6a-6.8.6　要員及び利用者に、疑いをもった情報セキュリティのぜい弱性の立証を試みないように要求する。

（6a-6.8.6参考）　ぜい弱性を検査することは、システムの不正使用の企てと見られる可能性があり、情報システム又はサービスに損傷を与える可能性もあり、それはディジタル証拠を破損又は不明瞭にする可能性がある。最終的に、検査した個人に法的責任が発生する可能性がある。

7　物理的管理策

7a　物理的領域の管理

7a-7.1　物理的セキュリティ境界

管理策：情報及びその他の関連資産のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いる。

目的：　組織の情報及びその他の関連資産への認可されていない物理的アクセス、損傷及び干渉を防ぐため。

詳細管理策

7a-7.1.1　物理的セキュリティ境界について、次の事項を、必要な場合には、考慮し、実施する。

a）境界内に設置している資産の情報セキュリティ要求事項に従って、セキュリティ境界並びにそれぞれの境界の位置及び強度を定める。

b）情報処理設備を収容した建物又は敷地が物理的に頑丈な境界をもつ（すなわち、境界には隙間がなく、又は容易に侵入できる箇所がない。）。敷地内の屋根、壁、天井及び床は、堅固な構造物とし、外部に接する全ての扉を、開閉制御の仕組みによって、認可されていないアクセスから適切に保護する。要員が不在のときには、扉及び窓を施錠し、窓（特に一階の窓）については外部からの保護を考慮する。換気口の位置も考慮する。

c）セキュリティ境界上にある全ての防火扉は、適切な標準が要求するレベルの抵抗力を確立するために、壁と併せて、警告、監視及び試験を行う。防火扉は、不具合が発生しても安全側に作動するように運用する。

7a-7.2　物理的入退

管理策：セキュリティを保つべき領域は、適切な入退管理策及びアクセス場所（受付など）によって保護する。

目的：　組織の情報及びその他の関連資産に、認可された物理的アクセスだけがなされることを確実にするため。

詳細管理策

【物理的入退全般】

7a-7.2.1　荷物の受渡場所などのアクセス場所（受付など）、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。

7a-7.2.2　可能な場合には、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。

7a-7.2.3　物理的入退の管理策の実施については、次の事項を考慮する。

a）敷地及び建物へのアクセスは、認可された要員だけに制限する。物理的領域へのアクセス権の管理プロセスに、認可の提供、定期的なレビュー、更新及び失効を含める。

b）全てのアクセスについて、物理的な記録簿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し、全ての記録及び取扱いに慎重を要する認証情報を保護する。

c）情報を処理する又は保管する領域へのアクセスを管理するためのプロセス及び技術的な仕組みを確立し、実装する。認証の仕組みには、アクセスカード、生体認証、又は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使用を含む。慎重を要する領域へのアクセスには、二重のセキュリティドアの採用を検討する。

d）要員が監視している受付エリア、又は敷地若しくは建物への物理的なアクセスを管理するその他の手段を設定する。

e）入退の際に要員及び利害関係者の持ち物を検査し、確認する。

f）全ての要員及び利害関係者に、何らかの形式の、目に見える証明書の着用を要求する。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。常勤の従業員、供給者及び訪問者を識別しやすくするために、容易に区別できるバッジの使用を検討する。

g）セキュリティを保つべき領域又は情報処理施設への、供給者の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。このアクセスは、認可を必要とし、監視する。

h）複数の組織の資産を保持する建物の場合、物理的なアクセスのセキュリティには特別な注意を払う。

i）物理的なインシデントの起こりやすさが高くなった場合に強化できるように物理的セキュリティ対策を設計する。

j）非常口などの他の入退場所を、認可されていないアクセスから保護する。

k）物理的な鍵又は認証情報の管理を確実にし、記録簿又は毎年の鍵監査、及び物理的な鍵又は認証情報へのアクセスの管理を確実にするための鍵管理プロセスを設定する。

【訪問者】

7a-7.2.4　物理的入退の訪問者に関する管理策では、次の事項を考慮する。

a）適切な手段によって訪問者のアイデンティティを認証する。

b）訪問者の出入りの日時を記録する。

c）特定の認可された目的で、かつ、領域のセキュリティ要求事項及び緊急時の手順に関する指示の下でだけ、訪問者にアクセスを許可する。

d）明示的に例外が許可されない限り、全ての訪問者を監視する。

【荷物の受渡場所及び入荷資材】

7a-7.2.5　荷物の受渡場所及び入荷資材に対する管理策では次の事項を考慮する。

a）建物外部からの受渡場所へのアクセスは、特定の認可された要員に制限する。

b）受渡場所は、配達要員が建物の他の場所に認可されていないアクセスを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。