令和７年２月17日

次期顔認証付きカードリーダーにおいて

満たすべき要件

令和７年２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７年２月17日	初版	初版作成

目次

1. 背景及び目的……4
2. 顔認証付きカードリーダーとは……5
3. 顔認証付きカードリーダーにおいて満たすべき要件 ……6

１．　背景及び目的

「オンライン資格確認」は、オンラインで資格を確認することにより、医療機関・薬局の窓口で、直ちに資格確認ができるようになり、失効した資格情報による過誤請求の減少が期待できるものです。また、マイナンバーカードに搭載されている利用者証明用電子証明書を活用することで、医療機関・薬局において診療時における被保険者の確実な本人確認が可能になります。

さらに、オンライン資格確認等システムを通じて、患者本人の同意の下、医療機関においては服薬履歴や特定健診情報の閲覧が、薬局においては服薬履歴の閲覧が可能になります。

これらは既に令和３年 10 月より導入が開始されておりますが、マイナンバーカードの機能がスマートフォンに搭載されることや、今後、現行の顔認証付きカードリーダーの保守期限が終了する医療機関・薬局が出始めることを踏まえ、次期顔認証付きカードリーダーにかかる認証について示したものが本書となります。

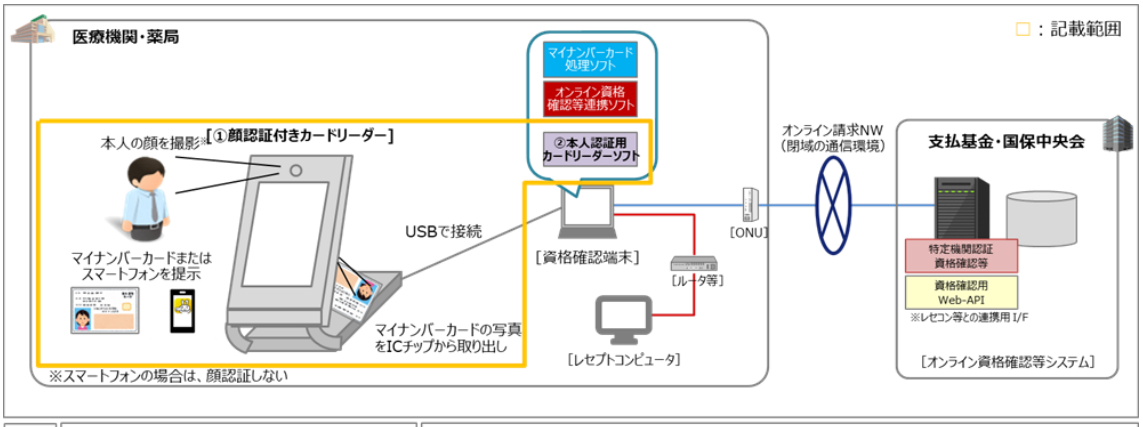
2. 顔認証付きカードリーダーとは

医療機関・薬局に導入するオンライン資格確認システムでは、顔認証付きカードリーダーの利用が可能です。顔認証付きカードリーダーによって、マイナンバーカードを用いた厳格な本人確認（※）を行うことが可能となり、窓口職員による確認の手間が減り、事務の効率化が期待されます。また、薬剤情報や特定健診情報を医療機関等が閲覧する際の患者の同意取得を、ディスプレイ上で案内することにより、スムーズかつ確実に行うことが可能となります。

オンライン資格確認等システムで使用することができる顔認証付きカードリーダーは、社会保険診療報酬支払基金（以下「支払基金」という。）の認証を受ける必要があります。

顔認証付きカードリーダーの構成イメージは、以下の通りです。マイナンバーカードの券面情報（照合番号 B を用いる）を読み取り、マイナンバーカードの顔写真データを IC チップから取り出し、撮影した本人の顔写真と照合を行います。

顔認証付きカードリーダーの構成イメージ



①	顔認証付きカードリーダー（機器）	機器として、以下の処理を行う 患者側カメラ：顔認証用顔写真の撮影 マイナンバーカード券面撮影用カメラ：マイナンバーカードの券面情報のスキャン ICカードリーダー：マイナンバーカード、マイナンバーカードの機能が搭載されたスマートフォンの読込 液晶ディスプレイ（タッチパネル）：患者の入力、選択操作（PIN入力、同意確認等）
②	本人認証用カードリーダーソフト（アプリ）	資格確認端末上で動作し、顔認証処理、患者へのガイダンス、意思確認等①の機器の制御等を行う

（※）マイナンバーカードに搭載されている利用者証明用電子証明書を利用するには、

①４桁の暗証番号（PIN）を入力する方法

②マイナンバーカードに表示及び記録された顔写真を用いる方法

のいずれかにより、本人確認を行うことが必要となります。

3.　顔認証付きカードリーダーにおいて満たすべき要件

項番	分類		必須	満たすべき要件
１．機器に係る要件				
1-1	患者側カメラ	機能要件	○	ISO/IEC 30107-3 で定義されるレベル 1 のプレゼンテーション攻撃を防御可能であること。（ソフトウェアによる実現でも可）。 ※一つの攻撃方法において、突破率 1%未満であること。 ※第三者機関（例：iBeta）による認証取得は必須ではない。
1-2			○	マイナンバーカード内の写真と照合に使用できること。
1-3		画素数	○	顔認証を行う上で必要な画質を担保できるものを選定すること。
1-4		色	○	カラー
1-5	マイナンバーカード券面撮影用カメラ	機能要件	○	マイナンバーカードの券面（表）から文字情報をスキャンできること。
1-6		画素数	○	券面情報をスキャンする上で必要な画質を担保できるものを選定すること。
1-7		色	○	カラー/モノクロは問わない。
1-8	IC カードリーダー		○	IC カード TypeB PC/SC に準拠、非接触型。 ＜今後発行されるマイナンバーカード類＞ ・2026 年に発行が予定されている次期マイナンバーカードに対応すること。 ・在留カードと一体化したマイナンバーカードに対応すること。 ・マイナンバーカードの機能が搭載されたスマートフォン(iPhone、Android)に対応すること。 ・IC カードリーダーは、5 年間の運用において衝撃耐性が 1000 回以上、読み取り耐久性が 10 万回以上を保証すること。 ・マイナンバーカードを置く場所を触覚で識別可能な凹凸や縁付きなどのデザインとすること。 ※ただし、触覚ガイド（凹凸や縁）を薄く設計し、マイナンバーカードの機能が搭載されたスマートフォンの読み取りに干渉しないようにすること。

			－	物理的なマイナンバーカードとマイナンバーカードが搭載されたスマートフォンの読み取り口は同一とすることが望ましい。 ※同一としない場合は、ユーザーに分かるように案内すること。
1-9	表示機能	液晶ディスプレイ	○	タッチパネルであること。（患者に対して表示し、同意等の意思確認を行うことを想定）
1-10		パネルサイズ・解像度／表示色	○	パネルサイズは５インチ以上であること。
1-11			○	640×480 ドット以上の表示が可能なこと。High Color（65,536 色）以上の表示が可能なこと。
1-12			○	なお、患者（老若男女問わず）に対して、顔認証時の写真撮影位置、説明文、案内文が簡単に認識・操作できること。
1-13	スピーカー		○	ユーザーに対し、認証状況（成功・失敗）の案内や患者が操作していない場合でも、エラーが発生した場合には、医療従事者向けに音声で知らせる機能を搭載すること。これらの機能については、言葉による動作指示を案内できる仕様であること。 テンキー（ディスプレイ）で押した場合に動作音がなること。（ビープ音や単純な電子音） ※音声に関しては、機械音声（合成音声）でも可とする。 医療機関等施設側での設定で音量調整ができること。（設定は本体のディスプレイ上で行うこととし、物理ボタンでの操作は不可とする） 暗証番号は読み上げないようにすること。 スピーカーは本体に取り付けること。（外付けは不可） ※資格確認端末からの引き回しは不可とする。
			－	ユーザーに対し、画面に表示されている文言の読み上げ等により、操作手順、動作指示を案内できる仕様であることを強く推奨する。 テンキー（物理）で押した場合に動作音がなること。（ビープ音や単純な電子音） 医療費助成受給者証・電子処方箋・診療情報提供書の選択画面において、受給者証名・医療機関名・診療科名等は読み上げないようにすること。

				※上記について、視覚障碍者等が個別の選択について詳細に確認したい場合、物理テンキー内の割り当てられたキーを押下すれば、受付職員が呼び出される仕様とすること。
1-14	入力装置（テンキー）		－	顔認証付きカードリーダーの操作(同意有無の選択や暗証番号入力)が行える物理テンキーを内蔵することを強く推奨する。 ※搭載する場合、数字の配列は、上から順に 123･･･と配列すること。テンキーについては、例えば、同意を『1』、同意しないを『3』、受付職員を呼ぶ場合は『8』等のように画面遷移の案内内容に沿ってキーを割り当てられるようにすること。また、直感的で視覚的・触覚的に操作しやすい設計とすること。さらにテンキーは、ISO/IEC Guide 71 に基づき、視覚・触覚による操作性や、ユニバーサルデザインの原則に従った設計を行うこと。 ※有償フォントを使うことは必須ではない。
1-15	接続インターフェース	USB	○	資格確認端末と USB で接続できること。（インターフェースは、資格確認端末における満たすべき要件に準拠し、最大 2 口までとする。） USB ポートが筐体内部で適切に固定されていること。内部の接続部分が頻繁な抜き差しで破損しないようにすること。 ※顔認証付きカードリーダーと資格確認端末を接続するケーブルは、推奨する製品を指定すること。 ※規格 2.0 以上、コネクタは資格確認端末側が Type-A とし、顔認証付きカードリーダー側は制限なし。 ※資格確認端末と顔認証付きカードリーダーを一体化させた仕組みとする場合は上記の限りではない。
1-16	電源供給方式		○	AC アダプタ又は USB バスパワー ※USB バスパワーを利用する場合は、バスパワーによる動作が不安定となる場合に備え、電源供給不足の検知機能または警告機能を搭載すること。
1-17	その他		－	ひし形 PSE、VCCI、SIAA 、防水・防滴の基準、難燃性規格等の取得は、製造者の判断とする。
1-18			○	ディスプレイ及び物理テンキーには、のぞき見防止の対策（のぞき見防止用フィルム等）を講ずること。

1-19		○	総務省の情報アクセシビリティ自己評価様式を基に、当該製品の評価結果を提出すること。
1-20		○	顔認証付きカードリーダーが利用不可となるエラーが発生した場合は、顔認証付きカードリーダー上の画面でそのエラー状況が把握できること。
1-21		○	１台の資格確認端末で最低２台（推奨は３台）の顔認証付きカードリーダーを接続できること。 ※資格確認端末と顔認証付きカードリーダーを一体化させた仕組みとする場合は上記の限りではない。
1-22		－	以下の機能について必要に応じて実装すること。 ①多言語対応（英語、中国語、韓国語)に対応していること。 ※多言語の音声対応も同様。 ※翻訳データや翻訳音声の提供は行わない。 ②ミラーリング機能を有していること。 ※暗証番号等の医療機関等で知りえない情報は分からない仕組みとすること。 ③資格確認端末の要件として、「メモリが 8GB 以上」となっていることを踏まえて、設計を行うこと。

項番	分類	必須	満たすべき要件
２．動作環境等に係る要件			
2-1	機器に係る動作環境	○	資格確認端末の Windows 上で PC/SC に準拠したカードリーダーとして認識され、単体のカードリーダーとして利用できる機能を有すること。
2-2		○	IC カードリーダーは、J-LIS が実施する「公的個人認証サービスに対応する IC カードリーダライタの適合性検証」を合格すること。 スマートフォン搭載の対応として、デジタル庁開発の検証ツールに合格すること。※提供予定
2-3	ソフトウェアに係る動作環境	○	本人認証用カードリーダーソフトは、資格確認端末上（Windows 10 IoT Enterprise 2019 LTSC、Windows 11 IoT Enterprise 2024 LTSC、Windows 10 IoT Enterprise 2021 LTSC）で動作するソフトウェアであること。 なお、Windows 10 Enterprise 2019 LTSC、Windows 10 Pro、Windows 11 Pro に対応する場合は、動作保証した上で、その旨を開示することも可能とする。 ※資格確認端末と顔認証付きカードリーダーを一体化させた仕組みとする場合は上記の限りではない。
2-4		○	顔認証付きカードリーダーには、安定性、拡張性、セキュリティを備えた OS を搭載すること。 推奨 OS： Windows OS Linux 系 OS（Debian, Ubuntu など） Android（AOSP 10 以降） RTOS（リアルタイム OS） QNX
2-5		○	使用する文字コードは、UTF8 であること。

項番	分類		必須	満たすべき要件
3. 本人認証用カードリーダーソフトに係る要件				
3-1	顔認証機能	前提事項	○	環境要件は、医療機関・薬局で利用することを想定すること。また、顔認証の性能要件を保証するため、設置環境要件を明示すること。また、車いす利用者や身長の低い方でも顔認証機能を快適に使用できるよう、設置位置の調整や可動性を考慮した設計とすること。
3-2			○	患者側カメラで撮影した患者の顔とマイナンバーカードの IC チップ内の顔写真で顔認証を行う機能を有すること。また、マイナンバーカードの IC チップ内の写真は白黒となるため、留意すること。
3-3			○	精度の設定は、更新ファイルの配信で変更ができる機能を有すること。
3-4			○	照合方式は、１：１照合で行うこと。
3-5			○	顔認証エンジンの品質証明として、以下の書類のうち、いずれかを日本語で提出できること。 -第三者機関（米国国立標準技術研究所（NIST）等）における顔認証精度に関する評価結果 -当該第三者機関の評価方法及び評価結果について説明した書類（低評価のものは除く） -当該顔認証エンジンの導入実績　等
3-6		性能要件	○	顔認証が求める精度は、理想的な環境下における１：１照合での認証精度として、FMR（誤合致率）0.01%の時に FNMR（誤非合致率）0.3%以下（0.1%以下を推奨）とすること。 なお、顔認証処理においてリトライを行うことにより本人拒否率を下げる仕組みとしていること。
3-7	スキャン機能	前提事項	○	マイナンバーカードの券面情報がスキャンできる機能を有すること。（生年月日 6 桁、有効期限の西暦部分 4 桁、セキュリティコード 4 桁）
3-8			○	マイナンバーカードの券面情報がスキャン時に券面情報の生年月日が和暦表示の場合、元年を 01 に変換する処理を行えること。

3-9		性能要件	○	マイナンバーカードの券面スキャンに関する認識率は、生年月日６桁、有効期限の西暦４桁、セキュリティコード４桁が視認できる券面状態のもので 99%以上とする。なお、券面撮影時、医療機関・薬局で利用することを考慮すること。ただし、視認できない券面状態のマイナンバーカードは、券面スキャンの対象外とする。
3-10	画面遷移		○	JIS X 8341-3:2016「高齢者・障害者等配慮設計指針－Web コンテンツ」の適合レベル AA に準拠することを目標とする。以下のレベル AAA 達成基準も可能な範囲で適用する： ①達成基準 2.4.8 現在位置（ユーザーが一連の手続の中で現在の位置を理解できること） ②達成基準 3.2.5 要求による状況の変化（自動更新しない） WCAG 2.1 の追加達成基準を可能な範囲で適用する： ①達成基準 2.5.5 ターゲットサイズ（一定以上のボタンサイズにする） ②達成基準 1.4.11 非テキストのコントラスト（UI のコントラスト比を 3:1 以上にする） 画面上のテキストは、背景とのコントラスト比を 4.5: 1 以上する 本要件は JIS X 8341-3:2016 に含まれる達成基準である。 同意画面は上に同意する、下に同意しないと表示すること。 ※アクセシビリティの観点より横型の配置は不可。 タッチパネルに表示されるテンキーは、以下の表示とすること。 ①レイアウト ３列×4 行の配置とする。 ボタンサイズは 10mm × 10mm 以上、間隔は 3mm 以上とする。

			②視覚と操作性 　数字や記号のコントラスト比は 4.5:1 以上（大きな文字は 3:1 以上）。 　タッチ時に視覚的（色変化）または音で操作フィードバックを提供する。 ③補助ボタン 　「削除」「完了」などの補助ボタンは、目立つ位置に配置し明確なラベルを付ける。 ※デジタル庁「ウェブアクセシビリティ導入ガイドブック」及び CUDO の「カラーユニバーサルデザイン推奨配色セットガイドブック」を設計時に参考とすること。
3-11		○	暗証番号（PIN）入力の際に桁数制限等を設け、制限値に満たない際は PIN 送信を行わない仕組みとすること。顔認証、暗証番号（PIN）入力等を患者側に操作指示、注意喚起、選択が可能な画面を提供すること。また、医療機関・薬局で一部の文言等のカスタマイズが行えること。
3-12		－	利用者（医療機関等）の設定によって、マイナンバーカードの暗証番号をタッチパネルで入力する際のテンキーについて、randomize する機能を有することが望ましい。 （物理テンキーは除く）
3-13	認証処理	○	顔認証時間を設定（処理時間によって、顔認証のリトライを行える設定等）できる機能を有すること。
3-14		○	支払基金が提供するプログラムを利用して、以下の処理が行えること。 　-PIN 入力で本人認証と資格確認が行えること。 　-PIN 入力で本人認証と初回登録が行えること。 　-PIN なし認証で資格確認が行えること。 　-PIN なし認証で初回登録が行えること。 　-オンライン資格確認等システムとの疎通確認。 　-マイナンバーカードの機能が搭載されたスマートフォンを用いた本人認証と資格確認が行えること。
3-15	セキュリティ	○	顔認証のために撮影した写真は、当該機器内外を含め保存しないこと。

3-16		○	認証処理に関連するデータは揮発性メモリ以外に保存せず、かつ、認証処理に関連するデータ及びその複製は、認証処理の終了のタイミングで能動的に消去すること。 認証処理に関連するデータには、最低限、暗証番号（PIN）、顔認証のために撮影した画像、マイナンバーカードの IC チップ内の写真、マイナンバーカードの券面情報を含む。また、能動的な消去とは、データを復元・再利用できなくする目的で上書き消去することを指す。
3-17		○	操作ログ等（操作ログ、接続・切断のログ、接続時の識別情報（ファームウェアバージョン等）のログ、認証率、認証結果等）を出力する機能を有すること。また、ログ上に個人を特定できる情報を出力しないこと。
3-18		○	エラー発生時にエラーログを出力する機能を有すること。また、ログ上に個人を特定できる情報を出力しないこと。
3-19		○	メモリダンプを不可とすること。
3-20		○	顔認証付きカードリーダーを管理する機能等において、デバッグモード等を用いて情報が詐取されない仕組みとすること。また、当該機器の構成以外の機器が接続された場合、動作しない仕組みとしていること。
3-21	その他	○	資格確認端末で顔認証付きカードリーダーの管理が行えること。ただし、顔認証付きカードリーダーを自動再来受付機等へ組込む場合は、対象外とする。
3-22		○	ネットワーク障害や資格確認端末の OS 再起動など外部機器の影響を受けても、自動的に再接続を試行し、再起動なしで運用を継続できること。必要に応じてリトライ機能を搭載し、一定時間後に自動で通信が復旧する設計とする。 また、ルーターや外部端末が障害から復帰した際には、ハートビート通信を通じて自律的に再接続されること。
3-23		○	当該機器に係る設定、操作方法、エラー発生時（マイナンバーカードのロック、一部の機能が正常に動作しない等）の対応手順をまとめた操作マニュアルを作成すること。
3-24		○	24 時間の連続動作できること。

項番	分類	必須	満たすべき要件
4．製造及び保守の体制に係る要件			
4-1	製造の体制	○	当該機器等の製造工程の履歴に関する記録を含む製造工程の管理体制が適切に整備されていること。また、当該管理体制を証明する資料を提出すること。
4-2		○	機器等に対して不正な変更が加えられないように製造者等が定めたセキュリティ確保のための基準等が整備されており、その基準等が当該機器等に適用されていること。また、それらを証明する資料を提出すること。
4-3		○	機器等の設計から部品検査、製造、完成品検査に至る工程について、不正な変更が行われないことを保証する管理が一貫した品質保証体制の下で行うこと。
4-4		○	機器等に不正が発見したときは、追跡調査や立入検査等、厚生労働省・支払基金と迅速かつ密接に連携して原因を調査し、排除できる体制を整備していること。
4-5	機器に係る保守の体制	○	医療機関・薬局からの当該機器に係る問合せを直接対応すること。
4-6		○	製品販売から 5 年間、当該機器の保守を行えること。（ハードウェア保守は、センドバック、オンサイト、ピックアップ保守のいずれかで対応すること。）
4-7	ソフトウェアに係る保守の体制	○	医療機関・薬局等からの顔認証機能に対する問合せを直接対応すること。
4-8		○	製品販売から 5 年間、顔認証機能の保守を行えること。なお、OS のパッチ適用やバージョンアップ時の動作検証は即座に対応すること。

4-9		○	当該機器・本人認証用カードリーダーソフトが使用するドライバ、ファームウェア等のアップデートが自動で行えること。また、新しいパッチが提供されてから原則 3 営業日以内に動作確認を行い、更新ファイルは、支払基金に事前に確認を得た上でオンライン請求ネットワーク経由で即座に配信を行うこと。なお、アップデートやパッチ適用にあたっては、マイナンバーカード処理ソフト及びオンライン資格確認等連携ソフトへの影響を確認し、当該機器の利用に支障が生じないよう留意すること。悪用可能な脆弱性の修正を行うこと。 アップデートやパッチ適用前には、運用環境に近いテスト環境（事前検証環境）にて、マイナンバーカードおよびオンライン資格確認等連携ソフトとの接続試験および総合試験を実施すること。再現性が確認できない場合はパッチの配信を見送るか、影響範囲を十分に説明した上で配信すること。 アップデートやパッチ適用に伴い、万が一動作不良が発生した場合は、前のバージョンへ速やかにロールバックできる仕組みを提供することを推奨する。 SBOM を生成し組み込まれるソフトウェアとそのバージョンを管理すること。

項番	分類	必須	満たすべき要件
５．顔認証付きカードリーダーの製造及び提供するための資格			
5-1	申し込み資格	○	サプライチェーン・リスクの確認として、当該機器で使用しているパーツ（部品）やソフトウェア（顔認証エンジン等）の一覧（一部のパーツ/ソフトウェアで他の製造者のものを使用する場合は、該当パーツ/ソフトウェアの製造者名に加え、開発を実際に行っている会社名（OEM元）も明記）を提示し、厚生労働省・支払基金の事前確認を受けること。
5-2		－	顔認証エンジンについては、調達先がさらに別のベンダーから調達している可能性を考慮し、二次・三次サプライヤーの確認も行うことが望ましい。
5-3		○	令和４・５・６年度全省庁統一資格審査において「物品の販売」のＡ又はＢの等級に格付けされている者であること。
5-4		○	品質管理体制について、ISO 9001 基準又は同水準と認められる品質管理体制を確立していること。
5-5		○	ISO/IEC27001（国際標準）又は JIS Q 27001（日本工業標準）のいずれかの認証を取得していること。
5-6		○	厚生労働省における物品等の契約に係る指名停止等措置要領に基づく指名停止を受けている期間中の者でないこと。
5-7		○	予算決算及び会計令第 70 条の規定に該当しない者であること。ただし、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者については、この限りではない。
5-8		○	予算決算及び会計令第 71 条の規定に該当しない者であること。
5-9		○	私的独占の禁止及び公正取引の確保に関する法律等に抵触する行為（談合等）は行わない旨を誓約すること。