千曲坂城消防組合情報セキュリティポリシー

（目的）

第１　千曲坂城消防組合情報セキュリティポリシー（基本方針）（以下「情報セキュリティポリシー」という。）は、千曲坂城消防組合（以下「消防組合」という。）が保有する情報資産を様々な脅威から防ぎょし、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について、基本的な事項を定めることを目的とする。

（定義）

第２　次の各項に掲げる用語の意義は、それぞれ当該各項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）　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。

（３）　情報資産

情報システム及び情報システムで取り扱うすべての情報をいう。

（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

本基本方針及び情報セキュリティ対策基準をいう。

（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）　特定個人情報

行政手続における特定の個人を識別するための番号の利用等に関する法律（以下「番号法」という。）第２条第８項に規定する、個人番号をその内容に含む個人情報ファイルをいう。

(10)　個人番号利用事務

番号法第２条第 10 項に規定する個人番号を利用して処理する事務をいう。

(11)　個人番号関係事務

番号法第２条第 11 項に規定する個人番号利用事務に関して行われる他人の個人番号を利用して行う事務をいう。

(12)　基幹系ネットワーク

消防組合の業務内容と直接関わるシステムであって、インターネットに接続された情報通信ネットワークをいう。簡単には代用が効かず、そのため運用するうえで堅固なセキュリティ環境が求められるシステムとなる。

(13)　情報系ネットワーク

消防組合が処理する事務に係る情報システムであって、インターネットに接続されないもののみにより構成される情報通信ネットワークをいう。

(14)　インターネット接続系ネットワーク

ホームページの更新及びウェブサイトの閲覧、その他主としてインターネットを利用して行う事務に係る情報システムのみにより構成される情報通信ネットワークをいう。

(15)　個別ネットワーク

前３項目に掲げる情報通信ネットワーク以外の情報通信ネットワークをいう。

(16)　LGWAN（総合行政ネットワーク）

地方公共団体情報システム機構が整備・運営する地方公共団体間のコミュニケーションの円滑化と情報の共有による情報の高度利用を図ることを目的とした行政機関専用のコンピュータネットワークをいう。

(17)　インターネット接続系

インターネット、ホームページ管理システム等に係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。

(18)　通信経路の分割

情報系ネットワークとインターネット接続系ネットワーク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。

(19)　無害化通信

インターネットメールの無害化やファイルの無害化により、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。

（対象とする脅威）

第３　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、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）　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漏えい・破壊・消去等

（３） 地震、落雷、火災等の災害、事故、故障等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等による職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

（情報資産の範囲）

第４　情報セキュリティポリシーの情報資産の範囲は、次のとおりとする。

（１） ネットワーク及び情報システムに関する次の情報資産（表１に分類する。）

ア　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

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構成図等のシステム関連文書

（２） 行政情報（千曲市情報公開条例第２条第１項第２号公文書）

※個人的資料及びメモ類は情報資産の範囲外とするが、作成から廃棄まで個人が確実に管理する。

表１　情報資産の種類と例示

情報資産の種類	情報資産の例
ネットワーク	通信回線、ルータ等の通信機器
情報システム	サーバ、パソコン、モバイル端末、オペレーティングシステム、ソフトウェア等
これらに関する施設・設備	情報システム室、コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル
電磁的記録媒体	サーバ装置、パソコン、通信回線装置等に内蔵される内蔵電磁的記録媒体、外付けハードディスク、CD、DVD、BD、USB メモリ、デジタルカメラ、IC レコーダー、磁気テープ等の外部電磁的記録媒体
ネットワーク及び情報システムで取り扱う情報	ネットワーク、情報システムで取り扱うデータ（これらを 印刷した文書を含む。）
システム関連文書	システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等

（職員の遵守義務）

第５　職員は、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を遵守しなければならない。

（情報セキュリティ対策）

第６　第３に掲げる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。

（１）　組織体制

消防組合の情報資産について、情報セキュリティ対策を確実に管理するため、消防組合情報セキュリティ対策委員会を設置する。

（２）　情報資産の分類と管理

本組合の保有する情報資産を侵害された場合に想定される影響の大きさに応じて分類し、当該分類に基づき情報セキュリティ対策を講じる。

分類	分類基準	取扱制限
機密性	業務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	・支給以外の端末での作業の原則禁止（機密性の情報資産に対して） ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
完全性	業務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	
可用性	機密性又は完全性の情報資産以外の情報資産	

（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 基幹系ネットワークにおいては、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 情報系ネットワークにおいては、LGWAN と接続する業務用システムと、インターネット接続系ネットワーク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ネットワークにおいては、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。

（4） 物理的セキュリティ

コンピュータ及びネットワーク機器等を設置する施設等への不正な立ち入り、情報資産への損傷、盗難等からの保護及び職員のパソコン等の管理について、物理的な対策を講じる。

（5） 人的セキュリティ

情報セキュリティに関し、遵守すべき事項を職員に周知及び徹底を図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） 技術的セキュリティ

情報資産を不正アクセス等から保護するために、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。

（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、緊急事態が発生した場合等に迅速かつ適正に対応するための危機管理体制の整備等による対策を講ずる。

（8） 業務委託と外部サービスの利用

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。

（情報セキュリティ監査及び自己点検の実施）

第7 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。

（情報セキュリティポリシーの見直し）

第８　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。

（情報セキュリティ対策基準の策定）

第９　上記第６、第７及び第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。

（情報セキュリティ実施手順の策定）

第10　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、情報セキュリティ実施手順は、公にすることにより消防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。

附　則

この訓令は、令和８年４月１日から施行する。