吉田町情報セキュリティ基本方針

令和５年４月１日

改版履歴

版数	作成日
第１版	平成１６年　３月２４日
第２版	平成２０年１０月２４日
第３版	平成２８年　１月　１日
第４版	令和　元年　９月　１日
第５版	令和　２年　４月　１日
第６版	令和　５年　４月　１日

序　文

情報セキュリティポリシーとは、組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた基本方針及び対策基準をいう。

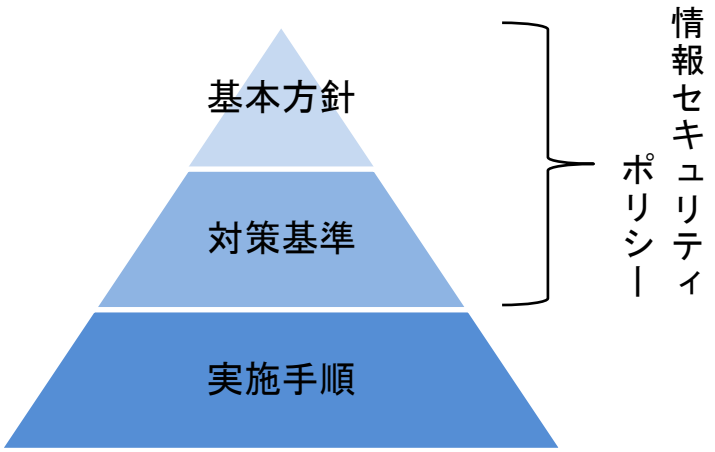
地方公共団体の取り扱う情報には、住民の個人情報のみならず行政運営上重要な情報が多数含まれており、これらが部外に漏えい、改ざんされた場合、極めて重大な結果を招くこととなる。このため、地方公共団体は、保有する情報資産を責任を持って保護していかなければならない。

行政手続等における情報通信の技術の利用に関する法律は、情報システムの安全性や信頼性の確保について規定しており、地方公共団体は、情報セキュリティポリシーの策定や見直しを行うことが求められている。

総務省では、地方公共団体における情報セキュリティポリシーの策定を推進するため、平成１３年３月に「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」を策定した。その後、情報セキュリティに関する状況の変化等を踏まえ、同ガイドラインを改定するとともに地方公共団体における情報セキュリティポリシーの見直しを推進している。

当町においては、同ガイドラインに基づき、平成１６年３月に「吉田町情報セキュリティ基本方針（第１版）」及び「吉田町情報セキュリティ対策基準（第１版）」を策定し、その後、同ガイドラインの改定にあわせ、必要に応じ、見直しを行っているが、情報セキュリティ対策の更なる実効性を確保するとともに、対策レベルを高めていくことを目的として、今回「吉田町情報セキュリティポリシー」を改定した。

今後も引き続き、情報の処理技術や通信技術等の進展に伴う急速な状況の変化に柔軟に対応していかなければならないが、この度策定した情報セキュリティポリシーにより、当町の全職員が情報の重要性を再認識するとともに、各部門において情報管理の枠組みを明確に定め実践していくことが重要である。



1　目的

吉田町情報セキュリティ基本方針（以下「基本方針」という。）は、当町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、当町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ものとする。

2　定義

(1)　情報資産

ア　ネットワーク、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

(2)　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（ハードウエア及びソフトウエア）をいう。

(3)　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。

(4)　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。

(5)　情報セキュリティポリシー

基本方針及び吉田町情報セキュリティ対策基準（以下「対策基準」という。）をいう。

(6)　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。

(7)　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。

(8)　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。

(9)　基幹系（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。

(10)　情報系（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（基幹系を除く）。

(11)　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。

(12)　通信経路の分割

情報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。

(13)　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　情報資産に関する脅威

情報資産に関する脅威として、以下の脅威を想定し、情報セキュリティ対策を講ずる。

(1)　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

(2)　情報資産の無断持ち出し、無許可ソフトウエ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、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・改ざん・消去等

(3)　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)　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)　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

4　実施機関

本基本方針が適用される実施機関は、町長(公営企業管理者の権限を含む。)、議会、教育委員会、選挙管理委員会、監査委員、農業委員会及び固定資産評価審査委員会とする。

5　職員等の遵守義務

職員及び非常勤職員等（以下「職員等」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。

6　情報セキュリティ対策

前記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ずる。

(1)　組織体制

当町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

当町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適正に分類し､情報の紛失や流出等を防止するための情報セキュリティ対策を講じ、管理する。

(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。

ア　基幹系においては、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　情報系においては、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、電算室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講ずる。

(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ずる。

(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ずる。

(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。また、情報資産への侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応マニュアルを策定する。

(8)　業務委託及び外部サービスの利用

ア　　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。

イ　　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。

ウ　　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。

7　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。

8　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となった場合には、情報セキュリティポリシーを見直すこととする。

9　対策基準の策定

前記６、７及び８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当町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。

10　情報セキュリティ実施手順の策定

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。

なお、情報セキュリティ実施手順は、公にすることにより当町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。