3.3.5　コミュニケーション

3.3.5.1　ガバナンス主体は、以下を実行する。

・外部の利害関係者を対象とする、組織体がその活動及び優先度の実態に見合った情報セキュリティのレベルを実践していることの報告
・規制上の義務、利害関係者の期待及び情報セキュリティに関する組織体の要求事項の特定及び優先度の決定
・注意及び決定が必要な問題についての、各情報セキュリティマネジメントシステムの責任者への助言
・関連する利害関係者に向けた、情報セキュリティの優先度決定を支援するために採用すべき詳細な対象に関する指導
・情報セキュリティに積極的な文化の奨励
・スタッフ及びその他の人々を対象とする、情報セキュリティマネジメントシステムの適用範囲での責任を果たすための訓練とコミュニケーション

Ⅳ. マネジメント基準

4.1　マネジメント基準

マネジメント基準は、ＪＩＳ　Ｑ　27001：2023を基に、情報セキュリティについて組織を指揮統制するために調整された活動である情報セキュリティマネジメントを確立、導入、運用、監視、維持及び改善するための基準を定める。マネジメント基準は、原則としてすべて実施しなければならないものである。

4.2　記載内容について

ＪＩＳ　Ｑ　27001：2023を基に、情報セキュリティマネジメントの計画、実行、点検、処置等の活動に必要な事項を定める。

4.3　凡例

4.4章以降は、以下の構成をとる。

4.4　情報セキュリティマネジメントの確立［27001-4.4］
4.4.1　組織の役割、責任及び権限［27001-5.3／5.1］
4.4.1.1　トップマネジメントは、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。［27001-5.1ｂ）／5.1ｅ）／5.1ｆ）］
・組織のプロセスへ、その組織が必要とする情報セキュリティマネジメント要求事項を統合する。
：
［27001-X.X.X］は、ＪＩＳ　Ｑ　27001：2023において関連する条項（X.X.X）を示す。

4.4　情報セキュリティマネジメントの確立［27001-4.4］

情報セキュリティマネジメントを確立するために、その基盤となる適用範囲を決定し、方針を確立する。これらをもとに、情報セキュリティリスクアセスメントを実施し、その対応を計画し実施する。それにより、必要なプロセス及びそれらの相互作用を含む、組織が有効な情報セキュリティマネジメントを実施するための基盤作りを行う。

4.4.1　組織の役割、責任及び権限［27001-5.3／5.1］

4.4.1.1　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。［27001-5.1ｂ）／5.1ｅ）／5.1ｆ）］

・組織のプロセスへ、その組織が必要とする情報セキュリティマネジメント要求事項を統合する。
・情報セキュリティマネジメントがその意図した成果を達成することを確実にする。
・情報セキュリティマネジメントの有効性に寄与するよう人々を指揮し、支援する。

また、トップマネジメントがリーダーシップ及びコミットメントを発揮していることを以下により確認する。

・経営会議等の議事録に、トップマネジメントの情報セキュリティマネジメントに関する意思、判断、指示等が記録されていること。
・情報セキュリティ方針、情報セキュリティ目的及びそれを達成する計画を策定する際に、トップマネジメントの意思、判断、指示等が含まれていること。
・達成すべきセキュリティの水準として、リスクレベルをトップマネジメントが決定していること。
・リスクレベルに応じて選択したセキュリティ管理策を実施させる際に、トップマネジメントの意思、判断、指示等が含まれていること。
・内部監査において確認すべき事項に、トップマネジメントが要求する情報セキュリティ要求事項等が含まれていること。
・内部監査報告書やそれに基づく是正処置、マネジメントレビュー議事録等に、トップマネジメントの意思、判断、指示等が含まれていること。

4.4.1.2　トップマネジメントは、組織の役割について、以下の責任及び権限を割り当て、組織内に伝達する。［27001-5.3］

・情報セキュリティマネジメントを、本管理基準の要求事項として適合させる。
・情報セキュリティマネジメントのパフォーマンス評価をトップマネジメントに報告する。

また、組織の情報セキュリティマネジメントを本管理基準の要求事項に適合させるために不可欠な責任・権限を明確にしたうえで、それぞれに適切な割り当てが行われていることを確認する。責任・権限の例を以下に示す。

・セキュリティ要求事項を盛り込んだ情報セキュリティ方針等の文書を策定する責任・権限
・リスクアセスメントにおいて、リスクを運用管理する責任・権限をもつリスク所有者
・セキュリティ要求事項を満たす管理策を教育、普及させる責任・権限
・セキュリティ要求事項を満たしているか監査する責任・権限
・各プロセスの結果及び効果をトップマネジメントに報告する責任・権限
・各プロセスの結果及び効果を組織内に周知する責任・権限

4.4.1.3　トップマネジメントは、その他の関連する管理層がその責任の領域においてリーダーシップを発揮できるよう、管理層の役割を支援する。［27001-5.1ｈ）］

その他の関連する管理層が、その職掌範囲、組織等において、リーダーシップを発揮できるよう、トップマネジメントは、管理層に、必要な権限を委譲していることを確認する。

4.4.2　組織及びその状況の理解［27001-4.1］

4.4.2.1　組織は、組織の目的に関連し、かつ、情報セキュリティマネジメントの意図した成果を達成する組織の能力に影響を与える、以下の課題を決定する。［27001-4.1］

・外部の課題
・内部の課題