4.4.7.3　組織は、以下によって、情報セキュリティリスクを分析する。[27001-6.1.2ｄ)]

ａ）以下の手順によりリスク分析を行う。

・特定されたリスクが実際に生じた場合に起こり得る結果の分析を行う。
・特定されたリスクの発生頻度の分析を行う。
・リスクレベルを決定する。
・特定した脅威やぜい弱性を基に、以下の点を考慮する。
　ーセキュリティインシデントが発生した場合の事業影響度
　ーセキュリティインシデントの発生頻度
　ー管理策が適用されている場合はその効果

ｂ）リスク分析の際には、以下の点についても考慮する。

・リスクの原因及びリスク源
・リスクの好ましい結果及び好ましくない結果
・リスクの発生頻度
・リスクの結果及び発生頻度に影響を与える要素

なお、リスク分析は、状況に応じて、定性的、半定量的、定量的、又はそれらを組み合わせた手法で行うことが可能である。

4.4.7.4　組織は、以下によって、情報セキュリティリスクを評価する。[27001-6.1.2ｅ)]

・リスク分析の結果、決定されたリスクレベルとリスク基準との比較をする。
・リスク対応のための優先順位付けを行う。
・リスク評価の結果は今後の改善に利用するため保管する。

なお、リスク対応の優先順位を決定する際には、より広い範囲の状況を考慮し、他者が負うリスクの受容レベルについて考慮するとともに、法律、規制、その他の要求事項についても考慮する。

4.4.8　情報セキュリティリスク対応［27001-6.1.3］

4.4.8.1　組織は、情報セキュリティアセスメントの結果を考慮して、適切な情報セキュリティリスク対応の選択肢を選定する。[27001-6.1.3ａ)]

情報セキュリティリスク対応の選択肢には、以下が含まれる。

・リスクを生じさせる活動を開始又は継続しないと決定することによるリスクの回避
・ある機会を目的としたリスクの引受け又はリスクの負担
・リスク源の除去
・発生頻度の変更
・結果の変更
・（契約及びリスクファイナンスを含む）他者とのリスクの共有
・情報に基づいた意思決定によるリスクの保有

さらに、リスク対応の評価や改善に役立てるため、どの選択肢を選んだ場合も、その理由を明確にし、記載する。

4.4.8.2　組織は、選定した情報セキュリティリスク対応の実施に必要な全ての管理策を決定する。[27001-6.1.3ｂ)]

リスク対応のための方針を決めた上で、管理策の目的（管理目的）及び管理策について検討する。以下を考慮しつつ、対応による効果と対応に必要な費用及び労力のバランスを取り、適切な情報セキュリティ対応の選択肢を選定する。

・リスクの受容可能レベル
・関連する法令
・規制や契約上の要求事項
・その他の社会的責任

なお、具体的な管理策の選定においては、管理目的に対応した「管理策基準」から適切なものを選択するが、「管理策基準」はすべてを網羅しているわけではないので、組織の事業や業務などによってその他の管理策を追加してもよい。

4.4.8.3　組織は、管理策が見落とされていないことを検証する。[27001-6.1.3ｃ)]

必要な管理策の見落としがないか、管理策基準を参照するが、管理策基準に示す管理目的及び管理策以外の管理目的及び管理策が必要になった場合、他の管理目的及び管理策を追加することができる。

4.4.8.4　組織は、情報セキュリティリスク対応計画を策定する。[27001-6.1.3ｅ)]

ａ）情報セキュリティリスク対応計画には、以下を含む。

・期待される効果を含む、対応選択肢選定の理由
・情報セキュリティリスク対応計画の承認者及び対応計画の実施責任者
・対応内容
・必要な資源
・費用・労力、制約
・後日の報告、監視に必要な要求事項
・対応時期及び日程

ｂ）責任及び権限について

情報セキュリティマネジメントにおいては最終的な承認をトップマネジメントが行っていることがほとんどであり、責任がトップマネジメントに集中している。

一方で、情報セキュリティリスクアセスメント及びリスク対応については、責任及び権限を持つリスク所有者が、責任及び権限を持つ。

リスク所有者は、トップマネジメント、又はトップマネジメントから任命され、責任及び権限が委譲された者であることが多いことから、情報セキュリティマネジメントにおいて、トップマネジメント及びリスク所有者が、どのような責任を持つかについて明確にする。

4.4.8.5　組織は、リスク所有者から、情報セキュリティリスク対応計画について承認を得、かつ、リスク所有者に、残留している情報セキュリティリスクを受け入れてもらう。[27001-6.1.3ｆ)]

すべてのリスクについて管理目的や管理策を選択した時点で、残留リスクについて明確にし、今後の対応計画を作成する。計画の作成においては以下の点について考慮する。

・技術的に対応可能になる時期
・コスト的に対応可能になる時期

残留リスクについては、定期的に見直しを行い、必要に応じて、対応の対象とするとともに、リスク対応後の残留リスクについては、リスク所有者のほか、経営時やその他の利害関係者に認識させることを考慮する。

また、リスク所有者の責任を明確にするために、承認された会議の議事録を正しく保管する。

4.5　情報セキュリティマネジメントの運用［27001-8］

4.5.1　資源管理［27001-7.1／5.1］

4.5.1.1　組織は、情報セキュリティマネジメントの確立、実施、維持及び継続的改善に必要な資源を決定し、提供する。[27001-7.1]

管理目的を満たすためには、継続的に管理策を実施するとともに、人員の増加、システムの増加などの環境の変化に対応するために、適切な時期に適切に提供できるよう、経営資源を確保する。