでの情報と整合性を計りつつ、国民にもわかりやすい形でまとめていきたい。

○渡辺会長　つきましては、この深刻度判断基準の検討を対処態勢検討ワーキンググループにおいて議論させていただきたいが、よろしいか。

○一同　異議なし。

○越後参事官　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13回会合の開催については、別途連絡をさせていただきたい。

(5) 閉会

○渡辺会長　これにて、第12回「重要インフラ専門調査会」を閉会する。

以　上