平泉町情報セキュリティポリシー
情報セキュリティ基本方針

目次

序　情報セキュリティポリシーの必要性と構成

町は、法令等に基づき、住民の個人情報や企業の経営情報等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、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、その保有する情報資産を守り、業務を継続することが必要となってくる。

そのために、町は、情報セキュリティポリシーを策定し、情報セキュリティを確保するための方針、体制、対策等を体系的かつ具体的に定めるものとする。

情報セキュリティポリシーは、町の基本的な考え方を定めた「基本方針」と、保有する情報資産の取扱い、及び全てのネットワーク、情報システムに共通する情報セキュリティ対策の基準を定めた「対策基準」とで構成するものとする。

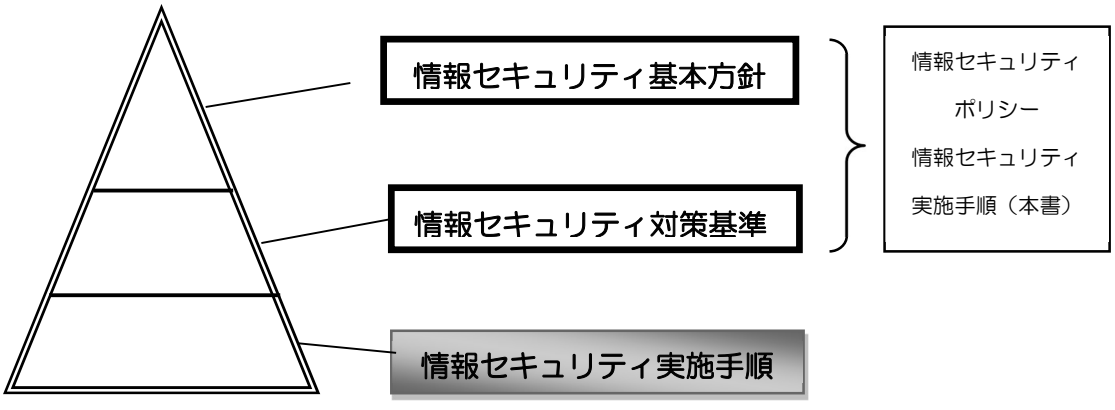
また、「対策基準」に基づき具体的なシステムや、手順、手続きに展開して「実施手順」として個別の実施事項を定めるものとする。

なお、本情報セキュリティポリシーの範囲は、「基本方針」と「対策基準」である。

情報セキュリティポリシーは、情報セキュリティ対策の頂点に位置するものであることから、すべての職員等及び外部委託事業者は、業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負うものとする。

情報セキュリティポリシーに関する体系

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保有する情報資産の取扱い、及び全てのネットワーク、情報システム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毎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。



第1章　情報セキュリティ基本方針

1　目的

本基本方針は、第4第1号に掲げるものが保有する情報システム、情報資産及び記録媒体を様々な脅威から保護し、機密性、 完全性及び可用性を維持するため、情報セキュリティに関する対策の統一的かつ基本的項目を定めるものとする。

2　定義

この訓令において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

(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) 記録媒体　電子計算機に使用される電子的方式、磁気的方式又は光学的方式その他人の知覚によっては認識することができない方式で作られたデータを記録するための機器媒体をいう。

(4) 情報資産　電子的、磁気的又は光学的に記録された情報(以下「情報」という。)及び情報を管理する仕組み(以下「プログラム」という。)の総称をいう。

(5) 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。

(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) 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。

(10) 情報セキュリティ基本方針　情報セキュリティを維持する方策に関する根本的な事項を定めたものをいう。

(11) 情報セキュリティ対策基準　情報セキュリティ基本方針に基づき、情報セキュリティの維持のために遵守すべき行為及び判断を示したものをいう。

(12) 情報セキュリティ実施手順　情報セキュリティ対策基準に基づき、情報システム及びこれを使用する業務において、どのような手順を実行していくかを示したものをいう。

(13) 不正アクセス　不正アクセス行為の禁止等に関する法律(平成11年法律第128号)第3条第2項各号に規定する行為をいう。

(14) 不正操作　正規のアクセス権を持たない人が、意図する意図しないにかかわらず本来の目的以外及び手法でコンピュータを利用することをいう。

(15) ウィルス　他人のコンピュータに勝手に入り込み、不具合を生じさせるプログラムをいう。

(16) 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。

(17) LGWAN 接続系　人事給与、財務会計及び文書管理等 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。

(18) 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。

(19) 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。

(20) 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)　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

この訓令の対象範囲は、次のとおりとする。

(1)　行政機関の範囲　対象となる組織は、平泉町のすべての執行機関、議会事務局及び公営企業(以下「町等」という。)とする。　また、対象となる者は、町等の情報資産を取り扱うすべての職員（非常勤職員及び会計年度任用職員等を含む）、契約に基づき情報資産を取り扱う外部委託業者その他の者(以下「職員等」という。)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、 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

5　職員等の遵守義務

職員等（職員、非常勤職員及び会計年度任用職員等をいう。以下同じ。）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するものとする。

6　情報セキュリティ対策

第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実施する。

(3)　情報システム全体の強靭性の向上　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。

② 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。

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、都道府県と市区町村のインターネット接続口を集約した上で、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。

(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正に対応するため、情報セキュリティインシデント対応要領を策定する。

(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。

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、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

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。

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。