阿波市情報セキュリティポリシー
阿波市議会情報セキュリティポリシー

平成17年7月1日 策定

令和 8年3月1日　改定

徳 島 県 阿 波 市

改 版 履 歴

改正年月日	改正内容	施行年月日
平成17年7月1日	阿波市情報セキュリティポリシーの制定	平成17年7月1日 (市長決裁)
平成19年5月1日	阿波市情報セキュリティポリシーの一部改正	平成19年5月1日 (市長決裁)
平成27年9月1日	阿波市情報セキュリティポリシーの一部改正	平成27年9月1日 (市長決裁)
平成29年7月28日	阿波市情報セキュリティポリシーの一部改正	平成29年7月28日 (市長決裁)
令和4年10月1日	阿波市情報セキュリティポリシーの一部改正	令和4年10月1日 (市長決裁)
令和5年4月1日	阿波市情報セキュリティポリシーの全部改正	令和5年4月1日 (情報化推進会議)
令和5年4月1日	阿波市情報セキュリティポリシーの一部改正	令和5年4月1日 (市長決裁)
令和6年12月1日	セキュリティポリシーガイドライン改定に伴う改訂	令和6年12月1日 (市長決裁)
令和7年4月1日	セキュリティポリシーガイドライン改定に伴う改訂	令和7年4月1日 (市長決裁)
令和8年4月1日	セキュリティポリシーガイドライン改訂に伴う改訂 阿波市議会情報セキュリティポリシー統合	令和8年3月1日 (市長決裁)

阿波市
情報セキュリティ
基本方針

目　　次

第１章　　情報セキュリティ基本方針

１．　目的

本基本方針は、阿波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ため、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を目的とする。

２．　定義

この基本方針において、使用する用語の意義は、個人情報の保護に関する法律（平成 15 年法律第 57 号）及び阿波市情報公開条例（平成 17 年 4 月 1 日条例第 9 号）で使用する用語の例によるほか、次の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、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

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） 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． 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。

（1） 意図的な人的脅威

①市関係者、委託事業者又は外部の権限外の者による情報資産の漏えい（口頭によるものを含む。）

②故意の不正アクセス及び不正操作

③機器及び記録媒体の盗難

④サービス停止攻撃など情報サービスへの妨害

⑤データ及びプログラムの持ち出し・盗難・改ざん・消去など

（2） 偶発的な人的脅威

①誤操作による機器の破壊又はデータ及びプログラムの消去又は破壊

②情報資産の持ち出し又は紛失

③誤操作による不正アクセス

（3） 技術的脅威

不正アクセス、ウイルス攻撃、サービス不能攻撃などのサイバー攻撃や部外者の進入等の意図的な要員による情報漏えい・破壊・改ざん・消去、重要情報の搾取等

（4） 物理的脅威等

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・設計ミス、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要因による情報資産の漏えい・破壊・消去等

（5） 災害

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

（6） パンデミック

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

（7） インフラ障害

電力の途絶、通信の途絶、水道供給の途絶などのインフラ障害からの波及等

（8） 情報システム、ネットワークの不具合

4． 適用範囲

（1） 人的範囲

本基本方針の対象範囲は、本市のすべての実施機関における情報資産に接するすべての阿波市の関係者（市長・副市長・市議会議員・市職員・非常勤職員及び臨時職員等）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、次のとおりとする。

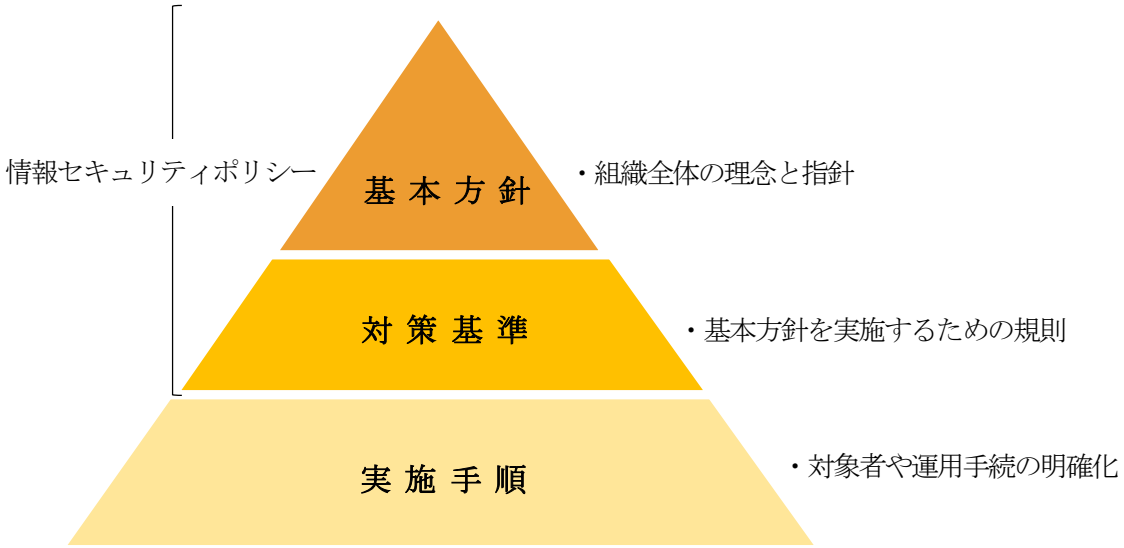
①ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

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

５．　ポリシーの位置付け

ポリシーは本市の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最高位に位置するものである。



情報セキュリティポリシーに関する体制図

６．　関係者の義務

阿波市の関係者（市長・副市長・政策監・市議会議員・市職員・非常勤職員及び臨時職員等。以下「関係者」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。

７．情報セキュリティ対策

上記３の脅威について、情報資産に対する脅威の大きさや発生頻度、適切性（利便性）、経済合理性（コスト）を考慮して、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ものとする。

（１）　組織体制

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

（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、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（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、都道府県 及び市区町村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。

（４）　物理的セキュリティ

サーバ、情報システム室、通信回線及び関係者のパソコン等の管理について、不正侵入や盗難から情報資産を保護するため、情報資産への物理的なアクセスを制御するための対策を講じる。

（５）　人的セキュリティ

情報セキュリティに関し、関係者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等の人的な対策を講じる。

（6） 技術的セキュリティ

情報資産を外部及び内部からの不正アクセス等から保護するため、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、不正アクセス対策等の技術的対策を講じる。

（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講じるものとする。

（8） 緊急時対応計画

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。

（9） 業務委託と外部サービスの利用

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、利用にかか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。

（１０） 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、情報セキュリティポリシーの見直しを行う。

８． 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。

９． 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。

１０． 情報セキュリティ対策基準の策定

上６，７、８及び９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。

１１．　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。

１２．　法令の遵守

関連する法令等の遵守について定める。

１３．　違反に対する対応

情報セキュリティポリシーに違反したものの対応を定める。

１４．　公開方針

住民の信頼と安心を得た住民サービスを実現するためには、本市の情報資産に対する取り扱い方法を公開することが望ましいが、公にすることによる本市の行政運営に重大な支障を及ぼす恐れがあることから、公開については、次のとおりとする。

（１）　情報セキュリティ基本方針

情報セキュリティ基本方針は公開する。

（２）　情報セキュリティ対策基準

情報セキュリティ対策基準は非公開とする。

（３）　情報セキュリティ実施手順

情報セキュリティ実施手順は非公開とする