広島市情報セキュリティ基本方針

（策定　令和８年４月１日）

１　目的

本基本方針は、本市が実施する情報セキュリティ対策について基本的な事項を定めることで、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ことを目的とする。

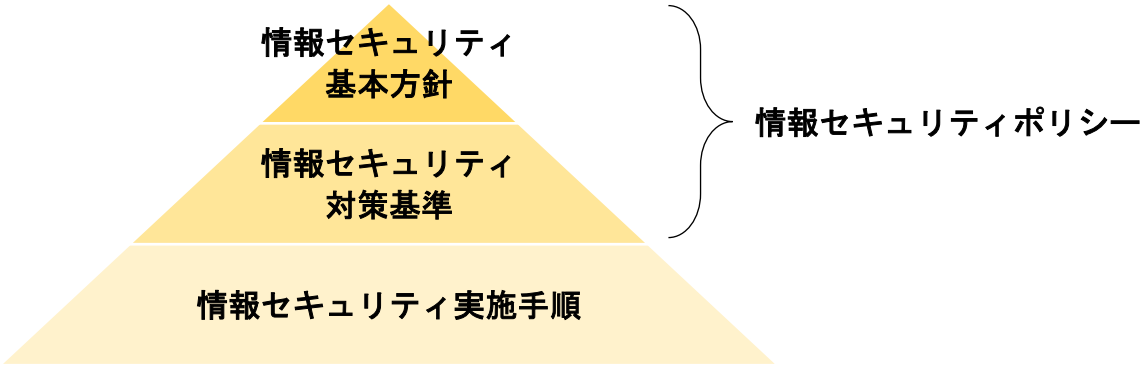
また、本基本方針の策定は、市長、議会、教育委員会、市・区選挙管理委員会、人事委員会、監査委員、農業委員会、固定資産評価審査委員会、消防長及び水道事業管理者が共同で行うものとし、地方自治法（昭和２２年法律第６７号）第２４４条の６第１項に規定する「サイバーセキュリティを確保するための方針」として位置付ける。

２　情報セキュリティ対策に係る規程体系

本市の情報セキュリティ対策に係る規定の体系は、基本的な考え方を定めた「情報セキュリティ基本方針」（本基本方針）、これに基づく情報セキュリティ対策の基準を定めた「情報セキュリティ対策基準」の階層構造とし、これらを総称して「情報セキュリティポリシー」とする。

さらに、対策基準を具体的なシステムや手順、手続に展開して個別の実施事項を定めた「情報セキュリティ実施手順」を加えた構成とする。

【体系図】



３　定義

⑴　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。

⑵　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。

⑶　情報資産

情報システムで取り扱うすべてのデータ（開発に係るデータを含む。）をいう。

⑷　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。

⑸　機密性

情報にアクセスすることを認められた者だけが、アクセスできる状態を確保することをいう。

⑹　完全性

情報及びその処理方法の正確さ並びに情報が破壊、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。

⑺　可用性

情報にアクセスすることを認められた者が、必要なときにアクセスできる状態を確保することをいう。

4　対象とする脅威

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。

⑴　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

⑵　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

⑶　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

⑷　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

⑸　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

5　適用範囲

⑴　対象とする機関の範囲

本基本方針は、市長、議会、教育委員会、市・区選挙管理委員会、人事委員会、監査委員、農業委員会、固定資産評価審査委員会、消防長及び水道事業管理者を対象として適用する。

⑵　情報セキュリティ対策を実施する範囲

情報セキュリティ対策を実施する範囲は、次のとおりとする。

①　ネットワーク及び情報資産（これらを印刷した文書を含む。）

②　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、電磁的記録媒体

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

6　職員等の遵守義務

本市の職員、臨時・非常勤職員等（議会の議員等及び各行政委員会の委員等を含む。）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、業務の遂行に当たり、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。

また、本市が設置する学校における児童・生徒も、情報セキュリティポリシー等に規定した対策を遵守するよう、職員等が適切に指導しなければならない。

7　情報セキュリティ対策

対象とする脅威から情報資産を保護するため、次の情報セキュリティ対策を実施する。

⑴　管理体制

本市が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し、管理するための全庁的な体制を確立する。

⑵　情報資産セキュリティ

本市の保有する情報資産を重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

⑶　情報システムの強靭性の向上

マイナンバーを利用する情報システム、ＬＧＷＡＮ接続及びインターネット接続をする情報システムの強靭性を向上させるため、必要なセキュリティ対策を実施する。

⑷　物理的セキュリティ

サーバ等を設置する部屋、可搬記録媒体や情報システム機器の管理などの物理的な対策を実施する。

⑸　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などの人的な対策を実施する。

⑹　技術的セキュリティ

コンピュータやネットワーク等の管理、不正アクセス対策などの技術的な対策を実施する。

⑺　調達・運用におけるセキュリティ

情報システムの機能設計・開発などの調達及び情報システム機器の保守・ユーザＩＤの利用者管理・情報セキュリティ事故等への対応などの運用における対策を実施する。

⑻　業務委託と外部サービスの利用におけるセキュリティ

①　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実施する。

②　外部サービスを利用する場合には、選定及び利用時に必要なセキュリティ対策を実施する。

③　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。

８　情報セキュリティ監査・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、定期的に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。

９　情報セキュリティポリシーの見直し

以下の事項を踏まえ必要に応じて情報セキュリティポリシーを見直す。

⑴　組織改正等による管理体制の変更
⑵　これまで認知されていない新たな脅威の発生
⑶　新たな技術又は情報システムの導入
⑷　社会情勢の変化等による情報セキュリティ対策の実効性の喪失
⑸　情報セキュリティ監査及び自己点検の結果

⑹　その他改善すべき事象の発生

10　対策基準・実施手順の策定

⑴　情報セキュリティ対策基準

本基本方針に基づき、本市が保有する情報資産に関する情報セキュリティ対策の実施に係る具体的な遵守事項、判断基準等を定めた情報セキュリティ対策基準を策定する。

⑵　情報セキュリティ実施手順

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システム毎に策定する。

11　方針の公表等

本基本方針は、情報セキュリティの確保に係る説明責任、情報セキュリティ対策の質の確保と実効性や透明性の維持・向上の観点から、公表する。

なお、情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることで本市の行政運営等に重大な支障を及ぼすおそれがあることから、非公表とする。