2.6.14. 作業者アクセス及び作業者ＩＤの管理

⑴　作業者は情報処理装置上においてユニークな作業者ＩＤにより識別されること。

⑵　作業者ＩＤを発行する際に、既存のＩＤとの重複を排除する仕組みを導入すること。

⑶　複数作業者で共用するためのグループＩＤの利用は原則として行わず、業務上必要であれば、ログ上で操作の実施者が特定できるように、作業者ＩＤでログオンしてからグループＩＤに変更する仕組みを利用すること。

⑷　作業者ＩＤの発行は医療情報システムの管理に必要な最小限の人数に留めること。

⑸　作業者が変更あるいは退職した際には、ただちに当該作業者ＩＤを利用停止とすること。

⑹　監視ログの監査時に作業者を確実に特定するため、作業者ＩＤは過去に使われたものを再利用しないこと。

⑺　不要な作業者ＩＤが残っていないことを定期的に確認すること。

⑻　特権ＩＤの発行は必要な最小限のものに留めること。

⑼　特権使用者に昇格可能な作業者ＩＤを制限すること。

⑽　特権の使用時には作業実施内容を記録すること。

⑾　管理端末以外からの特権ＩＤによる直接ログオンを禁止すること。

⑿　情報処理装置及びソフトウェアを使用する前に、製造ベンダが設定したデフォルトのアカウント及びメンテナンス用のアカウント等、必要のないアカウントについては削除あるいはパスワード変更を行うこと。

⒀　医療情報システムへのログオン用パスワードはハッシュ値での保存、暗号化等、パスワードを容易に復元できない形で情報を保管すること。

⒁　医療情報システムへのログオン用パスワードには有効期限の設定を行い、定期的な変更を作業者に強制すること。

⒂　医療情報システムへのログオン用パスワードの履歴管理を導入し、変更時には一定数世代のパスワードと同じパスワードを再設定することができないようにすること。

⒃　パスワード変更時には変更前のパスワードの入力を要求し、変更前のパスワード入力を一定回数以上失敗した場合には、パスワード変更を一定期間受けつけない機構とすること。

⒄　パスワード発行時には、乱数から生成した仮の医療情報システムへのログオン用パスワードを発行し、最初のログオン時点で強制的に変更させる等パスワード盗難リスクに対する対策を実施すること。

⒅　パスワードの満たすべき品質の基準を策定し、すべてのパスワードが品質基準を満たしていることを確実とすること。

⒆　パスワードをシステムに記憶させる自動ログオン機能を利用しないよう作業者に徹底すること。

⒇　パスワードに関連するデータを保存するファイルの真正性及び完全性を保つために、ファイルのハッシュ値の取得及び検証、ファイルに対するデジタル署名の付与及び検証、ファイルを暗号化して保存する等の保護策を採用すること。また、一般の作業者による閲覧を制限すること。

(21)　端末又はセッションの乗っ取りのリスクを低減するため、作業者のログオン後に一定の使用中断時間が経過したセッションを遮断、あるいは強制ログオフを行うこと。

(22)　パスワード入力が不成功に終わった場合の再入力に対して一定の不応時間を設定すること。連続してログオンが失敗した場合は再入力を一定期間受付けない機構とすること。この場合には、警告メッセージをシステムの管理者に送出する仕組みを導入すること。

2.6.15. 作業者の責任及び周知

各作業者に対しては、自己の責任範囲を認識し、責任を果たすことを周知することが必要である。以下の管理策について作業者に対し周知し、理解したことを確認すること。

⑴　各作業者は自身のパスワードを秘密にし、パスワードを記録する必要がある場合は、安全な場所に保管して、他者による閲覧、修正、廃棄等のリスクから保護すること。

⑵　システムに許可なくアクセスされた疑いがあるとき又はパスワードが第三者に知られた可能性がある場合には、直ちにパスワードを変更あるいはアカウントを無効化し管理者に通知すること。

⑶　離席時及び非利用時には、端末をロックする、あるいはログオフして第三者の利用を未然に防ぐこと。

2.7. 人的安全対策

医療情報処理を受託する情報処理事業者において医療情報処理に関する管理を的確に行うため、医療情報に触れる機会を持つ情報処理事業者職員は、原則として情報処理事業者の正規職員に限ることを原則とするが、雇用形態が多様化している実態を踏まえ、派遣従業員等の非正規職員についても、秘密保持契約や情報セキュリティ教育等の履行に万全を期し、正規職員のみによる管理と同等レベルの管理が行われることを前提として、認めることとする。

⑴　医療情報を操作する可能性のある情報処理事業者職員の全てについて、雇用契約時あるいは医療情報を扱う職務に着任する際の条件として秘密保持契約への署名を求めること。派遣従業員については秘密保持義務及び継続的な情報セキュリティ教育を課すことを条件に選定、派遣することを求めること。

⑵　医療情報を操作する可能性のある情報処理事業者職員の全てに情報セキュリティに関する教育を行い、一定水準の理解を得たものだけを選定すること。派遣従業員に関しては、派遣元に対し、情報セキュリティに関する一定水準の知識、理解を持つ、あるいは持つことができる人員を選定、派遣することを求め、受入れ後に正規職員同等の教育を行うこと。この教育は新しい脅威や情報セキュリティ技術の推移に合わせて定期的に行うこと。

⑶　情報処理事業者職員による安全管理策違反の疑いが発生した際には、ただちに医療情報へのアクセス権を停止し、改ざん又は破壊等の行為が行われていないことを検証すること。

⑷　医療情報を操作する情報処理事業者職員が退職する際には、貸与された情報資産の全てについて返却し、返却が完全であることを確認するための台帳及び返却確認手続きを予め規定しておくこと。また、業務上知りえた医療情報について退職後も秘密として管理することを記した合意書への署名を求めること。派遣従業員については、派遣契約解除時に同等の合意書への署名を求めること。

⑸　医療機関等との委託契約において、情報処理事業者職員との秘密保持契約を結ぶこと、情報セキュリティ教育を受けさせること、及び、規定に反して預託情報を不正に扱った際の懲罰規定等、預託情報の機密管理に関する条項を設けること。

2.8. 情報の破棄

⑴　ＣＤ－Ｒ等の廃棄については「2.6.7. 電子媒体の取扱」を参照すること。

⑵　ハードディスク等の廃棄については「2.5.4. 情報処理装置の廃棄及び再利用に関する要求事項」を参照すること。

⑶　情報処理事業者は「医療情報システムの安全管理に関するガイドライン」に従って情報の破棄を行った記録を提出すること。

2.9. 医療情報システムの改造と保守

オペレーティングシステムのアップグレード、セキュリティパッチの適用を行う場合、医療情報システムに対する影響を評価し、試験結果を確認してから実施すること。

2.10. 医療情報処理に関する事業継続計画

2.10.1. 要求事項の識別

⑴　医療情報処理に関わる業務プロセス（プロセスを実施するための作業員を含む）、情報処理設備等について識別すること。

⑵　業務プロセス間の相互関係を評価すること。

⑶　事業を継続するための業務プロセスの優先順位を明確にすること。