上野原市情報セキュリティポリシー
【第３版】

平成 20 年 10 月１日策定
令和 6 年 4 月１日改定

上野原市

制定・改定履歴

版数	内容	施行日
１	初版策定	平成２０年１０月１日
２	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の施行による改定	平成２８年１月４日
３	総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」改定に伴う改定及び部長制廃止に伴う改定	令和６年４月１日

注意事項
１　本ポリシーを総務課情報推進担当のキャビネットにて保管する。
２　本ポリシーの版番号は、新規制定を第１版とし、改定ごとに版数を整数で重ねる。
３　本ポリシーを一部改定したときは、当該一部改定に係る部分を加除方式により差し替える。
４　本ポリシーを全部改定したときには、改定後のポリシーに全てを差し替える。
５　ポリシーの改定の都度、改定履歴を記載したものと差し替える

目次

第１章　総則

１　上野原市情報セキュリティポリシー

上野原市情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）とは、上野原市（以下「本市」という。）が保有する情報資産に関する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る。

情報セキュリティポリシーは、本市の情報資産、情報資産を取り扱う職員、会計年度任用職員、その他本市の事務に携わる者（以下「職員等」という。）に浸透、普及、定着させるものであり、安定的な規範であることが要請される。また、情報の処理技術や通信技術等の進歩や新たな脅威に対応すべく、情報セキュリティポリシーの評価・見直しを行い、情報セキュリティ対策の実効性を確保する必要がある。

２　本市における情報セキュリティの考え方

本市は、法令等に基づき、住民の個人情報や企業の経営情報等の重要情報を多数保有するとともに、他に代替することができない行政サービスを提供している。また、本市の業務の多くが情報システムやネットワークに依存していることから、住民生活や地域の社会経済活動を保護するため、情報セキュリティ対策を講じて、その保有する情報を守り、業務を継続することが必要となっている。

今後、各種手続のオンラインや情報システムの高度化等、電子自治体が進展することにより、情報システムの停止等が発生した場合、広範囲の業務が継続できなくなり、住民生活や地域の経済社会活動に重大な支障が生じる可能性も高まる。また、ＬGWAN等のネットワークにより相互に接続しており、発生したＩＴ障害がネットワークを介して連鎖的に拡大する可能性は否定できない。

これらの事情から、情報セキュリティ対策の実効性を高めるとともに対策レベルを一層強化していくことが必要となっている。また、情報セキュリティの確保に絶対安全ということはないことから、情報セキュリティに関する事故の未然防止のみならず、事故が発生した場合の拡大防止・迅速な復旧や再発防止の対策を講じていくことが必要である。

３　情報セキュリティポリシーの構成

情報セキュリティポリシーの体系は、下表に示す階層構造となっている。

本市の情報セキュリティ対策における基本的な考え方を定めるものが、「基本方針」である。この基本方針に基づき、全ての情報システムに共通の情報セキュリティ対策の基準を定めるのが「対策基準」である。この「基本方針」と「対策基準」を総称して「情報セキュリティポリシー」という。この「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るものが「実施手順」である。

文書名		内容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティに関する統一的かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための、全ての情報資産に共通の情報セキュリティ対策の基準
情報セキュリティ実施手順		ネットワーク及び情報システムごとに定める情報セキュリティ対策基準に基づいた具体的な実施手順

表　情報セキュリティポリシーの構成

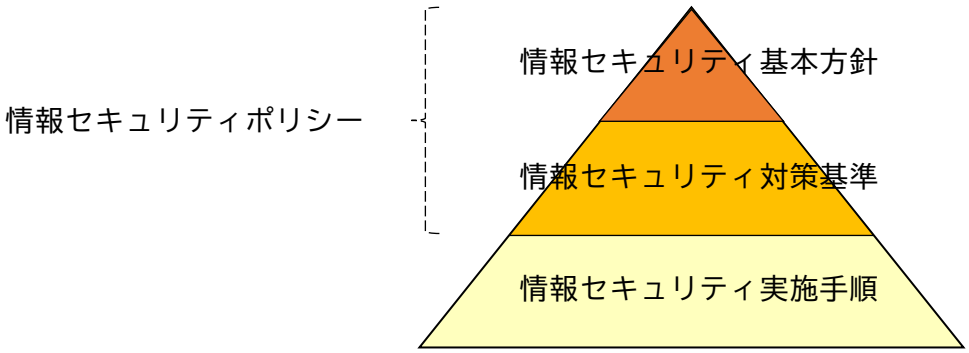

図　情報セキュリティポリシーの構成

４　情報セキュリティ対策の実施サイクル

　情報セキュリティ対策の実施プロセスは、下図のとおり、策定・導入（Ｐｌａｎ）、運用（Ｄｏ）、評価（Ｃｈｅｃｋ）、見直し（Ａｃｔｉｏｎ）の４段階に分けることができ、この実施サイクルを繰り返すことによって情報セキュリティは確保される。この実施サイクルは、それぞれの項目の頭文字をとって、ＰＤＣＡサイクルとも呼ばれる。

　情報セキュリティを取り巻く脅威や対策は常に変化しており、以上のＰＤＣＡサイクルは、一度限りではなく、これを定期的に繰り返すことで、環境の変化に対応しつつ、情報セキュリティ対策の水準の向上を図らなければならない。

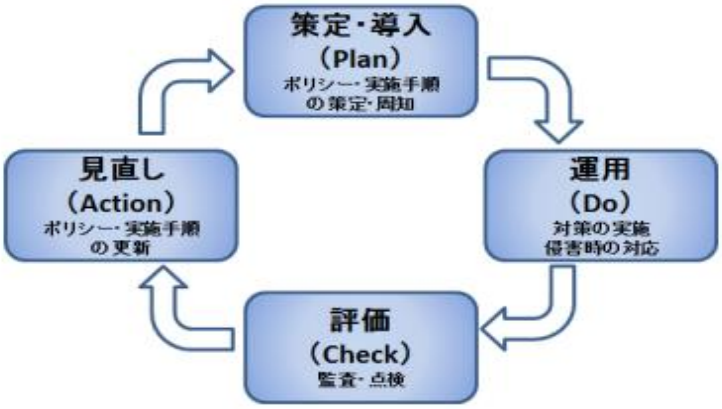

図　情報セキュリティ対策の実施サイクル

第２章　情報セキュリティ基本方針

１　目的

本基本方針は、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、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

（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、インターネット接続系、マイナンバー利用事務系（個人番号利用事務系）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）技術的脅威

不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入、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）物理的脅威

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要因による情報資産の漏えい・破壊・消去等

（３）災害等

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

（４）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

（５）インフラ障害

電力供給の途絶、通信の途絶等のインフラの障害からの波及等

４　適用範囲

（１）組織

本基本方針が適用される組織は、市長部局、会計課、議会事務局、教育委員会事務局、消防本部及びその他行政委員会事務局とする。

（２）対象者

本基本方針が適用される対象者は、本市の情報資産を取り扱う職員等とする。

（３）情報資産

本基本方針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、情報システム及びこれらに関する施設・設備、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及び関連する文書を含む。）

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

情報資産の種類	情報資産の例
ネットワーク	通信回線、ルータ等の通信機器
情報システム	サーバ、パソコン、モバイル端末、汎用機、オペレーティングシステム、ソフトウェア等
これらに関する施設・設備	コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル
電磁的記録媒体	サーバ機器、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、ＵＳＢメモリ、外付けハードディスクドライブ、ＤＶＤ－Ｒ、磁気テープ等の外部電磁的記録媒体
ネットワーク及び情報システムで取り扱う情報	ネットワーク、情報システムで取り扱うデータ（これらを印刷した文書及び関連する文書を含む。）
システム関連文書	システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等

表　情報資産の種類と例

５　情報セキュリティポリシーの位置づけ

情報セキュリティポリシーは、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。

６　職員等の遵守義務

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じる。

（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行う。

（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３段階の対策を講じる。

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

サーバ等、情報システム室、通信回線等及び職員等のパソコン等の管理について、物理的な対策を講じる。

（５）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等の人的な対策を講じる。

（６）技術的セキュリティ

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、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じるものとする。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切に対応するため、緊急時対応計画を策定する。

（８）業務委託と外部サービスの利用

ア　業務委託

業務委託を行う場合においては、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。

イ　外部サービス

外部サービスを利用する場合においては、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）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、適宜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、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

　上記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。

　なお、情報セキュリティ対策基準は、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。

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。

　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。