



Motion Gateway User Manual (MS01/Gateway)

MS01-UserD



株式会社 SyncWave

目次

目次	2
1. 安全上の注意	3
2. 機器構成	4
4. 起動前の準備	8
5. 初期設定(WebUI ログイン)	9
6. LTE	10
7. VPN	11
1. SSTP	11
2. IPSec	13
8. Acceleration/Gyroscope	15
1. Acceleration/Gyroscope 画面説明	15
2. Calibration 設定	16
3. Acceleration 設定	16
4. Gyroscope 設定	17
5. GPS	17
9. MQTT	18
10. Cloud Service	22
1. AWS に接続	22
2. Azure に接続	23
11. ソフトウェアアップデート	25
12. 改訂履歴	26
13. ご案内	27

1. 安全上の注意

本章では、安全上の注意について記載します。

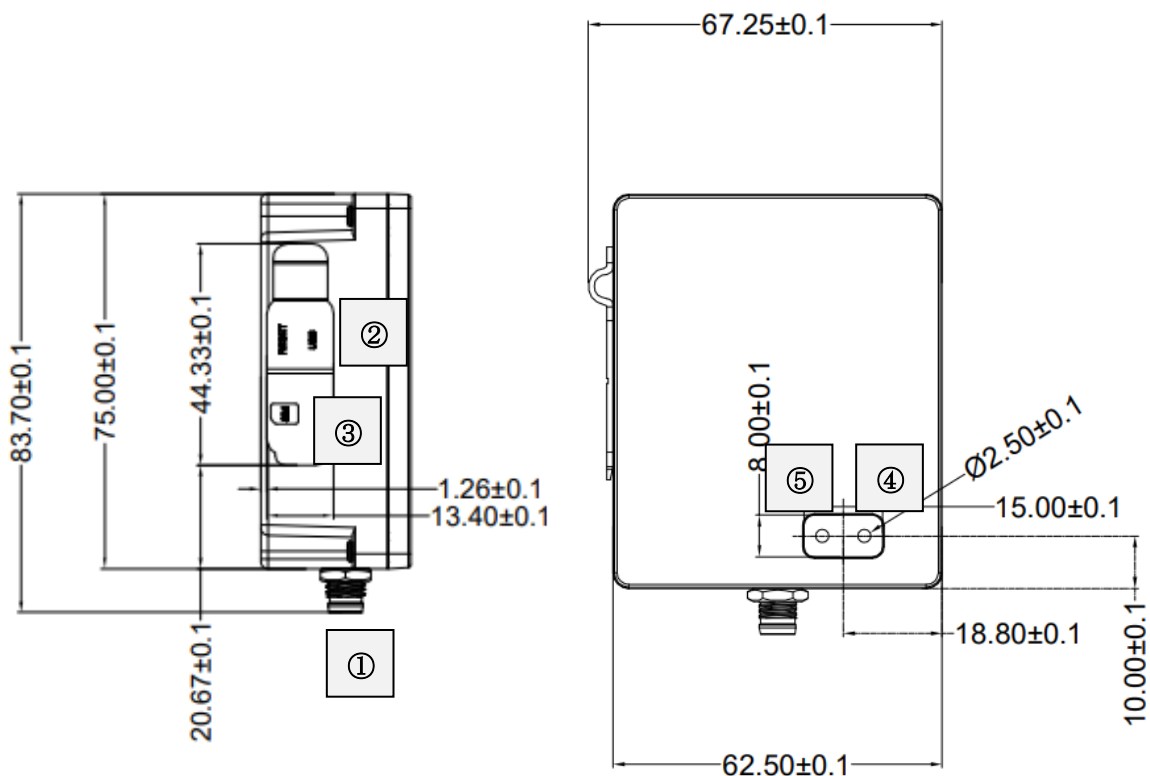
本製品を安全に使用するために、以下のことを守ってください。

- 本誌の記載内容を逸脱した方法で使用しないでください。
- 下記の環境では保管、設置、使用しないでください。
 - ・ 振動、衝撃の影響が大きい場所
 - ・ 不安定な場所
 - ・ 屋外や直射日光、風雨、水にさらされる場所
 - ・ 温湿度が仕様範囲外の場所
 - ・ 湿度変化が激しく、結露や氷結の恐れがある場所
 - ・ 電界及び磁界の影響を受ける場所
 - ・ 強い高周波ノイズやサージの影響を受ける場所
 - ・ 腐食性ガスや溶解性液体のある場所
- 放熱を妨げないよう、本製品の周辺をふさがしないでください。
- 発熱する機器と近接して取り付けしないでください。
- 火の中に投入したり、加熱したりしないでください。
- 分解、改造、修理をしないでください。
- 使用中に異音や異臭がする、煙がでる、過剰に発熱するなどの異常が起きた際は直ちに使用を中止してください。
- SIM カードの取り付けや取り外しを行う場合は必要以上の力を加えないでください。
- 本製品を廃棄する際は地方自治体の条例に従い正しい方法で廃棄してください。

2. 機器構成

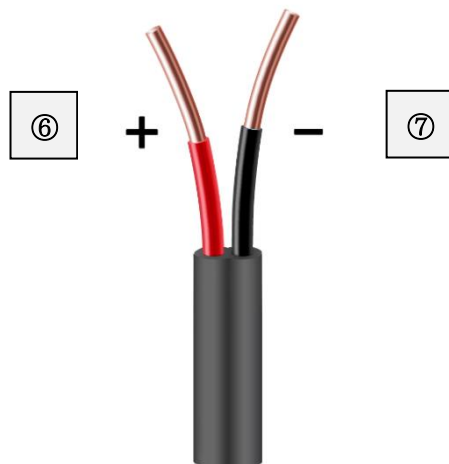
本章では、各部の名称と役割を記載します。

< 左側部 / 正面 >



名称	役割
① 電源ポート	電源ケーブル用の接続端子
② USB-C ポート	USB-Type-C を接続する端子
③ SIM スロット	nano SIM を挿入するスロット
④ LED-LTE (cellular network)	緑点灯：LTE 接続済み 消灯：LTE 未接続 緑点滅：データ送受信中
⑤ LED-電源	緑点灯：電源 ON 消灯：電源 OFF 緑点滅：キャリブレーション処理中

< ケーブル部 >



名称	役割
⑥ 赤ケーブル	プラス側
⑦ 黒ケーブル	マイナス側

3. 製品仕様

本章では、製品仕様について記載します。

Basic Hardware

項目	内容
CPU	DualCore; ARM Cortex-A7 up to 1.2GHz; ARM Cortex-R5
RAM	128MB DDR2
Flash	256MB Nandflash

Cellular Interface

項目	内容
4G	LTE Category 4
SIM	nano SIM ×1
LTE Frequencies	1,3,8,18,19,41

GNSS Interface

項目	内容
Technology	GPS/BeiDou (Compass) /QZSS

3-axis Accelerometer

項目	内容
Full Scale Range	± 2g, ± 4g, ± 8g, ± 16g
Sensitivity	16384 LSB/g, 8192 LSB/g, 4096 LSB/g, 2048 LSB/g

3-axis Gyroscope

項目	内容
Full Scale Range	± 125dps, ± 250dps, ± 500dps, ± 1000dps, ± 2000dps
Sensitivity	262 LSB/dps, 131 LSB/dps, 65.5 LSB/dps, 32.8 LSB/dps, 16.4 LSB/dps

Others

項目	内容
USB	Type C for configuration
LED indicators	LTE (cellular network)

Software

項目	内容
OS	Linux OpenWRT
Local Configuration	USB (Type C)
Remote management	SurfView remote management system

Cloud Connection

項目	内容
Type	MQTT, AWS, Azure, Others

Power Supply and Consumption

項目	内容
Input voltage	9 ~ 36V
Typical voltage	12V/24V
Power consumption	Idle: 0.2W Average: 1.2W

Physical Characteristics

項目	内容
Dimensions	75×62×30mm
Weight	80g
Housing	Plastic
Waterproof and Dustproof class	IP65
Operating temperature	-30 ~ +70 °C
Storage temperature	-40 ~ +85 °C

Certification

項目	内容
Japan	Telec/Jate

Regulatory

項目	内容
Surge	ISO16750-2 P5A : $U_s:80V$ $R_i:4\Omega$ $T_d:200ms$ ISO7637-2 P5a : U_s125V , $R_i:8\Omega$, $T_d:100ms$
ESD	EN61000-4-2, Level3

4. 起動前の準備

本章では、起動前の準備について記載します。

- SIM カードの挿入

SIM カードを本製品ラベルに記載された向きで挿入する。

*SIM の挿入方向に注意してください。無理に挿入すると取り出せなくなる場合があります。

*電源 ON 後に SIM を挿入しても認識しません、必ず電源 OFF 時に挿入してください。

- 電源接続

本製品の端子に電源を供給する。

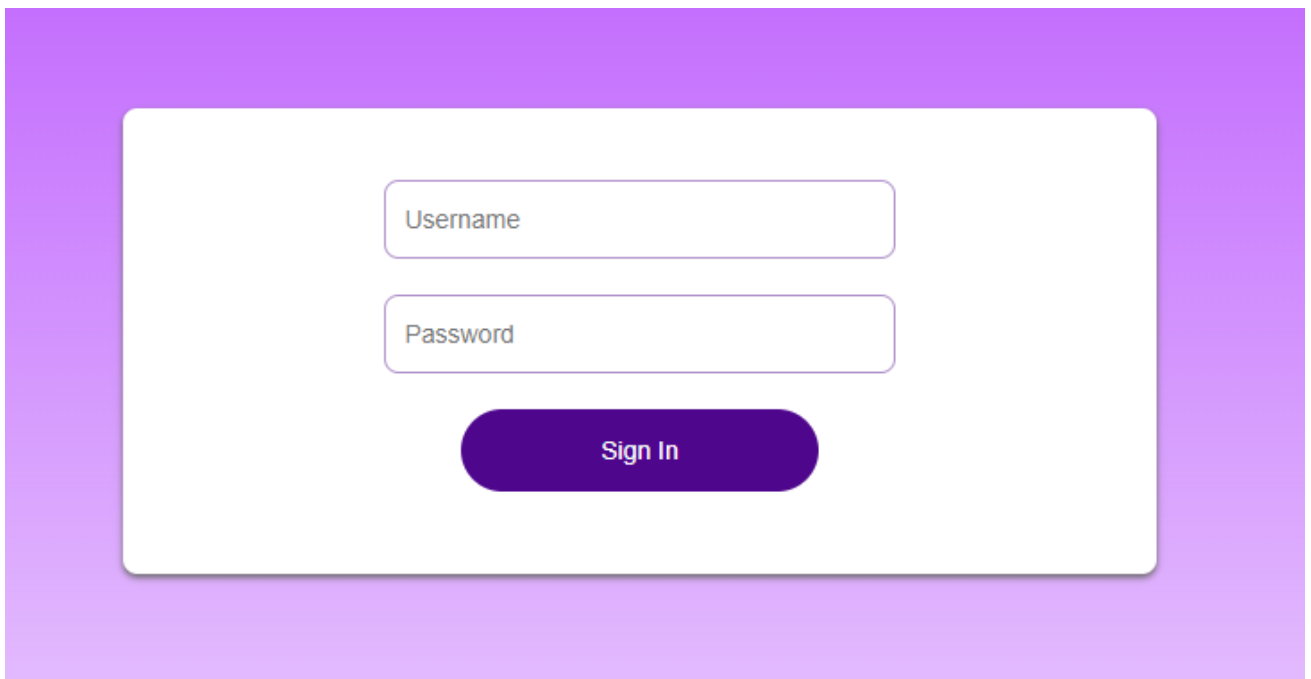
*電源供給を開始すると本体電源 ON となります。

*電源供給を停止すると本体電源 OFF となりますので、終了時は電源供給を停止してください。

5. 初期設定(WebUI ログイン)

本章では、WebUI へのログイン手順について記載します。

1. 本製品の SIM を挿入する。
*SIM の挿入方向に注意してください。
*電源 ON 後に SIM を挿入しても認識しません、必ず電源 OFF 時に挿入してください。
2. 本製品に電源供給を開始する。
3. パソコンを起動する。
4. 本製品の USB-C ポートとパソコンの USB ポートを USB ケーブルで接続する。
5. パソコン上で Web ブラウザを起動する。
6. アドレスバーに以下 URL を入力する。
192.168.1.1
7. ログイン画面が表示されるので以下のログイン情報を入力する。



>Username : admin

>Password : admin

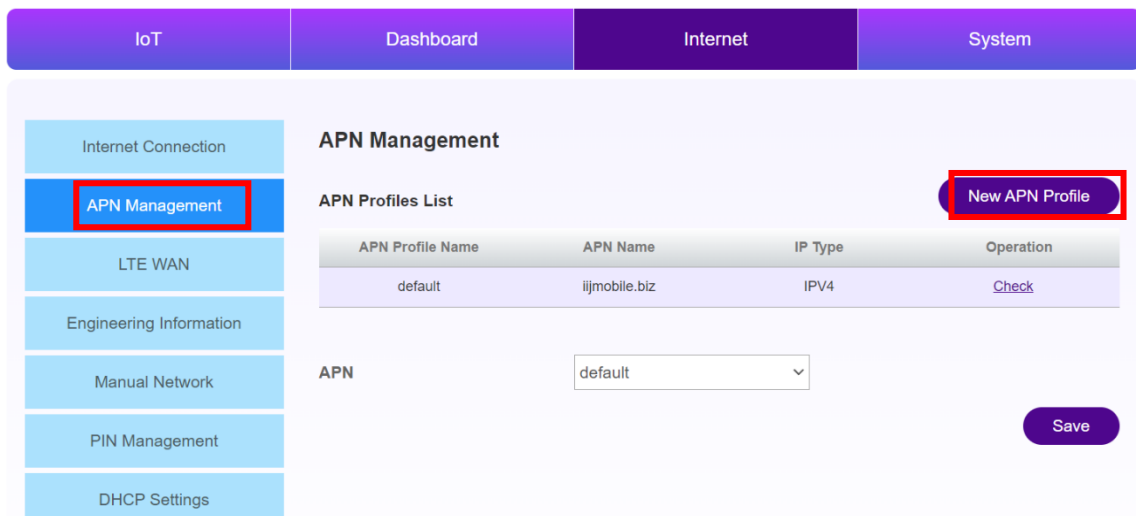
*本製品起動直後は表示に時間がかかる場合がありますので、繋がらない場合はしばらく置いてから再度接続してください。

8. ログインが完了しダッシュボードが表示される。

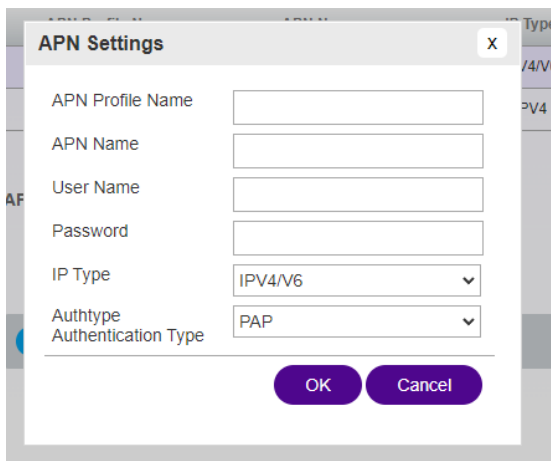
6. LTE (cellular network)

本章では、LTE 接続手順について記載します。

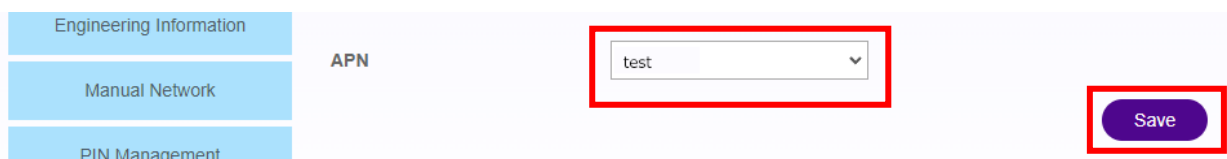
- 1.メインメニューより [Internet]を選択する。
- 2.サイドメニューより [APN Management]を選択する



- 3.[New APN Profile]を押下し、挿入されている SIM の APN 情報を設定する。



- 4.[OK]を選択する。
- 5.APN のドロップダウンメニューより作成した APN Profile を選択する。



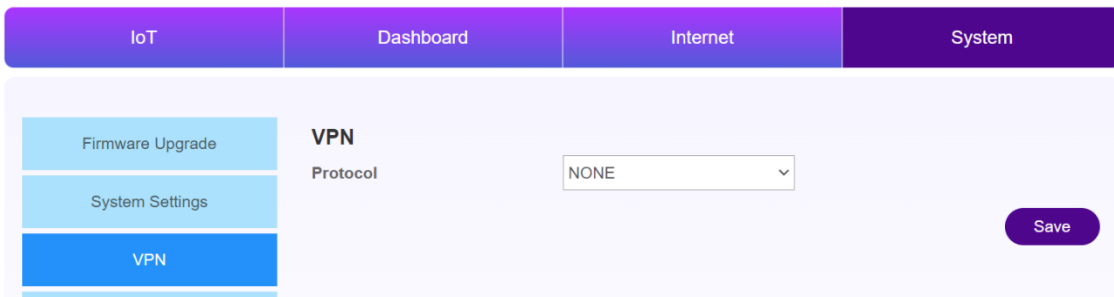
- 6.[Save]を押下する。

7. VPN

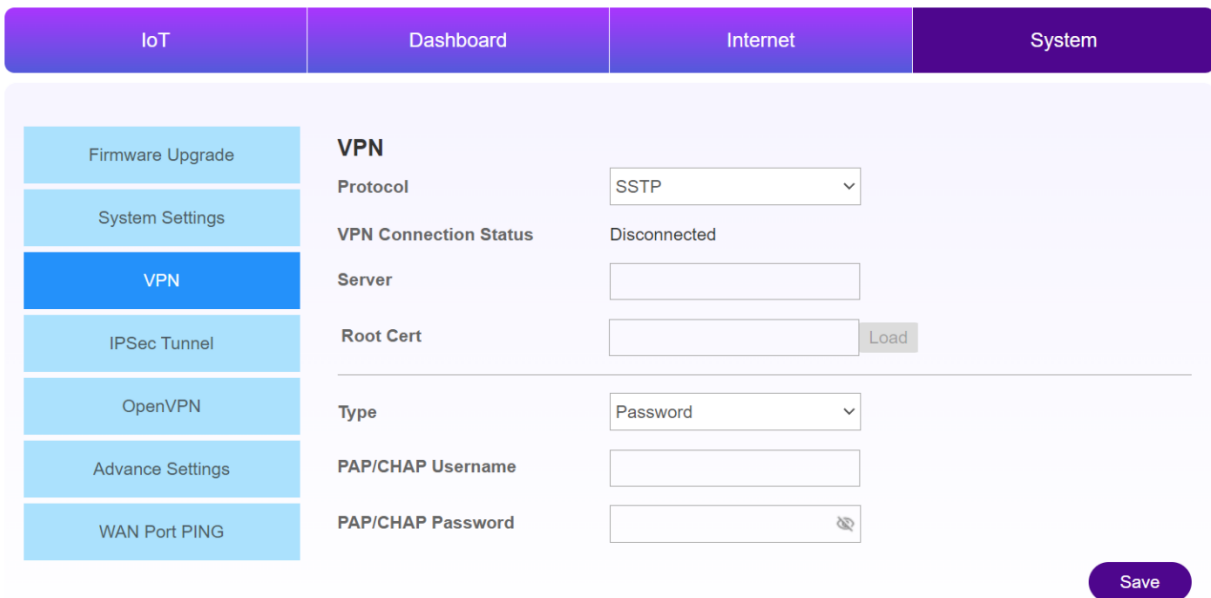
本章では、VPN 設定の手順を記載します。

1. SSTP

1. WebUI にログインし、メインメニューより [System] を選択する。
2. Protocol プルダウンメニューより SSTP を選択する。



3. Protocol プルダウンメニューより SSTP を選択する。
4. 以下を設定する。



-Server : 接続先 VPN サーバーアドレス

-Root Cert : 接続先 VPN の証明書を設定し[Load]を押下

-Type :

- Password : パスワード方式
- Certificates(TLS) : 証明書方式

- PAP/CHAP Username : (パスワード方式)ユーザネームを入力
- PAP/CHAP Password : (パスワード方式) パスワードを入力
- User certificate : (証明書方式)Certificate を設定し[Load]を押下
- User private key : (証明書方式)Private Key を選択し[Load]を押下

5. [Save]ボタンを押下する
6. VPN Connection Status が Connected になったら接続完了
7. WebUI のメニュー[Dashboard]を選択する。
8. VPN の部分に VPN 情報が表示されます。

The screenshot shows the WebUI Dashboard with the following components:

- Navigation Bar:** IoT, Dashboard (selected), Internet, System
- Connection Status:** A purple card with a cloud icon and a green toggle switch, indicating the VPN is connected.
- GPS:** A blue card with a location pin icon, showing Longitude: 0.000000 and Latitude: 0.000000.
- Network Settings:** A teal card with a globe icon, showing Signal Strength: -98 dBm.
- VPN:** An orange card with a network diagram icon, showing:
 - Protocol: SSTP
 - VPN Connection Status: Connected
 - Server: 112.124.110.213:5555
 - PAP/CHAP Username: 111
 - PAP/CHAP Password: 111
- Status Information:** A blue card with a table of device details:

Status Information	
IMEI	867113050347387
SN	N/A
IP Address	192.168.1.1
WAN IP Address	133.159.124.121
MAC Address	00:ab:df:19:73:25
IMSI	440030012524485
Connected Time	00:12:48

2. IPSec

1. WebUI にログインし、メインメニューより[System]を選択する。
2. IPSec Tunnel メニューを選択する。
3. 以下を設定する。

The screenshot shows the 'IPSec Tunnel' configuration page. The top navigation bar includes 'IoT', 'Dashboard', 'Internet', and 'System'. The left sidebar has 'Firmware Upgrade', 'System Settings', 'VPN', 'IPSec Tunnel' (selected), 'OpenVPN', 'Advance Settings', and 'WAN Port PING'. The main content area is titled 'IPSec Tunnel' and contains the following settings:

- IPSec Switch:** Enabled
- IPSec Connection Status:** Disconnected
- IPSec Mode:** Tunnel
- Remote Address:** 0.0.0.0
- DPD Delay(sec):** 30
- Key Exchange Mode:** ikev1
- Aggressive Mode:** no
- Local Subnets:** 0.0.0.0/0
- Remote Subnets:** 0.0.0.0/0
- Phase #1 Lifetime:** 3600
- Phase #2 Lifetime:** 3600
- IKE Encryption:** aes128
- ESP Encryption:** aes128
- IKE Hash:** sha1
- ESP Hash:** sha1
- DH Group:** modp1024
- PFS Group:** none
- Authentication Method:** psk
- Pre-Shared Key:** ****

A 'Save' button is located at the bottom right of the configuration area.

-IPSec Switch : Enabled / Disabled 接続先 VPN サーバーアドレス

-IPSec Connection Status : IPSec サーバとの接続状態を表示

-IPSec Mode : Tunnel / Transport から選択

-Remote Address : IPSec サーバのアドレスを入力

-DPD Delay (sec) : DPD(Dead Peer Detection)、IPsec トンネルの通信断をリアルタイムに
検出する期間を設定 (Heartbeat と同じ効果)

-Key Exchange Mode : ikev1 / ikev2 から選択

- Local Subnets : IPsec で保護されたローカルサブネットのアドレスを入力
- Remote Subnets : IPsec で保護されたリモートサブネットのアドレスを入力

Phase #1 (Security Association Phase1)

- Lifetime : Phase1 の生存可能時間を入力
- IKE Encryption : 暗号化アルゴリズムを aes128 / aes192 / aes256 / 3des から選択
- IKE Hash : 認証アルゴリズムを sha1 / sha256 / sha384 / sha512 / md5 から選択
- DH Group : DH Group を選択

Phase #2 (Security Association Phase2)

- Lifetime : Phase2 の生存可能時間を入力
- ESP Encryption : 暗号化アルゴリズムを aes128 / aes192 / aes256 / 3des から選択
- ESP Hash : 認証アルゴリズムを sha1 / sha256 / sha384 / sha512 / md5 から選択
- PFS Group : PFS Group を選択

- Authentication Method : 認証方式、psk (Pre-shared Key) で固定
- Pre-Shared Key : psk パスワードを入力

4.[Save]ボタンを押下する

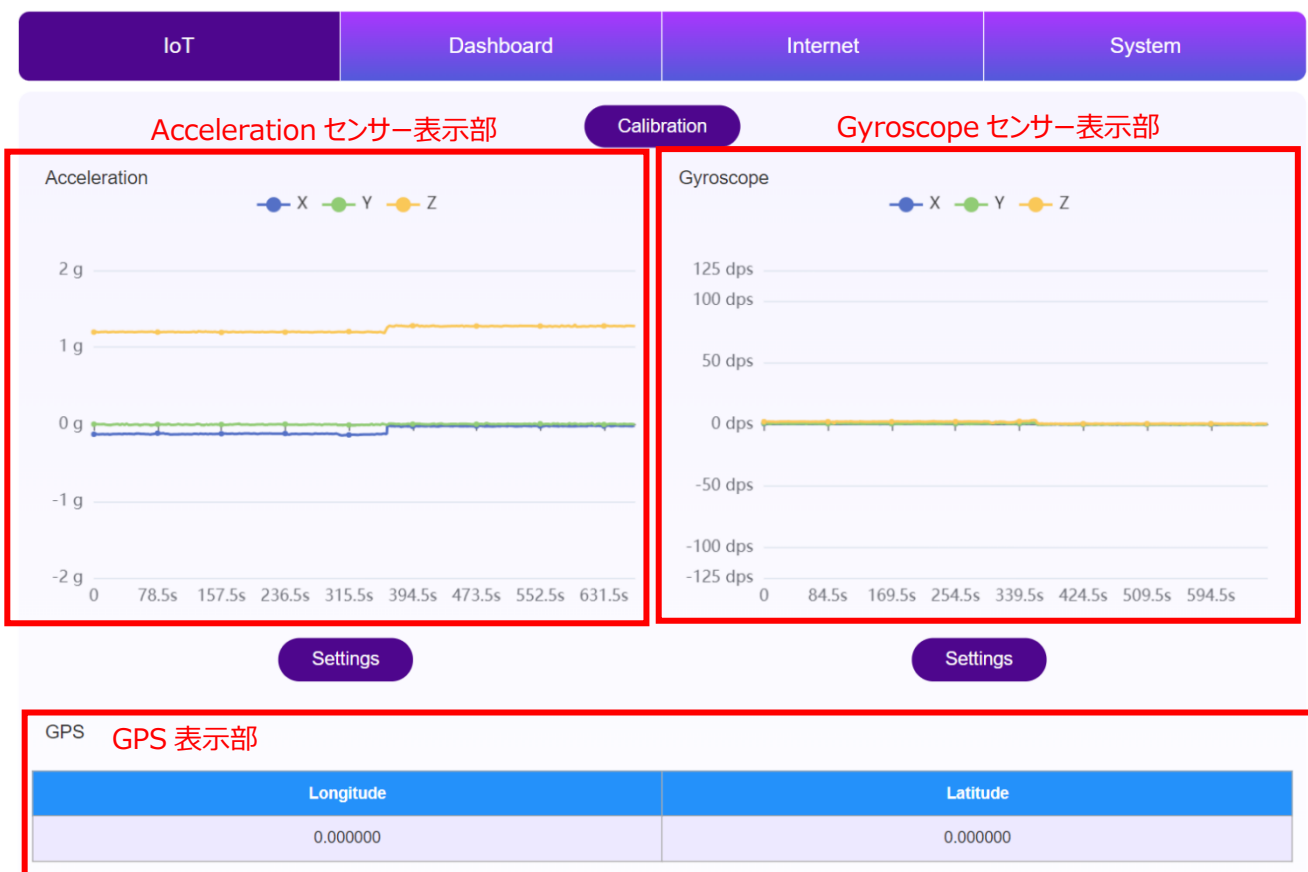
5. IPSec Connection Status が Connected になったら接続完了

8. Acceleration / Gyroscope

本章では、Acceleration/Gyroscope 関連の手順を記載します。

1.Acceleration/Gyroscope 画面説明

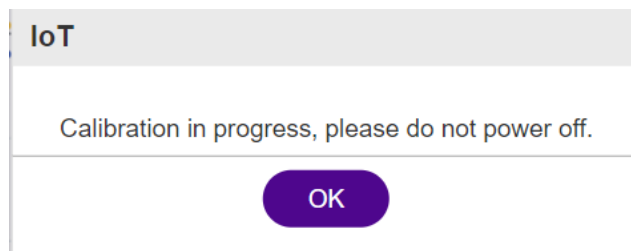
1.WebUI にログインし、メインメニューより [IoT] を選択する。



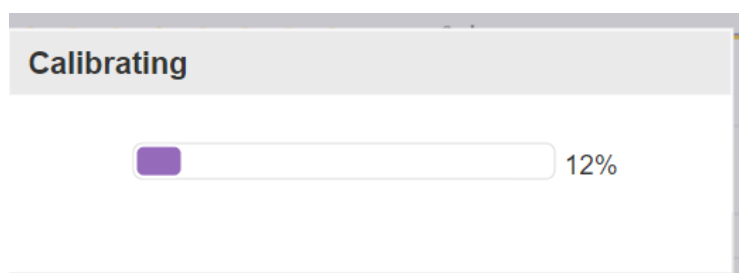
2. Calibration 設定

*押下した時点の位置を原点として設定

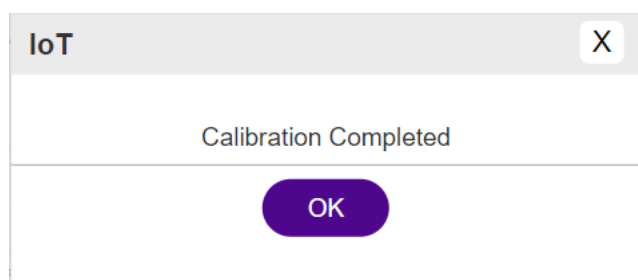
1. WebUI にログインし、メインメニューより [IoT] を選択する。
2. 画面上部 [Calibration] ボタンを押下する。



3. 上記 POPUP が表示されたら [OK] ボタンを押下する。



4. 進捗バーが 100%になるまで待つ。

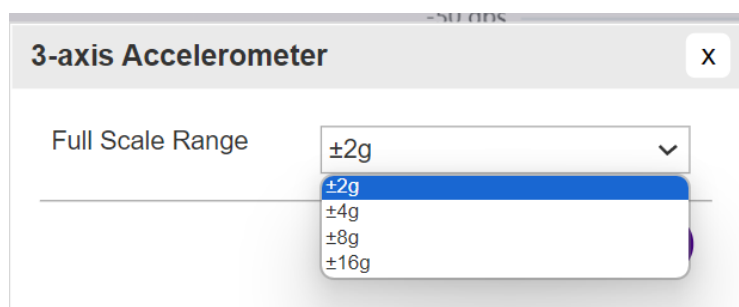


5. 上記 POPUP が表示されたら設定完了です。

3. Acceleration 設定

*Acceleration の測定範囲を設定

1. Acceleration 下部の [Settings] ボタンを押下する。

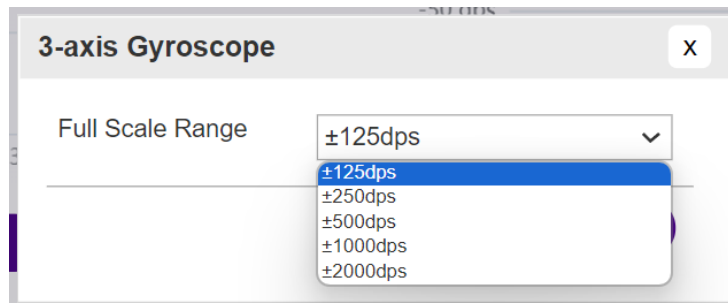


2. 測定範囲を選択する。
3. [OK] ボタンを押下する。

4. Gyroscope 設定

*Gyroscope の測定範囲を設定

1.Gyroscope 下部の[Settings]ボタンを押下する。



2.測定範囲を選択する。

3.[OK]ボタンを押下する。

5. GPS

*現在の位置情報が表示される。

*室内の場合は取得できないことがあります。

GPS	
Longitude	Latitude
139.427461	35.325155

9. MQTT

本章では、MQTT 関連の手順を記載します。

*AWS や Azure の SDK を使わずに MQTT を送信する機能

*SDK を使う場合は Cloud Service 章を参照

*自社クラウド等の利用。

1. WebUI にログインし、メインメニューより [IoT] を選択する。
2. メニューより [MQTT] を選択する。

Index	Enable	Name	Client id	Host	Port	Connection status	Start/Stop
1	Disabled	-	-	-	-	-	-
2	Disabled	-	-	-	-	-	-
3	Disabled	-	-	-	-	-	-
4	Disabled	-	-	-	-	-	-

3. Index の任意の番号を選択する。
*MQTT は同時に 4 つ同時に利用可能
4. Index の任意の番号を選択する。

Index	Enable	Name	Client id	Host	Port	Connection status	Start/Stop
1	Disabled	-	-	-	-	-	-
2	Disabled	-	-	-	-	-	-
3	Disabled	-	-	-	-	-	-
4	Disabled	-	-	-	-	-	-

General Settings

Index:

Enable:

Save

-Enabled : Enabled(有効にする場合)/Disable(無効にする場合)

5. [OK] ボタンを押下する。

6. 以下入力を行う。

General Settings	
Index	<input type="text" value="1"/>
Enable	<input type="text" value="Enabled"/>
* Name	<input type="text" value="zf1"/>
* Client id	<input type="text" value="1"/>
* Host	<input type="text" value="broker.hivemq.com"/>
* Port	<input type="text" value="8883"/>
User name	<input type="text"/>
Password	<input type="password"/>

-Name : 任意の名称

-Client id : 任意の ID

-Host : 送信先ホストアドレス

-Protocol : TCP/WS を選択

-Port : Port 番号を入力(MQTT:1883/MQTTS:8883)

7. MQTTS をご利用の場合は TLS を Enabled に設定し証明書を選択する。

The image shows a configuration form for MQTTS. The TLS setting is set to 'Enabled'. Three certificate files (CA File, Cert File, Key File) have been successfully uploaded, each with a 'Load' button and 'Upload successful' message. Other settings include Timeout (10s), Keep alive (60s), Version (V5.0), LWT Topic (empty), LWT Qos (1), LWT Retain (Disabled), and LWT Payload (empty). A 'Save' button is located at the bottom right.

8. [Save]ボタンを押下する。

9. Connection status が **Connected** になっていることを確認。

IoT > MQTT

MQTT List

Index	Enable	Name	Client id	Host	Port	Connection status	Start/Stop
1	Enabled	test	test	54.165.198.210	1883	Connected	Stop
2	Disabled	-	-	-	-	-	-
3	Disabled	-	-	-	-	-	-
4	Disabled	-	-	-	-	-	-

10. MQTT データのソース、パブリックの設定を行う。

Data Collection:	Enabled	▼
* Pub Data:	<input checked="" type="radio"/> Data Payload	<input type="radio"/> Gsensor
* Data Format:	<input checked="" type="radio"/> JSON	
Pub Topic	<input type="text"/>	
Pub Qos	1	▼
Pub Retain	Disabled	▼
Pub Mode:	Periodic reporting	▼
* Pub Interval	<input type="text"/> s	
Pub Payload	<input type="text"/>	

Save

-Data Collection : Enabled/Disabled

-Pub Data :

• Data Payload/G sensor

-Data Format : JSON(固定)

-Pub Topic : トピック名を入力

-Pub QoS : メッセージ保証レベルを選択

-Pub Retain : Retain 機能の Enabled(有効)/Disable(無効)を選択

-Pub Mode : Periodic reporting : インターバル指定での定期通信(固定)

-Pub Interval : 送信間隔を入力

11. [Save]ボタンを押下する。

10. Cloud Service

本章では、Cloud 関連の手順を記載します。

1. AWS に接続

1. WebUI にログインし、メインメニューより [IoT] を選択する。
2. メニューより [AWS] を押下する。
3. 以下を入力する。

IoT > AWS

AWS

Connection status: Connected Stop

Enable:

* Data Format: Json

* Host:

* Port Number:

User Name:

Password:

* CA File: Load Upload successful

* Cert File: Load Upload successful

* Key File: Load Upload successful

Reporting method:

* Interval Time: s

* Topic:

Additional Json Message:

OK

- Enable : Enabled(有効化)/Disabled(無効化)
- Data Format : Json(固定)
- Host : AWS のエンドポイントを入力する。
- Port Number : 8883
- CA File : 証明書を選択し[Load]を押下
- Cert File : certificate ファイルを選択し[Load]を押下
- Key File : 秘密鍵ファイルを選択し[Load]を押下
- Reporting method : Periodic reporting : インターバル指定での定期通信(固定)

- Interval Time : 送信間隔を入力
- Topic : MQTT のトピック名を入力
- Additional Json Message : JSON に付け加えたい文章がある場合に入力する。
 *例) "reciever_type" : "500J",
 *JSON フォーマットに沿った入力をお願いします。

- 4.[OK]を押下する。
5. Connection status の[Start]ボタンを押下する。
 ステータスが **Connected** になれば接続

2. Azure に接続

1. WebUI にログインし、メインメニューより [IoT] を選択する。
2. メニューより [Azure] を押下する。
3. 以下を入力する。

IoT > Azure

Azure

Connection status: **Disconnected**

Enable:

* Data Format: Json

* Host Name:

* Device ID:

* Shared Access Key:

Reporting method:

* Interval Time: s

Additional Json Message:

OK

- Enable : Enabled(有効化)/Disabled(無効化)
- Data Format : Json(固定)
- Host Name : Azure ホスト名前を入力
- Device ID : Device ID を入力
- Shared Access Key : アクセスキーを設定
- Reporting method : Periodic reporting : インターバル指定での定期通信 (固定)
- Interval Time : 送信間隔を入力

-Additional Json Message : JSON に付け加えたい文章がある場合に入力する。

*例) "Receiver_type" : "500J",

*JSON フォーマットに沿った入力をお願いします。

4.[OK]を押下する。

5. Connection status の[Start]ボタンを押下する。

ステータスが **Connected** になれば接続

11. ソフトウェアアップデート

本章では、ソフトウェアアップデートの手順を記載します。

- 1.WebUI にログインし、メインメニューより[System]を選択する。
- 2.サイドメニューより[Firmware Upgrade]を選択する。
- 3.[Browse]を選択し、別途提供するアップデートファイルを選択する。
- 4.[Upgrade]を選択する。

The screenshot displays the 'Firmware Upgrade' section of the WebUI. At the top, there are navigation tabs for IoT, Dashboard, Internet, and System. The 'System' tab is active. On the left, a sidebar menu lists various settings, with 'Firmware Upgrade' highlighted. The main content area is titled 'Firmware Upgrade' and contains the following text: 'Please refrain from closing your web browser or disconnecting the device while the update is in progress. Please be aware that during the update, there may be a temporary interruption in your internet connection. This is a normal part of the process. Your device will automatically restart once the update is complete.' Below this, the current firmware version is listed as 'MS01_UNIX_V001' and the current date as '20240422_22_58'. A message states: 'Please select the firmware upgrade file and then proceed by clicking the 'Upgrade' button.' There is an empty input field for the file path, a 'Browse' button, and an 'Upgrade' button. Both the 'Browse' and 'Upgrade' buttons are highlighted with red boxes in the original image.

- 5.アップデートが完了する。

※アップデート中は電源を抜いたりしないでください。故障の原因となります。

12. 改訂履歴

本章では、改訂履歴を記載します。

マニュアル改訂記号は、表紙尾に記載されているカタログ番号の末尾に付記されます。

カタログ番号：MC01 -User□

↑改訂記号

改訂記号	改訂年月	改訂ページ
A	2023年11月	初版
B	2023年12月	機器構成章の修正 社名変更 タイトル変更
C	2024年3月	写真変更 不要機能の削除
D	2024年4月	機器構成章の修正

13. ご案内

本誌に記載のない条件や環境での使用、および人命や財産に大きな影響が予測されるなど、特に安全性が要求される用途に使用される際には、当社の意図した特別の合意がある場合を除き当社は当社商品に対して一切保証を致しません。

株式会社 SyncWave

製品に関するお問い合わせ先

メール : info@syncwave.jp / ホームページ : <http://syncwave.jp/>

カタログ番号 : MC01・UserD 2024年4月現在