12.7.1.5　監査における試験を実施するための、特別又は追加の処理に関する要求事項を特定し、合意する。
12.7.1.6　監査における試験がシステムの可用性に影響する可能性がある場合、こうした試験は営業時間外に実施する。
12.7.1.7　監査における試験を実施する際には、参照用の証跡を残すために、全てのアクセスを監視し、ログをとる。

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

目的：ネットワークにおける情報の保護、及びネットワークを支える情報処理施設の保護を確実にするため

13.1.1　システム及びアプリケーション内の情報を保護するために、ネットワークを管理し、制御する。
13.1.1.1　ネットワークにおける情報のセキュリティ、及び接続したネットワークサービスの認可されていないアクセスからの保護を確実にするために、管理策を実施する。
13.1.1.2　ネットワーク設備の管理に関する責任及び手順を確立する。
13.1.1.3　ネットワークの運用責任は、コンピュータの運用から、分離する。
13.1.1.4　公衆ネットワーク又は無線ネットワークを通過するデータの機密性及び完全性を保護するため、並びにネットワークを介して接続したシステム及びアプリケーションを保護するために、特別な管理策を確立する。
13.1.1.5　ネットワークサービスの可用性及びネットワークを介して接続したコンピュータの可用性を維持するために、特別な管理策を確立する。
13.1.1.6　情報セキュリティに影響を及ぼす可能性のある行動、又は情報セキュリティに関連した行動を記録及び検知できるように、適切なログ取得及び監視を適用する。
13.1.1.7　組織に対するサービスを最適にするため、また、管理策を情報処理基盤全体に一貫して適用することを確実にするために、様々な管理作業を綿密に調整する。
13.1.1.8　ネットワーク上のシステムを認証する。
13.1.1.9　ネットワークへのシステムの接続を制限する。

13.1.2　組織が自ら提供するか外部委託しているかを問わず、全てのネットワークサービスについて、セキュリティ機能、サービスレベル及び管理上の要求事項を特定し、また、ネットワークサービス合意書にもこれらを盛り込む。
13.1.2.1　ネットワークサービスの提供者と合意したサービスをセキュリティを保って管理するために必要なネットワークサービス提供者の能力を定め、常に監視し、監査の権利についてネットワークサービス提供者と合意する。
13.1.2.2　それぞれのサービスに必要なセキュリティについての取決め(例えば、セキュリティ特性、サービスレベル、管理上の要求事項）を特定し、組織は、ネットワークサービス提供者によるこれらの対策の実施を確実にする仕組みを整備する。

13.1.3　情報サービス、利用者及び情報システムは、ネットワーク上で、グループごとに分離する。
13.1.3.1　大規模なネットワークのセキュリティを管理するために、必要に応じてネットワークを幾つかのネットワーク領域に分離する。
13.1.3.2　ネットワーク領域は、組織の単位（例えば、人的資源、財務、マーケティング）又は特定の組合せ（例えば、複数の組織の単位に接続しているサーバ領域）に従い、信頼性のレベル（例えば、公開されている領域、デスクトップ領域、サーバ領域）に基づいて選択する。
13.1.3.3　ネットワーク領域の分離は、物理的に異なるネットワーク又は論理的に異なるネットワーク（例えば、仮想私設網）を用いることによって行う。
13.1.3.4　各ネットワーク領域の境界は、明確に定める。
13.1.3.5　ネットワーク領域間のアクセスは、境界にゲートウェイ（例えば、ファイアウォール、フィルタリングルータ）を設けて制御する。
13.1.3.6　各ネットワーク領域のセキュリティ要求事項のアセスメントに基づき、ネットワークを領域に分離する際の基準及びゲートウェイを通じて認められるアクセスの基準を定める。
13.1.3.7　各ネットワーク領域のセキュリティ要求事項のアセスメントは、アクセス制御方針、アクセス要求事項、並びに処理する情報の価値及び分類に従い、また、費用対効果を考慮して適切なゲートウェイ技術を組み込む。
13.1.3.8　ネットワークの境界が十分に定められていない無線ネットワークでは、ネットワーク領域の分離のための特別な取扱いを定める。
13.1.3.9　取扱いに慎重を要する環境では、全ての無線アクセスは、外部接続として取り扱い、そのアクセスがネットワーク管理策の方針に従ってゲートウェイを通過して内部システムへのアクセスが許可されるまでは、内部ネットワークから分離する。

13.2　情報の転送

目的：組織の内部及び外部に転送した情報のセキュリティを維持するため

13.2.1　あらゆる形式の通信設備を利用した情報転送を保護するために、正式な転送方針、手順及び管理策を備える。
13.2.1.1　情報転送のために通信設備を利用するときに従う手順及び管理策には、転送する情報を、盗聴、複製、改ざん、誤った経路での通信及び破壊から保護するために設計された手順を反映する。
13.2.1.2　情報転送のために通信設備を利用するときに従う手順及び管理策には、電子的メッセージ通信を通じて伝送される可能性のあるマルウェアを検出し、これらから保護するための手順を反映する。
13.2.1.3　情報転送のために通信設備を利用するときに従う手順及び管理策には、添付形式として通信される、取扱いに慎重を要する電子情報の保護に関する手順を反映する。
13.2.1.4　情報転送のために通信設備を利用するときに従う手順及び管理策には、通信設備の許容できる利用について規定した方針又は指針を反映する。
13.2.1.5　情報転送のために通信設備を利用するときに従う手順及び管理策には、要員、外部関係者及びその他の利用者の、組織を危うくするような行為（例えば、名誉き(毀)損、嫌がらせ、成りすまし、チェーンメールの転送、架空購入）をしないことの責任を含める。
13.2.1.6　情報転送のために通信設備を利用するときに従う手順及び管理策には、暗号技術の利用（例えば、情報の機密性、完全性及び真正性を保護するための暗号の利用）を含める。
13.2.1.7　情報転送のために通信設備を利用するときに従う手順及び管理策には、関連する国及び地域の法令及び規制に従った、全ての業務通信文（メッセージを含む。）の保持及び処分に関する指針を反映する。
13.2.1.8　情報転送のために通信設備を利用するときに従う手順及び管理策には、通信設備の利用（例えば、外部のメールアドレスへの電子メールの自動転送）に関する管理策及び制限を反映する。
13.2.1.9　情報転送のために通信設備を利用するときに従う手順及び管理策には、秘密情報を漏えいしないように適切な予防策を講じることの、要員への助言を含める。
13.2.1.10　情報転送のために通信設備を利用するときに従う手順及び管理策には、留守番電話に残したメッセージの、認可されていない者による再生、共有システムに保管、又は誤ダイアルによる間違った先へ保管されることを防止するため、秘密情報を含んだメッセージを留守番電話に残さないことを含める。