長浜市訓令第１４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７年４月１日

長浜市長　浅見　宣義

目次中「・第９条」を「―第９条の２」に改め、「第６９条」を「第６９条の３」に、「第７章　外部サービスの利用」を「第７章　業務委託と外部サービスの利用」に、「外部委託」を「業務委託」に、「約款による外部サービスの利用」を「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）」に、「・第１１９条」を「―第１２４条」に、「ソーシャルメディアサービスの利用」を「外部サービスの利用（機密性２以上の情報を取り扱わない場合）」に、「第１２０条―第１２２条」を「第１２５条・第１２６条」に、「第１２３条―第１３０条」を「第１２７条―第１３４条」に、「第１３１条―第１３３条」を「第１３５条―第１３７条」に、「第１３４条」を「第１３８条」に改める。

第７条第６項中「外部の事業者等」を「委託事業者等」に改める。

第９条第１号イ中「情報資産が複製」を「情報セキュリティ管理者は、情報資産が複製され」に改め、同条第７号中「暗号化又はパスワード設定」を「、パスワード等による暗号化」に改め、同条第８号ア及び第９号ア中「暗号化又はパスワードの設定」を「パスワード等による暗号化」に改め、同条第１０号アからウまで以外の部分を次のように改める。

情報資産の廃棄等

第９条第１０号ア中「情報資産の廃棄」の次に「、リース返却等」を加え、「が不要になった場合は記録されている」を「について、その」に改め、「当該電磁的記録媒体の」を削り、「処置した上で廃棄しなければ」を「処置しなければ」に改め、同号イ及びウ中「情報資産の廃棄」の次に「、リース返却等」を加える。

第９条の２第１号ア（ウ）ただし書中「は、インターネット等からＬＧＷＡＮ－ＡＳＰを経由してマイナンバー利用事務系にデータを取込むことができるもの」を「については、この限りでなく、ＬＧＷＡＮを経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータ移送を可能」に改める。

第１２条第４項中「外部委託事業者」を「委託事業者」に改める。

第１３条第２項中「外部の」を削り、「あたり」を「当たり」に改める。

第１７条第２項中「外部委託事業者」を「委託事業者」に改める。

第１８条第１項中「委託した業者」を「委託事業者」に改める。

第２５条中「のワイヤーによる固定、」を「及び」に改める。

第３２条第４項を削る。

第４０条の見出し中「外部委託事業者」を「委託事業者」に改め、同条中「外部委託事業者」を「委託事業者」に、「外部委託事業者から再委託を受ける事業者」を「再委託事業者」に、「外部委託事業者が」を「委託事業者が」に改める。

第５１条中「情報システム管理者は」の次に「、業務システムのデータベース」を加え、「関わらず」を「かかわらず」に改める。

第５３条第３項中「外部委託事業者」を「委託事業者」に、「２名」を「２人」に改める。

第６１条の見出し中「特定用途機器」を「ＩｏＴ機器を含む特定用途機器」に改める。

第６３条第２項中「大量の」を削り、「の受信又は送信」を「が内部から送信されていること」に改め、同条第５項中「外部委託事業者」を「委託事業者」に改める。

第６４条第５項を削る。

第６５条第１項中「暗号化又はパスワード設定等」を「パスワード等による暗号化等」に改める。

第６８条を次のように改める。

（業務外でのネットワークへの接続の禁止）

第６８条　職員等は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう情報システム管理者によって定められたネットワークと異なるネットワークに接続してはならない。

２　情報セキュリティ管理者は、支給した端末について、端末に搭載されたＯＳのポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限することが望ましい。

第５章第１節中第６９条の次に次の２条を加える。

（Ｗｅｂ会議サービスの利用時の対策）

第６９条の２　統括情報セキュリティ責任者は、Ｗｅｂ会議を適切に利用するための利用手順を定めなければならない。

２　職員等は、本市の定める利用手順に従い、Ｗｅｂ会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

３　職員等は、Ｗｅｂ会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

４　職員等は、外部からＷｅｂ会議に招待される場合は、本市の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。

（ソーシャルメディアサービスの利用）

第６９条の３　情報セキュリティ管理者は、本市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

(1) 本市のアカウントによる情報発信が、実際に本市のものであることを明らかにするために、本市の自己管理Ｗｅｂサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

(2) パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ハードディスク、ＵＳＢメモリ、紙等）等を適切に管理するなどの方法で、不正アクセス対策を実施すること。

２　機密性２以上の情報は、ソーシャルメディアサービスで発信してはならない。

３　利用するソーシャルメディアサービスごとの責任者を定めなければならない。
４　アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。
５　可用性２の情報の提供にソーシャルメディアサービスを用いる場合は、本市の自己管理Ｗｅｂサイトに当該情報を掲載して参照可能とすること。

第７２条第４項中「外部委託事業者」を「委託事業者」に改める。

第７３条第７項中「公衆通信回線（公衆無線ＬＡＮ等）の庁外通信回線を庁内ネットワークに接続することは」を「内部のネットワーク又は情報システムに対するインターネットを介した外部からのアクセスを」に改める。

第８５条第７号に後段として次のように加える。

また、当該製品の利用を予定している期間中にパッチやバージョンアップなどの開発元のサポートが終了する予定がないことを確認しなければならない。

第８６条に次の１号を加える。

(5) 不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報システム管理者が許可した職員を除く職員等に当該権限を付与してはならない。

第９２条中「職員等」の次に「及び委託事業者」を加える。

第９５条を次のように改める。

（標的型攻撃）

第９５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、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。

第１１２条第４号中「（平成15年法律第57号）」を削り、同条第５号を次のように改める。

(5) 番号法

第１１２条第６号中「平成28年法律第31号」を「平成26年法律第104号」に改め、同条に次の１号を加える。

(7) 長浜市個人情報の保護に関する法律施行条例（令和４年長浜市条例第29号）

第７章の章名及び同章第１節の節名を次のように改める。

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条の見出し中「外部委託事業者」を「委託事業者」に改め、同条第１項中「外部委託事業者」を「委託事業者」に、「あたり」を「当たり」に改め、同条第２項中「事業者」を「委託事業者」に改める。

第１１６条中「情報システムの運用、保守等を外部委託する」を「重要な情報資産を取扱う業務を委託する」に、「外部委託事業者と」を「委託事業者と」に改め、同条第２号中「外部委託事業者」を「委託事業者」に改め、同条第４号中「外部委託事業者」を「委託事業者」に改め、「アクセス方法」の次に「の明確化等、情報のライフサイクル全般での管理方法」を加え、同条第５号中「外部委託事業者」を「委託事業者」に改め、同条第

６号中「受託者」を「委託事業者」に改める。
第１１７条中「外部委託事業者」を「委託事業者」に改める。
第１３４条を第１３８条とする。
第８章第２節中第１３３条を第１３７条とし、第１３２条を第１３６条とし、第１３１条を第１３５条とする。
第８章第１節中第１３０条を第１３４条とし、第１２７条から第１２９条までを４条ずつ繰り下げる。
第１２６条の見出し中「外部委託事業者」を「委託事業者」に改め、同条中「外部委託事業者に委託している」を「事業者に業務委託を行っている」に、「外部委託事業者から下請として受託している事業者も含めて」を「委託事業者（再委託事業者を含む。）に対して」に改め、同条を第１３０条とし、第１２５条を第１２９条とし、第１２４条を第１２８条とし、第１２３条を第１２７条とする。
第７章第２節及び第３節を次のように改める。

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）

（外部サービスの利用に係る規定の整備）

第１１８条　統括情報セキュリティ責任者は、次の各号を含む外部サービス（機密性２以上の情報を取り扱う場合）の利用に関する規定を整備しなければならない。

(1) 外部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（次条において「外部サービス利用判断基準」という。）

(2) 外部サービス提供者の選定基準

(3) 外部サービスの利用申請の許可権限者と利用手続

(4) 外部サービス管理者の指名と外部サービスの利用状況の管理

（外部サービスの選定）

第１１９条　情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討しなければならない。

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

(1) 外部サービスの利用を通じて本市が取り扱う情報の外部サービス提供者における目的外利用の禁止

(2) 外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制

(3) 外部サービスの提供に当たり、外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制

(4) 外部サービス提供者の資本関係・役員等の情報、外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定

(5) 情報セキュリティインシデントへの対処方法

(6) 情報セキュリティ対策その他の契約の履行状況の確認方法

(7) 情報セキュリティ対策の履行が不十分な場合の対処方法

3　情報セキュリティ責任者は、外部サービスの中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス提供者の選定条件に含めなければならない。
4　情報セキュリティ責任者は、外部サービスの利用を通じて本市が取り扱う情報の格付等を勘案し、必要に応じて次の内容を外部サービス提供者の選定条件に含めなければならない。
(1) 情報セキュリティ監査の受入れ
(2) サービスレベルの保証
5　情報セキュリティ責任者は、外部サービスの利用を通じて本市が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて本市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めなければならない。
6　情報セキュリティ責任者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本市に提供し、本市の承認を受けるよう、外部サービス提供者の選定条件に含めなければならない。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断しなければならない。
7　情報セキュリティ責任者は、外部サービスの特性を考慮した上で、外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定めなければならない。
8　統括情報セキュリティ責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス提供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。

（外部サービスの利用に係る調達・契約）

第１２０条　情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めなければならない。
2　情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めるなければならない。

（外部サービスの利用承認）

第１２１条　情報セキュリティ責任者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用申請を行わなければならない。
2　利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定しなければならない。
3　利用申請の許可権限者は、外部サービスの利用申請を承認した場合は、承認済外部サービスとして記録し、外部サービス管理者を指名しなければならない。

（外部サービスを利用した情報システムの導入・構築時の対策）

第１２２条　統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、次の各号を含む外部サービスを利用して情報システムを構築する際のセキュリティ対策を規定しなければならない。

(1) 不正なアクセスを防止するためのアクセス制御

(2) 取り扱う情報の機密性保護のための暗号化

(3) 開発時におけるセキュリティ対策

(4) 設計・設定時の誤りの防止

２　外部サービス管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録しなければならない。

（外部サービスを利用した情報システムの運用・保守時の対策）

第１２３条　統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、次の各号を含む外部サービスを利用して情報システムを運用する際のセキュリティ対策を規定しなければならない。

(1) 外部サービス利用方針の規定

(2) 外部サービス利用に必要な教育

(3) 取り扱う資産の管理

(4) 不正アクセスを防止するためのアクセス制御

(5) 取り扱う情報の機密性保護のための暗号化

(6) 外部サービス内の通信の制御

(7) 設計・設定時の誤りの防止

(8) 外部サービスを利用した情報システムの事業継続

２　情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスで発生したインシデントを認知した際の対処手順を整備しなければならない。

３　外部サービス管理者は、前２項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録しなければならない。

（外部サービスを利用した情報システムの更改・廃棄時の対策）

第１２４条　統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、次の各号を含む外部サービスの利用を終了する際のセキュリティ対策を規定しなければならない。

(1) 外部サービスの利用終了時における対策

(2) 外部サービスで取り扱った情報の廃棄

(3) 外部サービスの利用のために作成したアカウントの廃棄

２　外部サービス管理者は、前項において定める規定に対し、外部サービスの利用終了時に実施状況を確認し、記録しなければならない。

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わない場合）

（外部サービスの利用に係る規定の整備）

第１２５条　統括情報セキュリティ責任者は、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。

(1) 外部サービスを利用可能な業務の範囲

(2) 外部サービスの利用申請の許可権限者と利用手続
(3) 外部サービス管理者の指名と外部サービスの利用状況の管理
(4) 外部サービスの利用の運用手順

（外部サービスの利用における対策の実施）

第１２６条　職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で機密性２以上の情報を取り扱わない場合の外部サービスの利用を申請すること。また、承認時に指名された外部サービス管理者は、当該外部サービスの利用において適切な措置を講ずること。

２　情報セキュリティ責任者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。また、承認した外部サービスを記録すること。

附　則

この規程は、令和７年４月１日から施行する。