4.4.5　方針の確立［27001-5.2／6.2／5.1］

4.4.5.1　トップマネジメントは、以下を満たす組織の情報セキュリティ方針を確立する。［27001-5.2］

・組織の目的に対して適切であること。
・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
・情報セキュリティに関連して適用する要求事項を満たすことへのコミットメントを含むこと。
・情報セキュリティマネジメントの継続的改善へのコミットメントを含むこと。

また、情報セキュリティ方針は情報セキュリティマネジメントにおける判断の基盤となる考え方を記載したものであり、組織の戦略に従って慎重に作成する。

4.4.5.2　組織は、情報セキュリティ目的及びそれを達成するための計画を策定する。［27001-6.2］

a）情報セキュリティ目的は、以下を満たすこととする。
・情報セキュリティ方針と整合していること。
・（実行可能な場合）測定可能であること。
・適用される情報セキュリティ要求事項、並びにリスクアセスメント及びリスク対応の結果を考慮に入れること。

b）情報セキュリティ目的は、関係者に伝達し、必要に応じて更新するとともに、情報セキュリティ目的を達成するための計画においては、以下を決定する。
・実施事項
・必要な資源
・責任者
・達成期限
・結果の評価方法

4.4.5.3　トップマネジメントは、以下によって、情報セキュリティマネジメントに関するリーダーシップ及びコミットメントを発揮する。[27001-5.1a)]

・情報セキュリティ方針及び情報セキュリティ目的を確立すること。
・情報セキュリティ方針及び情報セキュリティ目的は組織の戦略的な方向性と相矛盾しないこと。

また、情報セキュリティ方針は組織に伝えられるように文書化され、しかるべき方法で利害関係者が入手できるようにするとともに、トップマネジメントが情報セキュリティ方針にコミットした証拠を、以下のような記録をもって示す。

・文書化された情報セキュリティ方針への署名
・情報セキュリティ方針が議論された会議の議事録

これらはトップマネジメントの責任を明確にするために実施する。

4.4.6　リスク及び機会に対処する活動［27001-6.1］

4.4.6.1　リスク及び機会を決定する。[27001-6.1.1]

a）組織は、外部及び内部の課題、利害関係者の情報セキュリティに関連する要求事項を考慮し、以下のために対処する必要があるリスク及び機会を決定する。
・情報セキュリティマネジメントが、組織が意図した成果を達成する。
・望ましくない影響を防止又は低減する。
・継続的改善を達成する。

当該決定の際、組織は、以下を計画する。
・決定したリスク及び機会に対処する活動
・リスク及び機会に対処する活動の情報セキュリティマネジメントプロセスへの統合及び実施方法
・リスク及び機会に対処する活動の有効性の評価方法

b）リスク及び機会に対処する活動の記録として、具体的な対処計画（実施時期、実施内容、実施者、実施場所、実施に必要な資源などを規定した計画）を作成していることを確認するとともに、当該計画を作成する際、各対処計画が、情報セキュリティマネジメントプロセスの一部として実施されるよう、考慮するとともに、当該対処の有効性を評価する方法（実施状況や実施したことによる効果を評価する方法）を作成していることも確認する。

4.4.7　情報セキュリティリスクアセスメント［27001-6.1.2］

4.4.7.1　組織は、以下によって、情報セキュリティリスクアセスメントのプロセスを定め、適用する。[27001-6.1.2a）／6.1.2b)]

a）以下を含む情報セキュリティのリスク基準を確立し、維持する。
・リスク受容基準
・情報セキュリティリスクアセスメントを実施するための基準

b）リスク受容基準に、以下を反映するよう、考慮する。
・組織の価値観
・目的
・資源

c）リスク受容基準を策定する際には、以下の点を考慮する。
・原因及び発生し得る結果の特質及び種類、並びにこれらの測定方法
・発生頻度
・発生頻度、結果を考える時間枠
・リスクレベルの決定方法
・利害関係者の見解
・リスク基準は、法律及び規制の要求事項、並びに組織が合意するその他の要求事項によって、組織に課せられるもの又は策定されるものもあること。

d）情報セキュリティアセスメントを繰り返し実施した際に、以下の結果を生み出すこと。
・情報セキュリティリスクアセスメントの結果に、一貫性及び妥当性があること。
・情報セキュリティリスクアセスメントの結果が比較可能であること。

なお、情報セキュリティマネジメントにおけるリスクアセスメント手法には、定番といえるものがなく、それぞれの組織に適合したものを選択している場合が多いことから、必要に応じてツールを利用するなどが必要になる。

4.4.7.2　組織は、以下によって、情報セキュリティリスクを特定する。[27001-6.1.2c)]

a）情報セキュリティリスクアセスメントのプロセスを適用し、情報の機密性、完全性及び可用性の喪失に伴うリスクを特定する。

b）リスクを特定する過程において、リスク所有者を特定する。

c）リスクを特定する際には、以下について考慮する。
・リスク源が組織の管理下にあるか否かに関わらず、リスク源又はリスクの原因が明らかでないリスクも特定の対象にすること。
・波及効果及び累積効果を含めた、特定の結果の連鎖を注意深く検討すること。
・何が起こり得るのかの特定に加えて、考えられる原因及びどのような結果が引き起こされることがあるのかを示すシナリオ
・全ての重大な原因及び結果
・以下を特定すること。
—リスク源
—影響を受ける領域、事象
—原因及び起こり得る結果

この段階で特定されなかったリスクは、今後の分析の対象から外されてしまうため、ある機会を追及しなかったことに伴うリスクも含め、リスクの包括的な一覧を作成する。