○矢板市情報セキュリティ対策基準

令和５年４月１日要綱

目次

第１章　総則

（趣旨）

第１条　この基準は、矢板市情報セキュリティ基本方針（令和５年４月１日制定。以下「基本方針」という。）第１０条の規定に基づき、本市のすべての情報資産、情報資産を活用するための設備及びこれらの情報資産に接する職員又は受託事業者が行う情報セキュリティ対策に関し必要な事項を定めるものとする。

（定義）

第２条　この基準に規定する用語の意義は、基本方針に規定する用語の例による。

第２章　組織体制

（最高情報セキュリティ責任者）

第３条　本市に最高情報セキュリティ責任者（Ｃｈｉｅｆ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｓｅｃｕｒｉｔｙ　Ｏｆｆｉｃｅｒ。以下「ＣＩＳＯ」という。）を置く。

２　ＣＩＳＯは、副市長をもって充てる。

３　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。

４　ＣＩＳＯは、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有する者を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。

（統括情報セキュリティ責任者）

第４条　総合政策部長を、ＣＩＳＯ直属の統括情報セキュリティ責任者とする。

２　統括情報セキュリティ責任者は、ＣＩＳＯを補佐するものとする。

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。

４　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。

５　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、情報システム管理者及び情報システム担当者に対して、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。

６　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の指示に従い、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行う権限及び責任を有する。

７　統括情報セキュリティ責任者は、情報セキュリティ等に係る緊急時等の円滑な情報共有を図るため、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、統括情報セキュリティ管理者、情報セキュリティ管理者、情報システム管理者及び情報システム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。

８　統括情報セキュリティ責任者は、情報セキュリティ等に係る緊急時には、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。

（情報セキュリティ責任者）

第５条　部長等の職にある者を、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、当該部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。

３　情報セキュリティ責任者は、その所管する部局等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

４　情報セキュリティ責任者は、その所管する部局等において所有している情報システムについて、情報セキュリティ等に係る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並びに職員等に対する教育、訓練、助言及び指示を行う。

（統括情報セキュリティ管理者）

第６条　総合政策課デジタル戦略推進室長を、統括情報セキュリティ管理者とする。

２　統括情報セキュリティ管理者は、統括情報セキュリティ責任者を補佐するものとする。

３　統括情報セキュリティ管理者は、統括情報セキュリティ責任者の指示により、本市の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及び管理を行う。

４　統括情報セキュリティ管理者は、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。

（情報セキュリティ管理者）

第７条　課長等の職にある者を、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、その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、その所掌する課等において、情報資産に対するセキュリティ侵害が発生した場合又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、統括情報セキュリティ管理者及びＣＩＳＯへ速やかに報告を行い、指示を受ければならない。

（情報セキュリティ担当者）

第８条　情報セキュリティ管理者を補佐するため、課等及びネットワークを使用している施設に情報セキュリティ担当者を置く。

２　情報セキュリティ担当者は、課等及びネットワークを使用している施設に所属する職員の中から当該課等の情報セキュリティ管理者が指名する職員をもって充てる。

３　情報セキュリティ担当者は、情報セキュリティ管理者の指示に従い、その所属する課等及び施設の情報セキュリティに関する対策の向上を図る。

（情報システム管理者）

第９条　情報システムを所管する担当課における課長等の職にある者を、情報システム管理者とする。

２　情報システム管理者は、所管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。

３　情報システム管理者は、所管する情報システム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　情報システム管理者は、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及び管

理を行う。

（情報システム担当者）

第１０条　情報システム管理者を補佐するため、情報システムを所管する担当課に情報システム担当者を置く。

２　情報システム担当者は、情報システム管理者の指示に従い、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。

３　情報システム管理者は、情報システム担当者を指定し、情報システム担当者報告書（別記様式第１号）により、統括情報セキュリティ責任者まで報告するものとする。

（情報セキュリティ委員会）

第１１条　情報セキュリティ対策を統一的に行うため、情報セキュリティ委員会を設置する。

（所掌事項）

第１２条　情報セキュリティ委員会は、次に掲げる事項について審議する。

⑴　情報セキュリティポリシーの評価及び見直しに関すること。

⑵　情報セキュリティポリシーの遵守状況に関すること。

⑶　情報セキュリティに関する教育及び研修に関すること。

⑷　情報セキュリティ監査に関すること。

⑸　前各号に掲げるもののほか全庁的な情報セキュリティ対策に必要な事項

（組織）

第１３条　情報セキュリティ委員会は、次に掲げる職にある者をもって組織する。

⑴　副市長

⑵　総合政策部長

⑶　総務部長

⑷　健康福祉部長

⑸　市民生活部長

⑹　経済建設部長

⑺　教育部長

⑻　選挙管理委員会事務局長

⑼　監査委員事務局長

⑽　上下水道事務所長

⑾　議会事務局長

⑿　総合政策課デジタル戦略推進室長

（委員長及び副委員長）

第１４条　委員会に、委員長及び副委員長各１人を置く。

２　委員長は副市長、副委員長には総合政策部長の職にある者をもって充てる。

３　委員長は、会務を総理し、委員会を代表する。

４　副委員長は、委員長を補佐し、委員長に事故があるとき又は委員長が欠けたときは、その職務を代理する。

（会議）

第１５条　委員会の会議（以下「会議」という。）は、必要に応じて委員長が招集し、会議の議長となる。

（庶務）

第１６条　委員会の庶務は、総合政策課デジタル戦略推進室において処理する。

（兼務の禁止）

第１７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、承認又は許可の申請を行う者とその承認者又は許可者は、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、やむを得ない場合を除き、同じ者が兼務してはならない。

（情報セキュリティに関する統一的な窓口の設置等）

第１８条　ＣＩＳＯは、情報セキュリティインシデント（情報セキュリティに関する障害、事故及び欠陥をいう。以下同じ。）の統一的な窓口の機能を有する組織（Ｃｏｍｐｕｔｅｒ　Ｓｅｃｕｒｉｔｙ　Ｉｎｃｉｄｅｎｔ　Ｒｅｓｐｏｎｓｅ　Ｔｅａｍ。情報セキュリティインシデントに対応するための即応対応するチームのこと。以下「ＣＳＩＲＴ」という。）を整備し、情報セキュリティインシデントについて部局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する。

２　ＣＩＳＯは、情報セキュリティ戦略の意思決定を行った際には、その内容を関係部局等に提供する。

３　ＣＩＳＯは、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、影響範囲等を勘案し、報道機関への通知及び公表の対応を行わなければならない。

４　ＣＩＳＯは、情報セキュリティに関して、関係機関及び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う。

第３章　情報資産の分類及び管理の方法並びにセキュリティ対策

第１節　情報資産の分類

第１９条　本市における情報資産は、別表のとおり分類を行い、その重要性を踏まえた管理を行わなければならない。

第２節　情報資産の管理

（管理責任）

第２０条　統括情報セキュリティ管理者又は情報セキュリティ管理者（以下「情報セキュリティ管理者等」という。）は、その所管する情報資産について管理責任を有する。

２　情報セキュリティ管理者等は、情報資産が複製され、又は伝送されたときには、当該複製され、又は伝送された情報資産について別表の分類に基づき管理しなければならない。

（情報資産の分類の表示）

第２１条　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、ヘッダー、フッター等をいう。）、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。

（情報の作成及び消去）

第２２条　職員等は、業務上必要のない情報を作成してはならない。

２　情報を作成する職員等は、当該情報が作成途上であっても別表の分類に基づき管理しなければならない。

３　前項の情報が不要になった場合は、速やかに当該情報を消去しなければならない。

４　情報の作成を依頼する職員等は、データ作成依頼書（別記様式第３号）により、当該情報を所管する情報システム管理者の承認を得るものとする。

５　庁外の者が情報の作成を依頼する場合は、データ利用許可願（別記様式第５号）を提出し、ＣＩＳＯの許可を得なければならない。この場合において、庁外の者が遵守すべき本データの取扱いについては、本情報セキュリティポリシーが職員等に求める取扱いに準じるものとする。

（情報資産の入手）

第２３条　自己以外の者が作成した情報資産を入手した職員等は、別表の分類に基づいた取り扱いをしなければならない。

２　職員等が他課所管のデータを使用する場合は、データ使用承認願（別記様式第７号）を提出し、当該データを所管する情報セキュリティ管理者等の許可を得なければならない。

（情報資産の利用）

第２４条　情報資産を利用する職員等は、業務以外の目的に情報資産を利用してはならない。

２　情報資産を利用する職員等は、別表に規定する情報資産の分類に応じ、同表第３欄に規定する取扱制限により適切な取扱いをしなければならない。

３　情報資産を利用する職員等は、電磁的記録媒体に別表の規定による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は、それらのうち最も高い同表の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

（情報資産の保管）

第２５条　情報セキュリティ管理者等又は情報システム管理者は、別表の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。

２　情報セキュリティ管理者等又は情報システム管理者は、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。

３　情報セキュリティ管理者等又は情報システム管理者は、別表の機密性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については、耐震、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。

（情報の送信）

第２６条　電子メール等により別表の機密性２以上の情報を送信する職員等は、情報セキュリティ管理者等の許可を得なければならない。この場合において、送信する情報には、必要に応じ暗号化及びパスワード設定を行わなければならない。

（情報資産の運搬）

第２７条　車両等により別表の機密性２以上の情報資産を運搬する職員等は、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。この場合において、車両等による運搬については、情報セキュリティ管理者等の許可を得なければならない。

（情報資産の提供及び公表）

第２８条　別表の機密性２以上の情報資産を外部に提供する職員等は、必要に応じ暗号化及びパスワードの設定を行わなければならない。この場合において、外部提供については、情報セキュリティ管理者等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等は、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。

（情報資産の廃棄）

第２９条　別表の機密性２以上の情報資産の廃棄やリース返却を行う職員等は、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。この場合において、廃棄やリース返却については、情報セキュリティ管理者等の許可を得なければならない。

２　情報資産の廃棄やリース返却を行う職員等は、当該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。

第４章　情報システム全体の強靭性の向上

（マイナンバー利用事務系）

第３０条　情報セキュリティ管理者等は、マイナンバー利用事務系と、他の領域と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、通信経路の限定及びアプリケーションプロトコルの限定を行わなければならない。

２　情報セキュリティ管理者等は、前項の規定により外部との通信をする場合は、インターネット環境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の接続先については、ＬＧＷＡＮ接続系を経由する場合において、この限りではない。

第３１条　情報セキュリティ管理者等は、マイナンバー利用事務系の情報システムにアクセスする認証手段のうち、二つ以上を併用する認証を利用しなければならない。

２　情報セキュリティ管理者等は、マイナンバー利用事務系が扱う情報については、原則として電磁的記録媒体による持ち出しができないよう設定しなければならない。

（ＬＧＷＡＮ接続系）

第３２条　情報セキュリティ管理者等は、ＬＧＷＡＮ接続系とインターネット接続系と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、次の各号に定める方法等により、無害化通信を図らなければならない。

⑴　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

⑵　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

⑶　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

（インターネット接続系）

第３３条　情報セキュリティ管理者等は、インターネット接続系については、通信パケットの監視

や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　情報セキュリティ管理者等は、栃木県及び栃木県内市町のインターネット通信を集約する栃木県自治体情報セキュリティクラウドに参加するとともに、関係省庁や栃木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。

第５章　物理的セキュリティ対策

第１節　サーバ等の管理

（機器の取付け）

第３４条　情報システム管理者は、サーバ等の機器の取付けを行う場合は、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。

（サーバの冗長化）

第３５条　情報システム管理者は、所管するサーバに格納している情報の重要性、可用性、停止することによる業務への影響度等を勘案し、必要に応じて冗長化（代替用の設備を用意し、情報システム等に故障、障害等が発生した場合にサービスを継続的に提供できるようにすることをいう。）を施し、サービスや業務を停止させないよう努めなければならない。

（機器の電源）

第３６条　情報システム管理者は、統括情報セキュリティ管理者及び各施設の管理所管課と連携し、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　情報システム管理者は、統括情報セキュリティ管理者及び各施設の管理所管課と連携し、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。

（配線）

第３７条　統括情報セキュリティ管理者及び情報システム管理者は、各施設の管理所管課と連携し、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、必要な措置を講じなければならない。

２　統括情報セキュリティ管理者及び情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、各施設の管理所管課から損傷等の報告があった場合は、連携して対応しなければならない。

３　統括情報セキュリティ管理者及び情報システム管理者は、ネットワーク接続口（ハブのポート

等をいう。）を他者が容易に接続できない場所に設置する等適切に管理しなければならない。

４　統括情報セキュリティ管理者及び情報システム管理者は、自ら又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又は追加をできないように必要な措置を施さなければならない。

（機器の定期保守及び修理）

第３８条　情報システム管理者は、別表の可用性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　情報システム管理者は、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は、保存された内容を消去した状態で行わせなければならない。この場合において、当該内容を消去できないときは、情報システム管理者は、外部の事業者に修理させるに当たり、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その他必要な措置を行わなければならない。

（庁外への機器の設置）

第３９条　統括情報セキュリティ管理者及び情報システム管理者は、庁外にサーバ等の機器を設置する場合は、ＣＩＳＯの承認を得なければならない。この場合において、統括情報セキュリティ管理者及び情報システム管理者は、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４０条　情報システム管理者は、機器を廃棄又はリース返却等をする場合は、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しなければならない。

第２節　管理区域、情報通信回線及び職員等のパソコンの管理

（管理区域の構造等）

第４１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及び電磁的記録媒体の保管庫をいう。

２　統括情報セキュリティ管理者は、管理区域を地階又は１階に設けてはならない。また、可能な限り外部からの侵入が容易にできないようにしなければならない。

３　統括情報セキュリティ管理者は、各施設の管理所管課と連携して、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者の立入りを防止しなければならない。

４　統括情報セキュリティ管理者は、管理区域内の機器等に、転倒、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　統括情報セキュリティ管理者は、各施設の管理所管課と連携して、管理区域を囲む外壁等の床下開口部を全て塞がなければならない。

6　統括情報セキュリティ管理者は、管理区域に配置する消火薬剤、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。

（管理区域の入退室管理等）

第４２条　統括情報セキュリティ管理者は、管理区域内のサーバを設置する場所への入退室を許可された者のみに制限し、特に委託事業者の入退出については、その日時等についてＩＣカード、指紋認証等の生体認証又は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　職員等及び委託事業者は、管理区域に入る場合は、身分証明書等を携帯し、統括情報セキュリティ管理者の求めに応じ提示しなければならない。

3　統括情報セキュリティ管理者は、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上で、管理区域への入退室を許可された職員等が付き添うものとし、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　統括情報セキュリティ管理者は、別表の機密性２以上の情報資産を扱うシステムを設置している管理区域においては、当該情報システムに関連しないコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

（機器等の搬入出）

第４３条　統括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、あらかじめ職員又は委託事業者に確認を行わせなければならない。

2　統括情報セキュリティ管理者は、管理区域の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。

（通信回線及び通信回線装置の管理）

第４４条　統括情報セキュリティ管理者は、庁内の通信回線及び通信回線装置（通信回線及び通信回線装置に関連する文書を含む。）を、各施設の管理所管課と連携し、適切に管理しなければならない。

2　統括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。

3　統括情報セキュリティ管理者は、行政系のネットワークをＬＧＷＡＮに集約するように努めなければならない。

４　統括情報セキュリティ管理者は、別表の機密性２以上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は、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。この場合において、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　統括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。

６　統括情報セキュリティ管理者は、別表の可用性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。この場合において、必要に応じ、回線を冗長構成（設備や装置を複数用意し、一部が故障しても運用を継続できるようにする構成をいう。）にする等の措置を講じなければならない。

（職員等のパソコン等の管理）

第４５条　情報システム管理者は、盗難防止のため、執務室等で利用するパソコン等にあっては、必要に応じてワイヤーによる固定、施錠管理等の物理的措置を講じ、電磁的記録媒体にあっ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　情報システム管理者は、情報システムの使用に当たっては、ログインパスワードの入力その他の認証を必要とするように設定しなければならない。

３　情報システム管理者は、マイナンバー利用事務系においては、二つ以上を併用する認証手段を行うよう設定しなければならない。

第６章　人的セキュリティ対策

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４６条　職員等は、情報セキュリティポリシー及び別に定める実施手順を遵守し、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等に相談し、指示を受けなければならない。

（情報セキュリティポリシー等の掲示）

第４７条　情報セキュリティ管理者等は、職員等が常に情報セキュリティポリシー及び別に定める実施手順を閲覧できるように掲示しなければならない。

（業務以外の目的での使用の禁止）

第４８条　職員等は、業務以外の目的で情報資産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。

（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）

第４９条　ＣＩＳＯは、別表の機密性２以上、可用性２及び完全性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、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は、情報セキュリティ管理者等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は、情報セキュリティ管理者等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５０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（以下「端末等」という。）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、支給以外の端末等の業務利用の可否判断をＣＩＳＯが行った後に、統括情報セキュリティ責任者の定める実施手順に従い、情報セキュリティ管理者等の許可を得て使用することができる。

２　職員等は、支給以外の端末等を用いる場合は、外部で処理する場合における安全管理措置を遵守しなければならない。

（持ち出し及び持込みの記録）

第５１条　情報セキュリティ管理者等は、端末等の持ち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。

（パソコン及びモバイル端末におけるセキュリティ設定変更の禁止）

第５２条　職員等は、パソコン及びモバイル端末のソフトウェアに係るセキュリティ機能の設定を情報セキュリティ管理者等の許可なく変更してはならない。

（机上の端末等の管理）

第５３条　職員等は、端末等及び個人情報等が印刷された文書等について、第三者に使用され、又は情報セキュリティ管理者等の許可なく情報を閲覧されることがないよう、離席時のパソコン、モバイル端末等のロック、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５４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、その職を離れた後も業務上知り得た情報を他に漏らしてはならない。

第２節　非常勤職員等及び委託事業者への対応

（情報セキュリティポリシー等の遵守）

第５５条　情報セキュリティ管理者等は、非常勤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、非常勤職員及び臨時職員が守るべき内容を理解させ、実施させ、及び遵守させなければならない。

（情報セキュリティポリシー等の遵守に対する同意）

第５６条　情報セキュリティ管理者等は、非常勤職員及び臨時職員の採用の際、必要に応じて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。

（インターネット接続及び電子メール使用等の制限）

第５７条　情報セキュリティ管理者等は、非常勤職員及び臨時職員にパソコン、モバイル端末等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、電子メールの使用等が不要の場合は、これを利用できないようにしなければならない。

（委託事業者に対する説明）

第５８条　情報セキュリティ管理者等は、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は、委託事業者（当該委託事業者から再委託を受ける事業者を含む。以下この条において同じ。）に対し、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について説明しなければならない。

第３節　研修及び訓練

（情報セキュリティに関する研修及び訓練）

第５９条　ＣＩＳＯは、職員等に対し定期的に情報セキュリティに関する研修及び訓練を実施しなければならない。

（研修計画の策定及び実施）

第６０条　ＣＩＳＯは、情報セキュリティ委員会の承認を得て、全ての職員等に対する情報セキュリティに関する研修計画の策定及びその実施体制の構築を定期的に行わなければならない。

２　前項の研修計画において、職員等は毎年度１回以上情報セキュリティに関する研修（以下「セキュリティ研修」という。）を受講できるようにし、新規採用の職員等については当該職員等を対象とするセキュリティ研修を実施しなければならない。

３　セキュリティ研修は、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等、情報セキュリティ担当者その他職員等に対して、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ものにしなければならない。

４　ＣＩＳＯは、毎年度１回、情報セキュリティ委員会に対して、セキュリティ研修の実施状況について報告しなければならない。

（緊急時対応訓練）

第６１条　ＣＩＳＯは、情報セキュリティ等に係る緊急時の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。この場合において、当該訓練に係る計画においては、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、効果的に実施できるようにしなければならない。

（研修及び訓練への参加）

第６２条　全ての職員等は、セキュリティ研修及び前条の訓練に参加しなければならない。

第４節　情報セキュリティインシデントの報告

（情報セキュリティインシデントの住民等からの報告窓口の設置）

第６３条　ＣＩＳＯ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。

（情報セキュリティインシデントの報告）

第６４条　職員等は、情報セキュリティインシデントについて認知した場合又は住民等から報告を受けた場合は、速やかに情報セキュリティ管理者及びＣＳＩＲＴに報告しなければならない。

２　情報セキュリティ管理者は、前項の報告を受けた場合は、速やかに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に報告しなければならない。

３　統括情報セキュリティ責任者は、前項の規定により報告のあった情報セキュリティインシデントについて、ＣＩＳＯ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の原因の究明、記録、再発防止等）

第６５条　ＣＳＩＲＴ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否かの評価を行わなければならない。

２　ＣＳＩＲＴは、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に速やかに報告しなければならない。

３　ＣＳＩＲＴ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。

４　ＣＳＩＲＴは、当該情報セキュリティインシデントの原因を究明し、記録を保存しなければならない。

５　ＣＳＩＲＴは、前項の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に報告しなければならない。

６　ＣＩＳＯは、前項の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５節　ＩＤ、パスワード等の管理

（ＩＣカード等の取扱い）

第６６条　職員等は、自己の管理するＩＣカード等に関し、次に掲げる事項を遵守しなければならない。

⑴　自己の認証に用いるＩＣカード等を職員等の間で共有しないこと。

⑵　業務上必要のないときは、ＩＣカード等をカードリーダ又はパソコン等の端末のスロット等から抜いておくこと。

⑶　ＩＣカード等を紛失した場合には、速やかに統括情報セキュリティ管理者及び情報システム管理者に報告し、その指示に従うこと。

第６７条　統括情報セキュリティ管理者及び情報システム管理者は、ＩＣカード等の紛失等の報告があった場合は、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。

２　統括情報セキュリティ管理者及び情報システム管理者は、ＩＣカード等を切り替える場合は、切替え前のＩＣカード等を回収し、破砕するなどの復元不可能な処理を行ったうえで廃棄しなければならない。

３　統括情報セキュリティ管理者及び情報システム管理者は、職員等の認証に用いるＩＣカード等について、ＩＣカード等の紛失等の報告があった場合は、その旨を必要に応じてＣＩＳＯに報告しなければならない。

（ＩＤの取扱い）

第６８条　職員等は、自己の管理するＩＤを厳重に管理し、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の利用を許可された者以外に利用させてはならない。

（パスワードの取扱い）

第６９条　職員等は、自己の管理するパスワードを厳重に管理し、次に掲げる事項を遵守しなければならない。

⑴　パスワードは、他者に知られないように管理すること。

⑵　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ないこと。

⑶　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すること。

⑷　パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更すること。

⑸　パスワードは、定期的に、又はアクセス回数に基づいて変更し、古いパスワードを再使用し

ないこと。

⑹　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ないこと。

⑺　仮のパスワードは、最初のログイン時点で変更すること。

⑻　パソコン等の端末にパスワードを記憶させないこと。

⑼　職員等の間でパスワードを共有しないこと。ただし、職員等が共用するＩＤに対するパスワードについてはその限りではない。

第７章　技術的セキュリティ対策

第１節　コンピュータ及びネットワークの管理

（文書サーバの設定等）

第７０条　統括情報システム管理者は、文書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の閲覧及び使用ができないように設定しなければならない。

２　統括情報システム管理者は、特定の職員等しか取扱えないデータについては、サーバ内に別の領域を作成する等の措置を講じ、同一課等であっても、当該特定の職員等以外の職員等が閲覧及び使用ができないようにしなければならない。

（文書管理システムの設定等）

第７１条　情報システム管理者は、文書管理システムの操作権限を適切に設定し、職員等が他課等のデータの閲覧及び更新ができないように設定しなければならない。

２　情報システム管理者は、特定の職員等しか取扱えないデータについては、当該データの閲覧及び更新の権限を付与する範囲を必要最小限の職員に限る等の措置を講じ、同一課等であっても、当該特定の職員等以外の職員等が閲覧及び更新を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７２条　統括情報セキュリティ管理者及び情報システム管理者は、情報資産の破損又は故障によるデータの消失等に備え、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７３条　情報システム管理者は、他の地方公共団体等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は、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責任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７４条　情報システム管理者は、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　統括情報セキュリティ管理者及び情報システム管理者は、所管する情報システムにおいて、システムの変更等の作業を行った場合は、当該作業内容について記録し、当該記録を詐取、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。

３　統括情報セキュリティ管理者、情報システム管理者又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人以上の者が作業し、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７５条　統括情報セキュリティ管理者及び情報システム管理者は、ネットワーク構成図、情報システム仕様書等について、記録媒体にかかわらず、業務上必要とする者以外の者が閲覧、紛失等をすることがないよう、適切に管理しなければならない。

（ログの取得等）

第７６条　統括情報セキュリティ管理者及び情報システム管理者は、各種ログ（システムに起こった出来事についての情報等を一定の形式で時系列的に記録し、及び蓄積したデータのことをいう。以下同じ。）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　統括情報セキュリティ管理者及び情報システム管理者は、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、適切にログを管理しなければならない。

３　統括情報セキュリティ管理者及び情報システム管理者は、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７７条　統括情報セキュリティ管理者及び情報システム管理者は、職員等からの情報システム障害の報告、情報システム障害に対する処理結果及び問題等を、障害記録として記録し、適切に保存しなければならない。

（ネットワークの管理）

第７８条　統括情報セキュリティ管理者は、既存のネットワークの安全性が脅かされることのないよう適切なセキュリティ対策に努めなければならない。

（ネットワークの接続制御、経路制御等）

第７９条　統括情報セキュリティ管理者は、フィルタリング（データを指定した条件によって通信

を許可するか遮断するかの分類をする機能をいう。）及びルーティング（ＩＰアドレスの情報をもとに通信する際、パケットをどの経路に配送するかを決める経路制御の機能をいう。）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（庁内ネットワーク、外部等への公開サーバへの不正侵入の防御を行うためのソフトウェア及びハードウェアをいう。以下同じ。）、ルータ（ネットワーク同士を接続するデバイスであって、ネットワーク上を流れるデータを他のネットワークに中継する機器をいう。）等の通信ソフトウェア等を設定しなければならない。

２　統括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８０条　情報システム管理者は、電子申請の汎用受付システム等の外部の者が利用できるシステムについては、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８１条　情報システム管理者は、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、ＣＩＳＯ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　情報システム管理者は、接続した外部ネットワークの瑕疵（かし）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　統括情報セキュリティ管理者及び情報システム管理者は、ウェブサーバ等をインターネットに公開する場合は、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８２条　統括情報セキュリティ管理者は、複合機（複写機、プリンター、イメージスキャナ、ファクシミリ等の機能が一つにまとめられている機器をいう。以下同じ。）をネットワークに接続

する場合は、次に掲げる対策を講じなければならない。

⑴　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、適切なセキュリティ要件を策定すること。

⑵　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ずること。

⑶　複合機のネットワーク接続を終了する場合は、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ずること。

（ＩｏＴ機器を含む特定用途機器のセキュリティ管理）

第８３条　統括情報セキュリティ管理者は、特定の用途に使用する情報システム機器について、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８４条　情報セキュリティ管理者は、無線ＬＡＮを利用する場合は、統括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　統括情報セキュリティ管理者は、無線ＬＡＮの利用を認める場合は、解読が困難な暗号化及び認証技術その他十分なセキュリティ対策の実施を義務付けなければならない。

（電子メールのセキュリティ管理）

第８５条　統括情報セキュリティ管理者は、電子メールのセキュリティ管理について次に掲げる対策を講じなければならない。

⑴　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を含む。）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うこと。

⑵　スパムメール（受信者の意向を無視して、無差別かつ大量に一括して送信されるメールをいう。）等の受信又は送信を検知した場合は、メールサーバの運用を停止すること。

⑶　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すること。

⑷　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すること。

⑸　情報システムの開発、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ること。

（電子メールの利用制限）

第８６条　職員等は、電子メールを利用する場合には、次に掲げる事項を遵守した上で、細心の注意を払い使用しなければならない。

⑴　自動転送機能を用いて、電子メールを転送しないこと。

⑵　業務上必要のない送信先に電子メールを送信しないこと。

⑶　複数人に電子メールを送信する場合は、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すること。

⑷　重要な電子メールを誤送信した場合は、情報セキュリティ管理者に直ちに報告すること。

（電子署名及び暗号化等）

第８７条　職員等は、別表の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、ＣＩＳＯが定めた電子署名、暗号化又はパスワード設定等の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、暗号化を行う場合は、ＣＩＳＯが定める方法以外の方法を用いてはならない。この場合において、職員等は、ＣＩＳＯ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　ＣＩＳＯ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（外部に送るデータの受信者をいう。）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８８条　職員等は、業務上使用するパソコン、モバイル端末等へ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、ソフトウェアを導入する必要がある場合は、情報セキュリティ管理者等の許可を得てソフトウェアを導入するものとする。

３　情報セキュリティ管理者等は、当該ソフトウェアのライセンスを適切に管理しなければならない。

４　職員等は、不正にコピー、改ざん等がされ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８９条　職員等は、業務上使用するパソコン、モバイル端末等に対し機器の改造、増設又は交換を行ってはならない。

２　職員等は、業務上、パソコン、モバイル端末等に対し機器の改造、増設又は交換を行う必要がある場合には、統括情報セキュリティ管理者及び情報システム管理者の許可を得なければならない。

（業務外ネットワークへの接続の禁止）

第９０条　職員等は、業務上使用するパソコン、モバイル端末等を、統括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は異なるネットワークに接続してはならない。

（業務以外の目的でのウェブ閲覧の禁止）

第９１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　統括情報セキュリティ管理者は、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。

（ウェブ会議サービスの利用時の対策）

第９２条　統括情報セキュリティ責任者は、ウェブ会議を適切に利用するための手順を定めなければならない。

２　職員等は、ウェブ会議を利用する場合には、次に掲げる事項を遵守しなければならない。

⑴　前項に定める利用手順に従い、ウェブ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。

⑵　ウェブ会議を主催するときは、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。

⑶　外部からウェブ会議に招待される場合は、前項に定める利用手順に従い、必要に応じて情報セキュリティ管理者等に利用申請を行い、承認を得ること。

（ソーシャルメディアサービスの利用）

第９３条　統括情報セキュリティ責任者は、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は、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。

⑴　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、本市の自己管理ウェブサイトにおいて、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により、なりすまし対策を実施すること。

⑵　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、紙等をいう。）等を適正に管理する等により、不正アクセス対策を実施すること。

２　職員等は、別表の機密性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　情報セキュリティ管理者等は、ソーシャルメディアサービスを利用する場合は、サービスごとの責任者を定めなければならない。

４　前項の責任者は、アカウントの乗っ取り等の不正利用を確認した場合は、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　情報セキュリティ管理者等は、別表の可用性２の情報の提供にソーシャルメディアサービスを利用する場合は、本市の自己管理ウェブサイトに当該情報を掲載して参照可能とするものとする。

第２節　アクセス制御

（アクセス制御等）

第９４条　統括情報セキュリティ管理者又は情報システム管理者は、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システム上制限を設けなければならない。

（利用者ＩＤの取扱い）

第９５条　統括情報セキュリティ管理者及び情報システム管理者は、所管する情報システムの利用者の登録、変更、抹消等の情報管理、職員等の異動、出向又は退職に伴う利用者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、利用者ＩＤが必要なくなった場合は、利用者登録の抹消について、統括情報セキュリティ管理者又は情報システム管理者に報告しなければならない。

３　統括情報セキュリティ管理者及び情報システム管理者は、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。

（特権を付与されたＩＤの管理等）

第９６条　統括情報セキュリティ管理者及び情報システム管理者は、管理者権限等の特権（以下「特権」という。）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管理者及び情報システム管理者の特権を付与されたＩＤを利用する者は、ＣＩＳＯが認めた者でなければならない。

３　統括情報セキュリティ管理者及び情報システム管理者は、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。

４　統括情報セキュリティ管理者及び情報システム管理者は、特権を付与されたＩＤ及びパスワードについて、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　統括情報セキュリティ管理者及び情報システム管理者は、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。

（職員等による外部からのアクセス等の制限）

第９７条　職員等は、外部から内部のネットワーク及び情報システムにアクセスする場合は、統括情報セキュリティ管理者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

２　統括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　統括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　統括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措置を講じなければならない。

５　統括情報セキュリティ管理者及び情報システム管理者は、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、統括情報セキュリティ管理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　統括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。ただし、止むを得ず接続を許可する場合は、利用者のＩＤ、パスワード及び多要素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。

（自動識別の設定）

第９８条　統括情報セキュリティ管理者及び情報システム管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

（ログイン時の表示等）

第９９条　統括情報セキュリティ管理者及び情報システム管理者は、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システムを設定しなければならない。

（認証情報の管理）

第１００条　統括情報セキュリティ管理者又は情報システム管理者は、所管するシステムを使用す

る職員等の認証情報を厳重に管理しなければならない。この場合において、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　統括情報セキュリティ管理者又は情報システム管理者は、所管する情報システムを使用する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、ログイン後直ちに当該仮のパスワードを変更させなければならない。

３　統括情報セキュリティ管理者又は情報システム管理者は、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。

（特権による接続時間の制限）

第１０１条　統括情報セキュリティ管理者及び情報システム管理者は、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。

第３節　システム開発、導入、保守等

（情報システムの調達）

第１０２条　統括情報セキュリティ管理者及び情報システム管理者は、システムの開発、導入、保守等を調達する場合は、技術的なセキュリティ対策を十分に講じなければならない。

２　統括情報セキュリティ管理者及び情報システム管理者は、所管する情報システム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、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１０３条　統括情報セキュリティ管理者及び情報システム管理者は、情報システムを開発する場合は、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。この場合において、当該システム開発のための規程を定めなければければならない。

２　統括情報セキュリティ管理者及び情報システム管理者は、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。

３　統括情報セキュリティ管理者及び情報システム管理者は、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。

４　統括情報セキュリティ管理者及び情報システム管理者は、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。

５　統括情報セキュリティ管理者及び情報システム管理者は、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は、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。

（開発環境と運用環境の分離及び移行手順の明確化）

第１０４条　統括情報セキュリティ管理者及び情報システム管理者は、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。

２　統括情報セキュリティ管理者及び情報システム管理者は、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、システム開発及び保守計画の策定の際にその手順を明確にしなければならない。

３　統括情報セキュリティ管理者及び情報システム管理者は、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、当該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。

４　統括情報セキュリティ管理者及び情報システム管理者は、導入するシステム及び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。

（情報システムの導入に係る試験）

第１０５条　統括情報セキュリティ管理者及び情報システム管理者は、新たに情報システムを導入する場合は、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。

２　統括情報セキュリティ管理者及び情報システム管理者は、新たに導入した情報システムの運用試験を行う場合は、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。

３　統括情報セキュリティ管理者及び情報システム管理者は、個人情報及び機密性の高いデータを試験データに使用してはならない。

４　統括情報セキュリティ管理者及び情報システム管理者は、開発したシステムについて受け入れ試験を行う場合は、開発した組織と導入する組織が、それぞれ独立した試験を行わせなければならない。

（システム開発及び保守に関連する資料等の整備及び保管）

第１０６条　統括情報セキュリティ管理者及び情報システム管理者は、システム開発及び保守に関連する資料並びにシステム関連文書を適切に整備し、保管しなければならない。

２　統括情報セキュリティ管理者及び情報システム管理者は、前条の規定による試験の結果を一定期間保管しなければならない。

３　統括情報セキュリティ管理者及び情報システム管理者は、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１０７条　統括情報セキュリティ管理者及び情報システム管理者は、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に情報システムを設計しなければならない。

２　統括情報セキュリティ管理者及び情報システム管理者は、故意又は過失により情報が改ざんされ、又は漏えいするおそれがある場合には、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しなければならない。

３　統括情報セキュリティ管理者及び情報システム管理者は、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１０８条　統括情報セキュリティ管理者及び情報システム管理者は、情報システムを変更した場合は、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。

（開発及び保守用のソフトウェアの更新等）

第１０９条　統括情報セキュリティ管理者及び情報システム管理者は、開発及び保守用のソフトウェア等を更新し、又はパッチ（ソフトウェアの欠陥修正や機能追加などを目的にソフトウェアの書き換えを行うプログラムをいう。以下同じ。）の適用をする場合は、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１１０条　統括情報セキュリティ管理者及び情報システム管理者は、情報システムの更新又は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又は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

（統括情報セキュリティ責任者の措置事項）

第１１１条　統括情報セキュリティ責任者は、不正プログラム対策として、次に掲げる措置をしなければならない。

⑴　外部ネットワークから受信したファイルについて、インターネットのゲートウェイ（ネットワークとネットワークを接続するためのハードウェア及びソフトウェアのことをいう。以下同じ。）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、不正プログラムの情報システムへの侵入を防止すること。

⑵　外部ネットワークに送信するファイルについて、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、不正プログラムの外部への拡散を防止すること。

⑶　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すること。

⑷　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ること。

⑸　不正プログラム対策ソフトウェアのパターンファイル（コンピュータウイルスを検知するために、各ウイルスの特徴をまとめたデータベースのことをいう。以下同じ。）を常に最新の状態に保つこと。

⑹　不正プログラム対策のソフトウェアを常に最新の状態に保つこと。

⑺　業務で利用するソフトウェアは、パッチ、バージョンアップ等の開発元のサポートが終了したものを利用しないこと。

（統括情報セキュリティ管理者の措置事項）

第１１２条　統括情報セキュリティ管理者は、不正プログラム対策として、次に掲げる措置をしなければならない。

⑴　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それらのシステムに常駐させること。

⑵　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つこと。

⑶　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は、コンピュータウイルス等の感染を防止するために、市が管理している電磁的記録媒体以外のものを職員等に利用させないこと。

⑷　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、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の更新を実施すること。

（職員等の遵守事項）

第１１３条　職員等は、不正プログラム対策に関し次に掲げる事項を遵守しなければならない。

⑴　パソコン、モバイル端末等において、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ないこと。

⑵　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うこと。

⑶　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、速やかに削除すること。

⑷　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すること。

⑸　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うこと。

⑹　インターネット接続系で受信したインターネットメール又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、無害化すること。

⑺　統括情報セキュリティ管理者が提供するコンピュータウイルスの情報を常に確認すること。

⑻　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、直ちに統括情報セキュリティ管理者に報告し、その指示を求めること。また、次のア及びイに掲げる端末の種類に応じ、当該ア及びイに定める対応を行うこと。

ア　パソコン等の端末　ＬＡＮケーブルを直ちに取り外すこと。

イ　モバイル端末　直ちに利用を中止し、通信を行わない設定への変更を行うこと。

（専門家の支援体制）

第１１４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、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

（統括情報セキュリティ責任者の措置事項）

第１１５条　統括情報セキュリティ責任者は、不正アクセス対策として、次に掲げる措置をしなければならない。

⑴　使用されていないポートを閉鎖すること。

⑵　不要なサービスについて、機能を削除又は停止すること。

⑶　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、データの書換えを検出し、統括情報セキュリティ管理者及び情報システム管理者へ通報するよう、設定すること。

⑷　総合政策課デジタル戦略推進室と連携し、監視、通知、外部連絡窓口との連携その他適切な対応を実施できる体制及び連絡網を構築すること。

（サーバ等への攻撃に対する措置）

第１１６条　ＣＩＳＯ及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けることが明確になった場合は、システムの停止を含む必要な措置を講じ、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１１７条　ＣＩＳＯ及び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行為の禁止等に関する法律（平成１１年法律第１２８号）の規定に違反する犯罪の可能性がある場合には、当該攻撃の記録を保存するとともに、警察及び関係機関と緊密に連携し、対応に努めなければならない。

（内部からの攻撃の監視）

第１１８条　統括情報セキュリティ管理者及び情報システム管理者は、職員等及び委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃及び外部のサイト等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１１９条　統括情報セキュリティ管理者及び情報システム管理者は、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、適切な処置を求めなければならない。

（サービス不能攻撃への対策）

第１２０条　統括情報セキュリティ管理者及び情報システム管理者は、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。

（標的型攻撃への対策）

第１２１条　統括情報セキュリティ管理者及び情報システム管理者は、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、次に掲げる措置を講じなければならない。

⑴　職員教育等の人的対策

⑵　標的型攻撃による組織内部への侵入を提言する入口対策

⑶　侵入範囲の拡大の困難度を上げる内部対策

⑷　外部との不正通信を検知して対処する出口対策

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及び共有並びにソフトウェアの更新等）

第１２２条　統括情報セキュリティ管理者及び情報システム管理者は、セキュリティホール（ソフトウェア等において、プログラムの不具合、設計上のミス等が原因となって発生した情報セキュリティ上の欠陥のことをいう。）に関する情報を収集し、必要に応じ、関係者間で共有し、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及び周知）

第１２３条　統括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１２４条　統括情報セキュリティ管理者及び情報システム管理者は、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、情報セキュリティに関する社会環境、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８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１２５条　統括情報セキュリティ管理者及び情報システム管理者は、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。

第１２６条　統括情報セキュリティ管理者及び情報システム管理者は、重要なログ等を取得するサーバの正確な時刻の設定及びサーバ間の時刻の同期ができる措置を講じなければならない。

第１２７条　統括情報セキュリティ管理者及び情報システム管理者は、外部と常時接続する情報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１２８条　情報セキュリティ管理者等は、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、問題を認める場合には、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。

第１２９条　統括情報セキュリティ責任者は、前条の問題が発生した場合は、適切かつ速やかに対処しなければならない。

第１３０条　統括情報セキュリティ管理者及び情報システム管理者は、ネットワーク、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、電磁的記録媒体等の利用状況調査）

第１３１条　ＣＩＳＯ及びＣＩＳＯ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、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１３２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は、直ちに情報セキュリティ管理者等に報告を行わなければならない。

第１３３条　情報セキュリティ管理者等は、前条の規定により報告を受けた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判断した場合は、次条に規定する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１３４条　ＣＩＳＯ又は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ける連絡、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の緊急時対応計画（以下「緊急時対応計画」という。）を定め、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１３５条　緊急時対応計画には、次に掲げる事項を定めなければならない。

⑴　関係者の連絡先

⑵　発生した事案に係る報告すべき事項

⑶　発生した事案への対応措置

⑷　再発防止措置の策定

（業務継続計画との整合性確保）

第１３６条　情報セキュリティ委員会は、矢板市業務継続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１３７条　ＣＩＳＯ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、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内容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１３８条　情報セキュリティ管理者等及び情報システム管理者は、情報セキュリティポリシーその他の規程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、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、別に定める申請書によりＣＩＳＯ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１３９条　前条の規定にかかわらず、情報セキュリティ管理者等及び情報システム管理者は、行政事務の遂行に緊急を要すると認める場合は、ＣＩＳＯの許可を得ずに例外措置を実施することできる。この場合において、情報セキュリティ管理者等及び情報システム管理者は、事後速やかにＣＩＳＯに当該例外措置について報告しなければならない。

（例外措置の申請書の管理）

第１４０条　ＣＩＳＯは、第１３８条に規定する例外措置の申請書及びその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。

第５節　法令遵守

（法令遵守）

第１４１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、次に掲げる法令のほか関係法令及び情報セキュリティポリシーその他の規程を遵守し、これに従わなければならない。

⑴　地方公務員法（昭和２５年法律第２６１号）

⑵　著作権法（昭和４５年法律第４８号）

⑶　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）

⑷　個人情報の保護に関する法律（平成１５年法律第５７号）

⑸　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）

⑹　サイバーセキュリティ基本法（平成２６年法律第１０４号）

⑺　個人情報の保護に関する法律（平成１５年法律第５７号）

（違反に対する対応）

第１４２条　職員等の前条の法令等に違反する行動を確認した場合の対応は、次に掲げるとおりとする。

⑴　統括情報セキュリティ責任者が違反を確認した場合は、当該職員等が所属する課等の情報セキュリティ管理者等に通知し、適切な措置を求めなければならない。

⑵　統括情報セキュリティ管理者が違反を確認した場合は、速やかに統括情報セキュリティ責任者及び当該職員が所属する課等の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。

⑶　前２号の規定による措置に基づく指導によっても職員等の違反行動が改善されない場合は、統括情報セキュリティ責任者は、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し、又は剥奪することができる。この場合において、統括情報セキュリティ責任者は、速やかに、職員等の権利を停止し、又は剥奪した旨をＣＩＳＯ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。

第９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１４３条　情報セキュリティ管理者等は、委託事業者の選定に当たり、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　情報セキュリティ管理者等は、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。

３　情報セキュリティ管理者等は、クラウドサービス（手元のコンピュータで利用していたデータ及びソフトウェアについてネットワークを経由し、サービスとして利用者に提供するものをいう。）を利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

（契約項目）

第１４４条　情報システムの運用、保守等を業務委託する場合には、当該委託事業者との間で必要に応じて次に掲げる情報セキュリティに係る要件を明記した契約を締結しなければならない。

⑴　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

⑵　委託事業者の責任者、委託内容、作業者及び作業場所の特定

⑶　提供されるサービスレベルの保証

⑷　委託事業者にアクセスを許可する情報の種類及び範囲並びにそのアクセス方法

⑸　委託事業者の従業員に対する教育の実施

⑹　提供された情報の目的外利用及び受託者以外の者への提供の禁止

⑺　業務上知り得た情報の守秘義務

⑻　再委託に関する制限事項の遵守

⑼　委託業務終了時の情報資産の返還、廃棄等

⑽　委託業務の定期報告及び緊急時報告の義務

⑾　市による監査及び検査

⑿　市による情報セキュリティインシデント発生時の公表

⒀　情報セキュリティポリシーが遵守されなかった場合の損害賠償等に関する規定

（業務委託に係るセキュリティの確認、措置等）

第１４５条　情報セキュリティ管理者等は、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、必要に応じ契約に基づく措置をしなければならない。この場合において、情報セキュリティ管理者等は、その確認した内容及び措置について統括情報セキュリティ責任者に報告するとともに、その重要度に応じてＣＩＳＯに報告しなければならない。

（再委託）

第１４６条　再委託は、原則禁止する。ただし、契約権者は、例外的に再委託を認める場合には、再委託事業者における情報セキュリティ対策が十分図られており、委託事業者と同等の水準であることを確認し、委託事業者との契約事項を担保させた上で許可しなければならない。

（再委託に係るセキュリティの確認、措置等）

第１４７条　情報セキュリティ管理者等は、前条ただし書の規定により、再委託が許可された場合は、当該再委託をされた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、必要に応じ契約に基づく措置をしなければならない。この場合において、情報セキュリティ管理者等は、その確認した内容及び措置について統括情報セキュリティ責任者に報告するとともに、その重要度に応じてＣＩＳＯに報告しなければならない。

第２節　機密性２以上の情報を取り扱う外部サービスの利用

（機密性２以上の情報を取り扱う外部サービスの利用に係る規定の整備）

第１４８条　統括情報セキュリティ責任者は、次に掲げる事項を規定した別表の機密性２以上の情報を取り扱う外部サービス（民間事業者等の庁外の組織が約款に基づきインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うもの（利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除く。）をいう。）の利用に関する規定を整備しなければならない。

⑴　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「外部サービス利用判断基準」という。）

⑵　外部サービス提供者の選定基準

⑶　外部サービスの利用申請の許可権限者と利用手続

⑷　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

（機密性２以上の情報を取り扱う外部サービスの選定）

第１４９条　情報セキュリティ責任者は、別表の機密性２以上の情報を取り扱う外部サービスを選定するときは、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ものとする。

２　情報セキュリティ責任者は、別表の機密性２以上の情報を取り扱う外部サービスを選定するときは、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ものとする。その際は、次に掲げる事項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ものとする。

⑴　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

⑵　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

⑶　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

⑷　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

⑸　情報セキュリティインシデントへの対処方法

⑹　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

⑺　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、別表の機密性２以上の情報を取り扱う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ものとする。

４　情報セキュリティ責任者は、別表の機密性２以上の情報を取り扱う外部サービスの利用を通じて本市が取り扱う情報について、必要に応じて次に掲げる内容を外部サービス提供者の選定条件に含めるものとする。

⑴　情報セキュリティ監査の受入れ

⑵　サービスレベルの保証

５　情報セキュリティ責任者は、別表の機密性２以上の情報を取り扱う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並びに契約に定める準拠法及び裁判管轄を選定条件に含めるものとする。

6　情報セキュリティ責任者は、別表の機密性２以上の情報を取り扱う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ものとする。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ものとする。

7　情報セキュリティ責任者は、別表の機密性２以上の情報を取り扱う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ものとする。

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、各種の認定及び認証制度の適用状況等から、別表の機密性２以上の情報を取り扱う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及び客観的に評価し判断するものとする。

（機密性２以上の情報を取り扱う外部サービスの利用に係る調達及び契約）

第１５０条　情報セキュリティ責任者は、別表の機密性２以上の情報を取り扱う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ものとする。

２　情報セキュリティ責任者は、別表の機密性２以上の情報を取り扱う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ものとする。

（機密性２以上の情報を取り扱う外部サービスの利用承認）

第１５１条　情報セキュリティ責任者は、別表の機密性２以上の情報を取り扱う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うものとする。

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ものとする。

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ものとする。

（機密性２以上の情報を取り扱う外部サービスを利用した情報システムの導入及び構築時の対策）

第１５２条　統括情報セキュリティ責任者は、別表の機密性２以上の情報を取り扱う外部サービス

の特性や責任分界点に係る考え方等を踏まえ、次に掲げる事項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。

⑴　不正なアクセスを防止するためのアクセス制御

⑵　取り扱う情報の機密性保護のための暗号化

⑶　開発時におけるセキュリティ対策

⑷　設計及び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し、及び記録しなければならない。

（機密性２以上の情報を取り扱う外部サービスを利用した情報システムの運用及び保守時の対策）

第１５３条　統括情報セキュリティ責任者は、別表の機密性２以上の情報を取り扱う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、次に掲げる事項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。

⑴　外部サービス利用方針の規定

⑵　外部サービス利用に必要な教育

⑶　取り扱う資産の管理

⑷　不正アクセスを防止するためのアクセス制御

⑸　取り扱う情報の機密性保護のための暗号化

⑹　外部サービス内の通信の制御

⑺　設計及び設定時の誤りの防止

⑻　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、運用及び保守時に実施状況を定期的に確認及び記録しなければならない。

（機密性２以上の情報を取り扱う外部サービスを利用した情報システムの更改及び廃棄時の対策）

第１５４条　統括情報セキュリティ責任者は、別表の機密性２以上の情報を取り扱う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、外部サービスの利用を終了する際における次に掲げるセキュリティ対策を規定しなければならない。

⑴　外部サービスの利用終了時における対策

⑵　外部サービスで取り扱った情報の廃棄

⑶　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及び記録しなければならない。

第３節　機密性２以上の情報を取り扱わない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外部サービスの利用に係る規定の整備）

第１５５条　統括情報セキュリティ責任者は、次に掲げる事項を規定した別表の機密性２以上の情報を取り扱わない外部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。この場合において、当該外部サービスの利用については、別表の機密性２以上の情報が取り扱われないようにしなければならない。

⑴　外部サービスを利用可能な業務の範囲

⑵　外部サービスの利用申請の許可権限者と利用手続

⑶　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

⑷　外部サービスの利用の運用手順

第１０章　評価及び見直し

第１節　監査

（実施方法）

第１５６条　ＣＩＳＯは、情報セキュリティ監査責任者を指名し、ネットワーク、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行わなければならない。

（監査実施計画の立案及び実施への協力）

第１５７条　情報セキュリティ監査責任者は、監査を行うに当たって、監査実施計画を立案し、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　被監査部署は、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１５８条　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、必要に応じて、情報セキュリティポリシーの遵守について監査を行わなければならない。

（報告）

第１５９条　統括情報セキュリティ監査責任者は、監査結果を取りまとめ、情報セキュリティ委員会に報告しなければならない。

（保管）

第１６０条　情報セキュリティ監査責任者は、監査の実施を通して収集した監査証拠及び監査報告書の作成のための監査調書を、適正に保管しなければならない。

（監査結果への対応）

第１６１条　ＣＩＳＯは、監査結果について、所管する情報セキュリティ管理者及び関連する情報セキュリティ管理者に対し、指摘事項への対処を指示しなければならない。

２　ＣＩＳＯは、監査結果について、庁内で横断的に改善が必要な場合は、統括情報セキュリティ責任者に対し、指摘事項への対処を指示しなければならない。

（情報セキュリティポリシー及び関係規程等見直し等への活用）

第１６２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２節　自己点検

（実施方法）

第１６３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、所管するネットワーク及び情報システムについて、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、所管する部局における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、必要に応じて自己点検を行わなければならない。

（報告）

第１６４条　統括情報セキュリティ責任者、情報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、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１６５条　職員等は、自己点検の結果に基づき、自ら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、前項の点検結果を情報セキュリティポリシー、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。

（情報セキュリティポリシー、関係規程等の見直し）

第１６６条　情報セキュリティ委員会は、情報セキュリティ監査、情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシー、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、必要があると認める場合は、改善を行うものとする。

第１１章　雑則

（補則）

第１６７条　この基準に定めるもののほか情報セキュリティ対策に関し必要な事項は、市長が別に定める。

附　則

この要綱は、令和５年４月１日から施行する。

別表（第１９条、第２０条、第２２条、第２３条、第２４条、第２５条、第２６条、第２７条、第第２８条、第２９条、第３８条、第４２条、第４４条、第４９条、第８７条、第９３条、第１４８条、第１４９条、第１５０条、第１５１条、第１５２条、第１５３条、第１５４条、第１５５条関係）

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	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	⑴　支給以外の端末での作業の原則禁止（機密性３の情報資産に限る。） ⑵　必要以上の複製及び配付の禁止 ⑶　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 ⑷　情報の送信、情報資産の運搬及び提供時における暗号化及びパスワード設定並びに鍵付きケースへの格納 ⑸　復元不可能な処理を施しての廃棄 ⑹　信頼のできるネットワーク回線の選択 ⑺　外部で情報処理を行う際の安全管理措置に係る内部規程の制定 ⑻　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１	機密性２又は機密性３の情報資産以外の情報資産	－

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	行政事務で取り扱う情報資産のうち、改ざん、誤り又は破損により、住民の権利が侵害され、又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれのある情報資産	⑴　バックアップ及び電子署名付与 ⑵　外部で情報処理を行う際の安全管理措置に係る内部規程の制定 ⑶　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	－

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	行政事務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、又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	⑴　バックアップ及び指定する時間以内の復旧 ⑵　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	－