01 ISO規格とは

ISOとは、スイスのジュネーブに本部を置く国際標準化機構（International Organization for Standardization）の略称です。ISOの主な活動は国際的に通用する規格を制定することであり、ISOが制定した規格をISO規格といいます。

ISOとは

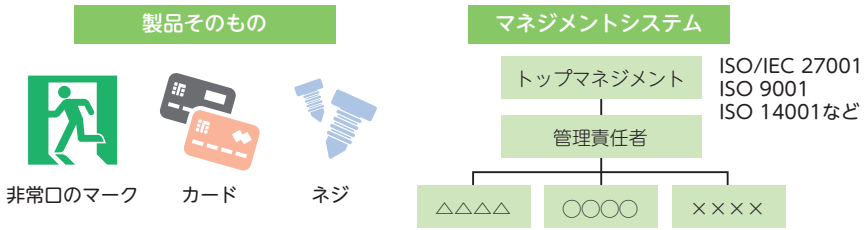
ISO（国際標準化機構）は、国際的な取引をスムーズにするため、**製品やサービスに関して「世界中で同じ品質、同じレベルのものを提供できるようにする」という国際的な基準を発行する機関**として、1974年2月23日に発足しました。

ISOでは、各国1機関のみの参加が認められており、日本からは日本産業規格（JIS）の調査・審議を行っている日本産業標準調査会（JISC）が加入しています。

ISO規格の身近な例としては、非常口のマークやカードのサイズ、ネジといった規格が挙げられます。これらは製品そのものを対象とする「モノに対する規格」です。

一方、製品そのものではなく、組織を取り巻くさまざまなリスク（品質、環境、情報セキュリティなど）を管理するためのしくみについてもISO規格が制定されています。これらは**「マネジメントシステム規格」**と呼ばれ、品質マネジメントシステム（ISO 9001）や環境マネジメントシステム（ISO 14001）、情報セキュリティマネジメントシステム（ISO/IEC 27001）などの規格が該当します。

■ ISOの例



ISO規格の制定や改訂は、ISO技術管理評議会（TMB）の各専門委員会（TC）で行われます。

各TCではさまざまな業務分野を扱うため、分科委員会（SC）、作業グループ（WG）を設置して、規格の開発活動を行っており、制定や改訂は、168の標準化団体（2021年12月現在）の投票によって決定します。

ISOでは、国際規格（IS）以外にも、技術仕様書（TS）、技術報告書（TR）、一般公開仕様書（PAS）なども発行しています。

■ ISOの主要な刊行物

分類	概要
国際規格 （IS：International Standard）	ISO参加国の投票に基づいて発行される国際規格
技術仕様書 （TS：Technical Specification）	WGで合意が得られたことを示す規範的な文書。TC/SCは、IS作成に向けて技術的に開発途上にあったり、必要な支持が得られなかったりして当面の合意が不可能な場合に、特定業務項目をISO/TSとして発行できる
技術報告書 （TR：Technical Report）	通常の規範的な文書として発行されるものとは異なる情報を含んだ情報提供型の文書。ISOの委員会が作業のために集めた情報をTRの形で発行することをISO中央事務局に要請して、ISO/TRの発行が決定される
一般公開仕様書 （PAS：Publicly Available Specification）	ISOの委員会で技術的に合意されたことを示す規範的な文書。TC/SCは、技術開発途上であり当面の合意が得られない場合、また、TSほどの合意が得られない場合に、特定業務項目をISO/PASとして発行できる

03 ISO/IEC 27000 ファミリー規格

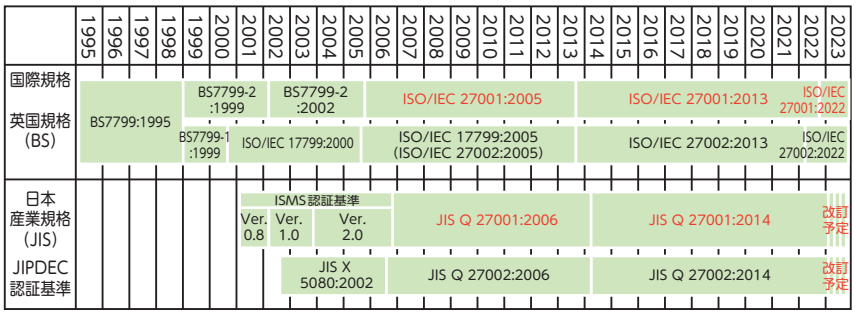
ISOとIECでは、ISO/IEC 27001以外にもさまざまな規格を発行し、改訂を行っています。それらは総称して「ISO/IEC 27000ファミリー規格」と呼ばれ、各規格によって発行状態が異なります。

ISO/IEC 27001の発行・改訂

ISO/IEC 27001の歴史は、1995年に発行されたISMS（情報セキュリティマネジメントシステム）の英国規格であるBS7799から始まります。BS7799は、ISMSを国際規格とするために1999年に改訂され、BS7799-1（情報セキュリティマネジメントの実践のための規範）とBS7799-2（情報セキュリティマネジメントシステム－要求事項）の2部構成になり、BS7799-2の認証制度が始まりました。

日本では、**JIPDEC（一般財団法人日本情報経済社会推進協会）**が、BS7799-2をもとにISMS認証基準を作成し、2002年4月からISMS適合性評価制度を開始しました。その後、BS7799-2は国際規格となることが決定され、ISO/IEC 27001（情報セキュリティマネジメントシステム－要求事項）の初版が2005年に発行されたことで国際的な認証基準となり、その後2013年、2022年に改訂されました。

■ ISO/IEC 27001の発行と改訂



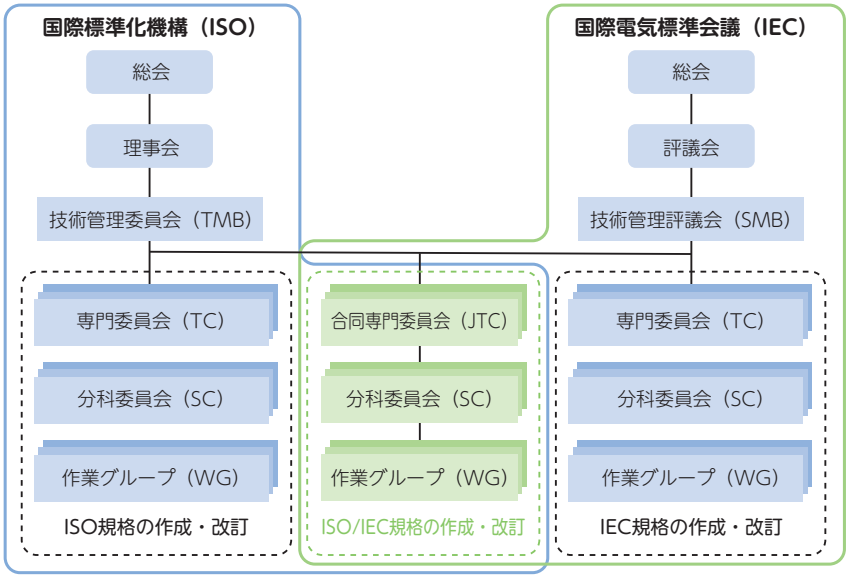
ISO/IEC 27000ファミリー規格と呼ばれるISO/IEC 27001などのISMS関連規格は、情報システムやネットワークなどが含まれるため、電気通信を除く全分野の国際規格を定める**国際標準化機構（ISO）**と、電気技術分野の国際規格を定める**国際電気標準会議（IEC）**とで共同発行されています。

ISOとIECが共同で国際規格を発行・改訂する場合は、合同専門委員会（JTC）の分科委員会（SC）と作業グループ（WG）において標準化作業を進めていきます。具体的には、ISO/IEC JTC1（情報技術）のSC27（セキュリティ技術）のWGが作業を担当しています。

ISO/IEC規格の発行・改訂は、ISOと同じ6段階の流れに分かれています。

① 新作業項目（NP）の提案
② 作業原案（WD）の作成
③ 委員会原案（CD）の作成
④ 国際規格原案（DIS）の照会及び策定
⑤ 最終国際規格案（FDIS）の策定
⑥ 国際規格（IS）の発行

■ ISO/IEC規格の発行と改訂の体制



05 ISMS 適合性評価制度の概要

情報セキュリティマネジメントシステム（ISMS）適合性評価制度とは、情報マネジメントシステム認定センター（ISMS-AC）が認定機関として運営するISO/IEC 27001の認証取得制度です。

ISMS適合性評価制度の成り立ち

ISMS（情報セキュリティマネジメントシステム）適合性評価制度は、情報処理サービス業における情報システムの施設・設備などに十分な安全対策を施しているかどうかを認定する制度としてあった「情報システム安全対策実施事業所認定制度（安対制度）」の廃止にともない、技術的なセキュリティのほかに、**組織の要員による運用・管理面をバランスよく取り込み、時代のニーズに合わせた新しい制度**として創設され、2002年4月から本格運用を開始しました。

ISMS適合性評価制度の創設時には、JIPDEC（一般財団法人日本情報経済社会推進協会、旧名称：財団法人日本情報処理開発協会）が運営していましたが、2018年4月からISMS-AC（一般社団法人情報マネジメントシステム認定センター）が制度を運営しています。

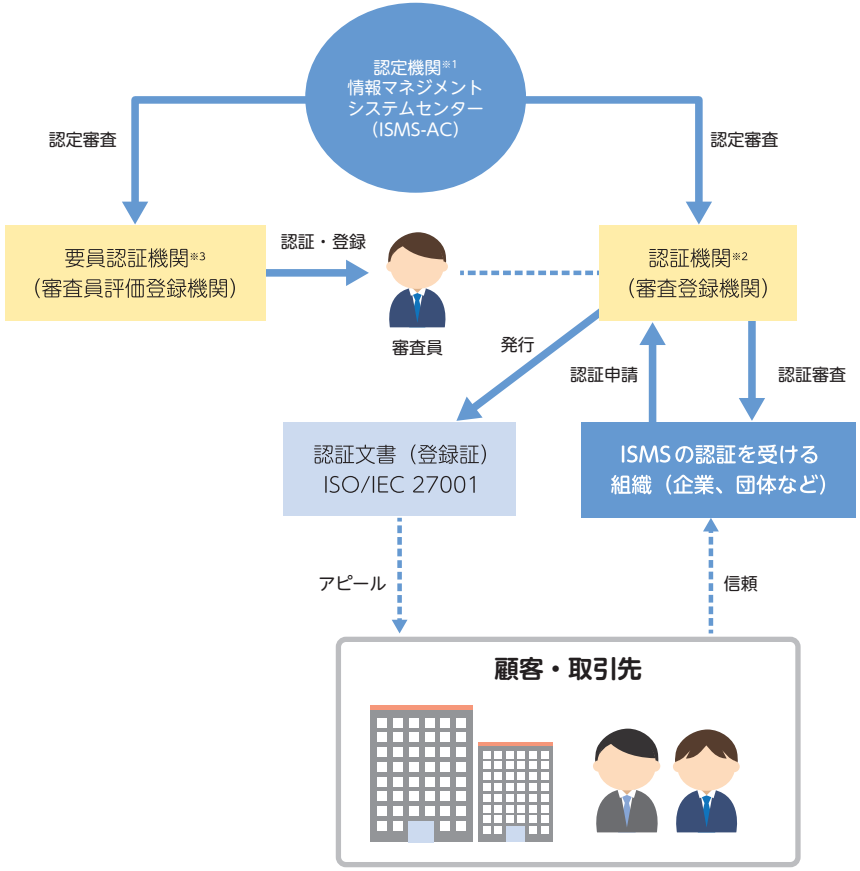
■ 情報マネジメントシステム認定センター（ISMS-AC）

https://isms.jp/

ISMS-ACと認証機関、認証希望組織の関係

認証希望組織がISO/IEC 27001を認証取得するためには、ISMS-ACから認定された26機関の認証機関（審査登録機関）のいずれかに審査を申し込み、審査を受けて認証組織として登録されなければなりません。認証希望組織は、制度や認証機関についての意見や苦情をISMS-ACに申し立てることができます。

■ ISMS-ACと認証機関、認証希望組織の関係図



※1 認定機関：認証機関が適切に認証審査を実施できることを審査して確認する
※2 認証機関：第三者機関として組織のISMSを審査する
※3 要員認証機関：認証審査に関する能力を持つ審査員を認証して登録する

参考：ISMS適合性評価制度の概要（https://isms.jp/isms/about）

09 マネジメントシステムに関する用語

ISO/IEC 27001は、情報セキュリティについてのマネジメントシステム規格です。ISO/IEC 27000（JIS Q 27000）には、情報セキュリティに関する用語以外にも、マネジメントシステムに関する用語の定義が定められています。

マネジメントシステムに関する重要な用語の定義

ISO/IEC 27001には、さまざまなマネジメントシステムに関する用語が使用されています。規格を理解するうえで重要な用語の定義は次の通りです。

(1) マネジメントシステム (management system)

【定義】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（JIS Q 27000:2019の3.41）

マネジメントシステムは単なるしくみではなく、PDCAサイクルの構築と継続的な運用・改善が求められます。

(2) 方針 (policy)

【定義】トップマネジメントによって正式に表明された組織の意図及び方向付け（JIS Q 27000:2019の3.53）

ISMSでは**情報セキュリティ方針**の策定が必須となります。

(3) 目的 (objective)

【定義】達成する結果（JIS Q 27000:2019の3.49）

ISMSの場合、組織は特定の結果を達成するため、情報セキュリティ方針と整合性の取れた**情報セキュリティ目的**を設定することが要求されます。

(4) プロセス (process)

【定義】インプットをアウトプットに変換する、相互に関連する又は相互に作用する一連の活動（JIS Q 27000:2019の3.54）

プロセスとは、仕事や作業などの業務を指します。

■ プロセスの例

インプット	プロセス	アウトプット
引合い情報	営業業務	受注・契約
注文書	製品販売業務	製品の出荷・配送

(5) 文書化した情報 (documented information)

【定義】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（JIS Q 27000:2019の3.19）

文書化した情報は、組織の運用のために作成された情報（文書類）や達成された結果の証拠（記録）が該当し、紙媒体やPDFだけでなく、情報システムへの登録情報などを電子化したものなど、あらゆる形式・媒体が含まれます。

(6) 力量 (competence)

【定義】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 27000:2019の3.9）

ISMSでは、担当する業務や責任の範囲に合わせて必要な力量を明確にし、必要に応じて教育・訓練を実施して力量を確保することが求められます。たとえば、ISMS内部監査員には、ISO/IEC 27001の知識や内部監査の実務、情報技術に関する知識などが求められます。

(7) 監査 (audit)

【定義】監査基準が満たされている程度を判定するために、監査証拠を収集し、それを客観的に評価するための、体系的で、独立し、文書化したプロセス（JIS Q 27000:2019の3.3）

ISMSでは内部監査が要求されます。監査では、**監査基準**（ISO/IEC 27001、ISMS関連ルール、法規制など）と**監査証拠**（質問の回答、目視での確認、文書

12 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

ISO/IEC 27001の「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」は、外部・内部の課題、利害関係者のニーズ、管理できる情報の範囲を考慮して、ISMSの適用範囲を決定することを要求しています。

合理的な理由に基づいて適用範囲を決定する

ISO/IEC 27001の「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」では、以下の①～③を考慮して、ISMSの適用範囲（活動範囲）を決定することが求められています。また、その**文書化**も求められています。

①「4.1 組織及びその状況の理解」で決定した外部・内部の課題
②「4.2 利害関係者のニーズ及び期待の理解」で決定した利害関係者の情報セキュリティに関連する要求事項
③ 組織が実施する活動（業務内容）や他の組織との情報のやり取り、システムやネットワークの共有などその方法

適用範囲の文書化については、組織の名称や部門名、場所や区画、対象業務や対象となる資産、ネットワークの範囲などを明確にする必要があります。

■ 適用範囲の文書化に含まれる内容

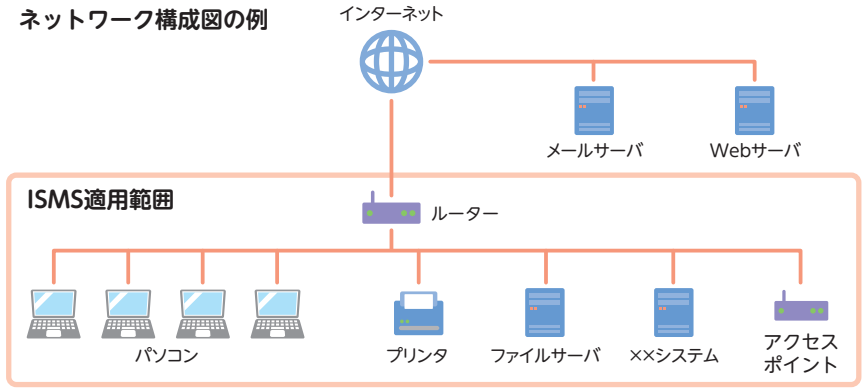
組織	・対象組織、その全体における位置付け ・適用範囲外の関連部門・外部組織とのインターフェース
ロケーション	・地域的ロケーションおよび同一建物内のレイアウト（区画）
事業・業務	・関連する事業・業務の中での位置付け、それらとの関連と境界 ・事業・業務のプロセス（しくみと流れ）の定義、そこにおける位置付けと境界
資産	・対象となる情報資産
技術	・対象とする情報システム、ネットワーク

ISMSの適用範囲は、組織全体や関連企業すべてなどのように複数の組織を対象にしたり、事業部や営業部などのように特定の部門だけを対象にしたりして適用範囲を決定することができますが、「なぜその適用範囲にしたのか？」という問いに対して、明確で合理的な理由が必要となります。

■ 適用範囲の記載例

組織	株式会社〇〇〇〇
ロケーション	本社：東京都〇〇〇〇 支社：大阪府〇〇〇〇
事業・業務	〇〇システムの設計、開発、販売および保守サポート
資産	当社が持つすべての資産および情報システム
技術	以下の図を参照

ネットワーク構成図の例



まとめ

- **適用範囲の決定には合理的な理由がなければならない**
- **適用範囲は文書化する**
- **ISMSを適用するネットワークの範囲も明確にする**

14 5.1 リーダーシップ及びコミットメント

ISO/IEC 27001の「5.1 リーダーシップ及びコミットメント」は、ISMSのトップマネジメントが責任を持たなければならない内容について要求しています。

トップマネジメントの責任の内容

トップマネジメントとは、**「最高位で組織を指揮し、管理する個人又は人々の集まり」(JIS Q 27000:2019の3.75)**と定義され、ISMSの適用範囲における最高責任者を指します。コミットメントは、誓約や約束、関与と訳されますが「トップマネジメントの責任において必ずやること」として、①～⑧が要求されています。また、箇条5はISMSのPDCAサイクルの中心（軸）となるものです。

■ トップマネジメントに求められる内容

①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【5.1 a)】
②組織のプロセスへのISMS要求事項の統合を確実にする【5.1 b)】
③ISMSに必要な資源が利用可能であることを確実にする【5.1 c)】
④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【5.1 d)】
⑤ISMSがその意図した成果を達成することを確実にする【5.1 e)】
⑥ISMSの有効性に寄与するよう人々を指揮し、支援する【5.1 f)】
⑦継続的改善を促進する【5.1 g)】
⑧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【5.1 h)】

まとめ

- **ISMSのPDCAサイクルを運用していくためには、トップマネジメントのコミットメントが重要**

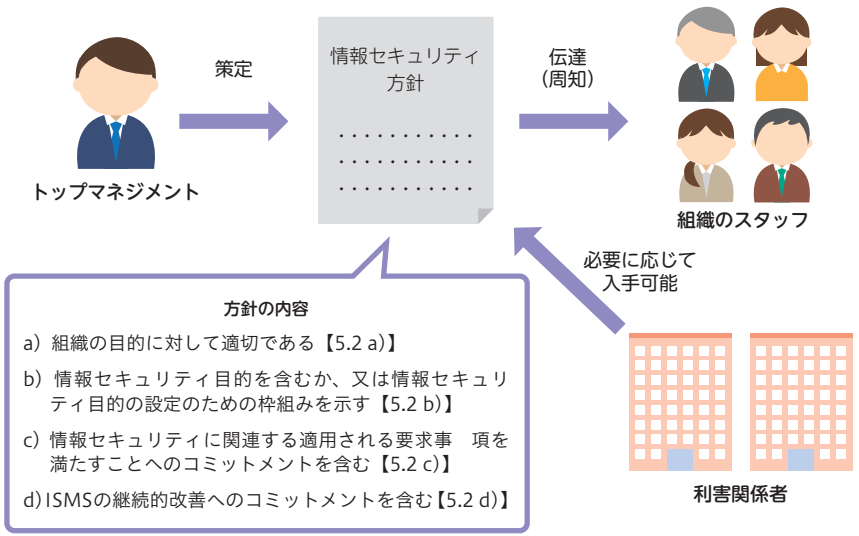
15 5.2 方針

ISO/IEC 27001の「5.2 方針」は、トップマネジメントが示すISMSの方向性や実施しなければならないことを「情報セキュリティ方針」として文書化することを要求しています。

「情報セキュリティ方針」の作成

ISO/IEC 27001の「5.2 方針」では、トップマネジメントが組織のISMSで成し遂げる成果や、実施しなければならないことを**「情報セキュリティ方針」**として文書化し、組織内への伝達（周知）や、必要に応じて利害関係者が入手できるようにすることを要求しています。情報セキュリティ方針は、以下のa)～d)の内容を満たすことが要求されますが、規格の文書をそのまま記載することは要求事項の趣旨ではないので、それを理解して組織の方針を作成する必要があります。

■ 情報セキュリティ方針の策定と伝達など



22 7.1 資源

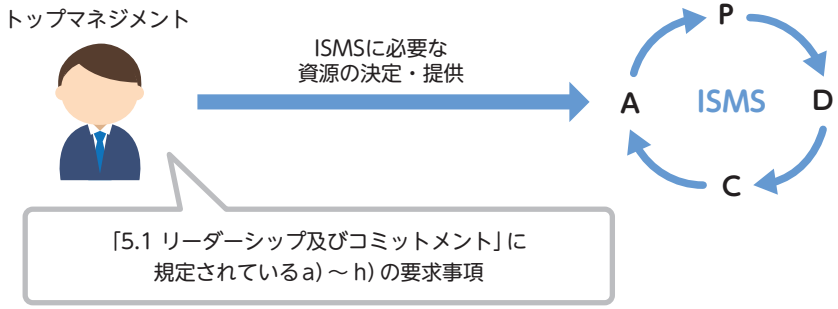
ISO/IEC 27001の「7.1 資源」は、ISMSを確立、実施、維持、そして継続的に改善するための資源を決定し、提供することを要求しています。

ISMSに必要な資源を決定・提供する

ISO/IEC 27001の「7.1 資源」では、ISMSに必要な資源を決定し、提供することが包括的に求められています。資源の具体的な例としては、「5.3 組織の役割、責任及び権限」で割り当てる責任と権限に整合した推進体制の確立や、運用に必要な情報処理機器や情報システム、物理的にセキュアな環境、それらを構築・維持するために必要となる資金など、一般的に**「人」「物」「金」「情報」**といった資源が考えられます。

この資源の提供については、「5.1 リーダーシップ及びコミットメント」で要求されるため、トップマネジメントがISMSの必要性を理解して、そのために必要な資源の決定と提供を行います。

■ トップマネジメントによる資源の提供



まとめ　ISMSを運用していくうえで必要な資源を決定して提供する

23 7.2 力量

ISO/IEC 27001の「7.2 力量」は、ISMSの各要員に求められる力量を明確にして、評価に応じて必要な力量を取得・維持する教育・訓練を実施することを要求しています。

要員に求められる力量を明確にする

ISO/IEC 27001の「7.2 力量」では、ISMSの適用範囲にある要員に求められる**力量（知識や技能など）**を明確にして、要員がどのような力量を持っているのかを評価し、必要な**教育・訓練を計画して実施**します。その後、必要な力量を取得・維持できたかどうかの**有効性を評価**して、それらの**記録を保持**することが求められています。

(1) 力量基準の決定【7.2 a)】

ISMSを運用するために、各要員が「5.3 組織の役割、責任及び権限」で割り当てられた役割と責任を果たすために必要な力量を備えておく必要があります。

■ 要員に求められる力量の例

要員	求められる力量
ISMS管理責任者 ISMS事務局	・ISMS運用（全社適用）に必要なISMS関連ルールの作成 ・ISMS運用支援業務（全体的業務）の実施 ・情報システムの導入、運用、管理、維持
部門長 ISMS部門担当者	・部門のISMS運用（リスクアセスメントなど）の実施 ・部門の情報セキュリティ対策の推進
従業員	・情報セキュリティ方針の重要性の理解 ・所属部門・担当業務で実施している情報セキュリティ対策の順守と重要性の認識 ・対策を実施しなかった場合に発生するリスクへの認識
ISMS内部監査員	・社内外における内部監査員教育の修了

28 9.1 監視、測定、分析及び評価

ISO/IEC 27001の「9.1 監視、測定、分析及び評価」は、ISMSの情報セキュリティパフォーマンスと有効性を評価することを要求しています。

情報セキュリティパフォーマンスとISMSの有効性を評価する

ISO/IEC 27001の「9.1 監視、測定、分析及び評価」では、情報セキュリティパフォーマンスとISMSの有効性を評価することが求められています。これらの監視・測定・分析・評価には、次の(1)～(6)を決定する必要があります。

(1) 監視・測定の対象【9.1 a)】

情報セキュリティパフォーマンスやISMSの有効性を評価するために、何を監視・測定するのかを決定します。たとえば、情報セキュリティ目的の達成状況や内部監査による管理策の順守状況の確認結果などです。

(2) 監視・測定・分析・評価の方法【9.1 b)】

監視・測定の対象を分析・評価するために必要な手順(方法)を決定します。手順には次の(3)～(6)が含まれます。

(3) 監視・測定の実施時期【9.1 c)】

月に1回など、監視・測定を実施する時期を決定します。

(4) 監視・測定の実施者【9.1 d)】

監視・測定の実施や結果(情報)を管理する部門を決定します。

(5) 監視・測定結果の分析と評価の時期【9.1 e)】

監視・測定した結果を分析・評価する方法と実施時期を決定します。

(6) 監視・測定結果の分析と評価の実施者【9.1 f)】

分析・評価された結果について、処置の必要性などを決定する責任者などを決定します。

■情報セキュリティパフォーマンスとISMSの有効性評価の例

評価方法＼評価項目	情報セキュリティ目的の達成状況	内部監査による管理策順守確認
a) 監視・測定の対象	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」に定める情報セキュリティ目的の達成結果	9.2「内部監査」に従い実施される内部監査結果(適合、不適合、観察事項などの内容・傾向など)
b) 監視・測定・分析・評価の方法	「情報セキュリティ目的管理規定」に定める	「内部監査規定」に定める
c) 監視・測定の実施時期	「年間情報セキュリティ目的実績表」に定める	「内部監査計画書」に定める
d) 監視・測定の実施者	報告責任部門 ISMS事務局	内部監査員 ISMS管理責任者
e) 監視・測定結果の分析と評価の時期	マネジメントレビュー	マネジメントレビュー
f) 監視・測定結果の分析と評価の実施者	トップマネジメント ISMS管理責任者	トップマネジメント

まとめ

- 監視・測定の対象を決め、評価・分析の手順を決める
- 監視・測定の実施時期と管理部門を決める
- 分析・評価の実施時期と判断する責任者を決める

附A.5.12 情報の分類

附A.5.12「情報の分類」では、情報の価値や重要性、無許可の開示や変更に対して、情報を分類することを要求しています。これにより、情報を取り扱う担当者に対して、どのような取り扱いをして保護するのかを簡潔に示すことができます。

情報の分類は、「公開」「社外秘」「秘」「極秘」など、**情報セキュリティリスクアセスメント（6.1.2）で定められている機密性の評価基準と整合し、情報の分類を定める**のが一般的で、情報の管理責任者が、情報の分類に対して責任を負います。

また、情報の分類には、一定期間を過ぎると公開情報となる「時限秘」があります。期間を経過して公開情報であっても編集権限を限定するなど完全性の高い情報であれば、その取り扱いについて情報セキュリティ管理策を実施する必要性があるため、機密性だけでなく、完全性や可用性を考慮した分類や基準にすることが望ましいです。

■ 情報の分類例

分類	分類基準
極秘	「秘」以上に取り扱いに注意を要するもの
秘	担当者及び秘密保持契約締結先にしか見せてはならない／使用させない
社外秘	従業員（グループ会社含む）にしか見せてはならない／使用させない
公開	一般に公開している情報

附A.5.13 情報のラベル付け

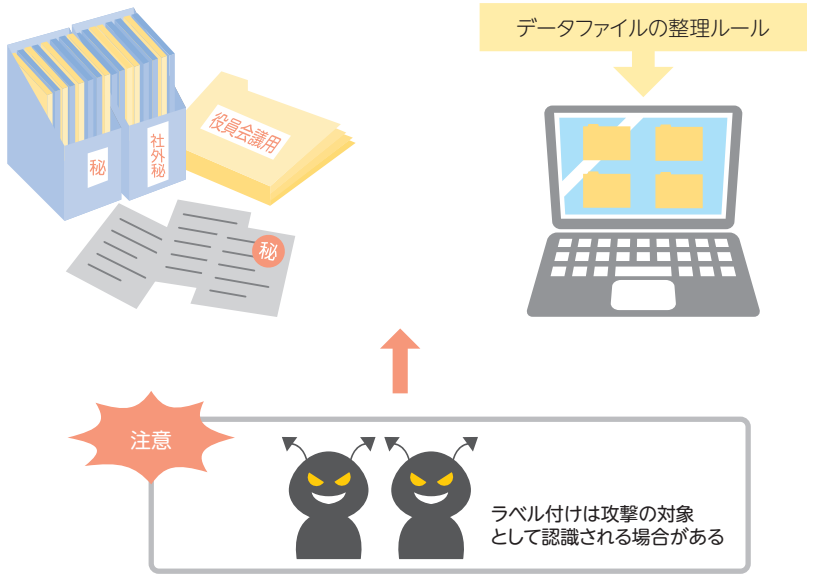
附A.5.13「情報のラベル付け」では、附A.5.12「情報の分類」で定めた分類体系に従って、紙やUSBメモリなどの媒体に物理的にラベルを付けたり、ファイルやデータベースなどの電子データにラベルを付けたりといった、ラベル付けの方法の決定と実施について要求しています。

具体的なラベル付けの方法としては、書類に「社外秘」や「秘」などを示す方法がありますが、「秘」についてのみファイルの背表紙に表示するなど、作業負荷を減らすように考慮する必要があります。

ラベル付けの目的は、取り扱う人がその情報をどのように取り扱うべきなのかをひと目でわかるようにするためなので、ファイル名で分類が想起できるのであれば、分類名の表示にこだわる必要はありません。従業員にとって情報の取り扱いがわかりやすいことと、書類や電子データの整理・整頓ができることが、ラベル付けの基礎となります。

なお、分類を示すことにより、悪意のある者にとって攻撃対象として認識されやすくなってしまう場合もあるので注意が必要です。

■ 情報のラベル付けのイメージ



34 附属書 A.7 物理的管理策

附A.7「物理的管理策」では、認可されていない物理的アクセスによる、組織の情報や情報処理施設の損傷・妨害を防止するための情報セキュリティ管理策について規定しています。

附A.7.1 物理的セキュリティ境界

附A.7.1「物理的セキュリティ境界」では、保護対象となる情報が存在している媒体や設備などについて、物理的なセキュリティ境界を設けるように要求しています。

物理的な保護は、情報や設備の周囲に、次の①～④の**物理的な障壁を1つ以上設ける**ことで達成でき、複数の障壁を利用すれば、保護のレベルも高くなる特徴があります。

①建物の敷地を取り囲む外周壁
②建物の外壁
③従業員が入場可能な入退管理されたエリア
④限られた従業員のみが入場可能な入退管理されたエリア

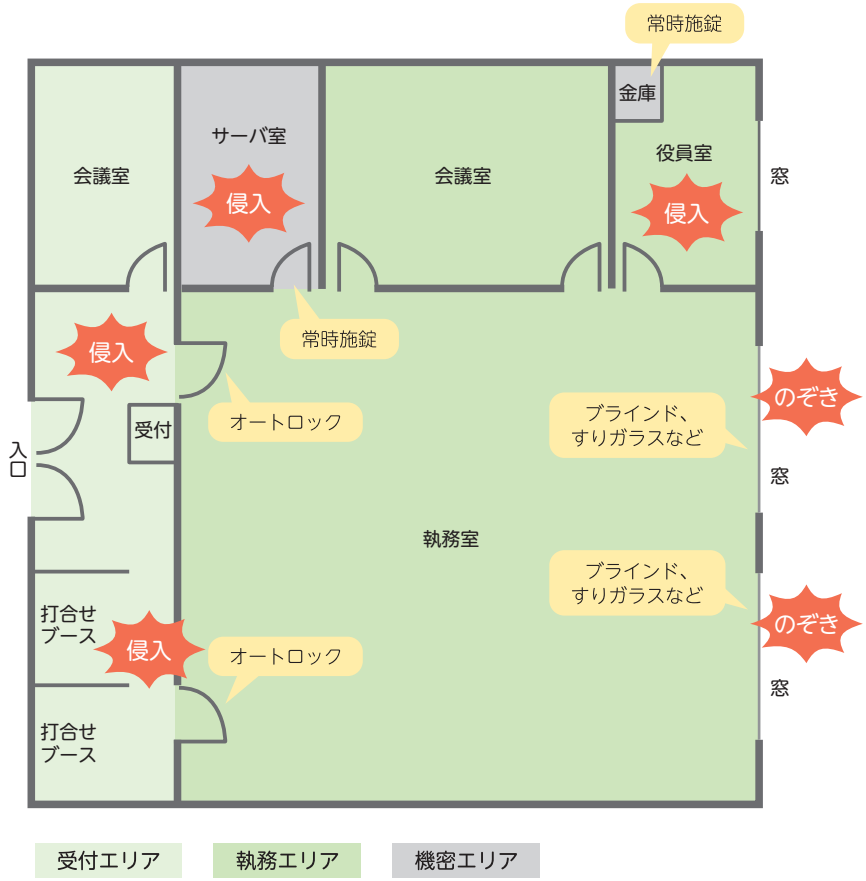
これらの物理的セキュリティ境界は、リスクアセスメントの結果に基づいて、情報が適切に保護されるように設計しますが、境界の設計や実装にはコストがかかる場合もあるため、組織の経済的状況も考慮する必要があります。

たとえば、ICカードや生体識別によって解錠するオートロック扉を導入しなくても、受付カウンター、パーテーションなどの仕切り、床への境界線表示、立て看板などを組み合わせる方法もあります。また、堅固さ以外に、サーバ室の壁を透明にして死角をなくすなど、監視のしやすさについても考慮する必要があります。

一般的な対策としては、認可されていない侵入やのぞき見などを考慮して、3つ程度の物理的なセキュリティ境界を設定します。

設定した領域は、入退管理ルールとして下図のように文書化し、組織内に周知します。ただし、重要な情報がどこにあるのかわかってしまう場合もあるため、どの程度の情報を記載するのかについては注意が必要です。

■物理的セキュリティ境界のイメージ



受付エリア：来訪者が従業員の同行なしに出入りできる領域
執務エリア：従業員及び従業員が同行した来訪者のみ出入りできる領域
機密エリア：特別に認可された従業員及び指定業者のみ出入りできる領域