BLE/W-Fi G1ゲートウェイ

サービス構築ガイド

RATOC Systems, Inc.

Version.1.02

目次

1-1 BLE/Wi-Fi G1ゲートウェイについて

BLE/Wi-Fi G1ゲートウェイ(以下、G1 ゲートウェイと呼ぶ)は、SHENZHEN MINEW TECHNOLOGIES CO LTD(以下、MINEW社と呼ぶ) の製品です。
プロダクト名およびモデル番号は下記になります。

プロダクト名	Bluetooth Smart IoT Gateway
モデル番号	G1-E-cherry
ホームページURL	https://www.minew.com/product/g1-iot-gateway

1-2 本構築ガイドの概要

本構築ガイドは、次ページFig.1のようなサービスをお客様ご自身で構築して頂くための解説書です。
①G1ゲートウェイをWi-Fiネットワークに接続させる。
②BLEアドバタイズデータを定期的に収集する。
③自分のAWSアカウントを作成して、AWS IoT Coreに接続する準備を行う
④G1 ゲートウェイをAWS IoT Coreに接続し、アップロードされたアドバタイズデータの履歴をログ表示する.

※1. 本構築ガイドは、MINEW社の ”Bluetooth Smart IoT Gateway”がサポートしている機能からBLEアドバタイズデータをAWSクラウドへアップロードする際に必要な機能に絞って解説を行っています。
※2. AWSクラウドへの設定作業が成功せず、G1ゲートウェイがダイナミックな6色回転表示のままになる場合は、Factoryリセットを行ってもう一度最初から設定をやり直してください、。

Fig.1 サービス構成図

1-3 G1ゲートウェイ操作概要

microUSBポートに5V電源を接続し、電源スイッチをオンにします。
Fig.3のようにゲートウェイのAPモードSSID名”GW-XXXXXXXXXXXX“が検出表示されます。
スマホを”GW-XXXXXXXXXXXX“に接続します。

注 1. Fig,3はAndroidスマホのWi-Fiネットワーク画面の例です。
注 2. ”XXXXXXXXXXXX”はゲートウェイのMACアドレス16進大文字表示です。
注 3. APモードSSID名が表示されない場合は、リセットボタンを押してリトライしてください。
※リセットボタンを2秒以上長押しし、5秒を超えると工場出荷時の設定に初期化されます。

Fig.2 外部インターフェイス

Fig.3

1-4 G1ゲートウェイカラーLED点灯仕様

LED点灯モード	動作説明
静的6色ライト	ゲートウェイが起動中であることを示し、この状態で RESET ボタンを押すことは無効です。
ダイナミックな6色ライト回転 （赤、黄、白の単色設定も可能）	ゲートウェイがサーバへの接続に失敗する場合、ゲートウェイのネットワーク・コンフィギュレーションに失敗しているか、サーバがオンラインでないことを意味します。
ダイナミックホワイト ライト回転	ゲートウェイが起動し、サーバに接続しようとしています。
ダイナミック・ブリージング・ライト ※呼吸のリズムで順番に色が変わる	ゲートウェイがサーバに正常に接続された（注：ゲートウェイがデフォルトでダイナミックブリージングライトになった後、省エネモードに入るために1分遅れて消灯する。コンフィギュレーション・ページで長時間点灯モードを設定できます）。
ライト消灯	ゲートウェイの電源が入っていないか、または省電力モードであることを示します。
緑色のランプが素早く点滅する	ゲートウェイが USB ディスクを認識し、正常にマウントされたことを意味する。USB ディスクがゲートウェイに挿入された後、15 秒以内に USB ディスクに問題がなければ、ゲートウェイはこの状態でカラフルなライトを表示する。
黄色のランプが素早く点滅する	ゲートウェイが USB ディスクにデータを読み書きしていることを示す。

Fig.20はG1ゲートウェイコンフィギュレーションツールの設定画面です。
AWSのMQTTに接続するためのエンドポイントURL情報や接続に必要なクラウドからダウンロードした各種証明書やキーファイルの指定が必要になります。
従って、コンフィギュレーションツールの設定を行う前に、AWSクラウド側の準備を行います。

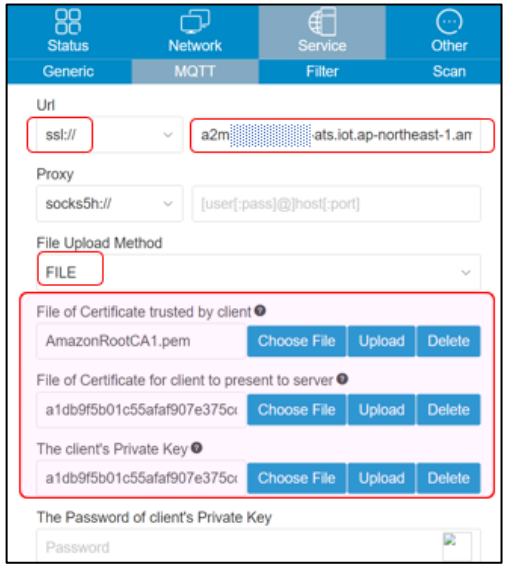


Fig.20コンフィギュレーションツール

AWSをはじめてご利用する場合は、アカウントを作成してFig.21の画面よりサインアップしてください。
サインアップすると、Fig.22のよなうなサービス(はじめての場合は全サービス)の一覧が表示されます。
本構築ガイドで使用する主なクラウドサービスは、下記になります。

- MQTT接続するためのIoT Coreサービス
- セキュリティ管理のためのIAMサービス
- ログを確認するCloudWatchサービス

※AWSへのサインアップはWindows環境で行っています。
G1ゲートウェイコンフィギュレーションツールの起動は、Windows環境で行っています。

Fig.21

AWSアカウント登録を行いクラウドにサインアップします。

最初にリージョンをデフォルトから”東京”に変更します。
※サインする毎に毎回変更が必要です。

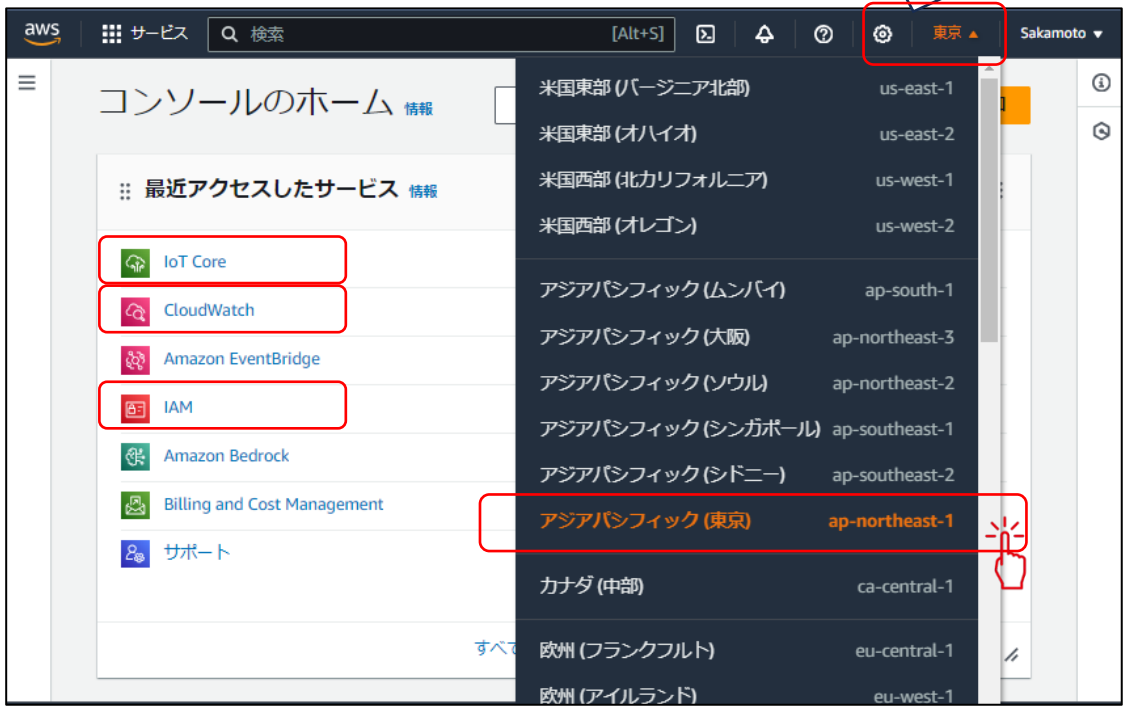


Fig.22

2-1 証明書に紐づけるポリシー作成

G1ゲートウェイからアップロードしたデータをIoT Coreサービスでpublishおよびsubscribeするためには、下記のJSONのポリシーを設定して、証明書にアタッチすることが必要です。

Fig.23

Fig.24

コピペ用JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "iot:Connect",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "iot:Publish",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "iot:Receive",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": "iot:Subscribe",
   "Resource": "*"
  }
 ]
}
```

2-2 証明書の作成とダウンロード

“証明書を追加”より、”証明書の作成”を選択します。

Fig.25

Fig.26

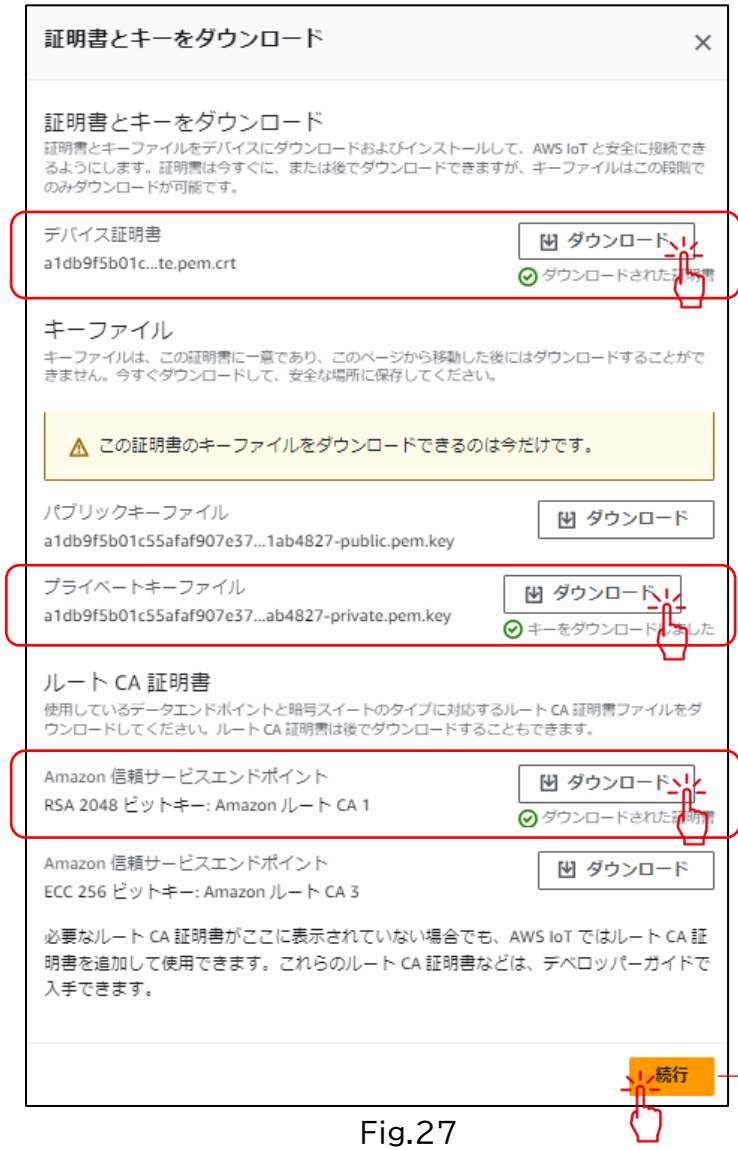


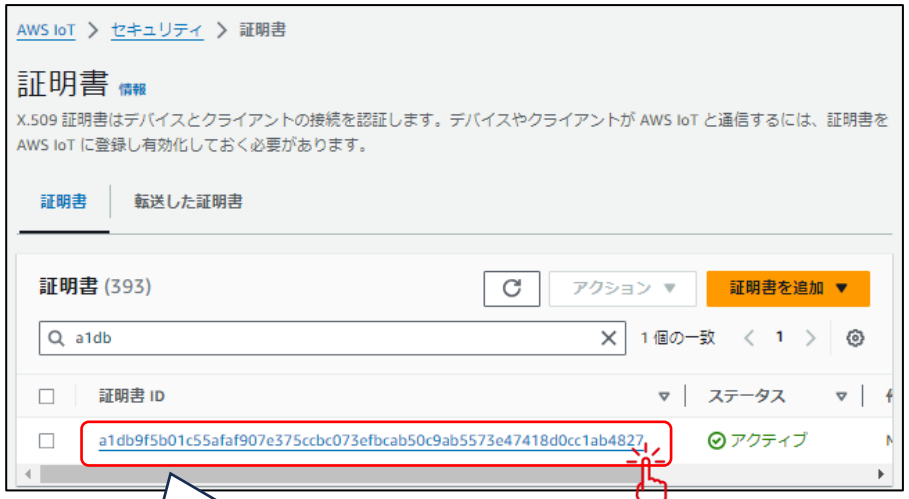
Fig.27

3つの証明者ダウンロードし、「続行」をクリック

- デバイス証明書
- プライベートキーファイル
- RSA 2048ビットキー：AmazonルートCA1

証明書idの先頭数桁はこの後必要になるので覚えておいてください。

2-3 証明書にポリシーをアタッチ



先ほど作成した”a1db”で始まる証明書をクリック

Fig.28

Fig.29

Fig.2A

2-1 項で作成した”G1_policy”を選択して、”ポリシーをアタッチ”をクリック

”ポリシーをアタッチ”をクリック

2-4 AWS IoTのURL

AWS IoTの”設定”を開いて、エンドポイント名をコピーして保存しておきます。
この後説明するG1ゲートウェイConfigurationアプリの「3-6項”MQTT With SSL Method”のURLに設定します。

Fig.2B

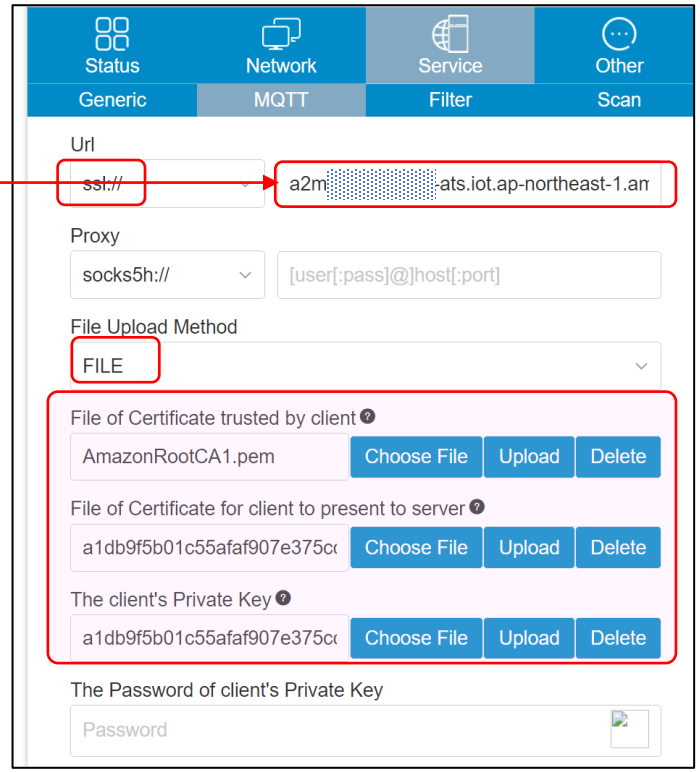


Fig.2C

2-5 G1ゲートウェイからのメッセージのルーティングルール作成

ここからは、G1ゲートウェイからアップロードされたメッセージ(アドバタイズデータ)をログ出力して目視確認するための方法の説明になります。

「ルールを作成」をクリック

Fig.2D

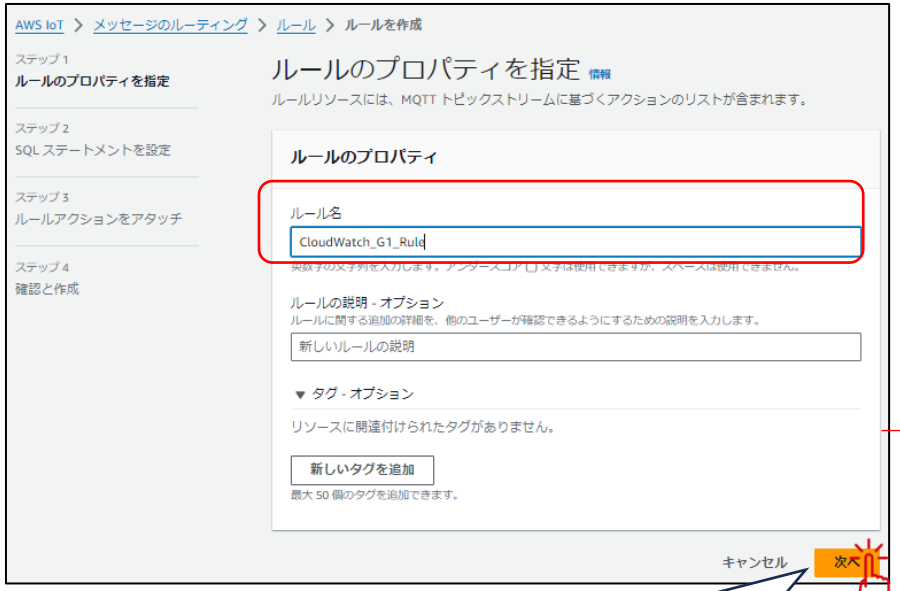


Fig.2E

ルール名を入力して「次へ」をクリック

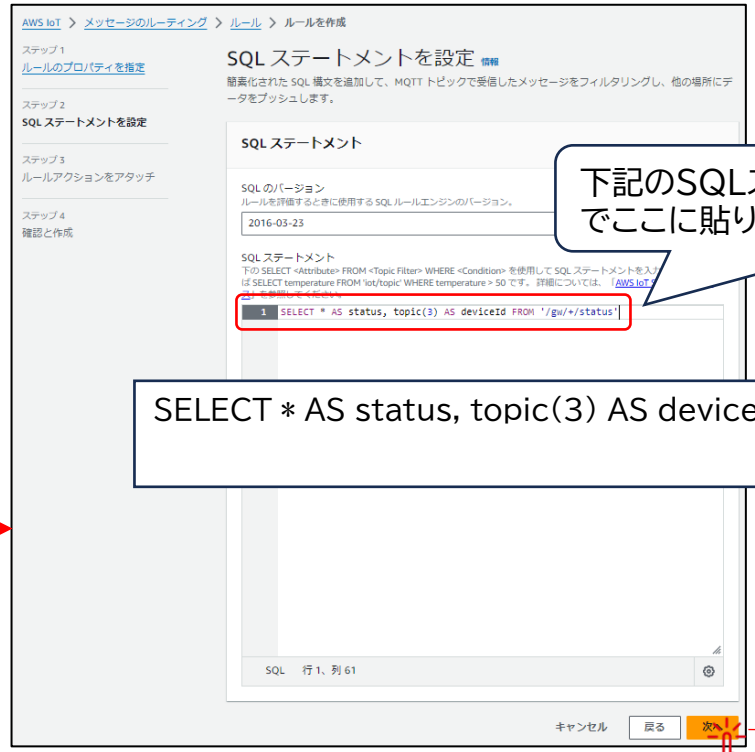


Fig.2F

下記のSQLステートメントをCopy&Paste
でここに貼り付けて、「次へ」をクリック

Copy&Paste用SQLステートメント

SELECT * AS status, topic(3) AS deviceId FROM '/gw/+/status'

ルールアクションをアタッチへ進む

CloudWatchサービスの設定が起動されます。

Fig.2H

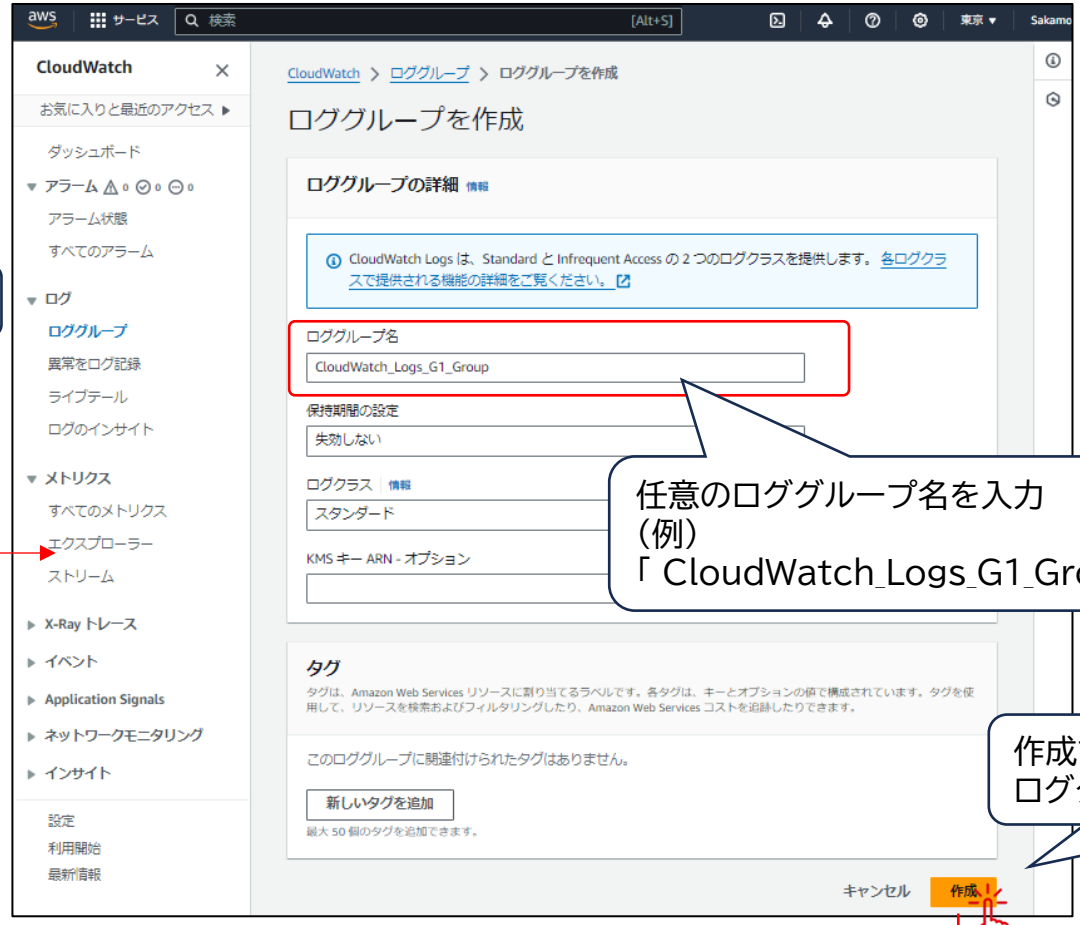
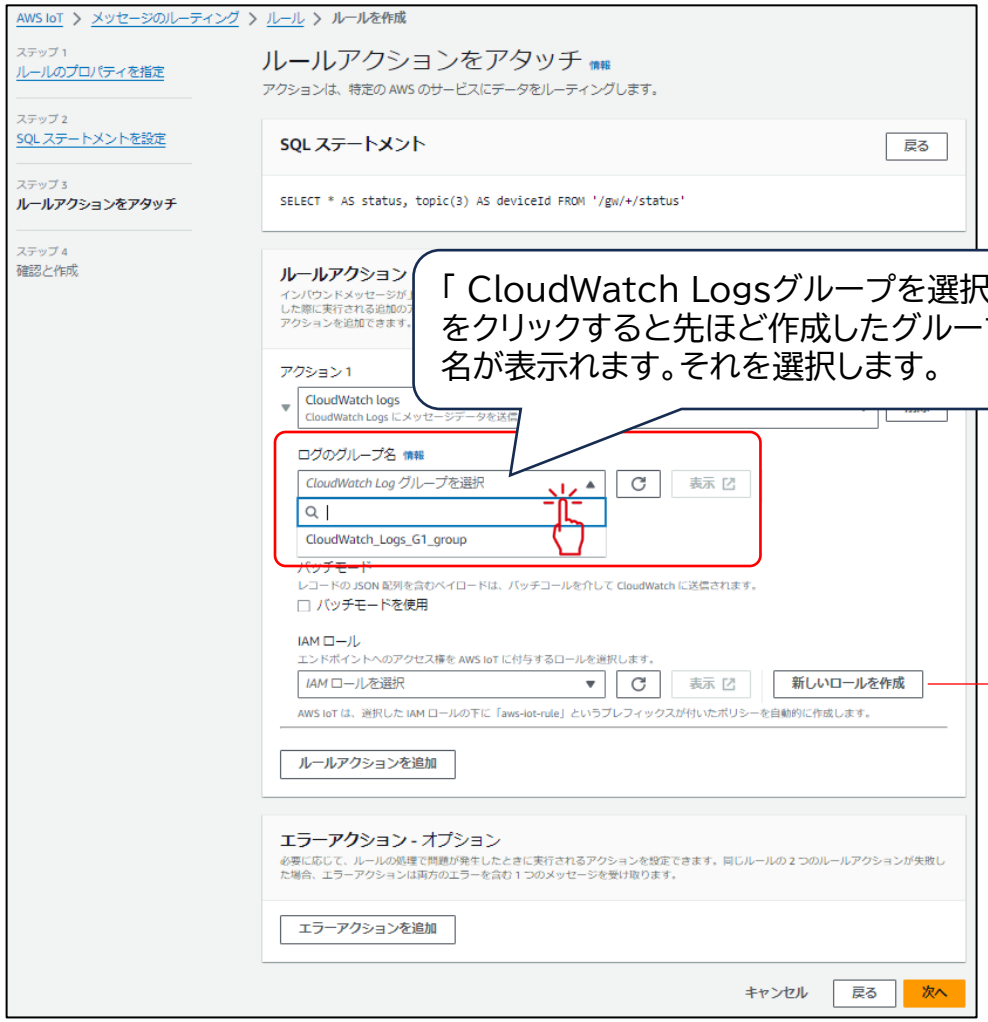


Fig.2I

作成すると下記完了画面に移ります。
ロググループの作成は終了です。

Fig.2J

“ルールアクションをアタッチ”の設定に戻ります。



「 CloudWatch Logsグループを選択」をクリックすると先ほど作成したグループ名が表示されます。それを選択します。

Fig.2K

ここに作成したロール名が表示されます

「 新しいロールを作成」をクリック

確認と作成へ進む

Fig.2L

任意のロール名を入力
（例）
「 CloudWatch_G1_Role」

Fig.2M

確認と作成

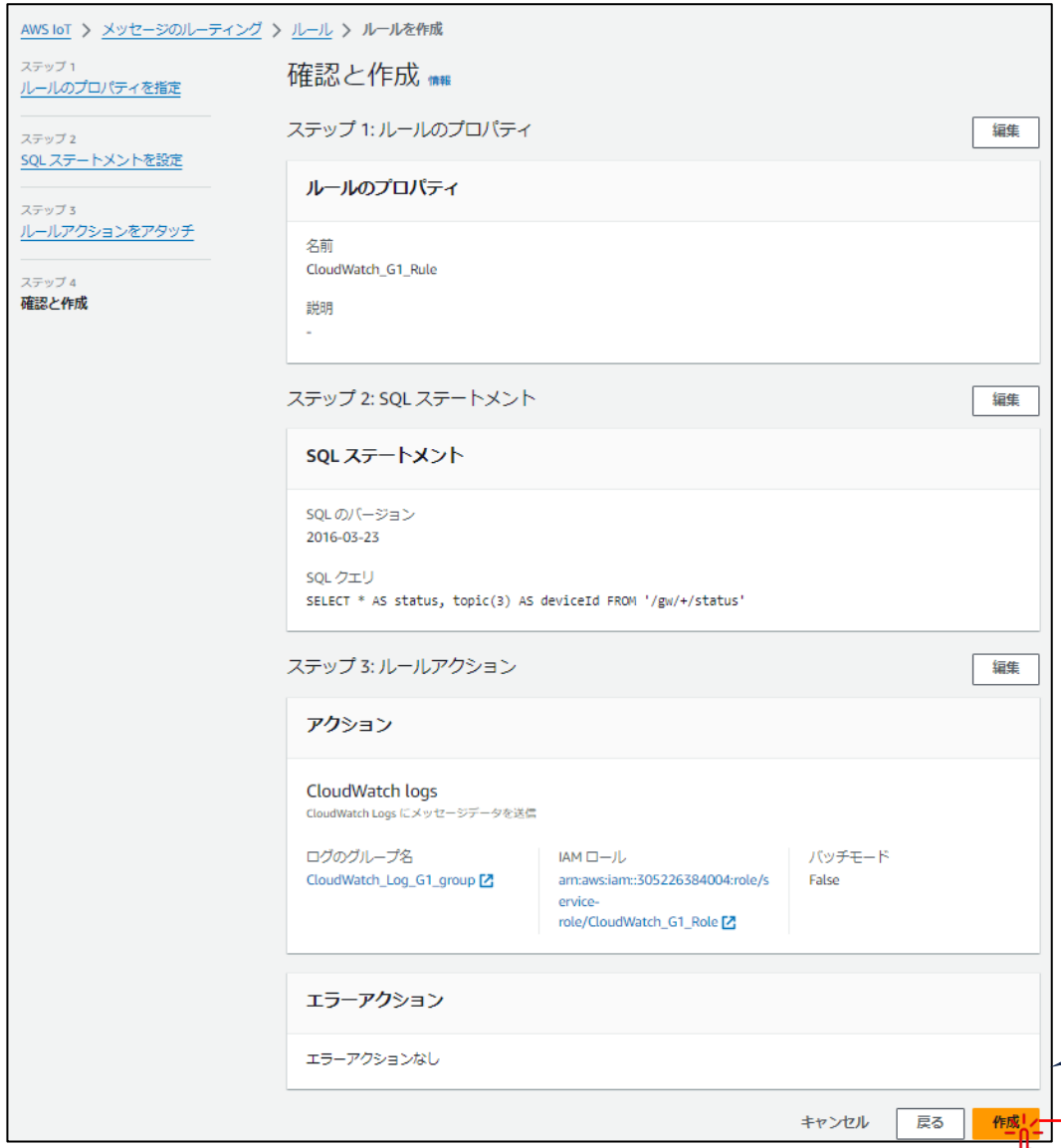


Fig.2N

各項目について設定した内容に問題なければ”作成”をクリックします。

Fig.2O

2-6 ログデータの確認

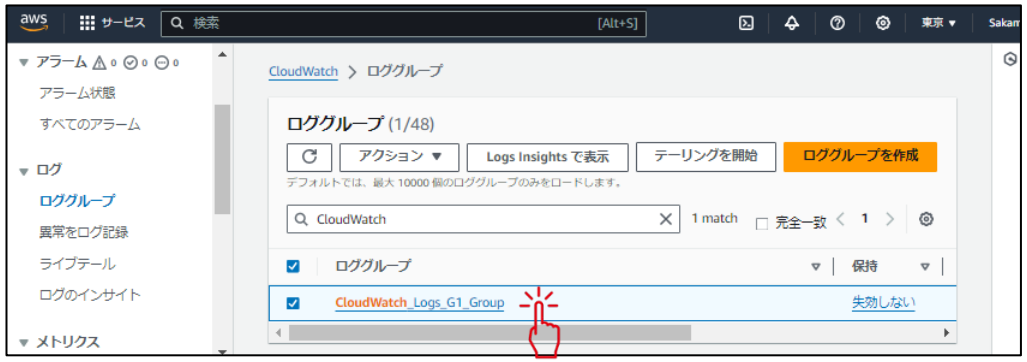


Fig.2P

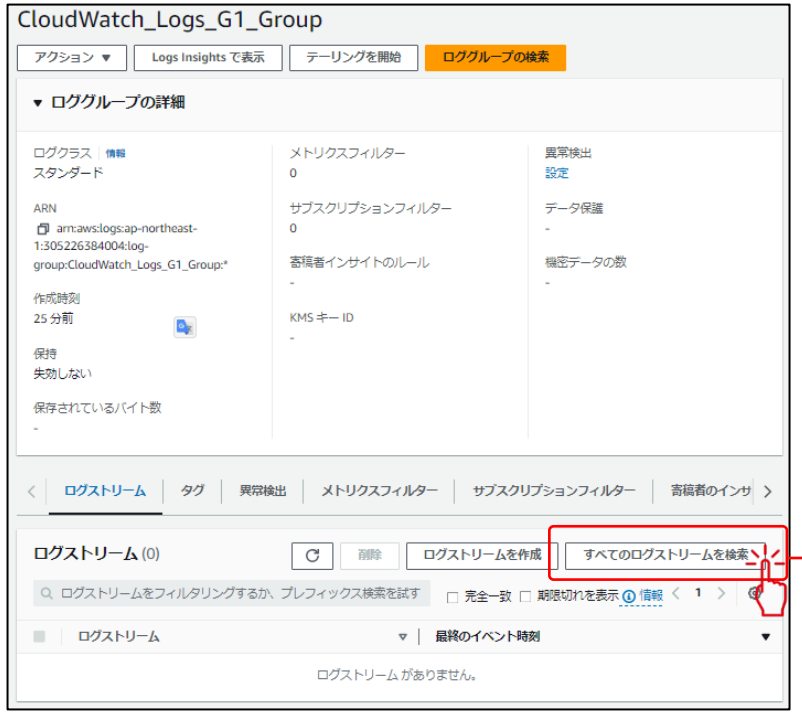
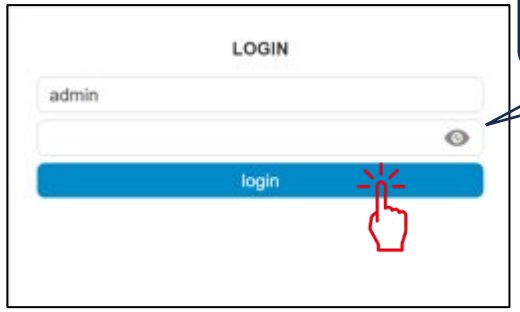


Fig.2Q

3-1 G1ゲートウェイConfigurationアプリに接続

ブラウザからG1 ゲートウェイのコンフィギュレーションページを開き、ログインを行ってWi-Fi設定を行います。

http://192.168.99.1



デフォルトではパスワードなしになっています。
そのままログインします。

Fig.30

ログインできない場合は、スマホがG1ゲートウェイに接続しているか確認してください。

Fig.31

本構築ガイドでG1 ゲートウェイのコンフィギュレーションページの設定変更を行っているページは下記のみです。
その他の項目はデフォルトのままで動作させています。

3-2 BLEアドバタイズデータ収集
　　unknownとgatewayのアドバタイズデータのみ指定
3-5 MQTT　アクセス
　　Update　Interval
3-6 MQTT With SSL Method
　　URLエンドポイントアドレスと証明書ファイルのUpload
3-7 Wi-Fi アクセスポイントに接続

Fig.32

● Statusページ設定項目の説明

各項目が正しく表示されているか確認します。特に変更が必要な項目はありません。

項目名	説明
MAC Address	G1 ゲートウェイのMACアドレス。(16進大文字表記)
Firmware Model	ファームウェアモデル名
WiFi Firmware Version	Wi-Fi ファームウェアバージョン
BLE Firmware Version	BLE ファームウェアバージョン
Network Mode	G1 ゲートウェイが接続中のネットワークが表示されます。Wi-Fi接続な場合は、”wireless”が表示され、接続されていない場合は”N/A”が表示されます。
WAN IP	クライアントとして外部ネットワーク接続により取得したIPが表示されます。接続されていない場合は”N/A”が表示されます。
Disable	チェックを入れるとWi-Fi APモードが無効になります、 ❓ フェイルオーバー機能が有効な場合、フェイルオーバー機能が ap_only モードに切り替わると、AP を無効にしてもG1 ゲートウェイはゲートウェイの AP を強制的にオンにする。しかし、G1 ゲートウェイのネットワークが正常であれば、ゲートウェイは ap の状態に戻すので心配はいらない。
Hidden	チェックを入れるとWi-Fi APモードがHiddenモードになります、 ❓ “Hidden”はWi-Fi APモードが非表示になるという意味です。
SSID	APモードのSSIDデフォルト名をカスタマイズします。
Key	APモードの接続に使用するパスワードを設定します。
LAN IP Address	APモードのIPアドレスを設定します。デフォルトは、”192.168.99.1”です。
New Password	コンフィギュレーションページへのログインパスワードを設定します。デフォルトではパスワードなしです。
Confirm Password	ログインパスワードの確認入力になります。

3-2 BLEアドバタイズデータ収集

G1 ゲートウェイは起動後、アドバタイズデータを収集し続け、ネットワークが利用可能になると、デフォルトでは毎秒1回の頻度で接続されたサーバにデータを送信します。

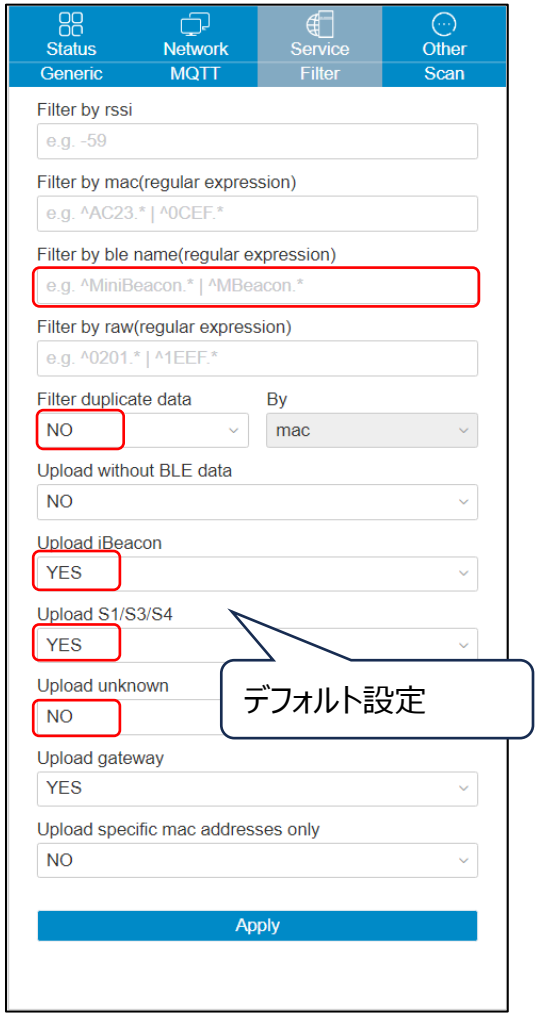


Fig.33

G1 ゲートウェイによってアップロードされるデータには、JSON 配列のデータ形式(long と short のデータ形式を含む)と、Binary のオリジナル・バイナリ・データ形式(long と short のデータ形式を含む)の 2 つの形式があります。
G1ゲートウェイは、デフォルトで JSON-LONG フォーマットを使用してサーバにアップロードします。現場に配置されたG1 ゲートウェイの帯域幅が小さい場合は、Binary フォーマットに切り替えることができます。Binary 形式のデータ量は、JSON データ形式の 2 倍以上です。

項目名	説明
Filter by rssi	RSSI値でフィルタリング 信号強度がこの値 (dBm) より大きいデータのみをアップロードします。値が入力されていない場合は、フィルタリングが行われていないことを意味します。値は -100 < rssi < 0 で入力できます。 例: -67 を入力すると、-68 以下の弱い信号はサーバにアップロードされません。
Filter by mac (regular expression)	MACでフィルタリング BLE Mac の正規表現例: AC23 または 0CEF で始まる BLE mac データのみを受信したい場合、正規表現は次のとおりです: ^AC23.*|^0CEF.* 注: ここで、BLE mac では大文字と小文字が区別されず、コロンも区別されません。
Filter by BLE name (regular expression)	BLE Name(正規表現)でフィルタリング たとえば、BLE 名が MiniBeacon または Minnew で始まるデータのみを受信する場合、正規表現は次のようになります: ^MiniBeacon.*|^Mbeacon.*
Filter by raw (regular expression)	Rawデータでフィルタリング Rawデータの正規表現このフィルタは、JSON/Binary-Long/Short を含むすべてのデータ型に適用できます。このフィルタ条件は、BLE デバイスのアドバタイズデータパケットが正規である限り使用できます。 例: FDA50693A4E24FB1AFCFC6EB07647825 として UUID のみを受け取りたいiBeacon ブロードキャスト パッケージの場合、式は ^.* FDA50693A4E24FB1AFCFC6EB07647825 .* として記述できます。 注: ここでの生データ文字列は大文字と小文字が区別されません。
Filter duplicate data / By	アップロード間隔内の重複データでフィルタリング デフォルトは NO、オプションで YES、NO。フィルタリング条件を設定するには、次の 3 つの方法があります。 mac: 同じ MAC アドレスを持つアドバタイズデータパケットは重複データとみなされます。 mac+type: 同じ MAC アドレスと同じタイプを持つブロードキャスト パケットは重複データとみなされます。 mac+raw: 同じ MAC アドレスと同じ raw データを持つアドバタイズデータパケットは重複データとみなされます。

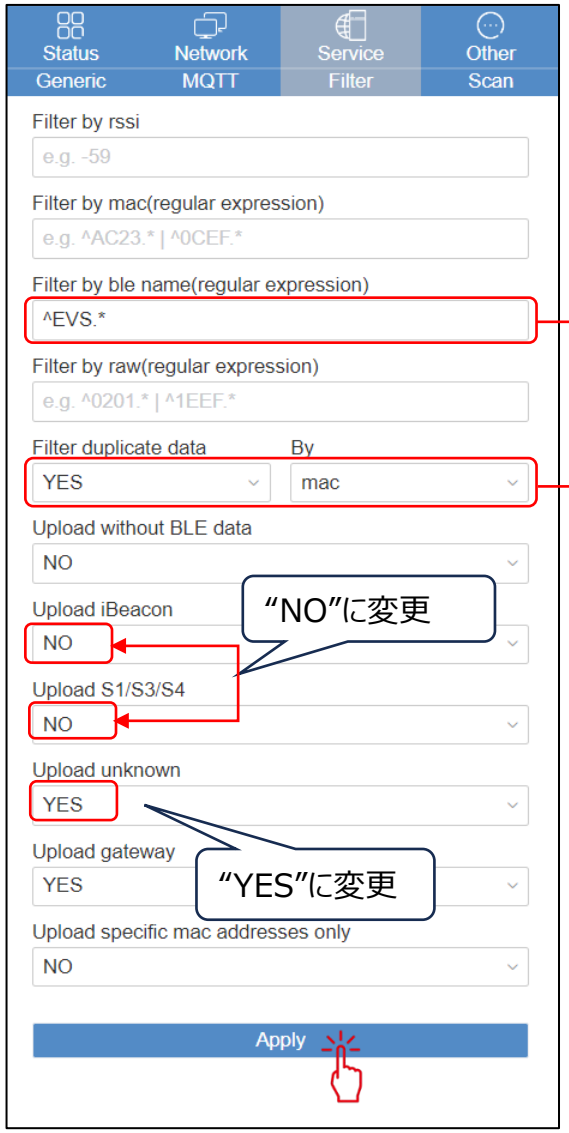


Fig.34

次ページ“アドバタイズデータの効率的なサーバへのアップロード方法”参照

“unknown”と”gateway”のアドバタイズデータのみAWSへアップロードします。

項目名	説明
Upload without BLE data	BLEデータがない場合にデータをアップロードするかどうか指定します ”YES”は本構築ガイドではサポート外になります。
Upload iBeacon	iBeaconタイプのデータをアップロードするかどうか指定します ”YES”は本構築ガイドではサポート外になります。
Upload S1/S3/S4	S1/S3/S4タイプのデータをアップロードするかどうか指定します ”YES”は本構築ガイドではサポート外になります。
Upload unknown	unknownタイプのデータをアップロードするかどうか指定します。 デフォルトの NOを“YES”の設定に変更して利用してください。
Upload gateway	ゲートウェイタイプのデータをアップロードするかどうか指定します NOもしくはYESのどちらかを指定してください。
Upload specific mac address only	特定の Mac アドレスからのデータのみをアップロードするかどうか指定します。 ”YES”は本構築ガイドではサポート外になります。

● アドバタイズデータの効率的なサーバへのアップロード方法

3-2 項の”BLEアドバタイズデータ収集”では、Fig.34のFilter by BLE nameに[~EVS.*]、Filter duplicate data に”YES”を設定しています。
この設定はFig.35のような当社製品”RS-BTEVS1” BLE環境センサのアドバタイズデータを効率的にサーバへアップロードするための設定です。
RS-BTEVS1は、Advertise Device Nameが”EVS-XXXX”という名前でアドバタイズ間隔150msで発信しています。

アドバタイズを発信するデバイスが複数存在する環境では、デフォルトではG1ゲートウェイは全てのデバイスのデータをサーバにアップロードします。
対象としない全てのデバイスのデータをサーバへアップロードすると無駄が発生するために、フィルタリング設定が有効です。
自分がハンドリングしたいデバイスがRS-BTEVS1と仮定し、そのアドバタイズデータのみをフィルタリングする目的で[~EVS.*]を指定しています。

3-5項” MQTT アクセス“のように、サーバにアップロードする間隔を1分に設定した場合、G1ゲートウェイは1分間にスキャンで検出されたアドバタイズデータを全てサーバにアップロードします。
同一デバイスからのアドバタイズデータは一つとするために、Filter duplicate data をMACアドレスを指定し”YES”に設定しています。

EVS-A15F　　EVS-6068

2台のBTEVS1を動作させG1ゲートウェイでアドバタイズデータをスキャン

左記のフィルタリング設定でCloudWatch上でログデータを確認すると、Fig.35のように2台のRS-BTEVS1より1分簡に一つのアドバタイズデータがサーバにアップロードされていることが確認できます。

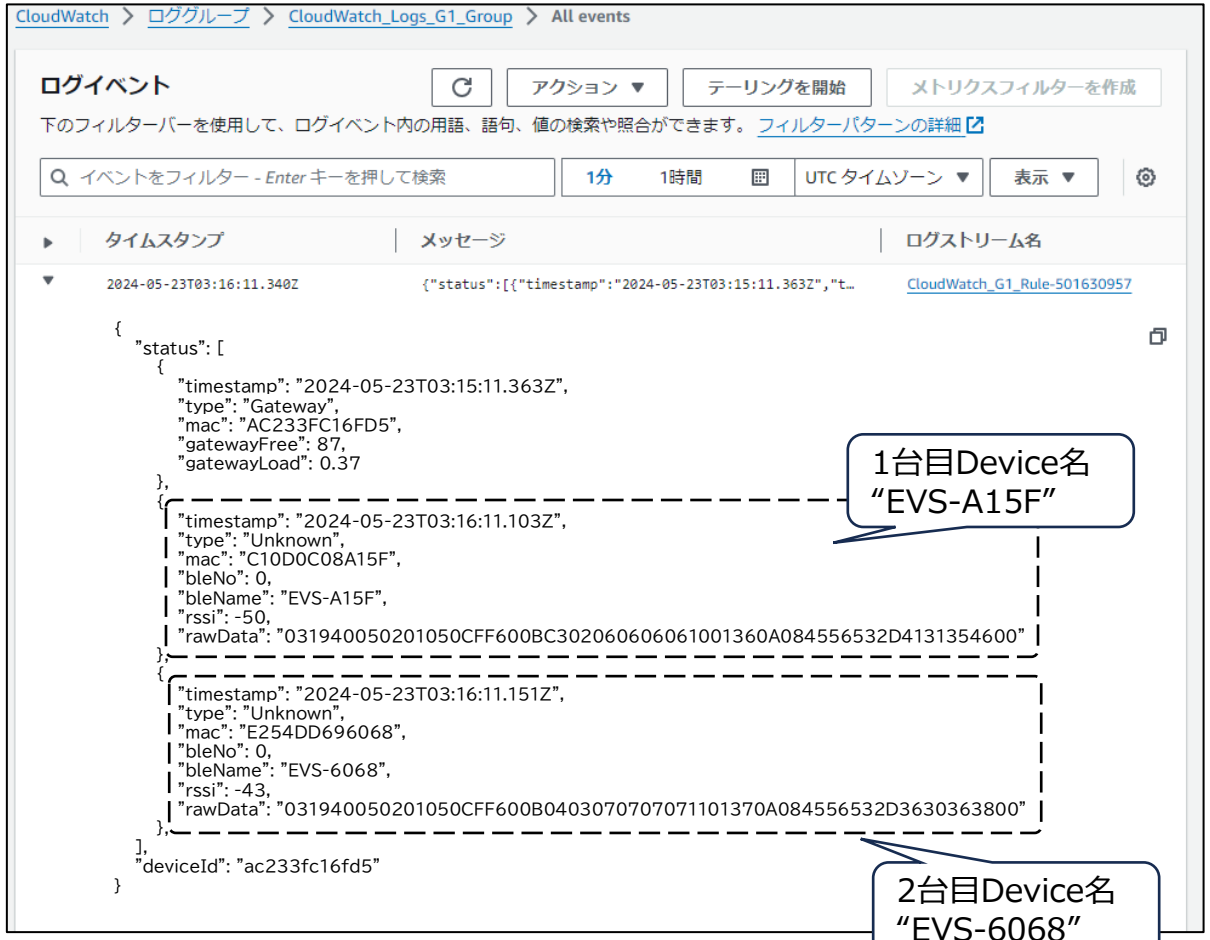


Fig.35

3-3 Scan Parameter 設定

Scanパラメータは、Bluetoothモジュールのスキャン間隔を希望する値に設定するために使用されます。

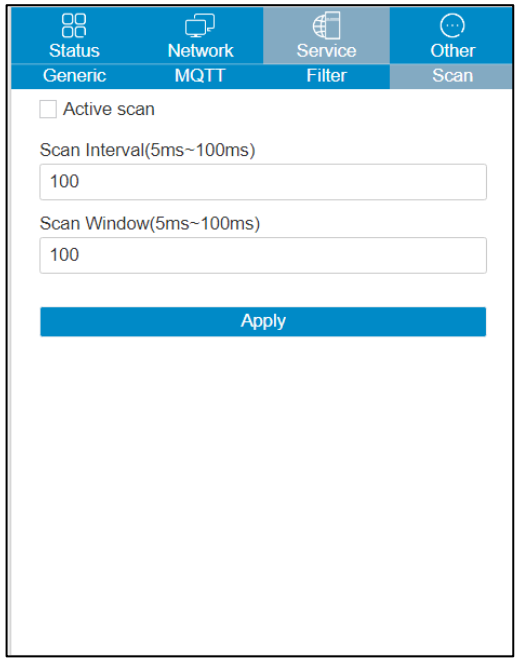


Fig.36

項目名	説明
Active scan	アクティブスキャンを有効にする場合はチェックを入れます。 1. BLEデバイスのアドバタイズデータパケットには 2 種類があります。ブロードキャストパケットとスキャン応答パケット。ブロードキャストパケットは、BLEデバイスによってアクティブにブロードキャストされます。スキャナがリクエストを送信した後、BLE タグがリクエストを受信すると、スキャン応答パケットがパッシブにブロードキャストされます。 2. G1 ゲートウェイの BLEデバイスのスキャン戦略は、それに応じてアクティブ スキャンとパッシブ スキャンの 2 つのタイプに分けられます。アクティブ スキャンは応答パケットの要求を BLEデバイスに送信しますが、パッシブ スキャンはブロードキャスト パケットのみを受信し、応答パケットの要求は送信しません。 3. BLEデバイスが応答パケットをスキャンしない場合は、このパラメータを NO に設定すると、BLE ブロードキャスト パケットのスキャン レートが向上します。
Scan Interval （5ms ~ 100ms）	5ms ~ 100msでスキャン間隔を指定します。 スキャン間隔とスキャン スキャン ウィンドウは併用されます。
Scan Window （5ms ~ 100ms）	5ms ~ 100msでスキャンWindowを指定します。 スキャン ウィンドウ パラメータをスキャン間隔パラメータより大きくすることはできません。2 つが等しい場合、スキャン率は 100% に達します。

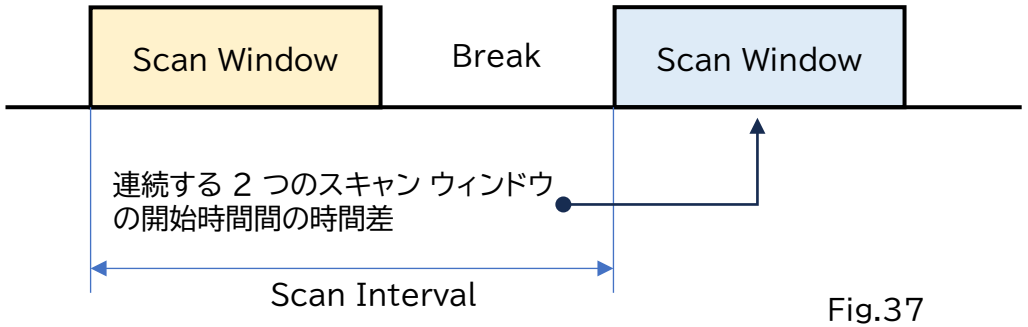


Fig.37

3-4 JSON Data Format

G1 ゲートウェイがサポートしている Bluetooth デバイスには、標準的な iBeacon デバイス、S1 センサー、S3 センサー、S4 センサーがあります。これらのタイプのBluetoothデバイスのデータに加えて、Bluetoothのオリジナルデータ がUnknownデータセグメントにアップロードされ、サーバ自身でパースできるようになっています。
また、G1 ゲートウェイによってアップロードされた JSON 配列のデータであることを示すために、Gateway というデータタイプが追加されています。
(重要)
本構成ガイドでは、上記の”Gateway”情報と”Unknown”データのみを利用します。iBeacon デバイス、S1 センサー、S3 センサー、S4 センサーについては未サポートとなります。

項目名	説明
timestamp	ISO 8601 timeフォーマット
Type	Data type
mac	MACの16進数大文字形式。タイプがGatewayの場合、macアドレスはG1 ゲートウェイのMACアドレス、その他はBluetoothデバイスのMACアドレスとなります。
bleNo	ブロードキャストパケットはBluetoothモジュールの数だけ収集される。ゲートウェイに複数のBluetoothモジュールがある場合は注意が必要です。
bleName	BLEタイプのデバイスが存在し、解析できない場合は空文字列となる
rssi	BLEデバイスのrssi強度
rawData	BLEアドバタイズデータの大文字の16進数表記データ。デバイスがUnknownの場合に存在する。
gatewayFree	ゲートウェイ残メモリ(単位:MB)
gatewayLoad	ゲートウェイ負荷

JSON Data Format サンプル例

```
[
  {
  ”timestamp” : ”2020-01-14T03:54:09.627Z”,
  ”type” : ”Gateway”,
  ”mac” : ”AC233FC0211B”,
  ”gatewayFree” : 86,
  ”gatewayLoad” : 1.96
  }, {
  ”type” : ”iBeacon”,
  **********************************************
  このタイプは、本サービスではサポート外のため省略
  **********************************************

  }, {
  ”type” : ”S1”,
  **********************************************
  このタイプは、本サービスではサポート外のため省略
  **********************************************
  }, {
  ”type” : ”S3”,
  **********************************************
  このタイプは、本サービスではサポート外のため省略
  **********************************************
  }, {
  ”type” : ”S4”,
  **********************************************
  このタイプは、本サービスではサポート外のため省略
  **********************************************
  }, {
  ”timestamp” : ”2020-01-14T03:54:09.644Z”,
  ”type” : ”Unknown”,
  ”mac” : ”0F030ED2BB0F”,
  ”bleNo” : 2,
  ”bleName” : ””,
  ”rssi” : -72,
  “rawData” : “1EFF0600010……8F143E042F”
  }
]
```

3-5 MQTT アクセス

G1 ゲートウェイは現在、ローカルまたはインターネット上のサーバと通信するために、MQTT、HTTP、TCP ネットワークプロトコルをサポートしています。
サーバのアーキテクチャに応じて適切なネットワークプロトコルを選択できますが、本構築ガイドでサポートするのはMQTTプロトコルのみになります。

※1.G1 ゲートウェイは、工場出荷時にデフォルトでYunliwuのTag Cloud IoTサービスに接続されています。G1ゲートウェイは、デモとしてデフォルトでYunliwuli でTag Cloud IoTサービスとコンソールが装備されているゲートウェイのアプリケーションを体験することができますが、本構築ガイドではサポート致しません。

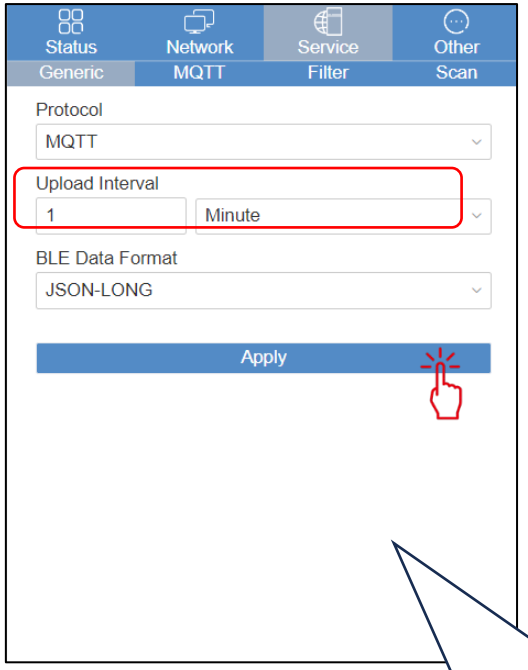


Fig.38

1分間隔でアップロードするように設定しています。
ご利用されるサービスの内容により適切な間隔を
設定します。

MQTTアクセスを使用する場合、G1 ゲートウェイは、定期的にBLEアドバタイズデータをアップロードし、リモートコマンド制御の機能をサポートしています。
G1 ゲートウェイは、MQTT 3.1.1プロトコル標準サーバをサポートします。
具体的なプロトコルについては、MQTT 3.1.1プロトコルドキュメントを参照し、詳細は
http://mqtt.org。

項目名	説明
Protocol	MQTTを指定します。
Upload Interval	G1 ゲートウェイからクラウドへUpload するインターバルにを指定、デフォルトは1秒ですが、通信量など考慮してサービスに見合ったインターバルに変更してください。 G1ゲートウェイがサーバに繋がった時点でアドバタイズデータのUploadが始まります。Upload Intervalで指定した通信頻度で課金が発生します。
BLE data format	G1 ゲートウェイによってアップロードされるデータには、 JSON-LONG（デフォルト）、JSON-SHORT、BINARY-LONG、BINARY-SHORT の4つの形式があります。

3-6 MQTT With SSL Method

MQTT アクセスを使用する場合、”SSL”もしくは”TLS”プロトコルを選択することができますが、本構築ガイドでサポートするのは” SSL”のみになります。
Urlパラメータのドロップダウンリストで ”ssl://”を選択した後、表示されるパラメータを使用してG1 ゲートウェイへのロード証明書を設定します。

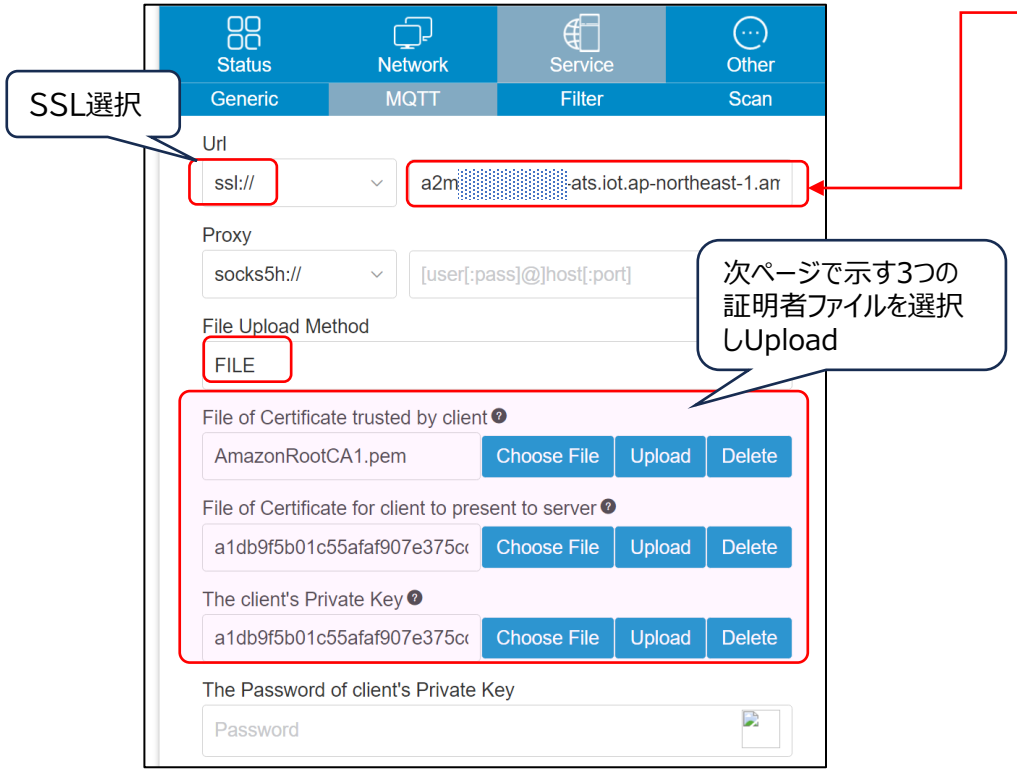


Fig.39

項目名	説明
Url	MQTTサーバのURLを “ssl://”を指定して設定します。 デフォルト: tcp://tagcloud.minew.com:2883 2-4項 “AWS IoTのURL” のエンドポイントに書き換えが必要 a2m[redacted]gpt-ats.iot.ap-northeast-1.amazonaws.com
Proxy	MQTT用socket5プロキシサーバのセットアップを行います
File Upload Method	本構築ガイドでサポートするMethodは、”FILE”のみになります。”FILE”を選択してください。 USB：USBを使用して証明書をアップロードする HFS： HFSを使用して証明書をアップロードする（Http ファイルサーバ） FILE：ブラウザ経由で証明書をアップロード
File of Certificate trusted by client	USB ディスク/HFS 内の CA 証明書のファイル名 USB：ゲートウェイは証明書ファイルを USB ディスクのルートディレクトリに直接ダウンロードする。 HFS: ゲートウェイは証明書ファイルを ${Urlpath} パスに直接ダウンロードします。 FILE：G1ゲートウェイは、ブラウザを通して証明書ファイルをダウンロードする。
File of Certificate for client to present to server	USB ディスク/HFS 内のゲートウェイ証明書のファイル名。 USB：HFS: FILE：の説明省略
The client ’s Private Key	USB ディスク/HFS 内のキーファイルのファイル名。 USB：HFS: FILE：の説明省略
The Password of client ’ s Private Key	ゲートウェイ証明書の秘密鍵が暗号化されている場合、このパスワードを提供する必要がある。

Fig.3A

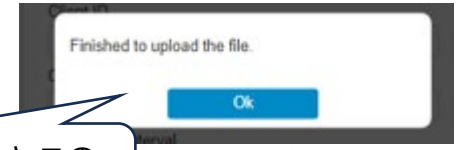
2-2項”証明書の作成とダウンロード”でダウンロード済みの下記のファイルを指定します。

- デバイス証明書
- プライベートキーファイル
- RSA 2048ビットキー:AmazonルートCA1

xxx･･･xxx-certificate.pem.crt

xxx･･･xxx-private.pem.key

AmazonRootCA1.pem



Uploadに成功するとこのメッセージが表示されます。

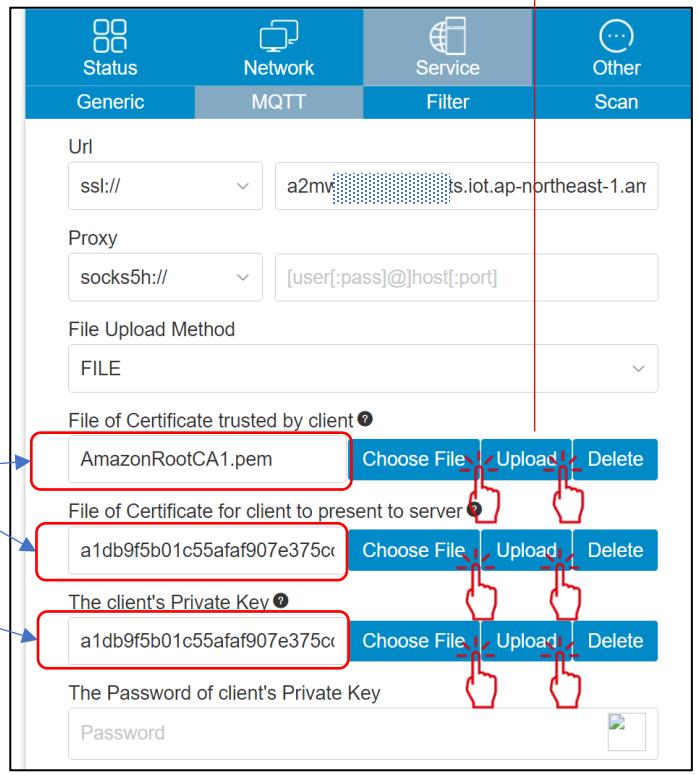


Fig.3B

3-6項 “MQTT With SSL Method”で説明している右図の2つの証明書と一つのキーファイルを指定し、それxぞれUploadします。

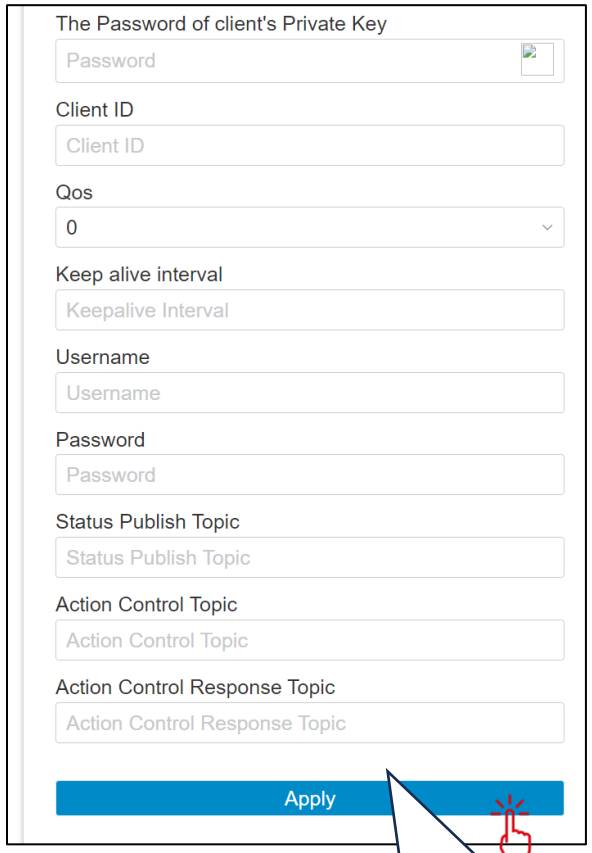


Fig.3C

最後に”Apply”をクリックします。
設定が正しく完了していれば、G1ゲートウェイは
AWSにデータのアップロードを開始します。
2-6項 ”ログデータの確認”に従って定期的にアップ
ロードされるデータを確認してください。

項目名	説明
Client ID	MQTT プロトコルによって定義されるクライアント ID は、クライアントの ID です。 デフォルト: ${gatewayMAC} ${gatewayMAC} は、ゲートウェイの MAC の 16 進数の小文字形式です（例: aabbcdeeff）
Qos	MQTT プロトコルによって定義される QoS レベル。 QoS=0:メッセージを失う可能性があり（デフォルト） QoS=1:メッセージの配信を保証しますが重複メッセージが存在する可能性がありQoS=2:メッセージが重複せずに 1 回だけ配信されることを保証
Keep alive interval	Keep Alive は秒単位の間隔です。送信するメッセージがない場合、クライアントは Keep Alive の値に従って定期的にハートビート メッセージをブローカーに送信し、ブローカーが接続を切断しないようにします。
Username	MQTTプロトコルで定義されたユーザー名
Password	MQTTプロトコルで定義された暗号化プロトコルのパスワード
Status Publish Topic	データを収集して公開するためのトピック BLE データを公開するゲートウェイのトピック デフォルト: /gw/${gatewayMac}/status$ {gatewayMac}は、ゲートウェイのMACの16 進小文字形式です（/gw/aabbcddeeff/status など）。
Action Control Topic	制御コマンドメッセージのトピック これは、ゲートウェイが制御コマンドを受信するために使用されます。メッセージは JSON 形式です。現在、「restart」コマンドのみがサポートされています。デフォルト: /gw/${gatewayMac}/action${gatewayMac} は、ゲートウェイの Mac の 16 進数の小文字形式です（/gw/aabbcddeeff/action など）。
Action Control Response Topic	コマンドの応答を制御するトピック これはゲートウェイが制御コマンドに応答するために使用され、メッセージは JSON 形式です。デフォルト: /gw/${gatewayMac}/response。${gatewayMac} は、ゲートウェイの Mac の 16 進数の小文字形式です（/gw/aabbcddeeff/response など）。

3-7 Wi-Fi アクセスポイントに接続

下記の手順でG1 ゲートウェイのWi-Fiアクセスポイントへの接続を行います。
※アクセスポイントへの接続が完了するとスマホとの接続は切断されアプリからはログアウト状態になります。

Wirelessを選択

Available Access Pointの一覧より接続するアクセスポイントを選択

Fig.3D

アクセスポイントのキーを入力

Fig.3E

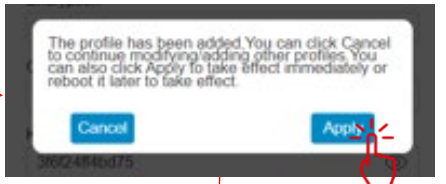


Fig.3F

Fig.3G

“Save Profile”をリックします。
上記の確認メッセージが表示されます。それぞれ”Apply”、“OK”をクリックします。
G1ゲートウェイはWindowsPCとの接続切って、アクスポイントの接続に移行します。

Fig.3H

● Wi-Fiアクセスポイント接続設定項目の説明

項目名	説明
Available Access Point	近傍にあるWi-FiアクセスポイントのSSIDを一覧表示
SSID	選択されたSSIDを表示
BSSID	G1 ゲートウェイが BSSID のみで AP を接続するように制限したい場合を除き、このパラメータをクリアしておいてください。
Encryption	使用する暗号方式を選択します
Cipher	Wireless Security 暗号化プロトコルで、通常デフォルト”auto”で利用します。
Key	選択したWi-Fiアクセスポイントの暗号化キー(パスワード)を設定します。
Proto	DHCPモード、スタティックモードのどちらを利用するか選択します。デフォルトはDHCPモードです。
Primary DNS Address	優先するDNSアドレス、デフォルトは”8.8.8.8”
Secondary DNS Address	代替DNSアドレス、デフォルトは”114.114.114.114”
Hidden property of ssid (failover)	SSIDに対応するHidden属性。 フェイルオーバー機能が有効な場合、Wi-Fiアクセスポイントの hidden プロパティを変更しないでください。 フェイルオーバー機能がWi-Fiアクセスポイントを見つけられない可能性があります。
Network checking (failover)	使用するIPアドレスまたはドメイン名 フェイルオーバーネットワーク 検出に使用する IPアドレス。 フェイルオーバー機能が有効になると、ゲートウェイはこの設定されたURL/IPを使用して、このIPにpingを送信するか、WEBページのURLに接続して、このホットスポットの接続信頼性を確認します。未設定のままでは、ルートをチェックする代わりに無線LAN接続のみをチェックします。

3-8 その他の設定項目

- LED Configuration

この6色LEDの点灯設定を行います。

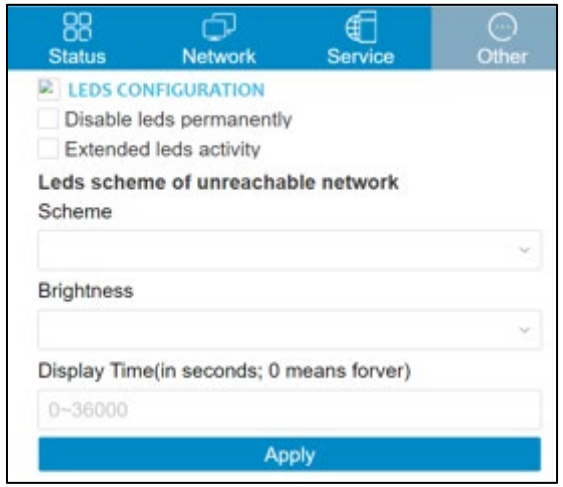


Fig.3I

項目名	説明
Disable leds permanently	チェックを入れるとLEDは消灯します。 ゲートウェイシステムがオンになったときのみ点灯する。システムが完全に起動した後に消灯する。 デフォルトが外された状態で、LEDを点灯します。
Extended leds activity	チェックを入れるとLEDは長時間点灯します。デフォルトが外された状態で、1分間遅れて消灯します。但し、G1 ゲートウェイがサーバに接続できない場合はカラーLEDトは常に点灯し、回転します。 注:”Disable leds permanently” がチェックされている場合、このフィールドは無効です。
Scheme	G1ゲートウェイがサーバに接続されていない場合、利用可能な配色は次のとおりです。 カラーLED配色:6色LEDローテーション、レッド、イエロー、ホワイト 黄色、白色
Brightness	カラーLEDの明るさは1～25に設定され、25が最も明るい。
Display Time （in seconds, 0 means forever）	点灯時間を秒単位で設定します。0をセットすると点灯したままの状態になります。

Time Configuration

1. Synchronization Using NTP Server

タイムゾーンとNTPサーバアドレスの両方を設定できます。ウェブページの「その他」の時間設定欄で「タイムゾーン(デフォルトはUTC)とNTPサーバ(デフォルトはopenwrtのntpサーバ)を設定できます。openwrtのntpサーバ)を設定します。入力後、”Apply ”ボタンをクリックして設定を完了します。設定完了です。すぐに有効になります。

デフォルトのUTCタイムゾーンは0タイムゾーンです。
タイムゾーンが東のタイムゾーンにある場合、UTCタイムゾーン番号を設定することができます。例えば、UTC-8に設定すると、東8ゾーンのタイムゾーンになります。
タイムゾーンが西のタイムゾーンに設定できる場合は、UTC+タイムゾーン番号に設定できます。例えば、UTC+8に設定すると、西8ゾーンのタイムゾーンになります。
Sync interval サーバとの時刻同期間隔を示します。例えば60に設定すると、サーバとの時刻同期が1分ごとに自動的に行われます。

タイムゾーンの詳細設定については、
https://wiki.openwrt.org/doc/uci/system
をご覧ください。

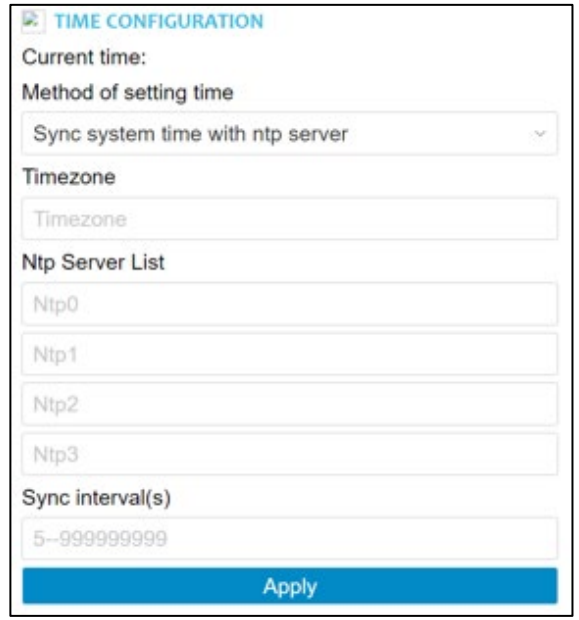


Fig.3J

2. Manual Time Setting

G1 ゲートウェイシステムの時間を手動で設定するには、[Apply with host time]ボタン、もしくは[Apply]ボタンをクリックします。
現在の時刻はゲートウェイシステムの時刻を表示します。
[Apply with host time]をクリックすると、ゲートウェイはブラウザがあるホストの時刻を積極的に取得し、ゲートウェイに時刻を同期します。
[Apply with host time]をクリックする前に、[Timezone]パラメーターはブラウザがあるホストのタイムゾーンと同じタイムゾーンでなければなりません。
[Apply]をクリックすると、ゲートウェイはゲートウェイに取得された時刻の時刻をゲートウェイに同期します。

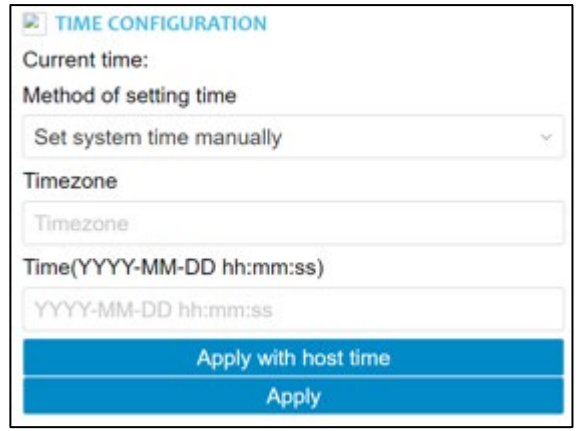


Fig.3K

● Automatic Management

[Automatic Management]機能は、[Automatic Reboot]（自動再起動）と[Timing Reboot]（タイミング再起動）に分けられる。

1. Automatic Reboot
デフォルトでは、Automatic Reboot機能は無効です。
サーバとの安定した接続中に、ゲートウェイがサーバから一定時間以上切断された場合（切断がサーバまたはゲートウェイに起因する場合）、ゲートウェイは[Watch Dog Timeout]で指定された時間が経過すると自動的に再起動します。
ゲートウェイが再起動された後、サーバと接続されていない場合、ゲートウェイは再度再起動されません。自動的な再起動は、途中で切断されている間にのみ行われます。

2. Timing Reboot
デフォルトでは、Timing Reboot機能は無効です。
この機能を有効にすると、ゲートウェイは指定された時刻に再起動します（この時刻で使用されるタイムゾーンは、以前のタイムコンフィギュレーションのタイムゾーンです）。

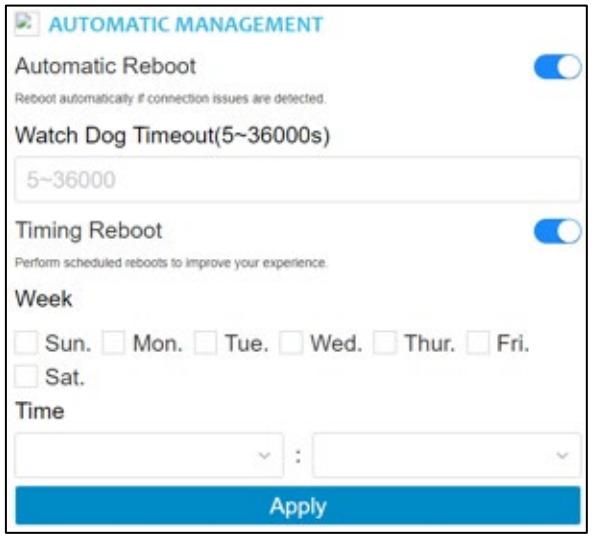


Fig.3L

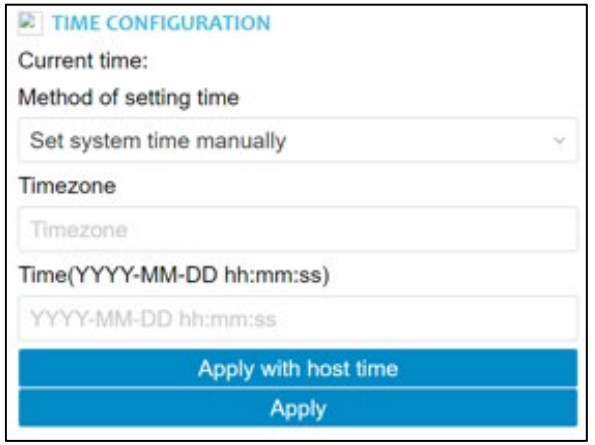


Fig.3M

● Firmware Upgrade

G1 ゲートウェイはWi-Fiモジュールと BLEモジュールで構成されているため、G1 ゲートウェイのアップグレードには、Wi-Fiファームウェアと BLEファームウェアが含まれるです。
アップグレードプロセスでは、まずBLEファームウェアをアップグレードし、次にWi-Fiファームウェアをアップグレードすることを推奨します。
ファームウェアのバージョンが異なると、機能の調整やアップグレードに対応し、必要に応じて選択できます。
詳細については、次の図を参照してください：。

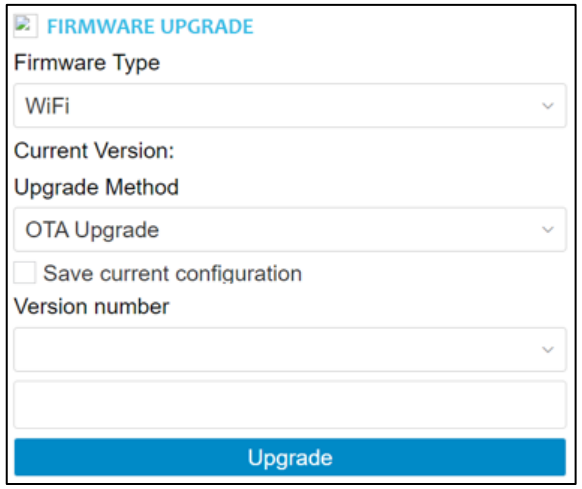


Fig.3N

● Troubleshooting

G1 ゲートウェイのネットワーク・コンフィギュレーションが正常かどうかを確認するには、pingコマンドと traceroute コマンドを使います。
ping コマンドはネットワークがブロックされていないかどうかを確認するための一般的なコマンドです。
tracerouteコマンドは、データパケットが宛先アドレスに到達するまでに通過したルーター tracerouteコマンドは、データ・パケットが宛先アドレスに到達するまでに通過したルーターを表示し、問題のあるノードを特定することができます。
この2つは この2つはよく一緒に使われます。

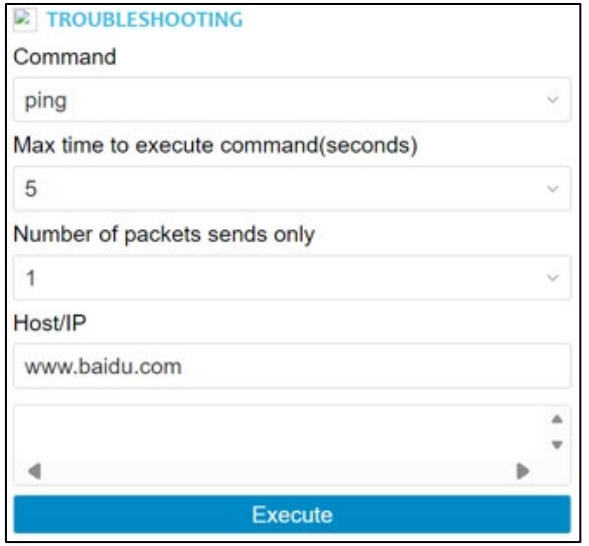


Fig.3P

1, Ping command

Pingは、指定されたターゲット・アドレスにアクセスできるかどうかを判断し、ゲートウェイ・ネットワークに障害がないかどうかを検出するために使用され

2. Traceroute command

tracerouteは、宛先アドレスへのデータパケットのルーティング状態をチェックし、問題のあるノードを特定することができる。

項目名	説明
Max time to execute command	コマンド最大実行時間の設定(5-120)、単位は秒、デフォルトは5秒
Number of packets sends only	送信パケット数(1～50)、デフォルトは1
Host/IP	ターゲットのホストまたはアドレス、デフォルトは www.baidu.com

3. Reboot the gateway
G1 ゲートウェイをリブートします。

4. Factory reset
G1 ゲートウェイに設定された内容を全てクリアして工場出荷値状態に戻します。

Fig.3Q

4-1 製品仕様

- 基本仕様

項目	仕様値
色	白色
重量	155g
付属品	USB ケーブル 1本、金属プレートと両面テープ 2セット、ネジ 2本と貼付シート
電源電圧	DC 5.0V(±5%),1A / 最大5.5V
動作温度範囲	-25～65℃
動作湿度範囲	Max.95%RH 但し、結露しないこと
保存温度範囲	-40～85℃
保存湿度範囲	Max.95%RH 但し、結露しないこと
工事設計認証番号	R 210-206999

- 外形寸法

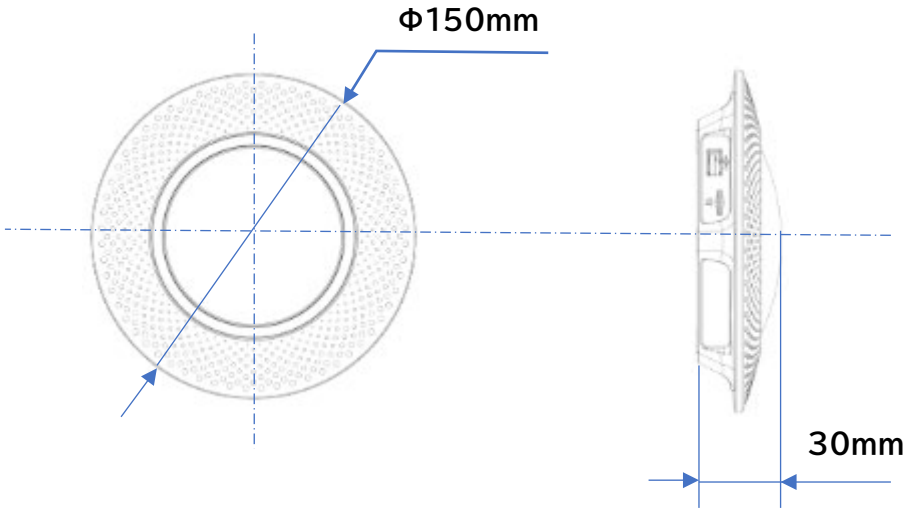


Fig.3R

● **Bluetooth RF 特性**

項目		仕様値
Bluetooth	準拠規格	Bluetooth 4.0
	周波数	2.4～2.4835GHz
	変調方式	GPSK
	送出電力	+4dBm
	受信感度	-108 dBm @ 1Mbps, 0.1 %BER
	Scan 処理能力	約400 パケット/秒
	到達レンジ	半径 約 300 m（見通し）

● **Wi-Fi RF 特性**

項目		仕様値
Wi-Fi	プロトコル	IEEE 802.11b/g/n
	周波数	2.4～2.4835GHz
	送出電力	typ.17dBm @802.11b typ.11.3dBm @802.11g typ.8.2dBm @802.11n
	データ送信速度	Up to 300Mbps @802.11b Up to 54Mbps @802.11g Up to 11Mbps @802.11n
	送信速度	2T2R 300Mbps
	最低受信入力レベル	-87dBm(typ. with PER <8%@11Mbps) -70dBm(typ. with PER <10%@54Mbps) -70dBm(typ. with PER <8%@MCS7)
	受信感度	270M -61dBm@10%PER 135M -65dBm@10%PER 108M -68dBm@10%PER 54M -68dBm@10%PER 11M -85dBm@10%PER 6M -85dBm@10%PER 1M -61dBm@10%PER
	変調方式	DBSK,DQPSK,CCK and OFDM (BPSK/QPSK/16-QAM/64-QAM)
	ネットワークプロトコル	HTTP(SSL/TLS)/MQTT(SSL/TLS and Proxy)/TCP
	セキュリティモード	WPA-PSK/WPA2-PSK,WPA-EAP/WPA2-EAP and TKIP

4-2 BLEアドバタイズ対応製品

当社のBLEアドバタイズ対応製品は下記になります。アドバタイズデータフォーマット仕様は下記のURLよりダウンロードすることができます。

BLEアドバタイズ対応製品	モデル番号	URL
Bluetooth 環境センサー	RS-BTEVS1	https://www.ratocsystems.com/products/sensor/airco2/rsbtevs1/
デジタル時計搭載スマート温湿度計	RS-BTTHM1	https://www.ratocsystems.com/products/sensor/thermo/rs-btthm1/
Bluetoothワットチェッカー	RS-BTWATTCH2	https://www.ratocsystems.com/products/sensor/watt/rsbtwattch2/
Bluetooth 開閉センサー	RS-BTDS1	https://www.ratocsystems.com/products/remocon/remowifi/rs-btds1/
スマートボタン	RS-SCBTN2	https://www.ratocsystems.com/products/remocon/remowifi/smaliaop/rs-scbtn/