

業履歴から作業者が特定できない。

- ・ ひとつの ID を複数の利用者が使用している。
- ・ 容易に推測できる、あるいは、文字数の少ないパスワードが設定されており、容易にパスワードが推測できてしまう。
- ・ パスワードを定期的に変更せずに使用しているために、パスワードが推測される可能性が高くなっている。
- ・ 認証用の個人識別情報を格納するセキュリティ・デバイス（IC カード、USB キー等）を他人に貸与する、または持ち主に無断で借用することにより、利用者が特定できない。
- ・ 退職した職員の ID が有効になったままで、ログインができてしまう。
- ・ 医療情報部等で、印刷放置されている帳票等から、パスワードが盗まれる。
- ・ コンピュータウイルスにより、ID やパスワードが盗まれ、悪用される。

<認証強度の考え方>

ID・パスワードの組合せは、これまで広く用いられてきた方法である。しかし、ID・パスワードのみによる認証では、上記に列挙したように、その運用によってリスクが大きくなる。認証強度を維持するためには、交付時の初期パスワードの本人による変更や定期的なパスワード変更を義務づける等、システムの実装や運用を工夫し、必ず本人しか知り得ない状態を保つよう対策を行う必要がある。

このような対策を徹底することは一般に困難であると考えられ、その実現可能性の観点からは推奨されない。

認証に用いる手段としては、ID・パスワードの組合せのような利用者の「記憶」によるもの、指紋や静脈、虹彩のような利用者の生体的特徴を利用した「生体計測」（バイオメトリクス）によるもの、IC カードのような「物理媒体」（セキュリティ・デバイス）によるものが一般的である。認証におけるセキュリティ強度を考えた場合、これらのいずれの手段であっても、単独で用いた場合に十分な認証強度を保つことは一般には困難である。そこで、IC カード等のセキュリティ・デバイス＋パスワードやバイオメトリクス＋IC カードのように利用者しか持ち得ない 2 つの独立した要素を用いて行う方式（2 要素認証）を採用することが望ましい。

また、入力者が端末から長時間、離席する場合には、正当な入力者以外の者による入力を防止するため、クリアスクリーン等の防止策を講じるべきである。

<IC カード等のセキュリティ・デバイスを配布する場合の留意点>

利用者の識別や認証、署名等を目的として、IC カード等のセキュリティ・デバイスに個人識別情報や暗号化鍵、電子証明書等を格納して配布する場合は、これらのセキュリティ・デバイスが誤って本人以外の第三者の手に渡ることのないような対策を講じる必要が