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。

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（ハードウェア及びソフトウェア）をいう。

（2）情報システム

小牧市が所管するコンピュータ（ハードウェア・ソフトウェア）、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、無許可ソフトウェ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しなければならない。

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。

（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。

（２）情報資産の分類と管理

情報資産を機密性に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

（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。

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。

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。

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。

（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）業務委託とクラウドサービスの利用

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（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。

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「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。

なお、情報セキュリティ対策基準は、公にすることによりサイバー攻撃を受けるリスクがあることから非公開とする。

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。

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。