次世代の情報セキュリティ政策に関する研究会（第５回）議事要旨

１　日時

平成２０年３月６日（木）１０：００～１２：００

２　場所

総務省第１特別会議室

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㈱（菅構成員代理））、小野寺 匠（マイクロソフト㈱（高橋構成員代理））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）、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）、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㈱）、水越 一郎（東日本電信電話㈱）、安田 浩（東京電機大学）、山口 英（奈良先端科学技術大学院大学）、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、柳島データ通信課企画官、荒木電気通信技術システム課企画係長、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、田邉情報セキュリティ対策室対策係長

４　議事

（１）開会

（２）議事

⑴ 今後の情報セキュリティに関する課題等について

⑵ 中間報告書の骨子について

⑶ 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４回会合の議事録につき説明が行われた。

（２）議事

⑴今後の情報セキュリティに関する脅威及び課題等について

ア．近い将来の情報セキュリティ～第四世代移動通信とユビキタスの視点から～（綾塚構成員）

資料 5-2 に基づき、説明が行われた。

（主な質疑）

・ウイルス届出件数がここ数年減少傾向にあるが、どのような理由からか。

⇒IPA セキュリティセンターの公開データであるため、特段の知見を持っているわけではないが、一般的には、従来はウイルスを撒き散らすことが攻撃としてよく行われていたのに対して、昨今では数ではなく特定の個人に対して攻撃を集中的に行っていくというような傾向にあると言われている。そういった傾向の表れなのではないかと推測している。

・「技術的な対策とともに、国際的な連携策も有効と考えられる」との記述があるが、具体的にどのような国際連携策をイメージされているのか。

⇒様々な形で発生しているインシデント情報を共有し、協力して対策を推進していくような取組が考えられる。攻撃を受ける側で対策を打つのには限界があり、攻撃を出している側で対策をするようなことも含めて、検討していく必要がある。

・「端末のオープン化」というのは、どのような意味か。

⇒ここで述べているのは、「端末プラットフォームのオープン化」という意味。様々なアプリケーションを自由に入れることができるような端末が出てきている。

・インターネット側の視点で言うと、境界防御というのはすでに有効に機能していない。もう少し、モバイル環境ならではの対策を考えていく必要があるのではないか。

・ボットも含め、踏み台にされる等、リソースが勝手に攻撃に利用される事例が増えてきている。ユビキタスデバイスに関しても、踏み台にされて他人に迷惑をかける可能性があるということを視野に入れていく必要があるのではないか。

イ．巧妙化する malware の現状（高倉構成員）

資料 5-3 に基づき、説明が行われた。

（主な質疑）

・Allaple 自体の動作の１つとして、エストニアの特定の IP に対して DDoS をするというものがあり、昨年エストニアにおいて非常に大きなインシデントがあっ

たところだが、そういった挙動もこの分析においては確認されているのか。

⇒そういう機能は全く確認できなかった。解析者をごまかすためにばら撒いているバージョンは、とにかくゴミだらけ。しかし、数万のうち１コか２コ変わったモノが含まれており、それらを上手く使って攻撃をしているのではないかとみている。それは普通に解析をしていると追いつかない。

・端末の機能やネットワークの速度等から、例えばある国、テリトリーにおける攻撃力というのは計算できるのか。

⇒乗っ取ったマシンがどういう環境にあってどこまで破壊力を持っているかを調べ上げた上で、ピンポイントでねらいを定めて DDoS 攻撃をかけるといったことが行われている。日本はかなりブロードバンドが普及しているので、一般家庭の端末１台１台も相当な破壊力を持っているものと推測される。

・「国内観測網の必要性」とあるが、情報がなければ対策が講じがたいというのは確かだが、どのようなものを想定しているのか。

⇒以前であれば、ハニーポットを置いておけば向こうからハッカーが繋がってきてくれたが、最近はどちらかというと、Web にマルウェアを置いておいて、ユーザが踏むと発症し、踏んだ後はマルウェアが消えてしまうというような、我々の方からアクティブに動かないと見えない状態になっていることが分かっている。自ら地雷を踏みに行くような追跡システムが必要。情報不足の１番の問題は、SE、CE の技術力不足である。何故かというと、顧客企業でのトラブルシューティング時に得られた貴重な経験データを、会社に持って帰って若手 SE の教育に使っていいかと聞くと、大体の会社はノーという。若手が実データに触れる環境が全くないものだから、経験が全く積めない。

ウ. 今後の情報通信環境の変化に対して必要となる情報セキュリティに関する取組

（福智構成員）

資料 5-4 に基づき、説明が行われた。

（主な質疑）

・セキュリティに関する競争原理の導入について、通常の市場競争は評価の軸が定まっているのに対して、セキュリティに関しては指標が定まっていないため、そのような評価軸を検討してからでないと、競争原理そのものがうまく動かないのではないか。その上で、商売としての市場競争と、セキュリティ上の市場競争の関係、例えば市場は取っているがセキュリティは低いだとか、またその逆といった状況をどう考えていくか、または、ユーザに考えてもらうような情報発信やまとめ方をしないと、全体としてうまく動かないのではないか。

⇒おっしゃるとおり。この場で申し上げたかったのは、単一のシステム仕様環境においては、Single Point of Failure になりやすいという側面から、市場

における競争関係が大切だということ。その次の段階としてセキュリティの競争というのがあって、その前段として評価制度が必要となるというのは、まさにそのとおり。

・セキュリティ対策の責任は供給者側が負うべきというところについて、個々のユーザを守る、或いはそれぞれの製品のセキュリティ度を上げるという意味での責任は当然供給側にあるというのは分かるのだが、逆に、例えばボットに感染していて CCC から連絡がいっても、自分は困っていないので何も対応しないという人たちに対して、そういう人たちをシャットアウトして他の人を守るという考え方もあると思うのだが、事業者側の責任というのは、どのあたりまでを想定しているのか。

⇒例えば CCC から連絡を受けた人が対応をしなかったからといって ISP が悪いかといったら、そうではない。セキュリティ対策は、ある部分は ISP がやる、ある部分は PC ベンダがやるというように、階層的にやらなければいけない。そういった総合的な枠組みを作る必要がある。通信事業者や ISP が１人で頑張っても無理なわけで、そういった意味ではベストエフォートを重層的に積み上げることによって、全体で維持していくということを考えなければならないのではないか。

⑵中間報告書骨子（案）

資料 5-5 に基づき、事務局より説明が行われた。

⑶自由討議

「中間報告書骨子（案）」に関しての意見交換が行われた。

（詳細は別記）

（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

６　自由討議概要

自由討議における主な議論は以下のとおり。

・産業界と政府の役割分担をどう考えるかいう点は、厚く書いたほうが良いのではないか。例えば、2003 年や 2004 年の頃は、まだセキュリティに関しての取組というのは薄く、そのような中では政府が多くの気付きを産業界に与えてきたが、昨今の市場の自由化と競争の結果を考えていくときに、セキュリティというところも含めて市場原理の中にしっかりと入り込むような形を作っていくということが必要だと思っている。そういう意味では、産業界の役割を明記するという議論も必要ではないかと思う。政府は産業界がうまく動けるための環境整備、例えば Telecom-ISAC Japan のような自律型機関の支援等を行っていく必要がある。

・犯罪の取締まりに関しても、検討項目として明記したほうが良いのはないか。現状は、セキュリティに関する技術的な議論が中心であるが、犯罪行為が増えてきているという現実があり、その中で ISP や消費者と警察の関係といったところを整理する必要があるのではないか。
・学術界の役割というのが、これまではあまり議論されてこなかったが、大学や研究機関の役割について言及しても良いのではないか。
・５年前、１０年前はこれほど犯罪組織に加担する技術者はいなかった。健全なセキュリティ技術に取り組む人たち、或いは技術者に対するインセンティブ向上策のようなことを明確に記載すべき。
・増幅するセキュリティリスクの実態は何なのかということを含めた、もう少し現状のセキュリティに対する本当の脅威を一般国民が分かるような啓発活動が、改めて必要になっている。
・迷惑メールが１番分かりやすいが、インターネットは自由で公平であることが大事だが、同時に社会のインフラとなった以上はそこに公益性・公共性が求められる。公益性・公共性を破る人たちに対する罰則の強化という視点があっても良いのではないか。
・個人認証や端末認証といったところは、ネットワークの中での重要な１つのファクターだと思うが、その関係で、その基盤となっている暗号の危殆化については、その現状をぜひ強調していただきたい。
・何が犯罪になるのか、例えばマルウェアを作ることが犯罪なのか、送信することが犯罪なのか、Web に置くことが犯罪なのかといったところが、整理されていない状況である。犯罪行為の定義も含め、法体系の整備についても追加していただきたい。
・現状では、犯罪にあっても警察に相談しても無駄だろうという無力感のようなものが市場に溢れているようなところがある。犯罪の被害にあったのだから被害届けを出さなければならないといったことを、もっと言っていかなければならないのではないか。
・海外からの攻撃のほうが多いという実態から、海外の警察とどう組んでいくか、国際連携の問題のほうが、我が国のセキュリティを考える上では重要ではないかと思う。
・NICT のトレースバック技術開発プロジェクトにおいて、技術面、運用面、法律面からの検討が進められているが、だいぶ実用化の目途が立ってきた。通信インフラとしての１つ仕組みという意味では、非常に重要なことであり、追記していただければと思う。
・悪いことをした人のアドレスや電話番号が技術的に分かったからと言って、誰が通信をしているかということを事業者が把握しているわけではない。事業形態、契約関係、公衆端末の存在等の関係であやふやになっている。犯罪への対策ということを考えていくのであれば、匿名性のある通信を許容するかどうか、その通信の記録に関する扱いをどうするかという議論を、もう１度しっかりする必要がある。
・利用者の役割に関する言及があるが、将来に渡って我々は利用者に何を期待するのか或いはしないのかということを議論した上で、その在り方を具体的に書いていったほうが

良いのではないか。これには２つあって、自衛は続くのか続かないのかという議論と、社会的責任、例えば踏み台になって他人に迷惑をかけている人を悪いと言えるのかという議論とがある。

・ユーザの役割をどのように考えるかというのは重要な議論だと思うが、ADR や第三者紛争解決機関のような紛争解決の仕掛けを作っていくべきではないか。例えば、この研究会の議論では届かないようないろいろな問題があるわけで、それを技術基準等ではなく、法律のような方法で、ダイナミックに適用できるフレームワークがあれば良い。また、プライバシーだとか消費者の権利といったことに対して、非常に過敏な社会になりつつあると感じており、そのようなところと、今起きているセキュリティのメカニズムというのは、非常に高度な技術のことであり、乖離が起きてきているところで、これはクラシックな紛争解決のスタイルでは解決しようがないのではないか。そういった意味でも、ADR や第三者紛争解決というのは考えるべきだと思っている。特に、個人の消費者の役割、プライバシーの保護、技術の高度化、紛争の複雑化といったあたりを加えていただければと思う。

・「事故状況等の報告の義務化」というのがあるが、これをもう少し強く書いても良いと思っている。Telecom-ISAC の活動から、情報共有なんていうのは実は幻想だったということを感じている。現在は同時に被害を受けるということもなくなってきており、状況が把握しづらくなってきていることを考えると、高度に変化していく環境の変化を踏まえ、事故状況等を第三者がしっかりと調査した上で、必要となる人に共有していくという、鉄道・航空でいうところの事故調査委員会のような仕組みが必要だと考えている。

・産業界が自発的に取組を行っていく上で、通信事業者にとっては正当業務行為の認識が非常に重要である。例えば、スパムメールを落とすことができればメールサーバの負荷も減ると思えば、金銭的な問題を言わずとも、セキュリティ対策がどんどん進む状況が生まれるかもしれない。そういったトライもできて競争も行えるという意味では、正当業務行為に関してきちんと議論する必要があると思う。

・大学のネットワークを管理していると、ISP と同じ状況で、ユーザは使う権利というのを強く主張する。どう見てもウイルスに感染しているというときによくやっているのは、ユーザに通知を出して１週間ほど観察させてもらい、経過を見た上で確実に感染しているということになったら、最後通告を出すという方法。ウイルスに感染しているかもしれないということを１度ユーザに通知し、ユーザが応じてくれなかったら少し様子を見るというところまで、ISP ができるようにしたほうが良いのではないか。本日の議論でも、すぐ切るか切らないかという話になっているが、それだとユーザが別の ISP に行ってしまうから困るという話になりそうな気がする。少し甘いのかもしれないが、そういう柔らかい対応ができれば良いのではないかと思う。