ネットワークセキュリティの研究

システム研究会第２グループ

＜担当委員＞

寺野純一(日本生命)

＜メンバー＞

佐藤一浩(住友生命)	小篠知史(日本生命)
小林孝司(住友生命)	池田光之(日本生命)
西崎光洋(大同生命)	益田毅久(明治生命)
中村靖英(大同生命)	小林俊之(同和火災)
品川　輝(日本生命)	田中和彦(同和火災)
阿部知之(日本生命)	松本孝治(富士火災)
松原聡明(日本生命)	武藤範嗣(富士火災)

＜目次＞

Ⅰ．はじめに

企業の情報システムは、ネットワーク技術の進歩に伴い大きく変化している。従来の情報システムは、自社内に閉じたオープンではないネットワークかつ独自の通信プロトコルで接続されていたため、自ずと保護されていたと言える。しかし、最近の情報システムはインターネットに代表されるように、ネットワークはオープンになり標準化されたプロトコルで通信でき誰でも簡単に接続できるようになっている。

誰でも簡単に利用できるようになったインターネットの普及率を見ると、日本における世帯あたりのインターネットの利用率は、平成８年に 3.3%、平成９年に 6.4%、平成１０年には 11.0%となっており、飛躍的に増加していることが分かる。また、ホストコンピュータも増加しており、平成４年に２万 3000 台であったものが、平成８年は 73 万台、平成９年は 117 万台、平成１０年には 169 万台まで増加している。

このようなインターネットの普及に伴い、不正アクセスなどのネットワーク犯罪も増加している。表Ⅰ－１はコンピュータ緊急対応センター(JPCERT)に報告された不正アクセスの件数の推移である。平成９年には 492 件報告されているが、平成１０年には 923 件、平成１１年も６月までの半年で 447 件報告されており毎年増加傾向にあることが分かる。しかし、ここに報告されているものは実際の被害のほんの一部であり、氷山の一角でしかないと考えられる。

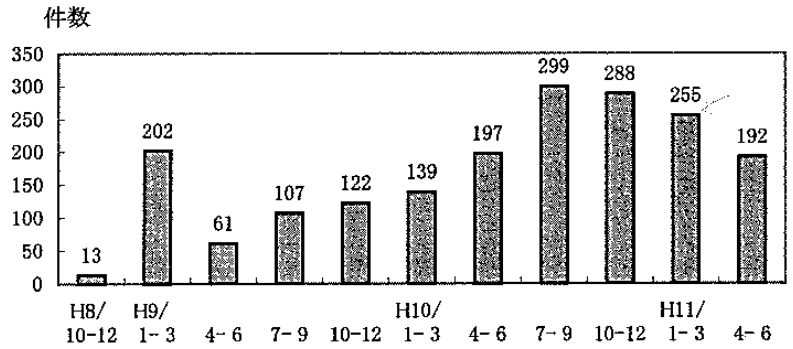

表 Ⅰ－１．不正アクセスの報告件数

では、増加しつづける不正アクセスから身を守るには何が必要なのだろうか。最近、企業ネットワークとインターネットの接続や、企業ネットワーク間の接続など、オープンネットワーク上でのデータのやりとりも実施されており、今後もさらに増加すると考えられる。このネットワーク上での商取引を、従来のネットワークと同様の確実性・信頼性で機能させるためには、ネットワークセキュリティ対策は非常に重要なものである。

このようにますます重要となるネットワークセキュリティについて、当研究グループでは、セキュリティの概要・考え方を整理し、不正アクセスの事例を通して原因と対策（セキュリティ技術）をまとめたうえで、保険業界におけるインターネット開放業務の現状と将来を比較し想定されるリスクを考察した。そして、最後にセキュリティ対策の実現に向けて必要な基本設計書とライフサイクルセキュリティの重要性を述べる。

Ⅱ．セキュリティの概要

1．セキュリティの定義

セキュリティを考えるにあたり、まず、セキュリティとは何かという定義を明らかにしておく必要がある。下記にセキュリティの定義を記す。

・Confidentiality（機密性）
　権限のない人に情報が漏れないように守ること
・Integrity（完全性）
　（広義）情報システム上での情報の生成から処理完了までを、現実世界と矛盾のないよう一致させておくこと
　（狭義）権限のない人が情報を変更しないように守ること
・Availability（可用性）
　権限のある人がシステムを何時でも利用可能な状態に維持すること
・Authenticity（真正性）
　情報の起源（作成者や送信者等）が本物であることを保証することで、電子商取引において特に重要とされる
・Accountability（責任追跡性）
　システムがいつ誰に利用されたかという責任を追跡できるようにすること
・Unobservability（非観察性）
　プライバシー保護の要件で、情報そのものやサービスの利用が他人に観察されないようにすること
・Anonymity（匿名性）
　プライバシー保護の要件で、身元を暴かれることなしに無名で情報やサービスを利用できるようにすること
・Pseudonymity（利用課金性）
　プライバシー保護の要件で、身元を示さずに情報やサービスを利用できるようにするがその利用に対する課金は行えるようにすること
・Unlinkability（非相関性）
　プライバシー保護の要件で、複数の情報やサービスを利用した場合に、他人がそれらの利用の相互の関連性を見出すことができないようにすること

2．セキュリティ要件

ネットワークセキュリティというものを考えるに当たり、前述のセキュリティの定義を満たす為には以下の６つの要件が必要である。

（1）本人認証
　アクセスしてきた人が登録されている人か、更に誰なのかという認証作業。
（2）アクセス制御
　（1）の認証の情報を基にその人に許された範囲内でのアクセスに制御する。
（3）改竄防止
　ネットワーク上でのデータ改竄の防止。
（4）機密保持
　ネットワーク上でのデータ盗聴の防止。
（5）否認防止
　特にインターネットでの商取引等では受発注等を行ったことを否認できないようにしなくてはならない。
（6）ウィルス対策

ネットワークが広がるほどウィルスに遭遇する危険は高まる。被害を受けるばかりでなく、加害者となる可能性も考慮しなくてはならない。

3．セキュリティ評価の基準

セキュリティ評価基準とは、情報システムや製品に対するセキュリティ対策がどの程度の有効性や強度を有しているかを世間の客観的な物差しで評価することを言う。

セキュリティ評価基準を満たしていれば、世間に対して自らのシステムや製品の安全性の高さをアピールすることが出来る一方、基準未達の場合はマーケットの競争力を失ってしまう危険性もある。ネットワーク上の脅威から自らのシステムを守るためには、以下のような考えと基準に基づいて行動する必要がある。

まず、守るべきものが何なのか、またそれが被害を受けた際にはどのような影響があるのか等を明らかにした上で、それに対する対策の考え方とどのようにして脅威から守るかという実現方式をまとめた基本設計書の策定が必要となる。

ここで基本設計書の策定手順を下記に記す。

（1） 保護すべき資源を明確化
（2） 保護すべき資源の利用規則を決定
（3） 脅威の見極め
（4） セキュリティポリシーの決定
（5） 機能要件と品質保証レベルを選択
（6） 評価対象の仕様や開発手法の決定
（7） 基本設計書の内容を検証

なお、基本設計書の具体的な策定手順は、Ⅴ章で詳細に後述する。

Ⅲ．ネットワークセキュリティにおける技術と不正事例

ここでは、ネットワークセキュリティ実現のための技術として、代表的なものを取り上げるにあたり、その技術を実施するべきと思われる不正事例を併せて紹介する。また、それぞれの技術がどういった技術であるのかについて概観する。

１．事例①「アクセス制御とＶＰＮ」

（１）事件

平成６年１２月、銀行の預金業務等のオンライン処理に使用する電子計算機に対し、実際には振り込み事実がないのにもかかわらず他行の指定口座に十数億円の振込をした旨の虚偽の情報を与え、不法に資金移動させて財産上の利益を得た。平成７年２月、電子計算機使用詐欺罪で検挙された。

（２）検証

犯人は、ネットワークに対する盗聴によって、まず銀行のオンラインシステムに入るためのユーザＩＤ・パスワードを探知していると考えられる。ユーザＩＤ・パスワードを探知した犯人は次に電話回線に接続したパソコンからオンラインシステムに入り、虚偽の情報を登録している。この事件は正当ユーザによる処理ではないことから不正アクセスである。

（３）ネットワーク上の危険

上記事件のように、ネットワークシステムは不正行為の脅威にさらされている。発生しうる不正行為の脅威を簡単なネットワーク図で表すと下図のようになる。

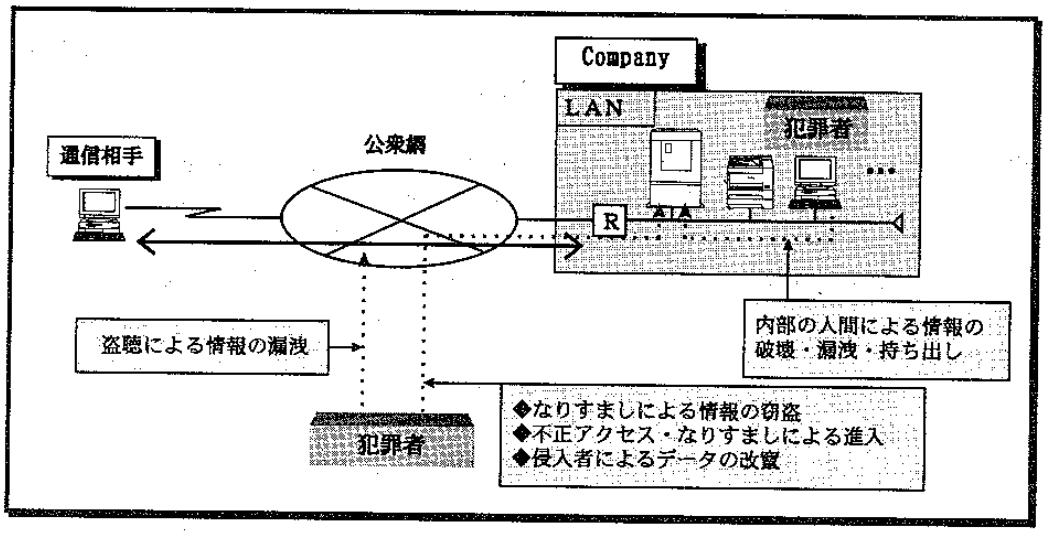

図 Ⅲ－１．ネットワーク上の危険

外部の犯罪者からの切り口は２つに大別される。まず、ネットワーク上を流れるデータに対する切り口である。ここでは、盗聴による情報の漏洩あるいは情報の改竄といった不正行為が行われ得る。もう一つは、ネットワークを介して情報を有する社内ＬＡＮ等に対する切り口である。ここでは、不正アクセス・なりすましによる侵入、情報の窃盗、侵入者によるデータの改竄が行われる可能性がある。

一方で、内部の犯罪者からの切り口もあり得る。ここからは、情報の破壊・窃盗・漏洩・改竄等、多様な不正行為が行われる危険が増加する。

（４）対応

上記（１）のような事件の発生を防ぐ対応として、以下２点の技術が挙げられる。

・不正アクセス・なりすまし　→　アクセス制御

・盗聴　→　暗号化

それぞれの技術がどういったものであるかを以下に述べる。

（5）技術

a．アクセス制御

イ．アクセス制御とは

ユーザが何かのセキュリティサービスを利用するとき、ユーザとセキュリティサービス提供側との間で通信の論理的な結合、いわゆるセションが確立される。このとき、識別やユーザ認証で結合の可否を制御することをアクセス制御という。

ロ．ユーザ認証

アクセス制御は、ユーザ認証の実施により実現される。ユーザ認証とは、セキュリティの機能を利用しようとしているユーザが、申請どおりの識別名をもつユーザであることを確認することである。ユーザの識別名が確認されたときに、確認されたユーザはどういう属性情報をもつものであるかということが認識される。このユーザ認証が正しく行われることが、その後の全てのセキュリティサービスが正しく行われるための根本となる。

ハ．アクセス制御の技術

アクセス制御技術の実現場所としては、人と装置との間の認証と、装置同士の装置間認証とがある。

人と装置との間の認証には、ユーザＩＤとパスワードによる認証と、生物学的認証とがある。

・ユーザＩＤとパスワードによる認証

ＰＡＰ　…ユーザＩＤとパスワードを送信してアクセスするログインスクリプトによるユーザ認証

ＣＨＡＰ…ＰＡＰでは、パスワードが平文のままで流れてしまうのに対し、乱数を使ってパスワードを暗号化するものがＣＨＡＰ

・生物学的認証

指紋や網膜パターンなど、人間を一意に特定できる特徴により認証を行うもの。

パスワードについても、人間の記憶による一種の生物学的認証ともみなせる。

装置同士の装置間認証は、暗号的認証で実現される。これは、乱数のやり取りなどにより、同一のアルゴリズムをもつ装置間でのみ相互認証がなされるというものである。

b．暗号化

イ．暗号化とは

暗号化とは、通信データの盗聴・改竄を防ぐための技術である。

ロ．暗号化の技術

暗号化の技術として、秘密鍵暗号方式・公開鍵暗号方式が代表的なものとして挙げられる。

・秘密鍵暗号方式

暗号のルール（鍵）を、送り手と受け手だけが知っている暗号方式を秘密鍵暗号方式と呼ぶ。秘密鍵と呼ぶ一つの鍵を使って暗号化と複合化を行う。秘密鍵暗号方式の代表的なものには、ＤＥＳ（Data Encryption Standard）と呼ばれる方式がある。

・公開鍵暗号方式

公開鍵・個人鍵のふたつの鍵を使用し、公開鍵については公開するものである。公開鍵暗号方式の代表的なものには、ＲＳＡと呼ばれる方式がある。公開鍵暗号の使い方としては、「電子署名」が挙げられる。

公開鍵暗号方式の運用においては、公開鍵が公開される性質上、「認証局」が重要な機能を果たすこととなる。

ハ．認証局

電子署名された証明書を正規の物であると認証する機関が、認証局である。公開鍵と個人鍵のペアを生成し、出来上がった公開鍵を認証局に送って認証局に署名してもらう。これに

より、その公開鍵が間違いなく本人の物であると証明されることとなる。

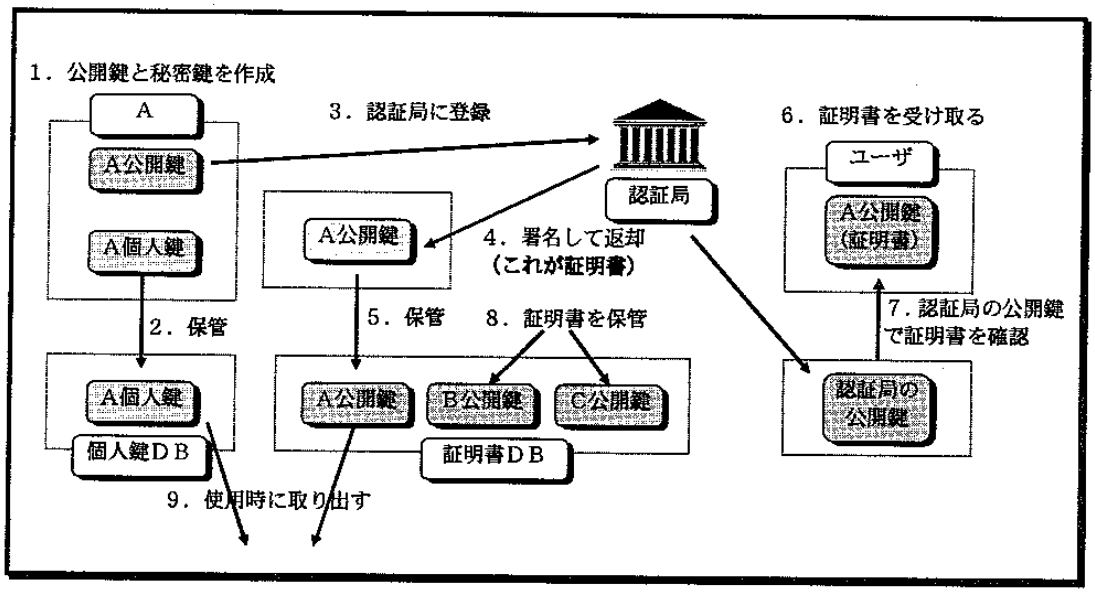

図 Ⅲ－２． 公開鍵暗号方式と認証局

（６）技術の実現方式

ａ．ファイアウォール

イ．ファイアウォールとは

インターネットと企業内ネットワークの接点において、あらかじめ決められた基準をもとに、あるデータについては通信を許可するが、他のデータについては通信を拒否するというアクセス制御を行うことにより、外部からの侵入を阻止するための技術である。

ロ．ファイアウォールの方式

ファイアウォールにつき、構成によるものと方式によるものとの両面から分類すると下図のようになる。

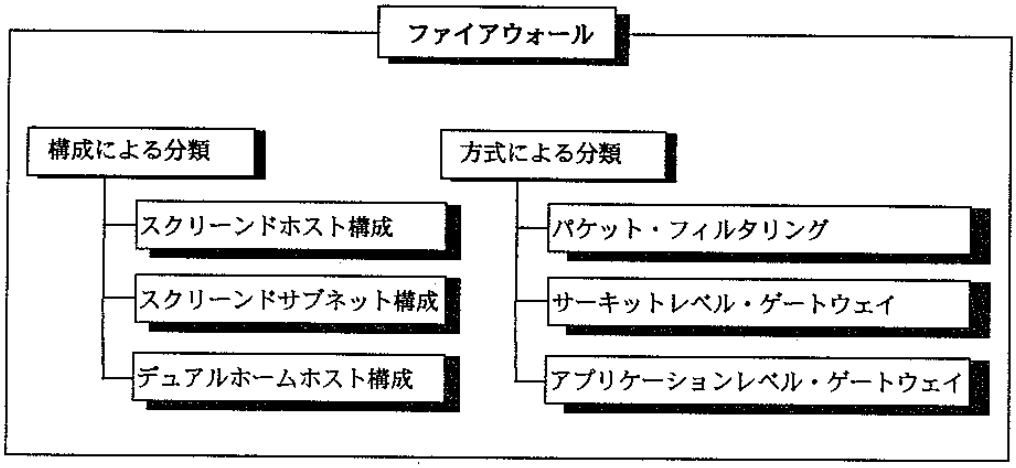

図 Ⅲ－３． ファイアウォールの分類

ｂ．ＶＰＮ（Virtual Private Network）

イ．ＶＰＮとは

ＶＰＮとは、公共のネットワークをあたかもプライベートネットワークを利用しているが如く、離れた２地点間で通信する手段である。

ロ．ＶＰＮの方式

ＶＰＮの方式は、その構成からグループＶＰＮとパーソナルＶＰＮとがある。

・グループＶＰＮ　… 組織ネットワークのゲートウェイ間で暗号化通信路を構築するもの。

・パーソナルＶＰＮ … インターネットに接続した端末と組織ネットワークのゲートウェイ間で暗号化通信路を実現するもの。任意のアドレスからＶＰＮを利用できるのが特徴。

ハ．ＶＰＮを構成する技術

ＶＰＮは、下図のように様々な切り口・要素から成立する技術である。

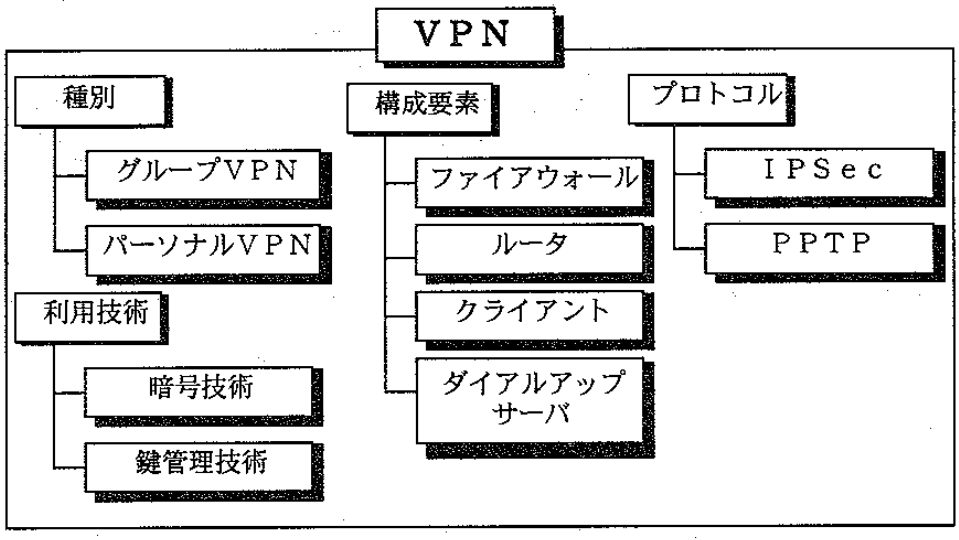

図 Ⅲ－４．　ＶＰＮの分類

（７）セキュリティ技術の適用

前述の（３）に表したネットワークの危険を、これまでにみた技術を利用して防御すると、以下のようになる。

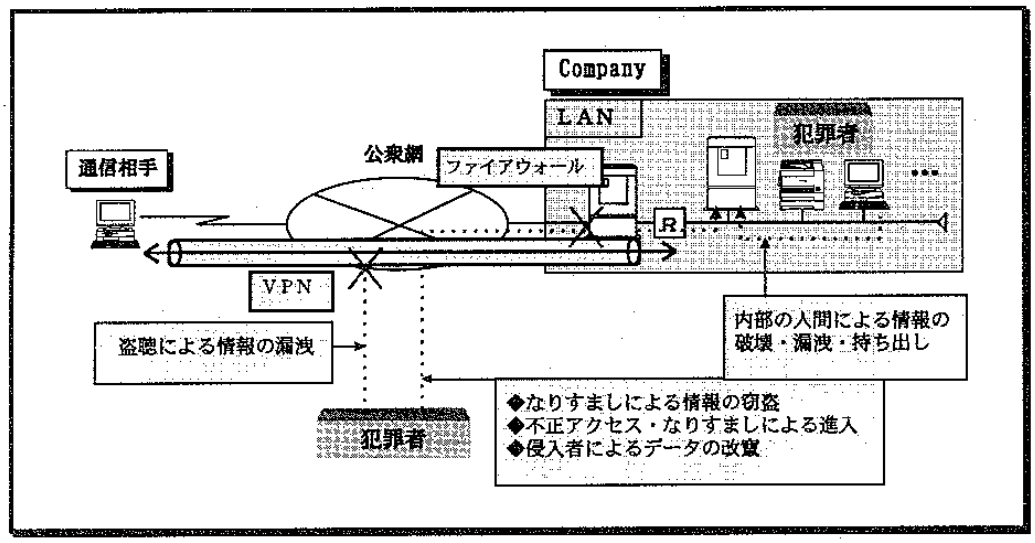

図 Ⅲ－５．　ネットワーク上の危険と防御技術

また、内部からの不正行為については、内部ファイアウォールによりある程度防御できる。

２．事例②「スパムメールとウイルス」

（1）事件

平成１０年８月、Ａ社は利殖の勧誘メールが海外から送りつけられ、Ａ社のサーバを経由して大量にばらまかれた。通常よりサーバの処理速度が遅いとは感じていたが、まさかスパムメールの踏み台にされているとは気が付かなかった。Ａ社は、その勧誘メールを受け取ったユーザからの苦情で、初めて踏み台にされた事実を知った。

更に悪いことに、その勧誘メールにはウイルスが混入されていた。メールに添付されていたＷＯＲＤ文書を開いた端末では、翌朝から端末が立ち上がらなくなってしまった。ウイルスの被害にあった端末は、ＯＳの再インストールによる復旧を余儀なくされた。ウイルスに感染し、システムファイルが破壊されてしまったのである。

たとえスパムメールの踏み台になったとしても情報漏洩などの実害はないが、社会的な信用を傷付けられるという意味で被害は大きい。さらに、ウイルスが混入しているとなれば、システムダウン等の実害を引き起こす可能性もあり、深刻な問題である。なぜなら、スパムにより送りつけられたユーザは、踏み台にされたサーバの所有者を加害者と認識するからである。

（2）検証

今回の事件は何故起きたのであろうか。スパムメールの踏み台、更にはウイルス混入という被害について、ここでその原因を分析してみる。

まず、スパムメールの踏み台にされた原因は、社外から送られてきたメールに対して、社内宛でないメールの配送を許していたことである。社外から送られてきたメールに対しては、社内宛のメールしか許さないのが原則である。

次に、ウイルスの被害にあった原因は、メールを受信する際に、ファイアウォールからメールサーバに格納する前で、ウイルスチェックを行っていなかったことである。さらに、メールに添付されている文書に対するウイルスチェックを行うことはインターネットメール環境を構築する上での基本であると言っても大袈裟ではない。

ここに挙げた原因は、インターネットメール環境（社外とのメール通信）を構築する上での最低限のセキュリティ対策と言える。

（3）一般的な被害

それでは、スパムメールとウイルスに関する一般的な被害について簡単に触れてみる。

ａ．スパムメールによる被害

スパムメールによる被害には、次の２つが挙げられる。

まず１つ目は、E-Mail 爆弾による障害である。E-Mail 爆弾として大量のメールが送りつけられると、不正なアドレスによる送信エラーや自社サイト向けのメールでディスクが溢れたり、大量のメール処理によるメモリバッファオーバーフローでシステムダウンを引き起こす危険性がある。

２つ目として、スパムメールの踏み台による被害である。スパムメールの踏み台にされると、不正に中継することで他サイトに対して被害を広げてしまったり、スパムメールの中継者として信用問題に発展する危険性がある。

ｂ．ウイルスによる被害

ウイルスによる被害には、感染方法や感染場所によって様々な種類があるが、ここでは代表的なウイルスをいくつか紹介することとする。

イ．ファイル感染型ウイルス

ファイル感染型ウイルスとはファイルに感染するタイプのウイルスに対する呼称で、主に「.com」や「.exe」の拡張子を持つ実行ファイルを感染対象とするウイルスである。例えば、このウイルスに感染すると、突如予期せぬ音楽を演奏し始めるというような事象が発生することがある。

ロ．ブートセクタ／パーティションセクタ感染型ウイルス

ブートセクタ／パーティションセクタ感染型ウイルスとは、ブートセクタ／パーティションセクタに感染するタイプのウイルスに対する呼称で、誤ってフロッピーディスクを差し込

んだままコンピュータを起動したときなどに感染するウイルスである。例えば、フロッピーディスクから目に見えないところで感染していき、ある一定条件を満たしたときに、突如ディスクの内容を破壊したりする。

ハ．マクロウイルス

マクロウイルスとはMicrosoft社の「Word」などのマクロ機能を利用して作成されたウイルスで、該当アプリケーションで作成された文書ファイルに感染するウイルスである。

例えば、メールの添付ファイルを開いた瞬間に、自動的にMicrosoft社の「Outlook」のアドレス帳に登録されている宛先に、ウイルスに感染しているファイルを添付してメール送信してしまうというものまである。

その他、コンピュータを400回起動したらハードディスクの内容を破壊するような「論理爆弾」と呼ばれるウイルスや、あたかも便利なユーティリティと見せかけて実行するとシステム破壊などを引き起こす「トロイの木馬」と呼ばれるウイルス（厳密にはウイルスではない）などもある。

（4）対策

今回の事件は、どのようなセキュリティ対策を行っていれば防げたのであろうか。ここで、スパムメールの踏み台とウイルスについての対策を考えてみる。

まず、スパムメールの踏み台は、メールの受信／中継を制限できるメールソフトを選択する、あるいは、バージョンアップすることで完全に防ぐことができる。具体的には、他サイトから送信された自サイト宛でないメールの受信を拒否するように設定できるメールソフトを選択することである。しかし、E-Mail爆弾を大量に送りつけられることを完全に防ぐことはできないのである。既知のスパム専門サイトからのメールはすべて拒否することしか打つ手がないのが現状である。スパムサイトの追跡という観点から、アクセスログを採取することは最低限行うべきことであると考えられる。

一方、ウイルスに感染しないためには、ウイルス対策ソフト（ワクチン）によってシステム全体をカバーし、ワクチンは随時最新バージョンにアップデートしていくことが基本である。しかし、ウイルス対策ソフトは既知のウイルスにしか有効でないという弱点がある。したがって、運用面における対策は必須であり、その対策には次のようなものが挙げられる。

・万一のウイルス被害に備えるために、定期的にデータのバックアップを行う。
・ウイルスの兆候を見逃さないようにし、ウイルス感染の可能性が考えられる場合はウイルス検査を行う。
・メールの添付文書はウイルス検査後に開く。
・ウイルスが感染している可能性のあるファイルを扱うときは、マクロの自動実行は行わない。
・外部から持ち込まれたフロッピーディスクおよびダウンロードしたファイルは、ウイルス検査後に使用する。
・コンピュータ共同利用時の管理を徹底する。

これらの運用面における対策を行っていれば、かなりの確率でウイルスによる被害を防ぐことができると考えられる。

3．事例③「ソーシャルエンジニアリング」

（1）事件

ある保険会社（仮にA社とする）の産業スパイが、同業種の競合会社である保険会社（仮にB社とする）のコンピュータに対して不正アクセスを行い、新商品開発情報や顧客情報を入手した。A社ではその情報をもとにB社に先駆けて新商品を発表、その広告効果は非常に大きくヒット商品となった。B社はその後新商品を発表したが、後発商品として特に目立つことはなかった。また、入手した顧客情報を利用し、B社に関する虚偽情報（経営が危ない、アフターサービスが良くない等）を営業活動の中で顧客に与え、保険の乗換をすすめた。顧客からの情報の伝達は早いもので、B社の解約高は急増し、社会的信用にまで影響を及ぼした。

（2）検証

今回の事件では不正アクセスが行われていたことは明らかである。つまり、何者かが、ユーザＩＤやパスワードを取得していたのである。ところが、Ｂ社では最新の技術を用いて、ネットワーク上での盗聴や漏洩を完全に防御している。そこで浮上してくるのが「ソーシャルエンジニアリング」である。

（3）ソーシャルエンジニアリング

ハッキングや、クラッキングなどの技術的な方法を使わずに、誘導尋問や、なりすましなどで相手のユーザＩＤやパスワード等の情報を取得することをソーシャルエンジニアリングと言う。例えば、プロバイダに成りすまして情報を聞き出したり、逆に本人になりすまして、プロバイダから聞き出すことで取得する。また、ユーザＩＤ・パスワード等をメモに書いてパソコンに貼ったり、机上に置いてあったりすることで、第三者が認証情報を知りうることもある。

今回の事件では、相手先不明の電話が複数の社員にあり、会話の流れから職員情報を話してしまったことが明らかになった。

（4）対策

事例①や②のように、コンピュータに関する技術的な手段に対しては、技術をもって制することが可能ではあるが、ソーシャルエンジニアリングはユーザに対する教育しかない。

・基本的なセキュリティ事例を教える
・組織内で普通に使われている情報（すぐに知り得る情報）を認証に使用しない
・定期的に認証情報を変更する
・実際にソーシャルエンジニアリングをしかける（訓練）　　等

ソーシャルエンジニアリングという言葉自体が最近になって耳にするようになったが、コンピュータに関する専門知識の必要がなく第三者は認証情報を取得することが可能であることに注目したい。今回の事例③は実例ではないが、米国を含め諸外国ではソーシャルエンジニアリングを巧みに利用した事件が多数起こっており、その影響も大きい。日本でも起り得る事件である。

４．技術一覧と防御範囲

このようにネットワークへの不正アクセス事例についてはあらゆる技術対策を講じて、防御を行なっているが、その対策を施すだけでは十分ではない。ここでは一般的な技術一覧とその防御範囲を表Ⅲ―１と共に再度振り返ってみることとする。

まず、ファイアウォールであるが、これはサーバへのダイレクトアクセスを防止するものだが、なりすまし等をされた場合、防御自体は不可能である。

次に認証であるがこれは通信者や通信サーバ自体の特定化によるアクセス制御であるが、この技術もなりすまし等を行なうと攻撃が可能である。

暗号化は公開鍵方式やＳＳＬの発展により、データ復元はほぼ不可能なレベルに達しているが、これはデータ・ファイル転送時の防御作成でありアクセス権限への防御は不可能である。

ＶＰＮはトータルサービスの中で暗号化技術やファイアウォールを包含しており、暗号化・ファイアウォールと同様のリスクを保有しているといえる。

ワクチンソフトは不特定者からのメール・実行ファイル防御を実施しているが、次々とそれを超えるウイルスが作成されるため限界性がある。

現実的にはこれら複数技術の組み合わせとソーシャルエンジニアリング教育の組み合わせにより強固なネットワークを守っていくことが必要である。

区分	技術名	技術定義と防御範囲
アクセス制御	ファイアウォール	インターネットの外部と企業内ネットワークの接点において一定基準以外のデータ通信制御を排除するセキュリティ機能。企業内ＬＡＮにある重要データを守る関所的な役割を担うが、なりすましを行うと、不正アクセスすることは不可能ではない。
	認証	インターネット上は通信先の相手や相手先サーバは不特定であり、その相手との商取引が安全かどうかが定かでない。そこで認証機関への申請通りの識別名を持つユーザ・サーバのみ通信アクセスを許可するもの。現在のインターネット普及に伴い、日本ベリサイン等認証機関自体も発展しつつある。但しこの技術も、なりすましを行うと、不正アクセスを完全防御することは不可能である。
データ保護	暗号化	データ通信時にネットワーク上でのハッキングを防止する為、素データに一定の乱数による変換を行って暗号化を行い、ハッキングしたものには復号化手順がわからない限り解読できないようにする技術。利用者が広く使える仕組みとして復号化情報を公開する公開鍵方式やＳＳＬ（Secure Sockets Layer：ＷＥＢサーバやブラウザ上に通信を暗号化する仕組みを組み込みユーザ側が意識せずに暗号を利用できる仕組み）が普及しつつあり、コード復元自体はほぼ不可能となっている。但しこの技術はデータ転送時の技術であり、特定ホームページの閲覧等アクセス制御は不可能である。
	ＶＰＮ	通常、企業は重要データを送受信するとき、専用回線を利用する。一方、このＶＰＮは公衆回線を利用しながらも専用回線に近い安全性を保持するセキュリティ機能を持つ統合サービスである。そのサービス内に上記ファイアウォールや暗号化技術が取り込まれている。
ウイルス対策	ワクチンソフト	メール送信時に実行ファイルを添付し、それを開かせることによりコンピュータ内の制御を狂わすといったウイルスを感知し、ユーザ側への観戦を防止する機能。但し、既知のウイルスへの対抗しかできない為、常に最新ソフトへの更新等新種のウイルス対策がつきまとう。

表Ⅲ－１．技術一覧

Ⅳ．保険業界におけるネットワーク開放リスク

１．他の金融業界におけるインターネット業務

保険業界におけるインターネット適用業務について説明する前に他の金融業界ではどのような業務がインターネット業務として提供されているのか、銀行・証券・投資信託の３つの業界についてそれぞれ調査した。

（１）銀行

銀行業界では振込に関しては事前に対象口座を登録している通常の振込と事前登録のない口座への都度指定振込が提供されている。また照会業務では入出金明細や振込入金明細、残高照会についても利用することができる。その他各種案内やローンのシミュレーション等が提供されている。

（２）証券

証券業界では株式売買手数料完全自由化という世間動向を反映して各社による多種多様なサービスが提供されている。売買注文等の手続業務のみならず、照会業務についてもサービスは充実している。

（３）投資信託

投資信託業界では、買付や解約、出金などの他にスイッチングと呼ばれる手続業務が提供されている。また照会業務では、注文照会や残高照会の他に取引経過を確認することもできる。

業界名	業務種類	サービス内容
銀行	振込・振替	当行本支店宛、他行宛、振込予約
	都度指定振込	事前登録のない口座への振込
	照会	入出金明細、振込入金明細、残高照会
	その他	各種案内、資料請求、ローン関連、住所変更
証券	売買注文 注文取消	株式売買注文 株式注文取消
	買付申込 解約申込	各種投資信託申込 各種投資信託申込
	注文約定照会	注文内容（契約）の照会
	株価照会	上場株式（東・大・名証）、店頭株式、上場ＣＢ（東・大証）、 主要指標・先物、投資信託
	その他	預かり明細照会、取引履歴照会、利用状況紹介、資産評価、掲示板
投資信託	買付・解約	投資信託買付、投資信託解約
	スイッチング	投資信託スイッチング
	注文取消	投資信託注文取消
	出金	出金申込
	照会	注文照会、残高照会、取引経過確認

表 Ⅳ－１．他の金融業界におけるインターネット業務

各業界とも様々なインターネット業務、インターネットサービスが提供されている。今後もインターネットの普及に伴い、その種類と数は増えていくと考えられる。

２．保険業界における個人データの取り扱い

前節では、保険業界以外の金融業界におけるインターネット適用業務について触れたが、ここでは保険業界の業務に入る前に、保険業界で取り扱うデータがどれほど重要なものかを述べる。

（１）データ保護のための指針

コンピュータを利用した情報処理と通信技術の飛躍的な進歩により、データの大量かつ高速な処理が可能になるとともに、データベースとネットワークの融合により、広域かつ即時のデータ

利用が一般化した。このような情報システムの進展に伴い、個人データ保護に関する世間の関心も高まり、主要国においては個人データ保護に関する法制化も含めた何らかの国レベルの措置がとられている状況にある。

このような状況の中で、業務の性格上多くの個人データを取り扱う金融機関等が、昭和６２年３月、ＦＩＳＣ（財団法人金融情報システムセンター）を中心に「金融機関等における個人データ保護のための取扱指針」を策定した。なお、この指針はその後の国際的な個人データ保護動向を踏まえ、一層の趣旨徹底を図るため、平成１１年４月に大幅な改訂が行われた。

保険業界においては、個人の生活保障にかかわる制度の特性上、契約関係者に関する医的情報をはじめ種々の個人データを大量かつ長期にわたって保有し、利用する必要があることから、業界としては個人データ保護に従来から問題意識をもって対応を図ってきた。そのうえで、ＦＩＳＣによって策定された指針を保険業における個人データ保護取扱いの基本方針として積極的に受け入れ、業界全体で守るべき指針として位置付けることとした。

・生命保険業界の場合

『生命保険業における個人データ保護のための取扱指針』

（社団法人　生命保険協会　策定）

・損害保険業界の場合

『損害保険業における個人データ保護のための取扱指針』

（社団法人　損害保険協会　策定）

（２）保険業界で取り扱う個人データの特徴

保険業界はその提供する商品・サービスの特性から、取り扱う個人データに関し、次のような特徴がある。

・データの長期性および多様性

個人の生涯にわたる保障のため個人情報を長期に保有する

顧客のさまざまなニーズに対応するため幅広い情報を保有する

・データの大量性

保険数理に立脚した保険制度に由来するデータを大量に保有する

・審査情報の存在

保険制度の健全性，公平性を維持するために各種審査情報を保有する

ＦＩＳＣによって策定された指針はすべての金融機関を対象に定められたものであり、保険業界としてはそれに準拠しつつ、上記のような保険業界の特性を踏まえた具体的な取扱指針を自主的に策定することとした。

次に、保険業界で取扱うデータを種類ごとに細かく分析する。生命保険業界・損害保険業界それぞれ分けて考えると表Ⅳ－２、表Ⅳ－３のようになる。

①募集データ	氏名、住所、電話番号、性別、生年月日、家族構成、加入状況　など
②契約データ	氏名、住所、電話番号、性別、生年月日、引去口座、保険金額、 保険期間　など
③審査データ	健康状態、病歴、入院・通院歴、身体障害、債務状態、財産、 審査結果　など
④企業データ	企業名、所在地、電話番号、決算報告　など

表 Ⅳ－２．生命保険業界の保有データ

①契約データ	氏名、住所、電話番号、性別、生年月日、引去口座、保険金額、保険期間　など
②保険金支払いデータ	障害・後遺障害の内容、支払額・支払日・支払先等保険金支払に関するデータ、履行遅滞発生日等の信用情報　など
③財務データ・カードデータ	債務状態、財産、収入状況、評価および審査結果データ　など

表 Ⅳ－３．損害保険業界の保有データ

氏名・住所・電話番号といったデータは金融業界では共通で保有しているデータであるが、生命保険業界においては、募集データの中の家族構成や保険の加入状況、契約データの中の保険金額、審査データの中の健康状態や病歴・入院歴は業界特有のデータである。また、損害保険業界においても、保険金支払データの障害・後遺障害の内容、履行遅滞発生日等の信用情報が業界特有のデータといえる。このように、保険業界においては、他の金融業界に比べ個人のプライバシーに関わる重要な情報を保有しており、そのデータの取扱いには細心の注意を払う必要がある。

３．現行業務のリスク分析

現在保険業界で行われている業務についてどのような危険性が存在するかみるために、業務を大きく９つ、ネットワーク上での危険性（脅威）を５つに分類し、分析する。

		脅威				
		なりすまし	漏洩	盗聴	改竄	破壊
業務種類	商品案内	－	－	－	○	○
	顧客相談	－	○	○	○	○
	資料請求	－	○	○	○	○
	設計	－	－	－	△	△
	申込	○	○	○	○	○
	入金	○	○	○	○	○
	照会	○	○	○	○	○
	保全	○	○	○	○	○
	支払	○	○	○	○	○

○：危険性があり、影響が大きい
△：危険性があるが、影響は小さい
－：危険性無

表 Ⅳ－４．現行業務と想定される脅威

以下に各業務に関して、ネットワーク上を流れるデータ、およびその危険性を示す。

・商品案内

保険会社からの情報提供であり、顧客の情報がネットワーク上を流れることはない。ただし、サーバ側の情報の改竄、破壊により誤った情報提供がされる危険性がある。

・顧客相談

顧客はプライバシーに関する情報を流す可能性があり、また、相談に対する回答で誤った情報を与えてしまう危険性がある。

・資料請求

発送に必要な顧客情報（住所等連絡先）がネットワーク上を流れ、また、第三者が保険会社に

なりすまして顧客情報を得る危険性もある。

・設計

保険の契約ではないため、直接影響はないが、この設計をもとに契約を左右すると言った意味では改竄破壊の危険性は存在する。

・申込

顧客の情報だけでなく、今後ネットワーク上での処理に必要な顧客自身のパスワードがネットワーク上を流れる。もし、この情報が漏れてしまえば、契約している保険に関して本人の知らない間に様々な処理が行われてしまう危険が存在する。

・入金

入金口座に関する情報がネットワーク上を流れ、本人の知らない間に第三者により保険がかけられたり、第三者の保険料の引去りが勝手に行われる危険性がある。

・照会

保険契約内容が勝手に第三者に漏れる。

・保全

本人の知らない間に、契約者貸付が行われたり、口座変更をされ祝金、満期保険金を盗まれる危険性がある。

・支払

第三者が勝手に保険金を請求し、他人の口座に振り込まれる危険性がある。

他の金融業界ほど多種多様な業務処理を提供していないが、前節で述べた保険業界のデータの重要性と業務処理内容から判断すると、セキュリティが破られた時の影響がいかに大きいかが推察できる。

４．将来業務のリスク分析

次に保険業界において、将来インターネットで開放が想定される適用業務のリスクを、現行業務のリスクと比較･分析する。

（１）４０１ｋ業務の特徴

ａ．将来業務として４０１ｋを選定した理由

わが国ではいま、２１世紀に向けた年金制度の改革が進められている。少子化、高齢化社会を迎えて、わが国の公的年金制度は、現在のままでは２１世紀には破綻の危機に瀕することは目に見えており、給付開始年令の引き上げや給付額の実質的削減などが検討されている。公的年金を補完する企業年金も財政難は深刻さを増している。低成長経済への移行や労働市場の流動化など企業を取り巻く環境の大きな変化によって、企業は年金給付に支障を来したり、年金基金が解散に追い込まれるところも出てきている。

このような企業年金の深刻な問題を解決するひとつの有力な方策として注目されているのが、米国で行われている確定拠出型の年金であり、とりわけ４０１ｋプランといわれる企業年金プランの日本への導入に、官民あげて検討が進められている。

今回、将来業務のリスク分析を行うにあたり、４０１ｋを例に挙げる理由は、複数の企業が提携して４０１ｋ共同センターを設立して業務を提供することが想定され、このことがインターネットを利用するのに最適であり、現行業務とは異なったネットワークを構成されることが確実であるからである。

ｂ．４０１ｋの提供業務

４０１ｋでは、表Ⅳ―５の業務開放が予想される。

外部系インターフェース業務、内部管理業務は一般的であるが、業界間連動業務については４０１ｋの特徴ともいえる。

外部系インターフェース業務		
	移行ｺﾝｻﾙﾃｨﾝｸﾞ業務	確定給付→確定拠出への移行サービス
	コールセンタ業務	(対従業員)電話情報照会・電話属性変更・電話預替・ その他サービス
	インターネット業務	(対従業員)情報照会・属性変更・預替・その他サービス (対事業主／基金)情報照会・属性変更
内部管理業務		
	確定給付／確定拠出統合サービス業務	・収納統合、給付統合、ディスクローズ統合 ・確定給付システム(税制適格年金・厚生年金基金) ・確定拠出システム 運営管理業務:実際の契約／制度情報を管理 資産管理業務:実際の入出金管理情報などを管理 資産運用業務:運用先情報・レコードキーピング管理
業界間連動業務		
	情報交換業務	共同保険(単・幹・非)などで必要となる保険業界交換情報ｲﾝﾀｰﾌｪｰｽ 信託・投信業界との交換情報ｲﾝﾀｰﾌｪｰｽ

表 Ⅳ－５． ４０１ｋの提供業務

（２） ４０１ｋ業務と想定される脅威

表Ⅳ－６のとおり、想定される脅威は前述の現行業務と同様であり、どの業務にも脅威が潜在化していることがわかる。

		脅威				
		なりすまし	漏洩	盗聴	改竄	破壊
業務種類	外部系インターフェース業務					
	移行コンサルティング業務	○	○	○	―	―
	コールセンタ業務	○	○	○	―	―
	インターネット業務	○	○	○	○	○
	確定給付／確定拠出統合サービス業務	○	○	○	○	○
	内部管理業務					
	確定給付システム	○	○	○	○	○
	確定拠出システム					
	運営管理業務	○	○	○	○	○
	資産管理業務	○	○	○	○	○
	資産運用業務	○	○	○	○	○
	業界間連動業務					
	情報交換業務	○	○	○	○	○

表 Ⅳ－６． ４０１ｋ業務と想定される脅威

（3）４０１ｋのネットワーク

図Ⅳ－１のとおり、４０１ｋでは、複数の企業が提携して業務開放することが可能であり、そのため、同一ネットワークに共同センタと他社が存在する。

図Ⅳ－２の現行業務ネットワークに比べ複雑になっていることが一目でわかる。

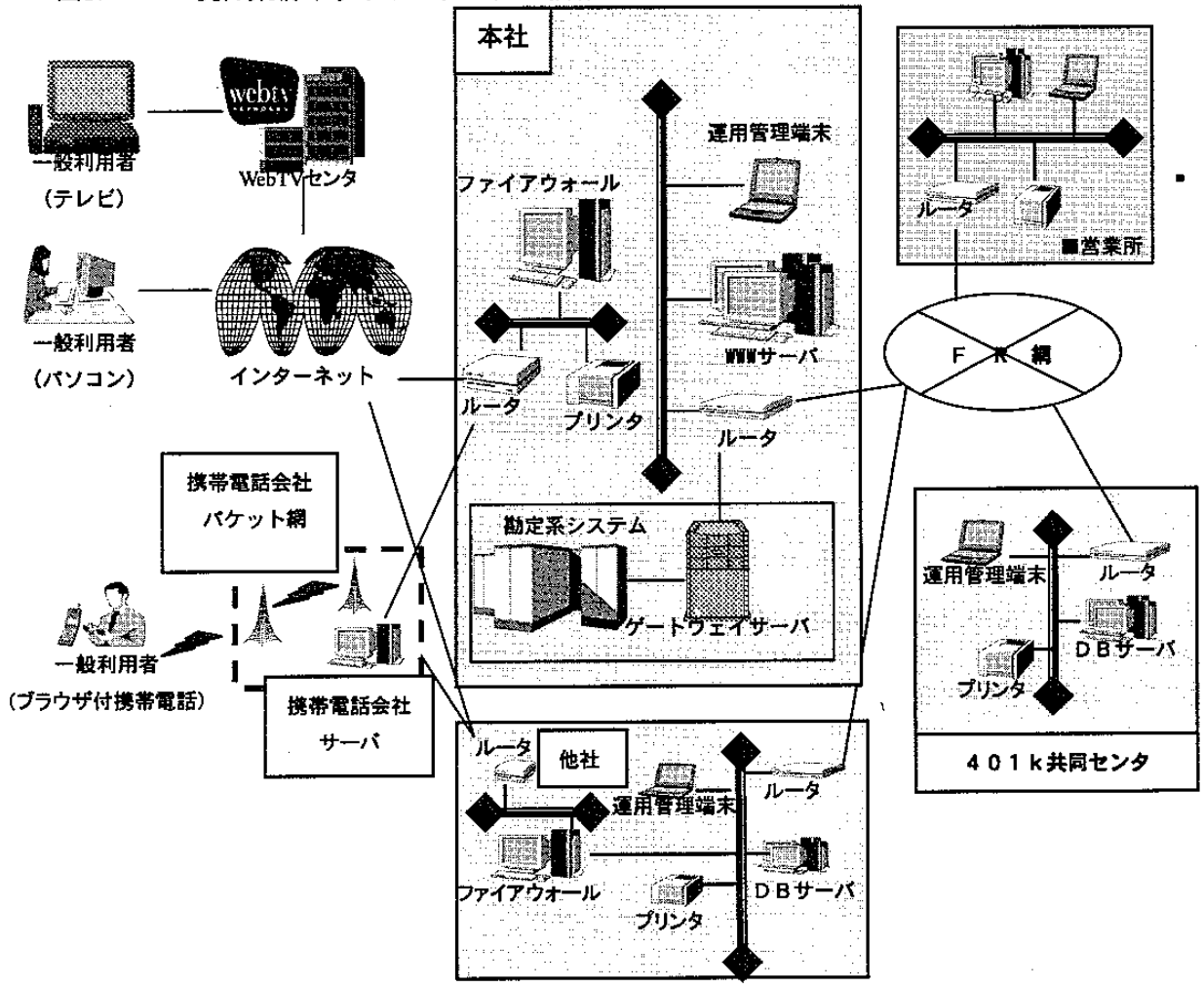

図 Ⅳ－１．４０１ｋのネットワーク

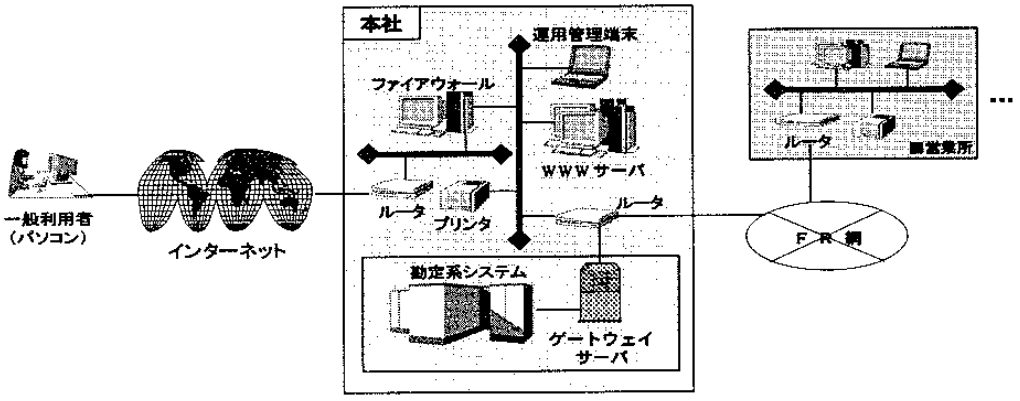

図 Ⅳ－２．現行業務のネットワーク

（4）４０１ｋ業務のリスク分析

ａ．Ａ生保のセキュリティが打破された場合に発生する風評リスク

４０１ｋ業務において、Ａ生保のセキュリティがハッカーにより打破された場合のリスク分析を行う。

Ａ生保のセキュリティが打破され、Ａ生保の顧客データが漏洩	
↓	
Ａ生保の信用力低下による顧客離れ	（信用リスク）
↓	
提携しているＢ銀行、Ｃ信託銀行、Ｄ投資信託も危ないという噂	（風評リスク）
↓	
提携しているＢ銀行、Ｃ信託銀行、Ｄ投資信託の顧客離れ	（信用リスク）
↓	
提携している全企業の業績悪化	（業績リスク）

上記例のとおり、Ａ生保のセキュリティが打破されることにより、提携している企業全体に影響が波及する。それが、たとえＢ銀行、Ｃ信託銀行、Ｄ投資信託のセキュリティ対策が確実なものであり、３社のデータが漏洩することがなくても、一般利用者、マスコミによる噂による風評リスクは発生する恐れが高い。このリスクは、現在世界中で話題となっている西暦２０００年問題で発生する恐れのあるリスクと同種のものである。

このように、これからの金融業界における業務においては、自社のセキュリティのみを意識していれば良い状況ではなく、提携している企業のセキュリティ対策も意識しておく必要がある。

ｂ．現行業務との比較

表Ⅳ―７のとおり、現行業務と４０１ｋ業務で脅威が発生した場合の大きな違いは二点挙げられる。

一点目は、脅威により、影響を被る対象が現行業務では単一企業であるが、４０１ｋ業務では複数企業であること。

二点目は、４０１ｋ業務では風評リスクという新たなリスクが発生すること。

このように、現行業務では特に注意する必要がなかったが、これからの業務の中では、他社のセキュリティ対策を意識することが必要であり、今まで以上にセキュリティ対策が重視される。

業務	発生脅威	影響対象	発生リスク
現行業務	データ漏洩	単一企業	信用リスク
	データ改竄　等	顧客	業績リスク
401k業務	データ漏洩	複数企業	信用リスク
			風評リスク
	データ改竄　等	顧客	業績リスク

表 Ⅳ－７．現行業務と４０１ｋ業務の比較

（5）将来想定されるインターネット業務

保険業界において、４０１ｋ以外に将来想定されるインターネット適用業務を挙げる。

・病院ネットワーク（給付金支払い）
・対企業収納事務ネットワーク
・送金、決裁ネットワーク
・顧客通知ネットワーク
・陸運局、警察（役所関連）ネットワーク

前節でも述べたが、４０１ｋをはじめ様々な業務がインターネットで開放され、新たなネットワークを構築する場合は、風評リスク等現行業務では想定されないリスクが発生することになる。つまり、保険業界においてもにセキュリティ対策を今以上に重視する必要があるということである。

Ⅴ．基本設計書とライフサイクルセキュリティ

セキュリティ対策は、企業のポリシーが重要である。情報システム部門だけでなく、企業のトップ主導で行うべきである。そういう意味でも、先に述べたとおり２０００年問題とよく似ている。経営層主導のもと、企業全体がしっかりとしたポリシーを持って実行に移さないと、企業の存続にも関わる問題にも発展しかねないのである。

そこで本章では、まず基本設計書について、次にライフサイクルセキュリティについて述べる。

１．基本設計書の重要性

まず基本設計書とは、どのような業務について、何を保護し、そのためには何が必要かを定義するものである。

インターネットに接続するということは、世界中どこからでも侵入される恐れが出てくることを意味する。そこでシステムの安全性について、世界標準の物差しとなるものが必要となり、コモンクライテリアをはじめとしたセキュリティ評価基準が各国共同で策定された。コモンクライテリアとは、ＩＳＯにより策定された国際標準の評価基準である。この評価基準に基づいて、セキュリティ対策についての方針をまとめた資料が「基本設計書」である。

基本設計書が適切でないと、例えばセキュリティが弱くて重要なデータを盗まれてしまったり、セキュリティが強すぎて使い勝手が悪くなってしまう恐れがある。また、他社システムと接続を検討する場合、リスクが大きいため他社が接続を見送るといったことも考えられる。複数の企業が関わる４０１ｋシステムの場合、これは致命的となるであろう。

以上のことから、企業の存続にも関わる基本設計書の作成は、企業のトップ主導で行うべき重要課題であることを十分認識する必要がある。

２．基本設計書の作成手順

「Ⅱ．セキュリティの概要」の中で説明したように基本設計書の作成手順として、下記のとおり７項目が挙げられる。ここでは各手順について、順を追って詳細の説明を行う。

・基本設計書の作成手順
（１）保護すべき資源の明確化
（２）保護すべき資源の利用規則を決定
（３）脅威の見極め
（４）セキュリティポリシーの決定
（５）機能要件と品質保証レベルを選択
（６）評価対象の仕様や開発手法の決定
（７）基本設計書の内容を検証

（１）保護すべき資源の明確化

まず１番目に、保護すべき資源を明確にする必要がある。ネットワークシステムに対する脅威を分析するためには、ネットワーク構成とそのネットワークに接続されている資源を洗い出す必要がある。具体的には、ネットワークを利用している業務処理とその使用資源を調査する。

まず、物理的なネットワーク構成と、そのネットワークに接続されている資源を調査する。資源とは、セキュリティ対策が施される単位でもある、各種サーバやデータベースを想定する。また資源の用途だけでなく、ＩＰアドレスや搭載ＯＳ、管理者についても調査しておく必要がある。そして、調査した結果はネットワーク構成図としてまとめておく必要がある。

この調査において重要な点は、企業が保有するもの全てを洗い出すことである。特に外部ネットワークとの接続点は全て把握しなければいけない。

物理的なネットワーク構成と、
そのネットワークに接続されて
いる資源を調査

調査項目
- ネットワーク構成とアドレス
- 各種サーバと管理者
- ルータやアクセスサーバなど
  外部との接続点

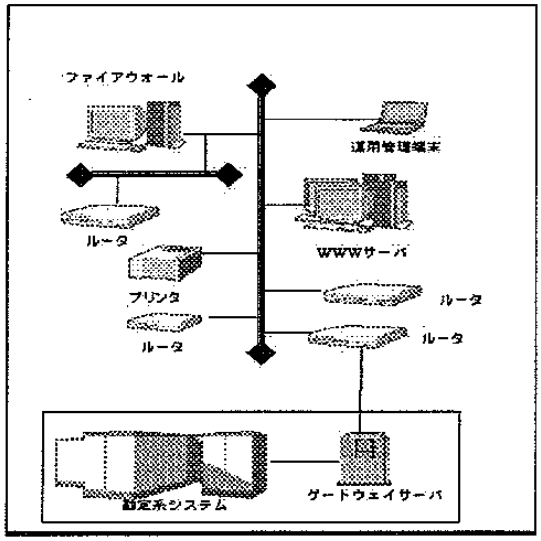

図 V－1．ネットワーク構成と資源の調査

次に、ネットワーク上で稼動している業務処理と、その使用資源を調査する。この目的は、洗い出した使用資源がどのように利用されているかを把握し、リスク分析の基礎情報とすることにある。特に注意が必要な点は、重要データの処理や外部ネットワークから処理される資源について洗い出すことである。この中では利用者の調査として、その業務の利用者を調査する。例えば、あるシステムについて、それが特定の部署の部員のみが利用する業務か、全従業員が利用するのか、あるいは社外へも公開した情報なのかを明確にする。次に利用環境の調査として、内部ネットワークのみからの利用なのか、あるいは、インターネットやモバイル端末により、社外ネットワークから利用するものなのかを調査する。また使用資源の調査として、業務処理アプリケーションが使用している資源、つまりサーバを調査する。これらの調査結果を前述したネットワーク構成の調査で洗い出したサーバと関連付ける。

（2）保護すべき資源の利用規則を決定

2番目に利用者が、保護すべき資源を利用する際の利用規則を決めておく必要がある。具体的には、「利用者の役割や責任範囲」、「保護すべき資源の導入・更新・運用・保守方法と責任の所在」、「組織内部の規則」の3点について決定しなければならない。

この中で、「利用者の役割や責任範囲」とは、システム管理者や運用担当者が、保護すべき資源であるプログラムやデータ等に対して、どのような役割と責任を持つか、ということになる。例えば『システム管理者はプログラムやデータを自由に利用できる。また、システム管理者が不正を行った場合には、直属の上司が責任を負う。』といったような規則を決める。次に、「保護すべき資源の導入・更新・運用・保守方法と責任の所在」とは、例えば『プログラムの保守は、システム管理者が決められた時間に、決められた手順に従って行う。保守に関する全ての責任はシステム管理者が負う。』といったようなことを指す。最後に、「組織内部の規則」とは、各企業が規定している従業員規則のうち、セキュリティに関連するもの等が挙げられる。

（3）脅威の見極め

ここでは、資源に対して想定される脅威ごとにリスクを分析し、セキュリティポリシーを決定する上での指針とする。保護すべき資源に対して想定される脅威は、資源に直接被害を与える可能性のあるものを網羅的に挙げることが重要である。誰、あるいは何が、いつ、どこで、どのような脅威を引き起こす可能性があるか、という点について具体的に分析する。脅威には、他人へのなりすまし、データの破壊や改竄、あるいは、システムが提供するサービスの利用妨害等が挙げられる。

（4）セキュリティポリシーの決定

これまでに行った脅威の洗い出しや現状のセキュリティ状況の調査は、いわば情報収集であり、セキュリティ環境を構築するための準備作業である。具体的なセキュリティ対策・ガイドライン・セキュリティに対する投資額などを決定するために、まず企業全体でセキュリティに対する意識統一を行い、セキュリティポリシーを決めておくことが重要である。

セキュリティポリシーを決定するには、企業のネットワークやコンピュータシステムに関わる全ての要素について「何から何を守るのか」という点を「不正アクセス」、「不正プログラム」、「セキュリティモラルの低下」、「ネットワーク上のデータセキュリティ」といった観点から検討しなければならない。特に、重要データや外部ネットワークからの処理に対しては注意深く検討する必要がある。

また、セキュリティポリシーにはデータの暗号化やアクセス権限の設定といった技術的な対策と、従業員規則やエンドユーザ教育といった運用規則による対策が挙げられる。このような技術的な対策と運用規則による対策のどちらを選択するのかという観点の他に、どの時点で対策を施すかという観点が重要になる。

ここで具体的なセキュリティポリシーの一例を表Ⅴ－１に挙げる。

対象	想定される脅威	セキュリティ方針			
		抑止	予防	検出	回復
記憶媒体上のデータ	正当な利用者以外の人間が業務システムのデータを参照・変更・削除・追加	業務システムや端末の使用を制限	データに対するアクセス権限を設定	ログの監視・データの改竄を検出・データのシーケンス番号を管理	データのバックアップやリストアを実施
	暗号化したデータの秘密鍵を紛失してデータを復元できない	暗号秘密鍵の管理			暗号秘密鍵の復旧
通信回線上のデータ	通信回線上のデータを盗聴・破壊	通信回線そのものの保護やネットワーク機器の管理	暗号化によるデータの盗聴防止	データの改竄を検出	データを再送
業務処理	データを送受信した事実や内容を否認	運用規則を明確化	証拠保管などによる否認防止		
	原データを否認	データに証明書をつけるなど運用規則を明確化			
	コンテンツの改竄・破壊	コンテンツの作成やダウンロードを管理	コンテンツの利用権限を設定	コンテンツの改竄を検出	コンテンツのバックアップ
システム	プログラムのセキュリティホールをついてセキュリティの機能を無効にする	プログラムに対する高い品質保証レベルを設定			
	業務処理の途中で正当な利用者が離席し、その間に正当な利用者以外の人間がシステムを利用	再認証などによる離席時の対策			
	ウイルスの侵入	外部からのデータやプログラムの持ち込みを禁止。新規ソフトの導入を管理	ダウンロードするプログラムやファイル、電子メールの添付ファイルのウイルスをチェック	システムの利用ログを監視	システムを停止、外部システムへの接続を切断
	外部からシステムへ不正侵入	システムの接続機器や接続先を管理	システムのログイン時に利用者を識別・認証、システムに対するアクセス権限を設定	システムの利用ログを監視	
利用者	正当な利用者以外の人間が認証データを盗聴して他人になりすます	認証データを参照できない記憶媒体に格納、アクセス経路の制限、ワンタイム・パスワードの利用	複数の認証機能を採用	システムの利用ログを監視	なりすまされた利用者の処理を停止
	正当な利用者以外の人間が、認証データを推測して他人になりすます	暗号の秘密鍵の鍵長を長くするなど、他人に推測されにくい認証データを採用	認証の試行回数を制限、有効期限を設定	システムの利用ログを監視	なりすまされた利用者の処理を停止
	認証データの偽造によって他人になりすます	信頼できる認証機関を利用	認証データに対するアクセス権限を設定、認証データの正当性を検証	認証データを偽造された利用者を早期に発見	
監査	監査者が利用者のログを改竄	ログの変更を禁止	監査者のログに対するアクセス権限を設定	監査業務の実行ログを監視	ログの自動バックアップを実施
	ログの内容が不十分で監査できない	ログ収集のタイミングやログの内容を規定			

表 Ⅴ－１． 脅威とそれに対するセキュリティポリシーの一例

ここでの「抑止」とは、脅威そのものを発生させないようにすることである。脅威が発生する元になる機能の利用を制限、または禁止したりする。これに対して「予防」とは、脅威が発生する可能性のある場合に、不正行為を阻止することである。また「検出」とは、保護すべき資源に対するアクセス履歴などを監視して、問題の発生を発見することである。最後に「回復」とは、セキュリティ上の問題が発生した後で、元の安全な状態に復旧することである。

ただし、セキュリティポリシーの決定には利用者の利便性やコストを考慮することも必要である。セキュリティレベルの向上だけを追求すると利便性が犠牲になり、結果として利用者が使用し難いシステムになってしまう、あるいは、コストがかかり過ぎてしまうといった問題も生じてくる。

（5）機能要件と品質保証レベルを選択

機能要件とは、セキュリティポリシーを実現するために必要となるセキュリティ機能のことを言う。コモンクライテリアでは表Ｖ－２のように、全部で１１の機能要件がある。基本設計書に記述する機能要件は、下表の中からセキュリティポリシーと照らし合わせて、開発者が必要と思うものを選択すれば良い。

ユーザデータの保護	企業が保有するデータに対して、利用者のアクセス権限を設定し、利用範囲を限定できること。ネットワークを流れるデータの盗聴や改竄を防止し、検出できること。電子商取引では、データの中身が正しいことを証明できること。
利用者の識別と認証	利用者個人を一意に識別できること。利用者を特定する必要がある場合は、できるだけ早い時点で正当な利用者かどうかを確認できること。確認に使用するパスワードや暗号鍵などの秘密情報が盗聴されたり、簡単に推測されないこと。
セキュリティプログラムの保護	製品やシステムに組み込まれたセキュリティプログラムが正常に動作しているかどうかを確認できるだけでなく、セキュリティプログラムが破壊されても資源の不正利用に対処できること。初期起動時や障害復旧時にセキュリティプログラムを初期化するフェイルセーフを正しく実行できること。
データやプログラムの利用	製品やシステムを安全に運用するために、特定のプログラムやデータがプロセッサや主記憶を占有して、他のプログラムやデータの処理を妨害しない様にすること。
製品やシステムの利用	製品やシステムの不正利用に対処できること。正当な利用者に他人がなりすます場合に備えて、不正を容易に検出できる環境を備えること。利用者が離席した時に行なわれる不正への対策も施していること。
通信路	セキュリティプログラムと利用者との間で、安全な通信を保証できること。利用者の認証やアクセス権限に関するデータが、不正なプログラムによって盗聴されたり、改竄されるのを防ぐ。
セキュリティ通信	契約書などの重要データをネットワーク経由でやり取りする場合に、データを送受信した事実やデータの中身の正しさなどが通信相手に否定されないこと。
利用者のプライバシ	利用者のプライバシーを保護するために、利用者が匿名を指定したりペンネームを使用できること。インターネットショッピングなどで利用した仮想店舗や、購入した商品が他人に知られない様にすること。
暗号鍵の管理	暗号鍵の生成や配布、保管を安全に行なうこと。暗号化アルゴリズムは広く公開されているため、暗号鍵が推測されたり盗聴されない様にする。ただし、暗号化アルゴリズムそのものの特定は行なわない。
セキュリティ監査	上記の全ての機能要件を満たすために、セキュリティ機能の動作履歴や保護すべき資源に対するアクセス履歴を漏れなく収集する。これらの履歴によって、製品やシステムがセキュリティ上問題なく動作していることを確認できること。問題が発生した場合は速やかに原因を究明し、対策を施せること。
セキュリティ管理	上記の全ての機能要件を維持・管理するために、利用者やシステム管理者の権限内容の登録・変更や、保護すべき資源の登録・変更を安全に実施できること。

表 Ｖ－２．コモンクライテリアで規定されている機能要件

次に品質保証レベルであるが、コモンクライテリアの中で設定されているセキュリティレベルは「ＥＡＬ１」から「ＥＡＬ７」までの７段階があり、数字が大きくなるに従ってセキュリティ

レベルが高くなる。この中で、一般の企業情報システムに要求される品質保証レベルは「ＥＡＬ１」から「ＥＡＬ５」までになる。「ＥＡＬ６」、「ＥＡＬ７」は軍事システムなどの特別な用途向けとなる。第三者機関の評価者はこの基準に従い、開発者が目標に設定したセキュリティの品質保証レベルを評価対象のシステムが満たしているかどうか評価する。

品質保証レベル	利用する環境	確認項目	評価者が確認する内容
ＥＡＬ１	社内に閉じた環境が保証されている	一般的な機能	メニューやコマンドを使って一般的な機能を確認。「ガイダンス文書」に記述された内容通りの機能を備えているか、想定される脅威に対して有効な対策が施されているかどうかを確認。
ＥＡＬ２	開発者や利用者が限定され、安全な運用を脅かす重大な脅威が存在しない	プログラム構造	開発者が作成した設計書を利用して、プログラムのモジュール構造にセキュリティ上の問題が無いことを確認。開発者が「テスト」のために作成したドキュメントを使ってテスト結果を確認。
ＥＡＬ３	不特定の利用者が存在し、不正行為への対策が要求される	テスト内容	開発者がテストのために作成したドキュメントやプログラムを利用して、「テスト」内容の正当性を確認。開発者から提供される「ぜい弱性分析」の結果や「構成管理」「配布と運用」の各品質保証用件を確認。
ＥＡＬ４	製品やシステムそのものに、最低限のセキュリティが要求される	プログラムの処理の流れ	開発者が作成した設計書を利用して、プログラムの処理の流れにセキュリティ上の問題が無いことを確認。セキュリティ上、特に重要な処理を行なっている部分はソースコードを確認。開発者が行なわなかったテストも実施して、開発者から提供される「ぜい弱性分析」の結果を確認。
ＥＡＬ５	製品やシステムそのものに、コストが許す範囲で最大級のセキュリティが要求される	すべてのソースコード	すべてのソースコードにセキュリティ上の問題が無いことを確認。「ぜい弱性分析」でセキュリティ管理の対象から外れた情報漏洩のルートの存在や影響も確認。
ＥＡＬ６	多大なコストを負担してでも保つべきセキュリティが要求される	設計書やソースコード（ソフトウエア工学による確認）	プログラムの処理の流れやプログラムの構造を検証するためのソフトウエア工学を利用して、設計書やソースコードにセキュリティ上の問題が無いことを確認。高度な知識やツールを利用して外部からの不正侵入に対処できるセキュリティが施されているかどうかを実際にテストして確認。
ＥＡＬ７	最高レベルのセキュリティが要求される	数学的に安全性を証明できる開発手法	数学的に安全性を証明できる開発手法でセキュリティ機能やプログラムを設計したかどうかを確認。

表 Ｖ－３．　品質保証レベル一覧

開発者が品質保証レベルを決定すると、そのレベルに対応した品質保証要件が決まる。この品質保証要件には表Ｖ－４のとおり８つの要件があり、システムの開発者は各レベルの評価内容を理解した上で品質保証レベルの目標を設定し、それを達成できるように開発を進めていくことになる。

例えば「ＥＡＬ４」の品質保証レベルを選択した場合には、品質保証要件の中から「テスト」、「ぜい弱性分析」、「構成管理」、「配布と運用」が含まれることになっている。この場合、特に重要なのは「テスト」と「ぜい弱性分析」である。「テスト」では、システムに外部から侵入できるかどうかを実際にテストすることになる。「ぜい弱性分析」では、プログラムの構造、処理の流れ、操作・運用など様々な側面からセキュリティ機能の強度を分析する。具体例を挙げると、問題が発生した時の対処方法がマニュアルに記載されているか、パスワードなどが盗聴される危険性はないか、等が挙げられる。

品質保証要件	内容
構成管理	製品やシステムを開発・保守するための環境を安全に維持・管理し、プログラムなどが不正に改竄されないようにすること。設計書、プログラムのテスト結果、検出されたセキュリティ上の問題とその対策内容、導入・運用のマニュアルやガイドライン、プログラムのソースコードなどを安全に管理すること。
配布と運用	製品を利用者に配布する際に、改竄などの不正を受けないようにすること。製品を安全に導入・運用できるように手順を明文化し、作業を標準化すること。
開発	製品やシステムを開発する際に作成した設計内容を、プログラムのモジュール構成やソースコードに正しく反映すること。セキュリティ管理のために採用するアクセス権限のチェック方式などを設計書に明記すること。
ガイダンス文書	製品やシステムのマニュアルやガイドラインに、システム管理者と利用者の責任範囲、安全な運用方法、セキュリティ機能の内容などを記述すること。
ライフ・サイクル	製品やシステムの開発から保守までの各工程で必要なセキュリティ対策を明確にすること。セキュリティ上の問題があった場合は、その内容を速やかに正しく利用者に伝え、修正を誤りなく実施するための手続きとそれを確認するための方法を明確にすること。
テスト	製品やシステムのテストを漏れなく実施し、テスト結果を十分に確認すること。
ぜい弱性分析	運用時に発生しうるセキュリティ上の問題を漏れなく分析し、問題を発見したら速やかに対策を施すこと。セキュリティ管理の対象から外した情報漏洩のルートがないことを確認すること。
保守	製品に修正や機能拡張を施したり、システムの構成や業務を変更する場合は、当初規定したセキュリティ機能を遵守し、セキュリティレベルを落とさないこと。セキュリティに影響を与える変更を施す場合は、十分なセキュリティ対策を行なった上で、変更履歴を記録すること。

表 Ⅴ－4． 品質保証要件の詳細一覧

（6）評価対象の仕様や開発手法の決定

ここでは、セキュリティの機能要件や品質保証要件に応じて、システムが備えるべき機能の仕様や、品質レベルを保証するための開発手法を決定する。開発手法とは、開発工程で生産される成果物の管理方法、仕様やプログラムの設計方法、テストの実施方法等を指す。

（7）基本設計書の内容を検証

セキュリティ基本設計書を作成する最後の段階として、今までに決定した作成手順の（1）から（6）までの、全ての内容の正当性や有効性を検証する。そして、検証の結果やその理由をセキュリティ基本設計書に明記することが必要となる。検証作業は、大きく３つの内容について実施する。

１つめは、作成手順の中での（4）にあたるセキュリティポリシーの検証である。個々の脅威に対処するセキュリティポリシーが「脅威を取り除けるか」、「脅威の影響範囲を許容範囲まで軽減できるか」という点について理由を付けて記述する。

２つめは、作成手順の中での（5）にあたる機能要件の検証である。複数の機能要件が互いに補完しあい矛盾がないこと、また他の機能要件を阻害するようなことがないことを検証する。

３つめも作成手順の中での（5）にあたるが、品質保証要件の検証である。目標に設定した品質保証レベルが想定される脅威に対して低くないか、また同時に、品質保証レベルが技術やコストの観点から実現可能であることを検証する。

以上の手順で、基本設計書が作成できる。

3．ライフサイクルセキュリティ

（1）ライフサイクルセキュリティとは

企業では、社内ネットワークに潜在するセキュリティリスクを評価し、リスク軽減や排除に向けた製品を導入しなければならない。そのためにはセキュリティポリシーを中心とした基本設計

書を策定しなければならないことは前節までに述べてきた通りである。ところが、業務環境の変化があまりにも急速であるために、対策が追いつかないのが多くの企業の現状である。なかでも最大の問題は、包括的な社内セキュリティ戦略の欠如である。社内の多様な情報システムやネットワークに必要なセキュリティレベルを提供するには、包括的なセキュリティ戦略を立て、それに応じて具体的な計画を作成する必要がある。この計画が欠けると、管理者は次々に登場するセキュリティ技術に戸惑いながら、その評価と導入をあてもなく繰り返すことになる。これでは、現在直面している新しいセキュリティ問題には対処できない。このような現状を打開する唯一の方法がライフサイクルセキュリティである。

ライフサイクルセキュリティは、全社規模の包括的なセキュリティを実現するための枠組みである。この枠組みによるセキュリティプログラムと手順は、社内ネットワークの動的な性質にも対処できるように設計されている。社内の情報システムやユーザは、追加・変更・削除により絶え間なく変化している。そこで求められているものは、変化の激しい環境において、系統的にセキュリティリスクを管理し、必要な制御を提供できるアプローチである。このようなアプローチをするにあたっては、ライフサイクルセキュリティモデルに従ってセキュリティ対策を実施することが重要である。

（2）ライフサイクルセキュリティモデル

ライフサイクルセキュリティモデルは以下の７つの要素によって構成されている。

①セキュリティポリシー、運用規定、手順、測定基準
- あらゆるライフサイクルマネジメントプログラムに適用される枠組みと基準

②脅威の洗い出しと評価
- セキュリティ管理を確立し維持するための出発点
- 脅威を評価し、攻撃されやすい弱点を明らかにする

③セキュリティロードマップの設計
- セキュリティの実現に向けた系統的な作業が可能になる
- 予算、資源、ベンダーおよび製品の選択をする際に役立つ

④ソリューションの選択と実施
- セキュリティロードマップに従い、製品・サービスを適切に選択できる

⑤教育の実施
- セキュリティの成果が大きく向上する
- 安全なシステム環境の実現と維持に必要な知識が得られる

⑥セキュリティの監視
- セキュリティプログラムの効果を確実にする
- ホストやネットワーク環境への侵入や異常を検知する

⑦問題発生後の対応および回復
- 発生した問題に対処して影響を軽減できる
- 元の状態に回復できる

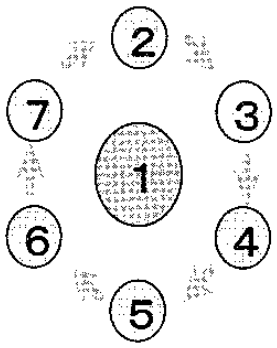

図 Ⅴ－２．７要素の関連

これら７つの要素は、図Ⅴ－２のように「①セキュリティポリシー」を中心として、残りの６要素がサイクリックに繰り返されるのである。このライフサイクルセキュリティモデルのサイクルに従って、定期的に評価とプログラム改良を実施すれば、セキュリティ対策を常に改善することができる。

セキュリティ対策の考え方としては、前節までに述べてきたように、セキュリティポリシーをしっかり持った基本設計書を作成し、ライフサイクルセキュリティモデルに従って常に見直しをかけていくことが必要である。それを怠ると、セキュリティはすぐに陳腐化してしまい、役に立たないものになってしまうのである。

Ⅵ. おわりに

最後の章では、ネットワーク社会がより発展していく中でセキュリティ対策としてまず何を重視していくべきかを論ずることとする。

今後、ネットワーク社会が本格化していく中での経営課題はまず何が挙げられるであろうか。それはビッグバン時代の中、どの業界も新商品・新サービスをインターネットに搭載していく流れが顧客ニーズ・競争力向上の観点から不可避になってきていること、いわばインターネットによる業務開放が優先的経営課題としての位置付けになってきていることである。当然、今後数年間において情報システム部門におけるインターネット業務搭載要望の開発が大幅増加していくことが想定され、この要望を円滑に引き受けておくことが各企業において業務命題になってくる。一方で、今までの章で記述してきたようにネットワークの開放は、自社のシステムをリスクの脅威にさらすことを覚悟しておかなければならない。また、今後のリスクヘッジ観点は、「連鎖影響への防御策」を講じることが今までのリスク管理に加えて考慮していく必要があり、セキュリティポリシーの作成を行なうことがますます重要になってくることが容易に想像できることと思われる。

しかし、現状の開発現場においての危機管理対策は実際、意識・基準面においてどうであろうか。機器導入時はベンダーからの評価を鵜呑みにしていないだろうか。自企業において、リスク判断・バージョンアップ可否判断基準を保有しているだろうか。自分のパスワード（権限者）を他人（部下）へ教えていないだろうか。限りあるシステム予算の中でリスク管理にどれだけ投資すべきか基準があるだろうか。経営者が「セキュリティポリシー」という言葉をそもそも認知しているだろうか。システム部門任せの姿勢になっており、根本的に「後ろ向きな仕事」と捉えていないだろうか。各企業において上記内容に思いあてはまる企業が少なくないと想像しているがどうであろうか。

セキュリティ関係の問題は２０００年問題に近いリスク性を保持しており、あいまいになりがちな対応範囲を厳格に管理する上でも「セキュリティポリシー」を自企業で構築することはより重要な作業となってくる。各企業は、当たり前ではあるが、まず「何から何を守るのか？」を改めて自分達で知り、そしてセキュリティポリシーを策定し、最適な投資を行なうことが重要なのである。

セキュリティポリシーの策定がネットワークセキュリティ対策上の基礎であり、定期保守を行なう上での基礎にもなることは自明の理である。これなしには自社の防衛も、他社への連鎖リスクも守ることができないということを理解しておく必要があるのではないだろうか。

(参考文献)

コンピュータ緊急対応センター	『http://www.jpcert.or.jp/』
財団法人金融情報システムセンター	『金融機関等における個人データ保護のための取扱指針』
社団法人生命保険協会	『生命保険業における個人データ保護のための取扱指針』
社団法人損害保険協会	『損害保険業における個人データ保護のための取扱指針』
昭晃堂	『ファイアウォール　～インターネット関連技術について』
日経ＢＰ社	『インターネット・セキュリティのしくみ』
日経ＢＰ社	『日経コミュニケーション』
日経ＢＰ社	『日経コンピュータ』
情報処理振興事業協会	『http://www.ipa.go.jp/』
ソフトバンクパブリッシング社	『ＩＮＴＥＲＯＰ　ＭＡＧＡＺＩＮＥ』
郵政省	『平成１１年版　通信白書』