ＩＳＭＳユーザーズガイド

-JIS Q 27001:2023(ISO/IEC 27001:2022）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

2025 年 3 月 31 日

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。

このたび、本制度に適用される認証基準が従来の JIS Q 27001:2014 から JIS Q 27001:2023 へと改正されました。これに伴い、2014 年に発行した ISMS ユーザーズガイド（以下、本ガイドという。）についても、新認証基準における変更点を反映するよう改訂いたしました。本ガイドでは、JIS Q 27001:2023 の要求事項について必ずしも網羅されている訳ではありませんが、一定の範囲でその意味するところを説明しています。なお、JIS Q 27001:2023 の附属書 A（規定）「情報セキュリティ管理策」の詳細は、管理策の指針である JIS Q 27002:2024 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 27001:2023 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。特に、序文において、JIS Q 27001:2023 の国際規格 ISO/IEC 27001:2022 の改訂の概要や規格理解のポイントなどについて説明します。本ガイドが JIS Q 27001:2023 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。

JIS Q 27001:2023 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、ご協力頂いた関係各位に対し厚く御礼申し上げます。

2025 年 3 月

ISMS 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.....12
２．引用規格.....13
３．用語及び定義.....16
４．組織の状況.....25
５．リーダーシップ.....32
６．計画策定.....38
７．支援.....51
８．運用.....57
９．パフォーマンス評価.....60
１０．改善.....70
附属書Ａ（規定）　情報セキュリティ管理策 73

０．序文

０．１ 国際規格（ISO/IEC 27001）について

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（国際標準化機構）と IEC（国際電気標準会議）が設置する情報技術の合同専門委員会 ISO/IEC JTC1 の分科委員会 SC 27（情報セキュリティ、サイバーセキュリティ及びプライバシー保護）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。
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（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）。

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。そのため、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す。

ISO/IEC 27001 は、ISO MSS 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です。ISO/IEC 27001 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 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。

2022 年 2 月の ISO/IEC 27002:2022 発行に合わせて、ISO/IEC 27001 も附属書 A を更新するために改訂が行われ、2022 年 10 月に ISO/IEC 27001:2022 が発行されました。この改訂では、附属書 A の更新とともに、ISO MSS 共通要素の改訂も反映されました。

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、2022 年 10 月に国際規格 ISO/IEC 27001:2022（第 3 版）を発行しました。ISO/IEC 27001:2022 の検討は、ISO/IEC 27002 改訂版に合わせて附属書 A を更新するために開始されました。

- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements（JIS Q 27001:2023 情報セキュリティ，サイバーセキュリティ及びプライバシー保護―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 27001:2022/Amd.1:2024 Information security, cybersecurity and privacy protection - Information security management systems - Requirements AMENDMENT 1: Climate action changes （情報セキュリティ，サイバーセキュリティ 及びプライバシー保護ー情報セキュリティマネジメントシステムー要求事項　追補 1：気候変動対応）は、2024 年 2 月 23 日に、気候変動への考慮を求める共通の記述を追加する追補項目として発行されました。詳細は本ガイドの 4 章を参照して下さい。

- ISO/IEC 27002:2022　Information security, cybersecurity and privacy protection - Information security controls（JIS Q 27002:2024 情報セキュリティ，サイバーセキュリティ及びプライバシー保護ー情報セキュリティ管理策）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 27000:2018　Information technology - Security techniques - Information security management systems-Overview and vocabulary（JIS Q 27000:2019　情報技術ーセキュリティ技術ー情報セキュリティマネジメントシステムー用語）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 27000:2019 は、ISO/IEC 27000:2018 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。

※ ISO/IEC 27001、ISO/IEC 27002 のタイトルについて、ISO/IEC JTC1 の分科委員会 SC 27 の名称が「セキュリティ技術」から「情報セキュリティ、サイバーセキュリティ及びプライバシー保護」に変更されたことに伴い、変更されました。

なお、JIS Q 27001 は、ISO/IEC 27001 の制定発行に伴って、日本産業標準調査会（JISC）により日本産業規格（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 の情報セキュリティ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 27001:2022 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 27001:2022 のリスクアセスメント及びリスク対応のプロセスは、ISO 31000:2018（JIS Q 31000:2019）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 27001:2022 は、基本的には ISO/IEC 27001:2013 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 27002:2022 に規定す

る情報セキュリティ管理策を提供していますが、ISO/IEC 27002:2022 以外からの管理策群の導入も許容しています。

ISO/IEC 27001:2022 の理解のポイントを説明します。
（注記）ISO MSS 共通要素については、「ISO/IEC 専門業務用指針 第 1 部及び統合版 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ための調和させる方法」の「Appendix 2（規定）MSSのための調和させる構造、及びその利用に関する手引」（以下、附属書 SL）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、今回のポイントの 1 つは、旧規格の制定以降に適用された附属書 SL（ISO MSS 共通要素）の改訂点を反映したことです。ISO/IEC 27001:2022 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、例えば、文書化した情報を「保持する」又は「維持する」という表現を,「利用可能な状態にする」に置換しています。その上で、情報セキュリティに不可欠な ISMS 固有の要求事項の内容においては,「文書化した情報を保持する」という表現も適用しています。

● ISO 31000:2018（リスクマネジメント－指針）との整合
ISO 31000:2018 との関連性については、3 つの観点で従来から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 31000:2018 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 31000:2018 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 31000:2018 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、本ガイドに記述しています。
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 27001:2022「6.1 リスク及び機会に対処する活動」の「6.1.1 一般」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を決定しなければならない。」としています。
ISO 31000:2018（JIS Q 31000:2019）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、「注記 1 影響とは、期待されていることから、乖離することをいう。影響には、好ましいもの、好ましくないもの、又はその両方の場合があり得る。影響は、機会又は脅威を示したり、創り出したり、もたらしたりすることがあり得る。」としています。一方、この定義を用いると、6.1 の「リスク及び機会」という用語には、「機会」という用語がダブることになり、リスク及び機会といった場合、リスク定義とは別の「機会」を検討する必要があるのでは、といった意見もありますが、この「機会」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「5.4.1 組織及び組織の状況の理解」を考慮し、本ガイドの 4 章に記載する「4.1 組織及びその状況の理解」との整合を確保し、組織が抱える外部及び内部の状況を把握することが、リスクマネジメントの重要なポイントであると考えられます。

● リスクアセスメント

ISO/IEC 27001:2022「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。」とし、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 31000:2018（JIS Q 31000:2019）に合わせたと考えられます。

また、6.1.2 c）では、CIA（機密性、完全性及び可用性）の喪失に伴う視点でリスクを特定することが要求されており、従来の規格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。

状況に応じた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情報セキュリティリスクアセスメントのプロセスの適用が可能となっていますが、組織は、これら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りません。

● 情報セキュリティリスク対応

ISO/IEC 27001:2022「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。」としています。リスク対応について、ISO 31000:2018（JIS Q 31000:2019）では以下のように規定しています。

> 6.5.1 一般
> リスク対応の意義は，リスクに対処するための選択肢を選定し，実施することである。リスク対応には，次の事項の反復的プロセスが含まれる。
> - リスク対応の選択肢の策定及び選定
> - リスク対応の計画及び実施
> - その対応の有効性の評価
> - 残留リスクが許容可能かどうかの判断
> - 許容できない場合は，更なる対応の実施
>
> （JIS Q 31000:2019　6.5 リスク対応　より引用）

ISO/IEC 27001:2022「6.1.3 情報セキュリティリスク対応」においても、これらのプロセスを反映し、要求事項として記載しています。詳細は、本ガイドの 6 章を参照して下さい。

● 文書管理

ISO/IEC 27001:2022「7.5.3 文書化した情報の管理」では、「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」とし、「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，不適切な使用又は完全性の喪失からの保護）」などを管理することを求めています。

なお ISMS 固有の内容においては，「文書化した情報を保持する」という表現も引き続き用いられています。

基本的には従来の ISO/IEC 27001 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 を参照して下さい。

０．２．３　ISO MSS 共通要素の概要

ISO/IEC 27001:2022 では、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」（2012 年当初の名称。現在の名称は本ガイドの 0.2.2 を参照）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 27001:2022 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）MSS のための調和させる構造、及びその利用に関する手引」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 27001:2022 はタイプ A の MSS 規格です。

ISO/IEC 専門業務用指針第 1 部及び統合版 ISO 補足指針
https://webdesk.jsa.or.jp/common/W10K0500/index/dev/std_shiryo1/
（ISO/IEC Directives Part 1 and Consolidated ISO Supplement
https://www.iso.org/directives-and-policies.html ）

この MSS 共通要素の適用により、ISO/IEC 27001:2022 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 27001:2022 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　XXX 方針
　5.3　役割、責任及び権限
6　計画策定
　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
　6.3　変更の計画策定
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　運用の計画策定及び管理
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　継続的改善
　10.2　不適合及び是正処置

（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。）

０．３　ISO/IEC 27001:2022（JIS Q 27001:2023）の概要

ここでは、ISO/IEC 27001:2022（JIS Q 27001:2023）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 27001:2022（JIS Q 27001:2023）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 27001:2022（JIS Q 27001:2023）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 27001:2023 は、ISO/IEC 27001:2022 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 0-1 参照）。

図 0-1　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 27001:2022（JIS Q 27001:2023）及び附属書 SL には「PDCA モデル」という表現は明記されておりませんが、上記の附属書 SL は「6 章：Plan、8 章：Do、9 章：Check、10 章：Act」といった構成となっています。この附属書 SL を適用した ISO/IEC 27001:2022（JIS Q 27001:2023）も同じ構成を採用しています。この附属書 SL を適用した ISO/IEC 27001:2022（JIS Q 27001:2023）でも、PDCA のアプローチが考慮されています（附属書 SL については、本ガイドの 0.2.3 参照）。

０．３．３　ISO/IEC 27001:2022（JIS Q 27001:2023）の構成

ISO/IEC 27001:2022（JIS Q 27001:2023）は、ISO MSS 共通要素の適用、リスクマネジメント（ISO 31000:2018（JIS Q 31000:2019））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 27001:2022（JIS Q 27001:2023）の構成

ISO/IEC 27001:2022 （JIS Q 27001:2023）	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 31000:2018 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 計画策定	
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。
6.3 変更の計画策定	組織が ISMS の変更の必要があると決定したときは、計画的な方法で変更を行う。
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 運用の計画策定及び管理	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 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。
10.2 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。

この ISO/IEC 27001:2022（JIS Q 27001:2023）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。

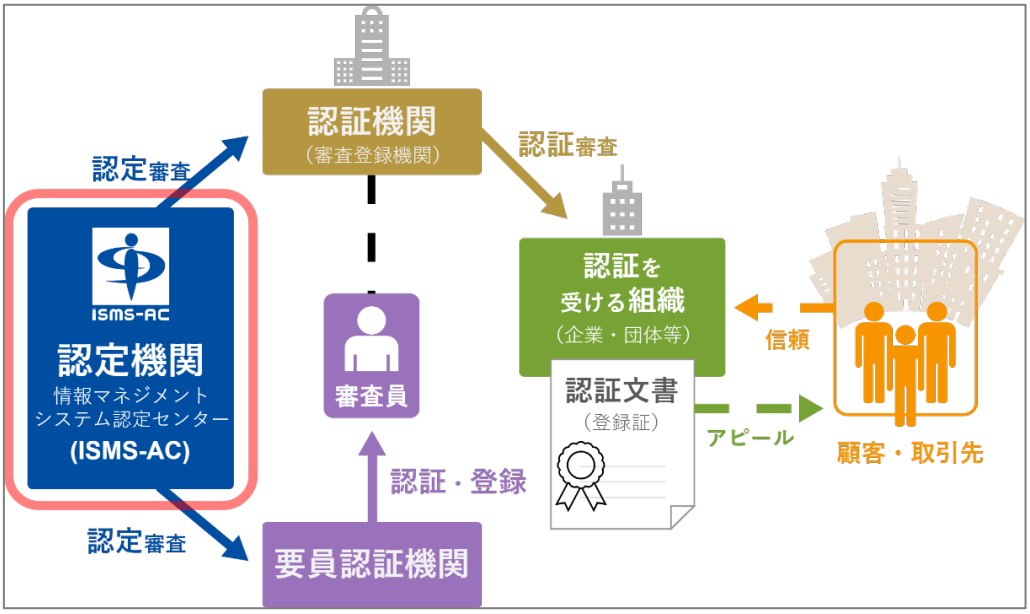
０．３．４　他のマネジメントシステムとの両立性

ISO/IEC 27001:2022（JIS Q 27001:2023）の他のマネジメントシステムとの両立性について、ISO/IEC 27001:2022 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っています（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 27001:2023（ISO/IEC 27001:2022）を認証基準とした組織の情報セキュリティの運用管理を、第三者（認証機関）が審査・認証する仕組みです。ISMS 適合性評価制度は、国際的な枠組みに基づく制度であり、「認証機関」、「認定機関」、「要員認証機関」から構成されています。
＜参考＞
JIPDEC では、国際規格 ISO/IEC 27001 の原案となった英国規格 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 が発行されたこと、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。



認証機関：第三者機関として組織の ISMS が ISO/IEC 27001 に適合しているか審査し登録する。
要員認証機関：審査員の力量を評価し、登録する。
認定機関※：上記の各機関がその業務を行う能力を備えているかを審査し、認定する。

※制度開始当初は JIPDEC が認定機関としての役割を果たしていましたが、認定機関としての独立性をより明確にし、引き続き客観性及び公平性のある認定活動を推進していくために、2018 年 4 月に認定業務を行う「一般社団法人情報マネジメントシステム認定センター（略称：ISMS-AC）」として法人化しました。現在、この ISMS-AC が、本制度の認定機関としての役割を担っており、JIPDEC は本制度の普及啓発活動を行っています。

認定機関が ISMS 認証機関を認定する意義

認定機関である情報マネジメントシステム認定センター（ISMS-AC）は、認証機関が適切に審査を実施できる体制・能力をもっているかを、国際規格（ISO/IEC 27006-1）に照らして審査し、適合していると認められる機関を認定して、「認定シンボル」の使用を許可しています。そのため、認定を受けた ISMS 認証機関は、適切な ISMS 認証審査を実施することのできる、信頼のおける認証機関であることを意味します。要員認証機関についても同様です。

認定シンボル（右）と認証機関マーク（左）が並んだ表示例

認定シンボルと認証機関のマークが２つ並んでいることは、その認証機関が国際規格に従った適切な審査を実施していることを、認定機関であるISMS-ACが保証していることを示します。

０．４．２　認定機関の国際的な協力体制

ISMS-AC は、国際認定フォーラム（International Accreditation Forum, Inc.）という、認証機関協議会、各国の産業団体等からなる国際組織に加盟しています。この IAF の国際相互承認協定（MLA）に署名した認定機関によって認定された認証機関による認証は、IAF によってその信頼性を保証されます。ISMS-AC も ISMS MLA に署名しているため、本制度の下で組織が認証を受けた場合、その認証は国際的にも同等レベルであるということが言えます。

１．適用範囲

前章の「0 序文」では、規格改訂の経緯等を説明するために、規格番号に発行年を付して記載しました。本章からは、最新版である JIS Q 27001:2023 の箇条に沿って説明することから、JIS Q 27001:2023 は発行年を省略して JIS Q 27001 と記載します。

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

JIS Q 27001 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、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おり、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 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の確立、実施、維持及び継続的な改善につながります。

利害関係者とは、JIS Q 27000:2019 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 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。

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「情報セキュリティ管理策」は、適用除外が可能となっています。附属書 A「情報セキュリティ管理策」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。

JIS Q 27001 の附属書 A「情報セキュリティ管理策」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。附属書 A に記載する情報セキュリティ管理策は、考えられる管理策のリストであり、これらの適用除外は、マネジメントシステムの一貫性に大きな影響を与え、重大な事故や無駄な投資につながることもありますので、除外した理由を明確にする必要があります。

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。詳細は、本ガイドの 6.1.3(4)を参照して下さい。

２．引用規格

引用規格では、JIS Q 27001 の規定の一部を構成するものであること、発行年のない規格はその最新版を適用することを規定しています。
JIS Q 27001 では、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。

２．１ JIS Q 27000 (ISO/IEC 27000)

ISO/IEC 27000:2018 の発行に伴って、日本産業標準調査会（JISC）により日本産業規格（JIS）として制定された国内規格です。
ISO/IEC 27000:2018 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 27000:2019 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 27000:2019 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

（注記）ISO/IEC 27002:2022 については、改訂時に規格の中で使用する用語を更新し、「3.1 用語及び定義」に記載しています。

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

２．２　JIS Q 27002（ISO/IEC 27002）

ISO/IEC 27002:2022 の制定発行に伴って、日本産業標準調査会（JISC）により日本産業規格（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て ISO/IEC 27002:2013 として発行され、その後 2022 年 9 月に 3 度目の改訂が行われ、ISO/IEC 27002:2022 として発行されました。

ISO 規格の改訂に伴い、JIS Q 27002 も改訂が行われ、現在 JIS Q 27002:2024 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。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。その後、ISO/IEC 27001 及び ISO/IEC 27002 の改訂に併せて改訂されています。

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産業規格が JIS Q 0073:2010 です。
ここでは、本ガイドの「2.1 JIS Q 27000（ISO/IEC 27000）」に示す通り、JIS Q 27001（ISO/IEC 27001）の用語及び定義の引用規格である JIS Q 27000:2019（ISO/IEC 27000:2018）で引用されている JIS Q 0073:2010（ISO Guide 73:2009）に基づき説明します。

＜参考＞
ISO Guide 73:2009 の後継として、「ISO 31073:2022 Risk management – Vocabulary」が発行されています（対応する JIS 規格は、2025 年 3 月現在発行されていません）。
その中の用語の多くが[SOURCE:ISO Guide 73:2009, x.x.x]としています（つまり、ISO Guide 73:2009 の用語の多くが ISO 31073:2022 にそのまま引き継がれています）。
https://www.iso.org/obp/ui/en/#iso:std:iso:31073:ed-1:v1:en

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 31000:2019（ISO 31000:2018）

JIS Q 31000:2019 は、ISO 31000:2018 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産業規格です。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、リスクの増大に伴い、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。JIS Q 31000「リスクマネジメント-指針（Risk management－Guidelines）は、この必要性にこたえるために、開発されました。
JIS Q 27001 では、リスクマネジメントについて、JIS Q 31000:2019（ISO/IEC 31000:2018）及び JIS Q 0073:2010（ISO Guide 73:2009）を引用しています。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 31000:2019（ISO/IEC 31000:2018）との整合が図られています。

1 適用範囲
この規格は，組織が直面するリスクのマネジメントを行うことに関して，適用可能な指針を示す。これらの指針は，あらゆる組織及びその状況に合わせて適用することができる。
この規格は，あらゆる種類のリスクのマネジメントを行うための共通の取組み方を提供しており，特定の産業又は部門に限るものではない。
この規格は，組織が存在している限り使用可能であり，あらゆるレベルにおける意思決定を含め，全ての活動に適用できる。

（JIS Q 31000:2019　1 適用範囲　より引用）

３．用語及び定義

JIS Q 27001 で用いる用語及びその定義について説明します。この規格の用語及び定義は、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。

- **情報セキュリティに関する用語の定義**
  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の定義**
  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の定義**
  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 部及び統合版 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ための調和させる方法」に規定する「Appendix 2（規定）MSS のための調和させる構造、及びその利用に関する手引」の「3. 用語及び定義」を引用しています。このうち、マネジメントシステムについては、本ガイドの「3.3 マネジメントシステムに関する用語」で説明します。

なお、本ガイドの「3.1.2 情報セキュリティ管理策」及び「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」については、ISO/IEC 27002:2022 において関連する用語定義が更新されていることから、ISO/IEC 27002:2022 をもとに説明します。

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。

> 3.28 情報セキュリティ（information security）
> 情報の機密性（3.10），完全性（3.36）及び可用性（3.7）を維持すること。
> 注記 さらに，真正性（3.6），責任追跡性，否認防止（3.48），信頼性（3.55）などの特性を維持することを含めることもある。
> （JIS Q 27000:2019 3 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。

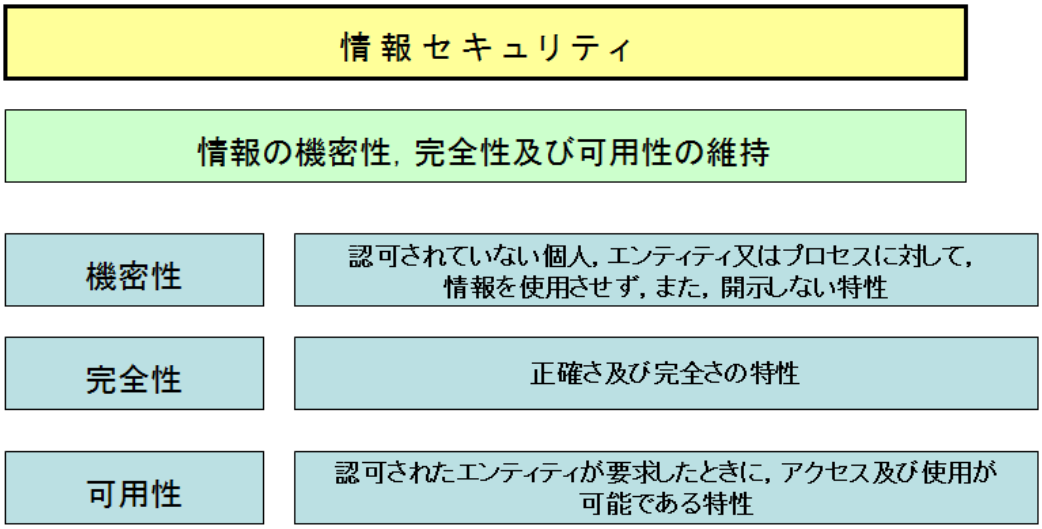


図 3-1　情報セキュリティの主な要素

「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。

> 3.10　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（3.54）に対して，情報を使用させず，また，開示しない特性。
>
> （JIS Q 27000:2019　3 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。

> 3.36　完全性（integrity）
> 正確さ及び完全さの特性。
>
> （JIS Q 27000:2019　3 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。

---

[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

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。

> 3.7　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 27000:2019　3 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。

> 3.6　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。
>
> 3.48　否認防止（non-repudiation）
> 主張された事象（3.21）又は処置の発生，及びそれらを引き起こしたエンティティを証明する能力。
>
> 3.55　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 27000:2019　3 用語及び定義　より引用）

３．１．２　情報セキュリティ管理策

「1 適用範囲」において、「（JIS Q 27001 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『情報セキュリティ管理策』の要求事項は、適用除外が可能となっています。附属書 A『情報セキュリティ管理策』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。」と説明しました。

ここでは、JIS Q 27001 に規定する情報セキュリティ管理策の手引である JIS Q 27002:2024 をもとに、情報セキュリティ管理策の構成やタイプなどを紹介します。
なお、附属書 A「情報セキュリティ管理策」に規定されている管理策については、本ガイドの附属書 A を参照して下さい。

情報セキュリティ管理策について

管理策については、JIS Q 27000 に定義があり、以下のようになっています。

> 3.14 管理策（control）
> リスク（3.61）を修正（modifying）する対策。
> 注記 1 管理策には，リスク（3.61）を修正するためのあらゆるプロセス（3.54），方針（3.53），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 0073:2010 の 3.8.1.1 参照）
> （JIS Q 27000:2019　3 用語及び定義　より引用）

JIS Q 27002:2024 では、「リスクを修正する対策」として、管理策のタイプ、特性、運用の領域などの属性を用いて管理策を分類し説明しています。

管理策は、「～望ましい」という表現を用いて表現され、各管理策は、以下の 4 つの見出しで構成されています。

■ **各管理策で適用される見出しの構成**
- 管理策
- 目的
- 手引
- その他の情報

また、管理策を記載した各箇条の構成は以下のとおりです。

■ **規格の構成**
- 箇条 5：組織的管理策
- 箇条 6：人的管理策
- 箇条 7：物理的管理策
- 箇条 8：技術的管理策

その他の構成として、「箇条 0：序文、箇条 1：適用範囲、箇条 2：引用規格、箇条 3：用語及び定義並びに略語、箇条 4 この規格の構成」となっています。

テーマ及び属性

JIS Q 27002:2024 の「4.2 テーマ及び属性」では、上記の箇条 5～箇条 8 に示す管理策の分類をテーマと呼び、以下のように分類しています。

管理策

管理策は、次のように分類されます。
- 箇条 6：個人に関係する場合は、人的管理策
- 箇条 7：物理的対象に関係する場合は、物理的管理策
- 箇条 8：技術に関係する場合は、技術的管理策
- 箇条 5：それ以外の場合は、組織的管理策と分類されます。

5 つの属性と属性値

各管理策には、次に示す属性及び該当する属性値を付けて説明しています。

（１）管理策タイプ

管理策タイプは、情報セキュリティインシデントの発生との関係において、リスクを管理策がいつどのように修正するかという観点から管理策を見る属性です。

属性値は、
- **予防**：情報セキュリティインシデントの発生を予防することを意図した管理策
- **検知**：情報セキュリティインシデントの発生時に機能する管理策
- **是正**：情報セキュリティインシデントの発生後に機能する管理策

から構成されています。

なお、情報セキュリティインシデント等に関連する用語については、本ガイドの「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」を参照して下さい。

（２）情報セキュリティ特性

情報セキュリティ特性は、管理策が情報のどの特性を維持するのに寄与するかという観点から管理策を見る属性です。

属性値は、
- 機密性
- 完全性

・可用性
から構成されています。

（３）サイバーセキュリティ概念

サイバーセキュリティ概念は、管理策を、ISO/IEC TS 27110 に記載されているサイバーセキュリティフレームワークで定義するサイバーセキュリティ概念に関連付ける観点から見る属性です。
属性値は,
・識別（Identify）
・防御（Protect）
・検知（Detect）
・対応（Respond）
・復旧（Recover）
から構成されています。

（４）運用機能

運用機能は、情報セキュリティ機能についての実践者の観点で管理策を見る属性です。
属性値は、
・ガバナンス
・資産管理
・情報保護
・人的資源のセキュリティ
・物理的セキュリティ
・システム及びネットワークのセキュリティ
・アプリケーションセキュリティ
・セキュリティを保った構成
・識別情報及びアクセスの管理
・脅威及びぜい弱性の管理
・継続
・供給者関係のセキュリティ
・法令及び順守
・情報セキュリティ事象管理
・情報セキュリティ保証
から構成されています。

（５）セキュリティドメイン

セキュリティドメインは、4 つの情報セキュリティドメインの観点から管理策を見る属性です。
・ガバナンス及びエコシステム：（属性値も同じ名称）
（内部及び外部の利害関係者を含め）、
■ 情報システムセキュリティのガバナンス
■ リスクマネジメント
■ エコシステムサイバーセキュリティマネジメント
を含む。
・保護：（属性値も同じ名称）
■ IT セキュリティアーキテクチャ
■ IT セキュリティ管理
■ 識別情報
■ アクセスの管理
■ IT セキュリティ保守
■ 物理的及び環境的セキュリティ

を含む。
・防御：（属性値も同じ名称）
■ 検知
■ コンピュータセキュリティインシデント管理
を含む。
・レジリエンス：（属性値も同じ名称）
■ 運用の継続
■ 危機管理
を含む。

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 では、情報セキュリティインシデントに関し、関連する用語がいくつか定義されています。例えば、「3.1.16 情報セキュリティインシデント管理」では、以下のように定義されており、「一貫した有効な取組」として１つの箇条にまとめられていますが、この中には、「3.1.15 情報セキュリティインシデント」が、また 3.1.15 には、「3.1.14 情報セキュリティ事象」が含まれています。

3.1.14 情報セキュリティ事象（information security event）
情報セキュリティ侵害（3.1.13）又は管理策（3.1.8）の不具合の可能性を示す事象
（出典：ISO/IEC 27035-1:2016 の 3.3 を変更）

3.1.15 情報セキュリティインシデント（information security incident）
組織の資産（3.1.2）に害を及ぼす又はその運用を危うくする可能性のある一つ以上の関連する特定された情報セキュリティ事象（3.1.14）
（出典：ISO/IEC 27035-1:2016 の 3.4）

3.1.16 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（3.1.15）の取扱いに対する一貫した有効な取組の実行
（出典：ISO/IEC 27035-1:2016 の 3.5）
（JIS Q 27002:2024　3.1 用語及び定義　より引用）

また、「情報セキュリティインシデント管理」には、関連する管理策として、「5.5 関係当局との連絡」が紹介されています。

5.5 関係当局との連絡
管理策
組織は、関係当局との連絡体制を確立し，維持することが望ましい。

目的
<<省略>>

手引
組織は、いつ、誰が関係当局（例えば、法執行機関、規制当局、監督官庁）に連絡するか、及び特定した情報セキュリティインシデントをいかにして時機を失せずに報告するかを規定することが望ましい。

その他の情報
攻撃を受けている組織は，関係当局に，攻撃元に対して対応をとることを求める場合もある。
このような連絡体制を維持することは，情報セキュリティインシデント管理（5.24～5.28 参照），又は緊急時対応計画及び事業継続プロセス（5.29 及び 5.30 参照）を支援するために必要な場合がある。
規制当局との連絡は，組織に影響を与える関連法令又は規制の改正動向を事前に把握し、対応することにも役立つ。
（JIS Q 27002:2024　5.5 関係当局との連絡　より引用）

まとめると、「情報セキュリティインシデント管理」については、JIS Q 27002:2024 の 5.24～5.28 を参照、緊急時対応計画及び事業継続プロセスについては、同じく 5.29 及び 5.30 を参照すると理解を深めることができます。

■情報セキュリティインシデント管理
5.24 情報セキュリティインシデント管理の計画策定及び準備
5.25 情報セキュリティ事象の評価及び決定
5.26 情報セキュリティインシデントへの対応
5.27 情報セキュリティインシデントからの学習
5.28 証拠の収集
■緊急時対応計画及び事業継続プロセス
5.29 事業の中断・阻害時の情報セキュリティ
5.30 事業継続のための ICT の備え

これらのことは、JIS Q 27001 の附属書 A に記載された個別の管理策一覧のみを参照するだけでは、関連する他の管理策との関係性が理解できず、結果として必要な管理策を見落とす原因となります。
情報セキュリティ管理策を決定する場合、JIS Q 27002:2024 も参照するように留意下さい。

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。

> 3.69　リスクマネジメント（risk management）
> リスク（3.61）について，組織（3.50）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 27000:2019　3 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 31000:2019 のリスクマネジメントの活動及びプロセスを導入し、JIS Q 27001 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。

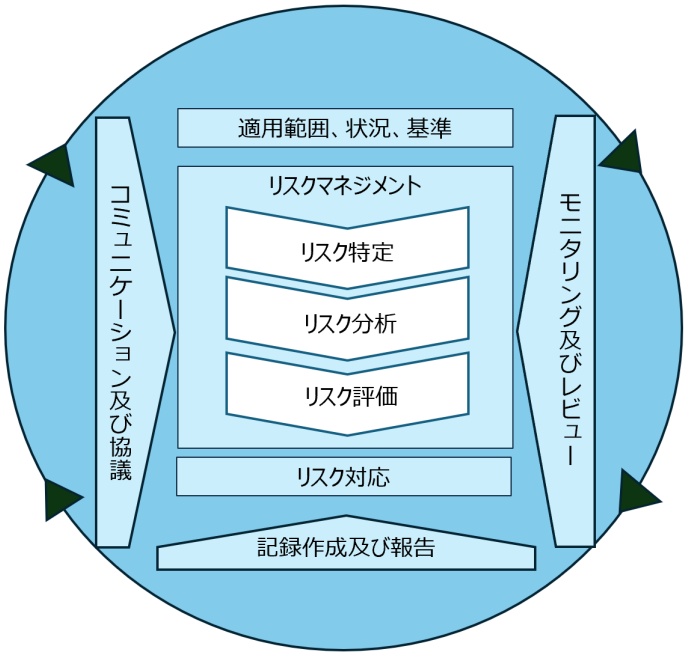


図 3-2　JIS Q 31000:2019 のリスクマネジメント（プロセス（箇条 6））
（JIS Q 31000:2019 の 6.1(図 4)より引用）

３．３　マネジメントシステムに関する用語

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。

3.41　マネジメントシステム（management system）
方針（3.53），目的（3.49）及びその目的を達成するためのプロセス（3.54）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（3.50）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，計画及び運用が含まれる。
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 27000:2019　3 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**

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システムであり、リスクマネジメントをその中心におくものです。

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。

その他の用語については、本ガイドの 4 章以降を参照して下さい。

４．組織の状況

JIS Q 27001 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。

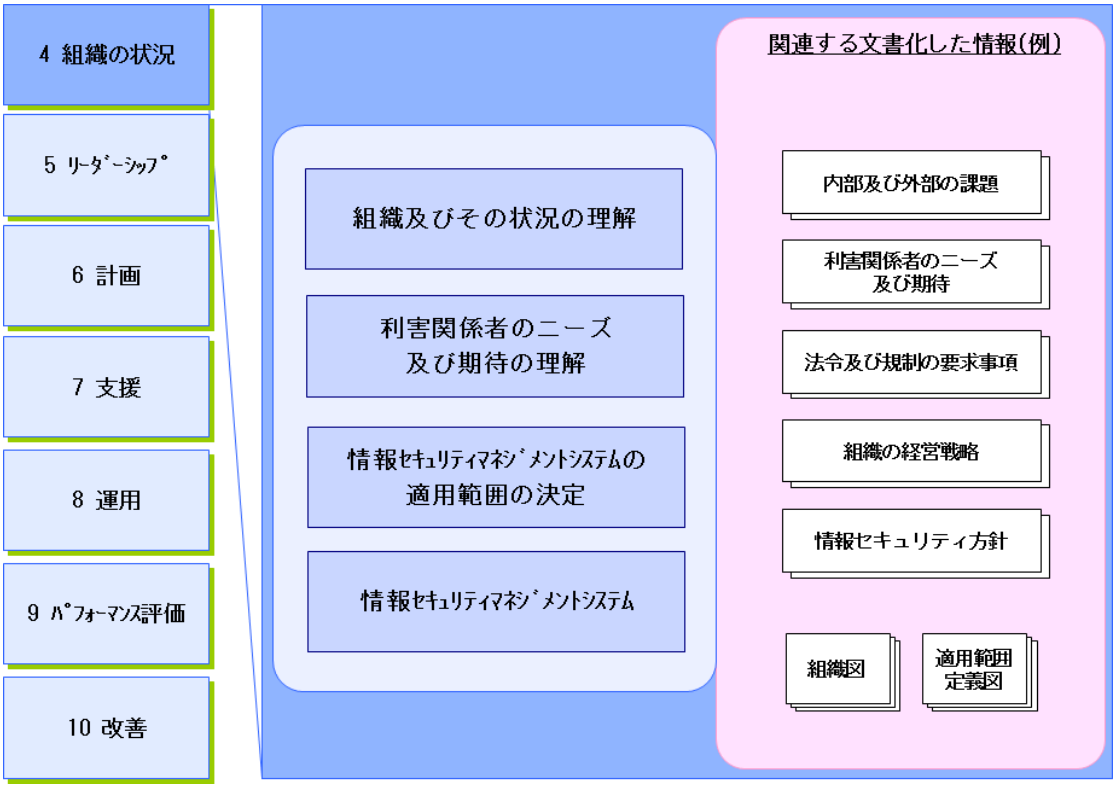


図 4-1　組織の状況の理解（事例）　注）文書名は全て例示

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」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。
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。

> 3.50　組織（organization）
> 自らの目的（3.49）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 27000:2019　3 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を決定しなければならない」とされていますが、これは組織の外部状況及び内部状況を確定することを指します。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。

3.22　外部状況（external context）
組織が自らの目的（3.49）を達成しようとする場合の外部環境。
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（3.50）の目的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ー（3.37）との関係並びに外部ステークホルダーの認知及び価値観
（JIS Q 0073:2010 の 3.3.1.1 参照）

（JIS Q 27000:2019　3 用語及び定義　より引用）

3.38　内部状況（internal context）
組織（3.50）が自らの目的を達成しようとする場合の内部環境。
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（3.53），目的（3.49）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（3.54），システム及び技術］
－ 情報システム（3.35），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ー（3.37）との関係並びに内部ステークホルダーの認知及び価値観
－ 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 0073:2010 の 3.3.1.2 参照）

（JIS Q 27000:2019　3 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や気候変動への関連を決定する状況は、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。
JIS Q 31000:2019の5.4.1によれば、「リスクのマネジメントを行うための枠組みを設計するに当たって、組織は、外部及び内部の状況を検証し、理解することが望ましい。」と記載されています。
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こと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。

（１）外部状況

外部状況を理解する上においては、JIS Q 31000:2019 の「5.4.1 組織及び組織の状況の理解」では、「国際、国内、地方又は近隣地域を問わず、社会、文化、政治、法律、規制、金融、技術、経済及び環境に関する要因」を考慮することが望ましいとしています。

外部状況には、例えば、次のようなものが考えられます。

- **地政学的リスクが発生する状況**
  - 国際関係の悪化や紛争の勃発により、特定国の IT インフラが標的となるリスク
  - 経済制裁や輸出規制による技術供給の制限
  - 国家主体によるサイバー攻撃の増加

- **経済的リスクが発生する状況**
  - 世界的な経済不況や金融危機に伴う投資・運用リスク
  - 為替変動による ICT 資産の調達・運用コストの増大
  - 企業倒産による情報資産管理の脆弱化

- **法的・規制リスクが発生する状況**
  - 新たなデータ保護規制（例：GDPR、CCPA）の施行に伴うコンプライアンス対応負荷の増加
  - 政府による IT システム監視やデータアクセス権の変更
  - 知的財産権の侵害やライセンス契約違反リスク

- **技術的リスクが発生する状況**
  - 新技術（AI、量子コンピューティング）の台頭による既存暗号技術の脆弱化
  - クラウド環境のセキュリティ脆弱性の悪用
  - ソフトウェアサプライチェーン攻撃の増加

- **社会・文化的リスクが発生する状況**
  - フェイクニュースや情報操作による世論誘導
  - デジタルデバイド※の拡大による情報格差
    ※デジタルデバイドとは、情報通信技術を活用できる人とできない人に生まれる格差を指します。
  - 社会運動やハクティビズムの活発化による企業攻撃リスク

また、上述の各状況において、例えば以下のようなサイバー攻撃によって、システム停止や情報漏洩が発生する可能性があります。

- **サイバー攻撃によりインシデントが発生する状況**
  - **国家・組織的攻撃**：APT（Advanced Persistent Threat）攻撃や DDoS 攻撃
  - **クラウド環境攻撃**：クラウド設定ミスを悪用した情報漏洩
  - **サプライチェーン攻撃**：ソフトウェアのアップデート経由のマルウェア感染
  - **プライバシー情報の奪取が含まれる類の攻撃**
    - **フィッシング攻撃**：標的型メールによる個人情報の窃取
    - **ランサムウェア攻撃**：個人情報を暗号化し、復号のための身代金を要求
    - **ソーシャルエンジニアリング**：人間の心理的弱点を突いた情報窃取

（２）内部状況

次に、内部状況について説明します。

組織の内部状況の検証には、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含まれます。検証は、組織の目的、方針、戦略、文化、価値観などを対象とします。

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れます。
JIS Q 31000:2019 の「5.4.1 組織及び組織の状況の理解」によると、これらには、以下のようなものが含まれます。

- **組織の文化**
- **組織が採用する規格、指針及びモデル**
- **資源及び知識として理解される能力（例えば、資本、時間、人員、知的財産、プロセス、システム、技術）**
- **データ、情報システム及び情報の流れ**

これらの活動の難しさは、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 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、関連する要求事項をまず特定し、その特定された要求事項の中から ISMS の中で取り組むものを決定することを求めています。

利害関係者は、以下のように定義されています。

> 3.37　利害関係者（interested party）（推奨用語）
> ステークホルダー（stakeholder）（許容用語）
> 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（3.50）。
> （JIS Q 27000:2019　3 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、関連する要求事項を決定します。関連する要求事項には、気候変動に関する要求事項も含まれてくる可能性があります。例えば、温室効果ガスの削減や消費電力の削減による天然資源への問題に取り組むために、サービス提供事業者に対してシステム基盤としてクラウド利用を要求したり、サービス提供事業者がクラウド利用を要求されたりする場合などがあります。
その後関連する要求事項の中から組織の ISMS を通して取り組むものを決定します。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。

JIS Q 27001 における利害関係者という用語は、JIS Q 31000:2019 において使用されるステークホルダーと同じ意味と考えられます。このことは、JIS Q 27001 の 4.1 の注記で、JIS Q 31000:2019（ISO 31000:2018）の 5.4.1 が参照されており、そこで、ステークホルダーの表現が使用されていることから分かります。

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、3.22 外部の状況、3.38 内部の状況において、外部ステークホルダー、内部ステークホルダー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。

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 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、及び適用範囲とする組織が実施する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、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 27000:2019 では次のように定義しています。

> 3.51　外部委託する（outsource）
> ある組織の機能又はプロセス（3.54）の一部を外部の組織（3.50）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（3.41）の適用範囲の外にある。
> （JIS Q 27000:2019　3　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 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 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。

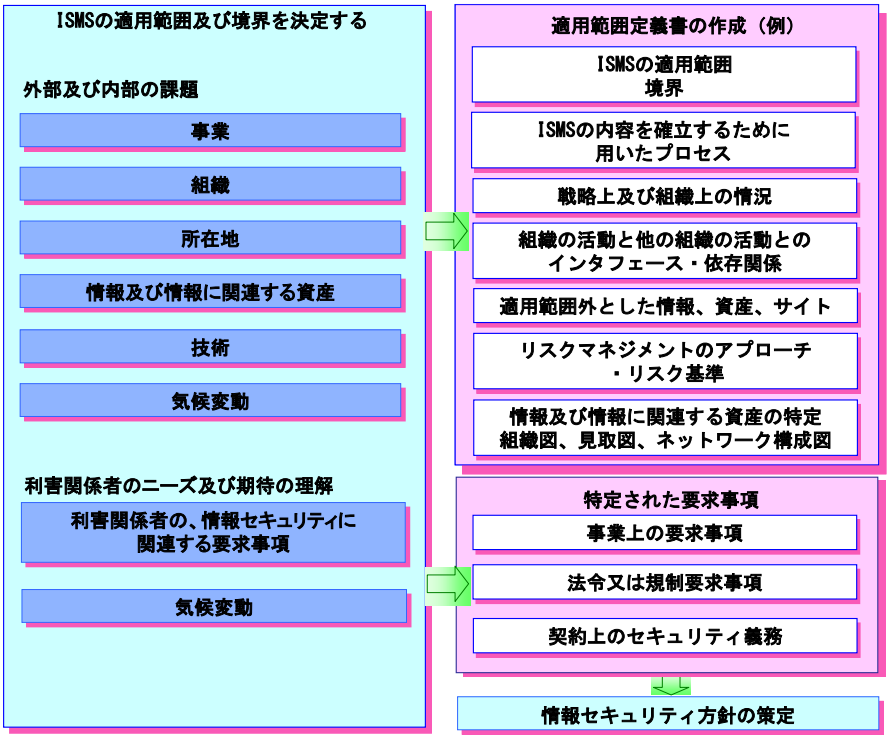


図 4-2　ISMS の適用範囲の定義（例）

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

ここでは、JIS Q 27001 の要求事項に従って、必要なプロセス及びそれらの相互作用を含む、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考慮されています。
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。

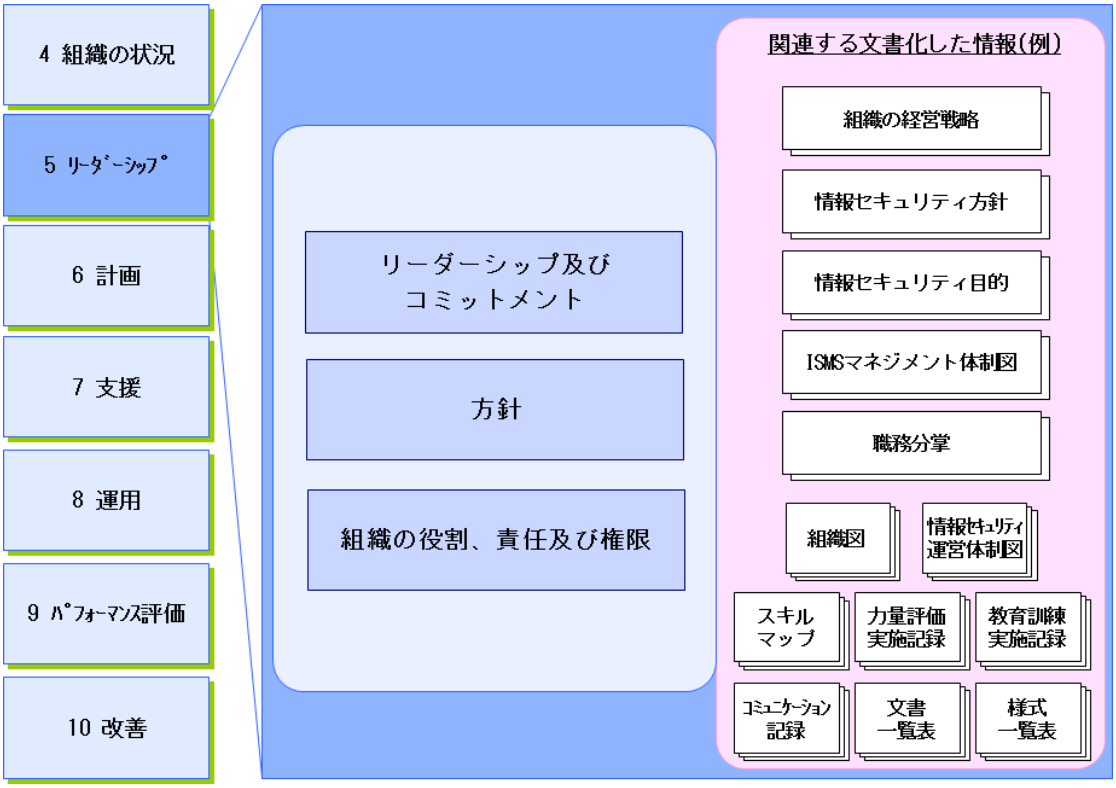


図 5-1　トップマネジメントの果たすべき役割（事例）　注）文書名は全て例示

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 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 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 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。
注記 この規格で“事業”という場合，それは，組織の存在の目的の中核となる活動という広義の意味で解釈され得る。
（JIS Q 27001:2023 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、上記 a)に記載の「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。このことは、ISMS を推進していく上で効果的な取組みであり、形骸化させない ISMS を構築する上でも重要な要因となります。

加えて、導入した ISMS の形骸化を防ぐためにも、b)に記載の「組織のプロセスへの ISMS 要求事項の統合を確実にする」が重要です。

c）に記載の「必要な資源を利用可能にする」については、ISMS を運用していく上で不可欠な考え方であり、「7.1 資源」、「7.3 認識」に関連する要求事項です。

d）～h）の要求事項に関しては、トップマネジメントに課せられる JIS Q 27000 の定義を参照して下さい。

3.75 トップマネジメント（top management）
最高位で組織（3.50）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，資源を提供する力をもっている。
注記 2 マネジメントシステム（3.41）の適用範囲が組織の一部だけの場合，トップマネジメントとは，組織内のその一部を指揮し，管理する人をいう。
注記 3 トップマネジメントは，ときに業務執行幹部（executive management）と呼ばれることもあり，最高経営責任者，最高財務責任者，最高情報責任者及び類似の役職が含まれることがある。
（JIS Q 27000:2019 3 用語及び定義 より引用）

ISMS を効果的に運用するためには、「5 リーダーシップ」の要求事項を認識し、ISMS を推進させ、関係者への意識向上を図るための支援など、トップマネジメントの積極的なリーダーシップとコミットメント及びコミュニケーション力が不可欠なものとなります。

５．２ 方針

JIS Q 27001 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。

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。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、各従業員が情報セキュリティ方針を理解せず、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。

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適用される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。また、必要に応じて利害関係者が入手可能であるようにする必要もあります。

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 27002:2024 の「5.1 情報セキュリティのための方針群」では、「情報セキュリティ方針及びトピック固有の方針は，これを定義し，管理層が承認し，発行し，関連する要員及び関連する利害関係者に伝達し，認識させ，あらかじめ定めた間隔で，及び重大な変化が発生した場合にレビューすることが望ましい。」としています。

（情報セキュリティ方針、策定事例）

組織は，方針群の最も高いレベルに，一つの“情報セキュリティ方針”を定めることが望ましい。この情報セキュリティ方針は，トップマネジメントが承認し，情報セキュリティの管理に対する組織の取組を示すものである。

情報セキュリティ方針は，次のものから導き出される要求事項を考慮に入れることが望ましい。

a) 事業上の戦略及び要求事項
b) 規制，法令及び契約
c) 現在の及び予想される情報セキュリティのリスク及び脅威

情報セキュリティ方針には，次の事項に関する記載を含めることが望ましい。

a) 情報セキュリティの定義
b) 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
c) 情報セキュリティに関する全ての活動の指針となる原則
d) 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
e) 情報セキュリティマネジメントシステムの継続的な改善へのコミットメント
f) 情報セキュリティマネジメントに関する責任の，定められた役割への割当て
g) 逸脱及び例外を取り扱う手順

情報セキュリティ方針のいかなる変更もトップマネジメントが承認することが望ましい。

（JIS Q 27002:2024 5.1 情報セキュリティのための方針群 手引　より引用）

これらの事項は、「5.1 情報セキュリティための方針群」の「手引」から引用したものであり、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

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 では 5.3a)及び b)で「ISMS が, この規格の要求事項に適合することを確実にする」こと、「ISMS のパフォーマンスをトップマネジメントに報告する」こと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、周知が必要な利害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 では主に、情報セキュリティ、サイバーセキュリティ及びプライバシー保護を取り扱うマネジメントシステムであるために、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（例えば、システム部門）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、及び人材の登用などについて考慮する必要があります。

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。

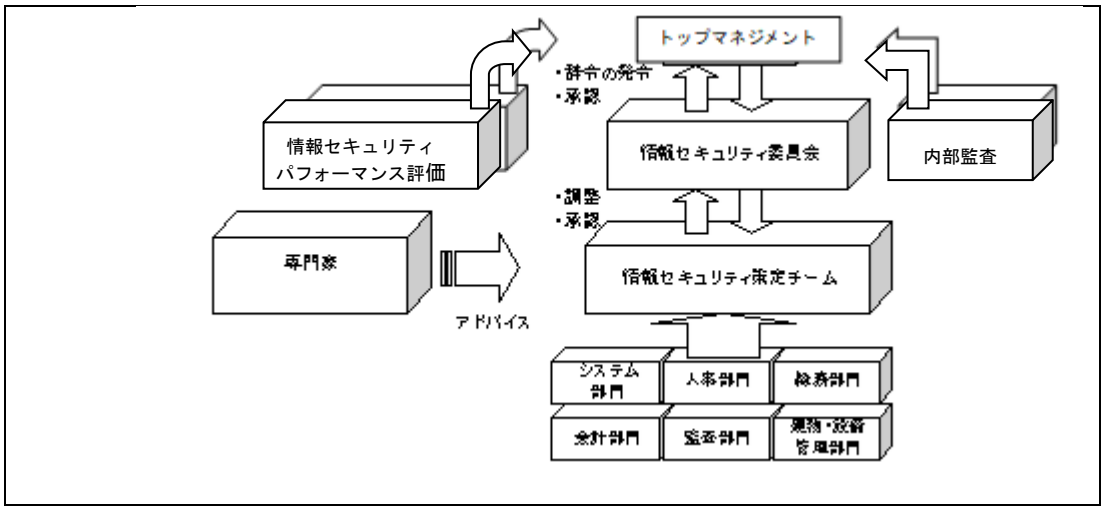


図 5-2　ISMS 構築・運用のための組織体制（例）

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。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。

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チームの役割

ISMS の構築・運用の実務を担当する策定チームは、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情報セキュリティ委員会と②情報セキュリティ策定チーム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

ISMS を成功させるには、その組織の全ての要員がこれを支持する必要があります。
また、課題ごとの専門家による助言が必要な場合もあります。

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。組織内の専門家、コンサルタントなどは、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役立つと思われます。

④ 内部監査

ISMS における内部監査の役割は、ISMS が適切に運用され、継続的に改善されることを保証するための重要なプロセスです。主な役割は以下のとおりです。

- **ISMS の適合性の評価**
- **効果的な運用の確認**
- **問題点や改善点の特定**
- **継続的な改善の促進**
- **客観的な評価の提供**

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。

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はありません。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定めなければなりません。

情報セキュリティに対する組織の取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。

６．計画策定

「6　計画策定」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及び情報セキュリティ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。

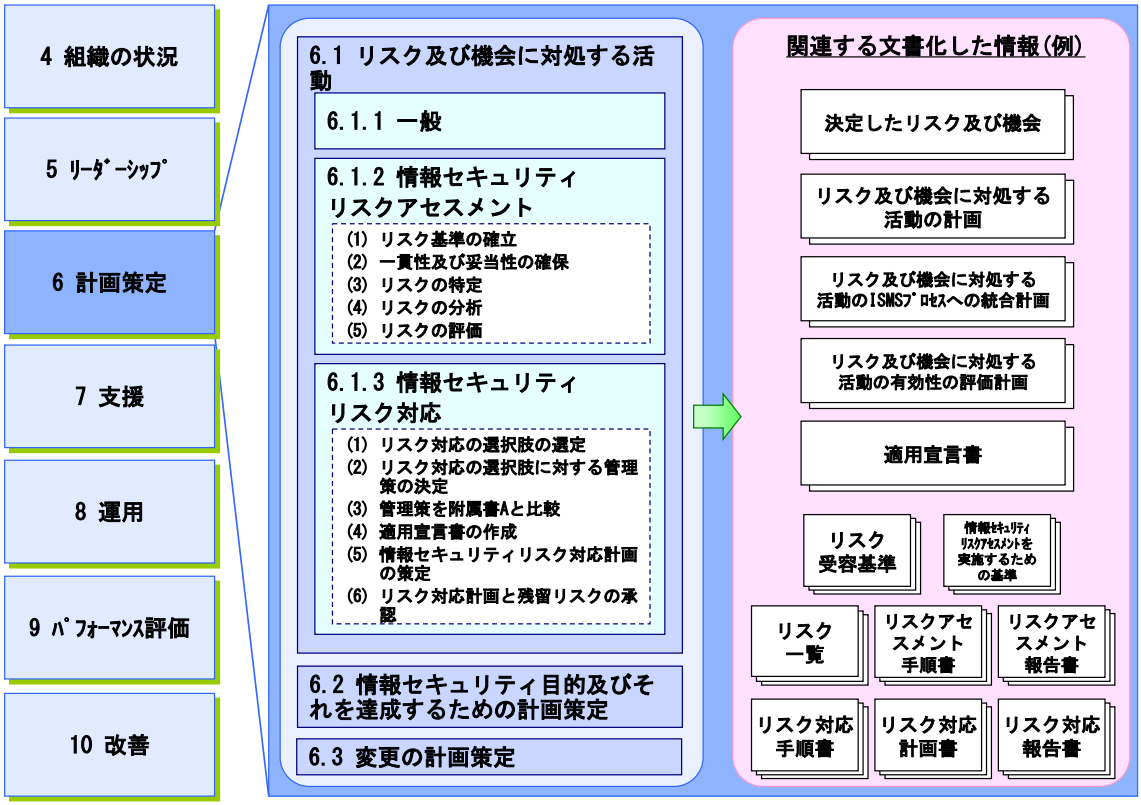


図 6-1　「6 計画策定」におけるプロセス（事例）　注）文書名は全て例示

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　一般」では、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　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。JIS Q 27001 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 31000:2019 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

マネジメントシステムの定義に当てはめると、ISMS は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す。6.1.1 では、この ISMS の計画を策定する際に

達成すべき 3 つの事項をあげ、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（リスクと機会については本ガイドの「0 序文」を参照）。

JIS Q 27001 におけるリスクの定義は ISO 31000:2018（JIS Q 31000:2019）すなわち ISO Guide 73:2009（JIS Q 0073:2010）の定義を引用しているので、「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 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「10.1 継続的改善」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。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（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 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）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統合して構築・維持すること、およびその活動の有効性の評価を求めています。これについては、「8.1 運用の計画策定及び管理」において、箇条 6 への言及があります。本ガイドの「8.1 運用の計画策定及び管理」も参照して下さい。

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。プロセスの大分類として、次の 5 つが提示されています。

（１）リスク基準の確立（6.1.2 a））
（２）一貫性及び妥当性の確保（6.1.2 b））
（３）リスクの特定（6.1.2 c））
（４）リスクの分析（6.1.2 d））
（５）リスクの評価（6.1.2 e））

また、情報セキュリティリスクアセスメントのプロセスは、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。文書化には、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。

（１）リスク基準の確立

リスク基準の確立は、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、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。

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。

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 情報セキュリティリスクアセスメント」は、この基準に基づいて実施されるものです。

（２）一貫性及び妥当性の確保

情報セキュリティアセスメントは、繰り返し実施した際に一貫性と妥当性があり、実施した結果が以前の結果と比較して評価でき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）リスクの特定

情報セキュリティリスクアセスメントの実施は、まず「情報セキュリティリスクを特定する」ことから始まります。「（１）リスク基準の確立」及び「（２）一貫性及び妥当性の確保」で確立した情報セキュリティリスクアセスメントのプロセスを用いて、保護すべき情報の機密性・完全性・可用性を喪失するリスクと、そのリスクの所有者を特定します。

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。

（４）リスクの分析

リスクの分析では、「（３）リスクの特定」で特定した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します。

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。

（５）リスクの評価

リスクの評価では、「（１）リスク基準の確立」で組織の状況を考慮して確定されたリスク基準と、「（４）リスクの分析」で決定したリスク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 情報セキュリティリスク対応」で詳細に説明します。

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では、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。

「6.1.2 情報セキュリティリスクアセスメント」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である、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

情報セキュリティリスク対応のプロセスの大分類として、次の 6 つが提示されています。

（１）リスク対応の選択肢の選定（6.1.3 a））
（２）リスク対応の選択肢に対する管理策の決定（6.1.3 b））
（３）管理策を附属書 A と比較（6.1.3 c））
（４）適用宣言書の作成（6.1.3 d））
（５）情報セキュリティリスク対応計画の策定（6.1.3 e））
（６）リスク対応計画と残留リスクの承認（6.1.3 f））

また、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。

（１）リスク対応の選択肢の選定

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。

－リスクの低減
－リスクの受容
－リスクの回避
－リスクの共有

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（リスクの低減）

「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。リスクを軽減する方法には、例えば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）を変えることなどが該当します。
例えば、JIS Q 27001 の附属書 A に記載されている 93 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 6-2 に示します。

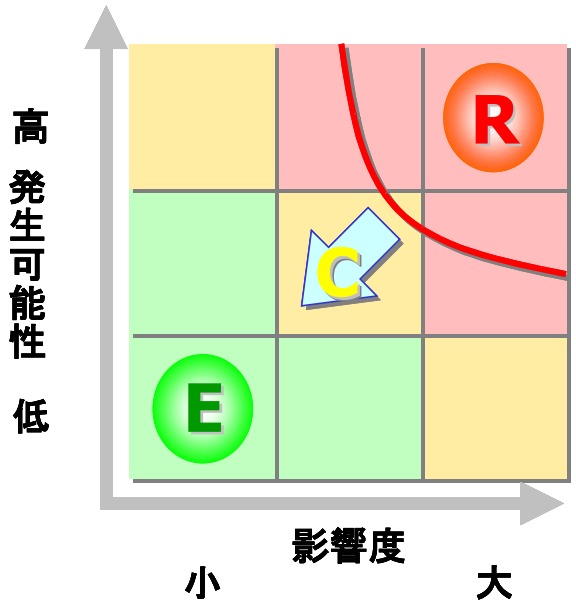


図 6-2　リスク低減の概念

図 6-2 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（リスクの受容）」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（リスクの受容）

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（リスクの回避）

「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（リスクの共有）

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クラウドサービスの利用、運用を委託するという方法などがあります。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、クラウド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 の附属書 A「情報セキュリティ管理策」には「5.19 供給者関係における情報セキュリティ」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。

リスク管理上は、JIS Q 27001 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管理策の決定

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 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 と比較

上記（２）で決定した管理策を、JIS Q 27001 の附属書 A「情報セキュリティ管理策」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、情報セキュリティ管理策の包括的なリストです。JIS Q 27001 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。適切な情報セキュリティ管理策が附属書 A に記載されていない場合は、組織が追加した情報セキュリティ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 に記載されている管理策のいくつかは、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、附属書 A「5.3 職務の分離」では、不正行為及び過失を防止するための職務の分離を管理策として規定していますが、その実施の手引を示

したJIS Q 27002:2024では、「小さな組織では、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、活動の監視、監査証跡、管理層による監督等の他の管理策を考慮することが望ましい。」と記載されているように、組織は管理策の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）適用宣言書の作成

上記（２）及び（３）で決定した管理策、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 に記載された情報セキュリティ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。

適用宣言書とは、ISMSに関連してその組織が適用する管理策を記述した、文書化された情報です。また、管理策とは、JIS Q 27001における「4.1 組織及びその状況の理解」及び「4.2 利害関係者のニーズ及び期待の理解」、並びに「6 計画策定」におけるリスクアセスメントから導き出される、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「情報セキュリティ管理策」の管理策を特定します。適用宣言書には、適用及び実施している管理策とその理由、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。

（５）情報セキュリティリスク対応計画の策定

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 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」参照）。

情報セキュリティ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、選択した情報セキュリティ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、十分な情報セキュリティ管理策が実装できないことにもつながりますので、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情報セキュリティ管理策を策定するだけではなく、導入した情報セキュリティ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策や、異常を検出するための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情報セキュリティ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）リスク対応計画と残留リスクの承認

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。

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「情報セキュリティ目的」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、組織と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情報セキュリティ目的については、組織としてその情報セキュリティ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て実施することが求められます。計画は、情報セキュリティ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。

６．３　変更の計画策定

変更の計画策定では、「6. 計画策定」でこれまでに説明した ISMS の計画について、変更する必要があると組織が決定した際の対応について示しています。
ISMS の計画策定にあたっては、「6.1 リスク及び機会に対処する活動」に示した通り、リスクアセスメント及びリスク対応を通じて実施します。ここで、リスクは常に変化しうることを前提として、変化したリスクに対応して計画を変更していくことが重要です。

リスクの変化は、組織の内部状況及び外部状況の変化によって発生します。
組織の内部状況の変化としては、ISMS 適用範囲の変更、取り扱う情報の変更、使用する情報システムの変更、情報を取り扱う人員の変更、外部委託の範囲や委託先の変更、などが考えられます。
組織の外部状況の変化としては、サイバー攻撃手法の高度化・巧妙化、関連する法規制の変更、取引先などの利害関係者の変更、などが考えられます。

ISMS の変更は、計画的に行う必要があります。つまり、ISMS の変更の要否を確認する方法やタイミングを場当たり的に行うのではなく、組織で定めた方法で実施することが求められます。
計画的に実施する典型的な例は、リスク分析とリスク対応に関する PDCA サイクルを定めて、計画の定期的な見直しを行うことです。例えば 1 年に一度、リスク分析を改めて実施して、リスクの変化が起きていないか確認します。リスクに変化が生じていた場合には、その変化に対するリスク対応を検討します。リスクの変化は、必ずしも増大するばかりではなく、減少するケースもあります。減少した場合は、リスク対応が過剰になりすぎないように調整する必要があります。

ISMS の変更の要否を確認する方法やタイミングとしては、「9. パフォーマンス評価」で説明する「9.1 監視、測定、分析及び評価」の方法や、「9.2 内部監査」のタイミングなどが代表的です。定期的に情報セキュリティリスクアセスメントを実施し、新たなリスク及び機会が生じていないか、特定したリスクのリスクレベルに変化がないかなどを確認して、リスク対応計画を見直すなどの対応を行う必要があります。

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。

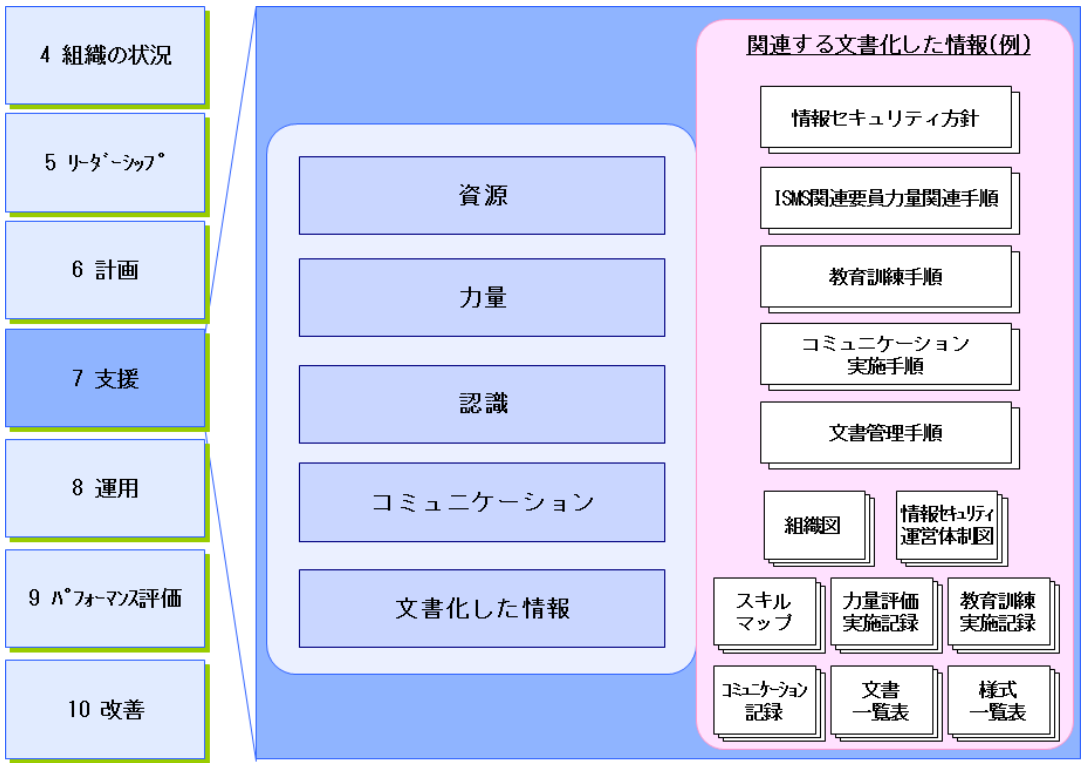


図 7-1　ISMS の支援（事例）　注）文書名は全て例示

７．１　資源

7.1 において、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。資源を提供する際の留意点として、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、ISMS の構築・実施から継続的な維持・改善に至るまでのライフサイクル全体で必要となる資源を予測し、事前に対応しておくことで、組織の活動を円滑化することが肝要です。
特にトップマネジメントは、この資源の予想や決定、配分に深く関与することになります。「人」、「物」、「金」、「情報」といった ISMS に必要な資源が利用可能であることを確実にするという重要な役割を果たすことが、トップマネジメントに求められます。そのためにトップマネジメントは、ISMS の必要性を理解しておくことが必要です。

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。

７．２　力量

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。

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。力量は、JIS Q 27000:2019 において「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」と定義されています。

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）[1]、公認会計士、公認システム監査人 [2]、システム監査技術者 [3]、公認情報システム監査人（CISA）[4]、ISMS 主任審査員、ISMS 審査員、公認情報セキュリティ監査人（CAIS）[5]
セキュリティ技術	情報処理安全確保支援士 [6]、公認情報セキュリティ管理者（CISM）[7]、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）[8]

７．３　認識

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、組織の管理下で働く人々自らの業務・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。

---

[1] 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） https://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、2024 年現在、全世界で約 245,000 名が内部監査人協会に所属している。

[2] 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（https://www.saaj.or.jp）が認定するシステム監査人の資格。

[3] 独立行政法人情報処理推進機構（https://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。

[4] 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 https://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 180,000 名以上（非会員の資格認定者を含む）が ISACA に所属している。

[5] 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。

[6]情報処理安全確保支援士は、サイバーセキュリティ対策を推進する人材の国家資格。

[7] 公認情報セキュリティマネージャー（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 https://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。

[8]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 https://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。

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。

７．４　コミュニケーション

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 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**

７．５　文書化した情報

７．５．１　一般

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。

JIS Q 27000:2019 では、文書化した情報を、「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」と定義しており、その注記を見ると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。

また、JIS Q 27001 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 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 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。 g) 文書化した情報として利用可能な状態にする。 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。
7.2	7.2 力量 組織は，次の事項を行わなければならない。 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 の計画策定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，必要に応じて識別し，管理しなければならない。
8.1	8.1 運用の計画策定及び管理 組織は，プロセスが計画どおりに実施されたという確信をもつために必要とされる，文書化した情報を利用可能な状態に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。
8.3	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，この結果の証拠として，文書化した情報を利用可能な状態にしなければならない。
9.2.2	9.2.2 内部監査プログラム 組織は，監査プログラムの実施及び監査結果の証拠として，文書化した情報を利用可能な状態にしなければならない。
9.3.3	9.3.3 マネジメントレビューの結果 組織は，マネジメントレビューの結果の証拠として，文書化した情報を利用可能な状態にしなければならない。
10.2	10.2 不適合及び是正処置 組織は，次に示す事項の証拠として，文書化した情報を利用可能な状態にしなければならない。 f) 不適合の性質及びそれに対して講じたあらゆる処置 g) 是正処置の結果

（JIS Q 27001:2023　上記各項　より引用）

７．５．２　作成及び更新

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

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 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

5.28	証拠の収集	組織は，情報セキュリティ事象に関連する証拠の特定，収集，取得及び保存のための手順を確立し，実施しなければならない。
5.33	記録の保護	記録は，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 27001:2023　附属書 A（規定）情報セキュリティ管理策　より引用）

詳細は、JIS Q 27002:2024 の「5.28 証拠の収集」、「5.33 記録の保護」を参照して下さい。

８．運用

８．１　運用の計画策定及び管理

運用の計画策定及び管理では、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計画・実施・管理することを規定しています。
これには「6.1　リスク及び機会に対処する活動」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。

また、「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「8.1　運用の計画策定及び管理」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。

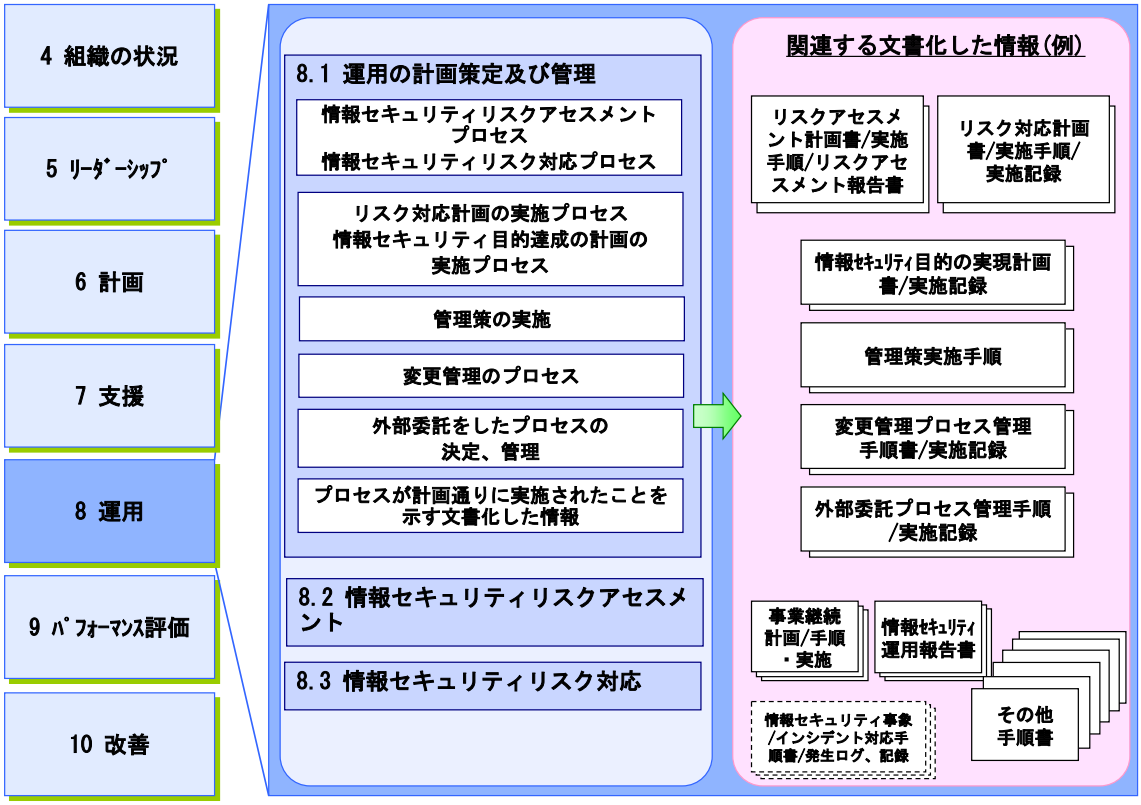


図 8-1　「8 運用」におけるプロセス（事例）　注）文書名は全て例示

ここからは図 8-1 で挙げた「8.1　運用の計画策定及び管理」における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 リスク及び機会の対処する活動」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 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」で定めた計画に従い、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した情報

計画通り実施されたことを示す文書化した情報とは、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、ISMS 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 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

情報セキュリティリスクアセスメントでは、「6.1.2 情報セキュリティリスクアセスメント」で確立したプロセスに従って、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）、リスクアセスメントを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。

８．３　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では、「8.2 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 情報セキュリティリスク対応」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。

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。

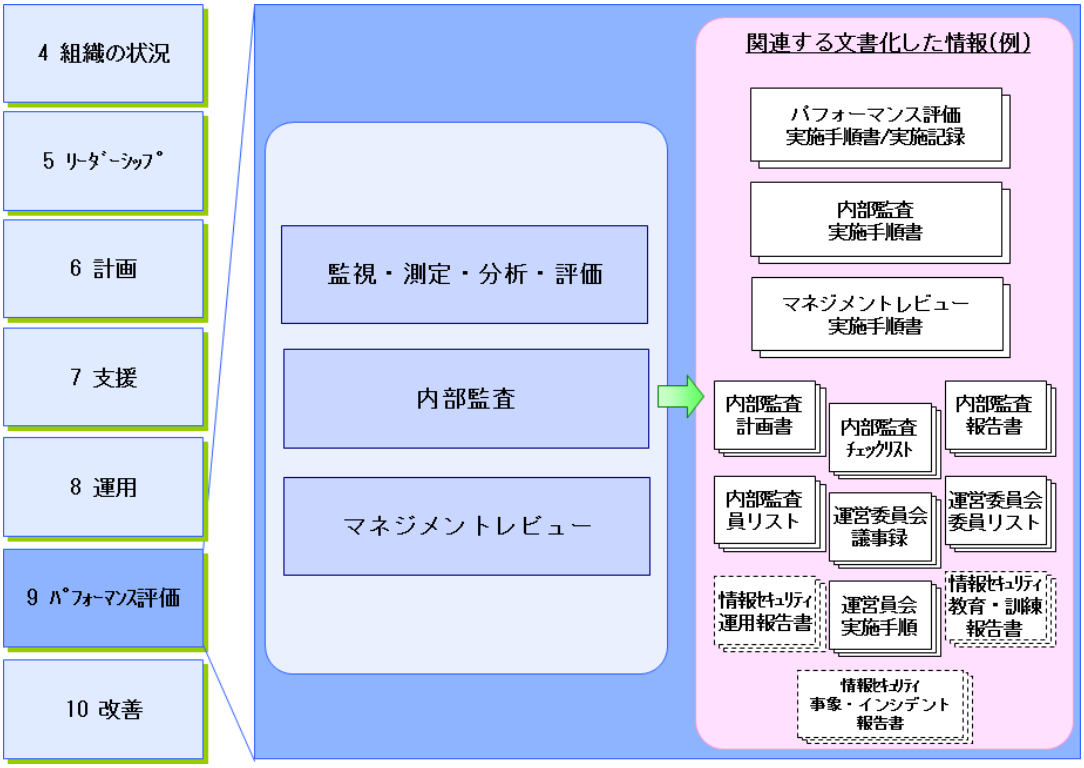


図 9-1　ISMS のパフォーマンス評価のプロセス　　注）文書名は全て例示

箇条 9 で使用されている以下の用語は、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、JIS Q 27000:2019 で定義されています。

3.13 継続的改善（continual improvement）
3.43 測定（measurement）
3.46 監視（monitoring）
3.52 パフォーマンス（performance）

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 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 6.1.1 d)及び e)で規定しています。

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「9.1.2 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

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。
また、監視及び測定の時期、実施者を定めることが要求されています。その監視及び測定の結果を分析、評価する時期と、その実施者を明確にすることも必要です。
監視、測定、分析及び評価の結果の証拠として、それらの結果を文書（文書化した情報）として利用可能な状態にしておくことが要求されています。

JIS Q 27001 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 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 以後では、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っています。

９．１．１　パフォーマンス測定

管理策の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。

例えば、JIS Q 27001 の 9.1「a) 監視及び測定が必要な対象（情報セキュリティプロセス及び管理策を含む）」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たかどうか評価し、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のインプットと結果

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の例としては、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「パフォーマンス測定結果」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。

パフォーマンス測定手順書の概要例

JIS Q 27001 の 9.1 では、パフォーマンスに関して文書化した情報を利用可能な状態にすることを要求しています。

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）

９．１．２　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。

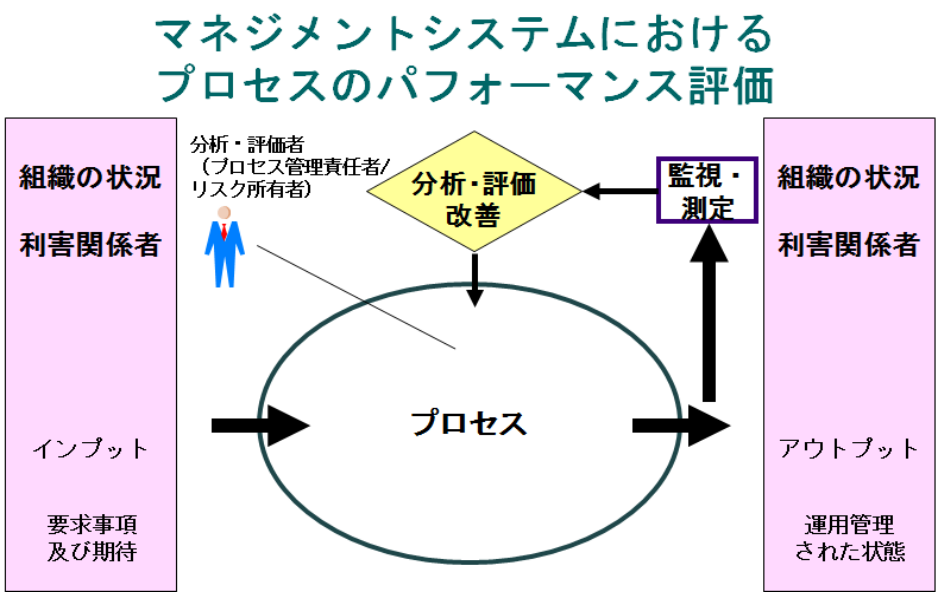


図 9-2　マネジメントシステムにおけるプロセスのパフォーマンス評価の位置づけ

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。

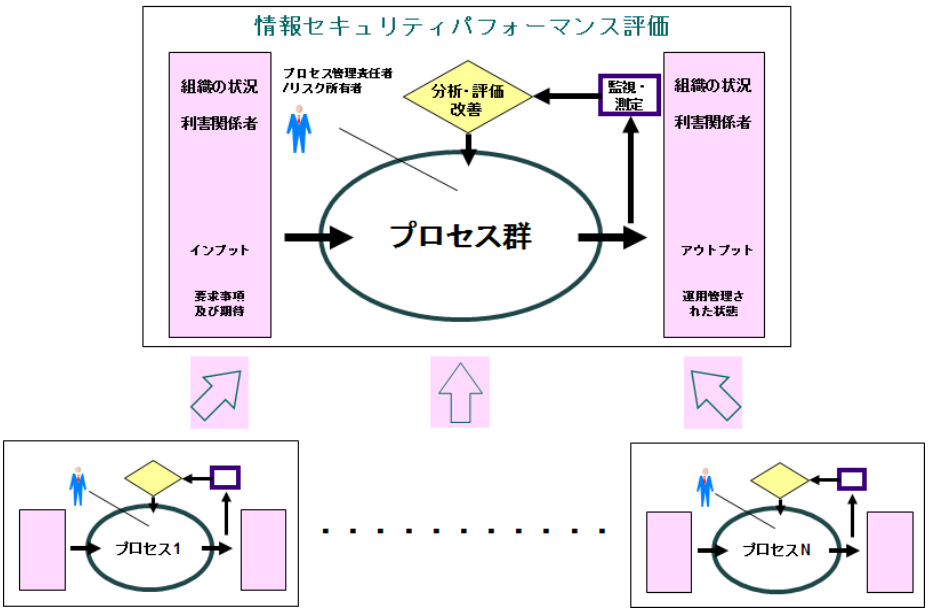


図 9-3　ISMS の情報セキュリティパフォーマンス

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、JIS Q 27000:2019 の 3.14 によると「リスクを修正するための対策」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
を含むパフォーマンス測定結果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。

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 の 5.3b)）、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（9.3.2）。

９．２　内部監査

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 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。

JIS Q 27001 の 9.2.2 では、内部監査プログラムについての考慮事項や報告、文書化について求められており、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。
監査員の独立性が求められているわけではありませんが、独立性については、JIS Q 19011:2019「マネジメントシステム監査のための指針」の箇条 4 e）で次のように説明されており、参考にすることができます。

> 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，実行可能な場合には，監査の対象となる機能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可能でない場合もあるが，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 19011:2019　4 監査の原則　より引用）

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 の理解、JIS Q 19011:2019 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。

9.2.1「a)2)この規格の要求事項」については、「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を含める場合がある。」と記述していることから、それらを含めた場合には、何を含めたかを確認できるように管理するのがよいと考えられます。

９．３　マネジメントレビュー

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 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 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。

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

JIS Q 27001 に基づくマネジメントレビューへのインプットとしては、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
- 情報セキュリティマネジメントシステムに関連する利害関係者のニーズ及び期待の変化
  －関連する利害関係者に過不足がないかの確認
  －各利害関係者よるニーズ及び期待の確認
- 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
  －とった処置の状況や処理の誤り、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 では「継続的改善の機会」と「ISMSのあらゆる変更の必要性に関する決定」の2つの事項を挙げています。

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 の 4.1）、利害関係者のニーズ及び期待（JIS Q 27001 の 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

改善のプロセスでは、ISMS を継続的に改善し、不適合が発生した場合の対処について規定しています。

例えば、10 章のプロセスを例示すると図 10-1 のようになります。

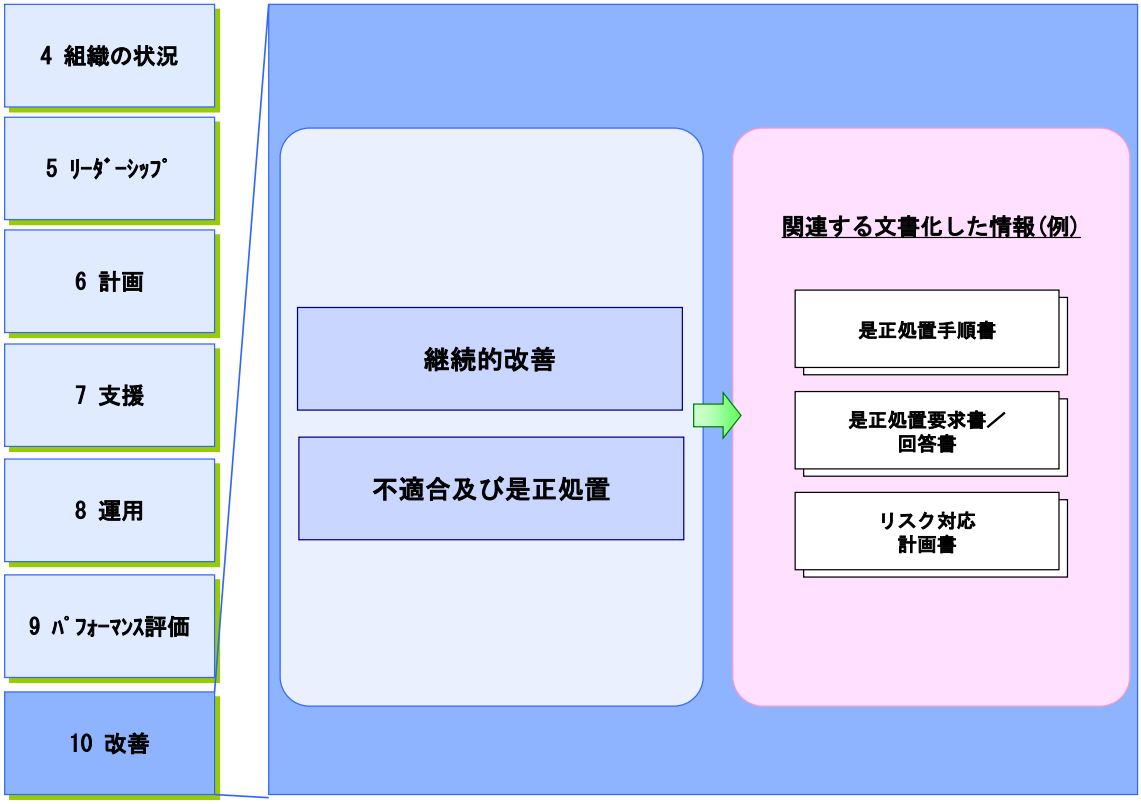


図 10-1　改善のプロセス　　注）文書名は全て例示

１０．１　継続的改善

10.1 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、JIS Q 27000:2019 では、継続的改善は「パフォーマンスを向上するために繰り返し行われる活動」と定義されています。また、パフォーマンスは、「測定可能な結果」と定義されています。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。10.1 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の訳ですが、continualという英語は継続的又は断続的であることから、時間的に切れ目なく連続である必要はなく、断続的でも繰り返して行われることを意味します。

この10.1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 27000:2019の3.20では「計画した活動を実行し，計画した結果を達成した程度」と定義しています。

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、本ガイドの10.2で例示したJIS Q 27001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 に関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。

１０．２　不適合及び是正処置

10.2 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 27000:2019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の規格要求事項
- JIS Q 27001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 27000:2019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、根本原因を精査し十分に評価することが重要となります。

また、10.2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」（10.2 a）1）で言及）と「是正処置」（10.2 b）で言及）は、異なります。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。」（10.2 b）3））は、是正処置の水平展開にあたりますが、発生する前に防止する、いわゆる、予防処置にあたるものでもあります。

－ 有効性のレビュー（10.2 d）で言及）は、計画した活動及び計画した結果がどの程度達成されているかをレビューすることです。

3.16 修正（correction）
検出された不適合（3.47）を除去するための処置。

3.17 是正処置（corrective action）
不適合（3.47）の原因を除去し，再発を防止するための処置。

3.20 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。

3.47 不適合（non-conformity）
要求事項（**3.56**）を満たしていないこと。
（JIS Q 27000:2019 3 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。

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ており、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っています。

附属書 A（規定）　情報セキュリティ管理策

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 93 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 27002:2024 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 27002:2024 との関係

従来の JIS Q 27001:2014 附属書 A が JIS Q 27002:2014 と整合がとられていたことと同じように、JIS Q 27001:2023 附属書 A も JIS Q 27002:2024 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 8 には、93 の管理策について記述されています。
また、JIS Q 27001:2024 附属書 A では項番の管理目的はなくなりましたが、その代わりに各管理策の意図を示すため管理策毎に目的が追加されました。

これらの管理策は、その項番、内容とも、JIS Q 27001 附属書 A の管理策と同じです。異なる点としては、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。この点以外は、両者の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、管理策以外にも、各管理策の内容を詳細に説明した「手引」、さらには各管理策に関連する情報をまとめた「その他の情報」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 27001:2023 附属書 A と JIS Q 27001:2014 附属書 A の対比

JIS Q 27001:2023 附属書 A の管理策は、JIS Q 27001:2014 附属書 A の管理策を大幅に再編成し、管理策数も 114 から 93 となりました。これに伴い、JIS Q 27001:2014 では管理策の箇条は 14（5～18）ありましが、JIS Q 27001:2023 では表 A-1 の通り 4 つ（5～8）に整理されています。

ISO/IEC 27001:2023 への改訂時に、ISO 中央事務局の編集によって項番から A が削除されましたが、ISMS の運用には直接的な影響はありません。

表 A-1　JIS Q 27001:2014 附属書 A と JIS Q 27001:2023 附属書 A の箇条構成

JIS Q 27001:2014 附属書A	JIS Q 27001:2023 附属書A
A.5 情報セキュリティのための方針群	5 組織的管理策
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	6 人的管理策
A.8 資産の管理	
A.9 アクセス制御	
A.10 暗号	7 物理的管理策
A.11 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.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.15 供給者関係	8 技術的管理策
A.16 情報セキュリティインシデント管理	
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.18 順守	

このように構成は大幅に変更されましたが、一方で管理策の内容は、基本的には JIS Q 27001:2014 を踏襲し、JIS Q 27001:2014 附属書 A の管理策を統合、更新したものとなっています。今回、箇条と内容の整理が行われた結果、JIS Q 27001:2014 附属書 A の 24 個の管理策が統合、58 個の管理策が更新されました。これは、新たな動向や技術の進歩に伴い、管理策が調整、変更されたことによります。さらに、新たな脅威や技術の進歩等に合わせて、表 A-2 に示す 11 の新規管理策が追加されています。

表 A-2　追加の管理策

5.7	脅威インテリジェンス
5.23	クラウドサービスの利用における情報セキュリティ
5.30	事業継続のための ICT の備え
7.4	物理的セキュリティの監視
8.9	構成管理
8.10	情報の削除
8.11	データマスキング
8.12	データ漏えい防止
8.16	監視活動
8.23	ウェブフィルタリング
8.28	セキュリティに配慮したコーディング

JIS Q 27001:2023 と JIS Q 27001:2014 の管理策の対応関係の詳細は、JIS Q 27002:2024 附属書 B（参考）「この規格と JIS Q 27002:2014 との対応」を参照すると良いでしょう。

ISMS 専門部会

（順不同・敬称略）

氏名	会社・機関名
委員	
【主査】 駒瀬　彰彦	株式会社アズジェント
相羽　律子	株式会社日立製作所
河野　省二	日本マイクロソフト株式会社
笹原　英司	一般社団法人日本クラウドセキュリティアライアンス
佐藤　慶浩	オフィス四々十六
澤部　直太	ナオサイバーテック株式会社
中村　良和	日本マネジメントシステム認証機関協議会 （BSI グループジャパン株式会社）
オブザーバ	
池田　佳高	経済産業省商務情報政策局サイバーセキュリティ課
角田　潤	経済産業省イノベーション・環境局　国際電気標準課
保木野　昌稔	一般社団法人情報マネジメントシステム認定センター（ISMS-AC）

JIPDEC
〒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
一般財団法人 日本情報経済社会推進協会
TEL 03-5860-7561 FAX 03-5573-0561
URL https://www.jipdec.or.jp/