1.2　本管理基準の位置付け

本管理基準は、組織体における情報セキュリティマネジメントの円滑で効果的な確立を目指して、マネジメントサイクル構築の出発点から具体的な管理策に至るまで、包括的な適用範囲を有する基準となっている。一方で、包括的な基準（参照基準）であるゆえに、組織体個別の事情への対応に最適化したものではない。また、情報セキュリティ監査を実施するにあたっては、判断の尺度をより具体的に規定する必要も生じ得る。そこで、本管理基準を適切に活用するためには、組織体が属する業界又は事業活動の特性等を考慮し、必要に応じて本管理基準の趣旨及び体系に則って、本管理基準に記載の管理策を取捨選択、追加、統合又は具体化することにより、該当する関係機関を取り巻く状況に適応させた個別管理策体系を策定する必要がある。

なお、本管理基準は、旧版と同様に、本管理基準と姉妹編をなす「情報セキュリティ監査基準」に従って監査を行う場合、原則として、監査人が監査上の判断の尺度として用いるべき基準となる。本管理基準は、日本におけるＩＳＭＳ認証制度である「ＩＳＭＳ適合性評価制度」において用いられる適合性評価の尺度にも整合するように配慮している。ただし、前述の通り包括的な基準である関係で、監査における判断の尺度として不十分な管理策（例：強力なパスワードを選択する）が想定され得るので、監査人は監査で用いる基準として十分と判断される程度に具体化させた管理策を個別管理基準としてとりまとめることが望ましい。

Ⅱ．構成

本管理基準は、ガバナンス基準、マネジメント基準及び管理策基準から構成される。

2.1　ガバナンス基準

「ガバナンス基準」は、組織体のガバナンスのうち、情報セキュリティガバナンスを確立するための目的及びプロセスについて示すものである。記載している事項は、情報セキュリティガバナンスに関する国際規格であるＩＳＯ／ＩＥＣ　27014：2020における規定事項を参考に策定している。

「ガバナンス基準」の内容は以下のとおりである。

3.1　情報セキュリティガバナンスの概要
3.2　情報セキュリティガバナンスの目的
3.3　情報セキュリティガバナンスのプロセス

2.2　マネジメント基準

「マネジメント基準」では、情報セキュリティマネジメントの計画、実行、点検、処置に必要な実施事項を定めている。それぞれの事項は、ＪＩＳ　Ｑ　27001：2023を基にして策定しているが、抽出に当たっては次の３点を考慮した。

・ＩＳＭＳ認証取得を目指している組織、独自に情報セキュリティマネジメントの確立を検討している組織、情報セキュリティ監査を実施する組織、情報セキュリティ監査を受ける組織など幅広い利用者を想定した記述とする。
・情報セキュリティマネジメントの計画、実行、点検、処置の各プロセスで行うべき事項を明確にする。
・「マネジメント基準」の章構成は、情報セキュリティマネジメントのプロセスを考慮し、ＪＩＳ　Ｑ　27001：2023における構成順序を一部変更する。その際、ＪＩＳ　Ｑ　27001：2023との対応が分かるように記載する。

「マネジメント基準」は、原則、全て実施すべき事項である。

「マネジメント基準」の内容は以下のとおりである（なお、[27001-X.X.X]は、ＪＩＳ　Ｑ　27001：2023において関連する条項（X.X.X）を示す。）。

4.1　マネジメント基準
4.2　記載内容について
4.3　凡例
4.4　情報セキュリティマネジメントの確立［27001-4.4］
4.4.1　組織の役割、責任及び権限［27001-5.3／5.1］
4.4.2　組織及びその状況の理解［27001-4.1］
4.4.3　利害関係者のニーズ及び期待の理解［27001-4.2］
4.4.4　適用範囲の決定［27001-4.3］
4.4.5　方針の確立［27001-5.2／6.2／5.1］
4.4.6　リスク及び機会に対処する活動［27001-6.1］
4.4.7　情報セキュリティリスクアセスメント［27001-6.1.2］
4.4.8　情報セキュリティリスク対応［27001-6.1.3］
4.5　情報セキュリティマネジメントの運用［27001-8］
4.5.1　資源管理［27001-7.1／5.1］
4.5.2　力量、認識［27001-7.2／7.3／5.1］
4.5.3　コミュニケーション［27001-7.4］
4.5.4　情報セキュリティマネジメントの運用の計画策定及び管理［27001-8.1］
4.5.5　情報セキュリティリスクアセスメントの実施［27001-8.2／8.3］
4.6　情報セキュリティマネジメントの監視及びレビュー［27001-5.1／8.2／9／10.2］
4.6.1　有効性の継続的改善［27001-10.2／8.2／9.2／9.3／5.1］
4.6.2　パフォーマンス評価［27001-9］
4.6.3　マネジメントレビュー［27001-9.3］
4.7　情報セキュリティマネジメントの維持及び改善［27001-10］
4.7.1　是正処置［27001-10.2］
4.8　文書化した情報の管理［27001-7.5］
4.8.1　文書化の指針［27001-7.5.1］
4.8.2　文書の作成・変更及び管理［27001-7.5.2／7.5.3］

2.3　管理策基準

「管理策基準」は、組織における情報セキュリティマネジメントの確立段階において、リスク対応方針に従って管理策を選択する際の選択肢を与えるものである。「管理策基準」のそれぞれの事項は、ＪＩＳ　Ｑ　27001：2023附属書Ａ「管理目的及び管理策」、ＪＩＳ　Ｑ　27002：2024をもとに、既存のＩＳＭＳ認証などとの整合性にも配慮しつつ、専門家の知見を加えて作成している。

ＪＩＳ　Ｑ　27002：2024においては、個別の管理策（Control）毎にその目的（Purpose）と管理策活用のための手引（Guidance）が規定されている。本管理基準では活用上の便宜の観点から、手引に示されている内容のうち、原則として「～ことが望ましい。」という表現で記述され、情報セキュリティマネジメントを実践する際に管理策の具体化に役立つと判断される項目を「詳細管理策」として付番し、それ以外の内容を「参考」として整理している。詳細管理策として規定した内容が管理策を実践する上で有効かどうかは組織体が属する業界又は事業活動の特性等によって異なり、すべての項目を取り入れる必要はない。詳細管理策に含まれる箇条書き形式の項目には、列挙されている項目をすべてに対処すべきもの、包含した上でさらに追加を考慮すべきもの、又は例示にとどまるものなどの種類があり、詳細管理策の内容によって意味が異なるため留意する必要がある。

また、本管理基準においては、個別管理策策定における便宜を図る観点から、ＪＩＳ　Ｑ　27002：2024における管理策の整理体系に加えて、以下の２種類の構造化を行っている。

①　管理策の構造化：ＪＩＳ　Ｑ　27002：2024では「５　組織的管理策」に37項目、「８　技術的管理策」に34項目の管理策がそれぞれ含まれるが、目的や対象の類似性を踏まえてこれらを最大７つのグループに分類し、5a，5b，…のように章番号にアルファベット小文字を付加することで識別可能とした。この結果、本管理基準では個別の管理策は「5a-5.1」のようにＪＩＳ　Ｑ　27002：2024の管理策番号の前にグループを示す記号を付加して表記されている。