鳥栖・三養基地区消防事務組合
情報セキュリティ基本方針

令和８年３月３０日　策定

目次

１．目的

この方針は、鳥栖・三養基地区消防事務組合（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基本的な事項を定めることを目的とする。

２．定義

⑴　この方針において「ネットワーク」とは、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。）をいう。

⑵　この方針において「情報システム」とは、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　この方針において「情報セキュリティ」とは、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　この方針において「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。

⑸　この方針において「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。

⑹　この方針において「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　この方針において「マイナンバー利用事務系（個人番号利用事務系をいう。）」とは、個人番号利用事務（社会保障、地方税若しくは防災に関する事務をいう。）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。

⑻　この方針において「LGWAN 接続系」とは、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。）。

⑼　この方針において「インターネット接続系」とは、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り扱うデータをいう。

⑽　この方針において「通信経路の分割」とは、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。

⑾　この方針において「無害化通信」とは、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。

３．対象とする脅威

情報資産に対する脅威として、次に掲げる脅威を想定し、情報セキュリティ対策を実施するものとする。

⑴　不正アクセス、ウイルス攻撃及び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、重要情報の詐取及び内部不正等

⑵　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、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及び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、落雷及び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、通信の途絶及び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　この方針が適用される行政機関は、組合、監査委員及び議会とする。

⑵　この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及び電磁的記録媒体

イ　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。）

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（臨時的に任用される職員その他の法律により任期を定めて任用される職員及び非常勤職員を含む。以下「職員等」という。）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、業務の遂行に関して、この方針その他の法令等の規定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、次に掲げる情報セキュリティ対策を講ずるものとする。

⑴　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こと。

⑵　組合が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講ずること。

⑶　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、次に掲げる対策を講ずるものとする。

ア　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こと。

イ　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、無害化通信を実施すること。

ウ　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こと。この場合において、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こと。

⑷　サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講ずること。

⑸　情報セキュリティに関し、職員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ずること。
⑹　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及び不正アクセス対策等の技術的対策を講ずること。
⑺　情報システムの監視、この方針その他の法令等の遵守状況の確認、業務委託を行う際のセキュリティ確保等及び情報セキュリティに関する運用面の対策を講ずること。
⑻　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、必要に応じて緊急時対応計画を策定すること。
⑼　業務委託を行う場合には、委託事業者を選定し、必要に応じ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ずること。
⑽　外部サービス（クラウドサービスをいう。）を利用する場合には、必要に応じ利用に係る規定を整備し対策を講ずること。
⑾　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に関し必要な事項を定め、適正な措置を講ずること。

７．情報セキュリティ監査及び自己点検の実施

この方針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こと。

８．　基本方針の見直し

情報セキュリティ監査及び自己点検の結果、この方針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見直すこと。