資料６－４

「次世代の情報セキュリティ政策に関する研究会」中間報告書（案）概要

2008年4月

1．情報通信環境の現状

【ICT利用環境の現状】

●我が国では、インターネットの普及とブロードバンド化が急速に進むとともに、モバイル端末やゲーム機といったPC以外でのインターネット利用も進展。

◇我が国のインターネット利用者数（2006年末）：8,700万人（人口普及率で約70%）
◇ブロードバンド契約者数（世帯数）（2007年12月末）：2,830万件（うち40%にあたる1,132万件が光ファイバ（FTTH）契約）
◇携帯電話・PHSの契約者数（2007年末）：1億件以上。携帯電話利用者の約7割が、週1回以上インターネットに接続。
◇TV、DVD/HDDレコーダー、家庭用ゲーム機などがインターネットに接続。

●インターネットを通じた商品・サービスの購入が進展し、ICTは様々な社会経済活動の基盤となる。また、ICT産業は我が国のGDPを押し上げている状況。

◇B2C、B2B電子取引市場も右肩上がりで推移。最近では、音楽配信・ミュージックビデオ配信が順調。
◇情報通信産業における実質GDPの推移は増加の一途。
◇また、情報通信産業は、我が国の実質GDP成長率に対して、1996年以降一貫してプラスに寄与。

●ICTが社会経済活動の基盤として進展する一方で、ICT利用の負の側面である情報セキュリティに関する問題や利用者の不安感が顕在化。

◇**重要インフラ関連**：電気通信サービスでのIT障害、医療機関でのウイルス感染、地方自治体等でのホームページ改ざんによる不正プログラム混入などが発生。
◇**サイバー犯罪の状況**：2007年中のサイバー犯罪の検挙件数は5,473件で、前年（4,425件）より23.7%の増加、過去5年間で約3倍。このうち、不正アクセス禁止法違反は1,442件で前年の2.1倍に増加。
◇**情報漏えい**：2006年の個人情報漏えいの公表件数は993件（2005年：1,032件）。一件あたりの被害が増加しており、情報漏えいの対象人数が前年比2.5倍の約2,200万人。
◇**インターネット利用における不安感**：インターネット利用世帯の40%以上は、依然として、その利用に何らか不安を抱えている状況。

2. 情報セキュリティに関する現状と課題①

【情報セキュリティ脅威の現状】

●ボット等マルウェアによる脅威やソーシャルエンジニアリングによる脅威によって引き起こされる問題が深刻化し、その手口は極めて巧妙化しつつある現状。
●また、その背後には不正な利益を得ることを目的とした犯罪組織等が存在し、盗み出された情報が闇市場において取引されているとの指摘もある。

ボット等マルウェアによる脅威

○ボットに感染したPCを踏み台にしたDoS・DDoS攻撃、多量のスパムメール送信等、ネットワークを通じた情報セキュリティ脅威が深刻化。

例）
◇英国カジノサイトに対するDDoS脅迫事件
◇エストニアの政府機関等に対するDDoS攻撃
◇世界最大のスパム送信ボットネットを構築するStorm Worm　等

ソーシャルエンジニアリングによる脅威

○ソーシャルエンジニアリングを駆使した感染手法などウイルス感染の手法が高度化・巧妙化。被害が局所化してきており、情報セキュリティ脅威の潜行化が進行。

例）
◇標的型メールによるウイルス感染の事例
◇フィッシングによる金銭に繋がる情報の搾取
◇正規のWebサイトを閲覧しただけでウイルス感染する事例
◇フィッシング、Webサイト改ざん等のための専用ツールキット流通　等

このような状況を改善するためにはどのような取組み・環境整備が必要となるか？

2．情報セキュリティに関する現状と課題②

【情報セキュリティの対策主体としての利用者を取り巻く状況】

●現状、様々な脅威に対して、利用者（個人、企業）による情報セキュリティ対策が主たる対策になっている。

●インターネット等を利用する上で、利用者（特に個人）における基本的な情報セキュリティ対策の実施は極めて重要であるにもかかわらず、以下のような状況にある。

①情報セキュリティ対策に対する意識やスキルが必ずしも高くないと考えられる、いわゆる「永遠のビギナー」に対しては、基本的な情報セキュリティ対策を全面的に委ねることは難しい場合がある。

②ボット等によって踏み台にされると、被害者となると同時に、加害者となる可能性がある。

上記のような状況を改善することができないか？

○基本的な情報セキュリティ対策を徹底を図るための普及啓発
○電気通信事業者による能動的な対策を実施するための方策
○被害にあった場合に利用者が身近にかつ気軽に相談等ができる環境の整備　　等

4. 近い将来のICT環境と情報セキュリティ脅威・課題①

【情報通信環境の変化の状況】

●近い将来（３年から５年後）の情報通信環境は、情報通信技術の高度化、ICTの利用領域や利用者の増加が進み、ユビキタスネット社会が進展していると予測。

① 情報通信ネットワーク技術の高度化が一層進展
（ブロードバンド・ゼロ地域の解消、電気通信網のIP化（NGN）とインターネットの並存、IPv6の利用促進とIPv4との共存、次世代無線アクセスシステムのサービスイン、第4世代移動通信システムの実現、情報家電等の普及、FMC、FMBCサービスの台頭、オーバーレイ・ネットワークの利用拡大　等）

② スマートフォン等、携帯電話の高機能化によるモバイル利用環境の進展
（OS等のオープン化、APIの公開、携帯端末からの各種サービスの利用、位置情報利用の拡大　等）

③ ネットワークを流通するデータ量、ネットワークと接続するデバイス数の爆発的増加
（インターネット利用者数の増加、non-PC端末によるインターネット利用の増加、ブログ、SNSなどのCGMの増加、大容量マルチメディアコンテンツの流通拡大、情報家電・RFIDの利用拡大　等）

④ 消費活動等の変化
（非接触ICカードの普及による電子マネーの利用拡大、こだわり型の消費活動の増大、商品情報・顧客情報の増大と営業戦略の変化　等）

⑤ ICT利用領域等の拡大、ICT利用による生産性向上等
（ASP・SaaSを始めとしたICTサービスの利用の拡大　等）

4. 近い将来のICT環境と情報セキュリティ脅威・課題②

【近い将来のICT環境における情報セキュリティ上の課題】

●近い将来（３年から５年後）のユビキタスネット社会においては、ネットワークに接続される機器が増加し、その利用者も拡大。また、ネットワークに流通する情報が質・量ともに増加。さらに、ビジネスモデルの多様化（水平連携モデルの推進）等により、関係者が複雑に絡み合い、情報セキュリティ対策の困難性が拡大。

脅威の対象となる範囲の拡大

○ネットワークに接続される機器･デバイスが爆発的に増大

○OS、アプリケーションの共通化により、1つの脆弱性が及ぼす対象範囲が拡大。

○情報セキュリティに関する意識や知識が必ずしも高くない利用者が増加。

○情報の保持、管理する場所･主体に変化。

脅威の対象となる情報の増加・多様化

○ビジネスモデルや利用形態の変化に伴い、決済情報、認証情報、位置情報等の個人情報や企業情報が、ネットワークを流通する機会の増大。

○仮想世界の通貨等、新しい価値ある情報の流通が増加。

対策の困難性の拡大

○情報通信技術、ビジネスモデルの恒常的な変化により、将来の脅威予測が困難。

○ネットワーク上の端末や情報量の爆発的な増大、利用する個人の増加、及び多数の関係事業者が複雑に絡む環境において、対策主体の責任範囲が不明確。

○ウイルス感染や意図的に情報漏えいを引き起こす手法の更なる高度化･潜行化。

○事案が発生した場合に、迅速かつ効果的な対策を実施するための体制が未確立。

5. 現状及び近い将来のICT環境における情報セキュリティ対策の重要性①

【現状及び今後の情報セキュリティに関する主な課題等（まとめ）】

① ボットネットに起因する様々なインシデントが継続して発生。また、Web感染型のマルウェア感染手法等、今後も悪意をもった攻撃者によるマルウェアの感染手法等が巧妙化・高度化。

② ビジネスモデルの多様化等により、より多くの関係者が複雑に絡み合って情報通信社会が形成され、効果的な情報セキュリティ対策手法や各情報セキュリティ対策実施主体としての責任範囲が不明確となることから、情報セキュリティ対策に遅れ等が発生。

③ 流通する情報の量の増加と質が変化するとともに、情報資産の保有の在り方の多様性も増すことが、情報セキュリティ対策が困難化。

④ いわゆる「永遠のビギナー」の利用が増加。この場合、悪意の第3者からの最大の標的とされる可能性が高いほか、適切な情報セキュリティ対策を行わない永遠のビギナー等がボット等に感染することにより、被害者となるだけではなく、他人に被害を及ぼす加害者となることから、一部の利用者が高度な情報セキュリティ対策を講じても、我が国の全体としての情報セキュリティ向上には繋がらない。

⑤ OS等の共通化によって１つの脆弱性が及ぼす影響範囲が拡大する可能性のほか、複数の通信経路を持つことによるマルウェア拡散が複雑化・広域化する可能性、新しい技術を導入することによるこれまで想定し得なかった脅威が発生する可能性等が増大 。

5. 現状及び近い将来のICT環境における情報セキュリティ対策の重要性②

【重点的に検討・実施すべき項目等】

① 利用者を取り巻く環境における情報セキュリティ対策の徹底

ア）利用者における対策徹底に向けた普及啓発

利用者がボット等に感染することにより、被害を受けるだけではなく、他人へ迷惑をかける加害者になってしまう場合があることを認識し、これまで以上に利用者における情報セキュリティ対策の徹底を図るため、サイバークリーンセンター等を通じて、普及啓発活動のより一層の充実。

イ）電気通信事業者による対策の推進

・電気通信事業者が、マルウェアの感染活動等に利用されている通信ポートを閉じてマルウェアが活動できない状態にするなど、情報セキュリティを確保するために電気通信事業者が取り得る正当業務行為の範囲についてのガイドラインを検討。

・利用者が誤ってフィッシングサイトやマルウェア配布サイト等の危険なWebサイトと通信することを防止するため、信頼性の高いレピュテーション・データベースの構築とその運営方法について実証。

ウ）ユーザサポート体制の充実

利用者が実際にマルウェア等に感染して被害を受けた場合等に、身近にかつ気軽に相談できるユーザーサポート体制を地域に根差したNPOの活動等として充実することが必要。

② 産学官連携による先進的な研究開発の実施

ア）ボット等マルウェア感染手法の巧妙化等への対策

従来型の受動的な観測システムに加え、利用者のプライバシーに配慮しつつ利用者側の状況を積極的に把握するための観測網の実現を検討。

イ）IPv6等の新しい技術が実装されていく過程で生じ得る技術的な課題への対策

ウ）Ｐ２Ｐネットワーク等において信頼できる情報を共有するレピュテーションＤＢ高度化技術の検討

P2Pネットワーク、ＣＧＭ等のオーバーレイ・ネットワークにおいて、利用者自身が情報発信元や情報そのものの信頼性を評価し共有できるレピュテーション機能や情報の質や信頼性を検証する技術等の実現方法について検討。

5. 現状及び近い将来のICT環境における情報セキュリティ対策の重要性③

【重点的に検討・実施すべき項目等】

③ 関係機関における連携強化

ア）実効性のある情報共有体制の充実

脅威が巧妙化、潜行化し、また被害が局所化していることから、感染事実が把握しづらい状況なっていることを踏まえ、関係者が、その時点で発生したインシデントや前述の観測網で収集・分析できた情報等を迅速に情報共有できるよう、分野を横断する連携の充実が必要。

イ）国際連携の促進

各国政府及び関係機関との間で、インシデント等に関する情報の共有・分析等における協調・連携体制を構築及び強化が必要。その際、我が国のボット対策プロジェクト等、先進的な取組については、世界に向けた情報発信及び海外展開・協力体制構築に向けた検討等を実施していくことを検討。

④ ユビキタスネットワーク社会における情報セキュリティ対策に関する業界横断的な検討体制の整備

電気通信事業者、サービス提供事業者、端末機器製造・販売事業者、情報セキュリティ関連事業者等の関係する全てのICTサービス提供者が参加し、かつ継続的に、情報セキュリティに関連する課題やその対策等について検討する業界横断的な検討体制を整備。この体制において、障害・対策事例等の共有のほか、各主体が個別に担うべき対策領域や、協調・連携して行うべき効果的な対策手法、そのコスト分担の在り方等について議論。

⑤ 利用者、情報通信環境、情報セキュリティが共生するICT社会モデルの検討

将来の情報通信環境では、ネットワークに接続される端末や利用者数、情報量が爆発的に増加し、関係主体が複雑に絡む状況において、ICTサービスの多様性・利便性を確保しつつ、併せて情報セキュリティ対策が施されている環境を、「利用者（利便性）、情報通信環境（多様なサービス）、情報セキュリティが共生するICT社会モデル」として実現することについて、具体的な実証モデルを構築して、その有効性や課題を検証。