

システム利用規程

社会福祉法人 恩賜 財団 済生会

特別養護老人ホーム 淡海荘

栗東デイサービスセンター

小規模多機能型居宅介護事業所 なでしこ栗東

システム利用規程

1 趣旨

2 対象者

3 対象システム

4 遵守事項

4. 1 P Cにおけるセキュリティ対策

4. 1. 1 P Cの利用

4. 1. 2 P Cで利用できるソフトウェア

4. 1. 3 P Cのパスワード管理

4. 1. 4 P Cでの情報の取り扱い

4. 1. 5 P Cの使用場所

4. 1. 6 P Cの利用者の変更

4. 1. 7 P Cの利用上の注意事項

4. 2 P Cや媒体の取り扱いに関するセキュリティ対策

4. 2. 1 使用機器に関する遵守事項

4. 2. 2 P Cの修理

4. 2. 3 媒体の保管

4. 2. 4 媒体の移動

4. 2. 5 P Cと媒体の再利用および廃棄

4. 3 マルウェア対策

4. 3. 1 マルウェアやサイバー攻撃に関する教育の受講

4. 3. 2 マルウェア対策ソフトの利用

4. 3. 3 電子メールやインターネット閲覧を介してのマルウェア被害の防止

4. 3. 4 マルウェアに感染した場合、または感染したと疑われる場合

4. 4 電子メール利用におけるセキュリティ対策

4. 4. 1 電子メールサービス利用端末機器のセキュリティ

4. 4. 2 電子メールで送受信される情報の保護

4. 4. 3 電子メールサービスとネットワーク保護

- 4. 5 W e bサービス利用におけるセキュリティ対策
- 4. 5. 1 W e bブラウザ利用端末機器のセキュリティ
- 4. 5. 2 W e bブラウザの利用
- 4. 5. 3 W e bサーバの利用
- 4. 5. 4 アクセス制御されたW e bサイトの閲覧に関して
- 4. 5. 5 W e bサイトの閲覧許可

4. 6 ネットワークの利用

- 4. 6. 1 社内ネットワーク及びインターネットの業務目的以外の利用禁止
- 4. 6. 2 社内ネットワークで利用可能なサービス
- 4. 6. 3 社内ネットワークへの接続時の注意事項

4. 7 リモートアクセスサービス利用時のセキュリティ対策

- 4. 7. 1 利用申請
- 4. 7. 2 使用機器に関する遵守事項
- 4. 7. 3 物理セキュリティ遵守事項

5 運用確認事項

6 例外事項

7 罰則事項

8 公開事項

9 改訂

1 趣旨

本規程は、システムやネットワーク利用時における可用性・機密性・完全性を確保し、発生し得る各種問題を未然に防ぐことを目的とする。

2 対 象 者 ： P C、システム、ネットワークを利用するすべての職員

3 対象システム：当施設より支給・貸与する P C、および利用するシステムと ネットワーク

4 遵守事項

4. 1 P Cにおけるセキュリティ対策

4. 1. 1 P Cの利用

当施設の業務に利用する P Cは、以下のものでなければならない。

(1) 当施設が支給・貸与する P Cのみとする。

4. 1. 2 P Cで利用できるソフトウェア

当施設が支給・貸与する P Cに導入するソフトウェアは、以下を遵守しなければならない。

- (1) 職員は、当施設の事務担当者（以下担当者）が初期導入したソフトウェアのみ使用すること。
- (2) 規定されたソフトウェア以外で、業務上やむを得ず使用する必要がある場合、 P Cの利用者は、担当者に申請し、許可を得なければならない。
- (3) 職員は、担当者が提供するソフトウェア情報をもとに最新の修正プログラム等を適用しなければならない。

4. 1. 3 P Cのパスワード管理

当社が支給・貸与する P Cの盗難、紛失に備え、以下を遵守しなければならない。

- (1) 職員は、支給・貸与を受けた場合、 P Cログオンの初期パスワードを 直ちに変更しなければならない。
- (2) 職員は、担当者の設定したパスワードポリシーに従い、パスワードを設定し、定期的に変更しなければならない。

- (3) 職員は、第三者が容易に推測できないパスワードを選択すること。

4. 1. 3 P Cでの情報の取り扱い

当施設が支給・貸与するP Cでの情報の取扱いは、以下を遵守しなければならない。

- (1) 職員は、P Cで機密情報を取り扱う場合には、機密情報を取り扱う許可を情報の管理責任者に申請し、許可を得なければならない。許可を得た機密情報は、万一の漏洩に備え、暗号化等の対策を実施しなければならない。
- (2) 職員は、情報の管理責任者の許可無く、機密情報を外部媒体に保管してはならない。
- (3) 職員は、機密情報取り扱い後には、不必要となった機密情報を直ちに P Cと外部媒体から削除しなければならない。

4. 1. 4 P Cの使用場所

当施設が支給・貸与するP Cの利用は、利用を許可した以下の場所のみとする。

- (1) 当施設の利用者スペース、事務フロア、会議室等、当施設内
- (2) 社外では不特定の他人の目にふれない場所。ただし、覗き見防止フィルターにより覗き見が困難な対策を施すP Cは除く。

4. 1. 5 P Cの利用上の注意事項

当施設が支給・貸与するP Cの利用にあたり、以下を注意する。

- (1) 職員は、社外にP Cを持ち出す場合、盗難・窃盗に注意し取り扱わなければならない。
- (2) 職員は、社外でP Cを利用する場合、情報の盗み見に注意しなければならない。
- (3) 職員は、利用環境を整理整頓すると共に、デスクトップを整理し、クリアスクリーンを心がけなければならない。
- (4) 職員は、P C利用に伴う、P C及びそれに付随する機器の紛失・盗難、また情報漏えい等セキュリティインシデントが発生した場合、個人情報保護規定に従い、統括個人情報管理者と連携の上、その事実の調査を行うと共に必要な措置を講ずるものとする。
- (5) P Cの利用状況は、担当者によってモニタリングされていることに留意しなければならない。

4. 2 P Cや媒体の取り扱いに関するセキュリティ対策

4. 2. 1 使用機器に関する遵守事項

- (1) 職員は、当施設が指定した P C や媒体を利用しなければならない。
- (2) P C や媒体は、盗難に遭わない様に、また紛失しない様に、利用者が管理を行わなければならない。

4. 2. 2 P C の修理

- (1) P C の修理を依頼する場合は、申請書を提出し、担当者を通して修理を依頼しなければならない。
- (2) P C 等の修理を依頼する利用者は、機密性の高い情報が保管されていないことを確認した上で修理を依頼しなければならない。故障の状況により、保管されている情報の確認や保護が実施できない場合には、利用者は、担当者から指定された方法にて修理を依頼しなければならない。

4. 2. 3 媒体の保管

- (1) 職員が、機密性の高い情報を媒体に保存する時は、保管された情報に権限のない人がアクセスできないよう、データまたは媒体に対して暗号化を行わなければならない。

4. 2. 4 媒体の移動

- (1) 職員は、機密性の高い情報を保管している媒体を、その情報の管理責任者の許可なく社外へ持ち出してはならない。
- (2) 職員は、機密性の高い情報を保管している媒体を郵送や宅配便等で送付する場合、セキュリティが保たれた郵送や宅配便等を利用すること。

4. 2. 5 P C と媒体の再利用および廃棄

- (1) P C または媒体の再利用および廃棄を行う場合は、担当者に廃棄申請を提出し、指定された方法にて再利用および廃棄処理を行う。

4. 3 マルウェア対策

4. 3. 1 マルウェア対策ソフトの利用

当社より支給・貸与する P C は、マルウェア対策ソフトにより以下の対策をしなければ

ならない。

- (1) 職員は、担当者が設定したマルウェア対策ソフトの設定を変更してはならない。
- (2) 職員は、ドライブ全体に対する定期スキャンを無効化してはならない。また、やむを得ずスキャンを停止した場合は、できるだけ早く定期スキャンを再開しなければならない。

4. 3. 2 電子メールやインターネット閲覧を介してのマルウェア被害の防止

電子メールや、インターネット閲覧による被害を招かないため、以下を遵守しなければならない。

- (1) 職員は、メールの受信にあたっては、メールや Web メール上でスパムメールや迷惑メールを分別する機能を有効にしなければならない。
- (2) 職員は、送信元不明（特にフリーメール）のメールに添付されたファイルや、実行形式のまま添付されたファイルなど、不審だと疑われるメールの添付ファイルは安易に開いてはならない。また、安易に URL リンクをクリックしてはならない。不審だと疑われるメールを受信した場合は、即座に担当者に報告しなければならない。
- (3) 職員は、ファイルを添付してメールを送信する場合、当該ファイルのマルウェア感染が無いことをマルウェア対策ソフトにて確認後、メールを送信しなければならない。
- (4) インターネット閲覧によるマルウェア感染を防ぐ為に、職員は、業務上関係のないサイトの閲覧をしてはならない。

4. 3. 3 マルウェアに感染した場合、または感染したと疑われる場合

マルウェアに感染、もしくは感染が疑われる場合は、利用者は以下を遵守しなければならない。

- (1) 職員は、以下の症状などが見受けられた場合には、担当者に報告し、対応方法の指示を受け、対応しなければならない。
 - ・マルウェア付のメールが送られたとの連絡が取引事業所などからあった。
 - ・メールの添付ファイルを開いたが、何も表示されなかった。
 - ・インターネットのサイトを閲覧中に表示される広告などの表示を消すことができなくなった。
- (2) 職員は、有線 LAN 接続の PC はネットワークケーブルを外し、無線 LAN 接続の PC は無線 LAN 機能を OFF にしなければならない。
- (3) 職員は、担当者の指示に従って、マルウェア駆除をしなければならない。
- (4) 職員は、マルウェア被害の影響範囲が施設外にまで至っている可能性が認められる場合、その影響について、担当者に報告しなければならない。

4. 4 電子メール利用におけるセキュリティ対策

4. 4. 1 電子メールサービス利用端末機器のセキュリティ

- (1) 電子メールの利用にあたっては、担当者が指定した電子メールソフトウェアを用いなければならない。また、担当者の指示に従い、当該ソフトウェアを最新の状態に保たなければならない。
- (2) 電子メールの利用者は、電子メールソフトウェアにパスワードを保存してはならない。電子メールソフトウェア起動時にユーザ認証を必要とする設定にしなければならない。

4. 4. 2 電子メールで送受信される情報の保護

- (1) 電子メールの利用者は、当施設の事業に関わる情報や、サービス利用者・職員等の個人情報などの機密情報をメールにて送受信する場合は、機密情報の内容に応じて暗号化、電子署名などの処置を施さなければならない。
- (2) 電子メールの利用者は、電子メールの送信にあたっては、送信先のメールアドレスに間違いがないか、確認の上送信しなければならない。
- (3) 電子メールの利用者は、電子メールを社外の個人的なメールアドレスに転送する場合は、担当者に申請をし、許可を得なければならない。

4. 4. 3 電子メールサービスとネットワーク保護

- (1) 電子メールの利用者は、業務目的以外に電子メールサービスを利用してはならない。
- (2) 電子メールの利用者は、スパムメールを受信した場合はこれを転送してはならない。
- (3) 電子メールの利用者は、社外のメーリングリストに参加する場合は、当該メーリングリストの信頼性、および業務への必要性を充分考慮した上で参加しなければならない。また、参加意義の無くなった場合は、直ちに脱退しなくてはならない。また公序良俗に反する発言をしてはならない。
- (4) 電子メールの利用者は、電子メールの送信にあたっては、添付するファイルの容量を考慮しなければならない。規定容量以上のファイルを送信せざるを得ない場合は、担当者的にて指定されたファイル共有サイト・ファイル転送サイトを利用しなければならない。
- (5) 電子メールの利用者は、その他、無用な電子メールを送受信することにより、ネットワークに負荷をかけてはならない。また、電子メールはテキスト形式で送信するよう

設定しなければならない。

4. 5 Web サービス利用におけるセキュリティ対策

4. 5. 1 Web ブラウザ利用端末機器のセキュリティ

- (1) 職員は、Web ブラウザの利用にあたって、担当者が指定した Web ブラウザを用いなければならない。また、情報システム部の指示に従い、当該ソフトウェアを最新の状態に保たなければならない。
- (2) 職員は、Web ブラウザの利用にあたって、担当者が指定した Web ブラウザの設定を施さなければならない。

4. 5. 2 Web ブラウザの利用

- (1) 職員は、社内及びインターネット上の Web サーバへのアクセスは、業務上必要な場合のみ利用することができる。
- (2) 職員は、URL リンクをクリックするとき、リンク先の URL を確認してからクリックしなければならない。この場合、リンク先が、信頼できない URL である場合は、クリックしてはならない。また、バナー広告についても同様に、業務上必要のないバナー広告はクリックしてはならない。
- (3) 職員は、業務上不必要なファイルやソフトウェア、不審なファイルなどをダウンロードしてはならない。
- (4) 職員は、署名の無いあるいは信頼できないサイトの ActiveX、Java、JavaScript、VBScript などのコードは実行してはならない。
- (5) 業務と関連の無い Web メールを利用してメールの送受信を行ってはならない。
- (6) 職員は、施設内外の Web サーバに対して、攻撃等不正なアクセスを行ってはならない。また、攻撃や不正なアクセスを目的として施設内外のシステムを利用してはならない。

4. 5. 3 Web サーバの利用

- (1) サービス提供時の情報の発信（掲示板、SNS などへの書き込み）に関しては、個人情報保護委員会です承された場合のみ許可される。このとき、情報の正確性を確保し、必要最小限の範囲で発信しなければならない。また、下記に該当する情報の発信は禁止する。また、情報の閲覧に関しても同様とする。
 - ・ 著作権、商標、肖像権を侵害するおそれのあるもの

- ・ プライバシーを侵害するおそれのあるもの
 - ・ 他者の社会的評価にかかわる問題に関するもの
 - ・ 他者の名誉・信用を傷つけるおそれのあるもの
 - ・ 施設の信用・品位を傷つける恐れのある者
 - ・ 性的な画像や文章に該当するおそれのあるもの
 - ・ 不正アクセスを助長するおそれのあるもの
 - ・ 差別的なもの
 - ・ 虚偽のもの
 - ・ 施設内の機密情報
 - ・ その他公序良俗に反するおそれのあるもの
- (2) 職員は、担当者の許可なく、インターネット上のサービス、たとえば、ファイル共有サイトやファイル交換サイトを通じて、他社とファイルを送受信するサービスなどを利用してはならない。

4. 5. 4 アクセス制御された Web サイトの閲覧に関して

- (1) 職員、パスワードによってアクセス制御された Web サイトの閲覧において、パスワードを Web ブラウザに記憶させる設定を行ってはならない。
- (2) 職員、アクセス制御された社内 Web サイトの閲覧時に離席、または閲覧しなくなった場合は必ず、Web ブラウザを終了させるか、OS のパスワード 付スクリーンロックを実施しなければならない。

4. 5. 5 Web サイトの閲覧許可

- (1) URL フィルタリングにより業務上必要とされるサイトが閲覧できない場合、利用者は、担当者に申請し、許可を得た場合のみ、閲覧できるものとする。

4. 6 ネットワークの利用

4. 6. 1 施設内ネットワーク及びインターネットの業務目的以外の利用禁止

- (1) 施設内ネットワークは、会社の情報資産であり、電子メールやWebサイトの利用などにおいて、業務目的以外の使用を禁止する。インターネットの利用についても同様である。
- (2) 管理責任者の許可無く、社内ネットワーク上に、電子メールサーバや、Webサーバ、FTPサーバなどを構築してはならない。
- (3) 他人の利用者IDを用いて、施設内ネットワーク及び、施設外のネットワーク、インターネット上のサイトへアクセスしてはならない。
- (4) 職員、故意もしくは不注意を問わず、施設内ネットワーク及び社外ネットワーク、インターネット上のサーバに対して、許可されたアクセス権限以上のアクセスを行ってはならない。

4. 6. 2 社内ネットワークで利用可能なサービス

- (1) 業務システム（人事、経営、経理、交通費管理、受発注システム、イントラネットサーバなど）へのアクセスは、許可された利用者以外利用してはならない。
- (2) 機密情報をネットワークを介して扱う場合は、管理責任者の指示に従い、暗号化電子署名などの処置を施さなければならない。
- (3) 職員、施設内ネットワークにおいて、ネットワークモニターなどの、ネットワーク上を流れるパケットを盗聴できる機器及びソフトウェアを使用してはならない。
- (4) 利用者は、施設内ネットワークサーバへのアクセス用のID及びパスワード、証明書は適切に管理しなければならない。

4. 6. 3 施設内ネットワークへの接続時の注意事項

- (1) 自宅や、他組織のネットワークに接続していたPCは、マルウェア対策ソフトを用いて、最新の定義ファイルによりマルウェアチェックを実施し、異常が発見されなかったことを担当者が確認した後でなければ、施設内ネットワークに接続してはならない。
- (2) 職員は、IPアドレスが固定の環境である施設内ネットワークの場合、与えられたIPアドレス以外のIPアドレスを使用してはならない。
- (3) 職員は、施設内ネットワークに接続中のPCを、管理責任者の許可の無いADSL回線、携帯電話、無線LAN（公衆Wi-Fiスポットなど）、専用線などを利用して、社

外のネットワークに接続してはならない。

4. 7 リモートアクセスサービス利用時のセキュリティ対策

4. 7. 1 利用申請

- (1) 業務上リモートアクセスサービスの利用が必要な者は、所属長の承認を得、管理責任者に申請しなければならない。

4. 7. 2 使用機器に関する遵守事項

- (1) 職員は、施設外から施設内ネットワークへのアクセスにおいて、担当者が指定した機器を利用しなければならない。
- (2) 職員は、インターネットから施設内ネットワークへの接続手段を、管理責任者の許可を得ることなく設置してはならない。
- (3) その他施設内LAN環境への接続にあたり、利用機器は、本規程に基づいて設定されなければならない。
- (4) リモートアクセスで使用するPCは、盗難に遭わない様に、また紛失しない様に、職員が管理を行わなければならない。

4. 7. 3 物理セキュリティ遵守事項

- (1) リモートアクセスで使用するPCやWi-Fiルーターは、所有者の目に届く範囲内で管理できるようにし、使用しない時には、セキュリティが確保できる場所に保管しなければならない。

5 運用確認事項

- (1) 施設内で実施される教育の内容を理解する。
- (2) メール及びインターネット利用時のリスクを理解する。
- (3) 施設外に情報を持ち出す場合は、その重要度を認識し、適切な管理策が取られていることを確認する。
- (4) PCの利用時、マルウェア対策、媒体管理等各種設定および設定が、正しく実施されていることを確認する。

6 例外事項

業務都合等により本規程の遵守事項を守れない状況が発生した場合は、担当者に報告し、例外の適用承認を受けなければならない。

7 罰則事項

本規程の遵守事項に違反した者は、その違反内容によっては罰則を課せられる場合がある。罰則の適用については賞罰委員会に従う。

8 公開事項

本規程は対象者にのみ公開するものとする。

9 改訂

- ・本規程は、令和 6 年 8 月 16 日に個人情報保護委員会によって承認され、令和 6 年 9 月 1 日より施行する。
- ・本規程の変更を求める者は、個人情報保護委員会に申請しなければならない。個人情報保護委員会は申請内容を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。
- ・本規程は、定期的（年 1 回）に内容の適切性を審議し、変更が必要であると認められた場合には速やかに変更し、その変更内容をすべての対象者に通知しなければならない。