資料２

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32回会合議事要旨（案）

１　日時　平成２５年６月２０日（木）１４：００～１５：４０

２　場所　中央合同庁舎4号館　12階　共用1208号特別会議室

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　名誉教授）
稲垣　隆一　　委員　（弁護士）
太田　英雄　　委員　（代理出席）（公益社団法人　日本水道協会）
大高　利夫　　委員　（神奈川県藤沢市）
大林　厚臣　　委員　（慶應義塾大学大学院　教授）
木内　　舞　　委員　（一般財団法人　電力中央研究所）
岸野　洋也　　委員　（一般社団法人　日本ガス協会）
小林　圭治　　委員　（一般社団法人　日本民営鉄道協会）
阪上　啓二　　委員　（野村ホールディングス株式会社）
佐藤　昌志　　委員　（電気事業連合会）
鈴木　　毅　　委員　（一般社団法人　日本損害保険協会）
関沢　雅士　　委員　（株式会社東京証券取引所）
谷合　通宏　　委員　（代理出席）（株式会社みずほ銀行）
土居　範久　　委員　（慶應義塾大学　名誉教授）
中尾　康二　　委員　（KDDI株式会社）
長島　雅夫　　委員　（日本電信電話株式会社）
永瀬　裕伸　　委員　（日通情報システム株式会社）
西村　敏信　　委員　（公益財団法人　金融情報システムセンター）
深澤　孝治　　委員　（株式会社セブン銀行）
松崎　吉伸　　委員　（株式会社ｲﾝﾀｰﾈｯﾄｲﾆｼｱﾃｨﾌﾞ）
松橋　孝範　　委員　（住友生命保険相互会社）
吉岡　克成　　委員　（横浜国立大学大学院　准教授）
渡辺　研司　　委員　（名古屋工業大学大学院　教授）

（政府）

内閣官房副長官補
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
経済産業省　ガス安全室
国土交通省　総合政策局情報政策課情報危機管理官
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　航空局安全部安全企画課
国土交通省　鉄道局総務課危機管理室
気象庁　　予報部業務課

４　議事内容

（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、以下の報告・議題について事務局より資料に基づき説明。

○報告1：2012年度補完調査（資料４）
報告2：サイバーセキュリティ戦略等について（資料５－１、５－２）
○議題：次期行動計画の検討について（資料２、３）

②委員意見開陳

<報告1>

○言葉の使い方だが、資料４の「ホームページ」とは何を指すのか。「トップページ」、「Webページ」という言葉も出てくる。これは止めた方が良い。

○事例１について、１度メールサーバを乗っ取ってから詐称メールを出すという流れだが、詐称メールを出すこと自体は、サーバを乗っ取らなくてもできる。今回のケースはサーバを乗っ取っているが、攻撃としてどういう意図・魂胆があるのか分かっているのか。信用のおける機関のメールサーバでは、受信側メールサーバでの認証などスパムメール対策を行う可能性があるので、より適切な送信元から送られたメールと見せ掛けるためではないか。

〇資料４のP6（１）について、気付きとして利用されたメールアドレスについて、システム管理者が覚知し、システム管理者が対策を講じるべきとあるが、組織によってセキュリティ対策やリスク管理の体制は様々であり、リスクを認識する主体や対策をする主体が誰であるかは組織で決まっている。
　本件はリスクを認識する主体が誰で対策するのが誰かという点の気付きに見えるが、システム管理者がリスクを認識し独自に対策するという考え方を示すものと読んではいけない。一般的なリスク管理に際し、リスク管理者はリスクを把握するための情報をシステム管理者にも与え、システム管理者が把握したリスクをリスク管理者にも伝えるという流れをスムースにするべきだという理解か。

〇再確認だが、質問の趣旨は非常に実際的で、組織内でリスク情報の共有を図るべき、システム管理者もリスクを認識し対策に関する情報共有をすべきということは分かるが、資料を率直に読むと、リスク管理者に属するシステム管理者が独自に対策をするべきという趣旨に見えるが、そうではないという理解で良いか。

〇今回の補完調査の対象の絞り込みについて、全体の案件の中からどのような観点でこの４件を選んだのか書いて頂きたい。

〇補完調査の対象事案の概要はあるが、１つ１つの中でインシデントに繋がったのか繋がらなかったのかは記載し難いので書いていないのか。クリティカルな状況で何が起こっていたのか。

〇P15の事例３の気付きで、１度侵入されてバックアップからデータを戻す際の手順で、確認を確実に行うとあるが、マルウェアの難読化が行われている例もあり実際には不可能に近い。
　書くとすれば、バックドアプログラムが仕掛けられている可能性を考慮するとか、ファイル変換をすると大抵のマルウェアは機能しなくなるので、例えばjpegからpngなどのファイル変換が有効とか、技術的な補足が必要ならこういった手段も併記する必要があるのではないか。「確認する」ことは現実的ではない。

〇補完調査の目的が、第２次行動計画の結果の評価をより実態に即するためとあるが、事例の収集と検討結果、行動計画の評価に対してどう影響したのか見えない。何らかの形で補充して貰えると有り難い。

〇行動計画のアウトカムの評価は難しい。この様な調査をアウトカムの評価にしようとしているのかどうか。アウトカムの評価とは何かという質問だが、一定の環境では評価できるのだろうが環境が変わると評価も変わる。

〈討議〉
〇事務局の説明で、平時・非常時という言い方があった。サイバーインシデントは大抵平時に起こっている。非常時というのは何か。東日本大震災の様なものが非常時なのか、平時のインシデントがどの程度大きくなったものを言うのか、平時のインシデントがどの程度大きくなったものを言うのかその辺りの境界点をサイバー検知の観点から、少し考えて行かなければならない。

〇インシデントのハンドリングについて、国際的な標準を色々な人と話していることと少し違っている。インシデントは事故。小さいものから大規模なものまである。事故の起きたタイミングで何かをしなければならない時の対応はインシデントレスポンスで、そこに書かれているのは平常時の対応なので、定常的に平時に何をしなければならないのかは、一般的にどの様な状態を監視しなければならないのか、これに対して、どの様なレポートを上げなければならないのかを押えておかなければならないと理解している。書く時はイメージを余りずらさずに書いて頂きたい。

〇重要インフラの分野や重要なシステムの選択の仕方で、10分野を闇雲に増やす必要はないと思う。少し柔軟的に、場合によっては入れ替えてみたり、優先順位をつけたりして少しメリハリをつけないと、並列的に運用しているにも関わらず、戦略的に広く遍くというのは対応が分散的になる。

〇重要システムの定義は、当初は事業者が自発的に出してきたものをリストアップしてきたが、これからは客観的にインシデントのあった時に国民生活や社会生活にどれだけのインパクトがあるのかなど、原因がサイバーなのか障害なのかに限らず、インパクトのあるものを選んでいく。少し客観的なクライテリアを作っておき、付け加えるとすればシステムが止まった時のインパクトを考え、その原因に関わらず止まった時のインパクトの大きいものを重要システムとして選びそれを管轄する事業者が重要インフラ事業者として入ってくる。これを毎年あるいは数年のタームで見直していく形で柔軟に対応して行かないといけないのではないか。これは準インフラ業者のような予備軍の形での位置付があってもいいのでは。

〇安全基準のところ、最低基準については概ね出来ているという評価になると思うが、我が国の経済活動や国民生活を支えているインフラに対しては、第三者なり事業者がこれまで行ってきたことを評価し公表するということを検討しても良いのではないか。

〇先程の事務局の（韓国の事例の）説明で、政府の中でレベルを上げたことや国民性とか政府の組織体制等々を勘案した上で詳しく調べ、追随すべきか否かを良く考えた方が良い。

ネットワークを全て監視できる国、毎日Webサイトのトップページを数回チェックするという様な国と同等なセキュリティを(我が国が)持っているとは思えず、その点は十分な配慮が必要。

○(資料2)P6の制御系のところで、右端の上から２段目に「『重要インフラ事業者等とサイバー空間関連事業者との脆弱性情報や攻撃情報の情報共有等による連携の促進』は、一般的な情報共有ではないものとして整理すべき。」とある。(書き振りとして、)脆弱性、攻撃情報といった情報について、制御系はIPA、JPCERT/CCでハンドリングをしており、情報系にプラスしてそのWeb系を行っている。同じスキームの中でハンドリングを変えるという形で取っている。そこへ制御系をどうするかということに関しては経済産業省が考えているので、P6の右端の２段目の一番下にある通り、所管省庁と要調整を図るとの程度の言葉で良いのではないか。

○P4の民間における情報共有のところなど、その課題の中で共有を困難にする事情について、共有を阻害する要素を検討することや可及的にこれを解消することなど、情報共有を組織的に進められるような体制を整備するといった項が欲しい。

情報共有は大事であり、本当に企業が経営レベルでその持っている資産で組織的にやろうとしたときに、制度基盤をしっかり整備をしておかないといけない。

少なくとも業法を持つ者は業法の中に、情報共有の仕掛けを少なくとも(業法等の)中に入れるなどしておかないと機能しなくなるのではないか。主務官庁の関係での吸い上げ、吸い上げがセブターに限られた場所であるならその場について、業法上の機能を持たす形で整備して頂きたい。

○制御系の話があったが、例えば、制御系のシステムがあり、そこに脆弱性があると。私の理解では、重要インフラ(事業者)の何処かに何らかの不正メールが侵入して、汎用サーバを乗っ取り、そこから一般的なルートで制御系の普通のAPIを叩いて落としていると理解。制御系に脆弱性がある無しに関係なく入っていると思った。重要インフラの事案として検討されている中では、制御系の脆弱性を衝いてきて入ってきているのか。

（４）その他

○次期行動計画について、項目毎に残されている検討点を整理、行動計画の素案に落とし込む作業を始める。論点が残る項目については、選択肢の整理も行う。

○次回会合の開催時期は９月頃を予定する。

（以　上）