蔵王町情報セキュリティポリシー

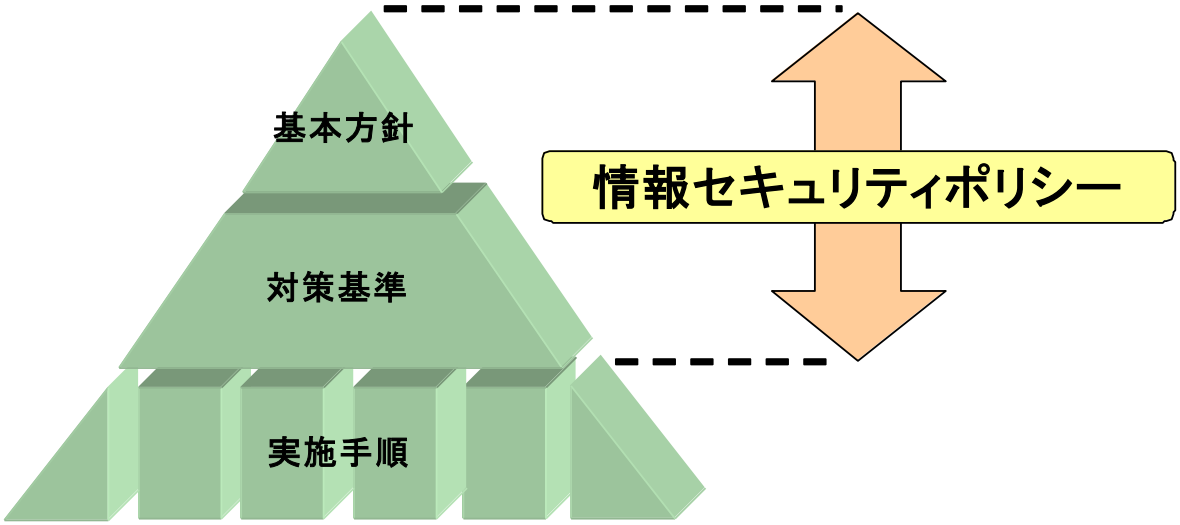
平成１６年　４月　制　　定
平成２７年１０月　一部改定
平成２７年１２月　一部改定

目　　次

序　蔵王町情報セキュリティポリシーの体系

情報セキュリティポリシーとは、蔵王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を総称する。情報セキュリティポリシーは、蔵王町が所掌する情報資産に関する業務に携わる全職員、非常勤、臨時職員(以下「職員等」という。)及び外部委託事業者に浸透、普及、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(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(対策基準)に分けて策定することとした。具体的には、情報セキュリティポリシーを、情報セキュリティ基本方針と情報セキュリティ対策基準の２階層に分け、それぞれを策定することとする。また、情報セキュリティポリシーに基づき、情報システム毎の具体的な情報セキュリティ対策の実施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。



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	基本方針を実行するための、全てのネットワーク、情報システム等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	対策基準をもとに、各課や情報システムごとに定める具体的なセキュリティ対策手続。

(蔵王町情報セキュリティポリシー体系図)

第１章　　情報セキュリティ基本方針

１　目的

蔵王町は、住民の皆様のために、生活環境の改善や産業、教育、福祉、医療、災害対策などのあらゆる生活の場面において、さまざまな行政サービスを展開しています。こうしたサービスはひと時も休むことが許されず、継続的に運営していく必要があります。

一方、近年のインターネットを中心とした情報通信技術の発展はめざましく、情報技術の活用によって行政サービスの利便性や効率性の向上等多くのメリットが期待できる反面、情報の改ざんや漏えいを目的とした不正アクセスやコンピュータウイルスといった様々な脅威が存在し、行政サービスの提供が脅かされています。

蔵王町ではこうした脅威から情報資源を保護し、住民の皆様の信頼確保と安定した行政サービスの提供を目的に、全組織、全職員一人ひとりが扱う情報の保護において取り組む基準を定めると共に、その継続的な遵守の決意表明として、ここに「情報セキュリティポリシー」（以下「ポリシー」）を定めることとしました。

２　定義

ポリシーにおいて、次の各号に掲げる用語の意義は、それぞれの各号に定めるところによる。

(1) 組織等に関する用語の定義

① 課等

「蔵王町行政組織規則」（平成６年規則第 16 号）に規定する課、「蔵王町教育委員会組織規則」（平成８年教委規則第２号）に規定する課等、「蔵王町議会事務局設置条例」（昭和 36 年条例第 72 号）に規定する事務局、「蔵王町選挙管理委員会規程」（昭和 32 年選管規程第７号）に規定する事務局、「蔵王町農業委員会規程」（昭和 50 年農委規程第１号）に規定する事務局、「蔵王町水道事業の設置等に関する条例」（昭和 61 年条例第 29 号）に規定する事業所、及び「蔵王町国民健康保険蔵王病院管理規程」（平成６年規程第１号）に規定する事務局をいう。

② 職員等

常勤職員、非常勤職員、臨時職員等の任用形態、職位を問わず、本町の全職員をいう。

③ 外部委託業者

町と委託契約等によって定められた範囲で町の業務を受託する者をいう。

(2) 情報資産等に関する用語の定義

①情報資産

行政情報及び情報システムをいう。

②情報セキュリティ

情報資産の機密性（情報にアクセスできる状態を確保することをいう。）、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。）及び可用性(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。)を確保し、維持することをいう。

③ 行政情報

職員等が職務上作成又は取得した情報で、その記録媒体の形態に関わらず本町が管理しているものをいう。

④ 個人情報

行政情報のうち、個人又は法人その他の団体に関する情報で、特定の個人又は法人その他の団体が識別され、又は識別され得るものをいう。

⑤ アクセス権限

情報資産を利用することのできる範囲をいう。

(3) 情報システム等に関する用語の定義

① 情報システム

ハードウェア、ソフトウェア、ネットワーク、電磁的記録媒体等で構成され、これら一部又は全体で情報処理を行う仕組みをいう。

② ハードウェア

電子的にデータを処理する機能を持ち、事務処理に使用する機器をいう。

③ ソフトウェア

ハードウェア上で稼働するプログラム等をいう。

④ 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。

⑤ 電磁的記録媒体

行政情報の記録、管理に使用される磁気ディスク、磁気テープ、光ディスク等をいう。

⑥ サーバ

情報システムのうち、ネットワーク上においてファイル管理、印刷等の機能を提供するために設置される機器をいう。

⑦ クライアント

情報システムのうち、ネットワーク上においてデータの入力、更新、検索、出力等の操作を行うための機器をいう。

⑧ 庁内ネットワーク

情報システムのうち、本町の所管する施設内に敷設されたネットワークをいう。

⑨ 外部ネットワーク

情報システムのうち、電気通信事業者が提供する各種情報通信網等を通じ、複数のネットワークを接続する機能を持った機器を用いることにより、庁内ネットワークに接続することが可能なネットワークをいう。

⑩ ネットワーク機器

情報システムのうち、ネットワークを構成するケーブル及びネットワーク制御装置等の機器並びに附帯設備をいう。

3　適用範囲

(1) 組織の範囲

ポリシーが対象とする組織は、2.定義(1)に定める課等とする。

(2) 情報資産の範囲

ポリシーが対象とする情報資産は、(1) に定める組織において行政事務を処理するために取扱う全ての情報資産とする。

(3) 適用者

ポリシーの適用者は、(2) に定める情報資産を取扱う全ての職員等及び外部委託業者を対象とする。

4　職員等及び外部委託事業者の義務

職員等及び外部委託事業者は、情報セキュリティの重要度について共通の認識を持つとともに、業務の遂行に当たってポリシーを遵守する義務を負う。

5　情報セキュリティ対策

(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行う。

(3) 情報資産への脅威

本町の情報資産の情報セキュリティを維持する上で、特に認識すべき脅威は次のとおりである。

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。

② 職員等又は外部委託事業者による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、搬送中の事故等による機器又は情報資産の盗難、規定外の端末接続によるデータ漏えい等。

③ 地震、落雷、火災等の災害及び事故、故障等によるサービス及び業務の停止。

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) 情報セキュリティ対策

本町の情報資産を(3) で示した脅威から保護するため、次の情報セキュリティ対策を実施する。

① 物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷、妨害等から保護するため、物理的な対策を実施する。

② 人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、全ての職員等及び外部委託事業者にポリシーの内容を周知徹底する等、十分な教育及び啓発が行われるよう必要な対策を実施する。

③ 技術的セキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策を実施する。

④ 運用におけるセキュリティ対策

情報資産を不正なアクセス等から適切に保護するため、システム開発等の外部委託、ネットワークの監視、ポリシー遵守状況の確認等、運用面の対策を実施する。

また、情報資産に対するセキュリティ侵害が発生した際に迅速かつ適切に対応するため、緊急時対応計画を実施する。

6　情報セキュリティに関する文書の整備

(1) 情報セキュリティ対策基準の策定

情報セキュリティ基本方針に基づく情報セキュリティ対策等を実施するために、本町において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。

(2) 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。

7　ポリシー違反時の対応

ポリシー違反に対しては、その重大性、発生した事件、事故等の状況等に応じて各関連法令の罰則の対象となり得る。

8　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。

9　評価及び見直しの実施

情報セキュリティ監査の結果等により、ポリシーに定める事項及び情報セキュリティ対策の有効性等について評価するとともに、情報セキュリティを取り巻く状況の変化に対応するために、適宜ポリシーの見直しを実施する。