山　形　市
情報セキュリティ対策基準

平成２８年４月
令和元年５月改定
令和５年10月改定
令和６年４月改定
令和７年１月改定

山　形　市

■目　次

山形市情報セキュリティ対策基準

１　対象範囲

（１）行政機関の範囲

本対策基準が適用される行政機関は、市長部局、行政委員会、議会事務局、消防本部及び上下水道部とする。（以下「本市」という。）但し、教育委員会の学校においては、マイナンバー利用系、ＬＧＷＡＮ接続系、インターネット接続系を取扱う範囲をその範囲とする。

２　組織体制

（１）最高情報セキュリティ責任者（ＣＩＳＯ：Chief Information Security Officer、以下「ＣＩＳＯ」という。）

①副市長（企画調整部に属する事務を担任する副市長をいう。以下同じ。）をＣＩＳＯとする。ＣＩＳＯは、本市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。

②ＣＩＳＯ は、ＣＩＳＯ を助けて本市における情報セキュリティに関する事務を整理し、ＣＩＳＯ の命を受けて本市の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者（以下「副ＣＩＳＯ」という。）１人を必要に応じて置く。

③ＣＩＳＯ は、本対策基準に定められた自らの担務を、副ＣＩＳＯ その他の本対策基準に定める責任者に担わせることができる。

（２）統括情報セキュリティ責任者

①企画調整部長をＣＩＳＯ直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は、ＣＩＳＯ及び副ＣＩＳＯ（以下「ＣＩＳＯ等」という。）を補佐しなければならない。

②統括情報セキュリティ責任者は、本市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。

③統括情報セキュリティ責任者は、本市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。

④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、情報セキュリティ管理者、個別システム管理者、及び情報セキュリティ担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

⑤統括情報セキュリティ責任者は、本市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、ＣＩＳＯ等又は副ＣＩＳＯの指示に従い、ＣＩＳＯ及び副ＣＩＳＯが不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。

⑥統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、ＣＩＳＯ、副ＣＩＳＯ、統括情報セキュリティ責任者、情報セキュリティ責任者、情報

セキュリティ管理者、個別システム管理者、情報セキュリティ担当者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。

⑦統括情報セキュリティ責任者は、緊急時にはＣＩＳＯ及び副ＣＩＳＯ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。

⑧統括情報セキュリティ責任者は、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ＣＩＳＯ及び副ＣＩＳＯにその内容を報告しなければならない。

（３）情報セキュリティ責任者

①情報企画課長を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は、統括情報セキュリティ責任者を補佐しなければならない。

③情報セキュリティ責任者は、共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

④情報セキュリティ責任者は、情報システムについて、緊急時等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（職員、再任用職員、会計年度任用職員及び臨時職員の他、情報セキュリティ責任者の許可を得て情報資産を取り扱う者をいう。以下同じ。）に対する研修、訓練、助言及び指示を行う。

（４）情報セキュリティ管理者

①各課等の長を情報セキュリティ管理者とする。

②情報セキュリティ管理者は、所管する課等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。

③情報セキュリティ管理者は、所管する課等において、情報資産に対するセキュリティ侵害が発生した場合またはセキュリティ侵害のおそれがある場合には、情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。

（５）個別システム管理者

①課等において自ら導入、設置した情報システム、コンピュータまたはネットワーク（以下「個別システム等」という。）を有する課等の長を個別システム管理者とする。

②個別システム管理者は、所管する個別システム等における開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③個別システム管理者は、所管する個別システム等における情報セキュリティに関する権限及び責任を有する。

④個別システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

（６）情報セキュリティ担当者

各課等のＩＴ推進リーダー（「ｅ－リーダー」）を情報セキュリティ担当者とする。

（７）電子情報処理推進委員会

本市の情報セキュリティ対策を統一的に行うため、電子情報処理推進委員会において、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。

（８）兼務の禁止

①情報セキュリティ対策の実施において、止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れを承認または許可する者は、同じ者が兼務してはならない。

②監査を受ける者とその監査を実施する者は、止むを得ない場合を除き、同じ者が兼務してはならない。

（９）ＣＳＩＲＴ（Computer Security Incident Response Team）の設置・役割

①統括情報セキュリティ責任者は、ＣＳＩＲＴを整備し、その役割を明確化しなければならない。

②統括情報セキュリティ責任者をＣＳＩＲＴ責任者とし、ＣＳＩＲＴ責任者は、ＣＳＩＲＴに所属する職員を選任しなければならない。また、ＣＳＩＲＴ内の業務統括及び外部との連携等を行う職員を定めなければならない。

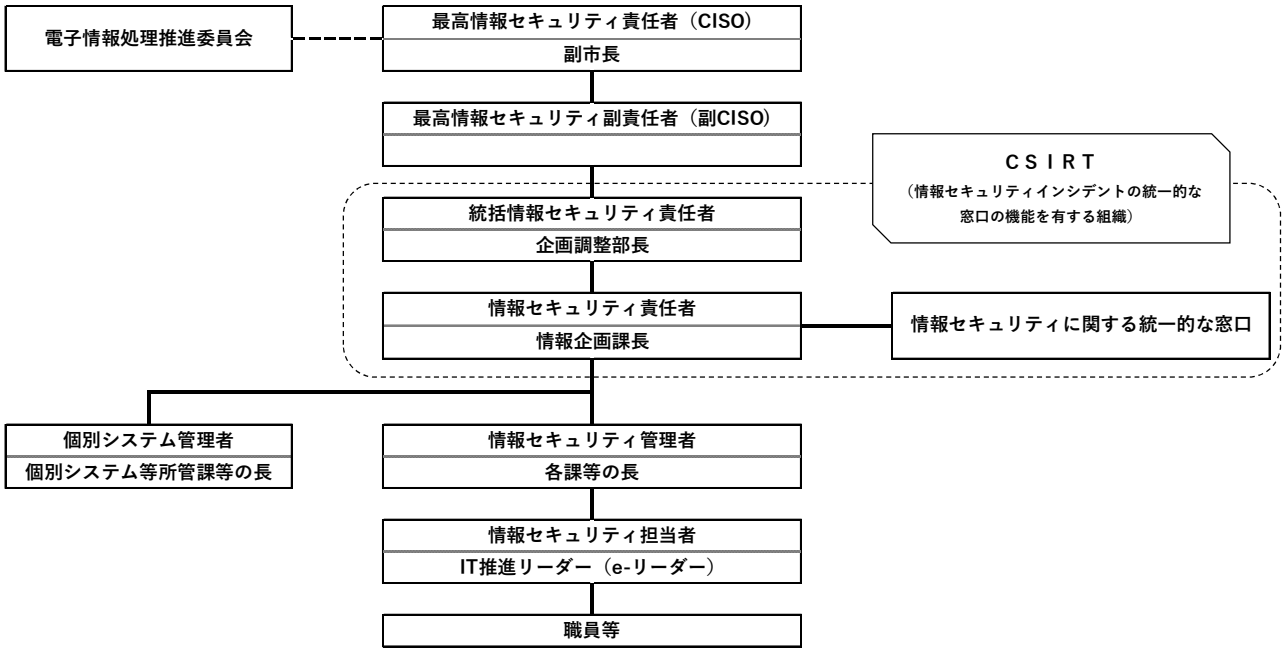
③統括情報セキュリティ責任者は、情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて各課等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。

④統括情報セキュリティ責任者は、電子情報処理推進委員会による情報セキュリティ戦略の意思決定が行われた際には、その内容を各課等に提供しなければならない。

⑤情報セキュリティインシデントを認知した場合には、ＣＩＳＯ、副ＣＩＳＯ、総務省、山形県等へ報告しなければならない。

⑥情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。

⑦情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行わなければならない。



（１０）クラウドサービス利用における組織体制

①統括情報セキュリティ責任者は、クラウドサービスを利用する際には、複数の事業者の存在・責任の所在を確認し、複数の事業者が存在する場合は、必要な連絡体制を構築しなければならない。また、クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制を確立しなければならない。

３　情報資産の分類と管理方法

（１）情報資産の分類

本市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。

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１	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	・支給以外の端末での作業の原則禁止（機密性１の情報資産に対して） ・必要以上の複製及び配付の禁止 ・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等の持ち込みの禁止 ・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 ・信頼の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	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３	機密性１または機密性２以外の情報資産	

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１	行政事務で取り扱う情報資産のうち、改ざん、誤びゅうまたは破損により、住民の権利が侵害されるまたは行政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	・バックアップの実施 ・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２	完全性１の情報資産以外の情報資産	

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１	行政事務で取り扱う情報資産のうち、滅失、紛失また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または行政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	・バックアップの実施 ・指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
可用性２	可用性１の情報資産以外の情報資産	

（２）情報資産の管理

①管理責任

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

（イ）情報セキュリティ管理者は、情報資産が複製または伝送された場合には、複製等された情報資産も（１）の分類に基づき管理しなければならない。

（ウ）情報セキュリティ管理者は、クラウドサービスの環境に保存される情報資産についても（１）の分類に基づき管理しなければならない。また、情報資産におけるライフサイクル（作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等）の取扱いを定める。クラウドサービスを更改する際の情報資産の移行及びこれらの情報資産の全ての複製のクラウドサービス事業者からの削除の記述を含むサービス利用の終了に関する内容について、サービス利用前に文書での提示を求め、又は公開されている内容を確認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（プロパティ）、ヘッダー・フッター等）、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正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）情報を作成する場合、職員等は、情報の作成時に（１）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）情報を作成する場合、職員等は、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）職員等が作成した情報資産を入手した場合、職員等は、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）職員等以外の者が作成した情報を入手した場合、職員等は、（１）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）入手した情報資産の分類が不明な場合、職員等は、情報セキュリティ管理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場合、職員等は、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場合、職員等は、情報資産の分類に応じ、適正な取扱いをしなければならない。

（ウ）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、職員等は、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）情報セキュリティ管理者および個別システム管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。

（イ）情報セキュリティ管理者および個別システム管理者は、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）情報セキュリティ管理者および個別システム管理者は、機密性１、機密性２、完全性１または可用性１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。

⑦情報の送信

電子メール等により機密性１または機密性２の情報を送信する場合、職員等は、パスワード等による暗号化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１または機密性２の情報資産を運搬する場合、職員等は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、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場合、職員等は、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１または機密性２の情報資産を外部に提供する場合、職員等は、パスワード等による暗号化を行わなければならない。

（イ）機密性１または機密性２の情報資産を外部に提供する場合、職員等は、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）情報セキュリティ管理者は、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情報資産の廃棄等

（ア）情報資産の廃棄やリース返却等を行う場合、職員等は、その情報の機密性に応じ、情報を復元できないように処置しなければならない。

（イ）情報資産の廃棄やリース返却等を行う場合、職員等は、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）情報資産の廃棄やリース返却等を行う場合、職員等は、情報セキュリティ管理者の許可を得なければならない。

（エ）クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理しなければならない。

４　情報システム全体の強靭性の向上

本市が運用する情報システム及び当該システムで取扱うデータを次のとおり領域分けし、強靭性向上のため、それぞれ必要な対策を実施する。

（１）マイナンバー利用事務系

（２）ＬＧＷＡＮ接続系

（３）インターネット接続系

（４）その他ネットワーク系

（１）から（３）以外の情報システム及び当該情報システムで取扱うデータをいう。

４．１　マイナンバー利用事務系

（１）マイナンバー利用事務系と他の領域との分離

情報セキュリティ責任者は、マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定(ＭＡＣアドレス、ＩＰアドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、外部接続先もインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、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の移送を可能とする。

（２）情報のアクセス及び持ち出しにおける対策

①情報のアクセス対策

情報セキュリティ責任者及び個別システム管理者は、所管する情報システムにおいて、情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上

を併用する認証（多要素認証）を利用しなければならない。

②情報の持ち出し不可設定

情報セキュリティ責任者及び個別システム管理者は、所管する情報システムにおいて、原則として、ＵＳＢメモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

③マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの扱い

マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるガバメントクラウド上の情報システムの領域については、マイナンバー利用事務系として扱い、本市の他の領域とはネットワークを分離しなければならない。

④マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱い

マイナンバー利用事務系の情報システムをガバメントクラウドにおいて利用する場合は、その情報資産の機密性を考慮し、暗号による対策を実施する。その場合、暗号は十分な強度を持たなければならない。

また、クラウドサービス事業者が暗号に関する対策を行う場合又はクラウドサービス事業者が提供する情報資産を保護するための暗号機能を利用する場合、クラウドサービス事業者が提供するそれらの機能や内容について情報を入手し、その機能について理解に努め、必要な措置を行わなければならない。

４．２　ＬＧＷＡＮ接続系

（１）ＬＧＷＡＮ接続系とインターネット接続系の分割

情報セキュリティ責任者は、ＬＧＷＡＮ接続系とインターネット接続系において両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータをＬＧＷＡＮ接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

①インターネット環境で受信したインターネットメールの本文のみをＬＧＷＡＮ接続系に転送するメールテキスト化方式

②インターネット接続系の端末から、ＬＧＷＡＮ接続系の端末へ画面を転送する方式

③インターネットに接続するためのアプリケーション環境を、インターネットに接続する度ごとに、ＬＧＷＡＮ接続系の端末内にＬＧＷＡＮ接続系と接続できないよう隔離した状態で構築し、接続終了時に、構築したアプリケーション環境を消去する方式

④危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

（２）ＬＧＷＡＮ接続系と接続されるクラウドサービス上での情報システムの扱い

ＬＧＷＡＮ接続系の情報システムをクラウドサービス上へ配置する場合は、その領域をＬＧＷＡＮ接続系として扱い、マイナンバー利用事務系とネットワークを分

離し、専用回線を用いて接続しなければならない。

４．３　インターネット接続系

（１）情報セキュリティ責任者は、インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及びＬＧＷＡＮへの不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

（２）情報セキュリティ責任者は、市区町村のインターネット接続口を集約する自治体情報セキュリティクラウドに参加するとともに、関係省庁や山形県等と連携しながら、情報セキュリティ対策を推進しなければならない。

４．４　その他ネットワーク系

（１）情報セキュリティ責任者及び個別システム管理者は、所管するその他ネットワーク系が外部との通信をする必要がある場合、通信経路の限定(ＭＡＣアドレス、ＩＰアドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。

５　物理的セキュリティ

５．１　サーバ等の管理

（１）機器の取付け

情報セキュリティ責任者及び個別システム管理者は、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固定する等、必要な措置を講じなければならない。

（２）機器の電源

①情報セキュリティ責任者及び個別システム管理者は、施設管理部門と連携し、所管する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、当該機器が適正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及び個別システム管理者は、施設管理部門と連携し、落雷等による過電流に対して、所管する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。

（３）通信ケーブル等の配線

①情報セキュリティ責任者及び個別システム管理者は、電源ケーブル及び所管する主要な箇所の通信ケーブルについて、その損傷等を防止するために、施設管理部門と連携し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個別システム管理者は、電源ケーブル及び所管する主要な箇所の通信ケーブルについて、損傷等の報告があった場合、施設管理部門と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個別システム管理者は、自らまたは情報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以外の者が配線を変更、追加できないように必要な措置を講じなければならない。

（４）機器の定期保守及び修理

①情報セキュリティ責任者及び個別システム管理者は、可用性１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及び個別システム管理者は、電磁的記録媒体を内蔵する機器を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及び個別システム管理者は、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等を行わなければならない。

（５）庁外への機器の設置

情報セキュリティ管理者は、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。

（６）機器の廃棄等

①情報セキュリティ責任者及び個別システム管理者は、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。

②クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）をする者は、セキュリティを確保した対応となっているか、クラウドサービス事業者の方針及び手順について確認しなければならない。

なお、当該確認にあたっては、クラウドサービス事業者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用する必要がある。

５．２　管理区域（サーバ室等）の管理

（１）管理区域の構造等

①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、当該機器等の管理並びに運用を行うための部屋（以下「サーバ室等」という。）や電磁的記録媒体の保管庫をいう。

②情報セキュリティ責任者及び個別システム管理者は、施設管理部門と連携して、

管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

③情報セキュリティ責任者及び個別システム管理者は、サーバ室等内の機器等に、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。

④情報セキュリティ責任者及び個別システム管理者は、施設管理部門と協議の上、管理区域に配置する消火薬剤や消防用設備等が機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

（２）管理区域の入退室管理等

①情報セキュリティ責任者及び個別システム管理者は、管理区域への入退室について、許可された者のみに制限し、ＩＣカード、指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行わなければならない。

②入退室を許可された職員等及び委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、管理区域の責任者の求めにより提示しなければならない。

③情報セキュリティ責任者及び個別システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限したうえで、管理区域への入退室を許可された職員等が付き添わせるとともに、外見上職員等と区別できる措置を講じなければならない。

④情報セキュリティ責任者及び個別システム管理者は、機密性１または機密性２の情報資産を扱う情報システムを設置している管理区域について、当該情報システムに関連しない、または個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体、飲食物等を、原則持ち込ませないようにしなければならない。当該端末等を持ち込む必要がある場合は、持ち込み状況を確認する措置を講じなければならない。

（３）機器等の搬入出

①情報セキュリティ責任者及び個別システム管理者は、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、あらかじめ職員等または委託事業者に確認を行わせなければならない。

②情報セキュリティ責任者及び個別システム管理者は、サーバ室等における機器等の搬入出について、職員を立ち会わせなければならない。

５．３　通信回線及び通信回線装置の管理

①情報セキュリティ責任者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適正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正に保管しなければならない。

②情報セキュリティ責任者は、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。

③情報セキュリティ責任者は、行政系のネットワークを総合行政ネットワーク（ＬＧＷＡＮ）に集約するように努めなければならない。

④情報セキュリティ責任者は、機密性１または機密性２の情報資産を取り扱う情報システムに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、適正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。

⑤情報セキュリティ責任者は、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情報セキュリティ対策を実施しなければならない。

⑥情報セキュリティ責任者は、可用性１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、回線を冗長構成にする等の措置を講じなければならない。

５．４　職員等の利用する端末や電磁的記録媒体等の管理

①情報セキュリティ責任者及び個別システム管理者は、盗難防止のため、執務室等で利用する端末のワイヤーによる固定、使用時以外の施錠保管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。

②情報セキュリティ責任者及び個別システム管理者は、情報システムへのログインに際し、パスワード、スマートカードあるいは生体認証等の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。

③情報セキュリティ責任者及び個別システム管理者は、マイナンバー利用事務系では「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証等）を行うよう設定しなければならない。

６　人的セキュリティ

６．１　職員等の遵守事項

（１）職員等の遵守事項

①情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び実施手順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管理者に相談し、指示を仰がなければならない。

②業務以外の目的での使用の禁止

職員等は、業務以外の目的で資産情報の外部への持ち出し、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。

③モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

（ア）統括情報セキュリティ責任者は、機密性１または機密性２、可用性１、完全性１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

（イ）職員等は、本市のモバイル端末、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。

（ウ）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。

④支給以外の端末及び電磁的記録媒体等の業務利用

（ア）職員等は、支給以外の端末及び電磁的記録媒体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、情報セキュリティ責任者の許可を得て利用することができる。

（イ）職員等は、支給以外の端末及び電磁的記録媒体を用いる場合には、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の安全管理措置に関する規定を遵守しなければならない。

⑤持ち出し及び持ち込みの記録

情報セキュリティ管理者は、端末の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

⑥端末におけるセキュリティ設定変更の禁止

職員等は、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責任者の許可なく変更してはならない。

⑦机上の端末等の管理

職員等は、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または情報セキュリティ管理者の許可なく情報を閲覧されることがないよう、離席時の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、適正な措置を講じなければならない。

⑧退職時等の遵守事項

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。

⑨クラウドサービス利用時等の遵守事項

職員等は、クラウドサービスの利用にあたっても情報セキュリティポリシー、対策基準を遵守し、クラウドサービスの利用に関する自らの役割及び責任を意識しなければならない。

（２）再任用職員、会計年度任用職員及び臨時職員への対応

①情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、再任用職員、会計年度任用職員及び臨時職員に対し、採用時に情報セキュリティポリシー等のうち、再任用職員、会計年度任用職員及び臨時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情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理者は、再任用職員、会計年度任用職員及び臨時職員が情報資産を取り扱う際、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インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、再任用職員、会計年度任用職員及び臨時職員に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。

（３）情報セキュリティポリシー等の掲示

情報セキュリティ責任者及び個別システム管理者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

（４）委託事業者に対する説明

情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守・運用等を事業者に発注する場合、委託事業者が第三者に実施させる（以下「再委託」という。）場合も含めて、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。

６．２　研修・訓練

（１）情報セキュリティに関する研修・訓練

①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・訓練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、定期的にクラウドサービスを利用する職員等及び委託先を含む関係者の情報セキュリティに関する意識向上、教育及び訓練を実施しなければならない。

（２）研修計画の策定及び実施

①情報セキュリティ責任者は、職員等に対する情報セキュリティに関する研修計画を策定し、またその実施体制を構築するとともに定期的に見直さなければならない。

②情報セキュリティ責任者は、新規採用の職員等を対象とする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。

③情報セキュリティ責任者は、それぞれの役割、情報セキュリティに関する理解度等に応じた研修を実施しなければならない。

（３）緊急時対応訓練

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。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

（４）研修・訓練への参加

職員等は定められた研修・訓練に参加しなければならない。

６．３　情報セキュリティインシデントの報告

（１）庁内からの情報セキュリティインシデントの報告

①職員等は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

②報告を受けた情報セキュリティ管理者は、速やかに情報セキュリティ責任者に報告しなければならない。

③情報セキュリティ責任者は、報告のあった情報セキュリティインシデントについて、必要に応じてＣＩＳＯ、副ＣＩＳＯ及び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情報セキュリティ責任者は、クラウドサービス利用における情報セキュリティインシデントの報告について連絡体制の対象者に報告しなければならない。

（２）住民等外部からの情報セキュリティインシデントの報告

①職員等は、本市が管理するネットワーク及び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、住民等外部からの通報を受けた場合、情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

②報告を受けた情報セキュリティ管理者は、速やかに情報セキュリティ責任者に報告しなければならない。

③情報セキュリティ責任者は、当該情報セキュリティインシデントについて、必要に応じてＣＩＳＯ、副ＣＩＳＯ及び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情報セキュリティ責任者 は、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、住民等外部から報告を受けるための窓口を設置し、

当該窓口への連絡手段を公表しなければならない。

⑤統括情報セキュリティ責任者は、クラウドサービス事業者が検知した情報セキュリティインシデントの報告や情報セキュリティインシデントの状況を追跡する仕組みの構築を契約等で取り決めなければならない。

（3）情報セキュリティインシデントの原因の究明・記録、再発防止等

①ＣＳＩＲＴ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。

②ＣＳＩＲＴは、情報資産への影響度が大きい情報セキュリティインシデントであると評価した場合、ＣＩＳＯ及び副ＣＩＳＯに速やかに報告しなければならない。

③ＣＳＩＲＴ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管理者に対し、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。

④ＣＳＩＲＴは、これらの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。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、ＣＩＳＯ及び副ＣＩＳＯに報告しなければならない。

⑤ＣＩＳＯは、ＣＳＩＲＴ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。

６．４　ＩＤ及びパスワード等の管理

（1）ＩＣカード等の取扱い

①職員等は、自己の管理するＩＣカード等に関し、次の事項を遵守しなければならない。

（ア）認証に用いるＩＣカード等を、職員等間で共有してはならない。

（イ）業務上必要のないときは、ＩＣカード等をカードリーダ若しくは端末のスロット等から抜いておかなければならない。

（ウ）ＩＣカード等を紛失した場合には、速やかに情報セキュリティ責任者または個別システム管理者に通報し、指示に従わなければならない。

②情報セキュリティ責任者及び個別システム管理者は、ＩＣカード等の紛失等の通報があり次第、当該ＩＣカード等を使用したアクセス等を速やかに停止しなければならない。

③情報セキュリティ責任者及び個別システム管理者は、ＩＣカード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

（２）ＩＤの取扱い

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。

（３）パスワードの取扱い

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パスワードを秘密にし、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または個別システム管理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、情報システム間で同一のパスワードを用いてはならない。

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端末、サーバにパスワードを記憶させてはならない。

⑧職員等間でパスワードを共有してはならない（ただし、共有IDのパスワード、ファイルサーバ接続パスワード等を除く）。

７　技術的セキュリティ

７．１　コンピュータ及びネットワークの管理

（１）ファイルサーバの設定等

①情報セキュリティ責任者及び個別システム管理者は、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情報セキュリティ責任者は、ファイルサーバを課等の単位で構成し、職員等が他課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情報セキュリティ責任者及び個別システム管理者は、特定の職員等しか取扱えないデータについては、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。

（２）バックアップの実施

①情報セキュリティ責任者及び個別システム管理者は、業務システムのデータベースや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。

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、クラウドサービス事業者のバックアップ機能を利用する場合、クラウドサービス事業者にバックアップ機能の仕様を要求し、その仕様を確認しなければならない。また、その仕様がバックアップに関する本市が求める要求事項を満たすことを確認しなければならない。クラウドサービス事業者からバックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行わなければならない。

（３）他団体との情報システムに関する情報等の交換

個別システム管理者は、情報システムに関する情報及びソフトウェアを他の団体と交換する場合または他の団体に利用させる場合は、その取扱いに関する事項をあらかじめ定め、情報セキュリティ責任者の許可を得なければならない。

（４）情報システム管理記録及び作業の確認

①情報セキュリティ責任者及び個別システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

②情報セキュリティ責任者及び個別システム管理者は、所管する情報システムにおいて、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、改ざん等されないように適正に管理しなければならない。

③情報セキュリティ責任者、個別システム管理者または情報システム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名以上で作業し、互いにその作業を確認しなければならない。

（５）情報システム仕様書等の管理

情報セキュリティ責任者及び個別システム管理者は、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、適正に管理しなければならない。

（６）ログの取得等

①情報セキュリティ責任者及び個別システム管理者は、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個別システム管理者は、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、適正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個別システム管理者は、取得したログを定期的に点検また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または分析を実施しなければならない。なお、クラウドサービス事業者が収集し、保存する記録（ログ等）に関する保護（改ざんの防止等）の対応について、ログ管理等に関する対策や機能に関する情報を確認し、記録（ログ等）に関する保護が実施されているのか確認しなければならない。

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、監査及びデジタルフォレンジックに必要となるクラウドサービス事業者の環境内で生成されるログ等の情報（デジタル証拠）について、クラウドサービス事業者から提供されるログ等の監視機能を利用して取得することで十分では無い場合は、クラウドサービス事業者に提出を要求するための手続を明確にしなければならない。

（７）障害記録

情報セキュリティ責任者及び個別システム管理者は、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または問題等を、障害記録として記録し、適正に保存しなければならない。

（８）ネットワークの接続制御、経路制御等

①情報セキュリティ責任者は、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情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

（９）外部の者が利用できる情報システムの分離等

情報セキュリティ責任者及び個別システム管理者は、電子申請の汎用受付システム等、外部の者が利用できる情報システムについて、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。

（１０）外部ネットワークとの接続制限等

①情報セキュリティ責任者及び個別システム管理者は、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、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。

②情報セキュリティ責任者及び個別システム管理者は、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、庁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及び個別システム管理者は、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、改ざんまた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情報セキュリティ責任者及び個別システム管理者は、ウェブサーバ等をインターネットに公開する場合、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しなければならない。

⑤情報セキュリティ責任者及び個別システム管理者は、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、統括情報セキュリティ責任者の判断に従い、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。

（１１）複合機のセキュリティ管理

①情報セキュリティ責任者及び複合機を調達、運用する課等の情報セキュリティ管理者は、複合機の調達に際し、当該複合機が備える機能、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、適正なセキュリティ要件を策定しなければならない。

②情報セキュリティ責任者及び複合機を調達、運用する課等の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正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情報セキュリティ責任者及び複合機を運用する課等の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すべての情報を抹消また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。

（１２）ＩｏＴ機器を含む特定用途機器のセキュリティ管理

情報セキュリティ責任者及び特定用途の機器を調達、運用する課等の情報セキュリティ管理者は、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。

（１３）無線ＬＡＮ及びネットワークの盗聴対策

①情報セキュリティ責任者は、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情報セキュリティ責任者は、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。

（１４）電子メールのセキュリティ管理

①情報セキュリティ責任者は、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情報セキュリティ責任者は、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情報セキュリティ責任者は、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情報セキュリティ責任者は、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情報セキュリティ責任者は、システム開発や運用、保守等のため庁舎内に常駐してい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。

（１５）電子メールの利用制限

①職員等は、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、情報セキュリティ管理者に報告しなければならない。報告を受けた情報セキュリティ管理者は、速やかに情報セキュリティ責任者に報告しなければならない。

（１６）電子署名・暗号化

①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または完全性を確保することが必要な場合には、情報セキュリティ責任者が定めた電子署名、パスワード等による暗号化等、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責任者が定める以外の方法を用いてはならない。また、情報セキュリティ責任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情報セキュリティ責任者は、電子署名の正当性を検証するための情報または手段を、署名検証者へ安全に提供しなければならない。

（１７）無許可ソフトウェアの導入等の禁止

①職員等は、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、情報セキュリティ責任者または個別システム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、情報セキュリティ管理者または個別システム管理者は、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。

（１８）機器構成の変更の制限

①職員等は、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、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または個別システム管理者の許可を得なければならない。

（１９）業務外ネットワークへの接続の禁止

①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責任者または個別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情報セキュリティ責任者及び個別システム管理者は、支給した端末について、端末に搭載されたオペレーティングシステム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しなければならない。

（２０）業務以外の目的でのウェブ閲覧の禁止

①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正な措置を求めなければならない。

（２１）Ｗｅｂ会議サービスの利用時の対策

①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しなければならない。
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じなければならない。
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。

（２２）ソーシャルメディアサービスの利用

①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。
（ア）本市のアカウントによる情報発信が、実際の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。

（イ）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）等を適正に管理する等の方法で、不正アクセス対策を実施すること。

②職員等は、機密性１及び機密性２の情報をソーシャルメディアサービスで発信してはならない。

③ソーシャルメディアサービスを利用する課等の情報セキュリティ管理者は、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ソーシャルメディアサービスを利用する課等の情報セキュリティ管理者は、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ソーシャルメディアサービスを利用する課等の情報セキュリティ管理者は、可用性１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。

７．２　アクセス制御

（１）アクセス制御等

①アクセス制御

情報セキュリティ責任者または個別システム管理者は、所管するネットワークまた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。

②利用者ＩＤの取扱い

（ア）情報セキュリティ責任者及び個別システム管理者は、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。

（イ）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または個別システム管理者に通知しなければならない。

（ウ）情報セキュリティ責任者及び個別システム管理者は、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。

③特権を付与されたＩＤの管理等

（ア）情報セキュリティ責任者または個別システム管理者は、所管する情報システムの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。

（イ）情報セキュリティ責任者または個別システム管理者は、その特権を代行す

る者を、あらかじめ指名しなければならない。

（ウ）情報セキュリティ責任者及び個別システム管理者は、特権を付与されたＩＤ及びパスワードの変更について、委託事業者に行わせてはならない。

（エ）情報セキュリティ責任者及び個別システム管理者は、特権を付与されたＩＤ及びパスワードについて、職員等の端末等よりも長いパスワードの設定、入力回数制限等によって、セキュリティ機能を強化しなければならない。

（オ）情報セキュリティ責任者及び個別システム管理者は、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。

（２）職員等による外部からのアクセス等の制限

①職員等が外部から内部のネットワークまたは情報システムにアクセスする場合は、情報セキュリティ責任者及び個別システム管理者の許可を得なければならない。ただし、情報セキュリティ責任者が指定する方法によりアクセスする場合は許可を不要とする。

②情報セキュリティ責任者は、内部のネットワークまた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情報セキュリティ責任者は、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情報セキュリティ責任者は、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措置を講じなければならない。

⑤情報セキュリティ責任者は、外部からのアクセスに利用する端末等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、持ち込んだまたは外部から持ち帰った端末等を庁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、情報セキュリティ責任者の許可を得るか、もしく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情報セキュリティ責任者は、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。ただし、止むを得ず接続を許可する場合は、利用者のＩＤ及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（ＩＣカード等）による認証に加えて通信内容の暗号化等、情報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。

（３）ログイン時の表示等

情報セキュリティ責任者及び個別システム管理者は、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情報システムを設定しなければならない。

（４）認証情報の管理

①情報セキュリティ責任者または個別システム管理者は、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または個別システム管理者は、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または個別システム管理者は、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。

（５）特権による接続時間の制限

情報セキュリティ責任者及び個別システム管理者は、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。

７．３　情報システム開発、導入、保守等

（１）情報システムの調達

①情報セキュリティ責任者及び個別システム管理者は、情報システム開発、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情報セキュリティ責任者及び個別システム管理者は、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。

（２）情報システムの開発

①情報システム開発における責任者及び作業者の特定

情報セキュリティ責任者及び個別システム管理者は、情報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、情報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情報システム開発における責任者、作業者のＩＤの管理

（ア）情報セキュリティ責任者及び個別システム管理者は、情報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）情報セキュリティ責任者及び個別システム管理者は、情報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らない。

③情報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）情報セキュリティ責任者及び個別システム管理者は、情報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）情報セキュリティ責任者及び個別システム管理者は、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情報システムから削除しなければならない。

（３）情報システムの導入

①開発環境と運用環境の分離及び移行手順の明確化

（ア）情報セキュリティ責任者及び個別システム管理者は、情報システム開発・保守及びテスト環境から情報システム運用環境への移行について、情報システム開発・保守計画の策定時に手順を明確にしなければならない。

（イ）情報セキュリティ責任者及び個別システム管理者は、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。

（ウ）情報セキュリティ責任者及び個別システム管理者は、導入する情報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）情報セキュリティ責任者及び個別システム管理者は、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）情報セキュリティ責任者及び個別システム管理者は、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）情報セキュリティ責任者及び個別システム管理者は、個人情報及び機密性の高い本番環境のデータを、テストデータに使用してはならない。

（エ）情報セキュリティ責任者及び個別システム管理者は、開発した情報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せなければならない。

（４）情報システム開発・保守に関連する資料等の整備・保管

①情報セキュリティ責任者及び個別システム管理者は、情報システム開発・保守に関連する資料及び情報システム関連文書を適正に整備・保管しなければならない。

②情報セキュリティ責任者及び個別システム管理者は、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及び個別システム管理者は、情報システムに係るソース

コードを適正な方法で保管しなければならない。

（５）情報システムにおける入出力データの正確性の確保

①情報セキュリティ責任者及び個別システム管理者は、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及び個別システム管理者は、故意または過失により情報が改ざんされるまたは漏えいする恐れがある場合に、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及び個別システム管理者は、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、出力されるよう情報システムを設計しなければならない。

（６）情報システムの変更管理

情報セキュリティ責任者及び個別システム管理者は、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。

（７）開発・保守用のソフトウェア更新等

情報セキュリティ責任者及び個別システム管理者は、開発・保守用のソフトウェア等を更新または修正プログラムの適用をする場合、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。

（８）情報システム更新または統合時の検証等

情報セキュリティ責任者及び個別システム管理者は、情報システム更新・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。

７．４　不正プログラム対策

（１）情報セキュリティ責任者の措置事項

情報セキュリティ責任者は、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、インターネットとの境界においてコンピュータウイルス等の不正プログラムの検査を行い、不正プログラムの庁内ネットワーク及び情報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、インターネットとの境界においてコンピュータウイルス等不正プログラムの検査を行い、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所管するサーバ及び端末に、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及びそ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等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等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。

⑦仮想マシンを設定する際に不正プログラムへの対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策及びログ取得等の実施）を確実に実施しなければならない。ＳａａＳ型を利用する場合は、これらの対応が、クラウドサービス事業者側でされているのか、サービスを利用する前に確認しなければならない。また、サービスを利用している状況下では、これらのセキュリティ対策が適切にされているのか定期的にクラウドサービス事業者に報告を求めなければならない。

（２）個別システム管理者の措置事項

個別システム管理者は、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個別システム管理者は、その所管するサーバ及び端末に、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及びそ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インターネットに接続していない情報システムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の不正プログラムの感染を防止するために、本市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そのパターンファイルを更新しなければならない。

④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、個別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。

（３）職員等の遵守事項

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端末に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データまたはソフトウェアを外部から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検査を行わなければならない。

③差出人が不明な、また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全体検査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検査しなければならない。インターネット接続系で受診したインターネットメールまたはインターネット経由で入手したファイルをＬＧＷＡＮ接続系に取り込む場合は無害化しなければならない。

⑥情報セキュリティ責任者が提供するコンピュータウイルス等の不正プログラムに関する情報を、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また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。初動対応時の手順が定められていない場合は、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ケーブルの取り外しや、通信を行わない設定への変更などを実施しなければならない。

（４）専門家の支援体制

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。

７．５　不正アクセス対策

（１）情報セキュリティ責任者の措置事項

情報セキュリティ責任者は、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、機能を削除また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、情報セキュリティ責任者及び個別システム管理者へ通報するよう、設定しなければならない。

④重要な情報システムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。

⑤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等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。

⑥本市が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）におけるアクセス制御に関する事項が、クラウドサービスにおいて実現できるのか又はクラウドサービス事業者の提供機能等により実現できるのか、利用前にクラウドサービス事業者に確認しなければならない。

⑦クラウドサービスを利用する際に、委託事業者等に管理権限を与える場合、多要素認証を用いて認証させ、クラウドサービスにアクセスさせなければならない。

⑧パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等が、本市が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たすことを確認しなければならない。

（２）攻撃への対処

統括情報セキュリティ責任者及び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または攻撃を受けるリスクがある場合は、情報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、総務省、山形県等と連絡を密にして情報の収集に努めなければならない。

（３）記録の保存

統括情報セキュリティ責任者及び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。

（４）内部からの攻撃

情報セキュリティ責任者及び個別システム管理者は、職員等及び委託事業者が使用している端末からの庁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。

（５）職員等による不正アクセス

情報セキュリティ責任者及び個別システム管理者は、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管理者に通知し、適正な処置を求めなければならない。

（６）サービス不能攻撃

情報セキュリティ責任者及び個別システム管理者は、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。

（7）標的型攻撃

情報セキュリティ責任者及び個別システム管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、研修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。

7．6　セキュリティ情報の収集

（1）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

①情報セキュリティ責任者及び個別システム管理者は、ソフトウェアの情報セキュリティ上の欠陥（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。

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、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、本市の業務に対する影響や保有するデータへの影響について特定する。そして、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者に確認しなければならない。

（2）不正プログラム等のセキュリティ情報の収集・周知

情報セキュリティ責任者は、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。

（3）情報セキュリティに関する情報の収集及び共有

情報セキュリティ責任者及び個別システム管理者は、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。

8　運用

8．1　情報システムの監視

①情報セキュリティ責任者及び個別システム管理者は、情報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。

②情報セキュリティ責任者及び個別システム管理者は、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。また、利用するクラウドサービスで使用する時刻の同期についても適切になされているのか確認しなければならない

③情報セキュリティ責任者及び個別システム管理者は、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。

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、必要となるリソースの容量・能力が確保できるクラウドサービス事業者を選定しなければならない。また、利用するクラウドサービスの使用において必要な監視機能を確認するとともに監視により、業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めなければならない。

⑤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、イベントログ取得に関するポリシーを定め、利用するクラウドサービスがその内容を満たすことを確認し、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討しなければならない。

⑥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、クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、確認しなければならない。

（ア）サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除

（イ）クラウドサービス利用の終了手順

（ウ）バックアップ及び復旧

８．２　情報セキュリティポリシーの遵守状況の確認

（１）遵守状況の確認及び対処

①情報セキュリティ責任者及び個別システム管理者は、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、適正かつ速やかに対処しなければならない。

③情報セキュリティ責任者及び個別システム管理者は、ネットワーク及びサーバ等の情報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正かつ速やかに対処しなければならない。

（２）端末及び電磁的記録媒体等の利用状況調査

情報セキュリティ責任者及び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。

（３）職員等の報告義務

①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責任者が判断した場合、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。

８．３　侵害時の対応等

（１）緊急時対応計画の策定

①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、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また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正に実施するために、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正に対処しなければならない。

②統括情報セキュリティ責任者は、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてクラウドサービスの障害時を想定した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正に対処しなければならない。

（２）緊急時対応計画に盛り込むべき内容

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

（３）業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、電子情報処理推進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。

（４）緊急時対応計画の見直し

統括情報セキュリティ責任者は、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。

８．４　例外措置

（１）例外措置の許可

情報セキュリティ管理者及び個別システム管理者は、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しまた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、統括情報セキュリティ責任者の許可を得て、例外措置を講じることができる。

（２）緊急時の例外措置

情報セキュリティ管理者及び個別システム管理者は、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。

（３）例外措置の申請書の管理

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正に保管し、定期的に申請状況を確認しなければならない。

８．５　法令遵守

（１）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26年法律第104号）
⑦山形市個人情報の保護に関する法律施行条例（令和４年条例第24号）

（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、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS 等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反を引き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従わなければならない。

８．６　懲戒処分等

（１）懲戒処分

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。

（２）違反時の対応

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情報セキュリティ責任者が違反を確認した場合は、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管理者に通知し、適正な措置を求めなければならない。

②個別システム管理者等が違反を確認した場合は、速やかに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管理者に通知し、適正な措置を求めなければならない。

③情報セキュリティ管理者の指導によっても改善されない場合、情報セキュリティ責任者は、当該職員等のネットワークまた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、情報セキュリティ責任者は、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管理者に通知しなければならない。

９　業務委託と外部サービスの利用

９．１　業務委託

（１）委託事業者の選定基準

情報セキュリティ管理者は、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）契約項目

情報システムの運用、保守等を業務委託する場合には、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。

・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
・委託事業者の責任者、委託内容、作業者、作業場所の特定
・提供されるサービスレベルの保証
・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の実施
・委託事業者の従業員に対する教育の実施
・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
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務

・市による監査、検査
・市による情報セキュリティインシデント発生時の公表
・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）

（３）確認・措置等

情報セキュリティ管理者は、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、（２）の契約に基づき措置しなければならない。また、その重要度に応じて情報セキュリティ責任者に報告しなければならない。

９．２　外部サービスの利用（機密性１または機密性２の情報を取り扱う場合）

（１）外部サービスの利用に係る規定の整備

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１または機密性２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（以下９．２節において「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
⑤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

（２）外部サービスの選定

①情報セキュリティ管理者は、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すること。
②情報セキュリティ管理者は、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すること。また、以下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ること。
③情報セキュリティ責任者は、以下の内容を含む情報セキュリティ対策に関する情報の提供を求め、その内容を確認し、利用する外部サービス（クラウドサービス）が、本市が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たしているか否かを評価すること。
（ア）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
（イ）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
（ウ）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

（エ）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

（オ）情報セキュリティインシデントへの対処方法

（カ）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

（キ）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

④情報セキュリティ管理者は、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ること。

⑤情報セキュリティ責任者は、クラウドサービス事業者と情報セキュリティに関する役割及び責任の分担について確認する。

⑥情報セキュリティ管理者は、必要に応じて以下の内容を外部サービス提供者の選定条件に含めること。

（ア）情報セキュリティ監査の受入れ

（イ）サービスレベルの保証

⑦情報セキュリティ管理者は、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ること。

⑧情報セキュリティ管理者は、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ること。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すること。

⑨情報セキュリティ管理者は、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ること。

⑩統括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すること。

（３）外部サービスの利用に係る調達・契約

①情報セキュリティ管理者は、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ること。
②情報セキュリティ管理者は、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こと。

（4）外部サービスの利用承認

①情報セキュリティ管理者は、外部サービスを利用する場合には、情報セキュリティ責任者に外部サービスの利用申請を行うこと。
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、利用の可否を決定すること。
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、承認済み外部サービスとして記録し、外部サービス管理者を指名すること。（クラウドサービスを利用する場合も同様の措置を行う。）

（5）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

①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、以下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すること。
（ア）不正なアクセスを防止するためのアクセス制御
（イ）取り扱う情報の機密性保護のための暗号化
（ウ）開発時におけるセキュリティ対策
（エ）設計・設定時の誤りの防止
（オ）クラウドサービスにおけるユーティリティプログラムに対するセキュリティ対策
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・記録すること。
③クラウドサービス管理者は、前各項において定める規定に対し、情報セキュリティに配慮した構築の手順及び実践がされているか、クラウドサービス事業者に情報を求め、実施状況を確認及び記録すること。

（6）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

①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、以下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すること。
（ア）外部サービス利用方針の規定
（イ）外部サービス利用に必要な教育

（ウ）取り扱う資産の管理
（エ）不正アクセスを防止するためのアクセス制御
（オ）取り扱う情報の機密性保護のための暗号化
（カ）外部サービス内の通信の制御
（キ）設計・設定時の誤りの防止
（ク）外部サービスを利用した情報システムの事業継続
（ケ）設計・設定変更時の情報や変更履歴の管理

②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、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すること。

③外部サービス管理者は、前各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・記録すること。

④クラウドサービス管理者は、情報セキュリティに配慮した運用・保守の手順及び実践がされているか、クラウドサービス事業者に情報を求め、実施状況を定期的に確認及び記録すること。

（7）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

①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、以下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すること。
（ア）外部サービスの利用終了時における対策
（イ）外部サービスで取り扱った情報の廃棄
（ウ）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・記録すること。

③クラウドサービス管理者は、クラウドサービス上で機密性の高い情報（住民情報等）を保存する場合は、機密性を維持するために暗号化するとともに、その情報資産を破棄する際は、データ消去の方法の一つとして暗号化した鍵（暗号鍵）を削除するなどにより、その情報資産を復元困難な状態としなければならない。

９．３　外部サービスの利用（機密性１または機密性２の情報を取り扱わない場合）

（1）外部サービスの利用に係る規定の整備

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１または機密性２の情報を取り扱わない場合）の利用に関する規定を整備しなければならない。
（ア）外部サービスを利用可能な業務の範囲
（イ）外部サービスの利用申請の許可権限者と利用手続
（ウ）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
（エ）外部サービスの利用の運用手順

（２）外部サービスの利用における対策の実施

①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１または機密性２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。

１０　評価・見直し

１０．１　監査

（１）実施方法

統括情報セキュリティ責任者を情報セキュリティ監査統括責任者とし、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について、毎年度及び必要に応じて監査を実施しなければならない。

（２）監査を行う者の要件

①情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

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でなければならない。

（３）監査実施計画の立案及び実施への協力

①情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、電子情報処理推進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。

（４）委託事業者に対する監査

①委託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統括責任者は、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または必要に応じて行わなければならない。

②クラウドサービスを利用している場合は、クラウドサービス事業者における情報セキュリティポリシーの遵守について、定期的に監査を行わなければならない。クラウドサービス事業者にその証拠（文書等）の提示を求める場合は、第三者の監査人が発行する証明書をこの証拠とすることもできる。

（５）報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、電子情報処理推進委員会に報告しなければならない。

（6）保管

情報セキュリティ監査統括責任者は、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正に保管しなければならない。

（7）監査結果への対応

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管理者に対し、当該事項への対処を指示しなければならない。また、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。なお、庁内で横断的に改善が必要な事項については、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。

（8）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

電子情報処理推進委員会は、監査結果を情報セキュリティポリシー及び関係規程、その他情報セキュリティ対策等の見直し時に活用しなければならない。

１０．２　自己点検

（1）実施方法

①情報セキュリティ責任者及び個別システム管理者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検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、情報セキュリティ管理者と連携して、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、毎年度または必要に応じて自己点検を行わなければならない。

（2）報告

個別システム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、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。統括情報セキュリティ責任者は報告結果を、必要に応じ電子情報処理推進委員会に報告しなければならない。

（3）自己点検の活用

①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電子情報処理推進委員会は、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、その他情報セキュリティ対策等の見直し時に活用しなければならない。

１０．３　情報セキュリティポリシー及び関係規定等の見直し

電子情報処理推進委員会は、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。

１１　用語解説

●「事業継続計画」
「事業継続計画」→「BCP」を参照。

●「情報セキュリティインシデント」
「情報セキュリティインシデント」とは、望まない単独若しくは一連の情報セキュリティ事象、または予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

●「ソーシャルメディアサービス」
「ソーシャルメディアサービス」とは、インターネット上で展開される情報メディアのあり方で、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通等といった社会的な要素を含んだメディアのことをいう。利用者の発信した情報や利用者間のつながりによってコンテンツを作り出す要素を持ったWeb サイトやネットサービス等を総称する用語で、電子掲示板(BBS)やブログ、動画共有サイト、動画配信サービス、ショッピングサイトの購入者評価欄等を含む。

●「端末」
「端末」とは、情報システムの構成要素である機器のうち、職員が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りが無い限り、地方公共団体が調達または開発するものをいう。

●「電子署名」
「電子署名」とは、情報の正当性を保証するための電子的な署名情報をいう。

●「特権ID」
「特権ID」とは、サーバの起動や停止、アプリケーションのインストールやシステム設定の変更、全データへのアクセス等、通常のID よりもシステムに対するより高いレベルでの操作が可能なID をいう。

●「パソコン」
「パソコン」とは、端末のうち、机の上等に備え置いて業務に使用することを前提とし、移動させて使用することを目的とはしていないものをいい、端末の形態は問わない。

●「標的型攻撃」

「標的型攻撃」とは、明確な意思と目的を持った人間が特定のターゲットや情報に対して特定の目的のために行うサイバー攻撃の一種をいう。

●「モバイル端末」

「モバイル端末」とは、端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

●「BCP（Business Continuity Plan：事業継続計画）」

「BCP」とは、組織において特定する事業の継続に支障をきたすと想定される自然災害、人的災害・事故、機器の障害等の事態に組織が適切に対応し目標とする事業継続性の確保を図るために当該組織において策定する、事態の予防及び事態発生後の事業の維持並びに復旧に係る計画をいう。