泉州南消防組合情報セキュリティポリシー
に基づく情報セキュリティ基本方針

施行日：令和７年　９月２２日
改正日：令和８年１０月　１日

目次

第１章　情報セキュリティ基本方針

内容

１　目的 1

２　用語の定義 1

３　対象とする脅威 2

４　適用範囲 3

５　職員等の遵守義務 3

６　情報セキュリティ対策 3

７　情報セキュリティ監査及び自己点検の実施 4

８　情報セキュリティポリシーの見直し 4

９　情報セキュリティ対策基準の策定 5

10　情報セキュリティ実施手順の策定 5

はじめに

泉州南消防組合情報セキュリティポリシーは、泉州南消防組合（以下、「消防組合」という。）が保有する情報資産の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まとめたものであり、情報セキュリティに対する取組姿勢を示す情報セキュリティ基本方針と、情報セキュリティを確保するために遵守すべき行為及び判断等の基準を示す情報セキュリティ対策基準から構成される。

第１章　情報セキュリティ基本方針

１　目的

本基本方針は、消防組合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、消防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。

また、本基本方針は地方自治法第 244 条の 6 第 1 項の規定に基づき、サイバーセキュリティを確保するための方針として位置付け、消防組合がどのように情報セキュリティの確保を図るかを住民に広く公表するものである。

２　用語の定義

情報セキュリティポリシーにおける用語の定義は、次のとおりとする。

⑴　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。

⑵　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。

⑶　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。

⑷　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。

⑸　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。

⑹　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。

⑺　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。

⑻　インターネット接続系

インターネットメール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。

⑼　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。

⑽　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。

⑾　ID

情報システムを利用する権利を有するものであることを識別するために割当てる文字列をいう。

⑿　パスワード

情報システムを利用する者が本人であることを識別するための暗証文字列をいう。

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。

⑴　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

⑵　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、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

⑶　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

⑷　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

⑸　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

⑴　範囲

情報セキュリティポリシーの適用範囲は、消防組合の情報資産を有するすべてとする。

⑵　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。

①　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

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

5　職員等の遵守義務

職員等（再任用職員、会計年度任用職員及び消防組合が認めた者を含む。以下同様。）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実施手順を遵守しなければならない。

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。

なお、個人情報を取り扱い、又は情報システムを構築し、若しくは利用するに当たっては、サイバーセキュリティ基本法第 26 条第 1 項第 2 号に規定するサイバーセキュリティに関する対策の基準に基づき、取り扱う保有個人情報の内容に照らして適正なサイバーセキュリティの水準を確保するものとする。

⑴　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推進する全庁的な組織体制を確立する。

⑵　情報資産の分類と管理

消防組合の保有する情報資産を機密性、完全性及び可用性等に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

⑶　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、次の二段階の対策を講じる。

①　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、

原則として無害化通信を実施する。

② 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。

⑷ 物理的セキュリティ

サーバ、情報システム室、ハードウェア等を設置する場所の安全確保及び通信回線や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。

⑸ 人的セキュリティ

情報セキュリティに関し、職員及び外部委託先等を含めた体制全体を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。

⑹ 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。

⑺ 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正に対応するため、緊急時対応手順を策定する。

⑻ 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、委託事業者のみならず、再委託先を含めたサプライチェーン全体での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、利用に係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。

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　情報セキュリティ対策基準の策定

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　情報セキュリティ実施手順の策定

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基準及び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。