社会福祉法人柏市社会福祉協議会 情報セキュリティポリシー

令和６年４月

目次

情報セキュリティ宣言書

社会福祉法人柏市社会福祉協議会（以下「本会」という。）では、充実した福祉サービスを安定的に提供するため、情報システムを活用し、住民情報等の重要な情報を取り扱っている。一方で、個人情報の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、自然災害や操作ミス等によるシステム障害、様々な脅威が存在する。

情報資産を様々な脅威から防御することは、市民の権利、利益を守るためにも、また、法人の安定的、継続的な運営のためにも必要不可欠である。

これらの状況を鑑み、本会における情報資産に対する安全対策を推進し、市民からの信頼を確保するため、以下のことに積極的に取り組むことを宣言する。

（１）情報セキュリティ対策を推進するための組織的な体制を構築

（２）情報セキュリティ基本方針を実行するための判断基準として、情報セキュリティ対策基準を策定し、その実行のための手順等を盛り込んだ実施手順の策定

（３）本会の保有する情報資産の適切な管理

（４）全ての職員等が、情報セキュリティ対策の重要性を認識し、当該対策を適切に実施するために、職員等に対して必要な教育の実施

（５）情報セキュリティインシデントが発生した場合又はその予兆があった場合に速やかに対応するため、緊急時対応計画の策定

（６）情報セキュリティ対策の実施状況の監査及び自己点検等を通して、定期的な対策の見直し

（７）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情報セキュリティ基本方針、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の遵守

ＣＩＳＯ（最高情報セキュリティ責任者）　秋　谷　　正

情報セキュリティ基本方針

2　情報セキュリティ基本方針

2.1. 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。

2.2. 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。

（３）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。

（４）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。

（５）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。

（６）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。

（７）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。

2.3. 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、無許可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、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

2.4. 適用範囲

（１）組織の範囲

本基本方針が適用される範囲は、次項で定義する本会の情報資産を有する、全ての拠点とする。

（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 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

2.5. 職員等の遵守義務

役員、職員、再雇用職員、契約職員及び派遣職員等（以下「職員等」という。）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。

2.6. 情報セキュリティ対策

上記 2.3 の脅威から情報資産を保護するため、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組織体制を確立する。

（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実施する。

（３）情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。

（４）物理的セキュリティ

サーバ、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。

（５）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。

（６）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。

（７）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、業務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正に対応するため、緊急時対応計画を策定する。

（８）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ことを確認し、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、利用にかかる規定を整備し対策を講じる。

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規定し、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。

（９）評価・見直し

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し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

2.7. 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。

2.8. 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。

2.9. 情報セキュリティ対策基準の策定

上記 2.6、2.7 及び 2.8 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。

2.10.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基準に基づき、情報システムを保有する課室等は、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。