介護事業所における情報安全管理の手引き

概要版

令和６年度厚生労働科学研究費補助金「介護事業所における情報の安全管理に関するガイドライン（案）作成のための調査研究」研究班（代表　三浦久幸）

令和７年３月

「介護事業所における情報安全管理の手引き」について

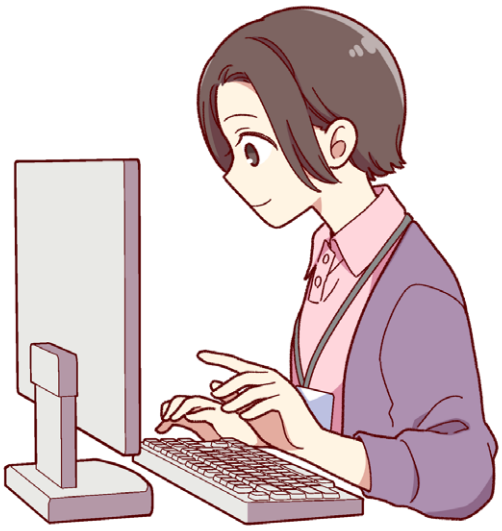
情報通信技術（ICT）が進み、介護現場においても電子機器を使用する場面が増えています。一方、介護においては利用者らの個人情報を多く使用し、情報漏えいを起こさないよう十分注意しなくてはいけません。

この「介護事業所における情報安全管理の手引き」は、介護事業所の職員および管理者の方を対象としたものです。介護事業所における情報安全管理については既に、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」（厚生労働省）などでまとめられていますが、この手引きは特に、ICT を得意としない方に、理解をいただきやすいよう作成しています。

この手引きは、概要版と解説編の２つで構成しています。概要版では情報の安全管理のため、知っておかなくてはいけないこと、行わなくてはいけないことについて、前半で全職員を対象に、後半に管理者を対象として、まとめています。

前半および後半とも、必要な対策を示した後、チェックリストを示しています。まず対策の概要を理解した上で、実践できているかをご確認ください。詳細は解説編をご覧ください。解説編は、背景や応用的、発展的な対策など、概要編で示す以外の内容も含めています。

概要編で示すチェック項目のうち、すべての対策を適切に行うことができていない方、事業所も多いかと思われますが、できていない項目について対策を進め、定期的に確認し、情報漏えい事故が生じないよう、安全管理対策を進めていきましょう。



情報安全管理の確認手順

介護事業所にて情報を安全に管理するため、次の手順で対策を検討、確認します。

1 個人情報の理解と管理

個人情報および要配慮個人情報の理解
情報の所在の把握
個人端末への保存禁止　等

2 電子端末の物理的な管理

端末の持ち出し制限、落下や盗難の予防
持ち出し端末の管理
外部記憶媒体の利用制限　等

3 ログイン・ログオフの管理

端末やソフトウェアにログイン時の個人認証
自動ログオフ、ログ管理　等

4 記録・入力

記録内容の適正化
情報の正確性と最新性の維持　等

5 外部とのメールなどの利用

インターネットや電子メールなど利用の制限　等

6 業務外の使用の制限

インターネットや電子メールなど私的利用の制限　等

7 組織的な管理体制の整備（管理者が行うこと）

情報システム安全管理責任者の選任や、方針規程やマニュアルの整備
端末およびアカウントの管理
入職時および定期的な研修　　等

第１部　全職員が知っておくべきこと・行うこと

１．個人情報の理解と管理

個人情報とは、氏名、生年月日、住所、顔写真など、特定の個人を識別できる情報を指し、介護事業所では、利用者や家族の個人情報を多く扱います。介護記録のように整理された情報だけでなく、メモや会話の中で出てくるような、個人につながる情報も含まれます。

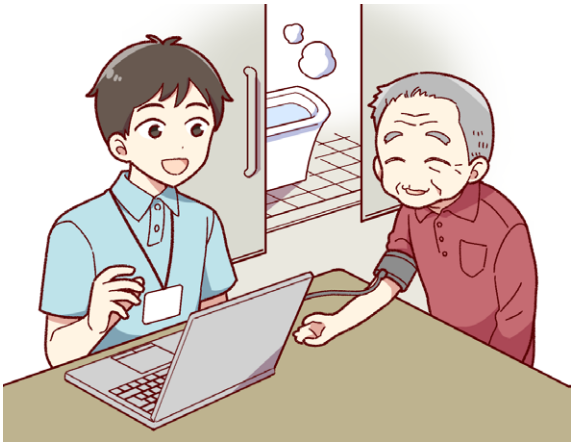
また、病状や治療、障害など、不当な差別や偏見その他の不利益が生じないようにその取扱いに特に注意して扱うべき情報は「要配慮個人情報」に該当します。介護事業所において扱うほとんどの情報は要配慮個人情報であり、一層慎重な管理が求められます。万一、要配慮個人情報が外部に漏れてしまった場合、個人情報保護委員会に報告するとともに、本人に知らせる必要があります。

個人情報は、管理者だけでなく、非常勤職員を含めたすべての職員はもちろん、送迎や清掃などの委託業者にも同様に、適切な管理が求められます。

また、個人情報を扱う仕組み自体も個人情報を扱う上で注意が必要です。重要書類のありか、システムの接続方法、ID パスワードも個人情報を守る上で重要です。

2．電子端末の物理的な管理

まず個人情報を含む電子端末はどれか、把握しておく必要があります。



- 介護ソフトを使用しているパソコンやタブレットは、個人情報が含まれています。
- 介護ソフトを使わなくても、送迎表や連絡帳などを扱う端末は、個人情報が含まれています。
- 個人情報は、事業所が管理し、セキュリティ対策を施した端末でのみ使用します。
- 業務に、職員個人のスマートフォンやパソコンなどの端末を利用することは避けます。
- どうしても職員個人の端末を使用する必要がある場合は、十分なセキュリティ対策を講じ、管理者の許可を得てください。

個人情報を含む端末や個人情報を含むシステムに接続する端末は、紛失や盗難、き損が生じないよう十分注意します。

- パソコンはできるだけワイヤーなどで物理的に固定し、盗難を防止しましょう。
- タブレット等のモバイル端末は、いつも目が届く場所に置き、盗難に注意してください。
- 端末は机の上などに置きっぱなしにせず、鍵のかかる棚など、安全な場所に保管します。
- 事業所に誰もいなくなる時は、確実に施錠します。
- 電子機器を事業所の外に持ち出す必要がある場合、管理者の許可を得てください。持ち出す場合は特に、紛失したり、置き引きにあったりしないよう、十分な注意が必要です。
- USB メモリや外付 HDD などの外部記憶機器の利用は、原則として使用せず、業務上、どうしても外部記憶機器が必要な場合、管理者の許可を得ます。

3．ログイン・ログオフの管理

- パソコンやタブレット等の端末を使う時は、ID とパスワード、または指紋や顔認証等の生体認証を使ってログインします。
- ID とパスワードは、一人一人が自分専用のものを使います。複数人で同じ ID・パスワードを共有することは避けてください。
- パスワードを付箋など、他の人の目に触れる方法で管理するのは避けてください。
- パスワードは、長く、複雑で、推測困難なものが推奨されます。推測されにくい強固なものを設定し、使い回さないようにしましょう。
- スマートフォンなどのモバイル端末を使う場合、画面ロックを設定します。
- 万一、端末が紛失や盗難にあっても、システムにアクセスされないよう、ID・パスワードを自動記憶させてはいけません。

4．記録・入力

- パソコンから離れる時は、関係のない人に画面を見られたり、操作されたりしないよう、ロックをかけます。

5．外部とのメールなどの利用

- メールやチャット等で情報を共有する際は、誤送信を防ぐため、宛先を十分に確認します。
- 誤送信を防ぐためには、あらかじめ登録したアドレス帳を使う、または組織外のアドレスに送る際、確認メッセージが表示されるよう設定する方法があります。アドレス帳は定期的に見直しを行ってください。

- 重要な情報は、メール本文に直接書くのではなく、添付するファイルに書いてパスワードで保護する方法がより安全です。
- 電子メールに添付ファイルや本文中の URL リンクからウイルスに感染する等の事故を生じないよう、送信元や内容に不審な点がないか、常に確認してください。
- 受信した電子メールに記載された URL リンクを安易にクリックしないでください。不正な WEB サイトに誘導される可能性があります。
- 受信した添付ファイルを開け、ウイルス感染等を生じてしまう場合もあり、添付ファイルの開封は慎重に行います。
- 特に、安全が確認できないプログラムは、絶対にダウンロードせず、ファイルも開封してはいけません。
- 「怪しいと思ったら開かない、クリックしない」という意識の徹底が重要です。
- 業務用の SNS、メーリングリストで情報共有を行う時、共有が不要な人、共有されたくない人が含まれていないことも理解しましょう。
- 公衆無線 LAN は業務における使用を控えます。

6．業務外の使用の制限

- 業務用端末を使って、SNS やネットショッピング、動画閲覧など、業務に関係のない目的でインターネットを利用することは控えましょう。

情報の安全管理に関するチェックリスト（全ての職員）

1．個人情報の理解と管理

- □ 介護事業所で扱う情報の多くは要配慮個人情報に該当し、特に慎重な管理が必要である。

2．電子端末の物理的な管理

- □ 個人情報を含む機器がどれかを把握している。
- □ 個人情報は、事業所が管理し、セキュリティ対策を施した端末でのみ使用する。
- □ 業務に、職員個人のスマートフォンやパソコンなどの端末を利用することは避ける。どうしても個人の端末を使用する必要がある場合は、管理者の許可を得る。
- □ 個人情報を含む端末は、紛失や盗難、き損が生じないよう十分注意している。
- □ 事業所に誰もいなくなる時は、確実に施錠している。
- □ 個人情報を含む端末を、許可なく事業所外に持ち出すことはない。
- □ USB メモリ等の外部機器を、許可なく端末に接続していない。

3．ログイン・ログオフの管理

- □ パソコンやタブレット等の端末を起動する際は、ID とパスワード、または生体認証を使ってログインしている。
- □ ID とパスワードは、一人一人が自分専用のものを使っている。
- □ 他の人が簡単に見ることができる場所に、パスワードを書いたメモや付箋を置いていない。

4．記録・入力

- □ 離席時に画面の覗き見や不正操作ができないように設定している。

5．外部とのメールなどの利用

- □ メールや FAX の宛先の十分な確認を徹底し、送信ミスを防止する。
- □ 誤送信を防ぐため、あらかじめ登録したアドレス帳を使っている。または組織外のアドレスに送る際、確認メッセージが表示されるよう設定している。
- □ 重要情報はメール本文に記載せず、パスワード保護した添付ファイルに記載している。
- □ 電子メールに添付ファイルや本文中の URL リンクからウイルスに感染する等の事故を生じないよう、送信元や内容に不審な点がないか、常に確認している。不審なプログラムやアプリのダウンロードを行わない。
- □ メールの URL リンクを不用意にクリックしないよう心がけている。
- □ 添付ファイルからウイルスに感染するリスクに注意し、開封は慎重に行っている。
- □ 公衆無線 LAN は業務で使用していない。

6．業務外の使用の制限

- □ 業務用端末を使って、業務に関係のない目的でインターネットを使っていない。

第２部　管理者や情報システム安全管理責任者が行うべき措置

介護事業所にて情報を安全に管理するためには、個人の注意や心がけだけではなく、組織としての体制が重要です。そのためには、ISMS（情報セキュリティマネジメントシステム）と呼ばれる枠組みに従い、「どんな危険があるか」「どうやって守るか」「リスク低減すること」を考え、常に改善に努めることが必要です。

事業所として講ずべき情報の安全管理措置の主なものとして、以下の６つが挙げられます。

１．組織的安全管理措置

- 情報システム安全管理責任者等を選任します。
- 個人情報保護指針や個人情報取扱規程等を作り、運用します。
- 情報漏えい等が発生した緊急事態の連絡体制や対応等も規程に明記し、万一の時に迷わず行動できるよう備えます。
- インターネットがつながらない、機器が動作しないといったトラブルが発生した際に備え、対応手順や事業継続計画を事前に作成しておきましょう。

２．人的安全管理措置

- すべての職員の雇用時、契約書等の文書に個人情報保護に関する内容を明記し、厳守されることを取り交わします。
- 入職時、職員へ情報安全管理について説明や研修を行います。これは派遣職員を含め、すべての職員に対して実施します。
- 定期的に情報セキュリティ研修・指導を行い、職員の意識や理解を高めます。
- 災害時対応や漏えい時を想定した定期的な訓練も有効です。

３．物理的安全管理措置

- 個人情報を保管する電子機器がある部屋への入退室を管理し、不要な人が出入りしないよう対策を講じます。
- 機器の盗難などの防止策として、カメラの設置等を行います。
- パソコンなどの機器は固定して動かないようにし、安全な場所に保管します。
- 情報が記録された機器は鍵付きの場所に保管します。
- 端末の持ち出しや持ち込みは、持ち出し記録簿で管理します。
- 個人所有の持ち込みパソコンや外部記憶媒体等を事業所内のネットワークに接続することは禁止します。

４．技術的安全管理措置

- インターネットに接続するすべての電子端末には、必ずセキュリティソフトを使用し、コンピュータウイルスやマルウェアなどの脅威から機器を保護します。
- 定期的に OS やセキュリティソフト、介護ソフトを更新し、常に最新の状態に保ちます。

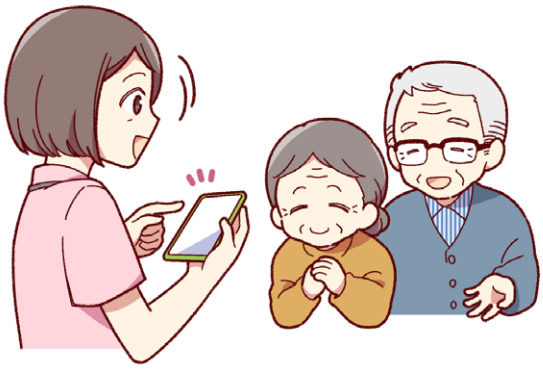
- パソコンやシステムへのアクセスは、適切な権限を設定、管理します。
- 職員ごとに固有のユーザー ID を割り当て、共有アカウントの使用は避けます。
- できるだけ指紋や顔認証などの生体認証を導入し、セキュリティを強化します。
- 権限は必要最小限に設定し、職務に応じたアクセス権限を付与します。
- 退職者のアカウントは速やかに無効化します。

- 一定時間操作がない場合、自動的にログアウトする機能を設定します。
- システムへのアクセス状況（ログイン、ログオフなど）を記録するログ機能を有効にし、定期的に確認して、不正アクセスや不審な操作がないか監視します。
- 個人情報を含まない端末でも、業務システムに接続する端末は、接続先やアクセス情報を記憶させない等、個人情報を含む端末同様に注意して扱います。

- 不要な通信は避け、よく使う外部サイトはお気に入り（ブックマーク）に登録するなどし、信頼できるサイトの利用を促します。
- 業務に関係のないサイトへのアクセスを制限します。フィルタリングソフトの利用も有効です。

- 重要なデータは定期的にバックアップします。
- 不要になったデータは、復元されないよう適切に処理してから、廃棄します。
- 外部から接続できるサーバーで稼働している不要なサービスや、管理する機器やシステムに存在する不要なユーザーアカウントは停止または削除します。

- 無線 LAN を安全に利用するためには、適切な暗号化方式を設定します。
- 情報漏えい防止のため、システムの使用状況を監視します。
- 私物のスマートフォンやタブレットの業務利用は、情報漏えいを生じるリスクが高く、原則として禁止します。業務でスマートフォンを利用する場合は、可能な限り業務専用端末を用意します。



5．外的環境の把握

- 情報システムが設置されている場所やその環境について把握し、安全性を確認します。
- 情報セキュリティに関する最新の脅威や対策に関する情報を日頃から収集、確認します。
- 介護ソフトベンダー社のセキュリティ対策を確認します。

6．委託先の監督

- システム運用やデータ処理などを外部業者に委託する場合は、その業者が適切なセキュリティ対策を行っているか確認して選定し、必要な契約書を交わします。
- 委託契約において、委託先が定める安全管理措置の内容を契約に盛り込み、委託先の義務とするほか、業務が適切に行われていることを定期的に確認します。
- 情報安全管理措置を正しく行い、委託業務がなされているか、定期的に監査を行います。

セキュリティ対策を進める際には、管理者や介護事業所の職員がすべてを抱え込む必要はありません。専門知識を持つ介護ソフトベンダー社の技術者など専門家から、必要に応じて情報を収集したり、支援を受けたりすることが効果的です。また、いざというときにすぐ相談できるように、信頼できるベンダーを日頃から確保しておくことも大切です。こうした専門家の力を借りることで、安全で効果的な運営が可能になります。

万一、要配慮個人情報が含まれる個人データ等の漏えい、滅失、毀損その他の個人データの安全の確保に係る事態が生じたときは、個人情報保護委員会に報告するとともに、本人への通知を行わなければいけません。詳細は個人情報保護委員会の WEB サイトをご覧ください。

個人情報保護委員会　https://www.ppc.go.jp/personalinfo/legal/leakAction/

情報の安全管理に関するチェックリスト（管理者用）

1．組織的安全管理措置

- □ 情報セキュリティ責任者の選任 ：情報セキュリティに関する責任者を明確に定め、権限と責任を与えている。
- □ 個人情報保護指針や個人情報取扱規程等を作り、運用している。
- □ 機器が動作しない等トラブル時に備えた対応手順や事業継続計画を作成している。

2．人的安全管理措置

- □ 全職員と、個人情報保護に関する内容を明記し、厳守されることを取り交わした契約を締結している。
- □ 入職時、派遣職員を含め職員へ情報安全管理について説明や研修を行っている。
- □ 定期的に情報セキュリティ研修・指導を行っている。
- □ 情報セキュリティインシデントが発生した場合の手順を定め、訓練を実施している。

3．物理的安全管理措置

- □ 電子機器がある部屋への入退室を管理し、不要な人が出入りしないよう対策を講じている。
- □ パソコンなどの機器は固定して動かないようにし、安全な場所に保管している。
- □ 情報が記録された機器は鍵付きの場所に保管している。
- □ 端末の持ち出しや持ち込みは、持ち出し記録簿で管理している。
- □ 個人所有のパソコンや外部記憶媒体等をネットワークに接続することを禁止している。

4．技術的安全管理措置

- □ インターネットに接続するすべての電子端末には、必ずセキュリティソフトを使用している。
- □ 定期的に OS やセキュリティソフト、介護ソフトを更新し、常に最新の状態に保っている。
- □ パソコンやシステムへのアクセスは、職員ごとに固有のユーザー ID を割り当て、適切な権限を設定、管理している。
- □ 複数名で共有するアカウントは使用していない。
- □ 指紋や顔認証などの生体認証を導入している。
- □ 退職者のアカウントはすべて無効化している。

- [ ] 一定時間操作がない場合、自動的にログアウトする機能を設定している。
- [ ] システムへのアクセス状況（ログイン、ログオフなど）を記録するログ機能を有効にし、定期的に確認して、不正アクセスや不審な操作がないか監視している。

- [ ] よく使う外部サイトはお気に入り（ブックマーク）に登録するなどしている。
- [ ] 業務に関係のないサイトへのアクセスを制限している。

- [ ] 重要なデータは定期的にバックアップしている。
- [ ] 不要になったデータは、復元されないよう適切に処理してから、廃棄している。
- [ ] 不要なサービスやユーザーアカウントは停止または削除している。

- [ ] 無線 LAN を安全に利用するため、適切な暗号化方式を設定している。
- [ ] 情報漏えい防止のため、システムの使用状況を監視している。
- [ ] 私物のスマートフォンやタブレットの業務利用は、原則として禁止している。

５．外的環境の把握

- [ ] 情報システムが設置されている場所やその環境について把握し、安全性を確認している。
- [ ] 情報セキュリティに関する最新の脅威や対策に関する情報を日頃から収集、確認している。
- [ ] 介護ソフトベンダー社のセキュリティ対策を確認している。

６．委託先の監督

- [ ] システム運用やデータ処理などを外部業者に委託する場合は、その業者が適切なセキュリティ対策を行っているか確認して選定し、必要な契約書を交わしている。
- [ ] 委託先が定める安全管理措置の内容を契約に盛り込み、委託先の義務として、業務が適切に行われていることを定期的に確認している。

参考文献等

■ 個人情報の保護に関する法律
（平成 15 年 5 月 30 日施行）

■ 個人情報の適正な取扱いのための研修資料（個人情報保護委員会）

■ 医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス
（平成 29 年 4 月 14 日通知、令和 6 年 12 月 2 日最終改定）

■「医療･介護関係事業者における個人情報の適切な取扱いのためのガイダンス」に関するQ&A（事例集）
（令和 6 年 12 月 2 日改正）

■ 医療情報システムの安全管理に関するガイドライン
（令和 5 年 5 月 31 日改正）

■ 地域医療情報連携ネットワークにおける同意取得方法の例について（事務連絡）
（令和 2 年 3 月 31 日）

発　行

令和６年度厚生労働科学研究費補助金「介護事業所における情報の
安全管理に関するガイドライン（案）作成のための調査研究」研究班

代表　国立長寿医療研究センター　三浦久幸

〒474-8511 愛知県大府市森岡町 7-430

介護事業所における情報安全管理の手引き
（解説編）

令和７年３月

令和６年度厚生労働科学研究費補助金「介護事業所における情報の安全管理に関する
ガイドライン（案）作成のための調査研究」研究班（代表　三浦久幸）

目次

１．はじめに

質の高い介護サービスを効率的に提供するためには、情報通信技術（Information and Communication Technology, 以後ICT）を上手に利用することが重要です。ICTを活用することによって、転記など手作業で記録する負担を軽くし、保管する紙の量を減らし、データ連携や情報共有によって介護サービスの質や利用者満足度の向上につなげることができます。厚生労働省においては、ケアプランデータ連携システムが開始され、介護情報基盤の構築が進められ、介護の質の向上、生産性向上が進められているところですが、パソコンなどの電子端末で適切な情報の安全管理を行わないと、大量の個人情報が漏えいしたり、不正に利用される危険があり、介護事業所における情報の安全管理は極めて重要です。

個人情報保護委員会によると、令和６年度上半期で個人データの漏えい等は7,735件報告されていますが、医療分野ではたびたび情報漏出事故やサイバー攻撃が発生している中、介護サービスにおいても情報の安全管理が求められています。特に介護では、病歴だけでなく、生活歴、人間関係、経済的状況、宗教観、さらには虐待に関する情報など、極めて機微な個人情報を扱うことが多いため、その保護には細心の注意を払わなければなりません。今や情報の安全管理は、介護従事者に必須の事項となっています。

情報を適切に管理するための基本は「情報の確かな保存」「情報の質の保証」「個人情報の保護」です。情報の確かな保存とは、介護記録やケアプランなど、必要な情報がいつでも取り出せて、情報が失われないよう適切に保管する必要があります。情報の質の保証とは、記録された情報が正確で信頼できるものであることで、常に最新かつ正確な情報を維持する必要があります。個人情報の保護とは、機微な情報が外部に漏れたり、不正にアクセスされたりしないよう防御することです。

また、組織が情報資産を適切に管理し、機密性・完全性・可用性を維持するための包括的な管理の仕組みを情報セキュリティマネジメントシステム（ISMS：Information Security Management System）と言います。ISMSは、単なる技術的対策だけでなく、組織の方針、手順、プロセス、責任体制を含む総合的な管理体系です。

この「介護事業所における情報安全管理の手引き」は、これら情報の安全管理のため、重要なポイントを簡単に、わかりやすく示しています。この手引きが介護の質向上に役立つことを切に願っています。

令和６年度厚生労働科学研究費補助金「介護事業所における情報の安全管理に関するガイドライン（案）作成のための調査研究」研究班　代表　三浦久幸

２．「介護事業所における情報安全管理の手引き」について

介護現場における情報の安全管理については、「個人情報の保護に関する法律」（以後、個人情報保護法）の他、厚生労働省から「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」およびQ&A（事例集）、「医療情報システムの安全管理に関するガイドライン第6.0版」などが公表されています。これらは厚生労働省のWEBサイト※に分かりやすくまとめられています。

※厚生労働分野における個人情報の適切な取扱いのためのガイドライン等
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000027272.html

情報安全管理に関しては複雑な事項が多い一方、介護現場ではICTを得意としない方も多く、この「介護事業所における情報安全管理の手引き」（以後、本手引き）は、介護事業所の理解していただきやすいよう作成しています。

本手引きは、概要版と解説編の２つで構成しています。概要版では情報の安全管理のため、知っておかなくてはいけないこと、行わなくてはいけないことについてまとめ、この解説編では、背景や応用的、発展的な対策などを加え、詳述しています。

本手引きを参考にして、情報管理における危険（リスク）を把握し、それぞれについて対策を講じながら、新しい安全管理に関する情報にも接し、日々の安全管理対策を進めてください。

３．個人情報について

３-1 個人情報と要配慮個人情報

「個人情報」とは、生存する個人に関する情報で、氏名、生年月日、住所、顔写真などにより特定の個人を識別できる情報を指します。介護サービス計画、利用者の状態に関する記録、家族構成なども個人情報にあたります。介護記録のように整理された情報だけでなく、メモや会話の中で出てくるような、個人につながる情報も含まれます、個人に紐づく情報は広く、「個人情報」にあたると考えるのが適切です。

＜介護事業所における個人情報の例＞
・利用者の基本情報（氏名、住所、生年月日、連絡先など）
・家族等の氏名や連絡先
・介護保険被保険者番号
・介護記録に記載された利用者を識別できる情報
・職員の個人情報（氏名、住所、連絡先など）

「要配慮個人情報」とは、不当な差別や偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報を指します。要配慮個人情報は以下などの事項が該当し、介護事業所において扱うほとんどの情報は要配慮個人情報であり、一層慎重な管理が求められます。

・診療録等の診療記録
・介護関係記録に記載された病歴
・患者の身体状況
・病状
・治療
・診療情報や調剤情報
・健康診断の結果
・保健指導の内容
・障害（身体障害、知的障害、精神障害等）

個人情報は、管理者だけでなく、非常勤職員を含めたすべての職員はもちろん、送迎や清掃などの委託業者にも同様に、適切な管理が求められます。

３-2.　個人情報の取り扱い

個人情報は、以下の事項に従い、注意深く管理します。

①利用目的や管理方法を明示し同意を得る

個人情報を扱う際には、その利用目的を契約書に明記して利用者に示し、同意書も得ることが望まれます。収集した個人情報は、本来の介護目的以外に使われてはいけません。例えば、営業活動に流用したり、関係のない第三者に提供したりすることは許されません。

また、利用者が自分の情報がどのように収集され、扱われているかについて知り、安心できることも求められます。情報の取り扱いルールを明確にし、それを実践していることを利用者に示す必要があります。

②適正な取得と内容の正確性を保つ

個人情報は正しい方法で集め、正確な内容で管理します。

③安全管理措置を徹底する

利用者の情報が外部に漏えいしないよう細心の注意が必要です。情報漏えいや紛失を防ぐため、以下のような対策を講じます。

- 組織的対策: 責任者を決めて管理体制を整える。
- 人的対策: 職員に個人情報保護の教育を行う。
- 物理的対策: 書類や端末を施錠できる場所に保管する。
- 技術的対策: 不正アクセス防止のためのセキュリティソフト導入やアクセス制限。
- 外的環境の把握：介護ソフトベンダー社のセキュリティ対策やサイバー攻撃のトレンドを把握する。
- 委託先の監督：委託契約の締結や定期的な点検・監査を行う。

④第三者提供の制限

個人情報は原則として、本人の同意がない限り第三者に勝手に提供してはいけません。提供が必要な場合は、内容や範囲をきちんと説明し、了承を得ることが重要です。

⑤本人からの請求への対応

利用者から情報の開示や訂正、利用停止などの請求があった場合は、迅速かつ適切に対応します。ただし、開示によって利用者や家族に不利益が生じる場合には、例外的に対応を要さないこともありえますが、その際は理由を示し、丁寧に説明します。

⑥透明性と苦情対応

個人情報の取り扱いについて公開し、利用者からの苦情に迅速かつ丁寧に対応する窓口を設置します。関係機関とも連携し、相談対応体制を整備します。

3-3. 委託事業者による個人情報の取り扱い

介護事業所が外部の事業者又は個人に仕事を頼む場合、その委託先も個人情報を大切に扱う必要があります。例えば、送迎や食事作り、掃除、金銭の管理を頼む場合などです。

介護事業所は、委託先を選ぶ時に、個人情報をきちんと守ることができる委託先かどうかを確認しなければなりません。そして、委託後も、その委託先が個人情報を正しく扱っているか、時々チェックする必要があります。委託契約においては、以下などの個人情報の事項も明記する必要があります。

- 個人情報をどのように守るか
- 個人情報を外部に漏らしてはいけないこと
- 介護事業所がどのように確認するか
- 委託終了後の個人情報の廃棄

3-4. 個人情報を扱う仕組

また、個人情報を扱う仕組み自体も個人情報を扱う上で注意が必要です。重要書類のありか、システムの接続方法、IDパスワードも個人情報を守る上で重要です。

４．情報の安全管理の考え方

紙で情報管理を行う場合に比べ、ICT製品やソフトウェアを利用することで、個人情報が一元的に集約されることとなり、個人情報の漏えいや滅失、き損が発生した場合、利用者に与える権利利益の損害は、より大きくなります。よって、安全管理のための組織的、人的、物理的、及び技術的安全管理措置を一層強化することが求められます。

情報を安全に管理する仕組みは、ISMS（情報セキュリティマネジメントシステム）と呼ばれます。サイバーセキュリティの基本は、情報を管理するための知識と方法です。

4-1. 情報の適切な管理

情報の適切な管理は、「情報の確かな保存」、「情報の質の保証」、「個人情報の保護」の主に三つの要素から成り立っています。これら3つのことをバランスよく行うことで、情報を適切に管理できます。

4-1-1. 情報の確かな保存

介護事業所での情報保存は単なるデータ蓄積ではなく、利用者の生活を支える重要な基盤です。大切な情報をしっかり守り、いつでも使えるようにしましょう。次の基本的な対策を日々の業務に取り入れることで、利用者さんの大切な情報を守り、質の高い介護サービスを続けることができます。

①破壊されない

ここでいう「破壊」とは、悪意ある攻撃によってデータの漏えいや改ざん等が生じることを指します。これらのリスクを回避するためにも、適切なセキュリティ対策を講じることが重要です。パソコンのウイルス対策ソフトを最新に保ち、強いパスワードを設定しましょう。不審なメールは開かず、管理者が不明なUSBメモリ等の外部機器は使用を控えます。

②劣化しない

データは正しい形式で保存し、定期的に内容を確認しましょう。紙の記録は湿気や日光の当たらない場所に保管し、長期間読める状態を保ちましょう。

③復旧できる

大切な情報は定期的にバックアップを取り、別の場所にも保管しましょう。たとえパソコンが不調になってしまっても、ウイルス感染してしまっても、データを復旧できるよう備えておくと安心です。

④モノとしての安心

情報を保存する機器は定期的に点検し、安全な場所に設置しましょう。誰でも触れる場所に

記録を置かず、情報の保管場所自体の安全確保にも留意してください。また、システムの不具合やランサムウェア等によるデータ破壊に備え、定期的に外部記憶媒体等へバックアップを行うことが望まれます。

4-1-2．情報の質の保証

利用者に適切なケアを提供するには、情報そのものが信頼できるものでなくてはいけません。信頼できる情報とは、主に以下の4つを満たす必要があります。

①改ざんされていない

改ざんとは、情報が途中で不正に変更されることです。その日のケア内容を記録された記載が、後日、または記録者以外の者によって、不適切に変更されてはいけません。もし変更される場合、その変更履歴（ログ）が残される必要があります。アクセス制限や編集履歴の管理で、記録の正確さを守ります。

②偽情報ではない

正確な情報源から得た情報を使うようにしましょう。利用者の言動を、自分で見る、又は聞いたのではなく、他の職員から間接的に聞いた場合などは、その旨を記載します。また、インターネット上の出所不明な健康情報や、確認されていない噂などに基づき、誤った記載を行わないよう注意します。

③原本であること

利用者や家族から署名をいただいた文書等は、コピーではなく、原本を正しく保管します。

④内容としての安心

当たり前のことですが、扱う情報は、介護に役立つ内容である必要があります。介護のための情報だから、信頼して扱うことができるのであって、介護に関係しない情報をむやみに集め扱うのは適切ではありません。信頼感を持って個人情報を扱うことを利用者に許していただき、安心してケアを受けていただけるようにしましょう。

4-1-３．個人情報の保護

①情報漏えいを防ぐ

利用者らの個人情報が外部に漏えいしないよう、常に細心の注意を払う必要があります。悪意がなくても、利用者の様子を近所の人に知らせる、親戚からの問合せに勝手に答えることも漏えいにあたる場合があります。当然、利用者の個人情報をSNSなどで勝手に公開したり、外部の人に送ったりしてはいけません。

②不適切な用途に利用されない

販売業者らに名簿等の個人情報を売ったり渡したりすることは決して許されません。その

他、介護に関係しない用途に個人情報を利用してはいけません。

③合意により利活用

個人情報は本人または本人を代理する家族らとの合意に基づき、利活用されるものです。その合意なく勝手に使うことは許されません。

④使い方の安心

利用者の個人情報は介護等のために使われるものであって、個人情報の扱いについて利用ら者に説明する通り、ルールを守って利用します。個人情報の使い方に信頼が得られないと、介護サービスを安心して使っていただくことも難しくなります。

4-２．セキュリティに対する意識

セキュリティについては「完全な安全はない」と意識することが必要です。どんなに対策を講じても、完全にリスクをなくすことはできません。たとえ、ICTを専門とした委託先を頼むことができても、高額の通信環境や端末、介護ソフトを備えたとしても、リスクをゼロにすることはできません。

効果的なセキュリティのためには、利用者の個人情報など、守るべき情報の範囲を明確にし、どんな危険にさらされているかを理解することが大切です。誰が情報を守る責任を持つのかを決め、様々な対策を組み合わせて守る仕組みを作ります。そして、情報の価値に見合った適切な労力とコストをかける必要があります。

完璧を目指すのではなく、リスクを理解した上で、現実的に対策を講じ継続的に改善していきます。

4-３．外部リスク

情報システムは、日々さまざまな危険（リスク）にさらされています。

まず、最も基本的なリスクは、パソコンやサーバーの故障です。これらが壊れると、長年集めてきた利用者の大切な情報が一瞬で失われてしまうかもしれません。また、水害や火事といった災害も、建物だけでなく情報システム全体を壊してしまう恐れがあります。

次に、特に注意が必要なのは、コンピュータウイルスやランサムウェア、ワームなど、不正なソフトフェアを指す「マルウェア」です。ウイルスに感染すると、利用者の情報が変えられたり消えたりして、適切なケアができなくなる可能性があります。近年、増えているランサムウェアというマルウェアは特に危険で、一度感染するとデータを人質に取られ、多額のお金を要求される場合があります。

情報が外部に漏れることも深刻な問題です。利用者の介護記録や身体の状態、家族の情報、お金の状況といった大切な情報は、一度漏れると取り返しがつきません。こうした情報が悪い人の手に渡ると、詐欺などの犯罪に使われてしまう可能性もあります。

これらの危険がシステムに入り込む道筋はさまざまです。例えば、職員が自宅から持ってき

たUSBメモリや、私物のスマートフォンを使うことで、ウイルスが広がることがあります。また、古いシステムや、パスワードが簡単なままの機器も、攻撃されやすい弱点となります。

本物そっくりの偽のメールも増えています。厚生労働省や自治体からの連絡を装ったメールに騙されて、リンクをクリックしたり添付ファイルを開いたりすると、ウイルスに感染してしまう場合があります。

これらの危険から身を守るためには、定期的に情報のコピー（バックアップ）を取ることが大切です。また、職員それぞれの役割に応じて、システムを使える範囲を適切に設定することも重要です。全ての職員に対して、情報を安全に扱うための教育を行うことも効果的です。

4-4．何を守るか

介護事業所は、多様なネットワークに接続し、大量の情報をやり取りしています。この環境下で、セキュリティ対策の出発点となるのは「守るべき情報」を明確にすることです。特に、介護ソフトに保存されている利用者の基本情報、介護記録、ケアプラン、アセスメント情報などは、最も重要な保護対象です。これらの情報は、外部接続を通じて漏えいや改ざんのリスクに常にさらされています。

守るべき情報の範囲は多岐にわたります。納入・サービス企業間で交換されるサービス情報には、介護用品の発注や請求に関わる重要なデータが含まれており、適切な保護が必要です。また、他施設との連携が増える中で、利用者の入退所情報や他事業所への紹介、業務委託の場面でも、利用者情報が共有されるため、情報の流れをしっかり管理しなければなりません。

さらに、地域包括支援センターや居宅介護支援事業所、医療機関との連携では、ケアプランや利用者状況の情報交換が行われます。この情報には利用者の状態や個人情報が含まれるため、漏えいすれば深刻なプライバシー侵害につながります。また、ICTを活用した新しいサービスも広がっており、家族が自宅から利用者情報にアクセスする際のセキュリティ管理も重要な課題です。

また、リモートワークや働き方改革の進行に伴い、職員が自宅から事業所のシステムにアクセスする場合も増えています。このような遠隔接続は新たなリスクをもたらし、特別な注意が必要です。さらに、インターネットを通じた情報検索や請求事務なども日常的に行われており、ここで意図せず情報漏えいが起こるリスクもあります。

これらの多様な接続と情報の流れを把握し、何を最も重点的に守るべきかを明確にすることで、効果的なセキュリティ対策の優先順位を決めることができます。限られた資源で最大の効果を得るためには、守るべき情報の価値を見極めることが不可欠です。

4-5．どのように守るか

介護事業所の情報を守るためには、多層的な防御策が必要です。システムとネットワークの周りに「ガードマン」のような防御の層を設けることで、重要な情報を外部の脅威から保護します。

内部規律を徹底することは、システムやネットワークに対する基本的な防御策となります。

職員全員がセキュリティルールを理解し、日常業務の中で実践することが重要です。パスワード管理や画面のロック、情報の取り扱いルールなど、基本的な対策を確実に行うことで、内部からの情報漏えいを防ぎます。

外部媒体の接続をさせないことも重要な対策となります。USBメモリなどの外部記憶媒体は、ウイルス感染の主要な経路となります。必要な場合は、事前にウイルスチェックを行うなどのルールを設け、不必要な接続は禁止することが効果的です。

他の施設や機関との情報連携は日常的に行われ、サービス提供には必要なやり取りではありますが外部接続は適切に保護されている必要があります。VPNなどの安全な通信技術を使用し、認証を強化することで、外部との接続を安全に保ちます。

機器の管理強化も欠かせません。パソコンやサーバー、ネットワーク機器などは、常に最新のセキュリティ更新プログラムを適用し、適切な設定を行うことが重要です。古い機器や脆弱性のあるソフトウェアは、攻撃者に狙われやすいため、計画的な更新が必要です。

常時監視によって、異常な活動や不審なアクセスを早期に発見することができます。ログの定期的な確認やセキュリティ監視ツールの導入により、問題が大きくなる前に対処することが可能になります。

危険アクセスの禁止も重要な対策です。不審なウェブサイトへのアクセスや、業務に関係のないサイトの閲覧を制限することで、ウェブからの脅威を減らすことができます。フィルタリングツールの導入や、安全なブラウジングの教育が効果的です。

これらの対策をバランスよく組み合わせることで、強固なセキュリティ体制を構築することができます。

５．情報の安全管理のための組織体制と基本方針

情報を安全に管理するためには、個人の注意や心がけだけではなく、組織としての体制が重要です。そのためには、ISMSに従い、「どんな危険があるか」「どうやって守るか」「リスク低減すること」を考え、常に改善に努めることが必要です。「完全な安全はない」ことを認識し、被害を受けた場合にも速やかに復旧できる準備をしておくことが重要です。最も大切なのは、職員全員が情報管理の重要性を意識し、基本的なセキュリティ対策を理解して、日常的に実践することです。

5-1.安全管理体制

介護事業所では、利用者の情報を安全に守るため、組織全体で適切な仕組みを作り、職員がそのルールを守るよう指導する責任があります。しかし事業所の管理者がすべてを直接監督するのが難しいこともあり、その場合は情報システム安全管理責任者などを選任し、管理を行います。

情報システム安全管理責任者は、次の役割を担います。

- 情報をどのようなルールで管理・保護するかを考え、ルールを策定する
- 職員に対して、情報セキュリティに関する教育や訓練を行う
- 実際にそのルールが守られているかを確認する

5-２. 個人情報保護指針、取扱規則等の策定

介護事業所は、個人情報を守るための考え方や決まりを個人情報保護指針として、分かりやすい形で作る必要があります。指針には、主に次のことを含めます。

- 施設や事業所の目的に合致していること
- 情報セキュリティの目的や、その目的を決めるための枠組みを示すこと
- 法律や規則など、守るべき決まりを遵守するという約束
- 情報セキュリティの仕組み（ISMS）を継続的に改善していく意思

また、具体的な取り扱い方法を定めた個人情報取扱規程には、以下などを記載します。

- 個人情報を安全に管理する方法
  例：書類を鍵のかかる場所に保管することや、パソコンにパスワードをかける
- 利用者や家族が自分の情報を見たいと言った時の対応方法
  例：どんな手続きが必要か、どのくらいの期間で対応するか
- 他の人や会社に個人情報を渡す時のルール
  例：どんな場合に渡せるのか、本人の同意が必要かどうか
- 苦情があった時の対応方法
  例：誰が対応するのか、どのように解決するのか

そして、これらの指針や規程は、事業所に掲示板する、またはWEBサイトに掲載するなど行い、公表します。

5-3. 利用者窓口の設置

利用者や家族に対して、「個人情報を大切に扱っています」ということを明確に示すことも重要です。例えば、事業所の入り口に「個人情報保護責任者：○○」「相談窓口：△△」といった表示をすることで、利用者に安心感を与えることができます。利用者等から、本人の個人情報の取扱いについて問い合わせがあった場合には、当該規則に基づき、迅速に情報提供等、必要な措置を取ることが義務付けられています。なお個人情報に関する説明や相談窓口、情報開示を行う方法等については、障害のある人にも分かりやすく対応できるよう配慮する必要があります。

介護サービス情報公表システムでは、各事業所がこれらの取り組みをしているかどうかを公表しています。介護事業者は必要な情報をシステムに入力し、最新の情報に更新する責任があります。

- 利用者のプライバシーを守る取り組み
- 相談や苦情に対応する取り組み
- 個人情報を守る取り組み

６．情報安全管理の流れ

利用者の大切な個人情報を安全に守るために、「情報をどう扱うか」、「どうやって守るか」をあらかじめ決めておくことが大切です。情報安全管理の流れとして、次の7つのステップを示します。

① 個人情報の理解と管理
↓
②電子端末の物理的な管理
↓
③ ログイン・ログオフの管理
↓
④ 記録・入力
↓
⑤ 外部とのメールなどの利用
↓
⑥ 業務外の使用の制限
↓
（管理者が行うこと）
⑦ 組織的な管理体制の整備

６－1．個人情報の理解と管理

個人情報がどこに保存されているのかを把握します。介護ソフト、介護ソフトを使っていないパソコン、USBメモリ等の他、紙の書類もあるはずです。紙の書類は、施錠されたキャビネットに保管するなど、物理的な対策も重要です。

電子データについては、どの端末、またはサーバーやクラウドに保存されているのか、誰がアクセスできるのかを明確にしておきます。

- 介護ソフトを使用しているパソコンやタブレットは、個人情報が含まれています。
- 入力のみに使うタブレット等のモバイル端末も通常、個人情報が含まれています。
- 介護ソフトを使わなくても、送迎表や連絡帳などを扱う端末は、個人情報が含まれています。
- 保存またはコンピュータ間の移動のために使うUSBメモリ等の外部機器も、個人情報を含むかもしれません。「ファイルの削除」だけでは完全な消去にならず、個人情報が残っているかもしれません。

＜個人端末への保存禁止＞

- 個人情報は、事業所が管理し、セキュリティ対策を施した端末でのみ使用します。
- 業務に、職員個人のスマートフォンやパソコンなどの端末を利用することは避けます。個人の端末はセキュリティ対策が不十分な場合が多く、ウイルス感染や紛失・盗難による情報漏洩のリスクが高まります。
- どうしても職員個人の端末を使用する必要がある場合は、十分なセキュリティ対策を講じ、管理者の許可を得てください。

６－２．電子端末の物理的な管理

６－２－１．紛失や盗難、き損の予防

個人情報を含む端末や個人情報を含むシステムに接続する端末は、紛失や盗難、破損が生じないよう十分注意します。

- パソコンはできるだけワイヤーなどで物理的に固定し、盗難を防止しましょう。
- タブレット等のモバイル端末は、いつも目が届く場所に置き、盗難に注意してください。
- 端末は机の上などに置きっぱなしにせず、鍵のかかる棚など、安全な場所に保管します。
- 離席時には必ず端末をロックします。
- 事業所内の電子端末（パソコン、タブレット、スマートフォン等）は、原則として外部への持ち出しを禁止します。
- 電子機器を事業所の外に持ち出す必要がある場合、管理者の許可を得てください。持ち出す場合は特に、紛失したり、置き引きにあったりしないよう、十分に注意します。
- 事業所に誰もいなくなる時は、確実に施錠します。
- 電子機器を事業所の外に持ち出すことを許可する時は、持ち出し理由、持ち出し先、利用期間と、持ち出し者の責任範囲を明確にします。管理者は、持ち出す端末が、適切にセキュリティ対策（後述）が施されていることを確認します。
- 持ち出す端末については、持ち出し記録簿で管理します。
- パソコンなどは、定期的に清掃し、埃による故障を防ぎます。

６－２－２．外部記憶機器の利用制限

- USBメモリや外付HDDなどの外部記憶機器の利用は、原則として禁止します。
- 業務上、どうしても外部記憶機器が必要な場合は、管理者の許可を得ます。
- 管理者は、外部記憶機器の利用を許可する場合、以下を行います。
    - 利用目的を明確にする。
    - 利用する外部記憶機器を特定する。
    - ウイルスチェックを実施する。
    - 暗号化などのセキュリティ対策を施す。
- 外部記憶機器を利用する場合、以下の情報を記録した利用記録で管理します。
    - 利用目的
    - 利用する外部記憶機器の種類、識別番号
    - 利用期間

- ウイルスチェックの記録

- 外部記録機器の利用後は速やかにデータを消去し、適切に保管します。
- 所有者が不明の外部記憶媒体はパソコンに接続してはいけません。

６－３．ログイン・ログオフの管理

電子端末の利用においては、職員ごとにアクセス権限を適切に設定し、不要な情報へのアクセスを制限します。

- パソコンやタブレット等の端末を使う時は、IDとパスワード、または指紋や顔認証等の生体認証を使ってログインします。
- よりセキュリティを強化するためには、ID・パスワードに加えて、指紋認証やICカードなどの別の認証要素を組み合わせます。特に、重要な情報を取り扱うシステムや、外部からアクセスする場合には、多要素認証を導入することが望まれます。
- ID・パスワードは長く、複雑なものを設定してください。
- IDとパスワードは、一人一人が自分専用のものを使います。複数人で同じID・パスワードを共有することは避けてください。
- ID・パスワードは、システムごとに異なる設定がなされることが推奨されます。
- デバイスやシステムの初期パスワードや、管理者により発行された初期パスワードは、利用者本人によって必ず変更します。
- 生年月日、氏名など、第三者に推測されやすいパスワード設定は避けてください。
- パスワードを付箋など、他の人の目に触れる方法で管理するのは避けてください。
- パスワードは長く、複雑で、推測困難なものが推奨されます。推測されにくい強固なものを設定し、使い回さないようにしましょう。

〈危険なパスワードの例〉
- 12345678 (単純な羅列)
- pa$$w0rd、i234567&9（単純な置換や、社会に流出済と確認されているパスワード）
- qwerty、7410（キーボードの配列）
- 0101（生年月日）、ichiro（自分や事業所の名前）

〈強固なパスワードとは〉
-13 桁以上（桁数が多いほど、機械的な総当たりでの解析が困難）
-英数字、大文字・小文字、記号が混在（組み合わせが多いほど解析が困難）
-ランダムな文字列（単語等の組み合わせによる解析を回避）

- 万一、端末が紛失や盗難にあっても、システムにアクセスされないよう、ID・パスワードを自動記憶させてはいけません。

- スマートフォンなどのモバイル端末を使う場合、画面ロックを設定します。

- また、ゴミ箱に捨てられた機密情報を盗む、人のパスワードを覗き見る、関係者を語りパスワードを聞き出したりするなどの情報窃取行為（ソーシャルエンジニアリング）に注意します。アカウントハイジャックに遭い、知らないうちに勝手に不正行為に使われるということがないよう、注意が必要です。

６－４．記録・入力

介護記録は、記録すべきケアを行った後、できるだけ早く記録します。時間が経つと正確に思い出せず、誤った内容を記録してしまう場合があります。必要な情報のみを記録し、業務に関係のない事情や憶測は書かないようにしましょう。

記録を訂正する場合は、誰が・いつ・どこを修正したかが分かるようにします。連絡先など、情報が古い場合、誤った判断や対応を生じる場合もあるため、常に最新の情報に更新します。

- パソコンから離れる時は、関係のない人に画面を見られたり、操作されたりしないよう、ロックをかけます。

６－５．外部とのメールなどの利用

- メール等で情報を共有する際は、誤送信を防ぐため、宛先を十分に確認します。
- 誤送信を防ぐためには、あらかじめ登録したアドレス帳を使う、または組織外のアドレスに送る際、確認メッセージが表示されるよう設定する方法があります。アドレス帳は定期的に見直しを行ってください。
- メールを書いた後、すぐに送信せず、一定の時間を置いてから送信する設定、または手動で送信する設定にすることも効果的です。

- 重要な情報は、メール本文に直接書くのではなく、添付するファイルに書いてパスワードで保護して暗号化する方法がより安全です。

- 電子メールに添付ファイルや本文中のURLリンクからウイルスに感染する等の事故が多く生じています。
- 不審なメールは開かず、添付ファイルやリンクは開かないようにしましょう。フィッシング詐欺やウイルス感染のリスクを避けるため、メールの送信元や内容には常に注意を払い、確認を行いましょう。
- 受信した電子メールに記載されたURLリンクを安易にクリックしないでください。不正なWEBサイトに誘導される可能性があります。
- 特に、安全が確認できないプログラムは、絶対にダウンロードせず、ファイルも開封してはいけません。
- 受信したメールの正当性が判断できない場合は、上長や情報システム安全管理責任者に相談します。
- 怪しいと思ったら「開かない、クリックしない」という意識の徹底が重要です。

- 業務用のSNS, メーリングリストで情報共有を行う時、共有が不要な人、共有されたくない人が含まれていないことも理解しましょう。
- 駅やカフェなどで提供されている「公衆無線LAN」は、無料で利用でき、便利ですが、情報が不正に読み取られてしまう危険が高いものです。介護業務においては使用を控えます。
- 近年、外部との通信だけでなく、事業所内外すべてを「信用できない領域」として、全ての通信を検査し認証を行うべきとするゼロトラストという考え方や対策も広がってきています。

６－６．業務外の使用の制限

業務用端末を使って、SNSやネットショッピング、動画閲覧など、業務に関係のない目的でインターネットを利用することは控えましょう。

７．管理者や情報システム安全管理責任者が行うべき措置

７－１．ISMS（情報セキュリティマネジメントシステム）のPDCAサイクル

ISMSの運用には、「何がどのような危険にさらされているか（リスク）」を見つけ、対策を決めて実行し、見直しと改善を行うという流れ（PDCAサイクル）が重要となります。このサイクルを繰り返すことによって、継続的に情報の安全を守ります。

ISMSに適用されるPDCAサイクルは、以下のとおりです。

PDCAサイクル	ISMSプロセス
Plan（計画）	介護事業所としてどのように情報を守っていくのか、その方針や目標を決めます。そのうえで、リスクへの対応方法や、情報を守るためのルールや手順を整えます。
Do（実行）	計画で決めた方針や手順を、実際の業務の中で実行します。
Check（点検）	実際に行っている情報の管理が、計画どおりにできているかを確認します。うまくいっている点や、改善が必要な点を見つけて、経営層に報告します。
Act（処置）	点検の結果をもとに、問題があれば修正したり、もっと良いやり方に変更したりします。こうして情報セキュリティのしくみを継続的に維持していきます。

７－２．管理者が講ずべき個人情報取り扱いの安全管理措置等

事業所として講ずべき情報の安全管理措置の主なものとして、以下の６つが挙げられます。

① 組織的安全管理措置：責任者の選任、個人情報取扱規則の策定　等

②人的安全管理措置：個人情報取り扱いに関する研修　等

③物理的安全管理措置：入退室管理、機器の盗難・紛失防止　等

④技術的安全管理措置：アクセス制御、外部からの不正アクセス防止　等

⑤外的環境の把握：介護ソフトベンダー社のセキュリティ対策、サイバー攻撃のトレンド等

⑥委託先の監督：委託契約の締結、定期的な点検・監査 等

７－２－１.組織的安全管理措置

（１）体制

個人情報保護管理者や情報システム安全管理責任者等を選任し、安全管理体制を整備します。

（２）情報資産の把握とリスクアセスメント

情報の安全管理は、どれほど注意深く対策を行っても、完全に防御することは不可能です。漏えい等が生じるリストと、その重大さを事前に考えておき、優先度を考慮して対策を進める必要があります。

- 個人情報ばかりでなく、事業所が保有する全ての情報資産を洗い出し、重要度に応じて分類します。
- 情報セキュリティ上のリスクを特定し、リスクの大きさや発生頻度を評価します。
- リスクアセスメントの結果に基づき、優先的に対策すべき事項を決定します。

（3）規程・マニュアル等

個人情報保護指針や個人情報取扱規程等を作り、運用します。情報の安全管理が適切に扱われているか確認する仕組みを整えます。

- 情報漏えい等が発生した緊急事態の連絡体制や対応等も規程に明記し、万一の時に迷わず行動できるよう備えます。
- 管理者や情報システム安全管理責任者への報告ルートを確立し、全職員に周知します。インシデントの大小にかかわらず、ささいなことであっても報告し、同僚や管理者と情報共有することが重要です。自分のミスも含め、速やかに報告・共有することで、被害の拡大防止や再発防止につなげることができます。報告内容は、必要に応じて同僚や管理者と共有し、組織全体での対応力を高めます。
- インターネットがつながらない、機器が動作しないといったトラブルが発生した際に備え、対応手順や事業継続計画を事前に作成しておきましょう。
- 定期的に実践状況を確認し、必要に応じてルールや対策を改善します。

（4）複数の介護施設・事業所等の管理

複数の介護施設・事業所等の管理するシステムを利用する事業所においては、施設・事業所等のシステム管理者と連携し、利用者規則、安全管理要項を理解し、システムを利用する職員としての教育を実施します。

7－2－2.人的安全管理措置

（1）雇用契約

すべての職員の雇用時、契約書等の文書に個人情報保護に関する内容を明記し、厳守されることを取り交わします。守秘義務は退職後も厳守されなくてはいけません。

（2）入職時の説明・研修

入職時、職員へ情報安全管理について説明や研修を行います。これは派遣職員を含め、すべての職員に対して実施します。

（3）研修・指導

- 定期的に情報セキュリティ研修・指導を行い、職員の意識や理解を高めます。
- 全従業員に対し、定期的に情報セキュリティに関する教育・訓練を実施する。

（４）訓練

災害時対応や漏えい時を想定した定期的な訓練も有効です。

７－２－３.物理的安全管理措置

（１）入退室管理

個人情報を保管する電子機器がある部屋への入退室を管理し、不要な人が出入りしないよう対策を講じます。

（２）紛失・盗難対策

- 機器の盗難などの防止策として、カメラの設置等を行います。
- パソコンなどの機器は固定して動かないようにし、安全な場所に保管します。
- 情報が記録された機器は鍵付きの場所に保管します。
- 端末の持ち出し、持ち込みは、以下などを記録した持ち出し記録簿で管理します。
    - 端末の種類、識別番号
    - 持ち出し者
    - 持ち出し理由、持ち出し先、利用期間
    - 返却日
- 管理者は、返却時に持ち出された端末の状態を確認し、異常がないかを確認します

（３）電子端末の整備

パソコン等が古いと、セキュリティが脆弱になる場合があります。最新のセキュリティ環境を保つことができるよう、機器の更新も計画的に行います。

（４）ネットワークの管理

- 個人所有の持ち込みパソコンや外部記憶媒体等を事業所内のネットワークに接続することは禁止します。
- 持ち込み機器を事業所のネットワークに接続する必要がある場合は、システム管理者が可否を判断します。
- 介護ソフトをタブレット端末やスマートフォンで活用する場合、前提としてクラウド型の介護ソフトであり、Wi-Fi 環境等が十分に整備されている必要があります。職員の私用スマートフォン（いわゆるBYOD）を業務上で活用する際は、厚生労働省「医療情報システムの安全管理に関するガイドライン」に基いた適切な管理が必要です。

７－２－４.技術的安全管理措置

（１）OSやソフトウェアの管理

サイバー攻撃は現在、様々な巧妙な手口でなされており、パソコンやスマートフォンなどの端末をサイバー攻撃から保護するエンドポイントセキュリティは欠かすことができません。

- インターネットに接続するすべての電子端末には、必ずセキュリティソフトを使用し、コンピュータウイルスやマルウェアなどの脅威から機器を保護します。
- 定期的にOSやセキュリティソフト、介護ソフトを更新し、常に最新の状態に保ちます。
- セキュリティソフトによって、定期的にチェック（スキャン）を実施し、異常が見つかった場合はすぐに情報システム安全管理責任者などに報告します。通常、このスキャンは自動的に行われますが、設定によっては手動でスキャンを要する場合があります。スキャンが自動的に行われる設定になっているか、確認しておきましょう。

（2）情報にアクセスする権限の管理

- パソコンやシステムへのアクセスは、必要な人だけができるよう適切な権限を設定、管理します。
- 職員ごとに固有のユーザーIDを割り当て、共有アカウントの使用は避けます。
- できるだけ指紋や顔認証などの生体認証を導入し、セキュリティを強化します。
- 権限は必要最小限に設定し、職務に応じたアクセス権限を付与します。
- 退職者のアカウントは速やかに無効化します。

（3）ログイン・ログオフの管理

- 離席時には必ずログアウトするよう職員を指導します。
- 一定時間操作がない場合（例：30分）、自動的にログアウトする機能を設定します。
- システムへのアクセス状況（ログイン、ログオフなど）を記録するログ機能を有効にし、定期的に確認して、不正アクセスや不審な操作がないか監視します。
- 不審なアクセスや操作を検知した場合、速やかに対応します。
- セキュリティ・インシデントが発生した場合、ログを分析して原因を特定します。
- 個人情報を含まない端末でも、業務システムに接続する端末は、接続先やアクセス情報を記憶させない等、個人情報を含む端末同様に注意して扱います。

（4）安全なサイト利用のための工夫

- 不要な通信は避け、よく使う外部サイトはお気に入り（ブックマーク）に登録するなどし、信頼できるサイトの利用を促します。
- 業務に関係のないサイトへのアクセスを制限します。フィルタリングソフトの利用も有効です。

（5）**クライアント証明書**

- 介護保険の資格確認などのWEBサービスを利用する際には、クライアント証明書のインストールが必要です。クライアント証明書は、国民健康保険中央会が発行・管理しています。
- クライアント証明書とは、通信相手が正しい相手かどうかを確認するための「電子的な身分証明書」です。クライアント証明書は、証明書を発行する機関（認定局）が、利用

者の身元確認を行い、信頼できる証明書として発行します。認定局は、証明書の正しさを保証する役割を担っており、証明書の安全性を守る重要な機関です。クライアント証明書を使うことで、第三者による情報の盗み見やなりすましを防ぐことができます。

（6）バックアップ

- 重要なデータは定期的にバックアップします。
- バックアップはできれば複数世代分を行います。
- データを3つ持ち（運用データ1つ、バックアップデータ2つ）、2種類の異なる媒体でバックアップし、そのうち1つは異なる場所（オフサイト）で保管するという321ルールは、バックアップの基本的な原則です。

- バックアップはネットワークから切り離して保存します。

（7）データ破棄、不要なサービスやアカウントの削除

- 不要になったデータは、復元されないよう適切に処理してから、廃棄します。
- 外部から接続できるサーバーで稼働している不要なサービスや、管理する機器やシステムに存在する不要なユーザーアカウントは停止または削除します。

（8）通信環境

- 外部との通信においては、危険な通信を削除する、ファイアウォールを有効にします。
- 無線LANを安全に利用するためには、適切な暗号化方式を設定します。
- 業務でネットワークを使う場合は、家庭用ではなく、法人向けのネットワーク機器を選びましょう。法人用機器は、家庭用に比べてセキュリティ機能が優れ、不正アクセスを検知・防御しやすくなります。
- 情報漏えい防止のため、システムの使用状況を監視します。
- 私物のスマートフォンやタブレットの業務利用は、情報漏えいを生じるリスクが高く、原則として禁止します。業務でスマートフォンを利用する場合は、可能な限り業務専用端末を用意します。
- スマートフォンやタブレットのアプリのインストールは業務に必要なものに限定し、公式マーケット以外からのインストールは原則禁止とします。また、生体認証やPINコードによる画面ロックを必ず設定し、紛失時の情報漏洩を防止しましょう。

7－2－5.外的環境の把握

- 情報システムが設置されている場所（国内外）やその環境について把握し、安全性を確認します。
- 情報セキュリティに関する最新の脅威や対策に関する情報を日頃から収集、確認します。
- 介護ソフトベンダー社のセキュリティ対策を確認します。
- サイバー攻撃のトレンドなど、新しい知識を適宜取り入れます。

７－２－６.委託先の監督

- システム運用やデータ処理などを外部業者に委託する場合は、その業者が適切なセキュリティ対策を行っているか確認して選定し、必要な契約書を交わします。
- 委託契約において、委託先が定める安全管理措置の内容を契約に盛り込み、委託先の義務とするほか、業務が適切に行われていることを定期的に確認します。
- 情報安全管理措置を正しく行い、委託業務がなされているか、定期的に監査を行います。

７－２－７.「医療情報システムの安全管理に関するガイドライン」が適用される場合

事業所が、医療情報を扱う情報システムを利用する場合、またはそのシステムに接続する場合、「医療情報システムの安全管理に関するガイドライン 第6.0版」(厚生労働省)に従う必要があります。

- 医療情報システムの機能仕様や運用手順等を文書化して管理する必要があります。
- 通常時の運用に関する仕様や手順が医療機関等の要求仕様や運用方針に則って機能しているか、定期的に監査を行い、その結果についても文書化することが求められます。
- 情報セキュリティインシデントの発生に備え、システム関連事業者又は外部有識者と非常時を想定した情報共有や支援に関する取決めや体制を整備する必要があります。
- 情報セキュリティインシデントの未然防止策として、通常時から医療情報システムに関係する脆弱性対策やEOS（End of Sale, Support, Service：販売終了、サポート終了、サービス終了）等に関する情報を収集し、速やかに対策を講じることができる体制を整える必要があります。
- 安全管理状況について、定期的に自己点検を行います。
- 事業継続計画（BCP)を整備します。
- システム関連事業者に業務委託する場合、JIS Q 15001、JIS Q 27001又はこれと同等の規格の認証を受けている事業者を選定します。
- 委託先のシステム関連事業者が提供する情報システム・サービスの内容を踏まえ、事業所と委託先事業者等との間で、責任分界の取決めを明確に行っておく必要があり、あす。また、安全管理に関する役割分担についても取り決めます。
- クラウドサービスを用いる場合、サービスを提供する委託先事業者とクラウドサービス事業者等の間における責任関係が複雑になることがあります。利用する情報システム・サービスに関連する情報機器等の責任所在と役割を明確にしておく必要があります。
- 記名・押印のための電子署名は法令に定められた形式で行い、電子署名を含む文書全体に付与するタイムスタンプを適切に行います。
- システム運用担当者は、利用している情報機器等に関して、どのような脆弱性があるか、最新の情報を収集する必要があります。
- 定期的にサイバー攻撃等のサイバーセキュリティに関する非常時対応が発生したことを想定した訓練や機能テストなどを行う必要があります。

なお、セキュリティ対策を進める際には、管理者や介護事業所の職員がすべてを抱え込む必要はありません。専門知識を持つ介護ソフトベンダー社の技術者など専門家から、必要に応じて情報を収集したり、支援を受けたりすることが効果的です。また、いざというときにすぐ相談できるように、信頼できるベンダーを日頃から確保しておくことも大切です。こうした専門家の力を借りることで、安全で効果的な運営が可能になります。

７－３．個人データの漏えい等の報告等

万一、要配慮個人情報が含まれる個人データ等の漏えい、滅失、毀損その他の個人データの安全の確保に係る事態が生じたときは、個人情報保護委員会に報告するとともに、本人への通知を行わなければいけません。詳細は個人情報保護委員会のWEBサイトをご覧ください。

個人情報保護委員会　https://www.ppc.go.jp/personalinfo/legal/leakAction/

なお、要配慮個人情報が含まれる個人データの漏えい等に限らず、医療機関等においてコンピュータウイルスの感染などによるサイバー攻撃を受けた疑いがある場合にあっては、直ちに医療情報システムの保守会社等に連絡の上、当該サイバー攻撃により医療情報システムに障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる又はそのおそれがある事案であると判断された場合には、速やかに当該医療機関等から厚生労働省に連絡することとされています。詳しくは「医療機関等におけるサイバーセキュリティ対策の強化について」（平成30年10月29日医政総発1029第１号・医政地発1029第３号・医政研発1029第１号）をご覧ください。

また、スマートフォンやパソコンなどの機器を紛失したり、盗まれたりした場合には、すぐに管理者へ報告し、遠隔ロックやデータの消去など、情報漏えいを防ぐための対応を速やかに行うことが重要です。必要に応じて、警察への届け出も検討してください。

8. まとめ

本手引では、介護事業における情報安全管理のあり方について解説してきました。介護事業所では利用者の記録など機微な個人情報を多く取り扱うため、情報の適切な管理は単なる法令遵守にとどまらず、利用者の尊厳を守り、信頼関係を築くための基本となります。

情報の確かな保存、情報の質の保証、個人情報の保護という三つの要素がバランスよく実践されることで、介護事業所における適切な情報管理が実現します。セキュリティ対策は「完全な安全はない」という現実を受け入れた上で、守るべき情報を明確にし、様々な対策を組み合わせて実施することが重要です。

個人情報保護の観点からは、個人情報と要配慮個人情報の区別、利用目的の特定と通知、本人同意の取得、第三者提供の制限など、法令に基づいた適切な取扱いが求められます。特に介護現場で起こりやすい個人情報漏えいの事例を理解し、予防策を講じることが大切です。

情報システムの安全管理においては、アクセス制限やパスワード管理、ソフトウェアの更新など基本的な対策を確実に実施するとともに、職員への教育・研修を通じてセキュリティ意識を高めることが効果的です。

本手引に示した考え方や対策を参考に、各事業所の状況に応じた取組みを進めてください。情報安全管理は一度整備して終わりではなく、新たな脅威や法改正に対応して継続的に見直し、改善していくことが必要です。日々の小さな取組みの積み重ねが、利用者の個人情報を守り、質の高い介護サービスの提供につながります。

用語集

あ行

アカウントハイジャック

不正な方法でユーザーのアカウントを乗っ取る行為。

アクセス制御

情報やシステムに対し、誰がどのような操作を行えるかを制限すること。介護事業所では、職員ごとに閲覧・編集できる情報を制限するために使用する。

暗号化

情報を第三者に読み取られないよう、特定の規則に従って変換すること。鍵（パスワード）がなければ内容を読み取れなくなる。

エンドポイントセキュリティ

パソコンやスマートフォンなどの端末をサイバー攻撃から保護するためのセキュリティ対策。

か行

外部記憶媒体

パソコンなどの端末に接続してデータを保存・読み込みする装置。USBメモリ、外付けHDD（パソコンのデータを大量に保存できる箱型の装置）などが含まれる。

可用性：必要なときに情報やシステムを確実に利用できること。システム障害やデータ消失から守るための対策が重要。

完全性

情報が破壊、改ざん、消去などされずに、正確性と完全性が保たれていること。

機密性

許可された人だけが情報にアクセスできる状態を確保すること。

クライアント証明書

利用者が特定のサービスに安全にアクセスするために、自身の正当性を証明するデジタル証明書

クラウド

インターネットを通じて、データの保存やアプリの利用などのコンピュータ資源を提供・利用する仕組み

クラウドセキュリティ
クラウドサービスを使用する際に発生しうるリスクに対して実施するセキュリティ対策。

ケアプランデータ連携システム
介護サービス事業者が作成したケアプランやサービス利用票などの情報を、関係機関と迅速かつ安全に共有するための仕組み。介護事業所の文書作成に要する負担が大幅に軽減されることが期待されている。

個人データ
個人情報データベース等を構成する個人情報。電子媒体に限らず、紙媒体の情報も含まれる。

さ行

321ルール
バックアップの原則。データを3つ持ち（運用データ1つ、バックアップデータ2つ）、2種類の異なる媒体でバックアップし、そのうち1つは異なる場所（オフサイト）で保管する方法。

サイバーセキュリティ
電子データの漏えい・改ざん、システムの不正利用などから守るための対策。

修正プログラム（セキュリティパッチ）
ソフトウェアの脆弱性を修正するためのプログラム。

情報セキュリティ基本方針
一般的に「情報セキュリティポリシー」の一部として扱われている。組織内での情報セキュリティに対する意思表明。

情報セキュリティ対策基準
一般的に「情報セキュリティポリシー」の一部として扱われている。基本方針に沿って、組織的にどのような対策を講じるのかをルール化したもの。

情報セキュリティポリシー
組織の情報セキュリティ対策の方針や行動方針をまとめたもの。「基本方針」、「対策基準」、「実施手順」で構成されている。

脆弱性（ぜいじゃくせい）
システムのセキュリティ上の弱点。攻撃者に悪用される可能性がある。

セキュリティインシデント
悪意ある第三者からの攻撃を受けたり、情報漏えいが生じたりするなど、事業運営が困難になるほどのセキュリティの脅威となる事象。

ゼロトラスト
組織のあらゆる情報資産は常に脅威にさらされていると考え、あらゆるアクセスは検証されるべきという概念。

ソーシャルエンジニアリング
アナログ的な手法で、IT技術を使わずに人間の心理的な弱みや不注意につけこみ、情報を盗み取ること。例えば、なりすまし電話をかけ、個人情報を聞き出すなど。

ソフトウェア
単にソフト、と呼ばれることも多い。アプリケーション、またアプリも同義。

た行
データベース
電子計算機を用いて検索できるように体系的に構成された情報の集合体。

な行
二要素認証（2FA）
インターネット上のシステムやサービスなどにログインする際に使用されるユーザー認証の1つ。「知識情報」「所有情報」「生体情報」の3つの要素のうち、異なる2つを組み合わせて認証を行う。通常のパスワードに加え、もう1つの要素（例：ワンタイムパスワード）で認証を行うことで、セキュリティを強化する。

認証システム
システムやデータにアクセスする際に、本人確認を行う仕組み。パスワード、二段階認証、バイオメトリクス認証などが含まれる。

は行
ハッカー
コンピュータ技術を利用して、ハッキングを行う人のこと。

ハッキング
コンピュータやネットワークに不正にアクセスし、情報を盗んだり、システムを破損したりする行為。

バックアップ
データの複製を作成し、原本の損失時に復元できるようにすること。

ハブ
ネットワーク機器の一種。LAN（ローカルエリアネットワーク）内で信号を複数の機器に分配する中継装置。

ファイアウォール
外部ネットワークからの不正アクセスを防ぐための仕組み。

フィッシング
偽のメールやウェブサイトを使って個人情報やパスワードを盗み取る行為。

不正アクセス
権限のない者がシステムに侵入し、データの窃取や改ざんを行うこと。

物理的セキュリティ
施設や設備の入退室管理、鍵の管理など、物理的な手段によるセキュリティ対策。

プライバシーポリシー
個人情報の取扱い方針を対外的に明示したもの。

ベンダー
ITに関する製品やサービスを提供する企業。また、通信会社や他の企業が利用するネットワークの開発や提供も行う。

ま行
マルウェア
悪意をもって作成された不正で有害な動作を行うプログラムの総称。マルウェアは他人のコンピュータに入り、データの改ざんや機密情報の流出などの不正行為を行う。代表的なマルウェアとしては次のものがある。

- マクロ感染型：メールなどで受信した感染したWordやExcelの添付ファイルを開くと、マクロが実行された瞬間に感染
- ファイル感染型：拡張子が「.com」「.exe」「.sys」などのファイルに付着する特徴があり、プログラムを書き換えることによって感染
- トロイの木馬型：正規のソフトウェアであるように見せかけ、添付ファイルやWEBサイトなどからダウンロード、実行することによって感染
- ワーム型：ネットワークやメールの添付ファイル、 USB ドライブなどから感染

無線LAN
ケーブルを使わずにインターネットに接続するための技術。WPA2などの暗号化方式で保護する必要がある。

メールフィルタリング
迷惑メールや不審なメールを自動的に検出・分類する機能。

ら行
リスク
組織の目標達成や事業継続を阻害する不確実性のこと。情報セキュリティでは、情報資産に対する脅威や脆弱性からくる損害発生の可能性を指す。

リスクアセスメント
リスク特定、リスク分析、リスク評価の3つのプロセスから構成される一連のプロセス。

ランサムウェア
感染したコンピュータのデータを暗号化し、「身代金」を要求するマルウェア。

ログ
システムの動作や利用者の操作の記録。不正アクセスや情報漏えいの調査に重要。

わ行
ワンクリック詐欺
Webサイトや電子メール、SMSなどのメッセージに記載されたURLを一度クリックしただけで、一方的にサービスへの入会などの契約成立を宣言され、多額の料金の支払いを求められるという詐欺

アルファベット
BCP（Business Continuity Plan）
事業継続計画。災害やシステム障害発生時に重要業務を継続するための計画。

BYOD（Bring Your Own Device）
従業員が個人所有の端末を業務に使用すること。セキュリティ上の課題が多い。

DLP（データ漏えい防止）

個人情報などの機密情報を監視し、外部への流出・紛失を防ぐためのセキュリティ対策。「個人情報」「営業秘密」「経営情報」などの機密情報を識別し、外部への送信やコピーを制限することにより、データを保護する仕組み。

DX（Digital Transformation）
デジタル技術を活用して、業務やサービスを変革すること。

ISMS（Information Security Management System）
情報セキュリティマネジメントシステム。組織の情報セキュリティを体系的に管理・運用する仕組み。

SNS（Social Networking Service）
ソーシャル・ネットワーキング・サービス。インターネット上で社会的ネットワークを構築できるサービス。

USB（Universal Serial Bus）
パソコンと周辺機器を接続するための規格。USBメモリは情報漏えいの原因になりやすい。

VPN（Virtual Private Network）
インターネット上に仮想的なプライベートネットワークを構築する技術。テレワークでの安全な通信に使用される。

Wi-Fi
無線LANの規格の一つ。パスワードなどで適切に保護する必要がある。

参考文献等

- 個人情報の保護に関する法律（平成15年5月30日施行）
- 個人情報保護委員会．個人情報の適正な取扱いのための研修資料
- 厚生労働省．医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス（平成29年4月14日通知、令和6年12月2日最終改定）
- 厚生労働省．「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」に関するＱ＆Ａ（事例集）（令和6年12月2日改正）
- 厚生労働省．医療情報システムの安全管理に関するガイドライン（令和5年5月31日改正）
- 厚生労働省.介護サービス事業所におけるICT機器・ソフトウェア導入に関する手引きver2
- 厚生労働省．地域医療情報連携ネットワークにおける同意取得方法の例について（事務連絡）（令和2年3月31日）
- 独立行政法人情報処理推進機構. 中小企業の情報セキュリティ対策ガイドライン」https://www.ipa.go.jp/security/keihatsu/sme/guideline/
- 独立行政法人情報処理推進機構. 付録 3：5 分でできる！情報セキュリティ自社診断
- 独立行政法人情報処理推進機構. 付録 7：リスク分析シート

令和６年度厚生労働科学研究費補助金
「介護事業所における情報の安全管理に関するガイドライン（案）作成のための調査研究」
研究班

代表
国立長寿医療研究センター　在宅医療・地域医療連携推進部 三浦久幸

分担研究者
国立長寿医療研究センター　老年内科部　大西丈二
国立長寿医療研究センター　医療経済研究部　大寺祥佑
日本遠隔医療協会　近藤博史
日本遠隔医療協会　長谷川高志

発行
令和６年度厚生労働科学研究費補助金「介護事業所における情報の安全管理に関するガイドライン（案）作成のための調査研究」研究班
代表　国立長寿医療研究センター　三浦久幸
〒474-8511 愛知県大府市森岡町7-430

別紙 1

別添資料．介護事業所における情報安全管理に関連する法令・ガイドラン等

	文書名	制定・公表	主体	最終更新
1	個人情報の保護に関する法律	平成15年法律第57号	法律	令和5年法律第79号による改正
2	行政機関の保有する個人情報の保護に関する法律	平成15年法律第58号	法律	令和3年法律第37号による廃止
3	独立行政法人等の保有する個人情報の保護に関する法律	平成15年法律第59号	法律	令和3年法律第37号による廃止
4	民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律	平成16年法律第149号	法律	令和3年法律第36号による改正
5	電子署名及び認証業務に関する法律	平成12年法律第102号	法律	令和4年法律第68号による改正
6	電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律	平成14年法律第153号	法律	令和6年法律第59号による改正
7	医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律	昭和35年法律第145号	法律	令和5年法律第84号による改正
8	厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令	平成17年厚生労働省令第44号	厚生労働大臣	令和6年厚生労働省令第141号による改正
9	政府情報システムにおけるクラウドサービスの利用に係る基本方針	令和4年9月30日初版決定	デジタル社会推進会議幹事会決定	令和5年9月29日 令和6年12月9日デジタル庁より更新あり
10	良質な医療を提供する体制の確立を図るための医療法の一部を改正する法律の一部の施行について	平成19年3月30日発出 医政発第0330010号	厚生労働省	平成19年3月30日発出
11	「診療録等の保存を行う場所について」の一部改正について	平成25年3月25日発出 医政発0325第15号 薬食発0325第9号 保　発0325第5号	厚生労働省	平成25年3月25日発出
12	「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等につい て」の一部改正について	平成28年3月31日発出 医政発0331第30号 薬生発0331第10号 保　発0331第26号 政社発0331第1号	厚生労働省	平成28年3月31日発出
13	医療機器におけるサイバーセキュリティの確保について	平成27年4月28日発出 薬食機参発0428第1号 薬食安発0428第1号	厚生労働省	平成27年4月28日発出
14	医療機関等におけるサイバーセキュリティ対策の強化について	平成30年10月29日発出 医政総発1029第1号 医政地発1029第3号 医政研発1029第1号	厚生労働省	平成30年10月29日発出
15	ランサムウエアによるサイバー攻撃に関する注意喚起	令和3年4月30日発出	内閣官房内閣サイバーセキュリティセンター（NISC）	令和3年4月30日発出
16	時刻認証業務の認定に関する規程	令和3年4月1日制定 法務省告示第146号	総務省	令和3年4月1日制定
17	個人情報の保護に関する法律についてのガイドライン（通則編）	平成28年11月	個人情報保護委員会	令和7年3月一部改正

	文書名	制定・公表	主体	最終更新
18	医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス	平成29年4月14日	個人情報保護委員会 厚生労働省	令和6年12月 一部改正
19	医療情報を取り扱う情報システ ム・サービスの提供事業者における安全管理ガイドライン	令和2年8月21日策定	経済産業省 総務省	令和5年7月7日改定（第1.1版）
20	政府機関等のサイバーセキュリ ティ対策のための統一基準群（令和5年度版）	令和5年7月4日	内閣官房内閣サイバーセキュリティセンター（NISC）	令和5年7月4日
21	利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するQ&A（電子署名法2条1項に関 するQ&A）	令和2年7月17日公表	総務省 法務省 経済産業省	令和2年7月17日公表
22	利用者の指示に基づきサービス提 供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するQ&A（電子署名法3条に関す るQ&A）	令和2年9月4日公表	総務省 法務省 経済産業省 デジタル庁	令和6年1月9日 一部改定
23	タイムビジネスに係る指針ーネットワークの安心な利用と電子データの安全な長期保存のためにー	平成16年11月5日公表	総務省	平成16年11月5日公表
24	医療機器のサイバーセキュリティの確保に関するガイダンス	平成30年7月24日発出 薬生機審発0724第1号 薬生安発0724第1号	厚生労働省	平成30年7月24日発出
25	クラウドサービス提供における情報セキュリティ対策ガイドライン （第３版）	平成26年に初版公表	総務省	令和3年9月30日
26	クラウドサービス提供・利用における適切な設定に関するガイドライン	令和4年10月策定	総務省	令和4年10月
27	厚生労働省標準規格	平成22年3月31日 医政発0331第1号 「保健医療情報分野の標準規格として認めるべき規格について	厚生労働省	令和7年1月29日 情参発0129第1号 産情発0129第2号 「保健医療情報分野の標準規格（厚生労働省標準規格）について」の一部改正について
28	JIS Q 27001（情報セキュリティマネジメントシステム）	平成18年5月20日制定(JIS Q 27001:2006)	経済産業大臣	令和5年9月20日改正（JIS Q 27001:2023）
29	ISO14533-1：2014CMS利用電子 署名(CAdES)の長期署名プロファイル	平成26年12月策定(ISO14533-1：2014)	ISO/TC154	令和4年6月策定（ISO 14533-1:2022）
30	ISO14533-2:2021XML署名利用電 子署名(XAdES)の長期署名プロファイル	令和3年8月策定	ISO/TC154	令和3年8月策定
31	ISO14533-3:2017PDF長期署名プ ロファイル(PAdES)	平成29年9月策定	ISO/TC154	平成29年9月策定
32	JIS Q 15001（個人情報保護マネジメントシステム）	平成11年3月20日制定	（原案作成）一般財団法人日本情報経済社会推進協会（JIPDEC）	令和5年9月20日発行(JIS Q 15001:2023)
33	「医療情報システムの安全管理に関するガイドライン」の実装事例に関する報告書	平成19年2月公表	保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム （HEASNET） 厚生労働省	平成19年3月
34	TLS暗号設定ガイドライン3.1.0版	平成27年5月8日初版発行	独立行政法人情報処理推進機構	令和6年6月17日

	文書名	制定・公表	主体	最終更新
35	『製造業者・サービス事業者による医療情報セキュリティ開示書』ガイド Ver.5.0	令和6年9月公表	一般社団法人保健医療福祉情報システム工業会（JAHIS）	令和6年9月公表
36	IoT セキュリティガイドライン ver1.0（IoT 推進コンソーシアム、総務省、経済産業省；平成28 年 7 月）	平成28年7月5日公表	IoT 推進コンソーシアム総務省 経済産業省	平成28年7月5日公表
37	標的型攻撃メールへの対処について	平成28年4月28日公表	日本医療情報学会	平成28年4月28日公表
38	IPA対策のしおりシリーズ	平成24年1月30日第1版策定（初めての情報セキュリティ対策のしおり）	情報処理推進機構（IPA）	平成24年1月30日第1版策定（初めての情報セキュリティ対策のしおり）
39	デジタル画像の取り扱いに関するガイドライン 3.0 版（平成 27 年 4 月）	平成11年4月公表	日本医学放射線学会電子情報委員会	平成27年4月
40	個人情報保護に役立つ監査証跡ガイド～あなたの病院の個人情報を守るために～（医療情報システム開発センター）	平成19年3月発行	一般財団法人医療情報システム開発センター（MEDIS）	平成19年3月発行
41	介護保険法	平成9年12月法律第123号	法律	令和5年法律第31号による改正
42	介護保険法施行法　抄	平成9年12月法律第124号	法律	平成29年法律第52号による改正
43	介護保険法施行令	平成10年第412号	法律	令和6年政令第151号による改正
44	介護サービスの基盤強化のための介護保険法等の一部を改正する法律の施行に伴う関係政令の整備等及び経過措置に関する政令	平成23年12月第376号	法律	平成30年政令第55号による改正
45	介護保険法施行規則	平成11年3月厚生省令第36号	厚生労働省	令和6年厚生労働省令第109号による改正
46	サイバーセキュリティ基本法	平成26年11月法律第104号	法律	令和4年法律第68号による改正
47	医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）	令和4年11月10日発出	厚生労働省	令和4年11月10日発出
48	時刻認証業務の認定に関する実施要項	令和6年3月7日時点版	総務省	令和6年3月7日時点版
49	障害者の日常生活及び社会生活を総合的に支援するための法律	平成17年法律第123号	法律	令和4年法律第104号による改正
50	個人情報の保護に関する法律施行令	平成15年政令第507号	施行令	令和6年政令第260号による改正
51	個人情報の保護に関する法律施行規則	平成28年個人情報保護委員会規則第3号	施行規則	令和6年個人情報保護委員会規則第5号による改正

	文書名	制定・公表	主体	最終更新
52	医療法	昭和23年法律第205号	法律	令和6年法律第52号による改正
53	老人福祉法	昭和38年法律第133号	法律	令和5年法律第31号による改正
54	独立行政法人通則法	平成11年法律第103号	法律	令和3年法律第61号による改正
55	地方独立行政法人法	平成15年法律第118号	法律	令和6年法律第47号による改正
56	医薬品の臨床試験の実施の基準に関する省令	平成9年厚生省令第28号	厚生労働省	令和5年厚生労働省令第161号による改正
57	国民健康保険法	昭和33年法律第192号	法律	令和5年法律第48号による改正
58	高齢者の医療の確保に関する法律	昭和57年法律第80号	法律	令和5年法律第48号による改正
59	統計法	平成19年法律第53号	法律	令和3年法律第37号による改正
60	医療法の一部を改正する法律の一部の施行について	平成5年2月15日 健政発第98号 厚生省健康政策局長通知	厚生労働省	平成5年2月15日
61	病院、診療所等の業務委託について	平成5年月2月15日 指第14号 厚生省健康政策局指導課長通知	厚生労働省	平成5年月2月15日
62	診療情報の提供等に関する指針の策定について〔医師法〕	平成15年9月12日 医政発第0912001号	厚生労働省	平成15年9月12日
63	「診療情報の提供等に関する指針」の一部改正について	令和5年１月25日 医政発0125第15号	厚生労働省	令和5年１月25日
64	個人情報の保護に関する法律についてのガイドライン （行政機関等編）	令和4年1月	個人情報保護委員会	令和6年11月一部改正
65	個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）	平成28年11月	個人情報保護委員会	令和5年12月一部改正
66	個人情報の保護に関する法律についてのガイドライン （第三者提供時の確認・記録義務編）	平成28年11月	個人情報保護委員会	令和5年12月一部改正
67	個人情報の保護に関する法律についてのガイドライン（仮名加工情報・匿名加工情報編）	平成28年11月	個人情報保護委員会	令和6年12月一部改正
68	個人情報の保護に関する法律についてのガイドライン（認定個人情報保護団体編）	令和3年8月	個人情報保護委員会	令和4年9月一部改正

	文書名	制定・公表	主体	最終更新
69	個人情報の保護に関する基本方針	平成16年4月2日 閣議決定	個人情報保護委員会	令和4年4月1日 一部変更
70	サイバーセキュリティ経営ガイドライン Ver 3.0	令和5年3月24日	経済産業省 独立行政法人情報処理推進機構	令和5年3月24日
71	医師法	昭和23年法律第201号	法律	令和3年法律第49号による改正
72	医療法施行規則	昭和23年厚生省令第50号	施行規則	令和6年厚生労働省令第59号による改正
73	医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律施行規則	昭和36年厚生省令第1号	施行規則	令和6年厚生労働省令第百65号による改正
74	医療機器のサイバーセキュリティ導入に関する手引書の改訂について	令和5年3月31日 薬生機審発0331第11号 薬生安発0331 第４号	厚生労働省	令和5年3月31日
75	医療機関における医療機器のサイバーセキュリティ確保のための手引書について	令和5年3月31日 医政参発0331 第１号 薬生機審発0331第16号 薬生安発0331 第８号	厚生労働省	令和5年3月31日
76	健康保険法	大正11年法律第70号	法律	令和5年法律第48号による改正
77	地域医療情報連携ネットワークにおける同意取得方法の例について	令和2年3月31日 事務連絡	厚生労働省	令和2年3月31日
78	指定訪問看護の事業の人員及び運営に関する基準	平成12年3月31日 厚生省令第80号	厚生労働省	平成12年3月31日
79	介護医療院の人員、施設及び設備並びに運営に関する基準	平成30年1月18日 厚生労働省令第5号	厚生労働省	平成30年1月18日
80	指定介護予防サービス等の事業の人員、設備及び運営並びに指定介護予防サービス等に係る介護予防のための効果的な支援の方法に関する基準	平成18年厚生労働省令第35号	厚生労働省	令和6年厚生労働省令第16号による改正
81	指定地域密着型サービスの事業の人員、設備及び運営に関する基準	平成18年3月14日 厚生労働省令第34号	厚生労働省	平成18年3月14日
82	指定居宅サービス等の事業の人員、設備及び運営に関する基準	平成11年厚生省令第37号	厚生労働省	令和6年厚生労働省令第16号による改正
83	指定介護老人福祉施設の人員、設備及び運営に関する基準	平成11年厚生省令第39号	厚生労働省	令和6年厚生労働省令第16号による改正
84	介護老人保健施設の人員、施設及び設備並びに運営に関する基準	平成11年厚生省令第40号	厚生労働省	令和6年厚生労働省令第16号による改正
85	高齢者の医療の確保に関する法律の規定による療養の給付の取扱い及び担当に関する基準	昭和58年1月20日 厚生省告示第14号	厚生労働省	昭和58年1月20日

	文書名	制定・公表	主体	最終更新
86	特別養護老人ホームの設備及び運営に関する基準	平成11年厚生省令第46号	厚生労働省	令和6年厚生労働省令第16号による改正
87	臨床検査技師等に関する法律施行規則	昭和33年厚生省令第24号	厚生労働省	令和6年厚生労働省令第19号による改正
88	歯科医師法	昭和23年法律第202号	法律	令和3年法律第49号による改正
89	歯科衛生士法	昭和23年法律第204号	法律	令和4年法律第68号による改正
90	歯科衛生士法施行規則	平成元年厚生省令第46号	厚生労働省	令和4年厚生労働省令第107号による改正
91	歯科技工士法	昭和30年法律第168号	法律	令和4年法律第68号による改正
92	保健師助産師看護師法	昭和23年法律第203号	法律	令和4年法律第68号による改正
93	救急救命士法	平成3年法律第346号	法律	令和4年法律第68号による改正
94	診療放射線技師法	昭和26年法律第226号	法律	令和4年法律第68号による改正
95	薬剤師法	昭和35年法律第146号	法律	令和4年法律第47号による改正
96	保険医療機関及び保険医療養担当規則	昭和32年厚生省令第15号	厚生労働省	令和6年厚生労働省令第154号による改正
97	保険薬局及び保険薬剤師療養担当規則	昭和32年厚生省令第16号	厚生労働省	令和6年厚生労働省令第154号による改正
98	理学療法士及び作業療法士法	昭和40年法律第137号	法律	令和4年法律第68号による改正
99	視能訓練士法	昭和46年法律第64号による改正	法律	令和4年法律第68号による改正
100	臨床工学技士法	昭和62年法律第60号	法律	令和4年法律第68号による改正
101	義肢装具士法	昭和62年法律第61号	法律	令和4年法律第68号による改正
102	言語聴覚士法	平成9年法律第132号	法律	令和4年法律第68号による改正

	文書名	制定・公表	主体	最終更新
103	あん摩マツサージ指圧師、はり師、きゆう師等に関する法律	昭和22年法律第217号	法律	令和4年法律第68号による改正
104	柔道整復師法	昭和45年法律第19号	法律	令和4年法律第68号による改正
105	精神保健福祉士法	平成9年法律第131号	法律	令和3年法律第37号による改正
106	感染症の予防及び感染症の患者に対する医療に関する法律	平成10年法律第104号	法律	令和4年法律第96号による改正
107	母体保護法	昭和23年法律第156号	法律	令和4年法律第76号による改正
108	私立学校教職員共済法	昭和28年法律第245号	法律	令和6年法律第47号による改正
109	船員保険法	昭和14年法律第73号	法律	令和5年法律第48号による改正
110	国家公務員共済組合法	昭和33年法律第128号	法律	令和5年法律第48号による改正
111	地方公務員等共済組合法	昭和37年法律第152号	法律	令和5年法律第48号による改正
112	少年法	昭和23年法律第168号	法律	令和5年法律第28号による改正
113	身体障害者福祉法	昭和24年法律第283号	法律	令和4年法律第66号による改正
114	知的障害者福祉法	昭和35年法律第37号	法律	令和4年法律第66号による改正
115	精神保健及び精神障害者福祉に関する法律	昭和25年法律第123号	法律	令和4年法律第104号による改正
116	発達障害者支援法	平成16年法律第167号	法律	平成28年法律第64号による改正
117	地方自治法	昭和22年法律第67号	法律	令和6年法律第70号による改正
118	学校教育法	昭和22年法律第26号	法律	令和4年法律第76号による改正
119	地方税法	昭和25年法律第226号	法律	令和6年法律第4号による改正

	文書名	制定・公表	主体	最終更新
120	国立研究開発法人情報通信研究機構法	平成11年法律第162号	法律	令和4年法律第93号による改正
121	国立研究開発法人新エネルギー・産業技術総合開発機構法	平成14年法律第145号	法律	令和6年法律第45号による改正
122	国立研究開発法人医薬基盤・健康・栄養研究所法	平成16年法律第135号	法律	令和4年法律第43号による改正
123	国立研究開発法人日本医療研究開発機構法	平成26年法律第49号	法律	令和4年法律第68号による改正
124	補助金等に係る予算の執行の適正化に関する法律	昭和30年法律第179号	法律	令和4年法律第68号による改正
125	心神喪失等の状態で重大な他害行為を行った者の医療及び観察等に関する法律	平成15年法律第110号	法律	令和5年法律第28号による改正
126	がん登録等の推進に関する法律	平成25年法律第111号	法律	令和3年法律第37号による改正
127	医療機器の臨床試験の実施の基準に関する省令	平成17年厚生労働省令第36号	厚生労働省	令和5年厚生労働省令第161号による改正
128	遺伝子治療等臨床研究に関する指針	平成31年厚生労働省告示第48号	厚生労働省	平成31年2月28日
129	人を対象とする生命科学・医学系研究に関する倫理指針	令和3年文部科学省・厚生労働省・経済産業省告示第1号	文部科学省・厚生労働省・経済産業省	令和3年3月23日
130	再生医療等製品の臨床試験の実施の基準に関する省令	平成26年厚生労働省令第89号	厚生労働省	令和5年厚生労働省令第161号による改正
131	医療における遺伝学的検査・診断に関するガイドライン	平成23年2月	日本医学会	2022年3月改定
132	配偶者からの暴力の防止及び被害者の保護等に関する法律	平成13年法律第31号	法律	令和5年法律第30号による改正
133	麻薬及び向精神薬取締法	昭和28年法律第14号	法律	令和5年法律第84号による改正
134	児童虐待の防止等に関する法律	平成12年法律第82号	法律	令和4年法律第104号による改正
135	児童福祉法	昭和22年法律第164号	法律	令和6年法律第417号による改正
136	社会保険診療報酬支払基金法	昭和23年法律第129号	法律	令和5年法律第31号による改正

	文書名	制定・公表	主体	最終更新
137	労働者災害補償保険法	昭和22年法律第50号	法律	令和4年法律第68号による改正
138	生活保護法	昭和25年法律第144号	法律	令和6年法律第417号による改正
139	指定医療機関医療担当規程	厚生省告示第222号	厚生労働省	昭和25年8月23日
140	がん登録等の推進に関する法律	平成25年法律第111号	法律	令和3年法律第37号による改正
141	内閣府設置法	平成11年法律第89号	法律	令和5年法律第79号による改正
142	国家行政組織法	昭和23年法律第120号	法律	令和3年法律第36号による改正
143	宮内庁法	昭和22年法律第70号	法律	平成29年法律第63号による改正
144	刑事訴訟法	昭和23年法律第131号	法律	令和5年法律第84号による改正
145	刑法	明治40年法律第45号	法律	令和5年法律第66号による改正
146	労働安全衛生法	昭和47年法律第57号	法律	令和4年法律第68号による改正
147	派遣先が講ずべき措置に関する指針	平成11年労働省告示第138号	労働省（現厚生労働省）	令和２年厚生労働省告示第346号による改正
148	医療情報システムの安全管理に関するガイドライン 第6.0版」の策定について	産情発0531第1号	厚生労働省	令和5年5月31日
149	医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン（第1.1版）	令和2年8月	経済産業省	令和5年7月改定
150	中小企業の情報セキュリティ対策ガイドライン（第3.1版）	令和5年（2023年）4月	独立行政法人情報処理推進機構(IPA)	令和5年（2023年）4月
151	電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律	平成10年法律第25号	法律	令和2年法律第8号による改正
152	指定居宅サービス等の事業の人員、設備及び運営に関する基準等の一部を改正する省令	厚生労働省令第9号	厚生労働省	令和3年1月25日
153	社会福祉法	昭和26年法律第45号	法律	令和6年法律第47号による改正

	文書名	制定・公表	主体	最終更新
154	軽費老人ホームの設備及び運営に関する基準	厚生労働省令第107号	厚生労働省	平成20年5月9日
155	養護老人ホームの設備及び運営に関する基準	昭和41年厚生省令第19号	厚生労働省	令和6年厚生労働省令第16号による改正
156	軽費老人ホームの設備及び運営に関する基準について	老発0530第2号	厚生労働省	平成20年5月30日
157	診療録等の記載方法等につ いて	総第17号・指第20号・医第29号・歯第12号・看第10号・薬企第20号・保険発第43号	厚生労働省	昭和63年5月6日
158	エックス線写真等の光磁気ディスク等への保存について	健政発第280号	厚生労働省	平成6年3月29日
159	診療録等の電子媒体による保存について	健政発第517号 写 医薬発第587号 保発第82号	厚生労働省	平成11年4月22日
160	法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン等について	11医情開第24号	財団法人医療情報システム開発センター	平成11年3月11日
161	診療録等の外部保存に関するガイドラインについて	医政発第0531005号	厚生労働省	平成14年5月31日
162	民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律	平成16年法律第149号	法律	令和3年法律第36号による改正
163	ASP･SaaSにおける情報セキュリティ対策ガイドライン	平成20年1月30日	ASP・SaaSの情報セキュリティ対策に関する研究会	平成20年1月30日
164	医療情報を受託管理する情報処理事業者における安全管理	経済産業省告示第228号	経済産業省	平成24年10月15日
165	ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン（第1.1版）	平成22年12月	総務省	平成22年12月
166	クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン（第1版）	平成30年7月	総務省	平成30年7月
167	医療等情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン	令和2年8月	総務省	令和2年8月
168	指定居宅サービス等及び指定介護予防サービス等に関する基準について	老企第25号	厚生労働省	平成11年9月17日
169	介護保険法施行規則第140条の63の6第1号に規定する厚生労働大臣が定める基準について	老認発0315第4号	厚生労働省	令和6年3月15日
170	個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律	平成27年法律第65号	法律	平成27年9月9日

別紙 2-1

介護事業者用

介護事業所におけるサイバーセキュリティ対策チェックリスト

	チェック項目	事業所内の担当者が行っている		事業所外だが、法人内の担当者が行っている		委託業者が行っている	
		チェック	確認した日	チェック	確認した日	チェック	確認した日
体制構築	情報システム安全管理責任者を設置している。		/				
	情報システム安全管理を委託する業者がいる。		/				
介護ソフトの管理・運用	**※介護ソフト等について、以下を実施している。**						
	コンピュータ、タブレット、スマホなど端末の台帳管理を行っている。		/				
	リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。		/		/		/
	※端末について、以下を実施している。						
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。		/		/		/
	退職者や使用していないアカウント等、不要なアカウントを削除している。		/		/		/
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。		/		/		/
	バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。		/		/		/
	※ネットワーク機器について、以下を実施している。						
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。		/		/		/
介護ソフトの管理・運用	セキュリティソフトをインストールし、最新化された状態で稼働させている。		/		/		/
	インシデント発生時における組織内と外部関係機関（介護ソフト業者、自治体、警察等）への連絡体制図がある。				/		/
	インシデント発生時に介護サービスを継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。		/		/		/
	災害時の事業継続計画（BCP）に情報管理のことを記載している		/				

事業者確認用

介護事業所におけるサイバーセキュリティ対策チェックリスト

	チェック項目	事業所内の担当者が行っている	
		チェック	確認した日
体制構築	事業所の情報システム安全管理責任者を確認した。		/
介護ソフトの管理・運用	**※介護ソフト等について、以下を実施した。**		
	リモートメンテナンス（保守）を利用している機器の有無を確認した。		/
	※端末PCについて、以下を実施していた。		
	利用者の職種・担当業務別の情報区分毎のアクセス利用権限が設定されている。		/
	退職者や使用していないアカウント等、不要なアカウントの削除行為がなされている。		/
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用される設定になっている。		/
	バックグラウンドで動作している不要なソフトウェア及びサービスが停止されている。		/
	セキュリティソフトがインストールされ、最新化された状態で稼働している。		/
	※ネットワーク機器について、以下を実施している。		
	セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。		/
介護ソフトの管理・運用	インシデント発生時におけるサポート範囲を説明してある。		/
	インシデント発生時における問合せ窓口を説明してある。		/

事例（場面想定）

利用目的の特定（法第 17 条第 1 項関係）

【具体的に利用目的を特定している事例】

（事例 1）

介護サービス計画（ケアプラン）の作成と実施

H ケアプランセンターでは、利用者から個人情報を取得する際に「介護サービス計画（ケアプラン）の作成と実施のため」と明記し、使途を明確にしています。これにより、どのような目的で個人情報を利用するのかが具体的に示されているため、利用者は自分の情報がどのように使われるかを理解することができます。このように具体的な目的を示すことは適切な対応です。

（事例 2）

介護保険サービスの請求事務

I 介護事業所では、利用者の個人情報の利用目的として「介護保険サービスの請求事務のため」と明示しています。介護報酬の請求に必要な情報を保険者（市町村等）に提供する目的であることが明確に示されているため、利用目的の特定として適切です。

【具体的に利用目的を特定していない事例】

（事例 1）

介護に関するあらゆる目的のため

J 訪問介護事業所では、利用目的を「介護に関するあらゆる目的のため」と表記しています。この表現では、どのような場面で、どのような目的に個人情報が使用されるのか具体性がなく、利用者は自分の情報の使われ方を予測できません。このような抽象的で広範な表現は、利用目的の特定の観点として不適切といえます。

（事例 2）

より良いサービス提供のため

K 通所リハビリテーション事業所では、利用目的を「より良いサービス提供のため」と記載しています。この表現は漠然としており、具体的にどのようなサービスの、どのような改善のために個人情報を利用するのかが明確ではありません。このような曖昧な表現は、利用目的の特定の観点として不適切です。

利用目的による制限の例外（法第 18 条第 3 項関係）

(1)法令に基づく場合（法第 18 条第 3 項第 1 号関係）

（事例 1）

介護事業所の従業者が高齢者虐待を発見した場合（高齢者虐待の防止、高齢者の養護者に対する支援等に関する法律 第 7 条）

L グループホームの介護職員は、利用者 A さんの身体に不自然なあざを発見し、家族による虐待を疑いました。職員は「高齢者虐待の防止、高齢者の養護者に対する支援等に関する法律」第 7 条に基づき、A さんの同意を得ることなく、市町村の高齢者虐待対応窓口に通報し、A さんの身体状況や生活歴等の情報を提供しました。このような法令に基づく通報は、本人の同意がなくても行うことができます。

（事例 2）

介護事業所で感染症が発生した場合（感染症の予防及び感染症の患者に対する医療に関する法律 第 12 条）

M 特別養護老人ホームでは、入所者の間でインフルエンザの集団感染が発生しました。施設長は「感染症の予防及び感染症の患者に対する医療に関する法律」第 12 条に基づき、感染者の情報（氏名、年齢、症状等）を保健所に届け出ました。この届出は法令に基づくものであり、感染者本人の同意がなくても行うことができます。

（事例 3）

介護サービス提供中に事故が起きた場合（介護保険法 第23条）
N訪問介護事業所のヘルパーが利用者Bさん宅でサービス提供中、Bさんが転倒し骨折する事故が発生しました。事業所管理者は「介護保険法」第23条に基づき、市町村に事故報告書を提出し、Bさんの情報（氏名、年齢、要介護度、事故状況等）を報告しました。このような法令に基づく報告は、本人の同意がなくても行うことができます。

（事例4）
都道府県知事等による立入検査時に、必要な書類の提出や質問への回答を行う場合（介護保険法 第24条）
O居宅介護支援事業所に都道府県の介護保険指導監査が入りました。監査担当者から特定利用者のケアプランや訪問記録の提示を求められたため、「介護保険法」第24条に基づき、本人の同意なく必要書類を提出し、質問に回答しました。法令に基づく立入検査への対応として、本人の同意がなくても情報提供を行うことができます。

(2)人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき（法第18条第3項第2号関係）
（事例1）
利用者が行方不明になった際、警察や地域の協力者に個人情報（写真、特徴等）を提供する場合（個人情報保護法 第18条第3項第2号）
P認知症グループホームの利用者Cさん（85歳・認知症）が散歩中に行方不明になりました。施設職員は、Cさんの写真や身体的特徴、服装等の情報を警察や地域の協力者に提供し、捜索協力を依頼しました。Cさんは認知症のため同意を得ることが困難な状況でしたが、安全確保のために必要な対応として、個人情報保護法第18条第3項第2号に基づき、情報提供が可能な事例といえます。

（事例2）
高齢者虐待が疑われる状況を発見した際、本人の同意なく関係機関に通報する場合（高齢者虐待の防止、高齢者の養護者に対する支援等に関する法律 第7条）
Q訪問介護事業所のヘルパーは、利用者Dさん宅で訪問介護サービスを提供中、Dさんの身体に不自然なあざを発見し、同居家族による虐待を疑いました。Dさんは日頃から家族を恐れており、通報に同意することを不安視していたため、ヘルパーは高齢者虐待の防止、高齢者の養護者に対する支援等に関する法律第7条に基づき、Dさんの同意を得ることなく市町村に通報し必要と判断し、情報提供を行いました。

（事例3）
利用者が急病で意識不明の際、救急搬送先の病院に既往歴や服薬情報を提供する場合（個人情報保護法 第18条第3項第2号）
R特別養護老人ホームの入所者Eさんが突然意識を失い、救急車で搬送されることになりました。施設職員は、Eさんの既往歴、服薬情報、アレルギー情報等を救急隊員や搬送先の病院に提供しました。Eさんは意識不明で同意を得ることができない状況でしたが、生命・身体の保護のために緊急の対応が必要と判断し、個人情報保護法第18条第3項第2号に基づき、情報提供を行った事例です。

（事例4）
大規模災害発生時、利用者の安否を確認するため、自治体や家族に情報を提供する場合（災害対策基本法 第49条の11）
S市で大規模地震が発生し、T居宅介護支援事業所は担当利用者の安否確認を行いました。連絡が取れない利用者については、市の災害対策本部や家族に対して、住所や要介護度、医療依存度等の情報を提供し、優先的な救助や安否確認を要請しました。災害の混乱の中で利用者全員から同意を得ることは困難でしたが、災害対策基本法第49条の11に基づく対応として、情報提供が可能な事例といえます。

（事例5）

認知症の利用者の財産が不正に使用されている疑いがある際、成年後見人や関係機関に情報を提供する場合（個人情報保護法 第18条第3項第2号）

U特別養護老人ホームの生活相談員は、入所者のFさん（重度の認知症）の利用料支払いが数か月滞っていることに気づきました。確認すると、Fさんの年金が入金される通帳を管理している息子が、その年金をFさんの施設利用料ではなく自身の生活費に使っていることが判明しました。Fさんは認知症のため状況を理解できず同意を得ることが困難なため、生活相談員は経済的虐待案件として地域包括支援センターや成年後見センターに相談し、Fさんの経済状況や生活状況に関する情報を提供しました。Fさんの財産と生活を守るために必要な対応として、個人情報保護法第18条第3項第2号に基づき、本人の同意なく情報提供が可能でした。

(3)公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき（法第18条第3項第3号関係）

（事例1）

介護施設内で感染症が発生した際、感染拡大防止のため、保健所や他の利用者、その家族に対して、感染者の情報（年齢、性別、症状等）を提供する場合（感染症の予防及び感染症の患者に対する医療に関する法律 第12条）

V特別養護老人ホームでは、入所者の間で新型コロナウイルス感染症のクラスターが発生しました。施設長は感染拡大防止のため、感染者の情報（年齢、性別、症状、行動歴等）を保健所に報告するとともに、他の入所者やその家族に対しても、個人が特定されない形で感染状況に関する情報を提供しました。感染者の中には認知症などにより同意能力がない方も含まれていましたが、感染症の予防及び感染症の患者に対する医療に関する法律第12条に基づく対応として、また公衆衛生の向上のために特に必要な場合として、本人の同意なく情報提供が可能でした。

（事例2）

介護サービス利用者の家庭内で児童虐待が疑われる際、児童相談所等に情報を提供する場合（児童虐待の防止等に関する法律 第6条）

W訪問介護事業所のヘルパーが、高齢の利用者G氏宅でサービスを提供している際、同居する小学生の孫に不自然なあざがあることや、極端に痩せていることに気づきました。G氏は認知症があり状況を十分に理解できず、また児童本人に状況を確認しようにも怖がってしまい、詳しく話そうとしません。ヘルパーは児童虐待の防止等に関する法律第6条に基づき、また児童の健全な育成の推進のために特に必要な事例であると判断し、G氏や児童本人の同意なく児童相談所に情報提供を行いました。

(4)国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して、事業者が協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき（法第18条第3項第4号関係）

（事例）

介護施設が地方自治体から委託を受けて行っている高齢者の健康管理や福祉サービスの提供において、施設が民間の医療機関や医療サービス提供者と連携する場合

- X市から介護予防事業を受託しているY通所介護事業所では、市の健康増進計画に基づく高齢者の健康状態調査に協力することになりました。この調査では、Y事業所の利用者の健康データを市に提供するとともに、必要に応じて地域の医療機関と連携して健康指導を行うことが求められています。対象となる高齢者の中には認知症等により同意能力が十分でない方も含まれていますが、X市の法令に基づく事務の遂行に協力するために必要な場合として、本人の同意なく情報連携を行うことが可能でした。

(5) 当該個人情報取扱事業者が学術研究機関等である場合であって、当該個人情報を学術研究の用に供する目的（以下この章において「学術研究目的」という。）で取り扱う必要があるとき（当該個人情報を取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）（法第18条第3項第5号関係）

（事例）

Z 大学介護福祉学部（学術研究機関）では、高齢者の筋力低下予防に関する研究を行っています。この研究では、大学が運営する介護予防教室の利用者データを分析していますが、一部の高齢者は認知症等により研究目的での個人情報利用に対する同意能力が十分でない状況です。Z 大学は、個人情報の匿名化処理を行い、個人を特定できないようにするなど、個人の権利利益を不当に侵害しないための措置を講じた上で、学術研究目的として本人の同意なく情報を利用することが可能な事例です。

(6)学術研究機関等に個人データを提供する場合であって、当該学術研究機関等が当該個人データを学術研究目的で取り扱う必要があるとき（当該個人データを取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）（法第 18 条第 3 項第 6 号関係）

（事例）

AA 介護老人保健施設では、認知症ケアの質向上を目的として、BB 大学医学部（学術研究機関）の研究プロジェクトに協力し、施設利用者の認知機能評価データを提供することになりました。利用者の中には進行した認知症により研究目的での情報提供に同意する能力がない方もいましたが、BB 大学が提供データを匿名化し研究倫理審査委員会の承認を得るなど、個人の権利利益を不当に侵害しないための措置を講じていることを確認した上で、AA 施設は学術研究目的として本人の同意なく情報を提供しました。

<u>不適正利用の禁止（法第 19 条関係）</u>

【個人情報取扱事業者が違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用している事例】

(事例 1)

認知症の利用者の資産状況を把握し、不必要なサービスや物品の購入を勧める場合（個人情報保護法第 19 条）

CC 介護サービス事業所の営業担当者は、認知症の H さんの資産状況（預金額や不動産所有状況等）を把握していました。担当者は H さんの判断能力の低下につけ込み、実際には必要のない高額な介護サービスプランや高級な福祉用具の購入を繰り返し勧めました。このような、認知症による判断力の低下を利用した不必要なサービス・物品の勧誘は、個人情報保護法第 19 条「個人情報の不適正な利用」に抵触する可能性があります。

（事例 2）

特定の疾患や障害を持つ利用者の情報を、不当なサービス制限や差別的対応の根拠として利用する場合（個人情報保護法 第 19 条、障害者差別解消法 第 8 条）

DD 訪問介護事業所では、利用者の医療情報から精神疾患の既往があることを知り、「対応が難しい」という理由で、他の利用者よりもサービス提供時間を短縮したり、特定のヘルパーのみを担当させたりするといった制限を設けていました。このような、障害を理由とした不当なサービス制限は、個人情報の不適正な利用だけでなく、障害者差別解消法第 8 条に抵触する可能性もあります。

（事例 3）

利用者の私生活に関する情報を、本人の同意なく他の利用者や第三者に漏らす場合（個人情報保護法第 19 条）

EE 通所介護事業所の職員は、利用者 I さんから離婚歴や家族との確執などのプライバシーに関する情報を知り得る立場にありました。この職員は、I さんの同意なく、これらの私生活に関する情報を他の利用者に漏らし、噂の種にしていました。このような、本人の同意なく私生活の情報を第三者に漏らす行為は、個人情報の不適正な利用に該当します。

（事例 4）

利用者の家族構成や収入状況を利用して、必要以上の高額サービスを執拗に勧める場合（個人情報保護法 第 19 条、老人福祉法 第 10 条の 4）

FF 居宅介護支援事業所のケアマネージャーは、担当利用者の収入や家族構成を把握する立場にありました。このケアマネージャーは、独居で年金収入が多い利用者を狙い、実際の介護ニーズを超えた過剰な

サービスプランを作成し、事業所の売上増加を図っていました。このような、利用者の経済状況を利用した必要以上のサービス勧誘は、個人情報の不適正な利用であるとともに、老人福祉法第 10 条の 4（心身の状況や環境に応じた適切な福祉サービスの提供）に反する行為です。

（事例 5）

利用者の政治的傾向や宗教に関する情報を利用して、特定の政党や宗教団体への加入を勧める場合（個人情報保護法 第 19 条）

GG 介護施設の管理者は、施設利用者の政治的傾向や宗教観に関する情報を収集し、特定の政党や宗教団体に近い思想を持つ利用者に対して、施設内で政治活動や宗教活動への参加を勧めていました。このような、利用者の思想・信条に関する情報を利用した特定の政治活動や宗教活動への勧誘は、個人情報の不適正な利用に該当します。

（事例 6）

採用活動において、応募者の病歴や家族の犯罪歴などをインターネットで調査し、採用の可否を決定する場合（個人情報保護法 第 19 条、職業安定法 第 5 条の 4）

HH 介護事業所の採用担当者は、職員採用の際、応募者の SNS を無断で調査し、過去の病歴や家族の犯罪歴などの情報を収集して、採用の可否判断に利用していました。このような、本人が提供していない機微な個人情報をインターネットで調査し、採用選考に利用する行為は、個人情報の不適正な利用であるとともに、職業安定法第 5 条の 4（求職者等の個人情報の取扱い）に違反する可能性もあります。

適正取得（法第 20 条第 1 項関係）

【個人情報取扱事業者が不正の手段により個人情報を取得している事例】

（事例 1）

介護サービスの提供を装って、実際は営業や勧誘目的で個人情報を収集する場合（個人情報保護法 第 20 条第 1 項）

II 介護関連会社の営業担当者は、「地域の高齢者実態調査」と称して戸別訪問し、介護サービスに関するアンケートを実施しました。しかし実際は、新規サービスの営業リストを作成するための情報収集が目的であったことが確認されました。このように、サービス提供や公的調査を装って、実際は営業や勧誘目的で個人情報を収集することは、偽りによる不正な手段での個人情報取得に該当します。

（事例 2）

利用者や家族の会話を無断で録音したり、隠しカメラで撮影したりして情報を取得する場合（個人情報保護法 第 20 条第 1 項、刑法 第 235 条）

JJ 訪問介護事業所の職員は、利用者宅での会話内容を、利用者や家族に知らせずに録音していました。また、別の職員は利用者宅のリビングに、本人に告げずに小型カメラを設置し、利用者の普段の生活の様子を撮影していました。このような、本人の同意なく会話を録音したり、隠しカメラで撮影したりする行為は、不正な手段による個人情報取得に該当するとともに、刑法第 235 条（住居侵入等）に違反する可能性もあります。

（事例 3）

他の介護事業所や行政機関になりすまして、利用者や家族から個人情報を騙し取る場合（個人情報保護法 第 20 条第 1 項）

KK 介護用品販売会社の従業員が、地域包括支援センターの職員を装って高齢者宅を訪問し、「介護保険サービスの利用状況調査」と称して、自社の営業目的として家族構成や収入、資産状況などの情報を聞き出していました。このように、公的機関や他の事業所になりすまして個人情報を騙し取る行為は、偽りによる不正な手段での個人情報取得に該当します。

（事例 4）

介護支援専門員が、担当外の利用者の情報を無断で閲覧・取得する場合（個人情報保護法 第 20 条第 1 項）

LL 居宅介護支援事業所のマネージャーが、利用者の知人について情報を得るため、同僚が担当する利用者の介護記録を、業務上の必要性がないにもかかわらず無断で閲覧していました。このように正当な業務の範囲を超えてアクセスし、個人情報を閲覧・取得する行為は、不正な手段による個人情報取得に該当します。

（事例 5）

利用者や家族の SNS アカウントに不正にアクセスし、個人情報を取得する場合（個人情報保護法 第 20 条第 1 項、不正アクセス禁止法 第 3 条）

MM 介護事業所の元従業員は、退職後も以前の業務用アカウントを使って利用者情報にアクセスし続けていました。また、別の従業員は利用者家族の SNS アカウントのパスワードを不正に入手し、プライベートな投稿内容を閲覧していました。このような不正アクセスによる情報取得は、不正アクセス禁止法第 3 条に違反するとともに、個人情報の不正取得に該当します。

（事例 6）

採用活動において、応募者の同意なく、過去の病歴や家族の情報を調査会社を使って収集する場合（個人情報保護法 第 20 条第 1 項、職業安定法 第 5 条の 4）

適正取得（法第 20 条第 1 項関係）に関するよくある事例は、以下のとおりです。

個人情報取扱事業者は、偽り等の不正の手段により個人情報を取得してはなりません。

NN 介護事業所の採用担当者は、新規職員の採用選考において、応募者の知らないうちに調査会社を使って過去の病歴や家族の情報、借金の有無などを調査していました。このような応募者の同意を得ない秘密裏の調査は、不正な手段による個人情報取得に該当するとともに、職業安定法第 5 条の 4（求職者等の個人情報の取扱い）に違反する可能性もあります。

<u>要配慮個人情報の取得（法第 20 条第 2 項関係）</u>

(1)法令に基づく場合（法第 20 条第 2 項第 1 号関係）

（事例 1）

虐待を受けたと思われる高齢者の身体状況や障害の状況などの情報を、市町村に通報する場合（高齢者虐待の防止、高齢者の養護者に対する支援等に関する法律 第 7 条）

OO 特別養護老人ホームの介護職員は、新規入所者 J さんの入浴介助の際、背中に複数の打撲痕を発見しました。以前の施設での虐待が疑われたため、「高齢者虐待の防止、高齢者の養護者に対する支援等に関する法律」第 7 条に基づき、J さんの同意を得ることなく、身体状況や障害の状況、認知症の程度などの要配慮個人情報を市町村の高齢者虐待対応窓口に通報しました。法令に基づく通報であるため、本人の同意がなくても要配慮個人情報を取得・提供することが可能です。

（事例 2）

介護施設内で感染症が発生した際、感染者の病状や検査結果などの情報を保健所に届け出る場合（感染症の予防及び感染症の患者に対する医療に関する法律 第 12 条）

PP 介護老人保健施設では、入所者の間で結核の集団感染が発生しました。施設長は「感染症の予防及び感染症の患者に対する医療に関する法律」第 12 条に基づき、感染者の病状や検査結果、基礎疾患などの要配慮個人情報を保健所に届け出ました。法令に基づく届出であるため、本人の同意がなくても要配慮個人情報を取得・提供することが可能です。

（事例 3）

市町村が行う要介護認定調査において、本人の心身の状況や疾病の状況などの情報を提供する場合（介護保険法 第 27 条）

QQ 居宅介護支援事業所のマネージャーは、要介護認定を申請した利用者 K さんの調査に立ち会いました。市町村の認定調査員に対して、「介護保険法」第 27 条に基づき、K さんの心身の状況や疾病の状況、日常生活動作の自立度などの要配慮個人情報を提供しました。法令に基づく調査協力であるため、本人の同意なく要配慮個人情報を取得・提供することが可能です。

（事例 4）

介護サービス提供中の事故について、利用者の障害や疾病の状況を含む報告を市町村に行う場合（介護保険法 第 23 条）

RR 通所介護事業所では、送迎中に利用者 L さん（パーキンソン病を患っている）が車内で転倒し、骨折する事故が発生しました。事業所管理者は「介護保険法」第 23 条に基づき、市町村に事故報告書を提出し、L さんの疾病の状況や障害の程度などの要配慮個人情報を報告しました。法令に基づく報告であるため、本人の同意なく要配慮個人情報を取得・提供することが可能です。

（事例 5）

障害福祉サービスの利用申請時に、障害の状況や医療情報などを市町村に提供する場合（障害者総合支援法 第 20 条）

SS 相談支援専門員は、新たに障害福祉サービスを利用することになった M さん（精神障害がある）の支援のため、「障害者総合支援法」第 20 条に基づく支給申請手続きを援助しました。この過程で、M さんの障害の状況や医療情報、生活歴などの要配慮個人情報を市町村に提供しました。法令に基づく申請手続きであるため、本人の同意なく要配慮個人情報を取得・提供することが可能です。

(2)人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき（法第 20 条第 2 項第 2 号関係）

（事例 1）

認知症の利用者が行方不明になった際、その方の病状や身体的特徴などの情報を警察や地域の協力者に提供する場合（個人情報保護法 第 20 条第 2 項第 2 号）

TT 認知症グループホームに入居している N さん（重度の認知症、持病に糖尿病あり）が、施設の見守りをすり抜けて外出し、行方不明になりました。施設職員は早急な捜索が必要と判断し、N さんの同意を得ることなく、警察や地域住民に対して、N さんの病状（認知症・糖尿病の状態）や必要な投薬情報、身体的特徴などの要配慮個人情報を提供しました。N さんは認知症のため同意を得ることが困難であり、また生命・身体の保護のために必要であるため、本人の同意なく要配慮個人情報を取得・提供することが可能です。

（事例 2）

利用者が急病で意識不明の状態になった際、その方の既往歴や服薬情報、アレルギー情報などを救急搬送先の病院に提供する場合（個人情報保護法 第 20 条第 2 項第 2 号）

UU 通所リハビリテーション施設で、利用者 O さんが突然意識を失い、呼吸が不安定になりました。施設職員は救急車を要請するとともに、O さんの診療情報提供書から既往歴（脳梗塞・心臓病）や服薬情報、アレルギー情報などの要配慮個人情報を救急隊員と搬送先の病院に提供しました。O さんは意識不明で同意を得ることができず、また緊急の医療処置のために必要な情報であるため、本人の同意なく要配慮個人情報を取得・提供することが可能です。

（事例 3）

大規模災害発生時、避難支援が必要な利用者の障害状況や医療的ケアの必要性などの情報を、自治体や避難支援者に提供する場合（災害対策基本法 第 49 条の 11）

VV 市で大規模地震が発生し、WW 居宅介護支援事業所は担当する重度障害のある利用者の安否確認と避難支援を行うことになりました。マネージャーは、自治体の災害対策本部や避難所スタッフに対して、人工呼吸器を使用している利用者や透析が必要な利用者などの医療的ケアの必要性や障害の状況に関する要配慮個人情報を提供しました。災害時で本人の同意を得ることが困難であり、また避難支援のために必要であるため、災害対策基本法第 49 条の 11 に基づき、本人の同意なく要配慮個人情報を取得・提供することが可能でした。

(3)公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき（法第 20 条第 2 項第 3 号関係）

（事例）

介護サービス利用者の家庭内で児童虐待が疑われる際、その児童の心身の状況や家庭環境などの情報を収集し、児童相談所等に提供する場合（個人情報保護法 第20条第2項第3号、児童虐待の防止等に関する法律 第6条）
XX訪問介護事業所のヘルパーが、高齢の利用者Pさん宅での介護サービス提供中、同居する小学生の孫に不自然なあざがあることや、極端に痩せていること、適切な医療を受けられていない様子に気づきました。ヘルパーは児童虐待を疑い、児童相談所に通報するとともに、その児童の心身の状況（体重減少、あざの状態、持病の治療状況など）や家庭環境に関する要配慮個人情報を提供しました。児童本人から同意を得ることは困難であり、また児童の健全な育成のために特に必要であるため、児童虐待の防止等に関する法律第6条に基づき、本人の同意なく要配慮個人情報を取得・提供することが可能です。

(4)国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して、事業者が協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき（法第20条第2項第4号関係）

（事例1）

保健所が行う感染症の疫学調査に協力し、感染者や濃厚接触者の健康状態、基礎疾患、行動履歴などの情報を提供する場合（個人情報保護法 第20条第2項第4号、感染症の予防及び感染症の患者に対する医療に関する法律 第15条）
YY介護老人保健施設では、入所者と職員の間で新型コロナウイルス感染症のクラスターが発生しました。管轄の保健所は感染症の予防及び感染症の患者に対する医療に関する法律第15条に基づき、クラスターの発生状況と感染経路の調査を開始しました。施設は保健所の疫学調査に協力し、感染者や濃厚接触者の健康状態、基礎疾患（糖尿病、心臓病など）、行動履歴などの要配慮個人情報を提供しました。緊急を要する感染拡大防止のための調査であり、全ての関係者から同意を得ることが時間的に困難であったため、本人の同意なく要配慮個人情報を提供することが可能でした。

（事例2）

災害対策基本法に基づく避難行動要支援者名簿の作成のため、市町村からの求めに応じて利用者の障害の状況、医療依存度などの情報を提供する場合（個人情報保護法 第20条第2項第4号、災害対策基本法 第49条の10）
ZZ市では、災害対策基本法第49条の10に基づき、避難行動要支援者名簿の作成を進めていました。市内のAAA居宅介護支援事業所は、市からの求めに応じて、担当する要介護高齢者や障害者の情報（障害の状況、医療依存度、日常生活自立度など）を提供しました。この情報には、人工呼吸器の使用や重度の認知症といった要配慮個人情報が含まれていましたが、災害時の迅速な避難支援のために必要な情報であり、すべての利用者から同意を得ることが実務上困難であったため、本人の同意なく要配慮個人情報を提供することが可能でした。

(5)当該個人情報取扱事業者が学術研究機関等である場合であって、当該要配慮個人情報を学術研究目的で取り扱う必要があるとき（当該要配慮個人情報を取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）（法第20条第2項第5号）

（事例）

BBB福祉大学（学術研究機関）の老年学研究センターでは、認知症の進行を遅らせるケア方法の研究を行っています。この研究では、大学が運営する介護施設の利用者の認知機能評価データ、既往歴、投薬情報など、認知症に関連する要配慮個人情報を収集・分析しています。研究対象となる高齢者の中には、認知症が進行しており本人から研究目的での情報利用に関する同意を得ることが困難な方が含まれています。

この場合、BBB福祉大学は以下の条件を満たすことで、本人の同意なく要配慮個人情報を取得することが可能です。
・学術研究機関としての立場で研究を行っていること
・認知症ケア研究という学術研究目的で情報を取り扱うこと
・収集するデータは研究に必要な範囲に限定していること
・個人を特定できないよう匿名化処理を行うこと

・研究倫理委員会の承認を得ていること
・研究結果は学術的な文脈でのみ公表すること

(6)学術研究機関等から当該要配慮個人情報を取得する場合であって、当該要配慮個人情報を学術研究目的で取得する必要があるとき（当該要配慮個人情報を取得する目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）（当該個人情報取扱事業者と当該学術研究機関等が共同して学術研究を行う場合に限る。）（法第 20 条第 2 項第 6 号関係）

（事例）

CCC 介護福祉法人（個人情報取扱事業者）は、DDD 医科大学（学術研究機関）と共同で「認知症高齢者の住環境改善に関する研究」を実施することになりました。この研究では、DDD 医科大学が過去の研究で収集した認知症患者の症状進行データ、生活環境評価、医療診断情報などの要配慮個人情報を、CCC 介護福祉法人が取得して分析することになりました。

この事例では、以下の条件を満たすことで、本人の同意なく要配慮個人情報を取得することが可能です。
・CCC 介護福祉法人と DDD 医科大学が正式な共同研究契約を締結していること
・取得する情報は学術研究目的（認知症ケア環境の改善研究）で必要なものに限定されていること
・個人を特定できないよう適切な匿名化処理がされていること
・研究倫理委員会の承認を得ていること
・情報セキュリティ対策が講じられていること

(7)当該要配慮個人情報が、本人、国の機関、地方公共団体、学術研究機関等、法第 57 条第 1 項各号に掲げる者その他個人情報保護委員会規則で定める者により公開されている場合（法第 20 条第 2 項第 7 号、規則第 6 条関係）

（事例 1）

車椅子を使用する障害当事者 Q さんが、自身のブログや SNS で「車椅子利用者の視点から見た介護サービスの課題」というテーマで情報発信をしています。EEE 介護事業所は、サービス改善のため Q さんの投稿内容（障害の種類、程度、日常生活での困難など）を参考資料として収集しました。これらは要配慮個人情報に該当しますが、Q さん自身が公開している情報であるため、改めて同意を得ることなく取得することが可能でした。

（事例 2）

FFF 市は「高齢者・障害者福祉計画」の策定過程で、一部の当事者の了解を得て、実際の介護事例（医療的ケアが必要な障害者の生活状況など）を市のウェブサイトで公開しました。GGG 介護事業所は、自社の介護職員研修用の事例集を作成するため、この公開情報を収集・活用しました。地方公共団体が公開している要配慮個人情報であるため、改めて本人の同意を得ることなく取得することが可能でした。

（事例 3）

全国紙の新聞で「難病と闘いながら社会活動を続ける高齢者」という特集記事が掲載され、特定の個人の病歴や治療状況などが本人の承諾のもとで詳しく紹介されました。HHH 介護事業所は、職員向けの事例研究会で、この記事の内容を教材として使用しました。報道機関により公開された要配慮個人情報であるため、改めて本人の同意を得ることなく取得することが可能でした。

(8)本人を目視し、又は撮影することにより、その外形上明らかな要配慮個人情報を取得する場合（法第 20 条第 2 項第 8 号、政令第 9 条第 1 号関係）

（事例 1）

車椅子を使用している利用者が来所した際、移動に関する障害があることを視認により把握し、記録する場合（個人情報保護法 第 20 条第 2 項）

III 通所介護事業所では、新規利用者の R さんが車椅子を使用して来所しました。受付担当者は、R さんが車椅子を使用していることから移動に関する障害があることを視認により把握し、施設内での移動

支援やトイレ介助などの適切なサービス提供のため、この情報を利用者記録に記載しました。車椅子の使用という外形上明らかな要配慮個人情報については、視認により取得する場合、本人の同意なく記録することが可能でした。

（事例 2）

白杖を使用している利用者が来所した際、視覚障害があることを視認により把握し、適切な介助を行うために記録する場合（個人情報保護法 第 20 条第 2 項）

JJJ 訪問介護事業所に相談に訪れた S さんは、白杖を使用していました。相談員は、S さんが白杖を使用していることから視覚障害があることを視認により把握し、適切な案内や介助を行うために、この情報を相談記録に記載しました。さらに、今後のサービス提供に備えて「視覚障害に配慮した環境整備と声かけが必要」と支援計画メモに記録しました。白杖の使用という外形上明らかな要配慮個人情報については、視認により取得する場合、本人の同意なく記録することが可能でした。

(9)法第 27 条第 5 項各号（法第 41 条第 6 項の規定により読み替えて適用する場合及び法第 42 条第 2 項において読み替えて準用する場合を含む。）に掲げる場合において、個人データである要配慮個人情報の提供を受けるとき（法第 20 条第 2 項第 8 号、政令第 9 条第 2 号関係）

（事例 1）

KKK 医療法人は、入院患者の退院後の在宅ケア支援のため、LLL 訪問看護ステーションに訪問看護業務を委託しました。この委託に伴い、LLL 訪問看護ステーションは患者 T さんの病歴、現在の治療内容、リハビリテーション計画などの要配慮個人情報の提供を受けました。この情報提供は、法第 27 条第 5 項第 1 号の「個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの委託をする場合」に該当するため、T さん本人の同意を改めて得ることなく、要配慮個人情報を取得することが可能でした。

（事例 2）

MMM 介護事業所は経営難のため、NNN 福祉法人に事業を譲渡することになりました。事業承継に伴い、NNN 福祉法人は MMM 介護事業所の利用者情報（要介護度、疾病の状況、障害の種類と程度などの要配慮個人情報を含む）の提供を受けました。この情報提供は、法第 27 条第 5 項第 2 号の「合併その他の事由による事業の承継に伴って個人データが提供される場合」に該当するため、利用者本人の同意を改めて得ることなく、要配慮個人情報を取得することが可能でした。

（事例 3）

OOO 地域包括ケアシステムの一環として、PPP 市内の医療機関、介護事業所、薬局などが利用者情報を共同利用する取り組みを行っています。この取り組みでは、事前に共同利用する旨を公表し、QQQ 訪問介護事業所は、同じ利用者を担当する RRR 診療所から、利用者 U さんの病名、処方薬情報、リハビリテーション計画などの要配慮個人情報の提供を受けました。この情報提供は、法第 27 条第 5 項第 3 号の「特定の者との間で共同して利用される個人データが当該特定の者に提供される場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき」に該当するため、U さん本人の同意を改めて得ることなく、要配慮個人情報を取得することが可能でした。

【法第 20 条第 2 項に違反している事例】

介護サービスの提供に直接関係のない過去の病歴や治療歴を、本人の同意なく詳細に聞き取り、記録する。（個人情報保護法 第 20 条第 2 項）

（事例 1）

初回の介護サービス利用時に、利用者の個人情報の利用目的を説明し、書面で通知する場合（個人情報保護法 第 21 条第 1 項）

TTT 訪問介護事業所では、新規利用者 W さんが初めてサービスを利用する際、担当者が個人情報の利用目的について詳しく説明しました。「ケアプラン作成」「サービス担当者会議での情報共有」「介護報酬

請求事務」などの具体的な利用目的を記載した文書を交付し、W さんの理解を確認しました。このように、初回サービス利用時に利用目的を書面で通知することで、個人情報の取扱いの透明性を確保しています。

（事例 2）
提供するサービスの内容が変更され、それに伴い個人情報の利用目的が拡大する場合、変更後の利用目的を通知または公表する場合（個人情報保護法 第 21 条第 3 項）
UUU 通所介護事業所では、従来の介護サービスに加えて、新たに送迎サービスと食事宅配サービスを開始することになりました。これに伴い、利用者の自宅周辺の道路状況や、食物アレルギー・嗜好などの追加情報を取得する必要が生じたため、変更後の利用目的（「安全な送迎サービス提供のための道路情報の利用」「食事宅配サービスにおける適切な食事提供のための情報利用」）を文書で通知するとともに、施設内の掲示板に掲載して公表しました。

（事例 3）
新たに電子的な介護記録システムを導入する際、個人情報の取り扱い方法の変更について利用者に通知する場合（個人情報保護法 第 21 条第 1 項）
VVV 特別養護老人ホームでは、紙媒体の介護記録から電子的な介護記録システムへの移行を行うことになりました。新システムでは、利用者情報がクラウド上で管理され、関係職種間で共有されることになるため、個人情報の取扱い方法が変更されることを利用者と家族に通知しました。通知内容には、情報セキュリティ対策の強化や、情報アクセス権限の設定など、電子化に伴う安全管理措置についても説明が含まれていました。

（事例 4）
匿名化したデータを外部機関による評価や研究に利用する際、その目的を施設内に掲示して公表する場合（個人情報保護法 第 21 条第 1 項）
WWW 介護老人保健施設では、施設内のケアの質向上のため、蓄積された介護データを匿名化した上で外部の研究機関に提供し、分析評価を依頼することになりました。施設は「匿名化した介護データの研究利用について」という掲示を施設内の掲示板に掲出し、「介護データの匿名化方法」「研究の目的と内容」「外部機関の名称」「個人を特定しない形での利用」などを明記して公表しました。

（事例 5）
介護実習生を受け入れる際、実習生が利用者の個人情報を取り扱うことについて、利用者に通知する場合（個人情報保護法 第 21 条第 1 項）
XXX 介護事業所では、地元の介護福祉士養成学校から実習生を受け入れることになりました。実習生は利用者の介護記録を閲覧したり、ケアの様子を実習日誌に記録したりする必要があるため、事前に利用者全員に対して「実習生による個人情報取扱いのお知らせ」を配布し、実習の目的、期間、実習生が取り扱う情報の範囲、実習生の守秘義務などについて通知しました。

（事例 6）
地域の見守りネットワークに参加し利用者情報を共有する際、その目的と範囲を利用者に通知または公表する場合（個人情報保護法 第 21 条第 1 項）
YYY 居宅介護支援事業所では、地域の高齢者見守りネットワーク（地域包括支援センター、民生委員、コンビニ、郵便局等が連携）に参加することになりました。このネットワークでは、認知症高齢者の徘徊時の早期発見などのため、必要最小限の利用者情報（顔写真、氏名、年齢、身体的特徴等）を関係者間で共有します。事業所は、この取り組みについて「地域見守りネットワークへの参加と個人情報の共有について」という文書を作成し、利用者に通知するとともに、事業所内に掲示して公表しました。

直接書面等による取得（法第 21 条第 2 項関係）
【あらかじめ、本人に対し、その利用目的を明示しなければならない事例】
（事例 1）
利用者の既往歴や現在の治療状況などの医療情報を取得する場合（個人情報保護法 第 21 条第 2 項）

ZZZ 介護老人保健施設では、入所予定の X さんに「医療情報提供同意書」という書面を提示し、既往歴や現在の治療状況などの医療情報を記入してもらうことになりました。この書面には「記入いただいた医療情報は、適切な介護サービス提供、緊急時の医療連携、服薬管理のために利用します」と利用目的が明記されていました。このように、書面で要配慮個人情報を直接取得する場合は、あらかじめ利用目的を明示する必要があります。

（事例 2）

サービス向上のためのアンケート調査を実施する場合（個人情報保護法 第 21 条第 2 項）

AAAA 訪問介護事業所では、サービス向上のため利用者アンケートを実施することになりました。アンケート用紙の冒頭には「本アンケートで収集した情報は、サービス品質の評価・改善、職員研修の内容検討、新規サービス開発の参考とするために利用します。個人を特定した形での公表は行いません」と利用目的が明示されていました。このように、アンケート等の書面で個人情報を直接取得する場合は、あらかじめ利用目的を明示する必要があります。

（事例 3）

広報誌や SNS での使用を目的とした写真撮影を行う場合（個人情報保護法 第 21 条第 2 項）

BBBB 通所介護事業所では、季節のイベント（夏祭り）の様子を広報誌や SNS で紹介するための写真撮影を行うことになりました。撮影前に「写真撮影・利用に関する同意書」を利用者に提示し、「撮影した写真は、当事業所の広報誌、公式ウェブサイト、公式 SNS アカウントでの活動紹介のために利用します」と利用目的を明示しました。写真という個人情報を直接取得する場合も、あらかじめ利用目的を明示する必要があります。

（事例 4）

緊急時の連絡先情報を取得する場合（個人情報保護法 第 21 条第 2 項）

CCCC 居宅介護支援事業所では、新規利用者の緊急連絡先情報を「緊急連絡先登録票」という書面で収集していました。この書面には「ご記入いただいた連絡先情報は、利用者様の容態急変時や災害発生時などの緊急事態における連絡のみに使用します」と利用目的が明示されていました。他者（家族等）の個人情報を含む緊急連絡先を取得する場合も、あらかじめ利用目的を明示する必要があります。

【利用目的の明示に該当する事例】

（事例 1）

介護サービスの利用申込書に個人情報の利用目的を明記し、申込時に本人に確認してもらう場合（個人情報保護法 第 21 条第 2 項）

DDDD 介護事業所では、サービス利用申込書の冒頭部分に「個人情報の利用目的について」という項目を設け、「ご記入いただいた個人情報は、①介護サービス提供、②介護報酬の請求、③サービス担当者会議での情報共有、④緊急時の連絡、⑤サービス向上のための統計分析のために利用します」と明記していました。利用者はこの内容を確認した上で申込書に署名しています。このように、申込書に利用目的を明記し、本人に確認してもらうことは、適切な利用目的の明示方法です。

（事例 2）

利用者の既往歴や現在の治療状況などの医療情報を取得する際、その利用目的を書面で明示する場合（個人情報保護法 第 21 条第 2 項）

EEEE 訪問看護ステーションでは、新規利用者の医療情報を収集する際、「医療情報提供依頼書」を使用しています。この書面の上部には「ご提供いただく医療情報（既往歴、服薬情報、アレルギー情報等）は、①適切な看護計画の作成、②医療機関との連携、③安全なケア提供、④緊急時の適切な対応のために利用します」と利用目的が太字で明示されています。このように、医療情報という要配慮個人情報を取得する際は、その利用目的を書面で明確に示すことが重要です。

（事例 3）

サービス記録や広報目的での写真・動画撮影時に、撮影同意書に利用目的を明記する場合（個人情報保護法 第 21 条第 2 項）

FFFF 介護老人福祉施設では、レクリエーション活動の様子を記録したり広報に使用したりするための写真・動画撮影を行う際、「撮影同意書」を用意しています。この同意書には「撮影した画像・映像は、①サービス記録としての利用、②施設内掲示による活動紹介、③広報誌への掲載、④公式ウェブサイトでの活動報告、⑤ご家族への活動報告のために利用します。この目的以外には使用しません」と詳細な利用目的が明記されています。このように、撮影同意書に具体的な利用目的を明記することで、本人が利用範囲を理解した上で同意できるようになります。

事例：

・携帯電話の紛失

私物スマートフォンを充電しようと、業務用パソコンに USB コネクタで接続したらデータの取り込みをしてしまい、どうしたらよいかわからずそのままにした。その後、そのスマートフォンを紛失してしまった。

利用者、家族、事業所スタッフの電話番号が入っていた業務用携帯電話を紛失。

利用者、家族、事業所スタッフの電話番号を私物携帯電話に登録していて、携帯電話を紛失した。

私物スマホの LINE で業務のやり取りをしていたが、引き継ぎをグループラインに、ながしたがそこに退職した職員がまだ参加していて情報が流出した。
私用スマートフォンの LINE で業務連絡等を行っていたが、退職者の残るグループ LINE に引き継ぎ情報を流した結果、情報が漏洩した。

・ウィルス感染

業務用パソコンでレクリエーションのポスターや動画を作成する際、利便性を優先するあまり編集ソフトなどのフリーソフトをインストールしたところ、ウィルスに感染してしまった。

業務での利用目的で事業所に Wi-Fi を導入したが、利用者などから Wi-Fi の利用希望が多く寄せられたため接続を解放した。その後、Wi-Fi 経由で事業所の端末がウィルス感染してしまった。

・個人情報が記録された USB メモリを紛失

(1)　個人情報を記録していた USB メモリを使用しようとしたところ、所定の保管場所に保管されていなかった。捜索するも発見できず、紛失してしてしまった。

(2)　リモートワークをするために、個人情報を記録した USB メモリを事業所外へ持ち出した。当該事業所では USB メモリの使用を禁じているにも関わらず実行し、結局紛失してしまった。

・単純な ID、パスワードなど

(1)　利用者やスタッフの個人情報が印刷され、外部に漏れてしまった。介護ソフトの設定にて ID ごとにアクセスできる範囲は制限されていた。操作履歴から、どのパソコンのどの ID から印刷されたかは判明したものの、該当スタッフは事故当日に公休で不在であり、漏洩経路等は結局不明のままであった。

(2)　備品などの購入目的に通販サイトにログインをして作業中、当該担当者は所用で離席した。席に戻ると身に覚えのない注文が大量にされていたことが発覚した。

・事業所の専用サイトの閲覧範囲

事業所の専用サイトで、利用者の家族が自分の家族の分のケアプランやケース記録を閲覧できるシステムを利用していた。しかし、閲覧範囲の誤設定があり身内ではない人のケース記録の閲覧ができる状態になっていた。

・メールファックス誤送信

月初に前月の利用実績票を FAX にて送信したが、誤って全く別の事業所に送信してしまったことが発覚した。

・バックアップ
停電でサーバーが壊れてしまい、バックアップがとれてなく情報が消滅した。
停電が原因でサーバーが故障し、バックアップを取っていなかったため、保存されていた情報が全て消失した。

・廃棄
廃棄予定のパソコンを紛失してしまった。

・退職者
デイサービスの職員が退職後に独立して自らデイサービスを立ち上げた。前事業所の利用者リストを持ち出して営業をかけていることが判明した。

デイサービスの元職員が退職後に独立し、自身のデイサービスを開業しました。その際、以前勤めていたデイサービスの利用者リストを無断で使用し、営業活動を行っていることがわかりました。

・書類の紛失
(1)　通院やサービス担当者会議で、個人情報が束ねられているファイルを事業所から持ち出した。その後どこに置いたかわからず紛失した。
(2)　事務所のキャビネットの中に入っていた個人情報が記載されているファイルがなくなっていた。キャビネットに鍵をかけていなかったことがのちに判明する。

・写真の無断流出
(1)　施設のパンフレットやチラシを作る際に、よく撮れた写真があったのでHPや広報用のチラシに掲載し多くの人の目に留まるようになった。家族(もしくはスタッフの場合もある）は承諾しておらず、苦情が入る。
施設のパンフレットやチラシを作る際、良い写真があったためホームページや広報用のチラシに掲載したところ、多くの人の目に触れるようになった。しかし、写真に写っている家族（またはスタッフ）からは掲載の許可を得ておらず、苦情が寄せられた。
(2)　レクリエーションで外出した際に、スタッフの私物スマホで写真を撮影していた。悪意なくスタッフ同士がLINEなどSNSで共有していたが、いつの間にか外部に漏れてしまった。
(3) レクリエーションで利用者の写真を撮った際に、仲の良い利用者Aさん、利用者Bさんが一緒に写真を撮ってAさん家族がその写真が素敵だったので欲しいと言われたので印刷してあげたら、Bさん家族からあげてほしくなかったとクレームになった。

レクリエーションで利用者の方々の写真を撮った。仲の良いAさんとBさんが一緒に写っている写真があり、Aさんのご家族がそれを気に入って欲しいと言われたので印刷して渡した。しかしその後、Bさんのご家族から、その写真を渡してほしくなかったという苦情があった。

・メモなど簡易的な書類の不適切な取扱い
(1)　メモ書きや印刷ミスした紙など、個人情報が記載されているものをシュレッダー 処理せずにそのままごみ箱に捨てていた。集積所でごみ袋に入っている紙に記載されている個人情報が外から見える状態になっていた。
(2)　経費節約の目的で、ミスコピーなどを裏紙コピーで利用していたが、個人情報が印刷してあるもので裏紙コピーをしてそのまま配布してしまった。
(3)　事務所内のホワイトボードや張り紙に個人情報が記載されており、来客から見える状態であった。

・スタッフの無造作な行為よる漏洩
(1)　事業所の近隣に住んでいるスタッフが、ご近所さんとの会話の中で「あそこの家のお祖母ちゃんがこの間、うちの施設に入所したんだよ。」と世間話をしていた。

事業所の近くに住むスタッフが、近所の人と話していた際、「先日、あそこの家のお祖母様がうちの施設に入所されたんですよ」と話していた。
(2) 事業所のスタッフ同士が公共交通機関で帰宅する際に、業務に関連する話をしていると、個人情報がほかの乗客に聞こえていた。
(3) 送迎をしているスタッフが、利用者を自宅に送っている際に「この家が、スタッフの〇〇さんの家なんですよ」と話してしまい、後日利用者がそのスタッフの家に手土産をもって訪ねてきてしまうことがあった。

・苦情に耐え切れず
(1) 利用者同士の喧嘩で、一方が相手に怪我をさせてしまい、怪我をさせられた利用者の家族が相手に謝罪を求めたいと強くクレーム。再三にわたる要求に相手の氏名を伝えてしまい、トラブルに発展した。
利用者同士が喧嘩になり、一方が相手に怪我を負わせた。怪我をした利用者の家族は、相手に謝罪を強く要求し、何度もクレームを申し立てた。再三の要求に対し、相手の氏名を伝えてしまったことで、トラブルがより深刻化した。

・郵送の送り先(中身間違い)
(1) 請求書を利用者家族に送付した際、封筒の中身をほかの利用者のものと入れ間違えて送付してしまった。

介護事業所における IT 機器の情報セキュリティ事例
（事例１）タブレット端末の紛失による個人情報漏えい
B ホームヘルパーステーションでは、ヘルパーが訪問介護時に利用者の状態や提供したサービス内容を記録するために、タブレット端末を使用しています。このタブレットには、利用者の氏名、住所、要介護度、既往歴、服薬情報などの個人情報が保存されています。あるヘルパーが訪問先から事務所に戻る途中でタブレット端末を紛失したため、パスワードロックや暗号化などの対策がされていなかったことから、保存されていた個人情報が漏えいするリスクが生じました。個人情報保護法第 23 条に基づく安全管理措置が十分でなかったため、法的責任が問われる可能性があります。これは物理的な紛失による IT 機器からの情報漏えい事例です。

（事例２）業務用パソコンのウイルス感染による情報流出
C 介護支援事業所では、ケアマネージャーがケアプラン作成や介護報酬請求のために業務用パソコンを使用しています。あるケアマネージャーが受信した「介護保険制度改正のお知らせ」という件名のメールに添付されたファイルを開いたところ、ウイルスに感染しました。このウイルスによって、パソコン内に保存していた利用者情報が外部に送信されてしまいました。個人情報保護法第 26 条に基づき、個人データの漏えい等が発生し個人の権利利益を害するおそれがある場合は、個人情報保護委員会への報告および本人への通知が必要となります。これはウイルス感染による IT 機器からの情報流出事例です。

（事例３）介護記録システムを提供するクラウドサービスの外国移転における法的問題
G 特別養護老人ホームでは、利用者の介護記録を管理するためクラウド型の介護記録システムを導入しています。このシステムは外国企業が提供するものであり、データは海外のサーバーに保存されています。個人情報保護法第 28 条では、外国にある第三者へ個人データを提供する場合、あらかじめ当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他本人に参考となる情報を提供したうえで本人の同意を得る必要があります。G 特別養護老人ホームは、この規定に基づいた対応ができておらず、法的リスクを抱えています。これはクラウドサービス利用における越境データ移転の法的問題事例です。

（事例４）介護施設における監視カメラの設置と個人情報保護
H 介護施設では、虐待防止や事故対応のため、施設内に監視カメラを設置しています。このカメラ映像は専用のデジタルレコーダーに記録され、施設長が管理するパソコンから閲覧可能です。映像には利用

者の日常生活の様子が記録されており、要介護状態や疾患の状況が推測できる場合もあるため、要配慮個人情報に該当する可能性があります。個人情報保護法第 20 条では、要配慮個人情報を取得する場合は本人の同意が必要と定めています。H 介護施設では、入所時に監視カメラの設置目的や映像の保存期間、閲覧権限などについて説明し、明示的な同意を得る書面を整備しています。これは IT 機器による要配慮個人情報の適法な取得事例です。

（事例５）自動記録システムによるバイタルサイン管理の共有ミス

J 介護老人保健施設では、利用者のバイタルサイン（血圧、体温、脈拍など）を自動測定し記録するシステムを導入しています。このシステムは施設内ネットワークで接続され、測定結果は利用者ごとにデータベース化されて医療スタッフ間で共有されています。ある日、システムの設定ミスにより、一部の利用者データが別の利用者のファイルに誤って記録されてしまいました。これに気づかなかった看護師が誤ったデータに基づいて対応したため、処置に一時的な混乱が生じました。個人情報保護法第 23 条では個人データの正確性の確保が求められており、システム管理においても定期的な点検や確認が必要です。これは IT 機器の設定ミスによる情報の完全性が損なわれた事例です。

（事例６）介護事業所での FAX 誤送信による個人情報漏えい

K 居宅介護支援事業所では、利用者の居宅サービス計画書を関係機関に送付する際に FAX 機能付きの複合機を使用しています。ある日、ケアマネージャーが急いでいた際に誤って番号を入力し、全く関係のない会社に FAX を送信してしまいました。送信した FAX には利用者の氏名、住所、要介護度、疾病情報など多くの個人情報が含まれていました。個人情報保護法第 23 条に基づく安全管理措置として、FAX 送信前の宛先確認手順の徹底や、可能な限り電子メールなど誤送信リスクの低い方法への移行が必要です。これは日常的に使用される IT 機器（FAX 複合機）の操作ミスによる情報漏えい事例です。

（事例７）電子カルテシステムの ID・パスワード共有による不正アクセス

A 訪問看護ステーションでは、利用者の医療情報管理のために電子カルテシステムを導入していました。業務の効率化のため、スタッフ間で「nursing123」という単純なパスワードを共有し、全員が同じ ID でログインしていました。ある日、退職した元職員が自宅から同じ ID・パスワードを使って電子カルテシステムにアクセスし、現役利用者の情報を閲覧していたことが発覚しました。個人情報保護法第 23 条では、アクセス権限の管理や認証の管理など適切な安全管理措置を講じることが求められています。これは ID・パスワード管理の不備による不正アクセスの事例です。

（事例８）介護支援ソフトのデータ移行時における個人情報の不適切な処理

B 居宅介護支援事業所では、使用している介護支援ソフトを A 社から B 社のものに変更することになりました。データ移行作業を業者に依頼した際、旧システムのデータベースを USB メモリに保存して業者に渡しました。この際、データに暗号化などの保護措置が施されておらず、また移行完了後も旧システムのデータベースが削除されないまま放置されていました。後日、事務所の模様替えの際に当該 USB メモリが紛失していることが発覚しました。個人情報保護法第 23 条に基づき、データ移行時の安全管理措置や不要になったデータの適切な消去・破棄が求められます。これはシステム更新時のデータ管理不備による情報漏えいリスクの事例です。

（事例９）リモートアクセス設定の不備による介護記録システムへの不正侵入

C 小規模多機能型居宅介護事業所では、管理者が外出先からでも業務が行えるように、介護記録システムへのリモートアクセス環境を構築していました。しかし、リモートデスクトップの接続ポートを初期設定のままにし、パスワードも単純なものにしていたため、外部からの不正アクセスを受けました。侵入者はシステム内の利用者データを暗号化し、復号するための身代金を要求するランサムウェア攻撃を行いました。バックアップが適切に取られていなかったため、過去 3 か月分の介護記録が失われてしまいました。個人情報保護法第 23 条では、外部からの不正アクセスを防止するための技術的安全管理措置を講じることが求められています。これはリモートアクセス環境の設定不備による不正侵入と情報喪失の事例です。

（事例１０）介護関連アプリのクラウドストレージ設定ミスによる情報公開

D 通所介護事業所では、利用者の活動記録や写真を家族と共有するためのアプリを導入していました。このアプリは利用者ごとのフォルダを作成し、クラウドストレージに保存・共有する仕組みでした。しかし、システム管理者がクラウドストレージの共有設定を誤り、一部のフォルダが「リンクを知っている全ての人が閲覧可能」な状態に設定されていました。この結果、検索エンジンによってインデックス化され、利用者の顔写真や活動記録が誰でも閲覧可能な状態になっていました。個人情報保護法第 23 条では、情報システムを外部と連携する場合の安全管理措置を講じることが求められています。これはクラウドサービス設定ミスによる意図しない情報公開の事例です。

（事例１１）介護記録用タブレットの非管理アプリによる情報流出

E 特別養護老人ホームでは、介護記録の効率化のために各フロアにタブレット端末を配備していました。職員は業務の合間に個人的な目的でもタブレットを使用しており、SNS アプリやゲームアプリなど様々なアプリをインストールすることが黙認されていました。ある日、職員がインストールした無料の写真編集アプリが、タブレット内の写真（利用者のケア記録写真を含む）に不正にアクセスし、外部サーバーにアップロードしていたことが発覚しました。個人情報保護法第 23 条では、情報システムの使用に伴う漏えい等を防止するための技術的安全管理措置を講じることが求められています。これは業務用端末における非管理アプリの使用による情報流出の事例です。

（事例１２）介護事業所の Wi-Fi 設定不備による情報盗聴

F 訪問介護事業所では、事務所内の通信環境向上のために Wi-Fi ネットワークを設置していました。しかし、セキュリティ設定が不十分で、パスワードが「12345678」という単純なものであり、暗号化方式も旧式の脆弱な WEP 方式のままでした。近隣から悪意ある第三者がこの Wi-Fi ネットワークに接続し、職員がメールで送受信していた利用者情報（アセスメントシートや介護計画書など）を盗聴・傍受していました。個人情報保護法第 23 条では、通信経路の暗号化など情報システムを外部からの不正アクセスから保護するための技術的安全管理措置を講じることが求められています。これは Wi-Fi 設定不備による情報盗聴の事例です。