高度情報通信ネットワーク社会推進戦略本部情報セキュリティ政策会議
重要インフラ専門委員会
第1回会合議事要旨

１．日時　平成 17 年 10 月 11 日(火)　13：00～16：00

２．場所　内閣府本府地下講堂

３．出席者

[委員]

浅野　正一郎　委員（国立情報学研究所教授）
石井　健睿　委員（（社）日本水道協会）
伊藤　友里恵　委員（JPCERT/CC）
岩田　隆　委員（（社）日本ガス協会）
大場　満　委員（東京地下鉄（株））
金澤　亨　委員（野村證券（株））
久保田　啓一　委員（日本放送協会）
九萬原　敏已　委員（電気事業連合会）
外川　雅通　委員（住友生命保険相互会社）
郡山　信　委員（（財）金融情報システムセンター）
小西　甲　委員（日本通運（株））
田中　正史　委員（全日本空輸（株））
土居　範久　委員（中央大学）
中尾　康二　委員（KDDI（株））
中原　周司　委員（あいおい損害保険（株））
沼澤　勝美　委員（日本医師会総合政策研究機構）
深谷　聖治　委員（東日本旅客鉄道（株））（佐藤氏代理）
前田　淳一　委員（東京都総務局IT推進室）
松田　栄之　委員（新日本監査法人）
渡辺　研司　委員（長岡技術科学大学助教授）

（五十音順）

[政府]

内閣官房情報セキュリティセンター長
内閣官房情報セキュリティセンター副センター長
内閣官房情報セキュリティセンター情報セキュリティ補佐官
内閣官房情報セキュリティセンター内閣参事官
内閣府政策統括官(防災担当)付地震・火山対策担当参事官
警察庁生活安全局情報技術犯罪対策課長
防衛庁長官官房情報通信課情報保証室長
金融庁総務企画局参事官

総務省自治行政局地域情報政策室長
総務省情報通信政策局情報通信政策課情報セキュリティ対策室課長補佐
厚生労働省医政局研究開発振興課医療機器・情報推進室長
厚生労働省健康局水道課課長補佐
経済産業省原子力安全・保安院電力安全課長
経済産業省原子力安全・保安院ガス安全課長
経済産業省商務情報政策局情報セキュリティ政策室長
国土交通省総合政策局情報管理部情報企画課長

４．議事概要

(1)内閣官房情報セキュリティセンター長挨拶

(2)委員長選出

○浅野委員を委員長に選出

(3)浅野委員長挨拶

(4)会議の公開等について

○事務局より説明、原案の通り了承

(5)専門委員会の進め方について

○事務局より説明

(6)論点説明

○事務局より説明

(7)委員意見開陳

○ 重要インフラ分野において対象事業者の同定を行う際に、同定された事業者の位置づけについてよく議論をする必要があるのではないか。私自身は同定された事業者はボランタリーに本行動計画の仕組みの中で活動していくと理解しているが、他業界や団体も含め、この場にいない事業者にとっては、どのような活動を行っていけば良いのかが解からず、戸惑うといった懸念が想定される。

○ 同定された事業者の活動が評価されることになるのであれば、行動計画が関係する全ての事業者の目に触れるプロセスを取る必要があり、これを考慮しないと、全体としてうまくいかないのではないか。

○ 重要インフラ事業者は「国民生活を守る」という考えを基礎に、既存の行動計画をさらに発展させていくのが、本委員会の目的であると認識しており、各業界でその

点を確認しながら、しかるべき新たな行動計画を策定して行く必要がある。

○ 事業法では事故が起きた場合の報告義務があり、法律で定められた以上のことが行動計画で求められれば、ボランタリーな活動ということになる。

○ 重要インフラのサービス（供給等）に支障が生じた場合、すでに定められている「各種報告規則」などに基づき所管省庁に報告実施している。これまでの仕組みを最大限活用、延長線上とする方向が現実的と考える

○ 情報提供の範囲の見直しについては、既存の法令、各分野で実際に行われている連絡体制の仕組みを活用する方向とする。新たな連絡体制をつくるのは混乱の元。

○ 既存の各種報告規則で定められている事項と、今回の情報連絡スキームで求められている事項をどう整理すればよいのか。例えば報告先は別々になるのか。

○ 別々に報告と言うことは考えていない。

○ 法的根拠があれば皆が納得することは理解するが、法制度だけでは変化への迅速な対応の面で難しい面もある。社会や国民を含め、国に貢献する際には、現行の特別行動計画のように法的根拠に基づかないが合意によって、行動する場合もある。今後、より社会における相互依存関係が増していく中で、社会活動を維持するためには、両者の合意に基づく行動が何か出てくるのではないか。あまり法律的な根拠を追求する議論はしたくない。

○ 本委員会では、どのような認識や意識を持って検討を行っているのか、を国民に正しく伝えることが必要。例えば、IT 障害の具体的例示によって、様々な脅威が存在することを国民に認識させることが必要。

○ 具体的な例示として、複合的要因や連鎖関係を示し、重要インフラ間の相互依存性により、連鎖的に発生するものであるということ、及び自分達にも波及が想定されるということを分かり易く伝えるのも一案。

○ ある特定の重要インフラ分野のみが細分化されるのは、他分野の横並びからして違和感がある。分野内での優劣もあり、細かい事業者の設定は、各分野の検討とさせていただきたい。

○ 地域によっては、同じ重要インフラであっても、利用者の数に格差があるという状況から、これら大小ある事業に対し、同じように同定を行うのは無理がある。

○ そういう意見は理解できるが、国民が重要インフラを利用する以上、その格差を理

由に、何もやらないということはやるべきではない。何らかの手段を講じて大小ある事業者をまとめるよう検討するべき。

○ いわゆる「サイバーテロ」から「非意図的要因」、「自然災害」へと要因を拡げる際に、サイバーテロ対策時の表を参照して良いのかどうかの議論が必要。

○ 情報共有については、類似の障害であるかを如何に早く抑えるか、加えて相互依存の観点から言えば、あるところで障害が発生したときに、それが如何に連鎖していくか、という二つの側面がある。これらの整理の仕方を、もう一段、踏み込むことにより基本計画と合うのではないか。

○ IT 障害の類型については、自然災害によるケースは明らかと思われるが、サイバー攻撃と非意図的要因の区分を直ちに下すのは難しい場合があると考える。

○ 想定される脅威の例示については、「サイバー攻撃」、「非意図的要因」、「自然災害」の 3 つが考えられるが、意図的か非意図的かは、情報が集まった段階で分かるものである。即ち、脅威自体をカテゴライズすると、人的要因で起こるものか、システムの障害で起こるものか、あるいはそれ以外の要因で起こるものかが分類されるものであり、人的要因でいえば、ネットワークを介してくる脅威なのか、物理的なアクセスによって起こされている脅威なのか、あるいはそれも外部からか内部からか等、それらの分析がしっかりなされた上で、意図的であったのか、非意図的であったのかが理解されるものではないか。

○ システムの障害でいえば、何らかの不具合であるとか、悪意のボットであるとか、ブレークダウンされた脅威のカテゴリとなる。その他の問題として自然災害とか、相互依存性の関係から他のセクタからの影響を受け、脅威が発生するというカテゴライズもあるのではないか。

○ 事業者からの情報提供範囲の見直しについては、事業の形態によって、かなりレベル差が見受けられると感じている。厳格に実施しているところがある一方、割と自由にやっている事業体もあると思う。実際の行動計画を作るにあたっては、同一のレベルで全てを見直すということではなく、適切なレベルでの情報提供の範囲という観点で、今後議論していければと思う。

○ 情報提供に関しては、結局、緊急度のレベルにかなり依存することだと考えている。行動計画には、緊急度を誰が判断するのか、ということはできるだけ明確に書かれなければならないと思うが、最終的にこれは事業者がどの程度の緊急度と判断するかということになるのではないか。

○ 情報提供に関する意見案として、「情報連絡の対象となる事案についての範囲とし

ては、法令等で報告が義務づけられている事故、障害、業務遅延等の他、特に重大なものとして事業者が連絡を要すると判断したものを含むということ」とする。

○ 連絡体制の見直しに関して、先ず「ISAC」という言葉が急に出てきている感がある。米国では ISAC という業界ごとの組織が存在し、業界内の情報を共有しているが、国内重要インフラ事業者の中では、まだ ISAC についての合意形成がなされていないため、今の時点では ISAC という表現は早急と認識している。

○ ISAC に関しては、今後この情報連絡体制の議論の中で、その位置づけをどうするかということを再検討していく。

○ 各分野間及び分野内の情報提供のあり方については、相互依存性分析が深く関わる。自らの分野にとって、依存性の高い分野が、他の分野においても依存性が高い場合、その脆弱点を事前に知らしめることにより、逆にリクエストを受けた産業が提示を行う。それが定期的であるべきか、動的な要因であればモニタリングをするのが良いのか。各分野間の相互連携を明確にしていく上で、どのレベルでどういう頻度で行っていくのか、責任の所在も含め議論していく必要がある。

○ IT 障害の連絡については、情報を付き合わせることにより、個別の事案としては大したことはないが、複合的な要因として裏に何らかの原因を見出すことが可能となる。この場合、それぞれ連携と言うよりも、各分野から出してきたものを統計解析し、相互依存性分析を行った上で各分野に知らしめるという形になるが、そういった分野間の間接的連携、情報の共有が必要。

○ 例えば自然災害のケースで、情報システムが破壊されてしまったが、他のものも壊れているという場合に、システム障害だけ個別に連絡しなければならないものなのかが疑問。

○ 構造的に潜在化されている脅威について、それをどのように顕在化させていくのか。また内部不正についても正式なルートと内部告発のルートの整理が必要。さらに動的なものと構造的なものをどのように整理するか等の工夫も必要。

○ IT 障害の連絡については、サービス提供に相当な支障を来たした IT 障害を連絡の対象として、軽微な IT 障害は対象に含めないのが現実的だと思う。他の重要インフラ分野のサービス停止が原因で発生した IT 障害については、その内容、規模にもよるが、統計的な発生状況をまとめて報告するという方法も採りうるのではないか。

○ サイバー攻撃のある部分については、現在も連絡を要しないとされている事項があり、この連絡する・しないは事業者が判断するということだが、その旨の注釈を田

の脅威についても明記していただきたい。また、非意図的要因のところでカテゴリ分けの見直しについて、社会的な影響が重大な場合は報告義務があるが、同様に事業者が重大と判断したら報告ということにさせていただきたい。

○ 意図的、非意図的の判断に加え、事業者の判断材料として、報告後にどのようなレスポンスが返ってくるのかを書き出すことなど、情報提供のメリットがわかりやすいと、事業者としても情報提供の意義が理解し易い。

○ 行動計画の推進体制に関して、これがもし監督省庁の検査とすると、事業者の同定と関連し、事業者を評価すると理解されてしまう。個別事業者の評価というよりも、むしろ仕組みの評価というようにしていただきたい。

○ 実施状況の評価・検証については、監督省庁の検査あるいは第三者機関による外部監査による評価・検証がベースになると思われる。また、行動計画の見直しについては、監督省庁の検査あるいは第三者機関による外部監査の評価・検証結果をもって、判断する必要があると思う。

○ 実施状況の評価検証については、申し合わせによって作られた体制の機能の評価を行い、事例の発生しない場合は、演習という形で評価していくことを想定している。また「安全基準・ガイドライン」も同様に評価サイクルを提案していくことを考えており、内閣官房は重要インフラ所管省庁からヒアリングを受ける形で状況把握を実施し、情報セキュリティ政策会議に報告することを想定している。

(9)　今後の予定

○ 事務局より説明

－以　上－