大垣市情報セキュリティポリシー

版数	施行日
第1版	平成15年 8月25日
第2版	平成18年 4月 1日
第3版	平成20年 4月 1日
第4版	平成22年 5月21日
第5版	平成26年 3月20日
第6版	平成28年 1月 1日
第7版	平成31年 1月 1日
第8版	令和 3年 6月 1日
第9版	令和 4年 6月 1日
第10版	令和 4年 6月21日
第11版	令和 5年 4月 1日
第12版	令和 6年 4月 1日

大垣市

はじめに

本市では、平成15年8月25日に「大垣市情報セキュリティポリシー」を策定し、この方針に基づいた運用をすることで、情報資産を様々な脅威から防御し、市民の財産、プライバシー等を守り、また、事務の安定的な運営に努めてきました。

前回改正時（令和3年6月）以降、総務省では、「デジタル庁設置法」、「デジタル社会形成基本法」、「地方公共団体情報システムの標準化に関する法律」等のデジタル改革関連法が成立・施行され、国及び地方のデジタル・トランスフォーメーション（DX）が推し進められています。

また、これらの地方公共団体におけるデジタル化の動向や令和3年7月の政府機関のサイバーセキュリティ対策のための統一基準の改定を踏まえて、令和4年3月25日には、「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定が行われました。

このため、本市では、「大垣市情報セキュリティポリシー」を改定し、業務委託・外部サービス利用時の情報資産の取扱いや、多様な働き方を前提とした情報セキュリティ対策などの規定を追加しました。

さらに、今後も、情報通信技術の進展に伴う急速な状況変化に柔軟に対応すべく、同ポリシーの不断の見直しを実施していきます。

本市の業務に携わるすべての職員、非常勤職員、会計年度任用職員及び再任用職員（以下、「職員等」という。）は、情報資産の厳格な管理・運用を徹底することで、市民が安心して行政サービスを利用できるようにするとともに、継続的かつ安定的に行政事務の執行を確保するために、日常業務において情報セキュリティの重要性を認識し、本情報セキュリティポリシーを遵守しなければなりません。

目　　次

第１章　情報セキュリティ基本方針

第１章　情報セキュリティ基本方針

１　目　　的

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

⑴　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。

⑵　情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

⑶　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。

⑷　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。

⑸　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。

⑹　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。

⑺　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。

⑻　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。

⑼　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。）。

⑽　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。

⑾　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。

⑿　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。

⒀　情報セキュリティインシデント

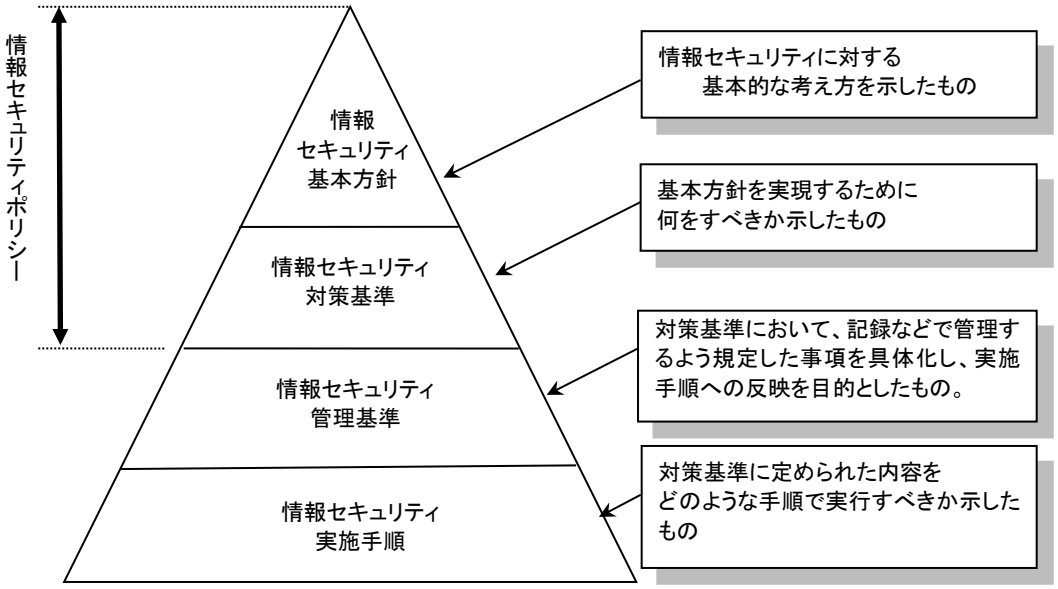
情報資産の管理上の脅威となる確率が高い現象や事案をいう。具体的には、ウイルス感染、第三者からの不正アクセスによる侵害、情報システム上の欠陥や誤動作による情報漏えい及び職員等による情報紛失等がある。

３　情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、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。

４　情報セキュリティポリシーの構成

情報セキュリティポリシーの構成は、一定の普遍性を備えた「情報セキュリティ基本方針」と、情報資産を取り巻く状況の変化に適切に対応する「情報セキュリティ対策基準」の二階層に分けて策定する。



５　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。

⑴　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

⑵　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、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

⑶　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

⑷　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

⑸　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

６　適用範囲

⑴　行政機関の範囲

本基本方針が適用される行政機関は、市長部局（市民病院は事務局に限る。）、選挙管理委員会事務局、農業委員会事務局、議会事務局、監査委員事務局及び教育委員会事務局とする。

⑵　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。

①　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記録媒体

②　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。）

③　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　職員等が職務上作成し、又は取得した文書等

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、オペレーティングシステム※、ソフトウェア等
ネットワーク及び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
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蔵記録媒体、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記録媒体等
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
職員等が職務上作成し、又は取得した文書等	申請書類、一覧のリスト、図画、写真等

７　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ち、業務の遂行に当たって情報セキュリティポリシー、情報セキュリティ管理基準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。

８　情報セキュリティ対策

前記５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。

⑴　組織体制

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

⑵　情報資産の分類と管理

本市の保有する情報資産をその重要度に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

⑶　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、次の三段階の対策を講じる。

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、住民情報の漏えいを防ぐ。

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通信経路の分割をする。

なお、両システム間で通信する場合には、無害化通信を実施する。

③ インターネット接続系においては、不正通信監視機能の強化等の高度な情報セキュリティ対策を実施する。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実施する。

⑷　物理的セキュリティ

サーバ、サーバ室、通信回線等及び職員等のパソコン等の管理について、物理的な対策を講じる。

⑸　人的セキュリティ

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、十分な教育及び啓発を行う等の人的な対策を講じる。

⑹　技術的セキュリティ

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。

⑺　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、業務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（インシデント）対応計画を策定する。

⑻　業務委託と外部サービスの利用

業務委託を行う場合又は指定管理者に実施させる場合には、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※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。

⑼　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な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の見直しを行う。

９　情報セキュリティ対策基準の策定

前記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。

10　情報セキュリティ管理基準の策定

情報セキュリティ対策基準において、記録などで管理するよう規定した事項を具体化し、情報セキュリティ実施手順へ反映させることを目的として情報セキュリティ管理基準を策定する。

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、ネットワーク及び情報システム、個人番号及び特定個人情報並びにそれらに準ずるものの取扱いにおいて、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。

12　公開の範囲

情報セキュリティ対策基準、情報セキュリティ管理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。

13　法令遵守

情報セキュリティに関する法令・ガイドライン等を遵守する。

14　問い合わせ先

情報企画課　電話　０５８４－４７－８２４９

大垣市情報セキュリティポリシー

令和６年４月

発行　岐阜県大垣市企画部
編集　情報企画課
岐阜県大垣市丸の内2丁目29番地
電話　(0584)81-4111　内線2287