

資料6

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31回会合議事要旨（案）

1 日時 平成25年3月26日（火）10:00～11:50

2 場所 内閣府本府仮設庁舎講堂

3 出席者

（委員）

浅野 正一郎 委員長（情報・システム研究機構 国立情報学研究所 教授）

稲垣 隆一 委員（弁護士）

井上 健一 委員（日本放送協会）

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 教授）

木内 舞 委員（一般財団法人 電力中央研究所）

岸野 広也 委員（代理出席）（一般社団法人 日本ガス協会）

阪上 啓二 委員（野村ホールディングス（株））

佐藤 昌志 委員（電気事業連合会）

鈴木 毅 委員（代理出席）（一般社団法人 日本損害保険協会）

鈴木 信 委員（公益財団法人 金融情報システムセンター）

関沢 雅士 委員（株東京証券取引所）

土居 範久 委員（慶應義塾大学 名誉教授）

留岡 正男 委員（代理人出席）（東京地下鉄（株））

中尾 康二 委員（KDDI 株式会社）

長島 雅夫 委員（日本電信電話（株））

永島 公明 委員（代理人出席）（（社）日本水道協会）

早貸 淳子 委員（一般財団法人 JPCERT コーディネーションセンター）

深澤 孝治 委員（（株）セブン銀行）

福島 雅哉 委員（定期航空協会）

松崎 吉伸 委員（（株）インターネットイニシアティブ）

松田 栄之 委員（新日本有限責任監査法人）

松橋 孝範 委員（住友生命保険（相））

三林 宏幸 委員 (東日本旅客鉄道(株))
吉岡 克成 委員 (横浜国立大学 准教授)

(政府)

内閣審議官

内閣参事官

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

厚生労働省 政策統括官付社会保障担当参事官室

厚生労働省 健康局水道課

経済産業省 商務情報政策局情報セキュリティ政策室

国土交通省 総合政策局情報政策課情報危機管理室

国土交通省 総合政策局情報政策課企画室

防衛省 運用企画局情報通信・研究課情報保証室

4 議事概要

(1) 内閣審議官挨拶

(2) 委員長挨拶

(3) 議事内容

①議事次第に基づき、以下の議題について事務局より資料に基づき説明。

○ 議題1：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」策定にあたっての指針(対策編)の改定について(資料2-1～資料2-2)

○ 議題2：第2次行動計画に基づく2012年度施策進捗状況について

(資料3-1～資料5)

○ 議題3：次期行動計画の検討について(資料6-1～資料6-3)

②委員意見開陳

<議題1>

○資料2-1のNo.22とNo.20(7)は、ほぼ同じご意見だが、意見に対する考え方の記載内容が違うので、どちらかに統一した方が良い。

○(システムの冗長化につき、システムを要素に分解して対策が記載されているとの事務局説明に対し、)システムというのは、要素に分解しても全部を包括して行うのがシステムなので、観点が変われば把握の仕方が変わってくる面があり、今後検討する上では問題ないが、もう少し記載しておかないといけない。

○No.5 の内容では、冗長化はハードウェアとネットワークだけだと定義し、後程の情報システムでは全体の中にアプリケーションが入っており、アプリケーションそのものについては冗長化していないとしている。No.15 の未然防止措置の所で「情報システムの多重化、通信回線の冗長化」を「情報システム・通信回線の冗長化」に直すことにしているが、ここでの兼ね合いを良く考えて記載しないと厳しいように思う。

○資料 2-2 の P20 「(イ) 外部委託実施における情報セキュリティ確保対策の徹底【要検討事項】」「○基本契約の締結」中「・契約内容の遵守状況を委託元が確認できる事項」とあり、基本契約の中に委託元が遵守状況を確認できる何かを定めるとする時、一般的にわかり難い。「契約内容の遵守状況を委託元に開示すること」という書き振りの方がわかり易いのではないか。「責任の明確化と合意形成が明示されるべき」と書かれおり、もう少し具体的な配慮が必要ではないか。

○P20 「・契約内容が遵守されない場合の対処手順（損害賠償請求）」についても法務の人が見た場合に混乱するのではないか。手順となるとより具体的になりかつ、損害賠償請求となると具体的にすべき。対処手順の意味をもう少し日常的な言葉に書き換えると良い。「遵守されない場合には、責任を確実に果たすこと」「責任を追及すること」を合意事項とすべき。

○P17 の「(エ) 内部関係者による脅威への対策【要検討事項】」「○内部関係者による情報漏えいを抑止するための措置」に幾つか記載があり、最後に「・責任の確実な追及」を入れるべきではないか。国土交通省が西宮事故を総括した時に、故意のヒューマンエラーを追及しており、情報セキュリティについても明確な責任の追及が必要ではないか。

○(対策編の事務局説明に対し、)本当に使えるのか気になる。全体を見えている人は問題ないと思うが、そうでない人は色々な文献を探したり、コンサルタントを雇ったりしないといけないが、そういうことを想定しているのか。

<議題3>

○重要インフラの定義に関し、今検討されているマイナンバーの問題があり、小売り等で消費税の徴税活動を系統的に連携させ国の下で行うが、徴税主体に対するサービスを行うことになる。国民に一番近い所の事業者が国の活動にサービスを提供する形になり、国の活動を文言として入れる必要があるかどうか検討すべきではないか。具体的には、重要インフラの定義の中に事業が形成する国民生活とあり、形成する国

の活動、3行目に「我が国の国民生活」とあり、我が国の活動及び国民生活という検討をすべき。

○大規模な災害発生時の国民を守る観点から、コンビニエンスストアチェーンを加えることを検討してはどうか。

○地震が起きた後、被災地で一番早く立ち上がっていたのはコンビニエンスチェーンで、高度に情報化されており消費が直ぐ活動に結び付く所があり、非常に大きなシステムで動いており、このような小売り・サプライチェーンといったものを考えるべき。

○(情報セキュリティ対策上、マイナンバーの基幹システムを一次的に利用する自治体に関する事務局説明に対し、)私の視点でも国、自治体も入っている。マイナンバー法制上、例えば消費税徴収業者は財務省への報告義務を負うことになるが、(重要インフラの定義上)どこまでが含まれるのかを整理しなければならない。これを行って頂く際は、内閣が一定のリーダーシップを果たすという認識を持って頂きたい。

○重要インフラ分野の対象について、資料 6-1 の中の関係主体に関し、関係主体の中に大学等の研究機関というのが入る可能性があるのか、既に入っているという認識か。

○安全基準等の対策編というのは具体的に何を行おうとしているのか。先週、ヨーロッパで重要インフラのプロジェクトがEUであり、重要インフラの中でユースケースを引き出し、要求事項やリスク・脅威の事実を精査して具体的な対策を導入する中に攻撃成功事例、詳細解析、侵入検知や、重要インフラ事業の中の脆弱性自動探査を行っている。EU の会議と今日伺った内容とに大分ギャップがある。安全基準等で謳っている最新の脅威のヒアリングや演習等、もう少しスペシフィックな重要インフラの特性を加味しながら、ユースケースのリスク分析があると思うが、もう一步国として進めていった方が良いのではないか。

(4) その他

○〈議題1〉について、委員の意見等の改定案への反映について、事務局で現状を調査し、適切な内容に書き換えることが出来るか検討し、検討結果を各委員に修正案を以て確認・了承を頂くこと、〈議題3〉について、委員の意見等の配布資料への反映として、必要な修正を行い、委員長及び発言委員等に確認、了承を頂くこと。

○ 次回を開催時期を6月頃に予定する。

(以 上)