PART 2

e-Community
KASHIWARA

# セキュリティについて

情報基盤としてますます広がるネットワークに伴い、たいへん重要になり情報整備とともに取り組まなければならない課題がネットワークセキュリティです。
この部では自治体の情報化におけるセキュリティの重要性や今後の対策についてまとめました。

## 柏原市情報推進計画における情報セキュリティの基本方針

# 柏原市情報推進計画における情報セキュリティの基本方針

2000年11月に発表されたIT基本戦略では「すべての国民がITのメリットを享受できる社会」を目指すことが謳われ、2001年1月のe-Japan戦略では「5年以内に世界最先端のIT国家になること」が掲げられています。その中で地域住民に対して、行政サービスの直接の提供窓口となる地方自治体の役割は大きいと言えます。

情報公開は安全性が確保されてはじめて推進できるものであり、今後の住民サービスにもセキュリティが前提で成り立つものが多く存在します。これらのことを踏まえ、柏原市ではセキュリティ技術やセキュリティ標準を継続的に研究し、恒久的に業務の中に取り込める体制作りを目指します。情報セキュリティは一般的に技術的な議論に偏りがちですが、最近では、情報セキュリティ管理システム（ISMS：Information Security Management System）の標準化が進み、人的な要因も含めすべての事象を考慮した管理技術として捉える傾向にあります。本計画においても、情報セキュリティ管理システムの考え方を取り入れ、セキュリティを管理・運用規定として定着させる方向で検討していきます。

以下に情報セキュリティの取り組み方について記載しますが、前半の1章から3章までがセキュリティを検討する際に認知しておくべき情報を整理した内容になっており、後半の4章から7章が、本題である情報セキュリティへの取り組み方を説明する内容となっています。

## 第1章　インフラが持つ脆弱性と被害の実態

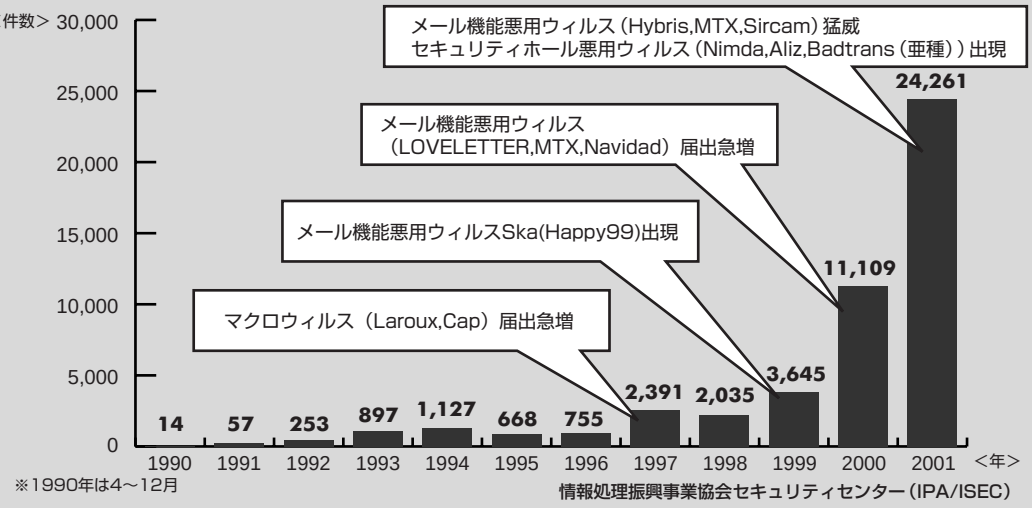
先にも述べましたがIT化を進める上で避けて通れないのがセキュリティの問題です。ネットワークを前提としたITの世界では従来のフィジカルな世界では予想されなかった様々な問題が発生しています。紙で保存された情報は持ち出された場合、物理的に消えるため気が付きやすいのですが、デジタルデータはコピーされ持ち出されてもほとんどの場合気がつきません。最近のPC端末は数十ギガバイトもの大容量のハードディスクが実装されています。これは一昔前のホストコンピュータの容量に匹敵し、ホストの情報が1台のノートPCにコピーできることになります。紙で数百ページのデータもデジタルデータにすると数メガバイトになるため、一度被害を受けた場合の影響は昔と比べものにならないほど大きくなります。またネットワーク上では顔が見えない相手と取引する場合、身元の保証や、経路途中の盗聴の問題も考えなくてはなりません。なによりインターネットで使用されているネットワークプロトコルにはもともとセキュリティがあまり考慮されていないことや、OS・アプリケーションなどソフトウェアには必ずといってよいほどバグ（欠陥といって良い）が存在し、インフラの基本部分に脆弱性が組み込まれたまま利用が広がっていることが問題です。

これは、IT関連技術が未だ発展途上なためであり、セキュリティについては利用者が自らの努力で補強することが求められます。特にコンピュータウィルス（以下ウィルス）は猛威を振るい、年々被害を拡大しています。

## 1-1.被害の実態

図１は情報処理振興事業協会（IPA）が公開している、ウィルスの届出件数の推移を表すグラフです。届出は毎年約２倍の伸び率となっています。ただし、実被害は20%と報告されており、大半の利用者が何らかの対策を事前に講じていて、ウィルスを受け取っても防御できているということが判ります。しかし、裏を返すと20%が十分な対策を講じていないということであり、ネットワーク社会ではどこか一箇所でも弱いところがあると、そこから被害が爆発的に波及します。ネットワーク社会においてはすべての者が責任をもって対策を講じることが望まれます。

図1 **ウィルスの届出件数の年別推移**




## 1-2.被害額の算定

ところで、セキュリティを検討する際に常にぶつかる壁が費用の問題です。セキュリティは効率を上げるための手段では無く、なにも起こらないところに価値があり、効果が目に見えないため、そこにどれだけの投資をすべきか適切な判断がとりにくいのです。後に述べる情報セキュリティ管理システムを運用しはじめると、リスク分析によりそこが明確になりますが、その前段階では大雑把な予算計画を立てるしかありません。そのような実態を受け、2002年３月に経済産業省とIPAの全面協力のもとNPO日本ネットワークセキュリティ協会(JNSA)が「インシデント被害調査」を実施しました。インシデントとは、「脅威」と訳される場合もありますが、ネットワークに何がしかの問題を生じさせる事象が発生し、それが現実の障害として認識される状態を一般的に表します。この調査は54社の企業を対象に直接ヒアリングする方法で実施されましたが、実際の被害を金額で現そうと試みているところが従来の調査と異なる点です。大半がウィルスの被害ですが、原因は別として何らかのインシデントが発生した場合、日常の業務が遂行できないという直接的な被害と、復旧のために余分な作業が発生するという副次的な被害の二重の被害を考慮する点が重要と分かります。

表１は調査により導き出した被害額の一覧です。一度の被害で最大6,000万円の被害を報告している企業がありますが、平均すると年間約500万円の被害があります。組織の規模にもよりますが、調査結果は何らかの目安になると思われます。

表1 **被害の状況**（インシデント毎の被害額。1企業最大3インシデントまで発生していた。）

（単位：円）

| 企業No. | コスト／日 | インシデント毎の被害額 | | | 年間合計 |
|---|---|---|---|---|---|
| | | 1回目 | 2回目 | 3回目 | |
| 1 | 40,000 | 60,000,000 | | | 60,000,000 |
| 2 | 40,000 | 200,000 | 20,000,000 | 60,000 | 20,260,000 |
| 3 | 40,000 | 1,860,000 | 15,000,000 | | 16,860,000 |
| 4 | 150,000 | 15,750,000 | | | 15,750,000 |
| 5 | 30,000 | 1,500,000 | 4,500,000 | | 6,000,000 |
| 6 | 45,000 | 3,915,000 | 549,000 | 450,000 | 4,914,000 |
| 7 | 150,000 | 1,500,000 | 3,000,000 | 20,000 | 4,520,000 |
| 8 | 40,000 | 2,004,000 | 40,000 | 2,400,000 | 4,444,000 |
| 9 | 40,000 | 416,000 | 800,000 | 800,000 | 2,016,000 |
| 10 | 40,000 | 220,000 | 1,620,000 | 80,000 | 1,920,000 |
| 11 | 40,000 | 800,000 | 800,000 | | 1,600,000 |
| 12 | 50,000 | 300,000 | 1,000,000 | | 1,300,000 |
| 13 | 32,000 | 320,000 | 12,800 | | 332,800 |
| 14 | 30,000 | 90,000 | 150,000 | | 240,000 |
| 15 | 25,000 | ? | 200,000 | | 200,000 |
| 16 | 30,000 | 180,000 | | | 180,000 |
| 17 | 15,000 | 60,000 | 50,000 | 50,000 | 160,000 |
| 18 | 160,000 | 120,000 | | | 120,000 |
| 19 | 18,000 | 9,000 | 99,000 | | 108,000 |
| 20 | 25,000 | 100,000 | | | 100,000 |
| 21 | 40,000 | 80,000 | | | 80,000 |
| 22 | 40,000 | 80,000 | | | 80,000 |
| 23 | 30,000 | 30,000 | 30,000 | | 60,000 |
| 24 | 40,000 | 60,000 | | | 60,000 |
| 25 | 40,000 | 16,000 | 30,000 | | 46,000 |
| 26 | 40,000 | 40,000 | | | 40,000 |
| 27 | 60,000 | 30,000 | | | 30,000 |
| 28 | 32,000 | 8,000 | 16,000 | | 24,000 |
| 29 | 40,000 | 20,000 | | | 20,000 |
| 30 | 30,000 | 15,000 | | | 15,000 |

※1　被害額はアンケート調査対象企業の報告をベースにしているが、コストが不明な部分（下線部）は、固定額（4万円）を設定し計算してある。
※2　被害額の算定に当たっては、「復旧に要した作業量」 n名×m日×1日あたりの人件費 により算出してある。

「インシデント被害調査」の被害額算定モデルなど詳細についてはIPAの公開情報を参考のこと。

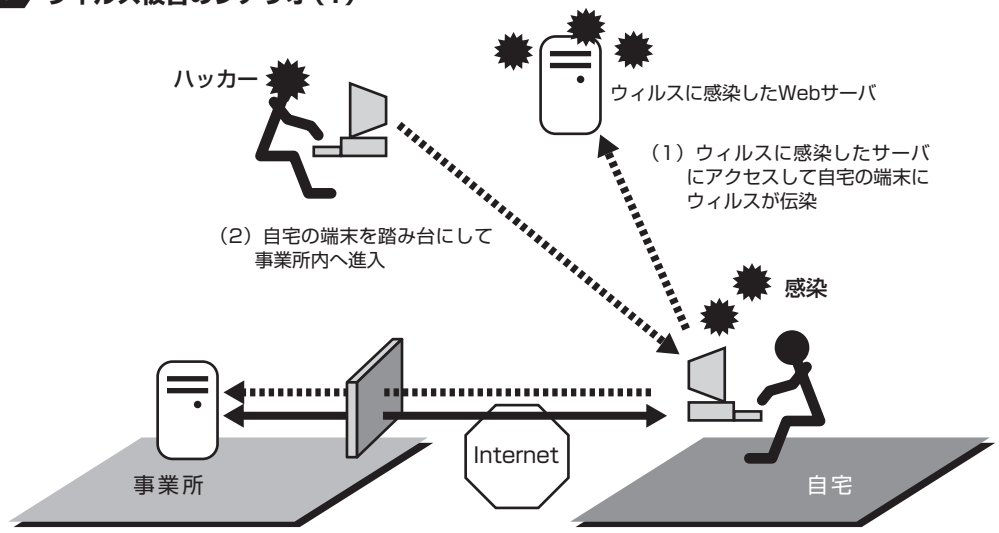
## 1-3. 攻撃のシナリオ

対策を練る時には、まず攻撃手法を知る必要があります。

従来はハッカーが（ハッカーとは善悪関係なく高度なテクニックを持つ者を指すしますが、ここでは一般的に用いられている呼び方として悪意を持った攻撃者をハッカーと呼びます）自らコンピュータを操作して特定の相手を攻撃していましたが、最近ではウィルスによる自動的かつ無差別な攻撃が主流となっています。自動的かつ無差別な攻撃により、地方の小さな公共団体であろうが、個人であろが関係なく被害を受けることになります。代表的なシナリオは以下の通りです。

### シナリオ1　ウィルスによる踏み台の設置

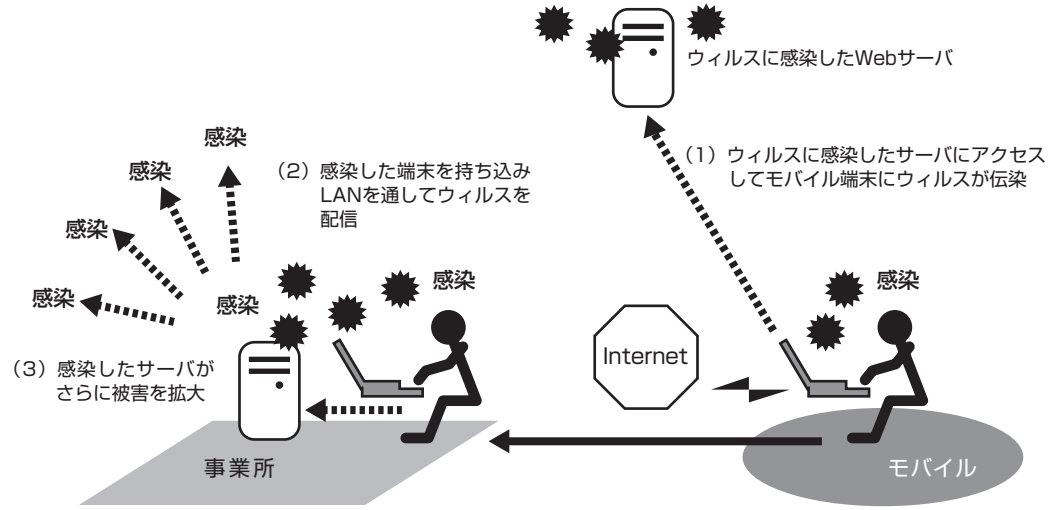
図2-a **ウィルス被害のシナリオ（1）**




ある大手IT企業の事例です。日常的に社員が自宅からインターネット経由で社内のサーバへアクセスしていましたが、それと知らずウィルスに感染したWebサーバへアクセスしてしまいました。ホームページを閲覧した瞬間、自宅の端末にウィルスが伝染してしまいバックドアを仕掛けられました。ハッカーがそれを発見し、バックドアを利用し社員の自宅の端末を踏み台にして事業所内へアクセスしました。この社員はファイアウォールを通過する権限をもっていたため、そのままハッカーも社内へ侵入が可能になりました。結果、重要な情報を持ち去られる被害を受けました。

## シナリオ2　事業所へのウィルスの持込

図2-b **ウィルス被害のシナリオ（2）**



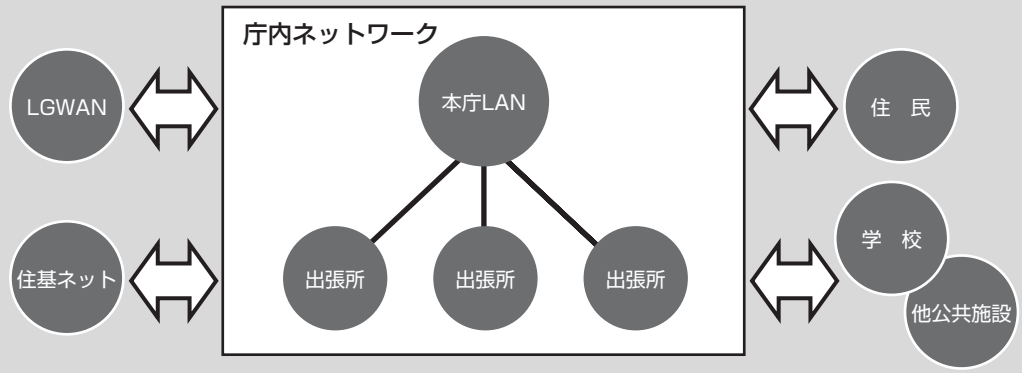

ある大手電機メーカの事例です。モバイル環境で社員がウィルスに感染したWebサーバへアクセスしホームページの閲覧を行いました。その際モバイル端末にウィルスが伝染してしまいましたが、それに気付かず帰社後に事業所内LANへ端末を接続。その瞬間端末からLAN上へウィルスが流れ出しサーバに感染。サーバからもウィルスが配信され、インターネットを経由して他社へも被害を広げました。

# 第2章　e-Japan戦略の中の地方自治体

e-Japan戦略を受けて2003年の電子政府実現に向け、「総合行政ネットワーク（LGWAN）」「住民基本台帳ネットワークシステム（住基ネット）」「電子政府認証基盤（GPKI）」などインフラの整備が進められています。これらインフラにより、各々の事情に関わり無く全国約3,300の地方自治体が一度に接続されることになります。さらに、そこには出先機関も接続され、各地方自治体の独自のサービスとして学校・病院・消防署など公共施設も接続されていきます。そこには今までに無い規模のネットワーク基盤が出現することになります。

ネットワーク化が進むことで既存のサービスの効率アップ、さらにまったく新しいサービスの創出が可能になります。これらサービスは、セキュリティが確保され安全性が保障されて始めて実現できるものです。しかし、前述した通り各自治体の内情に関わり無くすべてがネットワーク化される場合、いくら万全な対策を取っていても、接続を許可している相手が対策不十分だと、そこを踏み台にされ攻撃を受けてしまう可能性があります。セキュリティはレベルの低い方に合わされてしまうためですが、これは裏を返せば自身が攻撃者になる危険性もはらんでいることを意味します。これらのことを考慮し、電子政府基盤の一員である地方自治体として責任のあるセキュリティ対策を講じなくてはなりません。

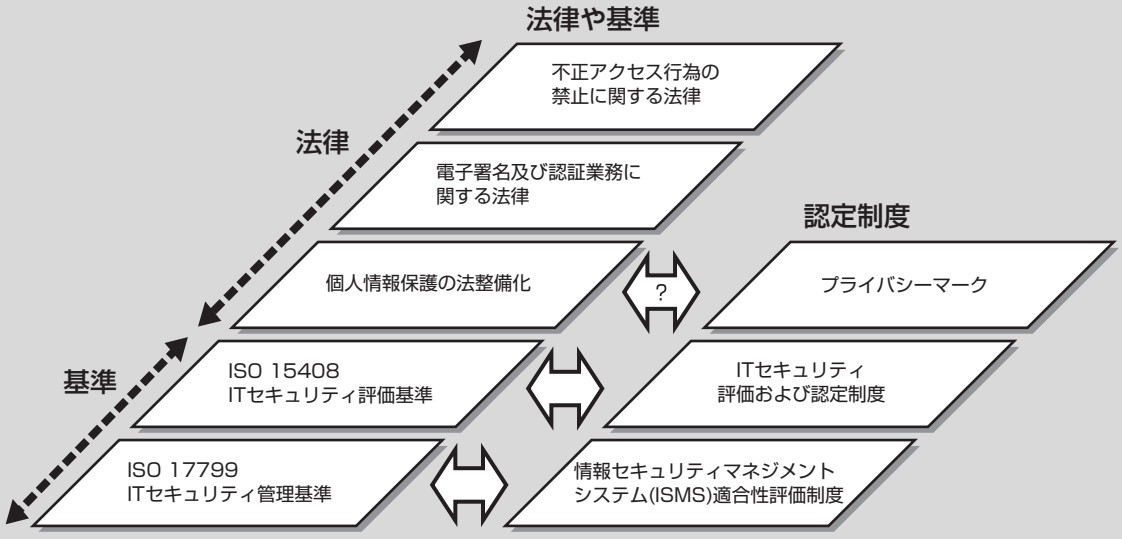
図3 **自治体の情報インフラ**




# 第3章 考慮すべき法律、セキュリティ標準および制度

セキュリティ対策の計画を立てる際に考慮すべき法律と、参考にすべき標準や制度を以下に挙げます。

図4 **情報セキュリティに関わる法律、基準、制度**



## 3-1. 各法律、セキュリティ標準および制度の概要

### 1）不正アクセス行為の禁止に関する法律

2000年2月に施行された不正アクセスを禁止する法律（不正アクセス禁止法）です。主に認証識別子（IDやパスワード）の不正使用によるコンピュータシステムへの不正な侵入を禁止する法律で、それまでの法律はコンピュータかデータが破壊あるいは改ざんされるか、フロッピーディスクなどが盗まれるなどしてはじめて適用できたのに対し、この法律では実被害が伴わずともアクセスしただけで取り締まりの対象になります。他人の認証識別子を使用し身元をなりすまして情報へアクセスする行為だけでなく、認証識別子を不正に他人に教えることも禁じています。

実際の現場で考慮する点は、各職員に発行したID・パスワードを他人に教える行為が不正アクセス禁止法に抵触する可能性があることを認知させることです。また、管理者がコンピュータや情報にアクセス制限を設定していることが前提として成り立つ法律であるので、それを実施していることを明確にしておくことが望まれます。セキュリティ対策を計画する際に、これらのことを庁内の規定（セキュリティポリシーなど）に盛り込むことを検討します。

### 2）電子署名及び認証業務に関する法律

2001年4月に施行された、電子署名に現在の実印と同等の法的根拠を待たせることを目的とした法律です。その信用性を裏付けるための基盤がPKI（Public Key Infrastructure：公開鍵基盤）です。

LGWANや住基ネットを通じてGPKIが地方自治体にも接続されます。2003年度から始まる住民基本台帳カードの配布等各種サービスにおいて地方自治体も間接的に関わりを持つ法律であるため、良く理解しておく必要があります。

### 3）個人情報保護について

行政機関については1988年に「行政機関の保有する電子計算機処理に係わる個人情報の保護に関する法律」が施行され、また、柏原市をはじめ多くの地方自治体は独自に個人情報保護条例を定め、運用を行い個人情報の保護に努めています。

また、別に「プライバシーマーク認定制度」がすでに運用されはじめています。これは1995年10月に採択されたEU指令などの動きを意識したものです。EU指令では、第三国にまで個人情報の十分なレベルの保護措置を求めていますが、世界的に同様の風潮がではじめています。このような状況の中で、個人情報を取り扱う事業者は取引先の信頼獲得のために適正性を裏づけられる必要があり、この要求に答えるのがプライバシー認定制度です。

そして、国でも個人情報保護については優先課題であり今後議論を重ねる案件のひとつです。このような状況を考慮し、新たに計画するセキュリティ対策には現行法案に準拠しさらに自治体の独自性を考慮した規定を盛り込む必要があります。また、2002年度内には個人情報保護を目的とした法整備も国レベルで活発化するようです。

### 4) ITセキュリティ評価基準

セキュリティ製品やセキュリティシステムの品質を保証する基準が1999年にISO 15408として国際標準となり、2000年7月にはJISX 5070として制定されました。政府調達においてこの基準を導入した制度を確立するために整備が始まっています。この制度では、ISO 15408に基づいて評価・認証された製品で構成することを入札要件とする方法をとるか、あるいは落札者が提供する製品やシステムについてISO 15408に基づくセキュリティ設計仕様書（ST：Security Target）を作成し、認定機関によりSTを評価し合格することを契約条件とする方法をとります。この制度により、政府が調達する製品・システムはISO 15408のセキュリティ基準を満たしたものになります。

地方自治体が同様の調達制度を設けるか否かは今後の課題として検討して行きたいと思います。

### 5) ITセキュリティ管理基準

情報セキュリティ管理システム（ISMS）の確立・運用を目指し1995年に英国規格BS 7799が制定され、その考え方を参考に2000年12月にISO 17799が作成されました。現在最も注目されている標準です。情報セキュリティはマネジメントプロセスであって技術的プロセスではないという考え方のもと、物理面、人的な面、電子的な面から総合的にセキュリティを構築・運用することを提唱しています。日本においても2002年4月からISMS認定制度を運用し、普及をめざしています。

この基準はISO 9000と同様の扱われ方をされると予想されています。ISO 9000は品質の保証を目的としたものですが、以前、商取引の世界では取引先から発注条件としてISO 9000の取得を求められたように、電子商取引においてもISO 17799の取得が接続相手先から条件付けられる可能性があります。

柏原市としてもセキュリティ対策において、ISMSの考え方を取り入れた設計をする方針で検討を進めていくことにします。

## 3-2. 柏原市としての取り組み

上記の通り、各法律、基準、制度について研究を重ね、できるだけ今後の制度に取り込んでいく方向で検討します。特に情報セキュリティ管理システム（ISMS）の考え方は柏原市のセキュリティ基盤として捉え、早急に取り組む方向で検討します。

その手順などはこの後の6章で述べることにします。

# 第4章 本計画における情報セキュリティの基本方針

本計画において、セキュリティは２つの次元で検討します。

1. **総合行政ネットワーク、住民基本台帳ネットワークシステムの導入に合わせた、短期計画。**（５章で解説）
2. **長期的な運用を見据えた、情報セキュリティ管理システム導入計画。**（６章で解説）

本来ならセキュリティ対策は6章で述べる情報セキュリティ管理システムに基づき、長期的なビジョンのもとで計画していくべきものではありますが、総合行政ネットワーク、住民基本台帳ネットワークシステムは今まさに進行中のプロジェクトであり、そのスケジュールに合わせた取り急ぎのセキュリティ対策を講じないわけにはいきません。何かしらの判断に基づき、短い時間の中でできる限り質の高いセキュリティを設計するために、５章でネットワークセキュリティ基本方針を定めました。内容は基本的な考え方と、実際にネットワークセキュリティを設計していく際の手順となっています。

続く６章は、長期的な運用を実現し、セキュリティを文化として根付かせるための方策として情報セキュリティ管理システムの導入について記述しています。

# 第5章 ネットワークセキュリティ基本方針

これより、IT 化の要であるネットワークに関するセキュリティの考え方と、
設計から導入にいたる基本方針について述べます。

## 5-1.ネットワークセキュリティの考え方

ネットワークの観点から、情報セキュリティを以下の３つに区分けして考えます。

1. 外部からの攻撃に対する防御
   ＝加害者にならないための施策
2. 内部の不正に対する防御
   ＝情報漏えい対策
3. 内部から外部へのトラフィックの制御
   ＝加害者にならないための施策
   ＝情報漏えい対策
   ＝業務の効率化

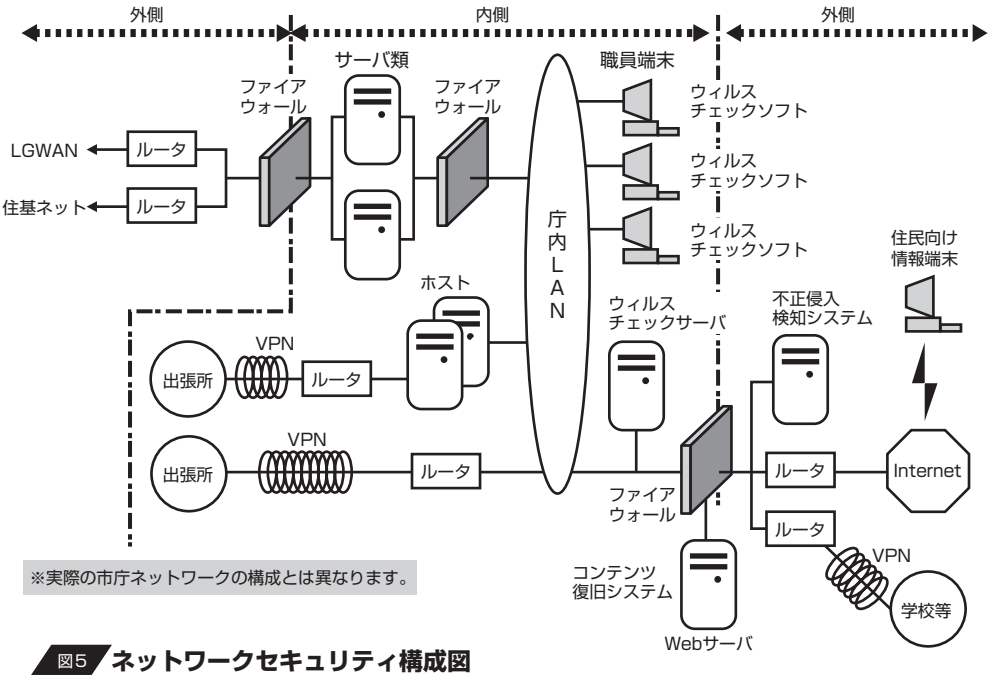



**図5 ネットワークセキュリティ構成図**

## 5-1-1.外部からの攻撃に対する防御

外部からの攻撃に対する防御は、“加害者にならないための施策”という基本思想のもとにセキュリティ設計を行います。すなわち、踏み台になって攻撃の中継をしてしまう、ウィルスの温床となってウィルスを配信してしまう、スパムメールの起点になってしまう、モラルの低い職員が直接的に他者を攻撃するなどの事態を未然に防ぐことに重点を置き、ネットワーク社会の一員としての責任をはたすことを目的とします。

図５は地方自治体のネットワークの概念図です。

地方自治体は外部との接点を、大きく分けて２種類持つことになります。ひとつは行政の基幹ネットワーク（「総合行政ネットワーク」「住民基本台帳ネットワークシステム」）との接点であり、もうひとつはローカルなサービスとして設ける公共施設（学校、病院、消防署など）や住民との接点です。

### 外部との接点

**1.行政の基幹ネットワーク**

●ネットワーク種別：
・総合行政ネットワーク
・住民基本台帳ネットワークシステム

●接続相手：
・他の地方公共団体など行政機関

**2.ローカルサービスネットワーク**

●ネットワーク種別：
・インターネット・CATV・その他

●接続相手：
・住民・学校・病院
・消防署・銀行・その他

外部の接続相手はコントロールできない要素であり、脅威として想定しておく必要があります。一般的には接点となる箇所にファイアウォールを設置し外部からの不正侵入を防ぎます。しかし、ファイアウォールはウィルスなど一見普通のプログラムやデータに見えるトラフィックは通過させてしまうため、併せてウィルスチェックサーバを設置します。外部との接点にウィルスチェックサーバを設置することにより、入ってくるウィルスは元より外部に出て行くウィルスも排除し、知らずに加害者になることを未然に防ぐことができます。同様にファイアウォールを補助するシステムとして不正侵入検知システム（IDS：Intrusion Detection System）も調査・検討します。

また、外部からの攻撃対象として最も狙われやすいWebサーバは上記システムの導入に加え、サーバ自身のセキュリティを高めるために、随時最新のパッチプログラムをインストールします。しかし、過去の例を見ても分かる通り、対策よりも攻撃手法が先に発見されることを考慮すると、完全に防御するという考え方とは別に、被害を受けた際にいかに早く復旧するかといった発想で、ホームページ復旧システムなども調査・検討します。

また、公共施設との接続にはVPN（Virtual Private Network）による暗号化通信の適用も検討します。通常セキュリティは受身の技術と捕らえられがちですが、VPNなどは、セキュリティが前提で初めて成り立つ新しいサービスの創出に結びつく可能性があるため、“積極的なセキュリティ”という観点からも検討しなくてはなりません。

## 5-1-2.内部の不正に対する防御

ネットワークセキュリティと言うと外部からの攻撃を論じることが多いのですが、ファイアウォールなどにより要塞化された組織に侵入することは困難であり、現実の被害は、外に公開されたホームページの改ざん程度で済むことが多いのです。過去の事件を振り返ると内部情報の漏えいは内部の者が行っていることが多いのです。一般的にも情報漏えいの80%は内部の犯行といわれています。このことを考慮すると、現実的に情報漏えいを防ごうとした時には、外部からの攻撃ではなく内部の不正を防御するという発想が必要になります。

情報の不正な取得を防ぐポイントはサーバへのアクセス制限と庁内LAN上での盗聴の防御です。サーバへのアクセス制限の基本は個人認証であり、パスワードの運用の強化やICカード・指紋認証といった個人認証デバイスの導入が具体的な方策となります。また、特に重要なサーバ類へのアクセス制御を強化するために、庁内LAN上にファイアウォールを設置することも考えられます。出張所も含めた庁内LANのどこかのセキュリティレベルが低くければ、そこから不正にアクセスされることも想定されるため、内部にファイアウォールという関所を設ける意味はあります。

ただし、いくらシステム的にセキュリティ対策をとったとしても、本来サーバへアクセスする権限を持った者の不正を防御することはできません。この問題は、後述する情報セキュリティ管理システムの範疇になりますが、少なくともサーバの管理者とは別の人員がアカウントの発行、アクセスログの監視などのオペレーションを実施し、サーバ管理者自身の管理を行う仕組みを用意することは必要でしょう。

次にLAN上での盗聴ですが、一般に市販されているスニファーあるいはパケットモニタリングソフトと呼ばれるような通信データ解析ソフトをPC端末にインストールすれば、誰もが簡単にLAN上を流れるデータを覗くことができます。無線LAN対応のソフトウェアも出てきていることから、今後普及が予想される無線LANにも同様の脅威があてはまります。ネットワーク上の盗聴を回避する方法としては、スイッチングHUBによるトラフィックの分離とVPNによる暗号化通信が代表的です。特にVPNは特定のサーバ・クライアント間のデータを秘匿できるので、庁内LAN内においても適用箇所を絞っての検討は行うべきだと考えます。

ところで、先に触れませんでしたが、ウィルスも内部ネットワーク上での脅威に数えられます。第１章で取り上げたように、外部で感染したPC端末をうっかり持ち込み、内部ネットワークに接続した途端にLANを介して伝染してしまう事例が多く報告されています。ウィルスは対策を講じていないと被害が広範囲にわたるため、各端末へのウィルスチェックソフトの導入は必須となります。また、内部のサーバにも基本的にウィルスチェックソフトを導入すべきですが、対応機種の問題もあるため、事前に調査した上で検討します。

## 5-1-3. 内部から外部へのトラフィックの制御

ネットワークセキュリティを考える時、内部から外部へのアクセスはあまり考慮されることはありません。しかし、就業時間中にネットサーフィンをして業務に関係のないスポーツや株価情報を見ることで、業務の効率の低下を招くし、ネットワークに無駄な負荷をかけることになります。さらに、メールの不正使用、たとえば中傷メール、身元を偽ってのメール、内部情報の発信を行うことにより、訴訟や信用の失墜、情報漏えいにつながりかねません。また、内部から外部へのトラフィックを制御することで加害者にならないための施策を補強することができるし、内部の不正を監視する役目もはたします。

内部から外部へのトラフィックを制御する方策は大きく２種類考えられます。ひとつはルールに基づき強制的にトラフィックを止める方法で、もうひとつは常時監視することにより抑制する方法です。

前者はコンテンツフィルタやメールフィルタを設置することで、事前に設定したルールに基づきアクセスを禁止されたホームページへの接続を拒否し、秘密情報に関するキーワードが入ったメールを強制的に止めます。この方法は実際にアクセスを止めるということでより直接的な制限になりますが、ルールを事前に検討する必要があり、かつ当該アクセスが業務上必要なものなのか、個人の興味によるものなのかを判断しかねる難しさもあります。一方、後者は常に内部のトラフィックを監視し、内部のユーザがアクセスしたホームページやメールの内容を保存しておき、必要に応じて閲覧することで、だれが過去にどこへアクセスしたのか、どのようなメールを送信したのかを監視する方法です。この場合強制的にトラフィックを止めることはしませんが、いつでも監視しているということを知らしめることで、ユーザ自ら規制することを促します。いずれの方法も一長一短があり、職員の行動を監視するという面も考えると、柏原市役所の文化と照らし合わせてどのような方策を採用するかを良く検討しなくてはなりません。

**図6-1 ルールに基づき強制的にアクセスを禁止**

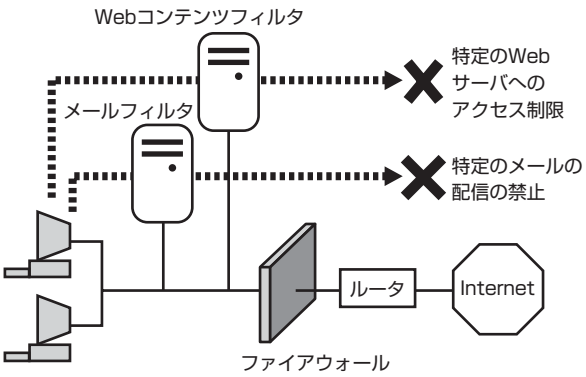
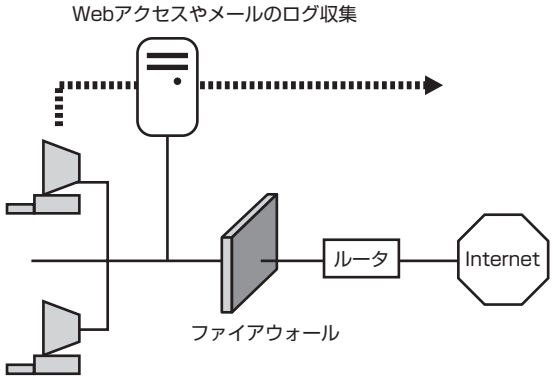



**図6-2 監視による抑制**



# 5-2. ネットワークセキュリティの設計手順

## 5-2-1. ネットワークセキュリティの設計のための検討事項

ネットワークセキュリティを設計するために以下の項目を検討します。

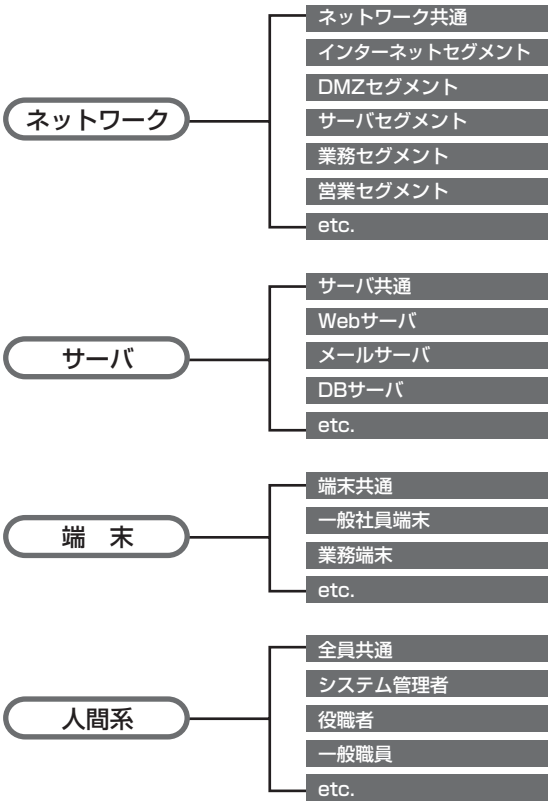
■保護の対象
　・対象資産のリストアップと適用範囲
■予想される脅威
　・誰から守るのか
　・どのような攻撃から守るのか
■防御の方法
■導入するシステムの仕様

以下に各項目について詳細を検討します。

### 1）保護の対象

#### a. 対象資産

保護の対象となる情報資産を洗い出します。情報資産は紙ベースのものも含みますが、ここではネットワークに注目しているため、それに関わる要素をリストアップします。



### b. 適用範囲の検討

セキュリティを適用する範囲は基本的に市がコントロールできる範囲とします。
具体的には以下の通りです。

・対象とするネットワーク
　図５で示すところの内部を対象とします。
・対象とするコンピュータ
　出張所を含み庁内LAN上のすべてのサーバおよび端末とします。住民サービス用に情報端末を設置する場合はそれも対象とします。
・対象とする人員
　常駐する業者を含む庁内に存在する者すべてとします。

## 2）予想される脅威

外部内部問わず以下のような攻撃手法が考えられます。

・不正侵入
・盗聴
・なりすまし
・改ざん
・ウィルス

それらを実行する者として以下が考えられます。

・外部：他の地方自治体、接続する公共施設、インターネットからアクセスしてくる者
・内部：出入りする住民、業者を含む庁内に存在する者

攻撃を試みる者がどの程度の技術力を有するのかも想定する必要があります。

## 3）防御の方法

防御の方法は、建物へのアクセスなど物理面あるいは人間の行動規定まで検討する必要がありますが、それらについては次章の「情報セキュリティ管理システムの導入」で触れることにして、ここでは実際に導入するセキュリティ技術の選定を主眼において検討します。

セキュリティ技術として以下のような項目が考えられます。

●サーバへの不正アクセスの防御
　・権限設定
　・パスワード強化
　・ワンタイムパスワード、指紋認証、IC カード、他
　・パッチプログラムの適用
●セグメントへの不正アクセスの防御
　・ルータフィルタリング、ファイアウォール、他
●VPN
●ウィルスチェック　…等

次のステップとして、ここまでの手順でリストアップした対象資産、予想される脅威、防御法を要求仕様に落とし込むために一覧にまとめ、その対策の必要性とコストを考慮して優先順位を決定していきます。

**表2 セキュリティ要求の選定表（サンプル）**

| 対象範囲 | 資　産 | 脅　威 | | | 対　策 | 手段と技術 | 優先度 |
|---|---|---|---|---|---|---|---|
| | | 大項目 | 中項目 | 小項目 | | | |
| サーバ関連 | サーバ共通 | 不正アクセス | セグメントへの侵入 | | ルータによるフィルタ | ルータ設定 | |
| | | | | | ファイアウォールによるフィルタ | ファイアウォールの導入 | |
| | | | 権限の取得 | パスワード漏洩 | パスワードファイルの保護 | アクセス権の設定 | |
| | | | | | パスワード運用の徹底 | 予測の困難さ | |
| | | | | | | サーバ毎に異なる | |
| | | | | | | 定期的に変更 | |
| | | | | | | ワンタイムパスワード導入 | |
| | Webサーバ | データ書き換え | | | 速やかな復旧 | 自動復旧システムの導入 | |
| | | | | | 囮による回避 | 囮サーバの導入 | |
| | メールサーバ | アカウントの漏洩 | | | アカウント・パスワードの秘匿 | 外向けサーバと内向けサーバの分離 | |
| | ⋮ | ⋮ | | | ⋮ | ⋮ | |
| ネットワーク関連 | 情報部門セグメント | 盗聴 | | | トラフィック分離 | スイッチングHUB導入 | |
| | | | | | データ暗号化 | VPNシステム導入 | |
| | 業務部門セグメント | 盗聴 | | | トラフィック分離 | スイッチングHUB導入 | |
| | | | | | データ暗号化 | VPNシステム導入 | |
| | | 不正アクセス | | | セグメント隔離 | 部内ファイアウォール設置 | |
| | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

（注）この表はサンプルであり、実際に利用するためには重要度や予算なども反映できるように作成する必要があります。

## 4）導入するシステムの仕様

表2で洗い出した項目には優先順位が付きます。優先順位の高いものから仕様に盛り込まれ、予算の関係によっては優先順位の低い項目は見送られることとなります。また、仕様を検討する場合は特に以下のことを考慮します。

・目的
・適用範囲
・要求する技術スペック
・運用性
・拡張性
・保守性

仕様が決定すると次は調達と実際のシステムの導入の段階となります。
導入後はいかに継続的に運用していくかがポイントになりますが、それは６章で検討します。

# 第6章 情報セキュリティ管理システムの導入

長期的な計画において、柏原市は継続的なセキュリティの運用を目指し、情報セキュリティ管理システムについて取り組む方針です。

先の章でも触れましたが権限を持つ者が不正を働くことを完全に防ぐことはできません。結局のところセキュリティは最終的に人のモラルといったところまで発展するのです。人為的な部分まで対象にした場合、技術的な側面だけでは限界があります。そのため最近では情報セキュリティ管理システム（ISMS：Information Security Management System）の考え方を導入する企業が増えています。地方自治体ではまだ本格導入をしているところはありませんが、セキュリティポリシーの策定など少しずつ取り組む自治体もでてきています。先に述べた通り、セキュリティの継続的また円滑な運用を図るために情報セキュリティ管理システムの導入を積極的に検討します。

一般的にセキュリティ対策はテクノロジーの発展と共に進化し続けるものですが、市としてのセキュリティ方針は恒久的に運用していくことを前提に決定していくべきであり、その手法として情報セキュリティ管理システムの考え方が適していると考えます。

情報セキュリティ管理システムにおいては「情報セキュリティはマネジメントプロセスであって、技術的プロセスではない。」と定義します。その対象とする範囲は物理的な面、人的な面、システム的な面すべてに亘り、対象とする脅威も人為的なものから偶発的なものまでを範囲とします。

現在、情報セキュリティ管理システムに関する標準規格としてはBS 7799、ISO 17799が良く知られています。すべての標準の手本になったのが英国規格のBS 7799であり、そこでは検討項目を以下のように記しています。

**表3 BS7799-2 第4章 要求仕様の一覧表**

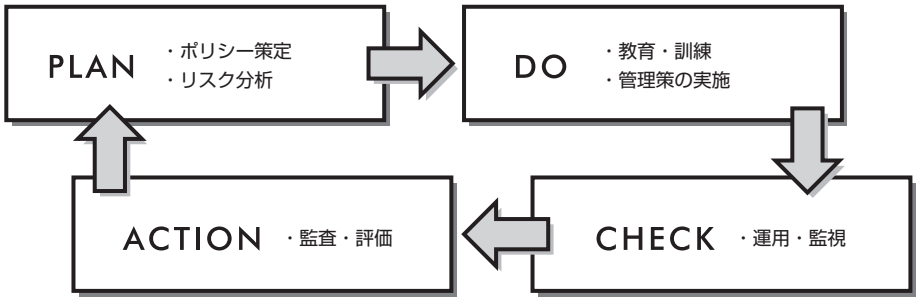
| 章 | 管理目的 |
|---|---|
| 4.1 情報セキュリティポリシー | 4.1.1 情報セキュリティポリシー |
| 4.2 セキュリティ組織 | 4.2.1 情報セキュリティ・インフラストラクチャー |
| | 4.2.2 第三者アクセスのセキュリティ |
| | 4.2.3 アウトソーシング |
| 4.3 財産の分類および管理 | 4.3.1 財産の説明責任 |
| | 4.3.2 情報の分類 |
| 4.4 スタッフのセキュリティ | 4.4.1 仕事の定義およびリソーシングにおけるセキュリティ |
| | 4.4.2 ユーザの訓練 |
| | 4.4.3 事故および誤動作への対処 |
| 4.5 物理的および環境的セキュリティ | 4.5.1 安全領域 |
| | 4.5.2 装置のセキュリティ |
| | 4.5.3 一般的管理策 |
| 4.6 通信および運用管理 | 4.6.1 運用手順および責任 |
| | 4.6.2 システム計画および受諾 |
| | 4.6.3 悪質なソフトウェアからの保護 |
| | 4.6.4 ハウスキーピング |
| | 4.6.5 ネットワークの管理 |
| | 4.6.6 媒体の取り扱いおよびセキュリティ |
| | 4.6.7 情報およびソフトウェアの交換 |

| 章 | 管理目的 |
|---|---|
| 4.7 アクセス制御 | 4.7.1 システムアクセスの事業要求事項 |
| | 4.7.2 ユーザアクセス制御 |
| | 4.7.3 ユーザの責任 |
| | 4.7.4 ネットワークのアクセス制御 |
| | 4.7.5 オペレーティングシステムのアクセス制御 |
| | 4.7.6 アプリケーションのアクセス制御 |
| | 4.7.7 システムアクセスおよびシステム使用の監視 |
| | 4.7.8 モバイルコンピューティングおよびシステム使用の監視 |
| 4.8 システム開発およびメンテナンス | 4.8.1 システムのセキュリティ要求事項 |
| | 4.8.2 アプリケーションシステムのセキュリティ |
| | 4.8.3 暗号による管理策 |
| | 4.8.4 システムファイルのセキュリティ |
| | 4.8.5 開発およびサポートプロセスにおけるセキュリティ |
| 4.9 事業継続管理 | 4.9.1 事業継続管理の側面 |
| 4.10 準拠 | 4.10.1 法的要求事項への準拠 |
| | 4.10.2 セキュリティポリシーおよび技術準拠のレビュー |
| | 4.10.3 システム監査の考慮事項 |

## 6-1. セキュリティライフサイクルによる継続的な運用

セキュリティシステムは導入したらそれで終わりでは無く、新たに発生するウィルス、頻繁に発見されるセキュリティホール、あるいは庁内の組織変更などにそなえ常に発展していく必要があります。そのためには、セキュリティライフサイクルを途切れることなく維持していくことが要求されます。

図7 セキュリティライフサイクル




## 6-2. 情報セキュリティ管理システムの導入メリット

**継続的にかつ普遍的にセキュリティの運用が可能になるというのが**情報セキュリティ管理システムの根本の目的でありメリットでありますが、他には以下のようなメリットが期待できます。

・組織のトップがコミットしたセキュリティポリシーの運用により信用が得られる。
・責任の所在が明確になり、曖昧な処理が回避できる。
・被害が発生した場合にも、再発防止のためのフィードバックができる体制が取れる。
・数値化の難しいセキュリティ施策の効果を客観的に評価できる。
・内部規定のリニューアルを図ることができる。

情報セキュリティ管理システムを構築・運用するために、組織のトップを含む「セキュリティ管理委員会」を組織しますが、ここで策定されるセキュリティポリシー等はすべてトップがコミットしたものとしてみなされます。前述したようにセキュリティは突き詰めると人の問題になり、最終的に誰を信用するのかというところに落ち着きますが、その時にトップがコミットしていることを内外に明示できることは有利にはたらきます。

また、管理システムでは業務上の役割を明確にして責任の所在を明らかにすると共に、権限を明確にすることで曖昧な判断を回避できる機構を作ります。役割や権限は人ではなく組織や役職に割り当てるため、後に人員構成が改変されても規則を変えず普遍的な運用が可能になります。

地方自治体は「保有する情報を公開しながら守る」という特殊な事情があり、一般企業と異なり完全な要

塞化は不可能に近いと言えます。したがってセキュリティ対策を講じたとしても何らかの被害を受ける可能性は残ります。しかし、その際も情報セキュリティ管理システムを導入することで、失敗を知見として取り込める構造を持つことが可能になり、より速やかに制度の改善を図ることが可能になります。これは情報セキュリティ管理システムが、ある割合で被害が発生することを前提として検討されるからです。

このように何よりも最優先で遵守すべきポリシーを持ち、責任と権限を明確にすることにより不正な行為の発生を抑止することになります。

## 6-3. セキュリティポリシー

情報セキュリティ管理システムでは、運用指針を明示するためにセキュリティポリシーの策定を行います。セキュティポリシーは以下の要件を考慮して作成します。

- セキュリティ要件をまとめ、効率化をはかるための基礎である。
- 組織に横断的に、全組織に関わる方針とする。
- 組織の上層部の支援が得られる必要がある。
- 組織の上層部が承認・発行し全職員が知覚する必要がある。
- 事業責任者はコミットしていると見られる必要がある。
- 法的要求、契約事項へ準拠する。
- 保護すべき情報資産を特定する。
- 責任・権限を明らかにする。
- 組織の業務内容や文化を反映させる。

セキュリティポリシーは図8のような構成で表わすことができます。まず憲法にあたる「基本ポリシー」を作成し、それに準拠した「スタンダード」を作成し、最後に現場での具体的な手順書である「プロシージャ」に落とし込みます。

セキュリティポリシーは策定後、組織内に教育を施し周知徹底します。また、基本ポリシーは外部への開示も検討します。

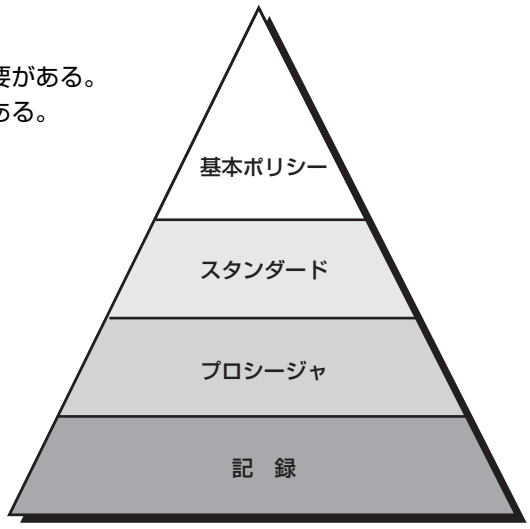



図8 セキュリティポリシー

### 1）基本ポリシー

セキュリティに関する基本的な考え方であり、普遍的な内容とします。組織としての方針を表わすもので基本的には改訂しません。参考として、次ページに企業の基本ポリシーのサンプルを挙げました。

一部の地方自治体では、まず基本ポリシーを作成し、首長が全職員の前で発表した後、個別に全職員から同意書にサインを取り、同意した者に対しメールなどのアカウントを発行するという手順を踏んでいるところがあります。柏原市としてもできるところから始めるという方向も検討する必要があると考えます。

## 情報セキュリティに関する基本ポリシー（サンプル）

2001年X月XX日
株式会社XXXXXX
代表取締役社長　XXXX

**1 基本方針**

当社の事業のすべては、有効な情報を活用することによって行われている。当社が所有する情報資産はすなわち経営資産そのものであり、事業継続および拡大のために、その機密性、完全性、利用の可能性を確保することが、経営上の重要な課題となる。

情報資産を適切に維持管理することは、対外的な当社の価値を高めることになり、取引において重要な競争優位性を生むことになる。国際水準を前提とした情報セキュリティ管理策の構築により、国際的に認められる企業価値を確立する。

**2 セキュリティポリシーの定義と役割**

当該セキュリティポリシーは、当社における情報セキュリティの方針を示すものであり、経営者を筆頭にすべての社員に、情報資産の使用権限に応じたセキュリティ管理の義務と責任を割り当てる。また、セキュリティ義務と責任を果たすために必要不可欠かつ適切な情報セキュリティ管理システムを構築し、その維持管理体制を確立する。

**3 セキュリティポリシーの適用範囲**

当該セキュリティポリシーの適用範囲は、当社のすべての組織と業務に関わる情報資産、情報システムおよびそれを扱うものを対象とする。

**4 セキュリティポリシーの構成**

当該セキュリティポリシーは基本ポリシー（*1）、スタンダード（*2）、プロシージャ（*3）から構成される。

**5 情報セキュリティ管理委員会**

情報セキュリティ管理委員会の構成員は、取締役会によって選任される。なお、情報セキュリティ管理委員会には経営陣が参加し、運営を支持する。

**6 セキュリティポリシーの管理体制と責任**

適切なセキュリティレベル維持のために、情報セキュリティ管理委員会は情報セキュリティ管理策および、関連プロシージャの定期的なレビューと評価を行う。また、定期的にセキュリティ監査を実施し、セキュリティポリシーの妥当性を確認する。

**7 セキュリティポリシーの教育管理体制**

業務に関わるすべての人員が情報セキュリティに関して共通の概念を持ち、適切な対応を可能とするために、セキュリティポリシー教育を定期的に行う。新人教育時のみではなく、定期的な教育・訓練を行うことで、当該セキュリティポリシーの周知徹底を図る。

**8 業務継続計画**

当該セキュリティポリシーは情報セキュリティ以外のインシデントとの整合性を図り、業務継続に支障のない管理策を講じる。

**9 遵守義務と罰則**

当該セキュリティポリシーでは、適用範囲で規定したすべてのものにその遵守を義務づける。また、セキュリティポリシーおよび関連するプロシージャを違反したものには、原則として罰則を課す。基本罰則は教育的指導および権限の移動とするが、個人の責任によって、情報セキュリティに重要な影響を与える行為、個人のプライバシー侵害に該当する行為、資産損失を招く悪質な行為を犯した場合には、取締役会で協議の上、職務規定上の処分を課す。

**10 例外事項**

当社の事業のすべては、有効な情報を活用することによって行われている。当社が所有する情報資産はすなわち経営資産そのものであり、事業継続および拡大のために、その機密性、完全性、利用の可能性を確保することが、経営上の重要な課題となる。

情報資産を適切に維持管理することは、対外的な当社の価値を高めることになり、取引において重要な競争優位性を生むことになる。国際水準を前提とした情報セキュリティ管理策の構築により、国際的に認められる企業価値を確立する。

**11 セキュリティポリシーの維持・管理**

当該セキュリティポリシーは情報セキュリティ管理委員会で策定され、独立したレビューによって、維持管理する。

以上

*1　基本ポリシーとは本書を指す
*2　基本ポリシーを遵守するために規定した具体的な管理策を示す文書
*3　スタンダードの中から、対象となる業務遂行者や業務内容に適応したセキュリティ規定を定義した文書群

### 2）スタンダード

スタンダードは具体的な規定集にあたるドキュメントです。この部分は基本ポリシーと異なり、技術の進歩に合わせて改訂していくことになります。スタンダードを策定するにあたり検討すべき項目は「表３ BS7799-2 第４章 要求仕様の一覧表」に挙げた通りですが、同様のものに平成 12 年３月に総務省が公開した「地方公共団体のためのコンピュータセキュリティに関する調査研究報告書（http://www.soumu.go.jp/kokusai/pdf/security.pdf）」があり、その内容がまさしくスタンダードに相当するものなので、まずは、その報告書をたたき台にして、柏原市としての特性や最新の情報を反映させた独自のスタンダードを構築する予定です。

### 3）プロシージャ

実際の手順書にあたるものがプロシージャで、そこには、物理的な面では事業所への出入りの手順や設備の扱いなどについて記述があり、人的な面ではゴミの捨て方や机の上の書類に関する規定、システム的にはコンピュータやネットワーク機器のログイン手順や、誰がどのように管理するかといった具体的な行動指針が明記されています。手順書は役割の異なる部門毎に作成されます。

マニュアル的なものであるので、実際のシステム導入などに伴って作成されます。

## 6-4. 教育

情報セキュリティ管理システムを運用するにあたり、教育は非常に重要な位置をしめます。ここで言う教育には訓練も含みます。教育は導入時だけではなく定期的に開催し、セキュリティポリシーの徹底を図ります。専門の教育チームが設置できるのが理想ですが、アウトソーシングも含め今後どのように実施すべきか、課題として検討します。

## 6-5. セキュリティ運営組織

情報セキュリティ管理システムを導入し継続的に運用するために、セキュリティの専門知識を有する者のコンサルテーションを受けることを考慮しつつ、既存の組織とは独立したセキュリティ管理及び運用のための専門委員会を設置し、検証や見直しを行っていきます。また、今後、専門委員会設置についての検討を進める中で、委員の構成が変わった場合を想定したポリシーも策定していく必要があります。具体的には、本来、情報セキュリティ管理システムにおいて、権限等は人ではなく役職や部門に対して規定するので問題なしとするのか、あるいは外部の有識者を専門委員会に参画願い、コミットしていくという手順にするのかといったことが考えられますが、さらに良い方策を検討していきます。

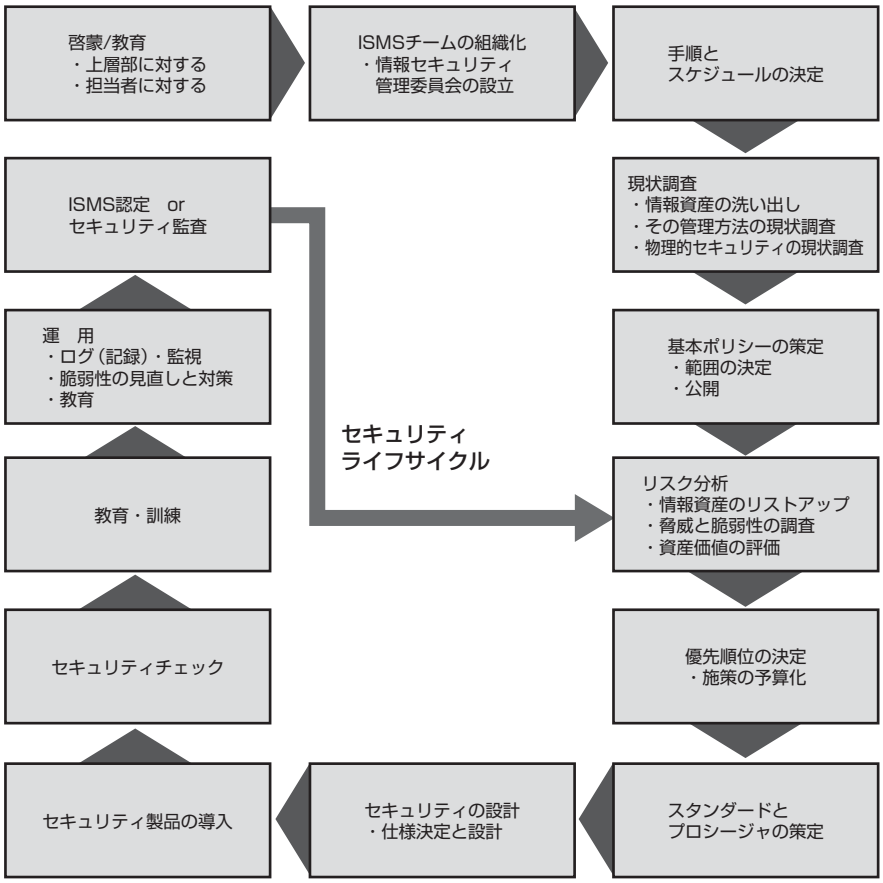
## 6-6. 情報セキュリティ管理システム導入までの手順

組織の確立から始まり、導入・運用までの手順を挙げます。

下図の手順ではISMS認定が最終項目となっていますが、ISMS認定は客観的にセキュリティレベルを表す意味で取得することが望ましいということで、認定は単なる通過点でありゴールではないということを認識しておきます。情報セキュリティ管理システムはあくまでも円滑にセキュリティライフサイクルを運用していくことを目的としていることを忘れてはなりません。また、ISMS認定は自治体のような業態にはなじまない可能性があり、それに代わる手順としてセキュリティ監査も検討しておく必要があります。

導入にいたるまでの工程は準備段階も含め約半年、また導入後運用してセキュリティライフサイクルが一巡するまで約半年の、合計約１年の期間をひとつの目安として考えます。

**図9 情報セキュリティ管理システム導入・運用手順**



# 第7章 本計画における セキュリティシステムの実施について

本計画におけるセキュリティシステムの実施については、別途、実施計画においてスケジュール等を立案していきます。

なお、本計画を推進するためにセキュリティシステム導入に先駆け、その要件を洗い出し、計画の妥当性の評価、スケジュールの立案、予算計画素案の策定等を検討するため、市職員とIT分野に精通した者、IT分野の法律に精通した者、ネットワーク技術者、本市のシステムを構築している事業者等で組織した検討委員会を設置します。

**＜セキュリティ検討委員会の役割（案）＞**

■組織

・既存組織（協議会やフォーラムなど）の下位組織として設置。

・メンバー

専門家：IT分野に明るい専門家、法律に詳しい専門家、ネットワーク技術者、庁内システムを構築している事業者

市の職員：現場を知る情報システム担当など

■役割

・事前調査
・電子政府の動向
・他の地方自治体の動向
・学校や病院など地域の公共施設の動向
・セキュリティ標準の動向
・柏原市の現状
・スケジュール立案
・啓蒙活動、勉強会
・セキュリティ製品導入時の支援
・予算の見通し