

佐倉市八街市酒々井町消防組合
情報セキュリティ基本方針

令和8年4月 初版

目次

1	目的	1
2	定義	1
(1)	職員等	1
(2)	ネットワーク	1
(3)	情報システム	1
(4)	情報セキュリティ	1
(5)	情報セキュリティポリシー	1
(6)	機密性	1
(7)	完全性	1
(8)	可用性	1
3	対象とする脅威	1
4	適用範囲	2
(1)	行政機関の範囲	2
(2)	情報資産の範囲	2
5	職員等の遵守義務	2
6	情報セキュリティ対策	2
(1)	組織体制	2
(2)	情報資産の分類と管理	2
(3)	情報システム全体の強靱性の向上	2
(4)	物理的セキュリティ	3
(5)	人的セキュリティ	3
(6)	技術的セキュリティ	3
(7)	運用	3
(8)	業務委託と外部サービスの利用	3
7	情報セキュリティ監査及び自己点検の実施	3
8	情報セキュリティポリシーの見直し	3
9	情報セキュリティ対策基準の策定	3
10	情報セキュリティ実施手順の策定	4

1 目的

この基本方針は、佐倉市八街市酒々井町消防組合(以下「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、組合が実施する情報セキュリティ対策についての基本的な事項を定めることにより、情報資産の適切な管理及び運用を図り、もって財産、個人情報等の保護に万全を期するとともに、事業の安定的な運営を確保することを目的とする。

2 定義

(1) 職員等

職員及び外部要員（組合との業務委託等の契約に基づき作業する者）をいう。

(2) 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。

(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

この基本方針及び組合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。

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。

- (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、重要情報の詐取、内部不正等

- (2) 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
- (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

4 適用範囲

(1) 行政機関の範囲

この基本方針が適用される行政機関は、管理者、監査委員及びその補助機関、議会及びその補助機関とする。

(2) 情報資産の範囲

この基本方針が対象とする情報資産は、次のとおりとする。

ア ネットワーク及び情報システム並びに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

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。

(1) 組織体制

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組織体制を確立する。

(2) 情報資産の分類と管理

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実施する。

(3) 情報システム全体の強靱性の向上

情報資産の分類に応じ、多層的なセキュリティ対策を講じる。

(4) 物理的セキュリティ

サーバ、サーバールーム、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。

(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) 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。

(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正に対応するため、緊急時対応計画を策定する。

(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、必要に応じてセキュリティ要件を明記した契約に基づく措置を講じる。

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セキュリティ対策を講じる。

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な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。

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。

なお、情報セキュリティ対策基準は、公にすることにより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、情報セキュリティ実施手順は、公にすることにより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。