# 金ケ崎町情報セキュリティ基本方針に関する規程

平成３１年３月２８日

訓令第３号

（目的）

第１条　この規程は、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により、町が保有する情報資産の機密性、完全性及び可用性を維持することを目的とする。

（定義）

第２条　金ケ崎町情報セキュリティ基本方針に関する規程（以下「規程」という。）において、次の各号に掲げる用語の意義は、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、完全性及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　金ケ崎町情報セキュリティ基本方針に関する規程及び金ケ崎町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、改ざん又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）　情報システム室　重要な情報システム及びネットワークの基幹機器を設置し、当該機器等の管理並びに運用を行うための部屋をいう。

（９）　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。

（10）　LGWAN接続系　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（マイナンバー利用事務系は除く。）。

(11)　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。

(12)　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。

(13)　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　町は、次の情報資産に対する脅威を想定し、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・外部監査機能の不備、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・消去等

（３）　地震、落雷、火災等の災害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

（適用範囲）

第４条　規程を適用する範囲は、次のとおりとする。

（１）　実施機関の範囲を町長、教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会、上下水道事業の管理者の権限を行う町長及び議会とする。ただし、教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会及び議会が別に定める場合を除く。

（２）　職員の範囲は、町の保有する情報資産に関わる職員（地方公務員法（昭和２５年法律第２６１号。以下「法」という。）第３条に規定する職員をいう。）とする。

（３）　情報資産の範囲は、町が所掌する次の情報資産とする。ただし、金ケ崎町立学校設置条例（昭和４０年金ケ崎町条例第２１号）で規定する各教育機関が保有する情報資産を除く。

ア　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

イ　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。）

ウ　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

（職員等の遵守義務）

第５条　職員は、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関係規定等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　町は、第３条に規定する脅威から情報資産を保護するために、次の情報セキュリティ対策を講じる。

（１）　組織体制　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）　情報資産の分類及び管理　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。

ア　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。

イ　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、無害化通信を行う。

ウ　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行う。高度な情報セキュリティ対策として、都道府県及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行う。

（４）　物理的セキュリティ　サーバ、情報システム室、通信回線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切に対応するため、緊急時対応計画を策定する。

（８）　業務委託と外部サービスの利用　業務委託を行う場合には、情報セキュリティ要件を明記した契約を締結するものとする。町は、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のうえ、必要に応じて契約に基づき措置を講じる。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。また、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。

（情報セキュリティ監査及び自己点検の実施）

第７条　町は、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。

（情報セキュリティポリシーの見直し）

第８条　町は、情報セキュリティ監査及び自己点検の結果、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等には、適宜情報セキュリティポリシーを見直す。

（情報セキュリティ対策基準の策定）

第９条　町は、前３条に規定する対策を実施するために、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。

（情報セキュリティ実施手順の策定）

第１０条　町は、情報セキュリティ対策を実施するため、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町の行政

運営に重大な支障を及ぼすおそれがあるため非公開とする。

附　則

この訓令は、平成３１年４月１日から施行する。

附　則（令和３年４月１日訓令第４号）

この訓令は、令和３年４月１日から施行する。

附　則（令和４年１１月２８日訓令第２号）

この訓令は、令和４年１２月１日から施行する。

附　則（令和８年３月１９日訓令第２号）

この訓令は、令和８年４月１日から施行する。