○社会福祉法人福利厚生センターにおける情報セキュリティに関する規程

（平成２７年６月１７日規程第１８号）

（目的）

第１条　この規程は、社会福祉法人福利厚生センター（以下「センター」という。）が保有する情報資産には、個人情報など極めて重要な情報が多数含まれ、情報を取り扱う者の故意又は過失による情報漏洩及びコンピュータウィルス又は不正侵入による情報資産の改ざん、窃取若しくは情報システムの破壊等が起こった場合、業務に重大な影響を及ぼすとともに個人の権利利益の侵害等、センターの信頼が大きく損なわれるおそれがあることから、これらの防止を図り情報資産の安全を確保するために必要な事項を定めることを目的とする。

（意義）

第２条　この規程における用語の意義は、次のとおりとする。

(1)　情報資産

情報（電磁的に記録されたものに限る。以下特段の記述がない場合、同様とする。）及び情報を管理する仕組み（情報システム及びシステム開発、運用及び保守のための資料等）の総称をいう。

(2)　情報セキュリティ

情報資産の機密の保持及び正確性、完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

(3)　情報システム

センター内において、ハードウェア、ソフトウェア、ネットワーク、記録媒体で構成されるものであって、これら全体で業務処理を行うものをいう。

(4)　コンピュータ

ハードウェア及びソフトウェアで構成されプログラムに従って情報処理を行う機器、周辺機器及び磁気ディスク等の記録媒体をいう。

(5)　ネットワーク

ハードウェアを相互に接続するための通信網及び通信機器（ハードウェア及びソフトウェア）で構成され、情報処理を行う仕組みをいう。

(6)　電子情報

センターの業務執行に関わる情報で、かつ、情報システムで取り扱う電子的方式または電磁的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。

(7)　コンピュータウィルス

第三者のプログラム及びデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、自己伝染機能、潜伏機能、発病機能のいずれか一つ以上を有するものをいう。

(8)　情報セキュリティポリシー

センターが所有する情報資産の情報セキュリティ対策について、総合的かつ具体的に取りまとめたものであって、情報セキュリティ対策基準及び実施手順をいう。

(9)　情報セキュリティ対策基準

この規程に定められた情報セキュリティを確保するために遵守すべき行為及び判断等の基準を定めるものをいう。

(10)　情報セキュリティ実施手順

　　情報セキュリティポリシーには含まれないものの、情報セキュリティ対策基準に定められた内容を実施するための手順を定めたものをいう。

（制定）

第 3 条　情報セキュリティ対策基準は理事長が定める。

2　情報セキュリティ実施手順は情報システム委員会において内容の審議を行い、常務理事が定める。

（最高情報セキュリティ責任者）

第 4 条　最高情報セキュリティ責任者は、理事長とする。

（運用）

第 5 条　情報セキュリティポリシーの運用にあたっては、情報技術等の進展に応じ必要な措置を講じるものとする。

（情報資産への脅威）

第 6 条　情報セキュリティ対策を講じるうえで、情報資産に対してその発生度合い及び発生した場合の影響を考慮して、以下に掲げる脅威の対策を講じるものとする。

(1)　アクセス権限を有する者以外の者による故意の不正アクセス又は不正操作によるデータ若しくはプログラムの持ち出し、盗聴、改ざん、消去、機器及び記録媒体の盗難等

(2)　アクセス権限を与えられた取扱者による意図しない操作、故意の不正アクセス又は不正操作によるデータ若しくはプログラムの持ち出し、盗聴、改ざん、消去、機器及び記録媒体の盗難、情報システムの機器操作によるデータ漏洩等

(3)　地震、落雷、火災等の災害や事故、故障等

（範囲及び責務）

第 7 条　センター役職員は情報セキュリティの重要性について共通の認識を持つとともに、情報資産の利用にあたっては、情報セキュリティポリシーを遵守するものとする。

2　センターは、労働者派遣に関する基本契約（以下「人材派遣契約」という。）に基づきセンターに派遣されセンター業務を行う者（以下「派遣職員」という。）に対し情報セキュリティポリシーを遵守させるものとする。

3　センターは、情報処理業務を外部に委託する場合にあっては、業務委託契約に基づきセンター業務を行う者（以下「委託先事業者」という。）に対し情報セキュリティポリシーを遵守させるものとする。

（違反に対する措置）

第 8 条　役職員が情報セキュリティポリシーに反したと認められる場合は、その役職員に対し必要な措置を講じるものとする。

2　派遣職員及び委託先事業者が、情報セキュリティポリシーに反したと認められる場合は、人材派遣

契約及び業務委託契約に基づく措置を含め必要な措置を講じるものとする。

（情報セキュリティ対策基準の策定）

第９条　次に掲げる事項に関し情報セキュリティ対策基準を別に定める。

(1)　管理体制

センターの情報資産について、適切に情報セキュリティ対策を推進・管理するための体制

(2)　人的セキュリティ対策

情報資産を取り扱う者の責務、情報セキュリティポリシーの啓発、情報資産に対する侵害が発生した場合の報告義務等の人的な対策

(3)　物理的セキュリティ対策

ハードウェアを設置する場所の安全確保並びに当該設置場所への入退室及び機器の管理上の物理的な対策

(4)　技術的セキュリティ対策

情報資産を不正なアクセスから適切に保護するため、情報資産へのアクセス制御及びコンピュータウィルス感染防止等の技術的な対策

(5)　運用

不正アクセス及び不正操作により情報システムに対して被害を及ぼすことを防ぐための情報システム監視等の運用面における必要な措置及び障害が発生した際の迅速な対応を行うための障害時の対応

(6)　評価及び見直し

情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価の実施、並びにその評価結果及び情報システムの変更、新たな脅威等情報セキュリティを取り巻く状況を踏まえた、情報セキュリティ対策基準の見直しを実施することを定める。

（規程の改廃）

第10条　この規程の改廃は、情報システム委員会の検討を経るものとする。

附　則

この規程は、平成２７年６月１７日から実施する。

○社会福祉法人福利厚生センター情報セキュリティ対策基準

（平成２７年６月１７日理事長伺い定め）

第１章　総則

（通則）

第１条　社会福祉法人福利厚生センター（以下「センター」という。）における情報セキュリティに関する規程（平成27年6月17日規程第18号）第9条に基づき、情報セキュリティ対策基準（以下「対策基準」という。）を定める。

（管理体制）

第２条　情報セキュリティ確保のため、次の各号に掲げる事項により管理を行う。

(1)　管理機関

情報セキュリティポリシーに関する事項については情報システム委員会で行う。

(2)　最高情報セキュリティ責任者

最高情報セキュリティ責任者は、情報システム委員会を主宰し、情報セキュリティポリシーの実施状況を継続的に点検管理し、改善点の調査及び見直し、並びに教育、啓発活動を行う。

(3)　情報セキュリティ管理者及び情報セキュリティ管理補佐官

情報セキュリティ管理者は、最高情報セキュリティ責任者を補佐して必要な情報の集約を図るとともに、センター各部署と連絡調整し、各部セキュリティ管理者への助言を行うものとし、常務理事をもってこれに充てる。

情報セキュリティ管理補佐官は、専門的な知識及び経験をもって情報セキュリティ管理者を補佐するものとし、最高情報セキュリティ責任者が選任する。

(4)　部セキュリティ管理者

部セキュリティ管理者は、部における情報セキュリティポリシーの遵守に関する意見の集約、当該部の職員（労働者派遣に関する基本契約に基づきセンターに派遣されセンター業務を行う者を含む）に対する教育、訓練、助言及び指示を行うこととし、各部の長又は副部長をもってこれに充てる。

第２章　人的セキュリティ対策

（人的セキュリティ）

第３条　情報セキュリティの向上は、利便性の向上とは必ずしも相容れないものであり、利用者の理解が得にくい場合もあることから十分な教育及び啓発が講じられるように必要な対策を人的セキュリティとして定める。

（役職員の責務）

第４条　役職員は次の各号に掲げる事項を遵守しなければならない。

(1)　役職員は情報セキュリティポリシーに定められている事項を遵守しなければならない。

(2)　役職員は、職務の遂行において情報資産を作成又は取り扱う場合は、法令規程等を遵守しなければならない。

(3)　役職員は、情報資産を業務上の目的以外で取り扱ってはならない。

(4)　役職員は、パーソナルコンピュータの使用を終了又は中断する場合は、適切な操作をしなければならない。

(5)　役職員は、パーソナルコンピュータにおける周辺機器の接続及び取り外し、ソフトウェアのインストール及びアンインストールなど、パーソナルコンピュータの環境及び設定を変更してはならない。ただし、業務上必要な場合は、別に定められた規程等により取り扱うものとする。

(6)　役職員は、センターが認めていないハードウェア及び媒体を執務室に持ち込み業務に使用してはならない。

(7)　職員は、不明な点、遵守することが困難な点がある場合には、速やかに部セキュリティ管理者に相談し指示を仰がなければならない。

（認証情報等の管理）

第 5 条　役職員は、情報システム毎付与された利用者 ID（情報システムを利用する権利を有する者であることを識別するために割当てる文字列をいう。）及びパスワード（情報システムを利用する者が本人であることを識別するための暗証文字列をいう。）に関し、次の各号に掲げる事項を遵守しなければならない。

(1)　管理者権限（情報システムの保守及び運用を行うことができる者に与えられる特別の権限をいう。）を有する者として識別される利用者 ID による情報システムの利用は、業務上必要最小限の範囲とする。

(2)　パスワードの設定に当たっては、十分な長さとして推測されやすいもの又は解読されやすいものを避ける。

(3)　パスワードは定期的に変更を行うこと。

(4)　ＩＤ及びパスワードは厳重に管理し、不用意に漏らさない、メモ等を作らないなど、秘密保持に努めなければならない。

（教育・訓練等）

第 6 条　情報セキュリティポリシーを実施する際、その一部は情報システムに組み込まれた技術的措置によって自動的に実現することが可能であるが、多くの部分は組織の責任者及び利用者の判断や行動に依存しているため、情報資産を取り扱う全ての者が情報セキュリティの重要性を認識し情報セキュリティポリシーを理解・実践させるため、計画的に教育・訓練等を行う。

（事故・欠陥に対する対処）

第 7 条　情報セキュリティに関する事故やシステム上の欠陥（以下「事故等」という。）が発見された場合、その事故又は欠陥による被害を拡大しないように対処方法を定める。

(1)　職員は、事故等を発見した場合には、独自に事故等の解決を図らずに速やかに部セキュリティ管理者に報告し、指示を仰がなければならない。

(2)　部セキュリティ管理者は、事故等の報告を受けた場合には速やかに解決方法を指示又は情報セキュリティ管理者の指示を仰ぎ対処することとし、部セキュリティ管理者自らが指示した時は情報セキュリティ管理者へ報告しなければならない。

(3)　情報セキュリティ管理者は、情報セキュリティに関する事故、情報システム上の欠陥や誤動作が発生した場合の報告体制及び復旧体制を定めなければならない。

(4)　情報セキュリティ管理者は、発生した事故等を分析し、再発防止に努めなければならない。

（情報漏えい発生に対する対処）

第 8 条　情報資産に関する漏えい（以下「情報漏えい」という。）が発生した場合、その情報漏えいによる直接的・間接的被害が最小限に抑えるように対処方法を定める。

(1)　職員は、情報漏えいに関する兆候や事実を発見した時又は情報漏えいを発見した時は、速やかに部セキュリティ管理者に報告し、指示を仰がなければならない。

(2)　部セキュリティ管理者は、情報漏えいの報告を受けた場合には速やかに解決方法を指示又は情報セキュリティ管理者の指示を仰ぎ対処することとし、部セキュリティ管理者自らが指示した時は情報セキュリティ管理者へ報告しなければならない。

(3)　情報セキュリティ管理者は、情報漏えいが発生した場合の報告体制及び被害の復旧体制を定めなければならない。

(4)　情報セキュリティ管理者は、発生した情報漏えいを分析し、再発防止に努めなければならない。

（外部委託に関する管理）

第 9 条　情報システムの開発・保守・運用管理等を外部委託事業者に発注する場合は、外部委託事業者から下請けとして受託する業者も含めて、情報セキュリティポリシーに関して外部委託業者が守るべき内容の遵守を明記した契約を行わなければならない。また、外部委託事業者との契約書には、情報セキュリティポリシーに関して守るべき内容が遵守されなかった場合の規定を定めなければならない。

第 3 章　物理的セキュリティ対策

（パーソナルコンピュータ）

第 10 条　役職員は、パーソナルコンピュータの盗難防止等、セキュリティ維持に必要な対策を講じなければならない。

（ハードウェアの持出し）

第 11 条　役職員は、ハードウェアを決められた設置場所から外に持ち出してはならない。ただし、業務上必要な場合は、別に定める規程等により取り扱うこととする。

第 4 章　技術的セキュリティ対策

（技術的セキュリティ）

第 12 条　情報資産を不正なアクセス及び情報漏洩から適切に保護するため、情報システムの構築及び管理対策、情報資産へのアクセス制御及びコンピュータウィルス等の対策を技術的セキュリティとして定める。

（セキュリティ要件の整備）

第 13 条　情報セキュリティ管理者は、情報セキュリティ対策が継続的に行える環境を整備する観点から、機器等を選定しなければならない。

2　情報セキュリティ管理者は、情報システムの構築又はソフトウェアの開発を外部委託により行う場合に、調達する情報システム又はソフトウェアの開発における適切な情報セキュリティ対策が実現されるようセキュリティ要件を定めなければならない。

（セキュリティ提案仕様の検討）

第 14 条　情報セキュリティ管理者は、提案者から提出されたセキュリティ提案仕様について、情報セ

キュリティ確保の観点から適切に検討しなければならない。

（データ保全）

第 15 条　情報セキュリティ管理者はサーバ等に記録された情報について、その重要度に応じて期間を設定し、定期的にデータの退避を行う。

（電子メール）

第 16 条　情報セキュリティ管理者は、情報システムを経由しての外部から外部への電子メール転送を不可能とする等、他の情報システムに悪影響を与えない設定を講じる。

（ウェブサイト）

第 17 条　情報セキュリティ管理者は、役職員が閲覧することが可能なウェブサイトを制限し、定期的にその見直しを行う。

（無許可ソフトウェア導入の禁止）

第 18 条　役職員はハードウェアに対して、情報システム管理者（情報システムを管理する者として理事長が選任した者をいう。以下同じ。）の許可なしにソフトウェアを導入してはならない。

（ハードウェア構成の変更）

第 19 条　役職員はハードウェアに対して、情報システム管理者の許可なしに改造及び増設・交換をおこなってはならない。

（利用者登録）

第 20 条　情報セキュリティ管理者は、情報システムの利用者の登録・変更・抹消等における管理方法を定めなければならない。

2　利用者ＩＤは、原則として個人単位に付与されなければならない。なお、業務システムについては、必要に応じた最小の単位を決めてその単位毎に付与することができる。

3　情報セキュリティ管理者は、長期間使用していない利用者ＩＤについては、すみやかに削除しなければならない。

（利用者認証手順）

第 21 条　情報セキュリティ管理者は、利用者を認証する手順及び利用者の追加・変更・削除する手順を定める。

2　利用者認証については、利用者ＩＤに加えてパスワードを付与する。

（ネットワークへの接続制御）

第 22 条　情報セキュリティ管理者は、必要ない他のネットワークサービスを使用できるようにしてはならない。

2　情報セキュリティ管理者は、不正アクセスを防止するため、適切なネットワーク経路制御を施さなければならない。

3　情報セキュリティ管理者は、役職員が閲覧することが可能な外部のホームページを制限し、定期的にその見直しを行わなければならない。

（外部からのアクセス）

第 23 条　情報セキュリティ管理者は、外部からのアクセスの許可について必要最小限にしなければならない。

（遠隔地にあるシステムへの接続）

第 24 条　情報セキュリティ管理者は、遠隔地にある情報システムへ接続する場合は、安全な接続が可能となるよう適切な制御を施さなければならない。

2　情報セキュリティ管理者は、保守・点検のため外部からの接続口を設ける場合には、必要十分なセキュリティ対策を講じなければならない。

(パスワード)

第 25 条　情報セキュリティ管理者は、パスワードの変更を行わない職員に対しては一定期間経過後に情報システムが使用できないようにするなど、パスワード変更を遵守させる措置を講じなければならない。

(コンピュータウィルス等対策)

第 26 条　コンピュータウィルス等の対策として、次の各号に掲げる事項を実施しなければならない。

(1)　情報セキュリティ管理者はコンピュータウィルス等情報について、利用者に対する注意喚起をおこなう。

(2)　情報セキュリティ管理者は定期的にコンピュータウィルス等に関する情報収集をおこなう。

(3)　役職員は重要なシステムの設定に係るファイル等について、定期的に当該ファイルの検査をおこなう。

(4)　情報セキュリティ管理者はサーバ及びパーソナルコンピュータにおいて、定期的にコンピュータウィルス等の確認を行えるよう対策を講じる。

(5)　情報セキュリティ管理者はコンピュータウィルス等確認用のパターンファイル等を常に最新のものに保つ。

(6)　情報セキュリティ管理者は添付ファイルのある電子メールを送受信する場合に、コンピュータウィルス等の確認を行えるよう対策を講じる。

第 5 章　運用

(運用)

第 27 条　情報セキュリティポリシーを確実に運用していくための対策を定める。

(情報システムの監視)

第 28 条　情報セキュリティ管理者は、情報システムの運用にあたって常に情報システムを監視するとともに情報セキュリティ障害に対して注意を払わなければならない。また、情報システムにおいて基準となる時刻に、端末等の時刻が同期されているかについて定期的に確認すること。

(情報セキュリティポリシーの遵守状況の確認)

第 29 条　情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について自己点検を実施し、運用上支障が生じていないかについて確認を行わなければならない。

(セキュリティ障害時の対応)

第 30 条　情報セキュリティ管理者は、セキュリティ障害が発生した場合、すみやかに対応するとともに、再発防止の措置を講じなければならない。特に、サイバー攻撃等重大なセキュリティ事案を検知した場合には、最高情報セキュリティ責任者へ報告し、必要な指示を仰ぐとともに、所管省庁等へ速やかに連絡しなければならない。

(障害拡大の防止措置)

第 31 条　情報セキュリティ管理者は、故意の不正アクセス又は不正操作により情報システムに障害を及ぼすことが明らかな場合には、情報システムの停止を含む必要な措置を講じるとともに、その障害の原因となる行為の記録の保存に努めなければならない。

（障害の調査）

第 32 条　情報セキュリティ管理者は、セキュリティ障害が発生した場合は次の各号に掲げる事項について調査を行わなければならない。

(1)　障害の内容

(2)　障害の発生した原因

(3)　確認した被害と影響範囲

（障害への対応）

第 33 条　情報セキュリティ管理者は、速やかにセキュリティ障害を復旧するとともに最高情報セキュリティ責任者へ報告しなければならない。なお、障害が外部に重大な影響を及ぼす恐れがある場合は、最高情報セキュリティ責任者から必要な指示を仰がなければならない。

（再発防止の措置）

第 34 条　最高情報セキュリティ責任者は、必要な再発防止の措置を講じなければならない。

（災害等の対応）

第 35 条　情報セキュリティ管理者は、災害等が発生した場合、すみやかに対応するとともに予防策を作成しなければならない。

（災害措置）

第 36 条　情報セキュリティ管理者は、災害等の発生により、情報システムに損害を及ぼすことが明らかな場合には、情報システムの停止を含む必要な措置を講じなければならない。

（災害の調査）

第 37 条　情報セキュリティ管理者は、災害等が発生した場合は次の各号に掲げる事項について調査を行わなければならない。

(1)　災害の内容

(2)　災害の発生した原因

(3)　確認した被害と影響範囲

（災害への対応）

第 38 条　情報セキュリティ管理者は、速やかにシステムを復旧するとともに最高情報セキュリティ責任者へ報告しなければならない。なお、外部に重大な影響を及ぼす恐れがある場合は、最高情報セキュリティ責任者から必要な指示を仰がなければならない。

（予防措置）

39 条　最高情報セキュリティ責任者は、必要な予防措置を講じなければならない。

第 6 章　評価及び見直し

第 40 条　最高情報セキュリティ責任者は、評価及び見直しが必要となる事象が発生した場合には必要な見直しを行い、適切な情報セキュリティポリシーの維持及び運用に努めなければならない。

第 7 章　実施手順の策定

第 41 条　対策基準に定めるほか、実施に必要な手順は別に定める。

附　則

この伺い定めは、平成２７年６月１７日から実施する。

附　則

この伺い定めの改正は、２０２２年１２月２日から実施する。