# リモート署名

# クライアントアダプタサービス

# インストール手順書

# v2.00版

## 2023/12/26

## 改版履歴

版	内容	日付
1.00	新規作成	2022/12/26
1.10	・プロキシ設定を追加	2023/2/2
1.20	Window10 32bit 環境サポートを追記	2023/3/8
2.00	マイナンバーカード認証に伴う設定追加	2023/12/26
	1)設定ファイルにマイナンバーカード認証用設定を追加	
	2)認証選択画面用の設定を追加	

## 目次

1	対応	応プラットフォーム	5
	1.1	対応プラットフォーム一覧	5
	1.2	推奨スペック	5
2	事前	前準備	6
	2.1	セキュリティおよびネットワーク	6
	2.2	モジュール入手	6
	2.3	接続情報の入手	6
3	概要	要説明	7
	3.1	構成	7
	3.2	クライアントアダプタの FQDN の統一化	8
4	IJŦ	モート署名クライアントアダプタ設定(Windows)	
	4.1	モジュール確認	
	4.2	モジュール配置	
	4.3	各種設定	11
	4.3	3.1 鍵管理サービス設定	11
	4.3	3.2 サーバ設定(ポート・HTTPS)	12
	4.3	3.3  認証選択画面設定	12
	4.4	起動・終了	12
	4.5	トークン管理(メンテナンス機能)	14
	5.1	モジュール確認	16
	5.2	モジュール配置	16
	5.3	各種設定	
	5.3	3.1 鍵管理サービス設定	
	5.3	3.2 サーバ設定(ポート・HTTPS)	
	5.3	3.3 認証選択画面設定	
	5.4	起動・終了	
	5.5	トークン管理(メンテナンス機能)	21

Windows10、Windows 11、Windows Server2019、Widows Server2022,は Microsoft Corporation の商標または登録商標です。

- 1 対応プラットフォーム
  - 1.1 対応プラットフォーム一覧
  - Windows10 64bit, 32bit
  - Windows11
  - Windows Server 2019
  - Windows Server 2022
  - Linux (Ubuntu 22.04 にて検証)
  - 1.2 推奨スペック
  - 上記オペレーティングシステムが動作する Intel 互換 CPU 搭載の IBM PC 互換機
  - メモリ 8GB 以上推奨

#### 2 事前準備

- 2.1 セキュリティおよびネットワーク
- 最新の「医療情報システムの安全管理に関するガイドライン(現:第5.2版)」に
   従い、十分なセキュリティ対策を実施したサーバに運用をさせること
- パラメータシートに記載される認証サービスとの通信が許可された状態であること
- 2.2 モジュール入手
- ダウンロードサイトより関連モジュールを取得しておくこと
- **2.3** 接続情報の入手

検証サイトに接続するためには以下の情報が必要になります。

[入手]

- (検証サイト)HPKI セカンド電子証明書接続情報パラメータシート
- (検証サイト) クライアント認証用証明書およびパスワード
- テスト用HPKIカード(もしくはHPKIカードファイル証明書)

#### 3 概要説明

3.1 構成

### ◆クライアントアダプタ利用構成



### ◆クライアントアダプタ利用構成例



3.2 クライアントアダプタの FQDN の統一化

リモート署名クライアントアダプタにより Web サーバが Server 名称とポート番号を確保 します。

サーバ名称	hpkicardless-clientadapter-server
ポート	3000

サーバ名称の設定としては以下の方法が考えられますが、環境に応じて設定をいただくようお願いします。

- 1) DNS へ登録する
- 2) サーバのマシン名そのものを変更する
- 3) サーバのマシン名に複数マシンを付与する
- 4) アクセスする端末の hosts を変更する

OpenID Connect の仕組み上、OpenID Provider はリダイレクト先(リモート署名クラ イアントアダプタのサーバ URL)をチェックしているため、上記のようにサーバ名称を設 定するようにお願いします。

もし上記のサーバ名称やポートを合わせられない場合は、個別に申請をお願いします。



1 OpenID Connect の仕組み

# インストール手順(Windows)

- 4 リモート署名クライアントアダプタ設定(Windows)
  - 4.1 モジュール確認

RemoteSignatureClientAdapter¥win-x64 (64bit 環境)

RemoteSignatureClientAdapter¥win-x86 (32bit 環境)

ファイル名	説明
client-adapter-win.exe	実行ファイル
config.json	設定ファイル

4.2 モジュール配置

RemoteSignatureClientAdapter¥win-x64 (64bit 環境) RemoteSignatureClientAdapter¥win-x86 (32bit 環境) のいずれかをインストールフォルダヘコピーしてください。

## 4.3 各種設定

接続先パラメータシートを参考に config.json の設定値を確認してください。

4.3.1 鍵管理サービス設定

authentication		
hpki (HPKI 認証設定)		
realm	レルム名	
auth-server-url	認可エンドポイント URL	
resource	クライアント ID	
credentials (クレデンシ	· ヤル情報)	
secret	クライアントアプリ認証用シークレット情報	
fido (FIDO 認証設定)		
realm	レルム名	
auth-server-url	認可エンドポイント URL	
resource	クライアント ID	
credentials (クレデンシャル情報)		
secret	クライアントアプリ認証用シークレット情報	
jpki (マイナンバーカード認証設定)		
realm	レルム名	
auth-server-url	認可エンドポイント URL	
resource	クライアントID	
credentials (クレデンシャル情報)		
secret	クライアントアプリ認証用シークレット情報	

server		
port	クライアントアダプタサービスのポート番号	
	動作する端末にて重ならない番号を設定すること	
enableHttps	httpsの有効=true/無効=falseを設定	
httpsOptions (https 設定情報)	· ※https を利用しない場合は不要	
key	秘密鍵証明書のファイルパス	
cert	公開鍵証明書のファイルパス	
passphrase	上記ファイルより証明書を取り出すためのパスフレーズ	
enableCors	クロスオリジン要求(CORS)の有効=true/無効=false	
	を設定	
corsOptions (CORS 設定情報) ※CORS を使用しない場合は不要		
origin	許可するオリジンを設定	
proxy	プロキシ URL を設定する	
	※使用しない場合は不要	
disableTlsRejectUnauthorize	証明書エラーを無視する	
d	無視する=true/無視しない=false	

## 4.3.2 サーバ設定(ポート・HTTPS)

### 4.3.3 認証選択画面設定

displayAuth	
hpki HPKI カード用認証ボタンの表示	
	表示=true / 非表示=false
fido	デバイス認証(FIDO)ボタンの表示
	表示=true / 非表示=false
jpki	マイナンバーカード用認証ボタンの表示
	表示=true / 非表示=false

## 4.4 起動・終了

起動: client-adapter-win.exe を実行

コンソールウィンドウが表示されます。

初回起動時に以下のような確認画面が表示された場合は、適切なファイアウォール設定を

行ってください。

🔐 Wind	ows セキュリティの重要な兽	告		×
۲	このアプリの機能の ています	いくつかが Windows	s Defender ファイアウォールでブ	ロックされ
すべての/ JavaScrip	パブリック、プライベート、ドメ・ it Runtime の機能のいくつ 名前( <u>N</u> ): 発行元( <u>P</u> ): パス( <u>H</u> ):	イン ネットワークで、Windov かがブロックされています。 Node.js JavaScrip Node.js	vs Defender ファイアウォールにより Node. vt Runtime	js
Node.js. □ ド ☑ /( (3	avaScript Runtime にこれ メイン ネットワーク (社内ネッ ブリック ネットワーク (空港、 のようなネットワークは多くの	らのネットワーク上での通信 トワークなど)( <u>D</u> ) 喫茶店など) (非推奨)( <u>U)</u> り場合、セキュリティが低いか	を許可する: ^セキュリティが設定されていません)	
<u> דלטובד</u>	アイアウォールの経由を許可	することの危険性の詳細	アクセスを許可する( <u>A</u> )	キャンセル

終了:コンソールウィンドウを閉じます。

参考情報:起動時にコンソールウィンドウを表示させたくない場合の設定例

◆タクスケジューラに登録

以下のいずれかの方法で実行ユーザを指定してください。

・SYSTEM アカウントを指定

・「ユーザがログオンしているかどうかにかかわらず実行する」オプションを有効に ※実行環境に合わせて設定を行ってください。

🕒 タスクの作成		×
全般 トリガー 打	操作 条件 設定	
名前( <u>M</u> ):	RemoteSignature_ClientAdapter	
場所:	¥RemoteSignature	
作成者:		
..   .   .   .		
ーセキュリティ オプシ	чэй	
タスクの実行時に	:使うユーザー アカウント:	
	ユーザーまたはグループの変更( <u>U</u> )…	
○ ユーザーがログ	ブオンしているときのみ実行する( <u>R</u> )	
💿 ユーザーがログ	ブオンしているかどうかにかかわらず実行する( <u>W</u> )	
□ パスワードを	:保存しない(P) (タスクがアクセスできるのはローカル コンピューター リソースのみ)	
🗌 🗌 最上位の特権	<b>崔で実行する(1)</b>	
□ 表示しない( <u>E</u> )	構成(C): Windows Vista™, Windows Server™ 2008 、	/
	OK キャンセル	6

開始:タスクを実行

終了:タスクを終了

4.5 トークン管理(メンテナンス機能)

無効なトークンを定期的に削除します。

database	
maintenance	
execution	実行時刻(1日1回実行)
hour	時
minute	分
second	秒
retentionDate	トークン保持日数(この期間を過ぎたトークンを削除)

※初期設定では、毎日2:00 に発行から3日経過したトークンを削除する設定になっています。

# インストール手順(Linux)

- 5 リモート署名クライアントアダプタ設定(Linux)
  - 5.1 モジュール確認

RemoteSignatureClientAdapter¥linux-x64

ファイル名	説明
client-adapter-linux	実行ファイル
config.json	設定ファイル

## 5.2 モジュール配置

RemoteSignatureClientAdapter¥linux-x64 をインストールフォルダヘコピーしてください。

## 5.3 各種設定

接続先パラメータシートを参考に config.json の設定値を確認してください。

5.3.1 鍵管理サービス設定

authentication		
hpki (HPKI 認証設定)		
realm	レルム名	
auth-server-url	認可エンドポイント URL	
resource	クライアントID	
credentials (クレデンシ	· ヤル情報)	
secret	クライアントアプリ認証用シークレット情報	
fido (FIDO 認証設定)		
realm	レルム名	
auth-server-url	認可エンドポイント URL	
resource	クライアント ID	
credentials (クレデンシャル情報)		
secret	クライアントアプリ認証用シークレット情報	
jpki (マイナンバーカード認証設定)		
realm	レルム名	
auth-server-url	認可エンドポイント URL	
resource	クライアント ID	
credentials (クレデンシャル情報)		
secret	クライアントアプリ認証用シークレット情報	

server		
port	クライアントアダプタサービスのポート番号	
	動作する端末にて重ならない番号を設定すること	
enableHttps	httpsの有効=true/無効=falseを設定	
httpsOptions (https 設定情報) ※https を利用しない場合は不要		
key	秘密鍵証明書のファイルパス	
cert	公開鍵証明書のファイルパス	
passphrase	上記ファイルより証明書を取り出すためのパスフレーズ	
enableCors	クロスオリジン要求(CORS)の有効=true/無効=false	
	を設定	
corsOptions (CORS 設定情報) ※CORS を使用しない場合は不要		
origin	許可するオリジンを設定	
proxy	プロキシ URL を設定する	
	※使用しない場合は不要	
disableTlsRejectUnauthorize	証明書エラーを無視する	
d	無視する=true/無視しない=false	

## 5.3.2 サーバ設定(ポート・HTTPS)

### 5.3.3 認証選択画面設定

displayAuth	
hpki	HPKI カード用認証ボタンの表示
	表示=true / 非表示=false
fido	デバイス認証(FIDO)ボタンの表示
	表示=true / 非表示=false
jpki	マイナンバーカード用認証ボタンの表示
	表示=true / 非表示=false

## 5.4 起動・終了

以下、インストールフォルダが/var/www/client-adapterの場合

適切な権限を付与する

sudo chown -R www-data:www-data /var/www/client-adapter
sudo chmod u+x /var/www/client-adapter/client-adapter-linux

サービスの登録

/etc/systemd/system/client-adapter.service

[Unit]

Description=RemoteSignature ClientAdapter

[Service]

WorkingDirectory=/var/www/client-adapter

ExecStart=/var/www/client-adapter/client-adapter-linux

Restart=always

RestartSec=10

KillSignal=SIGINT

SyslogIdentifier=client-adapter

User=www-data

[Install]

```
WantedBy=multi-user.target
```

サービスの有効化

sudo systemctl enable client-adapter

サービスの起動

sudo systemctl start client-adapter

サービスの状態を確認

systemctl status client-adapter

#### サービスのログを確認

journalctl -u client-adapter

5.5 トークン管理(メンテナンス機能)

無効なトークンを定期的に削除します。

database	
maintenance	
execution	実行時刻(1日1回実行)
hour	時
minute	分
second	秒
retentionDate	トークン保持日数(この期間を過ぎたトークンを削除)

※初期設定では、毎日2:00 に発行から3日経過したトークンを削除する設定になっています。