長浜市訓令第２３号

長浜市情報セキュリティ対策基準に関する規程（平成28年長浜市訓令第37号）の一部を次のように改正する。

令和８年４月１日

長浜市長　浅見　宣義

目次中「第８４条」を「第８４条の２」に、
「第７章　業務委託と外部サービスの利用
第１節　業務委託（第１１５条―第１１７条）
第２節　外部サービスの利用（機密性２以上の情報を取り扱う場合）（第１１８条―第１２４条）
第３節　外部サービスの利用（機密性２以上の情報を取り扱う場合）（第１２５条・第１２６条）
」
を
「第７章　業務委託と外部サービス（クラウドサービス）の利用
第１節　業務委託（第１１５条―第１１６条の３）
第２節　情報システムに関する業務委託（第１１７条―第１１７条の４）
第３節　外部サービス（クラウドサービス）の利用（自治体機密性２以上の情報を取り扱う場合）（第１１８条―第１２４条）
第４節　外部サービス（クラウドサービス）の利用（自治体機密性２以上の情報を取り扱わない場合）（第１２５条・第１２６条）
」
に改める。

第２条第５号中「第２条第８項」を「第２条第９項」に改め、同条第８号中「第９条第１項又は第２項」を「第９条第１項から第３項まで」に改め、同条第９号中「第９条第３項」を「第９条第４項」に改める。

第５条第８号イ中「（令和３年長浜市訓令第43号）」を削る。

第８条第１号の表中
「

機密性３	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産
機密性２	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産

機密性１	機密性２又は機密性３の情報資産以外の情報資産

」

を

「

自治体機密性３Ａ	行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」（平成23年４月１日内閣総理大臣決定）に定める秘密文書に相当する文書
自治体機密性３Ｂ	行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産
自治体機密性３Ｃ	行政事務で取り扱う情報資産のうち、自治体機密性３Ｂ以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産
自治体機密性２	行政事務で取り扱う情報資産のうち、自治体機密性３に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産
自治体機密性１	自治体機密性２又は自治体機密性３の情報資産以外の情報資産

」

に改め、同条第２号の表完全性２の項中「完全性２」を「自治体完全性２」に改め、同表完全性１の項中「完全性１」を「自治体完全性１」に、「完全性２」を「自治体完全性２」に改め、同条第３号の表可用性２の項中「可用性２」を「自治体可用性２」に改め、同表可用性１の項中「可用性１」を「自治体可用性１」に、「可用性２」を「自治体可用性２」に改める。

第９条第１号中イをウとし、アの次に次のように加える。

イ　情報システム管理者は、所管する情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳を整備しなければならない。

第９条第６号エ中「機密性２以上、完全性２又は可用性２」を「自治体機密性２以上、自治体完全性２又は自治体可用性２」に改め、同条第７号から第９号までの規定中「機密性２」を「自治体機密性２」に改める。

第１３条第１項中「可用性２」を「自治体可用性２」に改める。

第１７条第４項中「機密性２」を「自治体機密性２」に改める。

第１９条の次に次の１条を加える。

（セキュリティ対策の実施）

第１９条の２　統括情報セキュリティ責任者は、情報システムのセキュリティ要件として

策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施しなければならない。

第２２条中「機密性２」を「自治体機密性２」に改める。

第２３条の見出しを削り、同条の前に見出しとして「（完全性の確保）」を付し、同条中「生じないように」の次に「、不正な通信の有無を監視する等の」を加え、同条の次に次の１条を加える。

第２３条の２　統括情報セキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順を定めなければならない。また、必要なソフトウェアの状態等を調査し、認識したぜい弱性等について対策を講じなければならない。

第２４条中「可用性２」を「自治体可用性２」に改める。

第３２条第１項中「機密性２以上、可用性２、完全性２」を「自治体機密性２以上、自治体可用性２及び自治体完全性２」に改める。

第４５条に次の１項を加える。

４　情報セキュリティインシデントにより、個人情報又は特定個人情報の漏えい等が発生した場合は、必要に応じて個人情報保護委員会へ報告しなければならない。

第４５条の２の見出し中「による」を削る。

第４６条第３項に後段として次のように加える。

また、ＣＳＩＲＴは、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報システム管理者へ確認を指示しなければならない。

第５１条中「業務システム」を「情報システム」に改め、同条に次の２項を加える。

２　統括情報セキュリティ責任者及び情報システム管理者は、重要な情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得しなければならない。

３　統括情報セキュリティ責任者及び情報システム管理者は、重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し、保管しなければならない。

第５３条第２項中「なければならない」を「、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直さなければならない」に改める。

第５７条に次の１項を加える。

３　統括情報セキュリティ責任者は、保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保しなければならない。また、情報セキュリティ対策について、定期的な確認により見直さなければならない。

第５９条第４項中「庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続」を「次のセキュリティ対策を実施」に改め、同項に次の各号を加える。

(1)　庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続すること。

(2)　ぜい弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える

機能のうち、必要な機能のみを利用すること。

(3) ウェブサーバからの不用意な情報漏えいを防止するための措置を講じること。

(4) ウェブコンテンツの編集作業を行う者を限定すること。

第６２条の見出し中「無線ＬＡＮ」の次に「のセキュリティ対策」を加える。

第６８条の見出し中「での」を削る。

第６９条の２（見出しを含む。）中「Ｗｅｂ会議」を「ウェブ会議」に改める。

第６９条の３第１項第１号中「Ｗｅｂサイト」を「ウェブサイト」に改め、同条第２項中「機密性２」を「自治体機密性２」に改め、同条第５項中「可用性２」を「自治体可用性２」に、「Ｗｅｂサイト」を「ウェブサイト」に改める。

第７０条中「アクセスする権限のない職員等がアクセスできないように、システム上制限」を「必要最小限の職員等が利用できるように設定する等、適切にシステムのアクセス制御を」に改める。

第７１条に次の１項を加える。

４　統括情報セキュリティ責任者及び情報システム管理者は、利用者ＩＤに不要なアクセス権限が付与されていないか定期的に確認しなければならない。

第７２条中第６項を第７項とし、第２項から第５項までを１項ずつ繰り下げ、第１項の次に次の１項を加える。

２　統括情報セキュリティ責任者及び情報システム管理者は、管理者権限の特権を付与されたＩＤの識別コード及び認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び内部からの不正操作や誤操作を防止するための措置を講じなければならない。

第７３条第６項中「許可を得」を「許可を得るか」に改める。

第７７条の見出しを「（機器等及び情報システムの調達）」に改め、同条第１項に後段として次のように加える。

また、情報システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載しなければならない。

第７７条を第７７条の２とし、第５章第３節中同条の前に次の１条を加える。

（機器等の調達に係る運用規程の整備）

第７７条　統括情報セキュリティ責任者は、機器等の選定基準を運用規程として整備しなければならない。また、必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられないような対策を講じなければならない。

２　統括情報セキュリティ責任者及び情報システム管理者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備しなければならない。

第７８条第３号ア中「なければならない」を「、それ以外のものを利用させてはならない」に改め、同条に次の１号を加える。

(4) アプリケーション・コンテンツの開発時の対策

情報システム管理者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションのぜい弱性を排除するための対策を講じなければならない。

第７９条第１項第２号エ中「受け入れ」を「受入れ」に改め、同号に次のように加える。

オ　情報システム管理者は、情報システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮したテスト計画を策定し、確実に検証が実施されるよう、必要かつ適切に委託事業者の監督を行わなければならない。

第７９条第１項に次の１号を加える。

(3) 機器等の納入時又は情報システムの受入れ時

ア　情報システム管理者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、調達仕様書等に定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認しなければならない。

イ　情報システム管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引き継がれる項目に情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。

第７９条第２項を削り、同条の次に次の１条を加える。

（情報システムの基盤を管理又は制御するソフトウェア導入時の対策）

第７９条の２　情報システム管理者は、情報セキュリティの観点から情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護するための措置を講じなければならない。

２　情報システム管理者は、利用するソフトウェアの特性を踏まえ、以下の全ての実施手順を整備しなければならない。

(1) 情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順

(2) 情報システムの基盤を管理又は制御するソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順

第８０条第１項を次のように改める。

情報システム管理者は、次の各号に掲げる内容を含む、システム開発・保守に関連する資料及びシステム関連文書を適切に整備・保管しなければならない。

(1) 情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順

(2) 情報セキュリティインシデントを認知した際の対処手順

(3) 情報システムが停止した際の復旧手順

第８０条の次に次の１条を加える。

（情報システムの構築又は改廃時の対策）

第８０条の２　情報システム管理者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について統括情報セキュリティ責任者に報告しなければならない。

第８１条第２項を次のように改める。

２　情報システム管理者は、ウェブアプリケーション及びウェブコンテンツにおいて、次のセキュリティ対策を実施しなければならない。

(1) 利用者の情報セキュリティ水準の低下を招かぬよう、ウェブアプリケーション及びウェブコンテンツの提供方式等を見直すこと。

(2) 運用中のウェブアプリケーション及びウェブコンテンツにおいて、定期的にぜい弱性対策の状況を確認し、ぜい弱性が発覚した際は必要な措置を講じること。

(3) ウェブアプリケーション及びウェブコンテンツにおいて、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合は、これを検出するチェック機能を組み込むように情報システムを設計すること。

第５章第３節中第８４条の次に次の１条を加える。

（情報システムについての対策の見直し）

第８４条の２　情報システム管理者は、対策の推進計画等に基づき情報システムの情報セキュリティ対策を適切に見直さなければならない。

２　前項の規定による見直しの結果については、統括情報セキュリティ責任者へ報告しなければならない。

第９６条中「情報システム管理責任者は、」の次に「サーバ装置、端末及び通信回線装置等における」を加える。

第９９条を第９９条の３とし、第６章第１節中同条の前に次の２条を加える。

（情報システムの運用・保守時の対策）

第９９条　統括情報セキュリティ責任者及び情報システム管理者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用しなければならない。

２　統括情報セキュリティ責任者及び情報システム管理者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。

３　統括情報セキュリティ責任者及び情報システム管理者は、重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるように運用をしなければならない。

（情報システムの監視機能）

第９９条の２　統括情報セキュリティ責任者及び情報システム管理者は、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装しなければならない。

２　統括情報セキュリティ責任者及び情報システム管理者は、情報システムの運用において、情報システムに実装された監視機能を適切に運用しなければならない。

３　統括情報セキュリティ責任者及び情報システム管理者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直さなければならない。

４　統括情報セキュリティ責任者及び情報システム管理者は、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講じなければならない。

第７章の章名中「外部サービス」の次に「（クラウドサービス）」を加える。

第１１５条及び第１１６条を次のように改める。

（業務委託に係る運用規程の整備）

第１１５条　統括情報セキュリティ責任者は、業務委託に係る以下の内容を全て含む運用規程を整備しなければならない。

(1) 委託事業者への提供を認める情報及び委託する業務の範囲を判断する基準（以下「委託判断基準」という。）

(2) 委託事業者の選定基準

（業務委託実施前の対策）

第１１６条　情報セキュリティ管理者又は情報システム管理者は、業務委託の実施までに、以下の事項を全て実施しなければならない。

(1) 委託する業務内容の特定

(2) 委託事業者の選定条件を含む仕様の策定

(3) 仕様に基づく委託事業者の選定

(4) 重要な情報資産を取り扱う業務を委託する場合には、次の情報セキュリティ要件を明記した契約の締結（契約項目）

ア　情報セキュリティポリシー及び情報セキュリティ実施手順の遵守

イ　個人情報漏えい防止のための技術的安全管理措置に関する取決め

ウ　委託事業者の責任者、委託内容、作業者の所属及び作業場所の特定

エ　提供されるサービスレベルの保証

オ　委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法

カ　委託事業者の従業員に対する教育の実施

キ　提供された情報の目的外利用及び委託事業者以外の者への提供の禁止

ク　業務上知り得た情報の守秘義務

ケ　再委託に関する制限事項の遵守

コ　委託業務終了時の情報資産の返還、廃棄等

サ　委託業務の定期報告及び緊急時報告義務

シ　市による監査及び検査

ス　市による情報セキュリティインシデント発生時の公表

セ　情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

(5) 委託事業者に重要な情報を提供する場合は、秘密保持契約（ＮＤＡ）の締結

第１１７条を削る。

第７章第２節の節名中「外部サービス」の次に「（クラウドサービス）」を加え、「機密性２」を「自治体機密性２」に改める。

第１１８条を次のように改める。

（クラウドサービスの選定に係る運用規程の整備）

第１１８条　統括情報セキュリティ責任者は、自治体機密性２以上の情報を取り扱う場合、以下を含む外部サービス（クラウドサービス）（以下「クラウドサービス」という。）の選定に関する規程を整備しなくてはならない。

(1) クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下「クラウドサービス利用判断基準」という。）

(2) クラウドサービス提供者の選定基準

(3) クラウドサービスの利用申請の許可権限者と利用手続

(4) クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

第１１８条の次に次の１条を加える。

（クラウドサービスの利用に係る運用規程の整備）

第１１８条の２　統括情報セキュリティ責任者は、自治体機密性２以上の情報を取り扱う場合、以下を含むクラウドサービス（自治体機密性２以上の情報を取り扱う場合）の利用に関する規程を整備しなければならない。

(1) クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針

(2) クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針

(3) クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を全て含むクラウドサービスの利用を終了する際のセキュリティ対策の基本方針

ア　クラウドサービスの利用終了時における対策

イ　クラウドサービスで取り扱った情報の廃棄

ウ　クラウドサービスの利用のために作成したアカウントの廃棄

第１１９条の見出し中「外部サービス」を「クラウドサービス」に改め、同条第１項中「外部サービス利用判断基準に従って外部サービス」を「クラウドサービス利用判断基準に従って、業務に係る影響度等を検討した上でクラウドサービス」に改め、同条第２項各号列記以外の部分を次のように改める。

情報セキュリティ責任者は、クラウドサービスで取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス提供者の選定基準に従ってクラウドサービス提供者を選定しなければならない。また、以下の内容を含む情報セキュリティ対策をクラウドサービス提供者の選定条件に含めなければならない。

第１１９条第２項第１号から第４号までの規定中「外部サービス」を「クラウドサービス」に改め、同条第３項から第６項までの規定中「外部サービス」を「クラウドサービス」に改め、同条第７項中「外部サービス」を「クラウドサービス」に、「セキュリティ要件」を「以下を全て含むセキュリティ要件」に改め、同項に次の各号を加える。

(1) クラウドサービスに求める情報セキュリティ対策

(2) クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法

(3) クラウドサービスに求めるサービスレベル

第１１９条第８項中「外部サービス」を「クラウドサービス」に改める。

第１２０条の見出し及び同条第１項中「外部サービス」を「クラウドサービス」に改め、同条第２項中「外部サービス」を「クラウドサービス」に、「調達仕様の内容を契約に含めなければならない」を「利用承認を得なければならない」に改め、同項に後段として次のように加える。

また、調達仕様の内容を契約に含めなければならない。

第１２１条（見出しを含む。）中「外部サービス」を「クラウドサービス」に改める。

第１２２条の見出し及び同条第１項中「外部サービス」を「クラウドサービス」に改め、同条第２項中「外部サービス」を「クラウドサービス」に、「前項」を「第１項」に改め、同項を同条第４項とし、同条第１項の次に次の２項を加える。

２　クラウドサービス管理者は、情報システムにおいてクラウドサービスを利用する際には、情報システム台帳及び関連文書に記録又は記載しなければならない。なお、情報システム台帳に記録又は記載した場合は、統括情報セキュリティ責任者へ報告しなければ

ならない。
３　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の全ての実施手順を整備しなければならない。
(1) クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順
(2) クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順
(3) 利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

第１２３条の見出し及び同条第１項中「外部サービス」を「クラウドサービス」に改め、同条第３項中「外部サービス」を「クラウドサービス」に、「前２項」を「前各項」に改め、同項を同条第５項とし、同条第２項中「外部サービス」を「クラウドサービス」に改め、同項を同条第４項とし、同条第１項の次に次の２項を加える。
２　クラウドサービス管理者は、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合、情報システム台帳及び関連文書を更新又は修正しなければならない。なお、情報システム台帳を更新又は修正した場合は、統括情報セキュリティ責任者へ報告しなければならない。
３　クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。

第１２４条（見出しを含む。）中「外部サービス」を「クラウドサービス」に改める。

第７章第３節の節名中「外部サービス」の次に「（クラウドサービス）」を加え、「機密性２」を「自治体機密性２」に改める。

第７章中第３節を第４節とし、第２節を第３節とする。

第１１６条の次に次の２条及び１節を加える。

（業務委託実施期間中の対策）

第１１６条の２　情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間において、以下を全て含む対策を実施しなければならない。
(1) 委託判断基準に従った重要情報の提供
(2) 契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施
(3) 統括情報セキュリティ責任者へ措置内容の報告（重要度に応じてＣＩＳＯに報告）
(4) 委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合における委託事業の一時中断などの必要な措置を含む契約に基づく対処の要求
２　情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間において、以下を全て含む対策の実施を委託事業者に求めなければならない。
(1) 情報の適正な取扱いのための情報セキュリティ対策
(2) 契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告

(3) 委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における委託事業の一時中断などの必要な措置を含む対処

（業務委託終了時の対策）

第１１６条の３　情報セキュリティ管理者又は情報システム管理者は、業務委託の終了に際して、以下を全て含む対策を実施しなければならない。

(1) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収

(2) 委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認

２　情報セキュリティ管理者又は情報システム管理者は、業務委託の終了に際して、以下を全て含む対策の実施を委託事業者に求めなければならない。

(1) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検

(2) 提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

第２節　情報システムに関する業務委託

（情報システムに関する業務委託における共通的対策）

第１１７条　情報システム管理者は、情報システムに関する業務委託の実施までに、情報システムに本市の意図しない変更が加えられないための対策に係る選定条件を委託事業者の選定条件に加え、仕様を策定しなければならない。

（情報システムの構築を業務委託する場合の対策）

第１１７条の２　情報システム管理者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託事業者に求めなければならない。

(1) 情報システムのセキュリティ要件の適切な実装

(2) 情報セキュリティの観点に基づく試験の実施

(3) 情報システムの開発環境及び開発工程における情報セキュリティ対策

（情報システムの運用・保守を業務委託する場合の対策）

第１１７条の３　情報システム管理者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者に実施を求めなければならない。

２　情報システム管理者は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託事業者に速やかな報告を求めなければならない。

（本市向けに情報システムの一部の機能を提供するサービスを利用する場合の対策）

第１１７条の４　情報セキュリティ管理者又は情報システム管理者は、外部の一般の者が本市向けに重要情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託事業者の選定条件に業務委託サービスに特有の選定条件を加えなければならない。

２　情報セキュリティ管理者又は情報システム管理者は、業務委託サービスに係るセキュ

リティ要件を定め、業務委託サービスを選定しなければならない。
３　情報セキュリティ管理者又は情報システム管理者は、委託事業者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。
４　情報セキュリティ管理者又は情報システム管理者は、業務委託サービスを利用する場合には、統括情報セキュリティ責任者又は情報セキュリティ責任者へ当該サービスの利用申請を行わなければならない。
５　統括情報セキュリティ責任者又は情報セキュリティ責任者は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定しなければならない。
６　統括情報セキュリティ責任者又は情報セキュリティ責任者は、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名しなければならない。

第１２５条の見出し中「外部サービス」を「クラウドサービス」に改め、同条中「以下を含む外部サービス（機密性２以上の情報を取り扱わない場合）の利用に関する規定を整備すること」を「自治体機密性２以上の情報を取り扱わない場合、以下を含むクラウドサービスの利用に関する規定を整備しなければならない」に改め、同条第１号から第３号までの規定中「外部サービス」を「クラウドサービス」に改め、同条第４号中「外部サービスの」を「クラウドサービス」に改める。

第１２６条の見出し中「外部サービス」を「クラウドサービス」に改め、同条第１項中「機密性２」を「自治体機密性２」に、「外部サービス」を「クラウドサービス」に、「申請すること」を「申請しなければならない」に、「講ずること」を「講じなければならない」に改め、同条第２項中「外部サービスの」を「クラウドサービスの」に改め、同項中「決定すること」を「決定しなければならない」に、「外部サービスを記録すること」を「クラウドサービスを記録しなければならない」に改める。

第１３３条第１項中「対処」の次に「（改善計画の策定等）」を加え、同項後段を次のように改める。

また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。

第１３３条第２項を次のように改める。

２　ＣＩＳＯは、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。また、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処（改善計画の策定等）を指示しなければならない。なお、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。

第１３８条中「評価」を「リスク評価」に改め、同条に後段として次のように加える。

なお、横断的に改善が必要となる情報セキュリティ対策の運用見直しについて、内部の職制及び職務に応じた措置の実施又は指示を行い、措置の結果についてＣＩＳＯに報告しなければならない。

附　則

この規程は、令和８年４月１日から施行する。