令和７年度　老人保健事業推進費等補助金

厚生労働省　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
報告書

令和８年３月

ＭＳ＆ＡＤインターリスク総研株式会社

目次

I.　事業概要

１.事業実施目的

今後、「全国医療情報プラットフォーム」が創設され、介護領域においても自治体、介護事業所、医療機関が情報共有を行うための介護情報基盤の構築が検討されている。その一方で、近年の医療機関等に対するサイバー攻撃事案の増加に見られるように、介護事業所においても介護情報等を安全に共有・活用できるようネットワークの構築や端末の安全管理措置等を実施する必要がある。そのため、令和６年度厚生労働科学研究においてネットワークの構築や安全管理措置等の明確化を目的として「介護情報等システムの安全管理に関する手引き」（以下「手引き」という。）が作成された。

本事業では介護情報基盤の本格運用に向け、有識者の意見を踏まえながら、介護事業所及び介護ソフトベンダーに対してヒアリング調査等を実施し、その結果を基に既存の手引きをより実効性の高い物へと改訂を行うとともに、実際に介護事業所が介護情報基盤に参加する上での安全管理に係る課題を整理し、対応策等について提案として取り纏めることとした。

２．事業推進体制

本事業の業務全般にわたり、一貫して助言を得るために有識者により構成される委員会を設置した。検討委員会およびオブザーバーは以下のとおり。

＜検討委員会（敬称略、五十音順）＞

氏　　名	所　　属
石川　竜太	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
大西　丈二	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
香取　寛	社会福祉法人 奉優会 理事長
◎　高橋　肇	公益社団法人 全国老人保健施設協会 副会長
畠山　仁	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

（◎：委員長）

＜オブザーバー＞

厚生労働省　老健局　老人保健課

＜事務局＞

ＭＳ＆ＡＤインターリスク総研株式会社

リスクコンサルティング本部　リスクマネジメント第四部

社会保障・医療福祉グループ

３．事業全体の取組内容

本事業における取組内容は、以下（１）～（５）の通りである。

（１）　検討委員会の設置

本事業の業務全般にわたり、一貫して助言を得るために、有識者等により構成される検討委員会を設置した。検討委員会の構成についてはＰ．４、開催スケジュールおよび各検討委員会の議事についてはＰ．７を参照のこと。

（２）　ヒアリング調査の実施

検討委員会委員の推薦により、介護事業所及び介護ソフトベンダーに対してヒアリング調査を行った。ヒアリング調査対象者におけるセキュリティ対策状況、手引きの理解に係る課題、手引きの実践に係る課題および課題の解決に必要と考えられる支援等、手引きの改訂に向けた提言の検討に資する情報および実際に介護事業所が介護情報基盤に参加する上での安全管理に係る課題を整理、検討する際の有用な情報を得た。

（３）　改訂「手引き」及び「解説書」の作成

「医療情報システムの安全管理に関するガイドライン」の他、情報安全管理等に関する公開資料等の精査及び（２）ヒアリング調査で得られた介護事業所及び介護ソフトベンダーにおける手引きの理解や実践に係る課題や改善策等を踏まえ、検討委員会で協議し、既存の手引きの改訂作業を行った。既存の手引きは、介護事業所が情報安全管理の取組を推進するにあたって必要な情報は一定網羅されていたため、内容には大きく手を加えず、見せ方や構成等を主に改善することとし、「手引き」及び「解説書」の２組に再構築する形で改訂した。提供方法は厚生労働省のウェブサイト及び当社ホームページ上でダウンロード可能な形式での公開とした。

（４）　手引き解説動画の作成

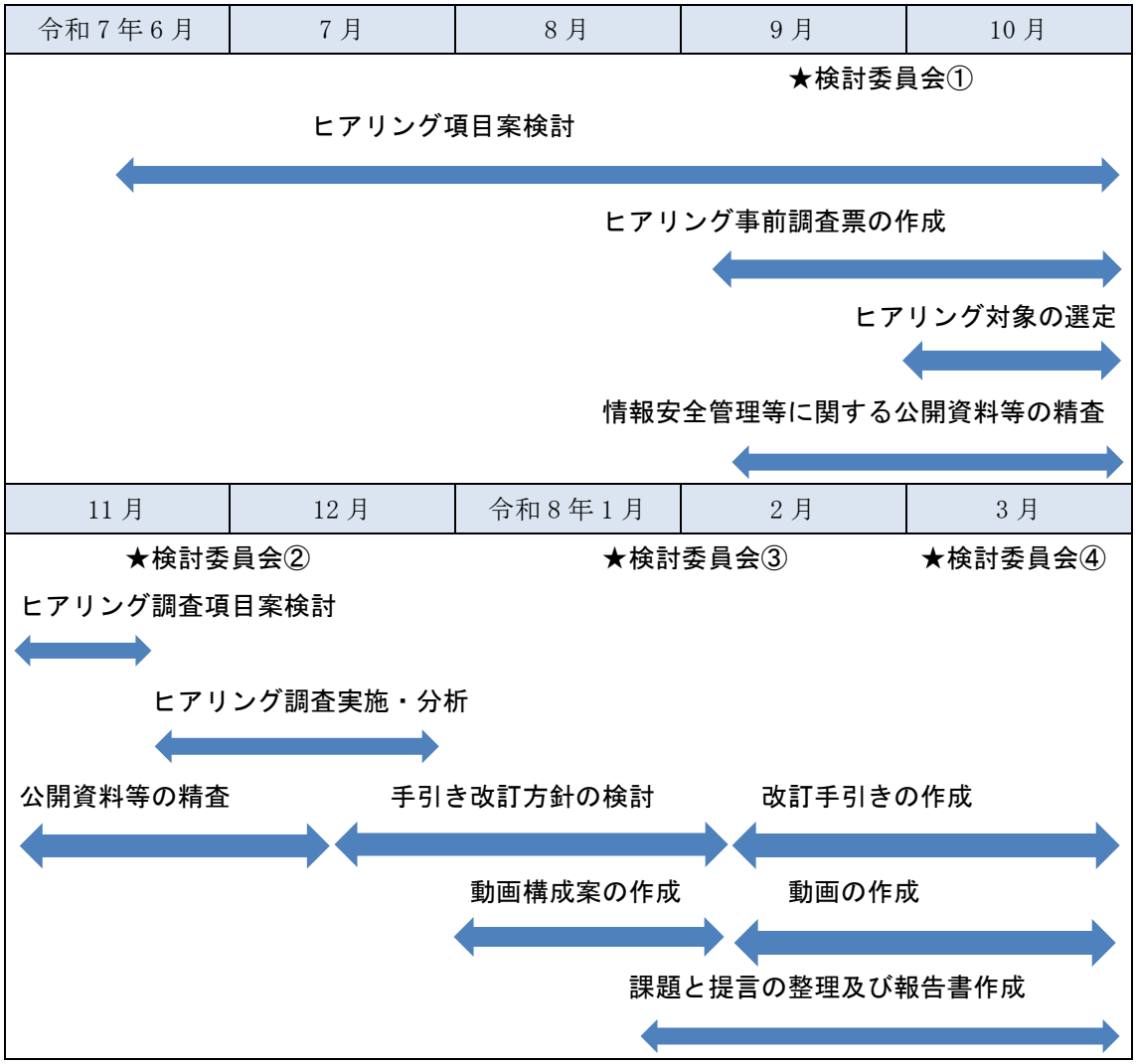
（２）ヒアリング調査から確認できた介護事業所の IT リテラシー水準や、手引き運用に関する意見や要望を踏まえ、改訂「手引き」の内容の理解をより促進できるよう、改訂「手引き」についての解説動画を作成した。提供方法は厚生労働省のウェブサイト及び当社ホームページ上にて視聴可能な形式での公開とした。

（５）　介護事業所における情報セキュリティに関する課題と提言の検討

（１）から（４）までの各業務内容を踏まえ、今後、実際に介護事業所が手引きを用いて介護情報基盤に参加する上での情報安全管理に係る課題について検討を実施し、提言として取り纏めた。

４．事業実施スケジュール

本事業は以下のスケジュールの通り実施した。



II. 事業実施結果

１．検討委員会開催概要

計4回の検討委員会を開催した。いずれの回も会場（弊社会議室）とWEB会議システムを併用した開催とした。

開催日	議題
第1回検討委員会 令和7年9月16日(火) 14:00-16:00	▪ 事業全体像の確認 ▪ 昨年度科研に関するご報告等（大西委員より） ▪ 手引きの改訂について ▪ ヒアリング調査について
第2回検討委員会 令和7年12月1日(月) 10:00-12:00	▪ 報告：ヒアリング調査について ▪ 議案：手引き改訂の方針について
第3回検討委員会 令和8年1月22日(木) 14:00-16:00	▪ 議案：ヒアリング調査結果について ▪ 議案：手引き及び解説書改訂（案）について ▪ 議案：動画構成（案）について ▪ 議案：事業報告書項目（案）について
第4回検討委員会 令和8年3月9日(月) 14:00-16:00	▪ 報告：手引き及び解説書について ▪ 報告：動画資料について ▪ 議案：介護事業所が介護情報基盤に参加する上での ▪ 介護事業所における情報セキュリティに関する課題及び提言について

２．ヒアリング調査の結果

（１）　ヒアリング調査の実施概要

①　ヒアリング調査の目的

介護事業所がセキュリティ対策を進める際には、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、支援を受けることなどが効果的とされており、また、介護事業所は介護ソフトベンダー側のセキュリティ対策状況等も把握しておく必要があることから、介護ソフト・システム等を使用している介護事業所と、介護ソフト・システムベンダー事業所の２者に対して、以下の３点を目的として、ヒアリング調査を行った。

- 介護事業所及び介護ソフトベンダーにおけるセキュリティ対策状況等の把握
- 「手引き」の理解及び実践に係る課題及び課題の解決に必要と考えられる支援等の把握
- 「手引き」の改善点及び改訂に関する要望等の把握

②　調査対象

介護事業所及び介護ソフトベンダーそれぞれについて以下の選定基準を踏まえ、検討委員から推薦が得られた計９件に対してヒアリング調査を実施した。

【選定基準】

１）介護事業所（計６件）

・入所、通所、訪問、居宅介護支援等の様々なサービス種類の施設・事業所を対象とする。

・複数の施設・事業所を運営している法人や情報システム専門の部署や担当者の設置有無等も考慮して選定する。

・施設・事業所におけるセキュリティ対策の実施状況を考慮して以下のように分類し、選定する。

A（２件）：医療法人が有する医療機関の中（又は併設）で運営されている介護事業所

B（２件）：医療法人だが医療機関以外の拠点で運営している、もしくは社会福祉法人や株式会社が運営している介護事業所

C（２件）：NPO 法人や小規模な民間法人の事業所（母体となる法人が分類ＡおよびＢに当てはまらない NPO 法人又は合同会社等の営利法人、事業所単位での利用者数が「300 名／月」以下程度）

２）介護ソフトベンダー（計３件）

・介護記録や請求業務等に使用する介護ソフト・システムを販売するベンダーを対象とする。

・令和３年度老健事業「自身の介護情報を個人・介護事業所等で閲覧できる仕組みについての調査研究」報告書（三菱総研）内の「利用している介護業務等支援ソフトウェア」をもとに以下のように分類し、選定する。

a （１件）：シェア率の高いソフトを扱う大手のベンダー

b （２件）：シェア率が低めのソフトを扱う小規模なベンダー

③ 調査方法

調査方法は WEB 会議システムを使用し、90 分～120 分で実施した。

④ 調査期間

調査期間は 2025 年 11 月 25 日（火）から 12 月 24 日（水）の間で実施した。

⑤ 主な調査項目

１）介護事業所

- 基本情報（法人名、施設名、施設種類、規模　等）
- 情報システム担当部署等の設置状況
- 情報安全管理の実施状況
- 手引きの理解に係る課題
- 手引きの実践に係る課題および課題の解決に必要と考えられる支援　等

２）介護ソフトベンダー

- 基本情報（法人名、会社名、規模　等）
- 扱っている介護ソフト
- 介護事業所との連携状況
- 介護事業所の手引きの理解に係る課題
- 介護事業所の手引きの実践に係る課題および課題の解決に必要と考えられる支援
- 介護事業所における情報安全管理全般に関する課題や意見
- 提供しているシステム・ソフト固有の課題　等

（2） ヒアリング調査結果

ヒアリングの調査の主要な結果は以下の通り。

① 概要版やチェックリストの有用性について

既存の手引きの概要版及びチェックリストの有用性について、以下のような回答が得られた。

回答者	回答
介護事業所Ａ－１	・特にチェックリストは見やすいと感じた
介護事業所Ｂ―１	・概要版は見やすく、理解しやすい。
介護事業所Ｃ－１	・チェックリストには個人情報の管理に必要な対策が具体的にまとめられているため、理解しやすく、活用しやすいと思われる。
ベンダーａ―１	・手引きの内容は網羅的でわかり易い。

② 用語集の有用性について

用語集の有用性について、以下のような回答が得られた。

回答者	回答
介護事業所Ａ－１	・解説編に用語説明があったため、用語等含めて理解の難しさは感じなかった。
介護事業所Ｂ―１	・用語集は非常にわかり易い。
介護事業所Ｃ－２	・最後の用語集は内容の理解に役立った。

③ 文章量や内容の重複・曖昧さについて

手引きの文章量や、内容が重複している点、曖昧な表現などについて、以下のような回答が得られた。

回答者	回答
介護事業所Ａ－１	・チェックリストと説明文の内容が重複していて読みづらい。
介護事業所Ｂ―２	・現場の全職員へ周知していく場合、さらに簡易なものの方が活用しやすい。例えば、重要な項目に絞って解説したものなどがあるとよい。
介護事業所Ｃ－１	・手引きの後半（解説編）は文字ばかりになるため、イラスト等を使用して内容を解説する方が読みやすく理解も進むだろう。
ベンダーｂ－２	・解説編のページ数が多く、読まれにくいだろう。簡易版と詳細版に分ける等の工夫が望ましい。

④ 理解・実践の難しさについて

手引きの理解や、手引きの内容を実践する際の難しさについて、以下のような回答が得られた。

回答者	回答
介護事業所Ａ－１	・介護職員は IT に苦手意識を持っている人が多く、専門用語が通じない点に配慮が必要。 ・メールのファイル添付では大容量メールサービスを使用しているが、これが推奨されている方法なのかどうか手引きで確認できると良い。新しいシステム導入は費用面などからも困難なので、既存環境で対応可能な、推奨される方法などが示されていると良い。
介護事業所Ａ―２	・フロー図やチェックリストを整理して、最低限の対応を図示すると、何をすべきかが順序だてて理解できる。
介護事業所Ｂ－２	・重要な内容であることが理解できたとしても、具体的にどう対応を進めていけばよいか分からないケースも少なくないと思われる。また、概要版は、もう少し文章を減らしてイラストなどを増やした方がよい。

⑤　手引きの内容に対する懸念点について

手引きの内容についての懸念点について、以下のような回答が得られた。

回答者	回答
介護事業所Ａ－１	・ワイヤーによる盗難防止など、対応が出来ていない項目もあったが、デスクトップやミニ PC はワイヤーロックが困難。これらについてどのような対策をすればよいか等、具体的に書かれているとなお良い。
ベンダーａ	・手引き概要版では介護事業所からの照会先が主に介護ソフトベンダーであるような記載となっているが、ベンダーの役割に応じて照会するような記載内容にしてほしい（ネットワークの構築などハード面のベンダーと、ソフトを提供するベンダーで役割が異なる）。また、「信頼できるベンダー」という記載も、対象範囲が広すぎるのではないか。 ・事業所における情報セキュリティ対策は介護事業所主体で考えるべきことである点は明記しておいてほしい。 ・ベンダー側のソフトには、指紋認証や顔認証が搭載されていないものもあるため、生体認証の採用については「推奨する」「端末の機能を活用して検討する」程度の記載が望ましいのではないか。
ベンダーｂ－１	・タブレットなど、据え置きでなく持ち歩きを前提とした端末で考えた場合、「部屋の入退室を管理する」といった記載内容は実態に馴染まず、違和感がある。 ・手引き概要版の記載内容では、ハード面のセキュリティに関する照会もソフトベンダーに寄せられることが懸念される。 ・ソフトベンダーとして介護事業所に各種アドバイスを実施するのは良

	いが、アドバイスした内容について責任が発生するのは困る。この辺りについて誤解がないように記載頂きたい。
ベンダーｂ－２	・ネットワーク業者と介護ソフトベンダーの責任分界点が曖昧である点が少し気になる。

⑥　チェックリストについて

手引き概要版のチェックリストについて、以下のような回答が得られた。

回答者	回答
介護事業所Ａ－１	・チェックリストの各項目については、解説編の参照ページが記載されていると良い。
介護事業所Ａ―２	・フロー図やチェックリストを整理して、最低限の対応を図示するとよいだろう。 ・現状のチェックリストは誰に向けたものなのか不明な項目や、チェック項目の形になっていない文章があると感じた。

⑦　解説動画の作成について

手引きに関する解説動画の作成要望等について、以下のような回答が得られた。

回答者	回答
介護事業所Ａ－１	・手引きに関して、３分くらいの短い解説動画が数本あるとよい。
介護事業所Ａ―２	・事例も交えて、交通教習ビデオのように『こうしてしまうと危険』といった禁止事項を強調する説明動画があると良いだろう。
介護事業所Ｂ－２	・１本３～５分程度の長さで職員の入職時に活用できる動画となるとさらに良い。
介護事業所Ｃ－１	・現状の概要版を凝縮して動画にすると見やすいと思われる。
ベンダーｂ－１	・１本数分程度ずつの解説動画を作成するのはよいと思う。
ベンダーｂ－２	・動画は概要版の内容を中心にするとよいだろう。また、失敗事例を紹介した後で、対策を解説するような構成にすると興味を持たれやすいと思われる。

３．改訂「手引き」及び「解説書」の作成について

（１） 改訂方針

ヒアリングで得られた結果から、以下の手引き改善点等が確認された。

- チェックリストや用語集について概ね好意的な反応だったため、改訂後も引き続き掲載する。
- 重複した内容はできるだけ削除し、説明は端的にする。
- IT に苦手意識のある職員でも理解できるよう、フロー図や図解を工夫する。
- チェックリストにおいて、具体的に何をすればいいか分からないものは削除し、何をすべきなのか明確にする。
- 「どの場面でどの項目を見ればよいか」わかるようにチェック項目等に関して詳細情報の参照ページを明記する。

上記の改善点等を踏まえ検討委員会で協議し、以下の方針で既存の手引きの改訂を行うこととした。

- 既存の「手引き（概要版）」と「手引き（解説編）」の２部構成から、電子端末を用いる際の「操作」や「情報管理手順」を参照することができる「手引き」と、手引きに沿って操作を行う上で、不明点が生じた際に参照することを想定した「解説書」の２部構成へ再構築する。
- 「手引き」は、ＩＴ機器に苦手意識を持つ介護事業所の職員でも理解しやすいように、文章量を適度に抑え、フロー図やチェックリスト等を主体とした内容にする。
- フロー図は、チェックリストや解説書、手引き解説動画の活用も含め、情報安全管理の取組の全体像を整理した内容とする。
- チェックリストには、個人情報を取り扱うすべての職員が情報の安全管理に際して具備するべき項目を掲載し、システム利用時に手元に置いて参照することで、情報セキュリティを担保しながら、利用者情報の入力、管理等が出来る内容とする。
- 「解説書」は手引きに沿って情報安全管理措置等を実施する上で、不明点が生じた際に辞書の用に参照することが出来る構成・内容とする。

（２） 「手引き」について

検討委員会での協議を踏まえ、本事業で作成した「手引き」の構成は以下の通りである。「手引き」の全文は巻末資料２を参照のこと。

「手引き」目次	各項目の概要
「介護事業所における情報安全管理の手引き」について	・手引き概要の解説 ・個人情報について ・要配慮個人情報について ・電子機器使用時以外の個人情報の取扱について

介護事業所における情報安全管理	・手引き、解説書、解説動画等の活用について ・チェックリストを用いた情報安全管理の実践について ・フロー図を用いた「学習」「実践」「対策強化」の取組の解説
介護事業所における情報安全管理チェックリスト	・個人情報を取り扱うすべての職員が情報の安全管理に際して具備するべき項目を掲載したチェックリスト ・各チェック項目の解説書参照ページの掲載
介護情報基盤について	・介護情報基盤の基本情報の解説
参考文献等	・参考文献の掲載

（3）　「解説書」について

検討委員会での協議を踏まえ、本事業で作成した「解説書」の構成は以下の通りである。「解説書」の全文は巻末資料３を参照のこと。

「解説書」目次	各項目の概要
「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	・解説書概要の解説
個人情報について	・個人情報と要配慮個人情報について ・個人情報の取り扱いについて ・委託事業者による個人情報の取り扱いについて ・個人情報を扱う仕組について
チェックリスト解説	・「手引き」チェックリストの各項目の詳細解説 ・安全な使用環境の確保について ・ログイン・ログオフの管理について ・閲覧・入力・送信について ・その他、注意事項について ・安全管理措置等（主に管理者・システム担当者向け）
「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」が適用される場合について
個人データの漏えい等の報告等	・個人データ漏えい等が生じた際の個人情報保護委員会への報告等について
まとめ	・まとめ
用語集	・「解説書」で使用される用語の解説
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の紹介
参考文献等	・参考文献等の掲載

（４）　「手引き」及び「解説書」の公開

本事業の報告書とともに、「手引き」及び「解説書」を厚生労働省のホームページ及び当社ホームページ上でダウンロード可能な形式での公開とした。

掲載先 URL

厚生労働省「介護情報基盤について」：https://www.mhlw.go.jp/stf/newpage_59231.html

当社ホームページ：https://www.irric.co.jp/reason/research/index.html#section5

４．手引き解説動画の作成

（１） 作成方針

ヒアリングで確認された、要点をおさえた短時間の解説動画が数本作成されると良いという要望等を踏まえ、検討委員会で協議し、以下の方針で手引き解説動画を作成することとした。

- 改訂したチェックリストの大項目ごとに１本の動画を作成する。
- 動画の長さは１本あたり５分程度とする。
- 適切な対応に関することだけでなく、禁止事項や事例を盛り込んだ内容とする。
- 個人情報の取り扱いに関わる全ての職員を対象としつつも、特にＩＴ機器等に苦手意識を持つ職員をメインターゲットとする。
- 主に管理者・システム担当者向けのチェック項目については動画の対象に含めない。

（２） 手引き解説動画について

前述の作成方針を踏まえ、以下の構成で計５本の動画を作成した。

動画構成	各動画の概要
はじめに：情報安全管理の概要	・「介護事業所における情報安全管理の手引き」をもとに、介護事業所におけるさまざまな情報を安全に扱うための基本的な考え方を解説するもの
１．安全な使用環境の確保	・チェックリストの「安全な使用環境の確保」の項目に沿って、個人端末の利用や端末の持ち出し・保管、公衆無線 LAN の利用など、基本的なポイントを解説するもの
２．ログイン・ログオフの管理棟	・チェックリストの「ログイン・ログオフの管理等」の項目に沿って、ログインにおける注意点やパスワードの管理方法、不正アクセス事例などを踏まえたポイントを解説するもの
３．閲覧・入力・送信	・チェックリストの「閲覧・入力・送信」の項目に沿って、画面の覗き見防止、記録の正確な入力、メールや FAX 送信時の注意点など、端末の使用時に起こりやすいリスクとその対策を解説するもの
４．その他、注意事項	・チェックリストの「その他、注意事項」の項目に沿って、USB メモリなどの外部機器の扱い、不審なメールやリンクへの対応、業務用端末の私的利用など、これまでの項目に当てはまらないものの、情報漏えいの原因になりやすいポイントを解説するもの

（３）　動画の公開

手引き解説動画は、介護情報基盤ポータル及び当社ホームページへ掲載し、公開する。

掲載先 URL

厚生労働省「介護情報基盤について」：https://www.mhlw.go.jp/stf/newpage_59231.html

当社ホームページ：https://www.irric.co.jp/reason/research/index.html#section5

III. 介護事業所における情報セキュリティに関する課題及び提言

本事業では、ヒアリング調査及び有識者による検討委員会での議論を踏まえ、既存の手引きの改訂を行った。一方で、検討の過程においては、手引きのへの反映には至らなかったものの、今後の運用や手引きの周知及び理解において重要と考えられる課題も明らかとなった。本章では、これらの課題を整理するとともに、今後の対応の方向性について提言として取りまとめることとした。

（1） 手引きの継続的なアップデートについて

① 課題

- 手引きや解説書だけではカバーしきれない内容がある。また、情報管理の進展や求められる対策の高度化・複雑化への対応が難しい。

② 課題に対する提言

- 今後も手引き及び介護情報基盤の運用の中で継続的に課題を集め、対策をアップデートしていくことが重要である。
- 「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」や「医療情報システムの安全管理に関するガイドライン」等の関連資料の更新内容や、定期的な調査事業等の実施による課題の収集を行い、その時々の環境や実情に合わせた内容で、手引きの継続的に改訂することが望まれる。
- 手引きだけですべての内容を網羅するのではなく、研修等の周辺活動を充実させる方向を検討するのも一案と考えられる。

（2） 事業所における体制の整備について

① 課題

- 規模等によってはセキュリティ対策に関して早期に体制を整えるのは困難な事業所もあることが予想される。
- 介護システム等の安全管理責任者を担う人材の確保が難しい。
- 各種対策について費用面の問題で対応が困難な部分がある。

② 課題に対する提言

- 厚生労働省の人材開発支援助成金を活用することで、費用面の負担を軽減して人材の育成を行うことが出来る。
- 業界団体等が主催するデジタル人材育成に関する講座等への参加も効果的である。
- セキュリティ対策に関する体制整備や機器・システム等導入に係る費用について、補助金の対象とされることが望まれる。
- 有事の際に備えてのサイバーリスク保険等の活用も有効な手段の一つと考えられる。

（３） 関係者間の責任分界点の整理について

① 課題

・ システムに関する障害や事後が発生した際、誰の責任範囲となるか、ユーザー（介護事業所）と介護ソフトベンダー、ネットワークベンダーの三者間での責任分界点の整理が重要であるが、多くの事業所で整理されていない状況がある。

② 課題に対する提言

・ 「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」において責任分界の取り扱いに関する記載があるため、それらを参考に対策を講じることが推奨される。 ・ 将来的には、手引きにも責任分界点の設定に関する記載が追加されることが望まれる。 ・ 介護事業所側だけでなく、各ベンダー側にも責任分界点の設定の重要性が理解される必要がある。 ・ 有事の際の責任の所在については、手引き及び介護情報基盤の運用の中で得られた情報等をユースケースのような形で整理し、提示することも効果的であると考えられる。 ・ 情報基盤の連結においては介護と医療それぞれのベンダーも関わることとなるので、今後、さらなる重要な課題となる。

（４） 地域単位の支援体制について

① 課題

・ 介護事業所におけるセキュリティ体制の構築や、リスクにさらされた際の対応等に関して困った際に相談できる公的な問合せ先が無い。

② 課題に対する提言

・ 独立行政法人　情報処理推進機構（IPA）の「サイバーセキュリティお助け隊サービス」のような、何かあった際に助けてくれる地域ごとの支援体制の構築が望まれる。 ・ 各都道府県の介護生産性向上総合センター等の相談窓口で、セキュリティ面を含めてよろず相談的に相談できると介護事業所にとって助けとなるだろう。 ・ なお、介護情報基盤に固有の問題であれば介護情報基盤ポータルからの問い合わせが可能である。

以上

IV. 資料編

1．ヒアリング調査票

①介護事業所向け事前調アンケート

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」
介護事業所におけるセキュリティ対策に係るヒアリング事前アンケート

0. 基本情報

Q.1 回答者および所属する法人、施設・事業所についてお答えください。

回答者氏名	
回答者役職	
回答者連絡先（電話番号）	
回答者連絡先（メールアドレス）	
施設・事業所の名称	
施設・事業所の主な事業種別	
その他の詳細	（ ）
施設・事業所の所在地	
施設・事業所が所属する法人の法人種別	
その他の詳細	（ ）
施設・事業所の従業員数・職員数 （正規・非正規を含む常勤換算数。職種を問わず。）	
施設・事業所の利用者定員数	
施設・事業所の開設年月（西暦）	年 月
法人内すべての施設・事業所数	

Ⅰ. 情報システムの担当部署等の設置状況について

Q.2 情報システムやセキュリティ専門の部署は設置されていますか。（1つに○）

	設置されている	→Q.3にお進みください
	設置されていない	→Q.5にお進みください

Q.3 情報システムやセキュリティ専門の部署の人数について教えてください。

専従数	人	兼任数	人

Q.4 情報システムやセキュリティ専門の部署の役割について教えてください。（→Q.6にお進みください）

Q.5 専門部署に代わって情報システムやセキュリティ業務を担っている部署について教えてください。

部署名		人数	人
どのように本来の業務と分担をしているか			

Q.6 情報システム安全管理者・責任者について教えてください。

役職名	
安全管理の理解度	

Q.7 使用している介護ソフトについて教えてください（「介護ソフト」とは、請求業務等、介護サービス施設・事業所での業務を支援するソフトウェアを指します）。

	使用している介護ソフトの名称	利用目的	導入時期	更新状況	サービスへの権限付与状況	サービスへの認証方法	提供形態（※）
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

※「クラウド」：インターネットを通じてサービスを利用する仕組み。事業所のPCやサーバーにシステムやソフトを設置しない。
「オンプレミス」：事業所のPCやサーバーにシステムやソフトを設置して利用する仕組み。
「スタンドアロン」：サービスを利用するPCがインターネットや他の機器につながっていない状態。

Q.8 セキュリティを含めて、ベンダや中間業者への問合せ方法について教えてください。（「方法」は当てはまるものすべてに○）

頻度									
方法		電話		メールやフォーム入力		面談（対面）		面談（オンライン）		その他

Ⅱ. 安全管理の実施状況について

Q.9　介護ソフトを利用する端末（PC）について教えてください。

台数	台
持出可否	
インターネット接続有無	
USBメモリなど私的デバイスの接続可否	
鍵など物理的な盗難防止策（方法を記述）	
セキュリティソフトの有無	
セキュリティソフトの更新状況	
業務と関係のないサイトへのアクセス制限状況	
端末・アクセス状況の管理者（役職名）	
端末のログの取得・監視状況	

Q.10　通信環境について教えてください。

無線LANの暗号化の有無	

Q.11　事業所におけるご対応について教えてください。

安全管理に係る指針や規程の作成状況	
職員への研修・教育状況	
バックアップの頻度・方法	

Q.12　各種安全管理事項・安全管理体制整備にあたって参考にした情報（資料等）があれば教えてください。

Q.13　情報システムやセキュリティの担当部署・担当者と現場との安全管理上のギャップがあれば教えてください。

Q.14　ベンダとのセキュリティ対策の責任分界点を明確にしておくべき項目に関してお考えがあれば教えてください。

「責任分界点」：サービスやシステムを使用する際、「どこまでを自分（利用者）が管理し、どこからをサービス提供者が管理するか」という分かれ目のこと。

Q.15　電子カルテの三原則を知っていますか。（1つに○）

	知っている
	知らない

Q.16　サイバーセキュリティ対策として保険をかけていますか。（1つに○）

	かけている
	かけていない

Q.17　ランサムウェアやエモテットといったサイバー攻撃を知っていますか。（1つに○）

	よく知っている
	ある程度知っている
	どちらともいえない
	あまり知らない
	全く知らない

質問は以上です。ご協力ありがとうございました。

②介護事業所向けヒアリングシート

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」
介護事業所向けヒアリングシート

０．（確認が必要な場合）事前アンケートのご回答内容について

１．手引きの理解に係る課題について（手引きの改訂に関する情報の収集）

１－１．手引きを読んだ結果、理解が難しい用語・手順・項目がありましたら教えてください。

例）対象者がわかりにくかった、内容が重複しており読むのが大変だった

１－２．手引きにおいてもっと知りたい、より詳しく説明してほしい、追加してほしい事項がありましたら教えてください。

例）●●という項目について、より具体的な手順・具体例を記載してほしい

１－３．上記以外に手引きの改善案がありましたら教えてください。

例）動画での解説があるとよい

２．手引きの実践に係る課題および課題の解決に必要と考えられる支援について（今後への参考情報）

２－１．手引きの内容を実践することで想定される、現在の業務からの変更点がありましたら教えてください。

例）全職員に理解してもらうための研修等が必要になる

２－２．（変更点がある場合）変更を実施するにあたり課題となる事項がありましたら教えてください。

例）研修等を実施するための時間を捻出できない

２－３．挙げられた課題に対して、必要と考えられる国や自治体、介護ソフトベンダ等からの支援がありましたら教えてください。

例）時間を捻出するための追加人員を配置するための補助金があるとよい

２－４．支援があったとしても、現実的に対応が難しい手順・項目がありましたら教えてください。

例）ID やパスワードの共有（使いまわし）をやめることは、費用や運用面から現実的ではない

３．関連する補助金について

ICT 導入支援事業など関連する補助金制度があることは知っていましたか。補助金を活用されている場合、どのように活用されているのか教えてください。

４．その他

４－１．「介護情報基盤」について、どの程度理解していますか。

４－２．施設・事業所内で情報システムやセキュリティに関して困った際、ベンダ以外の相談先はありますか。

以上

③ベンダー向け事前アンケート

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」
介護事業所におけるセキュリティ対策に係るヒアリング事前アンケート

0. 基本情報

Q.1　回答者および所属する法人、施設・事業所についてお答えください。

回答者氏名	
回答者所属部署	
回答者役職	
回答者連絡先（電話番号）	
回答者連絡先（メールアドレス）	
法人名	
従業員数・職員数 （正規・非正規を含む常勤換算数。職種を問わず。）	
法人設立年月（西暦）	年　月

Ⅰ. 扱っている介護ソフトについて

Q.2　扱っている介護ソフトの名称、種類、提供形態（クラウド、オンプレミス、スタンドアロン等）、仕様等について教えてください。（提供しているもの全て）

	名称	種類（用途）	提供形態	仕様（URL等）	備考等
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

Ⅱ. 介護事業所との連携状況について

Q.3　提供している介護ソフトについて、介護事業所のどの端末で使用されるか、およびモバイル端末で使用されることがあるか、把握していますか。

どの端末で使用されるか	
モバイル端末で使用されることがあるか	

Q.4　介護事業所における介護ソフトへのログイン運用について把握していますか。
例えば、ログイン認証が設定されていない、または共通ID・パスワードが使用されている、パスワードが本人・管理者以外にも確認可能な状態にある、などの運用はされていないでしょうか。

介護ソフトへのログイン運用状況	
例に挙げられたような運用がされていることを	

Q.5　介護ソフトを使用する端末（モバイル端末を含む）のセキュリティソフトのインストール状況を確認していますか。また、セキュリティソフトが自動更新になっているか確認していますか。

Q.6　セキュリティに関し、介護事業者と以下の契約を締結していますか。（当てはまるものすべてに○）

	秘密保持契約（NDA: Non-Disclosure Agreement）
	サービスレベル契約（SLA: Service Level Agreement）
	データ処理の管理（GDPRや個人情報保護）に関する契約（DPA: Data Processing Agreement）
	セキュリティ要件に関する契約条項（Security Addendum）
	責任の限定と免責条項（サイバー攻撃や不可抗力によるインシデント発生時の責任範囲を明確化して、リスクを管理）
	インシデント対応契約（Incident Response Agreement）
	その他（詳細を右枠に記載してください）

Q.7　セキュリティに関する契約は、定期的な見直しと更新を行っていますか。行っている場合、その頻度について教えてください。

Q.8　個人情報等に対する情報システムの安全管理措置について教えてください。
（ウイルス対策機能、アクセス制御・認証機能、データ保護機能、ガイダンス機能（エラーメッセージ）、など）

Q.9　ログの取得・監視に関する機能やサービスはありますか。
ある場合はその活用状況や介護事業者との共有状況（共有している場合はその方法）について教えてください。

Q.10　介護事業者とのセキュリティ対策の責任分界点を明確にしておくべき項目に関してお考えがあれば教えてください。

Q.11　情報システムの利用に際し、安全管理に関して介護事業者へ求めている事項や推奨している事項があれば教えてください。

Q.12　介護事業者に対する安全管理に関する支援があれば教えてください。
（技術的な情報提供、事業者がサービスへアクセスする際の、事業者における情報管理・認証方法の設定等に関する支援、など）

質問は以上です。ご協力ありがとうございました。

④ベンダー向けヒアリングシート

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」
ベンダー向けヒアリングシート

０．事前アンケートでの要確認事項

事前アンケートを拝見し、詳細を伺いたい内容について確認させていただきます

１．介護事業所との連携状況について

１－１．貴社自身の安全管理措置等の実施状況、および関連事項について介護事業者側からの確認がありましたら教えてください。

例）実際に介護事業者から、実施している安全管理措置の具体的な内容について確認されたことがある、これまでそのような問い合わせを受けたことはない

１－２．セキュリティ対策に関して介護事業所へ期待することを教えてください（期待する最低限の知識・対策・理解など）。

例）一般的と思われる用語については、関係する全職員がわかるようにしてもらいたい

１－３．介護事業者において、または介護事業者と貴社との連携に関して発生したセキュリティ上のトラブルなどがありましたら教えてください。

例）介護事業所における操作でセキュリティ上の問題が発生したが、当社に問い合わせがあり、解決を要請された

１－４．上記に関連して、ベンダー側としての失敗例がありましたら教えてください。

例）責任分界点について介護事業所に理解してもらえてなった

２．手引きの理解に係る課題について（ベンダー側から）

２－１．ベンダー側の立場から見て、介護事業所における手引きの活用に関して想定される課題がありましたら教えてください。

例）対象者がわかりにくく、内容が重複しているため、介護事業所の職員が読むのは大変だと思われる（当社が作成している介護事業所向けのマニュアルでは、●●の点に気をつけている）

２－２．ベンダー側の立場から見て、手引きにおいて改善すべき内容や追記すべき内容、手引きへの期待がありましたら教えてください。

例）●●という項目については、より具体的な手順・具体例の記載が必要だろう、●●については動画で解説すべきだろう

３－５．支援があったとしても、現実的に対応が難しい事項がありましたら教えてください。

例）IDやパスワードの共有（使いまわし）をやめることは、費用や運用面から現実的ではないと予想される

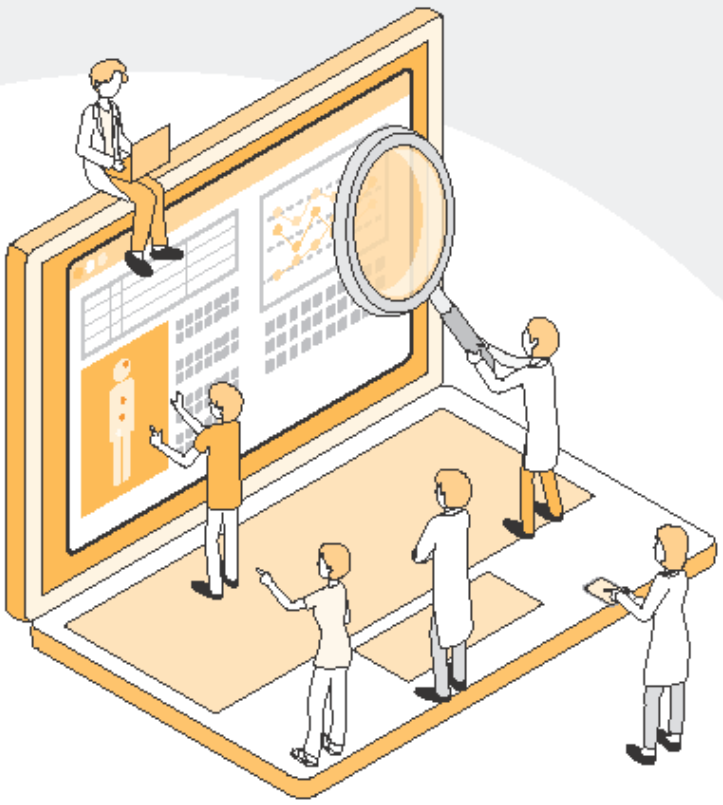
４．その他、介護事業者における情報安全管理全般に関する課題や意見等がありましたら教えてください。

５．提供しているシステム・ソフト固有の課題として考えられる事項がありましたら教えてください。

以上

２．改訂版「介護事業所における情報安全管理の手引き」

目次



「介護事業所における情報安全管理の手引き」について

この「介護事業所における情報安全管理の手引き（以下「手引き」）」は、介護事業所の職員、管理者、システム担当者、経営者などが、電子機器を使用する際に、個人情報や要配慮個人情報などが漏えいしないようにするための対策を解説しています。

必要な対策をまとめた手引きのチェックリストを活用し、介護現場における情報管理の徹底を図ってください。

対策の詳細や分かりにくい専門用語などは、解説編で確認してください。

個人情報とは

特定の個人を識別できる情報を指します。
氏名、生年月日、住所、顔写真などが該当します。

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注意して扱うべき個人情報を指します。
病状や治療、障害などが該当します。

電子機器使用時以外の個人情報の取扱いについて

電子機器使用時以外においても、個人情報を適切に取扱う必要があります。

・利用目的を本人に明示して同意を取得した上で、個人情報を取得し、利用する
・本人の同意がない限り、第三者に対して個人情報を勝手に提供しない

などのルールを遵守する必要があります。
詳細は、以下の資料を参照ください。

◆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ドライン」

◆個人情報保護委員会・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）

1

介護事業所における情報安全管理

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、特に慎重な安全管理が必要です。
手引きと解説書などを活用することで、職場における情報の安全管理を徹底し、情報漏えいやシステム障害などの防止を図ってください。

学習

- □ 手引きや解説書などで、情報安全管理を学習する。
- □ 入職者に対しても、情報安全管理を教育する。
- □ 必要に応じて、解説動画も活用する。

実践

- □ 使用する電子機器の横にチェックリストを備え、情報安全管理を実践する。
  - □ **安全な使用環境の確保**
    個人端末を業務に使用しない、紛失・盗難・き損を防止する、公衆無線LANは使用しない　など
  - □ **ログイン・ログオフの管理等**
    IDやパスワードを共用しない、パスワードを書いたメモを端末のそばに置いておかない　など
  - □ **閲覧・入力・送信**
    業務外で個人情報を利用しない、離席時には端末にロックをかける、誤送信を防止する　など
  - □ **その他、注意事項**
    不審なメールは開かない、業務外でインターネットを利用しない　など

- □ 適宜「解説書」を使って、チェックリストの各対策への理解を深める。

対策強化

- □ 各職場における安全管理措置等に関しては、「解説書」などを参考に、計画的に対策の強化を図る。

介護事業所における情報安全管理チェックリスト

本チェックリストは、介護現場の職員、管理者、システム担当者、経営者など、介護事業所で働くすべての人を対象としています。
職員は、本チェックリストを活用し情報安全管理の徹底を図るとともに、管理者、システム担当者、経営者は、職員が情報安全管理を徹底できるように、各種安全管理措置等を実施することが期待されます。
以下に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。
「チェック結果補足」欄は、各チェック結果について、現状対応できていない理由、対応できている範囲、今後の対応予定などを記載するのに利用してください。

	チェック項目	チェック結果補足	解説書等
1. 安全な使用環境の確保			
☐	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。		「解説書」…P.5 「用語集」 ・無線LAN…P.21
☐	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。		
☐	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。		
☐	事業所に職員がいなくなる時は、確実に施錠している。		
☐	公衆無線LANを業務で使用していない。		
2. ログイン・ログオフの管理等			
☐	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。		「解説書」…P.6
☐	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。		
3. 閲覧・入力・送信			
☐	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。		「解説書」…P.7 「端末ロック」… 一般的な端末ロックの方法は、 「Windows」キー＋ 「L」キー
☐	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。		
☐	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。		

介護事業所における情報安全管理チェックリスト

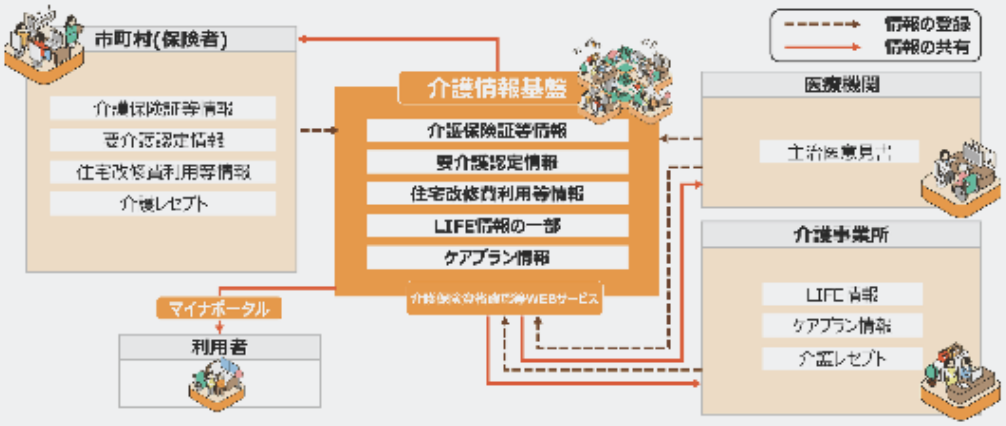
	チェック項目	チェック結果補足	解説書等
3. 閲覧・入力・送信（続き）			
☐	誤送信を防ぐため、あらかじめ登録したアドレス帳を使っている。または組織外のアドレスに送る際、確認メッセージが表示されるよう設定している。		「解説書」…P.7
☐	重要情報はパスワード保護した添付ファイルに記載している。		
4. その他、注意事項			
☐	USB メモリ等の外部機器を、許可なく端末に接続していない。		「解説書」…P.8
☐	知らない送信元や内容に不審な点があるメールの添付ファイルやURLリンクは開いていない、クリックしていない。		
☐	業務用端末を使って、業務に関係のない目的でインターネットを使用していない。		
5. 安全管理措置等（主に管理者・システム担当者向け）			
☐	【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。		「解説書」…P.9 「用語集」 ・セキュリティインシデント…P.20 ・ベンダー…P.21
☐	【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。		
☐	【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。		
☐	【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。		
☐	【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。		
☐	【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。		

介護情報基盤について

介護情報基盤とは、介護に関する情報をひとつに集約。介護に関わる方々を支えるための仕組みです。
利用者・市町村・介護事業所・医療機関の連携が深く強くなります。
複数のガイドラインに従って構築されているシステムとなるため、情報セキュリティが担保されています。

全体概念図

介護に関わる各システムの情報が、介護情報基盤に集まり、閲覧・登録・管理できるようになります。



介護事業所のみなさまが実現できること

いつでも情報を確認

ケアマネジャーや介護事業所の職員が、要介護認定に必要な情報や、ケアプラン作成に必要な情報などをタイムリーに確認できます。

やりとりの負担を軽減

給付に必要な情報をデジタル上で確認できるため、利用者や家族への確認や依頼、市町村（保険者）への問い合わせの負担が減ることが期待できます。

質の高いケア

介護に関する情報収集が効率化されることで、本来的な業務に集中できるようになり、利用者にさらに寄り添ったサービスを提供できます。

本頁は介護情報基盤ポータルサイトの情報を基に作成したものです。詳細は、以下を確認してください。
介護情報基盤ポータル　https://www.kaigo-kiban-portal.jp/

5

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7年6月一部改訂）
- 「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）
- 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）
- 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

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

■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 幸優会
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

※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。

３．改訂版「介護事業所における情報安全管理の手引き（解説書）」

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

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。

（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

■用語集
P.22
BCP

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。

26

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。

令和７年度　厚生労働省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
報告書

令和８年３月

作 成 者　MS&AD インターリスク総研株式会社
〒101-0063
東京都千代田区神田淡路町 2-105 ワテラスアネックス
TEL　03-5296-8976　FAX 03-5296-8941
http://www.irric.co.jp

本事業は、令和７年度老人保健事業推進費等補助金（老人保健健康増進等事業）の交付を受けて実施したものです。