津山圏域消防組合情報セキュリティ基本方針

津山圏域消防組合情報マネジメント委員会

令和８年４月１日

改定履歴

版	適用開始日	変更理由	変更内容	変更箇所	変更区分	備考
1.0	令和８年 ４月１日	初版			新規	令和８年 ４月１日 情報マネジメント委員会 策定

（目次）

１　目的

この基本方針は、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し、適正な管理及び円滑かつ安全な運用を図るため、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と共に、住民から信頼される情報マネジメントの実現に寄与することを目的とする。

２　定義

本組合の情報セキュリティポリシーにおける用語の定義は、津山圏域消防組合情報マネジメント要綱（令和８年津山圏域消防組合訓令第３号。以下「マネジメント要綱」という。）に定めるもののほか、それぞれ次の各号に定めるところによる。

（１）情報セキュリティ対策基準

情報セキュリティ対策を実行に移すための、全ての情報資産に共通の情報セキュリティ対策の基準、もしくは情報資産グループごとの情報セキュリティ対策の基準をいう。

（２）情報資産管理運用実施手順

情報資産グループごとに定める、情報セキュリティ対策基準に基づいた具体的な対策の手順をいう。

（３）脅威

情報資産に影響を与え、損失又は損害を発生させる潜在的かつ直接の要因をいう。

（４）脆弱性

脅威の発生を誘引し、脅威を受けた場合に情報資産の損失又は損害を発生しやすくさせ、かつ、拡大させる要因をいう。

（５）リスク

ある脅威が、情報資産の脆弱性を利用して、情報資産への損失又は損害を与える可能性をいう。

（６）職員等

特別職、一般職、会計年度任用職員をいう。

（７）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。

（８）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。

（９）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。

（１０）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。

（１１）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。

（１２）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。

（１３）マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税もしくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

（１４）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（マイナンバー利用事務系を除く。）。

（１５）インターネット接続系

インターネットメール、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。

（１６）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。

（１７）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ない等、安全が確保された通信をいう。

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、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

（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）組織等の適用範囲

情報セキュリティポリシーが適用される対象範囲は、津山圏域消防組合情報公開条例（平成１９年津山圏域消防組合条例第４号）第２条の規定により読み替えて準用する津山市情報公開条例（平成１１年津山市条例第２号）第２条第１号に規定する本組合の機関（以下「実施機関」という。）及び本組合が委託する業務の受託者（以下「受託者」という。）とする。

（２）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実施機関が保有する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実施機関が保有する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実施機関が保有する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

職員等及び受託者は、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は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

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

マネジメント要綱に基づき、最高情報統括責任者及び最高情報セキュリティ責任者を長とする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。

（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実施する。

（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、次の各号の対策を講じる。ただし、次の１号及び２号に関しては、例外として、ISMAP（政府情報システムのためのセキュリティ評価制度）に登録

されているクラウドサービス又は同等程度安全と評価できるサービスに関してのみ、適切なセキュリティ対策を施した上で接続して利用することができる。

①マイナンバー利用事務系においては、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。

②LGWAN 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、無害化通信を実施する。

③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、都道府県及び市区町村のインターネットとの通信を集約した上で、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

サーバ、重要機能室、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て、職員等が遵守すべき事項を定めると共に、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（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する。また、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の責任者を定める。

（9）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。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

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、リスクを検討した上で、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　情報資産管理運用実施手順の策定

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資産管理運用実施手順を策定するものとする。

なお、情報資産管理運用実施手順は、公にすることにより本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。

１１　違反への対応

情報セキュリティポリシーに違反した職員等は、地方公務員法等により懲戒処分等の対象となる場合がある。また、その違反により生じた損害等について責任を負わなければならない場合がある。