公益財団法人岡山市ふれあい公社

情報セキュリティポリシー

基本方針

令和８年２月

公益財団法人岡山市ふれあい公社

（目的）

第１条　公益財団法人岡山市ふれあい公社情報セキュリティポリシー（以下、「ポリシー」という。）は、公益財団法人岡山市ふれあい公社個人情報保護規則及び公益財団法人岡山市ふれあい公社特定個人情報保護規則に基づき、公益財団法人岡山市ふれあい公社（以下、「財団」という。）における情報セキュリティに対する基本方針を明らかにするとともに、情報セキュリティ対策の基準（以下、「対策基準」という。）を定めることにより、財団が保有する情報資産を様々な脅威から守り、円滑に事業を運営することを目的とする。

（定義）

第２条　このポリシーにおいて、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（１）情報セキュリティ

情報の機密性、可用性、完全性を維持することをいう。

（２）情報セキュリティポリシー

基本方針及び対策基準をいう。

（３）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。

（４）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。

（５）可用性

情報にアクセスすることを認められた者が、必要な時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。

（６）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並びにこれを構成するための機器（ハードウェア及びソフトウェア）をいう。

（７）情報システム

コンピュータ（ハードウェア及びソフトウェア）、ネットワーク及び電磁的記録媒体で構成された、情報処理を行う仕組みをいう。

（８）電磁的記録媒体

USB メモリ、CD/DVD、ハードディスク等、情報を保存するための機器等をいう。

（９）情報資産

第４条第２項に該当するものをいう。

（１０）秘密文書

財団文書取扱規程第４３条に規定する文書をいう。

（１１） 情報セキュリティインシデント

情報資産に対する不正アクセス、コンピュータウイルス等不正プログラムの感染、情報の流出や消失といった情報セキュリティ上の脅威となる事象や、その事象により発生した事件又は事故をいう。

(対象とする脅威)

第３条　情報資産に対する脅威として、次の脅威を想定し、情報セキュリティ対策を実施する。

（１） 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

（２） 故意又は過失による情報資産の漏洩・破壊・改ざん・消去又は紛失、重要情報の窃取、サービス停止等

（３） 無許可のハードウェア・ソフトウェアの仕様等の規定違反、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、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、機器故障等の偶発的要因による情報資産の漏洩・破壊・消去等

（４） 地震、水害、落雷、火災等の災害によるサービス及び業務の停止等

（５） 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

（６） 電力供給の途絶、通信の途絶等のインフラの障害からの波及等

(適用範囲)

第４条　この基本方針は、財団の全職員及び財団が事業を実施するために管理する全施設に適用する。

２　対象とする情報資産は、次のとおりとする。

（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） 他機関等から受領したデータ及び関連文書

（４） 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

３　前項第１号における電磁的記録媒体のうち、財団が所有するスマートフォン・タブレット・デジタルカメラ等機器については、別紙「公益財団法人岡山市ふれあい公社社用ポータブルデバイス使用ルール」に定めるところによる。

(職員等の遵守義務)

第５条　職員等（アルバイトを含む。以下同じ。）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ポリシー及び情報保護に関する対応マニュアルを遵守しなければならない。

(情報セキュリティ対策)

第６条　第３条に掲げる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。

（１） 組織体制

財団の情報資産について、情報セキュリティ対策を推進・管理するための組織体制を確立する。

（２） 情報資産の分類と管理

財団の保有する情報を、機密性、完全性及び可用性に応じて４段階の「重要度分類」に分け、当該分類に基づき情報セキュリティ対策を実施する。

（３） 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。

（４） 物理的セキュリティ

サーバ、通信回線及び職員が利用するパソコン等の端末並びに情報を取り扱うその他の設備及び機器の管理について、物理的な対策を講じる。

（５） 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、システムの開発・導入・保守、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。

（６） 運用面

情報やID、パスワードの管理、コンピュータウイルス対策、メールの取扱い等、運用面における対策を講じる。また、情報セキュリティインシデントが発生した場合等に迅速かつ適正に対応するため、緊急時対応手順を策定する。

（７） 外部サービスの利用

外部委託を行う際のセキュリティ確保、データセンター又はクラウドサービス、ソーシャルメディアサービス等の外部サービスを利用する際の対策を講じる。

(情報セキュリティ監査及び自己点検の実施)

第７条　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。

(ポリシーの見直し)

第８条　情報セキュリティ監査及び自己点検の結果、ポリシーの見直しが必要となった場合又は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となった場合には、ポリシーを見直す。

(対策基準の策定)

第９条　第６条から第８条まで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対策基準を策定する。なお、この対策基準は、公にすることにより財団の運営に重大な支障を及ぼす恐れがあることから非公開とする。

（情報保護に関する対応マニュアルの策定）

第１０条　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保護に関する対応マニュアルを策定する。なお、この対応マニュアルは、公にすることにより財団の運営に重大な支障を及ぼす恐れがあることから非公開とする。

附　則

この基本方針及び対策基準は、令和６年７月１日に制定する。

附　則

この基本方針及び対策基準は、令和８年２月１日から施行する。