

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7年4月1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。

目次

1. 目的.....	1
2. 定義.....	1
(1) ネットワーク	1
(2) 情報システム.....	1
(3) 情報セキュリティ	1
(4) 情報セキュリティポリシー	1
(5) 機密性.....	1
(6) 完全性.....	1
(7) 可用性.....	1
(8) マイナンバー利用事務系（個人番号利用事務系）	2
(9) L G W A N接続系	2
(10) インターネット接続系	2
(11) 通信経路の分割	2
(12) 無害化通信	2
3. 対象とする脅威	2
4. 位置付けと適用範囲	3
(1) 行政機関の範囲	3
(2) 情報資産の範囲	3
5. 職員等の遵守義務.....	3
6. 情報セキュリティ対策.....	4
(1) 管理体制.....	4
(2) 情報資産の分類と管理	4
(3) 情報システム全体の強靱性の向上	4
(4) 物理的セキュリティ	5
(5) 人的セキュリティ	5
(6) 技術的セキュリティ	5
(7) 運用	5
(8) 業務委託と外部サービス（クラウドサービス）の利用	5
(9) 評価・見直し.....	6
7. 情報セキュリティ監査及び自己点検の実施	6
8. 情報セキュリティポリシーの見直し	6

9. 情報セキュリティ対策基準の策定	6
10. 情報セキュリティ実施手順の策定	6

1. 目的

この基本方針は、本市の情報セキュリティ対策の基本的な方針として、この基本方針と高松市情報セキュリティ対策基準（以下「対策基準」という。）で構成する高松市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。）の位置付けと適用範囲等に関し必要な事項を定めることにより、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、危機発生時における適切な対応を図ることを目的とする。

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） 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。

（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た、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、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。

（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。

(9) L G W A N接続系

L G W A N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。）。

(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。

(11) 通信経路の分割

L G W A N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。

(12) 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。

- 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. 位置付けと適用範囲

情報セキュリティポリシーは、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で、本市における情報セキュリティ対策の最上位に位置するものとし、その適用範囲は、次に掲げるものとする。ただし、情報セキュリティポリシー及び対象業務等の性質により、個別に対策等を定める場合は、その規定等に定めのない重要な事項が発生した場合は、第6項第1号に規定する最高情報セキュリティ責任者の指示に従うものとする。

(1) 行政機関の範囲

本情報セキュリティポリシーが適用される行政機関は、市長部門、消防局、病院局、教育局、監査委員事務局、選挙管理委員会事務局、農業委員会事務局、市議会事務局及び公平委員会とする。

なお、教育局、病院局等においては、「教育学習に利用するネットワーク」（校務系、学習系、校務外部接続系等）や「医療情報系ネットワーク」（医療情報システム利用系、レセプトオンライン請求系、オンライン資格確認等システム接続系）がある。これらのネットワークについて、高松市の行政系ネットワーク（情報マネジメント課が管理する業務用ネットワーク）から、物理的又は論理的に完全に分離されている場合、セキュリティポリシーに関する対策基準のガイドラインとして、それぞれ「教育情報セキュリティポリシーに関するガイドライン」（文部科学省）及び「医療情報システムの安全管理に関するガイドライン」（厚生労働省）が策定されていることから、これらのネットワークに係る対策基準については本ガイドラインではなくそれぞれのガイドラインが適用されることとする。

(2) 情報資産の範囲

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。

5. 職員等の遵守義務

職員、会計年度任用職員及び臨時職員等（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。

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、総務局を所管する副市長を最高情報セキュリティ責任者（Chief Information Security Officer）とする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靱性の向上

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靱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) L G W A N接続系は、L G W A N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。

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。