2.6.8. 情報交換に関するセキュリティ

⑴　医療機関等と情報処理事業者間の情報交換に関して、次の事項を予め合意しておくこと。
・情報を電子媒体に記録して交換する際の手順
・情報をネットワーク経由で文書ファイル形式にて交換する際の手順
・情報をネットワーク経由でアプリケーション入力にて交換する際の手順
・情報に電子署名、タイムスタンプを付与する場合、その方式及び検証手順

⑵　情報交換手順では搬送の形態によらず次の事項を確実にすること。
・発送者、受領者を識別し記録すること。
・発送者の行為を後に否定できないように、発送伝票の保存、文書ファイルへの電子署名付与、アプリケーションログオン時の確実な認証等、否認防止策を行うこと。
・交換する情報の機密レベルに関して合意すること（受領側で機密レベルが低くならないこと。）。
・交換された情報に悪意のあるコードが含まれていないことを確実とすること。

⑶　物理的に情報を搬送する際には以下の対策を実施すること。
・医療機関等が合意する基準にもとづいて信頼できる配送業者を選択すること。
・配送時の作業者については、発送元、受領先の双方で身分確認を行い第三者によるなりすましを防ぐこと。
・配送業者等による電子媒体の抜き取り等を防ぐため、交換する電子媒体の数と種類について、予め情報交換して受領時に欠損が無いことを確認すること。
・配送業者等による電子媒体からの情報の抜き取りを防ぐため、不正な開封を検出することのできるコンテナ等を利用すること。
・電子媒体を発送、受領する際は、配送業者と直接行い、第三者を介さないこと。
・電子媒体により情報を交換する場合、移送中の安全管理上のリスクがある場合には電子媒体内のデータに暗号化を施すこと。

⑷　電子的に情報を転送する際には以下の対策を実施すること。
・送信者、受信者は相互に電子的に認証を行って相手の正当性を検証すること。認証方式は接続形態、転送に利用するアプリケーションによって異なるが、利用する機器同士及び利用者同士を認証することが望ましい。
・送受信する経路は適切な方法で傍受のリスクから保護されていること。
・受信した情報について経路途中での損傷、改ざんが無いことを検証する対策を講じること。
・送受信に失敗する時には、予め規定された回数を上限として再送受信を試み、上限に達した際には送受信者間の全ての通信を停止し、障害の特定等の作業を実施すること。

2.6.9. 医療情報システムに対するセキュリティ要求事項

⑴　運用システムの混乱を避けるため、開発用コード又はコンパイラ等の開発ツール類を運用システム上に置かないこと。

⑵　情報処理に不必要なファイル等を運用システム上におかないこと。

⑶　業務に供するソフトウェア及びオペレーティングシステムソフトウェアについて、十分な試験を行った上で導入すること。

⑷　運用システムに関わるライブラリプログラムの更新については監査に必要なログを取得すること。

⑸　システム運用情報（システム及びサービス設定ファイル等）の複製及び利用については監査証跡とするためにログを取得すること。

2.6.10. アプリケーションに対するセキュリティ要求事項

⑴　提供するアプリケーションについては、アプリケーションの種別による特定の脆弱性検出を含む安全性診断を定期的に行い、その結果に基づいて対策を行うこと。医療機関等とのデータ送受信の際にはデータの完全性を検証する機構を導入すること。

⑵　アプリケーション及びアプリケーション稼動に利用する第三者のソフトウェア（ライブラリ、サーバプロセス等）については、公開される最新の脆弱性情報を参照し、迅速に対応策をとること。

⑶　アプリケーションにて情報の登録、編集、削除等を行う際には、ユーザを特定し、権限を確認するため、ログオンを行うよう設計及び実装を行うこと。

⑷　アプリケーションにて医療事業者側の作業者を認証する情報（ＩＤ／パスワード認証の際のパスワード）は、十分な強度を持ったハッシュ関数の出力値として保存する、あるいは暗号化して保存すること。

⑸　アプリケーションによる情報操作については、医療機関等の職務権限に応じたアクセス管理を可能とし、正当なアクセス権限を持たないものによる情報の生成、編集、削除等を防止すること。

2.6.11. 暗号による管理策

アプリケーション及び情報処理装置で暗号を利用する場合には、以下の管理策を適用すること。

⑴　暗号アルゴリズムは十分な安全性を有するものを使用すること。選択基準としては電子政府推奨暗号リスト等を用いること。

⑵　暗号鍵が漏洩した場合に備えた対応策を策定しておくこと。

⑶　電子署名、ネットワーク接続等に電子証明書を利用する場合、電子証明書は信頼できる組織によって発行されたものとすること。

⑷　暗号アルゴリズム及び暗号鍵の危殆化に備え、暗号アルゴリズムを切り替えることができるように配慮すること。

⑸　医療機関等から受け付けるデータを検証するためのルート認証機関の公開鍵証明書は安全な経路で入手し、別の経路で入手したフィンガープリントと比較して、真正性を検証すること。

2.6.12. ログの取得及び監査

⑴　作業者の活動、機器で発生したイベント、システム障害、システム使用状況等を記録した監査ログを作成し管理すること。

⑵　監査ログを定期的に検証して不正な行為、システムの異常等を検出すること。

⑶　ログを利用して正確に事故原因等を検証するため、医療情報システムのすべてのサーバ機器等の時刻を時刻サーバ等の提供する標準時刻に同期しておくこと。

⑷　標準時刻に同期するための時刻提供元は信頼できる機関を利用すること。

⑸　ログ情報を不正なアクセスから適切に保護するため以下の管理策を適用すること。
・ログデータにアクセスする作業者及び操作を制限すること。
・容量超過によりログが取得できない事態を避けるため、ログサーバの記憶容量を常時監視し、電子媒体への書き出し、容量の増強等の対策をとること。
・ログデータに対する不正な改ざん及び削除行為に対する検出・防止策を施すこと。

2.6.13. アクセス制御方針

⑴　情報処理に用いる情報処理装置それぞれのセキュリティ要求事項を整理すること。

⑵　情報処理に用いるソフトウェアそれぞれのセキュリティ要求事項を整理すること。

⑶　アクセス権限の登録申請、変更申請、廃棄申請、及びそれらの承認、定期的な検証プロセスを規定すること。

⑷　それぞれの情報にアクセスする権限を持つ作業者を最小限に抑えるよう、適切に情報のグルーピングを行い、情報のグループに対するアクセス制御を行うこと。

⑸　業務内容を考慮した必要最小限のアクセス権限を設け、アプリケーションやオペレーションシステムでの権限を設定すること。