# 高度情報通信ネットワーク社会推進戦略本部 情報セキュリティ専門調査会
# 情報セキュリティ基本問題委員会 第２分科会
# 第４回会合 議事要旨

１　日時　　平成 17 年 1 月 21 日（金） 9:00～12:00

２　場所　　内閣府本府　地下講堂

３　出席者

（委員）

浅野正一郎（座長）（情報・システム研究機構　国立情報学研究所教授）
石幡　吉則（電気事業連合会情報通信部長）［代理］
板橋　功（財団法人　公共政策調査会第一研究室長）
稲垣　隆一（弁護士）
大場　満（東京地下鉄株式会社　鉄道本部安全・技術部長）
雄川　一彦（日本電信電話株式会社　第二部門担当部長）
喜入　博（KPMG ビジネスアシュアランス株式会社　顧問）
郡山　信（財団法人　金融情報システムセンター監査安全部長）
小林　俊徳（社団法人　日本ガス協会技術部長）［代理］
中尾　康二（KDDI 株式会社　技術開発本部情報セキュリティ技術部長）
廣川　聡美（横須賀市企画調整部情報政策担当部長）
前川　徹（早稲田大学　国際情報通信研究センター客員教授
　　／株式会社　富士通総研主任研究員）
松尾　明（中央青山監査法人代表社員）
三輪　信雄（株式会社　ラック代表取締役社長）
森田　元（株式会社　日本航空 IT 戦略企画室部長）

（五十音順、敬称略）

（政府）

内閣官房情報セキュリティ対策推進室長
内閣官房情報セキュリティ対策推進室情報セキュリティ補佐官
内閣官房情報セキュリティ対策推進室内閣参事官
警察庁警備局警備企画課
警察庁情報通信局情報技術解析課
防衛庁長官官房情報通信課情報保証室
金融庁総務企画局

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
総務省自治行政局自治政策課地域情報政策室
法務省大臣官房秘書課情報管理室
厚生労働省医政局研究開発振興課医療技術情報推進室
経済産業省商務情報政策局情報セキュリティ政策室
経済産業省原子力安全保安院電力安全課
経済産業省原子力安全保安院ガス安全課
国土交通省総合政策局情報管理部情報企画課

4　議事概要

（1）　重要インフラ事業者ヒアリング結果について

○　事務局より説明

（2）　重要インフラにおける情報セキュリティ対策の今後の方向性に係る論点整理（案）について

○　事務局より説明

（3）　委員意見開陳

○　「IT 事故」という表現は、適切でないような気がする。まだ「IT 事件・事故」というと、事件性もあり事故も含まれる感じが出る。いずれにせよ、国民経済社会とかに重大な影響を及ぼす重要インフラの問題なため、危機管理的な視点を含めて、もう少しそれにふさわしい用語にした方が良いのではないか。

○　個人的には「IT 障害」あたりが落としどころだと考えているが、具体的にはどういう事を指しているのか、という例示がないために、皆のコンセンサスが得難い可能性があるのではないか。IT に起因する障害の例示を示すべき。

○　インフラのシステムが与える影響という観点で考えてみると、「事件」だとか「事故」だとかは限定したようなイメージの言葉ではなく、例えば長時間のサービス停止、誤ったデータの送出、あるいは、他社の情報システムに対して誤ったデータを送信してしまったとか、等の影響が非常に大きい。即ち、今まで色々と社会的問題となってきたものの中の多くは、色々な攻撃というよりも、むしろ障害に起因するものが多かったように思う。そういった意味で、「IT に関する障害」であるだとか、「IT インシデント」等の言葉で纏められた方が良い。

○　重要インフラに関する議論であるため、国全体として取組むべきという姿勢、関係官庁の能力向上を論点整理に盛込むべき。

○　情報の相互依存性を前提として、どういう枠組みを作り、情報を相互連携するかの構造において、その担い手として、先ずは各府省庁が有する情報セキュリティ

に関する取組を強化することが重要。それを第１分科会で議論した政府内の体制と情報共有していくことが必要ではないか。

○　どの程度のレベルでの情報共有を行うか、という観点でいえば、合意に基づいて提供するということが想定されていると思うが、国民に対するあるいは国際的かつ構造的な担保という意味では、それぞれの事業者の意志に任せて情報共有する構造を作る、いうのでは脆弱。

○　法制化となると、この提言としては大きな問題になってしまい、なかなか悩ましい部分もあるが、構造的に堅固な仕組みを作っていく、という趣旨の提言にしてはどうか。

○　例示ももちろん必要だが、例えば、制御系において何が起こるとかは、今まで想定されてなかったり、思っていても具体的には考えられていなかったこと等も色々あるのではないか。即ち、そのようなアン・イクスペクティッドなインシデントに関するリサーチをする組織があっても良い。

○　各分野においても必要なリスク対策がとられているが、その内容をみると、各分野で共通的なものがある一方で、分野によって異なるところもある。個別の分野という観点からみれば、自ら可能なものはできる限りの対策を講じている現状を鑑みると、「重要インフラ相互の依存がサービス維持のために必須」の部分には違和感がある。

○　今回はあくまで全体の具体策の方向性についての検討であり、個別の分野から見た場合については、今後議論されるもの、と認識。

○　障害が発生した場合には、違法行為、あるいは過失、事故といったことがわからないが、違法行為として認定される過失もあるということを視野に入れてほしい。

○　基本的に重要インフラ間で可能な限り情報共有を行う。さらに、その解析結果を踏まえて、優先度の高いものは優先的に情報共有し、対策の向上に資するべき。

○　重要インフラの情報システムへの依存度が高まっているという事実を「重要インフラにおける情報セキュリティ対策の視点」の中に入れるべき。

○　重要インフラの国際性とセキュリティの観点を入れるべき。時間的に議論がまとまらないのであれば、宿題として残しておくべき。コスト論についても同様。

（４）その他

○　事務局より，次回会合の予定について説明。

－ 以 上 －