

長沼町 情報セキュリティ基本方針

1 目的

長沼町の各情報システムが取り扱う情報には、町民の個人情報のみならず行政運営上重要な情報など、外部へ漏洩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。

したがって、情報資産並びに情報資産を取り扱うネットワーク及び情報システムを様々な脅威から防御することは、町民の財産、プライバシー等の安全面、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが長沼町に対する町民からの信頼の維持向上に寄与するものである。

また、近年のIT技術の進歩により、電子商取引の発展や電子自治体の構築が広く行われるようになってきている。長沼町が電子自治体を構築するためには、すべてのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

そのため、長沼町の情報資産の機密性、完全性及び可用性^(注)を維持するための対策（情報セキュリティ対策）を整備するために長沼町情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については長沼町の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

(注)：国際標準化機構（ISO）が定めるもの（ISO7498 - 2 : 1989）

機密性（confidentiality）：情報にアクセスすることが許可された者だけがアクセスできることを確実にすること。

完全性（integrity）：情報及び処理の方法の正確さ及び完全である状態を安全防護すること。

可用性（availability）：許可された利用者が必要なときに情報にアクセスできることを確実にすること。

2 定義

このポリシーにおいて用いる用語の定義は、それぞれ次のとおりとする。

(1) 対象機関

長沼町における町長部局、教育部局、選挙管理委員会、公平委員会、監査委員、農業委員会、議会並びに南空知消防組合消防署長沼支署等をいう。

(2) ネットワーク

対象機関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）及び記録媒体で構成され、処理を行う仕組みをいう。

(3) 情報システム

電子計算機（ネットワーク、ハードウェア及びソフトウェア）及び記録媒体で構成され、処理を行う仕組みをいう。

(4) 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すべての情報並びにネットワーク及び情報システムで取り扱うすべての情報をいう。なお、情報資産には紙等の有体物に出力された情報も含むものとする。

(5) 情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

(6) 情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

(7) マイナンバー利用事務系（特定個人情報利用事務系）

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。

(8) LGWAN 接続系（特定個人情報関係事務）

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)

(9) 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。

(10) 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。

(11) ガバメントクラウド

「ガバメントクラウド (Gov-Cloud) 」とは、政府の情報システムについて、共通的な基盤・機能を提供する複数のクラウドサービス (IaaS、PaaS、SaaS) の利用環境であり、クラウドサービスの利点を最大限に活用することで、迅速、柔軟、かつセキュアでコスト効率の高いシステムを構築可能とし、利用者にとって利便性の高いサービスをいち早く提供し改善していくことを目指している。

各クラウドサービスを提供するサービス事業者である CSP (クラウドサービスプロバイダ) と、ASP (アプリケーションサービスプロバイダ) がシステム基盤となり、長沼町は「アプリケーション開発事業者」と利用契約を結び、ガバメントクラウドに接続する。

- ① アプリケーション開発事業者は、標準仕様に準拠して開発した基幹業務等のアプリケーションを、ガバメントクラウドに構築する。
- ② 基幹業務等のアプリケーションは、複数の事業者がガバメントクラウドに構築し、長沼町は、それらの中から選択することが可能となる。基幹業務等とは、基幹業務 (住基、税、介護等のいわゆる 17 業務) のほか、これに付属又は密接に連携する業務のこと。
- ③ 長沼町は、これまでのように、自らサーバ等のハードウェアや OS・ミドルウェア・アプリケーション等のソフトウェアを所有する必要がなくなる。

3 情報セキュリティポリシーの位置付け、職員等及び委託事業者の義務、外部サービス等

情報セキュリティポリシーは、長沼町が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の頂点に位置するものである。

したがって、長沼町長をはじめとして長沼町が所掌する情報資産に関する業務に携わるすべての職員等及び委託事業者は、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を遵守する義務を負うものとする。

業務委託する場合には、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、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、機密性 2 以上の情報を取り扱う場合と、取り扱わない場合に分け、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。

4 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、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

5 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

- (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

6 情報セキュリティ管理体制

長沼町の情報資産について、幹部が率先して情報セキュリティ対策を推進・管理するための体制を確立するものとする。

7 情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

8 情報セキュリティ対策

上記6で示した脅威から情報資産を保護するために、以下の情報セキュリティ対策を講ずるものとする。

(1) 情報システム全体の強靱性の向上

情報システム全体に対し、次の三段階の対策を講じる。

- ① 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。
- ② 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、無害化通信等実施する。
- ③ 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、都道府県と市区町村のインターネット接続口を集約した、自治体情報セキュリティクラウドを利用する。

(2) 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・妨害などから保護するために物理的な対策、及び、根本的な物理上の分離・分割対策を講ずる。

(3) 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、すべての職員等及び委託事業者の情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるように必要な対策を講ずる。

(4) 技術及び運用におけるセキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策のほか、システム開発等の委託、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等の運用面の対策を講ずるとともに、緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

(5) ガバメントクラウド利用におけるセキュリティ対策

ガバメントクラウドのうち、地方自治体が活用するクラウド事業者及び環境について

は、次の事項をはじめ対策を的確に講じることにより、高いセキュリティを確保する。

- ① ISMAP（政府によるクラウドセキュリティ評価制度）の評価・登録を受けたクラウドサービスを活用。
- ② データセンタの物理的所在地が日本国内であり、合意を得ない限り、一切の情報資産について日本国外への持ち出しを行わないこととする。
- ③ 一切の紛争は、日本の裁判所が管轄するとともに、契約の解釈が日本法に基づくものであることとする。
- ④ 地方自治体のシステムについて、データを団体ごとに論理的に分離するとともに、厳格なアクセス制御を行う等、高い機密性を確保する。
- ⑤ 地方自治体の他のシステムとの接続は、専用回線により行い、インターネットからの接続は、セキュリティアクラウドを設ける等、ネットワークのセキュリティを確保する。
- ⑥ 同一構成による東西の2センターを構築する等、高い可用性を確保する。

9 情報セキュリティ対策基準の策定

長沼町の様々な情報資産について、上記7の情報セキュリティ対策を講ずるに当たっては、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る必要がある。そのため、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策定するものとする。

10 情報セキュリティ実施手順の策定

情報セキュリティ対策基準を遵守して情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めていく必要がある。そのため、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、内部部局の長等が所掌する情報資産の情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ基本方針を除く情報セキュリティポリシー（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は、公にすることにより長沼町の行政運営に重大な支障を及ぼすおそれのある情報資産であることから非公開とする。

11 情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーが遵守されていることを検証するため、定期的に監査及び自己点検を実施する。

12 評価及び見直しの実施

情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを、その都度実施する。