技　術　解　説

情報セキュリティ技術

電　子　部　永吉弘己

1　はじめに

インターネットをはじめとするコンピュータネットワークの普及に伴って，情報セキュリティに関連したさまざまな事件が起きています。最近の例では，テレビ局のホームページの内容が改ざんされた事件や，厚生省のホームページのデータファイルがマクロウィルスに感染していた事件，そしてインターネットのサービスのひとつであるネットニュースを利用して，各組織のニュースサーバのパスワードファイル等を盗んだ事件等があげられます。

また，よく使われているWWWブラウザソフトのセキュリティ上の欠陥などもマスコミで大きく取り上げられるようになり，コンピュータネットワークにおける情報セキュリティ問題が，最近にわかにクローズアップされてきています。この背景には，ネットワークを利用した電子商取引や電子マネーなどが実験的に運用されはじめ，ようやく情報セキュリティ対策が非常に重要な課題として認識されはじめてきていることがあげられます。

（注）コンピュータシステムに不正侵入するなどの破壊行為を行う者を俗に「ハッカー」という場合が多いですが，システムの仕組みや動作について研究し，コンピュータ技術の進展や普及に寄与している人を指すのが本来の意味です。

一方，不正侵入などの破壊行為を行う者は，正しくは「クラッカー（攻撃者）」や「イントルーダ（侵入者）」と呼びます。

2　2つの情報セキュリティ

情報セキュリティについては，表1に示すように物理的セキュリティとコンピュータセキュリティに分類できます。物理的セキュリティとは，コンピュータでなくとも被ることのある盗難や災害，過失，事故あるいは破壊といったものです。しかし被害を受けるものがコンピュータであるため，各方面に重大な被害を及ぼすだけでなく，プログラムやデータの紛失など復旧にかなりの時間と労力を要します。また，完全に普及することが困難な場合もあります。対策としては，コンピュータの設置してある部屋の施錠や入室制限，そしてパソコンを盗難から守るための施錠・防犯キット，耐震用ブロックやベルトの取り付けなどがあります。さらに，無停電電源装置や万一の障害に備えるためにデータバックアップは極めて重要です。予算とセキュリティのトレードオフですが，ハードディスクをはじめとするシステムやネットワークの二重化と設置場所の分散化も考慮する必要があります。

最近のインターネットの普及によりクローズアップされているのは，この物理的なセキュリティではなく，不正アクセスやコンピュータウィルス等のコンピュータセキュリティです。一般的に情報セキュリティというと，後者のインターネットやイントラネットにおけるセキュリティを指す場合が多く，不正侵入などによる文書の破壊や盗聴・改ざん，コンピュータウィルスによる被害などがあります。

表1　2つの情報セキュリティ

	具体例	対策例
物理的セキュリティ	盗難，破壊，過失など 地震，落雷，火災，水害，台風など 停電，通信回線障害，システム障害	設置施設の施錠などの侵入・盗難対策 設置施設の耐震・耐火構造，ハロン系消火器 無停電電源装置，システムや回線の二重化 データ等のバックアップ
コンピュータセキュリティ	不正侵入 盗聴，改ざん，なりすまし ウィルス	ファイアウォール，パスワード，ワンタイムパスワード 暗号化，電子署名，公開鍵証明 ウィルスワクチン，バックアップ

3　コンピュータセキュリティ

インターネットが学術研究的な目的で発展してきたという歴史的な背景と，最近のような急速な普及もあってセキュリティ対策が結果的に後手に廻ってしまったことは否めません。また企業においては，セキュリティ対策にコストが掛かり過ぎる，対策の明確な基準や規格がない，対策のノウハウ不足，経営者等の認識不足，そしてセキュリティ対策そのものが売上げに寄与しないなどの理由から，対投資効果という面からもセキュリティ対策は重要な課題とされていませんでした。しかし，インターネットを利用した情報伝達や業務報告が日常的に利用されるようになり，電子マネーの試験運用が始まり，SET(Secure Electronic Transaction)などのクレジットカード決済のための仕様が規格化されるなど，電子商取引を取り巻く環境においてもセキュリティ対策が極めて重要になってきています。さらに，ネットワークを経由したコンピュータウィルスの被害が明るみに出るようになって，情報セキュリティは一層重要なものとして認識されるようになってきています。

コンピュータセキュリティについては，従来から一般的に

安全性×利便性＝一定

という式で表されてきました。要するに，安全性を高めれば利便性が低くなり，逆に，利便性を高めれば安全性が低くなります。例えば，非常に難しいパスワードを短い周期で変更すれば，安全性を高めることはできますが，非常に使いづらいものになってしまうということです。最近の技術開発の進展もあり，コストをかければあるいは技術力を高めれば，安全性も利便性もある程度，高めることができるようになってきています。しかし，最も重要なことはセキュリティポリシーの確立と，経営者から一般社員までのセキュリティに対する認識の向上，そしてセキュリティ対策の実行であることは間違いありません。

セキュリティ対策は，現在のところファイアウォールの設置やワンタイムパスワードの利用，暗号化技術を用いた電子メールや電子署名，あるいはウィルスチェッカーなどのさまざまな機器やソフトを利用して行われています。また動的署名照合システムとして，自分のサインをタブレット等から入力し，筆跡の特徴を抽出して認証を行うサーバーサインのほか，指紋や声紋，DNAなどのバイオメトリクス（生体情報）を用いた認証も一部実用化されています。さらに，ネットワーク層のインターネットプロトコルでセキュリティ機能をサポートする研究も進められています。

4　おわりに

増え続けるコンピュータセキュリティ被害に対処するため，不正侵入やウィルスなどの対策について技術的側面から支援し，コンピュータセキュリティに関連する技術情報の提供を行うJPCERT/CC（コンピュータ緊急対応センター）という非営利組織が，日本でも遅ればせながら昨年８月に設立されました。

セキュリティに関連する情報は常に更新されており，緊急性も高いため最新の情報を入手するように心掛けることが大切です。表２にコンピュータセキュリティ関連情報の主な入手先を示します。

表２　セキュリティ関連情報の主な入手先

WWWサーバ	コンピュータ緊急対応センター (JPCERT/CC) 認証実用化実験協議会 (ICAT) 情報処理振興事業協会 (IPA) CERT CIAC NIST CSRC FIRST	http://www.jpcert.or.jp/ http://www.icat.or.jp/ http://www.ipa.go.jp/ http://www.cert.org/ http://ciac.llnl.gov/ http://csrc.ncsl.nist.gov/ http://www.first.org/
ネットニュース	fj.comp.security tnn.internet.firewall comp.security.*	
メーリングリスト	firetalk-request@is.aist-nara.ac.jp scrtyl1@takamatsu-nct.ac.jp announce@jpcert.or.jp	