情報セキュリティ基本方針

社会福祉法人 光優会

1　目的

本方針は、社会福祉法人 光優会（以下「法人」という。）が運営する各事業所において実施するセキュリティ対策に関する基本的な事項を定め、様々な脅威から、法人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ことを本基本方針の目的とする。また、すべての職員等は、法人が保有する情報資産に対する脅威への対応が重大かつ喫緊の課題であることを改めて認識し、法人におけるセキュリティ対策の推進に積極的に取り組むこととする。

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及びその構成機器（ハードウェア及びソフトウェア）をいう。

（2）情報システム　法人の運営に必要な情報の収集・蓄積・処理・伝達・利用に関わるコンピュータのハードウェア、ソフトウェア、データベース、ネットワーク、保管・蓄積装置、記録媒体等の仕組みをいう。

（3）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。

※セキュリティには、サイバーセキュリティを含む。

（4）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規程をいう。

（5）職員等　役員、正職員、準職員、パート職員、アルバイト職員、嘱託職員その他法人の指揮命令を受けて業務に従事するすべての者をいう。

（6）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。

（7）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。

（8）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。

（9）業務用端末　職員等に対し、業務上利用することが許可されたパソコン及びスマートフォン、タブレット等のモバイル端末等をいう。

（10）業務用外部記録媒体　職員等に対し、業務上利用することが許可されたUSBメモリや光ディスク等の外部記録媒体をいう。

（11）管理区域　各事業所内に設定され、情報システムの機器類の設置、管理運用、保管等を行う専用の区域をいう。

（12）ソーシャルメディアサービス　インターネット上で展開される情報メディアであって、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった社会的な要素を含んだメディアである、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等のサービスをいう。

（13）外部サービス　法人以外の者が一般向けに情報システムの一部又は全部の機能を提供するクラウドサービス、Web会議サービス、ソーシャルネットワーキングサービス、検索サービス、翻訳サービス、地図サービス、ホスティングサービス等をいう。

（14）クラウドサービス　従来は手元のコンピュータに導入して利用していたソフトウェアやデータ、それらを提供するための技術基盤等を、インターネットなどのネットワークを通じて、利用できるサービスをいう。

（15）セキュリティ事象　3に定める脅威により業務の遂行及びセキュリティに影響を与えうる事象の全てをいう。

(16) セキュリティインシデント　セキュリティ事象のうち、業務の遂行を危うくする確率及びセキュリティを脅かす確率が高い事象をいう。

3　対象とする脅威

情報資産に対する脅威として、以下のものを想定し、セキュリティ対策を実施するほか、新たな脅威の発生に備え、最新の脅威動向を確認するなど、適切に対応する。

(1) 不正アクセス、ウイルス攻撃、ランサムウェア攻撃、サービス不能攻撃等のサイバー攻撃及び侵入等の意図的な要因による法人が保有する情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、サービス及び業務の停止のほか、内部管理の欠陥など職員等による不正行為等

(2) 法人が保有する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、外部サービス設定等の不備、メンテナンスの不備、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、メールの誤送信等の非意図的要因による情報資産の漏えい・破壊・消去、重要情報の詐取、サービス及び業務の停止、不正行為等

(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

4　適用範囲

(1) 法人組織の適用範囲

本基本方針が適用される範囲は、法人が運営するすべての事業所とする。

(2) 情報資産の適用範囲

本基本方針が対象とする情報資産は、次のとおりとする。

ア　情報システム等

イ　個人情報のほか、情報システム等で取り扱うデータ

ウ　情報システム等に関するシステム設計書、ネットワーク図等のシステム関連文書

エ　紙文書

5　職員等の遵守義務

職員等は、法人が保有する情報資産に対する脅威への対応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、セキュリティポリシー及び関連する規程等を遵守しなければならない。

6　セキュリティ対策

3 の脅威から情報資産を保護するために、以下のセキュリティ対策を講じる。

(1) 組織体制の確立

法人の情報資産についてセキュリティ対策を推進する法人全体の組織体制を確立する。

(2) 情報資産の分類と管理

法人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、セキュリティ対策を講じる。

(3) 物理的セキュリティ対策

サーバ、管理区域、通信回線、業務用端末等の管理について、物理的な対策を講じ

る。

(4) 人的セキュリティ対策

サイバー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。

(5) 技術的セキュリティ対策

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) 運用面での対策

情報システムの監視及びセキュリティポリシー等の遵守状況の確認のほか、(7)の業務委託及び外部サービスを利用する際のセキュリティ確保等、セキュリティポリシーの運用面で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、緊急時対応体制を整備する。緊急時対応体制については、危機管理規程の定めるところによる。

(7) 業務委託及び外部サービスの利用に係る対策

法人の業務を受託する事業者（当該事業者から派遣されている者を含む。）（以下「委託事業者等」という。）に当該業務を行わせる場合には、法人が定めるセキュリティ要件等、セキュリティ対策上、遵守させるべき事項を、委託事業者等の選定要件として提示する。

さらに、契約や協定等（以下「契約等」という。）の締結時等に、法人が定めるセキュリティ要件を契約等事項に明記し、委託事業者等において要件を満たすセキュリティ対策が確保されていることを確認し、又は、別途、書面による提出を求める等の措置を講じる。

なお、外部サービスの利用に当たっては、利用に関する手順等を定めるとともに、必要に応じて、当該利用の対象とする情報について定める等、規定を整備し、対策を講じる。

7　リスク評価の実施及び年度計画の策定

セキュリティに係る内部環境及び外部環境の変化を踏まえ、法人が保有する情報資産のセキュリティ上のリスクを評価し、リスク対応方針を策定する。

また、策定したリスク対応方針に基づき、リスク対応計画を毎年度策定する。

8　自己点検及びセキュリティに関する監査の実施

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、自己点検及びセキュリティに関する監査を実施する。

9　セキュリティポリシーの見直し

自己点検及びセキュリティに関する監査の結果、セキュリティポリシーの見直しが必要となった場合、又は、セキュリティに関する状況の変化に対応するため、新たな対策が必要となった場合には、セキュリティポリシーを見直す。

10　情報セキュリティ規程の策定

6 から 9 までに示す対策等を実施するため、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規程を策定する。

11　セキュリティ実施手順の策定

情報セキュリティ規程を踏まえ、セキュリティ対策を実施するための具体的な手順につい

て、情報セキュリティ管理者が必要に応じてセキュリティ実施手順を別に定めるものとする。

なお、当該実施手順は、関連する情報システム等のセキュリティ対策を具体的かつ詳細に定めるものであり、公にすることにより、関連する業務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。

12　附則

本方針は 2026 年 4 月 1 日より施行する。