身延町情報セキュリティ基本方針

令和８年１月

１．目的

身延町の各情報システムが取扱う情報には、町民の個人情報、行政運営上重要な情報など、外部への漏洩、消失、破壊、改ざん、情報システムの停止等が発生した場合、極めて重大な結果を招くものが含まれている。これらの情報及び情報を取り扱うシステムを様々な脅威から防御することは、事務の安定的な運営を図り、町民の財産、プライバシー等を守るため不可欠である。また、情報技術の進歩にともない、より高度で広範囲な行政の情報化が進められている。身延町がこれに対応していくためには、全ての情報システムの運用に対して十分な安全性を維持していくことが求められる。この要求に答えるため、身延町職員等が情報資産を安全に取り扱うための規範である身延町情報セキュリティポリシーを定める。身延町情報セキュリティポリシーは、これを職員等に浸透、普及、定着を図ることにより、取り扱われる情報資産の安全性を高め、町民からの信頼の維持向上に寄与するためのものである。

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）情報資産

ネットワーク及び情報システムの開発と運用に係る全ての情報並びにネットワーク及び情報システムで取り扱う全てのデータをいう。

（４）情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

（５）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。

（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、改ざん又は消失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。

３．対象とする脅威

情報資産への脅威は、情報を取り扱う環境に広く存在し、その形態も多様であるうえ、新たな種類の脅威が発生する場合もあるので、脅威の存在やその影響を常に監視するように努めるものとする。

本情報セキュリティポリシー策定時に特に考慮した、注意すべき脅威は以下のとおりである。

（１）部外者の侵入、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･盗聴･改ざん･消去、重要情報の搾取、内部不正等

（２）情報資産の持出、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、ファイブ委託管理の不備、マネジメントの欠陥、パスワードの不適切管理、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・盗聴・改ざん・消去等、搬送中の事故等による機器または情報資産の盗難等

（３）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

本セキュリティポリシーが適用される行政機関は、町長部局、附属機関、教育委員会、公営企業、議会事務局及び身延町早川町組合立飯富病院、早川町・身延町・南部町医療事務組合、切坂山恩賜県有財産保護組合とする。

（２）情報資産の範囲

本セキュリティポリシーが対象とする情報資産は、次のとおりとする。ただし、町立学校における学校教育情報、組合立病院における医療情報及びこれに関連する情報は除く。

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、非常勤職員及び会計年度任用職員（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．情報セキュリティ対策

上記３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講ずるものとする。

（１）組織体制

身延町の情報資産について、管理職が率先して情報管理対策を推進・管理するための全庁的な体制を確立するものとする。

（２）情報資産の分類と管理

身延町の情報資産を機密性、完全性及び可用性に応じて分類し、その重要度等、情報の特性に応じた情報セキュリティ対策を行うものとする

（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。

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、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対策

サーバ室、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に物理的な対策を講ずる。

（５）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情報セキュリティに関して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ずる。

（6）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、コンピュータの管理、情報資産へのアクセス制御、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ずる。

（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ずる。また、情報資産へのセキュリティ侵害が発生した場合等に迅速な対応を可能とするための緊急時対応体制を策定する。

（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。

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が遵守されていることを検証するために、定期的または必要に応じて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により、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を取り巻く状況の変化に対応するため新たに対策が必要となった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及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及び情報セキュリティ実施手順書の見直しを実施する。

９．情報セキュリティ対策基準の策定

身延町の様々な情報資産について、上記６，７及び８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。

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書は、公にすることにより身延町の行政運営に重大な支障を及ぼす恐れのある情報資産であることから非公開とする。