

西北五広域福祉事務組合情報セキュリティ基本方針

令和8年3月25日

西北五広域福祉事務組合

1. 目的

本基本方針は、西北五広域福祉事務組合（以下、「本組合」という。）が保有するネットワーク、情報システム及び情報資産を利用、運用、開発及び保守する者が遵守すべき情報セキュリティに関する基本的な事項を定めることを目的とする。

なお、本組合事務局（以下、「事務局」という。）は議会及び監査委員に関する事務を兼務しているため、議会及び監査委員の情報セキュリティ基本方針を兼ねるものとする。

2. 定義

(1) ネットワーク

本組合内に設置する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。

(2) 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。

(3) 情報資産

ネットワーク及び情報システムの開発と運用に係るすべてのデータ並びにネットワーク及び情報システムで取り扱うすべてのデータをいう。

(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) 機密性

情報資産にアクセスすることを認可された者だけが、情報資産にアクセスできる状態を確保することをいう。

(6) 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。

(7) 可用性

情報資産にアクセスすることを認可された者が、必要なときに中断されることなく、情報資産にアクセスできる状態を確保することをいう。

(8) 特定個人情報

行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号。）第2条に規定する個人番号をその内容にサービス個人情報ファイルをいう。

(9) インターネット接続系

インターネットメール、他システム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。

(10) 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無い等、安全が確保された通信をいう。

3. 適用範囲

(1) 機関の範囲

本基本方針の適用範囲は、事務局、森田学園、ステップアップセンターもりた、相談支援事業所もりたとする。

(2) 情報資産の範囲

本基本方針が対象とする情報資産は、次の通りとする。

- 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

4. 職員等の守秘義務

職員、会計年度任用職員等（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。

5. 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、サービス不納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な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) 災害等による電力供給の途絶、通信の途絶、水道供給の途絶等によるインフラの障害及び大規模・広範囲にわたる疾病の蔓延による要因不足

に伴うシステム運用の機能不全等

6 情報セキュリティ対策

上記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ずる。

(1) 組織体制

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

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行う。

(3) 情報システム全体の強靱性の向上

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。

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。

(4) 物理的セキュリティ

情報システムを設置する施設への不正な立入り、情報資産の損傷及び盗難から保護するために、物理的な対策を講ずる。

(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、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。

外部サービス（クラウドサービス）を利用する場合には、利用にかかる

規定を整備し、対策を講ずる。

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。

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監査及び自己点検を実施する。

8. 評価及び見直しの実施

情報セキュリティ監査及び自己点検の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く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、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の見直しを実施する。

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を定めるセキュリティ対策基準を策定し、本基本方針と併せて情報セキュリティポリシーと総称する。

10. 情報セキュリティ実施手順の策定

本基本方針及び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。