7a-7.5.5　リスクアセスメントの結果に基づいて、関連する物理的及び環境的脅威を特定し、次の状況のような例において適切な管理策の採用を考慮する。

a）火災：記憶媒体及び関連する情報処理システムの火災による損傷を防ぐために、火災を早期に検知し、警報を送信する又は消火システムを起動することができるシステムを設置し、構成する。消火は、周囲の環境に対して最も適切な物質を使用して実施する。

b）洪水：記憶媒体又は情報処理システムを含む領域の床の下に、洪水を早期に検知できるシステムを設置する。洪水が発生した場合に水ポンプ又は同等の手段をすぐに利用できるようにする。

c）電気サージ：サーバ及びクライアントの両方の情報システムを電気サージ又は同様の事象から保護し、そのような事象の結果を最小化することができるシステムを採用する。

d）爆発物及び武器：取扱いに慎重を要する情報処理施設に入る要員、車両又は商品に対して、爆発物又は武器がないかランダムな検査を実施する。

7a-7.6　セキュリティを保つべき領域での作業

管理策：セキュリティを保つべき領域での作業に関するセキュリティ対策を設計し、実施する。

目的：　セキュリティを保つべき領域にある情報及びその他の関連資産を、この領域で作業する要員による損傷及び認可されていない干渉から保護するため。

詳細管理策

7a-7.6.1　セキュリティを保つべき領域での作業のセキュリティ対策は、全ての要員に適用し、セキュリティを保つべき領域で行われる全ての活動を対象とする。

7a-7.6.2　セキュリティを保つべき領域での作業の管理策の実施については、次の事項を考慮する。

a）要員には、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を、知る必要性の原則に基づく範囲でだけ認識させる。

b）安全面の理由のため及び悪意のある活動の機会を低減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。

c）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、定期的に検査する。

d）画像、映像、音声又はその他の記録装置は、認可されたもの以外は許可しない。

e）セキュリティを保つべき領域での利用者エンドポイント機器の携行及び使用を適切に管理する。

f）見やすいように又はアクセスできるように緊急手順を掲示する。

7a-7.7　クリアデスク・クリアスクリーン

管理策：書類及び取外し可能な記憶媒体に対するクリアデスクの規則、並びに情報処理設備に対するクリアスクリーンの規則を定め、適切に実施させる。

目的：　通常の勤務時間内及び時間外の、机、スクリーン及びその他のアクセス可能な場所にある情報への認可されていないアクセス、情報の消失及び損傷のリスクを低減するため。

詳細管理策

7a-7.7.1　組織は、クリアデスク・クリアスクリーンに関するトピック固有の方針を確立し、全ての関連する利害関係者へ伝達する。

7a-7.7.2　クリアデスク・クリアスクリーンの管理策の実施については、次の事項を考慮する。

a）取扱いに慎重を要する業務情報又は重要な業務情報は、必要のない場合、特にオフィスに誰もいないときには、施錠して（理想的には金庫、書庫又はセキュリティを備えた他の形態の収納用具に）保管しておく。

b）使用していないとき又は離席時には、施錠又はその他のセキュリティ手段によって利用者エンドポイント機器を保護する。

c）利用者エンドポイント機器は、離席時には、ログオフ状態にしておくか、又は利用者認証機能で管理されたスクリーン及びキーボードのロック機能によって保護しておく。全てのコンピュータ及びシステムは、タイムアウト又は自動ログアウト機能をもつ構成とする。

d）印刷を実行した人に、プリンタ又は複合機からの出力をすぐに収集させる。印刷を実行した人だけが、プリンタの横に立ったときにだけ、印刷物を得ることができる認証機能をもつプリンタを利用する。

e）取扱いに慎重を要する情報を含む文書及び取外し可能な記憶媒体をセキュリティを保って保管し、不要になった場合はセキュリティを保った処分の仕組みを使用してそれらを破棄する。

f）画面上のポップアップの設定に関する規則及び手引を確立し、伝達する。

g）不要になった場合には、ホワイトボード上及びその他の種類の掲示上の取扱いに慎重を要する情報又は重要な情報を消去する。

7a-7.7.3　組織は、組織の資産を後に残さないことを確実にするために、退出する前に最後の清掃を行うことを含む、施設から退去する際の適切な手順をもつ。

7b　装置の管理

7b-7.8　装置の設置及び保護

管理策：装置は、セキュリティを保って設置し、保護する。

目的：　物理的及び環境的脅威、並びに認可されていないアクセス及び損傷によるリスクを低減するため。

詳細管理策

7b-7.8.1　装置を保護するために、次の事項を考慮する。

a）装置は、作業領域への不必要なアクセスを最小限とし、認可されていないアクセスを回避するように設置する。

b）取扱いに慎重を要するデータを扱う情報処理設備は、設備の使用中に認可されていない者が情報をのぞき見るリスクを低減するために、その位置を慎重に定める。

c）潜在的な物理的及び環境的脅威のリスクを最小限に抑えるための管理策を採用する。