塩尻市辰野町中学校組合情報セキュリティ基本方針

1　目的

組合が取り扱う情報には、生徒の個人情報をはじめ行政運営上重要な情報など、漏洩、改ざんがあった場合には、生徒及び行政サービスに極めて重大な影響を与える情報が多く含まれている。

これらの情報を保護し、生徒のプライバシー、財産等を守るとともに、安定的な行政運営を図るための情報セキュリティ対策の推進は、行政の責務である。

このため、塩尻市辰野町中学校組合情報セキュリティポリシーを定め、組合が保有する情報資産の機密性、完全性、可用性を維持するために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。

2　定義

(1)　組合等

組合長、教育委員会、公平委員会、監査委員及び議会をいう。

(2)　職員等

組合等の特別職を含む全ての職員（会計年度任用職員を含む）をいう。

(3)　行政情報

職員等が職務上作成し、取得した情報で、その記録媒体の形態にかかわらず本組合が管理しているものをいう。

(4)　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（ハードウエア及びソフトウエア）をいう。

(5)　情報システム

ハードウェア、ソフトウェア、ネットワーク、記録媒体等で構成され、これらの一部又は全体で業務処理を行う仕組みをいう。

(6)　記録媒体

行政情報の記録、管理に使用される帳票類及び電子媒体（磁気ディスク、磁気テープ、光ディスク等）をいう。

(7)　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確保し、維持することをいう。

(8)　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。

(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、情報にアクセスできる状態を確保することをいう

(10)　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。

(11)　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。

3　対象者の範囲

情報セキュリティポリシーの対象者の範囲は、職員等及び組合等の情報資産の取り扱いを含む業務を委託された者（以下「委託事業者」という。）とする。ただし、職員等以外の組織の者がネットワーク等を利用し、組合等の情報資産を利用する場合は、情報セキュリティポリシーの対象とする。

4　情報セキュリティポリシー対象者の義務

情報セキュリティポリシーの対象者は、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及び関係法令等を遵守しなければならない。

5　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、情報システム及びこれらに関する設備、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

6　情報資産に対する脅威

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)　情報資産の不適切な持ち出し、無許可ソフトウエアの使用等の規律違反、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破壊、漏えい、改ざん、消去等

(2)　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

(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

7　情報セキュリティ対策

組合等の情報資産を６の脅威から保護するため、次の情報セキュリティ対策を実施するものとする。

(1)　組織体制

本組合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

情報資産を、その重要度に応じて分類し、分類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

情報システム全体に対し、次の三段階の対策を講じる。

ア　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。

イ　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。

ウ　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、都道府県と市区町村のインターネット接続口を集約した上で、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

情報システムを設置する施設への不正な立入り及び情報資産の破損、盗難等から防止するため、物理的な対策を講ずるものとする。

(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を定めるとともに、職員等及び委託事業者に情報セキュリティポリシーの内容を周知徹底するため、教育及び啓発等の必要な対策を講ずるものとする。

(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技術面の対策を講ずるものとする。

(7)　運用におけるセキュリティ対策

情報資産を不正アクセス等から保護するため、情報システム監視、情報セキュリティポリシー遵守状況の確認等、業務委託を行う際のセキュリティ確保等、運用面

の対策を講ずるものとする。また、緊急事態が発生した際に迅速な対応を可能とするための緊急時対応計画を講ずるものとする。

(8)　業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、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（クラウドサービス）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。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

８　情報セキュリティ対策基準の策定

情報セキュリティ基本方針に基づく情報セキュリティ対策を実施するため、組合等において遵守すべき事項及び判断等の基準を統一的にレベルで定める情報セキュリティ対策基準を策定する。

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基準を遵守して情報セキュリティ対策を実施するため、個々の情報資産についての管理、利用等に関する取扱いを定める情報セキュリティ実施手順を策定する。なお、情報セキュリティ実施手順書は、公にすることにより本組合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。

１０　情報セキュリティ監査

情報セキュリティポリシーが遵守されていることを検証するため、定期的に情報セキュリティの監査を実施し、運用改善を行い情報セキュリティの向上を図る。

１１　評価及び見直しの実施

情報セキュリティの監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の有効性等について評価するとともに、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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーの見直しを実施する。