情報セキュリティ管理規程

はじめに

概要

本規程は、NPO法人タダカヨ（以下、「法人」という）が取得、保有するあらゆる情報資産を適切に管理し、情報セキュリティインシデントを防止することを目的とする。本法人は、介護業務に有益な無料ITツールの普及・活用支援、インターネット経由での介護職員の学習・教育支援、介護施設ニーズとソリューション提供企業のインターネット上でのマッチング支援、介護施設とボランティア可能者のインターネット上でのマッチング支援、介護事業所の手書き資料のデータ化支援などの事業を行い、IT活用による介護業界の業務改善と人手不足解消に努めることで、介護従事者が要介護高齢者に最期まで寄り添った介護ができる未来に寄与することを目的としている団体である。

情報セキュリティ管理規程の概要

情報セキュリティ管理規程は、法人における情報資産の保護を目的としている。保護対象の情報は、記録媒体や形式を問わず、電子化された情報だけでなく、紙文書などの非電子化情報や、人の記憶にある業務に関する情報も含む。この規程は、自社の情報だけでなく、社内に保管されている他社の情報も保護対象としている。特に、法人の信用に重大な影響を及ぼす可能性のある「極秘情報」や「厳秘情報」といった機密レベルの高い情報については、厳格な管理体制が求められる。

具体的には、以下の事項を定めている。

- 情報資産の目的外利用の禁止
- 情報開示の制限
- アクセス権限の設定
- 保管方法の規程
- 持ち出しや複製に関するルール
- 情報セキュリティに関する緊急事態発生時の対応
- 従業員に対する情報セキュリティ教育
- 情報セキュリティ監査の実施

この規程は、NPO法人タダカヨにおける情報セキュリティ対策の基本方針を定めるものであり、組織全体で情報セキュリティを維持・向上していくための指針となる。特に、NPO法人タダカヨは、メンバーのほとんどが専業ではなく、副業として事業に携わっており、リモートワークであることにも留意しなければならない。

第1章 総則

目的

この規程は、法人が保有する情報資産の機密性、完全性、可用性を確保し、情報セキュリティを維持することを目的とする。

適用範囲

この規程は、理事長、理事、認定ICT講師、ボランティア、その他法人から業務委託を受けた者など、法人の情報資産にアクセスするすべての者に適用される。

用語の定義

この規程において使用する用語は、次の各号に定めるところによる。

- ″情報資産″とは、電子データ、紙文書、その他の記録媒体に記録された情報、プログラム、ソフトウェア、システム等、法人が保有するすべての情報をいう。

- ″機密情報″とは、法人の業務運営上、特に機密性の高い情報であって、情報セキュリティ担当役員が別途指定するものをいう。
- ″情報セキュリティインシデント″とは、情報資産の機密性、完全性、可用性を脅かす事象をいう。

安全管理対策を講じるための組織体制の整備

法人は、情報セキュリティ管理に関する役割と責任を明確にし、安全管理対策を適切に運用できる組織体制を整備する。具体的には、情報セキュリティ責任者や情報システム担当者などの役割を明確にし、各担当者の役割を通じて、情報資産の管理体制を強化する。

情報セキュリティの基本方針

- 法人は、情報セキュリティを経営上の重要課題の一つと認識し、組織全体として情報セキュリティの確保に努める。
- 法人は、情報セキュリティに関するリスクを適切に評価し、必要な対策を講じる。
- 法人は、情報セキュリティに関する法令、ガイドライン、その他の規範を遵守する。
- 法人は、情報セキュリティに関する教育を定期的に実施し、会員の情報セキュリティ意識の向上を図る。
- 法人は、情報セキュリティインシデントに対する適切な対応体制を整備する。

責任者の明確化

情報セキュリティ管理体制の確立にあたり、法人内に情報セキュリティ責任者を設置する。情報セキュリティ責任者は、情報セキュリティに関するすべての管理業務およびインシデント発生時の指揮・対応を担う。また、情報セキュリティ責任者は、法人代表者に対して情報セキュリティ体制に関する報告を定期的に行う。

第2章 情報資産の管理

機密情報の管理

機密情報は、以下の区分に従い、適切に管理しなければならない。

- 極秘情報：法人の事業活動に重大な影響を与える可能性のある情報。アクセスは必要最低限の人員に限定する。
- 重要情報：法人の事業活動に影響を与える可能性のある情報。アクセスは業務上必要な人員に限定する。

機密情報は、施錠できる保管庫に保管するか、アクセス制御されたシステムに保存しなければならない。

機密情報を含む電子データは、パスワードの設定、アクセス権限の付与など、適切なセキュリティ対策を講じなければならない。

機密情報は、業務遂行上必要最低限の範囲においてのみ、アクセス権限を有する者に対して開示することができる。

機密情報の複製は原則として禁止する。

業務上必要な場合は、情報セキュリティ担当役員の承認を得た上で必要な範囲においてのみ作成することができる。

機密情報を含む記録媒体等は、漏えい、滅失、き損等の防止のために必要な措置を講じなければならない。

機密情報を含む記録媒体等は不要となった場合、速やかに裁断、消去、その他復元不可能な方法により廃棄しなければならない。

情報の区分管理

法人が保有する情報は、職務に応じて参照や編集が必要なものに限りアクセスできるよう管理します。情報区分を明確にし、知る必要のない情報は各メンバーに知らせないことを基本方針とします。

個人情報の取扱い

法人は、個人情報の保護に関する法令およびその他の規範を遵守し、個人情報を適切に取り扱う。

個人情報の収集、利用、提供、預託、廃棄等の取扱いについては、別途「個人情報保護方針」及び「個人情報保護規程」を定める。

知的財産権の尊重

法人は、自社の知的財産権を保護すると同時に、他者の知的財産権を尊重する。

ソフトウェアの違法コピー、著作権で保護された情報の無断利用は行わない。

規程および運用体制の整備

法人は、情報セキュリティに関する規程を整備し、策定した規程に従って日常業務を行う。情報セキュリティの目的を明確にし、職員が規程を遵守できるよう定期的な教育および訓練を実施する。遵守状況の確認と改善も適宜行い、規程が形骸化することなく機能するようにする。

情報および端末の外部持ち出しに関する規則

機密情報や端末を法人外に持ち出す場合、事前に情報セキュリティ責任者の許可を得るものとする。また、端末の持ち出しにはセキュリティ対策を講じ、利用者情報など機密性の高いデータについては暗号化などの保護策を必須とする。

在宅・テレワークにおける物理的安全管理対策

1. **在宅環境のセキュリティ**
   在宅勤務時は、機密情報を取り扱う際に他の家族や第三者に内容が見ら

れないように注意し、専用の作業スペースで作業することを推奨します。ディスプレイにはプライバシーフィルターの使用を推奨し、作業を離れる際には画面をロックします。

2. **情報機器の保護**
   ノートPCやスマートフォンなど、業務で使用する端末にはパスワードや生体認証を設定し、不正アクセスや盗難から守るための対策を徹底します。また、テレワーク端末の紛失時には、情報管理責任者に速やかに報告する手順を明記します。

3. **書類の管理と廃棄**
   業務上必要な場合を除き、紙媒体での資料印刷は避けることとし、機密情報を含む書類は適切に廃棄します。やむを得ず印刷した場合には、在宅での施錠可能な保管場所を確保し、不要になった際はシュレッダー等で廃棄します。

4. **会議や通話時の配慮**
   機密情報が含まれる会議や通話を行う際には、他者に聞かれない環境で行い、ヘッドセットの利用などで周囲への情報漏洩リスクを低減します。

情報の区分管理とアクセス権限の管理

1. **情報の区分管理**
   法人が保有する情報は、職務に応じて参照や編集が必要なものに限りアクセスできるよう管理します。情報区分を明確にし、知る必要のない情報は各メンバーに知らせないことを基本方針とします。

2. **アクセス権限の管理**
   Googleドライブ等のシステム上に保存されているフォルダやファイルには、適切な参照権限と編集権限を設定し、必要最低限の範囲でアクセスできるようにします。特定フォルダのアクセス権限は、情報管理責任者によって定期的に見直し、不要な権限の付与を防ぎます。

第3章 情報システムの利用

アクセス管理

情報システムへのアクセスは、業務上必要な者に限定する。
情報システムの利用者には、それぞれ固有のIDとパスワードを付与し、パスワードは定期的に変更する。
アクセス権限は、業務内容や責任の範囲に応じて適切に設定する。
アクセス状況を記録し、定期的に確認を行う。

インターネット利用

法人および個人の名誉・信用を毀損するような情報の発信、わいせつ情報の閲覧・配布は禁止する。

インターネット利用に関するログを取得し、不正アクセス等の監視、事後調査に活用する。

ウイルス対策

コンピュータウイルス対策ソフトを導入し、常に最新の状態に保つ。

不審なメールの添付ファイルを開封しない、信頼できないウェブサイトにアクセスしないなど、ウイルス感染防止に努める。

リモートアクセスにおける端末の管理規程

法人外部から医療・介護システムへのリモートアクセスを行う端末については、法人が指定したセキュリティ対策を実施すること。アクセスにはVPNや多要素認証を推奨し、セキュリティソフトのインストールおよび常時更新を義務付ける。

技術的安全管理対策

1. **パスワードポリシーの設定と管理**
   全メンバーは、定期的にパスワードを更新し、複雑かつ予測されにくい

パスワードを設定することを義務とします。二要素認証（2FA）の導入も推奨し、外部からの不正アクセスを防ぎます。

2. **端末のセキュリティ設定**
   業務で使用する端末には、必ず最新のOSおよびセキュリティパッチを適用します。ウイルス対策ソフトの導入を必須とし、端末の安全性を確保するために自動アップデートを有効にします。

3. **データの暗号化**
   機密情報や個人情報が保存されたファイルやデータベースには暗号化を施し、第三者がアクセスした場合でも情報が守られるようにします。特にクラウドストレージを利用する際には、データの暗号化が必須です。

4. **リモートアクセスのセキュリティ強化**
   テレワークでのリモートアクセスには、VPN（Virtual Private Network）を利用し、インターネット経由のデータ送信を安全に行います。VPNが利用できない場合は、少なくともHTTPS接続を推奨します。

5. **ログ管理とモニタリング**
   アクセスログやシステム操作ログを記録し、必要に応じて情報セキュリティ担当者が定期的に確認します。異常なアクセスや不正利用がないかをモニタリングすることで、迅速なインシデント対応が可能になります。

6. **バックアップ体制の確立**
   重要なデータについては定期的なバックアップを行い、データ消失リスクを軽減します。バックアップデータは暗号化し、かつ安全な場所に保存します。バックアップ体制を定期的に見直し、復元可能かどうかの確認も行います。

7. **不正攻撃の検知と遮断**
   法人のシステムが外部ネットワークから攻撃を受けた際、不正アクセスを早期に検知し遮断する仕組みを導入することを推奨します。これにより、外部からの不正アクセスによる情報漏洩リスクを軽減します。

8. **ネットワーク脆弱性の診断と対策**
   ネットワークにおける脆弱性がないか、定期的な診断を行い、必要に応じて適切な対策を実施します。これにより、システム全体のセキュリティレベルを継続的に維持・向上させます。

第4章 情報セキュリティインシデントへの対応

情報セキュリティインシデントの報告

情報セキュリティインシデントを発見した者、またはその疑いを認めた者は、速やかに所定のセキュリティ事故報告フォームを用いて報告しなければならない。

緊急を要する深刻なインシデントの場合、報告者は報告フォームの送信後、直ちに情報セキュリティ担当者にコミュニケーションツールで連絡しなければならない。

情報セキュリティインシデントへの対応

情報セキュリティ担当者は、報告フォームを受信後、以下の手順で対応する

a）報告内容の確認：報告された情報の正確性と完全性を確認し、必要に応じて報告者に追加情報を求める。

b）影響範囲の特定：インシデントの種類と重大性を評価し、潜在的な影響範囲を特定する。

c）初期対応：データの保護、被害の拡大防止など、必要な初期対応措置を講じる。

d）関係者への通知：インシデントの内容に応じて、理事長、関係部署、および必要に応じて外部の専門家に通知する。

e）調査の実施：インシデントの原因究明のための調査を行う。必要に応じて、外部の専門家の協力を得る。

f）再発防止策の策定：調査結果に基づき、再発防止のための対策を策定する。

g) 報告書の作成：インシデントの概要、対応措置、再発防止策をまとめた報告書を作成し、理事長に提出する。

h)理事長は、提出された報告書を確認し、必要に応じて追加の対策を指示する。

i)情報セキュリティ担当者は、インシデント対応の進捗状況を定期的に理事長に報告する。インシデントの内容によっては、法令に基づく関係機関への報告や、影響を受ける可能性のある個人・組織への通知を行う。

j)インシデント対応完了後、情報セキュリティ担当者は対応結果を理事会に報告し、必要に応じて情報セキュリティ管理規程の見直しを提案する。

事故および違反への対処

事故や規程違反が発生した場合、直ちに情報セキュリティ担当者へ報告し、必要な措置を講じる。再発防止策を策定し、該当者に対する再教育を実施することで、規程遵守の徹底とインシデント発生の防止を図る。

情報セキュリティ対策の評価、見直しおよび改善

法人は、情報セキュリティ対策の運用状況について定期的に評価し、必要に応じて見直し・改善を行う。これにより、情報セキュリティ管理体制の維持・向上を図り、変化するリスクに対応できる柔軟な管理を実現する。

第5章 教育および訓練

教育および訓練の実施

法人は、会員に対し、情報セキュリティに関する教育および訓練を定期的に実施する。情報セキュリティ教育の内容は、以下のとおりとする。

- 情報セキュリティに関する基本的な知識
- 情報セキュリティインシデントの発生状況およびその対策
- 情報セキュリティインシデント発生時の対応方法

- 情報セキュリティに関する法令、ガイドライン等の遵守
- その他、情報セキュリティの維持に必要な事項

情報セキュリティに関する意識向上を図るため、定期的に情報セキュリティに関する研修、訓練等を実施する。新入会員に対し、情報セキュリティに関する初期教育を実施する。管理職に対しては、情報セキュリティに関する責任と役割を理解させるための教育を定期的に実施する。

医療（介護）情報の取扱い台帳の整備

法人は、医療・介護情報の取扱いについて台帳を整備し、アクセス履歴や取扱い状況を記録・管理する。台帳は、情報の適正管理を徹底するための資料とし、情報保護の徹底を図る。

人的安全管理対策

1. **情報セキュリティ教育の徹底**
   タダカヨに所属する全メンバーは、情報管理規程を理解し、遵守するための基本的なセキュリティ教育を受けることを義務とします。教育内容には、パスワード管理、情報の取り扱い、リモートアクセス時の注意事項などが含まれます。

2. **情報セキュリティ誓約書の提出**
   全メンバーは、情報管理規程を理解し遵守することを誓約する文書（情報セキュリティ誓約書）に署名します。これにより、全員が情報セキュリティの重要性を意識し、責任を持って行動することを促します。

3. **情報セキュリティに関する定期的な確認**
   半年または1年ごとに、メンバーに対して情報管理規程の内容を再確認する機会を設けます。最新のセキュリティ対策や運用ルールについて定期的に周知し、変化するリスクに対応できるようにします。

4. セキュリティ意識向上のための連絡体制
   情報セキュリティに関する重要な変更点や新たなリスクについては、メンバーに定期的に通知し、注意喚起を行います。メンバーが気軽に情報セキュリティに関する質問や報告ができる連絡体制を整え、疑問点の解消や不安の軽減を図ります。

5. 不正行為の防止と適切な対処
   悪意ある行為や情報セキュリティ違反を未然に防ぐため、メンバーには高い倫理基準と責任を持つよう促し、不正行為を行わないことを強調します。違反が確認された場合には、状況に応じた適切な処置を講じます。

定期的な監査の実施

法人は、情報セキュリティ対策の実施状況および運用体制の有効性を確認するため、情報セキュリティ監査を定期的に実施する。監査の結果は、情報セキュリティの改善点を明確にし、必要に応じて適切な対応措置を取るために活用される。監査結果については、情報セキュリティ責任者を通じて法人代表者に報告し、全社的な改善を図る。

第6章 BYOD（個人所有デバイス）の利用

目的

本章は、NPO法人タダカヨの業務において、会員が個人所有のデバイス（以下、「BYOD」という）を使用する際の規程を定めることを目的とする。

適用範囲

本規程は、法人の業務に携わるすべての者（理事長、理事、認定ICT講師、ボランティア、その他法人から業務委託を受けた者）が、個人所有のデバイスを用いて法人の業務を行う場合に適用される。

セキュリティ対策

- OSやアプリケーションは常に最新の状態に更新すること。

- デバイスにはパスワードまたは生体認証による画面ロックを設定すること。
- 法人のデータを保存する場合は、暗号化を行うこと。
- 公共のWi-Fiネットワークを使用する場合は、必ずVPNを使用すること。
- 業務データは、クラウドストレージなど、法人が承認したサービスにのみ保存すること。
- 業務データと私的データは明確に分離して管理すること。

紛失・盗難時の対応

BYODの紛失または盗難が発生した場合、直ちに情報セキュリティ担当役員に報告すること。報告を受けた情報セキュリティ担当役員は、必要に応じてリモートワイプなどの措置を講じること。

附則

この規程は、理事会の承認を得た日から施行する。この規程は、必要に応じて改訂することができる。

参考情報

- システム監査学会 情報セキュリティ研究プロジェクト（2002.11）「情報セキュリティ管理規程」作成の手引