

42. IIoT

本章では、IIoT の通信プロトコルの使用方法について説明します。

42.1. MQTT	42-2
42.2. OPC UA サーバー	42-26

42.1. MQTT

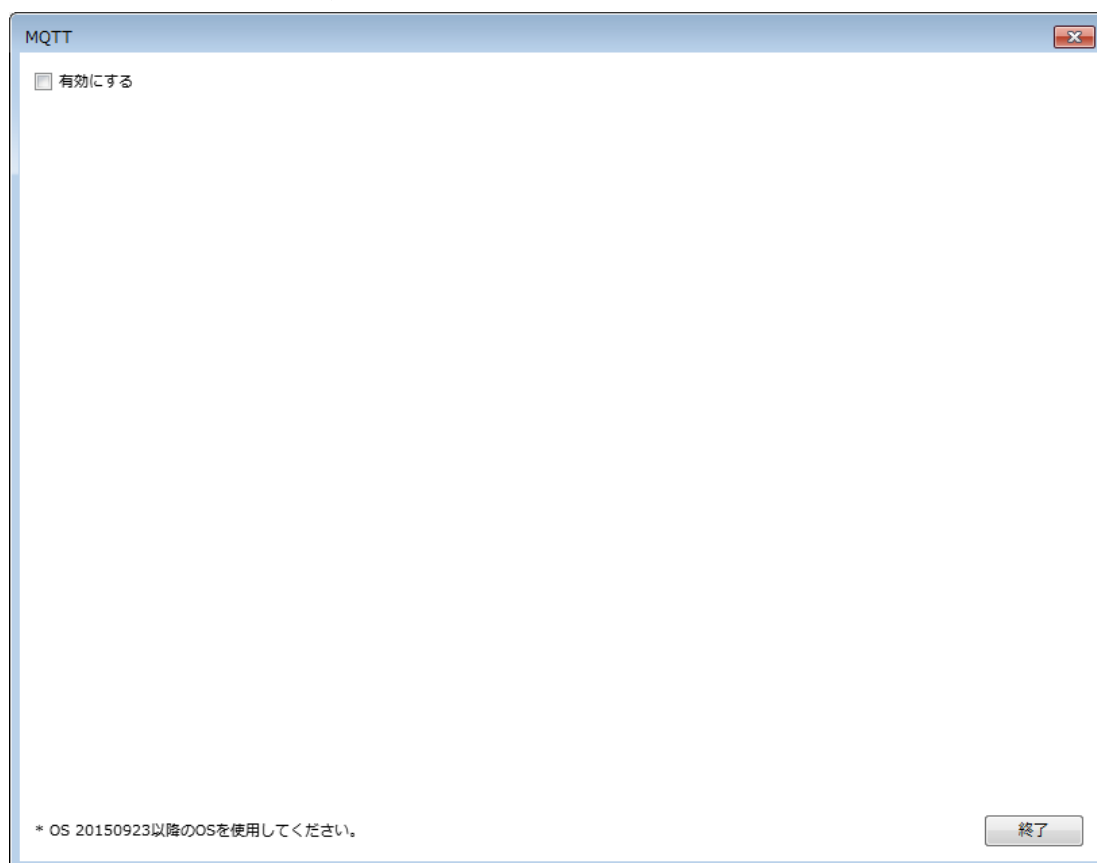
42.1.1. 概要

[MQTT]オブジェクトを使用すれば、メッセージを MQTT サーバーに送信でき、一方 MQTT サーバーからトピックを購読することもできます。HMI を MQTT サーバーとして使用することもできます。HMI を MQTT サーバーにする場合、メッセージを他のサーバーに送信しません。

42.1.2. 設定

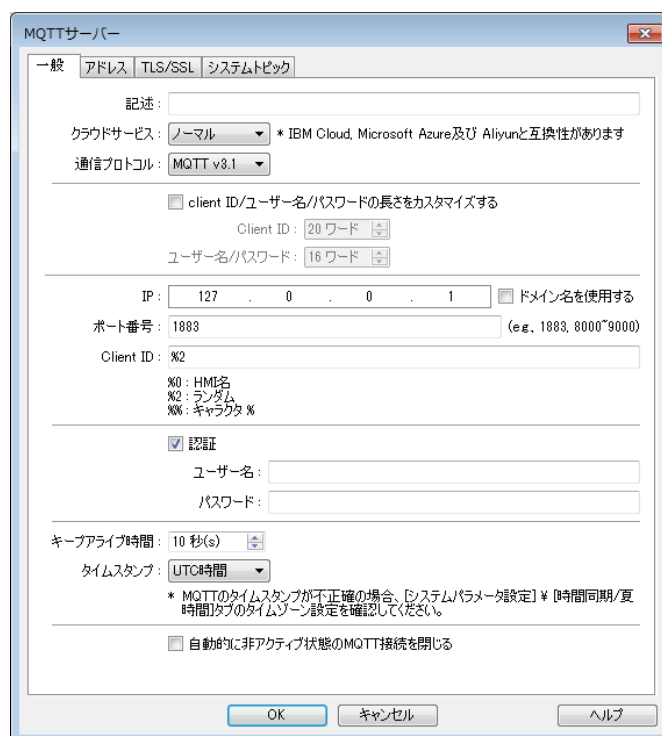


ツールバーの[オブジェクト]をクリックし、そして[IIoT] » [MQTT]をクリックして本オブジェクトを新規作成してください。有効にしたら、設定ダイアログボックスが現れます。



42.1.2.1. サーバー設定

一般的な属性の設定



MQTTサーバー

一般 | アドレス | TLS/SSL | システムトピック

記述:

クラウドサービス: ノーマル * IBM Cloud, Microsoft Azure及び Aliyunと互換性があります

通信プロトコル: MQTT v3.1

☐ client ID/ユーザー名/パスワードの長さをカスタマイズする

Client ID: 20 ワード

ユーザー名/パスワード: 16 ワード

IP: 127 . 0 . 0 . 1 ☐ ドメイン名を使用する

ポート番号: 1883 (e.g., 1883, 8000~9000)

Client ID: %2

%0: HMI名
%2: ランダム
%%: キャラクタ %

☒ 認証

ユーザー名:

パスワード:

キープアライブ時間: 10 秒(s)

タイムスタンプ: UTC時間

* MQTTのタイムスタンプが不正確の場合、[システムパラメータ設定] * [時間同期/夏時間]タブのタイムゾーン設定を確認してください。

☐ 自動的に非アクティブ状態のMQTT接続を閉じる

OK キャンセル ヘルプ

設定

クラウドサービス

記述

一般

一般的な MQTT トピックを発行-購読するモードです。

AWS IoT

AWS IoT をブローカーにします。Thing でデータを転送し、Shadow 機能をサポートします。詳細は“AWS IoT ユーザーマニュアル”をご参照ください。

Sparkplug B

Sparkplug B は IIoT 応用の特性に基づいてデザインされた規格です。本規格は標準 MQTT 規格が規制していないトピック及びメッセージ内容を定義するのに役立ち、それに MQTT 未対応の装置でも Edge of Network (HMI)と通じて間接に MQTT 送信ができるようにさせます。詳細は“Sparkplug B スタートアップガイド”をご参考ください。

Azure IoT Hub

Microsoft Azure IoT Hub を Broker にします。本サービ

スを使用する場合、正確なストリングを記入すれば通信でき、設定手順が簡単です。接続用のストリングは Microsoft Azure > IoT devices で見つかります。

Google Cloud IoT Core

Google Cloud IoT Core を Broker にし、接続パラメータ及び関連ファイルを検証すれば通信できます。

通信プロトコル	MQTT v3.1 と v3.1.1 をサポートします。
Client ID/ユーザー名/ パスワードの長さを カスタマイズする	Client ID : 長さ上限は 128 ワードです。 ユーザー名/パスワード : 長さ上限は 256 ワードです。
IP	メッセージを受信する MQTT サーバー IP を設定します。IP アドレスに 127.0.0.1 を入力すると、HMI の MQTT サーバーが起動されます。
ドメイン名を使用する	ドメイン名 : 127.0.0.1 <input checked="" type="checkbox"/> ドメイン名を使用する ドメイン名をサーバーアドレスとして使用するのをサポートします。
ポート番号	受信する MQTT サーバーの接続ポートを設定します。

Client ID	ログイン名です。変数を Client ID にすることができます。例えば: %0 を入力すれば、HMI の名前が Client ID になります。
検証	[ユーザー名]及び[パスワード]で MQTT サーバーに接続するのを選択します。
ユーザー名	MQTT サーバーに接続用の[ユーザー名]です。
パスワード	MQTT サーバーに接続用の[パスワード]です。
キープアライブ時間	[キープアライブ時間]を超えても、まだ HMI のキープアライブが送られてこない場合、MQTT サーバーは HMI との接続が切断されたと判断します。 備考: シミュレーションを使用する場合、メッセージの通信が遅延される可能性があります。但し、遅延時間は長くても[キープアライブ時間]を超えません。 HMI 上のメッセージは即時に送信します。
タイムスタンプ	ローカル時刻 HMI 時刻をタイムスタンプにします。 UTC 時刻 UTC+0 時刻を使用します。タイムスタンプが不正確だった場合、[システムパラメータ設定] » [時刻同期/夏時間]タブのタイムゾーンの設定を確認してください。
自動的に非アクティブ中の MQTT 接続を切断する	アイドル時間が[アイドル制限]に設定した値を超えると、自動的に接続を切断し、次回データが更新される時になってから、接続を再開します。 初めての接続の場合のみ、デフォルト数値及びトピックリストを更新するのを選択できます。 本設定を使用する場合、コントロールアドレスの開始/停止コマンドが無効になります。

アドレス設定

設定

記述

状態アドレス

LW-n: [MQTT]の接続状態を表示する

数値	記述
0	MQTT サーバーに接続していない
1	接続が切断された。MQTT サーバーに接続できない
2	MQTT サーバーとの接続に成功した

LW-n+1: エラー提示

数値	記述
0	エラー無し
1 or more	エラー有り

バッファ使用量アドレス

配信に成功していない場合、メッセージはバッファとしてメモリーに保存します。最大 10000 レコードです。アドレスに表示される単位は%で、端数を切り上げます。

LW-n: バッファ使用量を表示する

コントロールアドレス

LW-n: [MQTT サーバー]の実行または停止をコントロールする

数値	記述
----	----

0	準備完了
1	開始
2	停止
3	更新

LW-n+1: MQTT サーバーの IP アドレスを設定する

LW-n+5: MQTT サーバーの接続ポート番号を設定する

LW-n+6: MQTT サーバーに接続用の Client ID を設定する

LW-n+26: 検証を無効/有効にする

数値	記述
0	無効にする
1	有効にする

LW-n+27: MQTT サーバーに接続用のユーザー名を設定する

LW-n+43: MQTT サーバーに接続用のパスワードを設定する

- クラウドサービスに **Azure IoT Hub** を選択した場合、コントロールアドレスは以下の通りです：

LW-n: [MQTT サーバー]の実行・停止を制御する

数値	記述
0	準備完了
1	開始
2	停止
3	更新

LW-n+1: 接続ストリングを設定する(128 words)

TLS/SSL 設定



設定	記述
有効にする	TLS/SSL 暗号化を有効にします。手動でバージョン: TLS 1.0、TLS 1.1 或いは TLS 1.2 を選択することができます。 TLS 1.1 及び TLS 1.2 を使用する場合、HMI の OS には 20180323 以降のバージョンを使用すること。
サーバー検証	有効にする サーバーの認証が認証局(CA)の認証を得たのかを検証します。サーバー認証は接続の時に、サーバーから送られます。 サーバー名は認証情報に一致しなければなりません サーバーの IP はサーバー認証内の IP 記録に一致しているかどうかを検証します。IP 記録は認証内の Subject Alternative Name に記載されています。
クライアント検証	秘密鍵及び認証はサーバーにクライアントを検証させるための必要資料です。

システムトピック

現在は四種類のシステムトピックがあり、HMI はそれらを発行するかどうかを選択できます。HMI がシステムトピックを有効にした場合、購読者はそのトピックを購読することにより、その HMI のトピックリストまたは接続状態を知ることができます。

新規作成 MQTTサーバー オブジェクト

一般 アドレス TLS/SSL システムトピック

Topic List
Birth Topic
Close Topic
Last Will

☒ 有効にする

トピック: ot-2/type/mt/id/%1/evt/topics_update/fmt/json デフォルト

%0: HMI名
%1: サーバーのClient ID
%%: キャラクタ %

☒ メッセージを保持する

QoS: 2

内容フォーマット: JSON (Default)

リセット

設定	記述
Topic List	HMI 内のトピックリストです。 本メッセージは、HMI がサーバーと接続した後、サーバーに送信されます。
Birth Topic	HMI がサーバーに接続した後、送信するメッセージです。
Close Topic	HMI から自主的にサーバーとの接続を切断する前、最後に送信するメッセージです。
Last Will	クライアントがサーバーの間に異常が発生して接続が切断された場合、Last Will の購読者は本メッセージを受信します。クライアントが最初に CONNECT メッセージをサーバーに接続をリクエストした時も、同時に Last Will メッセージの内容を含めて送信します。
トピック	システムトピックの実際のトピック名です。
メッセージを保持	本項にチェックマークを入れると、MQTT サーバーは最新の 1 レコードのメッセージを確保します。
QoS	MQTT は 3 レベルの信頼性を提供します。即ち QoS(キューオーエス)のことです。メッセージ配布の信頼性はメッセージが確実に届くのかを決めます。 QoS 0: 最高一回：メッセージを一回だけ配布するが、確実に届くかは保証しません。 QoS 1: 最低一回：メッセージは最低一回届きます。 QoS 2: 正確に一回：メッセージは正確に一回届きま

内容フォーマット

す。

JSON (Default) : デフォルト値を使用します。

各システムトピックのデフォルト値 :

カレントの実際値は赤字で示します。

Topic list:

```
{
  "d": {
    "topics": [
      {
        "compression": "圧縮タイプ",
        "nickname": "トピック名",
        "topic": "トピック"
      },
      {
        "compression": "圧縮タイプ",
        "nickname": "トピック名",
        "topic": "トピック"
      }
    ]
  },
  "ts": "現在時刻"
}
```

topics 内のメッセージは実際のトピックの設定により異なります。上記はトピックが 2 個の例です。

Birth Topic:

```
{
  "d": {
    "connected": true
  },
  "ts": "現在時刻"
}
```

Close Topic:

```
{
  "d": {
```

```

        "connected":false
    },
    "ts":"現在時刻"
}

```

Last Will:

```


{
    "d":{
        "connected":false
    }
}

```

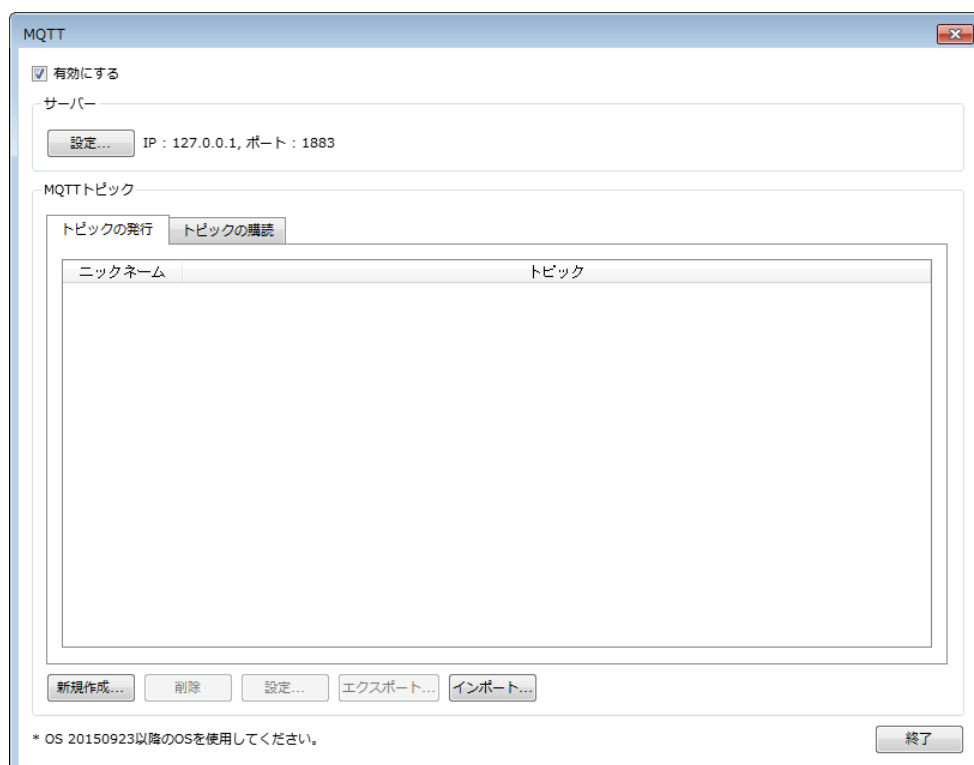
JSON (Customized) : カスタマイズした内容を使用します。

Note

クラウドサービスに Sparkplug B、Azure IoT Hub 及び Google Cloud IoT Core を選択した場合、[システムトピック]タブがサポートされません。

 このアイコンをクリックし、チュートリアルビデオを閲覧してください。閲覧する前に、インターネットケーブルが接続しているのを確認してください。

42.1.2.2. MQTT トピックの発行



[新規作成]を選択すれば、一般的な属性及びアドレスの設定に入ることができます。または直接に CSV ファイルを[エクスポート]/[インポート]する機能で MQTT 発行トピックを作成してもいいです。MQTT 発行トピックの数量上限は 255 です。

一般的な属性の設定

MQTTトピック発行者

一般 アドレス

ニックネーム: topic 1

トピック: iot-2/type/cMT3071/id/%0/evt/topic 1/fmt/json

%0: HMI名
%1: サーバーのClientID
%(DYNAMIC): 動的ストリング
%%: キャラクタ %

送信モード: アドレス(自動)

☒ 数値トリガー式
☐ 時間ベース式

圧縮タイプ: None

☐ メッセージを保持する
☒ タイムスタンプを含む
☒ 最上層の"d"記号をメッセージフォーマットに使用する

QoS: 2

内容フォーマット: JSON (一般)

OK キャンセル ヘルプ

設定

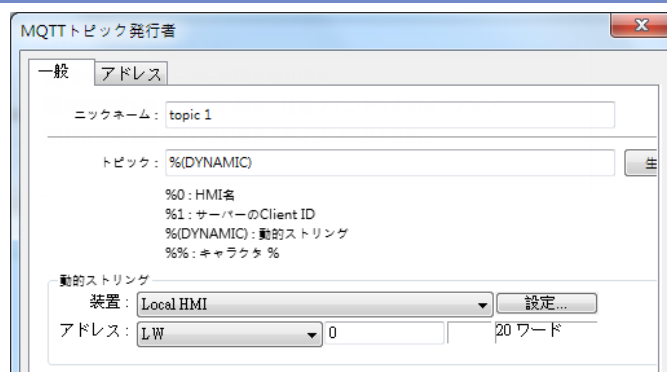
記述

ニックネーム

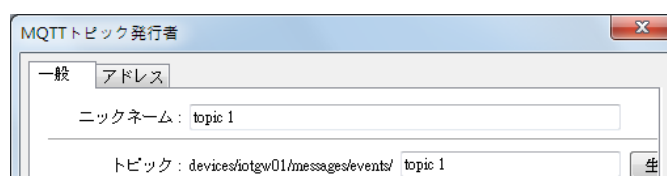
MQTT トピックの項目名を設定します。

トピック

メッセージを送信する時、MQTT サーバーが受け取れたトピックです。変数をトピックとして使用することができます。使用方法：トピック欄で%(DYNAMIC)を入力すれば、下側に動的ストリングアドレスの設定欄が現れます。%(DYNAMIC)のストリングに複数の topic level を含めることができます。例：myhome/groundfloor。



クラウドサービスに Azure IoT Hub を選択した場合、トピックは固定したフォーマットで、ユーザーは最後の level だけを指定可能です。



送信モード

アドレス(自動)

数値トリガー式：

数値に変化があるたびに、MQTT メッセージを送信します。

周期ベース式：

定期的に MQTT メッセージを送信します。

アドレス(ビットトリガー)

指定したビットがトリガーされたたびに、MQTT メッセージを送信します。

イベント(アラーム)ログ

イベントログをトピックのソースとして使用可能です。単一のイベント、もしくは指定したカテゴリでの任意のイベントがトリガーされた場合 MQTT メッセージを送信するのを選択できます。

圧縮タイプ

メッセージを圧縮してから転送します。圧縮されたメッセージを読み取る前、先に解凍する必要があります。メッセージを圧縮/解凍するには、zlib、gzip または DEFLATE 算法が選べます。

メッセージを保持する

本項にチェックマークを入れると、MQTT サーバーは最新のメッセージを保持します。

タイムスタンプを含む

内容フォーマットに[JSON(一般)]を使用した場合のみ、本機能がサポートされます。手動でタイムスタンプを含むかを決定できます。

最上層の"d"記号をメ

内容フォーマットに[JSON(一般)]を使用した場合のみ、本機

メッセージフォーマットに使用する

能がサポートされます。チェックマークを入れると、メッセージフォーマットは以下の通りになります：

```
{
  "d": {
    "addressName1": ...,
    "addressName2": ...
  },
  "ts": ...
}
```

チェックマークを入れないと、メッセージフォーマットは以下の通りになります：

```
{
  "addressName1": ...,
  "addressName2": ...,
  "ts": ...
}
```

上図に示された通り、チェックマークを入れていない場合、ts とアドレス名は同じ階層のキー(key)ですので、アドレス名を ts に命名することを避けてください。

QoS

MQTT は 3 レベルの信頼性を提供します。即ち QoS(キューオーエス)のことです。メッセージ配布の信頼性はメッセージが確実に届くのかを決めます。

0: 最高一回：メッセージを一回だけ配布するが、確実に届くかは保証しません。

1: 最低一回：メッセージは最低一回届きます。

2: 正確に一回：メッセージは正確に一回届きます。

内容フォーマット

Raw data：BYTE で組み合わせたデータです。

JSON(一般): 全てのデータをメンバー"d"に置く JSON フォーマットです。

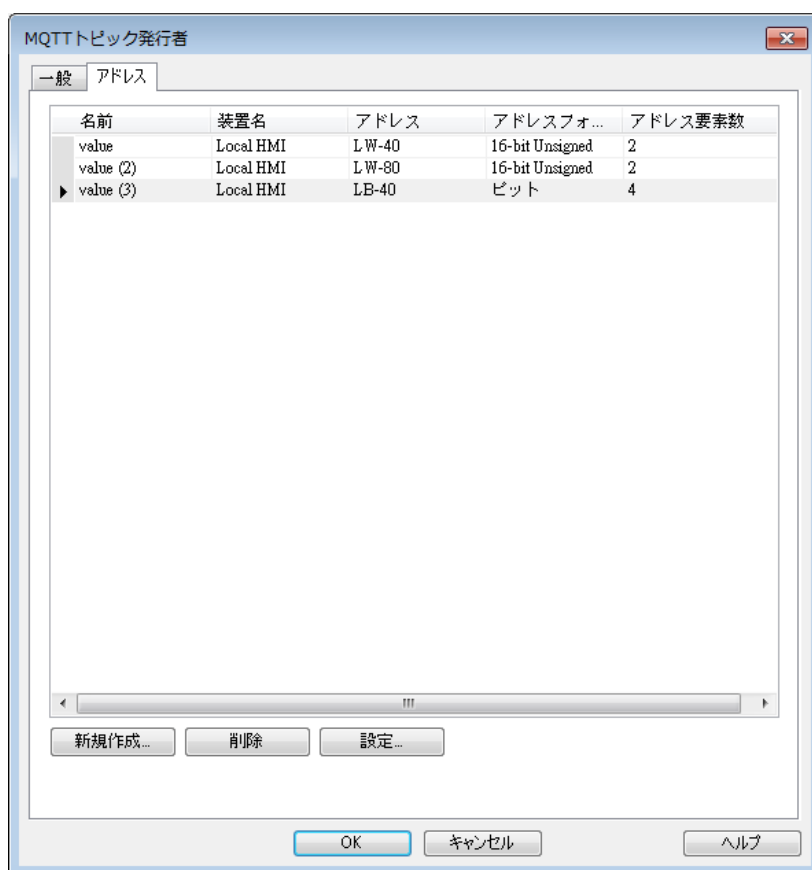
JSON(高度)：フレキシブルなネスト構造があるユーザー定義 JSON フォーマットです。

Note

- 一個の tag には最大 255 個の word を使用できます。

アドレス設定

本節では、内容フォーマットに[Raw Data]と[JSON(一般)]を使用する場合、アドレスの設定方法について説明します。



設定

記述

新規追加

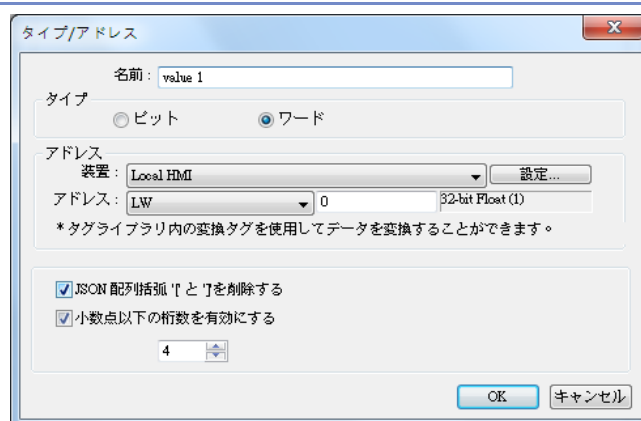
トピックのアドレスソースを作成します。各アドレスの長さを個別に設定することができます。

削除

アドレスを削除します。

設定

アドレス及び名前を変更します。



設定

記述

JSON 配列括弧 '[' と ']' を削除する

本項にチェックマークを入れると、JSON フォーマットのメッセージを使用する場合、手動で括弧を削除することができます。

小数点以下の桁数を有効にする

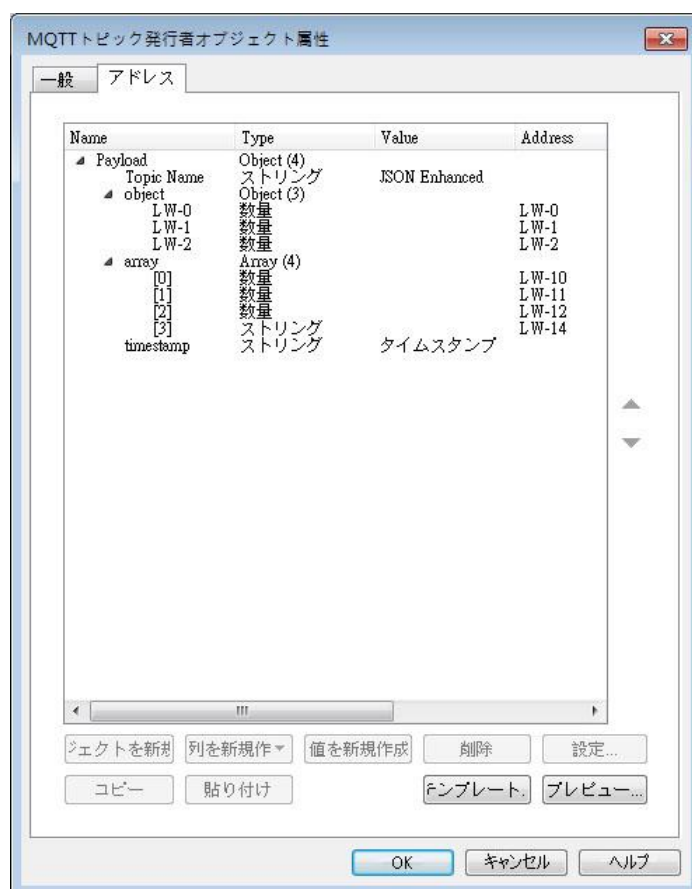
アドレスのデータ型を Float 浮動小数点数に設定する場合、小数点以下の桁数を選択することができます。



- tag の長さは最大 255 word です。

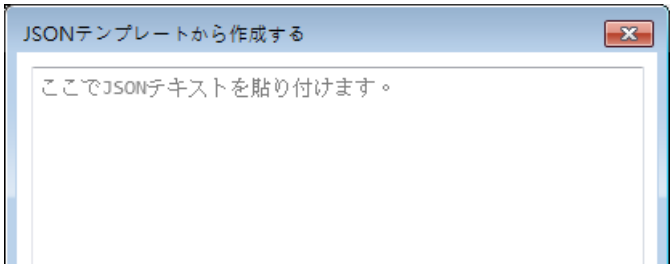
アドレス設定[JSON(高度)]

本節では、内容フォーマットに[JSON(高度)]を使用する場合、アドレスの設定方法について説明します。[JSON(高度)]はネスト構造をサポートし、オブジェクト、配列などのフォーマットを使用可能で、タイムスタンプ及びデータ名もカスタマイズでき、フレキシブルなデザインを実現できます。



上図を例に挙げると、上図のように設定すれば、購読側では以下のフォーマットの MQTT メッセージが届きます。

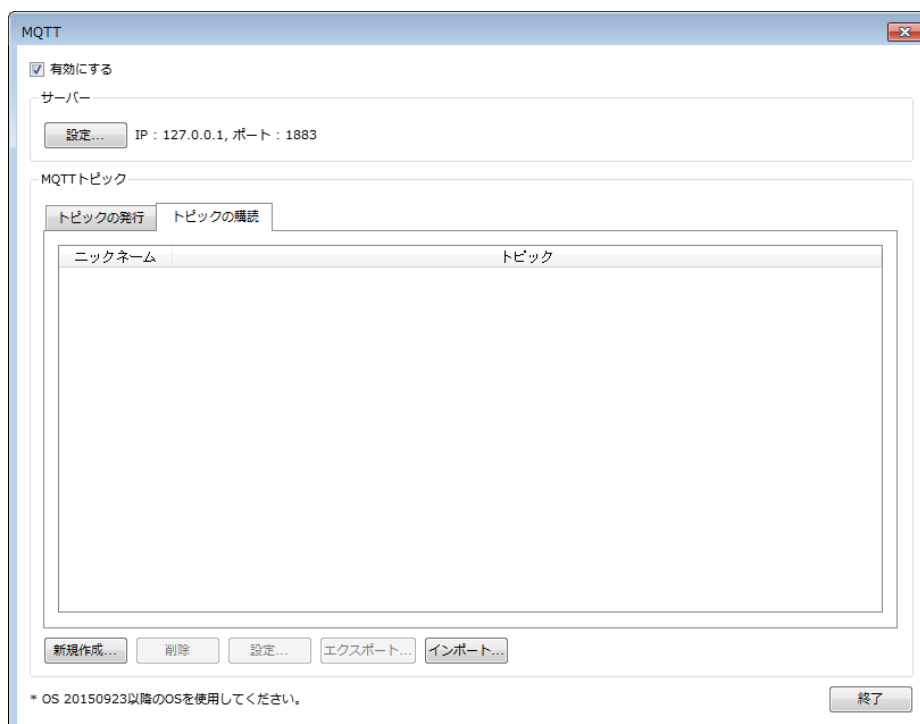
```
{
  "Topic Name" : "JSON Enhanced",
  "Object" : {
    "LW-0" : [ 1 ],
    "LW-1" : [ 2 ],
    "LW-2" : [ 3 ]
  },
  "Array" : [ [ 4 ], [ 5 ], [ 6 ], [ "AABBCCDD" ] ],
  "timestamp" : "2019-02-19T06:52:13.846038"
}
```


設定	記述
オブジェクトを新規追加	一個のデータオブジェクトを新規追加します。オブジェクトでは複数のデータフォーマットを含むことができ、各データフォーマットでは独自の名前と数値があります。オブジェクトのデータを大括弧{}で包括します。
配列を新規追加	一個のデータ配列を新規追加します。配列の中には複数のデータフォーマットを含むことができますが、名前は一個だけしかありません。オブジェクトのデータを中括弧[]で包括します。
数値を新規追加	一個の数値、ストリングまたはタイムスタンプを新規追加します。数値またはストリングである場合、固定した数値を使用、または指定のアドレスからデータを読み取ることができます。
削除	選択した欄を削除します。
設定	選択した欄を変更します。選択した欄はオブジェクト及び配列の場合、名前だけを変更できます。但し、オブジェクトと配列に包括された数値(例えば[数値を新規追加]のパラメータ)を変更できます。
コピー	選択した欄をコピーします。
貼り付け	選択した欄でコピーした内容を貼り付けます。
テンプレート	ここで JSON 文字を貼り付ければ、システムは自動的に本 JSON フォーマットに合致する構成を作成し、自ら定義する手間が省けます。
	
プレビュー	読みやすいフォーマットで JSON データをプレビューします。

Note

- 一個の Topic には最大 512 個のノード(payload を含む)を使用できます。一個の tag には最大 255 個の word を使用できます。

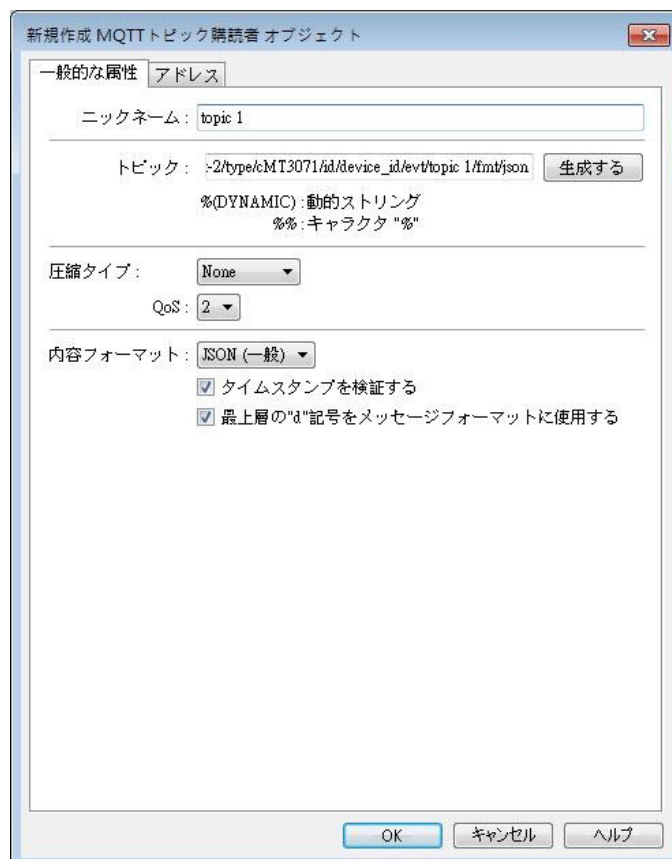
42.1.2.3. MQTT トピックの購読



[新規作成]を選択すれば、一般的な属性及びアドレスの設定に入ることができます。または直接に CSV ファイルを[エクスポート]/[インポート]する機能で MQTT 購読トピックを作成してもいいです。MQTT 購読トピックの数量上限は 255 です。

一般的な属性の設定

本節では、内容フォーマットに[Raw Data]と[JSON(一般)]を使用する場合、アドレスの設定方法について説明します。



設定

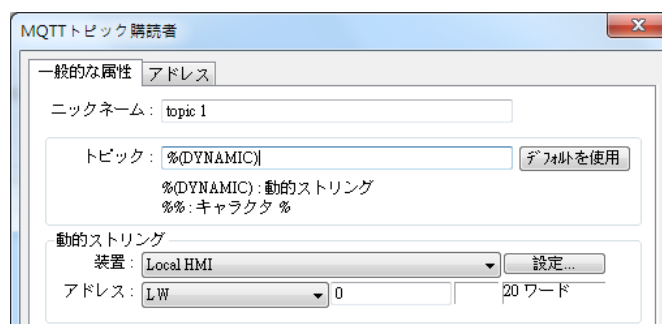
記述

ニックネーム

MQTT トピックの項目名を設定します。

トピック

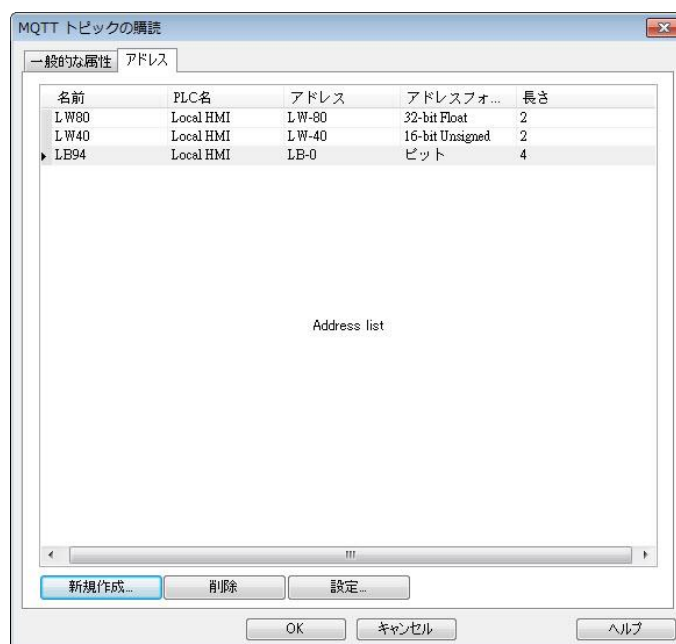
MQTT サーバーから購読するトピックです。動的ストリングで購読してもいいです。使用方法: トピック欄で%(DYNAMIC)を入力すれば、下側に動的ストリングアドレスの設定欄が現れます。%(DYNAMIC)のストリングに複数の topic level を含めることができます。例: myhome/groundfloor。



クラウドサービスに Azure IoT Hub を選択した場合、トピック

	クは固定したフォーマットで、ユーザーは最後の level だけを指定可能です。このトピック level はトピック発行者での設定と同じでなければなりません。
圧縮タイプ	ここは発行者での設定と同じでなければなりません。
タイムスタンプを検証する	本項にチェックマークを入れると、メッセージのタイムスタンプを検証することになります。タイムスタンプが増加する場合のみメッセージが更新され、そうでないと、メッセージは古いものと判断され、更新されません。
最上層の"d"記号をメッセージフォーマットに使用する	<p>チェックマークを入れると、メッセージフォーマットは以下の通りになります：</p> <pre> { "d": { "addressName1": ..., "addressName2": ... }, "ts": ... } </pre> <p>チェックマークを入れないと、メッセージフォーマットは以下の通りになります：</p> <pre> { "addressName1": ..., "addressName2": ..., "ts": ... } </pre> <p>データソースに基づいて適する設定を選択してください。</p>
QoS	<p>MQTT は 3 レベルの信頼性を提供します。即ち QoS(キューオーエス)のことです。メッセージ配布の信頼性はメッセージが確実に届くのかを決めます。</p> <p>0: 最高一回：メッセージを一回だけ配布するが、確実に届くかは保証しません。</p> <p>1: 最低一回：メッセージは最低一回届きます。</p> <p>2: 正確に一回：メッセージは正確に一回届きます。</p>
内容フォーマット	<p>Raw data：特定したフォーマットが無い原始データです。</p> <p>JSON (一般)：単層構造の JSON フォーマットです。</p> <p>JSON (高度)：フレキシブルにネスト構造を定義できる JSON フォーマットです。</p>

アドレス設定



設定

記述

新規追加

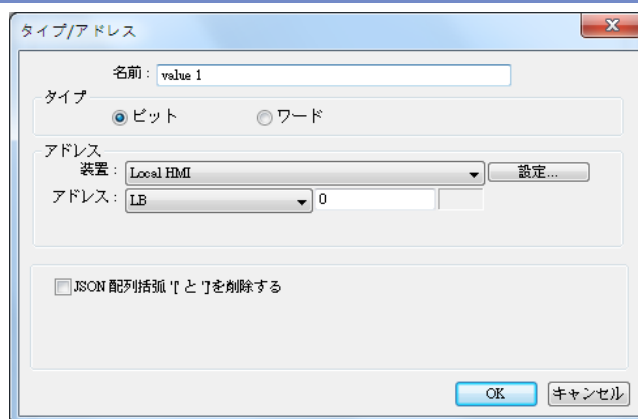
トピックの配布先のアドレスを追加します。各アドレスの長さを個別に設定することができます。

削除

アドレスを削除します。

設定

アドレス及び名前を変更します。



設定

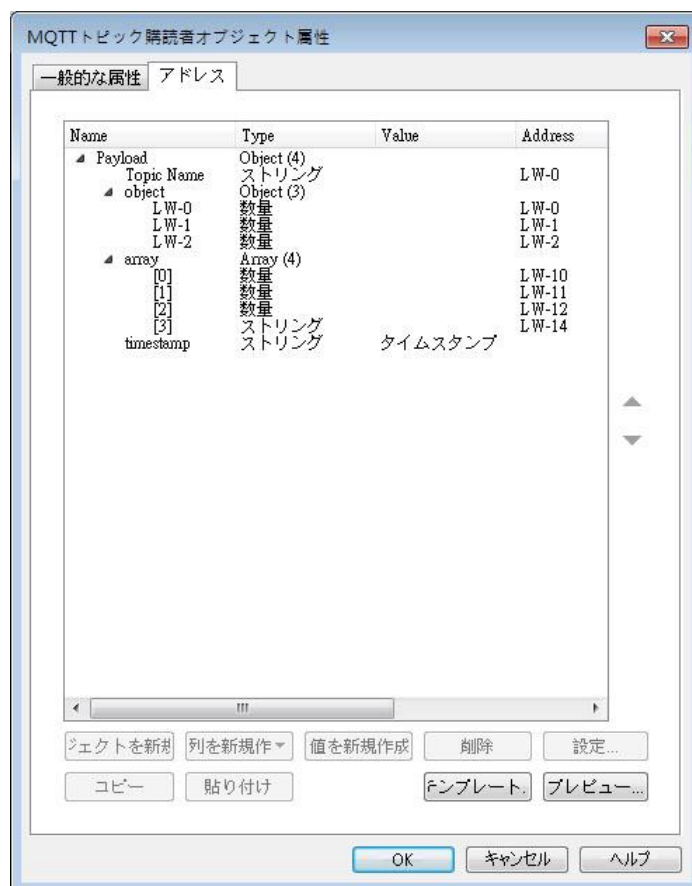
記述

JSON 配列括弧「[]」と「{}」を削除する

本項にチェックマークを入れると、JSON フォーマットのメッセージを使用する場合、手動で括弧を削除することができます。

アドレス設定[JSON(高度)]

本節では、内容フォーマットに[JSON(高度)]を使用する場合、アドレスの設定方法について説明します。[JSON(高度)]はネスト構造をサポートし、オブジェクト、配列などの形式を使用でき、タイムスタンプ及びデータ名を定義でき、よりフレキシブルにデザインできます。



設定

記述

オブジェクトを新規追加

一個のデータオブジェクトを新規追加します。オブジェクトでは複数のデータフォーマットを含むことができ、各データフォーマットでは独自の名前と数値があります。オブジェクトのデータを大括弧{ }で包括します。

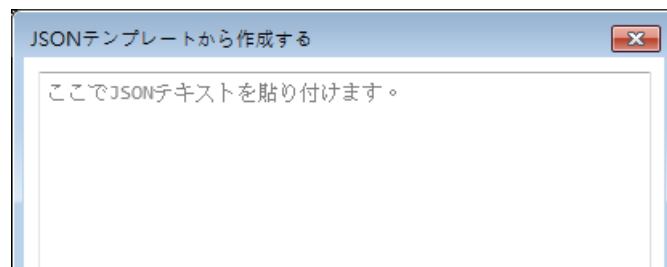
配列を新規追加

一個のデータ配列を新規追加します。配列の中には複数のデータフォーマットを含むことができますが、名前は一個だけしかありません。オブジェクトのデータを中括弧[]で包括します。

数値を新規追加

一個の数値、ストリングまたはタイムスタンプを新規追加します。数値またはストリングである場合、固定した数値を使用、または指定のアドレスからデータを読み取ることができます。

削除	選択した欄を削除します。
設定	選択した欄を変更します。選択した欄はオブジェクト及び配列の場合、名前だけを変更できます。但し、オブジェクトと配列に包括された数値(例えば[数値を新規追加]のパラメータ)を変更できます。
コピー	選択した欄をコピーします。
貼り付け	選択した欄でコピーした内容を貼り付けます。
テンプレート	ここで JSON 文字を貼り付ければ、システムは自動的に本 JSON フォーマットに合致する構成を作成し、自ら定義する手間が省けます。



Note

- Amazon Web Service(AWS) IoT Core は、標準の MQTT プロトコルをサポートします。使用する場合、下記の事項をご注意ください：
 1. トピックは最大 8 階層まで(iot-2/type は 2 階層)です。
 2. [一般的な属性]タブでの検証をサポートしません。検証するには、[TLS/SSL]タブで行ってください。
 3. QoS 0 と QoS 1 のみをサポートします。
 4. トピック発行の[メッセージを確保する]機能をサポートしません。

42.1.2.4. Sparkplug B

クラウドサービスに Sparkplug B を選択する場合、一般的な属性及び装置の設定方法は以下の通りです。

一般的な属性の設定

MQTT

☒ 有効にする

サーバー

設定... IP: 127.0.0.1, ポート: 1883

Sparkplug B

一般 装置

グループID: cMT Group

Edge node ID: cMT EoN

DDATA最小時間: 0 ms

*新しいDDATA (Device DATA)メッセージを送信する前の最小待ち時間(データの変更が検出された場合)

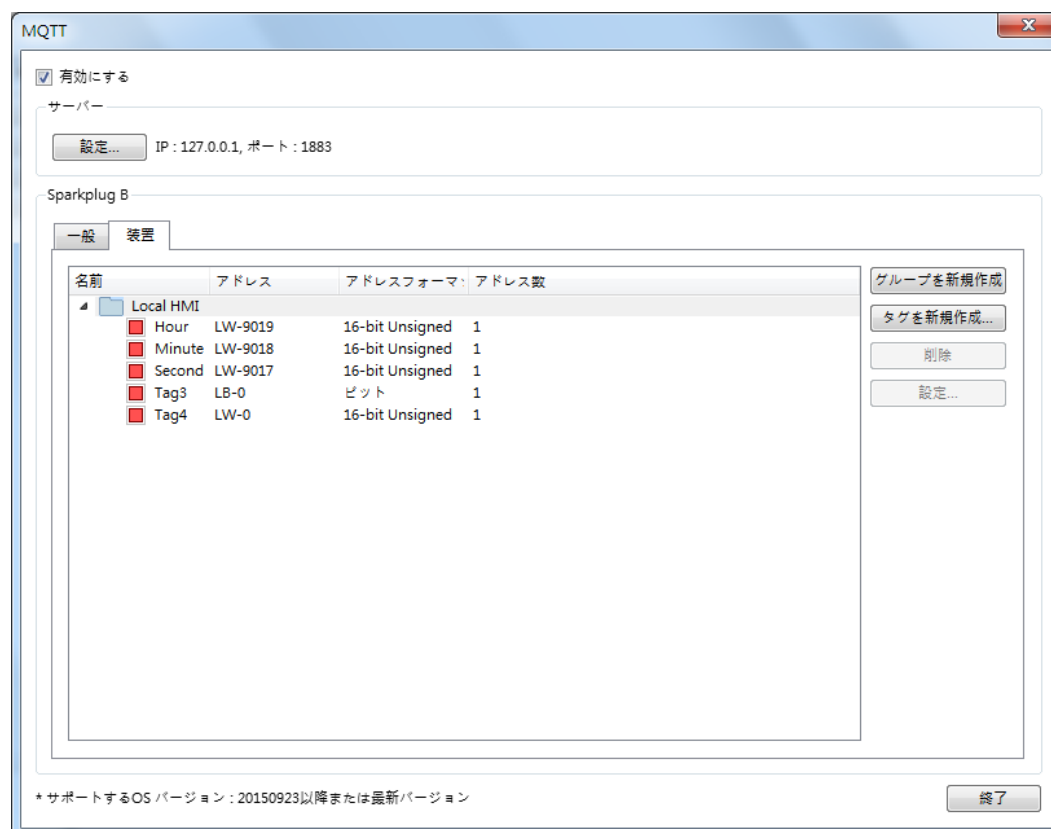
QoS: 1

* サポートするOSバージョン: 20150923以降または最新バージョン

終了

設定	記述
グループ ID	本 Edge Of Network Nodes が属するグループを識別するための ID です。
Edge node ID	本 Edge Of Network Node を識別するための ID です。
DDATA 最小時間	データに変化があったと検知すると、新しい DDATA (Device DATA) メッセージを送信する前の最小待ち時間です。
QoS	<p>MQTT は 3 レベルの信頼性を提供します。即ち QoS(キューオーエス)のことです。メッセージ配布の信頼性はメッセージが確実に届くのかを決めます。</p> <p>0: 最高一回：メッセージを一回だけ配布するが、確実に届くかは保証しません。</p> <p>1: 最低一回：メッセージは最低一回届きます。</p> <p>2: 正確に一回：メッセージは正確に一回届きます。</p>

装置の設定



設定

記述

グループを新規作成

タグを管理するため、グループを新規作成します。

タグを新規作成

本 EoN Node の MQTT Engine に監視されるタグを新規作成します。空白ではいけません。

削除

既存のグループまたはタグを削除します。

設定

既存のグループまたはタグを設定します。



このアイコンをクリックし、サンプルプロジェクトをダウンロードしてください。サンプルプロジェクトをダウンロードする前、インターネットケーブルが接続しているのを確認してください。

42.2. OPC UA サーバー

42.2.1. 概要

OPC UA(Unified Architecture)はファクトリーオートメーション業界での通信規格です。データの通信がプラットフォームに限られない、アクセス機構が統一、通信の標準化及びセキュリティ認証機構などの特長を持っています。cMT シリーズ HMI は OPC UA のサーバーの役目に相当し、OPC UA クライアント(Client)ソフトウェアで HMI、或いは PLC 上のアドレスタグ情報を読み取ることで、情報の垂直統合が求められます。

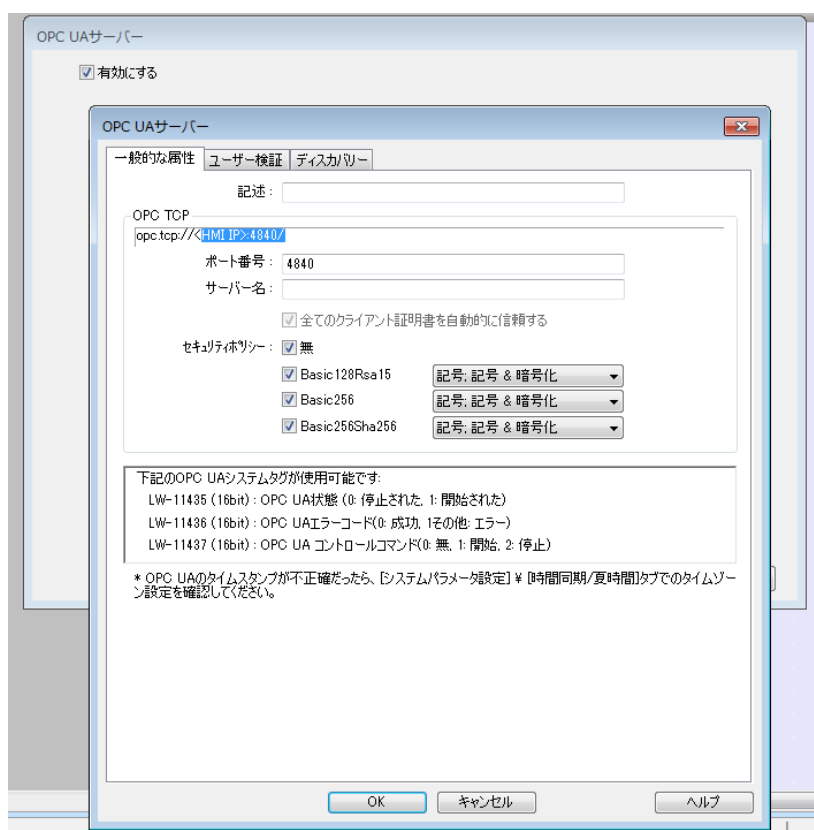
ソフトウェア・ハードウェア要件：

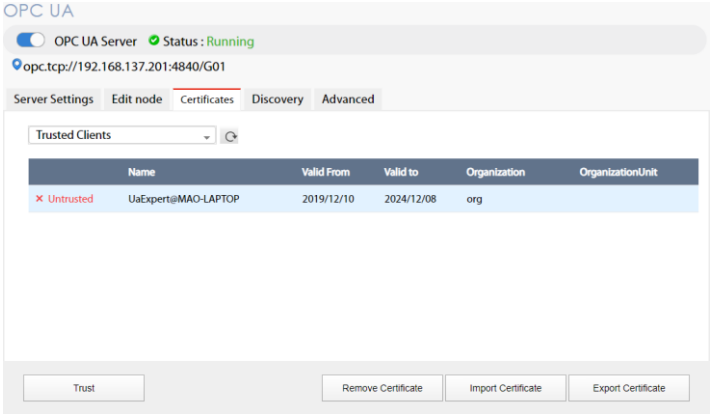
- 対応機種：cMT シリーズ。cMT-SVR / cMT-SVR-200 及び cMT-HDM / cMT-FHD は別途ライセンスをロードする必要があります。
- ソフトウェア：Easy Builder Pro v5.06.01 以降
- 推奨 OPC UA クライアント：Unified Automation UaExpert

42.2.2. 設定

ツールバーの[オブジェクト]をクリックし、そして[IIoT] » [OPC UA サーバー]をクリックして本オブジェクトを新規作成してください。有効にしたら、設定ダイアログボックスが現れます。

一般的な属性



設定	記述
記述	本オブジェクトに対する記述です。
OPC TCP	サーバーの URL ウェブアドレスです。
ポート番号	クライアント側に接続させるためのポート番号を設定します。デフォルトは 4840 です。
サーバー名	<p>サーバー名を設定します。空白にしてもいいです。</p> <p>全てのクライアント証明書を自動的に信頼する</p> <p>本項はデフォルトで有効にされ、cMT Gateway でのみ無効にすることができます。本項を有効にしていない場合、下図に示されたとおり、全ての OPC UA クライアントは OPC UA ウェブインタフェースで「信頼する証明書」に設定されていない限り、接続が全部拒否されます。</p>  <p>注意：OPC UA の規則により、セキュリティポリシーに [無] を選択した場合以外、OPC UA クライアントが OPC UA サーバーに接続するにはクライアント証明書を使用する必要があります。その証明書は OPC UA サーバーに正当性を検査されます。</p>
セキュリティポリシー	OPC UA が提供するセキュリティポリシーと、クライアントで選択可能な暗号化演算方法です。

ユーザー検証



設定

方式

記述

匿名

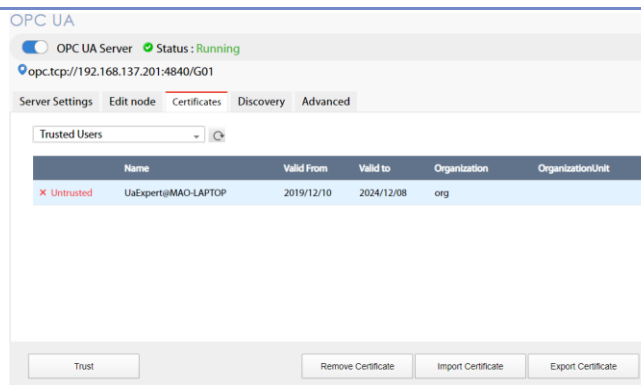
クライアントソフトウェアが匿名でログインした時、データアクセス(閲覧/読み取り/書き込み)の権限を設定します。

ユーザー名&パスワード

HMI のユーザー名&パスワードと共有しています。クライアントソフトウェアでログインした後、データアクセスの権限はレベルで分けられます。

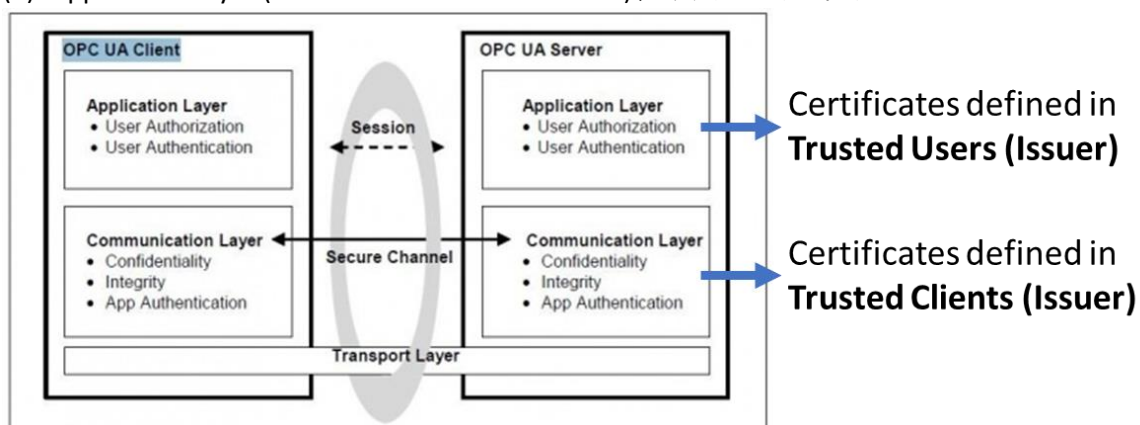
証明書

本項は cMT Gateway にのみ対応しています。OPC UA クライアントはユーザー名&パスワードでなく、証明書でログインすることができます。ウェブインタフェースで信頼する/しない証明書を設定します。下図を参考してください：



Note

- OPC UA のセキュリティレイヤーは以下のように分けられています：
 - (1) Communication Layer (通信レイヤー、例えば：セキュリティ)
 - (2) Application Layer (アプリケーションレイヤー)、下図をご参考ください：



セキュリティレイヤーの詳細については、次のリンクの説明をご参考ください：

(<http://wiki.opcfoundation.org/index.php/File:SecurityLayers.jpg>)

- クライアント検証は通信レイヤーに位置します。[無]以外のセキュリティポリシーを使用した場合、証明書が必須です。
- ユーザー検証はアプリケーションレイヤーに位置します。ログインの方法の1つとして、ユーザー証明書を使用してログインすることができます。

ディスカバリー(Discovery)設定



ネットワーク内で複数の OPC UA サーバーがある場合、OPC UA サーバーをディスカバリーサーバー(Discovery Server)に登録すれば、OPC UA クライアント側で Local Discovery Server (略称 LDS) を通じて OPC UA サーバーを探し出すことができます。

設定	記述
IP	OPC UA クライアント側の IP です。
ポート番号	OPC UA Client 側のポート番号です。
サーバー名	OPC UA Client 側のサーバー名です。
記述	備考として使用され、通信に影響を与えません。

例

以下の手順でどのようにディスカバリー機能を設定すればいいかを説明します：

1. まず、Local Discovery Sever（以下は LDS と称する）をインストールします。以下のウェブページで OPC UA 協議会が提供した LDS ファイルをダウンロードすることができます。

<https://opcfoundation.org/developer-tools/developer-kits-unified-architecture/local-discovery-server-lds/>

他のサードパーティーLDS ファイルを使用することも可能です。

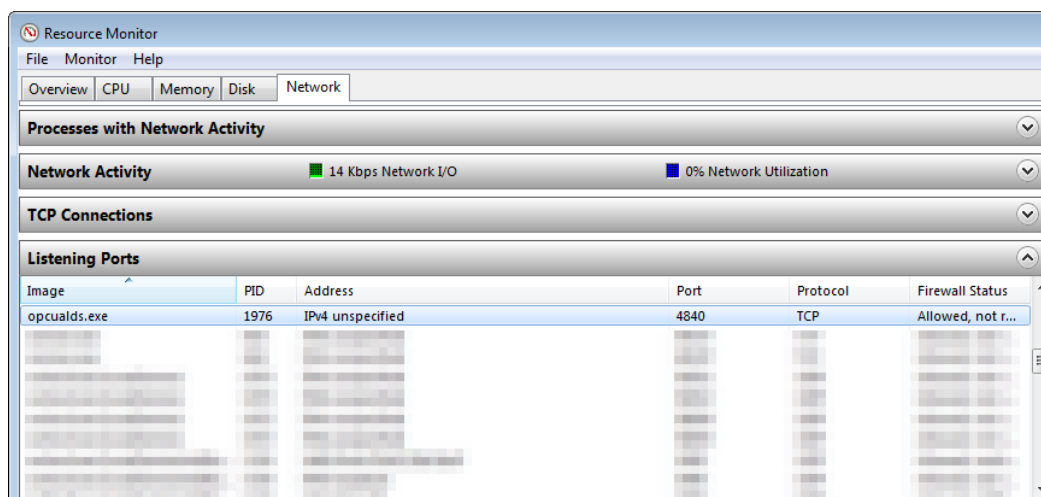
2. HMI が接続したルーターが HMI Name を識別できなかったら、HMI の名前を現在 HMI の IP

アドレス(もしくは 0.0.0.0 に変更してから、own certificate を再作成)に変更してください。
例えば: HMI の IP は 192.168.1.100 の場合、HMI の名前を 192.168.1.100 或いは 0.0.0.0 にしてください。

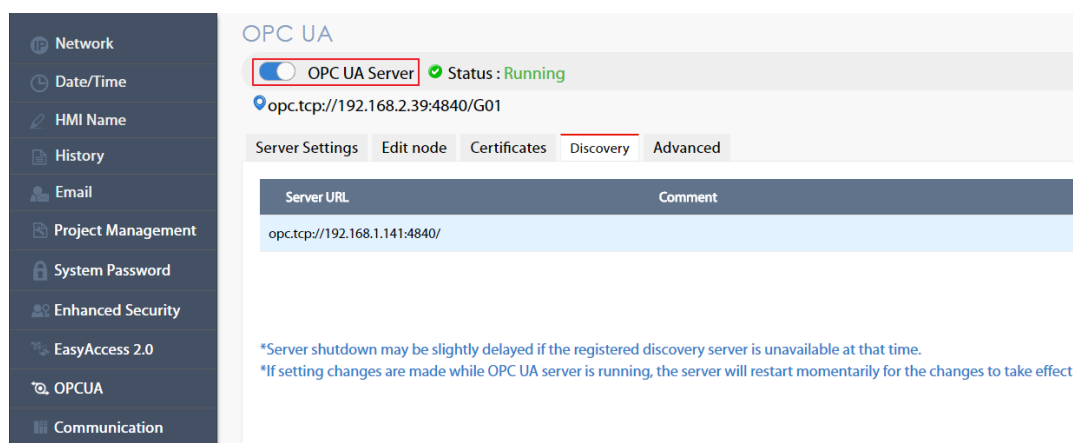
3. OPC UA サーバー実行後、C:\ProgramData\OPC Foundation\UA\pki\rejected\certs 内の Certificate を C:\ProgramData\OPC Foundation\UA\pki\trusted\certs にコピーしてください。
4. OPC UA クライアントソフトウェアを起動し、HMI の IP を入力するか、LDS Endpoint を使用することでディスカバリー機能を実行すれば、迅速に HMI の OPC UA サーバーに接続することができます。

ディスカバリー機能が正常に使用されない場合、以下の項目を確認してください：

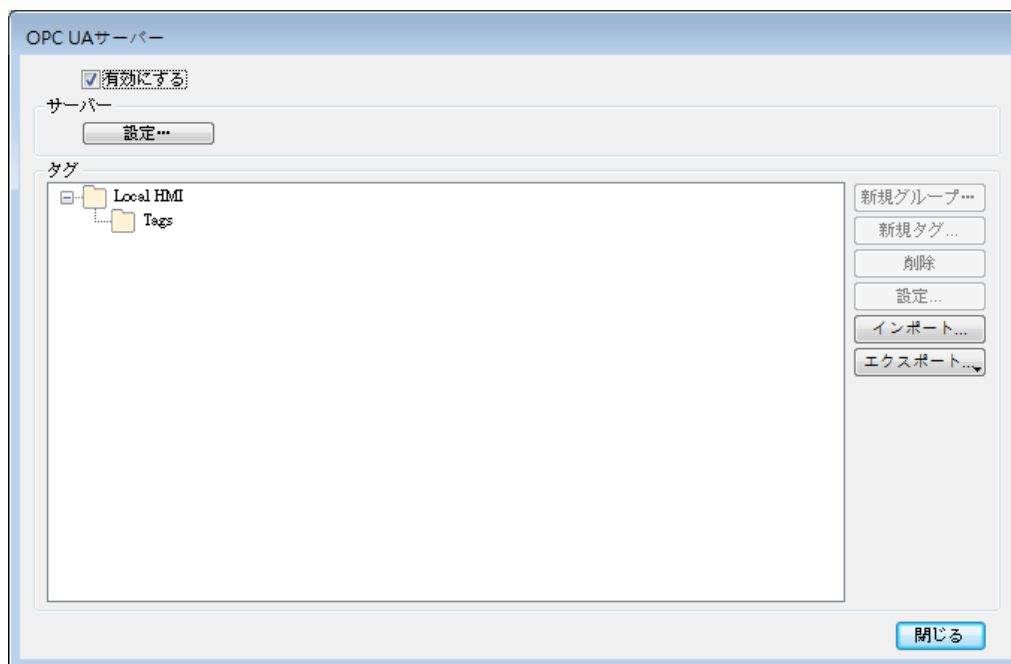
1. タスク マネージャーの起動 » [パフォーマンス] » [リソース モニター] » [ネットワーク] » [リッスンポート]でopcualds.exe が使用するポート番号を確認します。下図に示されたとおり、現在この PC の opcualds.exe が使用しているポート番号は 4840 です。



2. ウェブブラウザで HMI の IP を入力し、そしてパスワードを入力してログインします。[OPC UA] 設定ページで改めて OPC UA サーバーを起動します。注: 本 OPC UA タブは、cMT Gateway にのみサポートされます。注: 本 OPC UA タグは cMT Gateway にのみサポートされます。



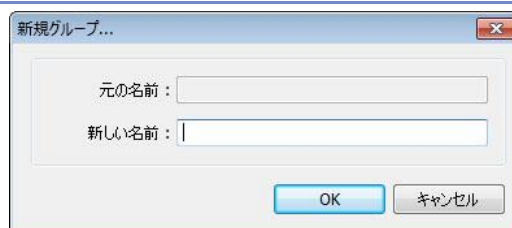
タグ設定



設定

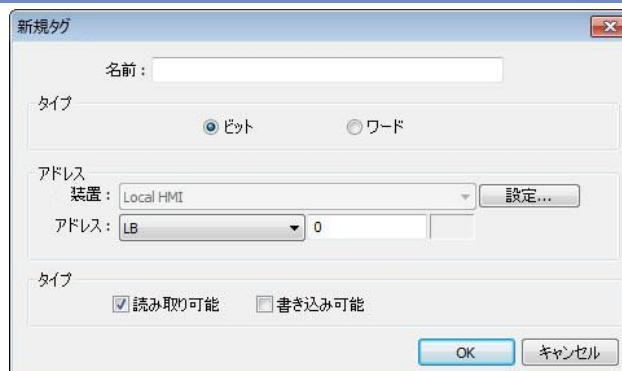
記述

新規グループ



タグを管理するために、グループを新規追加します。

新規タグ



クライアント側で監視・操作するタグを新規追加します。ここで本アドレスに書き込めるかを選択し、書き込む名前は空白にしてはいけません。

履歴(HDA)

OPC UA の HDA 機能を有効にします。


削除

既に存在しているグループ、或いはタグを削除します。

設定	既に存在しているグループ、或いはタグを設定します。
インポート	前に作成したタグをインポートします。*.xlsx、*.xls、*.csv、*.xml ファイルをインポートできます。
エクスポート	現在作成したタグをエクスポートします。Excel、または XML フォーマットにエクスポートできます。

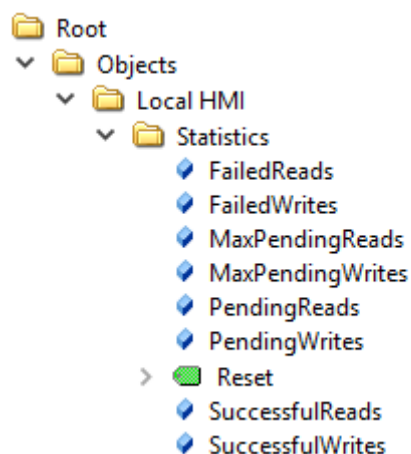
Note

- プロジェクトを HMI にダウンロードする前、まずは HMI の時刻及びタイムゾーンの設定が正確なのかを確認してください。それはクライアントソフトウェアが通信する際、検証時刻エラーで検証に失敗し、OPC UA サーバーに接続できないのを避けるためです。

 このアイコンをクリックし、チュートリアルビデオを閲覧してください。閲覧する前に、インターネットケーブルが接続しているのを確認してください。

42.2.3. 装置統計資料

装置の通信統計資料は、各装置 **Statistics** ノードで見つかります。下図をご参照ください：



各ノードの意味は以下の通りです：

ノード名	意味
FailedReads	失敗した読み取りコマンドの個数です。0 でない場合、通信に失敗した可能性があります。
FailedWrites	失敗した書き込みコマンドの個数です。0 でない場合、通信に失敗した可能性があります。
MaxPendingReads	発生した最大の読み取り待ちのコマンドの個数です。
MaxPendingWrites	発生した最大の書き込み待ちのコマンドの個数です。
PendingReads	読み取り待ちのコマンドの個数です。数値が長時間である程度の数量を維持することは、通信モジュールが全てのコマンドを処理しきれないと示しています。これで OPC UA ノードの更新を遅延させる可能性があります。極端な状況下、例えば長時間で 30 以上を維持する場合、OPC UA ノードがその期間内

	で更新されない可能性があります。
PendingWrites	書き込み待ちのコマンドの個数です。書き込みコマンドは読み取りコマンドより優先順位が高いため、本数値が長時間で高い場合、読み取りコマンドに影響します。
Reset	統計資料をリセットします。
SuccessfulReads	読み取りに成功したコマンドの個数です。
SuccessfulWrites	書き込みに成功したコマンドの個数です。

42.2.4. サポート及び制限

以下で OPC UA サーバーがサポートする機能及び制限を記します。

項目	記述
OPC UA Profile	Standard UA Server Profile には以下を含むが、これらに限定されません : <ul style="list-style-type: none"> * Core Server Facet * UA-TCP UA-SC UA-Binary * SecurityPolicy – None * Enhanced DataChange Subscription Server Facet * Standard DataChange Subscription Server Facet * Embedded DataChange Subscription Server Facet * User Token – X509 Certificate Server Facet * User Token – User Name Password Server Facet * Standard DataChange Subscription Server Facet * Embedded DataChange Subscription Server Facet 関連情報は Profile Reporting Visualization Tool by OPC Foundation をご参照ください。
Security policies	None Basic128Rsa15 Basic256 Basic256Sha256
最大 OPC UA ノード数	15 000
単一ノード最大配列長さ	255
読み取りキャッシュ	100ms (キャッシュは 100ms まで維持し、その後は改めて読み取る)
Client Session 数量	100

単一の Client Session が使用できる Subscription 個数	64
Publishing Interval 最小値	100ms
OPC UA HDA	<p>*最大 50 個までのノードアドレスをサポートします。 *各ノードアドレスは 10000 レコードのデータを記録できます。</p> <p>ノードアドレスの定義： 各 HDA を有効にしているノードは、その長さと同じのノードアドレスを使用すると視されます。データ型がストリングの場合、そのワード数に当たります。</p> <p>*HMI メモリーの空き容量が 10%より少なかった場合、新しいデータを保存するために、システムは空き容量が 10%以上になるまで、最初の HDA データから削除し始めます。</p>
パフォーマンス	
最大読み取りスループット (Security: None)	<p>内蔵レジスタ(例 : LW): 27000 words/second (WPS) MODBUS RTU@9600bps: 500 WPS MODBUS RTU@115200bps: 4000 WPS MODBUS TCP/IP: 10000 WPS</p> <p>テスト環境 EBPro version: V6.02.02.242 cMT-G02 OS version: 20180917 テストする時に、配列ノードを使用して読み取りの効率を最適化します。</p>

Note

OPC UA HDA ノードアドレスの例 :

仮に 50 個のノード(node1、node2、...、node 50)があり、各ノードが長さ=1 の bit アドレスにマッピングする場合、合計 50 個のノードアドレスを使用することになります。

もし 1 個のノードが長さ=50 の 16-bit Unsigned 整数配列(長さが 50 に設定された)にマッピングする場合、その配列の構造要素は個別に 1 個のノードアドレスに視され、当該ノードは 50 個のノードアドレスを使用することになります。

1 個のノードがワード数=50 のストリングにマッピングする場合、当該ノードは 50 個のノードアドレスを使用することになります。