JP-LINK Security Server インストールガイド

バージョン 1.1.0

目次

はじめに

1.1 Security Server とは

Security Server は、JP-LINK を利用する上で、各組織で最低一つずつインターネット接続部 に必要となるメインモジュールです。ACL の設定、ログの保存、セキュアな通信を実現します。 Security Server は、パブリックインターネットと組織内ネットワークの情報システムに接続され、 リクエストの証拠能力を担保した上で、クライアントとサービスプロバイダーの間のメッセージ 交換を保護します。

1.2 対象読者

本書は、JP-LINK への参加に必要な Security Server のインストール・操作・管理を行う Security Server システム管理者を対象としています。

1.3 必要な技能

本書は、Linux サーバーの管理、コンピューターネットワーク、および Security Server または X-Road の動作原理について中級程度の知識をお持ちの方を対象としています。

1.4 システム要件

Security Server でサポートされるプラットフォームは以下の通りです。

1.4.1 サポートされるプラットフォーム

オペレーティングシステム	Ubuntu 20.04 or 22.04 LTS (x86-64) Red Hat Enterprise Linux (RHEL) 7.3 and 8
CPU ＊	2 Core(or More)
RAM	4 GB(or More)
ディスク空き容量	OS パーティション 10GB 他パーティション(/var 配下) 20GB 以上

＊CPU につきましては、64bit dual core の Intel, AMD,またはその互換性のある CPU、且つ AES 対応しているものを推奨します。

1.4.2 ネットワーク要件

受信 – 受信用ポート(外部ネットワークから Security Server へ) Inbound ports from external network

ポート	用途
TCP 5500	Security Server 間のメッセージ交換
TCP 5577	Security Server 間の OCSP (Online Certificate Status Protocol)応答のクエリー

送信 – 送信用ポート(Security Server から外部ネットワークへ) Outbound ports to external network

ポート	用途
TCP 5500	Security Server 間のメッセージ交換
TCP 5577	Security Server 間の OCSP (Online Certificate Status Protocol)応答のクエリー
TCP 4001	中央サーバーとの通信
TCP 80	グローバル設定のダウンロード
TCP 80、443	一般的な OCSP およびタイムスタンプサービス

受信 – ローカルアクセス Inbound ports from internal network

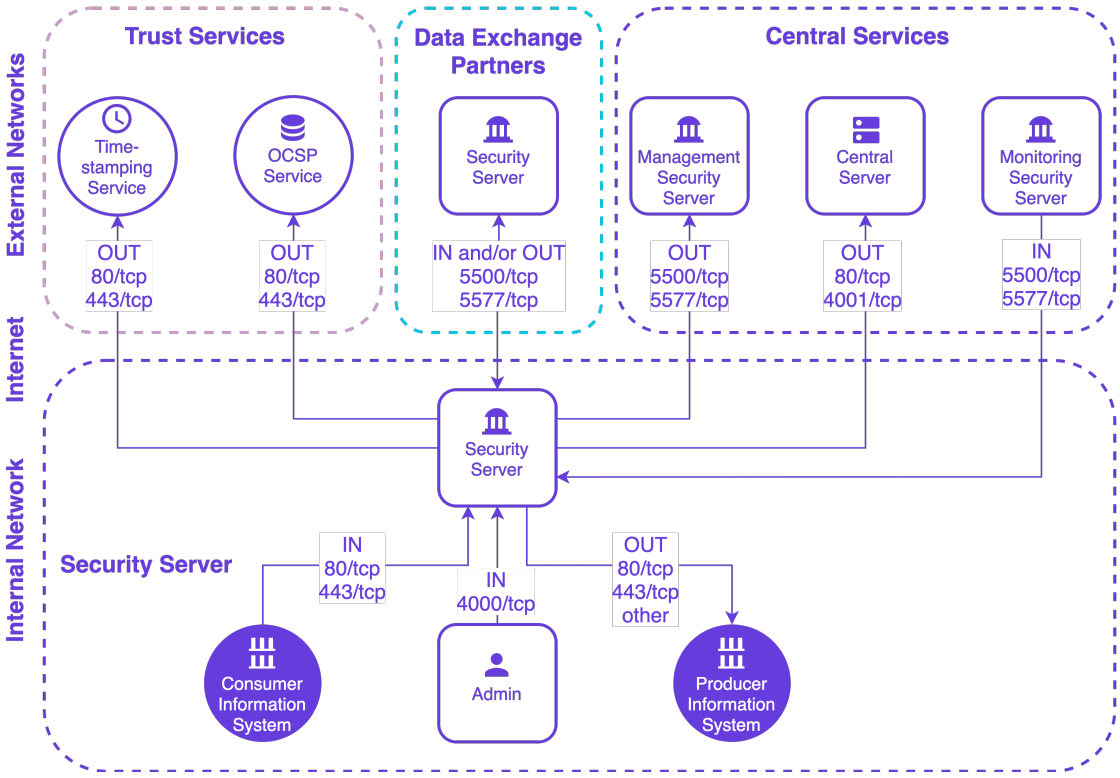
ポート	用途
TCP 4000	Security Server の WEB ユーザーインターフェースへのアクセス
Ubuntu TCP 80、443	情報システムからの接続
RHEL TCP8080/8443	情報システムからの接続

送信 – ローカルアクセス Outbound ports to internal network

ポート	用途
Ubuntu TCP 80、443	情報システムからの接続
RHEL TCP 8080/8443	情報システムからの接続
TCP 2080	Security Server と operational data monitoring daemon との通信
TCP 80/8085/8003	Adapter Server との通信

1.4.2 ネットワーク要件ネットワークダイアグラム Network Diagram（Ubuntu の場合）

※RHEL の場合は、上記ポート一覧から対応するところを読み替えてください。



2.インストール

2.1 事前準備（Ubuntu の場合）

2.1.1 ホスト名の設定

ホスト名の設定を行います。[/etc/hosts] ファイルの[127.0.0.1]に任意のホスト名を設定します。
[/etc/hosts]ファイルに下記設定が記述されていれば問題ありません。

```
$ cat /etc/hosts
127.0.0.1 {your-host-name-here}
```

2.1.2 ユーザーの追加

Security Server の管理ユーザーを登録します。
Password その他の情報は任意の値を設定してください。

```
$ sudo adduser {your-secuiry-server-admin-username}
```

2.1.3 Locale

Locale を[en_US.UTF-8]に設定してください。次の行を/etc/environment に追加します。

```
$ LC_ALL=en_US.UTF-8
```

2.1.4 パッケージリポジトリサーバーの登録

X-road のパッケージリポジトリを追加してください。下記コマンドは途中で改行を挟まず、1 行で入力してください。

```
$ sudo apt-add-repository -y "deb https://artifactory.niis.org/xroad-release-deb $(lsb_release -sc)-current main"
```

2.1.5 リポジトリの署名鍵の登録

X-road の apt-key を追加してください。 X-Road リポジトリの署名キーを信頼できるキーのリストに追加します。下記コマンドは途中で改行を挟まず、 1 行で入力してください。

```
$ curl https://artifactory.niis.org/api/gpg/key/public | sudo apt-key add -
```

2.1 事前準備（RHEL の場合）

2.1.1 ホスト名の設定

ホスト名の設定を行います。[/etc/hosts] ファイルの[127.0.0.1]に任意のホスト名を設定します。
[/etc/hosts]ファイルに下記設定が記述されていれば問題ありません。

```
$ cat /etc/hosts
127.0.0.1 {your-host-name-here}
```

2.1.2 Locale

Locale を[en_US.UTF-8]に設定してください。次の行を/etc/environment に追加します。

```
$ LC_ALL=en_US.UTF-8
```

2.1.3 パッケージリポジトリサーバーの登録

yum と統合してそのネイティブ機能を拡張するユーティリティのコレクションをインストールします。

```
$ sudo yum install yum-utils
```

X-Road パッケージリポジトリと Extra Packages for Enterprise Linux (EPEL) リポジトリを追加します。

```
$ RHEL_MAJOR_VERSION=$(source /etc/os-release;echo ${VERSION_ID%.*})
sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-
${RHEL_MAJOR_VERSION}.noarch.rpm
sudo yum-config-manager --add-repo https://artifactory.niis.org/xroad-release-
rpm/rhel/${RHEL_MAJOR_VERSION}/current
```

2.1.4 リポジトリの署名鍵の登録

X-Road リポジトリの署名鍵を信頼できる鍵のリストに追加します

```
$ sudo rpm --import https://artifactory.niis.org/api/gpg/key/public
```

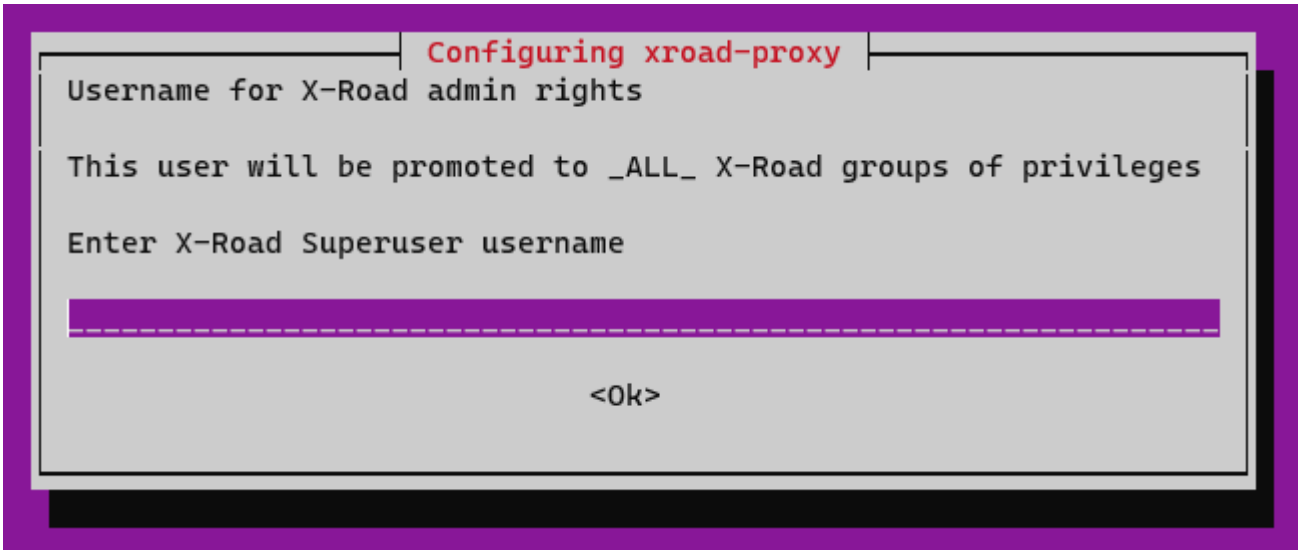
2.2 Security Server のインストール（Ubuntu の場合）

2.2.1 インストールコマンドの実行

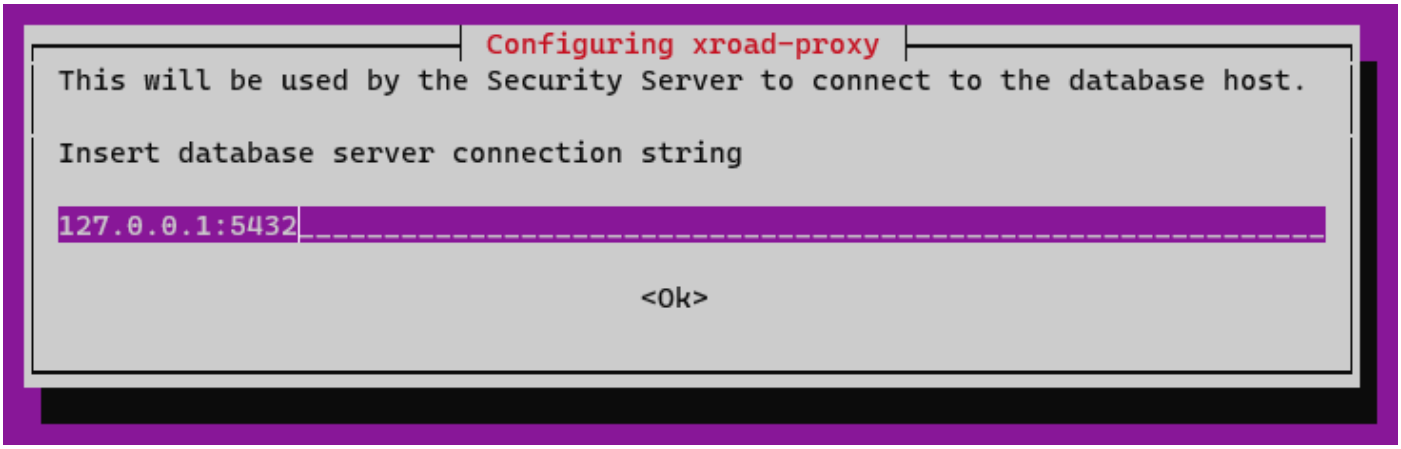
下記、パッケージリスト更新コマンド、およびインストールコマンドを実行してください。

```
$ sudo apt-get update
$ sudo apt-get install xroad-securityserver
```

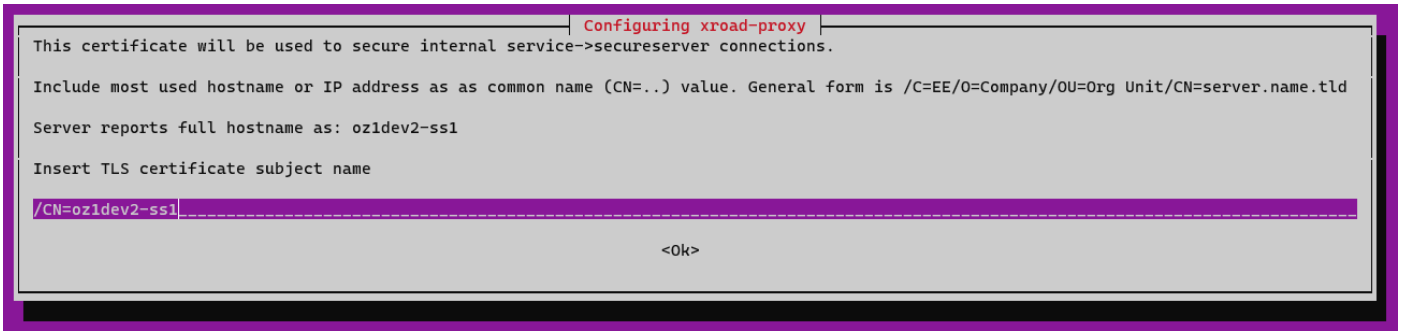
以下の管理者ユーザーを指定する画面が表示されたら、2.1.2 にて作成したユーザーを指定して、<OK>ボタンを押下します。



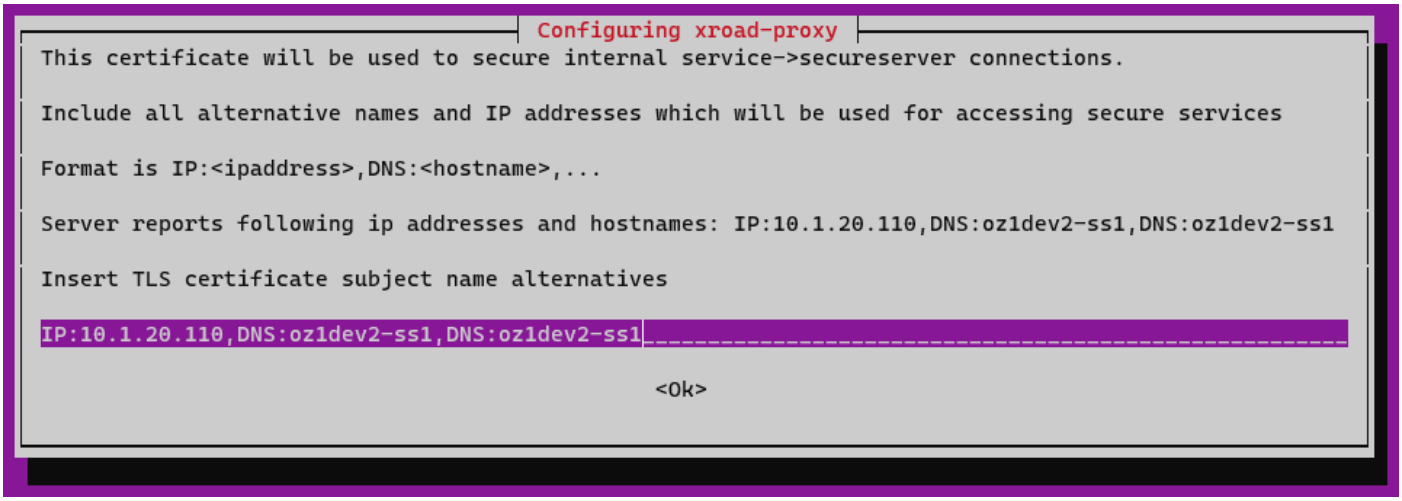
Security Server の設定情報などを保管する DB の IP アドレス及びポート番号を入力します。
デフォルトでは PostgreSQL が Security Server と同じタイミングでインストールされるので、デフォルトの内容(127.0.0.1:5432)のままで OK です。



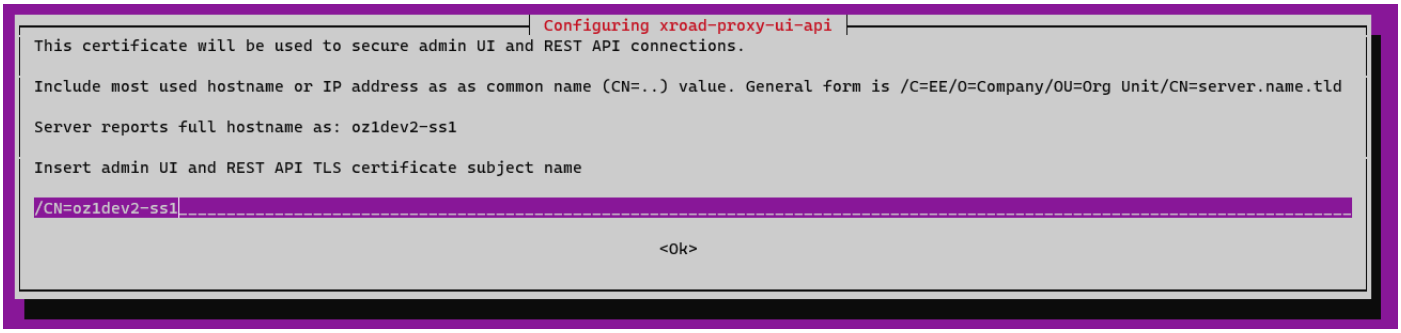
WEB インターフェースの管理画面で使用される証明書の Common Name(CN)を入力します。
アクセスする際に使用する IP アドレス、またはホスト名(DNS)を設定します。
ここでは CN(Common Name)設定は、/CN=以降をいったんすべて消去し、/CN={DNS 名}または/CN={グローバル IP アドレス}を設定ください。例：/CN=XX.XX.XX.XX
＊本設定は 63 字以下に設定する必要があります。



次に上記設定における Subject Alternate Names(SANs)を入力します。
CN とは異なる IP、またはホスト名を指定します。
SANs(Subject Alternate Names)設定も IP:以降をいったんすべて消去し、IP:{グローバル IP アドレス}をご設定ください。例：IP:XX.XX.XX.XX
＊本設定は 63 字以下に設定する必要があります。

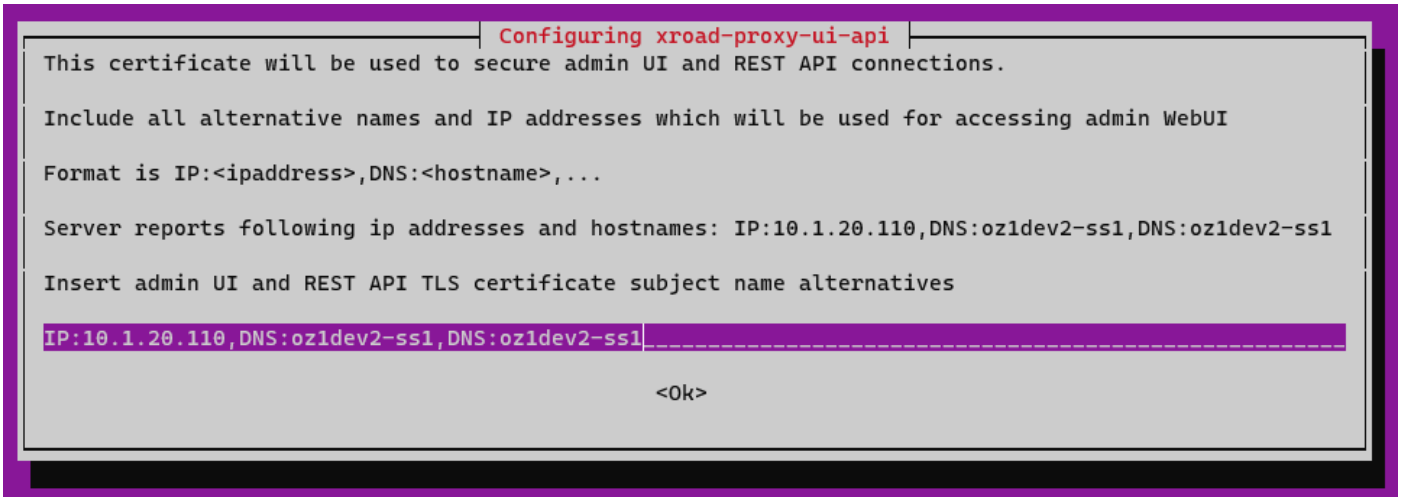


Security Server に対してリクエストを送る組織内のクライアントから Security Server にアクセスする際に使用される証明書の CN を入力します。
使用する IP アドレス、またはホスト名(DNS)を設定してください。
ここでも/CN=以降をいったんすべて消去し、/CN={DNS 名}または/CN={グローバル IP アドレス}を設定ください。
＊本設定は 63 字以下に設定する必要があります。



次に上記設定における Subject Alternate Names(SANs)を入力します。
CN とは異なる IP、またはホスト名を指定します。
＊本設定は 63 字以下に設定する必要があります。

!!注意!!:ここで設定するグローバル IP はインストール後変更する手段がありません。グローバル IP は予めて、固定化するようお願いします。



2.2 Security Server のインストール（RHEL の場合）

2.2.1 インストールコマンドの実行

※Ubuntu と異なり、インストール中に各種情報の入力は求められません。インストール確認のための質問はありますので、内容を確認の上、インストールを進めてください。

```
$ sudo yum install xroad-securityserver
```

ユーザインタフェースのすべてのロールが付与されているシステムユーザを追加します。
<ユーザー名>の箇所を任意の名称に置き換えてください。

```
$ sudo xroad-add-admin-user <ユーザー名>
```

セキュリティサーバを起動します。（インストール完了後、自動的に起動しないため）

```
$ sudo systemctl start xroad-proxy
```

2.3 確認（Ubuntu/RHEL 共通）

2.3.1 アプリケーションの稼働状況の確認

インストール完了後、サービスの稼働状況を確認します。
下記出力例と同様の結果が表示されれば問題はありません。

```
$ sudo systemctl list-units "xroad*"
```

<出力例>

```
UNIT                              LOAD   ACTIVE SUB     DESCRIPTION
xroad-addon-messagelog.service loaded active running X-Road Messagelog Archiver
xroad-base.service             loaded active exited  X-Road initialization
xroad-confclient.service       loaded active running X-Road confclient
xroad-monitor.service          loaded active running X-Road Monitor
xroad-proxy-ui-api.service     loaded active running X-Road Proxy UI REST API
xroad-proxy.service            loaded active running X-Road Proxy
xroad-signer.service           loaded active running X-Road signer
```

2.4 運用モニタリング機能の導入（Ubuntu/RHEL 共通）

運用モニタリング機能は、セキュリティサーバのメッセージ交換における統計情報を監視・管理する機能です。
各セキュリティサーバの稼働状況をセンター側で把握するために重要な機能のため、**必ず導入をお願いします。**
※収集されるデータは、通信のヘッダ情報（メタデータ）のみで、実際に行われたメッセージ交換のボディ情報（業務データ）は一切含まれません。

2.4.1 運用モニタリング機能のインストール

運用モニタリング機能をインストールするには下記コマンドを実行します。

Ubuntu の場合

```
$ sudo apt-get install xroad-addon-opmonitoring
```

RHEL の場合

```
$ sudo yum install xroad-addon-opmonitoring
```

インストール後の再起動／確認（Ubuntu/RHEL 共通）

運用モニタリング機能のインストール完了後、x-road-proxy サービスを再起動させます。

```
$ sudo service xroad-proxy restart
```

再起動完了後、プロセスの稼働確認します。

```
$ sudo systemctl list-units "xroad*"
```

次のサービスが実行されている必要があります。

```
UNIT                              LOAD   ACTIVE SUB     DESCRIPTION
xroad-addon-messagelog.service loaded active running X-Road Messagelog Archiver
xroad-base.service             loaded active exited  X-Road initialization
xroad-confclient.service       loaded active running X-Road confclient
xroad-monitor.service          loaded active running X-Road Monitor
xroad-proxy-ui-api.service     loaded active running X-Road Proxy UI REST API
xroad-proxy.service            loaded active running X-Road Proxy
xroad-signer.service           loaded active running X-Road signer
```

再起動後、ソフトトークンがログアウト状態になりますので、WEBUI 画面よりアクセスし、ソフトトークンの再ログイン(PIN の再入力)を実施してください。

3.初期設定

ここでは、Security Server のインストール及び稼働状況確認後に行う一連の初期設定について記載します。
Security Server の初期設定後の運用設定や詳細な設定などについては別途「Security Server ユーザガイド」を参照ください。

3.1 Security Server の初期設定において必要な情報

Security Server の初期設定を進めるうえで、JP-LINK のメンバー情報などを設定する必要があります。
データ・ファイルについては、OZ1 より連携するものと、お客様ご自身で設定していただく必要があるものとがあります。

3.1.1 参照ファイル・データ

OZ1 より提供するデータ・ファイル

#	参照データ	説明
1	＃開発検証環境用アンカーファイル {URL} ＃本番稼働環境用アンカーファイル {URL}	グローバル設定を取得するためのアンカーファイルです。利用したい環境ごとにファイルが異なります。 **OZ1 から通知されたものを設定ください。**
2	Security Server メンバークラス (Member Class) GOV：政府機関・公共機関 COM：民間企業・団体	Security Server の所有者のメンバークラスです。 **OZ1 から通知されたものを設定ください。**
3	Security Server メンバーコード (Member Code)	Security Server の所有者のメンバーコードです。 **OZ1 から通知されたものを設定ください。**

お客様ご自身で設定・入力する必要があるもの

#	参照データ	説明
4	Security Server の識別コード (Security Server Code)	Security Server を特定するための識別コードです。 事前に貴社管理内で一意に Security Server を識別できる英数字をご用意・ご検討していただく必要があります。 例）Dev-SS01, Prod-SS01 etc.
5	ソフトウェアトークンの PIN	ソフトウェアトークンの PIN 情報です。 大小英字を含む英数字 10 桁以上で入力ください。

3.1.2 初期設定

初期設定を行うには、インストールした Security Server が稼働していることを確認したうえで、Web ブラウザより下記 URL へアクセスする。{SECURITYSERVER}は、セキュリティサーバの IP 名または DNS 名です。
https：//{SECURITYSERVER}：4000/

3.1.3 初期設定の各段階で参照されるデータ

初回ログイン時

- グローバル設定アンカーファイル(3.1.1 #1)

設定情報ダウンロード後、初期設定時

- Security Server 所有者のメンバークラス(3.1.1 #2)
- Security Server 所有者のメンバーコード(3.1.1 #3)
- Security Server 所有者の Security Server コード(3.1.1 #4)
- ソフトウェアトークンの PIN(3.1.1 #5)
  ＊PIN は安全な場所に保管してください。万が一 PIN を紛失（失念）した場合、復元することはできません。

3.2 管理画面を開く

WEB ブラウザに以下の URL を入力し、アクセスしてください。
{SECURITYSERVER}は、セキュリティサーバの IP 名または DNS 名です。

https：//{SECURITYSERVER}：4000/

ネットワーク設定により、Security Server に対して 4000 番ポートに直接アクセスできない場合があります。
そのような場合には SSH トンネリング(ポートフォワーディング)を利用してアクセスを行ってください。
SSH トンネリング(ポートフォワーディング)を利用する場合、{SECURITYSERVER}には localhost と入力してください。
詳細なネットワーク設定については御社ネットワーク管理者へお問い合わせください。

以下は SSH トンネリング(ポートフォワーディング)を利用する場合のコマンドの一例になります。

$ ssh -L 4000:localhost:4000 **{user-name}@{securityserver-hostname or IP}** -i ~/.ssh/id_rsa -N

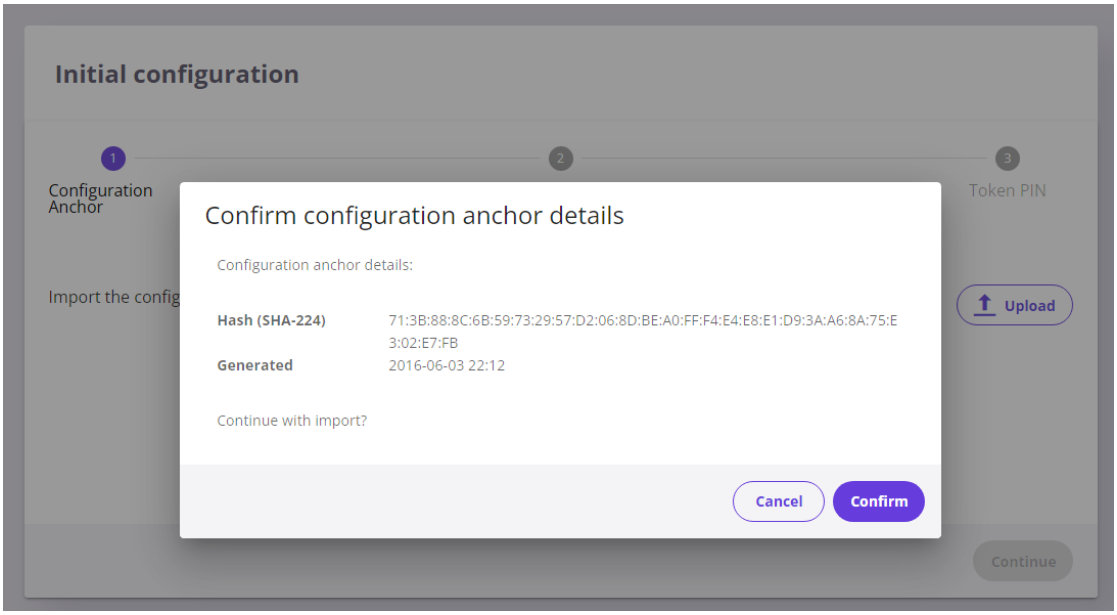
3.3 Security Server 管理画面へログイン

2.1.2 で設定した管理者ユーザーとしてログインします。

4.4 グローバル設定アンカーファイルのインポート

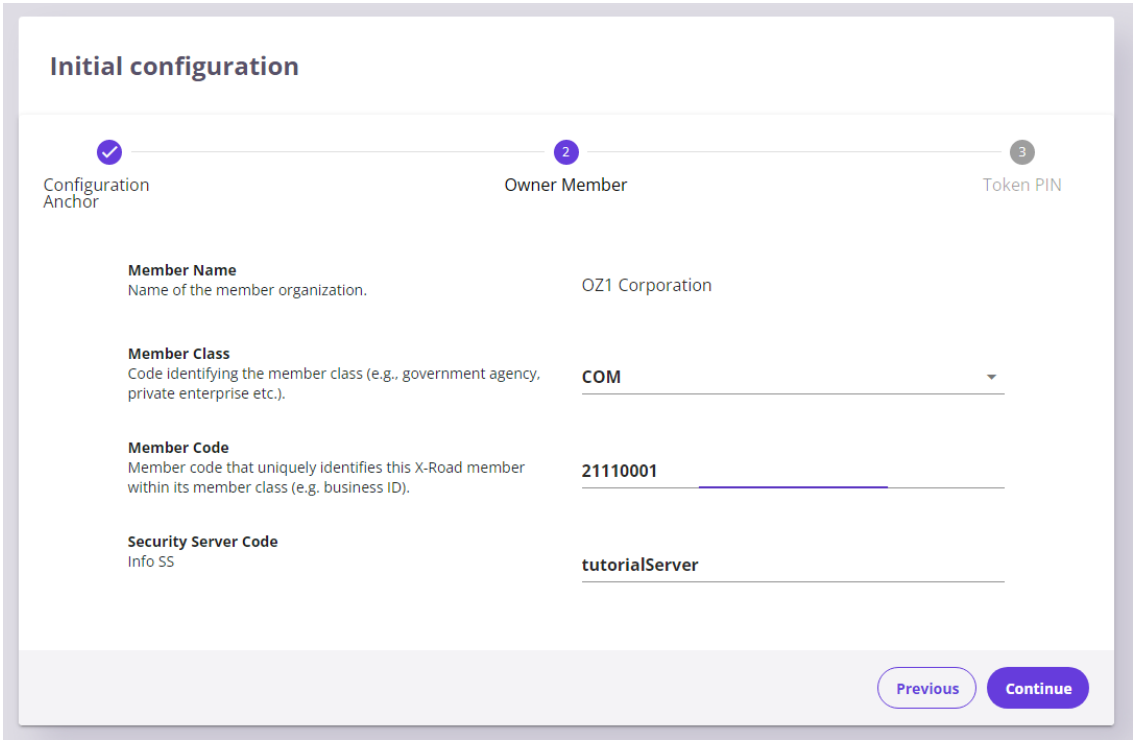
OZ1 社より提供するグローバル設定アンカーファイル(3.1.1 #1)をインポートします。
＊アンカーファイルは環境により本番環境向けと検証環境向けの 2 種類があります。
　誤ったアンカーファイルをインポートしないようご注意ください。

[Brose]ボタンを押下し、インポートするアンカーファイルを選択します。
その後、[Import]ボタンを押下します。
[ここに画像]
確認画面が表示され、インポートしたアンカーファイルに間違いがないか確認します。
確認後問題なければ、[Confirm]ボタンを押下します。

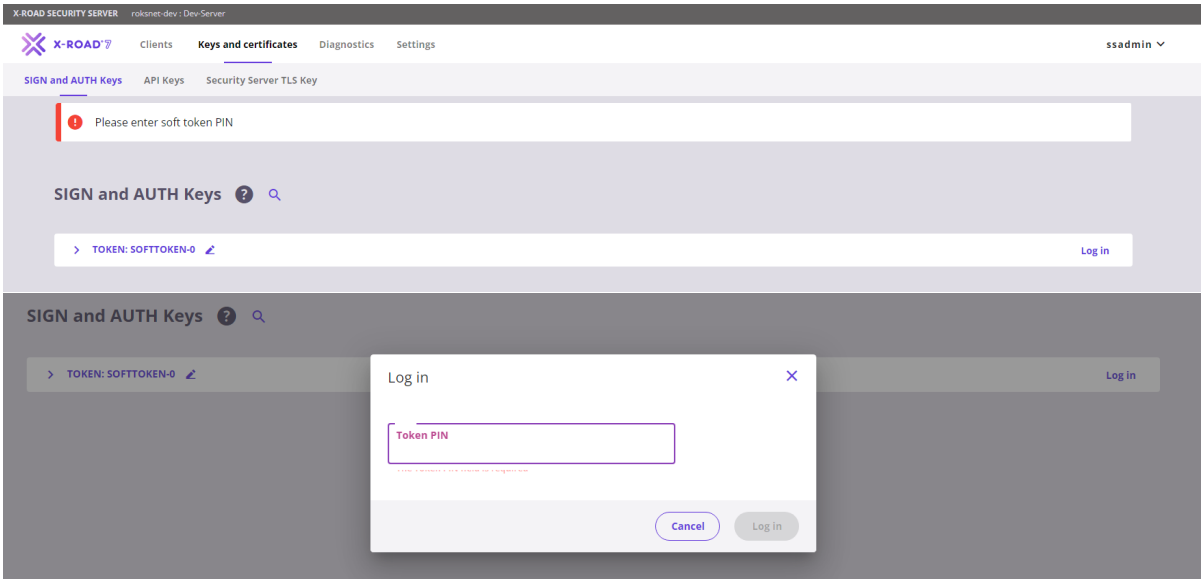


3.5 Security Server の初期設定

OZ1 社より提供するメンバーコード(3.1.1 #3)及びメンバークラス(3.1.1 #2)を入力してください。
正常にメンバーコード(3.1.1 #3)が入力され、認識されている場合、メンバー名（Member Name）欄にご自身のメンバー名が表示されます。



続いて、Security Server コード(3.1.1 #4)の入力を行ってください。
最後にソフトウェアトークンの PIN(3.1.1 #5)の設定を行います。
ページの上部にソフトトークンの PIN が入力されていないという警告メッセージが表示されます。赤いメッセージをクリックして PIN を入力します。または、[Keys and Certificate]メニューから、アクセスし、[Log in]テキストをクリックすることでも PIN の入力画面へ遷移できます。
＊PIN の入力は間違えないよう慎重に実行してください。万が一、紛失（失念）してしまった場合、復元することはできません。



確認画面が表示されたら、[OK]ボタンを押下します。

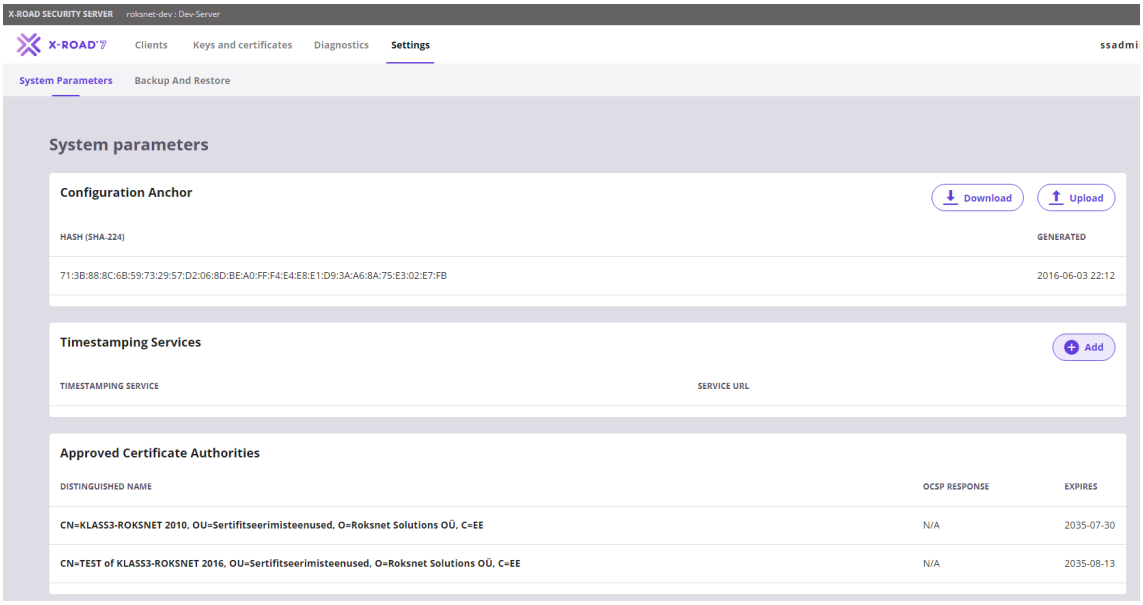
以上で、Security Server の初期設定は完了となります。

3.6 PIN の入力

Security Server の初回起動時、及び再起動後には PIN が未入力（認証未済）の状態となっています。
[Please enter softtoken PIN]を押下し、PIN を入力します。
＊PIN が未入力の状態では Security Server は、他の Security Server からのリクエストに対し、応答しません。

3.7 タイムスタンプサーバーの登録

タイムスタンプサーバーの登録を行います。
[System Parameter]を押下し、[Timestamping Services]の[Add]ボタンを押下します。

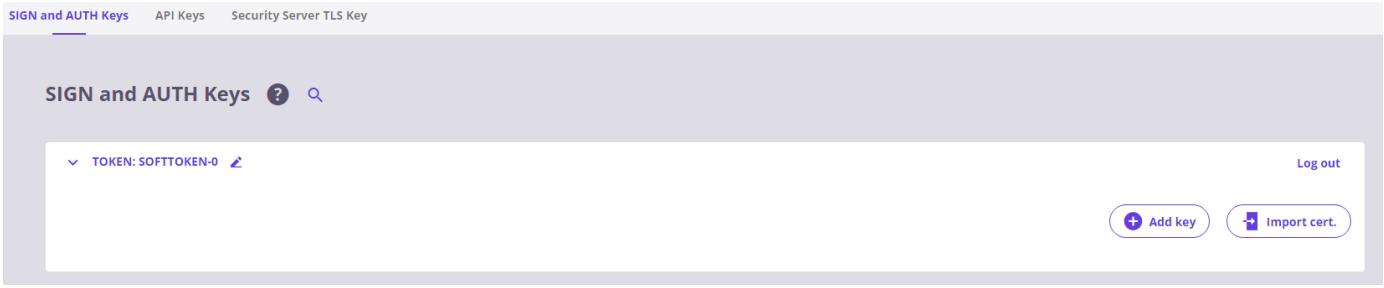


登録するタイムスタンプサーバーを選択し、[OK]ボタンを押下します。
指定するタイムスタンプサーバーは環境設定や用途により異なります。
ご不明の場合は OZ1 JP-LINK 担当までお問い合わせください。

開発検証環境	DEMO of ROKSNET TSA 2016
本番環境	ROKSNET TIMESTAMPING AUTHORITY

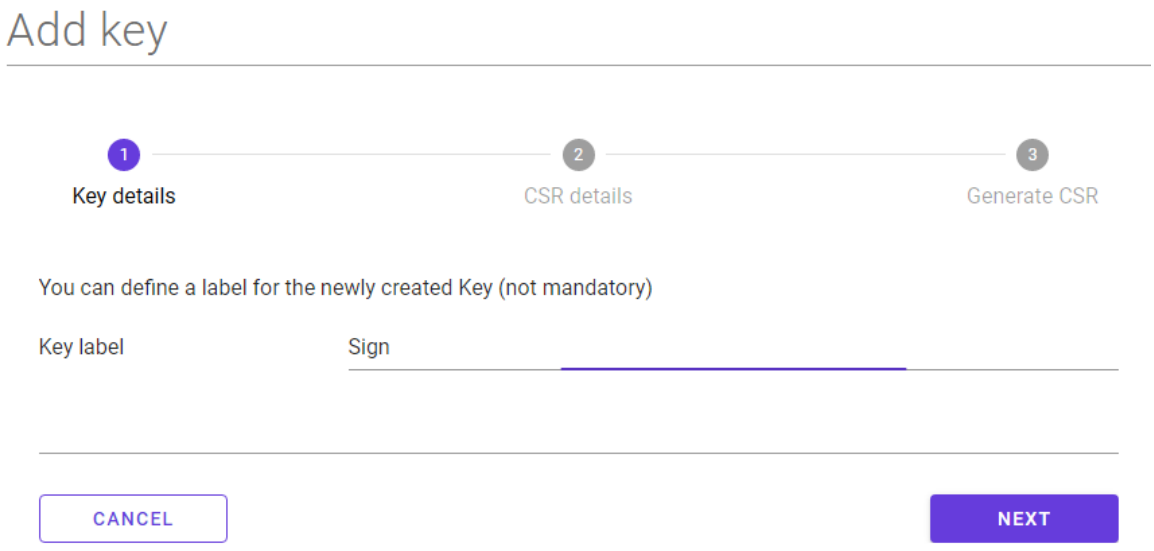
3.8 認証用及び署名用の秘密鍵の生成

[Key and Certificates]＞[softToken]を選択、[+Add Key]ボタンを押下し、AUTH キー（認証用）と SIGN キー（署名用）を生成します。



3.8.1 署名用秘密鍵の生成

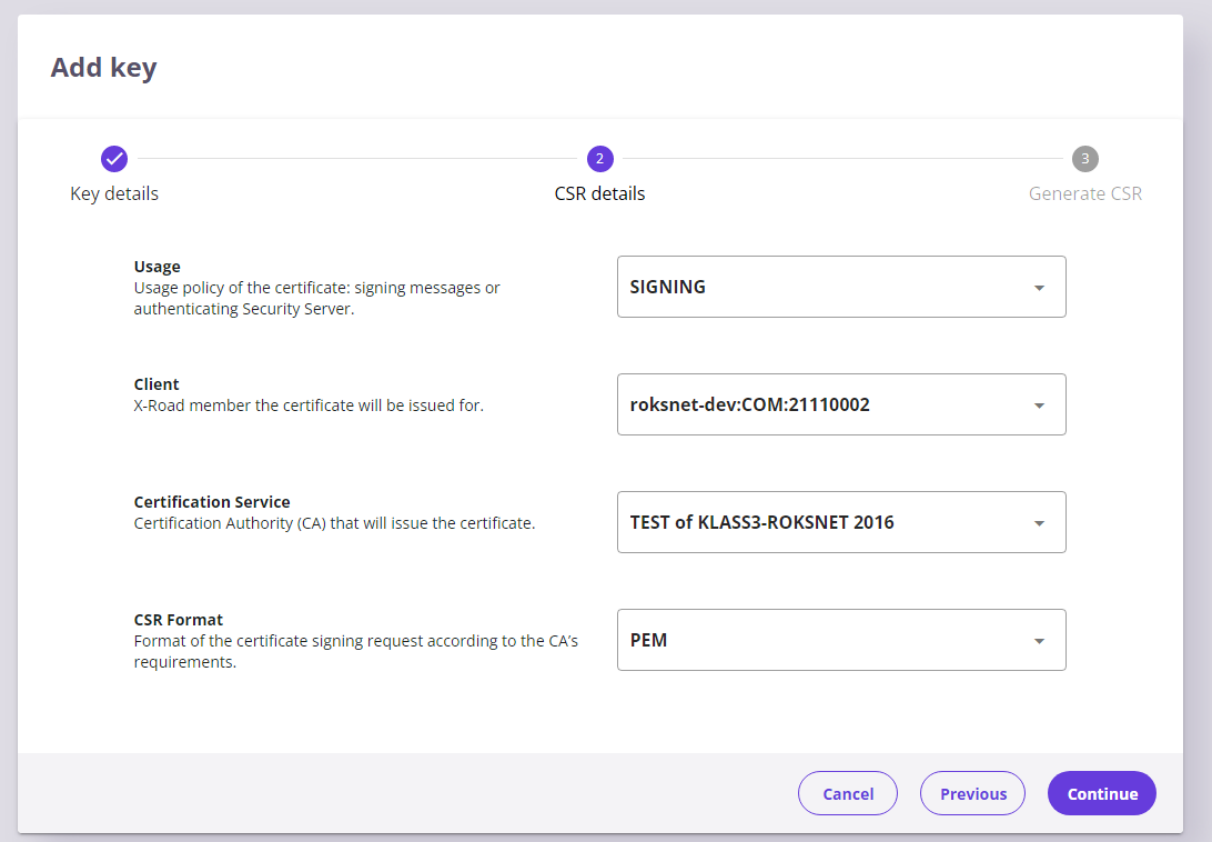
[+Add Key]ボタンを押下し、SIGN キー（署名用）を生成します。
Label は任意の値を入力してください。
＊認証用秘密鍵と署名用秘密鍵とで区別できること、及び署名用秘密鍵であることが誰の目にも分かるような名称にすることをお勧めします。
Key Label の例：Sign
当ガイドでは以下は、署名用秘密鍵の Label に[Sign]とした場合となります。



署名秘密鍵の登録後、署名用秘密鍵を選択し、[Generate CSR]ボタンを押下し、CSR の生成を行います。
入力内容は下記を参考に選択・入力してください。

Usage	SIGNING
Client	自身の Security Server を示す値 **{X-Road Instance}:{Member Class}:{Member Code}:***
Certification Service	利用環境により異なります。 ご不明の場合は OZ1 JP-LINK 担当までお問い合わせください。

	開発検証環境：**TEST of KLASS3-ROKSNET 2016** 本番環境：**Roksnet KLASS3-ROKSNET 2017 CA**
CSR Format	PEM ※必ず PEM 形式を選択してください。

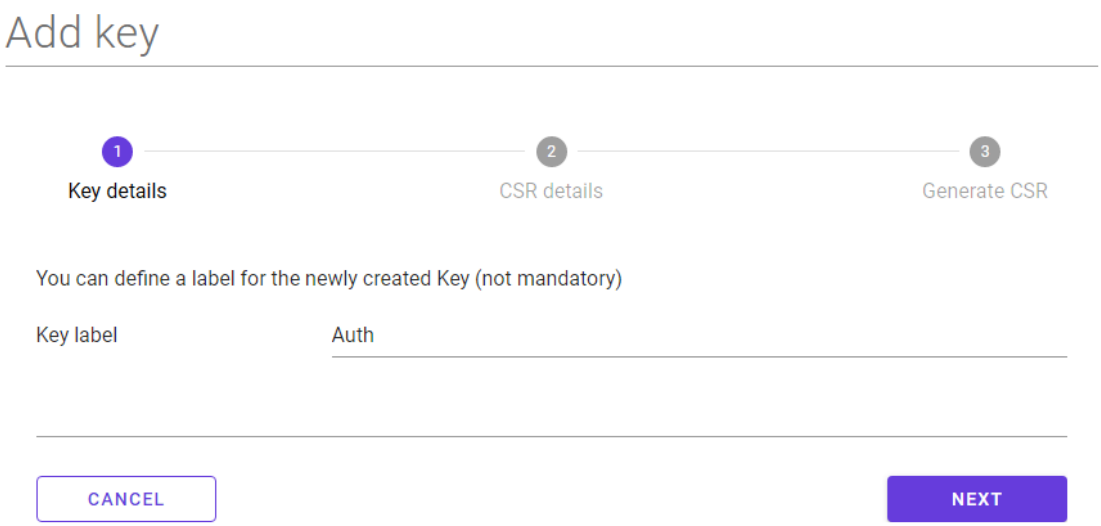


SN 及び CN の名称確認画面が表示されますので、確認し、[OK]ボタンを押下します。

署名用秘密鍵の CSR ファイルのダウンロードが開始されますので、大切に保管してください。

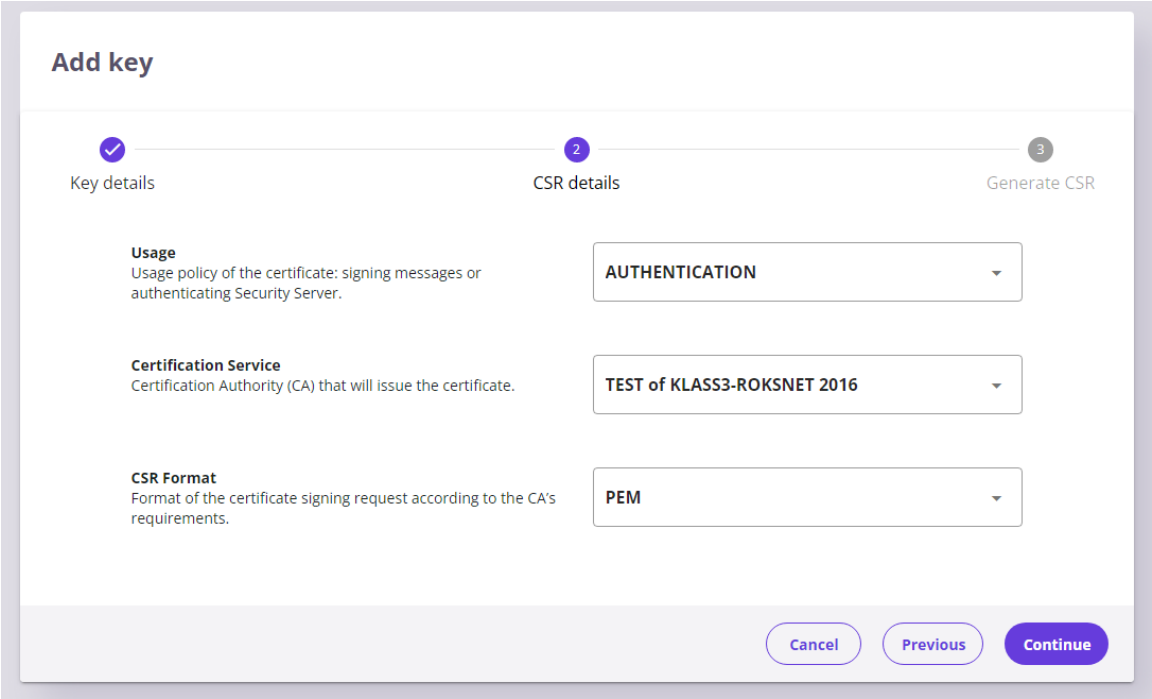
3.8.2 認証用秘密鍵の生成

[+Add Key]ボタンを押下し、AUTH キー（認証用）を生成します。
Label は任意の値を入力してください。
＊認証用秘密鍵と署名用秘密鍵とで区別できること、及び認証用秘密鍵であることが誰の目にも分かるような名称にすることをお勧めします。
Key Label の例：Auth
当ガイドでは以下は、認証用秘密鍵の Label に[Auth]とした場合となります。



認証用秘密鍵の登録後、認証用秘密鍵を選択し、[Generate CSR]ボタンを押下し、CSR の生成を行います。
入力内容は下記を参考に選択・入力してください。

Usage	AUTHENTICATION
Certification Service	利用環境により異なります。 ご不明の場合は OZ1 JP-LINK 担当までお問い合わせください。 開発検証環境：**TEST of KLASS3-ROKSNET 2016** 本番環境：**Roksnet KLASS3-ROKSNET 2017 CA**
CSR Format	PEM　※必ず PEM 形式を選択してください。



SN 及び CN の名称確認画面が表示されますので、確認し、[OK]ボタンを押下します。

認証用秘密鍵の CSR ファイルのダウンロードが開始されますので、大切に保管してください。

3.9 CSR ファイルの送付

上記で作成した署名用、認証用のＣＳＲファイルは、以下の情報をメールに記載し OZ1 社(techoz1@oz1.life)まで送付してください。

メール表題：Security Server CSR ファイルの送付（貴社名）

- X-Road Instance　　：開発環境もしくは本番環境
- Member Code　　：貴社のメンバーコード（8 桁の数字）
- Member Name　　：企業名または団体名
- Security Server Code　：当作業を行った Security Server の Security Server Code

添付ファイル

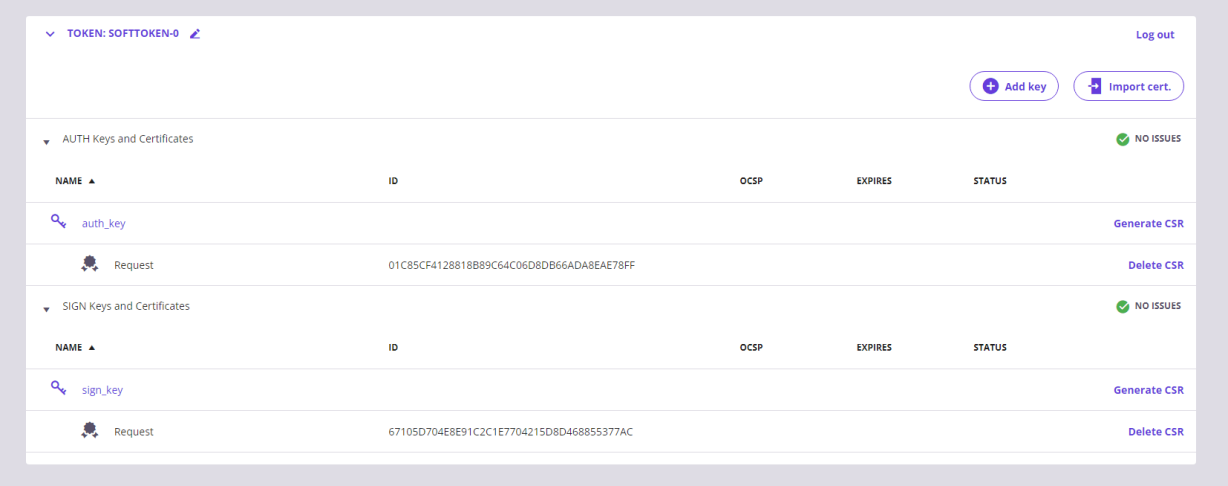
- 3.8.1 で生成した CSR ファイル（署名用）
- 3.8.2 で生成した CSR ファイル（認証用）

3.10 証明書の登録

3.9 にて OZ1 社へ CSR ファイル及び対象の Security Serve Code を送付頂いた後、OZ1 社から認証用及び署名用証明書を返送します。

3.10.1 署名用証明書のインポート

[Import cert.]ボタンを押下し、ＯＺ１より返送された**署名用**証明書のインポートを行ってください。



[Browse]ボタンよりインポートする**署名用**証明書を選択し、[OK]ボタンを押下します。

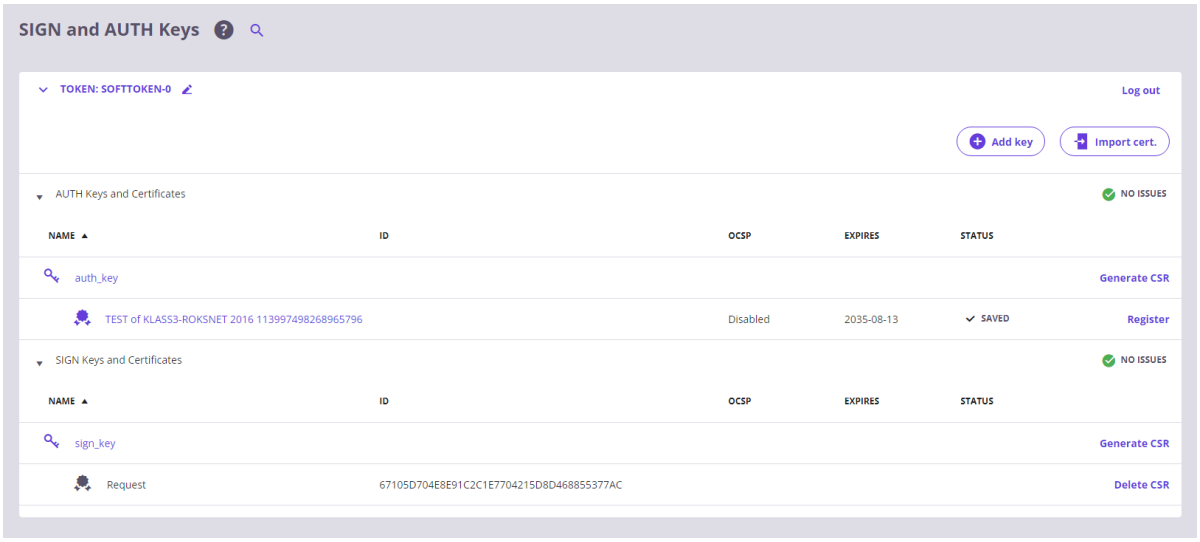
3.10.2 認証用証明書のインポート

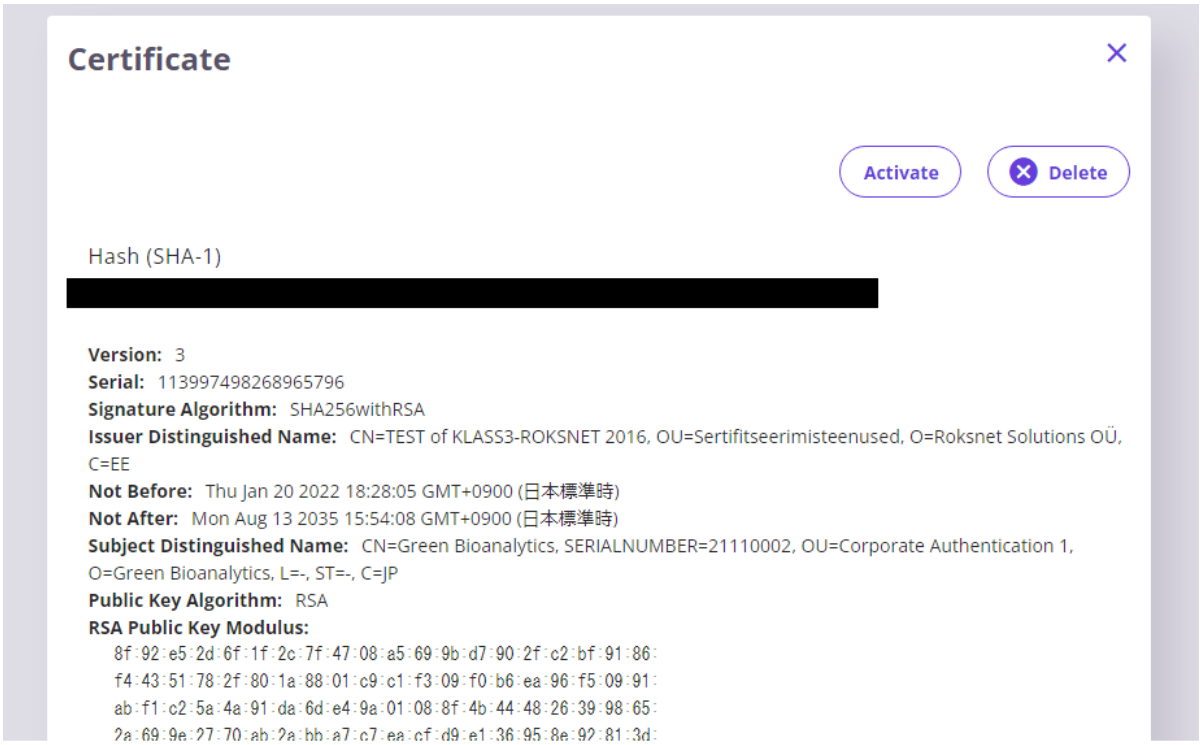
同様に[Import Certificate]ボタンを押下し、ＯＺ１より返送された**認証用**証明書のインポートを行ってください。

[Browse]ボタンより**認証用**証明書を選択し、[OK]ボタンを押下します。

認証用証明書はインポート直後の時点では、OCSP Disabled(無効)の状態で登録されます。

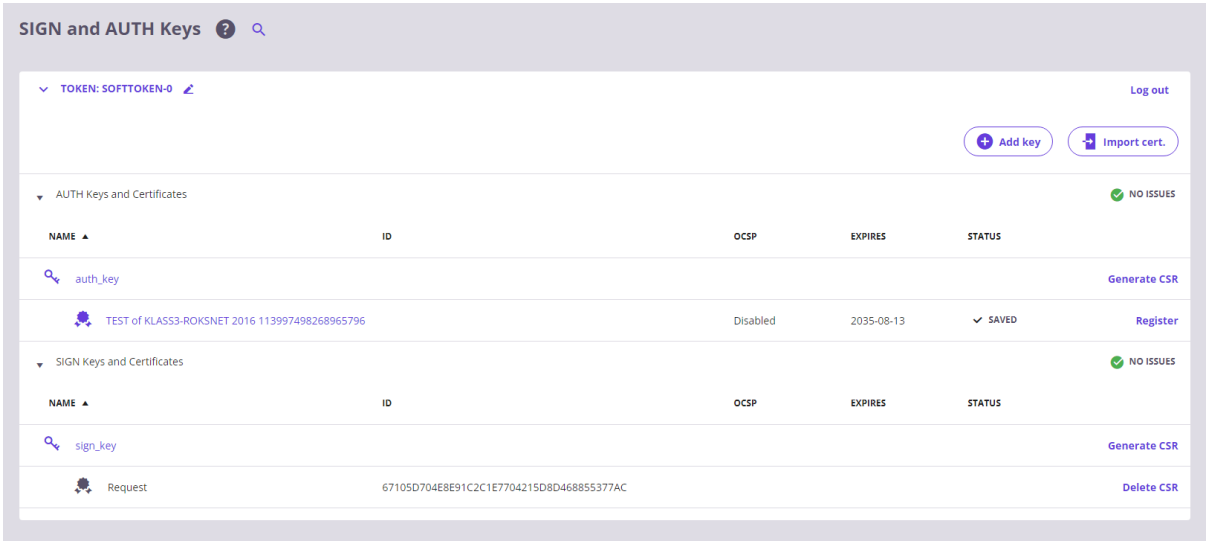
認証用証明書のラベルを選択し、[Activate]ボタンを押下してください。



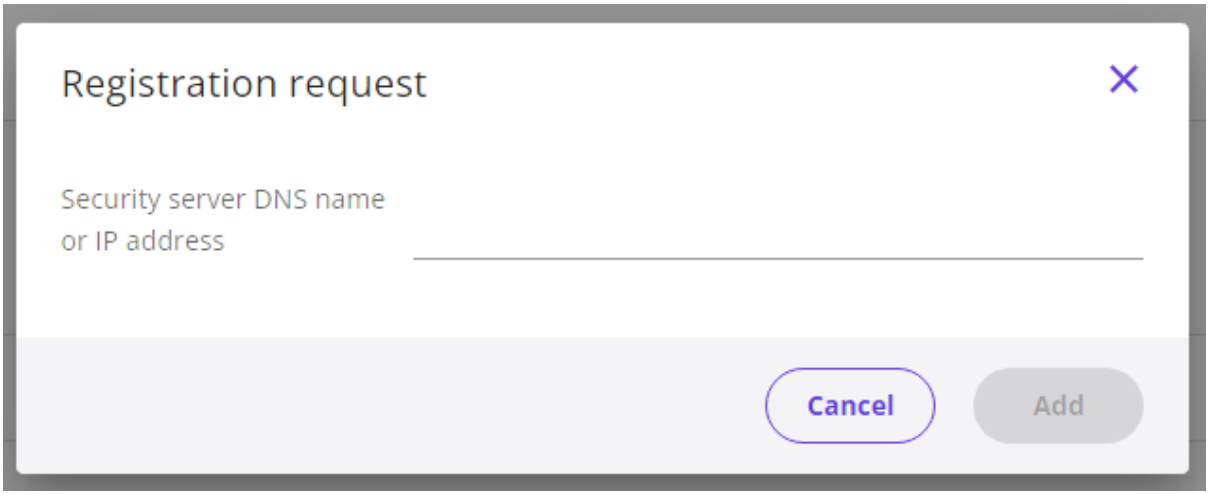


3.10.3 Security Serve の登録

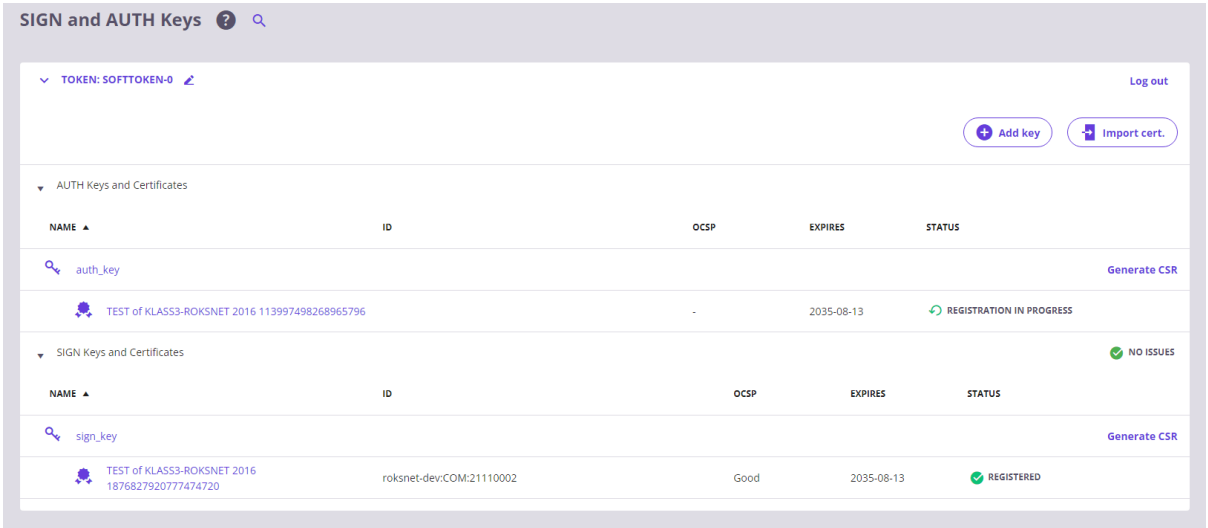
認証用証明書のレコードを選択し、[Register]ボタンを押下します。



Security server のグローバル IP またはホスト名の入力を求められますので、外部から当セキュリティサーバへアクセス可能である IP アドレス（グローバル IP アドレス）または DNS 名（63 文字以内）を入力してください。を入力し、[OK]ボタンを押下します。



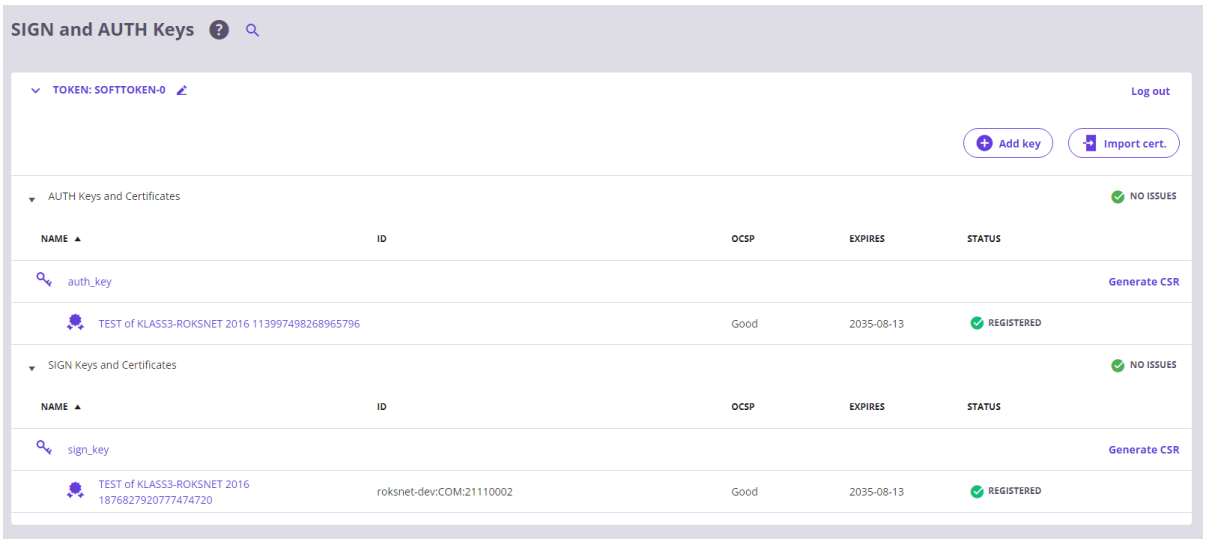
ここまでの操作が完了すると、Status が[registration in progress]となります。



OZ1 社へ以下の情報を送付してください。

- 当作業を行った Security Server の Security Server Code
- 認証用証明書（PEM 形式）

OZ1 社での作業が完了すると、以下のように[Registered]に Status が更新されます。



＊もし、2 営業日以内に[Registered]とならない場合には OZ1 JP-LINK 担当へご連絡ください。

以上で、Security Server のインストール及び初期設定は完了となります。
クライアントの追加、データサービスの追加を行う事で、他組織とのデータ連携が可能となります。
詳細な設定方法などについては「Security Server ユーザーガイド」を参照ください。

4.疎通確認
以下の方法で構築済みのセキュリティサーバから、OZ1 が用意した疎通確認用のサービスを実行して想定通り、JP-LINK に参加できているか確認することができます。
あくまで当サービスは疎通確認を目的としたサービスであるため、実際の業務において提供され運用されることを前提としたデータではなく、データ内容等については予告なく変更される可能性があります。

4-1. OZ1 へ疎通確認を実施したい旨の連絡とともに、次の情報を伝達ください。また、連絡する前に前手順 7.にて追加したサブシステムのステータスが登録済となっていることを確認してください。
- 環境（開発環境か本番環境のどちらか）
- メンバーコード（Member Code）
- サブシステムコード（Subsystem Code）

4-2. OZ1 にて連絡頂いたメンバーコード及びサブシステムコードに対して、疎通確認用サービスの利用許可を設定致します。設定完了後、その旨を連絡しますので、設定完了の連絡を受けてから以下の手順を実施ください。

4-3. セキュリティサーバがインストールされているサーバーにログインし、当ガイドが配置されていたページより[ryokan_search_for_name.xml]ファイルをダウンロードし、格納してください。
____xxxx_____となっている箇所は、ご自身で任意の情報を入力ください。

____実行環境____　：　実行する環境によって以下のどちらかをご選択ください。
本番環境：　roksnet-prod
開発環境：　roksnet-dev
____メンバーコード____　：　ご自身に割り振られたメンバーコードを指定してください。

____サブシステムコード____　：　セキュリティサーバで設定したサブシステムコードを指定してください。

____施設名称____　：　旅館の名称を記述ください。LIKE 句を利用した検索となりますので、ワイルドカード指定が可能です。（例： 大阪% や %大阪% など）

※疎通確認用サービスは大阪市オープンデータポータルサイトに掲載されている「旅館業施設一覧」の施設名称に対して、LIKE 句を利用した検索を行います。

民泊等宿泊施設一覧 - データセット - Open Data Osaka

改訂履歴

バージョン	日付	変更履歴
1.0.0	2022/1/1	初版発行
1.1.0	2023/1/1	主に構成変更