b）不適合は以下の活動によって検出される。
・定期的な情報セキュリティリスクアセスメント
・定期的な情報セキュリティ内部監査
・定期的なマネジメントレビュー
・不適合を手順どおりに検出するために、以下について文書化する。
－情報セキュリティマネジメントに対する不適合の特定
－情報セキュリティマネジメントに対する不適合の原因の決定
なお、単一の活動だけでは判断できない場合もあるので、複合的な結果の考察から不適合を検出する。

4.7.1.2　組織は、不適合が再発又は他のところで発生しないようにするため、その不適合の原因を除去するための処置をとる必要性を評価する。[27001-10.1b)]
必要性を評価する際は、以下を実施する。
・その不適合のレビュー
・その不適合の原因の明確化
・類似の不適合の有無、又はそれが発生する可能性の明確化

4.7.1.3　組織は、必要な処置を実施する。[27001-10.1c)]

4.7.1.4　組織は、とった全ての是正処置の有効性をレビューする。[27001-10.1d)]

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。[27001-10.1e)]

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。[27001-10.1]

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保持する。[27001-10.1f)／10.1g)]
・不適合の性質及びとった処置
・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、以下を行うことによって、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。
・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、不適切な使用及び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、特定し、管理する。

Ⅴ．管理策基準
管理策基準に記載される管理策［X．X．X］は、情報セキュリティリスクアセスメントの結果に基づき、適切に選択すべき事項である。詳細管理策［X．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　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
目的：情報セキュリティのための経営陣の方向性及び支持を、事業上の要求事項並びに関連する法令及び規制に従って提示するため

5.1.1　情報セキュリティのための方針群は、これを定義し、管理層が承認し、発行し、従業員及び関連する外部関係者に通知する。

5.1.1.1　組織は、経営陣によって承認され、組織の情報セキュリティ目的の管理に対する取組みを示すものとして、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。

5.1.1.2　情報セキュリティ方針は、事業戦略によって生じる要求事項を取り扱う。

5.1.1.3　情報セキュリティ方針は、規制、法令及び契約によって生じる要求事項を取り扱う。

5.1.1.4　情報セキュリティ方針は、現在の及び予想される情報セキュリティの脅威環境によって生じる要求事項を取り扱う。

5.1.1.5　情報セキュリティ方針には、情報セキュリティに関する全ての活動の指針となる、情報セキュリティの定義、目的及び原則に関する記載を含める。

5.1.1.6　情報セキュリティ方針には、情報セキュリティマネジメントに関する一般的な責任及び特定の責任の、定められた役割への割当てに関する記載を含める。

5.1.1.7　情報セキュリティ方針には、逸脱及び例外を取り扱うプロセスに関する記載を含める。

5.1.1.8　方針群のより低いレベルでは、情報セキュリティ方針は、トピックに応じて定める個別方針によって支持されるようにする。

5.1.1.9　個別方針のトピックとして、アクセス制御を含める。

5.1.1.10　個別方針のトピックとして、情報分類（及び取扱い）を含める。