笠岡市情報セキュリティポリシー

笠岡市情報セキュリティ基本方針

笠岡市

平成 29 年３月制定
平成 31 年３月改定
令和５年４月改定
令和７年２月改正

（目的）

第１条　この基本方針は，本市が保有するネットワーク，情報システム及びこれらに関する設備及びデータ（以下「情報資産」という。紙媒体を含む。）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関する基本的な事項を定めることにより，行政の適正かつ円滑な運営を図り，市政に対する市民の信頼を確保することを目的とする。

（定義）

第２条　この基本方針において，次の各号に掲げる用語の意義は，当該各号に定めるところによる。

(1) コンピュータ

パーソナルコンピュータ，サーバ，ストレージ等の機器をいう。

(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

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。

(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) 情報セキュリティポリシー

この基本方針及び情報セキュリティ対策基準をいう。

(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維持し，データの正当性，正確性，一貫性等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

文書管理，財務会計及びグループウェア等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（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)無害化処理

インターネットメールの添付ファイルやインターネット接続系からのファイルをダウンロードする際に，コンピュータウイルス等の不正プログラムと疑われるものを排除することをいう。

（対象とする脅威）

第３条　情報資産に対する脅威として，次の脅威を想定し，情報セキュリティ対策を実施する。

(1)人による脅威（故意）

不正アクセスやウイルス攻撃等のサイバー攻撃，機器の盗難，情報資産の不正な操作や持ち出し等の故意による情報資産の漏えい・破壊・改ざん・消去等

(2)人による脅威（過失）

情報資産の管理不備，無許可ソフトウェアの使用等の規定違反，プログラム上の欠陥，操作・設定ミス，メンテナンス不備，外部委託管理の不備等の過失による情報資産の漏えい・破壊・消去等

(3)災害による脅威

地震，落雷，火災，水害等の災害によるサービス及び業務の停止，情報資産の消失等

(4)必要資源の不足，故障等による脅威

災害の影響又はその他の原因による電力，通信，水道の途絶，交通機能の麻痺や大規模・広範囲にわたる疾病の蔓延による要員の不足，機器の故障等によるサービスや業務の停止，システム運用の機能不全等

（適用範囲）

第４条　この基本方針の適用範囲は，本市が保有する情報資産，情報資産に関する事務に携わる全ての職員，会計年度任用職員，労働者派遣事業により本市の事務に携わる者

（以下「職員等」という。）及び委託事業者とする。

２　情報資産の範囲

本基本方針が適用される情報資産は，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及びネットワーク図等のシステム関連文書

（遵守義務）

第５条　前条に規定する者は，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手順書を遵守しなければならない。

（情報セキュリティ対策）

第６条　第３条の脅威から情報資産を保護するために，次のとおり情報セキュリティ対策を講じるものとする。

(1) 組織体制

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　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，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，無害化処理を実施する。

ウ　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，都道府県と市区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。

(4) 物理的セキュリティ

サーバ等，電算室，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，外部委託を行う際の情報セキュリティの確保等，情報セキュリティポリシーの運用面の対策を講じる。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，緊急時対応計画を策定する。

(8) 業務委託と外部サービス（クラウドサービス等）の利用

業務委託する場合には，委託事業者を選定し，情報セキュリティ用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。また，外部サービス（クラウドサービス等）を利用する場合には，利用に係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。

（情報セキュリティに関する監査及び自己点検の実施）

第７条　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に関する監査及び自己点検を実施する。

（情報セキュリティポリシーの見直し及び改定）

第８条　情報セキュリティに関する監査及び自己点検の結果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，定期的に情報セキュリティポリシーの見直しを行い，必要に応じて改定する。

（情報セキュリティ対策基準の策定）

第９条　前３条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。

（情報セキュリティ実施手順の策定）

第１０条　情報セキュリティ対策基準に基づき，情報セキュリティに関する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と共に，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。

（懲戒処分）

第１１条　情報セキュリティポリシーに違反した職員等及びその監督責任者は，その重大性，発生した事案の状況等に応じて，地方公務員法（昭和 25 年法律第 261 号）による懲戒処分の対象とする。

（損害賠償）

第１２条　本市は，情報セキュリティポリシーに違反した外部の者（委託事業者を含む。）に対して，その重大性，発生した事案の状況等に応じて，損害賠償を求めることができる。