9　アクセス制御
9.1　アクセス制御に対する業務上の要求事項
9.2　利用者アクセスの管理
9.3　利用者の責任
9.4　システム及びアプリケーションのアクセス制御
10　暗号
10.1　暗号による管理策
11　物理及び環境的セキュリティ
11.1　セキュリティを保つべき領域
11.2　装置
12　運用のセキュリティ
12.1　運用の手順及び責任
12.2　マルウェアからの保護
12.3　バックアップ
12.4　ログ取得及び監視
12.5　運用ソフトウェアの管理
12.6　技術的ぜい弱性管理
12.7　情報システムの監査に対する考慮事項
13　通信のセキュリティ
13.1　ネットワークセキュリティ管理
13.2　情報の転送
14　システムの取得、開発及び保守
14.1　情報システムのセキュリティ要求事項
14.2　開発及びサポートプロセスにおけるセキュリティ
14.3　試験データ
15　供給者関係
15.1　供給者関係における情報セキュリティ
15.2　供給者のサービス提供の管理
16　情報セキュリティインシデント管理
16.1　情報セキュリティインシデントの管理及びその改善
17　事業継続マネジメントにおける情報セキュリティの側面
17.1　情報セキュリティ継続
17.2　冗長性
18　順守
18.1　法的及び契約上の要求事項の順守
18.2　情報セキュリティのレビュー

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　27001：2014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　27001：2014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確立　［27001-4］ 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　27001：2014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、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らに基づく是正処置、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、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。