日高村情報セキュリティポリシー
（令和７年６月版）

（目次）

第１章

情報セキュリティ基本方針

（目次）

第１章　情報セキュリティ基本方針

1.　目的

本基本方針は、日高村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、日高村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ことを目的とする。

2.　定義(用語定義)

①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。

②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。

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。

⑥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。

⑦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。

⑧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等をいう。

⑨LGWAN 接続系：人事給与、財務会計及び文書管理等 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等をいう。(マイナンバー利用事務系は除く)

⑩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等をいう。

⑪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。

⑫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.　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、外部委託管理の不備、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不全及び業務停止等

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等

4. 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の範囲は、日高村の村長部局、農業委員会、選挙管理事務局、議会事務局、監査委員事務局、及び教育委員会等とする。

（2） 情報資産の範囲

本基本方針が対象とする情報資産の範囲は、次のとおりとする。

① ネットワーク、情報システム及びこれらに関する設備、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

5. 職員等の遵守義務

職員、非常勤職員、会計年度任用職員及び議員（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情報セキュリティ実施手順を遵守しなければならない。

6. 情報セキュリティ対策

上記3の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じる。

（1） 組織体制

日高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

日高村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靭性向上

情報システム全体の強靭性向上のため、次の三段階の対策を講じる。

①マイナンバー利用事務系

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。

②LGWAN 接続系

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、無害化通信を適用する。

③インターネット接続系

インターネット接続系においては、不正通信に対する監視機能強化等の高度な情報セキュリティ対策を講じる。高度な情報セキュリティ対策として、高知県と日高村のインターネット接続口を集約した上で、高知県情報セキュリティクラウドを利用する。

ただし業務上必要な場合は、高知県情報セキュリティクラウドを利用しない端末を設置するが同様のセキュリティ対策を講じる。

（4） 物理的セキュリティ

サーバ等、電算室等、通信回線等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

職員等が遵守すべき情報セキュリティに関する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セキュリティ対策を講じる。

（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セキュリティ対策を講じる。

（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、外部委託を行う際のセキュリティ確保等、情報セキュリティ運用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、外部サービス（クラウドサービス、ソーシャルメディアサービス）の利用等

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（クラウドサービス）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） 評価・見直し

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、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。

8. 情報セキュリティポリシーの見直し

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な対策等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。

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ものとする。なお、情報セキュリティ実施手順は、公にすることにより日高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。