袋井市情報セキュリティポリシー

袋井市

目次

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、部外に漏洩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おり、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り、本市が管理しているすべ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な前提条件となる。

本基本方針は、本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、本市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

２　定義

（１） 電子計算機

ハードウェア及びソフトウェアで構成するコンピュータ及び周辺機器をいう。

（２） 記録媒体

電子計算機に使用される磁気ディスク、磁気テープ、光ディスク等をいう。

（３） 電算室

電子計算機を運用管理する目的で設置している部屋をいう。

（４）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。

（５）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。

（６）データ

電子計算機処理に係る入出力帳票、磁気テープ、磁気ディスク、光ディスクその他の記録媒体に記録されている情報又は通信回線により送信される情報をいう。

（７）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。

（８）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。

（9）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。

（10）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。

（11）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。

（12）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。

（13）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。）。

（14）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。

（15）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。

（16）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及び構成

情報セキュリティポリシーは、本市が保有する情報資産に関する情報セキュリティ対策について、総合的かつ体系的に取りまとめた情報セキュリティ対策の基本となるものであり、情報セキュリティ対策基本方針及び情報セキュリティ対策基準から構成される。

情報セキュリティ対策基準は、情報セキュリティ基本方針に基づき、情報セキュリティ対策等を実施するために最低限必要な水準として、職員、再任用職員、任期付職員、教員、臨時的任用職員、会計年度任用職員、特別職非常勤職員、労働者派遣契約等により本市業務に従事する者（以下「職

員等」という。）が遵守すべき事項及び判断基準をまとめたものである。

また、情報セキュリティポリシーに基づき、情報システムごとに、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。

ポリシーの構成		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、すべ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。

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、外部委託管理の不備、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

5　適用範囲

（1）組織の範囲

袋井市部設置条例（平成17年袋井市条例第９号）第１条に規定する部、袋井市支所設置条例第２条に規定する課、袋井市森町広域行政組合事務局、出納室、教育委員会、選挙管理委員会事務局、監査委員事務局、議会事務局をいう。

（2）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

ア　ネットワーク及び情報システム並びにこれらに関する施設・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システム関連文書

情報資産の種類	情報資産の例
ネットワーク	通信回線、ルータ等の通信機器等
情報システム	サーバ、パソコン、モバイル端末、汎用機、複合機、オペレーションシステム、ソフトウェア等
ネットワーク・情報システムに関する施設・設備	コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル等
電磁的記録媒体	サーバ装置、端末、通信回線装置等に内蔵される内臓電磁的記録媒体、USB メモリ、外付けハードディスクドライブ、DVD-R、磁気テープ等の外部電磁的記録媒体等
ネットワーク及び情報システムで取り扱う情報	ネットワーク、情報システムで取り扱うデータ等（これらを印刷した文書を含む。）
システム関連文書	システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等

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つとともに、業務の遂行にあたって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を遵守しなければならない。

7　情報セキュリティ対策

上記４の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、適切に情報セキュリティ対策を推進・管理するための体制を確立する。必要な体制、役割、権限等については情報セキュリティ対策基準にて定める。

（２）情報資産の分類と管理

本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講ずる。

（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、情報資産の分類に応じたセキュリティ対策を講じるとともに、次の対策も併せて講じる。

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。

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する。なお、両システム間で通信する場合には、特定の通信のみに限定し、原則として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の高度な情報セキュリティを実施する。高度な情報セキュリティ対策として、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入を実施する。

（4）物理的セキュリティ対策

電算室への入退室、サーバ等の管理、通信回線及び端末等への物理的な対策を講ずる。

（5）人的セキュリティ対策

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、十分な研修・訓練及び啓発を行なう等の人的な対策を講ずる。

（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、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。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（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、利用にかか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、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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、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

上記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。

なお、情報セキュリティ対策基準は、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。

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。