⑷　通信相手との相互認証
機構、認定委託先事業者、単独設置型地方団体及び機構委託クラウド事業者は、国税庁サーバ、市区町村サーバ、都道府県サーバ及び機構サーバそれぞれの間の通信について、通信相手との相互認証を行うこと。
⑸　データの暗号化
機構、認定委託先事業者、単独設置型地方団体及び機構委託クラウド事業者は、国税庁サーバ、市区町村サーバ、都道府県サーバ及び機構サーバそれぞれの間の通信について、送受信するデータの暗号化を実施すること。
⑹　模擬攻撃に対する防御訓練の実施
機構、認定委託先事業者、単独設置型地方団体及び機構委託クラウド事業者は、インターネット経由の、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
機構、認定委託先事業者、単独設置型地方団体及び機構委託クラウド事業者は、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に限ること。また、操作者による不正な行為及び誤操作による障害発生を防止するため、端末機を操作する際は複数の者で行うこととすることなど、必要な措置を講ずること。
⑵　端末機の操作者の認証
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付与された者であることを、機構、認定委託先事業者及び機構委託クラウド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、生体認証又はこれら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、生体認証又はこれら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。また、当該アクセス権限に関する情報を管理し、不正利用を防止するための措置を講ずること。
イ　端末機の操作が一定時間行われなかった場合に、再度、操作者の認証を行うよう端末機を設定すること。
⑶　暗証番号等の取扱い
暗証番号及び生体認証情報の管理及び運用の方法を定め、操作者に当該管理及び運用の方法を遵守させること。
⑷　ファイルに対する利用制限
端末機の操作者ごとに利用可能なファイルを設定する等、ファイルの利用を制限する方法を定めること。
⑸　操作履歴の記録等
機構、認定委託先事業者及び機構委託クラウド事業者は、端末機を操作した履歴を記憶媒体に記録し、各操作者の利用の正当性について確認すること。
⑹　強制的に終了する機能
機構、認定委託先事業者及び機構委託クラウド事業者は、端末機には、複数回アクセスに失敗した場合、強制的に終了する機能を設けること。
⑺　専用回線の使用
市区町村サーバ、都道府県サーバ及び機構サーバについて、端末機と相互に接続する電気通信回線は専用回線とすることとし、端末機を他の電気通信回線に接続しないこと。
道府県サーバ及び機構サーバそれぞれの間の通信について、送受信するデータの暗号化を実施すること。
⑹　模擬攻撃に対する防御訓練の実施
機構、認定委託先事業者及び単独設置型地方団体は、インターネット経由の、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
機構、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に限ること。また、操作者による不正な行為及び誤操作による障害発生を防止するため、端末機を操作する際は複数の者で行うこととすることなど、必要な措置を講ずること。
⑵　端末機の操作者の認証
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付与された者であることを、機構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、生体認証又はこれら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、生体認証又はこれら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。また、当該アクセス権限に関する情報を管理し、不正利用を防止するための措置を講ずること。
イ　端末機の操作が一定時間行われなかった場合に、再度、操作者の認証を行うよう端末機を設定すること。
⑶　暗証番号等の取扱い
暗証番号及び生体認証情報の管理及び運用の方法を定め、操作者に当該管理及び運用の方法を遵守させること。
⑷　ファイルに対する利用制限
端末機の操作者ごとに利用可能なファイルを設定する等、ファイルの利用を制限する方法を定めること。
⑸　操作履歴の記録等
機構及び認定委託先事業者は、端末機を操作した履歴を記憶媒体に記録し、各操作者の利用の正当性について確認すること。
⑹　強制的に終了する機能
機構及び認定委託先事業者は、端末機には、複数回アクセスに失敗した場合、強制的に終了する機能を設けること。
⑺　専用回線の使用
市区町村サーバ、都道府県サーバ及び機構サーバについて、端末機と相互に接続する電気通信回線は専用回線とすることとし、端末機を他の電気通信回線に接続しないこと。
５　市区町村サーバ、都道府県サーバ及び機構サーバの管理
⑴　秘密鍵の厳重な管理
機構、認定委託先事業者及び単独設置型地方団体は、市区町村サーバ、都道府県サーバ及び機構サーバにおいて、通信相手の認証及び送信するデータの暗号化を行うために必要な秘密鍵を厳重に保護し、外部に漏えいすることを防止するための措置を講ずること。
⑵　他のソフトウェアの作動の制限
機構、認定委託先事業者及び単独設置型地方団体は、市区町村サーバ、都道府県サーバ及