公益財団法人東京都福祉保健財団情報セキュリティ基本方針

１　目的

今日、インターネットを始めとする情報通信ネットワークや情報処理システムは、都民生活及び社会経済のあらゆる面で利用が拡大し、ＩＴ社会はますます発展している。

しかし一方で、個人情報の漏えい等、人為的な原因による情報セキュリティ事故が後を絶たない。また自然災害等によるシステム障害などにも備える必要があり、更に不正アクセス、新たな攻撃手法による重要な情報の破壊・改ざんといった、情報に対する新たな脅威も増大している。

公益財団法人東京都福祉保健財団（以下「財団」という。）では、事業運営上、都民の個人情報など重要な情報を多数取り扱っており、それらの情報を扱う多くの業務で情報処理システムや情報通信ネットワークの活用は必要不可欠となっている。

したがって、都民の権利利益を守るため、また、公正な事業の安定的、継続的な運営のため、これらの情報資産を様々な脅威から守ることは、財団に課せられた責務である。

このような状況の中で、すべての職員等は、情報セキュリティ対策が今日における重大かつ喫緊の課題であることをあらためて認識し、全組織を挙げて、様々な脅威に対応する必要がある。このため、財団情報セキュリティ基本方針を定め、各組織間において緊密な連携と情報共有を行いながら、財団として総合的、体系的、積極的に情報セキュリティ対策を実施する。

２　情報セキュリティ対策の体系

財団は、当情報セキュリティ基本方針に基づき、財団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定める。

（１）財団情報セキュリティ対策基準

財団情報セキュリティ基本方針に基づき、情報セキュリティ対策等を実施するために、各情報システム等共通の最低限必要な水準として、具体的な遵守事項及び判断基準等を定めたものである。

（２）情報セキュリティ実施手順

情報セキュリティ対策基準に基づき、情報処理システムごとに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ものである。

３　定義

（１）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（ハードウエア及びソフトウエア）をいう。

（２）情報処理システム

コンピュータ、端末装置、通信回線等により、電子情報を処理するシステムをいう。

（３）情報資産

以下のものをいう。

ア　ネットワーク、情報処理システム及びこれらに関する設備、電磁的記録媒体（以下「情報システム等」という。）

イ　情報システム等で取り扱う電磁的な情報
ウ　情報システム等の仕様書及びネットワーク図等のシステム関連文書

（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。

ア　機密性とは、情報にアクセスすることを認可された者だけが、情報にアクセスできる状態を確保することをいう。

イ　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。

ウ　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。

（5）情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

4　対象とする脅威

情報資産に対する脅威として、以下のものを想定し、情報セキュリティ対策を実施する。

（1）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要因による情報資産の漏えい、破壊、改ざん、消去及び不正な操作等

（2）情報資産の盗難、紛失、無断持ち出し、ウイルス感染、無許可ソフトウエアの使用等の規定違反、プログラム上の欠陥、人為的なミス、故障等の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、風水害等の災害や突発的な停電によるサービス及び業務の停止、情報資産のき損、喪失等

5　職員の遵守義務

職員は、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等を遵守しなければならない。

6　外部委託事業者等への対策

財団の業務を受託する事業者及び人材派遣職員に当該業務等を行わせる場合においては、セキュリティ対策上遵守させるべき事項を契約または協定等において明記するとともに、本基本方針及び対策基準と同様の水準での情報セキュリティを確保できるよう、財団が必要な措置をとるものとする。

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実施する。

（1）組織体制

財団の情報資産について、総合的な情報セキュリティ対策を推進するため、全体的な組織体制を確立する。また、情報セキュリティ対策に関し、各職層における管理者等の役割、権限及び責任を明確にする。

（２）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て分類し、当該分類に基づき情報資産の管理及び取り扱い方法等について具体的に定め、実効的な情報セキュリティ対策を行う。

（３）物理的セキュリティ

サーバ、情報システム室、通信回線等及びパソコン等の情報処理機器類の管理について、物理的な対策を講じる。

（４）人的セキュリティ

情報セキュリティに関し、情報セキュリティ対策基準等に職員等が遵守すべき事項を明確かつ具体的に定めるとともに、十分な教育及び啓発を行うなどの人的な対策を講じる。

（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、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）情報セキュリティポリシーの運用

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、外部委託等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運用上の対策を講じる。

また、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応体制を整備する。

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検証するため、定期的及び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への対応が必要となった場合には、情報セキュリティポリシーを見直す。

附　則

この方針は、平成２０年４月１日から施行する。

附　則

この方針は、平成２１年４月１日から施行する。

附　則

この方針は、平成２４年４月１日から施行する。

附　則

この方針は、平成３０年４月１日から施行する。

（　参　考　）

財団における情報セキュリティ規程体系図