紀南地方老人福祉施設組合情報セキュリティ基本方針

制定日：令和８年２月９日

改定日：　　年　月　日

施行日：令和８年２月９日

紀南地方老人福祉施設組合

１．目的

当施設組合の情報システムが扱う情報には、利用者の個人情報や施設運営上重要な情報が多数含まれており、情報資産を人的脅威や災害、事故等様々な脅威から防御することは、利用者の財産、プライバシー等を守るためにも、また、継続的かつ安全・安定的な施設サービスの実施を確保するためにも必要不可欠である。

紀南地方老人福祉施設組合情報セキュリティ基本方針（以下「基本方針」という）は、本施設組合が保有する情報資産の機密性、完全性及び可能性を維持するため、本施設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

この基本方針において、次の各号に掲げる用語の意義は、それぞれ当該各号の定めるところによる。

⑴　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。

⑵　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。

⑶　データ

電子計算機処理に係る入出力帳票、磁気テープ、磁気ディスクその他の記録媒体に記録されている情報又は通信回線により送信される情報をいう。

⑷　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。

⑸　情報セキュリティポリシー

本基本方針及び別に定める情報セキュリティ対策基準をいう。

⑹　機密性

情報にアクセスすることを認められた者だけが、その許可された範囲内でのみ情報にアクセスできる状態をいう。

⑺　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。

⑻　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。

⑼　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り扱うデータをいう。

⑽　通信経路

インターネットを接続する際は、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　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．情報セキュリティポリシーの位置付け及び構成

情報セキュリティポリシーは、施設組合が保有する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かつ体系的に取りまとめた情報セキュリティ対策の基本となるものであり、情報セキュリティ基本方針及び情報セキュリティ対策基準から構成される。

情報セキュリティ対策基準は、情報セキュリティ対策方針に基づき、情報セキュリティ対策等を実施するために最低限必要な水準として、本施設組合の全ての情報資産及び情報資産に接する全ての職員、再任用職員、任期付職員、臨時的任用職員、会計年度任用職員、特別職非常勤職員、労働者派遣契約等により本施設組合業務に従事する者（以下「職員等」）が遵守すべき事

項及び判断基準をまとめたものである。

４．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。

⑴　サイバー攻撃をはじめとする部外者の侵入、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

⑵　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、委託管理の不備、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、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

⑶　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

⑷　大規模・広範囲にわたる疾病による要因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、水道供給の途絶等のインフラの障害からの波及等

５．適用範囲

⑴　組織の範囲

本基本方針が適用される組織の範囲は、紀南地方老人福祉施設組合老人福祉施設設置条例（昭和46年紀南地方老人福祉施設組合条例第２号）第２条及び紀南地方老人福祉施設組合の事務局の設置に関する条例（昭和46年紀南地方老人福祉施設組合条例第２号）第２条に規定するもののほか、出納係、議会とする。

⑵　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。

ア　ネットワーク、情報システム及び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り扱う情報（これらを印刷した文書等を含む。）

ウ　コンピュータ等の情報機器において稼働するプログラム

エ　データ及び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

⑶　情報資産の対象

本施設組合が実施する業務で扱う情報資産を本施設組合の情報資産として本基本方針の対象とする。

６．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らばならない。

７．情報セキュリティ対策

上記４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。

⑴　組織体制

本施設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。

⑵　情報資産の分類と管理

本施設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。

⑶　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、情報資産の分類に応じた情報セキュリティ対策を講じるとともに、次の対策も併せて講じる。

① 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。

⑷　物理的セキュリティ

サーバ等の管理、通信回線及び端末等への物理的な対策を講じる。

⑸　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、必要な教育及び啓発を行う等の人的な対策を講じる。

⑹　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。

⑺　運用

情報システムの監視、情報セキュリティー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ー侵害が発生した場合等に迅速かつ適切に対応するため、情報セキュリティインシデント発生時の対応手順書を策定する。

⑻　業務委託と外部サービスの利用

業務委託する場合には、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する、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等、必要事項を確認し、必要に応じて措置を講じる。

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．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確認するため、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。

９．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は、必要に応じ情報セキュリティポリシーの見直しを行う。

10．情報セキュリティ対策基準の策定

上記７、８及び９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。

11．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当施設組合の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。