第５　機構等における運用管理上の安全性及び信頼性の確保

機構及び機構委託クラウド事業者は、次に掲げる事項（機構委託クラウド事業者にあっては９、10及び11⑵を除く。）を行わなければならない。

１　入退室管理

⑴　入室資格の付与

重要機能室へ入室できる者は、地方税共通納税システムの運用管理を適正に行うための必要最小限とすること。また、重要機能室に入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　重要機能室の出入口の鍵を所定の場所に保管し、その管理を定められた者が行うこと。

イ　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

重要機能室へ物品を搬出入する際は、重要機能室に入室する権限を有する職員が搬出入する物品の内容を確認すること。

⑷　事務室の管理

事務室における地方税共通納税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　地方税共通納税システム、利用者用ソフトウェア及び利用者用ソフトウェア開発要件の開発、作成又は変更

⑴　セキュリティを高める設計の実施

地方税共通納税システム、利用者用ソフトウェア及び利用者用ソフトウェア開発要件の開発、作成又は変更を行う際には、これらのセキュリティを高めるよう配慮すること。

⑵　地方税共通納税システム、利用者用ソフトウェア及び利用者用ソフトウェア開発要件の試験及び検査の実施

ア　地方税共通納税システム、利用者用ソフトウェア及び利用者用ソフトウェア開発要件の開発、作成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　地方税共通納税システムの試験を実施する場合には、ファイルの安全を確保するため、地方税共通納税システムと同様の機能を有する試験用のシステムを用意し、試験を行うこと。

ウ　地方税共通納税システム、利用者用ソフトウェア及び利用者用ソフトウェア開発要件の納入時又は受入れ時には、整備された検査手続に従い、セキュリティ機能が適切に組み込まれていることの検査を行うこと。

⑶　地方税共通納税システム、利用者用ソフトウェア及び利用者用ソフトウェア開発要件の開発、作成又は変更に際してのエラーの発生及び不正行為の防止

ア　地方税共通納税システム、利用者用ソフトウェア及び利用者用ソフトウェア開発要件の開発、作成又は変更を行う際には、開発、作成又は変更の計画を策定し、開発、作成又は変更の責任者を指定し、及びプログラムの作成、変更又は廃止を行う際には、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　地方税共通納税システム、利用者用ソフトウェア及び利用者用ソフトウェア開発要件を変更する場合は、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

地方税共通納税システム、利用者用ソフトウェア及び利用者用ソフトウェア開発要件のセキュリティ対策を向上させるために、定期的にこれらの見直しを行い、必要な措置を講ずること。

３　地方税共通納税システムの運用保守等

⑴　アクセス権限の限定

地方税共通納税システムを運用保守する職員は、地方税共通納税システムの適正な運用保守を確保するため必要最小限とし、これらの職員のみに対してアクセス権限を付与すること。

⑵　他のソフトウェアの作動の制限

機構サーバにおいて、地方税共通納税システムの管理及び運用保守並びに機構が行う他の地方税に係る電子的な手続のための電子計算機の管理及び運用保守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よう措置を講ずること。

⑶　ログの取得及びバックアップの実施

地方税共通納税システムの動作履歴、利用者のアクセス履歴その他運用管理等に必要な情報を記録すること。また、当該情報について、定期的にバックアップを実施すること。

⑷　記録の消去

機構サーバを使用しなくなった場合には、当該機器に内蔵する記憶媒体からファイル及びドキュメントを消去すること。

⑸　無害化処理の実施

インターネット回線を経由して送信された支払情報発行依頼情報及び納付情報は、無害化処理（インターネット回線を経由して送信された支払情報発行依頼情報及び納付情報をテキスト形式に変換する方法等により不正プログラムが混入しないよう安全を確保する措置をいう。）をした上で地方税共通納税システムに取り込むこととすること。

⑹　ファイアウォールによる通信制御

不正行為又は不正アクセス行為から地方税共通納税システムを保護するため、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。

⑺　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、通信については、電気通信関係装置相互の認証を行うこと。

⑻　通信相手との相互認証

機構サーバと地方団体サーバの間の通信について、通信相手との相互認証を行うこと。

⑼　データの暗号化

機構サーバと地方団体サーバの間の通信について、送信する支払情報及び納付書情報の暗号化を実施すること。

⑽　秘密鍵の厳重な管理

機構サーバにおいて通信相手の認証並びに送信する支払情報及び受信する納付書情報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。

⑾　模擬攻撃に対する防御訓練の実施

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。

⑿　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。

⒀　払込先の限定

共通口座からの払込先は、支払情報発行依頼情報又は納付情報に含まれる納付先の普通地方公共団体の指定する金融機関口座に制限すること。

⒁　利用状況の確認

利用者が歳入等の納付の手続に利用する預金口座又は貯金口座から共通口座へ送金された際に利用者に通知する等、利用者が利用状況を把握するための措置を講ずること。