令和５年度厚生労働省
老人保健事業推進費等補助金
（老人保健健康増進等事業分）

介護情報の安全管理に関する調査研究事業

報　告　書

MRI 三菱総合研究所

令和 6（2024）年3月

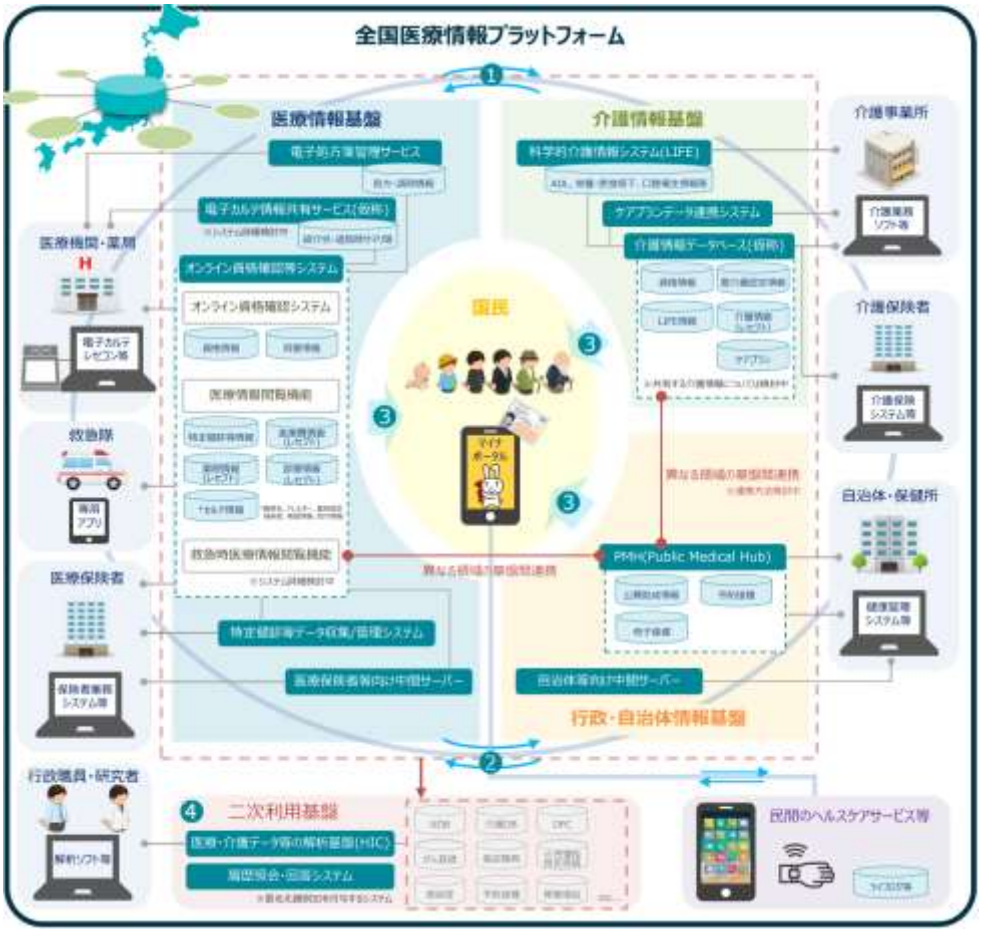
目次

第1章　事業の全体像

Ⅰ.本事業の目的

厚生労働省では、令和３年６月に示されたデータヘルス改革に関する工程表に則り、介護情報利活用ワーキンググループにおいて、利用者が閲覧する情報・介護事業所間等で共有する情報の選定について議論を行っている。さらに、第４回「医療 DX 令和ビジョン 2030」(令和５年８月 30 日)では、以下の図に示すとおり、全国医療情報プラットフォームの構築として、介護情報基盤と PMH(Public Medical Hub)、医療情報基盤(オンライン資格確認等システム)を介して、電子的に介護情報や医療情報のやり取りすることが示されており、医療機関や自治体、介護事業者等を含め、必要なときに必要な情報を共有・交換できる全国的なプラットフォームの実現を目指している。

図表 1　全国医療情報プラットフォーム1の全体像(イメージ)



本事業では、介護事業者も本プラットフォームを通じて情報の共有や交換が行われることが前提とされていることを踏まえ、電子化されている介護情報の活用時における安全管理措置の実態調査及び情報の整理を行った。その結果を基に、介護現場において安全管理措置を実施する際の課題を抽出し、あり得る支援策や対応案をまとめることを目的とした。

[1] 厚生労働省第4回「医療 DX 令和ビジョン 2030」(令和5年8月 30 日)　資料2－2

Ⅱ. 本事業の調査内容と調査目的

本事業の調査内容及び調査目的は以下のとおり。

① 調査検討委員会の開催

- 調査内容及び調査結果についての議論を行った。

② 医療現場における安全管理措置に関する取組の整理

- 医療分野では、介護分野に先んじてセキュリティに関する法令の改正もあり、介護分野と比較して安全管理等について推進されている。医療分野の法令、ガイドライン等の内容を調査し、介護分野との比較分析することにより、推進する上での課題を明らかにすることを目的として調査を行った。

③ 介護現場のセキュリティ対策の実態把握の調査

- 技術的観点から介護情報の取扱いの現状及び将来的な接続方式への対応可能性、課題を把握し整理することを目的として、介護ソフトベンダや IT 部門を持つ介護事業者へのヒアリング調査を行った。
- セキュリティ対策の実態を把握し、将来的な接続方式に対応する場合の運用上の課題やあり得る支援策を把握し整理することを目的として、幅広いサービス・規模の介護施設・事業所へのヒアリング調査を行った。

④ 介護情報基盤を介して電子的に介護情報や医療情報を共有する場合のセキュリティ要件の整理と、その実現に向けた介護施設・事業所における課題及びあり得る支援策・対応案の整理

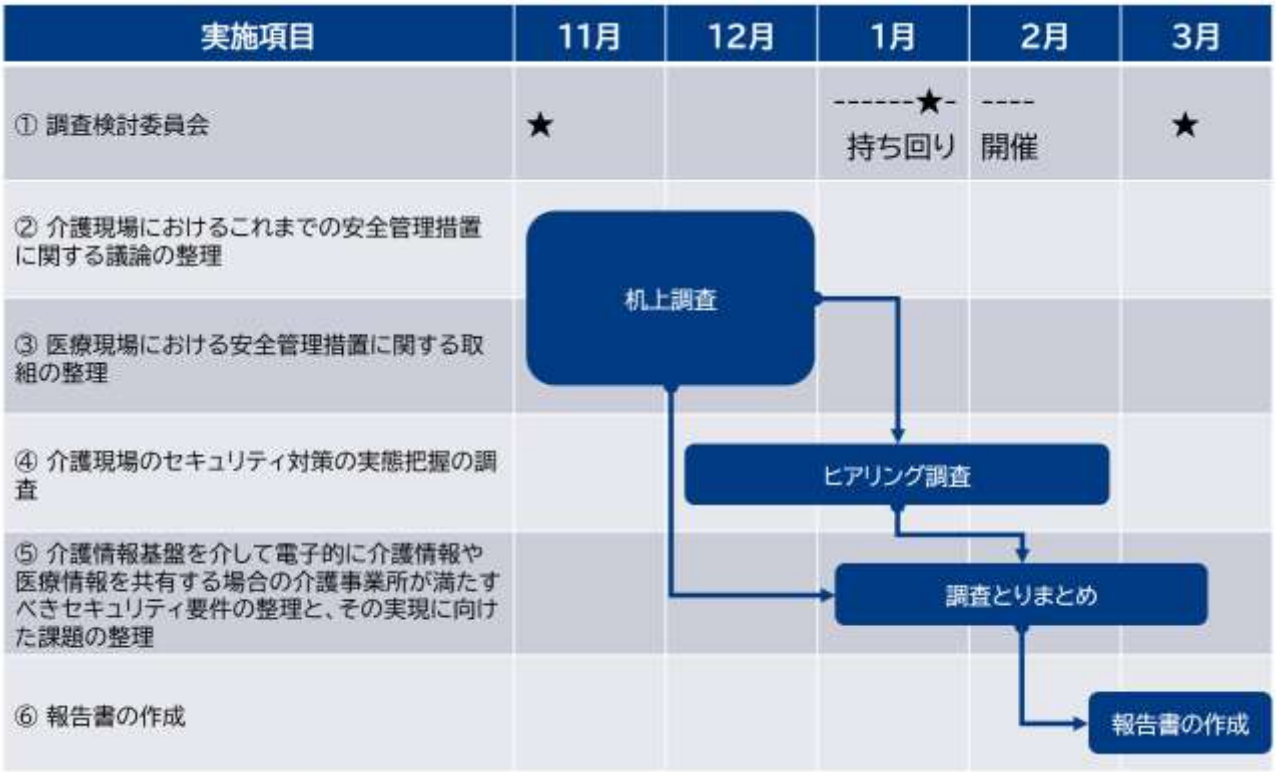
- ②、③の調査結果を踏まえ、介護情報基盤を介して電子的に介護情報や医療情報を共有する場合のセキュリティ要件の整理と、その実現に向けた介護施設・事業所における課題及びあり得る支援策・対応案の整理を行った。

⑤ 報告書の作成

- 上記①～④の調査結果を踏まえて報告書として取りまとめた。

本事業の流れは以下のとおり。

図表 2 本事業の流れ（概要）



Ⅲ. 本事業の検討体制

本事業の実施にあたって、医療および介護分野の有識者及び関連団体の関係者等から構成する調査検討委員会を設置した。

調査検討委員会では調査の実施方針の検討及び調査結果についての議論を行った。調査検討委員会のメンバーは以下のとおりである。

図表 3 調査検討委員会 構成員一覧(敬称略・五十音順)

氏名	所属・役職
◎井出 健二郎	兵庫県立大学 社会科学研究科経営専門職医療介護マネジメント 教授
伊藤 宏光	株式会社ワイズマン 商品企画本部 ソリューション企画 部長
柏本 英子	公益社団法人 日本介護福祉士会 副会長
加藤 浩一郎	株式会社エス・エム・エス 介護・障害福祉経営支援事業本部 カスタマーサクセスグループ グループ長 株式会社エス・エム・エスサポートサービス 介護領域 介護経営支援 グループ長
小林 広美	一般社団法人 日本介護支援専門員協会 副会長
小柳 貴嗣	一般社団法人 日本在宅介護協会 委員 株式会社ニチイホールディングス IT 事業部 ICT 企画推進課 プランニングマネージャー
迫田 武志	エヌ・デーソフトウェア株式会社戦略マーケティング部 シニアマネージャー
佐原 博之	公益社団法人 日本医師会 常任理事
髙橋 肇	公益社団法人 全国老人保健施設協会 常務理事
平井 政規	一般社団法人 全国デイ・ケア協会 理事 医療法人鴻池会 理事長
藤井 陽子	公益社団法人 全国老人福祉施設協議会 老施協総研運営委員会 委員
藤田 大	一般社団法人 全国介護事業者協議会 理事 三井ヘルスサービス株式会社 常務取締役
茗原 秀幸	一般社団法人 保健医療福祉情報システム工業会 セキュリティ委員会 委員長

※◎:委員長

調査検討委員会の開催スケジュールは以下のとおり。

図表 4 調査検討委員会 開催スケジュール

回数	時期	議題
第1回	令和５年 11 月１日 （オンライン開催）	・ 本事業の概要について ・ 本事業の実施計画について
第２回	令和６年１月 12 日～ 令和６年２月 13 日 （持ち回り、オンライン開催）	・ ステップ１ヒアリング調査結果について ・ ステップ2ヒアリング調査方針について
第３回	令和６年３月 14 日 （オンライン開催）	・ 報告書(案)について

第２章　医療現場における安全管理措置に関する取組

Ⅰ. 調査の目的

医療分野では、介護分野に先んじてオンライン資格確認・オンライン請求について原則義務化され、医療法施行規則のセキュリティ要件が明確化された一部改正及び第 25 条第1項に基づく立ち入り検査についてもセキュリティ確保について確認するため「医療法第 25 条第1項の規定に基づく立入検査要綱」が改訂されたこともあり、介護分野と比較して安全管理等について推進されている。医療分野の法令、ガイドライン等の内容を調査し、介護分野との比較分析することにより、DX 推進する上での課題を明らかにすることを目的として調査を行った。

Ⅱ. 調査方法

医療分野における安全管理に関わる法制度の要件、及び制度に基づく対応について、公表資料を基に文献調査を行い、実態調査を行った。既に公表されている調査報告等も合わせて、医療分野と介護分野の取り巻く環境の差異を確認し、安全管理措置についての取り組み状況を比較した。令和 6 年 1 月時点で最新のものとした。法令については、医療法、医療法施行規則を調査対象とし、比較対象は介護保険法、介護保険法施行規則とした。

主な調査対象のガイドライン、技術解説書は以下のとおり。

図表 5 主なガイドライン、技術解説書等の調査文献

発行元	主なガイドライン、技術解説書等の調査文献
厚生労働省 医政局	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） 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 版概説編 [Overview] 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 版経営管理編 [Governance] 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 版企画管理編 [Management] 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 版システム運用編 [Control]
厚生労働省保険局	オンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書【医療機関・薬局】（令和 3 年 12 月）
厚生労働省保険局	訪問診療等におけるオンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書【医療機関・薬局・訪問看護ステーション】（令和 5 年 11 月）
厚生労働省	オンライン資格確認等、レセプトのオンライン請求及び健康保険組合に対する社会保険手続きに係る電子申請システムに係るセキュリティに関するガイドライン（令和 2 年 10 月（令和 6 年 1 月一部改正））

Ⅲ. 調査内容

1. 医療法施行規則の一部改正によるセキュリティ要件ついて

医療法施行規則の一部を改正する省令（令和 5 年厚生労働省令第 20 号。以下「改正省令」[2]という。）が公布され、令和 5 年 4 月 1 日から施行された[3]。本改正省令は、令和 5 年 4 月 1 日より施行され、病院、診療所又は助産所の管理者は、医療の提供に著しい支障を及ぼすおそれがないように、サイバーセキュリティを確保するために必要な措置を講じなければならない」ことが定められた。そして、厚生労働省は留意事項として、この“必要な措置”とは、「最新の「医療情報システムの安全管理に関するガイドライン（以下、「医療情報システムガイドライン」という。）」を参照の上、サイバー攻撃に対する対策を含めセキュリティ対策全般について適切な対応を行うこと」であるとしている。介護分野においては、介護保険法の法体系においてセキュリティ要件は規定されていない。

2. 医療法第 25 条に基づく立ち入り検査について

医療機関への立入検査について、主にセキュリティ対策項目が含まれる第 25 条第 1 項に基づく立ち入り検査[4]について厚生労働省より公表された資料を基に文献調査を行った。

近年、増大しているサイバーセキュリティへの対策は急務であり、健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループ[5]での検討を踏まえ、医療法第 25 条第 1 項に規定に基づく立入検査要綱[6]の項目に、「サイバーセキュリティ確保のための取組状況」が位置付けられた。検査要綱には医療法施行規則第 14 条第 2 項に基づいて、「サイバーセキュリティの確保」の項目が追加されており、サイバーセキュリティを確保するために必要な措置を講じているか否かを確認することとされている。必要な措置については、「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」を参照することとされている。また、同ガイドラインのなかで、医療機関において優先的に取り組むべき事項として、「『医療機関におけるサイバーセキュリティ対策チェックリスト[7]』及び『医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～[8]』について」に示される「医療機関におけるサイバーセキュリティ対策チェックリスト」に必要な事項が記入されていることを確認することとされている。

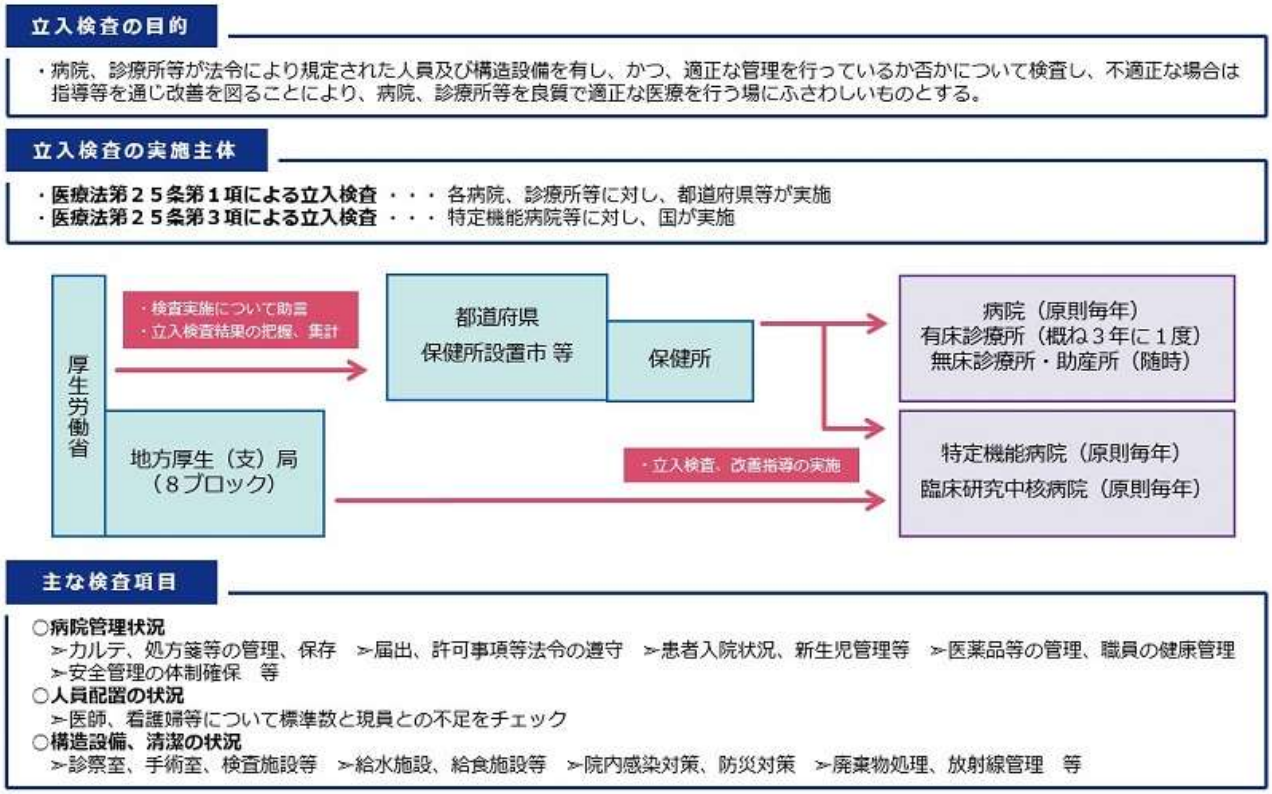
特に、上記チェックリストにおいて医療機関に求める項目のうち、インシデント発生時の連絡体制図については、連絡体制図の提示を求めることにより、その有無を確認することとされている。

立ち入り検査の概要について、以下に示す。

---

[2] 厚生労働省、医療法施行規則の一部を改正する省令の施行等について：
https://www.mhlw.go.jp/content/10800000/001096955.pdf
[3] 厚生労働省、医療法施行規則の一部を改正する省令について：
https://www.mhlw.go.jp/content/10808000/001075881.pdf
[4] 厚生労働省、医療法に基づく立入検査について：
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/i-anzen/tachiirikensa.html
[5] 厚生労働省、健康・医療・介護情報利活用検討会 医療等情報利活用ワーキンググループ」：
https://www.mhlw.go.jp/stf/shingi/other-isei_210261.html
[6] 厚生労働省、「医療法第 25 条第1項の規定に基づく立入検査要綱の一部改正について」：
https://www.mhlw.go.jp/content/10800000/001111903.pdf
[7] 厚生労働省、「医療機関におけるサイバーセキュリティ対策チェックリスト」：
https://www.mhlw.go.jp/content/10808000/001139055.pdf
[8] 厚生労働省、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～」：
https://www.mhlw.go.jp/content/10808000/001105752.pdf

図表 6 医療法第 25 条に基づく立ち入り検査



（出所）厚生労働省 HP、「医療法に基づく立ち入り検査について」より抜粋。

（https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/i-anzen/tachiirikensa.html）

医療分野では、法令に基づく立ち入り検査が実施されるため、介護分野よりセキュリティ対策についての強制力が働いていると思料する。介護分野においては、介護保険法関連法令の体系の中でセキュリティ対策を法令に基づいてチェックする仕組みを有してはいない。

3. 医療情報システムの安全管理に関するガイドラインについて

医療機関・薬局においては令和 5 年 4 月からオンライン資格確認の導入が原則義務化されており、医療情報システムの安全管理ガイドラインに記載されているネットワーク関連のセキュリティ対策がより多くの医療機関等に共通して求められるため、こうした状況を踏まえて医療情報システムの安全管理に関するガイドライン[9]（以下、「医療情報システムガイドライン」という。）は、令和5年5月に改定された。医療情報システムガイドライン第 6.0 版では、想定読者の役割に応じて、本文を概説編[10]、経営管理編[11]、企画管理編[12]及びシステム運用編[13]に分けられ、想定される読者に求められる遵守事項及び考え方を示す

[9]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）」
https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html
[10]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 版概説編[Overview]:
https://www.mhlw.go.jp/content/10808000/001102570.pdf
[11]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 版経営管理編[Governance]:
https://www.mhlw.go.jp/content/10808000/001102573.pdf
[12]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 版企画管理編[Management]:
https://www.mhlw.go.jp/content/10808000/001102575.pdf
[13]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 版システム運用編[Control]:
https://www.mhlw.go.jp/content/10808000/001112044.pdf

とともに、Q＆A等において現状で選択可能な具体的な技術に言及する構成に見直しされた。想定される読者と主要な内容は、概説編、「3.1 各編の目的・概要」に示されているように以下のとおりである。

- 経営管理編：主に医療機関等において組織の経営方針を策定し、意思決定を担う経営層を対象にしており、医療機関等における医療情報システムの安全管理の統制を主とする。
- 企画管理編：主に医療機関等において医療情報システムの安全管理（企画管理、システム運営）の実務を担う担当者（企画管理者）を対象にしており、医療機関等全体の安全対策の管理、組織的な対応に関する対策を主とする。
- システム運用編：主に医療機関等において医療情報システムの実装・運用の実務を担う担当者を対象にしており、技術的な対応に関する対策を主とする。

文書の構成のほか、併せて外部委託、外部サービスの利用に関する整理、情報セキュリティに関する考え方の整理、新技術、制度・規格の変更への対応について改定が行われた。

医療情報システムガイドラインについて、各編に対応し、経営管理、企画管理、システム運用編の 3 つの軸で整理した。

医療情報システムガイドライン 6.0 版に記載されているセキュリティ対策は幅広く、すべてを詳細に理解し、リスクを評価した上で自施設に関係する事項を選出してセキュリティ対策を検討して講じることは、特に情報システム部門を持たないような小規模な医療機関、介護事業者には難しい。そのため、医療情報システムガイドライン 6.0 版には別途、特集の文書として、サイバーセキュリティに関係する部分を要約し、具体的な例などにも触れてまとめられた『[特集]医療機関等におけるサイバーセキュリティ[14]』、及び小規模医療機関において、安全管理ガイドラインに示されている安全管理対策を実施するために必要な内容の概略を簡易的に示す『[特集]小規模医療機関等向けガイダンス[15]』がまとめられている。また、「医療機関等におけるサイバーセキュリティ対策チェックリスト[16]」も策定されており、「医療機関におけるサイバーセキュリティ対策チェックリストマニュアル～医療機関・事業者向け～[17]」を参照しながら、最低限のセキュリティ対策から始めることもできる。更に「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」に関する Q&A[18]を参照することにより、セキュリティ対策の考え方、具体的な手法も示されているため、適宜、参照して対策を検討することができる。

医療情報システムガイドライン 6.0 版各編における記載内容及び遵守事項について、抜粋し引用・要約を行った。

- 経営管理（経営者層）

経営管理編は、組織の経営方針を策定し、意思決定を担う経営層が認識すべき考え方や関連法制度等が示されている。経営層として遵守、または判断すべき事項が示され、経営者が企画管理やシステム運営の担当部署及び担当者に対して指示及び管理すべき事項並びにその考え方が示されている。経営管理

---

[14] 厚生労働省、[特集] 小規模医療機関等向けガイダンス：https://www.mhlw.go.jp/content/10808000/001102587.pdf
[15] 厚生労働省、[特集] 医療機関等におけるサイバーセキュリティ：https://www.mhlw.go.jp/content/10808000/001102586.pdf
[16] 厚生労働省、医療機関におけるサイバーセキュリティ対策チェックリスト：https://www.mhlw.go.jp/content/10808000/001139055.pdf
[17] 厚生労働省、医療機関におけるサイバーセキュリティ対策チェックリストマニュアル ～医療機関・事業者向け～：https://www.mhlw.go.jp/content/10808000/001105752.pdf
[18] 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」に関するQ&A https://www.mhlw.go.jp/content/10808000/001145860.pdf

編「はじめに」より、各章における概要を以下のとおり抜粋する。

1. 安全管理に関する責任・責務

・　医療情報の取扱いや医療情報システムの安全管理に関する法令上の遵守事項や義務などを負う。
・　通常時や非常時における安全管理上の説明責任や管理責任を負う。
・　医療情報や医療情報システムに関して委託や第三者提供を行う場合の責任を負う。

2. リスク評価を踏まえた管理運用

・　医療情報及び医療情報システムに対するリスク評価の重要性・リスク評価を踏まえた経営資源・資産の安全管理に関する方針の策定、安全管理対策の必要性を明確にする。
・　情報セキュリティマネジメントシステム（ISMS）を確立する。

3. 安全管理全般（統制、設計、管理等）

・　意思決定・経営層による統制のもと、組織的な対応・技術的な対応として必要な体制や文書を整備し、リスク評価に基づく安全管理方針に従って、適切な安全管理対策を設計し、管理する。
・　安全管理対策の実効性を担保するための自己点検や監査の意義や必要性を明確にする。
・　情報セキュリティインシデントが発生した場合の対応を明確にする。

4. 安全管理に必要な対策全般

・　技術的な安全管理対策について、情報システムの構成を踏まえた分類（クライアント側、サーバ側、インフラ、セキュリティ）と各分類で採用する安全管理措置を明確にする。

5. 医療情報システム・サービス事業者との協働

・　医療情報システム・サービス事業者（以下「システム関連事業者」という。）に対して委託を行う場合の事業者の選定、委託契約や体制の管理、委託先事業者との責任分界や役割分担の明確化と協働体制の確立と管理等を行う。

➢　企画管理（企画管理者、システムの安全管理者）

企画管理編は、経営者が策定した方針等に基づき、組織体制や情報セキュリティ対策に係る規程の整備等の統制等の安全管理の実務に当たり具体的に遵守が必要な事項を示している。整備した事項、統制実態については、経営者に報告、承認を受ける必要がある。また、企画管理者から医療情報システムの実装・運用に関する適切な対応をシステム運用担当者に指示、管理するために必要な事項を示している。

企画管理編に記載されている 1 章から 15 章（電子署名の章を除く）各章の遵守事項を抜粋した。

管理体系における遵守事項は以下のとおり。

1. 管理体系
①医療情報システムの管理に関する法令等について理解し、医療機関等の組織全体として法令等を遵守できるよう、必要な措置を講じること。 ②委託先の医療情報システム・サービス事業者（以下「委託先事業者」という。）等に対しても①に関して必要な措置を講じるよう契約において求め、その対応状況を定期的に把握すること。委託先事業者が再委託を用いる場合も同様の対応をすること。 ③医療機関等内における法令の遵守状況について経営層に報告し、経営層の確認を取ること。また、遵守状況に応じて必要な改善措置を講じること。 ④医療情報システムの安全管理に係る法令等が求める内容を把握した上で、対応策を整理すること。必要に応じて、システム運用担当者と具体的な対策について検討を求めて、その結果を反映すること。 ⑤組織における情報セキュリティ方針、医療情報の取扱いや保護に関する方針及び医療情報システムの安全管理に関する方針を策定し、経営層の承認を得ること。 ⑥⑤で経営層の承認を得た方針を実行するために必要な体制、規程、技術的措置等の整備を行うこと。またこれらが適切に運用されているか確認すること。 ⑦患者等からの照会に対応するために必要な医療情報システムの安全管理に関する窓口等を整備すること。

責任分界における遵守事項は以下のとおり。

2. 責任分界
①医療機関等において生じる責任の内容を踏まえて、委託先事業者その他の関係者との間で責任分界に関する取決めを行うこと。また、重要な委託等に関する責任分界については、取決めに当たり、事前に経営層の承認を得ること。 ②取決めを行う責任分界のうち技術的な部分に関しては、その具体的な内容を検討するようシステム運用担当者に指示を行い、その結果を責任分界の取決めに反映させること。 ③責任分界を取り決める際には、あらかじめ必要な情報を収集した上で、医療機関等におけるリスク管理を踏まえた仕様の適合性に関する調整を委託先事業者等と行うこと。 ④委託先事業者等と責任分界の取決めを行う際には、委託先事業者が提供する医療情報システム・サービスの内容を踏まえて、安全管理に関する役割分担についても取り決めること。 ⑤委託先事業者等において複数の関係者が関与する場合には、その関係を整理し、医療機関等が直接責任分界を取り決める相手方を特定すること。また、関与する関係者への管理なども責任分界の取決めに含めること。さらに、責任分界の取決めに際しては、委託先事業者間での役割分担なども含めて、取決め内容に漏れがないよう留意すること。 ⑥第三者提供を行う際の責任分界については、技術的な内容と手続的な部分の役割分担を含めて取り決めること。

安全管理のための体制と責任・権限は以下のとおり。

3. 安全管理のための体制と責任・権限

①医療情報システムの安全管理の責任を担う者としての位置付け、その業務範囲と権限を明確にし、その内容について経営層の承認を得ること。
②情報システム管理委員会等の組織が構成されている場合には、その業務内容、権限等の運営に関する規程等を策定し、経営層の承認を得ること。
③安全管理に関する技術的な対応を行う担当者を任命し、その業務内容、権限、業務上の義務等を明確にし、経営層の承認を得ること。
④非常時の対応を想定して、安全管理に必要な体制を構築すること。特に医療機関等において発生した情報セキュリティインシデントに対処するための体制として情報セキュリティ責任者（CISO）や CSIRT などの要否を検討し、必要な措置を講じ、その結果を経営層に報告し、承認を得ること。
⑤法律上の対応を含め医療情報の漏洩等が生じた際の必要な体制の構築や手順の策定等の必要な措置を講じ、その結果を経営層に報告し、承認を得ること。
⑥医療機関等内における医療従事者や職員等に対して、医療情報の安全な取扱いに必要な教育や訓練を講じるための体制を整備すること。
⑦医療情報の取扱いに関して委託等を行う場合には、委託先事業者を含めた安全管理に関する体制を整備すること。
⑧医療情報の取扱いの安全性が確保できるよう、内部検査及び監査等の体制を構築すること。
⑨患者等からの相談や苦情への対応を行うための体制を構築すること。
⑩①～⑨までの対応においては、整備した内容を可視化できるようにすること。

医療情報システムの安全管理において必要な規程・文書類の整備における遵守事項は以下のとおり。

4. 医療情報システムの安全管理において必要な規程・文書類の整備

①医療機関等が医療情報システムの安全管理に関して定める各種方針等を実現するために必要な規程等の整備を行い、経営層の承認を取ること。
②規程等に基づいて、医療情報の取扱いや医療情報システムの構築、運用を行うために必要な規則類の整備を行うこと。規則類は必要に応じて見直しを行うこと。
③医療情報システムの構築、運用における通常時の対応に必要なマニュアル類や各種資料の整備を担当者に指示し、確認すること。
④非常時における医療情報システムの運用等に関するマニュアル類や各種資料の整備を担当者に指示し、整備状況を確認の上、経営層に報告すること。

安全管理におけるエビデンスにおける遵守事項は以下のとおり。

5. 安全管理におけるエビデンス

①医療情報システムの安全管理の状況を把握するために必要な証跡について整理し、当該証跡の整備について必要な対応を行うこと。
②証跡の整備に当たっては、証跡により管理する安全管理の対象の目的や特性に応じたものとすることに留意すること。また証跡の改ざん等を防止する措置を講じること。
③収集した証跡に対するレビュー等を行い、医療情報システムの安全管理の状況を把握し、必要があれば証跡の整備に関する改善を行うこと。
④法令で求められる医療情報の管理に関する証跡を、必要に応じて、説明責任等を果たせるように管理すること。

リスクマネジメント(リスク管理)における遵守事項は以下のとおり。

6. リスクマネジメント(リスク管理)

①医療機関等内でリスクマネジメントが適切に実施されているかどうかを管理し、その状況を経営層に報告すること。また、リスクマネジメントに不備がある場合には、改善策を検討して必要な措置を講じること。
②医療情報システムで取り扱う医療情報及び関連する情報を全てリストアップし、安全管理上の重要度に応じて分類し、常に最新の状態が維持されていることを確認すること。
③医療情報システムで取り扱う情報及び関連する情報に関するリストを作成し、必要に応じて速やかに確認できる状態で管理すること。
④安全性が損なわれた場合の影響の大きさに応じて医療情報システムで取り扱う情報及び関連する情報の安全管理上の重要度を分類すること。
⑤②～④を踏まえて、リスク分析やリスク評価を、担当者と協働して行うこと。
⑥経営層がリスク評価を踏まえたリスク判断をする際に必要な資料を整理すること。
⑦リスク評価の結果、リスク管理の方針に関する説明責任に関する資料等を整理し、経営層が説明責任を果たすために必要な対応を行うこと。
⑧リスク評価の結果を経営層に報告し、承認を得ること。また承認を踏まえて安全管理対策を講じること。
⑨PDCA(Plan-Do-Check-Act)モデルに基づく ISMS(Information Security Management System:情報セキュリティマネジメントシステム)を構築し、管理すること。また、ISMS が適切に実施されていることを確認し、経営層にその状況を報告すること。
⑩PDCA モデルの実施において不備等が認められる場合には、その原因を確認した上で改善策を講じ、経営層に報告し、承認を得ること。

安全管理のための人的管理(職員管理、事業者管理、教育・訓練、事業者選定・契約)における遵守事項は以下のとおり。

7. 安全管理のための人的管理(職員管理、事業者管理、教育・訓練、事業者選定・契約)

①医療情報を取り扱う者を職員として採用するに当たっては、雇用契約に雇用中及び退職後の守秘・非開示に関する条項を含める等の安全管理対策を実施すること。
②個人情報の安全管理に関する職員への教育・訓練を採用時及び定期的に実施すること。また、教育・訓練の実施状況について定期的に経営層に報告すること。
③医療機関等の事務、運用等を外部の事業者に委託する場合は、委託契約の契約書に守秘・非開示に関する内容を含めること。
④③の委託契約の際に、当該委託先事業者の就業規則等に①及び②の対応を含めるよう求めること。
⑤外部の事業者との契約に基づいて医療情報を外部保存する場合、以下の対応を行うこと。重要度の高い委託の場合は、経営層に丁寧に報告し、承認を得ること。
－保存した医療情報の取扱いに関して監督できるようにするため、外部保存の委託先事業者及びその管理者、電子保存作業従事者等に対する守秘義務に関連する事項やその事項に違反した場合のペナルティを契約書等で定めること。
－医療機関等と外部保存の委託先事業者を結ぶネットワークインフラに関しては、委託先事業者にも本ガイドラインを遵守させること。
－総務省・経済産業省の定めた「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」を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等して遵守状況を確認すること。
－外部保存の委託先事業者の選定に当たっては、システム関連事業者の情報セキュリティ対策状況を示した資料を確認すること。(例えば、「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」における「サービス仕様適合開示書」の提供を求めて確認することなどが挙げられる。)
－外部保存の委託先事業者に、契約書等で合意した保守作業に必要な情報以外の情報を閲覧させないこと。
－保存した情報(Cookie、匿名加工情報等、個人を特定しない情報を含む。本項において以下同じ。)を独断で分析、解析等を実施してはならないことを契約書等に明記し、外部保存の委託先事業者に遵守させること。
－保存した情報を外部保存の委託先事業者が独自に提供しないよう、契約書等で情報提供のルールについて定めること。外部保存の委託先事業者に情報の提供に係るアクセス権を設定する場合は、適切な権限を設定させ、情報漏洩や、誤った閲覧(異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等)が起こらないよう求めること。
－保存された情報を格納する情報機器等が、国内法の適用を受けることを確認すること。
⑥外部保存の委託先事業者を選定する際は、少なくとも次に掲げる事項について確認すること。
a 医療情報等の安全管理に係る基本方針・取扱規程等の整備状況
b 医療情報等の安全管理に係る実施体制の整備状況
c 不正ソフトウェア等のサイバー攻撃による被害を防止するために必要なバックアップの取得及び管理の状況
d 実績等に基づく個人データ安全管理に関する信用度

e 財務諸表等に基づく経営の健全性
f プライバシーマーク認定又は ISMS 認証の取得
g「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」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無
・政府情報システムのためのセキュリティ評価制度（ISMAP）
・JASA クラウドセキュリティ推進協議会 CS ゴールドマーク
・米国 FedRAMP・AICPASOC2（日本公認会計士協会 IT7 号）
・AICPASOC3（SysTrust/WebTrust）（日本公認会計士協会 IT2 号）
上記認証等が確認できない場合、下記のいずれかの資格を有する者による外部監査結果により、上記と同等の能力の有無を確認すること
・システム監査技術者
・Certified Information Systems Auditor ISACA 認定
h 医療情報を保存する情報機器が設置されている場所（地域、国）
i 委託先事業者に対する国外法の適用可能性
⑦医療情報の外部保存の委託先事業者との契約には、以下の内容を含めること。
－委託元の医療機関等、患者等の許可なく保存を受託した医療情報を分析等の目的で取り扱わないこと。
－保存を受託した医療情報の分析等は正当な目的の場合に限り許可されること。
－匿名化した情報であっても、匿名化の妥当性の検証を行う、及び院内掲示等を使って取扱いをしている事実を患者等に知らせるなどして、個人情報保護に配慮した上で取り扱うこと。
－保存を委託する医療機関等に患者がアクセスし、自らの記録を閲覧できるような仕組みを提供する場合は、外部保存の委託先事業者に適切な利用者権限や閲覧の範囲を設定し、情報漏洩や、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないように配慮すること。
－情報の提供は、原則、患者が受診している医療機関等と患者との間での同意に基づいて実施すること。⑧委託先事業者が契約に基づいて必要な対応を行っていることを定期的に確認するため、委託先事業者に報告を求めること。当該報告の結果、改善が必要である場合にはその旨を求めること。また委託先事業者からの報告内容については、経営層に報告し、承認を得ること。
⑨委託契約終了に際し、医療情報の返却とその方法など、委託先事業者が行うべき内容についてあらかじめ契約により取り決めておくこと。
⑩外部保存の委託に当たり、あらかじめ患者に対して、必要に応じて個人情報が特定の外部の施設に送付・保存されることについて、その安全性やリスクを含めて院内掲示等を通じて説明し、理解を得ること。

情報管理(管理、持ち出し、破棄等)における遵守事項は以下のとおり。

8. 情報管理(管理、持ち出し、破棄等)

①医療機関等において保有する医療情報の管理、医療機関等外への持ち出し、破棄等の方針と手順等を含む情報管理に関する規程等を定め、当該規程等に基づいて適切に医療情報を管理すること。

②医療機関等において保有する医療情報の管理において、各医療情報に関する管理責任者を定め、適切に管理するよう指示すること。また、管理責任者から管理状況に関する報告を受け、必要に応じて改善を指示すること。

③医療情報が保存されている場所等については、記録・識別、入退室の制限等の管理を行うこと。また、医療情報の保管場所には施錠等の対応を行うこと。

④医療機関等における医療情報の管理状況を把握し、経営層の承認を得ること。管理状況の把握のため、医療機関等で保有する医療情報について定期的な棚卸や管理実態の確認を行うこと。特に患者に関する情報は、患者ごとに識別できるよう、管理すること。

⑤医療機関等外への医療情報の持ち出しに関する手順等を定める際は、リスク評価に基づいて、医療情報の持ち出しに関する対応方針や、持ち出す情報、持ち出し方法や管理方法について情報管理に関する規程で定めること。

⑥医療機関等外への医療情報の持ち出しに関する手順等を定める際は、医療情報を記録した媒体や情報機器を用いる持ち出しのほか、ネットワークを通じて外部に医療情報を送信し、又は外部から医療情報を保存する場所等にネットワークを通じて医療情報の閲覧や受信・取り込みを行う場合も想定すること。

⑦持ち出した医療情報を格納する(外部からアクセスして格納する場合を含む。)記録媒体や情報機器の盗難、紛失が生じた際の対応について情報管理に関する規程に定めること。

⑧医療機関等の外部からのアクセスについて、許諾対象者、許諾条件やアクセス範囲等、許諾を得るための手順等を定めること。

⑨患者等に情報を閲覧させるために医療情報システムへのアクセスを許可する場合には、患者等に対して、情報セキュリティに関するリスクや情報提供目的について説明を行い、それぞれの責任範囲を明確にすること。

⑩医療情報の持ち出し状況について定期的なレビューを行い、持ち出し状況の適切な管理を行うこと。

⑪医療情報の破棄に関する手順等を定める際は、情報種別ごとに破棄の手順を定めること。当該手順には破棄を行う条件、破棄を行うことができる職員、具体的な破棄方法を含めること。

⑫保存等を委託している医療情報を破棄する場合、委託先事業者に対して、医療情報の破棄等(格納する記録媒体・情報機器等の破壊含む)を行ったことについての証跡等の提出を求めること。システム関連事業者のサービス等の性格上、破棄等を行ったことの証跡の提出を求めることが困難な場合には、当該事業者における破棄等の手順等の提供を求め、委託先事業者における破棄の手順等が、医療機関等が定める破棄の手順等に適合するよう、事前に協議した上で、委託契約等の内容にも含めること。

医療情報システムに用いる情報機器等の資産管理における遵守事項は以下のとおり。

9. 医療情報システムに用いる情報機器等の資産管理

①医療情報システムにおいて用いる情報機器等の資産管理を行うのに必要な規程その他の資料を整備し、その管理を行うこと。(なお、情報機器等には、物理的な資産のほか、医療情報システムが利用するサービス、ライセンスなども含む。)

②医療機関等が管理する情報機器等について、台帳管理等を行うこと。台帳管理等の対象は、医療機関等内部の購入部署や購入形態に関わらず、医療情報システムで利用する情報機器等全てとすること。

③台帳管理されている医療情報システムに用いる情報機器等の棚卸を定期的に行い、存在確認を行うこと。また担当者と協働して、滅失状況などについても適宜確認すること。

④医療情報システムにおいて利用する情報機器等が、安全管理の観点から利用に適した状況にあることを定期的に確認すること。確認にあたっては、システム運用担当者に対して、情報機器等における状況(ソフトウェアやファームウェアのアップデートの状況、脆弱性に関する対応状況等)を確認するよう指示し、報告を受け、適宜必要な対応を行うこと。

⑤医療情報システムが利用するサービスに関して、安全管理の観点から、利用に適した状況にあることを定期的に確認すること。確認にあたっては、システム運用担当者に対してサービスにおける状況(サービスの機密性、クラウドサービス等における可用性、システム関連事業者が示す規約内容の変更状況等)が適切なものとなっていることを確認するよう指示し、報告を受けた上で、必要があれば契約変更等の対応を行うこと。

⑥医療機関等が管理しない情報機器で、医療情報システムに用いるもの(例えば BYOD(Bring Your Own Device:個人保有の情報機器)の利用による端末)について、利用を許諾する条件や、利用範囲、管理方法等に関する内容を規程等に含めること。また、これに基づいて利用される情報機器等について、利用の許諾状況も含めて、医療機関等が管理する情報機器同様に、台帳管理等を行うこと。

⑦医療情報システムで利用する情報機器等の資産管理状況を把握した上で、経営層に報告し、承認を得ること。

運用に対する点検・監査における遵守事項は以下のとおり。

10. 運用に対する点検・監査

①医療機関等における医療情報システムの安全管理が適切に行われていることを把握するため、運用の点検を行うこと。技術的な対応に関しては、担当者に点検を命じ、その報告を受け、確認すること。点検に際しては、各規程、手順等による運用が適切に行われていることを、「5. 安全管理におけるエビデンス」で整備した証跡に基づいて確認し、必要があれば改善を行うこと。

②医療情報システムの取扱いを委託している場合は、委託先事業者において医療情報システムの安全管理が適切になされていることを、委託先事業者からの報告に基づいて確認すること。医療情報システム・サービスの性格上、報告に基づく確認が難しい場合は、SLA に対する評価等の中で確認すること。

③医療情報システムの取扱いに関する点検結果を、経営層に報告し、承認を得ること。

④医療情報システムの取扱いの安全管理の状況を客観的に把握するために、定期的に、医療機関等内の企画管理者や担当者から独立した組織又は第三者による監査を実施すること。監査の実施に際しては、監査方針と監査計画を策定の上、経営層の承認を得ること。また、監査結果については、経営層に報告し、承認を得ること。監査結果における指摘事項を踏まえて、適宜管理の見直し等を図ること。

非常時(災害、サイバー攻撃、システム障害)対応と BCP 策定における遵守事項は以下のとおり。

11. 非常時(災害、サイバー攻撃、システム障害)対応と BCP 策定
①医療情報システムの安全管理に関して、非常時における対応方針と対応手順・内容の整理を行い、経営層の承認を得ること。対応方針には、非常時の定義のほか、通常時への復旧に向けた計画を含めること。 ②医療機関等が定める非常時の定義や BCP(Business Continuity Plan:事業継続計画)との整合性を確認して対応方針を策定すること。 ③非常時において、法令で求められる対応を事前に整理し、非常時に速やかに対応できる体制を講じること。 ④各種規程等に非常時における対応手順・内容も含めること。 ⑤非常時における安全管理対策について、担当者に対策の実装と対策を踏まえた文書の整備を指示し、確認すること。 ⑥非常時における対応に関して、医療機関等の職員、外部の関係者等に対する教育を行うほか、定期的に訓練を実施すること。訓練等の結果や評価を、適宜、非常時の対応手順等に反映させること。 ⑦非常時への対応状況を定期的に確認し、経営層に報告の上、承認を得ること。 ⑧非常時の事象が生じた場合、安全管理の状況を適宜把握し、経営層に報告すること。 ⑨非常時の事象が生じた場合、関係者に対する説明責任等を果たすため、報告対応や広報対応を行うこと。 ⑩非常時の事象発生に伴い対応した内容について、事後検証を行い、その内容を経営層に報告し、承認を得ること。その検証結果や評価を、適宜、非常時の対応手順等に反映させること。

サイバーセキュリティにおける遵守事項は以下のとおり。

12. サイバーセキュリティ

①サイバーセキュリティに関する組織的対策、医療機関等の職員等や委託先事業者などの対策を検討し、整理すること。技術的な対応・措置については、担当者にリスク評価を踏まえた対策の検討を指示し、状況を確認すること。

②医療機関等において整理したサイバーセキュリティ対策を踏まえ、サイバーセキュリティ対応計画を策定し、当該計画の内容について経営層に報告し、承認を得ること。

③サイバーセキュリティ対応計画を踏まえ、その内容を医療機関等で定める各規程や手順等に反映すること。

④サイバーセキュリティ対応計画を踏まえ、各対策の実施状況を確認する。技術的な対応・措置については、担当者に対応計画を踏まえた文書の整備を指示し、対応状況を確認すること。

⑤サイバーセキュリティ対応計画を踏まえた訓練を定期的に実施し、その結果を経営層に報告し、承認を得ること。また、訓練結果を踏まえ、対応計画の検証・見直しを実施し、必要に応じて対応計画等の改善を行うこと。

⑥サイバーセキュリティ事象による非常時対応が生じた場合に情報交換等を行う関係者の情報をあらかじめ整理した上で、必要に応じて契約等を行うこと。（ここでいう関係者には、利用する医療情報システム・サービスのシステム関連事業者をはじめ、報告対象となる行政機関等、その他必要に応じて助言等の支援を求める外部有識者等が含まれる。）

⑦サイバー攻撃を受けた（疑い含む）場合や、サイバー攻撃により障害が発生し、個人情報の漏洩や医療サービスの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、「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 日付け医政総発 1029 第 1 号・医政地発 1029 第 3 号・医政研発 1029 第 1 号厚生労働省医政局関係課長連名通知）に基づき、所管官庁への連絡等の必要な対応を行うほか、そのために必要な体制を整備すること。また、上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行うこと。

⑧サイバーセキュリティ事象による非常時対応が生じた場合には、その状況について、定期的に経営層に報告すること。また、当該事象を踏まえ、サイバーセキュリティ対応計画の検証・見直しを実施し、必要に応じて改善を行うこと。

⑨サイバーセキュリティ事象による非常時としての対応が生じた場合には、「11. 非常時（災害、サイバー攻撃、システム障害）対応と BCP 策定」に示す内容を実施すること。

医療情報システムの利用者に関する認証等及び権限における遵守事項は以下のとおり。

13. 医療情報システムの利用者に関する認証等及び権限

①リスク評価に基づいて、医療情報システムにおける利用者の認証等及びアクセス権限に関する規程を整備し、管理すること。

②医療情報システムで利用する認証方法が安全なものとなるよう、担当者に対して、リスク評価に基づいて適切な方法を採用することを指示し、その報告を受けること。

③医療機関等の内部における利用者については、医療機関等に所属することが前提となるよう管理すること。所属に関する実態を認証の仕組みにおいて適切に反映できるよう、担当者に対して、人事等の情報と整合性をとって利用者の ID 等を付与する等の必要な手順を作成するよう指示すること。

④医療情報システムの利用権限は、医療従事者の資格や医療機関内の権限規程に応じたものとなっていることが前提となるよう管理すること。資格や権限に関する実態を認証の仕組みにおいて適切に反映できるよう、担当者に対して、利用者が所属する部署等からの申請を踏まえて権限を付与し、その結果について申請部署の管理者から確認を得る等の必要な手順を作成するよう指示すること。

⑤医療機関等の外部の利用者について、医療情報システムの利用におけるアクセス権限とアクセス状況を管理すること。医療情報システムの利用用途とアクセス範囲、アクセス権限等をリスク評価に基づいて整理した上で、その内容に応じて ID やアクセス権限を付与すること。その具体的な手順については、担当者に作成を指示すること。

⑥医療情報システムの管理権限や、医療情報システム、情報機器等で用いる ID 等の安全管理を行うこと。管理権限については、担当者に対して、医療情報システムにおいて利用される管理権限の種類とその ID、利用が認められている者等を管理して一覧化するよう指示すること。システム等で用いる ID 等については、担当者に安全性の確認を指示し、必要に応じて認証に関する情報の変更等を指示すること。

⑦医療情報システムで利用する ID 等についての棚卸を定期的に行い、不要なものについては削除すること。棚卸については、担当者に具体的な手順等の策定を指示すること。また、棚卸結果を経営層に報告し、承認を得ること。

⑧電子カルテにおける記録の確定に関して、以下の事項を規程等に含めること。

－入力者及び確定者の識別・認証

－記録の確定手順、識別情報の記録の保存

－更新履歴の保存

－代行入力を実施する場合、代行入力を認める業務、代行が許可される依頼者と実施者

技術的な安全管理対策の管理における遵守事項は以下のとおり。

15. 技術的な安全管理対策の管理

①物理的安全管理対策のうち医療情報及び医療情報システムを保管する場所について、リスク評価を踏まえて、その場所の選定を担当者と協働して検討し、その結果を経営層に報告の上、承認を得ること。なお、選定にあたっては、医療機関等において医療情報システムに関する整備計画等を策定している場合には、これと整合性をとること。

②個人情報の保存場所及び入力・参照可能な端末等が設置されている区画等への入退室管理（施錠、識別、記録）を行うよう、管理内容を含む規程等を策定すること。

③記録媒体及び記録機器の保管及び取扱いについて、運用管理規程を作成し、適切な保管及び取扱いを行うよう関係者に周知徹底するとともに、教育を実施すること。また、保管及び取扱いに関する作業履歴を残すこと。

④医療情報システムが情報を保存する場所（内部、可搬媒体）を明示し、その場所ごとの保存可能容量（サイズ）、期間、リスク、レスポンス、バックアップの頻度や方法等を明確にすること。これらを運用管理規程に定め、その運用を関係者全員に周知徹底すること。

⑤記録媒体の劣化への対応を図るための一連の運用の流れを運用管理規程に定めるとともに、関係者に周知徹底すること。

⑥システム運用に関する安全管理対策として必要な項目を担当者と協働して検討すること。特に医療情報システムの脆弱性（不正ソフトウェア対策ソフトウェアやサイバー攻撃含む）への対策に関する項目については、定期的に見直しを図ること。

⑦医療機関等において利用するネットワークについて、リスク評価を踏まえつつその選定を担当者と協働して検討し、その結果を経営層に報告の上、承認を得ること。なお、選定にあたっては、医療機関等において医療情報システムに関する整備計画等を策定している場合には、これと整合性をとること。また、ネットワークの安全性確保を目的とした実装と運用設計を行った場合には、その内容を確認の上、経営層に報告し、承認を得ること。

⑧保守に関する安全管理対策として必要な項目を担当者と協働して検討すること。また、必要に応じて、保守を行うシステム関連事業者と契約や SLA 等により管理項目について取決めを行うこと。

⑨医療情報システムの動作確認や保守においては、原則として個人情報を含む医療情報を用いないことを運用管理規程等に含めること。また、やむを得ず医療情報を用いる場合には、漏洩等が生じないために必要な対策を講じる旨を示し、その具体的な手順の策定を担当者に指示すること。

⑩医療情報システムで用いるシステム、サービス、情報機器等の品質を適切に管理し、必要に応じて、改善措置を講じること。品質の管理方法については、担当者と協働して検討すること。

⑪情報機器、ソフトウェアの品質管理に関する対応を運用管理規程で定めるとともに、具体的な手順の作成と実施を担当者に指示すること。

⑫システム構成やソフトウェアの動作状況に関する内部監査を定期的に実施すること。

⑬医療情報システムが法令等で求められている要件を満たすよう適切に管理すること。特に「施行通知」、「外部保存通知」などで求める要件を満たしていることを確認し、調達においては当該要件を満たす内容とすること。具体的な確認項目や、医療情報システムにおける実装内容等については、担当者に確認の上、必要な検討を行うよう指示すること。

⑭①～⑬において、担当者が整備した対策について、関連規程等に反映すること。また、システム運用の実施状況については、定期的に担当者から報告を受け、その状況を把握の上、経営層に報告し承認を得ること。

➢ システム運用(システム運用担当者)

システム運用編は、経営層や企画管理者の指示に基づき、医療情報システムを構成する情報機器、ソフトウェア、インフラ等の各種資源の設計、実装、運用等の実務を担う担当者として適切に対応すべき事項とその考え方が示されている。なお、医療情報システムの実装・運用において、医療機関等が事業者に委託し、その業務や責任について分担を検討する必要がある。医療機関等と協働する際の業務や役割、責任の分担の在り方については、あらかじめ両者で取り決めておくこと必要がある。

安全管理を実現するための技術的対策の体系は 6 章で説明されており、システム運用担当者は、医療情報システムの安全管理に関する技術的な対応を検討する際に、下記の体系に従った内容を参考として検討することとされている。安全管理対策に関するシステムアーキテクチャ(クライアント側、サーバ側、インフラ、セキュリティ)に関して、以下図に示す。

図表 7 安全管理を実現するための技術的対策の体系の概要

クライアント側	・情報の持出し・管理・破棄等に関する安全管理措置 ・利用機器・サービスに対する安全管理措置
サーバ側	・ソフトウェア・サービスに対する要求事項・事業者による保守対応等に対する安全管理措置 ・事業者選定と管理 ・システム運用管理(通常時・非常時等)
インフラ	・物理的安全管理措置(サーバルーム等、バックアップ) ・ネットワークに関する安全管理措置 ・インフラ運用管理(通常時・非常時等)
セキュリティ	・認証・認可に関する安全管理措置 ・電子署名、タイムスタンプ ・証跡のレビュー、システム監査 ・外部からの攻撃に対する安全管理措置

(出所)医療情報システムガイドラインのシステム運用編[Control]6. 安全管理を実現するための技術的対策の体系 [Ⅰ～Ⅳ]①遵守事項に基づいて株式会社三菱総合研究所にて表を作成

医療情報システムガイドライン 6.0 版システム運用編[Control]では、クライアント側、サーバ側、インフラ、セキュリティとして区分し、それぞれ関する技術的な対策を遵守事項として整理しているため、7 章から 18 章(電子署名の章を除く)の安全管理措置等について遵守事項を抜粋した。

情報管理(管理・持出し・破棄等)における遵守事項は以下のとおり。

7. 情報管理(管理・持出し・破棄等)

①医療情報及び情報機器の持出しについて、運用管理規程に基づき、手順の策定と管理を行い、その状況を定期的に企画管理者に報告すること。
②保守業務を行う事業者に対して、原則として個人情報を含むデータの持出しを禁止すること。やむを得ず持ち出しを認める場合には、企画管理者の承認を得て許諾すること。
③医療情報及び情報機器等の持出しに際しての盗難、置き忘れ等に対応する措置として、医療情報や情報機器等に対する暗号化やアクセスパスワードの設定等、容易に内容を読み取られないようにすること。
④持ち出した利用者が情報機器を、医療機関等が管理しない外部のネットワークや他の外部媒体に接続したりする場合は、不正ソフトウェア対策ソフトやパーソナルファイアウォールの導入等により、情報端末が情報漏洩、改ざん等の対象にならないような対策を実施すること。
⑤持ち出した情報機器等について、公衆無線 LAN の利用がなされた場合には、利用後に端末の安全性が確認できる手順を策定すること。
⑥持ち出した医療情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールするとともに、原則として情報機器に対する変更権限がないような設定を行うこと。業務に使用しないアプリケーションや機能については削除又は停止するか、業務に対して影響がないことを確認すること。
⑦医療情報が格納された可搬媒体及び情報機器の所在を台帳等により管理する手順を作成し、これに基づき持出し等の対応を行う。併せて定期的に棚卸を行う手順を作成する。
⑧セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置の IoT 機器を患者等に貸し出す際は、事前に、情報セキュリティ上のリスクと、患者等が留意すべきことについて患者等へ説明し、同意を得ること。また、機器に異常や不都合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者等に情報提供すること。
⑨破棄に関する規程を踏まえて、把握した情報種別ごとに具体的な破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる職員、具体的な破棄方法を含めること。また情報の破棄については、企画管理者に報告すること。
⑩情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこと。また、破棄終了後に、残存し、読み出し可能な医療情報がないことを確認すること。
⑪外部保存を受託する事業者に破棄を委託した場合は、確実に医療情報が破棄されたことを、証憑または事業者の説明により確認すること。
⑫保守作業等のどうしても必要な場合を除いてリモートログインを行うことができないように、適切に管理されたリモートログインのみに制限する機能を設けなければならない。
⑬利用者による外部からのアクセスを許可する場合は、盗聴、なりすまし防止及びアクセス管理を実現した VPN 技術により安全性を確保した上で、仮想デスクトップ等を利用する運用の要件を設定すること。
⑭患者等に医療情報を閲覧させる場合、医療情報を開示しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、例えば、システムやアプリケーションを切り分け、ファイアウォール、アクセス監視、通信の TLS 暗号化、PKI(Public Key Infrastructure:公開鍵暗号基盤)認証等の対策を実施すること。

利用機器・サービスに対する安全管理措置における遵守事項は以下のとおり。

8. 利用機器・サービスに対する安全管理措置

①システム構築時、適切に管理されていない記録媒体の使用時、外部からの情報受領時には、コンピュータウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられる記録媒体を利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。
②常時不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持(例えばパターンファイルの更新の確認・維持)を行うこと。
③医療情報システムに接続するネットワークのトラフィックにおける脅威の拡散等を防止するために、不正ソフトウェア対策ソフトのパターンファイルや OS のセキュリティパッチ等、リスクに対してセキュリティ対策を適切に適用すること。
④メールやファイル交換にあたっては、実行プログラム(マクロ等含む)が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理を行うこと。なお、保守等でやむを得ずファイル送信等を行う場合、送信側で無害化処理が行われていることを確認すること。
⑤情報機器に対して起動パスワード等を設定すること。設定に当たっては製品等の出荷時におけるパスワードから変更し、推定しやすいパスワード等の利用を避けるとともに、情報機器の利用方法等に応じて必要があれば、定期的なパスワードの変更等の対策を実施すること。
⑥IoT 機器を利用する場合、次に掲げる対策を実施すること。検査装置等に付属するシステム・機器についても同様である。
(1)IoT 機器により医療情報を取り扱う場合は、製造販売業者から提供を受けた当該医療機器のサイバーセキュリティに関する情報を基にリスク分析を行い、その取扱いに係る運用管理規程を定めること。
(2)IoT 機器には、製品出荷後にファームウェア等に関する脆弱性が発見されることがある。システムやサービスの特徴を踏まえ、IoT 機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、運用すること。
(3)使用が終了した又は不具合のために使用を停止した IoT 機器をネットワークに接続したまま放置すると不正に接続されるリスクがあるため、対策を実施すること。
⑦企画管理者と協働して、医療情報システムで用いる情報機器等やソフトウェアの棚卸を行うための手順を策定し、定期的に実施すること。棚卸の際には、情報機器等の滅失状況なども併せて確認すること。
⑧BYOD の実施に関する規程に基づいて、具体的な手順と設定を行い、企画管理者に報告すること。
⑨BYOD であっても、医療機関等が管理する情報機器等と同等の対策が講じられるよう、手順を作成すること。

ソフトウェア・サービスに対する要求事項における遵守事項は以下のとおり。

9. ソフトウェア・サービスに対する要求事項

①システムがどのような情報機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかを明らかにするとともに、システムの機能仕様を明確に定義すること。
②情報機器、ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスを規定すること。
③医療情報システムで利用するシステム、サービス、情報機器等の品質を定期的に管理するための手順を作成し、これに従い必要な措置を講じ、企画管理者に報告すること。
④医療情報システムの目的に応じて速やかに検索表示又は書面に表示できるよう措置を講じること。

医療情報システム・サービス事業者による保守対応等に対する安全管理措置における遵守事項は以下のとおり。

10. 医療情報システム・サービス事業者による保守対応等に対する安全管理措置

①動作確認等の保守作業で事業者が個人情報を含むデータを使用するときは、保守終了後に確実にデータを消去することを求め、その結果の報告を求めること。
②診療録等の外部保存を受託する事業者においては、診療録等の個人情報の保護を厳格に行う必要がある。受託する事業者の管理者であっても、保存を受託した個人情報に、正当な理由なくアクセスできない仕組みが必要である。
③保守を実施するためにサーバに事業者の作業員（保守要員）がアクセスする際には、保守要員の専用アカウントを使用させ、個人情報へのアクセスの有無並びに個人情報にアクセスした場合の対象個人情報及び作業内容を記録すること。なお、これは利用者を模して操作確認を行う際の識別・認証についても同様である。
④リモートメンテナンス（保守）によるシステムの改造・保守作業が行われる場合には、必ずアクセスログを収集し、保守に関する作業計画書と照合するなどにより確認し、当該作業の終了後速やかに企画管理者に報告し、確認を求めること。
⑤リモートメンテナンス（保守）において、やむを得ず事業者が、ファイルを医療機関等へ送信等を行う場合、送信側で無害化処理が行われていることを確認すること。
⑥診療録等を保管している設備に障害が発生した場合等で、やむを得ず診療録等にアクセスをする必要がある場合も、医療機関等における診療録等の個人情報と同様の秘密保持を行うと同時に、外部保存を委託した医療機関等に許可を求めなければならない。

システム運用管理における遵守事項は以下のとおり。

11. システム運用管理（通常時・非常時等）

①非常時の医療情報システムの運用について、次に掲げる対策を実施すること。
－「非常時のユーザカウントや非常時用機能」の手順を整備すること。
－非常時機能が通常時に不適切に利用されることがないようにするとともに、もし使用された場合に使用されたことが検知できるよう、適切に管理及び監査すること。
－非常時用ユーザカウントが使用された場合、正常復帰後は継続使用ができないように変更すること。
－医療情報システムに不正ソフトウェアが混入した場合に備えて、関係先への連絡手段や紙での運用等の代替手段を準備すること。
－サイバー攻撃による被害拡大の防止の観点から、論理的／物理的に構成分割されたネットワークを整備すること。
－重要なファイルは数世代バックアップを複数の方式で確保し、その一部は不正ソフトウェアの混入による影響が波及しない手段で管理するとともに、バックアップからの重要なファイルの復元手順を整備すること。
②医療情報システムの稼働状況などを把握するため、パフォーマンス管理、死活監視などを行うこと。

物理的安全管理措置における遵守事項は以下のとおり。

12. 物理的安全管理措置[Ⅰ、Ⅲなお遵守事項⑤・⑥及び12. 3は、Ⅱ、Ⅳも参照]

①医療情報及び医療情報システムを保管する場所について、リスク評価を踏まえて、その場所の選定を企画管理者と協働して検討し、決定すること。検討に際しては、医療情報を格納する情報機器や記録媒体を物理的に保管するための施設が、災害(地震、水害、落雷、火災等並びにそれに伴う停電等)に耐えうる機能・構造を備え、災害による障害(結露等)について対策が講じられている建築物に設置することなどを考慮すること。

②医療情報を保護する施設について、医療情報を格納する情報機器や記録媒体の設置場所等のセキュリティ境界への入退管理が、個人認証システム等による制御に基づいて行われていることを確認すること。また建物、部屋への不正な侵入を防ぐため、防犯カメラ、自動侵入監視装置等が設置されていることを確認すること。

③個人情報が保管されている情報機器等の重要な情報機器には盗難防止を講じること。

④医療情報及び医療情報システムのバックアップは、企画管理者が定める運用管理規程等と整合性がとれる措置とし、確保したバックアップは非常時に利用できるよう、適切に管理すること。

⑤記録媒体、ネットワーク回線、設備の劣化による情報の読み取り不能又は不完全な読み取りを防止するため、記録媒体が劣化する前に、当該記録媒体に保管されている情報を新たな記録媒体又は情報機器に複写等の情報の保管措置を講じること。

⑥利用者が医療情報を入力・参照する端末から長時間離席する際など、正当な利用者以外の者による入力・参照が生じないよう対策を実施すること。

ネットワークに関する安全管理措置における遵守事項は以下のとおり。

13. ネットワークに関する安全管理措置[Ⅰ、Ⅲ]

①ネットワーク利用に関連する具体的な責任分界、責任の所在の範囲を明らかにし、企画管理者に対して報告すること。

②セッション乗っ取り、IP アドレス詐称等のなりすましを防止するため、原則として医療機関等が経路等を管理する、セキュアなネットワークを利用すること。

③オープンなネットワークからオープンではないネットワークへの接続までの間にチャネル・セキュリティの確保を期待してネットワークを構成する場合には、選択するサービスのチャネル・セキュリティの確保の範囲を電気通信事業者に確認すること。

④オープンではないネットワークを利用する場合には、必要に応じてデータ送信元と送信先での、ルータ等の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の選択するネットワークに応じて、必要な単位で、互いに確認し、採用する通信方式や、採用する認証手段を決めること。採用する認証手段は、PKI による認証、Kerberos のような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等、容易に解読されない方法が望ましい。

⑤ルータ等のネットワーク機器について、安全性が確認できる機器を利用し、不正な機器の接続や不正なデータやソフトウェアの混入が生じないよう、セキュリティ対策を実施すること。特に VPN 接続による場合は、施設内のルータを経由して異なる施設間を結ぶ通信経路の間で送受信ができないように経路を設定すること。

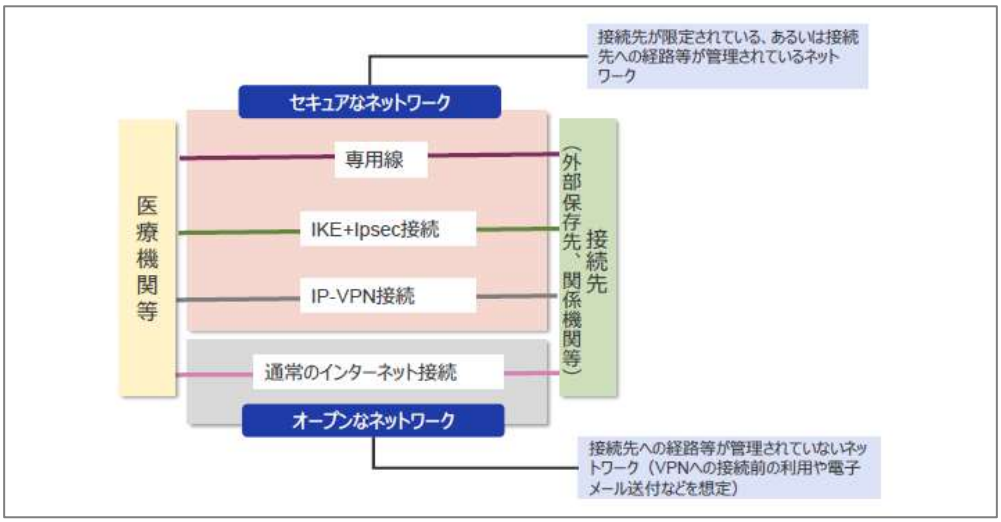
⑥オープンなネットワークにおいて、IPsec による VPN 接続等を利用せず HTTPS を利用する場合、TLS のプロトコルバージョンを TLS1.3 以上に限定した上で、クライアント証明書を利用した TLS クラ

イアント認証を実施すること。ただしシステム・サービス等の対応が困難な場合には TLS1.2 の設定によることも可能とする。その際、TLS の設定はサーバ/クライアントともに「TLS 暗号設定ガイドライン 3.0.1 版」に規定される最も安全性水準の高い「高セキュリティ型」に準じた適切な設定を行うこと。なお、SSL-VPN は利用する具体的な方法によっては偽サーバへの対策が不十分なものが含まれるため、使用する場合には適切な手法の選択及び必要な対策を行うこと。また、ソフトウェア型の IPsec 又は TLS1.2 以上により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃への適切な対策を実施すること。
⑦利用するネットワークの安全性を勘案して、送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。
⑧医療機関等で用いる通信において、ネットワーク上で「改ざん」されていないことを保証すること。またネットワークの転送途中で診療録等が改ざんされていないことを保証できるようにすること。なお、可逆的な情報の圧縮・解凍、セキュリティ確保のためのタグ付け、暗号化・復号等は改ざんにはあたらない。
⑨ネットワーク経路でのメッセージ挿入、不正ソフトウェアの混入等の改ざん及び中間者攻撃等を防止する対策を実施すること。
⑩施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策を実施すること。
⑪医療情報システムを、内部ネットワークを通じて外部ネットワークに接続する際には、なりすまし、盗聴、改ざん、侵入及び妨害等の脅威に留意したうえで、ネットワーク、機器、サービス等を適切に選定し、監視を行うこと。
⑫医療機関等がネットワークを通じて通信を行う際に、通信の相手先が正当であることを認識するための相互認証を行うこと。また診療録等のオンライン外部保存を受託する事業者と委託する医療機関等が、互いに通信目的とする正当な相手かどうかを認識するための相互認証機能を設けること。
⑬医療情報システムにおいて無線 LAN を利用する場合、次に掲げる対策を実施すること。
－適切な利用者以外に無線 LAN を利用されないようにすること。例えば、ANY 接続拒否等の対策を実施すること。
－不正アクセス対策を実施すること。例えば MAC アドレスによるアクセス制限を実施すること。ただし、MAC アドレスは詐称可能であることや、最近のモバイル端末においてはプライバシー保護の観点から MAC アドレスランダム化が標準搭載されていることから、MAC アドレスによるアクセス制限の効果が限定的であることに留意する必要がある。
－不正な情報の取得を防止するため、WPA2-AES、WPA2-TKIP 等により通信を暗号化すること。
－利用する無線 LAN の電波特性を勘案して、通信を阻害しないものを利用すること。

システム運用におけるセキュリティ対策の中で、オンライン資格確認・オンライン請求ネットワーク等の接続を考慮する場合、ネットワークのセキュリティ要件は非常に重要である。

医療情報システムガイドラインに基づくと、医療情報システムの利用は、「セキュアなネットワーク」を用いることとされている。医療情報システムガイドラインにおけるネットワークの整理について、以下に示す。

図表 8 医療情報システムガイドラインにおけるネットワークの整理



（出所）厚生労働省、医療情報システムガイドライン6．0医療情報システムガイドラインのシステム運用編[Control]図12－2より抜粋引用

通常のインターネット接続は、後述する技術解説書にオンライン資格確認・オンライン請求ネットワーク等の接続方式には、示されていない。

認証・認可に関する安全管理措置における遵守事項は以下のとおり。

14. 認証・認可に関する安全管理措置[Ⅰ～Ⅳ]

①医療機関等で用いる医療情報システムへのアクセスにおいて、利用者の識別・認証を行い、利用者認証方法に関する手順等に関して、規則、マニュアル等で文書化すること。
②利用者の識別・認証にユーザ ID とパスワードの組み合わせを用いる場合、それらの情報を、本人しか知り得ない状態に保つよう対策を実施すること。
③利用者の識別・認証に IC カード等のセキュリティ・デバイスを用いる場合、IC カードの破損等、セキュリティ・デバイスが利用できないときを想定し、緊急時の代替手段による一時的なアクセスルールを用意すること。
④アクセス管理に関する規程に基づいてアクセス権限を付与する場合、権限の実態が反映できるよう、システム運用担当者に対して、利用者が所属する部署等からの申請などを踏まえて権限を付与し、その結果について申請部署の管理者からの確認を得る等の手順を作成するよう指示すること。
⑤利用者認証にパスワードを用いる場合には、令和 9 年度時点で稼働していることが想定される医療情報システムを、今後、新規導入又は更新するに際しては、二要素認証を採用するシステムの導入、又はこれに相当する対応を行うこと。
⑥パスワードを利用者認証に使用する場合、次に掲げる対策を実施すること。
－類推されやすいパスワードを使用させないよう、設定可能なパスワードに制限を設けること。
－医療情報システム内のパスワードファイルは、パスワードを暗号化（不可逆変換によること）した状態で、適切な手法で管理・運用すること。
－利用者のパスワードの失念や、パスワード漏洩のおそれなどにより、医療情報システムのシステム運用担当者がパスワードを変更する場合には、利用者の本人確認を行うとともに、どのような手法で本人確認を行ったのかを台帳に記載（本人確認を行った書類等のコピーを添付）すること。また、変更したパス

ワードは、利用者本人以外が知り得ない方法で通知すること。なお、パスワード漏洩のおそれがある場合には、速やかにパスワードの変更を含む適切な処置を講じること。
－医療情報システムのシステム運用担当者であっても、利用者のパスワードを推定できないようにすること（設定ファイルにパスワードが平文で記載される等があってはならない）。
⑦医療情報システムにおいて用いる ID について、台帳管理等を行うほか、定期的に棚卸を行い、不要なものは適宜削除すること等を含む手順を作成すること。
⑧電子カルテシステムにおける記録の確定手順の確立と、識別情報の記録について、以下の機能があることを確認すること。
－電子カルテシステム等で PC 等の汎用入力端末により記録が作成される場合
a 診療録等の作成・保存を行おうとする場合、確定された情報を登録できる仕組みをシステムに備えること。その際、登録する情報に、入力者及び確定者の氏名等の識別情報、信頼できる時刻源を用いた作成日時を含めること。
b「記録の確定」を行うに当たり、内容を十分に確認できるようにすること。
c「記録の確定」は、確定を実施できる権限を持った確定者に実施させること。
d 確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止するための対策を実施するとともに、原状回復のための手順を検討しておくこと。
e 一定時間経過後に記録が自動確定するような運用の場合は、入力者及び確定者を特定する明確なルールを運用管理規程に定めること。
f 確定者が何らかの理由で確定操作ができない場合における記録の確定の責任の所在を明確にすること。例えば、医療情報システム安全管理責任者が記録の確定を実施する等のルールを運用管理規程に定めること。
－臨床検査システム、医用画像ファイリングシステム等、特定の装置又はシステムにより記録が作成される場合
a 運用管理規程等に当該装置により作成された記録の確定ルールを定義すること。その際、当該装置の管理責任者や操作者の氏名等の識別情報（又は装置の識別情報）、信頼できる時刻源を用いた作成日時を記録に含めること。
b 確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止するための対策を実施するとともに、原状回復のための手順を検討しておくこと。
－一旦確定した診療録等を更新する場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合わせることができるようにすること。
－同じ診療録等に対して複数回更新が行われた場合でも、更新の順序性が識別できるようにすること。
－代行入力が行われた場合には、誰の代行がいつ誰によって行われたかの管理情報を、代行入力の都度記録すること。
－代行入力により記録された診療録等は、できるだけ速やかに確定者による「確定操作（承認）」が行われるようにすること。この際、内容の確認を行わずに確定操作を行ってはならない。

証跡のレビュー・システム監査における遵守事項は以下のとおり。

17. 証跡のレビュー・システム監査［Ⅰ、Ⅲ］

①利用者のアクセスについて、アクセスログを記録するとともに、定期的にログを確認すること。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録すること。医療情報システムにアクセスログの記録機能があることが前提であるが、ない場合は、業務日誌等により操作者、操作内容等を記録すること。
②アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を実施すること。
③アクセスログの記録に用いる時刻情報は、信頼できるものを利用すること。利用する時刻情報は、医療機関等の内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で診療事実の記録として問題のない範囲の精度を保つ必要がある。
④監査等を行うに際し、技術的な対応に関する監査実施計画の作成や証跡の整理等を行い、企画管理者に報告すること。

外部からの攻撃に対する安全管理措置における遵守事項は以下のとおり。

18. 外部からの攻撃に対する安全管理措置［Ⅰ～Ⅳ］

①医療情報システムに対する不正ソフトウェアの混入やサイバー攻撃などによるインシデントに対して、以下の対応を行うこと。
－攻撃を受けたサーバ等の遮断や他の医療機関等への影響の波及の防止のための外部ネットワークの一時切断
－他の情報機器への混入拡大の防止や情報漏洩の抑止のための当該混入機器の隔離
－他の情報機器への波及の調査等被害の確認のための業務システムの停止
－バックアップからの重要なファイルの復元（重要なファイルは数世代バックアップを複数の方式（追記可能な設定がなされた記録媒体と追記不能設定がなされた記録媒体の組み合わせ、端末及びサーバ装置やネットワークから切り離したバックアップデータの保管等）で確保することが重要である）

主なセキュリティの論点について、後述するヒアリング調査内容で重点的に確認を行った内容について、以下のとおり要約した。

図表 9 主なセキュリティ対策概要

章項目	主なセキュリティ対策概要
7. 情報管理(管理・持出し・破棄等)	
7. 1外部へ持ち出す医療情報の管理対策外部へ持ち出す医療情報の管理対策	・医療機関外部の情報の持ち出しに関する規程の作成、管理、運用 ・紛失時に備えて端末のセキュリティ設定(パスワード等)や記録媒体の暗号化
7. 2医療機関等外から医療情報システムに接続する利用の場合への対策医療機関等外から医療情報システムに接続する利用の場合への対策	・医療機関等の外部から医療情報システムに接続して利用する場合、技術的対応への方策を講じること 例)訪問先やテレワークで外部からのアクセス
7. 3医療情報の破棄	・情報機器を破棄する際には専用ソフトウェア等で確実な破棄を行うこと
8. 利用機器・サービスに対する安全管理措置	
8. 1不正ソフトウェア対策	・スキャン用ソフトウェア(ウイルス対策ソフト)の導入 ・最新のセキュリティパッチの適用 ・不要なサービスの停止 ・ネットワークの構成分割
8. 2情報機器等の脆弱性への対策	・脆弱性や販売/サポート/サービス終了に関する情報収集及びその対策を実施
8. 3端末やサーバの安全な利用の管理	・情報機器のパスワード管理 ・使用していない時間帯では非稼働
8. 4情報機器等の棚卸	・利用対象端末の選別/把握
8. 5医療機関等が管理する以外の情報機器の利用に対する対策	・管理者による BYOD によるコスト・利便性とリスクを評価/検討すること。 ・BYOD について運用管理規程※を定めて管理するだけではなく、職員のモバイル端末で、他のアプリケーション等からの影響を遮断しつつ、仮想デスクトップのような技術を活用して端末内で医療情報を取り扱うことを制限する等技術的対策を施すこと。 ※Q&A シス 8 章第⑧条、第⑨条、企 9 章第⑥条シ Q-20 の回答に【BYOD に係る運用管理規程への記載事項(例)】が示されている。 ・管理していない端末での BYOD では業務は行わないこと。
11. システム運用管理(通常時・非常時等)	
11. 1通常時における運用対策	・ネットワーク、バックアップ、非常時の臨時措置用の機器の準備すること。 ・関係先への連絡手段や紙での運用等の代替手段を準備すること。

章項目	主なセキュリティ対策概要
	・サイバー攻撃による被害拡大の防止の観点から、論理的／物理的に構成分割されたネットワークを整備すること。 ・予めバックアップ計画を立て、バックアップからの復元手順を整備すること。
11. 2非常時における対応	・非常時発生時にあらかじめ対応措置を定義しておくこと。 ・「非常時のユーザカウントや非常時用機能」の手順を整備すること。
12. 物理的安全管理措置	
12. 1サーバルーム等の物理的要件	・入退管理をなされていること、カメラ等による監視も考慮すること ・自然災害(水害、停電等)に備えた措置を講じること
12. 3. 2端末・サーバ装置等の不適切な利用等に関する対策	・長時間の離席時にはクリアスクリーン等の対策を講じること
13. ネットワークに関する安全管理措置	
13. 1ネットワークに対する安全管理	・不正な機器との接続や不正なデータ等の混入しないようセキュアなネットワークを構築すること
13. 1. 2選択すべきネットワークのセキュリティ	・専用線:最も安全で、2 拠点間を物理的に接続し、利用者が独占的に使用する回線であることから、外部からの侵入や盗聴のリスクが小さいが高コストである。 ・IP-VPN(閉域網):インターネットを用いず、通信事業者が提供するものである。通信事業者以外の侵入のリスクは小さく、外部からの侵入のリスクは低いが、利用コストが高い。 ・IPsec+IKE:ネットワーク層レベルでの暗号化を図る方法で、インターネット VPN の中でも安全性が高い。 ・SSL-VPN:SSL 技術を利用した VPN でセッション層において暗号化を図る。端末側でのアプリケーションが不要など、導入が容易である反面、偽サーバへの対策リスク等があることに留意が必要。 ※オープンなネットワーク環境下において、IPsec による VPN を利用せずに、HTTPS を利用する場合、TLS1.3 以上でクライアント証明書を利用することとされている。 TLS1.2 はやむを得ない場合に、条件付きであれば可能であるが推奨されない。
13. 2不正な通信の検知や遮断、監視	・ファイアウォールや不正攻撃の検知/遮断するシステムの導入 ・パッチ適用等の対策
13. 3通信の暗号化・盗聴等の防止	・オープンなネットワークを利用する際には回線の暗号化等を講じること。 ・オープンなネットワークで外部との送受信がある場合には、情報そのものにも暗号化対策を講じること。 ・盗聴防止に管理者はネットワークや機器、サービス等の監視を行う

章項目	主なセキュリティ対策概要
	こと。 ・無線 LAN 利用時は、不正利用や盗聴、可用性に配慮した対策を講じること。
14. 認証・認可に関する安全管理措置	
14. 1利用者認証	・医療情報システムは利用者の識別・認証を行う機能を持たせること。 ・小規模な医療機関で利用者が限定されていても、上記の識別・認証機能は一般的に必須。 ・医療情報システムにアクセスする全ての利用者に識別・認証に用いる手段(ID/PW 等)を用意・管理する必要がある。 ・認証情報は本人しか知り得ない・又は持ち得ない状態に保つ必要がある。 ・パスワードは第三者に推定されにくいもので、システム運用担当者でも分からない措置を講じること。 ・令和 9 時点で稼働していることが想定されている医療情報システムについては、今後導入又は更新する場合、二要素認証の導入またはこれに相当する対応を行うこと。
14. 2アクセス権限の管理	・情報の区分ごと、組織における利用者や利用者グループごとに利用権限を規定する必要がある。
18. 外部からの攻撃に対する安全管理措置	
①不正ソフトウェアの混入やサイバー攻撃などによるインシデントへの対応 －攻撃を受けたサーバ等の遮断、外部ネットワークの一時切断 －不正ソフトウェアの混入した機器の隔離 －業務システムの停止 －バックアップからの重要なファイルの復元	
18. 1サイバーセキュリティ対応	・サイバー攻撃への対策については、PC や VPN 機器等の脆弱性対策。 「8. 2 情報機器等の脆弱性への対策」を参照。 NISC「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」、2021 年 4 月 30 日の「ランサムウェアによるサイバー攻撃に関する注意喚起について[19]」を参照。 ・非常時に備えたバックアップの実施と管理については、「11. システム運用管理(通常時・非常時等)」、「12. 2 バックアップの管理」を参照。

[19] NISC、ランサムウェアによるサイバー攻撃に関する注意喚起について：
https://www.nisc.go.jp/pdf/policy/infra/ransomware20210430.pdf

（出所）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 版システム運用編[Control]の遵守事項に基づいて、抜粋・要約し株式会社三菱総合研究所にて作成

4. オンライン資格確認・オンライン請求の仕組み等の整理

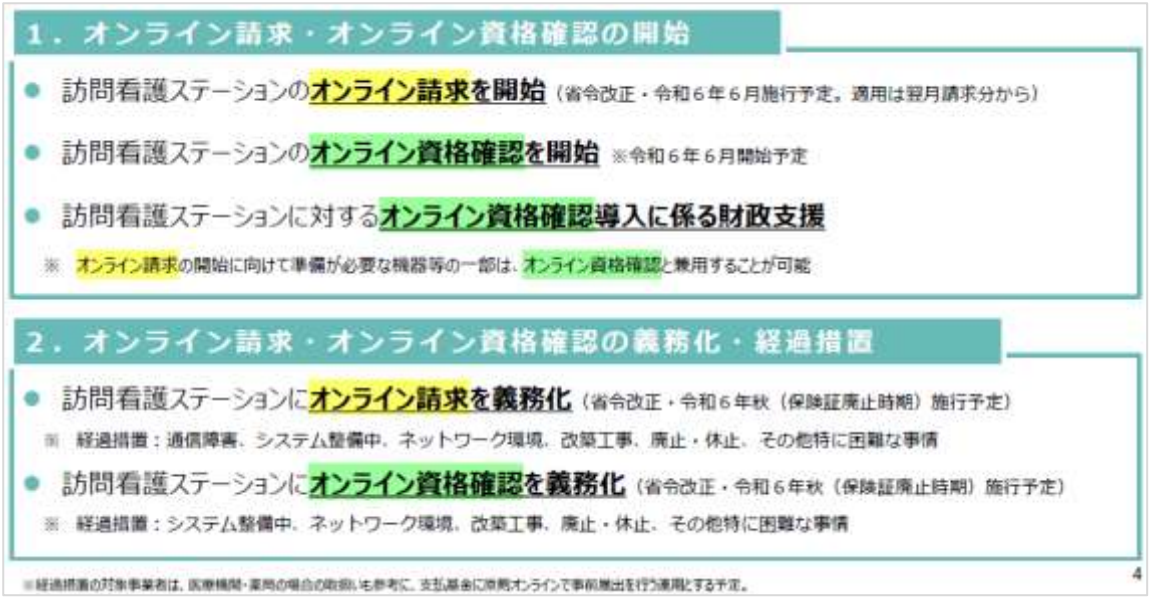
4－1. オンライン資格確認・オンライン請求義務化の状況について

医療機関・薬局については、令和5年度4月より、保険医療機関・薬局に、医療 DX の基盤となるオンライン資格確認等システムの導入が原則義務化された。オンライン請求システムの導入については、「療養の給付及び公費負担医療に関する費用の請求に関する命令及び介護給付費及び公費負担医療等に関する費用等の請求に関する命令の一部を改正する命令等の公布について[20]」が示され、令和6年 9 月末までに全てのオンライン資格確認導入済みの医療機関がオンライン請求に移行する予定である。

一方、訪問看護ステーションにおいて、令和 6 年6月よりレセプトのオンライン請求とオンライン資格確認が開始される。[21]オンライン資格確認、オンライン請求の導入について、訪問看護ステーションへの適用時期が保健医療機関・薬局と比較して、義務化のスケジュールは後ろ倒しになっている。

[20] 厚生労働省、保険医療機関・薬局におけるオンライン請求等サイト：
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000190624_00001.html
[21] 厚生労働省、【訪問看護ステーションの方々へ 】訪問看護(医療保険)における オンライン資格確認、オンライン請求が 令和6年6月から開始します！：https://www.mhlw.go.jp/content/10200000/001151918.pdf

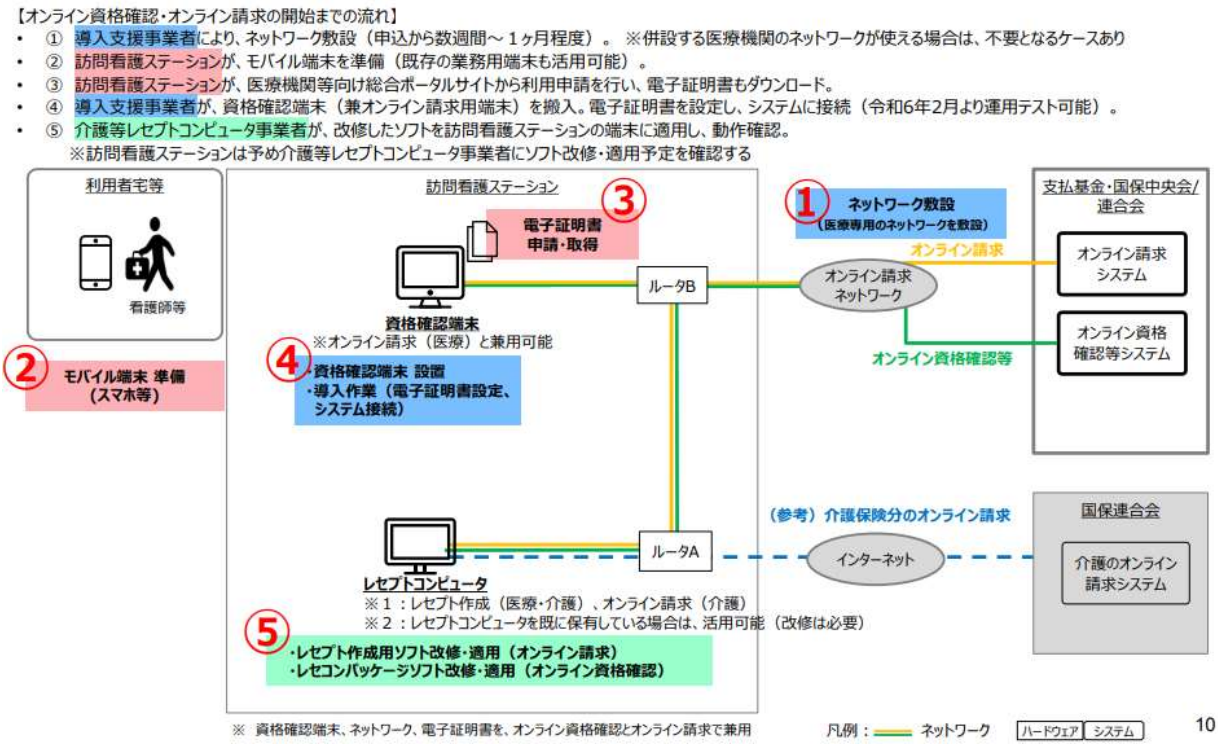
図表 10 訪問看護レセプトのオンライン請求・オンライン資格確認



（出所）厚生労働省、【訪問看護ステーションの方々へ】訪問看護（医療保険）におけるオンライン資格確認、オンライン請求が令和6年6月から開始します！」より抜粋引用

また、訪問看護ステーションにおけるオンライン資格確認・オンライン請求導入の作業イメージについては、以下のとおり。医療機関・薬局と同様のセキュリティ対策が求められる。なお、令和 6 年 3 月時点でレセプト（介護保険）のオンライン請求は、義務化されていない。

図表 11 訪問看護ステーションにおけるオンライン資格確認・オンライン請求導入の作業イメージ



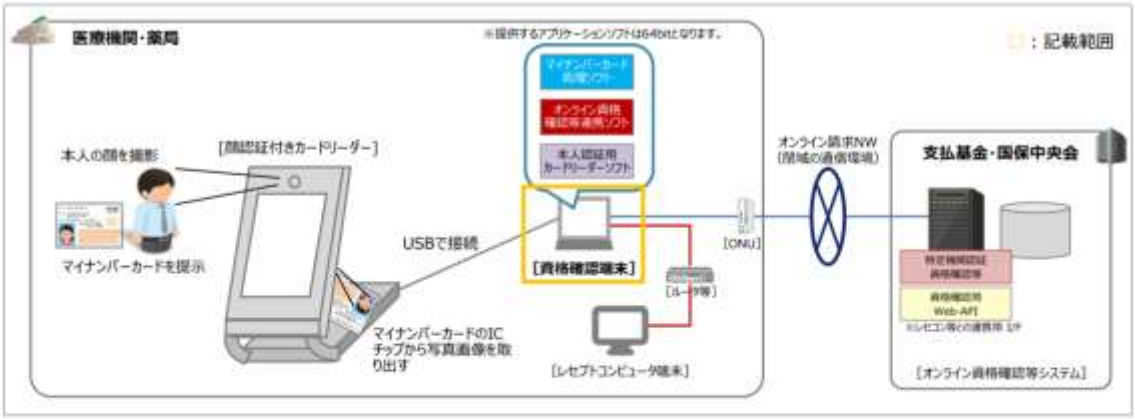
（出所）厚生労働省、【訪問看護ステーションの方々へ】訪問看護（医療保険）におけるオンライン資格確認、オンライン請求が令和6年6月から開始します！」より抜粋引用

訪問看護ステーションにおけるオンライン資格確認、レセプト（医療保険）のオンライン請求の令和６年６月開始にむけて、関係各所に対する説明会の実施、また、社会保険診療報酬支払基金のサイトには、令和６年２月に「訪問看護レセプトのオンライン請求開始に係る特設ページ[22]」が開設され、周知活動が行われている。

４－２. 調達する端末、機器、主なシステム要件について

オンライン資格確認等システムに接続する端末については、令和5年１月 13 日版「資格確認端末において満たすべき要件[23]」では、オンライン資格確認等システムで使用する資格確認端末として推奨する仕様を示しているため、導入時には参考にすることができる。オンライン資格確認等端末は、オンライン請求と併用することは可能である。同書における対象範囲は以下のとおり。

図表 12 資格確認端末において満たすべき要件



資格確認端末	• オンライン資格確認システムの業務利用（Webアプリケーション利用の場合） • 顔認証付きカードリーダーを制御する本人認証用カードリーダーソフトの実行 • マイナンバーカードの読込を行うマイナンバーカード処理ソフトの実行 • レセプトコンピュータ端末とオンライン資格確認等システム間で情報連携を行うための連携ソフトの実行・連携ファイル置き場 • オンライン請求システム（支払基金/国保連合会への診療報酬請求）の業務利用（資格確認端末とオンライン請求端末を共用する場合）

（出所）厚生労働省、「資格確認端末において満たすべき要件」：

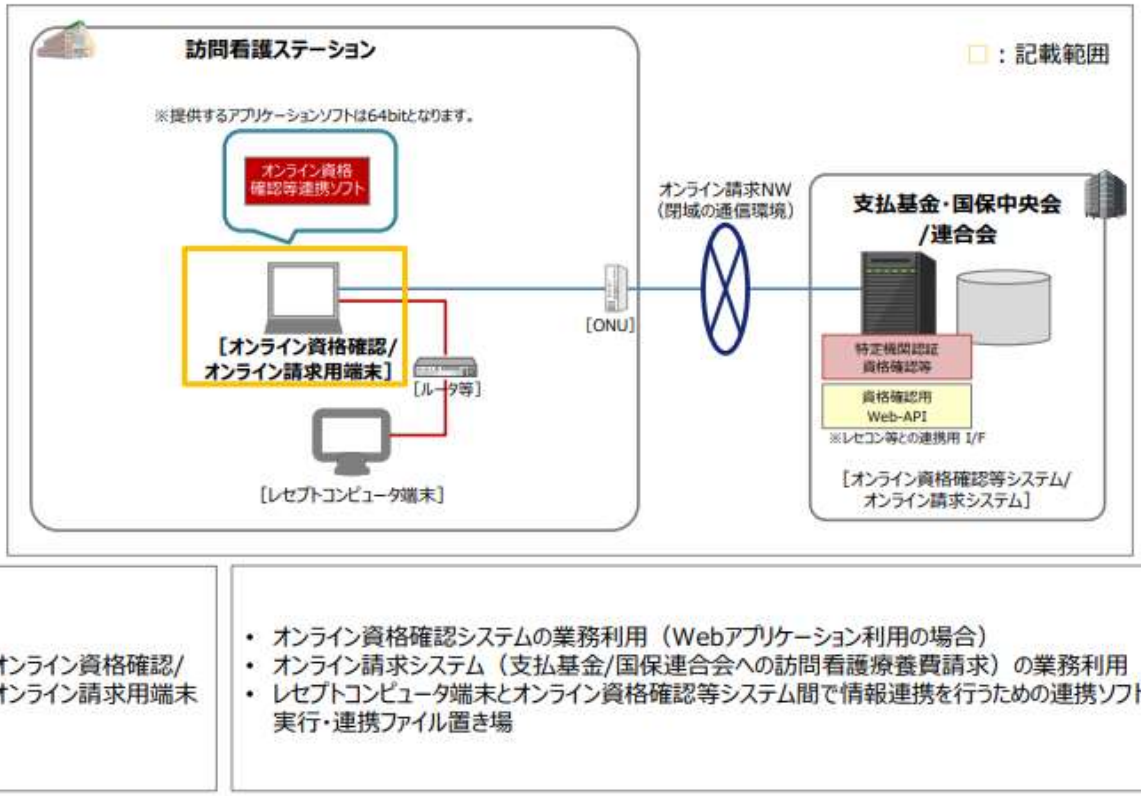
https://www.mhlw.go.jp/content/10200000/000623527.pdf より対象範囲の図を抜粋引用

[22] 社会保険診療報酬支払基金、「訪問看護レセプトのオンライン請求特設ページ」：
https://www.ssk.or.jp/oshirase/special_houkanr0601.html

[23] 令和５年１月 13 日版「資格確認端末において満たすべき要件」：
https://www.mhlw.go.jp/content/10200000/000623527.pdf

また、令和６年２月に訪問看護レセプトのオンライン請求特設ページが開設され「オンライン資格確認/オンライン請求用端末において満たすべき要件（訪問看護ステーション向け）」オンライン資格確認/オンライン請求用等システムを同一端末で使用する場合に推奨する仕様が示されているので、訪問看護ステーションで端末を導入する際に参考とすることができる。

図表 13 資格確認端末において満たすべき要件（訪問看護ステーション）」の対象範囲



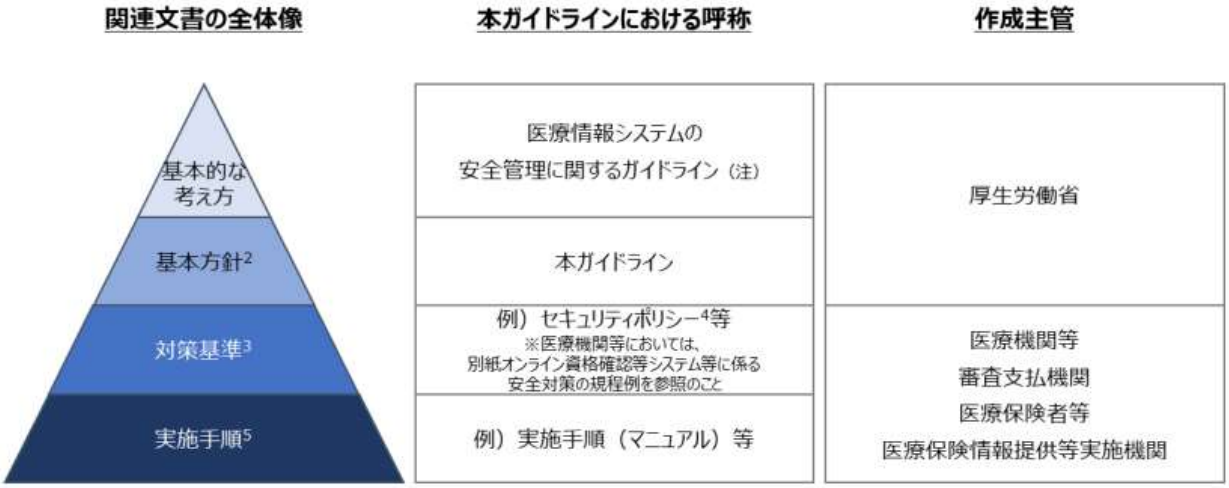
（出所）オンライン資格確認/オンライン請求用端末において満たすべき要件（訪問看護ステーション向け）より抜粋引用

https://www.mhlw.go.jp/content/10200000/001154935.pdf

令和５年11月公表された「訪問診療等におけるオンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書【医療機関・薬局・訪問看護ステーション】[24]（以下、「オンライン資格確認技術解説書」という。」及び令和２年10月に公表され、令和６年１月に改正された「オンライン資格確認等、レセプトのオンライン請求及び健康保険組合に対する社会保険手続きに係る電子申請システムに係るセキュリティに関するガイドライン（以下、「オンライン請求ガイドライン」という。）」に基づいて、オンライン資格・オンライン請求等に接続するためのシステム要件について主な項目を概説する。オンライン請求ガイドラインは、Ⅰ 総則、1目的に示されるとおり、オンライン資格確認等、診療情報閲覧、薬剤情報閲覧、特定健診情報閲覧、医療費通知情報閲覧及びレセプト振替に係る各業務（以下、「オンライン資格確認等業務」と総称する。）、レセプトのオンラインによる提出及び受取（以下「オンライン請求業務」という。）及び健康保険適用処理業務の実施に際し、個人情報等を適切に保護するとともに、円滑な業務遂行に資することを目的として、これらの業務及びこれらのシステムを利用する機関が遵守すべき事項を示すものである。ガイドラインの位置づけは、同ガイドラインより抜粋した図を以下に示す。

[24] 厚生労働省、「訪問診療等におけるオンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書【医療機関・薬局・訪問看護ステーション】」：https://www.mhlw.go.jp/content/10200000/001024239.pdf

図表 14 レセプトオンライン請求ガイドラインの位置づけ



（注）「医療情報システムの安全管理に関するガイドライン」は、主に医療機関等を対象としているが、本ガイドラインでは、支払基金・国保連合会により組織される審査支払機関及び実施機関においてもその考え方を参照する。

2 基本方針：組織におけるセキュリティ対策に対する根本的な考え方を表わすもので、組織がどのような情報資産をどのような脅威からなぜ保護しなければならないのかを明らかにし、組織の情報セキュリティに対する取組姿勢を示すものをいう。

3 対策基準：基本方針に定められた情報セキュリティを確保するために遵守すべき行為及び判断等の基準、即ち、基本方針を実現するために何を行なわなければいけないかを示すものをいう。

4 セキュリティポリシー：組織が所有する情報及び情報システム等の情報資産のセキュリティ対策について、総合的・体系的かつ具体的に取りまとめたものをいう。情報資産への脅威に対する対策について、基本的な考え方及び情報セキュリティを確保するための体制、組織及び運用を含めた規程をいう。基本方針及び対策基準からなる。

5 実施手順：セキュリティポリシーには含まれないものの、対策基準に定められた内容を具体的な情報システム又は業務において、どのような手順に従って実行していくのかを示すものをいう。

（出所）厚生労働省、「オンライン資格確認等、レセプトのオンライン請求及び健康保険組合に対する社会保険手続きに係る電子申請システムに係るセキュリティに関するガイドライン」図2より抜粋引用

オンライン資格確認等システム及びオンライン請求システムは、いずれも医療情報を扱う情報システムであり、両システムの導入に際しても、「医療情報システムの安全管理に関するガイドライン」に沿って導入、運用、利用、保守及び廃棄が行われるべきものとされている。レセプト請求ガイドラインでは、「医療情報システムガイドライン」は、厚生労働省サイトにて公開されており、情勢に応じて随時改定を行っているため、適宜最新版を参照することとれている。「医療情報システムガイドライン」のセキュリティ対策を参照して実施することとされているが、「訪問診療等におけるオンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書【医療機関・薬局・訪問看護ステーション】」に基づいて、詳細を後述する。

社会保険診療報酬支払基金(以下、「支払基金」という。)のセキュリティサイト[25]に以下のとおり示されている。オンライン請求に関するセキュリティについて厚生労働省からの通知により定められており、支払基金は、以前より、情報資産に係る安全対策の情報セキュリティ基本方針及び基本方針に基づく個別の対策の情報セキュリティ対策基準からなる情報セキュリティポリシー[26]を定めている。ガイドラインのセキュリティ条件を確保した体制[27]を構築している。主なセキュリティ対策は、以下のとおり。

(1)認証

- 電子証明書による認証
- ユーザ ID・パスワードによる認証

(2)システム

- 送信及び受信ログの保管
- 不正アクセスの監視

(3)ネットワーク

- ISDN 回線を利用したダイヤルアップ接続または、閉域 IP 網を利用した IP-VPN 接続、または、オープンなネットワークにおいては IPsec と IKE を組み合わせた接続
- SSL 暗号化通信

現在、レセプトのオンライン請求で実績のあるオンライン資格確認等システムの接続に用いる回線の仕様は、医療保険者等、医療機関・薬局が利用するネットワーク提供事業者において、支払基金が予め発行したオンライン請求用電子証明書による認証を確保することにより、インターネットから分離された安全な接続環境を構築している。既にオンライン資格確認ネットワークを利用している医療機関・薬局における現状の接続方式及び導入後の接続方式は、以下のとおり。ISDN のダイヤルアップ接続方式は令和 6 年 1 月、IP-VPN 接続方式(ADSL 回線)は令和 5 年 1 月にサービス停止となるため、IP-VPN 接続方式(光回線に限る)若しくは IPsec+IKE 接続方式へ移行する必要がある。(訪問看護ステーションにおいては「導入後」のみを参照することになる。)なお、光回線の未提供エリアにおいては ADSL を継続利用可能である。

接続方式について、医療情報システムガイドラインでは、必要となるインターネット接続方式も許容されているが、オンライン資格確認等システムでは、IP-VPN 接続方式及び IPsec+IKE 方式に限られる。訪問看護ステーションの医療保険請求分については、医療機関・薬局と同様に IP-VPN 接続方式及び IPsec+IKE 方式に限定されている。

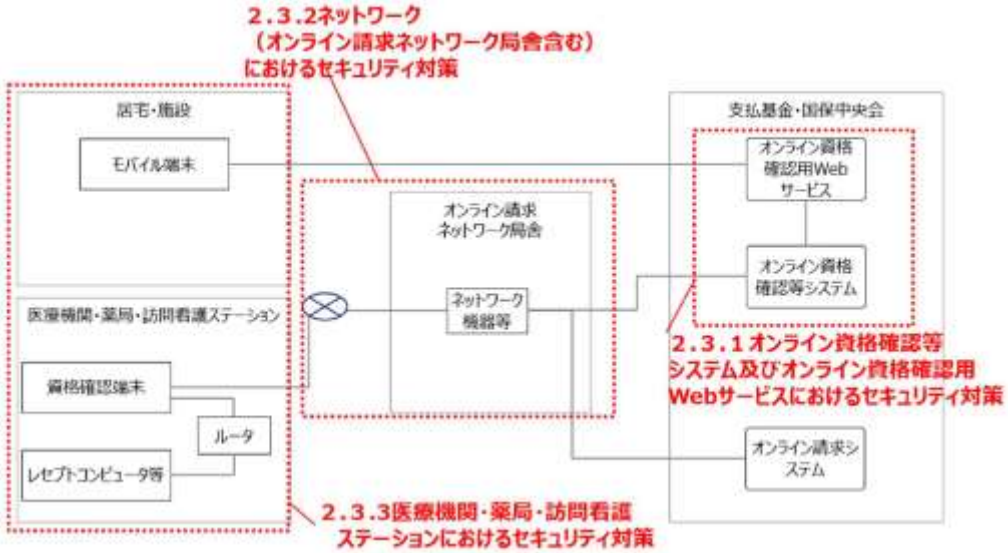
図表 15 オンライン資格確認ネットワークの現状及び導入後の接続方式

[25] 社会保険診療報酬支払基金「セキュリティサイト」:https://www.ssk.or.jp/seikyushiharai/online/online_02.html
[26] 社会保険診療報酬支払基金情報セキュリティポリシー:https://www.ssk.or.jp/smph/goannai/chotatsu/security.html
[27] 社会保険診療報酬支払基金「情報保護管理体制」:https://www.ssk.or.jp/johohogo.html

（出所）訪問診療等におけるオンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書【医療機関・薬局・訪問看護ステーション】の図 2. 2.1-1 より抜粋引用

医療機関・薬局におけるネットワークにおける主なセキュリティ対策を以下に示す。

図表 16 オンライン資格確認等システムと医療機関・薬局・訪問看護ステーションの接続に係るセキュリティ対策



（出所）訪問診療等におけるオンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書【医療機関・薬局・訪問看護ステーション】の図 2. 3.1-1 より抜粋引用

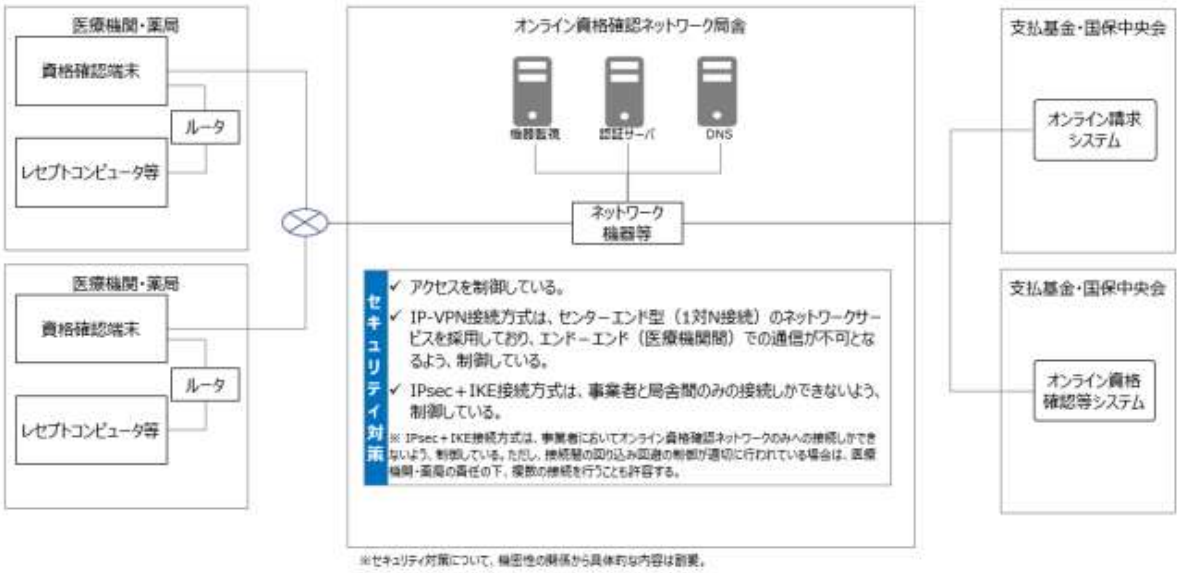
上記の図に示されたセキュリティ対策については、以下のとおりである。

【2. 3. 1】:オンライン資格確認等システム及びマイナ在宅受付 Web（サーバー側）において、「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」に準拠した対策を実施する。

【2.3. 2】:オンライン資格確認ネットワークにおけるセキュリティ対策においては、予め許可された医療機関・薬局・訪問看護ステーションのみが接続可能であり、他医療機関・薬局・訪問看護ステーションに応答を返さない仕組みである。また、医療機関・薬局・訪問看護ステーション間（例えば A 機関⇔B 機関）での通信が不可となるようアクセス制御等を実施する。各医療機関・薬局・訪問看護ステーションから指定された接続先のみ通信に制限されており、オンライン資格確認等システム及び資格確認端末を運用・保守するために必要な Windows セキュリティパッチの適用、アプリケーションソフト等配信サイトを指定する。万が一、ある医療機関・薬局・訪問看護ステーションでマルウェア等に感染した場合に、他の医療機関・薬局・訪問看護ステーションへ攻撃がされることを抑制するためである。

ネットワークにおける主なセキュリティ対策は以下のとおり。

図表 17　ネットワークにおける主なセキュリティ対策



（出所）訪問診療等におけるオンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書【医療機関・薬局・訪問看護ステーション】図2. 3. 2-1より抜粋引用

訪問診療等におけるオンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書【医療機関・薬局・訪問看護ステーション】図より2. 3. 2-1より、抜粋して要約して示す。

図表 18　オンライン資格確認ネットワーク局舎でのセキュリティ対策

オンライン資格確認ネットワーク局舎でのセキュリティ対策
アクセス制御
IP-VPN 方式は、センターエンド型（1対 N 接続）のネットワークサービスを採用 エンドーエンド（医療機関間）での通信は不可 IPsec＋IKE 方式は、事業者と局舎感のみの接続に制限し、制御 ※IPsec+IKE 接続方式については、事業者においてオンライン資格確認ネットワークのみへの接続のみに限定し、制御。ただし、接続間の回り込み回避の制御が適切に行われている場合、医療機関・薬局の責任の下、複数の接続を行うことを許容する。

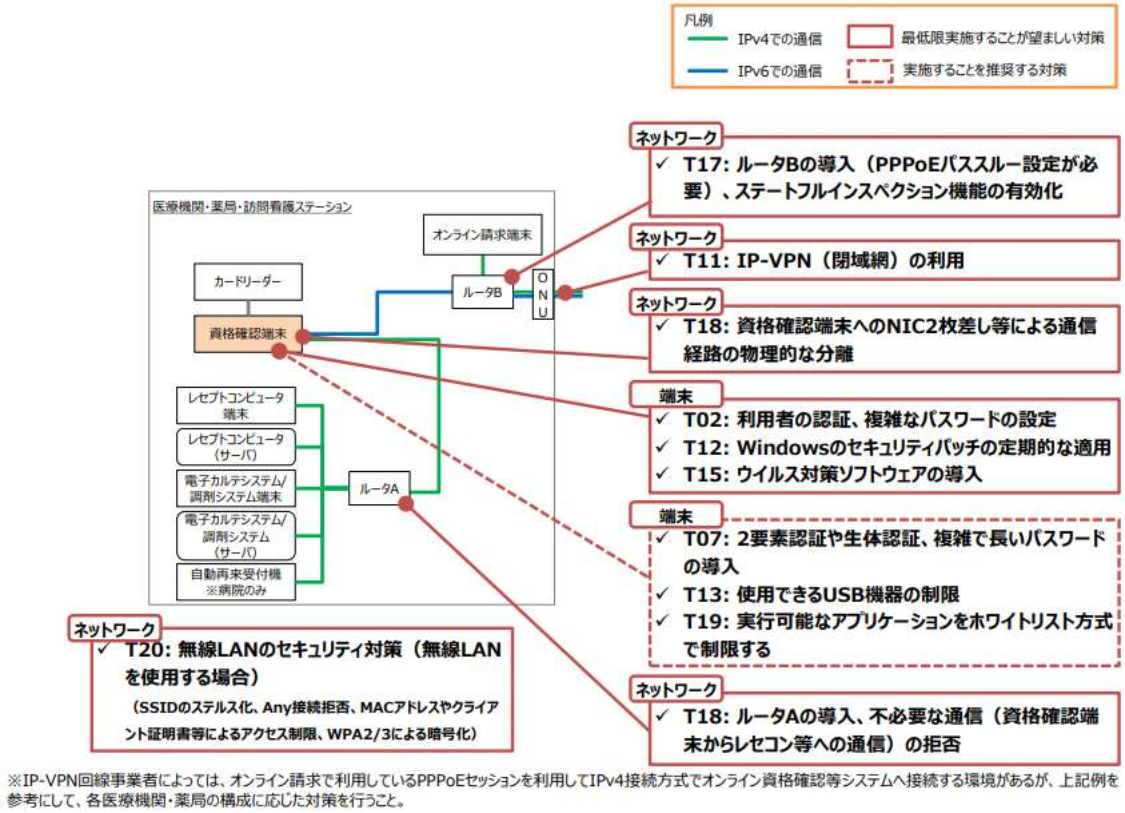
（出所）訪問診療等におけるオンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書【医療機関・薬局・訪問看護ステーション】図2. 3. 2-1より抜粋し、株式会社三菱総合研究所にて要約して作成

【2.3.3】:医療機関・薬局・訪問看護ステーションにおいて、「医療情報システムガイドライン第 6.0 版」に準拠し、必要なセキュリティ対策を行う必要がある。

そのため、2.3.3を中心に、各医療機関・薬局・訪問看護ステーションにおいて求められるセキュリティ対策について、接続方式に分けてセキュリティ対策例が示されているので、検討する参考として抜粋し、概説する。

医療機関・薬局・訪問看護ステーションにおける主なセキュリティ対策例(IP-VPN 接続方式の場合)は、以下のとおり。

図表 19 医療機関・薬局・訪問看護ステーションにおける主なセキュリティ対策例
(IP-VPN 接続方式の場合)

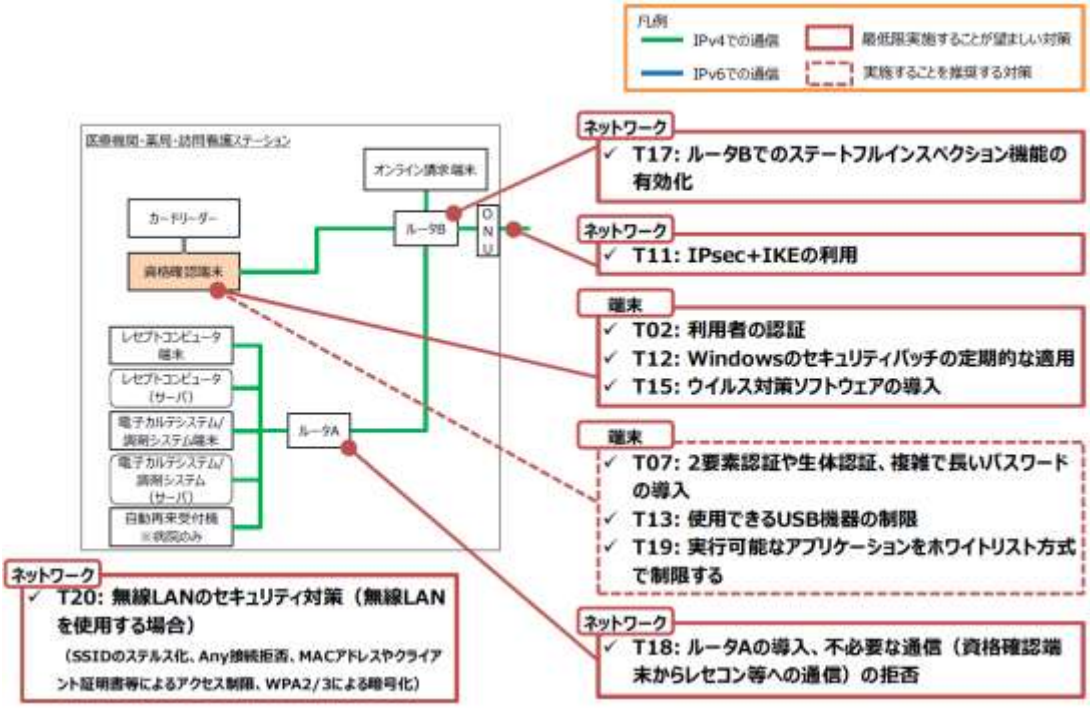


※IP-VPN回線事業者によっては、オンライン請求で利用しているPPPoEセッションを利用してIPv4接続方式でオンライン資格確認等システムへ接続する環境があるが、上記例を参考にして、各医療機関・薬局の構成に応じた対策を行うこと。

(出所)図2.3.3-1医療機関・薬局・訪問看護ステーションにおける主なセキュリティ対策例(IP-VPN 接続方式の場合)より抜粋

医療機関・薬局・訪問看護ステーションにおけるセキュリティ対策例としては、IPsec＋IKE 接続方式（ルーター型）の場合は以下のとおり。

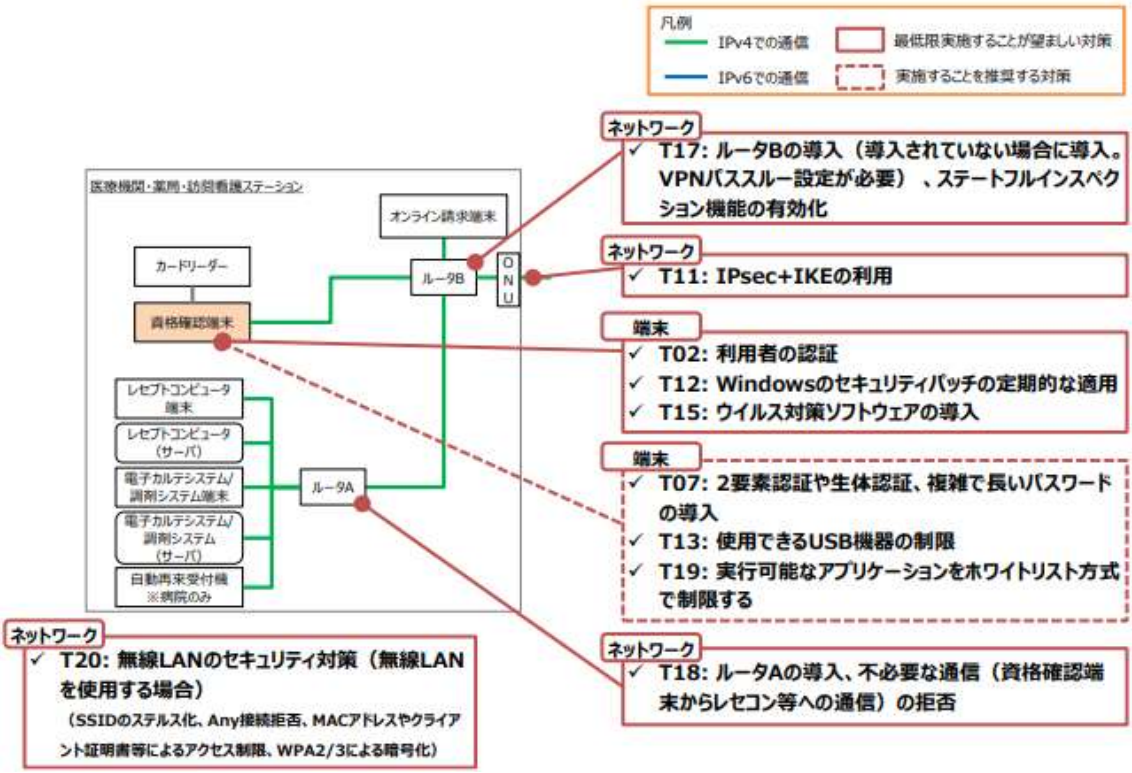
図表 20 医療機関・薬局・訪問看護ステーションにおける主なセキュリティ対策例（IPsec+IKE 接続方式（ルータ型）の場合）



（出所）訪問診療等におけるオンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書【医療機関・薬局・訪問看護ステーション】の図2．3．3－2より抜粋）

医療機関・薬局・訪問看護ステーションにおける主なセキュリティ対策例（IPsec+IKE 接続方式（クライアント型/PC キー型/USB キー型）の場合）は以下のとおり。

図表 21 医療機関・薬局・訪問看護ステーションにおける主なセキュリティ対策例（IPsec+IKE 接続方式（クライアント型/PC キー型/USB キー型）の場合）



（出所）訪問診療等におけるオンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書【医療機関・薬局・訪問看護ステーション】の図2．3．3-3より抜粋

オンライン資格確認技術解説書より、医療機関・薬局・訪問看護ステーションにおけるセキュリティ対策例について、以下の表にまとめた。

図表 22 医療機関・薬局・訪問看護ステーションにおけるセキュリティ対策例のまとめ

対象	セキュリティ採択例
院内ネットワーク環境	・T17：ステートフルインスペクション機能の有効化による外部からのアクセス制限 ・T18：不必要な通信の拒否（オンライン資格確認端末からレセコン等への通信拒否）
院内無線 LAN 環境 ※無線 LAN 接続時	・T20：セキュリティ対策 SSID のステルス化、Any 接続拒否、MAC アドレスやクライアント証明書等によるアクセス制御、WPA2/3による暗号化
回線	・T11：IP-VPN（閉域網）あるいは IPsec+IKE による VPN 接続（T11） ・T18：院内におけるルータの導入、不必要な通信の拒否（オンライン資格確認端末からレセコン等への通信拒否）
端末	・T02：利用者の認証 ・T12：Windows セキュリティパッチの定期適用 ・T15:・ウイルス対策ソフトの導入 ※以下は、実施を推奨する対策 ・強固な認証方式の導入（2 要素認証、生体認証、複雑で長いパスワード等） ・T13：使用できる USB の制限 ・T19:実行可能アプリケーションのホワイトリスト方式による制限

（出所）訪問診療等におけるオンライン資格確認等システムの導入に関するシステムベンダ向け技術解説書【医療機関・薬局・訪問看護ステーション】2. 3. 3. 医療機関・薬局・訪問看護ステーションにおけるセキュリティ対策に基づいて、株式会社三菱総合研究所にて要約して作成

訪問看護ステーションにおけるオンライン資格確認、レセプト（医療保険）のオンライン請求が令和6年6月から開始され、令和6年秋（保険証廃止時期）には義務化が予定されている。

5. 医療機関向けサイバーセキュリティ対策研修について

厚生労働省医政局の特定医薬品開発支援・医療情報担当参事官室は、医療機関向けサイバーセキュリティ対策研修を開始した。厚生労働省委託事業「医療情報セキュリティ研修及びサイバーセキュリティインシデント発生時初期対応支援・調査事業」により、医療機関向けに令和 4 年 12 月頃より「医療情報セキュリティ研修」を実施している[28]。「医療機関向けセキュリティ教育支援ポータルサイト」（MIST：Medical Information Security Training）は以下のとおり。

医療機関向けセキュリティ教育研修ポータル（MIST）：https://mhlw-training.saj.or.jp/

医療機関において、より一層のサイバーセキュリティ対策の強化を図ることを目的に、以下3点を中心

[28] 令和 4 年度 厚生労働省委託事業「医療情報セキュリティ研修及びサイバーセキュリティインシデント発生時初動対応支援・調査事業」医療情報セキュリティ研修サイト：https://www.saj.or.jp/mhlw_training/

に事業を行っている。

- 医療機関の経営層や医療従事者など階層別のサイバーセキュリティ対策研修の実施
- 医療機関内でのサイバーセキュリティ教育に活用できるコンテンツ集の掲載
- サイバーセキュリティインシデント発生時の相談・初動対応依頼窓口の設置

教育研修ポータルについては医療機関向けとされているが、介護事業者にも参考になる内容と思料する。

6. 医療セプター及びサイバーセキュリティ支援制度について

内閣サイバーセキュリティセンター（以下、「NISC」という。）[29]は、国民生活と社会経済活動が大きく依存する重要インフラのサイバーセキュリティの確保のための施策を行っている。NISC における重要インフラのサイバーセキュリティに係る行動計画（以下「行動計画」という。）[30]では、重要インフラ分野として特定している 15 分野のうち1つとして「医療分野」が特定されている。指定の重要インフラ分野にセプターを設置しており、日本医師会は、医療セプター[31]の事務局を担っている。

近年サイバー攻撃による医療機関等への被害は増加している。医療機関を標的としたランサムウェア攻撃、Emotet 等の標的型メール攻撃が多発しており、医療提供体制に影響をもたらしている。日本医師会では、こうした深刻な事態に対処し、サイバーセキュリティ対策を支援するため、「サイバーセキュリティ支援制度[32]」を創設した。本支援制度は、日本医師会 A①会員が開設・管理する医療機関または介護サービス施設・事業所が対象である。

本支援制度の相談窓口による具体的な提供サービスは以下の2つに大別される。

- **1 次対応**
  ネット接続の不具合やウイルス感染等の日常診療業務におけるトラブルに対して、初期のアドバイスやウイルス駆除、セキュリティ診断のリモートサポート等を行う。
- **2 次対応**
  不正アクセスや情報漏えい等の高度な専門性を要する重大なトラブルに対して、より専門的な観点でのアドバイスを実施する。また、会員からの要望に応じて専門事業者（フォレンジック事業者、弁護士）を紹介する。

7. サイバーセキュリティお助け隊サービス制度について

経済産業省の所管である独立行政法人情報処理推進機構（以下、「IPA」という。）では、中小企業向けサイバーセキュリティ対策支援の仕組みの構築を目的とした実証事業「サイバーセキュリティお助け隊事業」を実施した。実証事業で得られた知見、及びサプライチェーン・サイバーセキュリティ・コンソーシアム（以下、「SC3」という。）中小企業対策強化 WG における議論等に基づいて、サイバーセキュリティお助け隊サービス制度[33]が創設された。第 19 回健康・医療・介護情報利活用検討会医療等情報利活

[29] 内閣サイバーセキュリティセンター（NISC）:https://www.nisc.go.jp/
[30] NISC、重要インフラのサイバーセキュリティに係る行動計画 2022 年 6 月 17 日サイバーセキュリティ戦略本部 202 4 年 3 月 8 日サイバーセキュリティ戦略本部改定: https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2024.pdf
[31] 日本医師会、平成 30 年 9 月 19 日 定例記者会見：https://www.med.or.jp/dl-med/teireikaiken/20180919_2.pdf
[32] 日本医師会、日本医師会サイバーセキュリティ支援制度：https://www.med.or.jp/doctor/sys/cybersecurity/001566.html
[33] IPA、「サイバーセキュリティお助け隊サービス制度：https://www.ipa.go.jp/security/sme/otasuketai-about.html

用WGでは、資料 2-2[34]において、医療機関への意識調査の結果、自施設だけでなく、サプライチェーンリスクを念頭に置いたサイバーセキュリティ対策として、ネットワークの俯瞰的把握やインシデント発生に備えたバックアップ作成支援等について、下記の5点が挙げられている。

- NDR 等ネットワーク監視機器を効果的に配置するための、外部接続等を含むネットワーク構成の俯瞰的把握の支援
- ネットワークへの機器追加時の適切な接続に関する支援
- ネットワークへの機器追加後のフォローアップ支援
- バックアップ作成時の初期設定等の支援
- インシデント発生時の対応に関するコンサルテーション(初動対応支援)

こうした支援のなかでサイバーセキュリティお助け隊のサービスとの連携候補として、以下の 3 つのサービスが挙げられている。

1. バックアップ作成時の初期設定等の支援
2. インシデント発生時のコンサルテーション(初動対応支援)
3. 外部接続等を含むネットワーク構成の俯瞰的把握の支援

また、上記お助け隊サービス導入にあたり、既に中小企業等が利用できる補助金等の制度がある。「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」において紹介されており、セキュリティアクション制度[35]で情報セキュリティ対策に取り組むことを自己宣言することにより、IT 導入補助金を活用し、サイバーセキュリティお助け隊サービスを導入することができる。IT 導入補助金制度では、2022 年 8 月 9 日より通常枠のほか、セキュリティ対策推進枠が設けられ、IT 導入補助金 2024[36]においても継続されている。IT 導入補助金制度のセキュリティ対策推進枠の概要は以下のとおり。

図表 23 IT 導入補助金2024セキュリティ対策推進枠について

枠	通常枠		セキュリティ対策推進枠
補助額	5万円～150万円未満	150万円～450万円以下	5万円～100万円
機能要件	1プロセス以上	4プロセス以上	独立行政法人情報処理推進機構が公表する「サイバーセキュリティお助け隊サービスリスト」に掲載されているいずれかのサービス
補助率	1／2以内		1／2以内
対象経費	ソフトウェア購入費、クラウド利用費(クラウド利用料最大2年分)、導入関連費		サービス利用料(最大2年分)

(出所)IPA、『IT導入補助金2024公募要領セキュリティ対策推進枠』「IT 導入補助金2024セキュリティ対策推進枠について」より抜粋

サイバーセキュリティお助け隊サービス制度は、中小企業・小規模事業者を対象としており、中小企業・小規模事業者に該当する場合は医療分野、介護分野などの業界によらず支援対象となる。対象となる中

[34] 厚生労働省、令和5年 11 月6日第 19 回健康・医療・介護情報利活用検討会 医療等情報利活用ワーキンググループ「資料2-2サイバーセキュリティお助け隊サービスとの連携について」:https://www.mhlw.go.jp/content/10808000/001164214.pdf
[35] IPA、SECURIY ACTION:https://www.ipa.go.jp/security/security-action/
[36] 令和 5 年度補正サービス等生産性向上 IT 導入支援事業「IT 導入補助金 2024」:https://it-shien.smrj.go.jp/

小企業等は以下のとおり。

図表 24 中小企業等の定義

（中小企業等の定義）

業種分類	定義
①製造業、建設業、運輸業	資本金の額又は出資の総額が3億円以下の会社又は常時使用する従業員の数が300人以下の会社及び個人事業主
②卸売業	資本金の額又は出資の総額が1億円以下の会社又は常時使用する従業員の数が100人以下の会社及び個人事業主
③サービス業（ソフトウェア業又は情報処理サービス業、旅館業を除く）	資本金の額又は出資の総額が5千万円以下の会社又は常時使用する従業員の数が100人以下の会社及び個人事業主
④小売業	資本金の額又は出資の総額が5千万円以下の会社又は常時使用する従業員の数が50人以下の会社及び個人事業主
⑤ゴム製品製造業（自動車又は航空機用タイヤ及びチューブ製造業並びに工場用ベルト製造業を除く）	資本金の額又は出資の総額が3億円以下の会社又は常時使用する従業員の数が900人以下の会社及び個人事業主
⑥ソフトウェア業又は情報処理サービス業	資本金の額又は出資の総額が3億円以下の会社又は常時使用する従業員の数が300人以下の会社及び個人事業主
⑦旅館業	資本金の額又は出資の総額が5千万円以下の会社又は常時使用する従業員の数が200人以下の会社及び個人事業主
⑧その他業種（上記以外）	資本金の額又は出資の総額が3億円以下の会社又は常時使用する従業員の数が300人以下の会社及び個人事業主
⑨医療法人、社会福祉法人	常時使用する従業員の数が300人以下の者
⑩学校法人	常時使用する従業員の数が300人以下の者
⑪商工会・都道府県連合会及び商工会議所	常時使用する従業員の数が100人以下の者
⑫中小企業支援法第２条第１項第４号に規定される中小企業団体	上記①～⑧の業種分類に基づき、その主たる業種に記載の従業員規模以下の者
⑬特別の法律によって設立された組合又はその連合会	上記①～⑧の業種分類に基づき、その主たる業種に記載の従業員規模以下の者
⑭財団法人（一般・公益）、社団法人（一般・公益）	上記①～⑧の業種分類に基づき、その主たる業種に記載の従業員規模以下の者
⑮特定非営利活動法人	上記①～⑧の業種分類に基づき、その主たる業種に記載の従業員規模以下の者

（出所）IPA、『IT導入補助金2024公募要領セキュリティ対策推進枠』「２－２－１申請の対象となる事業者及び申請の要件（１）申請の対象となる中小企業・小規模事業者等の定義」の表より抜粋。

Ⅳ. 調査結果

Ⅲ. 調査内容の各項目 1 から 7 に対応した結果概要を示す。

1. 調査内容1の結果の概要

医療法施行規則の一部改正により、規則第 14 条第 2 項[37]が新設され、病院、診療所又は助産所の管理者が遵守すべき事項として医療の提供に支障をきたさないように、サイバーセキュリティを確保するために必要な措置を講じることが要件として追加された。介護事業者においてはセキュリティ要件について、介護保険法等の主要な法体系の中で明確にされていない。ただし、個人情報保護法については、介護分野においても、医療分野その他の分野と同様に個人情報を取り扱う性質上、安全管理措置等は義務付けられている。

2. 調査内容2の結果の概要

医療分野においては、医療法第 25 条に基づく医療機関等への立ち入り検査が実施されているが、介護分野においては立ち入り検査を規定する法的根拠はなく、実施されていない。セキュリティ対策実施について、医療機関等は法令の要件に加え、法令に基づいた立ち入り検査もあるため、介護分野と比較して強制力が強い。

3. 調査内容3の結果の概要

医療情報システムガイドライン 6.0 版では、対象事業者に介護事業者も想定されている。しかしながら、介護システムベンダは医療情報システムガイドラインへの対応を考慮はしているが、介護事業者では必要とされる安全対策措置等について、認識はまだ高くない状況にある。介護事業者にとって、医療情報システムガイドラインに示される事項をすべて理解し、リスク評価の上で対策事項を選択して対応することは難しい。介護事業者のセキュリティ対策については、どのレベルまで求められるのか、また実現可能な対策レベル等については今後の検討課題である。

4. 調査内容4の結果の概要

保険医療機関・薬局においてはオンライン資格確認の導入が令和 5 年 4 月から原則義務化されることを受け、医療機関等は、急速な対応が求められている。一方で、介護事業者については、オンライン資格確認の導入については、令和 6 年 3 月時点で原則、義務化はされていない。令和 5 年 11 月 30 日付けで「訪問看護療養費及び公費負担医療に関する費用の請求に関する命令の一部を改正する命令（令和 5 年内閣府・厚生労働省令第 9 号[38]）」が公布されたことにより、令和 6 年 6 月（7 月請求分）から、指定訪問看護事業者による電子情報処理組織を用いた費用の請求が開始されることとなる。医療分野と比較し、介護分野は、オンライン資格確認の導入の時期は後ろ倒しである。オンライン資格確認導入については、義務化されることにより、支援制度の拡充されたため、医療機関等の利用状況のように飛躍的に伸びる

[37] 医療法施行規則（昭和二十三年厚生省令第五十号）：https://elaws.e-gov.go.jp/document?lawid=323M40000100050

[38] 令和 5 年 11 月 30 日官報号外（第 251 号）：https://kanpou.npb.go.jp/old/20231130/20231130g00251/20231130g002510019f.html

ことが予想される。導入の際には、Ⅲ.3の調査内容にあるとおり、医療情報システムガイドラインで許容されているネットワーク接続方式の中でも厳しいセキュリティ対策が求められるため、副次的に安全管理措置等も強固になる可能性があり、同時並行してセキュリティ対策の向上が期待される。

厚生労働省のオンライン資格確認の導入について（医療機関・薬局、システムベンダ向け）サイト[39]によれば、保険医療機関・薬局における 2024 年 1 月 28 日時点の導入（運用開始）施設数は、206,863施設にのぼっている。保健医療機関・薬局の導入状況及びオンライン資格確認システムの利用状況については、以下のとおり。

図表 25 保健医療機関・薬局の導入状況

（出所）厚生労働省、オンライン資格確認の導入について（医療機関・薬局、システムベンダ向け）サイトより抜粋引用

図表 26 オンライン資格確認システムの利用状況

（出所）厚生労働省、オンライン資格確認の導入について（医療機関・薬局、システムベンダ向け）サイトより抜粋引用

5. 調査内容5の結果の概要

厚生労働省医政局では、サイバーセキュリティの脅威の増大により、政府主導でのサイバーセキュリティ教育を実施している。一方で、介護分野では所管省庁主導による介護事業者向けのセキュリティ教育は実施されていない。介護分野についてはセキュリティ教育が十分に実施されているとはいえないが、今後、介護分野におけるデジタル化の動向を踏まえて、介護事業者向けのセキュリティ教育は介護DXを

[39] 厚生労働省、オンライン資格確認の導入について（医療機関・薬局、システムベンダ向け）サイト：https://www.mhlw.go.jp/stf/newpage_08280.html

円滑かつ安全に推進する上で必要であると認識はされている。今後、セキュリティ教育をどのように主導していくのかは検討が必要である。

6. 調査内容6の結果の概要

医療分野は NISC による重要インフラ分野として特定されているが、介護分野については特定されていない。医療機関においては、既にサイバーセキュリティの脅威にさらされ、医療提供に重大な支障を及ぼす事案が発生している。医療セプター及び日本医師会のサイバーセキュリティ支援制度は、医療の提供においてサイバー攻撃等による支障をきたさないようにするため設けられた。介護事業者においても同様の情報共有の仕組みがあることが望ましい。サイバーセキュリティ支援制度は、会員の事業者であれば利用可能であることも認知が広がれば、介護事業者も利用すると推測される。現時点で、介護事業者では、医療機関等で既に起こったサイバー攻撃等の被害のように重大な支障が起きた事案について、公表資料及び報道等では確認されていない。しかしながら、今後、介護 DX 推進する上で、医療機関等と同様にサプライチェーンリスクに対処するため、介護分野のセキュリティ対策の底上げのためにも介護事業者が利用できる情報共有の仕組みの確立について検討が必要である。サイバーセキュリティの脅威について、セキュリティ事故の情報に直面することにより、セキュリティ意識向上に繋がる可能性がある。

7. 調査内容7の結果の概要

サイバーセキュリティお助け隊サービス制度については、対象となる中小企業等の定義に該当すれば、医療分野、介護分野等にかかわらず活用可能である。IT 導入補助金のセキュリティ対策推進枠もあり、本制度が広く周知され、介護事業者での認知を高める必要がある。セキュリティ対策支援制度については、既に整備された制度利用により、介護分野においても安全管理対策の推進に寄与すると思料する。

8. まとめ・考察

調査結果 1 から 7 に基づいて、以下のとおり、まとめ・考察を行った。

介護分野では、介護保険法等の法体系の中では、セキュリティ要件は明確に規定されていないが、医療分野では、医療法施行規則の一部改正、セキュリティ確保について確認する医療法第 25 条に基づく立ち入り検査の仕組みがある。これにより、医療分野と比較し、介護分野におけるセキュリティ対策の強制力が異なる。医療分野においては、医療法の体系の中でセキュリティ要件が明確化されたことにより、医療機関等のセキュリティ対策は必須となるため、医療分野のセキュリティ意識が必然的に高まりセキュリティ対策も進んだ。立ち入り検査というチェック機構は、セキュリティ対策を確実に進める上では必要な取組といえる。

医療機関等では、またオンライン請求、オンライン資格確認等のシステム導入の原則義務化、サイバー攻撃等の事案を受けてセキュリティ教育をはじめとして支援制度が拡充され、並行して安全管理措置等の対応も進展している。オンライン資格確認等システム導入、オンライン請求に伴う補助金等の制度拡充により、導入率は義務化にむけて飛躍的に伸びた。一方で、介護分野においては、医療分野と比較し、セキュリティ要件の明確化、立ち入り調査のような法的に大きな拘束力はない。また、オンライン資格確認・オンライン請求の原則義務化についても進んではいない。医療分野で採用されているオンライン資格確認・オンライン請求ネットワークの導入にあたっては、医療情報システムガイドラインで許容されている接続方式の中でもより厳しいセキュリティ要件に対応が必要となるため、介護分野で今後導入する場合、よ

り強固なネットワークセキュリティの安全管理措置等の対応が求められることになる。

また、こうしたデジタル化におけるサイバーセキュリティの脅威への対策に関して、医療は医療提供に支障が伴う事案の発生を受けて、厚生労働省所管局の主導での教育事業が行われている。一方で、介護分野は教育については自助努力によるところが大きく、厚生労働省所管局主導での教育事業が行われていない。介護事業者へのセキュリティ教育について、今後どのように進めるのか課題である。

サイバーセキュリティの脅威についても既に医療提供に支障をきたすような深刻な事態があった医療分野では、当事者意識を持ち、教育によるセキュリティ意識向上の機会ともなったといえる。介護分野においては、差し迫ったサイバーセキュリティの脅威について認識を深めるような教育の機会が医療分野と比較して乏しい可能性もある。

IPA による IT 導入補助金[40]、お助け隊サービスについては、中小企業等の定義に該当すれば医療機関と介護事業者はいずれも活用できる。こうしたセキュリティ対策も含めた IT 導入に係る制度について、介護事業者に周知をすることにより、デジタル化に伴うセキュリティ対策についても認識が拡がり、進展すると予想される。医療機関等と比較し、介護事業者には教育機会が乏しいため、こうした支援制度の認知度に差があるのではないかと推察される。

医療分野と介護分野の各項目の調査結果の概要を以下表に示す。

図表 27 医療分野と介護分野の調査結果のまとめ比較表

カテゴリ	医療分野	介護分野
法令に基づくセキュリティ要件	あり。 医療法施行規則でセキュリティ要件を明確化。	なし。 （ただし、個人情報保護法に基づく安全管理措置はある。医療分野も同様。）
法令に基づく立ち入り検査	あり。 医療法第25条に基づく立ち入り検査では、医療情報ガイドライン等を参照し、セキュリティ対策をチェック。	なし。
オンライン資格、オンライン請求の原則義務化	○ 原則義務化	△ 介護事業を行っている一部法人は医療保険請求について令和 6 年度に対象となる。
サイバーセキュリティに関する情報共有の仕組み（NISC の行動計画に基づいたセプター設置等の対応）	○ NISCの重要インフラの行動計画において、特定している重要インフラ分野に医療分野は特定され	× NISC の重要インフラの行動計画において、対象としている重要インフラ分野に介護分野は特定されて

[40] IPA、IT 導入補助金の申請要件になっています SECURIY ACTION：https://www.ipa.go.jp/security/security-action/it-hojo.html

カテゴリ	医療分野	介護分野
	ている。日本本医師会が医療セプター事務局。	いない。
日本医師会のサイバーセキュリティ支援制度	△ 日本医師会会員の医療機関等向け。	△ 日本医師会の会員が開設・管理する介護サービス施設・事業所向け。
厚生労働省が主体のセキュリティ教育	○ 医政局による教育事業で実施。	× 左記のような厚生労働省の所管局による事業実施はされていない。
IPA のお助け隊サービス導入の中小企業等の導入の補助金	○ 中小企業等は対象。	○ 中小企業等は対象。

（出所）調査結果を基に株式会社三菱総合研究所にて作成

医療分野と介護分野を比較した場合、法令に基づく制度的対応が進んでいることから、医療分野では、法的拘束力が強いため、対応せざるを得ない状況にある。医療分野においては、サイバーセキュリティに係る情報共有、教育等の仕組みを有することから、介護分野と比較してセキュリティ意識向上に繋がり、セキュリティ対策の重要性について認識を深めていると推測される。医療分野については、介護分野と比較してオンライン資格確認・オンライン請求ネットワーク等におけるデジタル化が先行して進んでいることから、それに伴って導入において接続要件が厳しい 2 つの接続方式に限定されるため、セキュリティ対策をより強固にしている可能性がある。

介護分野についても、今後、オンライン資格確認・オンライン請求ネットワーク等の導入の検討を進めていく上では、従来よりも厳しいセキュリティ対策が求められることもあり、安全管理措置について介護事業者が認識を深めていく必要がある。介護事業者においては、情報システム部門を有さない小規模法人も多いと想定されるため、制度面での整備だけでなく、教育・相談といった支援や、機器導入等に関連する支援制度のさらなる拡充が求められる。

第３章　介護現場のセキュリティ対策の実態把握の調査

Ⅰ. 調査の目的

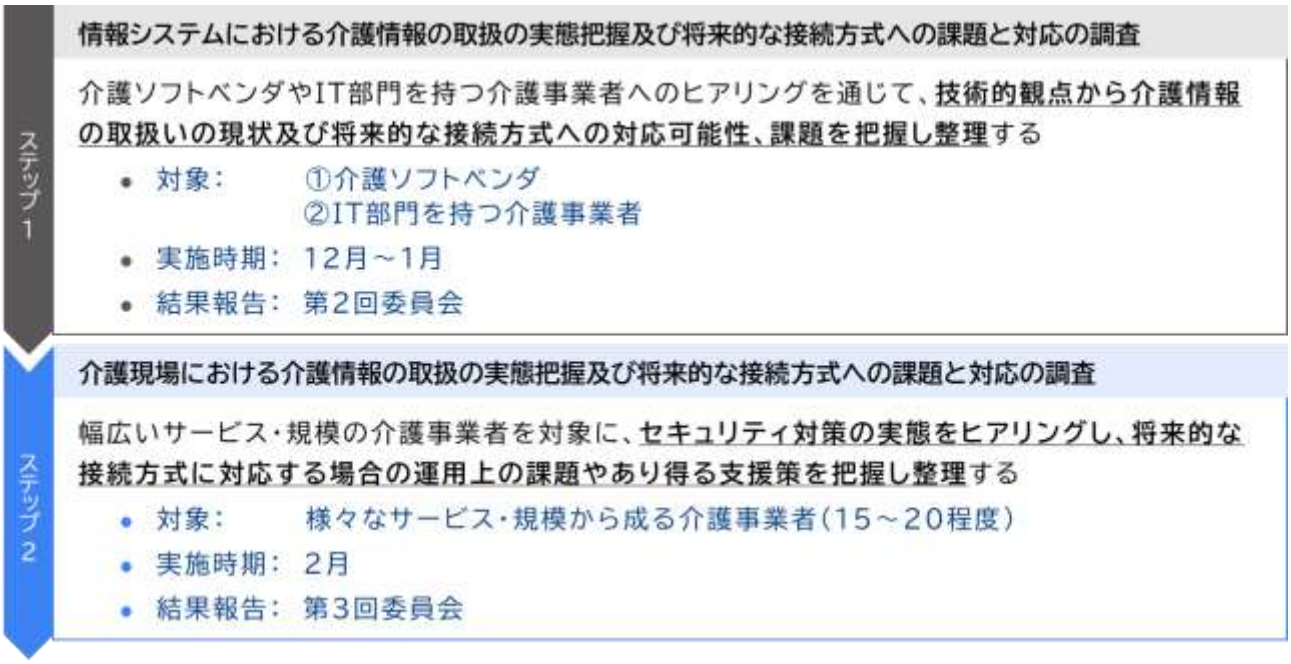
将来的に多くの介護事業所が医療情報を取り扱うことや、介護情報も医療情報と同様の取扱いが求められることを念頭に、将来的な取扱いにおける課題と支援策を検討するため、介護現場における安全管理措置の実態を把握することを目的とした。

Ⅱ. 調査方法

介護ソフトベンダや IT 部門を持つ介護事業者へのヒアリングを通じて、技術的観点から介護情報の取扱いの現状及び将来的な接続方式への対応可能性、課題を把握し整理することを目的としたステップ 1 と、幅広いサービス・規模の介護事業者を対象に、セキュリティ対策の実態をヒアリングし、将来的な接続方式に対応する場合の運用上の課題やあり得る支援策を把握し整理することを目的としたステップ２の二段階に分け、ヒアリング調査を行った。

調査概要は以下のとおり。なお、ヒアリング調査は原則対面またはオンライン会議で実施したが、対象者の都合のため、一部メールにて調査を行った。

図表 28 ヒアリング調査の概要



Ⅲ. 調査内容

ステップ 1、ステップ 2 の主な調査項目は以下のとおり。

図表 29 ステップ 1 調査項目

調査項目
○ 現状のセキュリティ対策について 【介護ソフトベンダの場合】 ・ 提供しているサービスの提供形態（クラウド、オンプレミス、スタンドアロン等） 【IT 部門を持つ介護事業者の場合】 ・ 法人内の介護施設・事業所で利用している介護ソフトの提供形態（クラウド、オンプレミス、スタンドアロン等） ・ サービスへのアクセス管理・認証方法への対応 ・ 介護事業者内の複数のユーザによるアクセスの管理・認証方法（職員単位/職種単位/事業所単位/といった単位（任意の単位含む）の設定や、単位別に閲覧可能な情報が設定・管理・コントロール可能かどうか等） ・ 介護事業者内のユーザによる操作ログの取得が可能かどうか、実際に取得しているかどうか、及びそのログの粒度（いつ、誰が、どの利用者の、どの項目を、どのように操作したか（印刷・データ出力含む）等） ・ 情報システムの利用に際し、安全管理に関して求めている事項や推奨している事項 ・ 介護事業者に対する安全管理に関する支援や、問い合わせ対応を行っている場合は問い合わせ内容と頻度 ・ 介護ソフトベンダや IT 部門として求める安全管理事項と、事業所側で実際に実施できている内容とのギャップとその原因 ・ 提供する情報システムが取扱う個人情報や要配慮情報に対する安全管理措置 【介護ソフトベンダの場合】 ①導入時に介護事業者から安全管理上の要件や第三者機関による認定・認証の取得の有無の確認を求められるケース ②導入後に介護事業者から運用状況や点検結果について定期的な報告を求められるケース ③OS やミドルウェア等において脆弱性が発見された場合や、マルウェアによる事件が発生した場合の、介護事業者からの問い合わせの数 【IT 部門を持つ介護事業者の場合】 ①第三者機関による認定・認証を取得しているもの ②通信の監視や点検等の運用状況、およびその結果について現場へのフィードバックの状況 ・ 「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」チェックリストにおいて、「いいえ」または「対象外」となる事項とその理由 ○ 医療機関・介護事業所間の情報共有・連携を想定したセキュアなネットワーク構成・接続方法について

調査項目
（訪問看護と同様に専用の端末及び回線を用いる方式が採用される場合を想定） 【介護ソフトベンダの場合】 ・ 介護ソフトベンダとして実施しなければならないと想定される事項 ・ 介護事業者が実施しなければならない（介護ソフトベンダでは実施できない）と想定される事項 【IT 部門を持つ介護事業所の場合】 ・ IT 部門として実施しなければならないと想定される事項 ・ 介護ソフトベンダが実施しなければならないと想定される事項 ・ 介護現場において実施しなければならないと想定される事項 【共通】 ・ 移行に当たり必要と考えられる支援 ・ 介護情報も医療情報と同等の扱いが求められるようになった場合に必要な対応や支援

図表 30 ステップ 2 調査項目

調査項目
○ 情報システムの利用・管理について ・ 情報システム・IT に関する部署・担当者の配置状況 ・ 介護情報の記録・請求における情報システム・IT の利用状況 ○ 電子化された利用者に関する情報を入力・閲覧する端末の管理について ・ 情報を利用する職員の人数に対する端末の台数 ・ 端末の管理方法 ・ 端末内への情報のアクセスの制限方法 ・ 端末が接続できるネットワーク ・ 職員の業務に応じた情報の整理分類や閲覧・編集制限 ・ 個人情報や医療情報の取扱いに関して職員向けの資料等の作成・周知・定期的な教育 ・ 職員個人の私有端末の業務利用（BYOD） ・ 端末に保存されている情報のバックアップの実施有無・方法・頻度 ○ 医療機関・介護事業所間の情報共有・連携を想定したセキュアなネットワーク構成・接続方法について （訪問看護と同様に専用の端末及び回線を用いる方式が採用される場合を想定） ・ 現在の業務からの想定される変更点 ・ 上記の変更を実施するにあたり課題となる事項 ・ 上記の課題に対し、必要と考えられる支援 （国や自治体、介護ソフトベンダ等による支援）

Ⅵ. 調査結果

1. ステップ 1(介護ソフトベンダや IT 部門を持つ介護事業者へのヒアリング)調査結果

調査対象となった介護ソフトベンダや IT 部門を持つ介護事業者は、介護ソフトベンダ 4 社、と大規模な IT 部門を抱える介護事業者 1 社の合計 5 社であった。

- 提供しているサービスの提供形態(クラウド、オンプレミス、スタンドアロン等)について

【介護ソフトベンダ】

- クラウド(SaaS)と一部オンプレミスを提供しているのが 2 社、クラウド(SaaS)を提供しているのが 1 社、クラウドを提供しており、調査対象となった全ての介護ソフトベンダにおいてクラウド型を提供していた。

【IT 部門を持つ介護事業所向け】

- 提供するサービス種別ごとに業務シーンに応じた複数の介護ソフトを組み合わせて利用しており、提供形態としてはクラウド(SaaS, PaaS, IaaS)がほとんどである。

- サービスへのアクセス管理・認証方法への対応について

【介護ソフトベンダ】

- 調査対象となった全ての介護ソフトベンダにおいて ID・パスワードによる認証が実装されており、その他の認証方法がないといった回答があった。
- また、認証方法として、クライアント証明書を導入しているといった回答があった。

【IT 部門を持つ介護事業者】

- ID パスワードによる認証を実装し、外部環境から接続が可能な SaaS 等の介護ソフトの場合は IP アドレス制限をかけている。また、利用者の情報を含む場合は 2 段階認証、2 要素認証を導入している。

- 介護事業者内の複数のユーザによるアクセスの管理・認証方法について

【介護ソフトベンダ】

- アクセス管理については、調査対象となった全ての介護ソフトベンダにおいて職員単位で管理が可能である。また、事業所単位や職員グループ(職種)で管理が可能であるところもあった。
- 認証方法については、クライアント証明書を導入しているところがあった。

【IT 部門を持つ介護事業者】

- 提供するサービス種別や職務権限に応じて、介護ソフト自体や個別機能の利用、データ参照の権限を設定・管理・コントロールしている。

- 介護事業者内のユーザによる操作ログの取得が可能かどうか、実際に取得しているかどうか、及びそのログの粒度について

【介護ソフトベンダ】

- ログの取得については、事業者側でログの取得が可能なところが 3 社、事業者側での取得は不可能であり、運営から取得できるが解析に時間を要するところが 1 社であった。

- ログの粒度については、追加、編集、削除のログは残しているが、閲覧や出力、読み込みについては残していないところがあった。

【IT 部門を持つ介護事業者】

- ログの取得については、システムによりレベルの差はあるが保存はされている。
- ログの粒度については、画面を開いたというログがあるため、基本的に誰がどの操作をしたかは把握できる。

● 情報システムの利用に際し、安全管理に関して求めている事項や推奨している事項について

【介護ソフトベンダ】

- ID やパスワードの管理はユーザ側管理であることを利用規約上に明記し、その他は特に設定せず介護事業所側に委ねているところが多かった。

【IT 部門を持つ介護事業者】

- IT 管理規定に紐づく要領にて、アカウント・パスワード管理、コンピュータウイルス対策、インターネット、Web、電子メール利用などのガイドラインを設けている他、定期的な社内ニュースにて意識醸成、啓蒙を図っている。

● 介護事業者に対する安全管理に関する支援や、問い合わせ対応を行っている場合は問い合わせ内容と頻度

【介護ソフトベンダ】

- 安全管理に対する支援については、導入時や問い合わせ時に行っているところがあった。一方で、特に何も行っていないところもあった。
- 問い合わせ内容については、「訪問看護ステーション」関連の顧客からガイドラインや医療オンライン請求関連の問い合わせがあるが、それ以外のセキュリティ関連の問い合わせはほとんどないといったころがあった。

【IT 部門を持つ介護事業所】

- 職員に対する情報の安全管理に関する教育・研修については、年次での全職員向け e-ラーニング、標的型攻撃メール訓練、および前述の定期的な社内ニュースによる意識醸成・啓蒙などを実施している。また、情報の安全管理に関する問い合わせについて社内コールセンターによる対応を行っている。

● 介護ソフトベンダとして求める安全管理事項と、事業所側で実際に実施できている内容とのギャップとその原因について

【介護ソフトベンダ】

- 介護事業所側の IT やセキュリティに関するリテラシーが低く、セキュリティについて顧客自身で考えなければいけない、といった意識が欠如しているといった回答がいくつかあった。
- また、複数人での端末の共有や介護ソフトの ID やパスワードの共有、システム専任者の不在といった回答もあった。

【IT 部門を持つ介護事業所】

- 対人業務を主業務とする実態から、法人本部と現場との意識レベルのギャップが一定程度存在するものと見受けられる。IT 部門としては P マークを取得したいが、現場サイドとしては対応が

難しく、特に執務室を離れるときに毎回施錠するといったことがかなりのハードルになる。

● 提供する情報システムが取扱う個人情報や要配慮情報に対する安全管理措置について

（a）導入時に介護事業者から安全管理上の要件や第三者機関による認定・認証の取得の有無の確認を求められるケース（介護ソフトベンダ向け）

- 医療系や民間の介護事業者の確認は多いが、一般的な介護事業者からの確認はあまりないといったところがあった。
- また、システム導入時に安全管理やセキュリティに関する言葉が出てくることが稀であるといったところもあった。

（b）導入後に介護事業者から運用状況や点検結果について定期的な報告を求められるケース（介護ソフトベンダ向け）

- 定期的な報告を求められるケース自体が多くないが、一部の民間の介護事業者や、地域包括支援センターのシステムにおいて自治体から ISMS の取得状況について問い合わせがあるといったところがあった。

（c）OS やミドルウェア等において脆弱性が発見された場合や、マルウェアによる事件が発生した場合の、介護事業者からの問い合わせの数（介護ソフトベンダ向け）

- 医療系や民間の介護事業者からの問い合わせはいくつかあるが、一般的な介護事業者からの問い合わせはほとんどないところが多かった。

（d）第三者機関による認定・認証の取得をしているもの（IT 部門を持つ介護事業者向け）

- サービスを外販する部門において ISMS 認証を取得している。取得したのは本社サイドであり、介護部門での管理については認証の対象外である。

（e）通信の監視や点検等の運用状況、およびその結果について現場へのフィードバックの状況（IT 部門を持つ介護事業者向け）

- 通信の監視については常時、点検については月例にて実施しているが、現場への結果のフィードバックは特に行っていない。

- 一般社団法人保健医療福祉情報システム工業会（JAHIS）「サービス事業者による医療情報セキュリティ開示書」（以下：SDS）において、「いいえ」または「対象外」となる事項とその理由（介護ソフトベンダ向け）
  - 運用管理規程等において組織的安全管理対策に関する事項等を定めているか？（SDS Ver4.1 質問 9）
    - 「患者等への説明と同意を得る方法」については製品の利用規約上、契約する事業所（医療機関等）に委ねている。
  - 保守作業等で医療情報システムに直接アクセスする作業を行う際には、作業者・作業内容・作業結果を医療機関等に報告できるようになっているか？（SDS Ver4.1 質問 28）
  - 改造や保守に関する作業の記録として、個人情報へのアクセス有無、及びアクセスした対象を特

定できる情報を医療機関等に提供できるか？（SDS Ver4.1 質問 40）

- メンテナンスを実施する場合は、事前に医療機関等に作業申請を提出できるか？（SDS Ver4.1 質問 44）
- メンテナンス終了時に、速やかに医療機関等に作業報告書を提出できるか？（SDS Ver4.1 質問 45）
  - 利用者に影響のあるメンテナンスを実施する際には事前に製品内お知らせという形で告知を行うが、完了報告や事前の承諾の取得、詳細内部情報の開示等は行っていない。
- 清掃等の直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行っているか？（SDS Ver4.1 質問 29）
  - 物理的なサーバを持たず、データは全て Amazon Web Services 上にあるため物理的なメンテナンスや確認は行っていない。
- ユーザに提示できる情報種別ごとの破棄の手順があるか？（SDS Ver4.1 質問 32）
  - 利用者に影響のあるメンテナンスを実施する際には事前に製品内お知らせといった形で告知を行うが、完了報告や事前の承諾を取る、詳細内部情報の開示等は行っていない。

● 訪問看護と同様に専用の端末及び回線を用いる方式が採用される場合、介護ソフトベンダとして実施しなければならないと想定される事項について （介護ソフトベンダ向け）

- 医療オンライン請求義務化については、端末・回線の提供まで関与は難しく、必要様式のデータを出力する対応を実施するのみにとどまった。介護でオンライン請求を導入した場合は、仕様にもよるが医療オンライン請求と同様の対応が必要になることが想定される。
- 医療機関であれば IT ベンダが出入りしている場合が多く、ガイドライン対応でそこまで困らないが、介護事業者はそのような頼れる先が無いのが通例であるため、介護ソフトベンダを頼る可能性が高い。医療のオンライン請求では、回線提供業者と提携してサービスを紹介や、関連情報の動画を提供等の対応をしたが、介護の場合も何らかの情報提供等の支援が必要になると考えられる。
- 顧客先に直接訪問する機会が少なく、導入支援事業者に対応していただくことが増えると見込んでいるため、導入支援事業者と顧客間の導入に関する調整を行う。顧客にサービスを利用いただけるように導入支援事業者と専用プランを準備することが想定される。
- システムそのものについては対応するが、専用端末や回線については販売店に対応いただくことになる。

● 介護事業者が実施しなければならない（介護ソフトベンダでは実施できない）と想定される事項について （介護ソフトベンダ向け）

- 改善準備、ネットワーク構築、PCセットなどを行う導入支援事業者との契約。
- 訪問看護での本格的な問い合わせがまだないため、実情が分からない。

● IT 部門として実施しなければならないと想定される事項について （IT 部門を持つ介護事業者向け）

- 介護の情報管理レベルと医療の情報管理レベルの違い、現場の意識レベルの違いといった事情や、専用の設備が必要になること等を踏まえて、物理的な専用の端末および回線の手配を行い、

セキュリティのレベルを医療情報と同等のレベルに強化する必要がある。また、本社部門と共同して現場の職員への教育や案内の準備を確実に実施する必要がある。

- 今は請求情報を現場ではなく本社部門が集約して請求を実施しており、それが現場の負担を軽減している。「訪問看護におけるネットワーク方式」の図では、請求も事業所別に実施することになっているように見えるが、本社で実施していた請求を現場で実施することになる場合、事業所には抵抗があると思われる。

● 介護ソフトベンダが実施しなければならないと想定される事項について （IT 部門を持つ介護事業者向け）

- 利用環境の変更に伴う介護ソフトの設定変更、セキュリティ対策の強化。

● 介護事業者が実施しなければならないと想定される事項について （IT 部門を持つ介護事業者向け）

- 変更後の介護ソフト利用手順の習熟、取得や、業務運用の変更。

● 移行に当たり必要と考えられる支援について

【介護ソフトベンダ】

- 回線や端末の提供やセットアップを支援する事業者や補助金、相談窓口の設置。
- 1 台の端末に複数の証明書、もしくは1つの証明書で複数の事業所の請求を担保する支援。

【IT 部門を持つ介護事業者】

- 医療分野での既存対応に関する具体的かつ詳細な仕様等や新方式運用におけるガイドラインなどの開示。そのようにすることで、諸々の対策事例を参考にできればスムーズに進むのではないかと考えられる。

● 介護情報も医療情報と同等の扱いが求められるようになった場合に必要な対応や支援について

【介護ソフトベンダ】

- 介護業界に安全管理、IT の知識がある人材が不足していることが課題であり、それを補う制度が必要と考えられる。介護ソフトベンダ側で相談窓口になることは考えられるが、介護ソフトベンダ側にも限界があり、制度の公式窓口と介護ソフトベンダの窓口の役割分担が必要と考えられる。
- 2 要素認証や出力ログは対応が必要な認識であるが、それ以外は正直把握できていない。システム側では現状を鑑みて、医療も介護も基本的に同様の対応で問題ないと考えられる。

【IT 部門を持つ介護事業者】

- インフラ面全般のセキュリティ対策強化、全職員のセキュリティ意識の向上などが考えられる。医療分野での展開時における具体的ノウハウの開示は有用な参考情報となる。

2. ステップ2（介護事業所へのヒアリング）調査結果

調査対象となった施設・事業所の基本情報は以下のとおり。

図表 31 ステップ 2 調査対象施設・事業所

No.	サービス	所在地	所在地の人口規模	利用者数	職員数	法人種別
1	訪問介護	東京都羽村市	56万人	25人	17人	営利法人
2	訪問看護	東京都渋谷区	20万人	54人	12人	営利法人
3	訪問リハビリテーション	神奈川県横須賀市	43万人	46人	8人	医療法人
4	訪問リハビリテーション	長野県松本市	24万人	432人	44人	医療法人
5	訪問リハビリテーション	大阪府八尾市	26万人	65人	9人	医療法人
6	通所リハビリテーション	埼玉県川越市	30万人	272人	17人	医療法人
7	看護小規模多機能型居宅介護	山形県新庄市	4万人	22人	18人	営利法人
8	居宅介護支援	北海道帯広市	20万人	195人	6人	医療法人
9	居宅介護支援	東京都江戸川区	70万人	264人	7人	営利法人
10	介護老人福祉施設	東京都杉並区	53万人	150人	103人	社会福祉法人（社協以外）
11	介護老人福祉施設	三重県鈴鹿市	19万人	80人	65人	社会福祉法人（社協以外）
12	地域密着型介護老人福祉施設	富山県富山市	41万人	22人	38人	社会福祉法人（社協以外）
13	地域密着型介護老人福祉施設	鹿児島県南さつま市	4万人	29人	36人	社会福祉法人（社協以外）
14	介護老人保健施設	北海道函館市	30万人	150人	67人	医療法人
15	介護老人保健施設	福島県福島市	30万人	90人	95人	医療法人
16	特定施設入居者生活介護	福岡県苅田町	3万人	50人	25人	医療法人
17	特定施設入居者生活介護	東京都三鷹市	18万人	60人	37人	営利法人
18	認知症対応型共同生活介護	岐阜県北方町	2万人	27人	27人	社会福祉法人（社協以外）

● 情報システム・IT に関する部署・担当者の配置状況について

- 比較的規模が大きく、施設や事業所を複数運営しているような法人の場合、法人本部としては情報システム専門の部署や担当者を配置していた。一部、施設や事業所ごとにも専任で配置しているところもあった。
- 法人本部の担当者は、情報インフラや介護ソフトの更新時等に各施設・事業所を回ることもあるが、安全管理措置の指導や点検を目的としたものではないとのことであった。
- 小規模な法人では、専任の人員を配置しておらず、管理者が兼任している場合が多かった。

● 介護情報の記録・請求における情報システムの利用状況について

- 介護ソフトを用いて請求や日々の記録を行っており、利用者に関する情報は介護ソフトで一括管理しているところがほとんどであったが、記録のみ紙で作成するところもあった。

● 情報を利用する職員の人数に対する端末の台数について

- 一部の施設や居宅介護支援事業所では 1 人 1 台支給しているところもあったが、何らかの形で共用しているところが多かった。

● 端末の管理方法について

- 施錠可能な部屋に設置しているところが多かったが、利用者が立ち入り可能な区域に、ワイヤーロック等の措置を講じずに設置しているところもあった。
- 規模が大きく、施設や事業所を複数運営しているような法人の場合は端末管理システム（MDM）を導入している傾向があった。

● 端末内の情報のアクセスの制限について

- 端末そのものへのアクセスと、インストールされている介護ソフトへのアクセスに分かれているところが多く、それぞれに独立して ID・パスワードを設定しているところと、いずれか一方のみ設定しているところがあった。
- ID の共用も比較的少ないが一部のところではあり、大規模な法人でも共用しているところがあった。理由として、ID 発行数に応じて介護ソフトのライセンス料が発生し、及び終業前等のごく一部の利用時間のためだけに利用する職員が大半であることから、該当する職員全員に ID を発行しようとすると大きな費用負担が発生することが挙げられた。
- 介護ソフトへのログインについては、職員毎に ID やパスワードの付与に加えて、職員ごとに保有している USB キー認証を取り入れているところもあった。また、大規模法人で、利用者の情報を含む場合は 2 段階認証、2 要素認証を導入しているところもあった。

● 端末が接続できるネットワークについて

- 法人内・社内ネットワークとインターネットに接続できるところがほとんどであった。また、これらに加え事業所内のネットワークに接続できるところもあった。
- 外部環境から接続可能な SaaS 等の介護ソフトについては IP アドレス制限をかけているところもあった。

● 職員の業務に応じた情報の閲覧・編集制限について

- 経営に関する情報については、職員の業務に応じて閲覧・編集制限をかけているところが多かった。
- 利用者の情報については、特に制限を設けていないところが多かった。制限を設ける例としては、同法人内の異なる施設や事業所の利用者情報については見られないよう制限をかけるところや、利用者の家族や職業等の特に配慮すべきと考えられる情報については一部の職員のみに制限をかけているところがあった。

● 個人情報や医療情報の取扱いに関して職員向けの資料等の作成・周知・定期的な教育について

- 入職時に教育することに加え、個人情報・倫理・プライバシーの法定研修の位置づけとして、年に 1 回の定期的な研修や社内ネットワークを通した周知を実施しているところが多かった。
- また、入職時のみ研修を実施しているところや、業務に追われ必要という認識はあるが実施できていないところもあった。

● 職員個人の私有端末の業務利用（BYOD）について

- BYOD は禁止されており、実際に行われていないところが多かった。ただ、稀なケースではあるが、各調査の際の手すりの位置の撮影や、事業所内のタブレット端末が持ち出されている時に一時的に私有スマホで写真を撮影するところがあった。
- 例外的な利用も含めて、BYOD のための運用管理規定を作成しているところはほとんどなかった。

● 端末に保存されている情報のバックアップの実施有無・方法・頻度について

- バックアップの有無については、情報を端末内に保存しておらず、クラウド管理の介護ソフトを使用しているところがほとんどであった。
- また、法人内のサーバに保存しているところや、介護ソフトとは別に一部、端末に保存している情報については、定期的に手動でバックアップを実施しているところが多かった。
- 手動バックアップの方法については、USB メモリで行っているところもあった。
- バックアップの頻度については、毎日や 3,4 ヶ月に 1 回等様々であった。

● 訪問看護と同様に専用の端末及び回線を用いる方式が採用される場合、現在の業務からの想定される変更点について

- 具体的なオペレーションは、実際に対応内容が決まらないことには想像できないという回答が多かった。
- 専用回線や専用端末を利用する方式になった場合、介護保険の請求で現在一般的に行われている代理請求の仕組みを引き続き利用できるのかどうかが気がかりという回答もあった。具体的には、法人本部がまとめて請求するといったことが不可能になる場合、大きなオペレーションコストが発生することになることを懸念していた。

● 上記の変更を実施するにあたり課題となる事項

- 医療保険のサービスも行っている施設では、新たにネットワーク構成を検討する必要があり、機器導入等のコスト面、設定等の技術面でも課題があるという回答があった。

● 上記の課題に対し、必要と考えられる支援

- 情報システムの担当が不在の介護事業所もあると思われるため、導入を促進するにはシステムのパッケージ化や補助金の付与等が必要ではないかという回答が多かった。
- システムや回線の手配など、特に大きく費用の掛かる導入時に補助金が必要であることに加え、端末のリース料金、故障時も含めた保守費用、老朽化による買い替え等、ランニングでかかるコストについても支援が必要になるという回答もあった。
- 運用面の支援については、医療分野での既存対応に関する具体的かつ詳細な仕様等や新方式運用におけるガイドラインなどを共有することで、先行対策事例を参考にできればスムーズに進むのではないかという回答もあった。

3. まとめ・考察

● ステップ 1

- 総論として、介護ソフトベンダは、現状の介護ソフトのセキュリティ面の機能・仕様には各社それぞれ差異があるものの、介護情報においても医療情報と同様の取扱いや接続方式が求められた場合には、求められる機能要件や連携仕様が十分な猶予をもって明確に示されれば、大きな技術的課題はないと考えている。一方で、エンドユーザの理解や認知にも時間はかかるため、やはり十分な猶予をもって、介護事業者に対して対応方針や具体の内容を国や自治体等から説明・周知する必要がある。
- システムを利用するユーザ（ID）単位で情報の閲覧権限を設定する機能はあるものの、「どのような情報をどのような職種が閲覧するべきか」といった判断は現場に委ねている。実態としては、職員 1 人 1 台の端末がない事業所がほとんどであること、またログイン・ログアウト等の運用上の効率性の観点から、介護ソフトベンダとして推奨するものではないが、複数の職員で ID を共有するケースがあるものと理解している。
- IT に専従する人材が存在しない・確保できないということもあって、自己の業務の範疇に情報の安全管理を十分に位置づけられていない可能性がある。
- 介護事業者に対するあり得る支援としては、訪問看護と同様の公的な補助金や、導入支援事業者による支援が必要と考えられる。介護ソフトベンダの役割としては、導入支援事業者との連携・調整が挙げられる。

● ステップ 2

- 経営管理・企画管理の面では、規模が大きい法人では情報システム・IT の専門部署を配置できる余力があるものの、規模が小さい場合には、専門的なスキルの有無にかかわらず、管理者が包括的に管理せざるを得ないように思われた。
- 介護情報の安全管理に関する教育については、入職時のほか、法定研修として定められているプライバシー保護の取り組みに関する研修を 1 年に 1 度実施している事業者が多く、具体的な研修の中身までは調査できていないものの、一定程度実施されていると考えられる。一部、研

修の中身については、厚生労働省が提供している様々なマニュアルやガイドラインを参照して独自に作成しているという意見もあり、一定のコストを投じて整備している印象を受けた。

- 端末の管理について、コストの問題から端末の共用は一定程度発生しているものの、ID については比較的１人につき１つの ID の運用がなされており、電子化されている介護情報について、「いつ」「誰が」「何の情報を」「どのように操作したのか」は確認できる状態であるように思われた。ID を共用している例のうち重要な場合として、介護ソフトによっては発行する ID 数に応じてライセンス料が必要なケースもあり、１日に僅かな時間しか使わない職員が多数存在するような業務形態のサービスでは、ID を発行するためのイニシャルコスト及び維持のためのランニングコストが大きな負担となり得ることが明らかとなった。
- BYOD については、積極的に利用を許可している事業者はいなかったが、業務用の記録用端末を忘れた際等、イレギュラー時に事実上 BYOD となっているケースがあり、その際にどのような運用であれば利用してよいのかという運用管理が十分に検討されていないまま、利用されている様子が見受けられた。例外運用も含めて、運用管理規定を定める必要があるということを認知してもらうための施策が必要であるように思われた。
- 閉域網を利用した請求が前提となった場合にあり得る運用上の課題については、イメージが難しい事業者がほとんどであったが、コスト面についてはイニシャルコストだけでなくランニングコストも含めて支援が必要であるという意見があった。病院でオンライン資格確認等システム導入の経験を持つ医療法人では、当初は導入支援事業者に積極的に対応してもらえず苦労したとのことで、介護ソフトベンダも含め、一つのパッケージとして国主導で対応窓口を設ける等の対策が必要ではないかとの意見が見られた。

第 4 章　調査まとめ

本事業では、安全管理措置について先行している医療分野の法令やガイドラインの整理を行い、介護分野との比較をベースとした調査・分析を行うことで、介護分野において安全管理措置を推進するうえでの課題を抽出した。また、介護現場における安全管理措置について、情報システムのサービス提供を担う介護ソフトベンダ側、及び、実際に介護情報の取扱いや情報システムの利用を行う介護施設・事業所側に対するヒアリングを通じて、実態把握及び整理を行った。

本章では、介護情報基盤を介して電子的に介護情報や医療情報を共有する場合の介護事業所が満たすべきセキュリティ要件の整理と、その実現に向けた課題の整理を行った。

○　医療現場と介護現場との比較

- 第 2 章の調査結果のとおり、医療分野では、介護分野と比較して ICT 導入、デジタル化の対応が進み、併せてセキュリティ対策の重要性についても認識が広まりつつあり、法令に基づくセキュリティ要件や、法令に基づく立入検査が規定されている。また、厚生労働省医政局の特定医薬品開発支援・医療情報担当参事官室により、医療機関向けサイバーセキュリティ対策研修が開始され、厚生労働省委託事業「医療情報セキュリティ研修及びサイバーセキュリティインシデント発生時初期対応支援・調査事業」により、「医療機関向けセキュリティ教育支援ポータルサイト」（MIST）が開設されるなど、セキュリティ教育も事業化されている。さらに、内閣サイバーセキュリティセンター（NISC）により医療分野は重要インフラとして指定され、日常診療業務における接続不良等のネットワーク関連のトラブルに対するアドバイスや、不正アクセスや情報漏えい等の高度な専門性を要する重大なトラブルに対して、より専門的な観点でのアドバイスを実施するとともに、会員からの要望に応じて専門事業者（フォレンジック事業者、弁護士）を紹介するといったサービスが提供されている。
- こうした前提を基に、医療分野ではオンライン資格確認やオンライン請求の原則義務化が進められていると考えられることから、介護分野でも同様の対応を推進する場合には、同様の制度や支援の検討を進める必要があると考えられる。

○　介護現場のセキュリティ対策における課題

- 介護現場におけるセキュリティ対策の実態と課題について、「医療情報システムの安全管理に関するガイドライン」で示されている経営管理/企画管理及びシステム運用の側面から、下表のとおり整理を行った。

図表 32 介護現場のセキュリティ対策の実態と課題

項目		実態	課題		
分類	内容		イニシャルコスト	ランニングコスト	業務負担
経営管理/企画管理面	個人情報管理やセキュリティ対策に関する職員への定期的な教育	プライバシー保護の取り組みに関する研修の一環として実施されていた	-	外部委託する場合は費用が発生	教育に一定の時間を要する
	組織的な対応のために必要な体制の整備	小規模事業者ではIT部署の設置や管理者の配置ができていない状況であった	採用コスト	人件費	社会全体でIT人材が不足しており、コストだけでなく様々なキャンペーンを行う等の負担が生じる可能性がある
	リスク評価に基づく安全管理方針に従った適切な安全管理対策の設計とその具体的対応を示した文書（運用管理規定等）の整備	例外的にBYODを認めているケースが見受けられたが、具体的にどのような場合に認めるかや認める際の対応方針について参照可能な運用管理規定を整備できていない状況であった	-	-	経営層があり得る運用をすべて含めて運用管理規定を定める必要がある
運用面	個人情報が保存されている機器のワイヤー固定又は施錠管理	施錠管理は行われていたが、一部の事業者では利用者が立ち入り可能な区画にてワイヤー固定等をせずに管理していた	・事務室は通常、施錠可能 ・ワイヤー	-	個人情報の保存端末を施錠可能な事務室等に移動させ、日々の記録を行う必要がある
	IDやパスワードの第三者からの秘匿	端末に付箋で貼るといった対応をしている事業者はなかった	-	-	個人情報を取り扱う職員が記憶する等の運用方針を定める必要がある
	職員ごとに固有のIDを発行	PCを用いた作業が一定以上発生すると考えられるサービス（ケアマネジャー等）では1人1IDの運用が比較的行われていたが、1日の間での利用時間が短いことや発行ID数に比例するライセンスコストを理由に共用している事業者も見られた	ID発行数に応じてライセンス費用が発生するソフトもある（多数の職員が各自僅かな時間だけ利用するシーンでは大きな負担）	サブスクリプションかつID発行数に比例する場合、継続的な負担となる	多数の職員が各自僅かな時間だけ利用するシーンではまたログイン・ログアウトの手間の負担が生じる
	個人情報の保存されている場所への立ち入る可能性のある来訪者の入退情報の記録	あまり来訪者はない、というケースが多かった。正規の職員と嘱託の職員とで管理を区別しており、嘱託の職員については入退の管理を行っている、というケースがあった	-	-	記録する来訪者が多いと負担になるため、施錠管理と合わせて検討する必要がある
	個人情報が保存されている機器等の持ち出し記録管理	ほとんどの事業者ではクラウド型の介護ソフトを利用しており、端末には個人情報は保存されていない状態であり、かつMDMを導入している事業者も一定数存在したが、例外的に写真を撮影するケース等があり、その場合に特別な管理をしているということはなかった	MDMを導入する場合は通常必要	MDMを導入する場合は必要	訪問サービスでのタブレット端末など持ち出しが多い場合、MDMの導入等とセットで検討する必要がある
	BYOD	利用者の家屋等の撮影に用いて業務用端末に転送しているケースがあり、そのような利用にあたっての運用管理規定は作成されていなかった	MDMを導入する場合は通常必要	MDMを導入する場合は必要	運用管理規定に明記し、運用管理規定に沿った運用を行う必要がある（MDMを利用する場合、MDMにおける対応も含める必要がある）

- 介護分野では事業所の管理者が医療情報システムの安全管理の担当者を兼任しているケースが多いが、このように経営管理と企画管理を分離できない状況であることも一つの課題となっている。課題の原因としては、安全管理に専従する人員を抱える経営上の余力がないことや、社会全体で IT 人材が不足しており採用コストも含めて高騰していることが挙げられる。必要な人材像としても、リーダーシップがあり、IT リテラシーを含めた教育ができ、さらに介護現場とベンダの橋渡し役も担う必要がある等、高いスキルが求められる。ヒアリングでは、経営が厳しくなった場合、セキュリティ対策関連の予算は最も削られやすい領域の一つであるという意見もあり、経済的支援も含め、介護現場に IT 人材を呼び込むための様々な施策が必要になると考えられる。
- 運用面では、大規模な法人であっても課題となり得るものとして、職員ごとに固有の ID を発行することが難しいケースが挙げられる。介護ソフトのライセンス費用が ID 数に比例する場合、大規模な法人では職員数も多くなる分、費用負担のスケールも大きくなることが要因である。全国医療情報プラットフォームによる自事業所や自法人以外の情報も共有され得ることも踏まえ、「いつ」「誰が」「何の情報を」「どのように操作したのか」を追跡できるような仕組みを必須とするに当たり、介護ソフトベンダも含めた 1 人 1ID を実現のための支援が必要であると考えられる。

- また、1 人 1ID について、費用面の支援ができない場合や、共有端末の場合の運用上の負担（共有端末を利用する職員が入れ替わるたびに、毎回ログイン・ログアウトを繰り返す必要がある等）が大きい場合には、実施可能なセキュリティの仕組みの代替案についても検討し介護事業者に示す必要があると考えられる。
- BYOD については、少ないものの例外運用が一部存在していたが、その運用が BYOD にあたり、特にリスクを伴うものであるという認識がやや希薄であることが課題として考えられる。具体的に例を示しつつ、例外運用も含めて運用管理規定を定める必要があるといったことを周知する必要があると考えられる。
- BYOD と関連し、利用者の自宅の家屋や手すり・段差等の写真を撮影するケースがあり、これらについては私有端末を使うことがある、といった回答もあったことから、どのような情報が機微であり取扱いに配慮すべき情報であるのかについても、医療分野とは別に、介護分野特有の機微な情報として整理する必要があると考えられる。
- 個人端末の利用には、介護ソフト以外のコミュニケーションアプリを用いるケースもあると考えられる。利用者に関する情報についてはコミュニケーションアプリ上で送信しないようにする等の運用も合わせて、運用管理規定をどのように定めるかを各事業者において検討する必要がある。
- 2 要素認証をはじめ、今後は介護分野でも医療分野と同等のセキュリティ対策が求められていくものと予想される。費用面の支援に加え、ID・PW の個別設定やバックアップ設定、サイバー保険加入等、介護職員に向けた IT リテラシー教育及び管理者に向けた分かりやすい手引書を準備するといった支援が必要になると考えられる。今回のヒアリング調査では、ITリテラシーが高い事業者も少なからず存在していた。こうした事業者を中心に先進事例・好事例を収集し、支援を要する事業者に向けた手引書を整備していくことが求められている。

参考資料　ヒアリングシート

ステップ1　ヒアリングシート（IT 関連の部署の方向け）

介護情報の安全管理に関する調査研究事業【ヒアリングシート】
（IT 関連の部署の方向け）

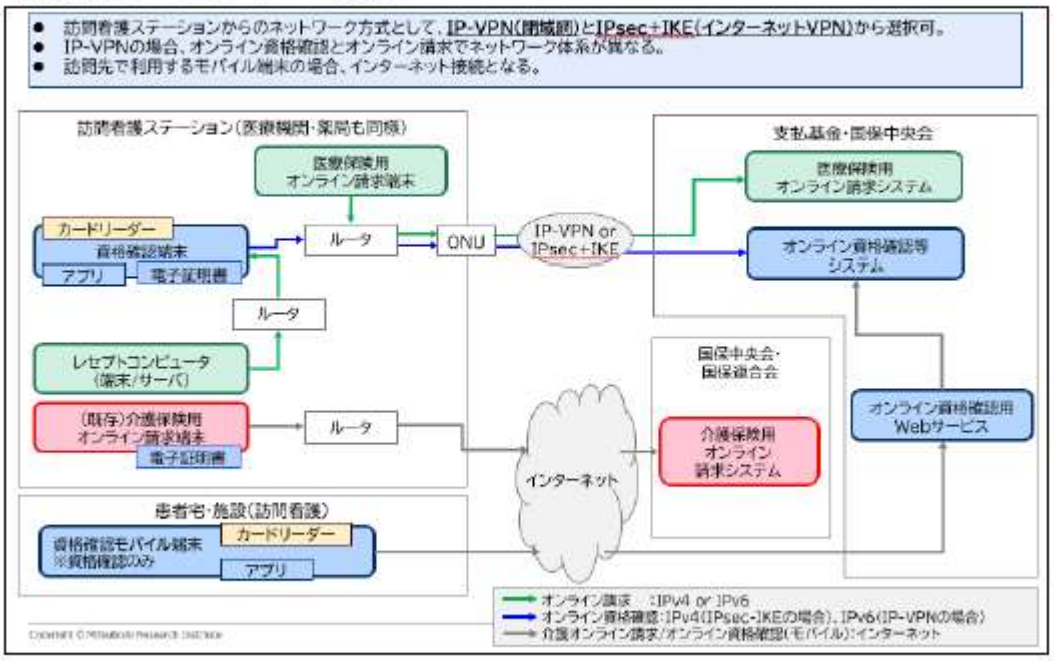
ヒアリング概要	
ヒアリング日時	
ヒアリング場所	
ヒアリング参加者	

1.現状のセキュリティ対策について
1-1）貴法人内の介護施設・事業所で利用している、介護ソフトの提供形態（クラウド（SaaS、PaaS、IaaS）、オンプレミス、スタンドアロン等）をお聞かせください。記録と請求でソフトが異なる場合等、複数利用している場合には、それぞれの提供形態をお聞かせください。
※以下、提供形態が複数ある場合にはそれぞれについてご回答ください。
1-2）サービスへのアクセス管理・認証方法（ID・パスワード、IP アドレス制限、入退室管理、2 段階認証、2 要素認証※、USB ドングルの使用有無等）について、現状と今後の予定についてお聞かせください。 ※「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、令和 9 年度時点で稼働していることが想定される医療情報システムを、今後、導入又は更新する場合、原則として二要素認証を採用することが求められています。
1-3）アクセスの管理・認証方法に関し、職員単位/職種単位/事業所単位/といった単位の設定や、単位別に閲覧可能な情報が設定・管理・コントロールの設定が可能かどうか、実際に設定しているかどうか等についてお聞かせください。
1-4）職員による操作ログの取得が可能かどうか、実際に取得しているかどうか、及びそのログの粒度（いつ、誰が、どの利用者の、どの項目を、どのように操作したか（印刷・データ出力含む）等）についてお聞かせください。

1-5)情報システムの利用に際し、職員(情報システムの利用者)に対して、情報の安全管理上求めている事項/推奨している事項(ID・パスワードの厳重な管理やバックアップ、USB メモリの利用可否やネットワーク共有の可否等)についてお聞かせください。
1-6)上記に関連して、情報の安全管理に関する教育・研修の実施や問合せ対応等についてお聞かせください。問合せ対応については、よくある問合せ内容についてもお聞かせください。
1-7)上記に関連して、IT 部署として求める安全管理事項と、介護現場で実際に実施できている内容にギャップがあればお聞かせください。また、そのギャップの原因と考えられるもの(コスト/教育等)があれば合わせてお聞かせください。
1-8)提供する情報システムが取扱う個人情報や要配慮情報に対する安全管理措置について、 ①第三者機関による認定・認証を取得しているものがあればお聞かせください。 ②通信の監視や点検等の運用状況、およびその結果について現場へのフィードバックの状況をお聞かせください。
【① 第三者機関による認定・認証の取得】
【② 通信の監視や点検等の運用状況、およびその結果について現場へのフィードバックの状況】

2. 医療機関・介護事業所間の情報共有・連携を想定したセキュアなネットワーク構成・接続方法について
2-1)訪問看護レセプト(医療保険請求分)のオンライン請求では、専用の端末及び回線を用いる方式が採用されています(下図参照)。将来的に介護領域でも同様の対応が必要となった場合、現行の方式から移行する際にどのような対応が必要と想定されるかをお聞かせください。 想定される対応事項として、IT 部門としての事項に加え、介護ソフトベンダや介護現場(情報システムの利用者)において対応が必要と考えられる事項をお聞かせください。 これらの実施事項について、介護事業者や介護ソフトベンダに対して必要と考えられる支援についてお聞かせください。
【IT 部門として実施しなければならないと想定される事項】
【介護ソフトベンダが実施しなければならないと想定される事項】
【介護現場において実施しなければならないと想定される事項】
【移行にあたり必要と考えられる支援】
2-2)介護情報も医療情報と同等の扱いが求められるようになった場合、必要な対応/必要な支援

（図：訪問看護におけるネットワーク方式）



その他
その他、介護情報の安全管理に関するご意見等があればお聞かせください。
【その他、介護情報の安全管理に関するご意見等】

以上

ステップ1ヒアリングシート（介護ソフトベンダ向け）

介護情報の安全管理に関する調査研究事業【ヒアリングシート】
（介護ソフトベンダ向け）

ヒアリング概要	
ヒアリング日時	
ヒアリング場所	
ヒアリング参加者	

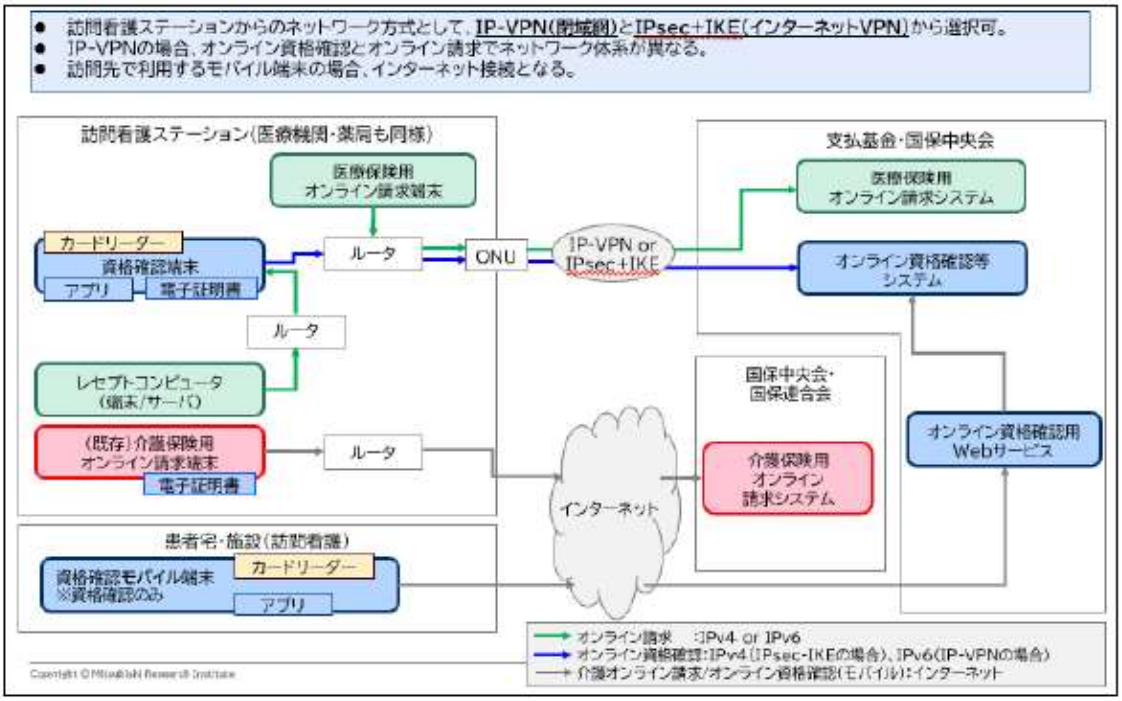
1.現状のセキュリティ対策について
1-1)サービスの提供形態（クラウド（SaaS、PaaS、IaaS）、オンプレミス、スタンドアロン等）について、提供しているものをすべてお聞かせください。
※以下、提供形態が複数ある場合にはそれぞれについてご回答ください。
1-2)介護事業者によるサービスへのアクセス管理・認証方法（ID・パスワード、IP アドレス制限、入退室管理、2 段階認証、2 要素認証※、USB ドングルの使用有無等）について、今後の対応予定も含めてお聞かせください。 ※「医療情報システムの安全管理に関するガイドライン 第 6.0 版」において、令和 9 年度時点で稼働していることが想定される医療情報システムを、今後、導入又は更新する場合、原則として二要素認証を採用することが求められています。
1-3)介護事業者内の複数のユーザーによるアクセスの管理・認証方法（職員単位/職種単位/事業所単位/といった単位（任意の単位含む）の設定や、単位別に閲覧可能な情報が設定・管理・コントロール可能かどうか等）についてお聞かせください。
1-4)介護事業者内のユーザーによる操作ログの取得が可能かどうか、実際に取得しているかどうか、及びそのログの粒度（いつ、誰が、どの利用者の、どの項目を、どのように操作したか（印刷・データ出力含む）等）についてお聞かせください。
1-4)情報システムの利用に際し、安全管理に関して求めている事項/推奨している事項（ID・パスワードの厳重な管理やバックアップ、USB メモリの利用可否やネットワーク共有の可否等）についてお聞かせください。

介護事業者への直接販売の場合は介護事業者への事項、販売代理店を経由する場合は販売代理店への事項として、それぞれご回答をお願いします。
【介護事業者に求める事項】 【介護事業者に推奨する事項】
【販売代理店に求める事項】 【販売代理店に推奨する事項】
1-5)上記に関連して、介護事業者に対する安全管理に関する支援(教育の実施や問合せ対応等)を行っていたらお聞かせください。問合せ対応については、問合せ内容と頻度についてもお聞かせください。
1-6)上記に関連して、介護ソフトベンダとして求める安全管理事項と、事業所側で実際に実施できている内容にギャップがあればお聞かせください。また、そのギャップの原因と考えられるもの(コスト/教育等)があれば合わせてお聞かせください。
1-7)提供する情報システムが取扱う個人情報や要配慮情報に対する安全管理措置について、 ①導入時に介護事業者から安全管理上の要件や第三者機関による認定・認証の取得の有無の確認を求められることがあればお聞かせください。 ②導入後に介護事業者から運用状況や点検結果について定期的な報告を求められることがあればお聞かせください。 ③OS やミドルウェア等において脆弱性が発見された場合や、マルウェアによる事件が発生した場合に、介護事業者からどの程度問合せがあるかについてお聞かせください。
【①導入時の安全管理上の要件等の確認】
【②導入後の定期的な報告】
【③脆弱性の発見やマルウェアによる事件発生時の問合せ状況】

1-8)事前にご回答をご依頼した別添「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」チェックリストについてお伺いします。「いいえ」または「対象外」と回答した事項について、その理由等をお聞かせください。また、当該項目について、今後対応を求められた場合、必要な支援等についてもしあればお聞かせください。
【いいえ の項目】
【対象外 の項目】

2. 医療機関・介護事業所間の情報共有・連携を想定したセキュアなネットワーク構成・接続方法について
2-1)訪問看護レセプト(医療保険請求分)のオンライン請求では、専用の端末及び回線を用いる方式が採用されています(下図参照)。将来的に介護領域でも同様の対応が必要となった場合、現行の方式から移行する際にどのような対応が必要と想定されるかをお聞かせください。 また、介護ソフトベンダではなく、介護事業者における実施が不可欠と考えられる事項をお聞かせください。 これらの実施事項について、介護事業者や介護ソフトベンダに対して必要と考えられる支援についてお聞かせください。
【介護ソフトベンダが実施しなければならないと想定される事項】
【介護事業者が実施しなければならない(介護ソフトベンダでは実施できない)と想定される事項】
【移行にあたり必要と考えられる支援】
2-2)介護情報も医療情報と同等の扱いが求められるようになった場合、必要な対応/必要な支援

（図：訪問看護におけるネットワーク方式）



その他
その他、介護情報の安全管理に関するご意見等があればお聞かせください。
【その他、介護情報の安全管理に関するご意見等】

以上

ステップ2ヒアリングシート

介護情報の安全管理に関する調査研究事業【ヒアリングシート】
（事業所・施設の担当者の方向け）

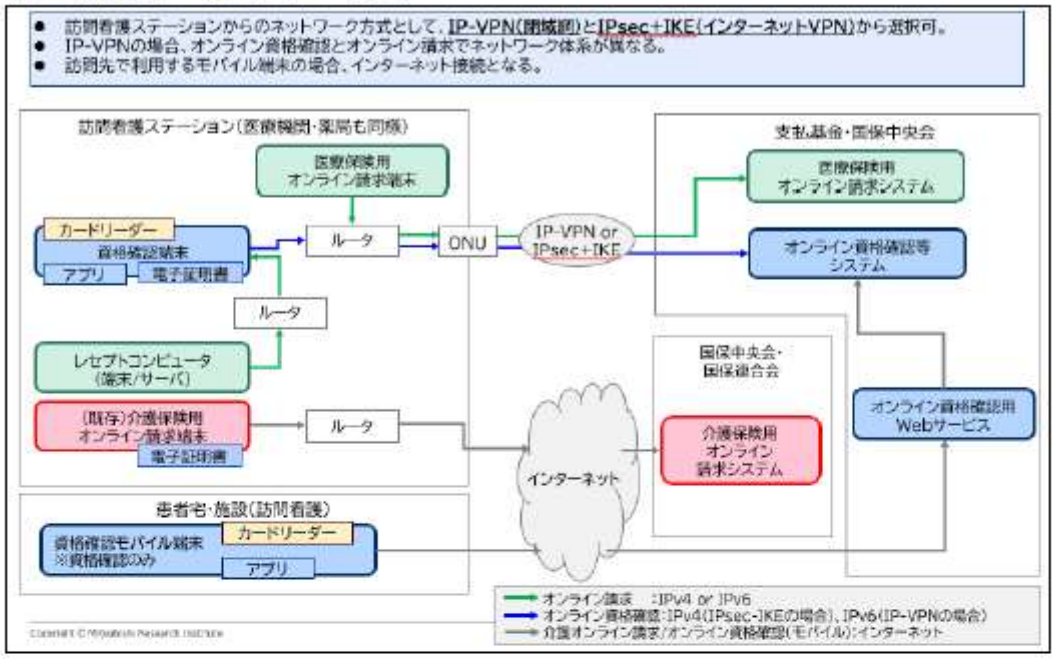
ヒアリング概要	
ヒアリング日時	
ヒアリング場所	
ヒアリング参加者	

1.情報システムの利用・管理について
1-1)情報システム・IT に関する部署・担当者を配置しているかどうかを教えてください。 配置している場合、担当者の専従・兼任状況や経験年数等を教えてください。 ※法人として複数の施設・事業所を運営している場合、法人の規模や提供サービスを教えてください。
1-2)介護情報を記録・請求するにあたり、情報システム・IT をどのように利用しているかを教えてください。 記録：紙、介護ソフトでない汎用ソフト（ワード、エクセル等）、介護ソフト 等 請求：紙、CDR、介護伝送ソフト（中央会）、介護ソフトの請求機能、代理請求（法人本部への送信） 等
2. 電子化された利用者に関する情報を入力・閲覧する端末の管理について
2-1)端末の台数は、情報を利用する職員の数に対してどの程度あるか教えてください。
2-2)端末は、どのように管理されていますか。（ワイヤーロックされている、各自で持ち歩く、紛失時に備えた位置情報の取得、デジタル証明書のインストール、端末管理システム（MDM）の導入等）
2-3)端末内への情報のアクセスはどのように制限していますか。（ID・パスワード等）
2-4)端末は、どのようなネットワークに接続できますか。（インターネット、社内ネットワーク、事業所内ネットワーク等）
2-5)職員の業務に応じて必要な情報を整理・分類し、閲覧・編集制限を掛けることはありますか。

2-6)個人情報や医療情報の取扱に関して職員向けの資料等を作成・周知していますか。 また、その内容を定期的に教育したり、周知したりしていますか。その方法(E-learning の実施、会議でのアナウンス、目に見える場所での掲示等)も合わせて教えてください。
2-7)職員個人の私有端末を、業務利用することはありますか。 もしある場合、端末の種類(スマホ、タブレット、PC 等)や、業務利用の仕方を教えてください。 例 1:自分のスマホからメールや LINE、チャットアプリを使って、被保険者の情報を送ることがある。 例 2:訪問先で私有のタブレット端末を用いてケアの記録を行い、事業所に戻って業務用 PC に転記している。 例 3:私有のノート PC に介護ソフトをインストールし、介護の記録や請求に使っている。 また、業務利用している場合には、運用管理規定の定めの有無、運用管理規定の内容についてお聞かせください。
2-8)端末に保存されている情報のバックアップは行っていますか。その方法や頻度等を教えてください。

3. 医療機関・介護事業所間の情報共有・連携を想定したセキュアなネットワーク構成・接続方法について
3-1)訪問看護レセプト(医療保険請求分)のオンライン請求では、専用の端末及び回線を用いる方式が採用されています(図 1 参照)。将来的に介護領域でも同様の対応が必要となった場合についての想定について、お伺いします。
現在の業務がどのように変更されると想定されるか、教えてください。
上記で想定される変更を実施するにあたり、課題となり得る事項を教えてください。
上記の課題に対し、必要と考えられる支援(国や自治体、介護ソフトベンダ等による支援)があれば教えてください。

（図 1:訪問看護におけるネットワーク方式）



その他
その他、介護情報の安全管理に関するご意見等があればお聞かせください。
【その他、介護情報の安全管理に関するご意見等】

以上

令和5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分）
介護情報の安全管理に関する調査研究事業報告書

令和 6（2024）年 3 月発行
発行　株式会社三菱総合研究所
ヘルスケア&ウェルネス事業本部
〒100-8141　東京都千代田区永田町 2-10-3
TEL　03（6858）0393　FAX　03（5157）2143