

社会福祉法人 西東京市社会福祉協議会 情報セキュリティ基本方針

1 目的

この基本方針は、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、社会福祉法人西東京市社会福祉協議会（以下「本会」という。）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 用語の定義

(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、電磁的記録媒体及び紙媒体で構成され、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規則(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、詐取、内部不正等
- (2)無許可ソフトウェアの使用、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的要因による情報資産の漏えい・破壊・消去等
- (3)情報資産の無断持ち出し、紛失・盗難・転売等による他者への流出等
- (4)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
- (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

4 適用範囲

(1)対象者の範囲

この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本会に勤務する正規職員、再任用職員、再雇用職員、嘱託職員、再雇用嘱託職員、臨時職員（以下「職員」という。）
- ②本会の理事、監事、評議員、各種部会・委員会委員等
- ③本会の事業にかかわる市民、関係機関・団体等のうち、個人情報保護規則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

この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資産
- 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。

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) 組織体制

本会の情報資産について、情報セキュリティ対策を推進する全組織的な体制を確立する。

(2) 情報資産の分類と管理

本会の保有する情報資産を機密性、完全性及び可用性（あるいは、機密性の段階に応じて）に応じて分類し、当該分類に基づき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、通信回線、パソコン及び紙媒体等の管理について、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、本方針の対象者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。

(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) 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切に対応するため、緊急時対応計画を策定する。

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、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 情報セキュリティポリシーの見直し

情報セキュリティポリシーは、以下の事象が発生した場合に見直す。

- ①情報セキュリティ監査及び自己点検の結果、見直しが必要となった場合
- ②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
- ③情報資産に対する脅威が生じたとき

9 情報セキュリティ対策規則(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規則(基準)を策定する。

10 情報セキュリティ実施手順の策定

情報セキュリティ対策規則(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本会の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。

平成29年2月22日制定

社会福祉法人 西東京市社会福祉協議会

会長 村田利夫