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13回会合議事要旨

1 日時 平成20年1月31日(木) 14:30～16:30

2 場所 三田共用会議所講堂

3 出席者

[委員]

浅野 正一郎 委員長 (国立情報学研究所 教授)
赤石 良治 委員 (東日本旅客鉄道(株))
稲垣 隆一 委員 (弁護士)
岩田 隆 委員 ((社)日本ガス協会)
大林 厚臣 委員 (慶応義塾大学教授)
雄川 一彦 委員 (日本電信電話(株))
小幡 篤 委員 (三井住友海上火災保険(株))
金澤 亨 委員 (野村ホールディングス(株))
九萬原 敏巳 委員 (電気事業連合会)
黒沢 昌幸 委員 ((株)日本航空インターナショナル)
郡山 信 委員 ((財)金融情報システムセンター)
小山 正嘉 委員 (三菱東京UFJ銀行)
田口 靖 委員 ((社)日本水道協会)
田中 正史 委員 (全日本空輸(株))
中尾 康二 委員 (KDDI(株))
永瀬 裕伸 委員 (日本通運株式会社)
早貸 淳子 委員 (有限責任中間法人 JPCERT コーディネーションセンター)
広瀬 雅行 委員 ((株)東京証券取引所)
森山 拓哉 委員 (住友生命保険相互会社)

[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(防災担当) 政策統括官(防災担当)付地震・火山対策担当参事官(代理)
警 察 庁 警備局警備企画課長

金　融　庁　総務企画局参事官（代理）
総　務　省　情報通信政策局情報セキュリティ対策室長
総　務　省　自治行政局地域情報政策室長（代理）
厚生労働省　政策統括官付社会保障担当参事官（代理）
厚生労働省　医政局　研究開発振興課　医療機器・情報室長（代理）
経済産業省　原子力安全・保安院　電力安全課長
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　情報管理部情報安全・調査課情報危機管理室長
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　政策統括官付参事官（物流政策）付（代理）
国土交通省　鉄道局危機管理室長（代理）
防　衛　省　運用企画局情報通信・研究課情報保証室長（代理）

4　議事要旨
（1）論点説明に関して

○　事務局より説明

（2）委員意見開陳

○　重要インフラの全分野で安全基準等の見直しが行われ、指針をトリガーとした分野横断的なPDCAサイクルが動き出したことが確認できたので、このサイクルがセキュリティレベルの底上げのツールとして有効に機能することが期待される。

○　航空分野においては、昨今、IT の活用、範囲が拡大してきているが、事業者としては、航空券の電子化については、すでにこの安全基準等の対象内としてチェックしている。また、鉄道事業者としては、昨今の事象に対し、業務継続計画、BCPの観点からは比較的適切な対応をとることが出来たものと考えており、行動計画で定義されている「国民生活または社会経済活動に多大なる影響を及ぼすおそれが生じるもの」とは異なるものと考えている。

○　指針の見直しに関連し、IPv4のアドレスの枯渇が言われているのは事実であるが、必ずしも IPv6へ移行することだけが対策として決まっているのではなく、今、色々な対策が検討されている段階であることに注意が必要である。また、システムについては、ミニマムにとらわれて全体を捉えることができず、システムとして全体的には不十分なものになってしまうということはよくあることなので、「きめ細かさ」や「品質向上」にとどまらず、信頼性向上、という視点が必要。さらに、情報漏えいに関しては、防止するだけではなく、漏えいの被害を最小化する

ための取り組みも重要。

○　CEPTOAR-Council については、今は意見を出し合っている段階であるので、自由闊達な意見のやり取りの中で、できることから始めるというのが筋道でないか。

○　演習については、少し実際に近い形になってきているが、参加している事業者全てのサーバーが攻撃を受けてしまうというようなものではなく、一部の事業者が攻撃を受けたというシナリオで、その影響を受けていない参加事業者が、その状況でどういった対応をしていくのかということも演習での検証とした方がもう少し色々なデータが取れて良かったのではないか。

○　行動計画の見直しの論点を整理する上で、共有する情報の利用者、あるいは共有する情報をどう利用するか、誰がどういうタイミングで利用していくのか、どういう利用の仕方が必要なのか、という視点で論点を洗い出す必要がある。今の段階ではいかに情報を共有できるのか、出してもらえるのかという視点を比較的重視して考えていくという形にならざるを得ないのではないか。

○　警察庁としては、テロ対策や危機管理を所掌する官庁として有するノウハウや情報をもって分野横断的演習に貢献できると考えているし、都道府県警察と重要インフラ事業者との間で、サイバーテロ共同対処訓練等を着実に積み重ねていくこととしている。現実の IT 障害発生時には事案対処省庁も絡んでくるのであり、事案対処省庁との連携に際して必要な課題は何か、事案対処省庁側も民の側も、現行動計画の枠組みを作る際に、何が障害になったのかを洗い出し、それを克服していく努力、取組みが必要。

○　重要インフラのサービスが根本的に脆弱性を抱えているインターネットにどれだけ依存する傾向にあるのかといったことについて継続的に監視しておく必要がある。

○　行動計画の見直しを検討するにあたり、目標が事前防止なのか、再発防止なのか、あるいは何か起こった時の機能回復まで含めた行動をすべきなのかということも含めた上での検討をするべきではないか。

○　情報セキュリティ対策に関して「費用対効果」が論点となるが、現場担当としては、リスク管理の概念とコンプライアンスとがほとんど同質化してしまい、コストとリスクを比べての取捨選択ができず、現実には選択肢がなくなっているというのが実感。とらないと許してもらえない対策が増えすぎている気がしており、こういった視点を改めてもう少し整理する必要があるというのが、現場の率直な思い。また、技術的な側面からの検討だけでなく、経営の観点からリ

スク管理や情報セキュリティというものについてトップダウン的に整理する必要もあるのではないか。

○　法的な視点から捉え直すと、重要インフラの情報セキュリティ対策を実現するための情報連携、あるいは情報セキュリティ対策を行うための労働法制の検討を入れるべきではないか。

○　情報セキュリティセンターの機能を発揮するためにはどうしたらいいのかを考えるべき。そのためには、国民から見えやすい、国民に対してどういう行動をすれば国民はそれに対して歓迎するのかということを分析しておかなければならないのではないか。