

情報セキュリティ基本方針

1 目的

本市の各情報システムで取り扱う情報には、市民の個人情報のみならず行政運営上重要な情報など、部外に漏えい等した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、これらの情報及び情報を取り扱う情報システムを様々な脅威から防御することは、市民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが本市に対する市民からの信頼の維持向上に寄与するものである。

また、近年のいわゆるIT革命の進展により、電子商取引の発展や電子自治体の実現が期待されているところである。本市がこれらに積極的に対応するためには、すべてのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

そのため、本市の情報資産の機密性、完全性及び可用性を維持するための対策（情報セキュリティ対策）を整備するために東広島市情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については本市の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

2 定義

(1) ネットワーク

本市における本庁内外の機関及び本庁舎外機関の各内部組織、各教育機関（事務室及び職員室に限る）等の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(confidentiality)

情報にアクセスすることを認可された者だけが、情報にアクセスできることを確保することをいう。

(6) 完全性(integrity)

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(availability)

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）また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) 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。）。

(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

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。

(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 適用範囲

(1) 行政機関の範囲

情報セキュリティポリシーが適用される行政機関は、市長部局、行政委員会、議会事務局、消防局、地方公営企業及び各教育機関（本市の内部ネットワークに接続する設備及び情報システムを利用する機関に限る）とする。

(2) 情報資産の範囲

情報セキュリティポリシーが対象とする情報資産は、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

4 情報セキュリティポリシーの位置付けと職員等の義務

情報セキュリティポリシーは、本市が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の頂点に位置するものである。

したがって、市長をはじめとして本市が所掌する情報資産に関する業務に携わる職員、非常勤職員及び臨時職員等（以下「職員等」という）及び外部委託事業者は、情報セキュリティの重要性について共通の認識を持つとともに業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負うものとする。

5 情報セキュリティ管理体制

本市の情報資産について、管理職が率先して情報セキュリティ対策を推進・管理するための全庁的な管理体制を確立するものとする。

6 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実施する。

7 情報資産への脅威

情報セキュリティポリシーを策定する上で、情報資産に対する脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

- (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、外部委託管理の不備、マネジメントの欠陥、機器故障等の非意図的の要因による情報資産の漏えい・破壊・消去等
- (3) 地震、落雷、火災等の災害並びに事故、故障等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

8 情報セキュリティ対策

上記7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ずるものとする。

(1) 物理的セキュリティ対策

サーバ、情報システム、通信回線及び職員等のパソコン等の管理について、物理的な対策を講ずる。

(2) 人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、すべての職員等に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるように必要な対策を講ずる。

(3) 技術的セキュリティ対策

情報資産を外部からの不正なアクセス等から適正に保護するため、コンピュータ等の管理、情報資産へのアクセス制御、不正プログラム対策、不正アクセス対策、ネットワーク管理等の技術面の対策を講じる。

(4) 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ずる。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正な対応するため、緊急時対応計画を策定する。

(5) 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とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

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。

②LGWAN 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。

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との通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

(6) 外部サービスの利用

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じる。

約款によ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 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。

10 評価及び見直しの実施

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を取り巻く状況の変化に対応するため新たに対策が必要となった場合には、情報セキュリティポリシーの見直しを実施する。

11 情報セキュリティ対策基準の策定

上記5、6、8、9及び10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統一的なレベルで定める必要がある。そのため、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情報セキュリティ対策基準を策定するものとする。

12 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。

平成16年	3月29日	策定
平成27年	10月1日	一部改訂
平成28年	4月1日	一部改訂
平成30年	4月1日	一部改訂
平成31年	4月1日	一部改訂
令和3年	4月1日	一部改訂

東広島市長