添田町情報セキュリティポリシー

平成１４年２月策定
平成２９年６月改定

総務課　研修・情報推進係

添田町情報セキュリティポリシーの改定について

本町では平成１４年から「添田町情報セキュリティポリシー」を策定し、情報資産の安全対策の推進、安定的な行政運営に取り組んできた。

今日の情報社会では、インターネットをはじめＩＣＴの活用が増加する等、生活が便利になる一方、個人情報の漏えい、サイバー攻撃による不正アクセス等の情報資産の破壊・改ざんなどの被害は後を絶たない。

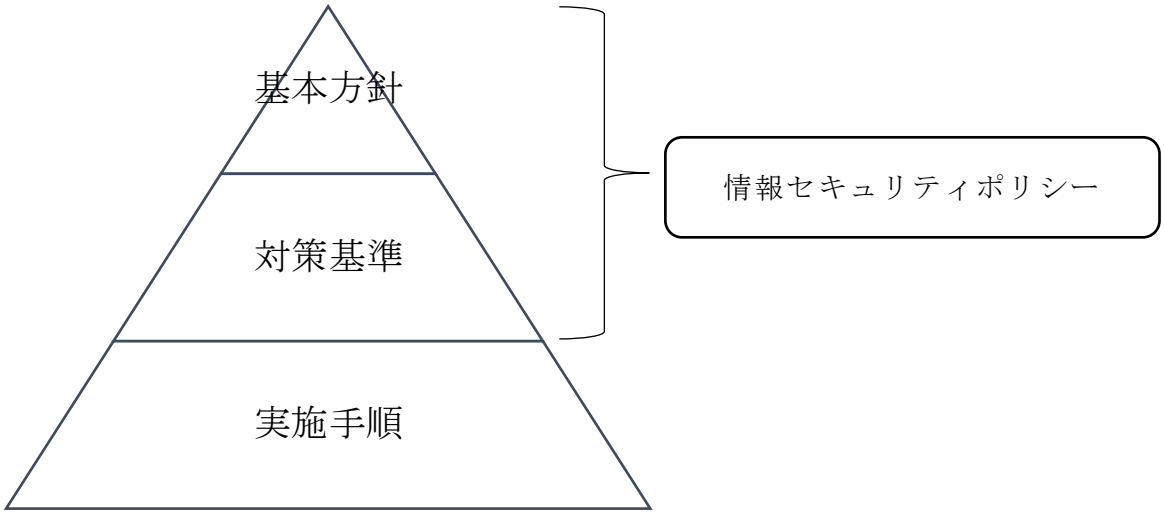
このように、社会経済活動の情報化が進展する中で、情報セキュリティへの脅威が拡大している。

本町の業務にも、住民の個人情報や行政運営上重要な情報等を多数取り扱うものがあり、それらの多くが情報システムやネットワークに依存しているため、この情報資産をさまざまな脅威から防御することは、住民の権利、利益を守るためにも、行政の安定的、継続的な運営のためにも必要不可欠になっている。

そのため、社会保障・税番号制度の導入を踏まえ、情報セキュリティ対策の一層の強化を図るため、「添田町情報セキュリティポリシー」を改定した。

なお、「対策基準」及び「実施手順」は公開することにより本町の行政運営に重大な支障を及ぼす恐れがありますので非公開とする。

情報セキュリティポリシーの構成



文書名	内　容
情報セキュリティ基本方針	情報セキュリティ対策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システムに共通の情報対策の基準。
情報セキュリティ実施手順	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。

添田町情報セキュリティ基本方針

１　目的

添田町情報セキュリティ基本方針（以下「基本方針」という。）は、添田町（以下「町」という。）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、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ことを目的とする。

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、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、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

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及びそれ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及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及びそれを確保することをいう。

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）　不正アクセス、ウイルス攻撃、サービスの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、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、外部委託管理の不備、マネージメントの欠陥、機器故障等の非意図的な要因による情報資産の漏えい・破壊・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等による要因不足に伴う情報システム運用の機能不全等

（５）　電力供給の途絶、通信の途絶等のインフラの障害からの波及等

４　対象範囲

（１）　行政機関の適用範囲

基本方針が対象とされる行政機関の範囲は、町長、教育委員会、選挙管理委員会、農業委員会、監査委員、固定資産評価審査委員会、水道事業の管理者の権限を行う町長及び議会とする。ただし、教育委員会所管の学校は除く。

（２）　情報資産の対象範囲

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、情報システム及びこれらに関する設備、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章を含む）
③　情報システムの仕様書及びネットワークの図等の情報システム関連文書
④　添田町文書規定(平成 26 年)に規定する文書

５　職員等の遵守義務

職員、非常勤職員及び臨時的任用職員（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

上記３の脅威から情報資産及び情報システムを保護するために、以下の情報セキュリティ対策を講じる。

（１）　組織体制

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し、権限、役割及び責任の明確化を図る。

（２）　情報資産の分類と管理

本町の保有する情報資産を機密性、完全性及び可用性の観点で分類し、当該分類に基づき情報セキュリティ対策を行う。

（３）　物理的セキュリティ

サーバ等、電算室等、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。

（４）　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。

（５）　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な対策を講じる。

（６）　運用

情報システム監視、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情報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敏速かつ適切に対応するため、緊急対応計画を策定する。

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になった場合には、情報セキュリティポリシーを見直す。

９　情報セキュリティ対策基準の策定

上記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、情報セキュリティ実施基準は、公にすることにより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

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。