次世代の情報セキュリティ政策に関する研究会（第６回）議事要旨

１　日時

平成２０年４月３日（木）１０：００～１２：００

２　場所

中央合同庁舎第７号館　共用会議室－１

３　出席者

（１）構成員（敬称略、五十音順）

新井 悠（㈱ラック）、有村 浩一（テレコム・アイザック・ジャパン）、綾塚 保夫（㈱NTT ドコモ）、飯塚 久夫（NEC ビッグローブ㈱）、小倉 博行（三菱電機㈱）、加藤 朗（慶応義塾大学大学院）、木村 孝（ニフティ㈱）、小屋 晋吾（トレンドマイクロ㈱）、小山 覚（㈱NTTPC コミュニケーションズ）、齋藤 衛（㈱インターネットイニシアティブ）、佐田 昌博（㈱ウィルコム）、篠田 陽一（北陸先端科学技術大学院大学）、下村 正洋（NPO 日本ネットワークセキュリティ協会）、高倉 弘喜（京都大学）、高橋 正和（マイクロソフト㈱）、手塚 悟（㈱日立製作所）、中尾 康二（KDDI㈱）、則房 雅也（日本電気㈱）、福智 道一（ソフトバンク BB㈱）、藤井 俊郎（松下電器産業㈱）、藤本 正代（富士ゼロックス㈱）、水越 一郎（東日本電信電話㈱）、安田 浩（東京電機大学）、山内 正（㈱シマンテック総合研究所）、横田 孝弘（KDDI㈱）、渡辺 芳明（日本アイ・ビー・エム㈱（徳田構成員代理））

（２）事務局

中田政策統括官、松井官房審議官、鈴木総合政策課長、竹内電気通信技術システム課長、柳島データ通信課企画官、河内情報セキュリティ対策室長、村上情報セキュリティ対策室課長補佐

（３）その他発表者

NTT コミュニケーションズ㈱

４　議事

（１）開会

（２）議事

⑴中間報告書について

⑵重点的に検討・実施すべき事項の具体化について

⑶自由討議

（３）その他

（４）閉会

５　議事概要

（１）開会

座長より、構成員変更の案内があった。

旧）菅 隆志（三菱電機㈱）

新）小倉 博行（三菱電機㈱）

中田政策統括官より挨拶があった。

事務局より、第５回会合の議事要旨につき説明が行われた。

（２）議事

(1)中間報告書について

事務局より、資料 6-2 に基づき説明が行われた。

（主な質疑）

・(P.48)「a-Japan」とは何か。

⇒2015 年以降をどのように呼ぶかは議論のあるところだと思う。呼称や定義については議論をさせていただいていないところ、当該記述については削除させていただきたい。

・(P.48)「何もしなくても個人向け情報発信」とあるが、どのような意味か。

⇒適格な表現に修正させていただきたい。

(2)重点的に検討・実施すべき事項の具体化について

ア. T-ISAC-J モデル（事業者間連携スキーム）2.0　官民連携スキーム 2.0 に関する考察（有村構成員）

資料 6-5 に基づき、説明が行われた。

（主な質疑）

・情報共有のメンバーにユーザ企業も入ると良いのではないか。提供する側と利用する側のリスク・コミュニケーションとして、共有された情報がメリットとして利用者側に提供される。近年では、企業の中でも情報セキュリティの専門家が育ってきており、そのようなことが十分可能になってきている。

⇒近年、各社の CSIRT 連携が活発化している。また、重要インフラ分野における CEPTOAR（情報共有・分析機能）も整備された。金融 CEPTOAR 等は、電気通信事業者から見れば顧客とも言え、そういう意味では利用者側の情報共有コミュニティの整備が着実に進展していると言える。今後は、それぞれのコミュニティがどのように連携するかが重要となる。

・事業者間の情報共有は重要であるが、無秩序に行われると非常に危険。事業者間

の情報共有に関するガイドラインはまだないため、そのようなガイドラインがあると事業者としても情報共有がしやすくなる。

・インシデント対応のフェーズは次の段階に入ってきている。問題は脅威の質の変化であり、動機のプロフェッショナル化とビジネスモデルの下で行われる各種攻撃に対して、今までのレベルでの情報共有では対応できない。社会的コンセンサスも含めた新しいルールが必要になっているのではないか。

・業界連携という切り口でお話いただいたが、それぞれの調査や対策において必要な専門家を適時加えていく柔軟さが、テレコム・アイザックの１つの成功モデルだったのではないか。今後、攻撃が複雑化していく中で、状況を把握するためにはいろいろなレイヤーの専門家の目が必要となるため、異業種間連携がより重要になる。

・テレコム・アイザックの枠組みが１番動きやすかったということだと思うが、事業者以外の人や海外との連携等、本当はもう少し広いスコープが必要になるのではないか。

⇒それを否定するわけではないが、１番動きやすかったテレコム・アイザックでさえ、今や危うくなってきているという現状がある。

・攻撃がビジネスモデル化しているという中で、ICT 分野の枠組みだけで解決できる問題ではなくなってきているのではないか。社会の仕組みとして検討することが重要。

・競争のある民間企業の場合、顧客は被害に遭ったことを出さないでほしいと思うため、インシデント情報を公表することはなかなか難しい。逆に国の場合には、国民はむしろ被害に遭ったことを公表してほしいと思っているのだから、国こそがそういった情報を率先して出すべきではないか。

・テレコム・アイザックの成功モデルは、情報共有というよりは、同じ要望を持ち、同じロジカルな判断ができる人たちが、同じ威力をもった対処を一斉にできたというところにあると思っている。現在動けなくなってきている原因は、そもそも当事者が誰なのか、どのような技術要件があるか、誰が対策に動くのが適切なのかという焦点が絞れなくなっているためではないか。そういった意味で、第三者的な立場からの効果測定まで含めたスキームを考える必要がある。

・例えば、暗号を使うことにより、自分がどのような情報を持っているかを相手に教えずに、相手と共通のインシデントを体験したかどうかといったことを調べることができる、テクニカルな解決方法がある。そういった技術を活用することで、より高度な情報共有が可能になるのではないか。

・テレコム分野の CEPTOAR は、テレコム・アイザックとほぼ対応していると考えてよいのだが、非常に良く機能している。他の重要インフラと比較しても、そこは誇っても良いところだと思う。

・情報共有がうまくいかないというのは、日本だけではなく、海外も同様である。国際の場では、Information sharing よりも、Joint activity や collaborative activity というほうがメインで議論されている。テレコム・アイザックはある意味それを地で行った組織だと思っている。情報共有だけを念頭に置いていると、いつか壁にぶつかるのではないか。

イ. 新たな安全・簡単アイデンティティ管理体系　セキュア・アイデンティティ流通基盤（NTT コミュニケーションズ）

資料 6-6 に基づき説明が行われた。

（主な質疑）

・一種のシングルサインオンに近い形だと思った。ID の管理という意味では便利だが、逆にそれを盗られたら全て盗られてしまう。このスキームを入れる際には、それに対応したしっかりとした認証が必要になる。

・社会としてこういうシステム１つだけを取り込んでいくというのは非常に危険。リスク分散を当人の意思でできなくなる。あくまで選択肢の１つとして考えていく必要がある。

・ID 管理の問題は、プライバシー等の問題と密接に関連している。社会として ID 管理に関するコンセンサスを得るとか、みんなに理解してもらえる技術的裏付けだとか、そういう土壌が整わないと難しいだろう。通信や情報セキュリティというコンテキストで語るには、まだ早いのではないか。

・このようなスキームがソフト的に可能かどうかをまず議論しなければいけない。暗号化の安全性については、技術的に担保する必要がある。

・識別子である「identifier」と属性情報を含む「identity」とがある。現状、identity を管理するための体系ができていないため、フレームワークや要求事項を整理しているところ。フォーカスを流通基盤だけではなく、identity をどのように管理するかというところにも当てなければならない。そういう意味で、もっと幅広にいろいろなセキュリティを考えていかなければならない。

・技術には技術で対抗するしかないという側面がある。そのためには、もっとセキュリティ技術のイノベーションが必要。事業者は膨大な設備負担等のため、R&D のための余裕がない。政府としても研究開発のための予算措置等の支援が必要。

・ID の管理だけが取り上げられていて、属性情報の問題にフォーカスが当たっていない。例えば、１８歳未満が入れないサイトに対して、自分を特定する情報を全部出してしまって良いのか。１つまたは少数の ID で管理していく場合、自分が誰であるかまでは識別できず、ただ有資格者であることだけが分かるような方法を考えていかなければならない。

⑶自由討議

なし。

（３）その他

事務局より、今後のスケジュールにつき説明が行われた。

（４）閉会