生坂村情報セキュリティポリシー

平成 29 年 6 月
令和　8 年 3 月　改訂

目次

序　生坂村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、生坂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文書を総称する。情報セキュリティポリシーは、生坂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。

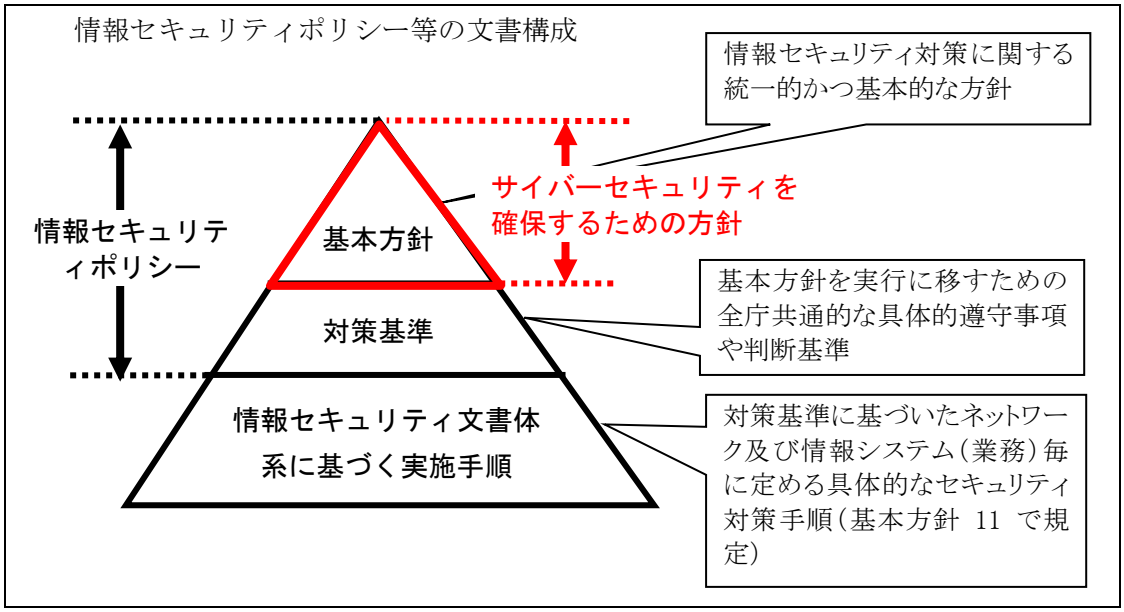
このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（対策基準）の２階層に分けて策定することとした。

（１）情報セキュリティ基本方針

生坂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生坂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。



第１章　情報セキュリティ基本方針

１　目的

生坂村の情報資産には、村民の個人情報をはじめ行政運営に必要な情報など、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、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、生坂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、生坂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、生坂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、生坂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、生坂村役場、出先機関、各種委員会、議会事務局、教育機関、福祉施設、医療機関等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

生坂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並びに業務で使用する書類、帳票等をいう。

（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。

（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ことを確保するこ

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) 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

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

(15) 関係機関の職員等

各種委員会、議会事務局、福祉施設、広域組合に勤務し、生坂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。

(16) 職員等

生坂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。

(17) 外部委託者

職務委託先社員（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、契約に基づいて生坂村の機関で作業する者の総称をいう。

(18) 公共端末

生坂村の情報資産のうち、生坂村の施設等に設置され、村民などが自由に操作する端末の総称をいう。

(19) 部外者

職員等及び外部委託者以外の生坂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。

(20) 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。

(21) マイナンバー利用事務系（個人番号利用事務系）

社会保障、地方税、防災等に関する個人番号利用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

LGWAN に接続された情報システム及び当該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刑を除く）。

(23) インターネット接続系

インターネットメール、ホームページ管理等のためインターネットに接続された情報システム及び当該システムで取り扱うデータをいう。

(24) 通信経路の分割

LGWAN 接続系とインターネット接続系を分離し、安全が確保された通信のみを許可することをいう。

(25) 無害化通信

インターネットメールのテキスト化や画面転送等により、ウィルス等の不正プログラムが付着していないか安全な通信をいう。

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、ウィルス攻撃、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

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、次の各号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、生坂村役場本庁、教育委員会、議会事務局、議会、選挙管理委員会、地方公営企業、監査委員等、教育機関、福祉施設等の事務室等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、前項に規定する適用資産に接する全ての職員等とする。

5　職員等の遵守事項

生坂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

生坂村の情報資産を３に示した脅成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

生坂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）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。

（4）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。

（5）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。

（6）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。

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

上記6、7及び8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。

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実施するための具体的な

手順を定めた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生坂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。