大桑村情報セキュリティ基本方針

令和７年３月 21 日改定

総務課　危機管理係

改訂履歴

改訂年月日	改訂理由・内容
平成 27 年 12 月 22 日	策定
令和７年３月 21 日	改定

大桑村情報セキュリティ基本方針

１　目的

本村の情報システムが取扱う情報には、村民の個人情報や行政運営上重要な情報が多数含まれており、情報資産を人的脅威や災害、事故等様々な脅威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、本村が保有する情報資産の機密性、完全性及び可用性を維持し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して、大桑村情報セキュリティ基本方針（以下「情報セキュリティ基本方針」という。）を定める。

２　定義

情報セキュリティポリシーにおいて、次の各号に掲げる用語の意義は、それぞれの各号に定めるところによる。

（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

情報セキュリティ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

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）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、ウイルス攻撃等のサイバー攻撃や部外者の進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、重要資産の詐取、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、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および業務の停止等

（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　対象範囲

（１）対象組織

情報セキュリティポリシーが対象とする組織は、村長部局、教育委員会事務局（小中学校、保育園を含む）、選挙管理委員会事務局、監査委員事務局、農業委員会事務局、固定資産評価審査委員会事務局及び議会事務局とする。

（２）対象情報資産

情報セキュリティポリシーが対象とする情報資産は、次のとおりとする。

ア　本村が管理するネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

イ　本村が管理するネットワーク及び情報システムで取扱う情報（これらを印刷し

た文書を含む。）

ウ　本村が管理する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、非常勤職員及び臨時職員（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、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

情報資産への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）情報セキュリティ管理体制の確立

情報セキュリティ対策を確実に管理するための全庁的な体制を整備する。

（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、その重要度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。

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上で、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）物理的セキュリティ対策

コンピュータ及びネットワーク機器を設置する施設への不正な立入り、情報資産への損傷、盗難等から保護するための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する権限や責任及び遵守すべき事項を明確に定め、職員等

に対する周知及び徹底を図るとともに、十分な教育、啓発が行われるよう必要な対策を講じる。

（６）技術的セキュリティ対策

情報資産を不正アクセス等から保護するため、情報資産へのアクセス制限、ネットワーク管理等の対策を講じる。

（７）情報システムの監視、情報セキュリティ対策の遵守状況の確認等、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。

７　監査等の実施

情報セキュリティポリシーの遵守状況やセキュリティ対策について検証するため、定期的又は必要に応じて監査等を実施する。

８　情報セキュリティポリシーの見直し

監査等の結果、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

上記６、７及び８に規定する対策等を実施するため、具体的な遵守事項及び判断基準等を定める大桑村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具体的に実施するために、情報セキュリティ実施手順を必要に応じて策定する。

11　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扱い

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。