

iGS03 ユーザーガイド

Ver 1.3

レンジャーシステムズ株式会社

RANGER 




改版履歴

改訂日	版数	変更箇所	変更内容
2020/06/30	初版	-	新規作成
2021/11/22	Ver1.1	P3	注意事項を追加
2023/7/26	Ver1.3	P10	LEDの種類>Network Status LED>点灯の文言を修正





monoコネクト機器を安全にお使いいただくために

- 使用者や他の人々への危害や財産への損害を防ぎ、安全にお使いいただくために、下記の内容を必ずお読みになり、ご理解のうえ、本製品をお使いください。






• 使用している表示と絵記号の意味

 警告	絶対に行ってはいけない事を記載しています。 この表示の内容を守らないと、使用者が死亡、重症を負う可能性があります。
 注意	この表示の内容を守らないと、使用者がけがをしたり、物的損害の可能性があります。
	してはいけない事項(禁止事項)を示します。




警告

	濡れた手で、電源プラグ部分(ACアダプタ)、コネクタ部分に触れないでください。 感電の恐れがあります。
	電源プラグ部分(ACアダプタ)、コネクタ部分が水に濡れたり、結露しないようにしてください。 感電や漏電の恐れがあります。
	煙が出たり変な臭いがしたら、コンセントから電源プラグ(ACアダプタ)を抜き、使用をおやめください。
	本製品を分解したり、改造、修理をしないでください。 カバーを取り外した場合保証の対象外となります。

注意

	本製品を落としたり、叩いたり、強い衝撃を与えないでください。 故障の原因になります。
	本製品の上に物を置かないでください。 動作不良や故障の原因になります。
	本製品をシンナーやベンジン等の有機溶剤で拭かないでください。
	本製品の電源プラグ部分(ACアダプタ)のホコリ等は取り除いてください。火災や故障の原因となります。
	本製品(防水対応製品以外)を雨や雪で濡れる場所で使用しないでください。 また、直射日光が当たる場所で使用しないでください。

その他

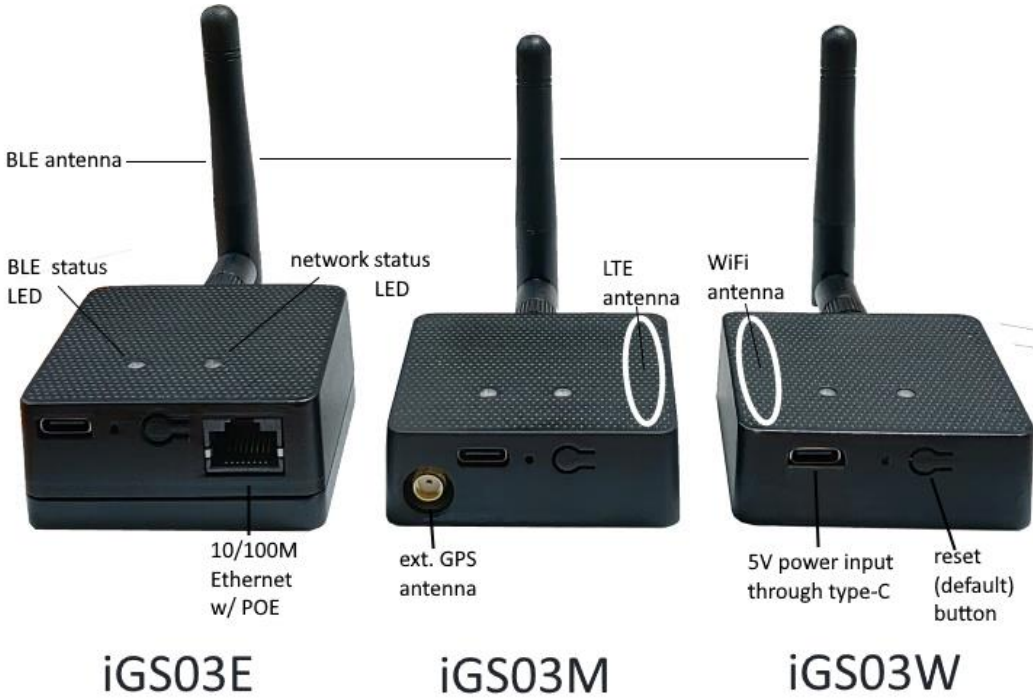
	本製品の動作環境をご確認の上、適切な環境でご利用ください。
	携帯電話の電波が入らない場所など、電波状況の著しく悪い環境でのご利用はできません。(LTE対応製品)
	多くのBLE機器がある場所など、電波状況の悪い環境では、正常に信号を受信できない場合がありますのでご注意ください。

概要

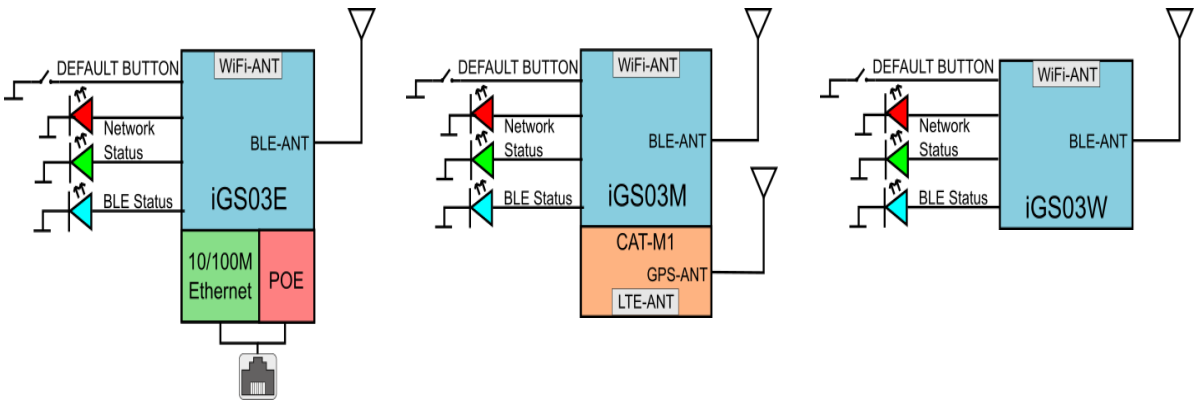
モデル

iGS03では、3つのモデルを採用しています。

- ① iGS03E (Ethernet通信を利用してデータを送信するモデル)
- ② iGS03M (LTE-M通信を利用してデータを送信するモデル)
- ③ iGS03W (Wi-Fi通信を利用してデータを送信するモデル)



ブロック図





概要

SIMカード

iGS03M(LTE-Mモデル)を使用するには、製品本体のカバーを開いて、Cat-M1マイクロSIMカードをソケットに挿入してください。



Step 1. Remove external BLE antenna	Step 2. Remove the screw from bottom cover
	
Step 3. Use finger to press and hold the arrow part	Step 4. Pull out the bottom cover
	

Wi-Fi 機能

iGS03は、DHCPをサポートするWi-Fiアクセスポイント(AP)として機能します。

この際、2.4GのWi-Fi通信を使用しています。

iGS03を設定する場合には、APに接続し、設定を行う必要があります。

※iGS03Eには含まれていません。

BLE

BLEサブシステムはリスニングモードで動作します。
BLEデバイスによってアドバタイズされたデータを収集します。
これらのデータはユーザーが設定したクラウドサーバなどに送信されま
す。

iGS03は2つのBLEモードをサポートしています。

①1M Phy

100%デューティサイクルで、BLE4.2 (regacy) / BLE 5 を含みます。

②Coded Phy

100%デューティサイクルのBLE 5 long range

ユーザーは次のコマンドを使用してBLEのモードを変更できます。
※telnetコンソールでのみ変更可能。

BLE PHYMODE X

Xの箇所は、設定値が入ります。

1 : 1M Phy

2 : Coded Phy

デフォルトの設定は、「1 : 1M Phy」となっています。

概要

GPS (※iGS03Mでサポート)

※ご利用には、別途GSPアンテナの購入が必要となります。

GPS機能はデフォルトでオフに設定されています。

ユーザーは下記のコマンドでGPSの動作を管理することができます。

コマンド	説明	デフォルト値
GPS ENABLE	GPS設定の有効化/無効化	OFF
GPS FIXCOUNT	測位の試行回数。0は連続測位を示しています。	0
GPS FIXRATE	1回目と2回目の測位の間隔時間	600(10min)
GPS INFO	最新のGPSステータスを取得します。	-

下記の様なケースでも使用できます。

Case. 1 : デバイスが定位置にある場合

```
GPS ENABLE 1  
GPS FIXCOUNT 5  
GPS FIXRATE 60
```

GPSが有効となり、60秒間隔で5回の位置情報を取得します。
GPSは位置を5回取得すると自動的にオフになります。

Case. 2 : デバイスが移動している場合

```
GPS ENABLE 1  
GPS FIXCOUNT 0  
GPS FIXRATE 600
```

GPSは有効となり、600秒間隔で継続的に位置情報を取得します。

ペイロードフォーマット

BLE

iGS03がサーバーに送信するペイロードフォーマットには6つの種類があります。

送信されるフォーマットは下記です。

`$<report type>,<tag id>,<gateway id>,<rssi>,<raw packet content>,*<unix epoch timestamp>¥r¥n`

項目名	説明
report type	レポート元を区別するためのタイプ
tag id	タグ/ビーコンのMACアドレス または ID
gateway id	ゲートウェイのMACアドレス
rssi	タグ/ビーコンのRSSI
raw packet content	ゲートウェイが受信した生パケットデータ
unix epoch timestamp	オプションで設定可能なタイムスタンプ

レポート形式には下記の種類があります。

\$GPRP BLE4.2 General Purpose Report
\$SRRP BLE4.2 Scan Response Report
\$LRAD BLE5 Long Range ADV
\$LRSR BLE 5 Long Range Scan Response
\$1MAD BLE 5 1M ADV
\$1MSR BLE 5 1M Scan Response

データ例)

```
$GPRP,CCB97E7361A4,CB412F0C8EDC,-49  
,1309696773206D65736820233220285445535429020106,1574921085
```

```
$GPRP,E5A706E3923A,CB412F0C8EDC,-87  
,0201041AFF590002150112233445566778899AABBCCDDEEFF0000100C3BB,1574921085
```

```
$LRAD,51A88AD374B7,CC4B73906F96,-87  
,02010212FF0D0083BC280100AAAAFFFF000010030000,1574921085
```


ペイロード フォーマット

GPS (※iGS03Mでサポート)

※ご利用には、別途GSPアンテナの購入が必要となります。

送信されるフォーマットは下記です。

```
$GPSR,<tag_mac>,<reader_mac>,<rsi>,yymmdd,hhmmss.ss,latitude,  
longitude,speed,hdop(,timestamp)¥r¥n
```

「\$GPSR,<tag_mac>,<reader_mac>,<rsi>」項目は、他のレポート形式との互換性の為にあります。

\$GPSRの場合、<tag_mac>は<reader_mac>と同じになります。また、<rsi>は常に-127です。

「yymmdd、hhmmss.ss」は、位置を取得するときのUTCの時間です。

それ以外の項目の説明は下記のとおりです。

項目名	説明
speed	スピードを表します。(単位：ノット)
hdop	位置の水平希釈を表します。

データ例)

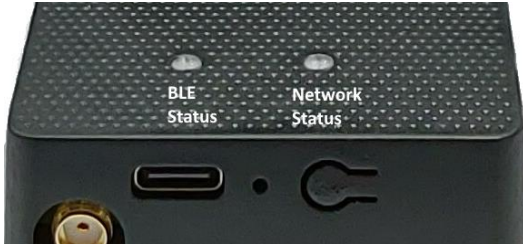
```
$GPSR,CC4B73906F96,CC4B73906F96,-127,191127,233821.00,24.993631,121.423264,0.0,2.4,1574897900
```

入力と出力について

LEDの意味について

下図に示すように、現在のステータスを2つのLEDで表しています。

左側のLED：BLEステータス
右側のLED：ネットワークステータス



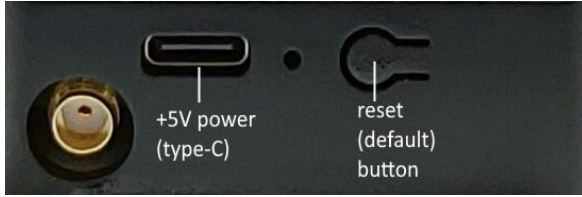
LEDの意味は、下記の表の通りです。

LEDの種類	点灯	点滅
BLE Status LED	範囲内のタグ/ビーコンを確認中	BLEデータ送信中
Network Status LED	Wi-Fi/Ethernet/LTE-M通信の接続成功及びサーバー接続成功 (ネットワークの接続またはサーバーからの応答がエラーの場合は赤色LEDが点灯します。)	緑： Wi-Fi/Ethernet/LTE-M通信が発生しています。 オレンジ： デバイス起動中

入力と出力について

リセット(デフォルト)ボタン

下図に示すように、iGS03の背面には、リセットボタンがあります。



工場出荷時の設定に戻す必要がある場合は、デバイスのモードに関係なく、リセットボタンを5秒以上押し続けます。

そうすると、ネットワークステータスを表すLEDがオフになり、ボタンを離すとiGS03が再起動して、工場出荷時の設定に戻すことが可能です。

OTA

リセットボタンは無線(Over-The-Air : OTA)ファームウェアのアップデートとしても使用できます。

このファームウェアのアップデートはWi-Fiインターフェイスを介してのみ行うことができます。

OTAを使用するには、このボタンを押してから電源を入れ、ネットワークステータスのLEDが点滅するまで押し続けます。

提供するファームウェアは最新のものをご提供しています。

重大な不具合がない場合は、ファームウェアのアップデートは必要ありません。

また、ファームウェアのバイナリファイルの提供も例外を除いてはお断りしております。

設定方法について

iGS03を設定するには、Wi-Fiでデバイスに接続する必要があります。
電源がオンになると、アクセスポイントとして、タブレットやスマートフォン、またはパソコンから接続できます。

iGS03Mでは、下記のようなSSIDとして表示されます。



※上記の6F_46は、デバイスの裏面に書いてあるMACアドレスの下4桁です。

SSIDに接続する際のデフォルトのキーは「**12345678**」です。
※このキーについては、後程ログインするWeb UIから変更できます。

Wi-Fi接続後、Webブラウザを開き、アドレスバーに下記を入力し接続します
「**192.168.10.1**」

※推奨Webブラウザ : Google Chrome

アクセス後、ユーザー名/パスワードの入力を求められる場合があります。
※ユーザー名/パスワードはどちらも「**admin**」です。
※パスワードは後で変更が可能です。

Web UIで設定変更を実施した場合、タブ毎に保存する必要があります。

保存する際は、画面に表示されているSaveボタン()を押してください。

また、すべての変更を行ったら設定を反映させるために再起動が必要になります。

再起動が必要な場合は、下記のメッセージバーが表示されるので、「REBOOT」をクリックしてください。

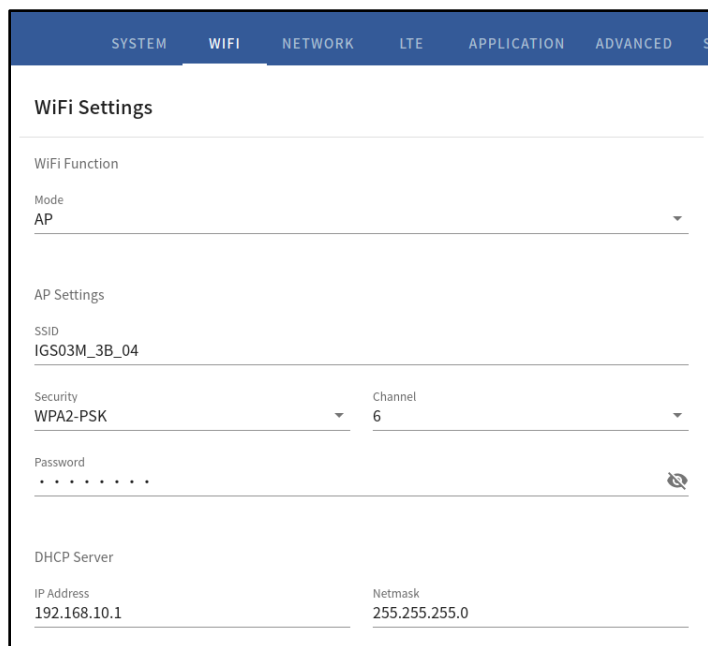
Require reboot for the changes to take effect.

REBOOT

次ページ以降で、Web UI画面の詳細について説明します。

Web ユーザーインターフェース(UI)について

Web UIにログイン後、下記の様なページが表示されます。



SYSTEM	WIFI	NETWORK	LTE	APPLICATION	ADVANCED	S
WiFi Settings						
WiFi Function						
Mode AP						
AP Settings						
SSID IGS03M_3B_04						
Security WPA2-PSK						
Channel 6						
Password						
DHCP Server						
IP Address 192.168.10.1						
Netmask 255.255.255.0						

SYSTEMタブ

ステーションモードでのMACアドレスと、IPアドレスを含むファームウェアとデバイスの情報が表示されます。

Wi-Fiタブ

ユーザーはAPに接続してiGS03を設定できます。
モードには2種類あり、①APモードと②Stationモードと呼ばれます。

次ページから各モードについて説明致します。

Web ユーザーインターフェース(UI)について

①APモード

APモードで表示される項目は下記の通りです。

項目名	項目の説明
SSID	デフォルト名はIGS03とMACアドレスの下4桁の数字です。
Security	オープン、WPA-PSK、WPA2-PSKおよびWPA-PSK / WPA2-PSKがサポートされています。WPA2-PSKを推奨しています。
Password	8～63文字が入力可能です。
Channel	1～11 (ch12およびch13は要望によってはサポート可能)
DHCP Server	WiFi APモードでのiGS03のデフォルトIPアドレスは192.168.10.1で、ネットマスクは255.255.255です。 ユーザーがAPモードでIPアドレスを変更する場合は、ここでIPとネットマスクを設定するだけです。 対応するDHCPクライアントアドレスも変更されます。 たとえば、DHCPサーバーのIPアドレスが192.168.0.1に変更された場合、iGS03 APに関連付けられているDHCPクライアントは192.18.0.Xになります。

②Stationモード

Stationモードは、Wi-Fiバージョンで使用します。
Stationモードで表示される項目は下記の通りです。

項目名	項目の説明
Scan	クリックして利用可能なAPをスキャンします。 スキャン結果がポップアップウィンドウに表示され、ユーザーはリストから正しいAPを選択できます。
SSID	手動入力はありません。ユーザーがスキャンリストからAPを選択すると、自動的に入力されます。
Security	基本的に、スキャンリストからAPを選択すると、自動的に検出および選択されます。ただし、AP設定がWEPオープンまたはWEP共有になっている場合は、ユーザーが自分で確認する必要があります。
Password	APに割り当てられているものを入力します。

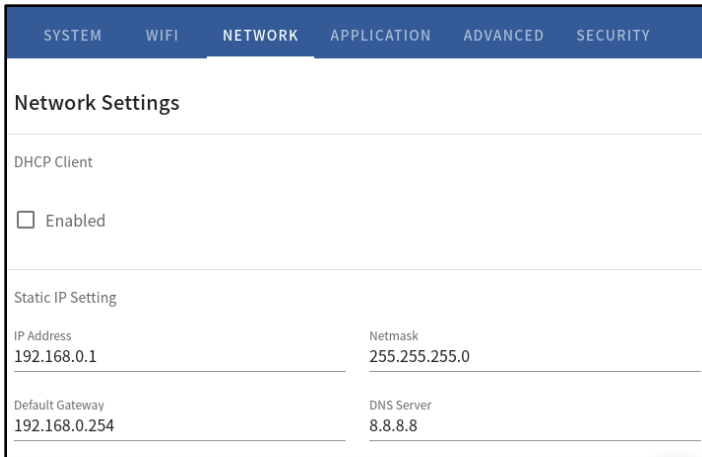
Web ユーザーインターフェース(UI)について

Networkタブ

この設定は主にWiFiステーションモードで構成するためのものです。通常、DHCPクライアントは、DHCPを使用してWiFi APに参加することができます。

iGS03のIPアドレスを手動で割り当てる場合は、DHCPクライアントを無効にする必要があります。

無効にしたら、ユーザーはIP、ネットマスク、ゲートウェイ、DNSサーバーを割り当てる必要があります。



SYSTEM	WIFI	NETWORK	APPLICATION	ADVANCED	SECURITY
Network Settings					
DHCP Client					
<input type="checkbox"/> Enabled					
Static IP Setting					
IP Address		Netmask			
192.168.0.1		255.255.255.0			
Default Gateway			DNS Server		
192.168.0.254			8.8.8.8		

Applicationタブ

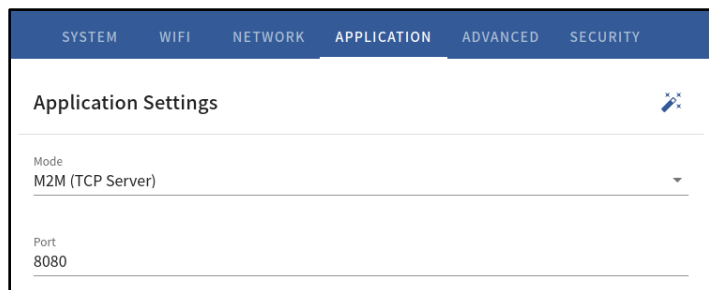
Applicationタブでは4つのモードを設定可能です。

- ① TCP Server
- ② TCP Client
- ③ HTTP Client
- ④ MQTT Client



Web ユーザーインターフェース(UI)について

① TCP Server

このモードは主にテスト用です。ユーザーは、WiFiインターフェイスを介してTCPサーバーに接続することで、受信したデータをすぐに確認できます。

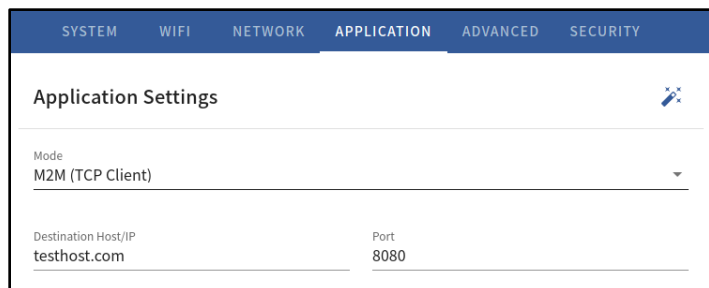


The screenshot shows the 'Application Settings' page in the 'APPLICATION' tab. The 'Mode' dropdown is set to 'M2M (TCP Server)' and the 'Port' is set to '8080'. There is a pencil icon for editing settings.



SYSTEM	WIFI	NETWORK	APPLICATION	ADVANCED	SECURITY
Application Settings 					
Mode M2M (TCP Server) 					
Port 8080					

② TCP Client

iGS03は、TCPクライアントとして動作し、未加工のTCPサーバーと通信します。接続するTCPサーバーのアドレスとポート番号を入力します。



The screenshot shows the 'Application Settings' page in the 'APPLICATION' tab. The 'Mode' dropdown is set to 'M2M (TCP Client)'. The 'Destination Host/IP' is set to 'testhost.com' and the 'Port' is set to '8080'. There is a pencil icon for editing settings.

SYSTEM	WIFI	NETWORK	APPLICATION	ADVANCED	SECURITY
Application Settings 					
Mode M2M (TCP Client) 					
Destination Host/IP testhost.com			Port 8080		

Web ユーザーインターフェース(UI)について

③ HTTP Client

このシナリオでは、BLEデータをゲートウェイ経由でHTTPサーバーに送信するために、HTTP URLを割り当てる必要があります。

一部のHTTPサーバーでは、ユーザー名とパスワードが必要な場合があります。

その場合は、追加のヘッダーと値を設定してください。

The screenshot shows the 'Application Settings' page for 'HTTP Client' mode. The 'Mode' dropdown is set to 'HTTP Client'. The 'Target URL' is 'http://testhost.com:8080/api/postdata'. There is an unchecked checkbox for 'Use Client Certificate' and a 'Server Root CA' dropdown set to 'No'. There are also fields for 'Extra Header' and 'Extra Header Value'.

The screenshot shows the 'Application Settings' page for 'MQTT Client' mode. The 'Mode' dropdown is set to 'MQTT Client'. The 'Target Host/IP' is 'testhost.com' and the 'Port' is '1883'. There is an unchecked checkbox for 'MQTT over TLS (MQTTS)'. The 'Publish Topic' is 'pub', the 'Client ID' is 'IGS03W_3B_04', and there are fields for 'Username' and 'Password'. There is also an unchecked checkbox for 'Use Client Certificate' and a 'Server Root CA' dropdown set to 'No'.

☆HTTPS通信

ユーザーは、URLでhttps://を使用してHTTPSを有効にできます。

また、サーバーの要件に基づいて、サーバールートCA /ユーザークライアント証明書も有効にすることもできます。

Web ユーザーインターフェース(UI)について

④ MQTT Client

この設定箇所では、MQTTホストアドレスとポート番号を割り当てる必要があります。

また、発行トピックを割り当てる必要があります。

クライアントIDは、デフォルトでMACアドレスの一部を持つゲートウェイ名として割り当てられますが、ユーザーも変更できます。

クライアントIDが設定されていない場合、システムはその乱数を生成します。ユーザー名とパスワードはオプションです。

☆MQTT通信

ユーザーはMQTTサポートを有効にできます。また、サーバーの要件に基づいて、サーバールートCA /クライアント証明書の使用を有効にすることもできます。

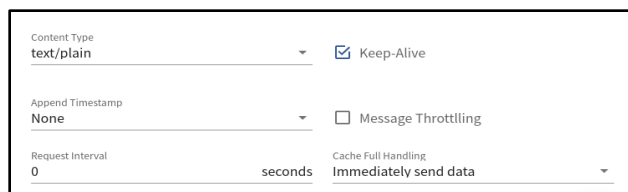
たとえば、AWS-IOTを有効にするには、ユーザーはMQTT / ROOT CA /証明書の使用オプションを有効にし、セキュリティページで証明書と秘密鍵をアップロードする必要があります。

Web ユーザーインターフェース(UI)について

共通設定

• Content Type

ユーザーは、プレーンテキスト形式またはJSON文字列のレポートデータを選択できます。



The screenshot shows a settings panel with four rows. The first row is 'Content Type' with a dropdown menu set to 'text/plain' and a checked checkbox for 'Keep-Alive'. The second row is 'Append Timestamp' with a dropdown menu set to 'None' and an unchecked checkbox for 'Message Throttling'. The third row is 'Request Interval' with a text input field containing '0' and a unit dropdown set to 'seconds'. The fourth row is 'Cache Full Handling' with a dropdown menu set to 'Immediately send data'.

• Keep Alive

このオプションは、HTTPおよびMQTTクライアントで使用できます。HTTPクライアントでは、デバイスはHTTP永続接続を送信して、既存のTCPセッションを再利用します。

これにより、HTTPの効率が向上します。

MQTTクライアントでは、デバイスはPINGREQパケットをブローカーに送信して、それが使用可能であることを確認し、ブローカーも引き続き使用可能であることを確認します。

• Append Timestamp

デバイスは、P7に記載されているように、BLEパッケージ形式でタイムスタンプ情報を追加します。

ユーザーは単位を秒またはミリ秒でを使用することを選択できます。

デバイスでNTP時刻同期が有効になっていないか、NTPサーバーに到達できない場合、レポートのタイムスタンプは予期しないものになります。

• Request Interval

データを送信先サーバーにアップロードするための要求間隔を割り当てることができます。

これは便利で、データ送信の回数を減らすことができます。

間隔を0に設定すると、データはすぐに送信されます。

秒単位でゼロ以外の値に設定すると、バッファがいっぱいになるか、時間間隔に達すると、データが送信されます。

• Throttle Control

ユーザーがスロットル制御を有効にすることを選択した場合、iGS03は各TAG /ビーコンIDの最後のレコードを指定された間隔（要求間隔）に保持します。

このようにして、HTTPサーバーへのアップロード接続を減らすことができます。

Web ユーザーインターフェース(UI)について

Advancedタブ

・ BLE設定

- BLE 5 PHY Mode

ユーザーは、オリジナルのBLE PHYまたはコード化PHT（ロングレンジモード）のどちらを使用するかを選択できます。

- Active Scan Mode

アクティブスキャンを有効にします。

・ BLE フィルタ設定

ユーザーはBLEフィルターを設定して、不要なBLE情報を除外できます。フィルターには2種類あります。

1つはBLE RSSI値によるもので、もう1つはパターン/マスクの組み合わせによるものです。

- RSSI Threshold

バーを-50dBmまで右に引くと、RSSIが-50dBm（たとえば-45dBm）以上のBLEタグ/ビーコンのみがサーバーに送信されます。

- Payload Whitelist

パターンを設定してホワイトリストを構成します。

デバイスは、いずれかのパターンに一致するBLEペイロードのみを報告します。

パターン内の文字「X」は無視を意味します。

ユーザーはペイロードフィルターの**6つ**のエントリを設定して、関係する情報のみが受信されるようにすることができます。

Payload Filter (Whitelist)		
ID	Payload Match Pattern	
1	0201061AFF4C00	×
2	020106XXFFXX008XBC	×

Web ユーザーインターフェース(UI)について

- BLE MAC Whitelist

BLE MACを設定してホワイトリストを構成します。

ユーザーは10個のMACを設定して、関係する情報のみが受信されるようにすることができます。

BLE MAC Whitelist		
ID	Beacon MAC Address	
1	F7:2E:90:9E:78:5F	X

SECURITYタブ

デバイスキー/認証/サーバーCAのアップロード
ユーザーはここで証明書とキーをアップロードできます。
これはMQTTおよびHTTPSで使用されます。

LTEタブ

LTE設定では下記の項目が設定可能です。

- APN
→キャリアが設定しているAPN情報を記載してください、
- Auth
→キャリア設定に基づく認証タイプが可能。
- Username/Password
→キャリア設定に基づくユーザー名/パスワード。
- GNSS設定
→GNSS機能の有効化

NTP設定

NTP設定UIを開くには、UIヘッダーの「時計」アイコンをクリックします。
ユーザーは、NTPを有効にするためにタイムサーバーと更新期間を設定する
必要があります。

設定を保存して再起動し、設定を有効にします。

ご不明の点、ご相談は下記までお気軽にご連絡ください。

お問い合わせ先

レンジャーシステムズ株式会社
IoT事業部まで

TEL : 03-6257-1850

FAX : 03-6257-1855

E-Mail : mono-support@ranger-systems.co.jp