二　障害の防止等
1　電気的・機械的障害の防止等
戸籍副本データ管理システムの構成機器又は関連設備の電気的・機械的障害の発生を防止し、これらの障害の発生を検知し、及びこれらの障害が発生した場合の対策を図るため、必要な設備の整備等について適切な措置を講ずること。
2　水又は蒸気による障害の防止等
戸籍副本データ管理システムの構成機器の水又は蒸気による障害の発生を防止し、これらの障害の発生を検知し、及びこれらの障害が発生した場合の対策を図るため、必要な設備の整備等について適切な措置を講ずること。
3　火災の防止等
建物等からの出火の防止のため、必要な措置を講ずること。また、火災による戸籍副本データ管理システムの構成機器又は関連設備の損傷を防止し、火災の発生を検知し、及び火災が発生した場合の対策を図るため、必要な設備の整備等について適切な措置を講ずること。
4　地震対策
地震による建物等又は戸籍副本データ管理システムの構成機器若しくは関連設備の損傷を防止し、及び地震が発生した場合の対策を図るため、必要な設備の整備等について適切な措置を講ずること。
5　急激な温湿度変化等に対する措置
空気調和設備は、その容量に配慮し、急激な温湿度変化等に対する措置を講ずること。
6　転倒、移動等に対する措置
戸籍副本データ管理システムの構成機器及び関連設備には、転倒、移動等に対する措置を講ずること。
7　その他の障害の防止等
動物その他による障害を防止し、これらの障害の発生を検知し、及び障害が発生した場合の対策を図るため、必要な措置を講ずること。
三　ネットワーク設備
1　専用回線の使用
電気通信回線からのデータの盗取を防止するため、戸籍副本データ管理サーバ、市区町村専用装置及び管轄法務局等端末を結ぶ電気通信回線は、地方公共団体及び国相互間通信用に設けた行政事務専用の回線を使用すること。
2　必要な伝送速度の確保
戸籍副本データ管理サーバ、市区町村専用装置及び管轄法務局等端末を結ぶ電気通信回線は、データを円滑に送信し、又は伝送するために必要な伝送速度を確保すること。

第五　戸籍副本データ管理システムの管理
一　入退室管理
1　入室資格の付与
重要機能室に入室する権限を有する者を限定すること。また、重要機能室に入退室する者に鍵を貸与する際には、その者が入室する権限を有することを確認すること、生体情報等による主体認証によって重要機能室に入退室する者が入室する権限を有することを確認すること等により、入退室の管理を適切に行うこと。
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　生体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者が内容を確認すること。
4　事務室の管理
重要機能室の出入口の鍵等を管理する事務室における盗難、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　設計の実施
イ　戸籍副本データ管理システムの開発又は変更を行う際には、戸籍副本データ管理システムのセキュリティを高める設計を行うこと。
ロ　戸籍副本データ管理システムの開発又は変更を行う際には、必要機能を明確にし、将来の規模の拡大等を考慮した設計を行うこと。
2　戸籍副本データ管理システムの試験の実施
戸籍副本データ管理システムの開発又は変更を行った場合には、その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、別途試験環境を用意することその他の適切な措置を講ずること。
3　戸籍副本データ管理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　戸籍副本データ管理システムの開発又は変更を行う際には、戸籍副本データ管理システムの開発又は変更の計画を策定すること、プログラムの作成、変更又は廃止を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　戸籍副本データ管理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　戸籍副本データ管理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　戸籍副本データ管理システムの管理
1　アクセス権限の限定
戸籍副本データ管理システムの運用に関係する者に対して、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戸籍副本データ管理システムを保護するため、戸籍副本データ管理サーバ及び市区町村専用装置間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当たっ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
戸籍副本データ管理サーバと市区町村専用装置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　データの暗号化
戸籍副本データ管理サーバ、市区町村専用装置及び管轄法務局等端末それぞれの間の通信については、交換するデータの暗号化を実施すること。
6　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。
7　情報収集等
セキュリティ対策に関する情報を収集して分析を行い、必要な措置を講ずること。
8　時刻の正確性確保
不正行為の追跡、セキュリティを侵害された場合における証跡の解析等を容易にするため、重要機能室内の機器を正確な時刻に同期するための必要な措置を講ずること。