

---

---

# ネットビジネスにおけるセキュリティについて

株式会社 さくら銀行

---

## 執筆者 Profile



阪 章 伸

1991年 (株) 太陽神戸三井銀行 (現さくら銀行) 入行。  
主に開発環境・開発支援ツールを担当。  
アプリケーション開発, オープン系サーバ管理,  
ネットワーク管理, リスク管理にも従事。



魚 木 正

1989年 (株) 三井銀行 (現さくら銀行) 入行。  
情報系システムや自動機システムなどを担当。  
現在, テレホン・バンキングやブラウザ・バン  
キングに関する業務に従事。

## 論文要旨

近年, インターネットは急速に発展・浸透しており, 社会的インフラとして認知される程にまで普及・成長している。これに伴い, 企業はインターネットを利用したビジネス (ネットビジネス) を展開している。ネットビジネス自体も急速に展開しているものであるため, 企業側におけるセキュリティの考え方や意識は, 企業によって大きな格差がある。欧米と比較した場合, 残念なことに日本企業はセキュリティに関するレベルが低いと言われている。

本論文ではネットビジネスにおける脅威とセキュリティの重要性について整理しその具体的な対応策や技術動向をまとめる。

本論文がセキュリティについての考え方や意識を高めるための動機づけとなることにより, ネットビジネスにおけるセキュリティレベル向上の一助となれば幸いである。

## 論文目次

<b>1 . はじめに</b> .....	《 3 》
1 . 1 インターネットの利用者の増大	
1 . 2 ネットビジネスについて	
<b>2 . 目的</b> .....	《 4 》
<b>3 . 背景と現状の問題点</b> .....	《 4 》
3 . 1 背景	
3 . 1 . 1 ネットワーク	
3 . 1 . 2 電子商取引に関する法整備について	
3 . 1 . 3 消費者向けの国内電子商取引市場の動向について	
3 . 2 現状の問題点	
<b>4 . ネットビジネスを支えるITについて</b> .....	《 6 》
4 . 1 ネットビジネス展開に必要な要素	
4 . 2 ネットビジネスに利用されるITの現状	
<b>5 . ネットビジネスにおけるセキュリティの重要性について</b> .....	《 8 》
5 . 1 B to Bにおけるセキュリティの重要性	
5 . 2 B to Cにおけるセキュリティの重要性	
<b>6 . セキュリティ技術について</b> .....	《 10 》
<b>7 . まとめ</b> .....	《 10 》
<b>8 . おわりに</b> .....	《 11 》

## 図表一覧

図5 - 1 インターネットで考慮すべき脅威 .....	《 8 》
図8 - 1 ネットビジネスと電子商取引の関係 .....	《 11 》

## 1. はじめに

近年、インターネットは急速に発展・浸透しており、社会的インフラとして認知される程にまで普及・成長している。これに伴い、企業はビジネスにおける変革とマーケットを求めて「インターネットを利用したビジネス」(以下「ネットビジネス」と言う)を展開している。

### 1.1 インターネットの利用者の増大

インターネットの利用者数は、これまで急激な勢いで増加してきており、現在もなお増加し続けている。米国においては、パソコンの高い普及率と安価なネットワークコスト、それに消費者のニーズにあわせたビジネスが多数展開されていることが牽引して、インターネットの利用者は既に8,000万人以上に達している。(参考：日本経済新聞) 今後、TVをインターネットに繋げるWEB-TVの普及によりインターネット人口は更に増加すると言われている。

一方、日本においてもインターネットの利用者は2,000万人近くに達している。(参考：アクセスメディアインターナショナル) 日本の特徴としては、iモードに代表される携帯電話によるモバイル・インターネットの利用が爆発的に増えていることである。例えば、ドコモのiモード契約数は平成12年5月23日現在で696万契約を突破している。今後もこの傾向は続く見通しである。

米国と日本を比較してみると年齢層毎の利用割合が大きく異なることが報告されている。日本では21歳～34歳の割合が高く10代や50歳以上は意外と少ない。米国では逆に50歳以上の利用者が多く、10代の利用者も比較的多い。米国がインターネット利用に関する先進国であることを勘案すると、日本においても今後は50歳以上の利用者が増加すると予測できる。(参考：日本経済新聞) 利用年齢層が高くなれば、平均所得の上昇によりマーケット価値は急激に増加し、企業にとってネットビジネスは非常に重要なものとなる。

### 1.2 ネットビジネスについて

近年、インターネットを利用したビジネスの拡大スピードはとても早く、また多岐のバリエーションに富んでいる。従来環境下での発想では考えられないようなビジネスが、いろいろな業界で展開されている。

例えば、既存の商品のみを扱っている場合でもネットワークを利用したスピードやポイントサービス等の付加価値を付けたサービスなどで差別化を図っているもの、逆オークションなどのような既存のチャンネルでは考えられなかった新しい販売方法を編み出しているものなどがある。概観すると、電子的にやり取りが可能になったことを前提としたスピードの向上・個々のニーズへの対応の差などをうたい文句にしているものが数多く出現している。

ネットワークを利用した取引では、そのウェブサイトの作りやレガシー・システムとの連携機能、取扱い商品の多さや斬新なビジネスモデルなどが脚光を浴びることが多い。しかしながら、これらのサイトを支える重要な要素として、本人認証・取引の安全性確保といったセキュリティに関する技術が必要であることを十分認識しなければならない。

## 2. 目的

本論文では、ネットビジネスへ参入している企業あるいは参入を検討している企業の経営者及び技術系の担当者を対象とし、そのネットビジネス展開における考慮点として重要なセキュリティにスポットをあて、その技術的動向を見通しその適用方法について論じた。本論文により、セキュリティについての考え方や意識を高めるための動機づけとなり、ネットビジネスにおけるセキュリティレベル向上の一助となれば幸いである。

## 3. 背景と現状の問題点

### 3.1 背景

ネットビジネスの背景として、ネットワーク、電子商取引に関する法整備、消費者向けの国内電子商取引市場の動向についてまとめた。

#### 3.1.1 ネットワーク

1980年代までは、企業の商取引に関してコンピュータの介在する部分あるいはネットワークは、企業内の限られた範囲や閉じていた。多くの環境では、大型の汎用コンピュータと呼ばれる機器をコンピュータ・センタに設置し、それを中心とした利用端末が各地に分散配備されていた。利用者はその端末設置場所に出向き、オペレーションを行って取引を実現した。また、一部の先進的ユーザは、ミニコンあるいはPCを繋ぎ合わせたネットワークを構築して、クライアント・サーバ(C/S)によるシステムを構築・利用し始めていた。しかし、既にこの頃にはアメリカを舞台として、今日脚光を浴びているTCP/IPをベースとしたネットワークが稼動しており、研究室を中心としてオープン・ネットワークを利用した仕組みが存在していた。

1990年代に入って、PCの処理能力が飛躍的に高まり、ネットワークの価値が認知されはじめ、それを利用したC/Sシステムが多く構築され始めた。

その後、Webを利用した文書閲覧のシステムとその利用ソフト(Webブラウザ)としてモザイクが開発されたことにより、爆発的なインターネットの利用拡大が今日まで続いていることは周知の事実である。この仕組みを利用して、単なる文書閲覧から情報共有そして電子商取引の基盤としてWebブラウザとWebサーバの位置付けが拡大してきているのである。

#### 3.1.2 電子商取引に関する法整備について

これまで、ネットビジネスを取り巻く関連法の整備が遅れていることが問題とされてきた。特に、日本における電子商取引に関する法整備の遅れが問題視されてきた経緯にある。しかし、本年5月24日電子署名・認証法が衆議院で可決され、2001年4月1日から施行されることが決定した。この法律により、電子署名は現行の署名・押印と同じ法的効力を持つものとなる。また、電子署名には、その電子署名が本人のものであることを証明する第三者、つまり電子認証業務が必要不可欠である。電子署名・認証法によると、この電子認証業務を行う事業者には国が認定する認定事業者と国の認定がない事業者の両方が認められているだけでなく、法的効力としては同じものとして扱うこととしている。つまり、電子商取引が広く普及する為に、取引の重要性と手数料コストを比較して利用者が選択できることを可能にしている。

### 3.1.3 消費者向けの国内電子商取引市場の動向について

通産省の所管団体である電子商取引実証推進協議会（ECOM）とアンダーセンコンサルティングの発表によると、B to C（企業と消費者との取引）の日本国内市場規模は、1999年では3360億円であった。また、今後もこの市場は拡大する見通しであり、2000年には7730億円（130%増）、2004年には6兆6620億円にまで達するとの予測を発表している。ここでは、オンライン証券取引などに代表される「ネット完結型」と不動産取引などに代表される「ネット非完結型」の両方が含まれた数字である。

また、最近の企業アンケートによれば、B to B（企業間取引）に取り組んでいる企業が39%、今後二年以内に開始する企業が28%となっている。さらにそこでは、B to Cについても2001年度中には58%の企業が何らかの開始を予定しているとの結果が示されている。

### 3.2 現状の問題点

上記に述べた背景を十分認識したうえで、日本におけるネットビジネスの直面する問題点を検討し、下記の4項目にまとめた。

#### ネットワーク利用コストの高さ

米国などに比べて、日本のネットワーク維持コストはかなり割高となっている。例えば、個人がインターネット・サービス・プロバイダ（ISP）を利用することを考えてみると、日本でもISP自身の利用費用がここ数年で劇的に安くかつ固定料金化、あるいは上限設定ありの形態となった。しかしながら、アクセスポイントまで接続するのにかかる電話料金は、米国での市内固定費用と比較すると、日本でのほとんどが従量での課金となっており、特に日中は固定費用となっているものはない。現に、この電話料金が米国との通商関係の課題にまで持ちあがっており、日々の動向から目が離せない状況となっている。

また、この結果によっては、法人が利用している専用線の維持コストにも低価格化が波及してくることも考えられる。

#### 周辺の法的整備の遅れ

最近ようやく電子署名・商取引法が成立し、来年の4月から施行されることになったが、例えば課税の有無や適用される税率と言った税制の問題について、明確になっていくスピードが米国と比較して遅いと言われている。現状においてネットビジネスを開始した場合、後になって法的あるいは金銭的な縛りが発生する危険性がある。そうなると、そういったリスクを侵してまでネットビジネスを始める価値があるのかどうかを考慮しなくてはならず、日本におけるネットビジネスの盛り上がりにも水をさすことにもなりかねない。また、米国でも議論になっているが、インターネットにおける取引に対して、国家的に規制をかけるべきか、あるいは自由競争とすべきかといったことに関しても、日本では未だ議論の種も見えて来ていないのが現状である。今後、ネットビジネスの先進国に遅れをとらない法整備・規制方針の進展を期待したい。

#### デジタル・ディバイドについて

ネットワークの利用が前提となってビジネスが拡大していくと、ネットワークへの通信手段と通信に関する知識や技術を「持つ者」と「持たざる者」との格差が拡大してくる。

この格差を「デジタル・ディバイド」として認知し、米国では公共の図書館などにアクセスできる環境を用意するなどして、インターネットを利用可能とする環境をできるだけ多くの人に提供しようとしている。即ち、社会のインフラとしてインターネットを位置づけており、すべての人が利用できるように是正する努力が見える。

日本では、iモードといった携帯電話を利用した商取引の環境は米国より進んではいるものの、PCベースの環境については「持つ者」と「持たざる者」の格差を是正する手立ては今のところ見えてきていない。

#### セキュリティに関する認識の低さ

日本の治安維持に関しては、世界の国々の中でもかなりレベルが高いことは確かである。それに慣れてしまっているためかもしれないが、日本ではセキュリティに関する意識が低く、インターネットでの取引に限ってみても、最近データの盗難や破壊といったニュースを目にすることが多い。

技術が進歩しても、その技術を理解しその必要性を認識し採用することがなければ、安全からはかけ離れてしまうのである。今後、欧米と同じくらいにまで、セキュリティに対する認識が高まり具体的な対策が講じられることを期待したい。

本論文では、上記で挙げた4つの問題点のうち、「セキュリティに関する認識の低さ」に論点を絞り込むこととした。

## 4. ネットビジネスを支えるIT (Information Technology) について

### 4.1 ネットビジネス展開に必要な要素

ネットビジネスを実現・展開する為には3つの要素が必要であると考えられる。

1つめは、実現しようとする『ビジネス・モデル』である。

これが明確に定義できていないと、実現する機能について、どこまで、どのようにするかという判断ができないことになる。単にネットワークを利用した注文受付システムを作りたいのか、オークションによる競争入札システムを提供するのかといった『ビジネス・モデル』のコンセプトをきちんと定義していることが必要であろう。

2つめは、ポリシー（例えばセキュリティ・ポリシー）の規定である。

どこまでの機能を想定してビジネスを実現するかを考えた場合、ポリシーの規定は重要となる。特にセキュリティに関するポリシーの規定は必須となろう。

3つめは、利用すべきIT（情報技術）の選択である。

ネットビジネスの実現の中核を支えるのはITである。又、同じビジネスモデルを実現するためにも、選択すべきITが異なれば、実現のしかたや運用方法も変わってくる。

以降は、このITの現状とその将来性を探ってみたい。

### 4.2 ネットビジネスに利用されるITの現状

最近のITは、いずれもネットワークに関連したあるいはネットワークを前提とした技術に立脚したものが多く。

ネットビジネスでの利用が想定される、重要な技術についてまとめた。

## Java言語及びJava環境

Java言語は既に発表から5年程度を経て成熟してきており、最近では、Java言語自体よりも、Javaをいろいろな形態に応用したJava環境に注目が集まっている。ここでは、最近特に注目を集めているJava環境について述べる。

- JSP (Java Server Pages)  
JSPとは、Webサーバから提供するページを動的に構成する技術のことである。この技術によって、Webページにデータベースからデータをリアルタイムに取り込んで表示するようなことが可能になった。  
Microsoft社のASP (Active Server Page) やフリーソフトのPHP (HTMLファイルへの埋込型のスクリプト言語) などでも同様のことが可能である。しかし、JSPのメリットにはJava言語の文法に準拠し、Javaで作成したサーブレットを呼び出せることにある。
- Servlet (サーブレット)  
Servletとは、サーバ側で実行するサーバ用のJavaプログラムのことである。このサーバ用のプログラムも一度作成すればJavaの実行環境さえあれば容易に移植が可能である。また、CGIプログラムのように要求の都度プロセスを起動することなく、処理量の増加に対応したスケーラビリティも確保されている。
- EJB (Enterprise Java Beans)  
EJBとは、Javaで記述されたサーバでのコンポーネント群のことである。このようなコンポーネントを利用すれば、業務処理を実現するためにプログラムを一から作成せずに、コンポーネントを組み合わせることによって実現が可能となる。開発のスピードや高品質を維持するには有効な技法である。

Java言語を応用したこれらの技術は、基本的にJava言語のもつ特色を継承しているので、堅牢性やネットワークとの親和性などに優れている。

## XML (eXtensible Markup Language)

XMLとは、SGMLのサブセットとしてW3C (World Wide Web Consortium) にて規定されたマークアップ言語である。

XMLを利用すれば、構造化されたデータをテキストで表現することが可能なので、システム間のデータ交換に共通の定義として利用することができる。今まで、システム間のデータ交換にファイルのレイアウトや電文形式を決めるにあたり、変更や追加がある度に関連するシステムに手を入れなければならなかったが、XMLを利用すれば必要な項目を選択できるし、項目追加などにも柔軟に対応が可能となる。又、必ずしも同期をとって変更する必要もなく、開発の平準化も可能となる。

XMLを取り巻く環境の変化は激しく、XMLのデータ構造のまま保存できるデータベースが出てきたり、編集用のツールが充実してきたりと、利用する立場から見ると使いやすい環境になって来ていると言える。

JavaやXMLといった技術は、ネットワークとの親和性を考慮すると、ネットビジネスに適用すべき有力候補であると言える。

## 5. ネットビジネスにおけるセキュリティの重要性について

ネットビジネスを成功させるための条件として、魅力あるWebページ、魅力ある商品・サービス、レスポンス、ポータルサイトから当該Webページへのリンク、セキュリティレベルの高さ、信頼できる企業、簡単さ、便利さなど一言では語れないが、今後はセキュリティレベルの高さが付加価値となり、やがてはセキュリティに無関心な企業はネットビジネス社会では生き残れない時代がくるであろう。

一般的にインターネットの世界における脅威は、従来のビジネスにはないものがある。その脅威を下記図5-1に示す。なりすましとは、正当な利用者になりすますことだけでなく、IPアドレスを偽って正当な端末になりすます、あるいは企業のWebサーバやそのサービスになりすますことも意味する。また、盗聴とは、通信上のやりとりを傍受しその内容を盗み見ることやWebサーバに盗聴用のプログラムを仕掛けて盗聴することである。改ざんとは、通信途中でその内容を不正に書き換えることや不正侵入されてサーバ内のデータを不正に書き換えることである。この他にも、不正アクセス、侵入、破壊などが挙げられる。

ネットビジネスは多種多様であるが、ここでは典型的な例としてビジネス・トゥ・ビジネス（以下B to Bという）およびビジネス・トゥ・コンシューマ（以下B to Cという）を挙げて、それらにおけるセキュリティの重要性について具体的に述べる。

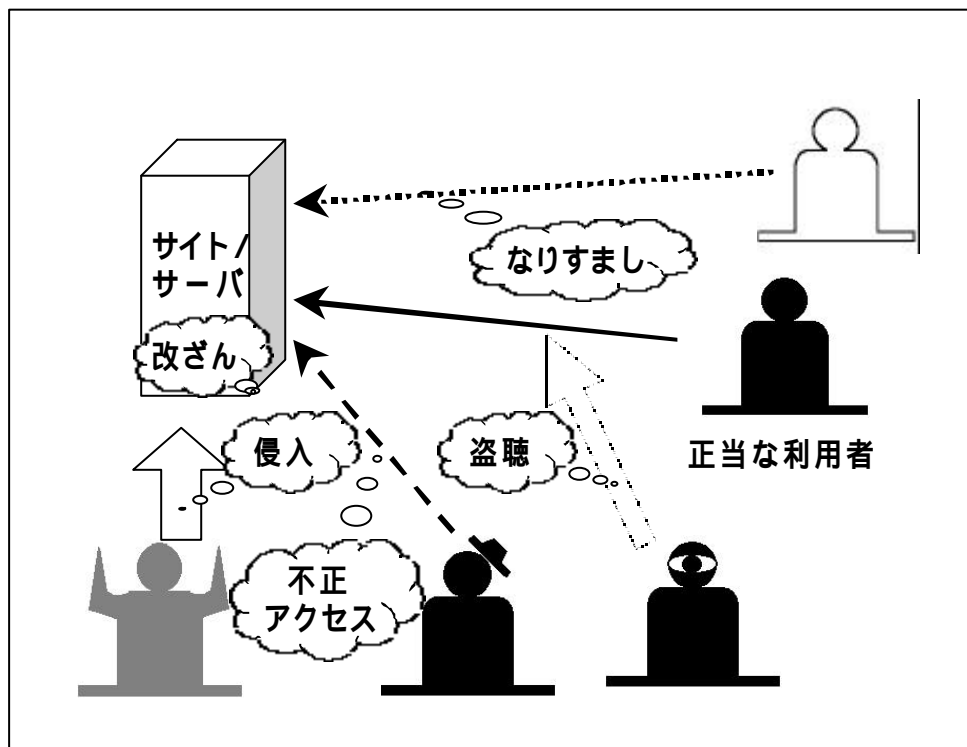


図5-1 インターネットで考慮すべき脅威



### 5.1 B to Bにおけるセキュリティの重要性

B to Bにおいて、BとはBusinessの略であるが、具体的には企業のことである。企業と企業の間でネットビジネスを行う場合、その特徴となるのが、その取り扱い量（注文量）の大きさや金額の大きさである。企業間の取引の場合、突然見知らぬ企業とネット上だけで取引することはなく、既に取引のある企業あるいは有名な企業と取引するのが通常である。しかし、ネットビジネスでは、本当にその企業であるかどうか。つまり「なりすまし」ではないか、正式な注文であり否認されることはないか、注文は改ざんされていないか、企業情報でもある注文内容は盗聴されていないか、それらの情報は流出することはないか、と言った問題をクリアしなければならない。

つまり、これらの問題を解決できるセキュアな企業とは安心してビジネスができるが、セキュアでない企業は敬遠されていくであろう。

一方、企業として発注することを勧奨すると、自社内でのセキュリティレベル向上に取り組む必要がある。つまり、権利を有する者による手続きがなされることを実現しなくてはならない。今後、自社内における認証やワークフローの厳正化と連携強化が必要となるであろう。

最近話題となっているビジネス・トゥ・ガバメント（企業と政府間のやりとり：B to G）についても同様のことが言える。

### 5.2 B to Cにおけるセキュリティの重要性

B to Cにおいては、B to Bと異なり、相手が対等な立場ではない。一般消費者は、企業の提供するサービスやシステムを利用するものであり、一般消費者が自分のセキュリティレベルを向上させる義務はない。また、B to Bと比較すると、個々の取引金額や量は小さい。一般消費者であっても個人認証を実施するために認証機関による証明書を取得するケースも考えられるが、証明書取得コストが無料あるいは安価になって、万人が証明書を容易に取得できるようになるか、あるいは高額取引や経常的な取引を伴う場合でもない限り、わざわざ自分で証明書を取得する一般消費者はいないであろう。つまり、企業側がなんらかの方法で消費者を認証する、あるいは企業側が証明書手数料を負担する必要があるということである。しかしながら、その場限りの取引であれば、法規制を遵守したうえで、決済だけをきちんと確認できれば特に認証などの問題を取りあげなくても良いものもあるであろう。

一方、消費者の立場から考えると、様々な脅威に対する不安がある。例えば、そのWebが本当にその企業のものであるかどうか、そのWebにはどのようなセキュリティ技術を採用しているのか、定期的な監査などセキュリティ上の安全性を維持する管理体制はきちんとしているのか、といったものがあげられる。

企業側はこれらの消費者の不安に対して、きちんと対応できなくてはならない。質問があった場合にその都度回答するという方法ではなく、消費者が常にセキュアであることを認識できるように、Web上に表示しておいたりインタラクションの中で表示することが必要である。セキュアであることは後ろ向きに守ることではない。セキュアであることが戦略であり高いステータスなのである。つまりセキュアであることをアピールすることも重要な戦略である。消費者がセキュアであるということを認識・実感できなければ、どんなにセキュリティレベルを上げてても無意味なのである。今後、セキュアでないと認識される企業は、他の企業だけでなく一般消費者からも敬遠されていくであろう。

## 6. セキュリティ技術について

今後のネットビジネスを展開していくにあたり，セキュリティに関するITをおさえておくことが重要となる．この技術については次の3つの視点から確認することが望ましい．

### ネットワーク上におけるセキュリティ技術

ここでは，基本的にネットワーク上を流れる情報の保護について実装が図られている．Webサーバとクライアントの間を暗号化された通信でデータ保護を図るSSL(Secure Socket Layer)や，インターネットを仮想的にポイント間を結んだ専用線として利用するVPN(Virtual Private Network)などがある．最近のVPN製品は，IP sec(IP secure)という技術でネットワーク上のデータの暗号化をサポートする機能を採用している．また，やり取りするデータを暗号化する公開鍵基盤(PKI:Public Key Infrastructure)などもある．

### サーバ側におけるセキュリティ技術

サーバ側では，どのようなデータがネットワークに流れてよいのか，あるいは誰がサーバにアクセスして良いのかといった観点での保護が行われる．Webサーバへの環境にアクセス可能な利用者のみを通すことができるファイヤーウォールを設置する一方，ネットワークに接続しているルータなどでは，通過可能なデータのみを通すパケットフィルタリングを行う．又，LAN上では不正な侵入に対してネットワークを遮断する侵入検知の仕組みも設定可能である．

最近では，JavaAPIの形式で暗号化アルゴリズムを提供する企業も現われ始めている．

### クライアント側におけるセキュリティ技術

クライアント側では，まずクライアントそのものへのアクセスを制御する必要がある．カードを利用してアクセスのパスワードを発生させたり，ICカード自体をアクセスの鍵としたり，最近ではバイオメトリクスの応用として指紋を鍵として利用する技術も開発され実用化が始まっている．

## 7. まとめ

上記にて述べたとおり，ネットビジネスを展開するうえで必要となるセキュリティ技術は徐々に実現されてきている．目的とするセキュリティレベルを実現・維持するには，それらの技術を選択・適用する必要性がある．実際に技術の導入あるいは製品の購入を行う場合，コストを勘案したうえで採用・不採用を決定するだけでなく，客観的な採択基準に基づき判断することが必要である．つまり，客観的な採択基準とは，上記で述べたセキュリティに関するポリシーあるいはガイドラインであり，セキュリティ技術を選択・適用する局面で考えるべきこと・守るべきものは何かということについて，しっかりとコンセンサスを得たものであることが重要である．

毎日のように，新たなセキュリティ・ホールが発見されたり，それに対する対応策やパッチが配布されたりしている．セキュリティに関する技術に対応していくためには，継続的な情報収集と細めなアップデートが必要不可欠となる．つまり，日頃からいろいろな情

報を収集し、それらの情報の中で自分の関わるネットビジネスに関係があるものかどうかを常に意識しておくことが重要となる。

また、セキュリティを強化していくためには、人的資源を強化する必要がある。自社内に堅牢なシステムを作り上げたとしても、その利用時や運用時などに無防備にしてしまうこともある。つまり、開発・運用部門において専門的な知識を有した人材が必要であることは当然のことであるが、利用部門においてもある程度以上の知識が必要であるということの意味している。万一、中途半端な知識だけしかない利用者がいた場合、仮に不正なことを行っているとしても自分が不正を行っていることが理解できないこともあり得るし、ある不正を行っても管理者がその不正をわからないかもしれないとの誤解から、モラルハザードを起こすこともあり得る。この様に考えると、利用者や運用要員の情報リテラシー教育も非常に重要であることが明確となる。さらには、ある特定の部門に所属しているセキュリティの専門的な知識を有した人材が、運用担当の部門に対して助言やサポートできるといった体制の整備が望まれる。

## 8. おわりに

ネットビジネスとは、本来、電子商取引を包含するものである。つまり、ネットビジネスはビジネスに変革をもたらす戦略的なインターネット活動のことであり、電子商取引はその一部分に過ぎない。ネットビジネスの世界で成功するためには、リーダーシップ、ガバナンス、コンピタンス、テクノロジーが必要であると言われている。

本論文では、ガバナンスの一部、コンピタンスの一部およびテクノロジーの一部について述べる事ができたと認識する。今後のネットビジネスを模索していく中で一助になれば幸いである。

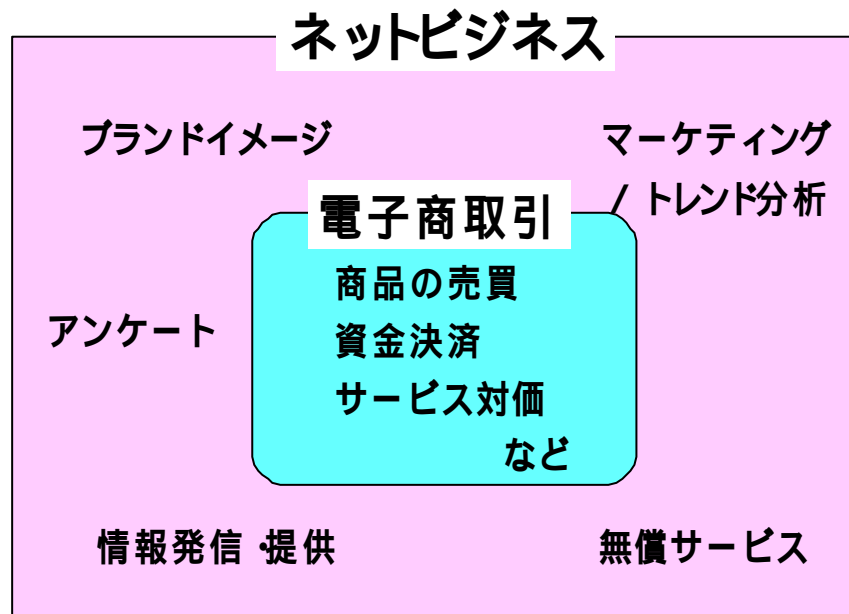


図 8 - 1 ネットビジネスと電子商取引の関係

## 参考文献

- ( 1 ) 米国商務省：デジタル・エコノミー，東洋経済新報社，1999年2月
- ( 2 ) 米国商務省：デジタル・エコノミー ，東洋経済新報社，1999年11月
- ( 3 ) 三輪 信雄：セキュリティポリシーでネットビジネスに勝つ，NTT出版，2000年6月
- ( 4 ) 熊谷 誠治：誰も教えてくれなかったインターネット・セキュリティのしくみ，日経BP社，1999年5月
- ( 5 ) 三輪 信雄：実践！セキュリティ対策，SRC，1999年5月
- ( 6 ) Amir Hartman, John Sifonis, John Kador ( 中野 広道訳 ): ネット・レディ，ソフトバンク・パブリッシング，2000年4月
- ( 7 ) 小林 暢子，高下 義弘，田口 潤：“ インターネット・ビジネス実態調査 ”，日経コンピュータ，7月3日号，( 2000.6 )，p174
- ( 8 ) 増田 晋：“ 電子商取引に不可欠，電子署名・認証法が成立 ”，日経ビジネス，2000年6月19日号，( 2000.6 )，p131
- ( 9 ) 日本証券アナリスト協会：“ N T T ドコモ ”，証券アナリストジャーナル別冊付録，第38巻第6号，( 2000.6 )，p82

## 参考サイト

- ( 1 ) J P C E R T  
<http://www.jpCERT.co.jp/>
- ( 2 ) 日本銀行金融研究所（論文など）  
<http://www.imes.boj.or.jp/>
- ( 3 ) 日経コミュニケーション  
<http://www4.nikkeibp.co.jp/NCC/>
- ( 4 ) 日本経済新聞  
<http://it.nikkei.co.jp/>
- ( 5 ) PC-Gaz  
<http://pcgaz.nikkeibp.co.jp/>
- ( 6 ) 日経オープンシステム  
<http://nos.nikkeibp.co.jp/>
- ( 7 ) 平成12年版通信白書（通商産業省）  
<http://www.mpt.go.jp/policyreports/japanese/papers/h12>