別紙②

小林市行政情報セキュリティポリシー

小林市
平成 18 年 3 月 20 日作成
小林市情報化推進委員会了承

序　小林市行政情報セキュリティポリシーの構成

第１章　情報セキュリティ基本方針

１　目的
２　定義
３　情報セキュリティポリシーの位置付け
４　対象とする脅威
５　適用範囲
６　職員等の遵守義務
７　情報セキュリティ対策
８　情報セキュリティ監査及び自己点検の実施
９　情報セキュリティポリシーの見直し
１０　情報セキュリティ対策基準の策定
１１　情報セキュリティ実施手順の策定

第２章　情報セキュリティ対策基準

１　組織体制
２　情報資産の分類と管理
　２．１　行政情報の分類
　２．２　情報資産の管理
３　情報システム全体の強靭性の向上
　３．１　マイナンバー利用事務系
　３．２　LGWAN 接続系
　３．３　インターネット接続系
　３．４　独立系
４　物理的セキュリティ
　４．１　サーバ等の管理
　４．２　管理区域（情報システム室等）の管理
　４．３　通信回線及び通信回線装置の管理
　４．４　職員等の利用する端末や電磁的記録媒体等の管理
５　人的セキュリティ
　５．１　職員等の遵守事項
　５．２　研修・訓練
　５．３　情報セキュリティインシデントの報告
　５．４　ＩＤ及びパスワード等の管理

序　小林市行政情報セキュリティポリシーの構成

小林市行政情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）とは、小林市が保有する情報資産に関するセキュリティ対策について、総合的、体系的に取りまとめたものである。

情報セキュリティポリシーは、本市の情報資産を利用する職員に浸透、定着させるものであり、安定的な規範であることが要請される。しかし一方では、情報セキュリティ対策は、情報の処理技術や通信技術等の進展に伴う急速な状況の変化に柔軟に対応することも必要である。

このようなことから、一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と、情報資産を取り巻く状況の変化に適正に対応する部分としての「情報セキュリティ対策基準」の２階層から成るものとして情報セキュリティポリシーを策定することとする。また、情報セキュリティポリシーに基づき、情報システム毎に、具体的な情報セキュリティ対策の実施手順（運用マニュアル）として「情報セキュリティ実施手順」を策定することとする。

小林市行政情報セキュリティポリシーの構成

文書名		内容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針。
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための、全ての情報資産に共通の情報セキュリティ対策の基準。
情報セキュリティ実施手順		情報システム毎に定める、情報セキュリティ対策基準に基づいた個々の情報資産に関する具体的な対策手順。

第１章　情報セキュリティ基本方針

１　目的

本市が取り扱う情報資産には、市民の個人情報を始めとし行政運営上重要な情報など、部外に漏えい等した場合には極めて重大な結果を招く情報が多数含まれている。これらの情報資産を人的脅威や災害事故等から防御することは、市民の財産、プライバシー等を守るためにも、また、継続的かつ安全・安定的な行政サービスの実施を確保するためにも必要不可欠である。

さらに、市民サービスの向上、業務効率化や合理化の要請に対応するために、本市における情報システムによる業務量及び利用範囲は拡大の一途をたどっており、今や行政運営基盤として欠かせないものとなっている。そのため、本市の業務執行を今後も円滑に進めるためには、本市が管理している全ての情報システムが高度な安全性を有することが不可欠である。

このため、本市の情報資産の機密性、完全性及び可用性を維持するための対策を整備するため、情報セキュリティポリシーを定めることとし、情報セキュリティの確保に最大限取り組むこととする。このうち情報セキュリティ基本方針においては、本市の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの適用範囲、位置付け等を定めるものとする。本市の情報資産を利用する職員は、情報セキュリティの重要性を認識し、この情報セキュリティ基本方針を遵守しなければならない。

２　定義

（１）コンピュータ

パーソナルコンピュータ、サーバ、ストレージ等の機器をいう。

（２）ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

（３）情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

（４）情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（５）情報資産

情報システムで取り扱う情報で、開発及び運用に係るものを含むすべての情報をいう。

（６）情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（７）機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保

することをいう。

（８）完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（９）可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（１０）マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

（１１）LGWAN 接続系

LGWAN に接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く。）。

（１２）インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

（１３）独立系

（１０）、（１１）、（１２）の要件に該当しない情報システムが接続する共用ネットワーク及び当該情報システム専用のネットワーク接続された情報システム及びその情報システムで取り扱うデータをいう。

（１４）通信経路の分割

LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

（１５）無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

３　情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、本市の情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の最高位に位置するものである。

４　対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

（１）不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（２）情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等
（３）地震、落雷、火災等の災害によるサービス及び業務の停止等
（４）大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等
（５）電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等
（６）その他、本市の情報資産の機密性、完全性、可用性を脅かす脅威

５　適用範囲

情報セキュリティポリシーの適用範囲は、以下に示すものとする。
（１）行政機関等の範囲
適用される行政機関等は、市長部局、議会事務局、行政委員会、水道事業、病院事業及びその他本市に属する機関とする。
（２）情報資産の範囲
適用される情報資産は、（１）の行政機関等が所掌する次の情報資産とする。
①ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体
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
（３）対象者
（２）の情報資産に接する組織の職員（会計年度任用職員及び臨時的任用職員等を含む。以下「職員等」という。）とする。

６　職員等の遵守義務

職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって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を遵守しなければならない。

７　情報セキュリティ対策

４に掲げた脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。
（１）組織体制
本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。
（２）情報資産の分類と管理

本市の保有する情報資産を重要度に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（３）情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

①マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

②LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、都道府県及び市区町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（４）物理的セキュリティ

サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

（５）人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（６）技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（７）運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

（８）業務委託と外部サービスの利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、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確認し、必要に応じて契約に基づき措置を講じる。

外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

（９）評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリテ

ィポリシーの見直しを行う。

８　情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

９　情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

１０　情報セキュリティ対策基準の策定

７、８及び９に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

１１　情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

第２章　情報セキュリティ対策基準

情報セキュリティ対策基準とは、情報セキュリティ基本方針を実行に移すための、本市の情報資産に関する情報セキュリティ対策の基準である。

1　組織体制

（1）統括情報管理者

統括情報管理者は、情報資産の情報セキュリティを統括する最高責任者とし、副市長をもってこれに充てる。

（2）情報セキュリティ責任者

①総合政策部長を、統括情報管理者直属の情報セキュリティ責任者とする。情報セキュリティ責任者は、統括情報管理者を補佐しなければならない。

②情報セキュリティ責任者は、部局情報管理者及び情報管理者に対して、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。

③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、統括情報管理者の指示に従い、統括情報管理者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と責任を有する。

④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、緊急連絡網を整備しなければならない。

⑤情報セキュリティ責任者は、緊急時には統括情報管理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。

（3）情報セキュリティ管理者

企画政策課長を情報セキュリティ管理者とする。情報セキュリティ管理者は、情報セキュリティ責任者を補佐し、その実務を担当する。

（4）部局情報管理者

①情報セキュリティの適正な運用及び管理を行うため、情報資産を取り扱う部局等に情報セキュリティに関する権限及び責任を有する部局情報管理者を置き、情報資産を取り扱う部局等の長をもってこれに充てる。

②部局情報管理者は、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。

③部局情報管理者は、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。

（5）情報管理者

①情報セキュリティの適正な運用及び管理を行うため、情報資産を取り扱う課等に情報セキュリティに関する権限及び責任を有する情報管理者を置き、情報資産を取り扱う課等の長をもってこれに充てる。

②情報管理者は、所管する情報システムの開発、設定の変更、運用、更新等を行う権限及び責任を有する。
③情報管理者は、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作成・維持・管理を行うとともに、定められている事項について職員等に実施及び遵守させなければならない。
④情報管理者は、使用する情報システムの機器や電磁的記録媒体について、第三者に使用させること、又は許可なく情報を閲覧させることがないように、適正な措置を施さなければならない。
⑤情報管理者は、非常勤職員及び臨時職員の雇用時に必ず情報セキュリティポリシーのうち、職員等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。
⑥情報管理者は、情報セキュリティに関する適正な運用及び管理を補佐する者（以下「情報マネージャー」という。）を指名するものとし、主幹をもってこれに充てる。
⑦情報管理者は、情報セキュリティに関する適正な運用及び管理を担当する者（「以下「情報クラーク」という。」を指名するものとする。

（６）情報マネージャー

情報マネージャーは、情報管理者の指示に従い、情報システムの開発、調査、設定の変更、運用、更新、記録の整備、企画政策課及び関係機関との連絡・調整、その他必要な調整を行うものとする。

（７）情報クラーク

①情報クラークは、情報マネージャーの指示に従い、情報システムの開発、調査、設定の変更、運用、更新、記録の整備等の作業を行うものとする。
②情報クラークが作業を行う際は、関係課等との連携を図り、特に情報セキュリティの適正な運用及び管理に影響を与える可能性のある作業については、事前に企画政策課と協議しなければならない。

（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情報セキュリティ監査の実施において、止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。

（９）情報セキュリティに関する統一的な窓口の設置

①統括情報管理者は、情報セキュリティインシデント等の統一的な窓口の機能を有する組織として、CSIRT（Computer Security Incident Response Team）を設置し、企画政策課がその役割を担う。

②CSIRT は、情報セキュリティ管理者の指示に従い、情報セキュリティインシデント等に対処し、被害拡大防止、復旧、再発防止等に向けた対応を、迅速かつ的確に実施する。
③情報セキュリティに関して、国や県等の関係機関との情報共有を行う。

２　情報資産の分類と管理

２．１　行政情報の分類

対象となる全ての行政情報は、次の重要性分類に従って分類する。

（１）重要性分類Ⅰ

①個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）第２条第１項に規定する個人情報
②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。以下「番号法」という。）第２条第８項に規定する特定個人情報
③小林市議会の個人情報の保護に関する条例（令和 5 年 4 月 1 日施行）第２条第１項に規定する個人情報
④法令又は条例（以下「法令等」という。）の定めにより守秘義務を課されている行政情報（個人情報を除く）
⑤法人その他の団体に関する行政情報で漏えいすることにより当該団体の利益を害するおそれのあるもの
⑥漏えいした場合、行政に対する信頼を著しく害するおそれのある行政情報を滅失し、又はき損した場合、その復元が著しく困難となり、行政の円滑な執行を妨げるおそれのある行政情報システムに係るパスワード及びシステム設定情報
⑦その他、情報の機密性、完全性及び可用性その他の事情を考慮して、重要性分類Ⅰとして管理することが適当と認める行政情報

（２）重要性分類Ⅱ

①脅威にさらされた場合に実害を受ける危険性は低いが、行政事務の執行において重要性は高いと評価される行政情報（公開されると行政の円滑な執行に著しい障害を生ずるおそれのある行政情報等）
②その他、情報の機密性、完全性及び可用性その他の事情を考慮して、重要性分類Ⅱとして管理することが適当と認める行政情報

（３）重要性分類Ⅲ

重要性分類Ⅰ及び重要性分類Ⅱ以外の行政情報

２．２　情報資産の管理

①管理責任

（ア）情報管理者は、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重要性分類に基づき管理しなければならず、業務上必要のない情報資産の複製を行ってはならない。また、重要性分類Ⅰ及び重要性分類Ⅱに該当する情報については、原則複製してはならず、例外的に、止むを得ず複製する必要がある場合は、情報管理者の許可を得なければならない。

（ウ）職員等は、重要性分類Ⅰ及び重要性分類Ⅱに該当する情報を複製する場合、その対象を必要最小限とし、不要となり次第速やかに消去しなければならない。

（エ）情報管理者は、所管する重要性分類Ⅰ及び重要性分類Ⅱに該当する情報の消去等の実施状況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、必要に応じて情報資産の分類を表示し、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）情報を作成する者は、情報の作成時に重要性分類に基づき、当該情報の分類と取扱制限を定める等適正な管理を行わなければならない。

（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、当該情報を速やかに消去しなければならない。

④情報資産の入手

（ア）庁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重要性分類に基づいた取扱いをしなければならない。

（イ）庁外の者が作成した情報資産を入手した者は、重要性分類に基づき、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重要性分類が不明な場合、情報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、情報資産の重要性分類に応じ、適正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）情報セキュリティ管理者又は情報管理者は、情報資産の重要性分類に従って、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又は情報管理者は、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）情報管理者は、重要性分類Ⅰ及び重要性分類Ⅱ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。また、保管状況等を記録しなければならない。

⑦情報の送信等

重要性分類Ⅰ及び重要性分類Ⅱに該当する情報を原則電子メールや FAX 等により送信してはならず、例外的に、止むを得ず送信する必要がある場合は、情報管理者の許可を得た上で、複数担当者の確認を経て送信しなければならない。また、必要に応じ、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）車両等により重要性分類Ⅰ及び重要性分類Ⅱ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、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）重要性分類Ⅰ及び重要性分類Ⅱの情報資産を運搬する者は、情報管理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）重要性分類Ⅰ及び重要性分類Ⅱの情報資産を外部に提供する者は、必要に応じパスワード等による暗号化を行わなければならない。

（イ）重要性分類Ⅰ及び重要性分類Ⅱの情報資産を外部に提供する者は、情報管理者に許可を得なければならない。

（ウ）情報管理者は、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者は、情報を記録している電磁的記録媒体について、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）情報資産の廃棄やリース返却等を行う者は、情報管理者の許可を得なければならない。

３　情報システム全体の強靭性の向上

３．１　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

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、その外部接続先について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。また、業務毎に専用端末を設置することが望ましい。

②情報の持ち出し不可設定

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。

３．２　LGWAN 接続系

（１）LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は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 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

３．３　インターネット接続系

（１）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）都道府県及び市区町村のインターネットとの通信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、関係省庁や都道府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。

（3）（β モデルを採用する場合）業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末を置き、入札情報や職員等の情報等重要な情報資産を LGWAN 接続系に配置する場合、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

（β´モデルを採用する場合）業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末と入札情報や職員等の情報等重要な情報資産を配置する場合、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

３．４　独立系

独立系ネットワークは、接続する情報システムの機密性、完全性、可用性を確保するために必要な対策を講じなければならない。また、複数の情報システムが接続する独立系ネットワークは、ネットワーク全体として均質なウイルス対策を講じなければならない。

４　物理的セキュリティ

４．１　サーバ等の管理

（1）機器の取付け

情報管理者は、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適正に固定する等、必要な措置を講じなければならない。

（2）サーバの冗長化

①情報管理者は、行政情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバ及びその他の基幹サーバを冗長化し、同一データを保持するよう努めなければならない。

②情報管理者は、メインサーバに障害が発生した場合は、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にするよう努めなければならない。

（3）機器の電源

①情報管理者は、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情報管理者は、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。

（４）通信ケーブル等の配線
①情報セキュリティ管理者及び情報管理者は、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情報セキュリティ管理者及び情報管理者は、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情報セキュリティ管理者及び情報管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適正に管理しなければならない。
④情報セキュリティ管理者、情報管理者は、自ら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施さなければならない。

（５）機器の定期保守及び修理
①情報管理者は、サーバ等の機器の定期保守点検を実施しなければならない。
②情報管理者は、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、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、情報管理者は、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、秘密保守体制の確認等を行わなければならない。

（６）庁外への機器の設置
部局情報管理者及び情報管理者は、庁外にサーバ等の機器を設置する場合、統括情報管理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。

（７）機器の廃棄等
情報管理者は、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。

４．２　管理区域（情報システム室等）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、当該機器等の管理及び運用を行うための部屋（以下「情報システム室等」という。）や電磁的記録媒体の保管庫をいう。

②情報セキュリティ管理者及び情報管理者は、施設管理部門と連携して、情報システム室等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情報セキュリティ管理者及び情報管理者は、情報システム室内の機器等に、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情報セキュリティ管理者及び情報管理者は、情報システム室等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情報セキュリティ管理者及び情報管理者は、情報システム室等への入退室を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職員等及び委託事業者は、情報システム室等に入室する場合、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。
③情報セキュリティ管理者及び情報管理者は、外部からの訪問者が情報システム室等に入る場合には、必要に応じて立ち入り区域を制限した上で、情報システム室等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情報セキュリティ管理者及び情報管理者は、情報資産を扱うシステムを設置している情報システム室等について、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。

（３）機器等の搬入出
①情報管理者は、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。

４．３　通信回線及び通信回線装置の管理
①情報セキュリティ管理者は、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情報セキュリティ管理者は、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情報セキュリティ管理者は、行政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。

４．４　職員等の利用する端末や電磁的記録媒体等の管理

①情報管理者は、盗難防止のため、執務室等で利用するパソコンのワイヤーによる固定、モバイル端末及び電磁的記録媒体の使用時以外の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。

②情報管理者は、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、或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情報セキュリティ管理者及び情報管理者は、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）を行うよう設定しなければならない。

５　人的セキュリティ

５．１　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。

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）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、情報管理者の許可を得なければならない。

（イ）職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許

可を得た上で、パスワード等による認証を必須とするなど、紛失等による情報漏えいを防止するための安全管理措置を講じなければならない。

④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

（ア）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、情報セキュリティ管理者の許可を得て利用することができる。

（イ）職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いて外部で情報処理作業を行う場合には、情報セキュリティ管理者の許可を得た上で、パスワード等による認証を必須とするなど、紛失等による情報漏えいを防止するための安全管理措置を講じなければならない。

⑤持ち出し及び持ち込みの記録

職員等は、端末等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

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。

⑦机上の端末等の管理

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管理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職員等は、インターネットに接続できる端末に、重要性分類Ⅰ及び重要性分類Ⅱの行政情報を保存してはならない。

（２）情報セキュリティポリシー等の掲示

情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び実施手順書を閲覧できるように掲示しなければならない。

（３）委託事業者に対する説明

情報管理者は、ネットワーク及び情報システムの開発・保守等を事業者に発注する場合、再委託事業者も含めて、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。

５．２　研修・訓練

①統括情報管理者は、職員等に対し情報セキュリティポリシーについて啓発に努めるとともに、職員等を対象とした情報セキュリティポリシーに関する研修を定期的に実施しなければならない。また、止むを得ず研修に参加できない職員等に対しては、欠席者が所属する部署の情報管理者においてフォローアップを実施しなければならない。

②情報管理者（情報マネージャー又は情報クラークを含む。）は、情報管理者として必要な知識を維持するための情報通信技術や情報セキュリティに関する研修を受けなければならない。

③情報システムを所管する情報管理者は、情報システムの運用に支障を来さない範囲において緊急時対応を想定した訓練等を職員等に定期的に行わせなければならない。

④情報マネージャー、情報クラーク及び職員等は、情報セキュリティポリシーに関する研修を受講し、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を理解し、情報セキュリティ上の問題が生じないようにしなければならない。

⑤情報システムの開発・保守・運用管理に携わる職員等は、担当者として必要な技術力を習得・維持するための研修を受けなければならない。

５．３　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、直ちに情報管理者に報告しなければならない。

②報告を受けた情報管理者は、直ちに CSIRT 及び部局情報管理者へ報告しなければならない。

③情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、必要に応じて統括情報管理者及び情報セキュリティ責任者に報告しなければならない。

④情報管理者は、情報セキュリティインシデントの内容が、個人情報の漏えい等又は漏えい等が発生したおそれがある場合であって、個人情報保護法第 68 条第 1 項の規定による委員会への報告及び同条第 2 項の規定による本人への通知を要する場合には、速やかに所定の手続を行うとともに、委員会による事案の把握等に協力する。また、統括情報管理者は、情報セキュリティインシデントの内容等に応じて、当該情報セキュリティインシデントの内容、経緯、被害状況等を速やかに市長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、住民等外部から報告を受けた場合、直ちに

情報管理者に報告しなければならない。

②報告を受けた情報管理者は、直ちに CSIRT 及び部局情報管理者に報告しなければならない。

③情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、必要に応じて統括情報管理者及び情報セキュリティ責任者に報告しなければならない。

④情報管理者は、情報セキュリティインシデントの内容が、個人情報の漏えい等又は漏えい等が発生したおそれがある場合であって、個人情報保護法第 68 条第 1 項の規定による委員会への報告及び同条第 2 項の規定による本人への通知を要する場合には、速やかに所定の手続を行うとともに、委員会による事案の把握等に協力する。また、統括情報管理者は、情報セキュリティインシデントの内容等に応じて、当該情報セキュリティインシデントの内容、経緯、被害状況等を速やかに市長に報告しなければならない。

（3）情報セキュリティインシデントの究明・記録、再発防止等

①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引き起こした部門の部局情報管理者、情報管理者、情報マネージャー、情報クラーク及び CSIRT と連携し、これらの情報セキュリティインシデントの影響範囲を特定、原因を究明し、記録を保存しなければならない。その際、事実関係の調査については、情報セキュリティインシデントが発生した部署の情報管理者が行うこととするが、当該インシデントに関与した職員等については、事情聴取の対象とするが、調査には関与させないこととする。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、統括情報管理者に報告しなければならない。

②統括情報管理者は、情報セキュリティ責任者から、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の必要な措置を指示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内容が個人情報の漏えい等である場合は、当該情報の性質や対象人数等に応じて、ホームページや記者会見等によって事実関係及び再発防止策等について公表しなければならない。

5．4　ID 及びパスワード等の管理

（1）IC カードの取扱い

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ー若しくはパソコン等の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は、速やかに情報管理者に通報し、指示に従わ

なければならない。

②情報管理者は、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情報管理者は、IC カード等を切り替える場合、切り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は、情報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、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等の端末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、共用 ID に対するパスワードは除く）。

⑨パスワードは定期的に変更しなければならない。

５．５　接続時間の制限

職員等は、情報システムへの接続について、必要最小限の接続時間で行うように努めるものとする。

６　技術的セキュリティ

６．１　コンピュータ及びネットワークの管理

（１）ファイルサーバ等の設定等

①情報セキュリティ管理者及び情報管理者は、職員等が使用できるファイルサーバ等の容量を設定し、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及び情報管理者は、職員等が他課室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及び情報管理者は、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、同一課室等であっても、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

情報セキュリティ管理者及び情報管理者は、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。

（３）システム管理記録及び作業の確認

①情報マネージャー及び情報クラークは、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情報マネージャー及び情報クラークは、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正に管理しなければならない。
③情報マネージャー及び情報クラークは、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う場合は、必要に応じて２名以上で作業し、互いにその作業を確認させなければならない。

（４）情報システム仕様書等の管理

情報セキュリティ管理者及び情報管理者は、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の閲覧、紛失等がないよう、その保管、複製、廃棄等について適切な措置を講じなければならない。

（５）ログの取得等

①情報セキュリティ管理者及び情報管理者は、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情報セキュリティ管理者及び情報管理者は、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情報セキュリティ管理者及び情報管理者は、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。

（６）障害記録

情報セキュリティ管理者及び情報管理者は、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、適正に保存しなければならない。

（７）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、ネットワークに適正なアクセス制御を施さなければならない。

（８）外部の者が利用できるシステムの分離等

情報管理者は、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。

（９）外部ネットワークとの接続制限等

①情報管理者は、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、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承認を得なければならない。

②情報管理者は、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及び情報管理者は、Web 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、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。

（１０）複合機のセキュリティ管理

①情報管理者は、複合機を調達する場合、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。

（１１）IoT 機器を含む特定用途機器のセキュリティ管理

情報セキュリティ管理者及び情報管理者は、テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている又は電磁的記録媒体を内蔵している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実施しなければならない。

（１２）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。

（１３）電子メールのセキュリティ管理

①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、必要な措置を講じなければならない。
②情報セキュリティ管理者は、大量のスパムメール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及び情報管理者は、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。
⑥情報セキュリティ管理者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように添付ファイルの監視等によりシステム上措置を講じなければならない。

（１４）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、情報管理者、情報マネージャー及び CSIRT に報告しなければならない。

⑤職員等は、フリーメールやフリーのネットワークストレージサービス等を使用してはならない。

（１５）電子署名・暗号化

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、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。

（１６）無許可ソフトウェアの導入等の禁止

①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及び情報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。

（１７）機器構成の変更の制限

①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、情報セキュリティ管理者及び情報管理者の許可を得なければならない。

（１８）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。

（１９）業務以外の目的での Web 閲覧の禁止

①職員等は、業務以外の目的で Web を閲覧してはならない。

②情報セキュリティ管理者は、職員等の Web 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、統括情報管理者及び情報セキュリティ責任者に通知し適正な措置を求めなければならない。

（２０）Web 会議サービスの利用時の対策

①職員等は、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。

②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。

（２１）ソーシャルメディアサービスの利用

①情報管理者は、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、次の情報セキュリティ対策を行わなければならない。

（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などの方法で、不正アクセス対策を実施すること。

②重要性分類Ⅰ及び重要性分類Ⅱ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。

６．２　アクセス制御

（１）アクセス制御等

①アクセス制御

情報セキュリティ管理者及び情報管理者は、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。

②利用者 ID の取扱い

（ア）情報セキュリティ管理者及び情報管理者は、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、情報管理者に通知しなければならない。

（ウ）情報セキュリティ管理者及び情報管理者は、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）情報セキュリティ管理者及び情報管理者は、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。

（イ）情報セキュリティ管理者及び情報管理者の特権を代行する者は、情報セキュリティ管理者及び情報管理者が指名した者でなければならない。

（ウ）情報セキュリティ管理者及び情報管理者は、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）情報セキュリティ管理者及び情報管理者は、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。

（オ）情報セキュリティ管理者及び情報管理者は、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及び当該情報システムを管理する情報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及び当該情報システムを管理する情報管理者は、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及び当該情報システムを管理する情報管理者は、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及び当該情報システムを管理する情報管理者は、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、情報セキュリティ管理者の許可を得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。ただし、止むを得ず接続を許可する場合は、利用者の ID、パスワード及び生体認証に係る情報等の認証情報並びに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。

（4）認証情報の管理

①情報セキュリティ管理者又は情報管理者は、職員等の認証情報を厳重に管理しなければならない。

②情報セキュリティ管理者又は情報管理者は、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。ただし、パスワード変更機能を有しないシステムについては、５．４　ID 及びパスワード等の管理（3）パスワードの取扱い③に従い、発行するものとする。

③情報セキュリティ管理者又は情報管理者は、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。

６．３　システム開発、導入、保守等

（1）情報システムの調達

①情報セキュリティ管理者及び情報管理者は、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情報セキュリティ管理者及び情報管理者は、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システム開発における責任者及び作業者の特定

情報管理者は、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。

（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するよう努めなければならない。

（イ）情報管理者は、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。

（４）システム開発・保守に関連する資料等の整備・保管

①情報管理者は、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正に整備・保管しなければならない。

②情報管理者は、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情報管理者は、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。

（６）情報システムの変更管理

情報管理者は、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の更新等

情報管理者は、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。

（８）システム更新又は統合時の検証等

情報管理者は、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。

６．４　不正プログラム対策

（１）情報セキュリティ管理者の措置事項

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。

（２）情報管理者の措置事項

情報管理者は、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情報管理者は、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、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。

（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、以下の対応を行うとともに、情報管理者、情報マネージャー、情報クラーク及び CSIRT に報告し、指示を仰がなければならない。
（ア）パソコン等の端末の場合
LAN ケーブルの即時取り外しを行わなければならない。
（イ）モバイル端末の場合
直ちに利用を中止し、通信を行わない設定への変更を行わなければならない。

（4）専門家の支援体制
情報セキュリティ管理者は、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。

6．5　不正アクセス対策

（1）情報セキュリティ管理者の措置事項
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 Web 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、CSIRT 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、監視、通知、外部連絡窓口及び適正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。

（2）攻撃への対処
統括情報管理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るリスクがある場合、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。

（3）記録の保存
統括情報管理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
情報セキュリティ管理者及び情報管理者は、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

情報セキュリティ管理者及び情報管理者は、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

情報セキュリティ管理者及び情報管理者は、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、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）等を講じなければならない。

６．６　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

情報セキュリティ管理者及び情報管理者は、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。

（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。

（３）情報セキュリティに関する情報の収集及び共有

情報セキュリティ管理者及び情報管理者は、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。

７　運用

７．１　情報システムの監視

①情報セキュリティ管理者及び情報管理者は、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できるよう設定しなければならない。また、必要に応じて、当該設定を定期的に見直さなければならない。

②情報セキュリティ管理者及び情報管理者は、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。

③情報セキュリティ管理者及び情報管理者は、外部と常時接続するシステムを常時監視できるよう設定しなければならない。また、必要に応じて、当該設定を定期的に見直さなければならない。

７．２　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部局情報管理者及び情報管理者は、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。

②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情報セキュリティ管理者及び情報管理者は、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正かつ速やかに対処しなければならない。

（２）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

情報セキュリティ管理者は、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。

（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管理者及び情報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管理者が判断した場合は、緊急時対応計画に従って適正に対処しなければならない。

７．３　侵害時の対応等

（１）緊急時対応計画の策定

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）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情報セキュリティ責任者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

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。

７．４　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情報管理者は、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、統括情報管理者の許可を得て、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情報管理者は、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管理者及び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

情報セキュリティ管理者は、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。

７．５　法令遵守

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（平成 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個人情報保護法
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）

７．６　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部局情報管理者、情報管理者及び CSIRT に通知し、適正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が違反を確認した場合は、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。また、当該職員等が所属する部局情報管理者及び情報管理者に通知し、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管理者及び当該職員等が所属する部局情報管理者及び情報管理者に通知しなければならない。

８　業務委託と外部サービスの利用

８．１　業務委託

（１）委託事業者の選定基準

情報管理者は、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、保守等を外部委託する場合には、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等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
・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受託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）の契約等に基づき措置しなければならない。また、その内容を部局情報管理者に報告しなければならない。

８．２　外部サービスの利用（重要性分類Ⅰ及び重要性分類Ⅱの情報を取り扱う場合）

（１）外部サービスの選定

①情報管理者は、取り扱う情報の重要性分類及び取扱制限を踏まえて、外部サービスの利用を検討すること。

②情報管理者は、外部サービスで取り扱う情報の重要性分類及び取扱制限を踏まえ、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。

（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

③情報管理者は、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。

④情報管理者は、外部サービスの利用を通じて本市が取り扱う情報の重要性分類等を勘案し、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

⑤情報管理者は、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、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。

⑥情報管理者は、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。

⑦情報管理者は、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。

⑧情報管理者は、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。

（２）外部サービスの利用に係る調達・契約

①情報管理者は、外部サービスを調達する場合は、外部サービス選定時に検討したセキュリティ要件を調達仕様に含めること。

②情報管理者は、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。

（３）外部サービスの利用承認

①情報管理者は、外部サービスを利用する場合には、情報セキュリティ管理者へ外部サービスの利用申請を行うこと。

②情報セキュリティ管理者は、情報管理者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情報セキュリティ管理者及び情報管理者は、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すること。

（４）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情報管理者は、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、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実施し、構築時に実施状況を確認・記録すること。

（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

（５）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情報管理者は、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、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講じること。

（ア）外部サービス利用に必要な教育

（イ）取り扱う資産の管理

（ウ）不正アクセスを防止するためのアクセス制御

（エ）取り扱う情報の機密性保護のための暗号化

（オ）外部サービス内の通信の制御

（カ）設計・設定時の誤りの防止

（キ）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明確にし、職員等に周知すること。

③情報管理者は、前各項の対策に対し、運用・保守時に実施状況を定期的に確認・記録すること。

（６）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情報管理者は、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、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実施し、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。

（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

８．３　外部サービスの利用（重要性分類Ⅰ及び重要性分類Ⅱの情報を取り扱わない場合）

（１）外部サービスの選定

職員等は、利用可能な業務の範囲や管理方法、運用方法等を整理し、外部サービスを選定すること。

（２）外部サービスの利用承認

①情報管理者は、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外部サービスの利用を情報セキュリティ管理者に申請すること。

②情報セキュリティ管理者は、情報管理者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情報セキュリティ管理者及び情報管理者は、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すること。

９　評価・見直し

９．１　監査

（１）実施方法

統括情報管理者は、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関する監査を行わせるために、情報セキュリティ監査責任者を置き、部局等の長をもって充てる。

（２）委託事業者に対する監査

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状況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。

（３）報告

情報セキュリティ監査責任者は、監査結果を取りまとめ、統括情報管理者に報告する。

（４）保管

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、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。

（５）監査結果への対応

統括情報管理者は、監査結果を踏まえ、指摘事項を所管する情報管理者に対し、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。

（６）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

情報セキュリティ責任者は、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。

９．２　自己点検

（１）実施方法

情報管理者は、所管する課等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、定期的に及び必要に応じて自己点検を行わなければならない。

（２）報告及び改善

①情報管理者は、自己点検結果と自己点検結果に基づく改善策を情報セキュリティ管理者に報告しなければならない。

②情報管理者は、自己点検結果に基づき、自己の権限の範囲内で改善を図らなければならない。

③報告を受けた情報セキュリティ管理者は、改善策への対応を確認し、必要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。

（３）自己点検結果の活用

情報セキュリティ管理者は、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。

９．３　情報セキュリティポリシー及び関係規程等の見直し

統括情報管理者は、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、評価及び見直しが必要となる事象が発生した場合には、「小林市情報化推進本部設置要綱（平成 25 年 3 月 29 日告示第 62 号）第６条に基づく情報化推進委員会」に諮り必要な見直しを行い、適正な情報セキュリティポリシー

の維持及び運用に努めなければならない。

改版履歴

版数	改版日	主な内容
第１版	平成 18 年３月 20 日	新規
第２版	平成 24 年 11 月１日	一部改正
第３版	平成 29 年３月 31 日	全部改正
第４版	令和５年３月 31 日	全部改正