大府市情報セキュリティ基本方針

1　目的

大府市の各情報システムが取り扱う情報には、市民の個人情報のみならず行政運営上重要な情報など、部外に漏洩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。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、市民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが大府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、大府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、情報セキュリティ対策の基本方針を定めることを目的とする。

2　定義

（1）情報セキュリティポリシー

本方針及び大府市情報セキュリティ対策基準をいう。

（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

ネットワーク、ハードウェア、ソフトウェア及び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）マイナンバー利用事務系

個人番号利用事務又は戸籍事務等に関わる情報資産をいう。

（6）ＬGWAN接続系

ＬGWANに接続された情報資産をいう（マイナンバー利用事務系を除く。）。

（7）インターネット接続系

インターネットメール、Ｗｅｂサイト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資産をいう。

（8）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。

（9）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、コンピュータウィルス等の不正プログラムの付着がない等、安全が確保された通信をいう。

３　適用範囲

（１）行政機関の範囲

本基本方針が適用される行政機関は、市長、選挙管理委員会、公平委員会、監査委員、農業委員会、固定資産評価審査委員会、消防長、公営企業及び議会事務局並びに教育委員会（各教育機関（事務室及び職員室を除く。）は対象外とする。）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、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

４　職員等の遵守義務

職員等は、情報セキュリティポリシー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を遵守する義務を負うものとする。

５　情報セキュリティ管理体制

大府市の情報資産について、幹部が率先して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ものとする。

６　情報資産の分類

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。

７　情報資産への脅威

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、業務委託管理の不備、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

８　情報セキュリティ対策

上記７で示し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ずるものとする。

（１）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出来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、市民の個人情報の流出を防ぐ。

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、無害化通信を行う。

ウ　インターネット接続系においては、自治体情報セキュリティクラウドを導入する等、不正通信の監視機能の強化等の高度なセキュリティ対策を行う。

（２）物理的セキュリティ対策

サーバー等、情報システムを設置する施設、通信回線等及び職員等のパソコン等の管理について、物理的な対策を講ずる。

（３）人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、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ずる。

（４）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、不正プログラム対応、ネットワーク管理等の技術的な対策を講ずる。

（５）運用

システム開発等の業務委託、ネットワークの監視、情報セキュリティポリシー遵守状況の確認等の運用面の対策を講ずる。また、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

（６）外部サービスの利用

ソーシャルメディア及びクラウドサービスの利用にあたり、情報漏洩、不正利用等のリスクに留意し、サービスの特性に応じた運用手順を作成し、必要なセキュリティ対策を講ずる。

９　情報セキュリティ対策基準の策定

上記８に規定する対策等を実施するために、具体的な遵守事項、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。

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、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、情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより大府市の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

１１　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、定期的に情報セキュリティ監査及び自己点検を実施する。

１２　評価及び見直しの実施

情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、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、情報セキュリティポリシーの見直しを実施する。

第１版　平成15年４月30日
第２版　平成23年４月１日
第３版　平成31年４月１日
第４版　令和４年４月１日
第５版　令和７年12月１日