ＩＳＭＳの基礎知識

あどばる経営研究所
A.V.MANAGEMENT

1. 情報セキュリティとは

そもそも「情報セキュリティ」とは何を意味するのか。

BS7799/ISMS 認証基準では、

「情報セキュリティ」・・・「情報の**機密性**、**完全性**及び**可用性**の維持」と定義されている。

機密性・・・アクセスを認可された者だけが情報にアクセスできることを確実にすること

完全性・・・情報及び処理方法が、正確であること及び完全であることを保護すること

可用性・・・認可された利用者が、必要な時に、情報及び関連する資産にアクセスできることを確実にすること

これらは裏を返せば、

機密性・・・情報の漏洩を防ぐこと

完全性・・・情報の間違いや改ざんを防ぐこと

可用性・・・情報の喪失・紛失を防ぐこと

と言うこともできる。

マスメディアが取り上げるニュースや人々の関心はとかく機密性に偏りがちであるが、ＩＳＭＳを構築する際は、「機密性」、「完全性」、「可用性」の三つに着目しなければならない。

2．マネジメントシステムとは

マネジメントシステムには情報セキュリティマネジメントシステム（ISMS）の他に、ISO9001の品質マネジメントシステム（QMS）、ISO14001の環境マネジメントシステム（EMS）などがよく知られているが、マネジメントシステムとはPDCA（Plan→Do→Check→Act）に基づいた管理の骨組みのようなものである。情報セキュリティや品質や環境で肉づけすることにより、ISMSになったりQMSになったりEMSになったりする。

マネジメントシステムの具体的な内容は、三つのマネジメントシステム規格に共通する要求事項の項目を見ていくとわかる。

- **基本方針の策定**
- **責任と体制**
- **手順の文書化**
- **文書管理**
- **記録**
- **教育**
- **内部監査**
- **不適合の是正**
- **経営層の見直し**
- **法令等準拠**

これら以外にそれぞれの規格に特有な要求事項もあるが、BS7799/ISMS認証基準にはISO14001を知っていると理解しやすい点がある。例えばISO14001で環境影響評価の結果、環境目的を設定し、環境マネジメントプログラムを実践することが求められるが、BS7799/ISMS認証基準ではリスク評価の結果、管理目的の設定と管理策の実践が要求される。また、ISO14001で緊急事態への対処があるが、BS7799/ISMS認証基準でも事業継続管理として、重大な事故や災害が起こった場合を想定した対策が求められている。なお、BS7799-2:2002とISMS認証基準Ver.2.0では、序文の中でISO9001、ISO14001との両立性について触れている。ISO9001、ISO14001をすでに取得している企業においては、それらと整合・統合してISMSを導入・運用することができる。つまり、要求事項の整合性が取られているので、リスク評価や事業継続管理などで手法や手順を応用することができ、また、内部監査やマネジメントレビューなど、他のマネジメントシステムとまとめて実施することで統一を図ることもできる。

3. ISMSの構築

情報セキュリティマネジメントシステムを構築するにあたり、何を準備すればよいのか迷う方もいらっしゃるかもしれないが、最初に必要なのは、実施体制（組織と責任）を決めることと、全体の活動スケジュールを立てることである。具体的な機器、設備、システム、規定、手順などが必要になってくるのはリスクアセスメントの後である。

① 実施体制の決定

まず、情報セキュリティマネジメントシステムを構築・運用するための実施体制を決定し、担当者を任命する。

BS7799/ISMS認証基準の「組織のセキュリティ」の要求事項をふまえると、下記の組織が最低限必要となる。

a. 情報セキュリティ運営委員会
b. 組織の関連部門からの管理者の代表を集めた委員会
c. 情報セキュリティの助言を行う内部または外部の専門家
d. 情報セキュリティ基本方針の実施をレビューする者

a.は、セキュリティを主導するための明瞭な方向づけおよび経営陣による目に見える形での支持を確実にするためのものであり、ISMS構築・運用のコアとなる組織である。事務局としての活動が多いが、どこの会社もいまや情報処理や通信にデジタル技術を導入しており、規格の詳細管理策もこうした情報技術に関するものが多いので、技術的な知識のある者を含めた方がよい。

b.については、大きな組織などで、情報セキュリティの管理策の実施を調整するために必要である。

c.は、情報セキュリティに関して助言ができる、特に技術的な面で高度な知識と経験のある専門家がよい。

d.については、第三者的に内部監査を行う組織が必要である。

② 活動スケジュール

実施体制が整ったところでいよいよ活動開始であるが、おおまかな活動予定表を作成しておくとよい。

活動の概要としては、まず、経営陣は基本方針を策定し、全体の方向性と概略を従業員に周知する。基本方針を理解させた上で、最初の作業として全従業員に情報資産についての情報を提出してもらう。そしてそれらの情報資産について事務局がリスクアセスメントおよびリスク対応を行う。その結果に基づき管理目的および管理策を選択し、適用宣言書を作成する。文書化された手順が必要なものについては手順書を作成する。手順書、規定、基本方針を基に全従業員を対象に教育を実施する。従業員は手順を実行する。内部監査チームは、ISMSの運用状況を監査する。内部監査で出た不適合については、是正を行う。経営層は見直しを行う。審査機関による審査を受ける。

全体的な流れは次ページの図のようになる。

4. ISMSの運用フロー

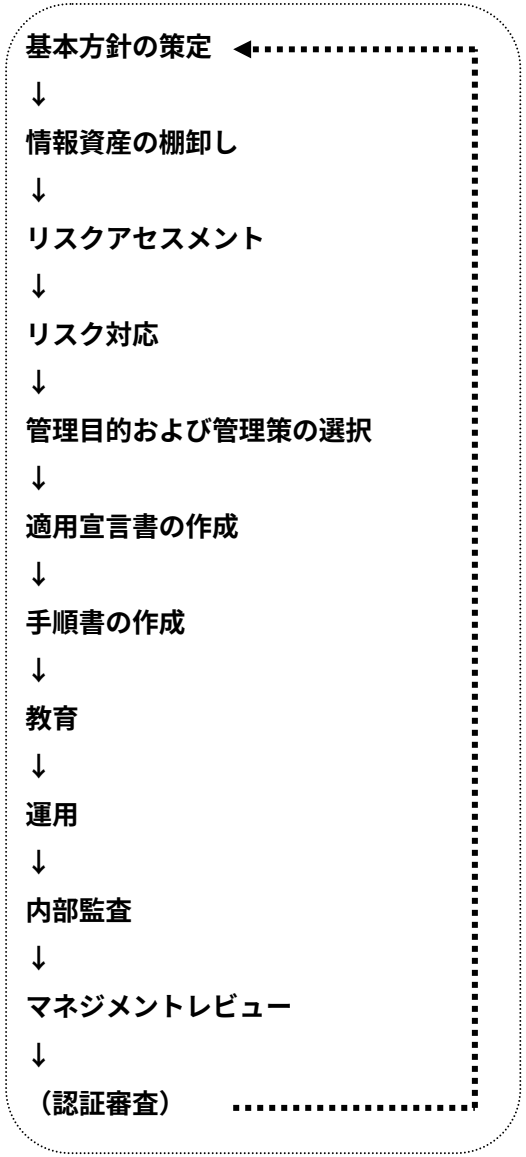


図1：ISMSの運用フロー

この流れは、情報セキュリティマネジメントシステムが確立したあとも定期的に繰り返される。
サイクルとしては、審査機関による認証審査が半年に一度であるので、それに合わせて実施すると運用しやすい。
審査を意識しすぎているように思われるかもしれないが、やはり従業員のモチベーションという点で、教育や内部監査などの際、協力を得やすいということがある。また、認証審査でISMSの根底に関する指摘を受けた場合などは、認証審査後すぐに基本方針に反映することができ好都合である。

あどばる経営研究所
A.V.MANAGEMENT

5．情報セキュリティの規格について

◇BS7799とは

○　BS7799の構成について

BS7799はPart1、Part2からなる。

Part1は情報セキュリティマネジメント実施基準として情報セキュリティに関する最良の慣行をまとめてあり、手引きおよび勧告の形式をとっている。

一方Part2は情報セキュリティマネジメントシステム仕様として情報セキュリティの様々な要求事項からなる。したがってPart2は認証審査の基準となる性質をもち、Part1は情報セキュリティマネジメントシステムを構築するための参考手引きとなる。

BS7799の認証審査はPart2のみをベースに実施される。

○　BS7799の要求事項について

それでは、BS7799のPart2はどんな要求事項からなるのか。

ISO9001やISO14001など他のマネジメントシステム規格と内容の整合が取られているということは、前述の通り既に紹介済みであるが、BS7799には以下の10項目の詳細管理策が提示されていることが特徴的である。

1．セキュリティ基本方針
2．組織のセキュリティ
3．資産の分類及び管理
4．人的セキュリティ
5．物理的及び環境的セキュリティ
6．通信及び運用の管理
7．アクセス制御
8．システムの開発及び保守
9．事業継続管理
10．適合性

リスクアセスメントおよびリスク対応の結果を基に選択すればよいことになっているが、選択しない場合には合理的な理由が必要となる。

又、取捨選択可能という前提ではあるが、「セキュリティ基本方針」、「組織のセキュリティ」、「資産の分類及び管理」、「人的セキュリティ」、「事業継続管理」、「適合性」などのISMSそのものの運用に関わる部分については事実上外すことはできない。

◇　BS7799の歴史について

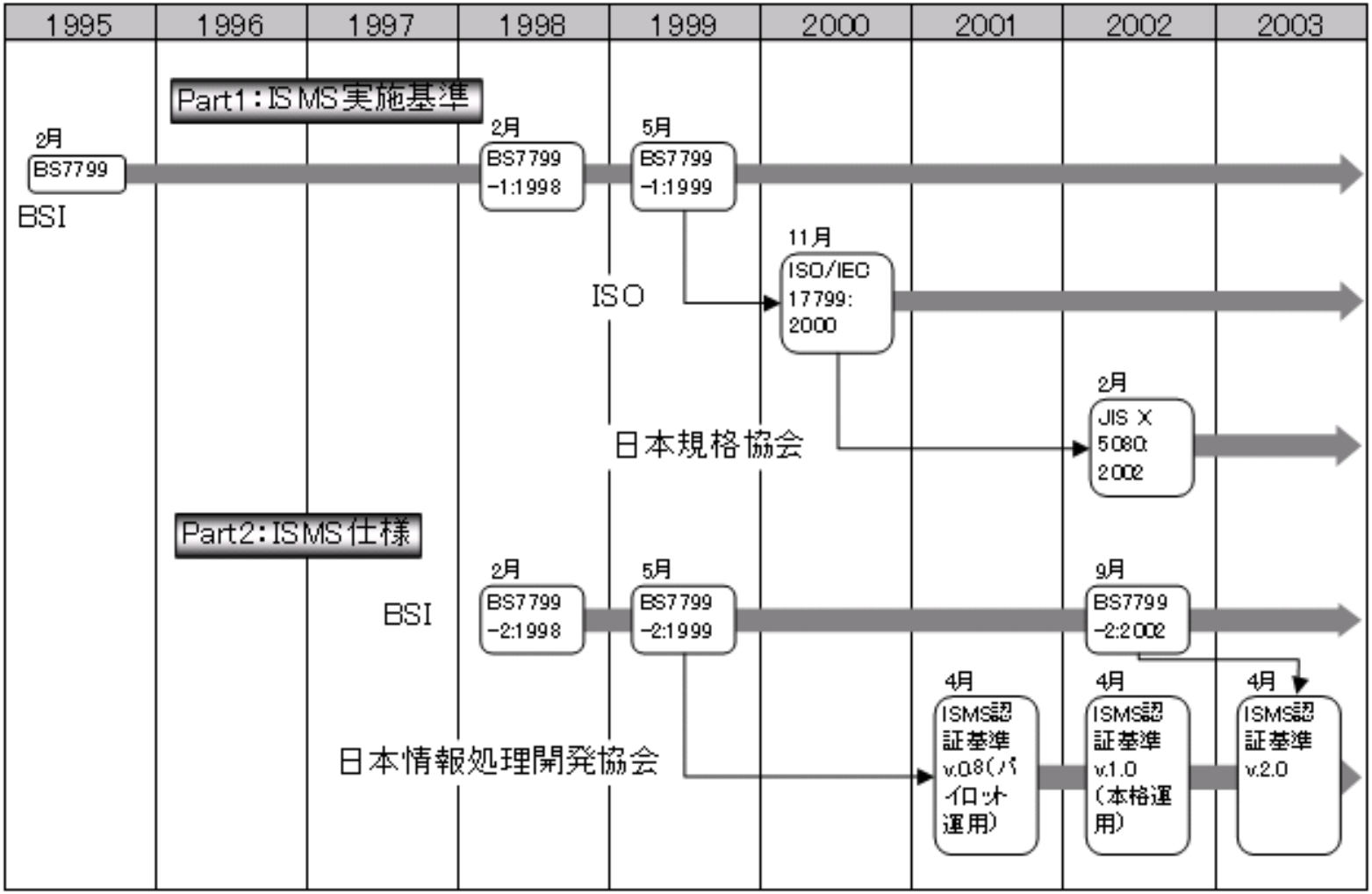
○BS7799は、工業・商業分野で情報システムが使用される際、必要な管理策の範囲を明確にするための基準として大中小の営利・非営利組織に　よって使用されることを目的とし、情報セキュリティに関する最良の慣行をまとめた包括的管理策として、1995年に英国で発行された。
そして1998年には、組織の全体もしくは一部の情報セキュリティマネジメントシステムの評価のための基礎とするべく、情報セキュリティマネジメントシステム仕様である**Part2**が発行された。

○Part1、Part2とも、その後、情報処理技術の利用における発展、特にネットワークおよび通信分野における発展を視野に入れ、1999年版が発行され、Part2に関しては、2002年に、ISO9001やISO14001など他のマネジメントシステム規格との整合性が取られ、マネジメントシステムの特徴であるPDCAの枠組みが強調された内容に改訂された。
なお、Part1はISO/IEC17799として2000年にISO化され、ISO/IEC17799は、日本で2002年にJISX5080として標準化された。

◇　ISMS 適合性評価制度について

○ISMS適合性評価制度の認証基準は、財団法人日本情報処理開発協会（JIPDEC）が**BS7799-2を基に作成**したもので、2001年4月にパイロット運　用がスタートした。
　2002年4月には適用範囲を情報処理サービス業以外の企業にも拡張し本格運用を開始した。
BS7799-2が2002年版に改訂されたことを受け、**ISMS認証基準もVer.2.0が2003年4月**に発行された。

6.ISMS規格の関連と流れについて



7．他の規格について

情報セキュリティに関する規制や基準は他にも様々なものが作られており、今日も進化しつつある。規格としては、マネジメントシステムに関するもの以外にもハードウェア／ソフトウェアに関するもの、個人情報の取扱いに関するものなどがある。ここでは簡単に他の規格についても紹介しておきたい。

◇　個人情報保護関連

個人情報の保護に関しては、先進諸外国ではコンピュータの活用が本格化するようになった1960年代以降、大量に蓄積された個人情報が不用意に漏洩するなどの危険性が増大したことから、1970年代にはすでに個人情報保護に関する立法措置等を講じてきた。1980年には、OECDでプライバシー保護と個人データの国際流通についてのガイドラインが採択され、これを受けてOECD加盟国は1980～90年に次々と法制化をとげた。また、1995年には「EU個人情報保護指令」が採択され、EU加盟国は３年以内に法律の制定・改正を求められた。

日本では、1988年に「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」が公布され、1997年３月４日には、通商産業省（現・経済産業省）が「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」を告示したが、その後も個人情報の漏洩などの事件が続発し、ガイドラインを補完する制度が必要となった。そこで、財団法人日本情報処理開発協会（JIPDEC）が、このガイドラインに準拠して個人情報の取扱いを適切に行っている民間事業者に対して“プライバシーマーク”の使用を認めるプライバシーマーク制度の運用を1998年４月１日より開始した。顧客の個人情報を扱う情報サービス・調査業、学習塾、印刷業などの企業が多く取得している。

また、財団法人日本データ通信協会では、電気通信事業者と発信者情報通知サービス（ナンバーディスプレイなど）の事業用利用者を対象に、適正な個人情報保護措置を講じている事業者の登録を行い、個人情報保護マークの表示を許可している。

なお、民間を対象にした「個人情報の保護に関する法律」が2003年5月に公布された。

◇　製品のセキュリティ性能関連

IT製品（ハードウェア／ソフトウェア）やシステムのセキュリティ性能に関しては、欧米諸国やロシアでは1980～90年代から軍事上の理由などでそれぞれ自国の評価・認証制度を運用していたが、CC(Common Criteria)として共通化・統合化を目指し、1999年６月には国際標準のISO/IEC15408として承認された。この規格では、セキュリティ機能要件を定め、それらの機能要件がいかに確実に製品に実装されているかを確認するための保証要件を定めている。ISO/IEC15408は、日本でも2000年７月にJISX5070として標準化された。

なお、ISO/IEC15408は、2001年４月から日本の各省庁の調達基準になっている。

◇　日本の情報セキュリティ規格

日本における情報セキュリティ関連制度の動向としては、1981年に通商産業省が、「情報処理サービス業における安全対策の実施の促進を図り、もって情報化の健全な発展に資すること」を目的に、情報処理サービス業を行う事業所を対象として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（安対制度）を開始した。しかしながらインターネットの普及にともない、ハードウェア／ソフトウェアによる対策や日々の管理運用におけるセキュリティ対策が必要不可欠となり、また、ネットワーク全体のセキュリティレベル向上のために国際的なスタンダードを踏まえる必要性が生じてきた。そこで、**ISMS 適合性評価制度のスタートにともない、2001年３月をもって安対制度は廃止された。**

8. ISMS文書について

◇　規格で要求される文書

○BS7799/ISMS認証基準における文書に関する要求事項は下記のとおりである。**最低限、これらを含めなければならない。**

（1）情報セキュリティ基本方針及び管理目的の表明。

（2）当該ISMSの適用範囲並びにISMSを支える手順及び管理策。

（3）リスクアセスメントの結果報告。

（4）リスク対応計画。

（5）情報セキュリティに関するプロセスの効果的な計画、運用及び管理を確実に実施するために、組織が必要と判断した、文書化された手順。

（6）本基準が要求する記録。

（7）適用宣言書。

○個々の文書については別資料であらためて解説するが、ここでは要求事項の表現が多少わかりづらいと思われるものについて説明を加える。

（2）の「ISMSを支える手順」について

ISMSを運用するための手順を文書化する。

情報セキュリティ基本方針策定からリスクアセスメント、リスク対応、適用宣言書の作成までの管理枠組み、規定・手順書の作成、文書管理、記録管理、教育、マネジメントレビュー、内部監査、改善、その他法規制関連、事業継続管理などISMSの運用に関する事柄を、誰が、いつ行うかということを手順として作成する。

（5）について

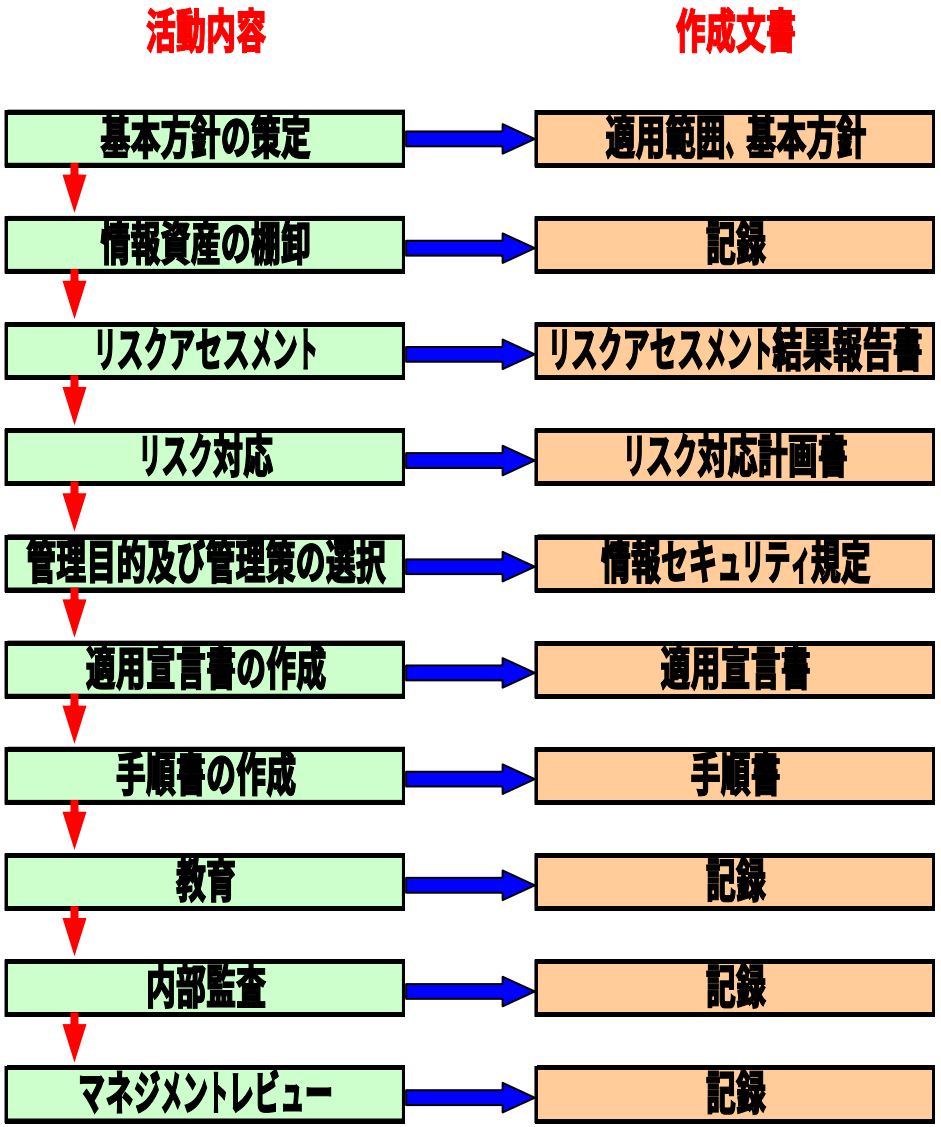
選択した管理策を実施するために文書化された手順が必要なものについて手順書を作成する。

分野ごとに手順書を作成し、全社共通でそれらを使用する方式が基本であるが、部門や担当業務によってセキュリティ手順が異なれば、それぞれの部門や担当業務ごとに手順書を作成してもよい。

9．文書作成順序

「情報セキュリティマネジメントマニュアル」はISMSの運用に関する手順書なので、本来は先に用意されているべきものであるが、初めてISMSを構築する場合は、実際の作業をやりながらその手順をまとめるようなつもりで作成していくと手順を整理でき、改善点などを思いつくきっかけとなってよい。

ISMSの活動スケジュールにあわせて文書を作成していく



10. 管理枠組み文書の作成