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］

4.5.4.1　組織は、情報セキュリティ要求事項を満たすため、リスク及び機会に対処する活動を実施するために必要なプロセスを計画し、実施し、かつ管理する。[27001-8.1]

4.5.4.2　組織は、情報セキュリティ目的を達成するための計画を実施する。[27001-8.1]

4.5.4.3　組織は、計画通りに実施されたことを確信するために、文書化した情報を、保持する。[27001-8.1]

文書化した情報に、以下の情報が集められているかどうかを確認する。

・管理策の実施状況
・管理策の有効性
・管理策を取り巻く環境の変化

また、これらの情報を把握し判断する体制を構築する。

4.5.4.4　組織は、計画した変更を管理し、意図しない変更によって生じた結果をレビューし、必要に応じて、有害な影響を軽減する処置をとる。[27001-8.1]

4.5.4.5　組織は、外部委託するプロセスを決定し、かつ、管理する。[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］

4.5.5.1　組織は、以下のいずれかの場合において、情報セキュリティリスクアセスメントを実施する。[27001-8.2]

・あらかじめ定めた間隔
・重大な変更が提案された場合
・重大な変化が生じた場合

4.5.5.2　組織は、情報セキュリティリスク対応計画を実施する。[27001-8.3]

情報セキュリティリスク対応計画の実施においては、明確にされた個々の責任について全うしていることを確認するための方策を講じる。

4.5.5.3　トップマネジメントは、情報セキュリティリスク対応計画のために十分な経営資源を提供する。

情報セキュリティリスク対応計画には相応の経営資源が必要になるところ、以下の点について考慮する。

・管理策の導入及び運用にかかる費用、人員、作業工数、技術
・セキュリティインシデント発生時の一時対応にかかる費用
・その他のリスク対応にかかる費用

運用においては管理策の効果測定などを実施するために必要な経営資源について考察し、予算化する。

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］

4.6.1.1　組織は、以下を実施し、情報セキュリティマネジメントの適切性、妥当性及び有効性を継続的に改善する。[27001-10.2／8.2／9.2／9.3]

・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
・トップマネジメントによる定期的なマネジメントレビュー

継続的改善においては、これまで実施してきた管理策だけはなく、環境の変化に伴う新たな脅威やぜい弱性についても不適合を検出し処置する。

4.6.1.2　トップマネジメントは、継続的改善を促進する。[27001-5.1ｇ)]

4.6.1.1.を実施するための、役割、責任及び権限を割り当て、実施するよう関係者に伝達する。

4.6.2　パフォーマンス評価［27001-9］

4.6.2.1　組織は、情報セキュリティパフォーマンス及び情報セキュリティマネジメントの有効性を評価し、以下を決定する。[27001-9.1]

・必要とされる監視及び測定の対象(情報セキュリティプロセス及び管理策を含む。)
・妥当な結果を確実にするための、監視、測定、分析及び評価の方法（比較可能で再現可能な結果を生み出す方法とする。）
・監視及び測定の実施時期
・監視及び測定の実施者
・監視及び測定の結果の、分析及び評価の時期
・監視及び測定の結果の、分析及び評価の実施者

4.6.2.2　組織は、あらかじめ定めた間隔で内部監査を実施する。[27001-9.2ａ）／9.2ｂ)]

ａ）内部監査を実施する際は、以下を確認する。

・以下に適合していること。
　―情報セキュリティマネジメントに関して、組織自体が規定した要求事項
　―本マネジメント基準の要求事項
・情報セキュリティマネジメントが有効に実施され、維持されていること。

ｂ）内部監査は、管理策の有効性を総合的に確認するために定期的に実施し、計画及び結果について以下の文書で管理する。

・内部監査基本計画
・内部監査実施計画
・内部監査報告書

基本計画書では対象範囲、目的、管理体制及び期間又は期日について、実施計画では実施時期や実施場所、実施担当者及びその割当て及び詳細な監査の手法についてあらかじめ決める。予定通り実施されたことを証明するためにも、実施報告書を作成する。

ｃ）適合性の監査においては、以下の項目を対象に含む。

・関連する法令又は規制の要求事項
・情報セキュリティリスクアセスメントなどによって特定された情報セキュリティ要求事項

ｄ）情報セキュリティマネジメントが有効に実施され、維持されていることの監査においては、以下の項目を対象に含む。

・管理策の有効性及び維持
・管理策が期待通りに実施されていること。

4.6.2.3　組織は、頻度、方法、責任及び計画に関する要求事項及び報告を含む、監査プログラムの計画、確立、実施及び維持する。[27001-9.2ｃ)]

監査プログラムでは、関連するプロセスの重要性及び前回までの監査の結果を考慮する。

監査は一度にすべての適用範囲について実施するだけではなく、範囲の一部のみを対象とする場合もあり、毎回の監査の目的を明確にし、適切な監査計画を実施することが重要であることから、監査プログラムの作成においては、以下の点を考慮する。

・監査の目的と重点目標
・対象となる監査プロセスの状況と重要性
・対象となる領域の状況と重要性
・前回までの監査結果