図4.1に情報管理の位置づけを示します。

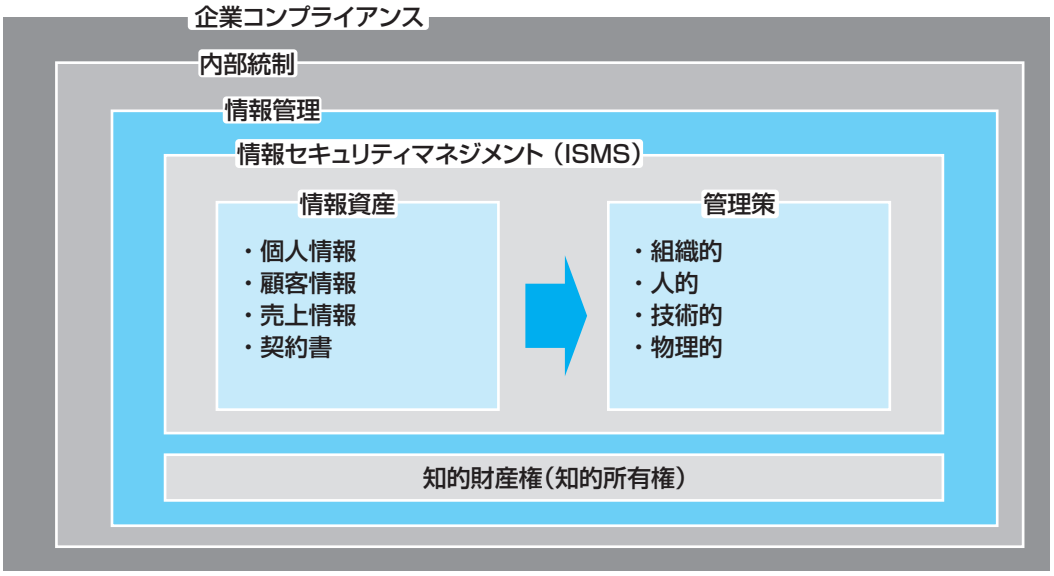

図4.1　情報管理の位置づけ

4.2 情報セキュリティマネジメントシステム（ISMS）

情報セキュリティマネジメントシステムは、情報セキュリティ管理を一般化し、管理および対策する要素を体系化したものです。情報セキュリティ管理を実施する際のガイドラインとして活用されます。

ISMSは、機密性、完全性、可用性を阻害するさまざまな脅威から情報資産を守ることを目的にしています。機密性、完全性、可用性とは情報セキュリティの3要素といわれ、情報セキュリティ対策を行なう上で重要なものです。3つの要素をまとめてCIA（Confidentiality：機密性、Integrity：完全性、Availability：可用性）ともいわれます。

■ 機密性

情報へのアクセスを許可された人のみに制限すること。例えば、企業の管理職しか人事情報を見ることができないなど。

■ 完全性

情報が完全であること。例えば、外部から侵入してデータを改ざんしたり、社内の人間が誤ってデータを変更したりできないようにすることなど。

■ 可用性

情報へのアクセスを許可された人が必要なときに情報を取出すことができること。例えば、災害などにより情報にアクセスできない状況を回避することなど。

ISMSの全体の流れを図4.2に示します。

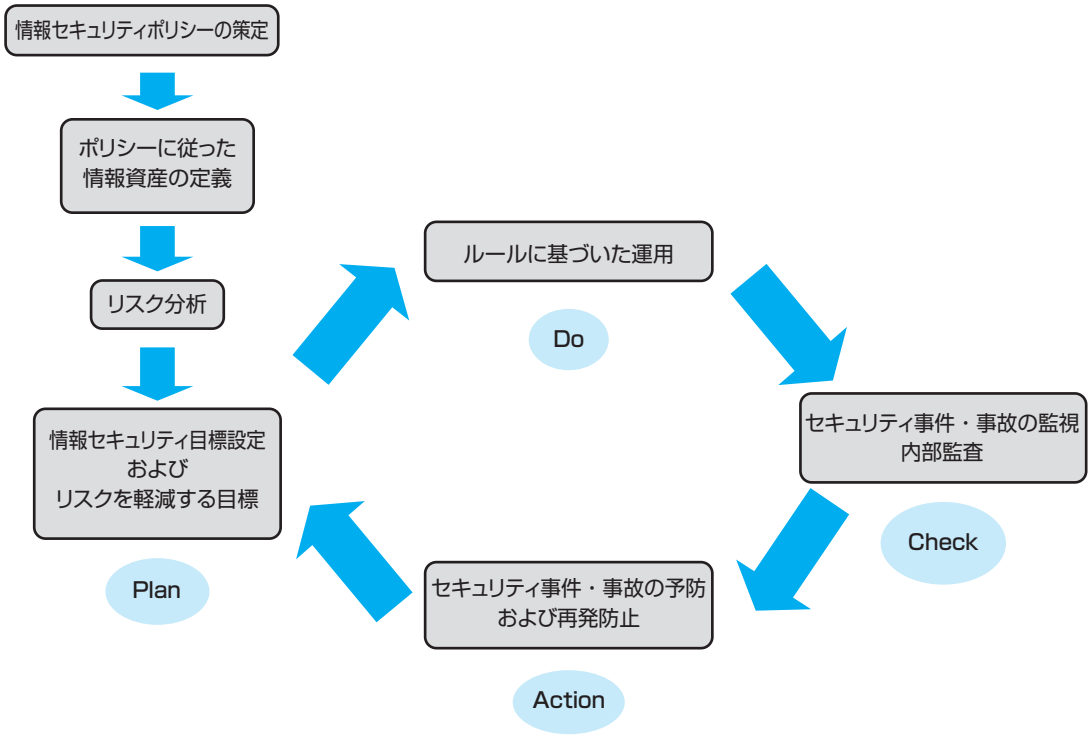

図4.2　ISMSの全体の流れ

最初に全体の方針である情報セキュリティポリシーを策定します。情報セキュリティポリシーはISMSの指針となるものですが、情報資産もこのポリシーに従って定義を行ないます。情報資産とは会社や組織が守るべき情報であり、盗難や漏えいによって組織がダメージを受けるものを指します。具体的には、顧客情報や販売情報などの電子情報に加え、ファイルやデータベース、CD-ROMなどのメディア、紙の資料も含まれます。次に、その情報資産に対す

るリスク分析を行ないます。どのような脅威や脆弱性があるかを洗い出し、それらのリスクに対する現状の対策を評価します。また、対策不足の場合は、そのリスクを回避または軽減するための目標を明確にします。

運用においては、ルールに基づいた情報資産の管理を行い、もし事件や事故があった場合は予防や再発防止に努め、随時セキュリティポリシーの見直しを行います。このようにPDCAサイクルを運用して情報セキュリティの質向上を図って行きます。

4.2.1 ISMSの管理策

ISMSでの具体的な対策のことを管理策といいます。管理策は4つの側面から検討する必要があります。その側面とは、組織的、人的、技術的および物理的側面です。それぞれの管理策は、各情報資産のリスクを軽減するものとなります。

■ 組織的管理策

ISMSを実施していく上では、それを管理運営する為の組織が必要になります。会社の代表を筆頭として情報セキュリティ最高責任者やセキュリティ委員会、セキュリティ監査などの組織を明確にする必要があります。業務とは別にセキュリティに関する責任を持ち、組織横断的に構成されます。4.3.1節で詳しく説明します。

■ 人的管理策

ISMSを実施していても、各個人の意識が薄ければ何にもなりません。きちんとした組織を作り、技術的に堅牢な情報システムを構築したとしても、会社のパソコンにファイル共有ソフトをインストールして、大切な会社の情報を漏えいさせては元も子もありません。日頃より、会社の方針を伝え、しっかりとした教育を行うことも重要な人的管理となります。4.3.2節で詳しく説明します。

■ 技術的管理策

インターネットを経由した不正アクセスや、情報資産へのアクセスをコンピューターやネットワーク機器で制限するものです。4.3.3節で詳しく説明します。

NOTE

PDCAサイクル：計画（Plan）し、それを実行（Do）した後、評価（Check）して改善（Action）する一連のサイクルを廻すことにより継続して改善向上していく手法。

■ 物理的管理策

情報資産を置いている場所への制限を設けるなどの入退室管理や、機器や接続回線などを冗長化するなどの物理的対策を指します。紙での情報資産を鍵付きキャビネットに保管するなども物理的管理策に入ります。4.3.4節で詳しく説明します。

以上、4つの側面からISMSの管理策を行なう必要があります。また、この管理策の内容はセキュリティポリシーの対策基準として適用宣言を行い、明確にしておく必要があります。

4.2.2 情報セキュリティポリシー

情報セキュリティポリシーとは、組織として情報資産を守るための方針や規準を明文化したものです。具体的には、情報資産の扱い方に関する内容を記載したもので、個々の情報機器の設定や取り扱いについての手順はもとより、建物への入退室管理や書類の管理方法、組織がどのようにあるべきかといった事柄なども、情報セキュリティポリシーに定められ、組織はこれに基づきISMSを実施します。

また、情報セキュリティポリシーは、セキュリティレベルの向上のためだけでなく、セキュリティ対策の費用対効果の向上、対外的な信頼向上などを目的として策定します。

情報セキュリティポリシーの参考例として、政府のガイドラインなどがありますが、それをそのまま自社に当てはめても、多くの場合は実情にそぐわない内容で、結果的に形骸化した運用になってしまうことがほとんどです。それは、企業によって社内規程や守るべき情報資産、それに対するリスクが異なるためです。情報セキュリティポリシーを機能的なものにするためには、自社の実情に即したものを策定する必要があります。

■ 情報セキュリティポリシーの構成

情報セキュリティポリシーには決まった形はありませんが、一般的に図4.3のような階層構造を持ちます。

このような情報セキュリティ体系を構築する場合、大まかな方針を策定すると同時に現状を分析して突き合わせ、方針と現状との間で整合しない部分を調整していく、いわゆるPDCAサイクルに沿った形で構築していくのが理想的な形であるといえます。

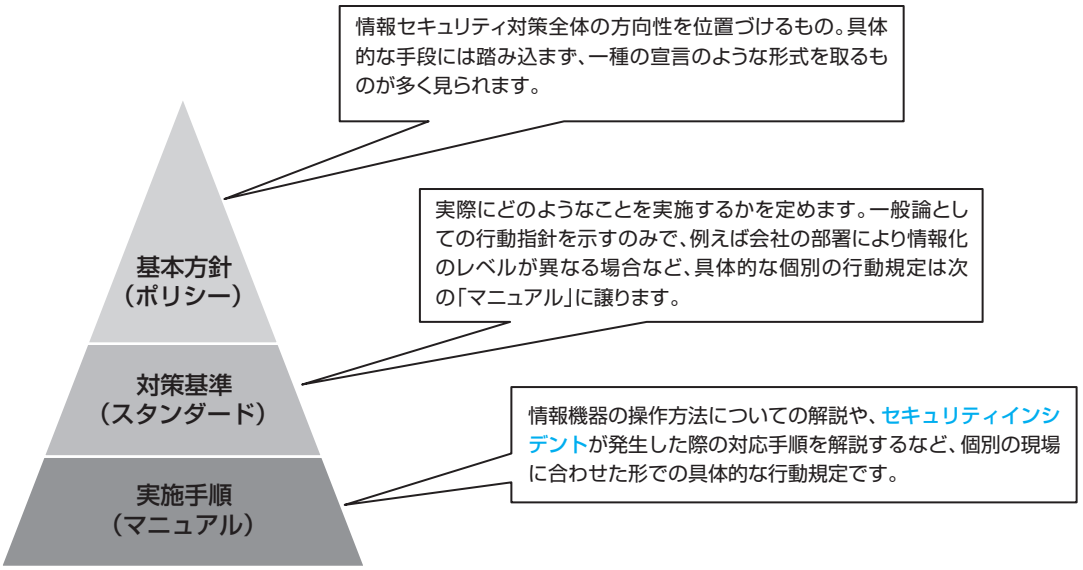

図4.3　情報セキュリティポリシーの構成

■ 情報セキュリティポリシーの策定体制

全社統一の指針ですので、各部署の協力は必須です。各部門が保有する情報資産の棚卸をしたり、既存の社内規程類との整合性を保ったりという意味でも、社内の関連部署から適切な人材を招集し、組織横断的に策定体制を整備します。また、必要であれば、外部のリスクマネジメントやシステム監査に関する専門家を加えます。

■ 情報セキュリティポリシーの記述例

表4.1に情報セキュリティポリシーの記述例を示します。情報セキュリティポリシーには具体的なルールを記載します。

NOTE

セキュリティインシデント：インシデントとは事件や出来事という意味で、全体では不正アクセス、情報漏えいやウイルス感染などのセキュリティに関する事件、事故を指します。

表4.1　情報セキュリティポリシー記述例

内容	文書名	文書
基本方針	基本方針文	当社は情報資産に対する不正アクセス、紛失、破壊、改ざんおよび漏えいなどが発生しないように、役員、従業員および全ての従業者に対して、適切な組織的・人的・技術的・物理的諸施策を講じ、法令およびその他の規範を遵守させます。 ○セキュリティ委員会が中心となり情報セキュリティマネジメントシステムを継続的に実施・改善していきます。 ○情報セキュリティに関するコンプライアンス、著作権法、不正競争防止法、労働基準法を遵守し、情報セキュリティマネジメントを実施します。
対策基準	適用宣言書	当社が実施する管理策は以下の内容とする。 ○組織：セキュリティ委員会を作り、メンバーを各部門から起用し、ISMSを推進する。 ○教育：半期に1回、セキュリティ意識を高めるための社内教育を実施する。 ○利用制限：社内の電子情報資産は、アクセス権を設定して制限をかけなければならない。
実施手順	電子情報管理規定文書	○情報資産を保管するフォルダーは、必ずアクセス権限を設け必要以上に閲覧、更新、削除ができないように設定する。 ○読み出しおよび書き込みにはパスワードを設定する。 ○保管時には予め定められた場所に保管する。 ○セキュリティ管理者はフォルダー名および設定したアクセス権を管理台帳で管理する。

4.2.3 リスク分析

リスク分析とは情報資産に対する脅威と脆弱性を洗い出し、リスクが組織のどこに、どの様に存在していて、またその大きさはどの程度かを測定する作業のことです。

■ リスクを構成する要素

リスクとは何らかの事態が発生する可能性であり、それ自体は実体を持った損失ではありません。ただし、そのリスクが顕在化したときに損失が発生します。そのため、どこにどのようなリスクが存在しているかを知ることは非常に重要なことです。

リスクは、情報資産と脅威と脆弱性の3つの要素から構成されます。

- 情報資産（守るべきもの）
  情報システムを構成するコンピューターや、ネットワーク機器などの有形資産と、プログラムやデータなどの無形資産に分類されます。
- 脅威（事故や不正行為）
  セキュリティを阻害する外的要因であり、ウイルスや、災害などが挙げられます。
- 脆弱性（事故や不正行為を助長させるような弱点）
  セキュリティを阻害する内的要因であり、セキュリティホール、運用ルールが明確化されていないシステムなどが挙げられます。

■ 情報資産

情報資産は企業が守るべき資産です。盗難や漏えいによって企業がダメージを受けるものを洗い出し、どのように守っていくのかを検討します。顧客や社員、取引先の個人情報も重要な情報資産となりますので、しっかりとした定義が必要になります。情報資産の定義に関して、表4.2に例を示します。このように情報資産の定義を行い情報資産台帳に記述して管理を行います。ここで示したのは一例で、項目として全ては掲載していませんので、企業ごとに必要な項目を検討する必要があります。

表4.2　情報資産の定義の一例（情報資産台帳）

部門	内訳	情報資産	機密区分	保管場所
総務部	顧客情報	得意先台帳	社外秘	ファイルサーバー
営業部	取引先情報	契約書	社外秘	キャビネット
営業部	個人情報	顧客内部資料	部外秘	キャビネット
技術部	設計資料	設計資料	社外秘	ファイルサーバー
・				
・				
・				

表4.2で定義した情報資産に対して、リスク分析をおこないます。表4.3にリスク分析を行なった例を示します。

表4.3　リスク分析の例

情報資産	想定される危険（脅威）	影響する領域			今後の対策
		機密性	完全性	可用性	
得意先台帳	情報漏えい	●			システム利用条件の厳格化
契約書	窃盗	●		●	鍵付きキャビネットに保管
顧客内部資料	自然災害			●	耐火金庫に保管
設計資料	誤削除		●		ログの取得、バックアップ、メディアの管理
・					
・					
・					