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 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	2023/12/26

目次

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。

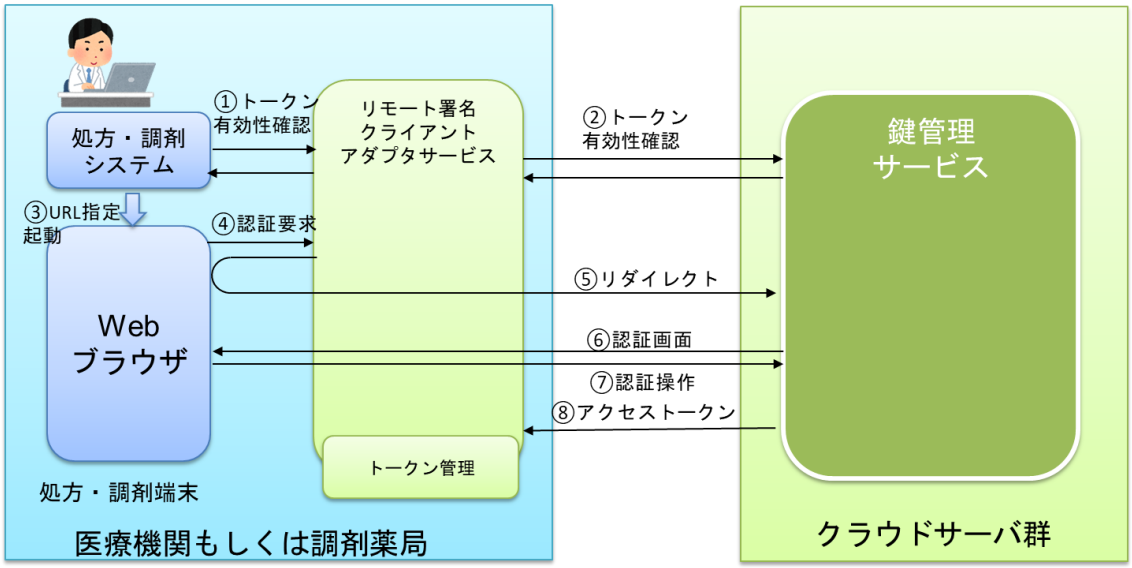
[入手]

- （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

- 端末１台から開始可能
- 端末移動時は再度認証

- クライアントアダプターサービスを配置する環境が必要
- 端末移動時も認証状態維持

- 集中管理方式
- 利用者またがるトークン横断的な管理
- シンプルな構成

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

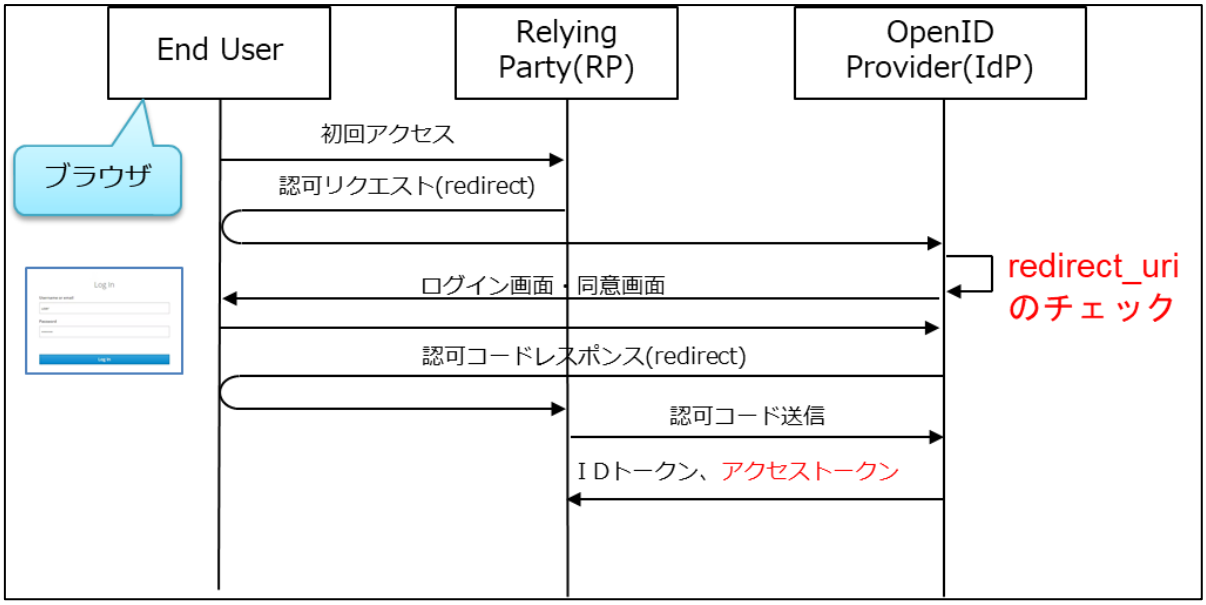
2) サーバのマシン名そのものを変更する

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へ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
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

4.3.2 サーバ設定（ポート・HTTPS）

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
disableTlsRejectUnauthorized	証明書エラーを無視する 無視する=true／無視しない=false

4.3.3 認証選択画面設定

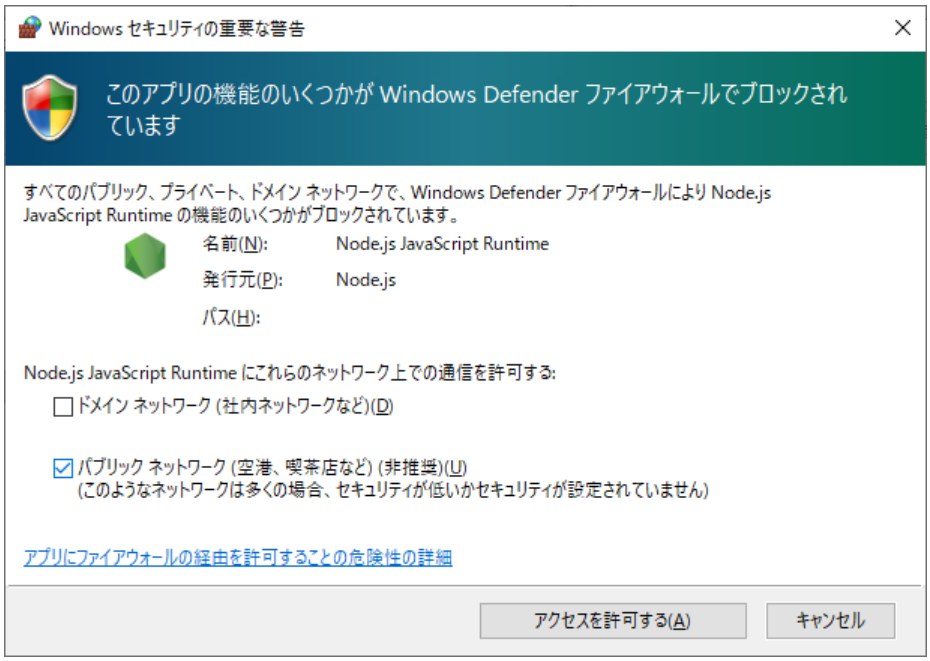
displayAuth	
hpki	HPKI カード用認証ボタンの表示 表示=true / 非表示=false
fido	デバイス認証(FIDO)ボタンの表示 表示=true / 非表示=false
jpki	マイナンバーカード用認証ボタンの表示 表示=true / 非表示=false

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。



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

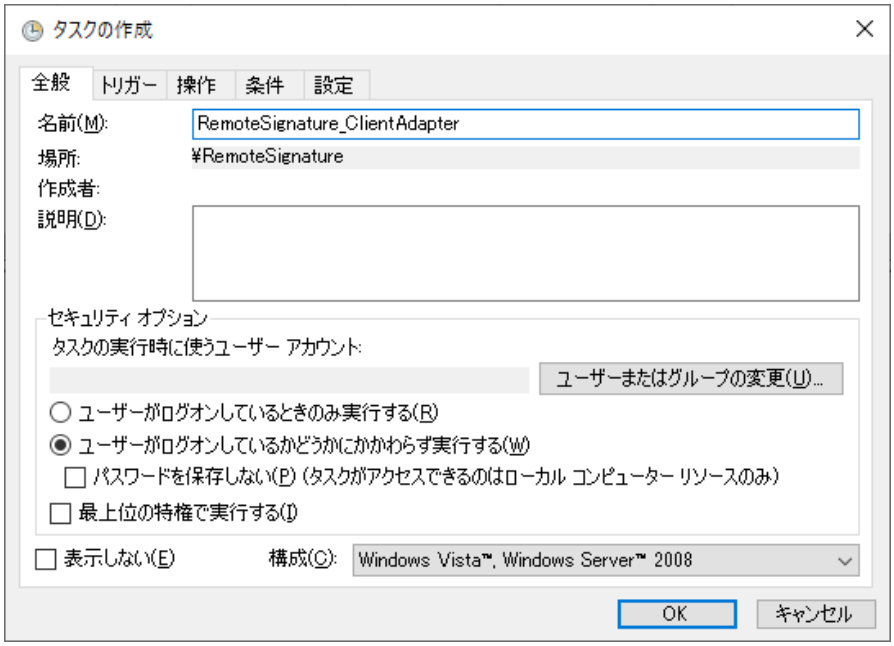
◆タクスケジューラに登録

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。



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へ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
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

5.3.2 サーバ設定（ポート・HTTPS）

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
disableTlsRejectUnauthorized	証明書エラーを無視する 無視する=true／無視しない=false

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。