企業における情報セキュリティ

日本大学　法学部　政治経済学科
＃0120232
高木　久仁枝

目次

１．はじめに

1.1　研究のねらい

今日、新聞等で個人情報が漏洩するといった記事を頻繁に目にする。当初は、自分自身が該当者になってしまったら嫌だ、これくらいにしか思わなかった。しかし、ソフトバンク BB！による情報漏洩により、自分自身の個人情報が漏洩してしまい、お見舞い金をもらう対象者になってしまったのだ。その際、情報漏洩、情報セキュリティに興味を持った。

1.2　何をしたいか

現在の企業におけるセキュリティシステムを自分なりの流れで研究し、考察する。その上で、私なりの企業におけるセキュリティシステムを提案したいと思う。

まず、情報セキュリティを研究するにあたり言葉から考えたい。そのため、第 2 章に情報についての章を設け、研究する。次に、その情報の脅威について研究する。そして、情報セキュリティについて調べ、考えることにする。第５章には、事例を挙げ実際に行われている情報セキュリティについて調べる。終章には、この流れを汲み情報セキュリティシステムの提案をしたい。

２．情報とは

情報セキュリティを考えるにあたり、まず「情報」というものは何なのか、を考えたい。そのため、この章で情報についての定義や形について研究する。

2.1　情報とは何か

普段、なにげなく「情報」という言葉を使っている。情報に囲まれているとか、情報が溢れているとか。これは新聞や雑誌、テンビやラジオ、携帯電話やWebページなどの情報メディアが氾濫している状況をいっている。しかし情報とはメディアのことではなく、そこから送り出される内容のことを指している。目や耳から入った「ことがら（知識）」で興味を抱いたり、判断を促したり、行動を起こさせたりする、そうした「ことがら（知識）」を情報といっている。

情報という言葉は英語のinformationの訳語として明治時代に生まれた言葉なのである。当時は特殊な用途での言葉であったと思われるが、現在では日常的に広範囲な場面で頻繁に使用される言葉である。特に70年以降、情報という言葉の使用が増えたようである。「情報」とひとくちでいうが、その使われている意味には４つある。

① 収集される事象（intelligences）
　知識や知性の源となるものである。アメリカのCIA（Central Intelligence Agency）のＩである。スパイが集める情報はこれである。

② 発信される事象（information）
　これは、本来的な意味である。英語のinformationのinformとは「伝える」という動詞である。そのformは元来「形づくる」ことを意味している。理解できる形（form）にすることがインフォメーションである。

③ 蓄積される事象（data）
　すでに日本語にもなっているデータのことである。

④「情報化」という言葉になった時の「情報」
　「情報インフラ」とか「情報通信」とかでも表れる「情報」である。この場合の情報は、デジタルやコンピュータ処理と情報インフラまでもが含まれ、サイバースペースおよびITを指している。この４つめの情報が現在の状況を表わしている。

発信された情報を受信したものが理解してはじめてコミュニケーションは成立するのである。コミュニケーションとは一方通行ではなく、受信者が理解することが重要なのである。現在の情報の多さは単にデータとしての情報が多い状況を指しているにすぎない。膨大なデータから必要とする情報を得るには、わかりやすくコミュニケーションを成立させる必要がある。わかりやすいコミュニケーションのためのデザインが情報デザインなのである。

2.2　情報の定義

情報の定義は長い歴史の間、さまざまな学者がさまざまな定義を唱えてきた。その中の一部ではあるが、下記に表記する。

表　　情報の定義　（出典・(財）電気通信総合研究所 / 名和小太郎 別冊宝島「シンクタンクの仕事術」JICC 出版 95 ページ）

人物名	出典	定義内容
マッハルプ	「知識産業」	「知識」「知られていること」という内容「知っている」という状態、「全ての知識は情報である」
ポラト	「情報経済入門」	組織化され、伝達されるデータ
村上泰亮	「情報と技術の経済分析」より第 1 章情報概念と経済分析	「客観的把握を目指す心的活動によって作り出されるもの/単なる抽象的な内容ではなく、具体的な表現形態を持ち、伝達の経路を経たもの
野口悠紀夫	「情報の経済理論」	（極小のエネルギーで）複製が可能であり、かつ複製された後も、なお同一の状態を保てるようなものについて、その複製された内容である。
小松崎清介	「情報産業」	人間の社会的諸活動を支える意味のある記号系列
マクドノウ	「情報の経済学と経営システム」	特定の状況における価値が評価されたデータ
梅沢忠夫	「放送朝日」（'63.1）掲載論文「情報産業論」	人間と人間の間で伝達される一切の記号系列
加藤秀俊	「情報行動」	環境からの刺激、固体を環境に結ぶもの
北川敏男	「組織と情報」	意味を持つところの秩序ある記号系列
坂本晋	「情報産業社会の演出者」	「コミュニケートする内容」に限定して、「人間精進の創造物」と考える。それは「物的生産物」に対立する概念としての「知的生産物」である。
中野収	「現代人の情報行動」	「メッセージ」「記号」「媒体」の複合体
林雄二郎	「情報化社会」	可能性の選択指定作用を伴う事柄の知らせ
藤竹暁	「現代マスコミュニケーションの理論」	人間の環境適応行動にとって、ある事情について判断を下すための材料となる刺激としてのメッセージ

吉田民人	「今日の社会心理学」シリーズ No.４「社会的コミュニケーション」所収「情報科学の構想」	物質・エネルギーの時間的・空間的・定性的・定量的パターン（パターンとは、「秩序・無秩序」の視覚から捉えられた物質・エネルギーの属性）
ウィーナー	「人間機械論、サイバネティクスと社会」	われわれが外界に適応しようと行動し、また調節行動の結果を外界から感知する際に、我々が外界と交換するものの内容
シャノン	「通信理論」	いま、起こりうる状況として、Z1,Z2,Z3,…Zn が考えられるが、このうちどれが実際に起こるかが、完全に明らかではないものとする。そのとき、この体系は「一定量の不確実性を持っている」というが、この不確実性の量を減らすもの

このように情報をどのように定義するかは、誰もが満足できる統一的な見解は存在しない。しかし、「何らかの現象についての認識」という理解は共通している。物理的であれ概念的であれ、実在の世界において認識された情報が、メディアに固定されて情報空間に投影され、管理され、処理されることが可能となり、何らかの働きを行うことになる。情報はさらに一定の媒体に表現されて、データや知識として資源化情報になるという一連の過程が想定される。このメディアへの固定、変換、使用のいずれの段階も、情報のコミュニケーションが不可欠である。

2.3　情報の形

情報の形はいろいろある。紙に書かれた情報、CD-ROM に入っている情報、ネットワークを流れる情報。この論文自体も情報の１つである。つまり、情報自体には形はなく、アナログ・デジタルなど様々な保存形態がある。それを伝送する形態も色々である。ともに技術の発展によってそのバリエーションが日々多様化している。昔、手紙は郵送であったが、今はパソコンなどを使い e-mail で相手に届けることができる。この以前から現在に至る情報の形態をまとめる。

① 物理的情報

紙などに書かれた物体が存在する情報。

② 電磁的情報

フロッピーディスク、CD-ROM などに収められているデータ。また、パソコン内のハードディスク、送受信した e-mail などのデータ。

③ 人の記憶

仕事のノウハウなどの頭の中に残っている情報。

さらに情報には、様々な性質がある。以下にまとめる。

① データ（Data）

主体が対象（ここでは、具体的対象とともに抽象的対象も含む）を意識的もしくは無意識的に観察・測定することによって得た対象の定量的もしく定性的属性を第 1 次データ（生データ）という。他の主体がもっているデータ、情報、知識の伝達を受けたときこれを第 2 次データという。第 1 次データと第 2 次データをまとめてデータという

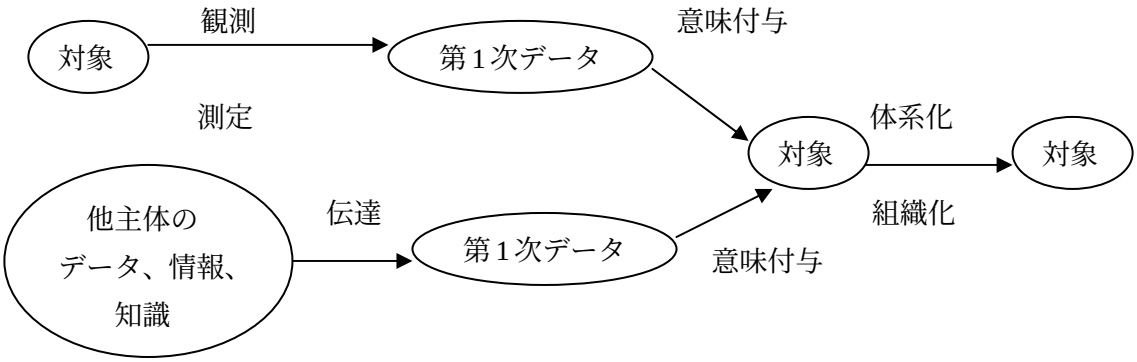
② 情報（Information）

主体がデータに意味を付与したものを情報という。

③ 知識（Knowledge）

主体がより大きな文脈の中で、情報を組織化、体系化したものを知識と呼ぶ。

下記にデータ、情報、知識の３つの間の関係を主体の活動に基づいて定義したものである。



３．情報の脅威

なぜ、情報セキュリティというシステムがあるのか。それは、企業にとって価値ある情報に対する脅威があるからだ。では、脅威とは何か。脅威とは、それに悪意が伴うかどうかによらず、結果として資産に害を及ぼす、発生する可能性のある事象を指す。別の言い方をすれば、脅威とは、資産に対して起こりえる、良くないすべてのことを言う。

「情報の脅威」という言葉を聞けば、ウイルスや不正アクセスが挙げられる。大きな要因である。だが、この論文では詳しく採り上げないが盗難、自然災害も情報の脅威の１つとして挙げることができるので、ここで自然災害について簡単に採り上げる。自然災害には、台風、竜巻、豪雨などあるが、日本にとってより重大な災害は地震である。「地震大国・日本」とも言われるほど頻繁に地震が襲ってくる。情報システム停止、ライフライン（電気など）の停止などの事故、情報資産の破壊、などに対しセキュリティシステムが必要である。

情報の脅威として、以下のものを挙げる。大きく２つにわけて研究していく。

3.1　外的要因

まず１つは、外的要因である。外的要因を「ウイルス」、「不正アクセス」の２つに大きく分け研究しいく。

3.1.1　ウイルス

この節では、コンピュータウイルスについて考える。

2003 年のインターネット白書によるとセキュリティ被害の内容で 1 番多い被害は、ウイルス感染によるものである。全体の 78.4%がウイルスによるもので、ついで 23.9%のワーム系悪質プログラム被害と続いている。

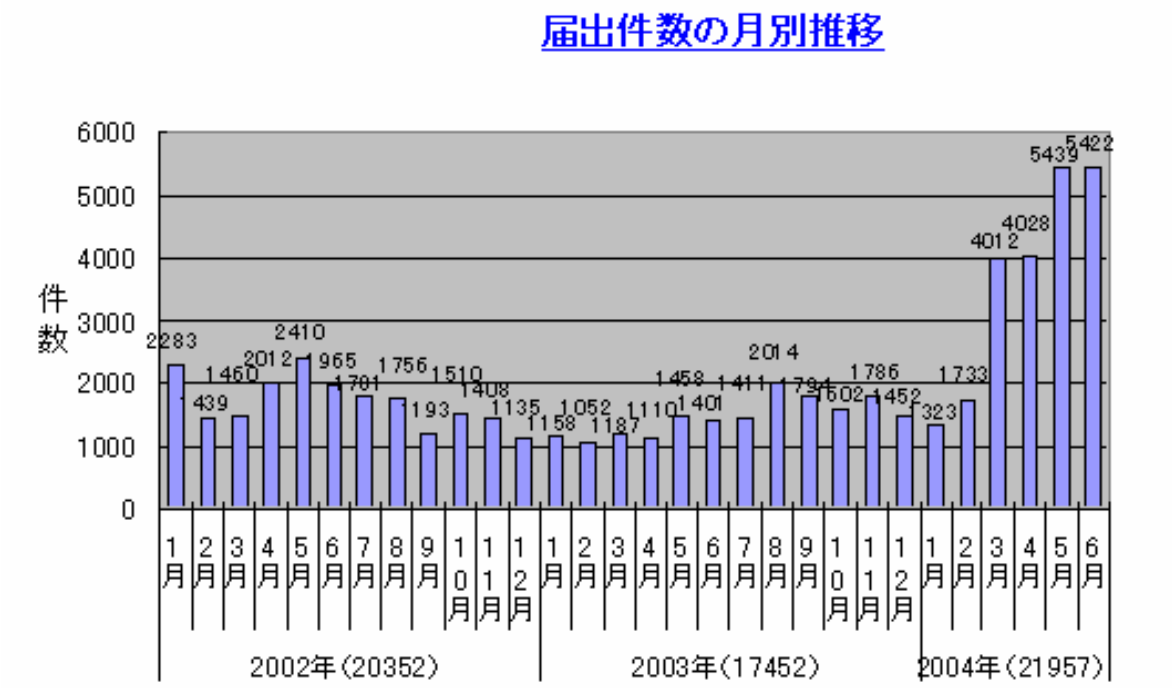
そもそもコンピュータウイルスとは、他のプログラムを書き換えた上、自分自身を複製して自己増殖できるプログラムのことである。1984 年、F・コーエン博士が「自己増殖プログラム」の研究成果を論文として発表したとき、使用したのが「コンピュータウイルス」という言葉である。以後、不正を行うプログラムは総称して「コンピュータウイルス」と呼ばれるようになった。

コンピュータウイルスが初めて発見されたのは 1986 年にパキスタンでの Brain（ブレイン）であった。このウイルスは、パキスタンの青年プログラマが、自分が作ったソフトウェアが不正にコピーされている状況に憤りを感じて作ったものだという。つまり本人は「コンピュータウイルス」ではなく「自己複製技術を応用した不正コピー警告プログラム」を作ったつもりだったのだ。そのため、ウイルスコードの中には「駆除ワクチンが欲しい方はこちらまで連絡されたし」というメッセージと共に電話番号が明記してあったのである。そして、日本で初めてコンピュータウイルスが発見されたのは 1989 年の Japanese Christmas であった。これは、MS-DOS の COM ファイルに付着するウイルスであった。12 月

25 日になると「A merry christmas to you!」というメッセージが表示される。機能としては、自己複製を行うということしか判っていないウイルスが日本で初めてのものであった。

ウイルスの被害調査を行っている情報処理振興事業協会（IPA）の調べによると、1998 年の一年間の被害届 2035 件に対して、2003 年には 17425 件にまで増え、2004 年 6 月末までの段階だけで前年の被害届を上回る 21957 件にまで達した。（下記、図、参照）

図　　（出典・情報処理振興事業協会（IPA）、ホームページより）



このようにウイルスの発生率はインターネット人口に比例する形で増え続けていることが解かる。年間に発見されるウイルスは約 3000 種類。亜種、変種も含めると、現在地球上に存在するコンピュータウイルスは 40000 種にのぼるのではないか、とも言われている。現在では、アンダーグラウンドで出回るウイルス作成ソフトを使って作られるような簡単ないたずらウイルスから、プロのプログラマが作成する被害の大きなウイルスまで、様々な種類のウイルスが続々と誕生しているのが現状である。

それ以来、コンピュータウイルスはネットワークなどといったコンピュータの歴史と共に進化し、より悪質なものへと発達した。この悪質なウイルスの作成者である犯人はプロのプログラマと考えられており、騒ぎを見て楽しんでいるハイテク愉快犯なのではないどろうか。

ここで、通商産業省（現在の経済産業省）が策定したガイドラインに基づき、ウイルスの３つの機能を以下に挙げる。

①　自己伝染機能

これは、自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、 他のシステムに伝染する機能 である。

② 潜伏機能

これは、発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能である。

③ 発病機能

これは、プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能である。

代表的なコンピュータウイルス、トロイの木馬、ワームを例にとってみる。まずトロイの木馬と呼ばれるウイルスは、一見、普通のプログラム（ソフト）のように見える。そして、これが電子メールなどで送られる。そのため受け取った人が、うっかりパソコン（コンピュータシステム）に入れてしまう。あるいは、実行してしまう。すると、そのウイルスが勝手にパソコンの中のプログラムを書き換えたり、データを削除したりする。そして、変なメッセージが出るようになったり、最悪の場合はシステムが壊れたりする。あるいは、あとで不正アクセスの手助けをしたり、ほかのコンピュータを攻撃したりする。語源は、ギリシャの詩人ホメロスの叙事詩に登場する「トロイの木馬」である。ギリシャの兵士が潜んだ木馬を城内に入れたというトロイ戦争の話。ユーザの目を欺いてパソコンに侵入し、あとで被害を与えるという方式が、敵の目を欺いて兵士を送り込み、夜中に中から奇襲攻撃をかけるという作戦と似ている点からである。そしてワームは、さらに自己増殖機能を持った厄介なウイルスである。例えば、電子メールソフトに登録してある電子メールアドレスに、勝手に自分の分身を送る。そのため、次から次へ、アッという間に世界中に被害が広がる。しかも最近は、プレビュー画面に電子メールを表示しただけで感染するタイプが登場して猛威を振るっている。

では、このようなウイルスが企業においてどのような被害をもたらすのか。実際に起こってしまった例では、ウイルスの検知システムをパソコン操作をしているうちに止めてしまい、ウイルスに感染したメールを開けてしまいウイルスに感染。感染したことを知らずに、e-mail を取引会社に送信してしまいウイルス感染をさせてしまった、という例である。幸い、対応が早くウイルス感染の被害は数社で済んだものの謝罪回りをしなければならなかった。このように、コンピュータを頻繁に活用している企業では、複数の者が 1 度ならずウイルスの被害にあっている。中には、フロアのパソコン全てが感染してしまったという例もある。

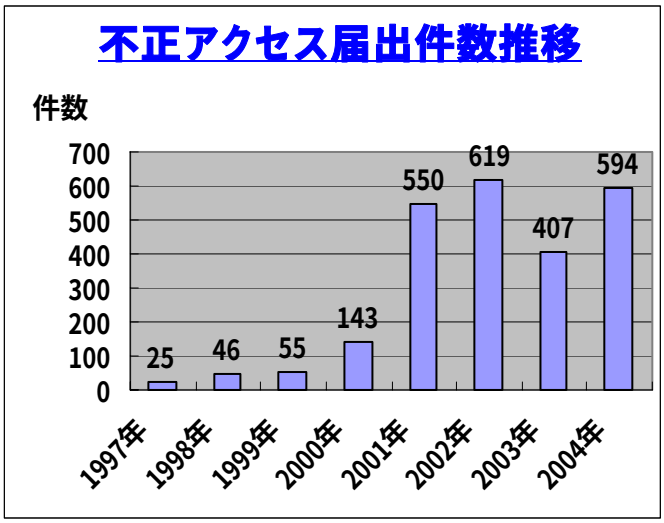
3.1.2 不正アクセス

外的要因のもう１つである、不正アクセスについてである。

最初に不正アクセスの現状は一概に被害件数が増え続けている、というわけではない。

IPA（独立行政法人　情報処理推進機構）によると、2004 年の 1 年間の届出件数は 594 件で、2003 年の届出件数（407 件）と比べて 45.9%増と再び増加に転じたのである。しかし、実被害数は 72 件と、2002 年の 225 件、2003 年の 126 件から更に減少した。（下記、図　　、参照）

図　　（出典・情報処理振興事業協会（IPA）、ホームページより）



届出件数が増加した原因としては、無差別に攻撃が行われることにより企業・個人ユーザ問わず攻撃を受けていることが推測される。そのような状況の中、被害届出が減少した理由としては、企業を中心にセキュリティ対策が普及していることが予測される。

一方、ブラウザのスタートページを書き換えられるなどの被害に関する相談が個人ユーザから多数寄せられており、個人ユーザにおけるセキュリティ対策は不十分であるものと推測されている。

まず不正アクセスとは、制限されている（許可されていない）コンピュータネットワークに接続することである。この不正アクセスに対して定められたものが「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）」である。この法律は、1999 年、国会において可決・成立し、一部を除き 2002 年 2 月から施行された。この法律の目的は電気通信回線を通じて行われる電子計算機に係る犯罪の防止及びアクセス制御機能により実現される電気通信に関する秩序の維持を図り、もって高度情報通信社会の健全な発展に寄与することである。（不正アクセス禁止法・第 1 条より）この法律に基づき、不正アクセスについて考える。

不正アクセス禁止法で禁止している行為は、「不正アクセス行為」と「不正アクセス行為を助長する行為」の２つがある。

① 不正アクセス行為　（罰則・１年以下の懲役又は 50 万円以下の罰金）

不正アクセス行為には２つのものがある。

① なりすまし行為

ネットワークを通じてアクセス制御機能により利用が制限されているコンピュータを利用する場合、ID・パスワード等の識別符号を入力する必要があり、手元のパソコンに入力画面が表示される。ここで、コンピュータの正規の利用者である他人の識別符号(ID・パスワードなど)を無断で入力する行為のことをいう。

② セキュリティ・ホールを攻撃する行為

コンピュータの安全対策上の不備(セキュリティ・ホール)を攻撃して、コンピュータを利用可能にする行為のことをいう。攻撃用プログラム等を用いて特殊なデータを入力し、アクセス制御機能を回避して、識別符号により制限されているコンピュータの機能を利用する行為のことをいう。

② 不正アクセス行為を助長する行為　（罰則・30 万以下の罰金）

不正アクセス行為を助長する行為は、他人の ID、パスワード等の識別符号を無断で第三者に提供する行為がそれにあたる。具体的には、「Aのパソコンは、ID 1234、パスワード 9876 で利用可能になる」など、識別符号の情報を教える行為である。教える方法はホームページ、電子メール、電話等手段は問わない。

上記から分かるように、外部からの不正アクセスには、侵入行為とサービス妨害の 2 種類がある。侵入行為は、事前調査、権限取得、不正実行、後処理の４つの段階を経て行われる、といわれている。

① 事前調査

事前調査とは、クラッカー達がターゲットを見つけた際に侵入の糸口をつかむために、まず、そのシステムについて詳しく調べ、システム情報を収集する。具体的にシステム情報とは、IP アドレス、サーバ名、サーバソフトウェア、OS の種類・バージョン、提供されているサービス、侵入検地システムなどに関する情報である。

② 権限取得

権限取得とは、ツールなどを使用して、パスワードなどを強引に解読し、操作や処理を実行するための権限を不正に取得する。これをパスワードクラッキングという。パスワードクラッキングには、一致する文字列を総当り的に調べるブルーフォース攻撃や、よく使われそうな単語を網羅した辞書を使用して照合する辞書攻撃などがある。

ID やパスワードを不正に入手することで、ユーザ権限を獲得することができる。特に特権ユーザには、情報の読み込み・書き込み・変更・削除などあらゆる操作が許されているので、この権限を奪われると、あらゆる不正行為が可能となる。

③ 不正実行

不正実行とは、実際の不正行為のことをいう。盗聴、改ざん、なりすまし、破壊、不正プログラムの埋め込み、踏み台など、その内容は多岐にわたる。ここで、不正アクセス禁止法に基づく不正行為も含め、一覧にする。

表　　不正行為の種類

不正行為	内容
盗聴	ネットワークを流れるデータや保存されているデータの不正入手。 （例）・パスワードの盗用

	・個人データ（メール、日記など）の盗み見 ・企業データの漏洩
改ざん	データの書き換え。 (例) ・Web ページの改ざん ・設定の書き換え
なりすまし	別の個人を装い、その者のふりをしたさまざまな行為。 （例）・管理者を装ってのユーザのパスワード取得 ・他人のクレジットカード番号によるショッピング
破壊	データやプログラムの削除、ハードディスク（磁気記録）初期化など。
コンピュータの 不正使用	コンピュータの不正使用。 （例）・コンピュータの遠隔地からの操作 ・コンピュータの夜中の自動起動
不正プログラムの 埋め込み	ユーザの知らない間に情報を入手して外部へ送信したり、ファイルを破壊したりするなどの不正プログラムの埋め込み。
踏み台	不正アクセスを行う際の中継地点として、他人のコンピュータを使用。 （例）・アカウントを不正使用し他のサイト攻撃の拠点とする ・スパムメールの中継

④ 後処理

後処理とは、不正行為を行った後、ログの消去などにより、侵入の形跡を消す証拠隠滅工作を行うことをいう。また、次回に侵入するのを用意にするための裏口工作を行う。裏口とは、管理者に気づかれないような侵入経路であり、バックドアともいう。

最後に不正アクセスに関連して、以下の２つのものも挙げる。

① スパイウェア

スパイウェアとは、パソコンを使うユーザの行動や個人情報などを収集したり、マイクロプロセッサの空き時間を借用して計算を行ったりするアプリケーションソフトのことである。得られたデータはマーケティング会社など、スパイウェアの作成元に送られる。

スパイウェアは他のアプリケーションソフトとセットで配布され、インストール時にはそのソフトと一括して利用条件の承諾などを求められる。また、スパイウェアはユーザに気づかれないよう、ウィンドウなどを
出さずにバックグラウンドで動作するため、ユーザはスパイウェアがインストールされていることに気づきにくい。

スパイウェアが行なう活動の内容は、実はインストール時に表示される利用条件の中に書かれているため、インストール時にその利用条件を承諾してしまっている以上、スパイ

ウェアの活動は直ちに違法と言えるものではない。しかし、利用条件をまともに読む人はほとんどいないため、ほとんどのユーザはスパイウェアに気づかず、スパイウェアごとソフトをインストールしてしまう。

このため、スパイウェアは事実上無断で個人情報を収集しているとして、プライバシー擁護団体などの消費者団体を中心に反スパイウェア活動が起こっている。また、スパイウェアは一般ユーザの間でもおおむね不評で、特にパソコンの扱いに慣れ、パソコンの動作を熟知しているユーザほどスパイウェアを嫌悪する傾向がある。

なお、広告を表示する代わりに無料でソフトを利用できるアドウェアというものもあるが、意味の上ではアドウェアとスパイウェアの間に直接関係はない。しかし、アドウェアではユーザに表示する広告を選別するなどの目的で情報収集を行っていることが非常に多く、かなりの割合のアドウェアがスパイウェアの機能を持っている。

実際のスパイウェアの調査結果を下記に表記する。

表　　スパイウェアの調査結果　（出典：Webroot 社，EarthLink 社）

	2004 年 １～３月	2004 年 ４～６月	2004 年 ７～９月	2004 年 １～９月合計
検査したパソコン	703,002	1,368,775	1,148,078	3,219,855
検出したスパイウェア	18,611,344	36,203,219	28,608,222	83,422,785
パソコン１台あたりのスパイウェア	26.5	26.5	25	26

（検出したスパイウェアの内訳）

アドウェア	3,558,595	7,887,557	5,978,018	17,424,170
アドウェア・クッキー	14,799,874	27,868,767	22,327,112	64,995,753
システム・モニター	122,553	210,256	154,878	487,687
トロイの木馬	130,322	236,639	148,214	515,175

このように昨今、スパイウェアの検出、被害が増えている。

② フィッシング（phishing）

フィッシングとは、金融融機関などからの正規のメールや Web サイトを装い、暗証番号やクレジットカード番号などを搾取する詐欺のことである。「釣り」を意味する「fishing」が語源だが、偽装の手法が洗練されている(sophisticated)ことから「phishing」と綴るようになったとする説がある。

2003 年頃からアメリカで見られるようになり、その年の 7 月には、米国連邦取引委員会が、一般ユーザに警告を出しました。日本ではまだ「架空請求メール」が主流ですが、ここにきてフィッシングの脅威が現実のものとして受け止められているのです。

代表的な手口は以下のとおりである。メールの送信者名を金融機関の窓口などのアドレスにしたメールを無差別に送りつけ、本文には個人情報を入力するよう促す案内文と Web ページへのリンクが載っている。リンクをクリックするとその金融機関の正規の Web サイトと、個人情報入力用のポップアップウィンドウが表示される。メインウィンドウに表示されるサイトは「本物」で、ポップアップページは「偽者」である。本物を見て安心したユーザがポップアップに表示された入力フォームに暗証番号やパスワード、クレジットカード番号などの秘密を入力・送信すると、犯人に情報が送信される。

URL に使用される特殊な書式を利用して、あたかも本物のドメインにリンクしているかのように見せたり、ポップアップウィンドウのアドレスバーを非表示にするなど非常に巧妙な手口を利用しており、「釣られる」被害者が続出している。

対応策としては、送信者欄を信用しない、フォームの送受信に SSL が利用されているか確認する、メールに示された連絡方法(リンクなど)以外の正規のものと確認できている電話番号や URL などから案内が本物かどうかを確認する、などが挙げられる。

最近、このフィッシングによる被害が日本でも報告されている。そのため警視庁や各都道府県の警察は、ホームページなどでフィッシングの被害にあわないよう、注意を呼びかけている。

3.2 内的要因

もう１つは、内的要因である。内的要因が個人情報の漏えいの要因になるケースが多い。内的要因とは、企業であれば企業内における事項が原因となった場合である。内的要因を「従業員」、「第三者」の２つに大きく分け研究しいく。

3.2.1 従業員

個人情報漏洩の最大の要因は、従業員である。情報システムが高度に発達するにつれ、コンピュータ制御を前提とした社会となりつつある。コンピュータは、人が組織し操作しているため起こっている事故も多い。そのため、人の管理が重要となる。

まず、コンピュータシステムの事故原因のうち、人が原因となるものには以下のようなことが考えられる。

① ソフトウェアやハードウェアの開発途中のミス
② システム構築上の設計ミス
③ システム運用前の設定ミス
④ 設定やプログラム変更後のリリース時のミス
⑤ 運用時の操作ミス

⑥ システムに関わる者の故意による障害
⑦ システム利用者の操作ミス、ルール違反、妨害
⑧ 許可されていない利用者による妨害

また、さまざまなセキュリティ機器の登場で本来であればリスクが減るはずだが、それを運用し利用する人の管理が不十分であるためにかえってリスクが増大していることがある。

また、社員による不正により、情報が漏洩したケースが多く見られる。そのうち、多いのが社員による社内情報の持ち出しである。増えている理由は２つある。１つは、大量の企業情報が市販の磁気媒体（MO や CD-ROM など）やインターネットを通じて簡単に外部へ持ち出せるようになった点。もう１つが、情報が会社の貴重な財産であるという意識が希薄な社員が多いことである。このため、どのような情報でもノートパソコンに入れて、社員が安易に外部へ持ち出してしまう。また、持ち出した情報の管理もずさんなことが多い。したがって、従業員の管理が重要なのである。

3.2.2 第三者

第三者とは、誰を指すのか。

第三者とは、サービス利用や打ち合わせのための来訪者、納品・配送による訪問者、あるいは警備員、清掃業者などを指す。これらの人々が建物の中に入って、机上に放置されている重要書類を見てしまったり、外部からのネットワーク経由の利用者からパソコンやサーバにアクセスされ機密情報を見られたりする可能性がある。この場合、一般に情報漏洩による信用失墜というリスクが懸念される。JIS X 5080 では、事務所、電算機室、ファイリングキャビネットなどへのアクセスを物理的アクセス、組織のデータベースや情報システムへのアクセスを論理的アクセスと区別している。これらのアクセスに伴うリスクは識別し評価する必要がある。

また、上記の第三者が事務所内で知りえた情報に関する守秘義務は、第三者に対する必須の要求事項である。そのため、契約書に明記することで、情報漏洩に至る行為を未然に防ぐことができる。

情報の取り扱いを他の組織に外部委託する場合、その組織も第三者となる。この外部委託の組織に対しても、情報セキュリティの維持を求める。さらに、その顧客や外部の利害関係者には、情報システムやネットワークあるいはデスクトップ環境において、情報システムやネットワークの管理や制限あるいは制御を外部委託する場合には、当然委託先の組織と外部委託契約を締結することが必要となってくる。

４．情報を守る＝情報セキュリティ

情報を守るための仕組みとしての情報セキュリティをこの章では研究する。今までの章では、情報やその情報の脅威などについて研究してきた。

この章では、企業にとって大切な情報を、脅威からどのように守るか、つまりこれが情報セキュリティだが、この情報セキュリティについて研究していく。

4.1　情報セキュリティとは？

情報セキュリティとは何か。情報セキュリティとは、「正当な権利を持つ個人や組織が、情報や情報システムを意図通りに制御できること」であり、情報セキュリティマネジメントシステムの国際標準である ISO/IEC17799 には、「情報セキュリティとは、機密性（confidentiality）、一貫性（integrity）、可用性（availability）を維持すること」と定義されている。以下にそれぞれの内容を示す。

① 機密性

情報を誰にも見られないように秘密の場所に保管したり、暗号化して、第三者に見られても絶対に理解できない状態にしておくこと。つまり、許可された者が許可された時間内に、許可された権限に従ってアクセスできるようにすることである。

② 一貫性

情報が正確であり、発生してから消去されるまでの間、改ざんや破壊をされることなく、発生時点の状態が完全に維持されていること。さらに、情報が誰によって作成され、その情報がいつ送信、または受信されたかという、情報の発信源を確認できることも含まれる。

③ 可用性

コンピュータシステムのハードウェアが常に効率よく安定して稼動し、大きな障害が発生しても中断することなく利用し続けることができるようにすること。コンピュータシステムが、安定して稼動しなければ機密性や一貫性が確保されているかどうかを確認することはできない。情報セキュリティの根幹であるといっても過言でもない。

情報セキュリティという言葉を聞いて、「情報システムの安全性」や「インターネット取引の安全性」などいうインターネットセキュリティの部分を思い浮かべがちである。しかし、情報セキュリティは本来、人や組織や事業プロセス上のマネジメント要素のことである。

4.2　情報セキュリティの目的

情報化社会では、ハードウェアの故障や自然災害などの確率的に生じるリスクを防御する安全性と、意図的な不正行為や組織的な犯罪行為などの非確率的に生じるリスクを防御するセキュリティとを確保する必要がある。情報化社会では、この 2 つをまとめて「情報セキュリティ」とし、情報システムに対するあらゆる脅威から防御することを目的とする。

情報セキュリティを行う目的のポイントを以下に示す。

① 情報資産を守るため

② 業務を通常通り行うため

③ 顧客からの信頼を獲得するため（失わないため）

④ 競争力を維持・向上させるため

⑤ 収益を維持・向上させるため

⑥ 強い経営体質を作るため

以上のものが情報セキュリティの目的のポイントとなる。要するに、最終的な目的は「経営体質の強化」なのである。

4.3 情報セキュリティの対象

情報セキュリティの対象は、脅威から守るべき「情報資産」である。情報資産とは、ISMSによれば、情報と情報システム、ならびにそれらが正当に保護され機能するために必要な要件の総称である。情報資産とは、情報そのものだけでなく、情報の作成・保存・利用・廃棄等のライフサイクルにおいて、情報を保護するために必要となる環境要素を含めた保護対象資産」と言うことができる。「人の記憶」という形態の情報を守るには、情報を知りうる立場の人間に対し、「情報の価値」「セキュリティ事故の発生による事業への影響」、「情報を守ることに対する個人の利害」などについてきちんと意識付けを行うことが必要である。その意味では、「人」も立派な情報資産であり、意識付けのための「周知」・「教育」・「訓練」等を実施するための環境要素も情報資産と考えることができる。

情報資産の具体例としてよく参考にされる JIS X 5080 5.1.1 資産目録の記述では、「情報システムに関連付けた資産の例と」として以下のものが挙げられている。

① 情報資産

物理的情報、電磁的情報、人の記憶

② ソフトウェア資産

コンピュータシステム上で情報を取り扱う場合のソフトウェア要素

③ 物理的資産

コンピュータシステムの装置設備、通信装置設備、記憶媒体、収納設備など情報を取り扱う環境要素

④ サービス

通信サービスや暖房、照明、電源、空調

ISMS 認証基準でも「情報資産」の取り扱いを規定しているが、こちらは上記の①情報資産だけを指すのではなく、①～④のすべてを指している。JIS X 5080 5.1.1 の例では IT 関連資産を中心に記述されている。

「情報セキュリティ」では、保護対象資産について「網羅性」を強く求められている。この点からも、「情報資産」＝「保護対象」とすると、より適切である。

4.4　情報セキュリティ対策

情報セキュリティ対策として以下の方法を挙げる。

以下は、技術的方法と本質的方法の２つに大きく分けられている。この理由は、インターネットセキュリティなどによる技術を使用して対策を施せる場合と、日ごろから人が意識し、行える対策との２点があると考えたからである。

4.4.1　技術的方法

技術的方法として、個人認証と暗号化の技術について研究する。また、インターネットをする際に守ってくれる技術についても触れていく。

4.4.1.1　個人認証

実社会では、顔をみたり声を聴いたりするなど、本人を判断する材料がたくさんあるが、ネットワークでは電子的なデータの流れしかないため、ユーザが誰であるのか、それが本人であるかどうかを確認する手段は非常に限定される。

そのため、ネットワークに入る際に認証するシステムとして、① アカウント、ID、パスワードによる認証を挙げる。また、建物やネットワークへの出入りの際、より強固なチェックシステムが必要となってきている。そのため、② バイオメトリック認証をもう１つの個人認証システムとして挙げる。

① アカウント、ID、パスワードによる認証

ネットワークやシステム、パソコンへのログインなどは誰にでも利用（アクセス）が認められているわけではない。利用できるユーザを限定するとともに、ユーザの利用できる範囲（権限）を決めなければならない。アカウントとは、この利用権限のことをいう。また ID は、個人を識別するための番号のことである。そして、パスワードは、正しいユーザ（本人）であることを示す証明となる。

そして、ID、パスワードは設置するだけでなく、ユーザに定期的にパスワードを変更することも必要となってくる。

② バイオメトリック認証

バイオメトリック認証とは、人体の特徴に基づいて個人を認証する技術のことである。指紋、声紋、網膜のパターン、虹（こう）彩のパターン、手の大きさのほか、署名をするときのペンの速度や筆圧などを使用するシステムもある。指紋や虹彩のパターンを使う方式の実用性が高く、大規模の実験データで、ほぼ 100%の正しい判定が行われたことが報告されている。

4.4.1.2　暗号化

インターネットはコンピュータの端末を色々な種類の回線でつなぎ合わせただけの仕組みである。そのため、他人に自分のパソコンの中を勝手にいじられる可能性がある。その

ため、暗号化が必要となる。また、暗号化は e-mail の送受信の際にも使用される。

暗号とは、原文の意味を当事者以外には判読できないようにした情報を指す。その際、見て意味の判る元の文のことを「平文」、その文を誰にも理解できない暗号に変える行為を「暗号化」、そして暗号化されたデータを「暗号文」と呼ぶ。さらに、暗号文を元の平文に戻す行為は「複合化」と呼ぶ。

暗号は、大きく分けて「共通鍵暗号」と「公開鍵暗号」の 2 種類がある。公開鍵暗号は、秘密を守るために利用されることに加え、認証にも利用される。

① 共通鍵暗号

共通鍵暗号は、主に秘密を守るために利用され、長い歴史を持つ暗号である。一般に、暗号というと共通鍵暗号を指している場合が多い。

この暗号方式では、簡単に説明すると暗号化する鍵と複合化する鍵が同じであるものを指す。

② 公開鍵暗号

公開鍵暗号は、秘密を守るために利用されることに加え、認証にも利用される。この暗号は、1970 年代後半に誕生した暗号で、暗号化と復号に異なる鍵（公開鍵と秘密鍵）を利用し、「一方の鍵で暗号化すれば、もう一方の鍵でしか復号できない」という特徴を持っている。この特徴をうまく利用し、サイバー空間でも認証を行うこともできる。

この方式では、自分で秘密裏に持つ「秘密鍵」と、世の中の人々に公開してしまう「公開鍵という異なる形の鍵 2 本をペアとして使用する暗号方式である。

公開鍵暗号を行うためには、まず「公開鍵」と「秘密鍵」の「鍵ペア」を作成する。公開鍵で平文を暗号化する場合、その公開鍵とペアの秘密鍵でしかその暗号化文を復号化することができない。要するに、お互いに自分で暗号化したものは相手にしか復号化できないような鍵のペアを作る。その際２つの鍵は、どちらかを使ってもう片方を類推できないように作る必要がある。

鍵ペアを作成したら、インターネット上で交信したい相手に公開鍵を送る。その際、共通鍵暗号方式であれば、鍵を相手に送る途中で第 3 者に盗まれてしまっては大変なことになってしまうが、公開鍵暗号方式の場合には、このプロセスで鍵を盗まれても問題はない。そもそも公開鍵から秘密鍵を類推できないような鍵の作り方わしており、「公開」というほどなので、世の中の皆に配ってしまってもよいのである。

4.4.1.3　ファイアウォール

企業などのネットワークでは、インターネットなどの外部ネットワークを通じて第三者が侵入し、データやプログラムの盗み見・改ざん・破壊などが行なわれることのないように、外部との境界を流れるデータを監視し、不正なアクセスを検出・遮断する必要がある。このような機能を実現するシステムがファイアウォールである。

ファイアウォールとは、直訳すれば「防火壁」であり、組織内のコンピュータネットワークへ外部から侵入されるのを防ぐシステムのことである。また、そのようなシステムが組みこまれたコンピュータのことでもある。多くの場合はソフトウェアの形で提供され、コンピュータに組みこんで使用するが、高い性能が要求されるため、専用のハードウェアが用いられる場合もある。

実際には、インターネットと LAN の間に、アクセス制御という仕組みを果たしている。

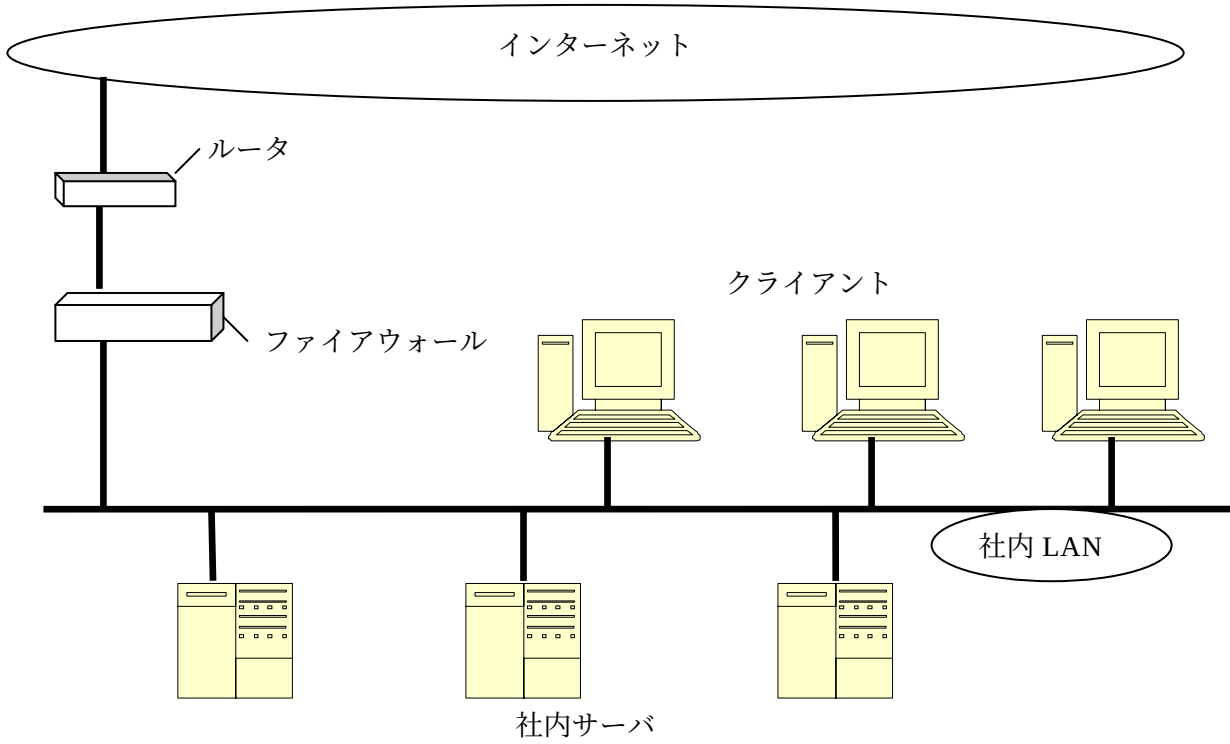
① 外部との出入り口を絞り

② LAN の内部構造を LAN の外部からは見えないようにし

③ 外部からの不正なアクセスを排除しつつ

④ 必要なアクセスだけを通過させる

ファイアウォールは、ネットワークの規模や目的などに応じてさまざまな構成にできるが、基本的な構成は以下の通りである。



次にファイアウォールの機能についてである。基本的な機能には、① パケットフィルタリング、高機能なファイアウォールには、② アプリケーションゲートウェイ、さらに内部ネットワークに、③ プライベートアドレス、を割り当て、アドレス変換技術を使用して、セキュリティを保ちながら、外部へのアクセスを可能にするケースもある。

この３つを以下に説明する。

① パケットフィルタリング

インターネットや社内 LAM などの TCP/IP ネットワークでは、データはパケットと呼

ばれる単位で伝送される。

各パケットにはヘッダが付いていて、ヘッダには、送信元 IP アドレス、相手先 IP アドレス、送信元ポート番号、相手先ポート番号、パケットの連番などの情報が含まれている。

パケットフィルタリングとは、送られてきたパケットの持つこれらの情報に基づいて、検査して通過させるかどうか判断する機能のことである。パケットのヘッダにはプロトコルや送信元アドレス、送信先アドレスやポート番号などの情報が含まれており、これを参照して通過するかどうかが決定される。通過できなかったパケットは送信元に通知されたり、破棄されたりする。どのような方針に基づいて判断するかは、そのネットワークの管理者が任意に設定することができる。最も一般的かつ簡便なセキュリティ技術として知られており、最近のルータは大半が持っている機能だが、よく知られているだけに破る手段も多く、他の技術と併用することが肝要である。

② アプリケーションゲートウェイ

アプリケーションゲートウェイとは、HTTP、FTP、POP、SMTP などのアプリケーションプロトコルに基づいてアクセス制御を行う。例えば、HTTP は通すが、FTP は通さないなど、プロトコルごとに制御ができる。

また、アプリケーションゲートウェイでは、ユーザやグループ、実行するコマンドなどに基づいて詳細なアクセス制御が可能である。

③ プライベートアドレスの割り当て

インターネットに接続する機器にも IP アドレスが割り当てられている。IP アドレスは世界中を通してただ１つで同じものは他になく、機器と IP アドレスは１対１に対応している。これをグローバルアドレスと呼ぶ。

しかし、インターネットの爆発的な普及にともない、IP アドレスの不足が心配されるようになった。そこで、組織や会社内の閉ざされた空間だけで通用する IP アドレスが利用されるようになった。これが、プライベートアドレスである。

プライベートアドレスは、グローバルアドレスの不足を補うだけでなく、セキュリティ面での利点もある。プライベートアドレスに対しては、インターネットからアクセスされることがないからであえる。

ただし、プライベートアドレスのままではインターネットへのアクセスができないので、ネットワークアドレス変換技術などといった技術を使用する。

4.4.1.4　IDS

IDS とは侵入検知システムのことで、通信回線を監視し、ネットワークへの侵入を検知して管理者に通報するシステムのことである。ネットワーク上を流れるパケットを分析し、パターン照合により不正アクセスと思われるパケットを検出して、管理者に通知する。製品によっては疑わしい通信を切断するなどして防衛措置を講じる場合もある。不正アクセ

スでよく用いられる手段をパターン化して記録しておき、実際に流れてくるパケットとパターンを比較することによって、正常な通信であるかどうか判断する。

IDS には 2 種類がある。2 種類とは、ネットワーク型 IDS と、ホスト型 IDS である。

① ネットワーク型 IDS

ネットワーク上を流れるパケットを直接監視する。監視は、あらかじめデータベースに蓄積されている攻撃手法や侵入パターンのデータと比較して、一致した場合に不正な通信がおこなわれている可能性が高いことを通知する。

② ホスト型 IDS

ホストコンピュータ上で起こったイベントの情報（ログなど）を監視する。監視は、あらかじめ決めておいたルールと比較し、ルールに従っていなければ不正行為が行われている可能性が高いことを通知する。

4.4.2 本質的方法

本質的方法として、以下の４点を挙げる。

4.4.2.1 保管方法

保管方法では、主に物理的情報資産を対象とする方法を研究する。

まず、情報資産を適切な重要度のレベルに分け保管、管理していく。

情報の分類及び関連する保護管理策では、情報を共有又は制限する業務上の必要、及びこのような必要から起こる業務上の影響を考慮にいれなければならない。

さらに、組織が採用した分類体系に従って情報ラベル付け及び取り扱いをするための、一連の手順を定めなければならない。

4.4.2.2 バックアップ

バックアップについては、電磁的情報資産を主な対象とする。

オペレーションミス、システム障害、あるいは自然災害などによって、貴重な業務情報やソフトウェアが破壊されてしまうことが想定される。そのような場合にも確実に回復が行えるよう、十分なバックアップ設備を整え、定期的にバックアップをとる必要がある。また、バックアップの完全性について定期的に検査することも必要である。復旧にあたっては当該情報や情報システムを速やかに復旧し、業務を継続できるようにする。

バックアップは、リスクアセスメントによる識別・評価に基づいて行う。例えば、地震などの大規模災害に備えたバックアップは、オペレーションミス対応のバックアップコピーとは識別し、保管すべきである。

4.4.2.3 リスク対策

災害、人為的事故、情報流出などのリスクに対し対策を講じておかなければならない。

なかでもリスクに対する保険が各損害保険会社から販売されているので、これに対し以下で研究する。

1989 年頃から損害保険各社は相次いで不正アクセスやウイルスの被害を補償する保険商品の販売を開始した。

各保険会社がこの時期に一斉に参入をした理由としては、この年から保険商品の開発に際して規制が緩和され、自由な商品設計が可能となったことが挙げられる。損保各社は、かねてから企業の情報化の進展により、不正アクセスなどの新たなリスクを補償する分野を有望な新規市場と考えていた。そのため、この規制緩和にタイミングを合わせて競って商品化を行ったのである。

商品化にあたり、ネットワークセキュリティ対策を専門に行っている企業などと提携し、企業情報システムのリスク診断をする手法は各社それぞれで開発を行っている。これらの診断手法の差は、商品サービスの内容や保険料設定に大きな差となって表れている。

保険料算定時の診断のポイントは、対象となる企業情報システムのリスクを的確に判断し、保険料に反映させることである。保険料に占める診断コストを抑えれば、小規模な保険設定が可能となる。

また、新しい保険ということで各社とも補償条件が異なっている。

4.4.2.4　従業員教育

社会人教育やジョブトレーニングと同様に教育・訓練を受ける者に対して、なぜ、何を、どのようにを的確にすることが肝要である。

組織内のすべての従業員や関連の外部の関係者、それぞれに対して、情報セキュリティに関するリスクを認識してもらい、セキュリティ基本方針を遵守することを理解してもらい、その達成のためにどのように行動するかを理解してもらうための教育・訓練が必要となる。

教育・訓練は集合研修だけをさすのではない。「意識付け教育」おいては、集合研修でもっともな話しを聞いたとしても、経営者や管理職の姿勢が伴わなければ誰も従いはしないだろう。常日頃、経営者が自分の考えを明確に示し、管理職も経営者の姿勢を最大限尊重し、業務との関係について明確な方向性を指し示すことが、まさに理想的な教育環境となる。

現在、多くの組織では、個人の行動規範を定めているにすぎず、なぜ行動規範が求められるのかを正確に理解させるところまで教育されているとは言えない。今日の社会問題を考慮した場合は、より積極的な教育が求められている。

4.5　規制

やはり何らかの規制がなければならない。ここでは規制として、法律、ガイドライン、セキュリティポリシの 3 つに分け、研究する。

4.5.1　法律

法律としては、「3.1.2　不正アクセス」で述べたように、「不正アクセス行為の禁止等に関する法律」も１つ挙げられる。この法律については、先の節で述べたのでここでは省くことにする。

① 不正アクセス行為の禁止等に関する法律

「3.1.2　不正アクセス」に述べてあるため、ここでは省略。

② 刑法

古くは、刑法の記述にある。

刑法第 157 条 1 項には、公正証書原本不実記載等について記載がある。ここには、「公正証書の原本として用いられる電磁的記録」という記載があり、電磁的データに関する改ざんについても罰則が規定されている。

また、第 161 条 2 号 2 項には、電磁的記録不正作出及び作用についての記載もある。ここには、電磁的データを不正に作った者にたいする罰則が規定されている。

他にもカード電磁的記録不正作出等の法律などもある。

以下にまとめておく。

・電子計算機損壊当業務妨害罪

コンピュータや電子的データを破壊することによる業務妨害。

・電磁的記録不出及び供用罪

事務処理を誤らせる目的で、電子的データを不正に作成する。

・電子計算機使用詐欺罪

コンピュータに虚偽の情報や不正指令を入力する等により不正に利益を得る詐欺行為。

③ 電子署名及び認証業務に関する法律(電子署名法)

この法律の目的は、電子署名（デジタル署名）に署名や押印と同じ効力を持たせることである。契約書などの私文書は、本人またはその代理人の署名または押印があるときは、訴訟において真正に成立したものとして取り扱われる。しかし、電子政府や電子商取引の進展に伴い、デジタルな情報の真正性をデジタルな署名や押印により保証するということが必要になってきた。この法律では、電子署名とは何か、電子証明書とは何かを規定し、電子的に認証を行う認証業務や認証事業者についても規定している。

④ 個人情報の保護に関する法律（個人情報保護法）

この法律は、個人情報の漏洩や不正利用などに対して、個人の権利を保護するために、個人情報を取り扱う事業者の遵守すべき義務を規定している。一方、個人情報の適正な利用はできるように配慮されている。個人情報とは、氏名、生年月日その他の記述等により特定の個人を識別することができるものを指す。「個人情報の保護に関す

る法律施行令」では、5,000 件以上の個人情報を有する個人情報データベースを、事業のために使用している組織や企業がこの法律の対象となると定められている。

この法律により、本人の了解無しに個人情報を流出したり、売買したり、譲渡をすることが規制されている。個人情報は適正な方法により取得し、利用は収集目的の範囲内で行うこと、個人情報の漏洩を防ぐためのセキュリティ対策を行うことなど、個人情報保護の基本原則が定められている。

この法律は、2005 年 4 月より本格施行され、これらに違反した場合、本人の届け出などにより、事業者の刑罰が科されることがある。

4.5.2 ガイドライン

ガイドラインとしては、国際規格や規定を挙げる。

① ISO/IEC 17799:2000

これは、情報セキュリティマネジメントの国際規格である。

この規格は、2000 年にイギリスで発行されたものである。この規格では、情報セキュリティとは何か、から始まり、情報の脅威、情報セキュリティの運用管理、基本方針などが規定されている。この規格を見れば、情報セキュリティマネジメントの全てが分かるようになっている。また、国内の規格、規定もこの規格に基づき策定されている。

② ISMS 認証基準

この基準は、財団法人日本情報処理開発協会（JIPDEC）が規定するものである。

これは、情報セキュリティは「セキュリティ品質の継続的維持」および「リスクマネジメント」を目的とし、それを実現するマネジメントシステムは、複数のプロセスにより構成されている。ISMS のプロセスモデルは、確立、導入及び運用、監視及び見直し、維持及び改善の４つの要素で構成されている。

現在は、認証基準が Ver.2.0 に改訂され、当初の国内独自路線から、国際基準として認定されているイギリスの BS7799 との完全整合がはかられている。

4.5.3 セキュリティポリシ

ここでは企業においての情報セキュリティの法律である、セキュリティポリシについて研究する。

情報セキュリティマネジメントシステム（ISMS）を構築する際の基盤となる、企業・組織のセキュリティに関する基本的な考え方を示したものが「情報セキュリティポリシ」である。セキュリティポリシは、全社を貫くセキュリティへの取り組みの基本方針、規則体系を明文化した文書を意味する。セキュリティ対策を進めるうえのスタート地点にあたるもので、セキュリティの総合指針というべきものである。セキュリティの成否は、この「セキュリティポリシ」が企業の実務、セキュリティのニーズに適合したものであることが重

要なポイントとなる。このためには、技術的な側面と、（セキュリティを担当する）人員的な側面のバランスが統合されなければならない。

５．事例

ここでは企業で実際行われている情報セキュリティの事例を挙げる。対比的にするために、業界が同じ IT 業界 2 社を挙げる。

情報セキュリティにおいて成功という概念はないため、一方は ISMS のホームページにて紹介されている事例の中の 1 社を、もう一方は顧客の個人情報を流出させてしまい話題になった 1 社を挙げる。

5.1　実際行われている情報セキュリティ

ここでは ISMS に基づいて、企業で実際行われている情報セキュリティについて事例として挙げる。以下は、ソフトウェア開発やソリューションサービスのアウトソーシングサービス事業を行っている、TIS 株式会社についてのものである。

① ISMS 導入の経緯

情報セキュリティや安全に関わる会社の資格はお客様に安心感を与えることができ、そのため TIS 株式会社では安心感をもとにお客様との信頼関係を構築していくことができる。そこで、安心感を抱いてもらうため ISMS 認証が必要であると感じた。

TIS 株式会社では既に「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」（以下「安対」）の認定を受けており、セキュリティの地盤はあった。そのため、チャレンジするために導入を決めた。

② ISMS 構築

構築期間は、これまでの安対+ISO9001 の下地があったため意思決定後すぐ ISMS 構築に着手できた。そのため期間は、６ヶ月間であった。また、ISMS Ver.2.0 への移行は情報セキュリティ機能を追加した会議体で展開し、３ヶ月間であった。

③ 強化部分

アクセス管理の強化を必要と判断し、パスワードの都度発行ならびにアクセスの３者認証の手続きをシステム化した。

開発部門がデータを加工・納品したり、障害対応にて本番データへアクセスする場合、開発部門と運用部門とがアクセスの承認を確認の上、運用部門から本番データにアクセスできる権限(パスワード)を通知する手続きとした。また、データの所有者である顧客への承認は、開発部門が得ることとし、パスワードはアクセスが終了した時点で、都度変更している。

④ 社員教育

各部門のキーパーソンと一般社員向けの教育の２種に分け行う。

まず、各部門のキーパーソンには、ISMS の運用及び規則についての講習会を実施した。また、情報処理技術者試験の「セキュリティアドミニストレータ」の資格取得も奨励した。また、一般社員向けには、対象部門以外にもセキュリティの勉強会を開催した。

このように TIS 株式会社では、ISMS に基づきセキュリティ対策を施している。TIS 株式会社にとっては、このようなセキュリティを行うことは、お客様にとっても企業にとっても当たり前のことであり、何のメリットもない、とのことである。この ISMS 取得により、顧客から ISMS 取得の相談を持ちかけられるようになったそうだ。

5.2 失敗例

昨年、企業による個人情報漏洩が相次いだ。その中でも被害が甚大であったソフトバンク BB！社による漏洩事故について挙げ、例とする。

① 事件の経緯

事件は、2004 年 1 月 14 日にあるユーザからの情報流出の可能性の指摘を受け、10 日後の１月 23 日「お客様情報の流出についての詳細とお詫びについて」のプレスリリースを発表したことにより発覚した。２月 27 には、孫社長が東京・虎ノ門のホテルオークラで会見を開き、451 万 7039 件もの「Yahoo! BB」ユーザの個人情報が流出したことを初めて認めたのである。

通信事業者の顧客情報漏洩事件はこれまでもあった。例えば 99 年に NTT 東日本で約 5000 件，NTT 西日本で約 3000 件の情報が社員経由で流出した。KDDI でも 2000 年 10 月，代理店から 3 万 2000 人分の情報が流出した。しかし，今回の流出件数は桁違いの 451 万件。ソフトバンク BB は，情報管理体制の甘さを指摘されても当然である。

まず，簡単に経緯を振り返ってみる。警視庁は 2 月 10 日，流出した顧客情報を基にソフトバンクを恐喝していた湯浅輝昭容疑者など 3 人と木全泰之容疑者を逮捕した。湯浅容疑者は Yahoo！BB の販売代理店の役員で，木全容疑者は Yahoo！BB のコール・センターで勤務していた。

警察から分析を依頼された「japan.internet.com」によると、451 万 7,039 件の個人情報が流出したことが判明した。湯浅容疑者分が 444 万 7,751 件、木全容疑者分が 55 万 6,611 件だが、両者で重複しているデータもあり、流出データは合計 451 件 7,039 件。クレジットカード番号や銀行口座、パスワード、取引実績などの信用情報は流出していないという。また、調査の結果、原因はグループアカウントであると分かった。

顧客データベースに直接アクセスする権限を持つ人は，社員と業務委託先を含めて 135 人いた。このうち，いくつかのアカウントは，3～4 人で共用するグループ・アカウントだったという。さらにコール・センターでは，顧客対応のために数千人のオペレータが個人情報にアクセスできる。オペレータは 2003 年 9 月まで，一度に多くの情報にアクセスできることができた。

社員などの中に悪意を持った人間がいれば，大量に顧客情報を引き出せる状況にあった。ソフトバンク BB の鬼頭周システム＆サプライチェーン本部長は，「アクセス権限を持つ人やサポート・センターのオペレータが，物理的に情報を持ち出すことは全くなかったとは断定できない」と言う。

情報流出が確認されたユーザには全員メールで連絡するが、メールアドレスのない BB フォン単独ユーザには郵送で連絡をした。さらに、 Yahoo! BB 全会員に対し、情報流出の有無に関わらず 500 円相当の金券などを送付した。つまり、総額約 40 億円という巨額の支出となった。

また、この顧客情報流出により、また、今回の事態に関する社内処分として、代表取締役社長兼 CEO の孫正義氏を 6 か月間 50%減給、取締役副社長兼 COO 宮内謙氏と取締役 CTO 筒井多圭志氏を 3 か月間 30%減給とした。

② 事件後…

事件後、ソフトバンク BB！は、現状を見直し様々な対策を講じた。

まず、全社レベルのセキュリティ対策を迅速に行えるようにするための組織改革を実施した。情報セキュリティ責任者（CISO）として元マイクロソフト社長の阿多親市氏を据えた。また、ソフトバンク BB！は 649 項目に渡る再発防止対策を実施した。それらの対策の一部を参照する。

同社は、まず建物内におけるセキュリティのレベルを 5 段階に定義した。そのうえで、レベルに応じた認証方法を採用。例えば、レベル 1 のエリアの入り口には警備員が立つ、レベル 2 のエリアの入り口ではカード認証が必要といった具合だ。レベル 3～5 のエリアは「高セキュリティエリア」と位置づけた。監視カメラを設置したうえで、個人特有の生体情報（指紋）を認証に利用し、複数の手段で不正侵入を防ぐようにした。他人の IC カードを使って不正に入室する“なりすまし”を避けるためだ。例えば、レベル 3 のエリアではレベル 2 と同じくカード認証が必要。加えて、監視カメラを設置し、警備員も立つ。指紋認証も必要だ。間違っても、ちょっと借りた IC カードを使って入室なんてことは不可能となった。

高セキュリティエリアへの入室時には指紋認証

レベル 4 とレベル 5 のエリアでは、認証に加えて身分証明および利用申請が必要になる。特にレベル 4 のエリアの入り口には、金属探知器が埋め込まれたセキュリティゲートを設置。センター内への携帯電話などの持ち込み／持ち出しを取り締まる。

また、個人情報保護のための方針として、以下の文章をホームページに発表した。

ソフトバンク BB 株式会社は、「電気通信事業における個人情報保護に関するガイドライン」（平成 10 年 12 月 2 日郵政省告示第 570 号）、「個人情報の保護に関する法律」（平成 15 年 5 月 30 日法律第 57 号）および「個人情報保護に関するコンプライアンス・プログラムの要求事項」（JISQ15001）の遵守徹底を図るため次の各項の実施に努めます。

1.社員教育の強化

個人情報保護に関する学習教材を作成し、全社員および派遣社員に配布するとともに、最低 1 年に 1 回は個人情報を扱う全社員および派遣社員を対象に研修を実施します。

2.個人情報保護に関する内部規程の整備

個人情報保護に関する内部規程を整備し、個人情報の取扱いについて明確な方針を示すとともに、個人情報の漏えい等に対しては、厳しい態度で望むことを社内に周知徹底します。

3.「個人情報管理者」の配置及び機能強化

「個人情報管理者」を設置するとともに、その役割を明確にし、個人情報管理者が適切に個人情報保護に関する活動を行えるように環境整備を行います。

4.適切な情報セキュリティ対策の実施

個人情報を取り巻くリスクを把握し、不正アクセス、紛失、改ざんおよび漏えい等の予防や是正に関する適切な情報セキュリティ対策を講じます。

5.業務委託の見直し・改善

業務委託については、より個人情報の保護に配慮したものに見直し・改善を図ります。業務委託契約を締結する際には、業務委託の相手としての適格性を十分審査するとともに、契約書の内容についてもより個人情報の保護に配慮したものとします。

6.監査体制の整備・充実

個人情報の保護が適切に行われているかどうかについて、社内で監査できる体制を整備してまいります。

また、アクセスログを活用した監査は、社内での個人情報漏えい者の早期発見及びそれによる抑止効果の発揮による漏えいの未然防止に有効と考えられますので、その実施方法を検討してまいります。

8. 個人情報保護に関する活動の継続的改善

個人情報保護に関する上記 1～7 の活動について、継続的な見直し・改善を図ります。

7.個人情報の適切な収集、利用および提供

個人情報の収集、利用および提供にあたっては、事業の内容および規模を考慮した上で、

適切に実施します。

個人情報保護のための行動指針の対象

当社の顧客、取引先企業の社員、当社の社員を問わず、個人に関する情報であり、当該情報に含まれる氏名、生年月日その他の記述、または個人別に付された番号、その他の符号、画像もしくは音声により当該個人を識別できるもの（当該情報のみでは識別できないが、他の情報と容易に照合することができ、それにより当該個人を識別できるものを含む）をいう。この個人情報保護のための行動指針は、当社が、保有する全ての個人情報に適用されます。

このように、ソフトバンク BB！は、顧客情報漏洩を機に、情報セキュリティ対策を見直すことができた。しかし、約 451 万件にも及ぶ顧客情報の流出の打撃は小さなものではなかったはずだ。

６．終わりに（今後考えられる対策）

この研究の終わりとして、今後考えられる対策をこの章で考え、この論文の終章とする。

6.1　企業における情報セキュリティ

企業における情報セキュリティとして、従業員教育の徹底を挙げる。

５章までにおいて、「情報セキュリティ」ついて研究してきたが、情報が漏洩する原因となっているものは人為的によるものが多い。そのため、その「人」の管理の徹底が情報セキュリティを行うにあたり重要であると感じ、従業員教育の徹底を提案したいと思う。

現在の従業員教育は、「4.4.2.4　従業員教育」の節で述べたような教育体制である。

そこで、ここでは入社直後の研修に「情報セキュリティ」という項目を加えてはどうか、という提案をしたい。この理由は、入社直後に情報セキュリティに関する研修を行うことで、新入社員の従業員にも情報が企業にとっては資産であることを、意識に深く植え付けることができるのではないかと思うからである。

また、転職によう入社した者、アルバイトなどの者にも同様、入社直後に情報セキュリティ教育を行うことが必要である。

6.2　学校における情報セキュリティ

次に、身近な学校についてのセキュリティについて考えてみる。S

現状の学校の情報セキュリティポリシは、県あるいは市の教育委員会から配布されたものがあるものの実情に合っていないために運用されていなかったり、運用されている場合でもネットワークやパソコンを対象とした限定的なものが多い。本来の情報セキュリティポリシとは、ネットワークなどに対象を限定したものでもなく、幹部教職員を中心に学校が組織として取り組むものであり、組織のセキュリティ・レベルを継続的に向上させていくものにしなければならない。

本来、学校の情報セキュリティポリシは、学校が児童・生徒の成長に関わる機微な個人情報を保有することや、児童・生徒に対して情報セキュリティ教育や情報モラル教育を行う場でもあることから、官庁や民間の情報セキュリティポリシとは異なった要件が求められる。加えて多くの学校では、授業時間以外に教職員が情報システムの保守管理業務などの兼務している状態がある。これらの学校の実情を踏まえた、情報セキュリティポリシのあるべき姿を示すガイドラインが提示されることが望まれる。

参考文献

① NTT ラーニングシステムズ・編　山口伸弥・著
『情報セキュリティマネジメントが見えてくる』　日刊工業新聞社　2003 年
② 独立行政法人　情報処理推進機構・編　本郷充・著
『情報セキュリティ読本　IT 時代の危機管理入門』　実教出版株式会社　2004 年
③ 田中克政・著　『情報セキュリティ・マネジメント入門』　日本経済新聞社　1999 年
④ 安澤秀一、原田三朗・編　登坂治彦・著
『文化情報学-人類の共同記憶を伝える-』　北樹出版　2002 年
⑤ 高津信三・共著　『ユビキタス時代の情報管理論-情報・分析・意思決定・システム・問題解決』　共立出版株式会社　2003 年
⑥ 板倉正俊・著　『インターネット・セキュリティとは何か-暗号、認証、ウイルス、セキュア通信からセキュリティ・ポリシーまで』　日経 BP 社　2002 年
⑦ 坪根直毅、中島尚紀、小川創生、原田辰彦・共著
『-情報技術のすべてがわかる-SE 教科書』　翔泳社　2003 年
⑧ 財団法人日本規格協会・編　『情報セキュリティマネジメントの国際規格』
財団法人　日本規格協会　2003 年

参考 URL

http://www.ipa.go.jp/　独立行政法人　情報処理推進機構
http://www.johotsusintokei.soumu.go.jp/index.html　情報通信統計データベース　総務省
http://www.isms.jipdec.jp/　ISMS 適合性評価制度　財団法人　日本情報処理開発協会　ISMS　制度推進室