資料 4

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 4 回会合議事要旨

1．日時　平成 17 年 11 月 1 日(火)　13：00～17：00

2．場所　経済産業省別館 10 階　第 1028 号会議室

3．出席者

[委員]

浅野　正一郎　委員長　(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)
稲垣　隆一　委員　(弁護士)
岩田　隆　委員　((社) 日本ガス協会)
大場　満　委員　(東京地下鉄 (株))
雄川　一彦　委員　(日本電信電話 (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))
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))
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)
森田　元　委員　((株) 日本航空)

(五十音順)

[政府]

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・情報室課長補佐
厚生労働省健康局水道課長補佐
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
国土交通省政策統括官付政策調整官
国土交通省航空局管制保安部保安企画課新システム技術企画官
国土交通省鉄道局危機管理室長

4．議事概要

(1) 論点説明に関して
○ 事務局より説明

(2) 委員意見開陳
○ 安全基準等の位置づけについて。今回の案では「それぞれの事業分野で最低限必要となる情報セキュリティ対策の水準」との記述となっており、以前の「最低限必要となる及び望ましい」に比べ、「望ましい」という文言が落ちている。指針として出された際に「最低限」として規定されてしまうと、満たしてない部分についての引き上げ労力が発生することが予想されるため、「望ましい」という言葉を残して頂きたい。

○ それぞれ法律で決められている部分は、「最低限」という文言でも良いが、これにプラスして各事業者等において守った方が良いと思われる指針の中に高い目標等が書かれる可能性があるのなら、この部分に対しては「最低限」或いは「望ましい」という文言を入れて頂きたい。

○ 実際にセキュリティ対策の現場で、色々なシステムの基盤の種類等がある中、対策を推進している。障害を起こす技術、ハッキング技術も日進月歩なため、少し高めのハードルを目指してどんどんやって行っており、基準もアップデートしていくということを日々感じている観点で言えば、むしろ「最低限」プラス「望ましい」ということを入れ、ポジティブに捉えるということが望ましい。

○ 最低限必要となる基準等に反映されるような情報セキュリティ対策の水準に対する表現については、指針との整合性を見るべき。

○ 「安全基準」、「個人情報の保護」、「情報セキュリティマネジメント」の話について、JIS

の国内規格では「水準」という言葉は使っていない。基準というのは一つの安全を保証するための「セキュリティレベル」を意味し、これを決めているものであって、恐らく「安全基準等」とカッコ書きをしたために、それにあたるような言葉というので「水準」というのを敢えて使ったと思うが、ここでは「水準」という文言を使わずに表現した方が良い。

○ 「安全基準等の策定若しくは見直しにおける遵守事項」とあるが、「遵守」という「法令を守る」という厳しい表現となっている。業界によっても異なるため、「遵守」という言葉を使って良いのか否か、他の分野の委員に確認する必要があるのではないか。

○ 国民の側からすると、「遵守する」ではなく、例えば「留意する」という表現を用いると、インフラ業者が自分で責任を負うということに加え、「国は留意するだけで良い」ということに対して責任を負うということを意味する。さらに「やる」といっておきながら、骨抜きにした責任は当然問われることになる。

○ 「遵守」とは、必ず守らなければならない、かなり具体性のある約束事を指し示すものであり、記されている事項はかなり一般的で幅があり、かつ何を守るのかが明確に書かれていない。したがって、「遵守」という言葉は適切ではない。そこに「遵守」と書かれると、少し業界の中でまごつくのではないかと懸念される。

○ 安全基準等の策定及び見直しにおける「リスク分析」は外れた形になっているが、外してはいけない。セキュリティについては責任の観点から言うと、このリスク分析こそが従うべき基準を選択する合理性を基礎付けるものであり、さらに取るべき対処策の合理性を基礎付けるわけであって、このようなプロセスが必ず仕組みの中に存在するはず。それを載せないのは奇異。

○ 上記の「リスク分析」がなければ、次項目の「対策項目及び実施レベルの明示」に繋がらない。リスク分析は色々な手法があり、脆弱性と周りの脅威、情報資産の価値の判断とする方法もあれば、criteria と比較を行いながら、ギャップを見ていくというやり方もあり、何かの形でリスク分析のプロセスを実施することが必要。

○ 情報提供の方法において。「・・・その重要度や種類、性格等に応じた情報の流れが」という箇所の「情報の流れ」という文言が解り難い。この意味というのは情報共有範囲、情報を受けた際にそれをどこまで共有できるのか、組織の中だけなのか若しくは第三者に出せるのか等を明確にした方が良い。

○ 所管官庁から事業者への情報の流れのパスに関しては、現在各々の所管官庁が持っているパスを最大限に活用するというのが基本的な考え方。もし現段階でパスがないあるいは機能していないのであれば、その際には新たなパスを考えれば良い。

○ 情報連絡の対象となるIT障害の分類表において。サービス停止、不能とか、サイバー攻撃に関わるインシデントが幾つか挙げられているが、予兆現象と実際の障害とが混在されているように見受けられるので、表の内容をもう少し整理した方が良い。

○ 情報連絡の対象となる IT 障害の分類表は、この内容の細かさから見て、必ずしも行動計画に添付する必要はないのではないか。実際には、後の段階で演習等を通じ、実績を積みながら、ブラッシュアップしつつ見直していくべきものではないか。

○ 情報連絡の対象となるIT障害の分類表については、各事業者がこの分類に従って報告することが可能かどうかと言うことをしっかり検証しなければ、この内容で本当に良いのか否かが判断できないと考える。

○ IT 障害の分類をどこで決めるのか、いつ決定されるのかと言うことが明示されていないことに問題があるのではないか。したがって、新たな行動計画において、分類を例示として引用する箇所で、踏まえるべき決定機関及びプロセスなりを明確に記述した方が良い。

○ 情報共有･分析機能を有する機関が設置された時に他の機関との関係を通じて発生し得る、情報の流出等の問題に対する責任論が出てくることが予想されるため、法人格を取得する必要も検討する必要があるのではないか。加えて構成員の責任をどう決めるのかの問題もあり、これら機関について何らかの法的根拠付けが必要になると思われる。

○ 情報共有･分析機能を有する機関の設立にあたっては、国による実効的かつ財政的な支援も必要との記述もあったほうが良いのではないか。

○ 設立に向けての支援は、それぞれ行政側の事情もあるだろうし、そこは解釈できる範囲で支援をしていくということが適切ではないか。各々の重要インフラ分野の特性や事情に応じたことに係るため、一律的に財政上の支援を行う、ということは書くべきでない。

○ 情報共有･分析機能を有する機関の設置については、業界によっては非常に有効で大いにメリットがあると思われるが、一方で、当該機関を作っても、各社独自のハードウエア構成あるいはソフトウエアの特徴を持っており、殆ど共有する情報が見当たらないことを踏まえると、設置についての理解がなかなか難しい。したがって、事業者で設置あるいは運営の費用負担を行うことは非常に受け入れ難い。

○ 情報の共有ということについて、共有すべき情報は当然あると考えている。しかしながら、現状では一般的に分野内の事業者同士では既に共有できているところが多いのではないか、と考えている。各々の事業者で使われているシステムは、目的に類似性

があるにしても、各々の作り方等は個々に別々。今以上に共有することに意味があるのか、と言われれば、その必要性があまり理解されないのでは、と感じる。

○ 情報共有・分析機能を有する機関の設置について、既存の組織で出来る・出来ないはともかく、先ずは構築し、その上で、それぞれ微調整をしていくことが重要。各事業分野においては、各々の歴史や行政手法は色々とあろうが、新しい取り組みを官民一体となって行うといった時に、あとは「主務官庁がやる」、「やらされる重要インフラも今までどおりやる」ということであれば、制度的に生産関係にならないし、それでは国民に対して非常にまずいのではないか。

○ 情報セキュリティについては民間事業者の自主性に任せ、国がとやかく言わずに済むのが理想である。逆に国が財政面で支援することになると、最終的にはそのやり方に口を出さざるを得なくなってしまう。もちろん、金を出さないと決めるのであれば、口を出さなくとも円滑に回るよう、国が陰に陽にさまざまな支援を行うことが必要となる。

○ やると言った以上は全員が協力し、体制を構築する。それに伴う負担は皆が負って当然という発想でなければ、結局現状の課題を解決できない。

○ 組織運営するには「人」、「金」、「時間」が必要であり、そういうものが流れるしくみを作るということはしっかりと謳うべき。例えばこれは国民の金が流れるわけだから、国民に対し運営については適正にやっているということを組織が立証するのは当たり前の話である。

○ 複数の主務大臣の監督を受けている企業において、大きな企業であればあるほど、その情報の流れはこれら省庁間で意外と同期されていない。したがって、横串となる組織が必要であり、その担い手もマネージャーレベルから従業員等のいわゆる現場レベルまで含めた情報共有体制あるいは少なくとも情報の流れの中にそのような人達を参加させて、将来このような組織を作っていくことが有用。

(3)今後の予定

○ 事務局より説明

－以　上－