11.1.2　セキュリティを保つべき領域は、認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によって保護する。

11.1.2.1　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、訪問者の入退の日付及び時刻を記録する。

11.1.2.2　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、アクセスが事前に承認されている場合を除いて、全ての訪問者を監督する。

11.1.2.3　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、訪問者には、特定され、認可された目的のためのアクセスだけを許可し、その領域のセキュリティ要求事項及び緊急時の手順についての指示を与える。

11.1.2.4　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、適切な手段によって、訪問者の識別情報を認証する。

11.1.2.5　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、適切なアクセス制御（例えば、アクセスカード及び秘密の個人識別番号のような、二要素認証の仕組みの導入）を実施する。

11.1.2.6　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、秘密情報を処理又は保管する領域へのアクセスを、認可された者だけに制限する。

11.1.2.7　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、全てのアクセスについて、物理的な記録日誌又は電子形式の監査証跡を、セキュリティを保って維持及び監視する。

11.1.2.8　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、全ての従業員、契約相手及び外部関係者に、何らかの形式の、目に見える証明書の着用を要求する。

11.1.2.9　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、関係者が付き添っていない訪問者及び目に見える証明書を着用していない者を見かけた場合は、直ちにセキュリティ要員に知らせる。

11.1.2.10　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、セキュリティを保つべき領域又は秘密情報処理施設への、外部のサポートサービス要員によるアクセスは、限定的かつ必要なときにだけ許可する。

11.1.2.11　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、セキュリティを保つべき領域又は秘密情報処理施設への、外部のサポートサービス要員によるアクセスは認可を必要とし、監視する。

11.1.2.12　セキュリティを保つべき領域が認可された者だけにアクセスを許すことを確実にするため、セキュリティを保つべき領域へのアクセス権は、定期的にレビューし、更新し、必要なときには無効にする。

11.1.3　オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用する。

11.1.3.1　オフィス、部屋及び施設のセキュリティを保つために、主要な施設は、一般の人のアクセスが避けられる場所に設置する。

11.1.3.2　オフィス、部屋及び施設のセキュリティを保つために、建物を目立たせず、その目的を示す表示は最小限とし、情報処理活動の存在を示すものは、建物の内外を問わず、一切表示しないように設計する。

11.1.3.3　オフィス、部屋及び施設のセキュリティを保つために、施設は、秘密の情報又は活動が外部から見えたり聞こえたりしないように構成する（該当する場合、電磁遮蔽も含める。）。

11.1.3.4　オフィス、部屋及び施設のセキュリティを保つために、秘密情報処理施設の場所を示す案内板及び内線電話帳は、認可されていない者が容易にアクセスできないようにする。

11.1.4　自然災害、悪意のある攻撃又は事故に対する物理的な保護を設計し、適用する。

11.1.4.1　火災、洪水、地震、爆発、暴力行為、及びその他の自然災害又は人的災害からの損傷を回避する方法について、専門家の助言を得る。

11.1.5　セキュリティを保つべき領域での作業に関する手順を設計し、適用する。

11.1.5.1　セキュリティを保つべき領域での作業に関する手順の設計においては、要員は、セキュリティを保つべき領域の存在又はその領域内での活動は、業務上知る必要のある要員にのみ知らせることを含める。

11.1.5.2　セキュリティを保つべき領域での作業に関する手順の設計に、安全面の理由のため及び悪意ある活動の機会を防止するための両面から、セキュリティを保つべき領域での監督されていない作業は、回避することを含める。

11.1.5.3　セキュリティを保つべき領域での作業に関する手順の設計に、セキュリティを保つべき領域が無人のときは、物理的に施錠し、定期的に点検することを含める。

11.1.5.4　セキュリティを保つべき領域での作業に関する手順の設計に、画像、映像、音声又はその他の記録装置（例えば、携帯端末に付いたカメラ）は、認可されたもの以外は許可しないことを含める。

11.1.5.5　セキュリティを保つべき領域での作業に関する取決めには、その領域で作業する従業員及び外部の利用者に対する管理策を含める。

11.1.5.6　セキュリティを保つべき領域での作業に関する取決めは、セキュリティを保つべき領域で行われる全ての活動に適用する。

11.1.6　荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所は、管理する。また、認可されていないアクセスを避けるために、それらの場所を情報処理施設から離す。

11.1.6.1　荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、建物外部からの受渡場所へのアクセスは、識別及び認可された要員に制限する。

11.1.6.2　荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、受渡場所は、配達要員が建物の他の場所にアクセスすることなく荷積み及び荷降ろしできるように設計する。

11.1.6.3　荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、受渡場所の外部扉は、内部の扉が開いているときにはセキュリティを保つ。

11.1.6.4　荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、入荷物は、受渡場所から移動する前に、爆発物、化学物質又はその他の危険物がないかを検査する。

11.1.6.5　荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、入荷物は、事業所へ持ち込むときに資産の管理手順に従って登録する。

11.1.6.6　荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、入荷と出荷とは、物理的に分離した場所で扱う。

11.1.6.7　荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所を管理するため、入荷物は、輸送中に開封された痕跡がないかを検査する。開封の痕跡が見つかった場合には、直ちにセキュリティ要員に報告する。