清川村情報セキュリティポリシー

（概要）

序文

清川村(以下、「村」という。)が取り扱う情報には、住民の個人情報のみならず、行政運営上重要な情報などが、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いる。

したがって、情報、情報を取り扱うネットワーク及び情報システム等を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、また、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが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。

また、近年のいわゆる IT 革命の進展により、村民生活においても高度情報化が急速に普及し、電子自治体の実現に対する村民のニーズも高まりをみせている。このような状況において本村が電子行政サービスを提供するためには、全ての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である。

このため、本村の有する情報等の機密性、完全性及び可用性を維持する上で必要な対策を整備するために情報セキュリティポリシーを定めることとする。

本村の職員等全員がこれに関与し、有効に機能するようこれを遵守することとする。

第1章　本書の目的

第1節　本書の目的

本書は、情報セキュリティポリシーの構成文書の一つである基本方針書として、本村の職員及び委託会社社員等の情報資産を扱う者全員が、情報資産を使用するときに従うべき、情報セキュリティを守るための基本的な考え方や方向性を定めるものである。

第2節　適用範囲

セキュリティポリシーの適用範囲は、本村の本庁が保有する情報資産、及び当該情報資産に接する本村の職員及び委託会社社員とする。

第3節 用語定義

(1) 機密性
アクセスを許可された者だけが情報にアクセスできることを確実にすること。

(2) 完全性
情報及び情報処理が、正確であること及び完全であることを保護すること。

(3) 可用性
認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。

(4) ネットワーク
本村におけるシステム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)及び記録媒体で構成され、処理を行う仕組み。

(5) 情報システム
ネットワーク、ハードウェア、ソフトウェア及び記録媒体で構成された情報を処理する仕組み。

(6) 情報資産
ネットワーク及び情報システムそのもの、及びそれらで取り扱う全ての電磁的情報。
職務において作成又は取得した文書、図画及び磁気テープや磁気ディスクその他これに類する媒体に記録された情報。

(7) 情報セキュリティ
情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持すること。

(8) 職員

本村の正職員、嘱託職員、非常勤職員、臨時職員。

(9) 情報主管者

主管する業務において、情報を収集、作成、又は村民等の第三者から情報を預託された部門の所属長をいう。

(10) 重要情報資産

セキュリティ面で何らかの管理が必要な情報資産。使用許可を得た入出力媒体等もこれに含む。

(11) 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。

(12) 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）

(13) 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燈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。

(14) 通信網の分割

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。

(15) 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等、安全が確保された通信をいう。

第2章　基本的な考え方

第1節　情報資産に関する脅威

情報資産に対する脅威の発生度合や発生した場合の影響の大きさを考慮すると、特に認識すべき脅威は以下のとおりである。

(1) 外部からの不正アクセス又は不正操作によるデータ又はプログラムの持ち出し・盗聴・改ざん・消去、機器及び媒体の盗難等
(2) 職員及び委託会社社員による誤操作、不正アクセス又は不正操作によるデータ又はプログラムの持ち出し・盗聴・改ざん・消去、機器及び媒体の盗難及び規定外の端末接続によるデータ漏洩等
(3) 地震、落雷、火災、風水害等の災害によるサービスの停止
(4) 事故、故障、障害等によるサービスの停止
(5) 大規模・広範囲にわたる疫病等による要員不足に伴う運用の機能不全等

第2節　セキュリティレベル

前節で示した脅威から情報資産を保護するために、情報が不当に他者に漏洩しない(機密性)、情報が改ざんされない(完全性)、障害発生時にも継続して提供できる(可用性)の3つの側面を定義する。

情報資産の重要度に応じて、情報資産の機密性、完全性及び可用性を維持するために、セキュリティレベルを設定する。

セキュリティレベルごとに情報資産の保護管理要件を明確にし、想定されるリスク及びその対策を明確にする。

第3節　情報セキュリティ対策

情報資産を保護するために、以下の情報セキュリティ対策を講ずるものとする。

(1) 人的対策

情報セキュリティに関する権限及び責任を定め、職員等に基本方針及び情報セキュリティに関する法令等の内容を周知徹底する等、十分な教育及び啓発が行われるよう必要な対策を講ずる。

(2) 物理的対策

情報システム及びネットワークを設置する施設への不正な立ち入り、並びに情報システム、ネットワーク及び情報資産への損傷・妨害等から保護するための物理的な対策を講ずる。

(3) 技術的対策

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、ネットワーク管理等の技術面の対策を講ずる。

(4) 開発・運用上の対策

情報システム開発の外部委託、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等、開発・運用面の対策を講ずる。

また、緊急事態が発生した場合に速やかな対応を可能とするための危機管理対策を講ずる。

(5) 情報システム全体の強靭性の向上

情報システム全体に対し、次の対策を講じる

① マイナンバー利用事務系においては、他の領域との通信をできないようにし、端末からの情報の持出し不可設定や多要素認証等を導入する。

② LGWAN 接続系においては、接続する業務システムと、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、両システム間での通信にあっては、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、自治体情報セキュリティクラウド等を導入し、不正通信の監視機能の強化や高度な情報セキュリティ対策を実施する。

(6) 外部サービスの利用

外部委託する場合には、必要な情報セキュリティ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を利用する場合には、利用に係る規定を整備し必要な対策を講じる。

ソーシャルメディアサービスを利用する場合には、運用手順を定め、発信できる情報を規定する。

第３章　情報セキュリティポリシー等の取り扱い

第１節　基本方針

基本方針は、住民の個人情報及び行政運営上の情報の管理及び情報セキュリティ対策についての基本的な考え方や方向性を定める。外部に対し公開する。

第２節　対策基準

基本方針に基づいた情報セキュリティ対策を講じるに当たって、遵守すべき行為、判断等の基準を統一的に定めるために、必要となる基本要件を明記した対策基準を定める。

対策基準は、本村の情報資産を扱うすべての職員及び委託会社社員に対し、周知徹底する。対策基準は、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恐れのある情報であることから非公開とする。

第３節　実施手順

情報セキュリティポリシーを遵守して情報セキュリティ対策を実施するため、個々の部署や情報システムについて具体的な手順を明記した実施手順を定める。

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恐れのある情報であることから非公開とする。

第４節　情報セキュリティポリシーの改訂

情報セキュリティを取り巻く状況の変化に速やかに対応するため、情報セキュリティ監査の結果等も踏まえ、情報セキュリティポリシーは定期的に見直し、必要に応じて改訂する。