社会福祉法人北区社会福祉協議会　情報セキュリティ基本方針

１．目的

本基本方針は、本会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、本会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

（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（ハードウェア及びソフトウェア）をいう。

（２）情報資産

データ、ハードウェア、ソフトウェア、設備、文書等をいう。

（３）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。

（４）電磁的記録媒体

コンピュータによる情報処理に用いられる記憶媒体（フロッピーディスク、ハードディスク、ＵＳＢメモリ、ＤＶＤ－ＲＯＭ、ＣＤ－ＲＯＭ等のコンピュータ用メディア）をいう。

（５）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。

（６）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。

（７）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。

（８）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。

（９）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。

３．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

（２）情報資産の無断持ち出し、無承認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、水害等の災害によるサービス及び業務の停止等

（４）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

（５）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

４．適用範囲

（１）対象者の範囲

本基本方針が適用される対象者の範囲は、次のとおりとする。

①職員就業規則第３条に定める全ての職員（以下、「職員」という。）

②本会の理事、監事、評議員、顧問、各種部会・委員会委員等

③本会の事業にかかわる区民、関係機関・団体等のうち、個人情報保護規程に規定される個人情報を取り扱う者

④この基本方針の対象となる業務を担う外部委託業者

（２）情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①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

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

５．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本基本方針を遵守しなければならない。

６．情報セキュリティ対策

上記３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。

（１）物理的セキュリティ

サーバ等、通信回線等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。

（２）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。

（３）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。

（４）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、定期的又は必要に応じて情報セキュリティの自己点検を実施し、運用改善を行い情報セキュリティの向上を図る。

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の遵守状況を検証するため、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．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には、情報セキュリティポリシーを見直す。

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等を定める情報セキュリティ対策基準を策定する。

１０．情報セキュリティ実施手順について

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定めるものとする。

なお、情報セキュリティ実施手順は各業務の手順書等に代えて構わない。