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
技術戦略専門委員会
第 17 回会合議事要旨

１．日時　平成２３年４月１１日（月）１５：００～１７：００

２．場所　中央合同庁舎第４号館共用１２１４特別会議室

３．出席者

［委員長］
後藤 滋樹（早稲田大学教授）
［委員］
阿草 清滋（名古屋大学大学院教授）
小柳 和子（情報セキュリティ大学院大学教授）
志方 俊之（帝京大学教授）
田尾 陽一（セコム株式会社顧問）
宮川 晋（NTT コミュニケーションズ株式会社　先端 IP アーキテクチャセンタ・経営企画部（兼務）担当部長）

（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内閣審議官
内閣官房情報セキュリティセンター内閣参事官
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
（内閣府政策統括官付代理参事官付）

議事概要

（1） 後藤委員長　挨拶

（2） 今回の技術戦略の検討課題について

【事務局より資料に沿って説明】

（3） 委員・補佐官コメント

○　ディペンダブルというのは、これまでのいわゆるRASに代表されるようなアベイラビリティやリライアビリティとは異なり、セキュリティやセーフティを含めてディペンダビリティという言葉を使っているので、「信頼性の高い（ディペンダブルな）」という言葉に違和感を感じるが、国民目線からその方が分かりやすいというのであれば、このままでよい。

○　「震災」を踏まえて「災害復興」というキーワードが出てきたものと理解している。現場において気になるのは、例えば二次バックアップを行わずに一次バックアップのみで運用するなど、バックアップ系が節電に回されることである。節電によってウィークネスを発生させるべきではない。また、データや機能の疎開を行う考え方もあるが、これは当該データのアクセスコントロールに問題が発生する可能性がある。しかし、緊急時にやむを得ない対策として実行する可能性も否定できない。このように具体的なイメージにより、「災害復興」と情報セキュリティが結びつくと考える。キーワードとなる「節電」と「分散化」については、ディペンダビリティを向上させるために検討する必要がある。

　ただこれは、民間単独でも実行可能かもしれない。重点投資に関する国の動き方は十分検討するべきである。

○　今回の震災において、リスクマネジメント概念がないと思う。計画停電に関しても、どういう計画性を持って、あるいは停電時のリスクを正しく検討して実施する必要がある。

○　リスクマネジメント、アクシデントマネジメントの分野を盛り込んだ方がよい。また、省エネや高度交通システムは、民でもかなり追究すると思うが、国は民がやらないようなことを追究した方がよい。

○　リスクマネジメントは言うなれば、どのリスクに対してはプロテクトし、どのリスクは受容するというかを考えることにある。今回の震災を踏まえると、リスクマネジメントのリスクの対象に、セキュリティの分野だけではないリスクを入れてみてもよいと思う。どのシステムに対してお金をかけるかということのコンセプトの違いというのは、まさにリスクマネジメントの考え方の違いから起きていると思う。

○補佐官：　いわゆるリスクマネジメントとか、あるいはクライシスマネジメントをもう少し前に出した方がいいと思う。特に、リスクマネジメントの中でリスクコミュニケーションは非常に重要になってきており盛り込んだ方がよい。

○　危機管理の観点で情報をコントロールするためのマネジメントと、現場の社員を守るための情報伝達のマネジメントの両方が必要である。

○　電力を流す者も、しっかりとしたアクシデントマネジメント的なプログラムに従って流していき、足りなくなったらその分だけは分散していくといった守りの姿勢のセキュリティも必要である。

○補佐官：　セキュリティの概念は広がってきており、また広がっていかなければいけないと思う。まず現状では、ディペンダビリティを考える上で、不正や故意いかんに関わらず両方含めて考えようという動きになっている。また、ＩＴのアプリケーションの安全性は当然考えなければいけないので、そこを組み込みながらＩＴの方を考えていく時期になっている。さらに、動的なリスク・動的なセキュリティを含めて考える時期になっていると思う。

○補佐官：　１日に何度も計画停電が実施されることは想定外となっている。重要インフラにおいて、実際にシステムがどういう運用をするかを今こそ見直すいい機会であると思う。

　また、ＶＭによる機能の疎開もこの契機に加速するのではないかと思う。その際のセキュアな移動や、情報のアクセスに関する権限について整理しておくと、加速する前に先回りしてチェックができると思う。

○　重要インフラなどの基幹系だけでなく、身近な自分のパソコンのセキュリティ向上の実感の沸く施策が必要である。

○　「⑤攻撃者の行動分析等による予防基盤技術」において、緊急対応型の分野もやっていただきたい。例えば、攻撃したら損をするという防御的なものも考えてもよいと思う。

○　緊急対応型の分野として、重要インフラを防護する上で局所的な対処をするのではなく、キャリア間のネットワークを連携して止めるなどのオペレーションを国が支援して実施してもよいと思う。また、攻撃者を黙らせるというオペレーションの研究も必要であると思う。

○　クラウドのセキュリティを向上させることにより、利用者側でのセキュリティも向上することができる。

○　サイバーセキュリティとフィジカルセキュリティは表裏一体であり、全体としてセキュリティを考える必要がある。

　また、最近は海外のデータベースを使っており、知らないうちにデータがどこにあるかわからないといった状況では不安が増大する。

○補佐官：　クラウドの話をどこかに記述すべきである。

○　「重要分野のコンセプト」において、事件を発生させるのは攻撃者だけではないので、重要分野のコンセプトを見直した方がよい。

○　⑦のプライバシ情報は医療の情報よりも、震災により戸籍が流されたといった事例の方が重要であると思う。

○補佐官：　プライバシのリスクは他のリスクとのトレードを考える必要があり、状況に応じて変わっていく。

○　節電も含め、３月11日の前後で、評価の考え方のエバリュエーションが変わったと思う。ダイナミックにエバリュエーションを変えてもいいと思う。

○補佐官：　評価の変化に対応できるような仕組みが必要である。

（４）今後のスケジュールについて

○事務局：　貴重な御意見を踏まえ、今回の震災を考慮して構成の見直しなどの作業をさせていただきたい。これからも引き続き、御指導、御鞭撻をお願いいたします。

以上