⑵　情報セキュリティ管理基準（平成20年改正版）

その後、平成17年には、情報セキュリティマネジメントに関わる重要な国際規格として、ＩＳＯ／ＩＥＣ　27001：2005　ＩＳＭＳ要求事項（ＪＩＳ　Ｑ　27001：2006）及びＩＳＯ／ＩＥＣ　27002：2005（旧ＩＳＯ／ＩＥＣ　17799：2000）情報セキュリティマネジメントのための実践規範（ＪＩＳ　Ｑ　27002：2006）が策定された。

このようなＩＳＯ／ＩＥＣにおける国際規格化の動きを受け、平成20年に「情報セキュリティ管理基準」をより効果的に活用できるように、国際規格と整合を取る形で見直しを行った。見直しにおいては、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て、情報セキュリティマネジメントの基本的な枠組みと具体的な管理項目を規定することによって、組織体が効率的に情報セキュリティマネジメント体制の構築と、適切な管理策の整備と運用を行えるように規定した。

⑶　情報セキュリティ管理基準（平成28年改正版）

さらに、平成25年には、ＩＳＯ／ＩＥＣ　27001及び27002は、ＩＳＯ／ＩＥＣ　27001：2013（ＪＩＳ　Ｑ　27001：2014）及び、ＩＳＯ／ＩＥＣ　27002：2013（ＪＩＳ　Ｑ　27002：2014）に改訂され、マネジメントシステムの共通化、構成の変更、ＩＴ環境の変化等に伴う管理策の新規追加、削除、統合など、大幅な変更が加えられたところである。

「情報セキュリティ管理基準（平成28年改正版）」（以下「本管理基準」という。）は、このように大幅な変更が加えられたＪＩＳ　Ｑ　27001：2014及びＪＩＳ　Ｑ　27002：2014と整合を取り、旧版に引き続き、多くの利用者がＩＳＯに則った情報セキュリティマネジメント体制の構築と、適切な管理策の整備と運用を行えるよう、構成の変更も含め、情報セキュリティ管理基準（平成20年改正版）を大幅に改正し、実施すべき管理策の見直しも行ったものである。

Ⅱ．本管理基準の位置づけ

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。当然のことではあるが、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、本管理基準の項目等を取捨選択、追加又は統合することにより、該当する関係機関において独自の管理基準を策定し活用することが望ましい。

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」（平成15年経済産業省告示第114号）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。また、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。

Ⅲ．構成

本管理基準は、マネジメント基準と管理策基準から構成される。

「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　27001：2014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　27001：2014における構成順序を一部変更する。その際、ＪＩＳ　Ｑ　27001：2014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　27001：2014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［27001-10.1］
4.8　文書化した情報の管理［27001-7.5］
4.8.1　文書化［27001-7.5.1］
4.8.2　文書管理［27001-7.5.2／7.5.3］

「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　27001：2014附属書Ａ「管理目的及び管理策」、ＪＩＳ　Ｑ　27002：2014をもとに専門家の知見を加えて作成しており、管理目的と管理策で構成される。また、既存のＩＳＭＳ認証などとの整合性にも配慮している。

「管理策基準」の内容は次のとおりである。

5　情報セキュリティのための方針群
5.1　情報セキュリティのための経営陣の方向性
6　情報セキュリティのための組織
6.1　内部組織
6.2　モバイル機器及びテレワーキング
7　人的資源のセキュリティ
7.1　雇用前
7.2　雇用期間中
7.3　雇用の終了又は変更
8　資産の管理
8.1　資産に対する責任
8.2　情報分類
8.3　媒体の取扱い