

ユビキタス情報社会について

徳島大学工学部 森井 昌克

1. はじめに

「ユビキタス社会」という語句が紙上に溢れるようになってすでに久しいが、技術や制度ではなく、確実に社会が、そして既存の文化も変わろうとしている。この変革の時代において、その底辺を支える概念が「デジタル」であり、「インターネット」と称される文化である。インターネットとは決して、その技術のみを意味するものではなく、コミュニケーション、すなわち人だけでなくすべての「物」との会話を中心とした考え方なのである。このインターネットが作る社会の一つの特徴がユビキタスという概念である。このユビキタス社会を官・産・民の三方から急速に推し進められ、あるいは押し進めようとしている。

行政からは「e-Japan」の旗の下に、国の業務を電子化し、インターネットで行うことができる「電子政府」が稼働し始め、その動きは地方自治体に至り、「電子自治体」という言葉も定着し、実現が急速に進められている。行政における申請書類の「電子化」については1994年から取り組んでいるものの、申請書類をワープロ等で作成し、そのファイルを物理的媒体（例えば、フロッピーディスク）を通して提出すると言う形式を指していた。物理的媒体ではなく、ネットワークを介して、しかも実時間（リアルタイム）で対話的（インタラクティブ）に申請やその受理に関する手続きを行う、文字通りの「電子行政」を目指している。その際、もっとも大きな障害は「セキュリティ」に関する問題である。人の行動や物に対する警備等、物理的なセキュリティは当然のこととして、通信やコンピュータネットワークに対するセキュリティの問題も今に始まったわけではない。社会が大きく変わっていく中で、セキュリティの概念自体も大きく変えなければなら

いのである。2004年2月、政府は「e-Japan 戦略」（2003年7月、IT戦略本部決定）を加速させ、「2005年までに世界最先端のIT国家になる」との目標を達成するため、「e-Japan 戦略 加速化パッケージ」を策定し、重点施策を与えた。その6つの重点施策の一つがセキュリティであり、セキュリティ政策の強化と名うって、「安全・安心」をキーワードに、特に組織と人材の育成に力を入れている。

産側においても、インターネットを中心とするIT技術を利用したサービスが急速に進められている。例えばインターネットバンキングや携帯電話を利用したモバイルバンキングと言った銀行窓口業務の「電子化」である。また、24時間サービスを目指して、ATM（現金自動支払機）が全国数千というコンビニ店舗に設置されている。銀行や郵貯のキャッシュカードを、そのまま利用できるデビットカードも全国数万の店舗で利用できるようになり、利便さを追求したサービスが提供されつつある。さらに、Eddy等の電子マネーも実用化に具されつつある。実際にビジネスの場面においても、「在宅勤務」という言葉はすでに死語になり、もっともユビキタス化が進んでいると言っても過言ではない。ビジネスにおいて、場所、時間、相手を選ぶことなく、無線LANや携帯電話、PHS等によるモバイルインターネット環境、さらにADSL等のブロードバンド環境を利用して、オフィスや業務窓口と変わらないサービス、事務作業を提供している。この場合もセキュリティの問題は深刻である。ネットワークを利用することによって、第三者の不正アクセスや未必の故意による情報漏えいの可能性が大幅に増大したのである。また、ネットワークの一般的普及によって、2次的な情報漏えいが加速度的に拡散し、そ

ユビキタス情報社会について（森井昌克）

電子自治体時代の情報政策

の実質的損害の大きさは計り知れないほどのものとなりつつある。コンピュータ(パソコン)自体の高性能化低価格化、データ記憶媒体の小型大容量低価格化によって個人情報を含む機密情報自体の取り扱いが容易になり、特に個人情報においては、その収集方法も従来に比較して容易になっていることから安易な取り扱いとなることも少なくなく、これが情報漏えいの温床となっている感がある。

民側の個人に目を移すと、インターネットや携帯電話の急速な普及は、その効果や影響力を必ずしも理解せずに利用することから大小さまざまな問題を起こしながら、現在に至っている。特にインターネット上の掲示板や携帯電話メールは予想できない状況で、その内容や影響が急激に膨張する可能性があり、社会的混乱を引き起こすことも少なくない。さらに、それらを利用することによる、不利益への不安、特にセキュリティへの不信感、プライバシーの流出に関する不安が大きい。このことは産から民へのネットワークを利用したサービスへの障害となっており、事実、インターネットやICカードを利用したサービスを拒否する理由の第一がセキュリティへの不安という調査結果が知られている。

本稿では、インターネットという概念によるユビキタス社会の理解を目的として、その現状と動向、およびその問題点をセキュリティという切り口から取り上げ、最近の事例から動向を分析するとともに、その対策について考察する。

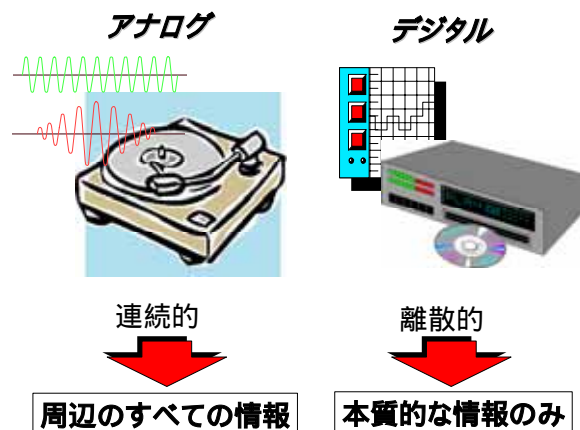
2. ユビキタス社会の脅威

本章では、インターネットという考え方、言わば思想を与え、その結果としてのユビキタス社会を概観する。

2.1 インターネットとは何なのか。

インターネットは「時間と空間」を超越する。古

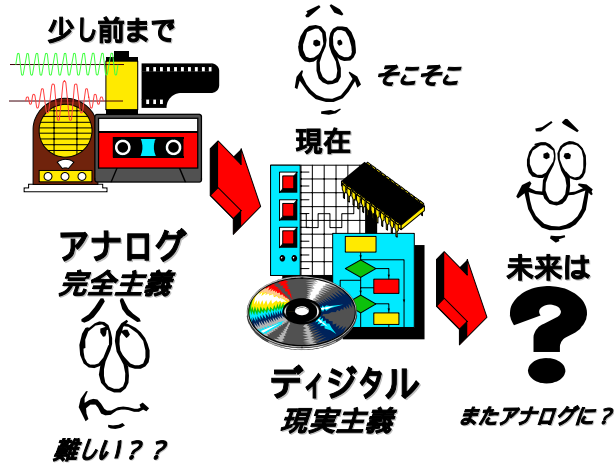
来、様々な技術は、この「時間と空間」からの開放を目標・理想として発達してきた。デジタルという発想は、その技術における新しい展開のブレークスルーであり、インターネットは特に、人だけでなく、もの(機械)を交えた会話を中心に添えた技術革命の思想である。



技術用語としてのデジタルは、連続という意味を持つアナログに対する言葉であり、離散的、非連続などの意味を有する。ある情報の量を表そうとするとき、その量を厳密に表そうとする連続量(アナログ)か、どの程度多いか少ないかを表そうとする離散量(デジタル)かの違いである。元来、情報はアナログで表されるべきものである。事実、世の中の現象はすべてアナログ量であるといっても過言ではない。現在、このアナログを正確に扱うには非常に高い技術が必要であり、事実上困難なのである。しかし、一步退き、正確に表すことを諦めることによって、極めて容易にその情報の量を扱うことが出来る。言うなれば、完璧を目指して、高いコストをかけて、ほぼ完璧を実現するのではなく、最初から完璧を目指すことなく、ほぼ完璧を目指せば、非常に低いコストによって実現できるのである。アナログレコードとCDの音質の差がアナログとデジタルの差を顕著に表している。非常に高いコストをかけた十分な設備があれば、アナログレコードの情報をすべて引き出すことができ、結果として高音質を得られるが、逆に高いコストをかけなければ、その

電子自治体時代の情報政策

音質は極めて劣るものとなる。しかしながら、最初から高いコストをかけて高音質を引き出すことを諦めることによって、極めて低いコストで、そこそこの高音質を実現できることが可能となる。この「そこそこの」という、完全なものから一步退くことで、新しい可能性が見えてくること、いわゆる「発想の転換」がデジタルという考え方なのである。



インターネットは、このデジタルの発想を具体的に実現する一つの形となっている。そのキーワードが「ベストエフォート (Best Effort)」である。それは最善努力と訳することができる。インターネット以前では、ベストエフォートではなく、最低保証 (Guarantee) という概念からシステムの構築を行っていた。例えば電話である。電話では、データ (音声) を送る仕組みが非常に複雑であることに対して、インターネットでは非常に単純である。電話という単に信号を音に変えるだけの機械であるがゆえに、音声を送る部分、すなわち通信システムの部分を複雑にせざる得ないのである。最低保証がゆえに、相手の電話機へ確実に、それも正確に音声をお届けしなければならないからである。インターネットでは電話ほど確実に相手にデータをお届けする必要がなく、確実に相手にデータをお届けを保証をしない仕組みになっている。そうすることによって、データを送り届ける仕組みが非常に簡単になり、その結果、装置も安価に、しかも運用管理も容易になる。もちろん、インターネットにおいてデータが確実に相手に

届かないということでは決してなく、単に保証していないだけである。一般にはインターネット端末はコンピュータ、あるいは同等の能力を持つ機械であり、電話機に比べて極めて複雑な処理をすることができる。データを送るという処理の一端を機械に担わせることによって通信システムを簡素化している。これは必ず通信できる、つまり確実に相手へデータを送ることは保証しないが、最善努力を行う仕組みを提供している。インターネットは「いいかげんなネットワーク」と呼ばれることもあるが、この意味はデジタルと同様、発想の転換を表している。完璧ではなく、ほぼ完璧を目指すことによって大きな技術変革や発想のブレークスルーになる場合があり、インターネットはその典型ともなっている。



ネットワークの集合体

自律分散 + インターオペラビリティ = インターネット

ひとつひとつのネットワークがそれぞれ独自に機能する。

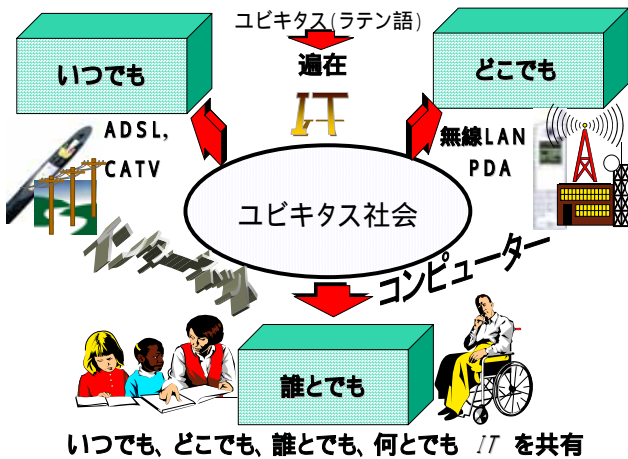
独立したネットワークが相互に協調して機能すること (相互運用性)

この「いいかげんなネットワーク」の特徴は、決して不安定な信頼性のないネットワークであるということではなく、必要最小限の約束事を決めて、インターネットを構成するひとつひとつのネットワーク (LAN 等) および端末が、それぞれ独自に機能させることができるということである。すなわち「自立分散型ネットワーク」と呼ばれる。



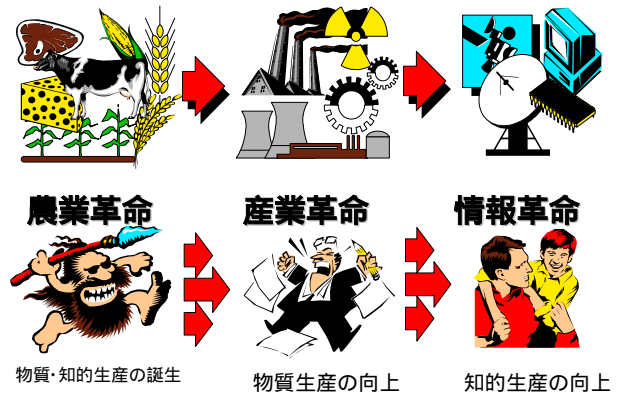
2.2 ユビキタス社会とは

ユビキタス Ubiquitous はラテン語で、「遍在」という意味である。遍在とは、「どこにでもある」という意味であり、情報通信の世界で用いられる場合は、「いつでも、どこでも、誰とでもコンピューターやインターネットを利用できること」となる。この偏在性のあるインターネットが普くすべての人に恩恵を与えることをユビキタスコンピューティングと呼び、それが実現する社会をユビキタス社会と呼ぶ。



ユビキタス社会は、以前、「第三の波」あるいは「情報革命」と呼ばれた人類における第三番目の革命の実現である。人間の歴史は、個々の人間の自由な時間を作るため、いかに努力したかの歴史であるという見方ができる。すなわち、太古の時代、人類は食糧の確保にほとんどすべての時間を取られていた。それが農耕・牧畜を行なうようになり、食量

の確保以外の時間が取れるようになった。これが第一の革命、農業革命である。この革命によって生まれた時間が知的生産活動を生み出した。文化の誕生である。この知的生産活動の一つの産物として、機械を生み出した。蒸気機関の発明に始まる産業革命である。この産業革命によって、より物質の生産性が高まり、さらに人間に自由な時間が与えられた。情報革命は、コンピュータとネットワークを主たる道具に、知的生産性自体を向上させようとしているのである。

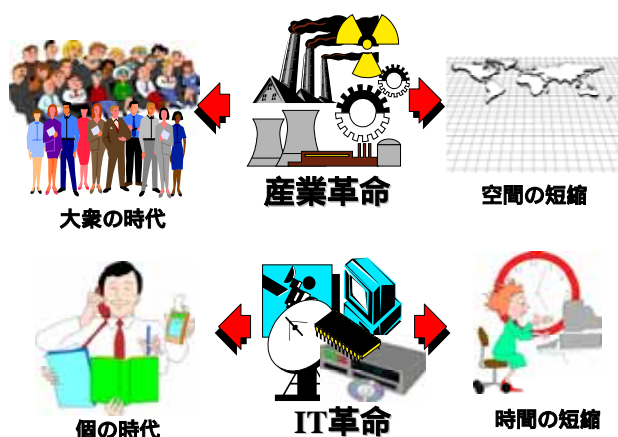


この社会変革を理解するために 18 世紀から 19 世紀にかけて進められた産業革命をさらにひも解くことが早道である。蒸気機関の発明によって、大量に物を、さらにその物を作る機械自身を生産できるようになった。この物質の豊かさは人々の生活、つまりライフスタイルを一変させ、特に 20 世紀は、この産業革命の集大成の時代となった。20 世紀、特にその後半のライフスタイルを一言で表せば「マス(大衆)」の時代と言える。鉄道網さらに自動車道路、空路が整備され、結果として「距離(空間)」という障害が緩和され、生産物を運ぶと共に、大衆が集団としての情報を共有する時代である。さらにラジオやテレビに代表される放送は、大衆が情報を共有するために要する時間を縮めることとなった。

情報革命の実現であるユビキタス社会は「個」の時代と考えられる。大衆が一方向の情報を共有する時代から個人が双方向の情報を共有する時代にな

電子自治体時代の情報政策

るのである。さらに電話程度の技術であった、個々の情報を共有する手段が、情報通信技術の発達によって、三次元画像や触覚、臭覚といった感覚を共有できるようになり、無限大の情報を一瞬にして双方向で伝達できる時代となる。世の中は「時空」という言葉が表すように、「空間」と「時間」から成り立っている。人間のコミュニケーションを考えた場合、産業革命は「空間」を著しく縮めることに成功した。情報革命は「時間」を著しく縮める可能性を秘めている。産業革命以上にライフスタイルを一変させ、大きな社会変革をもたらすことは必然であろう。従来の組織と大衆との間のサービス（生産）活動から、組織と個人のサービス活動に、そして個人と個人のサービス活動に移行することにより、経済を含む社会構造が激変する。それがユビキタス社会である。



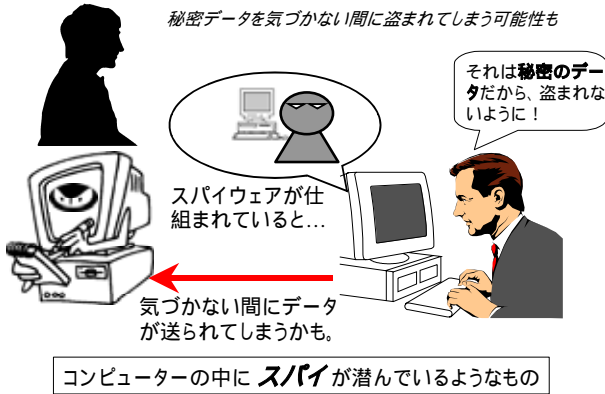
3. 新たな時代の危機管理

3.1 不正アクセスの脅威

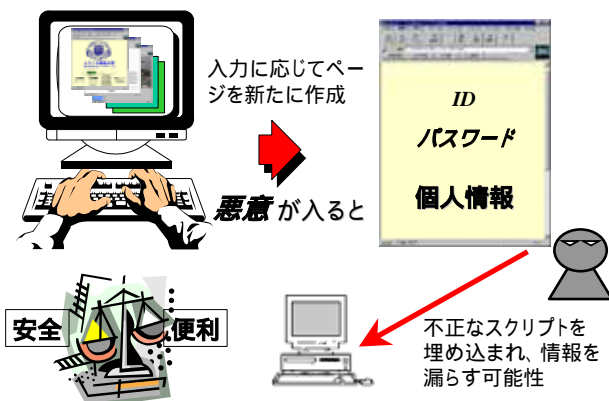
不正アクセスとは、ネットワークの外部から、あるいは権限のない内部のものが、ネットワークを通してコンピュータに許可なくアクセスする行為である。2000年2月に施行された不正アクセス禁止法では、このような行為、もしくはアクセスに必要なパスワード等を盗んだり、そのパスワードの不正な授受に対して、1年以下の懲役刑等の厳しい罰則で臨んでいる。この法律は、コンピュータに許可なくアクセスした場合だけでなく、IDやパスワード

を不正に入手、あるいは授受しただけで取り締まりの対象となる。すなわち、友人、知人のIDをその許可無く使用しただけで罪に問われ、公の掲示板で記載されていたIDであっても、その所有者の許可無く使用した場合も同等である。さらに、IDを利用しなくとも、第三者に告げただけで罪を問われる可能性もある。これは欧米に比較しても厳しい処罰規定であり、特に不正アクセスからファイルの改ざん等を行って詐欺行為に及んだ場合は、電子計算機使用詐欺罪等が適用され、懲役10年という重い処罰が科される。この法律は欧米主要諸国がすでに不正アクセスに対して処罰を行う法律を整えていた中で、それらの国からの強い要請によって成立したものである。すなわち、この法律の施行までは、ファイルを壊すことなく不正にアクセスした場合、それを処罰する明確な規定が存在しなかったのである。このため、不正なアクセスを試みるものは、直接、目的のコンピュータに侵入することは行わず、日本のコンピュータを介して侵入する傾向があった。理由は国際捜査に対する相罰制の原則によって、捜査の及ばない可能性が高かったからである。しかし法律の整備によって不正アクセスの問題が解決されたわけではない。特にインターネットの場合、法律の有無にかかわらず、接続された世界中のコンピュータから標的にされる可能性がある。特に急速に普及したADSLやCATV等を利用する高速で常時接続型の、いわゆるブロードバンドと呼ばれるインターネット接続形態をとるコンピュータは少なからず自己防御する必要がある。

スパイウェア



クロスサイトスクリプティング

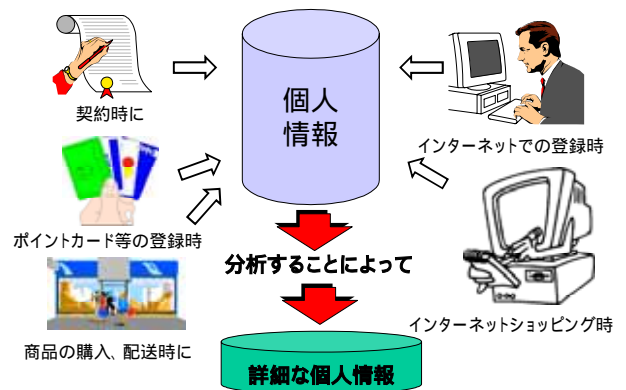


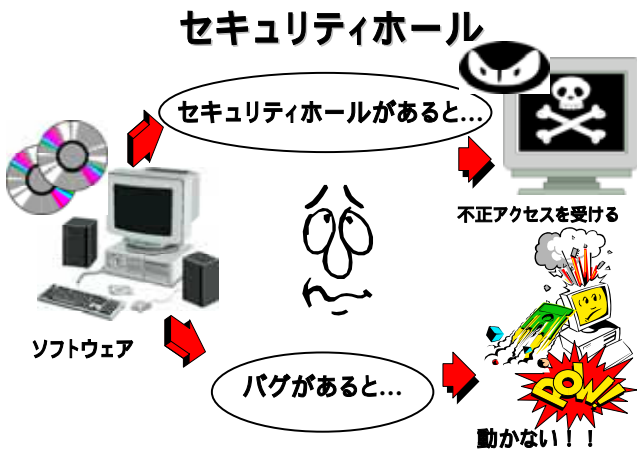
3.2 情報の不正流出と管理

不正アクセスによる情報流出、特に個人情報の流出が問題となっている。しかし、情報流出そのものは、ネットワークやコンピュータへの不正アクセスが、その方法として主たる以前に、大きな問題となっていた。特に企業や自治体において、その情報管理意識と能力の欠落から、その組織内部のものや管理を委託している組織のものから流出していたのである。近年、ネットワークの利用によって、情報流出の危険性が増大し、実際、個人情報の流出は事件として、マスコミ等に取り上げられるだけでも少なくない。この背景には次の原因があると考えられる。一つは、守るべき情報そのものが、ネットワークを介して、不特定多数の手の届く領域に存在しているという事実である。すなわち、セキュリティ対策を施していなければ、情報を奪取することが可能となったのである。例えば言えば、現金を引き出す銀行ATM(現金自動支払機)が管理の目が行き届

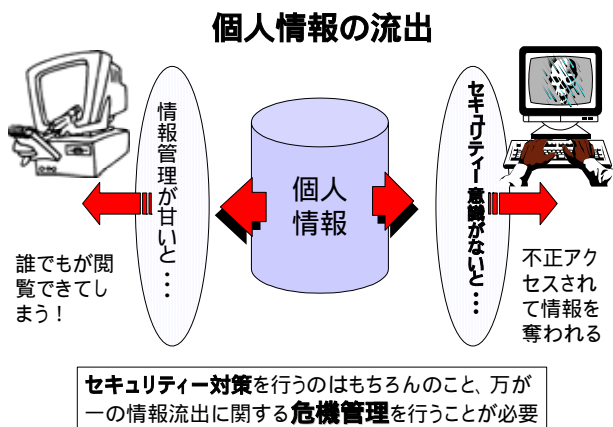
いている銀行内や公衆の面前ではなく、誰も見ていない個人の面前に設置されたようなものである。現在まで問題となったネットワークを介した個人情報流出のほとんどの原因は、セキュリティ対策の欠如であり、特別な不正アクセス手法を使うまでも無く、誰でも容易にWebから閲覧可能であったことによる。さらに一つは個人情報に対する意識の低さである。ネットワーク利用以前は、個人情報の収集においては多額のコストを要し、その整理分析にもコストを要することから、その管理において少なからず意識を持って対処を行っていた。しかしながらネットワーク利用が一般化することによって、個人情報の収集もWebを用いて、半自動的にを行い、その整理分析も自動化され、その管理においての意識が低くなっているのである。他の原因として、ネットワークによる急速、広範囲な情報拡散が上げられる。個人情報や企業情報が漏れ出した場合、その情報がネットワークを介して、極めて短時間かつ広範囲に流出するのである。いったん流出した場合、短時間の間に多くのWebに、そのコピーが貼り付けられ、事実上、流出を止めることが困難になる。ある自治体のWebにおいて個人情報が入り込んでいたとしても誰でもが閲覧可能である設定となり、一定時間の後に、設定を変更し、閲覧を不可能にしたにも関わらず、検索サイトのキャッシュページ(ある時点でのWebのコピーが保存されている)に保存されたまま公開され続けたことがあった。

個人情報の収集





企業情報や個人情報の流出は、その価値に関わらず、その企業および組織のセキュリティ意識、しいては管理能力の低さを示すものである。特にその情報流出の露見が、その企業自身によるものではなく、第三者からの通報によるものであり、事後の十分な対策を練ることもなく、危機管理能力が欠如している企業も少なくないのである。特に個人情報の代償に関しては、かつてある自治体での住民の個人情報流出に対する慰謝料請求において、1件あたり1万5千円の支払いが認められている。また、最近では、あるカード会員の情報のうち、56万人分の個人情報流出し、その企業は各会員に対して500円分の商品券と詫言状を郵送する代償を支払い、その代償にかかるコストとして約6億円を要することとなった。



「個人情報へのアクセスをコントロールする権利」
 ウィリアム・ボガードの著書「監視ゲーム プライヴァシーの終焉」より

不正アクセスとは異なるものの、ネットワークでのセキュリティに関する大きな問題として、風説の流布がある。「風説」とは、いわゆる噂（うわさ）のことであり、風説の流布とは、株式相場を意図的に操る目的で、虚偽の情報や噂を流すことである。最近では、株式相場の分野だけでなく、会社や個人を誹謗・中傷する情報を不特定多数に伝え、損害を与える行為全体に使われている。最近、ある地方銀行がつぶれるという内容のメールが不特定多数に配信され、その内容に惑わされた人たちが、預金を下ろすために銀行に殺到するという事件があった。銀行では、突然の大量の預金引き落としによって、ATM内の紙幣が不足したり、窓口や電話での対応に係員が追われるという事態が発生し、信用を失墜させられるという大きな損害を受けた。ある大型小売店では、問題のあった食品を購入した顧客に、その購入証明なしに代金を返納するということが、ネットワークを通じて誇大に広まり、購入に関係なく、全国各地から返納を求める人が殺到し、その食品の売買代金の3倍以上の金額を返納するまで続けたという事件も起こっている。この事件では、噂がインターネットの掲示板を通じて広まっており、この事実に対して、大型小売店が何も対処しなかったことが原因である。その他にも企業の信用を失墜させる原因となり得る誹謗中傷の類がネットワークで流され、通常は大きな問題となることも無く消えていくものの、その情報が引き金となって大きな問題を誘発することも少なくない。自組織内の情報

電子自治体時代の情報政策

の管理は当然のこととして、自組織外の情報に関しても無視することなく、管理することが重要となってきた。



4. むすびにかえて - ハザードトレラントシステム -

最近の不正アクセス、情報流出、および風説の流布の問題は上述のように深刻であるものの、その本質自体は今に始まったわけではない。ユビキタス社会の到来によってその発現の可能性が増すとともに、被害規模が拡大したのである。したがって対策方法は当然異なるものの対策の本質は大きく異なるわけではない。ユビキタス社会の到来を自覚し、それを本質的に理解することによって自ずから具体的な対策は見えてこよう。ただ、最近の風説の流布による被害や情報流出、特にその結果による組織の信用に対するダメージを考えると、セキュリティポリシーを定める等、組織内の情報管理とともに、組織外の情報管理の必要性は指摘されよう。

組織の機密情報の流出や風説の流布自体、組織にとっては防ぐべきものであり、それが起こりうる組織の体質、状態に問題があることは否めない。しかし、その以上の問題は、情報の流出や風説の流布等が起こった際の早急な事実確認の大幅な遅れである。ユビキタス社会では、今まで述べたように「時間と空間」が極めて縮小された世界である。一刻の

遅れが大きな被害をもたらすのである。最近の個人情報流出も、それが起こったこと自体、大きな問題ではあるものの、さらに大きな問題はその発覚が組織内で調査されたものではなく、外部からの指摘、それも流出した時点から大幅な時間が経過していることである。組織の情報、すなわち広い意味で組織が組織外においてどのように考えられているかを可能な限り監視する必要がある。すなわち、不正アクセスや機密情報流出、風説の流布を未然に防ぐために、組織内教育、セキュリティポリシーの策定・厳守、さらに技術的対策とともに、不幸にして、上記に類する事件・事故が起こった場合、その被害を最小に抑えるための事前の対策を講じることが必要なのである。例えば、機密情報流出に対しては、それが保存されたハードディスクや磁気テープ、CD、DVD等のデータ蓄積媒体の盗難や紛失を予め想定し、データ自体については、堅固な暗号化を施す等の処置が必須となる。風説の流布に対しては、常にネットワーク上での自組織に関する情報(評判、うわさ、中傷、意見等)を監視し、風説の流布を誘発する危険度が高い情報に関しては、対抗記事を投稿する、あるいは正確な情報をそのネットワーク上だけでなく、新聞・雑誌等によって発表し、事前に封じ込めることを試みる必要がある。WEBや掲示板の情報に関してはプロバイダに問い合わせ、質問、警告等を発することも考えられる。先にも述べたように、機密情報の流出に対しても、その流出したという事実以上に、インターネットを通じての二次被害が深刻である。この場合にもネットワークでの自組織に関する情報監視は有効である。

このように事件・事故を想定し、被害を最小に抑えるための危機管理が必要となっており、情報セキュリティの分野でも、セキュリティ技術を含めて、被害(危険)を未然に防ぐ対策ではなく、被害(危険)を想定し、被害に耐性のあるシステムの構築、すなわちハザードトレラントシステム(Hazard Tolerance System)の構築が進められている。

ユビキタス情報社会について(森井昌克)