香南市情報セキュリティ基本方針

（目的）

第１条　香南市情報セキュリティ基本方針（以下「基本方針」という。）は、市の情報セキュリティ対策の基本的な考え方及び方策を定め、市の所有する個人情報の保護並びに行政情報の機密性、完全性及び可用性を維持向上することを目的とする。

（適用範囲）

第２条　この基本方針の適用範囲は以下の業務、組織、所在地及び情報資産とする。

（１）　業務　市の実施する全ての業務

（２）　組織　市の全ての組織

（３）　情報資産　市の所有する全ての情報資産

①　ネットワーク、情報システム及び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　市が保有する文書

④　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

（用語の定義）

第３条

（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）　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。

（６）　完全性

情報が破壊され、改ざんされ、又は消去されていない状態を確保することをいう。

（７）　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、情報にアクセスすることができる状態を確保することをいう。

（８）　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、地方税又は防災に関する事務）又は戸籍事務等住民に関する個人情報等に関わる情報システム及びデータをいう。

（９）　ＬＧＷＡＮ接続系

人事給与、財務会計、文書管理及びホームページ管理システム等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。

(10)　インターネット接続系

インターネットメール、ホームページ等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。

(11)　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相互に許可できるようにすることをいう。

(12)　特定通信

マイナンバー利用事務系とＬＧＷＡＮ接続系、又は、ＬＧＷＡＮ接続系とインターネット

接続系の各環境間で、送信元及び送信先並びに通信に関する仕様等を限定することで、許可された通信をいう。

(13)　無害化処理

インターネットメール本文中のタグ情報の除去及びリンクの無効化及び添付ファイルの除去等並びに端末への画面転送等により、安全を確保する処理をいう。

(14)　香南市教育情報セキュリティ基本方針

教育委員会及び各学校（小学校、中学校及び教育支援センターをいう。以下同じ。）が保有する情報資産に対し、機密性、完全性及び可用性を維持向上することを目的として別に定める基本方針をいい、対象となる情報資産及び適用範囲等は当該基本方針に規定する。

（対象とする脅威）

第４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）　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

（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・消去等

（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、水道供給の途絶等のインフラの障害からの波及等

（職員等の遵守義務）

第５条　職員、非常勤職員、会計年度任用職員及び臨時職員（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は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。

（情報セキュリティ対策）

第６条　第４条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行う。

（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、両システム間で情報の交換を行う場合には、無害化処理を行う。

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行う。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、自治体情報セキュリティクラウドの導入等を行う。

④　市民等からの手続をオンライン化する場合に必要となるＬＧＷＡＮ接続系とマイナンバー利用事務系との接続は、利用する通信機器等のＩＰアドレス等を明確に特定することで特定通信とし、その限りにおいて許可する。

（４）　物理的セキュリティ

サーバー室等、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。

（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迅速かつ適切に対応するため、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） 評価及び見直し

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。

（情報セキュリティ監査及び自己点検の実施）

第７条　情報セキュリティ対策の評価及び新たな脅威への対応等を踏まえ、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。

（情報セキュリティポリシーの見直し）

第８条　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を見直す。

（情報セキュリティ対策基準の策定）

第９条　第６条から前条まで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。

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。

附　則（令和８年４月１日）

この基本方針は、公表の日から施行する。