岡山市
情報セキュリティポリシー
（抜粋版）

平成 25 年 6 月

（最終改定　平成 31 年 4 月 1 日）

岡　山　市

第１章　情報セキュリティ基本方針

１　目的

情報セキュリティポリシーは、本市が所掌する情報資産に係る機密性、完全性及び可用性を維持するための対策の基準を定めることにより、市民のプライバシー、財産等を保護するとともに、行政事務の適正な運営に資することを目的とする。

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並びにその構成機器(ハードウェア及びソフトウェア）をいう。

（２）外部ネットワーク

インターネットや他団体が管理しているネットワークなどの本市が管理していないネットワークの総称をいう。

（３）ウェブサイト

インターネット上に公開された、文字、画像、動画等から成るホームページの集まりをいう。

（４）庁舎外

本庁舎、分庁舎、保健福祉会館、区役所、支所、地域センター等の建物やその敷地以外の場所で、本市の管理していない場所をいう。

（５）行政情報

岡山市情報公開条例第２条第２号に規定する「公文書」と同義とし、実施機関の職員が職務上作成し、又は取得した文書、図画、写真、フィルム、テープ及び電磁的記録(電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作成された記録をいう。以下同じ。)であって、当該実施機関の職員が組織的に用いるものとして、当該実施機関が保有しているものをいう。ただし、次に掲げるものを除く。

ア　官報、白書、新聞、雑誌、書籍その他不特定多数の者に販売することを目的として発行されるもの

イ　図書館その他の施設において一般の利用に供することを目的として管理されているもの

ウ　実施機関において歴史的若しくは文化的な資料又は学術研究用の資料として特別の管理がなされているもの

（６）情報システム

コンピュータ（ハードウェア及びソフトウェア)、ネットワーク及び電磁的記録媒体で構成された、情報処理を行う仕組みをいう。

（７）情報資産

情報システム及び情報システムで取り扱う行政情報をいう。

（８）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。

（９）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。

（１０）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。

（１１）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。

（１２）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。

（１３）情報セキュリティインシデント

不正アクセス、ウイルス感染、ハードウェア・ソフトウェア障害、人為的ミス等により、情報資産の漏えい・破壊・改ざん・消去や情報システムのサービス停止等が発生することをいう。

（１４）業務系（マイナンバー利用事務系）

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。

（１５）情報系（ＬＧＷＡＮ接続系）

人事給与、財務会計及び文書管理等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。

（１６）公開系（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。

（１７）通信経路の分割

情報系と公開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。

（１８）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）サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃、内部不正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、サービス停止等

（２）無許可のハードウェア、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、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、機器故障等の偶発的要因による情報資産の漏えい・破壊・消去等

（３）地震、水害、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、通信の途絶等のインフラの障害からの波及等

４　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、市長の事務部局の局室及び区役所、水道局、市場事業部、消防局、議会事務局、選挙管理委員会事務局、監査事務局、人事委員会事務局、農業委員会事務局並びに教育委員会事務局とする。

（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。ただし、ＩＣカード等に行政情報を記録したものを市民に交付する等により、当該情報資産の管理者が本市でなくなった場合は対象としない。

ア　情報システム及びこれらに関する設備

イ　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

５　職員等の遵守義務

職員等（任期付職員、再任用職員、嘱託職員、臨時職員及びアルバイトを含む。）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。

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実施する。

（３）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　業務系においては、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　情報系においては、情報システムと、公開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。

ウ　公開系においては、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、市区町村のインターネット接続口を集約する自治体情報セキュリティクラウドに参加する。

（４）物理的セキュリティ

サーバ、情報システム室、通信回線及び職員が利用するパソコン等の端末並びに情報資産を取り扱うその他の設備及び機器の管理について、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、システムの開発・導入・保守、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、情報セキュリティインシデントが発生した場合等に迅速かつ適正に対応するため、緊急時対応手順を策定する。

（８）外部サービスの利用

外部委託する場合には、外部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、外部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。

約款によ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、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、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、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又は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となった場合には、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 情報セキュリティ実施手順の策定

情報セキュリティに関する対策の具体的な実施手順は、情報セキュリティポリシーで定める情報セキュリティ対策基準に基づき、全庁共通の実施手順及び情報システムごとの実施手順としてそれぞれ策定し、必要に応じて見直しを行うものとする。全庁共通の実施手順は情報セキュリティを統括する課において、また、情報システムごとの実施手順は該当の情報システムを所管する課及びこれらに相当する組織において管理するものとする。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において情報セキュリティインシデントを誘発する可能性があり、また、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。

附　則

この基本方針は、平成２５年６月１日から施行する。

この基本方針は、平成２６年１０月１日から施行する。

この基本方針は、平成２８年３月１日から施行する。

この基本方針は、平成３１年４月１日から施行する。