安全・安心な社会を構築するための情報セキュリティ技術の現状

教授　瀬戸洋一

クラウド・コンピューティング、スマートグリッドやスマートフォンなどの新しいIT技術環境の発展に伴い、新たなセキュリティ問題が生じている。以下に最新の情報セキュリティの動向と本学におけるカリキュラムとの関係を述べる[1][2]。

１．情報セキュリティ技術の最新動向

(1) 暗号の危殆化

暗号技術が社会の様々な分野で利用されている。暗号技術は解読に莫大な時間や費用を要することを前提に安全性を保障している。しかしながら、暗号解読技術の進歩や計算機の処理能力の向上により、従来「安全だ」と言われていた暗号技術が解読されたという事例も報告されている。暗号の安全性が危ぶまれるのことを「暗号の危殆化」と言う。暗号の危殆化は、運用上の問題やソフトウェア/ハードウェアあるいは暗号アルゴリズム自体に問題があることに起因している。米国国立標準技術研究所（NIST）が定めるSP800-57（Recommendation for Key Management）では、ハッシュ関数のSHA-1、共通鍵暗号の2-key Triple DES、公開鍵暗号の鍵長1024bitのRSA/DSAなどが危殆化しているため、より強度な暗号アルゴリズムへ移行することを推奨している。この移行時期が2010年であり、「暗号アルゴリズム2010年問題」と呼ばれている。日本でも、2013年を目処に電子政府推奨暗号リストの改訂が検討されている。

(2) スマートフォンへの脅威

高機能な携帯情報端末として、世界的にスマートフォンの利用が広がっている。スマートフォンはパソコンのようにアプリケーションをインストールし、自由に拡張することが可能である。これらアプリケーションの中には、位置情報や利用者情報を自動的に外部サーバに送信するものが存在しており、注意が必要である。2010年にはAndroidで動作する世界初のボット型ウイルスが発見された。また、Android向けのスパイウエアも出現した。Android端末のGPSが動作し、端末の位置情報を定期的に攻撃者に知らせ、ユーザーの居場所、そして行動情報が筒抜けになった。つまり、利用者の個人情報が漏えいされ、ユーザーの身を危険にさらす可能性もでてきた。スマートフォンは携帯電話の延長線上というよりパソコンに近いものであるが、パソコンと同様の脅威があることを利用者は十分認識できていない。さらにスマートフォンの利用は、ビジネスの場でも広がっている。このような状況から今後のセキュリティ対策の重要性が高まっている。

(3) クラウド・コンピューティングが抱えるセキュリティ

クラウド・コンピューティングが急速に社会に浸透している。クラウドには、グリーンITへの貢献も含め実務的な利点がある反面、社会インフラとして活用する上で安全性、信頼性、可用性などの観点でセキュリティ課題が存在する。悪意ある者が、クラウドに対しどのような形態や手段をつかって攻撃をしかけてくるか想定することができない。また、計算機リソースが利用者の内部統制下にないため、より安全・安心して活用できる環境の整備が望まれる。特にセキュリティに関する論点は、Gartner社のレポートによれば、７つのセキュリティリスクがあると言われている。このため、経済産業省では、クラウドサービスを安全に安心して利用するために「クラウドサービス利用のための情報セキュリティマネジメントガイドラインを策定し、2010年、国際標準化委員会ISO/IEC JTC1/SC27にクラウドサービスの

セキュリティ仕様文書案を提案し標準化がスタートした。

（４）重要インフラへの脅威

プラント等の重要インフラは、経済活動や社会活動を維持するための基礎であるため、十分なセキュリティ対策が必要である。イランの原子力発電所の制御システムが 2009 年から 2010 年にかけて APT（Advanced Persistent Threats）と呼ばれる「新しいタイプの攻撃」を受けていた。この事件では、Windows の自動実行機能の無効化を回避する Stuxnet（スタックスネット）と呼ばれるウイルスが用いられた。Stuxnet はこれら制御システムに感染し、ターゲットなる制御システム上の装置を攻撃していたことが判明し、重要インフラへの脅威が高まった。また、スマートグリッドと呼ばれる高機能な次世代電力システムが電力供給不足に悩む国々で注目されている。スマートグリッドは、電力を制御するために、通信/IT 技術を駆使して電力事業者と家庭を接続しており、情報セキュリティ対策と各家庭のプライバシー保護対策が求められている。

(5)アイデンティティエコシステムによる個人 ID 管理

現在，日本政府は，社会保障・税に関わる番号制度（国民 ID）の導入を検討している．本制度は，社会保障と税に共通の番号を国民一人ひとりに割り振る制度である．一方，2010 年 6 月，米国政府は Identity Ecosystem の構築を促進することを発表した．アイデンティティエコシステムとは，アイデンティティ管理（ID 管理）のエコシステムを実現するというものである．これは社会保障，税務サービス，医療介護サービス，電子政府サービス，民間ポータルサービス，金融サービスなど個別に発行された ID を相互運用し，国民が安心安全にオンラインサービスを受け入れる認証基盤を構築するものである．今後、行政、民間サービスを利用する際に個人を識別するための ID を統合的に管理するアイデンティティエコシステムの開発および新しいアーキテクチャに対する情報セキュリティ対策が重要となる。

２．本学のカリキュラムとの関係

大学などの高度教育期間では、専門分野に関する「知の細分化」が起こっている。専門化・細分化されて局所的の技術論に陥り、全体の相関や総合的ソリューションを求める「全体知」の伝授が弱くなっているのが実態である。社会で生じている様々な問題は、「全体知」をもって解決することが多い。つまり、IT 分野においては、「部分知」では、物事の本質を見極めることは難しく、対象に対する「全体知」を学ぶ努力を怠ってはいけない。

産業技術大学院大学の情報セキュリティ教育は、「部分知」を知って「全体知」に活かす教育方針をとっている。具体的には「情報セキュリティ特論」で社会が求める技術の体系を理解する。これは、上記（1）-（5）の問題の本質を見極めるのに役に立つ。「情報セキュリティ特別講義 1」ではリスクの可視化と組織内への対策の組み込み、「情報セキュリティ特別講義 2」「セキュアプログラミング特論」では（2）（3）（4）におけるセキュア設計理論と具体的な実装技術、情報セキュリティ特別講義 3 では（1）-（5）の問題が発生した場合のビジネス上の事業継続などを学ぶ。Project Based Learning では、具体的な事例を用いて、(2)（4）（5）に関係するプライバシー保護に関する総合的な手法に関し修得する。

参考文献

[1]情報セキュリティ白書 2011、（独）情報処理推進機構、2011 年 6 月

[2]瀬戸洋一ほか：情報セキュリティ概論、日本工業出版、2007 年 11 月