石岡市行政情報
セキュリティポリシー

＜情報セキュリティ基本方針＞

石　岡　市

総務部情報政策課

令和８年３月版

＜　目　　次　＞

石岡市情報セキュリティポリシー改正履歴

平成 15 年　策定

平成 25 年　４月　一部改正

平成 27 年　９月　全部改正

令和元年　５月　一部改正

令和４年１１月　一部改正

令和７年　２月　全部改正

令和８年　３月　一部改正

1　目的と位置付け

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必要な情報など、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。

これらの情報資産を始めそれを取り扱うネットワーク及び情報システムを様々な脅威から防御することは、事務事業の安定的な運営のためだけでなく、市民の財産や個人情報等を守るために必要不可欠であり、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、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とともに「石岡市情報セキュリティに関する規程」に基づき、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ことを目的とする。

なお、本基本方針については、地方自治法（昭和22年法律第67号）第244条の６第１項に規定するサイバーセキュリティを確保するための方針として位置付けるものとする。

2　定義

⑴　ネットワーク

市における市長部局、各行政委員会、各事務局、消防本部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。

⑶　情報資産

ネットワーク及び情報システムの開発と運用に係るすべての情報並びにネットワーク及び情報システムで取り扱う情報をいう。

⑷　情報セキュリティ

情報資産の機密性、完全性、可用性を維持することをいう。

⑸　情報セキュリティポリシー

市における情報セキュリティ基本方針及び情報セキュリティ対策基準をいう。また、具体的な実施手順として、情報セキュリティ実施手順書を定める。

⑹　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。

⑺　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。

⑻　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。

⑼　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）又は戸籍事務等に係る情報システム及びデータをいう。

⑽　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。）。

⑾　インターネット接続系

インターネットメール等に係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。

⑿　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。

⒀　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。

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

４　適用範囲

⑴　行政機関の範囲

この情報セキュリティポリシーが対象とする行政機関の範囲は、市長部局、各行政委員会、各事務局、消防本部、地方公営企業等とし、市とネットワーク接続している市の施設を対象とする。ただし、議会、各行政委員会等その他部局において情報セキュリティポリシーを別に定める場合は、所管する部局のセキュリティポリシーに従うとともに、利用するネットワークや機器に応じて本基本方針の対象とする。

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、情報システム、これらに関する設備、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及びネットワーク図等のシステム関連文書

5　職員等の遵守義務

職員、再任用職員、常勤の特別職を含む特定職員及び会計年度任用職員等（以下、「職員等」という。）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。ただし、当市の職員等でない者が本基本方針で対象とするネットワークやソフトウェア等を限定的に利用する場合においては、基本方針のみを遵守し、その他の利用規定については当該ネットワークや機器等を所管する部局の指示に従うこととする。

6　情報セキュリティ対策

上記３の脅威から市の情報資産を保護する為に、以下の情報セキュリティ対策を講じる。

⑴　組織体制

市情報管理組織に関する規則及び情報セキュリティに関する規程に基づき、市の情報資産について、管理職が率先して情報セキュリティ対策を推進・管理する組織体制を確立する。

⑵　情報資産の分類と管理

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行う。

⑶　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。

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、県と市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等を実施する。

⑷　物理的セキュリティ

情報システムを設置する施設への不正な立入り、情報資産への損傷・妨害等を防止するために物理的な対策を講ずる。

⑸　人的セキュリティ

情報セキュリティに関し、職員等の権限や遵守すべき事項などを定めるとともに、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、ネットワーク監視対策、不正プログラム対策、不正アクセス対策等の情報資産の保護に関する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切に対応するため、緊急時対応計画を講ずる。

⑻　業務委託と外部クラウドサービス等の利用

①　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。

②　外部クラウドサービス等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。

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、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。

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、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。

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や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、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必要に応じて分析し、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。

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。

情報セキュリティ対策基準は、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恐れのある情報資産であることから非公開とする。

１０　情報セキュリティ実施手順書の策定

情報管理責任者は、各情報セキュリティ対策基準を遵守して情報セキュリティ対策を実施するために、情報セキュリティ対策基準の基本的な要件に基づき、具体的な手順を定めた情報セキュリティ実施手順書を策定するものとする。

情報セキュリティ実施手順書は、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恐れのある情報資産であることから非公開とする。