田舎館村情報セキュリティ基本方針

第１章　情報セキュリティ基本方針

１　趣旨

田舎館村（以下「村」という。）の各情報システムが取り扱う情報には、住民の個人情報を筆頭に、外部への漏えい等が発生した場合に、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、情報セキュリティポリシーを策定し、機密性、完全性及び可用性（注）を維持するために情報セキュリティに関する基本的事項を定めることにより、情報資産、情報資産を取り扱うネットワーク及び情報システムを様々な脅威から防御するよう高度な安全性を有することは、住民の財産やプライバシー等を守るためにも、また、業務の安定性確保のためにも必要不可欠であり、ひいては、このことが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。

（注）機密性（confidentiality）：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。
　　完全性（integrity）：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。
　　可用性（availability）：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。

２　定義

（１）ネットワーク

パソコン、サーバ等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）をいう。

（２）情報システム

電子計算機（ハードウェア及びソフトウェア）、ネットワーク及び電磁的記録媒体で構成され、処理を行う仕組みをいう。

（３）情報資産

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、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。）並びに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をいう。

（４）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。

（5）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。

3　情報セキュリティポリシーの位置付けと職員等の義務

情報セキュリティポリシーは、村の情報資産に関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であり、情報セキュリティ対策の頂点に位置するものである。

したがって、村の情報資産に関する業務に携わる全ての職員（再任用職員及び任期付職員を含む。）、非常勤職員、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。

4　情報セキュリティ管理体制

情報セキュリティ対策を推進し、村が保有する情報資産を適切に管理するため、情報セキュリティ対策の最高責任者を定め全庁的な組織体制を確立する。

必要な体制、役割、権限等については、情報セキュリティ対策基準にて定める。

5　情報資産の分類

村が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、当該分類に基づいて情報セキュリティ対策を実施する。

6　情報資産への脅威

情報セキュリティ対策を講ずるうえで、情報資産に対する脅威の発生度合いや発生した場合の影響を考慮すると、特に認識すべき脅威は以下のとおりである。

（1）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

（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提供サービスの障害からの波及等

7　情報セキュリティ対策

村の情報資産を上記６の脅威から保護するため、以下の情報セキュリティ対策を講ずるものとする。

（１）物理的セキュリティ対策

管理区域への不正な立入りを防ぎ、情報システム損傷等から保護するために物理的な対策を講ずる。

（２）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を定め、職員等に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発を行う。

（３）技術的セキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため、情報システムの管理、情報資産へのアクセス制御、不正プログラムの防御等の技術面の対策を講ずる。

（４）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　情報セキュリティ対策基準の策定

村の情報資産について、上記７の情報セキュリティ対策を講ずるに当たっては、職員等が遵守すべき事項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こととする。

なお、情報セキュリティ対策基準は、公開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のある情報であることから非公開とする。

9　情報セキュリティ実施手順（運用マニュアル）の策定

情報セキュリティ対策を確実に実施していくためには、個々の情報資産に関する対策の手順を具体的に定めておく必要があることから、情報セキュリティ対策基準に基づき、情報セキュリティ実施手順を策定することとする。

なお、情報セキュリティ実施手順は、公開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のある情報であることから非公開とする。

10　自己点検及び見直しの実施

情報セキュリティポリシーの遵守状況を検証するため、必要に応じて自己点検を実施する。

自己点検の結果等により、情報セキュリティ対策基準に定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、情報セキュリティポリシーの見直しを実施する。