真狩村情報セキュリティ基本方針

（ 令和８年３月 ）

＜　目　次　＞

第１章　情報セキュリティ基本方針

1. 目的

真狩村の各情報システムが取り扱う情報には、住民の個人情報のみならず行政運営上重要な情報など、外部に漏洩等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、これらの情報及び情報を取り扱う情報システムをさまざまな脅威から防御することは、住民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。

また、今日インターネットを始めとする情報通信ネットワークや情報システムの利用は、生活、経済、社会のあらゆる面で拡大しており、これらに積極的に対応するためには、全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、真狩村の情報資産の機密性、完全性及び可用性を維持するための対策(情報セキュリティ対策)を整備するために真狩村情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ方針については真狩村の情報セキュリティ対策の基本的な方針として、情報セキュリティの対象位置付け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…情報にアクセスすることが認可された者だけがアクセスすることを確実にすること。

完全性…情報及び処理の方法の正確さ及び完全である状態を完全防護すること。

可用性…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

(1) ネットワーク

真狩村の内外部局を相互に接続するための通信網、その構成機器（ハードウエア及びソフトウエア）及び記録媒体で構成され、処理を行う仕組みをいう。

(2) 情報システム

業務系の電子計算機（業務系におけるネットワーク、ハードウエア及びソフトウエ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データならびにネットワーク及び情報システムで取り扱う全てのデータをいう。

(4) 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。

(5) 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

(6) 気密性

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。

(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) 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。

(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（マイナンバー利用事務系を除く）。

(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。

3. 情報セキュリティポリシーの位置付けと職員等の義務

情報セキュリティポリシーは、真狩村が保有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、体系的且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、真狩村長をはじめとして真狩村が所掌する情報資産に関する業務に携わる全ての職員等及び外部委託者は、情報セキュリティポリシー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当たって情報セキュリティポリシーを遵守しなければならない。

4. 情報資産への脅威

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) 部外者による故意の不正アクセスまたは不正操作による情報資産の漏えい・破壊・詐取・持出・盗聴・改ざん・消去、機器及び媒体の盗難、ウィルス攻撃、サービス不能攻撃等のサイバー攻撃等

(2) 職員等及び外部委託による設計・開発の不備、プログラムの欠陥、無許可ソフトウェ

アの使用、意図しない操作、故意の不正アクセスまたは不正操作による情報資産の持出・盗聴・改ざん・消去、機器及び媒体の盗難及び規定外の端末接続によるデータ漏洩等

(3) 地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止

(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

5. 適用範囲

(1) 行政機関の範囲　本基本方針が適用される行政機関は、行政内部部局、行政委員会及び議会とする。

(2) 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. 情報セキュリティ対策

上記 4. 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) 組織体制

真狩村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) 情報資産の分類と管理

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、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、無害化通信を実施する。

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、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に物理的な対策を講ずる。

(5) 人的セキュリティ

情報セキュリティに関する権限や責任を定め、全ての職員等に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。

(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) 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（クラウドサービス）を利用する場合には、利用に係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。

なお、ＬＧＷＡＮ－ＡＳＰ、自治体クラウド、ガバメントクラウドなど閉域網や専用回線の利用等により安全性を確保できる外部サービスは対象外とする。

(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 上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

7. 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施する。

8. 評価及び情報セキュリティポリシー見直しの実施

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、リスクを検討したうえで、情報セキュリティポリシーを見直す。

9. 情報セキュリティ対策基準の策定

上記6、7及び8に規定する対策等を実施するために、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。

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。

なお、情報セキュリティ実施手順は、公にすることにより本村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。。