情報セキュリティ基本方針

平成 17 年 3 月 28 日制定
平成 29 年 7 月 12 日一部改正
令和 6 年 12 月 19 日一部改正

１．目的

本町の各情報システムが取扱う情報には、町民の個人情報のみならず行政運営上重要な情報など、外部に漏洩等した場合には極めて重大な結果を招くものが多数含まれている。したがって、情報資産及び情報資産を取り扱うネットワーク及び情報システムを様々な脅威から防御することは、町民の財産、プライバシー等を守るためにも、また、事務の安定的運営のためにも必要不可欠である。ひいては、このことが本町に対する町民からの信頼の維持向上に寄与するものである。

また、近年のいわゆるＩＴ革命の進展により、電子商取引の発展や電子自治体の構築が現実のものとなっている。本町が電子自治体を構築するためには、すべてのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

そのため、本町の情報資産の機密性、完全性及び可用性（注）を維持するための対策（情報セキュリティ対策）を整備するために熊取町情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については本町の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

（注）：国際標準化機構（ISO）が定めるもの（ISO7498-2:1989）
機密性：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。
完全性：情報及び処理の方法の正確さ及び完全である状態を安全防護すること。
可用性：許可された利用者が必要なときに情報にアクセスできることを確実にすること。

２．定義

（１）情報システム

電子計算機を利用して行う業務処理の体系で、本町が管理するものをいう。

（２）電子計算機

与えられた一連の処理手順に従って、情報の入出力、蓄積、編集、加工、修正、

更新、検索、消去その他これらに類する処理を自動的に行う電子的機器をいう。

（３）サーバ

ネットワーク上で、データの共有、印字出力、通信制御等のサービスを端末機等に対して提供する電子計算機をいう。

（４）端末機

電子計算機に対して処理を指示し、情報の入出力を行うことができるものをいう。

（５）ネットワーク

通信媒体により電子計算機を相互に接続し、一体として処理を行う情報通信網をいう。

（６）情報資産

情報システムで取り扱うすべての電子計算機、ネットワーク、プログラム、データ、ドキュメントをいう。情報資産には紙等の有体物に出力された情報も含むものとする。

（７）プログラム

電子計算機を動作させる命令や手順を記述したものをいう。

（８）データ

電子計算処理に係る入出力画面、帳票、光ディスク、磁気ディスク、磁気テープその他これらに類する媒体に記録されているもの及び通信上の内容等で、電子計算機で処理されるものすべてをいう。

（９）ドキュメント

システム設計書、プログラム仕様書、電子計算機操作手順書、コード表等をいう。

(10) パスワード

特定の電子計算機又はデータにアクセスする権限を持つことを認証するための文字列をいう。

(11) アクセス

電子計算機又はネットワークを通じデータの参照及び書換え等を行うことをいう。

(12) ポート

サーバ及び端末機内でプログラムを識別するためにサービスごとに割振られた番号をいう。

(13) プロトコル

ネットワークを介してデータ通信を行う際の規約及び手順等をいう。

(14) コンピュータウイルス

電子計算機に対し意図的に何らかの被害を及ぼすように作成されたコンピュータプログラム。自己伝染機能（自らの機能によって他のプログラムに自らをコピーし

又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能をいう。）、潜伏機能（発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能をいう。）又は発病機能（プログラム、データ等のファイルの破壊や外部へ漏えい等を行ったり、設計者の意図しない動作をする等の機能をいう。）のいずれかを有するものをいう。

（15）セキュリティホール

情報セキュリティ上問題となるソフトウェアの欠陥をいう。脆弱性。

（16）修正プログラム

情報セキュリティ上のソフトウェアの欠陥を修正する為の追加的ソフトウェアをいう。

（17）バックアップ

データの毀損、滅失又は改ざん等に備え、これらの複製を作成することをいう。

（18）アクセスコントロール

情報資産の利用を適切な権限を持つ人に制限するための方法をいう。

（19）モバイル端末

情報システムへのリモート接続を前提とする携帯用端末機をいう。

（20）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。

（21） 無線ＬＡＮ

電波等を利用してデータの送受信を行う構内通信網システム

（22） 広域無線通信

電波等を利用してデータの送受信を行う、事業者が提供する広域向けの通信網システム

（23） ＡＳＰ／クラウド

庁外データセンター等でプログラムやデータベースを管理し、ネットワークを介してこれを利用する仕組みや概念。

（24） データセンター

耐震性に優れた建物にシステムを収容して高速な通信回線を引き込み、空調設備や入退室管理、カメラによる監視等のセキュリティ対策を施した施設

３．情報セキュリティポリシーの位置付けと職員等及び外部委託事業者の義務

情報セキュリティポリシーは、個人情報の保護に関する法律（平成１５年法律第５７号）の目的を尊重し、町が保有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、具体的に取りまとめたものであり、情報セキュリティ対策の頂

点に位置するものである。

したがって、本町の情報資産に携わるすべての職員等及び外部委託事業者は、情報セキュリティの重要性について共通の認識を持ち、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。

4．情報セキュリティ管理体制

本町の情報資産について、適切に情報セキュリティ対策を推進、管理するための体制を確立するものとする。

5．情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

6．情報資産への脅威

情報セキュリティポリシーを策定するうえで、情報資産を脅かす脅威の発生度合いや発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

（1）部外者の侵入による機器又は情報資産の破壊、盗難、故意の不正アクセス又は不正操作による機器又は情報資産の破壊、盗聴、改ざん、消去等

（2）職員等及び外部委託事業者による機器又は情報資産の持出、誤操作、アクセスのための認証情報又はパスワードの不適切管理、故意の不正アクセス又は不正行為による破壊、盗聴、改ざん、消去等、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洩等

（3）コンピュータウイルス、地震、落雷、火災等の災害並びに事故、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提供サービスの障害からの波及等

7．情報セキュリティ対策

上記6で示した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おこなうものとする。

（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ち入り、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

（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、すべての職員等及び外部委託事業者に情報セキュリティ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講じられるように必要な対策を講ずる。

（３）技術的セキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、アクセス制御及びネットワーク管理等の技術的な対策を講ずる。

（４）運用におけるセキュリティ対策

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の確保等、緊急事態が発生した場合の危機管理対策その他の運用における対策を講ずる。

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．情報セキュリティ対策基準の策定

本町の様々な情報資産について、上記７の情報セキュリティ対策を講ずるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定するものとする。

９．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を遵守して情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めていく必要がある。そのため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、情報システムごとの情報セキュリティ実施手順（以下「実施手順」という。）を策定するものとする。

なお、情報セキュリティ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のある情報であることから非公開とする。

10．情報セキュリティ監査の実施

情報セキュリティポリシーの運用が適切であるかどうかを検証するために必要に応じ監査を実施するものとする。

11. 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、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、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、情報セキュリティポリシーの見直しを実施するものとする。