仁淀川町情報セキュリティポリシー

仁淀川町情報セキュリティ委員会

〈 目　　次 〉

序　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文書をいう。

仁淀川町における情報セキュリティは、町が保有する情報資産に自ら責任を持って確保すべきものであり、情報セキュリティポリシーは、その業務に携わる職員、特別職（※地方公務員法(昭和25年法律第261号)第３条に規定する職員）、非常勤職員、会計年度任用職員（以下、「職員等」という。）及び外部委託業者に浸透、普及、定着させ安定的な規範となるものである。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化への柔軟な対応も必要である。

このようなことから、情報セキュリティポリシーを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「基本方針」と、それに基づき、すべ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「対策基準」に分けて策定することとした。

具体的には、セキュリティポリシーを、

○　情報セキュリティ基本方針

○　情報セキュリティ対策基準

の２階層に分け、それぞれ策定することとする。また、情報セキュリティ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情報セキュリティ実施手順の策定も必要である。

情報セキュリティポリシーの構成

文　書　名		内　容
情報セキュリティポリシー	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、すべての情報システム共通の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毎に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。

なお、情報セキュリティ対策基準、情報セキュリティ実施手順は、公にすることにより本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。

第１章　情報セキュリティ基本方針

１　目的

本基本方針は、仁淀川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、本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。

(2) 情報システム

コンピュータ、ネットワーク及び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、災害対策に関する事務）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。

(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。

(13) テレワーク

情報通信技術(ICT = Information and Communication Technology)を活用した、場所や時間にとらわれない柔軟な働き方のことであり、当町においては、在宅勤務、モバイルワークをいう。

(14) 情報セキュリティインシデント

望ましくない単独若しくは一連の情報セキュリティ事象又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

(15) 端末

情報システムの構成要素である機器のうち、情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボード、マウス等の周辺機器を含む。）をいう。

(16) パソコン

端末のうち、机の上等に備え置いて業務に使用することを前提とし、移動させて使用することを目的とはしていないものをいい、端末の形態は問わない。

(17) モバイル端末

端末のうち、業務上の必要に応じて、移動させて使用することを目的としたものをいい、端末の形態は問わない。

(18) 電磁的記録媒体

コンピュータによる情報処理に使用する、電子的又は電磁的な記録方式により作成された記録を保持するための媒体。ハードディスク、CD、DVD、USBメモリ、SDカード、コンパクトフラッシュ、フロッピーディスク、磁気テープ類等をいう。

(19) サーバ室

ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理並びに運用を行うための部屋をいう。

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、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) 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　適用範囲

(1) 行政機関の範囲

本基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局、地方公営企業及び議会とする。

(2) 情報資産の範囲

本基本方針が対象とする情報資産は、以下を含む本町が保有する全ての資産とする。

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（これらを印刷した文書を含む。）

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

④紙文書

5　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。

6　職員等の処分等

(1) 職員等の処分

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、職員の処分を仁淀川町職員処分審議委員会に委任する。

(2) 違反時の対応

職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やか

に次の措置を講じる。

①統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な措置を求める。

②情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括情報セキュリティ責任者及び当該職員等が所属する課室等の情報セキュリティ管理者に報告し、適正な措置を求める。

③情報セキュリティ管理者の指導によっても改善されない場合、統括情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、統括情報セキュリティ責任者は、職員等の権利を停止あるいは剥奪した旨を CISO 及び当該職員等が所属する課室等の情報セキュリティ管理者に通知する。

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管理運営組織体制を確立する。

(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、次の三段階の対策を講じる。

①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するが、仮想環境及びUSB等機器との接続が必要なシステム等については仮想環境で運用できないため物理端末で運用を行う。その際、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。

②LGWAN 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。

③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、高知県及び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。

(4) 物理的セキュリティ

サーバ、情報システム室、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) 外部サービスの利用

外部委託する場合には、外部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、外部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。

約款によ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。

(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。

ただし、情報セキュリティポリシーの見直しは、本部会議で決定するものとするが、簡易な見直しについては、CISO の通知により行う。

8　テレワークの実施

仁淀川町情報セキュリティポリシーに基づき、情報セキュリティリスクを明確にし、テレワーク実施のための運用方法、順守事項を策定する。

9　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。

なお、セキュリティチェックについては、本町が確認する項目において、外部委託業者の報告書を活用することができる。

10　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。

11　情報セキュリティ対策基準の策定

上記６、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。

12　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。