平成１４年度 社会安全研究財団委託調査研究報告書

インターネットビジネスの安全性
および信頼性における調査研究

平成１４年９月
(２００２年)

コンピュータセキュリティ対策委員会
代表　清瀬 紀次

はじめに

2000 年にネットバブルが崩壊し、米国では多くのインターネットビジネス企業が倒産や撤退に追い込まれた。日本においてもインターネットビジネスに対する風潮は変わり、それまでのような甘い期待を抱くことは不可能になった。現在は、的確なビジネス戦略のもと､多くの企業がインターネットを活用して BtoB や BtoC などのビジネスを展開している。現在、自動車産業や不動産産業が BtoC インターネットビジネスを牽引しており、BtoB においては e マーケットプレイスが注目され、市場規模は年々拡大する傾向にある。

1993 年、アメリカではゴア副大統領(当時)が情報スーパーハイウェイ構想を打ち出したことで情報通信分野の規制緩和が急速に進み、ネットワークインフラストラクチャが整備され、インターネットの発展に寄与した。日本においても、e-Japan 計画のもと、世界最高水準のネットワークインフラストラクチャの整備、人材育成、電子商取引などのインターネットビジネスの普及、電子政府の実現に取り組んでいる。インターネットの普及拡大により、インターネットビジネスへの参加主体も増加することと考えられる。しかし、インターネットビジネスは、その利便性や多様性といった多くのメリットがある反面、商品やサービスを購入する企業にとっては取引相手が見えないこともあり、ビジネスの安全性および信頼性確保のために、一定コストの負担が求められるのが現状である。

インターネットビジネスの安全性および信頼性確保への取り組みは、各企業において、既に行われているものの、ビジネスに与える脅威に見合ったシステムを構築することはきわめて困難である。そこで、ビジネスに与える脅威と経済定期観点とのバランスを図りつつ、ビジネスモデルに対する安全性および信頼性のためにシステム構築について調査研究し、インターネットビジネスの更なる発展に寄与することを目的とし、本書を纏め報告するものとする。

委員長 清瀬 紀次

執筆者

栢沼 伸芳 **株式会社ラック**

八子 浩之 **株式会社ラック**

村上 晃 **株式会社ラック**

西本美緒 **株式会社ラック**

目次

第 1 章　調査の概要

1. 調査の目的

インターネットが登場して以来、ビジネスに活用されるようになって久しい。この間、ドットコムブームの隆盛やネットバブルの崩壊を経て、インターネットビジネスに対する企業の取り組み姿勢やビジネスモデル、企業を取り巻くインターネット環境やサービスは大きく変化している。

いまやインターネットは企業活動や生活において切り離せない道具となっているが、ビジネスの手段としてインターネットが今後も大きく活用されていくためには、その負の側面である不正アクセスや詐欺、悪徳商法などの被害を受けないシステムの構築と運用が行われる必要がある。インターネットビジネスの発展のためには、安全性と信頼性が確保されなければならない。

本書では、日本や世界におけるインターネットビジネスの取り組みおよびビジネスの枠組みについて整理し、そこに存在する問題点や脅威を抽出する。その上で、今後のインターネットビジネスの安全性や信頼性を確保するための課題を分析することを目的とする。

2. 調査の方法

(1) インターネットビジネスの事業動向に関する調査

インターネットビジネスの基本的な枠組みに関して調査を行い、BtoB、BtoC を代表する電子商取引を調査対象として代表的なビジネスを挙げる。また、インターネットビジネスの基盤となるインフラストラクチャやプラットフォームとなる中間層のサービスなど、インターネットビジネスを支える構造について調査を行う。

調査対象：枠組み(インターネット環境、BtoB、BtoC)
　　構造(企業間構造、産業構造)
調査手法：インターネット、書籍、雑誌などのメディアから情報を収集
調査項目：枠組み(人口、代表的なビジネス)
　　構造(ネットワークインフラ層、プラットフォーム層、コンテンツ層の代表的なビジネス、各産業におけるインターネットビジネス例)

(2) インターネットビジネスの市場動向に関する調査

日本企業におけるインターネット活用状況と、インターネットビジネス市場の変遷、また世界各国におけるインターネットビジネスの市場動向を調査する。

調査対象：日本
　　世界（米国、アジア･太平洋、ヨーロッパ、ラテンアメリカ、アフリカ・

中東）

調査手法：インターネット、書籍、雑誌などのメディアから情報を収集

調査項目：各地域の BtoB、BtoC **の市場規模、動向**

(3) **インターネットビジネスの安全性および信頼性に関する調査**

インターネットビジネスを行う企業に損害を与える脅威と、その被害を防止するための情報セキュリティ製品・サービスに関して調査を行う。

調査対象：インターネットビジネスにおける脅威(情報漏洩、なりすまし、改ざん、DoS**、踏み台)**

情報セキュリティビジネス動向(製品、サービス)

調査手法：インターネット、書籍、雑誌などのメディアから情報を収集

調査項目：インターネットビジネスにおける脅威(事例、影響など)

情報セキュリティビジネス動向(市場規模、ビジネス例)

(4) **インターネットビジネス発展のための課題検討**

安全性を確保するための製品の欠点や運用の不備、企業や消費者のセキュリティ意識の低さといった問題点を取り上げ、本来あるべき情報セキュリティの形と現状を改善するための法制度や評価認定などの取り組みを明らかにし、企業や消費者の意識向上のための課題を分析する。

調査対象：問題点(情報セキュリティ製品、企業のセキュリティ確保体制、消費者の認識)

課題(企業における対策、関連法制度など)

調査手法：インターネット、書籍、雑誌などのメディアから情報を収集

第 2 章　インターネットビジネスの事業動向に関する調査

1. インターネットビジネスの枠組みに関する概念整理

インターネットの急速な普及に伴い、インターネットビジネスは急激に発展を遂げている。インターネットそのものは、日本においては 1990 年代前半から普及が始まっており、企業や学術面などの一部の分野においてその恩恵を被っていたが、2000 年から 2001 年初旬にかけての企業、一般家庭に対する普及率は著しい。本節では、BtoB、BtoC などに代表されるインターネットビジネスの枠組みの概念整理を行い、本調査研究の対象を明らかにする。

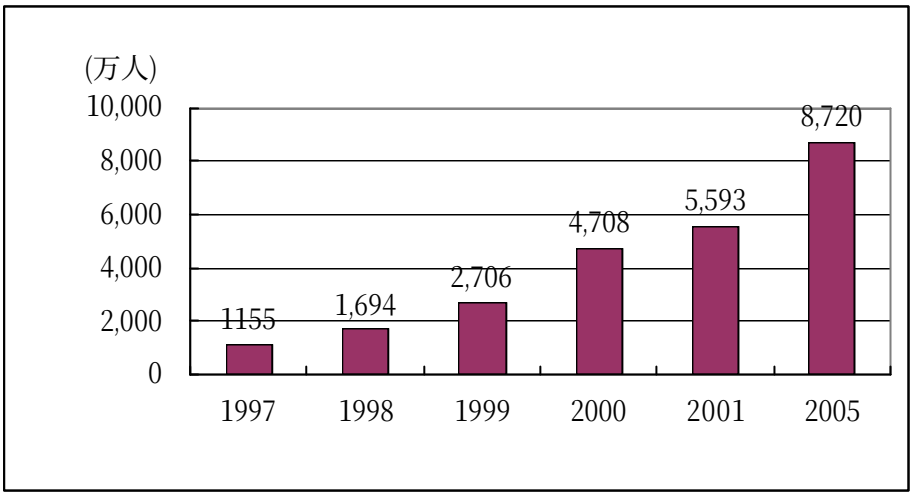
(1) インターネットビジネスを取り巻く環境

a. インターネット人口の変化

総務省が毎年実施している通信利用動向調査によると、2001 年末における日本のインターネット利用者数は 5,593 万人と推計されている。これは前年の 2000 年と比較して 18.8%増加しており、1 年間で 885 万人が新たにインターネット利用を開始したということを示している。2005 年には、インターネット利用者数は 8,720 万人に達する見込みである。日本の総人口におけるインターネット普及率は 44.0%となっているが、このうち、インターネットの世帯普及率については、2000 年末の 34.0%から 2001 年末には 60.5%と増加して全世帯の 6 割を超え、世帯でのインターネット利用が急速に進んでいるということを示している。

また、インターネット事業所普及率は 68.0%と対前年比で 20 ポイント以上も増加し、企業普及率についても 97.6%と既にほとんどの企業で利用されているなど、インターネットの普及は着実に進んでいる。

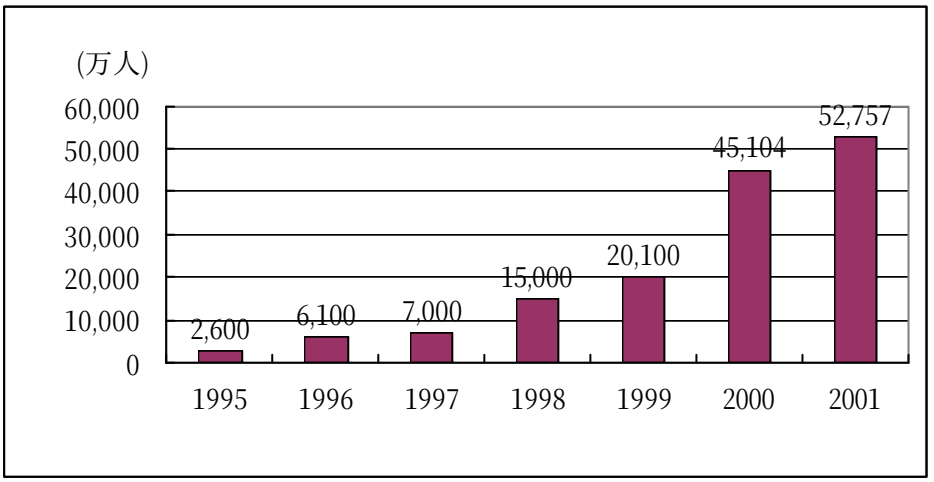
日本におけるインターネット人口の普及状況



(出典) 総務省「通信利用動向調査」

http://www.soumu.go.jp/s-news/2002/pdf/020521_1_01.pdf

世界のインターネット人口



(出典) NUA --- How Many Online?

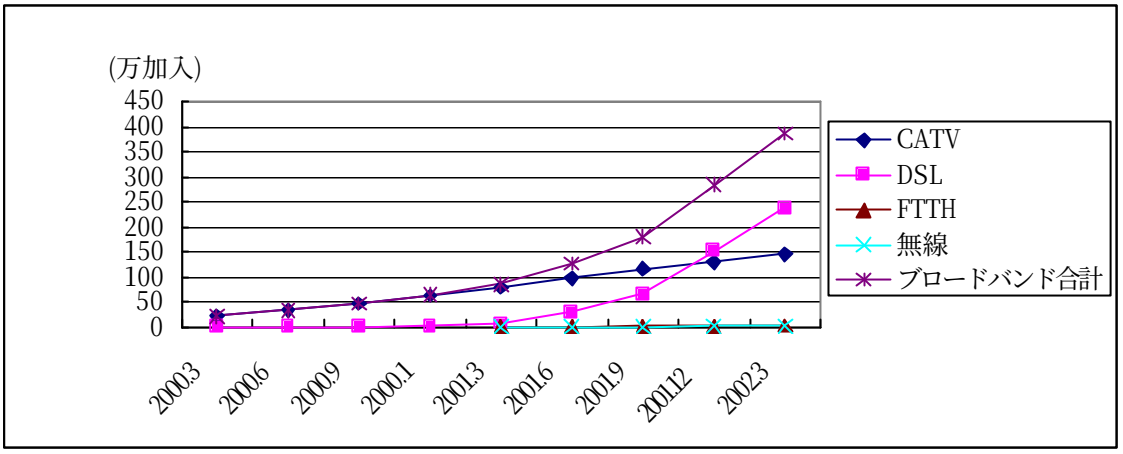
http://www.nua.com/surveys/how_many_online/world.html

b. ブロードバンドネットワークの普及

インターネット人口が急増している背景として、技術の進歩に伴うブロードバンドネットワーク化が進み、利便性が向上したことが挙げられる。日本においては、光ファイバー網への支援や競争促進によって環境が整備され、DSL(Digital Subscriber Line:**デジタル加入者線)やケーブルインターネットといった常時接続サービスの価格が低化したことから、インターネットが企業や家庭に急速に普及した。**

2001 年はまさしく「ブロードバンド元年」だったと言える。

ブロードバンド・アクセスの加入数の推移



(出典) 総務省「平成 14 年版情報通信白書」

http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h14/index.html

c. 接続端末の多様化

ブロードバンドネットワークの普及と並んでインターネット人口を急増させている要因の一つに、携帯電話や PDA といったインターネット接続端末の多様化が挙げられる。インターネット利用者における PC および携帯電話・PHS 端末利用者の数は、2000 年の 571 万人から 2001 年にはおよそ 4 倍の 2,364 万人に増加し、同年 3 月末には 3,456 万加入に達した。特に携帯電話は日本においては急速に普及しており、インターネット利用者も非常に多く、世界にも類を見ない。PC と携帯電話の双方でインターネットを利用している人は、全インターネット利用者の 32.9%を占める 1,548 万人と大幅に増加しており、場所と場面によって利用端末を使い分けているものと想定される。

携帯電話以外にも、インターネット利用が可能な新たなインターネット接続端末が普及しつつあり、代表的なものにゲーム機器がある。インターネットとゲームというとオンラインゲームを連想するが、ゲーム機器メーカーは、オンラインゲーム以外にも、映画や音楽の配信や出版物に添付した DVD との連携、インターネット放送など、あらゆるコンテンツの提供を企画している。ゲーム機器以外にも、インターネットに接続可能なワイヤレステレビや、外出先からインターネットを介して制御できるエアコン、インターネットを介して献立情報を取得する電子レンジなど、情報家電と言われる機器が挙げられる。インターネットはオープンで自由な接続が可能なため、このような特徴を活かした端末は、今後ますます多様化することが予想される。これらの端末はインターネットに常時接続されていることで活用できる

ため、常時接続型のアクセス環境の普及と情報家電端末が広く応用される可能性は密接に関連している。

d. インターネット利用ユーザ層

インターネット接続端末の多様化に伴い、利用ユーザ層にも変化が生じている。PC は近年低廉化しているとは言え依然高価なものであるため、未成年者などは購入が難しいが、携帯電話は PC と比較して非常に廉価であり、未成年者にも手が届きやすい。携帯電話を利用したインターネットコンテンツビジネスも活発になっており、インターネット利用のきっかけになっていることも考えられる。数年前までは、学校や職場での利用が大半を占めていたインターネットも、接続サービスの変化や端末の多様化に伴い、利用ユーザ層が変化しており、もはや老若男女を問わなくなった。

上述したさまざまな要因のもとで、日本のインターネット環境は急速に変化を遂げている。それにともない、インターネットビジネスも多様化しつつある。本書では、インターネットビジネスを「通信経路としてインターネットを介し、物品やサービス、情報などの財の対価を支払う電子商取引」と定義し、その安全性と信頼性に関して調査を行う。

取引主体を基準にインターネットビジネスを分類すると、インターネットビジネスは、企業間における原材料取引を行う電子商取引である BtoB(Business to Business)と、企業対個人において PC・家電製品等や日用品といった最終消費財や、有料ネットワークコンテンツなどのサービスの取引を行う電子商取引である BtoC(Business to Customer)に大別される。これら二つの中に、企業対政府機関の取引である BtoG(Business to Government)や個人間の取引である CtoC(Customer to Cusomer)が含まれる。

(2) BtoB

BtoB は、行政機関や企業がインターネットを介して物品、サービス、情報などの財の対価を企業に支払う企業間電子商取引全般を指す。企業間の取引という性質上、取引規模が大きいものが多く、電子商取引市場の大半は BtoB が占めている。文具などのオフィス用品やパソコン、書籍などの物品販売から、航空チケットの手配やホテルの予約などのサービス、部品や原料などの調達、人材仲介など、BtoB に含まれる分野は多岐にわたる。最近では、特定の業界に取引市場を提供するバーティカルポータルと呼ばれる Web サイトや、インターネットを通じてビジネス用のアプリケーションソフ

トのレンタルを行う ASP(アプリケーションサービスプロバイダ)といった事業者が注目を集めている。BtoB は、取引形態から、電子調達・販売、e マーケットプレイス、BtoG に大別される。

a. 電子調達・販売

電子調達・販売は、インターネットを使って調達や販売を行うことで、それまで主流だった EDI(Electronic Data Interchange)に代わり、受発注や見積もり、商品の販売を行うものである。EDI は、従来電話や FAX などを媒体に行われてきた企業間の取引業務を、円滑かつ迅速に行うことを目的とし、商取引に関する情報を標準的な書式に統一して電子的に交換する仕組みである。受発注や見積もり、決済、出入荷などに関わるデータを、あらかじめ定められた形式にしたがって電子化し、専用線や VAN などのネットワークを通じて送受信する。EDI は、専用 OS の使用などによって機密性に富んでいるが、業界ごとのデータ形式やネットワーク接続形態の差異があるため汎用性に乏しく、他の業界の企業との取引を EDI 化するのは困難であった。

インターネットの普及によって、通信経路としてインターネットが活用できるようになり、比較的低コストで利用できることや地理的な制限がないことをを背景として、取引相手の幅も広がった。販売側においても営業担当者の人件費や店舗などにかけるコストの削減、管理の効率化を図ることができ、オフィス用品やパソコンなど、比較的標準化しやすい商品を扱う産業で広がっている。電子調達・販売では、XML などによって、業界や買い手ごとのデータの伝送方式に違いを無くし、作業の効率化を図っている。

b. e マーケットプレイス

e マーケットプレイスは、売り手と買い手ともに複数の企業が利用する、インターネットを利用したオープンな電子商取引の共通プラットホームシステムである。一般に、電子調達・販売が特定の企業間で行われているのに対して、e マーケットプレイスは、インターネット技術を応用することで自由度の高い電子商取引を行えるようにしたものである。e マーケットプレイスを活用することで、企業は市場の動向に合わせて、必要なときに必要な数量の部品を調達したり、製品によって販売先を柔軟に広げたりすることが可能になる。また、売り手と買い手が直接取引を行うことで、競争が働き柔軟なやり取りが行われる上に、これまで中間に位置していた流通業者を介さずに取引を行うため、流通コストの削減が可能となる。

e マーケットプレイスの実現で、売り手にとっては新規取引先の開拓や営業コストの削減、取引先の増加による在庫リスクの平準化、在庫調整などが実現でき、買い手にとっては調達コストや物流コストの削減、スポットでの取引による緊急時の調

達手段の確保などが実現できる。

c. BtoG

BtoG は、行政機関が物品、サービス、情報などの財の対価を企業に支払う電子商取引を指す。日本では政府の IT 戦略本部が 2001 年 1 月に e-Japan 戦略を打ち出している。これは、超高速のインターネットインフラの普及と規制改革によるインターネットビジネスの拡大を図るとともに、それを推進する人材育成と生活者に利便性をもたらす電子政府を実現し、米国をしのぐ世界最高水準の IT 国家に生まれ変わろうという戦略である。この戦略のもとで、政府組織も電子化され、政府関連事業の調達などがインターネットを活用して行われるため、BtoG 市場はこの数年間活発になるものと考えられる。

(3) BtoC

BtoC とは、インターネットを利用して、企業が消費者向けに取引およびビジネスを行うことである。BtoC は、インターネット上に店舗を構えて消費者に商品を販売するオンラインショップと、ソフトウェアや画像、音楽などのコンテンツの販売、オンラインゲームやオンライントレードやオンラインバンキング、e ラーニングといったサービスを提供するコンテンツビジネスとに大別される。

a. オンラインショップ

オンラインショップは、インターネット上で消費者を対象に物品を販売する店舗である。インターネットを利用することで、企業にとっては、24 時間営業が可能で便利であること、商品を保管・陳列するスペースが必要ないこと、商品の検索や比較が容易であることといったメリットがあり、また消費者にとっても店舗まで出向かずに在宅にて物品を購入できるメリットがある。オンラインショッピングで取り扱われる商品も、本や音楽などのエンタテインメント、衣料、アクセサリー、趣味や雑貨、家具、旅行の手配など、個人の日常生活に深く依存しており、家庭へのインターネットの普及に伴い、より急速な発展が見込める分野である。

オンラインショップには、自社で仕入れた商品を販売する「小売型」と、商品の在庫を持たずに注文だけを伝える「仲介型」とがある。また、企業形態も店舗を持たずインターネット上だけで営業する無店舗型企業と、店舗やカタログ販売の小売事業からインターネットに進出したクリックアンドモルタル企業に分類される。クリックアンドモルタルは、現実の店舗や流通機構をインターネットと組み合わせる手法であり、受注をインターネット上で行い、商品受け渡しと支払いを現実店舗で行う方式や、インターネットでの在庫検索サービスなどの例が挙げられる。クリッ

クアンドモルタル型の店舗は、現実に店舗を構えている企業がインターネットに参入するという形の店舗が多い。米国のインターネットビジネス売上の上位 50 位以内に入っているオンライン専用企業は 8 社と少なく、インターネットビジネス市場をリードしているのは、クリックアンドモルタル企業であるとされている。

b. コンテンツビジネス

コンテンツビジネスの分野では、音楽や映像などを CD やビデオ・DVD といった物品ではなくデータのまま販売するサービスや、オンラインゲームなどがある。現在は、コンテンツ自体の販売ではなく、コンテンツの提供は無料で行い、Web サイトや電子メール等に広告を表示することで、広告主から収入を得るインターネット広告事業が大半を占める。

PC などの固定端末だけでなく、モバイル端末を対象にインターネット経由でコンテンツの配信を行う形の電子商取引であるモバイルコマースも急増している。代表的なサービスでは、携帯電話の着信メロディや待ち受け画面などが挙げられる。また、旅行やエンタテインメントなどもモバイルコマースにおける成長分野であり、今後、固定端末向けだけでなくモバイル端末向けにおいても各種サービスが拡大することで、BtoC 全体の発展に寄与するものと考えられる。

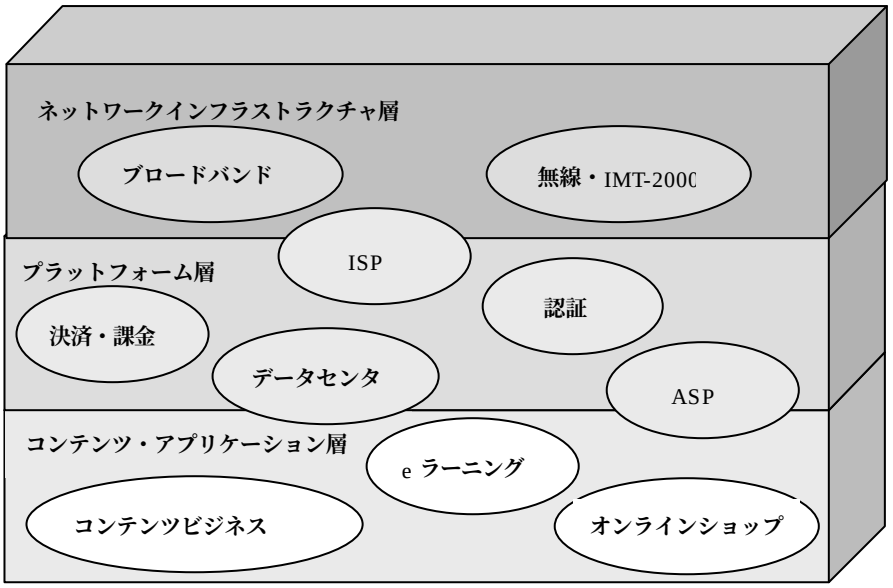
2. インターネットビジネスの構造に関する調査

本節では、インターネットビジネスの構築に関与する企業間構造や産業構造に関して調査を行い、その実態を明らかにする。

(1) 企業間構造

前節で BtoB、BtoC のインターネットビジネスの枠組みと形態について記述したが、インターネットビジネスにおいては、さまざまな取引主体のもとで多種多様なサービスが展開されていることがわかる。企業などの事業者がインターネットを介してビジネスを提供するためには、通信事業者やインターネットへのアクセスポイントを提供する ISP など、様々な仕組みを利用する必要がある。ここでは、インターネットビジネスを構築する構造に注目し、インターネットビジネスを支えるサービスに着目する。インターネットビジネスを構築する構造は、ネットワークインフラストラクチャ層、プラットフォーム層、コンテンツ・アプリケーション層の 3 つに分類することができる。

インターネットビジネスを構築する構造



a. ネットワークインフラストラクチャ層

インターネットの通信基盤を提供するネットワークインフラストラクチャ層のビジネスは、DSL、CATV、FTTH などのブロードバンドサービスの普及や、無線 LAN や IMT-2000 といったモバイルサービスの展開など、急速に発展している。

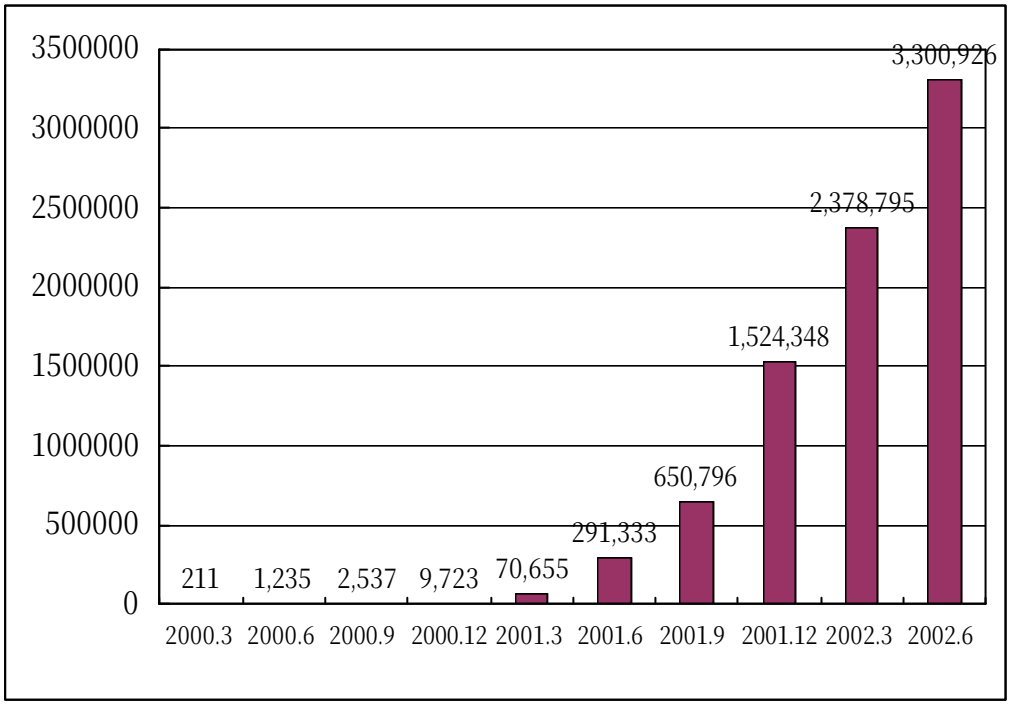
2001 年に発表された「e-Japan 戦略」は、日本が 5 年以内に世界最先端の IT 国家となることを目的としている。この戦略の具体的な行動計画である「e-Japan 重点計画」においては、5 年以内に少なくとも 3,000 万世帯が高速インターネットアクセス網に、また 1,000 万世帯が超高速インターネットアクセス網に常時接続可能な環境を整備することを目標としている。また、過疎地域などにおいては、採算性が取れないという問題が障害となり、民間事業者による光ファイバー網の整備などが進んでいない現状があるが、それに伴う情報格差を是正することも同様に目標に掲げられている。

a-1. DSL(Digital Subscriber Line)

DSL は電話線を使用して高速なデジタルデータ通信をする技術である。既存の電話線を流用できるため設備投資が必要なく、光ファイバーが普及するまでの代替サービスという位置付けで登場した。NTT 東日本と NTT 西日本では 2000 年末に ADSL サービスの本格提供を開始し、国内で当時 17 万 9,000 人だった利用者中の約 9 万 6,000 人を獲得していたが、2001 年 8 月にソフトバンクと関連会社のヤ

フーが NTT 東西の半額に近い料金で ADSL サービス「Yahoo!BB」を開始し、日本の ADSL ブームを加速させた。その後、NTT 東西も ADSL サービスの値下げを断行、他企業の ADSL サービスも増え、価格競争を通じて 2000 年末から爆発的に普及しつづけている。登場時は、1.5Mbps が主流だったが、2001 年には 8Mbps のサービスが登場、2002 年 10 月には 12Mbps のサービスが実現し、提供される予定である。ADSL は、ノイズに弱く、NTT の収容局からの距離が大きい場合にサービスのレベルが低下することや、使用できないことなどの問題がある。

DSL サービスの利用者数



(出典) 総務省「DSL 普及状況公開ページ」

http://www.soumu.go.jp/joho_tsusin/whatsnew/dsl/index.html

a-2. FTTH (Fiber To The Home)

FTTH は、光ファイバーを家庭などのユーザ環境に直接引き込み、超高速の通信環境を提供するもので、「ブロードバンドにおける大本命」とまで称されるサービスである。2001 年 3 月に有線ブロードネットワークスからサービスが提供開始されており、同年 6 月末時点で 3,383 件の契約数を獲得している。また NTT 東日本・西日本においても、2001 年 8 月に光ファイバーを利用した、最大速度 100Mbps の「B フレッツ」サービスを開始しており、2002 年 4 月には 11,600 件の契約を獲得している。

また、ISP 各社も FTTH に対応したサービスメニューを準備しており、光ファ

イバーを利用したインターネット接続サービスの動きも活発化してきている。だが、現時点では提供エリアが狭いことや、申し込みから開通までに時間がかかることが影響し、幅広い普及には至っていない。また、分譲マンションなどの集合住宅では、バックボーンから光ファイバーを引き込む際に大規模な工事が必要になるため、導入が難しく、普及にはまだ時間を要するものと考えられる。

a-3. CATV

2000 年末から沸騰した DSL に先駆けて大衆的なブロードバンドの提供を行っていたのが、CATV である。CATV 網を利用したインターネット接続サービスは、2002 年 3 月末現在 146 万加入となり、2002 年 5 月末の段階で 156 万人が加入している。2001 年と比較して、普及率は約 2 倍となっているが、ADSL 普及の波に押されている。米国と異なり、CATV が元来それほど普及していなかった日本においては、ADSL の台頭によって CATV の普及率は鈍化してきたものと考えられる。

a-4. 無線 LAN

有線ケーブルを使わず、電波や光などの無線で通信を行う無線ネットワークは、2000 年に無線 LAN の規格である IEEE802.11b に対応した製品が各社から発売されたこともあり、普及が進んでいる。有線ケーブルの敷設が必要なく、オフィスでの配置換えなどの際もケーブルを再敷設する必要がないため、手間を省けるほか、ケーブルが敷設しにくい学校や家庭内においても需要が高まっている。

NTT 東日本は、2002 年 6 月から無線によるインターネット接続サービス「M フレッツ」の試験提供を開始した。半年間は試験運用となるが、無線 LAN が普及することで、光ファイバーの集合住宅への引き込み問題も解決されるため、企業や家庭に高速なネットワークが導入されることになる。現在の技術・製品では暗号化のセキュリティレベルが弱いことや、公衆の帯域を使用しているため医療器具や電子レンジなどによって混信してしまうという課題がある。

a-5. IMT-2000

IMT-2000 は、International Mobile Telecommunications - 2000 の略であり、次世代移動通信方式の規格である。アナログ方式、デジタル方式に次ぐ、第 3 世代の携帯電話といわれている。IMT-2000 の特徴としては、送受信できるデータ量の大容量化と規格の統一がある。データ量は従来と桁違いに大きくなり、最大で、静止時 2Mbps、歩行時 384kbps、自動車などの高速移動時 144kbps の通信が可能となる。通信速度の高速化によって、音声の明瞭化や携帯テレビ電話の実現、音楽データなどのダウンロードや購入など、携帯電話を利用したサービスが多様化

される。また携帯電話の方式の世界統一が進むことによって、日本の携帯電話を外国でそのまま使用することが可能になる。現在は、ドコモグループ、J-フォングループが日欧方式の W-CDMA(DS-CDMA)を、KDDI(au)が北米方式の cdma2000(MC-CDMA)を採用している。

ネットワークインフラストラクチャはインターネットビジネスの基盤であり、上述したようなサービスや技術が発展することで、インターネット環境における利便性が大きく向上する。送受信可能なデータ量が拡大することで、従来のテキストや静止画像だけでなく、音声や画像データをリアルタイムに送受信できるようになるため、インターネット環境で提供されるサービスにも大きく影響する。ネットワークインフラストラクチャ層のビジネスは、コンテンツ・アプリケーション層、プラットフォーム層のビジネス展開に大きな影響を与え、インフラの発展によって、他層のビジネスは恩恵を受けるものと考えられる。

b. プラットフォーム層

プラットフォーム層のビジネスは、ネットワークインフラストラクチャ層とコンテンツ・アプリケーション層との間に位置し、ネットワークを有効に活用してコンテンツ・アプリケーションサービスを発展させるために必要となる。代表的なビジネスとしては、データストレージサービスや ASP(Application Service Provider)、インターネットデータセンタ、セキュリティ、認証、課金・決済システムなどが挙げられる。

この中で今後のインターネットビジネスの発展のための重要な要素となるのが、企業がサービスを提供するためのアプリケーションの肩代わりを行う ASP、安全で安定したサービスを提供するために欠かせないデータセンタ、そしてセキュリティとその一端を担う認証ビジネスである。

b-1. ASP

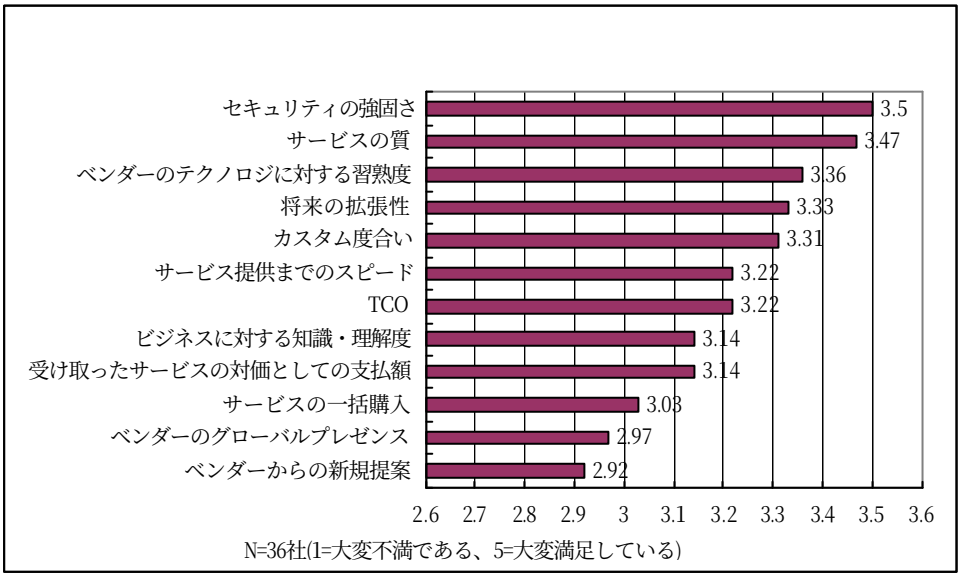
プラットフォーム層において、ASP はインターネットビジネスを行う企業にとって欠かせない存在になってくるものと考えられる。ASP はインターネットを介してパッケージソフトウェアなどのアプリケーションを提供するサービスであり、企業は自ら所有しなくても、そのアプリケーションを利用することができる。また ASP を利用することで、サービスを提供するためのアプリケーションの導入や運用、バージョンアップに対応するコストを削減できるほか、運用の失敗や設備投資などに関わるリスクを回避できる。企業においては、アウトソーシングの一環として利用されていることが多い。

日本においては 2000 年初頭から ASP 事業者が急増し、新しいアプリケーショ

ン提供モデルとして一躍ブームとなった。しかし、当時は高速ネットワーク回線の不足といったインフラストラクチャの整備が十分でなく、また、収益力のあるビジネスモデルを確立できなかったことから、市場は当初期待されていたほどには成長しなかった。ASP に対する過剰な期待は 2001 年には落ち着き、こぞって ASP 事業に参入した企業は苦戦を強いられた。

IDC Japan の 2002 年の調査によると、ASP サービスを利用している企業は、ASP サービスにおけるセキュリティの強固さを高く評価しているという結果が出ている。サービスの質、ベンダのテクノロジに対する習熟度、将来の拡張性なども高く評価されている。ただ、受け取ったサービスの対価としての支払額、TCO(Total Cost of Ownership：管理コストを含む経費の総計)などにあまり満足していない企業も多く、期待通りのコスト削減は達成できていない、という結果になっている。

ASP サービス利用後の評価



(出典) IDC Japan

http://www.idcjapan.co.jp/Press/Current/20020214Apr.html

平成 14 年版情報通信白書の調査では、2001 年度における ASP 市場規模は 60.3 億円と推計され、内訳を見ると、2001 年度は大企業が 56.5 億円で市場シェアの 9 割以上を占めており、残りが中小企業の 3.8 億円となっている。ASP 市場は 5 年間で約 18 倍に成長し、2006 年度には 1,076.5 億円になると予測されているが、そのなかでも 2004 年度頃から中小企業においても市場が成立し、2006 年度には大

企業が 699 億円でシェアが 6 割強、中小企業が 377.5 億円と 3 割強になり、中小企業のシェアが増加するものと予測されている。

また、ガートナージャパンが発表した日本市場規模予測では、2001 年の ASP の日本市場規模は 377 億円であり、2006 年には 2,525 億円に達する見込みとしている。これら 2 つの調査結果には大きな差があるが、これは ASP の定義の違いによって調査対象となるサービスに差が生じ、結果に現れたものと考えられる。

b-2. インターネットデータセンタ

インターネットの普及によって、ビジネスにおけるインターネットの重要度は急激に増大している。トラフィックの増大など、インターネットを取り巻く環境は急速に変化を遂げており、ASP が成長した理由と同様、自前でシステムを新規構築し、アップグレードや増設といった運用を行うことが時間とコストの面から困難になってきている。そのような企業を対象として、サーバの貸し出しや運用代行を行うインターネットデータセンタ業者が台頭してきた。データセンタは、セキュリティを備えた物理的に堅牢なサーバルーム、サーバの安定的な保守・運用、広帯域バックボーン回線を用いた安全で高速なインターネット接続環境、の 3 つを提供するサービスである。データセンタを利用することで、企業は迅速にサービスを開始し、回線やサーバを拡張することが可能となるため、データセンタは今後インターネットビジネスにおけるインフラ拠点になっていくものとして注目されている。

ビジネスにおけるインターネットの役割や活用方法が変化してきたことに伴い、日本におけるデータセンタ事業者のサービスも出現当初から変化しつつある。ハウジングやホスティングなどの汎用的なサービスを提供する事業者と、それらの機能に加え、開発、管理・監視といった付加価値サービスを顧客ごとにカスタマイズして提供する事業者の 2 つのグループに分類される。

2001 年度におけるデータセンタ市場は、1,371.4 億円と推計され、2006 年度には、4,317.2 億円と、約 3 倍に増加すると予想されている。付加価値のあるサービスを提供する事業者が、より成長するものと考えられている。

b-3. 課金・決済

インターネットビジネスは急速に拡大し、決済方法も多岐にわたっている。振込、代引き、コンビニ決済といった既存の決済手段に加え、クレジットカード、プリペイド、電子マネー、ネットバンキングといった、様々な決済手段が登場している。2000 年以降、こうした決済サービスを提供する事業者が急増し、競争を行っているが、日本は欧米と異なりクレジットカードや小切手といった文化が浸

透しきっていないため、現金による決済がもっとも信頼性が高いと考えられており、振込みや代引き、コンビニ決済など、既存の方法で決済する傾向が根強い。クレジットカードを所有していない人がいることも原因のひとつである。

その中で、コンビニ決済は以前と比較して多用されるようになっており、その背景として、コンビニ自身が公共料金の収納といった代金回収代行業に本腰を入れただけでなく、消費者側に対する利便性が高いため、利用する企業が増加したことがある。地理的制限のないオンラインショッピングのメリットを生かすためには、決済の仕組みも全国規模である必要がある。そこで銀行や郵便局よりも気軽で、24 時間営業で利便性の高いコンビニの代金回収業務が多用されるようになったと言える。

課金・決済市場は 2000 年には 97 億円であり、そのうちの 25.7%の 25 億円がインターネットを利用したオンライン決済であった。2006 年には全体で 1,155 億円にまで市場が拡大するものと予測されており､そのうちのオンライン決済も 45.7%を占める 528 億円まで成長するとされている。

b-4. 電子認証

インターネットビジネスや行政手続のオンライン化など、インターネットを利用した情報の流通が急速に増加しつつある。オープンで匿名性の高いネットワークを利用するインターネットビジネスにおいて、取引相手を特定するためには認証は欠かせないものである。そのため、相手の信頼性の確保や情報漏洩の保護を目的として、従来の手書きの署名や押印に相当する仕組みが求められており、電子認証市場規模が拡大している。

現在、電子認証基盤において主流となっている技術が PKI(Public Key Infrastructure)である。PKI では公開鍵暗号方式を用い、公開鍵と秘密鍵のいずれかを使用して文書を暗号化し、暗号化した鍵に対応する他方の鍵を使用して復号する仕組みを用いて情報の漏洩を回避する。公開鍵を使用して暗号化したデータは、秘密鍵の所有者だけが復号できるため、誰からでも秘密鍵の所有者に安全に電子データを送ることができる。反対に自分の秘密鍵で電子データを暗号化して送信すれば、自分が配布した公開鍵を所有している人は誰でも復号して電子データの内容を確認することができ、そのデータを作成した人が秘密鍵の所有者であることが確認できる。このような特徴を利用して、電子署名を作成し本人の認証を行うのが電子認証である。

また、電子署名を行った秘密鍵の所有者が信頼しうる取引相手であることを証明するために、認証機関によって発行される電子証明書がある。認証機関は、こ

れらの電子署名・電子認証の利用にあたって、秘密鍵を所有する者の本人確認を厳格に行い、電子署名に用いる秘密鍵に対応する公開鍵を証明する電子証明書を発行することにより、秘密鍵の所有者を証明する。

今後の認証ビジネスの中心は、PKI のインフラストラクチャをいかに安全に運用できるか、また、PKI アプリケーションをいかに容易に構築するかにかかってくるものと考えられる。今後、電子政府の実現やインターネットビジネスの拡大などに伴って、電子署名・認証業務などのビジネスは必要不可欠となる。平成 14 年版情報通信白書によると、2001 年度の電子認証ビジネス市場規模は約 63.4 億円と推計され、今後も順調に拡大し、2006 年度には約 419.5 億円になるものと予測される。インターネットビジネスの先進である米国と比較して日本の市場は小さいものだが、この成長の結果、2001 年度は約 8.5 倍の差があった米国市場と日本市場の規模は、2006 年度には約 4.5 倍にまで縮小するとされている。

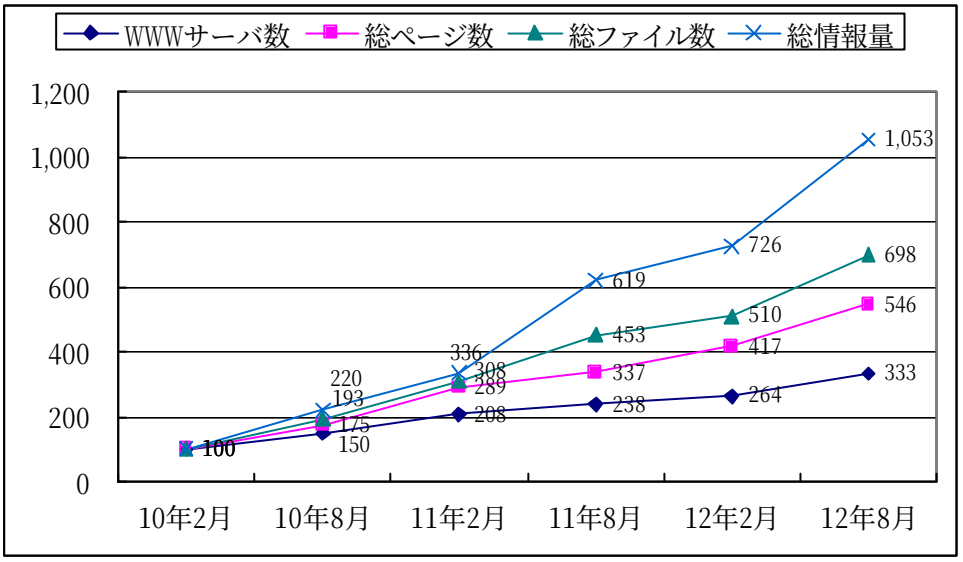
c. コンテンツ・アプリケーション層

コンテンツ・アプリケーション層のビジネスには、物品の購入を行うオンラインショップを始め、音楽や映像のストリーミング配信やチャットなどのコミュニケーション、オンライン出版やオンラインゲームなどが挙げられる。近年の DSL の爆発的な普及で、日本においても画像や音楽のストリーミング配信が盛んに行われている。ビジネスにおいてだけではなく、一般の Web ページにおいてもグラフィックが多用されており、以前のようにダイヤルアップが主流な環境では想定できなかった状況になっている。

総務省郵政研究所が 2000 年度より実施している「WWW コンテンツ統計調査」によると、日本の JP ドメインにおけるインターネットコンテンツの総データ量は、1998 年から 2001 年の 3 年間で 6.7 倍になっており、急激に増加している。これらのコンテンツをファイル数で比較すると、HTML ファイルと画像ファイルが圧倒的に多く、動画ファイルと音声ファイルの総ファイル数に占める構成比は全体の 0.1～0.2%となっている。だが、1998 年からの 3 年間における動画ファイルや音声ファイルの増加率は、HTML ファイルや画像ファイルの増加率を上回って大きく伸びている。今後、ブロードバンドの普及進展に伴い、これらの高度なコンテンツの利用が進み、インターネットが広く活用されることが期待される。

我が国(JP ドメイン)の WWW コンテンツ量の推移(平成 10 年 2 月を 100 とする)

	10年2月	10年8月	11年2月	11年8月	12年2月	12年8月
WWW サーバ数 (万台)	3.6	5.4	7.5	8.5	9.5	12
総ページ数 (万ページ)	1,020	1,790	2,950	3,850	4,250	5,570
総ファイル数 (万ファイル)	1,890	3,650	5,820	8,570	9,630	13,200
総情報量 (G バイト)	305	670	1,024	1,889	2,214	3,212



「第 1～6 回 WWW コンテンツ統計調査」(郵政省(現総務省) 郵政研究所)より作成
http://www.soumu.go.jp/hakusyo/tsushin/h13/html/D1117000.htm

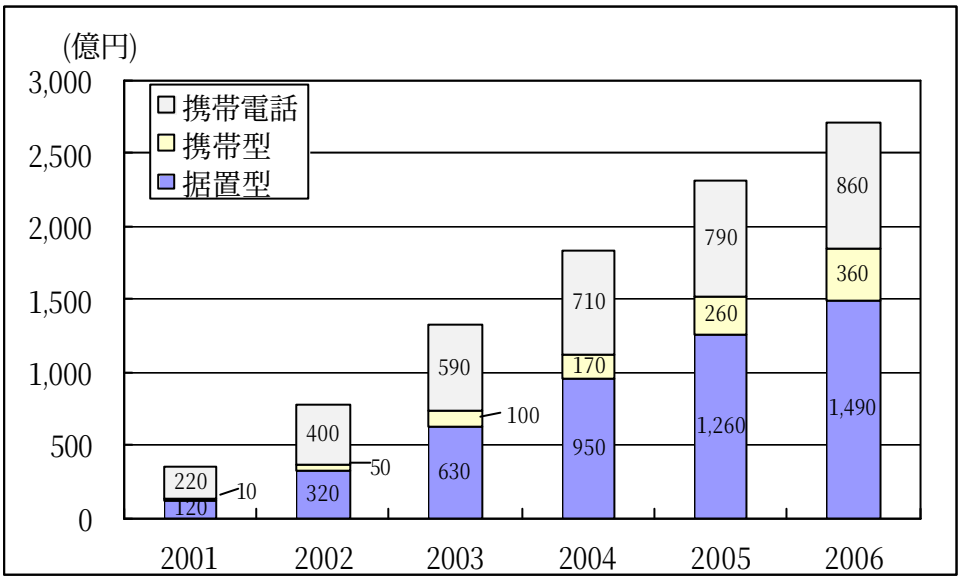
c-1. コンテンツビジネス

現在主流のコンテンツビジネスは、映像や音楽などのコンテンツ配信とオンラインゲームである。

コンテンツ配信については、ブロードバンドネットワークの普及により、ストリーミング技術を用いて、映画や音楽の配信、スポーツライブ中継などの配信を有料で行うサービスが普及しつつある。インターネットによる音楽配信については、Napster や Gnutella などのシステムを利用し、不正にコピーした楽曲を MP3 で圧縮して個人間でやり取りを行う環境が拡大していたこともあり、デジタルコンテンツは無料だという意識が消費者の間に根強くある。また、デジタルコンテンツはコピーが容易なため著作権問題が発生し、大きな市場を形成するまでには至っていない。そのため、音楽の配信ビジネスが軌道に乗るには課題が多い。今後の幅広い普及のためには、コピー防止等の課題を解決し、音楽業界が本格的に参入して競争を行っていくことが望まれる。

世界のオンラインゲーム利用者は 5,000 万人に達すると言われている。日本においては、米国や韓国ほどオンラインゲームの利用は一般的ではないが、2001 年以降、主な家庭用ゲーム機がネットワーク接続への対応を発表しており、ブロードバンドの普及とともに今後オンラインゲームも普及していき、2006 年にはオンラインゲーム市場は 2,710 億円にまで達すると予測されている。また、日本は携帯電話が他国と比較して広く普及しており、携帯電話によるインターネットでのゲームコンテンツ利用が人気を集めている。

オンラインゲーム市場予測



(出典) 野村総合研究所

http://www.nri.co.jp/report/itnavi2006/pdf/itnavi2006_10.pdf

c-2. e ラーニング

e ラーニングは Web ベースのシステムを中心的に使って行う教育・学習システムであり、自習型の教育システムとして広く普及している。コンピュータシステムを使って、教育や学習を行うシステムを CBT(Computer Based Training)というが、その中でも特に Web ベースのシステムを使うものを WBT(Web Based Training)という。従来のコンピュータ教育システムでは、サーバやクライアントに特別なプログラムを使用しており、利用できる環境やシステムが限られていたが、WBT では、ユーザは Web ブラウザでインターネットに接続できる環境を、サーバ側も Web サービスを提供するためのシステムを用意するだけでよい。インターネットのメリットである時間や場所に制約されずに、自由に教育を受けるこ

とができる。また、コストの削減やスケーラビリティの向上を容易に行うことができる。

(2) 産業構造

インターネットビジネスの発展は、従来の産業構造に依存しない取引形態を生みだしている。インターネットのメリットを生かすことで、流通チャネルや情報収集力によって保護されてきた既存の産業構造の重要性が薄くなり、参入障壁が低下したことから、新規参入が容易になり、結果として産業構造が改革されつつある。各産業におけるインターネットビジネスの動向をまとめた。

産業構造	
第一次産業	農業、林業、狩猟業、漁業、水産養殖業
第二次産業	鉱業、建設業、製造業
第三次産業	卸売業、小売業、金融・保険業、不動産業、運輸・通信業、電気・ガス・水道・熱供給業、サービス業、公務

総務省は、平成 13 年事業所・企業統計調査の概数集計として、会社企業の電子商取引導入状況を発表している。企業産業大分類別では、「金融・保険業」が 13.7%と最も高く、次いで「卸売・小売業、飲食店」の 12.8%、「サービス業」の 11.9%となっている。

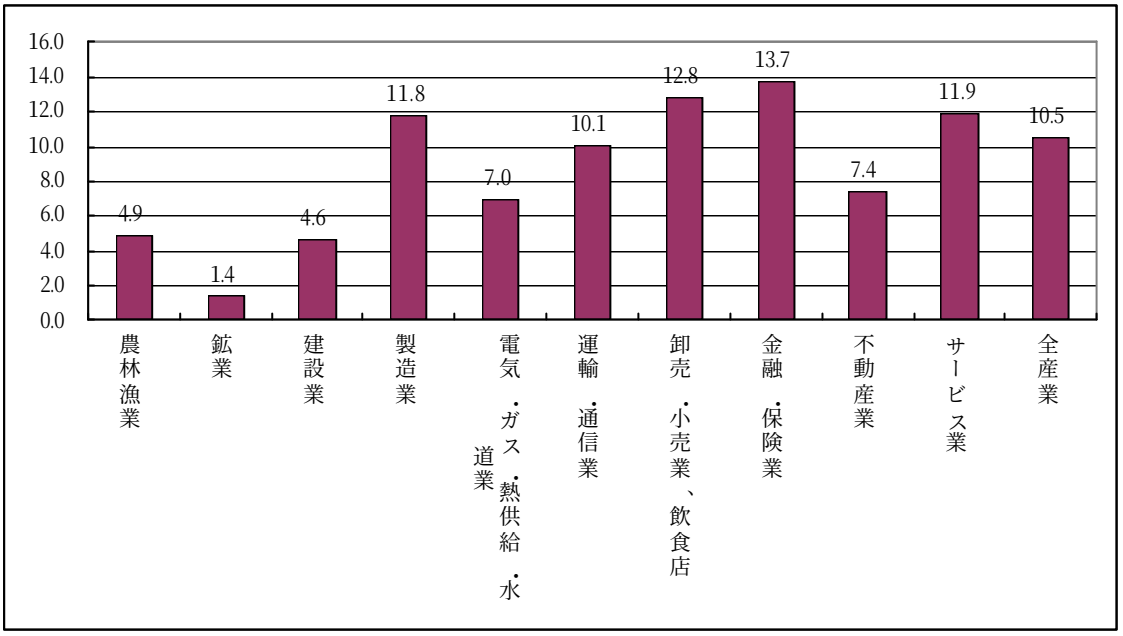
産業大分類別電子商取引の状況別企業数

産業大分類別	企業総数	電子商取引を行っている企業	電子商取引を行っていない企業数
農林漁業	9,784	475	9,309
鉱業	2,139	31	2,108
建設業	298,587	13,874	284,713
製造業	296,470	35,072	261,398
電気･ガス･熱供給･水道業	545	38	507
運輸･通信業	56,403	5,697	50,706
卸売･小売業、飲食店	566,824	72,565	494,259
金融･保険業	16,875	2,314	14,561
不動産業	95,852	7,070	88,782
サービス業	269,161	32,095	237,066
総　数	1,617,250	169,826	1,447,424

(出典) 総務省「平成 13 年事業所・企業統計調査概数集計による電子商取引の状況」

http://www.pref.hokkaido.jp/skikaku/sk-kctki/deta/tokusu/h13gi/jig.htm

産業大分類別電子商取引の導入率



(出典) 総務省「平成 13 年事業所・企業統計調査概数集計による電子商取引の状況」
http://www.pref.hokkaido.jp/skikaku/sk-kctki/deta/tokusu/h13gi/jig.htm

a. 第一次産業

a-1. 農業

農業において、最も活発にインターネットが利用されている分野は生花取引といわれている。生花は市場ごとに商品の集まりが著しく異なり価格差が激しいため、インターネットを活用することで流通の合理化を図ることができ、多くのインターネット市場が手がけられている。大田花きの「花きインターネット取引システム」では、せり前取引の受発注をインターネット上で行っている。大田花きは、産地から送られてくる出荷予定情報をもとに、場内仲卸などへ情報公開・受発注を行う。会員の小売店は、Web ページから仲卸を通じて情報を閲覧し、発注を行うというものである。

生花以外の農産物においても、インターネットビジネスを取り入れる動きが広がっている。「あぐりぷらっと」は、農産物の生産者及び加工業者と小売業者の間において、農産品の直接取引を行う e マーケットプレイスである。生産者と小売業者双方が情報共有を図ることで信頼関係を築き、消費者へ安定した商品提供を行うことを目的としている。生産者は「あぐりぷらっと」上で農産品の種類、数量、出荷計画などを画像と共に提示し、小売業者は Web サイトを通じて応答、返答、確認などを行い、取引が成立した場合、生産者から小売業者へ農産品が直送

される。小売業者は、生産者が登録した情報をそのまま店舗に掲載することで、顔が見える農作物を消費者に提供でき、生産者側は、小売業者のニーズにあわせた出荷計画を策定することで安定した取引を行うことができる。農業分野では、ショッピングモールを活用し、農家から消費者に直接農作物を販売する BtoC も活発である。無農薬栽培のため値が張るものを流通過程で買い叩かれずに消費者に提供したいという農家と、高価なものでも良いものであれば購入したいという消費者の要望を満たすシステムである。

a-2. 水産業

水産業においては、e マーケットプレイスが 2001 年に相次いで登場している。「フィッシュオンライン」は 2001 年 6 月に登場した e マーケットプレイスであり、原材料を仕入れる加工メーカーや問屋、量販店、レストランや居酒屋などの外食産業、ホテル、旅館、民宿、ペンション、惣菜、弁当・仕出し、給食業者、小売商など、企業や個人事業主に対して売買を行う。2001 年 3 月に稼動を開始した「スイサンドンヤドットコム」も、全国の飲食店やホテル、ペンション、旅館などをターゲットに、業者のためのインターネット水産問屋として開設された、会員制の BtoB サイトである。他に、2001 年 7 月に登場した e マーケットプレイス「アイフィッシュ」も同様のサービスを展開している。また、水産業においても、農業と同様、ショッピングモールを活用した BtoC が行われている。

b. 第二次産業

b-1. 建築業

建設業界におけるインターネットビジネスの動向は、以前は大手建設会社による資材調達が主流であったが、建設資材の e マーケットプレイスへと推移しつつある。

「CMNet」は、コストパフォーマンスを重視し、インターネットを利用することで良いものを安く提供する仕組みを作るべく発足し、登録会員数は 2002 年 7 月現在で 1,193 社である。発注者となる建築主と、CM(コンストラクションマネジメント)会社(発注者の代理として発注者の立場から設計・工事全般の見直し、請負者との交渉、監督を行い、発注者の希望に沿った家を完成させる会社)、設計事務所、積算事務所、施工者やサプライヤー、ビルメンテナンスといった建設に関わる多分野のスペシャリストらが共同で建設を行い、個々の企業で蓄積され研鑽された専門的技術やノウハウを活かすことで、品質の良い建築を安く実現しようという構想である。これらの参加企業に対しては、第三者機関の格付審査情報を照会する機能があり、発注者は信頼できるパートナーを幅広く選択することができる。2000 年 9 月に発足した「とりりおんコミュニティ」は、全国の地方地場ゼネ

コンが結束して、事業の共同化、ニュービジネスへの共同取組、各社のベストプラクティスの融合等を図っている。発足当時の参加企業は 25 社だったが、2002 年 6 月には 42 社に成長した。また、他産業、同業異業種と積極的にアライアンス化を図りながら、事業の推進にあたっている。他にも「コンストラクション・イーシー・ドットコム」など、e マーケットプレイスが多く存在している。

b-2. 自動車業

米国では、自動車メーカーがインターネットを用いて消費者に直接自動車を販売するサイトが活発である。Ford Motor や GM はインターネット上で、車種の選択や車体の色、内装やその他のオプションをつけ、最終的に消費者の自宅付近のディーラーと価格交渉や納車予約まで行うことができる。GM は日本においても、資本提携先の企業と同様のサービスを行っており、将来的には BTO(Buy To Order)の実施も検討している。

日本においては、2001 年 2 月にマツダがネット上で消費者向けの BTO サービス「Web Tune Factory」を開始した。BTO はパソコンの分野で既に定着しているが、日本の自動車業界ではマツダが初の試みである。ボディーカラーなど仕様の選択から電子メールによる見積り、商談の申し込みまでを Web 上で行い、商談から契約、登録、納車手続きは販売店を通して行う。販売店向けに商談の簡略化を提供するオンライン見積りサービスと捉えることができる。マツダは BTO を導入することで、商品の販売だけでなく消費者のニーズを捕らえることも目的としている。

c. 第三次産業

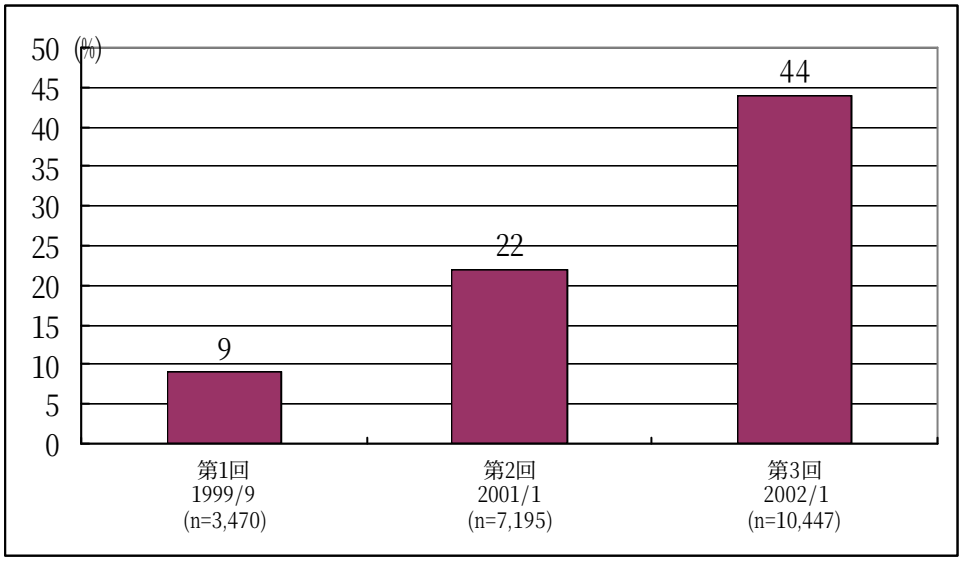
c-1. 金融業

金融業界においては、インターネットバンキングとインターネット証券取引が代表的なインターネットビジネスである。

インターネットバンキングでは、預金の残高照会や入出金照会、口座振り込み、振替といった ATM で対応しているサービスが銀行の Web ページから利用可能なほか、複数口座の一括管理や電子メールによる相談の受付など、独自のサービスを展開している銀行もある。また、コストのかかる店舗を現実世界に持たずに営業を行うオンライン専用銀行も登場している。日本では 2000 年後半にジャパンネット銀行が登場し、次いで IY バンク銀行、ソニー銀行、イーバンク銀行が登場した。これらの銀行は、ネットオークションやネットトレーディングなどと決済の連携サービスを行うことで口座数を伸ばしている。インターネットでは銀行取引が夜中の 23～24 時に集中しており、インターネットを介してリアルタイムに残高

や取引明細の照会や全件照会ができ、深夜でも決済が反映されるところが既存の銀行との大きな差となる。マイボイスコムが、2002 年 1 月に 10,447 人を対象に調査したところによると、日本のインターネットバンキング経験者は、全体の 44%にのぼり、2001 年 1 月の調査結果と比較して倍増している。また、インターネットバンキングを使用する理由としては、「手数料が安い」が 74%でもっとも多く、続いて「信頼できる」が 50%、「セキュリティ対策が充実」の 45%と続いており、今後も発展が見込めるものと考えられる。

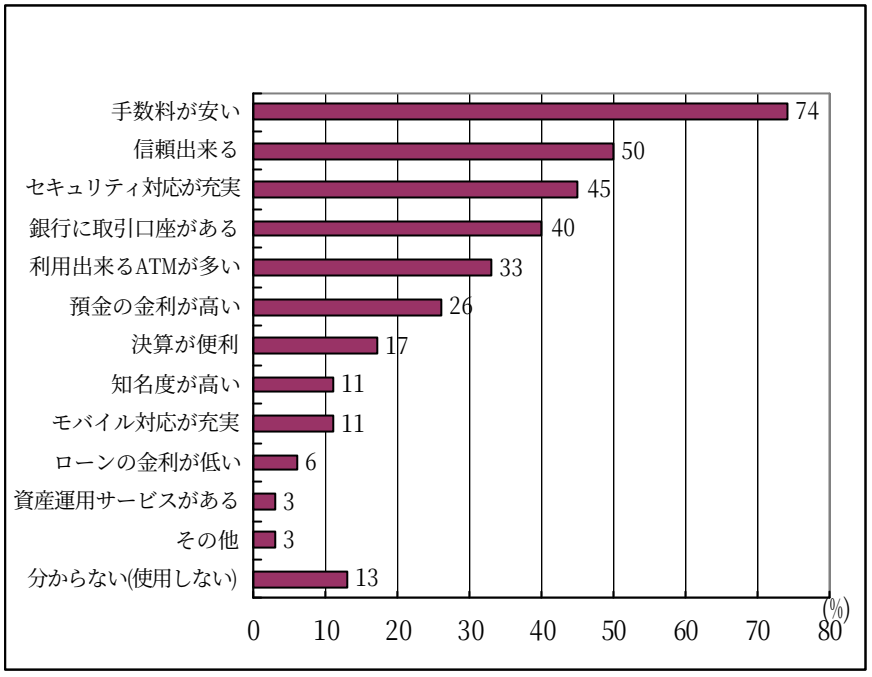
インターネットバンキングの利用状況



(出典)マイボイスコム「インターネットバンキングの利用(第３回)」

http://www.myvoice.co.jp/voice/enquete/4204/index.html

インターネットバンキングの銀行選択時の重視点



(出典)マイボイスコム「インターネットバンキングの利用(第３回)」

http://www.myvoice.co.jp/voice/enquete/4204/index.html

日本におけるインターネット証券取引は 1997 **年** 4 **月から開始されており、**1999 **年** 1 **月には** 19 **社、**2000 **年** 8 **月には** 60 **社程度の証券会社がインターネット証券取引サービスを提供している。インターネット証券取引サービスでは、利用者がインターネット上で市場の動向を確認し、即時に売買注文が出せるというメリットがあり、急速に普及した。インターネット取引を中心的に行っている証券会社の中には、すでに全口座数の** 20%**がインターネット取引口座であるというところもある。**

電通が 2001 **年に行った「金融ビッグバン」に関する意識や行動についての生活者調査によると、インターネットバンキングを利用している人は、全体の** 3%**であり、利用したいと考えている人は** 33%**であった。一方、インターネット証券取引に関しては、すでに利用している人は全体の** 2%**であり、利用したいと考えている人は** 27%**であった。証券会社利用者に限定してみると、インターネット証券取引を利用している人は** 13%**にのぼり、インターネットを通じて証券取引を行う人の割合は、銀行取引よりはるかに多いことが判明した。**

*c-2. **不動産業***

不動産業界においては、インターネットを利用した土地やマンション、一戸建

ての販売や賃貸物件の仲介が数年前から行われている。利用者は場所や価格、敷地面積などの項目から好みのものを検索し、実際の契約は不動産の店舗にて紙面上で行われるため、利用者にとってのメリットは、不動産店舗まで行かずに物件を探すことができる、というものである。

株式会社大京は、2002 年 3 月末までの 1 年間でインターネットをきっかけとして同社が販売したマンションの戸数が前年度比 20%増の 2,056 戸、金額では同 23%増の 766 億 4,344 万円という大幅増を達成したと発表した。大京のホームページへのアクセス件数は 59 万 1,322 件(前年実績 57 万 9,204 件)であり、そのうち資料請求件数は 2 万 8,854 件(同 2 万 6,425 件)であった。大京の年間売上等から推計すると現状既に約 2 割程度がインターネットをきっかけとした販売からの契約となっており、これらの結果から、インターネットが販売における重要な役割を担っていることが分かる。

不動産業界では、中小企業やベンチャー企業も参入し、BtoC だけでない特徴的なサービスを提供している。エフバイネットが運営するサイト「CtoC 不動産」では、CtoC(Customer to Customer)、つまり個人間での住居売買を扱っている。仲介業者を挟まずに売り手と買い手が直接取引を行うことで、数十万から数百万に及ぶ仲介手数料を節約することが可能となる。このような新規ビジネスが発展し普及すれば、従来の不動産取引に大きな影響を与え、高価で手が出せないマイホーム購入も進むことも考えられる。

c-3. 運輸業

航空業界では、航空会社が代理店を介さずに、直接消費者に航空券を販売するビジネスが活発だ。このようなシステムは米国で最も普及しており、市場規模は年間約 1,000 億ドルにのぼる。通常、一般の航空会社は自社航空券しか取り扱わないが、複数企業の航空券を取り扱うサイトも登場し、競争が増している。日本においても、インターネットを通じて航空券を購入した場合に割引を適用する「e 割」を 2000 年に開始した JAL などが、積極的に航空券のオンライン販売を進めている。2001 年には ANA、JAL、JAS の国内大手 3 社が出資し、「国内線ドットコム」をスタートした。国内航空会社 11 社の空席状況を一度に確認することができ、複数の航空会社の航空券も同時に購入できる。また、航空券の購入をクレジットカードで行い、航空券は搭乗時に空港の自動チェックイン機もしくはカウンターで受け取るサービスを実施しており、利便性が高い。

電車業界、バス業界においてもインターネットによる座席予約と乗車券の販売

が普及している。コンビニエンスストアでの専用端末での乗車券購入も可能であり、利用者に対する利便性が格段に向上している。バス業界においては、運行状況を確認できるサービスも登場している。国土交通省の九州地方整備局が運営している「九州 IT's(いつ)バス」は、福岡-大分間を走行する高速バスを対象に、高速バスの運行状況を利用者へ通知するサービスを提供している。利用者は PC や携帯電話を使用して、バスの到着時刻や空席状況などを確認できる。これらは GPS をバスに搭載する方法で実現されている。

運送業界では、トラックがいまどこを走っており配送先までどのくらい時間がかかるのかといったインターネットを利用した運行管理が進んでいる。バスの運行状況確認と同様、個々のトラックに GPS のアンテナを取り付けることで、GPS からの情報をインターネットで収集し、車両の位置や所要時間などを把握することができる。運送会社の Web ページ上で問合せ伝票番号を入れることで、利用者からも宅急便の配達状況を確認することもでき、サービスの質が向上していると言える。

c-4. 通信業

通信業においては、音声通話に IP(Internet Protocol)を用いた電話サービスである IP 電話が近年注目を浴びている。IP 電話はもともとは 1996 年頃から登場していたが、音質が悪かったことや、通話できる相手が限定されるといった条件があり、当時は大きな普及には至らなかった。矢野経済研究所の調査によると、日本国内におけるインターネット電話、IP 電話個人ユーザは 2001 年末で 158 万回線、2005 年末には 651 万回線になる、と予測されている。ADSL や CATV インターネットなどによるブロードバンド常時接続環境の普及や認知度の向上したこと、2002 年 9 月から行われる IP 電話に番号が割り当てられ公衆電話網からの発信が可能になることなどが普及を後押ししており、各 ISP も IP 電話サービスへの対応を始めている。

IP 電話の課題は、信頼性が低いこと、通信の混雑に弱いこと、使い勝手が悪いことが挙げられる。現状、IP 電話には、場所を特定する手がかりが無く、緊急通報（119 番や 110 番）に対しては著しく信頼性が低くなる。また、現状の IP ネットワークと同様、IP 電話は、ネットワークトラフィック増加時に通信の信頼性を保つための余計な通信が発生してしまい、その結果、正常な通信ができなくなってしまう。2002 年のワールドカップ開催の際には、ソフトバンクが展開する IP 電話サービス「BB フォン」は、FIFA ワールドカップチケットの電話受付の時間帯、公衆電話網に通話を迂回させる措置を取っていた。使い勝手の面では、現在、

展開されているIP電話サービスの大半は、パソコンを起動してマイクを装着する方式を取っており、一般電話との操作性の違いがある。今後のIP電話の発展のためには、質の向上と、使い勝手の向上が課題となる。

c-5. 電気・ガス・水道・熱供給業

エネルギー業界では、インフラストラクチャとしてのインターネット化が進んでいる。米国では1998年3月にカリフォルニア州が、全米に先駆けて電力小売の完全自由化に踏み切った。これによって需要家は自由に電力供給事業者を選択し、直接電気を購入することができるようになり、1999年3月のデータでは、需要家のうち約13万件、契約口数全体の1.3%、需要全体の13.5%が、電気の購入先を既存の電力会社から新規参入者に変更した。米Forrester Researchによると、米国における天然ガスおよび電力のオンライン取引は2000年には300億ドルに達しており、2004年には2,660億ドルに拡大する見込みだ。

日本においては、東北電力が、2000年10月に電気工事組合・電気工事店・電材店等を対象に、インターネット環境を活用することによりコストや時間を効率化するための「Web型インターネットEDIサービス」を開始しており、将来的にはeマーケットプレイスも視野に入れている。また、2002年4月には業界初のインターネットEDIを活用した競争入札による燃料調達システムを運用開始している。電力会社はインフラストラクチャ事業にも注力しており、東京電力は2002年から保有している光ファイバー網をプロバイダ向けに提供するサービスを開始している。

すべての産業において、インターネットビジネスが行われており、今後も時代の流れに沿い、発展していくものと考えられる。取引がすべてオンラインで行われることで時間の短縮が見込まれ、仲介業者を介さないことで価格の低廉化が実現する。物品の運搬作業自体は短縮化しないが、運輸業界においてもインターネットを用いた制御が行われている。今後の産業形態はインターネットビジネスの発展によって、急速に変化していくものと考えられる。

第 3 章　インターネットビジネスの市場動向に関する調査

1. 日本のインターネットビジネスの市場動向に関する調査

本項では、日本におけるインターネットビジネスについて、過去から現在までの市場動向と今後の予測を調査し、その位置付けを明らかにする。

(1) 日本におけるインターネットビジネス動向

a. インターネットビジネスの歴史

日本では 1995 年に電子メールが企業に浸透し始め、ビジネスにおいて柔軟なコミュニケーションが可能になりつつあった。インターネットでのオンラインショッピングも、この頃普及し始めた。Web ページを使用し、膨大な種類の商品やサービスを収録したカラフルなオンラインカタログが表示できるようになって以降、オンラインショッピングによる販売活動が急増し、中小企業でも容易に開始できることで人気が上昇した。集客効果向上のためにオンラインショップが集まったショッピングモールが主流となった。当初、日本ではオンラインショッピングはなじみが薄かったが、カタログによる通信販売が一般に受け入れられていることもあり、媒体がインターネットになっただけのオンラインショッピングは、インターネットの普及加速に伴い、急激に発展すると見込まれていた。同時に、広告宣伝・広報の分野においても Web ページ上での宣伝活動が活発になり、インターネット広告がビジネスとして確立した。また、それまで、紙媒体や電話で行っていた顧客サポートにもインターネットが活用されるようになった。1998 年には、インターネットオークションサイトが、日本でも開始された。

資金の移動や債権債務の清算といった業務の重要性から、全て専用線を用いた通信が行われていた金融業界においても、1994 年 9 月に米国サンフランシスコの Bank of America がインターネットを利用したサービスを開始、1995 年には、インターネットバンキングサービスを開始し、1995 年後半には、現実世界に店舗を持たないオンライン専用銀行も出現した。日本では 1997 年にようやく住友銀行がサービスを開始し、翌 1998 年には多くの銀行でインターネットバンキングが開始された。

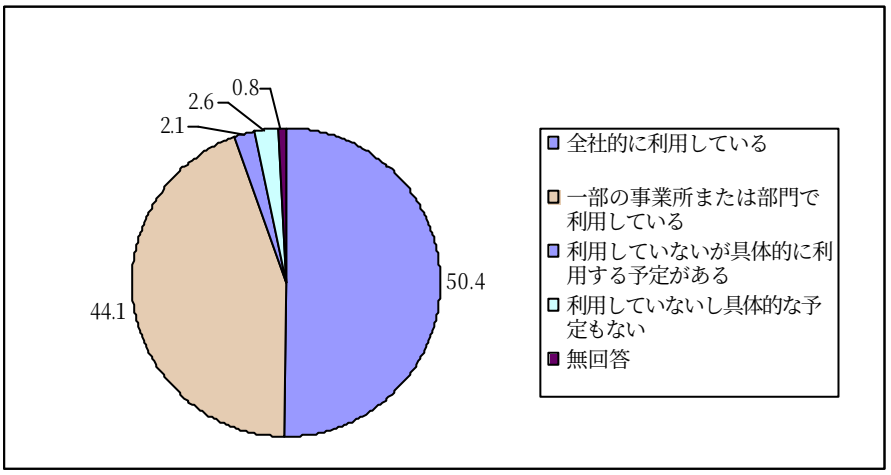
このような急速なインターネットの普及に伴い、インターネット関連企業の株への投資が進み、株価の急上昇を呼んだ。企業はこぞってインターネットビジネスに進出し、空前の「ドットコムブーム」となった。だが、インターネットが手段でなく目的となってしまっていたこのブームは数年のちに終焉を迎え、「ネットバブル」と名称を変えた。ブームの間に乱立したインターネットビジネスサイトは淘汰され、着実なビジネスモデルを持ったサイトが存続しているのが現状である。

b. 企業におけるインターネット利用動向

総務省が 2001 年 10 月におこなった調査によると、インターネットを利用している企業は 94.5%となり、企業におけるインターネット利用が一層進んでいることがわかる。近い将来、すべての企業において、インターネットが利用されることになると考えられる。内訳は「全社的に利用している」が 50.4%、「一部の事業所または部門で利用している」が 44.1%となっており、2 社に 1 社が全社的にインターネットを利用している。

産業別では建設業が最も利用率が高く 99.8%、最も低い利用率は運輸・通信業の 86.8%であり、2000 年の調査と比較して、産業による利用率格差はほぼ解消されつつあることがわかる。従業者規模でみると、従業者 300 人以上の大企業では普及率はすでに 95%を超えているが、300 人未満の企業でも普及が進み、その格差は急速に縮小しつつある。商工中金が 2001 年 8 月に行った調査によると、中小企業におけるインターネットの導入率は 82.1%であった。このことから、全企業がインターネットを利用する時代に突入したものと考えられる。

インターネットの利用状況



(出典) 総務省 「平成 13 年 通信利用動向調査報告書 企業編」

http://www.johotsusintokei.soumu.go.jp/public/data2/HR200100_002.pdf

c. ホームページ開設状況

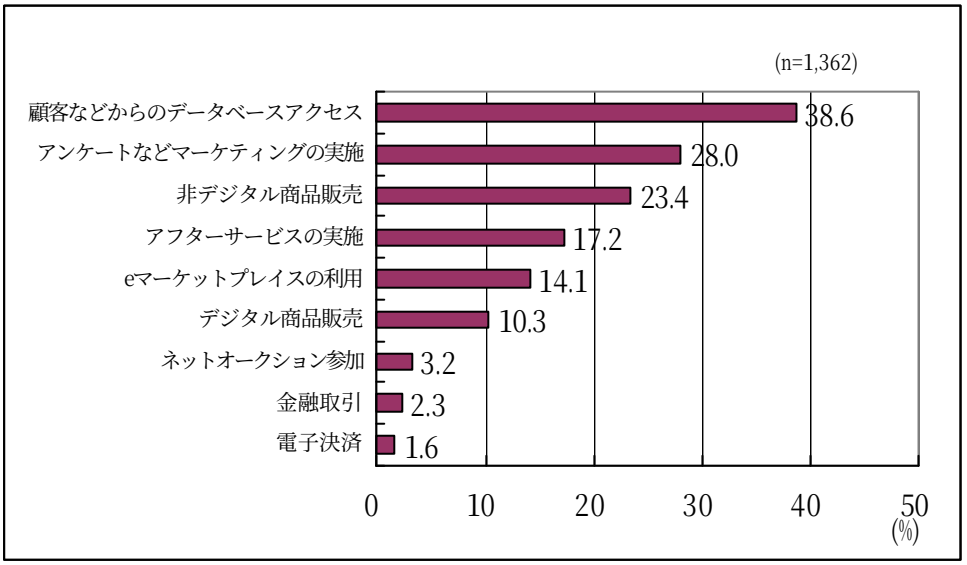
インターネット導入企業のうち、ホームページを開設している企業は 69.9%であった。ホームページ開設率に関しては、産業間でややばらつきがあり、卸売・小売業・飲食店、サービス業・その他で比較的高くなっている。中小企業においては、インターネット導入企業のホームページ開設率は 63.3%となっており、全体に対する半数程度に達していることが分かる。中小企業においてもインターネット、ホー

ムページの普及はかなり進んでいる。

開設したホームページを介した活動として、オンラインによる商品取引を行っている企業は、「デジタル様式でない商品の販売(受注を含む)」が 23.4%、「e マーケットプレイス(調達活動)の利用」が 14.1%、「デジタル様式の商品の販売(受注を含む)」が 10.3%となっており、1 割～2 割の企業において、自社ホームページを介して電子取引が行われている。また、「電子決済」を行っている企業は 1.6%、「金融取引」は 2.3%、「ネットオークション参加」は 3.2%となっており、まだ小数派である。

ホームページ開設企業のみを対象とすると、そのうちの 36.9%が販売あるいは調達などの電子商取引を行っている。その内訳は、調達及び販売ともに電子商取引を行う企業が 7.4%、調達のみを行う企業が 6.7%、販売のみを行う企業が 22.7%と、調達よりも販売で普及が進んでいる。産業別にみると、最も電子商取引が普及しているのは卸売・小売業・飲食店となっており、4 割(41.8%)の企業が実施している。

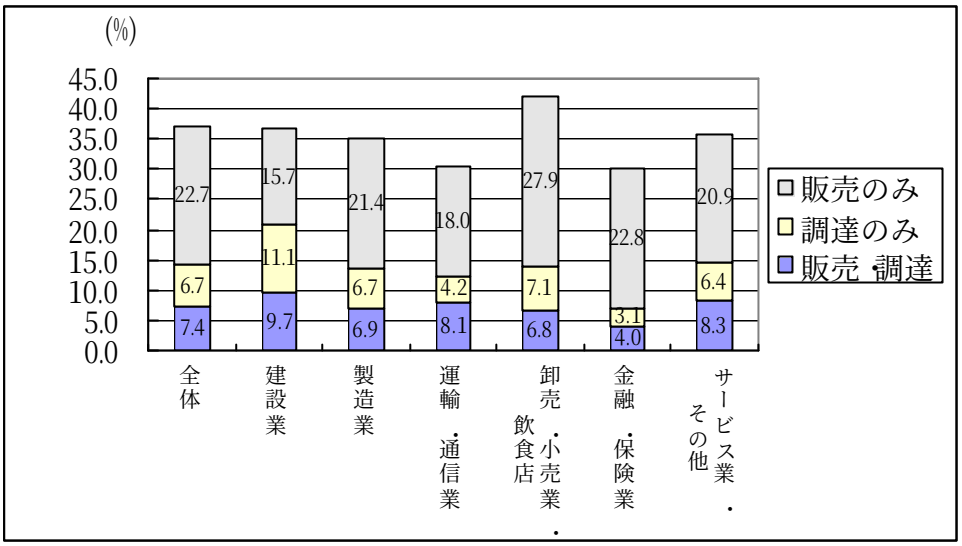
自社ホームページを介した活動



(出典) 総務省 「平成 13 年 通信利用動向調査報告書 企業編」

http://www.johotsusintokei.soumu.go.jp/public/data2/HR200100_002.pdf

電子商取引の実施率



(出典) 総務省 「平成 13 年 通信利用動向調査報告書 企業編」

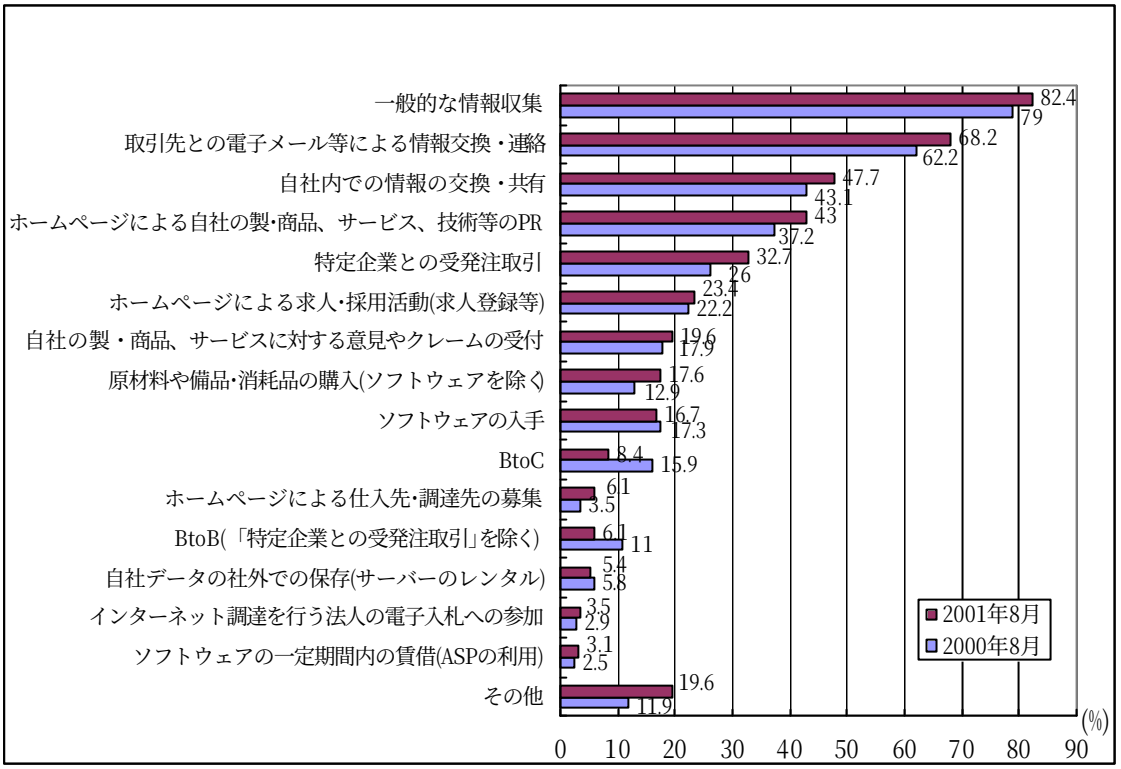
http://www.johotsusintokei.soumu.go.jp/public/data2/HR200100_002.pdf

d. 中小企業における動向

中小企業においては、インターネットビジネスを展開中の企業はホームページ開設企業の 37.5%となっており、2000 年には 40.1%であったことに比べて比率はやや低下している。インターネットの導入やホームページの開設に比べるとインターネットビジネスの普及ピッチは相対的に遅い。一方、インターネットビジネスの実施予定なしとしている企業は 27.5%であり、実施中や検討中の企業よりは比率が低いものの、2000 年の時点では 20.7%であったことと比較すると、取り組みに慎重な企業が増加していることがうかがえる。

また、インターネットの利用目的においても、インターネット導入済みの企業では BtoC、不特定企業向け BtoB が 2000 年に比べて減少しており、導入を検討中の企業でも激減している。ただ、情報収集や取引先との電子メール交換といった基本的な目的や特定企業との受発注、原材料等の購入では実施企業が増加しており、これらについては効果を認めている。

現在実施中のインターネットの利用目的



(出典) 商工中金

「中小企業のインターネットの利用等に関する調査 [2001 **年** 8 **月調査**]」

http://www.shokochukin.go.jp/pdf/cb2001jyoho.pdf

2001 年次の調査では、インターネットの利用に対して、経営の改善に有効だと考えている企業が増加している一方、インターネットビジネスの普及や拡大に対しては、自社に好影響を与えると考えている企業は減少しており、あまり影響はないと考えている企業が増加して、全体の半数を占めている。この結果から、技術の進歩や時代の変化に沿いホームページ開設率は増加しているが、企業のインターネットビジネスに対する過大な期待は沈静化し、インターネットを活用する目的も、効果が確実に見込めるものに変化しつつある事がわかる。

e. 今後のインターネットビジネス動向

インターネットを支えるインフラストラクチャの発展や、プラットフォームとなるシステムやアプリケーションの発展によって、インターネットビジネスは今後も普及し、個人がインターネットビジネスに参加する機会はますます増加するものと考えられる。今後、個人を対象としたビジネスである BtoC **および** CtoC **は、急速に拡大していくだろう。また、現在、人気を呼んでいるインターネットオークション**

やファイル交換、チャットなどを含め、企業をまったく介さない個人間の取引も増加してくるものと考えられる。

さらに、携帯電話などモバイル機器も急速に発展し、携帯電話でのメールの送受信は、現在ほとんどの機種で基本機能として付属しており、画像の送信も可能となっている。画像も、静止画像だけでなく、業者や機種によっては数秒の動画まで送信可能である。今後、IMT-2000 のサービスが確立されれば、それに伴い、モバイル機器を対象としたビジネスがこれまで以上に発展するものと考えられる。

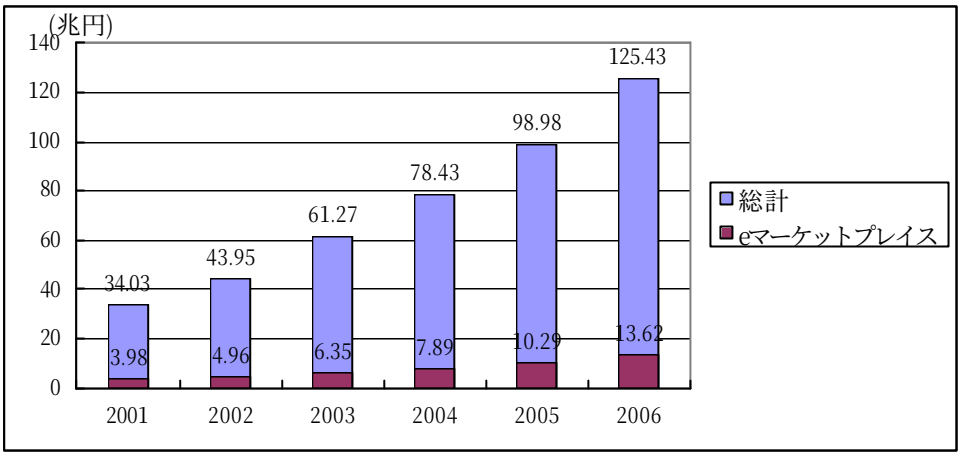
(2) BtoB 市場動向

a. 市場規模

平成 14 年版情報通信白書によると、日本における BtoB 市場の規模は、2001 年では 53.9 兆円となっており、2000 年と比較すると、41.5%の伸びを示している。1999 年から 2000 年の伸び率は 37.7%であり、順調に成長していることがうかがえる。このうち、e マーケットプレイス市場は、2000 年では 800 億円にすぎないが、2005 年には 16 兆円近くに成長すると予測されている。業種別の市場規模については、現状では電気業界・自動車業界が先行しているものの、2005 年には他の業界でも普及が進むと予測されている。

また、電子商取引推進協議会の調査では、2001 年の BtoB 市場規模は 34 兆円であり、そのうち、e マーケットプレイスの取引規模は約 4 兆円となっている。2006 年には、BtoB 市場規模は、125 兆円に達し、e マーケットプレイスもそのうちの約 14 兆円を占めるものと予測されている。

BtoB の市場規模及び電子商取引化率の推移



(出典) 経済産業省、電子商取引推進協議会、(株)ＮＴＴデータ経営研究所

http://www.ecom.or.jp/home/20020218_2_Press.pdf

日本における産業別 BtoB 市場規模 (100 万円)

	1999 年	2000 年	2001 年	2002 年	2003 年	2004 年
農林漁業 ･鉱業	16	114	591	1,454	2,718	5,132
建設業	75,203	115,923	214,713	598,701	903,641	1,766,024
製造業	1,746,753	4,254,163	10,094,438	17,646,664	24,475,371	32,484,011
電気 ･ガス ･熱供給 ･水道業、運輸 ･通信業	31,121	60,447	89,451	120,986	157,121	211,747
卸売 ･小売業	1,478,502	3,878,831	6,640,462	10,203,748	14,091,101	18,705,735
金融業、サービス業、不動産業	82,515	187,212	288,432	595,217	1,025,285	1,480,711
TOTAL	3,414,110	8,496,690	17,328,088	29,166,770	40,655,237	54,653,359

(出典) イーシーリサーチ

http://www.ec-r.co.jp/press_m/20010516.htm

b. 市場動向

米国のドットコムブームに遅れをとり、ブームの波に乗れないままネットバブルの終局を迎えた日本においては、ビジネスにおける手段としてのインターネット導入に不安を抱く傾向があったが、EDI のインターネット化であり元来ビジネスとして成立している分野の発展形態である BtoB に対してはネットバブルの余波はそれほど大きいものではなかった。今後の BtoB の発展を担うのは e-Japan 構想によって勢いを増す BtoG と e マーケットプレイスであると考えられるが、インターネットデータセンタサービスや ASP サービスが発展・展開していくことで、BtoB 市場全体がより活性化していくものと考えられる。

b-1. e ***マーケットプレイス***

BtoB は BtoC と異なり、新規ビジネスでない場合が多く、比較的順調に発展してきているが、e マーケットプレイスは乱立する傾向にあり、今後、淘汰の時代に入るものと考えられる。

産業別に専門特化した企業間電子商取引を支援する e マーケットプレイスサイトの運営を行っていたバーティカルネットが 2001 年末に解散した。解散の理由として、マーケットプレイスサイト運営事業には成長の可能性があるが、事業環境が激変し、また米国 VirticalNet 社が戦略転換したことなどで、日本国内における事業の展開が難しくなったことをあげている。

b-2. BtoG

日本においては、e-Japan 構想に伴い、この数年間で、政府系の事業がシステム化される予定である。現時点で、目に見える変化は多くはないが、2002 年度中には中央省庁における電子化に対する体制は整い、地方自治体においても電子化に向けた施策や実証実験などが行われることで、消費者も身近にその実現を感じ、恩恵を受けるものと考えられる。地方自治体においても業務の電子化が行われており、2002 年 4 月には岡山県が全国初の都道府県レベルでの電子入札を実行した。2005 年度までには各種の申請や届け出が電子化され、国民の広範にわたりそのサービスが受けられるように、計画および構築が現在進められている。

運用開始にあたって、大きな話題を呼んだ住民基本台帳ネットワーク(住基ネット)も e-Japan 構想の一部である。住基ネットは、住民基本台帳法の一部を改正して住民基本台帳を電子化し、中央省庁や全国の自治体から利用できるネットワークであり、この住基ネットの情報をもとに住民基本台帳カードといわれる IC カードが発行される。IC カードの発行によって、他のビジネスにも影響するものと考えられる。

電子商取引推進協議会の調査によると、e-Japan 戦略の実行に伴い、中央政府、地方自治体の電子入札・調達が 2003 年以降急拡大することが見込まれることで、BtoG 市場規模は、2006 年には 6 兆円を超える見通しとなっている。

(3) BtoC 市場動向

a. 市場規模

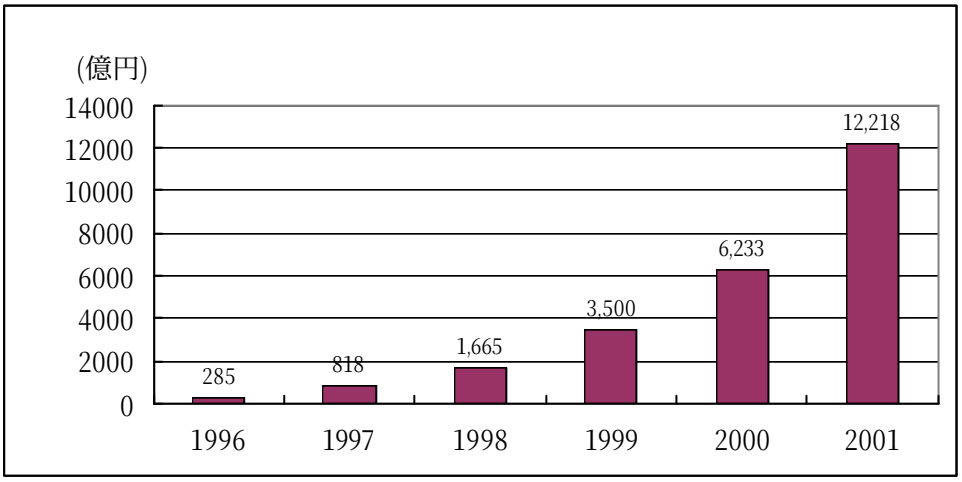
平成 14 年版情報通信白書によると、日本の BtoC 市場規模は、2000 年は 6,223 億円、2001 年は 1 兆 2,218 億円となっており、96.0%の増加となっている。BtoC は

着実に拡大を続けており、2005 年には 8 兆円近くまで拡大すると予測されている。

また、電子商取引推進協議会の調査によると、2001 年の BtoC 市場規模は 1 兆 4,840 億円となり、2000 年の 8,240 億円に対して約 80%拡大している。モバイルコマース市場規模に関しては、約 1,200 億円に拡大し、着信メロディなどのエンタテインメント系のコンテンツを中心に、2000 年に比べほぼ倍増した。旅行、エンタテインメント、衣料・アクセサリー、趣味・雑貨･家具、不動産等の品目が大きな伸びを見せ、電子商取引市場規模の拡大に寄与していることがうかがえる。2006 年の BtoC 市場規模は、約 16 兆円にまで達し、電子商取引化率も現在の 0.5%から 5%強にまで増加すると見込まれている。モバイル BtoC 市場規模に関しては、3 兆円を超えるものと予測されている。

いずれの結果からも、BtoC が厳しい経済情勢の中でも依然として順調な伸びを示していることが分かる。

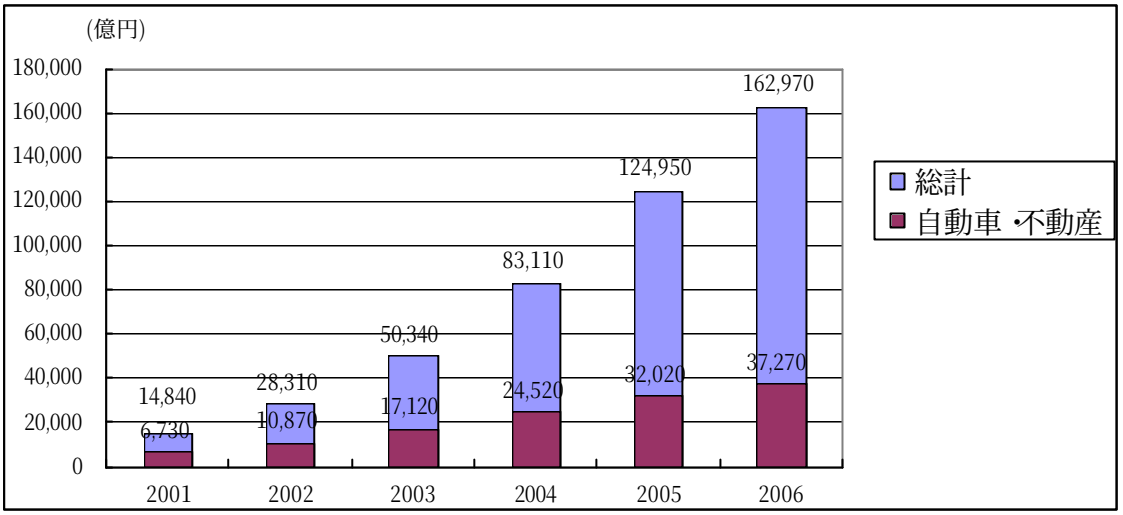
電子商取引(最終消費財)市場の推移



(出典) 平成 14 年版 情報通信白書

http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h14/index.html

BtoC の市場規模及び電子商取引化率の推移



(出典) 経済産業省、電子商取引推進協議会、(株)ＮＴＴデータ経営研究所

http://www.ecom.or.jp/home/20020218_2_Press.pdf

日本における産業別 BtoC 市場規模 (100 万円)

	1999 年	2000 年	2001 年	2002 年	2003 年	2004 年
農林漁業・鉱業	7	17	70	138	222	379
建設業	0	36	149	653	1,403	3,495
製造業	21,122	45,511	95,708	141,807	194,634	263,034
電気・ガス・熱供給・水道業、運輸・通信業	12,650	35,803	58,741	78,793	109,224	147,350
卸売・小売業	34,430	97,569	193,809	343,012	521,112	732,441
金融業、サービス業、不動産業	8,221	21,181	33,296	67,023	107,667	151,991
TOTAL	76,430	200,117	381,773	631,425	934,262	1,298,689

(出典) イーシーリサーチ

http://www.ec-r.co.jp/press_m/20010516.htm

日本における商品別 BtoC の市場規模 **(億円)**

	1999 年	2000 年	2001 年	-	2005 年	2006 年
PC および関連製品	510	910	1,480	-	5,560	5,670
旅行	230	610	1,190	-	20,590	23,770
エンタテインメント	30	590	1,090	-	9,800	11,240
書籍・音楽	70	200	340	-	4,950	5,360
衣類・アクセサリー	140	270	580	-	10,500	13,290
ギフト商品	15	40	70	-	1,400	1,590
食料品	170	330	560	-	8,370	11,830
趣味・雑貨・家具	100	220	490	-	6,950	10,630
自動車	860	2,020	3,470	-	20,020	23,110
不動産	880	1,760	3,260	-	11,850	14,160
その他物品販売	100	540	980	-	8,330	10,510
金融	170	440	630	-	5,290	6,140
各種サービス	85	310	700	-	19,390	25,670
合計	3,360	8,240	14,840	-	133,000	162,970

(出典) 平成 13 年度電子商取引に関する市場規模・実態調査

http://www.ecom.or.jp/home/20020218_2_Press.pdf

日本のオンラインショップは 2000 年には 2 万 7,000 店を超え、楽天市場に代表されるインターネット上のショッピングモールや、インターネットオークション、旅行、不動産、自動車等の仲介型も行われている。

日本における用途別のインターネット利用率の推移を見ると、オンラインショッピングやオークションの分野で利用率が伸びているのが分かる。

日本における用途別のインターネット利用率の推移

	2 年前	現在
電子メール	87.8	96.4
メールマガジン	40.4	76.3
情報収集 ･検索	42.1	70
ネットショッピング	14.4	52.2
ニュース閲覧	27.8	48.8
オークション	11	36.6
オンラインゲーム	8.3	21.4
各種チケット予約 ･購入	6	21.4
動画の受信 ･ダウンロード	6.2	26.1
画像 ･音楽等のダウンロード	12.1	33
インターネット電話	1.8	4.9
e ラーニング	0.9	3.6

(出典)「IT と国民生活に関する調査分析」

http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h14/summary/summary01.pdf

*b. **市場動向***

米国でのインターネットビジネスの成功を目の当たりにした日本のベンチャー企業は、数年遅れて 1997 年頃から一斉にインターネットビジネスへの取り組みを開始した。米国に倣い、次々に BtoC サイトが立ち上がり、日本においてもネットベンチャーブームが起こったが、米国のネットバブル崩壊に伴い、日本におけるインターネットビジネスへの取り組みも減速している。

ただ、現在でも多くの BtoC サイトがビジネスを続行しており、これらのサイトでは、きめ細かいサービスの提供によって他社との違いを強調し、ユーザの利便性を向上すると同時に買い物を楽しくするための工夫をこらしているサイトが多い。インターネット人口の増加によって、オンラインショッピングに参加する消費者は比例的に多くなると考えられる。そこでビジネスを成功させるためには、インターネットビジネス戦略を確立しておく必要がある。

2. インターネットビジネス市場における、日本と世界の比較

本項では、日本と世界のインターネットビジネスを比較し、世界における日本の位置付けを明らかにする。

(1) 世界のインターネットビジネス市場動向

1990 年代後半、世界中はドットコムブームに沸いた。ネットバブルは、1995 年に Netscape 社が上場したときに始まったといわれ、Sun Microsystems や Oracle、Cisco といった有名企業が上場し、1990 年代後半にはアメリカの経済成長の 3 割を支えていたという。ネットブームが株高を生み、市場で調達した資金で企業は IT に投資して生産性を高め、ハイテク企業も売上を伸ばすという好循環が続いていた。しかし、アメリカの家庭での PC の普及が 50%を越えたことなどから売れ行きが伸び悩み、2000 年にハイテク株が暴落し、それをきっかけにブームは終了した。ネットバブルの崩壊によって、アメリカの経済は後退し、多くの企業が株価の低迷や倒産に追い込まれ、インターネットビジネスから撤退した。

Webmergers.com によれば、2000 年から 2001 年にかけて、インターネット企業の閉鎖及び倒産件数が倍増している。2001 年には、少なくともインターネット企業 537 社が閉鎖または破産申請を行っており、2000 年の 225 件の 2 倍を上回り、累計では 762 社を記録している。

ドットコム企業の倒産数

	第 1 四半期	第 2 四半期	第 3 四半期	第 4 四半期	計
2000 年	5	31	52	135	223
2001 年	162	179	118	78	537

(出典) Webmergers.com
http://www.webmergers.com/editorial/article.php?id=49&PHPSESSID=93ed7779995d70d76f74a2ea51991831

倒産した企業を分別すると、e コマース系が 43%を占めて最も多く、コンテンツ系が 25%、次いでインフラ系、インターネットアクセス業者系という順になっている。

倒産企業のジャンルごとの分類

ジャンル	数	割合
インターネットアクセス	71	9%
コンテンツ	190	25%
E コマース	325	43%
インフラストラクチャ	130	17%
プロフェッショナルサービス	46	6%

(出典) Webmergers.com
http://www.webmergers.com/editorial/article.php?id=49&PHPSESSID=93ed7779995d70d76f74a2ea51991831

2000 年 3 月より淘汰は底入れ傾向に入り、11 月～12 月のネット関連企業の閉鎖・倒産件数は 2000 年 8 月以来最も少ない 21 件で、1999 年 12 月の 49 件と比べると半分以下の数字になった。さらに、2000 年第 4 四半期には 135 件であった倒産件数は、2001 年第 4 四半期には 78 件に減少している。

ドットコム倒産企業における対象顧客

	2000 年	割合	2001 年	割合
企業	49	22%	217	40%
消費者	165	73%	223	43%
一般	11	5%	86	17%
計	225		537	

(出典) Webmergers.com

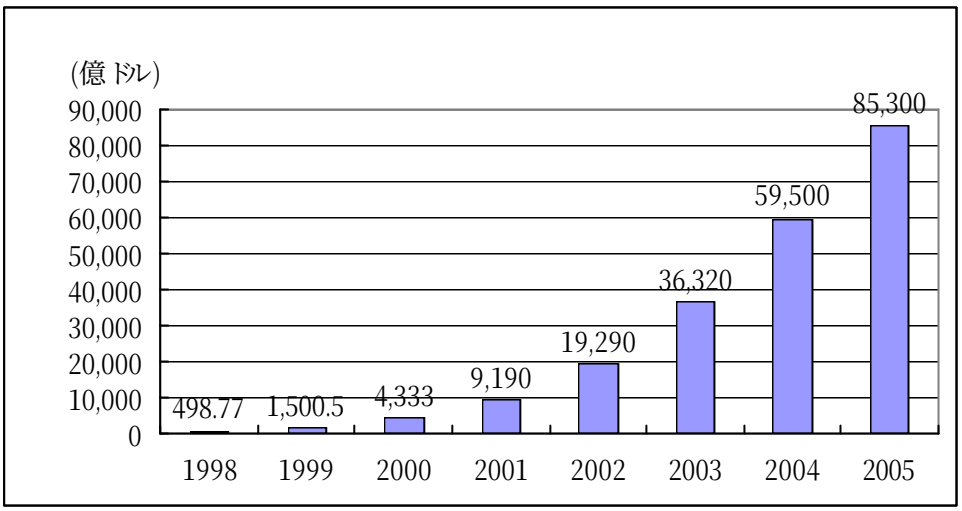
http://www.webmergers.com/editorial/article.php?id=49&PHPSESSID=93ed7779995d70d76f74a2ea51991831

ネットバブルが一転して IT 不況となったが、2001 年に IT 不況は底を打ち、2002 年においては徐々に復調の兆しがみえつつあるとの見方もある。

(2) BtoB 市場動向

昨今の IT 不況、経済の低迷などインターネットビジネスを取り巻く環境は決して順風ではないが、世界の BtoB 市場は急成長している。これは、BtoC が消費者を対象としたものであり、企業が新しい分野に着手したものだったのに対して、BtoB は既存の取引ルートを拡張するものであるため、時代の波にさほど左右されないという性質の違いによるものである。米 Gartner の調査によると、世界の BtoB 市場規模は 2000 年においては約 4,000 億ドルだったものが、2005 年には 8 兆 5,000 億ドルに達するといわれている。

世界の BtoB 市場規模



(出典) Gartner --- Worldwide BtoB Internet Commerce

http://www3.gartner.com/5_about/press_room/pr20010313a.html

地域別の BtoB 市場予測 (100 万ドル)

	2000 年	2001 年	2002 年	2003 年	2004 年
北米	159.2	316.3	563.9	964.3	1,600.8
アジア･太平洋	36.2	68.6	121.2	199.3	300.6
ヨーロッパ	26.2	52.4	132.7	334.1	797.3
ラテンアメリカ	2.9	7.9	17.4	33.6	58.4
アフリカ・中東	2.7	3.2	5.9	10.6	17.7
全世界	226.2	448.4	841.1	1,541.9	2,774.8

(出典) eMarketer --- The eCommerce: BtoB Report

http://www.emarketer.com/products/report.php?ecommerce_b2b

A.T.カーニー社が世界の主要企業 147 社を対象に行ったインターネットを使用した資材調達の実態調査の結果によると、対象企業の 96%が電子調達システムを導入し、インターネット上での資材の受発注や共同開発に取り組んでおり、そのうちの半数が「コスト削減に効果があった」と回答している。ただ、現状では、現行の調達システムとの整合性が取れていない、新システムの情報提供が不十分などの理由で、設定した目標を達成できない企業が半数を占め、現時点では思うように運用しきれていないことが分かる。

a. 米国

The Boston Consulting Group によると、米国における BtoB 市場は 2000 年の 1 兆 2,000 億ドルから 2004 年には 4 兆 8,000 億ドルにまで成長すると見込まれている。

その中でもやはりｅマーケットプレイスが伸びるものと考えられている。

アメリカの BtoB 市場動向

調査会社	2000 年	2001 年	2002 年	2003 年	2004 年
eMarketer	1,410.4	2,806.7	4,996	8,543.1	14,181.5
Yankee	7,400	11,800	16,700	22,100	27,800
Kenan	1,410	3,140	6,920	13,110	2,071
Forrester Research	4,490	7,990	13,102	20,434	30,045
International Data Corporation	1,008	1,880	3,380	6,070	8,374
Goldman	2,940	5,220	7,820	11,130	15,000

(出典) eMarketer 2001 年 6 月

米国において、ネットバブルの時代に乱立したｅマーケットプレイスだが、バブルの崩壊に伴い、多くのｅマーケットプレイスが閉鎖に追い込まれた。しかし、ｅマーケットプレイスの淘汰に伴い、新たなビジネスモデルや手法が生まれたため、米国の BtoB は一層の発展に向けての転換期を迎えていると言える。

b. アジア・太平洋

米 eMarketer の調査によるとアジア・太平洋地域では 2000 年には 362 億ドルであった市場は 2004 年には 3,000 億ドルに達すると予測されている。2000 年には世界の 16%のシェアを占めていたが、2004 年にはその他の地域の発展に伴い、世界に占めるシェアは 10.8%に下がるとしている。対して、Gartner の調査では、2005 年には世界の 28%のシェアをアジア・太平洋地域が占めると予測しており、アジアの成長が見込まれている。

韓国においては、電子商取引市場の 80%以上を BtoB が占めている。韓国統計庁の電子商取引企業統計調査によると、2000 年の韓国の電子商取引販売規模は 23 兆 6,691 億ウォンである。そのうち、第 4 四半期の実績が 7 兆 8,416 億ウォンであり、第 1 四半期の 4 兆 1,261 億ウォンに比べ、90.0%の増加となっている。この背景には、電子部品や自動車業種における販売が 2000 年の間に EDI からインターネットを基盤にした取引に移行したことがある。韓国統計庁の調査によると、2000 年 12 月の時点で韓国には 191 のｅマーケットプレイスがあり、そのうち、2000 年度にサービスを開始した企業は 88%をしめる 168 社である。韓国において、2000 年度はｅマーケットプレイス市場が急激に拡大した年であるが、収益については芳しくなく、大部分のｅマーケットプレイス企業が赤字であると見られる。この背景には、日本と

同様、ビジネスモデルや戦略を熟考しないまま市場に参入してしまったことがある。

シンガポールにおいても BtoB 市場規模が 2000 年には 1999 年の倍以上の 920 シンガポールドルにまで発展している。

中国は巨大な潜在的市場規模を有しており、2001 年の WTO 加盟後、ますます注目を浴びている。中国における電子商取引の市場規模は、2000 年の 22 億ドルから、2004 年までに 600 億ドルを超える額へ拡大すると予測されており、そのうち BtoB 取引が、総額の 75%以上を占めている。

しかし、中国では企業間での債務不履行や偽造品や粗悪品の横行といった信頼に関する問題や、金融インフラの改善の問題、政府によるメディアや娯楽についての監視や規制など、インターネットビジネスの発展を阻害する要素があり、これらの克服がインターネットビジネスの発展のための課題として挙げられている。また、IDC チャイナの調査レポート「Internet eCommerce Adoption in Key Vertical Industries」（IDC #CN180311H、2001 年 9 月）においては、多くの企業が、技術面と費用面に問題があるため、今後 2 年は電子商取引戦略の展開や実施を予定していない、とされている。

c. ヨーロッパ

ヨーロッパ地域では 2000 年には 2,620 万ドルであった市場は 2004 年には約 8 億ドルに達すると予測されている。eMarketer によるとヨーロッパは 2000 年からの 5 年間で市場規模を 30 倍以上に広げ、世界におけるシェアを 28.7%占めるという。Jupiter MMXI の調査によると、ヨーロッパにおける BtoB 市場規模は、2000 年には 2,000 億ユーロだったが、2004 年には 1.8 兆ユーロにまで成長するとしている。

2001 年初期の IDC の調査によると、ヨーロッパにおいても、e マーケットプレイスはもっとも成長する分野であり、2005 年までに急速に発展するものと考えられている。BtoB においては、国別に見ると、イギリスが中心的に活動しているが、データから判断すると、フランスは他の 11 カ国をしのいでおり、2005 年までに電子調達の分野で年平均 275%の成長をすると考えられる。ドイツの成長率は 236%、UK は 221%である。

ヨーロッパは 3 億 2,000 万人の消費者の市場だが、均質な市場ではなく、文化の違いが BtoB に大きな影響を及ぼしている。たとえば、フランスで設立された e マーケットプレイスはフランス語で構成されており、他の言語が追加されない限り、フランス市場でのみ利用されることになる。ただ、統一通貨ユーロの導入によって、価格比較が促進され、市場に透明性が増し、売上高は急増するものと考えられている。

d. ラテンアメリカ

eMarketer の調査によると、ラテンアメリカ地域では 2000 年には 290 万ドルであった市場規模は 2004 年には 5,840 万ドルに達すると予測されている。2000 年からの 5 年間で市場規模を 20 倍以上に広げることになるが、世界におけるシェアはほとんど占めないとされている。

e. アフリカ・中東

eMarketer の調査によると、アフリカ・中東地域では 2000 年には 170 万ドルであった市場規模は 2004 年には 1,770 万ドルに達すると予測されている。2000 年からの 5 年間で市場規模を 10 倍以上に広げるが、ラテンアメリカと同様、世界におけるシェアはほとんど占めず、ラテンアメリカとあわせても 3%にも満たないという予測である。

(3) BtoC 市場動向

米 eMarketer の調査によると、世界の BtoC 市場は 2000 年には 600 億ドル、2004 年には 4,000 億ドルに達すると予測されている。

a. 米国

米 eMarketer によると、2000 年には 383 億ドルだった BtoC 市場は 2001 年には 542 億ドルに拡大し、2004 年には 1,260 億ドルにまで達するとされている。

米国においては、インターネット利用ユーザが多く、1998 年から 1999 年にかけて BtoC が広く普及し、オンラインショッピングが先進ユーザから一般大衆へと広まった。オンラインショッピングを行っている人は、2000 年の 6,410 万人から 2003 年には 1 億人に達するとされている。米国では、クリスマス時期のオンラインショッピング商戦が最も活発な時期であるが、2001 年のクリスマス時期には、多くの Web サイトがオンラインで注文を受け付け、店頭で品物を受け取るという販売方法が推進され、クリスマス間際まで注文が殺到する状態だったという。ネットバブル時代に乱立した BtoC サイトは淘汰される傾向にあるが、適切なビジネス戦略を確立しているサイトでは、収益が増加しており、購買側の意欲も衰えていないことがうかがえる。

b. アジア・太平洋

IDC の調査によると、日本を除いたアジア・太平洋地域におけるインターネットビジネス市場は 2001 年には 15 億ドルだが、今後 5 年間で、平均 24%ずつ上昇し、2006 年には 45 億ドルに達すると見込まれている。この成長は中国やオーストラリ

ア、韓国などが牽引するものと考えられる。また、The Boston Consulting Group によると、アジア・太平洋地域の BtoC 市場規模は 2000 年で 68 億ドルだったものが、2001 年には 140 億ドルに増加すると予測されている。

韓国においては、2000 年における BtoC 市場規模は 7,337 億ウォンであり、全体の商取引額の 4.5%を占める。これは、アジア諸国において、非常に高い数値となっており、韓国において急速に電子商取引が発展していることが分かる。その背景には、韓国において、ブロードバンドネットワークが急速に発展していることが挙げられる。米 RHK が行った調査によると、2001 年末の時点でアジア・太平洋地域には750万人を超えるDSL加入者がおり、世界中のDSL加入者の44%を占めている。そしてそのうちの 400 万人は韓国のユーザであり、2002 年におけるアジア・太平洋地域の成長を牽引するのは韓国であるとしている。

またシンガポールにおいても、BtoC は急速に発展しており、2000 年の市場規模は 1999 年の 5 倍以上にあたる 11 兆 7,000 億シンガポールドルにまで成長した。

c. ヨーロッパ

eMarketer の調査によると、ヨーロッパにおける BtoC 市場規模は 2000 年には 80 億ドルだったのに対して、2004 年には 1,825 億ドルにまで成長すると予測されている。IDC の調査では、2000 年には 125.6 億ドルだった市場は、2004 年には 1,679 億ドルにまで成長し、2005 年には 2,532 億ドルに達すると予測されている。

米 IDC の調査「Internet Commerce Market Model (ICMM) version 7.3」によると、2001 年末の時点で、西ヨーロッパのインターネット利用者人口は、米国の利用者人口を上回り、さらに BtoC および BtoB を合わせた電子商取引市場規模においても、2001 年に日本を抜き、米国に次ぐ 2 位になったという。1 位の米国と比較すると市場規模の差は依然大きいが、その差は 2005 年までに狭まるとされている。

Nielsen/NetRatings の調査によると、スウェーデン人の 4 人に 1 人が、過去 6 ヶ月間にインターネットで買い物をしているとのことである。ヨーロッパ諸国におけるインターネット取引は、平均 9%であり、スウェーデンは 26%と、平均を大きく上回る結果となった。スウェーデン以外には、スイスが 17%、デンマークが 16%、ノルウェーが 14%、オーストリアが 12%となっており、フィンランド、オランダ、ドイツおよびイギリス各国は 11%となっている。

d. ラテンアメリカ

ラテンアメリカ地域におけるインターネット利用人口は 2,070 万人といわれているが、BtoC は発達しているとはいえない。

e. アフリカ・中東

アフリカではすべての国がインターネットに接続できる環境があるが、インターネット利用は金銭にゆとりのある限られた人間のみであり、定期的にインターネットを利用する人は総人口 8 億人のうち 400 万人と言われている。中東においてはイスラエルがインターネット技術の面で発達しているが、これらの地域では、イスラム文化に基づく規制や内乱、通信インフラの未発達などが原因でインターネットの普及が進んでいない地域が多く、BtoC の普及は先の話である。

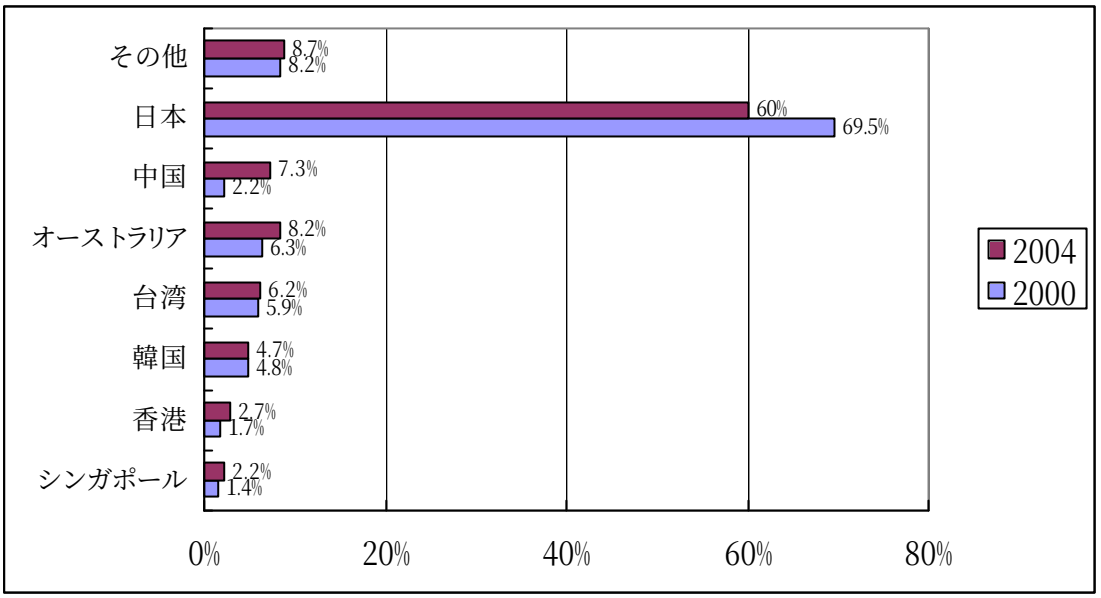
(4) 比較分析

米国ではネットバブル時代に非常に多くのインターネットビジネスサイトが成長し、そしてバブルの崩壊とともに消えていったが、日本においては、米国レベルまで成長・普及する前にバブルの崩壊を迎えたため、インターネットビジネスに対する不信感や躊躇が根強いものと考えられる。

a. アジアの中の日本

BtoB 市場においては、アジアの中で日本は現状では圧倒的なシェアを獲得しており、市場規模も群を抜いている。しかし世界全体で見ると、規模もシェアも依然として低く、発展が望まれる。インターネットの技術がますます発展し、産業としてのレベルが低い地域においてインターネット導入が進んだ際に、日本が競争力を維持するためには、企業は調達分野を積極的にオンライン化することでコストを下げ、利益を上げることが求められる。

アジアにおける各国の BtoB 市場シェア



(出典) The BtoB Market in Asia (eMarketer)

https://www.emarketer.com/analysis/easia/20010116_asiab2b.html

b. 米国と日本の比較

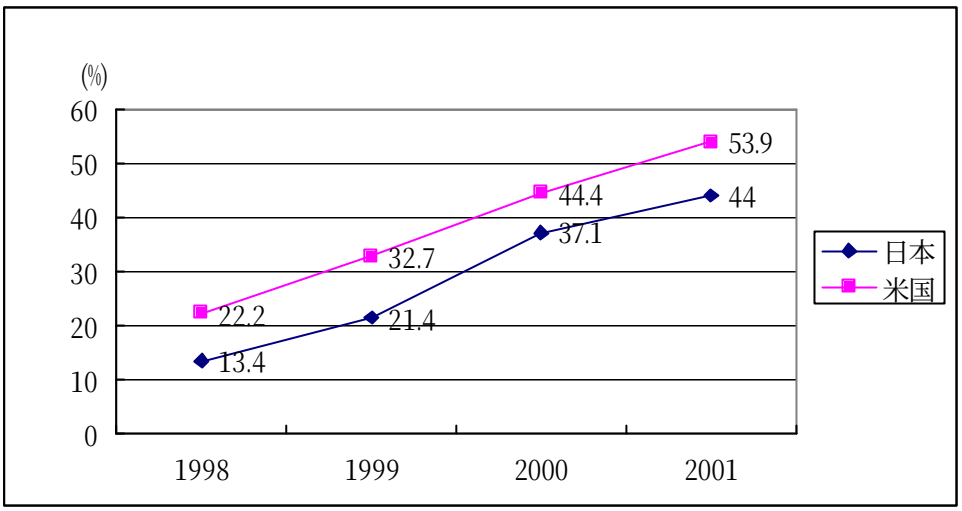
先の eMarketer の調査によると、2000 年には米国は世界の BtoB 市場で 70.3%を占めており、アジア・太平洋地域は 10.8%、そのうち日本は 6.5%となっている。2004 年には、米国が 57.7%、アジア・太平洋地域は 16%、そのうち日本は 11%となる。ここから、2000 年には 10 倍以上あった日米の差は 2004 年には約 5 倍近くにまで縮小する見込みであることが分かる。

日米の世界における BtoB シェア

	2000 年	2004 年
米国	70.3%	57.7%
日本	6.5%	11%
ヨーロッパ(参考)	11.6%	28.7%

また、BtoC に関しては、日本においてはまだ日常生活にオンラインが浸透しきっておらず、買い物や銀行分野での利用が少ない。これらの数字から、日本では依然インターネットショッピングに消極的であることがうかがえる。

日米におけるインターネット人口普及率の格差



(出典) 日本総務省「通信利用動向調査」、米国商務省「A NATION ONLINE」

http://www.soumu.go.jp/s-news/2002/pdf/020521_1_01.pdf

http://www.ntia.doc.gov/ntiahome/dn/anationonline2.pdf

日米における用途別のインターネット利用率の比較（複数回答）

	日本	米国
電子メール	64.8	84
ニュース･スポーツ等の情報収集	45.9	61.8
ネットショッピング	18.9	39.1
掲示板、チャット等の利用	15.6	17.3
オンラインバンキング	3	17.9
インターネット電話	3	5.2
e ラーニング	0.9	3.5

(出典) 日本総務省「通信利用動向調査」、米国商務省「A NATION ONLINE」

http://www.soumu.go.jp/s-news/2002/pdf/020521_1_01.pdf

http://www.ntia.doc.gov/ntiahome/dn/anationonline2.pdf

第 4 章　インターネットビジネスの安全性および信頼性に関する調査

1. インターネットビジネスにおける脅威に関する動向調査

本項では、一般的なビジネスには無いインターネットビジネス独自の脅威を調査し、その脅威が企業経営者に与える影響度を分析する。

(1) インターネットビジネスにおける脅威の種類

一般に、インターネットにおける脅威としては、ホームページの改ざんが連想されることが多いが、企業の紹介を目的としたホームページが改ざんされたような場合は、その企業に対する信用度は下がるが、他社に被害を与えるようなものではない。

インターネットビジネスのメリットは、地理的、時間的制約を受けないことであり、世界中に対して、24 時間・365 日ビジネスを行うことができるという点である。また、誰でも利用できるオープンな環境であるため新しく設備を敷設する必要が無いこと、情報が即時に伝達されることから諸々の手間が省け結果的にコストが低下することが挙げられる。このメリットを生かすためには、24 時間・365 日常に業務を稼働し、障害発生からも即座に復旧する連続運転体制が必須となる。また、企業の持つ機密情報をネットワーク上で常時公開することになるため、情報の漏洩や運用妨害を目的とした攻撃などネットワーク上に氾濫するさまざまな脅威が生じ、それらの脅威から 24 時間・365 日体制で情報資産を守る必要が生じる。取引においては、相手方の顔が見えないことから、本当に信頼できる取引相手かという判断がつかないことも挙げられる。

インターネット上の脅威は、機密性に対する脅威、完全性に対する脅威、可用性に対する脅威の 3 つに分類される。

カテゴリ	詳細
機密性(Confidentiality)に対する脅威	ネットワーク上のデータやサーバ上のデータを許可されていない人に見られること。
完全性(Integrity)に対する脅威	ネットワーク上のデータやサーバ上のデータが不当に改ざんされたり、破壊されたりすること。
可用性(Availability)に対する脅威	システムの機能、サービス、データが、悪意を持つ人によって利用できなくされること。

a. 機密性に対する脅威

インターネットビジネスにおける機密性に対する脅威としては、取引の情報が漏洩すること、また、漏洩した情報が悪用されて、企業の信頼が失墜することが挙げられる。

a-1. 情報漏洩

漏洩する情報としては、取引における顧客情報などの機密情報や、消費者の個人情報やクレジットカード情報、公開サーバのアカウントやパスワードなどがある。これらの情報は漏洩すること自体が危険なのではなく、悪用されることに危険性があり、正当な取引相手へなりすまされること、取引情報データが改ざんされることなどが考えられる。情報漏洩が発生する可能性として、侵入攻撃によるもの、盗聴によるもの、設定の不備によるものが挙げられる。

侵入攻撃は、悪意の第三者がターゲットサーバのアクセス権を不正に取得することを目的とした攻撃である。攻撃を受け、サーバへの不正侵入を許した場合、サーバに保管してある情報は漏洩する。また、盗聴によって取得したアカウント情報から、侵入攻撃を受け、サーバにバックドアが作成されたり、別のサイトへの攻撃の踏み台として利用されたりする可能性がある。

インターネットにおける盗聴とは、ネットワーク上に盗聴ツールなどを設置することで、ネットワーク上を流れる情報を盗み取るものである。インターネット上の通信は、経路となる機器やケーブルを多くの人が共有しているため、送信する情報が相手方に届くまでのルートを特定できず、通信の秘密が保証されない。盗聴によりサーバのアカウントやパスワードなどの情報が第三者に入手されてしまった場合、その情報をもとに、侵入攻撃など行うことが可能になる。また、特にインターネットビジネスにおいては、消費者が送信した個人情報や商品情報、クレジットカード番号などの情報や企業間の取引情報が第三者に漏洩する危険性がある。悪意の第三者による盗聴を免れるためには、インターネットビジネスにおいての通信は、すべて暗号化される必要がある。

サーバやアプリケーションの設定や運用の不備によって脆弱性が生じた場合、サーバ上に保管されている情報が漏洩する可能性がある。適切な管理下で収集した情報を保管していない場合や、Web サイトにおいてプログラミングの際の不備でクロスサイトスクリプティング(CSS：Cross-Site Scripting)の脆弱性がある場合に、個人情報やユーザの Cookie 情報が悪意の第三者に送信されてしまう恐れがある。Cookie はオンラインショッピングサイトなどで認証やセッション管理の方法として使用されており、Cookie が盗まれた場合、Cookie を入手した第三者がなりすましを行う可能性がある。

企業の信頼を失墜させる情報漏洩だが、インターネットを介した個人情報流出の事例が後を絶たない(付録 1 参照)。漏洩する情報は、懸賞への応募やインターネ

ットオークションなどでユーザが入力した個人情報が多く、適切なセキュリティの下で管理されていないことが多いと言われている。また、近年は漏洩が発覚すると閲覧方法がインターネット上の掲示板に書き込まれる傾向があり、情報の伝播が早い。警察庁も「個人情報の流出事案に関する対策について」という警告を発し、企業への注意を呼びかけている。

b. 完全性に対する脅威

インターネットビジネスにおける完全性に対する脅威としては、商品情報や取引情報の改ざんによる個別取引に関するトラブルの発生、情報漏洩を引き金としたなりすましによる不正な取引、などの可能性が挙げられる。

b-1. なりすまし

盗聴や不正侵入などを通じて個人情報を入手して、悪意の第三者が正当な取引相手になりすまし、取引を行うことが考えられる。この場合、なりすましの第三者と取引をした企業が商品を騙し取られて損害を被る、なりすまされた側が代金を請求されるなどの危険がある。なりすましを防ぐためには、取引相手が正当な本人であることを確認するための認証を行う必要がある。盗聴や Cookie の漏洩によって、個人の ID やパスワードが悪意の第三者に知られてしまった場合、なりすましを行うことは比較的容易であり、これを回避するのは困難である。

2002 年の 5 月には、元派遣社員として銀行に勤務していた男が、口座の暗証番号に生年月日の数字を使用していた 2 人の顧客を探り出し、インターネットバンキングサービスを悪用して、3 ヶ月にわたって合計 370 万円の不正送金を続けていたという事件が発生しており、インターネットビジネスにおけるなりすましの脅威を一般消費者にも知らしめる衝撃的な事件であった。

b-2. 改ざん

Web サイトが侵入攻撃などを受け、商取引を行っている Web ページが改ざんされた場合、企業や取引先は損害を被る可能性がある。例えば、商品情報を掲載している Web ページが大規模に改ざんされた場合は分かりやすいが、価格などを一部改ざんされたような場合は発見が遅れることが考えられ、その間に実取引において被害が生じる可能性がある。また、発見した後も、復旧までの期間運用が妨げられることになり、損害を被ることになる。

また、通信経路における盗聴が可能な場合、悪意の第三者によって取引情報を改ざんされる可能性がある。消費者が購入した商品の数量や届け先などが第三者に改ざんされ、正規の消費者のもとに届かないといったトラブルや、第三者に商品を不正に購入されるといった危険性がある。不正アクセスによる侵入を許して

しまった場合、取引自体が正当に終了した後に、サーバに保管してある取引データが改ざんされる可能性もある。

対処方法としては、通信に暗号化を施し、盗聴を防ぐことで通信経路における改ざんを防止する方法、デジタル署名を使用したデータの認証、システム上のデータ改ざんの前段階となるサーバへの不正アクセスの防止がある。

b-3. 信頼性の欠如

また、信頼性の欠如という観点からは、悪徳業者による商品代金の詐取、不良品の押し付けや、禁制品や盗品などの不法な販売といった脅威も考えられる。

c. 可用性に対する脅威

インターネットビジネスにおける可用性に対する脅威としては、システムの破壊や改ざんなどの攻撃によってシステムが運用できなくなること、ネットワークおよびシステムに対して攻撃が行われることで通信が利用できなくなり取引相手からアクセスができなくなることが考えられる。

c-1. DoS(Denial of Service：サービス不能)

DoS はネットワークやサーバに対して何らかの方法によって過剰な負荷をかけることでサービスの提供を妨げる攻撃である。インターネットビジネスにおいては、DoS 攻撃を受けることで、運用が妨害される可能性がある。2000 年 2 月に Yahoo やアマゾン・ドットコムといった米国の有力ネット企業に対する DDoS (Distributed Denial of Service)攻撃が行われ、Web サイトに接続できない状態に陥った事件は、世界中に衝撃を与えた事件であった。この攻撃によって Yahoo がサービス不能状態になっていた時間は 3 時間ほどだが、その損失は数百万ドルにのぼると言われている。このような事例を考えてみると、24 時間 365 日の連続稼動が妨害されることが、収益に多大な影響を及ぼすことがよくわかる。スパムメールなどによって、ネットワークトラフィックが増加し、本来目的とする通信に支障が出るなどという事象も、DoS の一部と捉えることができる。

c-2. 踏み台

セキュリティホールの悪用や、アクセス制御などの設定の不備、パスワードの漏洩などから、攻撃者が自サイトのシステムにログイン可能な状態にある場合、攻撃者が自分の情報を隠蔽するための踏み台にされる可能性がある。踏み台にされたサイトは被害者であるといえるが、攻撃を受けたサイトから見ると、踏み台サイトが攻撃元に見えるため、自サイトは加害者という扱いを受け、信頼の失墜

や、法的に訴えられる可能性がある。

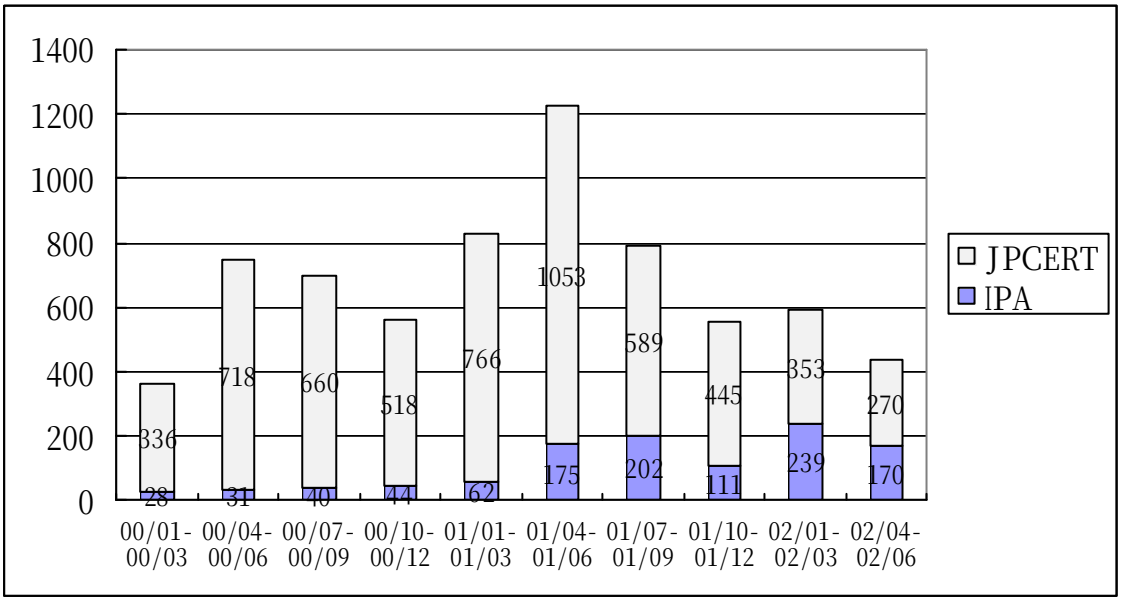
(2) インターネットビジネスにおける脅威の現状

a. 不正アクセス

インターネットビジネスにおいては、他の一般的なビジネスと異なり、店舗やコンピュータ本体を直接物理的に攻撃する以外に、ネットワークを通じた脅威がある。アクセス制御を施して、ID やパスワードといった認証を行った上で利用できるようになっているネットワーク上の資源に対して、使用を許可されていない者がネットワークを通じて何らかの方法でアクセスし使用することを不正アクセスという。

現実世界と比較してインターネット上には特別に危険性が多いということではないが、インターネットを通じた攻撃や不正アクセスは匿名で、コストをかけず、なおかつ低リスクで行うことができるため、現実世界と比較して比較的容易であるという特徴がある。2002 年 6 月末までに報告された不正アクセスの被害状況は以下のとおりである。

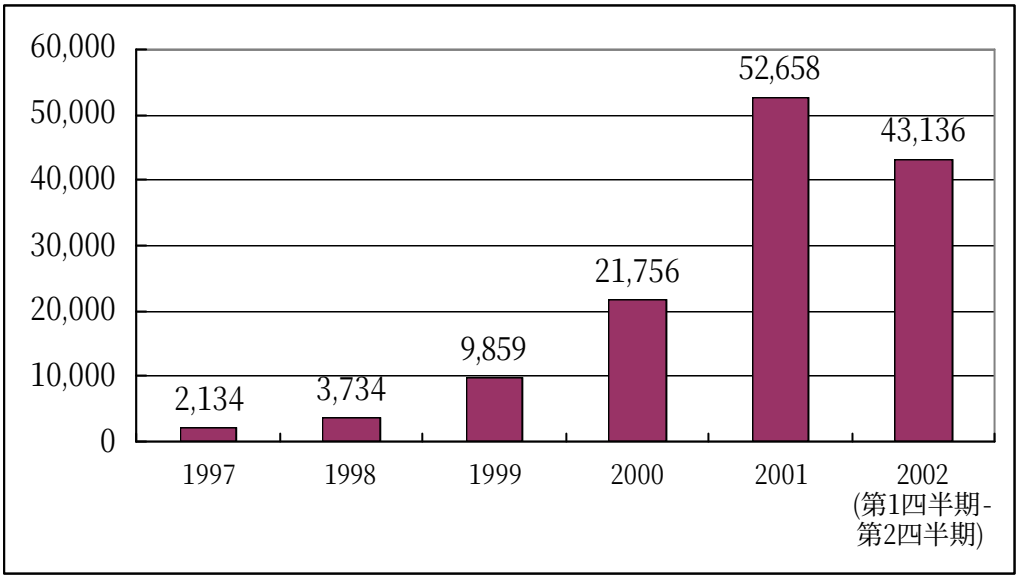
IPA、JPCERT が受け付けた不正アクセスに関する届け出



(出典) IPA 「2002 年第 2 四半期[4 月～6 月]不正アクセス届出状況」

http://www.ipa.go.jp/security/crack_report/20020726/02q2.html

CERT/CC に報告された不正アクセス届け出件数



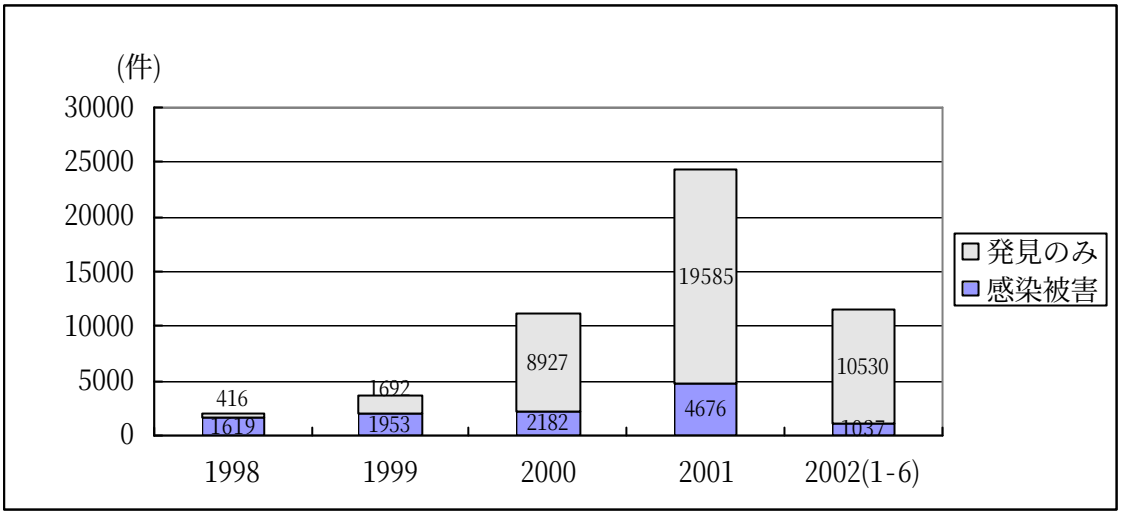
(出典) CERT/CC --- Number of incidents reported
http://www.cert.org/stats/cert_stats.html

これらはあくまで不正アクセスを受けたという「報告」の統計であり、不正アクセス行為自体の数ではないが、届け出数だけでも増加の一途をたどっており、不正アクセス自体が増加しているものと予測できる。

b. コンピュータウィルス

不正アクセス以外に、一般的に広く知られている脅威として、コンピュータウィルスが挙げられる。コンピュータウィルスは、1986 年に初めて発見されたが、当時のウィルスはフロッピーディスクなどを媒体にシステムに感染し、データを破壊するものが主流だった。1995 年には Word などのドキュメントに感染するウィルスが登場し、マクロウィルスが登場するきっかけとなった。1999 年には、電子メールを媒体に感染するウィルスが登場した。これは Internet Explorer のセキュリティホールを利用したもので、メールを読むことで感染するタイプである。近年は、「Nimda」や「Code Red」など、ソフトウェアのセキュリティホールを利用して感染するワームや、「Sircam」や「Bad Trans」など感染すると自らを電子メールに添付して拡散するウィルス、感染後、特定の Web サイトなどを攻撃するようなものが主流となっている。

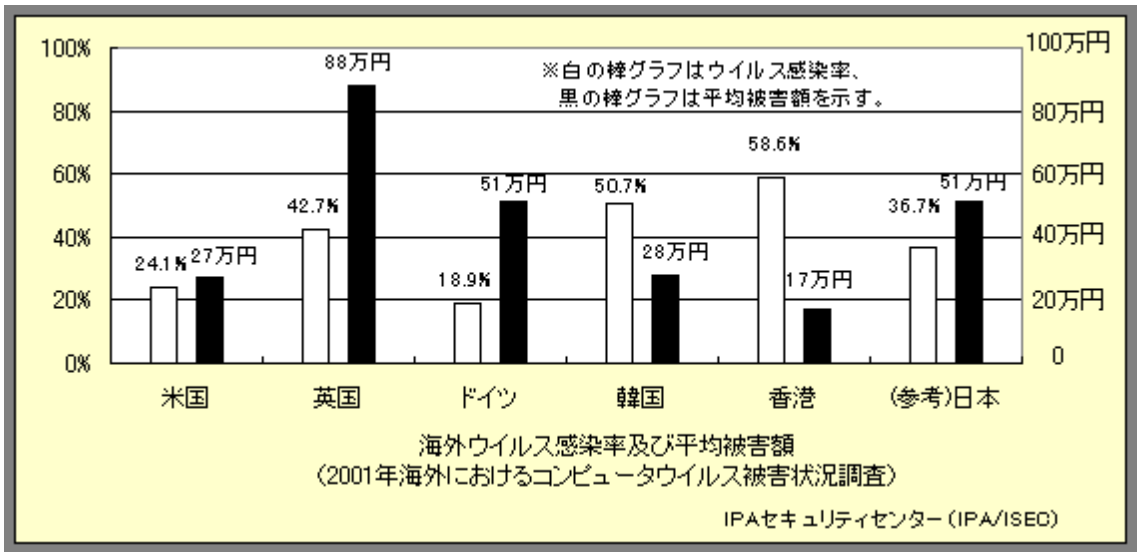
ウィルス感染報告



(出典) 情報処理振興事業協会 セキュリティセンター

http://www.ipa.go.jp/security/

海外ウィルス感染率および平均被害額



(出典) 情報処理振興事業協会 セキュリティセンター「コンピュータウイルス被害状況調査結果要約」

http://www.ipa.go.jp/security/txt/attach/2002_04-1.html

ウィルスの被害は一般ユーザ同士の感染や、社員の感染を発端とした企業内の感染だけではなく、企業から消費者に対してウィルスを添付したメールが送信されてしまい、消費者に被害を与え企業の信頼が失墜する可能性がある。2001 年には衣料品の販売を行うワコールが、会員向けに発行しているメールマガジンにおいて

「HYBRIS」ウィルスが添付したメールを約 6,500 人の会員宛に送信し、数百人単位で感染者が出た。この事件では、メーリングリストの会員にウィルスに関する知識が低い PC 初心者の女性が多く、被害が拡大した。

また、2002 年には、地域 CATV 会社の豊島ケーブルネットワークが、CATV インターネット接続会員約 7,000 人全員に「Frethem」ウィルスの亜種が添付されたメールを送信した。ISP という、インターネットへの接続口となるサービスで、このような事件が発生することは非常に望ましくなく、信頼の失墜は避けられないと考えられる。

(3) 被害額の算出

インターネットビジネスを提供する企業にとって、最も脅威となることはビジネスを提供できなくなり、損害を被ることである。また、悪意の第三者による商売への直接的な妨害や、サービスを提供する基盤となるインフラへの攻撃による妨害に加え、そのような攻撃に対して脆弱であるという管理体制の露見による信頼の失墜、ユーザの個人情報を公開してしまったことによる信頼の失墜が、企業にとっては最も脅威であり、避けなければならない点である。

KPMG は 2002 年に、世界規模で活動している 641 の企業や組織に対して、情報セキュリティに関する電話インタビューを実施した。

遭遇したセキュリティトラブルはコンピュータウィルスが最も多く、また、被害額は年平均で 162,000 ドルにもおよぶ。調査結果として、セキュリティトラブルによる損害金額は平均 108,000 ドルであるとされているが、この金額にはシステムダウン時の機会損失や従業員の生産性の低下、セキュリティ改善のコストは含まれていない。つまり、本来の損失額は上記金額を上回るものと考えられる。

CSI/FBI Computer Crime and Security Survey によると、米国の企業、政府系機関、金融機関、医療機関および大学の 503 人のコンピュータセキュリティ管理者に対して調査を行ったところ、コンピュータ犯罪および他の情報セキュリティ違反などの脅威は依然衰えておらず、被害額が増大していることがわかった。

回答者(主に大手企業および政府系機関)の 90%は過去 12 か月以内にコンピュータセキュリティ犯罪があり、80%の割合で金銭的な被害があったとしている。コンピュータ犯罪の被害があった回答者のうちの 44%(223 人)は金銭的な損失を算出しており、その結果、被害総額は 455,848,000 ドルにのぼることがわかった。

これらの調査では被害額が算出されて記載されているが、実際に不正アクセスなどのセキュリティ侵害に対して、被害額を算出するのは非常に困難である。セキュリティ侵害によって発生する企業イメージや信頼度の低下、取引企業への被害、ビジネス

チャンスの喪失などは、企業によって被害額の判断が異なるからである。

この被害額の算出モデルを作成する試みがなされている。IPA と NPO 法人の JNSA は、コンピュータウィルスやホームページの改ざんなど「サイバーテロ」による被害額を算出する手法をはじめて開発した。

同手法では、被害を金額として認識できる「表面化被害額」と、金額として表出しにくい「潜在化被害額」とに分類している。加えて、表面化被害額を、逸失利益や復旧に要したコストなどの「1 次的な被害額」と、補償や補填、損害賠償などの「2 次的な被害額」に分類し、表面化被害額と潜在化被害額の総和を全体的な被害額として位置づけている。

(4) 今後の動向

セキュリティホールや新たな攻撃手法、コンピュータウィルスなどは日々発見されており、今後もセキュリティに関する攻撃と防御のいたちごっこは続くものと考えられる。今後の新たな脅威として、増加する個人ユーザに対する攻撃が考えられる。

現在のウィルスは、PC を対象としたものが主流だが、今後モバイルコマースが発展すれば、携帯電話や PDA がビジネス用の情報端末として主流となるため、ウィルスのターゲットに含まれてくることが考えられる。すでに、携帯電話を対象としたウィルスや PDA に対するトロイの木馬などは事例があり、いつ悪意のあるプログラムが出現するかわからない状態と言える。

また、個人間でのファイル交換用ソフトウェアなどの普及によって、これまでも違法コピーされたソフトウェアや音楽コンテンツがやり取りされていたが、今後の個人ユーザの増加によって、ソフトウェアや音楽コンテンツ以外にも、悪意のある情報の売買が増加するといった脅威が考えられる。

2. 情報セキュリティに関する動向調査

「情報セキュリティ」という言葉からは、インターネット上の脅威や電子データを守ることが連想されるが、情報セキュリティの範囲はもっと広く、プリントアウトし配布した書類の取り扱いや、電車内などの公共の場所などでの業務に関する会話など、PC 上のデータとしての情報だけではなく、紙の上の情報、口頭でやり取りがなされる情報が全て含まれる。それらの取り扱いをどのように制御していくかということが情報セキュリティである。本項では、情報セキュリティに関する動向について、調査を行い分析する。

(1) 情報セキュリティ製品に関する市場動向

増加しつづける脅威への対策として、企業はセキュリティ製品やサービスを導入している。情報処理振興事業協会セキュリティセンターが行った「情報セキュリティビジネスに関する調査」によると、日本の情報セキュリティ製品市場規模は、1999 年には 455 億円だったが、2004 年には 1,530 億円にまで発展すると予測されている。

また、ブロードバンドネットワークの普及によって、企業のみでなく消費者においてもセキュリティ製品を導入する必要性が増している。米 Cahners In-Stat Group の調査によると、常時接続型の消費者が増加することで、消費者側でのセキュリティ需要も増加する、としている。消費者向けの広帯域セキュリティ製品の市場規模は、ファイアウォール製品の売上が増加したこともあり、2000 年の 7,400 万ドルから 2005 年末には 8 億ドルにまで拡大するという。

ここでは、セキュリティ製品において主要なものであるアンチウィルス製品、ファイアウォール、認証製品、暗号製品に関する市場動向を調査した。

日本の情報セキュリティ製品市場 (億円)

	1999 年	2000 年	2001 年	2002 年	2003 年	2004 年
アンチウィルス	235	325	395	493	633	858
ファイアウォール/VPN	113	124	133	142	151	158
認証	67	120	151	197	261	367
暗号	22	31	40	53	74	112
セキュリティマネジメント	18	21	24	27	31	35
計	455	621	743	912	1,150	1,530

(出典) 情報処理振興事業協会セキュリティセンター「情報セキュリティビジネスに関する調査」

http://www.ipa.go.jp/security/fy12/report/sec_biz.pdf

米国の情報セキュリティ製品市場　　(１００ 万$)

	1999 年	2000 年	2001 年	2002 年	2003 年	2004 年
アンチウィルス	613	746	881	972	1,065	5,328
ファイアウォール/VPN	274	309	350	393	429	481
認証	1,013	1,329	1,653	2,047	2,566	3,234
暗号	65	81	93	100	105	108
セキュリティマネジメント	104	135	167	204	255	317
計	2,069	2,600	3,144	3,716	4,420	9,468

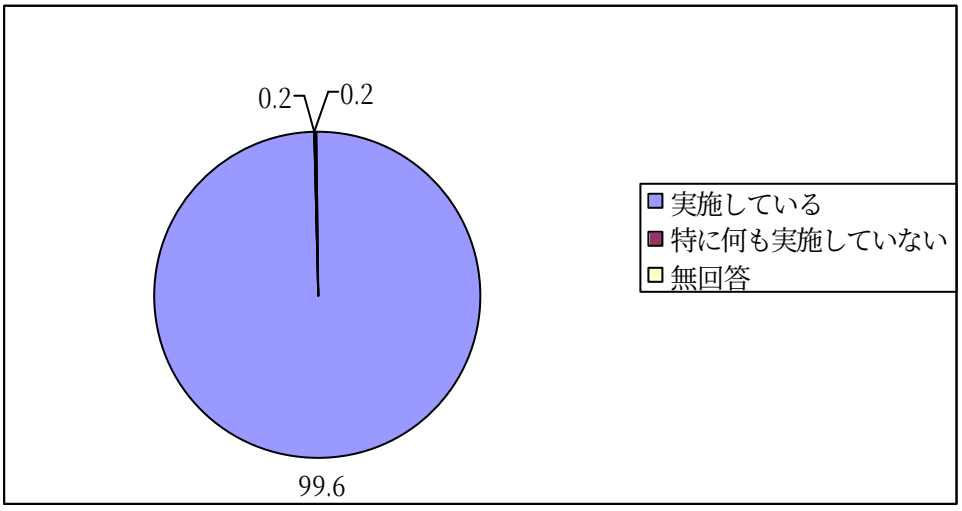
(出典) 情報処理振興事業協会セキュリティセンター「情報セキュリティビジネスに関する調査」

http://www.ipa.go.jp/security/fy12/report/sec_biz.pdf

a. アンチウィルス

総務省の調査によると、民間企業におけるアンチウィルス製品の導入状況は、クライアントマシンで 95.2%、サーバマシンで 81.5%と比較的高い水準となっている。しかし、アンチウィルス製品はパターンファイルの常時更新など、導入後も適切に運用する必要があり、導入すれば安心という製品ではない。PC 起動時に必ずアップデートを行うなど、定期的にウィルス情報を更新している割合は民間企業全体の 64.3%にしか満たない。ただ、近年の電子メールを媒体に感染するウィルスの蔓延に伴い、企業に対する被害が増加したため、ウィルス対策に対する企業の意識が以前より格段に高まってきていることがウィルス届け出状況からも見て取れる。

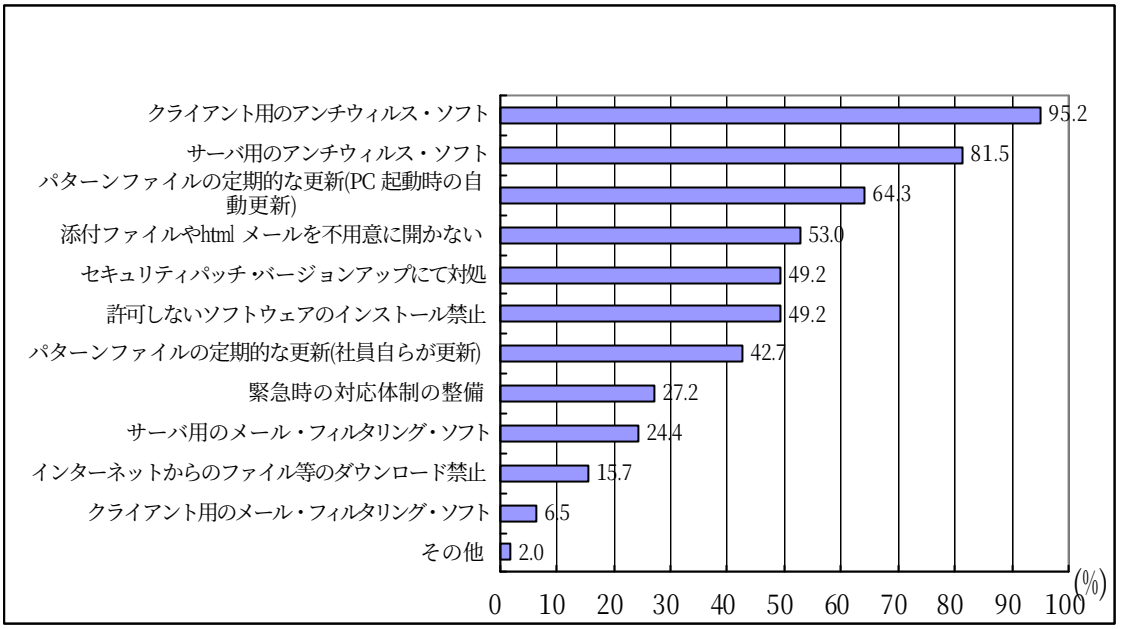
民間企業におけるウィルス対策の実施有無



(出典) 総務省「情報セキュリティ対策の状況調査結果」

http://www.soumu.go.jp/s-news/2002/pdf/020509_2_1.pdf

民間企業におけるウィルス対策



(出典) 総務省「情報セキュリティ対策の状況調査結果」

http://www.soumu.go.jp/s-news/2002/pdf/020509_2_1.pdf

ウィルスの感染後の活動形態や感染媒体が多様化している今日では、アンチウィルスソリューションもクライアント PC 上での感染を防御、検出、駆除するものから、ウィルスが添付されたメールをメールサーバ上で検出、防御するというゲートウェイ型の製品が普及しつつある。ただ、現在主流のアンチウィルスソフトはパターンマッチング方式であり、新種や亜種のウィルスが発見されてからパターン定義ファイルを更新するまでの間は無防備である。ウィルスに対する認識は広く普及しつつあるが、情報処理振興事業協会セキュリティセンターが行ったコンピュータウィルスの被害状況を調べるアンケート調査によると、2001 年の 1 年間で国内企業がこうむった被害額は最大で 5000 億円以上にのぼると試算されており、ウィルスによる損失が甚大であることが分かる。今後も定義ファイルの更新方法や、検知技術の進化・発展によって、アンチウィルス製品市場は拡大し続けるものと考えられる。

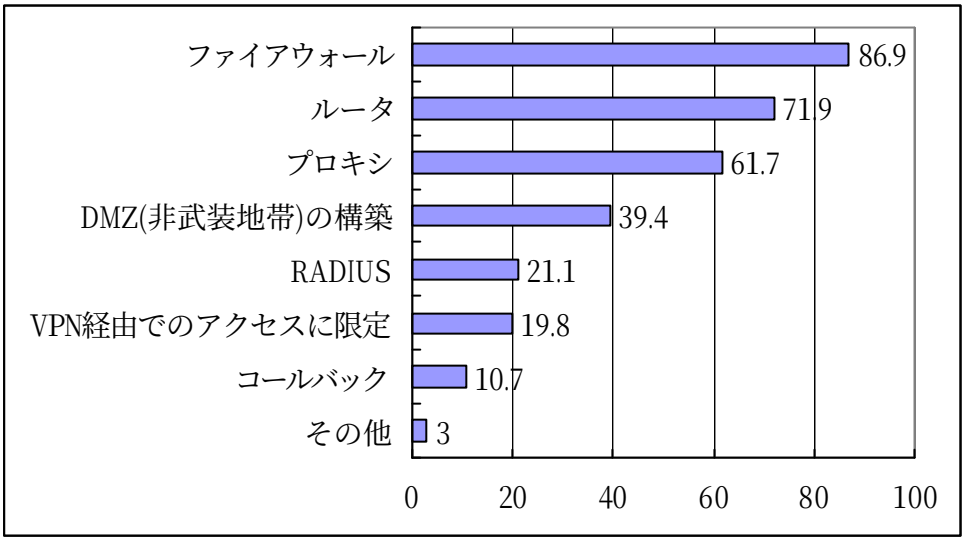
日本におけるアンチウィルス製品の市場規模は、1999 年の 235 億円から 2004 年には 858 億円に成長するものと予測されている。

b. ファイアウォール

ファイアウォールはインターネットと社内ネットワークとの通信においてアクセス制御を行うために不可欠である。総務省の調査によると、ファイアウォールを導

入している民間企業は 86.9%にのぼり、外部から社内ネットワークへの接続に関しては、ほぼ 100%の民間企業で何らかのアクセス制御対策が実施されている。日本企業においてはファイアウォールさえ導入していれば安心であると誤解し、ファイアウォールを過信している風潮があるが、現在はインターネットセキュリティに関する報道や雑誌記事への掲載の機会なども増加し、このような認識にも徐々に変化が表れつつある。

社外からのアクセス制御



(出典) 情報セキュリティ対策の状況調査結果

http://www.soumu.go.jp/s-news/2002/pdf/020509_2_1.pdf

近年、ゲートウェイ型のファイアウォール以外にも、PC にインストールして使用するパーソナルファイアウォールや、他のセキュリティ製品の機能を搭載したファイアウォールが登場している。ブロードバンドネットワークの普及に伴い、常時接続されている PC が急増し、一般消費者の不正アクセス被害や、他のホストに対する不正なアクセスの踏み台にされるといった危険性が増加している。パーソナルファイアウォールはそのような個人向けのファイアウォールとして 2000 年に画期的に登場した。小型のルータに組み込まれているものもある。

他製品の機能を搭載したファイアウォールには、前述のアンチウィルスソフトと連携し、最新のパターンファイルに更新していない PC に対しては、インターネット接続を遮断するといったものや、IDS(侵入検知システム)機能を追加した製品などが登場している。一般に、パケットフィルタリング方式のファイアウォールはアクセス許可しているサービスを通じた不正アクセスを防ぐことはできないが、そのような攻撃に対して、パターンマッチングにより攻撃を検知する IDS 機能をファイアウ

ォールに搭載することで対応し、ファイアウォール機能と連携して攻撃のトラフィックを遮断することができる。

日本におけるファイアウォール製品の市場規模は、1999 年の 113 億円から 2004 年には 158 億円に成長するものと予測されている。

c. 認証

インターネットの発展には、利便性とともに匿名性が大きく寄与してきたと言える。しかし、インターネットビジネスにおいては、取引相手の本人確認や取引情報となる文書が正しいものであることの信頼性を確保することが最重要事項であり、信頼しうる情報であることを確認するための、手書きの署名や押印といった従来の仕組みと同等の機能としての認証が重要視されている。認証方法は以下の 3 つに大別できる。

認証方法	代表例
知識による認証	暗証番号、パスワード
持ち物による認証	IC カード、トークン
身体的特徴による認証	バイオメトリクス、くせ

c-1. 知識による認証

古くから使用され、最も一般的な認証方法が暗証番号とパスワードである。パスワードは半角英数と特殊文字を組み合わせ、類推しにくく長い文字列であることが要求されるが、ユーザがパスワードを考える場合、管理は自分に任されるため、簡単に覚えやすく類推しやすいものを選ぶ傾向がある。反対に、管理者が設定してユーザに配布する場合、覚えにくくユーザが管理しきれないという問題がある。

パスワード管理の問題を解消するために、グラフィカルなインタフェースを使用することで使い勝手を考慮した認証製品も登場している。シー・エス・イーが開発した「SecureMatrix」は、ブラウザに表示される数字の書かれた表を用いてログインを行う。ユーザは数字を覚えるのではなく、「形と順番」をパスワードとして利用する。たとえば左上から V 字型に抜き出す法則をパスワードとして使用する場合は、その V の字の下に記入されている数字がログイン時に使用するパスワードになる。画面に表示される数字の配列表はログインのたびに変更されるため、パスワードとなる数字列は毎回異なる。また数字を抜き出す方法と固定のパスワードを組み合わせることも可能であり、法則を推測されても安全に運用することが可能だ。

例)左上から V 時に抜き出す場合

1	9	7	3	2	8	6	0	7	1	9	4	2	3	9	6
0	2	5	8	9	3	5	1	4	2	5	3	7	5	8	1
7	6	3	0	1	0	4	7	9	8	0	6	1	0	2	5
4	8	2	9	7	6	2	8	3	7	2	8	6	9	4	8

この場合パスワードは「12397050」になる

c-2. 持ち物による認証

持ち物による認証には、一般に IC カードによるものとトークンによるものがある。IC カードは PC やネット接続機器で利用することが可能であり、管理が容易である。個人のアクセスを管理するために、他製品と組み合わせて導入している企業もあり、今後、住民基本台帳ネットワークにおいても、IC カードが導入されることになっているため、生活に深く関わってくる。それに伴い、IC カードの読み取りシステムの発展など、IC カード関連市場も拡大するものと考えられる。

トークンを利用したワンタイムパスワードは、毎回パスワードを使い捨てることでパスワードを保護し、パスワードを安全に運用するための方式である。ユーザが使用するパスワード生成機(トークン)と、認証を行うワンタイムパスワードサーバにより構成され、パスワードはランダムに自動生成されるため予測がきわめて困難であり、また盗聴されてもそのパスワードは再度使用しないため二次利用による攻撃を防ぐことができる。

IC カードやトークンを偽造することは現在の一般的技術では不可能に近いため、知識を利用した認証方式と比較するとセキュリティ強度は高い。ただ、持ち物だけで認証を行うため、その物自体の紛失や盗難、貸与によって、本人以外の人が容易になりすましを行うことができる。持ち物による本人認証を行う場合は、セキュリティレベルを強固に保つために、物による認証以外の方式と併用する必要がある。

c-3. バイオメトリクス認証

紛失したり忘れる可能性のない物として、身体的特徴(バイオメトリクス)を利用した認証がある。身体的特徴という本人のみが使用できる情報を利用することで、なりすましを排除し、その利用者が正当な利用者本人であることが証明できる。バイオメトリクス技術を使用した認証製品は一般に広く登場している。現在は指紋認証が最も普及しており、その他に網膜や虹彩、顔、声紋、掌形、静脈パターン、署名といったものがある。

最近では、マウスの握り方やキーボードのたたき方などのくせを利用した本人認証の方法や製品が開発されている。富士ゼロックスは、マウスをクリックする

たびにマウスの握り方をチェックして、本人であるかどうかを判断する認証技術を開発している。これによって、ログイン時の本人認証だけでなく、その後の操作間も本人確認が可能だ。他人を本人と誤認識する確率が 1〜2%であり、指紋認証の 0.1〜0.0001%などよりも照合精度は劣るが、他の認証技術と併用することで実用できる。また、米 Net Nanny Software が発売している「BioPassword」は入力する文字列をあらかじめ決定しておき、キーボードをたたくリズムなどでユーザを認証するための製品である。

これらの技術を併用することで、たとえ ID やパスワードが漏洩しても、それだけではログインできない強固なシステムを構築することができる。また、特別な入力デバイス(ハードウエア)が不要という点も導入者にとっては魅力となる。

c-4. シングルサインオン

利用者の負担を削減する技術として、複数のサービスをひとつの ID で利用して、認証の手間を省くシングルサインオンシステムが挙げられる。社内 LAN などの管理されたネットワークや、インターネットを介した特定のシステム間においては、シングルサインオンの技術は広く活用されているが、インターネットでの利用は困難であり、現時点では汎用的に実装できる製品や技術は登場していない。

Microsoft は、複数の組織やサービスをまたがってシングルサインオンを利用できるようにするために、同社の電子認証サービスである Passport を企業やネットワーク事業者、サービス事業者などに開放する計画を明らかにした。Passport は、複数の Web サイトにまたがってシングルサインオン機能を提供する認証サービスであり、氏名やパスワードなどの個人情報をあらかじめ登録しておけば、Web サイトにおいてそれらを自動入力するものである。また、2001 年 10 月には Sun Microsystems を代表とする 33 社が、インターネットにつながっているどのようなデバイスからでもシングルサインオンできる Web サービス用の認証システムを共同開発するための業界団体「Liberty Alliance Project」を発足し、2002 年 7 月にシングルサインオンを実現する仕様「Liberty version 1.0」を公開した。

シングルサインオンがインターネット上で広く普及するには、これらの仕様が統一される必要があるが、いったん個人認証がなされれば複数のサービスでわずらわしい認証を介さずにサービスが利用できるため、今後のインターネットインフラの発展、ひいてはインターネットビジネスにもに大きく貢献するものとなる。

c-5. PKI(Public Key Infrastructure)

インターネット上において、取引相手の本人確認を行うと同時に情報の漏洩や改ざん等に対応する仕組みとして電子署名・認証があるが、現在、最も利用されているものとして公開鍵基盤(PKI)に基づくものが挙げられる。PKI とは、公開鍵

暗号方式という暗号技術を使用したセキュリティインフラである。デジタル署名によって、プライバシーの保護や情報改ざんの検出、本人認証などを行うことができる。

c-6. 電子署名

公開鍵暗号方式では、公開鍵と秘密鍵のいずれかを使用して文書を暗号化し、暗号化した鍵に対応する他方の鍵を使用して復号する。秘密鍵の所有者あてに公開鍵を用いて暗号化した電子文書を送信すれば、復号できるのは唯一その秘密鍵を持つ受信者だけであり、誰もが秘密鍵の所有者に安全に電子文書を送信できる。また、自分の所有する秘密鍵を用いて電子文書を暗号化すれば、対応する公開鍵を所有している者は誰でも復号化を行って、電子文書の内容を確認することができる。同時に、その電子文書の作成者が秘密鍵の所有者であることが確認できる。電子署名はこの特徴を用い、電子証明書によって電子署名を行った者を確認する仕組である。PKI によって、以下のことが実現できる。

PKI によって実現できる効果	
通信の機密性の確保	データを盗聴から防ぎ、意図した特定の相手のみデータを閲覧できる。
相互認証	送信者が確実に本人であることを保証する。なりすましを防止。
事後否認の防止	送信者はデータを作成・送信したことを後から否定できない。
完全性の確保	通信の間にデータが改ざんされていないことを保証する。

PKI は 1998 年から 1999 年にかけて、認証に欠かせない技術として注目を浴びたが、主要となるアプリケーションがなかったことや運用の困難さから大規模成長にはおよばなかった。しかし、今後、インターネットビジネスの発展や電子政府の実現などから PKI を利用した認証は発展するものと考えられる。

日本における市場規模は拡大する傾向にある。総務省が行った調査によると、2001 年度の電子認証ビジネス市場規模は約 63.4 億円と推計され、現時点では電子認証ビジネスは初期段階であることが示唆されている。しかし、今後の電子認証ビジネス市場規模は順調に拡大する事が予想され、2006 年度には約 419.5 億円にまで市場規模が拡大するものと予測されている。日本における発展の背景には、2003 年度に開始される電子政府が大きな影響を与えるという予測がある。 2001 年度においては、米国における電子認証ビジネス市場規模の予測値は、日本市場の約 8.5 倍だが、2006 年度には、その差が約 4.5 倍にまで縮小すると予測されている。

d. 暗号

インターネットにおいては盗聴ツールをネットワークに接続することで、誰もが比較的容易に盗聴を行うことができるため、オンラインショッピングに必要なクレジットカード情報やその他の個人情報などの人に知られたくない情報や、ビジネスにおける取引内容などの機密情報は暗号化する必要がある。暗号を使用したソフトウェアとしては、PC 側で電子メールの内容の暗号化を行う暗号化ソフトや他人に見られたくないファイルを暗号化するものなどがある。クライアント・サーバ間の通信の暗号化では、SSL が用いられることが多い。

暗号化には、暗号化と復号化に同じ鍵を用いる共通鍵暗号方式と自分の持つ秘密鍵と配布する公開鍵とで暗号化・復号化を行う公開鍵暗号方式とがある。認証と共に暗号化のインフラとしても重要視されている PKI だが、サーバにおける情報保管時の暗号化に関しても考慮する必要がある。

米 Frost & Sullivan が行った調査によると、多くの国内外の政府機関や団体がネットワークのセキュリティ強化に乗り出しており、機密情報を保護する暗号機器の導入を拡大、その結果として、暗号技術市場は 2007 年には 4 億 5760 万ドル規模に成長すると予測されている。

e. 今後の動向

これらの動向から、ファイアウォールにアンチウィルス機能を連携させたウィルスゲートウェイやファイアウォールへの IDS 機能の追加、クライアント PC 向けのアンチウィルスソフトとパーソナルファイアウォールを統合した製品など、他の機能を持った製品と連携させることで、製品を多機能にしていくといったトレンドがうかがえる。また、製品のパターンファイル更新の自動化といった、管理者への負担を軽減するメンテナンスフリーの製品が好まれる傾向にある。

アンチウィルス製品分野では、従来のパターンマッチング方式では防ぐことのできない未知のコンピュータウィルスに対して、ウィルスの特徴を使用した検出方法を利用した製品が発表されている。既知のマクロウィルスと類似した処理を行うマクロを持つファイルをウィルスとして検出するものや、電子メールを媒体に感染するウィルスの特徴を利用し、同じ件名のメールや同じファイルが添付されたメールが一定時間内に大量に来た場合にはウィルスとして判断する機能を持つ製品などである。これらのウィルスの特徴を把握するための時間はパターンファイルを作成するための時間よりも短いため、パターンファイル配布前でも、ウィルス対策が可能

になる。

また、従来のアンチウィルスソフトでは、感染したホストをネットワークから切り離す以外に拡散を食い止める方法はないが、メールクライアントのアドレス帳に登録されているメールアドレスを暗号化することで、感染したウィルスがアドレス帳からメールアドレスを取得して、自動送信するのを回避する製品も登場している。

その他､感染力の強いウィルスが発見された場合にその情報をユーザの PC にポップアップ表示をする、ユーザの許可をスキップして常に最新のパターンファイルを適用する、といった機能が追加された製品が発表されている。

ファイアウォール製品においても、新しい試みがなされている。ネットワークインタフェースカード(NIC)にファイアウォールの機能を組み込んだ製品である。ファイアウォールのポリシーを中央のサーバで一括管理、設定し、挙動を監視することができる。もし内部からの不正アクセスや、ウィルスによる外部への攻撃を開始したホストを発見した場合、中央管理サーバからポリシーを操作することで、未然に事故を防ぐことができる。ポリシーの設定に必要な鍵があらかじめ NIC に設定されており、鍵は中央のサーバのみが保持しているため、セキュリティ上の信頼性も高い。

日本においてインターネットビジネスが今後発展していくにあたり、企業のセキュリティレベルの保持に役立つセキュリティ製品市場は成長していくものと考えられる。ファイアウォールやアンチウィルスに関しては、導入数のみを考慮すれば、すでに市場は飽和状態にある。しかし、情報セキュリティ製品も運用を間違えば、背後に過信がある分だけセキュリティレベルを下げかねない。製品は運用によって生きるものであり、導入したことに安心せず、適切な運用を心がける必要がある。

(2) 情報セキュリティサービスに関する市場動向

ここでは、主要な情報セキュリティサービスである、セキュリティシステム構築、コンサルティング/監査、セキュリティシステム管理、セキュリティ保険における市場動向についてまとめている。

日本の情報セキュリティサービス市場規模 (億円)

	1999 年	2000 年	2001 年	2002 年	2003 年	2004 年
セキュリティシステム構築	206	248	302	349	410	499
コンサルティング/監査	19	26	35	48	66	92
セキュリティ管理	50	68	98	145	247	456
セキュリティ保険	16	25	37	52	69	89
計	291	367	472	594	792	1,136

(出典) 情報処理振興事業協会セキュリティセンター「情報セキュリティビジネスに関する調査」

http://www.ipa.go.jp/security/fy12/report/sec_biz.pdf

米国の情報セキュリティサービス市場規模 (100 万$)

	1999 年	2000 年	2001 年	2002 年	2003 年	2004 年
セキュリティシステム構築	1,038	1,266	1,549	1,819	2,194	2,822
コンサルティング/監査	796	959	1,168	1,372	1,724	2,217
セキュリティ管理	675	840	1,185	1,410	1,755	2,312
計	2,509	3,065	3,902	4,601	5,673	7,351

(出典) 情報処理振興事業協会セキュリティセンター「情報セキュリティビジネスに関する調査」

http://www.ipa.go.jp/security/fy12/report/sec_biz.pdf

a. セキュリティシステム構築

インターネット上でビジネスを行うにあたり、ネットワークやサーバなどのシステムは安全に設計されている必要がある。従来のセキュリティシステム構築は、システム構築時にサーバの要塞化などのセキュリティ対策を行う、ファイアウォールを導入しネットワーク上のトラフィックを制限する、などの個別の対応が主流であった。近年、セキュリティに対する意識が向上する中で、セキュリティに特化したシステム構築の提供や、単体の製品導入ではなくネットワーク全体の総括的なソリューションを提供する、といったシステムインテグレータ業者が増加している。

セキュリティシステム構築サービスの市場規模は、1999 年には 206 億円だったが、2004 年には 499 億円に成長すると予測されている。

b. コンサルティング/監査

近年、企業におけるセキュリティ意識の向上に伴い、セキュリティ対策はシステム的観点からのコンサルティングのみでは不十分であり、経営的観点からのコンサルティングが重要であるという認識が広まってきた。そのため、システムのセキュリティ対策を依頼されたシステムベンダやシステムインテグレータなどの事業者が

経営的なコンサルティングを必要とする際に、コンサルティング・会計監査企業が持つコンサルティングのノウハウやスキルが非常に期待されており、提携や協業によってコンサルティングを行うことも多くなっている。

限られた予算内で効果的なセキュリティ対策を行う場合、セキュリティポリシーを確立することが最も重要と言われており、セキュリティポリシーの構築支援サービスをビジネスとする動きが出はじめている。セキュリティポリシーの目的は、各々の企業におけるリスクとその対応を明確にし、社員全員のセキュリティに関する意思統一を促すことにある。セキュリティポリシーに沿ってシステムや保護すべき最低限のセキュリティ要件を定義することで、必要以上の対策を行うことによるコストの偏りや無駄な投資を防ぐため効率的にセキュリティ対策を実施することができる。

ただ、問題として挙げられることは、不正アクセス監視やウィルス対策製品などはその効果を説明しやすいが、セキュリティポリシーの場合は費用に対する効果を定量的に説明することが難しいことや、ポリシーの策定は社内の全部門に関わるため、組織運営や規程類の変更が必要になる場合があることなどがある。セキュリティポリシーの策定のビジネス化を行うにあたっては、顧客へ必要性を論理的に説明できることなどが必須となる。

コンサルティング/監査サービスの市場規模は、1999 年には 19 億円だったが、2004 年には 92 億円に成長すると予測されている。

c. セキュリティシステム管理

インターネットビジネスを円滑に行うためには、大容量の高速回線や強力なサーバシステムが不可欠となる。また、災害や事故でシステムダウンが突然発生する可能性もあるため、その対策も必要になる。また、多くの企業がセキュリティ製品を導入しているが、インストールやアップグレードなどの保守が余計な手間となり、個々の企業では対応しきれないことが多い。このような企業のインターネットビジネスをサポートするシステム管理サービスが普及している。

システム管理サービスとしては、大容量 IP バックボーンを備えたインターネットデータセンタにおける Web ホスティングなどが挙げられる。また、サイト自体の運営から、データセンタに設置したシステムに対する監視など、多くのサービスが提供されている。

セキュリティシステム管理サービスの市場規模は、1999 年には 50 億円だったが、2004 年には 456 億円に成長すると予測されている。

d. セキュリティ保険

1998 年 1 月に実施された企業保険分野の自由化によって、保険会社が企業分野に関する保険商品を自由に設計できるようになり、ネットワーク保険サービスが本格的に導入された。また、2000 年初めの有名 Web サイトへの DDoS 攻撃は、企業に自サイトのセキュリティに対する意識を向上させたうえ、踏み台にされることによって自サイトが加害者にならないようにといった認識も広がり、セキュリティ保険は勢いを加速している。現在は各事業者ともメニューの体系化を進めており、ネットワークを用いてビジネスを行う事業者向けの保険および一般企業向けの保険が主な商品となっている。セキュリティ保険の対象としては、以下のものが挙げられる。

セキュリティ保険対象
・コンピュータ、コンピュータ周辺機器などの情報機器 ・情報およびその記録媒体 ・業務を継続して行うための費用 ・自己発生時の営業中断による利益 ・情報漏洩などによる損害賠償 ・ISP や SI 業者の場合の補償

セキュリティ保険の分野においては、保険会社の社員には、契約から支払いといった一連の保険業務知識と情報セキュリティに関する知識との双方に精通していることが要求される。このような性質のものであるがゆえに、損害保険会社ではコンサルティング企業と協力するケースが多い。この場合は、損害保険会社と協力したコンサルティング企業が保険加入の際のリスク分析・評価を代行する、コンサルティングを希望したユーザに対しトータルなセキュリティプランの一環として保険を紹介する、という協業体制になっていることが多い。

セキュリティ保険サービスの市場規模は、1999 年には 16 億円だったが、2004 年には 89 億円に成長すると予測されている。

e. 今後の動向

インターネットがビジネスのツールとして普及している現在では、企業が自社内部のみで情報セキュリティを確立することは困難になってきている。また、セキュリティの確保を提供するこれらのサービスはますます多様化していくことが考えられ、インターネットビジネスに参加する企業の増加に伴い、情報セキュリティサービスも発展の一途をたどるものと考えられる。

第 5 章　インターネットビジネス発展のための課題検討

1. インターネットビジネスの安全性および信頼性における問題点の抽出

インターネットビジネスに関するトラブルは増加しており、特に BtoC においては、個人情報やクレジットカード情報の漏洩、代金を支払ったにも関わらず商品が届かない、購入していないのに代金が請求される、などの事例が後を絶たない。BtoB に関しても、インターネットの匿名性や不確実性、米国におけるネットバブルの影響が災いし、早期発展には至っていないのが現状である。本項では、今後の日本におけるインターネットビジネス発展のための安全性および信頼性における問題点を抽出する。

(1) セキュリティ製品に対する過信

企業は自社サイトを防衛するために、セキュリティ製品を導入しているが、製品の性能を過信しており、導入したことだけで満足しているような場合、その製品の性質を把握した適切な運用ができていないことが多い。また、面倒を避けるために、適切に運用を行っていないこともある。

a. ファイアウォール、アンチウィルス

「情報セキュリティ対策の状況調査結果」によると、日本におけるアンチウィルス導入企業は 95%に達し、ファイアウォールも 87%の導入率となっている。しかし、日本の企業では、アンチウィルスソフトとファイアウォールが情報セキュリティの 2 大柱であるかのような捉えられ方をしていることが多く、この数字のみでは情報セキュリティ対策が万全であるとは言えない。ファイアウォールもアンチウィルスも最も基礎的な情報セキュリティ対策であり、これらの製品を導入していても、ずさんな管理では本来防げるはずの不正アクセスも防ぐことができない。また、内部犯行や情報漏洩などに対しては、何の効果もないため、「セキュリティ対策＝ファイアウォール、アンチウィルス」といった認識は即刻捨てるべきである。

b. バイオメトリクス認証

米国防総省が同省の陸軍研究所(Army Research Laboratory)のもとで、米イリディアン・テクノロジーズ社の虹彩認識技術と米ビジョニクス社の人相照合技術を利用した認証製品に関する検証を実施した。これらのシステムに対して、イリディアン社は自社製品の精度は 99.5%であるとし、ビジョニクス社も 75～99.3%の確度で人相照合が可能であると公表していた。しかし、検証の結果、ビジョニクス社のシステムが正しく個人を識別できた割合はわずか 51%であり、より精度が高いとされていたイリディアン社の虹彩スキャナーにおいても識別率は 94%にとどまった。こ

のように、セキュリティ製品もメーカーの宣伝ほど精度が高くないことがありえるため、利用者は製品を過信せずに厳格に運用を行う必要がある。

2000 年 11 月には、大半の指紋認証製品において、ゼラチンで作成した人工指によって認証を行うことができるという研究発表が公表された。指を乗せたプリズムに光を当ててその反射した画像を読み取る方法で認証を行う製品の場合、ゼラチンで作成した人工指で認証をごまかすことが可能である。この研究に使用された人工指は、特別な資材を使用したものではなく、一般に入手できるゼラチンと粘土などを用いて 500 円ほどの費用で作成することができるものであった。そのような手軽なもので、強固だと考えられていたセキュリティ製品の壁が突破されてしまうことは、認証業界に波紋を投げかける結果となった。

また、バイオメトリクス認証製品は、けがをした場合に使用できなくなるといった問題を回避するため、バックアップパスワードを設定して運用できる仕様になっているものが多い。体質などで手が汗ばんでいたり、職業事情で手が荒れていたりするような場合も、指紋による認証が困難なため運用をパスワードで行う場合が多い。いずれの場合もセキュリティレベルはパスワードレベル、もしくはそれ以下に下がってしまうことを認識しなければならない。

さらに、紛失や盗難の危険性が無いバイオメトリクス認証は運用におけるリスクが高い、という考えもある。認証手段が鍵やカードなどの所有物の場合は、それを渡すことで資産は失っても生命を守ることができる。認証手段が知識によるものの場合、パスワードを教えずにいることもできる一方で、やむをえない場合は生命を優先して教えるという選択も可能だ。しかし、バイオメトリクス認証の場合は、容易に渡すことができないため、システムを守るためにユーザの生命が失われた、という事件も発生し得る。最悪の場合としてシステムも守れず人命も失われた、といったことも考えられる。

セキュリティを守る際に最重要視しなければならないものは、民間の企業であれば、人命、身体があり、そして資産・システムの順であると考えられる。軍事組織などは除いて、システムを守るために、人命を危険にさらす可能性のある手段は現実的であるとはいえない。

(2) 企業のセキュリティ対策の認識不足

取引は信頼関係の上に成立するものであるため、個人情報の管理は、インターネットビジネスにおいても最重要課題である。インターネットビジネスにおいては、現実

社会と異なり、全世界からアクセス可能であるため、情報の管理が不適切な場合は漏洩する可能性が高く、また電子データは複製が容易であるため、一旦漏洩すると、情報が劣化しないまま短期間で拡散してしまい、追跡は困難となる。

インターネットビジネスにおいては、通信経路上で盗聴されることで発生する個人情報の漏洩が注目されることが多いが、第 3 章で取り上げたように、企業側の保管対策によって回避できるものが大半である。

a. 収集した情報の保管方法

これまで、Web サーバ上に保管されていた個人情報の漏洩が発生した企業では、データが保管されているディレクトリに対して適切なアクセス制御がなされていなかったことが原因であるといわれている。Web サーバにおいて、ディレクトリに対する閲覧が可能な状態にある場合、そのディレクトリ上にあるファイルの一覧は、ブラウザを通じて誰もが容易に閲覧することができる。末端ページからホームページに向かってディレクトリをさかのぼるという方法は、多少の知識があるユーザは試みることであり、Web システムを通じて収集したアンケートの結果データを同じディレクトリ上に保存するような設定になっている場合、それらの情報は確実に漏洩してしまう。

同じディレクトリに保管するという運用自体に危険性があるのだが、ディレクトリに対する閲覧を拒否しておくことである程度は危険性が減少する。一方、ディレクトリに対する閲覧を拒否する設定になっていたとしても、容易に想像できるようなファイル名で保管されていれば、こちらも情報が漏洩する確率は高い。個人情報などの機密データは適切な場所で、なおかつ暗号化された上で保管されなければならない。

b. プログラムの不備

HTTP プロトコルにはセッション管理という概念がないため、ショッピングサイトなどでは個人認証とセッション管理に Cookie を利用しているサイトが多い。何度も個人情報の登録を行うことなく、ショッピングサイトへのログインや、ショッピングカートへの商品の追加などができるのは、ブラウザがその Web サイトに対する Cookie を保有しており、サイト側がその Cookie 情報を用いてセッション管理をしているからである。つまり、Cookie が盗まれた場合、悪意の第三者がそのユーザになりすますことができる。インターネットビジネスにおいて、クロスサイトスクリプティングが非常に危険なのは、第三者に Cookie を盗まれてしまう危険性があるからである。インターネットビジネスサイトの設計者および管理者はこの点に十分に注意する必要がある。

クロスサイトスクリプティングは、HTML や XML などのマークアップ言語で記述された Web ページのソースコードを、CGI などを用いて動的に生成する仕組みを設けている場合に発生し得るセキュリティ上の問題である。ある Web ページに記述されたスクリプトが別のサイトへとまたがって(クロスして)実行されることから、クロスサイトスクリプティングと呼ばれている。

Web ページを自動生成する過程で、悪意の第三者がその Web ページを構成する部分を記述できてしまうような設定の場合、悪意の第三者は、アクセスしてきたユーザに対して他のサイトにある悪意あるプログラムをダウンロードさせるようなスクリプトを記述することができる。そのような場合、その Web ページにアクセスしたユーザは、そのスクリプトによって、知らぬ間に悪意あるプログラムを実行してしまう可能性がある。

c. 暗号化の不備

オンラインショッピングやオンライン会員登録など、個人情報をインターネットで送信する場合、クレジットカード番号や個人の住所や電話番号など他人に知られたくない通信データを盗聴されないように内容を暗号化する必要がある。

Web サイトで一般に広く用いられているのが SSL(Secure Socket Layer)である。SSL は PKI を利用してクライアント・サーバ間の通信を保護するセキュリティプロトコルであり、SSL の導入で暗号化と認証を行うことができる。

SSL 導入で実現できる効果	
暗号化	セキュリティパイプを構築し、ブラウザとサーバの間を行き来する情報を暗号化したりスクランブル化することによって、悪意の第三者が送受信中にデータを傍受したり改ざんしたりすることを防止する。
認証	サーバを認証できるため、ユーザは自分が目的の Web サイトにアクセスしていることを確認できる

SSL は、一般的に Web ブラウザと Web サーバの間で送受信されるデータを保護するために利用されている。SSL で保護されている Web サイトは、「https」で始まるアドレスになっており、ユーザは通信経路が暗号化されていることを確認できる。クライアント側の SSL 処理機能は Web ブラウザに搭載されており、ユーザは SSL 接続に際して特別な操作を行う必要が無く、意識せずに使用できるため、広く普及している。

また、認証機能として、認証局から発行された証明書を用いる。インターネットビジネスを行う企業は、企業が登記に基づき実在するかどうかを確認するための外部団体である認証局から、証明書を取得する。認証を取得することで、Web サーバ

を SSL 接続用に設定することができる。SSL 接続を行う場合は、Web サーバ側で処理を行う必要があるため、通常のデータを転送する場合よりもサーバに負荷がかかる。サーバへの負担を減少し効率の良い運用を行うためには、企業は SSL 設定をする Web ページを厳選する必要がある。

ただ、SSL はデータが転送される 2 点間の経路を保護するものであるため、転送先で個人情報などの機密情報をサーバに保管する場合には、サーバ上で別の方法を用いて暗号化がなされる必要がある。

d. ユーザに対する脆弱な設定の推奨

システムを使用するユーザに対して InternetExplorer のセキュリティの設定を低くするように推奨し、その後の適切な対応の記述が無い Web サイトも存在している。そのような Web サイトでは、運用担当者自身がその危険性を意識していないものと考えられるが、セキュリティに対して知識のないユーザを極めて危険な状態にさらす結果になることを認識する必要がある。

ActiveX は HTML で書かれた Web ページに特殊機能を追加することで、そのサイトにアクセスしてきた人に対して、ユーザ側にプログラムをダウンロードさせて実行させる技術であり、これらの技術によって、Web サイトはインタラクティブなものに変化した。ただ、ユーザ側のブラウザで ActiveX を使用しない設定になっている場合、ActiveX を使用しているサイトは正しく機能せず、活用してもらうことができない。そのため、サイト側はユーザ側に ActiveX の使用を許可してもらうような設定方法を記述しているが、その設定方法の記述が不適切な場合がある。

プログラムをユーザ側に一時的にダウンロードさせ実行させるという、ActiveX で実現可能な機能を悪用することで、悪意のある Web サイト運営者は、ハードディスクの初期化やシステムファイルの削除、ウィルスの感染といった悪意のあるプログラムを実行させることができる。アダルトサイトなどを閲覧したユーザが、ISP のアクセスポイントの電話番号を国際電話に書き換えられ、多額の請求をされるといった手口が有名になり、Internet Explorer で、ActiveX に対する注意を喚起するダイアログを表示したり、実行させなくしたりする設定が可能になった。

しかし、ダイアログが表示されても、この問題に関する知識のない一般ユーザはダイアログの意味を理解できないため、危険を回避することができないという問題がある。比較的多くの Web サイトで、自サイトの ActiveX を正しく機能させるために、未署名の ActiveX コントロールや安全だとマークされていない ActiveX コントロールに対して、InternetExplorer の設定を「ダイアログを表示する」に変更させ、その後、元に戻すよう指示していないことが多い。セキュリティについて考慮され

ていないサイトでは、ActiveX コントロールを「有効にする」ように設定の指示をしているものもある。このような設定をしたままで Internet Explorer を使用しつづけたユーザは、悪意を持った管理者が運営している Web サイトを意図せず閲覧して、被害を受ける可能性がある。

こういった設定を推奨している企業は、明らかに顧客に対する配慮に欠けていると言える。このような事態は、サイト作成の担当者が危険性を十分に理解することで回避することができる。

e. 問題発生後の企業の対応

個人情報を漏洩してしまった企業は、しかるべき対処を行う必要がある。Web サイトからの情報漏洩事件が数多く発生しているが、情報を漏洩した企業側の対応にはばらつきが出ている。問題発覚時は「悪意の第三者による不正アクセスがあり、その結果、適切に保管しておいた個人情報が一般から閲覧できる状態になってしまった」「閲覧方法が掲示板などを媒体に広まったため大規模な被害に至ってしまった」という釈明をしていたが、後日、本当の原因は企業側の設定ミスだったと公表した企業もある。情報漏洩の実際は、不正アクセスによるものではなく、企業側の対策や保護方針に不備がある、もしくはまったく保護がなされていないことが原因であることが多いと考えられている。事実関係を確認しないまま、メディアに対してこのような釈明をしている企業においては、

・推測できるようなディレクトリに個人情報を放置してある
・ディレクトリへのアクセス制御を行っていない
・暗号化は施してあるが、通信経路のみであり保存時は復号化されている

といった管理の甘さ、すなわちセキュリティに関する認識の低さがあり、また、自サイトの管理体制を把握できていないため、結果として、発生してしまった事故の影響を過小評価しているものと考えられる。このような対応は消費者にますますの不信感を植え付けることになり、インターネット、ひいてはインターネットビジネスの発展を妨げかねない。

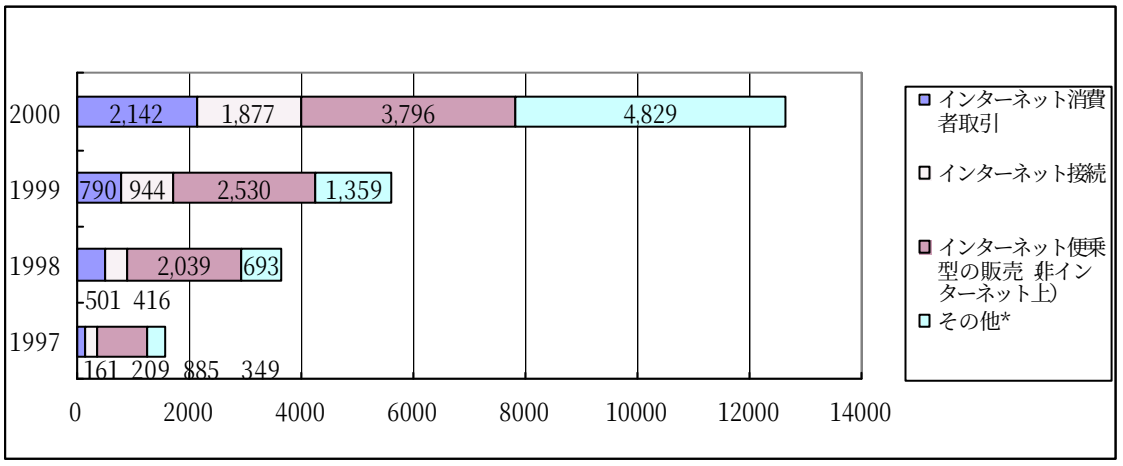
自社サイトにクロスサイトスクリプティングなどの脆弱性が発見されたと報告された場合は、報告を受けた担当者は早急に対処する必要がある。迅速に対処できない場合、その企業の信頼性が揺らぐことになるため、Web サイトの運営担当者は自サイトが被害を受ける可能性がある攻撃や脆弱性を把握するために、セキュリティの動向を常に把握しておく必要がある。

(3) 消費者の知識不足

トラブルが増大する原因として、インターネット利用ユーザが相対的に増加していることが挙げられる。ブロードバンド接続料金の低下や、インターネットに接続して楽しむことが PC 購入の大きな目的となったこと、店頭で販売されている PC への LAN ポートの付属や無線機能のプレインストールなど、セキュリティに関する知識を持っていないユーザでも容易にインターネットに接続できるような環境が整備されつつある。しかし、それに伴い確立されていくべきセキュリティに対する認識や対策、法整備などは、整備されているとはいえないのが現状である。

国民生活センターによると、インターネットや携帯電話機の急速な普及により、若い世代を中心にインターネット関連の相談が増加している、とされている。相談の主な内容は、インターネットオークションに関する代金未払いや商品の未配送、インターネット接続サービスの契約に伴う ISP とのトラブル、インターネットを使用したギャンブルや有料のアダルトサイトなどからの超過請求などが挙げられる。

インターネットに関する相談件数の推移



(出典) 国民生活センター「消費生活相談にみる 2001 年の 10 大項目」
http://www.kokusen.go.jp/cgi-bin/byteserver.pl/pdf/n-20011205_3.pdf

イーシーリサーチが 2001 年 11 月に行ったアンケートによると、ブロードバンドインターネットによる常時接続サービスにおいて、利用者の 82.2%がセキュリティに対して不安を抱えていることが明らかになった。ナローバンドを利用していたころのセキュリティに対しては、52.5%が不安と回答していることから、常時接続の利用により、セキュリティに対する不安が約 1.5 倍に拡大したことになる。特に「とても不安を感じている」とした回答は、ナローバンドの頃の 15.7%から、常時接続では 43.0%と 2.7 倍にまで拡大している。

ただ、多くのユーザがこのように不安を感じているにも関わらず、自衛のための適切な処置を行っているユーザが少ないのが現状である。米 Cahners In-Stat Group が 2001 年に米国の 1,000 世帯を対象に行ったアンケート調査によると、広帯域接続・常時接続環境を持つ家庭において、50%の家庭がセキュリティ対策を行っていないことがわかった。

ダイヤルアップ環境で、使用するときだけ短時間インターネットに接続する場合と異なり、常時接続の環境であれば、サーバだけでなくクライアント PC でも、不正なプログラムを送り込まれ、ほかのサーバを攻撃するための踏み台にされることも考えられる。このようなクライアント PC がインターネット上に多く存在するということは、インターネットビジネスを展開する企業にとって脅威となりうる。情報セキュリティに関する知識のないユーザの存在は、企業にとって攻撃元となる可能性があるホストが物理的に増加するということだけでなく、そのようなユーザがオンラインショッピングに不安を感じ躊躇することで、企業のビジネスチャンスをつぶしてしまう存在となりうる、という脅威になる。

インターネットの普及とブロードバンドサービスの低廉化によって、常時接続ユーザが増加している中で、ソフトウェア会社やサービスプロバイダによって、セキュリティの各種サービスが提供されてはいるが、業界全体としての包括的なサポートの必要性が高まっていくものと予測される。

2. インターネットビジネス発展のための課題分析

ネットワークに対する攻撃は増加しつづけており、米国のセキュリティサービスプロバイダ、Riptech 社(現 Symantec 社)のレポートによると、インターネットに接続されたネットワークへの攻撃はこの半年間で 64%増加している。しかし、これはまだ序の口に過ぎないとされており、攻撃の増加はとどまるところを知らない状況だ。

これまで、インターネットの急速な発展とそれに伴うインターネットビジネスの発展の現状を述べ、インターネットビジネスにおける脅威について述べてきたが、本項では、今後の日本におけるインターネットビジネス発展のための課題を提示する。

インターネットビジネスが今後発展していくためには、インフラなどの基盤が整備・発展するとともに、認証技術の発展や運営体制が確立されることがセキュリティの観点から必須と言える。インターネットビジネスにおいて、第 3 章で挙げたような危険性の発生は、適切な認証体制を確立することで回避することが可能となる。

(1) 企業におけるセキュリティ対策

インターネットビジネス産業全体のセキュリティを向上させるためには、そこに参加する企業が自社サイトのセキュリティを堅牢にしておくことが、大前提として挙げられる。それには、まず自社サイトに存在する個々のサーバを要塞化すること、そしてそれらのサーバ間で通信が発生する場合には暗号化などでその通信を保護すること、そのサーバ上でサービスを提供するアプリケーションのセキュリティレベルを向上させることが必要である。また、自社サイトのセキュリティが万全でも、親密に取引を行っている企業のセキュリティレベルが低い場合は、そちらが不正アクセスを受けて踏み台にされた場合に、自社サイトに被害がおよぶ危険性が増加する。このような事態を回避するために、取引相手企業のセキュリティ意識が低い場合には、セキュリティを強化するよう促進していき、改善されないようであれば取引を停止するなどの強攻策をとることも視野に入れる必要がある。

a. セキュリティに関する認識の強化

情報漏洩時の対応からもうかがえるように、インターネットビジネスサイトを運営している企業のセキュリティに関する認識はさほど高くないのが現状である。Cyber Security Management の調査においても、システムセキュリティ費用を通常のシステム予算と別で確保している企業はきわめて少なく、「人とコスト」に対する認識に関しても「対策が必要である」という認識を持った人が少ないという結果が出ている。また、インターネットビジネスにおいては事故に直面した際に、いち早く復旧を行うことが欠かせないが、企業のバックアップ体制についても整っているとはいえないのが現状である。

たとえば、クレジットカード情報を漏洩された被害者は、そのショッピングサイトではもう買い物をしない。適切な対応が取れない企業においては、せっかくインターネットビジネスに着手しても、いずれ不具合や事故に直面し、ユーザや企業から信頼を得られず、収益も見込めず撤退することになるだろう。

インターネットビジネスを行う各サイトは、セキュリティに対する認識を改め、安全な取引を行うために、安全なシステムを構築し、安全に運用し、消費者保護に重点を置いた上で、その安全性を主張していく必要がある。

1. システムを安全に構築する
2. 安全な運用を行う
3. 消費者保護に取り組む
4. 安全性を主張する

あらかじめ安全に構築されたものを、安全に運用していけば、セキュリティの脅

威が発生する余地がない。脅威の原因を完全に取り除いた上で、消費者の不安を取り除くべく、安全性を主張していくことが、今後のインターネットビジネスの発展には欠かせない。以下に、上記 4 項目について具体的に何を行うべきかを記述する。

b. 安全なシステム構築

安全なシステムを構築するには、サーバの要塞化などのセキュリティ強化と、それにつながるネットワークといったサイト全体におけるセキュリティの強化が必要となる。インターネット上において、不正アクセスが発生する原因は以下のものが挙げられる。

1. アクセス制御の不備
2. 認証の不備
3. セキュリティホールの存在
4. 内部犯行

b-1. アクセス制御

アクセスを許可する人物と拒否する人物を明確に認識できない限り、どのアクセスが不正であるかを判断することはできない。不正アクセス禁止法は、「アクセス制御をしているシステム」への不正侵入を犯罪行為として取り締まるものであり、アクセス制御がなされていない場合もしくは不適切な場合は、侵入されてしまっても犯罪として認められない。システムにおいては、OS とサービスの双方においてアクセス制御ポリシーに基づいた対策を実施する必要がある。また、サーバ内においては、アカウントに対するアクセス制限だけでなく、コマンドに対しても適切な制限を設定する必要がある。

b-2. 認証

安全な取引を行うにあたっては、適切な認証メカニズムを的確に実装した上でユーザ管理を徹底し、認証情報の管理を徹底する必要がある。現在、インターネットビジネスにおける認証システムとしては、PKI を活用したものが主流である。ただ、重要なのは、PKI そのものではなく PKI インフラを生かした付加価値ソリューションが提供されることである。PKI が重要視されて以降、たびたび、PKI ならではのキラーアプリケーションが存在しないことが指摘され、普及の障害になっている。

b-3. セキュリティホール

ほとんどの OS やアプリケーションには、製品の不具合がある。それらの不具合の中で、セキュリティを侵害しうるものはセキュリティホールと呼ばれる。一般

の不具合と同様、セキュリティホールに対してもパッチ(修正プログラム)がリリースされるため、システムの管理者はそれを適用する必要がある。一般的に広く普及し使用されているソフトウェアは、セキュリティホールが発見された時の影響が大きいため、これを探す人が多く、セキュリティホールが発見される可能性が高い。攻撃者は、ただ闇雲に攻撃を行うのではなく、OS や使用しているアプリケーションのバージョンなどを調べ、セキュリティホール情報から当てはまるものがないかを検索し、そこを突いて攻撃を行う。システムの構築時には、ベンダからリリースされているパッチを適用し、セキュリティホールをふさぐ必要がある。

b-4. アクセス許可されたものによる工作

不正アクセスや情報漏洩の大半が内部犯行によるものであるということは、たびたび言及されている。要塞化や適切なアクセス制御を行っていても、実際にアクセスを許可されたものによる犯行や、アクセス権を盗用されたような場合は、事前に対処することは非常に困難である。そのような場合は、適切な事後対処を取ることが要求される。不正にアクセスされてしまった場合の対処として、早急に復旧できるような体制を整備しておくことで、適切な事後対処が可能になる。そのためには、データのバックアップを確保しておくことが必要となる。また、早急な復旧にはあらかじめ、復旧手順を確立しておくことが重要である。

これらの準備があらかじめなされていれば、不正アクセス対策以外にも、災害や事故が発生した場合の早急な復旧が可能である。ただ、まったく同様のシステムを再構築したところで、そのシステムは再度不正にアクセスされてしまうため、原因を究明し、対策をとる必要がある。原因を究明するには、システムやアプリケーションのログが重要な役割を果たすため、アクセスしてきた者のログをとるような設定にしておくことが望ましい。ただ、高度な知識をもった攻撃者はログを削除する方法を知っていることが多いため、IDS などを用いて侵入を検知したり、リアルタイムにログを別の場所に保存したりするような仕組みを整えておくことで、システムの安全性はより高まると言える。

c. 安全な運用

安全に構築したシステムの効果を最大限に生かす方法は、その後の運用にかかっている。いくらシステムを安全に構築しても、運用を適切に行っていなければ、セキュリティレベルが下がるのは時間の問題である。適切な運用を行うには、以下のことに留意する必要がある。

c-1. セキュリティホールへの継続的な対処

システムの構築時には、すでに発見されているセキュリティホールにはパッチ

を適用して安全な状態にしているが、毎日何らかのセキュリティホールが発見され、攻撃手法も日々進化している。そのため、サイトの管理者は自サイトにおいて使用しているソフトウェアや製品の名称やバージョンを把握し、ソフトウェアベンダからの情報やCERTのAdvisoryといったセキュリティ情報を収集しながら、パッチがリリースされたら適用するなどの対策を行う必要がある。使用している製品の情報を登録しておくことで、関係あるセキュリティ情報を有料で配信してくれるサービスなどを活用するのも方法のひとつである。

c-2. 運用ルールの作成・徹底

セキュリティパッチの適用といった運用や障害が発生した場合の対応に関しては、手順を明文化し、徹底することが重要である。システムの運用と異なり、運用に不可欠なセキュリティの概念は身につきにくい。システムを安全に運用するためには、運用ルールが必要であり、セキュリティポリシーを策定し遵守させる企業体制が必要となる。運用ルールには、適切な運用ポリシーに基づいた障害対策手順と障害復旧手順が記述される必要がある。

c-3. 情報セキュリティポリシーの策定

近年の情報技術の発展により、企業内ではあらゆる情報や仕組みが電子化され、社員にはメールアドレスが与えられ、常にインターネットにアクセス可能な環境が整えられている。そのような状況において、ファイアウォールによる外部からのアクセス制御やウィルス対策を筆頭に、さまざまなソフトウェアを導入し、社内ネットワークを守る動きは高まっているが、その反面、操作ミスや設定ミスなどによる情報漏洩や内部犯行なども後を絶たない。その背景には、社員のモラルの低下や対策の不備など、組織の運用体制に問題があることが多い。

このような状況においては、組織としての情報セキュリティに関する方向性を具体的に示し、それに基づいて、社員の教育、体制の管理を行うセキュリティポリシーが効果を発揮する。セキュリティポリシーは、「企業としての取り組みを示す基本方針」と「守るべき規準・標準」の 2 つから構成される。基本方針として、機密情報の取り扱いやプライバシーに関する考え方が記述され、規準ではネットワークや個々のシステムに関する個別の管理方法について規定される。作成手順としては、保護すべき情報資産と利用方針を特定するとともに、どのようなリスクがあるかを具体的に分析し、対応のための基本方針を策定することになる。

セキュリティポリシーの策定によって、「セキュリティ対策における費用対効果の向上」や「情報セキュリティレベルの向上」、「対外的な信頼性の向上」といった効果が得られる。情報セキュリティ対策では、技術的な対策だけではなく、社員のセキュリティ意識向上を図り、内部関係者によるミスや犯行を防ぐ必要がある。

従って、個々の企業には、明確なセキュリティポリシーを持った上で、インターネットビジネス環境全体を捉えた包括的なセキュリティを構築することが要求される。

セキュリティポリシーの策定によって得られる効果	
セキュリティ対策における費用対効果の向上	ポリシーに基づいて、リスクレベルに対する適切なセキュリティ対策を行うことで、個々の判断でセキュリティ対策を行うことがなくなり、企業全体のセキュリティレベルが統一される。限られた予算内で適切な対策ができ、結果として、企業全体のセキュリティレベルがあがる。
情報セキュリティレベルの向上	個々の PC がネットワークに接続するために、一定のセキュリティ基準を満たすことで、全体のセキュリティレベルが向上する。作業を通じて、社員の認識が向上し、設定ミスや内部犯行を防止できる。
対外的な信頼性の向上	社内において、情報セキュリティポリシーを策定し、それに基づいてセキュリティ対策を行っていることを対外的に主張することで、取引先企業からの信頼が増す。

「情報セキュリティ対策の状況調査結果」によると、民間企業においては、28.5%の企業がすでにポリシーを策定しており、20.5%の企業が現在策定作業中である。39.6%の企業は策定を検討中だが、現在策定しておらず今後も策定する予定がない、と回答した企業も 10.5%におよんでいる。約 10 社に 1 社が「予定なし」という結果になるが、セキュリティ対策とプライバシー保護は、企業の信頼性に深く関わるものであり、社員のセキュリティの認識向上にもつながるため、企業の経営者は信頼性の確保の一環として、ビジネス戦略に組み込み、積極的に働きかけていく必要がある。

情報技術の先端は発展し続けているが、インターネットビジネスを開始する企業内には、セキュリティ技術や脅威を把握し、安全なシステムの提案や導入ができるような技術者は圧倒的に少ない。技術者やセキュリティの現状を正確に把握できる担当者を置く体制が確保できない場合には、サイトの構築や運営を専門のサービスベンダに依頼するのが適切である。万全なセキュリティ対策を施すことができれば問題はないが、技術的な対策のみに闇雲にコストをかけるだけでは、リスクは軽減できない。また、有能なセキュリティ担当スタッフを抱えるだけの資金がない企業もある。

情報セキュリティ対策においては、技術面だけでなくセキュリティポリシーやルールの設定と運用、それを実行する社員のセキュリティ意識の高さが必要になる。ただ、情報セキュリティはお金をかけた分だけ安全になるというものでもなく、一定の基準もないため、対策コストの妥当性を一概に特定することは難しい。

インターネットビジネスのセキュリティ対策にかけるコストを算出するためには、セキュリティを侵害された場合のリスクを分析する必要がある。すべてのものに対して中途半端にセキュリティ対策を行うのではなく、リスク分析を通して「最低限守らなくてはならない情報」を把握し、バランスを見てコストをかけていく必要がある。

d. 消費者保護への取り組み

これまでにクレジットカード情報の漏洩や詐欺、個人情報の漏洩が何度も発覚し、報道されてきたことで、消費者のインターネットビジネスに対する不信感は増長している。米ジュピターの調査によると、一般消費者の 60%はセキュリティに対する不安のためにオンラインショッピングをしたことがないという結果となっている。

米コンシューマー・リポート誌が 1500 人の米国インターネット利用者を対象に、電子商取引サイトに対する信頼度に関する調査を実施したところ、消費者の電子商取引サイトに対する信頼度は非常に低く、商品やサービスを販売している Web サイトに対する信頼度は 29%であるという結果になった。新聞やテレビのニュースへの信頼度は 58%、ワシントンの連邦政府への信頼度は 47%であり、電子商取引サイトと比較すると、非常に高い割合となっている。また同報告によると、80%の消費者が、Web サイト上の情報を信頼するために、サイトの運営者や問題が起きた場合に連絡する方法、プライバシー方針、サイトがミスを処理する方法を確認したいと考えている。消費者にこのような不安感を植え付けたのは、企業の Web サイトから個人情報が流出したという過去の事実であるため、消費者の不安感を払拭し、信頼を得るために、企業は障害対策体制を公表する必要に迫られている。

d-1. オンラインマーク制度

オンラインマーク制度とは、オンラインショッピングの事故を防止するために、商工会議所が定めた制度であり、通信販売事業者が実在することを確認し、かつ、Web ページの表記が通信販売の法令等を守っている事業者であることを審査するものである。このマークによって、消費者はその事業者が実在することを確認でき、架空のショッピングページから物品を購入してしまうといったトラブルを防ぐことができる。ただ、オンラインマークは事業者が販売する商品やサービス等の品質や内容、消費者と事業者の売買契約内容、事業者の経営内容を保証するものではないため、オンラインマークがあるというだけですべて信頼できるというわけではない。

d-2. 決済方法の強化

インターネットビジネスの発展に伴い、第 2 章で述べたとおり、課金・決済市

場も拡大していくものと予測されている。ただ、やはりインターネットビジネスの本来あるべき姿は注文から決済まですべてインターネット上で行われるというものである。バガボンド社が 2002 年 2 月から 3 月にかけて行った調査によると、注文から決済までをすべてインターネット上で行っているサイトは、全サイトの 3 割に満たないという結果になった。現在、インターネット上での決済の主流はクレジットカードだが、総務省が行った「インターネット利用者が電子商取引を行う際に感じる不安」に関する Web アンケート調査の結果においても、回答者の 77.7%の人が「クレジットカード番号や個人情報が第三者に盗まれないか」を挙げており、消費者はクレジットカード情報をインターネット上に送信することに強いためらいを持っていると言える。

決済に関する消費者の不安を解消するためには、通信経路に暗号化を施しクレジットカード情報の盗聴を防ぐことと、収集したデータにも暗号化などの適切な処置を施し、適切な場所に保管する体制が必要である。通信経路での情報漏洩を防ぐために、クレジットカード情報をインターネットで送信せずに決済を行う方法も開発されている。三井住友銀行・UFJ 銀行・スルガ銀行などでは、決済をクレジットカードではなく口座引き落としで行う「ネットデビット」を提供している。このサービスでは、決済に使用する情報は消費者と銀行間で暗号化された上で通信されるため、オンラインショップには個人情報が届かない。また、既に取引のある銀行を使用するため、面倒な手続きが不要で利便性に富んでいる。

クレジットカードの盗用を懸念しているのは消費者だけではない。インターネット上でのクレジットカード詐欺が発生した場合、被害額を負担することになるのは小売業者であり、最も大きな被害を受ける。GartnerG2 が販売業者を対象に行った調査によると、2001 年においては、クレジットカード詐欺の被害で約 7 億ドルが回収できなかったという。これはオンライン売上全体の 1.14%にあたるが、同時期の実店舗の販売ではこの割合は 0.06%だったことから、オンラインショッピングにおいては、クレジットカード詐欺の被害が 10 倍以上あることになる。また、販売業者は平均で 5%のクレジットカード決済を「疑わしい取引」として拒否しており、自社製品とサービスの 25%以上をオンラインで扱っている大手業者の場合では、7%の決済を拒否している。

被害が一定額を超えた場合、クレジットカード会社は、その業者のカード決済を停止できるため、小売店にとっては、決済の過程でクレジットカード情報の暴露、盗難があった場合のイメージダウンと被害額の支払いが懸念事項となる。

実在の店舗でカードを見せて署名をする対面取引と異なり、オンラインショッピングでは非対面取引となるため、正規のカード会員であることの確認が必要と

なる。クレジットカード大手の米ビザ・インターナショナルは、既存の決済システムを改良して、電子商取引の安全性を高める試み「Visa Authenticated Payment」(VAP)に取り組んでいる。VAP システムを導入した電子商取引業者は、カード発行元の銀行にリアルタイムに情報を照会し、カードの持ち主の存在有無が確認できるため、偽の決済を行う危険性を回避できる。VAP システムを導入しても、消費者がクレジットカード番号をインターネットで入力することには変わりはないが、こちらもクレジットカード情報は消費者と銀行間のみで通信され、ショッピングサイトには、本人であることが確認されたという情報のみが送信されて決済が完了する。この仕組みによって、消費者はカード情報を守ることができ、小売店は認証精度が向上によってなりすましによるカードの不正利用被害を回避し、銀行は顧客に対してセキュリティ強化をアピールできる。日本においても、ビザ・インターナショナルとビザ系の主要カード会社 7 社が、インターネット決済における本人認証を行うサービス「VISA 認証サービス」(Verified by Visa)を 2002 年度中に開始することで合意しており、2002 年 7 月末にディーシーカードがサービスを開始している。

新たな認証システムの登場や、今後インターネットビジネスがより発展するという見通しから、決済サービス市場は今後大規模に拡大するものと予測されている。2001 年度の決済サービス市場規模は、300 億円、2002 年度には、600 億円市場に倍増し、2006 年度の市場規模は 1,700～2,300 億円になると推計される。

クレジットカード情報などを適切に取り扱っているショッピングサイトが存在しているにもかかわらず、一部の情報漏洩事件が消費者に余計な不安を与える結果となっている。消費者が抱いているクレジットカード情報漏洩の不安を解消し、信頼に転換するための確実な情報が不足しているのが原因のひとつと言える。消費者がこのような懸念からインターネットビジネスに消極的になっていることが、インターネットビジネスの発展を妨げていることは確実である。また、消費者の意欲を活発化させるためには、安全性だけでなく利便性を追求することが必要となる。各社が安全なオンライン決済方法を導入することは重要だが、ショッピングサイト毎に決済の種類が多様になると反対に利便性に欠け、消費者の混乱を招きかねないため、規格の統一が求められる。

e. 安全性の主張

e-1. プライバシーポリシーの明確化

オンラインショッピングサイトや製品のユーザ登録といった個人情報を収集する Web サイトでは、そのサイトが個人情報をどのように保護して運用するかとい

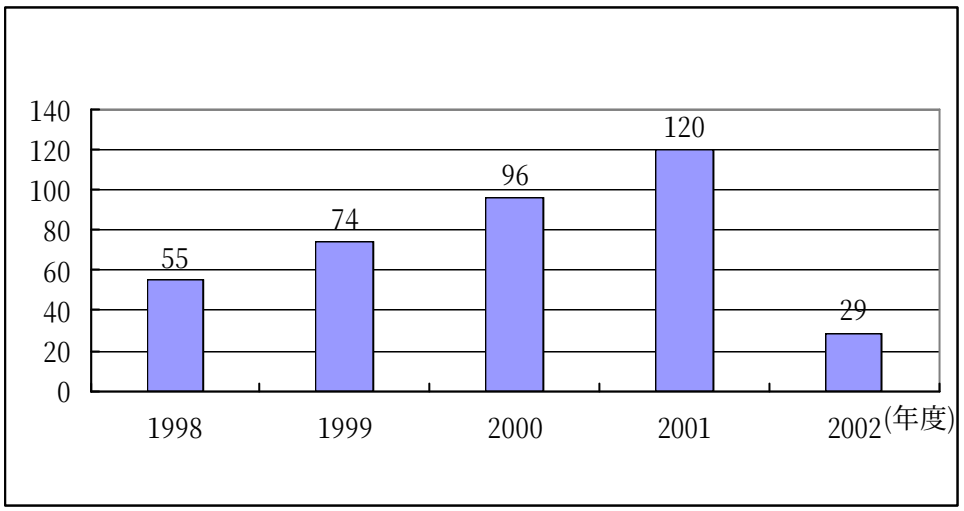
った方針をプライバシーポリシーとして公表している。米 Harris Interactive が、米国の成人 1,529 人を対象に、企業の個人情報の取り扱いに対する消費者の意識調査を行った結果、84%の消費者は、企業はプライバシーポリシーについて第三者による検査を受ける義務があると考えており、62%の消費者が、そのような検査が行われた場合は安心であると考えている。また、91%の消費者が、検査を受けた企業との取引を増やすと回答しており、83%の消費者が、企業が個人情報を誤用したとわかった場合にはその企業との取引を一切やめると回答している。プライバシーポリシーの明記のみでなく、そのプライバシーポリシーが検査を受けていることを併記することで、消費者に対する効果が高くなることが分かる。

e-2. プライバシーマーク制度の認定取得

プライバシーマーク制度は、個人情報保護 JIS に適合したコンプライアンス・プログラムを整備し個人情報の取り扱いを適切に行っている事業者を、第三者機関である財団法人日本情報処理開発協会(JIPDEC)及び JIPDEC に指定された機関が評価･認定し、事業者に対して個人情報の保護に関する信頼獲得へ意欲を向けさせる制度である。この制度は 2000 年 4 月より制定され、認定された事業者はその証としてプライバシーマークと称するロゴを使用することができる。

企業がプライバシーマーク制度に認定されている場合には、Web サイト上のプライバシーポリシーにその旨の記述がなされているため、消費者はプライバシーマークを確認することで、その企業が個人情報を適切に取扱っているかを容易に判断できるようになる。プライバシーマークを明示することで、その企業は第三者機関によってプライバシーポリシーが監査、認定されていることになるため、消費者が個人情報を自分で守るという意識の向上を図ることが可能になり、先のアンケート結果からも、消費者がその Web サイトを信頼に足ると判断することがわかる。

プライバシーマーク認定数(2002 年 7 月)



(出典) プライバシーマーク®制度

http://privacymark.jp/seminar/pms-cp.pdf

内閣府の国民生活局消費者企画課は、オンラインショッピングにおけるトラブル増加に対応するために、消費者に分かりやすい画面表示を行うよう、「特定商取引に関する法律」で義務付けている。また、事業者に対してオンラインショッピングに関係する規制の周知徹底を行うとともに、官公庁がインターネットを介して電子商取引サイトを見て回り、法令を守って運用を行っているかを点検する「インターネットサーフデイ」の拡充を図り、情報収集と法執行体制の強化に取り組んでいる。

インターネットビジネスに関するトラブルを未然に防止し、消費者が安心して取引を行うためには、インターネット上の取引で発生しやすいトラブルの性質とその回避方法、また実際に被害にあった場合の対処法などを消費者に正しく理解してもらう必要がある。これらは自治体や各地の消費生活センターなどが、一般的な脅威やプライバシーポリシー、プライバシーマーク制度などのトレーニングを開催し、情報提供を行うことによって実現できるだろう。

電子商取引推進協議会では、電子商取引を営む事業者に対して求められる個人情報の適切な取り扱いについて具体的に解説したハンドブック「個人情報保護ガイド」を公表している。このようなガイドに従って、適切に個人情報を取り扱い、その姿勢を前面に主張していくことが必要である。

2001 年 7 月に産業技術総合研究所のセキュリティ研究グループが行った調査論文によると、多数の電子商取引サイトでクロスサイトスクリプティングの脆弱性が発

見されている。オンラインマーク取得サイトでも 84%、プライバシーマーク取得サイトでも 68%のサイトに脆弱性が発見された。オンラインマークはサイトそのものの安全性を保証するものではないが、プライバシーマークは「個人情報の取り扱いが適切である」ことを証明するものであるため、取得サイトでこのような脆弱性が発見されたということは、認証の方法に不備があるものと考えられ、この点も改善される必要がある。

(2) 法制度の整備

インターネットにおける通信、取引を安全なものにするためには、企業の自助努力だけでなく、個人情報の保護や著作権の保護などを含めた法整備が必要となる。政府が発表した e-Japan 構想を実現するためには、技術の進化と、利用者のモラルやリテラシーといった人間的な面、また、個人情報や著作権の保護と法的な面の整備が必要になる。以下に、インターネットビジネスに深く関わってくる「不正アクセス」「認証」「個人情報保護」「著作権」に関する法律について説明する。

a. 不正アクセス行為の禁止等に関する法律

「不正アクセス行為の禁止等に関する法律」(以下、「不正アクセス禁止法」という)は、他人の ID やパスワードを無断で使用したり、OS やソフトウェアのセキュリティ上の欠陥を悪用したりして、本来、利用する権利のないコンピュータを使用する行為を禁止した法律である。警察庁、郵政省(現総務省)、通産省(現経済産業省)が共同でまとめ、1999 年に国会において可決・成立した。一部を除き 2000 年 2 月から施行されている。

不正アクセス禁止法の施行によって、以下の行為は犯罪に相当し、罰則として 1 年以下の懲役または 50 万円以下の罰金を科されることになる。

- 人の ID・パスワードを奪取・盗用してなりすましを行い、アクセス認証を通過する
- なりすまし以外の攻撃手法を用いて、認証サーバをだまし、目標の端末を利用可能にする
- 目標の端末の属するネットワークのゲートウェイ端末のアクセス認証をだまして、その内部ネットワークで目的の端末を利用可能にする

また、ID やパスワードなどの認証情報を、第三者に漏らす行為も「不正アクセスを助長する行為」として犯罪となり、30 万円以下の罰金刑となる。

さらに、本法律では、システム管理者は担当するシステムが不正アクセスを受けないように、常に適切な防御や管理措置を講じなければならないことが努力義務として

規定されている。

b. 電子署名および認証業務に関する法律

2001 年 4 月に「電子署名および認証業務に関する法律」(以下、「電子署名法」という)が施行され、電子署名はインターネットにおいて法的に本人を証明するものとなった。電子署名法では一定の条件を満たした電子署名を電子的データ全般に付属させることで、それらのデータが署名者の意志に基づいて作成されたものであると推定されることを定めている。電子署名は電磁的に記録できる情報について行われる措置で、以下の要件に該当するものを指す。

・当該情報が電子署名を行った者の本人性を確認することができるものであること ・当該情報について改変が行われていないかどうかを確認することができるものであること

電子署名法においては、認証機関の運営主体を民間に任せることも規定されている。認証機関になるには、安全・信頼性に関する必要最小限の要件を満たし、主務大臣に「特定認証業務」の認定を受ける必要がある。認証機関は、認証業務の安全・信頼性を維持し、利用者保護を遂行するために、以下の義務を負う。

・業務に関する帳簿書類の作成・保存義務 ・利用者の真偽の確認に関する情報の目的外使用の禁止 ・主務大臣による報告徴収および立入検査などを受ける義務

このほか、外国の認証事業者などに関する取り扱いについても規定されており、多くの諸外国で認定制度が導入されていく中で、日本の認証機関が海外でも通用するために、海外の制度との相互認証を視野に入れた制度とすることも目的としている。

b-1. GPKI

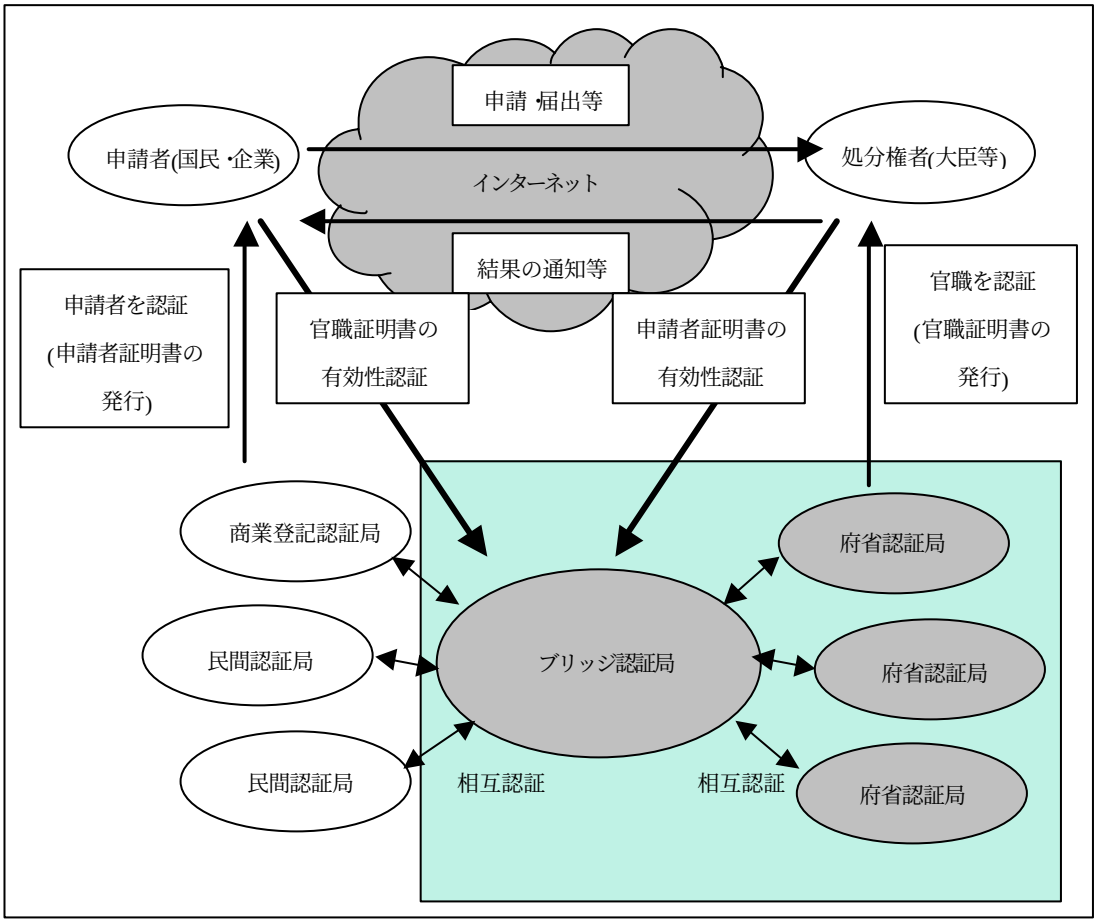
この電子署名法と密接な関係にある GPKI は、Government Public Key Infrastructure の略であり、政府が運営する PKI である。GPKI としてのシステムの範囲は、「ブリッジ認証局」と各省庁が運営する「府省認証局」の 2 つで構成される。それぞれは以下の役割を担っている。

ブリッジ認証局は、府省認証局と民間認証局等が相互に認証する際の仲介を行い、府省認証局と民間認証局とが個別に相互認証する煩雑さを解消するものである。また、民間認証局などが発行する、申請者の公開鍵証明書である「申請者証明書」の有効性検証機能を各府省に対して提供し、政府認証基盤全体の効率的な

構築・運用を可能にする。

府省認証局は、処分権者である大臣などの官職証明書を発行する。これによって、申請者に対する結果の通知等の作成者が処分権者であり、結果の通知などの内容が改ざんされていないことを証明する。なお、申請者に対しては、商業登記認証局や民間認証局から申請者証明書が発行される。

GPKI の仕組みと構成



(参照)　http://www.gpki.go.jp/documents/gpki.html

ブリッジ認証局と行政機関認証局によって実現する GPKI だが、これらは、2001 年 4 月の電子署名法の施行に伴い、実際の運営が始まっている。今後、GPKI のブリッジ認証局と相互接続を取る形で、自治体や民間の認証局が設置されていき、一般の申請者は、それぞれの認証局から証明書を入手することで電子署名を使用し、これまで紙ベースで行ってきた各種届け出や申請などといった諸手続きをオンラインで行えるようになる。

GPKI においては、証明書の配布方法や保管、紛失時の扱いなどが適切に行われるかなど、問題点は多い。また、オンラインでやり取りを行った場合、これまで窓口で徴収してきた手数料をどのように回収するかといった問題や、リテラシーの不足によるデジタルディバイドなど、解決しなければならない課題も多い。

c. 個人情報保護法

個人情報保護法は、個人情報の本人の意図しない不正な流用や、個人情報を扱う事業者のデータ管理を徹底するために、一定数以上の個人情報を取り扱う事業者を対象に義務を課す法律である。2002 年の時点ではまだ施行されていないが、2 年後をめどに施行される見通しとなっている。

個人情報保護法は、第二章で基本原則が記述されており、「個人情報が個人の人格尊重の理念の下に慎重に取り扱われるべきものであることにかんがみ、個人情報を取り扱う者は、次条から第八条までに規定する基本原則にのっとり、個人情報の適正な取扱いに努めなければならない」としている。

個人情報保護法の原則	
利用方法による制限 (第四条)	個人情報は、その利用の目的が明確にされるとともに、当該目的の達成に必要な範囲内で取り扱われなければならない。
適正な取得(第五条)	個人情報は、適法かつ適正な方法で取得されなければならない。
正確性の確保(第六条)	個人情報は、その利用の目的の達成に必要な範囲内で正確かつ最新の内容に保たれなければならない。
安全性の確保(第七条)	個人情報の取扱いに当たっては、漏えい、滅失又はき損の防止その他の安全管理のために必要かつ適切な措置が講じられるよう配慮されなければならない。
透明性の確保(第八条)	個人情報の取扱いに当たっては、本人が適切に関与し得るよう配慮されなければならない。

個人情報保護法が施行されると、本人の了解が無い場合の個人情報の流用や売買、譲渡が規制される。また、個人情報を収集しデータベース化する事業者は、個人情報を第三者に提供する際に利用目的を本人に通知し了解を得る必要があり、不正流用防止のための管理を行う義務が発生する。もし、これが守られず、許可なく情報を提供された人の届け出や訴えがあった場合は、事業者に最高で刑罰が科されるという実効性を持つ。この法律により、現在、個人情報の売買などを行っている名簿業者などは、存在自体が完全に否定されることとなる。

ただ、許可なく情報を提供された本人が苦情を訴えでない限り、個人情報保護法は実効性を持たない。また、政府による監査機能がないため、事業者がこの法律に

沿って個人情報を取り扱うかどうかは定かでなく、一概にこの法律によって自分の個人情報が守られるようになるとは言えない。

d. 著作権保護

デジタルコンテンツはコピーが比較的容易であり、海賊版が出回っているのが現状である。代表的な例が、音楽を MP3 で圧縮し、インターネット上で配信するものである。これは、従来のように店舗から物品を盗むわけではないため、消費者側にも罪の意識が生じにくく、インターネット上のコンテンツは無料で入手できるという考えが広まる結果になっている。また、個人情報の漏洩などと同様に、デジタルコンテンツはコピー、配布が非常に容易であることから、著作権も侵害されやすくなる。

不正コピーをされた場合に著作権を主張するための電子透かしや著作権を守るためのコピー防止機能などの技術が開発されており、著作権の主張を行うことができるようになっている。不正コピー防止のためには、このような規制をかける必要があるが、ただ、規制の強化によって、大きなビジネスチャンスであるデジタルメディアを十分に成長させることができないという弊害が生じる可能性もあり、十分な検討が必要である。

(3) 消費者への対策

a. セキュリティの認識の向上

消費者の不安がインターネットビジネスの普及を阻害していることは先述のとおりである。オンラインショッピングなどのインターネットビジネスに参加している消費者のセキュリティの認識は決して高いとは言えず、やみくもに恐れを抱いている消費者もいる。米 Jupiter Media Metrix は、消費者のプライバシーやセキュリティに対する懸念によって、オンライン事業は 2006 年には 245 億ドルの売上を失うと予測している。2001 年の損失は 55 億ドルであるとされており、大幅に損失が拡大している。ただし、消費者の懸念が解消されることで、2006 年のオンライン収入は約 24%増加するとされている。

インターネットビジネスの発展のためには、参加する消費者の側がインターネットにおける脅威を認識する必要がある。自力で安全性を確認することで、トラブルを防ぎ、安全なオンラインショッピングを楽しむことができ、インターネットビジネスの発展につながるため、消費者は自衛のためにできることを行うべきである。

a-1. 暗号化の確認

オンラインショッピングサイトでは、サイトと消費者間でやりとりされる情報

は盗聴や改ざんを避けるために暗号化されなければならない。一般的には、通信の暗号化として SSL が使用されているため、消費者は、自分の情報が通信経路で盗聴されないために、情報を送信する際に、その通信が SSL で守られているかどうかを確認する必要がある。SSL を使用していることを確認するには、Web ページに明記されているか、URL が https になっているか、ブラウザに鍵のマークが表示されているか、といった確認方法があるが、このような確認を行うことで、消費者は少なくとも通信経路での盗聴に対する自己防衛が可能になる。確認を必ず行い、暗号化がなされていないような場合には、送信を控えるなどの自衛策を取るべきである。

a-2. プライバシーポリシーの確認

米 Jupiter Media Metrix が行った調査によると、セキュリティに対して不安を感じている消費者が多いにも関わらず、Web サイトで個人情報を入力する前に Web サイトのプライバシーポリシーを確認しているユーザはわずか 40%であった。また、Web サイトのプライバシーポリシーが分かりやすいと回答したオンラインユーザは 30%のみであった。同調査によると、100 ドル程度の賞金と引き換えに、オンラインショッピングサイトに個人情報を提供しても良いと考えているユーザは 82%にのぼり、少しの利益のために、個人情報を提供してしまうことがわかった。その背景には、自分の個人情報がどのような目的で使用されるかを明確に理解していないことがある。インターネットにおける危険性を理解することなく、サイトにおける個人情報の取り扱いや、有事の際に責任を取る方法の確認をしないまま、やみくもに不安がる消費者が多いことが分かる。

消費者の意識向上は、インターネットビジネスの発展に貢献するが、セキュリティに関する認識は、コンピュータやインターネットの理解の上に培うことができるものであり、消費者の意識を向上させることは非常に困難なことである。セキュリティに対する認識を幅広く啓蒙していくためには、企業内におけるトレーニングの実施、一般消費者に対する行政や自治体からの連絡、教育の実施などの情報発信方法を考案する必要がある。教育を通じて、消費者がインターネットに対する安心感を抱くことで、インターネットビジネスへの参加が増加すれば、企業の収益の増加につながるため、一般消費者の教育は企業のビジネス戦略の一部であると言える。だが、今後恒久的に消費者に教育を続けていくことは現実問題としては難しく、OS ベンダやインフラに携わる企業が、消費者がより安全にインターネットビジネスを楽しめるような土壌を意識して形成していく必要がある。

(4) 今後の動向と課題

a. ネットワークインフラレベルでの対策

DoS 攻撃やスパムメールなど、ネットワークやサーバに負荷をかけるような攻撃に対しては、企業側の努力や対策のみでは対処しきれない。そのような攻撃に対して、サイトの運営を中断させないためには、ISP などのインフラストラクチャ部分での対策やデータセンタでの包括的な取り組みが望まれている。

コンピュータウィルス対策の分野では、近年の電子メールを媒介としたウィルスの蔓延を背景に、多くの ISP が既にウィルス対策サービスを提供している。企業においては、ウィルスゲートウェイの導入が可能だが、個人ユーザは自己判断で、自らの PC にアンチウィルスソフトを導入することになる。近年は、PC の販売時にアンチウィルスソフトがプレインストールされているが、セキュリティの知識のないユーザにとっては、アンチウィルスソフトを適切に運用することは困難であり、常に最新のパターンファイルがインストールされた状態にあるとは限らない。そのため、ISP レベルでウィルスメールを排除することで、ウィルスの感染による蔓延を防ぐことが可能になる。

ただ、このようなサービスにおいても、作業ミスによる不具合が発生する可能性は否定できない。大手 ISP がインターネット接続サービスの会員向けに提供している「メールウィルスチェックサービス」において、運用会社の設定ミスによって、定義ファイルが古いものになっていたため、その期間にメールをやり取りしたサービス利用者が古い定義ファイルでは検出できないウィルスの被害を受けた可能性があるという事件が発生している。このような事例の発生や、ウィルスの感染媒介はメールに限らないことを考慮すると、ISP のサービスだけで自分の PC を守ることはできないが、ISP のサービスを併用することで、ウィルス感染の可能性を減らすことは可能である。

b. サービスプロバイダの活用

インターネットデータセンタや ASP など、企業が自らリソースを所有することなく、サイトを運用できるようなサービスが多く存在している。自社でシステムの運用を確保できない企業は、ASP にアウトソースすることで、良いコストパフォーマンスが得られる。ただ、その場合にどのような基準で ASP を選択するかが課題となるが、この場合は希望するアプリケーションを提供していること以外に、セキュリティを重視するとよい。セキュリティの壁が破られて、サービスが提供できなくなる事態を考えると、企業にとってセキュリティはアプリケーションの機能やパフォーマンスと同様に重要なものとなる。IDC の調査によると、50 社の ASP サービス

のうち、ほぼ 25%のサービスでユーザ認証やウィルス対策、ファイアウォールなどの基本的なセキュリティを提供していないという結果が出ており、一概に ASP といってもセキュリティレベルはさまざまであることがわかる。

ただ、日進月歩の情報セキュリティ分野において、企業が求めているすべてのセキュリティ対策を ASP が行うのは非常に困難なことであり、すべての要望を満たす ASP はあったとしても、非常に高価になることが多い。企業は自サイトのリスクを分析し、重視するセキュリティにバランスよくコストをかけることができるように、日々、情報セキュリティの感覚を意識し、研鑽していく必要がある。

c. 賠償リスクの増加

先に、インターネットビジネスにおける脅威として、なりすましによる被害やシステムの運用を妨げられたことによる損失について述べたが、今後より重要視されてくると考えられているのが、情報漏洩による脅威である。個人情報の漏洩による企業へのダメージは信頼の失墜が挙げられるが、今日では賠償問題に発展し、賠償金を支払うことになる可能性が大きい。

1998 年に京都府宇治市で、同市の宇治市の乳幼児健診システム作成を下請けした情報処理会社のアルバイト従業員が住民基本台帳のデータ約 22 万件をコピーして持ち帰り、名簿会社に売却、インターネット上で情報が売り出された事件があった。この事件では、流出対象となった 3 人が「いつ誰に購入され、どんな目的で利用されるか分からない不安感を生じさせた」として同市に損害賠償を求め訴訟を起こしていたが、2002 年 7 月、大阪最高裁は 1 人あたり 15,000 円、計 45,000 円を支払うことを命じた。

また、2001 年 11 月に米ジフ・デイビス・メディアが、自社サイトでゲーム専門誌の購読プロモーションを行った際に、プログラムのエラーが原因で、プロモーション時に契約した顧客のクレジットカード番号を含む 12,000 件の個人情報が漏洩し、すくなくとも 5 人がクレジットカードを悪用されたという事件があった。この事件では、ニューヨーク州をはじめとする各州が調査を行った結果、ジフ・デイビス・メディア社のサイトでは、データの暗号化やパスワードによる保護、アクセスログの確保などの基本的なセキュリティ対策が行われていなかったことが判明した。2002 年 8 月に、同社は、バーモント、ニューヨーク、カリフォルニア各州の検事総長と和解し、自社システムでのデータ保護のためのセキュリティ対策を施すことに合意した。同社はこの件に関して、自社の過失は一切認めていないが、3 州に調査費用として 10 万ドル、情報が漏洩した顧客のうちの 50 人に対して 1 人 500 ドルずつを支払うことになった。

これらの事件では賠償金の額は情報漏洩の規模に対してあまり大きくないが、情報を漏洩した企業が被害者ではなく加害者として扱われ、賠償責任が生じていることがわかる。これはインターネット上でのプライバシー保護に関する大きな進歩であり、今後は、情報漏洩に対しては実害がなくても賠償責任が生じることは避けられない時代になってくるだろう。ひとりに対する賠償額がさほど高くない場合でも、対象人数が多ければ多いほど総金額は増大し、企業に深刻なダメージを与えることになりかねない。

d. 評価認定制度の普及

企業がインターネットビジネスにおいて取引の安全性や信頼性を確保するためには、対外的に信頼を得ることができる情報セキュリティ対策を実施することが重要である。情報セキュリティ対策は、技術的なセキュリティ対策だけではなく、情報セキュリティポリシーに則り、人間面の運用や管理などのセキュリティ対策を行うことでより有効になるため、企業の経営者はマネジメントに対する視点から問題に取り組む必要がある。

情報セキュリティの取り扱い規格としては、国際的には、英国および国際標準である BS7799 がある。BS7799 は、1995 年に発行された Part1 と、1998 年に発行された Part2 で構成されている。Part1 には情報セキュリティの管理方法がガイドラインとして記述されており、2000 年に ISO/IEC17799 として国際規格化され、発効しており、国内においても JISX5080 として JIS 化されている。Part2 には、情報セキュリティ管理システム仕様が記述されており、2003 年に、国際規格化される見通しである。

IT セキュリティマネジメントに関する標準には、情報セキュリティ管理に対する普遍的、包括的な国際的ガイドラインである「ISO/IEC TR 13335 (GMITS: Guidelines for the Management of IT Security)」や上述の ISO/IEC 17799 などがある。日本においても、これらに対応する標準の策定として情報セキュリティ管理ガイド「ISMS 適合性評価制度」が策定されている。

情報セキュリティへの取り組みは日本においても古くから行われており、ISMS 適合性評価制度以前にも、情報処理サービス業に対して、事業所の設備を中心とする認定制度「情報処理サービス業情報システム安全対策実施事業所認定制度」が 1981 年から設けられていた。この制度は、旧通商産業省(現経済産業省)の大臣認定制度として、20 年間に約 200 社の適合証を登録していたが、近年のインターネットの急速な普及に基づき、世界的なインターネットビジネスが展開されていくにつれて、世界中から信頼を得られる基準が必要になってきたため、この制度を廃止し、2002 年

4 月に新たに ISMS 適合性評価制度が創設された。従来の制度の下では、設備などの物理的な対策に比較的重点が置かれていたが、ISMS 適合性評価制度は、ISMS の観点からの管理策を付加し、設備・運用面に関する基準がバランスよく盛り込まれている。英国の基準をベースにしつつも日本の風土に見合った認証基準となっている。

ISMS 適合性評価制度は 2001 年にパイロット運用が始まり、2002 年 4 月から本格運用が開始された。2002 年 8 月現在で 13 社が認定されている。インターネット上には国境はないため、ISMS 適合性評価制度は、日本のみでなく国際的にも信頼を得られる情報セキュリティ管理に対する第三者適合性評価制度として、日本企業の情報セキュリティレベル全体の向上を図ることを目的としている。また、同制度は、民間主導の第三者認証制度であり、本制度をより広く普及させようという姿勢が表れている。

ISMS の認定取得を希望する事業者は、JIPDEC の指定する審査登録機関に、認定取得にあたっての申請を行い、ISMS に基づく審査と監査を行う。審査機関からの結果報告を受けて、JIPDEC が事業者を認定済み事業者としての登録を行う。

ISMS 適合性評価制度を導入することで、企業は情報セキュリティを実質的な向上とセキュリティを維持する組織体系の確立を図ることができる。情報セキュリティは、システムを安全に構築し、適切なセキュリティポリシーに基づき安全に運用することで確立されるものであり、ISMS 適合性評価の認定を受けることで、より一層の効果が得られる。また、ISMS の導入で、企業内部でのセキュリティの向上だけでなく、取引相手に対する信頼性やサービス品質の向上につながるという利点があり、企業戦略のうえで欠かせない重要な要素と言える。今後、これらの評価認定を受けていることが、電子政府が実現した際の調達基準になっていくものと考えられる。さらに、インターネットに問わず、取引を行う場合に、各取引会社から ISMS 適合性評価認定を受けていることや情報セキュリティ規格に対応した資料作成を要求されることが増加していくものと考えられる。評価認定を受けることは、「第三者の客観的な基準」で認められたことになるため、企業は標準規格の利用に積極的に取り組むべきである。

ISMS 適合性評価制度は、本格始動して間もない。ISMS はセキュリティポリシーを策定し遵守することから始まるが、情報セキュリティのマネジメントコンサルティングの重要性を企業に理解してもらうのは、いまだ困難な状況にある。また、ネームバリューのために、真の目的をないがしろにしたまま認定の取得を目指すことも考えられる。

また、情報システムや製品のセキュリティ評価を実際に行うことは容易なことではない。よく考えられた基準で厳密に詳細な評価を行っても、評価の過程において

評価者の解釈に差異が生じることや、評価者がその評価結果により利益を得るような状況にある場合、その評価結果が疑わしいものになる可能性もある。セキュリティ評価において非常に重要なことは、評価が関係者の利益とは独立に公正に行われること、定められた基準と手法に従い、評価に要求される技術水準に沿って厳密に行われること、他の評価機関や評価者が評価しても同じ結果が得られることである。

企業がハイレベルな情報セキュリティ意識を持ち、積極的にこの制度を取得・活用していくことで、制度自体の浸透と確立を促進していくことが重要である。

ここまで、インターネットビジネスの動向と、インターネットにおける脅威、対策について述べてきた。現実世界では、顧客の個人情報を収集してまとめた資料は、「社外秘」の判が押され、関係者以外が出入りできないところに保管されており、むき出しの状態で会社の入り口の外に放置されたり、「個人情報入れ」などという名札が張られた引出しに保管されたりするようなことはないと考えられる。しかし、インターネット上では、保管ディレクトリの閲覧が許可されている場合や、容易に想像がつく場所に容易に想像がつくファイル名で保管されていることは少なくない。また、電車などの公共の場所で企業の機密情報を大声で話すようなことはないだろうが、インターネットでは暗号化をせずに通信を行うことが多い。一般消費者も日常生活でカードの番号を簡単にアンケートなどに記述することは少ないが、インターネット上では勝手がわからず行ってしまう。

これらの事例が発生する原因は、インターネットを利用したビジネス、サービスの提供を実施している企業や、買い物を行う消費者のセキュリティの認識が低いことにある。これはインターネットがどのようにして実現しているものかわからないといった背景があるものと考えられる。しかし、現実世界でできることはインターネットでもできると考えれば、家も企業も入り口のドアに鍵をかけるように、インターネットビジネスサイトにも鍵や開けるための合言葉や部外者に情報を知られないようにする仕組みが必要であることは容易に想像し得る。インターネットは魔法の手段ではないため、新しいビジネスを始める際に、あいまいな戦略のまま会社やサービスを興してみても行き着く先は袋小路である。

ネットバブルの崩壊によるサイトの撤退や倒産、経済の低迷、個人情報漏洩事件などインターネットビジネスに対して逡巡する材料は非常に多い。しかし現在でも多くの企業がインターネットビジネス分野で発展を続けている。BtoB では参加する企業が安全性を主張し、BtoC では消費者が安全であることの証明を相手企業に要求し続けることで、情報セキュリティに対する認識が向上し、インターネットビジネスの安全性

や信頼性が向上していくものと考えられる。また企業が主体となって法の整備を要求していく必要がある。セキュリティの認識を高く持った市場では、悪徳業者やセキュリティ対策が十分でないサイトは淘汰されていく。

日本は元来、性善説を重んじる傾向が強いが、そのような認識ではセキュリティは確保できない。インターネットの特徴はボーダレス、タイムレスであることであり、どこの国からどのような攻撃がされるか予測はつかない。日本のインターネットビジネスが発展するためには、安全と信頼を確保すべく、いかにセキュリティの認識を成長させていけるかが今後の課題となるだろう。

参考資料

第 2 章

(a) **総務省「通信利用動向調査」**

http://www.soumu.go.jp/s-news/2002/pdf/020521_1_01.pdf

(b) NUA --- How Many Online?

http://www.nua.com/surveys/how_many_online/world.html

(c) **総務省「平成 14 年版 情報通信白書」**

http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h14/index.html

(d) **総務省「DSL 普及状況公開ページ」**

http://www.soumu.go.jp/joho_tsusin/whatsnew/dsl/index.html

(e) IDC Japan **株式会社「国内 xSP 市場におけるユーザー実態調査を発表」**

http://www.idcjapan.co.jp/Press/Current/20020214Apr.html

(f) **ガートナージャパンが発表した日本市場規模予測**

http://www.gartner.co.jp/press/pr20020718.html

(g) **総務省「平成 13 年版 情報通信白書」**

http://www.soumu.go.jp/hakusyo/tsushin/h13/index.htm

(h) **野村総合研究所**

http://www.nri.co.jp/report/itnavi2006/pdf/itnavi2006_10.pdf

(i) **総務省「平成 13 年事業所・企業統計調査概数集計による電子商取引の状況」**

http://www.pref.hokkaido.jp/skikaku/sk-kctki/deta/tokusu/h13gi/jig.htm

(j) **大田花き**

http://www.otakaki.co.jp/

(k) **あぐりぷらっと**

http://www.e-agri.co.jp/

(l) **フィッシュオンライン**

http://www.fishonline.jp/

(m) **スイサンドンヤドットコム**

http://suisandonya.foods.co.jp/

(n) **アイフィッシュ**

http://www.ifish.co.jp/index.jsp

(o) CMNet

http://www.cmnetcorp.com/

(p) **とりりおんコミュニティ**

http://www.trillioncommunity.com/

(q) **コンストラクション・イーシー・ドットコム**

http://www.construction-ec.com/visitor/v_top/index.html

(r) マツダ「Web Tune Factory」

http://www.w-tune.com/home.html

(s) マイボイスコム

http://www.myvoice.co.jp/voice/enquete/4204/index.html

(t) 電通 「金融ビッグバン」に関する意識や行動について

http://www.dentsu.co.jp/marketing/bigbang/index.html#05

(u) 株式会社 大京

http://www.daikyo.co.jp/news/2002/20020422.html

(v) CtoC 不動産

http://www.ctoc2103.com/

(w) 国内線ドットコム

https://www.kokunaisen.com/counter/reservation/index.jsp

(x) 九州 IT's(いつ)バス

http://road.qsr.mlit.go.jp/itsbus/

(y) 矢野経済研究所 「インターネット電話／IP 電話市場の調査結果」

http://www.yano.co.jp/press/2002/020510b.htm

(z) BB フォン 一時迂回のお知らせ

http://www.bbtec.net/information.php?mode=Show&code=44

第 3 章

(a) 総務省 「平成 13 年 通信利用動向調査報告書 企業編」

http://www.johotsusintokei.soumu.go.jp/public/data2/HR200100_002.pdf

(b) 商工中金 「中小企業のインターネットの利用等に関する調査[2001 年 8 月調査]」

http://www.shokochukin.go.jp/pdf/cb2001jyoho.pdf

(c) イーシー リサーチ株式会社「国内電子商取引（e コマース）市場の 2001 年の売上金額は 17 兆 7,099 億円で、対前年 103.6%成長との予測を発表」

http://www.ec-r.co.jp/press_m/20010516.htm

(d) A NATION ONLINE

http://www.ntia.doc.gov/ntiahome/dn/anationonline2.pdf

(e) Webmergers.com --- Year End Shutdowns Report: Shutdowns More Than Doubled in 2001

http://www.webmergers.com/editorial/article.php?id=49&PHPSESSID=93ed7779995d70d76f74a2ea51991831

(f) Gartner --- Woridwode BtoB Internet Commerce

http://www3.gartner.com/5_about/press_room/pr20010313a.html

(g) eMarketer --- The eCommerce: BtoB Report
http://www.emarketer.com/products/report.php?ecommerce_b2b
(h) 日本経済新聞　8/5 付「電子調達導入でコスト 1910 億ドル減 ? A.T. カーニー、147 社調査」
(i) The Boston Consulting Group --- BCG Research Reveals that U.S. E-Marketplace Revenues to Approach $9 Billion in 2005
http://www.bcg.com/media_center/media_press_release_subpage28.asp
(j) ABC Magazine「韓国の電子商取引・その実態と課題」
http://www.wiaps.waseda.ac.jp/user/iwamura/abcmagazine/news/02061703.html
(k) 電子商取引推進協議会　「「海外における電子商取引　推進状況に関する調査報告書 2001」を発表」
http://www.ecom.or.jp/press/20020528/20020528_kokusai.html
(l) IDG Japan 「中国が世界貿易機関（WTO）加盟で電子商取引に弾み」
http://www.computerworld.jp/contents/free/200112/20011210reseach.html
(m) Jupiter MMXI --- Europe's Online B-to-B Winners
http://uk.jupitermmxi.com/xp/uk/press/releases/pr_021201.xml
(n) Line56.com --- Europe B2Bec to hit $1.4 trillion
http://www.line56.com/articles/default.asp?NewsID=2137
(o) eMarketer --- The eCommerce: BtoC Report
http://www.emarketer.com/products/report.php?ecommerce_b2c
(p) IDC --- Asia/Pacific eCommerce Solutions Market Still Hot After Dot-com Burst, Says IDC
http://www.idc.com/getdoc.jhtml?containerId=pr2002_06_04_174012
(q) The Boston Consulting Group --- BCG Reports 100 Percent Growth in Online Business-to-Consumer Revenues in Asia-Pacific This Year, Reaching Close to U.S.$14 Billion
http://www.bcg.com/media_center/media_press_release_subpage48.asp
(r) RHK --- Asia-Pacific Leads the World in DSL Subscriber Growth and Network Build-outs, According to RHK
http://www.rhk.com/pressrelease.asp?id=155
(s) eMarketer --- Europe E-Commerce: B2B & B2C
http://www.emarketer.com/products/report.php?2000105
(t) IDG Japan 「米国を追い抜いた西ヨーロッパのインターネット利用者数」
http://www.computerworld.jp/contents/free/200201/20020108res.html

第 4 章

(a) 警察庁 「個人情報の流出事案に関する対策について」
http://www.npa.go.jp/hightech/notice/privacy.htm
(b) IPA 「2002 年第 2 四半期[4 月～6 月]不正アクセス届出状況」
http://www.ipa.go.jp/security/crack_report/20020726/02q2.html
(c) CERT/CC --- Number of incidents reported
http://www.cert.org/stats/cert_stats.html
(d) 情報処理振興事業協会 セキュリティセンター「コンピュータウイルスに関する届出について」
http://www.ipa.go.jp/security/
(e) 情報処理振興事業協会 セキュリティセンター「コンピュータウイルス被害状況調査結果要約」
http://www.ipa.go.jp/security/txt/attach/2002_04-1.html
(f) 総務省「情報セキュリティ対策の状況調査結果」
http://www.soumu.go.jp/s-news/2002/pdf/020509_2_1.pdf
(g) Cahners In-Stat Group --- "Always On" Broadband Drives Demand for Consumer Internet Security: Firewall Sales Lead Growth
http://www.instat.com/pr/2001/rc0107hn_pr.htm
(h) KPMG ビジネスアシュアランス株式会社「第 1 回 グローバル情報セキュリティ調査結果(抄訳)」
http://www.kpmg.or.jp/interactive/press_20020501j.pdf
(i) Computer Security Institute --- Cyber crime bleeds U.S. corporations, survey shows;financial losses from attacks climb for third year in a row
http://www.gocsi.com/press/20020407.html
(j) NPO 日本ネットワークセキュリティ協会 「情報セキュリティ被害調査ワーキンググループ活動発表」
http://www.jnsa.org/nsf2002/pdf/C9.pdf
(k) 情報処理振興事業協会セキュリティセンター「情報セキュリティビジネスに関する調査」
http://www.ipa.go.jp/security/fy12/report/sec_biz.pdf
(l) Cahners In-Stat Group --- "Always On" Broadband Drives Demand for Consumer Internet Security: Firewall Sales Lead Growth
http://www.instat.com/pr/2001/rc0107hn_pr.htm
(m) 株式会社シー・エス・イー「ブラウザによるセキュアなユーザ認証」
http://www.cseltd.co.jp/security/release/020624securematrix_pre.htm

(n) 総務省「電子認証ビジネス市場規模調査の結果」
http://www.soumu.go.jp/s-news/2002/020412_2.html
(o) スリーコムジャパン株式会社 「3Com® Embedded Firewall」
http://www.3com.co.jp/products/security/

第 5 章

(a) Testing Iris and Face Recognition in a Personnel Identification Application
http://www.aclu.org/issues/privacy/FINAL_1_Final_Steve_King.pdf
(b) 横浜国立大学大学院 「週刊バイオ 第 33 号 」
http://www.mackport.co.jp/WEEKLY-BIO/bio033/bio033.htm
(c) 国民生活センター「消費生活相談にみる 2001 年の 10 大項目」
http://www.kokusen.go.jp/cgi-bin/byteserver.pl/pdf/n-20011205_3.pdf
(d) イーシーリサーチ株式会社(ECR)「ブロードバンドインターネットの個人利用者アンケート調査結果を発表」
http://www.ec-r.co.jp/press/index.htm
(e) Consumer WebWatch --- A Matter of Trust: What Users Want From Web Sites
http://www.consumerwebwatch.org/news/1_abstract.htm
(f) Cyber Security Management 2002 JULY vol.3 no.33
(g) Harris Interactive --- First Major Post-9/11 Privacy Survey Finds Consumers Demanding Companies Do More To Protect Privacy; Public Wants Company Privacy Policies To Be Independently Verified
http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=429
(h) Gartner --- GartnerG2 Says 2001 Online Fraud Losses Were 19 Times as High as Offline Fraud Losses
http://security1.gartner.com/story.php.id.252.s.1.jsp
(i) プライバシーマーク®制度「2002 プライバシーマークセミナー資料」
http://privacymark.jp/seminar/pms-cp.pdf
(j) 警察庁「不正アクセス行為は処罰されます！」
http://www.npa.go.jp/hightech/fusei_ac1/main.htm
(k) 消費者の窓「消費者行政の推進について」
http://www.consumer.go.jp/kankeihourei/hogo/32hogo.html
(l) 産業技術総合研究所「クロスサイトスクリプティング攻撃に対する電子商取引サイトの脆弱さの実態とその対策」
http://securit.etl.go.jp/research/paper/css2001-takagi-dist.pdf
(m) 経済産業省「電子署名及び認証業務に関する法律」
http://www.meti.go.jp/policy/netsecurity/digitalsign-law.htm

(n) **政府認証基盤**(GPKI)

http://www.gpki.go.jp/

(o) **首相官邸ホームページ「個人情報の保護に関する法律案 」**

http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/

(p) Jupiter Media Metrix --- Seventy Percent Of US Consumers Worry About Online Privacy, But Few Take Protective Action, Reports Jupiter Media Metrix

http://www.jmm.com/xp/jmm/press/2002/pr_060302.xml

(q) **電子商取引推進協議会 「個人情報保護ガイド」**

http://www.ecom.or.jp/protection/guidebook/index.html

(r) IDC --- Twenty-Five Percent of ASPs Have Sub-Par Security, IDC Survey Reveals

http://www.idc.com/getdoc.jhtml?containerId=pr2002_02_13_111513

付録

1：2002 年以降の個人情報漏洩事件

1 月 31 日	静岡朝日テレビ	番組への意見などをメールで寄せた視聴者約 1,900 人に対し担当者が会員制サイトの案内メールを送った際、ほかの視聴者のアドレスを誤って送信。
2 月 5 日	愛媛 CATV のインターネットサービス	加入者のメールアドレス最大 56 件を、誤って他の加入者に送信。
4 月 30 日	小学館	インターネット上で募集したアンケート応募者(約 800 人)の個人データがネット検索可能。本来は ID とパスワードが必要な検索のための認証設定が外れてしまい、自動的にデータが Google に登録され閲覧可能。
5 月 18 日	日本テレビの関連会社「日本テレビエンタープライズ」	ホームページに寄せられた 242 人分の意見が住所や名前とともに流出。
5 月 18 日	全日空の関連会社「全日空ワールド」	ホームページでパンフレットを請求した約 1,500 人分の住所や名前などが流出。
5 月 25 日	日大のホームページ	通信制大学院の願書を請求した約 1800 人分の名前や住所などが、専門知識があれば外部からアクセス可能な状態になっていた。
5 月 26 日	エステサロンの TBC	アンケートに回答した男女 37,810 人の住所、年齢などのほか電話番号やメールアドレスを含む個人情報データが流出。これらの個人データは、以前から同ディレクトリに保存されており、同ページへのアクセス制限はなされていなかった。
5 月 26 日	TVQ 九州放送	ホームページにあるプレゼントコーナーに登録したユーザ約 280 人分の個人情報(住所、氏名、電話番号、メールアドレス)が、11 時間、閲覧可能。
5 月 29 日	岩手県のホームページ	県の情報公開制度で個人情報を開示請求した 8 人の氏名がホームページで閲覧可能。
6 月 8 日	女性向けホームページ「eコレ!ねっと」	過去 1 年間に懸賞に応募した 1,101 人の応募者の住所や電話番号などが 3 時間にわたって閲覧可能。
6 月 30 日	菓子メーカ「山芳製菓」	キャンペーンに応募した約 1200 人のメールアドレスや名前などの個人情報が、同社のホームページで閲覧可能な状態に。
7 月 3 日	アビバ	同社に Web から講座内容などを問い合わせた 1,225 件と、新卒の就職希望者 374 件など合計 2,093 件。氏名とメールアドレス、電話番号と問い合わせ内容

7 月 8 日	結婚情報誌「ノッツェ」を発行する「結婚情報センター」	PC を通して結婚相手のデータ検索や交際申し込みをする「結婚ナビ」というシステム上の写真 200 枚以上が流出。認証なしでサーバにアクセス可能な状態に。
5 月 27 日	YKK アーキテクチュラルプロダクツ	ホームページで実施したアンケートの回答、約 45,000 件の個人情報のうち、大半が漏洩。
7 月 29 日	関西電力系のインターネット接続サービス業者、ケイ・オプティコム	同社が運営するインターネットカフェ「optic@fe(オプティ・カフェ)」の会員 17,324 人分の個人データが流出。
8 月 19 日	三宅島警察署	「ニフティ」が避難生活に役立ててもらおうと、島民に無料で提供したメールアドレス約 350 人分。
8 月 20 日	東日本ハウス	2001 年 11 月からの約 9 ヶ月間、顧客 398 人の住所、氏名、職業、電話番号、メールアドレスが掲載されたリストが閲覧可能。
8 月 22 日	カバヤ食品	同社ホームページで募集したプレゼントに応募した顧客 3,244 人分の、応募者の住所、氏名、年齢、性別、職業、電話番号、メールアドレスなどの個人データが外部に流出。
8 月 23 日	ブルドックソース	同社のメールマガジンの購読申し込みと、2001 年に実施したプレゼント付き企画に応募した約 45,000 人分のメールアドレス、名前、住所、性別、誕生日、職業を含む個人情報が流出。
8 月 24 日	金印わさび	プレゼントに応募した人の住所、氏名など個人情報リスト約 1,200 人分が、同社のホームページで閲覧可能。
8 月 27 日	学育舎のホームページ「教育ジャングル」	アンケートに回答した人の住所や氏名、学歴、メールアドレスを含む個人情報 426 人分が流出。

2：2000 年以降のクレジットカード情報漏洩

2000 年 5 月 1 日	米セールスゲート・コム SalesGate.com	クレジットカード番号などを含む約 2,000 件の個人情報データが盗難。
2000 年 12 月 12 日	Creditcards.com	サイトが不正アクセスされ、55,000 件以上のクレジットカード番号が公開された。
2001 年 6 月 22 日	イギリス消費者協会の運営するサイト Which? Web Trader	プログラムの不具合が原因で、「TaxCalc」という税務ソフトを購入した膨大な数の消費者のクレジットカード番号が外部に公開。
2001 年 11 月 19 日	ジフ・デイビス・メディア社	12,500 人の雑誌購読者の個人情報をウェブサイトに掲示。
2001 年 11 月 20 日	米プレイボーイ誌運営サイト Playboy.com	サイトが不正アクセスを受け、顧客のクレジットカード番号が盗難。
2001 年 12 月 22 日	コンピュータや家電製品のオンライン販売 Egghead.com	不正アクセスによって 360 万人に上る顧客のクレジットカード情報が盗難の可能性。

2002 年 6 月 16 日	コンピュータ関連製品のオンライン販売サイト ComputerHQ.com	JavaScript プログラムにおけるミスが原因で、同サイトを利用した多くの顧客のクレジットカード番号を含む個人情報 15,000 件以上が、過去 1 年間にわたって漏洩。

不正アクセス禁止法違反

2000 年 7 月 12 日	ソフトウェアを使用して、他人の ID とパスワードを入手し、プロバイダに不正にアクセスを行い、販売目的で向精神薬などを所持していたとして無職の男性が逮捕される。
2000 年 8 月 29 日	電話帳に掲載されている携帯電話の番号からパスワードを推測し、転送サービスを勝手に設定した上、コレクトコールを用いて NTT ドコモ九州から 43,000 円を騙し取ったとして無職の男性が逮捕される。
2000 年 8 月 31 日	伝言サービス会社の元経営者の男性が、他人の携帯電話にかかった電話を勝手に自分の電話に転送するように設定し、伝言サービスを用いて知り合った女性と交際。伝言サービス料 67,200 円の支払いを逃れたとして逮捕される。
2000 年 11 月 23 日	開設したホームページを通じて知り合い、不正アクセスの方法を教え合うなどしていた会社員と大学生の 3 人が逮捕される。3 人はインターネットを通じて国立大学のコンピュータなどに侵入し、パスワードを盗んだうえ、同大学の学生が開いたホームページのデータ部分に不正アクセスを行った。また、新潟県湯沢町内の観光協会のホームページに侵入、ホームページの内容やパスワードの書き換えなどを行った。
2000 年 11 月 27 日	知り合いの会社役員の ID とパスワードを使ってインターネット上のオークションに参加した、として元ロックバンドのメンバーが逮捕される。
2001 年 5 月 17 日	携帯電話を使って大阪府の主婦がインターネット上に開設した人生相談のホームページを閲覧し、不正入手したパスワードなどを利用して相談内容などを盗み見た疑いで大学生が逮捕される。
2001 年 7 月 11 日	インターネットカフェの PC を使用して、学習塾のホームページが開設されているプロバイダのサーバに侵入し、ホームページの背景画像をわいせつ画像に書き換えた疑いで、元学習塾の職員を逮捕。
2001 年 9 月 27 日	掲示板「２ちゃんねる」に書き込まれた ID とパスワードを無断に使用し、オークションを利用した会社員 6 人を逮捕。
2001 年 12 月 3 日	インターネット上でゲームサイトを開設している男性の ID とパスワードを不正に利用し、ゲームのデータを書き換えた 13 歳の少年を児童相談所に通告。
2001 年 8 月 9 日	同じプロバイダに所属する友人女性の ID とパスワードを不正に利用し、その女性のメールの盗み見を行った会社員の女性を逮捕。
2001 年 12 月 25 日	22 歳の男子学生が同サークルに所属する女子学生の電子メールのＩＤ（識別符号）などを勝手に入力し、学内の認証サーバに接続。就職内定辞退のメールを大手自動車メーカーに出したとして逮捕。
2002 年 5 月 30 日	宇宙開発事業団で超高速インターネット衛星の製造を受注した NEC 東芝スペースシステムの社員が、事業団のコンピューターシステムに不正侵入し、ライバル企業の機密情報を入手したとして逮捕。

索引

A

B

C

D

E

F

G

I

P

S

X

あ

い

お

か

き

く

こ

さ

し

も