神栖市情報セキュリティポリシー

神栖市情報セキュリティ基本方針

改訂履歴

版数	修正年月日	内容	備考
1	平成２７年１０月５日	初版策定	
2	平成２９年　４月１日	一部改正	
3	平成３１年　４月１日	一部改正	
4	令和　２年　４月１日	一部改正	
5	令和　３年　４月１日	一部改正	
6	令和　５年　８月１日	一部改正	
7	令和　７年　４月１日	一部改正	

神栖市情報セキュリティ基本方針

第１　目的

神栖市では、市民の個人情報のみならず行政運営上重要な情報など多数取り扱っており、これらの情報資産を様々な脅威から防御することは、市民の権利、利益を守るためにも、また、行政の安定的、継続的な運営のためにも必要不可欠である。

さらに近年、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大しており、それにより電子政府や電子自治体の実現が期待されているところであるが、本市がこれらに積極的な対応をするためには、本市が管理しているすべての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となる。

よって、この基本方針は、本市が保有する情報資産を様々な脅威から防御し、機密性、完全性及び可用性（注）を維持するため、本市が行う情報セキュリティ対策の統一的かつ基本的な考え方及び方策を定め、情報資産の管理を徹底することを目的とする。

※注

１　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。

２　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。

３　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。

第２　定義

１　ネットワーク

コンピュータを相互に接続するための通信網及びその構成機器をいう。

２　情報システム

コンピュータ（ハードウェア、ソフトウェア及び外部記録媒体）やネットワークで構成され、特定の業務を処理するための仕組みをいう。

３　情報資産

情報システム及び情報システムの開発と運用に係る全ての情報並びに情報システムで取り扱う全ての情報をいう。

なお、情報資産には紙等の有体物に出力された情報も含むものとする。

４　情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

5　情報セキュリティインシデント

情報セキュリティに関する事故、システム上の欠陥及び誤動作をいう。

6　特定個人情報

行政手続における特定の個人を識別するための番号の利用等に関する法律（以下「番号法」という。）第２条に規定する、個人番号をその内容に含む個人情報ファイルをいう。

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。

8　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。）。

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。

第３　適用範囲

１　組織の範囲

本基本方針が適用される組織は、市長、教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会及び議会とする。

なお、学校における教育のために用いるネットワーク及びパソコン等は、本基本

方針の対象外とする。

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。

（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（印刷した文書も含む。）

（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

３　対象者の範囲

本基本方針が適用される対象者は、情報資産を取り扱う全ての職員、非常勤職員、会計年度任用職員、労働者派遣事業により本市の事務に携わる者（以下「職員等」という。）及び委託事業者とする。

４　職員等及び委託事業者の義務

職員等及び委託事業者は、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は、情報セキュリティに関係する法令等、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する義務を負うものとする。

５　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、情報資産を脅かす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次のとおりである。

（１）　部外者の侵入、不正アクセス、ウイルス攻撃やサービス不能攻撃等のサイバー攻撃、機器の盗難、情報資産の不正な操作や持ち出し等の故意による情報資産の漏えい・破壊・改ざん・消去等

（２）情報資産の管理不備、無許可ソフトウェア使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、ネットワークの誤接続、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、機器故障等の過失による情報資産の漏えい・破壊・改ざん・消去等

（３）地震、落雷、火災、水害等の災害及び大規模・広範囲にわたる疾病による要員不足に伴うサービス及び業務の停止等

（４）災害の影響又はその他原因による電力、通信、水道の途絶等のインフラの障害に伴うサービス及び業務の停止等

６　情報セキュリティ対策

上記５で示した脅威から情報資産を保護するために、以下の対策を講ずるものとする。

（１）組織体制

本市の情報資産を守るため、適切に情報セキュリティ対策を推進・管理するため

の体制を確立するものとする。

（２）情報資産の分類と管理

情報資産をその重要性に応じて分類し、その分類に基づき情報セキュリティ対策を行うものとする。

（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ずる。

（ア）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。

（イ）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。

（ウ）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として、県及び市町村のインターネットとの通信を集約した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対策

情報システムを設置する管理区域への不正な立入り、及び情報資産を損傷、盗難等から保護するために物理的対策を講ずる。

（５）人的セキュリティ対策

情報セキュリティに関して職員等が遵守すべき事項を定め、職員等及び委託事業者に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人的対策を講ずる。

（６）技術的セキュリティ対策

情報資産を不正アクセスやコンピュータウイルス等から保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術的対策を講ずる。

（７）運用におけるセキュリティ対策

情報資産の管理、情報セキュリティ対策の遵守状況の確認及び外部サービスを利用する際のセキュリティ確保等運用面の対策を講ずる。また、緊急事態が発生した際に迅速かつ適切な対応を可能とするため、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

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ずる。

外部サービス（クラウドサービス）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ずる。

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。

7　情報セキュリティ対策基準の策定

本市の様々な情報資産について、上記６の情報セキュリティ対策を講ずるに当たっては、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ため、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。

なお、情報セキュリティ対策基準は、公開することにより本市の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

8　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確実に実施するため、個々の情報資産について具体的な遵守事項と実施手順を明記し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、公開することにより本市の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

9　情報セキュリティ研修の実施

情報セキュリティポリシーの運用を徹底するため、職員等及び委託事業者に十分な教育及び啓発が実施できるように必要な対策を講ずるものとする。

１０　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が遵守されていることを確認するため、定期的に自己点検を行い、必要に応じて情報セキュリティ監査を行う。

１１　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等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、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に必要に応じて、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、リスクを検討したうえで、情報セキュリティポリシーの見直しを行う。

施行日　平成２７年１０月５日