白馬村情報セキュリティポリシー

【情報セキュリティ基本方針】

平成15年10月22日　策定

令和4年8月30日　改定

令和8年３月３日　改定

白　馬　村

目　次

序　章　白馬村情報セキュリティポリシーの構成

白馬村情報セキュリティポリシー（以下「情報セキュリティポリシー」という）とは、白馬村が保有する情報資産に関する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る。

情報セキュリティポリシーは、本村の情報資産を取り扱う職員（会計年度任用職員及び臨時的任用職員を含む。以下「職員等」という。）及び外部委託事業者に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、情報セキュリティ対策は、情報の処理技術や通信技術等の進展に伴う急速な状況の変化に、柔軟に対応することも必要である。

以上のことから、情報セキュリティポリシーは、一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（対策基準）に分けて策定する。

具体的には、情報セキュリティポリシーを、

① 情報セキュリティ基本方針

② 情報セキュリティ対策基準

の2階層に分け、それぞれを策定することとする。

また、情報セキュリティポリシーに基づき、情報システムごとに、具体的な情報セキュリティ対策の実施手順（運用マニュアル）として「情報セキュリティ実施手順」を策定する。

白馬村情報セキュリティポリシーの構成

文 書 名		内　　容
情報セキュリティポリシー	基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	対策基準	情報セキュリティ基本方針を実行に移すための、全ての情報資産に共通の情報セキュリティ対策の基準
情報セキュリティ実施手順		情報システムごとに定める、情報セキュリティ対策基準に基づいた個々の情報資産に関する具体的な対策手順

第1章　情報セキュリティ基本方針

1　目的

本村が取り扱う情報資産には、村民の個人情報を始めとし行政運営上重要な情報など、部外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おり、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、プライバシー等を守るためにも、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る。

このため、本村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を整備するため、情報セキュリティポリシーを定めることとし、情報セキュリティの確保に最大限取り組むこととする。

このうち情報セキュリティ基本方針においては、本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。

(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認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完全防御すること。

可用性(availability)　:許可された使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)課等

白馬村課設置条例(平成7年3月27日条例第2号)第 1 条に規定する課、会計室、教育委員会事務局、議会事務局、をいう。

(2)事務所管課

その保有するデータの一部又は全部の電子計算機処理を行うことにより所管する事務を行う課(これに準ずるものを含む以下同じ。)をいう。

(3)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並びに記録媒体(磁気ディスク等並びに入出力帳票及び情報システム仕様書等)をいう。

(4)電磁的記録媒体等

電子計算機に使用される磁気ディスク、磁気テープ、光ディスク、その他これらに類する記録媒体をいう。

(5)電算室等

電子計算機を運用管理する目的で設置している部屋をいう。

(6)ネットワーク

電子計算機等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)等をいう。

(7)情報システム

電子計算機、ネットワーク及び電磁的記録媒体で構築され、情報処理を行う仕組みをいう。

(8)行政情報

本村の行政事務の執行に関わる情報で、かつ情報システムで取扱うものをいう。

(9)情報資産

①ネットワーク、情報システム、行政情報及びこれらに関する設備、電磁的記録媒体等

②コンピュータ、ネットワーク及び情報システムで取り扱うデータ(これらを印刷した文章を含む。)

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

(10)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。

(11)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。)

(12)インターネット接続系

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。

(13)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。

(14)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。

(15)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。

3 情報セキュリティポリシーの位置づけ

情報セキュリティポリシーは、本村の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最高位に位置するものである。

したがって、情報資産に関する業務に携わるすべての職員等及び外部委託業者は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行にあたっては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。

4 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対象範囲は、本村における情報資産及び情報資産に接する職員等を含む及び外部委託事業者とする。

5 職員等の義務

職員等は、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、情報資産の利用にあたっては情報セキュリティポリシーを遵守しなければならない。

6 情報セキュリティ管理体制

本村の情報資産について、適切に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 情報資産への脅威

情報セキュリティポリシーを講ずるにあたっては、情報資産に対する脅威の発生度合いや発生した場合の影響を考慮するものとする。特に認識すべき脅威は以下のとおりである。

(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・消却、重要情報の搾取、内部不正使用等

(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・委託監査機能の不備、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完全等

(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

8 情報セキュリティ対策

本村の情報資産を上記7の脅威から保護するため、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

本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

本村の所有する情報資産をその重要度に応じて分類し、それに応じたセキュリティ対策を行うものとする。

(3)情報システム全体の強靭化の向上

情報セキュリティの強化を目的とし、業務の効率化・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ずる

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。

②ＬGWAN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うえで、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)人的セキュリティ対策

情報資産に接する職員等の情報セキュリティに関する権限や責任等を定めるとともに、すべての職員に情報セキュリティポリシーの内容周知徹底するため、教育・訓練等の人的な対策を講ずる。

(5)物理的セキュリティ対策

サーバ等、電算室等、通信回線等及職員等のパソコン等の管理について不正な立入り、情報資産への損傷、盗難等から保護するため、入退室や機器管理上の物理的な対策を講ずる。

(6)技術的セキュリティ対策

情報資産を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、コンピュータウィルス対策等技術的な対策を講ずる。

(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、セキュリティポリシー運用面の対策を講する。また、緊急事態が発生した場合に、迅速かつ適切な対応が可能となるような危機管理体制の整備等による対策を講ずる。

9 業務委託等及び外部サービス(クラウドサービス)の利用

業務委託等をする場合は、業務委託事業者等を選定し、情報セキュリティ要件を明記した契約を締結し、業務委託事業者等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ずる。

クラウドサービスを利用する場合には、外部サービス(クラウドサービス)利用基準を整備し対策を講ずる。

10 情報セキュリティ対策基準の策定

本村の情報資産について、上記8、9の情報セキュリティ対策を講ずるに当たっては、職員等が遵守すべき事項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。

11 情報セキュリティ運用マニュアルの策定

情報セキュリティ対策を確実に実施していくためには、個々の情報資産に関する対策の手順を具体的に定めておく必要があることから、情報セキュリティ対策基準に基づき、情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ運用マニュアルは、公開することにより本村の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

12 評価・見直し

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、情報システムの変更、新たな脅威等情報セキュリティを取り巻く状況の変化を踏まえ、適宜情報セキュリティ対策基準の見直しを実施するものとする。

13 情報セキュリティポリシーに関する違反への対応

セキュリティポリシーに違反した者については、その重大性、発生した事案の状況等に応じて懲戒処分を含む必要な処置を講ずる。