古賀市情報セキュリティ基本方針

（目的）

第１条　この古賀市情報セキュリティ基本方針（以下「基本方針」という。）は、市の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ため、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を目的とする。

（用語の定義）

第２条　この基本方針において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

⑴　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及びその構成機器（ハードウェア及びソフトウェア）をいう。

⑵　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。

⑶　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。

⑷　情報セキュリティポリシー　基本方針及び第９条の規定に基づき定める情報セキュリティ対策基準の総称をいう。

⑸　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。

⑹　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。

⑺　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。

⑻　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、地方税又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。

⑼　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を除く。）。

⑽　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。

⑾　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。

⑿　無害化通信　インターネットメール本文のテキスト化、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ない等、安全が確保された通信をいう。

（対象とする脅威）

第３条　市の情報資産に対する脅威として、次の各号に掲げるものについて認識しなければならない。

⑴　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、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

⑵　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

⑶　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

⑷　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

⑸　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　この基本方針が適用される行政機関は、市長、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、議会及び公営企業管理者の権限を行う市長をいう。

２　この基本方針が対象とする情報資産は、次の各号に掲げるとおりとする。

⑴　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

⑵　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。）

⑶　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

（職員等の義務）

第５条　前条第１項に規定する行政機関における情報資産に関する業務に携わる全ての職員（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もつとともに、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。

２　外部委託業者に対しては、契約により情報セキュリティポリシーを遵守させるための必要な措置を講じるものとする。

（情報セキュリティ対策）

第６条　第３条に規定する脅威から情報資産を保護するために、次の各号に掲げる区分に応じ、当該各号に定める情報セキュリティ対策を講じるものとする。

⑴　組織体制　市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の確立

⑵　情報資産の分類と管理　市の情報資産について機密性、完全性及び可用性に応じた分類に基づき実施する情報セキュリティ対策

⑶　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て講じる次の３段階の対策

イ　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対策

ロ　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とともに、両システム間で通信する場合の無害化通信によるセキュリティ対策

ハ　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（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の自治体情報セキュリティクラウドの導入等）

⑷　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・妨害から保護するための物理的な対策

⑸　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、職員等に基本方針及び情報セキュリティに関する法令等の内容を周知徹底し、十分な教育及び啓発が講じられるようにするための対策

⑹　技術的セキュリティ対策　情報資産の管理、アクセス制御、不正プログラム対策、不正アクセス行為対策等の技術的対策

⑺　運用におけるセキュリティ対策　情報システムの監視、情報セキュリティに関する法令等及び基本方針の遵守状況の確認、業務委託を行う際のセ

キュリティ確保等の運用面の対策及び緊急事態が発生した場合に迅速な対応を可能とするための危機管理対策

⑻　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の情報セキュリティ要件を明記した契約の締結、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の確認、必要に応じて契約に基づき講じる措置及び外部サービス（クラウドサービス）を利用する場合の利用に係る規定の整備、ソーシャルメディアサービスの運用手順又は発信できる情報の規定

⑼　評価　情報セキュリティポリシーの遵守状況検証のために定期的又は必要に応じて実施する情報セキュリティ実施状況の検証及び自己点検

（情報セキュリティ監査又は自己点検）

第７条　情報セキュリティポリシーが遵守されていることを確認するため、定期的又は必要に応じて情報セキュリティ実施状況の監査又は自己点検を行う。

（情報セキュリティポリシーの見直し）

第８条　情報セキュリティ実施状況の監査又は自己点検の結果、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、リスクを検討した上で、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　前３条に規定する対策を講じるに当たって、遵守すべき行為及び判断等の基準を統一的に定めるため、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」（以下「対策基準」という。）を策定するものとする。

（情報セキュリティ実施手順の策定）

第１０条　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実施手順を明記した「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。

２　対策基準及び実施手順は、公にすることにより、市の行政運営に重大な支障を及ぼすおそれのあることから非公開とする。

附　則

（施行期日）

１　この訓令は、令和８年４月１日から施行する。

（古賀市情報セキュリティ基本方針の廃止）

２　古賀市情報セキュリティ基本方針（平成１４年７月訓令１６号・教育委員会訓令第１０号）は、廃止する。