情報セキュリティ基本方針

第5版

笛吹市

（改訂履歴）

版数	章・頁	改訂年月日	改訂内容	承認
第1版	―	平成18年4月1日	初版発行	
第2版	―	平成22年4月1日	情報セキュリティガイドラインの改定等に伴う改定	
第3版	―	平成28年5月24日	情報セキュリティガイドラインの改定等に伴う改定	
第4版	―	令和元年5月9日	情報セキュリティガイドラインの改定等に伴う改定	
第5版	―	令和4年4月1日	情報セキュリティガイドラインの改定等に伴う改定	

笛吹市情報セキュリティ基本方針

第1章　総則

（目的）

第1条　笛吹市情報セキュリティ基本方針（以下「基本方針」という。）は、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基本的な方針について総合的かつ体系的に定めることにより、市民の財産及び個人情報等の保護並びに安定的な行政事務の運営を図ることを目的とする。

（定義）

第2条　基本方針において、次の各号に掲げる用語の意義は、当該各号の定めるところによる。

(1) 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。

(2) 機密性　アクセスを認可された者だけが情報にアクセスできることを確実にすること。

(3) 完全性　情報が破壊され、改ざんされ、又は消去されていない状態を確実にすること。

(4) 可用性　アクセスを認可された利用者が、必要なときに、情報にアクセスできる状態を確実にすること。

(5) ネットワーク　情報通信を行うために用いられる機器及び回線をいう。

(6) 記録媒体　電子計算機に使用される電子的方式、磁気的方式又は光学的方式その他人の知覚によっては認識することができない方式で作られたデータを記録するための機器媒体をいう。

(7) 情報システム　コンピュータ、ネットワーク及び記録媒体等で構成され、情報処理を行う仕組みをいう。

(8) 情報　職員等が職務上作成し、又は取得した文書、データ及びファイル等のうち電磁的に記録されたもの及びこれらを印刷した紙等をいう。

(9) 情報資産　情報、情報システム及び記録媒体の総称をいう。

(10) 職員等　市長、副市長、教育長、一般職の職員（臨時的任用職員、再任用職員、会計年度任用職員を含む）の総称をいう。

(11) 個人情報等　笛吹市個人情報保護条例（平成16年笛吹市条例第11号）第2条第2号に規定する個人情報及び第5号に規定する特定個人情報をいう。

(12) LGWAN　地方公共団体を相互に接続する行政専用のネットワーク

(13) 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、税及び災害対策等において、保有している個人情報の検索や管理のためにマイナンバーを利用する特定の事務のこと）又は戸籍事務等に関わる情報システム及びデータ（以下「マイナンバー利用事務系」という。）

(14) LGWAN接続系　LGWANへの接続が可能なネットワークで、業務に利用する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。）

(15) 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。

(16) 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。

(17) 無害化通信　インターネットメール本文のテキスト化や添付ファイルの削除等により、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。

(18) 情報セキュリティポリシー　基本方針及び笛吹市情報セキュリティ対策基準(以下「対策基準」という。)をいう。

(対象とする脅威)

第 3 条　情報資産に対する脅威として、以下の脅威を想定し、市の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、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、改ざん及び消去、重要情報の詐取並びに内部不正等

(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、設計及び開発の不備、プログラム上の欠陥、操作及び設定のミス、メンテナンスの不備、内部及び外部監査機能の不備、委託事業者の管理の不備、マネジメントの欠陥並びに機器故障等の非意図的要因による情報資産の漏えい、破壊及び消去等

(3) 地震、落雷、火災及び水害等の災害によるサービス及び業務の停止等

(4) 大規模かつ広範囲に及ぶ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、通信の途絶及び水道供給の途絶等のインフラの障害からの波及等

(行政機関の範囲)

第 4 条　基本方針の適用となる行政機関は、市長部局、消防本部、教育委員会、農業委員会、監査委員、選挙管理委員会、公平委員会、固定資産評価審査委員会及び議会とする。

第 2 章　基本的な考え方

(職員等の責務)

第 5 条　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、実施手順及び関係法令等を遵守しなければならない。

(組織及び体制)

第 6 条　市は、第 3 条の脅威から情報資産を保護するために、全庁的な組織及び体制のもとに、情報セキュリティ対策を講じる。

(情報資産の分類及び管理)

第 7 条　市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

(情報システム全体の強靭性の向上)

第 8 条　情報セキュリティの強化を目的とし、業務の効率性及び利便性の観点から、市の情報システム全体に対し、次の各号に掲げる対策を講じる。

(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。

(2) 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、無害化通信を講じる。

(3) インターネット接続系においては、県及び市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行い、不正通信の監視機能を強化する等の高度な情報セキュリティ対策を講じる。

（物理的セキュリティ）

第 9 条　市は、不正な立入り、損傷及び妨害から情報資産を適切に保護するため、物理的な対策を講じる。

（人的セキュリティ）

第 10 条　市は、情報セキュリティに関する役割及び責任を明確化し、職員等に情報セキュリティポリシー及び実施手順の内容を周知徹底するため、教育及び研修等の人的な対策を講じる。

（技術的セキュリティ）

第 11 条　市は、情報資産を不正なアクセス等から適切に保護するため、アクセス制御、不正プログラム対策及び不正アクセス対策等の技術的対策を講じる。

（運用）

第 12 条　市は、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及び外部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。

2　市は、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、緊急時対応計画を定めるものとする。

（外部サービスの利用）

第 13 条　外部に業務を委託する場合には、委託事業者を選定し、情報セキュリティに関する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く措置を講じる。

2　約款による外部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。

3　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た上で、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。

（対策基準の策定）

第 14 条　基本方針に基づき、情報セキュリティ対策を実施するために必要となる統一的な基準を定める対策基準を策定する。

（実施手順の策定）

第 15 条　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る笛吹市情報セキュリティ実施手順（以下「実施手順」という。）を策定する。

2　実施手順は、公にすることにより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。

（情報セキュリティ監査及び自己点検の実施）

第 16 条　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。

（情報セキュリティポリシーの見直し）

第 17 条　情報セキュリティ監査及び自己点検の結果により、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及び実施手順の見直しを行う。

（違反への対応）

第 18 条　職員等が情報セキュリティポリシーに違反した場合は、地方公務員法等に基づいた処分の対象とする。