

JIPDECガイドラインとISO17799:2005との対比から見る情報セキュリティツールの必要性

JIS Q 15001をベースにした個人情報保護マネジメントシステム実施のためのガイドライン

具体的措置としての参考
(ISO17799 管理策No.)

ツールによる措置の必要性と特徴

1. 物理的安全管理措置

1.2 盗難等の防止

- | | | |
|--|-------------------------------|---------------------------------|
| ② 個人情報を取扱うPCの操作において、離席時は、パスワード付きスクリーンセーバーの起動又はログオフを実施している。 | A.11.3.3 b) クリアデスク・クリアスクリーン方針 | 離席時の意図しない使用を避けるための ロック機能 |
| ⑤ 個人情報を記録した媒体(記録媒体、紙)の廃棄は、再利用できない措置を講じている。 | A.10.7.2 媒体の処分 | データの 再利用の防止機能 (シュレッダーなど) |

1.3 機器・装置等の物理的な保護

- | | | |
|--|---|---|
| ① 個人情報を取扱う機器・装置等について、安全管理上の脅威(盗難、破壊、破損等)や環境上の脅威(漏水、火災、停電、地震等)からの物理的な保護装置がある。 | A.9.1.1 物理的セキュリティ境界
A.9.1.4 外部及び環境の脅威からの保護 | 侵入者を検地するシステム、安全な距離をといった データのバックアップ機能 等 |
|--|---|---|

2. 技術的安全管理措置

2.1 個人情報へのアクセスにおける識別と認証

- | | | |
|--|---|---|
| ① 個人情報へのアクセスにおいて、識別情報(ID、パスワード等)による認証が実施されている。 | A.11.5.2 利用者の識別及び認証
A.11.5.3 パスワード管理システム | 適切な 認証技術 |
| ④ 識別情報は平文で記録していない。 | A.11.5.3 i) パスワード管理システム | 暗号化 |
| ⑥ 個人情報へのアクセス権限を有する従業者が使用できる端末又はアドレス等は、MACアドレス認証、IPアドレス認証、電子証明書や秘密分散技術を用いた認証等により、制限されている。 | A.11.4.3 ネットワークにおける装置の識別 | 装置識別における、装置に内蔵された又は付属した 識別子による認証 等 |

2.2 個人情報へのアクセス制御

- | | | |
|--|-------------------------|----------------------------------|
| ① 個人情報にアクセスできる従業者の数は必要最小限である。 | A.11.4.7 ネットワークルーティング制御 | ネットワーク経路 を予め指定する |
| ⑥ 個人情報を格納した情報システムを無権限アクセスから保護している。(例えば、ファイアウォール、ルータ等の設定) | A.11.4.5 ネットワークの領域分割 | ファイアウォール、ルーティング 等 |
| ⑦ 個人情報にアクセス可能なアプリケーションの無権限利用を防止している。 | A.11.6.1 情報へのアクセス制限 | 各業務で必要な機能につりあ うアクセス権 を与える |

2.4 個人情報へのアクセス記録

- | | | |
|--------------------------------------|------------------|------------------|
| ① 個人情報へのアクセスや操作の成功と失敗の記録を取得し、保管している。 | A.10.10.1 監査ログ取得 | ログ監視ソフト 等 |
| ② 取得した記録について、漏えい、滅失及びき損から適切に保護している。 | A.10.10.1 監査ログ取得 | ログ監視ソフト 等 |

2.5 個人情報を取扱う情報システムに関する不正ソフトウェア対策

- | | | |
|--|--------------------------|----------------------|
| ① ウイルス対策ソフトウェアが導入され、常に最新版が適用されている。 | A.10.4.1 悪意のあるコードに対する管理策 | ウイルスソフト 等 |
| ② OSやアプリケーション等に対するセキュリティ対策用修正ソフトウェア(いわゆるセキュリティパッチ)を適用している。 | A.10.4.1 悪意のあるコードに対する管理策 | 修復ソフトウェア の導入等 |

2.6 個人情報の移送・通信時の対策

- | | | |
|---|----------------------|--------------|
| ② 個人情報を媒体で移送する時に、移送時の紛失・盗難が生じた際の対策が講じられている。 | A.10.8.3 配送中の物理的媒体 | 暗号化 等 |
| ③ 盗難される可能性のあるネットワーク(例えばインターネットや無線LAN等)で個人情報を送信(例えば本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等)する際に、個人情報の暗号化又はパスワードロック等を実施している。 | A.10.8.1 情報交換の方針及び手順 | 暗号化 等 |