6.4　物理的安全対策

B. 考え方

物理的安全対策とは、情報システムにおいて個人情報が入力、参照、格納される情報端末やコンピュータ、情報媒体等を物理的な方法によって保護することである。具体的には情報の種別、重要性と利用形態に応じて幾つかのセキュリティ区画を定義し、以下の事項を考慮し、適切に管理する必要がある。

① 入退館（室）の管理（業務時間帯、深夜時間帯等の時間帯別に、入室権限を管理）
② 盗難、窃視等の防止
③ 機器・装置・情報媒体等の盗難や紛失防止も含めた物理的な保護及び措置

なお、情報及び情報機器を医療機関等以外に持ち出して取り扱う場合についての詳細については、別途、「6.9　情報及び情報機器の持ち出しについて」に記載しているので参照されたい。

C. 最低限のガイドライン

1. 個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。
2. 個人情報を入力、参照できる端末が設置されている区画は、業務時間帯以外は施錠等、運用管理規程に基づき許可された者以外立ち入ることが出来ない対策を講じること。

   ただし、本対策項目と同等レベルの他の取りうる手段がある場合はこの限りではない。
3. 個人情報の物理的保存を行っている区画への入退管理を実施すること。例えば、以下のことを実施すること。
   - 入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録する。
   - 入退者の記録を定期的にチェックし、妥当性を確認する。
4. 個人情報が存在する PC 等の重要な機器に盗難防止用チェーンを設置すること。
5. 窃視防止の対策を実施すること。

D. 推奨されるガイドライン

1. 防犯カメラ、自動侵入監視装置等を設置すること。