資格確認限定型レセコン連携機能
に関するシステムベンダ向け技術解説書

令和６年８月
厚生労働省保険局

改　訂　履　歴

版数	改訂年月日	該当箇所	内容
１．０	令和６年７月２日	初版	初版作成
１．１	令和６年８月９日	図１．３ 図１．４．１-１ 図１．４．１-２ 図１．５ 図１．６-２ 表１．４．２	名称変更 「資格確認限定型用 Web サービス」を「マイナ資格確認アプリ用 Web サービス」に変更
		表１．４．２	「医療機関等コード」の追記
		１．４．３ 図１．４．１-２ 図１．４．２ 図３．２．２	名称修正　「機関コード」を「医療機関等コード」に変更
		１．３ 図１．４．１-２ 表１．４．２ ３．２	名称修正 「ユーザ ID」/「ID」を「ログイン ID」に変更

※　版数は新規制定を第１．０版とし、改訂が発生した際は第１．１版と版数を上げる。

目次

資格確認限定型レセコン連携機能 に関するシステムベンダ向け技術解説書..... 1
１．　はじめに..... 2
１．１　本書の趣旨 2
１．２　技術解説書の構成と使い方 3
１．３　資格確認限定型の概要 5
１．４　レセプトコンピュータの既存システム改修 7
１．４．１ 資格確認限定型レセコン連携機能の概要 7
１．４．２ 改修内容 8
１．４．３ 照会番号の登録機能 9
１．４．４ レセコンシステムベンダ向け接続テスト 10
１．４．５ 共通補足 10
１．５　ネットワーク環境 11
１．６　セキュリティ対策 12
１．６．１ オンライン資格確認等システムにおけるセキュリティ対策 13
１．６．２ 各施設におけるセキュリティ対策 14
２．　作業の全体像..... 15
３．　導入作業..... 16
３．１　利用申請 16
３．２　認証方法の設定 17
３．３　パッケージソフトの適用 19
３．４　オンライン資格確認等を利用した運用に向けた準備 19
３．４．１ 業務フローの見直し 19
３．４．２ ルール等の見直し 19
３．５　運用テスト 20
４．　その他..... 21
４．１　医療情報システムの安全管理に関するガイドラインの準拠 21
４．２　施術所内のセキュリティ対策の見直し 21
４．３　資格確認限定型レセコン連携機能の導入に伴う問合せ先 21

１．　はじめに

１．１ 本書の趣旨

本書は、オンライン資格確認等システムが提供する「資格確認限定型レセコン連携機能」及び当機能を導入する施設のシステムベンダに実装いただきたい内容等について記載しています。

マイナンバーカードを用いた資格確認については、令和６年４月に運用開始した資格確認限定型のオンライン資格確認で行うことができますが、資格確認限定型レセコン連携機能は、その資格確認した結果をレセプトコンピュータ等に連携するための機能になります。当機能の導入は、各施設にとって必須ではありませんが、利用するにあたってはシステムベンダにおいて、システム改修等を行う必要があります。

資格確認限定型レセコン連携機能の概要を以下に記載します。

表１．１　資格確認限定型レセコン連携機能の概要

運用開始時期	令和６年 12 月目途
対象施設	オンライン資格確認の資格確認限定型を導入する施設（任意）
提供サービス	資格確認限定型を導入する施設が、マイナ資格確認アプリを用いてマイナンバーカードで資格確認した結果を、オンライン資格確認等システムからレセプトコンピュータ等へオンラインで連携する。

本書の内容は、令和６年６月までの整理結果に基づいてシステムベンダにおける準備事項をまとめたものです。

１．２ 技術解説書の構成と使い方

本書の構成は、以下のとおりです。必要に応じて詳細内容は別添で示します。

表１．２-１　本書の構成及び概要

分類	概要	
本書	資格確認限定型を導入する施設が既存のレセコン等システムとオンライン資格確認等システムと接続し資格確認結果を取得する機能、既存システムの改修すべき内容、想定される導入作業等を記載し、システムベンダが準備作業内容を把握するための情報とする。	
別紙	１．オンライン資格確認等に係る業務フロー	資格確認限定型レセコン連携機能を行う際の各施設の業務フローを記載。
関連	資格確認限定型レセコン連携機能に関するシステムベンダ向け外部インターフェイス仕様書	オンライン資格確認等システムが外部システムと連携して行う業務を実現するためのインターフェイス仕様（資格確認限定型レセコン連携機能)、提供機能範囲等を記載。
	システムベンダ向け接続テスト計画書	オンライン資格確認等システム接続に向けたシステム改修に先駆けて実施する接続テストの内容やテスト環境の詳細を記載。

表１．２-２　用語の定義

用語	内容
資格確認限定型	オンライン資格確認において、患者の資格情報のみを取得できる簡素な資格確認の仕組み。専用のアプリ（マイナ資格確認アプリ）を、パソコンやスマートフォン、タブレットにインストールし、マイナンバーカードを読み取ってオンライン資格確認を行うことができる。
マイナ資格確認アプリ	患者のマイナンバーカードで認証を行い、患者の資格情報を確認できるアプリケーション。
施術所等向け総合ポータルサイト	受領委任契約を締結している柔道整復師・あん摩マッサージ指圧師・はり師・きゅう師の施術所、健診実施機関等（保険医療機関（歯科）、保険薬局、保険医療機関以外の施設、保険者）又は助産所がオンライン資格確認の利用に係る申請や問合せを行うことができるポータルサイト。
資格情報	加入者情報のうち、当該加入者の加入資格、受給資格に関する項目（保険者番号、個人単位被保険者番号、資格取得日、資格喪失日等）。
マイナンバーカード	氏名、住所、生年月日、個人番号、その者の写真、その他その者を識別する事項のうち政令で定める事項が記載されたカード。IC チップに JPKI 認証局が発行する署名用電子証明書と利用者証明用電子証明書が格納される。
利用者証明用電子証明書	インターネットを閲覧する際などに、利用者本人であることを証明するための電子証明書。マイナポータルのログイン等、本人であることの認証手段として利用するもの。
汎用カードリーダー	公的個人認証サービスに対応した IC カードリーダー。
PIN	「Personal Identification Number」 個人を識別する番号（暗証番号）。
PIN 認証	暗証番号入力を求める認証。利用者証明用電子証明書を利用するに当たり４桁の暗証番号が必要。
PIN なし認証	暗証番号入力を求めない認証。マイナンバーカードでのオンライン資格確認等では、暗証番号を入力しないでカードをかざすだけで利用者証明用電子証明書の読み取りを行う「PIN なし認証」を可能としている。
MFA	「Multi Factor Authentication」 本人確認の手段として、性質の異なる複数の要素を組み合わせて認証を行うこと（多要素認証）。
Authenticator	認証用のワンタイムパスコードを生成するアプリケーション。
JWT	「JSON Web Token」 JSON 形式で表現された認証情報などを安全に送受信できるよう符号化やデジタル署名の仕組みを規定した標準規格。
個人単位被保険者番号	被保険者証記号・番号(世帯単位)に２桁の枝番がついた番号。
照会番号	レセプトコンピュータ等で管理されている、患者を特定する任意の番号。

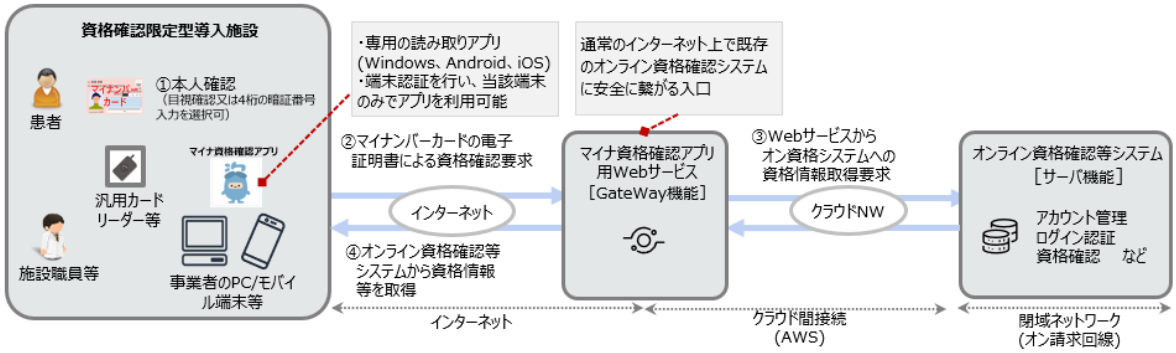
１．３ 資格確認限定型の概要

資格確認限定型のオンライン資格確認とは、専用の読み取りアプリであるマイナ資格確認アプリをインストールしたモバイル端末等で患者のマイナンバーカードを読み取り、通常のインターネットから Web サービスを経由して、オンライン資格確認等システムに接続し、患者の資格情報を取得する仕組みとなります。

利用にあたっては、施術所等向け総合ポータルサイトへの利用申請と、マイナ資格確認アプリのインストール、インターネット回線の用意等が必要となります。

資格確認限定型レセコン連携機能は、マイナ資格確認アプリで資格確認した結果について、API によりレセコンへ連携する機能であるため、導入するためには資格確認限定型のオンライン資格確認を導入している必要があります。

図１．３　資格確認限定型の仕組み（概要）



読み取り端末（スマートフォン・タブレット・PC 端末）

資格確認を行うための端末として、マイナンバーカードを読み取るための端末の導入が必要となります。スマートフォンの場合は、マイナンバーカードの読み取りに対応した機種、PC・タブレットの場合は、マイナンバーカードの読み取りに対応した汎用カードリーダーが必要となります。

※利用可能な端末・機種については施術所等向け総合ポータルサイト等をご参照ください。

マイナ資格確認アプリ

マイナ資格確認アプリは、資格確認を行う施設向けに提供されるアプリケーションになります。アプリストアからインストールし、利用申請時に発行されるログイン ID・パスワード・アクティベーションコードで、端末認証・ログインすることで使用可能となります。

表１．３　マイナ資格確認アプリの主な機能

機能	概要
資格確認（目視） ※PIN なし認証	特定機関認証でマイナンバーカードの IC チップから利用者証明用電子証明書を取り出し、利用者証明用電子証明書の有効性を確認。利用者証明用電子証明書が有効な場合は、利用者証明用電子証明書のシリアル番号と紐づく資格情報を取得し返却する。 ※施設職員の目視による顔写真の確認を正常に終えた後に呼び出される
資格確認（PIN 認証）	暗証番号でマイナンバーカードの IC チップから利用者証明用電子証明書を取り出し、利用者証明用電子証明書の有効性を確認。利用者証明用電子証明書が有効な場合は、利用者証明用電子証明書のシリアル番号と紐づく資格情報を取得し返却する。 ※患者が入力した暗証番号を引数に呼び出される
履歴閲覧	資格確認した患者利用者の資格確認結果を事後的に閲覧する。 ※閲覧可能期間は資格確認した日の翌月末まで有効
健康保険証利用の申込（初回登録） ※今後、実装予定	特定機関認証でマイナンバーカードの IC チップ、もしくは暗証番号でマイナンバーカードの IC チップから利用者証明用電子証明書を取り出し、利用者証明用電子証明書の有効性を確認。利用者証明用電子証明書が有効な場合は、利用者証明用電子証明書のシリアル番号を利用し、健康保険証利用の申込（初回登録）を行う。処理が正常に完了した場合は、資格情報を返却する。 ※暗証番号認証の場合、患者が入力した暗証番号を引数に呼び出される想定

詳細に関しては、施術所等向け総合ポータルサイトに掲載されている手順書・マニュアル等をご参照ください。

１．４ レセプトコンピュータの既存システム改修

資格確認限定型レセコン連携機能を利用するために、施設に導入しているレセプトコンピュータ等のシステムを改修していただくことになります。

１．４．１ 資格確認限定型レセコン連携機能の概要

マイナ資格確認アプリで資格確認した患者利用者の資格確認結果情報を通常のネットワーク環境でレセプトコンピュータにダウンロードできます。

利用に関しては、マイナ資格確認アプリの利用申請とは別に、施術所等向け総合ポータルサイトにおいて利用申請を行う必要があります。また、セキュリティの観点から多要素認証（MFA）の仕組みを採用しており、各施設において、多要素認証（MFA）に関する初期設定を行っていただきます。

図１．４．１-１ 資格確認限定型レセコン連携機能の仕組み（概要）

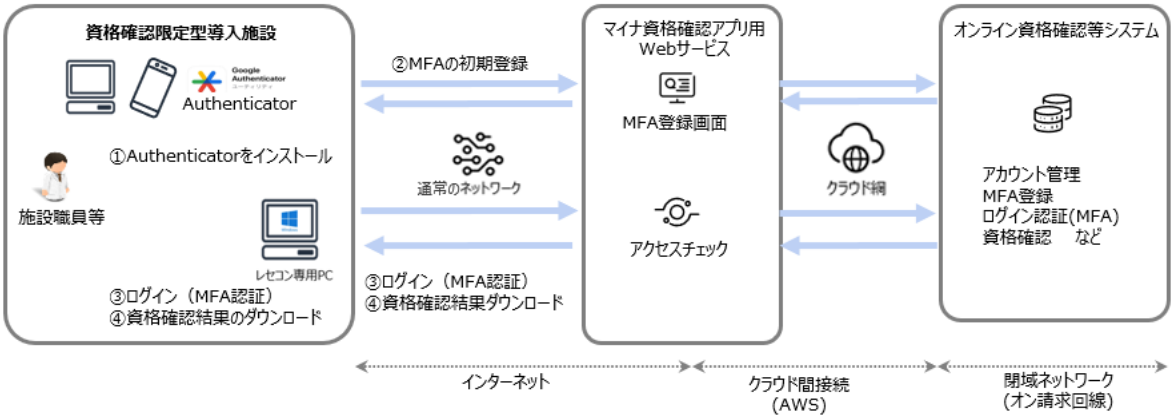
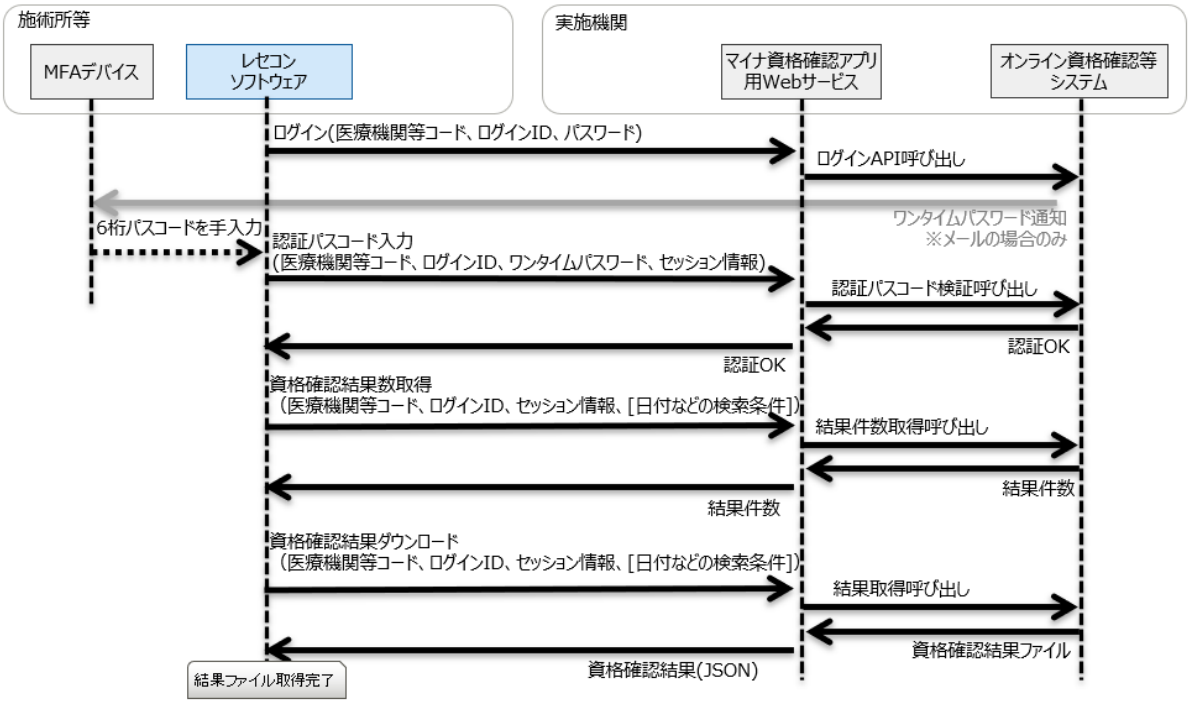


図１．４．１-２ 資格確認限定型レセコン連携機能のシーケンス図



１．４．２　改修内容

資格確認限定型レセコン連携機能を利用するために、システムベンダにて改修が必要と想定される内容を記載します。

※記載している改修内容以外の機能についても、施設のニーズを踏まえ、システムベンダにて改修の必要性をご検討ください。

表１．４．２　資格確認限定型レセコン連携機能に係る実装内容

No.	改修項目	改修内容
1	ログイン	医療機関等コード/ログイン ID/パスワードをもとに、マイナ資格確認アプリ用 Web サービスのログイン API を呼び出すこと。 ・　パスコード入力画面へ遷移する
		ログインに必要なログイン ID/パスワードを入力する画面を追加すること。
2	多要素認証（MFA） パスコード入力	多要素認証（MFA）パスコードをもとに、マイナ資格確認アプリ用 Web サービスの多要素認証（MFA）用 API を呼び出すこと。
		多要素認証（MFA）に必要なパスコードを入力する画面を追加すること。
3	トークンリフレッシュ	JWT の有効期限切れ時、ログイン ID/パスワード等をもとに、マイナ資格確認アプリ用 Web サービスのトークンリフレッシュ API を呼び出すこと。
4	資格確認結果 ダウンロード要求画面	資格確認結果ダウンロードにあたり、検索条件に対象期間等を指定する画面を追加すること。
5	資格確認結果数取得	検索条件を指定し、マイナ資格確認アプリ用 Web サービスの資格確認結果数取得 API を呼び出す。 ※取得可能期間は資格確認した日の翌月末まで
		検索条件に基づき、表示される資格確認結果数に関するポップを表示すること。
6	資格確認結果 ダウンロード	検索条件を指定し、マイナ資格確認アプリ用 Web サービスの資格確認結果ダウンロード API を呼び出す。
7	資格確認結果一覧画面	資格確認結果ダウンロードによって取得した結果情報の一覧を表示する画面を追加すること。

No.	改修項目	改修内容
8	資格確認結果（個人）画面	資格確認結果ダウンロードによって取得した結果情報の個人の資格確認結果を表示する画面を追加すること。
9	照会番号の登録機能	照会番号が空白だった場合、新規カルテを起票し、取得した資格情報等を登録・照会番号を送信すること。
		取得した資格情報等の照会番号情報でレセプトコンピュータ内の患者情報と紐付けすること。

詳細は、「資格確認限定型レセコン連携機能に関するシステムベンダ向け外部インターフェイス仕様書」として医療機関等 ONS 上で公開します。

図１．４．２　レセコンにおける画面実装イメージ

１．４．３　照会番号の登録機能

患者の加入先保険者が変更した場合、保険者番号、個人単位被保険者番号等が変わるため、施設のレセプトコンピュータで管理されている資格情報について手作業を介さずにシステムで更新するためには、紐づけのキーが必要になります。

このため、医療機関等コードと照会番号をオンライン資格確認等システムに登録し、資格確認結果と共に施設に送付することで、レセプトコンピュータで管理されている資格情報と紐付けできるようになります。

オンライン資格確認等システムでの照会番号は、50 文字が登録可能です。

１．４．４　　レセコンシステムベンダ向け接続テスト

レセコンシステムベンダ向け接続テスト要件及びテスト環境に係る詳細は、レセコンシステムベンダ向け接続テスト計画書として令和６年 10 月に医療機関等 ONS 上で公開します。

表１．４．４　接続テスト実施概要

対策	内容
スコープ	オンライン資格確認システム、レセコンシステム（各パッケージソフト）
実施期間	令和６年 11 月～
目的	レセコンシステムベンダが開発したレセコンシステム（パッケージソフト）が、資格確認限定型レセコン連携機能に関して、オンライン資格確認等システムと正常に情報連携できることを確認する。
参加機関	・実施機関 ・申し出のあったレセコンシステムベンダ
システム及び使用環境	・資格確認限定型レセコン連携機能　接続検証環境 ・レセコンシステム（パッケージソフト）
実施事項	オンライン資格確認等システムから提供されるマイナ資格確認アプリでの資格確認結果を、レセコンシステムに正常に取り込めることを確認する。
使用データ	テストデータは支払基金が用意したものを使用する。
テスト内容	資格確認限定型レセコン連携機能を対象とする。 ※詳細は別途公開予定

１．４．５　　共通補足

データ形式

資格確認結果は JSON 形式で連携されます。

文字コード

オンライン資格確認等システムから連携される情報の文字コードについて、UTF-8 を使用します。

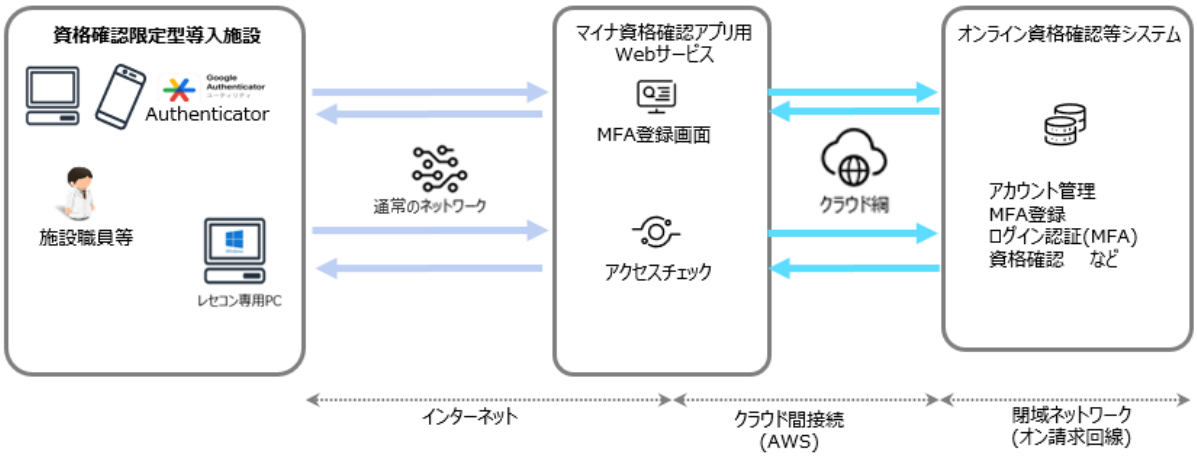
詳細は、「資格確認限定型レセコン連携機能に関するシステムベンダ向け外部インターフェイス仕様書」として医療機関等 ONS 上で公開予定。

１．５ ネットワーク環境

資格確認限定型レセコン連携機能に関して、「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版」に準拠し、セキュアなネットワーク環境を整備しています。

資格確認限定型レセコン連携機能を利用する際のネットワーク回線に関しては、公共の Wi-Fi 等安全性が確認できない回線を利用せず、通信事業者等と契約したネットワーク回線をご利用ください。

図１．５　ネットワーク連携の考え方



１．６ セキュリティ対策

資格確認限定型レセコン連携機能を利用できる端末はレセプト作成のソフトウェアを導入した PC 端末を想定しており、持ち運び等による紛失リスクを踏まえ、モバイル端末上での資格確認限定型レセコン連携機能の利用は行わないようにしてください。

オンライン資格確認等システム、ネットワーク、利用施設がセキュリティ対策を講じる上で、以下の責任分界（通信経路、情報到達）に基づいて、セキュリティ対策の範囲を整理しています。

図１．６－１　通信経路の責任分界

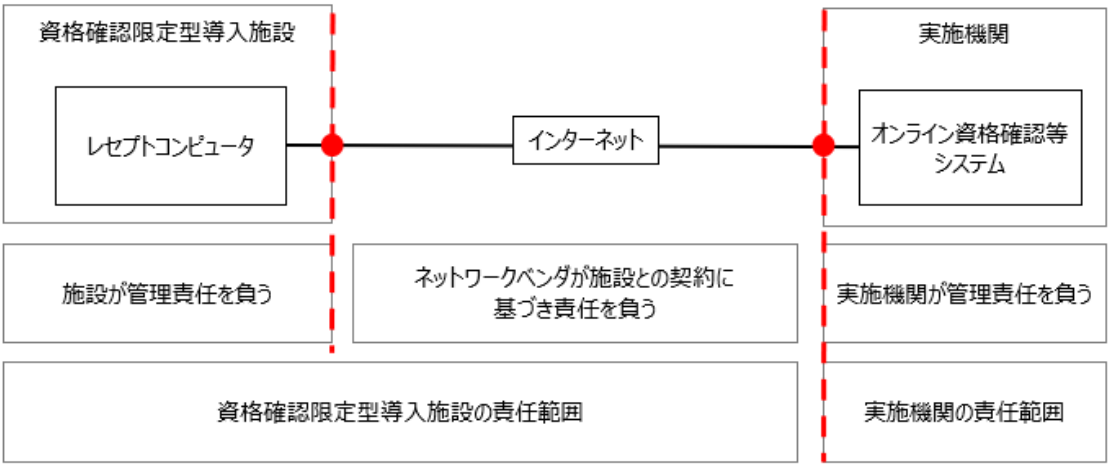
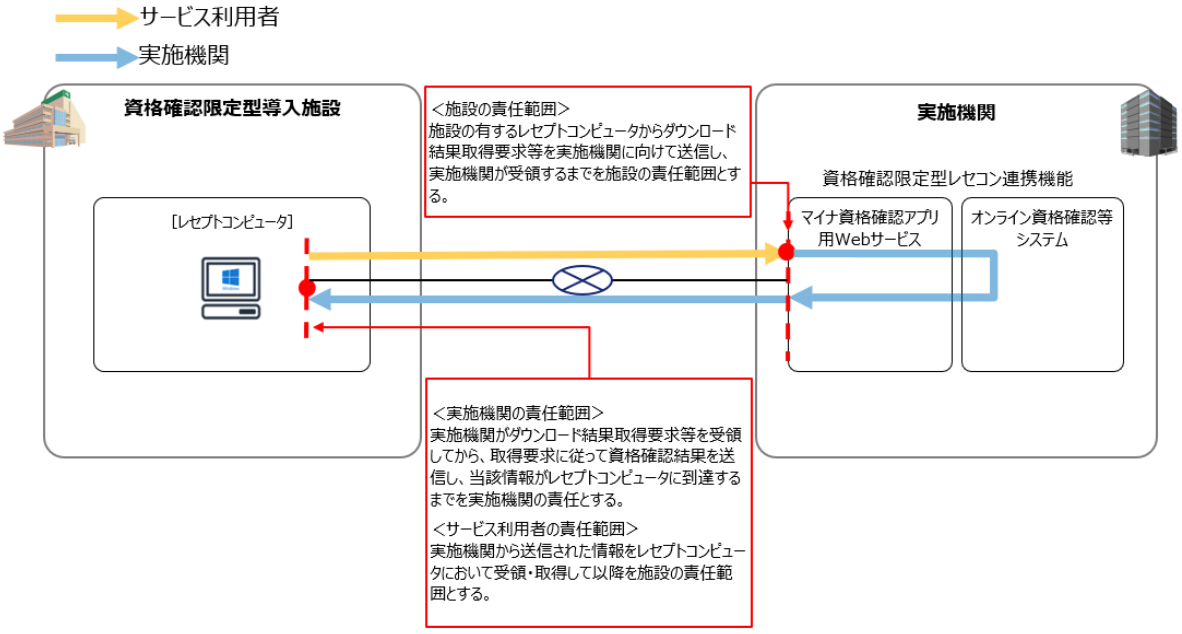


図１．６－２情報到達点の責任分界



１．６．１　オンライン資格確認等システムにおけるセキュリティ対策

オンライン資格確認等システム（サーバー側）においては、「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版」に準拠した対策を実施します。

オンライン資格確認等システムでは、以下のセキュリティ対策を講ずることとしており、ネットワークに接続した施設側に対し、ネットワークを介した不正アクセスや提供データの改ざん等が生じないように、対策を講ずることとしています。

図１．６．１　オンライン資格確認等システムにおける主なセキュリティ対策

対策	内容
アクセス・利用制限	情報資産へのアクセスを許可された者のみに限定するため、利用する主体を識別するための認証を行う。 管理者に対するアクセス制御を検討し、内部職員によるデータ漏えいを防止する仕組みを実現する。
セキュリティリスク分析・セキュリティ診断・セキュリティリスク管理	設計・開発するソフトウェアの緊急性の高いセキュリティパッチなどの適用を適宜正確かつ迅速に行う。脆弱性が生じないよう留意して設計・開発し、定期的な検査を通じた確認により修正を適用できるようにする。
マルウェア対策	アンチウイルスソフトウェア等の導入によりマルウェアへの対策を講じるための機能を備える。 外部ネットワークからのマルウェアの侵入や、万が一マルウェアに侵入された場合の外部ネットワークへの不正な通信等を監視し、侵入の検知、防止及び当該マルウェアによる通信の遮断等を行う。
データの秘匿	情報の搾取や漏えいを防止するため、保護すべき情報に対してアクセス制御を行うことに加えて、保存された情報及び情報にアクセスするための通信回線を暗号化する機能を備える。
不正アクセス・内部不正対策	ネットワーク機器及びサーバ機器への不正アクセス等による被害を極小化するため、全てのサーバ、ネットワーク機器を対象に、ネットワークおよびサーバ機器への不正アクセスの防止や万が一侵入された場合の検知・通知を行う。 正当な権限を持つ内部職員による内部不正や、外部攻撃によるセキュリティインシデントの放置を防止するため、ログ等の証跡に対し、当該事象を特定できるようにする。

対策	内容
ネットワーク対策	通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上で遮断する機能を備える。不正な通信、サービス停止攻撃等に対し通信の遮断や通信量の抑制、レピュテーション情報を活用したセキュリティ監視等により、サービス停止の脅威を軽減する機能（自動的に遮断する仕組みも含める）を備える。
Web 対策	L７レイヤーまでのセキュリティ対策（Cookie、パラメータの改ざん、URL の改ざんなどへの対応）を行う。 DDoS 攻撃を回避する仕組みを設ける。新たに発見された脅威に対し、速やかに対応する必要がある場合、WAF の導入による対策が必要。WAF を導入した場合に、WAF を経由した攻撃等にも対処を実施する。

１．６．２　各施設におけるセキュリティ対策

各施設においては、「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版」に準拠し、必要なセキュリティ対策を行っていただく必要があります。

また、モバイル端末等に関する安全管理や職員個人の所有する又は個人の管理下にある端末の業務利用（Bring Your Own Device; BYOD）に関しては、「資格確認限定型オンライン資格確認等システム　運用マニュアル」をご確認ください。

２．　作業の全体像

各施設において資格確認限定型レセコン連携機能を利用開始するためには、レセコンシステムベンダにおいて、既存システムを改修していただく必要があります。資格確認限定型レセコン連携機能の実装に向け、既存システムの改修（準備作業）の実施をお願いいたします。

令和６年 12 月からの資格確認限定型レセコン連携機能の利用開始に向けて、レセコンシステムベンダにて対応いただきたいスケジュールは以下のとおりです。

図２　資格確認限定型レセコン連携機能利用開始に向けたロードマップ

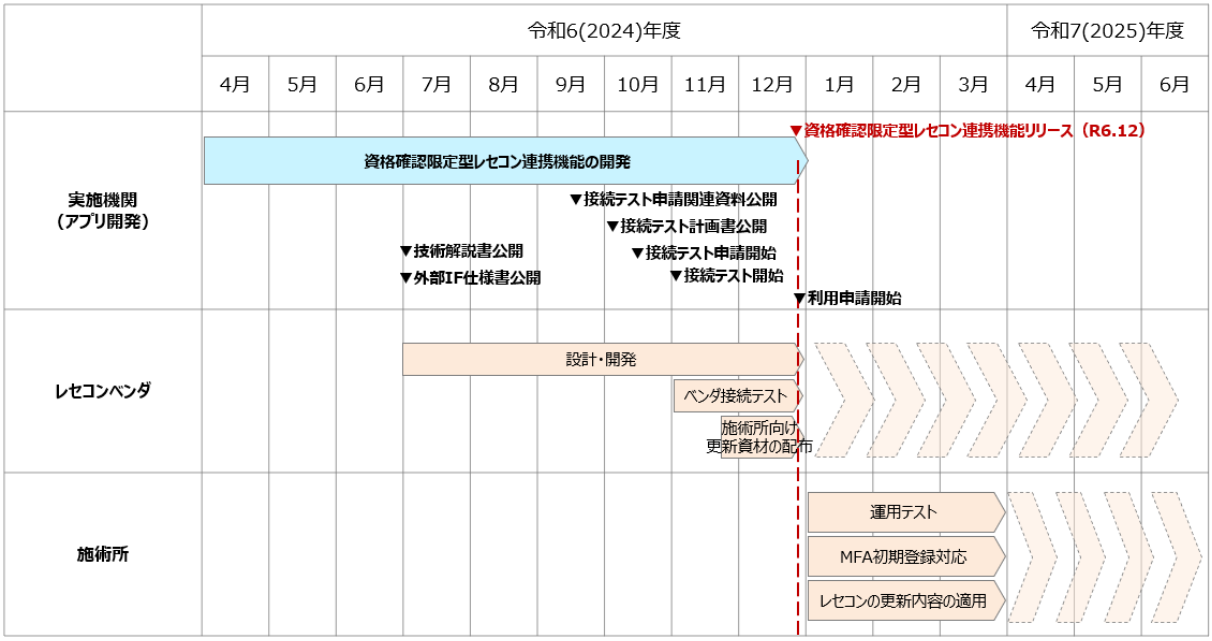


表２　主なマイルストン

	マイルストン	概要	時期
①	資格確認限定型レセコン連携機能利用開始	各施設が資格確認限定型レセコン連携機能を利用できるようになります。	令和６年 12 月
②	資格確認限定型レセコン連携機能テスト環境公開	レセコンシステムベンダにおいて、テスト環境を利用したテストを実施できるようになります。	令和６年 11 月

なお、各種情報の共有は医療機関等 ONS にて行います。

３．　導入作業

資格確認限定型レセコン連携機能を導入するに当たっては、利用申請、認証方法の設定、パッケージソフトの適用、オンライン資格確認等を利用した運用に向けた準備等を行っていただく必要があるため、導入先の施設と導入内容等を相談してください。

３．１ 利用申請

資格確認限定型レセコン連携機能を利用するためには施術所等向け総合ポータルサイトにて利用申請し、資格確認限定型レセコン連携機能専用のアカウントを取得します。（マイナ資格確認アプリのアカウントとは別に必要）※義務化対象外医療機関の場合、医療機関等向け総合ポータルサイトでの手続きになります。

URL：https://iryohokenjyoho.service-now.com/omf

図　３－１　施術所等向け総合ポータルサイト画面イメージ

表３－１　　アカウントの種類

ユーザーアカウント		概要
①	マイナ資格確認アプリ	・マイナ資格確認アプリの利用に必要 ・ポータルサイトの利用申請時に発行される“W”から始まるアカウント
②	資格確認限定型レセコン連携機能（Authenticator）	・資格確認限定型レセコン連携機能の利用に必要 ・ポータルサイトの利用申請時に発行される“WA”から始まるアカウント
③	資格確認限定型レセコン連携機能（メール）	資格確認限定型レセコン連携機能の利用において、Authenticator の利用ができない等、やむを得ない事情がある場合、使用可能な臨時アカウント（継続的な利用は不可）

３．２ 認証方法の設定

資格確認限定型レセコン連携機能を利用するに当たって、セキュリティ対策として、多要素認証（MFA）を実装しています。多要素認証（MFA）を行うためには、各施設において認証方法の設定が必要になります。

多要素認証（MFA）の認証方法の設定は、利用申請時に発行される URL から Web ブラウザ上で、登録を行っていただきます。事前に Authenticator（Google Authenticator 等）をインストールし Web ブラウザ上に表示される多要素認証のキー情報を基に、Authenticator を用いて初期設定を行います。

図３－２－１　Authenticator のダウンロードイメージ（iPhone の例）

図３－２－２　Web ブラウザにおける多要素認証（MFA）の登録画面イメージ

図　3－2－3　Authenticator の初期設定イメージ

初期設定後、Authenticator を開くたびに、ワンタイムのパスコードが表示されるようになります。レセコンにおけるログイン時において、ログイン ID・パスワードに加えて、このワンタイムのパスコードを使用し、レセコンへのログインを行います。

※多要素認証（MFA）については、原則 Authenticator を使用するため、メールアドレスによる認証はセキュリティの観点から、通常の認証方法として提供しません。ただし、Authenticator が使用不可かつ急ぎログインの必要がある場合等については、メールアドレスに届くワンタイムのパスコードを使用してログインできる臨時アカウントを提供することを想定しています。（継続・通常利用は不可）

なお、メールアドレスによる臨時の運用を行う場合、ワンタイムのパスコードを受領するメールアドレスは、各施設がポータルサイトに登録しているメールアドレスを使用することを想定しています。

３．３ パッケージソフトの適用

各施設が導入しているレセプトコンピュータのソフトウェアに資格確認限定型レセコン連携機能に係る更新を適用してください。

３．４ オンライン資格確認等を利用した運用に向けた準備

３．４．１　業務フローの見直し

資格確認限定型レセコン連携機能の利用を踏まえて、現行業務フローを必要に応じて変更することとなります。

３．４．２　ルール等の見直し

各施設において、セキュリティポリシー等の規定を、資格確認限定型レセコン連携機能の利用に伴う内容に応じて適宜更新することとなります。

３．５ 運用テスト

実際の業務フローの流れで資格確認限定型レセコン連携機能を正常に設定し、運用できるか、運用テストを実施してください。

表３．５　運用テスト実施概要

対策	内容
スコープ	多要素認証（MFA）用 Web ブラウザ、Authenticator、 レセコンシステム（各パッケージソフト）
実施期間	令和７年１月～
目的	施設において、資格確認限定型レセコン連携機能の一連の作業（利用申請・多要素認証(MFA)登録・ログイン・ダウンロード等）を実施できることを確認する。
参加機関	・資格確認限定型レセコン連携機能を利用する施設
システム及び使用環境	・マイナ資格確認アプリ ・Web ブラウザ（多要素認証（MFA）の登録 URL） ・Authenticator ・資格確認限定型レセコン連携機能　本番環境 ・レセコンシステム（パッケージソフト）
実施事項	・ポータルサイトから利用申請を行う。 ・多要素認証（MFA）の設定を行い、レセコンシステムにログインする。 ・資格確認限定型レセコン連携機能として、資格確認結果をレセコンシステムにダウンロードできることを確認する。
使用データ	本番環境でのマイナ資格確認アプリの資格確認結果を使用する。
テスト内容	資格確認限定型レセコン連携機能を対象とする。

４．　その他

４．１　医療情報システムの安全管理に関するガイドラインの準拠

資格確認限定型レセコン連携機能を導入するにあたっては、「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版」に準拠し、必要なセキュリティ対策を行っていただく必要があります。

４．２　施術所内のセキュリティ対策の見直し

各施設においては、１．６．２セキュリティ対策が行われるものと想定するため、今一度、各施設内のセキュリティ対策を広く見直すことを推奨します。

４．３　資格確認限定型レセコン連携機能の導入に伴う問合せ先

システムベンダ向け HP（医療機関等 ONS）を開設しています。当該 HP 上に令和元年 10 月よりサービスデスクを設置し、本書の内容等について、Web フォームによる問い合わせの受付を行っています。

アカウント発行を希望されるシステムベンダは、以下宛先へアカウント発行申請の連絡をお願いします。

なお、医療機関等 ONS は、オンライン資格確認等システムの導入に従事するシステムベンダに対し、環境整備やシステム改修を行う上で必要な情報等の提供及び問い合わせ受付を行うものです。

登録には一定の審査があり、場合によってはアカウント発行をお断りさせていただくことがございますので、あらかじめご了承ください。

医療機関等 ONS アカウント発行申請先：vender_onsinf@ssk.or.jp