

VI 物理的セキュリティ対策

1 装置の物理的セキュリティ対策

(1) サーバの物理的セキュリティ対策

①目的

- ・許可されないアクセスからの不正なアクセスの防止
- ・許可されたアクセスの誤使用の防止
- ・システム障害につながるホコリからの保護及び空調管理等
- ・地震や火災などの災害からの保護

②サーバ装置はロックで管理し、電子情報の重要性に応じて以下の管理策を講ずる。

a 管理策

管理レベル	管理策
高	専用施設での管理
↑	サーバールームでの管理
↓	パーティション設置などの管理
低	上記以外の管理

b サーバ別の管理策の詳細は、電子情報資産管理台帳に定める。

③専用施設及びサーバールーム（セキュリティ区画）の管理

a 管理策

電子情報の重要性に応じて、以下の管理策を講ずる。

管理対象	管理策
表示など	原則としてセキュリティ区画と判断できる表示は行わない。
不正侵入者の防止	常に施錠を行う。（IDカード、パスワードキー等の利用）
入退室管理	入退室者の管理を行う。
空調管理	空調設備の設置等による適切な温度管理を行う。
納品及び出荷管理	セキュリティ区画での直接の納品及び出荷は原則として禁止する。
防災対策	耐震補強、防火設備等必要な措置を講ずる。

b セキュリティ区画への立入許可

外部委託者に、セキュリティ区画への立入を許可する場合は、次の要件を満たすものとする。

- ・契約書に守秘義務を含むセキュリティ要求事項を明確にする。
- ・事前に名簿を提出するとともに、名札、制服等の着用を義務付ける。
- ・管理者若しくは管理者が任命した者が立会い、作業を行わせる。

(2) クライアントの物理的セキュリティ対策

①目的

- ・許可されないアクセスからの不正なアクセスの防止
- ・許可されたアクセスの誤使用の防止
- ・盗難又は紛失による情報漏えいの防止
- ・故障又は破損による利用不能状態の防止

②管理策

管理対象名		管理策
モニター画面		<p>離席時は、以下の管理の内、適切な措置を講ずる。</p> <p>a 長時間の場合</p> <ul style="list-style-type: none"> ・パソコン又はモニターの電源を切る ・パスワード付スクリーンセイバーを設定する ・コンピュータのロックを行う <p>b 短時間の場合</p> <ul style="list-style-type: none"> ・画面表示を起動初期状態にする
I Dカードの利用 (該当する端末のみ)		<p>以下の行為を禁止する。</p> <p>a 他人の I Dカードの利用又は他人への貸し出し</p> <p>b 装置付近への I Dカードの放置</p>
ノート型 パソコン	保管	<p>以下の管理の内、適切な措置を講ずる</p> <p>a 鍵付キャビネット等で保管する</p> <p>b 鍵付チェーンなどで保護しデスク上で管理する</p>
	外部への 持ち出し	<p>原則として禁止する。</p> <p>ただし、業務上やむを得ない場合は、所属長の許可を得ること。なお、重要な電子情報がパソコンに保存されている場合は、以下の管理の内、適切な措置を講ずること。</p> <p>a ファイルを削除する</p> <p>b ファイルへのパスワード設定又は暗号化</p> <p>c 装置のロック</p>

(3) プリンタ、コピー機及びFAXの物理的セキュリティ対策

①目的

- ・許可されないアクセスからの不正なアクセスの防止
- ・許可されたアクセスの誤使用の防止
- ・印刷物等の盗難又は紛失による情報漏えいの防止

②管理策

設置にあたっては、印刷物等が第三者による意図しない参照又は盗難を予防できる場所とする等、適切な管理を行う。また、利用後の原紙や印刷物等の長時間の放置や取り忘れを防止する。

(4) 装置の廃棄又はリース機器の返却

①目的

- ・廃棄装置からの情報漏えいの防止
- ・返却装置からの情報漏えいの防止

②管理策

廃棄又は返却時は、データの完全消去やハードディスク等を物理的に破壊するなど、各システム管理者が責任をもって実施する。