次世代の情報セキュリティ政策に関する研究会（第２回）議事要旨

１　日時

平成１９年１２月５日（水）１０：００～１２：００

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）

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㈱）、菅 隆志（三菱電機㈱）、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）、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）、横田 孝弘（KDDI㈱）

（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、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情報セキュリティに関する脅威及び課題等について

⑵研究会検討の方向性及び取りまとめ方法について

⑶自由討議

（３）その他

（４）閉会

５　議事概要

（１）開会

第１回会合を所用により欠席した中田政策統括官より挨拶があった。

事務局より、第１回会合の議事録につき説明が行われた。

（２）議事

(1)情報セキュリティに関する脅威及び課題等について

ア．最近のセキュリティ動向について（山内構成員）

資料 2-2 に基づき、説明が行われた。

（主な質疑）

・リスクの評価をどのように考えるか。

⇒リスクの評価とは、いろいろな脅威がある中で、それらが資産にどれだけのインパクトを与えるかということを定量化する作業であり、発生確率や損害額といった主観が入り込む。そこに、対応に割けるリソースを勘案し、優先付けを行うことになる。企業には全くリスクがないという状態はなく、考えうるリスクにどれだけしっかり対応しているかという姿勢が問われる。

・P.19 にある「グローバル・インテリジェント・ネットワーク」につき、他の組織との関係及びネットワーク自身の防護方法はどのようになっているか。

⇒ぜい弱性情報を収集している公的組織（CERT 等）等と情報交換をしている。解析技術に関しても、別コミュニティにおいて情報交換をしている。防護方法としては、ネットワークをいくつかにゾーン分けし、１番奥のゾーンに一旦入ったパソコンについては、外に持ち出す際にディスクを全部破壊する等の対応をしている。

イ．マルウェアの現況（新井構成員）

資料 2-3 に基づき、説明が行われた。

（主な質疑）

・P.18 における提案の中に、キープレイヤとして ISP が含まれているが、具体的にどのような期待をされているのか。

⇒ISP の提供している個人向けブログサービスの中にも、ブラックリストに指定されているブログがあった。このようなところにも注視していただければ。

・P.5、P.6 に収集に成功したウイルスの内訳があるが、「UNKNOWN」とされているものには、具体的にどのような行動をするものが含まれているのか。

⇒ほとんどが、ダウンローダ。ウイルスをダウンロードするだけのシンプルなマルウェアであるダウンローダを簡単に作れるソフトが売られており、そういったものを使ってダウンローダが作られた結果、多くが UNKNOWN となったものと考えられる。

・P.19 において、コード署名されたマルウェアがあるとのことだが、どのような手口でこのようなことができたのか。

⇒ペーパーカンパニーを設立し、正当なステップを踏んで証明書を取得するという手口がパソコンの世界であり、スマートフォンにも転用されているものと推測される。

・最終的にダウンロードされるものが従来通りのマルウェアであるならば、マルウェア対策システムにおいて対応できるはずであり、キープレイヤとして「情報セキュリティベンダ」が最も大きく書かれるべきだと思うが、いかがか。

⇒いろいろな方策が考えられ、そのような考え方も１つの方策だと思う。

ウ. 次世代情報セキュリティ対策について（小山構成員）

資料 2-4 に基づき、説明が行われた。

（主な質疑）

・リスクに関する広範な情報の集積と解析が必要だということが１つの合意点だと思うが、その方法として具体的なアイデアはあるか。

⇒データベースの作成者同士が連携し、関連情報を１箇所に集め、そのデータを分析・解析することで、考えをまとめていくことから始めてはどうか。

・レピュテーション DB を各社の DNS に反映させて、DNS を操作してリダイレクトするということか。

⇒具体的な方法までは考えが至っていないが、そのような方法も有効な手段だと考えている。

・ブラックリストを作成してフィルタリングをかけるという方法は、瞬間的には効果があると思うが、本質的な解決にはならないのではないか。

⇒対処療法と根治対策の両面から対策を実施する必要があると考えている。啓発活動と共に、ISP などの通信事業者でも対処療法的な対応をしていかなければならないのではないか。

⑵研究会検討の方向性及び取りまとめ方法について

資料 2-5 に基づき、事務局より説明が行われた。

⑶自由討議

研究会検討の方向性及び取りまとめ方法につき、意見交換が行われた。

（詳細は別記）

（３）その他

座長より構成員に対して、資料 2-5 論点５の表の作成に係る作業依頼がされた。

（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。

・議論のスコープの境界線はどこに設定しているのか。

⇒まずは、脅威や課題について幅広に捉えたいと考えている。重点化していく中で、総務省としてやるべきこと、民間としてやるべきことを少しずつ色分けしていきたい。

・ISP が情報セキュリティ対策として設備関連投資に費やしているコストは非常に大きなものであり、そのような実態も考慮していただきたい。

・資料 2-5 論点４において、情報セキュリティ対策の実施主体として、企業等と個人が利用者として一括りにされているが、企業と個人とでは守るべき資産や求められる対策も異なるため、企業等と個人を分けて考えたほうが良いのではないか。
・対策を実施する側だけではなく、脅威から守られる側の視点も取り入れ、両方の視点から検討する必要があるのではないか。

・資料 2-5 論点１に検討対象が提示されているが、地デジ、NGN、携帯電話の 4G 化等、今後求められる社会構造・産業構造の変化を踏まえ、２０１１年前後に必ず到来する環境の変化への対応、すなわち②を優先的に議論したほうが良いのではないか。
⇒研究会のアウトプットとして、現状の分析は必要なプロセスであり、まずは①につき検討することとしたい。

・今後増えることが予想される、情報リテラシーが非常に高く、ツールを駆使し、国境を越え、能動的に様々な情報にアクセスする個人に対する対応も懸念される。

・電気通信事業者は通信を止めることを非常にためらっているようだが、利用者保護の立場で行うフィルタリングを躊躇する理由を教えてほしい。
・事業者の設備を守るための帯域制御は、電気通信事業法上問題になりにくいのに対して、利用者保護のためのフィルタリングは、これまでの法解釈上実施しにくい現状がある。
・技術や脅威の進化に対する法整備のような体系整備が追いついていないため、本当に法に抵触しないかどうかの判断が難しく、フィルタ１つにも躊躇しているのではないか。
・インターネットの中立性、負担の公平性等の問題は、広い意味でのセキュリティの話ではあるが、総務省の他の研究会等でも議論されているところ。

・資料 2-5 論点５の表の作成にあたり、その対策のビジネスモデルにおける位置付け、法的な問題点も記載していただきたい。

・資料 2-5 論点４につき、インシデントレスポンスのような、何かが起こった際にどこと連携してどのように動くかといった観点を加えてほしい。
・インシデントレスポンスの観点を加えるとすると、資料 2-5 論点４の表には、時系列という新たな軸が加わるのではないか。
・インシデントレスポンスの際、何を信じて動けば良いかというのは、重要な視点である。