

10. パスワードを利用者識別に使用する場合

システム管理者は以下の事項に留意すること。

- (1) システム内のパスワードファイルでパスワードは必ず暗号化(可能なら不可逆変換が望ましい)され、適切な手法で管理及び運用が行われること。(利用者識別に IC カード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理規程にて定めること)
- (2) 利用者がパスワードを忘れてたり、盗用されたりする恐れがある場合で、システム管理者がパスワードを変更する場合には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載(本人確認を行った書類等のコピーを添付)し、本人以外が知りえない方法で再登録を実施すること。
- (3) システム管理者であっても、利用者のパスワードを推定できる手段を防止すること。(設定ファイルにパスワードが記載される等があってはならない。)

また、利用者は以下の事項に留意すること。

- (1) パスワードは定期的に変更し(最長でも 2 ヶ月以内)、極端に短い文字列を使用しないこと。英数字、記号を混在させた 8 文字以上の文字列が望ましい。
- (2) 類推しやすいパスワードを使用しないこと。

11. 無線 LAN を利用する場合

システム管理者は以下の事項に留意すること。

- (1) 利用者以外に無線 LAN の利用を特定されないようにすること。例えば、ステルスモード、ANY 接続拒否等の対策をとること。
- (2) 不正アクセスの対策を施すこと。少なくとも SSID や MAC アドレスによるアクセス制限を行うこと。
- (3) 不正な情報の取得を防止すること。例えば WPA2/AES 等により、通信を暗号化し情報を保護すること。
- (4) 電波を発する機器(携帯ゲーム機等)によって電波干渉が起こり得るため、医療機関等の施設内で利用可能とする場合には留意すること。
- (5) 無線 LAN の適用に関しては、総務省発行の「安心して無線 LAN を利用するために」を参考にすること。

<b>D. 推奨されるガイドライン</b>
-----------------------

1. 情報の区分管理を実施し、区分単位でアクセス管理を実施すること。
2. 離席の場合のクローズ処理等を施すこと(クリアスクリーン: ログオフあるいはパスワード付きスクリーンセーバー等)。
3. 外部のネットワークとの接続点や DB サーバ等の安全管理上の重要部分にはファイアウォール(ステートフルインスペクションやそれと同等の機能を含む)を設置し、ACL(アクセス制御リスト)等を適切に設定すること。