ニセコ町情報セキュリティポリシー規程

目次

第１章　情報セキュリティ基本方針

（目的）

第１条　この規程は、本町が保有する情報資産の機密性、安全性及び可用性を維持するため、本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並びにセキュリティ対策の基準を定めることを目的とする。

（定義）

第２条　この規程において、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）　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。

（２）　情報資産：個人情報及び行政運用上の重要な情報を含む町が取り扱う情報及び情報の活用に関連する資産の全てをいう。

（３）　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。

（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　権限のある者に、常時情報の利用を可能にすることをいう。

（７）　個人情報　個人に関する情報であって、特定の個人が識別され、又は識別され得るものをいう。

（８）　情報セキュリティポリシー　情報資産に対する安全対策を推進するため、組織内の情報セキュリティに関する方針、体制、対策等を包括的に網羅したものをいう。情報セキュリティポリシー規程に基づいて策定される。

（９）　情報セキュリティインシデント　情報セキュリティに関する障害・事故及びシステム上の欠陥をいう。

（１０）　コンピュータ　処理事務を自動的に行う電子的機器（サーバ及びパソコンに区分される。）をいう。

（１１）　サーバ　ネットワークで接続された情報システムにおいて、周辺機器（プリンタ等）、ファイルサーバ、情報共有サーバ等の共用利用を主機能としたコンピュータをいう。

（１２）　パソコン　小型のコンピュータをいう。

（１３）　オペレーティングシステム　コンピュータの入出力やディスク・メモリの管理などの基本的な機能を提供するソフトウェアをいう。

（１４）　ログイン　コンピュータやシステムの資源にアクセス可能な状態になることをいう。

（１５）　ログアウト　コンピュータやシステムの資源にアクセス可能な状態を解消することをいう。

（１６）　ネットワーク　複数の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。

（１７）　セキュリティホール　情報システムの脆弱性に関する表現で、コンピュータの欠陥（バグ、不具合、あるいはシステム上の盲点）をいう。放置された状態でコンピュータを利用すると、コンピュータウイルス等の攻撃対象となる危険性がある。

（１８）　ソースコード　プログラミング言語の文法に従って定義したプログラムを実際に動作させるための元になるテキストデータをいう。２進数の機械語に翻訳されて処理が実行される。

（１９）　パスワード　コンピュータ及びネットワークの利用許可を証明する識別用暗号記号等

（２０）　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。

（２１）　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。ただし、マイナンバー利用事務系を除く。

（２２）　インターネット接続系　インターネットメール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。

（２３）　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。

（２４）　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。

（職員等の義務）

第３条　情報資産に関する全ての職員（非常勤職員及び地方公務員法（昭和２５年法律第２６１号）第２２条の２に規定する会計年度任用職員を含む。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及び情報セキュリティ実施手順を遵守する義務を負うものとする。

（適用範囲）

第４条　この規程が適用される行政機関は、町長部局、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並びに羊蹄山ろく消防組合に設置するニセコ町の情報資産とする。

２　この規程が対象とする情報資産は、次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

（対象とする脅威）

第５条　情報資産に対する脅威として、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、火災等の災害又は事故若しくは故障によるサービス・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

(情報セキュリティ対策)

第６条　前条で示した脅威から情報資産を保護するために、次の各号に掲げる情報セキュリティ対策を講ずるものとする。

（１）　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）　本町の所有する情報資産をその内容に応じて分類し、その重要性に応じた情報セキュリティ対策を実施する。

（３）　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、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。）を行う。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。

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する。高度な情報セキュリティ対策として、北海道及び市区町村のインターネット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）　情報システム等を設置する施設への不正な立入り、情報資産への損傷・妨害等から保護するために、情報システム等に対する物理的な対策を講ずる。

（５）　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）　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）　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。

（８）　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。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）　攻撃者からの攻撃機会を低減するため、法令等で定められた場合を除き、メールアドレス及び職員氏名のインターネットでの公開は原則として行わないものとする。

（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。

（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、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条の情報セキュリティ対策を講ずるにあたって、遵守すべき行為及び判断等の基準を統一的なレベルで定め、情報セキュリティ対策を行う上で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を第２章に定めるものとする。

（情報セキュリティ実施手順の策定）

第１０条　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（以下「実施手順」という。）を策定するものとする。実施手順は、公にすることにより本町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。

抜粋終了