情報資産活用のための情報セキュリティガイドライン

平成 12 年 7 月

社団法人　情報サービス産業協会

はじめに

近年、インターネットおよびイントラネットの普及により、情報システム及びネットワークが社会的な基盤として重要な役割を果たすようになってきています。また、企業においても情報資産（情報および情報システム）の有効な活用がその企業の将来を左右するといっても過言でない程､重要な経営課題となっています。

このような情報化社会において企業内および企業間で自由な情報の流通を行うためには、交通社会における交通ルールのようにある種の秩序が必要であり、それがまさに情報セキュリティであると言えます。一方、不正アクセスやプライバシー侵害などの情報資産に関わる犯罪が大きな社会問題となっており、情報資産が適切に運用されないことによる社会生活への影響も大変大きなものとなってきています。

こうした状況の中で、「情報関連技術の開発促進、情報化の基盤整備等を通じ、情報サービス産業の健全な発展を図るとともに、我が国の情報化を促進し、もって経済・社会の発展に寄与すること」を目的とする情報サービス産業協会会員企業においては、情報セキュリティに対する取組み方針を明らかにすることや実効的なセキュリティ対策を実現することが求められています。

情報サービス産業協会セキュリティ委員会では、会員企業を含むユーザの皆さまが情報セキュリティに対する取組み姿勢を明確にしたり、セキュリティ対策を実現する際に役立つよう、「情報資産活用のための情報セキュリティガイドライン」を作成いたしました。本ガイドラインが、皆さまの会社における情報セキュリティについて検討される際の一助となれば幸いです。

平成 12 年 7 月

（社）情報サービス産業協会
セキュリティ委員会
委員長　井上　友二

セキュリティ委員会・ガイドライン策定部会　名簿

部会長	西尾　秀一	(株)エヌ・ティ・ティ・データ　技術開発本部 マルチメディア技術センタセキュリティ担当
WGリーダ	君塚　邦男	住友金属システム開発(株)　品質保証部
〃	谷川　智則	東芝エンジニアリング(株)　システムインテグレイション事業本部　企画開発室事業開発推進担当
委　　員	長内　雅春	(株)アルゴテクノス21　サービスビジネス事業部 ネットワークサービス部長
〃	上髙　正義	(株)伊勢丹データーセンター　システム監査室室長
〃	伊藤　成人	(株)インテック　ネットワーク事業本部 ネットワークセキュリティセンター担当課長
〃	神　博史	(株)インフォメーション・ディベロプメント NW 事業本部 NS 部長
〃	山城　健司	(株)エスシーシー　システム開発事業部 事業開発部　担当部長
〃	長谷川　新	(株)エヌ・ケー・エクサ 技術部 IT コンサルティング推進チーム担当部長
〃	藤沢　寛岳	(株)オージス総研　ヘルプデスク事業部 テクニカルサポートチームマネジャー
〃	野村　武史	オムロンソフトウェア(株)　技術開発部
〃	増田　邦彦	川鉄情報システム(株)　技術管理本部 技術総括部長
〃	今井　豊治	(株)シー・エス・イー　技術営業本部統括部長
〃	柏木一亜紀	住商情報システム(株)　ネットワーク営業部 ネットワーク第 2 課
〃	河合　基	中電コンピューターサービス(株)　常務取締役
〃	大篭　高之	東芝アドバンストシステム(株) リーディングソフト開発第三部主任
〃	国井　孝昭	日本アイ・ビー・エム(株) ＦＭコンサルティング次長
〃	足海　義雄	(株)日本システムディベロップメント 東京オープンシステム営業部　課長代理
〃	松井　泰	(株)日本総合研究所 セキュリティ事業推進部部長
〃	大神　祐二	日本ナレッジインダストリ(株) ニューテクノロジ推進部
〃	中井　真治	日本ユニシス情報システム(株) 業務企画部　業務グループマネジャー
〃	阿河喜一郎	(株)菱化システム　取締役機器部長兼技術室部長
事務局	佐藤　厚夫	(社)情報サービス産業協会　調査企画部

タイトル：「情報資産活用のための情報セキュリティガイドライン」

目次

本ガイドラインの構成

本ガイドラインの構成は以下のようになっています。

第１章 用語の定義と他ガイドラインとの関係

本ガイドラインにおける用語の定義及び通産省等から出されている他のガイドラインとの関係について述べる。

第２章 セキュリティ対策の基本的な考え方

企業のセキュリティ対策の方針決定から運用までの標準的な手順について述べる。

第３章 セキュリティポリシー

情報セキュリティに対する企業の取組み方針を明確にするセキュリティポリシーに関する解説と、その作成方法について述べる。

第４章 セキュリティ対策策定手順

セキュリティ対策を策定する標準的な手順と、その際に注意すべき項目について述べる。

第５章 情報システムのセキュリティ対策

第４章の手順に従ってセキュリティ対策を実現する上で特に重要な、ネットワークセキュリティ、アクセス制御、及び、コンピュータウイルス対策を取り上げ、その実現方法の概要について述べる。

第６章 セキュリティ対策の運用

セキュリティ対策は技術的な対策を行うだけでなく、日々継続して適切に運用することが重要である。この章ではセキュリティ監査、セキュリティ侵害の検知方法、セキュリティ教育について述べる。

第７章 参考文献および関連リンク

ガイドライン策定にあたり参考にした文献およびインターネット上の関連リンクを記載する。

第１章　用語の定義と他ガイドラインとの関係

１．１　用語の定義

本ガイドラインで用いられる主な用語の定義は、以下のとおりである。
なお、【番号】で巻末に参考資料または参考 URL があることを示す。

（1）コンピュータ

ここにいうコンピュータとは、クライアント・サーバ・システムにおけるサーバ及びクライアント（ネットワークの接続を制御する装置およびネットワークに接続され得る装置であり，ルータ，交換機等の通信用装置及びその他専用装置を含むもの)、メインフレーム・システムにおけるホスト・コンピュータ及び端末機で、通信回線等で接続された演算、記憶、制御及び入出力の各機能を有する装置を示す。

（2）ネットワーク

コンピュータとその周辺機器が、ＬＡＮ等の通信網でシステムとして結合され､更に外部とはインターネット､イントラネット等により情報のやり取りが可能となっているオープンネットワークシステムを指す。

（3）情報システム

企業活動に必要な種々の情報を処理するためのシステム。コンピュータ、端末機、ネットワーク、プログラム及びオフライン機器等により構成される。

（4）データ

コンピュータシステムの記憶装置又は記録媒体上に蓄積／保存されているもので、システムが実行中に派生するもの、オンラインにより蓄積されたもの、バックアップのために圧縮されたもの、通信メディアで転送中のもの、ログ、データベースなどを総称して言う。

（5）情報

一般にはデータと区別され、「データを解析して得られる人間の知識や知的行動に影響を及ぼすもの」とされているが、本ガイドラインではデータを含む広い意味で情報という言葉を用いている。

（6）プログラム

著作権法では、電子計算機を機能させて一意の結果を得ることが出来るように、これに対する指令を組合せたものとして表現したもの、と定義されている。【1】

（7）ドキュメント

システム開発に関する一切の書類、運用に関する手順書、マニュアル類、およびプログラムリスト・データリスト、さらに業務上知り得た顧客名簿などの情報資料のこと。なお、これらの電子化されたものも含むものとする。

（8）記録媒体

プログラム、情報を記録するための機器。ディスク、磁気テープ、フィルム、カード、用紙等。

（9）ファイル

コンピュータシステムの記憶装置又は記録媒体上に記録されているプログラム、データなどを総称して言う。

（１０）セキュリティポリシー

本ガイドラインでは企業レベルのセキュリティポリシーを対象としており、経営的な観点から情報セキュリティに対する基本的な考え方や取組み姿勢を明文化したもので、その企業のすべての社員を対象とした情報セキュリティに対する行動指針のことを示す。

（１１）セキュリティ方針

セキュリティ方針とは、情報を管理、保護、配布するといった情報のライフサイクルに関するさまざまな要件について、その目標、適用範囲、責任範囲などの方針を示したものであり、セキュリティポリシーの骨格をなすものである。システムレベルのセキュリティ方針においては、情報の扱いに関する規則や手順の集りで、システムの信頼性を確立する枠組となるものである。すなわちこれは、システムにおいてユーザ、プロセス、プログラムなどの主体が、ファイル、ディレクトリ、デバイス、ウィンドウなどの特定のオブジェクトにアクセスできるかどうかを判定するための規則である。【2】

（１２）情報資産

企業の第４の経営資産として重要性を増す「情報資産」は、情報そのものと情報システムの両方を指す。すなわち、社内の各種情報、社員が業務上知り得た顧客情報等、および、ハードウェア、ソフトウェア、ネットワーク、各種データファイル、システム開発・運用に必要な要員やドキュメントなどを含む。

（１３）セキュリティ機能

情報及び情報システムの機密性、保全性及び可用性を確保するために情報システムが装備する機能。

（１４）識別・認証

システムは、システムを利用する者が利用に際して確かに本人であることを確認（識別）できなければならない。そのための情報には、本人しか知り得ない情報（例えばパスワード）や本人の生態的な特徴（例えば指紋、声紋、網膜紋など）を利用する。識別により確かに本人であることが確認されたとき、システムは、その識別により許された権限の範囲内でシステムを利用することを許可（認証）する。

（１５）アクセス制御

アクセス制御とは、コンピュータシステムのすべてのプログラムやデータに対する利用者ごとのアクセス資格をあらかじめ設定して登録し、実際のアクセスの都度その資格をチェックし、権限外の利用を排除する機能である。なお、通産省告示第５１８号「情報システム安全対策基準」の、技術基準　故意・過失対策機能の中では、アクセス制御機能として個別の機能があげられている。【3】

（１６）セキュリティ侵害

セキュリティポリシーに基づく対策のセキュリティホール（弱点）を探し出して攻撃し、侵入･破壊・改ざん・盗聴・なりすまし・盗難・流出・否認・ウイルスなどの企業の情報資産への脅威を与えること。

（１７）不正アクセス

アクセス制御機能を有する情報システムにネットワークを通じて他人の識別符号あるいは制限を免れる情報または指令を入力して侵入し、不正な使用を意図的に行なおうとする行為。【4】

（１８）コンピュータウイルス

プログラムファイル、ハードディスク等に寄生するプログラムで、自分自身を勝手に他のプログラムにコピーすることにより増殖し、あらかじめ用意されていた内容により予期できない動作を起こすことを目的としたプログラムである。寄生しても全く被害を及ぼさないものからシステムに重大な被害を及ぼすものまで存在し、日々新しいウイルスが発生している。

（１９）緊急時対応計画

緊急時対応計画とは、システムの異常事態の発生に応じた早期発見、応急対応、機能回復のそれぞれに関する行動規準を定め、機能に障害が生じた際の業務中断や機密漏洩を防止軽減するものである。すなわち、一般的な予防対策としてのリスクコントロールに加え、緊急事態を考慮した対策によって、セキュリティシステムが構築されるのである。【5】

（２０）セキュリティ監査

企業内の各部門に対し、セキュリティポリシーおよびそれに基づく対策・取り決め・手順等が遵守されているかをチェックし、それらが機能しているかを評価すること。社内／外の専門家により行われ、経営層へ報告されるが、情報システム監査の一部として行ってもよい。

（２１）バックアップ

記録媒体に記録しているプログラム、情報等と同一の内容を別の媒体に一定間隔で保存・記録すること。

（２２）ログ

システムのセキュリティ方針に基づいたシステムの動作履歴／動作経緯、使用／利用記録などを記録することで、記録の改ざん、削除、破壊及び漏洩の防止措置を施し、安全な方法で一定期間保存する。

１．２　国際標準、他ガイドライン等との関係

国際標準化機構(ISO)で ISO/IEC 15408 Evaluation Criteria for Information Technology Security として製品やシステムのセキュリティ評価基準が国際規格化された。この国際規格の基となったものは、Common Criteria for Information Security Evaluation Version 2.0（通称、Common Criteria、以下、CC または CC V2.0）である。CC V2.0 は、セキュリティ評価基準を持っている米、英、仏、独、加、蘭の各国が共同で開発したものである。【9】

CC V2.0 は、次の３つのパート構成となっている。

Part１：概説と一般モデル

CC で使用する用語、セキュリティコンセプトや評価コンセプトについて規定

Part２：セキュリティ機能要件

製品やシステムに必要な監査や暗号化、データ保護などのセキュリティ機能要件を規定

Part３：セキュリティ保証要件

上記機能要件を実装するために必要な要件（保証要件）とそのレベル（保証レベル）を規定

CC V2.0 は、市場に投入される製品でも、一般企業のネットワークシステムでもセキュリティを評価する基準として、あるいはセキュリティポリシーを検討するベースとして使用できる。とくに、Common Criteria をベースに米国標準技術局（NIST：National Institute of Standards and Technology）が開発した CS2 – Protection Profile Guidance for Near Term COTS Version 0.3 は、汎用的な商用システムへの適用を前提にしており、一般ユーザのネットワークシステムのセキュリティやセキュリティポリシーの開発を検討する上でガイドとして有用である。

Common Criteia 以外のセキュリティ関係の標準としては、IETF(Internet Engineering Task Force)の技術報告、RFC 2196 Site Security Handbook がある【7】。これは、インターネットを使用する際のセキュリティポリシーを作成するガイドである。この他にも、経済協力開発機構（OECD）の Guidelines for the Security of Information Systems や、財団法人金融情報システムセンターが作成した「金融機関等におけるセキュリティポリシー策定のための手引書」などがある。いずれも、システムのセキュリティを考察したりセキュリティポリシーを作成する際に大変有用な情報が記載されている。

当委員会では、Common Criteria に規定されている用語やモデル、機能要件などを主に調査した。また、必要に応じて、上記のサイトセキュリティハンドブックや金融機関等におけるセキュリティポリシー策定のための手引書なども調査した。したがって、本書の考え方の基本は Common Criteria に由来し、あるいはその底流として Common Criteria を使用している。

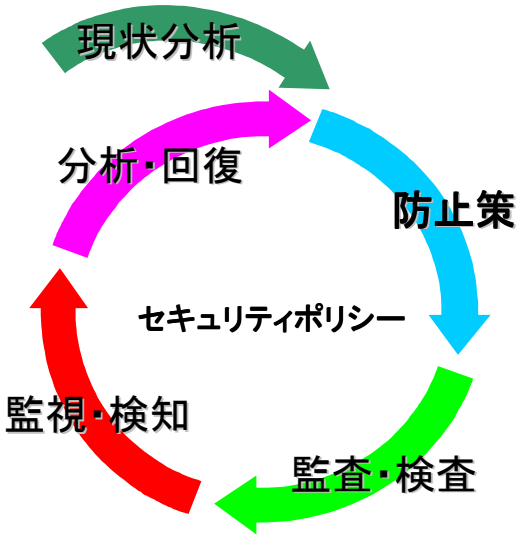
第２章　セキュリティ対策の基本的な考え方（セキュリティ管理サイクル）

企業においてセキュリティ対策を考える際に注意しなければならない重要な点のひとつが「セキュリティは技術だけでは守れない」ということである。企業を取り巻く多様な脅威の存在に対して、技術ばかりでなく、しくみ・運用・教育等を含めた総合的･全社的な情報セキュリティに対するアプローチが必要である。

また、セキュリティ対策は一度防止策を考えればそれで十分ということはなく、新たなセキュリティホールや脅威が日々発見されているというのが実情である。

このため、図表２－１に示すように、「現状分析」→「防止策」→「監査・検査」→「監視・検知」→「分析・回復」→「防止策」→…という、セキュリティ管理サイクルに沿ったセキュリティ対策を考えることが重要である。さらに、それらのセキュリティ管理サイクルの各フェーズにおける実施事項は、情報セキュリティに対する企業の取組み方針であるセキュリティポリシーに立脚したものであることが重要であり、これにより保護すべき情報資産が明確にされ、それに対してどのような手段でセキュリティ対策を実現するかを決定することが可能となる。

図表２－１　セキュリテイ管理サイクル



第３章　セキュリティポリシー

３．１　セキュリティポリシーとは

３．１．１　セキュリティポリシーの必要性

近年、情報および情報システムの活用が企業にとって重要な経営課題となってきている。それに伴い、企業が保有している情報や情報を活用するための基盤（情報システム）が企業にとって重要な情報資産であるという認識が高まっている。その一方で、情報漏洩や不正アクセスなどの情報に関わる社会問題が急増しており、いかにして企業の情報資産を守るかが課題となっている。情報サービス産業関連企業においてはその事業の性格上、情報資産の取り扱いについて特に注意が必要であることはいうまでもない。

しかしながら、企業ネットワークの高度化・分散化やインターネット接続などにより、従業員が情報を扱う場面が多様化しており、企業内における情報の取扱いが個人に委ねられるケースが多くなっている。このような環境下では、情報資産の保護が従業員の個人的な考え方や判断によってなされることがないように、企業としての統一的な情報セキュリティへの取組み姿勢を明確に示す必要がある。

３．１．２　セキュリティポリシーの定義

セキュリティポリシーと呼ばれるものにはさまざまなレベルのものが存在するが、一般的にはその適用範囲によって以下の３つのレベルに分類される。

（1）企業レベル

企業において、経営的な観点から情報セキュリティに対する基本的な考え方や取組み姿勢を明文化したものであり、その企業のすべての社員を対象とした情報セキュリティに関する行動指針といえる。

（2）システムレベル

経理システムや人事システムといった特定のシステムに関するセキュリティ対策を網羅的に規定したものであり、そのシステムに関わるすべての社員を対象としたポリシーである。例えば、人事データベースに含まれる各種社員情報へのアクセス権限をどのように設定するかというルール

がこれにあたる。

（3）技術レベル

情報システムに関わる製品や技術を安全に導入するための詳細なルールやパラメータの設定を示す。例えば、ファイアウォール製品において、どのようなパケットの通過を許可するかといった設定がこれにあたる。

本ガイドラインでは（1）の企業レベルのセキュリティポリシーを対象とし、以下これを「セキュリティポリシー」と呼ぶことにする。

セキュリティポリシーは、経営者が従業員に対して示すものであり、企業の情報セキュリティに対する目標及び目標を達成するために従業員がとるべき行動の原則を伝えるメッセージである。その意味で、セキュリティポリシーを示すことは重要な経営方針のひとつを示すことに他ならない。一方、従業員全員がこの経営方針を共通認識として理解し実践することは、従来個人的な判断で行っていた情報資産の保護を、統一された判断基準で行えるような企業風土を生み出すことにもなる。このようなことから、一般にセキュリティポリシーは企業固有のものであり、他企業のセキュリティポリシーをそのまま持ってきても使うことはできない。

３．１．３セキュリティポリシーの位置づけ

セキュリティポリシーと企業の経営理念、各種規定、ガイドライン等との関係を図表３－１に示す。

■企業理念

企業の哲学や信念を示したものである。例えば、「お客様の秘密は必ず守ります」といったスローガン的な示され方をする場合がある。

■セキュリティポリシー

企業理念に基づき、企業の目標、考え、価値観などを経営者の言葉で明確に述べたものである。例えば「お客様の秘密情報は当社にとって最重要の情報であり、正当な必要性に基づく情報へのアクセスのみが許可される」といった方針が示される。

■規定・標準

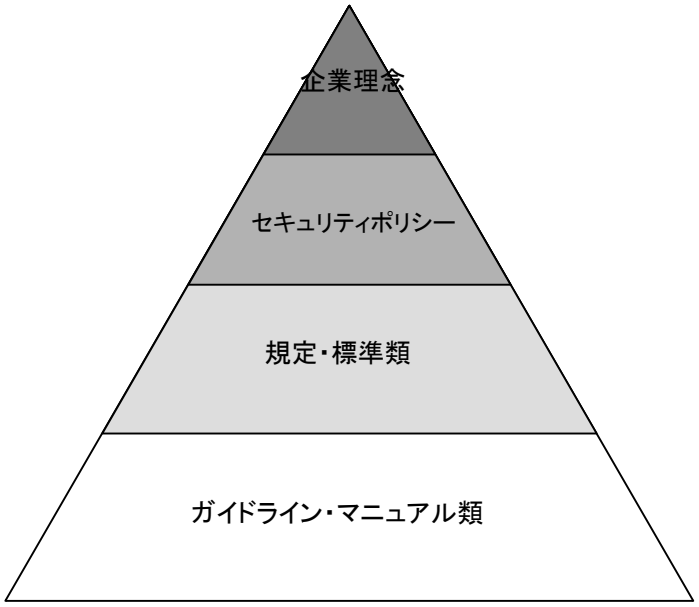
セキュリティポリシーに基づき、従業員が必ず守らなければならない企業としての規則・標準類である。例えば、「お客様の秘密情報は（極秘）情報とし、ネットワークを通じて情報を流通させる場合には必ず暗号化しなければならない」という規定が示される。

＊セキュリティポリシーの一部として規定・標準類を含める考え方もある。

■ガイドライン・マニュアル

ある特定分野・製品・システムにおいて、セキュリティポリシーや規定などを適用するための実施方法や手順を明文化したものである。一般的には強制力のない推奨事項について記述する。例えば、「営業部内メールシステムにおけるファイル暗号化手順書」といった形で示される。

図表３－１　セキュリティポリシーの位置づけ



３．１．４　セキュリティポリシーの構成

セキュリティポリシーの構成としては、例えば以下のような項目について記述することが考えられる。

（1）趣旨・目的

セキュリティポリシーがなぜ必要で、どのような課題を解決し、何を達成するのかということを明らかにする。経営者の意思表明であり、経営者自らの言葉で記述すると良い。

（2）適用範囲

セキュリティポリシーが適用される人、情報資産を明らかにする。

（3）位置付け

社内の他の規定類との関係や企業理念等との関係を明らかにする。現存する規定に抵触する場合の扱いについても記述しておく。一般的にセキュリティポリシーは他の規定よりも優先される。

（4）セキュリティ方針

「ドキュメント管理」「情報システム利用」「入退室管理」などの情報セキュリティに関する様々な要件について、それぞれの方針、目的、目標、適用範囲、責任範囲、適用の例外などを記述する。さらにその方針が守られなかった場合にどのような不利益をもたらすかについても記述すると効果的である。

（5）運用体制

セキュリティポリシーを統括する役員、運用する全社組織や各部門におけるセキュリティ管理体制を明らかにすると共に、それぞれの責任範囲を明確にする。

（6）監査体制

セキュリティポリシーが適切に運用されているかどうかを監査する組織とその方法、権限について記述する。

（7）違反者への罰則

セキュリティポリシーに対して違反行為があった場合の罰則等について記述する。

３．１．５　セキュリティポリシーの効果

セキュリティポリシーを作成することによる具体的な効果には以下のようなものがある。

○企業が保護すべき資産を明確にでき、効果的かつ効率的なセキュリティ対策が実現可能である

○情報資産が企業秘密として不正競争防止法上保護される

○従業員のセキュリティに関する意識の高揚と共有化が図れる

○従業員の義務、権利、責任を明確化できる

○不正従業員に対する懲戒処分や解雇といった対処を可能とする

３．２　セキュリティポリシーの作成と運用

３．２．１　セキュリティポリシーの作成から運用までの手順

セキュリティポリシーを作成する手順についてはいろいろな方法があり、各企業の実情に合わせた作成方法を選択する必要がある。

以下に、セキュリティポリシーの作成から運用までの標準的な手順を示す。これらを全て自社で行うことが難しい場合は、市販されているセキュリティポリシーに関する文献を叩き台として自社セキュリティポリシーを作成したり、外部のセキュリティコンサルテーション会社の協力を仰ぐことも有効な手段である。

（1）作成準備

・セキュリティポリシー作成プロジェクトチームの立上げ

・役員のサポートのとりつけ

・外部ガイドライン等の調査

（2）保護すべき情報資産の明確化

・社内を流通する情報の洗出し

・社内で利用されている情報システム、情報伝達手段（媒体）の洗出し

・情報資産の重要度に関する優先順位付け（どの資産が重要か？）

（3）リスク分析

・重要な情報資産に対する脅威の洗出し

・情報資産の侵害による影響、被害の見積もり

・セキュリティ要件の決定

（4）セキュリティ目標の明確化

・リスク分析の結果を受けて、セキュリティをどこまで確保すべきかを決定

（5）セキュリティポリシー（セキュリティ方針）の明確化

・セキュリティ要件毎に順次セキュリティ方針を決定

（6）セキュリティポリシーの執筆およびレビュー

・ドラフト版の執筆

・社内関連部署への照会

・現行の規定類との整合性チェック

・修正作業

（7）経営者の承認・施行

・経営者、役員等による承認

・セキュリティポリシーの施行

・運用、監査組織の整備

（8）セキュリティポリシーの教育

・啓蒙活動

・社員教育

（9）セキュリティポリシーの運用、監査

・セキュリティポリシーの遵守状況のチェック

・必要に応じたセキュリティポリシーの改訂

なお、この手順はあくまで企業レベルのセキュリティポリシーの作成および運用手順であり、この後に社内規定、標準類の制定や各種ガイドライン、マニュアルの整備、緊急時対応計画の策定などを行う必要がある。

３．２．２　セキュリティポリシーの記載内容

セキュリティ方針等として記述すべきセキュリティ要件、および、運用・監査に関する項目の例を示す。

■情報に関する項目

・情報取扱い種別

情報の価値や重要性に応じたランクづけの基準と、ランクに応じた情報の取り扱い方法を記述。

・情報取扱者

情報管理者、情報所有者、情報利用者などの定義とそれぞれの役割、責任を記述。

・情報のライフサイクル

情報取得、生成、流通、保管、複製、破棄といった情報のライフサイクルと、それぞれのサイクルにおける情報管理ルールの考え方を記述。

・その他特に重要と思われる項目

プライバシー情報の保護、知的財産権の保護など。

■情報システムに関する項目

・情報システム種別

情報システムの重要性に応じたランクづけの基準と、ランクに応じた情報システムが具備すべきセキュリティ機能について記述。

・情報システム取扱者

情報システム管理者、情報システム利用者などの定義とそれぞれの役割、責任、権利を記述。

・情報システムの物理セキュリティ

情報システムを設置する場所などに関する物理的なセキュリティ対策の方針を記述。

・情報システム管理方針

情報システムの管理における、ハードウェア管理、ソフトウェア管理、操作方法、ドキュメント管理などの方針を記述。

・情報システム利用方針

情報システムを利用する際の原則的な方針を記述。私的利用に関するルールについても記述。

・情報システム選定、構築基準

情報システムを構成する製品や構築のための外注先、取引先を選定する際の基準を示す。

・その他特に重要と思われる項目

ネットワークセキュリティ（外部接続条件など）、コンピュータウイルス対

策、インターネット、イントラネットの利用ルールの考え方、電子メールの利用ルールの考え方など。

■アクセス制御に関する項目

・識別、認証

情報にアクセスする際に個人を特定するためのＩＤおよびパスワード付与基準、個人の正当性や情報アクセス権限を検証するしくみ等について記述。ＩＤやパスワードの管理方法についても明確に定義。

・アクセス認可

さまざまな情報資源へのアクセスルールの考え方、権限取得や設定のルールの考え方などを記述。

・物理的アクセス制御

入退館、入退室に関するルールや資格定義等の考え方や、鍵の管理方法などについて記述。

■運用・監査に関する項目

・運用体制

セキュリティポリシーを実践していく体制を記述する。情報セキュリティ統括役員、管理職、一般社員、協力会社社員などそれぞれの役割、責任について明らかにする。

・監査体制

セキュリティ監査の体制、実施方法、ログの取得方法などに関するルールの考え方を記述。

・教育、訓練

セキュリティポリシーの従業員等への教育及び訓練に対する考え方を記述。

・セキュリティ侵害発生時の対応

セキュリティポリシーに違反する事が発生した場合の対処方法、罰則等について記述。緊急時対応計画や復旧計画に関する事項を記述してもよい。

３．２．３　セキュリティポリシー作成上の注意

有効なセキュリティポリシーを作成する上での注意点やセキュリティポリシーを考える上で誤解されやすい点などを以下に述べる。

○作成に際しては十分に現状分析、ヒアリング等を行い、社内の現状の運用状況と大きな乖離が発生しないように考慮する。これを怠ると理想論の押し付けになってしまい、従業員に受け入れられなくなってしまう。実行不可能なセキュリティポリシーは意味がないだけでなく、新たなセキュリティホールを作り出してしまう危険がある。
○セキュリティポリシーは全従業員が遵守すべきものであり、強制力を持たせることが必要である。このためには、経営者や役員の承認を得ることが重要である。
○他の社内規定と矛盾のないものにする必要がある。場合によっては他の社内規定を改定または廃止することも考える。もちろん新たな規定を制定する必要がある場合もある。
○各種役割を担う組織や人の義務、権利、責任については複数の解釈が存在しないよう、明確に記述する。特に責任範囲を明確にしておくことは重要である。
○セキュリティポリシーは特定の技術や製品に依存するようなものであってはならない。また、ガイドライン、手順、マニュアル等と混同されがちであるので注意が必要である。
○市販のセキュリティポリシーの辞書や他社のセキュリティーポリシーをそのまま引用したりしてはならない。あくまで自社の言葉で記述することが重要である。なぜなら、セキュリティポリシーは経営方針であり、企業風土に根ざしたものでなければならないからである。

３．２．４　セキュリティポリシー運用上の注意

セキュリティポリシーを実効的なものにするためには､運用段階が重要であり､そこで注意する点を以下に述べる。

○セキュリティポリシーは重要な経営方針であることから社外に公開してはならない。
○全従業員に理解、実践してもらうためには広報が重要である。経営者自らが先頭に立ち、本気でセキュリティに取組んでいる姿勢を示す必要がある。
○セキュリティポリシーを根付かせるためには、監査が重要である。ただし、監査は従業員から誤解を受けやすいため、信頼できる方法を示すと共に、会社側

の権利と従業員のプライバシの関係を明確にしておく必要がある。

○セキュリティポリシーは頻繁に更新されるべきものではない。しかし技術の進歩等によって新たな脅威が発生したり、組織変更などにより運用、監査体制の変更を余儀なくされる場合もあり、適切な時期に見直しを行う必要がある。

○セキュリティを強化することにより業務の利便性、効率性が損なわれてはいけない。このために、企業は情報インフラおよび情報セキュリティインフラを整備し、情報の自由な流通が行われるような環境を構築する必要がある。

第４章　セキュリティ対策策定手順

４．１　手順の概略

セキュリティ対策はどこまで実施した方が良いのか、またその効果算定も難しい。このためセキュリティ対策は非常に重要だと分かっても、なかなか実際の対策に結びついていないといわれている。

ＩＳＯで作成されたガイドライン「Guidelines for Management of Information Technology Security(1996-1997)」において、次の２つのバランスが強調されている。

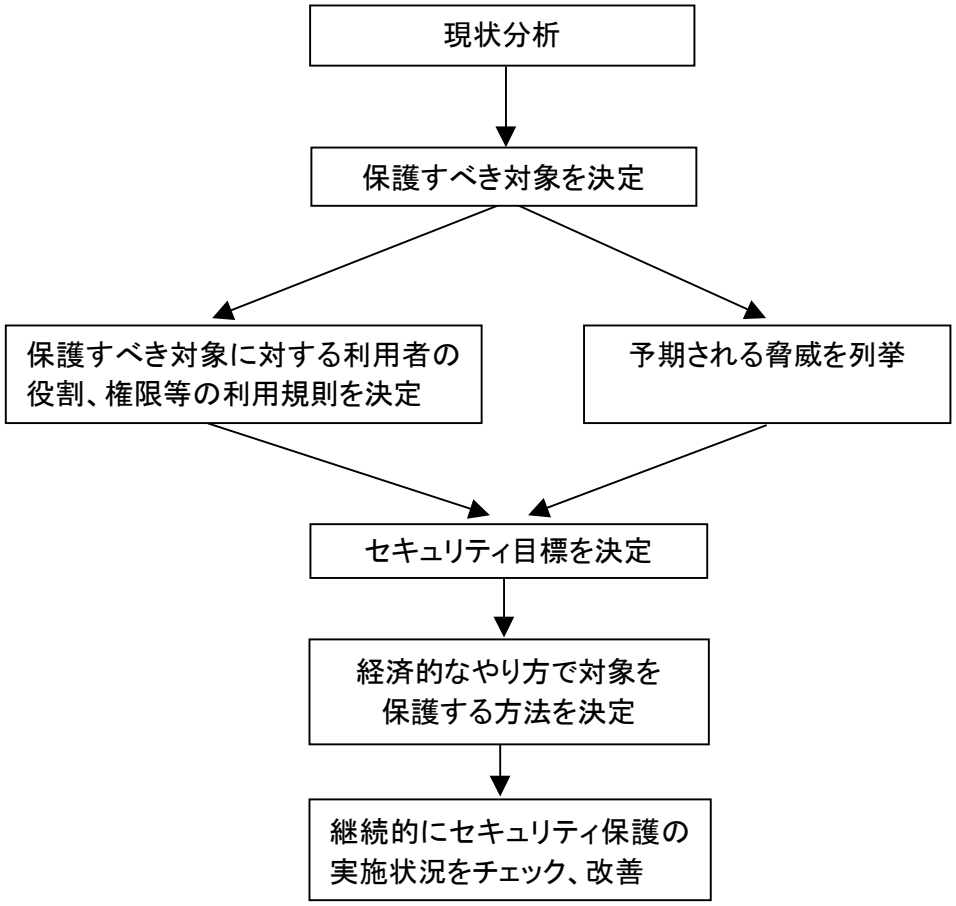
１．セキュリティ対策とリスクとのバランス
２．セキュリティ対策と運用・管理の手間とのバランス

またＩＳＯが 1999 年 6 月 8 日に国際標準 ISO/IEC15408 として制定した「セキュリティ評価基準」の Part１「概論とモデル」においてセキュリティ対策の基本的考え方とその実現方法が記述されている。【9】

これらを参考に考えられる基本的な手順は以下の通り。

（１）情報セキュリティに対する現状分析を実施する
（２）保護すべき対象（情報、もの、人）を決定する
（３）保護すべき対象に対する利用者の役割、権限等利用規則を決定する
（４）予期される脅威を列挙する
（５）セキュリティ目標を決定する
（６）経済的なやり方で対象を保護する方法を決定する（費用対効果）
（７）継続的にセキュリティ保護の実施状況をチェックし、改善する
（**P**lan-**D**o-**C**heck-**A**ction）

図表４－１　セキュリティ対策策定の基本的な手順



４．２　手順の詳細

（1）情報セキュリティに対する現状分析を実施する

対象分野におけるセキュリティ対策の実情を調査

・業務の特性上保護すべきものは何か、その候補

・予期すべき脅威に対する保護が現在どのように実施されているか

・今までにセキュリティを破られた事実があるか

等

（2）保護すべき対象（情報、もの、人）を決定する

＜情報システム関連＞

①ハードウェア

・コンピュータ本体
・周辺機器
・ネットワーク接続機器
・通信回線
等

②ソフトウェア

・ＯＳ（付属プログラムを含む）
・通信プログラム
・ＤＢＭＳ、開発ツールなど基本的ミドルウェア
・アプリケーションプログラム
等

③データ

・テストデータ
・本番データ（オンラインで新規に生成されたものを含む）
・データ原票
・監査ログ
等

④文書

・ハードウェア文書
・ソフトウェア文書
・システム全体の文書（運用手続きを含む）
等

＜その他＞

①知的財産権該当文書

・特許権文書
・意匠権文書
・商標権文書
・サービスマーク文書
・無体財産権文書（字体、データベース配列など）
等

②商業上の機密（トレードシークレット）

・顧客情報
・自社の人事情報（個人情報を含む）
・代理店情報
・営業戦略
等

③人員

・管理者
・保守担当者
・ユーザ
等

（3）保護すべき対象に対する利用者の役割、権限等利用規則を決定する

・保護すべき対象に対して利用者が従うべき役割と責任範囲
・導入、更新、運用、保守の方法と責任の所在
・組織内部の規則

（4）予期される脅威を列挙する

・資源情報への不正アクセスによるデータの改竄等サービス妨害
・資源情報への意図しない、不正な情報の公開

（5）セキュリティ方針を決定する

・サービスの提供　対　セキュリティ
・操作性　対　セキュリティ
・セキュリティのコスト　対　セキュリティ

これらの観点からセキュリティ対策上の方針を決定する。

（6）経済的なやり方で対象を保護する方法を決定する

セキュリティに要するコストの側面として以下のものがある。

・金銭面（セキュリティ対策のためにハードとソフトを購入する費用）
・性能面（暗号化複合化は性能を劣化させる）

・操作性（安全性を高めるには操作性を犠牲にする）

リスク算定は各レベルの損失に対する復旧の費用から見積もる

・データの喪失

・サービスが不能になる状態（計算機資源の枯渇、ネットワークアクセス不能等）

・プライバシーの侵害（承認されていないものが情報を取得、他人に漏洩等）

（７）継続的にセキュリティ保護の実施状況をチェックし、改善する

・対外的な環境や社内の状況変化に対応すべく、定期的計画的にセキュリティ保護の実施状況をチェックする必要がある。

・ＩＰＡ（情報処理振興事業協会）やＪＰＣＥＲＴ／ＣＣ（コンピュータ緊急対応センター）のホームページ等より継続的にセキュリティ情報を入手する。

・監査を定期的に行い、実施の徹底化及びセキュリティ方針と、実施施策そのものの見直しを行う。

第５章　情報システムのセキュリティ対策

５．１　ネットワークセキュリティ対策

ネットワークシステムに求められる本質的な機能は、必要な情報を安全かつ円滑に交換することである。

これを妨げる脅威として、通信データの「盗聴」、「暴露」、「改ざん／破壊」等があげられるが、ネットワークセキュリティ対策とは、これらの脅威に対する予防策や対処策を講じることに他ならない。

本章では、これらの脅威とその対応策についてのべる。

（1）インターネット

インターネットへ接続することによってもたらされる有用なリソースやデータへのアクセスの可能性は、その規模の点で絶大である。その反面、アクセスが容易であるために、潜在的脅威も存在する。インターネットを通じての外部からの攻撃等の脅威に対応するためにはファイアウォールを使用し、インターネットから自分の組織内部のネットワークへのアクセスを制限することが重要である。

また、インターネットを通じてやり取りされる電子メールやファイルを保護するためには、暗号化ソフトや VPN を利用すること。

ファイアウォールの外側に公開 Web サーバを設置する場合は、外部からアクセスする必要のあるデータのみをそのサーバ上に置き、重要な機密データ等はファイアウォールの内側の保護されたイントラネットや、インターネットから物理的に切り離された安全なネットワーク上に置くこと。

（2）イントラネット

イントラネットを構築しインターネットへ接続する際、ファイアウォールを設置して組織内のネットワークを保護する。

（3）エクストラネット

複数の組織毎に独立して構築されたイントラネットを相互接続する際、

・各々のセキュリティポリシーの違い
・ネットワーク保護の必要性の有無
等を考慮し、ファイアウォールやＶＰＮ等を構築する。

（4）ファイアウォール

（ａ）フィルタリングルータ

フィルタリングルータを使用してファイアウォールを構築する際は、パケットの流れる方向、発信元と宛先の IP アドレス等を基に、出入りするパケットをフィルタリングする。外部から流入するパケットをフィルタリングしない場合、そこから侵入される恐れがある。逆に、外部との唯一の接点であるフィルタリングルータのセキュリティを強固にすることで、対外的な脅威からネットワークシステムを保護することが容易になる。

（ｂ）プロキシサーバ

ユーザに対して提供する様々な機能を限定するためにはプロキシサーバを使用する。フィルタリングルータはパケットの出入りを制御するだけで、許可されたパケットがどのようなサービスを実行するかは把握できないが、プロキシサーバを使用すれば、例えばファイルへのアクセスを読み出しのみに限定できる。

（ｃ）分散サーバ（負荷／リスク分散）

保護すべきネットワークの規模や出入りする通信データ量、また保護すべきデータの重要性や機密性に応じて、ファイアウォールを構築するサーバを冗長化する。

（5）暗号化

ネットワーク上の全ての通信データを保護しなければならない場合と、特定のデータ(ファイル、ハードディスク等)だけを保護するのみで良い場合がある。

（ａ）通信データの暗号化(VPN)

ルータ間や、ルータとクライアント間等の通信を暗号化し、ネットワーク上を通過するデータを保護する。

（b）データファイルの暗号化

保護するべきデータが限定されている場合には、その限定されたデータ（ファイル、ハードディスク等）のみを暗号化する。

VPN を構築するよりも、一般的にコストが押さえられることが特徴。

（c）暗号化の実装レベル

暗号化を施す階層（実装レベル）は、概ね以下のように分類できる。

①アプリケーションレベル:

PGP、S/MIME、SHTTP、SSL、またはその他汎用の暗号化エンジンを利用して、アプリケーション毎に暗号化を行う。

②ネットワークレベル:

IP パケットレベルで暗号化を行う。IP パケットによる全ての通信が暗号化の対象となる。ファイアウォールに暗号化機能を持たせる場合もある。

③リンクレベル:

専用のルータ等のリンクレベルで暗号化を行う。

（6）リモートアクセス

（a）公衆網上の脅威

公衆網を利用してデータのやり取りを行う場合、そのデータは大きな脅威にさらされていると考えて良い。公衆網には不特定多数のユーザがアクセス可能で、データの盗聴や改竄等の危険性が極めて高いと言える。

（b）対策

コールバック、リモート VPN、暗号メール等を利用する。モデムを設置する際、モデムの使用中にそのモデムの設定を変更する機能や、通話後も変更した設定が継承されるような機能は、外部からの攻撃の糸口となりやすいので、これらの機能は利用できないように設定しておく。

５．２　アクセス制御

５．２．１　システムにアクセスする際の認証

（1）パスワード

パスワードは一般的で手軽な認証手段である。以下、パスワード認証の安全性を高めるための主なポイントを述べる。なお、実施方法など詳細については、各種システム管理マニュアルを参照のうえ作成する。

（ａ）ユーザ

・パスワードを紙（付箋）やファイルなど、見える形に残さない。

・推測が難しいパスワードをつける。

・パスワードエイジング（定期的変更）を実施する。

（ｂ）システム管理

・全アカウントがパスワードを持っていることを確認する。

・システムのデフォルトアカウントのパスワードは全て変更する。

（2）ワンタイムパスワード

ワンタイムパスワードは、ユーザが暗号発生器を持ち、その暗号を使って認証を行うものである。（チャレンジアンドレスポンス方式と時間同期方式とがある。）

認証する都度、パスワードを変更（一回限り）するため、盗聴されても再利用されないため、安全強度は高い。

（3）スマートカード（IC カード）

認証をさらに強化する方法として、磁気ストライプカードやスマートカード等のメディアの利用がある。そのメディアを持つ人だけ利用可となるため、アカウントとパスワードだけの認証よりセキュリティは高い。パスワードと併用すればさらに安全性は高まる。

スマートカードは、高価だがメリットも多く、今後高度な利用法が期待できる。

（4）バイオメトリクス（生体認証）

人間の身体的・行動的・形態的な特徴を利用した認証方法がバイオメト

リクス（生体識別システム）である。実用化されている主なバイオメトリクスを以下に示す。

・網膜パターンシステム
・指紋システム
・手形システム
・声紋システム
・キーストロークパターンシステム
・署名システム
　など

（5）その他

アプリケーション毎の認証手法もいくつか存在する。必要に応じて利用を検討のこと。

・Web 関連：SSL（Secure Sockets Layer）、https 等
・電子メール関連：ssmtp、spop3、apop 等

5．2．2　メッセージ認証

（1）デジタル署名

デジタル署名は、電子メッセージの発信者確認とそのメッセージが改ざんされていないことを確認する機能により、メッセージの送受信にまつわる認証の問題を解決するものである。実現方法には、以下のものがある。

・特定のアプリケーション／機器で実現しているもの
・一般的な共通鍵暗号／公開鍵暗号によるもの

前者は、特定アプリケーション／機器の利用という閉じた世界であるため、実現は容易でセキュリティも高いが、範囲が限られる。

後者は、広い範囲で利用できるが、利用する暗号の種類と、暗号鍵の管理方法についてはこれから整備が進められていくものである。（後述の認証局など）

（2）認証局

認証を行う場合、あらかじめ相手を証明するためのデータ（電子証明書）が必要であり、この証明書の発行及び更新を行うのが、認証局である。

認証局として、ＴＴＰ（第三者の信頼できる組織）を採用するか、独自で運用するかについては下記の項目を踏まえ、ニーズに合うものを選択すること。

品質：どの程度の安全性が必要か、TTP はその安全性を維持するレベルか
　　認証を必要とする相手は少数か／多数か、関係の深い相手か
費用：TTP のコストはどのくらいか、独自運用時のコストはどのくらいか
納期：登録変更の頻度はどの程度か、その際 TTP の対応は充分なレベルか
技術：独自運用をするための技術力・要員は確保できるか

（3）ＰＫＩ (Public Key Infrastructure)

公開鍵インフラストラクチャ（ＰＫＩ）とは、暗号化・認証をより一般的で広くの分野で共通に利用できるようにするための取組である。欧米を中心に標準化／法制化が進められているが、日本はまだ立ち後れているのが実状である。政府機関、金融システム、電子商取引等個々に進められており、下記の課題がある。

・証明書廃棄リストのサポート（解決策がまだない）
・インターオペラビリティ（異なるＰＫＩ間の相互認証を期待）
・モビリティ（移動環境下での認証）
・個人の本人認証情報

５．２．３　リソースのアクセス制御

（1）ファイアウォール

ファイアウォールは、外部（インターネット等）と内部（社内ネットワーク）とのアクセスを制御するためのゲートウェイシステムである。外部との接続をファイアウォール一箇所に限定することで、外部からの脅威に対する防御（内部への不正アクセスの禁止、電子メールの不正中継の禁止、ウイルスブロックなど）を一箇所で行うことを目的としている。

（ａ）ファイアウォールのポリシー

ファイアウォール構築に関するポリシーには代表的な下記の二つの考え方がある。いずれにせよ、会社としてのポリシーを明確にすることが必要である。

・Allow　all（全面許容）：明確に禁じていないものは許されている

・Deny　All（全面拒否）：明確に許していないものは禁じている

（ｂ）ファイウォールの種類

ファイアウォール製品は、次の２種類に大別される。ニーズに応じて決定すること。

・パケット・フィルタ型：パケットを、ポート番号とその方向で制御

・アプリケーション・プロキシ型：OSI モデルの APL 層で制御

（ｃ）ファイアウォールの設置台数

ファイアウォールの設置台数は、必要性と安全性のバランスを考慮して決定すること。

・会社で１台：コントロールは一括して実施できるが、負荷は集中する

・事業所毎に１台：負荷は分散されるが、管理機器台数が増える

（2）プロキシサーバ

内部からインターネットを利用する場合、ユーザはインターネット接続のためのプロキシ（代理）サーバを内部に設置して利用するのが一般的である。特徴を以下に示す。

・インターネットから入手した Web データをキャッシュできる。そのため、ユーザレスポンスの高速化、並びにインターネット用回線も圧迫しない。
・不適切な Web サイトへのアクセスに対して制限が可能。
・内部に対するセキュリティ管理が容易になる。
・プロキシサーバを複数拠点に設置して、内部ネットワークの負荷分散が可能。

（3）ファイルアクセス権限

ファイルに対するアクセス権限の設定は重要である。以下、基本的な考え方を示す。詳細は、個々のシステムのマニュアル等を参照のこと。

・一般ユーザには、そのユーザが作成したものだけが変更可能なことを原則とする。他のファイルはアクセス不可か参照のみ（変更できない）。
・管理者権限とするファイルは、管理者しか変更できないことを原則とする。できれば、一般ユーザは参照できないことが望ましい。
・管理者権限は特定担当者にしか与えないものとする。（誰もが管理者権限を使えるのは望ましくない。）

（4）IPsec

IPSec は、暗号化通信の標準プロトコルであり、今後異機種間でも暗号化通信が可能になってくる。ただ、製品群が充実してくるのはこれからである。

従って、用途が限定する場合や特に今後の拡張性を必要としない場合には、従来の独自プロトコルによる機種を選択するのも一つの方法である。

５．３　コンピュータウイルス対策

５．３．１　概要

コンピュータウイルスとはその名の示す通り、コンピュータに感染して様々な悪い症状を引き起こすものである。初期のウイルスは単純なものであったが、新種発生の都度ウイルスの構造が複雑化し、現在では多種多様なコンピュータウイルスが発生し社会問題化するに至っている。

本ガイドラインでは、企業におけるウイルス対策という観点でコンピュータウイルス対策について、なるべく具体例を織り交ぜて説明する。

５．３．２　コンピュータウイルスの特徴

コンピュータウイルスは、感染、潜伏、増殖、伝染、発病といった自然のウイルスと変わらないライフサイクルを持つ悪意を持って作られたプログラムである。

・感染：ウイルスが正常なプログラムに付着したり、ウイルスを含んだプログラムやデータがコンピュータに侵入することを指す。
・潜伏：ウイルスがコンピュータ内にあって、まだ発病していない状態を言う。
・増殖：ウイルスが自己の複製を作成しウイルスを増やすことを言う。
・伝染：ウイルスが他コンピュータに侵入し、ウイルスを広げることを言う。
・発病：ウイルスが活動を開始し、正常なコンピュータ機能を阻害しはじめることを言う。

ウイルスの影響は、発病しないと症状がなかなか表に現れないため、発病時にはすでに増殖、伝染している場合がある。

（1）感染経路について

ウイルスの感染経路は、大きく分けて次の３つに大別される。

・ＦＤ感染：どこかで入手した（購入した）ＦＤにウイルスが付着しそこからコンピュータに感染するケースや、別のウイルスに感染したコンピュータでＦＤを使用しそこからＦＤにウイルスが付着して感染するケースなどがある。
・メール感染：第３者からの添付ファイルにウイルスが付着しそこから感染するケースや、メーラーが自動展開するデータに付着し感染するケースなどがある。1999 年以降､伝染の手段として自分で自分を添付したメールを発信するウイルスが増大した。この活動は上記ライフサイクルの「伝染」に当たるが、種によってはメーラーのアドレス帳を参照して膨大な宛先に大量のメールを発信してメールシステムの運用を妨害するため発病症状以上に問題となることも多い。また、伝染はウイルスの存在を知らない善意の第三者が過失で媒介してしまうことが殆どだが､2000 年前後はメールの発信者をプロバイダやソフトベンダのサポートと偽装してバグフィクスパッチと偽ってウイルスファイルを送りつけるという悪質な例も目立っている。
・ネットワーク感染：ダウンロードデータにウイルスが付着しているケース、ＵＲＬでＪＡＶＡ等のプログラムにウイルスが付着しており自動ダウンロードされるケースなどがある。

多くのケースは、適切なウイルスチェックと十分な注意があれば防げるものである。

（2）発病の形態

ウイルスによって、その症状はさまざまである。ここでは、代表的なウイルスの形態をいくつか紹介する。

・ブートセクタ感染型：ＦＤやＨＤ等の媒体のシステム領域に感染するウイルス。ウイルスは、他のＯＳより先にメモリに常駐し、パソコンの制御を奪う。
・ファイル感染型：実行モジュール（ＥＸＥ、ＣＯＭなどのファイル）に感染しするウイルス。ファイルが実行される度にウイルスも実行する。

・複合感染型：ファイル感染型とブートセクタ感染型の両方の特徴を併せ持つウイルスのこと。システム領域に感染したウイルスが次に実行するプログラムに感染しウイルスが広がる。
・メモリ常駐型：ウイルスがメモリ上の常駐するタイプのウイルス。一度活動を開始すると、コンピュータの電源を切るまでウイルスはメモリに常駐し、感染可能なファイルなどに次々に感染を広める。
・ステルス型：ファイルサイズや内容の変更を外部に出さない巧妙なウイルス。単純なウイルス検索プログラムでは、発見が困難なため知らぬ間に感染が広がる危険性がある。
・ポリモルフィック型：感染する度に、異なった方法でウイルスのプログラムコードを暗号化し、自分の姿を変異させるウイルス。変異すると、ウイルスコードの特徴を検索するウイルス検索プログラムでも発見が困難な厄介なウイルスである。
・マクロ感染型：従来のウイルスがプログラムファイルに感染するのに対し、マクロ感染型ウイルスはデータファイルに感染する。マクロウイルスが感染するのは、マクロ機能があるデータファイルに限られるが、Microsoft Excel / Word といった世界的に普及した使用頻度が非常に高いアプリケーションのデータに感染するため、従来のウイルスに比べ感染する危険性が高くなっている。また、マクロウイルスは、ウイルスのソースコードを簡単に見ることができるため、マクロプログラムの知識がある人ならウイルスコードを流用／悪用し簡単に別のウイルスを作成することができる。このため、マクロウイルスは従来のウイルスに比べ非常に多くの新種ウイルスが日々発生している。

それぞれ発病すると多大な被害が発生する可能性があるが、ウイルスは発病させない限り被害は発生しない。仮にウイルスに感染したとしても、発病／伝染させないことが重要である。

５．３．３　ワクチンソフト

コンピュータウイルスに対する直接的な対処方法として最も有効な方法としては、ワクチンソフトの有効利用があげられる。今や 50,000 種を超えるコンピュータウイルスが出回っている状況であり、ウイルスの検知にワクチンソフトは欠かせないものとなっている。ワクチンソフトの機能としては、次のものがあげられる。

・ウイルスの検索： データ、ファイルを検索し、ウイルスの感染をチェックすること。コンピュータにファイルをＦＤなどからコピーする前にこの検査を行うと、コンピュータへのウイルス侵入を未然に防ぐことができる。多くのワクチンソフトは、膨大な数のウイルスのデータベースを持ち、検査対象のファイルとデータベースを照合することでウイルス検索を行う。ただ、データベースにない新種のウイルスを検知できないため、最新のウイルス情報を記録したパターンファイルを常に用意する必要がある。
・ウイルスの監視： ファイルへのアクセスを監視し、ウイルスの侵入を防ぐ機能。ファイルのコピーなどを行おうとした場合、もしコピー対象のファイルにウイルスが付着していた場合、コピーを停止しウイルスの侵入を防ぐことができる。
・ウイルスの駆除： ウイルスに感染したファイル、メモリからウイルスを取り除く機能のこと。ファイルに対してウイルスがデータとして追加されているようなケースでは有効だが、ウイルスがファイルデータに上書きされている場合は元ファイルの復元は事実上不可能である。ワクチンソフトも万能ではないので、日頃のこまめなバックアップを励行することが重要である。
・ワクチンソフトの選択：クライアントＰＣ用ワクチンソフトの他に、サーバー用ワクチンソフト、グループウェア用ワクチンソフト等、用途に合わせた製品が販売されている。使い勝手、コスト、サービス等を考慮し、最適のものを選択し購入／運用するのが望ましい。

５．３．４　企業としてのウイルス対策

通産省のコンピュータウイルス対策基準（通商産業省告示第４２９号）では、以下の基準が定められている。

① システムユーザ基準

② システム管理者基準
③ ソフトウェア供給者基準
④ ネットワーク事業者基準
⑤ システムサービス事業者基準

本稿では、この中で特にシステムユーザ基準及びシステム管理者基準について述べる。

ユーザに対しては、運用ルールの徹底と事後対応及びコンピュータウイルスに対する教育、啓蒙活動を行っていく必要がある。

ウイルス対策とは、時間とデータの損失を招くウイルスの感染リスクを最小限にするために講じる必要がある。以下に対策事例を述べる。

（1）ウイルス対策

① ウイルス対策のガイドラインの設定

・ウイルス対策のガイドラインとは、ウイルスに感染させないように、あらゆる可能な予防策を立てる事である。
・ウイルスの侵入を防ぐ為の予防策、ウイルスが発生した際の対応・体制を定める。

② システムへのウイルス対策ツールの導入

・ウイルス対策を行うには、組織としてツールを備えておく必要がある。
・ツールの選択、導入に関しては組織内のＬＡＮ、ＷＡＮの運用を把握しているシステム管理部門が適任である。
・担当者は、組織内で利用されるアンチウイルス製品を標準ソフトとして指定する。
指定した標準アンチウイルスソフトは「すべてのクライアント」、「すべてのサーバ」にインストールしておく。
・インターネット通信のゲートウェイ用(SMTP、http、ftp)やグループウェア用のワクチンを検討する
・ウイルスは、月に数百という単位で増加し続けている。このため最新のウイルス検出用パターンファイルを入手し、定期的にバージョンアップ

する必要がある。

③ 具体的なウイルス予防策の実施

ウイルス予防策は、組織のユーザのすべてが実施しなければ効力がない。以下に予防策の例をのべる。

・コンピュータにインストールするすべてのファイルは、アンチウイルスソフトを使用し、ウイルスチェックを行う。
・シェアウェア、フリーウェアはウイルスチェック後、使用する。
・メールの添付ファイルは、発信者が誰であってもウイルスチェック無しでオープンはしない
・ＦＤ等メディアの授受の際はウイルスチェックを行う。
・OS のファイル操作に割込んで使用ファイルを自動的にウイルスチェックするタイプのアンチウイルスソフトをインストールする。

また、通産省やＩＰＡ（情報処理振興事業協会）から提示されているコンピュータウイルスに関する対策基準をもとに予防策を策定する。【16】

５．３．５　運用

（1）ウイルス発生時の対応・体制の確立

ウイルス発生時の対応は迅速に行う必要がある。万が一組織内でウイルスが発見された場合は、被害の拡大を防ぐために短時間で駆除を行なわなければならない。

そのためウイルスが発生した場合、ユーザにはあらかじめ定められたルートで情報を管理者へ伝え、管理者は適切な判断と対応を行うことができるよう体制を整える必要がある。

以下に、対応例を述べる。

①ウイルス発生時の対応

・状況の把握（ウイルスかどうかを確認する）
　機種、ＯＳ、発生時期等を確認する
・感染コンピュータの確認と隔離（ウイルスの感染を防ぐ）
　ネットワークからの隔離を行う

・ウイルスの駆除を行なう
　アンチウイルスソフトを使用してのウイルス駆除を行う
・コンピュータの復旧
　被害状況を確認し、データの損失がある場合にはデータの復元を行う

②ウイルス発生時の緊急体制

　ウイルス発生時には、迅速に必要な情報が管理者のもとに届けられ、迅速な対処がされることが重要である。以下はその例である。

情報の流れ：ウイルス発生ユーザ → 部門管理者 → システム管理部門担当者
対処の流れ：システム管理部門担当者 → ウイルス発生ユーザ
警告の流れ：システム管理部門担当者 → 各部門管理者 →全ユーザ

（2）ユーザへの教育

　ユーザへの教育はウイルス対策を推進する上で有効な手段である。ユーザ自身がコンピュータウイルスに対する知識を持つ事により、ウイルス対策を効果的に進めることが出来る。エンドユーザに対する教育は以下の項目が考えられる。

・ウイルスの基礎知識
・アンチウイルス製品の操作方法
・ウイルス発生時の対処方法
・具体的なウイルス予防策

第６章　セキュリティ対策の運用

６．１ セキュリティ監査　　【17】

（1）目的

セキュリティ監査とは、監査対象から独立かつ客観的立場のセキュリティ監査人が、情報セキュリティの観点から情報システムを総合的に点検及び評価し、組織体の長に助言及び勧告するとともにフォローアップする一連の活動である。「セキュリティ管理基準」に従い、企画、開発、運用、エンドユーザなどが遵守すべきことについて実施対策状況や費用対効果を検討する。また信頼性と安全性に関する現状の点検・評価を行い、利用者向けのセキュリティに関する教育実施状況を点検・評価するとともに関係者にセキュリティ管理基準の改善見直し、助言・勧告を行う。

（2）本質

①独立かつ専門的な立場からする保証であり、批判性という役割を監査に期待する考え方…外部監査（公共性が高い又は人命にかかわるような情報システム向け）

②情報システムに特定の保証を与えるというよりも、むしろ情報システムの安定的な運用にとって障害となっている欠陥や問題点を抽出し、それを解決するための適切な助言・勧告およびそのフォローアップに重点を置く、指導性という役割を監査に期待する考え方…内部監査

（3）監査対象

①システム企画

計画、調査、分析、開発検討、要員管理、外部委託管理、運営費用、資産管理や施設などの管理の実施状況、開発実施後の運用状況や利用状況、合理化状況や予定されていた効果が実績としてあげられているかなどの評価の実施状況、改善や勧告に対する実施状況。

②システム開発

システム開発手順、外部設計、内部設計、プログラム設計、プログラミング、テストなどの管理、要員管理、外部委託管理の実施状況、改善や勧告に対する実施状況。

③システム運用

オペレーション、データ管理、プログラム管理、機器管理、ファシリティ管理、出力情報管理、要員管理、外部委託管理、入退室管理、各種報告の実施状況、改善や勧告に対する実施状況。

④システム利用者

入力データ管理、出力情報管理、端末管理、要員管理、外部委託管理、各種報告の実施状況。

（4）監査（内部不正）の着目点

〇不正を働こうとする人が情報への正当なアクセス権をもっている。

〇高いアクセス権限を有するシステム管理者を監視する体制が確立されているか。

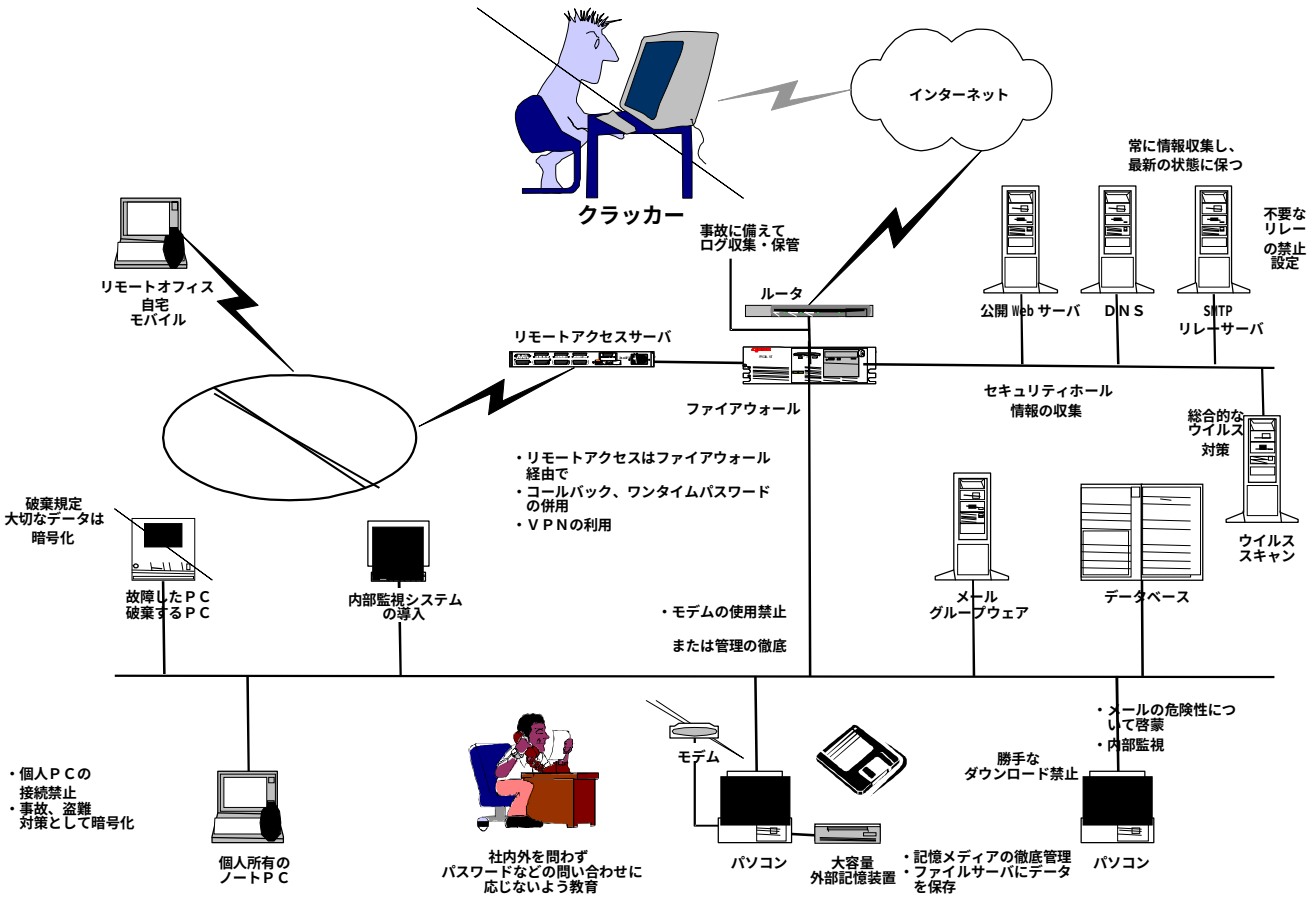
〇企業情報システムに内在する脆弱性の大半は、人間に起因していると指摘されている。防止技術よりもむしろ内部社員やパートナー企業の社員まで含めた“人”の管理が重要。

６．２　セキュリティ侵害の検知とその対応方法

６．２．１　セキュリティ侵害の形態

ネットワーク化されたインフラストラクチャーにおいて、セキュリティ侵害が以下のような形態で発生する事が経験的に知られている。（図表６－１「ネットワークからのセキュリティ侵害」を参照）

図表６－１　ネットワークからのセキュリテイ侵害



① インターネットを通じてのアタック
(1) ポートスキャン
(2) 成りすまし。「踏み台」に悪用される（ＳＰＡＭメール）
(3) 公開サーバのコンテンツ改ざん
(4) 内部への侵入
② リモート･アクセス･サーバからの侵入
③ 外部記憶媒体（フロッピィー･ディスク等）の流出
④ 内部不正アクセス（端末機の不正使用や権限外アクセスなど）
⑤ 電子メールなどによる情報漏洩
⑥ コンピュータ･ウイルス、悪意のあるプログラムの侵入

セキュリティ対策は、外部からのセキュリティ侵害（①、②、③、⑥）に対し講じるとともに内部からのセキュリティ侵害（③、④、⑤）に対しても考慮が必要である。

６．２．２　セキュリティ侵害の検知

セキュリティ侵害に対しては、既知のアタック手法をシミュレーションするツールによる診断などで侵害そのものを防止することが大切であるが、常に完全に防御できるわけではない。このため被害を最小限に食い止めるためには、予兆段階で検知することが重要である。

検知の方法としては、

・システム・ログの確認
・平常の利用状況を把握し、しきい値を超えた異常なトラフィック、異常な時間帯の利用などを検知する
・データの改ざんの有無を照合により検知する

などが考えられる。

６．２．３　セキュリティ侵害の対策

侵害を検知した場合には、

① 被害状況の把握
② 被害拡大の防止
③ 復旧作業
④ 再発防止対策

を速やかに行う必要がある。

このためには、

① 責任者
② 対策の体制、連絡ルート
③ 対策手順
④ 関連機関（IPA や JPCERT など）への報告基準　【21,22】

などを明確にした「対応計画」を準備しておくことが重要である。

特に被害・影響の大きさによっては、ネットワーク接続の遮断などが必要になることも考えられるが、この場合のサービス停止による影響などについて十分な検討を事前に行っておくことが必要である。

６．３　教育 【18】

６．３．１　教育の必要性

セキュリティ管理の重要性を情報処理システムの作成者、運用者、使用者が認識し実行して初めて効果がでるものである。特に、内部の人間による故意の不正使用などの極めて防御しにくい脅威に対しては、教育による行動の牽制が最も重要となる。このために教育体制を確立し、実行計画を立てることが大切である。（全体教育、部門教育、啓蒙活動等）

６．３．２　具体的教育内容

（1）セキュリティ対策の教育

システムの企画、開発、運用の各段階でセキュリティ対策は異なるため、各々の担当者へ各段階毎に対策内容の教育及びセキュリティ技術の一般向け基礎教育を行い、システムの構築や変更時に有効な対策が行えるようにする。また、セキュリティ対策の研究により新たに有効な対策が導入される際も、教育を忘れずに実施する必要がある。

（2）内部要員への牽制教育

新入社員教育、中堅社員教育などのカリキュラムへセキュリティ対策の重要性を含めるとともに、日常業務で繰り返し訓練し、朝礼や打ち合わせなどで絶えず喚起を促すことが大事である。

（3）点検の教育

システムドキュメントなどの整理整頓、貸出資料の返却状況の確認を行うことで資料の不正持ち出しを牽制し、また巡回点検で日頃見慣れない不審物の発見と通報を励行し、危険防止を行うなどの教育も大切である。

６．３．３　教育カリキュラムの例

○企業独自に作成したセキュリティガイドライン及び、管理規定等の解説

企業が設けたセキュリティルールを理解していなかったり、ルールを知りながら守ろうとしない社員がいる。ルールを守らない社員は、本人に悪いことをしているという意識がないが、これは内部ハッカーと同様に大きな脅威になりえる。結果的にシステムを止めたり、システムに弱点を作ってしまうことにつながる。

○コンピュータを取り巻く危険
　システム停止、コンピュータエラー、コンピュータ犯罪、脅威の事例（ユーザ及びシステムが被害を受ける事例）
○コンピュータセキュリティとは
○最近の話題
　不正アクセス、コンピュータウイルス、プライバシー侵害、電子メール爆弾
○セキュリティ対策
　物理的保護対策、管理的保護対策、技術的保護対策
○罪悪意識調査（不正か否か）

６．４　契約

６．４．１　機密保持契約

　情報サービス産業においては、自社業務の一部を協力会社へ委託したり派遣社員へ委託するケースが多い。このような場合、協力会社社員や派遣社員が会社の重要な情報に接する機会を持つことになる。各企業の業務を円滑に行うためにも、協力会社社員等との信頼関係を築くことは重要であると共に、情報資産が適切に取扱われるように留意しなければならない。

　このために、協力会社社員等が企業の重要な情報に接する機会が想定される場合には、事前に機密保持義務を負わせる等の情報セキュリティに関連した事項を含む契約を締結するなどの措置をとる必要がある。機密保持契約を締結する際には、業務上必要な情報資産へのアクセスのみを許可する内容とすると共に、そこに定めた以外の情報資産へ接することがないように、所要の措置をとることも重要である。

６．４．２　誓約書

　社員、協力会社社員等を問わず、各企業の業務を支える全ての人が情報セキュリティを守ることを保証するために、場合によっては誓約書や念書の提出を求めても良い。特に、財務会計処理、企業戦略立案、研究開発等の企業にとって極めて重要な情報に接する機会が特に多い社員等については機密保持義務等を具体的に定めた誓約書の提出を求めることも重要である。

参考資料および関連リンク（ＵＲＬは、2000 年７月時点）

【1】著作権法第 2 条 1 項第 10 の 2 号
【2】「コンピュータセキュリティの基礎」，Deborah Russell/G.T.Gangemi Sr 著，山口 英 監訳，(株)アスキー
【3】「セキュリティ マネジメント ハンドブック」, 日本セキュリティマネジメント学会編，日刊工業新聞社
【4】不正アクセス行為の禁止等に関する法律（案）
【5】「セキュリティ ハンドブック Ⅰ」, 日本セキュリティマネジメント学会編, 日科技連
【6】「金融機関等におけるセキュリティポリシー策定のための手引書」, (財)金融情報システムセンター　平成 11 年 1 月
【7】RFC2196　サイトセキュリティハンドブック(Request For Comments, IETF)
http://www.ipa.go.jp/SECURITY/index-j.html
【8】ＩＳＰＭＥ　(Information Security policies Made Easy)，CHARLES CRESSON WOOD
【9】Common Criteria v2.0
http://csrc.nist.gov/cc/
【10】ＢＳ７７９９，British Standard，1995
【11】ＧＭＩＴＳ　(Guidelines for the Management of IT Security, ISO/IEC TR 13335, 1996-1997)
【12】「セキュリティ七つの不安」, 日経コンピュータ, 日経ＢＰ社, 1998.11.23
【13】「セキュリティ評価基準」の詳細と対策（後編）　田淵治樹氏―日経コンピュータ，日経ＢＰ社，1999.1.4
【14】「ワイリー　コンピュータセキュリティハンドブック」，フジ・テクノシステム
【15】How to Secure Your Network (by Peter Morrissey)
http://www.networkcomputing.com/netdesign/security3.html

【16】「パソコン・ユーザーのためのウイルス対策７箇条」,
情報処理振興事業協会
【17】「セキュリティハンドブックⅡ」，日本セキュリティマネジメント学会編,
日科技連
【18】「システム運用管理エンジニアテキスト」,（財）日本情報処理開発協会
【19】「コンピュータウイルス　なぜ感染するのか　どう防ぐか」，渡辺 章,
日本実業出版社
【20】「情報システムのセキュリティ」，上園 忠弘，トッパン
【21】IPA セキュリティセンター
http://www.ipa.go.jp/SECURITY/index-j.html
【22】コンピュータ緊急対応センター　JPCERT/CC
http://www.jpcert.or.jp/
【23】「コンピュータセキュリティの基礎」，アスキー出版局
【24】「Unix_configuration_guidelines」
ftp://ftp.jpsert.or.jp/pub/cert/tech_tips/
【25】「AUSCERT_checklist1.1」
ftp://ftp.jpcsrt.or.jp/pub/cert/tec_tipcs/

情報資産活用のための情報セキュリティガイドライン

－　平成 12 年 7 月発行　－

発行所　社団法人　情報サービス産業協会

〒135-8073　東京都江東区青海 2-45　タイム 24 ビル 17 階

Telephone　03-5500-2610(代表)

Facsimile　03-5500-2630

Web Site　http://www.jisa.or.jp/