4.7.1.5　組織は、必要な場合には、情報セキュリティマネジメントの変更を行う。［27001-10.2ｅ)］

4.7.1.6　組織は、是正処置は、検出された不適合のもつ影響に応じたものとする。［27001-10.2］

4.7.1.7　組織は、是正処置の証跡として、以下の文書化した情報を利用可能な状態にする。［27001-10.2ｆ）／10.2ｇ)］

・不適合の性質及びそれに対して講じたあらゆる処置
・是正処置の結果

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］

4.8.1.1　組織は、情報セキュリティマネジメントが必要とする以下の情報を文書化する。［27001-7.5.1］

・情報セキュリティ方針
・情報セキュリティ目的
・情報セキュリティリスクアセスメントのプロセス
・情報セキュリティリスク対応のプロセス
・情報セキュリティリスクアセスメントの結果
・情報セキュリティリスク対応計画
・パフォーマンス測定の結果

これらの内容についてはどの文書に記載されていてもかまわないが、その内容を知る必要がある担当者には必ず伝わるように構成するとともに、知る必要性のない者が閲覧できないことを確実にする。

4.8.2　文書の作成・変更及び管理［27001-7.5.2／7.5.3］

4.8.2.1　組織は、以下を行うことによって、文書化した情報を作成及び更新する。［27001-7.5.2］

・適切な識別情報の記述（例えば、表題、日付、作成者、参照番号）
・適切な形式（例えば、言語、ソフトウェアの版、図表）及び媒体（例えば、紙、電子媒体）の選択
・適切性及び妥当性に関する、適切なレビュー及び承認
・文書化した情報のライフサイクルの定義や、それに応じた処理ができるような手順の策定
・文書を発行する前における、適正性のレビュー及び承認
・必要に応じた、文書の更新及び再承認
・廃止文書の誤使用の防止
・廃止文書を何らかの目的で保持する場合における、廃止文書であることが分かる適切な識別情報の記述

また、これらのすべての活動が文書管理に反映されているか、またその活動が業務に大きな障害を与えていないかなどを考慮し、適切な文書管理手順を策定する。

4.8.2.2　組織は、以下のことを確実にするために、情報セキュリティマネジメントで要求された、文書化した情報を管理する。[27001-7.5.3]

・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こと。
・文書化した情報が十分に保護されていること（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）。
・文書化した情報の配付、アクセス、検索及び利用
・文書化した情報の読みやすさが保たれることを含む、保管及び保存
・文書化した情報の変更の管理（例えば、版の管理）
・文書化した情報の保持及び廃棄

また、情報セキュリティマネジメントの計画策定及び運用のために組織が必要と決定した文書は、外部から入手したものであっても、必要に応じて、識別し、管理する。

Ⅴ．管理策基準

管理策基準に記載される管理策［Xx-X.X］は、情報セキュリティマネジメントの単位毎に、リスク対応のための方針に基づき適切に選択すべき事項である。詳細管理策［Xx-X.X.X］については、管理策を実装するために組織・環境・技術等に応じて必要とする事項を選択するものである。

5　組織的管理策

5a　組織的管理

5a-5.1　情報セキュリティのための方針群

管理策：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。

目的：　事業、法令、規制及び契約上の要求事項に従って、情報セキュリティに対する管理層の指示及び支援の継続的な適合性、適切性、及び有効性を確実にするため。

詳細管理策

5a-5.1.1	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。
（5a-5.1.1参考）	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。
5a-5.1.2	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。 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
5a-5.1.3	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。 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
5a-5.1.4	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。
5a-5.1.5	方針群のより低いレベルでは、情報セキュリティ方針は､情報セキュリティ管理策の実施を更に義務付けるために、必要に応じてトピック固有の方針によって支持する。