トピックス

オープンネットワークにおける情報セキュリティー
ー 産業インフラとしての「電子認証」ー

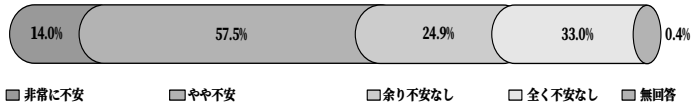
経済産業調査部門　末廣　譲凡

IT技術の進歩、なかんずくインターネットに代表される情報通信ネットワークの発展は、距離あるいは時間の制約を取り除くことにより、経済社会活動を効率化させることが期待されている。しかしながら、インターネットなどのオープンなネットワークを通じた通信においては、通信相手を特定できないなど、セキュリティ面での不安を抱えており、このことが情報ネットワークの活用の障害となっている。このネットワーク上での安全性を確保する手段が「電子認証」であり、情報のネットワーク化が進むにつれ、その一層の普及が見込まれている。

1．ネットワーク上のセキュリティ

インターネットなどオープンなネットワーク上での通信は、その非対面性あるいはオープン性から、通信相手が特定できず、また、通信内容が盗聴されたり、改ざんされたりするリスクにさらされることになる。こうしたリスクは広く認識されており、最近の調査では、７割以上の企業がネットワークのセキュリティに不安があるとしている。

図表－１　セキュリティに関する不安



（資料）日本ベリサイン社00/8調査

また、同調査では具体的な不安事項として、ネットワークへの不正侵入、データを盗まれること、データの盗聴・改ざん、顧客情報の漏洩などに加え、電子商取引分野における偽りの発注や事後否認などがあげられており、ネットワークに絡むリスクが、企業として無視し得ない重大なものであることがわかる。

図表－２　セキュリティに関する不安事項

不正侵入	53.6%	顧客情報漏洩	30.0%
ﾃﾞｰﾀを盗まれる	46.0%	ﾎｰﾑﾍﾟｰｼﾞ書換	24.5%
盗聴	45.2%	偽り発注	14.9%
改ざん	45.0%	事後否認	8.8%

（資料）日本ベリサイン社00/8調査

2．公開鍵基盤による電子認証

こうした事態を回避するため、ネットワーク上で通信相手の本人確認を行うのが、電子認証であり、これがセキュリティの基本となる。この電子認証方法には、単純なものではパスワードが用いられるが、堅牢性・カバー範囲の広さなどから、公開鍵基盤(Public Key Infrastructure：以下、ＰＫＩ)と呼ばれる暗号技術を用いた認証システムがネットワーク時代のセキュリティを支えるものとして注目されている。このPKIに基づく認証システムにおいては、暗号技術に基づく電子署名と認証局と呼ばれる証明機関が発行する電子証明書とを照合することで認証を行う、というのがその基本的な仕組みとなっている。電子署名されたメッセージを電子

証明書に添付のうえ送付し、受取側でメッセージ上の署名と電子証明書にある署名の一致を確認するするという手続きを経ることによって、発信者の本人確認、改ざんの有無などがチェックされることになる。そこでは、各企業・個人の電子署名を電子証明書が証明し、その有効性を認証局が保証するという、現実世界における印鑑証明制度と同様の構造となっている。

3．電子認証の活用事例

ＰＫＩによる電子認証（電子証明書）は様々な用途に用いられている。一般によく知られているものに、ウェブ上のサーバーに対する電子証明書を用いたＳＳＬ（Secure Socket Layer）と呼ばれる暗号化のための通信プロトコルがある。これは電子商取引などで利用が進んでおり、消費者に電子商店の実在性の確認やクレジットカード番号の盗聴防止など、電子商取引の安全性をもたらすことになる。サーバー証明書の分野で圧倒的な市場シェアを有するベリサイン社が認証しているサーバー数は世界で25万にのぼる。

これに対して、クライアント側の証明書を用いてセキュリティを守るシステムも多数存在する。このうち、ネットワークの安全確保を目的としたものに、クライアント側の電子証明書によるネットワークへのアクセス制御がある。これによって、なりすましなどによる不正侵入やデータベースの改ざんを防ぐことが可能となる。また、電子メールでは、盗聴を防止するために暗号化されるケースがあるが、これにもＰＫＩによる電子証明書が利用されている。

この他にも、各企業がＰＫＩを基盤とする様々なシステムの開発を進めており、今後も電子認証は多様な形態で利用が進んで行くものと思われる。

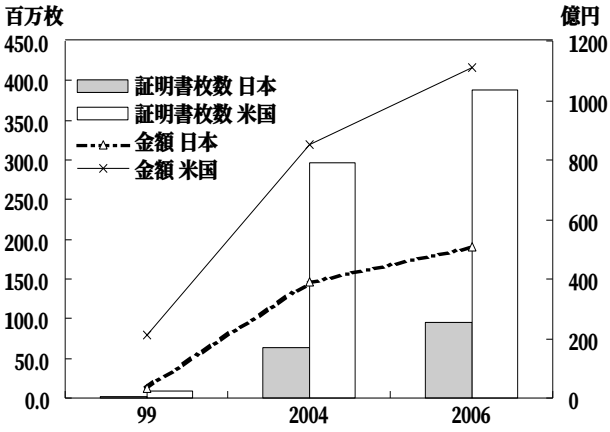
4．電子認証ビジネス

このような電子認証業務、すなわち電子証明書の発行・管理を行ったり、その基盤提供等を行うのが電子認証ビジネスである。認証ビジネスは事業の内容により次の3つに分類することができる。

①事業者が自ら申請者を認証し電子証明書を発行するもので、前述のウェブ・サーバーに電子証明書を発行するサービスがこれに当る。
②各企業が自ら設置したプライベート認証局の運営を代行するもの。
③自ら電子認証業務を行おうとする企業などに電子認証のためのシステムを設計・販売するもの。

現在のところ、わが国における電子認証ビジネスの市場規模は30億円程度(99年現在)と米国の10分の1の水準に止まる。しかしながら、昨今のセキュリティへの関心の高まりなどを背景に、今後は急速な成長が見込まれている。通産省の試算では、2006年の電子認証書の発行枚数は現行の100倍に当たる9,600万枚に達するものと予測されている。

図表－3　電子認証市場



（資料）通商産業省/日本ﾌﾞｰｽﾞ・ｱﾚﾝ・ｱﾝﾄﾞ・ﾊﾐﾙﾄﾝ共同調査

以上のとおり、電子認証はネットワーク社会における産業インフラとして成長していくポテンシャリティを有する。しかしながら、現実に一層の普及を果たしていく上では、暗号技術の更なる進歩やサービス単価の低下など、電子認証ビジネスに従事する企業の一層の経営努力が求められることになろう。