別紙２

高松市情報セキュリティ基本方針

平成29年6月1日

平成31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。

目次

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で構成する高松市情報セキュリティに関する方針（以下「セキュリティ方針」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、本市の情報資産の機密性（許可を受けた者のみが情報を利用できることをいう。以下同じ。）を保持し、その完全性（情報の整合性が確保され、かつ、情報が過不足なく保存されていることをいう。以下同じ。）と可用性（必要な時に情報が利用できることをいう。以下同じ）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

セキュリティ方針において、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）　ネットワーク

市長部門、消防局、病院局、教育委員会、監査委員、選挙管理委員会、公平委員会、農業委員会及び市議会事務局のコンピュータ等（専ら教育の用に供するために教育機関に設置されたもの（以下「教育用コンピュータ」という。）を除く。）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）　電磁的記録媒体等

磁気ディスク、磁気テープ、光ディスクその他の電子データを記録することのできる媒体及びこれに係る入出力帳票をいう。

（３）　情報システム

本市の全ての電子計算機（教育用コンピュータ及び専ら市民の利用に供するためのコンピュータ等を除く。）及びネットワークで構成され、処理を行う仕組みをいう。

（４）　情報資産

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。）をいう。

（５）　情報セキュリティ

情報資産の機密性の保持並びに完全性及び可用性の維持をいう。

（６）　情報セキュリティ対策

情報セキュリティの確保に関する事務又は業務をいう。

（７）　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）に関わる情報システム及びデータをいう。

（８）　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。

（９）　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。

（１０）　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。

（１１）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. セキュリティ方針の位置付けと適用範囲

セキュリティ方針は、情報セキュリティ対策の最上位に位置し、情報セキュリティ対策に関する事項を総合的・体系的・具体的にとりまとめたもので、その適用範囲は、次に掲げるとおりとする。ただし、セキュリティ方針に定めのない重要な事項が発生した場合は、第１０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）　情報資産及びこれを取り扱う業務

（２）　情報資産の取扱い及び管理に携わる従事者

（３）　情報資産を取り扱う業務の用に供する施設又は設備

4. 職員等の義務

情報資産を取り扱う者（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、セキュリティ方針を遵守するものとする。

5. 情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

6. 情報セキュリティ対策

情報資産を漏えい、廃棄、破壊等の脅威から保護するため、次に掲げる情報セキュリティ対策を講ずるとともに、緊急事態に対応するための危機管理対策を講ずるものとする。

（1） 物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷、妨害等を防ぐために物理的な対策を講ずることをいう。

（2） 人的セキュリティ対策

情報セキュリティ対策に関する権限及び責任を定め、全ての職員等にセキュリティ方針の内容を周知徹底するなど十分な教育及び啓発が行われるように必要な対策を講ずること。

（3） 技術及び運用におけるセキュリティ対策

情報資産を外部からの不正な侵入等から適切に保護するため、情報資産への接続及び操作の制御、ネットワーク管理等に関する技術面の対策を講ずるとともに、システム開発等の外部委託、ネットワークの監視及びセキュリティ方針の遵守状況の確認等に関する運用面の対策を講ずることをいう。

（4） 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ずるものとする。

a　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。

b　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、無害化通信を実施する。

c　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、県と本市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。

（5） 外部サービスの利用

a　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ずるものとする。

b　約款による外部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ずるものとする。

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ものとする。

7. 高松市情報セキュリティ対策基準の策定

情報資産について前項各号に掲げる情報セキュリティ対策を講ずるにあたっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、各情報セキュリティ対策を行う上で必要となる基本的な要件を明記した高松市情報セキュリティ対策基準（以下「対策基準」という。）を策定するものとする。

8. 情報セキュリティ実施手順の策定

対策基準を遵守して情報セキュリティ対策を実施するためには、情報資産の種別に応じたセキュリティ対策手順等をそれぞれ定めていく必要がある。そのため、情報資産に対する脅威及び情報資産の重要度に対応する対策基準の基本的な要件に基づき、情報システムごとに情報セキュリティ実施手順（以下「実施手順」という。）を策定するものとする。

9. セキュリティ方針の公開

セキュリティ方針は、公開する。ただし、実施手順は、公にすることにより本市の行政運営に支障を来すおそれのある情報であることから、非公開とする。

10. 情報セキュリティ管理体制

情報セキュリティ対策を推進するため、全庁を対象とした情報セキュリティ管理体制を整備する。

（１）　最高情報セキュリティ責任者の設置

情報システム、情報資産及び情報セキュリティ対策を統括する最高情報セキュリティ責任者を置く。

（２）　情報セキュリティ管理組織の設置

情報セキュリティの管理に関する事務を所掌し、情報セキュリティ対策を推進するため、高松市ＩＣＴ推進会議を置く。

（３）　情報セキュリティに関する権限と責任の明確化

情報セキュリティに関する権限と責任は、対策基準で定める。

（４）　情報セキュリティの監査

セキュリティ方針が遵守されていることを検証するため、定期的に監査を実施する。

（５）　セキュリティ方針の見直し

情報セキュリティ監査の結果及び情報セキュリティを取り巻く状況の変化を踏

まえ、セキュリティ方針の見直しを適時適切に実施する。

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。