能登町情報セキュリティ基本方針

（目的）

第1条　能登町（以下「町」という。）が取扱う情報には、町民の個人情報をはじめとして行政運営上重要な情報を保有しており、外部への漏えい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。このような情報資産を様々な脅威から防御することは、町民の財産及びプライバシーの保護並びに行政サービスの安定性のために必要不可欠である。このことから、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し、町民からの信頼を確保するため、町が実施する情報セキュリティ対策について次に掲げる事項に積極的に取り組むほか、基本的な事項を定めることを目的とする。

(1)　情報セキュリティ対策に取り組むための全庁的な体制を確立する。

(2)　情報セキュリティ対策の基準として情報セキュリティ対策基準を策定し、その実行のための手順等を盛り込んだ実施手順を策定する。

(3)　町の保有する情報資産を適正に管理する。

(4)　情報セキュリティ対策の重要性を認識させ、当該対策を適正に実施するために、職員等に対して必要な教育を実施する。

(5)　情報セキュリティインシデントが発生した場合又はその予兆があった場合に速やかに対応するため、緊急時対応計画を定める。

(6)　情報セキュリティ対策の実施状況の監査及び自己点検等を通して、定期的に対策の見直しを実施する。

(7)　全ての職員等は、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は、情報セキュリティ基本方針、情報セキュリティ対策基準及び情報セキュリティ実施手順を遵守する。

(8)　地域全体の情報セキュリティの基盤を強化するため、地域における広報啓発、注意喚起、官民の連携・協力等に積極的に貢献する。

（定義）

第2条　この告示において、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　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扱う全ての情報（紙等の有体物に出力された情報を含む。）をいう。

(4)　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。

(5)　情報セキュリティポリシー　この能登町情報セキュリティ基本方針（以下「基本方針」という。）及び能登町情報セキュリティ対策基準（令和7年能登町訓令第11号）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情報を確保することをいう。

(7)　完全性　情報が破壊、改ざん又は消去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。

(9)　職員等　職員、地方公務員法（昭和25年法律第261号）第22条の2第1項の規定により採用された会計年度任用職員、同法第22条の4の規定により任用された定年前再任用短時間勤務職員及び同法第22条の3第4項若しくは第26条の6第7項第2号又は地方公務員の育児休業等に関する法律（平成3年法律第110号）第6条第1項第2号の規定により任用された臨時的任用職員をいう。

(10)　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）又は戸籍事務等に関わる情報システム及びデータをいう。

(11)　ＬＧＷＡＮ接続系　ＬＧＷＡＮに接続された情報システム及び当該情報システムで取扱うデータをいう。（マイナンバー利用事務系を除く。）

(12)　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当該情報システムで取扱うデータをいう。

(13)　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。

(14)　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　情報資産に対する脅威は、次の各号に掲げる脅威を想定し、情報セキュリティ対策を実施するものとする。

(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及び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及び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)　大規模又は広範囲にわたる疾病による要因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　基本方針が適用される行政機関の範囲は、能登町個人情報保護法施行条例（令和4年能登町条例第45号）第2条第1項に規定する実施機関及び議会事務局とする。

2　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。

(1)　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

(2)　ネットワーク及び情報システムで取扱う情報（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

（職員等の遵守義務）

第5条　職員等は、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は、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。

（情報セキュリティ対策）

第6条　町は、第3条の脅威から情報資産を保護するため、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。

(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)　情報の資産の分類と管理　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実施する。

(3)　情報システム全体の強じん性の向上　情報セキュリティの強化を目的として、業務の効率性及び利便性の観点を踏まえ、情報システム全体に対し、次の3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及び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。この場合において、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。

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実施し、高度な情報セキュリティ対策として、石川県と町又は町のインターネット接続口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。

(4)　物理的セキュリティ　サーバ、サーバ室、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、業務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、情報資産に対するセキュリティ侵害が生じた場合等に速やかに対応するため、緊急時対応計画を策定する。

(8)　業務委託及び外部サービス（クラウドサービス）の利用　業務委託を行う場合は、委託事業者を選定して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するとともに、必要に応じて契約に基づき次に掲げる措置を講じる。

ア　外部サービス（クラウドサービス）を利用する場合は、利用に係る規定を整備し対策を講じる。

イ　ソーシャルメディアサービスを利用する場合は、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り、当該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は、適宜情報セキュリティポリシーの見直しを行う。

（情報セキュリティ監査及び自己点検の実施）

第7条　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。

2　前項の監査及び自己点検の実施方法等については、能登町情報セキュリティ監査実施規程（令和7年能登町訓令第9号）による。

（情報セキュリティポリシーの見直し）

第8条　前条の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ものとする。

（情報セキュリティ対策基準の策定）

第9条　第6条、第7条及び前条に規定する対策等を実施するため、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ものとする。

（情報セキュリティ実施手順の策定）

第10条　前条の情報セキュリティ対策基準に基づき、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　前項の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。

（基本方針の公表）

第11条　町長は、基本方針を変更したときは、速やかにホームページ等に公表しなければならない。

（その他）

第12条　この告示に定めるもののほか情報セキュリティに関し必要な事項は、町長が別に定める。

附　則

この告示は、令和7年10月1日から施行する。