2　鍵等の管理
イ　重要機能室の出入口の鍵は所定の場所に保管し、その管理は定められた者が行うこと。
ロ　入退室管理カード又は生体認証情報等の管理方法を定めること。
3　搬出入物品の確認
重要機能室への搬出入物品は、重要機能室に入室する権限を有する職員が内容を確認すること。
4　事務室の管理
事務室における本システムの構成機器、関連設備等の盗難、損壊等を防止するため、職員が不在となる時の事務室の施錠等、必要な措置を講ずること。
二　ソフトウェア開発等の管理
1　セキュリティを高める設計の実施
本システムの開発又は変更を行う際には、本システムのセキュリティを高める設計を行うこと。
2　本システムの試験の実施
本システムの開発又は変更を行った場合には、試験を適切に実施すること。また、試験の実施に当たっては、ファイルの安全を確保するため、別途の試験環境の用意その他の適切な措置を講ずること。
3　本システムの開発等に際してのエラー及び不正行為の防止
イ　本システムの開発又は変更を行う際には、本システムの開発又は変更の計画を策定すること、本システムの開発又は変更の責任者を指定すること、プログラムの作成、変更又は廃止は責任者の承認を得て行うこと等エラー及び不正行為の防止のための手続を明確にすること。
ロ　本システムの開発又は変更の各段階で使用するドキュメントの様式を標準化すること。
ハ　本システムの変更に応じてドキュメントを更新し、責任者が確認すること。
三　本システムの管理
1　アクセス権限の限定
本システムを運用する職員に対して、電子計算機、端末機、電気通信関係装置、電気通信回線、ファイル等に関し、必要なアクセス権限を付与すること。
2　ファイアウォールによる通信制御
電気通信回線に接続する電子計算機における不正行為又は電子計算機への不正アクセス行為に対して本システムを保護するため、連携サーバ及び情報連携端末等の必要な部分には、ファイアウォールを設置し、通信制御を行うこと。
3　電気通信関係装置の管理
エラー及び不正行為により電気通信関係装置の不当な運用が行われないようにするため、電気通信関係装置の管理に際しては厳重な確認を行う等、管理権限がある者以外の者による操作を防止するための措置を講ずること。
4　通信相手相互の認証
連携サーバと情報連携端末等との間の通信については、通信相手相互の認証を行うこと。
5　模擬攻撃の実施
ネットワーク経由の模擬攻撃を適宜実施し、その実施結果に基づき必要な措置を講ずること。
6　情報収集等
セキュリティ対策に関する情報を収集し、分析を行い、必要な措置を講ずること。
四　情報連携端末等操作の管理
1　情報連携端末等の管理
情報連携端末等の取扱いは、当該情報連携端末等の管理を行う責任者の指示又は承認を受けた者が行うこと。
2　情報連携端末等の操作者の確認
情報連携端末等の取扱いに際しては、操作者が正当なアクセス権限を有していることを、暗証番号又はこれと同等以上のものと認められる方法により確認すること。
3　暗証番号の取扱い
暗証番号の管理方法を定め、操作者は当該管理方法を遵守すること。
4　操作履歴の記録等
情報連携端末等を操作した履歴を、適切に記録し管理すること。
5　強制的に終了する機能
情報連携端末等には、複数回のアクセスの失敗に対して、強制的に終了する機能を設けること。
6　データの暗号化
連携サーバと情報連携端末との間の法務省通知及び市町村通知に関する通信については、交換するデータの暗号化を実施すること。
五　電子計算機の管理
1　秘密鍵の管理
暗号化等に必要な秘密鍵について、外部に漏えいすることを防止するための適切な措置を講ずること。
2　他のソフトウェアの作動禁止
情報連携端末等では、原則として本システムの管理及び運用に必要なソフトウェア以外のソフトウェアを作動させないこと。
六　磁気ディスクの管理
1　保管場所
磁気ディスクは、保管庫等を設けること等により、できるだけ常温常湿の場所に保管すること。
2　持ち出し及び返却の確認等
イ　磁気ディスクの盗難の防止等のため、その保管位置を指定し、持ち出し及び返却の措置を講ずること。
ロ　重要な磁気ディスクは他の磁気ディスクと判別することができるようにすること。
七　構成機器及び関連設備等の管理
1　管理方法の明確化
イ　本システムに機器を接続するための手続、方法等を定めるとともに、構成機器、関連設備等の管理方法を明確にすること。
ロ　利用するハードウェア、ソフトウェア及び磁気ディスクの種類、数量等を文書等で体系的かつ一元的に記録管理し、現況と一致させること。また、これを関係職員に周知し、管理しているハードウェア、ソフトウェア又は磁気ディスク以外のものを使用しないこと。
2　保守の実施
本システムの構成機器及び関連設備の保守を定期に又は随時に、実施すること。また、保守の実施に当たっては、エラー及び不正行為を防止し、データを保護するため、必要な措置を講ずること。