

SRPC-MBL for AWS IoT

# SRPC-MBL for AWS IoT



## Table of contents

初期設定	
使用方法	
工場出荷時	
フォーマット	
変更履歴	



SRPC-MBL for AWS IoT

## 初期設定

## 手順1

AWS Console (<u>https://aws.amazon.com/jp/console/</u>)を開いて、ログインしてください。この後の手順で AWS IoT に"モノ"を登録するので、ログインユーザーにはその操作が可能な権限(ポリシー)が与えられている必要があります。

"IoT Core"サービスを開いてください。見つからない場合には、サービスの検索をしてください。

aws サービス、	〃 リソースグループ → 🔸	東京 👻 サポート 👻
AWS IOT	モノ	作成 夕
モニタリング オンボード <b>管理 モノ</b> タイブ モブのグループ 請求グループ ジョブ トンネル	モノの検索     Q     フリートインデックス作成     ③	カード 🗸

"管理"→"モノ"を選択し、右上の"作成"ボタンを押してください。

aws サービス ∨ リソースグループ ∨ ★ <sup>転</sup>	▼ サポート ▼
AWS IoT モノを作成する	₽ ⊗
IoTの「モノ」とはクラウド内部の物理デバイスの表現とレコードを意味します。物理デバイス が AWS IoT と連携するには、モノのレコードが必要です。詳細はごちら。 単一の AWS IoT モノの登録 レジストリにモノを作成します	
AWS IoT モノの一括登録 すでに AWS IoT を使用している多数のデバイスのモノをレジストリに作成します。または、 参数のモノの作成 AWS IoT に接続できるようにデバイスを登録します。	
キャンセル 単一のモノを作成	<b>9</b> 8

"単一のモノを作成する"ボタンを押してください。



<sub>モノの作成</sub>	ステップ
Thing Registry にデバイスを追加	1/3
このステップは、デバイスの Thing Registry と Thing Shadow にエントリーを作成します。 名前 MONO_TEST X	

"名前"を入力して、一番下にある"次へ"ボタンを押してください。

÷	モノの作成 モノに証明書を追加	ステップ 2/3
	証明書は、AWS IoT へのデバイスの接続を認証するために使用されます。	
	1-Click 証明書作成 (推奨) AWS IoT の認証局を使用して証明書、パブリックキー、ブライベートキーを作成します。	証明書の作成
	CSR による作成 所有しているプライベートキーに基づいて固有の証明書署名リクエスト (CSR) をアップロ ードします。	<b>土</b> CSR による作成
	お持ちの証明書を使用する CA 証明書を登録し、1 つ以上のデバイスに独自の証明書を使用します。	開始方法
	証明書をスキップしてモノを作成 デバイスを AWS IoT に接続できるようにする前に、後で証明書をモノに追加する必要があり ます。	証明書なしでモノを作成

"証明書なしでモノを作成"ボタンを押して、"モノ"の登録を完了します。

捕捉)

"証明書の作成"ボタンを押すと、AWS がデバイス用(SRPC-MBL 用)の証明書を作成してくれるのですが、SRPC-MBL はその証明書のシリアル番号の桁数をサポートできないため使用できません。自前で証明書を作成する必要があります。



## 手順2

AWS のルート証明書(Amazon Root CA1)をダウンロードします。SRPC-MBL から AWS に送信するデータを暗号化するために使用されます。

しポジトリ(<u>https://www.amazontrust.com/repository/</u>)を開いて下さい。

**Root CAs** 

SHA-256 Hash of Subject Public Key Information	Self-Signed Certificate	Test URLs
fbe3018031f9586bcbf41727e417b7d1c45c2f47f93be372a17b96b50757d5a2		Valid Revoked Expired
7f4296fc5b6a4e3b35d3c369623e364ab1af381d8fa7121533c9d6c633ea2461	DER PEM	Valid Revoked Expired
36abc32656acfc645c61b71613c4bf21c787f5cabbee48348d58597803d7abc9	DER PEM	Valid Revoked Expired
	SHA-256 Hash of Subject Public Key Information           fbe3018031f9586bcbf41727e417b7d1c45c2f47f93be372a17b96b50757d5a2           7f4296fc5b6a4e3b35d3c369623e364ab1af381d8fa7121533c9d6c633ea2461           36abc32656acfc645c61b71613c4bf21c787f5cabbee48348d58597803d7abc9	SHA-256 Hash of Subject Public Key Information         Certificate           fbe3018031f9586bcbf41727e417b7d1c45c2f47f93be372a17b96b50757d5a2         DR PEM           7f4296fc5b6a4e3b35d3c369623e364ab1af381d8fa7121533c9d6c633ea2461         DER PEM           36abc32656acfc645c61b71613c4bf21c787f5cabbee48348d58597803d7abc9         DER PEM

Amazon Root CA1の PEM を右クリックして、ファイルに保存してください。

ファイル名は、"AmazonRootCA1.pem"とします。

#### 手順3

AWS CLI をインストールします。

インストール方法は、<u>https://docs.aws.amazon.com/ja\_jp/cli/latest/userguide/install-windows.html</u>を参 照してください。

インストールが完了後、Windowsの「スタートメニュー」を開いて、"cmd"を検索して実行してください。コマンドプロンプトが起動されます。

コマンドプロンプト上で、aws --version と入力し、バージョン番号が表示されればインストールは成功しています。(ハイホンは2つ)





#### 手順4

OpenSSL をインストールします。

ダウンロード画面(<u>https://slproweb.com/products/Win32OpenSSL.html</u>)を開いてください。

			Download Win32/Win64 OpenSSL	
Dow	nload Win32/Win64 OpenSSL toda	ay using the link	s below!	
	File	Туре	Description	
	Win64 OpenSSL v1.1.1d Light EXE   MSI (experimental)	3MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v1.1.1 d (Recommended for users by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.	
Wing OpenSSL v1.1.1d 43MB Installs Win64 OpenSSL v1.1.1d (Recommended for software developers by the creators of <u>OpenSSL</u> ). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL are subject to local and state laws. More information can be found in the legal agreement of the installation.				
	Win32 OpenSSL v1.1.1d Light EXE   MSI (experimental)	3MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v1.1.1 d (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.	
	Win32 OpenSSL v1.1.1d [MIS2 OpenSSL v1.1.1d [NIS2 OpenSSL v1.1.1d (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.			
	Win64 OpenSSL v1.1.0L Light	3MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v1.1.0L (Recommended for users by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.	
	Win64 OpenSSL v1.1.0L	37MB Installer	Installs Win54 OpenSSL v1.1.0L (Recommended for software developers by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is a which to the local advectories of the local advectories.	

Win64 OpenSSL の "MSI"を選択し、インストーラーをダウンロードしてください。ダウンロード後、 インストーラーを起動して、インストールを行ってください。この際、インストール先を覚えておいてく ださい、後で使用します。

Windows の「スタートメニュー」を開いて、"環境変数"と検索し、実行してください。システムのプロパティ画面が表示されます。

システムのプロパティ	×
コンピューター名 ハードウェア 詳細設定 システムの保護 リモート	
Administrator としてログオンしない場合は、これらのほとんどは変更できません。 パフォーマンス 視覚効果、ブロセッサのスケジュール、メモリ使用、および仮想メモリ	
設定(S)	
ユーザー プロファイル サインインに間連したデスクトップ設定	
設定(E)	
起動と回復 システム起動、システム障害、およびデバッグ情報	
設定(T)	
環境変数(N)	)
OK キャンセル 適用(A)	)

"環境変数"ボタンを押してください。



のユーサー環境変数(U) 変数	値		
Path			
		<u> 新</u> 田(A1) (百年)	
		新規(N)	E) 削除(D)
ステム環境変数(S)		新規(N)	E) 削除(D)
ステム環境変数(S) 変数	値	新規(N) [ 編集(	E) 削除(D)
ステム環境変数(S) 変数	值	新境(N) 攝業(	E))削除(D)
ステム環境変数(S) 変数	値	新魂(N) [ 編集(	E))削除(D)
ステム環境変数(S) 変数	位	新娊(N) [ [ [ [ [ [ [ [ [ [ [ [ [ [ [ [ [ [	E))利除(D)
ステム環境変数(S) 変数	位	新規(N) [ 攝集(	E)) 削除(D)

"Path"を選択し、"編集"ボタンを押して下さい。

環境変数名の編集	×
	新規(N)
the second states of the second states	編集(E)
the same factor with	参照(B)
D:¥Program Files¥OpenSSL-Win64¥bin	削除(D)
	上へ(U)
	下へ(0)
	テキストの編集(T)
OK	キャンセル

先ほどのインストール先を追加して "OK" ボタンを押してください。最後の"bin"まで指定してください。



SRPC-MBL for AWS IoT

環境変数の設定が完了したら、Windowsの「スタートメニュー」を開いて、"cmd"を検索して実行して ください。コマンドプロンプトが起動されます。

コマンドプロンプト上で、openssl version と入力し、バージョン番号が表示されれば正しく設定されています。





#### 手順4

AWS CLI で使用する AWS アカウントを登録します。AWS のルートアカウントは使用されないことを 推奨します。

AWS Console (<u>https://aws.amazon.com/jp/console/</u>)を開いて、ログインしてください。この後の手順でユーザーとポリシーを登録するので、ログインユーザーにはその操作が可能な権限(ポリシー)が与えられている必要があります。

"IAM"サービスを開いてください。見つからない場合には、サービスの検索をしてください。

aws サービス v リ	リソースグノ	<b>レ</b> −プ ~ <b>ኊ</b>		グローバ	レマ サポー
Identity and Access Management (IAM)	ポリ	シーの作成 ポリシーアクション ▼			2
ダッシュボード	ポリシ	シーのフィルタ v Q 検索			
		ポリシー名 🗸	タイプ	次として使用	説明
グループ	0	AccessAnalyzerServiceRole	AWS による管理	なし	Allow Acce
ユーザー		AdministratorAccess	ジョブ機能	なし	Provides f
ロール		AlexaForBusinessDeviceSe	AWS による管理	なし	Provide de
ポリシー		AlexaForBusinessFullAccess	AWS による管理	なし	Grants full
ID プロバイダー		AlexaForBusinessGateway	AWS による管理	なし	Provide ga
アカウント設定		AlexaForBusinessNetworkP	AWS による管理	なし	This policy
		AlexaForBusinessPolyDele	AWS による管理	なし	Provide ad
Access analyzer		AlexaForBusinessReadOnly	AWS による管理	なし	Provide re
Anchive rules		AmazonAPIGatewayAdmini	AWS による管理	なし	Provides f
		AmazonAPIGatewayInvoke	AWS による管理	なし	Provides f
認証情報レホート Organization activity	<	*			

"ポリシー"を選択し、"ポリシーの作成"ボタンを押してください。



术	リシーの作成		1 2
ポリシ 使用し	シーにより、ユーザー、グループ ノてポリシーを作成または編集で	、またはロールに割り当てることができる AWS アクセス権限が定義され きます。 詳細はこちら	はす。ビジュアルエディタで JSON を
E	ジュアルエディタ JSON		管理ポリシーのインポート
すべ	て展開 すべて折りたたむ		
-	IoT (1 つのアクション)		クローン 削除
	▶ サービス	IoT	
	▼ アクション	許可されるアクションを IoT で指定 💿	アクセス権限の拒否に切り替え 🚯
	閉じる	Q GetRegi	
		GetRegistrationCode 💿	
	リソース	選択したアクションはすべてのリソースをサポートします。	

"サービス"の項目には、"IoT"を選んでください。

"アクション"の検索を利用して、"GetRegistrationCode"を表示させ、✓を入れてください。

👻 IoT (1 つのアクション) 🛕 1 つの	D警告	クローン 削除
▶ サービス	IoT	
<i>▼ アク</i> ション 閉じる	許可されるアクションを IoT で指定 ⑦ Q UpdateC ✓ UpdateCACertificate ⑦ ✓ UpdateCertificate ⑦	アクセス権限の拒否に切り替え 🔒
▶ リソース	Specify <b>cacert</b> resource ARN for the <b>UpdateCACertificate</b> アクション. Specify <b>cert</b> resource ARN for the <b>UpdateCertificate</b> アクション.	
▶ リクエスト条件	リクエスト条件の指定 (オプション)	

再び、"アクション"の検索を利用して、"UpdateCACertificate"と"UpdateCertificate"を表示させ、✓を入れてください。



SRPC-MBL for AWS IoT

▼ IoT (1 つのアクション)		クローン 削除
▶ サービス	IoT	
▶ アクション	読み込み	
	GetRegistrationCode	
	書き込み	
	UpdateCACertificate	
	opuacocrimicaio	
<b>▼ リソース</b> 閉じる	<ul><li>○ 指定</li><li>● すべてのリソース</li></ul>	
▶ リクエスト条件	リクエスト条件の指定 (オプション)	
	0 toc	アクセス許可を追加する
	キャンセ	ルポリシーの確認

"リソース"で"すべてのリソース"に✔を入れて、"ポリシーの確認"ボタンを押してください。

ポリシーの作	眎龙			1 2
ポリシーの確認				
名前*	CLI_USER_POLICY	×		
	英数字と「+=,.@」を使	用します. 最大 128 文字。		
説明				
	最大 1000 文字。英数字と	「+=,.@」を使用します。		
概要	Q 77119-			
	サービス 🗸	アクセスレベル	リソース	リクエスト条件
	許可 (214 サービス中	1) 残りの 213 を表示		
	IoT	制限:読み込み,書き込み	すべてのリソース	なし
				>
* 必須			キャンセル	戻るポリシーの作成

"名前"の項目を入力して、"ポリシーの作成"ボタンを押して登録を完了させてください。



	ソースグループ 🗸 🛧
Identity and Access Management (IAM)	ユーザーを追加ユーザーの削除
Identity and Access Management (IAM) ダッシュボード ・ Access management グループ ロール ポリシー ID プロバイダー アカウント設定 ・ Access reports Access analyzer Archive rules Analyzer details 認証情報レポート Organization activity Service control policies (SCPs)	ユーザーを追加 ユーザー名またはアクセスキーでユーザーを検 ユーザー名 ▼
Q IAM の検索	

"ユーザー"を選択し、"ユーザーを追加"ボタンを押してください。

ユーザーを追加	1 2 3 4 5
ユーザー詳細の設定	
同じアクセスの種類とアクセス権限を使	<b>使用して複数のユーザーを一度に追加できます。 詳細はこちら</b>
ユーザー名*	CLI_USER
	● 別のユーザーの追加
AWS アクセスの種類を選択	
これらのユーザーから AWS にアクセス	てする方法を選択します。アクセスキーと自動生成バスワードは前のステップで提供されています。 詳細はごちら
アクセスの種類*	<ul> <li>プログラムによるアクセス</li> <li>AWS API、CLI、SDK などの開発ツールの アクセスキー ID とシークレットアクセス</li> <li>キー を有効にします。</li> </ul>
	AWS マネジメントコンソールへのアクセス ユーザーに AWS マネジメントコンソールへのサインインを許可するための パスワー ド を有効にします。
* 必須	キャンセル 次のステップ:アクセス権限

"ユーザー名"を入力し、"アクセスの種類"の "プログラムによるアクセス" に✔を入れてください。 "次のステップ"ボタンを押してください。



ユーザーを追加	1 2 3 4 5
▼ アクセス許可の設定	
2-ザーをグルーブに追 加 アクセス権限を既存のユ ーザーからコピー	展存のポリシーを直接ア タッチ
ポリシーの作成	3
ポリシーのフィルタ ~ Q CLI_USER	1 件の結果を表示中
ポリシー名 🗸	タイプ 次として使用
CLI_USER_POLICY	ユーザーによる管理 なし
	キャンセル 戻る 次のステップ:タグ

"既存のポリシーを直接アタッチ"を選択してください。

ポリシーのフィルタを利用して、先ほど登録したポリシーを表示させ、✓を入れてください。 "次のステップ"ボタンを押してください。

ユーザーを追加		1	2 3 4 5
タグの追加 (オプション)			
IAM タグは、ユーザー に追加できるキー できます。タグを使用して、この ユー	ーと値のペアです。タグには、E メールアドレスな ザー のアクセスを整理、追跡、制御できます。 詳	↓どのユーザー情報を含めるか、 細はこちら	役職などの説明文とすることが
<b>‡</b>	値 (オプション)		削除
新しいキーを追加			
さらに 50 個のタグを追加できます。			
		キャンセル	える 次のステップ:確認

"次のステップ"ボタンを押してください。



ユーザーを追加		1 2 3 4 5
確認		
選択内容を確認します。ユーザーを作用	或した後で、自動生成パスワードとアクセスキーを確認してダウ:	ンロードできます。
ユーザー <mark>詳細</mark>		
ユーザー名	CLI_USER	
AWS アクセスの種類	プログラムによるアクセス - アクセスキーを使用	
アクセス権限の境界	アクセス権限の境界が設定されていません	
アクセス権限の概要 一 次のポリシー例は、上記のユーザーに、	アタッチされます。	
タイプ 名前		
管理ポリシー CLI_USER_F	POLICY	
タグ		
追加されたタグはありません。		
		キャンセル 戻る ユーサーの作成

## "ユーザーの作成"ボタンを押してください。

	0.71		
0	成功 以下に示すコーザーを正常に作成しました。 コー	ザーのヤキュリティ認証情報を確認してダウンロード	できます、AWS マネジメントコン
	ソールへのサインイン手順を E メールでユーザー	に送信することもできます。今回が、これらの認証情	報をダウンロードできる最後の機
	会です。ただし、新しい認証情報はいつでも作成	できます。	
	AWS マネジメントコンソールへのアクセス権を招	「つユーザーは 「	でサインイン
	できます		
	v のダウンロード		
		アクセスキー ID	シークレットアクセスキー
	ユーサー		
, .	ユーサー CLI USER		
	L-U- CLI_USER		

ここに表示されている"アクセスキーID (AccessKey)"とシークレットアクセスキー(SecretKey)を 後ほど使用しますので、記録もしくは".csv のダウンロード"ボタンでダウンロードしておいてください。 AccessKey と SecretKey は、他に流出しないように注意してください。流出してしまった場合には、 先ほどの登録したユーザーを削除すれば問題ありません。



SRPC-MBL for AWS IoT

## 手順5

AWS のドキュメントに詳細な説明があります (<u>https://docs.aws.amazon.com/ja\_jp/iot/latest/developerguide/device-certs-your-own.html</u>) 一部のコマンドが違うので、注意してください。

以降のコマンドは、全てコマンドプロンプトで実行されていきます。コマンドプロンプトは、Windows の「スタートメニュー」を開き、"cmd"を検索して実行すると起動します。

#### コマンド) aws configure

手順3で入手した AccessKey と SecretKey を入力します リージョンは、" ap-northeast-1"、出力フォーマットは、"json"を選択してください。

クライアント側のルート証明書を作成します。AWS IoT は、登録されたルート証明書を使用できるの で認証局に登録する必要はありません。作成者は紛失しないよう管理してください。

#### コマンド) openssl genrsa -out rootCA.key 2048

"rootCA.key"というファイルが出力されます。このファイルは、ルート証明書の秘密鍵なので、流出することが無いように管理してください。

コマンド) openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem "rootCA.pem"というファイルが出力されます。このファイルは、ルート証明書の公開鍵なので、他に渡 しても問題ありません。AWS には、このファイルがアップロードされます。

Country Name (2 letter code) [AU]:JP State or Province Name (full name) [Some-State]:Kanagawa Locality Name (eg, city) []:Yamato-Shi Organization Name (eg, company) [Internet Widgits Pty Ltd]:Nomura Engineering Co.,Ltd Organizational Unit Name (eg, section) []:Tech Common Name (e.g. server FQDN or YOUR name) []: Email Address []:

"Country Name"には、"JP"と入力してください。それ以外は、自由に入力することができます。

製品の故障や誤動作が直接人命に関わるような使い方は絶対にしないで下さい。 野村エンジニアリング株式会社 <u>http://www.nomura-e.co.jp</u> e-mail:<u>engineer@nomura-e.co.jp</u> 〒242-0023 神奈川県大和市渋谷1丁目7-2 TEL: 046-244-0041 FAX: 046-244-3551



#### コマンド) aws iot get-registration-code

AWS IoT の登録コードが出力されます(AWS のコンソール画面でも確認できます)。

C:¥Users¥	≻aws iot g	et-registration-code	
{			
└ ″registrat	ionCode":		"
1 100101140			
1			

赤線の部分をコピーして、保管してください。後ほど使用します。

## コマンド) openssl genrsa -out verificationCert.key 2048

"verificationCert.key"というファイルが出力されます。AWS IoT にルート証明書を登録するには、先ほどの登録コードを AWS IoT に渡す必要があります。AWS IoT は、証明書の情報の一部として渡すことで実現しています。このコマンドでは、その証明書(検証証明書)用の鍵を作成しています。

## コマンド) openssl req -new -key verificationCert.key -out verificationCert.csr

"verificationCert.csr"というファイルが出力されます。

Country Name (2 letter code) [AU]:JP State or Province Name (full name) [Some-State]:Kanagawa Locality Name (eg, city) []:Yamato-Shi Organization Name (eg, company) [Internet Widgits Pty Ltd]:Nomura Engineering Co.,Ltd Organizational Unit Name (eg, section) []:Tech Common Name (e.g. server FQDN or YOUR name) []: Email Address []:

"Country Name"には、"JP"と入力し、"Common Name"には、先ほどの AWS IoT の登録コードを貼り 付けてください。それ以外は、自由に入力することができます。

## コマンド) openssl x509 -req -in verificationCert.csr -CA rootCA.pem -CAkey rootCA.key (続く) -CAcreateserial -out verificationCert.pem -days 500 -sha256

"verificationCert.pem"というファイルが出力されます。AWS IoT には、このファイルがアップロードされます。

## コマンド) aws iot register-ca-certificate --ca-certificate file://rootCA.pem (続<) --verification-cert file://verificationCert.pem

AWS IoT にクライアント側のルート証明書(rootCA.pem)と検証証明書(verificationCert.pem)をア ップロードします。成功すると、AWS IoT から証明書 ID(certificateId)が返ってきます。



#### 手順6

"IoT Core"サービスを開いてください。

aws <del>y</del> -ビス v	・ リソースグループ →   ★
	認証機関
モニタリング	CA 証明書 ID 別に CA を検索する         Q
オンボード	
管理	···
Greengrass	
安全性	
証明書	
小リシー (A	
ロールエイリアス	
オーソライザー	
防御	
ACT	
テスト	

"安全性"→ "CA"を選択してください。先ほど登録したクライアント側のルート証明書が"無効"の状態で表示されています。表示されている番号は、証明書 ID になります。



"…"を選択すると、サブメニューが表示されます。 その中の"有効化"を選択してください。

	•••
アクティブ	

"無効"から"アクティブ"に変化したことを確認してください。

製品の故障や誤動作が直接人命に関わるような使い方は絶対にしないで下さい。
 野村エンジニアリング株式会社 <u>http://www.nomura-e.co.jp</u> e-mail:<u>engineer@nomura-e.co.jp</u>
 〒242-0023 神奈川県大和市渋谷1丁目7-2 TEL: 046-244-0041 FAX: 046-244-3551



#### 手順7

"モノ"に関連付けるデバイス証明書を作成します。SRPC\_MBLの台数分、この手順を繰り返してください。

以降のコマンドは、全てコマンドプロンプトで実行されていきます。コマンドプロンプトは、Windows の「スタートメニュー」を開き、"cmd"を検索して実行すると起動します。

コマンド) openssl genrsa -out deviceCert.key 2048

"deviceCert.key"というファイルが出力されます。このファイルはデバイス証明書の秘密鍵なので、流 出することが無いようにしてください。

コマンド) openssl req -new -key deviceCert.key -out deviceCert.csr

"deviceCert.csr"というファイルが出力されます。デバイス証明書の情報を入力します。

Country Name (2 letter code) [AU]:JP State or Province Name (full name) [Some-State]:Kanagawa Locality Name (eg, city) []:Yamato-Shi Organization Name (eg, company) [Internet Widgits Pty Ltd]:Nomura Engineering Co.,Ltd Organizational Unit Name (eg, section) []:Tech Common Name (e.g. server FQDN or YOUR name) []: Email Address []:

AWS IoT の登録コードはもう使用しないので、"Common Name"に貼り付ける必要はありません。

コマンド) openssl x509 -req -in deviceCert.csr -CA rootCA.pem -CAkey rootCA.key (続<) -set\_serial 1 -out deviceCert.pem -days 500 -sha256

"deviceCert.pem"というファイルが出力されます。このファイルはデバイス証明書の公開鍵なので、他に渡しても問題ありません。AWS IoT にはこのファイルをアップロードします。

AWS IoT のドキュメントには、-CAcreateserial と記述されているのですが、SRPC-MBL ではこのオ プションで自動で作成されたシリアル番号の桁数をサポートできないので、-set\_serial X でシリアル番号 を手動で設定してください。

コマンド) aws iot register-certificate --certificate-pem file://deviceCert.pem (続<) --ca-certificate-pem <u>file://rootCA.pem</u>

AWS IoT にクライアント側のルート証明書(rootCA.pem)と一緒に、デバイス証明書(deviceCert.pem) をアップロードします。成功すると、AWS IoT から証明書 ID(certificateId)が返ってきます。



## 手順8

"IoT Core"サービスを開いてください。

aws <del>y</del> -ビス v	リソースグループ 🗸 🔖
💮 AWS ют	証明書
モニタリング	証明書の検索
オンボード	
管理	
Greengrass	mV/I
<b>安全性</b> <b>証明書</b> ポリシー CA ロールエイリアス オーソライザー 防御 ACT テスト	

"安全性"→"証明書"を選択してください。先ほど登録したデバイス証明書が"無効"の状態で表示 されています。表示されている番号は、証明書 ID になります。

無効	*** 有効化 無効化 取り消し 転送を許可する 転送を指めする 転送を開始する ポリシーのアタッチ モノをアタッチ ダウンロード 削除	"…"を選択するとサブメニューが表示されます。 "有効化"を選択してください。
アクテ	イブ	•••

"無効"から"アクティブ"に変化したことを確認してください。



アクティブ	・・・ 有効化 無効化 取り消し 新学を許可する	"…"を選択するとサブメニューが表示されま "モノをアタッチ"を選択してください。
アクティブ	無効化 取り消し	│ "…"を選択するとサブメニューが表示されま <sup>…</sup>
	取り消し	"モノをアタッチ"を選択してください。
	転送を許可する	
	FAX:COTEJ 7 W	
	転送を拒否する	
	転送を取り消す	
	転送を開始する	
7	ポリシーのアタッチ	
	モノをアタッチ	
	ダウンロード	
	削除	

登録した"モノ"を選択して、"アタッチ"ボタンを押してください。

1モノが選択されています キャンセル **アタッチ** 

以上で AWS 側の初期設定は完了になります。

1 つ以上のモノを選択 Q モノの検索 MONO\_TEST



## 手順9

SRPC-MBL に AWS のルート証明書 (AmazonRootCA1.pem)、デバイス証明書の公開鍵 (deviceCert.pem)、デバイス証明書の秘密鍵 (deviceCert.key) を登録します。

注意!! 先に SIM カードの設定を行う必要があります。

SRPC-MBL のディップスイッチ#1をON にして、メンテナンスソフトに接続してください。



登録ボタンを押すと、空欄になっていない証明書がインストールされます。全て空欄の場合、証明書の 登録の確認が行えます。

ок



AT+USECMNG=2,0,"Root CA"	6 sec.	^
T+USECMNG=0,0, "Root CA", 1208	6 sec.	
	1 sec.	-
	1 sec.	-
	1 sec.	
	1 sec.	-
	1 500	

インストール中は、上記の画面が表示されています。インストールが終了すると自動で閉じられます。

明書の設定	×		
Root CA (Server) : D:¥Work¥aws¥AmazonRootCA1.pem			
Client CA : D:¥Work¥aws¥deviceCert.pem			
Client Private Key : D:¥Work¥aws¥deviceCert.key			
	登録		
AT+USECMNG=2,0,"Ro OK AT+USECMNG=0,0,"Ro +USECMNG: 0,0,"RootC OK AT+USECMNG=2,1,"Clie OK AT+USECMNG=0,1,"ClientCA",1216> +USECMNG: 0,1,"ClientCA",'			
ок	~		
	ОК		

3種類の証明書が全て登録されていた場合、"成功しました"と表示されます。

SRPC-MBL に登録された証明書は抜き出すことができないようになっています。





<b>AWS</b> IOT	設定		
モニタリング	カスタムエンドポイント		
オンボード	AWS IoT に接続することができるカスタムエンドポイントです。モノにはそれぞれ		
管理	リます。これは、MQTI シリイアントまたは AWS IOT トナハイス SDKJ を使用す エンドボイントはプロビジョンされ、使用を開始できるようになりました。これで		
Greengrass	できます。		
安全性	エンドポイント		
防御	.iot.ap-northeast-1.amazonaws.com		
ACT			
テスト			
	ログ		
	AWS IoT を使用すれば、CloudWatch ログに役立つ情報をログ記録することができ ーカーとルールエンジンを通過すると、AWS IoT は、トラブルシューティングに行		
	ロール		
	詳細レベル		
	無効		
	編集		
ソフトウェア			
設定			

"設定"を選択すると、右画面に"エンドポイント"が表示されます。この"エンドポイント"を送信 先に設定するので、記録しておいてください。



アイコンを右クリックすると、サブメニューが表示されます。"ネットワークの設定"を選択してください。



ネットワークの設定	2
アップロードサーバー         サーバー名:       .iot.ap-northeast-1.am         ボート番号:       8883         パス名:       srpc/data         タイムアウト:       30	タイムサーバー(SNTP) ☑ 使用する サーバー名: ntp.nict.jp ポート番号: 123 VN JP UTC時差: 540 分
プロトコル 〇 HTTP (● MQTT Thing名: MONO_TEST	その他 ビ セーフティ更新を有効にする OK

"サーバー名"の欄に、先ほどの"エンドポイント"を貼り付けてください。

"ポート番号"の欄は、8883 固定になります。

"パス名"の欄は、トピック名を入力してください。

"プロトコル"の枠内の、"MQTT"を選択して、"Thing 名"を入力してください。"Thing 名"は AWS IoT サービスに登録されている必要があります。

メンテナンスソフトから切断して、SRPC-MBLのディップスイッチ#1をOFFにすると、AWS IoTへの送信が開始されます。

確認するために、"IoT Core"サービスを開いてください。

Г

AWS IOT	MQTT クライアント の	0
モニタリング オンボード	サブスクリプション トビックヘサブスクライブする	
<sup>回注</sup> Greengrass 安全性 防御	トビックへの発行	サンスクリフション デバイスは、トビックに関する MQTT メッセージを発行します。このクライアントを使用すると、トビックにサブスクライ ブしてこれらのメッセージを受信できます。 トビック Dサブスクリプション #
TRACE		メッセージキャプチャの最大数 ③ 100 サービスのPFE ⑦
		<ul> <li>ワークル・アントは、メッセージが受信されるデバイスゲートウェイに対して認識されません。</li> <li>□ 1 - このクライアントは、メッセージが受信されるデバイスゲートウェイに対して認識されます。</li> </ul>
		<ul> <li>● ISON ペイロードを自動フォーマット(読みやすさが向上)</li> <li>ペイロードを文字列として表示(より正确)</li> <li>未加工のペイロードを表示(16 進数)</li> </ul>
ソフトウェア		

"テスト"を選択した後、"トピックのサブスクリプション"の欄に"#"を入力して、"トピックのサ ブスクライブ"ボタンを押してください。



SRPC-MBL for AWS IoT

サブスクリブション	+	エクスボート クリア 一時停止
トピックヘサブスクライブする トピックへの発行 # ×	発行 QoSを0にして発行するトピックとメッセージを指定します。 # 1 { *message*: "Hello from AWS IOT console*	トビックに発行
	srpc/data 2019/12/12 15:49:45 {     "RAW": "1692002C2558582500581692000000FDF8" }	エクスポート 非表示

設定されたパス名(トピック名)でデータが送られてくることを確認してください。インターバル間隔の設定によっては、数分かかることもあるのでインターバル間隔は事前に把握しておいてください。

SRPC-MBL からは、"RAW"の項目だけが上がります。"RAW"の項目は、1 バイトを2 文字の 16 進数 で表現したデータになっています。データを抜き出すために、Lambda 関数等を使用することができます。

以上で、初期設定は完了です。



## 使用方法

メンテナンスソフトを利用する場合の使用方法について

メンテナンスソフトが使用する AWS IoT の証明書を準備します。上記の手順を例にすると、 deviceCert.key、deviceCert.pem、rootCA.pem の3つになります。

メンテナンスソフトが制御するために、上記の3つのファイルを1つのファイル(PKCS12)に纏めま す。

以降のコマンドは、全てコマンドプロンプトで実行されていきます。コマンドプロンプトは、Windows の「スタートメニュー」を開き、"cmd"を検索して実行すると起動します。

コマンド) openssl pkcs12 -export -out deviceCert.pfx -inkey deviceCert.key -in deviceCert.pem -certfile rootCA.pem

上記のコマンドを実行すると、パスワードが求められます。入力したパスワードはメンテナンスソフトの設定で使用します。

"deviceCert.pfx"というファイルが作成されます。

メンテナンスソフトを起動してください。 SRPC System メジテナンスソフト[無題] ファイル(F) 表示(V) サービス(S) 帳票(R) ツール(T) Help(H) デザイン SRPC Battery Controller Gateway Listener Wobile SRPC UbxMobile Mobile MVSI (ソターネットに接続(C)...

左ツリー内の "AWS IoT"を右クリックし、"インターネットに接続 "を選択してください。または、上のツールバー内の"AWS IoT アイコン"を押してください。

製品の故障や誤動作が直接人命に関わるような使い方は絶対にしないで下さい。 野村エンジニアリング株式会社 <u>http://www.nomura-e.co.jp</u> e-mail:<u>engineer@nomura-e.co.jp</u> 〒242-0023 神奈川県大和市渋谷1丁目7-2 TEL: 046-244-0041 FAX: 046-244-3551



AWS IoT 接続		×
証明書		
AWSルート証明書:		
クライアント証明書(pk	ccs12) :	
いえつ	- (5) :	
AWS IoT		
エンドポイント:		ポート番号:
クライアントID:	SRPC_SOFT	
トピック名:		
		接続

AWS ルート証明書

エンドポイント

クライアント ID

ポート番号

トピック名

- … アマゾンの証明書(AmazonRootCA1.pem)へのファイルパス
- クライアント証明書(pkcs12) … 作成した PKCS ファイル(deviceCert.pfx)へのファイルパス (パスワード)
  - … PKCS ファイル (deviceCert.pfx) を作成したときに入力した
  - パスワード … AWS IoT のエンドポイント
  - … AWS IoT のポート番号(8883)
  - … SRPC-MBL のモノ名以外であれば問題ありません
  - … ここで設定されたトピックに対してサブスクライブするため、 SRPC-MBL の設定で入力したパス名と同じにしてください

接続ボタンを押してください。



デザインビューに AWS IoT アイコンが表示されれば、接続は成功になります。

製品の故障や誤動作が直接人命に関わるような使い方は絶対にしないで下さい。 野村エンジニアリング株式会社 <u>http://www.nomura-e.co.jp</u> e-mail:<u>engineer@nomura-e.co.jp</u> 〒242-0023 神奈川県大和市渋谷1丁目7-2 TEL: 046-244-0041 FAX: 046-244-3551



## SRPC-MBL と SRPC を追加します



## SRPC-MBL を右クリックし、"プロパティの設定"を選択してください。

プロパティの設定 (SRPC-M	IBL-TSR)		x
ネットワーク インタ	マーバリレ プロパティ		
- アップロードサーバ サーバー名:	(-	プロトコル О нттр ()	) MQTT
ポート番号:	8883	Thing名:	SRPC_MBL_TEST
パス名:	/srpc/data	追加ヘッダー情	報
タイムアウト:	30 秒		
タイムサーバー(SN	ITP)		
☑ 使用する			· ·
サーバー名:	ntp.nict.jp	その他	
ポート番号:	123 VN JP	🗹 セーフティ更新	新を有効にする
UTC時差:	540 分		
			ОК

サーバー名 … AWS IoT のエンドポイント

ポート番号 … AWS IoT のポート番号(8883)

パス名 ··· SRPC-MBL がパブリッシュするトピック名

MQTT … 選択してください

Thing 名 ···· SRPC-MBL のモノ名

OK ボタンを押して画面を閉じてください。メンテナンスソフト上の設定情報なので、OK ボタンを押しても SRPC-MBL は更新されません。



赤い警告は、"サービス"メニューの"全てアップロード済みにする"を選択すると表示されなくなり ます。アイコンを右クリックし、"親ノードの設定"や"起点 SRPC の設定"を行い、経路を設定してく ださい。



"サービス"メニューの "開始" を実行してください。 "開始" を実行しても、SRPC-MBL や SRPC の 設定情報は変更されません。変更する場合には、アップロードを使用します。

メンテナンスソフトが起動している間に AWS IoT に送られたデータを受信して画面に表示していきま す。メンテナンスソフトが起動していない間のデータは破棄されます。破棄されないようにするには、AWS サービスを使用してください。



## 工場出荷時

弊社で初期設定を全て行ってから出荷できます。その場合には、御社で契約している AWS に初期設定 で使用するユーザーを作成して頂いて、そのユーザーの AccessKey と SecretKey を弊社に送ってくださ い。初期設定が終了したら、そのユーザーを無効にしていただいて結構です。

弊社で証明書を作成して、AWS にアップロードしたらご連絡致します。その後、御社でアップロード された証明書を有効化してください。通信テストが完了したら製品と一緒に証明書一式を全てお送りいた します。

セキュリティの関係上、弊社で行ってはいけない場合には、御社で初期設定を行ってください。弊社で はテスト用の証明書を使用して、弊社が契約している AWS IoT サービスに正常に通信できることを確認 してから出荷致します。

フォーマット

回収したデータは、"RAW"という項目で AWS IoT に上がります。 "RAW"データは、1byte を 2 文字の 16 進数で表現したデータになります。 詳しくは、別紙のデータシートを参照してください。



SRPC-MBL for AWS IoT

## 変更履歴

2019.12.11Rev0.1新規作成2020.01.30Rev0.2メンテナンスソフト部分追記