大分県・地域情報化の普及啓発情報誌

HYPER FLASH

[ハイパーフラッシュ]

vol. 33

Jan. 2006

樹氷（九重町）

情報セキュリティ対策は身近な課題（1）

独立行政法人　情報処理推進機構（IPA）セキュリティセンター長　三角　育生

1 はじめに

最近、頻繁に情報システムに関する事故などの報道を目にします。証券取引などのシステムの障害、インターネットバンキングなどに関する情報の盗難、クレジットカードの個人情報の流出、商品の価格を比較できる情報を提供するホームページの不正な書換え・同サイトの一時閉鎖など、枚挙にいとまがありません。こうした事故などは大企業のみの問題ではありません。インターネットを活用して地方から全国を商圏として活動している中小企業においても、例えば、ゲーム会社のホームページの不正な書き換え、サイトの一時閉鎖に追い込まれた例などがあり、また、消費者の立場である個人においても、インターネットを通じた詐欺事件などに巻き込まれたりと、情報システムを利活用している全ての人々にとっての問題と考えるべきです。

日本のインターネット利用人口は平成17年度版情報通信白書によると2004年でほぼ８千万人、人口普及率は62%以上と報告されています。こうしたインターネットの普及に伴い、日本の電子商取引の規模も大幅に拡大しつつあります。経済産業省の調査によると、2004年に、企業間の取引規模は約103兆円（前年比33%増）、企業と消費者間の取引規模が約5.6兆円（前年比28%増）とされています。インターネットを活用することで、消費者は、時に世界中から自分の好みに合った商品を24時間いつでも注文することができ、また、営業時間に関係なく金融などの手続きができるなど、とても便利になってきています。しかし、前述の様な情報システムに関するリスクは、この便利さとは切り離せない状況にあることは事実です。

情報システムに関するリスクを歴史的に見ると、かつてインターネットがさほど普及していなかった90年代前半には、フロッピーで感染するウイルスなどが代表的な脅威でした。この当時のものは、技術を誇示したい愉快犯的なもので、その被害も限定的でした。しかし、インターネット、電子メールの普及により、こうしたネットワークを通じてウイルスに感染したり、また、ホームページ書き換えなどの不正アクセスなどが見られるようになり、被害の大規模化が進みました。昨年あたりからは、愉快犯というよりも、銀行の口座番号などの情報を入手するなどの経済的利得を目的とした情報搾取などが増大し、手口も高度化しつつあります。

こうした情報システムの事故・事件に、一旦巻き込まれてしまいますと、個人の場合には大事な財産に被害が及ぶ可能性があり、また、企業の場合に、ビジネスの一時的な停滞のみならず、個人情報保護の問題、社会的信用問題、賠償問題などにまで発展する可能性があります。利便性の向上や大きなビジネス・チャンスと引き換えに、どこまで、情報システムのリスク対策をすべきかどうか、消費者、また、企業の経営者・システム管理者の方々は迷うことが多いのではないかと思います。このため、以下に、情報システムにとっての脅威、特に、新たな脅威とはどの様なものがあるのか、どのように対策を講ずるべきかなどについての検討の一助となるべく、主な情報セキュリティ対策の

動向などについて述べます。

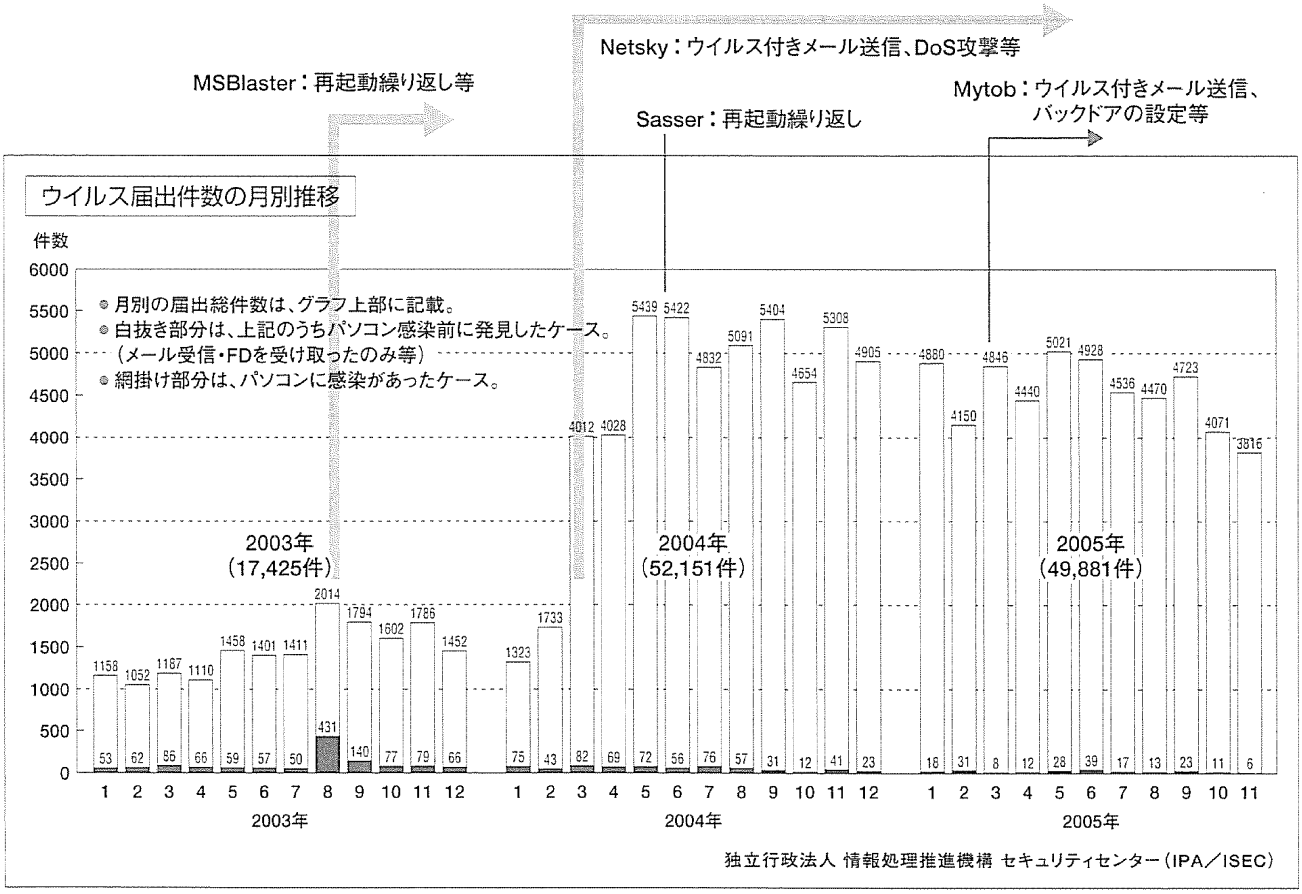
2 被害の現状と対策

(1) ウイルス

図に最近のコンピュータウイルス発見・被害届出件数の推移を示します。最近2年間は高水準で推移していることがわかります。これは、大量のウイルス付メールの送信などをするウイルスなどが蔓延していることが主な原因と考えられます。ウイルス対策などが施されていないコンピュータがかなり存在しているのではないかと考えられます。

最近は、ウイルスの亜種が次々に出現し、被害も長期化しています。ウイルス対策のワクチンソフトは、ウイルスを特定するためのパターンを持っていて、メールに添付されたファイルやホームページからダウン

図 コンピュータウイルス被害の状況



出典：IPAコンピュータウイルス届出状況　http://www.ipa.go.jp/security/txt/2005/documents/virus-full0512.pdf

ロードしようとするファイルなどがウイルスかどうかをチェックします。パターンが微妙に異なる亜種が続々出現している現状などを踏まえると、ワクチンソフトのウイルス定義ファイルは常に最新のものに更新するよう心がけることなどが重要です。ワクチンソフトには、ウイルス定義を自動的に更新する機能が付いていますのでこの機能を利用すると便利です。

メールの送受信に使用するメーラーや、インターネット上のWebサイトを閲覧するためのブラウザなどを使用する場合は、それぞれのソフトウェアに用意されているセキュリティ機能の設定も重要です。例えば、マイクロソフト社のInternet Explorerをお使いの場合には、インターネットオプション（［スタート］→［設定］→［コントロールパネル］→［インターネットオプション］）で、セキュリティのレベルを設定できます（セキュリティレベルを「中」以上と設定することを勧めます。）。

さらに、最近のコンピュータウイルスは、システムやソフトウェアなどのセキュリティホール（情報セキュリティを損なうような予定外の事象につながる可能性のある情報システム・製品の弱点、設計・プログラム化のエラーなど）をねらったウイルスなども続出しています。こうしたセキュリティホールに関する情報は、マイクロソフトなどのソフトウェア・ベンダーなどが、セキュリティホールを修正するプログラムなど（セキュリティパッチ）が準備された段階などに公表していますので、こうした情報を踏まえて、パッチをあてるなどの対策も重要です。（ＩＰＡでは、「ウイルス対策のしおり」をホームページからダウンロードができるようにしています。
(http://www.ipa.go.jp/security/antivirus/shiori.html)。

(2) 新たな脅威－その1：スパイウェア

最近、「スパイウェア」という用語が報道などで頻繁に出現しています。「スパイウェア」が埋め込まれ、銀行のオンライン取引に必要なＩＤやパスワードが不正に奪取され、預金が勝手に他の口座へ送金されてしまった、電子商取引を運営する企業へのクレームメールに「スパイウェア」が添付されていたため、クレームの内容を示したファイルと思ってクリックしてしまった結果、企業の情報が流出してしまったといった事件などです。

スパイウェアとは、「利用者や管理者の意図に反してインストールされ、利用者の個人情報やアクセス履歴などの情報を収集するプログラム等（ＩＰＡ等による定義）」です。企業内のパソコンなどがスパイウェアに感染すれば、企業の秘密情報などが、あたかも産業スパイによって盗み出されたかのようなことが起こりかねないわけです。したがって、スパイウェアは企業の経営にとって新たな脅威であり、これへの対策は必要なものとなります。

スパイウェアには、ホームページからの安易な無償プログラムなどのダウンロードなどを通じて感染します。対策としては、ウイルス対策のワクチンソフトやスパイウェア対策ソフトを利用して検査することなどが挙げられます（ＩＰＡでは、「スパイウェア対策のしおり」をウイルス対策のしおりと同じページからダ

ウンロードができるようにしています。）

（3）新たな脅威－その2：ボット

この奇妙な名前（ボット）のプログラムは、コンピュータウイルスの一種で、コンピュータに感染し、そのコンピュータを、インターネットを通じて外部から操ることを目的として作成されたプログラムです。感染すると、外部からの指示を待ち、与えられた指示に従って内蔵された処理（悪意を持った命令があった場合に、メールの大量送信、特定のコンピュータに過剰な負荷をかけてサービス提供をできなくするような攻撃など）を実行します。この動作が、ロボットに似ていることからボットと呼ばれています。

ボットは、ウイルスメールの添付ファイルの実行などにより感染しますが、感染したコンピュータの利用者に気づかれないように様々な手法が用いられていますので、ウイルス対策のワクチンソフトの定義ファイルを最新にして、ウイルス検査を実施するなどの対策が必要です（ＩＰＡでは「ボット対策のしおり」をウイルス対策のしおりと同じページからダウンロードができるようにしています。）。また、ホームページの運営者は、不正に侵入され、ホームページがボットの感染用に改ざん（ウイルスの埋め込みなど）されないように注意することも重要です。

（4）新たな脅威－その3：フィッシング

実在する会社（金融機関などのケースが多い）などのホームページにそっくりな画面を表示させてパスワードやクレジットカード番号などの重要な情報をユーザーに入力させ、盗み出す詐欺の手口をフィッシング詐欺といいます。こうした詐欺をすべく送りつけるフィッシングメールは、ウイルス対策のワクチンソフトには引っかからないので特に注意が必要です。メールの送信元のアドレスは簡単に偽装されてしまいますので、安易に信用すべきではありません。またメールの本文中にあるホームページアドレスを安易にクリックすることのないように心がけることが必要です。

（5）

以上、ウイルスや新たな脅威の主なものについて、概要と対策を説明しました。これらの他にも、パスワード解析ツールなどによって、外部からコンピュータシステムにログインするためのパスワードを解読してコンピュータシステムに侵入したりする不正な行為などが増大しつつあります。パスワードは、推測容易なものは避けるとともに定期的に変更するなどの管理も重要です。見慣れないファイルやプログラムが置かれていないか、パスワードが推測可能でないか、公開すべきでないファイルを公開していないかなど、ホームページのセキュリティ対策を再確認することをお勧めします。

以上、情報セキュリティの観点から、消費者として、また、企業として知っておくべきと考えられる主たる被害の現状と対策について概説しました。次回は、中小企業を含む企業において取り組むことが望ましいと考えられる組織的な対策等について概説する予定です。

ケーブルテレビの役割とパブリックアクセスの導入

九州大学大学院 比較社会文化研究院　大杉　卓三

パブリックアクセスとは、一般の地域住民が自主的に企画、制作した番組を自由に放送する制度、そしてそれを保障する概念である。番組は当然ながら一定のルールにしたがい制作する。放送にはケーブルテレビが主に利用されることから、パブリックアクセスを実現するためにケーブルテレビが果たす役割は大きい。ケーブルテレビは２つの意味でパブリックアクセスを導入することを求められている。第１にはパソコンの普及で映像や音声を記録、編集することが容易になったためにパブリックアクセスが身近に感じやすい概念となったという技術的な理由、第２にはケーブルテレビが地域に根ざしたサービスを今後も続けていくためにはパブリックアクセスの概念を導入することで存在の価値を見いだす必要にせまられていることである。

まず大分県のケーブルテレビの状況であるが、九州総合通信局の「平成17年九州における情報通信の現状」によると、大分県のケーブルテレビ普及率は52.6%。これは全国平均の52.3%を九州で唯一こえる数字である。自主放送をおこなうケーブルテレビについては、大分県45.5%であり、福岡県36.9%、佐賀県42.9%と共に、全国平均35.9%を上回る。大分県は九州においてケーブルテレビの普及が進んだ県と言える。

ケーブルテレビの役割は難視聴対策や多チャンネル放送をおこなうテレビ放送の機能だけではなく、ＡＤＳＬや光ファイバーと並びブローバンドのインターネット接続サービスを提供する通信の機能も併せて持っている。特にＮＴＴなど民間通信事業者によるブロードバンドのサービス提供が困難な地域では、ケーブルテレビを整備することがブロードバンドを普及させることも同時に意味する。

このようにケーブルテレビの役割は大きく、また医療、福祉、災害などの行政の情報システムが動作するためにも欠かせないことから地域の重要な総合的な情報通信基盤として認識されている。しかしケーブルテレビの置かれた状況が、競合する情報通信サービスからの脅威を受ける状況では無いかといえば、むしろ逆である。ＡＤＳＬや光ファイバーなどのブロードバンドが普及したことでダイアルアップのインターネット接続の時代には不可能であった動画コンテンツのインターネット配信やいわゆるインターネットテレビのサービスを登場させた。大手の参入も相次いでおり無料の動画配信サイト「GyaO」は既に登録者が500万人をこえる。動画をスムーズに配信できるほどのブロードバンドであれば、ケーブルテレビのテレビ放送を含むほぼ全ての機能を実現できる。このためケーブルテレビは「ケーブルテレビにしかできないこと」を見いだし、競合するサービスから生き残りを図る必要がある。ケーブルテレビにしかできないこととは地域の住民のニーズにあった地域密着の番組（コンテンツ）を制作しチャンネルとして編成して放送することであり、これを生き残り手段とするためにパブリックアクセスを導入しようとしているのである。

地域住民が制作した映像を番組として放送することは現在でもケーブルテレビで一般的に行われている。ケーブルテレビには地域に密着した情報を発信するために「コミュニティチャンネル」や「行政チャンネル」が用意されており行政が放送の費用を負担するこ

とが多い。これらのチャンネルで放送される番組の内容はケーブルテレビやスポンサーである行政の意向に添うように制作され、番組制作そのものはケーブルテレビや委託された映像制作会社がおこなう。つまりチャンネルの番組編成や番組の制作そのものに一般の地域の住民が介在することは少ない。パブリックアクセスという概念はこれとは異なり、地域の住民が自発的に番組の企画、制作することで本当に地域に必要とされる番組を放送することができ、またそれが制度としても保障される。現状、コミュニティチャンネルや行政チャンネルの番組を制作するためにケーブルテレビ職員は運動会など地域イベントがおこなわれる祝祭日にも出勤して番組制作をおこなっているが取材できる内容は限りがあり、番組が視聴者である地域住民のニーズに適応しているか判断は難しい。

パブリックアクセスという単語を初めて聞くと難しく感じがちであるが、内容を知るとコミュニティチャンネルが本来果たすべき役割であると容易に認識することができる。パブリックアクセスの導入について、例えばアメリカでは1984年に権利として法律で保障され、ヨーロッパやアジア諸国をみても取り組みとしてめずらしいものではない。日本でも米子市、三鷹市、神戸市など多くの地域でみることができる。九州の事例として身近なところでは熊本県山江村の住民ディレクター制度が有名である。山江村では2005年９月に第３回市民メディア全国交流集会が開催され（写真）、日本全国のパブリックアクセスの取り組みが紹介された。

大分県はケーブルテレビの普及が進んだ県として、インフラの面ではパブリックアクセス導入を進める素地が整っているといえる。ただし導入のためには制度としての準備も必要となり、また地域住民の側にもＮＰＯなどの団体を設立したり協議会を立ち上げるなどの体制作りが必要となる。ケーブルテレビが地域の総合的な情報通信基盤として存在し、また地域情報の重要な発信源であるために、さらに行政が地域情報化施策のなかに地域住民に保障する制度として導入するために、パブリックアクセスという概念を理解すべきである。

熊本県山江村で開催された第３回市民メディア全国交流集会の様子

中国最新ハイテク産業事情調査

2005年3月10日～2005年3月14日

財団法人ハイパーネットワーク社会研究所 所長　宇津宮 孝一
財団法人ハイパーネットワーク社会研究所 主任研究員　江原 裕幸

1 はじめに

研究所では、研究所が過去10年間にわたって開催してきたハイパーネットワーク別府湾会議の新たな展開が東アジアを見据えて実施できるのかの可能性を探るため、また成長著しい中国の最近の状況を肌身で感じ今後の研究の礎とするため「中国最新ハイテク産業事情調査」を企画した。年度末の忙しい時期であったが、賛助会員、共同研究員および所員等12名からなる視察団が編成でき、2005年３月10日から５日間、中国のなかでも著しい発展をとげる長江デルタ地域に立地するハイテク産業や政府関係機関などを視察した。

大分－上海直行便を利用し、下記の機関、開発区、合弁企業、および中国進出の日本企業等を視察した。

●上海　上海市科学技術中心、創注（上海）信息技術有限公司（ＣＥＣ上海）
●蘇州　蘇州高新区（ハイテク産業開発区）、蘇高新創業園（SND PIONEERING PARK）、科学技術シティ（開発中）、蘇州不二工機有限公司
●昆山　昆山経済技術開発区京阪工業園、ユニテック社、昆山軟件園（Softpark）、中創軟件工程有限責任公司

2 視察報告

ここでは、視察先で強く印象に残ったことがらについて報告する。

〈上海浦東国際空港〉

大分と上海では１時間40分のフライトとなる。上海浦東国際空港は新しい上海の空の玄関として1999年にオープンしており、中国、さらにはアジアのハブ空港となることを目指している。

〈リニアモーターカー〉

上海市へはリニアモーターカーで移動する。このリニアモーターカーはドイツとの技術提携により2003年12月から営業が始まっている。

浦東空港から龍陽路站までの約30kmを７分ほどでむすんでおり、最高速度は431kmに達する。

〈上海市科学技術中心（科学創業センター）〉

科学創業センターはいわゆるインキュベータであるが、他の31ヶ所のインキュベータの統括や新規インキュベータの設立補助業務も行っている。現在中国では上海市に限らず、各種インキュベータが非常に盛んであり、国力の向上（＝産業力の向上）を急いでいるそうである。

〈創注（上海）信息技術有限公司（ＣＥＣ上海）〉

独立系のシステムインテグレータとして昭和43年に創業した株式会社シーイーシーの子会社である創注（上海）信息技術有限公司（以下 創注）を訪問した。シーイーシーは1986年から中国でビジネス展開を行ってきており、創注はその流れの中で設立され、2003年６月13日に設立している。

まず、開発現場を視察させていただいたが平均年齢25才のプログラマーが数十名従事しており非常に若い印象を受けた。また、ドキュメントのオンライン化が進んでおり、机の上にドキュメントがほとんどないことに驚いた。

業務内容は日系企業へのＩＴサービスやインフラ構築、ＳＩ、システム開発・移植システム運用・保守サービスを行っており、人材育成と派遣も行っている。システム開発においてはシーイーシーで上流工程を行い、創注で下流工程を担当している。中国と日本で協業する上で重要となるマネージャ（ブリッジＳＥ）をしっかり確保しているそうだ。

〈蘇州高新区管理委員会〉

（１）蘇州市は、歴史のある古くからの都市である

こと、（2）高新区は、旧市街地とその西側の太湖にはさまれた地域であり、（3）国務院に承認されたハイテク産業開発区であること、（4）単なる企業誘致ではなく、居住地区、国際教育地区、観光開発地区を備えた総合的な開発区であるとのこと。

〈蘇高新創業園（SND Pioneering Park）〉

蘇高新創業園は、蘇州高新区の中核施設であり、創業したばかりのハイテク企業にオフィススペースを貸し出している。1階は、従業員の厚生施設、会議室、レクチャルーム等の共通スペースで、2階～5階が企業に貸し出すオフィススペースになっている。各オフィスは、100Mbpsの帯域幅でインターネットに接続できるようになっているとのことであった。

〈蘇州不二工机有限公司〉

この会社は、蘇州高新区に隣接する光福鎮の工業園（工業団地）にあり、2001年に日本の不二工機の100%出資の子会社として設立され、現在、日本人管理者5名を含めて、280名ほどの従業員がおり、冷凍・冷房用の制御機器とその関連製品を製造・販売している。創業して、4年目になって、現地採用の人の中から、係長級の管理者が育ってきたとのことである。また、あえて市の中心からはずれた、日本人にとっては不便な土地に工場を建設したことにより、就職待ちが常に30人以上おり、採用はいつでもでき、人件費が日本の15分の1程度というメリットを得ている。

〈京阪（昆山）科技工業園〉

昆山市の京阪科技工業園は、日系企業の誘致を目的とした工業団地である。「京阪」という名前も「東京」と「大阪」に由来するものである。もちろん、東京と大阪だけでなく日本全国の大企業から中小企業までを誘致の対象としている。

〈ユニテック・ジャパン〉

第2期工事で作られた京阪（昆山）科技工業園の標準工場に入居した日系企業であるUNITECH ELECTRONICS社は、まだ稼働前の段階であったが、日本人管理者が工場設備の設置や製造機械の据付け・調整から人事、教育、生産計画など、あらゆることを一人でやっていたのに驚かされた。将来的に市場が飽和することが見えているので、3年で回収するつもりと語っていたのが印象的であった。

〈昆山軟件園（KUNSHIAN Software Park）〉

全体で6平方キロの敷地をもち、教育区、商業展示区、研究区、インキュベーション区、高級住宅区から構成されている。2003年9月からソフトウェア技術者の人材養成学校を開校し、現在の生徒数は2000名とのこと。中国の10大ソフト会社、蘇州大学の大学院生が働いており、外国からの受注を受けている。

3 全体を通して

実質3日間の調査を振り返ると

（1）世界の製造工場として、国策で開発区に海外のさまざまな企業や工場を誘致するとともに、ハイテク産業を育成・振興するために、さまざまな優遇策を講じて投資や起業を奨励していること。

（2）進出日系企業は安価で豊富な労働力を基盤にして、優遇策のある期間内に投資コストを回収し、世界での熾烈な競争を制覇しようとしていること。しかし、人材と処遇には苦労していること。

（3）この地域では海外からのソフトウエア受注の期待は高いが、日本語ができる情報技術者不足が深刻である。そのため、中国ビジネスに精通した日本のＩＴ企業向けサービス会社の存在が大きいこと。

この点は、現地化などの推進で成功を収めている台湾ＩＴ企業に見習うべきことが多いこと。

（4）高速交通網の整備を始め、インフラ整備が急ピッチで進められている。雇用の拡大もあるのか人海戦術で北京五輪、上海万博開催までを照準に当てて、すべてが進んでいるように見えること。

参加された賛助会員の皆様とともに、何とか所期の目的を達成できたのではないかと考えている。また、上海で活躍なさっている大分県人会の方々ともお会いし、友好を深めることができたのも副産物であった。最後に、今回の視察に際して、ご支援・ご協力をいただいた関係各位に改めて感謝する。

アメリカ合衆国の情報セキュリティ調査に同行して

財団法人ハイパーネットワーク社会研究所　研究員　中田　優一

2005年7月19日から7月30日まで、アメリカ合衆国を訪問する機会を得た。私にとっては初めての訪米、二度目の海外であった。今回の訪米は、日本電信電話（ＮＴＴ）が多摩大学情報社会学研究所に委託している「欧州・米国・アジアにおけるサイバーセキュリティの動向調査」のうち、アメリカ合衆国における企業や業界団体の取り組みや情報セキュリティ・ビジネスの現状などについての現地調査に、研修として同行するものであった。

今回の訪問地は、東海岸のニューヨーク、ワシントンＤＣ、西海岸のシアトル、サンフランシスコであった。東部では主に業界団体を、西部では企業やベンダーを訪問した。情報セキュリティについて、この訪問を通じて学び、考えたことについて、以下にまとめることにする。

はじめに、企業における情報セキュリティへの取り組みについてであるが、企業における情報漏洩はアメリカ合衆国内でも後を絶たず、その原因として、ネットワークを介しての侵入やパソコンなどの窃盗だけではなく、企業の内部関係者による覗き見や顧客データの誤った使用によるものが多いようである。このような事態を防ぐための取り組みとして、企業内において、ＣＩＯ（最高情報責任者）やＣＩＳＯ（最高情報セキュリティ責任者）といった役職を置き、その人物を中心に、セキュリティ・ポリシーの策定や有効な技術の導入を進めているところが多い。ところが、ＣＥＯ（最高経営責任者）自身がその重要性に気づいていなかったり、具体的な対策やアセスメントなどの考えの相違によってＣＩＯやＣＩＳＯが対立したり、またコストを優先するＣＥＯとセキュリティを優先するＣＩＯやＣＩＳＯとの議論が尽きなかったりしていることが実際には多く、企業の全社員にまで情報セキュリティの意識を浸透させるまでに至っていない企業も多いようである。企業における情報セキュリティを考える上で、まずは社内における役員間での同意と、セキュリティ・ポリシーなどに基づく強固な組織作りを目指すことが重要ではないかと考えた。

次に、情報セキュリティに対する法制度についてであるが、アメリカ合衆国内において、セキュリティが声高に叫ばれるようになったのは、やはり2001年９月11日のテロ事件以降のことである。政府機関として、ＤＨＳ（Department of Homeland Security）が設置されたり、ＳＯＸ法（サーベンス・オックスレー法）などの法律が制定・施行されたりしている。ＳＯＸ法は、上場企業に対して会計情報の開示を求めるものであるが、企業の情報セキュリティに関係する法律として話題性が高い。他にも州単位や連邦政府において、個人情報保護に関する法律が制定・施行されている。しかしながら、これらの法律も企業における情報セキュリティの確保に対して完璧なものではないようである。一般に、アメリカ社会ではプライバシーが重要視されていて、インターネット社会における情報セキュリティについても、法整備も含め国家として相当の取り組みがなされていると想像していたが、必ずしもそうではないようである。

最後に、情報セキュリティ確保のための技術および製品の動向についてであるが、そもそも製品のセキュリティについては、従来の製品の危険な部分を新技術

によって回避するというアプローチによることが多いようである。それ以外にも、例えば、ＢＩＯＳレベルでのセキュリティ強化に取り組んだり、強固な認証システムの開発にあたったりしている企業もあり、ユーザーが外部からの侵入への対策と内部からの情報漏洩への対策に取り組めるような製品を開発し、市場に送っている。また、製品や技術の開発側は、情報セキュリティへの対策について、その開発した責任も考慮しつつ、まずは民間で行われなければならないという認識が強く、国家によって強制されるべきものではないと考えているようである。しかし、政府と民間の役割を明確にしながら、政府は法律の制定や必要な国家予算を充てる、民間はより洗練された信頼性の高いシステムを開発するというように、それぞれがそれぞれの役割を果たすことが重要であることも認識しているようである。

一般的に、自国の安全を守るために必要な政策を決定・実行したり、必要な機関を設置し、法律を制定・施行したりするのはその国の政府の重要な役割である。情報セキュリティ対策についてもこの例外ではないが、インターネット社会においては、ある特定の国家や集団の中だけで情報セキュリティ対策が行えないのも事実である。そのような中、情報セキュリティの専門機関や大学、政府機関や企業などの専門家が集まり設立されたAgoraという集団のように、シアトルという地域に始まり、伝統的な組織の形態を持たずに政府と民間が一緒に活動を行うという珍しい取り組みも見られる。今後、インターネット社会全体のセキュリティを確保し、維持していくためにも、アメリカ合衆国のみならず、各国の政府と民間とが議論したり、共同に研究したりすることができるような組織や機関がより重要になると考えられる。

私にとって初めての訪米で、一度に東部と西部の主要都市を回ることができたのは大変貴重な経験であった。海外では、言語や文化的背景の違いなどにより、交通機関の利用、宿泊先の確保や食事など慣れない場面が多い。幸いにも、今回の訪米で事件や事故に巻き込まれることはなかったが、慣れない土地では、やはり慎重にかつ余裕を持った行動をとることが大切であると改めて感じた。また、日頃から英語力を磨き続けるとともに、情報セキュリティに関する知識を増やしたり、その動向を把握したりすることが必要であることを痛感した。

結びに、今回の訪米に同行させていただいたハイパーネットワーク社会研究所の会津副所長並びに国際大学ＧＬＯＣＯＭの上村主任研究員には、この紙面をお借りして改めて感謝の意を表したい。また、事前・事後に多大なるご支援をいただいたハイパーネットワーク社会研究所の皆様にも敬意を表したい。

第48回ハイパーフォーラム開催報告

テーマ「情報セキュリティ最前線」

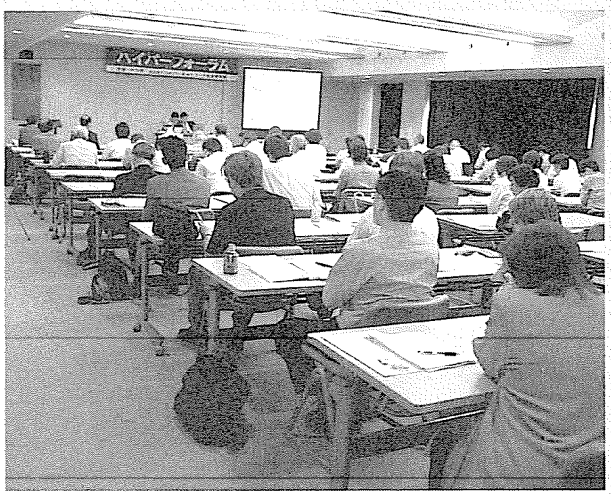
～現状と最新動向について日本と韓国から～

2005年８月19日（金）13：30－17：00大分第２ソフィアプラザビルの２階ソフィアホールにて、約100名の参加者をいただき、48回目となるハイパーフォーラムを開催した。

今回のフォーラムでは、ここ数年急激に重要性を増してきた情報セキュリティについて、その最前線で活躍されている二つの団体から講師を招いて、講演いただいた。一つは日本の独立行政法人で情報処理推進機構（ＩＰＡ）である。もう一つは海外から、ＩＴ先進国である韓国の韓国情報保護振興院（ＫＩＳＡ）である。どちらもまさに最前線に立って活動されており、現在の情報セキュリティはどういった状況にあるのか、また今後どういった方向に進んでいこうとしているのか、といった最新の情報について理解を深めることができるものであった。

まず講演に先立って、ハイパーネットワーク社会研究所副所長会津氏より、情報セキュリティについて、これまで研究所で取り組んできた経緯や現在の状況について、概要説明を伺った。その事例として、平成16年度に経産省からの委託調査として実施した海外の情報セキュリティの予算と政策、また平成15年度から取り組み始めた中小企業委託事業「情報モラル」啓発などである。

ＩＰＡは、ソフトウェア及び情報処理システムが21世紀の知識経済を支える基盤となることに鑑み、技術・人事の両面から、ソフトウェア及び情報処理システムの健全な発展を支える戦略的なインフラを提供するプロフェッショナルな集団として活動している。情報セキュリティに関しては、セキュリティセンターを中心に、被害状況の把握と情報の発信、暗号技術調査・評価、システムのセキュリティ評価・認定、セキュリティを高めるための技術開発・調査



研究を行っている。そのセンター長である三角氏に、日本における情報セキュリティの現状、そして今後の状況について事例を参照しながら話を伺った。

ＫＩＳＡは、民間の情報保護政策全般の執行を行うために2001年に情報通信部の下部機関として設立された。前身は、1996年に韓国電算院傘下の「情報保護センター」である。組織の主なミッションは、政策の立案・技術開発であり、具体的にはセキュリティインシデントへの対応、個人情報保護、スパム、認証、セキュリティ技術、情報セキュリティ産業支援、ポータルサイトやサイバー空間などについての調査研究を行っている。

今回のフォーラムでは、リ・ホンソプ院長自ら来県いただき逐次通訳という形態にて、講演いただいた。テーマは、「u-Korea戦略と情報セキュリティ」ということで、ユビキタス社会を推進するためのＩＴ839戦略と情報セキュリティについて、詳細な説明を伺った。

発行：大分県　www.pref.oita.jp
編集：財団法人ハイパーネットワーク社会研究所
www.hyper.or.jp　post@hyper.or.jp　Tel.097-537-8180
〒870-0037　大分市東春日町51-6　大分第２ソフィアプラザビル４Ｆ