佐久環境衛生組合
情報セキュリティポリシー

令和８年３月

佐久環境衛生組合総務課

目　次

序　佐久環境衛生組合情報セキュリティポリシーの構成

佐久環境衛生組合情報セキュリティポリシーとは、佐久環境衛生組合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。佐久環境衛生組合情報セキュリティポリシーは、佐久環境衛生組合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。（図 1 情報セキュリティポリシー等の文書構成）

① 佐久環境衛生組合情報セキュリティ基本方針
　佐久環境衛生組合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 佐久環境衛生組合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佐久環境衛生組合における全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。

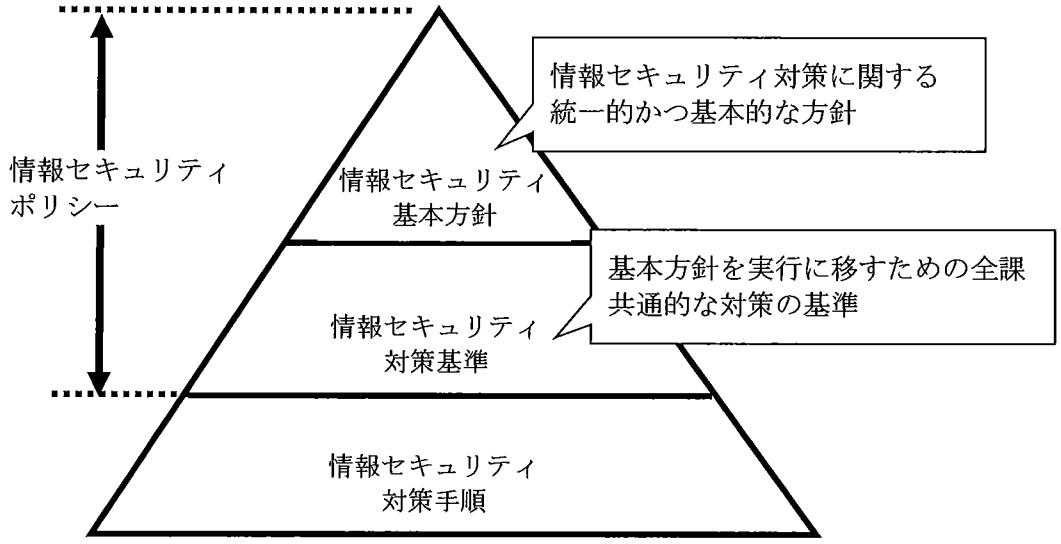

図 1 情報セキュリティポリシー等の文書構成

※　情報セキュリティ対策手順については、別途、手順書、運用の手引きのほか、
対応マニュアル等に示す。

第１章

情報セキュリティ基本方針

改版履歴

版　数	改　正　日	
第１版	令和 ８年　３月　27 日	策定

第1章　情報セキュリティ基本方針

1　目的

組合の情報資産には、住民の個人情報をはじめ行政運営に必要な情報など、部外に漏えい、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、住民の財産、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、組合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。

また、デジタル技術の活用による行政サービスの向上及び業務の効率化を推進する上で、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となる。

本基本方針は、佐久環境衛生組合（以下「本組合」という。）が保有する情報資産の機密性、完全性及び可用性を維持するため、本組合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する。

2　定義

佐久環境衛生組合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、該当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) 庁内ネットワーク
　ネットワークのうち、本組合の事務室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。

(3) 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。

(4) 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をいう。

(5) 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。

(6) 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。

(7) 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。

(8) 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。

(9) 職員

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

(10) 関係機関の職員等

南佐久浄化センター・佐久平環境衛生センターに勤務し、組合が管理する情報資産を職務で利用する者の総称をいう。

(11) 職員等

組合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会計年度任用職員等を含む）の総称をいう。

(12) 情報系（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。(佐久市の情報系端末であるため、扱いについては佐久市情報セキュリティポリシーを準用する。)

(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。

(14) 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。

(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。

ア 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

イ 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

ウ　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

エ　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

オ　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　適用範囲

4.1 行政機関の範囲

情報セキュリティポリシーが対象とする機関は、内部の課、下水道事業、し尿処理事業とする。

4.2 情報システムの範囲

情報セキュリティポリシーが対象とする情報システムは、組合長の権限に属する課等が管理運営するものに限る。なお、組合長の権限に属する課等以外の管理運営する情報システムを利用する場合において、この情報セキュリティポリシーを準用することを妨げない。

4.3 情報資産の範囲

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　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　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。）

ウ　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

職員等は、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及び情報セキュリティ対策手順を遵守する義務を負うものとする。

6　情報セキュリティ対策

上記3の脅威から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じる。

6.1 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。

6.2 情報資産の分類と管理

本組合の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、当該分類に基づき情報セキュリティ対策を行う。

6.3 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。

ア　情報系（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。

イ　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セキュリティ対策を実施する。

6.4 物理的セキュリティ

サーバ、電算エリア、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

6.5 人的セキュリティ

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、十分な教育及び啓発を行う等の人的な対策を講じる。

6.6 技術的セキュリティ

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。

6.7 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、業務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の緊急時対応計画を策定する。

6.8 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。

6.9 評価・見直し

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し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

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、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を見直す。

9　セキュリティポリシー対策基準の策定

及び上記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　情報セキュリティポリシー対策手順の策定

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。

なお、情報セキュリティ対策手順は、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。