二　障害の防止等
1　電気的及び機械的障害の防止等
本システムの構成機器又は関連設備の電気的及び機械的障害の発生を防止し、検知するため、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
本システムの構成機器又は関連設備の水又は蒸気による障害の発生を防止するため、これらの障害の発生を検知するため、及び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
建物等並びに情報連携端末等を設置する建物及び部屋からの出火の防止のため、必要な措置を講ずること。また、火災による本システムの構成機器又は関連設備の損傷を防止するため、火災の発生を検知するため、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本システムの構成機器若しくは関連設備の損傷を防止するため、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
連携サーバの管理に係る空気調和設備は、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
本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するため、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、連携サーバと情報連携端末等を結ぶ電気通信回線（既設ネットワーク（第六の一1イの方法により情報の連携を行う場合における電気通信回線を含む。以下同じ。）を除く。）は、専用回線（接続先が固定されており、所定の伝送速度が保証されている回線をいう。以下同じ。）を使用すること。また、当該既設ネットワークは、第七の一に定める接続条件をすべて満たしていること。
2　必要な伝送速度の確保
連携サーバと情報連携端末等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　本システムの管理
一　入退室管理
1　入室資格の付与
重要機能室への入室者を限定すること。また、重要機能室に入退室する者に鍵を貸与する際に、その者が入室する権限を有することを確認すること、入退室管理カード又は生体認証等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　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。