

## はじめての IoT ~AWS IoT Core ハンズオン~

アマゾン ウェブ サービス ジャパン

エバンジェリスト

亀田 治伸

### 1. IoT ダミークライアントの作成

AWS IoT Core と通信 (MQTT 及び HTTP) を行う IoT クライアントを構築しま

す。このハンズオンでは、デバイスを用いず、VPS 相当のサービスである

Amazon Lightsail に開発環境である、AWS Cloud9 及び AWS IoT SDK をインス

トールします。

#### 1-1. Amazon Lightsail の起動。

トップページにアクセスします。

リージョンはどこでも動作しますが、特にこだわりがない場合東京リージョンを選

択します。



- 1-2. 【インスタンスの作成】を押します

## インスタンスを作成する

### インスタンスロケーション



東京、ゾーン A (ap-northeast-1a) でこのインスタンスを作成しています

 AWS リージョンとアベイラビリティゾーンの変更

### インスタンスイメージの選択

#### プラットフォームの選択



Linux/Unix  
20 個の設計図



Microsoft  
Windows  
3 個の設計図

#### 設計図の選択

- 1-3. 【Linux】、【アプリ+OS】 → 【Node.js】を選択します。OS は【Amazon

Linux】を選択してください。

### プラットフォームの選択



Linux/Unix  
20 個の設計図



Microsoft  
Windows  
3 個の設計図

### 設計図の選択

アプリ + OS

OS のみ



Amazon Linux  
2018.03.0.20190826



Ubuntu  
16.04 LTS



Ubuntu  
18.04 LTS



Debian  
8.7



Debian  
9.5



FreeBSD  
12



openSUSE  
42.2



CentOS  
7 1901-01

- 1-4. インスタンス名に適切な名前を入力し、【インスタンスの作成】を押します。

## インスタンスを確認

Lightsail リソース名は一意である必要があります。

Amazon\_Linux-1

 × 

1

タグ付けオプション

Lightsail コンソールでリソースをフィルタリングして分類するには、タグを使用します。キー/値タグは、請求を分類する、およびリソースへのアクセスを制御するためにも使用できます。

[タグ付けについてさらに学ぶ](#)

### キーオンリータグ ?


+ キーオンリータグの追加

### キー値タグ ?

+ キー値タグの追加

インスタンスの作成

- 1-5. 【保留中】のステータスに変更になるまで待ちます。




**iotteest20190906**  
512 MB RAM、1 vCPU、20 GB のSSD

保留中

13.113.80.184  
東京、ゾーン A

- 1-6. 【実行中】になれば起動は完了です。



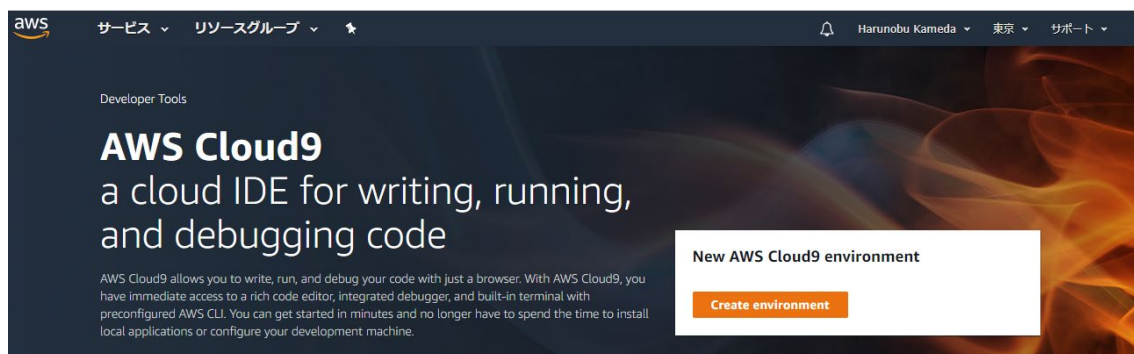
**iotteest20190906**  
512 MB RAM、1 vCPU、20 GB のSSD

実行中

13.113.80.184  
東京、ゾーン A

- 1-7. 続いて AWS Cloud 9 の画面にアクセスします。(ブラウザの別タブで開くことを

お勧めします)



1-8. 【Create Environment】を押します。

適当な名前を付けて、【Next Step】を押します。

1-9. 【Connect and run in remote server(SSH)】を選びます。Cloud9 は自前環境 (インスタンス) で起動するプランと、外部サーバにインストールするプランを選ぶことができます。自前環境でインストールする場合、VPC の設定が必須となり手順が長くなり

ますが、VPC 設定はこのハンズオンでは主目的ではないため、Lightsail にインストールします。

## Configure settings

### Environment settings

Environment type [Info](#)  
Choose between creating a new EC2 instance for your new environment or connecting directly to your server over SSH.

☐ Create a new instance for environment (EC2)  
Launch a new instance in this region to run your new environment.

☒ Connect and run in remote server (SSH)  
Display instructions to connect remotely over SSH and run your new environment.

SSH server connection [Info](#)  
AWS Cloud9 can use an SSH public key to connect securely to your server. To start, you need to add our public key to your `~/.ssh/authorized_keys` file and provide your remote login credentials below.

User

Host

Port

1-10. 先ほど構築した Lightsail の画面に戻り、起動したインスタンスの名前をクリックします。

1-11. IP アドレスとユーザー名をコピーします。

パブリック IP ⓘ  
**13.114.8.175** ▲▼  
ユーザー名 ⓘ  
**bitnami**

1-12. Cloud9 の【User】と【Host】にそれぞれコピーします。

User

13.114.8.175

Host

bitnami

Port

22

1-13. 【Copy Key to clipboard】で Cloud9 が Lightsail へのアクセスに使用する SSH の鍵をコピーします。

▼ View public SSH key

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDDjX9xsfi/VwHs0tzQCGd5jWALIgfF6b4JAbwX25s021Y6cvCyR9475HG4+UxqRAz6/+ggEapyxg40DJ9ZReS0SDTrb7Ti1o0oXhHTy82epiScnSHJcxPFa14e/7kS/yZ40vZgYSCFafe9VoIttAzrMaRPWtbn623rdQnqpthnL6hqnbI8+02UDybVZWv1fkhEnbfD1ZFjJl7INpony8dwJpf/qPCR7LX8NvQYS3iET1YbVQnID0nq/pxZyakFi7XyVPEN97PXss1o1YWl9/z6XN/H4q61hA3LLEfpGh56g9NHcxXosz86rGNBxyXfokpr1scVrNmF2mvNTCf/dGWiL39kmpuUyk4cwvdWT1gNU70TCCnxdcmj4CEmcY68F1pwRBab41LcczR+e4DQst8hBoCy3Rsk7GN8s9532sEMt5s07spNGHm/y7QFwSIwe08Hqde9dkLu+L57SVoxAe2Se13EY/mMlZlCMbUQkSs9ka4QKGaB8F2tjvuOG0tU3gEg1HOEtBhX6qj8F4z8sciyoMoYbJX0Rg3h0NyknzePn90dTMB1hgvy8q1mTA2sT3yZZ9aa0orkNORGAfhX8E7RGR8h3FDFqhPj6dIx9YMrIt+WiDwYaH0TV8J23to6hp5emEslgnFvQjKGIQkVfzFQwZvW7aYBIGOqQzKJDTBQw== root+294963776963@cloud9.amazon.com
```

Copy key to clipboard

1-14. Lightsail の画面に戻り【SSH を使用して接続】のボタンを押します。

接続 ストレージ メトリクス ネットワーキング スナップショット タグ 履歴 削除

## ブラウザを使用して安全に接続する ?

引き続き、デバイスまたはソフトウェアで独自の互換 ssh クライアントを使用してインスタンスに接続することができます。独自の SSH クライアントを使用して接続する方法について説明します

SSH を使用して接続

1-15. ターミナルを起動します

The screenshot shows a terminal window titled "iotteest20190906 - ターミナル | Lightsail - Google Chrome". The address bar shows the URL "lightsail.aws.amazon.com/ls/remote/ap-northeast-1/instances/iotteest20190906/terminal?protocol=ssh". The terminal output displays the Amazon Linux AMI logo, the text "Amazon Linux AMI", and the URL "https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/". Below this, there are three lines of the shell prompt "[ec2-user@ip-172-26-14-43 ~]\$". The terminal window has a scrollbar on the right side. At the bottom of the window, there is a status bar showing the instance name "iotteest20190906" and the IP address "13.113.80.184".

1-16. ターミナル上で「nano .ssh/authorized\_keys」と入力しエンターを押す。

この画面で、Cloud9 から Lightsail への SSH アクセスに用いる Cloud9 側の SSH 鍵を、  
Lightsail に信頼できる鍵として登録します。

```
iotteest20190906 - ターミナル | Lightsail - Google Chrome
lightsail.aws.amazon.com/ls/remote/ap-northeast-1/instances/iotteest20190906/terminal?protocol=ssh
GNU nano 2.5.3 File: .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDBm0yzIO50TncaqZJ70+J92J3GcH1s4yqVEpdx23yMPw0kyKnml$

[ Read 1 line ]
^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line

iotteest20190906
13.113.80.184
```

1-17. 右下のバインダーアイコンをクリックしてそこにさっきコピーした SSH key をペーストします。

```
iotteest20190906 - ターミナル | Lightsail - Google Chrome
lightsail.aws.amazon.com/ls/remote/ap-northeast-1/instances/iotteest20190906/terminal?protocol=ssh
GNU nano 2.5.3 File: .ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDBm0yzIO50TncaqZJ70+J92J3GcH1s4yqVEpdx23yMPw0kyKnml$

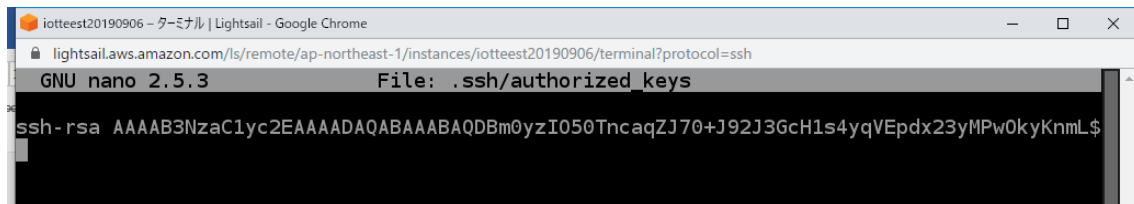
lvW7aYBIGoQzKJDTEQw== root+294963776963@cloud9.amazon.com

^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line

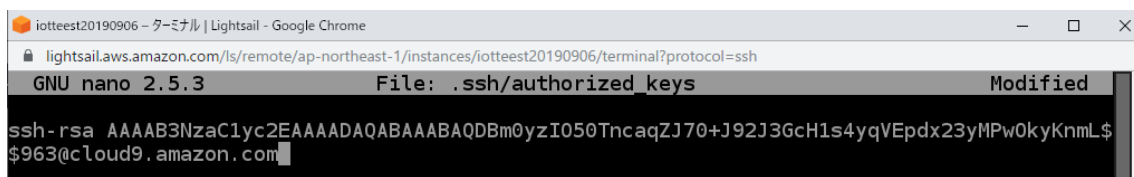
iotteest20190906
13.113.80.184
```



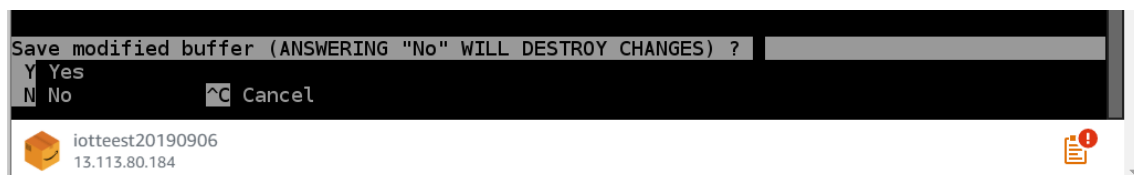
1-18. ターミナルに戻り、白いカーソルを 1 行だけ下に持っていきます。以下の画面と同じ状態に白いカーソルがなっていることを確認してください。鍵情報は人によって異なるため、細かい文字などは異なります。



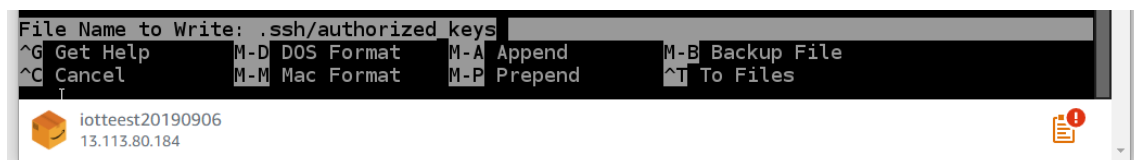
1-19. 以下のようになります。細かい文字列などが異なるのは上記同様ですが、おおよそ似たような見た目になっていることを確認してください。



1-20. 【ctr+x】を押します。



1-21. 【Y】を押します。



1-22. Return キーを押して保存します。



1-23. Cloud9 の画面に戻ります。Cloud 9 から Lightsail へのアクセス許可ができてい  
るので Cloud 9 本体のインストールを続行します。【Next】を押します。

AWS Cloud9 Installer

**Can we quickly set up AWS Cloud9 on your environment?**

AWS Cloud9 needs a few dependencies to be able to work with this SSH environment. If you agree, we'll install a few things in the ~/.c9 folder. This will not affect any other part of your system, it's fully self-contained!

**How can I revert this later?**

To fully remove AWS Cloud9 from your machine, all you need to do is remove the ~/.c9 folder! Nothing will be left over on your system.

**Can I install this manually?**

See [C9 install](#)

Next

1-24. もう一度【Next】を押します

AWS Cloud9 Installer

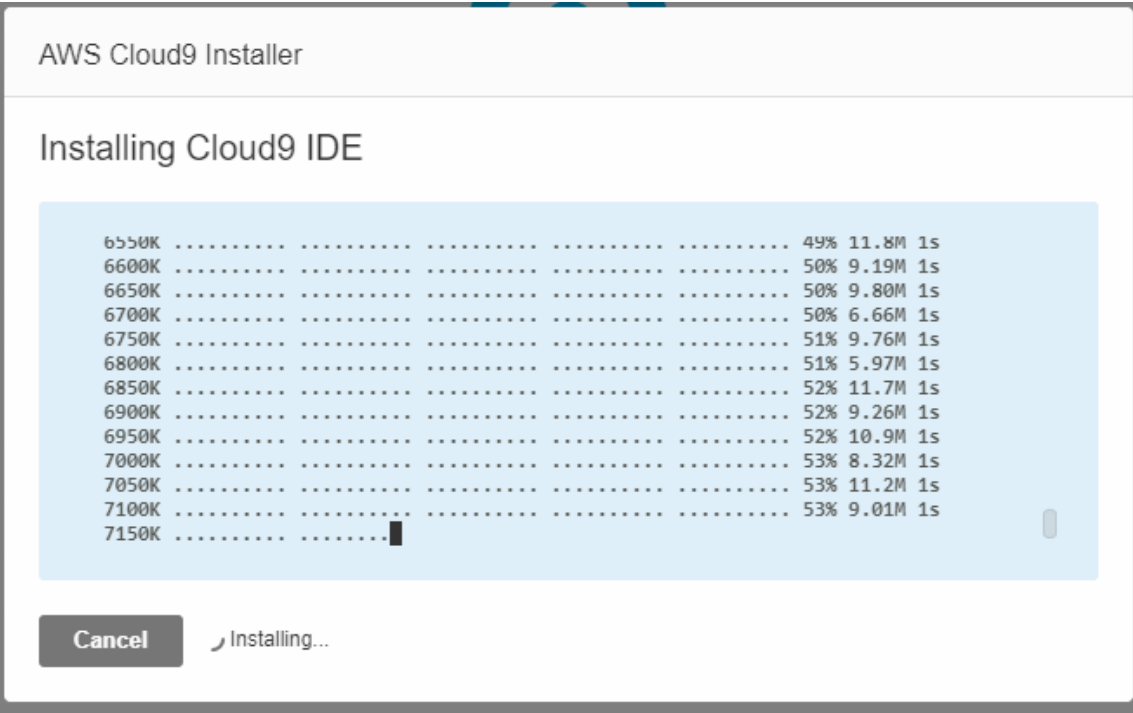
The following components will be installed. You can untick any of the optional components.

Name	Description
▶ <input checked="" type="checkbox"/> Cloud9 IDE	Version 1
▶ <input checked="" type="checkbox"/> c9.ide.find	Version 1
▶ <input checked="" type="checkbox"/> c9.ide.collab	Version 1
▶ <input checked="" type="checkbox"/> c9.ide.language.go	Version 1

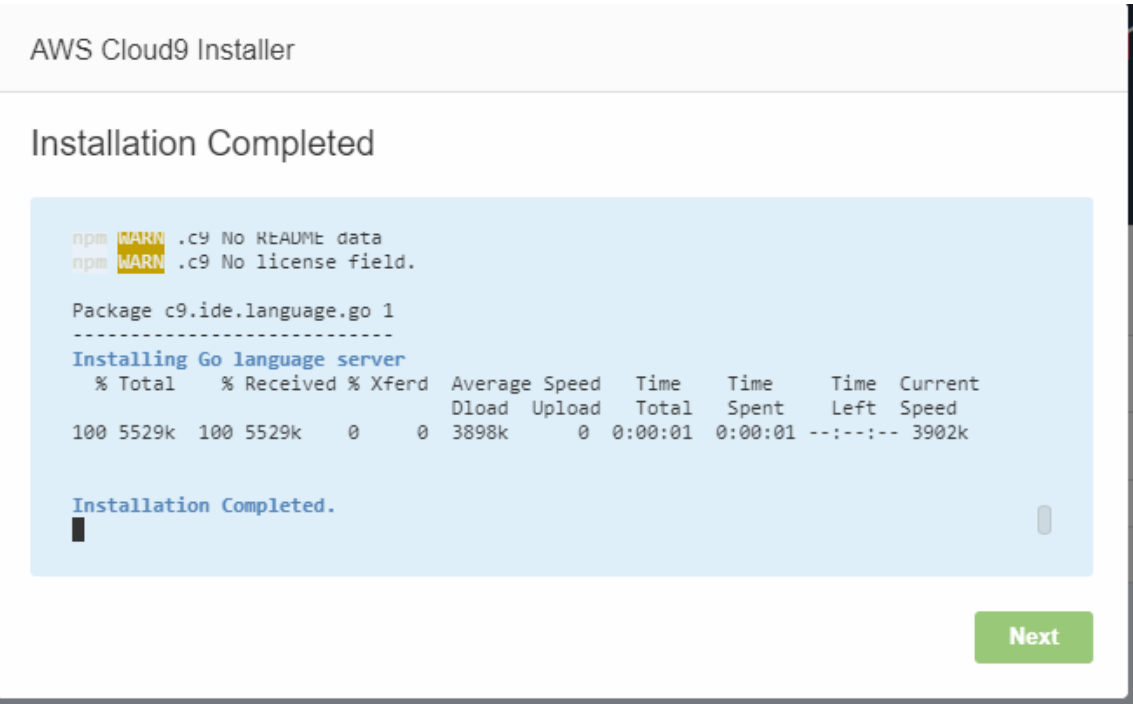
Previous

Next

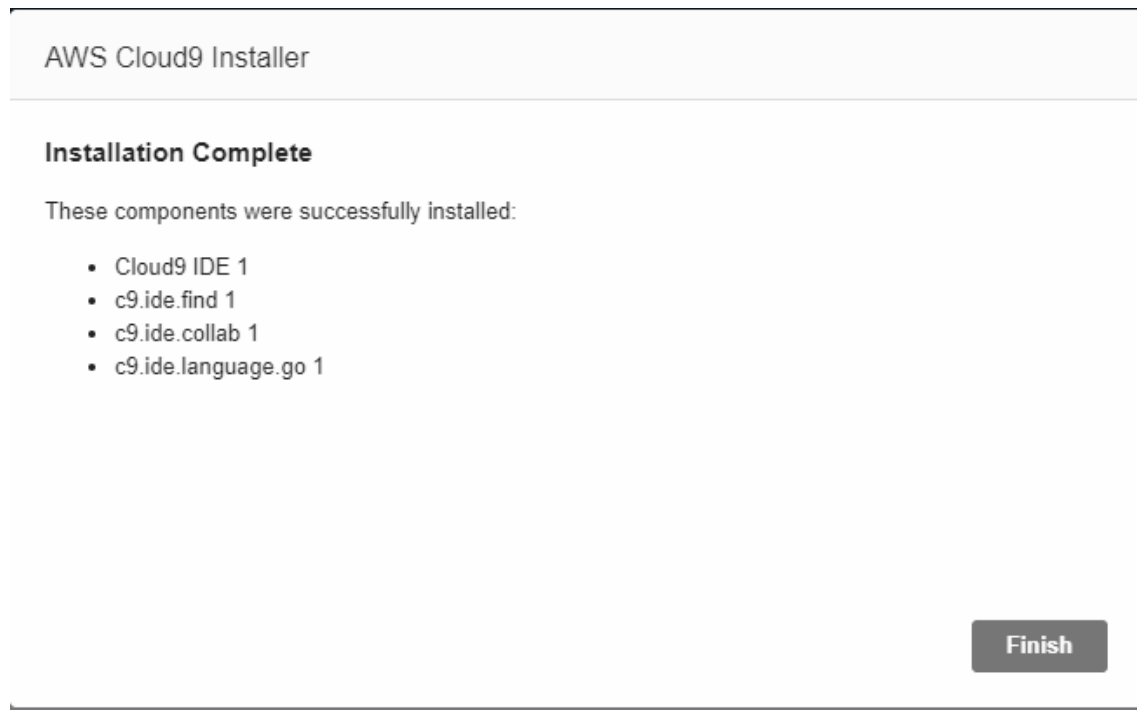
1-25. インストールが終わるのを待ちます。



1-26. 【Installation Complete】を表示されたら【Next】を押します。



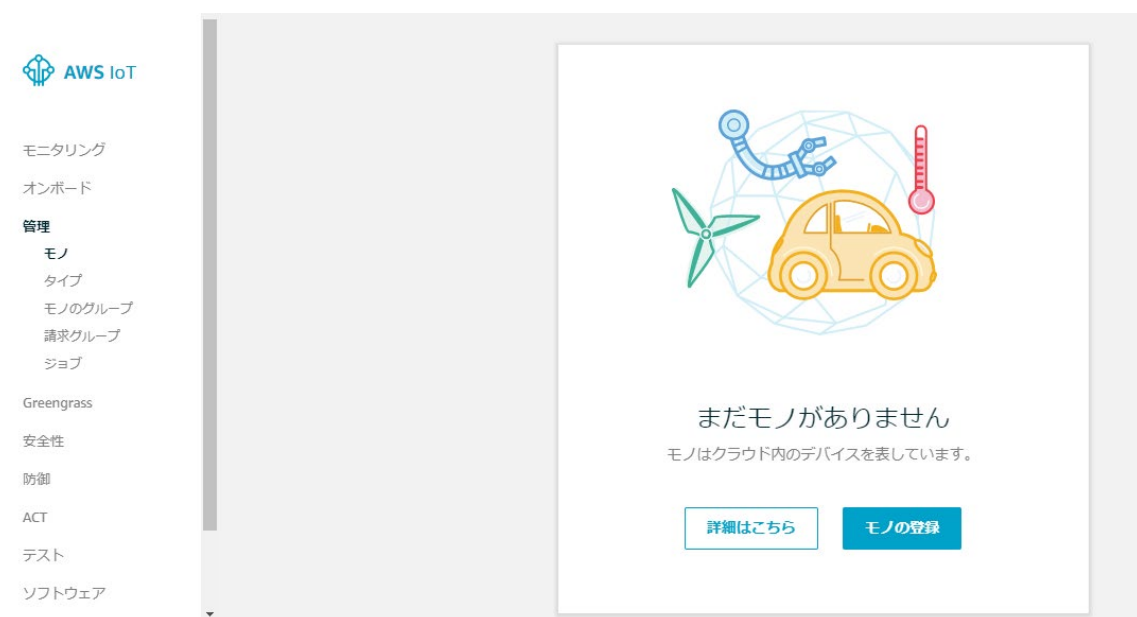
1-27. 【Finish】を押します



1-28. Cloud9 が Lightsail にインストールされました。

## 2. AWS IoT クライアントの設定

### 2-1. AWS IoT のトップ画面へアクセスします



## 2-2. 画面左下の【設定】を押します

安全性

防御

ACT

テスト

ソフトウェア

設定

学習

2-3. 【エンドポイント】をコピーしておき、テキストファイルなどにペーストしておきます。IoT クライアントが通信を行う先の URI です。はじめて利用する場合、右上のボタンを操作し、【有効】と表示されるように設定してください。

### カスタムエンドポイント 有効

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、このエンドポイントで利用できる REST API があります。これは、MQTT クライアントまたは AWS IoT [「デバイス SDK」](#) を使用する際に挿入される重要なプロパティでもあります。

エンドポ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、トピックのパブリッシュとサブスクライブを開始できます。

エンドポイント

afhmd7pja59at-ats.iot.ap-northeast-1.amazonaws.com

2-4. 【安全性】 → 【Policy】を選びます。

## 安全性

証明書

ポリシー

CA

ロールエイリアス

オーソライザー

2-5. 【ポリシーの作成】をクリックします。



ポリシーはまだ作成されていません。

AWS IoT ポリシーは、AWS IoT リソース (その他のモノ、MQTT トピック、デバイス、Thing Shadow など) へのアクセス許可をモノに付与します。

[詳細はこちら](#)

[ポリシーの作成](#)

2-6. 適当な名前を付けます。ここで作成したポリシーは、AWS IoT Core と通信を行うクライアントが持つべきセキュリティポリシー（AWS IoT Core の複数の機能と連携できる・できない等）になります。

## ポリシーの作成

ポリシーを作成して、認可アクションのセットを定義します。1 つ以上のリソース (モノ、トピック、トピックフィルター) のアクションを承認できます。IoT ポリシーの詳細については、「[AWS IoT ポリシーのドキュメントページ](#)」を参照してください。

名前

### ステートメントを追加

ポリシー構文は、リソースで実行できるアクションの種類を定義します。

アドバンスモード

アクション

カンマを使用してアクションを区切ってください (例: `iot:Publish`, `iot:Subscribe`)

リソース ARN

- 2-7. 以下の表示と同じ値を入力し、【作成】を押します。このハンズオンでは AWS IoT のすべての機能を使えるポリシーを作成します。(AWS のその他リソースを操作できる権限ではないことに注意してください) 【`iot:*`】 【`*`】

### ステートメントを追加

ポリシー構文は、リソースで実行できるアクションの種類を定義します。

アドバンスモード

アクション

`iot*`

リソース ARN

`*`

効果

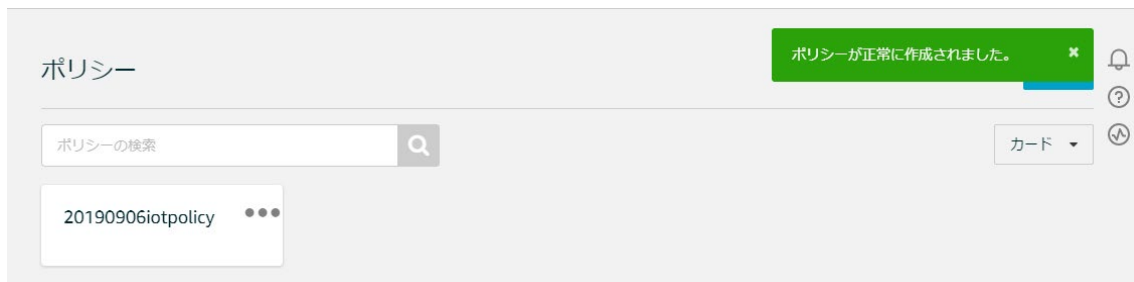
☒ 許可 ☐ 拒否

削除

ステートメントを追加

作成

- 2-8. ポリシーが作成されました。



2-9. 【管理】→【モノ】を選んでください。モノ、は AWS IoT が管理する IoT クライアント（デバイス）になります。このハンズオンではダミークライアントとして Cloud9 を使います。商用環境では大量の登録が発生するため、CLI 等プログラム化しておくことをお勧めしています。



モニタリング

オンボード

管理

モノ

タイプ

モノのグループ

請求グループ

ジョブ

2-10. 【モノの登録】を押します。





## まだモノがありません

モノはクラウド内のデバイスを表しています。

[詳細はこちら](#)

[モノの登録](#)

2-11. 【単一のモノを作成する】を選びます。

## 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。[詳細はこちら](#)。

単一の AWS IoT モノの登録  
レジストリにモノを作成します

単一のモノを作成する

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、AWS IoT に接続できるようにデバイスを登録します。

多数のモノの作成

キャンセル

単一のモノを作成する

### 2-12. 適当な名前を入力します。

モノの作成

ステップ  
1/3

Thing Registry にデバイスを追加

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

このモノにタイプを適用

モノのタイプを使用すると、タイプを共有するモノに対して一貫した登録データを提供することで、デバイス管理が簡単になります。タイプは、デバイスのアイデンティティと機能を説明する共通の属性と説明を提供します。

モノのタイプ

タイプが選択されていません

▼

タイプの作成

### 2-13. その他の設定は行わず、画面下の【次へ】を押します

検索可能なモノの属性の設定 (オプション)

レジストリ内のモノを検索できるように、これらの属性 (複数可) に値を入力してください。

属性キー

属性キー (メーカーなど) を指定します

値

属性値 (Acme-Corporation など) を指定します。

別のを追加

Thing Shadow の表示 ▼

クリア

キャンセル

戻る

次へ

## 2-14. 【証明書の作成】を押します

AWS IoT Core は通信及びデバイスのセキュリティ管理、制御に電子証明書を用いるため、認証局の機能を内蔵しています。ここで発行された認証局をクライアント (Cloud9) に組み込むことによって通信が可能となります。

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、プ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。

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

## 2-15. すべてを DL して【有効化】のボタンを押します。

デバイスを接続するには、次の情報をダウンロードします。

このモノの証明書	d8fee7d0d2.cert.pem	<a href="#">ダウンロード</a>
パブリックキー	d8fee7d0d2.public.key	<a href="#">ダウンロード</a>
プライベートキー	d8fee7d0d2.private.key	<a href="#">ダウンロード</a>

また、AWS IoT のルート CA をダウンロードする必要があります。

AWS IoT のルート CA [ダウンロード](#)

有効化

2-16. 【ポリシーのアタッチ】を押します。ポリシーは先ほど作成したデバイスが操作可能な AWS IoT の権限が設定されたものです。AWS IoT Core はデバイスの制御を証明書を使いますので、ポリシーを証明書に結び付けることになります。

デバイスを接続するには、次の情報をダウンロードします。

このモノの証明書	d8fee7d0d2.cert.pem	<a href="#">ダウンロード</a>
パブリックキー	d8fee7d0d2.public.key	<a href="#">ダウンロード</a>
プライベートキー	d8fee7d0d2.private.key	<a href="#">ダウンロード</a>

また、AWS IoT のルート CA をダウンロードする必要があります。

AWS IoT のルート CA [ダウンロード](#)

無効化

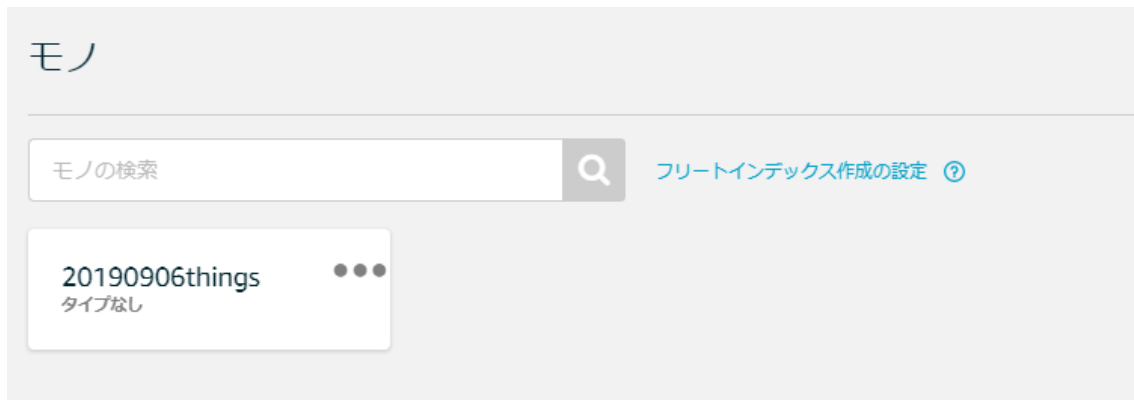
キャンセル

完了

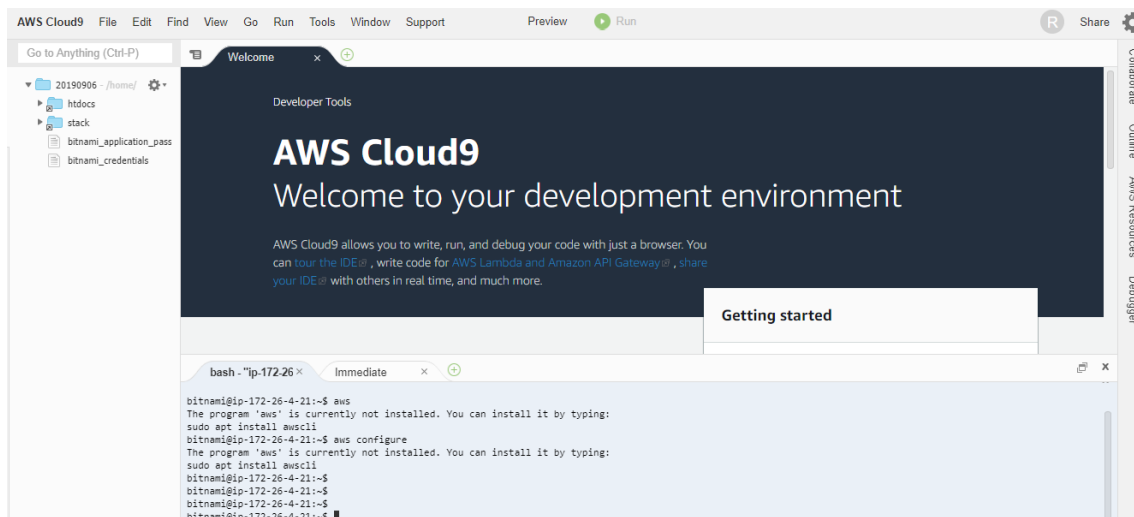
ポリシーをアタッチ

2-17. 先ほど作成したポリシーを選び【モノの登録】を押します。モノが作成されまし

た。



2-18. 作成した Cloud9 でターミナルの画面にいきます。



2-19. 以下のコマンドを実行

- `sudo apt install python3-pip`
- `sudo ln -s /usr/bin/pip-3.6 /usr/bin/pip3`

ln: failed to create symbolic link /usr/bin/pip3: File exists

が表示された場合、すでに Python3.5 がインストール済みですので、先に作業を進めてく

ださい。# IoT 用 SDK は Python3 が動作に必要です。

2-20. pip3 -V を実行し、以下の表示がされたらインストール完了です。

```
bitnami@ip-172-26-4-21:~$ pip3 -V
pip 8.1.1 from /usr/lib/python3/dist-packages (python 3.5)
bitnami@ip-172-26-4-21:~$
```

2-21. Python SDK をインストールします。以下のコマンドを実行します。

- sudo pip3 install AWSIoTPythonSDK

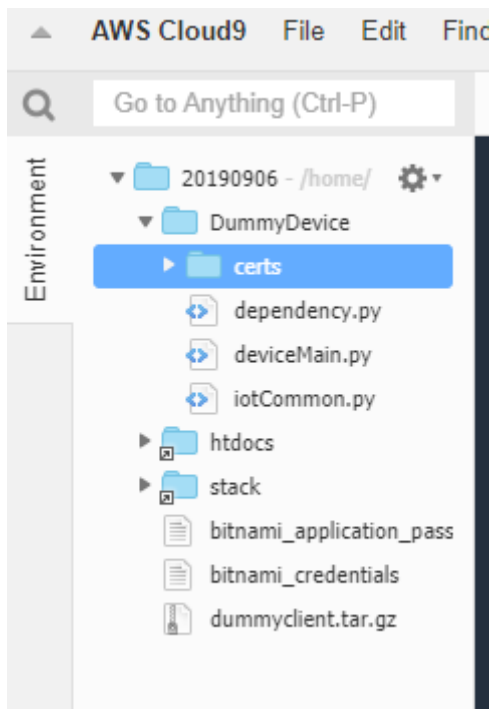
2-22. ダミークライアントのソースコードをダウンロードします。

- wget <http://bit.ly/2QggRgx> -O dummyclient.tar.gz

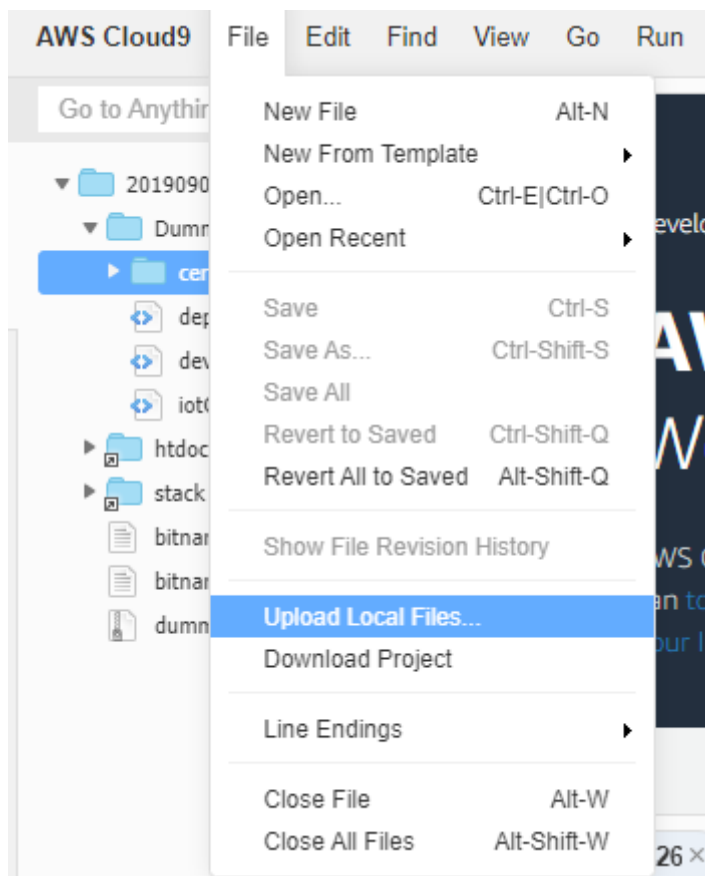
2-23. ダウンロードしたクライアントを解凍します。

- tar -zxvf dummyclient.tar.gz

2-24. 今の解凍で新しいフォルダができていますので、【DummyDevice】【certs】を選んで開きます。

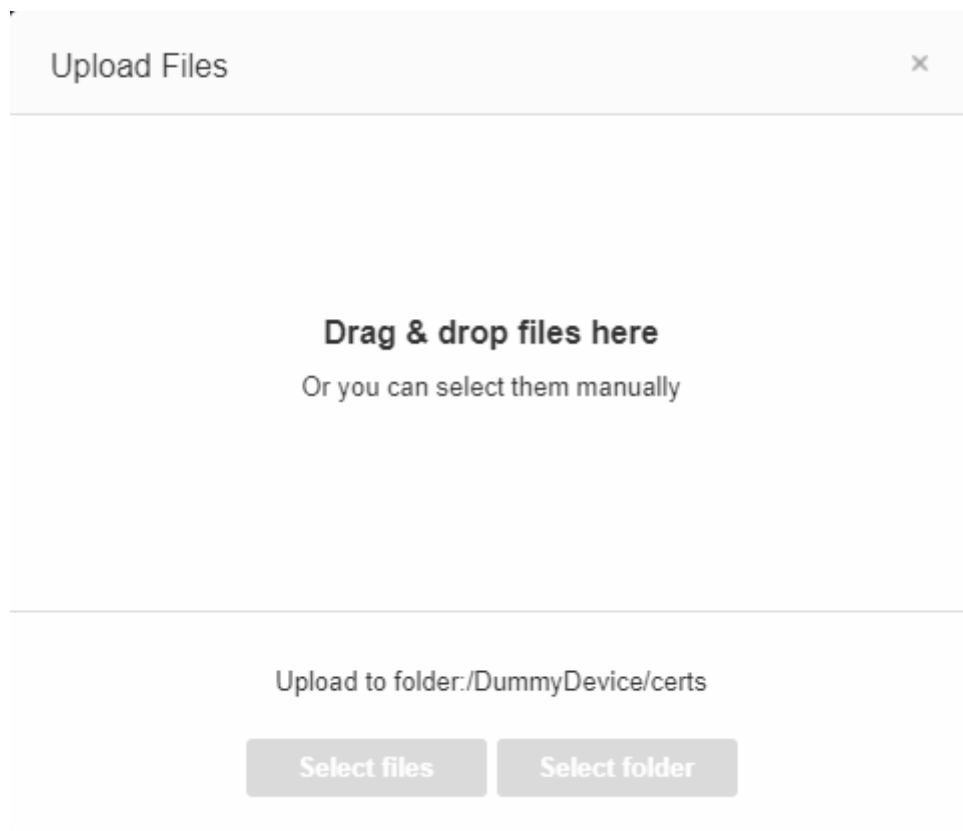


2-25. 【File】【Upload Local Files】を開きます。



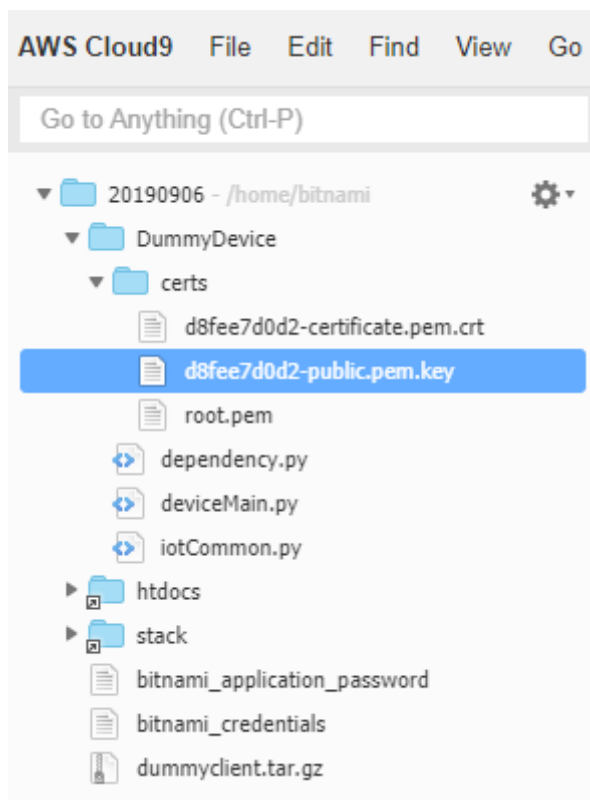
2-26. 先ほど DL した 2 つの電子証明書ファイル【\*\*-certificate.pem.crt 】【\*\*-private.pem.key】を Upload します。

注意 : Windows 環境であれば、\*.crt ファイルは証明書を表すアイコンマークとなり、拡張子が表示されず\*.pem ファイルとなっています。



2-27. ファイルがコピーされたことを確認します。





2-28. \*\*\*private.pem.key のファイル名を private.pem に変更します。Cloud9 のシェルで変更してもいいですし、エクスプローラーで rename を選んでもいいです。

2-28. ディレクトリをシェル上で移動します。移動先は【DummyDevice】です。TAB を使うことができますので、たとえば cd D だけ入力して TAB を押すと残りは自動で補完されます。

```
bash - "ip-172-26" × Immediate × (+)
bitnami@ip-172-26-4-21:~$ tar -zxvf dummyclient.tar.gz
DummyDevice/
DummyDevice/deviceMain.py
DummyDevice/dependency.py
DummyDevice/certs/
DummyDevice/certs/root.pem
DummyDevice/iotCommon.py
bitnami@ip-172-26-4-21:~$ ls
bitnami_application_password bitnami_credentials dummyclient.tar.gz DummyDevice htdocs stack
bitnami@ip-172-26-4-21:~$ cd DummyDevice/
bitnami@ip-172-26-4-21:~/DummyDevice$
```

2-29. 以下のコマンドを入力します。赤字は置き換えてください。

python3 deviceMain.py --device\_name **ご自分の作ったモノ名** --endpoint **AWS IoT の endpoint\_url**

2-30. 疎通が完了すると以下のような画面が表示されます。

```
bitnami@ip-172-26-4-21:~/DummyDevice$ python3 deviceMain.py --device_name 20190906things --endpoint afhmd7pja59at-ats.iot.ap-northeast-1.amazonaws.com
start >>>
device_name: 20190906things
endpoint: afhmd7pja59at-ats.iot.ap-northeast-1.amazonaws.com
rootca cert: ./certs/root.pem
private key: ./certs/private.pem
certificate: ./certs/d8fee7d0d2-certificate.pem.crt
connect to AWS IoT >>>
topic: data/20190906things
send back state payload:{"state": {"reported": {"wait_time": 5}}}
```

2-31. AWS IoT の管理画面でテストを選びます。



モニタリング

オンボード

管理

Greengrass

安全性

防御

ACT

テスト

2-32. 【トピックのサブスクリプション】の欄に data/{モノの名前}を入力し【サブスクライブ】ボタンを押します。{モノの名前}は皆さんが作成した名前です。

data/20190906things

エクスポート   クリア   一時停止

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。

data/20190906things

トピックに発行

```
1 {
2   "message": "Hello from AWS IoT console"
3 }
```

data/20190906things

2019/09/06 16:39:11

エクスポート   非表示

```
{
  "TIMESTAMP": "2019-09-06T07:39:11",
  "DEVICENAME": "20190906things",
  "VALUE": 25
}
```

2-33. ダミークライアントの設定が 5 秒間隔でのステータス同期となっているので、5 秒ごとにデータが 1 個ずつ増えていきます。

data/20190906things

2019/09/06 16:40:37

エクスポート   非表示

```
{
  "TIMESTAMP": "2019-09-06T07:40:37",
  "DEVICENAME": "20190906things",
  "VALUE": 22
}
```

data/20190906things

2019/09/06 16:40:32

エクスポート   非表示

```
{
  "TIMESTAMP": "2019-09-06T07:40:32",
  "DEVICENAME": "20190906things",
  "VALUE": 21
}
```

data/20190906things

2019/09/06 16:40:27

エクスポート   非表示

```
{
  "TIMESTAMP": "2019-09-06T07:40:27",
  "DEVICENAME": "20190906things",
  "VALUE": 20
}
```

### 3. デバイスシャドウによるデバイスの操作

AWS IoT にはデバイスシャドウという機能があります。クライアントデバイスが送ってきたステータスを、管理者側が書き換えることでクライアントデバイスの挙動を変更させることができます。上記でテストした 5 秒おきに送られてくるデータを 10 秒おきに送られてくるように変更します。

3-1. データ間隔が 5 秒おきになっていることを確認します。

data/20190906things	2019/09/06 16:52:58	<a href="#">エクスポート</a> <a href="#">非表示</a>
<pre>{   "TIMESTAMP": "2019-09-06T07:52:58",   "DEVICENAME": "20190906things",   "VALUE": 18 }</pre>		
data/20190906things	2019/09/06 16:52:53	<a href="#">エクスポート</a> <a href="#">非表示</a>
<pre>{   "TIMESTAMP": "2019-09-06T07:52:53",   "DEVICENAME": "20190906things",   "VALUE": 15 }</pre>		

3-2. 【管理】【モノ】を選びます。



3-3. 【シャドウ】を選択します。



3-4. データが 5 秒間隔で上がってくることが定義されています。これを 10 秒に書き

換えるため【編集】を押します。

シャドウ ARN は、この Thing Shadow を一意に識別します。詳細はこちら

```
arn:aws:iot:ap-northeast-1:294963776963:thing/20190906things
```

シャドウドキュメント

削除 編集

最終更新日: 2019/09/06 16:32:18

シャドウステータス:

```
{
  "reported": {
    "wait_time": 5
  }
}
```

こちらの値が空欄の場合、Cloud9 上の Dummy Client を一度停止して、再度起動し 5 秒待ってください。

3-5. 以下のように置換し【保存】を押します。

シャドウドキュメント

削除 キャンセル 保存

最終更新日: 2019/09/06 16:32:18

シャドウステータス:

```
1
2 {
3   "desired": {
4     "wait_time": 10
5   },
6   "reported": {
7     "wait_time": 5
8   }
9 }
10
```

3-6. Cloud9 の画面に戻ると、指示を受信した旨が表示されています。

```
-----
send back state payload:{"state": {"reported": {"wait_time": 5}}}
delta payload:{"version":4,"timestamp":1567756601,"state":{"wait_time":10},"metadata":{"wait_time":{"timestamp":1567756601}}}
{"state": {"reported": {"wait_time": 10}}}
send back state payload:{"state": {"reported": {"wait_time": 10}}}
```

3-7. AWS IoT Core のテスト画面で、同期間隔が 10 秒になっていることを確認します。

data/20190906things	2019/09/06 16:58:14	<a href="#">エクスポート</a> <a href="#">非表示</a>
<pre>{   "TIMESTAMP": "2019-09-06T07:58:14",   "DEVICENAME": "20190906things",   "VALUE": 23 }</pre>		
data/20190906things	2019/09/06 16:58:04	<a href="#">エクスポート</a> <a href="#">非表示</a>
<pre>{   "TIMESTAMP": "2019-09-06T07:58:04",   "DEVICENAME": "20190906things",   "VALUE": 19 }</pre>		

#### 4. ルールエンジン

AWS IoT Core にはルールエンジンという機能が存在しています。クライアントデバイスから上がってきたデータの中身をもとに、SQL を実行し、データの中身によりその後の AWS 上の挙動を変更させます。このハンズオンでは、データが[s3]という文字列であった場合のみ、s3 にデータを保存する手順を行います。

4-1. 【ACT】を押します。





モニタリング

オンボード

管理

Greengrass

安全性

防御

**ACT**

テスト

4-2. 【ルール作成】を押します。



ルールはまだ作成されていません。

ルールを使用すると、AWS などのウェブサービスとやり取りする権限をモノに許可できます。ルールは、モノより送信されるメッセージに基づいて、分析し、アクションを実行します。

[詳細はこちら](#)

[ルールの作成](#)

4-3. 適当な名前を入力します。

## ルールの作成

モノにより送信されるメッセージを評価し、メッセージを受信したときの処理を指定するルールを作成します (DynamoDB テーブルにデータを書き込む、Lambda 関数を呼び出すなど)。

名前

20190906s3rule

説明

4-4. 以下の SQL を入力します。

```
select name from data/ {モノの名前} where name = s3
```

ルールクエリステートメント

SELECT <Attribute> FROM <Topic Filter> WHERE <Condition>. For example: SELECT temperature FROM 'iot/topic' WHERE temperature > 50. SQL ステートメントを構築する方法については、「[AWS IoT SQL リファレンス](#)」を参照してください。

```
1 select name from 'data/20190906things' where name = 's3'
```

4-5. 【アクションの追加】を押します。

1 つ以上のアクションを設定する

インバウンドメッセージが上記のルールに一致すると、1 つ以上のアクションが選択されます。メッセージ受信時に発生する追加アクティビティ (データベースへの格納、クラウド関数の呼び出し、通知の送信など) を定義するアクション。(\*必須)

アクションの追加

4-6. 複数の AWS リソースとの連携が用意されています。S3 を選びます。

<input type="radio"/>	 Amazon Kinesis ストリームにメッセージを送信する AMAZON KINESIS
<input type="radio"/>	 AWS IoT のトピックにメッセージを再パブリッシュする AWS IoT の再パブリッシュ
<input type="radio"/>	 Amazon S3 バケットにメッセージを格納する S3
<input type="radio"/>	 Amazon Kinesis Firehose ストリームにメッセージを送信する AMAZON KINESIS FIREHOSE
<input type="radio"/>	 CloudWatch にメッセージデータを送信する CLOUDWATCH メトリクス
<input type="radio"/>	 CloudWatch アラームの状態を変更する CLOUDWATCH アラーム

4-7. 【アクションの設定】を押します。

キャンセル
アクションの設定

4-8. 【新しいリソースを作成する】を押します。

### アクションの設定

 Amazon S3 バケットにメッセージを格納する  
S3

このアクションによって、メッセージは S3 バケットのファイルに書き込まれます。

\*S3 バケット

リソースの選択

↺

新しいリソースを作成する

\*キー 

4-9. 【バケットを作成する】を押します。



4-10. 適当なバケット名を入力し、すべてデフォルトのまま【次へ】を3回押し【バケットの作成】を押します。

4-11. IoT の画面に戻り、ぐるぐるしたマークをおすと、先ほど作成したバケットが表示されますので、選択します。



4-12. キーに「test」と入力します。



#### 4-13. 【ロールの作成】を押します。

このアクションを実行するための AWS IoT アクセス権限を付与するロールを選択または作成します。

選択されたロールがありません	更新	ロールの作成	閉じる
<input type="text" value="IAM ロールを検索"/>			

#### 4-14. 適当な名前を付けて【ロールの作成】を押します。

### 新しいロールの作成

新しい IAM ロールがお客様のアカウントに作成されます。AWS IoT がお客様に代わってリソースにアクセスすることを許可するスコープダウンされたアクセス許可を提供するロールにインラインポリシーがアタッチされます。

名前

このフィールドは必須です。

キャンセル

ロールの作成

#### 4-15. 【アクションの追加】 ボタンを押します。

このアクションを実行するための AWS IoT アクセス権限を付与するロールを選択または作成します。

20190906iottestrole	アタッチされたポリシー ✓	ロールの作成	選択
---------------------	---------------	--------	----

キャンセル

アクションの追加

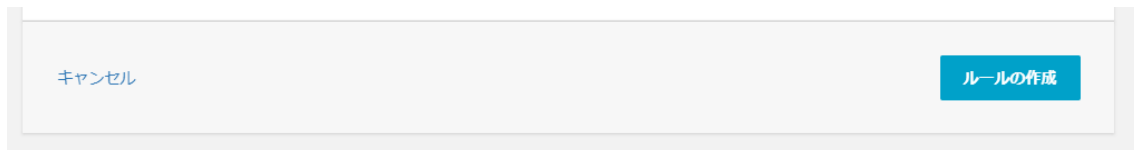
#### 4-16. S3 への書き込み設定が完了しました。

##### 1 つ以上のアクションを設定する

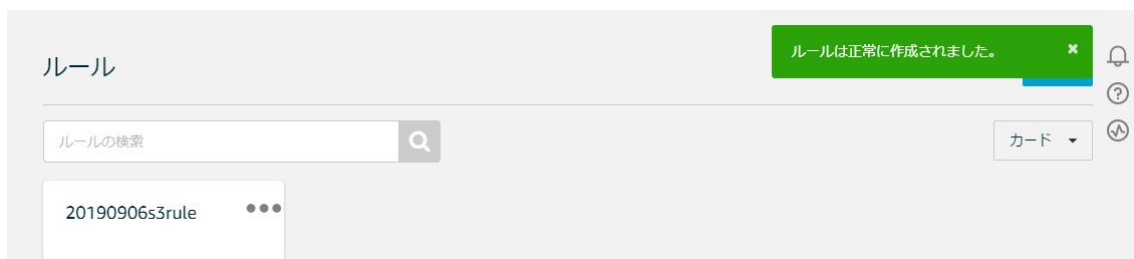
インバウンドメッセージが上記のルールに一致すると、1 つ以上のアクションが選択されます。メッセージ受信時に発生する追加アクティビティ (データベースへの格納、クラウド関数の呼び出し、通知の送信など) を定義するアクション。(\*必須)

	Amazon S3 バケットにメッセージを格納する 20190906iottest	削除	編集
---	--	----	----

4-17. 【ルール作成】を押します。



4-18. ルールが作成されています。これで「s3」というデータを含んだ通信が来た際に、S3 上にファイルが作成されるようになります。

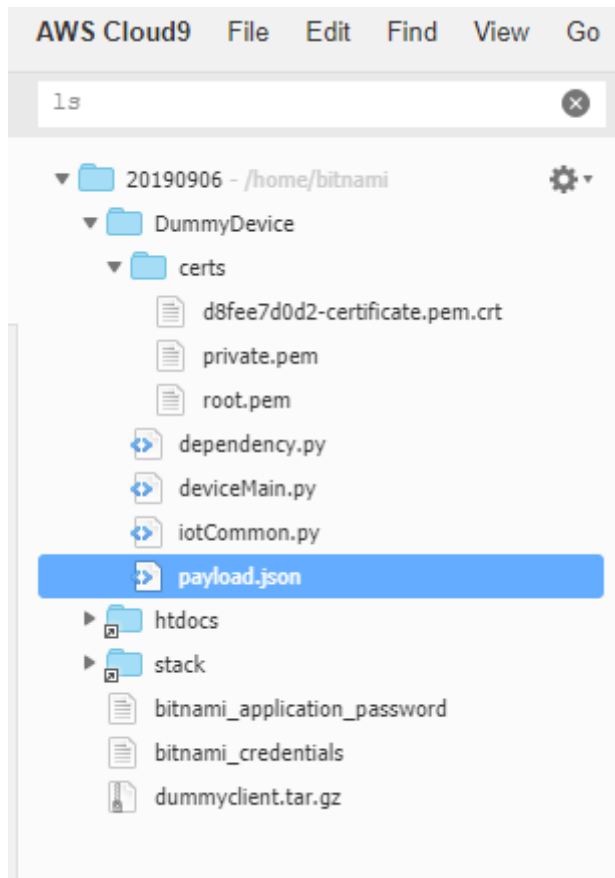


4-19. テキストファイルを開いて以下のコマンドを入力します。(AWS IoT のデータは JSON 形式です。)(シェルでの作業に慣れている方は、Cloud9 上でそのままファイルを作成しても問題ありません。)

```
{ "name": "s3" }
```

入力後、ファイル名を【payload.json】で保存します。

4-20. 保存したファイルを Cloud9 上の【DummyDevice】フォルダにアップロードします。



4-21. シェルで `ctr + c` を押して、先ほどの通信を止めます。

4-22. 以下のコマンドを入力します。

```
curl -D - --tlsv1.2 -X POST --cert ./certs/{証明書ファイル名} --
```

```
key ./certs/private.pem --cacert ./certs/root.pem https://{エンドポイン
```

```
ト}:8443/topics/data/{モノの名前}?qos=0 -d @payload.json
```

動作すると以下の表示になります。

```
HTTP/1.1 200 OK
content-type: application/json
content-length: 65
date: Fri, 06 Sep 2019 08:22:31 GMT
x-amzn-RequestId: 4202a6c5-a439-c1de-de50-f79bc2f4990c
connection: keep-alive
```

```
{"message":"OK","traceId":"4202a6c5-a439-c1de-de50-f79bc2f4990c"}bitnami@ip-172-26-4-21:~/DummyDevice$
```

4-23. テスト画面で受信したデータの確認が可能です。[s3]と表示されていれば成功です。

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。

data/20190906things

トピックに発行

```
1 {  
2   "message": "Hello from AWS IoT console"  
3 }
```

data/20190906things 2019/09/06 17:26:21 [エクスポート](#) [非表示](#)

```
{  
  "name": "s3"  
}
```

4-24. 作成した s3 バケットを見てみましょう。データが保存されています。

Amazon S3 > 20190906iottest

概要	プロパティ	アクセス権限	管理
----	-------	--------	----

🔍 プレフィックスを入力し、Enter キーで検索します。ESC を押してクリアします。

[アップロード](#) [フォルダの作成](#) [ダウンロード](#) [アクション](#) アジアパシフィック(東京) 🔄

表示中 1 ~ 1			
<input type="checkbox"/> 名前 ▼	最終更新日時 ▼	サイズ ▼	ストレージクラス ▼
<input type="checkbox"/> 📄 test	9月 6, 2019 5:26:22 午後 GMT+0900	13.0 B	スタンダード

データを送るたびに最終更新日時が上書きされています。この手順ではデータが単一ファイルを上書きしていきますが、Timestamp をベースとして都度都度ファイル名を変更させることができます。また、payload.json の中身を書き換えて、s3 が含まれていない通信は、s3 のファイル更新日が上書きされないことを確認しましょう。



## 5. 削除

お疲れ様でした！以上でハンズオン終了です。

以下を必ず削除してください。

- Amazon Lightsail

- AWS Cloud9

- AWS IoT のモノ