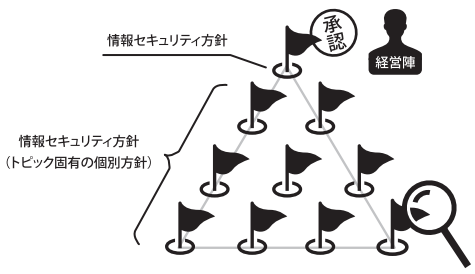
ISO/IEC 27001:2013 ANNEX A

Reference control objectives and controls

35 管理目的 及び 114 管理策

A.5 情報セキュリティのための方針群
Information security policies

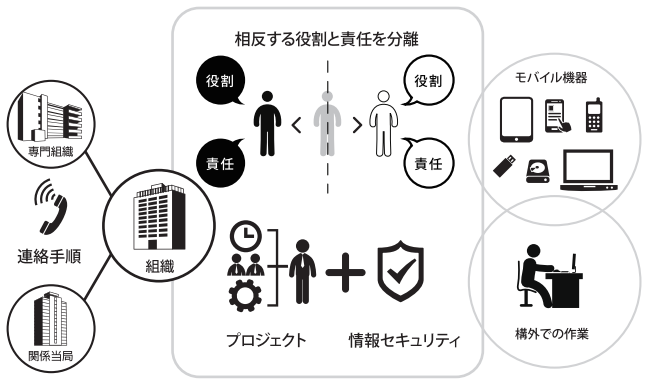
A.5.1 情報セキュリティのための経営陣の方向性
A.5.1.1 情報セキュリティのための方針群
A.5.1.2 情報セキュリティのための方針群のレビュー



A.6 情報セキュリティのための組織
Organization of information security

A.6.1 内部組織
A.6.1.1 情報セキュリティの役割及び責任
A.6.1.2 職務の分離
A.6.1.3 関係当局との連絡
A.6.1.4 専門組織との連絡
A.6.1.5 プロジェクトマネジメントにおける情報セキュリティ

A.6.2 モバイル機器及びテレワーキング
A.6.2.1 モバイル機器の方針
A.6.2.2 テレワーキング



A.7 人的資源のセキュリティ
Human resource security

A.7.1 雇用前
A.7.1.1 選考
A.7.1.2 雇用条件

A.7.2 雇用期間中
A.7.2.1 経営陣の責任
A.7.2.2 情報セキュリティの意識向上, 教育及び訓練
A.7.2.3 懲戒手続

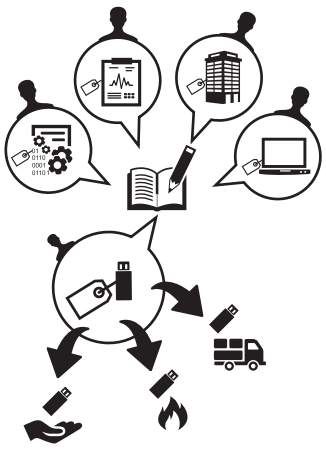
A.7.3 雇用の終了及び変更
A.7.3.1 雇用の終了又は変更に関する責任

A.8 資産の管理
Asset management

A.8.1 資産に対する責任
A.8.1.1 資産目録
A.8.1.2 資産の管理責任
A.8.1.3 資産利用の許容範囲
A.8.1.4 資産の返却

A.8.2 情報分類
A.8.2.1 情報の分類
A.8.2.2 情報のラベル付け
A.8.2.3 資産の取扱い

A.8.3 媒体の取扱い
A.8.3.1 取外し可能な媒体の管理
A.8.3.2 媒体の処分
A.8.3.3 物理的媒体の輸送



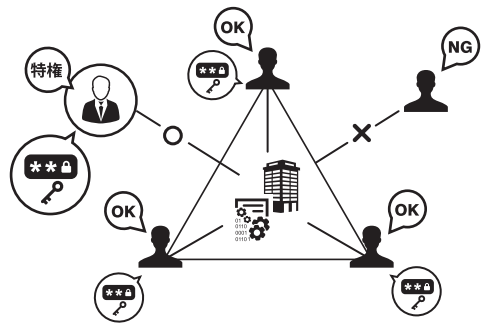
A.9 アクセス制御
Access control

A.9.1 アクセス制御に対する業務上の要求事項
A.9.1.1 アクセス制御方針
A.9.1.2 ネットワーク及びネットワークサービスへのアクセス

A.9.2 利用者アクセスの管理
A.9.2.1 利用者登録及び登録削除
A.9.2.2 利用者アクセスの提供
A.9.2.3 特権的アクセス権の管理
A.9.2.4 利用者の秘密認証情報の管理
A.9.2.5 利用者アクセス権のレビュー
A.9.2.6 アクセス権の削除又は修正

A.9.3 利用者の責任
A.9.3.1 秘密認証情報の利用

A.9.4 システム及びアプリケーションのアクセス制御
A.9.4.1 情報へのアクセス制限
A.9.4.2 セキュリティに配慮したログオン手順
A.9.4.3 パスワード管理システム
A.9.4.4 特権的なユーティリティプログラムの使用
A.9.4.5 プログラムソースコードへのアクセス制御



A.10 暗号
Cryptography

A.10.1 暗号による管理策
A.10.1.1 暗号による管理策の利用方針
A.10.1.2 鍵管理

A.11 物理的及び環境的セキュリティ
Physical and environmental security

A.11.1 セキュリティを保つべき領域
A.11.1.1 物理的セキュリティ境界
A.11.1.2 物理的入退管理策
A.11.1.3 オフィス, 部屋及び施設のセキュリティ
A.11.1.4 外部及び環境の脅威からの保護
A.11.1.5 セキュリティを保つべき領域での作業
A.11.1.6 受渡場所

A.11.2 装置
A.11.2.1 装置の設置及び保護
A.11.2.2 サポートユーティリティ
A.11.2.3 ケーブル配線のセキュリティ
A.11.2.4 装置の保守
A.11.2.5 資産の移動
A.11.2.6 構外にある装置及び資産のセキュリティ
A.11.2.7 装置のセキュリティを保った処分又は再利用
A.11.2.8 無人状態にある利用者装置
A.11.2.9 クリアデスク・クリアスクリーン方針

A.12 運用のセキュリティ
Operations security

A.12.1 運用の手順及び責任
A.12.1.1 操作手順書
A.12.1.2 変更管理
A.12.1.3 容量・能力の管理
A.12.1.4 開発環境, 試験環境及び運用環境の分離

A.12.2 マルウェアからの保護
A.12.2.1 マルウェアに対する管理策

A.12.3 バックアップ
A.12.3.1 情報のバックアップ

A.12.4 ログ取得及び監視
A.12.4.1 イベントログ取得
A.12.4.2 ログ情報の保護
A.12.4.3 実務管理者及び運用担当者の作業ログ
A.12.4.4 クロックの同期

A.12.5 運用ソフトウェアの管理
A.12.5.1 運用システムに関わるソフトウェアの導入

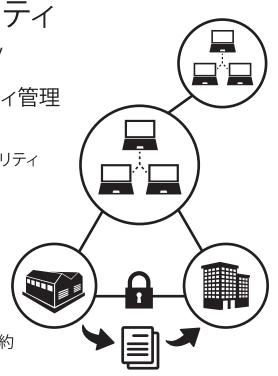
A.12.6 技術的ぜい弱性管理
A.12.6.1 技術的ぜい弱性の管理
A.12.6.2 ソフトウェアのインストールの制限

A.12.7 情報システムの監査に対する考慮事項
A.12.7.1 情報システムの監査に対する管理策

A.13 通信のセキュリティ
Communications security

A.13.1 ネットワークセキュリティ管理
A.13.1.1 ネットワーク管理策
A.13.1.2 ネットワークサービスのセキュリティ
A.13.1.3 ネットワークの分離

A.13.2 情報の転送
A.13.2.1 情報転送の方針及び手順
A.13.2.2 情報転送に関する合意
A.13.2.3 電子的メッセージ通信
A.13.2.4 秘密保持契約又は守秘義務契約



A.14 システムの取得, 開発及び保守
System acquisition,development and maintenance

A.14.1 情報システムのセキュリティ要求事項
A.14.1.1 情報セキュリティ要求事項の分析及び仕様化
A.14.1.2 公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮
A.14.1.3 アプリケーションサービスのトランザクションの保護

A.14.2 開発及びサポートプロセスにおけるセキュリティ
A.14.2.1 セキュリティに配慮した開発のための方針
A.14.2.2 システムの変更管理手順
A.14.2.3 オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー
A.14.2.4 パッケージソフトウェアの変更に対する制限
A.14.2.5 セキュリティに配慮したシステム構築の原則
A.14.2.6 セキュリティに配慮した開発環境
A.14.2.7 外部委託による開発
A.14.2.8 システムセキュリティの試験
A.14.2.9 システムの受入れ試験

A.14.3 試験データ
A.14.3.1 試験データの保護

A.15 供給者関係
Supplier relationships

A.15.1 供給者関係における情報セキュリティ
A.15.1.1 供給者関係のための情報セキュリティの方針
A.15.1.2 供給者との合意におけるセキュリティの取扱い
A.15.1.3 ICT サプライチェーン

A.15.2 供給者のサービス提供の管理
A.15.2.1 供給者のサービス提供の監視及びレビュー
A.15.2.2 供給者のサービス提供の変更に対する管理

A.16 情報セキュリティインシデント管理
Information security incident management

A.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
A.16.1.1 責任及び手順
A.16.1.2 情報セキュリティ事象の報告
A.16.1.3 情報セキュリティ弱点の報告
A.16.1.4 情報セキュリティ事象の評価及び決定
A.16.1.5 情報セキュリティインシデントへの対応
A.16.1.6 情報セキュリティインシデントからの学習
A.16.1.7 証拠の収集

A.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
Information security aspects of business continuity management

A.17.1 情報セキュリティ継続
A.17.1.1 情報セキュリティ継続の計画
A.17.1.2 情報セキュリティ継続の実施
A.17.1.3 情報セキュリティ継続の検証, レビュー及び評価

A.17.2 冗長性
A.17.2.1 情報処理施設の可用性

A.18 順守
Compliance

A.18.1 法的及び契約上の要求事項の順守
A.18.1.1 適用法令及び契約上の要求事項の特定
A.18.1.2 知的財産権
A.18.1.3 記録の保護
A.18.1.4 プライバシー及び個人を特定できる情報（PII）の保護
A.18.1.5 暗号化機能に対する規制

A.18.2 情報セキュリティのレビュー
A.18.2.1 情報セキュリティの独立したレビュー
A.18.2.2 情報セキュリティのための方針群及び標準の順守
A.18.2.3 技術的順守のレビュー