ＩＳＭＳユーザーズガイド

-JIS Q 27001:2014(ISO/IEC 27001:2013) 対応

ISMS:　Information Security Management System
情報セキュリティマネジメントシステム

平成 26 年 4 月 14 日

JIPDEC

一般財団法人　日本情報経済社会推進協会

はじめに

我が国における情報セキュリティマネジメントシステム（ISMS）適合性評価制度は、2002 年 4 月より本格運用を開始しました。本制度は、我が国の情報セキュリティ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レベルの情報セキュリティを達成し、維持することを目的としています。

本制度に適用される認証基準は、JIS Q 27001:2014 です。このたび、従来の認証基準である JIS Q 27001:2006 から JIS Q 27001:2014 への移行に伴い、2008 年に発行した ISMS ユーザーズガイドの改訂版（以下、本ガイドという。）を改訂いたしました。本ガイドでは、JIS Q 27001:2014 の要求事項について一定の範囲でその意味するところを説明していますが、必ずしも網羅されている訳ではありません。なお、JIS Q 27001:2014 の附属書 A（規定）「管理目的及び管理策」の詳細は、管理策の指針である JIS Q 27002:2014 を参照して下さい。

本ガイドの主な読者として想定しているのは、ISMS 認証取得を検討若しくは着手している組織において、実際に ISMS の構築に携っている方及びその責任者です。本ガイドでは、JIS Q 27001:2014 に記述された主要な条項を紹介し、要求する内容、要求の意図、コンセプトなどについて解説しています。JIS Q 27001:2014 の全てが網羅されている訳ではありませんが、できるだけ丁寧な解説を試みました。特に、序文において、JIS Q 27001:2014 の国際規格 ISO/IEC 27001:2013 の改訂の概要や理解のポイントなどについて説明しております。本ガイドが JIS Q 27001:2014 を理解する上での一助となり、ISMS を構築・運用する上で参考になる事を期待しています。

改訂された認証基準である JIS Q 27001:2014 の有効活用は、ISMS 認証の分野拡大を進めるだけでなく、他のマネジメントシステムとの統合化を図り、ISMS を構築する組織の経営のツールとして確立させることができ、ISMS 認証の付加価値をさらに向上させていくものとして期待されています。

本ガイドの作成にあたり、ISMS 適合性評価制度運営委員会の委員の皆様をはじめご協力頂いた関係各位に対し厚く御礼申し上げます。

2014 年 4 月

ISMS 適合性評価制度技術専門部会
一般財団法人日本情報経済社会推進協会

目　　次

はじめに
０．序文 1
１．適用範囲 15
２．引用規格 17
３．用語及び定義 21
４．組織の状況 27
５．リーダーシップ 35
６．計画 42
７．支援 61
８．運用 69
９．パフォーマンス評価 73
１０．改善 87
附属書 A（規定）　管理目的及び管理策 91
付録１　ISMS 構築・運用とコーポレートガバナンス（参考） ... 93
付録２　情報セキュリティリスクアセスメント（事例） 96
参考文献 114

注記 1：
本文中の規格文書の引用について、実線の枠は JIS Q 27001:2014 からの引用であることを示し、点線の枠はその他の規格、参考文献からの引用であることを示していることにご留意下さい。

注記 2：
これまでのガイドでは、ISMS 認証基準という用語を使用しておりましたが、本ガイドでは JIS Q 27001:2014 と表現しています。

０．序文

０．１ 国際規格（ISO/IEC 27001）改訂の意義

情報セキュリティマネジメントの国際規格を制定している ISO（国際標準化会議）と IEC（国際電気標準会議）が設置する合同専門委員会 ISO/IEC JTC1/SC27（情報技術の委員会・分化委員会・情報セキュリティ）では、ISMS 認証の国際規格として ISO/IEC 27001 を発行しています。第１版の ISO/IEC 27001 は 2005 年に発行され、その後、2008 年 10 月に ISO による定期見直しが開始されました。

その一方で、マネジメントシステム規格（MSS: Management System Standard）間の整合化を図るために、ISO においてマネジメントシステムの上位構造（High Level Structure）、共通テキスト（Identical Core Text）及び共通用語・定義が開発されたことにより、ISO/IEC 27001 においてもこれらに基づいて改訂作業が進められることになりました（本ガイドでは、このマネジメントシステム規格に共通の上位構造、共通テキスト、及び共通用語・定義を、ISO MSS 共通要素と呼びます）。
その結果、2013 年 10 月 1 日に MSS の上位構造、共通テキスト、共通用語・定義を適用した ISO/IEC 27001:2013 が発行されました。

MSS の共通テキストは、組織が複数のマネジメントシステムを導入することを考慮して、マネジメントシステム間の整合性を図り、組織の負担を軽減することを目的にしております。その結果、組織のマネジメントシステムの統合的な構築・運用がスムーズにできるよう配慮されています。特に、2 つ以上のマネジメントシステム規格に基づいたマネジメントシステムを 1 つのマネジメントシステムとして構築・運用する組織にとっては有効であり、統合されたマネジメントシステムを効率よく構築することが可能となりました。

ISO/IEC 27001:2013 は、ISO MSS の共通要素を取り込んだマネジメントシステム規格となっているので、効果的に組織のマネジメントシステムを構築・運用することが可能となります。ISO/IEC 27001:2013 の構成（本ガイドの 0.3.3 参照）には、ISO MSS 共通の上位構造（構成）、共通テキストが適用されているため、組織が運用する他のマネジメントシステムとの親和性も高まり、ISMS 導入の一層の効果が期待できます。なお、ISO MSS の共通要素の詳細は、本ガイドの「0.2.3　ISO MSS 共通要素の概要」で説明します。

また、既に ISMS 認証を取得されている組織は、現在の仕組みを大幅に変更することはありませんが、従前に比べ計画段階における経営的な視点での見直しが必要となります。例えば、組織の状況を理解するために外部及び内部の課題を特定しなければなりません。また、トップマネジメントは、組織の戦略的な方向性を確実にするとともに、リーダーシップとコミットメントを明示する必要があり、その責任に重点が置かれるようになっています。新規に ISMS 認証の取得を目指している組織は、従前のマネジメントシステムに比べて経営的要素が加味された仕組みを構築することができます。その結果、組織のガバナンスを強化できるので、組織のマネジメントシステムを見直し、改善する良い機会となります。

０．２　国際規格（ISO/IEC 27001）改訂の概要

０．２．１　規格改訂の経緯

本ガイドの 0.1 に記載のとおり、ISO は、2013 年 10 月 1 日に国際規格 ISO/IEC 27001:2013（第 2 版）を発行しました。ISO/IEC 27001:2013 の検討は、第 1 版の ISO/IEC 27001:2005 に対する 5 年ごとの国際規格見直し作業として開始され、リスクマネジメントの国際規格である ISO 31000:2009（JIS Q 31000:2010）との整合を図るとともに、ISO

MSS（Management System Standard）共通要素を取り込んだマネジメントシステム規格として、制定されました。

また、並行して見直し作業が進められていた ISO/IEC 27002:2005 も、ISO/IEC 27001:2013 と同時に、ISO/IEC 27002:2013 として発行されました。
ISO/IEC 27001 及び ISO/IEC 27002 の用語定義については、ISO/IEC 27000 に記載することとなり、これを受けて ISO/IEC 27000:2014 が 2014 年 1 月に発行されました。各国際規格の改訂作業の経緯は、図 0-1 に示す通りです。

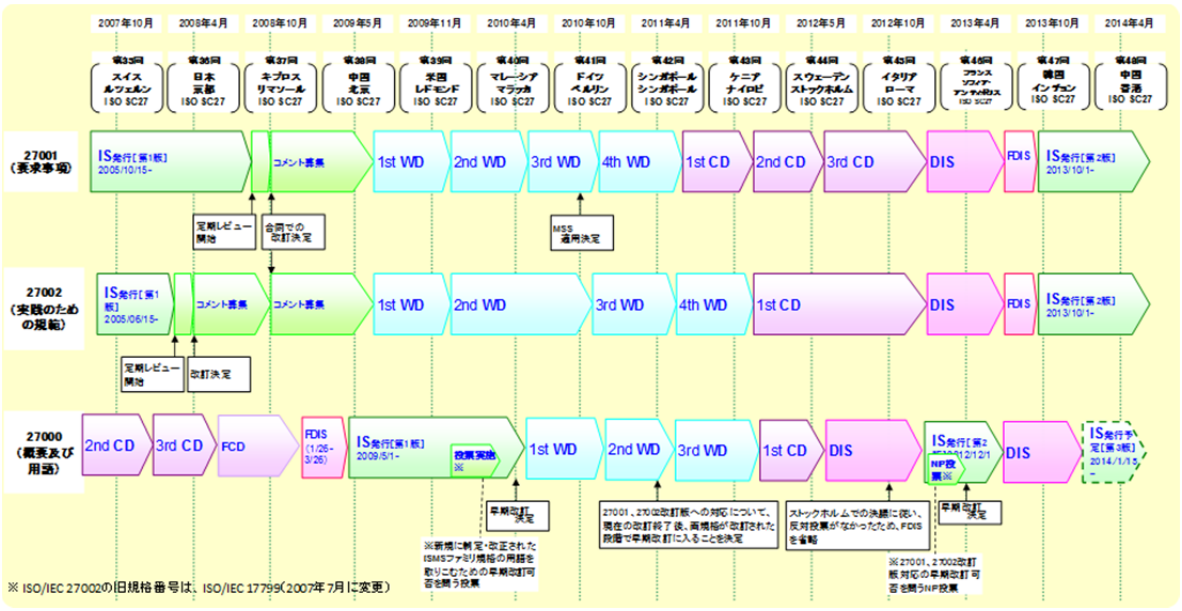


図 0-1　各国際規格の改訂作業の経緯

- ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements（JIS Q 27001:2014 情報技術―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、組織が情報セキュリティマネジメントシステム（ISMS）を確立し、実施し、維持し、継続的に改善するための要求事項をまとめた国際規格です。ISMS が、リスクマネジメントプロセスを適用することによって情報の機密性、完全性及び可用性を保護し、かつ、リスクを適切に管理しているという信頼を利害関係者に与えることを意図しています。

- ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls（JIS Q 27002:2014 情報技術―情報セキュリティ管理策の実践のための規範）は、組織が、ISO/IEC 27001 に基づく ISMS を実施するプロセスにおいて、管理策を選定するための参考として用いる、又は一般に受け入れられている情報セキュリティ管理策を実施するための手引・規範（ベストプラクティス－最良の慣行）をまとめた国際規格です。また、この規格は、それぞれに固有の情報セキュリティリスクの環境を考慮に入れて、業界及び組織に固有の情報セキュリティマネジメントの指針を作成する場合に用いることを意図しています。

- ISO/IEC 27000:2014 Information technology - Security techniques-Information security management systems-Overview and vocabulary（JIS Q 27000:2014 情報技術－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－用語）は、ISMS の概要等について記載し、関連する用語及び定義について規定しています。

JIS Q 27000:2014 は、ISO/IEC 27000:2014 の用語及び定義部分について技術的内容を変更することなく国内規格化したものです。

なお、JIS Q 27001 は、ISO/IEC 27001 の制定発行に伴って、日本工業標準調査会（JISC）により日本工業規格（JIS）として制定された国内規格です。内容は、ISO/IEC 27001 を忠実に日本語に翻訳し、国際規格との整合性が厳密に保たれたものになっています。
同様に、JIS Q 27002、JIS Q 27000 も、ISO/IEC 27002、ISO/IEC 27000 との整合性が厳密に保たれています。

JIS Q 27000（ISO/IEC 27000）は用語及び定義を規定していること、また JIS Q 27002（ISO/IEC 27002）は附属書 A の管理策についての指針を提供していることから、本ガイドでは、この両規格を参照しながら JIS Q 27001（ISO/IEC 27001）に記述された重要な条項などを紹介し、ISMS の構築・運用に役立つ情報を提供することを目的とします。

０．２．２　国際規格（ISO/IEC 27001）理解のポイント

ISO/IEC 27001:2013 は、ISO MSS 共通要素を適用したタイプ A のマネジメントシステム規格（要求事項を提供する MSS）となっています。ISO/IEC 27001:2013 のリスクアセスメント及びリスク対応のプロセスは、ISO 31000:2009（JIS Q 31000:2010）との整合を考慮しています（ISO MSS 共通要素、タイプ A 等の詳細は、本ガイドの 0.2.3 参照）。

ISO/IEC 27001:2013 は、基本的には ISO/IEC 27001:2005 の要求事項（本文）及び附属書 A（規定）を継承した要求事項となっています。附属書 A は、ISO/IEC 27002:2013 の要求事項を満足させる管理策を提供していますが、ISO/IEC 27002:2013 以外からの管理策群の導入も許容しています。

ISO/IEC 27001:2013 の理解のポイントを、主に従来の ISO/IEC 27001:2005 を参照しながら説明します。

（注記）ISO MSS 共通要素については、「ISO/IEC 専門業務用指針 第 1 部 統合版 ISO 補足指針」の「附属書 SL（規定）マネジメントシステム規格の提案」の「Appendix 2（規定）上位構造、共通の中核となるテキスト、共通用語及び中核となる定義」に規定されています。詳細は、本ガイドの 0.2.3 を参照して下さい。

● ISO MSS 共通テキストの適用
本ガイドの 0.1 でも触れましたが、今回の大きな改訂のポイントの 1 つは、ISO MSS 共通テキストを適用したことです。ISO/IEC 27001:2013 は、ISO MSS 共通要素を適用して開発されたマネジメントシステム規格となっており、その上で、情報セキュリティに不可欠な ISMS 固有の要求事項が規定されています。

ISO/IEC 27001:2013 の構成は、前規格である ISO/IEC 27001:2005 のマネジメントシステムの仕組みを大幅に変更することはありませんが、計画段階における組織の状況については、経営的な視点での見直しが必要となります。これは、情報セキュリティ方針及び情報セキュリティ目的を確立し、それらが組織の戦略的な方向性と両立することを確実にしなければならない主旨の要求事項が追加されたためです。
図 0-2 に示す通り、ISO/IEC 27001:2013 の構成は、MSS 共通要素と整合がとられています。

図 0-2 では、要求事項の構成について、ISO/IEC 27001:2013 と ISO/IEC 27001:2005 を対比させて記載しています。

ISO/IEC 27001:2013	ISO/IEC 27001:2005
0 序文 1 適用範囲 2 引用規格 3 用語及び定義 4 組織の状況 5 リーダーシップ 6 計画 7 支援 8 運用 9 パフォーマンス評価 10 改善 附属書A(規定) 管理目的及び管理策 参考文献	0 序文 1 適用範囲 2 引用規格 3 用語及び定義 4 情報セキュリティマネジメントシステム 5 経営陣の責任 6 ISMS内部監査 7 ISMSのマネジメントレビュー 8 ISMSの改善 附属書A(規定) 管理目的及び管理策 附属書B(参考) OECD原則及びこの規格 附属書C(参考) 規格の比較 参考文献

図 0-2　ISO/IEC 27001:2013 と ISO/IEC 27001:2005 との対比

● 適用範囲

従来の ISO/IEC 27001:2005 では、「事業・組織・所在地・資産・技術の特徴の見地から、ISMS の適用範囲及び境界を定義する。この定義には、適用範囲からの除外についてその詳細及びそれが正当である理由も含めるものとする。」としていました。
ISO/IEC 27001:2013「4.3 ISMS の適用範囲の決定」では、「その境界及び適用可能性を決定し、適用範囲を決定するとき、外部及び内部の課題、利害関係者のニーズ及び要求事項、インタフェース及び依存関係を考慮しなければならない。」としています。

このように、より広い観点から ISMS の適用範囲及び境界を定義することを求める内容となりました。

● 予防処置の概念

従来の ISO/IEC 27001:2005「8.3 予防処置」の要求事項では、「組織は、ISMS の要求事項に対する不適合の発生を予防するために、起こり得る不適合の原因を除去する処置を決定しなければならない。とられる予防処置は、起こり得る問題の影響に見合ったものでなければならない。」としていました。
ISO/IEC 27001:2013「4.1 組織及びその状況の理解」では、「組織は、組織の目的に関連し、かつ、その ISMS の意図した成果を達成する、組織の能力に影響を与える、外部及び内部の課題を決定しなければならない。」としています。

この箇条では、マネジメントシステムの目的には、本来、予防的なツールとしての役割をもつために、組織の目的に関連し、意図した成果を達成する組織の能力に影響を与える、外部及び内部の課題を広い視点で評価をすることを要求しています。さらに「6.1 リスク及び機会に対処する活動」においても、広い視点で情報セキュリティマネジメントシステムが、規定した課題に対して、意図した成果を達成できること確実にすることを要求しています。

これらの 2 つの要求事項は、不適合の発生となりうる外部および内部の課題を決定し、ISMS の構築・運用を通じて適切に対処することを意図しており、従来の「予防処置」の概念を網羅しているものと考えられます。

● 法令及び規制の要求事項

従来の ISO/IEC 27001:2005 では、「法令及び規制の要求事項並びに契約上のセキュリティ義務を明確にし、これを扱う。」としていました。
ISO/IEC 27001:2013「4.2 利害関係者のニーズ及び期待の理解」では、「組織は、ISMS に関連する利害関係者及びその利害関係者の情報セキュリティに関連する要求事項を決定しなければならない。」としています。また、「利害関係者の要求事項には、法的及び規制要求事項並びに契約上の義務を含めてもよい。」としています。

このように、要求事項の記載上では、「～含めてもよい」という記載には変わりましたが、組織が、利害関係者の利益のため、適用される法令及び規制の要求事項を特定し、常に最新化させ、周知し、順守状況を意識して取り組むことは当然の要求事項であると考えられます。

● ISO 31000:2009（リスクマネジメントー概要）との整合

ISO 31000:2009 との関連性については、3 つの観点での整合が図られています。
第 1 点目は、共通テキストに相当する部位で、ISMS 固有の要求事項ではありませんが、箇条 4 の概念、内容及び、そのタイトルは、ISO 31000:2009 に該当するものが存在し、それが記述されたものと考えられます。また、「6.1 リスク及び機会に対処する活動」が、箇条 8 で組織のプロセスとして統合されるという構造についても同様のことが言えます。
第 2 点目は、「6.1.2 情報セキュリティリスクアセスメント」及び「6.1.3 情報セキュリティリスク対応」です。これは ISO 31000:2009 のリスクアセスメントとリスク対応のプロセスを基本として記述されています。
第 3 点目は、リスクマネジメントに関する用語及び定義を ISO 31000: 2009 及びその用語定義の規格 ISO Guide 73:2009（2.2.3 参照）から採用し、ISO/IEC 27001:2013（第 3 版）に記述しています。詳細については、次項の「リスクと機会」、「リスクアセスメント」及び本ガイドの本文を参照して下さい。

● リスクと機会

ISO/IEC 27001:2013「6.1 リスク及び機会に対処する活動」の 6.1.1 では、「ISMS の計画を策定するとき、組織は、4.1 に規定する課題及び 4.2 に規定する要求事項を考慮し、次の事項のために対処する必要があるリスク及び機会（opportunities）を決定しなければならない。」としています。
ISO 31000:2009（JIS Q 31000:2010）によると、リスクは「目的に対する不確かさの影響」のことであり、「影響とは、期待されていることから、好ましい方向又は好ましくない方向に乖離すること」としています。一方、ISO 31000:2009（JIS Q 31000:2010）では、「機会（opportunity）」を特に定義していません。「機会（opportunity）」が好ましい方向への乖離に対する処置の意味と解釈される場合もあるようですが、そうするとリスクの定義にある「好ましい方向への乖離への対応」と「6.1 リスク及び機会（opportunity）」はダブることになります。従って、この「機会（opportunity）」をどのように解釈するかということよりも、リスクマネジメントにおける事業リスクを理解することが重要です。事業リスクを理解する上では、ISO 31000 の「5.3 組織の状況の確定」を考慮して、「4.1 組織及びその状況の理解」との整合を確保することが、リスクマネジメントの重要なポイントとであると考えられます。

● リスクアセスメント

リスクアセスメントに関して、従来の ISO/IEC 27001:2005 では、「リスクアセスメントに対する組織の取組み方を定義する。これには、ISMS、特定された事業上の情報セキュリティの要求事項、並びに特定された法令及び規制の要求事項に適したリスクアセスメントの方法の特定、リスクを評価するに当たっての基軸の確立、リスク受容基準の設

定、リスクの受容可能レベルの特定、リスク受容基準及びリスクの受容可能レベルを決定する。」としていました。
ISO/IEC 27001:2013「6.1.2 情報セキュリティリスクアセスメント」では、「組織は、次の事項を行う、情報セキュリティリスクアセスメントのプロセスを定め、適用しなければならない。これには、情報セキュリティのリスク基準（リスク受容基準、情報セキュリティリスクアセスメントを実施するための基準等）を確立し、維持する。」としています。

これは、リスクアセスメントに関する要求事項の記述レベルを ISO 31000:2009（JIS Q 31000:2010）に合わせたと考えられます。そのため、ISO/IEC 27001:2005 の資産、脅威、ぜい弱性等による詳細なリスクアセスメントプロセスの記述ではありませんが、要求事項の上位レベルの記述（情報セキュリティリスクを特定する）には、CIA（機密性、完全性及び可用性）の視点でリスクを特定することが要求されており、ISO/IEC 27001:2005 に沿ったリスクアセスメントも具体的な方法の 1 つとして引き続き有効です。さらに、ISO/IEC 27001:2013 では、リスクアセスメントの選択の幅が広がり、組織の実情に沿ったリスクアセスメントの方法の適用が可能になりました。

● 情報セキュリティリスク対応
リスク対応に関して、従来の ISO/IEC 27001:2005 では、「リスク対応のための選択肢を特定し、評価する。適切な管理策は、リスクアセスメント及びリスク対応のプロセスにおいて特定した要求事項を満たすために選択・導入し、この選択には、法令、規制及び契約上の要求事項と同じく、リスク受容基準も考慮する。適用宣言書及びリスク対応計画を作成する。リスク対応計画及び残留リスクについて、経営陣の承認を得る」こととしていました。
ISO/IEC 27001:2013「6.1.3 情報セキュリティリスク対応」では、「組織は、情報セキュリティリスク対応のプロセスを定め、適用しなければならない。これには、リスクアセスメントの結果を考慮して、適切な情報セキュリティリスクの対応の選択肢を選定し、選定した情報セキュリティリスク対応の選択肢の実施に必要な全ての管理策を決定する。決定した管理策を附属書 A に示す管理策と比較し、必要な管理策が見落とされていないことを検証し、適用宣言書及び情報セキュリティリスク対応計画を作成する。情報セキュリティリスク対応計画及び残留している情報セキュリティリスクの受容について、リスク所有者の承認を得る」こととしています。

このように、情報セキュリティリスク対応については、附属書 A からの選択ではなくなり、まずは管理策を組織で決め、必要な管理策の見落としがないか附属書 A と比較することが求められるようになりましたが、基本的には ISO/IEC 27001:2005 のリスク対応とほぼ同様のプロセスであると考えられます。

● 文書管理
文書管理について、従来の ISO/IEC 27001:2005 では、「ISMS が要求する文書は、保護し、管理しなければならない。また、必要な管理活動を定義するために、文書化した手順を確立しなければならない。」としていました。
ISO/IEC 27001:2013「7.5 文書化した情報」では、「ISMS 及びこの規格で要求されている文書化した情報及び ISMS の有効性のために必要であると組織が決定した文書化した情報は、確実に管理しなければならない。」としています。ここでの文書化した情報の定義は、組織が管理し、維持するよう要求されている情報、及びそれが含まれている媒体としています。

従来は、「文書と記録の管理」が区別され異なる要求事項でしたが、ISO/IEC 27001:2013「7.5 文書化した情報」では、ISO MSS の共通テキストの要求事項を適用した結果、「文書化した情報の管理」としてまとめられました。基本的には従来の

ISO/IEC 27001:2005 とほぼ同様の管理プロセスであると考えられます。詳細は、本ガイドの 7.5.1 を参照して下さい。

● 2005 年版の主要な機能を継承（リスクアセスメント・リスク対応、管理策の導入・適用宣言書等）
リスクアセスメント、リスク対応については、従来の ISO/IEC 27001:2005 の内容（ISO/IEC 27001:2005 の 4.2 参照）を機能的に継承しています。また、リスクアセスメント・リスク対応の結果に対して、リスク選択肢とそれによる管理策（リスクを修正する手段）を特定し、適用宣言書に反映させるといった一連の仕組みは、ISO/IEC 27001:2005 と同一です。

● 附属書 A（管理目的及び管理策）の見直しと、27002 以外からの管理策の導入
ISO/IEC 27002:2013 は、新しい管理策の追加、既存の管理策の見直し改善が行われた結果、情報セキュリティ管理策については、14 の箇条で構成、35 のカテゴリ（管理目的ごとの分類）及び 114 の管理策とその実施の手引を記述しています。
ISO/IEC 27001:2013 の附属書 A「管理目的及び管理策」は、ISO/IEC 27001:2005 と同じく ISO/IEC 27002 との整合が維持されております。そのため、上記 ISO/IEC 27002:2013 の管理目的及び管理策の改正を受けて、14 の箇条、35 の管理目的、そして 114 の管理策となりました。

また、ISO/IEC 27001:2005 では、「附属書 A の中から～管理目的及び管理策を選択」することが要求されていましたが、ISO/IEC 27001:2013 では、まず「必要な全ての管理策を決定」し、この管理策を「附属書 A に示す管理策と比較し、必要な管理策が見落とされていないことを検証する」ことが求められるようになりました。これにより、組織は附属書 A だけではなく、任意の管理策群を適用することも可能となりました。

この背景には、現在、ISO/IEC 27011（電気通信業者向けの管理策群）や ISO/IEC 27017（クラウドユーザー・プロバイダー向けの管理策群。2014 年 3 月現在策定中。）など、各分野における管理策群の開発・改訂が進められていることがあります。ISO では、ISO/IEC 27001:2013 の改訂に加えて、このような各分野ごとの管理策群の適用に関する検討が進められています。このような状況から、ISO/IEC 27002:2013 では、従来の規格と比較すると、近年の脅威の変化に対応すべくその範囲を広め、管理策の記載に関しては表現をやや抽象化することで、いくつかの管理策を統合させ、詳細な管理策については、関連する ISO/IEC 27000 ファミリ規格を参照させるようになりました。
詳細は、本ガイドの「附属書 A 管理目的及び管理策」を参照して下さい。

０．２．３　ISO MSS 共通要素の概要

ISO/IEC 27001:2013 では、上述のとおり、ISO MSS 共通要素が適用されています。ここでは、その概要について説明します。
ISO マネジメントシステム規格の増加を受けて、ISO によりマネジメントシステム規格（MSS: Management System Standard）間の整合化が検討されました。その結果、2012 年 5 月に「ISO/IEC 専門業務用指針 第 1 部 統合版 ISO 補足指針」「附属書 SL（規定）マネジメントシステム規格の提案」として発行され、今後全ての MSS はこれを適用することになりました。

附属書 SL の狙いは、「合意形成され、統一された、上位構造、共通の中核となるテキスト、並びに共通用語及び中核となる定義（MSS 共通要素）を示すことによって、ISO マネジメントシステム規格の一貫性及び整合性を向上させることである。」とされています。また、個別のマネジメントシステム規格には、必要に応じて、「分野固有」の要求事項が追記さ

れることが想定されていますので、ISO/IEC 27001:2013 では、ISO MSS 共通要素を適用するとともに、必要に応じて ISMS 固有の要求事項を規定しています。

MSS 共通要素は、この附属書 SL の「Appendix 2（規定）上位構造、共通の中核となるテキスト、共通用語及び中核となる定義」に規定されています。なお、MSS には要求事項を提供するタイプ A の MSS と指針を提供するタイプ B の MSS があり、ISO/IEC 27001:2013 はタイプ A の MSS 規格です。

http://www.jsa.or.jp/itn/pdf/shiryo/isohosoku_taiyaku1304.pdf

この MSS 共通要素の適用により、ISO/IEC 27001:2013 の要求事項そのものが MSS 共通テキストに包含されるような構成になっています。これは組織のマネジメントシステムに組み込むことを考慮されたものであり、結果として、次のような共通テキストの特徴を引き継いだものとなっています。

- 全体として 1 つのマネジメントシステムに組み込むことが可能なように、一連の要求事項として定義されている。
- どのように達成すべきかではなく、何を達成すべきであるかを定義している。
- 要求事項が組織によって実施すべき順序や順番をあらかじめ想定することはしていない。
- 要求事項の特定の箇条の全ての活動が、別の箇条に示される活動に先んじて行われなければならないということを求めない。

また、ISO MSS 共通要素では上位構造も規定されており、各章の構成は、次の表 0-1 を適用することが求められます。本ガイドの 0.3.3 の表 0-2 と比較すると、ISO/IEC 27001:2013 の構成が MSS 共通要素の構成と整合していることがわかります。

表 0-1　ISO MSS 共通要素の各章の構成

1　適用範囲
2　引用規格
3　用語及び定義
4　組織の状況
4.1　組織及びその状況の理解
4.2　利害関係者のニーズ及び期待の理解
4.3　XXX マネジメントシステムの適用範囲の決定
4.4　XXX マネジメントシステム
5　リーダーシップ
5.1　リーダーシップ及びコミットメント
5.2　方針
5.3　組織の役割、責任及び権限
6　計画
6.1　リスク及び機会への取組み
6.2　XXX 目的及びそれを達成するための計画策定
7　支援
7.1　資源
7.2　力量
7.3　認識
7.4　コミュニケーション
7.5　文書化した情報
8　運用
8.1　運用の計画及び管理

9章　パフォーマンス評価 9.1　監視、測定、分析及び評価 9.2　内部監査 9.3　マネジメントレビュー 10　改善 10.1　不適合及び是正処置 10.2　継続的改善

（注記　共通テキストの XXX には、分野固有の修飾語が入ります。
ISO/IEC 27001 の場合には、情報セキュリティが入ります。）

０．２．４　ISO/IEC 27001:2013 と ISO/IEC 27001:2005 との対比

ISO/IEC 27001:2013 の規格を担当する標準化組織である ISO/IEC JTC 1/SC 27/ WG 1 より、旧版である ISO/IEC 27001:2005、ISO/IEC 27002:2005 との新旧対比表「N13143：SD3（Standing Document 3） Mapping Old-New Editions of ISO/IEC 27001 and ISO/IEC 27002」が発行されました。これは、以下の Web サイトで公開されており、ISO/IEC 27001:2005（JIS Q 27001:2006）、ISO/IEC 27002:2005（JIS Q 27002:2006）を構築している組織にとって有用な情報を提供しています。

http://isotc.iso.org/livelink/livelink/open/jtc1sc27

ISO/IEC 27001:2005（JIS Q 27001:2006）との対応関係及び差分については、本ガイドでも触れていますが、詳細はこの SD 3 を参照して下さい。なお SD 3 では、「関連が示されている場合でも、その内容が同一であることを意味するわけではない。」と序文にあるとおり、対応関係が示されている場合でも、1 対 1 の対応を意味するわけではないことに留意する必要があります。組織は、自らの ISMS において今回の変更の影響を評価する必要があります。

０．３　ISO/IEC 27001（JIS Q 27001）の概要

ISO/IEC 27001 の改訂経緯や改訂内容については、上記 0.2 で触れました。ここでは、ISO/IEC 27001（JIS Q 27001）全体についての概要を説明します。詳細な説明については、本ガイドの４章以降を参照して下さい。

ISO/IEC 27001（JIS Q 27001）は、組織が情報セキュリティマネジメントシステム（ISMS）を確立し、実施し、維持し、継続的に改善するための要求事項を提供することを目的として作成されています。この規格は、ISMS の確立及び実施について、それをどのように実現するかという方法ではなく、組織が何を行うべきかを主として記述しています。

組織のニーズ及び目的、セキュリティ要求事項、組織が用いているプロセス、並びに組織の規模及び構造によって、組織は、戦略的に、ISMS の採用を決定し、ISMS の確立及び実施を行います。これは、多くの情報を取り扱うようになっている、現代の組織のマネジメント及び業務プロセスを取り巻くリスクの変化に対応できるように、組織基盤を構築する抜本的な業務改革をする目的に適しています。

また、ISO/IEC 27001（JIS Q 27001）は、組織自身の情報セキュリティ要求事項を満たす組織の能力を、パフォーマンス評価及び内部監査などにより、組織の内部で評価する基準としても、第二者監査・第三者監査といわれる、外部関係者が評価するための基準としても用いることができます。

（注記）本ガイドの 0.2.1 に記載のとおり、JIS Q 27001 は、ISO/IEC 27001 との整合性が厳密に保たれています。本ガイドの 1 章以降では、JIS Q 27001 と表記していますが、言語の違いのみで内容は ISO/IEC 27001 と同一であり、ISO/IEC 27001（JIS Q 27001）、JIS Q 27001（ISO/IEC 27001）と表記されることもあります。

０．３．１　一般

ISMS が達成すべきことは、リスクマネジメントプロセスを適用することによって情報の機密性、完全性及び可用性を保護し、かつ、リスクを適切に管理しているという信頼を利害関係者に与えることにあります。そのためには、ISMS を、組織のプロセス及びマネジメント構造（management structure）全体の一部とし、かつ、その中に組み込むことが重要です。したがって、情報セキュリティを考慮した、プロセス、情報システム及び管理策を設計し、組織のニーズに合わせた規模で ISMS を導入することが考慮されます。

このようにリスクを把握し管理策を特定するマネジメントを実施することによって、組織のプロセス基盤及びその改革の方向性や方針が明確となり、これにより、組織全体に情報セキュリティに対する期待の達成やその情報セキュリティの能力に関するパフォーマンスの監視、測定が徹底されます。さらに、監視・測定したパフォーマンス評価の結果をフィードバックすることにより改善が行われ、本質的なプロセス基盤の改革、確立へとつながります。このことは、プロセスアプローチという考え方にもとづくマネジメントシステムを採用することでより明確になります。

０．３．２　プロセスアプローチ

このプロセスアプローチという考え方は、当初、品質マネジメントシステムの規格（ISO/IEC 9001:2000（JIS Q 9001:2000））等で紹介され、以降日本においても多くの組織で活用されています。プロセスアプローチでは、インプットをアウトプットに変換するために、経営資源を使用して運営管理されるあらゆる活動をプロセスとみなします。そして、組織内に存在するプロセスを明確にし、それらの相互関係を把握し、これら一連のプロセスをシステムとして適用して、運営管理する考え方のこと（アプローチ）を言います（図 0-3 参照）。

図 0-3　プロセスアプローチ

プロセスアプローチでは、それぞれのプロセスにおいて「インプット」されるものが何で、処理結果として「アウトプット」されるものが何かを多角的に検討し、明確にする必要があります。つまり、マネジメントシステムの構築を一連のプロセスとして捉え、各々のプロセスをプロセスアプローチに従って明確にし、その相互関係にあるインプットとアウト

プットを把握することで、マネジメントシステムの構築に要求される重要な事項が認識できます。

マネジメントシステムの構築では、ここで検討され明確にされた要求事項を実現するために、プロセスアプローチに基づいて、組織がプロセスを計画、実施、管理することが求められています。

ISMS プロセスは、利害関係者のニーズ及び期待をインプットとしてどう取り入れ、必要となる活動及びプロセスを経て、その要求事項及び期待を満たした成果を達成するために必要な活動及びプロセスを表しています。この ISMS プロセスは、PDCA モデルを採用することで整理されます。

なお、ISO/IEC 27001:2013（JIS Q 27001:2014）には PDCA モデルという表現は明記されておりませんが、附属書 SL の「SL5.2 MSS－マネジメントシステム規格」には、「有効なマネジメントシステムには、通常、意図した成果を達成するために、“Plan-Do-Check-Act（PDCA）”のアプローチを用いた組織のプロセス管理を基盤とする」という記述があります。この附属書 SL を適用した ISO/IEC 27001:2013（JIS Q 27001:2014）でも、PDCA のアプローチが ISO/IEC 27001:2005（JIS Q 27001:2006）から継続して考慮されています（附属書 SL については、本ガイドの 0.2.3 参照）。

０．３．３　ISO/IEC 27001:2013（JIS Q 27001:2014）の構成

ISO/IEC 27001:2013（JIS Q 27001:2014）は、ISO/IEC 27001:2005（JIS Q 27001:2006）を機能的に継承し、さらに ISO MSS 共通要素の適用、リスクマネジメント（ISO 31000:2009（JIS Q 31000:2010））への対応を考慮した改訂内容となっています。表 0-2 に、その構成を示します。

表 0-2　ISO/IEC 27001:2013（JIS Q 27001:2014）の構成

ISO/IEC 27001:2013 （JIS Q 27001:2014）	概略
0 序文	ISMS は、リスクマネジメントを適用することで、情報セキュリティを確保し、かつ、リスクを適切に管理しているという信頼を利害関係者に与える。 ISMS を、組織のプロセス及びマネジメント構造全体の一部として、組み込む。 この規格で示す要求事項の順序は、その重要性を反映するものでもなく、またそれを実施する順序を示すものでもない。
1 適用範囲	箇条 4 から箇条 10 に規定する要求事項の例外はみとめられない。
2 引用規格	ISO/IEC 27000 を適用する。
3 用語及び定義	ISO/IEC 27000 で規定されている用語及び定義を適用する。
4 組織の状況	
4.1 組織及びその状況の理解	組織における状況を理解することが重要である。外部・内部の課題の決定については、ISO 31000:2009 の 5.3 の外部・内部の状況を参照する。
4.2 利害関係者のニーズ及び期待の理解	関連する利害関係者の特定とその要求事項を決定する。利害関係者の要求事項には、法的及び規制の要求事項並びに契約上の義務を含めることが考慮される。
4.3 情報セキュリティマネジメントシステムの適用範囲の決定	組織は、ISMS の適用範囲を決めるために、その境界及び適用可能性を決定する。このとき、組織は、4.1 に規定する外部及び内部の課題、4.2 に規定する要求事項を考慮する。
4.4 情報セキュリティマネジメントシステム	組織は、ISMS を確立、実施、維持及び継続的に改善する。

5 リーダーシップ	
5.1 リーダーシップ及びコミットメント	トップマネジメントは、ISMS に関するリーダーシップとコミットメントを実証する。
5.2 方針	トップマネジメントは、情報セキュリティ方針を確立する。
5.3 組織の役割、責任及び権限	トップマネジメントは、情報セキュリティに関連する役割に対して、責任及び権限を割り当て、伝達することを確実にする。
6 計画	
6.1 リスク及び機会に対処する活動	
6.1.1 一般	ISMS の計画を策定するとき、組織は、4.1 の課題及び 4.2 の要求事項を考慮し、リスク及び機会を決定する（ISMS がその意図した成果を達成できることを確実にするため、望ましくない影響を防止又は低減するため、継続的改善を達成するため）。
6.1.2 情報セキュリティリスクアセスメント	情報セキュリティのリスク基準を確立し、リスクを特定・分析・評価する。
6.1.3 情報セキュリティリスク対応	情報セキュリティリスク対応のプロセスを定め、リスク対応の選択肢を選定し、管理策を決定、適用宣言書及び情報セキュリティリスク対応計画を策定する。
6.2 情報セキュリティ目的及びそれを達成するための計画策定	組織は、関連する部門・階層において、情報セキュリティ目的を確立し、それらを達成するための計画を策定する。
7 支援	
7.1 資源	組織は、ISMS の確立、実施、維持及び継続的改善に必要な資源を決定、提供する。
7.2 力量	情報セキュリティパフォーマンスに影響を与える業務を組織の管理下で行う人々に必要な力量を決定、力量を備えることを確実にする。
7.3 認識	組織の管理下で働く人々は、情報セキュリティ方針、ISMS の有効性に対する自らの貢献、及び ISMS 要求事項に適合しないことの意味に関して認識をもつ必要がある。
7.4 コミュニケーション	組織は、ISMS に関する内部及び外部のコミュニケーションを実施する必要性を決定する。
7.5 文書化した情報	組織は、規格が要求する文書化した情報、及び ISMS の有効性のために必要であると組織が決定した文書化した情報を ISMS に含む。
8 運用	
8.1 運用の計画及び管理	組織は、情報セキュリティ要求事項を満たすため、及び 6.1 で決定した活動を実施するために、必要なプロセスを計画、実施、管理する。また、組織は、6.2 で決定した情報セキュリティ目的を達成するための計画を実施する。
8.2 情報セキュリティリスクアセスメント	組織は、あらかじめ定めた間隔で、又は重大な変更の提案・重大な変化の発生のとき、情報セキュリティリスクアセスメントを実施する。
8.3 情報セキュリティリスク対応	組織は、8.2 に対するリスク対応を実施する。
9 パフォーマンス評価	
9.1 監視、測定、分析及び評価	組織は情報セキュリティパフォーマンス及び ISMS の有効性を評価する。
9.2 内部監査	組織は、あらかじめ定めた間隔で内部監査を実施する。
9.3 マネジメントレビュー	トップマネジメントは、あらかじめ定めた間隔で、ISMS をレビューする。
10 改善	
10.1 不適合及び是正処置	組織は、不適合が発生した場合、その不適合に対処し、その原因を除去するための必要な処置を実施し、是正処置の有効性をレビューする。
10.2 継続的改善	組織は、ISMS の適切性、妥当性及び有効性を継続的に改善する。

この ISO/IEC 27001:2013（JIS Q 27001:2014）では、組織が、そのマネジメントシステムに合わせて ISMS を全体の一部として組み込み、その組織のマネジメントシステムとしての PDCA のプロセスを構成、管理することを求めています。

０．３．４　他のマネジメントシステムとの両立性

ISO/IEC 27001（JIS Q 27001）の他のマネジメントシステムとの両立性について、ISO/IEC 27001:2005 では、ISO 9001:2008 及び ISO 14001:2004 との調和がとられるように考慮されていました。今回の改訂では、附属書 SL を採用した他の全てのマネジメントシステム規格と、上位構造、 共通テキスト、 共通用語において両立性が保たれるようになりました（附属書 SL については、本ガイドの 0.2.3 参照）。附属書 SL を採用することによって、複数のマネジメントシステム規格の要求事項を満たす、1 つの統合マネジメントシステムを効率的に確立・運用することを可能としています。

０．４　ISMS 適合性評価制度

０．４．１　制度の概要

ISMS 適合性評価制度は、JIS Q 27001（ISO/IEC 27001）を認証基準とした情報セキュリティの運用管理に対する第三者認証制度です。
JIPDEC では、国際規格 ISO/IEC 27001 の原案となった英国 BS 7799-2 を基に ISMS 認証基準を作成して、2001 年にパイロット事業を開始しました。
その後、2002 年 4 月に本格運用を開始し、2005 年 10 月に ISO/IEC 27001 が発行されこと、及び 2006 年 5 月に JIS Q 27001 が発行されたことを受けて、認証基準を JIS Q 27001（ISO/IEC 27001）へと移行しました。
また、2013 年 10 月に改訂版である ISO/IEC 27001:2013 が発行され、これに合わせて 2014 年 3 月に JIS Q 27001:2014 が発行されたことから、現在、JIS Q 27001:2014（ISO/IEC 27001:2013）への移行を行っています。

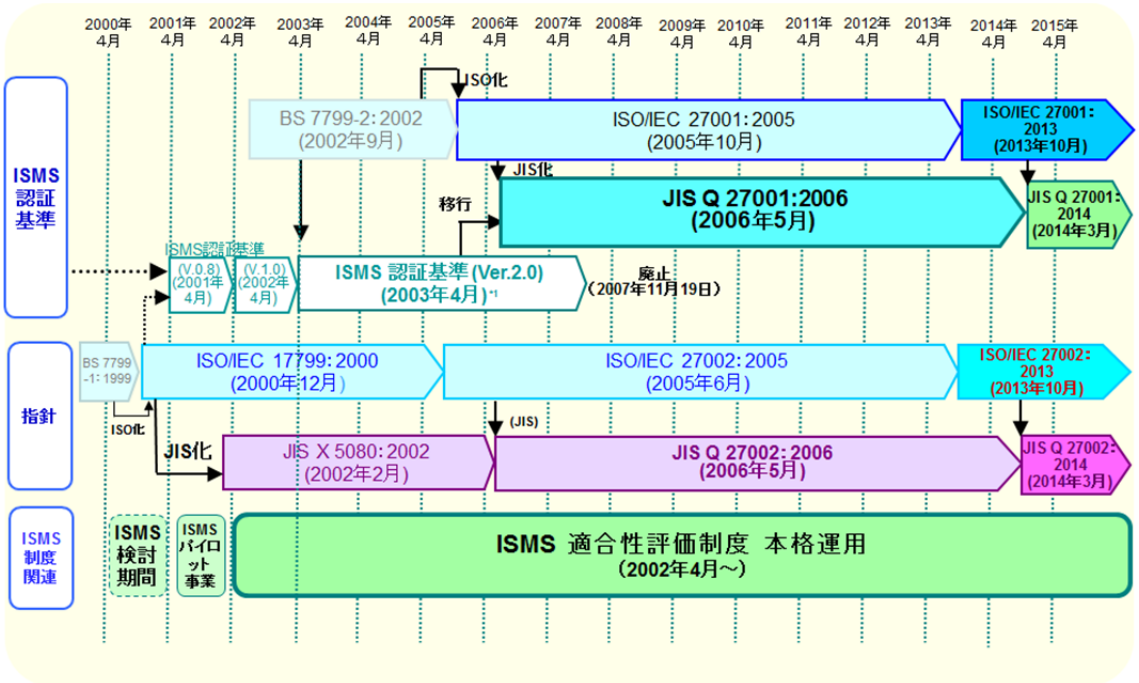


図 0-4　ISO 規格及び JIS 規格制定の経緯

０．４．２　27001 改訂版（第 2 版）のへの移行

2013 年 10 月 1 日に ISO/IEC 27001:2013 が発行されたことに伴い、ISO/IEC 27001:2013 への移行が開始されました。ISO/IEC 27001:2013 への移行は、発行と同時に開始し、移行期間は 2 年間です。この移行計画は、2013 年 10 月 25 日の第 27 回 IAF（国際認定フォーラム）年次総会の決議に従っています。
JIS Q 27001:2006（ISO/IEC 27001:2005）から JIS Q 27001:2014（ISO/IEC 27001:2013）への移行のケースは以下のとおりです。

① JIS Q 27001:2006（ISO/IEC 27001:2005）による初回認証審査（新規の認証）は、ISO/IEC 27001:2013 の規格発行後 1 年以内に登録を完了する。また 2015 年 10 月 1 日までに、JIS Q 27001:2014（ISO/IEC 27001:2013）への移行を完了する。

② JIS Q 27001:2014（ISO/IEC 27001:2013）発行後、認証機関は適用規格として JIS Q 27001:2014（ISO/IEC 27001:2013）又は JIS Q 27001:2006（ISO/IEC 27001:2005）のいずれの規格を使用するかについて組織と合意するとともに、適用規格として使用した規格を審査計画、審査報告書及び認証文書で明記する。また、JIS Q 27001:2014（ISO/IEC 27001:2013）による初回審査の場合には、認証機関は JIS Q 27001:2014（ISO/IEC 27001:2013）に基づいて認証審査をするための手順が完備している。

③ JIS Q 27001:2006（ISO/IEC 27001:2005）で認証登録されている組織に対しては、組織の維持審査（サーベイランス）又は再認証審査において、JIS Q 27001:2014（ISO/IEC 27001:2013）への移行のための差分審査を含むことが望ましい。

④ 移行の終了までに、全ての既存の認証文書は、JIS Q 27001:2014（ISO/IEC 27001:2013）の新しいものにする。ISO/IEC 27001:2013 発行後、24 ヶ月経過時点で、JIS Q 27001:2006（ISO/IEC 27001:2005）の認証文書は有効でなくなる。

JIS Q 27001:2006（ISO/IEC 27001:2005）から JIS Q 27001:2014（ISO/IEC 27001:2013）への移行のイメージは図 0-5 のとおりです。

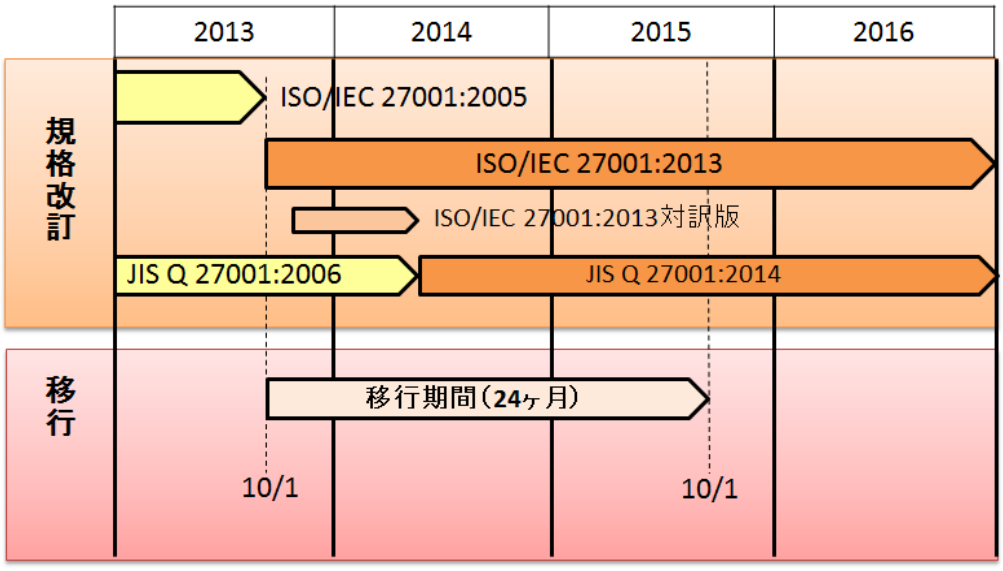


図 0-5　移行のイメージ

１．適用範囲

本ガイドの「0 序文」では、規格改訂の経緯や概要などを詳しく説明してきましたが、本章からは、JIS Q 27001:2014 の箇条に沿って説明します。そのため、規格の表記も JIS Q 27001:2014 としています。

JIS Q 27001:2014 の「1 適用範囲」では、組織における ISMS の位置付けと、JIS Q 27001:2014 の適用について述べています。

この規格は、組織における ISMS を確立、実施、維持及び継続的に改善するための要求事項と情報セキュリティのリスクアセスメント及びリスク対応を行うための要求事項を規定しています。つまり、企業や組織が所有し、管理、運用する情報及び情報に関連する資産の価値に見合うリスク対策の実施や、コンプライアンスの観点から法令等を順守し、それを維持するための枠組みを確立、実施、維持及び継続的改善を行うことを意味しています。

また、この規格は、あらゆる形態及び規模の組織（例えば、営利企業、政府機関、非営利団体）に適用できることを意図していると記述し、様々な組織に対して適用できる汎用的な規定であるとしています。

JIS Q 27001:2014 では、箇条 4 から箇条 10 までに規定する要求事項は、組織において必ず実施するものであり、例外は認められません。これに対し、附属書 A「管理目的及び管理策」の要求事項は、適用除外が可能となっています。附属書 A「管理目的及び管理策」に規定された管理策の適用を除外する場合は、除外した理由が求められています。

従来の JIS Q 27001:2006 では、「1 適用範囲」で、管理策の適用除外への言及が記載されていましたが、今回の改訂では、管理策の適用除外について「6.1.3 情報セキュリティリスク対応」に規定されており、重複を避けるために、「1 適用範囲」には記載されなくなりました。

> この規格は，組織の状況の下で，ISMS を確立し，実施し，維持し，継続的に改善するための要求事項について規定する。この規格は，組織のニーズに応じて調整した情報セキュリティのリスクアセスメント及びリスク対応を行うための要求事項についても規定する。この規格が規定する要求事項は，汎用的であり，形態，規模又は性質を問わず，全ての組織に適用できることを意図している。組織がこの規格への適合を宣言する場合には，箇条 4～箇条 10 に規定するいかなる要求事項の除外も認められない。
>
> （JIS Q 27001:2014　1 適用範囲　より引用）

JIS Q 27001:2014 の要求事項を適切に実施することは、利害関係者からの信頼を確保するために十分なバランスのとれた情報セキュリティを確立し、維持していくことにつながります。

利害関係者とは、JIS Q 27000 の定義によると、組織の「ある決定事項若しくは活動に影響を与え得るか、その影響を受け得るか、又はその影響を受けると認識している、個人又は組織」となります。顧客や投資家、供給者、関係当局等といった組織外部の人々のみならず、組織内の人々等を含みその対象は広範囲に及びます。詳細は、本ガイドの「4.2 利害関係者のニーズ及び期待の理解」を参照して下さい。

JIS Q 27001:2014 は、どのような組織であっても必ず適用させる事が必要な要求事項と、事業の特性により適用除外が可能である要求事項で構成されており、広く利用可能な基準としてあらゆる組織に適用できるよう配慮されています。

表 1-1　要求事項の適用について

JIS Q 27001:2014	要求事項の取扱い
JIS Q 27001:2014 の箇条 4,5,6,7,8,9 及び 10	必ず適用させる事が必要な要求事項
JIS Q 27001:2014 の附属書 A「管理目的及び管理策」	適用除外が可能となっている要求事項

JIS Q 27001:2014 の附属書 A「管理目的及び管理策」に規定された要求事項の適用を除外する場合は、除外した理由としてリスクアセスメントに基づく合理的な説明が求められます。

リスクを内包した情報及び情報に関連する資産を保護するには、それらがもつ価値や脅威、ぜい弱性などのリスクの源を明らかにし、リスクの大小を判別して適切な対策を講じなければなりません。安易な適用除外または理由の明確でない適用は、マネジメントシステムの一貫性に大きな影響を与えます。

適用理由が特定されていることの明示とともに、以下に例示するような「除外の原則」を定め、ある要求事項について条件が全て満たされる場合にのみ適用を除外するなど適切な判断が求められます。

- **ISMS の能力、責任に影響を及ぼさないこと**
- **情報セキュリティ方針、情報セキュリティ目的と相反しないこと**
- **関連法規や規制に関する要求事項でないこと**

このような適用除外の理由は、適用宣言書に記載することが求められています。
適用宣言書とは、ISMS に関連してその組織が適用する管理目的及び管理策を記述した、文書化された情報です。
管理目的及び管理策は、JIS Q 27001:2014 における 4.1 及び 4.2、並びに箇条 6 から導き出される、組織の情報セキュリティに対する、次のものに基づきます。

- **リスクアセスメント及びリスク対応のプロセスの結果及び結論**
- **法令又は規制の要求事項**
- **契約上の義務**
- **事業上の要求事項**

リスクアセスメント及びリスク対応の作業結果を踏まえ、附属書 A「管理目的及び管理策」の管理目的及び管理策を特定します。適用宣言書には、適用した結果とその理由、適用しない場合にもその理由を明記します。また、組織で必要と判断した管理策が、附属書 A の詳細管理策の項目には無く、他の任意の情報源の中から独自に追加した場合は、その内容と理由についても記述します。

このようにして作成された適用宣言書は、組織が ISMS を確立、実施、運用、継続的に改善するために適用した情報セキュリティ管理策を表明するものであり、特定の利害関係者に開示又は交換することによって、ISO という共通言語に基づいたセキュリティレベルの確認ができ、情報セキュリティを維持しているという信頼の保持にもつながります。

２．引用規格

JIS Q 27001:2014 では、以下のとおり JIS Q 27000 を引用規格として挙げています。ここでは、JIS Q 27000 も含めて情報セキュリティ及びマネジメントシステムについての規格を紹介します。

> 次に掲げる規格は，この規格に引用されることによって，この規格の規定の一部を構成する。この引用規格は，その最新版（追補を含む。）を適用する。
> JIS Q 27000　情報技術－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－用語
> 注記　対応国際規格：ISO/IEC 27000, Information technology － Security techniques － Information security management systems － Overview and vocabulary (MOD)
>
> （JIS Q 27001:2014　2 引用規格　より引用）

２．１　JIS Q 27000:2014 (ISO/IEC 27000:2014)

ISO/IEC 27000:2014 の発行に伴って、日本工業標準調査会（JISC）により日本工業標準（JIS）として制定された国内規格です。
ISO/IEC 27000:2014 は、ISMS の概要、ISMS ファミリ規格の概要、ISMS ファミリ規格で用いられる用語及び定義をまとめた規格です。
JIS Q 27000 は、そのうち用語及び定義部分について技術的内容を変更することなく国内規格化したものです。

JIS Q 27000 は、ISMS に関連する、次のような用語及び定義を対象として規定しています。

- ISMS ファミリ規格で共通して用いている用語及び定義を対象とする。
- ISMS ファミリ規格で適用している全ての用語及び定義を対象としているわけではない。
- 新しい用語を定義することについて、ISMS ファミリ規格を制限するものではない。

ISMS ファミリ規格には、次の規格が含まれます。

- ISMS 及び ISMS を認証する機関に対する要求事項を規定する規格（ISO/IEC 27001、ISO/IEC 27006）
- ISMS を確立し、実施し、維持し、改善するためのプロセス全体に関する直接的な支援、詳細な手引及び／又は解釈を提供する規格（ISO/IEC 27002 他）
- ISMS に関する分野固有の指針を取り扱う規格
- ISMS に関する適合性評価を取り扱う規格

これらの規格は、あらゆる形態及び規模の組織（例えば、営利企業、政府機関、非営利団体）に適用できます。

また、この規格に記載されている用語及び定義は、次のように大別されます。

- 情報セキュリティに関する用語
- リスクマネジメントに関する用語（JIS Q 0073:2010 から引用）
- マネジメントシステムに関する用語（附属書 SL から引用）
  （注記）附属書 SL については、本ガイドの 0.2.3 参照

従来の JIS Q 27001:2006（ISO/IEC 27001:2005）では、引用規格は JIS Q 27002:2006（ISO/IEC 27002:2005）でしたが、その後 JIS Q 27001:2006（ISO/IEC 27001:2005）が参

照していた用語及び定義が JIS Q 27000（ISO/IEC 27000）に移されたこと、また附属書 A に管理目的及び管理策を記載しており JIS Q 27002（ISO/IEC 27002）への参照は箇条 4～10 からではなく附属書 A からであることにより、今回の改訂で、引用規格は JIS Q 27000（ISO/IEC 27000）とされました。これは、JIS Q 27001:2014 に対して、JIS Q 27002:2014 の位置づけや重要性が変化したわけではなく、ISO 及び JIS での引用規格の定義に適合するようにしたためです。

２．２　JIS Q 27002:2014 (ISO/IEC 27002:2013)

ISO/IEC 27002（ISO/IEC 17799）の制定発行に伴って、日本工業標準調査会（JISC）により日本工業標準（JIS）として制定された国内規格です。現在の内容は、ISO/IEC 27002 を忠実に日本語に翻訳し、国際規格との整合性が厳密に保たれたものとなっています。

ISO/IEC 27002 は、情報セキュリティに対するマネジメントシステムの国際規格として、2000 年に ISO/IEC 17799 として制定発行されました。この規格は英国規格 BS 7799-1:1999 を基にしており、実践のための規範をまとめたものです。2005 年に改訂され、2007 年 7 月に規格番号が変更され、ISO/IEC 27002 となりました。2013 年 10 月に 2 度目の改訂が行われ ISO/IEC 27002：2013 として発行されました。

これに伴い、JIS Q 27002 も改訂が行われ、JIS Q 27002:2014 が発行されています。

＜参考＞　BS 7799
1995 年に英国で制定発行された情報セキュリティに関する英国規格（British Standard）で、情報セキュリティの技術的対策だけではなく、人及び組織の管理を含めたマネジメントに関する実践のための規範をまとめたものです。その後、1998 年に認証の基準となる第 2 部が制定されて 2 部構成になりました。なお、この第 1 部と第 2 部は、それぞれ BS ISO/IEC 17799:2005 及び BS ISO/IEC 27001:2005 に置き換わりました。さらに、2013 年の改訂で、BS ISO/IEC 27002:2013 及び BS ISO/IEC 27001:2013 に置き換わりました。

２．３　JIS Q 0073:2010 (ISO Guide 73:2009)

2002 年に ISO/IEC Guide 73 として制定されたリスクマネジメントの用語を改訂することを目的に検討が開始されましたが、改訂原案に対して国際電気標準会議（IEC）の同意が得られず、2009 年に第 1 版として ISO Guide 73 が発行されました。これを技術的内容及び構成を変更することなく作成した日本工業規格が JIS Q 0073:2010 です。

この規格は，リスクマネジメントに関する一般的な用語及びその定義について規定する。この規格は，リスクの運用管理に関連する活動の記述に関する一貫性のある相互理解及び首尾一貫した取組み，並びにリスクマネジメントに対処するプロセス及び枠組みにおける統一されたリスクマネジメント用語の使用を奨励することを目指している。
この規格は，次のような利用者を想定している。
－　リスクの運用管理に関与する人
－　リスクの運用管理にかかわる規格又は産業分野特有なガイド，手順及び実務規範を策定する人

リスクマネジメントに関する原則及び指針については，JIS Q 31000:2010 を参照。

（JIS Q 0073:2010　0 適用範囲　より引用）

用語は、リスクマネジメントの一般的領域を網羅する形で、以下の順番で並べられています（JIS Q 0073:2010 の序文を参照）。

- リスクに関する用語
- リスクマネジメントに関する用語
- リスクマネジメントプロセスに関する用語
- コミュニケーション及び協議に関する用語
- 組織の状況に関する用語
- リスクアセスメントに関する用語
- リスク特定に関する用語
- リスク分析に関する用語
- リスク評価に関する用語
- リスク対応に関する用語
- モニタリング及び測定に関する用語

２．４　JIS Q 31000:2010（ISO 31000:2009）

JIS Q 31000:2010 は、ISO 31000:2009 の構成及び技術的内容を変更することなく作成された日本工業規格です。各分野の個別手法として開発されてきたリスクマネジメントの用語及び運営法に関して、社会の高度化、リスクの増大にともない、企業全社の経営手法として採用できるリスクマネジメント手法の必要性が生じました。ISO 31000:2009「リスクマネジメント- 原則及び指針（Risk management－Principles and guidelines）」は、この必要性にこたえるために、開発されました。
なお、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、この規格が発行された時点で廃止となりました。

JIS Q 27001:2014 では、リスクマネジメントについて、TR X 0036-1～5（GMITS）及び JIS Q 0008:2003（Guide 73:2002）のものから、JIS Q 31000:2010（ISO/IEC 31000:2009）及び JIS Q 0073:2010（ISO Guide 73:2009）のものに更新しています。また、本ガイドの 0.2.2 に記載のとおり、ISO MSS の共通要素も JIS Q 31000:2010（ISO/IEC 31000:2009）との整合が図られています。

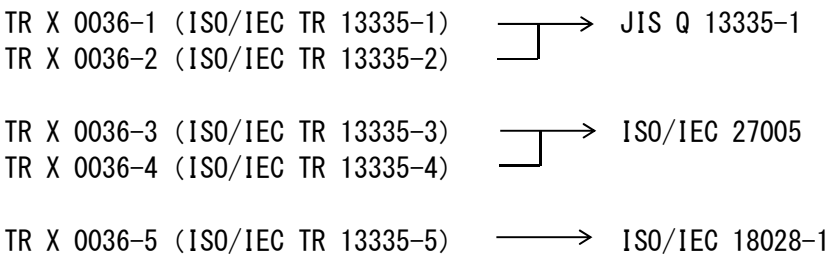
この規格は，リスクマネジメントに関する原則及び一般的な指針を示す。
この規格は，あらゆる公共，民間若しくは共同体の事業体，団体，グループ又は個人が使用できる。したがって，この規格は，いかなる産業にも分野にも特有なものではない。
　注記 1　便宜上，この規格の使用者はすべて“組織”という一般用語で表現する。
この規格は，組織の存在期間全体を通して適用できるものであり，戦略及び意思決定，業務，プロセス，機能，プロジェクト，製品，サービス，並びに資産を含む，広範囲にわたる活動に対して適用できる。
この規格は，その特質にかかわらず，好ましい結果をもたらすものか好ましくない結果をもたらすものかを問わず，あらゆる種類のリスクに適用できる。
この規格は一般的な指針を提供するものであるが，組織間でリスクマネジメントの画一性を高めることを意図するものではない。リスクマネジメントの計画及び枠組みの設計，及び実践に当たっては，それぞれの組織の多様なニーズ，特有の目的，組織の状況，体制，業務，プロセス，機能，プロジェクト，製品，サービス，資産及び行われている特有の実務について考慮する必要がある。
この規格は，既存及び将来制定される規格において，リスクマネジメントのプロセスを整合化することを意図している。この規格は，特有のリスク及び／又は産業分野に対応している規格を支援する上で共通の取組みを提供するものであり，それらの規格に取って代わるものではない。
この規格は，認証に用いることを意図したものではない。

（JIS Q 31000:2010　1 適用範囲　より引用）

＜参考＞　TR X 0036-1～5（GMITS）
「IT セキュリティマネジメントのガイドライン（Guidelines for the management of IT security）」と称し、ISO/IEC TR 13335 として国際化された標準情報です。このガイドラインは、IT セキュリティの管理をどのように構築していくかをリスクマネジメントを含めて記述した解説書です。
以下の 5 部で構成されていました。

■　第 1 部:IT セキュリティの概念およびモデル
■　第 2 部:IT セキュリティのマネジメント及び計画
■　第 3 部:IT セキュリティマネジメントのための手法
■　第 4 部:セーフガードの選択
■　第 5 部:ネットワークセキュリティに関するマネジメントの手引

これらの規格は 1996 年から順次制定発行されましたが、2006 年に有効期限が切れ廃版となっています。ただし、この旧標準情報にも、本ガイドにおいて有益な情報が含まれていますので、旧標準情報からの内容を引用しています。
なお、これらの標準情報は改訂によって、次のような規格に一部が引き継がれています。



３．用語及び定義

JIS Q 27001:2014 で用いる用語及びその定義について説明します。JIS Q 27001:2014 の用語及び定義は、JIS Q 27000 に記載されています。JIS Q 27000 の用語及び定義の表記順序は、英語表記のアルファベット順となっています。そのため一見すると脈絡無く用語が並んでいるように見えますが、内容により以下の 3 つに大別して整理すると理解し易いと思います。
なお、JIS Q 27001:2014 で用いる用語として、新たにマネジメントシステムに関する用語の定義が追加され、また情報セキュリティやリスクマネジメントに関する用語の定義の見直しが行われました。

表 3-1　用語の分類

<table>
<tr><td rowspan="6">情報セキュリティに関する用語の定義</td><td colspan="3">2.33 情報セキュリティ（information security）</td></tr>
<tr><td colspan="3">2.12 機密性（confidentiality）</td></tr>
<tr><td colspan="3">2.40 完全性（integrity）</td></tr>
<tr><td colspan="3">2.9 可用性（availability）</td></tr>
<tr><td colspan="3">2.35 情報セキュリティ事象（information security event）</td></tr>
<tr><td colspan="3">2.36 情報セキュリティインシデント（information security incident）</td></tr>
<tr><td rowspan="13">リスクマネジメントに関する用語の定義</td><td colspan="3">2.68 リスク（risk）</td></tr>
<tr><td colspan="3">2.76 リスクマネジメント（risk management）</td></tr>
<tr><td colspan="3">2.77 リスクマネジメントプロセス（risk management process）</td></tr>
<tr><td rowspan="3">（組織の状況に関する用語）</td><td colspan="2">2.42 内部状況（internal context）</td></tr>
<tr><td colspan="2">2.27 外部状況（external context）</td></tr>
<tr><td colspan="2">2.73 リスク基準（risk criteria）</td></tr>
<tr><td rowspan="7">2.71 リスクアセスメント（risk assessment）</td><td rowspan="2">2.75 リスク特定（risk identification）</td><td>2.25 事象（event）</td></tr>
<tr><td>2.78 リスク所有者（risk owner）</td></tr>
<tr><td rowspan="3">2.70 リスク分析（risk analysis）</td><td>2.45 起こりやすさ（likelihood）</td></tr>
<tr><td>2.14 結果（consequence）</td></tr>
<tr><td>2.44 リスクレベル（level of risk）</td></tr>
<tr><td>2.74 リスク評価（risk evaluation）</td><td>2.69 リスク受容（risk acceptance）</td></tr>
<tr><td rowspan="3">2.79 リスク対応（risk treatment）</td><td colspan="2">2.16 管理策（control）</td></tr>
<tr><td colspan="2">2.64 残留リスク（residual risk）</td></tr>
<tr><td colspan="2">2.65 レビュー（review）</td></tr>
<tr><td rowspan="25">マネジメントシステムに関する用語の定義</td><td colspan="3">2.57 組織（organization）</td></tr>
<tr><td colspan="3">2.41 利害関係者（interested party）（推奨用語）</td></tr>
<tr><td colspan="3">2.63 要求事項（requirement）</td></tr>
<tr><td colspan="3">2.46 マネジメントシステム（management system）</td></tr>
<tr><td colspan="3">2.84 トップマネジメント（top management）</td></tr>
<tr><td colspan="3">2.24 有効性（effectiveness）</td></tr>
<tr><td colspan="3">2.60 方針（policy）</td></tr>
<tr><td colspan="3">2.56 目的（objective）</td></tr>
<tr><td colspan="3">2.11 力量（competence）</td></tr>
<tr><td colspan="3">2.23 文書化した情報（documented information）</td></tr>
<tr><td colspan="3">2.61 プロセス（process）</td></tr>
<tr><td colspan="3">2.59 パフォーマンス（performance）</td></tr>
<tr><td colspan="3">2.58 外部委託する（outsource）（動詞）</td></tr>
<tr><td colspan="3">2.52 監視（monitoring）</td></tr>
<tr><td colspan="3">2.48 測定（measurement）</td></tr>
<tr><td colspan="3">2.5 監査（audit）</td></tr>
<tr><td colspan="3">2.13 適合（conformity）</td></tr>
<tr><td colspan="3">2.53 不適合（nonconformity）</td></tr>
<tr><td colspan="3">2.18 修正（correction）</td></tr>
<tr><td colspan="3">2.19 是正処置（corrective action）</td></tr>
<tr><td colspan="3">2.15 継続的改善（continual improvement）</td></tr>
</table>

（注記）上記の番号は、JIS Q 27000 における各用語の項番です。

上記の情報セキュリティに関する用語は、本ガイドの「3.1 情報セキュリティに関する用語」で説明します。

リスクマネジメントに関する用語は、JIS Q 0073:2010 から引用されています。なお、殆どのこれらの用語は、JIS Q 31000 でも用語の定義で引用されています。このうちリスクマネジメントについては、本ガイドの「3.2 リスクマネジメントに関する用語」で説明します。

マネジメントシステムに関する用語は、ISO/IEC 専門業務用指針 第 1 部 統合版 ISO 補足指針の「附属書 SL（規定）マネジメントシステム規格の提案」に規定する「Appendix 2（規定）上位構造、共通の中核となるテキスト、並びに共通用語及び中核となる定義」の「3. 用語及び定義」を引用しています。

３．１　情報セキュリティに関する用語

組織経営に不可欠である情報は、適切に保護されなければなりません。情報が適切に保護されていないと、漏洩したり、内容が不正確であったり、必要な時に使えない等、業務の遂行に支障をきたすといったリスクがあります。「情報セキュリティ」とは、重要な情報をこうしたリスクから守ることです。

３．１．１　情報セキュリティ

JIS Q 27000 では、情報セキュリティを以下のように定義しています。

> 2.33 情報セキュリティ（information security）
> 情報の機密性（2.12），完全性（2.40）及び可用性（2.9）を維持すること。
> 注記　さらに，真正性（2.8），責任追跡性，否認防止（2.54），信頼性（2.62）などの特性を維持することを含めることもある。
>
> （JIS Q 27000:2014　2 用語及び定義　より引用）

情報セキュリティに関わるリスクを明確にするために、情報セキュリティの主たる 3 要素である「機密性」、「完全性」、「可用性」のそれぞれの観点から分析を行います。その他の 4 つの特性は、通常上記 3 つの要素から導くことができると考えられます。

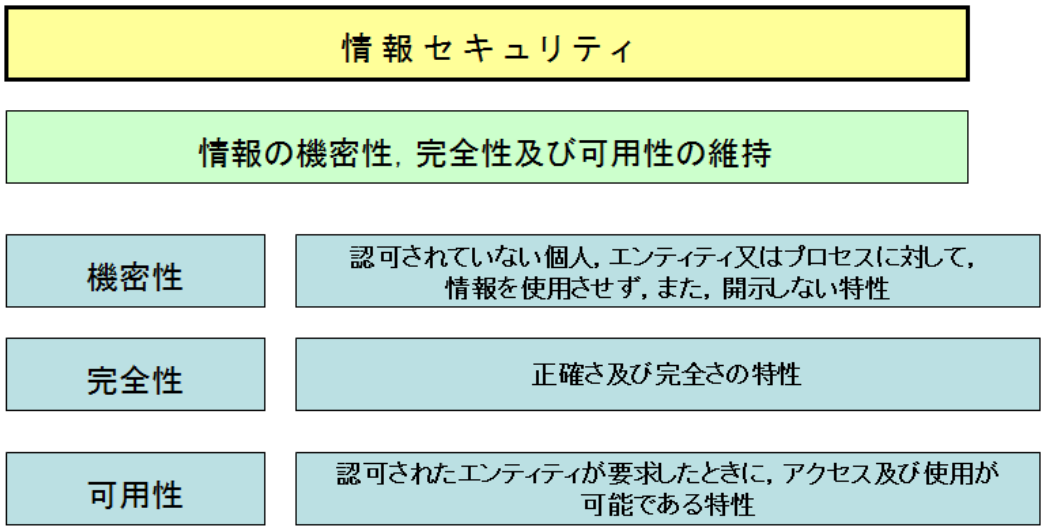


図 3-1　情報セキュリティの主な要素

「機密性」、「完全性」、「可用性」は、1992 年に発行された「OECD 情報セキュリティガイドラインに関する委員会勧告」[1]の附属文書「情報システムのセキュリティガイドライン」[2]（以下、「OECD ガイドライン」という。）において定義されて以来使われてきました。

> 情報システムの機密性、完全性及び可用性を阻害する危害（harm）から情報システムを保護すること
>
> （OECD ガイドライン:1992　より引用）

この 3 つの「～性」は、その頭文字をとって「情報セキュリティの C.I.A」と言われることがあります。
JIS Q 27000 では、機密性、完全性、可用性を以下のように定義しています。

> 2.12　機密性（confidentiality）
> 認可されていない個人，エンティティ又はプロセス（2.61）に対して，情報を使用させず，また，開示しない特性。
>
> （JIS Q 27000:2014　2 用語及び定義　より引用）

なお、「エンティティ」は、「実体」や「主体」とも言います。ここでは、情報を使用する組織及び人、情報を扱う設備、ソフトウェア及び物理的媒体などを意味します。

情報の機密性は、「情報を漏洩しないようにする」ことにより確保されます。

> 2.40　完全性（integrity）
> 正確さ及び完全さの特性。
>
> （JIS Q 27000:2014　2 用語及び定義　より引用）

完全性には 2 つの意味があります。1 つは情報そのものの完全性を確保することです。これは「情報が改ざんされないようにする」ことに関連します。
もう 1 つは情報処理の方法の完全性です。これは、「情報システムが勝手に変更されないようにする」ことや「情報の取扱いが手順化されていて、その手順が確実に順守されるようにする」こと等に関連します。

> 2.9　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。
>
> （JIS Q 27000:2014　2 用語及び定義　より引用）

可用性は、「自然災害やシステムダウンなどにより、情報が使えなくなること」から保護することに関連します。

なお、その他の特性については、JIS Q 27000 に定義があり、以下のようになっています。

> 2.8　真正性（authenticity）
> エンティティは，それが主張するとおりのものであるという特性。

[1] Recommendation of the Council concerning Guidelines for the Security of Information Systems(adopted by the Council at its 793rd Session of 26-27 November 1992)
[2] Guidelines for the Security of Information Systems,26 November 1992

2.54 否認防止（non-repudiation）
主張された事象又は処置の発生，及びそれを引き起こしたエンティティを証明する能力。

2.62 信頼性（reliability）
意図する行動と結果とが一貫しているという特性。

（JIS Q 27000:2014 2 用語及び定義 より引用）

３．１．２ 情報セキュリティマネジメントシステム

情報セキュリティマネジメントシステム（ISMS）とは、企業や組織の目的を達成するために、情報セキュリティ分野におけるマネジメント実践のための仕組みであり、リスクマネジメントをその中心におくものです。マネジメントシステムを JIS Q 27000 では以下のように説明しています。

2.46 マネジメントシステム（management system）
方針（2.60），目的（2.56）及びその目的を達成するためのプロセス（2.61）を確立するための，相互に関連する又は相互に作用する，組織（2.57）の一連の要素。
注記 1 一つのマネジメントシステムは，単一又は複数の分野を取り扱うことができる。
注記 2 システムの要素には，組織の構造，役割及び責任，計画，運用などが含まれる。
注記 3 マネジメントシステムの適用範囲としては，組織全体，組織内の固有で特定された機能，組織内の固有で特定された部門，複数の組織の集まりを横断する一つ又は複数の機能，などがあり得る。

（JIS Q 27000:2014 2 用語及び定義 より引用）

また、マネジメントシステムを導入することにより、以下のような効果が期待されます。

- **組織の目的を明確にし、確実に伝達し実施されるようになる**
- **実施の状況を継続的に管理し、適正な水準に保つ**
- **定期的な見直しを実施し、対策や実施の体制等を柔軟に改善できる**
- **社会環境や要請を認識し、組織の目的に反映できる**

ISMS は、情報セキュリティに関するマネジメントシステムです。ISMS の確立とは、企業や組織が所有し、管理、運用する情報及び情報に関連するエンティティに見合う対策の実施や、コンプライアンスの観点から法令等を順守し、それを維持するための枠組みを確立することを意味します。

情報セキュリティは、以下のように定義されていますので、情報セキュリティマネジメントシステムとは、「情報の機密性、完全性及び可用性の維持に関する、方針、目的及びその目的を達成するためのプロセスを確立するための、相互に関連する又は相互に作用する、組織の一連の要素。」となります。

2.33 情報セキュリティ（information security）
情報の機密性（2.12），完全性（2.40）及び可用性（2.9）を維持すること。
注記 さらに，真正性（2.8），責任追跡性，否認防止（2.54），信頼性（2.62）などの特性を維持することを含めることもある。

（JIS Q 27000:2014 2 用語及び定義 より引用）

３．１．３　情報セキュリティ事象、及び情報セキュリティインシデント

JIS Q 27002:2014 において、「16 情報セキュリティインシデントの管理」として 1 つの箇条にまとめられています。JIS Q 27000 では、以下のとおり関連した用語の定義が定められています。

> 2.35　情報セキュリティ事象（information security event）
> 情報セキュリティ方針への違反若しくは管理策の不具合の可能性，又はセキュリティに関係し得る未知の状況を示す，システム，サービス又はネットワークの状態に関連する事象（2.25）。
>
> 2.36　情報セキュリティインシデント（information security incident）
> 望まない単独若しくは一連の情報セキュリティ事象（2.35），又は予期しない単独若しくは一連の情報セキュリティ事象であって，事業運営を危うくする確率及び情報セキュリティ（2.33）を脅かす確率が高いもの。
>
> 2.37　情報セキュリティインシデント管理（information security incident management）
> 情報セキュリティインシデント（2.36）を検出し，報告し，評価し，応対し，対処し，更にそこから学習するためのプロセス（2.61）。
>
> （JIS Q 27000:2014　2 用語及び定義　より引用）

詳細は、「JIS Q 27002:2014　16 情報セキュリティインシデントの管理」及び「ISO/IEC 27035 Information Security Incident Management」を参照して下さい。

参考:「ISO/IEC 27035 Information Security Incident Management（情報セキュリティインシデントの管理））」の概要

JTC1/SC27 では、情報セキュリティインシデントの管理に関して ISO/IEC 27035 という国際規格を発表しています。
これは、以下のような点から助言及び指針を与えています。

情報セキュリティ方針群または管理策のみでは、情報、情報システム、サービスまたはネットワークの包括的な保護を保証できないでしょう。管理策が実施されていたとしても、ぜい弱性はまだ残っているでしょうし、それによって情報セキュリティはその効果を失う可能性があり、情報セキュリティインシデントが起きる可能性があります。これは、組織の事業の運営に、直接及び間接の負の影響を与える可能性があります。さらに、以前には特定されなかった脅威が新たに出現するであろうことも避けられません。

そのようなインシデントに対処することに組織の用意が不十分であれば、どのような対応も効果を少なくし、また事業への負の影響の可能性の程度を増加させるでしょう。

したがって、情報セキュリティに関して真剣に取り組んでいる組織はいずれも、次の事項を行うために系統立てて計画したアプローチをもつことが本質的に重要となります。

- 情報セキュリティインシデントの検知、報告及びアセスメント
- 影響に対する予防策、その軽減策、及び影響から回復するための適切な管理策を含む、情報セキュリティインシデントへの対応（例えば、危機管理領域のサポート）
- もし侵されると、情報セキュリティ事象及び情報セキュリティインシデントが引き起こされる、情報セキュリティぜい弱性の報告、並びにその適切なアセスメント及び取扱い
- 情報セキュリティインシデント及びぜい弱性からの学習、予防策の整備、及び情報セキュリティインシデント管理に対する包括的アプローチへの改善

ISO/IEC 27035 は、その箇条 4～9 で、情報セキュリティインシデント管理に関する手引を提供しています。この規格では、「情報セキュリティインシデント管理」という用語は、情報セキュリティインシデントのみではなく情報セキュリティぜい弱性についても、その管理を行うことに言及するように使用されています。

（ISO/IEC 27035　序文　より）

３．２　リスクマネジメントに関する用語

３．２．１　リスクマネジメント

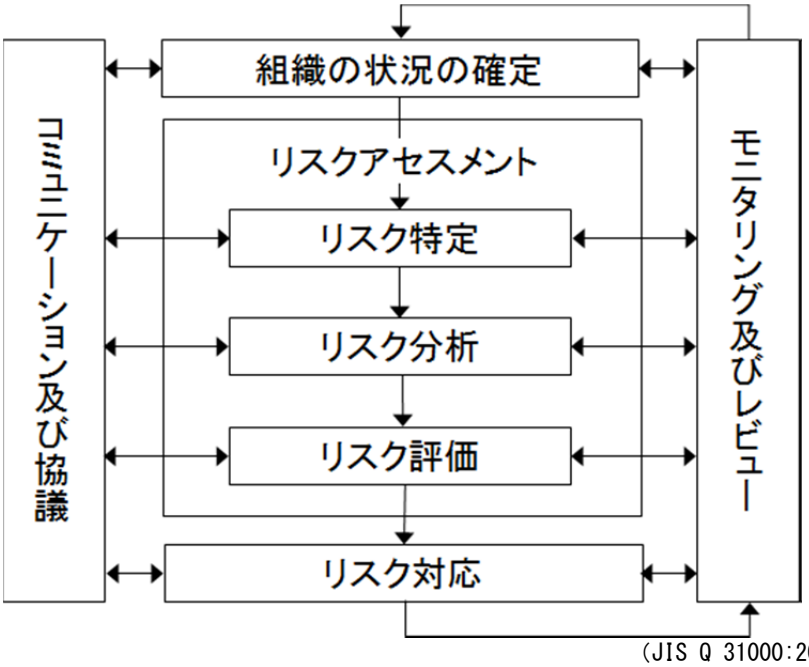
JIS Q 27000 では、リスクマネジメントについては以下のように定義しています。

2.76 リスクマネジメント（risk management）
リスク（2.68）について，組織（2.57）を指揮統制するための調整された活動。
（JIS Q 0073:2010 の 2.1 参照）

（JIS Q 27000:2014　2 用語及び定義　より引用）

ISMS の目的は、リスクマネジメントプロセスを適用することによって情報の機密性、完全性及び可用性を保護し、かつ、リスクを適切に管理しているという信頼を利害関係者に与えることにあります。
JIS Q 31000:2010 のリスクマネジメントの活動及びプロセスを導入し、JISQ 27001:2014 の要求事項として、ISMS に統合したテキストとしています。

図 3-2 は、プロセス間の情報の流れを示しています。



（JIS Q 31000:2010 より引用）

図 3-2　JIS Q 31000:2010 のリスクマネジメント

４．組織の状況

JIS Q 27001:2014 の「4 組織の状況」では、組織をとりまく内外の状況や利害関係者のニーズ及び期待を理解、決定し、それらを考慮に入れたうえで ISMS の適用範囲を定めることが求められています。例えば、４章の内容を例示すると図 4-1 のようになります。

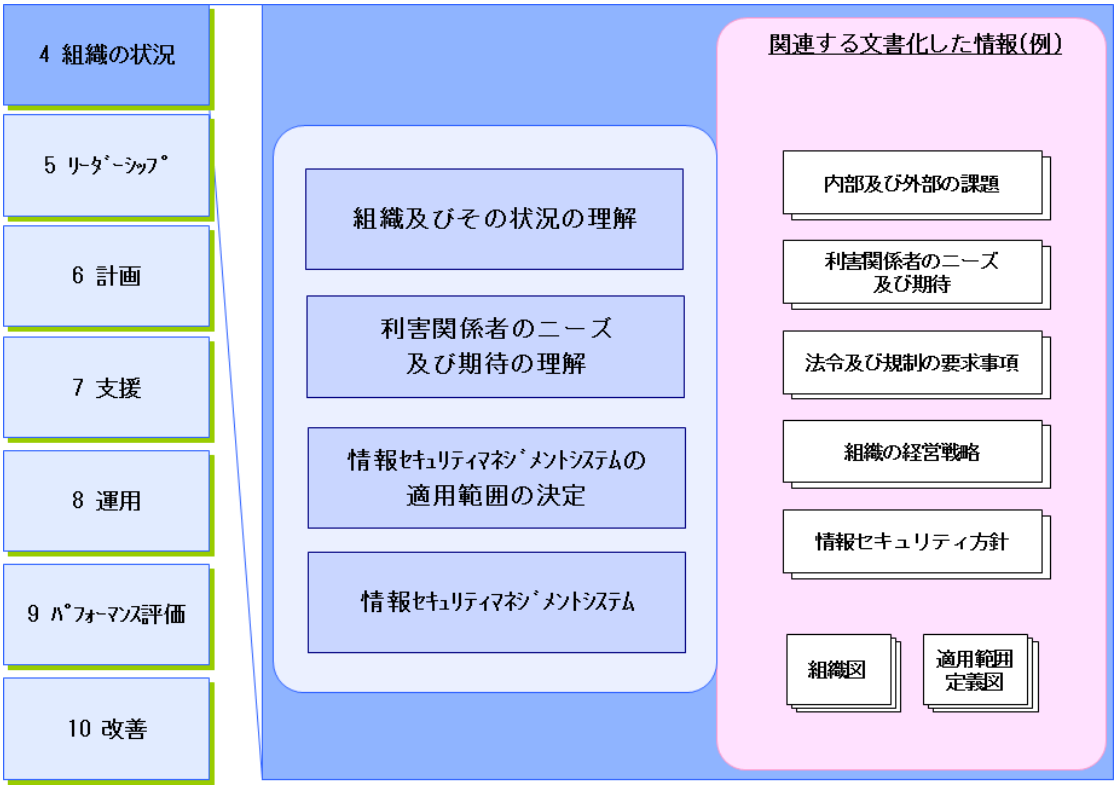


図 4-1　組織の状況の理解（事例）　注）文書名は全て例示

４．１　組織及びその状況の理解

ISMS の重要な目的の 1 つは、その活動が予防的な役割をもつことです。JIS Q 27001 では、4.1 と 6.1 の 2 つの要求事項が、「予防的活動」というコンセプトをカバーすると考えられます。4.1 は「組織」の「目的に関連し、意図した成果（規格、プロセスなどの適用の結果）を達成する組織の能力に影響を与える、外部及び内部の課題」を評価することを要求し、6.1 は、「ISMS が、その意図した成果を達成できることを確実にするため、望ましくない影響を防止又は低減するため、及び継続的改善を達成するため、それらに対処するリスク及び機会の決定」を求めています。ここでは、4.1 の要求事項が意味するところを説明し、6.1 の要求事項については、本ガイドの６章で説明します。

組織は，組織の目的に関連し，かつ，その ISMS の意図した成果を達成する組織の能力に影響を与える，外部及び内部の課題を決定しなければならない。

注記　これらの課題の決定とは，JIS Q 31000:2010 の 5.3 に記載されている組織の外部状況及び内部状況の確定のことをいう。

（JIS Q 27001:2014　4.1 組織及びその状況の理解　より引用）

ここでは、4.1 で使用されている用語および表現のうち、留意すべきものについて説明します。まず、「組織」については次のように定義されています。組織の定義自体に「目的を達成するため、独自の機能をもつ」という表現があることに注目して下さい。

2.57 組織（organization）
自らの目的（2.56）を達成するため，責任，権限及び相互関係を伴う独自の機能をもつ，個人又は人々の集まり。
注記 組織という概念には，法人か否か，公的か私的かを問わず，自営業者，会社，法人，事務所，企業，当局，共同経営会社，非営利団体若しくは協会，又はこれらの一部若しくは組合せが含まれる。ただし，これらに限定されるものではない。

（JIS Q 27000:2014 2 用語及び定義 より引用）

「ISMS の意図した成果」は、その ISMS を確立しようとする組織が定めるものであり、ISMS 導入の目的及び効果を考慮すると、以下を含むものであると考えられます。

－リスクマネジメントプロセスを適用することによって情報の機密性、完全性及び可用性を維持する。
－リスクを適切に管理しているという信頼を利害関係者に与える。

また、組織の「外部及び内部の課題の決定」とは、組織の外部状況及び内部状況の確定とされていますが、外部状況、内部状況とは、以下に示されるものとされています。

2.27 外部状況（external context）
組織が自らの目的を達成しようとする場合の外部環境。
（JIS Q 0073:2010 の 3.3.1.1 参照）
注記 外部状況には，次の事項を含むことがある。
― 国際，国内，地方又は近隣地域を問わず，文化，社会，政治，法律，規制，金融，技術，経済，自然及び競争の環境
― 組織（2.57）の目的（2.56）に影響を与える主要な原動力及び傾向
― 外部ステークホルダ（2.82）との関係並びに外部ステークホルダの認知及び価値観

（JIS Q 27000:2014 2 用語及び定義 より引用）

2.42 内部状況（internal context）
組織が自らの目的を達成しようとする場合の内部環境。
（JIS Q 0073:2010 の 3.3.1.2 参照）
注記 内部状況には，次の事項を含むことがある。
― 統治，組織体制，役割及びアカウンタビリティ
― 方針，目的及びこれらを達成するために策定された戦略
― 資源及び知識としてみた場合の能力（例えば，資本，時間，人員，プロセス，システム，技術）
― 情報システム，情報の流れ及び意思決定プロセス（公式及び非公式の両方を含む。）
― 内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観
― 組織の文化
― 組織が採択した規格，指針及びモデル
― 契約関係の形態及び範囲

（JIS Q 27000:2014 2 用語及び定義 より引用）

組織に影響を及ぼし、その情報セキュリティの方向性を決定する状況は、全て考慮することが望まれます。その原因は組織内にあり、多少とも管理可能な場合もあれば、組織外に

あるために一般に交渉が困難な場合もあります。資源の制約（予算、要員）及び緊急事態の状況は、もっとも重要なものの１つです。

（１）外部状況

外部状況には、例えば、次のようなものが考えられます。

政治的性格の状況

この状況は、行政府、公共機関又はより広範に、政府の決定を適用しなければならない組織にかかわるものです。この状況は通常、戦略又は運用の方向性に関して、政府省庁又は意思決定機関が下す決定であり、適用することが望ましいものです。

例えば、請求書又は管理文書のコンピュータによる処理によって、内部統制などに関するような情報セキュリティ問題が発生します。

戦略的性格の状況

状況は、組織の構成又は方向性の変更計画又は変更の可能性からも発生することがあります。この状況は、組織の戦略計画又は運用計画の中で表されます。例えば、取扱いに慎重を要する情報の共有に関する国際協力のためには、安全な情報交換に関する合意が必要となります。

地勢的状況

組織の構成及び/又は目的は、国土全体又は外国に広がったサイトの分布のような固有の状況を生み出すことがあります。郵便事業、大使館、銀行、大手企業グループの子会社などの例が挙げられます。

経済及び政治動向から発生する状況

組織の運営は、ストライキ又は国内外の危機のような特別の事象によって大きな変更を余儀なくされることがあります。

例えば、ある種のサービスは、重大な危機のときも継続して運営されることが望まれます。

方法に関連する状況

プロジェクト計画、要件定義、開発などの側面には、組織のノウハウに適した方法を用いる必要があります。例えば、この種の代表的な状況は、組織の法的義務をセキュリティ方針に盛り込む必要性などがあります。

文化的性格の状況

組織によっては、社会的慣習、宗教、労働習慣又は主要な事業が組織内に固有の「文化」を生み出し、これがセキュリティ管理策と相容れないということが起こることがあります。この文化は、要員が一般的に拠り所とする枠組みであり、これは教育、指示、専門家としての経験、仕事以外の経験、意見、哲学、信念、社会的地位など、数多くの側面によって決定されます。

（２）内部状況

次に、内部状況について説明します。

JIS Q 31000:2010 の 5.3 によれば、組織は、目的を明確に表現し、リスクの運用管理において考慮するのが望ましい外部及び内部の要因を定め、それ以降のプロセスに関する適用範囲及びリスク基準を設定することができます。

この要因には、リスクマネジメントの枠組みの設計において検討する要因と類似したものも多いのですが、リスクマネジメントプロセスに関して組織の状況を確定する場合には、

要因を一層詳細に考慮する必要があります。特に、情報セキュリティのリスクマネジメントプロセスの適用範囲とどのように関係し合うのかについて考慮する必要があります。例えば、要因の代表的な例として、情報及び情報に関連する資産、さらには、事業、組織、所在地、技術などがあります。

組織の内部状況の調査では、組織のアイデンティティを定義する特徴的な要素を確認することが該当します。調査は、組織の目的、事業、使命、価値及び戦略を対象とします。これらは、その発展に寄与する要素（下請負契約など）と合わせて特定することが望ましいようです。

この活動の難しさは、組織がどのように構成されているかを正確に理解することにあります。その実際の構成を特定すれば、組織の目的達成のうえでの各事業部の役割及び重要性の理解が得られます。

４．２　利害関係者のニーズ及び期待の理解

JIS Q 27001:2014 は、組織が、ISMS に関する利害関係者を特定し、さらに、それらの利害関係者の、情報セキュリティに関連するニーズと期待（要求事項の定義）を特定することを求めています。

> 組織は，次の事項を決定しなければならない。
> a) ISMS に関連する利害関係者
> b) その利害関係者の，情報セキュリティに関連する要求事項
> 注記 利害関係者の要求事項には，法的及び規制の要求事項並びに契約上の義務を含めてもよい。
>
> （JIS Q 27001:2014　4.2 利害関係者のニーズ及び期待の理解　より引用）

利害関係者は、以下のように定義されています。

> 2.41　利害関係者（interested party）
> ある決定事項若しくは活動に影響を与え得るか，その影響を受け得るか，又はその影響を受けると認識している，個人又は組織（2.57）。
>
> （JIS Q 27000:2014　2 用語及び定義　より引用）

利害関係者として、取引先の顧客、事業に必要なサービスを提供する供給者、組織の従業員、親会社など、組織の情報セキュリティの取組みに期待している者、情報セキュリティの取組みによって影響を受ける者などを、広い視点で洗い出す必要があります。
利害関係者を決定するとともに、利害関係者のニーズなどを考慮し、情報セキュリティに関連する要求事項を決定します。例えば、取引先の顧客が国や地方自治体であり、その機密性の高い情報を取り扱うのであれば、国や地方自治体からの情報セキュリティに関する要求事項を考慮しなければならないことになります。

利害関係者とは何かをより理解するために、同じマネジメントシステムである JIS Q 9000:2006 の定義「組織のパフォーマンス及び成功に利害関係をもつ人又はグループ」を参照することも有効です。この定義によると、顧客、投資家、所有者、供給者、銀行家、組合、パートナ又は社会等といった組織外部の人々のみならず、組織内の人々等を含みその対象は広範囲に及びます。
ここで、組織とは、責任、権限及び相互関係が取り決められている人々及び施設の集まりで、例えば、会社、法人、事業所、企業、団体、慈善団体、個人業者（sole trader）、協

会、若しくはこれらの一部又は組合せのことです。また、グループとは、1 つの組織、その一部又は複数の組織のこともあります。

3.3.5　顧客（customer）
製品（3.4.2）を受け取る組織（3.3.1）又は人。
　例　消費者，依頼人，エンドユーザ，小売り業者，受益者及び購入者
　注記　顧客は，組織の内部又は外部のいずれでもあり得る。

3.3.6　供給者（supplier）
製品（3.4.2）を提供する組織（3.3.1）又は人。
　例　製品の生産者，卸売業者，小売り業者，納入業者，サービス提供者又は情報提供者
　注記 1　供給者は，組織の内部又は外部のいずれでもあり得る。
　注記 2　契約関係においては，供給者は“契約者”と呼ばれる。

（JIS Q 9000:2006　3 用語及び定義　3.3 組織に関する用語　より引用）

JIS Q 27001:2014 における利害関係者という用語は、JIS Q 31000:2010 において使用されるステークホルダと同じ意味と考えられます。このことは、認証基準の 4.1 の注記で、JIS Q 31000:2010（ISO 31000:2009）の 5.3 が参照されており、そこで、ステークホルダの表現が使用されていることから分かります。

JIS Q 31000:2010 によれば、リスクマネジメントは、次のような重要なステークホルダのニーズを満たすことを意図しています。これは、リスクマネジメントに関する組織の活動を行う、利害関係者に言及しています。

a）組織の中でリスクマネジメント方針の開発に責任をもつ人
b）リスクが、組織全体又は特定の領域、プロジェクト若しくは活動で、効果的に運用管理されていることを確実にすることにアカウンタビリティをもつ人
c）リスクの運用管理において、組織の有効性を評価する必要のある人
d）規格、指針、手順及び実務基準の特定の内容について、全体としてでも又は部分的にでも、リスクをどのように運用管理すべきかを設定しているこれらの文書の開発者

このように、利害関係者には、外部の利害関係者と内部の利害関係者が含まれます。それぞれ、JIS Q 27000 の用語及び定義、2.27 外部の状況、2.42 内部の状況において、外部ステークホルダ、内部ステークホルダとして言及されています。
また、法的及び規制の要求事項、契約上の義務は、ISMS の利害関係者の要求事項に含まれます。

４．３　情報セキュリティマネジメントシステムの適用範囲の決定

ISMS の構築・運用を考慮する際、ISMS の適用範囲及び境界を検討します。

4.3　情報セキュリティマネジメントシステムの適用範囲の決定
組織は，ISMS の適用範囲を定めるために，その境界及び適用可能性を決定しなければならない。
この適用範囲を決定するとき，組織は，次の事項を考慮しなければならない。
a）4.1 に規定する外部及び内部の課題
b）4.2 に規定する要求事項
c）組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係
ISMS の適用範囲は，文書化した情報として利用可能な状態にしておかなければならない。

（JIS Q 27001:2014　4.3 情報セキュリティマネジメントシステムの適用範囲の決定　より引用）

組織として真に効果的な情報セキュリティマネジメントシステムを構築、運用するためには、重要な情報及び情報に関連する資産の取扱いが適正に保たれるのに必要な範囲を、1つの組織体としてなりたつように、ISMS の適用範囲を確定することが必要です。

企業全体を 1 つのマネジメントシステムとして適用範囲とすることも可能ですし、1 つの事業部門を適用範囲にすることもできます。また、顧客に提供する「サービス」のように、複数の部門（部門全体または一部）にまたがった横断的なマネジメントシステムを 1 つの組織体として適用範囲とすることも可能です。

適用範囲を決定する上で重要なことは、1 つのマネジメントとして包括的かつ網羅的であること、適用範囲の境界線が明確で、その適用範囲が、組織として自らの目的を達成するため、責任・権限及び相互関係を伴う独自の機能をもつものであること、並びにリスクマネジメントの観点で合理的に説明可能であることです。例えば、守るべき重要な情報及び情報に関連する資産、並びに情報セキュリティに関する主要な活動及びサイト（事業所）は、適用範囲に含まれていなければなりません。

JIS Q 27001：2014 では、適用範囲を決定するにあたり、4.1 で規定する「外部及び内部の課題」、4.2 で規定する「利害関係者の要求事項及びその利害関係者の情報セキュリティ要求事項」、及び「適用範囲とする組織の行う活動と適用範囲外とした組織の活動の関係」を考慮した観点から検討し、適用範囲の境界とその適用範囲の適用可能性を決定することを要求しています。

例えば、具体的な観点の例としては、従来の JIS Q 27001:2006 の 4.2.1a）で要求されていた事項も含めて、4.1 で示されている外部の状況、内部の状況、及び 4.2 で示されている利害関係者の要求事項を考慮する必要があります。なかでも、重要な事項としては、以下が考えられます。

- **情報及び情報に関連する資産**
- **事業**
- **組織**
- **所在地**
- **技術**

さらに、ISMS では、他の組織が実施する活動とのインタフェース及び依存関係を考慮することが求められています。事業を行う上で、あるプロセスを外部に委託することがあります。例えば、事業で利用している業務システムの開発・保守を外部に委託している場合、境界をどう定義し、どこまでを ISMS の適用範囲に含めるかが重要となります。外部委託について、JIS Q 27000:2014 では次のように定義しています。

> 2　用語及び定義
> 2.58　外部委託する（outsource）
> ある組織の機能又はプロセス（2.61）の一部を外部の組織（2.57）が実施するという取決めを行う。
> 注記　外部委託した機能又はプロセスはマネジメントシステム（2.46）の適用範囲内にあるが，外部の組織はマネジメントシステムの適用範囲の外にある。
>
> （JIS Q 27000:2014　2　用語及び定義　より引用）

業務プロセスの一部を外部委託する場合には、委託先で実施する活動とのインタフェースに注意して、適用範囲を決めることが重要です。

適用範囲は、その境界及び適用可能性として決定しますが、それに基づいて実施する内容により ISMS 構築・運用の作業負荷が大きく影響されます。

また、情報及び情報に関連する資産の洗い出しやリスクアセスメントなどの作業のみならず、プロセスの実施、管理策の適用や運用管理など適用対象の情報セキュリティ水準を維持する活動全般にも影響します。

４．３．１　適用範囲を定義する文書

JIS Q 27001:2014 では、適用範囲は、文書化した情報とすることが求められています。
適用範囲を定義する文書に含むことが望ましい事項としては、以下のような項目が挙げられます。

- **ISMS の適用範囲及び内容を確立するために用いたプロセス**
- **戦略上及び組織上の情況**
- **利害関係者に関する要求事項**
- **ISMS の適用範囲にある情報及び情報に関連する資産の特定**
- **（もしあれば）適用範囲外とした、情報及び情報に関連する資産、サイト、及び活動・プロセスと、その適用範囲外とした理由**
- **組織の活動と適用範囲外の組織の活動とのインタフェース・依存関係**
- **組織で採用した情報セキュリティのリスクマネジメントのアプローチ**
- **情報セキュリティのリスク基準（リスク受容基準を含む）**

これらの事項は、必ずしもその全てが文書化される必要はありませんが、適用範囲を定める際に考慮すべきポイントとして理解して下さい。適用範囲の文書化した情報は、決定後も ISMS の構築・運用のマネジメント及び作業の過程において常に見直されるべきものです。

４．３．２　適用範囲の定義の作業

JIS Q 27001:2014 に求められる適用範囲の定義に関する事項を、事例としてまとめると図 4-2 のようになります。

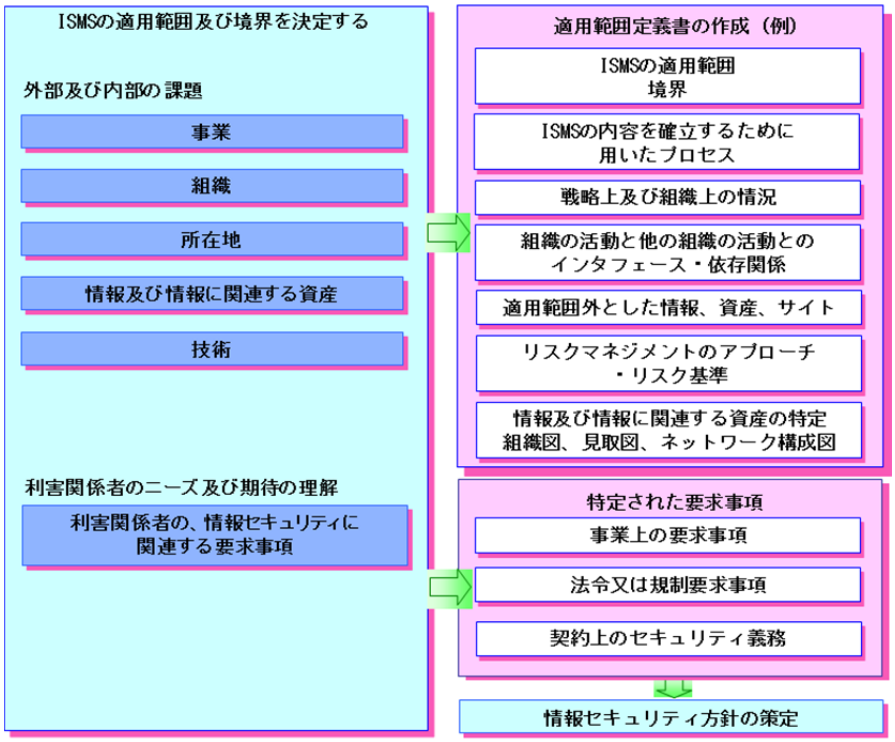


図 4-2　ISMS の適用範囲の定義（例）

適用範囲を定義し、該当するマネジメントシステムを検討する際に、同時に情報セキュリティ上の要求事項も明確になります。本ガイドの５章で述べる「情報セキュリティ方針」の策定にも、4.1 に規定する「外部及び内部の課題」、4.2 に規定する「利害関係者及びその情報セキュリティ要求事項」から導きだされる事項を考慮することが重要ですが、中でも、以下の事項について、明確化する必要があります。

- **事業上の要求事項**
- **法令又は規制の要求事項**
- **契約上のセキュリティ義務**

４．４　情報セキュリティマネジメントシステム

> 組織は，この規格の要求事項に従って，ISMS を確立し，実施し，維持し，継続的に改善しなければならない。
>
> （JIS Q 27001:2014　4.4 情報セキュリティマネジメントシステム　より引用）

ここでは、JIS Q 27001:2014 の要求事項に従って、組織内に ISMS を確立し、実施し、維持し、かつ、継続的に改善することが求められています。

有効なマネジメントシステムは、組織のプロセス管理の基盤として、「Plan-Do-Check-Act」のプロセスアプローチを採用するものであることが、従来の JIS Q 27001:2006 から継続して考慮されています（本ガイドの 0.3.3 参照）。
4.4 は、これに対応していて、どのようなプロセスで実施すべきかという表現ではなく、何を達成するべきかの見方としての要求事項を述べるという形式で、記述されたものです。

５．リーダーシップ

ISMS における様々な活動が実施されていることについて、トップマネジメントの果たすべき役割は非常に重要です。ISMS を推進し、関係者の意識向上を図るためには、トップマネジメントの強力なリーダーシップが不可欠なためです。
「5 リーダーシップ」では、トップマネジメントの果たすべき役割について定めており、例えば、これを例示すると図 5-1 のようになります。

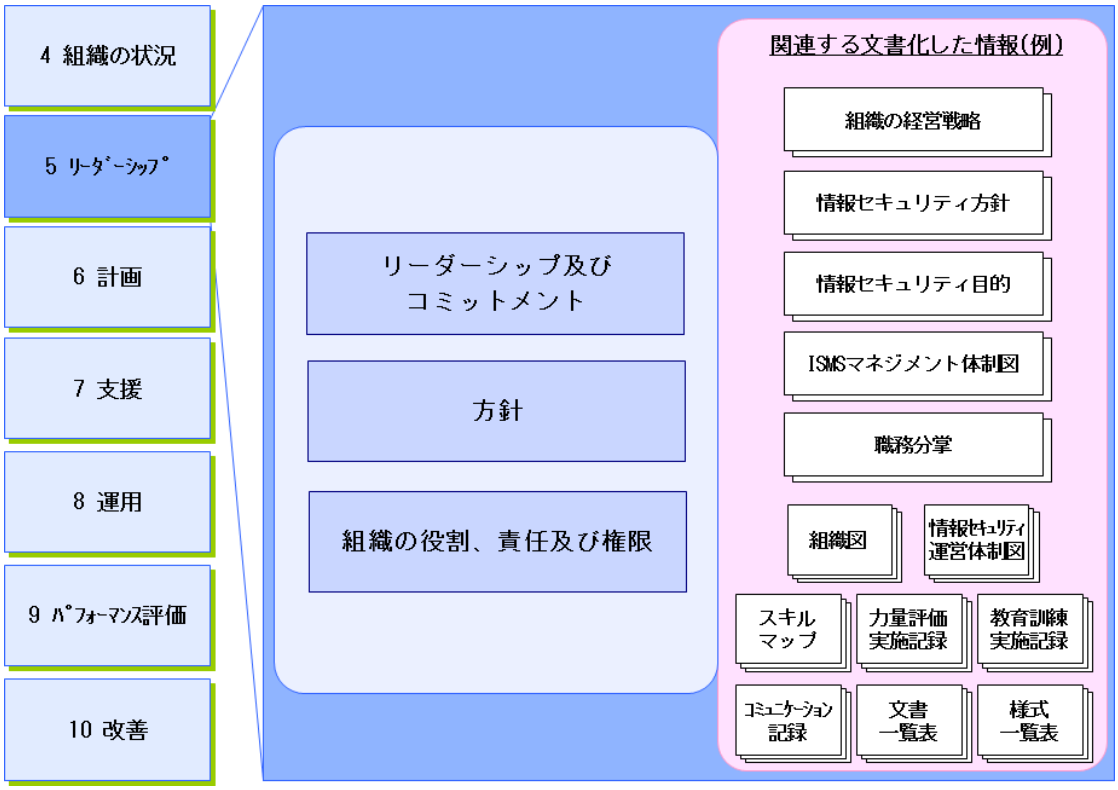


図 5-1　トップマネジメントの果たすべき役割（事例）　注）文書名は全て例示

５．１　リーダーシップ及びコミットメント

トップマネジメントの果たすべき重要な役割の 1 つにコミットメントがあります。ISMS の確立、実施、運用及び維持等に関与し、組織として情報セキュリティの実施責任を利害関係者に宣言する「コミットメント」は、執行権限を有するトップマネジメントにのみ実施する事が許されるからです。

JIS Q 27001:2014 では、トップマネジメントのコミットメントを次のように規定しています。

トップマネジメントは，次に示す事項によって，ISMS に関するリーダーシップ及びコミットメントを実証しなければならない。 a) 情報セキュリティ方針及び情報セキュリティ目的を確立し，それらが組織の戦略的な方向性と両立することを確実にする。 b) 組織のプロセスへの ISMS の要求事項の統合を確実にする。 c) ISMS に必要な資源が利用可能であることを確実にする。 d) 有効な情報セキュリティマネジメント及び ISMS の要求事項への適合の重要性を伝達する。 e) ISMS がその意図した成果を達成することを確実にする。 f) ISMS の有効性に寄与するよう人々を指揮し，支援する。 g) 継続的改善を促進する。

> h）その他の関連する管理層がその責任の領域においてリーダーシップを実証するよう，管理層の役割を支援する。
>
> （JIS Q 27001:2014　5 1 リーダーシップ及びコミットメント　より引用）

ここでは、トップマネジメントがどのような事項によってそのリーダーシップとコミットメントを実証しなければならないかについて定めています。

トップマネジメントはまず、ISMS の方向性を示す情報セキュリティ方針を確立することが求められます（情報セキュリティ方針については、「5.2 方針」で説明します。）。次に、情報セキュリティ目的を確立し、それらを組織の戦略的な方向性と両立させることが求められます。このように、情報セキュリティ方針・目的が組織の戦略的な方向性と一致していることは、ISMS を推進していく上でも、効果的な ISMS を構築する上でも重要な要因となります。

また、組織のプロセスへの ISMS 要求事項の統合を確実にすることも、トップマネジメントに求められています。これは、組織の戦略的な方向性と一致した情報セキュリティ目的の達成には、組織のプロセスに合った ISMS を導入することが重要となるためです。この統合が行われず、組織のプロセスと ISMS 要求事項のプロセスが別々になってしまうと、ISMS を運用することが組織にとって重荷になってしまい、導入した ISMS が形骸化してしまう恐れがあります。

そして、必要な資源を確保し、組織の従業員が ISMS 要求事項へ適合する意味を認識させ、ISMS の有効性に寄与するように従業員を支援することなどによって、ISMS への積極的な関与を示すことがトップマネジメントに求められています。これらは ISMS を運用していく上で重要な要因であり、「7.1 資源」、「7.3 認識」に関連してくる要求事項です。また、管理層が所属する部門・担当するプロジェクトなどでリーダーシップを発揮できるように、その役割を支援することも求められています。

最後に、トップマネジメントは、ISMS が意図した成果を達成できるように、自ら責任をもって推進していく必要があります。また、意図した成果が達成できない状況であれば、継続的に改善していくことに責任をもたなければなりません。
トップマネジメントについて、JIS Q 27000:2014 では次のように定義しています。

> 2.84　トップマネジメント（top management）
> 最高位で組織（2.57）を指揮し、管理する個人又は人々の集まり。
> 注記 1　トップマネジメントは、組織内で、権限を委譲し、資源を提供できる力をもっている。
> 注記 2　マネジメントシステム（2.46）の適用範囲が組織（2.57）の一部だけの場合，トップマネジメントとは，組織（2.57）内のその一部を指揮し，管理する人をいう。
>
> （JIS Q 27000:2014　2 用語及び定義　より引用）

ISMS を効果的に運用するためにも、「5 リーダーシップ」の要求事項を実施する権限をもつ人がトップマネジメントに就き、ISMS の運用に積極的に関与していく必要があります。

５．２　方針

JIS Q 27001:2014 では、トップマネジメントは、情報セキュリティ方針を確立することが求められています。

> トップマネジメントは，次の事項を満たす情報セキュリティ方針を確立しなければならない。
> a）組織の目的に対して適切である。
> b）情報セキュリティ目的（6.2 参照）を含むか，又は情報セキュリティ目的の設定のための枠組みを示す。
> c）情報セキュリティに関連する適用される要求事項を満たすことへのコミットメントを含む。
> d）ISMS の継続的改善へのコミットメントを含む。
>
> 情報セキュリティ方針は，次に示す事項を満たさなければならない。
> e）文書化した情報として利用可能である。
> f）組織内に伝達される。
> g）必要に応じて，利害関係者が入手可能である。
>
> （JIS Q 27001:2014　5.2 方針　より引用）

情報セキュリティ方針は、情報セキュリティに対する組織の意図を示し、方向付けをするものであり、組織の目的と整合をとる必要があります。

この情報セキュリティ方針では、「6.2 情報セキュリティ目的及びそれを達成するための計画策定」で決定する情報セキュリティ目的を含むか、又は情報セキュリティ目的の設定のための枠組みを示すことが求められています。6.2 では、情報セキュリティ目的は情報セキュリティ方針と整合することが求められており、組織にとって有益な情報セキュリティ目的を設定するためにも、ここで組織の事業目的に沿った情報セキュリティ方針を策定する必要があります。

そして、トップマネジメントは、自ら ISMS の運用に積極的に関与すること（コミットメント）を情報セキュリティ方針で表明しなければなりません。そのため、トップマネジメントが確立した情報セキュリティ方針を文書化して利用可能とし、組織内に伝達し、各従業員がそれに従って行動できるように組織内の意識を高めることが必要となります。逆に、各従業員が方針を理解せず、各々の感覚で情報セキュリティに取り組んでしまった場合、組織としての ISMS にほころびが生まれ、情報漏えいなどが起きてしまう可能性があります。また、利害関係者が必要に応じて情報セキュリティ方針を入手可能にしておくことも必要です。

従来の JIS Q 27001:2006 では、上位概念の ISMS 基本方針（ISMS policy）と下位概念の情報セキュリティ基本方針（Information security policy）の 2 つがありましたが、JIS Q 27001:2014 では、これらを区別することなく情報セキュリティ方針（Information security policy）となっています。JIS Q 27001:2014 では、方針は ISO のマネジメントシステム規格共通の要求事項になり、他のマネジメントシステムの方針と整合するような要求事項となっています。

５．２．１　情報セキュリティ方針の策定

情報セキュリティ方針を策定するためには、組織の状況の把握（例えば、組織の目的、事業、使命、価値観、事業遂行上の主要な原理及び行動規範、想定された適用範囲に含まれる組織の人員構成、規程類の整備状況、情報及び情報に関連する資産の保有状況、情報シ

ステムの利用状況等、広範に情報と情報関連の資産とそれを取り巻く環境）、並びに利害関係者からの要求事項を確認する必要があります。

情報セキュリティ方針は、トップマネジメントの情報セキュリティマネジメントに対する基本的な考え方を示したものです。同時に、組織として情報セキュリティに関する要求事項に対して責任を負うという、意思表示の位置付けとして重要な文書です。その内容は、企業としての使命、目的を表明した経営方針（ビジョン）や、行動規範（価値観）と整合性がとられている必要があります。情報セキュリティ目的を含むか、又は情報セキュリティ目的の設定のための枠組みを示す必要があります。

また、「情報セキュリティに関連する、組織として適用可能とされている情報セキュリティ要求事項を満たすこと」、及び「ISMS の継続的改善」への誓約（コミットメント）がなされることが示される必要があります。
情報セキュリティ方針は、文書として利用可能とし、組織全体に伝えて知ってもらうようにすることが重要です。

５．２．２　情報セキュリティ方針の策定事例

情報セキュリティ方針は、情報セキュリティに対する組織の方向付けをするものです。

JIS Q 27002:2014 の「5.1.1 情報セキュリティのための方針群」には、最上位の情報セキュリティ方針に含まれる事が望ましい内容が提示されています。以下は、それを参考にして策定した情報セキュリティ方針の事例です。

（情報セキュリティ方針、策定事例）
情報セキュリティ方針文書では，トップマネジメントの責任を明記し，情報セキュリティの管理に対する組織の取組み方を示すことが望ましい。この情報セキュリティ方針文書には，次の事項に関する記述を含むことが望ましい。

a）情報セキュリティの定義，情報セキュリティ目的及び適用範囲，並びに情報共有を可能にする基盤としてのセキュリティの重要性
b）事業戦略及び事業目的に沿った情報セキュリティ目的及び原則を支持するトップマネジメントの意思を示す記述
c）リスクアセスメント及びリスクマネジメントの構造を含む，管理目的及び管理策を設定するための枠組み
d）組織にとって特に重要な，セキュリティの個別方針，原則，標準類及び順守の要求事項の簡潔な説明。これらには，次のようなものがある。
　1）法令，規制及び契約上の要求事項の順守
　2）セキュリティ教育，訓練及び意識向上に関する要求事項
　3）事業継続管理
　4）情報セキュリティ方針群への違反に対する処置
e）情報セキュリティインシデントを報告することも含め，情報セキュリティマネジメントに関する一般的な責任及び特定の責任の定義
f）情報セキュリティ方針を支持する文書（例えば，特定の情報システムのためのより詳細なセキュリティ方針及び手順，又は利用者が順守することが望ましいセキュリティ規則）への参照

この情報セキュリティ方針は，想定する読者にとって，適切で，利用可能で，かつ，理解しやすい形で，組織全体にわたって利用者に知らせることが望ましい。

これらの事項は、例示であり、必ずしもその全てが策定する方針に含まれる必要はありません。4.3 で定義した適用範囲により内容が変わることも想定されます。
上記の策定事例は、方針の内容を検討する際に考慮すべきポイントを示すものです。

５．３　組織の役割、責任及び権限

トップマネジメントは，情報セキュリティに関連する役割に対して，責任及び権限を割り当て，伝達することを確実にしなければならない。 トップマネジメントは，次の事項に対して，責任及び権限を割り当てなければならない。 a)　ISMS が，この規格の要求事項に適合することを確実にする。 b)　ISMS のパフォーマンスをトップマネジメントに報告する。 注記　トップマネジメントは，ISMS のパフォーマンスを組織内に報告する責任及び権限を割り当ててもよい。 （JIS Q 27001:2014　5.3 組織の役割，責任及び権限　より引用）

組織が自らの情報セキュリティ目的に向かって活動するためには、役割を決め、それに対する責任及び権限を割り当てることは重要なことです。自分が ISMS でどのような役割を担い、どこまでする責任があるのか明確になっていなければ、各従業員は何をしたら良いか迷うか、何もせずに終わってしまうでしょう。このような状況に陥らないためにも、トップマネジメントが情報セキュリティに関連する役割を決め、それに対する責任と権限を割り当てたことを組織内に周知する必要があります。

この責任及び権限について、JIS Q 27001:2014 では上記 a)及び b)が求められています。その具体例としては、次の 5.3.1、5.3.2 のような取組みが考えられ、実践され効果を上げている組織もあります。

５．３．１　ISMS 構築・運用のための組織体制

トップマネジメントは、情報セキュリティに関連する役割に対して、責任及び権限を明確にし、これを割り当て、ISMS を実施・運用する組織体制を確立し、情報セキュリティを確立し維持するために、周知が必要な利関係者に確実に伝達する仕組みを構成しなければなりません。

ISMS を構築・運用する組織の人選においては、様々な情報の取扱いに関する問題を討議するのに必要かつ十分な範囲から人を召集すると同時に、実際の ISMS 運用の体制について考慮し、関連部門から広くメンバーを募るべきです。

ISMS で取り扱う情報セキュリティとは、単に「情報リスク」、「IT リスク」を考慮することにとどまりません。また、マネジメントシステムの局面も、日常の管理に属する部分の他、リスクが顕在化した後の被害を最小限にとどめるための対応なども要求されています。このような包括的・網羅的な「管理」を実現するためには、適用範囲に含まれる現場組織だけではなく、法務部門、総務部門など会社組織全体を横断する、関連する管理層への働きかけ、組織の再構成、及び人材の登用が求められます。

図 5-2 は、ISMS 構築・運用のための組織体制の一例です。
この例を基に、主要な組織の役割と責任を紹介します。

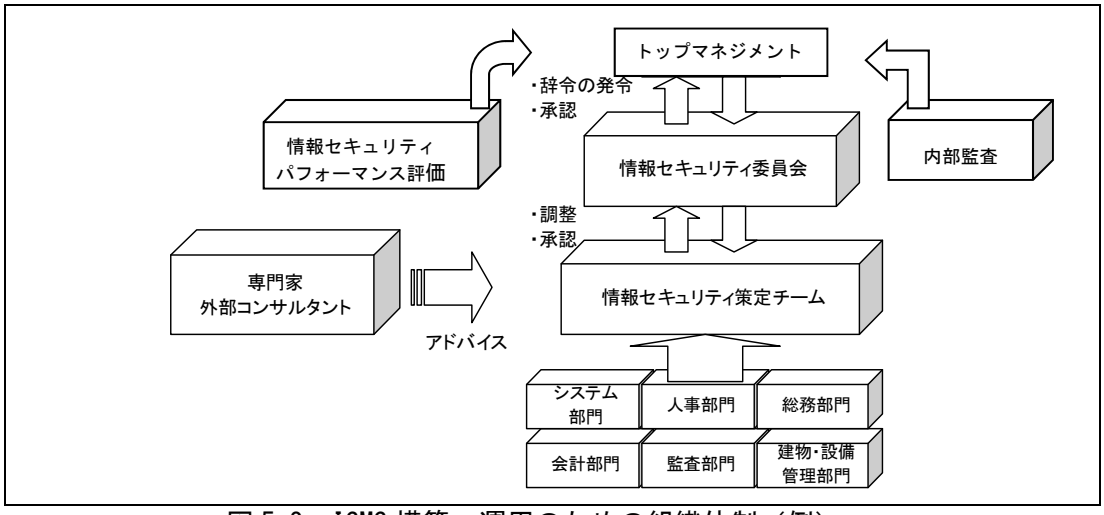


図 5-2　ISMS 構築・運用のための組織体制（例）

① 情報セキュリティ委員会の役割

情報セキュリティ委員会を中心とした体制で策定される ISMS 関連文書は、委員会だけでなく組織のトップマネジメントにより承認された規程として必要に応じて関係者に周知し、定期的に見直しを行います。こちらは、主として関連する管理層のメンバーで構成され、マネジメントレビューを行う仕組みともなります。

この委員会は、組織の保有する情報及び情報に関連する資産の取扱いに責任を持ち、情報セキュリティの方向性を提言できるだけの情報セキュリティに関する理解と実行力をもった組織であるべきです。情報セキュリティのリスク所有者としての役割を担う組織ともなります。

情報セキュリティ委員会は、組織において ISMS の中心的役割を負います。以下は情報セキュリティ委員会の役割の例示です。

- **リスクマネジメントのための環境整備について検討機関となる**
- **ISMS 関連文書の策定時には内容について実質的な決定機関となる**
- **導入段階の ISMS を推進する各種施策や改訂を検討する**
- **運用段階でセキュリティ問題等が発生した場合の検討機関となる**
- **ISMS 運用の評価結果に基づいた改善について検討機関となる**

② 情報セキュリティ策定・運用チームの役割

ISMS の構築・運用の実務を担当する策定・運用チームは、適用範囲内の重要な情報及び情報に関連する資産について広く現状を把握し、その取扱いを検討するのに十分な知見をもつメンバーで構成されるべきです。例えば、情報及び情報に関連する資産の取扱い方法の決定にあたり、適用範囲内の部署間での見解の相違や、利害関係の調整が必要になる場合があり、策定・運用チームはそのような摩擦の調整役として、部門間の枠をこえて当事者に対してうまく働きかけることが求められます。この場合は、高いセキュリティ知識も当然必要ですが、調整能力や経験に基づくコミュニケーションのスキルも重要になります。組織の規模によりますが、①と②を一体の組織として運営する場合も考えられます。

③ 専門家・外部コンサルタント

ISMS の構築作業は、組織が自前で（できれば専任の）要員を確保した上で進めるべきです。しかし、「情報セキュリティ」の対象とする範囲は「IT 技術」、「経営的な判断」や「ビジネスへの理解」など、求められる知識や経験は多岐にわたり、これらの領域をバランスよく俯瞰的に見通す力量が求められます。

組織の主要な業務はその業務に携わっている人が一番知っているものですが、時としてミクロな視点での判断に終始してしまうことがあります。附属書 A に言及されている「外部の専門家・コンサルタントの登用」は、この判断にマクロな視点を与え、また最新の情報を提供してくれる窓口の機能が期待されます。情報セキュリティ委員会へのオブザーバ参加、規定文書のレビューや監査計画策定など、必要な局面で彼らのもつ専門知識を効果的に活用することも良いと思います。しかし、外部の専門家やコンサルタントはあくまでも ISMS の構築・運用の支援を行うものであり、当事者ではないので、意思決定を含めた丸投げは避けなければなりません。

上記の例は、ISMS 構築のための組織体制として、役立つものではありますが、情報セキュリティ委員会、外部コンサルタント等の固有名詞にこだわる必要はありません。これらの機能をもつ、内部組織を策定し、情報セキュリティの調整、「専門組織との連絡」が行われることが重要です。（JIS Q 27002:2014「6.1.1 情報セキュリティの役割及び責任」、「6.1.3 関係当局との連絡」、「6.1.4 専門組織との連絡」等を参照して下さい。）

５．３．２　ISMS 要求事項への適合と ISMS パフォーマンス

トップマネジメントには、「情報セキュリティ方針」において、情報セキュリティに対する組織のビジョンを示し、ISMS の活動に対する支援についてコミットメントすることが求められています。コミットするということは、単に出来上がった「情報セキュリティ方針書」に承認印を押す事でありません。詳細は、本ガイドの「5.1 リーダーシップ」を参照して下さい。

「5.2 方針」の要求事項では、ISMS の構築・運用に対するトップマネジメントのコミットメントの証拠として、情報セキュリティ方針の確立を挙げています。
また、トップマネジメントは、その管理下におき、直接の報告をさせる組織として、情報セキュリティ委員会のほかに、内部監査の責任及び権限、ISMS のパフォーマンス報告の責任及び権限をさだめなければなりません。内部監査（9.2 参照）において、ISMS の適合性、有効性の状況が確認されます。ISMS のパフォーマンス評価については、９章で説明します。

情報セキュリティに対する組織の取り組み姿勢の定着にトップマネジメントが積極的に関与し、その責任の下に継続的な改善を行うことより、情報セキュリティは組織文化として定着します。
情報セキュリティについての意識が浸透している組織では、突発的な事態に対して従業員がトップマネジメントの意図する行動を自然に取ることが期待されます。これは、めまぐるしく変化する環境においては非常に重要なポイントです。
事業環境の変化の激しい組織における型にはまった手順書は、更新に時間がかかり、常に実業務との整合性を確保することに多大な労力を要することがあります。
そのような場合にも、情報セキュリティの意識を組織文化として浸透させる活動を実施すれば、規模が大きく業種や業態が多岐にわたる組織でも従業員が等しく安全な行動をとるようになります。なお、トップマネジメントの役割と責任については、「付録 1 ISMS 構築・運用とコーポレートガバナンス」を参照して下さい。

６．計画

「6 計画」では、ISMS におけるリスク及び機会を決定し、情報セキュリティリスクアセスメント、リスク対応のプロセスを定めて適用するよう求めています。
例えば、６章のプロセスを例示すると図 6-1 のようになります。

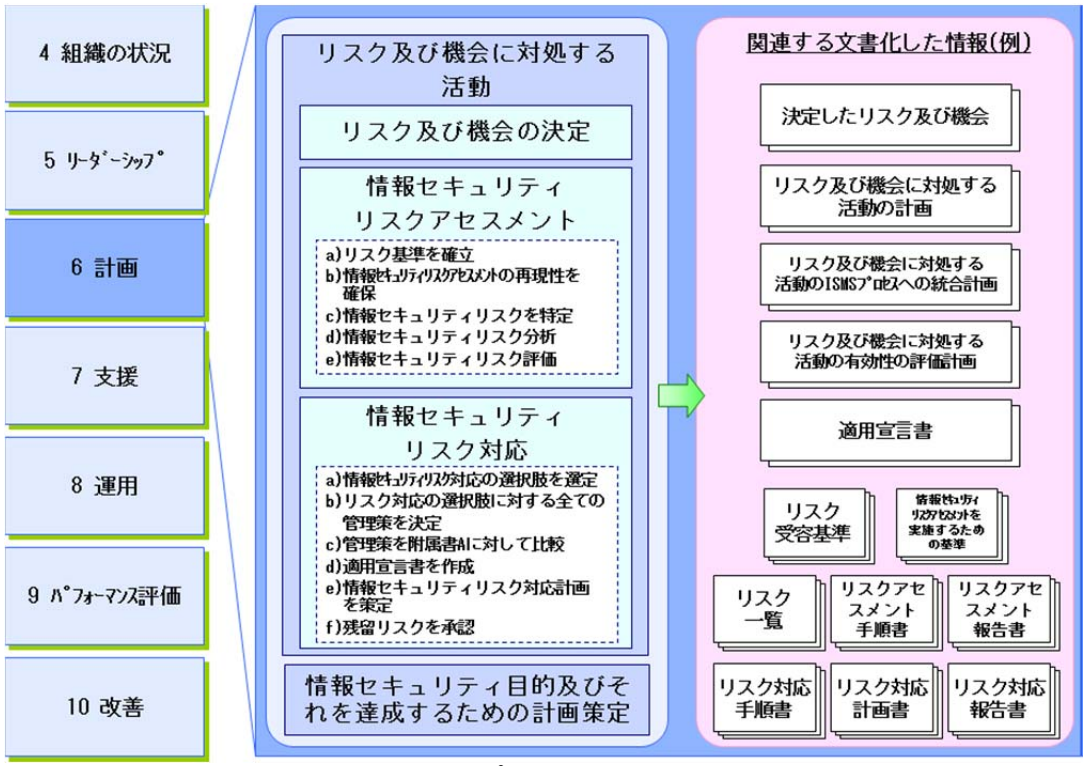


図 6-1　「6 計画」におけるプロセス（事例）　注）文書名は全て例示

６．１　リスク及び機会に対処する活動

ここでは、リスクマネジメント活動を実施する上での組織の取組みについて説明します。
6.1.1 は、ISMS の計画を策定するとき、組織が対処する必要があるリスク及び機会について述べています。リスクマネジメント活動においては、ISMS の意図した成果を達成するために、情報セキュリティに関連する固有のリスクだけではなく、マネジメントシステムのリスクを含めた ISMS 全体に対するリスクを対象とします。

6.1.2 及び 6.1.3 では、それぞれ、情報セキュリティリスクアセスメントプロセス、情報セキュリティリスク対応プロセスが記述されています。本ガイドの 0.2～0.3 でも触れましたが、JIS Q 27001:2014 の 6.1.3 の注記にあるように、リスクマネジメントのプロセスは、JIS Q 31000:2010 に規定する原則及び一般的な指針に整合したものとなっています。

６．１．１　一般

6. 計画 6.1 リスク及び機会に対処する活動 6.1.1 一般 ISMS の計画を策定するとき，組織は，4.1 に規定する課題及び 4.2 に規定する要求事項を考慮し，次の事項のために対処する必要があるリスク及び機会を決定しなければならない。 a) ISMS が，その意図した成果を達成できることを確実にする。

b）望ましくない影響を防止又は低減する。
c）継続的改善を達成する。

組織は，次の事項を計画しなければならない。
d）上記によって決定したリスク及び機会に対処する活動
e）次の事項を行う方法
1）その活動の ISMS プロセスへの統合及び実施
2）その活動の有効性の評価

（JIS Q 27001:2014　6.1.1 一般　より引用）

ここで、ISMS は、マネジメントシステムの定義に当てはめると、情報セキュリティ方針、情報セキュリティ目的及びその目的を達成するためのプロセスを確立するための、相互に関連する又は相互に作用する、組織の一連の要素であり、6.1.1 では、この ISMS の計画を策定する際達成すべき 3 つの事項として 6.1.1a）～c）をあげ、そのために対処すべきリスクと機会の決定を要求しています。

「リスクと機会」という用語は、エンタープライズ・リスクマネジメント（ERM）のフレームワークで用いられています。ERM において、「企業をめぐる事象の中で悪影響を与えるもの」とリスクと定義し、「好影響を与えるもの」は「機会」として区別されました。その上で、リスクだけでなく機会への対応も ERM の中には、明確に組み込まれていました。また、ISO/IEC Guide 73:2002（TR Q 0008:2003）におけるリスクの定義の備考 1 でも、「用語“リスク”は、一般に少なくとも好ましくない結果を得る可能性がある場合にだけ使われる」とされていました。

しかし、ISO 31000 が開発される際に、併せて ISO/IEC Guide 73:2002 の改訂検討も開始されることになり、その結果 ISO Guide 73:2009（JIS Q 0073:2010）のリスクの定義の注記１で、「影響とは、期待されていることから、好ましい方向及び/又は好ましくない方向にかい（乖）離することをいう。」とされ、リスクの定義において、好ましい方向への影響が含まれることとなりました。

JIS Q 27001:2014 におけるリスクの定義は ISO 31000:2009（JIS Q 31000:2010）すなわち ISO Guide 73:2009（JIS Q 0073:2010）の定義を引用していますので（本ガイドの 6.1.2（3）に記載の「リスク」の定義を参照して下さい。）、「好ましい及び/又は好ましくない影響」を含んでいます。一方「機会」は定義されていないため、通常の辞書の意味からすると、6.1.1 における「機会」は「好ましい時機や状況」と考えることができ、リスクマネジメント活動のタイミングなどを決定することにつながります。

6.1.1 a）にある「ISMS の意図した成果」は、以下を含み、この ISMS を確立しようとする組織が定めるものとなります。

- リスクマネジメントプロセスを適用することによって情報の機密性、完全性及び可用性を維持する。かつ、
- リスクを適切に管理しているという信頼を利害関係者に与える。

言い換えると、例えば、次のような考慮がなされます。
ISMS は、情報セキュリティに関わるマネジメントが対象です。情報セキュリティに関するマネジメントシステムの構築とは、企業や組織が所有し、管理、運用する「情報及び情報に関連する資産」の価値に見合うセキュリティ対策の実施や、コンプライアンスの観点から法令等を順守し、それを維持するための枠組みを構築・運用することを意味します。また、単に「情報」や「IT」に直接関わるリスクにとどまらず、マネジメントシステムの局面に関しては、日常の管理に属する部分の他、リスクが顕在化した後の被害を最小限にと

どめるための対応なども要求されます。このような包括的・網羅的な管理を実現するためには、適用範囲の直接の対象である現場組織だけではなく、法務部門、総務部門など組織全体を横断する、管理層への働きかけ、組織の再構成、人材の参画が求められます。このような局面に関してもリスクとしての考慮が求められます。

6.1.1 b）にある「望ましくない影響の防止又は低減」は、リスクが顕在化する前に行う、予防・抑止の活動に言及しています。
「予防」という観点から見ると、JIS Q 27001:2014 には「予防処置」の記述はありません。MSS の共通テキストにおいて、「マネジメントシステム自体が予防処置の概念で構成されている」という考え方がなされ、JIS Q 27001:2014 もこれに従ったためです。

予防処置に関連して、ISO マネジメントシステム共通要素を規定した ISO/IEC 専門業務用指針には次のような記述があります。

> 全般的コメント
>
> この上位構造及び共通テキストには，“予防処置”の特定の要求事項に関する箇条がない。これは，正式なマネジメントシステムの重要な目的の一つが，予防的なツールとしての役目をもつためである。
> したがって，上位構造及び共通テキストは，4.1 において，組織の，“目的に関連し，意図した成果を達成する組織の能力に影響を与える，外部及び内部の課題”の評価を要求し，さらに 6.1 において，“XXX マネジメントシステムが，その意図した成果を達成できることを確実にすること；望ましくない影響を防止，又は低減すること；継続的改善を達成すること，に取り組む必要のあるリスク及び機会を決定”することを要求している。これらの二つの要求事項はセットで“予防処置”の概念を網羅し，かつ，リスク及び機会を見るような，より広い観点をもつと見なされる。
>
> （ISO/IEC 専門業務用指針　統合版 ISO 補足指針　Appendix 3（参考）より引用）

このように、「予防処置」が必要ないということではなく、4.1 と 6.1 の要求事項の組合せにより予防処置の概念を網羅しているという考え方となっています。

6.1.1 c）にある「継続的改善の達成」は、その記述で明らかなように 10.2 との関わりを示し、「ISMS の継続的改善という目的に対する不確かさの影響」へのアセスメントを行うことを求めています。

また、「4.1 に規定する課題及び 4.2 に規定する要求事項を考慮し、」という記述は、4.1 及び 4.2 の要求事項との強い関連を示しています。（図 6-2 参照）
すなわち、組織の課題（4.1）や情報セキュリティの要求事項（4.2）に基づき、活動のフレームワーク、ひいては組織及び組織のそれぞれの部署の目的（6.2 情報セキュリティ目的）を決定することを要求しています。

さらに ISMS の計画策定において取り組むべきものとして、6.1.1 の d）及び e）が示されています。6.1.1 d）は、対処することが必要と決定されたリスク及び機会に対処するために行われる活動です。6.1.1 e）1）では、ISMS プロセスへの統合、すなわちリスクマネジメント活動のプロセスを、組織の全体プロセスに組み込み、統合して構築・維持することを求めています。これについては、8.1 から、6.1 への言及があります。本ガイドの「8.1 運用の計画及び管理」も参照下さい。6.1.1 e）2）は、これらの活動の有効性の評価についての計画なので、箇条 9 のパフォーマンス評価と関連します。本ガイドの「9.1.1 パフォーマンス評価」で触れます。

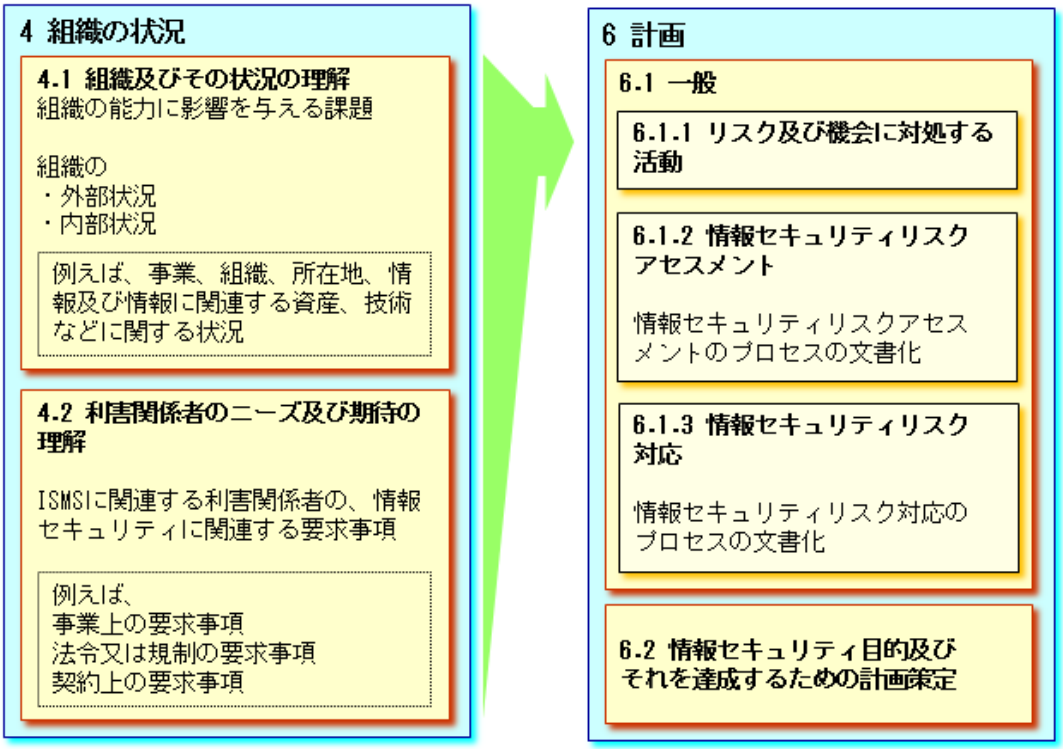


図 6-2　リスク及び機会に対処する活動

６．１．２　情報セキュリティリスクアセスメント

6.1.2　情報セキュリティリスクアセスメント
組織は，次の事項を行う情報セキュリティリスクアセスメントのプロセスを定め，適用しなければならない。
a）次を含む情報セキュリティのリスク基準を確立し，維持する。
　1）リスク受容基準
　2）情報セキュリティリスクアセスメントを実施するための基準
b）繰り返し実施した情報セキュリティリスクアセスメントが，一貫性及び妥当性があり，かつ，比較可能な結果を生み出すことを確実にする。
c）次によって情報セキュリティリスクを特定する。
　1）ISMS の適用範囲内における情報の機密性，完全性及び可用性の喪失に伴うリスクを特定するために，情報セキュリティリスクアセスメントのプロセスを適用する。
　2）これらのリスク所有者を特定する。
d）次によって情報セキュリティリスクを分析する。
　1）6.1.2 c）1）で特定されたリスクが実際に生じた場合に起こり得る結果についてアセスメントを行う。
　2）6.1.2 c）1）で特定されたリスクの現実的な起こりやすさについてアセスメントを行う。
　3）リスクレベルを決定する。
e）次によって情報セキュリティリスクを評価する。
　1）リスク分析の結果と 6.1.2 a）で確立したリスク基準とを比較する。
　2）リスク対応のために，分析したリスクの優先順位付けを行う。

組織は，情報セキュリティリスクアセスメントのプロセスについての文書化した情報を保持しなければならない。

（JIS Q 27001:2014　6.1.2 情報セキュリティリスクアセスメント　より引用）

情報セキュリティリスクアセスメントとは、識別された情報及び情報に関連する資産に関するリスクを識別し、それらの大きさをプロセスに従い決定することです。

2.71　リスクアセスメント（risk assessment）
リスク特定（2.75），リスク分析（2.70）及びリスク評価（2.74）のプロセス（2.61）全体。
（JIS Q 0073:2010 の 3.4.1 参照）

（JIS Q 27000:2014　2 用語及び定義　より引用）

情報セキュリティリスクアセスメント手法の、情報及び情報に関連する資産、脅威、ぜい弱性をリスク源とした適用事例を本ガイドの付録 2 に示しています。

（1）リスク基準を確立（6．1．2 a））

6.1.2　情報セキュリティリスクアセスメント
組織は，次の事項を行う情報セキュリティリスクアセスメントのプロセスを定め，適用しなければならない。
a）次を含む情報セキュリティのリスク基準を確立し，維持する。
　1）リスク受容基準
　2）情報セキュリティリスクアセスメントを実施するための基準
b）繰り返し実施した情報セキュリティリスクアセスメントが，一貫性及び妥当性があり，かつ，比較可能な結果を生み出すことを確実にする。

（JIS Q 27001:2014　6.1.2 情報セキュリティリスクアセスメント　より引用）

これは、組織に遍在しかつ多岐にわたる、情報及び情報に関連する資産に関して、そのリスクアセスメントを複数の担当者で実施する上で、必要なプロセスです。

・リスク基準とは

リスク基準は、以下のように定義されています。

2.73　リスク基準（risk criteria）
リスク（2.68）の重大性を評価するための目安とする条件。
（JIS Q 0073:2010 の 3.3.1.3 参照）
　注記 1　リスク基準は，組織の目的，外部状況及び内部状況に基づいたものである。
　注記 2　リスク基準は，規格，法律，方針及びその他の要求事項から導き出されることがある。

（JIS Q 27000:2014　2 用語及び定義　より引用）

リスク基準は、組織の価値観、目的及び資源を反映し、情報セキュリティ目的、組織の外部状況及び内部状況に基づき、情報セキュリティ要求事項、関連する法規制からの要求事項及び契約上の義務、並びに情報セキュリティ方針等から導き出されるものです。リスク基準は、1 つではなく、導き出された複数の基準を組み合わせて考慮することが望まれます。

またリスク基準は、少なくとも次の要素を考慮して定めることが望まれます。

- リスクの原因及び発生し得る結果の特質及び種類、並びにこれらを測定する方法
- リスクの起こりやすさをどのように定めるか
- リスクの起こりやすさ及び／又はその発生する結果を考える時間枠
- リスクレベルをどのように決定するか
- 利害関係者の見解
- リスクが受容可能になるレベル（リスク受容基準）
- 複数のリスクの組合せを考慮に入れるのが望ましいか、また、考慮に入れる場合の組合せ

さらに、リスク受容基準以外に、情報セキュリティリスクアセスメントを実施するための基準として、リスク評価基準、影響基準などの名称で定義する例もあります。

例えば、リスク評価基準は、組織の情報セキュリティリスクを評価するために設定する基準で、リスク対応の優先順位を規定することに利用します。影響基準は、情報セキュリティ事象に起因して組織の被る損害又はコストの程度によって規定します。
本ガイドの付録 2 に、詳細な適用事例を記載しています。

リスク受容基準

リスク受容基準とは、リスクを受容するかどうかの判断基準のことです。リスク受容については、JIS Q 27000 では、以下のように定義されています。リスク受容の意思決定は、リスク所有者により行われます。リスク所有者とは、リスクに対する責任及び権限を負う組織あるいは管理者のことです。情報及び情報に関連する資産の管理責任者（オーナ：owner）の多くは、リスク所有者でもあります。

2.69 リスク受容（risk acceptance）
ある特定のリスク（2.68）をとるという情報に基づいた意思決定。
（JIS Q 0073:2010 の 3.7.1.6 参照）
注記 1 リスク対応（2.79）を実施せずにリスク受容となることも，又はリスク対応プロセス中にリスク受容となることもある。
注記 2 受容されたリスクは，モニタリング［監視（2.52）］及びレビュー（2.65）の対象となる。

（JIS Q 27000:2014 2 用語及び定義 より引用）

2.78 リスク所有者（risk owner）
リスク（2.68）を運用管理することについて，アカウンタビリティ及び権限をもつ人又は主体。
（JIS Q 0073:2010 の 3.5.1.5 参照）

（JIS Q 27000:2014 2 用語及び定義 より引用）

情報セキュリティリスクアセスメントを実施するための基準

情報セキュリティリスクアセスメントを実施するための基準として、リスクアセスメントを実施する要件である、その実施条件、計画、契機、時期、タイミング、及び頻度などを規定しておくことが求められます。8.2 の情報セキュリティリスクアセスメントは、このリスク基準に基づいて実施されるものです。

（2）情報セキュリティリスクアセスメントの一貫性及び妥当性を確保（６．１．２ b））

このリスク基準は、「繰り返し実施した情報セキュリティリスクアセスメントが、一貫性及び妥当性があり、かつ、比較可能な結果を生み出すこと」（6.1.2 b））を実現するものであることが望まれます。加えて、これが実現できていることを、リスクアセスメント実施の記録などで、証拠として検証できる仕組みが求められます。

（3）情報セキュリティリスクを特定（６．１．２ c））

c）次によって情報セキュリティリスクを特定する。
1）ISMS の適用範囲内における情報の機密性，完全性及び可用性の喪失に伴うリスクを特定するために，情報セキュリティリスクアセスメントのプロセスを適用する。
2）これらのリスク所有者を特定する。

（JIS Q 27001:2014　6.1.2 情報セキュリティリスクアセスメント　より引用）

リスクアセスメントは、まず「リスクを特定する」ことから始まります。

リスクは、JIS Q 27000 で、以下のように定義されています。

2.68
リスク（risk）
目的に対する不確かさの影響。
（JIS Q 0073:2010 の 1.1 参照）
注記 1　影響とは，期待されていることから，好ましい方向又は好ましくない方向にかい（乖）離することをいう。
注記 2　不確かさとは，事象（2.25），その結果（2.14）又はその起こりやすさ（2.45）に関する，情報，理解又は知識が，たとえ部分的にでも欠落している状態をいう。
注記 3　リスクは，起こり得る事象（2.25），結果（2.14）又はこれらの組合せについて述べることによって，その特徴を記述することが多い。
注記 4　リスクは，ある事象（周辺状況の変化を含む。）の結果（2.14）とその発生の起こりやすさ（2.45）との組合せとして表現されることが多い。
注記 5　ISMS の文脈においては，情報セキュリティリスクは，情報セキュリティ目的に対する不確かさの影響として表現することがある。
注記 6　情報セキュリティリスクは，脅威（2.83）が情報資産のぜい弱性（2.89）又は情報資産グループのぜい弱性（2.89）に付け込み，その結果，組織に損害を与える可能性に伴って生じる。

（JIS Q 27000:2014　2 用語及び定義　より引用）

また、このリスクを生成する源（source）として、リスク源が JIS Q 0073:2010 で以下のように定義されています。

3.5.1.2　リスク源（risk source）
それ自体又はほかとの組合せによって，リスク（1.1）を生じさせる力を本来潜在的にもっている要素。
注記　リスク源は，有形の場合も無形の場合もある。

（JIS Q 0073:2010　3.5 リスク特定に関する用語　より引用）

情報及び情報に関連する資産に対する脅威、ぜい弱性等はリスク源の典型的な例です。
リスクの定義の注記で示されている、起こり得る事象、結果は、これらの組み合わせで構成されており、その起こりやすさと合わせてリスクが表されます。

リスク源の具体的事例についての詳細は、本ガイドの付録 2 を参照して下さい。
付録 2 の説明では、リスク源の例示として、情報及び情報に関連する資産に対する、脅威、ぜい弱性を使っています。

リスク特定は、次のように定義されています。

2.75　リスク特定（risk identification）
リスク（2.68）を発見，認識及び記述するプロセス。
（JIS Q 0073:2010 の 3.5.1 参照）
注記 1 リスク特定には，リスク源，事象，それらの原因及び起こり得る結果の特定が含まれる。
注記 2 リスク特定には，過去のデータ，理論的分析，情報に基づいた意見，専門家の意見及びステークホルダのニーズを含むことがある。

（JIS Q 27000:2014　2 用語及び定義　より引用）

リスクの特定とは、リスク源、影響を受ける領域、事象（周辺状況の変化を含む。）、並びにこれらの原因及び起こり得る結果を特定し、その事象の中の次の特性をもったものに基づいて、リスクの包括的な一覧を作成することです。

その特性がある事象とは、組織の情報セキュリティ目的の達成を実現、促進、抑止、劣化、加速又は遅延させる可能性を有する事象です。

ある機会を追求しないことに伴うリスクを特定することも重要です。
また、この段階で特定されなかったリスクは、その後の分析の対象からは外されてしまうので、包括的にリスクの特定を行うことが極めて重要です。

リスク特定において、次を含めることが望まれます。

- リスク源が組織の管理下にあるか否かにかかわらず、行うこと。リスク源又はリスクの原因が明らかではないかもしれないリスクも含めること。
- リスクの波及効果及び累積効果を含めた、特定の結果の連鎖を注意深く検討すること。
- リスク源又はリスクの原因が明らかではないかもしれない場合でも、広範囲の結果について考慮すること。

何が起こり得るかの特定に加えて、考えられる原因及びどのような結果が引き起こされることがあるかを示す（情報セキュリティインシデント）シナリオについて考慮する必要があります。
全ての重大な原因及び結果を考慮することが望まれます。

組織は、その情報セキュリティ目的及び能力、並びに組織が直面するリスクに見合った、リスク特定の手段及び手法を適用することが望まれます。

リスクを特定するときは、現況に即した最新の情報が重要です。
可能な場合には、これに適切な背景情報も含めること、また、適切な知識をもつ人をリスクの特定に参画させることが望まれます。

前述のとおり、リスクの定義の注記 6 には「情報セキュリティリスクは、脅威が情報資産のぜい弱性又は情報資産グループのぜい弱性に付け込み、その結果、組織に損害を与える可能に伴って生じる。」という記述があります。
情報及び情報に関連する資産、脅威、ぜい弱性をリスク源とした適用事例については、本ガイドの付録 2 を参照してください。

（４）情報セキュリティリスク分析（６．１．２ ｄ））

d）次によって情報セキュリティリスクを分析する。
1）6.1.2 c）1）で特定されたリスクが実際に生じた場合に起こり得る結果についてアセスメントを行う。
2）6.1.2 c）1）で特定されたリスクの現実的な起こりやすさについてアセスメントを行う。
3）リスクレベルを決定する。

（JIS Q 27001:2014　6.1.2 情報セキュリティリスクアセスメント　より引用）

JIS Q 27000 では、リスク分析について以下のように定義しています。

2.70　リスク分析（risk analysis）
リスク（2.68）の特質を理解し，リスクレベル（2.44）を決定するプロセス。
（JIS Q 0073:2010 の 3.6.1 参照）
注記 1 リスク分析は，リスク評価（2.74）及びリスク対応（2.79）に関する意思決定の基礎を提供する。
注記 2 リスク分析は，リスクの算定を含む。

（JIS Q 27000:2014　2 用語及び定義　より引用）

リスク分析とは、リスクの結果及びその起こりやすさを特定し、その結果と起こりやすさの組合せとしてリスクレベルを決定することです。

リスク分析には、リスクの原因及びリスク源、リスクの好ましい結果及び好ましくない結果、並びにこれらの結果の起こりやすさに関する考慮が含まれます。
また、結果及び起こりやすさに影響を与える要素を特定することが望まれます。
1 つの事象が複数の結果をもたらし、複数の目的に影響を与えることがあります。既存の管理策に加えて、それらの有効性及び効率も考慮に入れることが望まれます。

リスクの結果及び起こりやすさを表す方法、並びにリスクレベルを決定するためにこの 2 つを組み合わせる方法は、次を反映したものであることが望まれます。

- リスクの種類
- 利用可能な情報
- リスクアセスメントからのアウトプットを使用する目的

これらの方法は、全てリスク基準と矛盾しないものであることが望まれます。
また、異なったリスク及びそれらのリスク源の間の相互依存性を考慮することも重要です。

リスクレベルの決定に対する信頼性、並びに必要条件及び前提に対する関連度は、リスク分析の中で考慮され、意思決定者及び適切な場合にはその他の利害関係者に効果的に伝達されることが望まれます。

専門家の間の意見の相違、情報の「不確かさ、利用可能性、品質、量、及び現況に対する鮮度」、またモデル化の限界などの要素は、明記し、留意されることが望まれます。
リスク分析をどの程度まで詳細に行えるかは、リスクによって、また分析の目的並びに利用可能な情報、データ及び資源によって、様々です。
分析は、それを取り巻く環境によって、定性的、半定量的、定量的、又はそれらの組み合わせによって行うことができます。

リスクの結果及びその起こりやすさは、1 つの事象からの、若しくは一組の事象からの出力をモデル化することによって、又は実験調査若しくは利用可能なデータからの推定によって、定めることが可能です。結果は、有形及び無形の影響として表現することができます。
場合によっては、異なった時間、場所、集まり、状況における結果及びその起こりやすさを特定するために、複数の数値又は記述子が必要となることがあります。

リスク分析は、リスク特定のプロセスで特定したリスクについて、より深く理解することが含まれます。リスク分析は、リスク評価及びリスク対応の必要性、並びに最適なリスク対応の戦略及び方法に関する意思決定に対するインプットを提供します。意思決定のために、選択を行わなければならず、かつ、選択肢に異なったリスクの種類及びレベルが含まれる場合には、リスク分析は、また、その意思決定に対するインプットを提供できます。

リスクレベルは、以下のように定義されています。

2.44　リスクレベル（level of risk）
結果（2.14）とその起こりやすさ（2.45）の組合せとして表現される，リスク（2.68）の大きさ。
（JIS Q 0073:2010 の 3.6.1.8 を変更）

（JIS Q 27000:2014　2 用語及び定義　より引用）

（５）情報セキュリティリスク評価（６．１．２ e））

e）次によって情報セキュリティリスクを評価する。
　1）リスク分析の結果と 6.1.2 a）で確立したリスク基準とを比較する。
　2）リスク対応のために，分析したリスクの優先順位付けを行う。

（JIS Q 27001:2014　6.1.2 情報セキュリティリスクアセスメント　より引用）

JIS Q 27000 では、リスク評価について以下のように定義しています。

2.74　リスク評価（risk evaluation）
リスク（2.68）及び／又はその大きさが受容可能か又は許容可能かを決定するために，リスク分析（2.70）の結果をリスク基準（2.73）と比較するプロセス（2.61）。
（JIS Q 0073:2010 の 3.7.1 参照）
　注記　リスク評価は，リスク対応（2.79）に関する意思決定を手助けする。

（JIS Q 27000:2014　2 用語及び定義　より引用）

リスク評価は、組織の状況を考慮して確定されたリスク基準と、リスク分析プロセスで発見されたリスクのレベルとの比較を行い、この比較に基づいて、リスク対応の必要性について決定し、リスク対応の実践の優先順位を与えます。

リスク評価の目的は、リスク分析の成果に基づき、どのリスクへの対応が必要か、対応の実践の優先順位はどうするかについての意思決定を助けることです。

意思決定では、リスクのより広い範囲の状況を考慮し、そのリスクから便益を得る組織以外の、他者が担うリスクの許容度についても考慮に含めることが望まれます。
意思決定は、法律、規制及びその他の要求事項に従って行われることが望まれます。

周辺状況によっては、リスク評価の結果、更なる分析を実行するという意思決定が導き出されることがあり得ます。また、リスク評価の結果、そのリスクについては、既存の管理策を維持する以外はいかなる対応もしないという意思決定が行われることもあり得ます。
この意思決定は、組織のリスクに対する態度、及び確定されているリスク基準に影響されるでしょう。

「リスク対応」の内容については、本ガイドの 6.1.3 で詳細に説明します。

（６）情報セキュリティリスクアセスメントの手順について文書化

リスクアセスメントには、作業を実施するために必要な手順が文書化されている必要があります。

- **リスクアセスメントの定義**
- **リスクアセスメントの目的**
- **リスクアセスメントの方法**

また、上記の「リスクアセスメントの方法」には、リスクに関する判断の基準（リスク基準）が含まれます。リスク基準については、本ガイドの 6.1.2 の「（１）リスク基準を確立（６．１．２ a））」を参照して下さい。

これらの文書策定は、繰り返し実施する情報セキュリティリスクアセスメントが、一貫性及び妥当性があり、かつ、比較可能な結果を生み出すことを確実にするために行う必要があります。このことは、仮にリスクアセスメントの方法を変更した場合でも、その変更を管理し、必要に応じてリスクアセスメントの結果の比較が可能な状態にしておくことを含みます。

６．１．３　情報セキュリティリスク対応

リスクアセスメントの結果、評価されたリスクに対し、リスク対応を実施します。

6.1.2e）に従って優先順位が定められたリスクのリストをインプットとし、リスクの低減、保有、回避又は共有といったリスク対応選択肢を選定し、その実施に必要な全ての管理策を決定します。また、リスク対応計画を策定することが求められます。
リスク所有者の承認を受けた、リスク対応計画及び残留リスクが、アウトプットとなります。

リスク対応には、リスクを修正するために 1 つ以上の選択肢を選び出すこと及びそれらの選択肢を実践することが含まれます。一度選択肢が実践されると、リスク対応は、新たな管理策を提供するか又は既存の管理策を修正することとなります。
リスク対応には、次の循環プロセスが含まれます。

- あるリスク対応のアセスメントの実施
- 残留リスクレベルが許容可能かの判断
- 許容できない場合の、新たなリスク対応の策定
- その対応の有効性のアセスメントの実施

6.1.3 情報セキュリティリスク対応
組織は，次の事項を行うために，情報セキュリティリスク対応のプロセスを定め，適用しなければならない。
a) リスクアセスメントの結果を考慮して，適切な情報セキュリティリスク対応の選択肢を選定する
b) 選定した情報セキュリティリスク対応の選択肢の実施に必要な全ての管理策を決定する。
注記　組織は，必要な管理策を設計するか，又は任意の情報源の中から管理策を特定することができる。
c) 6.1.3 b) で決定した管理策を附属書 A に示す管理策と比較し，必要な管理策が見落とされていないことを検証する。
注記 1 附属書 A は，管理目的及び管理策の包括的なリストである。この規格の利用者は，必要な管理策の見落としがないことを確実にするために，附属書 A を参照することが求められている。
注記 2 管理目的は，選択した管理策に暗に含まれている。附属書 A に規定した管理目的及び管理策は，全てを網羅してはいないため，追加の管理目的及び管理策が必要となる場合がある。
d) 次を含む適用宣言書を作成する。
－ 必要な管理策［6.1.3 の b) 及び c) 参照］及びそれらの管理策を含めた理由
－ それらの管理策を実施しているか否か
－附属書 A に規定する管理策を除外した理由
e) 情報セキュリティリスク対応計画を策定する。
f) 情報セキュリティリスク対応計画及び残留している情報セキュリティリスクの受容について，リスク所有者の承認を得る。

組織は，情報セキュリティリスク対応のプロセスについての文書化した情報を保持しなければならない。
注記　この規格の情報セキュリティリスクアセスメント及びリスク対応のプロセスは，JIS Q 31000 に規定する原則及び一般的な指針と整合している。

（JIS Q 27001:2014　6.1.3 情報セキュリティリスク対応　より引用）

リスク対応の選択肢の候補は、リスク対応の定義（注記 1）に示されています。

2.79　リスク対応（risk treatment）
リスク（2.68）を修正するプロセス（2.61）。
（JIS Q 0073:2010 の 3.8.1 参照）
注記 1 リスク対応には，次の事項を含むことがある。
－ リスクを生じさせる活動を，開始又は継続しないと決定することによって，リスクを回避すること。
－ ある機会を追求するために，リスクをとる又は増加させること。
－ リスク源を除去すること。
－ 起こりやすさを変えること。
－ 結果を変えること。
－ 一つ以上の他者とリスクを共有すること（契約及びリスクファイナンシングを含む。）。
－ 情報に基づいた選択によって，リスクを保有すること。
注記 2 好ましくない結果に対処するリスク対応は，“リスク軽減”，“リスク排除”，“リスク予防”及び“リスク低減”と呼ばれることがある。
注記 3 リスク対応が，新たなリスクを生み出したり，又は既存のリスクを修正したりすることがある。

（JIS Q 27000:2014　2 用語及び定義　より引用）

リスク対応とは、「リスクを修正するプロセス」と説明されています。

（１）情報セキュリティリスク対応の選択肢を選定（６．１．３ a））

情報セキュリティリスクアセスメントで明確にされた管理対象とするリスクに対し、次の選択肢からどれを選択するかについて評価します。
情報セキュリティでは、基本的にリスクを低減する方向でアプローチします。
リスクとその対策の関係によっては、リスク対応によって、新たなリスクが生まれたり、増加したり、又は既にあるリスクを修正したりすることがあります。その主な選択肢について説明します。

好ましくない結果に対してリスク対応を行う

「適切な管理策を採用し、リスクを低減する」方法は、リスク対応の実施の際にもっとも多く採用されます。リスク対応の定義（注記 1）の、リスク源を除去すること、リスクの起こりやすさを変えること、リスクのもたらす結果（影響度）を変えることが該当します。
例えば、JIS Q 27001:2014 の附属書 A に記載されている 114 項目の管理策の適用や、要求事項に明記されていない対策の追加実施等はこれに相当します。
リスク低減について概念的に示したものを図 6-3 に示します。

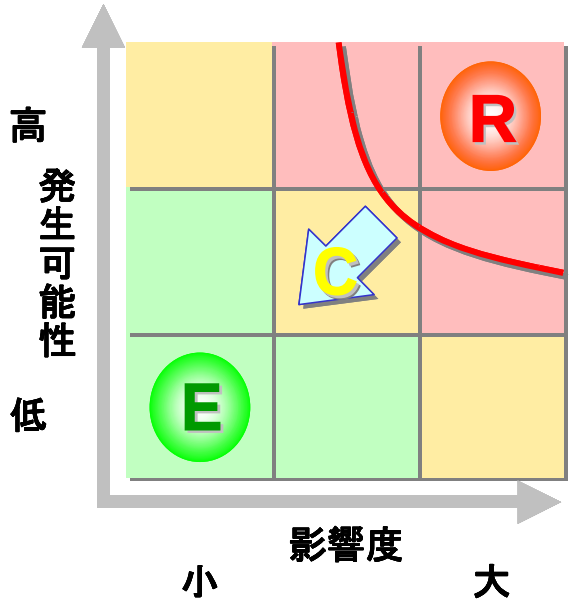


図 6-3　リスク低減の概念

図中で、
R はリスク：Risk
C はリスクを低減させるための対策：Control
E は対策を講じた後のリスク：Exposure
を示しています。

この場合、リスク低減は「リスクの発生の可能性を低減する」ことと、「リスクが顕在化した場合の影響度を低減する」ことにより実現されることが分かります。

リスク発生可能性（起こりやすさ）の低減の例として、「入退室をより厳重に管理する」などの対策が考えられます。
影響度の低減（結果を変えること）では、「バックアップ頻度を増やし、修復可能なデータを増やす」などの対策が考えられます。

現実には、対策の実施によるリスクの完全な除去は不可能です。
多くの場合、利便性の確保や、対策にかかる費用と効果の比較により、顕在化したときのリスクを受容可能な水準にとどめるのに十分な費用を投入して対策を実施し、残留リスクを次項「情報に基づいた選択によって、リスクを保有すること（リスクを意識的、かつ、客観的に受容すること）」の対象として管理します。

情報に基づいた選択によって、リスクを保有する

リスクを意識的、かつ、客観的に受容することに該当します。リスクが組織の方針及びリスク基準を明らかに満たす場合に用いる選択肢です。
保有するリスクは、以下の 2 つに大別できます。

- **リスク対応により受容されるリスク**
- **リスク対応を実施せずに、又はリスク対応プロセス中に、受容となるリスク**

リスクを回避する

「リスクを回避する」とは、リスク対応を考えてもコストの割にベネフィットが得られない場合、リスクを回避するために、業務を廃止したり、資産を破棄するといった方法をとることです。

例えば、個人情報の保管には、漏えいするリスクがあります。また、それらの情報を各個人（各従業者）が保有し、管理する方法では、適切に開示できないというリスクが想定されます。これらのリスクに対し業務上の必要性が乏しくなった個人情報であれば、廃棄するというリスク対応が考えられます。

また、売上に寄与していないメーリングリストの場合、不注意で個人情報を漏えいしたり、ウィルス蔓延に利用されるリスクがあるので、メーリングリストを廃止するというリスク対応が考えられます。

リスクを共有する

リスクを共有するとは、契約等によりリスクを他者（他社）と共有することです。
リスクを共有する方法は大別すると 2 種類あります。1 つは資産や情報セキュリティ対策を外部に委託する方法（アウトソーシング）で、もう 1 つはリスクファイナンスの一種として保険等を利用する方法です。

例えば、前者の例として資産を外部のデータセンターに預けるというコロケーションサービスの利用や、運用を委託するという方法があります。一般にデータセンター、インターネットサービスプロバイダー、アプリケーションサービスプロバイダー、マネジメントサービスプロバイダーといわれている事業者がこのようなリスクの共有先となります。

組織は、このようなアウトソーシング等でリスクを共有する場合、「共有したリスク」、「共有しなかったリスク」、「共有したことにより新たに発生するリスク」の 3 つを明確にすることが重要となります。また、共有したリスクを明確にするために、セキュリティ対策について契約書等に織り込むことが重要となります。

JIS Q 27001:2014 の附属書 A「管理目的及び管理策」には以下のような管理策が記載されており、リスクを共有することにより新たに発生するリスクを低減するための管理策といえます。

表 6-1　管理策 A.15.1 供給者関係における情報セキュリティ

A.15.1 供給者関係における情報セキュリティ 目的： 供給者がアクセスできる組織の資産の保護を確実にするため。		
管理策		
A.15.1.1	供給者関係のための情報セキュリティの方針	管理策 組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について，供給者と合意し，文書化しなければならない。 （JIS Q 27001:2014　A.15.1.1 より引用）

リスク管理上は、JIS Q 27001:2014 の管理策を適用できない場合や、適用してもリスク値が受容水準以上の場合、リスク共有を検討します。

リスクファイナンスとしてリスクを共有する典型的な例は保険の採用です。例えば、地震等の不可避な脅威について、事業に与える影響は大きいが、比較的発生する可能性が低いので保険の利用を検討する等ということが相当します。

今日では、情報システム障害に対応するための保険が販売されています。例えば、顕在化したリスクの影響から復旧するために必要な費用や機器の買い替え費用が保険により支払われるというものです。

保険の場合、保証されるのは損害に対する金銭的な保証の一部に過ぎません。そのため、保険のみを利用したリスク対策には限界があります。（例えば、情報漏えいを起こし、企業ブランドが低下しても保険により損害を補填することは困難です）。つまり、保険によるリスク対応は万能ではありません。あくまでも、管理策を実施しても補填できないリスクがある場合に予備的に利用するのが本来の目的と思われます。

また、保険は、免責事項などが細かく決められていますので、契約を結ぶ前に細かく確認することが重要です。

（２）リスク対応の選択肢に対する全ての管理策を決定（６．１．３ b））

選定した情報セキュリティリスク対応の選択肢の実施に必要な全ての管理策を決定します。組織は、必要な管理策を設計するか、又は任意の情報源の中から管理策を特定することができます。JIS Q 27001:2014 の附属書 A を参考にして決定することも可能です。

（３）管理策を附属書 A に対して比較（６．１．３ c））

上記（２）で決定した管理策を、JIS Q 27001:2014 の附属書 A「管理目的及び管理策」と比較し、リスク対応に関する必要な管理策が見落とされていないことを検証します。

附属書 A は、管理目的及び管理策の包括的なリストです。JIS Q 27001:2014 の利用者は、必要な管理策の見落としがないことを確実にするために、附属書 A を参照することが求められています。適切な管理目的又は管理策が附属書 A に記載されていない場合は、組織が追加した管理目的及び管理策として特定し、適用宣言書に記録します。

また、この比較では、リスクアセスメント及びリスク対応プロセスの結果に基づいてその妥当性を検証することが重要です。

また、附属書 A「管理目的及び管理策」に記載されている管理策の幾つかは、全ての情報システム又は環境に適用できるとは限らないこと、及び組織によっては実施できない場合もあることを認識しておく必要があります。例えば、JIS Q 27002:2014「6.1.2 職務の分離」は、不正行為及び過失を防止するための職務の分離について規定していますが、その実施の手引では、「小さな組織にとって、職務の分離を実現するのは難しい場合がある。」と記載されています。

しかし、このような場合でも、「分離が困難である場合には、他の管理策（例えば、活動の監視、監査証跡、管理層による監督）を考慮することが望ましい。」と記載されているように、組織は（管理）目的を達成するにあたり、リスクが受容可能な範囲に低減できる代替措置を講じられるのであれば、他の管理策を、また附属書 A に記載されている管理策に該当するものがなければ、それ以外からの管理策を特定し、リスク対応として確実に実装していく必要があります。

（４）適用宣言書を作成（６．１．３ d））

上記（２）及び（３）で決定した管理目的及び管理策、並びにこれらを決定した理由を文書化し、適用宣言書を作成します。これらの管理策を実施しているか否かについても、記載する必要があります。
また、附属書 A に記載された管理目的及び管理策の中から適用除外としたものは、当該管理策と除外した理由について記録を残すことが要求されています。

（５）情報セキュリティリスク対応計画を策定（６．１．３ e））

リスクアセスメント及びリスク対応の結果を考慮して、情報セキュリティ目的が策定されます（6.2 参照）。

リスク対応計画とは、リスクアセスメントの結果に基づき、受容できないリスクを低減するためにとるべき活動と、選択した管理目的及び管理策の実装に関する実行計画を明らかにすることで、情報セキュリティ目的の達成を目指すものです。
リスクマネジメントに必要な経営資源の割当てや実際の作業は、このリスク対応計画に基づいて実施されます。

情報セキュリティ目的又は情報セキュリティ目的を設定するための枠組みは、情報セキュリティ方針に含まれます。情報セキュリティ方針及び情報セキュリティ目的の確立は、トップマネジメントのリーダーシップとコミットメントにより実施されるものです（5.2 参照）。これを受けて、組織は、この計画が策定されることを確実にする責任があります。詳細は、次の「6.2 情報セキュリティ目的及びそれを達成するための計画策定」で触れます。

リスク対応計画に不備があれば、十分な管理目的及び管理策が実装できないことにも繋がりますので、様々な条件を考慮に入れて計画を策定する必要があります。

リスク対応計画では、単にリスクを低減するための管理目的及び管理策を策定するだけではなく、導入した管理目的及び管理策が適切かつ効果的に動作していることを確認するための管理目的及び管理策や、異常を検出するための管理目的及び管理策等を導入する計画も合わせて策定する必要があります。

例えば、管理策としてアンチウィルスソフト、ファイアウォール、アクセス制御などのセキュリティ製品を導入する場合について考えてみます。これらの製品を導入する際には、セキュリティを強化するための設定に留まらず、それらの状態を示す情報や、処理した結果のログなどを抽出して解析することにより、異常検出を考慮した設定を実装することなども計画に盛り込むことが必要です。
また、解析に必要な装置などが高価な場合、その導入による効果を確実にするための管理策も視野に入れて検討することが重要です。

リスク対応計画により、組織が識別したリスクに対する管理目的及び管理策の実施状況と、対策は実施したが残留リスクが受容可能な水準以下に低減されていないリスクへの追加的対策の進捗状況とを容易に把握することが可能となります。

リスク対応計画に含むことが望ましい内容として、以下の 5 点が含まれます。

- **実施項目**
- **資源**
- **実施する責任者**
- **完了予定時期**
- **実施結果の評価方法**

（6）残留リスクを承認（6．1．3 f））

情報セキュリティリスク対応計画と、残留リスク（リスク対応の後に残っているリスク）の受容について、リスク所有者の承認をもらいます。守るべき情報及び情報に関連する資産の管理責任者の多くが、リスク所有者であり、また最上位のリスク所有者は、トップマネジメントになります。

（7）情報セキュリティリスク対応の手順の文書化

情報セキュリティリスク対応のプロセスについては、リスク対応計画策定及び実施に係る基準、手順等の文書化した情報を保持しなければなりません。

6．2　情報セキュリティ目的及びそれを達成するための計画策定

6.2　情報セキュリティ目的及びそれを達成するための計画策定 組織は，関連する部門及び階層において，情報セキュリティ目的を確立しなければならない。 情報セキュリティ目的は，次の事項を満たさなければならない。 a）情報セキュリティ方針と整合している。 b）（実行可能な場合）測定可能である。 c）適用される情報セキュリティ要求事項，並びにリスクアセスメント及びリスク対応の結果を考慮に入れる。 d）伝達する。

e）必要に応じて，更新する。

組織は，情報セキュリティ目的に関する文書化した情報を保持しなければならない。
組織は，情報セキュリティ目的をどのように達成するかについて計画するとき，次の事項を決定しなければならない。
f）実施事項
g）必要な資源
h）責任者
i）達成期限
j）結果の評価方法

（JIS Q 27001:2014　6.2 情報セキュリティ目的及びそれを達成するための計画策定　より引用）

組織は、情報の機密性、完全性及び可用性を維持するための組織としての目的をもたなければなりません。

インターネットのような相互につながった世界では、情報は、情報に関連するプロセス、システム、ネットワーク並びにこれらの運営、取扱い及び保護に関与する人々も含め、他の重要な事業資産と同様、組織の事業にとって不可欠であり、また高い価値をもつ資産です。すなわち、様々な危険から保護する必要があります。

このような組織の状況において、組織それぞれに固有の情報セキュリティリスクの環境を考慮に入れて、情報セキュリティの目的を策定、維持することが求められます。
組織は、関連する部門及び階層において、それぞれの情報セキュリティ目的を確立しなければなりません。

情報セキュリティ方針と情報セキュリティ目的は、組織を導く方向を提示するものとして確立することが求められます。この 2 つの仕組みは、組織をして望まれる結果を確定し、これらの結果を達成するために資源を適用することの助けになります。
情報セキュリティ方針は、情報セキュリティ目的を確立し見直しするための枠組みを提供します。情報セキュリティ目的は、情報セキュリティ方針及び、継続的改善に対するトップマネジメントのコミットメントと、整合している必要があり、その達成が測定可能なものであることが求められます。そのままでは測定することが難しい目的には、組織としてその目的の達成度を判断するための指標を設定し、測定可能なものとすることができます。

情報セキュリティ目的を達成することにより、情報セキュリティ、運用上の有効性及びセキュリティパフォーマンスに良いインパクトを与えることができ、それによって、利害関係者の要求事項を満たし、その信頼性に応えることが可能となります。

情報セキュリティ目的は、利害関係者からの情報セキュリティ要求事項に応えるものでなければなりません。それは、主に次の 3 つによって導き出されます。

a）組織全体における事業戦略及び目的を考慮に入れた、組織に対するリスクアセスメント、リスク対応の実施。リスクアセスメントによって資産に対する脅威を特定し、事故発生につながるぜい弱性及び事故の起こりやすさを評価し、潜在的な影響を推定する。
b）組織、その取引相手、契約相手及びサービス提供者が満たさなければならない法的、規制及び契約上の要求事項、並びにその社会文化的環境。
c）組織がその活動を支えるために策定した、情報の取扱い、処理、保存、伝達及び保管に関する一連の原則、目的及び事業上の要求事項。

情報セキュリティ目的は文書化し、関連する部門や関係者への伝達、見直しを行い、組織の状況、利害関係者からの要求事項の変化に対応して更新していくことが必要です。

組織は、関連する部門及び階層において、リスク対応計画をはじめ、情報セキュリティ目的に対応させて、それらを達成するための計画を立て実施することが求められます。計画は、目的を達成するために何を実施するか、それに必要な資源は何か、計画の責任者は誰か、いつまでに達成するか、実施結果の評価をどのように行うかを含めて、具体的に決定し、推進することが求められます。

７．支援

支援のプロセスでは、7.5 で要求される文書類を文書化し、管理し、維持しながら、人々の力量、並びに利害関係者との反復的及び必要に応じたコミュニケーションを確立することを通じて、ISMS の運用の支援について規定しています。
例えば、７章のプロセスを例示すると図 7-1 のようになります。

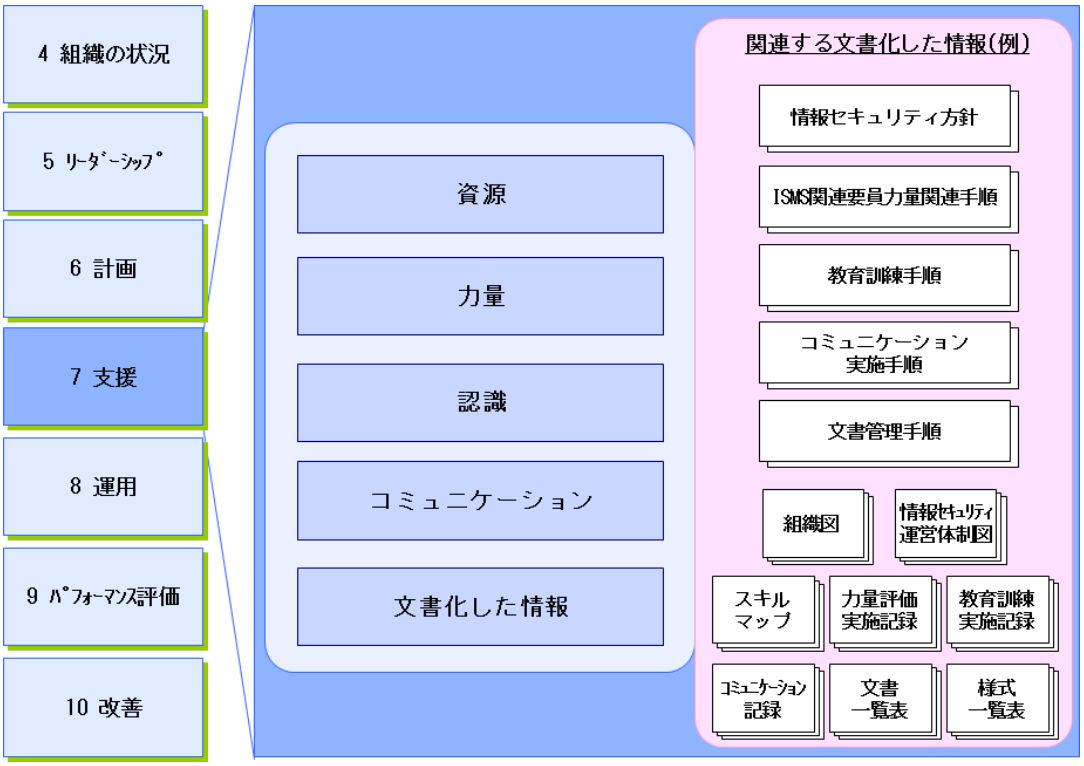


図 7-1　ISMS の運用の計画及び管理（事例）　注）文書名は全て例示

７．１　資源

組織は，ISMS の確立，実施，維持及び継続的改善に必要な資源を決定し，提供しなければならない。 （JIS Q 27001:2014　7.1 資源　より引用）

組織は、ISMS に必要な資源を決定し提供しなければなりません。

例えば、資源は、ISMS 推進体制及び要員、情報機器を含む物品、活動経費となる資金、リスクに関する情報といった、「人」、「物」、「金」、「情報」といった資源が考えられます。資源を提供する際に留意する点として、資源を必要とする時点には、必要な資源を確保しておかなければなりません。そのためには、今後必要となる資源を予測して事前に対応しておくことで手遅れになることが防げるといえます。
特にトップマネジメントは、この資源の決定に深く関与することになり、トップマネジメントの重要な役割の 1 つとして、「人」、「物」、「金」、「情報」といった資源の提供があります。トップマネジメントは、ISMS の必要性を理解し、そのために必要な資源の決定と提供を行わなければなりません。

トップマネジメントの掛け声だけでは、ISMS の確立、実施、維持及び継続的改善は難しいと思われます。ISMS の構築に必要な一連のプロセスには、資源の割当てが必要となります。

また、従来の JIS Q 27001:2006 5.2.1 a）～f）では、「事業上の要求事項を満たすことに、情報セキュリティの手順が寄与することを確実にする」のに必要な資源など、より詳細な事項を要求していましたが、JIS Q 27001:2014 では包括的な表現で要求されています。

７．２　力量

組織は，次の事項を行わなければならない。
a）組織の情報セキュリティパフォーマンスに影響を与える業務をその管理下で行う人（又は人々）に必要な力量を決定する。
b）適切な教育，訓練又は経験に基づいて，それらの人々が力量を備えていることを確実にする。
c）該当する場合には，必ず，必要な力量を身につけるための処置をとり，とった処置の有効性を評価する。
d）力量の証拠として，適切な文書化した情報を保持する。
注記　適用される処置には，例えば，現在雇用している人々に対する，教育訓練の提供，指導の実施，配置転換の実施などがあり，また，力量を備えた人々の雇用，そうした人々との契約締結などもある。

（JIS Q 27001:2014　7.2 力量　より引用）

7.2 では、7.1 で特定された人的資源に対して、各々の役割と責任に応じた必要な力量を備えていることを確実するために、行わなければならないことを規定しています。つまり、
・　力量を構成する要件を決定する。
・　必要とする力量と要員の力量とのギャップを分析し、必要な教育・訓練と経験によって力量をもたせる。
・　教育以外にも注記にあるように再配置や雇用や外部委託契約も含め、とった処置がギャップを埋めるに有効であったか、狙い通り課題解決が図られたかを評価する。
・　一連のこれらの活動の記録を力量の証拠として作成する。
ということを行うことになります。

また、従来の JIS Q 27001:2006 では、「教育、訓練、技能、経験及び資格についての記録を維持する」と具体的な記録の内容を要求していましたが、JIS Q 27001:2014 では「力量の証拠」となるため、具体的な「文書化した情報を保持」しておく必要があるとの包括的な表現で要求されています。

例えば、ISMS の確立、実施、運用、維持及び継続的改善を行っているのは、人であるということを忘れてはなりません。組織の各個人が情報セキュリティに関連する責任を果たし、期待される役割を実行するためには、本人の力量が伴わなければならないことは明らかです。力量については、次のように定義されています。

2.11 力量（competence）
意図した結果を達成するために，知識及び技能を適用する能力。

（JIS Q 27000:2014　2 用語及び定義　より引用）

トップマネジメントには、明確にされた役割を割り当てられた要員全てが、要求される職務を実施する力量をもつことを確実にするために、教育・訓練を実施させる責任があります。
実施した教育・訓練については、その有効性を評価し、力量をもった要員の確保に役立てることが重要です。必要とされる力量は、それぞれの業務により異なることになります。

ISMS の確立、実施、運用、維持及び継続的改善のために必要となる知識・技能としては、表 7-1 のような分野が考えられます。

表 7-1　力量の分野

マネジメントに関連する知識・技能	マネジメント論全般、リーダーシップなど
監査に関連する知識・技能	監査理論全般、監査の実務
情報セキュリティ技術に関連する知識・技能	ネットワークセキュリティ、サーバアプリケーションセキュリティ、OS セキュリティ、ファイアウォール、侵入検知システム、ウィルス、セキュアプログラミング、暗号などに関する理論や実践

これらの知識・技能に関する力量及び必要とされる力量を有しているかどうかの判断基準を適切に定義し、その達成度を確認することが重要となります。

また、力量を判断する手段の一部として、資格制度を利用することも可能です。それぞれの知識・技能に関連する資格の例としては表 7-2 のような資格、試験が考えられます。資格、試験の合格の記録、及びその資格、試験の内容をレビューし、確認することが、どのような知識・技能を有しているかの判断材料となります。

表 7-2　力量と関連する資格

内部監査	公認内部監査人（CIA）[3]、公認会計士、公認システム監査人[4]、システム監査技術者[5]、公認情報システム監査人（CISA）[6]、ISMS 主任審査員、ISMS 審査員、公認情報セキュリティ監査人（CAIS）[7]
セキュリティ技術	情報セキュリティスペシャリスト[8]、公認情報セキュリティ管理者（CISM）[9]、公認情報システムセキュリティ専門家（CISSP）、公認システムセキュリティ熟練者（SSCP）[10]

また、情報セキュリティについての業務毎に必要とされる力量を決定する際に、経済産業省が発表している情報セキュリティ教育についての報告書[11]や、独立行政法人情報処理推

[3] 公認内部監査人（Certified internal Auditor）は内部監査人協会（The Institute of Internal Auditors,Inc.（IIA）　http://www.theiia.org）が認定する内部監査人の資格。内部監査人協会は 1941 年に米国で設立され、2012 年現在、全世界で約 175,000 名が内部監査人協会に所属している。

[4] 公認システム監査人は特定非営利活動法人日本システム監査人協会（http://www.saaj.or.jp）が認定するシステム監査人の資格。

[5] 独立行政法人情報処理推進機構（http://www.ipa.go.jp/）により行われている、システム監査技術を有していることを認定するための国家試験。

[6] 公認情報システム監査人は、ISACA（Information Systems Audit and Control Association 情報システムコントロール協会 http://www.isaca.org）により認定されるシステム監査人の資格。情報システムコントロール協会は 1967 年に米国で設立され、全世界で 110,000 名以上（非会員の資格認定者を含む）が ISACA に所属している。

[7] 公認情報セキュリティ監査人は、特定非営利活動法人日本セキュリティ監査協会により認定される情報セキュリティ監査人の資格。

[8]情報セキュリティスペシャリストは独立行政法人情報処理推進機構（http://www.ipa.go.jp/）により行われている、情報セキュリティ機能の企画、開発、運用などについての一定の専門的知識・能力を有していることを検定するための国家試験。

[9] 公認情報セキュリティ管理者（Certified information security manager）は、情報システムコントロール協会（Information Systems Audit and Control Association　http://www.isaca.org）により認定されるセキュリティ管理者としての専門的能力を有していることを証明する資格。

[10]公認情報システムセキュリティ専門家（Certified information system security professional）、公認システムセキュリティ熟練者（System security certified practitioner）は（ISC）[2]（International Information Systems Security Certification Consortium http://www.isc2.org）により認定される情報セキュリティについての専門的能力を有していることを保証する資格。

[11] http://www.meti.go.jp/policy/netsecurity/edu_report.html

進機構（IPA）が発表しているスキルマップ[12]、報告書[13]などを参考にされるとよいと思われます。

７．３　認識

組織の管理下で働く人々は，次の事項に関して認識をもたなければならない。 a）情報セキュリティ方針 b）情報セキュリティパフォーマンスの向上によって得られる便益を含む，ISMS の有効性に対する自らの貢献 c）ISMS 要求事項に適合しないことの意味 （JIS Q 27001:2014　7.3 認識　より引用）

7.3 では、組織の管理下で働く人々が、情報セキュリティ方針や ISMS の有効性に対する自らの貢献、ISMS 要求事項に適合しないことの意味を認識することを規定しています。組織の管理下で働く人々は、自らの情報セキュリティについての活動の意味とその重要性を認識し、情報セキュリティ方針及び目的の達成に向けてどのように貢献できるかを認識できるものとすることが必要です。7.2 で実施する教育・訓練の内容は、それを実現するものであることが求められます。

例えば、情報セキュリティマネジメントシステムの活動は、トップマネジメントが確立した情報セキュリティ方針及び目的に基づいて、またリスクアセスメント及びリスク対応の計画された活動によって、並びにその活動結果によって特定した管理策及びプロセスによって実施されます。

情報セキュリティについての活動の意味とその重要性を認識するためには、情報セキュリティ方針についての認識が必要となります。
管理策がリスクアセスメント及びリスク対応の活動の結果に基づき特定され、さらに、それらの活動が情報セキュリティ方針に基づき、情報セキュリティ目的に関連付けられていることを認識することが求められます。

また、情報セキュリティを効果的に管理するためには、情報セキュリティパフォーマンスの向上、ISMS の有効性に対して、自らの業務・活動がどのように位置づけられ、寄与することができるのかを認識することが必要です。

それらとともに、情報セキュリティ及びその管理に関して、組織の情報セキュリティの活動を支える人々、関連する人々が、順守を含め適合して活動することが求められていることに従わなかった場合、どのような影響がもたらされるか、情報セキュリティにどのような損害をもたらすかを認識することも求められています。

[12] http://www.ipa.go.jp/security/manager/edu/training/expert.html
[13] http://www.ipa.go.jp/security/fy14/reports/professional/sec-pro-outline.pdf

７．４　コミュニケーション

組織は，次の事項を含め，ISMS に関連する内部及び外部のコミュニケーションを実施する必要性を決定しなければならない。
a）コミュニケーションの内容（何を伝達するか。）
b）コミュニケーションの実施時期
c）コミュニケーションの対象者
d）コミュニケーションの実施者
e）コミュニケーションの実施プロセス

（JIS Q 27001:2014　7.4 コミュニケーション　より引用）

7.4 では、内外関係者との意思疎通が求められています。コミュニケーション手段としては、メール・会議・Web 掲載など多岐にわたりますが、それらの利用に際して明確にしなければならない点を 7.4 で規定しています。

例えば、顧客からの苦情や情報セキュリティインシデントなど突発的な事象に関しての対応は、短時間で処理する必要があり、あらかじめ対応者・担当者・連絡経路を特定しておき、対処の手順を定めて、適用対象者に徹底することが必要です。特に事業の中断となるようなインシデントの場合、早急なエスカレーションと迅速なコミュニケーションが求められます。緊急時のレスポンス体制と、連絡網、対応プロセスが整備されていることが必要でしょう。

また、JIS Q 27001:2014 が要求する文書化した情報、及び情報セキュリティマネジメントシステムの有効性のために必要であると組織が決定した、文書化した情報は、コミュニケーションの対象と考えられます。
組織は、コミュニケーションについて、上記を含め、具体的に実施すべき事項を決めることが求められています。
コミュニケーションの対象には、少なくとも、以下が含まれますが、これに限定されるものではありません。

- **情報セキュリティ方針**
- **情報セキュリティ目的**
- **情報セキュリティマネジメントの重要性**
- **情報セキュリティマネジメントシステムの要求事項への適合性の重要性**
- **情報セキュリティマネジメントシステムのパフォーマンスの報告**
- **内部監査の報告**
- **情報セキュリティインシデント**

なお、従来の JIS Q 27001:2006 4.2.4 c）では、「すべての利害関係者に、状況にあった適切な詳しさで、処置及び改善策を伝える。該当するときは、処置及び改善策の進め方について合意を得る」とありましたが、JIS Q 27001:2014 では、処置及び改善策以外でもコミュニケーションの必要性を特定することが要求されています。

７．５　文書化した情報

７．５．１　一般

組織の ISMS は，次の事項を含まなければならない。
a）この規格が要求する文書化した情報
b）ISMS の有効性のために必要であると組織が決定した，文書化した情報
　注記　ISMS のための文書化した情報の程度は，次のような理由によって，それぞれの組織で異なる場合がある。

1）組織の規模，並びに活動，プロセス，製品及びサービスの種類
2）プロセス及びその相互作用の複雑さ
3）人々の力量

（JIS Q 27001:2014　7.5.1 一般　より引用）

7.5.1 では、ISMS の文書化について、何を文書として含めなければならないのかを規定しています。

例えば、文書化した情報は、次のように定義されています。文書と記録の両方を含んだ表現として使われています。また、記録された映像や動画、ログ、WEB のデータ等も文書化した情報に含まれます。

2.23　文書化した情報（documented information）
組織（2.57）が管理し，維持するよう要求されている情報，及びそれが含まれている媒体。
注記 1　文書化した情報は，あらゆる形式及び媒体の形をとることができ，あらゆる情報源から得ることができる。
注記 2　文書化した情報には，次に示すものがあり得る。
― 関連するプロセス（2.61）を含むマネジメントシステム（2.46）
― 組織の運用のために作成された情報（文書類）
― 達成された結果の証拠（記録）

（JIS Q 27000:2014　2 用語及び定義　より引用）

また、JIS Q 27001:2014 で、「文書化した情報」を明確に記載している部分は、表 7-3 のとおりです。

表 7-3　要求事項に示された文書化した情報

4 3	4.3 情報セキュリティマネジメントシステムの適用範囲の決定 ISMS の適用範囲は，文書化した情報として利用可能な状態にしておかなければならない。
5.2	5.2 方針 情報セキュリティ方針は，次に示す事項を満たさなければならない。 e）文書化した情報として利用可能である。
6.1.2	6.1.2 情報セキュリティリスクアセスメント 組織は,情報セキュリティリスクアセスメントのプロセスについての文書化した情報を保持しなければならない。
6.1.3	6.1.3 情報セキュリティリスク対応 d）次を含む適用宣言書を作成する。 ― 必要な管理策［6.1.3 の b）及び c）参照］及びそれらの管理策を含めた理由 ― それらの管理策を実施しているか否か ― 附属書 A に規定する管理策を除外した理由 組織は，情報セキュリティリスク対応のプロセスについての文書化した情報を保持しなければならない。
6.2	6.2 情報セキュリティ目的及びそれを達成するための計画策定 組織は，情報セキュリティ目的に関する文書化した情報を保持しなければならない。
7.2	7.2 力量 d）力量の証拠として，適切な文書化した情報を保持する。
7.5.3	7.5.3 文書化した情報の管理 ISMS の計画及び運用のために組織が必要と決定した外部からの文書化した情報は，必要に応じて，特定し，管理しなければならない。
8.1	8.1 運用の計画及び管理 組織は，プロセスが計画通りに実施されたという確信をもつために必要な程度の，文書化した情報を保持しなければならない。
8 2	8.2 情報セキュリティリスクアセスメント 組織は，情報セキュリティリスクアセスメント結果の文書化した情報を保持しなけ

	ればならない。
9.1	9.1 監視，測定，分析及び評価 組織は，監視及び測定の結果の証拠として，適切な文書化した情報を保持しなければならない。
9.2	9.2 内部監査 g）監査プログラム及び監査結果の証拠として，文書化した情報を保持する。
9.3	9.3 マネジメントレビュー 組織は，マネジメントレビューの結果の証拠として，文書化した情報を保持しなければならない。
10.1	10.1 不適合及び是正処置 組織は，次に示す事項の証拠として，文書化した情報を保持しなければならない。 f）不適合の性質及びとった処置 g）是正処置の結果

（JIS Q 27001:2014　上記各項　より引用）

７．５．２　作成及び更新

文書化した情報を作成及び更新する際，組織は，次の事項を確実にしなければならない。
a）適切な識別及び記述（例えば，タイトル，日付，作成者，参照番号）
b）適切な形式（例えば，言語，ソフトウェアの版，図表）及び媒体（例えば，紙，電子媒体）
c）適切性及び妥当性に関する，適切なレビュー及び承認

（JIS Q 27001:2014　7.5.2 作成及び更新　より引用）

7.5.2 では、文書化した情報を作成及び更新する際に確実にしなければならないことを規定しています。

- 適切な識別及び記述
- 適切な形式
- 適切性及び妥当性に関する、適切なレビュー及び承認

７．５．３　文書化した情報の管理

ISMS 及びこの規格で要求されている文書化した情報は，次の事項を確実にするために，管理しなければならない。
a）文書化した情報が，必要なときに，必要なところで，入手可能かつ利用に適した状態である。
b）文書化した情報が十分に保護されている（例えば，機密性の喪失，不適切な使用及び完全性の喪失からの保護）。

文書化した情報の管理に当たって，組織は，該当する場合に，は必ず，次の行動に取り組まなければならない。
c）配付，アクセス，検索及び利用
d）読みやすさが保たれることを含む，保管及び保存
e）変更の管理（例えば，版の管理）
f）保持及び廃棄

ISMS の計画及び運用のために組織が必要と決定した外部からの文書化した情報は，必要に応じて，特定し，管理しなければならない。
注記　アクセスとは，文書化した情報の閲覧だけの許可に関する決定，文書化した情報の閲覧及び変更の許可及び権限に関する決定，などを意味する。

（JIS Q 27001:2014　7.5.3 文書化した情報の管理　より引用）

7.5.3 では、文書及び記録の管理は、文書化した情報の管理として規定されています。

ISMS 文書は、版管理され適切な文書を必要とする人が必要なときに使用可能な状態で管理されている必要があります。

記録は、組織の ISMS が要求事項へ適合していること及び運用の効果を示す証拠として作成、維持、管理します。ISMS プロセス全般における活動の記録、管理策の実施状況の記録、及び ISMS に関連する監視及び測定（セキュリティインシデントの発生等を含む。）に関する記録を維持することが要求されます。

例えば、記録の管理としては、以下の事項の実施などが効果的です。

- **識別、保管、保護、検索、保管期間及び廃棄に関して必要な管理をすること**
- **記録の必要性及び記録の範囲を定めること**
- **会社法等保管期間が定められている場合には、法的要求事項に適合した保存期間を決定すること**

証拠として文書化された情報

組織の ISMS が要求事項へ適合していること及び運用の効果を示す証拠として作成、維持、管理する文書化された情報があります。

JIS Q 27001:2014 の附属書 A に、表 7-4 に示すような管理策があることに留意する必要があります。

表 7-4　証拠として文書化された情報に関する管理策

A.16.1.7	証拠の収集	組織は，証拠となり得る情報の特定，収集，取得及び保存のための手順を定め，適用しなければならない。
A.18.1.3	記録の保護	記録は，法令，規制，契約及び事業上の要求事項に従って，消失，破壊，改ざん，認可されていないアクセス及び不正な流出から保護しなければならない。

（JIS Q 27001:2014　附属書 A（規定）管理目的及び管理策　より引用）

詳細は、JIS Q 27002:2014 の「16.1.7 証拠の収集」、「18.1.3 記録の保護」を参照して下さい。

８．運用

８．１　運用の計画及び管理

組織は，情報セキュリティ要求事項を満たすため，及び 6.1 で決定した活動を実施するために必要なプロセスを計画し，実施し，かつ管理しなければならない。また，組織は，6.2 で決定した情報セキュリティ目的を達成するための計画を実施しなければならない。

組織は，プロセスが計画通りに実施されたという確信をもつために必要な程度の，文書化した情報を保持しなければならない。

組織は，計画した変更を管理し，意図しない変更によって生じた結果をレビューし，必要に応じて，有害な影響を軽減する処置をとらなければならない。

組織は，外部委託したプロセスが決定され，かつ，管理されていることを確実にしなければならない。

（JIS Q 27001:2014　8.1 運用の計画及び管理　より引用）

8.1 では、情報セキュリティの要求事項を実現するために必要なプロセス群を、策定し、導入・実施し、管理することを規定しています。
これには 6.1 で決定した、リスク及び機会に対する活動（リスクアセスメント、リスク対応の活動）をプロセスとして組み込み、実施・運用管理を行うことを含みます（6.1.1 e）参照）。

また、6.2 で確定された情報セキュリティ目的を実現するための計画を実施することも含まれます。計画した変更、意図しない変更に対する、変更管理のプロセス、外部委託したプロセスに対する管理が、考慮されなければなりません。

組織にとって適切な基準によって、必要なプロセス群の設定、プロセスの構成と組み合わせ及び管理を行うことが求められています。

例えば、これらのプロセスを例示すると図 8-1 のようになります。
図 8-1 に例示するプロセスにそって手順書が整備され、その手順にそって進捗や結果が記録、報告されるよう運用されることが期待されます。

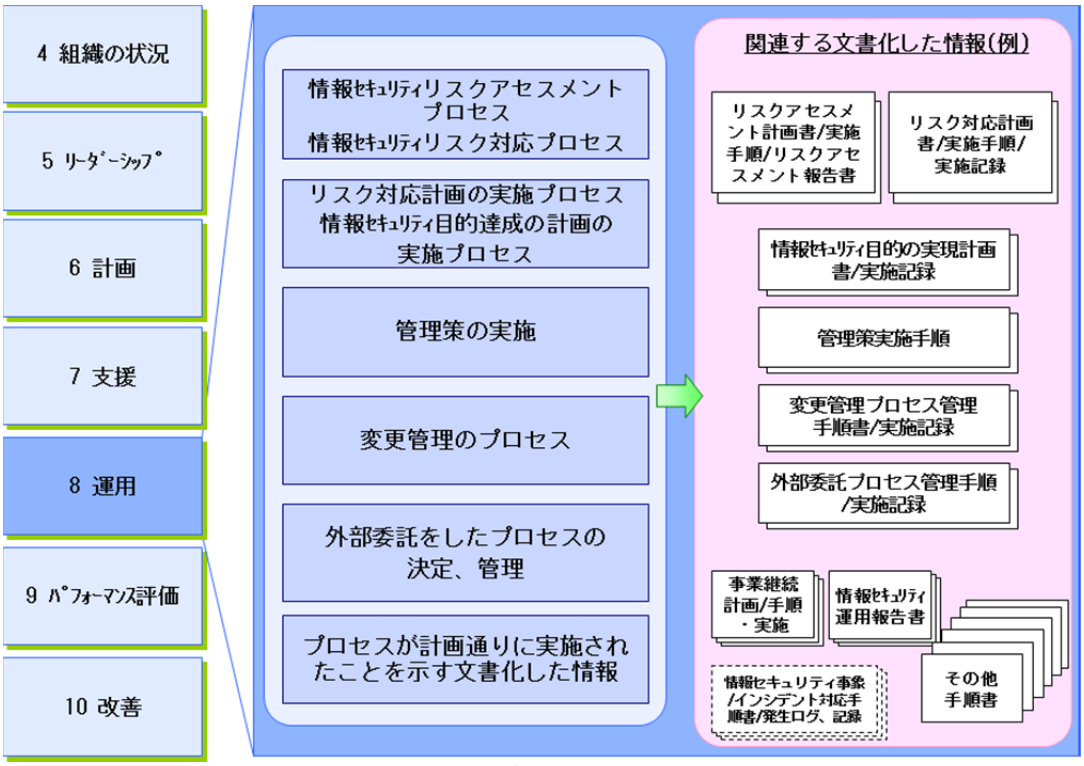


図 8-1　ISMS の運用の計画及び管理（事例）　注）文書名は全て例示

ここからは図 8-1 で挙げた各々のプロセスについて説明します。

情報セキュリティリスクアセスメントプロセス、情報セキュリティリスク対応プロセス

ISMS がその意図した成果を達成し、望ましくない影響を防止又は低減し、継続的改善を達成すべく、組織が対処する必要があるリスク及び機会を決定し、そのリスク及び機会に対して情報セキュリティリスクアセスメントプロセス、及び情報セキュリティリスク対応プロセスを実施します。ここでは、6.1 で定めた項目に従いプロセスを実施します。

例えば、情報セキュリティリスクアセスメントプロセスを実施するために作成される文書として、リスクアセスメント計画書、リスクアセスメント実施手順、リスクアセスメント報告書などが挙げられます。また、情報セキュリティリスク対応プロセスを実施するために作成される文書として、リスク対応計画書などが挙げられます。

リスク対応計画の実施プロセス、情報セキュリティ目的達成の計画の実施プロセス

特定した情報セキュリティ目的（管理目的である場合もあります。）を達成するためにリスク対応計画を実施します。ここでは、6.2 で定めた項目（6.2 f）～ j）参照）に従い、必要資源の手当て並びに役割及び責任の割当て等を考慮に入れ、確実に情報セキュリティ目的を達成するために当該責任者を中心にリスク対応計画を実施します。

例えば、リスク対応計画の実施プロセスで作成される文書としては、リスク対応実施手順などが挙げられます。

管理策の実施

リスク対応計画に従い、優先順位の高い管理策から実施していきます。
その際には、管理策の運用に関する手順や、セキュリティインシデントに対応する手順などを文書化し、関係者に周知する必要があります。

情報セキュリティインシデントへの対応としては、顕在化したセキュリティインシデントに対する被害を最小限に抑えるために、まずそれらを適切に検出し、迅速な処置をとることが重要です。

セキュリティインシデントに対応するための手順書の策定と、その内容の定期的な検証は重要な作業です。特に、初期段階における対応の責任者の設定及び必要な関係者を対象とした連絡・報告の体制、適切な処置の実施に関する一連の手順の策定は重要です。

また、検出されたセキュリティインシデントを報告し、適切な処置として組織全体に反映することは、今後の再発防止のために重要です。セキュリティインシデントを報告する報告書には、以下の事項を含めることに留意して下さい。

- **セキュリティインシデントの記録**
- **管理策の不具合**
- **処置の内容**
- ***必要な追加の管理策など***

変更管理のプロセス

計画の変更では、計画変更についての承認プロセスなどを明確に定め、定めた手順により管理することが必要です。変更する際には、その変更が妥当であったのかをレビューするプロセスが重要です。特に、取引先や発注先が法令違反をして事業停止したことに伴い、取引先や発注先の変更を余儀なくされるといった、意図しない事象による変更については、その変更が妥当であったのかをレビューしなければなりません。

例えば、変更管理のプロセスを実施するために作成される文書として、変更管理プロセス管理手順書などが挙げられます。

外部委託をしたプロセスの決定、管理

外部委託のプロセスは、情報セキュリティを運営管理するための重要な課題です。そのため、外部委託したプロセスの決定、及び外部委託したプロセスが確実に管理されていることが必要となります。
例えば、外部委託をしたプロセスの決定、管理を実施するために作成される文書として、外部委託プロセス管理手順などが挙げられます。

プロセスが計画通り実施されたことを示す文書化された情報

計画通り実施されたことを示す文書化された情報とは、例えば、次のような記録類が挙げられます。
・　リスクアセスメント報告書
・　リスク対応計画実施記録
・　変更管理プロセス実施記録
・　外部委託プロセス実施記録

ここで注意しなければならないのは、ISO の記録のための記録にならないようにすることだと言えます。そのためには、何故、記録を採るのかという目的を明確にしなければなりません。記録をとる目的は、様々あると思いますが、例えば、何か問題が起きた時の根本的な原因を客観的な証拠によって遡及できることや、内部監査や外部監査においてプロセスが JIS Q 27001:2014 や組織の定めた手順に適合していることの実証として用いられる点が挙げられます。

８．２　情報セキュリティリスクアセスメント

> 8.2 情報セキュリティリスクアセスメント
> 組織は，あらかじめ定めた間隔で，又は重大な変更が提案されたか若しくは重大な変化が生じた場合に，6.1.2 a）で確立した基準を考慮して，情報セキュリティリスクアセスメントを実施しなければならない。
>
> （JIS Q 27001:2014　8.2 情報セキュリティリスクアセスメント　より引用）

8.2 では、情報セキュリティリスクアセスメントを 6.1.2 a）で確立した基準に従って、あらかじめ定めた間隔、また必要な都度（重大な変更が提案されたか若しくは重大な変化が生じた場合）、実施することが要求されています。組織内外の環境は、常に変化しているため、リスクも変動していることを念頭に置き、リスクアセスメントを適時に実施することが必要となります。なお、重大な変更が提案され若しくは重大な変化が生じた場合の情報セキュリティリスクアセスメントの実施は、JIS Q 27001:2014 で新たに追加された要求事項です。

８．３　情報セキュリティリスク対応

> 8.3 情報セキュリティリスク対応
> 組織は，情報セキュリティリスク対応計画を実施しなければならない。
>
> 組織は，情報セキュリティリスク対応結果の文書化した情報を保持しなければならない。
>
> （JIS Q 27001:2014　8.3 情報セキュリティリスク対応　より引用）

8.3 では、8.2 での情報セキュリティリスクアセスメントの結果により、対策の必要のあるリスクへの対応策を実施すること、及び対応結果の文書化した情報を保持することを規定しています。情報セキュリティリスク対応計画については、6.1.3 においてこれを作成するプロセスを定め、適用することが求められています（6.1.3 参照）。情報セキュリティリスク対応計画は、8.2 に従って実施した情報セキュリティリスクアセスメントの結果を考慮して（6.1.3 a））実施することとなります。

なお、情報セキュリティリスク対応結果が有効であるかどうかは、「9 パフォーマンス評価」を参照して下さい。

９．パフォーマンス評価

「9 パフォーマンス評価」では、次に関することを規定しています。

- 情報セキュリティパフォーマンスを評価します（監視、測定、分析及び評価を行います）。監視及び測定の対象として必要とするものは組織が決定しますが、その候補には情報セキュリティプロセス及び管理策が含まれます。
- 内部監査及びマネジメントレビューには、情報セキュリティマネジメントシステムの有効性の評価が含まれています。

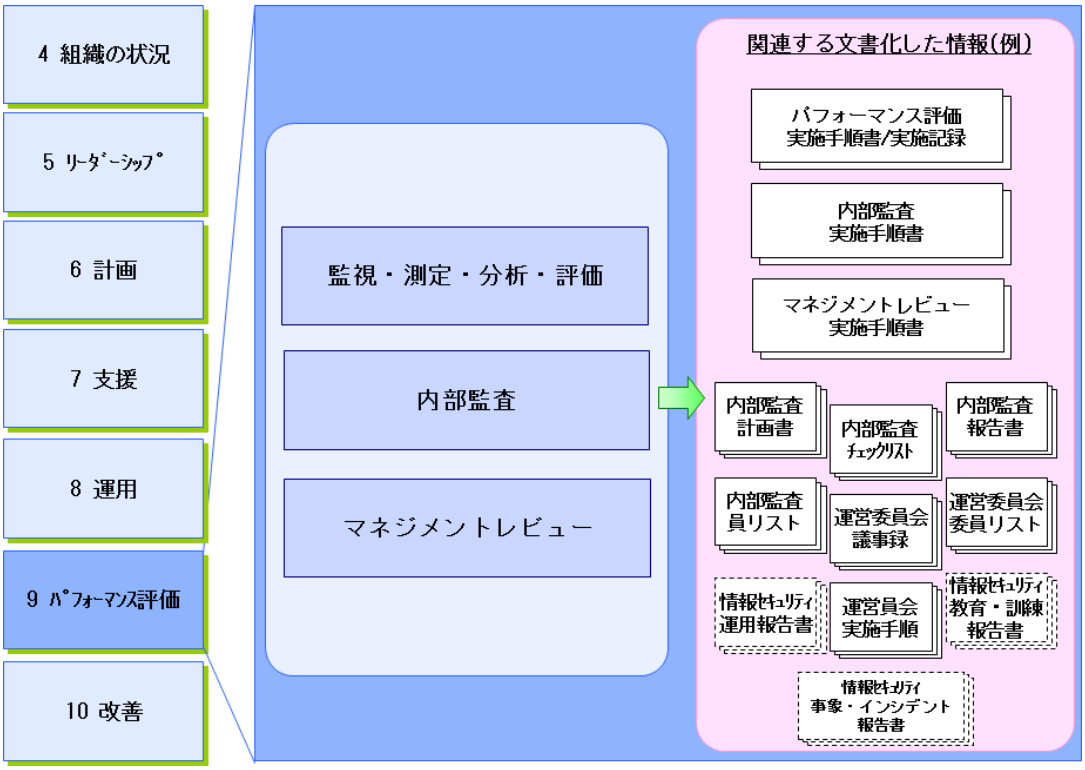


図 9-1　ISMS のパフォーマンス評価のプロセス　　注）文書名は全て例示

9.1　監視，測定，分析及び評価
組織は，情報セキュリティパフォーマンス及び ISMS の有効性を評価しなければならない。
組織は，次の事項を決定しなければならない。
a）必要とされる監視及び測定の対象。これには，情報セキュリティプロセス及び管理策を含む。
b）該当する場合には，必ず，妥当な結果を確実にするための，監視，測定，分析及び評価の方法
　注記　選定した方法は，妥当と考えられる，比較可能で再現可能な結果を生み出すことが望ましい。
c）監視及び測定の実施時期
d）監視及び測定の実施者
e）監視及び測定の結果の，分析及び評価の時期
f）監視及び測定の結果の，分析及び評価の実施者

組織は，監視及び測定の結果の証拠として，適切な文書化した情報を保持しなければならない。

（JIS Q 27001:2014　9.1 監視，測定，分析及び評価　より引用）

ここで使用されている用語、パフォーマンス、監視、測定及び有効性について、どのような意味で使用しているか、留意しておく必要があります。これらは、どのマネジメントシステムでも共通の意味をもたせるように、次のように定義されています。

2.59　パフォーマンス（performance）
測定可能な結果。
　注記 1　パフォーマンスは，定量的又は定性的な所見のいずれにも関連し得る。
　注記 2　パフォーマンスは，活動，プロセス（2.61），製品（サービスを含む。），システム，又は組織（2.57）の運営管理に関連し得る。

2.48　測定（measurement）
値を決定するプロセス（2.61）。

2.52　監視（monitoring）
システム，プロセス（2.61）又は活動の状況を明確にすること。
　注記　　状況を明確にするために，点検，監督，又は注意深い観察が必要な場合もある。

2.24　有効性（effectiveness）
計画した活動を実行し，計画した結果を達成した程度。

2.15 継続的改善（continual improvement）
パフォーマンス（2.59）を向上するために繰り返し行われる活動。

（JIS Q 27000:2014　2 用語及び定義　より引用）

パフォーマンス評価

これらの定義を使用すると、パフォーマンス評価は、「組織は、情報セキュリティの測定可能な結果を評価する。組織は、情報セキュリティマネジメントシステムの、計画した活動を実行し、計画した結果を達成した程度を評価する。」と言い換えることができます。

リスク及び機会に対処する活動の有効性の評価

JIS Q 27001:2014 ではリスクアセスメント・リスク対応を含むリスク及び機会に対処する活動の有効性を評価することを計画し、実施することを求めています。これには、リスク及び機会に対処する活動の仕組み全体（6.1 参照）が含まれています。有効性の評価を計画することを次に規定しています。

組織は，次の事項を計画しなければならない。
d）上記によって決定したリスク及び機会に対処する活動
e）次の事項を行う方法
　1）その活動の ISMS プロセスへの統合及び実施
　2）その活動の有効性の評価

（JIS Q 27001:2014　6.1.1 一般　より引用）

情報セキュリティプロセス及び管理策を含む、情報セキュリティパフォーマンスの評価をリスクアセスメント・リスク対応を含む活動の有効性評価にフィードバックし、その活動の改善、必要に応じて再度、リスクアセスメント・リスク対応を含む活動・プロセスを実施する改善等に向けたアクションを取ることになります。

本ガイドの「9.1.1 パフォーマンス評価」に「プロセスのパフォーマンス評価」と「管理策のパフォーマンス評価」を記載しています。

９．１　監視、測定、分析及び評価

組織は，情報セキュリティパフォーマンス及び ISMS の有効性を評価しなければならない。
組織は，次の事項を決定しなければならない。
a）必要とされる監視及び測定の対象。これには，情報セキュリティプロセス及び管理策を含む。
b）該当する場合には，必ず，妥当な結果を確実にするための，監視，測定，分析及び評価の方法
　注記 選定した方法は，妥当と考えられる，比較可能で再現可能な結果を生み出すことが望ましい。
c）監視及び測定の実施時期
d）監視及び測定の実施者
e）監視及び測定の結果の，分析及び評価の時期
f）監視及び測定の結果の，分析及び評価の実施者

組織は，監視及び測定の結果の証拠として，適切な文書化した情報を保持しなければならない。

（JIS Q 27001:2014　9.1 監視，測定，分析及び評価　より引用）

監視、測定、分析及び評価は、その対象を理解し測定することから始まります。対象を測定したら、その対象を評価するための指標を定めます。既存の指標から選定しても良いですし、組織自らが指標を開発することもできます。
監視及び測定の結果は、証拠として文書化した情報として保持することが要求されています。

JIS Q 27001:2014 の他の箇条との関連について説明します。例えば、「5 リーダーシップ」との関連では、5.3 b）で ISMS のパフォーマンスをトップマネジメントに報告するための責任及び権限を割り当てることを要求しており、ここでいう ISMS のパフォーマンスとは、9 のパフォーマンス評価の一部を指しているともいえます。
「5.3 組織の役割、責任及び権限」では責任と権限の割当てが要求されていますが、ISMS のパフォーマンスの評価結果をトップマネジメントに報告するということも重要なことです。トップマネジメントへの報告は、マネジメントレビューとも関連しており、マネジメントレビューの要求事項は「9.3 マネジメントレビュー」にある. 9.3 c）で情報セキュリティパフォーマンスに関するフィードバックをマネジメントレビューでは考慮するよう要求しています。

また、「6 計画」との関連でいいますと、6.1.1 e） 2）でリスク及び機会に対処する活動の有効性の評価を行う方法を計画することが要求されています。この有効性の評価を実施することがパフォーマンス評価の一部を指しています。

JIS Q 27001:2014 では、例えば、監視及び測定の実施時期について、及び監視及び測定の結果の分析及び評価の実施時期について明確にすることが要求されるようになり、JIS Q 27001:2006 と比較すると、より明確で具体的な要求事項となりました。

９．１．１　パフォーマンス評価
プロセスのパフォーマンス評価

情報セキュリティマネジメントシステムにおいては、個々のプロセスが要求される情報セキュリティ要求事項や期待を満たしていることを確実にするために、必要な PDCA を構築し、プロセスのインプット、アウトプット及びプロセスの振舞いに関して、情報セキュリティリスクに関する特性を考慮した監視・測定を行い、その結果を組織が決めた分析・評価の実施者（多くの場合、プロセスの管理責任者/リスク所有者）にフィードバックさせる機能を有することが、有効なマネジメントシステム確立のために重要となります。このことを、図 9-2 を基に考えてみるとより明確になります。

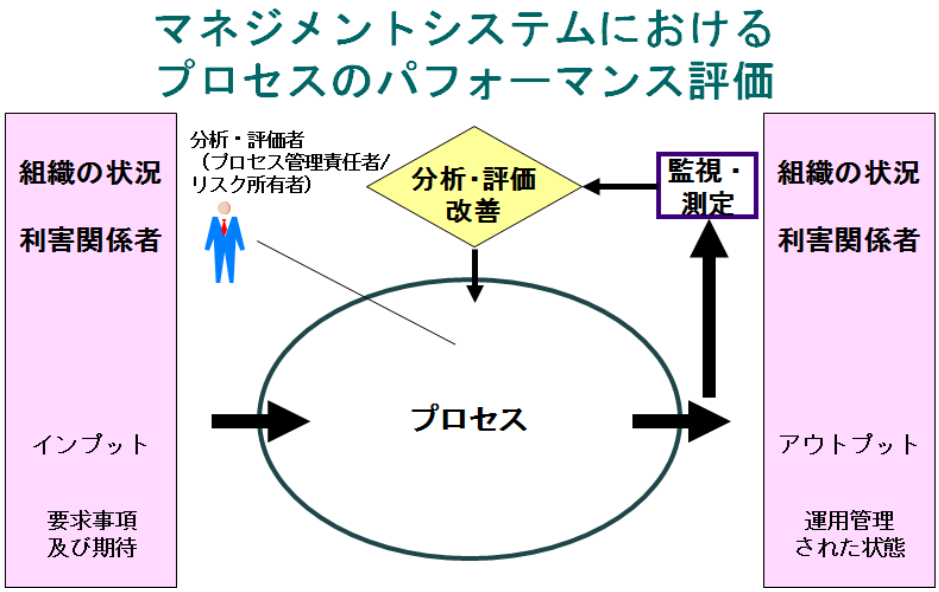


図 9-2　マネジメントシステムにおけるプロセスのパフォーマンス評価の位置づけ

図中の「分析・評価」は、情報セキュリティに関するプロセスの能力について、プロセスの監視、適用可能な場合には適切な方法により測定し、その結果を分析・評価することで行います。適切な方法とは、プロセスが計画通りの結果を達成する能力があることを実証する監視、測定であることです。比較可能で再現可能な結果を生み出すことが求められます。

一連の ISMS の活動は、複数のプロセスから構成されていると捉えることも可能です。従って、図 9-3 のように、複数のプロセスのパフォーマンスの測定及び評価の結果から、全体として、情報セキュリティパフォーマンス評価を得ることができます。

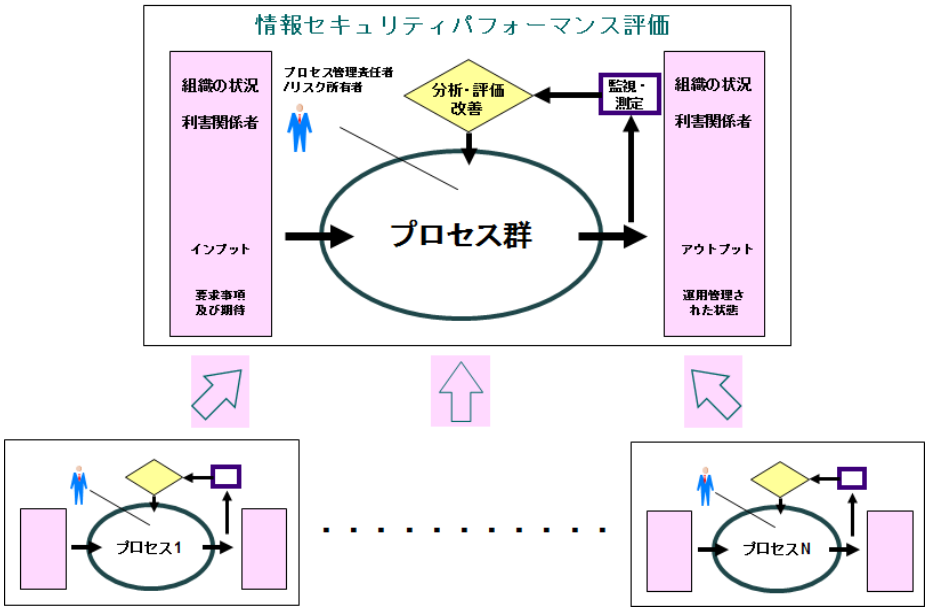


図 9-3　ISMS の情報セキュリティパフォーマンス

個々のプロセスのパフォーマンスを測定することは、そのプロセスに導入した管理策または一群の管理策のパフォーマンスを測定し、プロセス全体のパフォーマンスを把握するのに役立ちます。特に、一連のプロセスが複雑な場合、測定可能な個々のプロセスに分けて、各々の結果からプロセス全体のパフォーマンスを把握することは効果的な手法です。

管理策のパフォーマンス評価

管理策は、次のように定義されています。

> 2.16　管理策（control）
> リスク（2.68）を修正（modifying）する対策。
> （JIS Q 0073:2010 の 3.8.1.1 参照）
> 注記 1 管理策には，リスクを修正するためのあらゆるプロセス，方針，仕掛け，実務及びその他の処置を含む。
> 注記 2 管理策が，常に意図又は想定した修正効果を発揮するとは限らない。
>
> （JIS Q 27000:2014　2 用語及び定義　より引用）

管理策は、リスクを修正する対策であり、それには、方針、プロセス、手順、製品、サービス、技術、設備などが含まれます。プロセス、手順の場合は、前述の「プロセスのパフォーマンス評価」で述べていますが、プロセス、手順以外の場合は、その対策の特性を監視、測定し、情報セキュリティ要求事項が満たされていることを検証することが求められます。

そのような管理策のパフォーマンスを測定し評価する上で、
・管理策の配下にある情報及び情報に関連する資産やそれらをとりまく環境
・リスクアセスメントの結果等
などがパフォーマンス評価のインプットとして役立ちます。

特に直感的に管理策のパフォーマンスを測定する上で役立つインプットとしては、インシデントや管理策の配下の情報及び情報に関連する資産の状態などが考えられます。影響が大きいインシデントが複数回起きた、また、管理策配下の資産が既に消去されているなどの場合、管理策はもはやそのリスクを修正する対策としての能力がないと即座に導くことが可能です。このことは、パフォーマンスの測定プロセスにはインシデント管理、情報及び情報に関連する資産の管理等との密接な連携を取り合う仕組みが必要であることを示唆しています。

管理策または一群の管理策に対して、パフォーマンスを測定するための測定表などを用いて測定したことによって把握できた内容のことを「情報セキュリティパフォーマンス測定の結果」といい、パフォーマンスの分析・評価のインプットになります。

この際、情報セキュリティの目的、すなわち情報の C（機密性）、I（完全性）、A（可用性）の維持という視点から、また必要に応じて真正性、責任追跡性、否認防止及び信頼性のような特性の維持のために、実行している管理策のパフォーマンスを評価する必要があります。情報セキュリティでは、よく機密性と可用性の維持をバランス良くとっていくことが困難であるといわれています。機密性を高めれば利便性が損なわれ（可用性が低下し）、可用性を高めれば機密性は損なわれる可能性が高くなるという情報セキュリティの特性の中で、各プロセスのリスクに応じるために実施、運用している管理策のパフォーマンス測定結果を評価し、管理策をチューンアップしていくことは、重要なプロセスです。

また、管理策は、維持させたい情報セキュリティの特性、すなわち C（機密性）、I（完全性）、A（可用性）毎に異なる場合があります。例えば、機密性であれば暗号化、可用性であればシステムの冗長化という具合に管理策を考えることが通常です。その際、個別に暗号化のみのパフォーマンス測定や冗長化のみのパフォーマンス測定を評価しても、プロセスがもつ両方の管理策がはたして組み合わさってその能力をもたらしているかを評価していなければ、バランスがとれた管理策の実施には繋がりません。プロセス全般のリスクを考慮した上で、管理策または一群の管理策のパフォーマンス測定結果を評価することが効果的です。

フィードバックとしては、上記のようにプロセス全体を考慮して、管理策または一群の管理策のパフォーマンスについて評価を導き出すことは当然重要ですが、これらの評価結果をどのように活用するかを考慮することも重要です。パフォーマンス評価結果のフィードバック先としては、以下のように考えることが可能です。

・ 管理策または一群の管理策のパフォーマンスについて測定・評価した場合のフィードバック先：
  ■ ISMS の情報セキュリティパフォーマンス評価へのインプット
    ISMS の情報セキュリティパフォーマンス評価の一要素として活用する。
  ■ リスクアセスメント・リスク対応プロセス
    プロセスの管理責任者/リスク所有者に報告し、リスクアセスメント・リスク対応の結果の妥当性確認や必要に応じて再リスクアセスメントを実施し、追加の管理策の必要性等を検討する。
  ■ 監視（モニタリング）プロセス
    パフォーマンス評価をする上で必要な監視について再検討する
  ■ インシデント管理
    測定・評価結果を基に、インシデント対応をするための基準等を再検討する
  ■ パフォーマンス測定・評価プロセス
    パフォーマンス評価結果を基に、パフォーマンスの測定及び評価の方法自体や測定及び評価の頻度などについて再検討する等

上記は、パフォーマンスに関する報告として、トップマネジメントに伝えられ（JIS Q 27001:2014 の 5.3 b））、またマネジメントレビューのインプットとして活用されます（9.3 c）2））。

９．１．２　パフォーマンス測定

パフォーマンスを測定するためには、まずどのように測定するかを定義しておく必要があります。
JIS Q 27001:2014 では、パフォーマンス測定の方法を以下のように規定しています。

> 組織は，情報セキュリティパフォーマンス及び ISMS の有効性を評価しなければならない。
> 組織は，次の事項を決定しなければならない。
> a）必要とされる監視及び測定の対象。これには，情報セキュリティプロセス及び管理策を含む。
> b）該当する場合には，必ず，妥当な結果を確実にするための，監視，測定，分析及び評価の方法
> 注記　選定した方法は，妥当と考えられる，比較可能で再現可能な結果を生み出すことが望ましい。
>
> （JIS Q 27001:2014　9.1 監視，測定，分析及び評価　より引用）

例えば、JIS Q 27001:2014 の 9.1a)に記載の、測定の対象に含まれる管理策のパフォーマンス測定を定義付ける場合、以下のような項目を考慮すると比較可能で再現可能な測定に役立つでしょう。

- ■ 管理策の目的
  組織にとって当該管理策の目的は何なのかを明確化する。管理策を実施した結果、この目的を達成したかどうかが、管理策に能力があるかどうかのポイントとなる。
- ■ 測定する単位
  選択した管理策又は関連する管理策をグループ化した一群の管理策の単位で、測定を実施するのかを定義する。
- ■ パフォーマンス測定の方法
  パフォーマンスを測定するために必要な項目を定義する。
  また、その方法は比較可能で再現可能な結果を生み出す必要がある。
- ■ パフォーマンスを評価（判定）する方法
  測定された結果を基に、パフォーマンスを評価するための方法を定義する。
  また、その方法は比較可能で再現可能な結果を生み出す必要がある。
- ■ 測定結果のフィードバック先
  測定結果のフィードバック先を定義する。
  測定結果は、管理策のパフォーマンスの評価で活用され、管理策が能力あると認められない場合は、改善実施のために活用する。

パフォーマンス測定の方法に関するポイント

パフォーマンス測定を定義する場合、次の 2 つの視点を考慮すると、測定に対し評価や判定を行なう上で有用であると考えられます。

パフォーマンスを測定するためには、まず何を測定するかを定義する必要があります。パフォーマンス評価のための活用を考慮して、例えば次の 2 つの項目の測定が考えられます。

a）実施度
実施度は管理策を実装し運用した結果、計画した管理策に対してどの程度実施されたかを測定したものを言います。この測定値は、管理策の実装・運用の妥当性をチェックしたり、そのような実装・運用で不足しているものを特定するために使用します。

b）達成度
達成度は計画した管理策を実施した結果、それに対して計画した情報セキュリティ目的が達成された程度（目的の達成度）を言います。この測定値は、セキュリティ管理策の実装・運用が、当初の当該管理策の目的や目標を達成するために能力を果たしかどうか評価し、機能していない場合は管理策の実装・運用の仕方を改善するために使用します。

上記のように管理策の a）実施度、b）達成度を測定することにより、パフォーマンスを評価し、管理策の改善に向けた対応を実施することが可能となります。

パフォーマンス測定手順書の概要例

JIS Q 27001:2014 では、パフォーマンスに関する「文書化に関する要求事項」を以下のように規定しています。

組織は，監視及び測定の結果の証拠として，適切な文書化した情報を保持しなければならない。

（JIS Q 27001:2014　9.1 監視，測定，分析及び評価　より引用）

これまでのパフォーマンス測定に関する内容をまとめて、以下に文書化する上で有用だと思われる項目を例示します。

「パフォーマンス測定手順の概要」（例示）

１．パフォーマンス測定概要
　　１－１　概要及び目的
　　１－２　適用範囲
　　１－３　改訂履歴
２．測定手法
　　２－１　プロセス/管理策の目的/目標の設定
　　２－２　実施度と達成度
　　２－３　測定値及び算定式の定義
　　２－４　測定体制
３．パフォーマンスの評価
　　３－１　評価の方法
　　３－２　評価結果への対応
　　　３－２－１　能力があると評価された管理策
　　　３－２－２　機能していなく改善が必要と評価された管理策
　　　３－３－３　経過監視が必要と評価された管理策

添付１．プロセス/管理策パフォーマンス測定票（プロセス/管理策毎又は一群のプロセス/管理策）

９．２　内部監査

組織は，ISMS が次の状況にあるか否かに関する情報を提供するために，あらかじめ定めた間隔で内部監査を実施しなければならない。
a)　次の事項に適合している。
　1）ISMS に関して，組織自体が規定した要求事項
　2）この規格の要求事項
b）有効に実施され，維持されている。

組織は，次に示す事項を行わなければならない。
c）頻度，方法，責任及び計画に関する要求事項及び報告を含む，監査プログラムの計画，確立，実施及び維持。監査プログラムは，関連するプロセスの重要性及び前回までの監査の結果を考慮に入れなければならない。
d）各監査について，監査基準及び監査範囲を明確にする。
e）監査プロセスの客観性及び公平性を確保する監査員を選定し，監査を実施する。
f）監査の結果を関連する管理層に報告することを確実にする。
g）監査プログラム及び監査結果の証拠として，文書化した情報を保持する。

（JIS Q 27001:2014　9.2 内部監査　より引用

内部監査においては、ISMS の取組みが組織の規定した要求事項に従って実施されているか、JIS Q 27001:2014 の要求事項に適合しているか、有効に実施され継続的に維持されているかを評価します。

また、内部監査の手順を含む監査プログラムについて文書化が要求されています。監査プログラムには、内部監査の計画、実施、報告、フォローアップの一連の流れと、関連する記録の保持についての責任、力量及び要求事項を文書化することが要求されています。
なお、監査基準、監査範囲についても明確化を求めています。監査員の選定については、監査プロセスの客観性及び公平性を確保することを要求しています。
これは、有益な監査結果を得るために重要なことです。監査員の独立性については、JIS Q 19011:2012「マネジメントシステム監査のための指針」では次のように説明しています。

> 4　監査の原則
> e）独立性：監査の公平性及び監査結論の客観性の基礎
> 監査員は，実行可能な限り監査の対象となる活動から独立した立場にあり，全ての場合において偏り及び利害抵触がない形で行動することが望ましい。内部監査では，監査員は監査の対象となる機能の運営管理者から独立した立場にあることが望ましい。監査員は，監査所見及び監査結論が監査証拠だけに基づくことを確実にするために，監査プロセス中，終始一貫して客観性を維持することが望ましい。
> 小規模の組織においては，内部監査員が監査の対象となる活動から完全に独立していることは難しい場合もあるが，偏りをなくし，客観性を保つあらゆる努力を行うことが望ましい。
>
> （JIS Q 19011:2012　より引用）

なお、内部監査の結果は、マネジメントレビューの重要な検討項目となります。

内部監査自体の有効性を向上させるためには、内部監査の仕組みの拡充や、そこから出てくるチェックリストなどの様式類の内容、内部監査での焦点の明確化（内部監査における重点確認事項の明確化）といったことと共に、内部監査員の力量を向上させるということも重要です。すなわち、良い指摘や、指摘への対応に関連する有益なコメントを出せる内部監査員を確保することです。

そのためには、内部監査員に対する力量基準と力量評価方法を十分に検討することが必要です。内部監査員の力量基準について、例えば、JIS Q 27001:2014 の理解、JIS Q 19011:2012 の理解、組織の ISMS に関連する法規制要求事項の理解、組織の作成した情報セキュリティ関連文書の理解、組織の業務における情報セキュリティ側面の理解、業務経験、コミュニケーション能力といった力量基準が挙げられます。

また、監査員に求める力量は上述のように組織全般に対する専門性、マネジメントシステムに対する専門性、情報セキュリティの専門性といった多岐にわたる力量が要求されるため、場合によっては、情報セキュリティ監査制度、システム監査制度を利用し、専門家に内部監査の実施を依頼することも考えられます。

従来の JIS Q 27001:2006 と比較すると、内部監査について、MSS 共通要素を適用したことによる表現の変更はあるものの、内容についての大幅な変更は無いといえます。また、表現の変更の例としては、JIS Q 27001:2006 では、6 a）で、「この規格及び関連する法令又は規制要求事項に適合しているかどうか」と内部監査での判断事項として「関連する法令又は規制要求事項の適合状況」を含めていましたが、JIS Q 27001:2014 では、「この規格の要求事項」との記述となり、「関連する法令又は規制要求事項」という文言は削除されています。
この理由は、「4.2 利害関係者のニーズ及び期待の理解」の注記で、「利害関係者の要求事項には、法的及び規制の要求事項並びに契約上の義務に含めてもよい」と記述しており、

利害関係者の要求事項は、この規格の要求事項であるので特に「関連する法令又は規制要求事項」を明記することにはならなかったといえます。

９．３　マネジメントレビュー

トップマネジメントは，組織の ISMS が，引き続き，適切，妥当かつ有効であることを確実にするために，あらかじめ定めた間隔で，ISMS をレビューしなければならない。
マネジメントレビューは，次の事項を考慮しなければならない。
a）前回までのマネジメントレビューの結果とった処置の状況
b）ISMS に関連する外部及び内部の課題の変化
c）次に示す傾向を含めた，情報セキュリティパフォーマンスに関するフィードバック
　1）不適合及び是正処置
　2）監視及び測定の結果
　3）監査結果
　4）情報セキュリティ目的の達成
d）利害関係者からのフィードバック
e）リスクアセスメントの結果及びリスク対応計画の状況
f）継続的改善の機会

マネジメントレビューからのアウトプットには，継続的改善の機会，及び ISMS のあらゆる変更の必要性に関する決定を含めなければならない。
組織は，マネジメントレビューの結果の証拠として，文書化した情報を保持しなければならない。

（JIS Q 27001:2014　9.3 マネジメントレビュー　より引用）

マネジメントレビューは、トップマネジメントが俯瞰的視点から、ISMS 全体の取組みを定期的に確認し、構築・維持された ISMS について改善する必要があるのか、変更する必要があるのかについて判断するプロセスです。

マネジメントレビューは、組織が定めた間隔で実施する必要があります。マネジメントレビューでの考慮事項としては、前回までのマネジメントレビューの結果によりとった処置の状況、ISMS に関連する外部及び内部の課題の変化、情報セキュリティパフォーマンスに関するフィードバック、利害関係者からのフィードバック、リスクアセスメントの結果及びリスク対応計画の状況、継続的改善の機会が求められています。

ここからは、マネジメントレビューについての詳細を説明します。

JIS Q 27001:2014 では、プロセス及び管理策のパフォーマンスを評価し、それに基づいて ISMS 全体の有効性を評価することを示しています。パフォーマンス評価及び有効性の評価結果を、ISMS の継続的な改善の機会と捉え、マネジメントが適切な行動をとることを促し、組織の情報セキュリティ目的及び事業（業務）目的を達成すること、プロセス及び管理策の実施を含む活動、計画を推進し、マネジメントシステムをより有効な確実なものとしていくことは重要な意味を持ちます。トップマネジメントは、マネジメントレビューの結果として以下の事項について決定しなければいけません。

- **継続的改善の機会**
- **情報セキュリティマネジメントシステムのあらゆる変更の必要性**

パフォーマンス評価は、マネジメントレビューに必要なインプット情報の収集に関する項目を主な監視・測定の対象の題材として含めることになるでしょう。トップマネジメントはマネジメントレビューを実施し、マネジメントシステムが定められたプロセス・手順に従ってプロセスが実施されているか、また計画の段階で期待されている成果が予定通り上がっているか検証します。これは ISMS の維持や継続的な改善活動に必要不可欠な作業です。

これらの活動については、JIS Q 27001:2014 の「5 リーダーシップ」から「10 改善」に規定されています。具体的内容については、本ガイドの「5 リーダーシップ」以降の各章（9 章以外）の説明を参照して下さい。

トップマネジメントは、ISMS のパフォーマンスに関する情報を直接入手する仕組みを持たねばならないことが規定されています。

> 5.3 組織の役割，責任及び権限
> トップマネジメントは，情報セキュリティに関連する役割に対して，責任及び権限を割り当て，伝達することを確実にしなければならない。
> トップマネジメントは，次の事項に対して，責任及び権限を割り当てなければならない。
> a) ISMS が，この規格の要求事項に適合することを確実にする。
> b) ISMS のパフォーマンスをトップマネジメントに報告する。
>
> （JIS Q 27001:2014　5.3 組織の役割，責任及び権限　より引用）

トップマネジメントの責任として、マネジメントレビューの実施が重要であることは 5.1 で触れましたが、このマネジメントレビューは、ISMS を維持し、今後の活動を効果的に実施するために必要な活動です。これは、「パフォーマンス評価」のプロセスに属します。ISMS が意図した通り有効に機能していることをトップマネジメント自身が把握し、改善のための意思決定等を行います。

マネジメントレビューとは、トップマネジメントが ISMS の効果を把握し、改善のための意思決定をする一連のプロセスです。ISMS のマネジメントレビューは、あらかじめ定められた間隔で実施しなければなりません。
マネジメントレビューでは、ISMS に対する改善の機会の評価、情報セキュリティ目的の達成を含む ISMS の変更の必要性に関する評価を実施することになります。また、マネジメントレビューの結果は、文書化した情報（記録）として維持されていることが必要です。

（1）マネジメントレビューへのインプット

マネジメントレビューのためのインプット情報として、JIS Q 27001:2014 では次のものを挙げています。

> マネジメントレビューは，次の事項を考慮しなければならない。
> a）前回までのマネジメントレビューの結果とった処置の状況
> b）ISMS に関連する外部及び内部の課題の変化
> c）次に示す傾向を含めた，情報セキュリティパフォーマンスに関するフィードバック
> 1）不適合及び是正処置
> 2）監視及び測定の結果
> 3）監査結果
> 4）情報セキュリティ目的の達成
> d）利害関係者からのフィードバック
> e）リスクアセスメントの結果及びリスク対応計画の状況
> f）継続的改善の機会
>
> （JIS Q 27001:2014　9.3 マネジメントレビュー　より引用）

マネジメントレビューへのインプットとして具体的には次のようなものが挙げられます。

- ■ 過去のマネジメントレビューの結果に適切に対応したかどうかについてのフォローアップの状況等についての報告
- ■ 情報セキュリティマネジメントシステムに関連する外部及び内部の課題の変化

－経営環境の変化、組織の変化などを含む ISMS に影響を及ぼす可能性のある全ての組織内外の変化
－新たに利用可能となった技術、ベンダー等が発表した新製品・新サービスに関する情報

■ 傾向を含めた、情報セキュリティパフォーマンスに関するフィードバック
－実施した予防処置及び是正処置の実施状況及びその効果
－不適合及び是正処置
－とった処置の状況処理の誤りや、セキュリティインシデントの記録を含む監視及び測定の結果
－監査結果
－情報セキュリティ目的の達成（目的を達成するための計画及び活動、すなわち、リスク対応計画や是正計画、資源計画、教育計画などの実施状況、目的の達成状況に関するフィードバックを含む）

■ プロセス/管理策または一群のプロセス/管理策に対して、パフォーマンスを測定するための測定表などを用いて測定したことによって把握できた内容
■ 内部監査や外部監査の結果（例えば、認証機関による不適合の指摘や観察事項など）
■ 顧客、取引先、従業員といった利害関係者からのフィードバック
■ リスクアセスメントの結果及びリスク対応計画の状況
■ 継続的改善の機会

（2）マネジメントレビューからのアウトプット

トップマネジメントは、インプットされた情報に基づいて経営的な判断、つまり経営の意思決定を行わなければなりません。その際の意思決定のポイント、つまりマネジメントレビューからのアウトプットとして、JIS Q 27001:2014 では次の 2 つの事項を挙げています。

> マネジメントレビューからのアウトプットには，継続的改善の機会，及び ISMS のあらゆる変更の必要性に関する決定を含めなければならない。
>
> （JIS Q 27001:2014　9.3 マネジメントレビュー　より引用）

トップマネジメントは、マネジメントレビューのアウトプットとして、現状の ISMS をより効果的なものにするための改善を示さなければなりません。

また、ISMS の組織及びその状況（JIS Q 27001:2014　4.1）、利害関係者のニーズ及び期待（JIS Q 27001:2014　4.2）が変化している場合は、それらの変化に対応して、ISMS の適用範囲、方針、リスク及び機会に対処する活動、情報セキュリティを実現する手順を見直し、修正しなければなりません。これら組織及びその状況、及び利害関係者のニーズ及び期待に関するものとしては、例えば次のようなものが含まれることが考えられます。

ISMS に影響を与える可能性がある内外の事象に対応するために、必要に応じた、情報セキュリティを実現する手順及び管理策の修正が必要となります。そのような事象には、次について起きた変化が含まれます。

1）事業上の要求事項
2）情報セキュリティ要求事項
3）現在の事業上の要求事項を実現する業務プロセス
4）法令又は規制の要求事項
5）契約上の義務
6）リスクのレベル及び／又はリスク受容基準

「1）事業上の要求事項」としては事業ドメインの重要性に変化が生じた場合、また「3）現在の事業上の要求事項を実現する業務プロセス」としては業務プロセスに変更が行わ

れた場合などが考えられ、そのような場合には、現在実施されている情報セキュリティ対策が引き続き適切であることを確認しなければなりません。

「4）法令又は規制の要求事項」としては、新たな法令の施行、既存の法令の改正、規制の新設、改正が行われている場合が考えられます。その場合、現在のプロセスが引き続き法令等に準拠していることを確認することは重要です。個人情報保護法、ｅ文書法、知的財産関連の法令、IT 関連の法令、不正競争防止法など ISMS 構築に当たって特定した法令の施行、改正や、判例にも注意を払う必要があります。

「5）契約上の義務」は他社との関係をもつ業務であり、このような業務では、その相手方と締結した契約上の義務についても順守しなければなりません。これについては相手方が個別に求めてくるものですので、その内容を個々に確認することが必要です。また、求められる実施事項が具体的になっていない場合には、相手方に対して何をもって義務を果たしたことになるのかなどを確認しておくことが必要です。

「2）情報セキュリティ要求事項」や「6）リスクのレベル及び／又はリスク受容基準」に関しても注意が必要です。情報技術の進歩は著しく、それに伴って新たな脅威（例えば、新しい攻撃手法の出現）が生じたり、新たなぜい弱性（例えば、新たなオペレーティングシステムやアプリケーションシステムのぜい弱性）が発見されたりします。また、既存の対応策に関するぜい弱性が変化し、リスクの度合いが変化することもあります。このような環境変化に対応して情報セキュリティを実現する手順を修正することが重要です。

トップマネジメントは、マネジメントレビューを通じて必要と認識された、ISMS の改善のために必要となる経営資源の提供についても確約する必要があります。改善に必要な経営資源の提供が確約されなければ、改善の実施は達成されないからです。

１０．改善

１０．１　不適合及び是正処置

不適合が発生した場合，組織は，次の事項を行わなければならない。
a）その不適合に対処し，該当する場合には，必ず，次の事項を行う。
 1）その不適合を管理し，修正するための処置をとる。
 2）その不適合によって起こった結果に対処する。
b）その不適合が再発又は他のところで発生しないようにするため，次の事項によって，その不適合の原因を除去するための処置をとる必要性を評価する。
 1）その不適合をレビューする。
 2）その不適合の原因を明確にする。
 3）類似の不適合の有無，又はそれが発生する可能性を明確にする。
c）必要な処置を実施する。
d）とった全ての是正処置の有効性をレビューする。
e）必要な場合には，ISMS の変更を行う。

是正処置は，検出された不適合のもつ影響に応じたものでなければならない。
組織は，次に示す事項の証拠として，文書化した情報を保持しなければならない。
f）不適合の性質及びとった処置
g）是正処置の結果

（JIS Q 27001:2014　10.1 不適合及び是正処置　より引用）

10.1 では、不適合が発生した場合の処置について、及び処置の文書化について規定しています。ここでは、不適合と是正処置について説明します。

不適合とは、JIS Q 27000:2014 では「要求事項を満たしていないこと」と定義されています。ISMS における要求事項の例として次が挙げられます。

- JIS Q 27001:2014 の規格要求事項
- JIS Q 27001:2014 に基づいて組織が自ら定めた要求事項
- 法規制による要求事項
- 顧客からの契約による要求事項

是正処置とは、JIS Q 27000:2014 では「不適合の原因を除去し、再発を防止するための処置」と定義されています。不適合の原因を除去するためには、まず、何故、その不適合が起きたのかを根本原因にまで遡って突き止める必要があります。その上で、根本原因を除去する処置を実施することで、不適合の再発を防止することが可能となります。根本原因の遡及が不足していると、その遡及が不足した原因を除去するための処置が是正処置となることから、本当の原因に対する是正処置とならず、不適合が再発する可能性があるため、根本原因の妥当性評価を十分にすることが重要となります。

また、10.1 の要求事項に対応する上での留意事項として、次が考慮されます。

－「修正」（10.1 a）1）で言及）と「是正処置」（10.1 b）で言及）は、異なります。修正は、従来の JIS Q 27001:2006 の是正処置、予防処置に記載されていませんでした。以下の定義を参照して下さい。

－「類似の不適合の有無、又はそれが発生する可能性を明確にする。」（10.1 b）3））は、是正処置の水平展開にあたりますが、従来の JIS Q 27001:2006 の予防処置にあたるものでもあります。

－ 有効性のレビュー（10.1 d）で言及）は、従来の JIS Q 27001:2006 の是正処置、予防処置に記載されていませんでした。有効性の意味については、以下の定義を参照して下さい。

2.18 修正（correction）
検出された不適合（2.53）を除去するための処置。

2.19 是正処置（corrective action）
不適合（2.53）の原因を除去し，再発を防止するための処置。

2.24 有効性（effectiveness）
計画した活動を実行し，計画した結果を達成した程度。

2.53 不適合（nonconformity）
要求事項（2.63）を満たしていないこと。

（JIS Q 27000:2014 2 用語及び定義 より引用）

例えば、不適合と是正処置について教育・訓練を例として挙げてみます。ISMS の適用範囲内に新たに配属された要員については、配属後のオリエンテーションにおいて、ISMS に関する教育を実施する必要があるとしていたのだが、新規に配属された要員の教育を確認した結果、特に ISMS に関する教育をオリエンテーション時に実施していなかったという不適合があったとします。

新規配属者に対して ISMS に関する教育を実施するということが修正であり、それを更に掘り下げて、そもそもの教育・訓練の手順に不備はなかったのか、手順に対する周知状況に不備がなかったのか、手順の実施状況の確認・承認に問題が無かったのかなど、不適合の原因を突き詰めたうえで、同様なことが他の部門でも存在しないか、潜在的に発生しうるかなどを明らかにし、不適合の再発、または他での発生の防止を確実にするための処置が是正処置となります。

さらに、発見された不適合についての対応については、文書化した情報として保持しておく必要があります。すなわち、文書化した情報とは、不適合の性質及びとった処置、是正処置の結果を示す証拠です。不適合の性質とは、不適合の内容や、不適合が及ぼした ISMS への影響であり、とった処置とは、不適合についての対応であり、是正処置の結果とは、不適合についての対応が狙い通り機能しているか、効果測定を基にした結果を記録することです。

なお、従来の JIS Q 27001:2006 と比較すると、より拡充した要求事項となったといえます。例えば、不適合に対して、修正と是正処置とを分けて要求するようになったことや、類似の不適合の有無や類似の不適合が発生する可能性を明確にすることが要求されるようになりました。

10.1 を含む１０章のプロセスを例示すると図 10-1 のようになります。

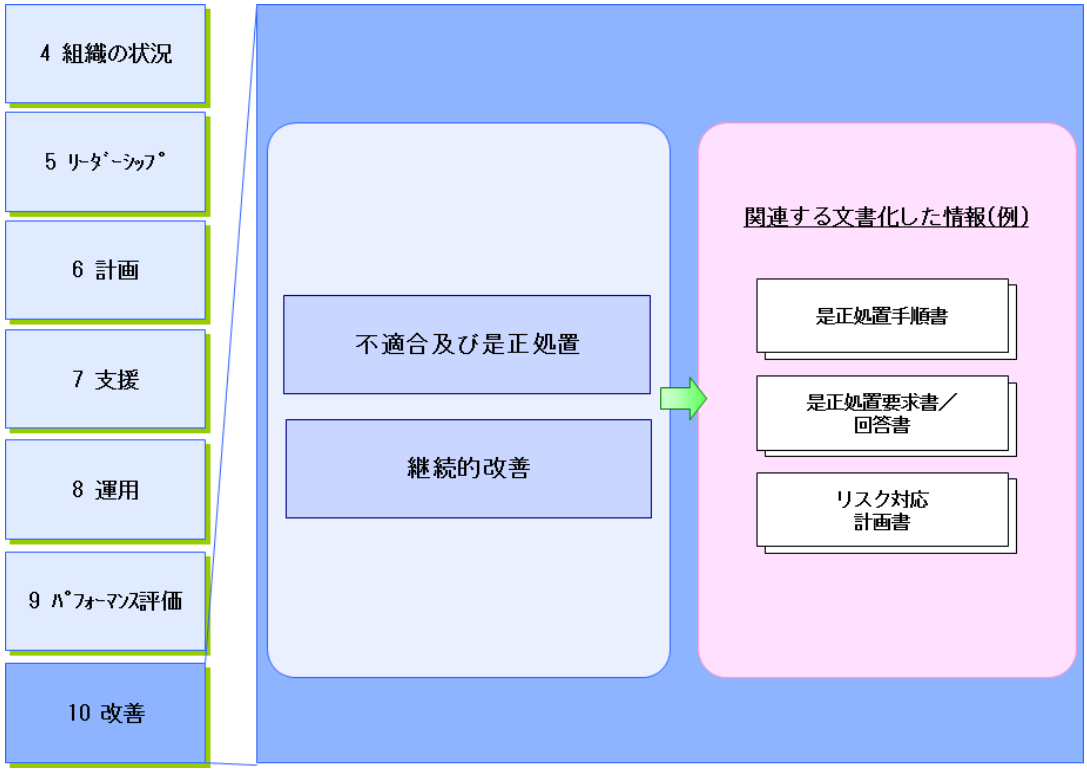


図 10-1　改善のプロセス　　注）文書名は全て例示

１０．２　継続的改善

組織は，ISMS の適切性，妥当性及び有効性を継続的に改善しなければならない。 （JIS Q 27001:2014　10.2 継続的改善　より引用）

10.2 では、組織に対して ISMS の適切性、妥当性及び有効性を継続的に改善することを規定しています。

ISMS の活動は、常に継続的改善に結び付けることが重要です。すなわち、情報セキュリティ方針及び目的、リスクマネジメント、監査結果、監視した事象の分析、是正処置、並びにマネジメントレビューを通じて、ISMS の適切性、妥当性及び有効性を継続的に改善することが重要となります。その際に、トップマネジメントがリーダーシップをとりコミットメントを示すことで、情報セキュリティ対策が確実に実施され、組織の ISMS の水準も継続して向上することが期待できます（5.1 g））。

例えば、継続的改善は、次のように定義されています。

2.15　継続的改善（continual improvement）
パフォーマンス（2.59）を向上するために繰り返し行われる活動。

2.59　パフォーマンス（performance）
測定可能な結果。
　注記 1　パフォーマンスは，定量的又は定性的な所見のいずれにも関連し得る。
　注記 2　パフォーマンスは，活動，プロセス（2.61），製品（サービスを含む。），システム，又は組織（2.57）の運営管理に関連し得る。
（JIS Q 27000:2014　2 用語及び定義　より引用）

上記の 2 つの定義をつなぎあわせると、継続的改善は、「測定可能な結果を向上するために繰り返し行われる活動」となります。

翻ってみると、継続的改善というのは、測定可能なものでなければならないという意味となります。10.2 をこれで言い換えると、「組織は、ISMS の適切性、妥当性及び有効性について、それらの測定可能な結果を向上するための活動を繰り返し行わなければならない。」となります。

また、継続的改善は continual improvement の訳ですので、continual ということから、時間的に切れ目なく連続である必要はなく、断続的でも継続して行われることを意味します。

この 10.2 の要求事項でいう ISMS の適切性とは、ISMS が組織の情報セキュリティ目的に合っている状態であることといえます。また、ISMS の有効性について、JIS Q 27000:2014 では次のように定義しています。

> 2.24　有効性（effectiveness）
> 計画した活動を実行し、計画した結果を達成した程度。
>
> （JIS Q 27000:2014　2 用語及び定義　より引用）

ISMS の有効性を改善するとは、情報セキュリティ目的が達成されるよう、さらに ISMS を改善することです。

例えば、10.1 で例示した JIS Q 27001:2014 の規格要求事項などに対する不適合が減少することなどが挙げられます。また、ISMS にかかわる各種の取組みについても、内部監査等で発見された不適合に対応し、継続的に維持・改善していく必要があります。その際は、ISMS の適切性、妥当性及び有効性の視点から適宜確認し、より組織に合った ISMS となるよう継続的に改善していくことが重要となります。

ISMS の適切性、妥当性及び有効性の視点から確認するとは

ISMS の適切性、妥当性及び有効性を継続的に改善するとは、言い換えると、ISMS が組織の情報セキュリティ方針及び情報セキュリティ目的に当てはまっている状態であるのかという適切性の視点、要求事項が満たされているのかなどの妥当性の視点、計画した活動が実行され、計画した結果が達成された程度という有効性の視点から適宜確認することといえます。

また、ISMS の有効性についての継続的改善と ISMS の重要な成功要因に関しては、ISO/IEC 27000:2014 の「3.5.6 ISMS の有効性を監視、維持及び改善する」や「3.6 ISMS の重要な成功要因」を参照されると良いでしょう。

附属書 A（規定）　管理目的及び管理策

附属書 A には、組織が ISMS を構築・導入する際に適用することができる 35 の管理目的と 114 の管理策が記載されています。

附属書 A は、JIS Q 27002 が改訂されたことを受けて、改訂版の JIS Q 27002:2014 との整合を保つよう変更されました。ここでは、その変更点について説明します。

A.1　附属書 A と JIS Q 27002:2014 との関係

従来の JIS Q 27001:2006 附属書 A が JIS Q 27002:2006 と整合がとられていたことと同じように、JIS Q 27001:2014 附属書 A も JIS Q 27002:2014 と整合がとられています。
JIS Q 27002 は、組織が ISMS を実施する際に、管理策を選定するための参考として用いることができるガイドラインであり、その箇条 5 から箇条 18 には、35 の管理目的と 114 の管理策について記述されています。

これらの管理目的、管理策は、その項番、内容とも、JIS Q 27001 附属書 A の管理目的、管理策と同じです。異なる点としては、2006 年版と同じく、項番については、JIS Q 27001 では附属書に記述されているため、項番の前に「A.」が付くことです。また、内容については、JIS Q 27001 は要求事項のため「～（し）なければならない」と記述されているのに対し、JIS Q 27002 はガイドラインであるため「～することが望ましい」と記述されていることです。この 2 点以外は、両者の管理目的、管理策は同じものです。
また、JIS Q 27002 は、ガイドラインであることから、管理目的、管理策以外にも、各管理策の内容を詳細に説明した「実施の手引」、さらには各管理策に関連する情報をまとめた「関連情報」も記載されています。そのため、JIS Q 27001 附属書 A をよりよく理解するには、JIS Q 27002 を参照すると良いでしょう。

A.2　JIS Q 27001:2014 附属書 A と JIS Q 27001:2006 の対比

JIS Q 27001:2014 附属書 A では、表 A-1 に示すとおり、多くの箇条において従来の JIS Q 27001:2006 の箇条との連続性が保たれています。

表 A-1　JIS Q 27001:2006 附属書 A との対応

JIS Q 27001:2014 附属書 A		JIS Q 27001:2006 附属書 A
A.5 情報セキュリティのための方針群		A.5 情報セキュリティ基本方針
A.6 情報セキュリティのための組織		A.6 情報セキュリティのための組織
A.7 人的資源のセキュリティ		A.8 人的資源のセキュリティ
A.8 資産の管理		A.7 資産の管理
A.9 アクセス制御		A.11 アクセス制御
A.10 暗号		
A.11 物理的及び環境的セキュリティ		A.9 物理的及び環境的セキュリティ
A.12 運用のセキュリティ		A.10 通信及び運用管理
A.13 通信のセキュリティ		
A.14 システムの取得，開発及び保守		A.12 情報システムの取得，開発及び保守
A.15 供給者関係		
A.16 情報セキュリティインシデント管理		A.13 情報セキュリティインシデントの管理
A.17 事業継続マネジメントにおける情報セキュリティの側面		A.14 事業継続管理
A.18 順守		A.15 順守

※対応がわかりやすいよう、JIS Q 27001:2006 附属書 A の項番は並べ替えています。

表 A-1 にみられるとおり、JIS Q 27001:2014 の附属書 A では JIS Q 27001:2006 の附属書 A の箇条をほぼ継承しています。ただし、2006 年版よりも箇条が 3 つ追加されています。追加された箇条については、以下のとおり、新規の内容もありますが、1 つの箇条が 2 つに分けられたものもあります。

表 A-2　追加の箇条

A.10 暗号：2006 年版の「A.12 情報システムの取得、開発及び保守」から、暗号に関する管理目的と管理策を移動して、独立の箇条となったものです。
A.13 通信のセキュリティ：2006 年版の「A.10 通信及び運用管理」が、2014 年版では「A.12 運用のセキュリティ」と「A.13 通信のセキュリティ」の 2 つの箇条に分けられたため、追加となったものです。
A.15 供給者関係：供給者を管理するための管理策をまとめた、新設の箇条です。2006 年版で別の箇条に記載されていた関連する管理策もここに移動されました。

また、今回、箇条と内容の整理が行われたことから、別の箇条へ移動された管理目的・管理策もあります。なお、従来の JIS Q 27001:2006 の附属書 A の管理策は 133 でしたが JIS Q 27001:2014 の附属書 A では管理策は 114 となっています。これは、新たな動向や技術の進歩に伴い、管理策が調整、変更、又は追加されたことによります。また、より幅広く一般に利用可能となるよう、技術的な詳細については他の規格を参照する方向にするなどの全体的な見直しも行われました。
詳細は、ISO/IEC JTC 1/SC 27/ WG 1 発行の新旧対比表「N13143：SD3 （Standing Document 3） Mapping Old-New Editions of ISO/IEC 27001 and ISO/IEC 27002」を参照して下さい。

http://isotc.iso.org/livelink/livelink/open/jtc1sc27

付録１　ISMS 構築・運用とコーポレートガバナンス（参考）

本ガイドの「5 リーダーシップ」では、ISMS の様々な活動において、トップマネジメント（経営陣）が果たすべき役割を説明しています。ここでは、さらにトップマネジメント（経営陣）の役割及び責任についてコーポレートガバナンスの視点から説明します。

ISMS の活動のあらゆる段階において、様々な活動が確実に実施されていることについて、トップマネジメントの果たすべき役割は非常に重要です。ISMS の対象を組織全体ではなく、ある組織階層とし、マネジメントの対象を限定する場合も多いと思われますが、その時でも組織全体としてのマネジメントを意識することが重要です。

トップマネジメントが ISMS の構築に関与することは、コーポレートガバナンスの視点からも重要です。コーポレートガバナンスとは、株式会社においては経営者による会社の経営責任を株主からの受託責任ととらえ、その遂行責任を問うものです。

コーポレートガバナンスは、「株主による取締役会及びそれを通じた執行者の統治」と、「執行者による企業運営の統治」の 2 つの局面が考えられます。執行者による企業の統治（運営）が行われずして、株主による取締役会及びそれを通じた執行者の統治は意味がありません。従って、まず執行者による企業の統治が重要となります。この統治を行うためにマネジメントが必要となります。

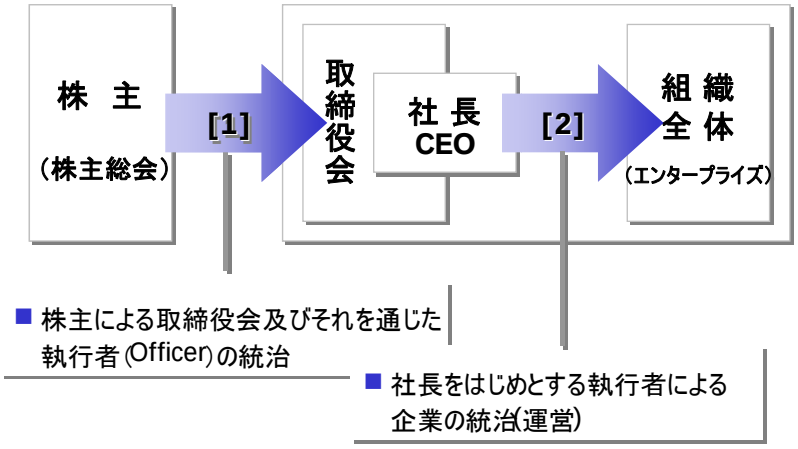


図 付 1-1　コーポレートガバナンス（ＣＧ）の２つの局面

執行者によるマネジメントの対象は多岐にわたります。マネジメントの対象の１つとして、情報セキュリティも考えることができます。その他、品質や環境もマネジメントの対象となります。

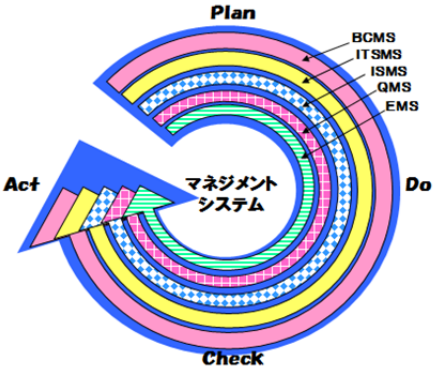


図 付 1-2　マネジメントシステムの対象

情報セキュリティ、品質、環境、IT サービス、事業継続のマネジメント・プロセスを手順化したものが、それぞれ ISMS、QMS、EMS、ITSMS、BCMS と言われるものです。これらのマネジメントシステムは事業全体を対象としたマネジメント、とりわけリスクマネジメントの一部として、企業の事業目的達成を側面から支援することになります。このことは組織論的には、事業全体のマネジメントができていないにもかかわらず、その一部にのみ力を入れても高い効果を得られないことを示唆しています。ISMS は、全体のマネジメントシステムとの関係を考えながら確立していくことが重要です。

また、企業グループ全体を統治することを必要とする組織においては、最近コーポレートガバナンスの観点から、法律上の企業体ではなく、支配力の及ぶ企業グループ全体についての統治、マネジメントの重要性が強調されています。連結経営などはその象徴といえます。ISMS も企業グループ全体で構築することが、コーポレートガバナンスの観点からは必要となります。

典型的な組織のマネジメントは、図 付 1-3 のように階層構造を持ち、下位組織階層のマネジメントシステムは上位組織階層のマネジメントシステムと協調して活動します。

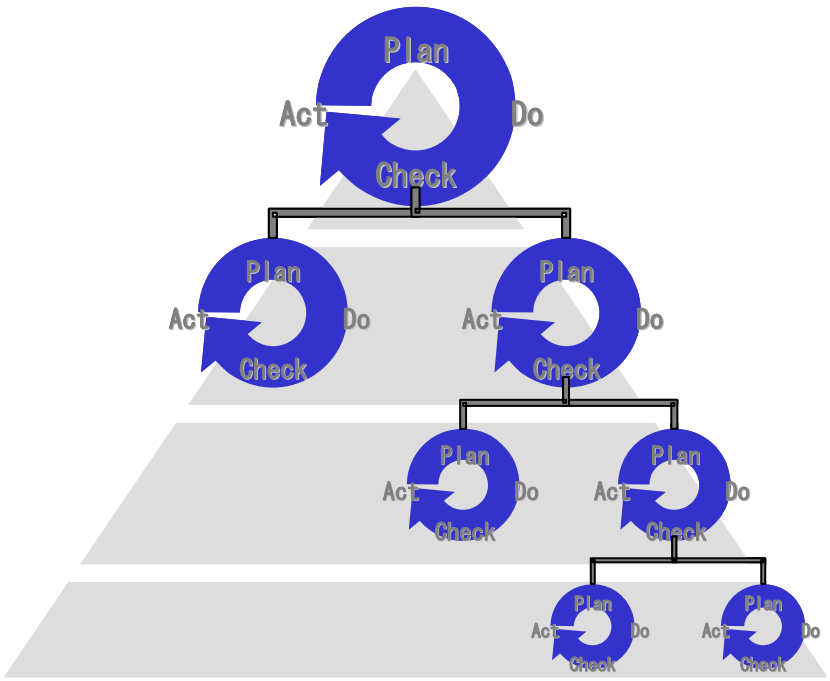


図 付 1-3　典型的な組織のマネジメントシステム

ISMS の構築の初期段階においては、適用範囲を限定し、特にリスクの大きい領域への対策を優先することに注力することもあります。しかし、トップマネジメントはその場合においても前述のマネジメントシステム間の連携を認識し、最終的に想定したゴールに導く責任を負います。

付録２　情報セキュリティリスクアセスメント（事例）

本ガイドの「6.1.2 情報セキュリティリスクアセスメント」では、リスク源を用いて情報セキュリティリスクアセスメントを説明しています。

リスク源とは、JIS Q 0073:2010 によると「それ自体又はほかとの組合せによって，リスクを生じさせる力を本来潜在的にもっている要素」です。
情報及び情報に関連する資産に対する脅威、ぜい弱性等は、リスク源の典型的な例といえます。リスクは、これらの組み合わせで構成される起こり得る事象・結果と、その起こりやすさとを合わせて表されます（詳細は、本ガイドの 6.1.2 の「（３）情報セキュリティリスクを特定（６．１．２ c））」を参照して下さい。）。

ここでは、情報セキュリティリスクアセスメント手法（以下の（１）、（２））を含め、情報及び情報に関連する資産、脅威、ぜい弱性（固有の弱点）をリスク源としたリスクアセスメント（以下の（３）以降）についての具体的な適用事例を説明します。

リスクアセスメントでは、組織が保有する情報及び情報に関連する資産を対象に以下の事項を把握します。

- リスクを受容するかどうかの判断基準は何か。
  また、情報セキュリティリスクアセスメントを実施するための基準、すなわち、実施時期、頻度、手法、プロセス、運用、モニタリング、見直し、改善などをどのようにするか。
- 情報セキュリティリスクアセスメントをマネジメントシステムに組み込んで、繰り返し実施することになるが、それが、一貫性及び妥当性があり、かつ、比較可能な結果を生み出すことを確実にするためには、どのような仕組みとするか。
- 情報の機密性、完全性及び可用性の喪失に伴うリスクにどのようなものが存在するか、そのリスクに対する責任及び権限を負う組織あるいは管理者は誰か。
- そのリスクが実際に生じた場合に起こり得る結果は何か、どの程度の影響を受けるか、及びそのリスクが現実的に発生する可能性はどの程度か、並びにこの影響の程度と発生する可能性によって、どれ位のレベルのリスクがもたらされるか。
- このリスクレベルを、リスク受容基準と比較して、リスク対応及びその優先度をどのように定めるか。

（１）適切な情報リスクアセスメント/リスク対応手法の選択

リスク特定とは、例えば、情報及び情報に関連する資産にとって、「発生しては困る脅威」と「固有の弱点（ぜい弱性）」を明確にすることです。この一連の組み合わせが出現すること、また組み合わせが変化することが、情報セキュリティ事象または情報セキュリティインシデントと呼ばれるものとなります。

リスク分析では、リスク個別の情報及び情報に関連する資産の価値と、脅威、ぜい弱性を総合的に分析し、リスクレベルを導き出し、それをリスク受容基準に照らし合わせて、リスク対応の要否とリスクの大小（対処の優先度）を判別するリスク評価を行い、リスク対応が必要とされた情報及び情報に関連する資産に対して効率的な保護対策を打つことが求められます。

以下に紹介するリスクアセスメントの手法の特徴を理解し、JIS Q 27001:2014 の「4.1 組織及びその状況の理解」に示される課題と「4.2 利害関係者のニーズ及び期待の理解」により洗い出される要求事項とを考慮し、「組織の保有する情報及び情報に関連する資産」、「情報セキュリティ上の要求事項」に基づいてリスクアセスメントのプロセスを決定して下さい。

図 付 2-1 は情報セキュリティリスクアセスメント/リスク対応の手法を中心に、プロセスの事例を示したものです。

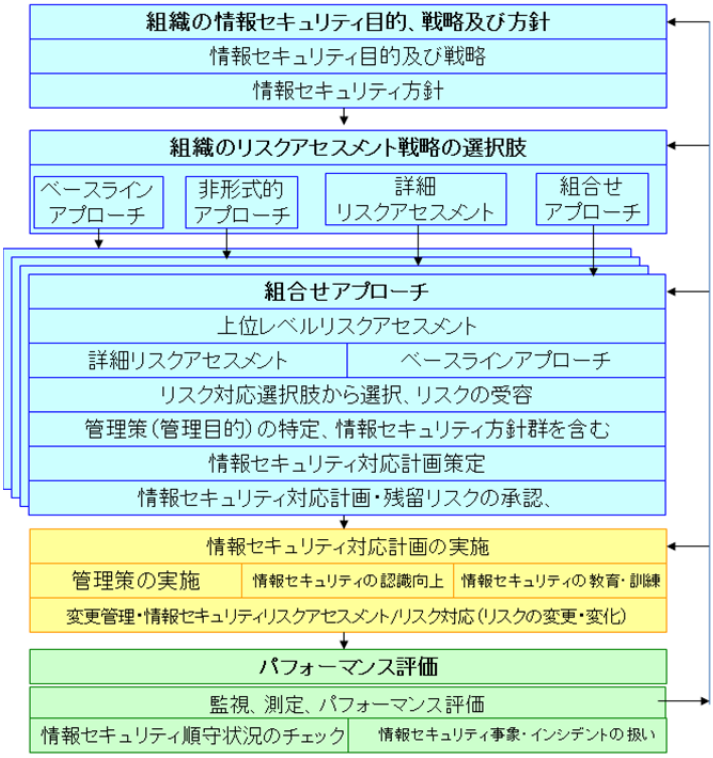


図 付 2-1　情報セキュリティリスクアセスメント/リスク対応を中心とした事例

（２）リスクアセスメントの手法

次に、情報セキュリティリスクアセスメントを実施するための基準として 4 つのアプローチを紹介します。

■ **ベースラインアプローチ（Baseline Approach）**
あらかじめ一定の確保すべきセキュリティレベルを設定し、実装するのに必要な対策を選択し、対象となるシステムに一律に適用することを指す

■ **非形式的アプローチ（Informal Approach）**
組織や担当者の経験や判断によってリスクを評価することを指す

■ **詳細リスクアセスメント（Detailed Risk Assessment）**
システムについて詳細なリスクアセスメントを行うアプローチで、資産に対し、「資産価値」、「脅威」、「ぜい弱性」やセキュリティ要件を識別し、評価することを指す

■ **組合せアプローチ（複合アプローチ）（Combined Approach）**
複数のアプローチを併用し、それぞれのアプローチの長所短所を相互に補完し、作業の効率化や分析精度の向上を図る

①ベースラインアプローチ

ベースラインアプローチとは、後述する詳細リスクアセスメントと異なり、資産ごとのリスク評価はしません。また単独で使用せず、他のアプローチと組み合わせて使います。

一般の情報セキュリティに関する基準や、業種・業界で採用されている標準やガイドラインなどを参照し、組織全体で共通のセキュリティ対策を実施します。実現可能な水準の管理策を採用し、組織全体でセキュリティ対策に抜け漏れが無いように補強していくアプローチです。

ベースラインアプローチは、大きく分けると以下の 2 つの手順で実施されます。

- **ベースラインの決定**
- **ギャップ分析の実施**

ベースラインアプローチでは、組織の達成する情報セキュリティ管理について独自の「対策の標準」を作成します。一般に、この対策の標準のことを「ベースライン」と呼びます。

しかし、JIS Q 27001:2014 では、情報セキュリティマネジメントシステムに関する規格として一定の管理の枠組みが簡潔に規定されています。
実際に採用すべき管理策について余り詳細な記述が無く、採用する管理策についてもう少し詳細な情報がほしいと感じる時には、まず JIS Q 27002:2014 を参照して下さい。
特に新たに採用する管理策については、JIS Q 27002:2014 を精査して下さい。

本ガイドの「参考文献」の一覧にも、ベースラインに採用すべきコントロールの例として参照可能な法律、ガイドライン、報告書、文献などが収集され、活用可能な内容となっています。

また、上記以外にも有用な情報源が入手できる機会があると思います。今後策定されるであろう情報セキュリティに関する基準、制度や、外部コンサルタントから提供されるノウハウなどです。実際にどのようなコントロールを導入するのか、「出来る、出来ない」の判断をする前に広く管理策についての情報を収集し、組織が要求する情報セキュリティの管理水準が、達成可能なベースラインであるかを検討して下さい。

次に、ギャップ分析について説明します。

ギャップ分析実施の目的は、組織の定める基準への準拠状況の把握にあります。
基準で要求される管理のレベルと事業者の管理レベルの現状を比較し「大きな差が認められる個所」、「明らかに管理策の適用を必要としている個所」、「過度に管理策が適用されている個所」等を確認します。

図 付 2-2 は、それぞれの資産を対象に、現状の対策の度合いと組織によって定められる「リスク受容基準」（要求される保証の度合い）との乖離を示しています。図 付 2-2 のリスク受容基準はひとつの平面として表現されていますが、本来、受容基準は一律ではなく、資産の属性や性質、組織における重要度により資産ごとに決定されます。

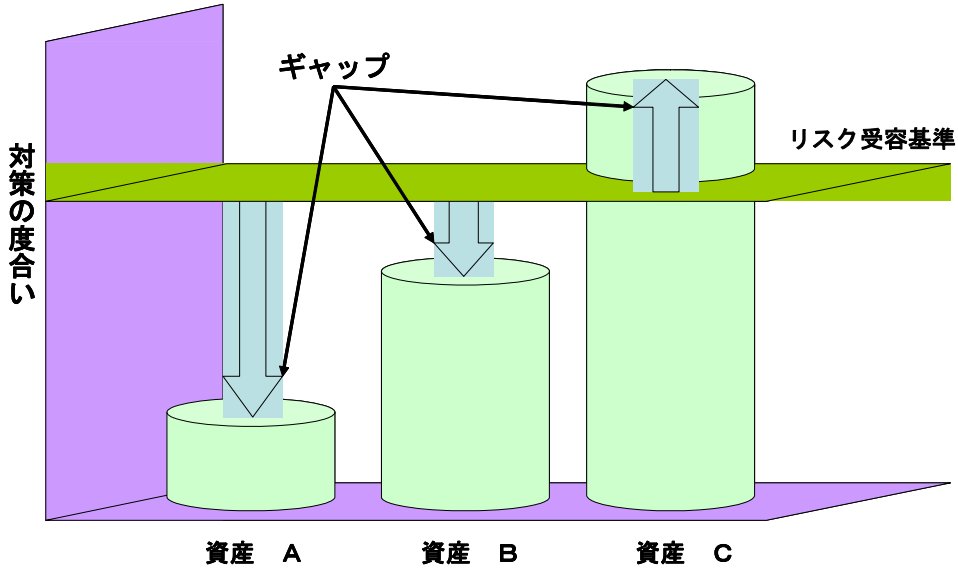


図 付 2-2　リスク受容基準

①詳細リスクアセスメント/上位リスクアセスメント

詳細リスクアセスメントでは、情報及び情報に関連する資産ごとの関連するリスクの特定を個別に実施します。
リスクが顕在化する頻度は、脅威が発生する（顕在化する）可能性、管理上の弱点につけ込まれる可能性（ぜい弱性）の他に、資産が攻撃者から見てどれほど魅力的なものであるのか等にも依存します。

まずリスクアセスメントの対象範囲の定義付けをしなければなりません。プロセスが密接に絡み合っているにも関わらず、安易に範囲を狭め、慎重な定義付けを怠ると、後に不必要な作業が発生したり、抜けが見られたりすることに繋がるからです。

上位レベルのリスクアセスメントは、活動の優先順位及び順番を定めることを可能にします。予算など、様々な理由で、全ての管理策を同時に実施することが不可能であり、リスク対応プロセスによって対応可能なのは、もっとも重大なリスクだけとなることがあります。
加えて、1 年後又は 2 年後の導入を検討している場合は、詳細リスクマネジメントの開始が時期尚早ということがあります。この目的を達成するために、脅威、ぜい弱性、資産及び結果の系統的なリスクアセスメントの代わりに、結果に対する上位レベルのアセスメントをすることで開始することもあります。

上位レベルのアセスメントを開始するもう 1 つの理由は、変更管理（事業継続）に関連する他の計画と同期させることです。例えば、近い将来、システム又はアプリケーションを外注する予定になっている場合、システム又はアプリケーションを完全にセキュアであるというアセスメントをする意味はありませんが、外注契約を定義する目的でのリスクアセスメントを行うだけの価値はあるというようなケースです。

②　組合せアプローチ

一般には、ベースラインアプローチと詳細リスクアセスメントを併用する組合せアプローチを採用することが効率的であると紹介されています。

どのような場合にどのアプローチを採用するかは一概には決定できません。適切なアプローチの採用のための判断材料は、情報及び情報に関連する資産に求められるセキュリティ要求事項（前述の事業上の要求事項、法令又は規制の要求事項、契約上のセキュリティ義務など）に依存します。

組合せアプローチには、それぞれの情報及び情報に関連する資産を取り巻くリスク環境を確認し、適切なリスクアセスメントのアプローチを採用し、それぞれのアプローチの弱点を相互に補完し合うことにより、ISMS 適用範囲全体のリスク分析を効率的に実施する目的があります。
「ベースラインアプローチ」のみでは、高い水準でセキュリティ対策が実装されるべきリスクの高いシステムについて対応策が不充分になる可能性があること、また、「詳細リスクアセスメント」を全てのシステムに適応することは効率的な観点から現実的でないことが大きな理由です。

図 付 2-3 は、前述の組合せアプローチの例です。

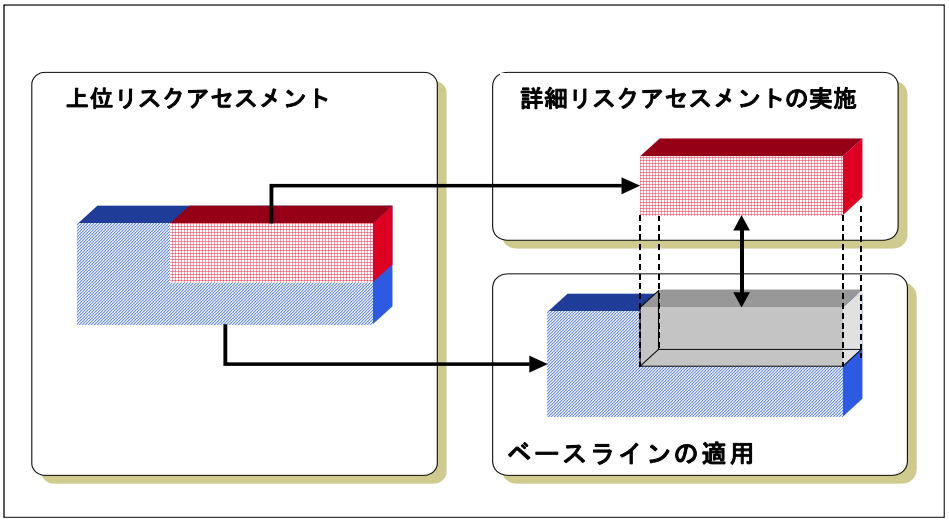


図 付 2-3　組合せアプローチ

③非形式的アプローチ

非形式的アプローチは、ここまで説明をしてきたリスクアセスメントと異なり体系的なアプローチをとりません。この手法は主に、リスク所有者である現場担当者の長年にわたり培われた経験、知見に基づいてリスク源の特定や対策の選択を実施します。
このアプローチは、分析を実施する際に手法について新たに学習すべき事項も少なく迅速に作業に着手できます。また、詳細なアセスメントを実施する場合に比べ投入する人的資源や時間が少なくて済みます。

一般にリスクの特定、分析や評価の作業において、客観性がもっとも重視される事項です。このアプローチは、リスク所有である担当者の特定の考え方に結果が影響される可能性があることは明らかです。しかし、体系的なリスクアセスメントが実施できない場

合などに対象を限定し、次項で説明する点に留意し、他のアプローチと組み合わせて実施することは有用です。

④留意事項

ISMS の構築の初期にある組織では、ここまで説明をしてきたリスク分析の体系的なアプローチを採用しても表 付 2-1 のような問題に直面することがあります。

表 付 2-1　リスクアセスメントの留意事項

現状	問題点
情報及び情報に関連する資産の管理責任が不明確	詳細リスクアセスメントを実施しても、情報・資産の重要度や取扱い範囲が特定できない
リスク判断の基準が未整備	資産の価値を客観的に判断できない リスク管理の水準が属人的に偏る
情報セキュリティインシデントの事例収集が不十分	脅威・ぜい弱性を定量的に扱えない 対策が不適切になる（不足・過度になる）

組織の ISMS が未成熟の場合、要員の不足、周知・教育の不徹底、規程文書や記録の不備などにより円滑に運営できないことも想定されます。ISMS 適用範囲の一部に非形式的アプローチを採用し、担当者の経験に基づいて緊急性の高い対策の実施を優先することも考えられます。そのような場合には、先に述べた問題点に留意し、速やかに他の手法を用いて網羅的なリスク分析を実施することが望まれます。

（3）リスク基準（6.1.2a））

リスク基準とは、risk criteria と複数形で表現されているように、複数の基準で構成されています。ISO/IEC 27005:2011 では、リスク受容基準以外に、情報セキュリティリスクアセスメントを実施するための基準として、リスク評価基準、影響基準などを決定することが記載されています。

リスク評価基準は、次の点を考慮して、組織の情報セキュリティリスクを評価するために設定する基準です。リスク対応の優先順位を規定することに利用します。

- 事業情報プロセスの戦略的価値
- 関係する情報資産の重大性
- 法令及び規制の要求事項並びに契約上の義務
- 可用性、機密性及び完全性の運用上及び事業上の重要性
- 利害関係者の期待及び認知並びに信用及び評判に及ぼす好ましくない結果

影響基準は、次の点を考慮して、情報セキュリティ事象に起因して組織の被る損害又はコストの程度によって規定します。

- 影響を受ける情報資産の分類レベル
- 情報セキュリティ違反（例えば、機密性、完全性及び可用性の喪失）
- 運用障害（内部又は第三者）
- 事業及び金融資産価値の損失
- 計画及び期限の遅れ
- 評判の失墜
- 法令、規制又は契約上の要求事項違反

（４）情報セキュリティリスクアセスメントの再現性を確保する（6.1.2 b））

このリスク基準は、「繰り返し実施した情報セキュリティリスクアセスメントが、一貫性及び妥当性があり、かつ、比較可能な結果を生み出すこと」（6.1.2 b））を実現するものであることが望まれます。加えて、これが実現できていることを、リスクアセスメント実施の記録などで、証拠として検証できる仕組みが求められます。

（５）リスクを特定する（6.1.2 c））

リスク特定では組織が保有する情報及び情報に関連する資産を対象に以下の事項を把握します。

■ どのようなリスク源、事象、並びにそれらの原因及び起こり得る結果が存在するのか
リスク源としては、情報及び情報に関連する資産、それらに対する脅威、その脅威に対する情報及び情報に関連する資産のぜい弱性があります。

リスク特定とは、情報及び情報に関連する資産、脅威、ぜい弱性の組み合わせによって、情報セキュリティイベント・インシデントなどの一連の周辺状況が出現し、それが情報セキュリティ目的に（情報の機密性、完全性及び可用性の喪失に伴う観点において）影響を与える結果を特定するプロセスです。

単にリスクを特定するといっても、リスクそのものは手に取って認識することは出来ません。

本来、リスクは様々なリスク源（リスクの構成要素、例えば、情報及び情報に関連する資産、脅威、ぜい弱性）の因果関係により成り立っています。図 付 2-4 は、リスクとリスク源の関係を例示したもので、リスクレベル（値で表現されることが多い）がそれを取り巻く「資産価値」、「脅威」、「ぜい弱性」により決定されることが表現されています。

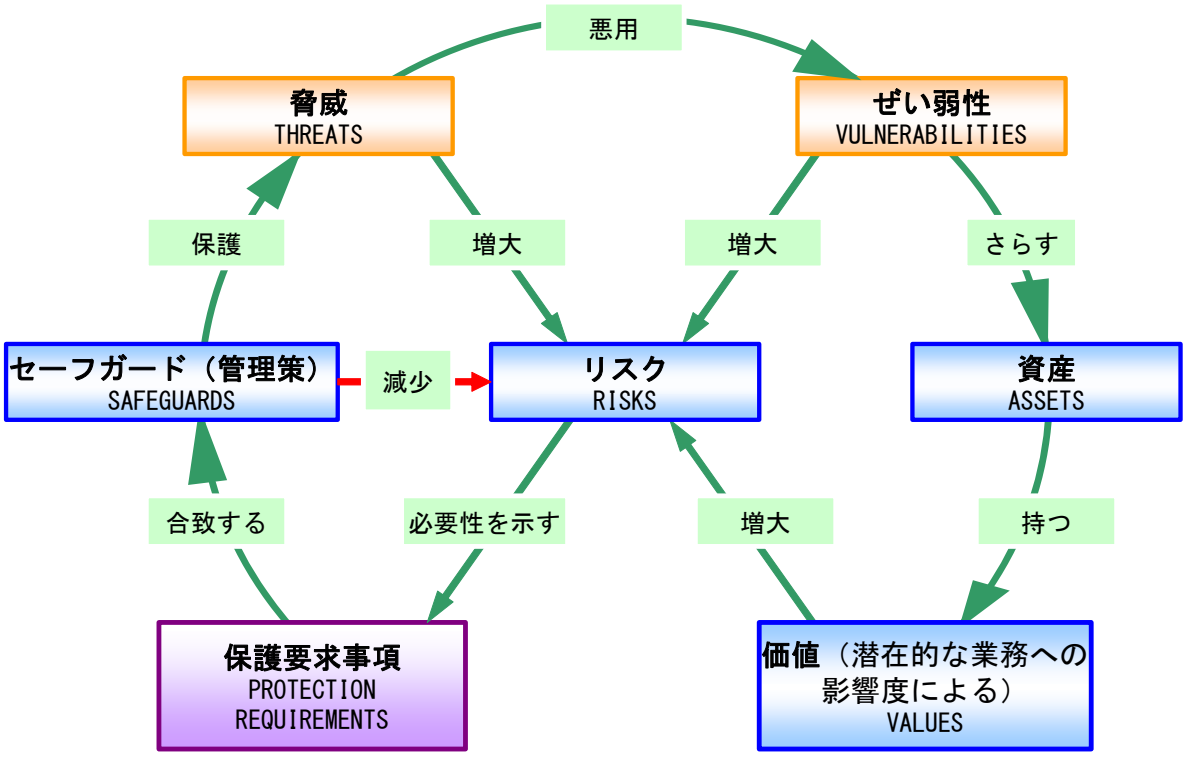


図 付 2-4　リスクとリスク源の因果関係

リスクの特定では、この例では以下の 2 つの作業が実施されます。

- **情報及び情報に関連する資産の洗い出し**
- **脅威・ぜい弱性の明確化**

以下、それぞれの内容について紹介します。

１）情報及び情報に関連する資産（以下、資産として総称）の特定

ここでは、組織の ISMS 適用範囲における資産の保有状況を確認します。ISMS の管理対象の詳細を把握し、適切な管理策を選択するためには、各々の資産の属性や価値を明確にすることが理想です。また JIS Q 27001:2014 では、資産の特定において、それぞれの「資産のリスク所有者（管理責任者）」を特定することが求められています。

実施するリスクアセスメントの適用範囲及び境界、オーナー、場所、機能などの構成要素のリストをインプットとし、リスクマネジメントの対象となる資産のリスト、資産関連の事業プロセス及びその関連性のリストがアウトプットとなります。

資産は、組織にとって価値あるものであり、したがって保護が必要となるものです。資産を特定する場合、情報システムは、ハードウェアやソフトウェア以外からも構成されていることを明記することが望まれます。

資産の特定は、リスクアセスメントのための十分な情報が得られるだけの、適切な詳細さのレベルで実施することが望ましく、その詳細さのレベルは、リスクアセスメントのときに収集する情報量全体に影響します。レベルは、リスクアセスメントを繰り返す中で見直しができます。

資産に関するリスク所有者は、資産ごとに特定し、その資産のリスクに対する責任とアカウンタビリティを示すことが望まれます。資産のリスク所有者は、資産の所有権をもつとは限りませんが、その生産、開発、維持、使用及びセキュリティに関する責任を適宜、保有します。資産の管理責任者は、組織に対して資産の価値を決定するもっとも適切な人、リスク所有者であることが多いようです。

見直す境界は、情報セキュリティリスクマネジメントプロセスによって管理すると定義される、組織の資産に関する境界線です。

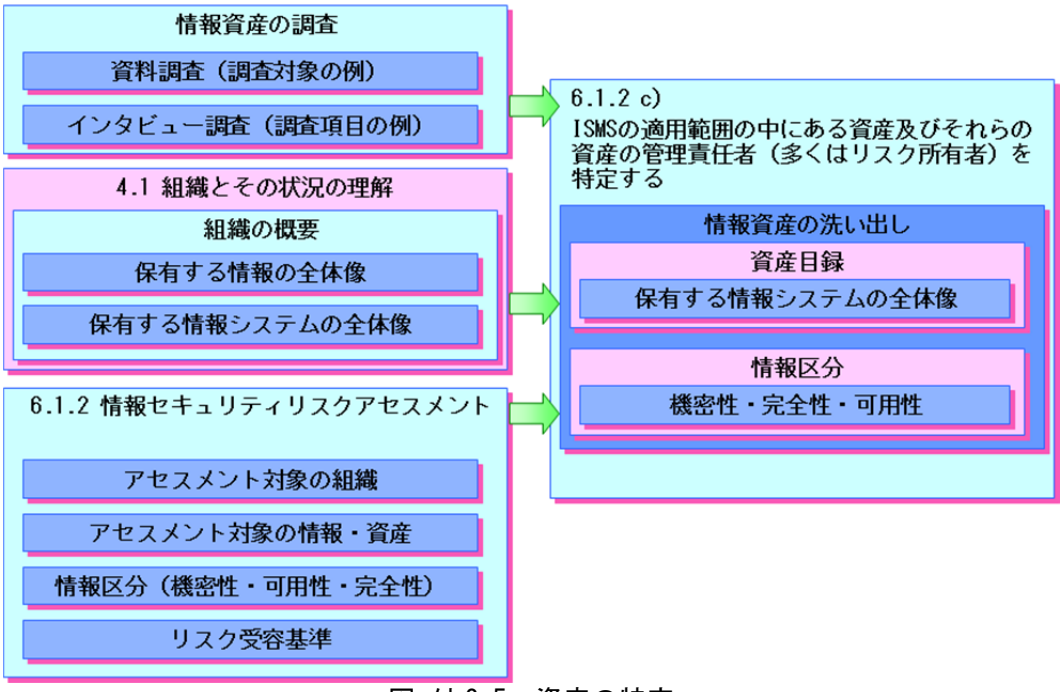


図 付 2-5　資産の特定

①　資産目録の作成

「資産目録」を作成することは、JIS Q 27002:2014 では、「8.1.1 資産目録」という項目で推奨しています。これに対応して、附属書 A では管理策「A.8.1.1 資産目録」という要求事項となっています。

実施の手引
組織は，情報のライフサイクルに関連した資産を特定し，その重要度を文書化することが望ましい。
情報のライフサイクルには，作成，処理，保管，送信，削除，破壊及び保護を含めることが望ましい。文書化は，必要に応じて，専用の目録又は既存の目録で行うことが望ましい。
資産目録は，正確で，最新に保たれ，一貫性があり，他の目録と整合していることが望ましい。
特定された各資産について，管理責任者を割り当て（8.1.2 の管理策を参照。），分類する（8.2 参照）必要がある。

（JIS Q 27002:2014　8.1.1 資産目録　より引用）

特定の活動の結果、資産目録に書き込む情報としては、以下の内容を参考に検討して下さい。JIS Q 27002:2014 の「8.1 資産に対する責任」、「8.2 情報分類」が参考になります。

- **資産の管理責任者（資産の所有者・管理者名）**
- **資産の形態**
- **保管形態**
- **保管場所**
- **保管期間**
- **廃棄方法**
- **用途**
- **利用者の範囲（＋業務プロセス）**
- **他のプロセスとの依存性**

資産を個別に識別しその性質を理解することは、後の作業に関わる脅威やぜい弱性の識別と資産価値の判定の手助けとなります。

② 資産の例示

ISO/IEC 27005 の「附属書 B」には、資産の例示があります。
主要資産：適用範囲の活動の中核のプロセス及び情報
支援資産：表 付 2-2 資産の例示

表 付 2-2 資産の例示

資産の種類	例示
情報	データベース及びデータファイル、契約書及び同意書、システムに関する文書、調査情報、利用者マニュアル、訓練資料、運用手順又はサポート手順、事業継続計画、代替手段の取決め、監査証跡、保存情報
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、ユーティリティソフトウェア
物理的資産	コンピュータ装置、通信装置、取外し可能な媒体、その他の装置
サービス	計算処理サービス、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

この例では、電子的なデータはもちろんそれらを処理するコンピュータ本体、記録媒体やファームウェアなども含まれています。また、紙媒体の情報や会話、物理的な施設・設備といったものも該当します。

③ 資産のグループ化

ISMS 適用範囲に存在する資産の洗い出し作業の負荷が非常に大きいことは容易に想像できます。
リスク分析の作業を進めるにあたり、「資産のグループ化」は作業負荷軽減と今後の分析作業の効率化に有効な考え方です。
例えば、資産価値や属性（保管形態や保管期間、用途等）が一致するものを 1 つのグループとする等です。重要性や属性が同じで、結果的に適用されるセキュリティ対策が同じであれば、同じグループとしてまとめて管理することが効率的です。

そもそも資産の特定をする目的は、ISMS の適用対象全体で適切なセキュリティ対策を決定することです。組織の全ての資産を網羅し、一つひとつの資産の属性を明記した詳細な資産台帳を作成することが必ずしも重要ではありません。

④ 情報区分（影響度の基準）

資産目録の作成後、資産価値を評価します。資産価値は、組織の事業上重要なプロセスに対する影響度ととらえることが可能です。

組織のニーズに基づく資産の識別と評価は、リスクアセスメントにおける重要な要因となります。従って、主要な資産の価値の評価は、組織のビジネスをよく理解した情報の管理責任者（「リスク所有者」という。）によって行われなければなりません。

組織は、資産の価値を判定する際に C.I.A.の 3 要素に関する組織独自の判断基準を開発しなければなりません。表 付 2-3 に、機密性の判断基準の例を示します。

表 付 2-3　機密性の基準の例

資産価値	クラス	説明
1	公開	第三者に開示･提供可能 内容が漏洩した場合でも、ビジネスへの影響はほとんど無い
2	社外秘	組織内では開示･提供可能（第三者には不可） 内容が漏洩した場合、ビジネスへの影響は少ない
3	秘密	特定の関係者または部署のみに開示･提供可能 内容が漏洩した場合、ビジネスへの影響は大きい
4	極秘	所定の関係者のみに開示･提供可能 内容が漏洩した場合、ビジネスへの影響は深刻かつ重大である

個別の資産の価値は、表 付 2-3 の例示のようにあらかじめ規定された情報区分に基づき、主に情報の管理責任者により判定されます。

２）脅威・ぜい弱性の明確化

リスクは、個別の資産、それがさらされるであろう「脅威」、及び資産管理上の問題点などからの「ぜい弱性」の組合せで表されます。

①脅威の特定

「脅威」とは、情報システムや組織に損失や損害をもたらす情報セキュリティインシデントの潜在的な原因です。脅威は後述する「ぜい弱性」により誘引され、顕在化することにより組織及び組織の業務に影響を与えます。脅威の大きさは、その要因や対象となる資産ごとに、その発生の可能性を評価して決定します。

脅威の分類は、例えば表 付 2-4 のように大別して説明しています。

表 付 2-4　脅威の分類例

人為的脅威		環境的脅威
意図的（計画的）脅威	偶発的脅威	環境的脅威
deliberate ⇒ D	accidental ⇒ A	environmental ⇒ E

情報の管理責任者は、前述した資産の価値の決定同様、情報利用者や他事業部門の関係者、外部の専門家から提供される脅威に関する情報を元に、自らが管理する資産がさらされる脅威を識別し、表 付 2-5 の例示のような一覧表を作成します。

表 付 2-5　脅威の例示とその分類例

脅威	分類 (D,A,E)
地震	E
停電	D,　A　,E
静電気	E
オペレータの操作ミス	D,　A
人的リソース（スタッフ）不足	A
ID の偽り	D
悪意のあるソフトウェア	D,　A
……	……

脅威の特定は、上記の表の例などを参考に実施します。
例えば、意図的（計画的）脅威は、攻撃者の動機、攻撃に必要とされるスキル、利用できるリソースを考慮に入れ、資産の特性、魅力、ぜい弱性から、どのような要因が脅威であるかを識別します。

偶発的な脅威は、立地条件、極端な気候条件の可能性及び要員によるミスや誤動作などから影響を及ぼす可能性を識別します。

次に、脅威の発生頻度を評価します。

頻度についても、脅威の識別と同様に自身の業務と関連する他部門と協力して整理します。作成した脅威一覧に基づき、業務上の経験や過去に収集した統計的なデータに基づいて検討します。

評価にどの程度の正確性を要求されるかにもよりますが、「低い」、「中程度」、「高い」の 3 つの区分とする場合が多いようです。表 付 2-6 に、3 つに区分した場合の判断基準を例示します。

表 付 2-6　脅威の判断基準

脅威		
発生可能性	区分	説明
1	低い	発生する可能性は低い。発生頻度は 1 年に 1 回あるかないかである。
2	中程度	発生する可能性は中程度である。発生頻度は半年以内に 1 回あるかないかである。
3	高い	発生する可能性は高い。発生頻度は 1 ヶ月に 1 回以上である。

②既存の管理策の特定

管理策の文書、リスク対応実施計画をインプットとし、既存の管理策及び計画した管理策を特定し、全ての既存の管理策及び予定の管理策のリスト、その実施及び使用状態を特定することが求められます。

既存の管理策の特定は、管理策の重複など、不要な活動又はコストを回避するために実施することが望まれます。さらに、既存の管理策を特定するとき、管理策が正しく働いていることを確実にするための点検を行うことが望まれます。

リスク対応実施計画に従って実施する予定の管理策は、すでに実施されている管理策と同じように考慮することが望まれます。

既存の管理策又は予定した管理策を特定する場合は、次の活動などが有用です。

- ■ 管理策に関する情報を記載した文書（例えば、リスク対応実施計画）を見直す。情報セキュリティマネジメントのプロセスが適切に文書化されていれば、全ての既存の管理策又は予定した管理策、及びその実施状態がわかるはずである。
- ■ 情報セキュリティ担当者（例えば、情報セキュリティ担当員及び情報システムセキュリティ担当員、ビルマネージャ又は運用マネージャ）及びユーザに、検討中の情報プロセス又は情報システムに、実際にはどの管理策が実施されているかを問い合わせる。
- ■ 物理的管理策の現場レビューを実施し、実施されている管理策と、本来実施されているべき管理策のリストを比較し、実施されている管理策が正しく、有効に働いているかどうかを点検する。
- ■ 監査の結果のレビューを行う。

③ぜい弱性の特定

ぜい弱性とは、脅威発生を誘引する資産固有の弱点やセキュリティホールのことです。ぜい弱性は、それだけでは何ら障害とはなりませんが、脅威を顕在化させ、損害や障害を導く可能性があります。逆にいえば、脅威が存在しないぜい弱性は、あまり気を配らなくても良いということになります。

ぜい弱性の分類の例を表 付 2-7 に示します。ぜい弱性をリスト化する際には、表 付 2-7 のように脅威と関連づけて整理する必要があります。

表 付 2-7　ぜい弱性の識別

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
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、情報漏洩
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、情報漏洩
	不適切なパスワード	不正アクセス、改ざん、情報漏洩
	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
……	……	……

ぜい弱性は、資産の性質や属性と関連付けて検討すると特定が容易です。
例えばノート PC を例にとれば、その性質として、「持ち運びやすい」、「衝撃に弱い」、「公共の場で用いられる」などが挙げられます。と同時にその性質は、「盗難や置き忘れ」、「故障」、「情報漏洩」という脅威に対するぜい弱性を示しています。

このことは、その資産の利用環境や保管場所、プロセスの進行状況（ステージ）、形態、時間など、その環境によっては全く異なるぜい弱性が存在することを示しています。同じ資産（例えばノート PC）であっても、その利用形態や性質などから「ノート PC（社内利用）」、「ノート PC（社外利用）」などと分けて識別して管理すべき場合もあることに留意しなければなりません。

ぜい弱性の評価は、その資産のもつ弱点がどの程度であるかを評価することになります。何も対応策を施しておらずその弱点が剥き出しであるような場合は、ぜい弱性は高いと判断できます。組織によりどの程度分類するかは異なりますが、脅威同様、ぜい弱性に関しても、「低い」、「中程度」、「高い」などで区分します。

３）結果（リスク）の特定

資産のリスト、事業プロセスのリスト、また適切ならば資産とその関係物に関連する脅威及びぜい弱性のリストをインプットにし、機密性、完全性及び可用性の喪失が資産に招いた結果を特定し、資産及び事業プロセス関連の結果を含めたインシデントシナリオ（リスク）のリストをアウトプットします。

結果は、有効性の欠如、好ましくない運用条件、事業上の損失、評判の失墜、損害などが挙げられます。

このプロセスは、インシデントシナリオによって引き起こされる損害、又は組織に及ぼす結果（リスク）を特定します。インシデントシナリオは、情報セキュリティインシデントで、ある 1 つのぜい弱性又は一連のぜい弱性につけ入る脅威を記述したものです。インシデントシナリオの影響は、状況の設定活動で定義した影響基準（リスク基準の一部）を考慮して決定します。影響は 1 つ以上の資産に影響することもあれば、資産の一部に影響することもあります。
したがって、資産は、それが損害を受けるか又は危険にさらされた場合、その財務コストのため、及び事業に及ぼす結果のための両面で付与された価値をもつことがあります。結果は、一時的な性質のものもあれば、資産の破壊の場合などのように、恒久的なものもあります。

組織は、インシデントシナリオの運用結果を、次のものによって（ただし、これらだけに限らない。）特定することが望まれます。

- **調査及び修復時間**
- **損失（活動）時間**
- **機会の損失**
- **全衛生**
- **損害の修復のための特殊技能の財務コスト**
- **評判及び信用**

（６）リスクを分析する（6.1.2 ｄ））

> d）次によって情報セキュリティリスクを分析する。
> 1）6.1.2 c）1）で特定されたリスクが実際に生じた場合に起こり得る結果についてアセスメントを行う。
> 2）6.1.2 c）1）で特定されたリスクの現実的な起こりやすさについてアセスメントを行う。
> 3）リスクレベルを決定する。
>
> （JIS Q 27001:2014　6.1.2 情報セキュリティリスクアセスメント　より引用）

リスク分析の方法

リスク分析は、組織にかかわる資産の重要性、既知のぜい弱性の範囲及び以前のインシデントに応じて、様々な程度の詳細さで実施することができます。リスク分析の方法は、状況に応じて、定性的なもの又は定量的なもの、若しくはその組合せのいずれでもよいものです。

実際には、最初に定性的な分析を採用してリスクレベルの一般的な兆候を得て、重大なリスクを明らかにすることがよく使われます。その後、重大なリスクについて、より具体的な分析又は定量的分析を実施しなければならないことがあります。定性的な分析は定量的な分析に比べて一般に複雑でなく、経費がかからないからです。

分析形式は、組織の状況の設定の一部から導き出される、リスク評価基準（リスク基準の一部）に整合したものであることが望まれます。

リスク分析は、分析手順を決定し、資産目録を作成し、資産の重要性の分類及び脅威・ぜい弱性の評価基準を明確にすることにより実施が可能になります。

資産の重要性は、前述の C.I.A.毎に分けて情報の管理責任者が評価します。

脅威・ぜい弱性の評価は、作業を専門家に依頼して実施した方が客観性や効率性の確保の面から良い場合もあります。また、情報セキュリティ監査制度を利用し、外部の専門家がぜい弱性評価の支援することも考えられます。

① 起こり得る結果のアセスメント

脅威、ぜい弱性、影響を受ける資産、資産及び事業プロセスに対する結果の特定を含む、特定された関連インシデントシナリオ（リスク）のリストをインプットとします。

現実の、又は考えられる情報セキュリティインシデントから生じるかもしれない、組織に及ぶ事業上の影響は、資産の機密性、完全性又は可用性の喪失のような、情報セキュリティ違反の結果を考慮して評価します。

資産及び影響基準（リスク基準の一部）によって表されるインシデントシナリオの評価結果のリストをアウトプットします。

② インシデントの起こりやすさのアセスメント

脅威、影響を受ける資産、つけ込まれるぜい弱性並びに、資産及び事業プロセスに対する結果の特定を含む、特定された関連インシデントシナリオのリストをインプットとします。さらに、全ての既存の管理策及び予定した管理策、そのパフォーマンス、実施及び使用状態のリストをインプットに含めます。

インシデントシナリオの起こりやすさを評価し、その起こりやすさ（定量的又は定性的）をアウトプットとします。

③ リスクレベルの決定

資産及び事業プロセスに関連した結果並びにその起こりやすさ（定量的又は定性的）を含めたインシデントシナリオのリストを、インプットとし、リスクレベルを、関連する全てのインシデントシナリオについて決定します。価値をあらわすレベルを付与されたリスクのリストが、アウトプットされます。

リスク分析は、リスクの起こりやすさ及び結果に対する価値を付与します。これらの値は定量的なこともあれば、定性的なこともあります。リスク分析は、評価した結果及び

起こりやすさに基づきますが、あるいは、さらに、費用便益、ステークホルダの関心及び、リスク評価に適っていればその他の変数を考慮することができます。決定されたリスクは、インシデントシナリオの起こりやすさとその結果との組合せです。

リスクレベル（値）の決定（例）

リスクレベル（値）は、前の作業で明確になった「資産の価値」、「脅威の大きさ」、「ぜい弱性の度合い」を用いて、例えば、簡易的に以下のような式で算出、決定します。

リスクレベル（値） ＝ 「資産の価値」 × 「脅威」 × 「ぜい弱性」

（例）

特性	資産の価値
C:機密性	4（内容が漏洩した場合、ビジネスへの影響は深刻かつ重大である）
I:完全性	2
A:可用性	1
脅威	3（発生する可能性は高い。発生頻度は１ヶ月に１回以上である。）
ぜい弱性	3（全ての作業担当者に特権が付与されていたので）

この場合のリスク値は、以下のようになります。
機密性に関わるリスク値：4×3×3＝36
完全性に関わるリスク値：2×3×3＝18
可用性に関わるリスク値：1×3×3＝9

図 付 2-5　リスクレベル（値）の計算例

（７）リスクを評価する（6.1.2 e））

e） 次によって情報セキュリティリスクを評価する。
1） リスク分析の結果と 6.1.2 a）で確立したリスク基準とを比較する。
2） リスク対応のために，分析したリスクの優先順位付けを行う。

（JIS Q 27001:2014　6.1.2 情報セキュリティリスクアセスメント　より引用）

付与された価値レベルでのリスクのリスト及びリスク評価基準をインプットとし、リスクレベルを、リスク評価基準及びリスク受容基準に対して比較します（6.1.2 e）1））。

リスクに至るインシデントシナリオに関連して、リスク評価基準に従って優先順位の定められたリスクのリストをアウトプットします（6.1.2 e）2））。

リスク評価に関係する意思決定の性質及び、この決定を下すために採用するリスク評価基準（リスク基準の一部）は、組織の状況の確定に基づき決められます。この決定及び組織の状況は、特定された個々のリスクについて詳細が判明したこの時点で、再度検討することが必要です。リスクを評価するとき、組織は、算出・決定したリスクと、組織の状況の確定に基づくリスク評価基準とを比較することが求められます。

意思決定に用いるリスク評価基準は、確定された組織の外部及び内部の情報セキュリティリスクマネジメントの状況と整合するものであることが必要で、組織の目的及び利害関係者（ステークホルダ）の見解などを考慮したものであることが必要です。

リスク評価活動で下す決定は、主にリスクの受容基準に基づいています。ただし、リスクの特定及び分析における結果、起こりやすさ及び信頼の程度も考慮することが望まれ

ます。低度のリスク又は中度のリスクでも、それが集まれば、全体ではるかに高いリスクとなることがあるので、相応に対処する必要があります。

次の事項を考慮に含めます。
- 情報セキュリティ特性：
  1 つの基準（例えば、機密性の喪失）が組織に関係しないとすれば、この基準に影響する全てのリスクが関係しない可能性があります。
- 特定の資産又は一連の資産によって支援される事業プロセス又は活動の重要性：
  プロセスの重要性が低いと判断されれば、それに関連するリスクには、より重要なプロセス又は活動に影響するリスクと比べて、配慮の度合いを下げることが望まれます。

リスク評価は、将来のアクションに関する決定を下すために、リスク分析によって得られたリスクの理解を用います。決定事項には、次のものを含めることです。
- 活動に着手すべきか否か。
- 決定されたリスクレベルを考慮したリスク対応の優先順位

リスク評価の段階では、契約、法令及び規制の要求事項が、決定されたリスクに加えて考慮すべき要素となります。

リスク評価（例）

リスクレベル（値）を算出し表 付 2-8 の例のようなマトリクス「リスク値早見表」を作成すると、以降の作業を効率的に進める助けになります。

表 付 2-8　リスクレベル（値）早見表例

	脅威								
	1			2			3		
	ぜい弱性								
資産の価値	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

例えば、これにリスク受容基準を適用すると、受容可能なリスクレベル（値）は表 付 2-9 の例のような一覧表になることが考えられます。

表 付 2-9　リスク受容一覧の例（1）

	脅威								
	1			2			3		
	ぜい弱性								
資産の価値	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

リスクを受容できる範囲
リスクに対して何らかの対策を講じる範囲

表 付 2-9 のリスク受容一覧の例（1）は、6.1.2 a）で特定したリスク受容基準をリスクレベルで表現した「9」とした場合です。リスク評価作業の際に作成したリスクレベル（値）のマトリクス（「リスク値早見表」）で、リスクレベル（値）が「9」未満のものについては、現状の管理を受容し、受容したリスクについては「残留リスク」として管理します。残留リスクとは、以下のように定義されます。

2.64 残留リスク（residual risk）
リスク対応（2.79）後に残っているリスク（2.68）。
注記 1 残留リスクには，特定されていないリスクが含まれ得る。
注記 2 残留リスクは，“保有リスク”ともいう。

（JIS Q 27000:2014 2 用語及び定義 より引用）

表 付 2-10 リスク受容一覧の例（2）

	脅威								
	1			2			3		
	ぜい弱性								
資産の価値	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

リスクを受容できる範囲
リスクに対して何らかの対策を講じる範囲

また、表 付 2-10 のリスク受容一覧の例（2）では、資産の価値が最大の「4」であれば無条件に対策をとるべきであるというリスク受容基準を適用して、リスクレベル（値）の需要水準は「4」未満となります。

このリスク受容一覧は、あくまでリスク評価実施時のリスク環境を表わすもので、資産の価値や脅威、ぜい弱性等の環境に変化が生じた場合は、適宜リスクレベル（値）の見直し及びリスク基準（受容基準及び評価基準）の見直しを実施しなければなりません。

参考文献

参考文献は、ISMS を構築する上で有用だと思われる書籍や文献、法令などを、紹介するものです。

本版から、参考文献の維持管理を向上させるために、下記サイトに別ファイルとして開示致しておりますので、以下の URL をご参照ください。

http://www.isms.jipdec.or.jp/doc/JIP-ISMS111-B.1.pdf

IMS 運営委員会

（順不同・敬称略）

氏名	会社・機関名
土居　範久	慶應義塾大学【委員長】
大木　榮二郎	工学院大学【副委員長】
島田　洋之	大同火災海上保険株式会社【副委員長】
稲垣　隆一	稲垣隆一法律事務所
榎木　千昭	慶應義塾大学大学院
大畑　毅	日本電気株式会社
熊谷　堅	KPMG ビジネスアドバイザリー株式会社
駒瀬　彰彦	株式会社アズジェント（ISMS 技術専門部会 主査）
小山　條二	特定非営利活動法人 itSMF Japan
伊藤　毅志	独立行政法人　情報処理推進機構
塩田　貞夫	洛 IT サービス・マネジメント株式会社（ITSMS 技術専門部会 主査）
杉浦　昌	日本電気株式会社
髙﨑　誠	日本マネジメントシステム認証機関協議会 （日本検査キューエイ株式会社）
田原　幸朗	一般社団法人情報サービス産業協会
出口　幹雄	富士通株式会社
中尾　康二	KDDI株式会社
藤本　正代	富士ゼロックス株式会社
八木　隆	株式会社日立製作所

（2014 年 3 月 31 日現在）

ISMS 技術専門部会

（順不同・敬称略）

氏名	会社・機関名
駒瀬　彰彦	株式会社アズジェント【主査】
丸山　満彦	デロイト　トーマツ　リスクサービス株式会社【副主査】
相羽　律子	株式会社日立製作所 情報・通信システム社
佐藤　慶浩	日本ヒューレット・パッカード株式会社
竹下　和孝	株式会社筑波総合研究所
中村　春雄	日本マネジメントシステム認証機関協議会 （一般財団法人　日本品質保証機構）
平野　芳行	一般社団法人 情報処理学会
牧野　敬一朗	KPMG ビジネスアドバイザリー株式会社
松尾　正浩	株式会社三菱総合研究所

（2014 年 3 月 31 日現在）

一般財団法人日本情報経済社会推進協会
〒106-0032 東京都港区六本木1丁目9番9号 六本木ファーストビル内
TEL 03-5860-7570　FAX 03-5573-0564
URL http://www.jipdec.or.jp/