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５回会合 議事要旨

１　日時　　平成 17 年 2 月 17 日（木） 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）
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）
土居　範久（中央大学　理工学部教授）
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）
渡辺　研司（長岡技術科学大学　経営情報系助教授）

（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）　第４回情報セキュリティ基本問題委員会における審議結果の報告

○　事務局より説明

（２）　重要インフラが直面する脅威の具体像（サイバー攻撃を中心として）について

○　三輪委員より説明

（３）　重要インフラ間の相互依存性解析の有効性について

○　渡辺委員より説明

（４）　第２次提言における対策の具体化項目（案）の検討について

○　事務局より説明

（５）　委員意見開陳

○　重要インフラ障害の復旧、拡大防止、再発防止の流れというものと、一方で犯罪の予防・捜査といった、警察への取り組みへの協力といった関係整理の問題について、違法行為があれば、手続きに従って対応するのは当然のことであり、当然のこととして心配をすると、返って誤解を生み弊害を招くのではないか。

○　従来の進め方で何ら問題がなければ、重要インフラの部分は、サービスの維持・復旧を一番大きな目的として進めていきたい。

○　重要インフラに何らかの障害が発生した場合に、復旧、拡大防止等を時系列で行い、その過程で違法行為の可能性が出たら、その段階で通報するという表現にすべき。

○　危機管理という視点から、この重要インフラ障害の復旧、拡大防止、再発防止の

流れという中には、当然、恣意的な攻撃に対する被害拡大の防止あるいは再発防止の流れは当然入っているはずであり、別に考えるのは、逆に不自然。

○ 重要インフラを安全に運用していくためには、復旧したり、被害の拡大を防止したり、発生を防止したりすることが非常に重要であり、そこに必要な情報収集とか共有が必要。この流れで進めていくべき。

○ 事業法では、既に主管省庁に対して、事故等が起きた場合には報告を行うという義務があり、現場では安全を第一に、速やかに復旧ということは当然ながらなされる。その一方で、もう一つ別の通報口が必要だということになると、現場としては非常に大きな負担と成り、混乱を招く恐れがある。

○ 事件の防止策という観点で見た場合、恣意性を持ったもの、単なる障害に起因するものとを分けて、議論するのが一般的。それに対し、事件発生後の復旧となると、これは、恣意的あるいは障害によるものにかかわらず、第一に復旧というのが現実問題であり、復旧の過程で恣意性を持ったものという疑いをもたれてくると、それなりの対処を取るというのが現実的と思われる。

○ 情報共有が一方的な情報提供の流れになると機能しなくなるので避けるべき。

○ 障害発生時に事業継続性を優先するという安全対策の流れと、犯罪の防止、犯罪捜査の流れは分けて整理するべき。

○ ログの保全は、あくまでも重要インフラ事業者が主体となって判断するものであるべき。

○ サイバーテロのヒントとなりうる情報が公開されることは問題であるため、セキュリティ案件の一般への情報公開は注意して行うべき。

○ ISAC という特定の組織が必ずしも必要というわけではなく、業界内にある既存の仕組みを利用して、事業者の負担を十分に配慮しつつ、情報共有の仕組みを検討するべき。

○ 官民連携組織それぞれの役割分担は、現場の動きやすさ等の実務の観点から明確化していくべき。

○ 重要インフラの対象範囲として、システムインテグレータ、IT ベンダーも入れるか否かについて検討することは重要である。

○ 具体的な方策実施に係るコストの観点から、その実行可能性を突き詰めて、検証をしっかりと行っていく必要がある。

○ 平時あるいは緊急時において、いかに現場で重要インフラ事業者が動きやすい体制を作るということが一番。基本的な視点として、インフラ事業者の皆さんがどうすれば事業者が動きやすいのか、その上で政府がどういった体制にすべきか、という、あくまで事業者からの観点を忘れてはならない。

○ 重要インフラ分野を見直す際に、「ＳＣＭを実現する基盤」というのがあるが、非常に分かりにくい、「物流」という方が明解ではないか。

○　SCM（サプライチェーンマネージメント）を実現する場合、SCM は生産から物流、販売まで入るため、省庁における所管の範囲が明確でない。したがって、当該分野を例えば「物流」と置き換えたとしても、曖昧さは変わらないため、具体的な対応が出来ない可能性がある。

（6）　その他

○　事務局より，次回会合の予定について説明。

－ 以 上 －