檜原村情報セキュリティポリシー

令和８年１月

檜原村

目　次

第１章　情報セキュリティ基本方針 1
1　目的 1
2　定義 1
3　対象とする脅威 2
4　適用範囲 3
5　職員等の遵守義務 3
6　情報セキュリティ対策 3
7　情報セキュリティ対策基準の策定 5
8　情報セキュリティ実施手順の策定 5
9　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の非公開 5
第２　情報セキュリティ対策基準 7
1　組織体制 7
2　情報資産の分類と管理 9
3　情報システム全体の強靭性の向上 12
4　物理的セキュリティ 14
5　人的セキュリティ 16
6　技術的セキュリティ 21
7　運用 33
8　業務委託と外部サービスの利用 36
9　評価・見直し 40

第１章　情報セキュリティ基本方針

１　目的

本基本方針は、本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、本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。

また、情報セキュリティに関する社会環境・技術環境の変化（サイバー攻撃の高度化、クラウド・IoT の普及等）に適切に対応し、行政サービスの安定的提供及び住民の信頼確保、法令遵守及び情報セキュリティ対策の継続的な改善を図ることも目的とする。

２　定義

（１）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。

（２）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。

（３）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。

（４）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。

（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をいう。

（９）LGWAN 接続系

総合行政ネットワーク（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。）。

（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をいう。

（11）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ないなど、安全が確保された通信をいう。

（12）クラウドサービス

インターネット等を通じて外部事業者が提供する、データ保存・システム運用等のサービスをいう。

（13）IoT 機器

インターネットを介して相互接続されるセンサー、カメラ等の機器をいう。

（14）サプライチェーン

村の情報資産保護に関する、委託先・外部サービス・再委託等の関係性をいう。

3　対象とする脅威

情報資産に対する脅威として、次の脅威を想定し、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、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障害からの波及等

（６）委託先・外部サービス利用等に起因する情報資産への脅威。

４　適用範囲

（１）行政機関の範囲

本基本方針が適用される範囲は、村長部局、教育委員会、地方公営企業、選挙管理委員会、監査委員、固定資産評価審査委員会及び議会事務局とする。ただし、教育委員会については、村長が管理運用する情報システムを利用する部署のみを対象とする。

（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

５　職員等の遵守義務

正規職員、会計年度任用職員（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、檜原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。）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。また、委託事業者及び外部サービス利用者も、村の情報セキュリティポリシー等を遵守し、必要な教育・研修・同意書等の取得を義務付けなければならない。

６　情報セキュリティ対策

３に規定する脅威から情報資産を保護するために、次の情報セキュリティ対策を講じる。

（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）情報資産の分類と管理

本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靱性の向上

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（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）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、東京都及び区市町村のインターネットとの通信を集約する自治体情報セキュリティクラウドの導入等を実施する。加えて、ランサムウェア等の高度化するサイバー攻撃に対し、多層防御体制を構築し、外部専門機関との連携を図る。

（4）物理的セキュリティ

サーバー、OA 室、通信回線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

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、十分な教育及び啓発を行うなどの人的な対策を講じる。

（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。

情報資産に対するセキュリティ侵害が発生した場合に迅速かつ適正に対応するため、情報セキュリティインシデント対応手順の標準化と、全職員等への訓練を定期的に実施する。

（8）業務委託と外部サービスの利用

業務委託する場合には、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。

（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。

7　情報セキュリティ対策基準の策定

６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。情報セキュリティ対策基準は、少なくとも年１回以上、リスクアセスメント（定期的なリスク分析・評価）を実施し、社会・技術環境の変化、サイバー攻撃の動向、国や都道府県のガイドライン改定等も踏まえたリスク評価と対策の見直しを行うこととする。クラウド・IoT・外部サービス利用時の特有リスク（データ保存場所・管轄法令・再委託・サービス停止・情報資産返還・廃棄・移行等）についても事前に評価し、契約に明記する。

8　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、標準化した情報セキュリティインシデント対応手順等を含む情報セキュリティ実施手順を策定することとする。実施手順は定期的に見直し、全職員等への周知・訓練を実施する。

9　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の非公開

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、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。

ただし、法令や国等の指導により必要な範囲で公表する場合がある。