JCCH・セキュリティ・ソリューション・システムズ

プライベートCA Gléas ホワイトペーパー

MQ Telemetry Transport （MQTT）での
クライアント証明書認証

Ver.1.0
2015 年 11 月

目次

1. はじめに

1.1. 本書について

本書では、弊社製品 プライベートCA Gléas で発行したクライアント証明書を利用して、MQ Telemetry Transport （MQTT）で接続する際にクライアント証明書による認証をおこなう環境を構築するための設定例を記載します。

本書に記載の内容は、弊社の検証環境における動作を確認したものであり、あらゆる環境での動作を保証するものではありません。弊社製品を用いたシステム構築の一例としてご活用いただけますようお願いいたします。

弊社では試験用のクライアント証明書の提供も行っております。検証等で必要な場合は、最終項のお問い合わせ先までお気軽にご連絡ください。

1.2. 本書における環境

本書は、以下の環境で検証をおこなっております。

- MQTTブローカー：Ubuntu 14.04 / Mosquitto 1.4.4
  以後、「ブローカー」と記載します
- JS3 プライベートCA Gléas（バージョン1.12.96）
  以後、「Gléas」と記載します
- MQTTパブリッシャー：
  Windows10 Pro / Mosquitto 1.4.4 （mosquitto_pub）
  以後、「パブリッシャー」と記載します
- MQTTサブスクライバー：
  Windows8.1 Pro / Mosquitto 1.4.4（mosquitto_sub）
  以後、「サブスクライバー」と記載します

以下については、本書では説明を割愛します。

- Mosquittoの基本的な設定や操作
- Gléasでのユーザ登録やクライアント証明書発行などの基本操作
- 各サーバ・クライアント端末におけるネットワーク設定など

これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱っている販売店にお問い合わせください。

1.3. 【ご参考】インストール手順

本書での環境におけるMosquitto(ブローカー)のインストール手順を記載します。
tar.gzパッケージはホームディレクトリに事前にダウンロードされているものとし、また以下手順に含まれるコマンドもインストールされているものとします。

■インストール

```
$ sudo apt-get install gcc make g++ libssl-dev libc-ares-dev libc-ares2
   uuid-dev
$ cd ~
$ tar zxvf mosquitto-1.4.4.tar.gz
$ cd mosquitto-1.4.4
$ make
$ sudo make install
```

■デーモン化

```
$ sudo vi /etc/init/mosquitto.conf
```

```
start on net-device-up
respawn
exec /usr/local/sbin/mosquitto -c /etc/mosquitto/mosquitto.conf
```

```
$ sudo initctl reload-configuration
```

2. ブローカーの設定

2.1. 各種証明書・失効リストの準備

次のファイルをブローカーにアップロードします。
ファイル名、アップロード先ディレクトリ共にサンプルとなります。本書では以下の名前であることを前提に記載します。

	ファイル名	アップロード先ディレクトリ名
CA 証明書	ia1.pem	/etc/mosquitto/ca_certificates/
サーバ証明書	cert.pem	/etc/mosquitto/certs/
サーバ秘密鍵	key.pem	/etc/mosquitto/certs/
失効リスト（CRL）	crl_ia1.pem	/etc/mosquitto/crls/

【CA 証明書】
Gléas では次の URL から取得します。
http://{Gléas のホスト名 or IP アドレス}/crl/ia1.pem
ダウンロード後、上記ディレクトリに配置します。

【サーバ証明書・秘密鍵】
Gléas からダウンロードしたサーバ証明書は PKCS#12 という形式になっているため、PEM 形式に変換・分離する必要があります。
※ここでは Gléas より取得したファイルを broaker.p12 というファイル名と仮定します
1） PKCS#12 ファイルより証明書を取得

```
$ openssl pkcs12 -in broaker.p12 -clcerts -nokeys -out cert.pem
```

2） PKCS#12 ファイルより秘密鍵を取得

```
$ openssl pkcs12 -in broaker.p12 -nocerts -nodes -out key.pem
```

取得したファイルを上記ディレクトリに配置します。
また、秘密鍵は mosquitto の実行ユーザをオーナーにし、パーミッションを 400 に変更します。

【失効リスト（CRL)】
Gléas では CRL ファイル（PEM 形式）は次の URL から取得できます。
http://{Gléas ホスト名 or IP アドレス}/crl/crl_ia1.pem
取得したファイルを上記ディレクトリに配置します。

本書の設定では、Gléas で証明書を失効してもブローカー上の CRL が自動的に更新されることはありません。新しい CRL が発行された後には既存の CRL と置き換える必要があります。
Gléas では CRL 更新用の ruby スクリプト（copycrl.rb）を準備しております。
corycrl.rb では、以下のとおりにすることで Gléas より CRL を取得・置換することが可能です。

```
$ ./copycrl.rb [CRL 取得 URL] /etc/mosquitto/crls/crl_ia1.pem
```

また CRL 更新後にはサービス再起動が必要になります。

```
$ sudo service mosquitto restart
```

2.2. 設定ファイルの編集

設定ファイル（本書環境では以下のファイル）に記述を追加します。

/etc/mosquitto/mosquitto.conf

```
cafile /etc/mosquitto/ca_certificates/ia1.crt
certfile /etc/mosquitto/certs/servercert.gleas.example.crt
keyfile  /etc/mosquitto/certs/servercert.gleas.example.key
crlfile /etc/mosquitto/certs/crl_ia1.pem
require_certificate true
use_identity_as_username true
```

証明書に関係する設定は以下の通りです。

※設定ファイルの詳細な説明はここではおこないません。man などをご参照ください

- cafile には、ルート証明書のファイルパスを設定します
- certfile には、サーバ証明書のファイルパスを指定します
- keyfile には、サーバ秘密鍵のファイルパスを指定します
- crlfileには、失効リストのファイルパスを指定します
- require_certificateには、trueを指定しクライアント証明書認証を有効にします
- use_identity_as_userをtrueにすると、クライアント証明書のサブジェクトCNをログインユーザ名として扱うようになります

2.3. ブローカーの起動

Mosquitto を起動します。

```
$ sudo service mosquitto start
```

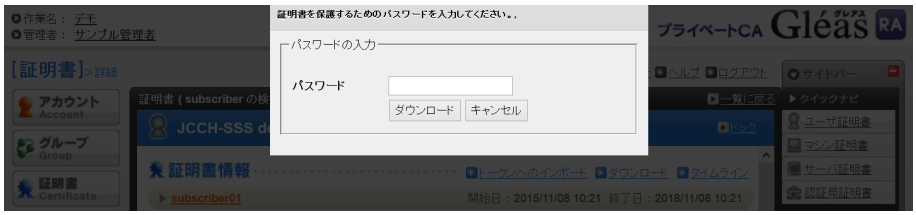
※既に起動している場合は、restart を指定します

以上でブローカーの設定は終了です。

3. Gléas からの証明書の取得

Gléas の RA から発行済み証明書をダウンロードします。
RA に管理者ログインし、大メニュー[証明書]よりサブスクライバー用の証明書を検索します。

証明書詳細画面より[ダウンロード]リンクをクリックし、証明書ファイル（*.p12）をダウンロードします。



1.2 項でサーバ証明書ファイルを証明書と秘密鍵に分離したのと同様にクライアント証明書も分離し、サブスクライバーに配置します。

パブリッシャーにも同じ手順で、証明書を配置します。

Gléasでは、管理者用コマンドラインインターフェースから makeiso コマンドを使って、クライアント証明書を一括ダウンロードすることも可能です。詳細は最終章の問い合わせ先までお問い合わせください。

4. 機器間でのメッセージ送受信

4.1. サブスクライバーの接続

クライアント証明書を指定してブローカーに接続します。
※ここではトピックを topic/test01 とします
> mosquitto_sub -h［ブローカーのホスト名或いは IP アドレス］-t "topic/test01" --cafile［ルート証明書ファイル］--cert［クライアント証明書ファイル］--key［クライアント秘密鍵ファイル］

接続に成功すると、待ち受け状態になります。

4.2. パブリッシャーからのメッセージ送信

クライアント証明書を指定してブローカーに接続しメッセージを送信します。
> mosquitto_pub -h［ブローカーのホスト名或いは IP アドレス］-t "topic/test01" -m "送信メッセージ" --cafile［ルート証明書ファイル］--cert［クライアント証明書ファイル］--key［クライアント秘密鍵ファイル］

送信成功すると、サブスクライバーにメッセージが表示されます。

5. 問い合わせ

■Gléasに関するお問い合わせ先
株式会社JCCH・セキュリティ・ソリューション・システムズ
Tel: 050-3821-2195
Mail: sales@jcch-sss.com