公益財団法人札幌市生涯学習振興財団

情報セキュリティ基本方針

１　目的

公益財団法人札幌市生涯学習振興財団（以下「財団」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、財団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　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憶媒体で構成され、情報処理を行う仕組みをいう。

⑶　情報資産

財団が作成や収集をした情報をいう。

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、情報セキュリティ対策基準及び情報セキュリティ実施手順をいう（以下「ポリシー」という）。

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、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、必要な時に中断されることなく、情報にアクセスできる状態をいう。

３　本基本方針の位置づけ

本基本方針は、財団の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とりまとめたものであり、情報セキュリティ管理の最上位の位置付けとする。

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　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、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、重要情報の搾取、内部不正等

⑵　情報資産の不正な持ち出し、無許可ソフトウェアの使用等の規程違反、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、通信の途絶等のインフラの障害からの波及等

５　適用範囲

⑴　対象の範囲

本基本方針は、財団の全ての施設及び財団の業務に携わる全ての役職員（以下「職員等」という。）を対象とする。

⑵　情報資産の範囲

本基本方針は、財団が保有する全ての情報資産を対象とする。

６　職員等の遵守義務

財団の情報資産に接する全ての職員等は、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。

また、情報資産を取り扱う委託事業者等に対しても、ポリシーの趣旨に従い必要なセキュリティを確保するための措置を講じなければならない。

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、以下の情報セキュリティ対策を講じる。

⑴　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する組織体制を確立する。

⑵　情報資産の分類と管理

財団の保有する情報資産を機密性、完全性及び可用性に応じた重要性で分類し、当該分類に基づき情報セキュリティ対策を行う。

⑶　物理的セキュリティ

サーバ、情報システム、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。

⑷　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。

⑸　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。

⑹　業務委託と外部サービスの利用

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かを確認し、必要に応じて契約に基

づき措置を講じる。

外部サービスを利用する場合には、サービス提供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かを確認し、適宜必要な措置を講じる。

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できる情報を限定し、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。

⑺　運用

ポリシーの遵守状況の確認及びポリシーの運用面の対策を講じる。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切に対応するため、緊急時対応計画を策定する。

⑻　評価・見直し

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。ポリシーの見直しが必要な場合は、適宜ポリシーの見直し行う。

８　情報セキュリティ監査及び自己点検の実施

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。

９　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、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あった場合には、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。

なお、情報セキュリティ対策基準は、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。

11　情報セキュリティ実施手順の策定

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

この方針は令和６年４月１日から施行する。