情報セキュリティポリシー

有限会社ノリテック

情報セキュリティ基本方針

有限会社ノリテックは、社会保険・社会福祉・介護事業として、高齢者向けのグループホーム、デイサービス、介護支援サービスなどを提供しています。特に、個人の健康情報や介護記録を扱うため、情報セキュリティの確保は極めて重要です。私たちは、顧客や職員の個人情報を含む全ての情報資産を保護し、情報漏洩や不正アクセスのリスクを最小限に抑えることを最優先事項として位置づけています。このポリシーは、当社が運営する全ての施設とサービスに適用され、情報資産の適切な管理と利用を職員全員に義務づけます。

組織的対策

有限会社ノリテックは、介護事業としての特性を考慮し、情報セキュリティ組織を設置し、個人情報の取り扱いに関する定期的なリスクアセスメント、教育・訓練を実施します。

介護施設と居宅介護支援事業所を含む全拠点で、情報共有の迅速化と、現場の実情に即したセキュリティ対策の実施を目指します。

１　組織的対策

（１）情報セキュリティ組織の設置

情報セキュリティの責任者を明確に指名し、組織全体の情報セキュリティ対策の推進と統括を行う。情報セキュリティ関連の業務を担当する部署やチームを設置し、専門的な知識とスキルを持つメンバーを配置する。

（２）情報セキュリティ方針の策定

組織の情報セキュリティに関する基本的な方針や目的を明文化し、全職員に周知徹底する。方針は定期的に見直しを行い、最新の脅威やリスクに対応する内容を維持する。

（３）リスクアセスメントの実施

情報資産のリスクアセスメントを定期的に実施し、リスクの大きさや脅威の変動に応じて対策を見直す。アセスメント結果は文書化し、管理者や関連部署と共有する。

（４）教育・研修

全職員を対象とした情報セキュリティ教育や研修を定期的に実施する。最新の脅威や対策方法についての知識を更新し、意識の向上を図る。

（５）定期的な監査・検証

情報セキュリティの状況や対策の効果を確認するための監査や検証を定期的に行う。問題点や改善点を明確にし、必要に応じて対策を強化する。

２　人的対策

（1）雇用条件

職員を雇用する際には、秘密保持契約を締結することで、情報の漏洩や不正利用を予防する。

（2）新入社員の情報セキュリティ教育

全ての新入社員に対して、入社時に情報セキュリティに関する基本的な教育を実施する。 社内の情報資産の取り扱い方や、セキュリティポリシー、行動指針についての説明を行う。

（3）定期的な研修・再教育

職員全員を対象に、定期的な情報セキュリティ研修や再教育を行う。 最新のセキュリティリスクや脅威についての情報を共有し、職員の意識を高める。

（4）情報セキュリティ意識の啓発活動

ポスターや社内ニュースレター、メール等を用いて、情報セキュリティに関する啓発活動を継続的に行う。セキュリティ事故の事例紹介や、具体的な対策方法の共有を行う。

（5）退職時の情報セキュリティ対策

退職者が保有する情報資産やアクセス権限を迅速に回収・削除する。 退職者に対して、社外への情報の持ち出しや漏洩に関する義務や禁止事項を再確認する。

（6）適切なアクセス制御の実施

職員の役職や業務内容に応じて、情報へのアクセス権限を適切に設定する。不要なアクセス権限は速やかに削除し、アクセス権限の最小化を図る。

3　情報資産管理

（1）情報資産の識別

すべての情報資産を一覧化し、それぞれの重要度や機密性を識別する。資産ごとに管理者や責任者を設定し、定期的に資産リストの更新を行う。

（2）アクセス権限の管理

情報資産へのアクセス権限を役職や業務内容に応じて設定し、最小権限の原則に基づき適切なアクセス制御を行う。アクセス権限の変更や削除は迅速に対応し、不要な権限の付与を避ける。

（3）情報資産の保管・廃棄

情報資産の保存場所や保管方法を明確にし、適切なセキュリティ対策を講じる。 廃棄が必要な情報資産は、情報が復元できないように適切に破棄する。

（4）定期的なリスクアセスメント

情報資産に関連するリスクを定期的に評価し、新たな脅威やリスクに対応するための対策を検討する。アセスメント結果は文書化し、関連部署や管理者と共有する。

（5）情報漏洩の予防

職員への教育や研修を通じて、情報の不正な持ち出しや共有を防ぐ。情報資産の取り扱いに関するガイドラインやポリシーを策定し、職員に周知徹底する。

4　アクセス制御及び認証

（1）アクセス権限の設定

すべての情報システムや資産に対して、必要最小限のアクセス権限を持つ原則を採用する。 各職員の役職や業務内容に応じて、適切なアクセス権限を設定し、定期的に見直しを行う。

（2）認証手段の強化

パスワードのみの認証から、二要素認証や多要素認証を導入し、セキュリティを強化する。パスワードポリシーを策定し、定期的なパスワード変更や、強度の要件を設定する。

（3）アクセスログの取得・監視

すべての情報システムやサービスにおいて、アクセスログを取得する。不正アクセスや異常な操作を検知するため、ログの定期的な監視や分析を行う。

（4）リモートアクセスの管理

外部からのリモートアクセスを許可する場合、ＶＰＮや専用のゲートウェイを通じて安全な接続を確保する。リモートアクセスの際も、強化された認証手段を適用する。

（5）無効化されたアカウントの管理

一定期間利用されていないアカウントや、退職者のアカウントは速やかに無効化する。アカウントの有効・無効状態を定期的に確認し、管理を行う。

5　物理的対策

（1）セキュリティ対策を施した施設

情報システムやサーバーを設置する場所には、鍵やセキュリティカードによるアクセス制限を行う。セキュリティカメラや警備員を配置し、不正アクセスを防止する。

（2）災害対策

情報システムやデータを保護するため、耐震構造や防火設備を備えた施設を利用する。万が一の災害時にも迅速な復旧を目指し、バックアップや災害復旧手段を確立する。

（3）情報機器の物理的管理

パソコンやモバイル機器などの情報機器は、施錠可能な保管場所に格納する。機器　の持ち出しや移動は厳格に管理し、必要に応じて持ち出し履歴を記録する。

（4）媒体の管理

バックアップデータや機密情報が記録されている媒体（ＵＳＢメモリ、外付けＨＤＤなど）は適切に保管する。不要となった媒体は、情報が復元できないように物理的に破壊して廃棄する。

（5）訪問者の管理

社外からの訪問者は、受付での身分確認や訪問目的の確認を行う。訪問者用の待合室や会議室を設け、不要な場所へのアクセスを制限する。

6　ＩＴ機器利用

（1）利用ガイドラインの策定

ＩＴ機器の適切な利用方法やセキュリティ対策に関するガイドラインを策定し、職員に周知する。

（2）パーソナルデバイスの管理

ビジネス用途での私有機器の利用（ＢＹＯＤ）を許可する場合、セキュリティポリシーを策定し、適切なセキュリティ対策を施す。私有機器からの情報アクセスやデータの保存を制限する。

（3）ソフトウェアの管理

認可されたソフトウェアのみをＩＴ機器にインストールする。不要となったソフトウェアは定期的に削除し、最新のセキュリティパッチを適用する。

（4）インターネット利用の管理

インターネット利用に関するポリシーを策定し、危険なサイトへのアクセスを制限する。ダウンロードやファイルの送受信に関するガイドラインを設ける。

（5）電子メールの利用

電子メールの利用に関するガイドラインを策定し、不審なメールの取り扱いや添付ファイルの開封に関する注意点を共有する。機密情報の送信には、暗号化やパスワード保護を適用する。

7　ＩＴ基盤運用管理

（1）サーバー・ネットワークの管理

すべてのサーバーやネットワーク機器の適切な設定や管理を行い、セキュリティを確保する。不正アクセスやサービス拒否攻撃（ＤｏＳ攻撃）に対する防御策を講じる。

（2）バックアップ・復旧

重要なデータや情報システムの定期的なバックアップを実施し、データロスのリスクを低減する。災害や障害時の迅速な復旧を目指し、復旧手順やプロセスを明確にする。

（3）セキュリティアップデートの適用

ＯＳやアプリケーションのセキュリティアップデートを定期的に確認・適用する。ゼロデイ攻撃や既知の脆弱性を利用した攻撃を防ぐため、最新のセキュリティパッチの適用を怠らない。

（4）監視・モニタリング

ＩＴ基盤の動作状態やセキュリティイベントをリアルタイムで監視する。異常な動作や不正アクセスの兆候を早期に検知し、迅速に対応する。

（５）システムの冗長化

システム障害やダウンタイムのリスクを低減するため、重要なシステムやサービスの冗長化を行う。ロードバランシングやフェイルオーバーの仕組みを導入し、システムの可用性を高める。

８　システム開発及び保守

（１）セキュリティ要件の定義

開発初期段階からセキュリティを考慮し、システムの要件定義時にセキュリティ要件を明確にする。

（２）セキュアコーディングの実践

開発者にセキュアコーディングの教育や研修を実施し、コードの脆弱性を減少させる。セキュリティチェックリストやガイドラインを用意し、開発プロセスに組み込む。

（３）テスト環境と本番環境の分離

システムのテスト環境と本番環境は物理的または論理的に分離する。テストデータと本番データの混在を避け、情報の漏洩リスクを低減する。

（４）定期的なセキュリティテスト

システムのセキュリティテストやペネトレーションテストを定期的に実施し、脆弱性の特定と修正を行う。

（５）パッチ管理とシステムのアップデート

システムに関連するソフトウェアやライブラリのセキュリティアップデートやパッチを定期的に適用する。新たな脅威や脆弱性に迅速に対応するためのプロセスを確立する。

（６）システムのエンド・オブ・ライフ管理

サポート終了や更新の停止が予定されているシステムやソフトウェアについては、適切な移行計画を策定する。セキュリティリスクの高まる非サポートのシステムは速やかに更新または置き換える。

９　委託管理

（１）委託先の選定

情報セキュリティに対する取り組みや実績を基に、信頼性の高い委託先を選定する。委託先のセキュリティポリシーや過去の事故履歴を確認し、リスク評価を行う。

（２）委託契約の明確化

委託に関する契約を締結する際には、情報セキュリティに関する条項を明確に記載する。データの取り扱い、アクセス制限、事故時の報告義務など、具体的な取り決めを文書化する。

（３）定期的な監査・確認

委託先の情報セキュリティ対策の状況や取り組みを定期的に監査・確認する。必要に応じて、改善要求やアドバイスを行い、セキュリティ水準の向上を促す。

（４）教育・研修の提供

委託先の職員に対して、情報セキュリティに関する教育や研修を提供する。委託業務に関連するセキュリティリスクや取り組みを共有し、意識の向上を図る。

（５）事故・インシデントの対応フレームワークの確立

委託先での情報セキュリティ事故やインシデント発生時の対応フレームワークを確立する。速やかな報告と共同での対応を行い、影響の拡大を防ぐ。

10　情報セキュリティインシデント対応及び事業継続管理

（１）インシデント対応体制の構築

インシデント発生時の対応体制や役割分担を明確にする。速やかな対応と情報の共有を行うためのプロトコルや手順を策定する。

（２）インシデント報告システムの設置

職員や関連するステークホルダーが、インシデントを速やかに報告するための専用のシステムや連絡先を設置する。

（３）インシデント分析と改善

インシデントの原因を分析し、再発防止策を検討・実施する。インシデントからの学びを通じて、情報セキュリティの向上を図る。

（４）業務継続計画（ＢＣＰ）の策定

災害や大規模なインシデント発生時にも事業を継続するための計画を策定する。事業の中断リスクを低減するための予防策や対応策を明確にする。

（５）定期的なＢＣＰのテストと見直し

業務継続計画の有効性を確認するために、定期的なテストやドリルを実施する。外部環境や組織の変化に応じて、ＢＣＰを見直し・更新する。

（６）復旧策の確立

インシデントや災害からの迅速な復旧を目指し、データバックアップやシステムのリカバリー手順を明確にする。

11　テレワークにおける対策

（１）テレワークガイドラインの策定

テレワークに関するガイドラインを明確にし、職員に周知する。

（２）セキュアな接続の確保

ＶＡＮや仮想デスクトップなど、セキュアな接続手段を提供し、外部からの安全なアクセスを確保する。

（３）端末のセキュリティ対策

テレワークに利用する端末は、最新のセキュリティアップデートやアンチウイルスソフトを常に適用する。個人の端末を利用する場合、企業のデータや情報を端末内に保存しないようにする。

（４）データの取り扱い

機密情報や重要なデータの外部への持ち出しや共有を制限する。必要なデータのみをアクセスできるようにし、データの取り扱いに関する教育を行う。

（５）通信の暗号化

テレワーク中の通信は暗号化することで、中間者攻撃やデータの傍受を防ぐ。

（６）テレワーク環境の監査・モニタリング

テレワーク中のシステムやネットワークの利用状況を監視し、不正アクセスや異常な操作を検知する。

（７）教育・啓発活動

テレワーク特有のセキュリティリスクに対する教育や啓発活動を実施し、職員のセキュリティ意識を向上させる。

附則

令和５年 12 月 21 日制定