第１章　情報セキュリティ基本方針

第１条　目的

山形村の情報資産には、村民の個人情報をはじめ行政運営に必要な情報など、外部に漏えい、あるいは滅失した場合には、極めて重大な結果を招く情報が多数含まれている。これらの情報資産を人的脅威や災害、事故等から防御することは、村民の財産、プライバシーを守るためにも、また、継続的、かつ、安全・安定的な行政サービスの実施を確保するためにも必要不可欠であり、ひいては、山形村に対する村民からの信頼の維持向上に寄与するものである。

このため、山形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を整備することを目的として、山形村情報セキュリティポリシーを定め、情報セキュリティの確保に最大限取り組むものである。

このうち情報セキュリティ基本方針は、山形村の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

第２条　用語の定義

（１）電子計算機

ハードウェア及びソフトウェアで構成するコンピュータ、及び周辺機器をいう。

（２）ネットワーク

電子計算機を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）で構成され、情報処理を行う仕組みをいう。

（３）庁内ネットワーク

ネットワークのうち、山形村役場、出先機関等及び教育機関の事務室等で使用される電子計算機を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア）で構成され、情報処理を行う仕組みをいう。

（４）部署ネットワーク

庁内ネットワークのうち、特定の部署のみで使用されるネットワークをいう。

（５）外部ネットワーク

ネットワークのうち、庁内ネットワーク以外のものをいう。

（６）情報システム

山形村の各種電子計算機（ネットワーク、ハードウェア及びソフトウェア）及び電磁的記録媒体で構成され、処理を行う仕組みをいう。

（７）情報資産

ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体並びに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。）並びに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をいう。

（８）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。

（９）機密性

情報にアクセスすることを認められた者だけがアクセスできる状態を確保することをいう。

(10) 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。

(11) 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。

(12) サイバーセキュリティ

サイバーセキュリティ基本法（平成 26 年法律第 104 号）第２条に規定されるサイバーセキュリティをいう。

(13) 情報セキュリティインシデント

望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、行政事務の運営を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

(14) 職員等

山形村が管理する情報資産に関する業務に携わる職員、会計年度任用職員等をいう。

(15) 委託事業者

業務委託先社員（地方自治法（昭和 22 年法律第 67 号）第 244 条の２第３項に規定する指定管理者を含む。）等、契約に基づいて山形村の機関で作業する者の総称をいう。

(16) 公共端末

山形村の情報資産のうち、山形村の施設等に設置され、村民等が自由に操作する端末の総称をいう。

(17) 部外者

職員等及び外部委託者以外の山形村の情報資産に接することが認められていない者の総称をいう。

(18) 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。

(19) 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。）

(20) 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。

(21) 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。

(22) 無害化通信

インターネットメールの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ない等、安全が確保された通信をいう。

第３条　対象とする脅威

情報資産に対する脅威として、次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。

（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

第４条　情報セキュリティポリシーの対象範囲

情報セキュリティポリシーの適用範囲は、次に掲げるものとする。

（１）適用資産

情報セキュリティポリシーの適用対象資産は、山形村における全ての情報資産とする。

（２）適用実施機関の範囲

情報セキュリティポリシーの適用対象実施機関は、村長部局、教育委員会事務局、選挙管理委員会事務局、監査委員、農業委員会事務局、固定資産評価審査委員会及び議会事務局とする。

（３）適用対象者

情報セキュリティポリシーの適用対象者は、前号に規定する適用資産に接する全ての職員等とする。

（４）適用情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。ただし、小中学校で利用しているネットワーク及び情報システムについては、内部情報系システムに限る。

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

第５条　職員等の遵守事項

山形村が所掌する情報資産に関する業務に携わる職員等及び外部委託者は、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。

第６条　情報セキュリティ対策

山形村の情報資産を第３条に示した脅威から保護するために、次に掲げる情報セキュリティ対策を講じる。

（１）組織体制

山形村の情報資産について、適正に情報セキュリティ対策を推進・管理するための全庁的な組織体制を確立する。

（２）情報資産の分類と管理

情報資産をその内容の重要度に応じて分類し、当該分類に基づいた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。

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、LGWAN と接続する業務システムと、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。

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、長野県と長野県内市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を実施する。

（４）物理的セキュリティ対策

サーバ等、情報システムを設置する施設等、通信回線等及び職員等のパソコン等の管理について、情報資産の盗難、損傷・妨害等から保護するために物理的な対策を講じる。

（５）人的セキュリティ対策

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、全ての職員等に対して情報セキュリティポリシーの内容を周知徹底する等、教育、訓練、啓発等を実施し、外部委託者に対しても情報セキュリティポリシーの内容のうち必要となる部分を周知徹底する。

（６）技術的セキュリティ対策

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、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）業務委託と外部サービスの利用

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情報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。

第７条　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。

第８条　情報セキュリティポリシーの見直し

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。

第９条　情報セキュリティ対策基準の策定

第６条～第８条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。

第 10 条　情報セキュリティポリシーの情報公開

情報セキュリティ基本方針及び対策基準は、公にすることにより山形村の行政運営に重大な支障を及ぼすおそれのある情報であることから非公開とする。