吉賀町
情報セキュリティ基本方針

令和８年３月３１日　策定

（目次）

第１章　情報セキュリティ基本方針

１　目的

吉賀町の各情報システムが取り扱う情報には、町民の個人情報のみならず行政運営上重要な情報など、外部への漏洩等が発生した場合には極めて重大な結果を招く情報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為にも、また、事務の安定的な運営の為にも必要不可欠である。ひいては、このことが吉賀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。吉賀町が電子自治体を構築する為には、全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。

その為、吉賀町の情報資産の機密性、完全性、可用性[注]を維持する為の対策（情報セキュリティ対策）を整備する為に吉賀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概要については吉賀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（IS07498-2：1989）

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）ネットワーク

吉賀町における町長部局、各行政委員会、消防及び各教育機関（事務室及び職員室のみ）等を相互に接続する為の通信網、その構成機器（ハードウェア及びソフトウェア）及び記録媒体で構成され、処理を行う仕組みをいう。

（２）情報システム

業務系の電子計算機（業務系におけるネットワーク、ハードウェア及びソフトウェア）及び記録媒体で構成され、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かかる全ての情報、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情報（印刷した文書、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を含む）をいう。

なお、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。

（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）脅威

情報資産に対して障害や損害を与える原因となるものをいう。

（６）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。

（７）LGWAN 接続系

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。

（８）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。

（９）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。

（１０）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　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、吉賀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、かつ具体的にと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、吉賀町長をはじめとして吉賀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もつとともに業務の遂行にあ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。

なお、情報セキュリティポリシー（情報セキュリティ対策基準）は、公にすることにより吉賀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。

但し、町長又は副町長が承認した情報セキュリティ基本方針のみホームページやポスターなどで公開できるものとする。

４　情報セキュリティ管理体制

吉賀町の情報資産について、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　適用の範囲

（１）行政機関の範囲

本基本方針が適用される行政機関の範囲は、町長部局、各行政委員会及び各教育機関（事務室及び職員室のみ）とする。なお、各教育機関における教育のために用いるネットワーク及びシステム等は、この情報セキュリティポリシーの対象となるネットワーク及び情報システムと物理的に分けなければならない。

（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

６ 情報資産の分類・評価

情報資産をその内容に応じて分類・評価し、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。

７ 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上で、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 職員等又は外部委託事業者による機器又は情報資産の持ち出し、誤操作、アクセスの為の認証情報又はパスワードの不適切管理、故意の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インフラの障害からの波及等

８ 情報セキュリティ対策

上記７で示した脅威から情報資産を保護する為に、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

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、県と町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、緊急時対応計画を策定する。

①　緊急時対応計画に盛り込むべき内容　緊急時対応計画には、以下の内容を定めなければならない。

(ｱ)　関係者の連絡先

(ｲ)　発生した事案に係る報告すべき事項

(ｳ)　発生した事案への対応措置

(ｴ)　再発防止措置の策定

②　業務継続計画との整合性確保　自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、情報電算運営委員会は当該計画と情報セキュリティポリシーの整合性を確保しな ければならない。

③　緊急時対応計画の見直し　CISO　又は情報電算運営委員会は、情報セキュリティを取り巻く状況の変化や 組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければな らない。

（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。

９　情報セキュリティ対策基準の策定

吉賀町の様々な情報資産について、上記８の情報セキュリティ対策を講ずるに当たっては、遵守すべき基準を定める必要がある。その為、情報セキュリティ対策を行う上で必要となる基本的な基準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為、定期的又は必要に応じて監査及び自己点検を実施する。

１１　評価及び見直しの実施

情報セキュリティ監査及び自己点検の結果等により、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為に定期的に情報セキュリティポリシーの見直しを実施する。

１２　職員の順守義務

職員、非常勤職員及び臨時職員（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。