

# 大垣消防組合情報セキュリティポリシー

版数	施行日
第 1 版	令和 8 年 4 月 1 日

大垣消防組合

## 目 次

### 第 1 章 情報セキュリティ基本方針

1	目 的	1
2	定 義	1
3	情報セキュリティポリシーの位置付け	2
4	情報セキュリティポリシーの構成	2
5	対象とする脅威	3
6	適用範囲	3
7	職員等の遵守義務	3
8	情報セキュリティ対策	3
9	情報セキュリティ対策基準の策定	4
10	情報セキュリティ実施手順の策定	4
11	法令遵守	5

# 第1章 情報セキュリティ基本方針

## 1 目的

本基本方針は、本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、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

### (1) 情報資産

情報資産とは、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、記録媒体
- イ ネットワーク及び情報システムで取扱う情報
- 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
- エ 職員等が職務上作成し、又は取得した文書等

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、モバイル端末等、汎用機、複合機、オペレーティングシステム、ソフトウェア(ウェブアプリケーション※を含む)、クラウドサービス等
ネットワーク及び情報システムに関する施設・設備	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
記録媒体	サーバ装置、端末、通信回線装置等に内蔵される内蔵記録媒体、USBメモリ、外付けハードディスクドライブ、DVD-R、磁気テープ等の外部記録媒体
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
職員等が職務上作成し、又は取得した文書等	申請書類、一覧のリスト、図画、写真等

### (1) 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。

### (3) 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。

### (4) 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。

(5) 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。

(6) 情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

(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維持することをいう。

(8) 情報セキュリティインシデント

情報資産の管理上の脅威となる確率が高い現象や事案をいう。具体的にはウイルス感染、第三者からの不正アクセスによる侵害、情報システム上の欠陥や誤動作による情報漏えい及び職員等による情報紛失等がある。

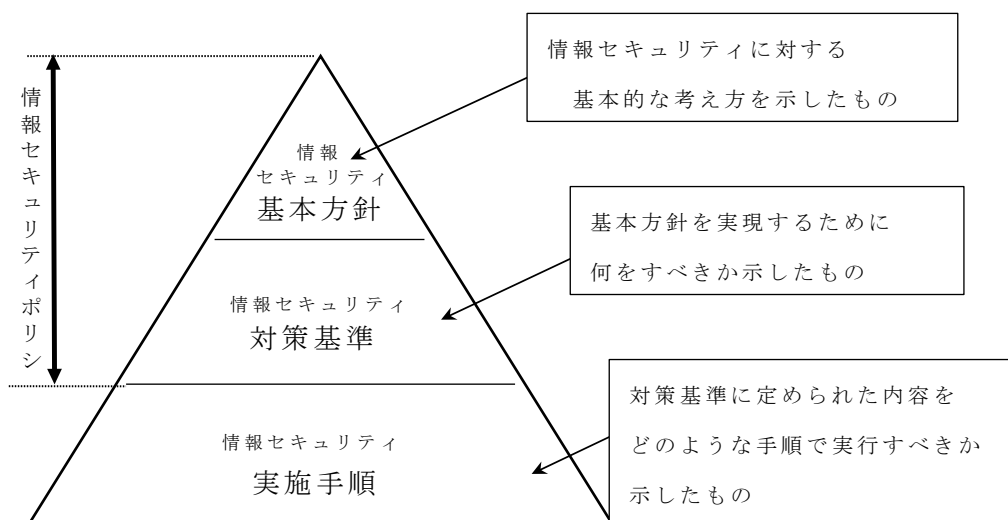
### 3 情報セキュリティポリシーの位置付け

(1) 情報セキュリティポリシーは、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。

(2) 情報セキュリティポリシーは、地方自治法第 244 条の 6 第 1 項に規定する「サイバーセキュリティ確保のための方針」として、本組合のサイバーセキュリティ対策の基本的な考え方を示すものである。

### 4 情報セキュリティポリシーの構成

情報セキュリティポリシーの構成は、一定の普遍性を備えた「情報セキュリティ基本方針」と情報資産を取り巻く状況の変化に適切に対応する「情報セキュリティ対策基準」の 2 階層に分けて策定することとする。



## 5 対象とする脅威

情報資産に対する脅威として、次の脅威を想定し、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、消去等
- (2) 情報資産の無断持出し、無許可ソフトウェアの使用等の規定違反、プログラム上の欠陥、操作、設定、送付ミス、故障等の非意図的な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

## 6 適用範囲

### (1) 組織の範囲

本基本方針が適用される組織は、大垣消防組合消防本部、各署所(3署、3分署、1分駐所)、大垣消防組合議会及び監査委員とする。

### (2) 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

## 7 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、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を遵守しなければならない。

## 8 情報セキュリティ対策

5の脅威から情報資産を保護するために、次の情報セキュリティ対策を講じる。

### (1) 組織運営対策

情報セキュリティ対策を推進するための全庁的な組織体制を確立する。

### (2) 情報資産の分類と管理

本組合の保有する情報資産をその重要度に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

(3) 物理的セキュリティ

サーバ、通信回線、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。

(4) 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など、人的な対策を講じる。

(5) 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) 運用

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。

(7) 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。

約款による外部サービス（クラウドサービス、以下「外部サービス」という。）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) 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。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な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の見直しを行う。

## 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。

## 11 法令遵守

情報セキュリティに関する法令・ガイドライン等を遵守する。