セキュリティとは何か

ー 安全性を確立する為の技術的ガイドライン ー

H15 年度　OISA 技術研究会　技術論文

「セキュリティ部会」

～　目　次　～

Ⅰ　部会員紹介 1

Ⅱ　部会開催履歴 1

1　はじめに 2

2　ネットワーク構成 3

3　ネットワークインフラのセキュリティ 4

3.1　脅威 5
3.2　対策技術 9

4　WEB アプリケーションプログラムのセキュリティ 14

4.1　Web アプリケーションとは 15
4.2　Web アプリケーションの基本構成 16
4.3　Web アプリケーションに潜む脅威の具体例 17

5　モラル 23

5.1　人間に依存するセキュリティ事故 23
5.2　情報セキュリティマネージメントシステムとセキュリティポリシー 25
5.3　セキュリティポリシーの階層構造 26
5.4　組織の形成 27
5.5　対策基準の作成 27
5.6　実施手順の策定 28
5.7　ISMS の運営 28

6　まとめ 30

Ⅰ　部会員紹介

進来玄一郎	（部会長）	株式会社富士通大分ソフトウェアラボラトリ
加藤　正治	（副部会長）	九州東芝エンジニアリング株式会社
盛田　朋宏		株式会社エイビス
阿部　高晴		株式会社シーエイシー
国本　修平		大分シーイーシー株式会社
嶋　　大助		新日鉄ソリューションズ株式会社
橋本　真帆		新日鉄ソリューションズ株式会社
三宮　由裕	（技術委員）	三井造船システム技研株式会社
臼杵　敏雄	（技術委員）	システムエイジ株式会社

Ⅱ　部会開催履歴

2003 年 8 月 12 日
2003 年 9 月 12 日
2003 年 10 月 10 日
2003 年 11 月 7 日
2003 年 12 月 4 日
2004 年 1 月 9 日
2004 年 1 月 16 日
2004 年 1 月 30 日
2004 年 2 月 6 日

1 はじめに

ここ数年の爆発的なインターネットの普及に伴って、コンピュータは私たちの業務にますます身近な存在となり、企業活動のさまざまな分野においてネットワークシステムの利用が進展している。高度情報通信社会における企業活動では、取り扱われる情報の信頼性や機密性、プライバシー保護等の重要性が叫ばれている。

ネットワークを利用するにあたって企業や個人が安心して利用できる環境を整備していく為には、総合的なセキュリティ対策が必要になる。
しかし、一言でセキュリティと言っても範囲は広く、技術的な面、人為的な面、外部的な要因、内部的な要因、さらには社会の情勢、新技術導入の側面からの見方も存在する。
情報に対するセキュリティとは一般に、守るべき情報資源を明確にした上で、その情報を外部や内部からの攻撃や漏洩等から守る事であると定義できる。

我々セキュリティ部会では、「ネットワークに潜む脅威」を研究テーマに掲げ、広範なテーマに対し「インフラ」、「Web システム」、「モラル」の３つの観点からレポートをまとめた。今後セキュリティを考える上での足懸かりとなるよう、それぞれについて代表的な脅威や対策技術、手法等を紹介するものである。

2　ネットワーク構成

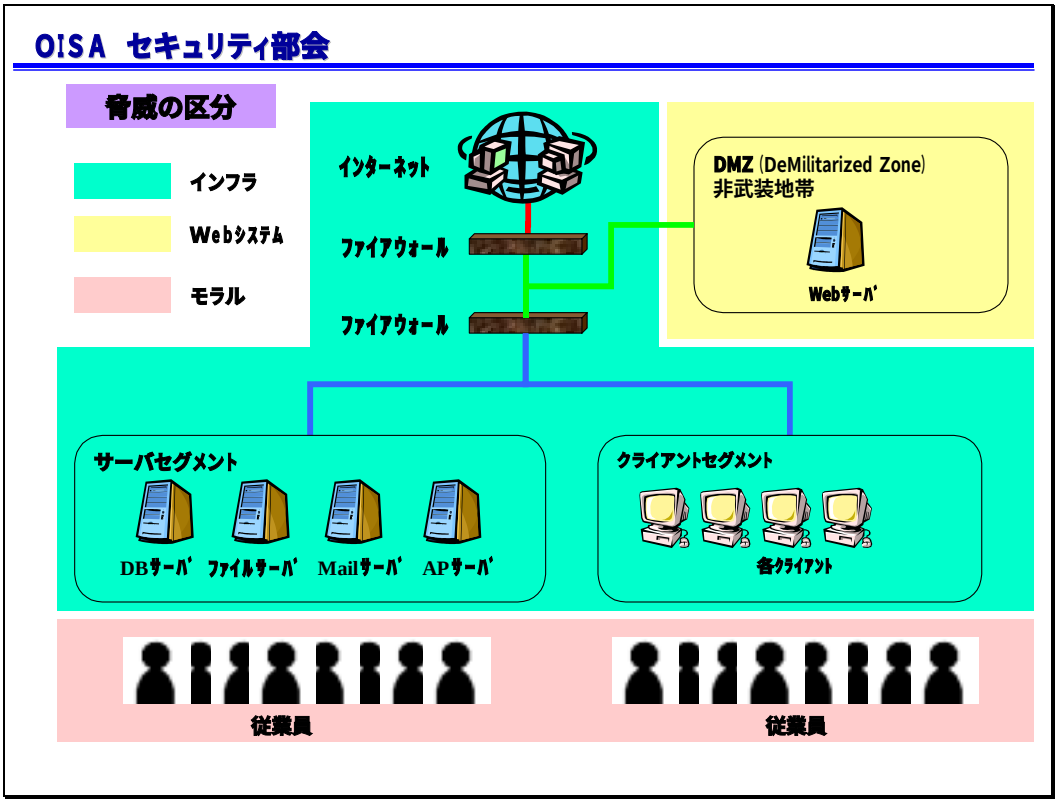

図 2 - 1 一般的なネットワーク構成

上記は一般的なサービス企業のネットワーク構成である。このネットワークではサーバセグメントとクライアントセグメントに別れており、一般従業員はクライアントセグメントで通常作業を行ない、サーバセグメントではネットワークを管理する担当の従業員が管理作業を行なっている。さらにファイアウォールを通じてインターネットと接続しており、制限はあるが各端末は外部と通信が可能になっている。さらに DMZ（非武装地帯）にはＷｅｂサーバが稼動しており、Ｗｅｂを使ったサービスを行なっている。このモデルからテーマを「インフラ」、「Web システム」、「モラル」に分け、それぞれセキュリティ上に一体どのような脅威があるか、さらにどのような対策があるのか調査を行った。

3　ネットワークインフラのセキュリティ

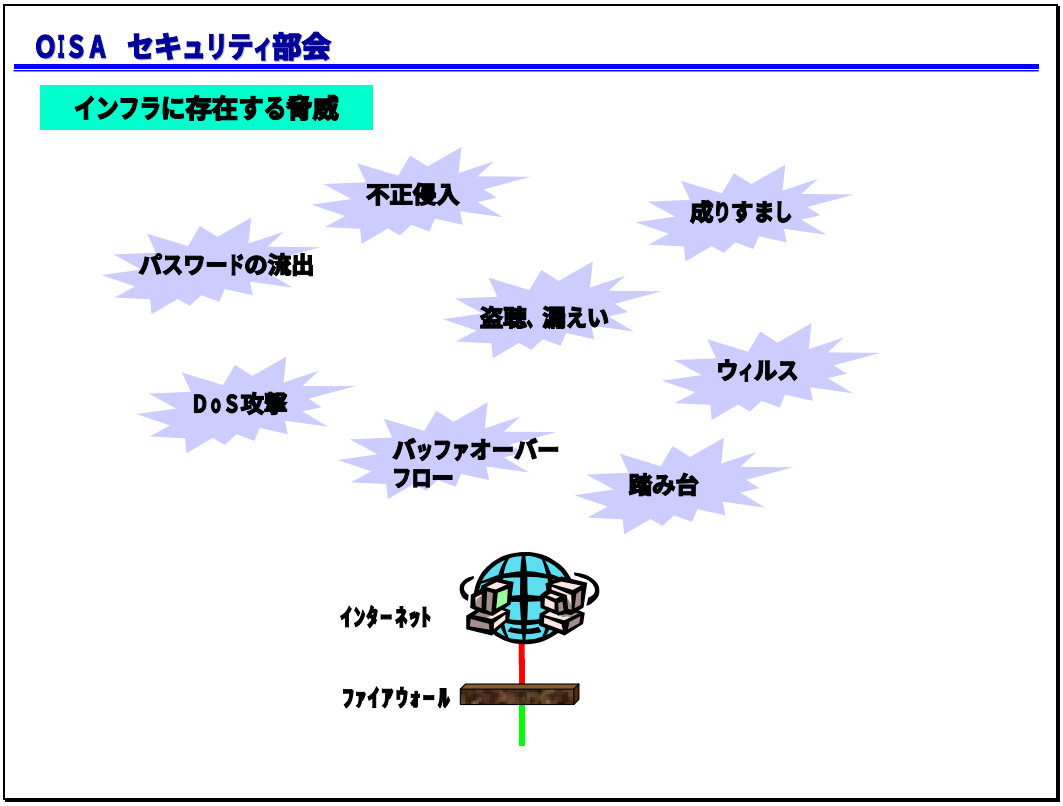

図 3 - 1 インフラに存在する脅威

近年、インターネット上に様々なサービスを手がけるサイトが多くなり、その規模も世界レベルで拡大している。このような急速なネットワークの拡大が実現できた背景の一つに、さまざまなネットワーク媒体やプロトコル、機能などを階層的に分類して構築することができるネットワーク・アーキテクチャの存在が上げられる。一般的にＯＳＩ参照モデルと呼ばれ、このモデルを参照しているＴＣＰ／ＩＰという技術が、現在の事実上業界標準（デファクトスタンダード）となっている。この技術のおかげで、消費者は異なるメーカのネットワーク機器、異なるコンピュータ会社のコンピュータ、異なるソフトウェア会社のオペレーティングシステム、異なるソフトウェア会社のアプリケーションソフト等を好きな用途で選ぶことが可能になった。

通信プロトコルであるＴＣＰ／ＩＰでは、情報を伝えるべきその経路を、状況に応じて自動的に選択している。どの経路を通ってデータを送るかを判断する技術はルーティングプロトコルと呼ばれ、そのネットワークの煩雑さによって常に情報経路が更新されている。このネットワークインフラ環境は世界中の通信事業者、プロバイダ、教育施設、一般企業、個人、等が行っている。各ホストはルーティングサーバと呼ばれ、ＴＣＰ／ＩＰに基づいて接続されており、所定の手続きを行えば誰でもインターネットに参加することができる。ネットワークインフラを運営する側は、ルーティングサーバの設定等、ネットワークへ入

ってくる情報、出て行く情報、両方の管理を行う。
各ネットワークの運営方針については、技術的背景からその管理者に権限が任せられるよう作られており、インターネットに参加している全ての人の慈善的な活動によって支えられている。
インターネットに流れる情報は参加者全員で共有することができ、かつてそこに流れるデータは誰でも閲覧が可能であった。
しかし現在、多くのサービスを提供する企業が、オンラインショッピング、ネットワーク申請、会員専用情報サービス等、利権や金銭、個人情報、クレジットカード番号など、他者に知られるのはあまりよくない、現在の社会市場理念に基づいた価値のある情報まで扱うようになった。
社会的システムの道具の一つとしてインターネットの価値が認められた現在では、自分と相手以外の第三者に対し極めて漏洩されにくい情報管理の技術、さらにウイルスなどの悪意あるプログラムに対する警戒などが必要とされている。
これらリスクを正しく認識し、ネットワークインフラを有効に活用できる環境を常に保たせるためにも、セキュリティに関する情報収集と管理業務を怠ってはならない。
この章ではネットワーク管理者が知っておかなければならないインフラに存在する技術的な脅威と対策についてまとめた。

3.1 脅威

【ウイルス】
ウイルスとは様々な脅威の複合体であり。その体系的分類に分ける作業はこれまで幾度となされてきた。しかし、新しい技術が次々と生み出されていく度、その新技術に潜む隙間を見つけ、侵入し破壊的な活動をするウイルスの出現も後が絶たない。ここでは２００３年夏、猛威を振るったＭＳＢＬＡＳＴを例にその活動を検証し、そこでどのような目的で活動するプログラムなのかに着目してまとめた。
ＭＳＢＬＡＳＴ
感染の方法は Windows のサービス：RPCSS（Remote Procedure Call Server Service）の脆弱性(MS03-026)を利用して侵入する。

1) 当該脆弱性を有するコンピュータの TCP135 番ポートを通じて、バッファオーバーフローを起こすパケットを送信する。
2) バッファをオーバーしたスタック領域内にはバックドアを開かせるリモートシェルが組み込まれており、RPCSS はそのスタック領域に上書きされたリモートシェルを動かしてしまう。
3) 感染先のリモートシェルはバックドア TCP4444 番ポートを開く。
4) 感染元から tftp コマンドで UDP69 番ポートから TCP4444 番ポートへ接続。
5) 感染元のコンピュータの、ワームの本体プログラム(msblast.exe)をダウンロードさせ、実行させる。

感染後の動作は非常に巧妙であり、RPCSS は Administrator 権限で動いているため、RPCSS から実行された MSBLAST も管理者の許可したプログラムとして活動することができる。

1) コンピュータがリブートされた場合でも、ワームの本体が再実行されるようにレジストリを更新する。
2) 感染したコンピュータの直近の IP アドレスまたはランダムな IP アドレスについて脆弱性を有するコンピュータを探し、さらなる感染を試みる。
3) マイクロソフト社のサイト windowsupdate.com に対して、ＤｏＳ攻撃を行う。

このように MSBLAST にはバッファオーバーフロー、バックドア、管理者への成りすまし、不正操作、ＤｏＳ攻撃等、多くの脅威が巧みに組み合わされている。総合してウイルスの持つ特徴は、「技術的欠陥を利用して侵入し、一般社会の業務に混乱と破壊を目的とした活動をする」ことであるといえる。対策としてはウイルス検索ソフトを購入しインストールすること。素性の知れない実行ファイルは実行しない。などが上げられる。

【バックドア】

クラッカーにより侵入を受けたサーバに設けられた、不正侵入を行なうための「裏口」。クラッカーはコンピュータへの侵入に成功すると、次回も侵入できるように、管理者に気づかれないようこっそりと侵入経路を確保する。これがバックドアである。バックドアが設置されていると、管理者が不正侵入に気づいて侵入路をふさいでも、クラッカーは前回侵入時に設置したバックドアから再び不正侵入を行なうことができる。また、コンピュータウイルスが感染する際に、外部からの操作を受け入れるための窓口としてバックドアを設置する場合もある。バックドアを使って侵入すると、たいていの場合はコンピュータのすべての機能を不正に使用できるため、他のコンピュータへの攻撃の踏み台として利用されてしまうことも多い。不正アクセスが確認された後に、ディスクのフォーマットや OS の再インストールを行なうべきとされているのは、バックドアを完全に消去するためでもある。

【Ping of Death】

ネットワーク管理に使う「ping」と呼ばれるプログラムを悪用し、対象のコンピュータを使用不能にする攻撃手法。ping はもともと相手のコンピュータが応答するかどうかを調べる単純なプログラムだが、Ping of Death はこれを使って規定のサイズを遥かに超える巨大な IP パケットを相手に送り付け、対象のコンピュータやルータをクラッシュさせてしまう。　1996 年に問題が表面化し、多くの OS が被害に遭う可能性があることや、ping 以外の様々なプロトコルでも同様の手法が使えることなどから、有名になった。IP パケットの分割機能を悪用したものであったが、現在ではほぼ全ての OS が対処されているか、パッチ(修正プログラム)が配布されている。1996 年以前の OS は影響を受ける可能性があるので、パッチの使用かバージョンアップが推奨されている。

【パケットスニッファリング】

ネットワークを流れるパケットを盗聴し、そこから ID やパスワードを拾い出すこと。「パ

ケット盗聴」とも呼ばれ、パスワード以外にもメールの盗聴などが行われることもある。多くのネットワークでは管理の必要から、管理者はネットワーク内のパケットを自由に見ることができるようになっている。そのため、悪意を持った人物が管理者権限を手に入れた場合、ネットワーク内部から外部へアクセスしている人物のパケットを盗聴し、様々な情報を知ることもできる。また、ネットワークによっては管理者でなくとも盗聴が可能な場合があり、注意が必要である。　パケットスニッファリングへの対抗手段は、通信経路の暗号化や定期的なパスワード変更が一般的である。インターネットなどの開かれたネットワークでは、どこで誰がパケットを盗み見ているかわからないため、暗号化できない Telnet や FTP などのアプリケーションは使用すべきでないとされる。

【ウォーダイヤリング】
非公開のダイヤルアップ回線などを求めてダイヤルアップを繰り返すクラッキングの手口。1983 年公開のハリウッド映画「WARGAMES」中で題材にされ、この名前で呼ばれるようになった。

　ウォーダイヤリングを自動的に行なうアプリケーション「ウォーダイヤラ」も存在し、データベースと連携した電話番号の記録、モデムが応答した場合のパスワードの解析まで行なう機能を持つものも存在する。

　ウォーダイヤリングはその組織のネットワークに直接接続する手口であるため、インターネットとの接続点に設置されているファイアウォールは無力である。ネットワークを守るためにはパスワードの厳重な管理だけでは不十分で、ダイヤルアップ先にコールバック機能を付加するなどの手法が求められる。これと同様のクラッキング手法として、無線 LAN のアクセスポイントを探し出す「ウォードライビング」という手口も最近になって登場した。

【Dos 攻撃】
ネットワークを通じた攻撃の一つ。相手のコンピュータやルータなどに不正なデータを送信して使用不能に陥らせたり、トラフィックを増大させて相手のネットワークを麻痺させる攻撃。

【DDoS(分散 DoS)】
読み方 ： ディーディーオーエス 2001/3/6 更新
フルスペル ： Distributed Denial of Service

　複数のネットワークに分散する大量のコンピュータが一斉に特定のサーバへパケットを送出し、通信路をあふれさせて機能を停止させてしまう攻撃。実際にパケットを送る(攻撃を実行する)コンピュータの管理者や利用者に攻撃の意図はなく、外部の悪意ある第三者(クラッカー)にコンピュータを操られて、気づかないうちに攻撃に参加させられてしまうという特徴がある。2000 年 2 月、何者かの手によって、Yahoo!、Amazon.com、Buy.com、eBay、CNN、E*TRADE、ZDNet などアメリカの大手 Web サイトが次々と DDoS の被害にあい、

注目を集めた攻撃手法である。クラッカーは、攻撃対象とは無関係な多数のコンピュータに侵入し、ユーザに気づかれないように攻撃実行用のプログラム(トロイの木馬)をこっそりしかける。攻撃を開始する時には、あらかじめ仕掛けたトロイの木馬に対して、一斉にパケットの送出命令を発行する。標的となったサーバには、トロイの木馬が仕掛けられたコンピュータからパケットが送り込まれるため、攻撃されたサーバからは真の攻撃元である「黒幕」のコンピュータを割り出すことは難しい。DDoS による妨害アクセスは通常のアクセスと見分けがつきにくく、選択的に排除するのが難しい。このため、標的のサーバにセキュリティ上の弱点を放置するなどの管理のミスがなくても被害が発生してしまう。DDoS を阻止するためには、クラッカーにトロイの木馬を仕掛けられないよう各コンピュータの管理者が注意する必要がある。

【バケツリレー攻撃】
データの送信者と受信者の間で、悪意のある第三者が双方に気づかれないようにデータを中継すること。「中間一致攻撃」とも呼ばれる、ネットワーク上でのよく知られた攻撃方法の一つである。条件さえ満たしていれば公開鍵暗号も無効化できると言われており、パスワードやデータの盗聴、データの偽造など様々な目的で行われる。データの送信者と受信者が相互に認証し合うことで、ある程度まで防ぐことができる。

【反射攻撃(replay attack)】
不正侵入の手段の一つで、パスワードや暗号鍵などを盗聴し、そのまま再利用することでそのユーザになりすます方法。パスワードが暗号化されていたとしても、暗号化された後のデータを記録して使うので、受け取った方では「正しいパスワードを正しく暗号化している」と判断してしまう。パスワードを復号化する必要がないので、強力な暗号化システムでもこの攻撃を防ぐことは困難とされている。これを防ぐために考案されたのが、毎回パスワードを変化させるという「ワンタイムパスワード」方式である。

【ウォードライビング war driving】
企業内の無線 LAN のアクセスポイントを求めてオフィス街などを車で移動するクラッキングの手口。
「ウォーダイヤリング」と類似のクラッキングの手口のためこの名称で呼ばれるようになった。無線 LAN は障害物がなければオフィスビルに面した道路上でも十分にビル内のアクセスポイントに接続できる場合がある。これを悪用し自動的にセキュリティで保護されていない、あるいは保護が甘い無線 LAN のアクセスポイントを探し出し、ネットワークに侵入するのが目的であり、これを自動的に行なうためのアプリケーションも存在する。このため、ノートパソコンを車に載せて、オフィス街を走り回るだけでクラッキングが行える。ウォードライビング行為からネットワークを保護するためには、暗号化 WEP の導入や MAC アドレス制限などが考えられる。

【IP スプーフィング(IP spoofing)】
偽の IP アドレスを送信元にセットしたパケットを送り込む攻撃手法。 不正侵入の手段として使われることが多く、その際、信頼されているコンピュータに成りすまして認証をパスするという手口が利用される。企業の情報システムでは、プライベート IP アドレスからアクセスすると利用できる機能などがあるが、IP スプーフィングによってプライベートアドレスを詐称することにより、外部から不正にこうした機能にアクセスできてしまう。ほかにも、DoS 攻撃の際に送信元が割り出されないように別のコンピュータの IP アドレスを名乗るなどの応用例もある。

3.2 対策技術

【ファイアウォール】
インターネットなどの信頼できないネットワークからの攻撃や、不正アクセスから組織内部のネットワークを保護するためのシステム。内部ネットワークと外部のネットワークの間に設置し、必要な通信のみを通過させ、不要な通信を遮断するのが主な用途。通常、内部のネットワークから外部はアクセスできるが、外部から内部のネットワークにアクセスができないような制御にするのが一般的な使われ方である。また、ログを蓄積する機能も搭載されている。一般的にパケットフィルタリングとアプリケーションゲートウェイの２つの技術で構成されている。パケットフィルタリングとは、通過するパケットの IP ヘッダ情報とポート番号を読み取り、定義されているフィルタリング・ルールを比較走査することによって､通過するパケットに制限をかけている｡アプリケーションゲートウェイとは、パケットの中身までチェックを行い、不正な要求や不正な操作を監視している。もし、見つけた場合はその通信を強制切断させて、管理者に報告するなどの機能を持つ。パケットフィルタリングは動作が高速であるがセキュリティレベルが低い。逆に、アプリケーションゲートウェイはパフォーマンスが悪いが高いセキュリティレベルを実現できる。

【APOP】
ある会社で、外回りしている従業員の人たちにもメールの確認ができるようにと、Post Office Protocol（POP）のポートを外部ネットワークへ公開していた場合、POP サーバのログから、メールの内容が外部に漏れる危険性がある。POP はアカウントやパスワードといった情報を平文（テキスト）で送信するため、通信線路上での盗聴により容易に盗み出すことが原理上可能である｡よってある従業員の POP サーバのアカウントとパスワードが、悪意ある第三者に盗まれる危険性がある。
対策として Authenticated Post Office Protocol（APOP）を導入すれば、従来の POP を拡張し、パスワードを暗号化してやりとりをすることで盗聴によるアカウント情報の奪取などを防止することができる。これによりメールアカウントのパスワードが外部の第三者に漏れ、POP サーバへ進入される危険性を減らすことができる。制約として、APOP はメールサーバ、クライアントがともに対応可能でなければ利用できない点が上げられる。現時点

の Windows 環境では Becky や AL-Mail、PostPet といったメールクライアントで APOP を利用することができる。明示的に設定を変更する必要があり、メールアプリケーションに APOP の設定作業をユーザが行わなければならない。

【PKI（Public Key Infrastructure)】
公開鍵基盤/公開鍵暗号基盤と呼ばれるサービス。用途は顔の見えない相手を信頼するための技術である。知名度のある認証機関がそのサービス会社の調査を行い審査をする。まず「このサービス会社は信頼できる」と判断されることが第１条件となる。審査に合格すると、認証機関はそのサービス会社に新しい秘密鍵を渡す。新しい公開鍵は認証機関が公開する。利用者は公開された公開鍵をもとにデータを暗号化し、暗号データをそのサービス会社に送信する。暗号化に使われた公開鍵は認証機関が発行した鍵なので、サービス会社から正しい復号データが返ってくれば信用できるサービス会社であると判断できる。PKI はこのように署名技術として使える。さらに通信の暗号化にも応用して使うことができる。一般的にＷｅｂデータを暗号化するＳＳＬ。ネットワークそのものを暗号化するＶＰＮ。メールの中身を暗号化するＰＧＰ等は、認証機関が発行した公開鍵で暗号化することが多い。

【SSL（Secure Sockets Layer)】
　主に Web サーバと Web ブラウザ間の HTTP 通信を暗号化して送受信する業界標準の通信プロトコル。Internet Explorer や Netscape など、一般の Web ブラウザに標準で搭載されており、ブラウザ右下に鍵マークと Web ブラウザの URL 入力画面に「https://」 と出力されているのが SSL による通信の目印になる。これらの Web ブラウザには、あらかじめ第三者認証機関が発行した公開鍵（電子証明書）が組み込まれており、SSL で通信することにより以下の保証が得られる。
１、そのサーバは第三者認証機関の調査によって存在が確認されている。
２、その存在が確認されているサーバから送られてきたデータである。
３、暗号化されて他者からはほぼ傍受される危険がない。
の３点が保証されている。

【IDS（Intrusion Detection System)】
不正侵入検知システムと呼ばれているセキュリティ技術である。攻撃が発生している事実を識別するための支援を行い、攻撃者／侵入者の識別に役立つ犯罪科学的な証拠の収集を支援するシステムである。IDS の侵入検知技術には「シグネチャベース」と「統計ベース」２つの種類がある。「シグネチャベース」の侵入検知とは、データベースに過去に被害のあったシステムを危険な状態に至らせる攻撃情報が記録されており、ユーザーの活動とデータベースを比較することによって侵入の試みを検知しようとするシステム形態のことをいう。「統計ベース」の侵入検知システムとは、システムの監査証跡データを常に蓄積させ、それから通常から外れた活動がないかどうか詳しく調べるシステム形態のことをいう。侵

入者の活動が正当なユーザーのそれと顕著に異なるだろうという前提のもとに、侵入の検知を試みている。どちらも発見した場合は潜在的な侵入の試みとして管理者に報告するなどの処置を行う。

【VPN(Virtual Private Network) 】
IT 環境の普及に伴い、インターネットを使って情報のやりとりをする行為が一般的になってきており、ビジネスにおいては特定の相手へり高いセキュリティでの通信を確保することへの要求が高まっている。
以前は、このような要求に対しては、専用線か、Web ベースでの暗号化接続を提供する SSL（Secure Sockets Layer）やメールの暗号化という方法が主流であった。しかし、サービスが多様化するにつれて、利用するアプリケーションを意識することなく暗号化したいというニーズが高まってきている。そうした環境に対して、VPN は最も有効なソリューションといえる。
VPN とは（Virtual Private Network）の頭文字を採ったもので日本語では「仮想閉域網」や「仮想私設網」等と訳される。インターネットを経由するにもかかわらず、拠点間を専用線のように相互に接続し、安全な通信を可能にするセキュリティ技術である。
VPN を利用した通信を行なうには、接続点に VPN 機能を備えた専用装置が必要だが、最近ではルータやファイアウォールにその機能が含まれるものも多い。
VPN の機能は大きく分けて 2 つある。1 つは、「トンネリング（Tunneling)」と呼ばれる技術で、パケットに新しいヘッダを付け加え、別のプロトコルデータとして通信を行う、これは VPN 装置によって行われるため､本来は IP パケットのみしか通らないインターネットに、たとえばプライベートアドレスや、TCP/IP でないプロトコルを利用した通信を可能とするため、インターネット通信の中に別の通信を通すという意味合いから「トンネリング」と呼ばれているが、他には、カプセル化（Encapsulation）と呼ばれることもある。
もう 1 つは、「通信パケットを暗号化する機能」である。トンネリングだけではデータの内容は見えてしまうため、パケットを暗号化しトンネリングされたパケットの盗聴や改ざんなどを防止する。暗号化／復号化には大きく分けて「秘密鍵暗号化方式」と「公開鍵暗号方式」の 2 つの方法があり、VPN では、これらの暗号化方式を組み合わせて使うのが一般的になっている。

【公開鍵暗号方式】
データを暗号化することによって、第三者への閲覧を困難にすることができる。インターネットで広く一般的に使われている暗号技術が「ＲＳＡ公開鍵暗号方式」と呼ばれる技術で、鍵なしで解読するのに膨大な量の時間とコストがかかることがわかっている。

ここで「ＲＳＡ公開鍵暗号方式」の例を上げる。
”ＡからＢへ、数字６桁の番号を暗号化して送信する場合”

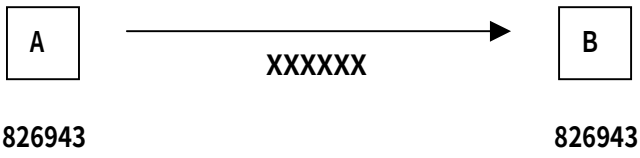

図 3-2-1 暗号通信

この場合必要となる暗号の鍵となるパラメータを、
＜１０を法として公開鍵３で暗号化＞
＜１０を法として秘密鍵７で復号化＞
と設定した。
まず、暗号を行う。
＜１０を法として公開鍵３で暗号化＞とは、
平文を３乗して１０で割った余りを暗号文として扱うという意味である。
826943 の最初の数字 8 を暗号化する。

８＾３／１０＝５１ 余り ２

８を３乗すると５１２で、それを１０で割った余りは２である。つまり８を暗号化すると２になる。これと同じ要領で各桁の番号を３乗して１０で割っていくと、

２＾３／１０＝ ０ 余り ８
６＾３／１０＝２１ 余り ６
９＾３／１０＝７２ 余り ９
４＾３／１０＝ ６ 余り ４
３＾３／１０＝ ２ 余り ７

826943 → 286947
と暗号化できる。
この「286947」を送信すれば、途中で閲覧されても第三者には意味が分からない。
次に復号を行う。
＜１０を法として秘密鍵７で復号化＞とは、
暗号文を７乗して１０で割った余りを平文として扱うという意味である。
286947 の最初の数字 2 を複合化する。

２＾７／１０＝１２ 余り ８

２を７乗すると１２８で、それを１０で割った余りは８である。これと同じ要領で各桁の番号を７乗して１０で割っていくと、

８＾７／１０＝209715 余り ２
６＾７／１０＝ 27993 余り ６
９＾７／１０＝478296 余り ９
４＾７／１０＝ 1638 余り ４
７＾７／１０＝ 82354 余り ３

286947 → 826943

と、元の番号を得ることができる。
この１０(法)、３(公開鍵)、７(秘密鍵)、という数字の関係は、

P × Q = 法　(PとQは2つの異なる素数)
n(P-1)(Q-1)+1 = 公開鍵 × 秘密鍵

という式に基づいて求められたものである。
ここでは簡単な例を出したが、(法)の組み合わせの桁数を上げればいくらでも複雑にすることができる。公開鍵暗号の欠点は時間があれば解読されてしまうこと。利点は暗号化した本人ですら簡単に元に戻せないこと。よって桁数が多ければ多いほど、秘密鍵を求める作業は困難になり、暗号解読は難しくなる。簡単に復号できるのは公開鍵を公開した本人の秘密鍵のみということになる。秘密鍵なしで解読にかかる時間はかなりの大きさで、１５５桁(512bit)の鍵を解読するのに３００台のコンピュータで７ヶ月強を要したという報告がある。３００桁(1024bit)くらいの長い鍵で暗号化を行えば、現代のコンピュータ技術で短期間のうちに解読を行うのは、ほぼ不可能であると考えられている。

4 Web アプリケーションプログラムのセキュリティ

近年、インターネット、特にブロードバンド環境の整備によって、インターネット上でのビジネスサービスの幅は広がりつつある。

情報を一方的に提供するのみではなく、企業間、あるいは、企業と個人、個人と個人の間で情報のやり取りを行う、よりダイナミックなビジネスサービスが多くなっているのである。

これを実現するのが、Web アプリケーションであり、その用途は以下のように様々である。

BtoB
　企業間の電子商取引(e マーケットプレイス)
BtoC
　オンラインショッピング
　オンライントレード
　オンラインバンキング
　Web マーケティング
CtoC
ネットオークション

Web アプリケーションとは、「Web サーバ上に存在し、クライアントからのリクエストを受けて動作するアプリケーション」のことであり、クライアントが不特定多数であるといった点が特徴である。

まず、この「クライアントが不特定多数である」といった点で、セキュリティについての考慮は必要不可欠であるということを明確にしておきたい。

次に、「Web アプリケーションのセキュリティは、ネットワークレベルでのセキュリティとは別に論じなければならない」ということを明確にしたい。

サーバから一方的に情報を受け取るだけだった、従来の Web のあり方では、扱う情報量も少なく、クライアントのオペレーション可能範囲も限られていた。それは同時に、リスクが少ないということを表しており、そのため、ファイアウォールを用い、パケットレベルでセキュリティを確保すればよかった。

しかし、クライアントのリクエストに動的なアクションをする Web アプリケーションにおいては、クライアントの不用意な、あるいは悪意あるオペレーションであっても、ブラウザ上で可能なことであれば問題なく行うことができる。したがって、いくらネットワーク側が万全でも、アプリケーションがセキュアでなければ、本来絶対に見られてはいけないような重要な情報も吐き出してしまうことになる。

つまり、パケットレベルでのセキュリティとは、まったく別のレベルで論じる必要があるということである。

Web アプリケーションのセキュリティは、ネットワークレベルとはまったく別のレベルで論じなければならない。そして、Web アプリケーションを作るのは「プログラマ」である。

本章では、ネットワーク管理者だけではなく、開発者(プログラマ)をターゲットとしたセキュリティガイドラインを作成するべく、Web アプリケーションに潜む脅威と対策についてまとめる。

4.1 Web アプリケーションとは

Web アプリケーションとは、
「ネットワーク上の Web サーバ上に存在し、クライアントのリクエストをきっかけに、そのサーバ上で動作するアプリケーション」である。
その動作には、別のサーバに存在するデータを取得する、クライアントにレスポンスを返すといった動作が含まれる。
これにより、オンラインでのダイナミックなアプリケーション機能を提供できるのである。

クライアントは、オペレーティングシステムに依存しない。ただ Web ブラウザさえあれば、Web アプリケーションの提供するサービスを利用することができる。

4.2 Web アプリケーションの基本構成

Web システムの最も簡単な構成の例は以下のとおりである。

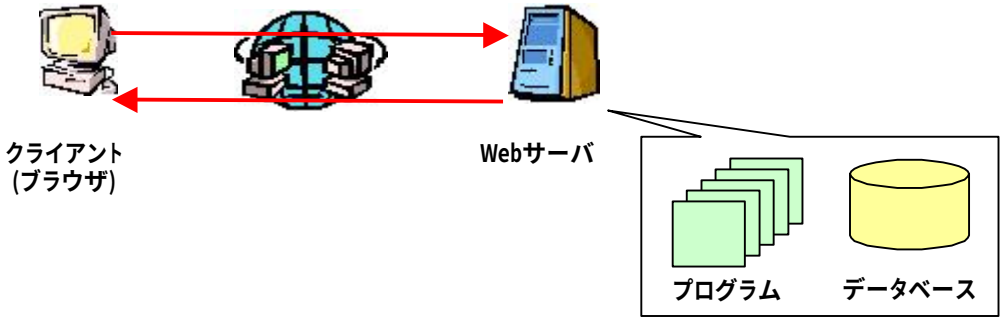

図 4 - 2 - 1

多くの Web アプリケーションには、データベース、そのデータベースを操作するプログラム、クライアントからのリクエストを処理するプログラムが存在する。

場合によっては、データベース、および各プログラムは、Web サーバ上に存在せず、データベースサーバ、アプリケーションサーバのように分散することもある。

前章「2. インフラシステムにおけるセキュリティ」で論じたように、ネットワーク管理者は、通常、以下のようにファイアウォールを設置し、パケットレベルでのセキュリティを高めることになる。

図 4 - 2 - 2

「Web アプリケーションにおけるセキュリティ」で論じる脅威は、上図における通常のやり取り(赤線)に潜む脅威であり、これはファイアウォールでは検知することは難しいものである。

4.3 Web アプリケーションに潜む脅威の具体例

Web アプリケーションに潜む脅威の具体例を図に表すと、以下のようになる。

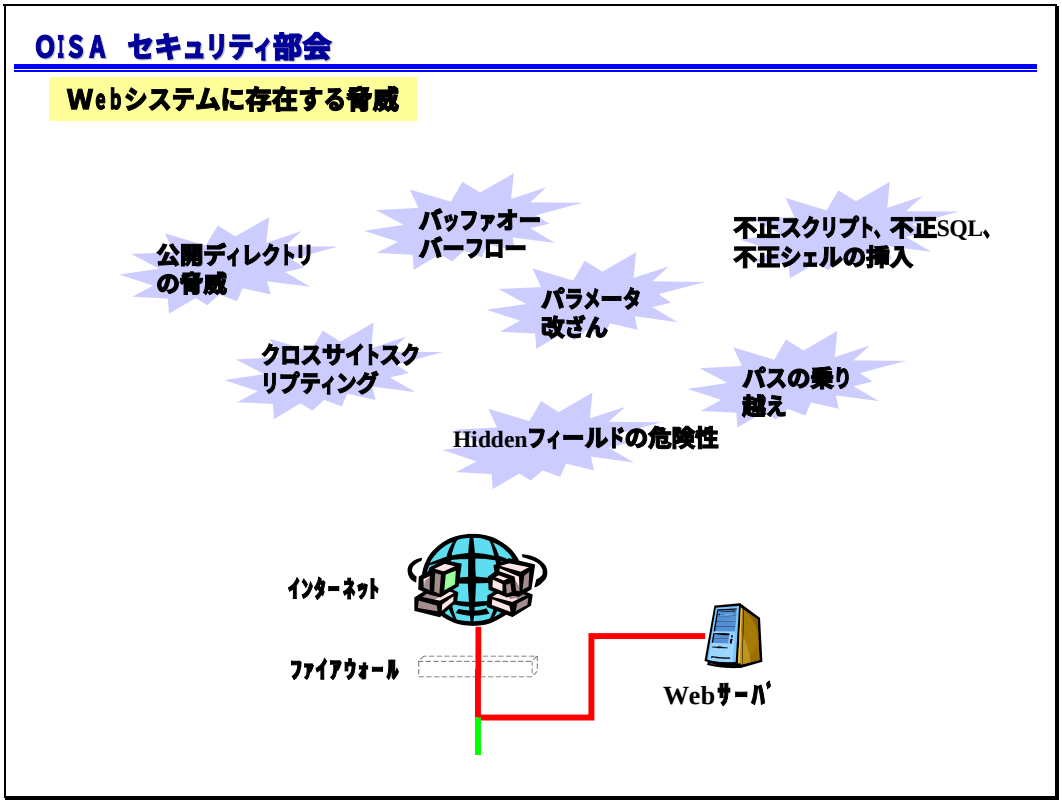

図 4 - 3 - 1

本節では、この脅威それぞれについて詳しく見ていこうと思う。

4.3.1 公開ディレクトリの脅威

ここでは、一つの事例を用いて論じようと思う。

株式会社 A で、応募者にプレゼントが当たるキャンペーンをホームページで行った。応募方法はインターネットのホームページで住所、氏名、年齢、性別、職業、電話番号、メールアドレスなどの情報を入力するものであった。

しかしこの応募者の情報ファイル「応募者.csv」が外部へ流出するという事件が発生した。

おそらく、保存場所が外部から閲覧できる場所であったため、知識をもつ第三者にディレクトリの構成内容を悟られたものと思われる。

このシステムは HTML と CGI プログラムで作られ、応募者の送信したデータを、CSV ファイルに書き足すしくみであった。
外部から閲覧されてしまった原因は次の２点である。

（１）保存するディレクトリは、CGI プログラムの保存場所の直下「./data/」であった。
（２）「./data/」は外部からディレクトリ構成が見えないようにさせる「index.html」も置いていなかった。

結局 A 社はキャンペーンを中止し、応募者へお詫びのメールと、総務部長の謝罪の会見を開いた。

この事例における問題点は、プログラマのセキュリティに対する認識不足である。
Web のような不特定多数からのアクセスを許すシステムにおいては、重要な情報を扱うときに、以下のようなガイドラインを掲げるべきである。

（ガイドライン１）
データを保存するディレクトリは公開しているディレクトリ以外にする。
（ガイドライン２）
公開しているディレクトリでは、ディレクトリの構成そのものを、外部に見せないようにする。

4.3.2 不正スクリプト、不正 SQL、不正 OS コマンドの挿入

Web アプリケーション側では、フォームに入力されたデータを使って次のアクション（次ページの表示など）を行うことになるが、このときデータとして特殊なコードが入力されると、本来は想定しない処理（他のユーザーのデータを盗み見るなど）が可能になってしまう場合がある。

例えば、クレジットカードを扱う Web アプリケーションにおいて、「CARD」というテキストボックスに入力されたユーザの入力値を元に、SQL を生成しデータを取得する処理が行われていたとする。
もちろん、ここで予期されている値は「01234567」といった数値であるが、この入力値のチェックを行う処理が抜けていた場合、「6;delete * from Card」のように 2 つの SQL を続けて記述するための「;」という文字を打つことによって、悪意あるユーザはプログラマがまったく予期していない 2 つ目の SQL を発行することが可能になるのである。

これを防止するには、ユーザから入力されたデータを不用意に次の処理に使わず、特殊

文字の検査などを実施する必要がある。

この処理はサニタイジング（sanitizing：「sanitize」は「無菌化する」の意）と呼ばれ、具体的なサニタイジングのタイミングは、サーバ・オブジェクトを使って HTML データをエンコードするときや HTML データを生成する直前に行う。

間違って解釈される可能性のある特定の文字をエスケープするか、削除するのである。

以下に不正スクリプト、不正 SQL、不正シェルとなりうる特定の文字の例を挙げる。

不正スクリプトとなりうるもの「<」「>」「"」「'」「;」「|」「&」「`」「(」「)」

不正 SQL となりうるもの「'」「;」

不正シェルとなりうるもの「;」「|」「&」「`」「()」「」」

（ガイドライン）

プログラマは、受け取った入力値、出力する出力値を必ず確認する。HTML データに埋め込まれるユーザからの入力データは、すべてサニタイジングの対象とする。

4.3.3 パラメータ改ざん

ここでも、一つの事例を用いることとする。

Web 上でオンラインショッピングを行っている A 社のサイトでは、会員専用の処理を実行するために、以下の URL パラメータを使用していた。

「～.com/info.cgi?user=123&pw=456」

しかし、URL パラメータを利用していたことから、悪意あるユーザにより、他のユーザのデータが盗まれてしまった。ブラウザのアドレス欄を、「user=124&pw=457」のように、予測し入力することで、成りすましが可能であったのである。

この例では、「ユーザ ID」と「パスワード」がパラメータであり、「ユーザ ID」は予測できても、「パスワード」は予測できないのではないかと考えるかもしれない。確かにその通りであるが、「パスワードを入力できる」こと自体に問題があり、何度も値を買えて挑戦していれば、悪意あるユーザはいつかパスワードを破ることができるかもしれない。
ましてや、連番で振ることの多い「ユーザ ID」を入力可能にしておくことは、さらに危険である。

このように、URL パラメータをユーザに見える状態にしておくことは、

1．情報漏えい
2．成りすまし

を招くことになる。

その他、セッション ID によるセッションの管理に URL パラメータを用いることも多いが、同じく危険である。

（ガイドライン）
プログラマは、特定ユーザしかアクセスできないページに URL パラメータを用いることは極力避けるべきである。URL パラメータを用いる場合は、まったく別のユーザが見ることを予測して、重要度の低い情報を扱う場面に限定するべきである。

4.3.4 クロスサイトスクリプティング

攻撃者が、脆弱な踏み台サイトを経由して、ユーザのブラウザ上で、巧みに不正スクリプトを実行させる脅威である。攻撃者のサイトから、踏み台のサイトというようにサイトをクロスすることから、クロスサイトスクリプティングと呼ばれる。

脆弱な踏み台サイトでは、不正スクリプトの混入を避けるためのチェック、サニタイジングをまったく行っていなかったとする。さらに、URL パラメータにユーザからの入力値をそのまま使用していたとする。
その場合、攻撃者は、自らのサイトに、踏み台サイトへのリンクを張り、その URL パラメータの部分に不正スクリプト(Cookie 情報を盗むなど)をあらかじめ埋めておく。ユーザは、攻撃者サイトに設置されたリンクをクリックしただけで、不正スクリプトを実行されてしまうのである。
この手法を用いれば、攻撃者は自ら苦労することなく、攻撃を実施できる。

クロスサイトスクリプティングは、攻撃者がサイトを設置しなくても、掲示板サイトなどに同様のリンクを書き込むだけでも実施できてしまうという点、また、善意のユーザに対して被害を与えてしまうという点で、この脅威は厄介である。
そして、この脅威を取り除くには、Web アプリケーション自らが自衛するしかないのである。

（ガイドライン）
プログラマは、受け取った入力値、出力する出力値を必ず確認する。HTML データに埋め込まれるユーザからの入力データは、すべてサニタイジングの対象とする。

4.3.5 hidden フィールドの危険性

Web ページ間のデータ受け渡しの際に、フォームの hidden フィールドを利用する方法があることはよく知られている。そして、これを用いる Web アプリケーションは非常に多い。

しかし、hidden フィールドを多用することは非常に危険である。

Web ページ間のデータ受け渡しにフォームの hidden フィールドを利用する場合の問題は、次のページに受け渡されるデータが一度 WWW ブラウザを経由することにある。

データが一度 WWW ブラウザを経由することで、悪意あるユーザは、HTML ソースを表示・編集し、容易に、情報を盗み出したり、成りすましを行ったりできるのである。

hidden フィールドで指定したデータはブラウザには表示されないため安全であるかのように錯覚しがちであるが，実際には他のデータと同様にブラウザに送られているのである。

個人情報のような重要なデータを hidden フィールドで扱うことはもちろん､セッションの管理に hidden フィールドを用いることも危険である。

「hidden」とは言っても、決して「完全に隠されている」というわけではないということを認識する必要がある。

（ガイドライン）

プログラマは、重要なデータを hidden フィールドに持たせない。セッション管理には、Web アプリケーション実行環境が提供するセッションメカニズムを利用する。

4.3.6 バッファオーバーフロー

システムがネットワークから受信したパケットを、確保したメモリサイズを越えてメモリに格納してしまい、予期しない動作を起こす現象であり、代表的なセキュリティホールの一つである。

通常は、バッファ領域を超える書き込みが発生しないように、プログラマが受け取ったパケット長を確認すべきところ、その確認を怠ることで簡単に発生してしまう。システム開発者側の人為的なバグの一種といえる。破壊者はこの脆弱性を利用して大量のデータをバッファに送り込むことにより、システムを破壊させることや、特別なプログラムを実行させたりすることを試みる。２００３年夏に流行した MSBlast ウイルス、及びその亜種ウイルスは、このバッファオーバーフローの原理を利用して感染し、猛威をふるった。

バッファオーバーフローは、何も Web システムに限った事ではない。メモリ領域の制御は、すべてのプログラマが気をつけていなければならないことである。

ここで言いたいことは、バッファオーバーフローはセキュリティホールであり、単なるバグではないということである｡この脅威は､「セキュリティがネットワーク管理者任せでは解決しないものである」ということを最も顕著に表しているであろう。

（ガイドライン１）

プログラマは、受け取ったパケット長を必ず確認する。
（ガイドライン２）
プログラミングに用いる言語選択の際は、より安全性の高い言語を使うことも検討すべきである。

4.3.7 Path Traversal（パスの乗り越え）

アプリケーションに渡されるパラメータを基にファイルの読み込みをしている場合に、この危険がある。例えば、すべてのページを共通のフォーマットにするためにテンプレートを使用して、メインのコンテンツをパラメータで指定するようなアプリケーションが挙げられる。
次のような Perl プログラムが実装されているとする。

```
#!/usr/bin/perl
# コンテンツの出力
open FILE, "$PARAMETER{file}.html";
while (<FILE>) {
print;
}
```

もし、

```
/etc/passwd%00
```

という値がパラメータにわたされたら、本来はＷｅｂディレクトリ以下のファイルしか表示されないはずが、/etc/passwd の内容がすべて出力されてしまうことになる。 このように別のディレクトリのファイルにアクセスさせることから、Path Traversal（パスの乗り越え）と呼ばれている。ユーザーがアクセスできるファイルに認証を掛けていたとしても、アプリケーションがアクセスできるファイルの制限とは別物のため、表示されてしまうことになる。
もちろん/etc/passwd に限らず、アプリケーションのソースファイル、サーバの設定ファイル、顧客情報データベースなどほぼすべてのファイルが対象になる。この対策はパラメータとして受け付ける値を制限するなどの方法がある。

参考 URL
「IPA ISEC セキュア・プログラミング講座」
http://www.ipa.go.jp/security/awareness/vendor/programming/
「@ＩＴ セキュリティフォーラム」
http://www.atmarkit.co.jp/fsecurity/

5　モラル

以上述べたようにセキュリティを保つにはハードウェアやインフラの面からのアプローチが必要であり、外部にサービスを提供するに当たっては、そのアプリケーションの作りこみにおいて注意するべき点が多々あることが分かった

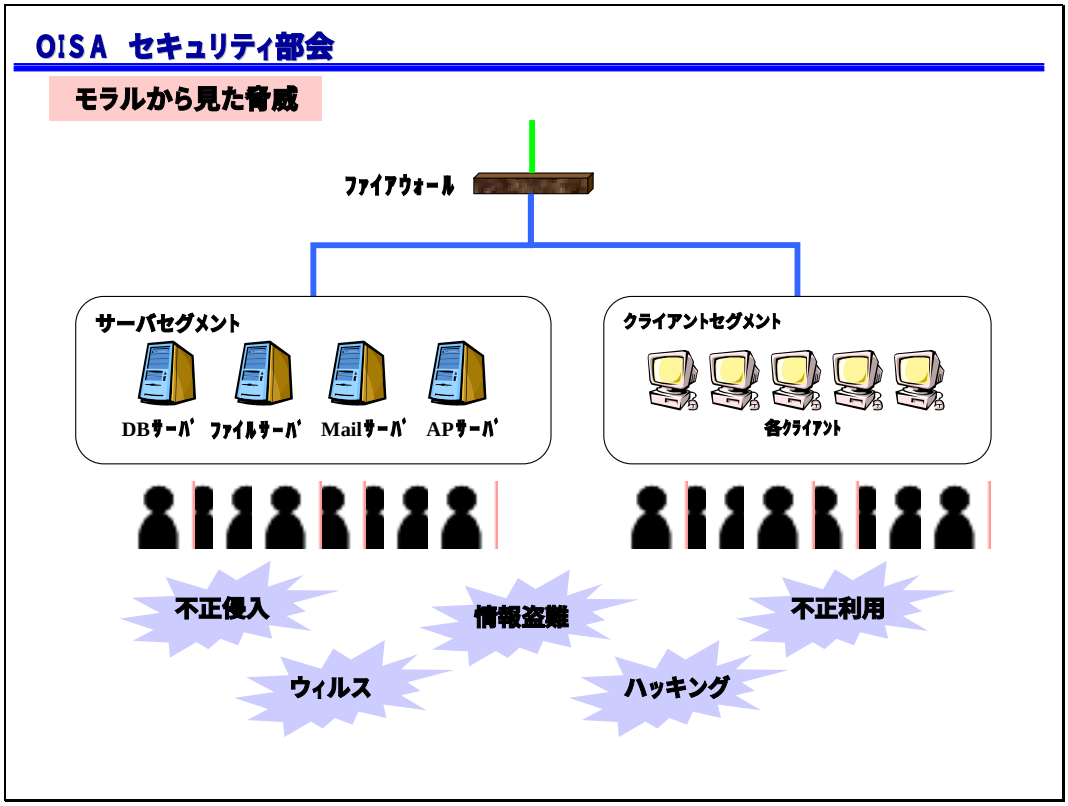

図 5 - 1 社内のセキュリティ

ところが、近年のセキュリティ事故を見ると、特に社内情報の漏洩においてはそのほとんどが社内で起こっていることが多く、社外アクセスに対抗するセキュリティ対策のみでは不十分であることが明らかになってきている。本節では、社内従業員個人のセキュリティ意識、すなわちモラルを高めることの重要性と、施策として情報セキュリティマネジメントシステムの構築を挙げ、その留意点について判りやすく述べる。

5.1 人間に依存するセキュリティ事故

近年起こった人的要因によるセキュリティ事故には、次のようなものがある。

例１　社内のアクセス制限

信販大手Ａ社のシステム開発・運用を請け負ったＴ社のサーバからＡ社のクレジットカード会員の個人情報がダイレクトメール会社に流出した。信販大手Ａ社は事実を公表し、対象者に対して商品券とお詫び状を配布した。結果、Ａ社にとって 8000 万円以上の損害となり、情報漏洩をおこしたＴ社にとっては信用失墜という大きな痛手をこうむることになった。

例２　社外からのアクセスの制限

Ｆ社で開発中のＷｅｂシステムについて、顧客からレビューを受けることになった。そこで、Ｆ社は開発サーバを一時的に社外ネットワークに接続し、顧客からインターネット経由で操作性やユーザインタフェースなどのレビューが行えるようにした。しかし、ある日、開発サーバ上の顧客のマスタデータなどの重要なデータが流出してしまう事件が起きた。

例３　ウイルス対策の規定

Ｉ社の社員Ｊがある日、覚えのないところからのメールを受け取った。メールには見たことのない拡張子のファイルが添付されており、とりあえず社員Ｊはファイルを開いてみることにした。その後、パソコンの挙動がおかしくなり、社員Ｊはウイルスに感染してしまったと思ったが、どのように対処すればよいかわからず、とりあえず、ウイルス駆除ソフトをインストールし、再起動をしてその日は退社した。翌朝、そのウイルスは全社に広まっており、業務に支障をきたすことになってしまった。

例４　持ち込みノートＰＣの危険性

Ｂ社の営業員が出先の業務でノートＰＣを使っていた。社内に戻り、ノートＰＣを社内ＬＡＮに接続したところ、社内にウイルスが蔓延してしまった。

例５　貸与ソフトウェアの管理

ある日、Ｅ社を退職した職員が、ソフトウェアのライセンス違反でメーカ(ソフトウェアを開発した企業)から訴えられた。

例６　バックアップに関する規定

Ｇ社では、毎日定時に顧客データベースのバックアップをＣＤ－ＲＯＭにとり、サーバ横の開架棚におかれたケースに入れている。ある日、悪意をもった者が開架棚からＣＤ－ＲＯＭを持ち出し社外に顧客情報が漏洩してしまった。

例７　社内のゴミの管理

Ｈ社では、社内のゴミはごみ処理業者が指定するビル内の共有スペースに廃棄されることになっている。ある日、表面に「焼却」と朱書きされたＨ社の帳票が共有スペー

スに廃棄されており、第三者がH社の帳票を持ち去ってしまい悪用されてしまった。

例８　メール送信による情報漏えい

Ｃさんは会社において、業務に関するメールの他に、私用メールの送信なども行っていた。ある日、業務機密の書かれたメールを取引先のＡｂさんに送信しようとしたところ、誤って知人のＡｃさんに送信してしまい、業務機密が社外に漏れることになってしまった。

例９　パスワード管理

Ｄさんは業務に用いるパソコンのパスワードをメモに書き、机に貼っていた。ある時、社内の悪意ある人間が、Ｄさんのパソコンにアクセスし、重要な業務機密を持ち出してしまった。

例で挙げたこれらの事故は、社内規定や従業員のモラルの欠如が原因で起こっている。例１、例２は社内の重要機密へのアクセス制限や社外からのアクセス方法に十分な規定や対策を考察していなかったために起こった事件である。また、例３、例４のウイルスによる事故例に関しては、技術的に対策をたてることと同時に、ウイルスを人為的に持ち込まない規定や、また、ウイルスが社内に持ち込まれたときの連絡・対策体制をあらかじめ策定しておく必要があるだろう。その他では例５、例６、例７に挙げたように、社内には情報漏洩が起こり得る要因がいくつもあることを認識し、規定を策定せねばならない。

また、社内規定だけでなく、従業員、個々人のモラルも求められる。例８で挙げたようにメールやインターネット接続を私用で用いることや、例９のようなずさんなパスワード管理は会社のリソースを脅かすことにつながることを認識しておきたい。

以上より、会社のセキュリティは技術的な要素ばかりでなく、人為的な要素からのアプローチも重要であることがわかる。

5.2 情報セキュリティマネジメントシステムとセキュリティポリシー

社内での個人個人のモラルを高く保つためには、いったいどのような取り組みを行えばよいのであろうか。近年、情報セキュリティマネジメントシステム（以下 ISMS と略す）という言葉が盛んに使われているが、これが、会社や組織全体のセキュリティを高めるのに効果的なアプローチである。

モラルは、個人に依存するものであるが、では従業員の行動は、社内でどのように決定されうるだろうか。例えば社内での行動が厳しく規制されている会社や組織ではモラルが高く、規制のゆるい組織ではモラルが低いように思えるが、実はそうではない。モラルの高さは、実際に従業員が主体となりその根底にあるルールを理解し、それを実践しているかどうかによって決まる。特に日本の企業ではこの傾向は高いと思われる。そして、従業

員のモラルが高ければ社内の規制をもコントロールすることができ、自主的な運営と効果の永続性が生まれる。この理想的な状態を実現するためには、これから述べるように組織的なアプローチが必須で、資産（人、物、金）も必要になるため、経営陣の大きな関与が必要となってくる。

つまり、まず企業が行うことは、このモラルの重要性をあまねく宣言することである。会社経営において、信用第一を標榜していることを、従業員に認知させることであり、そのことを、社外にもアピールすることである。これを核にして、ISMS を形作ってゆくことが大切である。この宣言をセキュリティ基本方針といい。企業の情報セキュリティの指針、すなわちセキュリティポリシーの要となる。

5.3 セキュリティポリシーの階層構造

セキュリティポリシーは、次のような階層構造から構成している。

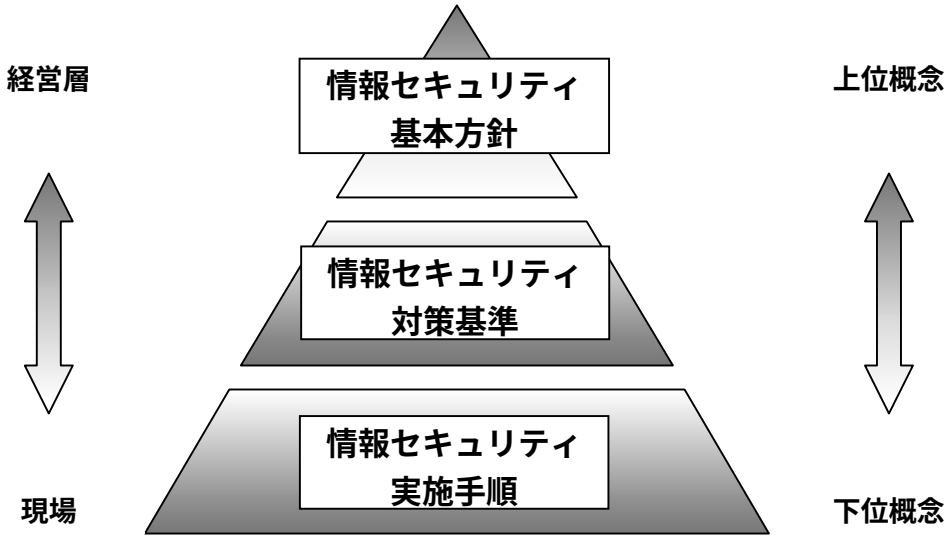

図 5 - 3 セキュリティ階層構造

①情報セキュリティ基本方針（以下「基本方針」という。）

企業における、情報セキュリティ対策に対する根本的な考え方を表すもので、企業が、どのような情報資産を、どのような脅威から、なぜ保護しなければならないのかを明らかにし、企業の情報セキュリティに対する取組姿勢を示すもの。

社内外にあまねく知らせられるべき宣言である。

②情報セキュリティ対策基準（以下「対策基準」という。）

「基本方針」に定められた情報セキュリティを確保するために遵守すべき行為及び判断

等の基準、つまり「基本方針」を実現するために何をやらなければいけないかを示すもの。

社内での基本的な考え方やルールを定めたものである。

③情報セキュリティ実施手順等（以下「実施手順」という。）
ポリシーには含まれないものの、対策基準に定められた内容を具体的な情報システム又は業務において、どのような手順に従って実行していくのかを示すもの。

セキュリティを守るための、個々の手順書、運用マニュアル等である。

通常、セキュリティポリシー文書といわれているものは、上位の 2 つであり、それに日々に守るべき実施手順が連なっている。これらの階層構造が企業の隅々まで行き渡り、ISMS が実施されていることを示すことが、企業の情報セキュリティ、従業員の情報セキュリティ確保の証となる。

5.4 組織の形成

それでは、ISMS の策定に当たるにはどのような取り組みが必要であろうか。まず実施体制の確立が必要であり、情報セキュリティを推進する責任部門を定めることになる。これは大きな企業では情報システム部門が当たることが多く、中小企業では社内のネットワーク管理者がその任に当たることが多い。但し、該当組織のみでなく、全社的な協力が不可欠であるため、関連する部門の代表が出席する、セキュリティ委員会を設けることがあわせて行われる。
いずれにせよ、以上の組織は、経営陣トップダウンで作成され、責任と権限を明らかにすることがポイントであり、この組織作りの良否がその後の作業を決定する。また、この時に上記基本方針の作成も行われることになる。

5.5 対策基準の作成

対策基準を作るには、闇雲に思いついた要件をルール化するのではなく、どこまでの対策を、どのように行うかということを定めなければならない。これを、リスク評価という。
まず、守るべきものを明らかにする必要があるが、これは、その企業が業務を行う上で重要な資産を分類し、その価値を洗い出すことからはじめる。そのポイントは、
①機密性　　外部にもれてはいけない
　　（例えば、人事情報、顧客情報などは機密性の高い資産である）
②完全性　　正確でなくてはいけない、変更されてはいけない

（経営データや、公開 Web など）

③可用性　いつでも使えなくてはいけない、使いやすくなくてはいけない

（情報機器や、ソフトウェアなど）

の 3 点であり、この度合いにより、その資産の価値を定めることになる。

続いて、これら情報資産に対する脅威をあらゆる方面から洗い出し、これらを組み合わせて、考えられるリスクを抽出する。脅威の大きさと、先ほどの資産価値の大きさに応じて、リスクの値が求められる。リスクには網羅性が求められるため、定量的な判断が困難なリスクについても、一般的な知識や、過去の経験値によってリスク値を判断する。

リスクの値が決まれば、これに対して、どのレベルのリスクまで対策を講じるべきかという具体的な基準と、対策の優先順位が決められる。このように、リスクの評価を行ったうえで初めて、対策検討に移ることができるのだが、対策の実施には資源を使うため、どの対策をどこまで行うかという判断には経営的な判断が求められる。つまり、前述のセキュリティ委員会などを開き、ここでも経営陣の意志を確認することが必要となる。

5.6 実施手順の策定

基本対策を基にして、実施手順を策定する。通常、作業の現場で作成されるマニュアルや手順書は、これに当たる。これは現場の意思が反映されているが、ここで重要なのは、この各々の手順が、全社のセキュリティポリシーに照らし合わせて妥当なものであり、それが全社レベルの方針と合致していることが示されることである。

簡単に言うと、この「手順書」や「運用マニュアル」が、何のために存在し、何を守るために必要なのかを、現場で働く従業員が常に把握しておくことが、全社の情報セキュリティのレベルを維持するためにもっとも必要なことである。

5.7 ISMS の運営

ISMS は、単にマニュアルを作り、それを守らせることができれば終わりというものではない。現在の情報社会の変化はめざましく、それに対応して、技術も刻々と変化している。また、設備や人的要因も変化する。そのため、この中にあって、情報セキュリティの取り組みについても、迅速な対応が迫られる。また、対策基準や実施手順についても完全ではなく、運営してゆく上で、様々な問題点が発生し、これに対しても対策を講じる必要がある。

これらを有効に利用して、ISMS の継続的な改善を行うこと。つまり、PDCA を回し、システム全体を「活きのいい状態に保つ」ことが ISMS 運営の大きな意義である。

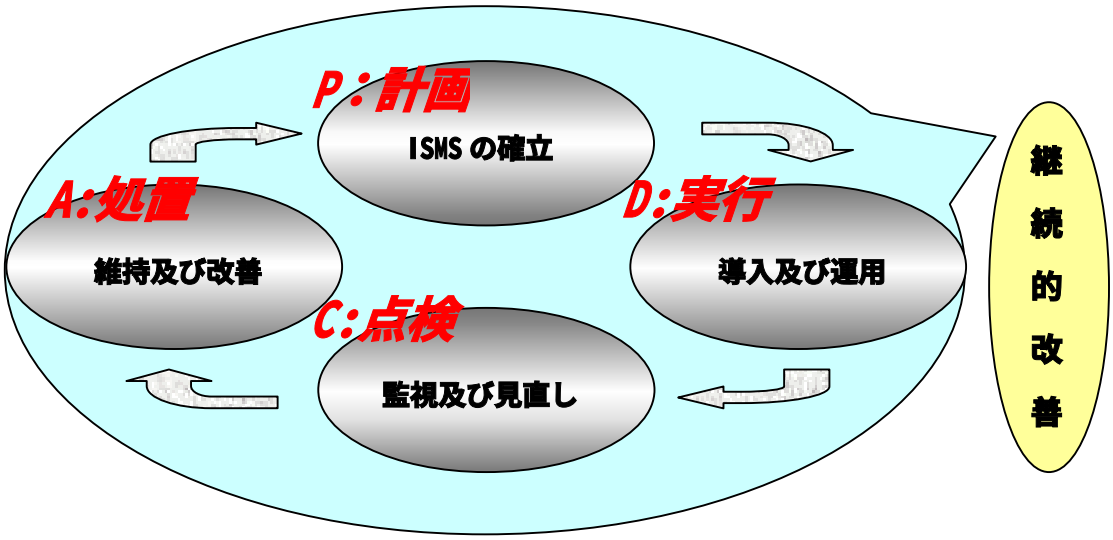

図 5 - 7 ISMS の PDCA サイクル

図に示すように、一連のサイクルを常に意識して作業を行うことが求められる。特に、実施状況を評価して見直しを行い、新たな対策をセキュリティ委員会の場で検討した上で、次の計画に生かしてゆくことにより、継続的改善を行うことが、動き出したシステムには不可欠である。以上のように、永続的に向上を図ってゆくことが、ISMS の基本理念である。

以上、ISMS は、企業のセキュリティを確保する上で有効なアプローチであり、現在、このシステムを認証する制度として、BS7799 や ISMS 適合性評価制度が挙げられ、約 400 社が認証を受けている。(2004 年 1 月調べ)。

参考 URL

「情報セキュリティポリシーに関するガイドライン」
http://www.kantei.go.jp/jp/it/security/taisaku/guideline.html
「経済産業省、情報セキュリティ管理に関する国際的なスタンダードの導入及び
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の改革について」
http://www.meti.go.jp/kohosys/press/0000831/
「情報セキュリティマネジメントシステム（ISMS）適合性評価制度の状況（JIPDEC)」
http://www.isms.jipdec.or.jp/

6 まとめ

旧来よりある企業内に閉じたビジネスネットワークや、公衆ネットワークである電話網などは、中央管理型であり、中央のセキュリティレベルを高めることによって、ネットワーク全体のセキュリティを強固に保つことが可能であった。中央の責任は重大であったが、そこには専門家が配置され、高レベルのセキュリティ管理が行われていたのである。そのため利用者がセキュリティに関与する所は少なく、単にサービスを享受するレベルにとどまっていても問題はなかった。これに対してインターネットは分散型のネットワークであるために、セキュリティに関する責任も分散されている。言い換えると、個々のネットワークのセキュリティレベルを高めない限り、そのネットワーク内のみならず、他のネットワークにまで被害を与えてしまうといった特徴を持っており、個別ネットワークの管理責任は大きい。今後インターネット社会の中でビジネスを行ってゆく我々は、その脅威とセキュリティ事故による社会的な影響を認識することが大切である。そして、企業においては、単にサービスを利用するのみに留まらず、ネットワーク全体への参加意識を持って組織ぐるみでセキュリティ確保に取り組むことが必要である。経営陣以下、従業員個々がセキュリティの重要性を理解し、対策を実践してゆくことが、企業としてのインターネット社会への責任あるかかわり方であろう。