介護事業所における情報安全管理の手引き
（解説書）

令和８年３月

令和７年度老人保健健康増進等事業
「介護情報基盤の運用に向けた介護事業所におけるセキュリティ対策のための調査事業」
検討委員会

目次

１．「介護事業所における情報安全管理の手引き（解説書）」について

「介護事業所における情報安全管理の手引き（解説書）」（以後、本解説書）は、別冊の「介護事業所における情報安全管理の手引き」（以後、別冊の手引き）で使用される専門用語やチェックリストの各チェック項目などについて、介護現場の方などに向けて分かりやすく解説しています。また、管理者やシステム担当者などに向けて、応用的、発展的な対策などについても記述しています。

本解説書を参考にして、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。

なお、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※1に分かりやすくまとめられていますので、合わせて参考にしてください。

また、介護情報基盤においても、個人情報を含む様々な情報を取り扱いますので、介護情報基盤への参画にあたっては、別冊の手引きと本解説書をご活用ください。介護情報基盤の詳細については、介護情報基盤ポータル※２をご確認ください。

※1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
※２介護情報基盤ポータル
https://www.kaigo-kiban-portal.jp/

２．個人情報について

２－１．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）

なお、当該利用者が死亡した後においても、介護事業者が当該利用者の情報を保存している場合には、漏えい、滅失又はき損の防止のため、個人情報と同等の安全管理措置を講じることが求められます。

「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。

＜介護事業所における要配慮個人情報の例＞
・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。

２－２．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。

２－３. 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

２－４. 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。

3．チェックリスト解説

以下では、別冊の手引きに掲載しているチェックリストの各チェック項目について、具体的な対策や考え方などを解説しています。

3－1．安全な使用環境の確保

1）原則、職員個人のスマートフォンやパソコンなどの端末で、個人情報を取り扱う業務は行わない、介護ソフトなどを利用していない。

＜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・盗難による情報漏えい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。

2）個人情報を含む端末は、紛失や盗難、き損が生じないよう人通りの少ない安全な場所で使用している。

＜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物理的に固定するなどして、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。
- 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。

■用語集
P.21
物理的セキュリティ
■事例１
P.23
ﾀﾌﾞﾚｯﾄ端末の紛失

3）個人情報を含む端末を、管理者等からの許可なく事業所外に持ち出していない。

- 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。
- 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。

4）事業所に職員がいなくなる時は、確実に施錠している。

- 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。

5）公衆無線LANを業務で使用していない。

- 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。

■用語集
P.20
ｾﾞﾛﾄﾗｽﾄ
P.21
無線LAN

3－2．ログイン・ログオフの管理等

1）パソコンやタブレット等の端末を起動する際は、自分専用の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。

2）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。

- 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。
- 認証については、認証の３要素である「記憶」、「生体情報」、「物理媒体」のうち、２つの独立した要素を組み合わせて認証を行う方法（二要素認証）を採用することが望まれます。
- 利用者認証を ID とパスワードにより行う際には、システム運用担当者は、パスワードが第三者に推定されにくいものとするよう、安全性を考慮した機能仕様とする必要があるほか、システム側でのパスワードの管理については、システム運用担当者でもわからないようにする措置を講じることが求められます。
- 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。
- 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。

■事例７
P.24
IDﾊﾟｽﾜｰﾄﾞ共有による不正ｱｸｾｽ

■用語集
P.19
ｱｸｾｽ制御
P.20
二要素認証

<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、関係者を騙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。

■用語集
P.20
ｿｰｼｬﾙｴﾝｼﾞﾆｱﾘﾝｸﾞ
P.19
ｱｶｳﾝﾄﾊｲｼﾞｬｯｸ

3－3．閲覧・入力・送信

1）利用時に覗き見されないように覗き見防止シート等を使用している。離席時は、端末にロックをかけている。

- 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、端末にロックをかけます。
- 一般的な端末ロックの方法は、「Windows」キーを押しながら「L」キーを押します。

2）個人情報は、正確な情報源から得た情報を正しく入力し、正確な内容で管理している。

- 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。

■事例 5
P.24
自動記録ｼｽﾃﾑによるﾊﾞｲﾀﾙｻｲﾝ管理の共有ﾐｽ

3）メールや FAXの宛先の確認を徹底し、送信ミスを防止している。
4）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。
5）重要情報はパスワード保護した添付ファイルに記載している。

- 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、又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、又は手動で送信する設定にすることも効果的です。

■事例6
P.24
FAX誤送信による個人情報漏えい

3－4．その他、注意事項

1）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。

- 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。

■用語集
P.22
USB
P.19
外部記憶媒体
P.19
暗号化

2）知らない送信元や内容に不審な点があるメールの添付ファイルやURLリンクは開いていない、クリックしていない。

- 電子メールの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。

■事例2
P.23
ｳｲﾙｽ感染による情報流失

- 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。

■用語集
P.21
ﾌｨｯｼﾝｸﾞ
P.22
SNS

3）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用していない。

- 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。

■事例11
P.25
非管理ｱﾌﾟﾘによる情報流出

３－５．安全管理措置等（主に管理者・システム担当者向け）

管理者や情報システム安全管理責任者は、ISMSを運用し、安全管理措置を行うことが推奨されます。

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。

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

1）組織的安全管理措置
個人情報保護指針や個人情報取扱規程等を作り、情報セキュリティ責任者を選任するなど、組織体制とルールを整備している。

（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。
  <情報システム安全管理責任者の役割>
  ・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

（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クと、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。

■用語集
P.22
ﾘｽｸｱｾｽﾒﾝﾄ
P.21
ﾘｽｸ

- 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（BCP）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。

■用語集
P.22
BCP

（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。

（5）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。介護事業所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

2）人的安全管理措置

入職時、派遣職員を含め、職員へ定期的に情報セキュリティ研修やインシデント発生時の対応訓練を行っている。

（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。

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。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。

（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。

■用語集
P.19
ｸﾗｳﾄﾞ
P.22
Wi-Fi
P.22
BYOD

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。また、定期的に OSやセキュリティソフトを更新し、常に最新の状態に保っている。

（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。

■事例9
P.25
ﾘﾓｰﾄｱｸｾｽ設定不備による不正侵入
■事例12
P.25
Wi-Fi設定不備による情報盗聴

■用語集
P.20
ｿﾌﾄｳｪｱ
P.19
ｴﾝﾄﾞﾎﾟｲﾝﾄｾｷｭﾘﾃｨ
P.21
ﾏﾙｳｪｱ

（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。
- 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。

■用語集
P.22
ﾛｸﾞ
P.20
ｾｷｭﾘﾃｨｲﾝｼﾃﾞﾝﾄ

（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。

■用語集
P.19
ｸﾗｲｱﾝﾄ証明書

（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。
- 重要なデータは２世代以上のバックアップを確保します
- バックアップデータの持ち方は、「物理的な外付け機器（SSD/HDD）」と「オンラインストレージ（クラウド）」を組み合わせ、２か所以上の場所に保管するという321ルールが最適です。
- バックアップデータの一つはネットワークから切り離して保存します。

■用語集
P.20
ﾊﾞｯｸｱｯﾌﾟ
P.19
ｸﾗｳﾄﾞ
P.19
321ﾙｰﾙ

（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又は削除します。

（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、紛失時の情報漏えいを防止しましょう。

■用語集
P.21
ﾌｧｲｱｳｫｰﾙ
P.21
無線LAN
P.19
暗号化

5）外的環境の把握

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し、介護ソフトベンダー社等のセキュリティ対策を確認している。

- 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。

■用語集
P.21
ﾍﾞﾝﾀﾞｰ

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すとともに、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。

- 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。

４.「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

医療機関等（介護事業所を含む）において、医療情報システムの導入、運用、利用、保守及び廃棄に関わる場合、「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)に則り、技術的及び運用管理上の観点から所要の対策を行うことが示されています。

- 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ます。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やWi-Fi等のネットワーク環境ベンダー等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。

５．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、き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、個人情報の漏えい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。

６．まとめ

本解説書では、介護事業における情報安全管理の具体的な対策など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。

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。

別冊の手引きと本解説書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。

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

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）、「物理的な外付け機器（SSD/HDD）」と「オンラインストレージ（クラウド）」を組み合わせ、2か所以上の場所で保管する方法。

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
情報システムの利用者を認証する方式のうち、IC カード等のセキュリティ・デバイス+パスワードやバイオメトリクス（指紋、顔等）+IC カード、ID・パスワード+バイオメトリクスのように、認証の 3 要素である「記憶」、「生体情報」、「物理媒体」のうち、2つの独立した要素を組み合わせて認証を行う方式のこと。

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、二段要素証、バイオメトリクス認証などが含まれる。

は行

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。

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。

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電波を利用してネットワークに接続するための技術。不正アクセスや盗聴を防止するため、通信を暗号化して保護する必要がある。

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。

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。

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。

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。

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。

介護事業所におけるIT機器の情報セキュリティ事例集

介護事業所において実際に発生した、情報漏えいや不正アクセス等の事例を紹介します。

（事例１）タブレット端末の紛失による個人情報漏えい

A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

B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

C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

D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

E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

F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

G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

H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

I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

J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

K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

L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。

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7年6月一部改定）
- 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7年6月改正）
- 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第6.0版（令和5年5月）
- 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）
- 介護情報基盤ポータル　https://www.kaigo-kiban-portal.jp/
- 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７年度老人保健事業推進費等補助金
「介護情報基盤の運用に向けた介護事業所におけるセキュリティ対策のための調査事業」
検討委員会

委員長

公益社団法人 全国老人保健施設協会
副会長　高橋　肇

委員

一般社団法人 保健医療福祉情報システム工業会
医事コンピュータ部会 介護システム委員会 副委員長　石川　竜太

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　地域医療連携室長　大西　丈二

社会福祉法人 奉優会
理事長　香取　寛

一般社団法人 保健医療福祉情報システム工業会
医事コンピュータ部会 介護システム委員会 委員長　畠山　仁

事務局

ＭＳ＆ＡＤインターリスク総研株式会社

発行
令和７年度老人保健事業推進費等補助金
「介護情報基盤の運用に向けた介護事業所におけるセキュリティ対策のための調査事業」
検討委員会　事務局　ＭＳ＆ＡＤインターリスク総研株式会社

※本手引きは、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」の
研究班（代表 国立長寿医療研究センター三浦久幸）が発行した資料を基に作成したものです。