

小川村情報セキュリティポリシー

基本方針

【令和8年 3月改訂】

目次

序 情報セキュリティポリシーの構成	3
(1) 情報セキュリティ基本方針	3
(2) 情報セキュリティ対策基準	3
1 目的	4
2 用語の定義	4
3 対象とする脅威	6
4 情報セキュリティポリシーの対象範囲	6
(1) 適用資産	6
(2) 適用対象者	6
(3) 適用対象行政機関	7
5 職員等の守事項	7
6 情報セキュリティ対策	7
(1) 組織体制	7
(2) 情報資産の分類と管理	7
(3) 情報システム全体の強靱性の向上	7
(4) 物理的セキュリティ対策	7
(5) 人的セキュリティ対策	7
(6) 技術的セキュリティ対策	8
(7) 運用	8
(8) 外部サービス(クラウドサービス)の利用	8
7 情報セキュリティ監査及び自己点検の実施	8
8 情報セキュリティポリシーの見直し	8
9 情報セキュリティ対策基準の策定	8
10 情報セキュリティ実施手順の策定	8
11 情報セキュリティポリシーの情報公開	9

序 情報セキュリティポリシーの構成

情報セキュリティポリシーとは、小川村の情報資産に対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とする。情報セキュリティポリシーは、小川村の情報資産に関する業務に携わる職員等、及び外部委託業者に浸透、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、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを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)の2階層に分けて策定することとした。

(1)情報セキュリティ基本方針

小川村としての情報セキュリティ対策に関する取り組み姿勢及び統一的な方針。

(2)情報セキュリティ対策基準

情報セキュリティ基本方針を実行に移すための小川村におけるすべてのネットワーク及び情報システムに共通の情報セキュリティ対策の基準。

1 目的

小川村の情報資産には、住民の個人情報をはじめ行政運営に必要な情報など、部外に漏洩、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、住民の財産、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、小川村に対する住民からの信頼の維持向上に寄与するものである。

また、近年のいわゆるIT革命の進展により、電子政府や電子自治体の実現が期待されている中で、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となる。

このため、小川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、小川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、小川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。

2 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。

(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、小川村役場本庁、出先機関、各種委員会、議会事務局、教育機関、福祉施設等の事務室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

小川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

ネットワーク及び情報システムの開発と運用に係る全てのデータ並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。

(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。

(10) 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安全防護すること。

(11) 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。

(12) 職員

地方公務員法で規定された特別職、一般職の中で、小川村に勤務する者の総称をいう。

(13) 関係機関の職員等

各種委員会、議会事務局、福祉施設等に勤務し、小川村が管理する情報資産を職務で利用する者の総称をいう。

(14) 職員等

小川村が管理する情報資産を職務で利用する職員及び関係機関の職員等(それぞれ非常勤職員及び臨時職員等を含む)の総称をいう。

(15) 外部委託者

職務委託先社員等、契約に基づいて小川村の機関で作業する者の総称をいう。

(16) 部外者

職員等及び外部委託者以外の小川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。

(17) 公共端末

小川村の情報資産のうち、小川村の施設等に設置され、職員等及び外部委託者以外の者が利用できる端末の総称をいう。

(18) 不正アクセス

不正アクセス行為の禁止等に関する法律(平成11年法律第128号)第3条第2項に規定する不正アクセス行為その他の不正な手段により利用者以外の者が行うアクセス又は利用者が行う権限外のアクセスをいう。

(19) 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。

(20) 部外者

職員等及び外部委託者以外の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。

(21) 個人番号利用事務系

個人番号利用事務(行政手続における特定の個人を識別するための番号の利用等)

関する法律第9条第1項及び第2項に定める事務)、その他の基幹系事務、及び戸籍事務等に関わる情報システム及びデータをいう。

(22) LGWAN接続系

人事給与、財務会計、グループウェア及び文書管理等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扱うデータをいう。

(23) 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扱うデータをいう。

(24) 通信経路の分割

LGWAN接続系とインターネット接続系及び個人番号利用事務系とLGWAN接続系のそれぞれの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するようにすることをいう。

(25) 無害化通信

インターネットメールの本文及び添付ファイルのテキスト化やPDF化及びマクロ除去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

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適用範囲は、次の各項に定めるものとする。

(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、小川村における全ての情報資産とする。

(2) 適用対象者

情報セキュリティポリシーの適用対象者は、小川村における情報資産に接する全ての職員等

とする。

(3)適用対象行政機関

情報セキュリティポリシーの適用対象行政機関は、小川村の内部部局、行政委員会、議会及び地方公営企業とする。

5 職員等の遵守事項

小川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しなければならない。

6 情報セキュリティ対策

村の情報資産を上記3に示した脅威から保護するために、以下の情報セキュリティ対策を講ずる。

(1) 組織体制

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・管理するための全庁的な体制を確立する。

(2) 情報資産の分類と管理

情報資産をその内容に応じて分類し、当該分類に応じた情報セキュリティ対策を行う。

(3) 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 個人番号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、住民情報等の流出を防止する。
- ② L G W A N接続系においては、L G W A Nと接続する情報システムを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、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ずる。

(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、全ての職員等及び外部委託者に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切に対応するため、緊急時対応計画を策定する。

(8) 外部サービス（クラウドサービス）の利用

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。

約款による外部サービス（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。

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。

9 情報セキュリティ対策基準の策定

小川村の様々な情報資産について、上記6、7及び8に規定する対策等を講ずるに当たっては、職員等が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ことから、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、情報セキュリティ実施手順を策定するものとする。

11 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小川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。

附則

令和8年3月31日 改定