

# 竜王町 情報セキュリティポリシー

平成18年12月25日 策定  
令和8年3月31日 改定

# 序章

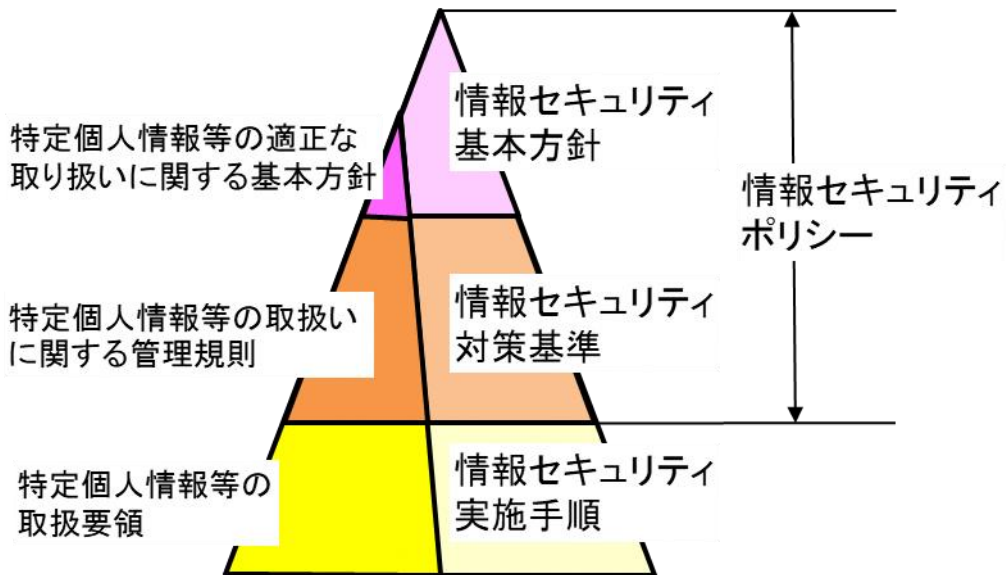
情報セキュリティポリシーとは、本町が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものである。情報セキュリティポリシーは、本町が所掌する情報資産に関する業務に携わる全ての職員および外部委託事業者に浸透、普及および定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分(情報セキュリティ基本方針)と情報資産を取り巻く状況の変化に依存する部分(情報セキュリティ対策基準)に分けて策定する。

また、情報セキュリティポリシーに基づき、情報システム毎等の具体的な情報セキュリティ対策を示す手順として情報セキュリティ実施手順を策定することとする(下表参照)。

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かつ基本的な方針を定めるもの
	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、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もの
情報セキュリティ実施手順		情報セキュリティ対策基準を具体的なシステムや手順、手続きに展開して個別の実施事項を定めるもの

なお、特定個人情報(マイナンバー)等の取扱いに関しては、より厳格な保護措置を定める必要があるため、特定個人情報等の適正な取扱いに関する基本方針、特定個人情報等の取扱いに関する管理規則、特定個人情報等の取扱要領等を別途定めることとする。



## 目 次

### 情報セキュリティ基本方針

第1条 目的	1
第2条 定義	1
第3条 対象とする脅威	1
第4条 適用範囲	2
第5条 職員等の遵守義務	2
第6条 情報セキュリティ対策	2
第7条 情報セキュリティ監査および自己点検の実施	3
第8条 情報セキュリティポリシーの見直し	3
第9条 情報セキュリティ対策基準の策定	3
第10条 情報セキュリティ実施手順の策定	3

# 情報セキュリティ基本方針

(目的)

## 第1条

本基本方針は、本町が保有する情報資産の機密性、完全性およ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。

(定義)

## 第2条

このセキュリティポリシーにおいて、次の各号に掲げる用語の意義は、それぞれ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(ハードウェアおよびソフトウェア)をいう。
- (2) 情報システム  
コンピュータ、ネットワークおよ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、完全性およ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  
本基本方針およ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、改ざんまた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) 基幹系  
個人番号利用事務(社会保障、地方税もしくは防災に関する事務)または戸籍事務等に関わる情報システムおよびデータをいう。
- (9) 内部事務系  
LGWANに接続された情報システムおよ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。)
- (10) インターネット系  
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およ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  
内部事務系ネットワークとインターネット系ネットワーク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。

(対象とする脅威)

## 第3条

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および業務の停止等
- (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

(適用範囲)

第4条

本基本方針の適用範囲は次の各号に定めるところによる。

(1) 行政機関の範囲

本基本方針が適用される行政機関は、町長部局、教育委員会事務局、選挙管理委員会事務局、公平委員会事務局、監査委員事務局、農業委員会事務局、固定資産評価審査委員会事務局および議会事務局(以下併せて「内部部局」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。

ア ネットワークおよび情報システムならびにこれらに関する設備および電磁的記録媒体

イ ネットワークおよ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およびネットワーク図等のシステム関連文書

(職員等の遵守義務)

第5条

職員、臨時・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およ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。

(情報セキュリティ対策)

第6条

上記第3条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、完全性およ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靱性の向上

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 基幹系ネットワークにおいては、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 内部事務系ネットワークにおいては、LGWAN と接続する業務用システムと、インターネット系ネットワーク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 インターネット系ネットワークにおいては、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行う。高度な情報セキュリティ対策として、都道府県およ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、サーバ室、通信回線およ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、十分な教育およ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、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、緊急時対応計画を策定する。

(8) 業務委託と外部サービス(クラウドサービス)の利用

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。

外部サービス(クラウドサービス)を利用する場合には、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、定期的または必要に応じて情報セキュリティ監査およ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。

(情報セキュリティ監査および自己点検の実施)

第7条

情報セキュリティポリシーの遵守状況を検証するため、定期的または必要に応じて情報セキュリティ監査および自己点検を実施する。

(情報セキュリティポリシーの見直し)

第8条

情報セキュリティ監査および自己点検の結果、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およ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、保有する情報および利用する情報システムに係る脅威の発生の可能性および発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーの見直しを行う。

(情報セキュリティ対策基準の策定)

第9条

上記第6条、第7条および第8条に規定する対策等を実施するために、具体的な遵守事項およ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、対応基準については、公表することにより本町の行政運営に重大な支障をおよぼすおそれがあることから、非公表とする。

(情報セキュリティ実施手順の策定)

第10条

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およぼすおそれがあることから非公表とする。