⑵　水又は蒸気による障害の防止等
　指定法人、認定委託先事業者及び単独設置型地方団体は、国税連携ネットワーク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。
⑶　火災の防止等
　指定法人、認定委託先事業者及び単独設置型地方団体は、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、建物等の火災による国税連携ネットワーク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。
⑷　地震対策
　指定法人、認定委託先事業者及び単独設置型地方団体は、地震による建物等又は国税連携ネットワーク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。
⑸　急激な温湿度変化等に対する措置
　指定法人、認定委託先事業者及び単独設置型地方団体は、空気調和設備について、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。
⑹　転倒、移動等に対する措置
　指定法人、認定委託先事業者及び単独設置型地方団体は、国税連携ネットワークシステムの構成機器及び関連設備に、転倒、移動等に対する措置を講ずること。
⑺　その他の障害の防止等
　指定法人、認定委託先事業者及び単独設置型地方団体は、動物その他による障害を防止するため、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、必要な措置を講ずること。
3　ネットワーク設備
⑴　専用回線の使用
　指定法人、認定委託先事業者及び単独設置型地方団体は、電気通信回線からのデータの盗取を防止するため、政府サーバ、市区町村サーバ、都道府県サーバ及び指定法人サーバを結ぶ電気通信回線について、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。
⑵　必要な伝送速度の確保
　指定法人、認定委託先事業者及び単独設置型地方団体は、政府サーバ、市区町村サーバ、都道府県サーバ及び指定法人サーバを結ぶ電気通信回線について、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4　国税連携ネットワークシステムの管理
1　入退室管理
⑴　入室資格の付与
　指定法人、認定委託先事業者及び単独設置型地方団体は、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とともに、入退室管理カード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。
⑵　鍵又は入退室管理カードの管理
ア　指定法人、認定委託先事業者及び単独設置型地方団体は、重要機能室の出入口の鍵を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。
イ　指定法人、認定委託先事業者及び単独設置型地方団体は、入退室管理カードの管理方法を定めること。
⑶　搬出入物品の確認
　指定法人、認定委託先事業者及び単独設置型地方団体は、重要機能室へ物品を搬出入する際、重要機能室に入室する権限を有する職員に搬出入する物品の内容を確認させること。
⑷　事務室の管理
　事務室における国税連携ネットワーク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。
2　ソフトウェア開発等の管理
⑴　セキュリティを高める設計の実施
　指定法人、認定委託先事業者及び単独設置型地方団体が国税連携ネットワークシステムの開発又は変更を行う際には、国税連携ネットワークシステムのセキュリティを高める設計を行うこと。
⑵　国税連携ネットワークシステムの試験の実施
ア　指定法人、認定委託先事業者及び単独設置型地方団体が国税連携ネットワークシステムの開発又は変更を行った場合には、障害試験、負荷試験その他必要な試験を適切に実施すること。
イ　指定法人、認定委託先事業者及び単独設置型地方団体は、ファイルの安全を確保するため、別途、試験環境を用意し、試験を行うこと。
⑶　国税連携ネットワークシステムの開発等に際してのエラーの発生及び不正行為の防止
ア　指定法人、認定委託先事業者及び単独設置型地方団体が国税連携ネットワークシステムの開発又は変更を行う際には、国税連携ネットワークシステムの開発又は変更の計画を策定し、国税連携ネットワークシステムの開発又は変更の責任者を指定し、及びプログラムの作成、変更又は廃止は責任者の承認を得て行う等エラーの発生及び不正行為の防止のための手続を明確にすること。
イ　指定法人、認定委託先事業者及び単独設置型地方団体は、国税連携ネットワーク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。
ウ　指定法人、認定委託先事業者及び単独設置型地方団体は、国税連携ネットワークシステムの変更に応じてドキュメントを更新し、責任者に確認させること。
⑷　セキュリティ対策の定期的な見直し
　指定法人、認定委託先事業者及び単独設置型地方団体は、国税連携ネットワークシステムの変更を実施しない場合においても、定期的に変更を行う必要性の有無を検討し、必要があると認めた場合にはその見直しを行い、必要な措置を講ずること。
3　国税連携ネットワークシステムの管理
⑴　アクセス権限の限定
　国税連携ネットワークシステムを運用保守又は利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。
⑵　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市区町村サーバ、都道府県サーバ、指定法人サーバ、端末機若しくは電気通信関係装置における不正行為又は市区町村サーバ、都道府県サーバ、指定法人サーバ、端末機若しくは電気通信関係装置への不正アクセス行為に対して国税連携ネットワークシステムを保護するため、政府サーバ、市区町村サーバ、都道府県サーバ及び指定法人サーバ間等、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。
⑶　電気通信関係装置の管理
　エラーの発生又は不正行為により電気通信関係装置の不適切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。また、通信に際しては、電気通信関係装置相互の認証を行うこと。
⑷　通信相手相互の認証
　指定法人、認定委託先事業者及び単独設置型地方団体は、政府サーバ、市区町村サーバ、都道府県サーバ及び指定法人サーバそれぞれの間の通信について、通信相手相互の認証を行うこと。
⑸　データの暗号化
　指定法人、認定委託先事業者及び単独設置型地方団体は、政府サーバ、市区町村サーバ、都道府県サーバ及び指定法人サーバそれぞれの間の通信について、交換するデータの暗号化を実施すること。
⑹　模擬攻撃の実施
　指定法人、認定委託先事業者及び単独設置型地方団体は、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。
⑺　情報収集等
　指定法人、認定委託先事業者及び単独設置型地方団体は、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。
4　端末機操作の管理
⑴　端末機の管理
　端末機の取扱いは、当該端末機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。
⑵　端末機の操作者の確認
ア　端末機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、指定法人及び認定委託先事業者の使用に係るものにあっては操作者識別カード及び暗証番号、生体認証又はこれと同等以上のものと認められる方法により、委託利用型地方団体及び単独設置型地方団体の使用に係るものにあっては暗証番号、生体認証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。