秦野市情報セキュリティポリシー
（基本方針）

令和５年４月

秦　　野　　市

秦野市情報セキュリティポリシー（基本方針）

１　目的

秦野市情報セキュリティポリシー（以下「ポリシー」という。）は、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ため、組織を挙げて情報セキュリティの確保に取り組み、市民に信頼される市政運用の進展を図ることを目的とする。

本ポリシーは、情報セキュリティ維持のために統一的な方針を示す秦野市情報セキュリティポリシー（基本方針）（以下「基本方針」という。）と、技術の進歩等情報資産を取り巻く最新の状況に対応した基準を示す秦野市情報セキュリティポリシー（対策基準）（以下「対策基準」という。）に分けて策定する。

２　定義

ポリシーにおいて、次の各号に掲げる用語の意義は、それぞれの各号に定めるところによる。

(1)　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確保し、維持することをいう。

(2)　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。

(3)　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。

(4)　可用性

情報にアクセスすることを認められた者が、必要な時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。

(5)　行政情報

本市の特別職（市議会議員を除く）及び一般職の職員（常勤職員、再任用職員、会計年度任用職員等の任用形態、職位を問わない。以下「職員等」という。）が職務上作成し、又は取得した情報で、その記録媒体の形態に関わらず本市が管理しているものをいう。

(6)　個人情報

行政情報のうち、個人又は法人その他の団体に関する情報で、特定の個人又は法人その他の団体が識別され、又は識別され得るものをいう。

(7)　特定個人情報

行政手続き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条第８項に規定する特定個人情報をいう。

(8)　個人番号利用事務
　　番号法第２条第１０項に規定する個人番号利用事務をいう。
(9)　個人番号関係事務
　　番号法第２条第１１項に規定する個人番号関係事務をいう。
(10) 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、これら一部又は全体で情報処理を行う仕組みをいう。
(11) 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。

３　対象範囲
(1)　対象組織
　　ポリシーが対象とする組織は、市長部局、上下水道局、議会局、農業委員会事務局、監査事務局、選挙管理委員会事務局、教育委員会事務局、各教育機関及び消防本部とする。
(2)　対象情報資産
　　ポリシーが対象とする情報資産は、次のとおりとする。
　ア　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
　イ　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。）
　ウ　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
　エ　特定個人情報（印刷した文書を含む。）
(3)　対象者
　　ポリシーが対象とする者は、職員等とする。

４　職員等及び外部委託事業者の義務
　職員等は、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　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。

５　情報セキュリティ管理体制
　本市の情報資産に関する情報セキュリティ対策を、組織として統一された意思の下に、継続的に実施するため、幹部職員が率先して推進、管理する体制を確立する。

６　情報セキュリティ対策の実施

(1)　情報資産の分類

本市の情報資産を、機密性、完全性及び可用性に応じて分類し、当該分類に基づきその重要度に応じた情報セキュリティ対策を実施する。

(2)　対象とする脅威

本市の情報資産の情報セキュリティを維持する上で、特に認識すべき脅威は次のとおりである。

ア　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、部外者の侵入等の意図的な要因による機器又は情報資産の漏えい・破壊・改ざん・消去及び重要情報の詐取等

イ　情報資産の不適切な持ち出し又は利用、搬送中の事故、認証情報（パスワード等）の不適切な管理、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、業務委託管理の不備、マネジメントの欠陥及び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

ウ　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

エ　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

オ　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によるサービスおよび業務の停止等

(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。

ア　個人番号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、原則として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、神奈川県及び県内市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。

なお、各教育機関等におけるインターネットと通信するネットワークについては、接続形態に応じて、不正アクセスやマルウェア対策の実施

及びファイル暗号化等による安全管理措置を講じること。

(4)　情報セキュリティ対策

本市の情報資産を(2)で示した脅威から保護するため、次の情報セキュリティ対策を実施する。

ア　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、妨害等から保護するため、物理的な対策を実施する。

イ　人的セキュリティ対策

情報セキュリティに関する、権限、責任、職員等が遵守すべき事項を定めるとともに、職員等にポリシーの内容を周知徹底、十分な教育及び啓発が行われるよう必要な対策を実施する。

ウ　技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、不正プログラム対策、ネットワーク管理等の技術面の対策を実施する。

エ　運用におけるセキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報システムの監視、システム開発等の業務委託を行う際のセキュリティ確保、ネットワークの監視、ポリシー遵守状況の確認等、運用面の対策を実施する。

また、緊急事態が発生した際に迅速な対応を可能とするため緊急時対応計画を策定し、必要な危機管理対策を実施する。

(5)　業務委託と外部サービスの利用

業務委託する場合には、本市が情報資産の取扱いを含む業務を委託する者（以下「委託事業者」という。）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。

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。

7　情報セキュリティに関する文書の整備

(1)　対策基準の策定

本基本方針に基づく情報セキュリティ対策を実施するために、本市において遵守すべき行為、判断等の基準を統一的なレベルで定め、情報セキュリティ対策の基本的な要件を明記した対策基準を策定する。

(2)　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、本市の所

管する個々の情報資産の管理、利用等に関する取扱い手順等を、それぞれの情報資産に対する脅威及び重要度に対応する対策基準の基本的な要件に基づいて取りまとめ、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。

(3)　情報セキュリティに関する文書の取扱い

対策基準及び実施手順は、公にすることにより本市の情報セキュリティの維持に支障が生じるおそれがあるため、非公開とする。

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評価及び見直し

情報セキュリティ監査及び自己点検の結果等により、ポリシーに定める事項及び情報セキュリティ対策の有効性等について評価するとともに、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、適宜ポリシーの見直しを実施する。