川越地区消防組合情報セキュリティ基本方針

平成２８年９月１日　　策定
令和　５年８月１日一部改正
令和　８年４月１日一部改正

１　目的

この基本方針は、本組合が保有する情報資産を様々な脅威から防御し、その機密性、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の基本的な事項を定めることを目的とする。

２　定義

（１）行政情報

職員が職務上作成し、又は取得した電磁的記録（※１）及びこれらを印刷した文書であって、本組合が保有しているものをいう。

（※１）電磁的記録とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録であって、コンピュータによる情報処理の用に供されるものをいう。以下同じ。

（２）ネットワーク

コンピュータを相互に接続するための通信網、その他構成機器（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等により構成され、データを電子的に処理するための仕組みをいう。

（４）情報資産

行政情報及びそれを扱う情報システムをいう。

（５）情報セキュリティ

情報資産の機密性（※２）、完全性（※３）及び可用性（※４）を維持することをいう。

（※２）機密性とは、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）完全性とは、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）可用性とは、情報にアクセスすることを認められた者が、必要なときに情報にアクセスできる状態を確保することをいう。

（６）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扱うデータをいう。

（７）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扱うデータをいう。

（８）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。

３　対象とする脅威

情報資産に対する脅威として、主に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）部外者による脅威

不正アクセス、ウィルス攻撃等のサイバー攻撃や部外者の侵入による盗難・盗聴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、重要情報の詐取等

（2）職員、外部委託業者等による脅威

・情報資産の無断持出、無許可ソフトウェア使用等の規定違反、操作・設定ミス、メンテナンス不備、機器故障等による情報資産の漏えい・破壊・改ざん・消去
・認証情報の不適切管理による認証情報の漏えい等
・情報資産の搬送中における事故、盗難等による情報資産の漏えい等
・規定外の端末接続による情報資産の漏えい等

（3）災害等による脅威

・地震、落雷、火災等の災害による情報資産の消失及び機能停止
・電力供給の途絶、通信の途絶等のインフラ障害による情報資産の消失及び機能停止

4　適用範囲

（1）適用範囲

この基本方針は、本組合職員、組合議会書記、監査委員書記、公平委員会書記及び外部委託業者（以下、「職員等」という。）に適用する。

（2）情報資産の範囲

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　職員等の義務

（1）職員等は、情報資産を取扱う際、情報セキュリティ関係法令等を遵守しなければならない。

（2）職員等は、情報資産を適正に管理及び利用し、情報資産を取り巻く様々な脅威から保護しなければならない。

（3）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つとともに、業務の遂行に当たって、この基本方針、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（以下、「情報セキュリティポリシー」という。）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、以下の情報セキュリティ対策を実施するものとする。

（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。

（3）情報システム全体の強靭性向上

①ＬＧＷＡＮ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回路を分割する。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。
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。高度な情報セキュリティ対策として、埼玉県及び県下自治体のインターネットとの通信を集約した上で、埼玉県自治体情報セキュリティクラウド

の導入等を実施する。

（4）物理的セキュリティ

侵入、盗難、災害、事故、故障等から情報資産を保護するため、情報システムに係る施設・設備の整備等の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する権限や責任にもとづき、職員等に情報セキュリティを周知徹底するための教育・啓発を講じるとともに、認証情報の管理、事故・欠陥の報告等に関するルールを定める。

（6）技術的セキュリティ

情報資産に対する脅威全般から情報資産を保護するため、ネットワーク等の管理、システム等の使用、アクセス制御、システム導入・保守等に関する技術的基準を定めるとともに、ウィルス対策、不正アクセス対策等を講じる。

（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、外部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、緊急時対応計画を策定する。

（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に責任者を定める。

7　情報セキュリティ対策基準の策定

情報セキュリティ対策を実施するに当たっての具体的な遵守事項及び判断基準等を明記した情報セキュリティ対策基準を策定するものとする。

なお、情報セキュリティ対策基準は、公開することにより本組合の行政運営に支障を及ぼす可能性がある情報であることから非公開とする。

8　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、情報システムに関する情報セキュリティ対策を実施するための具体的な手順等を明記し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、公開することにより本組合の行政運営に支障を及ぼす可能性がある情報であることから非公開とする。

9　情報セキュリティ点検

情報セキュリティポリシーが遵守されていることを検証するため、定期的又は必要に応じて情報セキュリティ点検を実施する。

１０　評価及び見直し

　情報セキュリティ点検の結果等により、情報セキュリティポリシーの評価を実施し、必要に応じて見直しを行うものとする。

１１　事件・事故への対応

　情報セキュリティを侵害する事件及び事故が発生した場合は、被害の拡大防止に努めるとともに、早期解決に向けて、迅速かつ適切に対応しなければならない。

附　則

（施行期日）

１　この基本方針は、平成２８年９月１日から施行する。

（川越地区消防組合情報安全対策指針の廃止）

２　川越地区消防組合情報安全対策指針（平成１７年２月１日決裁）は、廃止する。

附　則

（施行期日）

この基本方針は、令和５年８月１日から施行する。

附　則

（施行期日）

この基本方針は、令和８年４月１日から施行する。