次世代ＩＰインフラ研究会
セキュリティＷＧ（第５回）議事要旨（案）

１　日　時：平成１７年4月２７日（水）１０：００～１２：００
２　場　所：総務省　９階　第三特別会議室
３　出席者：
〔ＷＧ構成員〕
新井構成員（村上代理）、飯塚構成員（サブリーダー）、歌代構成員、内田構成員、笠原構成員、加藤幹之構成員、加藤佳実構成員、桑子構成員、笹木構成員、佐々木構成員（グループリーダー）、武智構成員、手塚構成員、永瀬構成員、南浮構成員、藤谷構成員、星澤構成員、松島構成員（丹代代理）、森構成員
〔総務省〕
江嵜電気通信事業部長、金谷電気通信技術システム課長、吉田情報セキュリティ対策室長
〔事務局〕
坂巻データ通信課長、秋本データ通信課調査官、山路データ通信課課長補佐

４　議　事

セキュアブレイン　星澤構成員より、資料ＷＧ５－２（ボットネットのメカニズムについて）に沿って説明があった。主な意見は以下のとおり。

○：ボットをコントロールする人（以下「攻撃者」という）からすると、ボットはリソースになる。一度自分のものにしたボットを、他の攻撃者に使われないようにするためにセキュリティを強化するなど、乗っ取られた側は普段よりも安全になるとは考えられないのか。

○：一度支配下においたボットを使われないようにするというよりも、使えるボットを使うのではないか。

○：常時接続が普及しているが、家庭ではパソコンを使わない場合には電源を切ることを考えると、ゾンビ予備軍は、企業で使われていたパソコンのうち、管理されずに放置されているパソコンではないか。ネットワーク管理者がしっかりしている会社ではそのようなことがないと思うが、実態としてそのようなことがありうる。

○：振り込め詐欺対策と同様に、ゾンビ予備軍となるパソコンが減少するように社会的に啓発が必要。犯罪行為として取り締まるのもなかなか難しいため、攻めるほうが圧倒的に有利。

○：啓発は必要。ただ、５、６年前からウイルス対策の状況はあまり変わっておらず、啓発をしても興味のない人は見ないことから、啓発はなかなか難しい。

○：ＩＲＣサーバは、ダイナミックＤＮＳを使っているから特定することが難しい。フィッシングサイト同様、気がつくと違うところへ移るなどライフサイクルが短く、攻撃者が危険を感じると閉じてしまうことなどから、発見は困難。

○：ＩＰトレースバックでボットまではたどり着くことができると思うが、そこからＩＲＣサーバまでたどり着くのは、今の方式では難しいのではないか。それについても考えていかなければならないと思う。

検討報告（素案）の第１章について、事務局から説明の後、質疑。以下は主なやりとり。

○：「攻め」の方が「守り」よりもやりやすく、攻撃側の技術スキルも高い。そのため、ユーザのセキュリティを確保するため、まずはＩＳＰが対策を講じることが必要。ただ、そのための経費確保は問題。

○：最近では攻める側は、「技術」だけでなく「ソーシャルエンジニアリング」を活用して攻めてくる場合がある。米国ではソーシャルエンジニアリングに関する研究も進んでいるが、今後日本においても守る側のソーシャルエンジニアリングの研究が必要ではないか。ＩＳＡＣの支援だけではなく、研究についても記載して欲しい。

○：本文ｐ１０について、「ネットワーク感染型ワーム」という文言が使われているが、「ネットワーク攻撃型ワーム」とした方がよいのではないか。訳はきちんとしておいた方がよい。コンピュータにはワクチンソフトといわれているが、いまはワクチンソフトでも対応できないものも出てきている。

○：報告書のまとめ方によるが、それぞれの対策がばらばらにまとまっている。包括的な対策についてもう一歩踏み込めないか。対策を網羅的にまとめられないか。

○：力を入れてやるべき事、ＩＳＰや行政の役割分担について分類してまとめるのがよいのではないか。

検討報告（素案）の第２章について、事務局から説明の後、質疑。以下は主なやりとり。

○：この検討報告のとらえ方として、次世代のＩＰインフラとして、従来とは違うセキュリティ対策を検討している、というとらえ方をすればよいか、それとも、現状のセキュリティ課題を踏まえた上での対策を検討しているというとらえ方をすれば良いか。

○：序章などで、そもそも次世代ＩＰインフラ研究会で何故このテーマについて取り上げているかを説明する記述が必要なのではないか。

○：ｐ３３の表題が「政府による支援の必要性」となっている。人材育成についても政府の支援が触れられている。課題は、政府が支援する前に、企業やユーザ自身が解決すべき課題でもあるので、もっと大きな問題から落とし込むなどまとめ方を工夫してもらいたい。

○：第１章、第２章を通じて啓発の話が出ているが、守る側の啓発だけでなく、インシデントによって人が死ねば重い罰をうけるということを攻撃側に知らしめないといけないのではないか。

○：「必要である」という記述が多いが、「具体的な実施内容」に関する提言を記述することを検討してもよいと思う。

○：情報家電に関連しては、セキュリティ人材育成は、ＩＳＰやメーカーだけでなく、国民一般へのセキュリティ教育が重要。従来は「情報倫理」に関する教育はあったが、今後は「セキュリティ教育」として小学校などの単位に組み入れこむことも必要ではないか。

○：序章において、①　社会経済活動の重要インフラとなっているインターネット、特にインターネット接続サービス提供事業者（ＩＳＰ；Internet Service Provider）のネットワークを守る、②ＩＳＰによるサービスの継続性とユーザのデータ保護を確保する、と記述されているが、これと比べると、第１章、第３章、第４章はよいと思うが、第２章がやや異質な感じがする。ビジネスターゲットとして、ＩＳＰが情報家電をどう取り込めばよいかというトーンで第２章に追加してほしい。

○：ユーザについては、教育というよりは啓発という観点からの取り組みが必要。また、遊びでも犯罪者になるというトーンを出した方が良いのではないか。

検討報告（素案）の第３章について、事務局から説明の後、質疑。特段の意見はなかった。

○：ISMS-T については事業者が必ず取らないといけないような印象を受けるが、取得するかは事業者の判断。この報告書にどういうトーンで記載するのかについて、検討してもらいたい。

検討報告（素案）の第４章について、事務局から説明の後、質疑。以下は主なやりとり。

○：全体をみるとやはり第２章の情報家電の位置付けが気になる。第２章については、情報家電を含むあらゆる端末が繋がるユビキタスネット社会の到来を想定し、今後日本がフロントランナーを目指すにあたり、情報家電のセキュリティ確保を先

んじて取り組んでいく、という理解でよいか。これからのネット社会が今とどう違うのかを入れて頂いた方が腑に落ちやすい。

○：個人情報保護法が施行されたが、相変わらず個人情報漏洩が起こっている。個人情報の取扱いに関する方針（プライバシーポリシー）は、事業者が自ら策定・公表することとなっているが、このＷＧで個人情報保護をどう捉えるべきかを示す必要があるのではないか。

○：個人情報保護については、「電気通信事業分野におけるプライバシー情報に関する懇談会」で検討を行っている。個人情報保護については、電気通信事業者に特化したものを作るべきではないかという議論もあったが、検討の結果、個人情報保護については事業者横断的な事項であり、電気通信事業者だけに特化したものを作るというのは無理との結論になった。なお、事業者横断的な事項については、現在議員立法で対処することが可能かどうかについて、検討が行われている。

検討報告（素案）について、追加コメントがある場合には５月１１日（水）までに事務局に送付することとなった。

以上