小牧市情報セキュリティポリシー

平成１５年１０月２１日策定
平成２０年　３月　４日改定
平成２３年　７月　１日改定
平成２８年　３月　７日改定
平成３１年　２月　４日改定
令和　２年　４月　１日改定
令和　２年　９月　１日改定
令和　４年　９月　１日改定
令和　６年　３月　１日改定

小　　牧　　市

目　　次

小牧市情報セキュリティ基本方針

小牧市情報セキュリティ対策基準

サ　複合機のセキュリティ管理（※注）
シ　特定用途機器のセキュリティ管理（※注）
ス　無線ＬＡＮ及びネットワークの盗聴対策
セ　電子メールのセキュリティ管理
ソ　電子メールの利用制限
タ　ネットワークストレージサービス等の制限
チ　電子署名及び暗号化
ツ　無許可ソフトウエアの導入等の禁止
テ　機器構成の変更の制限
ト　無許可でのネットワーク接続の禁止
ナ　業務以外の目的でのウェブ閲覧の禁止
（２）アクセス制御
ア　アクセス制御
イ　利用者ＩＤの取扱い
ウ　特権を付与されたＩＤの管理等
エ　職員等による外部からのアクセス等の制限
オ　ログイン時の表示等
カ　認証情報の管理
キ　特権による接続時間の制限
（３）情報システムの開発、導入、保守等
ア　情報システムの調達
イ　情報システムの開発
（ア）システム開発における責任者及び作業者の特定
（イ）システム開発における責任者、作業者のＩＤの管理
（ウ）システム開発に用いるハードウエア及びソフトウエアの管理
ウ　情報システムの導入
（ア）開発環境と運用環境の分離及び移行手順の明確化
（イ）テスト
エ　情報システムの開発及び保守に関連する資料等の保管
オ　情報システムにおける入出力データの正確性の確保
カ　情報システムの変更管理
キ　開発及び保守用のソフトウエアの更新等
（４）不正プログラム対策
ア　統括情報セキュリティ責任者の措置事項
イ　情報システム管理者の措置事項
ウ　職員等の遵守事項
（５）不正アクセス対策
ア　統括情報セキュリティ責任者の措置事項
イ　攻撃の予告
ウ　記録の保存
エ　内部からの攻撃

（２）自己点検
ア　実施方法
イ　報告
ウ　自己点検結果の活用
（３）情報セキュリティポリシー及び関係規程等の見直し

小牧市情報セキュリティ基本方針

1　目的

小牧市が管理し、又は保有する情報システムが取り扱う情報には、市民等の個人情報のみならず行政運営上重要な情報など、外部に漏えい等を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。

したがって、これらの情報及び情報を取り扱う情報システムを様々な脅威から防御することは、市民の生命、財産、プライバシー等を守るため、また、小牧市の情報処理業務の安定的な運営のために必要不可欠であり、ひいては、このことが小牧市に対する市民からの信頼の維持向上に寄与するものである。

そのため、小牧市が保有する情報資産の機密性、完全性及び可用性を維持するための情報セキュリティ対策を整備するため小牧市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。）を定める。このうち、情報セキュリティ基本方針については、小牧市の情報セキュリティ対策の基本的な事項を定めるものとする。

2　定義

（1）ネットワーク

小牧市が所管する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（ハードウエア及びソフトウエア）をいう。

（2）情報システム

小牧市が所管するコンピュータ（ハードウエア・ソフトウエア）、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。

（3）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。

（4）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。

（5）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事故やシステム上の欠陥、並びにその原因や結果。庁内外の情報の漏えい（職員等の規定違反に起因するものを含む）や、情報システムに対するサイバー攻撃等をいう。

（6）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。

（7）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。

（8）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。

（9）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。

（１０）ＬＧＷＡＮ接続系

人事給与、財務会計及び文書管理等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）。

（１１）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。

（１２）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。

（１３）無害化通信

インターネットメール本文のテキスト化やパソコン、モバイル端末、携帯電話等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　情報資産への脅威

情報資産に対する脅威として、次の事項を想定し、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）情報資産の無断持出、無許可ソフトウエアの使用等の規定違反、プログラム上の欠陥、誤操作、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

４　対象範囲

（１）行政機関の範囲

本基本方針が適用される行政機関は、小牧市における市長部局、各行政委員会、議会事務局、消防本部、水道事業、病院事業等（以下、「各行政組織」という。）とする。

（２）情報資産の範囲

本基本方針が対象とする情報資産は、小牧市が所掌する次のものとする。

ア　ネットワーク、情報システム、これらに関する設備及び電磁的記録媒体

イ　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。）

ウ　情報セキュリティポリシー、情報セキュリティ実施手順、情報システムの仕

様書及びネットワーク図等の情報システム関連文書

５　情報セキュリティポリシーの位置付けと職員等の遵守義務

情報セキュリティポリシーは、小牧市が所掌する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頂点に位置するものである。

したがって、小牧市が所掌する情報資産に関する業務に携わる全ての職員（他の団体からの出向職員、非常勤職員、会計年度任用職員、再任用職員等を含む。以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持つとともに、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する義務を負うものとする。

６　情報セキュリティ対策

上記３で示した脅威から情報資産を保護するため、次に掲げる情報セキュリティ対策を講じるものとする。

（１）組織体制

小牧市の情報資産について、情報セキュリティ対策を推進及び管理するための全庁的な組織体制を確立するものとする。

（２）情報資産の分類と管理

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

（３）情報システム全体の強靭性の向上

情報システム全体に対し、次の三段階の対策を講じるものとする。

ア　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を制限し、端末への多要素認証の導入により、住民情報の流出を防ぐものとする。

イ　ＬＧＷＡＮ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し、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ものとする。

ウ　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高度な情報セキュリティ対策として、県及び県内市町村のインターネット接続口を集約するあいち情報セキュリティクラウドを導入するものとする。

（４）物理的セキュリティ対策

情報システム、管理区域、ネットワーク接続及び職員等の端末等の管理について、物理的な対策を講じる。

（５）人的セキュリティ対策

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対策

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、セキュリティホールへの迅速な対応等の技術的対策を講じる。

（７）運用面での対策

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、外部委託を行う際のセキュリティ確保等の運用面の対策を講じる。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切に対応するため、緊急時対応計画を策定する。

（８）外部サービスの利用

ア　外部委託する場合には、情報セキュリティ要件を明記した契約を締結し、契約により小牧市の情報資産を扱う業務を委託された事業者（再委託された事業者を含む。以下「委託事業者等」という。）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。

イ　約款によ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。

ウ　ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、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、情報セキュリティポリシーの見直しを行う。

７　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が遵守されていることを検証するため、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。

８　情報セキュリティポリシーの見直しの実施

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を取り巻く状況の変化に対応するために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の見直しを実施する。

９　情報セキュリティ対策基準の策定

小牧市の様々な情報資産について、上記６、７及び８の情報セキュリティ対策を

実施するため、遵守すべき行為及び判断等の基準を具体的に定める情報セキュリティ対策基準を策定するものとする。

１０　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個々の情報資産における情報セキュリティ対策を実施するために、別途、情報セキュリティポリシーに基づく具体的な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小牧市の行政運営に重大な支障を及ぼすおそれのある情報であることから非公開とする。

小牧市情報セキュリティ対策基準

１　組織体制

（１）組織体制

小牧市の情報セキュリティ管理については、次の組織体制で行うものとする。

ア　最高情報セキュリティ責任者（ＣＩＳＯ）

（ア）情報システム部門を統括する小牧市副市長を、最高情報セキュリティ責任者（ＣＩＳＯ）とする。

（イ）最高情報セキュリティ責任者（ＣＩＳＯ）は、小牧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。

イ　最高情報統括責任者（ＣＩＯ）

（ア）最高情報セキュリティ責任者（ＣＩＳＯ）は最高情報統括責任者（ＣＩＯ）を兼務する。

（イ）最高情報統括責任者（ＣＩＯ）は、小牧市における情報通信技術の活用による住民の利便性の向上及び行政運営改善等に関して統括する責任を有する。

ウ　統括情報セキュリティ責任者

（ア）市長公室長を、最高情報セキュリティ責任者（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、最高情報セキュリティ責任者（ＣＩＳＯ）を補佐しなければならない。

（イ）統括情報セキュリティ責任者は、小牧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。

（ウ）統括情報セキュリティ責任者は、小牧市の全てのネットワーク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。

（エ）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、情報システム管理者、情報セキュリティ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。

（オ）統括情報セキュリティ責任者は、小牧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は、最高情報セキュリティ責任者（ＣＩＳＯ）の指示に従い、最高情報セキュリティ責任者（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。

（カ）統括情報セキュリティ責任者は、小牧市の全てのネットワーク、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権限及び責任を有する。

（キ）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、最高情報セキュリティ責任者（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、情報システム管理者、情報セキュリティ管理者、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。

（ク）統括情報セキュリティ責任者は、緊急時には最高情報セキュリティ責任者（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。

エ　情報セキュリティ責任者

（ア）各行政組織の部長あるいは部長に準ずる者を、部長を置かない組織にあっては、次長あるいは次長に準ずる者を、情報セキュリティ責任者とする。

（イ）情報セキュリティ責任者は、当該部署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。

（ウ）情報セキュリティ責任者は、その所管する部署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。

（エ）情報セキュリティ責任者は、その所管する部署における情報システムの情報セキュリティに関する統括的な権限及び責任を有する。

（オ）情報セキュリティ責任者は、その所管する部署等において所有している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並びに職員、非常勤職員及び臨時職員等（以下「職員等」という。）に対する教育、訓練、助言及び指示を行う。

オ　情報システム管理者

（ア）各情報システムの担当課室長等を当該情報システムに関する情報システム管理者とする。

（イ）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。

（ウ）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。

（エ）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・管理を行う。

カ　情報セキュリティ管理者

（ア）各行政組織の課長あるいは課長に準ずる者を情報セキュリティ管理者とする。

（イ）情報セキュリティ管理者は、その所管する組織内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。

（ウ）情報セキュリティ管理者は、その所管する組織内において、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は、ＣＳＩＲＴ、情報セキュリティ責任者及び最高情報セキュリティ

責任者（ＣＩＳＯ）へ直ちに報告を行い、指示を仰がなければならない。

キ　情報システム担当者

情報セキュリティ管理者の指示等に従い、情報システムの開発、設定の変更、運用、見直し等の作業を行う者を情報システム担当者とする。

ク　小牧市情報セキュリティ委員会

小牧市の情報セキュリティ対策を統一的に行うため、小牧市情報セキュリティ委員会において、情報セキュリティポリシー等の情報セキュリティに関する重要な事項を決定する。

ケ　ＣＳＩＲＴ

ＣＳＩＲＴ:Computer Security Incident Response Team の略で、情報セキュリティインシデントが発生した場合に通知を受け取る統一的な窓口として機能し、その状況を他のセキュリティ関連組織と連携して把握・分析して適切なレスポンスを提供する組織。

（ア）ＣＳＩＲＴ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、情報システム管理者、情報セキュリティ管理者及び行政改革課職員で構成し、統括情報セキュリティ責任者をその責任者とする。
（イ）ＣＳＩＲＴは、情報セキュリティインシデントの統一的な窓口の機能を有する組織とする。
（ウ）ＣＳＩＲＴは、情報セキュリティインシデントについて部局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する。
（エ）ＣＳＩＲＴは、最高情報セキュリティ責任者（ＣＩＳＯ）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、その内容を関係部局等に提供する。
（オ）ＣＳＩＲＴは、情報セキュリティインシデントを認知した場合には、最高情報セキュリティ責任者（ＣＩＳＯ）に報告し、必要に応じて関係省庁、県等へ報告する。
（カ）ＣＳＩＲＴは、情報セキュリティインシデントを認知した場合には、情報セキュリティインシデントが発生した部局等と協議の上、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。
（キ）ＣＳＩＲＴは、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う。

なお、上記ク及びケの組織構成員は以下の通りとする。

小牧市情報セキュリティ委員会	最高情報セキュリティ責任者（副市長） 統括情報セキュリティ責任者（市長公室長） 情報セキュリティ責任者（各部長） 事務局（行政改革課）
ＣＳＩＲＴ	統括情報セキュリティ責任者（市長公室長） 情報セキュリティ責任者（該当部長） 情報システム管理者（該当課長） 情報セキュリティ管理者（該当課長） 事務局（行政改革課）

（２）兼務の禁止

ア　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。

イ　監査を受ける者と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。

２　情報資産の分類及び管理

（１）情報資産の分類

対象となる情報資産は、各々の情報資産の機密性、完全性及び可用性を踏まえ、次の重要性分類にしたがって分類する。また、情報資産のライフサイクルに応じて取るべき管理方法を規定する。

重　要　性　分　類
Ⅰ　個人情報及び情報セキュリティ侵害が小牧市の住民の生命、財産、プライバシー等へ重大な影響を及ぼす情報
Ⅱ　公表することを前提としていない情報及び情報セキュリティ侵害が行政事務の執行等に重大な影響を及ぼす情報
Ⅲ　上記以外の情報

※以下、重要性分類Ⅰ、Ⅱの情報資産を「重要な情報資産」という。

（２）情報資産の管理

ア　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（１）の分類に基づき管理しなければならない。

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

ウ　情報資産の入手

（ア）職員等は業務上必要のない情報資産を入手してはならない。
（イ）職員等が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。
（ウ）職員等以外の者が作成した情報資産を入手した者は、（１）の分類に基づき、取り扱わなければならない。
（エ）情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ管理者に判断を仰がなければならない。

エ　情報資産の利用

（ア）情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。
（イ）情報資産を利用する者は、情報資産の分類に応じ、適切な取扱いをしなければならない。
（ウ）情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

オ　情報資産の保管

（ア）情報セキュリティ管理者又は情報システム管理者は、情報資産の分類に従って、情報資産を適切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システム管理者は、情報資産の情報を記録した外部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又は情報システム管理者は、重要度が高い外部電磁的記録媒体や情報システムのバックアップで取得したデータを記録する外部電磁的記録媒体を長期保管する場合は、必要に応じて自然災害を被る可能性が低い地域に保管しなければならない。
（エ）情報セキュリティ管理者又は情報システム管理者は、重要な情報資産の情報を記録した外部電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。
（オ）複数の重要性分類の情報資産を同一場所に保管する場合は最高分類の保管方法に従うこと。

カ　情報の送信

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

キ　情報資産の運搬

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

（イ）重要な情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければならない。

ク　情報資産の提供及び公表

（ア）重要な情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

（イ）重要な情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

（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。

ケ　情報資産の廃棄

（ア）重要な情報資産の廃棄を行う者は、情報を記録している電磁的記録媒体を廃棄する場合、電磁的記録媒体の初期化等、情報を復元できないように処置しなければならない。

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

（ウ）重要な情報資産の廃棄を行う者は、情報セキュリティ管理者の許可を得なければならない。

3　情報システム全体の強靭性の向上

（1）マイナンバー利用事務系

ア　マイナンバー利用事務系と他の領域との分離

（ア）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。

（イ）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。

イ　情報のアクセス及び持ち出しにおける対策

（ア）情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、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。

（イ）情報の持ち出し不可設定

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は、原則として、できないように設定しなければならない。ただし、やむを得ない事情により電磁的記録媒体による端末からの情報を持ち出す場合は、次の手段を実施しなければならない。

a　端末には利用許可された媒体のみ接続可能とすること。

b　データは暗号化し、パスワードを設定すること。

c　利用媒体は、全て管理し利用履歴を残せること。

d　外部業者等へのデータの受け渡しを行う場合は、必ず情報セキュリティ管理者の承認と承認記録を残すこと。

（２）ＬＧＷＡＮ接続系

ア　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。

（ア）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

（イ）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

（ウ）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）インターネット接続系

ア　インターネット接続系においては、通信パケットの監視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。

イ　県及び県内市町村のインターネット接続口を集約するあいち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　物理的セキュリティ対策

（1）情報システム装置（基幹系業務サーバ、その他サーバ等の主要装置）の管理

ア　装置の取付け等

情報システム管理者は、情報システム装置の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない。

イ　二重化

情報システム管理者は、重要な情報資産を格納している情報システム装置を二重化するなどして、情報システムの運用が停止しないようにしなければならない。

ウ　電源

（ア）情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、情報システム装置の電源について、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。

（イ）情報システム管理者は、統括情報セキュリティ責任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情報システム装置を保護するための措置を施さなければならない。

エ　配線

（ア）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、施設管理部門と連携し、配線の損傷等を防止するため、必要な措置を講じなければならない。

（イ）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、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。

（ウ）情報セキュリティ責任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）を他の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。

（エ）情報セキュリティ責任者及び情報システム管理者は、情報システム担当者及び契約により小牧市の情報資産を扱う業務を委託された事業者（再委託された事業者を含む。以下「委託事業者等」という。）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。

オ　外部に設置する情報システム装置

（ア）情報セキュリティ責任者及び情報システム管理者は、市の施設の敷地外に情報システム装置を設置する場合は、最高情報セキュリティ責任者（ＣＩＳＯ）及び統括情報セキュリティ責任者の承認を受けなければならない。

（イ）情報システム管理者は、当該装置への情報セキュリティ対策状況について適宜確認しなければならない。

カ　情報システム装置の点検、修理、廃棄及び撤去

（ア）情報システム管理者は、機器の定期点検を実施しなければならない。

（イ）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委託事業者等に修理させる場合、可能な限り業務上の情報資産が消去され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は、委託事業者等と守秘義務契約を締結しなければならない。

（ウ）情報システム管理者は、機器を廃棄、リース返却等する場合において、機器内部の記憶装置から全ての情報を消去し、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）管理区域

ア　管理区域の条件

（ア）管理区域とは、小牧市の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、管理運用するための部屋や電磁的記録媒体の保管庫をいう。

（イ）情報セキュリティ責任者及び情報システム管理者は、管理区域から外部に通ずるドアに、制御機能、鍵、警報装置等を施し、許可されていない者の立入りを防止する構造にしなければならない。

（ウ）情報セキュリティ責任者及び情報システム管理者は、管理区域内の機器等に、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。

（エ）情報セキュリティ責任者及び情報システム管理者は、管理区域に設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。

イ　管理区域の入退室管理

（ア）情報システム管理者は、管理区域の入退室は許可された者のみとし、指紋認証等の生体認証、ＩＣカード又は入退室管理簿等の記載による入退室管理を行うようにしなければならない。

（イ）情報システム管理者は、職員等及び委託事業者等が管理区域へ入室する場合において、身分証明書あるいは指定された入室許可書を携帯させ、求めにより提示させなければならない。

（ウ）情報システム管理者は、外部からの訪問者が管理区域に入る場合には、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必要に応じて付き添うものとし、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。

（エ）情報システム管理者は、重要な情報資産を扱う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。

ウ　機器等の搬入出

（ア）情報システム管理者は、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、あらかじめ情報システム担当者又は委託事業者等に十分な確認を行わせなければならない。

（イ）情報システム管理者は、管理区域の機器等の搬入出について、情報システム担当者を立ち会わせなければならない。

（３）通信回線及び通信回線装置の管理

ア　情報セキュリティ責任者及び情報システム管理者は、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、適切に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない。

イ　情報セキュリティ責任者及び情報システム管理者は、外部ネットワークとの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。

ウ　情報セキュリティ責任者及び情報システム管理者は、情報資産の送受信に利用する外部ネットワークを別に指定されたものを除き、総合行政ネットワーク（ＬＧＷＡＮ）に集約するよう努めなければならない。

エ　情報セキュリティ責任者及び情報システム管理者は、重要な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、適切な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。

オ　情報セキュリティ責任者及び情報システム管理者は、ネットワークに接続する回線について、伝送途上において破壊、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。

カ　情報セキュリティ責任者及び情報システム管理者は、重要な情報資産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）職員等の利用する端末や電磁的記録媒体等の管理

ア　情報システム管理者及び情報セキュリティ管理者は、盗難防止のため、業務で利用する端末について、業務後は必ず所定の場所に保管又は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、利用後は必ず所定の場所に保管し、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。

イ　情報システム管理者は、端末のディスクデータの暗号化等の機能を必要に応

じて利用しなければならない。

ウ　情報システム管理者は、管理する情報システムへログインする場合、ログインパスワード、生体認証等複数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。

エ　情報システム管理者は、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）を行うよう設定しなければならない。

5　人的セキュリティ対策

（1）職員等の遵守事項

ア　情報セキュリティ対策の遵守義務

（ア）情報セキュリティポリシー等の遵守義務

職員等は、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に定められている事項を遵守しなければならない。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については、速やかに情報セキュリティ管理者等に相談し、指示を仰がなければならない。

（イ）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。

（ウ）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

a　職員等は、端末、電磁的記録媒体、情報資産、ソフトウエア等を所定の場所外に持ち出す場合は情報セキュリティ管理者の許可を得なければならない。

b　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の許可を得なければならない。

（エ）端末等におけるセキュリティ設定変更の禁止

職員等は、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。

（オ）支給以外の端末及び電磁的記録媒体等の利用制限

職員等は、許可なく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、業務上必要な場合においては情報セキュリティ管理者が必要と認めた場合はその限りではない。

（カ）端末及び電磁的記録媒体等の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、端末及び電磁的記録媒体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。

（キ）机上の端末等の管理

職員等は、端末及び電磁的記録媒体等、情報が印刷された文書等について、第三者に使用されること、又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時の端末画面のロック、電磁的記録媒体や文書等を容易に閲覧されない場所に保存する等、適切な措置を講じなければならない。

（ク）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、その後も知り得た情報資産を守秘する義務を負う。

イ　非常勤職員等の雇用及び契約

（ア）情報セキュリティポリシー等の遵守義務

情報セキュリティ管理者は、非常勤職員等の雇用及び契約時には、必ず情報セキュリティポリシーのうち、非常勤職員等が守るべき内容を理解させ、これを実施及び遵守させなければならない。

（イ）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、非常勤職員等の雇用及び契約の際、必要な場合は情報セキュリティポリシーを遵守する旨の同意書に署名を求めるものとする。

（ウ）インターネット接続及びネットワーク等の利用制限

情報セキュリティ管理者は、非常勤職員等に端末による作業を行わせる場合においては、インターネットへの接続及び市が管理するネットワークの使用が不要の場合には、これを利用できないように設定しなければならない。

ウ　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を閲覧できるように掲示しなければならない。

エ　委託事業者等に対する説明

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、保守等を委託事業者等に発注する場合、情報セキュリティポリシー等のうち委託事業者等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。

（２）研修及び訓練

ア　最高情報セキュリティ責任者（ＣＩＳＯ）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するとともに、職員等が情報セキュリティの重要性を認識し、情報セキュリティポリシーを理解し実践するため、定期的に情報セキュリティに関する研修・訓練等を実施しなければならない。また、緊急時に対応するために必要な研修、訓練等を定期的かつ計画的に実施しなければならない。

イ　新規採用の職員等に情報セキュリティポリシーに関する研修を受けさせなければならない。

ウ　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、情報システム管理者、情報セキュリティ管理者、情報システム担当者、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。

エ　職員等は、定められた研修等に参加しなければならない。また、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。

（３）情報セキュリティインシデントの報告・評価

ア　職員等は、情報セキュリティインシデントの発生を認知、または、それらに関する通報及び連絡を住民等外部から受けた場合には、直ちに情報セキュリティ管理者へ報告し指示を受けなければならない。報告を受けた情報セキュリティ管理者は、直ちにＣＳＩＲＴ及び情報セキュリティ責任者に報告し、必要な措置を講じなければならない。

イ　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の評価を行わなければならない。

ウ　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、若しくは報告のあった事故等について市民へ影響が及ぶと判断した場合は、最高情報セキュリティ責任者（ＣＩＳＯ）に速やかに報告しなければならない。

（４）情報セキュリティインシデント原因の究明・記録、再発防止等

ア　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。

イ　ＣＳＩＲＴ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、最高情報セキュリティ責任者（ＣＩＳＯ）に報告しなければならない。

ウ　最高情報セキュリティ責任者（ＣＩＳＯ）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。

（５）パスワードの管理

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。

ア　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ないこと。

イ　パスワードのメモを端末に貼るなど、他者に読み取られやすい状況を作らないこと。

ウ　パスワードは十分な長さとし、文字列を想像しにくいものとすること。

エ　パスワードが流出したおそれのある場合には、パスワードを直ちに変更するとともに、情報セキュリティ管理者に報告すること。

オ　パスワードは定期的に、若しくは当該利用者の交代あるいは要請時に変更し、古いパスワードを再利用しないこと。

カ　複数の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。

キ　仮のパスワードは、最初のログイン時点で変更しなければならない。

ク　端末のパスワード記憶機能を利用しないこと。

ケ　職員等の間でパスワードを共有しないこと。ただし、情報システム管理者が必要と認めた場合はその限りではない。

（6）ＩＣカード等の管理

ア　情報セキュリティ管理者は、その所管する当該情報システムのＩＣカード等を管理しなければならない。

イ　職員等は、個人認証に用いる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）職員等は、ＩＣカード等を紛失した場合には、情報システム管理者及び情報セキュリティ管理者に直ちに通報し、指示を仰がなければならない。また、通報を受けた情報システム管理者は、直ちに当該ＩＣカード等を使用したアクセス等を停止しなければならない。

（イ）職員等は、個人認証に用いるＩＣカード等を、職員等間で共有してはならない。ただし、情報システム管理者が必要と認めた場合はその限りではない。

（7）ＩＤの管理

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。

（ア）自己が管理しているＩＤは、他人に利用させてはならない。

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

6　技術的セキュリティ対策

（1）コンピュータ及びネットワークの管理

ア　フォルダの設定等

（ア）情報システム管理者及び情報セキュリティ管理者は、課室等のフォルダ

及びファイルについて、他課室等のアクセス権を適切に設定しなければならない。

（イ）情報システム管理者及び情報セキュリティ管理者は、住民の個人情報、人事記録等特定の職員しか取り扱えないデータについて、パスワードを付与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が閲覧及び使用できないようにしなければならない。

イ　バックアップの実施

情報セキュリティ責任者及び情報システム管理者は、ファイルサーバ等に記録された情報について二重化対策に関わらず、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。

ウ　他団体との情報システムに関する情報等の交換

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

エ　情報システム管理記録及び作業の確認

（ア）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。

（イ）情報セキュリティ責任者及び情報システム管理者は、その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、窃取、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。

（ウ）情報セキュリティ責任者、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等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。

オ　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情報システム管理者は、ネットワーク構成図及び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や紛失等がないように、適切に管理しなければならない。

カ　アクセス記録の取得等

（ア）情報セキュリティ責任者及び情報システム管理者は、その所管する情報システムに関する各種アクセス記録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。

（イ）情報セキュリティ責任者及び情報システム管理者は、アクセス記録等が窃取、改ざん、誤消去等されないように必要な措置を講じなければならない。

（ウ）情報セキュリティ責任者及び情報システム管理者は、システムから自動

出力したアクセス記録等について、必要に応じ、外部電磁的記録媒体にバックアップしなければならない。

キ　障害記録

情報セキュリティ責任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の障害の報告、情報システムの障害に対する処理結果又は問題等を障害記録として記録し、適切に保存しなければならない。

ク　ネットワークの接続制御、経路制御等

（ア）情報セキュリティ責任者及び情報システム管理者は、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、ルーター等の通信ソフトウエア等を設定しなければならない。

（イ）情報セキュリティ責任者及び情報システム管理者は、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。

ケ　外部の者が利用できる情報システムの分離等

情報システム管理者は、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。

コ　外部ネットワークとの接続制限等

（ア）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、最高情報セキュリティ責任者（ＣＩＳＯ）及び統括情報セキュリティ責任者の承認を得なければならない。

（イ）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、小牧市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。

（ウ）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によりデータの漏えい、破壊、改ざん、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責任管理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。

（エ）統括情報セキュリティ責任者、情報セキュリティ責任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、小牧市の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うえで接続しなければならない。

（オ）情報システム管理者は、接続した外部のネットワークにセキュリティ上の問題が認められ、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、直ち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。

サ　複合機のセキュリティ管理（※注）

（ア）情報セキュリティ責任者及び情報システム管理者は、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、適切なセキュリティ要件を策定しなければならない。

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

（ウ）情報セキュリティ責任者及び情報システム管理者は、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。

（※注）複合機:プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器。

シ　特定用途機器のセキュリティ管理（※注）

（ア）情報セキュリティ責任者及び情報システム管理者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を実施しなければならない。

（※注）特定用途機器：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機器。

ス　無線ＬＡＮ及びネットワークの盗聴対策

（ア）統括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づけなければならない。

（イ）統括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。

セ　電子メールのセキュリティ管理

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

（イ）情報セキュリティ責任者及び情報システム管理者は、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。

（ウ）情報セキュリティ責任者及び情報システム管理者は、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。

（エ）情報セキュリティ責任者及び情報システム管理者は、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なければならない。また、上限を超えた場合には職員等が自らメールを削除しなければならない。
（オ）情報セキュリティ責任者及び情報システム管理者は、情報システムの開発や運用等のため庁舎内に常駐している外部委託事業者等の作業員による電子メールアドレスの利用について、外部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。

ソ　電子メールの利用制限

（ア）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。
（イ）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。
（ウ）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わからないようにしなければならない。
（エ）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。
（オ）職員等は、ウェブで利用できるフリーメールを使用してはならない。
（カ）差出人が不明又は不審なメールを受信した場合は、速やかに情報セキュリティ管理者に報告すること。

タ　ネットワークストレージサービス等の制限

職員等は、ウェブで利用できるネットワークストレージサービス等を、業務に使用してはならない。ただし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管理者が業務上必要と認め、許可した場合はこの限りではない。

チ　電子署名及び暗号化

（ア）職員等は、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、最高情報セキュリティ責任者（ＣＩＳＯ）が定めた電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。
（イ）職員等は、暗号化を行う場合に最高情報セキュリティ責任者（ＣＩＳＯ）が定める以外の方法を用いてはならない。また、最高情報セキュリティ責任者（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。
（ウ）最高情報セキュリティ責任者（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、署名検証者へ安全に提供しなければならない。

ツ　無許可ソフトウエアの導入等の禁止

（ア）職員等は、パソコン等の端末に無断でソフトウエアを導入してはならな

い。

（イ）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及び情報システム管理者の許可を得て、ソフトウエ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又は情報システム管理者は、ソフトウエアのライセンスを管理しなければならない。

（ウ）職員等は、不正にコピーしたソフトウエアを利用してはならない。

テ　機器構成の変更の制限

（ア）職員等は、端末等に対し機器の改造、増設及び交換を行ってはならない。

（イ）職員等は、業務上、端末等に対し機器の改造、増設及び交換を行う必要がある場合には、情報セキュリティ責任者及び情報システム管理者の許可を得なければならない。

ト　無許可でのネットワーク接続の禁止

職員等は、統括情報セキュリティ責任者の許可なく端末等をネットワークに接続してはならない。

ナ　業務以外の目的でのウェブ閲覧の禁止

（ア）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。

（イ）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、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処置を求めなければならない。

（2）アクセス制御

ア　アクセス制御

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。

イ　利用者ＩＤの取扱い

（ア）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、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又は情報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。

ウ　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及び情報システム管理者は、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及び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及び情報システム管理者の特権を代行する者は、情報セキュリティ責任者及び情報セキュリティ管理者が指名し、最高情報セキュリティ責任者（ＣＩＳＯ）が認めたものでなければならない。

（ウ）最高情報セキュリティ責任者（ＣＩＳＯ）は、代行者を認めた場合、速やかに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及び情報システム管理者に通知しなければならない。

（エ）情報セキュリティ責任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、委託事業者等に行わせてはならない。

（オ）情報セキュリティ責任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、職員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。

（カ）情報セキュリティ責任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。

エ　職員等による外部からのアクセス等の制限

（ア）職員等が外部から内部ネットワーク又は情報システムにアクセスする場合は、情報セキュリティ責任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。

（イ）情報セキュリティ責任者及び情報システム管理者は、内部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。

（ウ）情報セキュリティ責任者及び情報システム管理者は、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。

（エ）情報セキュリティ責任者及び情報システム管理者は、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。

（オ）情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者は、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。

（カ）職員等は、外部から持ち帰った端末等を小牧市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なければならない。

（キ）情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者は、公衆通信回線（公衆無線ＬＡＮ等）の庁外通信回線を小牧市のネットワークに接続することは原則として禁止しなければならない。ただし、や

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。

オ　ログイン時の表示等

情報システム管理者は、ログイン時におけるメッセージ及びログイン試行回数の制限、アクセスタイムアウトの設定、ログイン者の表示、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。

カ　認証情報の管理

（ア）情報セキュリティ責任者又は情報システム管理者は、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、これを有効に利用しなければならない。

（イ）情報セキュリティ責任者又は情報システム管理者は、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、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。

（ウ）情報セキュリティ責任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。

キ　特権による接続時間の制限

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。

（3）情報システムの開発、導入、保守等

ア　情報システムの調達

（ア）情報セキュリティ責任者及び情報システム管理者は、情報システム開発、導入、保守等の調達にあたっては、調達仕様書等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。

（イ）情報セキュリティ責任者及び情報システム管理者は、機器及びソフトウエアの調達にあたっては、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。

イ　情報システムの開発

（ア）システム開発における責任者及び作業者の特定

情報システム管理者は、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。

（イ）システム開発における責任者、作業者のＩＤの管理

a　情報システム管理者は、システム開発の責任者及び作業者が使用するＩ

Ｄ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。

b　情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならない。

（ウ）システム開発に用いるハードウエア及びソフトウエアの管理

a　情報システム管理者は、システム開発の責任者及び作業者が使用するハードウエア及びソフトウエアを特定しなければならない。

b　情報システム管理者は、利用を認めたソフトウエア以外のソフトウエアが導入されている場合、当該ソフトウエアをシステムから削除しなければならない。

ウ　情報システムの導入

（ア）開発環境と運用環境の分離及び移行手順の明確化

a　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。

b　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時にその手順を明確にしなければならない。

c　情報システム管理者は、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。

d　情報システム管理者は、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。

（イ）テスト

a　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、既に稼動している情報システムに接続する前に十分なテストを行わなければならない。

b　情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による動作確認を行わなければならない。

c　情報システム管理者は、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。

d　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。

エ　情報システムの開発及び保守に関連する資料等の保管

（ア）情報システム管理者は、情報システムの開発及び保守に関連する資料、システム関連文書等を適切な方法で保管しなければならない。

（イ）情報システム管理者は、テスト結果を一定期間保管しなければならない。

オ　情報システムにおける入出力データの正確性の確保

（ア）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。

（イ）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。

（ウ）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。

カ　情報システムの変更管理

情報システム管理者は、情報システムを変更した場合、情報システム開発事業者（委託事業者）より変更内容の教示を受け、プログラム仕様書等の変更履歴を保管しなければならない。

キ　開発及び保守用のソフトウエアの更新等

情報システム管理者は、開発及び保守用のソフトウエ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。

（4）不正プログラム対策

ア　統括情報セキュリティ責任者の措置事項

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、次の事項を措置しなければならない。

（ア）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、不正プログラムの情報システムへの侵入を防止しなければならない。

（イ）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。

（ウ）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。

（エ）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エアを常駐させなければならない。

（オ）不正プログラム対策ソフトウエアは、常に最新の状態に保たなければならない。

（カ）不正プログラム対策ソフトウエ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。

（キ）不正プログラム対策ソフトウエアによるフルチェックを定期的に実施し、実行を途中で止めないこと。

（ク）業務で利用するソフトウエアは、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エアを利用してはならない。ただし、業務システムの利用環境等で、サポートが終了したソフトウエアを利用する必要がある場合は、直ちにセキュリティを確保する措置を講じると伴に、速やかにパッチの適用やバージョンアップができるよう努めなければならない。

イ　情報システム管理者の措置事項

情報システム管理者は、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。

（ア）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エアを常駐させなければならない。

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

（ウ）不正プログラム対策ソフトウエ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。

（エ）インターネットへの接続の有無に関わらず、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感染を防止するために、情報セキュリティ管理者が許可した場合を除き、小牧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エアを導入し、定期的に当該ソフトウエ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。

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

ウ　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。

（ア）パソコン等の端末において、不正プログラム対策ソフトウエアが導入されている場合は、当該ソフトウエアの設定を変更してはならない。

（イ）外部からデータ又はソフトウエ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エアによるチェックを行わなければならない。

（ウ）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。

（エ）端末に対して、不正プログラム対策ソフトウエ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。

（オ）事業者等から、入手したデータをＬＧＷＡＮ接続系又はマイナンバー利用事務系に取込む場合は、不正プログラム対策ソフトウエアでのチェック及びファイル無害化を実施しなければならない。

（カ）情報システム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。

（キ）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は、以下の対応を行わなければならない。

a　パソコンの場合

ＬＡＮケーブル等の取り外し等を行い、当該端末をネットワークから即時切断しなければならない。

b　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。

（５）不正アクセス対策

ア　統括情報セキュリティ責任者の措置事項

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、次の事項を措置しなければならない。

（ア）使用されていないポートを閉鎖しなければならない。

（イ）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。

（ウ）不正アクセスによるウェブページの改ざんに対応するため、改ざんの有無やデータの書換えを検出するように設定しなければならない。改ざん等を検知した場合は、速やかに情報セキュリティ責任者及び情報システム管理者に対策を講じるよう、指示しなければならない。

（エ）統括情報セキュリティ責任者は、ＣＳＩＲＴと連携し、監視、通知、外部連絡窓口及び適切な対応などを実施できる体制並びに連絡網を構築しなければならない。

イ　攻撃の予告

最高情報セキュリティ責任者（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、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、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。

ウ　記録の保存

最高情報セキュリティ責任者（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。

エ　内部からの攻撃

統括情報セキュリティ責任者、情報セキュリティ責任者及び情報システム管理者は、職員等及び委託事業者等が使用しているパソコン等の端末から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。

オ　職員等による不正アクセス

統括情報セキュリティ責任者、情報セキュリティ責任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。

カ　サービス不能攻撃

統括情報セキュリティ責任者、情報セキュリティ責任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。

キ　標的型攻撃

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

（6）セキュリティ情報の収集

ア　情報セキュリティに関する情報の収集、共有及びソフトウエアの更新等

統括情報セキュリティ責任者、情報セキュリティ責任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、関係者間で共有しなければならない。また、緊急度に応じて、ソフトウエア更新等の対策を実施しなければならない。更に、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、セキュリティ侵害等を未然に防止するための対策を講じなければならない。

イ　不正プログラム等のセキュリティ情報の収集及び周知

統括情報セキュリティ責任者及び情報セキュリティ管理者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対策方法について、職員等に周知しなければならない。

7　運用

（1）情報システムの監視

ア　情報セキュリティ責任者及び情報システム管理者は、セキュリティに関する侵害を検知するため、常に情報システムの監視に努めなければならない。

イ　情報セキュリティ責任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について常時監視しなければならない。

ウ　情報セキュリティ責任者及び情報システム管理者は、重要なアクセス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同期ができる措置を

講じなければならない。

（２）情報セキュリティポリシーの遵守状況の確認

ア　遵守状況の確認及び対処

（ア）情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーが遵守されているかどうか確認を行い、問題が発生していた場合には速やかに最高情報セキュリティ責任者（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。

（イ）報告を受けた最高情報セキュリティ責任者（ＣＩＳＯ）は、発生した問題に適切に対処しなければならない。

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

イ　端末及び電磁的記録媒体等の利用状況調査

最高情報セキュリティ責任者（ＣＩＳＯ）及び最高情報セキュリティ責任者（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。

ウ　職員等の報告義務

（ア）職員等は、情報セキュリティポリシーの違反を発見した場合は、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しなければならない。

（イ）情報セキュリティ責任者は、問題や違反が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、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。

（３）緊急時対応計画

最高情報セキュリティ責任者（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、復旧等の必要な措置を迅速かつ円滑に実施し、再発防止の措置を講じるため緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適切に対処しなければならない。

緊急時対応計画には次の事項を明記すること。

- 関係者の連絡先
- 発生した事案に係る報告すべき事項
- 侵害への対処

・ 再発防止の措置

ア　業務継続計画との整合性確保

最高情報セキュリティ責任者（ＣＩＳＯ）は、情報セキュリティポリシーについて、小牧市で策定した業務継続計画との整合性を確保しなければならない。

イ　緊急時対応計画の見直し

情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画を見直さなければならない。

（4）委託事業者の利用

ア　委託事業者の選定基準

（ア）情報セキュリティ管理者は、委託事業者の選定に当たり、委託事業者との間で必要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。

（イ）情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、事業者の選定に努めなければならない。

（ウ）情報セキュリティ管理者は、クラウドサービスを利用する場合は、情報資産の重要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。

イ　委託による運用契約

情報システムの運用等を委託する場合は、委託に関する責任を有する部署を明確にするとともに、委託事業者等に対し、次の情報セキュリティ要件のうち必要事項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
・ 委託先の責任者、委託内容、作業者、作業場所の特定
・ 業務上知り得た情報の守秘義務
・ 権利及び義務の譲渡禁止
・ 再委託に関する制限事項の遵守
・ 提供された情報の複写及び複製の禁止
・ 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
・ 委託業務終了時の情報資産の返還、廃棄等の義務
・ 小牧市に対する委託業務の定期報告及び緊急時報告義務
・ 小牧市による監査、検査に応じる義務
・ 小牧市による情報セキュリティインシデント発生時等の公表
・ 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）

・ 提供されるサービスレベルの保証
・ 委託事業者等にアクセスを許可する情報の種類と範囲、アクセス方法
・ 委託事業者等の従業員に対する監督・教育

ウ　確認、措置等

情報セキュリティ管理者は、委託事業者等が委託内容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、上記（4） 委託事業者の利用　イ　委託による運用契約で示した契約に基づき措置しなければならない。また、その内容を情報セキュリティ責任者に報告するとともに、その重要度に応じて統括情報セキュリティ責任者、最高情報セキュリティ責任者（ＣＩＳＯ）に報告しなければならない。

エ　再委託について

再委託は原則禁止する。但し、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取られており、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。

再委託等をおこなう場合、情報セキュリティ管理者は、委託事業者等に対して、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、報告をさせるとともに、必要に応じて、上記（4） 委託事業者の利用　　イ　委託による運用契約で示した契約に基づき措置しなければならない。また、その内容を情報セキュリティ責任者に報告するとともに、その重要度に応じて統括情報セキュリティ責任者、最高情報セキュリティ責任者（ＣＩＳＯ）に報告しなければならない。

（5）約款による外部サービスの利用

ア　約款による外部サービスの利用に係る規定の整備

情報セキュリティ管理者は、以下を含む約款による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。また、当該サービスの利用において、重要な情報資産が取り扱われないように規定しなければならない。

（ア）約款によるサービスを利用して良い範囲
（イ）業務により利用する約款による外部サービス
（ウ）利用手続及び運用手順

イ　約款による外部サービスの利用における対策の実施

職員等は、利用するサービスの約款、その他提供条件から、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約款による外部サービスの利用を申請し、適正な措置を講じた上で利用しなければならない。

（6）ソーシャルメディアサービスの利用

ア　情報セキュリティ管理者は、小牧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、本市の自己管理ウェブ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。

イ　重要な情報資産はソーシャルメディアサービスで発信してはならない。

ウ　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。

エ　アカウント乗っ取りを確認した場合には、アカウントを一時停止にする等の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。

（7）例外措置

ア　例外措置の許可

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、最高情報セキュリティ責任者（ＣＩＳＯ）の許可を得て、例外措置を取ることができる。

イ　緊急時の例外措置

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、事後速やかに最高情報セキュリティ責任者（ＣＩＳＯ）に報告しなければならない。

ウ　例外措置の申請書の管理

最高情報セキュリティ責任者（ＣＩＳＯ）は、例外措置の申請書及び審査結果を適切に保管しなければならない。

（8）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、次の法令等のほか関係法令を遵守し、これに従わなければならない。

・ 地方公務員法（昭和２５年法律第２６１号）

・ 著作権法（昭和４５年法律第４８号）
・ 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
・ 個人情報の保護に関する法律（平成１５年法律第５７号）
・ 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）
・ サイバーセキュリティ基本法（平成２８年法律第３１号）
・ 小牧市個人番号の利用に関する条例（平成２７年条例第３２号）

（9）情報セキュリティポリシーに違反した場合の対応

ア　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。

（ア） 統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該職員等が所属する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。

（イ） 情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括情報セキュリティ責任者及び当該職員等が所属する課室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。

（ウ） 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、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あるいは剥奪することができる。その後速やかに、統括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最高情報セキュリティ責任者（ＣＩＳＯ）、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通知しなければならない。

イ　罰則等

情報セキュリティポリシーに違反した職員等及び管理監督者は、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の定めにより懲戒処分等の対象となる。

委託業者等が情報セキュリティポリシーに違反した場合の対応については、予め契約に定めておくものとする。

8　評価及び見直し

（1）監査

ア　実施方法

小牧市情報セキュリティ監査実施要綱で定める情報セキュリティ監査統括責任者（以下、「監査統括責任者」という。）は、ネットワーク及び情報システム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、必要に応じて監査を行わなければならない。

イ　監査実施計画の立案及び実施への協力

（ア）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、必要に応じて情報セキュリティ委員会の承認を得なければならない。

（イ）被監査部門は、監査の実施に協力しなければならない。

ウ　委託事業者等に対する監査

委託事業者等に委託している場合、情報セキュリティ責任者及び情報セキュリティ管理者は委託事業者等に対し、情報セキュリティポリシーの遵守について、監査を必要に応じて行わなければならない。

エ　報告

監査統括責任者は、監査結果を取りまとめ、情報セキュリティ委員会に報告するものとする。

オ　保管

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。

カ　監査結果への対応

監査統括責任者は、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。

キ　情報セキュリティポリシーの見直し等への活用

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の見直し、その他情報セキュリティ対策に活用しなければならない。

（2）自己点検

ア　実施方法

（ア）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、必要に応じ自己点検を実施しなければならない。

（イ）情報セキュリティ責任者及び情報セキュリティ管理者は、所管する部署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、必要に応じ自己点検を実施しなければならない。

イ　報告

情報セキュリティ責任者は自己点検結果を取りまとめ、情報セキュリティ委

員会に報告するものとする。

ウ　自己点検結果の活用

（ア）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。

（イ）情報セキュリティ委員会は、この点検結果を情報セキュリティポリシーの見直し、その他情報セキュリティ対策に活用しなければならない。

（3）情報セキュリティポリシー及び関係規程等の見直し

情報セキュリティ委員会は、情報セキュリティポリシー及び関係規程等について新たに対策を必要とする問題点や重大な変化が発生した場合及び監査や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、必要があると認めた場合、その見直しを行うものとする。

策定及び改定履歴

平成１５年１０月２１日策定
平成２０年　３月　４日全面改定
平成２３年　７月　１日改定
平成２８年　３月　７日改定
平成３１年　２月　４日改定
令和　２年　４月　１日改定
令和　２年　９月　１日改定
令和　４年　９月　１日改定
令和　６年　３月　１日改定