5.1.1.11　個別方針のトピックとして、物理的及び環境的セキュリティを含める。
5.1.1.12　個別方針のトピックとして、エンドユーザ関連のトピック（資産利用の許容範囲、クリアデスク・クリアスクリーン、情報転送、モバイル機器及びテレワーキング、ソフトウェアのインストール及び使用の制限）を含める。
5.1.1.13　個別方針のトピックとして、バックアップを含める。
5.1.1.14　個別方針のトピックとして、情報の転送を含める。
5.1.1.15　個別方針のトピックとして、マルウェアからの保護を含める。
5.1.1.16　個別方針のトピックとして、技術的ぜい弱性の管理を含める。
5.1.1.17　個別方針のトピックとして、暗号による管理策を含める。
5.1.1.18　個別方針のトピックとして、通信のセキュリティを含める。
5.1.1.19　個別方針のトピックとして、プライバシー及び個人を特定できる情報（以下「ＰＩＩ」という。）の保護を含める。
5.1.1.20　個別方針のトピックとして、供給者関係を含める。
5.1.1.21　トピック別の個別方針は、従業員及び関係する外部関係者にとって適切で、アクセス可能かつ理解可能な形式で伝達する（例えば、情報セキュリティの意識向上、教育及び訓練のプログラムに従う。）。
5.1.2　情報セキュリティのための方針群は、あらかじめ定めた間隔で、又は重大な変化が発生した場合に、それが引き続き適切、妥当かつ有効であることを確実にするためにレビューする。
5.1.2.1　各々の情報セキュリティのための方針には、その方針の作成、レビュー及び評価についての管理責任を与えられた責任者を置く。
5.1.2.2　情報セキュリティのための方針群のレビューには、組織環境、業務環境、法的状況又は技術環境の変化に応じた、組織の情報セキュリティのための方針群及び情報セキュリティの管理への取組みに関する、改善の機会の評価を含める。
5.1.2.3　情報セキュリティのための方針群のレビューでは、マネジメントレビューの結果を考慮し、反映する。
5.1.2.4　改訂された情報セキュリティのための方針は、管理層から承認を得る。

6　情報セキュリティのための組織

6.1　内部組織

目的：組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため

6.1.1　全ての情報セキュリティの責任を定め、割り当てる。
6.1.1.1　情報セキュリティの責任の割当ては、情報セキュリティのための方針群によって行う。
6.1.1.2　個々の資産の保護に対する責任及び特定の情報セキュリティプロセスの実施に対する責任を定める。
6.1.1.3　情報セキュリティのリスクマネジメント活動に関する責任、特に残留リスクの受容に関する責任を定める。
6.1.1.4　必要な場合には、この責任を、個別のサイト及び情報処理施設に対する、より詳細な手引で補完する。
6.1.1.5　資産の保護及び特定の情報セキュリティプロセスの実行に関する局所的（local）な責任を定める。
6.1.1.6　情報セキュリティの責任を割り当てられた個人は、情報セキュリティに関する職務を他者に委任してもよいが、責任は依然としてその個人にあり、委任した職務がいずれも正しく実施されていることを、その個人が確認する。
6.1.1.7　個人が責任をもつ領域を規定する。
6.1.1.8　個人が責任をもつ領域を規定するために、資産及び情報セキュリティプロセスの識別及び規定を実施する。
6.1.1.9　個人が責任をもつ領域を規定するために、各資産又は情報セキュリティプロセスに対する責任主体の指定、及びその責任の詳細の文書化を実施する。
6.1.1.10　個人が責任をもつ領域を規定するために、承認レベルの規定及び文書化を実施する。
6.1.1.11　個人が責任をもつ領域を規定するために、情報セキュリティ分野における責任を果たせるよう、任命された個人が当該分野の力量をもつこと、及び最新の状況を把握するための機会が与えられるようにする。
6.1.1.12　個人が責任をもつ領域を規定するために、供給者関係における情報セキュリティの側面の調整及び管理に関する事項の特定及び文書化を実施する。
6.1.2　相反する職務及び責任範囲は、組織の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために、分離する。
6.1.2.1　認可されていない状態又は検知されない状態で、一人で資産に対してアクセス、修正又は使用ができないように注意する。
6.1.2.2　ある作業を始めることと、その作業を認可することとを分離する。
6.1.2.3　管理策は、共謀のおそれを考慮して設計する。
6.1.2.4　職務の分離が困難である場合には、他の管理策（例えば、活動の監視、監査証跡、管理層による監督）を実施する。
6.1.3　関係当局との適切な連絡体制を維持する。
6.1.3.1　組織は、いつ、誰が関係当局（例えば、法の執行機関、規制当局、監督官庁）に連絡するかの手順を備える。
6.1.3.2　法が破られたと疑われる場合に、特定した情報セキュリティインシデントをいかにして時機を失せずに報告するかの手順を備える。
6.1.4　情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持する。
6.1.4.1　最適な慣行に関する認識を改善し、関係するセキュリティ情報を最新に保つ手段として、情報セキュリティに関する研究会又は会議へ参加する。
6.1.4.2　情報セキュリティ環境の理解が最新かつ完全であることを確実にする手段として、情報セキュリティに関する研究会又は会議へ参加する。
6.1.4.3　攻撃及びぜい弱性に関連する早期警戒警報、勧告及びパッチを受理する手段として、情報セキュリティに関する研究会又は会議へ参加する。
6.1.4.4　専門家から情報セキュリティの助言を得る手段として、情報セキュリティに関する研究会又は会議へ参加する。
6.1.4.5　新しい技術、製品、脅威又はぜい弱性に関する情報を共用し、交換する手段として、情報セキュリティに関する研究会又は会議へ参加する。
6.1.4.6　情報セキュリティインシデントを扱う場合の、適切な連絡窓口を提供する手段として、情報セキュリティに関する研究会又は会議へ参加する。
6.1.5　プロジェクトの種類にかかわらず、プロジェクトマネジメントにおいては、情報セキュリティに取り組む。
6.1.5.1　情報セキュリティリスクがプロジェクトの中で特定及び対処されることを確実にするために、情報セキュリティを組織のプロジェクトマネジメント手法に組み入れ、プロジェクトの特性にかかわらず、一般にあらゆるプロジェクト（例えば、中核事業プロセス、ＩＴ、施設管理、その他のサポートプロセスのためのプロジェクト）に適用されるようにする。
6.1.5.2　プロジェクトマネジメント手法においては、情報セキュリティ目的をプロジェクトの目的に含める。