■3 群（コンピュータネットワーク）－ 7 編（コンピュータネットワークセキュリティ）

8 章 情報セキュリティマネジメント

（執筆者：長谷川長一）［2009 年 4 月 受領］

■概要■

【本章の構成】

■3 群 － 7 編 － 8 章

8-1 情報セキュリティマネジメントの概要

（執筆者：長谷川長一）［2009 年 4 月 受領］

ここでは，情報セキュリティマネジメントの目的や基本的なアプローチなど，その概要を説明する．

8-1-1 情報セキュリティマネジメントの目的

組織が活動を続けていくためには，活動に関する様々な要素を包括的かつ体系的な視点で評価し，継続して管理（マネジメント）していく必要がある．同様に，情報セキュリティを確保する際にも，組織の情報セキュリティに関する要素を包括的かつ体系的な視点で評価し，対策を講じ，継続的に管理していく必要がある．

情報セキュリティマネジメントとは，組織の情報セキュリティ対策を包括的かつ体系的に，更に継続的に実施することである．

なお，情報セキュリティについての基本的な用語を，以下に示す．ここでは，これらの定義を用いて，情報セキュリティマネジメントを説明していくこととする．

表 8・1　情報セキュリティの定義～ISO/IEC 27001:2005(JIS Q 27001)

用　語	意　味
情報セキュリティ（information security）	情報の機密性，完全性及び可用性を維持すること．更に，真正性，責任追跡性，否認防止及び信頼性のような特性を維持することを含めてもよい．
機密性（confidentiality）	認可されていない個人，エンティティまたはプロセスに対して，情報を使用不可または非公開にする特性．
完全性（integrity）	資産の正確さ及び完全さを保護する特性．
可用性（availability）	認可されたエンティティが要求したときに，アクセス及び使用が可能である特性．
真正性（authenticity）	ある主体または資源が，主張どおりであることを確実にする特性．真正性は，利用者，プロセス，システム，情報などのエンティティに対して適用する．
責任追跡性（accountability）	あるエンティティの動作が，その動作から動作主のエンティティまで一意に追跡できることを確実にする特性．
否認防止（non-repudiation）	ある活動または事象が起きたことを，後になって否認されないように証明する能力．
信頼性（reliability）	意図した動作及び結果に一致する特性．

8-1-2 情報セキュリティマネジメントの基本的なアプローチ

(1)　情報セキュリティのリスク

情報セキュリティマネジメントを実施していくには，まず組織にどのような資産があり，どのような情報セキュリティ上のリスクがあるのか，を明らかにする必要がある．

この場合の「リスク」とは「ある脅威が，情報資産または情報資産グループのぜい弱性を利用して，情報資産への損失，または損害を与える可能性」（JIS Q13335-1:2006）である．

情報セキュリティにおけるリスクは，一般的に以下のような式で示される．

リスク ＝資産の価値 × 脅威 × ぜい弱性

この式によって求められる値を「リスク値」と呼んでいる．

そして，このリスク値により情報セキュリティ上のリスクがどの程度なのか，その度合いを知ることができる．また，リスクを知るためには，この「資産」「脅威」「ぜい弱性」が識別，評価できなければならない．

ここからは，この式の三つの要素「資産」「脅威」「ぜい弱性」について説明する．

(2) 資産

まずは「資産」だが，これが情報セキュリティでは対策を実施して「守るべき対象」ということになる．以前は「情報資産」と呼ばれることが多かったが，JIS Q27002 では「資産」という用語を用いている．「資産」は何が存在し，どの程度の価値をもつものかは，その組織によって異なる．

なお，JIS Q 27002:2006 であげられている資産の例が以下の**表 8･2** である．

表 8・2 「資産」の例示～JIS Q 27002:2006

資産区分	例 示
情 報	データベース及びデータファイル，システムに関する文書，ユーザマニュアル，訓練資料，操作手順または支援手順，継続計画，代替手段の手配，記録保管された情報
ソフトウェア資産	業務用ソフトウェア，システムソフトウェア，開発用ツール及びユーティリティ
物理的資産	コンピュータ装置（プロセッサ，表示装置，ラップトップ，モデム），通信装置（ルータ，PBX，ファクシミリ，留守番電話），磁気媒体（テープ及びディスク），そのほかの技術装置（電源，空調装置），什器，旧称設備
サービス	計算処理及び通信サービス，一般ユーティリティ（例えば，暖房，照明，電源，空調）
人	保有する資格，技能，経験
無形資産	例えば，組織の評判，イメージ

(3) 脅 威

「脅威（threat）」は，「システムまたは組織に損害を与える可能性があるインシデントの潜在的な原因」（JIS Q13335-1:2006）とされている．「資産」には，必ず何らかの「ぜい弱性」をもっており，そこに「脅威」が付け込むことで，リスクが顕在化し，被害や影響が発生する．

以下の**表 8･3** は，脅威の分類の例である．

表 8・3　脅威の分類例

脅威の分類		例　示
人為的脅威	意図的脅威	攻撃（不正侵入，ウイルス，改ざん，盗聴，なりすまし，など）
	偶発的脅威	人為的ミス（ヒューマン・エラー），障害
環境的脅威	環境的脅威	災害（地震，洪水，台風，落雷，火事，など）

(4)　ぜい弱性

「ぜい弱性（Vulnerability)」は「データ処理システムの弱点または欠陥」(JIS X 0008:2001) とされている．よく「セキュリティホール」という表現がされているが，以下のような定義もある．

ソフトウェア製品やウェブアプリケーションなどにおけるセキュリティ上の問題箇所である．コンピュータ不正アクセスやコンピュータウイルスなどにより，この問題の箇所が攻撃されることで，そのソフトウェア製品やウェブアプリケーションの本来の機能や性能を損なう原因となり得るものをいう．

個人情報などが適切なアクセス制御のもとに管理されていないなど，ウェブサイト運営者の不適切な運用により，ウェブアプリケーションのセキュリティが維持できなくなっている状態も含む．

～「ソフトウェア等ぜい弱性関連情報取扱基準」（平成 16 年経済産業省告示第 235 号）

つまり，「ぜい弱性」という用語は「セキュリティホール」のみならず，不適切な運用・管理などにより，セキュリティが維持できなくなっている状態も指すもの，と理解しておくべきであろう．

以下の**表 8･4** は，ぜい弱性の分類と関連する脅威を結びつけたものである．

表 8・4　ぜい弱性の識別～JIS Q 27002:2006

ぜい弱性の分類	ぜい弱性の例	関連する脅威の例
環境，施設	ドア，窓などの物理的保護の欠如	盗　難
	不安定な電源設備	停電，誤作動
	災害を受けやすい立地条件	洪水，地震，災害
ハードウェア	温湿度変化に影響を受けやすい	故障，誤作動
	記憶媒体のメンテナンス不足	故障，情報漏えい
ソフトウェア	仕様書の不備	ソフトウェア障害，誤作動
	アクセスコントロールの欠如	なりすまし，改ざん，情報漏えい
	不適切なパスワード	不正アクセス，改ざん，情報漏えい
	監査証跡（ログ管理）の欠如	不正アクセス
	バックアップコピーの欠如	復旧不能
……	……	……

■3 群 － 7 編 － 8 章

8-2 リスクアセスメントとリスク対応

（執筆者：長谷川長一）［2009 年 4 月 受領］

情報セキュリティ上のリスクに包括的かつ体系的に対応するためには，リスクの分析や評価を行ったうえで，対応を決定していく．ここでは，これらの作業項目である「リスクアセスメント」と「リスク対応」について説明する．

8-2-1 リスクアセスメント

「リスクアセスメント」とは，「リスク分析から評価までのすべてのプロセス」を指す．つまり，「リスクアセスメント」は，大きくは「リスク分析」と「リスク評価」の二つに分類される．

8-2-2 リスク分析

「リスク分析」とは，「リスク因子を特定するための，及びリスクを算定するための情報の系統的使用」とされている．また，リスク分析は「リスク因子の特定」と「リスク算定」の二つからなり，この結果により，リスク評価，リスク対応の基礎となる情報が提供されることになる．「リスク因子」はハザードとも呼ばれ，脅威とぜい弱性を組み合わせたものに相当する．リスク分析では，まずこのリスク因子を特定することになる．

続いて「リスク算定」が実施される．「リスク算定」は，特定されたリスク因子の発生可能性とそれにより引き起こされる事象の結果を検討することである．

なお，リスク分析には様々な手法がある．大きく分類すると，「定性的リスク分析」と「定量的リスク分析」の二つに分けられる．両者の大きな違いは，分析に数値を当てはめるか否かである．「定量的リスク分析」が数値を当てはめる方式であるが，リスク分析の要素（資産の価値，脅威，ぜい弱性）のすべてを数値にすることが極めて難しいとされている．

以下に，主なリスク分析の手法をあげる．

(1) ベースラインアプローチ

ベースラインアプローチは，一定の情報セキュリティ対策の最低限実施すべきこととなる基準（ベースライン）を策定し，一律にその基準を適用する方法である．ベースラインは，一般的には社内外の規定や標準，業界ルールなどを参考に作成することになる．

ベースラインアプローチは，資産の一つひとつについてリスク分析を実施しない．そのため，ある資産に対しては過剰なセキュリティ対策になる一方，別の資産に対しては不十分な対策となることもある．

その一方，詳細リスク分析手法と比較して，セキュリティ対策が短期間に決定，実施することができるというメリットがある．

(2) 詳細リスク分析

詳細リスク分析とは，資産について脅威及びぜい弱性を識別と評価し，個々の資産の脅威に対する対策を検討する方法である．次に，それぞれの脅威ぜい弱性の組合せが発生する可能性を検討し，リスクを評価する．

詳細リスク分析では，資産ごとのリスクに応じて，望ましい情報セキュリティ対策の選択

が可能となる．また，システムの変更などが生じても変更管理が容易となる．その反面，実施には手間と時間がかかるため，重要な資産についてのみ実施されることが多い．

(3) 非形式的アプローチ

非形式的アプローチとは，有識者などが個人の知見や過去の経験を踏まえてリスク分析をする方法である．詳細リスク分析より手間と時間をかけずに実施することができる．しかし，体系的，構造的な手法ではないため，重要な項目が漏れたり，評価者の主観がリスク分析の結果に入ることがある．そのため，リスク分析の結果を正当化するためには，リスク評価者自体の能力を評価し証明することが必要になることが多い．

(4) 組合せアプローチ

組合せアプローチとは，上記の三つの手法の問題点を踏まえたうえで，それぞれのリスク分析手法の長所と短所を考慮し，最適なリスク分析手法を採用する考え方である．基本的な情報セキュリティ対策についてはベースラインアプローチを採用し，識別された一部の重要なデータやシステムについては詳細リスク分析を実施する，というのが組合せアプローチである．

(5) スパニングツリー分析

この手法は，シナリオベースで故障や事象の見極め，リスクを分析する．代表的な手法として，以下のようなものがある．

- **FTA（Fault Tree Analysis）：**
  システムの特定故障を想定して，その発生原因を上位レベルから下位レベルまで論理的に展開し，最下位レベルのシステムの機能の故障発生率からシステムの特定故障の発生原因や発生確率を求める手法．
- **ETA（Event Tree Analysis）：**
  ある初期事象からスタートして，いろいろな経路をとることにより結果がどうなるかを明らかにする手法．

(6) ALE 法

米国標準技術院（NIST）が推奨する定量的リスクアセスメントの手法であり，年間の予想損失額 ALE（Annual Loss Exposure）を求める．年間損失予測（ALE）により，年間のセキュリティ予算を決定するための指標やセキュリティ対策の費用対効果を測定する指標となる．

$$ALE = F \times I$$

F：年間に損失が発生する予想頻度（ARO）
I：1 回あたりの予想損失額（SLE）

※1 年間発生頻度 （ARO：Annual Rate of Occurrence）
年間を通じて予期されるイベントの数．環境によって発生頻度も増減する．

※2 単一損失予測 （SLE：Single Loss Expectancy）
資産価値（¥）×顕在化（%）で求められる．実質的な損失だけではなく，それに関連して発生する損失，一次対応，再発防止費用なども検討する必要がある．

8-2-3 リスク評価

「リスク評価」は,「リスクの重大さを決定するために，算定されたリスクを与えられたリスク評価基準と比較するプロセス」とされている．なお，リスク評価基準は，関連するコストと利益，法規制の要求事項，社会への経済的な影響，ステークホルダーの関心事，優先度などを考慮し決定される．

8-2-4 リスク対応

「リスク対応」とは「リスクを変更させるための方策を選択及び実施するプロセス」としている．リスク分析の結果に基づき，対応策を選択し，実施することになる．

リスク対応には，以下のような四つがある．

表 8・5　リスク対応

資産区分	例　示
リスクの回避	リスクのある状況に巻き込まれないようにする意思決定，またはリスクのある状況から撤退する行為.
リスクの最適化（リスクの低減）	リスクに関連して，好ましくない結果及びその発生確率最小化し，かつ，好ましい結果及びその発生確率を最大化するプロセス（リスクに伴う発生確率もしくは好ましくない結果またはそれら両方を小さくするために取られる行為）.
リスクの移転	リスクに関して，損失の負担または利益の恩恵を他者と共有すること（リスクに関して，損失の負担を他者と共有すること）.
リスクの保有	あるリスクからの損失の負担または利得の恩恵の受容.

リスク対応後にまだ残っているリスクを「残留（残存）リスク」という．そして，この「残留リスク」が，組織が許容できる範囲にすることがリスク対応の基本的な考え方となる．

また，リスク対応で決定された内容は，情報セキュリティポリシーとして，方針，標準（スタンダード），手順（プロシージャー）などの文書として定められる．この情報セキュリティポリシーが，組織において遵守すべき規定（ルール）となる．

■3 群 － 7 編 － 8 章

8-3 情報セキュリティマネジメントシステム

（執筆者：長谷川長一）［2009 年 4 月 受領］

情報セキュリティマネジメントシステム（ISMS）とは，個別の問題ごとの技術対策のほかに，組織のマネジメントとして，自らのリスクアセスメントにより必要なセキュリティレベルを決め，プランをもち，資源配分して，システムを運用するためのフレームワークである．

そして，「組織が保護すべき情報資産について，機密性，完全性，可用性をバランス良く維持し改善することが情報セキュリティマネジメントシステム（ISMS）の基本コンセプト」である（ISO/IEC 13335-1:2004 より引用）．

情報セキュリティマネジメントシステム（ISMS）の要求事項を示した規格 ISO/IEC 27001 では，組織において ISMS を確立，導入，運用，監視，見直し，維持し，かつその ISMS の有効性を改善する際に，プロセスアプローチを採用することを奨励している．そして，この PDCA サイクルを継続的に繰り返し，情報セキュリティレベルの維持・向上を図る．

表 8･6　「ISMS プロセスに適用される PDCA モデルの概要」

～「ISMS ユーザーズガイド-リスクマネジメント編－財団法人日本情報処理開発協会（JIPDEC）」

Plan-計画 （ISMS の確立）	組織の全般的方針及び目的に従った結果を出すための，リスクマネジメント及び情報セキュリティの改善に関連した，ISMS 基本方針，目的，プロセス及び手順の確立.
Do-実行 （ISMS の導入及び運用）	ISMS 基本方針，管理策，プロセス及び手順の導入及び運用.
Check-点検 （ISMS の監視及びレビュー）	ISMS 基本方針，目的及び実際の経験に照らした，プロセスのパフォーマンスのアセスメント（適用可能ならば測定），及びその結果のための経営陣への報告.
Act-処置 （ISMS の維持及び改善）	ISMS の継続的な改善を達成するため，ISMS の内部監査及びマネジメントレビューの結果またはそのほかの関連情報に基づいた，是正処置及び予防処置の実施.

■3 群 － 7 編 － 8 章

8-4 情報セキュリティマネジメントの規格・基準・制度など

（執筆者：長谷川長一）［2009 年 4 月 受領］

情報セキュリティマネジメントには，様々な規格・基準・制度などがある．ここでは，それらの中の主なものを説明する．

8-4-1 OECD ガイドライン

OECD（経済開発協力機構）は，1960 年に設立されている．日本は 1964 年に加盟が承認された．

現在の「情報システム及びネットワークのセキュリティのためのガイドライン－セキュリティ文化の普及に向けて－」は，2002 年 7 月 25 日の第 1037 回会合で OECD 理事会の勧告として採択された．この新しいガイドラインでは，「セキュリティ文化」という概念を提唱し，情報システムやネットワークのすべての参加者が情報セキュリティに対する責任を負う，としている．

OECD が初めて「情報システムのセキュリティのためのガイドライン」を発表した 1992 年以来，情報システム及びネットワークの利用と情報技術をとりまく全体的な環境は，劇的に変化してきた．これらの継続的な変化は，大きな利益をもたらす一方，情報システム及びネットワークを開発，所有，提供，管理，サービス提供及び使用する政府，企業，そのほかの組織及び個人利用者（「参加者」）がセキュリティを一層重視することを要求している．

以下の九つの原則は互いに補い合うものであり，一体のものとして読まれるべきである．それらは，方針及び運用のレベルを含む，すべてのレベルで参加者に関係する．このガイドラインのもとで，参加者の責任は，彼らの役割に応じて変化する．すべての参加者は，セキュリティのより良い理解及び実践の採用を導き得るべく認識，教育，情報共有及び訓練によって助けられる．情報システム及びネットワークのセキュリティを強化させる努力は，民主主義社会の価値，特に情報の公開された，かつ自由な情報の流通の必要性及び個人のプライバシーに対する基本的な関心と合致すべきである，とされている．

表 8・7　「OECD 情報システムのセキュリティのためのガイドライン」

原　則	内　容
1) 認識（Awareness）	参加者は，情報システム及びネットワークのセキュリティの必要性並びにセキュリティを強化するために自分達にできることについて認識すべきである．
2) 責任（Responsibility）	すべての参加者は，情報システム及びネットワークのセキュリティに責任を負う．
3) 対応（Response）	参加者は，セキュリティの事件・事故に対する予防，検出及び対応のために，時宜を得たかつ協力的な方法で行動すべきである．
4) 倫理（Ethics）	参加者は，他者の正当な利益を尊重するべきである．
5) 民主主義（Democracy）	情報システム及びネットワークのセキュリティは，民主主義社会の本質的な価値に適合すべきである．

6) リスクアセスメント（Risk assessment）	参加者は，リスクアセスメントを行うべきである.
7) セキュリティの設計及び実装（Security design and implementation）	参加者は，情報システム及びネットワークの本質的な要素としてセキュリティを組み込むべきである.
8) セキュリティマネジメント（Security management）	参加者は，セキュリティマネジメントへの包括的アプローチを採用するべきである.
9) 再評価（Reassessment）	参加者は，情報システム及びネットワークのセキュリティのレビュー及び再評価を行い，セキュリティの方針，実践，手段及び手続に適切な修正をすべきである.

(1) 「OECD のプライバシーに関する 8 原則」1980 年，OECD

「OECD のプライバシーに関する 8 原則」は，国境を越えて個人情報がやりとりされる機会が増えた当時の情勢等を踏まえ，情報の自由な流通とプライバシー保護の調和を図るための国際標準を定めることを目的に策定された．この原則は，OECD 加盟国をはじめとする多くの国において法制度や規制に多くの影響を与えている．我が国においても，個人情報保護法やプライバシーマーク制度に，この八つ原則が反映されている．

表 8･8 「OECD のプライバシーに関する 8 原則」

原　則	内　容
収集制限の原則	個人データの収集には制限を設けるべきであり，いかなる個人データも，適法かつ公正な手段によって，かつ適当な場合には，データ主体に知らしめまたは同意を得たうえで，収集されるべきである.
データ内容の原則	個人データは，その利用目的に沿ったものであるべきであり，かつ利用目的に必要な範囲内で正確，完全であり最新なものに保たれなければならない.
目的明確化の原則	個人データの収集目的は，収集時よりも遅くない時点において明確化されなければならず，その後のデータの利用は，当該収集目的の達成または当該収集目的に矛盾しないでかつ，目的の変更ごとに明確化されたほかの目的の達成に限定されるべきである.
利用制限の原則	個人データは，第 9 条により明確化された目的以外の目的のために開示利用そのほかの使用に供されるべきではないが，次の場合はこの限りではない. (a) データ主体の同意がある場合，または， (b) 法律の規定による場合
安全保護の原則	個人データは，その紛失もしくは不当なアクセス，破壊，使用，修正，開示などの危険に対し，合理的な安全保護措置により保護されなければならない.
公開の原則	個人データにかかわる開発，運用及び政策については，一般的な公開の政策が取られなければならない．個人データの存在，性質及びその主要な利用目的とともにデータ管理者の識別，通常の住所をはっきりさせるための手段が容易に利用できなければならない.

個人参加の原則	個人は次の権利を有する． （a） データ管理者が自己に関するデータを有しているか否かについて，データ管理者またはそのほかの者から確認を得ること （b） 自己に関するデータを， （i）合理的な期間内に， （ii）もし必要なら，過度にならない費用で， （iii）合理的な方法で，かつ， （iv）自己に分かりやすいかたちで， 自己に知らしめられること． （c） 上記（a）及び（b）の要求が拒否された場合には，その理由が与えられること及びそのような拒否に対して異議を申し立てることができること． （d） 自己に関するデータに対して異議を申し立てること，及びその異議が認められた場合には，そのデータを消去，修正，完全化，補正させること．
責任の原則	データ管理者は，上記の諸原則を実施するための措置に従う責任を有する．

8-4-2 JIS Q 27000（ISO/IEC27000）シリーズ

JIS Q 27000 シリーズは，情報セキュリティマネジメントに関連する規格である．

1995 年に英国規格協会（BSI）が情報セキュリティマネジメントの規格（実践の規範）として BS7799 の Part1 を策定し，それをベースとして 2000 年に ISO/IEC17799:2000 が策定された．更に 2005 年にこの ISO/IEC17799:2000 が改訂され，それが翌 2006 年に JIS 化されたものが JIS Q 27002:2006 である．

また，英国規格協会（BSI）は，もう一つの情報セキュリティマネジメントの規格（情報セキュリティマネジメントシステムの要求事項）として，1998 年に BS7799 の Part2 を策定した．これをベースとして，2005 年には ISO/IEC27001:2005 が策定され，それが翌 2006 年に JIS 化されたものが JIS Q 27001:2006 である．

表 8・9 ISO/IEC27000 シリーズの概要

～「ISO/IEC27000 ファミリーについて」，JIPDEC，などをもとに作成

番 号	内 容
ISO/IEC 27000	概要及び用語 Overview and vocabulary
ISO/IEC 27001	情報セキュリティマネジメントシステムの要求事項 ISMS requirement
ISO/IEC 27002	情報セキュリティマネジメントの実践のための規範 Information security management Code of Practice
ISO/IEC 27003	情報セキュリティマネジメント導入に関する手引き（作成中） ISMS Implementation guide
ISO/IEC 27004	情報セキュリティマネジメントの測定 ISM Measurements

ISO/IEC 27005	情報セキュリティリスクマネジメントに関する指針 ISMS Risk management
ISO/IEC 27006	認証機関に対する要求事項 Accreditation requirements for certification bodies
ISO/IEC 27007	監査の指針（作成中） ISMS Audit guidelines
ISO/IEC 27008	ISMS 管理策に関する監査員のための指針（作成中） Guidance on auditing ISMS controls
ISO/IEC 27010	業界間コミュニケーションのための情報セキュリティマネジメント（予定） Sector to sector interworking and communications for industry and government
ISO/IEC 27011	電気通信組織のための指針 Information security management guidelines for telecommunications based on ISO/IEC 27002
ISO/IEC 27012	電子政府サービスのための ISMS 指針（中止） ISMS guidelines for e-government
ISO/IEC 27013	ISO/IEC20000-1 と ISO/IEC27001 との統合導入についての手引き（予定） ISMS for service management
ISO/IEC 27014	情報セキュリティガバナンスフレームワーク（予定） Information security governance framework
ISO/IEC 27015	金融及び保険サービスに対する情報セキュリティマネジメントガイドライン（予定） ISMS for the financial and insurance sector
ISO/IEC 27031	ビジネス継続のための ICT 準備技術（予定） ICT readiness for business continuity
ISO/IEC 27032	サイバーセキュリティ（予定） Cyber security
ISO/IEC 27033	ネットワークセキュリティ（予定） Network security
ISO/IEC 27034	アプリケーションセキュリティの指針（予定） Guidelines for application security
ISO/IEC 27035	情報セキュリティインシデントマネジメント（予定） Information security incident management
ISO/IEC 27036	セキュリティのアウトソーシングのためのガイドライン（予定） Guidelines for security of outsourcing
ISO/IEC 27037	デジタルエビデンス（証拠）の識別，収集，及び／または取得，保存のためのガイドライン（予定） Guidelines for identification, collection and/or acquisition and preservation of digital evidence

「JIS Q 27001:2006（ISO/IEC27001:2005）情報技術－情報セキュリティ技術－情報セキュリティマネジメントシステム－要求事項」は，情報セキュリティマネジメントシステムを確立，導入，運用，監視，レビュー，維持及び改善するためのモデルを提供している．

表 8・10

章	内　容
情報セキュリティマネジメントシステム	一般要求事項，ISMS の確立及び運営管理，文書化の関する要求事項
経営陣の責任	経営陣のコミットメント，経営資源の提供
ISMS 内部監査	－
ISMS のマネジメントレビュー	一般，レビューへのインプット，レビューからのアウトプット
ISMS の改善	継続的改善，是正処置，予防処置

「JIS Q 27002:2006（ISO/IEC17799:2005）情報技術－情報セキュリティ技術－情報セキュリティマネジメントシステムの実践のための規範」は，情報セキュリティマネジメントシステムの実践のための規範として，管理目的及び管理策を最適な実施慣行（ベストプラクティス）として示している．

表 8・11

分　野	管理策
セキュリティ基本方針	情報セキュリティ基本方針
情報セキュリティのための組織	内部組織，外部組織
資産の管理	資産に対する責任，情報の分類
人的資源のセキュリティ	雇用前，雇用期間中，雇用の終了または変更
物理的及び環境的セキュリティ	セキュリティを保つべき領域，装置のセキュリティ
通信及び運用管理	運用の手順及び責任，第三者が提供するサービスの管理，システムの計画作成及び受け入れ，悪意のあるコード及びモバイルコードからの保護，バックアップ，ネットワークセキュリティ管理，媒体の取扱い，情報の交換，電子商取引サービス，監視
アクセス制御	アクセス制御に対する業務上の要求事項，利用者アクセスの管理，利用者の責任，ネットワークのアクセス制御，オペレーティングシステムのアクセス制御，業務用ソフトウェア及び情報のアクセス制御，モバイルコンピューティング及びテレワーキング
情報システムの取得，開発及び保守	情報システムのセキュリティ要求事項，業務用ソフトウェアでの正確な処理，暗号による管理策，システムファイルのセキュリティ，開発及びサポートプロセスにおけるセキュリティ，技術的ぜい弱性管理
情報セキュリティインシデントの管理	情報セキュリティの事象及び弱点の報告，情報セキュリティインシデントの管理及びその改善

事業継続管理	事業継続管理における情報セキュリティの側面
順　守	法的要求事項の順守，セキュリティ方針及び標準の順守並びに技術的順守，情報システムの監査に対する考慮事項

8-4-3 ISMS 適合性評価制度

ISMS（Information Security Management System）適合性評価制度は，財団法人 日本情報処理開発協会（JIPDEC）が運営する ISO 国際規格（ISO/IEC 27001）に準拠している情報セキュリティマネジメントに対する第三者適合性評価制度である．

ISMS 適合性評価制度は，日本の情報セキュリティレベル全体の向上に貢献するとともに，諸外国からも信頼を得られる情報セキュリティレベルを達成することを目的としている．

JIPDEC は，ISMS を「個別の問題ごとの技術対策のほかに，組織のマネジメントとして，自らのリスクアセスメントにより必要なセキュリティレベルを決め，プランをもち，資源配分して，システムを運用すること」と定義している．

以前には，「情報システム安全対策実施事業所認定制度」（1981 年 7 月 20 日通商産業省告示 342 号．以下，安対制度と表記）と呼ばれる制度があった．この制度は，情報システムの施設・設備などの物理的対策に重点が置かれた制度であった．組織のセキュリティ対策として物理的対策や技術的対策のみならず，人的セキュリティ対策を含む組織全体の総合的なセキュリティ対策のニーズが広がった結果，経済産業省では，2000 年 7 月 31 日に「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事業所認定制度の改革」を公表し，ISMS 適合性評価制度を創設して，従来の安対制度を廃止することを決定した．

ISMS 適合性評価制度は，JIPDEC による 2001 年度事業として，対象範囲を主に情報技術分野でパイロット事業として開始された．2002 年 4 月の本格運用からは，すべての業種，業務分野を対象範囲としている．なお，適用する業種・業務分野は ISO 9000s や ISO 14000s との整合性を確保するために，「経済活動に関する統計的分類基準」（NACE Rev.1）に基づく業種分類が適用されている．

(1)　JIS Q 13335（ISO/IEC13335）

「JIS Q 13335-1:2006（ISO/IEC13335-1:2004）情報技術－情報セキュリティ技術－情報通信技術セキュリティマネジメント－第 1 部：情報通信技術セキュリティマネジメントの概念及びモデル」は，IT セキュリティマネジメントやセーフガードの選択などについて記述されたガイドラインである．このガイドラインは，通称 MICTS（management of ICT security）と呼ばれ，IT セキュリティにおけるリスクアセスメントの手法として広く参照されている（MICTS は，以前は GMITS : Guidelines for the Management for IT Security，と呼ばれていた）．

8-4-4 JIQ Q 2001

「JIS Q 2001:2001 リスクマネジメントシステム構築のための指針」は，組織がリスクマネジメントの導入及び定着化を図っていくための枠組み（リスクマネジメントシステム）を提供するものです．そして，組織にかかわる様々なリスクに共通するリスクマネジメントシステム構築のための原則や諸要素を提供している．

表 8・12　リスクマネジメントのための原則及び要素

項　目	内　容
一般原則	-
リスクマネジメントシステム構築及び維持のための体制	組織の最高責任者の役割，リスクマネジメントシステム担当者の役割，
リスクマネジメント方針	リスクマネジメント方針の表明，リスクマネジメント行動方針，リスクマネジメント基本目的の設定
リスクマネジメントに関する計画策定	リスク分析，リスク評価，リスクマネジメントの目標，リスク対策の選択，リスクマネジメントプログラムの策定
リスクマネジメントの実施	リスクマネジメントプログラムの実施，緊急時に特徴的な追加事項，復旧に特徴的な追加事項，運用管理
リスクマネジメントパフォーマンス評価及びリスクマネジメントシステムの有効性評価	リスクマネジメントパフォーマンス評価，リスクマネジメントシステムの有効性評価
リスクマネジメントシステムに関する是正・改善の実施	リスクマネジメントシステムに関する是正・改善の継続的実施，実施の確認
リスクマネジメントシステム維持のための仕組み	能力・教育・訓練，シミュレーション，リスクコミュニケーション，リスクマネジメント文書の作成，文書管理，発見したリスクの監視，記録の維持管理，リスクマネジメントシステム監査
組織の最高責任者によるレビュー	-

また，リスクマネジメントに関する基本的な 29 の用語については，ISO/IEC ガイド 73:2002（TR Q 0008:2003）「リスクマネジメント－用語－規格において使用するための指針」に定義されている．

※TR（Technical Report）：ISO/IEC の技術報告書．

なお，リスクマネジメントの新たな規格として，「ISO31000:2009 リスクマネジメント－原則及び指針－Risk management－Principles and guilines」が，2009 年 11 月に発行されている．

8-4-5 JIS Q 15001

「JIS Q 15001:2006（個人情報保護マネジメントシステム－要求事項）」は，個人情報保護にかかわる枠組みを提供している．

JIS Q 15001:2006 では，表のような要求事項がある．

表 8・13 JIS Q 15001:2006 要求事項

要求事項	内　容
個人情報保護方針	-
計　画	個人情報の特定，法令・国が定める指針そのほかの規範，リスクなどの認識・分析及び対策，資源・役割・責任及び権限，内部規定，計画書，緊急事態への準備
実施及び運用	運用手順，取得・利用，適正管理，教育
苦情及び相談への対応	-
点　検	運用の確認，監査
是正処置及び予防処置	-
事業者の代表者による見直し	-

プライバシーマーク制度とは，事業者の保有するすべての個人情報が，適切な保護体制の下に収集・管理されているかについて，財団法人 日本情報処理開発協会（JIPDEC）またはその指定機関が JIS Q 15001（個人情報保護に関するコンプライアンス・プログラムの要求事項）に基づいて審査して，JIPDEC が認定する制度である．認定された事業者には，その旨を示すマークとしてプライバシーマークが付与され，事業活動に際してそのマークをパンフレットやウェブサイトなどに使用することができ，個人情報の適切な取り扱いを社会に示すことができる．

この制度の認定期間は 2 年間で，2 年ごとに更新審査が行われるほか，認定後であっても勧告や取り消しなどの措置がある．

1999 年に制定された JIS Q 15001 は，2006 年 5 月に JIS Q15001:2006（個人情報保護マネジメントシステム要求事項）として改正されました．また，要求事項を正しく反映した個人情報保護マネジメントシステムを効率的に構築及び運用できるようにするために，2006 年 9 月に「JISQ15001：2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン−第 1 版−」が JIPDEC より公表された．

8-4-6 情報セキュリティ監査基準／管理基準

情報セキュリティ監査制度は，2003 年に創設された．情報セキュリティ監査とは「情報セキュリティに係るリスクのマネジメントが効果的に実施されるように，リスクアセスメントに基づく適切なコントロールの整備，運用状況を，情報セキュリティ監査を行う主体が独立かつ専門的な立場から，国際的にも整合性のとれた基準に従って検証または評価し，もって保証を与えあるいは助言を行う活動」と定義されている．

この定義からも分かるとおり，情報セキュリティ監査には「助言型監査」と「保証型監査」，さらに「合意された手続による監査」という方式がある．

この制度では，監査業務を実施するのに欠かせない「情報セキュリティ監査基準」と「情報セキュリティ管理基準」の二つの基準がある．

「情報セキュリティ監査基準」は，情報セキュリティ監査における監査人の行為規範となるものである．情報セキュリティ監査業務の品質を確保し，有効かつ効率的に監査を実施す

ることを目的としている．「情報セキュリティ監査基準」は，監査人としての適格性及び監査業務上の遵守事項を規定する「一般基準」，監査計画の立案及び監査手続の適用方法を中心に監査実施上の枠組みを規定する「実施基準」，監査報告に係る留意事項と監査報告書の記載方式を規定する「報告基準」からなっている．

「情報セキュリティ管理基準」は，情報セキュリティ監査において，被監査主体における情報セキュリティマネジメントの体制やコントロールの整備，監査主体における実際の監査項目（判断の尺度）となるものである．2008 年に平成 20 年度改正版に改訂され，その際に「マネジメント基準」18 項目，「管理策基準」133 項目という構成になった．「マネジメント基準」「管理策基準」は更に細分化され，「作業項目」63 項目，「詳細管理策」1153 項目という構成になっている．

表 8・14

	社会的合意方式	利用者合意方式	被監査主体合意方式
監査手続の十分性の担保	社会的に合意された基準に照らして十分な監査手続であるとの監査人の判断	監査目的に照らした監査手続の十分性について利用者の合意が存在	監査目的に応じた手続として監査主体と被監査主体が合意し 1 次利用者の確認がある
実施する監査手続	監査人が必要と考える手続	1 次利用者と合意した，期待にこたえられる監査手続	被監査主体と合意し利用者の確認を得た監査手続
保証の内容	設計監査または実装監査	設計監査または実装監査	実装監査
保証の方法	意見表明方式	意見表明方式	結果報告方式
保証の対象	言明方式	言明方式	非言明方式
保証の対象とする期間	時点監査（期間監査も条件を満たせば可能）	時点監査（期間監査も条件を満たせば可能）	時点監査または期間監査
監査の対象範囲	監査の主題にかかわる重要部分を欠いていないこと	監査の主題にかかわる重要部分を欠いていないこと	被監査主体と合意し利用者の確認を得た部分
監査報告書の利用者	不特定	特定された 1 次利用者に限定	特定された 1 次利用者に限定
報告書記載	信じるに足る	期待する水準にある	結果を報告する
適用可能な具体例	委託先の監査結果を広く利害関係者に公表したい場合	報告書利用者である委託者が委託先に期待する水準が明確な場合で，委託先がその期待に応えていることについて保証を得たい場合	受託者として求められる事項の遵守について保証を得たい場合

「情報セキュリティ監査」と類似するものに「システム監査」がある．システム監査は，情報システムを対象範囲としており，ライフサイクルに従った情報システム戦略及び計画，

設計，運用，保守といった一連のプロセスを監査するものである．その目的は「組織体の情報システムにまつわるリスクに対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを，独立かつ専門的な立場のシステム監査人が検証または評価することによって，保証を与えあるいは助言を行い，もって IT ガバナンスの実現に寄与すること」（「システム監査基準」）とされている．

システム監査の対象は「情報システム」であるのに対し，情報セキュリティ監査の対象は，情報資産に係る「情報セキュリティ」であるという点が大きく異なる．すなわち，システム監査は情報システムの全体最適化（情報セキュリティの側面を含んだ信頼性，安全性，及び効率性）を目的に行うものである．対して，情報セキュリティ監査は情報システム以外の部分も対象として情報セキュリティ確保のためのマネジメントが効果的に行われることを目的として行う監査である．

システム監査と情報セキュリティ監査は，目的と成り立ちが異なるため，被監査主体のニーズや要請に応じて適切に選択されるべきものである．

■3 群 － 7 編 － 8 章

8-5 そのほかの情報セキュリティマネジメントに関連する規格・基準・制度など

（執筆者：長谷川長一）［2009 年 4 月 受領］

ここでは，情報セキュリティマネジメントの規格・基準・制度などではないが，関連する主なものを説明する．

8-5-1 ISO/IEC20000（JIS Q 20000）IT サービスマネジメント

1989 年に英国政府が ITIL を IT サービスマネジメントプロセスのベストプラクティスとして発表し，英国規格協会が 2000 年に英国規格 BS15000 を制定した．2004 年に国際規格の手続きがなされ，2005 年 12 月に ISO/IEC20000 が制定された．日本では，2007 年 4 月 20 日に JIS Q20000 として，制定された．

ISO/IEC20000 シリーズは，ISO/IEC JTC1（情報技術）の分科会 SC27（セキュリティ技術）において，ISO/IEC 27013 として，ISO/IEC 20000-1 と ISO/IEC27001 との統合導入が提案されているなど，ISO/IEC27000 シリーズと密接な関係をもつ規格である．

JIS Q20000 は，以下の 2 部構成となっている．

・JIS Q20000-1（第 1 部 仕様）

事業上の要求事項及び顧客要求事項を満たす，管理されたサービスを効果的に提供するため，統合されたプロセスアプローチの採択を促進するものであり，顧客に受け入れられる品質の管理されたサービスを提供するため，サービス提供者に対する要求事項を規定しており，認証の基準ともなるものである．

・JIS Q20000-2（第 2 部 実践のための規範）

実践のための規範として，手引き及び推奨のかたちをとり，要求事項に沿ったかたちで IT サービスマネジメントプロセス運営に対する推奨事項を記載したものである．

表 8・15 JIS Q 20000 の概要

章	内 容
1.適用範囲	本規格の目的及び用途について，記述している．
2.用語及び定義	本規格で用いる用語及び定義について説明している．
3.マネジメントシステム要求事項	ITSMS を支えるための要素（経営陣の責任，文書化，教育・訓練など）について，規定している．
4.サービスマネジメントの計画立案及び導入	ITSMS が備えるべき機能／活動について，PDCA サイクルについて規定している．
5.新規サービスまたはサービス変更の計画立案及び導入	新規／変更のサービスを提供する場合に対応すべき事項について規定している．
6.サービス提供のプロセス	ITIL のサービス提供に相当するプロセスに加えて，情報セキュリティ管理について規定している．
7.関係プロセス	顧客関係管理と供給者管理の側面を扱っている．
8.解決プロセス	インシデント管理と問題管理について，規定している．

9.統合的制御プロセス	構成管理と変更管理について，規定している.
10.リリースプロセス	リリース管理について，規定している.

（～「ITSMS ユーザーズガイド」，JIPDEC より）

8-5-2 BS25999 事業継続マネジメント

「BS25999」は，英国における事業継続マネジメントの標準規格である.「事業継続マネジメント（BCM; Business Continuity Management）」は，BCI（Business Continuity Institute）では「組織を脅かす潜在的なインパクトを認識し，利害関係者の利益，名声，ブランド及び価値創造活動を守ることを目的とし，復旧力及び対応力を構築するための有効な対応を行うフレームワーク，包括的なマネジメントプロセス」と定義されている．また，BCM で策定される「事業継続計画（BCP; Business Continuity Plan）」は，「組織が重要な製品やサービスを供給できるよう，事故時の使用に備えて開発，維持され文書化された一連の手順や情報」と定義されている.

BS25999 発行までの経緯は，以下のとおりである.

・2002 年：BCI が「Good Practice Guideline（実践的なガイドライン）」を発行.
・2003 年：英国規格協会（BSI）が，「Good Practice Guideline（実践的なガイドライン）」をベースに PAS56 を発行.
・2006 年 6～8 月：英国規格協会（BSI）が，BS25999-1 のドラフト版を作成.
・2006 年 6～8 月：英国規格協会（BSI）から，BS25999-1 が正式発行.
・2007 年 11 月：英国規格協会（BSI）から，BS25999-2 が発行.

BS25999 は，Part1，2 の 2 部構成となっており，それぞれ以下のような内容になっている.

表 8・16 BS25999-1 の（事業継続管理-実践規範）構成

章	内　容
1.適用範囲及び適用性	BS25999-1 の目的
2.用語及び定義	BCP，BCM，リスクマネジメントなどの定義
3.事業継続管理（BCM）の概要	BCM と組織戦略の関係，リスクマネジメントの関係，BCM のライフサイクル
4.事業継続管理方針	BCM にかかわる文書の構成
5.BCM プログラムマネジメント	BCM の維持管理，責任の明確化，利害関係者との関係
6.組織の理解	事業影響度分析（BIA），重要な機能，リスク評価
7.事業継続戦略の決定	戦略的オプション（キーパーソン，拠点，技術，情報，利害関係者など）
8.BCM を実現する手法の開発と実装	組織体制，BCP の策定
9.BCM への取組みに関する訓練，維持管理，レビュー	訓練，維持管理，経営陣による見直し
10.BCM の組織文化への導入	意識向上，要員のスキルの向上

表 8・17 BS25999-2（事業継続管理-仕様）の構成

章	内 容
1.適用範囲	－
2.用語及び定義	
3.事業継続マネジメントシステム（BCMS）の計画	BCMS の確立及び管理，BCM の組織文化への導入, BCMS 文書及び記録
4.BCMS の導入及び運用	組織の理解，事業継続戦略の決定，BCM 対応の開発と実装，BCM アレンジメントの訓練・維持・レビュー
5.BCMS のモニタリング及びレビュー	内部監査，BCMS のマネジメントレビュー
6.BCMS の維持及び改善	是正及び予防措置，継続的改善

BCMS 適合性評価制度は，2008 年度には，JIPDEC によってパイロット運用が開始されている．2010 年 4 月より，本運用が開始されており，また，近年中には ISO/IEC 化，JIS 化されるであろうと予測されている．

■参考文献

1) 経済産業省，“OECD 情報システムのセキュリティのためのガイドライン”
http://www.meti.go.jp/policy/netsecurity/OECD020917set.htm
2) OECD，“OECD のプライバシーに関する 8 原則，”1980.
http://www.mofa.go.jp/mofaj/gaiko/oecd/privacy.htm
3) 日本規格協会，“JIS Q 27001:2006（ISO/IEC27001:2005）情報技術-情報セキュリティ技術－情報セキュリティマネジメントシステム－要求事項”
4) 日本規格協会，“JIS Q 27002:2006（ISO/IEC17799:2005）情報技術－情報セキュリティ技術－情報セキュリティマネジメントシステムの実践のための規範”
5) 日本規格協会，“JIS Q 13335-1:2006（ISO/IEC13335-1:2004）情報技術－情報セキュリティ技術－情報通信技術セキュリティマネジメント－第 1 部：情報通信技術セキュリティマネジメントの概念及びモデル”
6) 日本規格協会，“JIS Q 2001:2001 リスクマネジメントシステム構築のための指針”
7) 日本規格協会，“JIS Q 15001:2006（個人情報保護マネジメントシステム－要求事項)”
8) 日本規格協会，“JIS Q 20000-1:2007 情報技術－サービスマネジメント－第 1 部：仕様”
9) 日本規格協会，“JIS Q 20000-1:2007 情報技術－サービスマネジメント－第 2 部：実践のための規範”
10) JIPDEC，“ISMS 適合性評価制度”
http://www.isms.jipdec.jp/isms.html
11) JIPDEC，“プライバシーマーク制度”
http://privacymark.jp/
12) 経済産業省，“システム監査基準”
http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm
13) 経済産業省，“情報セキュリティ監査制度”
http://www.meti.go.jp/policy/netsecurity/audit.htm
14) 経済産業省，“ソフトウェア等ぜい弱性関連情報取扱基準”
http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html
http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm
15) JIPDEC，“ITSMS 適合性評価制度”
http://www.isms.jipdec.jp/itsms.html