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住居地伝達等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。
3　不正プログラムの混入防止等
本システムにコンピュータウイルス等の不正プログラムが混入されていないかどうかを監視する措置を講じ、混入されていた場合には駆除する措置を講ずること。また、コンピュータウイルス等の不正プログラムが発見された場合の必要な措置を定め、本システムを運用する職員に周知すること。

八　データ、プログラム、ドキュメント等の管理
1　データ等の取扱い及び管理
イ　データ、プログラム及びドキュメントについては、定められた場所に保管すること、受渡し及び保管に関し必要な事項を記録すること、使用、複写、消去及び廃棄は責任者の承認を得て行うとともにその記録を作成すること等、その取扱い及び管理の方法を明確にすること。
ロ　データ、プログラム及びドキュメントの内容については、最新の状態にしておくこと。
ハ　データ、プログラム及びドキュメントを変更した場合については、変更者及び版数の管理を行うこと。
ニ　プログラムの改ざん、消去等を防止するために、プログラムの登録及び抹消は、責任者の指示又は承認を受けた者が行うこと。
ホ　データ、プログラム及びドキュメントを廃棄する場合には、消磁、破砕、溶解等の措置を講ずること。
ヘ　市町村長は、法務大臣からデータ、プログラム及びドキュメントの返却又は廃棄を求められたときは、これに応じるよう努めること。
2　帳票の管理
イ　未使用の重要な帳票の在庫管理及び廃棄の方法を定めること。また、重要な印字済みの帳票の受渡し及び廃棄の方法を定めること。
ロ　事務室の出力装置から出力する場合のデータの漏えいを防止するため、必要な措置を講ずること。

九　障害時等の対応
1　障害の早期発見
イ　連携サーバの障害箇所を発見するための機能を整備すること。
ロ　情報連携端末等については、日常的な運用において障害箇所の早期発見に努めること。
2　早期回復のための代替機能等の整備
イ　本システムの重要な構成機器及び関連設備について、障害が発生したときに代替することができる機能を整備する等、必要な措置を講ずること。
ロ　あらかじめ定められた作業手順に従って代替機能等が確実に機能することを、試験等により確認すること。
ハ　連携サーバの重要なファイルについては、他の磁気ディスクに複製することとし、必要に応じ、複製された磁気ディスクを当該ファイルを記録した磁気ディスクとは別に保管すること。
ニ　障害が発生したときに、複製された重要なファイル等を基に速やかに連携サーバを回復させるための機能を整備すること。
3　不正アクセスの早期発見
連携サーバにおいて、不正アクセスを早期に発見するための機能を整備すること。
4　不正アクセスが判明した場合の対応
法務大臣は、不正アクセスが判明した場合、市町村長と連絡調整を行い、被害状況の把握、被害拡大を防止するための措置等必要な措置を講ずること。

十　委託を行う場合等の措置
1　委託先事業者等の社会的信用の確認等
法務大臣が本システムの開発、変更、運用、保守等について委託を行う場合は、委託先事業者等の社会的信用及び能力を確認すること。また、委託先事業者等に対し、この基準と同様のセキュリティ対策を実施させるとともに、適切な監督を行うこと。さらに、委託先事業者等による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。