

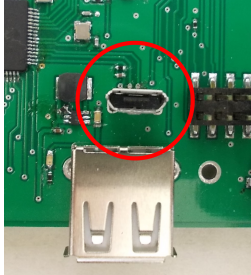
## SECTION 03\_1 : WAN設定 (Cellular)

### 特徴

- セルラーモジュール(LTEモジュール)の設定ができます。
- AWS、Azureなどのクラウドサービスと通信を行うために必要なTLS/SSL証明書を登録できます。
- アップロードするデータフォーマットを設定することができます。
- 基地局とSRPC2間の信号強度を確認することができます。信号強度を確認することで、適切な設置場所を決定できます。
- ブラウザ画面を使用すると簡単に設定できます。コマンド入力でも設定できます。

## ブラウザ画面による設定

### 1-a. パソコンと接続 (USB)

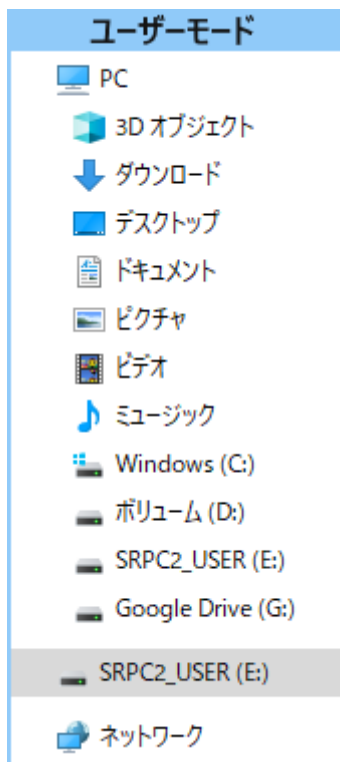


左写真のUSBコネクタ (USB Micro-B) と Windows パソコンを USB ケーブルで接続してください。下記のデバイスドライバが自動で起動します。電源は入れたままで構いません。

USB-CDC / USB-MSD / USB-RNDIS

Windows パソコン以外に接続される場合には、上記のデバイスドライバがインストールされていない場合があります。

パソコンに接続した時に、USBメモリを接続した時と同じようにフォルダ画面が表示されます。なお、お使いの環境によっては自動では表示されない場合もあります。

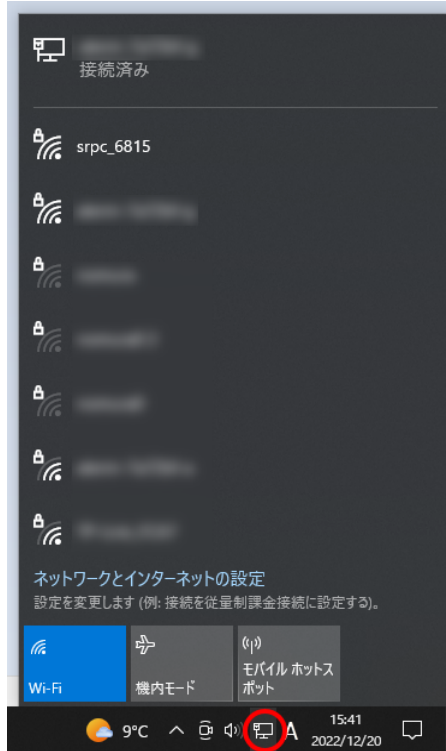


SRPC2がEドライブ (SRPC2\_USER) として認識されている場合

このフォルダ画面は、今回は使用しないので閉じてください。

## 1-b. パソコンと接続 (WiFi)

srpc2のwifiは、電源投入後60分間だけ有効になっています (設定で変更可)。電源を投入してから60分以内に作業を完了する必要があります。

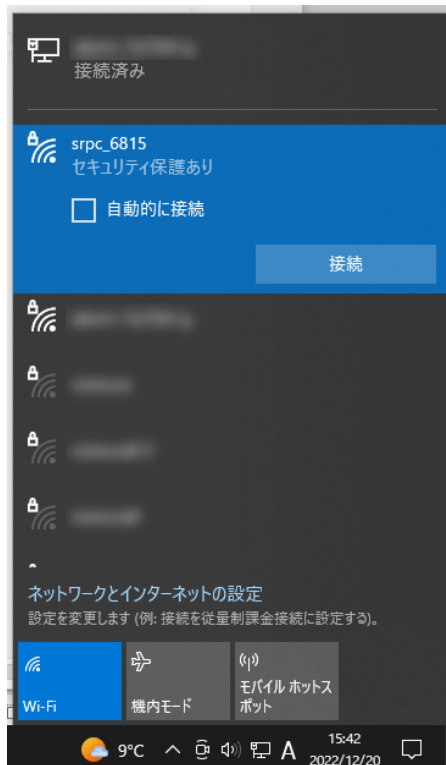


パソコン画面の右下の赤丸をクリックすると、現在の検知できているWiFiのアクセスポイントの一覧が表示されます。

その中に「**srpc\_XXXX**」というアクセスポイントがあります。XXXXは、srpc2のHW IDになります。srpc2のHW IDは、製品情報のページで確認できます。

「srpc\_XXXX」の項目をクリックすると、表示が下写真のように変化します。

なお、表示名は「NIF設定」で変更することができます。



「接続」ボタンを押すと、パスワードの入力を求められます。工場出荷時のパスワードは、「**nomuraeng**」になります。

「接続」の表示が「切断」になれば、WiFi接続が確立できたことになります。

なお、パスワードは「NIF設定」で変更することができます。

## 2. ブラウザを起動

### USB接続

<http://10.130.11.1> 左のリンクをクリックしてください。自動でブラウザ画面が表示されます。表示されない場合、お使いのパソコンにインストールされているブラウザ (Edge、Chrome等) を起動し、URLの項目に<http://10.130.11.1>と入力してください。

10.130.11.1というアドレスは、変更することができます。もし、変更している場合には文章を置き換えてください。

### WiFi接続

<http://10.130.22.1> 左のリンクをクリックしてください。自動でブラウザ画面が表示されます。表示されない場合、お使いのパソコンにインストールされているブラウザ (Edge、Chrome等) を起動し、URLの項目に<http://10.130.22.1>と入力してください。


10.130.22.1というアドレスは、変更することができます。もし、変更している場合には文章を置き換えてください。

SRPC2	
稼働状態	稼働状態
基本設定	現在の状況
アップロード	ソーラー電圧 1728 mV
スケジュール	バッテリー電圧 3280 mV
WAN設定	バッテリー充電電流 0 mA
LAN設定	バッテリー放電電流 15 mA
PAN設定	消費電流 15 mA
NIF設定	基板温度 27.00 °C
IF設定	ローバッテリー電圧 3100 mV(温度補正後)
製品情報	ローバッテリー解除 3200 mV(温度補正後)
	本日の状況
	バッテリー充電量 0 mAh
	バッテリー放電量 0 mAh
	消費電流量 0 mAh

上写真の画面が表示されることを確認してください。

### 3. WAN設定

左メニューの「WAN設定」をクリックすると、下写真の画面が表示されます。表示されない場合、製品情報で「Cellular」と「WAN」の項目がOFFになっていないか、確認してください。OFFになっている場合、お使いのSRPC2にはセルラーモジュールが搭載されていないため、「WAN設定」を行うことができません。



**SRPC2**

稼働状態	WAN設定	
基本設定	セルラー	
アップロード	常時オン	<input type="radio"/> する <input checked="" type="radio"/> しない
スケジュール	電波レベル	1
	カテゴリ	LTE-CAT-M1
	IPアドレス	100.95.144.1
WAN設定	アップロード	
LAN設定	タイプ	<input checked="" type="radio"/> なし
PAN設定		<input type="radio"/> MQTT
NIF設定		<input type="radio"/> HTTP POST (JSON)
IF設定		<input type="radio"/> HTTP POST (CSV)
拡張機能		<input type="radio"/> Azure
製品情報	<input type="button" value="更新のみ"/> <input type="button" value="保存&amp;更新"/> <input type="button" value="SIM設定"/> <input type="button" value="証明書設定"/>	

各項目の設定が完了したら、一番下の「更新のみ」か「保存&更新」ボタンを押してください。「更新のみ」ボタンで設定した場合には、電源を切ると設定した内容が破棄されます。「保存&更新」ボタンで設定した場合には、電源を切っても設定した内容は破棄されず、次の電源オン時の初期値になります。

## WAN設定

### 常時オン

セルラーモジュール(LTEモジュール) を常時オンにする場合には、「する」の項目にチェックを入れてください。常時オンにすると、消費電流が増えますが、アップロードするデータを直ぐにサーバーに送信できるようになります。

### 電波レベル

基地局とSRPC2間の信号強度を表示しています。数値が大きい方が通信が安定します。3以上が推奨値になります。

### カテゴリー

無線周波数のカテゴリーを表示しています。

### IPアドレス

基地局からSRPC2に割り振られたIPアドレスを表示しています。このIPアドレスは基地局の判断で変更される場合があります。SIMカードを固定IPで契約していると変更されません。SRPC2自体は、固定IPである必要はありません。

### タイプ

サーバーにデータをアップロードする場合、データフォーマットを設定します。選択したデータフォーマットによって、画面が変化します。

### なし

アップロードは行われません。「なし」の間のセンサデータは、破棄されます。その後、アップロードを有効にしても「なし」の間のセンサデータは存在しないため、送信されません。

## MQTT

MQTT(S)プロトコル+JSONフォーマットでサーバーにデータが送信されます。

アップロード	
タイプ	<input type="radio"/> なし <input checked="" type="radio"/> MQTT <input type="radio"/> HTTP POST (JSON) <input type="radio"/> HTTP POST (CSV) <input type="radio"/> Azure
サーバー名	<input type="text"/>
ポート番号	<input type="text" value="9000"/>
証明書の使用	<input checked="" type="radio"/> なし <input type="radio"/> あり
クライアントID	<input type="text"/>
ユーザ名	<input type="text"/>
パスワード	<input type="text"/>
トピック	<input type="text" value="srpc2"/>
受信成功確認	<input checked="" type="radio"/> する <input type="radio"/> しない
最新メッセージの保管	<input checked="" type="radio"/> する <input type="radio"/> しない
<input type="button" value="更新のみ"/> <input type="button" value="保存&amp;更新"/> <input type="button" value="SIM設定"/> <input type="button" value="証明書設定"/>	

### サーバー名

送信先サーバーのホスト名またはIPアドレスを設定します。

### ポート番号

送信先サーバーのポート番号を設定します。

### 証明書の使用

SRPC2とサーバー間をTLS/SSL通信で行う場合、「あり」を選択します。「あり」を選択すると、証明書番号の入力ができるようになります。

証明書番号とは、SRPC2内部で証明書を区別するために使用している番号になります。0を選択すると、SRPC2に搭載されている標準の証明書が使用されます。

AWS IoTのような送信元を保証したTLS/SSL通信を行う場合、後述する「証明書登録」を行い、そこで取得した証明書番号を入力する必要があります。

### クライアントID

MQTTでログインする時に使用するクライアントIDになります。

空欄の場合は、「srpc\_xxxx」(xxxxは、srpc\_id(小文字))が使用されます。AWS IoTを使用される場合には、同じクライアントIDでログインできないので重複しないIDであれば、何

でも構いません。Azure IoTを使用される場合には、Azure IoTに登録されているデバイス名になります。

### ユーザ名

MQTTでログインする時に使用するユーザ名になります。AWS IoTを使用される場合には、空欄で構いません。Azure IoTを使用される場合には、{IoT Hub名}.azure-devices.net/{デバイス名}/?api-version=2021-04-12になります。

### パスワード

MQTTでログインする時に使用するパスワードになります。AWS IoTを使用される場合には、空欄で構いません。Azure IoTを使用される場合も同様に空欄で構いません。

### トピック

トピックのルートディレクトリを設定します。ルートディレクトリが「srpc2」なら、アップロードデータは全て「srpc2」直下に置かれることになります。

### 受信成功確認

「あり」にすると、MQTTのQoSが1で送信されます。「なし」にすると、MQTTのQoSが0で送信されます。

### 最新メッセージの保管

「あり」にすると、MQTTのRetainがTrueで送信され、サーバーがRetainに対応している場合、最後に送信したメッセージが保存されます。「なし」にすると、MQTTのRetainがFalseで送信され、サーバーではメッセージの保存が行われません。

パソコンや他のデバイスが、送信先のトピックをサブスクライブする場合、最新メッセージの保管を行っていると、サブスクライブした時に最新データを受信することができます。

なお、Azure IoTは、Retainがサポートされていないため、メッセージの保管は行われません。



## HTTP POST(JSON)

HTTP(S)プロトコル+JSONフォーマットでサーバーにデータが送信されます。

アップロード

タイプ	<input type="radio"/> なし <input type="radio"/> MQTT <input checked="" type="radio"/> HTTP POST (JSON) <input type="radio"/> HTTP POST (CSV) <input type="radio"/> Azure
サーバー名	<input type="text"/>
ポート番号	<input type="text" value="9000"/>
証明書の使用	<input checked="" type="radio"/> なし <input type="radio"/> あり
Content-Type	<input type="text" value="text/plain"/>
パス	<input type="text" value="srpc2"/>
追加ヘッダ 1	<input type="text"/> : <input type="text"/>
追加ヘッダ 2	<input type="text"/> : <input type="text"/>
追加ヘッダ 3	<input type="text"/> : <input type="text"/>
追加ヘッダ 4	<input type="text"/> : <input type="text"/>
追加ヘッダ 5	<input type="text"/> : <input type="text"/>

### サーバー名

### ポート番号

### 証明書の使用

### Content-Type

HTTPプロトコルのContent-Typeを設定します。

JSONフォーマットなので、「application/json」と設定することを推奨します。

### パス

送信先のパス名になります。HTTPプロトコルの最初のメッセージに使用されます。

例) POST (パス) HTTP/1.1

### 追加ヘッダ 1～5

設定したパラメータが、HTTPプロトコルのヘッダ情報に追加されます。

## HTTP POST (CSV)

---

HTTP(S) プロトコル+CSVフォーマットでサーバーにデータが送信されます。

アップロード

タイプ	<input type="radio"/> なし <input type="radio"/> MQTT <input type="radio"/> HTTP POST (JSON) <input checked="" type="radio"/> HTTP POST (CSV) <input type="radio"/> Azure
サーバー名	<input type="text"/>
ポート番号	<input type="text" value="9000"/>
証明書の使用	<input checked="" type="radio"/> なし <input type="radio"/> あり
DQ	<input checked="" type="radio"/> あり <input type="radio"/> なし
Content-Type	<input type="text" value="text/plain"/>
パス	<input type="text" value="srpc2"/>
追加ヘッダ 1	<input type="text"/> : <input type="text"/>
追加ヘッダ 2	<input type="text"/> : <input type="text"/>
追加ヘッダ 3	<input type="text"/> : <input type="text"/>
追加ヘッダ 4	<input type="text"/> : <input type="text"/>
追加ヘッダ 5	<input type="text"/> : <input type="text"/>

### [サーバー名](#)

### [ポート番号](#)

### [証明書の使用](#)

### DQ

ダブルクォーテーションを付加するか設定します。

### [Content-Type](#)

### [パス](#)

### [追加ヘッダ 1～5](#)

---

## Azure

Azure IoTにデータを送信します。Azure IoTの各種設定は別ページで行います。ここでは、Azure IoTにデータを送信することだけを設定します。

アップロード

タイプ

- なし
- MQTT
- HTTP POST (JSON)
- HTTP POST (CSV)
- Azure

証明書を使用してAzure IoTにデータを送信する場合には、MQTTを選択して送信することも可能です。

SIM設定

## SRPC2

稼働状態

基本設定

アップロード

スケジュール

**WAN設定**

LAN設定

PAN設定

NIF設定

IF設定

拡張機能

製品情報

WAN設定 | SIM設定

---

SIM情報

ICCID

APN名

ユーザ名

パスワード

認証方式  PAP  CHAP

各項目の設定が完了したら、一番下の「更新のみ」か「保存&更新」ボタンを押してください。「更新のみ」ボタンで設定した場合には、電源を切ると設定した内容が破棄されます。「保存&更新」ボタンで設定した場合には、電源を切っても設定した内容は破棄されずに、次回の電源オン時の初期値になります。

### ICCID

SIMカードに割り振られている固有の識別番号が表示されます。

**注意！！**

SIMカードは、電源を切った状態で抜き差ししてください。回路がショートして故障の原因になります。

#### APN名／ユーザ名／パスワード／認証方式

SIMカードの情報を設定してください。認証方式は、PAPとCHAPの両方に対応している場合、SIMカードの契約情報に記載されていない場合もあります。

## 証明書設定

WAN設定とSIM設定の確認が終わった後に実行することができます。SRPC2にデバイス証明書を登録することで、サーバーはデータの送信元を保証できます。

AWS IoTやAzure IoTにデータを送信する場合、証明書登録を行う必要があります。証明書は、PEM形式(テキスト文字)に対応しています。

WAN設定の画面の右下の「証明書設定」ボタンを押すと、下記の画面が表示されます。

### SRPC2

稼働状態 | WAN設定 | 証明書登録

---

WANモジュール

状態 停止中

10分間電源オン

---

TLS/SSL 証明書

番号	<input type="text"/> (1~3)
タイプ	<input checked="" type="radio"/> ルート証明書 <input type="radio"/> デバイス証明書(クライアント証明書) <input type="radio"/> デバイス秘密鍵(クライアント秘密鍵)
データ	<input type="text" value="ファイルを選択"/> 選択されていません

(ファイルをドラッグ&ドロップできます)

登録 削除

WANモジュールの電源が入っていないと、証明書の登録が行えません。WANモジュールの状態が「停止中」になっている場合には、「10分間電源オン」ボタンを押して、WANモジュールの電源を10分間オンにしてください。

## 状態

セルラーモジュール (LTEモジュール) の動作状態を表示しています。

## 処理中

### WANモジュール

状態

処理中

現在、他の処理を行っているため、証明書の設定ができません。処理が終わるまで、しばらくお待ちください。画面の表示は自動で再読み込みされるため、画面を開いたままでも構いません。

## 停止中

### WANモジュール

状態

停止中

10分間電源オン

現在、セルラーモジュール (LTEモジュール) の電源が落ちているため、証明書の設定ができません。「10分間電源オン」ボタンを押してください。

## 起動中

### WANモジュール

状態

起動中

証明書の設定が行える状態になります。「登録」と「削除」ボタンが押せるようになります。

## 番号

操作対象の証明書番号を入力します。証明書は、「ルート証明書」「デバイス証明書」「デバイス秘密鍵」の3つがセットになっています。一つの証明書番号に、この3つのセットが関連付けられています。

## タイプ

証明書のタイプを選択します。

## データ

証明書を登録する場合に必要な作業になります。

証明書のデータを読み込みます。「ファイルを選択」ボタンを押して、対象のファイルを選択するか、対象のファイルをドラッグし、下の枠内にドロップしてください。

下の枠内にファイルの内容が表示されます。もし、文字化けしたデータが表示された場合は、PEM形式ではないので変換する必要があります。opensslを使用して変換することができます。コマンドのみ記載します、詳細についてはopensslのドキュメントを参照して下さい。

```
openssl x509 -inform der -in {変換前ファイル名} -out {変換後ファイル名}
```

## 登録／削除

状態が起動中になってから、10分以上経過するとセルラーモジュール(LTEモジュール)の電源が切れます。その場合、エラーが表示され処理に失敗します。状態が起動中になってから、10分以内に作業を終わらせてください。

「登録」ボタンを押すと証明書が登録され、「削除」ボタンを押すと証明書が削除されます。

### 注意！！

証明書は、SRPC2のCPU内には保存されません。セルラーモジュール(LTEモジュール)内に保存されます。セルラーモジュール(LTEモジュール)を交換する場合には、証明書も一緒に交換されます。データの流出や証明書設定のし忘れなどに注意が必要です。

## 処理中の画面

証明書の登録もしくは削除を実行している間は、下図のように表示されます。しばらく経過すると、成功時の画面もしくは失敗時の画面が表示されます。



更新しています。しばらくお待ちください。

成功時の画面

---

更新に成功しました。

失敗時の画面

---

更新に失敗しました。再設定をお願いいたします。

## 通信の確認方法

WAN設定またはSIM設定の「更新のみ」または「保存&更新」ボタンを押すと、セルラーモジュール(LTEモジュール)が再起動されます。再起動には、数十秒掛かる場合があります。数十秒経過した後、再びWAN設定画面を開いてください（もしくは、ブラウザの更新を実行してください）。

信号強度／カテゴリー／IPアドレスの項目に値が表示されていれば、SIMカードの設定は問題ありません。

送信先のサーバーにアップロードデータが届いているか確認してください。確認できるまでは、アップロードの間隔を短くしておいた方が早く確認できます。アップロードの間隔を変更する方法については、別紙のドキュメントを参照して下さい。



AWS IoTで「モノを作成」をクリックして、必要な情報を入力します。



デバイス証明書の設定で、「新しい証明書を自動生成 (推奨)」を選択します。

### 証明書とキーをダウンロード ×

AWS に接続できるように、証明書とインストールするキーファイルをデバイスにダウンロードします。

#### デバイス証明書

証明書は今すぐアクティブ化することも、後でアクティブ化することもできます。デバイスが AWS IoT に接続するためには、証明書がアクティブである必要があります。

デバイス証明書 証明書を非アクティブ化 📄 ダウンロード

**デバイス証明書**

#### キーファイル

キーファイルはこの証明書に固有であり、このページを離れるとダウンロードできません。今すぐダウンロードして、安全な場所に保存してください。

⚠ この証明書のキーファイルをダウンロードできるのは、この時点のみです。

パブリックキーファイル 📄 ダウンロード

プライベートキーファイル 📄 ダウンロード

**デバイス秘密鍵**

#### ルート CA 証明書

使用しているデータエンドポイントと暗号スイートのタイプに対応するルート CA 証明書ファイルをダウンロードします。ルート CA 証明書は後でダウンロードすることもできます。

Amazon 信頼サービスエンドポイント  
RSA 2048 ビットキー: Amazon ルート CA 1 📄 ダウンロード

**ルート証明書**

Amazon 信頼サービスエンドポイント  
ECC 256 ビットキー: Amazon ルート CA 3 📄 ダウンロード

ここで必要なルート CA 証明書が表示されない場合、AWS IoT では追加のルート CA 証明書がサポートされます。これらのルート CA 証明書などは、デベロッパーガイドで入手できます。 [詳細はこちら](#)

必要になるのは、赤枠でダウンロードしたファイルになります。この3つの証明書を証明書番号に登録し、WAN設定のアップロードで「証明書あり」を選択し、その証明書番号を入力すると、AWS IoTに送信することができます。

サーバー名には、AWS IoTのエンドポイントを設定します。ポート番号は、**8883**固定になります。AWS IoTのエンドポイントは、AWS IoTの設定画面で確認できます。

AWS IoT > 設定


## 設定 情報

### デバイスデータエンドポイント 情報

デバイスは、アカウントのデバイスデータエンドポイントを使用して AWS に接続できます。

各モノには、このエンドポイントで使用可能な REST API があります。MQTT クライアントと [AWS IoT デバイス SDK](#) もこのエンドポイントを使用します。

エンドポイント

 .iot.ap-northeast-1.amazonaws.com

SRPC2のWAN設定画面にAWS IoTを設定した場合の例

## アップロード

- タイプ
- なし
  - MQTT
  - HTTP POST (JSON)
  - HTTP POST (CSV)
- サーバー名
- ポート番号
- 証明書の使用  なし  あり 番号  (0~3)
- トピック
- 受信成功確認  する  しない
- 最新メッセージの保管  する  しない

更新のみ

保存&更新

証明書設定

送信に成功すると、「srpc2/{SRPCのID}/{パス名}」というトピック名でパブリッシュされます。SRPCのIDとパス名は、設定されている値になります。

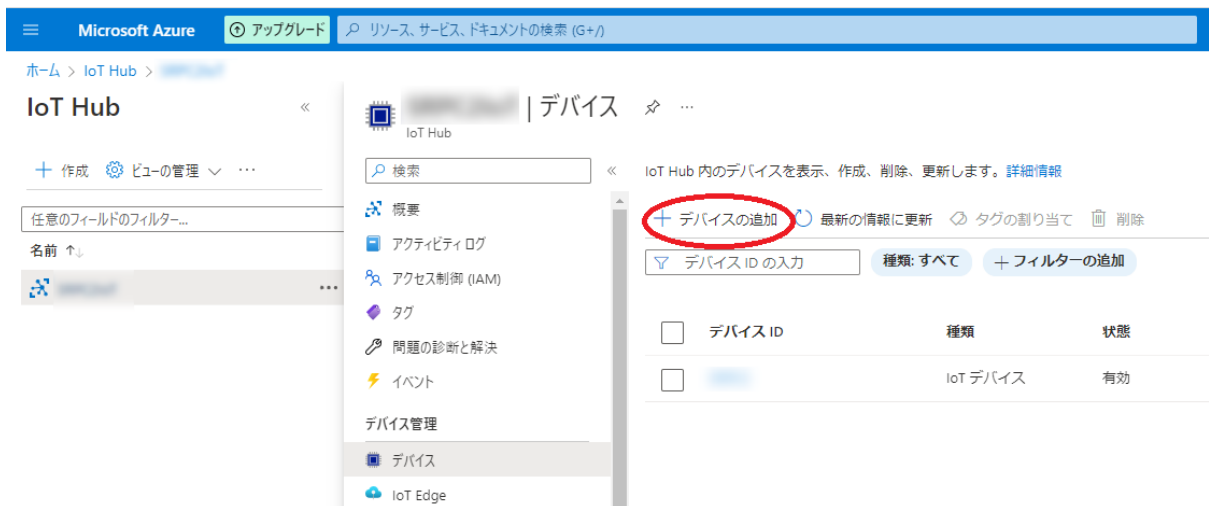
## Azure IoT

### Azure Portalでの操作

最初にIoT Hubを作成します。



次にそのIoT Hubに対してデバイスを登録します。



デバイスの登録には、「対称キー」を使用する方法と、「証明書」を使用する方法の2通りがあります。SRPC2では、どちらの方法も対応しています。

## 対称キーによる認証

Microsoft Azure リソース、サービス、ドキュメントの検索 (G+)

ホーム > | デバイス >

### デバイスの作成 ...

**i** Azure IoT 用に認定されたデバイスをデバイス カタログで検索します

デバイス ID \*

IoT Edge デバイス

認証の種類  対称キー  X.509 自己署名済み  X.509 CA 署名済み

自動生成キー

このデバイスを IoT ハブに接続する  有効化  無効化

親デバイス   
[親デバイスの設定](#)

**保存**

「認証の種類」で対称キーを選択して、デバイスを作成してください。「自動生成キー」にチェックが付いている場合、Azure IoTが自動で対称キーを生成します。

証明書による認証

Microsoft Azure アップグレード リソース、サービス、ドキュメントの検索 (G+/)

ホーム > IoT Hub > | デバイス >

### デバイスの作成

Azure IoT 用に認定されたデバイスをデバイス カタログで検索します

デバイス ID \* ⓘ  
新しいデバイスの ID

IoT Edge デバイス

認証の種類 ⓘ  
 対称キー  X.509 自己署名済み  X.509 CA 署名済み

プライマリ証明書 \* ⓘ  
ここにプライマリ証明書を入力してください

セカンダリ証明書 \* ⓘ  
ここにセカンダリ証明書を入力してください

このデバイスを IoT ハブに接続する ⓘ  
 有効化  無効化

親デバイス ⓘ

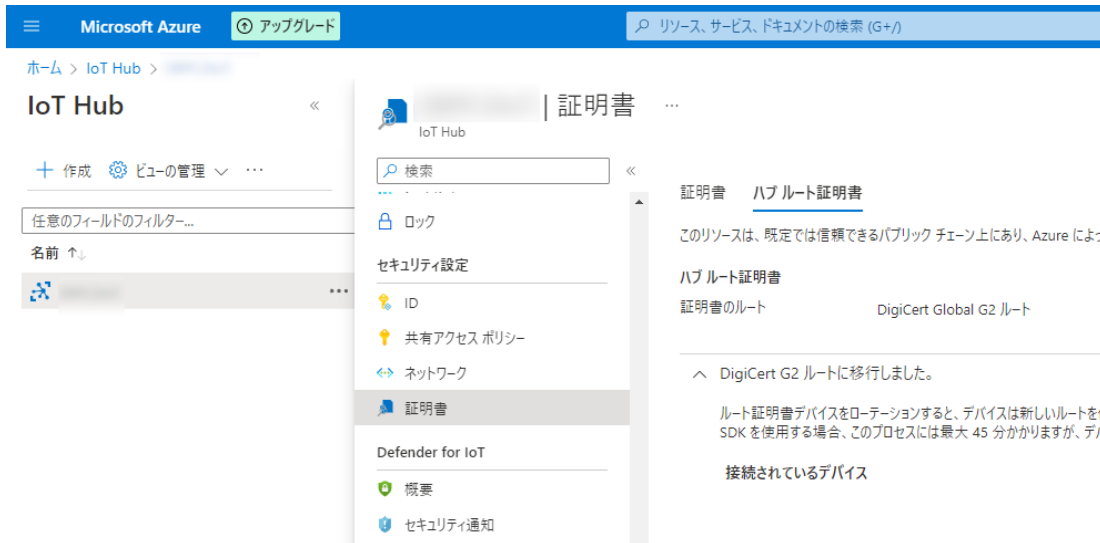
保存

SSL/TLSの証明書でログインするため、「X.509自己署名済み」か「X.509 CA署名済み」を選択します。第3機関で署名されていない証明書を使用する場合、つまり自分で作成した証明書を使用される場合には、「X.509自己署名済み」を選択します。証明書の作成については、[OpenSSL を使用して Azure IoT Hub 向けの自己署名証明書を作成する | Microsoft Learn](#)を参照して下さい。

この段階で、クライアント証明書とクライアント秘密鍵の2つのファイルが手元にあることとなります。



Azure IoTのルート証明書は、有効期限があるため複数存在しています。現在のIoT Hubでどのルート証明書が使用されているかを確認します。証明書のメニューを開きます。



上の画面の場合は、ハブ ルート証明書の項目に「DigiCert Global G2 ルート」と表示されています。有効期限が迫ると、画面上には警告文が表示されるようになります。ルート証明書は、[Azure TLS 証明書の変更 | Microsoft Learn](#)からダウンロードすることができます。証明書によっては、ダウンロードしたファイルがPEM形式ではない場合があります。ファイルをメモ帳等で開いて、-----BEGIN CERTIFICATE-----のように文字が読めるのであれば、PEM形式なのでそのままSRPC2に登録できます。もし文字化けしているなら、PEM形式に変換する必要があります。opensslを使用して変換することができます。コマンドのみ記載します、詳細についてはopensslのドキュメントを参照して下さい。

```
openssl x509 -inform der -in {変換前ファイル名} -out {変換後ファイル名}
```

以上の3つの証明書を証明書番号に登録し、WAN設定のアップロードで「証明書あり」を選択し、その証明書番号を入力すると、Azure IoTにログインすることができます。Azure IoTにデータを送信するためには、その他にサーバー名・クライアントID・ユーザ名・トピック名に決まり事があります。

Azure IoTの各種設定は、「拡張機能」の中の「Azure」の項目で行います。

SRPC2	
稼働状態	拡張機能
基本設定	メール設定
アップロード	Azure
スケジュール	
WAN設定	
LAN設定	
PAN設定	
NIF設定	
IF設定	
拡張機能	
製品情報	

基本設定

## Azure

基本設定	基本設定
DPS設定	識別情報
NE Portal	IoT Hub <input type="text"/>
	IoT デバイス <input type="text"/>
	API Version <input type="text" value="2021-04-12"/>
戻る	接続情報
	認証方法 <input checked="" type="radio"/> 対称キー <input type="radio"/> X.509証明書
	主キー <input type="text"/>
	セカンダリキー <input type="text"/>
	<input type="checkbox"/> 入れ替え
	OTA
	状態 <input type="radio"/> 有効 <input checked="" type="radio"/> 無効
	ダイレクトメソッド
	状態 <input type="radio"/> あり <input checked="" type="radio"/> なし
	要求待ち時間 <input type="text" value="1"/> 分
	<input type="button" value="更新のみ"/> <input type="button" value="保存&amp;更新"/>

各項目の設定が完了したら、一番下の「更新のみ」か「保存&更新」ボタンを押してください。「更新のみ」ボタンで設定した場合には、電源を切ると設定した内容が破棄されます。「保存&更新」ボタンで設定した場合には、電源を切っても設定した内容は破棄されずに、次回の電源オン時の初期値になります。

### IoT Hub

IoT Hub名を設定します。この設定は必須になります。

### IoT デバイス

IoT デバイス名を設定します。この設定は必須になります。

## API Version

Azure IoTのAPIバージョンを設定します。この日付は特に変更する必要はありません。  
デフォルトの「2021-04-12」のままでも問題ありません。

## 認証方式

対称キーを使用するか、証明書を使用するかを選択します。証明書を選択した場合、証明書の番号を入力する画面に切り替わります。

接続情報

認証方法  対称キー  X.509証明書

証明書番号  (0~3)

## 主キー

Azure Portalの画面から主キーを取得できます。Azure Portalで対象のデバイスを選択すると下図の画面が表示されます。

Microsoft Azure リソース、サービス、ドキュメントの検索 (G+)

ホーム > [デバイス名] | デバイス >

保存 デバイスへのメッセージ ダイレクトメソッド モジュールIDの追加 デバイス

デバイスID

主キー

セカンダリキー

プライマリ接続文字列

セカンダリ接続文字列

タグ (編集)

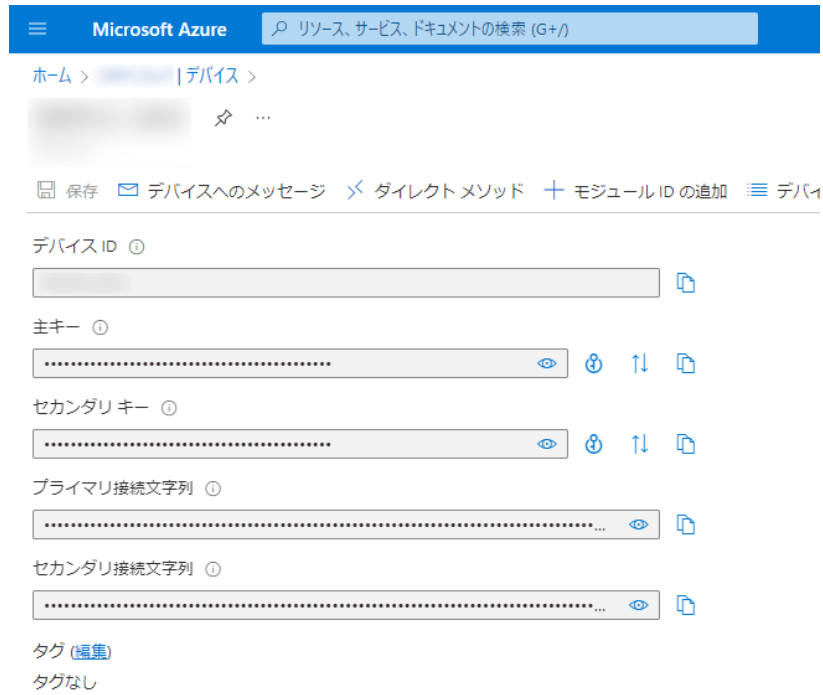
タグなし

主キーの項目の一番右にあるコピーアイコンをクリックすると、主キーの内容をコピーできます。その後、SRPC2のWEBページ上の主キーの欄に貼り付けてください。この項目は、対称キーによる認証を使用する場合、必須になります。

## セカンダリキー

---

Azure Portalの画面からセカンダリキーを取得できます。Azure Portalで対象のデバイスを選択すると、下図の画面が表示されます。



セカンダリキーの項目の一番右にあるコピーアイコンをクリックすると、セカンダリキーの内容をコピーできます。その後、SRPC2のWEBページ上のセカンダリキーの欄に貼り付けてください。この項目は、必須ではありません。

## 入れ替え

---

SRPC2に設定した主キーとセカンダリキーは、内容を確認することができません。ただし、主キーとセカンダリキーを入れ替えることは可能です。入れ替えの項目にチェックを入れ、「更新のみ」もしくは「更新&保存」ボタンを押すと、主キーとセカンダリキーを入れ替えることができます。

## OTA

---

デバイスツインを使用してSRPC2の設定を変更することができます。状態を有効にすると、追加の設定項目が表示されます。

OTA

状態  有効  無効

共有アクセスポリシー

主キー

セカンダリキー

入れ替え

デバイスツインの情報を取得する時に使用する共有アクセスポリシー名と主キーを設定してください。共有アクセスポリシーには、「レジストリ書き込み」「サービス接続」「デバイス接続」のアクセス許可が割り振られている必要があります。

### ダイレクトメソッド

Azure IoTのダイレクトメソッド機能を使用する場合には、状態の項目で「あり」を選択してください。ダイレクトメソッド機能を使用する場合、Azure IoTにデータを送信した後に、設定されている要求待ち時間の間、ダイレクトメソッドを待ちます。

### 要求待ち時間

ダイレクトメソッドを使用する場合に使用される設定になります。Azure IoTにデータを送信した後に、設定されている要求待ち時間の間、ダイレクトメソッドを待ちます。

### DPS設定

Azure DPSを使用しなくても、SRPC2からAzure IoTにデータを送信することは可能です。ただ、Azure DPSを使用するとAzure Portalを使用してデバイスを登録する必要がなくなるため、SRPC2の台数が多い場合などに利用すると作業工数を減らすことができます。

**Azure**

基本設定 DPS設定

DPS設定

NE Portal

戻る

接続情報

状態  要求する

ID Scope

API Version 2019-03-31

主キー

セカンダリキー

入れ替え

更新のみ 保存&更新

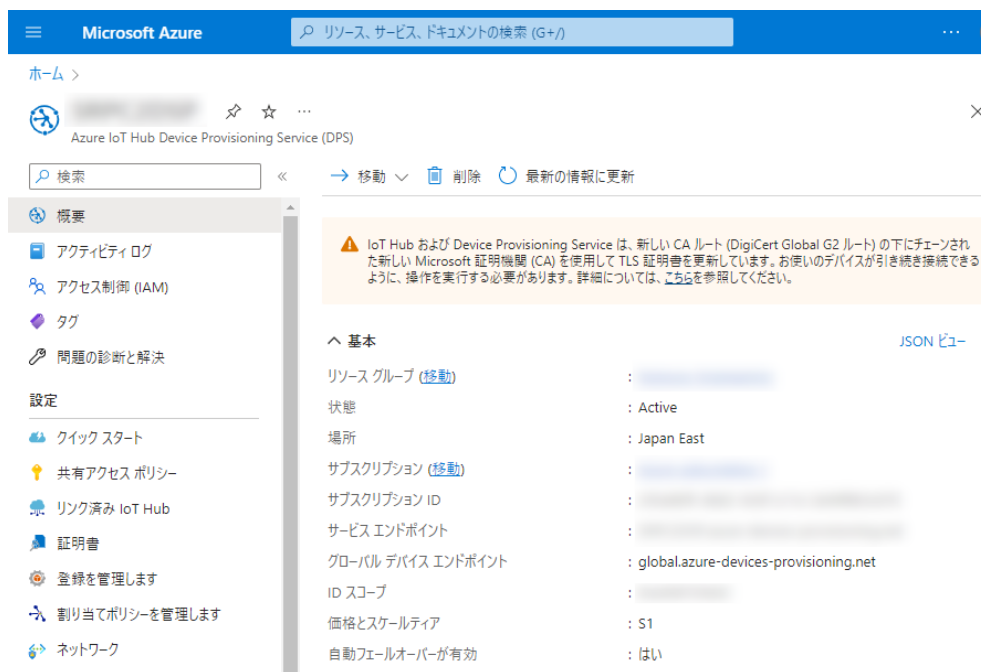
各項目の設定が完了したら、一番下の「更新のみ」か「保存&更新」ボタンを押してください。「更新のみ」ボタンで設定した場合には、電源を切ると設定した内容が破棄されます。「保存&更新」ボタンで設定した場合には、電源を切っても設定した内容は破棄されずに、次の電源オン時の初期値になります。

## 状態

「要求する」にチェックを入れると、Azure IoTにログインする時に自動でデバイスが登録されるようになります。

## ID Scope

Azure Portalに登録したDPSを選択すると、下図の画面が表示されます。



IDスコープの項目を入力してください。DPSを使用する場合、この設定は必須になります。

## API Version

Azure DPSのAPIバージョンを設定します。この日付は特に変更する必要はありません。デフォルトの「2019-03-31」のままで問題ありません。

## 主キー

「個々の登録」を使用すると、通常のデバイス登録と同じくデバイス名、主キー、セカンダリキーが生成されるため、基本設定でその内容を設定します。

「登録グループ」を使用する場合には、基本設定にはデバイス名だけを設定して、主キーとセカンダリキーは空欄にします。登録するデバイスの主キーとセカンダリキーは、DPS設定の主キーからSRPC2が自動で生成します。

よって、「登録グループ」を使用する場合には、主キーの設定は必須になります。

Microsoft Azure | リソース、サービス、ドキュメントの検索 (G+)

ホーム > | 登録を管理します | Azure IoT Hub Device Provisioning Service (DPS)

検索 << 登録グループ 個々の登録

登録グループの表示、追加、編集を行います。 [詳細情報](#)

+ 登録グループの追加 更新 削除

登録グループ ID を入力してください

<input type="checkbox"/>	グループ名 ↑	構成証明	有効...	作成...	最終...
<input type="checkbox"/>		対称キー	✓ はい	2023/4...	2023/4...



グループを選択すると、主キーとセカンダリキーを確認できます。

Microsoft Azure リソース、サービス、ドキュメントの検索 (G+)

ホーム > | 登録を管理します >

### 登録の詳細

保存

登録 ID	登録状態	詳細
作成済み	2023/4/7 13:50:41 JST	
最終更新日時	2023/4/7 13:50:41 JST	

登録とプロビジョニング IoT ハブ デバイス設定

#### 構成証明

構成証明は、登録中にデバイスの ID を確認するプロセスです。デバイスは、登録の選択した構成証明メカニズムを使用して ID を証明する必要があります。

構成証明メカニズム\*

対称キー

#### 対称キーの設定

デバイスとデバイス プロビジョニング サービスは、対称キーの構成証明を使用して、主キーとセカンダリ キーを共有します。キーは自動的に生成されるか、手動で入力できます。

主キー\*

.....

セカンダリ キー\*

.....

#### グループ名

グループ名は登録グループを一意に識別し、デバイス登録レコードを検索するために使用されます。

主キーの項目の一番右のコピーアイコンをクリックして、内容をコピーした後、SRPC2のWEBページ画面上の主キーの欄に貼り付けてください。

## セカンダリキー

セカンダリキーの設定は必須ではありません。主キーと同様にDPSのグループの画面からセカンダリキーを取得できます。

## 入れ替え

SRPC2に設定した主キーとセカンダリキーは、内容を確認することができません。ただし、主キーとセカンダリキーを入れ替えることは可能です。入れ替えの項目にチェックを入れ、「更新のみ」もしくは「更新&保存」ボタンを押すと、主キーとセカンダリキーを入れ替えることができます。

NE Portal

**Azure**

基本設定 NE Portal

DPS設定

NE Portal

戻る

接続情報

パスワード  表示

保存&更新

弊社のSRPC2サービス(<https://srpc2dev.azurewebsites.net/>)をご利用される場合には、パスワードを設定する必要があります。パスワードを入力後、「保存&更新」ボタンを押してください。なお、表示ボタンを押すと、入力しているパスワードが見えるようになります。

**SRPC2 Portal**  
Solar energy, wireless networks and sensor solutions.

**SRPC2の端末認証**

Azure IoT デバイス名

パスワード

サインイン

上画面が弊社のSRPC2サービス「SRPC2 Portal」のログイン画面になります。ここのパスワードの項目に先ほど入力したパスワードを使用してください。なお、パスワードを変更した後の次のアップロードのタイミングで、SRPC2 Portalのパスワードが更新されます。アップロードの間隔が長い場合には、更新されるまで時間が掛かることになります。

## コマンド

SRPC2は、USB接続以外からでも制御用のコマンドを入力できます。UART、RS232-C、RS485のいずれかの通信手段でSRPC2を制御することができます。

弊社で開発したカメラ付きのSRPC2も、この方法を使用してカメラの画像をサーバーに送信しています。コマンドについては別紙のドキュメントを参照してください。

AzureのBlob機能もコマンドを使用して、利用することができます。ブロックBlobとして画像ファイルをアップロードしたり、AppendBlobとしてデータを追記することができます。

変更履歴

2022/12/22	Rev1.0	新規作成
2023/01/16	Rev2.0	Azure IoT対応
2023/05/23	Rev2.1	Azure IoT、DPSを追記
2023/06/23	Rev2.2	Azure IoT(OTA)、NE Portalを追記