HPKI セカンド電子証明書管理・認証プラットフォーム 利用者マニュアル

Ver. 2.11

目 次

CONTENTS

1	はじ	めに	$\dots 5$
	1.1.	HPKI セカンド電子証明書とはどういうものか	$\dots 5$
	1.2.	HPKI セカンド電子証明書で何ができるようになるのか	$\dots 5$
	1.3.	必要なものは何か	$\dots 5$
	1.4.	JPKI 利用者証明書連携ツールのインストール	6
	1.5.	ご利用にあたっての注意	8
2	最初	のにするべきこと:代替デバイスの登録	9
	2.1.	モバイルデバイス登録(HPKI カードをすでにお持ちの方)	9
	2.2.	モバイルデバイス登録(マイナポータル経由で HPKI 証明書を申請された方)	. 16
	2.3.	モバイルデバイス登録(登録用 URL をお持ちの方)	. 23
	2.4.	マイナンバーカード登録	. 30
3	HP	KI カードまたは代替デバイスを使った認証	. 33
	3.1.	ログイン(モバイルデバイスによる認証)	. 33
	3.2.	ログイン(HPKI カードによる認証)	. 37
	3.3.	ログイン(マイナンバーカードによる認証)	. 37
	3.4.	ログアウト	. 38
4	署名	ろをするとき	. 39
5	更新	所するとき	. 40
!	5.1.	HPKI カードを更新する場合	. 40
!	5.2.	モバイルデバイスを機種変更する場合	. 40
!	5.3.	マイナンバーカード(利用者証明書)を更新する場合	. 50
6	こん	なときは	. 51
(5.1.	日常の運用時	.51
(5.2.	モバイルデバイス登録時	.51
(5.3.	マイナンバーカード登録時	. 52
(5.4.	その他、わからないことがあったら	. 52
7	用語	吾	. 53
8	エラ	- メッセージと対応方法	. 54
8	3.1.	アカウントが無効です。管理者に連絡してください。	. 54
8	3.2.	WebAuthn is not Supported by this browser.	. 55
8	3.3.	セキュリティーキーの登録結果が無効です。	. 56
8	3.4.	NotReadableError: An unknown error occured while talking to the credential manager	. 57
8	8.5.	NotAllowedError: Operation failed	. 58
8	8.6.	セキュリティーキーによる認証に失敗しました。	. 59
8	3.7.	NotAllowedError: The 'navigator.credentials.create' API is only permitted in application	ons
v	vith th	e 'com.apple.developer.web-browser' entitlement	. 60
8	3.8.	NotAllowedError: The operation either timed out or was not allowed	. 61
8	3.9.	NotSupportedError: The specified 'userVerification' requirement cannot be fulfilled by t	his
Ċ	levice	unless the device is secured with a screen lock	. 62

8.	10.	403 Forbidden	. 63
8.	11.	mahpki-auth.2nds.medis.or.jp でセキュリティキーを使用する	. 64
8.	12.	mahpki-auth.2nds.medis.or.jp にサインインする方法を選択してください。	65
8.	13.	画面のロックを使用する	. 66
8.	14.	パスコードで続ける	. 67
8.	15.	Cookie が見つかりません。	. 68
8.	16.	(画面が真っ白または真っ黒になる)	. 69
8.	17.	スマートフォンの画面に QR コードが表示される	. 70
8.	18.	すでにこのセッションで異なるユーザーxxxxxxx として認証されています。	.71
8.	19.	無効なアクセス、または、URLの有効期限切れにより処理を中断します。	. 72
8.2	20.	405 Method Not Allowed	73
8.2	21.	パスキーを管理する方法を選択してください	.74
8.2	22.	Autheticator:パスキーを追加できませんでした	. 75
8.2	23.	利用可能なパスキーがありません	. 76
8.2	24.	ログインできません。クレデンシャルのセットアップが必要です。	. 77
9	PC	でのメッセージ	. 78
9.3	1.	このサイトは安全に接続できません	. 78
9.2	2.	このサイトへの接続はセキュリティで保護されていません	. 79
9.3	3.	このページは現在機能していません	. 80
9.4	4.	HPKI(JPKI)証明書のユーザが無効となっています。	. 81
9.	5.	予期せぬエラーが発生しました。	. 82
9.0	5.	Cookie が見つかりません。	. 83
9.	7.	該当のユーザが登録されていません	. 84
9.8	8.	デバイス認証に必要なユーザ情報が登録されていません。	. 85
9.9	9.	デバイス認証でエラーが発生しました。	. 86
9.	10.	Unauthorized	. 87
9.	11.	ユーザ情報の取得ができませんでした。	. 88
9.	12.	認証用デバイスが未登録です	. 89
9.	13.	「マイナンバーカードを登録」をクリックしても画面が変わらない	. 90
9.	14.	登録対象のマイナンバーカードの証明書は、別のユーザが登録済です。	. 90
9.	15.	既にアプリケーションが起動しています。	. 91
9.	16.	個人番号カードに接続できません。	. 92
9.	17.	Forbidden	. 93
9.	18.	HPKI(JPKI)証明書が失効しています。	. 94
9.	19.	HPKI(JPKI)認証でエラーが発生しました。	. 95
9.2	20.	マイナンバーカードに紐づくユーザが存在しません。	. 96
9.2	21.	mahpki-auth.2nds.medis.or.jp へのアクセスが拒否されました	. 97
9.2	22.	FIDO 認証情報の登録ができませんでした	. 98
10	各	種設定の確認・変更方法	. 99
1 C).1.	ブラウザのキャッシュクリア	. 99
1 C).2.	IC カードからの証明書の読み取り確認1	107
1 C).3.	スマートフォンの標準ブラウザ設定確認	111

10.4.	スマートフォンの OS,ブラウザのバージョン確認	114
10.5.	iCloud キーチェーンを有効にする	117
10.6.	スマートフォンでのブラウザの見分け方	123

1 はじめに

1.1.<u>HPKI セカンド電子証明書とはどういうものか</u>

医療分野にも IT 化・クラウド化・ネットワーク化の波が押し寄せ、情報共有や業務効率化のためには外に開かれた システムを使用することが必須となってきています。一方で、外に開かれるということは悪意のあるハッカーなどからの攻撃 にさらされることも意味しています。攻撃により機微な個人情報である医療情報が漏洩すると患者様の利益を著しく損 なうことになり、医療システムが使用不能となると病院の機能そのものに多大な影響を及ぼします。

医療情報システムでは、医療従事者の本人認証および資格確認を行える「HPKI カード」があります。「HPKI カード」では IC カードによる電子署名が行えますが、物理的なカードが必要であるため利用環境に制限があります。HPKI カードに付与される電子証明書と同等の証明書(セカンド鍵)をクラウド上に保管することで、HPKI カードがない状態でも電子署名を行うことが可能となります。

クラウド上に保管されている証明書を利用するために確実な本人認証が必要となるため、HPKIカードによる認証に加え、スマートフォン等を使った生体認証またはマイナンバーカードでの本人認証機能を提供します。

1.2.<u>HPKI セカンド電子証明書で何ができるようになるのか</u>

医療従事者の電子署名を行う場合、「HPKI カード」を使用して電子署名を行う事で、その文書の作成者および 作成者の資格情報を確認することができます。しかし、「HPKI カード」では以下の課題があります。

- ・システムを使う PC すべてに IC カードリーダーが必要となる。
- ・HPKIカードを常に持ち歩く必要がある。置き忘れや紛失時に業務に支障がでる。
- ・電子署名時に毎回 PIN(暗証番号)を入力する必要があり、業務負荷が高くなる。

HPKI セカンド電子証明書ではこれらの点を改善するシステムで、次のような利用ができます。

(a)生体認証付のスマートフォンを登録することで、HPKI カードを使用しない本人認証が可能です。

- (もちろん HPKI カードによる本人認証をすることも可能です。)
- (b)マイナンバーカードの登録を行う事で、マイナンバーカードによる本人認証が可能になります。(マイナポータ ル経由で HPKI 証明書を申請するか、HPKI カードとマイナンバーカードを用いてご自分で登録操作を実 施する必要があります。)
- (c)一旦認証したら、その認証情報を利用する事により、一定期間(約一日程度)署名時の都度認証が不要 になります。

1.3. 必要なものは何か

HPKI セカンド電子証明書管理・認証プラットフォームを利用するには、以下のものが必要となります。 ※各認証方式に合わせ必要なものを準備してください。

- (1)生体認証(指紋認証、顔認証など)が可能なモバイルデバイス(スマートフォン、タブレット) 本システムにてデバイス認証を行う場合、事前に使用するモバイルデバイスを登録する必要があります。 「FIDO2」準拠の生体認証機能を備えた iOS 端末と Android 端末が利用できます。iOS 端末はバ ージョン 14 以上、Android 端末はバージョン 7 以上の OS で、かつ指紋認証などの生体認証機能を備 えていれば、「FIDO2」準拠と判断できます。
- (2) HPKI カード

本システムにて HPKI 認証を行う場合に必要となります。

日本医師会電子認証センターから発行されている「医師資格証」、日本薬剤師会認証局から発行されている「薬剤師資格証」、一般財団法人医療情報システム開発センター(MEDIS) HPKI 電子認証局か

ら発行されている「MEDIS-HPKI 資格証」を利用できます。

- (3)マイナンバーカード 本システムにて JPKI 認証を行う場合に必要となります。 マイナポータルから HPKI 証明書の発行依頼を行った場合、マイナンバーカードの情報も HPKI セカンド 電子証明書管理・認証プラットフォームに登録されマイナンバーカードによる認証も可能です。
- (4)システムに接続できる WindowsPCと、その PC 上で動作する IC カード読取装置

IC カード読み取り装置にあわせ、IC カードドライバや IC カードと接続するアプリケーションが必要となります。

実施したい操作	必要なソフトウェア
HPKI カードでの認証	・HPKI カードドライバセット
マイナンバーカードでの認証	・公的個人認証サービスの利用者クライアントソフト
	・JPKI利用者証明書連携ツール
マイナンバーカードの登録	・HPKI カードドライバセット
	・公的個人認証サービスの利用者クライアントソフト
	・公的個人認証サービスの利用者クライアントソフト(Edge/
	Chrome ブラウザ利用版)
	・ブラウザ拡張機能「利用者クライアントソフト Edge/Chrome」
	※上記「利用者クライアントソフト(Edge/Chrome ブラウザ利用
	版)」と同時にインストールされます。

PCのOSなどの動作条件、および利用できるICカード読取装置の機種や必要なモジュールについて は、それぞれの認証局にご確認ください。 公的個人認証サービスの利用者クライアントソフト等のセットアップに関しては公的個人認証サービスの ポータルサイトにてご確認ください。(https://www.jpki.go.jp/index.html) JPKI利用者証明書連携ツールのインストールに関しては、1.4章に記載しています。

1.4.JPKI利用者証明書連携ツールのインストール

マイナンバーカードを用いて認証を実施する場合は、事前に JPKI 利用者証明書連携ツールを PC にインストールする 必要があります。

(1) PC のブラウザ(※1) で以下の URL にアクセスします。

https://mahpki-srv.2nds.medis.or.jp/index.html

ブラウザ上部の URL 表示欄に上記 URL 文字列を全て入力して Enter キーを押すと、URL が示すサイトにアクセ スされます。

新しいタブ × +	-	
C A (the https://mahpki-srv.2nds.medis.or.jp/index.html	<i>t</i> ≡ ⊕	PC 画面
▶ おすすめサイト 🎦 abouttabs	🛅 र	

(※1)ブラウザは Edge (Windows10 に標準で存在しているブラウザ)もしくは Chrome を利用してください。

(2) 下記の画面が表示されるので、「マイナンバーカードを使ってスマートフォンを登録する」をクリックします。

HPKIセカンド電子証明書管理・認証プラットフォーム 認証用デバイス/マイナンバーカード登録サイト	PC 画面
このサイトにしついて このサイトに、クラッド上に保管されている(セカンド電子証明書)を電子賞名警に利用する場合の本人認証を、HPKIカード(※)の代わりのデバイスで認証できるようにするためのサイトです。 (※) HPKIカード:日本医師会発行の「医師賞慎証」、日本薬剤師会発行の「薬剤師賞権証」、MEDIS発行の「MEDIS HPKI 貴飯証」 本サイトはPDCよる操作が領接となります。スマートフォンやタブレットからは利用できません。	
Fini 中 IPKIカードを使ってスマートフォンを登録する	
マイナンバーカードを使ってスマートフォンを登録する ※マイナホータル経営で10402頃高を発行したユーザが利用間端	
□ ➡	
Test HPKIカードを使ってマイナンバーカードを登録する	

(3) 画面が展開するので、「「JPKI 認証連携ツール」は、こちらから取得してください」の「こちら」リンクをクリックします。

マイナンバーカードを使ってスマートフォンを登録する =マイナホークル経動でHPK辺研測を発行したユーザが利用問題	PC 画面
ご利用にあたって マイナンバーカードを使っ、スマートフォンを認定デバイスとして登録することができます。 すでご覧またでいる場合、このゲイトで同覧登録することができます。 マイナボークル語で使いな認識の使行手続を行い、マイナンバーカードの構成が出サールに登録されているこ ジロイボークル語で使いな認識の使行手続を行い、マイナンバーカードの構成が出サールに登録されているこ マイナンバーカード ・スマートフォン ・バロケード ・スマートフォンは、以下の条件を整たすちのです。 10たカード ・スマートフォンは、以下の条件を整たすちのです。 11た力・ビリーダー 12年40至25月の増売してものうけ、 12月4日の通貨は「スワンビントランド」カッドカンド本用に登録してもること (2)予約men、Androidの通貨は「スジートフォン集成に登録してもること (3)Phonen、Androidの通貨は「スジートフォン集成に登録してもること (3)Phonen、Androidの通貨は「スジートフォン本用に登録してもること (3)Phonen、Androidの運貨は「スジートフォン集成に登録してもること (3)Phonen、Androidの運貨は「スジートフォン本に登録してもること (3)Phonen、Androidの運貨は「スジートフォン本に登録してもること (3)Phonen、Androidの運貨は「スジートフォン本に登録してあること (3)Phonen、Androidの運貨は「スジーリーン」アメロトレ、プラジーは、100日の「スジートマントリー」 (4) Phone Androidの運貨は「スジートフォントマントラントラント (4) Phone Androidの運貨は「スジートフォントラント (1) Phone Androidの運貨は「スジートラント (4) Phone Androidの運貨は「スジートラント (5) Phone Androidの運貨は「スジートラント (4) Phone Androidの運貨は「スジート」 (5) Phone Androidの運貨は「スジート」 (5) Phone Androidの運貨は「スジート」 (5) Phone Androidの単」 (5) Phone A	
「PKIEEE連携ツール」は、ごちらから取得してください。 ・マイナンバーカードがりにカードリーダーにゼットされている状態で下のボタンをクリックしてください。・ マイナンバーカードで登録 クリリック	

(4) JPKI 利用者証明書連携ツールダウンロードページが表示されるので、お使いの PC の OS が 64bit の場合は 「64bit OS 用インストーラ」、32bit の場合は「32bit OS 用インストーラ」をクリックします。 インストーラ(exe ファイル)がダウンロードされます。

公的個人認証サービス(JPKI)利用者証明書連携ツール ダウンロードページ	PC 画面
マイナンバーカードを利用してHPKIセカンド電子証明書管理・認証ブラットフォームで認証を行うには、以下のマニュアルを読み、インストーラをダウンロードして実行してください。 インストールにはPCの管理者権限が必要となります。	
<u>IPKI利用者連携ツールマニュアル</u> IPKI利用者連携ツールのインストール方法、および操作方法の説明書です。 インストール前に必ずご一法ください。 ダウンロードファイルのハッシュ値 (SHA512)は <u>こちら</u>	
<u>64bit 05用インストーラ</u> Windows11または、Windows10 (64bit版) 用のインストーラです。 ダウンロードファイルのハッシュ値 (SHA512)は <u>ごちら</u> 32bit の場合はこちら	
<u>32bit 05用インストララ</u> Windows10 (32bitk) 用のインストーラです。 ダウンロードファイルのハッシュ値 (SHA512)は <u>ごちら</u>	

※ブラウザやウイルスソフトの設定によっては、exeファイルのダウンロードが保留・拒否される場合があります。 ダウンロードがうまくいかない場合は、ブラウザやウイルスソフトの設定を確認してください。 (5)「JPKI利用者証明書連携ツールマニュアル」をクリックして、ツールのインストールマニュアル(PDF)をダウンロードしま

す。

公的個人認証サービス(JPKI)利用者証明書連携ツール ダウンロードページ	PC 画面
マイナンバーカードを利用してHPKIセカンド電子証明書管理・認証プラットフォームで認証を行うには、以下のマニュアルを読み、インストーラをダウンロードして実行してください。 インストールにはPCの管理者権限が必要となります。	
JPKI利用者連携ツールマニュアル JPKI利用者連携ツールマニュアル JPKI利用者連携ツールのインストール前にあずび一語ください。 インストール前に必ずご一語ください。 ダウンロードファイルのハッシュ値 (SH4512)はごちら	
<u>64bit OS用インストーラ</u> Windows11または、Windows10 (64bit版) 用のインストーラです。 ダウンロードファイルのハッシュ値 (SHA512)はごちら	
<u>32Dit OS用インストーフ</u> Windows10 (32bit版) 用のインストーラです。 ダウンロードファイルのハッシュ値 (SHA512)は <u>ごちら</u>	

(6) ダウンロードした「JPKI 利用者証明書連携ツールマニュアル」を開き、その 2.1 章の手順に従って、 ダウンロードした exe ファイルを操作し、 インストールします。

1.5.ご利用にあたっての注意

HPKIカード、認証用に登録したモバイルデバイス・マイナンバーカードは、紛失や盗難などに注意して保管し、他人 に貸すことのないようにしてください。

万一、紛失や盗難にあった場合は、速やかに失効手続きを行ってください。

2 最初にするべきこと:代替デバイスの登録

HPKIカードによる認証を行わず、代替デバイス(マイナンバーカードまたはスマートフォン等のモバイルデバイス)による認証を実施したい場合、認証に使用する代替デバイスを登録する作業が必要となります。

2.1. Eバイルデバイス登録(HPKI カードをすでにお持ちの方)

【必要なもの】モバイルデバイス、HPKI カード、PC

- ※PC は HPKI カードドライバのインストールが完了し、使用する IC カード読取装置のドライバもインストールされて 動作可能となっている必要があります。
 ※PC およびモバイルデバイスはインターネットに接続できる環境が必要となります。
- (1)HPKI カードと、生体認証機能のあるモバイルデバイスを準備し、HPKI 認証ができる PC で操作します。
- (2) HPKIカードを IC カード読取装置にセットし、PC のブラウザ(※1)で以下の URL にアクセスします。 https://mahpki-srv.2nds.medis.or.jp/index.html

ブラウザ上部の URL 表示欄に上記 URL 文字列を全て入力して Enter キーを押すと、URL が示すサイトにアクセ スされます。

	🔄 新しいタブ	x +	-	
	CA	tttps://mahpki-srv.2nds.medis.or.jp/index.html	t,≡ ⊕	F
Ь	おすすめサイト 🎦 abo	uttabs	ि र	

(※1)ブラウザは Edge (Windows10 に標準で存在しているブラウザ) もしくは Chrome を利用してください。

(3) 下記の画面が表示されるので、「HPKIカードを使ってスマートフォンを登録する」をクリックします。

HPKIセカンド電子証明書管理・認証プラットフォーム 認証用デバイス/マイナンバーカード登録サイト	PC 画面
このサイトについて このサイトは、クラッド上に保留されている「セカンド電子経動賞」を電子賞を等に利用する場合の本人総証を、HPKIカード(※)の代わりのデバイスで認証できるようにするためのサイトです。 (※) PKCカード: 日本医療免疫行の「医療資産証」、日本解剖時免疫行の「薬剤的質解証」、MEDIS別行の「MEDIS HFMC 賞修証」 本サイトはPCによる操作が崩倒となります。スマートフォンやタブレットからは利用できません。	
₩₩₩ ► HPKIカードを使ってスマートフォンを登録する	
マイナンバーカードを使ってスマートフォンを登録する #マイナボータル経済で14901度期高を発行したユーザが利用可能	
■ → REV スマートフォンを変更する	
〒## ■ HPK(カードを使ってマイナンバーカードを登録する	

(4) 画面が展開するので、「HPKIカードで登録」をクリックします。



(5) HPKI 証明書選択画面が表示されるので、証明書を選択します。

HPKIカードに格納されている証明書が表示されるので、その証明書をクリックしてから「OK」をクリックします。 ※ブラウザにより証明書選択画面の外観は異なります。以下に掲げるのは Edge の場合の画面です。

認証用の証明書の選択 サイトmahpki-auth.2nds.medis.or.jp:443 では資格情報が必要です:		×	①証明書部クリック	PC 画面
Ę	JMACombi30047 HPKI-01-HPKI_JV2-forAuthentication-forIndividual 2022/11/1		②OK ボタンクリック	
証明書情	般 OK 4	ャンセル		

(6)「PIN を入力してください」という画面が表示されるので、HPKI カードの PIN(暗証番号)を入力して「OK」をクリックします。



(7) PC 画面に QR コードが表示されるので、モバイルデバイスのカメラで QR コードを読み取り、登録サイトにアクセスします。

※画面には QR コードの有効期限も表示されます。
有効期限内に読み取らないと QR コードは無効になりますのでご注意ください。
無効になってしまった場合は再度(2)からやり直してください。

PC 画面



モバイルデバイスでの読み取り、および登録サイトへのアクセス方法は以下の手順で実施します。

a) iPhone(iOS)の場合

「カメラ」のアプリを起動します。



モバイル画面

対象の QR コードを読み取り、「"2nds.medis.or.jp"」というポップアップが表示されたら、右下にあるメニュー選択 ボタンをタップします。



メニュー画面から「Safari で開く」を選択します。

۲	<u> </u>	۲		
Ŧ	テストC20944	C RATTE		モバイル画面
Vizio	Intersu/maade-sauth_ande.ms Intersu/maade-sauth_ande.ms Intersuper Status Interstrest Intersupe	dis.orjp/ 32 Mazižt/T ODązWi NazyMU 22MD roG C Mass Mark Mark Mark Mark Mark	[Safa:	ri で開く」をタップ
	●v: リーディングリストに 追加 Safariで開く	~~ ©		
12 7 0-	- ビデオ 写真 ポートし-	(88) - N (7/2)		
		Ð		

※「Safari で開く」ではなく、別のアプリケーションが表示される場合は、Safari で開く設定を行う必要があります。 「設定」から「Safari」を選んでいただき、"デフォルトのブラウザ App"を選択して Safari にチェックを入れてください。

モバイル画面

b) Android の場合

「Chrome」アプリを開きます。



検索キーワードを入力する項目の右にあるカメラボタンをタップします。



QRの情報を読み取り、ポップアップ表示された「2nds.medis.or.jp~」のボタンをタップします。

12 / 123



(8)QRコードを読み取ったモバイルデバイスに、ログイン画面が表示されます。

(以降、(12)までモバイルデバイス操作の画面説明となります)

直前に HPKI 認証を実施しているため、Username 欄には HPKI カードから取得した本人 ID が表示されています。 値が正しいことを確認して「ログイン」ボタンをタップします。



(9)認証情報登録開始画面が表示されるので、「登録」ボタンをタップします。

11552 G □	モバイル画面
HPKIセカンド電子証明書管 理・認証プラットフォーム ♪セキュリティーキーの登録	
## 4	ボタンタップ
< —	

(10)モバイルデバイスによる生体認証の画面が表示されるため、生体認証を実施します。

画面や生体認証の方法は、モバイルデバイスにより異なります。

下記の例は指紋認証です。指紋認証の場合、あらかじめ登録してある指を検知部にセットして、デバイスに指紋認証をさせます。

※事前にモバイルデバイスに生体認証登録を実施していない場合は、ここで Security Key Error となります。 生体認証の登録を実施したうえで、(2)からやり直してください。

47X7 ♥	18:48	3	3% 🛄
கக் 🔒 der	v.2nds.mistyauth.sv	capps.net	Ç
HPKIセス 管理・副	カンド電子証明 認証プラット	月書	
フォーム	A • Security Key Regist	ration	
	*		
То	uch IDで続けてくだ キャンセル	さい。	
			8

(11)生体認証登録が完了したら、「ラベル登録画面」が表示されます。

作成した鍵情報をモバイルデバイス側で識別するためのラベル情報を設定する画面ですが、値はシステムで自動設定されるため、特に何も入力せず、「OK」をタップします。

11:52 G 🖬	发 🗢 🖬 38%		
X 🗎 mahpki-auth-regitest.2nds.medis.o	sjo 🤞 🗄		
			モバイル画面
HPKIセカンド電子証明 理・認証プラットフォー	書管 -ム		
mahpki-auth-reg.test. 2nds.medis.or.jp の内 容 Please input your registered authent <u>VebAuthn Authenticator (De</u> キャンセル	cator's label fault Label) OK	0	K ボタンタップ
<u> </u>			

(12) モバイルデバイス側の処理が完了し、完了画面が表示されます。

17:00 G 🖬	र्थ्र 🗣 🖬 37%
X amaado auth-reg.test.2nds.medis.or	- < :
スマートフォンでの手続き(登録)は 完了しました。 操作したPCにて登録が完了している 確認してスマートフォンのブラウザ	ことを を
終了してください。	
登録情報が築れる可能性があるた 戻るボタンは押さないでくたさい	Ø.
<	

モバイル画面

(13) 同時に、PC 側にも完了画面が表示されます。ブラウザを閉じてください。

FIDO認証の登録が完了しました 画面を閉じてください

nds.mistyauth.svcapps.net/regist/

PC 画面

※PC 側のブラウザは必ず閉じてください。タブだけでなくブラウザ全体を終了させる必要があります。 ブラウザ右上の×をクリックして閉じてください。

2.2.<u>モバイルデバイス登録(マイナポータル経由で HPKI 証明書を申請さ</u> <u>れた方)</u>

【必要なもの】モバイルデバイス、マイナンバーカード、PC

※PCは公的個人認証サービスの利用者クライアントソフト、およびJPKI利用者証明書連携ツールのインストールが完了し、使用するICカード読取装置のドライバもインストールされて動作可能となっている必要があります。
 ※PCおよびモバイルデバイスはインターネットに接続できる環境が必要となります。
 ※マイナポータル経由で HPKI 証明書を申請した利用者が対象となります。

- (1)マイナンバーカードと、生体認証機能のあるモバイルデバイスを準備し、JPKI認証ができる PC で操作します。
- (2) マイナンバーカードを IC カード読取装置にセットし、PC のブラウザ(※1) で以下の URL にアクセスします。 https://mahpki-srv.2nds.medis.or.jp/index.html

ブラウザ上部の URL 表示欄に上記 URL 文字列を全て入力して Enter キーを押すと、URL が示すサイトにアクセ スされます。

田 新しいダブ x +	-
C A ttps://mahpki-srv.2nds.medis.or.jp/index.html	t≞ @
▶ おすすめサイト 🎦 abouttabs	ै 🔁 र

(※1)ブラウザは Edge (Windows10 に標準で存在しているブラウザ)もしくは Chrome を利用してください。

(3) 下記の画面が表示されるので、「マイナンバーカードを使ってスマートフォンを登録する」をクリックします。

HDKTヤカンド電子証明書祭神・読証プラットフォール]
認証用デバイス/マイナンバーカード登録サイト	PC 画面
<mark>このサイトについて</mark> このサイトは、クラウド上に保留されている「セカンド電子証明書」を電子署各等に利用する場合の本人認証を、HPKIカード(※)の代わりのデバイスで認証できるようにするためのサイトです。 (※) HPKIカード:日本医療会発行の「医師県成証」、日本薬剤除会発行の「薬剤的資格証」、NEDIS発行の「MEDIS HPKI 賞格証」 本サイトはPDによる硬作が崩退となります。スマートフォンやタブレットからは利用できません。	
■■■■ ■■■ HPKIカードを使ってスマートフォンを登録する	
▶ ▶ ■ スマートフォンを変更する	
Terr HPKIカードを使ってマイナンバーカードを登録する	

(4) 画面が展開されるので、「マイナンバーカードで登録」をクリックします。

マイナンバーカードを使ってスマートフォンを登録する マイナオータル経営でHPK編開業を発行したユーザが利用問題 ご利用にあたって	PC 画面
マイナンバーカードを使って、スマートフォンを超近デバイスとして登録することができます。 すでに登録されている場合、このサイトで再変登録することにより新しいスマートフォンへ登録更新ができます。 マイナポークル経営で体に認識の多時形を終たり、マイナンバーカードの情報が見ませっパに容易ませれているユーザが利用可能です。	
になった。 ボタンクリック マイナンパーカード ボタンクリック マイナンパーカード ボタンクリック マイナンパーカード ボタンクリック マイナンパーカードで会話 ボタンクリック マイナンパーカードで会話 ボタンクリック マイナンパーカードで会話 ボタンクリック マイナンパークションクもの ・ ・約400日また ションクシュンターションクまれ ・101日になるかの話・はなくをありためスマーシフェンネルに登録してあること ・ ・101日になるのの話を、1051-ワションクレークションクもの ・ ・101日になるのの話を、1051-ワションノンクションクションクリングリックションクションクションクションクションクションクションクションクションクション	

(5)証明書選択画面が表示されるので、証明書を選択します。

マイナンバーカードに格納されている証明書が表示されるので、その証明書をクリックしてから「OK」をクリックします。 ※ブラウザにより証明書選択画面の外観は異なります。以下に掲げるのは Edge の場合の画面です。

認証用の証明書の選択	×		
サイト mahpki-auth2.test.2nds.mistyauth.svca す:	pps.net:443 では資格情報が必要で	。①証明書部クリック	PC 画面
24EBD7E747EFHH13101001B JPKI-TEST 2023/4/7	4 [^]	②OK ボタンクリック	
証明書情報	ОК ++77511		

(6) マイナンバーカードログイン画面が表示されるので、利用者証明用パスワード(数字 4 桁)を入力して「OK」をクリックします。



(7) PC 画面に QR コードが表示されるので、モバイルデバイスのカメラで QR コードを読み取り、登録サイトにアクセスします。

※画面には QR コードの有効期限も表示されます。

有効期限内に読み取らないと QR コードは無効になりますのでご注意ください。

無効になってしまった場合は再度(2)からやり直してください。



モバイルデバイスでの読み取り、および登録サイトへのアクセス方法は以下の手順で実施します。

a) iPhone(iOS)の場合

「カメラ」のアプリを起動します。



対象の QR コードを読み取り、「"2nds.medis.or.jp"」というポップアップが表示されたら、右下にあるメニュー選択 ボタンをタップします。



メニュー画面から「Safari で開く」を選択します。



※「Safari で開く」ではなく、別のアプリケーションが表示される場合は、Safari で開く設定を行う必要があります。 「設定」から「Safari」を選んでいただき、"デフォルトのブラウザ App"を選択して Safari にチェックを入れてください。

b) Android の場合

「Chrome」アプリを開きます。



モバイル画面

検索キーワードを入力する項目の右にあるカメラボタンをタップします。



QRの情報を読み取り、ポップアップ表示された「2nds.medis.or.jp~」のボタンをタップします。



(8) Q Rコードを読み取ったモバイルデバイスに、ログイン画面が表示されます。

(以降、(12)までモバイルデバイス操作の画面説明となります) 直前に HPKI 認証を実施しているため、Username 欄には HPKI カードから取得した本人 ID が表示されていま す。値が正しいことを確認して「ログイン」ボタンをタップします。



(9)認証情報登録開始画面が表示されるので、「登録」ボタンをタップします。

11:52 G □ N ♥ 0 38% X ⊕ mahpki-auth-regisett Zndalmedia or, p < :		モバイル画面
HPKIセカンド電子証明書管理・認証プラットフォーム		
2411974-4-00±k	ボ	タンタップ
< -		

(10)モバイルデバイスによる生体認証の画面が表示されるため、生体認証を実施します。

画面や生体認証の方法は、モバイルデバイスにより異なります。

下記の例は指紋認証です。指紋認証の場合、あらかじめ登録してある指を検知部にセットして、デバイスに指紋認 証をさせます。

※事前にモバイルデバイスに生体認証登録を実施していない場合は、ここで Security Key Error となります。 生体認証の登録を実施したうえで、(2)からやり直してください。

■ 77×7 5	18:48	33% 🛄
st at	dev.2nds.mistyauth.svcapps.ne	et C
HPKI 管理	セカンド電子証明書 ・認証プラット	
フォ・	−∠ P Security Key Registration	
	Touch ID 7時はてください	
	キャンセル	
1	۰ A M	ß
N		U

(11) 生体認証登録が完了したら、「ラベル登録画面」が表示されます。

作成した鍵情報をモバイルデバイス側で識別するためのラベル情報を設定する画面ですが、値はシステムで自動設定されるため、特に何も入力せず、「OK」をタップします。



(12) モバイルデバイス側の処理が完了し、完了画面が表示されます。

17:00 G 🖬 🕅 X 🔒 maado auth-reg.test.2nds.medis.or.jp	x	モバイル画面
スマートフォンでの手続き(登録)は 完了しました。 操作したPCにて登録が完了しているこ 確認してスマートフォンのブラウザを 終了してください。	ことを	
※ブラウザの戻るボタンを押すと、 登録情報が壊れる可能性があるため 戻るボタンは押さないでください。	~	
<		

(13) 同時に、PC 側にも完了画面が表示されます。ブラウザを閉じてください。



※PC 側のブラウザは必ず閉じてください。タブだけでなくブラウザ全体を終了させる必要があります。 ブラウザ右上の×をクリックして閉じてください。

2.3. モバイルデバイス登録(登録用 URL をお持ちの方)

HPKI カードが発行・送付されず、HPKI セカンド電子証明書のみが発行されている場合でも、モバイルデバイス登録の案内に従ってモバイルデバイスを登録することで、HPKI セカンド電子証明書の利用が可能となります。

PC での操作は不要です。

【必要なもの】モバイルデバイス、通知カード(登録 URL が記載された QR コード)

※マイナポータルから HPKI 証明書発行依頼した場合は、通知カードではなくマイナポータルに表示される登録 URL のリンクが対象となります。

- (1) FIDO2 対応の生体認証機能のあるモバイルデバイスを準備します。 あらかじめモバイルデバイス本体に生体認証登録をしておく必要があります。
- (2) 電子認証センターから発行された QR コードが記載された通知カードを取り出し、スマホで読み取りデバイスの登録 サイトにアクセスします。
 - ※QR コード(または登録 URL のリンク)には有効期限があります。期限内にアクセスしないと無効になります。その場合は、 発行した認証局にお問い合わせください。
 - ※マイナポータルからHPKI証明書発行依頼した場合はc),d)の内容を参考にデバイス登録サイトにアクセスしてください。

a) iPhone(iOS)の場合

「カメラ」のアプリを起動します。



モバイル画面

対象の QR コードを読み取り、「"2nds.medis.or.jp"」というポップアップが表示されたら、右下にあるメニュー選択 ボタンをタップします。



メニュー画面から「Safari で開く」を選択します。



※「Safari で開く」ではなく、別のアプリケーションが表示される場合は、Safari で開く設定を行う必要があります。 「設定」から「Safari」を選んでいただき、"デフォルトのブラウザ App"を選択して Safari にチェックを入れてください。

b) Android の場合

「Chrome」アプリを開きます。



モバイル画面

検索キーワードを入力する項目の右にあるカメラボタンをタップします。



QRの情報を読み取り、ポップアップ表示された「2nds.medis.or.jp~」のボタンをタップします。



c)マイナポータルからのアクセス(モバイルデバイスでマイナポータルにアクセスしている場合) マイナポータルにて発行が完了した画面に表示されているリンクをタップしてください。



d) マイナポータルからのアクセス(PC でマイナポータルにアクセスしている場合) Edge を使用してマイナポータルにアクセスし、発行が完了した画面に表示されているリンクをクリックしてください。

1 マイナポータル	⑦ よくあるご質問 凹 おき 野の電子裏先利用申請(資格:)K(的)	webt <mark>久</mark> ログイン中 ≡	×==-		
トップインノ Factors / Sametymole Factometer (Info Lano) 医療等分野の電子署名————————————————————————————————————					PC 画面
◎ 申請が完了しました		2023年12月21日 14時18分 更新			
圖 中語日時 2023年12月20日 13時42分	(点) 申請先機問受付番号 202312201346124323	① 中間先 日本医師会電子部証センター			
 ・ 開発期限について ・ 審査結果を確認できる期間には期間 問究期限 2024年03月21日 14時18分 	見があります。				
中部先からの連絡内容 PR・ための PR PR			2	リンクをクリック	
2023年12月21日 14時13分		۲			
	申請状況照会一覧へ	•			
画面素号:R-02					
デジクル庁	B機 I 第6人情報(単語 I 単用用規約 I ア・ む 2017 Digital Agency, Government of Japan	2858UF4			

Edge 上にパスワード入力画面が表示されます。

アドレスバーをクリックしてください。その後、アドレスバー右側に「田」のアイコン "このページの QR コードを作成"をク リックして QR コードを表示してください。表示された QR コードを a),b)の要領にてモバイルデバイスで読み取ってくだ さい。

"このページの QR コードを作成"のアイコンをク	PC 画面		
The maade-auth.dev.2nds.mistyauth x +			-
← C 💮 https://maadc-auth.dev.2nds.mistyauth.svcapps.net/adc/auth?id=AC_3dc77060-b7f9-4e46-95fc-ca6dc34e	b106&token=MTE5ND 🎞 📳	^ ☆ ↔ ⊄)
通知力ードの本人確認を行うためパスワードを入力してください。 Password OK	QR J-FEZT+V2	Х Мричис= 7920-К	

(3) QR コードを読み取ったモバイルデバイスに、パスワード入力画面が表示されます。

通知カードに従って入力欄にパスワード情報を入力し、「OK」ボタンをタップしてください。

※パスワードを一定回数間違った場合、モバイルデバイスの登録ができなくなります。その場合は、発行した認証 局にお問い合わせください。

 カメラ マ 18:51 100% ### ああ ≜ dev.2nds.mistyauth.svcapps.net ぐ 		
通知カードの本人確認を行うためバスワードを入 力してください。	①パスワード入力	モバイル画面
Password		
	― ②OK ボタンタップ	

(4) 正しいパスワードが入力された場合、ログイン画面が表示されます。

Username 欄に本人 ID(通知カードに記載されている情報)が入力されていることを確認して、「ログイン」ボタン をタップします。

11:52 G 대 및 약 요38% X 홈 matpki suth regisest 2nds media ocip < :	モバイル画面
HPKIセカンド電子証明書管 理・認証プラットフォーム _{アカウントにログイン}	
Username 100001-jpa ログイン	
	ボタンタップ
< 	

(5)本人 ID が正しく認証されたら、認証情報登録開始画面が表示されるので、「登録」ボタンをタップします。



※ここでボタンに「登録」ではなく「セキュリティキーによるサインイン」と表示されている場合は、その QR コードにすでにモ バイルデバイスが登録されていますので、操作を終了してください。 (6) モバイルデバイスによる生体認証の画面が表示されるため、生体認証を実施します。

画面や生体認証の方法は、モバイルデバイスにより異なります。

下記の例は指紋認証です。指紋認証の場合、あらかじめ登録してある指を検知部にセットして、デバイスに指紋認 証をさせます。

※事前にモバイルデバイスに生体認証登録を実施していない場合は、ここで Security Key Error となります。 生体認証の登録を実施したうえで、(2)からやり直してください。

4.3.7.7	ę	19:20	90% 🖸
#B	•	dev.2nds.mistyauth.svcapps.ne	I C
HPI 管理 ファ	< −t 里・	zカンド電子証明書 ・認証プラット -ム	
		Security Key Registration	
		び Touch IDで続けてください。	
		キャンセル	
<		> @ m	G

(7)生体認証登録が完了したら、「ラベル登録画面」が表示されます。 作成した鍵情報をモバイルデバイス側で識別するためのラベル情報を設定する画面ですが、値はシステムで自動設定されるため、特に何も入力せず、「OK」をタップします。

11:52 G 🖿	段 💎 🖬 38%			
X 🗎 mahpki-auth-reg.test.2nds.medis.o				
HPKIセカンド電子証明 理・認証プラットフォー	書管 -ム	モバイ	い画面	
mahpki-auth-reg.test. 2nds.medis.or.jpの内容 容 Please input your registered authenti <u>WebAuthn Authenticator (De</u> キャンセル	cator's label fault Label) OK		OK ボタンタッ	ップ

※この画面で「キャンセル」としても、処理は正常に終了します。

(8) モバイルデバイス側の処理が完了し、完了画面が表示されます。

16:59 G 🖬 🔉 🏵 🗋 38%	
X ● masde-authreg test 2nds medils or jp く : スマートフォンでの手続き(登録)は 完了しました。 スマートフォンのブラウザがを終了してください。	モバイル画面
スマードフォンのフラフリを終了してくたさい。	
<	

【注意】

- ◆生体認証画面(6)で「キャンセル」をタップすると、以下のメッセージが出力されます。 「セキュリティーキーによる認証に失敗しました。」 この場合は、その下にある「再試行してください」ボタンを押して再度生体認証を実施してください。
- ◆モバイルデバイスのブラウザの「戻る」ボタンは使用しないでください。
- ◆登録をリトライしてもうまくいかない場合、モバイルデバイスのブラウザの古い閲覧履歴が原因の場合があります。 モバイルデバイスのブラウザの閲覧履歴のクリア(キャッシュクリア)を実施してください。

操作方法については各モバイルデバイスのブラウザにより異なりますので、各ブラウザの手順を参照ください。

2.4.<u>マイナンバーカード登録</u>

HPKI カードとマイナンバーカードを用いて、マイナンバーカードを本システムの認証デバイスとし登録します。 【必要なもの】HPKI カード、マイナンバーカード、JPKI 利用者ソフト類(※1.3(4)に記載) 全て PC 上で操作します。

PC のブラウザで以下の URL にアクセスします。
 https://mahpki-srv.2nds.medis.or.jp/index.html

※ブラウザは Edge もしくは Chrome を利用してください。

ブラウザ上部の URL 表示欄に上記 URL 文字列を全て入力して Enter キーを押すと、URL が示すサイトにアクセ スされます。



(2) 下記の画面が表示されるので、「HPKIカードを使ってマイナンバーカードを登録する」をクリックします。



(3) 画面が展開されるので、HPKIカードをカードリーダーにセットして「HPKIカードで登録」をクリックします。



(4) HPKIカードでの認証を選択すると HPKI 証明書選択画面が表示されるので、証明書を選択します。 HPKIカードに格納されている証明書が表示されるので、その証明書をクリックしてから「OK」をクリックします。 ※ブラウザにより証明書選択画面の外観は異なります。以下に掲げるのは Edge の場合の画面です。

認証用の証明書の選択 サイト mahpki-auth.2nds.medis.or.jp:443 では資格情報が必要です:	①証明書部クリック	PC 画面
JMACombi30047 HPKI-01-HPKI_V2-forAuthentication-forIndividual 2022/11/1	②OK ボタンクリック	
<u>証明書情報</u> OK キャンセル		

(5)「PIN を入力してください」という画面が表示されるので、HPKI カードの PIN(暗証番号)を入力して「OK」をクリックします。



(6)「HPKI セカンド電子証明書管理・認証プラットフォーム マイナンバーカード登録サイト」画面が表示されます。 表示されている「本人 ID」がご自分のものであることを確認してから、IC カードリーダーから HPKI カードを抜き、 代わりにマイナンバーカードをセットします。

マイナンバーカードをセットしてから「マイナンバーカードを登録」ボタンをクリックします。(※)

HPKIセカンド電子証明書管理・認証プラットフォーム マイナンバーカード登録サイト	PC 画面
本人ID: testc30382 本人 ID を確認	
◆マイナンバーカードがICカードリーダーにセットされている状態で下のボタンをクリックしてください。◆ マイナンバーカードを登録	×

(※) HPKI カードを入れたままこのボタンをクリックすると、「個人番号カードをカードリーダライタにセットし、OK ボタ ンをクリックしてください。」という画面が表示されるので、HPKI カードとマイナンバーカードを差し替えてください。



PC 画面	
-------	--

(7)マイナンバーカードのパスワードを求める画面が表示されるので、マイナンバーカードの利用者証明用のパスワードを 入力して「OK」ボタンをクリックしてください。(署名用のパスワードではありません)



(8)「個人番号カードと通信をしています」と表示された画面が閉じられるまでお待ちください。

個人番与リートと通信でしていより。
++>.+71

(9)「マイナンバーカードの登録が完了しました。ブラウザを終了してください。」と表示されたら完了です。 ブラウザを終わらせてください。



3 HPKI カードまたは代替デバイスを使った認証

HPKI カードまたは代替デバイス(モバイルデバイス/マイナンバーカード)を使った認証(ログイン)の手順を以下に記載します。

※認証機能は、署名サービスなどのシステムで提供されているものから連携するため、HPKI セカンド電子証明書管 理・認証プラットフォーム単独では動作しません。以下には、認証を行うシステムから呼び出された時の、HPKI セカ ンド電子証明書管理・認証プラットフォームの操作のみを記載しております。

一度ログインすると、HPKI セカンド電子証明書管理・認証プラットフォーム側にログイン情報が保存され、ログイン情報の有効期限が来るまでは、そのログイン情報を使うことでログイン操作を不要にする事が可能です。

3.1.<u>ログイン(モバイルデバイスによる認証)</u>

(1) PC のブラウザで FIDO 認証を用いるシステム(電子署名サービス等)にログイン操作を実施します。
 ※ブラウザは Edge (Windows10 に標準で存在しているブラウザ)もしくは Chrome を利用してください。

※スマートフォンのみでは認証できません。

※ログイン画面はシステムにより異なります。

※認証したいシステム側から FIDO 認証用の URL にリダイレクトして頂く必要があります。

(2)本人 ID (Username)の入力画面が表示されますのでご自身の ID を入力して「OK」ボタンをクリックします。



(3) 認証用の QR コードが画面に表示されるので、登録済のモバイルデバイスのカメラを使って QR コードを読み取ります。

HPKIセカンド電子証明書管理・認証プラットフォーム		PC 画面	
100001-jpa に 明に発想したスマートフォンにてのスートや読み込み、スマートフォンに 定定であまい Terry Terry State S	モバイルデバ てこの QR 音	、イスの「カメラ」アプリ 『を読み取ります。	を起動し

モバイルデバイスでの読み取り、および認証サイトへのアクセス方法は以下の手順で実施します。

a) iPhone(iOS)の場合

「カメラ」のアプリを起動します。



モバイル画面

対象の QR コードを読み取り、「"2nds.medis.or.jp"」というポップアップが表示されたら、右下にあるメニュー選択 ボタンをタップします。





※「Safari で開く」ではなく、別のアプリケーションが表示される場合は、Safari で開く設定を行う必要があります。 「設定」から「Safari」を選んでいただき、"デフォルトのブラウザ App"を選択して Safari にチェックを入れてください。

メニュー画面から「Safari で開く」を選択します。

b) Android の場合

「Chrome」アプリを開きます。



モバイル画面

検索キーワードを入力する項目の右にあるカメラボタンをタップします。



QRの情報を読み取り、ポップアップ表示された「2nds.medis.or.jp~」のボタンをタップします。



(4)QRコードを読み取ったモバイルデバイスに、ログイン画面が表示されます。 Username 欄に入力した ID が記載されていることを確認して、「ログイン」ボタンをタップします。



(5)次の画面が表示されるので「セキュリティキーによるサインイン」ボタンをタップします。

11:43 G 🖬 🕅 🕅 🖓 🗣 🖬 39%	
🗙 🗎 mahpikkauth-reguest.2nds.medis.orga < 🗄	モバイル画面
HPKIセカンド電子証明書管 理・認証プラットフォーム	
t00001-jpa 🖻	
セキュリティーキーによるサインイン	ボタンタップ
< —	

(6) モバイルデバイスによる生体認証の画面が表示され、生体認証が実施されます。 画面や生体認証の方法は、モバイルデバイスの種類により異なります。下記の例は指紋認証の場合です。



(7) モバイルデバイスによる生体認証が完了したら、PC の方でログインが成功し、ログイン後の画面が表示されます。 下記はスマートフォンによる認証が完了した画面となります。スマートフォンのブラウザを終了してください。


モバイル画面

3.2.<u>ログイン(HPKI カードによる認証)</u>

- (1) HPKI 認証を用いるシステム(電子署名サービス等)でログイン操作を実施します。
 ※ログイン画面はシステムにより異なります。
 ※認証したいシステム側から HPKI 認証用の URL にリダイレクトして頂く必要があります。認証したいシステム側での対応が必要となります。
- (2) HPKI 証明書選択画面が表示されるので証明書を選択し、カードの PIN(暗証番号)入力を求められるので、 PIN(暗証番号)を入力します。
- (3) HPKIカードによるログインが成功し、ログイン後の画面が表示されます。

3.3.ログイン(マイナンバーカードによる認証)

- (1) JPKI 認証を用いるシステム(電子署名サービス等)でログイン操作を実施します。
 ※ログイン画面はシステムにより異なります。
 ※認証したいシステム側から JPKI 認証用の URL にリダイレクトして頂く必要があります。認証したいシステム側での対応が必要となります。
- (2)証明書選択画面が表示されるので、JPKIの証明書を選択します。※JPKI利用者証明書連携ツールを導入していない場合、証明書の選択表示が行われずログインに失敗します。
- (3) 証明書の PIN(暗証番号)入力を求められるので、 PIN(暗証番号)を入力します。 マイナンバーカードの PIN は利用者証明用パスワード(数字 4 桁)を入力してください。
- (4)マイナンバーカードによるログインが成功し、ログイン後の画面が表示されます。

3.4.<u>ログアウト</u>

HPKI 認証を用いるシステムでログイン後、ログアウトを実施すると、HPKI セカンド電子証明書管理・認証プラットフォ ーム側に保存されているログイン情報が破棄されます。

その後にまたログインする場合は、再度認証が必要になります。

4 署名をするとき

上記で認証した認証情報を使って HPKI セカンド電子証明書による電子署名を行う事が可能です。電子署名を行う システムから認証情報と署名を行う対象データを HPKI セカンド電子証明書管理・認証プラットフォームに連携する必要が あります。操作等については、電子署名を行うシステムに従ってください。

5 更新するとき

5.1.<u>HPKI カードを更新する場合</u>

HPKIカードには有効期限があります。期限は HPKIカードに記載されていますのでご確認ください。

期限が切れる前に、各認証局に更新手続きをしますが、その場合、HPKIカードの更新にあわせ HPKI セカンド電子 証明書は自動的に更新されますので、利用者側での操作は不要です。

5.2. モバイルデバイスを機種変更する場合

認証に使っているスマートフォン等のモバイルデバイスを機種変更する場合は、以下の2通りの手順が可能です。 (a)新旧のモバイルデバイスを用いる手順

(b)HPKI カードと新しいモバイルデバイスを用いる手順

古いモバイルデバイスが故障などで使えなくなっている場合でも、(b)の手順で機種変更が可能です。 いずれの場合も、PC での操作が必要になります。

(a)新旧のモバイルデバイスを用いる手順

新旧のモバイルデバイスを用いる手順は、

・まず旧モバイルデバイスで QR コード・生体認証で認証する

・ついで新モバイルデバイスで QR コード・生体認証を行って新しいものに認証を切り替える

という手順となります。

QR コード読み取りと生体認証を2回行うことになりますので、お間違いのないようにお願いいたします。 【必要なもの】PC、古いモバイルデバイス、新しいモバイルデバイス

(1) PC のブラウザで以下の URL にアクセスします。

https://mahpki-srv.2nds.medis.or.jp/index.html

※ブラウザは Edge (Windows10 に標準で存在しているブラウザ) もしくは Chrome を利用してください。

ブラウザ上部の URL 表示欄に上記 URL 文字列を全て入力して Enter キーを押すと、URL が示すサイトにアクセスされます。

	🔄 新しいタブ	x +		-
	C A C	https://mahpki-srv.2nds.medis.or.jp/index.html	ζ <u>=</u>	Ē
Ь ð	すすめサイト 🎦 about	tabs		ि २

PC 画面

(2) 下記の画面が表示されるので、「スマートフォンを変更する」をクリックします。



PC 画面

(3) 画面が展開されるので、「スマートフォン変更」をクリックします。



(4)以下の画面が PC に表示されるので、入力欄にご自身の ID を入力して「OK」をクリックします。



(5) PC 画面に QR コードが表示されるので、古いモバイルデバイスのカメラで QR コードを読み取ります。 (まず登録済の古いデバイスで認証を行います)



モバイルデバイスでの読み取り、および認証サイトへのアクセス方法は以下の手順で実施します。

a) iPhone(iOS)の場合

「カメラ」のアプリを起動します。



対象の QR コードを読み取り、「"2nds.medis.or.jp"」というポップアップが表示されたら、右下にあるメニュー選択 ボタンをタップします。



メニュー画面から「Safari で開く」を選択します。



※「Safari で開く」ではなく、別のアプリケーションが表示される場合は、Safari で開く設定を行う必要があります。 「設定」から「Safari」を選んでいただき、"デフォルトのブラウザ App"を選択して Safari にチェックを入れてください。

b) Android の場合

「Chrome」アプリを開きます。



モバイル画面

検索キーワードを入力する項目の右にあるカメラボタンをタップします。



QRの情報を読み取り、ポップアップ表示された「2nds.medis.or.jp~」のボタンをタップします。



(6) QR コードを読み取ったモバイルデバイスに、ログイン画面が表示されます。
 Username 欄に入力した ID が記載されていることを確認して、「ログイン」ボタンをタップします。



(7)次の画面が表示されるので「セキュリティキーによるサインイン」ボタンをタップします。



(8)モバイルデバイスによる生体認証の画面が表示され、生体認証が実施されます。

画面や生体認証の方法は、モバイルデバイスにより異なります。

下記の例は指紋認証です。指紋認証の場合、あらかじめ登録してある指を検知部にセットして、デバイスに指紋認 証をさせます。



(9) 古いモバイルデバイス画面に「処理が完了しました」と表示されます。



(10) 同時に、PC の画面に、「デバイスがすでに登録済みとなっています。現在のデバイスを削除して再度登録をし直しますか?」と表示されます。

ここで「はい」を選択します。

A LACA	PC 画面
HPKIセカンド電子証明書管理・認証プラットフォーム	
testc20946 😖	
デバイスがすでに置録逐みとなっています。 現在のデバイスを制除して再度登録をし直しますか?	
はいといえ	――― 「けい」ボタンクトック

【注意】ここで「はい」を選択すると、以降(11)から(14)までの手順を途中で終了した場合(QRコードを読み取ら なかった場合や、処理途中で「キャンセル」を選択した場合、「Security Key Error」が表示されてエラーにな った場合など)新旧どちらのモバイルデバイスでも認証ができなくなります。 その場合は、「(a)新旧のモバイルデバイスを用いる手順」での機種変更はできなくなりますので「(b) HPKI カードと新しいモバイルデバイスを用いる手順」に従い、HPKI カードを用いて再登録を実施してくださ い。

(11) PC の画面に QR コードが表示されます。

新しいモバイルデバイスのカメラで、このQRコードを読み取ります。

(以降、(16)まで新しいモバイルデバイス操作の画面説明となります)

yauth.svcapps.net/auth/realms/r	rediauth/login-actions/authenticate?execution=88060944-f6de-41e1-819c-639558c127e68chient_id=FIDO&tab_id=r2iA_t
НРК	ロカンド電子証明書管理・認証プラットフォーム
	testc20946 🖻
	Tripperframade auth.dev.2rds.misryauth.av.capps.ret/adc/auth?id=4950c;957-656c- 45c: 4756
	4114171788988esker=M0Y80Ts20TMwZTM5Ny62NTHyLT8ZCMe0T6MC00MTE0 MTex4eYeYyZMsMAMasyM0YLEGLeAADEwOQXQArDaM0TT7aGVe6GMyMDk 0Ng==
	+r>21

	PC 画面	
モバイルデバイスの	「カメラ」アプリを起動	してこの
QR 部を読み取りま	す。	
モバイルデバイスの排	操作方法については	(4)と
同じ要領にて操作で	をしてください。	

(12)QRコードを読み取ったモバイルデバイスに、ログイン画面が表示されます。

Username 欄には本人 ID が表示されています。値が正しいことを確認して「ログイン」ボタンをタップします。



(13)認証情報登録開始画面が表示されるので、「登録」ボタンをタップします。

11:52 G 🖿 X 🔒 mahpki-auth-reg.test	% ♥ û 38% Indamedia.or.jp <		モバイル画面
HPKIセカンド電 理・認証プラッ↓ ₽セキュリテ	子証明書管 ~ フォーム ィーキーの登録		
	ŝi 🔶	ボ	タンタップ
< 4	•		

(14) モバイルデバイスによる生体認証の画面が表示されるため、生体認証を実施します。 画面や生体認証の方法は、モバイルデバイスにより異なります。

下記の例は指紋認証です。指紋認証の場合、あらかじめ登録してある指を検知部にセットして、デバイスに指紋認証をさせます。

4 л×? ♥	18:48	33% 🛄
3.88 🔒	dev.2nds.mistyauth.svcapps.	net Č
HPKH 管理・	zカンド電子証明書 認証プラット	
24-	►ZA Security Key Registration	
	Youch IDで続けてください。	
	キャンセル	
<	> 🖞 🕮	0

(15) 生体認証登録が完了したら、「ラベル登録画面」が表示されます。

作成した鍵情報をモバイルデバイス側で識別するためのラベル情報を設定する画面ですが、値はシステムで自動設定されるため、特に何も入力せず、「OK」をタップします。



(16) モバイルデバイス側の処理が完了し、完了画面が表示されます。 モバイルデバイス側のブラウザを閉じてください。

17:00 G 🖬	¥, ⊕ 1 37% • < :
スマートフォンでの手続き(登録)は 完了しました。 操作したPCにて登録が完了している。 確認してスマートフォンのブラウザ考 終了してください。	ことを
※ブラウザの戻るボタンを押すと、 登録情報が壊れる可能性があるため 戻るボタンは押さないでください。	5.
<	

同時に、PC 側にも完了画面が表示されます。



※新しいモバイルデバイスが登録されると古いモバイルデバイスでの認証は出来なくなります。

(b)HPKIカードと新しいモバイルデバイスを用いる手順

HPKIカードと新しいモバイルデバイスで実施します。 モバイルデバイスの情報が新しいもので上書きされ、古いモバイルデバイスの利用は停止されて新しいモバイルデ バイスで認証できるようになります。

【必要なもの】PC、IC カードリーダライタ、新しいモバイルデバイス、HPKI カード

- (1) PC で、2.1 の手順を(1)~(6) まで実施します。
- (2)「デバイスがすでに登録済みとなっています。現在のデバイスを削除して再度登録をし直しますか?」と表示されます。 ここで「はい」を選択します。

HPKIセカンド電子証明書管理・認証プラットフォーム		PC画面
testc20946 🖻		
デバイスからに国際部分ではつくいよう。 現在のデバイスを制除して再変登録をし直しますか?		
	- 「はい」ボタン	クリック

(3) 2.1の手順の(7)以降を実施します。新しいモバイルデバイスで、登録作業を実施します。

(c)マイナンバーカードと新しいモバイルデバイスを用いる手順

マイナンバーカードと新しいモバイルデバイスで実施します。

モバイルデバイスの情報が新しいもので上書きされ、古いモバイルデバイスの利用は停止されて新しいモバイルデバイスで認証できるようになります。

※マイナポータル経由申請した利用者が対象となります

【必要なもの】PC、IC カードリーダライタ、新しいモバイルデバイス、HPKI 証明書と紐づけられたマイナンバーカード

- (1) PC で、2.2 の手順を(1) ~ (6) まで実施します。
- (2)「デバイスがすでに登録済みとなっています。現在のデバイスを削除して再度登録をし直しますか?」と表示されます。 ここで「はい」を選択します。



(3) 2.2 の手順の(7)以降を実施します。新しいモバイルデバイスで、登録作業を実施します。

5.3.マイナンバーカード(利用者証明書)を更新する場合

マイナンバーカードに格納される利用者証明書が更新された場合、更新後の認証時に、自動的に登録状況が更新されますので、利用者側での操作は不要です。

6.1.日常の運用時

6.1.1. HPKI カードを紛失した

HPKI カードを紛失した場合は、HPKI カードを発行した認証局に紛失届を出してください。紛失の状況は正確に 伝えてください。その状況により、HPKI カードの証明書のみを失効とするか、モバイルデバイスを使った認証の HPKI セ カンド電子証明書まで失効とするか、認証局側が判断します。

HPKI カードの証明書のみを失効とする場合、モバイルデバイスを使った認証は今まで通り利用できます。

6.1.2.モバイルデバイスを紛失した

認証に用いているモバイルデバイスを紛失した場合は、HPKIカードを発行した認証局に失効依頼を出してください。 紛失の状況は正確に伝えてください。その状況により、HPKIセカンド電子証明書の失効や登録したモバイルデバイスの認証情報を削除するかは、認証局側が判断します。

モバイルデバイスの認証情報を削除しても、HPKIカードを使った認証は今まで通り利用できます。また、あらたなモバイルデバイスを用意して登録しなおす事は可能です。

6.1.3.マイナンバーカードを紛失した

マイナンバーカードを紛失した場合は、マイナンバーカードの運用に従って機能停止のお手続きを行ってください。

6.1.4. 認証エラーになる

HPKI カードとモバイルデバイスまたはマイナンバーカードのいずれで認証しようとしてもエラーになる場合は、HPKI カードの有効期限を確認してください。有効期限を過ぎると認証はできなくなりますので、認証局に連絡して更新手続きを行なってください。

有効期限を過ぎていないのに認証エラーになる場合は、認証局にお問い合わせください。

モバイルデバイスの認証でのみエラーになる場合は、生体認証がうまくいっていない可能性があります。生体認証はモ バイルデバイスの読み取り状態や、指紋などの生体の状態によって認識率が変わります。どうしても生体認証がうまくい かない場合は、まずは HPKI カードによる認証に切り替えると共に、モバイルデバイスの再登録を試みてください。

6.2. モバイルデバイス登録時

6.2.1.送付された QR コードの有効期限が切れた

認証局から送付する QR コードには有効期限があります。期限内にアクセスしないとモバイルデバイス登録ができなくなりますので、アクセスしないまま期限が切れた場合は、発行した認証局にお問い合わせください。

6.2.2.パスワードの入力を間違って登録ができない

通知カードによるモバイルデバイスの登録時はパスワードの入力が必要です。パスワードを一定回数間違った場合、 モバイルデバイスの登録ができなくなります。その場合は、発行した認証局にお問い合わせください。

6.3.マイナンバーカード登録時

6.3.1.マイナンバーカード登録ボタンが効かない

2.3(6)の画面で、「マイナンバーカードを登録する」ボタンをクリックしても何も反応が無い場合は、以下のいずれかである可能性があります。

(a)以下のソフトウェアがインストールされていない

・JPKI利用者クライアントソフト

・利用者クライアントソフト(Edge/Chrome ブラウザ利用版)

公的個人認証サービスのポータルサイトから Windows 版をダウンロード・インストールしてください。

(b)拡張機能をインストールしたブラウザとは違うブラウザを用いている

利用者クライアントソフト(Edge/Chrome ブラウザ利用版)インストール時に指定した方のブラウザで操作を実施してください。

(c)ブラウザ上で拡張機能が有効になっていない

ブラウザ右上の「…」(または縦の「・」3つ)をクリックして「拡張機能」→「拡張機能の管理」で「利用者位アウト ソフト Edge/Chrome」が有効になっているか確認してください。

6.4.その他、わからないことがあったら

利用している時にわからないことがある場合は、HPKIカードを申し込んだ認証局にお問い合わせください。

本書で用いる主な用語を以下にまとめます。

用語	意味
HPKI	保健医療福祉分野の公開鍵基盤(Healthcare Public Key Infrastructure)
	の略称で、医療現場において、公的資格の確認機能を有する電子署名や電子認証
	を行う仕組み。以下も参照のこと。
	https://www.medis.or.jp/8_hpki/about.html
HPKI 証明書	HPKIの認証局にて発行する、本人および資格を証明するための電子証明書。
	電子証明書は、HPKIカード(ICカード)内に格納して利用される。
HPKI 認証	HPKIカードに含まれる証明書を用いた認証方式。
HPKI セカンド電子証	HPKI カードに格納される HPKI 証明書と連携した、鍵管理システムで管理する第二
明書	の証明書。
セカンド鍵	HPKI セカンド電子証明書に含まれる署名用の鍵。
FIDO 認証	FIDO=Fast IDentity Online の略。
	従来のパスワードに代わる認証技術のひとつで、生体認証をモバイルデバイス上で使う
	ことでパスワードのやり取りが不要になる認証方式。
	この認証方式の最新の規格が「FIDO2」である。
ЈРКІ	日本政府が提供している公的個人認証サービス。
	マイナンバーカードに格納されている署名用電子証明書および利用者証明用電子証
	明書を使用して様々なサービスの本人確認に活用される。
利用者証明書·	マイナンバーカードに格納されている証明書のうち、認証用途に利用される証明書。証
利用者証明用電子証	明書には住基4情報は含まれず、証明書を識別するランダムな文字列の情報のみ記
明書	載されている。
利用者クライアントソフ	公的個人認証サービスにて配布しているマイナンバーカード用の IC カードドライバおよ
ト	び証明書確認等のアプリケーションのセット
利用者クライアントソフ	Edge/Chrome からマイナンバーカードにアクセスするためのアプリケーション。動作させ
ト (Edge/Chrome	るためには Chrome ウェブストアからブラウザ拡張機能「利用者クライアントソフト
ブラウザ利用版)	Edge/Chrome」のインストールも必要

8.1.アカウントが無効です。管理者に連絡してください。

[表示画面]

HPKIセカンド電子証明書 管理・認証プラットフォ ーム
アカウントにログイン
アカウントが無効です。管理者に連絡してください。
Username
TESTC30383
ログイン

[原因]

・当該ユーザが無効になっている(削除されている)。

[対策]

・各認証局に本人 ID (医籍登録番号、薬剤師登録番号等)を連絡の上、ユーザ登録がされているか問い合わせ してください。

8.2. WebAuthn is not Supported by this browser.

[表示画面]



[原因]

・ブラウザまたは OS が FIDO2 をサポートしていない。

・iCloud キーチェーンが有効になっていない。(iPhone)

[対策]

- ・iPhone の場合は Safari、Android の場合は Chrome のブラウザを使用してください。
- ・OSを最新のものにバージョンアップしてください。
- ・iCloud キーチェーンを有効にしてください。

8.3.セキュリティーキーの登録結果が無効です。

[表示画面]



[原因]

デバイス登録時に以下のいずれかの事象が発生した。

- ・生体認証に失敗した。
- ・生体認証を実施している最中にキャンセル操作をした。
- ・ブラウザまたは OS が FIDO をサポートしていない。
- ・iCloud キーチェーンが有効になっていない。(iPhone)
- ・スマートフォンに生体認証情報を登録していない。
- ・「TouchID とパスコード」で「パスコードをオフにする」設定になっている。(iPhone)

[対策]

- ・iPhone の場合は Safari、Android の場合は Chrome のブラウザを使用してください。
- ・OSを最新のものにバージョンアップしてください。
- ・iCloud キーチェーンを有効にしてください。
- ・ブラウザのキャッシュをクリアして(10.1参照)もう一度最初から操作してください。
- ・再度生体認証を実施してください。
- ・スマートフォン本体に生体認証が登録されていない場合は、生体認証を登録してください。
- ・「設定」→「TouchIDとパスコード」から「パスコードをオンにする」操作を実施してください。

8.4.<u>NotReadableError: An unknown error occured while talking</u> to the credential manager.

[表示画面]



[原因]

・生体認証後、不明なエラーが発生した。

・ブラウザまたは OS が FIDO をサポートしていない。

[対策]

・デバイス登録作業、認証作業を一からやり直してください。 ・何回かやり直しても同じエラーになる場合は、お使いのスマートフォンの OS またはブラウザが FIDO2 をサポートしてい ないことが考えられます。お使いのスマートフォンの機種の機能を確認してください。 また、iPhone の場合は Safari、Android の場合は Chrome のブラウザを使用してください。

8.5. NotAllowedError: Operation failed.

[表示画面]



[原因]

- ・生体認証に連携できていない。
- ・ブラウザが FIDO2 をサポートしていない。
- ・iCloud キーチェーンが有効になっていない。(iPhone)

[対策]

- ・iPhone の場合は Safari、Android の場合は Chrome のブラウザを使用してください。
- ・iCloud キーチェーンを有効にしてください。

8.6.セキュリティーキーによる認証に失敗しました。



[原因]

認証時に以下のいずれかの事象が発生した。

・鍵登録したスマートフォンと違うスマートフォンで認証している。

・入力した本人 ID が間違っている。

・登録済のスマートフォン内の鍵を削除してしまった。

(iPhone:「設定」→「パスワード」で表示されるパスキーを削除してしまった)

(Android:「設定」→「セキュリティ」→「画面ロック」を「なし」または「スワイプ」に変更してしまった)

※変更した時点で鍵が削除されてしまうため、元に戻しても鍵は戻りません。

・ブラウザが FIDO2 をサポートしていない。

・生体認証に失敗した。

・生体認証を実施している最中にキャンセル操作をした。

・「TouchID とパスコード」で「パスコードをオフにする」設定になっている。(iPhone)

[対策]

・登録したスマートフォンでアクセスしているか確認してください。

・入力した本人 ID が正しいか確認してください。

・iPhone の場合は Safari、Android の場合は Chrome のブラウザを使用してください。

・ブラウザのキャッシュをクリアして(10.1参照)もう一度最初から操作してください。

・スマートフォン内の鍵を削除してしまった場合は、再登録が必要になります。

HPKI カード、または HPKI 証明書と紐づけられたマイナンバーカードをお持ちの方は、利用者マニュアル 5.2(b)、 または 5.2(c)の手順に従って、再度登録してください。

カードをお持ちでない方は、セカンド鍵を発行した各認証局にお問い合わせください。

8.7.<u>NotAllowedError: The 'navigator.credentials.create' API is</u> <u>only permitted in applications with the</u> <u>'com.apple.developer.web-browser' entitlement.</u>

[表示画面]



[原因]

・Apple で認証されていないブラウザを使っている。

[対策]

・iPhone の場合は Safari、Android の場合は Chrome のブラウザを使用してください。

8.8.<u>NotAllowedError: The operation either timed out or was not</u> <u>allowed.</u>

[表示画面]



[原因]

・ブラウザが FIDO2 をサポートしていない。

[対策]

・iPhone の場合は Safari、Android の場合は Chrome のブラウザを使用してください。

8.9.<u>NotSupportedError: The specified 'userVerification'</u> requirement cannot be fulfilled by this device unless the device is secured with a screen lock.

[表示画面]



[原因]

・画面ロックに生体認証を設定していない。(Android)

[対策]

・「設定」→「セキュリティ」→「画面ロック」を選択して、「PIN」を選択してください。 選択後、生体認証(指紋、顔など)をスマートフォン内に設定してください。

8.10. <u>403 Forbidden</u>

[表示画面]



[原因]

・何らかの理由で接続が禁止されているネットワークから接続されている。

[対策]

・スマートフォンでアクセスしていてこのエラーが出る場合は、Wi-Fi 接続ではなくネットワークキャリアを使った接続を行ってください。

8.11. <u>mahpki-auth.2nds.medis.or.jp でセキュリティキーを使用す</u>る

[表示画面]



[原因]

- サーバ側に記録してあるセカンド鍵情報とスマートフォン内に登録されているセカンド鍵情報が異なる。 (このエラーが表示される利用者は、FIDO 鍵がサーバ側に登録済みです)
- ・認証開始時に入力した Username(本人 ID)が、スマートフォン内の FIDO 鍵と一致していない
 - (認証開始時に誤った Username を入力した)

・FIDO 鍵情報がスマートフォンから削除されている

※デバイス保護機能を無効化したり変更したりすると、スマートフォン内の FIDO 鍵情報が削除される場合があります

[対策]

・認証開始時に入力した Username がご自身のものであるか確認してください。

・ご自身で FIDO 認証に登録したスマートフォンを使用していることを確認してください。

・上記2点が問題なく、かつスマートフォンのデバイス保護機能を変更していた場合は、FIDO鍵情報がスマートフォンから削除されていると判断されます。

その場合は、FIDO 鍵の再登録が必要になります。HPKI カードを保有している場合は、利用者マニュアルの「5.2 (b) HPKI カードと新しいモバイルデバイスを用いる手順」、HPKI 証明書が紐づけられているマイナンバーカードを 保有している場合は、利用者マニュアルの「5.2(c) マイナンバーカードと新しいモバイルデバイスを用いる手順」に 従ってデバイスの登録を実施してください。カードを保持していない利用者は認証局に問い合わせてください。

8.12. <u>mahpki-auth.2nds.medis.or.jp にサインインする方法を選択</u> してください。

[表示画面]



[原因]

- ・「TouchID とパスコード」で「パスコードをオフにする」設定になっている
- ・サーバ側に記録してあるセカンド鍵情報とスマートフォン内に登録されているセカンド鍵情報が異なる。 ・認証開始時に入力した Username (本人 ID) が、スマートフォン内の FIDO 鍵と一致していない (認証開始時に誤った Username を入力した)
 - ・FIDO 鍵情報がスマートフォンから削除されている
 - ・FIDO 鍵の登録完了画面(処理が終了しました)で戻るボタンを押したうえ、再度登録行為を実施した。

[対策]

- ・「設定」→「TouchID とパスコード」からパスコードの設定を確認し、「パスコードをオンにする」と表示されている場合 は、タップしてパスコードをオンにした後、登録・認証操作をやりなおしてください。「パスコードをオフにする」と表示され ている場合は、さらに下記の確認をお願いします。
- ・認証操作時にこのエラーが出る場合は、認証開始時に入力した Username がご自身のものであるか確認してくだ さい。
- ・ご自身で FIDO 認証に登録したスマートフォンを使用していることを確認してください。
- ・「設定」→「パスワード」を選択して、ご自身のUsernameが記載された鍵情報があるか確認してください。ない場合 は、FIDO 鍵情報がスマートフォンから削除されていると判断されます。
- その場合は、FIDO 鍵の再登録が必要になります。HPKI カードを保有している場合は、利用者マニュアルの「5.2 (b) HPKI カードと新しいモバイルデバイスを用いる手順」、HPKI 証明書が紐づけられているマイナンバーカードを 保有している場合は、利用者マニュアルの「5.2(c) マイナンバーカードと新しいモバイルデバイスを用いる手順」に 従ってデバイスの登録を実施してください。カードを保持していない利用者は認証局に問い合わせてください。
- ・以上の確認で全て問題がない場合は、FIDO 鍵の登録時に戻るボタンを押したうえ、再度登録行為を実施したことが原因である可能性があります。

この場合も、FIDO 鍵の再登録が必要になります。HPKI カードを保有している場合は、利用者マニュアルの「5.2 (b) HPKI カードと新しいモバイルデバイスを用いる手順」、HPKI 証明書が紐づけられているマイナンバーカードを 保有している場合は、利用者マニュアルの「5.2(c) マイナンバーカードと新しいモバイルデバイスを用いる手順」に 従ってデバイスの登録を実施してください。カードを保持していない利用者は認証局に問い合わせてください。

8.13. 画面のロックを使用する



[原因]

・スマートフォンに登録した生体認証情報が削除されている(または登録されていない)

- ・FIDO 認証時に生体認証を一定回数失敗している
- ・FIDO 認証時に「PIN を使用」をタップした

[対策]

・スマートフォンに設定されている PIN を入力する事で FIDO 認証を行う事が可能ですが、セキュリティを確保するため、スマートフォンに生体認証の登録を実施してください。

8.14. <u>パスコードで続ける</u>

[表示画面]



[原因]

・スマートフォンに登録した生体認証情報が削除されている(または登録されていない)

- ・FIDO 認証時に生体認証を一定回数失敗している
- ・FIDO 認証時に PIN 入力をタップした

[対策]

・スマートフォンに設定されている PIN を入力する事で FIDO 認証を行う事が可能ですが、セキュリティを確保するため、スマートフォンに生体認証の登録を実施してください。

8.15. <u>Cookie が見つかりません。</u>

[表示画面]

HPKIセカンド電子証明書 管理・認証プラットフォ ーム
申し訳ございません
Cookieが見つかりません。 ブラウザで Cookie が有効になっ ていることを確認してください。

[原因]

・ブラウザで Cookie をブロックする設定になっている。

・Android 端末の場合、Chromeの「サイトの設定」の「デバイス上のサイトデータ」の保存が OFF になっている。

[対策]

・iPhone の場合は「設定」→「Safari」を選択し、設定画面中央あたりの「プライバシーとセキュリティ」欄の「すべての Cookie をブロック」が ON になっている場合は OFF にしてください。

・Android の場合は Chrome を開き、画面右上のメニューマークをクリックして、「設定」→「サイトの設定」→ 「Cookie」として「すべての Cookie をブロックする」にチェックがある場合はそれ以外を選択してください。

※Android 端末によっては「すべての Cookie をブロックする」設定が無い場合があります。

また「設定」→「サイトの設定」→「デバイス上のサイトデータ」」を選択し、「サイトによるデバイスへのデータの保存を許可しない」になっている場合は ON にして「サイトはデバイスにデータを保存できます」にしてください。

8.16. (画面が真っ白または真っ黒になる)

[表示画面]



[原因]

・ブラウザで JavaScript を OFF にしている。

・スマートフォンに「フィルタリングアプリ」「コンテンツブロッカー」等をインストールして使っている

・携帯電話会社のフィルタリングサービスを使っている

[対策]

・ブラウザの設定で JavaScript を使えるようにしてください。

iPhoneの場合は「設定」→「Safari」を選択し、いちばん下の「詳細」→「JavaScript」がOFF になっている場合は ON にします。

・Android の場合は Chrome を開き、画面右上のメニューマークをクリックして、「設定」→「サイトの設定」→ 「JavaScriot」を選択し「JavaScript ブロック」となっている場合は ON にします。

・フィルタリングアプリやサービスをお使いの場合は、以下の URL をフィルタリング対象からはずしてください。

https://maadc-auth.2nds.medis.or.jp/ https://mahpki-auth.2nds.medis.or.jp/

8.17. <u>スマートフォンの画面に QR コードが表示される</u>



[原因]

- ・登録しているスマートフォンと違うスマートフォンで認証しようとしている
- ・生体認証の設定の解除を行った
- ・「パスワード」に保存されている鍵を削除してしまった(iPhone)

[対策]

・本システムに登録したスマートフォンにて認証してください。

・HPKIカードまたはマイナンバーカードを使用してスマートフォンの再登録を実施してください。カードがなく登録できない場合は各認証局へ問合せ願います。

8.18. <u>すでにこのセッションで異なるユーザーxxxxxx として認証されて</u> います。

[表示画面]

HPKIセカンド電子証明書 管理・認証プラットフォ ーム 申し訳ございません ^{すでにこのセッションで異なるユーザー'testc30442'として認 ^{証されています。まずログアウトしてください。}}

[原因]

・1 台のスマートフォンを複数のユーザの認証デバイスとして使っている場合、ユーザの認証に使った後に別のユーザの認証にも使おうとした。

[対策]

・1 台のスマートフォンを複数ユーザの認証デバイスとして使う場合は、認証の都度、ブラウザの「履歴」をクリアするよう にしてください。

8.19. <u>無効なアクセス、または、URL の有効期限切れにより処理を中</u> <u>断します。</u>

[表示画面]

無効なアクセス、または、URLの有効期限切れに より処理を中断します。 発行した認証局にお問い合わせください。

[原因]

・認証局から送付された登録用 QR コードの期限が切れている。または新しい QR コードが発行されて無効になっている。

・HPKI カード/マイナンバーカードによるデバイス登録時に表示される登録用 QR コードを所定の時間(10分)を過ぎて読み込んだ。

・デバイス認証時に表示される QR コードを所定の時間(10分)を過ぎて読み込んだ。

[対策]

・認証局から送付された登録用 QR コードを読み込んでこのエラーが出た場合は、QR コードの有効期限を確認してください。有効期限内であるにもかかわらずこのエラーになった場合は、発行した認証局にお問い合わせください。

有効期限が切れていた場合は、発行した認証局に再発行を依頼してください。

・デバイス登録時や認証時に表示される QR コードは所定の時間内に読み込むようにしてください。時間を過ぎてしまった場合は操作を最初からやり直してください。
8.20. <u>405 Method Not Allowed</u>

[表示画面]

405 Method Not Allowed

許可されていないメソッドを使用 しようとしました

発生日時: 2024/4/24 14:20:46 MA-T-T アクセス元:

by HPKI-KAGURA

[原因]

・ブラウザの「戻る」ボタンで操作をやり直した。

・ブラウザから処理中に誤ったリクエストが送付された。

・Android 端末でデバイス登録時、スマートフォンのカメラで QR コードを読み取った後に本人 ID が自動で入力枠に 入らない事象が発生すると、登録作業の最後に本画面が表示されます。

[対策]

・一度ブラウザを終了してデバイスの登録作業をはじめからやり直してください。

但し、登録作業の最後(「ラベル登録画面」で「OK」をタップした後)でこの画面が表示された場合は、登録作業 自体は正常に終了していますので、やり直す必要はありません。

・本人 ID が自動で入力枠に入らなかった場合、再度カメラで QR コードを読み込んでください。

※再発する場合、10.1ブラウザのキャッシュクリアを実施して再度登録作業をやり直してください。

※デバイス登録が完了している場合、登録画面がスキップされて終了します。

8.21. パスキーを管理する方法を選択してください

♣,サインイン ↓

[原因]

[表示画面]

・iPhone(iOS17 以降)で、「パスワードオプション」で「パスワードとパスキーを自動入力」が ON になっていない。 または、「次の提供元からのパスワードとパスキーを使用」の部分が全て OFF になっている。

[対策]

・「設定」→「パスワード」→「パスワードオプション」で「パスワードとパスキーを自動入力」を ON にしてください。

・また、「次の提供元からのパスワードとパスキーを使用」で「iCloud キーチェーン」を ON にしてください。

8.22. <u>Autheticator:パスキーを追加できませんでした</u>

[表示画面]



[原因]

・iCloud キーチェーンの設定が有効になっておらず、別の Autheticator アプリが起動している。

[対策]

・「設定」→「パスワード」→「パスワードオプション」で「パスワードとパスキーを自動入力」をON にしてください。 ・また、「次の提供元からのパスワードとパスキーを使用」で「iCloud キーチェーン」をON にしてください。

8.23. 利用可能なパスキーがありません

[表示画面]



[原因]

Android 端末で、サーバ側に記録してあるセカンド鍵情報とスマートフォン内に登録されているセカンド鍵情報が異なる。

・認証開始時に入力した Username (本人 ID) が、スマートフォン内の FIDO 鍵と一致していない

(認証開始時に誤った Username を入力した)

・FIDO 鍵情報がスマートフォンから削除されている

Android 端末においては、「設定」→「セキュリティとプライバシー」→「デバイスのロック解除」で「画面ロック」選択し、

「新しい画面ロックの選択」で「なし」または「スワイプ」に変更すると、登録済の情報が削除されます。

[対策]

- ・認証開始時に入力した Username がご自身のものであるか確認してください。
- ・ご自身で FIDO 認証に登録したスマートフォンを使用していることを確認してください。
- ・鍵情報を削除してしまった場合は、FIDO 鍵の再登録が必要になります。HPKIカードを保有している場合は、利用 者マニュアルの「5.2(b)HPKIカードと新しいモバイルデバイスを用いる手順」、HPKI 証明書が紐づけられている マイナンバーカードを保有している場合は、利用者マニュアルの「5.2(c)マイナンバーカードと新しいモバイルデバイ スを用いる手順」に従ってデバイスの登録を実施してください。カードを保有していない利用者は認証局に問い合わ せてください。

8.24. ログインできません。クレデンシャルのセットアップが必要です。

[表示画面]

HPKIセカンド電子証明書 管理・認証プラットフォ ーム

申し訳ございません

ログインできません。クレデンシャルのセットアップが必要 です。

[原因]

・デバイス単独 FIDO 認証を利用している場合、未登録のデバイスで単独 FIDO 認証を実施しようとした。

[対策]

・システムに登録したデバイスで認証を実施してください。 認証用のデバイスをまだ登録していない場合は登録を行ってください。

9 PC でのメッセージ

9.1.このサイトは安全に接続できません

[表示画面]



[原因]

- ・HPKI(JPKI)認証時、ICカードの PIN を求める画面が表示されずに表示画面になった場合、ICカードの読み取り に失敗しています。
- ・IC カードの証明書の有効期限が切れている。
- ・IC カードの証明書情報を中継しない Proxy サーバを経由して接続している。

[対策]

・IC カードリーダーが PC に接続され、IC カードドライバ等の必要なソフトウェアがインストール済であるか確認してください。

(確認方法については10.2を参照してください)

- ・IC カードは有効なものであるか(期限切れカードでないか等)確認してください。
- ・Proxy サーバを経由せずに直接アクセスするか、SSL クライアント認証のリクエストも中継する Proxy サーバに変更 して接続してください。
- ・ウィルス対策ソフトウェアが Web ブラウザの機能を制限して IC カードが利用できない場合があります。ウィルス対策ソフトウェアの設定を変更するか、ソフトウェア自体を終了させて動作を確認してください。
- ・非接触型の IC カードリーダライタを使用している場合、金属板上にリーダライタを置くと IC カードが読み取れないケースがあります。木やプラスチックなど、金属でないものの上にリーダライタを置いて動作させてください。

9.2.このサイトへの接続はセキュリティで保護されていません

[表示画面]

	0				×	+													-	
\leftarrow	C	Ŵ	()	https:,	//an1le.	1377/le	st/test	totol		$\forall_{\mathscr{Y}}$	€	τô		12	Hini	ß		Ē	12	
	1	٦																		
	С																			
	20	ひサ-	۲ŀ	<u>~0</u>)接	続は	セキ	キュリ	リテ	ィで	呆護	1t	n	τ	いま	せ	ю			
	mahr ログィ	oki-auth イン証明	1.2nd 書が損	s.mec 提供され	lis.or. いません	ip によ んでし1	:りユ- た。	ーザーの	のログ	イン証明	書が受	きけ入	n:	5nt	こかつ	たか、				
	組織(こお問い	合わt	さくだ	±ιν。															
	ERR_BA	D_SSL_CLIE	NT_AUT	TH_CERT																

[原因]

・HPKI(JPKI)認証時、ICカードの PIN を求める画面が表示されずに表示画面になった場合、ICカードの読み取り に失敗しています。

・IC カードの証明書の有効期限が切れている。

・IC カードの証明書情報を中継しない Proxy サーバを経由して接続している。

[対策]

・IC カードリーダーが PC に接続され、IC カードドライバ等の必要なソフトウェアがインストール済であるか確認してください。

(確認方法については10.2を参照してください)

・IC カードは有効なものであるか(期限切れカードでないか等)確認してください。

・Proxy サーバを経由せずに直接アクセスするか、SSL クライアント認証のリクエストも中継する Proxy サーバに変更 して接続してください。

・ウィルス対策ソフトウェアが Web ブラウザの機能を制限して IC カードが利用できない場合があります。ウィルス対策ソフトウェアの設定を変更するか、ソフトウェア自体を終了させて動作を確認してください。

・非接触型の IC カードリーダライタを使用している場合、金属板上にリーダライタを置くと IC カードが読み取れないケースがあります。木やプラスチックなど、金属でないものの上にリーダライタを置いて動作させてください。

9.3.このページは現在機能していません

[表示画面]

- 📴 医療機関等ONS 🗅 医療機関等ベンダー 늦 日本医師会電子認	
このページは現在機能していません	
mahpki-auth.2nds.medis.or.jp からデータは送信されませんでした。	
ERR_EMPTY_RESPONSE	
	_

[原因]

・IC カードの証明書情報を中継しない Proxy サーバを経由して接続している。

[対策]

・Proxy サーバを経由せずに直接アクセスするか、SSL クライアント認証のリクエストも中継する Proxy サーバに変更 して接続してください。

9.4.<u>HPKI(JPKI)証明書のユーザが無効となっています。</u>

[表示画面]

<HPKI 認証の場合>



<JPKI 認証の場合>

нркіセカ	ンド電子証明書管理・認証プラットフォーム
	mediauth
	JPKI証明書のユーザが無効となっています。 管理者に問い合わせてください。

[原因]

- ・当該ユーザが無効になっている(削除されている)状態で HPKI 認証を実施した。
- ・当該ユーザが無効になっている(削除されている)状態で JPKI 認証を実施した。

[対策]

・各認証局に本人 ID (医籍登録番号、薬剤師登録番号等)を連絡の上、ユーザ登録がされているか問い合わせ してください。

9.5.予期せぬエラーが発生しました。

[表示画面] ログイン × 予期せぬエラーが発生しまし た。 OK

[原因]

・HPKIカードを用いた認証を実施した後、続けてマイナンバーカードによる認証を行った。

[対策]

・IC カードを用いた認証を実施した後、別のカードで認証を続ける場合は、ブラウザのキャッシュクリア後、一度ブラウザ を閉じてから実施してください。

(ブラウザのキャッシュクリアについては10.1を参照してください)

9.6.Cookie が見つかりません。



[原因]

・他のユーザで認証された状態で認証を行った。(ブラウザにキャッシュの情報が残っており、悪影響を与えている場合が あります)

[対策]

・ブラウザのキャッシュ情報をクリアして、ブラウザを閉じてからもう一度最初から操作を実施してください。 (ブラウザのキャッシュクリアについては10.1を参照してください)

9.7.該当のユーザが登録されていません

[表示画面]



[原因]

・Username に本人 ID を入力されていない状態で「送信」を実施した。

[対策]

・正しい本人 ID を入力してください。

9.8.デバイス認証に必要なユーザ情報が登録されていません。

[表示画面]



[原因]

・当該ユーザが未登録または FIDO デバイスが無効になっている(削除されている)状態で FIDO 認証を実施した。 または FIDO 認証時に誤った本人 ID を入力した。

[対策]

- ・正しい本人 ID を入力してください。
- ・各認証局に本人 ID (医籍登録番号、薬剤師登録番号等)を連絡の上、ユーザ登録がされているか問い合わせ してください。

9.9.デバイス認証でエラーが発生しました。



[原因]

・一度ログオンした後に、再度ログオンしようとしている。

[対策]

- ・ブラウザを一度終了してから再度認証してください。
- ・ブラウザのキャッシュをクリアしてください。

9.10. <u>Unauthorized</u>

[表示画面]



[原因]

接続途中経路に認証を要求する Proxy サーバ等を経由している。

[対策]

・経路途中に認証を要求するサーバがある場合にはそのサーバに対する適切な認証情報を設定してください。

・直接インターネットに接続する等、認証を行うサーバを経由しないでアクセスしてください。

9.11. ユーザ情報の取得ができませんでした。

[表示画面]

<HPKI 認証の場合>



<JPKI 認証の場合>

нркเセカ	ンド電子証明書管理・認証プラット	フォーム
	mediauth	
	 ユーザ情報の取得ができませんでした。 マイナンバーカードをご確認の上用度認証をお願いします。 	
X		

[原因]

・当該ユーザが未登録の状態で HPKI 認証または JPKI 認証を実施した。

[対策]

・各認証局に本人 ID (医籍登録番号、薬剤師登録番号等)を連絡の上、ユーザ登録がされているか問い合わせ してください。

9.12. 認証用デバイスが未登録です

[表示画面]



[原因]

・デバイス登録がされていない状態で FIDO 認証を実施しようとした。

[対策]

・デバイス(スマートフォン)の登録を実施してください。



[表示画面]

HPKIセカンド電子証明書管理・認証プラットフォーム マイナンバーカード登録サイト	,
本人ID:testc30382	
カードドライバに挿入するカードをHPKIカードからマイナンバーカードに差し替えてください。	
◆マイナンバーカードがICカードリーダーにセットされている状態で下のボタンをクリックしてください。◆	
マイナンバーカードを登録	

[原因]

- ・拡張機能がインストールされていない。
- ・拡張機能が有効になっていない。

[対策]

・利用者クライアントソフトの拡張機能がブラウザにインストールされているか確認してください。「三」から「拡張機能」-「拡張機能の管理」を選択してインストール済の拡張機能の中に"利用者クライアントソフト Edge/Chrome"が入 っている事、チェックがオンになっていることを確認してください。ない場合、公的個人認証サービスのポータルサイトから 公的個人認証サービスの利用者クライアントソフト(Edge/Chrome ブラウザ利用版)をダウンロードしてインストール をして下さい。

9.14. 登録対象のマイナンバーカードの証明書は、別のユーザが登録

<u>済です。</u>

[表示画面]

エラーコード:JPKIHREGERR003

登録対象のマイナンバーカードの証明書は、別のユーザが登録済です。HPKI証明書を発行した認証局にお問い合わせく ださい。

ページを閉じてください。

[原因]

・登録しようとしたマイナンバーカードは、既に別の利用者に割り付けられている。

(一人で複数の HPKI カードをお持ちの場合でも、マイナンバーカードはそのうちの一つにしか登録することができません)

[対策]

・マイナンバーカードの登録状況の確認や、登録解除手続きなどは、各認証局にお問い合わせください。

9.15. 既にアプリケーションが起動しています。

[表示画面]

利用者クライアントソフト エラー	_	×
既にアプリケーションが起動しています。 エラーコード:EW000J0200		0
ОК		

[原因]

・マイナンバーカードの利用者クライアントが複数個起動された。

Edge と Chrome で同時に操作したり、表示されたダイアログ画面を閉じないまま処理を続行したりすると表示されます。

[対策]

・開いているダイアログ画面がある場合は閉じてください。

・Edge もしくは Chrome のいずれかで操作するようにしてください。

9.16. 個人番号カードに接続できません。

[表示画面]



[原因]

マイナンバーカード登録時、マイナンバーカードが読み取れなかった。 ・カードがセットされていない。もしくは正しくセットされていない。 ・HPKI カードを入れたままにしている。 ・マイナンバーカードではないカードをセットした。

[対策]

・マイナンバーカードがカードリーダーに正しくセットされているか確認してください。



Forbidden

You don't have permission to access this resource.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.

[原因]

・HPKI カードやマイナンバーカードで、証明書選択してから PIN 入力までに1 分以上経過した。

・何らかの理由で接続が禁止されているネットワークから接続している。

[対策]

・PIN 入力に時間がかかった結果、この画面が出た場合は、ブラウザのキャッシュをクリアして閉じた後で、証明書選択から再度やりなおしてください。

・ネットワークに原因がある場合は、ネットワークの管理者にお問い合わせください。

9.18. <u>HPKI(JPKI)証明書が失効しています。</u>

[表示画面]

<HPKI 認証の場合>



<JPKI 認証の場合>



[原因]

- ・認証に使用している HPKI カードの証明書が失効している。
- ・認証に使用しているマイナンバーカードの認証用証明書が失効している。

[対策]

- ・HPKIカードが失効されているの場合、再発行を認証局に依頼してください。
- ・マイナンバーカードが失効されている場合、の証明書再発行を自治体に依頼してください。

9.19. <u>HPKI(JPKI)認証でエラーが発生しました。</u>

[表示画面]

<HPKI 認証の場合>



<JPKI 認証の場合>



[原因]

・マイナンバーカードを用いて HPKI 認証を実施した。

・HPKI カードを用いて JPKI 認証を実施した。

HPKI認証を実施した後、ブラウザを閉じずにマイナンバーカードによる認証を行った場合、もしくはその逆の場合に発生します。

[対策]

・HPKI 認証では HPKI カードを使用して認証を行ってください。

・JPKI 認証ではマイナンバーカードを使用して認証を行ってください。

・IC カードを用いた認証を実施した後、別のカードで認証を続ける場合は、一度ブラウザを閉じてから実施してください。

9.20. マイナンバーカードに紐づくユーザが存在しません。



[原因]

・HPKI-KAGURA に登録されていないマイナンバーカードを使用して JPKI 認証を行った。

[対策]

・使用しているマイナンバーカードがHPKI-KAGURAにご自身の認証用として登録したものであるか確認してください。 (HPKIカードを用いてご自身のマイナンバーカードを登録(再登録)することができます。)



[原因]

- ・HPKI(JPKI)認証時、ICカードの PIN を求める画面が表示されずに表示画面になった場合、ICカードの読み取り に失敗している。
- ・IC カードの証明書の有効期限が切れている。
- ・IC カードの証明書情報を中継しない Proxy サーバを経由して接続している。
- ・証明書選択画面でキャンセルを実施した。

[対策]

・IC カードリーダーが PC に接続され、IC カードドライバ等の必要なソフトウェアがインストール済であるか確認してください。

(確認方法については10.2を参照してください)

・IC カードは有効なものであるか(期限切れカードでないか等)確認してください。

- ・Proxy サーバを経由せずに直接アクセスするか、SSL クライアント認証のリクエストも中継する Proxy サーバに変更 して接続してください。
- ・ウィルス対策ソフトウェアが Web ブラウザの機能を制限して IC カードが利用できない場合があります。ウィルス対策ソフトウェアの設定を変更するか、ソフトウェア自体を終了させて動作を確認してください。
- ・非接触型の IC カードリーダライタを使用している場合、金属板上にリーダライタを置くと IC カードが読み取れないケースがあります。木やプラスチックなど、金属でないものの上にリーダライタを置いて動作させてください。

9.22. <u>FIDO 認証情報の登録ができませんでした</u>

FIDO認証情報の登録ができませんでした 画面を閉じてください

[原因]

・デバイス登録処理の途中でキャンセルを実施した。(スマートフォン側の設定不備などで、デバイス登録がうまくいかなかった場合も含む)

・デバイス登録処理がタイムアウトになった。(※1)

(※1) デバイス登録処理のタイムアウト: 10 分。

スマートフォン変更の場合、最初の認証用 QR コードが表示されてからデバイス登録が完了するまでの時間 を「デバイス登録処理」とみなす。

[対策]

・設定不備などを修正した後、ブラウザを終了させてから、再度デバイス登録処理を実施してください。

※スマートフォン側の処理が完了しているのにこの画面が表示された場合には、デバイス登録自体は正常に行われているため、特に対策は必要ありません。

10 各種設定の確認・変更方法

10.1. <u>ブラウザのキャッシュクリア</u>

操作する PC のブラウザにキャッシュが残っている場合、正常に認証ができない場合があります。以下の方法でキャッシュをクリアしてください。

a) Edge(PC)の場合

メニューマークをクリックし、メニュー選択画面の「設定」をクリックします。



「プライバシー、検索、サービス」をクリックし、"閲覧データをクリア"の項目の"今すぐで閲覧データをクリア"の「クリアす るデータの選択」をクリックします。



時間の範囲を"すべての期間"とし、"Cookie およびその他のサイトのデータ"にチェックを入れて「今すぐクリア」のボタ ンをクリックします。



b) Chrome(PC)の場合



「メニューマーク」をクリックしてメニュー一覧を開き「設定」をクリックします。

「プライバシーとセキュリティ」をクリックします



"プライバシーとセキュリティ"から「閲覧履歴データの削除」をクリックします。

章 設定・ブライバシー	-دومعالي المراجع	~	-	-		×
← → C ⊕	Chrome chrome://settings/privacy	Ŀ	2 \$:
■ 設定					c	
	プライバシー ガイドを開始 Chrone のプライバシーとセキュリティに発する重要な設 を登録じます しいえ					
	安全線路	±:0				l
	Chromeでテータ提着や小正な証拠機能などの背気から構成されているか確認します ブライバシーとセキュリティ	E12				l
ſ	■ 開発電気データの削除 開発電気、Cookie、キャッシュなどを削除します	•			-	1
	プライパシーカイド プライパシーとセキュリティに関する最要な設定を確認する	•				ł
	Cookle と他のサイトデータ シークレットモードでサードバーティの Cookle がブロックされています	•				
	♥ セキュリティ セーフ ブラウジング (会論なサイトからの展開機能) などのセキュリティ設定	•				

期間を"全期間"にして"Cookieと他のサイトのデータ"にチェックを入れて「データを削除」のボタンをクリックします。



- c) Safari(iPhone)の場合
 - ① iOS17以前

iPhoneの設定を開き、Safariをタップします。

SIMなし 🗢	13:15	100% 🔲	
	設定		
> ×	ッセージ	>	
🗖 Fac	ceTime	>	Safari をタッ
🧭 Sa	fari	>	
林	西	>	

Safariの設定項目の中から「履歴と Web サイトデータを消去」をタップします。



確認画面が表示されるため、「履歴とデータを消去」をタップします。



② iOS18 以降

iPhoneの設定を開き、「アプリ」をタップします。



Safariの設定項目の中から「履歴と Web サイトデータを消去」をタップします。



確認画面が表示されるため、「すべての履歴」にチェックがついていることを確認の上、「履歴を消去」をタップします。



d) Chrome(Android)の場合

Chromeのアプリを開き、メニューを開き「設定」をタップします。

13:34 ឆំ 🗟 🖶			
an	● 新しいタブ		
•			
検索語句また	高 新しいシークレットタフ		
	④ 履歴		
	✓ ダウンロード		
Yahoo!ニュ… アメ	★ ブックマーク		
 ③ 引き続き開 HPKIセカ 	□□ 最近使ったタブ		
			「設定」をタップ
Discover - オフ	♀ 設定		
	⑦ ヘルプとフィードバック		
プライバシ	ーとセキュリティをタッ	プします。	
13:34 🏟 🗄 🛞	r€ ♥ i 83%	7	
← 設定	0		
検索エンジン			
Google			
パスワード マネ	ージャー ^{New}		
お支払い方法			
		_	
住所やその他の	情報		- プライバシーとセキュリティをタップ
プライバシーと	セキュリティ		
安全確認			
閲覧履歴	データの削除をタッ	プします。	
13:34 章 🛙 😣			
< 7⇒.	イバシーとセキュリのの		
プライバシー			問覧房麻ゴ カの削除をかって
閲覧履歴データ 履歴、Cookie、5	?の削除 ナイトデータ、キャッシュを削除		・ 別見 復歴ナークの則 味をクツノ
	D	-?	
ワードバーティ シークレットモー	しоокіе ードでサードパーティの Cookie がブロ		
ックされています		_	
庁牛のゴニノバ	*2,		

期間が全期間、Cookieとサイトデータにチェックがあることを確認して「データを削除」をタップします。



再度、Chromeのメニューを開き「閲覧履歴データの削除」をタップします。



閲覧履歴データ削除画面が表示されるので、左上の「過去 15 分間」をタップします。



前回、HPKI-KAGURA にアクセスした時期を含む期間を選択します。 (前の日にアクセスしているのであれば「過去 24 時間」など)

閲覧履歴デー	ータの削除	どわかを選択
過去 15 分間		
1 時間以内	}間 にアクセスしたサイトは… バイスのアイテム	
過去 24 時間	計問に閉じられたタブはありま	
過去7日間	キャッシュ、その他のサイト	
過去 4 週間		
全期間	(=) >	
	T	

「データを削除」をタップします。

閲覧履歴データの削除	
過去 15 分間 🔻	
 過去15分間にアクセスしたサイトは… 同期したデバイスのアイテム 	
□ 過去 15 分間 に閉じられたタブはありま せん	
Cookie、キャッシュ、その他のサイト データ	
その他のオプション >	
Google アカウントに検索履歴やその他のアクティビ ティが保存される可能性があります	
キャンセル データを削除	タップ

10.2. IC カードからの証明書の読み取り確認

IC カードが PC から正しく読み取ることができない場合、HPKI 認証(または JPKI 認証)に失敗します。正しく読み取ることができているか IC カードを IC カードリーダライタにセットした上、以下の方法にて確認してください。

- (1) Edge からの確認
 - ① Edgeを起動し、画面右上の[…]から[設定]メニューを押してください。

C	G Q 検索または W	'eb アドレスを入力			50 Do	ଓ କାର୍ମ	
				🔄 新しいタブ		Ctrl+T	
				□ 新しいウインドウ		Ctrl+N	- 1
				😨 新しい InPrivat	* ウインドウ	Ctrl+Shift+N	
				7-14		- 100% +	2
				☆ お気に入り		Ctrl+Shift+O	
				Dv95aV		Ctrl+Shift+Y	- 1
				🖲 展歴		Ctrl+H	- 1
				② ショッピング			- 1
		- Mie	crosoft	<u>↓</u> ダウンロード		Ctrl+J	- 1
				8 779			>
				£₽ 7-1.			- 1
			_	(3) 抗張機能			- 1
		職場と Web を検索	Ŷ	P Microsoft Rev	vards		- 1
				☞ パフォーマンス			
				0 DN		Ctrl+P	
				♥ Web キャプチャ		Ctrl+Shift+S	- 1
				💭 Web 選択		Ctrl+Shift+X	- 1
				12 共有			- 1
				A) ページ内の検索		Ctrl+F	
				A ^N 音声で読み上(15	Ctrl+Shift+U	
				internet Explo	rer モードで再読み込;	みする	
				その他のツール			>
			[(\$ 9)E			
				⑦ ^ルブとフィード/	ペック		>
	🗮 📕 Microsoft 365	マイ フィード ニュース スポーツ …	(合個人用設)	Microsoft Edg	e を閉じる		
)				A starting			

②左画面のメニューから、「プライバシー、検索、サービス」をクリックし、セキュリティの項目から「証明書の管理」をク リックしてください。



③「個人」タブを選択すると証明書の一覧が表示されます。 証明書ウィンドウに以下の証明書の情報が表示されているか確認してください。

・HPKI カードの証明書:発行者が HPKI-...で記載されているもの

・マイナンバーカードの証明書:発行者が「Japan Agency for local Authority Information Systems」
 で記載されているもの

証明書	ł											3
1的(N):		<র%্রে>										
個人	ほかの人	中間証明	月機関	信頼され	たルート証明	機関	信頼	された発行	īπ	信頼さ	ntel	• •
発行分 同JM	ŧ ACombi2	0944		発行者 HPKI-	t 01-hpkij	有交 202	时期 7/0	フレンド JMACo	リ名 mbi2			
1ンボー	F(D]	.夕又杰—卜i	<u>E</u>)	創辞()	8)					37.1	相設定	(A)
インボーー	►(D.~] D目的	ウスボート	<u>E</u>)	前门车()	8)					57.5	目設定	(A)
インボー! 証明書の	►(D]	- クスホート	E)	前降山	BJ					314	●酸症	((A)

(2) Chrome からの確認

①Chromeを起動し、画面右上の[:]から[設定]メニューを押してください。

③ 新しいタブ	× +			
← → C			le ☆ [1 4 🕕
		新しいタブ 新しいウィンドウ 新しいシークレット	・ウィンドウ Ctr	Ctrl+1 Ctrl+N l+Shift+N
		履歴 ダウンロード ブックマーク		Ctrl+J
	Google	ズーム 印刷 キャスト	- 100% +	Ctrl+P
	ooogie	その他のツール	11 - 11. ²	Ctrl+F
	Q Google で検索または URL を入力	通道 設定 人ILプ		POULITIT
	+	終了		
	ウェブストア ショートカッ			
		0	🖍 Chrome を力ス	গ্রহনর
②左画面のメニューから、「プライバシーとセキュリティ」を押してください。右画面をスクロールし、プライバシーとセキュリ ティの「セキュリティ」を押してください。

🌻 設定 - ブライバシーとセキュリティ 🗙 🕇	
← → C	
◎ 設定	Q、 設定項目を検索
 Google の設定 自動入力とパスワード 	定を確認します <u> 始める</u> 同意しない
 ⑦ ブライバシーとセキュリティ ④ パフォーマンス 	安全チェック
 デザイン Q、検索エンジン 	② Chrome でデータ侵害や不正な拡張機能などの脅威から保護されているか確認します 今すぐ確認
 団 既定のブラウザ () 起動時 	ブライバシーとセキュリティ
 ● 言語 ▲ ダウンロード 	 ■ 開発調査に クラの用語 ■ 開発調査: Cookie、キャッシュなどを制除します プライパシー ガイド プライパシー ナイド プライパシーとセキュリティに関する重要な設定を確認する ・
 オ ユーザー補助機能 ▲ システム 	サードパーティ Cookie シークレットモードでサードパーティの Cookie がブロックされています
 43 説法のリゼット 第4 拡張機能 区 	 ◎ セニン・レガ広告表示に使用する情報をカスタマイズします ● セキュリティ セーフ ブラウジング (危険なサイトからの保護機能) などのセキュリティ設定
© Chrome について	サイトの設定 サイトが使用、表示できる情報(位置情報、カメラ、ポップアップなど)を刺御します

③右画面をスクロールし、詳細設定の「証明書の管理」を押してください。

•							
÷	← → C						
0	設定	Q、 設定項目を検索					
ی ا ا ا ا ا ا	Google の設定 自動入力とパスワード プライパシーとセキュリティ パフォーマンス デザイン 検索エンジン 既定のブラウザ 起動時	詳細設定 常に安全な接続を使用する 移動先を HTTPS にアップグレードし、HTTPS をサポートしていないサイトは読み込む前に警告を表示します セキュア DNS を使用する ウェブサイトに安全に提続する方法を決定します ● 現在のサービスプロバイダを使用する セキュア DNS は使用 できない場合があります ● 次を使用 カスタム ▼					
● ± † × ① ★ ③	 言語 ダウンロード ユーザー補助機能 システム 設定のリセット 拡張機能 Chrome について 	スマートフォンの管理 セキュリティ キーとして使用するスマートフォンを管理します 証明書の管理 HTTPS / SSL の証明書と設定を管理します Chrome で管理されている証明書 Chrome でのルート証明書の管理方法に関する情報 Google の高度な保護機能プログラム 個人の Google アカウントを標的型攻撃から保護します	, 2 2 2				

④「証明書マネージャ」画面が表示されるので、「ローカル証明書」の「Windows からインポートした証明書を管理 する」を選択して、証明書管理画面を表示させます。

0	証明書マネージャ		
	ローカル証明書	ローカル証明書	
1ª	ユーザーの証明書	オペレーティングシステムまたは管理者が追加したローカル証明書です。	
0	Chrome Root Store	ウィンドウ	
		オペレーティング システムからインポートしたローカル証明書を使用する 61 件の証明書	
		Windows からインポートした証明書を表示する	>
		Windows からインポートした証明書を管理する	Ľ

⑤「個人」タブを選択すると証明書の一覧が表示されます。 証明書ウィンドウに以下の証明書の情報が表示され ているか確認してください。

・HPKIカードの証明書:発行者がHPKI-...で記載されているもの

・マイナンバーカードの証明書:発行者が「Japan Agenncy for local Authority Information Systems」で記載されているもの



※ウィルス対策ソフトウェア等でブラウザからの IC カードアクセスを阻止している場合、証明書が表示されず IC カード による認証ができません。

例えば、ESET インターネットセキュリティでは以下の設定でブラウザから IC カードへのアクセスを阻止しています。設 定をオフにして証明書が表示されるか確認してください。

	ПҮ	0 -	□ ×
08 概要 0	< セキュリティツール		?
Q コンピューターの検査 C アップデート	インターネット/じキング保護 有効:オンライン/じノキングWeebサイトと暗号資産ウォレットを保護します。 すべてのブラウザーを保護 すべてのブラウザーを保護 ローム ロー ローム ローム		¢×
 ラール 設定 	 永久的に無効:すべてのサポートされているブラウザーを安全なモードで実行します。 アンチセント 停止: 盗まれたとき、ノートをcの保護と検索 		
② ヘルプとサポート			
Progress. Protected.	*4 脱注のインボート/エクス3	ポート ウ 詳細的	定

110 / 123

10.3. スマートフォンの標準ブラウザ設定確認

FIDO 認証を行う場合、iPhone の場合は Safari、Android の場合は Chrome のブラウザを使用してください。カ メラのアプリから QR を読み込んだ際に、Safari や Chrome 出ないブラウザアプリが起動する場合、標準ブラウザの設 定として Safari や Chrome を指定してください。指定の方法は以下のとおりです。

- A) iPhone の場合
 - a) iOS17 以前

「設定」を開いて、下にスクロールして Safari を見つけます。

SIMなし 🗢	19:25		•
	設定		
	電話	SIMなし >	
	メッセージ	>	
	FaceTime	>	Safari をタッフ
0	Safari	Þ	
and the	株価	>	

Safari をタップし、「デフォルトのブラウザ App」をタップします。

SIMなし 🗢 く 設定	^{19:25} Safari	-		
SAFARIにアクセ	スを許可			
💽 Siriと樹	検索	>		
				デフォルトのブラウザ App をタップ
デフォルトの	ブラウザApp	Chrome >		11
検索				
検索エンジン		Google >		
検索エンジン	の候補			

※デフォルトのブラウザが Safari の場合"デフォルトのブラウザ App"の項目は出てきません

Safariを選択すると、Safari にチェックマークが表示されます。



b) iOS18 以降

iPhoneの設定を開き、「アプリ」をタップします。



「Safari」をタップします。

P	N O P	
Z Pages	> R S	
	T U V	
S	w ×	Sofori をないプ
🧭 Safari	>	Salar (199)
т	さ た な	
€tv TV) 2 2 2	
	ら わ #	

「デフォルトのブラウザアプリ」をタップします。

ר ד	プリ	Safari	
SA	AFARIにアクセス	を許可	
(Siri		>
	2 検索		>
_			
デ	「フォルトのブ	゙ラウザアプリ	Safari >

Safariを選択すると、Safariにチェックマークが表示されます。



B) Android の場合

Android デバイスで設定を開きます。 [アプリ] をタップします。

^{13:37} 設	♥₫56%			
٩	設定を検索			
÷	電話番号 ^{不明}			
Ģ	ネットワークとインターネット モバイル、WiFF、テザリング			
[10]	接続済みのデバイス Bluetooth、ベア設定			 アプリをタップ
	アプリ 最近使ったアプリ、デフォルトのアプリ] 🔨		
^	诵知			

"全般"で [デフォルトのアプリ] をタップします。





Chrome をタップして Chrome チェックがある事を確認します。



10.4. <u>スマートフォンの OS,ブラウザのバージョン確認</u>

調査のため、スマートフォンのバージョンを確認させて頂くことがあります。バージョンの取得方法について説明します。

A) iPhone の場合

OS のバージョン

「設定」を開き「一般」をタップします。

< 6余宗 令 19:33 設定	-	一般を タ ップ
⊙ −₩	>	
🔋 コントロールセンター	>	
AA 画面表示と明るさ	>	
「情報」をタップします	- •	
▲ 股定 — 般	-	
		情報をタップ
情報	>	
ソフトウェアアップデート	>	

記載されている iOS バージョンおよび機種名をお知らせ願います。



ブラウザ(Safari)のバージョン Safari のバージョンについては OS に紐づくため取得不要です。

B) Android の場合

OS のバージョン

スマートフォンの設定アプリを開き、[デバイス情報]をタップしますます。

٥	セキュリティ 画面ロック、顔認証、指紋	
@	プライバシー 権限、アカウント <i>アク</i> ティビティ、個人データ	
0	位置情報 OFF	
*	緊急情報と緊急通報 ^{緊急} SOS、医療情報、アラート	
ା	パスワードとアカウント 保存されているバスワード、自動入力、同期さ れているアカウント	
Ŷ	Digital Wellbeing と保護者による 使用制限 ^{利用時間、アブリタイマー、おやすみ時間のス ケジュール}	
G	Google サービスと設定	
()	システム 言語、ジェスチャー、時間、パックアップ	デバイス情報をタップ
ī	デバイス情報 AQUOS sense7	

[Android バージョン] をタップします。

^{14:03} ← デバイス情報	♥ 🔒 55%		
モデル SH-M24			
IMEI (SIM スロット1) 359482550409517			
IMEI (SIM スロット 2) ³⁵⁹⁴⁸²⁵⁵⁰⁴⁹⁸⁸⁴¹			Android バージョンをタッフ
Android バージョン ¹²			Anurolu N= 2322392
デバイフリ			

"Android バージョン"、"ビルド番号"をお知らせ願います。

14:03 ♥ 🔒 55%
Android バージョン
Android バージョン ¹²
Android セキュリティ アップデート 2022年9月1日
Google Play システム アップデート ^{2023年3月1日}
ベースバンド バージョン 01.00.02,01.00.02
カーネル バージョン 5.4.161-ggki #1 Wed Oct 26 02:55:45 JST 2022
ビルド番号 01.00.02

ブラウザ(Chrome)のバージョン

Chrome を起動してアドレスバーに「chrome://version」と入力し、キーボードの確定ボタンをタップすると、 Chrome のバージョンが表示されます。



10.5. <u>iCloud キーチェーンを有効にする</u>

iPhone で FIDO デバイス登録を行うためには、iCloud キーチェーンの設定を ON にする必要があります。以下の手順で実施します。

A) iOS17 以前

「設定」をタップし、「[ユーザ名]」をタップします。

設定		
二支二述 Apple ID、iCloud、メディ	> アと購入	_ ユーザ名をタップ
▶ 機内モード		
ᅙ Wi-Fi MobileDe	vG2323 →	
Bluetooth	オン >	
(い) モバイル通信	>	
「iCloud」をタップします。 く設定 Apple ID		
■■ ■	>	
パスワードとセキュリティ	>	
お支払いと配送先	なし >	
サブスクリプション	>	
	_	iCloud をタップ
iCloud	5 GB >	
🙏 メディアと購入	>	

「パスワードとキーチェーン」をタップします。



「iCloud キーチェーン」をオンにします。



※パスコードまたは Apple ID のパスワードの入力を求められる場合があります。

また、パスワードオプションにて iCloud キーチェーンが動作する設定が必要です。

"設定"から「パスワード」をタップします。



「パスワードオプション」をタッ	パします。	0
く 設定 パスワード	十編集	
Q、 検索	Ŷ	
セキュリティに関する勧告 問題は見つかりませんでした	0 >	ハスワードオフショフをダップ
🔒 パスワードオプション		

「パスワードとパスキーを自動入力」が ON になっていない場合は ON にします。 「次の提供元からのパスワードとパスキーを使用」の欄にある「iCloud キーチェーン」が ON になっていない場合は ON にします。(iOS17.4 以降)

※iOS17.3 以前は指定方法が異なります。iCloud キーチェーンにチェックを入れてください。



B) iOS18 以降

「設定」をタップし、「[ユーザ名]」をタップします。



119 / 123

「iCloud」をタップします。

く設定 Apple ID			
名前、電話番号、メール	>		
パスワードとセキュリティ	>		
お支払いと配送先	なし >		
サブスクリプション	>		
			iCloud をタップ
iCloud	5 GB >		
「パスワード」をタップします。 SMなし	97% 🗩		
 ストレージ 242.2MB/5 iCloud+にアップグレード プレミアム機能ともっと多くのスペースをできます。 あなたへのおすすめ iCloudについての詳細、その他2件 	5GB > 利用 3 >		
● iCloud に保存済み すべて見 ● iCloud に保存済み すべて見 ● iSloud に保存済み 138 個の項目	見る >	パスワードをタップ	
×ッセージ オフ ×→ル 2.9MB			

「パスキー」をタップします。

パスワ-	ード			
Q 検索			Ŷ	
? すべて	52 >	ふ パスキー	52 >	パスキーをタップ
<mark>6)</mark> א–ב	0 >	🥱 Wi-Fi	1>	
マセキュリティ	0 >	値 削除済み	0 >	

「この iPhone を同期」をオンにします。

Cloud パスワードとキーチェーン	
ę	
iCloud パスワードとキー チェーン	
パスワード、クレジットカードなどを iCloud に安全に保存し、お使いのすべてのデ バイス上の Safari やその他の対応 Web ブラ ウザで情報を自動入力します。詳しい情報	ON にする
この iPhone を同期	

※パスコードまたは Apple ID のパスワードの入力を求められる場合があります。

また、パスワードオプションにて iCloud キーチェーンが動作する設定が必要です。

"設定"から「一般」をタップします。



"一般"のメニューから「自動入力とパスワード」をタップします。

🐻 アプリのバックグラウンド更新	>	
= キーボード	>	
Aa フォント	>	
() 言語と地域	>	自動入力とパスワ-
1 自動入力とパスワード	>	タップ
注 辞書	>	
🔜 日付と時刻	>	

「パスワードとパスキーを自動入力」が ON になっていない場合は ON にします。 「自動入力の取得元」の欄にある「パスワード」が ON になっていない場合は ON にします。



10.6. スマートフォンでのブラウザの見分け方

カメラアプリから連動されて起動されたアプリケーションが Safari や Chrome ではない場合があります。画面上で違う ブラウザが動作しているか画面からでもある程度確認することが可能です。 ※あくまでも一例であるため、バージョンやブラウザの設定によっては異なる表示となっている可能性があります

