# HPKI セカンド電子証明書管理・認証プラットフォーム

# エラー対応・確認マニュアル

Ver. 2.15

2025 年 7 月

# 目　　次

CONTENTS


1　はじめに....4
2　スマートフォンでのメッセージ....4
2.1.　アカウントが無効です。管理者に連絡してください。....4
2.2.　WebAuthn is not Supported by this browser....5
2.3.　セキュリティーキーの登録結果が無効です。....6
2.4.　NotReadableError: An unknown error occured while talking to the credential manager....7
2.5.　NotAllowedError: Operation failed....8
2.6.　セキュリティーキーによる認証に失敗しました。....9
2.7.　NotAllowedError: The 'navigator.credentials.create' API is only permitted in applications with the 'com.apple.developer.web-browser' entitlement....10
2.8.　NotAllowedError: The operation either timed out or was not allowed....11
2.9.　NotSupportedError: The specified 'userVerification' requirement cannot be fulfilled by this device unless the device is secured with a screen lock....12
2.10.　403 Forbidden....13
2.11.　mahpki-auth.2nds.medis.or.jp でセキュリティキーを使用する....14
2.12.　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。....15
2.13.　画面のロックを使用する....16
2.14.　パスコードで続ける....17
2.15.　Cookie が見つかりません。....18
2.16.　（画面が真っ白または真っ黒になる）....19
2.17.　スマートフォンの画面に QR コードが表示される....20
2.18.　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。....21
2.19.　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。....22
2.20.　405 Method Not Allowed....23
2.21.　パスキーを管理する方法を選択してください....24
2.22.　Autheticator：パスキーを追加できませんでした....25
2.23.　利用可能なパスキーがありません....26
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。....27
3　PC でのメッセージ....28
3.1.　このサイトは安全に接続できません....28
3.2.　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....29
3.3.　このページは現在機能していません....30
3.4.　HPKI(JPKI)証明書のユーザが無効となっています。....31
3.5.　予期せぬエラーが発生しました。....32
3.6.　Cookie が見つかりません。....33
3.7.　該当のユーザが登録されていません....34
3.8.　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。....35
3.9.　デバイス認証でエラーが発生しました。....36
3.10.　Unauthorized....37

３．１１．ユーザ情報の取得ができませんでした。 38
３．１２．認証用デバイスが未登録です 39
３．１３．「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 40
３．１４．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。 40
３．１５．既にアプリケーションが起動しています。 41
３．１６．個人番号カードに接続できません。 42
３．１７．Forbidden 43
３．１８．HPKI(JPKI)証明書が失効しています。 44
３．１９．HPKI(JPKI)認証でエラーが発生しました。 45
３．２０．マイナンバーカードに紐づくユーザが存在しません。 46
３．２１．mahpki-auth.2nds.medis.or.jp へのアクセスが拒否されました 47
３．２２．FIDO 認証情報の登録ができませんでした 48
３．２３．情報不足のため、この証明書を検証できません。 49
３．２４．この証明書の整合性を保証できません。 50
４　各種設定の確認・変更方法 51
４．１．ブラウザのキャッシュクリア 51
４．２．IC カードからの証明書の読み取り確認 59
４．３．スマートフォンの標準ブラウザ設定確認 63
４．４．スマートフォンの OS,ブラウザのバージョン確認 66
４．５．iCloud キーチェーンを有効にする 69
４．６．スマートフォンでのブラウザの見分け方 75

# 1　はじめに

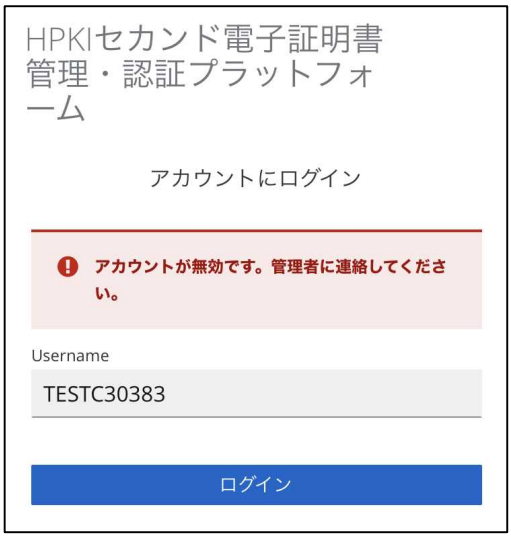
本文書は、HPKI セカンド電子証明書管理・認証プラットフォーム（以下、HPKI-KAGURA）にて発生しているエラー画面の内容とその対応策についてまとめたものとなります。

画面に表示される内容にあわせ、どのような対応を利用者が行えばよいかをまとめております。また、PC やスマートフォンの設定内容の確認や変更方法について操作方法を記載しています。

# 2　スマートフォンでのメッセージ

## 2．1．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]**




**[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。

## 2.2. WebAuthn is not Supported by this browser.

**[表示画面]**

**[原因]**

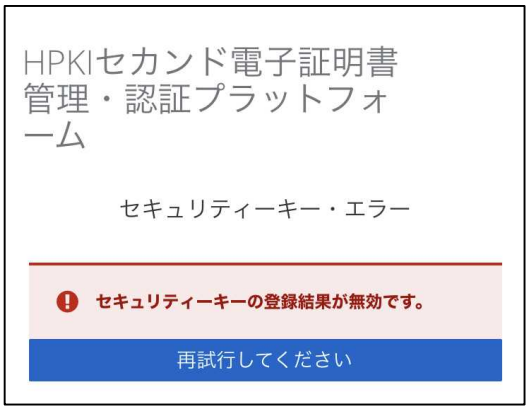
・ブラウザまたは OS が FIDO2 をサポートしていない。
・iCloud キーチェーンが有効になっていない。(iPhone)

**[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。

## ２．３．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。

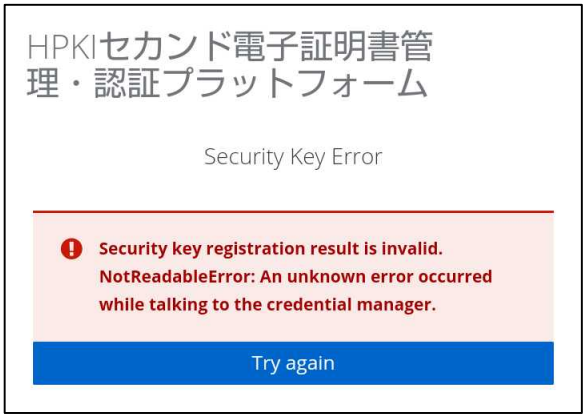
・生体認証に失敗した。
・生体認証を実施している最中にキャンセル操作をした。
・ブラウザまたは OS が FIDO をサポートしていない。
・iCloud キーチェーンが有効になっていない。(iPhone)
・スマートフォンに生体認証情報を登録していない。
・「TouchID とパスコード」で「パスコードをオフにする」設定になっている。(iPhone)

**[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（４．１参照）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。

## ２．４．NotReadableError: An unknown error occured while talking to the credential manager.

**[表示画面]**




**[原因]**

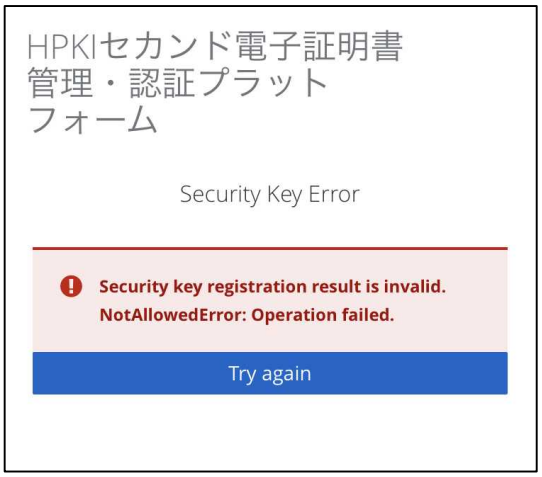
・生体認証後、不明なエラーが発生した。
・ブラウザまたは OS が FIDO をサポートしていない。

**[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。

## 2.5. 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)

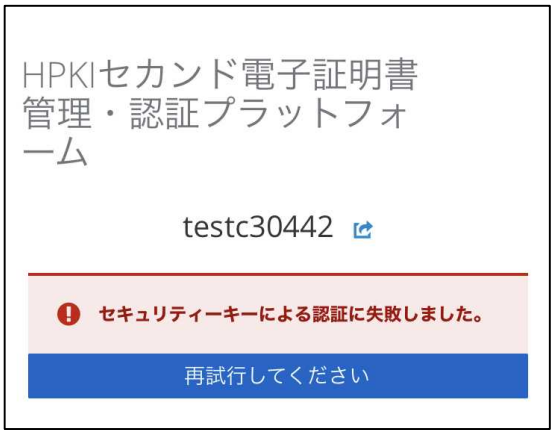
**[対策]**

・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。

## ２．６．セキュリティーキーによる認証に失敗しました。

**[表示画面]**




**[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（４．１参照）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。

## ２．７．NotAllowedError: The 'navigator.credentials.create' API is only permitted in applications with the 'com.apple.developer.web-browser' entitlement.

**[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。

## 2.8. NotAllowedError: The operation either timed out or was not allowed.

**[表示画面]**

**[原因]**

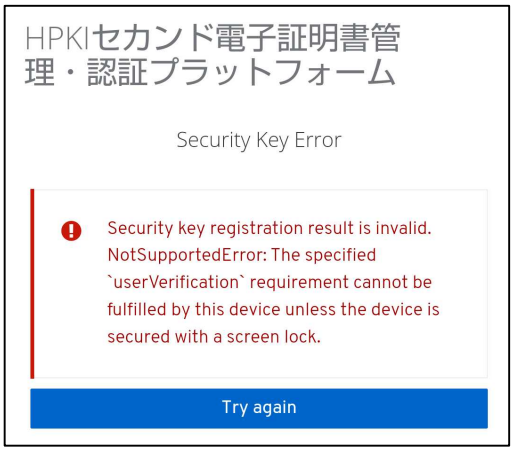
・ブラウザが FIDO2 をサポートしていない。

**[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。

## 2.9. NotSupportedError: The specified 'userVerification' 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。

## ２.１０.　403 Forbidden

**[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。

## ２．１１．　mahpki-auth.2nds.medis.or.jp でセキュリティキーを使用する

**[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。

## ２．１２．　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。

**[表示画面]**

**[原因]**

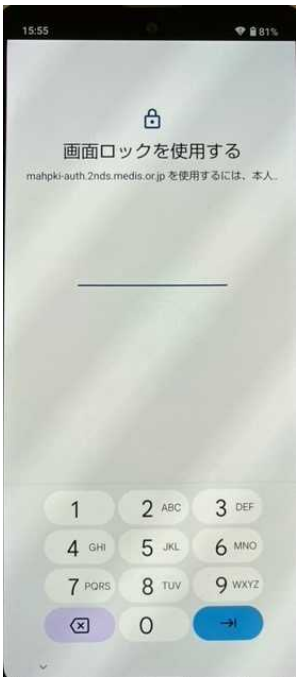
・「TouchID とパスコード」で「パスコードをオフにする」設定になっている
・サーバ側に記録してあるセカンド鍵情報とスマートフォン内に登録されているセカンド鍵情報が異なる。
　・認証開始時に入力した Username（本人 ID）が、スマートフォン内の FIDO 鍵と一致していない
　（認証開始時に誤った Username を入力した）
　・FIDO 鍵情報がスマートフォンから削除されている
　・FIDO 鍵の登録完了画面（処理が終了しました）で戻るボタンを押したうえ、再度登録行為を実施した。

**[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。

## ２.１３.　画面のロックを使用する

**[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 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。

## ２.１４.　パスコードで続ける

**[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

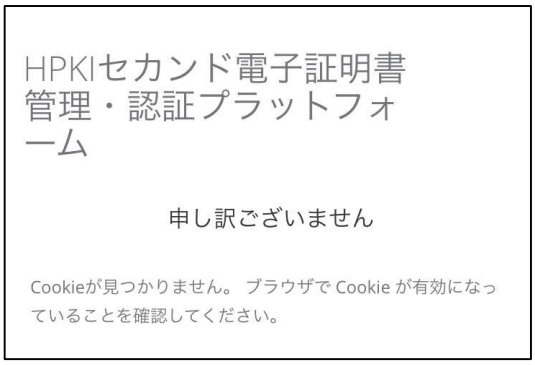
・FIDO 認証時に PIN 入力をタップした

**[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。

## ２.１５.　Cookie が見つかりません。

**[表示画面]**




**[原因]**

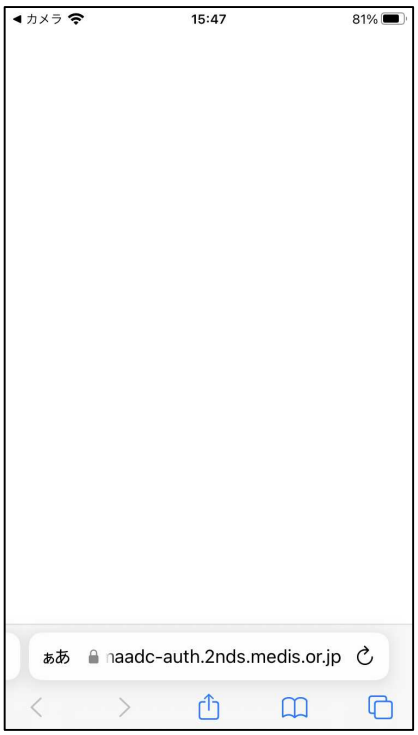
・ブラウザで Cookie をブロックする設定になっている。
・Android 端末の場合、Chrome の「サイトの設定」の「デバイス上のサイトデータ」の保存が OFF になっている。

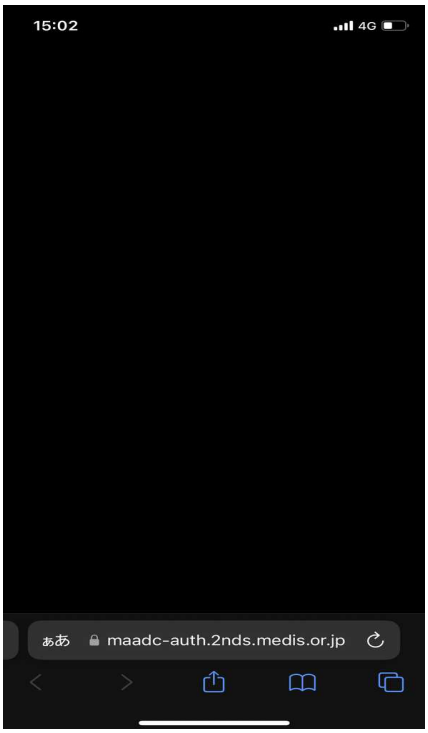
**[対策]**

・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。

## ２.１６.　（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/

## ２.１７.　スマートフォンの画面に QR コードが表示される

**[原因]**

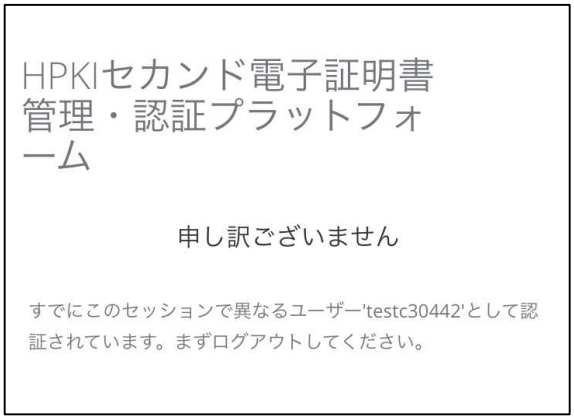
・登録しているスマートフォンと違うスマートフォンで認証しようとしている
・生体認証の設定の解除を行った
・「パスワード」に保存されている鍵を削除してしまった（iPhone）

**[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。

## ２.１８.　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。

**[表示画面]**




**[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。

## ２.１９.　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。

**[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。<br>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。

## ２.２０.　405 Method Not Allowed

**[表示画面]**

**[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。

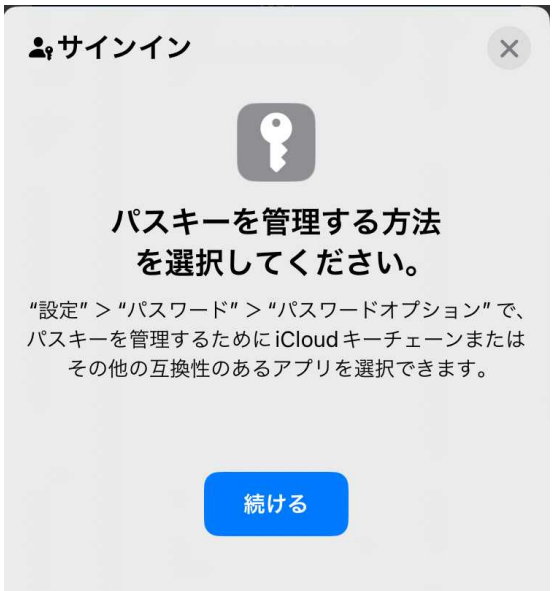
・本人 ID が自動で入力枠に入らなかった場合、再度カメラで QR コードを読み込んでください。

※再発する場合、４.１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。

## ２.２１.　パスキーを管理する方法を選択してください

**[表示画面]**




**[原因]**

・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。

## ２.２２.　Autheticator：パスキーを追加できませんでした

**[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。

## ２.２３.　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）

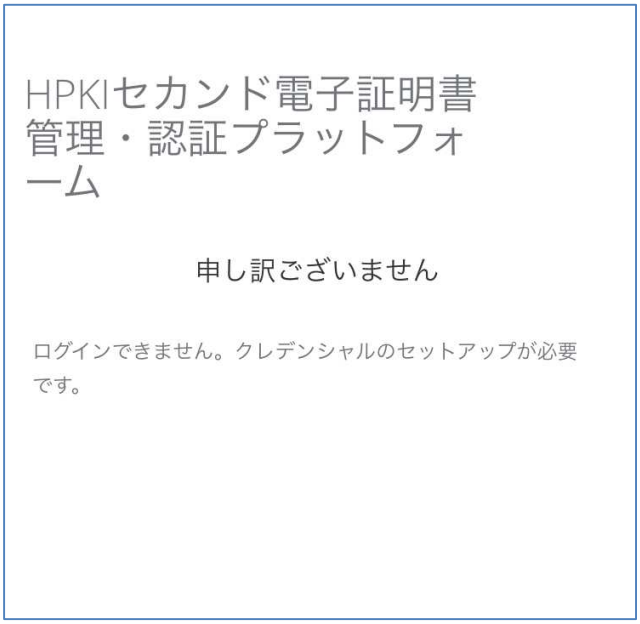
・FIDO 鍵情報がスマートフォンから削除されている
Android 端末においては、「設定」→「セキュリティとプライバシー」→「デバイスのロック解除」で「画面ロック」選択し、「新しい画面ロックの選択」で「なし」または「スワイプ」に変更すると、登録済の情報が削除されます。

**[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。

## 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。

**[表示画面]**




**[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。

# 3　PC でのメッセージ

## 3．1．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４．２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。

## ３．２．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]**

**[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４．２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。

## 3.3.このページは現在機能していません

**[表示画面]**

**[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。

## ３．４．HPKI(JPKI)証明書のユーザが無効となっています。

**[表示画面]**

＜HPKI 認証の場合＞

＜JPKI 認証の場合＞

**[原因]**

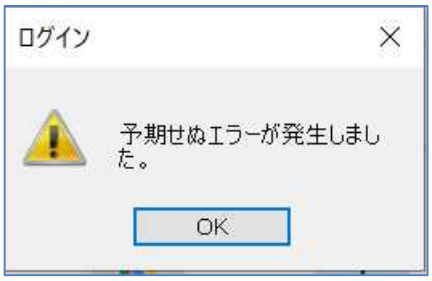
・当該ユーザが無効になっている（削除されている）状態で HPKI 認証を実施した。
・当該ユーザが無効になっている（削除されている）状態で JPKI 認証を実施した。

**[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。

## ３．５．予期せぬエラーが発生しました。

**[表示画面]**




**[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４．１を参照してください)

## ３．６．Cookie が見つかりません。

**[表示画面]**

**[原因]**

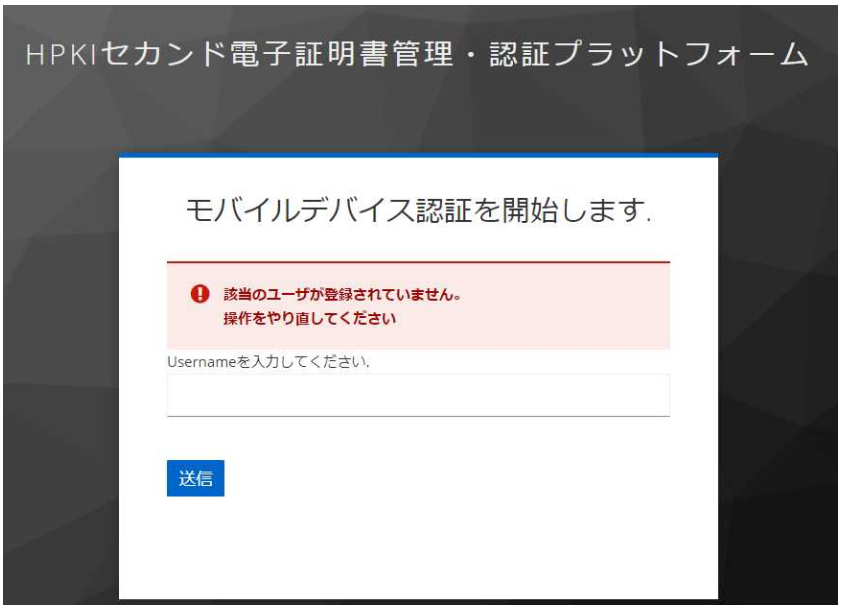
・他のユーザで認証された状態で認証を行った。(ブラウザにキャッシュの情報が残っており、悪影響を与えている場合があります)

**[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４．１を参照してください)

## 3.7.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。

## 3.8.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。

## 3.9.デバイス認証でエラーが発生しました。

**[表示画面]**

**[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。

・デバイス認証画面（QR コードが表示された画面）でキャンセルボタンを選択した場合に、まれにこの画面が出ることがあります。

**[対策]**

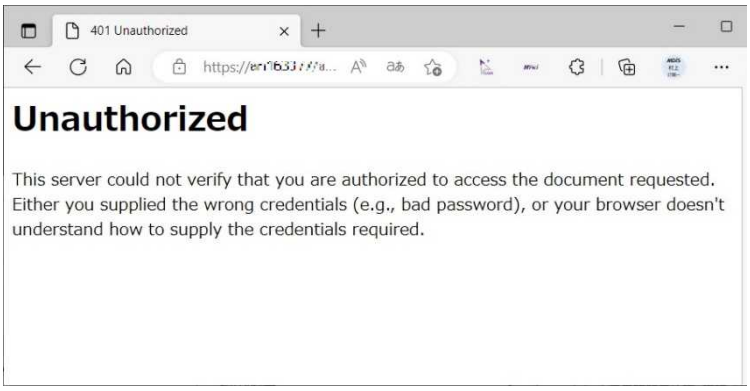
・ブラウザを一度終了してから再度認証してください。

・ブラウザのキャッシュをクリアしてください。

・キャンセルボタンを押した結果、この画面が出た場合は、特に問題はありませんので、そのままブラウザを閉じてください。

## ３.１０.　Unauthorized

**[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。

## ３.１１.　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＞

**[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。

## ３.１２.　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。

## ３．１３．　「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

**[表示画面]**

**[原因]**

・拡張機能がインストールされていない。

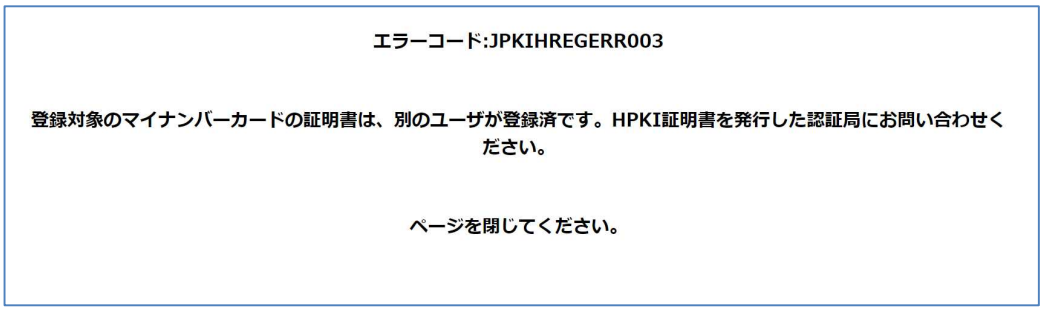
・拡張機能が有効になっていない。

**[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。

## ３．１４．　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。

**[表示画面]**




**[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。

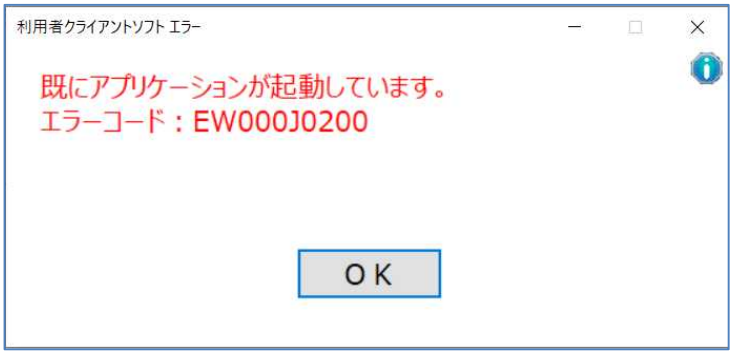
（一人で複数の HPKI カードをお持ちの場合でも、マイナンバーカードはそのうちの一つにしか登録することができません）

**[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。

## ３．１５．　既にアプリケーションが起動しています。

**[表示画面]**




**[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。

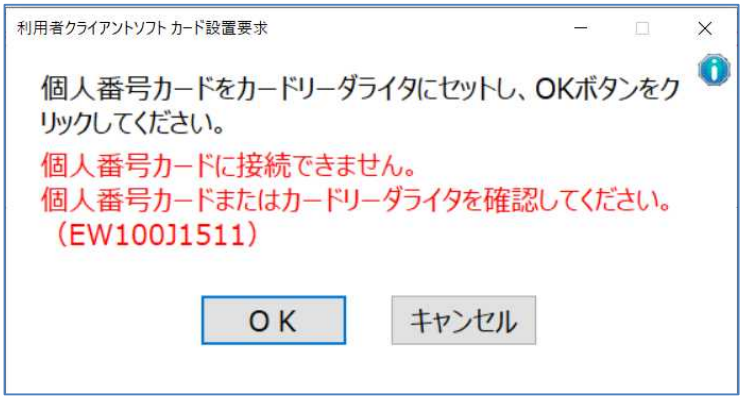
**[対策]**

・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。

## ３．１６．　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。

## ３．１７．　Forbidden

**[表示画面]**

# 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。

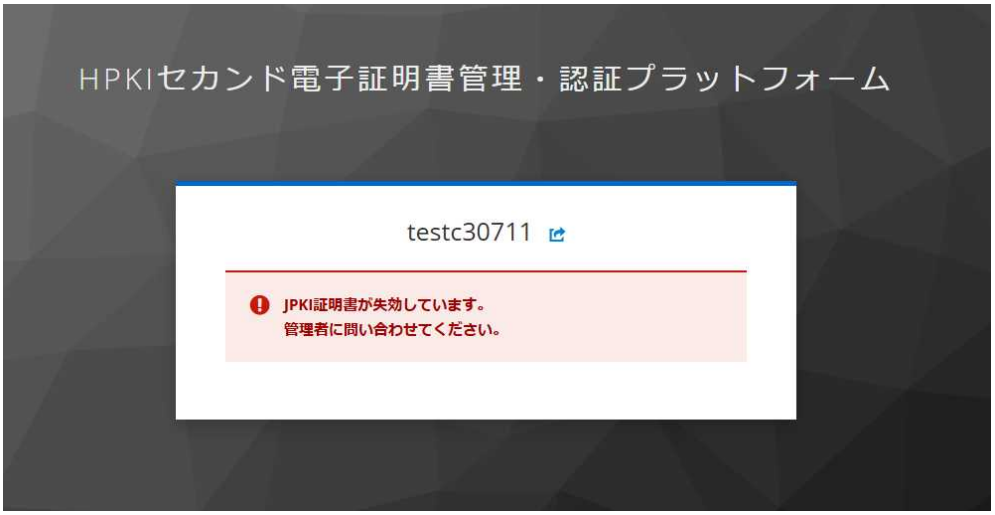
・ネットワークに原因がある場合は、ネットワークの管理者にお問い合わせください。

## ３.１８.　HPKI(JPKI)証明書が失効しています。

**[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。

## ３.１９.　HPKI(JPKI)認証でエラーが発生しました。

**[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。

## ３.２０.　マイナンバーカードに紐づくユーザが存在しません。

**[表示画面]**

**[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。

※一部のアプリケーションでは、マイナンバーカード更新後にマイナンバーカードによる認証を行った際に HPKI-KAGURA に誤った情報で更新されたため正しく認証できなくなるケースが報告されています。

**[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。
=>利用者マニュアルの「２.４.マイナンバーカード登録」を参照してください）

## ３．２１．　mahpki-auth.2nds.medis.or.jp へのアクセスが拒否されました

**[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４．２を参照してください）

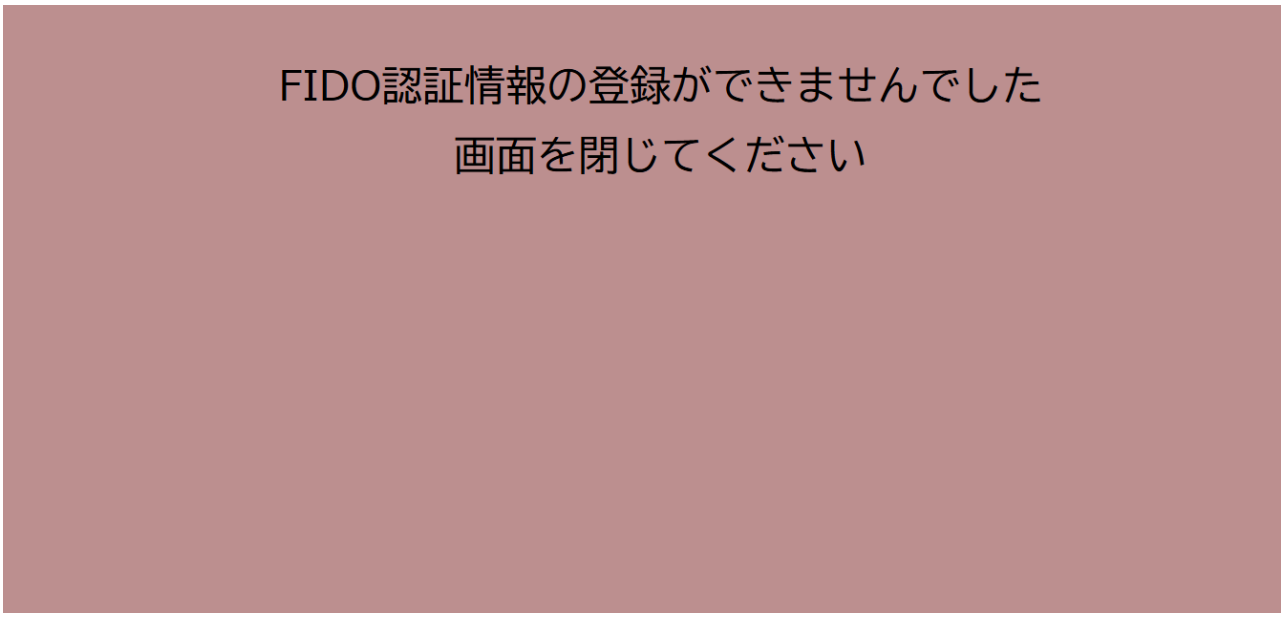
・IC カードは有効なものであるか（期限切れカードでないか等）確認してください。

・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。

## ３.２２.　FIDO 認証情報の登録ができませんでした




**[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。

## ３.２３.　情報不足のため、この証明書を検証できません。

**[原因]**

・上位証明書が PC に登録されていない。

※HPKI 証明書では上位証明書である日本医師会/MEDIS 認証局および厚生労働省ルート証明書がインストールされていない状態で証明書の詳細表示を行った場合に表示されます。

**[対策]**

・該当する上位の証明書をインストールする。

※上位証明書を PC にインストールしなくても、認証時に HPKI-KAGURA 側で必要な証明書情報を取得して確認を行っているため HPKI/JPKI 認証は成功します。

## ３.２４.　この証明書の整合性を保証できません。

**[原因]**

・古い上位証明書が登録されている。

**[対策]**

・該当する最新の上位の証明書をインストールする。

※日本医師会認証局は 2024/11/15、MEDIS 認証局は 2025/3/17 に CA 証明書が更新されています。

※上位証明書を PC にインストールしなくても、認証時に HPKI-KAGURA 側で必要な証明書情報を取得して確認を行っているため HPKI/JPKI 認証は成功します。

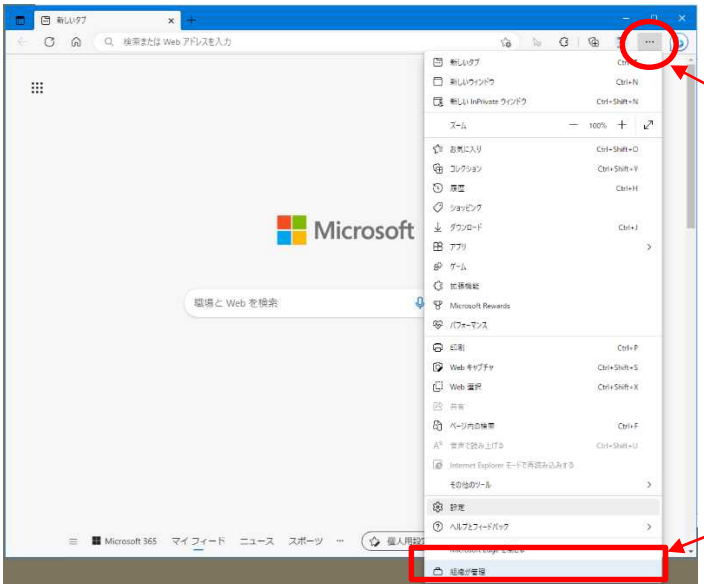
# 4　各種設定の確認・変更方法

## 4．1．ブラウザのキャッシュクリア

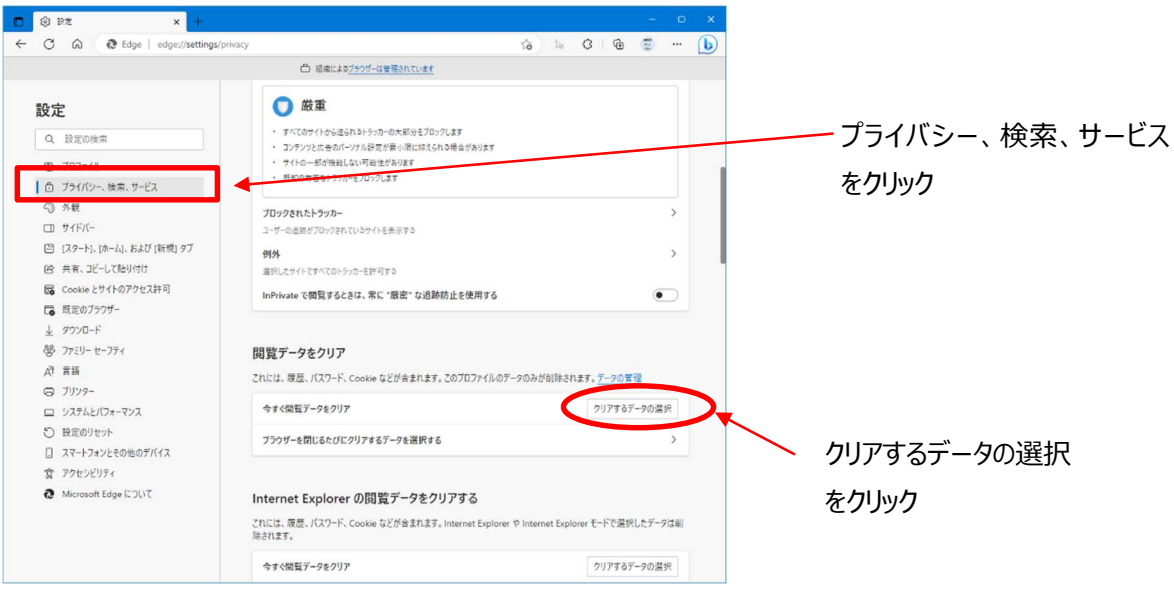
操作する PC のブラウザにキャッシュが残っている場合、正常に認証ができない場合があります。以下の方法でキャッシュをクリアしてください。

a）Edge(PC)の場合

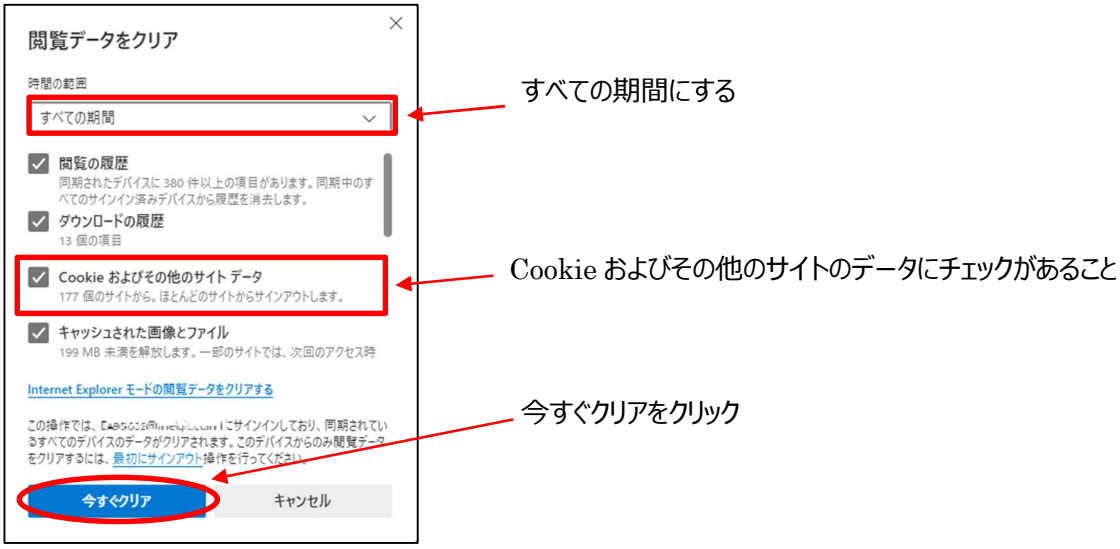
メニューマークをクリックし、メニュー選択画面の「設定」をクリックします。




「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。

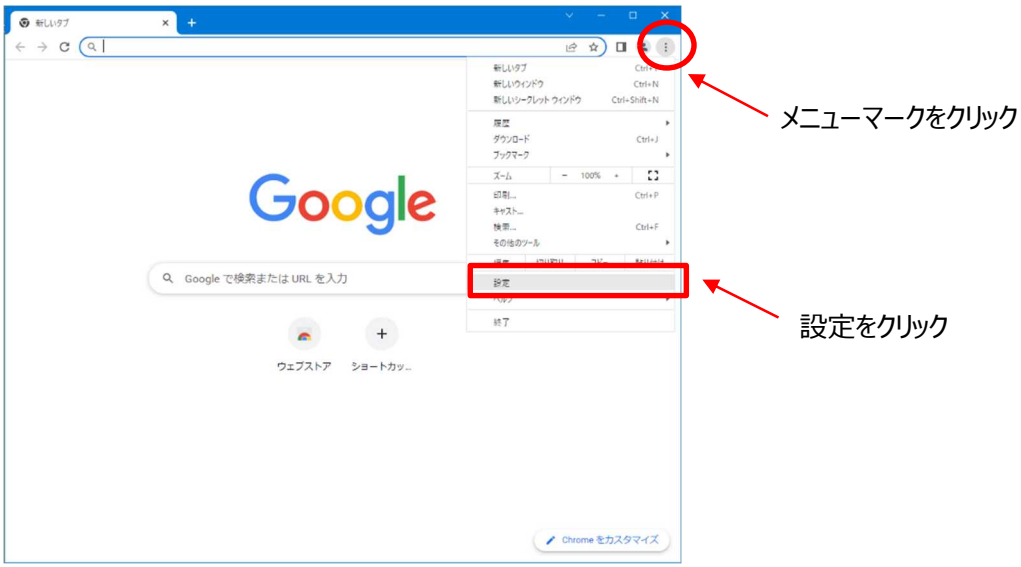



時間の範囲を“すべての期間”とし、”Cookie　およびその他のサイトのデータ”にチェックを入れて「今すぐクリア」のボタンをクリックします。

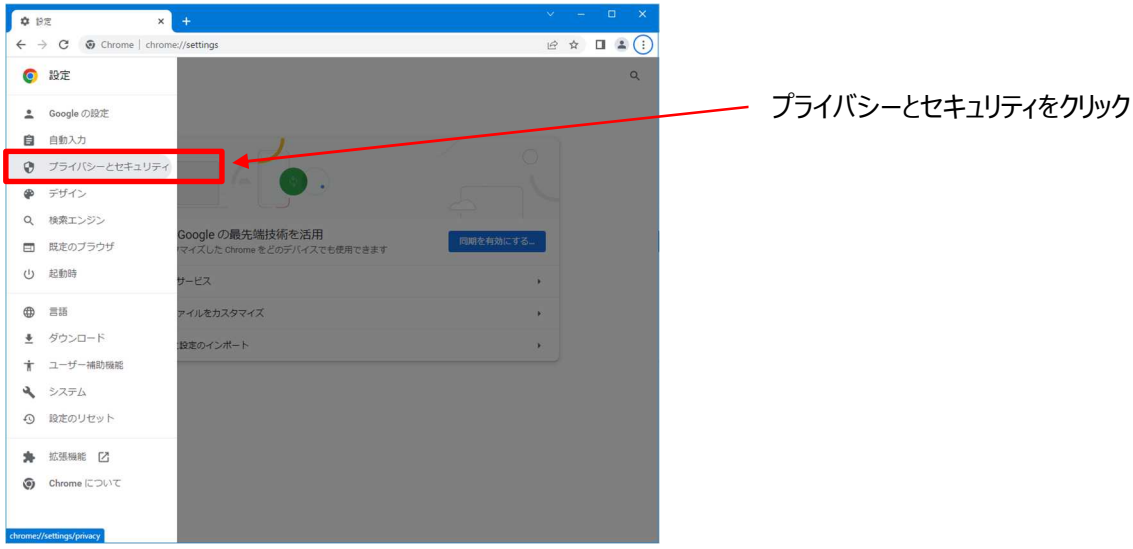



b) Chrome(PC)の場合

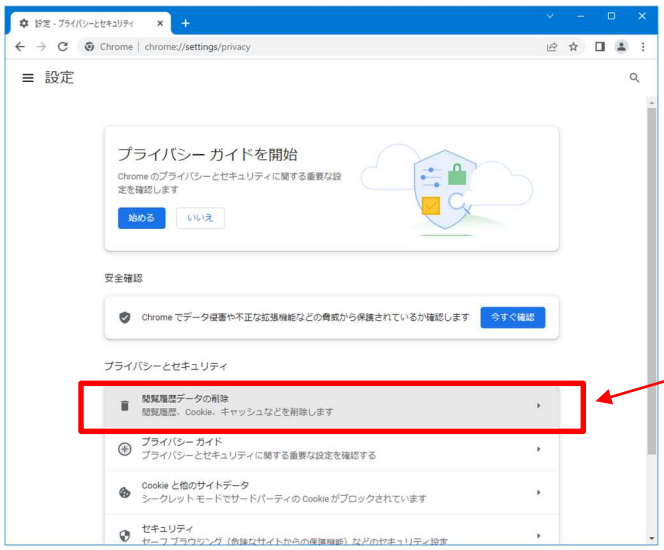
「メニューマーク」をクリックしてメニュー一覧を開き「設定」をクリックします。




「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。




閲覧履歴データの削除をクリック

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。

全期間にする

Cookie と他のサイトのデータにチェックがあること

「データを削除」をクリック

c) Safari(iPhone)の場合

① iOS17 以前

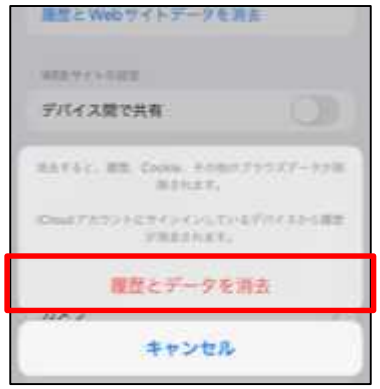
iPhone の設定を開き、Safari をタップします。

Safari をタップ

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。

「履歴と Web サイトデータを消去」をタップ

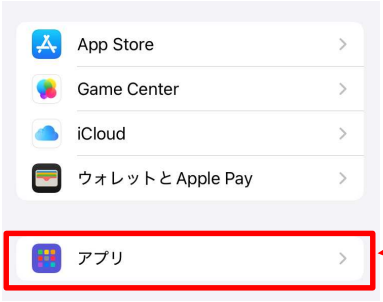
確認画面が表示されるため、「履歴とデータを消去」をタップします。




「履歴とデータを消去」をタップ

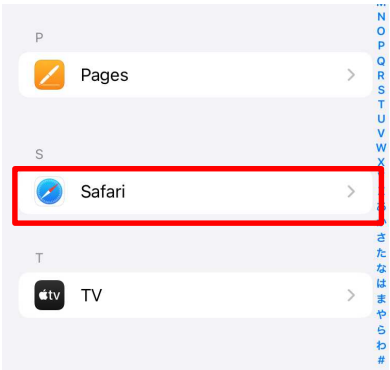
② iOS18 以降

iPhone の設定を開き、「アプリ」をタップします。




アプリをタップ

「Safari」をタップします。




Safari をタップ

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。

「履歴と Web サイトデータを消去」をタップ

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。

チェック

「履歴を消去」をタップ

d) Chrome(Android)の場合

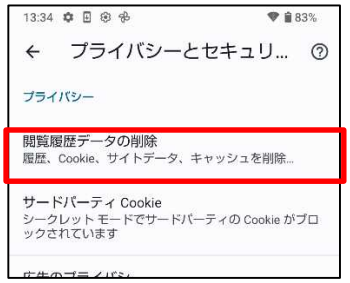
Chrome のアプリを開き、メニューを開き「設定」をタップします。

「設定」をタップ

プライバシーとセキュリティをタップします。

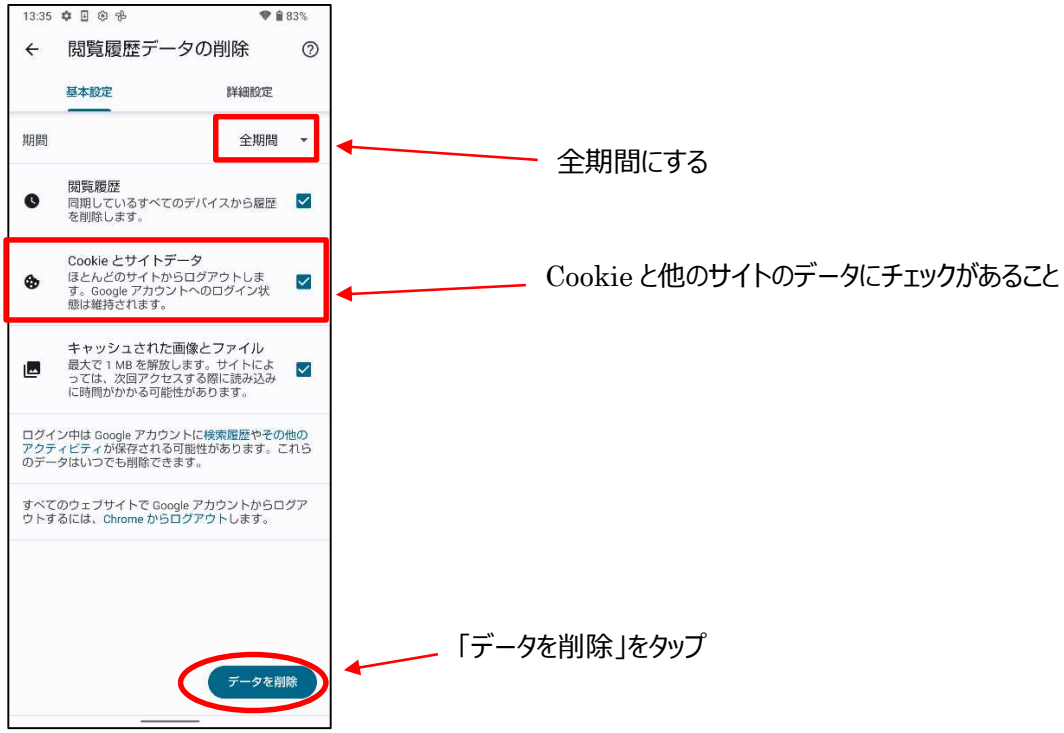
プライバシーとセキュリティをタップ

閲覧履歴データの削除をタップします。



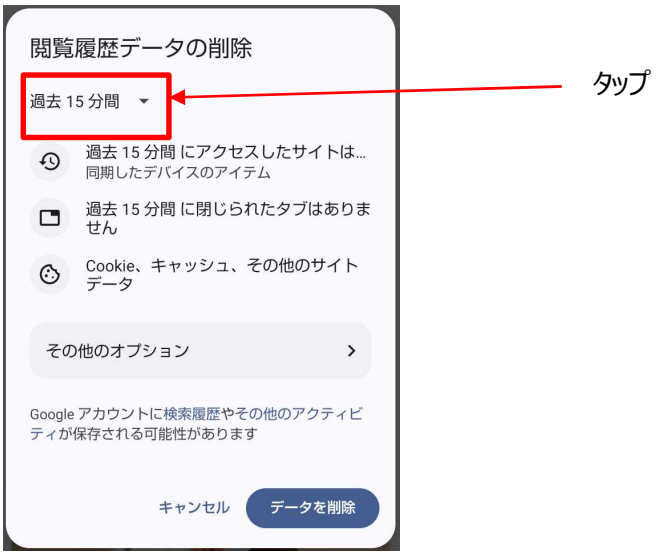

閲覧履歴データの削除をタップ

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。

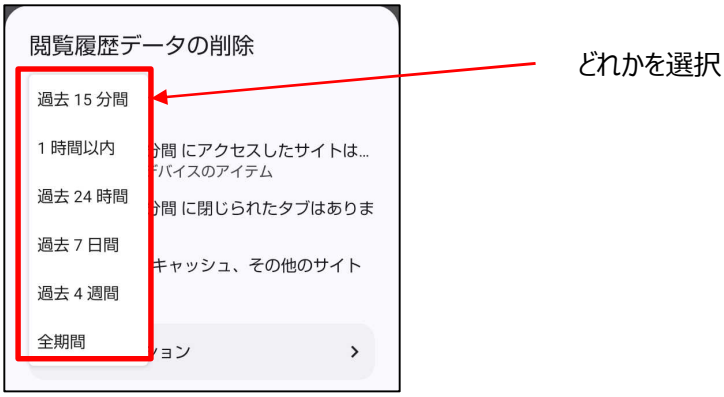



再度、Chrome のメニューを開き「閲覧履歴データの削除」をタップします。

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）



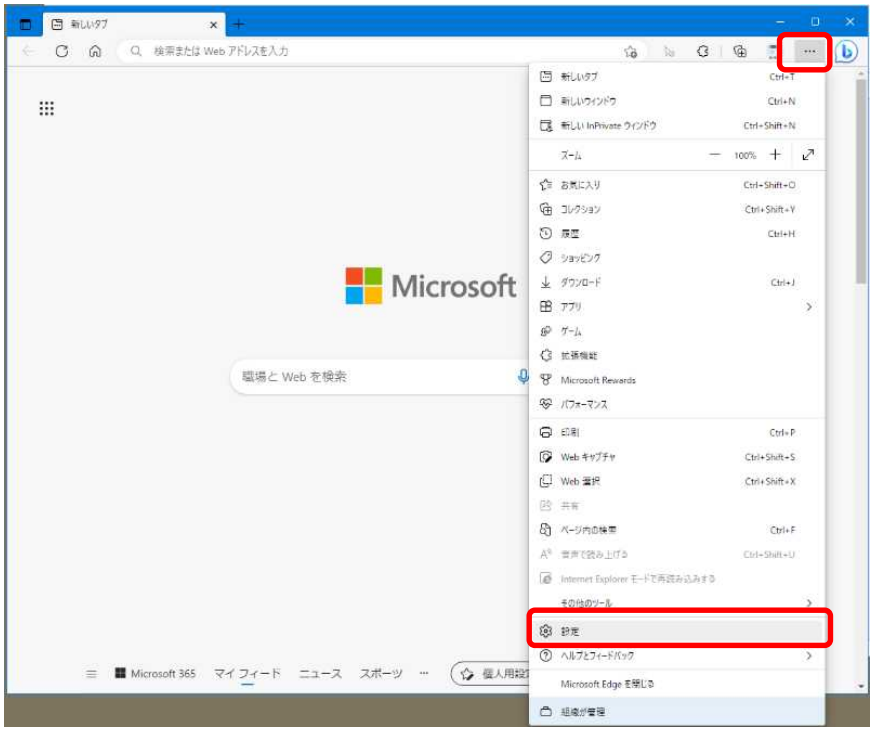

「データを削除」をタップします。

## ４．２．IC カードからの証明書の読み取り確認

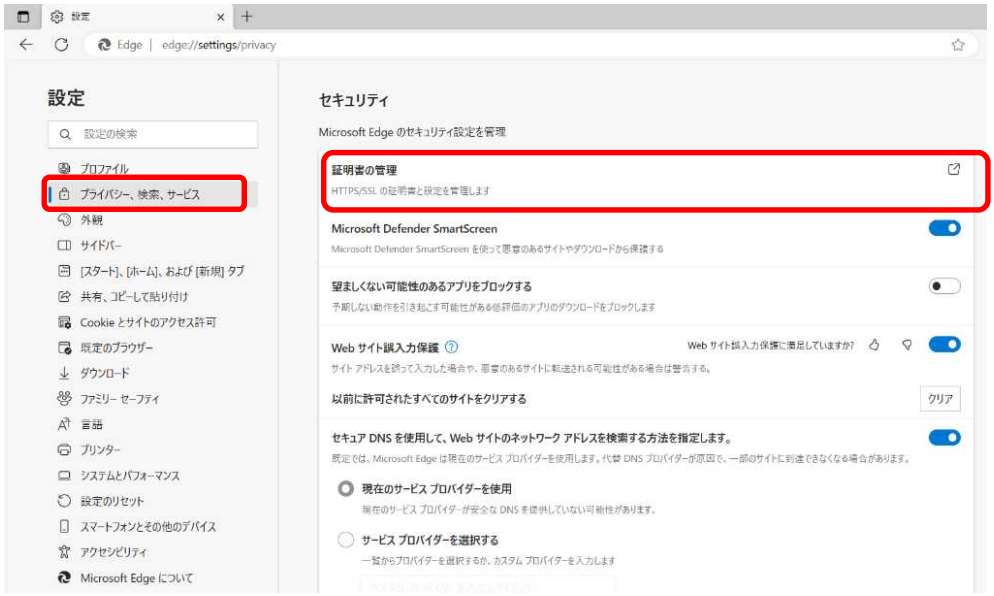
IC カードが PC から正しく読み取ることができない場合、HPKI 認証（または JPKI 認証）に失敗します。正しく読み取ることができているか IC カードを IC カードリーダライタにセットした上、以下の方法にて確認してください。

（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。




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。

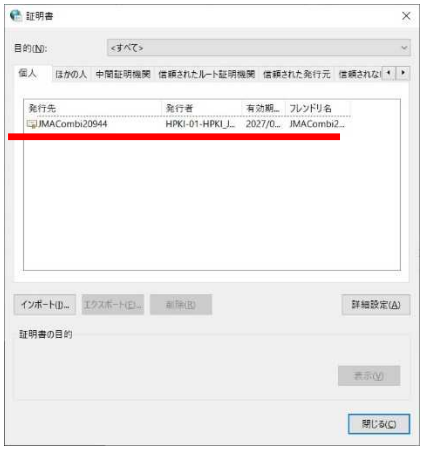



③「個人」タブを選択すると証明書の一覧が表示されます。 証明書ウィンドウに以下の証明書の情報が表示されてい

るか確認してください。

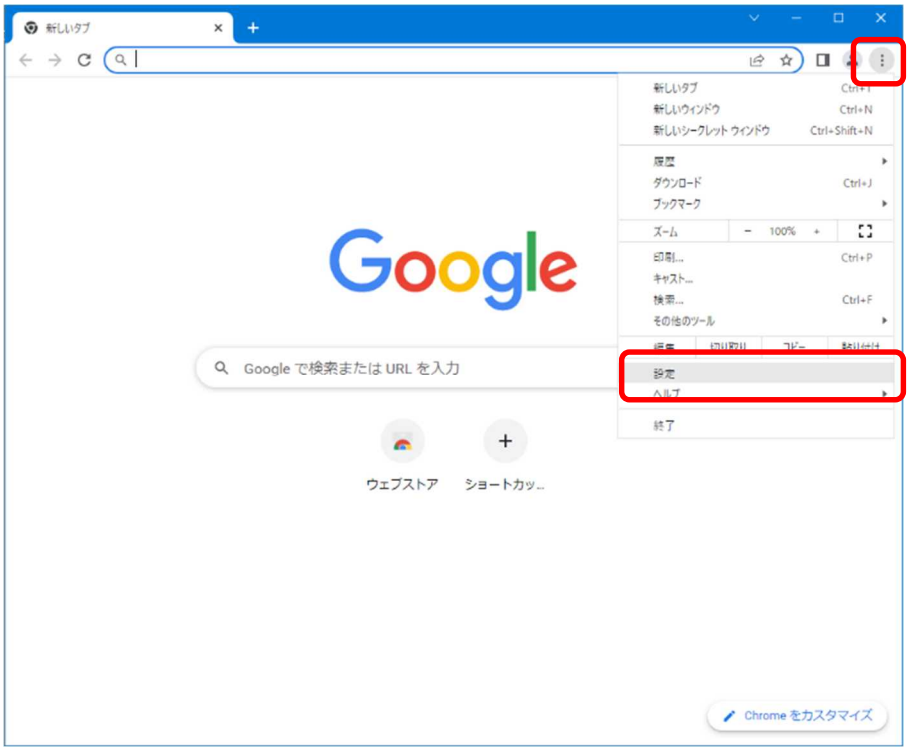
・HPKI カードの証明書：発行者が HPKI-…で記載されているもの

・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

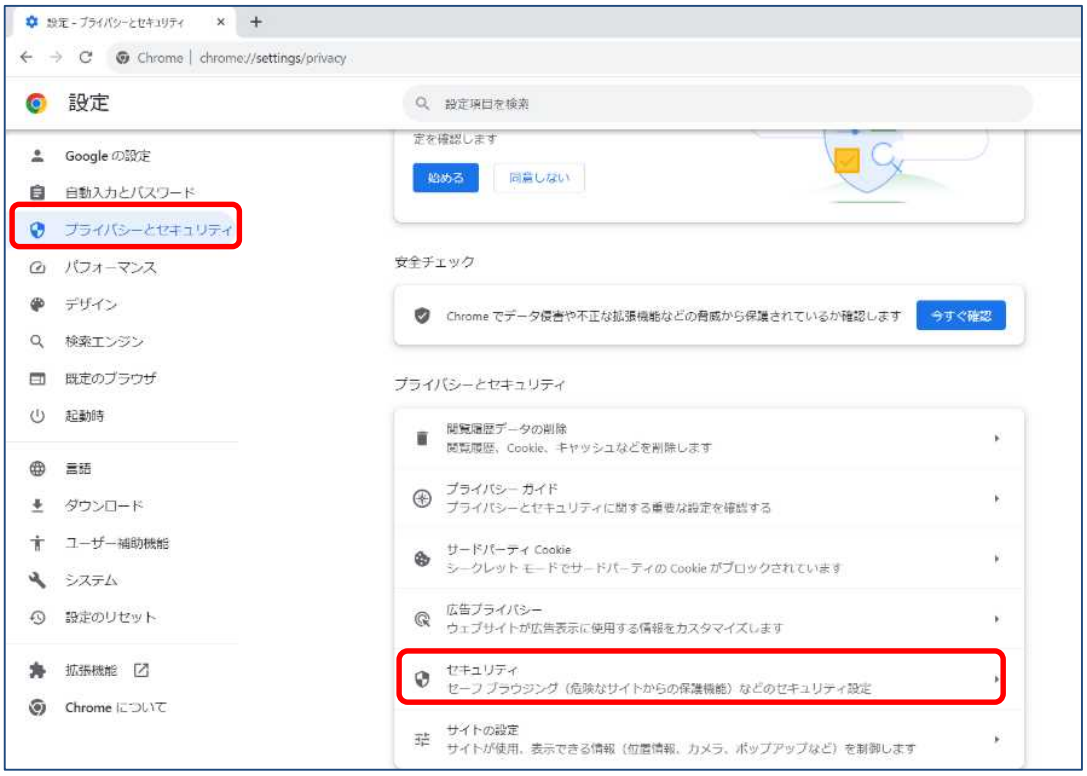



（２） Chrome からの確認

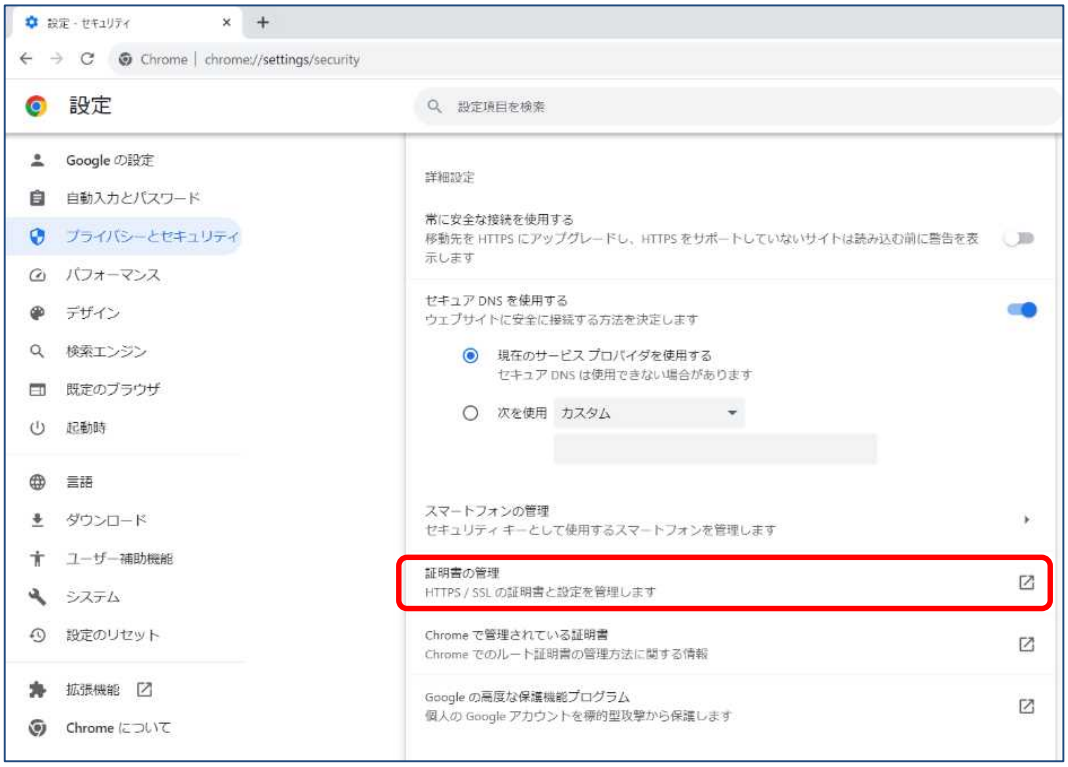
①Chrome を起動し、画面右上の[⋮]から[設定]メニューを押してください。



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。




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。

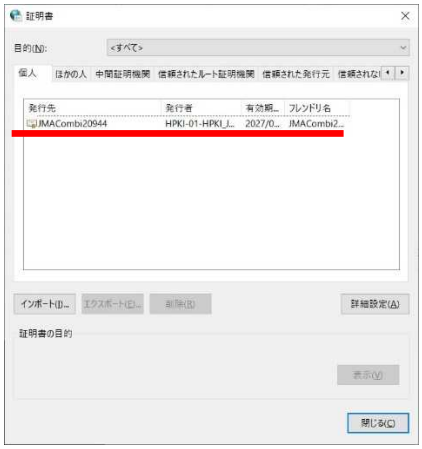


④「証明書マネージャ」画面が表示されるので、「ローカル証明書」の「Windows からインポートした証明書を管理する」を選択して、証明書管理画面を表示させます。

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。

## 4.3.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。

Safari をタップ

Safari をタップし、「デフォルトのブラウザ App」をタップします。

デフォルトのブラウザ App をタップ

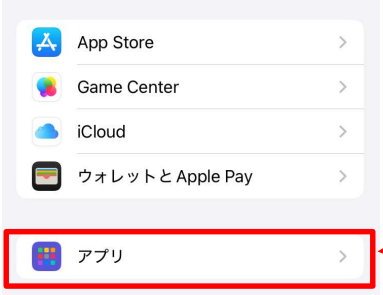
※デフォルトのブラウザが Safari の場合“デフォルトのブラウザ App”の項目は出てきません

Safari を選択すると、Safari にチェックマークが表示されます。

Safari にチェックマークがつける

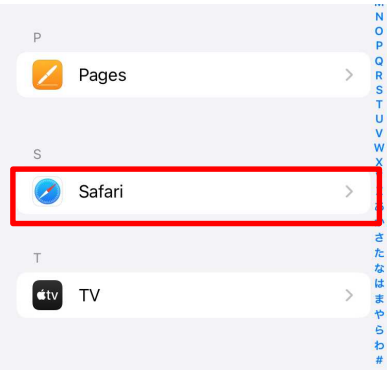
b) iOS18 以降

iPhone の設定を開き、「アプリ」をタップします。




アプリをタップ

「Safari」をタップします。




Safari をタップ

「デフォルトのブラウザアプリ」をタップします。

デフォルトのブラウザアプリをタップ

Safari を選択すると、Safari にチェックマークが表示されます。

Safari にチェックマークがつける

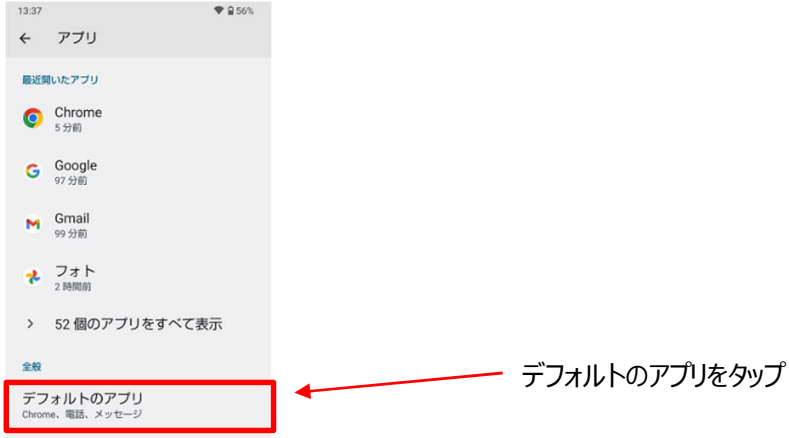
B）Android の場合

Android デバイスで設定を開きます。

[アプリ] をタップします。

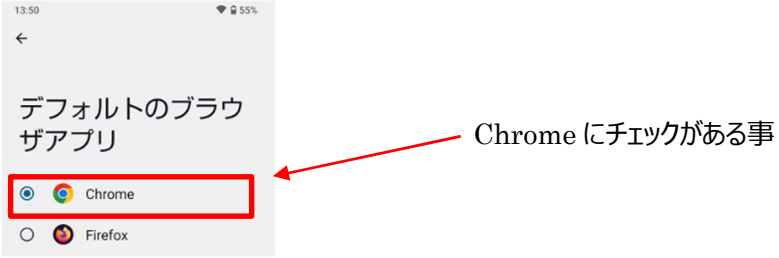
アプリをタップ

“全般”で［デフォルトのアプリ］をタップします。




［ブラウザアプリ］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。



## ４．４．スマートフォンの OS,ブラウザのバージョン確認

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。

一般をタップ

「情報」をタップします。

情報をタップ

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

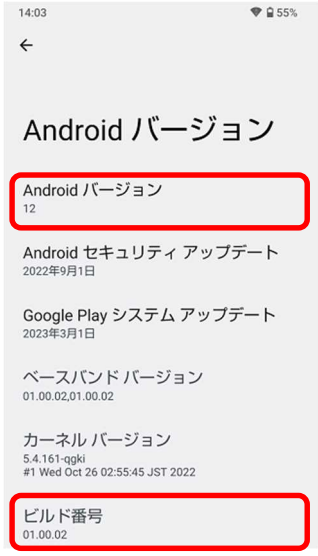
スマートフォンの設定アプリを開き、[デバイス情報]をタップしますます。

デバイス情報をタップ

[Android バージョン] をタップします。

Android バージョンをタップ

“Android バージョン”、”ビルド番号”をお知らせ願います。




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。

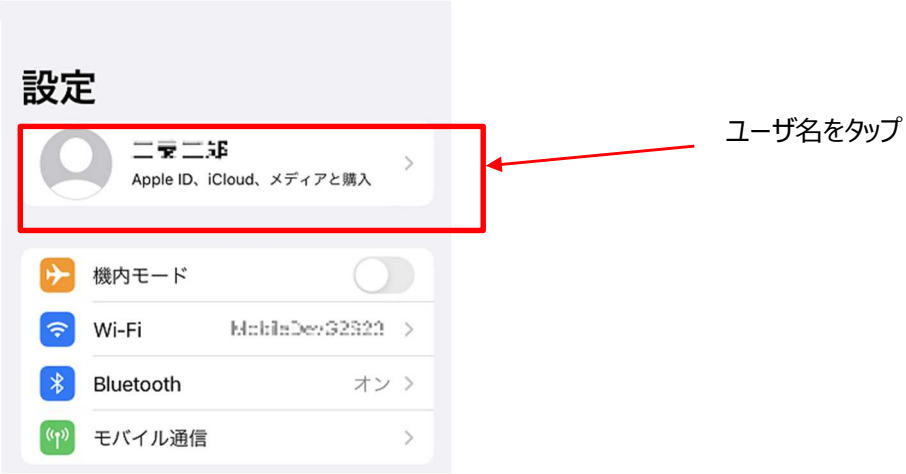
chrome://version
chrome
Google LLC
Copyright 2023 Google LLC. All
rights reserved.
Google Chrome: 111.0.5563.116
(Official Build)
（32 ビット）
変更履歴: 7f37e256a2a5cd4512a
7b7ecb0ca12d6fb9b83
e8-refs/branch-
heads/5563@{#1208}
OS: Android 12; SH-M24
Build/S922C

## 4.5. iCloud キーチェーンを有効にする

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。

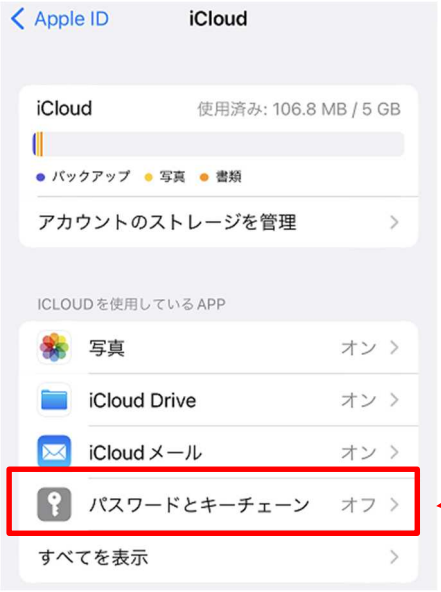
A) iOS17 以前

「設定」をタップし、「[ユーザ名]」をタップします。



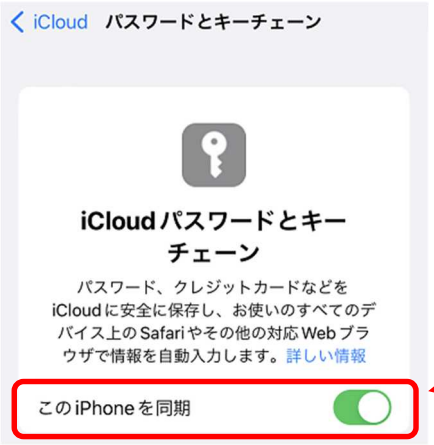

「iCloud」をタップします。

「パスワードとキーチェーン」をタップします。




パスワードとキーチェーンをタップ

「iCloud キーチェーン」をオンにします。




ON にする

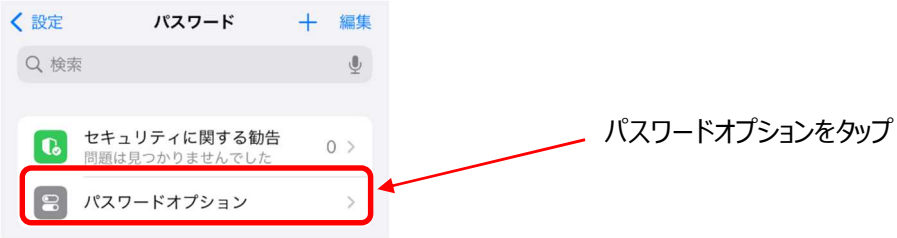
※パスコードまたは Apple ID のパスワードの入力を求められる場合があります。

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。

パスワードをタップ

「パスワードオプション」をタップします。

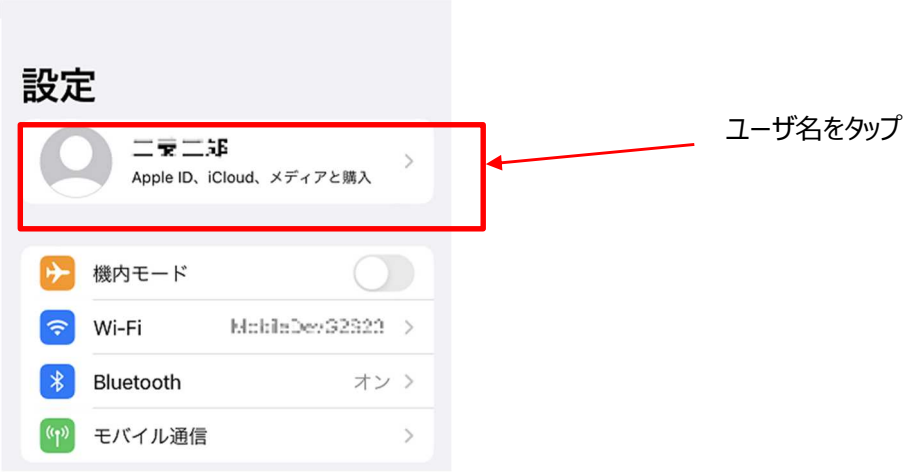



「パスワードとパスキーを自動入力」が ON になっていない場合は ON にします。
「次の提供元からのパスワードとパスキーを使用」の欄にある「iCloud キーチェーン」が ON になっていない場合は ON にします。（iOS17.4 以降）

※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

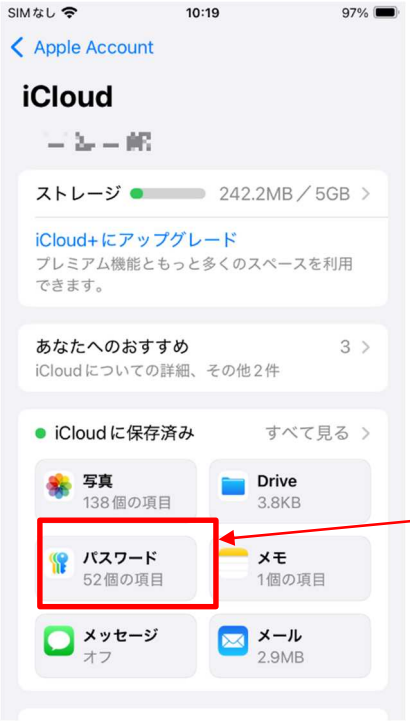
「設定」をタップし、「[ユーザ名]」をタップします。



「iCloud」をタップします。

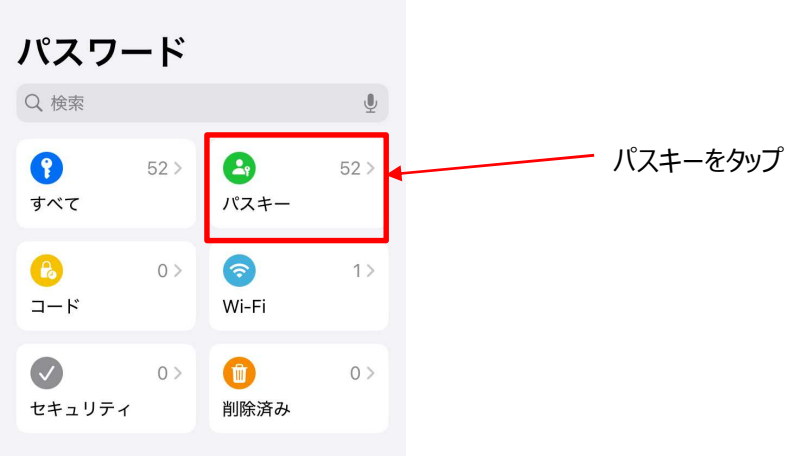
iCloud をタップ

「パスワード」をタップします。

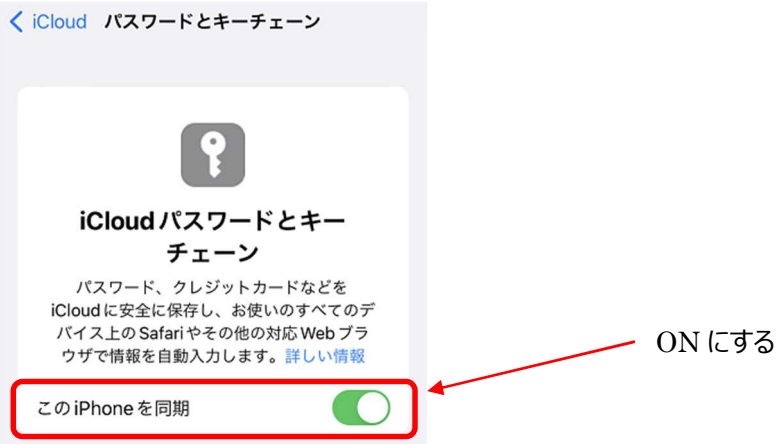



パスワードをタップ

「パスキー」をタップします。




「この iPhone を同期」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。

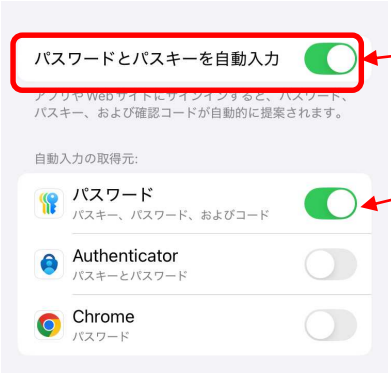
また、パスワードオプションにて iCloud キーチェーンが動作する設定が必要です。

”設定”から「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。

自動入力とパスワードを
タップ

「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。




ON にする

ON にする

# 4.6.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

Safari(iPhone)の画面

アドレスバーが横幅いっぱいに広がっている。
※アドレスバーが下に表示されているケースもあり

戻る、進む、共有、ブックマーク、タブのメニューが表示されている

Chrome(Android)の画面

家のマークの横にアドレスバーが表示
タブ数やメニューボタンが表示

OS のボタンが表示されている
（Chrome としてのボタン表示なし）

違うブラウザの例

アドレスバーのデザインが異なっている

広告が表示されている

操作ボタンのアイコンが異なっている