⑾　起動パスワードを設定しても合理的に運用が可能な情報処理装置に対しては起動パスワードを設定すること。設定されるパスワードの品質、管理については「2.6.14.作業者アクセス及び作業者ＩＤの管理」に従うこと。

⑿　情報処理装置の障害発生時においても業務を継続できるよう、代替機器の準備、冗長化、バックアップ施設の設置等の対策を実施すること。

⒀　不正な情報処理装置がネットワークに接続されることの悪影響を避けるため、登録されたネットワークアドレスとの整合性、悪意のあるプログラムに未感染であること、脆弱性パッチが適用されていること等を接続前に検査を行う仕組みを整備運用すること。

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

⑴　ハードディスク等を医療情報システム内の別の機器で再利用する場合には、再利用前に、複数回のデータ書き込みによる元データの消去等の確実な方法でデータを消去し、再利用前に情報が消去されていることを確認すること。

⑵　サーバ等のＢＩＯＳパスワード、ハードディスクパスワード等のハードウェアに対するパスワードを設定している場合には、それらを消去すること。

⑶　ハードディスクを機器に接続する際には、再利用であるかどうかに関わらず、検証用の機器で不正なプログラム等が記録されていないことを検証すること。

⑷　ハードディスクの廃棄については、再利用及びデータの読み出しが不可能となるよう、複数回のデータ書き込みによる元データの消去、強磁気によるデータ消去措置、物理的な破壊措置（高温による融解、裁断等）等を適用し、当該装置に実施した措置の概要の記録（対象機器の形式、管理番号、作業担当者、作業実施日時、作業内容等）について、医療機関等の求めに応じ、速やかに提出できるよう整備すること。

2.5.5.情報処理装置の外部への持ち出しに関する要求事項

利用中の情報処理装置を外部に持ち出す行為は原則として禁止するが、製造元でのみ可能な補修が必要な場合など、止むを得ない事情により外部への持ち出しを行う場合には、以下の管理策を適用すること。

⑴　情報処理装置が設置されている室内及び情報処理事業者の管理する領域から持ち出す場合に備え、適切な持ち出し手順を策定すること。

⑵　持ち出した機器を再度設置するための適切な検証手順を策定すること。

2.6.技術的安全対策

2.6.1.情報処理装置及びソフトウェアの保守

⑴　保守に伴う情報処理装置及びソフトウェアの変更がもたらす影響の評価を行うこと。

⑵　変更が既存の業務及び設備に悪影響を及ぼす可能性がある場合には、安全なデータの保存を保証するため、影響を最小限に抑える方策を検討すること。

⑶　医療情報を保存・交換するためのデータ形式、プロトコルが変更される場合、変更前のデータ形式、プロトコルを使用する医療機関等が存在する間、以前のデータ形式、プロトコルの利用をサポートすること。

⑷　情報処理装置及びソフトウェアの保守作業については、情報処理業務の停止時間を最小限に留めるように計画を立てて実施すること。

⑸　情報処理装置及びソフトウェアの適切な変更手順を策定すること。保守作業については十分な余裕を持って事前に医療機関等に通知し承認を受けること。

⑹　不正な改ざんを受けていないことを検証するため、定期的にソフトウェアの整合性検査（改ざん検知）を実施すること。

⑺　医療情報システムに関連する技術的脆弱性については台帳等を利用して管理すること。

⑻　潜在的な技術的脆弱性が特定された場合には、リスク分析を行った上で必要な処置（パッチ適用、設定変更等）を決定すること。

⑼　修正パッチの適用前にパッチが改ざんされていないこと及び有効性を検証すること。

⑽　保守作業を外部事業者に再委託する場合には、上記要件を満たしていることを確認して選定し、「2.6.5.第三者が提供するサービスの管理」の管理策を実施すること。選定した外部事業者について医療機関等に報告し、合意を得ること。

2.6.2.開発施設、試験施設と運用施設の分離

⑴　情報処理に供するアプリケーションについては、情報処理事業者自身で開発したアプリケーションを用いること。外部開発事業者が開発したアプリケーションを用いる場合には、事前に安全性を十分に検証した上で用いること。

⑵　ソフトウェア開発を行う際には、ソフトウェア障害の影響を避けるため、運用施設とは直接に接続されていない開発用の情報処理施設（以下、「開発施設」という。）を用いて行うこと。

⑶　開発施設では、悪意のあるコードが混入することを避けるため、不特定多数が利用するネットワーク（インターネット等）と接続を持つ場合には「2.6.3.悪意のあるコードに対する管理策」に従うこと。

⑷　不正なソフトウェアの書き換えリスクを避けるため、開発したソフトウェアを運用施設に導入する際、ソフトウェアに対する改ざん防止、検知策を実施すること。

⑸　運用施設に保存されている医療情報を開発施設及び試験施設にコピーしないこと。

⑹　医療情報を開発及び試験用データとして直接、利用しないこと。利用する場合には、個人情報の消去及び元のデータを復元できないように一部データのランダムデータとの入れ替え等のデータ操作を定め、十分な安全性が保証されていることを医療機関に示し、了解を得た上で利用すること。

2.6.3.悪意のあるコードに対する管理策

⑴　最新の脅威についての情報収集に努め、導入している悪意のあるコード対策ソフトウェアの対応範囲を確認し、対策漏れが無いことを確認すること。対応すべき脅威の例としては、コンピュータウイルス（ワーム）、バックドア（トロイの木馬）、スパイウェア（キーロガー）、ボットプログラム（ダウンローダー）等がある。

⑵　悪意のあるコード対策ソフトウェアにおいて次の設定が行われていること。

・リアルタイムスキャン（ディスク書き出し・読み込み、ネットワーク通信）
・リスク評価の結果として必要であれば定期的にスキャンを実施
・電子媒体へのデータ書き出し・読み込み時におけるオンデマンドスキャン
・定義ファイル、スキャンエンジンの自動アップデート又は十分な頻度による手動での更新
・管理者以外による設定変更やアンインストールの禁止

⑶　一定期間、悪意のあるコードのチェックが行われていない場合や定義ファイル、スキャンエンジンが更新されていない機器については、利用者への警告を表示する、管理者への通知を行う、施設内ネットワーク接続の禁止又は隔離措置をとるといった対策が行われていること。

2.6.4.ウェブブラウザを使用する際の要求事項

医療情報システム内で必要とする、ネットワーク監視ソフトウェア、サーバ制御ソフトウェア等でユーザインタフェースとしてウェブブラウザを使用する場合は、以下の要求事項を満足する体制を確立すること。

⑴　ウェブブラウザの接続するサーバを業務上必要なサーバに限定すること。

⑵　ウェブブラウザの設定で、認可していないサイトから、ActiveX、Javaアプレット、Flash等のコードをダウンロード及び実行することができない設定になっていること（管理ソフトウェアが実行されるサーバのみを認可する。）。

⑶　認可したサイトからダウンロードされるコードについても「2.6.3.悪意のあるコードに対する管理策」に即して検査されること。