6.1.5.3　プロジェクトマネジメント手法においては、必要な管理策を特定するため、プロジェクトの早い段階で情報セキュリティリスクアセスメントを実施する。
6.1.5.4　プロジェクトマネジメント手法においては、適用するプロジェクトマネジメントの方法論の全ての局面において、情報セキュリティを含める。
6.1.5.5　全てのプロジェクトにおいて、情報セキュリティの組織への影響を明確にし、これを定期的にレビューする。
6.1.5.6　プロジェクトマネジメント手法で定められた役割を明確にするため、情報セキュリティに関する責任を定め、割り当てる。

6.2　モバイル機器及びテレワーキング

目的：モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため

6.2.1　モバイル機器を用いることによって生じるリスクを管理するために、方針及びその方針を支援するセキュリティ対策を採用する。
6.2.1.1　モバイル機器を用いる場合、業務情報が危険にさらされないことを確実にするために、特別な注意を払う。
6.2.1.2　モバイル機器の情報セキュリティ方針は、保護されていない環境におけるモバイル機器を用いた作業のリスクを考慮して定める。
6.2.1.3　モバイル機器の情報セキュリティ方針には、モバイル機器の登録を含める。
6.2.1.4　モバイル機器の情報セキュリティ方針には、物理的保護についての要求事項を含める。
6.2.1.5　モバイル機器の情報セキュリティ方針には、ソフトウェアのインストールの制限を含める。
6.2.1.6　モバイル機器の情報セキュリティ方針には、モバイル機器のソフトウェアのバージョン及びパッチ適用に対する要求事項を含める。
6.2.1.7　モバイル機器の情報セキュリティ方針には、情報サービスへの接続の制限を含める。
6.2.1.8　モバイル機器の情報セキュリティ方針には、アクセス制御を含める。
6.2.1.9　モバイル機器の情報セキュリティ方針には、暗号技術を含める。
6.2.1.10　モバイル機器の情報セキュリティ方針には、マルウェアからの保護を含める。
6.2.1.11　モバイル機器の情報セキュリティ方針には、遠隔操作による機器の無効化、データの消去又はロックを含める。
6.2.1.12　モバイル機器の情報セキュリティ方針には、バックアップを含める。
6.2.1.13　モバイル機器の情報セキュリティ方針には、ウェブサービス及びウェブアプリケーションの使用を含める。
6.2.1.14　公共の場所、会議室、その他保護されていない場所でモバイル機器を用いるときは、注意を払う。
6.2.1.15　モバイル機器に保管され、処理される情報について、認可されていないアクセス又は漏えいを防止するため、例えば、暗号技術の使用、秘密認証情報の使用の強制などの保護を実施する。
6.2.1.16　モバイル機器は、盗難、特にどこか（例えば、自動車、他の輸送機関、ホテルの部屋、会議室、集会所）に置き忘れたときの盗難から、物理的に保護する。
6.2.1.17　モバイル機器の盗難又は紛失の場合の対策のために、法規制、保険及び組織の他のセキュリティ要求事項を考慮した特定の手順を確立する。
6.2.1.18　重要度の高い、取扱いに慎重を要する又は影響の大きい業務情報が入っているモバイル機器は、無人の状態で放置しない。
6.2.1.19　重要度の高い、取扱いに慎重を要する又は影響の大きい業務情報が入っているモバイル機器は、可能な場合には、物理的に施錠するか、又はモバイル機器のセキュリティを確保するために特別な錠を用いる。
6.2.1.20　作業形態に起因する追加のリスク及び実施すべき管理策についての意識向上のために、モバイル機器を用いる要員に対する教育・訓練を計画・準備・実施する。
6.2.1.21　モバイル機器の情報セキュリティ方針で、個人所有のモバイル機器の使用が許されている場合は、その方針及び関連するセキュリティ対策において、機器の私的な使用と業務上の使用とを区別する（このような区別を可能とし、個人所有の機器に保存された業務データを保護するためのソフトウェアの使用も含む。）。
6.2.1.22　モバイル機器の情報セキュリティ方針で、個人所有のモバイル機器の使用が許されている場合は、その方針及び関連するセキュリティ対策において、エンドユーザ合意書に利用者が署名した場合にだけ、業務情報にアクセスできるようにする（エンドユーザ合意書には、利用者の義務（物理的な保護、ソフトウェアの更新など）についての確認、業務データに対する所有権を主張しないこと、及び機器の盗難若しくは紛失があった場合又はサービス利用の認可が取り消された場合に組織が遠隔操作でデータを消去することへの合意を含む。この方針では、プライバシーに関する法令を考慮する。）。

6.2.2　テレワーキングの場所でアクセス、処理及び保存される情報を保護するために、方針及びその方針を支援するセキュリティ対策を実施する。
6.2.2.1　テレワーキング活動を許可する組織は、テレワーキングを行う場合の条件及び制限を定めた方針を発行する。
6.2.2.2　テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、建物及び周辺環境の物理的セキュリティを考慮に入れた、テレワーキングの場所の既存の物理的セキュリティの状況を考慮して定める。
6.2.2.3　テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、提案された物理的なテレワーキングの環境を考慮して定める。
6.2.2.4　テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、組織の内部システムへの遠隔アクセスの必要性、通信回線からアクセスし、通信回線を通過する情報の取扱い慎重度及び内部システムの取扱いに関する慎重度を考慮した、通信のセキュリティに関する要求事項を考慮して定める。
6.2.2.5　テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、個人所有の装置で情報を処理及び保管できないようにする仮想デスクトップへのアクセスを考慮して定める。
6.2.2.6　テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、住環境を共有する者（例えば、家族、友人）による、情報又は資源への認可されていないアクセスの脅威を考慮して定める。
6.2.2.7　テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、家庭のネットワークの使用及び無線ネットワークサービスの設定に関する要求事項又は制限を考慮して定める。
6.2.2.8　テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、個人所有の装置の上で開発した知的財産の権利に関する論争を防ぐための方針及び手順を考慮して定める。
6.2.2.9　テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、個人所有の装置へのアクセス（装置のセキュリティ検証のためのもの、又は調査期間中に行うもの）を考慮して定める。なお、このアクセスは、法令が禁じている場合がある。
6.2.2.10　テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、従業員又は外部の利用者が個人的に所有するワークステーション上のクライアントソフトウェアの使用許諾について、組織が責任をもつことになる場合の、ソフトウェアの使用許諾契約を考慮して定める。