能代市情報セキュリティ対策に関する規程

（趣旨）

第１条　この訓令は、地方自治法（昭和２２年法律第６７号）第２４４条の６第１項の規定に基づき、本市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ため、本市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ものとする。

（定義）

第２条　この訓令において、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）　情報資産　次に掲げるものをいう。

ア　ネットワーク、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、ネットワーク図等のシステム関連文書

（４）　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。

（５）　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。

（６）　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。

（７）　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。

（８）　情報セキュリティポリシー　この訓令及び第９条に規定する情報セキュリティ対策基準をいう。

（９）　マイナンバー利用事務系　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。

（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。

（１４）　外部サービス（クラウドサービス）　クラウドサービスをいう。

（対象とする脅威）

第３条　この訓令に基づく情報セキュリティ対策は、次に掲げる脅威を想定して行うものとする。

（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、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、メンテナンスの不備、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３条の２　この訓令は、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、公営企業（市長又は管理者）及び財産区並びに能代市議会に適用する。

（職員等の遵守義務）

第４条　職員等（非常勤の者を含む。以下同じ。）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第１０条に規定する情報セキュリティ実施手順を遵守しなければならない。

（組織体制）

第５条　統一的な情報セキュリティを確保するため、次に掲げる責任者等を置く。

（１）　最高情報セキュリティ責任者

（２）　統括情報セキュリティ責任者
（３）　情報セキュリティ責任者
（４）　情報セキュリティ管理者
（５）　情報システム管理者
（６）　情報システム担当者
（７）　能代市情報セキュリティ対策委員会

（情報セキュリティ対策）

第６条　市長は、第３条各号の脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講じる。

（１）　本市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こと。

（２）　情報システム全体の強靭性の向上対策として、業務の効率性・利便性の観点を踏まえ、次の三段階の対策を講じること。

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こと。

イ　ＬＧＷＡＮ接続系においては、ＬＧＷＡＮと接続する情報システムと、インターネット接続系の情報システムとの通信経路の分割をし、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こと。

ウ　インターネット接続系においては、秋田県及び本市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実施すること。

（３）　物理的セキュリティ対策として、サーバ、情報システム室、通信回線、職員等のパソコン等の管理について、必要な対策を講じること。

（４）　人的セキュリティ対策として、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必要な対策を講じること。

（５）　技術的セキュリティ対策として、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必要な対策を講じること。

（６）　情報セキュリティポリシーの運用面の対策として、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、業務委託を行う際のセキュリティ確保等の対策を講じるとともに、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こと。

（７）　業務委託の実施及び外部サービス（クラウドサービス）の利用における対

策として、次に掲げる場合に応じ、それぞれ次に定める対策を講じること。

ア　業務委託を行う場合　業務委託事業者と情報セキュリティ要件を明記した契約を締結し、業務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く措置を講じること。

イ　外部サービス（クラウドサービス）を利用する場合　利用にかかる規定を整備し必要な対策を講じること。

ウ　ソーシャルメディアサービスを利用する場合　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こと。

（情報セキュリティ監査及び自己点検の実施）

第７条　市長は、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　市長は、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　市長は、情報セキュリティ対策等を実施するために、具体的な遵守事項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ものとする。

（情報セキュリティ実施手順の策定）

第１０条　市長は、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

２　情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。