佐賀市情報セキュリティポリシー

佐賀市

令和５年９月

改 定 履 歴

No	年 月	主な改定内容
1	平成16 年3 月	初版策定
2	平成19 年8 月	名称変更、項目追加による一部改定
3	平成20 年4 月	名称変更による一部改定
4	平成30 年6 月	全面改定 ・セキュリティポリシーの適用範囲の明確化 ・特定個人情報の取扱いに関する管理規程の策定を明記 ・統括情報セキュリティ責任者の設置 ・情報セキュリティインシデント対応実施手順の策定に伴うCSIRT（情報セキュリティ対応チーム：Computer Security Incident Response Team）の設置 ・ソーシャルメディアサービスを利用する際のルールの明記 等
5	令和元年7 月	項目追加、内容整備による一部改定 ・情報システム全体の強靭性向上（強靭化）を講じることについて明記 ・マイナンバー利用事務系では、多要素認証を実施しなければならないことについて明記 ・退庁時には、特段の理由がない限りパソコンの電源を切らなければならないことについて明記 ・認証情報を適正に管理し、認証情報の不正利用の防止をしなければならないことについて明記 ・情報セキュリティインシデントへの対処として、CSIRT の役割について明記 等
6	令和3 年4 月	名称変更、項目追加による一部改定 ・情報資産の廃棄に関して、情報を復元できないよう処置したうえで廃棄するよう文言を修正 ・システムに保存するデータの重要度に応じ、適切に取り扱うよう契約書に記載する旨を明記 ・クラウドサービスの利用に関して明記 等
7	令和5 年1 月	内容整備による一部改定 ・情報資産の廃棄等に関して、リース物件の返却も含める旨の文言を追記 ・LGWANを経由して、インターネット等とマイナンバー利用事務系ネットワークとの双方向通信でのデータの移送を可能とする旨の記載に修正 ・フリーメールの利用に関する文言を修正 等
8	令和5 年4月	名称、遵守法令変更による一部改定
9	令和5 年9月	項目追加、内容整備による一部改定 ・業務以外の目的でのウェブ閲覧の禁止及びWeb会議サービス利用時の対策にかかる文言等を追記 ・外部サービスの利用にかかる文言を追加　等

佐賀市情報セキュリティポリシー

（基本方針）

佐賀市

1 目的

佐賀市（以下、「本市」という。）が取り扱う情報には、特定個人情報を含む市民の個人情報のみならず行政運営上重要な情報など、外部への漏洩等が発生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。そのため、情報資産及び情報資産を取り扱うネットワーク並びに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。

このことから、本市は、情報資産に対する情報セキュリティ対策を実施するために、情報セキュリティポリシーを定めることとする。情報セキュリティポリシーは、情報セキュリティ対策についての基本的な事項を定める「基本方針」と、「基本方針」を実行に移すための遵守事項と判断基準を示す「対策基準」で構成される。

本文書は、本市の情報セキュリティ対策の基本的な方針を定めるものである。

2 定義

(1) 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。

(2) 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。

(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) 職員等

本市の情報資産を取り扱う全ての者（会計年度任用職員及び委託契約により常駐する者等を含む。）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

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 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

(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、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

(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

(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

(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

(6) その他、本市の情報資産の機密性、完全性、可用性を脅かす脅威

4 適用範囲

(1) セキュリティポリシーの範囲

適用される行政機関は、市長部局、議会事務局、監査事務局、公平委員会、選挙管理委員会事務局、農業委員会事務局、教育委員会事務局とする。

(2) 情報資産の範囲

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電磁的記録媒体
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およびネットワーク図などのシステム関連文書

5 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、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。

(2) 情報資産の分類と管理

本市の保有する情報資産を重要度に基づき 4 段階に分類し、分類に応じた情報セキュリティ対策を実施する。

(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、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、住民情報の流出を防ぐ。

②LGWAN 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、無害化通信を実施する。

③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対策を実施する。高度な情報セキュリティ対策として、佐賀県及び佐賀県内市町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。

(4) 物理的セキュリティ

サーバ室、通信回線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。

(5) 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。

(6) 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。

(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、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は迅速かつ適正に対応するものとする。

(8) 業務委託と外部サービスの利用

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確にした契約を締結し、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。

(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。

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の遵守状況を検証するため、毎年度及び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

情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合には、情報セキュリティポリシーを見直す。

9 情報セキュリティ対策基準の策定

上記6、7及び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 情報セキュリティ運用マニュアルの策定

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運用マニュアルを策定するものとする。なお、情報セキュリティ運用マニュアルは、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 特定個人情報の取扱いに関する管理規程の策定

基本方針を実行に移すための遵守事項と判断基準および具体的手順として特定個人情報の取扱いに関する管理規程を策定するものとする。