8b-8.10　情報の削除
8b-8.11　データマスキング
8b-8.12　データ漏えい防止
8b-8.13　情報のバックアップ
8b-8.14　情報処理施設・設備の冗長性
8b-8.15　ログ取得
8b-8.16　監視活動
8b-8.17　クロックの同期
8b-8.18　特権的なユーティリティプログラムの使用
8b-8.19　運用システムへのソフトウェアの導入

8c　情報システムの適正利用の管理
8c-8.20　ネットワークセキュリティ
8c-8.21　ネットワークサービスのセキュリティ
8c-8.22　ネットワークの分離
8c-8.23　ウェブフィルタリング
8c-8.24　暗号の利用

8d　情報システム開発／導入の管理
8d-8.25　セキュリティに配慮した開発のライフサイクル
8d-8.26　アプリケーションセキュリティの要求事項
8d-8.27　セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則
8d-8.28　セキュリティに配慮したコーディング
8d-8.29　開発及び受入れにおけるセキュリティテスト
8d-8.30　外部委託による開発
8d-8.31　開発環境、テスト環境及び本番環境の分離
8d-8.32　変更管理
8d-8.33　テスト用情報
8d-8.34　監査におけるテスト中の情報システムの保護

Ⅲ．ガバナンス基準

ガバナンス基準は、組織体のガバナンスのうち、情報セキュリティガバナンスを確立するための目的及びプロセスについて示すものである。

3.1　情報セキュリティガバナンスの概要

情報セキュリティガバナンスでは、組織体における複数のガバナンスの領域のうち、組織体の情報セキュリティ確保の達成に関するガバナンスを扱う。情報セキュリティに関するガバナンスモデルの策定にあたっては、情報技術等の他のガバナンスの領域とのモデルの対象範囲の重複の可能性があり、コーポレートガバナンスの観点からそれぞれの整合についての考慮が求められる。

ガバナンス主体は、組織体内に情報セキュリティマネジメントシステムを構築する。情報セキュリティマネジメントシステムの目的は、組織のサイズ、スケール及び構造により異なる可能性があり、それらを整合させるようにする。

なお、本管理基準の「Ⅳ．マネジメント基準」に示す管理策にも、情報セキュリティマネジメントシステムにおけるガバナンスに対応する内容が含まれている。

3.2　情報セキュリティガバナンスの目的［27014-7.2］

ガバナンス主体は、以下に示す目的に照らして適切であるような、組織体における情報セキュリティガバナンスの目的を設定する。

目的１：組織体全体の統合された包括的情報セキュリティを確立する
目的２：リスクに基づく取組を採用して意思決定を行う
目的３：投資の方向性を決定する
目的４：内部及び外部の要求事項との適合性を確実にする
目的５：セキュリティに積極的な文化を醸成する
目的６：セキュリティのパフォーマンスが現在及び将来の組織体の要求事項を満たすことを確実にする

3.3　情報セキュリティガバナンスのプロセス［27014-7.3］

3.3.1　概要

情報セキュリティガバナンスは、評価、指示、モニタ及びコミュニケーションの各プロセスで構成される。次項以降において、各プロセスにおいて、ガバナンス主体及び各情報セキュリティマネジメントシステムの責任者が実行する内容を示す。

3.3.2　評価

3.3.2.1　ガバナンス主体は、以下を実行する。
・事業に取り組む際の関連するリスク及び機会の確実な考慮
・情報セキュリティに関する報告に対応するための、情報セキュリティマネジメントシステムにおける目的と優先度の規定

3.3.2.2　各情報セキュリティマネジメントシステムの責任者は、以下を実行する。
・組織体の目的を適切に支援し、維持するような情報セキュリティの確立
・重大な影響を伴う新規の情報セキュリティプロジェクトを実施する際の、組織体のガバナンス主体への承認依頼

3.3.3　指示

3.3.3.1　ガバナンス主体は、以下を実行する。
・組織体全体の戦略の方向性と目的の設定
・その組織体のリスク選好の決定
・情報セキュリティ戦略の承認

3.3.3.2　各情報セキュリティマネジメントシステムの責任者は、以下を実行する。
・適切な投資及び資源の配分の実施
・組織体の目的に合致するように情報セキュリティの目的を調整
・情報セキュリティに関する役割と責任の割当
・情報セキュリティポリシーの規定

3.3.4　モニタ

3.3.4.1　ガバナンス主体は、以下を実行する。
・各情報セキュリティマネジメントシステムの活動の有効性に関する報告の受領
・組織体の優先度の文脈での、前項で報告された内容の評価
・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優先度の伝達

3.3.4.2　各情報セキュリティマネジメントシステムの責任者は、以下を実行する。
・情報セキュリティマネジメントシステム活動の有効性の評価
・内部及び外部の要求事項への確実な適合の確保
・組織体に関わる変化、法令及び規制の環境、並びに情報リスクへの潜在的影響の考慮
・適切なパフォーマンス指標を選定し、組織的な観点から適切なタイミングで報告が実施されるよう要求を伝達
・情報セキュリティの実績に関する結果のフィードバックを組織体の経営陣に提供
・情報リスク及び情報セキュリティに影響する新規の開発についての、組織体の経営陣への注意喚起