財団法人国民工業振興会　講演会
(第 21 回情報技術・マルチメディア　研究会例会)
日時: 平成 22 年 9 月 1 日(水)14:00～16:00
場所: ニューオータニイン東京　4F 「ももきりの間」

講演「ここまで来た情報セキュリティの脅威とその対応」
前総務省 CIO 補佐官(兼)最高情報セキュリティアドバイザー
ＩＴプロ技術者機構　会長　　安田　晃氏

インターネットの普及は、社会にさまざま利便性をもたらし、革新をうながしたが、一方、情報セキュリティに関する脅威も年々高まり、個人情報の漏洩事件や情報システムの大規模障害などが頻発している。必要な対策を怠り、対応を誤れば、企業の存続すら危うい事態を招く。本講演では、様々な分野に及んでいる情報セキュリティに関する脅威の実態をとりあげ、被害を最小限に食い止めるための取組等について、斯界の権威である講演者に解説をお願いした。

1)情報セキュリティの脅威の実態

情報セキュリティを脅かすものとして、家庭用のＤＶＤブレーヤー、ランケーブルのモジュラージャック等家庭で使用する機器を踏み台として不正なアクセスをするもの、2009 年 7 月に米国、韓国の政府機関に対して発生した複数のコンピューター(踏み台)による DDos(分散サービス妨害)攻撃などがある。　ウエブブラウザ関連では、フィッシング詐欺(本物と同じようなサイトを作りだますもの)　正規なサイトに不正な HTML タグを埋め込み悪質なサイトに誘導するもの、SQL インジェクション(データーベース言語(SQL)システムを不正に操作する攻撃方法)、ガンブラーウイルス(ソフトウエアの脆弱性をついて感染し、コンピュータ内の ID、パスワードを流出させるウイルス)、クロスサイトスクリプティング(サイト間を横断して悪意あるスクリプトを混入させること)、ボットネット(悪意あるプログラムにより乗っ取った多数のコンピュータ(ゾンビ PC)で構成されるネッワーク)等がある。電子メール関連では、スパイウエア(知らないうちに PC にインストールされてスパイ活動するプログラム)、画像スパム(画像を用いたスパム)がある。その他の攻撃例として、ダウンアドウイルス(インターネットから侵入したり、メモリなどを使って LAN 内部からも侵入するウイルス)、ウインドウズショートカットファイル感染ウイルス、ファイル交換ソフト(ウイニー)等数多くの感染源がある。

2) 更に広がるセキュリティの課題

2-1)クラウドコンピューティングにおけるセキュリティ

クラウドコンピューティングには、IaaS/HaaS(システム及びネットワークなどのインフラをサービスとして活用)、PaaS(アプリケーション実行用のプラットフォームを提供)、SaaS(インターネットを利用してソフトウエアそのものを提供)があり、短時間でのシステムの立ち上げ、必要な規模で使用できるメリットがある。

クラウドコンピューティングでの事件としては、Twitter 社の情報漏洩事故があった。これは 1 人の Gmail アカウントの奪取から全社の重要情報の漏洩に至ったものであり、対策としては、個人用と会社用のパスワードを共有しないことが重要である。クラウドコンピューティングのセキュリティ上の問題点として、データの物理的な保存先が分からないとか、監査や脆弱性診断の実施を顧客が受け入れてくれない等の実施上の制約があることがあげられる。SaaS では、大事なデータをクラウド上には保存しない等の対策が必要である。

2-2)機器・産業用システムにおけるセキュリティ

機器製品からの PC ウイルス混入としては、カーナビ、MP3 プレーヤー、iPod、携帯電話、壁紙アプリ(スクリーンセーバー等)の多くがスパイウエア等の事例がある。カーナビの電子制御ユニットにウイルスが侵入し安全性に被害を及ぼす事例が実証されている。原子力発電所の監視制御システム(SCADA)が停止した例では、電力網をコントロールしているコンピューターネットワークがセキュリティホールだらけで、テロに利用される恐れがあるため、国際的な対応が今後行われる。2010 年 7 月に発見された Windows ショートカットファイル感染ウイルスは、シーメンス社の監視システムを攻撃しており、かなり大がかりな組織で作られた形跡がある。組み込みソフトに対する特有のセキュリティの課題としては、開発段階でセキュリティに取り組むこと、フェールセイフ機能の充足が必要である。また、セキュリティや安全を保つための制度の充実が必要である。

2-3)IPv6(次世代のインターネットプロトコル)におけるセキュリティ

1981 年に仕様が公開された IPv4 は、インターネット利用者の急増により、アドレス数が限界を迎えつつあり、また、セキュリティ面で様々な問題が指摘されている。1998 年に仕様が公開された IPv6 は、実質無制限のアドレスを割り当てることができるので、今後のインターネット利用者の拡大に対応することができる。日本ではまだ普及していないが、中国では積極的に採用している。 IPv6 では、暗号化しているので、セキュリティ的にはチェックできない問題がある。 Windows VISTA 及び Windows 7 にも IPv6 は入っており、IPv4 の中に IPv6 のデータを作るトンネル機能がある。

3)政府の「国民を守る情報セキュリティ戦略」と「2010 年度戦略」

現状の課題として、大規模なサイバー攻撃の脅威の増大、急速な技術革新の進展、社会経済活動の情報通信技術への依存度の増大、グローバル化の進展等がありこれらの課題に対応する新戦略が必要である。

国民を守る情報セキュリティ戦略(2010～2013)の基本的な考え方として、ＩＴリスクを克服して、安心・安全な国民生活の実現、サイバー空間上の我が国の安全保障・危機管理の確保、情報通信技術の利活用を促進し、我が国の経済成長に寄与することが決められている。実現すべき成果目標としては、2020 年までにインターネットや情報システム等の情報通信技術を利用者が活用するにあたっての脆弱性を克服し、全ての国民が情報通信技術を安心して利用できる環境を整備し、世界最先端の「情報セキュリティ先進国」を実現するとしている。その具体的な取組として、国民生活を守る情報セキュリティ基盤の強化、国民・利用者保護の強化を挙げている。

4)セキュリティの取組に必要な考え方

情報セキュリティへの取組としては、PDCA サイクルをまわしながら継続的取組のレベルを一段と向上させていくことが重要である。即ち、1)守るべき情報の特定、2)守るべき情報の価値を算定、3)脅威と脆弱性を想定、4)リスクを算定(被害の大きさ×発生の可能性)、5)対策の立案・評価、6)対策のルール化・実施、7)教育を実施し対策を徹底、8)見直しを実施(点検、監査)、9)改善の実施のＰＤＣＡサイクルを回してセキュリティ向上に取り組むことが重要である。

5)政府機関における情報セキュリティ対策

内閣官房情報セキュリティセンターから政府機関の情報セキュリティ対策のための統一基準(基本編、情報システム編)が作成されインターネット上で公開されており、情報セキュリティ要件の明確化に基づく対策が報告されている。情報セキュリティについての機能として、1)主体認証機能、2)アクセス制御機能、3)権限管理機能、4)証跡管理機能、5)補償のための機能、6)暗号化機能と電子署名機能が挙げられている。また、情報セキュリティについての脅威としては、セキュリティホール、不正プログラム、サービス不能(Dos)攻撃、踏

み台等が挙げられており、これらに取り組む必要がある。

6)情報対策のまとめ

各部署や各システムにおいて、守るべき重要な情報や情報資産をもれなく把握し、明確化することが出発点である。そして、取り扱う情報資産の重要度や特性等を考慮して、リスク(被害の大きさ)に応じた積極的なセキュリティ対策を実施する事が基本である。

2010 年 8 月 14 日西日本新聞に掲載されたユニーなど 8 社のネットスーパーの顧客情報の大量盗難事件(SQL インジェクションの事件例)があり、カードの不正使用について 100 件以上が報告されており、被害届を受けた大阪府警では捜査をつづけているが、当面、ネットスーパーの再開の目途は立っていない。

今後の対策としては、システム構築の早い段階から、セキュリティを意識した取組が必要であり、市場に出る前の段階での対策が重要と考えられる。

以上

講演会風景