湖北広域行政事務センター情報セキュリティ対策基準に関する規程

目次

第１章　総則

（趣旨）

第１条　この対策基準は、湖北広域行政事務センター（以下「センター」という。）情報セキュリティ基本方針に基づきセンター内の情報資産のセキュリティ管理に必要な事項を定める。

（定義）

第２条　この対策基準において使用する用語の意義は、湖北広域行政事務センター情報セキュリティ基本方針第２条に規定する用語の定義に定めるところによる。

（対象範囲）

第３条　この対策基準は、センターの全ての実施機関における情報資産に接する職員等を対象とする。

２　この対策基準が対象とする情報資産は、次のとおりとする。

（１）ネットワーク、情報システム及びこれらに関する設備、電磁的記録

（２）ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

（３）情報システムの仕様書及びネットワーク図等のシステム関連文書

（組織体制）

第４条　適切に情報セキュリティ対策を推進・管理するため、次の者をおく。

（１）統括情報セキュリティ責任者　事務局長を統括情報セキュリティ責任者とする。

（２）情報セキュリティ責任者　各課・施設（以下「課等」という。）の所属長を情報セキュリティ責任者とする。

（３）セキュリティ担当者　情報セキュリティ責任者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者で、課等の情報推進リーダーを充てる。

（４）情報セキュリティ管理者　総務課長を情報セキュリティ管理者とする。

（５）情報セキュリティ委員会　必要に応じて統括情報セキュリティ責任者が、情報セキュリティ委員会を招集する。委員会事務局は総務課とする。

（権限と責任）

第５条　情報セキュリティ管理体制における権限と責任について、以下のとおりとする。

（１）統括情報セキュリティ責任者

ア　センターにおける全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

イ　情報セキュリティインシデントに対処するための体制を整備し、役割を明確化する。

ウ　この対策基準に定められた自らの担務を、この対策基準に定められた他の責任者に負わせることができる。

（２）情報セキュリティ責任者

ア　当該所属の情報セキュリティ対策に関する権限及び責任を有する。

イ　当該所属の所有する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

ウ　当該所属の所有する情報システムについて、緊急時などにおける連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約及び職員等に対する教育、訓練、助言及び指示を行う。

（３）情報セキュリティ管理者

ア　センターの全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

イ　所管する情報システムに係る実施手順の維持・管理を行う。

ウ　センターの全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

エ　情報セキュリティ責任者及び情報システム担当者に対して、情報システムに関する指導及び助言を行う権限を有する。

オ　センターの情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、統括情報セキュリティ責任者の指示に従い必要かつ十分な措置を行う権限及び責任を有する。

カ　センターの情報システム及び情報資産に関して維持・管理を行う権限及び責任を有する。

キ　緊急時等の円滑な情報共有を図るため、統括情報セキュリティ責任者、情報セキュリティ責任者等を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

ク　緊急時には統括情報セキュリティ責任者に早急に報告を行うとともに、回復のための対策を講じなければならない。

ケ　情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて統括情報セキュリティ責任者にその内容を報告しなければならない。

（４）情報セキュリティ委員会

ア　センターの情報セキュリティ対策を統一的に行う権限及び責任を有する。

イ　情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する。

（兼務の禁止）

第６条　情報セキュリティ対策の実施において、やむを得ない場合を除き、承認または許可の申請を行う者とその承認又は許可者は、同じ者が兼務してはならない。

２　情報セキュリティ監査の実施において、やむを得ない場合を除き、監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。

（情報セキュリティインシデントに対する対応）

第７条　統括情報セキュリティ責任者は、情報セキュリティインシデントの統一的な窓口の機能を有する組織を整備し情報セキュリティインシデントについて、課等から報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。

２　統括情報セキュリティ責任者は、情報セキュリティ責任者を選任し、情報セキュリティ管理者をその代表に充てる。

３　情報セキュリティ責任者は、情報セキュリティインシデントを認知した時は、ほかの情報セキュリティ責任者及び情報セキュリティ管理者へ報告しなければならない。

４　情報セキュリティ管理者は、情報セキュリティインシデントを認知した時は、速やかに統括情報セキュリティ責任者に報告する。その後、その重要度や影響範囲等を勘案し、構成市などの関係機関や報道機関への通知・公表対応を行わなければならない。

第２章　情報資産の分類と管理方法

（情報資産の分類）

第８条　センターにおける情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

(1)　機密性による情報資産の分類

分類	分類基準	取扱制限
機密性３	センター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	・支給以外の端末での作業の原則禁止（機密性３の情報資産に対して） ・必要以上の複製及び配布禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体などの持込禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼できるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
機密性２	センター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	なし

(2)　完全性による情報資産の分類

分類	分類基準	取扱制限
完全性２	センターで取り扱う情報資産のうち、改竄、誤謬又は破損により、住民の権利が侵害される又はセンター事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
完全性１	完全性２の情報資産以外の情報資産	なし

(3)　可用性による情報資産の分類

分類	分類基準	取扱制限
可用性２	センターで取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又はセンター事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、指定する時間以外の復旧 ・電磁的記録媒体の施錠可能な場所への保管
可用性１	可用性２の情報資産以外の情報資産	なし

（情報資産の管理）

第９条　情報資産の管理は、次に定めるところにより行うものとする。

（１）管理責任

ア　情報セキュリティ責任者は、その所管する情報資産について管理責任を有する。

イ　情報資産が複製又は伝送された場合には、複製等された情報資産も前条の分類に基づき管理しなければならない。

（２）情報資産の分類の表示

職員等は、情報資産について、ファイル（ファイル名、ファイルの属性等)、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない。

（３）情報の作成

ア　職員等は、業務上必要のない情報を作成してはならない。

イ　情報を作成する者は、情報の作成時に前条の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

ウ　情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

（４）情報資産の入手

ア　センター内の者が作成した情報資産を入手した者は、入手元の情報資産

の分類に基づいた取扱いをしなければならない。

イ　センター外の者が作成した情報資産を入手した者は、前条の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

ウ　情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ責任者に判断を仰がなければならない。

（５）情報資産の利用

ア　情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

イ　情報資産を利用する者は、情報資産の分類に応じ適切な取扱いをしなければならない。

ウ　情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って当該電磁的記録媒体を取り扱わなければならない。

（６）情報資産の保管

ア　情報セキュリティ責任者又は情報セキュリティ管理者は、情報資産の分類に従って、情報資産を適切に保管しなければならない。

イ　情報セキュリティ責任者又は情報セキュリティ管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

ウ　情報セキュリティ責任者又は情報セキュリティ管理者は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。

エ　情報セキュリティ責任者又は情報セキュリティ管理者は、機密性２以上、完全性２又は可用性２の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

オ　情報の保存年限については、湖北広域行政事務センター文書管理規程（平成１８年５月１日訓令甲第４号）に従う。

（７）情報の送信

電子メール等により機密性２以上の情報を送信する者は、必要に応じ暗号化又はパスワード設定を行わなければならない。

（８）情報資産の運搬

ア　車両等により機密性２以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

イ　機密性２以上の情報資産を運搬する者は、情報セキュリティ責任者に許可を得なければならない。

（９）情報資産の提供・公表

ア　機密性２以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

イ　機密性２以上の情報資産を外部に提供する者は、情報セキュリティ責任者に許可を得なければならない。

ウ　情報セキュリティ責任者は、住民に公開する情報資産について、完全性を確保しなければならない。

（１０）情報資産の廃棄

ア　情報資産の廃棄を行う者は、情報を記録している電磁的記録媒体が不要になった場合は記録されている情報の機密性に応じ、当該電磁的記録媒体の情報を復元できないように処置した上で廃棄しなければならない。

イ　情報資産の廃棄を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

ウ　情報資産の廃棄を行う者は、情報セキュリティ責任者の許可を得なければならない。

（情報システム全体の強靭(じん)性の向上）

第９条の２　情報システム全体の強靭性の向上は、次に定めるところにより行うものとする。

（１）マイナンバー利用事務系

ア　マイナンバー利用事務系及び他の領域の分離

（ア）マイナンバー利用事務系及び他の領域は、総務課以外の職員が干渉できないようにしなければならない。

（イ）マイナンバー利用事務において外部に情報提供をする必要がある場合は、情報セキュリティ管理者の承認を得なければならない。

イ　情報のアクセス及び持出しにおける対策

（ア）情報のアクセス対策　情報システムが正規の利用者かどうかを判断するためにパスワード等による本人認証を利用しなければならない。

（イ）情報の持出し不可設定　ＵＳＢメモリその他の電磁的記録媒体からは、

原則として情報を持ち出すことができないように設定しなければならない。

（３）インターネット接続系

インターネット接続系においては、通信パケットの監視、迷惑メール等の排除など、情報セキュリティインシデントの早期発見及び対策を講じなければならない。

第３章　物理的セキュリティ

第１節　サーバ等の管理

（機器の取付け）

第１０条　情報セキュリティ責任者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

（機器の電源）

第１１条　情報セキュリティ責任者は、情報セキュリティ管理者及び施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適切に停止するまで
の間に十分な電力を供給する容量の予備電源を備え付けなければならない。

２　情報セキュリティ責任者は、情報セキュリティ管理者及び施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

（通信ケーブル等の配線）

第１２条　情報セキュリティ責任者及び情報セキュリティ管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等、必要な措置を講じなければならない。

２　情報セキュリティ責任者及び情報セキュリティ管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。

３　情報セキュリティ責任者及び情報セキュリティ管理者は、ネットワーク接続口に他者が容易に接続できないよう適切に管理しなければならない。

４　情報セキュリティ責任者及び情報セキュリティ管理者は、当該管理責任者、セキュリティ担当者及び契約により操作を認められた外部委託事業者を除き、配線を変更し、又は追加することができないように必要な措置を講じなければならない。

（機器の定期保守及び修理）

第１３条　情報セキュリティ責任者は、可用性２のサーバ等の機器の定期保守を実施しなければならない。

２　情報セキュリティ責任者は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報セキュリティ責任者は、外部の事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認などを行わなければならない。

（庁外への機器の設置）

第１４条　情報セキュリティ責任者は、庁外にサーバ等の機器を設置する場合、情報セキュリティ管理者及び統括情報セキュリティ責任者の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（機器の廃棄等）

第１５条　情報セキュリティ管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

第２節　管理区域（情報システム室等）の管理

（管理区域）

第１６条　管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための部屋（以下「情報システム室」という。）又は電磁的記録媒体の保管庫をいう。

２　管理区域から外部に通ずるドアは必要最小限とし、施錠により許可のない立ち入りを防止しなければならない。

３　管理区域への入退室は、許可された者のみに制限するなど、入退室の管理を行わなければならない。

４　情報システム室内の機器等には、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

５　管理区域に配置する消火薬剤、消防用設備等が、機器、電磁的記録媒体等に影響を与えないようにしなければならない。

６　職員等又は外部委託事業者が、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

（機器等の搬入出）

第１７条　情報セキュリティ管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員等又は委託した業者に確認を行わせなければならない。

２　情報セキュリティ管理者は、情報システム室の機器等の搬入出について、職員等を立ち会わせなければならない。

第３節　ネットワークの管理

（通信回線及び通信回線装置の管理）

第１８条　情報セキュリティ管理者は、センター内の通信回線及び通信回線装置について、適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

（外部へのネットワーク接続）

第１９条　情報セキュリティ管理者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

（情報システムの通信回線の接続）

第２０条　情報セキュリティ管理者は、機密性２以上の情報資産を取扱い、情報システム通信回線を接続する場合、必要なセキュリティ水準を検討の上、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

（完全性の確保）

第２１条　情報セキュリティ管理者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施しなければならない。

（可用性の確保）

第２２条　情報セキュリティ管理者は、可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ冗長構成にする等の措置を講じなければならない。

第４節　端末等の管理

（盗難防止措置）

第２３条　情報セキュリティ管理者は、盗難防止のため施錠管理等の物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

（情報システムへのログイン）

第２４条　情報セキュリティ管理者は、情報システムへのログインに際し、パスワ

ードによる認証情報の入力を必要とするように設定しなければならない。

（データの暗号化）

第２５条　情報セキュリティ責任者は、パソコンやモバイル端末におけるデータの暗号化の機能を有効に利用しなければならない。

２　情報セキュリティ責任者は、端末にセキュリティチップが搭載されている場合は、その機能を有効に利用しなければならない。

３　情報セキュリティ責任者は、データの暗号化の機能を備える電磁的記録媒体を使用しなければならない。

第４章　人的セキュリティ

第１節　職員等の遵守事項

（情報セキュリティポリシー等の遵守）

第２６条　職員等は、情報セキュリティポリシー等を遵守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不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ責任者に相談し、指示を仰がなければならない。

（業務以外の目的での使用の禁止）

第２７条　職員等は、業務以外の目的で情報資産の外部への持出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

（モバイル端末や電磁的記録媒体等の持出し及び外部における情報処理作業の制限）

第２８条　統括情報セキュリティ責任者は、機密性２以上、可用性２、完全性２の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

２　職員等は、センターのモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ責任者の許可を得なければならない。

３　職員等は、外部で情報処理業務を行う場合には、情報セキュリティ責任者の許可を得なければならない。

（支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用）

第２９条　職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、業務上必要な場合は、支給以外のパソコン、モバイル端末及び電磁的記録媒体の業務利用の可否判断を情報セキュリテ

ィ責任者が行う。

２　職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には情報セキュリティ責任者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置に関する規定を遵守しなければならない。

（持出し及び持込みの記録）

第３０条　情報セキュリティ責任者は、端末等の持出し及び持込みについて、記録を作成し、保管しなければならない。

（パソコンやモバイル端末におけるセキュリティ設定変更の禁止）

第３１条　職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。

（机上の端末等の管理）

第３２条　職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ責任者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適切な措置を講じなければならない。

（退職時等の遵守事項）

第３３条　職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

（会計年度任用職員への対応）

第３４条　情報セキュリティ責任者は、会計年度任用職員に対し、採用時に情報セキュリティポリシー等のうち、会計年度任用職員が守るべき内容を理解させ、また実施及び遵守させなければならない。

２　情報セキュリティ責任者は、会計年度任用職員の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

３　情報セキュリティ責任者は、会計年度任用職員にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

（情報セキュリティポリシー等の掲示）

第３５条　情報セキュリティ責任者は、職員等が常に情報セキュリティポリシー等を閲覧できるように掲示しなければならない。

（委託事業者に対する説明）

第３６条　情報セキュリティ責任者は、ネットワーク及び情報システムの開発・保守等を委託事業者に発注する場合、再委託業者も含めて、情報セキュリティポリシー等のうち委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

第２節　研修・訓練

（情報セキュリティに関する研修）

第３７条　統括情報セキュリティ責任者は、定期的に情報セキュリティに関する研修を実施しなければならない。

２　統括情報セキュリティ責任者は、職員等が毎年度最低１回は情報セキュリティに関する研修を受講できるようにしなければならない。

（緊急時対応訓練）

第３８条　統括情報セキュリティ責任者は、緊急時対応を想定した訓練を定期的に実施しなければならない。

（情報セキュリティに関する研修・訓練への参加）

第３９条　全ての職員等は、定められた情報セキュリティに関する研修・訓練に参加しなければならない。

第３節　情報セキュリティインシデントの報告

（住民等による外部からの情報セキュリティインシデントの報告）

第４０条　職員等は、センターが管理するネットワーク、情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等による外部からの報告を受けた場合は情報セキュリティ責任者に報告しなければならない。

２　前項の規定による報告を受けた情報セキュリティ責任者は、速やかに統括情報セキュリティ責任者及び情報セキュリティ管理者に報告しなければならない。

（情報セキュリティインシデント原因の究明・記録、再発防止等）

第４１条　情報セキュリティ管理者は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

２　情報セキュリティ管理者は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。

３　情報セキュリティ管理者は、情報セキュリティインシデント原因を究明し、記録を保存しなければならない。この場合において、情報セキュリティインシデントの原因を究明した結果から、再発防止策を検討し、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。
４　統括情報セキュリティ責任者は、情報セキュリティ管理者から情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

第４節　ＩＤ及びパスワード等の管理

（ＩＤの取扱い）

第４２条　職員等は、自己の管理するＩＤに関し、次の事項を遵守しなければならない。

（１）自己が利用しているＩＤは、他人に利用させてはならない。

（２）共用ＩＤを利用する場合は、共用ＩＤの利用者以外に利用させてはならない。

（パスワードの取扱い）

第４３条　職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

（１）パスワードは、他者に知られないように管理しなければならない。

（２）パスワードは秘密にし、パスワードの照会等には一切応じてはならない。

（３）パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。

（４）パスワードが流出したおそれがある場合には、情報セキュリティ責任者に速やかに報告し、パスワードを速やかに変更しなければならない。

（５）複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。

（６）仮のパスワード（初期パスワードを含む。）は、最初のログイン時点で変更しなければならない。

（７）サーバ、ネットワーク機器及びパソコンの端末にパスワードを記憶させてはならない。

（８）職員等の間でパスワードを共有してはならない。ただし、共有ＩＤに対するパスワードは除く。

第５章　技術的セキュリティ

第１節　コンピュータ及びネットワークの管理

（ファイルサーバの設定等）

第４４条　情報セキュリティ管理者は、職員等が使用できるファイルサーバの容量

を設定し、職員等に周知しなければならない。

２　情報セキュリティ管理者は、ファイルサーバを課・施設等の単位で構成し、職員等が他課・施設等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

３　情報セキュリティ管理者は、住民の個人情報、人事記録等、特定の職員等しか取扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一課等であっても、担当職員等以外の職員等が閲覧及び使用できないようにしなければならない。

（バックアップの実施）

第４５条　情報セキュリティ責任者及び情報セキュリティ管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

（他団体との情報システムに関する情報等の交換）

第４６条　情報セキュリティ責任者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、統括情報セキュリティ責任者及び情報セキュリティ管理者の許可を得なければならない。

（システム管理記録及び作業の確認）

第４７条　情報セキュリティ責任者は、所管するシステムにおいてシステム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない。

２　情報セキュリティ管理者、情報セキュリティ責任者又はセキュリティ担当者及び契約により操作を認められた委託事業者がシステム変更等の作業を行う場合は、２人以上で作業し、互いにその作業を確認しなければならない。

（情報システム仕様書等の管理）

第４８条　統括情報セキュリティ責任者及び情報セキュリティ管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適切に管理しなければならない。

（ログの取得等）

第４９条　情報セキュリティ責任者及び情報セキュリティ管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

２　情報セキュリティ責任者及び情報セキュリティ管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。

３　情報セキュリティ責任者及び情報セキュリティ管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

（障害記録）

第５０条　情報セキュリティ責任者及び情報セキュリティ管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない。

（ネットワークの接続制御、経路制御等）

第５１条　情報セキュリティ管理者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

２　情報セキュリティ管理者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない。

（外部の者が利用できるシステムの分離等）

第５２条　情報セキュリティ管理者は、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

（外部ネットワークとの接続制限等）

第５３条　情報セキュリティ責任者は、所管するネットワークを外部ネットワークと接続しようとする場合には、情報セキュリティ管理者及び統括情報セキュリティ責任者の許可を得なければならない。

２　情報セキュリティ責任者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、センター内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

３　情報セキュリティ責任者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

４　情報セキュリティ管理者は、ウェブサーバ等をインターネットに公開する場

合、センター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しなければならない。

５　情報セキュリティ責任者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、情報セキュリティ管理者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

（複合機のセキュリティ管理）

第５４条　情報セキュリティ管理者は、複合機を調達する場合は当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適切なセキュリティ要件を策定しなければならない。

２　情報セキュリティ管理者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

３　情報セキュリティ管理者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消し、又は再利用できないようにする対策を講じなければならない。

（ＩｏＴ機器を含む特定用途機器のセキュリティ管理）

第５５条　情報セキュリティ管理者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

（無線ＬＡＮ及びネットワークの盗聴対策）

第５６条　情報セキュリティ管理者は、無線ＬＡＮの利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

２　情報セキュリティ管理者は、機密性の高い情報を取り扱うネットワークについて情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

（電子メールのセキュリティ管理）

第５７条　情報セキュリティ管理者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

２　情報セキュリティ管理者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止しなければならない。

３　情報セキュリティ管理者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

４　情報セキュリティ管理者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。
５　情報セキュリティ管理者は、システム開発や運用、保守等のため作業する委託事業者の作業員による電子メールアドレス利用について、委託事業者との間で利用方法を取り決めなければならない。

（電子メールの利用制限）

第５８条　職員等は、情報セキュリティ責任者の許可なく、自動転送機能を用いて、電子メールを転送してはならない。
２　職員等は、業務上必要のない送信先に電子メールを送信してはならない。
３　職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。
４　職員等は、重要な電子メールを誤送信した場合、情報セキュリティ責任者に報告し、必要な措置をとらなければならない。

（電子署名・暗号化）

第５９条　職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、情報セキュリティ管理者が定めた電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。
２　職員等は、暗号化を行う場合に情報セキュリティ管理者が定める以外の方法を用いてはならない。また、情報セキュリティ管理者が定めた方法で暗号のための鍵を管理しなければならない。
３　情報セキュリティ管理者は、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

（無許可ソフトウェアの導入等の禁止）

第６０条　職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。
２　職員等は、業務上の必要がある場合は、情報セキュリティ管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ責任者がソフトウェアのライセンスを管理しなければならない。
３　職員等は、不正にコピーしたソフトウェアを利用してはならない。

（機器構成の変更の制限）

第６１条　職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。

２　職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、情報セキュリティ責任者及び情報セキュリティ管理者の許可を得なければならない。

（業務外でのネットワーク接続の禁止）

第６２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セキュリティ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。

（業務以外の目的でのウェブ閲覧の禁止）

第６３条　職員等は、業務以外の目的でウェブを閲覧してはならない。

２　情報セキュリティ責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し適切な措置を求めなければならない。

（Ｗｅｂ会議サービスの利用時の対策）

第６３条の２　情報セキュリティ管理者は、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、センター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、センター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６３条の３　情報セキュリティ管理者は、センター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）センターのアカウントによる情報発信が、実際にセンターのものであることを明らかにするために、センターの自己管理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、センターの自己管理Ｗｅｂサイトに当該情報を掲載して参照可能とすること。

第２節　アクセス制御

（アクセス制御等）

第６４条　情報セキュリティ管理者は、所管するネットワーク又は情報システムごとに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、システム上制限しなければならない。

（利用者ＩＤの取扱い）

第６５条　情報セキュリティ管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者ＩＤの取扱い等の方法を定めなければならない。

２　職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、情報セキュリティ責任者に通知しなければならない。

３　情報セキュリティ管理者は、利用されていないＩＤが放置されないよう、人事管理部門と連携し、点検しなければならない。

（特権を付与されたＩＤの管理等）

第６６条　情報セキュリティ管理者は、管理者権限等の特権を付与されたＩＤを利用する者を必要最小限にし、当該ＩＤのパスワードの漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理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セキュリティ管理者の特権を代行する者は、統括情報セキュリティ責任者及び情報セキュリティ管理者が指名し、情報セキュリティ委員会が認めた者でなければならない。

３　情報セキュリティ責任者は、特権を付与されたＩＤ及びパスワードの変更について、外部委託事業者に行わせてはならない。

４　情報セキュリティ責任者は、特権を付与されたＩＤ及びパスワードについて、職員等の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。

５　情報セキュリティ管理者は、特権を付与されたＩＤを初期設定以外のものに変更しなければならない。

（職員等による外部からのアクセス等の制限）

第６７条　職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、情報セキュリティ管理者の許可を得なければならない。

２　情報セキュリティ管理者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

３　情報セキュリティ管理者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

４　情報セキュリティ管理者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の必要な措置を講じなければならない。

５　情報セキュリティ管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

６　職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末をセンター内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し、及び情報セキュリティ責任者の許可を得、又は情報セキュリティ責任者によって事前に定義されたポリシーに従って接続しなければならない。

７　情報セキュリティ管理者は、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原則として禁止しなければならない。

（ログイン時の表示等）

第６８条　情報セキュリティ管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ職員等がログインしたことを確認することができるようシステムを設定しなければならない。

（認証情報の管理）

第６９条　情報セキュリティ責任者又は情報セキュリティ管理者は、職員等の認証情報を厳重に管理しなければならない。認証情報ファイルを不正利用から保護するため、オペレーティングシステム等で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

２　情報セキュリティ責任者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させなければならない。

３　情報セキュリティ責任者は、認証情報の不正利用を防止するための措置を講じなければならない。

（特権による接続時間の制限）

第７０条　情報セキュリティ管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

第３節　システム開発、導入、保守等

（情報システムの調達）

第７１条　情報セキュリティ管理者は、情報システムの開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

２　情報セキュリティ管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（情報システムの開発）

第７２条　情報セキュリティ管理者は、システム開発にあたっては、次の事項を定める。

（１）システム開発における責任者及び作業者の特定

情報セキュリティ管理者は、システム開発の責任者及び作業者を特定しなければならない。また、システム開発のための規則を確立しなければならない。

（２）システム開発における責任者、作業者のＩＤの管理

ア　情報セキュリティ管理者は、システム開発の責任者及び作業者が使用するＩＤを管理し、開発完了後、開発用ＩＤを削除しなければならない。

イ　情報セキュリティ管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならない。

（３）システム開発に用いるハードウェア及びソフトウェアの管理

ア　情報セキュリティ管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

イ　情報セキュリティ管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

（情報システムの導入）

第７３条　情報セキュリティ管理者は、システム導入にあたっては、次の事項を定める。

（１）開発環境と運用環境の分離及び移行手順の明確化

ア　情報セキュリティ管理者は、システム開発・保守及びテスト環境とシステム運用環境を分離しなければならない。

イ　情報セキュリティ管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

ウ　情報セキュリティ管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

エ　情報セキュリティ管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

（２）テスト

ア　情報セキュリティ管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

イ　情報セキュリティ管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

ウ　情報セキュリティ管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

エ　情報セキュリティ管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

（システム開発・保守に関連する資料等の整備・保管）

第７４条　情報セキュリティ責任者は、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。

２　情報セキュリティ責任者は、テスト結果を一定期間保管しなければならない。

３　情報セキュリティ責任者は、情報システムに係るソースコードを適切な方法で保管しなければならない。

（情報システムにおける入出力データの正確性の確保）

第７５条　情報セキュリティ責任者は、情報システムに入力されるデータについ

て、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

２　情報セキュリティ責任者は、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に、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しなければならない。

３　情報セキュリティ責任者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

（情報システムの変更管理）

第７６条　情報セキュリティ責任者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

（開発・保守用のソフトウェアの更新等）

第７７条　情報セキュリティ責任者は、開発・保守用のソフトウェア等を更新、又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

（システム更新又は統合時の検証等）

第７８条　情報セキュリティ責任者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

第４節　不正プログラム対策

（情報セキュリティ管理者の措置事項）

第７９条　情報セキュリティ管理者は、不正プログラム対策として、次の事項を措置しなければならない。

（１）外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

（２）外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

（３）コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

（４）所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

（５）不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

（６）不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

（７）業務で利用するソフトウェアは、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したソフトウェアを利用してはならない。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。

（情報セキュリティ責任者の措置事項）

第８０条　情報セキュリティ責任者は、不正プログラム対策に関し、次の事項を措置しなければならない。

（１）情報セキュリティ責任者は、その所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させなければならない。

（２）不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

（３）不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

（４）インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、センターが管理している媒体以外を職員等に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

（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、情報セキュリティ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。

（職員等の遵守事項）

第８１条　職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

（１）パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

（２）外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラ

ム対策ソフトウェアによるチェックを行わなければならない。

（３）差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

（４）端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

（５）添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。

（６）情報セキュリティ管理者が提供するウイルス情報を、常に確認しなければならない。

（７）コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、事前に決められたコンピュータウイルス等感染時の初動対応の手順に従って対応を行わなければならない。この場合において、初動対応時の手順が定められていないときは、被害の拡大を防ぐ処置を慎重に検討し、該当の端末においてＬＡＮケーブルの取外し、通信を行わない設定への変更等を実施しなければならない。

（専門家の支援体制）

第８２条　統括情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

第５節　不正アクセス対策

（情報セキュリティ管理者の措置事項）

第８３条　情報セキュリティ管理者は、不正アクセス対策として、以下の事項を措置しなければならない。

（１）使用されていないポートを閉鎖しなければならない。

（２）不要なサービスについて、機能を削除又は停止しなければならない。

（３）不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括情報セキュリティ責任者へ通報するよう設定しなければならない。

（４）情報セキュリティ管理者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適切な対応などを実施できる体制並びに連絡網を構築しなければならない。

（攻撃への対処）

第８４条　統括情報セキュリティ責任者は、サーバ等に攻撃を受けた場合又は受け

るリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

（記録の保存）

第８５条　統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

（内部からの攻撃）

第８６条　情報セキュリティ管理者は、職員等が使用しているパソコン等の端末からのセンター内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（職員等による不正アクセス）

第８７条　情報セキュリティ管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課等の情報セキュリティ責任者に通知し、適切な処置を求めなければならない。

（サービス不能攻撃）

第８８条　情報セキュリティ管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

（標的型攻撃）

第８９条　情報セキュリティ管理者は、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６節　セキュリティ情報の収集

（セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等）

第９０条　情報セキュリティ管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

（不正プログラム等のセキュリティ情報の収集・周知）

第９１条　情報セキュリティ管理者は、不正プログラム等のセキュリティ情報を収

集し、必要に応じ対応方法について、職員等に周知しなければならない。

（情報セキュリティに関する情報の収集及び共有）

第９２条　情報セキュリティ管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

第６章　運用

第１節　情報システムの監視

（情報システムの監視）

第９３条　情報セキュリティ管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

（時刻同期）

第９４条　情報セキュリティ管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

（外部と接続するシステムの監視）

第９５条　情報セキュリティ管理者は、外部と常時接続するシステムを常時監視しなければならない。

第２節　情報セキュリティポリシーの遵守状況の確認

（遵守状況の確認及び対処）

第９６条　情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに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。

２　統括情報セキュリティ責任者は、発生した問題について、適切かつ速やかに対処しなければならない。

３　情報セキュリティ管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適切かつ速やかに対処しなければならない。

（パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査）

第９７条　統括情報セキュリティ責任者及び統括情報セキュリティ責任者が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

（職員等の報告義務）

第９８条　職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに情報セキュリティ責任者及び情報セキュリティ管理者に報告を行わなければならない。

２　前項の違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると情報セキュリティ管理者が判断した場合において、職員等は、緊急時対応計画に従って適切に対処しなければならない。

第３節　侵害時の対応等

（緊急時対応計画の策定）

第９９条　統括情報セキュリティ責任者及び情報セキュリティ委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適切に対処しなければならない。

（緊急時対応計画に盛り込むべき内容）

第１００条　緊急時対応計画には、以下の内容を定めなければならない。

（１）関係者の連絡先

（２）発生した事案に係る報告すべき事項

（３）発生した事案への対応措置

（４）再発防止措置の策定

（業務継続計画との整合性確保）

第１０１条　自然災害、大規模・広範囲に感染が広がる疾病等に備えて別途業務継続計画を策定し、情報セキュリティ委員会は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

（緊急時対応計画の見直し）

第１０２条　統括情報セキュリティ責任者又は情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

第４節　例外措置

（例外措置の許可）

第１０３条　統括情報セキュリティ責任者又は情報セキュリティ管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継

続するため、遵守事項とは異なる方法を採用すること又は遵守事項を実施しないことについて合理的な理由がある場合には、情報セキュリティ委員会の許可を得て、例外措置を取ることができる。

（緊急時の例外措置）

第１０４条　情報セキュリティ管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに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。

（例外措置の申請書の管理）

第１０５条　統括情報セキュリティ責任者は、例外措置の申請書及び審査結果を適切に保管し、定期的に申請状況を確認しなければならない。

（法令遵守）

第１０６条　職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

（１）地方公務員法（昭和２５年法律第２６１号）

（２）著作権法（昭和４５年法律第４８号）

（３）不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）

（４）個人情報の保護に関する法律（平成１５年法律第５７号）

（５）行政手続における特定の個人を識別するための番号の利用等に関する法律（平成２５年法律第２７号）

（６）サイバーセキュリティ基本法（平成２８年法律第３１号）

（７）湖北広域行政事務センター個人情報の保護に関する法律施行条例（令和７年湖北広域行政事務センター条例第２号）

（懲戒処分）

第１０７条　情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

（違反時の対応）

第１０８条　職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

（１）統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該職員等が所属する課等の情報セキュリティ責任者に通知し、適切な措置を求めなければならない。

（２）情報セキュリティ管理者等が違反を確認した場合は、違反を確認した者は速

やかに統括情報セキュリティ責任者及び当該職員等が所属する課等の情報セキュリティ責任者に通知し、適切な措置を求めなければならない。

（３）情報セキュリティ責任者の指導によっても改善されない場合、情報セキュリティ管理者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、情報セキュリティ管理者は、職員等の権利を停止あるいは剥奪した旨を統括情報セキュリティ責任者及び当該職員等が所属する課等の情報セキュリティ責任者に通知しなければならない。

第７章　業務委託と外部サービスの利用

第１節　業務委託

（委託事業者の選定基準）

第１０９条　情報セキュリティ責任者は、委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

２　情報セキュリティ責任者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況情報セキュリティ監査の実施状況等を参考にして、委託事業者を選定しなければならない。

（契約項目）

第１１０条　重要な情報資産を取扱う業務を委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

（１）情報セキュリティポリシーの遵守

（２）委託事業者の責任者、委託内容、作業者、作業場所の特定

（３）提供されるサービスレベルの保証

（４）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等、情報のライフサイクル全般での管理方法

（５）委託事業者の従業員に対する教育の実施

（６）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

（７）業務上知り得た情報の守秘義務

（８）再委託に関する制限事項の遵守

（９）委託業務終了時の情報資産の返還、廃棄等

（１０）委託業務の定期報告及び緊急時報告義務

（１１）センターによる監査、検査

（１２）センターによる情報セキュリティインシデント発生時の公表
（１３）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
（確認・措置等）
第１１１条　情報セキュリティ責任者は、委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、前条の契約に基づき措置しなければならない。また、その内容を情報セキュリティ管理者に報告するとともに、その重要度に応じ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１１２条　情報セキュリティ管理者は、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１１３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センター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、センター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センター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センター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、必要に応じてセンター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センターに提供し、センター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　情報セキュリティ管理者は、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１１４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なければならない。

（外部サービスの利用承認）

第１１５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１１６条　情報セキュリティ管理者は、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１１７条　情報セキュリティ管理者は、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１１８条　情報セキュリティ管理者は、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１１９条　情報セキュリティ管理者は、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１２０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。

第８章　評価・見直し

第１節　監査

（監査の目的）

第１２１条　センターの情報セキュリティポリシーに基づき、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況の監査を行い、情報セキュリティの維持と質の向上に資することとする。

（監査担当者）

第１２２条　情報セキュリティ監査は総務課が担当し、監査責任者を総務課長とする。

２　監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者をもってする。

（監査の実施と協力）

第１２３条　情報セキュリティ監査を行うに当たって、監査責任者は実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。

２　被監査部門は、監査の実施に協力しなければならない。

（委託事業者に対する監査）

第１２４条　事業者に業務委託を行っている場合、情報セキュリティ監査責任者は、委託事業者（再委託事業者を含む。）に対して、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

（報告）

第１２５条　監査責任者は、監査結果を取りまとめ、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。

（保管）

第１２６条　監査責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

（監査結果への対応）

第１２７条　統括情報セキュリティ責任者は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。この場合において、指摘事項を所管していない情報セキュリティ責任者に対しても、同種の課題及び問題点がある可能性が高いとき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。

（情報セキュリティポリシー及び関係規程等の見直し等への活用）

第１２８条　情報セキュリティ委員会は、監査結果を情報セキュリティポリシー及び関係規定等の見直しその他情報セキュリティ対策の見直し時に活用しなければならない。

第２節　自己点検

（自己点検の実施）

第１２９条　統括情報セキュリティ責任者、情報セキュリティ管理者及び情報セキュリティ責任者は、情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行わなければならない。

（報告）

第１３０条　統括情報セキュリティ責任者、情報セキュリティ管理者及び情報セキュリティ責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティ委員会に報告しなければならない。

（自己点検結果の活用）

第１３１条　職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

２　情報セキュリティ委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

第３節　改善

（情報セキュリティポリシー及び関係規程等の見直し）

第１３２条　情報セキュリティ委員会は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。