次世代の情報セキュリティ政策に関する研究会（第８回）議事要旨

１　日時

平成２０年５月２３日（金）９：３０～１２：００

２　場所

三田共用会議所 第４特別会議室

３　出席者

（１）構成員（敬称略、五十音順）

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）、下村 正洋（NPO 日本ネットワークセキュリティ協会）、鈴木 和幸（㈱ウィルコム（佐田構成員代理））、高倉 弘喜（京都大学）、高橋 郁夫（弁護士）、高橋 一行（トレンドマイクロ㈱（小屋構成員代理））、高橋 正和（マイクロソフト㈱）、手塚 悟（㈱日立製作所）、徳田 敏文（日本アイ・ビー・エム㈱）、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）

（２）事務局

中田政策統括官、松井官房審議官、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、長屋情報セキュリティ対策室対策係長

（３）発表者

㈱セキュアブレイン、日本電気㈱

４　議事

（１）開会

（２）議事

⑴ 中間報告書の意見募集結果について

⑵ モバイル環境及び Linux システムにおける Malware の脅威について

⑶ ISP の活動と通信の秘密について

⑷ 自由討議

（３）その他

（４）閉会

５　議事概要

（１）開会

事務局より、第７回会合の議事要旨につき説明が行われた。

（２）議事

(1)中間報告書の意見募集結果について

事務局より、資料 8-2 に基づき説明が行われ、パブリックコメントに対する研究会の考え方につき、構成員の合意が得られた。

(2)モバイル環境及びLinux システムにおけるMalware の脅威について

ア.モバイル環境におけるMalware 等の調査（㈱セキュアブレイン）

資料 8-3 に基づき説明が行われた。

（主な質疑）

・「脅威のシナリオ」とあるが、PC においては画像を使った攻撃というものが発生してきている。モバイルにおいても、プロフ等ユーザがプッシュできる画像サイトが多くあるため、そういうところから何かフックがかけられるといった脅威も考えられる。

・Bluetooth を使ったMalware の収集という話があったが、実現可能性は別として、駅の改札において行うと効果的ではないか。携帯電話に定期券の機能が組み込まれていたり、何より通行量が圧倒的に多いため、非常に効率的だと思う。

イ.Linux システムにおけるMalware の脅威に関する調査研究（日本電気㈱）

資料 8-4 に基づき説明が行われた。

（主な質疑）

・攻撃の手法にもいろいろあると思うが、手動と自動とどちらのタイプのものが多いのか。

⇒今回のケースで言うと、ツールを使って攻撃を仕掛けてくるのだが、侵入者自身が手動でそのツールを動かしているケースが多かったと考えられる。

・研究開発等、総務省主導でやるべきこととして、どのようなことが考えられるか。

⇒今、総務省でセキュア VM というプロジェクトをやっているが、そういった技術の活用が考えられる。また、現状では、Linux 用のアンチウイルスソフトを開発しようとしても、ディストリビューション等の違いによってそのままでは動かないといったことがある。オープンソースにおいても、ベンダが標準的にアンチウイルスの機能を埋め込めるような、仕様の標準化が必要ではないか。

(3)ISP の活動と通信の秘密について

ア.ISP の活動と「通信の秘密」（高橋郁夫構成員）

資料 8-5 に基づき説明が行われた。

（主な質疑）

・P.46 に「大量通信等ガイドライン」「帯域制御の運用基準に関するガイドライン」が列挙されているが、当該ガイドラインは政府の公式見解ではなく、民間の自主的ガイドラインである。

⇒当該ガイドラインのアプローチは、これまでの流れとは違ってきている。政府の公式見解ではないが、電気通信事業者等に対する影響力は大きいものであり、その限りにおいて、近時の見直しの傾向を示すものとして記載しているところ。

⇒そういう意味では、総務省では迷惑メールに関する OP25B ついて見解を示しており、そちらのほうが適切ではないか。

・電気通信事業者に管理する権利を与えた場合、一方で、管理する責任・義務も電気通信事業者に発生するのではないか。利用者にリスクを伝える義務や、事案が発生した際の責任といったものをどのように考えれば良いか。

⇒ネットワーク管理というものに関しては、ある意味全てが程度問題ではないか。法執行機関との関係もそうだし、通信データの部分について ISP がどのような形でどの程度コントロールできるかといった部分もある。ただし、ISP が一定の役割を果たすことを認める以上は、行為規範を定め、少なくとも事後的に検証できる仕組みにすべき。ISP が一定の役割を果たす中で、バランスをどのようにとっていくかということは、今後の最大のテーマではないか。

・通信の内容をリアルタイムと記録に分けて議論しているが、記録については、ISP はどのような形で記録を保存すれば良いのか。また、ユーザとしては記録を取られることの抵抗感もあると思う。例えば、普段は誰も見ることができないが法執行機関の許可があった際に該当する記録だけが見ることができるといったような、技術面の議論というのも必要になってくるのか。

⇒少なくとも法律のレベルだと、各 ISP は自らのビジネスとして任意にやっていると思う。EU では、National security との関係もあり、データ保全が義務付けられている。ただし、各国において、実務としてどの程度実装されていて、どのような影響を及ぼしているかについては、まだ調査が及んでいない。

⇒データを保全することはとても難しい問題で、何%取得しなければいけないか、データの完全性を誰が保障するかといったことがあり、例えばそれを電気通信事業者に義務付けるとすると大変なことになると思う。どの程度までやる必要があるかということに関しては、何らかのガイドラインや枠組みを国が提示する必要があるのではないか。

・原則論として、自由でオープンなインターネットということも大事だとは思うが、社会・経済活動を健全に維持するためには、おそらく今の日本の仕組みでは難しいのではないか。自由に対する責任と、利用者も含めたその責任に伴うコスト負担に関する議論は、本研究会とは別のところでということになるかと思うが、継続していただきたい。

・P.48 に「定義の明確化」とあるが、定義の明確化はぜひしていただきたい。少なくとも「窃用」の概念を明確化しないことには、次のアクションに結び付かないのではないか。また、この定義については、電気通信事業法の逐条解説のような形で整理されないと、どうしても使いづらい。

・他国の電気通信事業者が、日常の運用の中で、法律とどう折り合いをつけながら、どのように対応しているかという点については、電気通信事業者側としても、向こうの事業者団体や ISP との繋がりといった部分で、協力できるかもしれない。

・電気通信事業者の観点として、１．事業者設備に支障を与えるような通信への対応、２．受信した設備が異常をきたすような通信への対応があるかと思うが、P.8 の表の中では、こういった観点はどこに含まれるのか。

⇒普通の解釈本のレベルでは、そこまでは記載されておらず、調査が及んでいない。

・ITU-T における標準化で、電気通信事業者のための情報セキュリティマネジメントガイドラインの勧告化を行った際、通信の秘密（secrecy of communications）をガイドラインの項目に入れたのだが、その言葉を使っているのは英国と日本だけだったため、通信を交換する際に見えた情報を外に出してはいけないという nondisclosure of communications に用語を変更したということがあった。法制度等の調査を行う際には、このようなアクティビティの場でアンケートをするという方法も考えられるのではないか。

⇒海外の比較調査では、世界的なフレームワークの基準となるような国の制度を徹底的に調べ、日本と比較したときに問題となるようなところについて各国にアンケートを実施し、さらにより細かく調査する必要がある部分については現地に赴くという手法が、最もうまくいく手法だと思っている。

⑷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