高松市情報セキュリティ基本方針

平成29年6月1日

令和8年3月2日改正

改版履歴

版数	改版日	改版項	改版履歴
1.0	2017/6/1	全体	高松市情報セキュリティ基本方針（平成１５年７月１日施行）の一部を改正する。
1.1	2018/4/1	2.（２）	組織機構の見直しに伴い、一部を改正する。
1.2	2019/4/1	全体	高松市情報セキュリティ基本方針（平成２９年４月１日施行）の一部を改正する。
1.3	2022/10/5	全体	高松市情報セキュリティ基本方針（平成３１年４月１日施行）の全部を改正する。
1.4	2025/4/1	全体	高松市情報セキュリティ基本方針（令和４年１０月５日施行）の全部を改正する。
1.5	2026/3/2	全体	高松市情報セキュリティ基本方針（令和７年４月１日施行）の一部を改正する。

目次

１．目的と位置付け

本基本方針は、本市が取り組む情報セキュリティ対策の土台となるもので、対象とする脅威、適用対象や具体的な範囲を明確にし、本市が保有する情報資産の機密性、完全性及び可用性を守ること、また、万が一の危機が発生した場合には、適切に対応できるようにすることを目的とする。

また、本基本方針と高松市情報セキュリティ対策基準（以下「情報セキュリティ対策基準」という。）とで構成する本市の情報セキュリティに関する方針（以下「情報セキュリティポリシー」という。）は、本市における情報セキュリティ対策に関する事項を総合的・体系的・具体的に取りまとめたものとして、本市の情報セキュリティ対策の最上位に位置するものとする。

２．定義

情報セキュリティポリシーにおいて、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）　職員等

地方公務員法(昭和２５年法律第２６１号)第３条第２項に規定する一般職に属する本市の職員並びに市長、副市長、教育長、病院事業管理者、代表監査委員及び同条第３項第３号に掲げる職に属する本市の職員をいう。

（２）　委員

地方公務員法(昭和２５年法律第２６１号)第３条第３項第１号及び同条第３項第２号に規定する教育委員会、監査委員、選挙管理委員会、農業委員会、公平委員会及び固定資産評価審査委員会（以下「行政委員会等」という。）の委員をいう。ただし、前号の教育長及び代表監査委員を除く。

（３）　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及びその構成機器（ハードウェア及びソフトウェア）をいう。

（４）　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た、情報処理を行う仕組みをいう。

（５）　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。

（６） 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。

（７） 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。

（８） 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。

（９） 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。

(10) 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。

(11) 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。）。

(12) 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。

(13) 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。

(14) 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。

（15） 本市

本基本方針が適用される行政機関をいう。

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。

a） 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、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

b） 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

c） 地震、落雷、火災等の災害によるサービスや業務の停止等

d） 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

e） 電力供給の途絶、通信の途絶又は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

情報セキュリティポリシーの適用範囲は、次に掲げるものとする。

（１） 行政機関の範囲

本基本方針が適用される行政機関は、市長部門、消防局、病院局、行政委員会等及び市議会事務局とする。

（２） 情報資産の範囲

本基本方針が対象とする情報資産は、本市が管理するネットワーク、情報システム、これらに関する設備、電磁的記録媒体及び全ての行政文書（高松市公文書等の管理に関する条例（平成２５年高松市条例第２号）第２条第２項で規定する行政文書をいう。）とする。ただし、情報マネジメント課が管理する行政系のネットワークから、物理的又は論理的に完全に分離されている教育委員会が管理する教育学習に利用するシステム及びネットワーク等並びに病院局が管理する医療情報系システム及びネットワーク等については、文部科学省の

「教育情報セキュリティポリシーに関するガイドライン」や厚生労働省の「医療情報システムの安全管理に関するガイドライン」の範囲であることから、個別に策定した対策基準を適用することとする。

（３） 対象者

本基本方針が適用される対象者は職員等及び委員とする。なお、委員については、職員等と取り扱う情報資産の範囲が大きく異なることから、個別に策定した対策基準を適用することとする。

５．職員等及び委員の遵守義務

職員等及び委員は、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） 管理体制

本市の保有する情報資産について、情報セキュリティ対策を推進するため、全庁的な管理体制を構築する。

（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、可用性の維持の程度からなる重要性分類ⅠからⅢに分類し、当該分類に応じた取扱いを定めた上で、情報資産の管理責任を明確にし、情報資産のライフサイクルに応じて取るべき管理方法と情報セキュリティ対策を実施する。

a) **重要性分類Ⅰ**

ア　行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」（平成 23 年４月１日内閣総理大臣決定）に定める秘密文書に相当する文書。

イ　行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きいもの。

ウ　行政事務で取り扱う情報資産のうち、基本的に公表することを前提としていないもの。

b） **重要性分類Ⅱ**

行政事務で取り扱う情報資産のうち、直ちに一般に公表することを前提としていないもの。

c） **重要性分類Ⅲ**

上記ａ）及びｂ）以外の情報資産

（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に、業務の効率性や利便性の観点を踏まえ、情報システム全体の強靭性を次の三段階に分類し、分類に応じた対策を行う。

a） マイナンバー利用事務系は、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。

b） ＬＧＷＡＮ接続系は、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は、無害化通信を実施する。

c） インターネット接続系は、不正通信の監視機能の強化など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、県と本市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を利用する等の対策を講じる。

（４） 物理的セキュリティ

サーバ、サーバ等を管理する区域、通信回線や職員等のパソコンなどの管理について、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等の必要な対策を講じる。

（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や不正アクセス対策等の技術的な対策を講じる。

（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行う。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）の利用

a) 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く措置を講じる。

b) 外部サービス（クラウドサービス）を利用する場合には、必要に応じて利用に係る規定を整備し対策を講じる。

c) 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、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、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分析し、リスクを検討した上で、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。

なお、情報セキュリティ対策基準は、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（４.（２）ただし書き等の個別に策定した対策基準も同様とする。）。

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

この基本方針は、平成１５年７月１日から施行する。

附　則

この基本方針は、平成２４年４月１日から施行する。

附　則

この基本方針は、平成２７年８月３１日から施行する。

附　則

この基本方針は、平成２９年６月１日から施行する。

附　則

この基本方針は、平成３０年４月１日から施行する。

附　則

この基本方針は、平成３１年４月１日から施行する。

附　則

この基本方針は、令和４年１０月５日から施行する。

附　則

この基本方針は、令和７年４月１日から施行する。

附　則

この基本方針は、令和８年３月２日から施行する。