Security Server インストールガイド

目次

1. はじめに

1.1 Security Server とは

Security Server は、PlanetCross 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、PlanetCross ソフトウェアのインストール、操作、管理を行う PlanetCross 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 PlanetCross 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 サポート OS による差分について

Seccurity Server v6.20.2（PlanetCross v1.2.0）より Ubuntu に加え、Red Hat Enterprise linux をサポートします。OS コマンドなど OS 差分がある箇所につきましては、基本的には章題ベースで分けて記載しておりますが、一部文中で分かれて記載する場合がありますのでご注意願います。

尚、「Red Hat Enterprise linux」に付きましては、必要な場合を除き「RHEL」と表記させて頂きます。

1.5 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。

1.5.1 サポートされるプラットフォーム

Ubuntu

全 Security Server のバージョンが対象

オペレーティングシステム	Ubuntu 16.04
CPU	2 core
RAM	4GB
ディスク空き容量	20GB

Red Hat Enterprise linux

Security Server v6.20.2 以降からサポート

オペレーティングシステム	RHEL7.2 x86-64
CPU	2 core
RAM	4GB
ディスク空き容量	10GB：OS パーティション 20～40GB：/var パーティション
ネットワーク	100Mbps（Network Interface Card）

RHEL について、OS に対応しているサーバーを選定してください。

Ubuntu、RHEL ともに 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強く推奨します。

1.5.2 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)

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)

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

ローカルアクセス（OS 差分あり）

Ubuntu

TCP 4000	ユーザーインターフェース
TCP 80	情報システムからの接続
TCP 80、443	情報システムからの接続

RHEL

TCP 4000	ユーザーインターフェース
TCP 8080	情報システムからの接続
TCP 8080、8443	情報システムからの接続

2. インストール(Ubuntu)

本章は Ubuntu におけるインストール手順です。RHEL におけるインストールについては「3.インストール(RHEL)」を参照願います。

2.1 事前準備

2.1.1 ホスト名の設定

ホスト名を設定します。「/etc/hosts」ファイルの「127.0.1.1」の行に任意のホスト名を指定します（下記**{your-host-name}**の箇所にホスト名を指定）。

```
127.0.1.1   {your-host-name}
```

2.1.2 Locale

Locale を「en_US.UTF-8」に設定してください。

```
$ sudo apt-get update
$ sudo apt-get install locales
$ sudo locale-gen en_US.UTF-8
```

2.1.3 apt-key とパッケージリポジトリサーバーの登録

apt-key を登録します。

以下の各コマンドは改行せず 1 行で入力してください。

```
$ sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys
731E775DF768EF67

$ sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys
00A6F0A3C300EE8C

$ sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys
EB9B1D8886F44E2A
```

「Planetway Ops <apt@pwlvc.com>」、「Launchpad Stable」、および「Launchpad OpenJDK builds (all archs)」が登録されたことを確認します。

```
$ sudo apt-key list
```

＜出力例＞

```
/etc/apt/trusted.gpg
--------------------
（省略）
```

```
pub   4096R/F768EF67 2017-10-31
uid                  Planetway Ops <apt@pwlvc.com>
sub   4096R/254BD796 2017-10-31

pub   1024R/C300EE8C 2010-07-21
uid                  Launchpad Stable

pub   1024R/86F44E2A 2010-04-12
uid                  Launchpad OpenJDK builds (all archs)
```

次にパッケージリポジトリサーバーの登録を行います。

PlanetCross v1.1.2（2019 年 6 月 12 日）よりパッケージリポジトリサーバーが統一されました。V1.1.2 以前より導入済のお客様は大変お手数ですが環境(本番／検証)によらず下記リポジトリサーバーのみを使用願います（旧マニュアル上、「本番環境(JP)」と記載があったものとなります）。

2020 年 1 月 20 日より{username}と{password}の入力が不要となりました(以下コマンドの 1 行目です)。以前のコマンドをご使用のお客様はご注意願います。

以下コマンドで設定します。

以下の各コマンドは改行せず 1 行で入力してください。

```
$ sudo sh -c 'echo "deb [arch=amd64] https://deb.planetcross.net/planetx trusty
non-free" > /etc/apt/sources.list.d/planetx.list'

$ sudo sh -c 'echo "deb http://ppa.launchpad.net/nginx/stable/ubuntu trusty
main" >> /etc/apt/sources.list.d/planetx.list'

$ sudo sh -c 'echo "deb http://ppa.launchpad.net/openjdk-r/ppa/ubuntu trusty
main" >> /etc/apt/sources.list.d/planetx.list'
```

入力内容が正しいことを確認してください。

```
$ cat /etc/apt/sources.list.d/planetx.list
```

＜出力例＞

```
deb [arch=amd64] https://deb.planetcross.net/planetx trusty non-free
deb http://ppa.launchpad.net/nginx/stable/ubuntu trusty main
deb http://ppa.launchpad.net/openjdk-r/ppa/ubuntu trusty main
```


2.1.4 ユーザーの追加

Unix group を使用して権限設定を行います。

このユーザーを後ほど PlanetCross 管理者として指定します。

{password}は任意の値を設定してください。

以下の各コマンドは改行せず 1 行で入力してください。

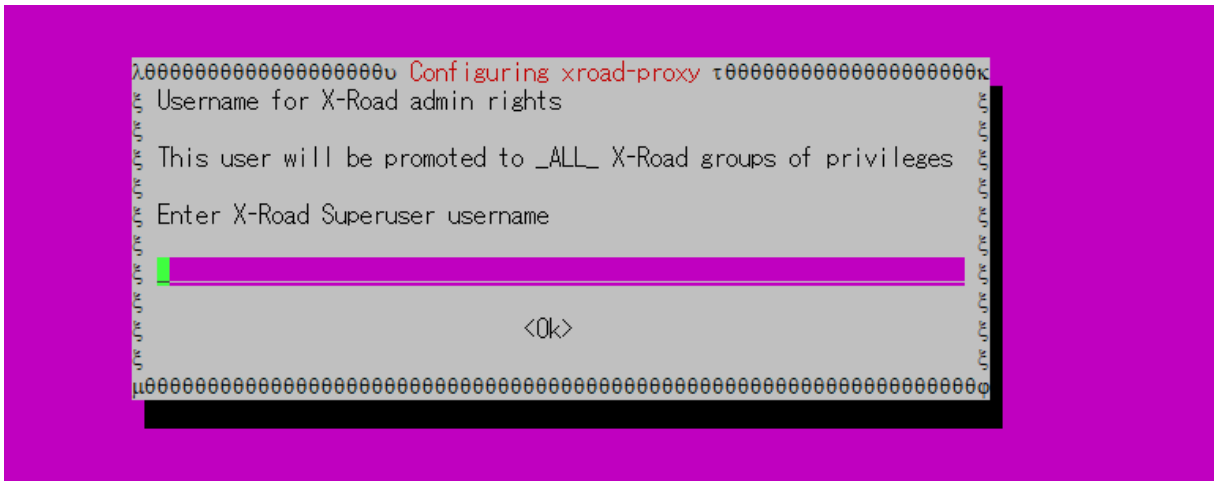
```
$ sudo adduser --disabled-password --no-create-home --gecos "xuser,,," xuser

$ echo "xuser:{password}" | sudo chpasswd
```

2.2 Security Server のインストール

```
$ sudo apt-get -y update
$ {インストールコマンド}
```

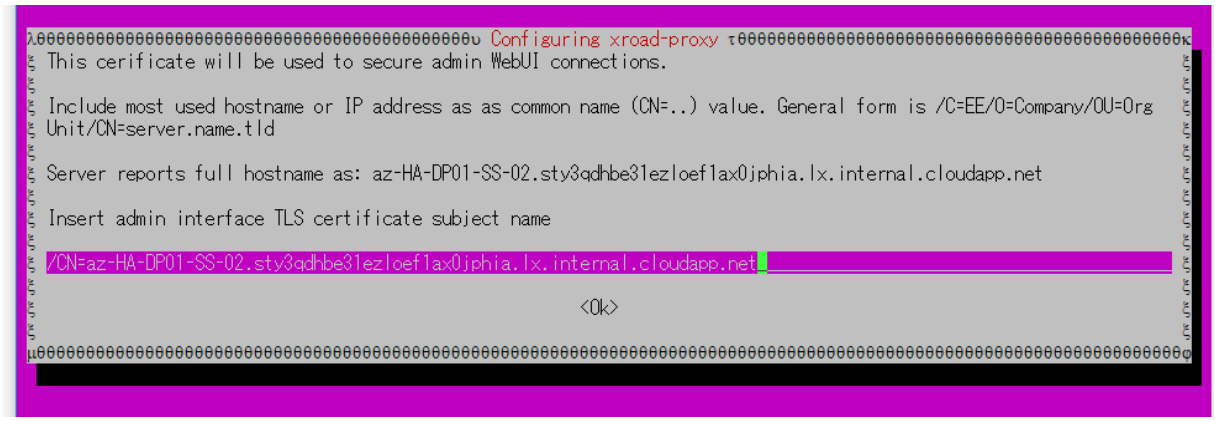
※{インストールコマンド}は『リリースノート』をご参照ください。

以下の管理者を指定する画面が表示されたら、2.1.4 にて作成したユーザー名を入力し、Enter を押します。



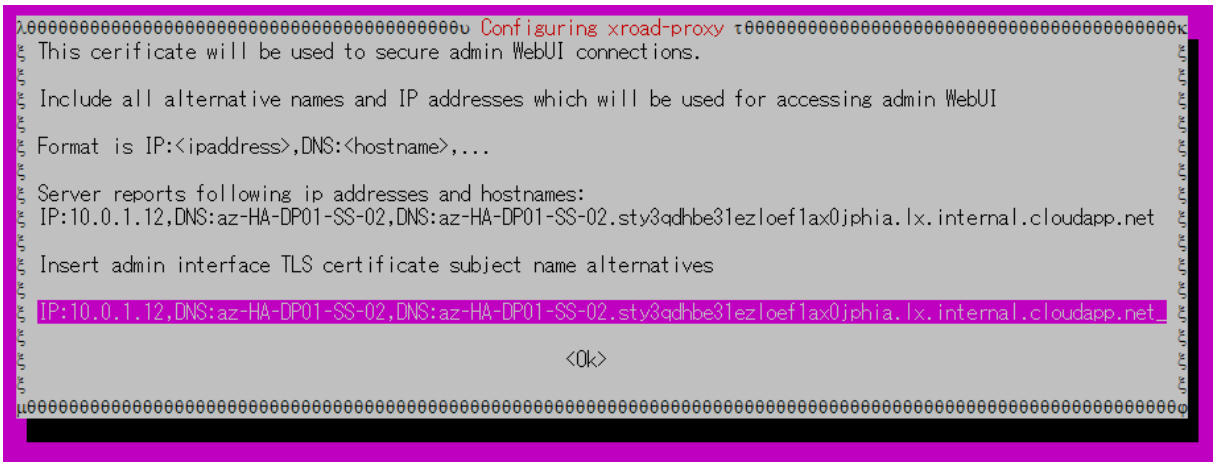
次に WebUI の管理画面で使用される証明書の Common Name(CN)を入力します。

アクセスする際に使用する IP アドレス、またはホスト名を設定します。本設定は 63 字以下にする必要があります。

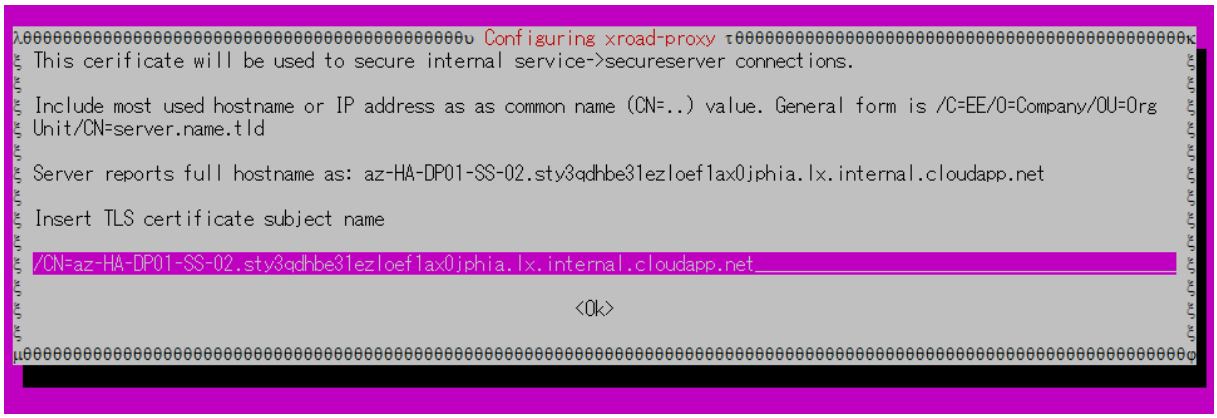


次に Subject Alternate Names(SANs)を入力します。

上記の 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 字以下にする必要があります。

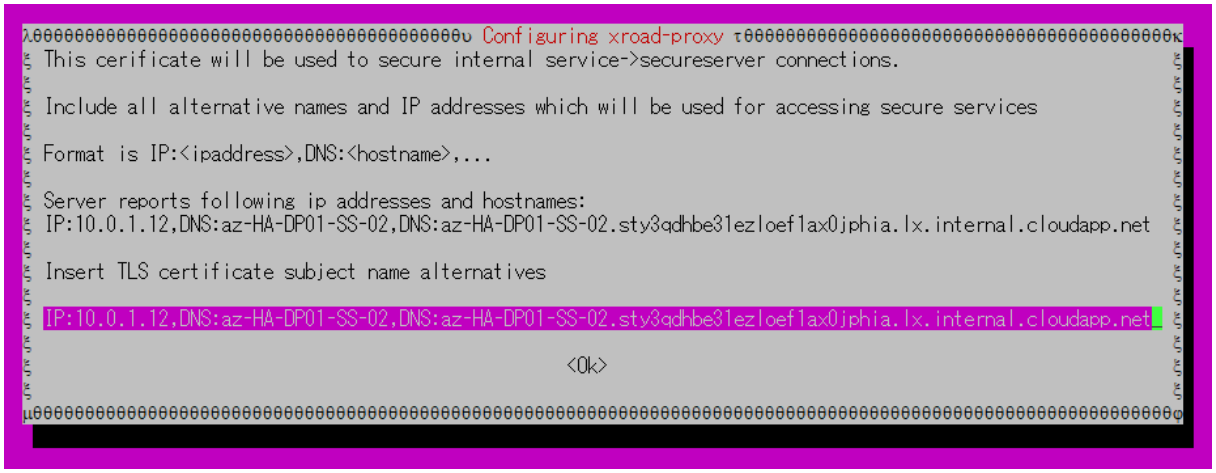


同様に、Security Server に対してリクエストを送る組織内のクライアントから Security Server にアクセスする際に使用される証明書の CN を入力します。使用する IP アドレス、またはホスト名を設定してください。本設定は 63 字以下にする必要があります。



次に Subject Alternate Names(SANs)を入力します。

上記の 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 字以下にする必要があります。



2.3 確認

サービスの稼働状況を確認します。以下と同様であれば問題ありません。

```
$ systemctl list-units|grep xroad-
```

＜出力例＞

```
xroad-confclient.service          loaded active running X-Road Configuration Files Service
xroad-jetty.service               loaded active running X-Road Proxy Frontend Jetty Service
xroad-monitor.service             loaded active running X-road Monitoring Service
xroad-opmonitor.service           loaded active running X-Road Operational Monitoring Service
xroad-proxy.service               loaded active running X-Road Proxy Backend Service
xroad-signer.service              loaded active running X-Road Signer Service
```

ポートに listen しているかを確認します。

以下のポートに listen できれば問題ありません。

```
$ netstat -anp|grep LISTEN
```

＜出力例＞

```
（省略）
tcp        0      0 0.0.0.0:4000            0.0.0.0:*               LISTEN      -
（省略）
tcp6       0      0 :::5577                 :::*                    LISTEN      -
（省略）
tcp6       0      0 :::80                   :::*                    LISTEN      -
（省略）
tcp6       0      0 :::443                  :::*                    LISTEN      -
tcp6       0      0 :::5500                 :::*                    LISTEN      -
```


3. インストール(RHEL)

本章は RHEL におけるインストール手順です。Ubuntu におけるインストールについては「2.インストール(Ubuntu)」を参照願います。

3.1 事前準備

3.1.1 Locale

以下の通り「/etc/environment」ファイルを作成し、ロケールを設定します。

「/etc/environment」ファイル作成

```
$ sudo vi /etc/environment
```

＜設定内容＞

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

3.1.2 ホスト名・FQDN 名の確認・修正

Security Server のアクセス（WEB-UI）に使用するホスト名・FQDN 名を確認し、必要に応じて修正します。ホスト名、並びに FQDN のラベルの長さは 63 字以下で設定する必要があります。特にクラウド環境において、デフォルトの FQDN 名が長く設定されているケースを確認しております。**64 字以上の状態で後続のインストールを行った場合、インストールに失敗しますので必ず確認してください。**

１．設定の確認

下記出力結果より、任意の設定値（それぞれ同値）、且つ 63 字以下であることを確認してください。本出力結果が Security Server のインストール時に使用されます。

ホスト名の確認

```
$ hostname
```

もしくは「uname -n」でも構いません。

FQDN 名の確認

```
$ hostname -f
```

上記出力結果が 64 文字以上 or 任意のホスト名を設定したい場合、後続作業を実施します。

２．「/etc/hosts」に IP アドレスとホスト名のペアを追加します

＜設定内容（{ }は任意の値です）＞

```
{private IP Address} {hostname}
{global IP Address} {hostname}
```

上記はプライベート IP とグローバル IP を定義する場合です。両方登録する場合はそれぞれの{hostname}を同値としてください。

３．「/etc/hostname」を修正します

＜修正内容（{ }は任意の値です）＞

```
{hostname}
```

「/etc/hosts」と同値を設定します。

【注意】AWS 環境の場合、恒久的な設定にするには上記に加え、「/etc/cloud/cloud.cfg」を下記の通り編集する必要があります。

＜設定内容＞

以下を追記

```
preserve_hostname: true
```

尚、上記は AWS の仕様、RHEL の仕様に依存するため詳細は各社のマニュアルを参照願います。

４．設定の確認

下記出力結果より、任意の設定値（それぞれ同値）、且つ 63 字以内であることを確認してください。

ホスト名の確認

```
$ hostname
```

FQDN 名の確認

```
$ hostname -f
```


3.1.3 パッケージリポジトリの登録

PlanetCross のパッケージリポジトリサーバーを登録します。

「/etc/yum.repo.d/planetx.repo」ファイルを新規作成し、環境に合わせて以下の通り設定してください。

2020 年 1 月 20 日より、{username}と{password}の設定が不要となりました。以前のコマンドをご使用のお客様はご注意願います。

＜設定内容＞

```
[planetx]
name=PlanetCross for RHEL/CentOS
baseurl=https://rpm.planetcross.net/7/
enabled=1
gpgcheck=1
gpgkey=https://static.planetcross.net/prod/gpgkey.asc
```

Ubuntu 含め、PlanetCross v1.1.2（2019 年 6 月 12 日）よりパッケージリポジトリサーバーが統一されました。環境(本番/検証)によらず上記を登録願います。

3.1.4 yum-utils のインストール

yum-utils パッケージをインストールします

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

途中「Is this ok [y/d/N]:」と許可を求められるため、「y」を応答してください。

出力結果最後尾に「Complete!」が表示されればインストール完了です

3.1.5 /tmp マウント状態確認・変更

「/tmp」ディレクトリが「noexec」オプションでマウントされている場合、「noexec」オプションを外す必要があります。（対応しない場合、WebUI が起動されません）

１．/tmp マウント状態確認

下記コマンドにてマウント状態を確認します

```
$ mount | grep /tmp
```

＜出力例＞

```
/dev/loop0 on /tmp type ext3 (rw,noexec,nosuid,nodev)
```

出力例のように、「/tmp」に「noexec」が設定されている場合は「２．/tmp マウントオプション変更」の作業が必要です。「noexec」オプションが設定されていないか、マウントされていない場合は対応不要です。

２．/tmp マウントオプション変更

「/etc/fstab」に記載されている場合は、「/etc/fstab」を修正してください。再マウントする際は以下コマンドを入力します。

```
$ mount -o remount,exec /tmp
```

3.2 Security Server のインストール

3.2.1 Extra Packages for Enterprise Linux (EPEL) 導入

１．EPEL リポジトリの追加

以下のコマンドは改行せず１行で入力してください。

```
$ sudo yum install
https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

途中「Is this ok [y/d/N]:」と許可を求められるため、「y」を応答してください。

出力結果最後尾に「Complete!」が表示されればインストール完了です

２．追加パッケージのインストール

EPEL より「crudini」「rlwrap」「nginx」を導入します。それぞれ以下コマンドを入力します。

```
$ sudo yum install crudini
$ sudo yum install rlwrap
$ sudo yum install nginx
```

それぞれ途中「Is this ok [y/d/N]:」と許可を求められるため、「y」を応答してください（「crudini」のみ 2 回求められます）。

出力結果最後尾に「Complete!」が表示されればインストール完了です。

3.2.2 Security Server パッケージインストール

１．パッケージインストール

以下コマンドを入力し、Security Server パッケージをインストールします。

なお、インストールコマンドはバージョンによって変更の可能性があります。導入にあたっては必ず各バージョンのリリースノートをご確認願います。

```
$ sudo yum install xroad-securityserver-planetway-{導入バージョン}
```

途中複数回「Is this ok [y/d/N]:」と許可を求められるため、「y」を応答してください。

それぞれ出力結果最後尾に「Complete!」が表示されればインストール完了です

２．管理ユーザー追加

Security Server の管理ユーザーを登録します。ここで登録したユーザー名が後続の WebUI のログイン項目となりますので控えておいてください。

{username}については任意のユーザー名を入力してください

```
$ sudo xroad-add-admin-user {username}
```

上記入力後、パスワードの入力を求められるため任意のパスワードを設定してください。

３．Security Server の起動

インストール完了後、Security Server を起動させます。

以下コマンドで起動させてください。

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

起動確認は以下コマンド

```
$ sudo systemctl status xroad-proxy
```

3.3 Security Server のインストール確認

１．サービス稼働状態確認

以下コマンドを入力します。

```
$ systemctl list-units|grep xroad-
```

以下の通りであれば問題ありません。

＜出力例＞

```
  xroad-confclient.service
          loaded active running   X-Road confclient
  xroad-jetty9.service
          loaded active running   X-Road Jetty server
  xroad-monitor.service
          loaded active running   X-Road Monitor
  xroad-opmonitor.service
          loaded active running   X-Road opmonitor daemon
  xroad-proxy.service
          loaded active running   X-Road Proxy
```



```
  xroad-signer.service
          loaded active running   X-Road signer
```

２．nginx サービス状態確認

nginx サービスが実行状態であることを以下コマンドで確認します。

```
$ sudo systemctl status nginx
```

以下の通り「active(running)」であれば問題ありません。

＜出力例＞

```
● nginx.service - The nginx HTTP and reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; disabled; vendor
preset: disabled)
   Active: active (running) since Wed 2019-06-26 01:54:56 UTC; 8h ago
  Process: 2234 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
  Process: 1121 ExecStartPre=/usr/sbin/nginx -t (code=exited,
status=0/SUCCESS)
  Process: 1096 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited,
status=0/SUCCESS)
 Main PID: 2236 (nginx)
   CGroup: /system.slice/nginx.service
           ├─2236 nginx: master process /usr/sbin/nginx
           ├─2237 nginx: worker process
           └─2238 nginx: worker process
```

３．管理画面（WEBUI）の接続確認

この時点で管理画面（WEBUI）を確認することを推奨致します。ログイン方法につきましては、「4.2 管理画面を開く」をご確認ください。

接続不可の場合、ファイアウォールなどネットワーク要件が満たされていることを確認願います。

尚、WEBUI が起動中の場合、「502 Bad Gateway」エラーが表示される場合があるため時間をおいて再度試行願います。

4. 初期設定

ここでは、Security Server のインストール後に行う初期設定について紹介します。
Security Server の詳細設定については、『Security Server 設定ガイド』を参照してください。

4.1 Security Server の初期設定で必要なデータ

Security Serer の初期設定の際に、PlanetCross メンバーの情報やソフトウェアトークンの PIN などを設定する必要があります。

4.1.1 参照データ

設定で必要な参照データを以下の表に整理します。

注意: 参照データの No.1.1～1.3 は、Planetway 担当者から Security Server 所有者に提供されます。

Security Server コードとソフトウェアトークンの PIN は、インストール中にインストール実行者が入力します。

No	参照データ	説明
1.1	■検証用アンカーファイル http://static.planetcross.net/test/configuration_anchor.xml ■本番用アンカーファイル http://static.planetcross.net/prod/configuration_anchor.xml	グローバル設定アンカーファイルが提供されます。
1.2	GOV - 政府機関 COM - 民間企業	Security Server の所有者のメンバークラス。お客様のメンバークラスは「COM」を指定してください。
1.3	<Security Server 所有者登録コード>	Security Server の所有者のメンバーコードがお客様に提供されます。
1.4	<Security Server の識別子名を選択>	Security Server のコード。お客様にて事前に用意が必要です。
1.5	<ソフトウェアトークンの PIN を選択>	ソフトウェアトークンの PIN。大小アルファベットと数字の組み合わせで 10 桁以上で記載します。お客様にて事前に用意が必要です。

注: No.1.4 以降 - Security Server コードの命名規則を取り決めてください。

4.1.2 初期設定と対応する参照データ

初期設定を行うには、Web ブラウザでアドレス

https:// {WebUI 接続用 IP アドレス or ホスト名}:4000/

を開きます。ログインには、インストール時に選択した 2.3 で指定した管理者アカウント名を使用します。

初回ログイン時に、以下の情報の入力が求められます。

- グローバル設定アンカーファイル(参照データ: 1.1)。

設定が正常にダウンロードされると、以下の情報の入力が求められます。

- Security Server 所有者のメンバークラス(参照データ: 1.2)。
- Security Server 所有者のメンバーコード(参照データ: 1.3)。メンバークラスとメンバーコードが正しく入力されると、PlanetCross センターに登録されている Security Server 所有者の名前が表示されます。
- Security Server コード(参照データ: 1.4)。Security Server 管理者が選択し、同じ PlanetCross メンバーに属するすべての Security Server で一意の値である必要があります。
- ソフトウェアトークンの PIN (参照データ: 1.5)。PIN は、ソフトウェアトークンに保存されているキーを保護するために使用されます。PIN は安全な場所に保管しておいてください。万一 PIN を紛失すると、トークンに保管されている秘密キーは使用できなくなり、復元することもできません。

4.2 管理画面を開く

以下の URL を Web ブラウザで開いてください。{**WebUI 接続用 IP アドレス or ホスト名**}は Security Server の IP アドレスを入力してください。

```
https://{WebUI 接続用 IP アドレス or ホスト名}:4000/
```

なお、ネットワークの設定によっては、管理者が Security Server に SSH 接続できてもポート 4000 番を直接ブラウザで開けない場合があります。そのような場合には、以下のコマンドを実行し SSH トンネルを使用することで Web ブラウザで接続できます。SSH トンネルを使用する場合は**{WebUI 接続用 IP アドレス or ホスト名}**は**"localhost"**を指定します。

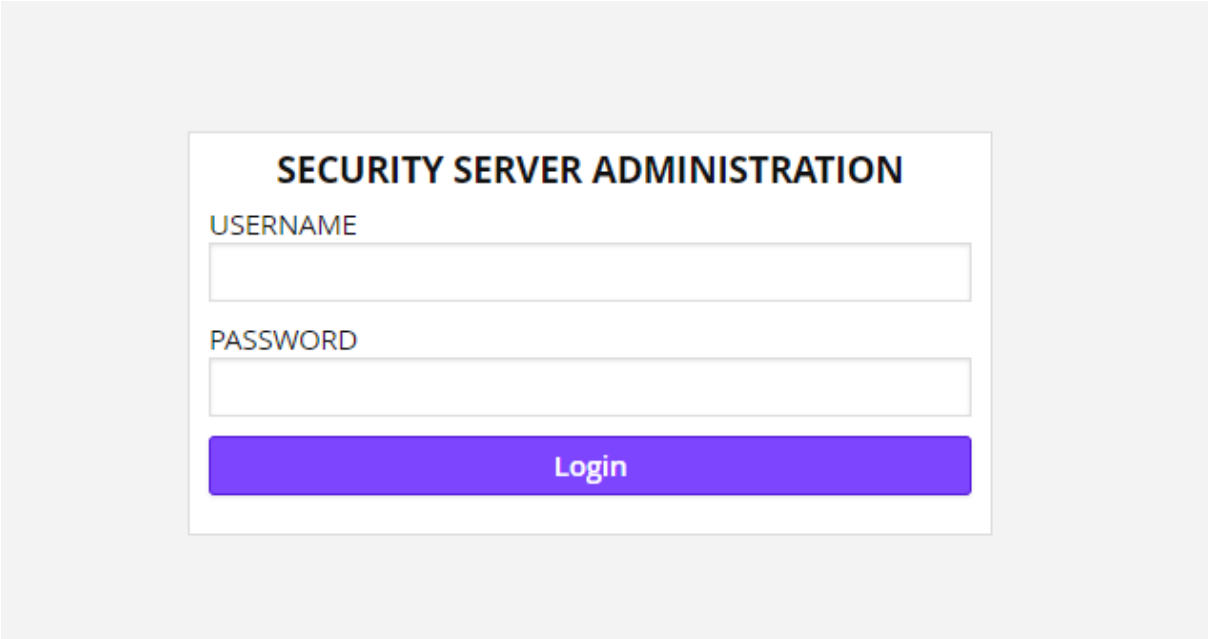
以下のコマンドを手元のマシンのシェル(新規プロンプトをオープン)で実行してください。

```
$ ssh -L 4000:localhost:4000 ubuntu@securityserver-hostname -i ~/.ssh/id_rsa
-N
```

上記のコマンドは、実行後ブロックします。

4.3 管理画面へのログイン

2.1.4、3.2.2 で設定した管理者ユーザーとしてログインします。

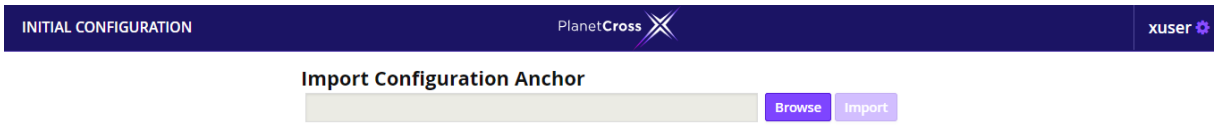


4.4 コンフィギュレーションアンカーのインポート

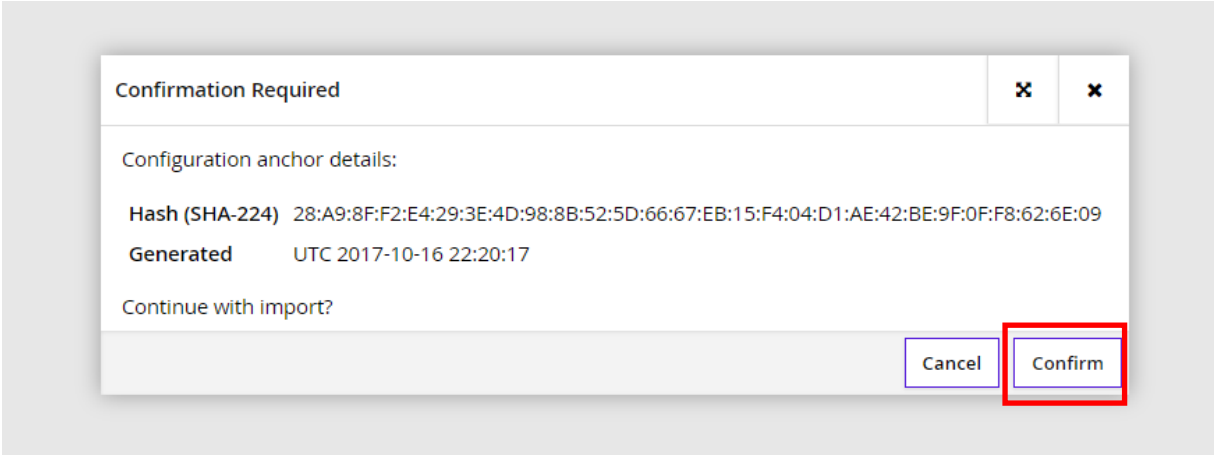
Planetway 社より提供するコンフィギュレーションアンカー(Configuration Anchor)の XML ファイルをインポートします。

[Browse]ボタンを押し、アンカーファイルを選択します。

その後、[Import]ボタンを押します。



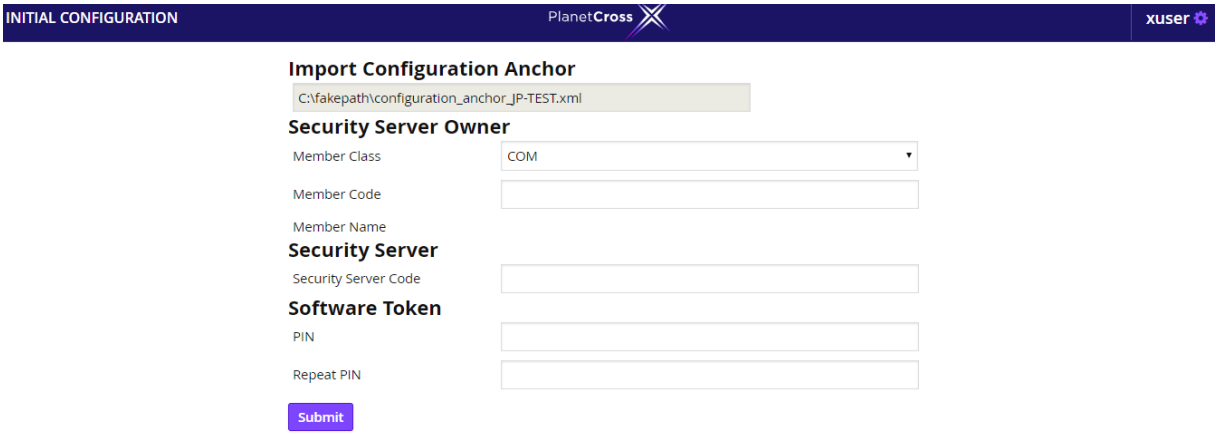
確認画面が表示されたら、[Confirm]ボタンを押します。



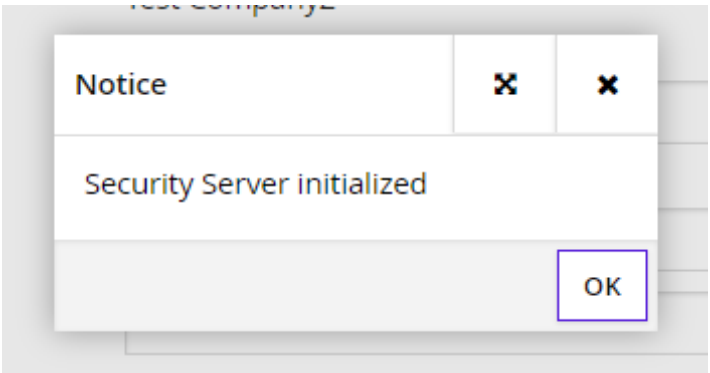
4.5 Security Server の初期化

Planetway 社より提供する Member Code を入力し、Security Server Code、Software Token の PIN を決定して入力し、SUBMIT します。

Security Server Code は、この Security Server を組織内で一意に特定する ID です。Software Token の PIN は、以降で生成する秘密鍵を暗号化して保存するための PIN コードです。



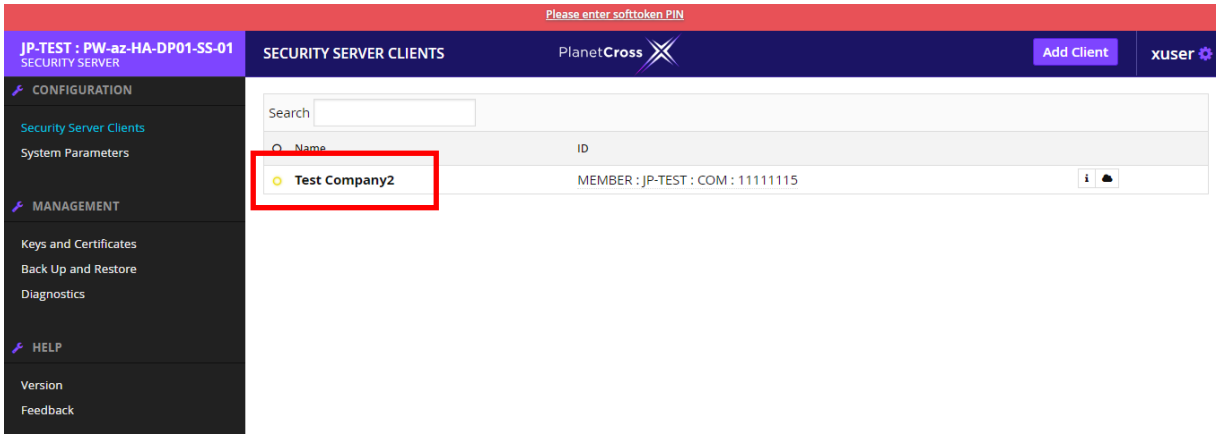
Notice 画面が表示されたら、[OK]ボタンを押します。



これが初めての Security Server の設定である場合は、初期化が完了したことを Planetway 社に通知します。

Planetway 社の方で PlanetCross メンバーの登録を行います。

下記のように「Client not found」と表示されている状態から、PlanetCross メンバー名が表示された状態に変わったら登録完了です。

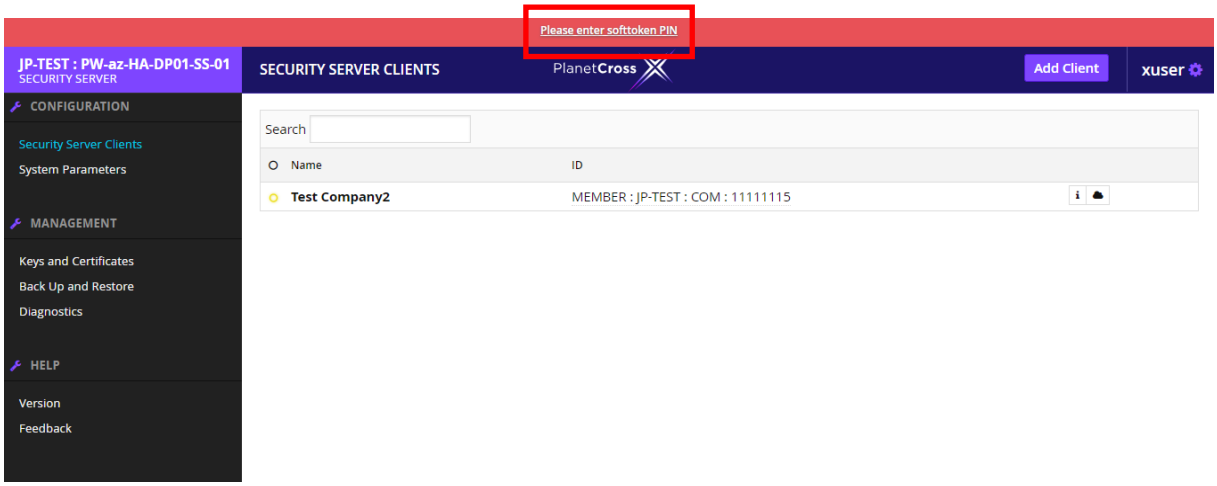


4.6 PIN の入力

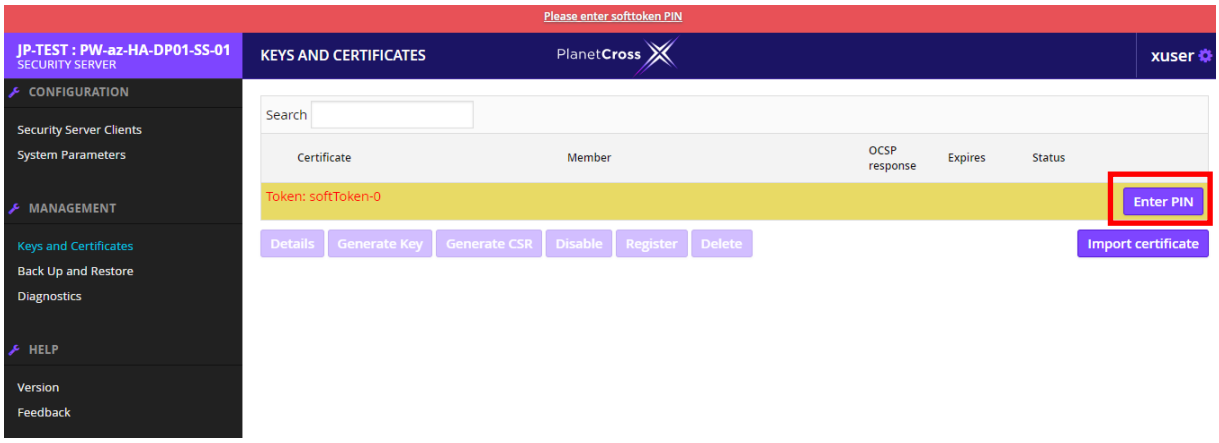
PIN を入力します。

Security Server は起動後、PIN の入力後から PlanetCross のリクエストに応答します(再起動後も同様)。

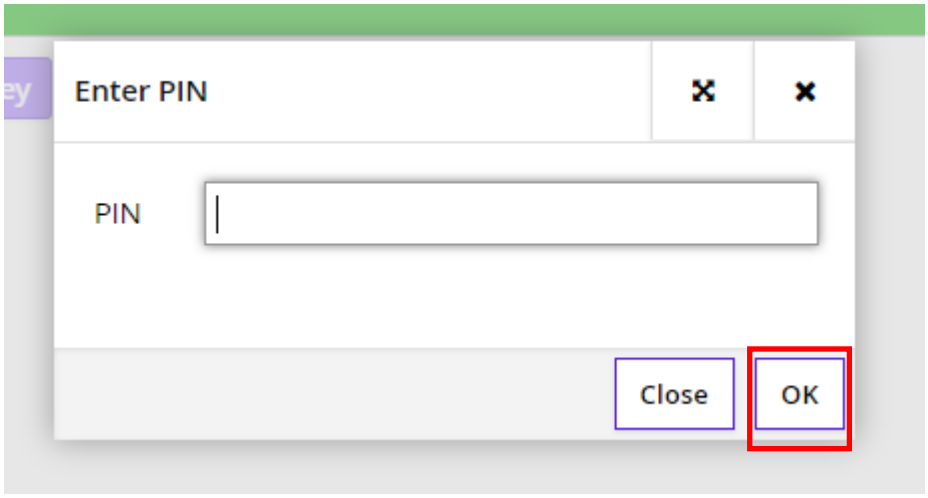
[Please enter softtoken PIN]を押します。

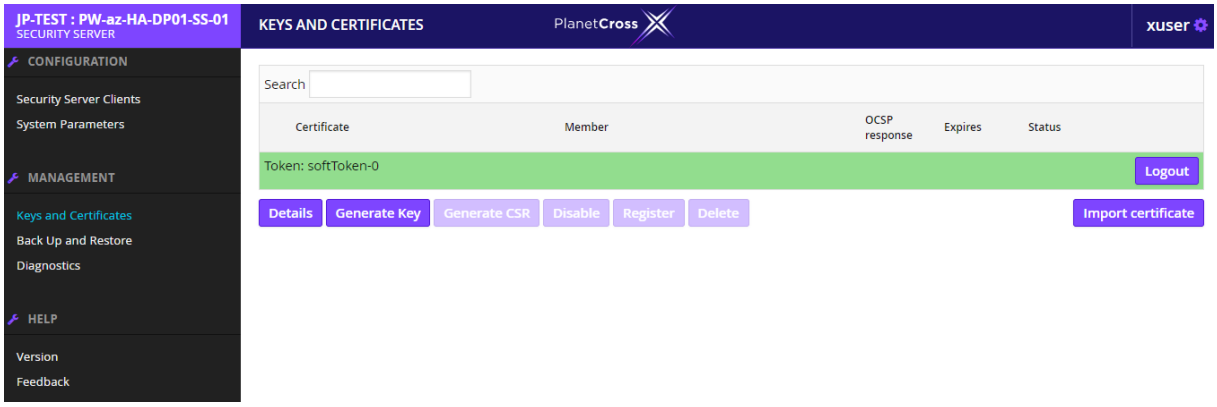


[Enter PIN]ボタンを押します。



PIN を入力し、[OK]ボタンを押します。

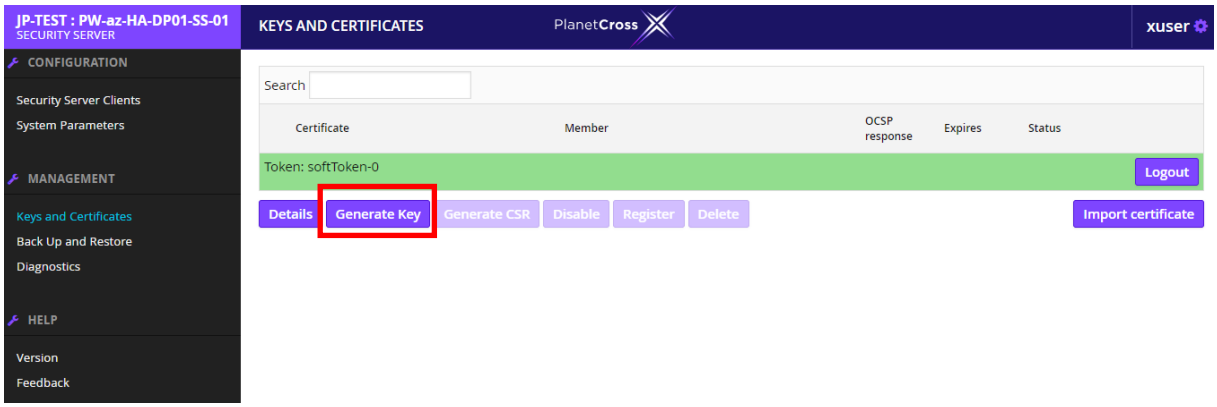




4.7 認証用、署名用の秘密鍵の生成

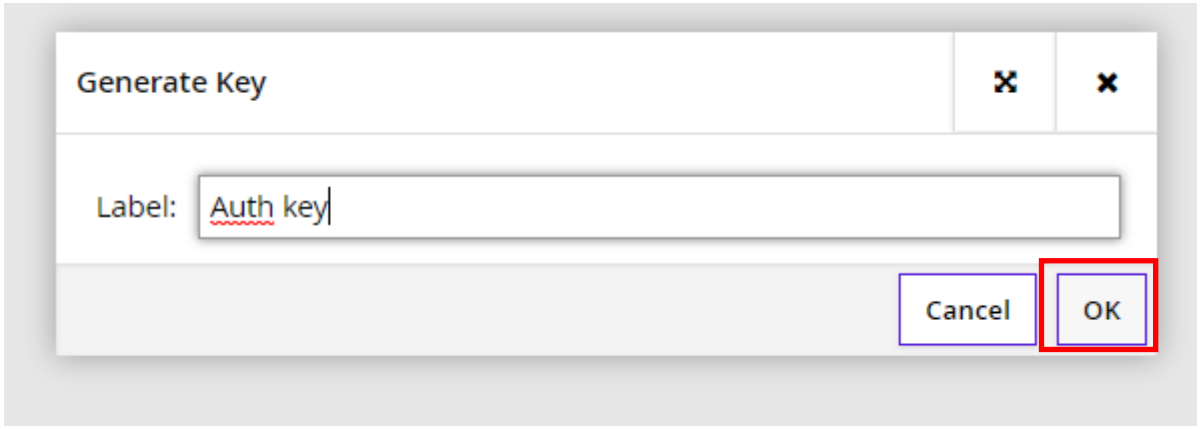
「softToken」を選択し、認証用、署名用の秘密鍵を生成します。

[Generate Key]ボタンを押します。

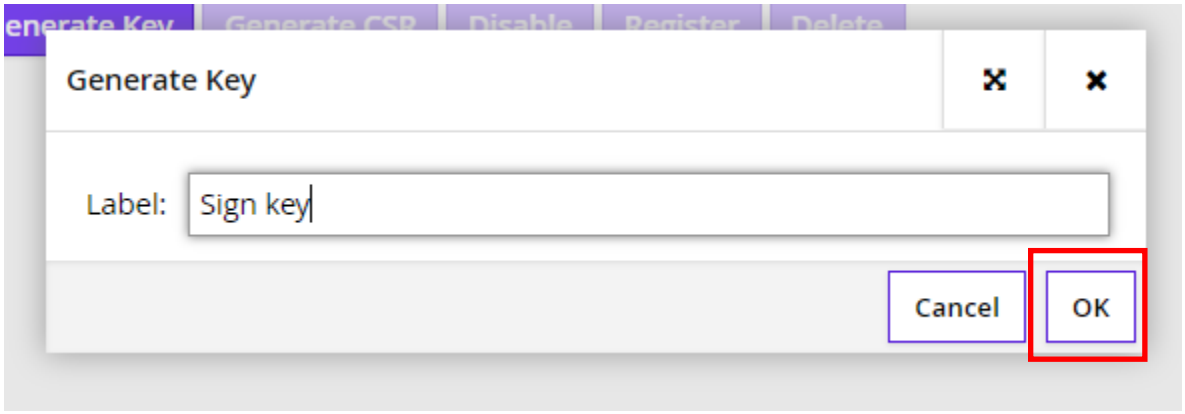


認証用、署名用の区別がつくように Label を入力し、[OK]を押します。

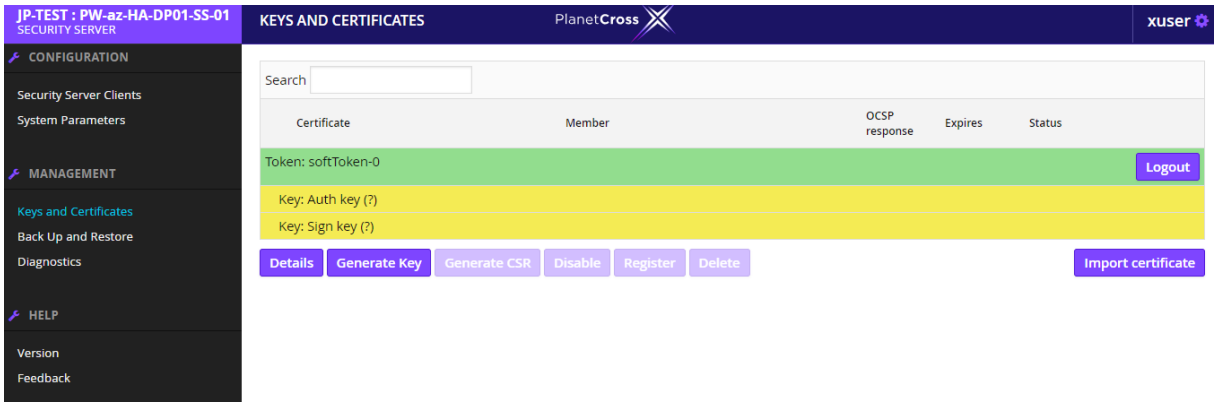
認証用 Label の例:



署名用 Label の例:



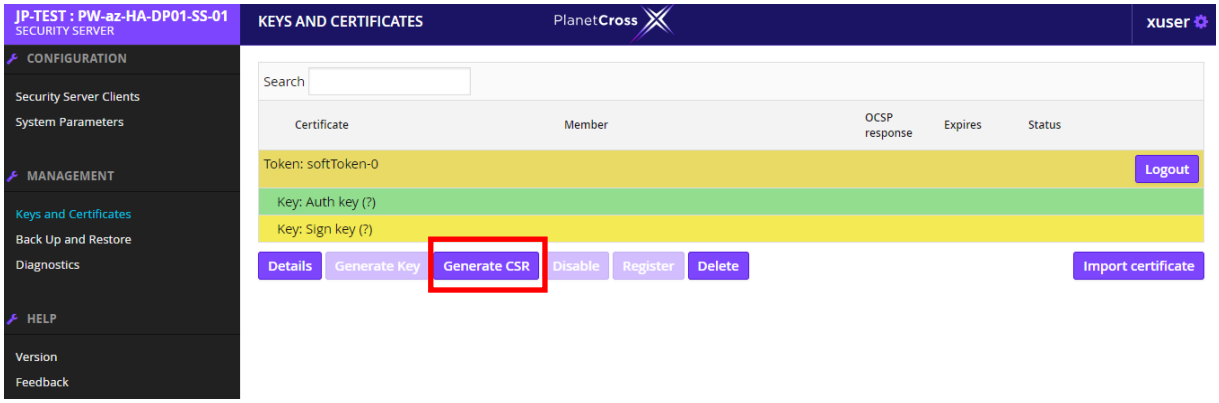
認証用を「Auth key」、署名用を「Sign key」として作成した例は以下の通りです。



4.8 Planetway 社で PlanetCross メンバーの登録完了を待つ

認証用、署名用の CSR を生成して Planetway 社に送付します。

署名用の秘密鍵を選択し、[Generate CSR]ボタンをクリックします。



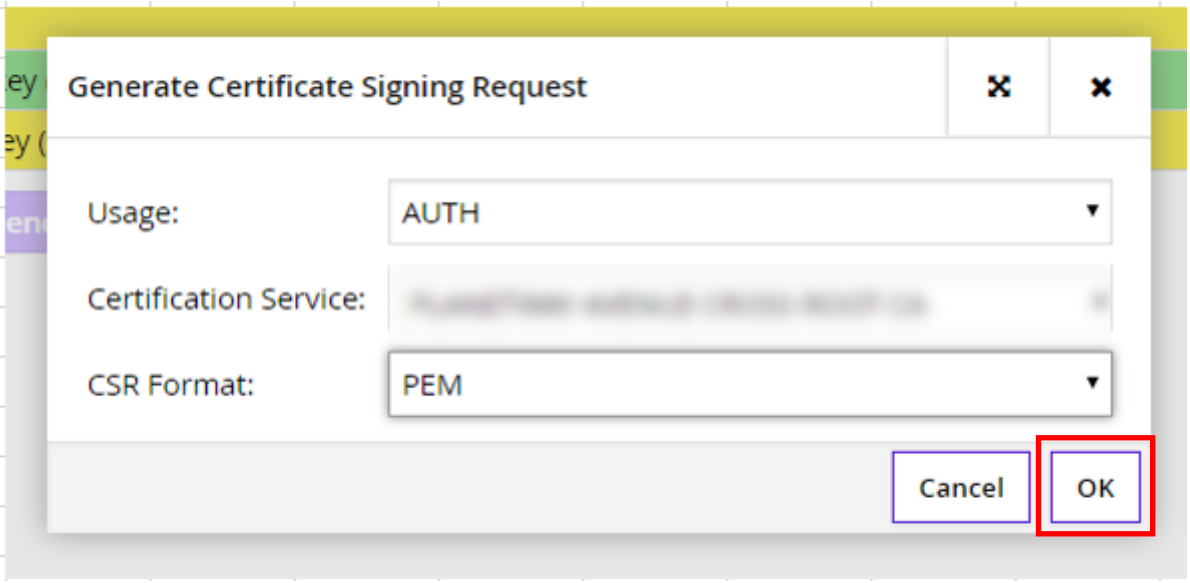
[Usage]: 「AUTH」を選択します。

[Certification Service]: 対象の CA※を選択します。

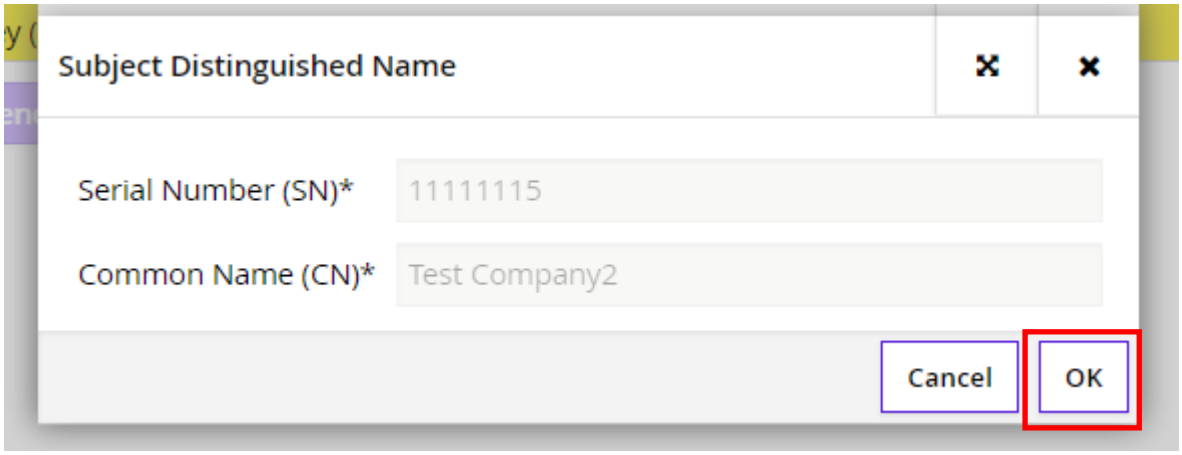
※指定する CA はご利用の環境、用途により異なりますのでご注意願います（本番／検証／PoC 開発）。各 CA はリリースノート別紙（指定事項）に記載しておりますのでご確認願います。不明の場合は Planetway 担当にご確認願います。

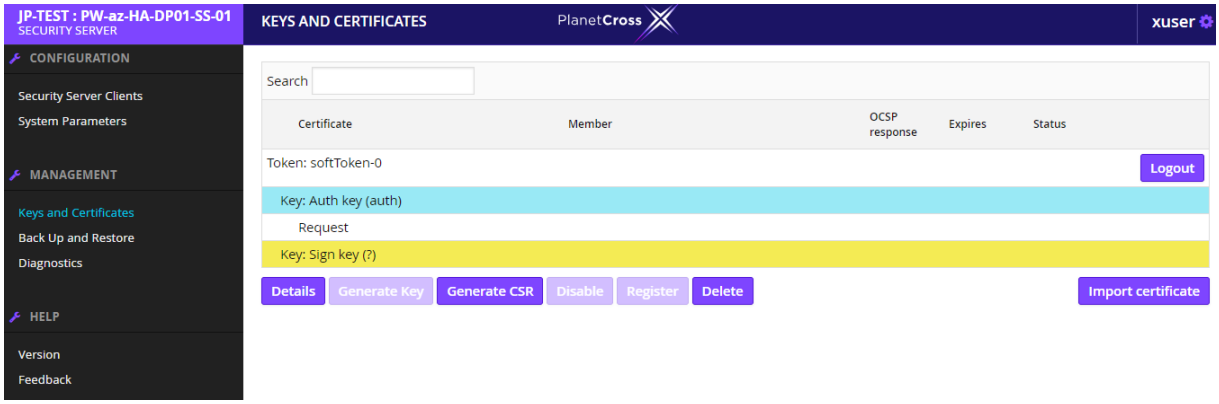
[CSR Format]: 「PEM」を選択します。

上記を選択後、[OK]ボタンを押します。

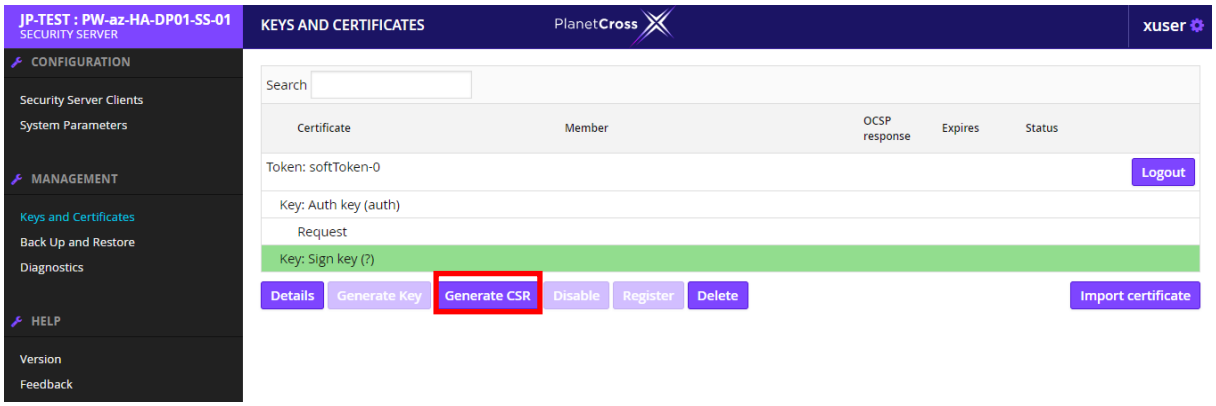


続いて、[OK]ボタンを押します。





認証用の秘密鍵を選択し、[Generate CSR]ボタンをクリックします。



[Usage]: 「SIGN」を選択します。

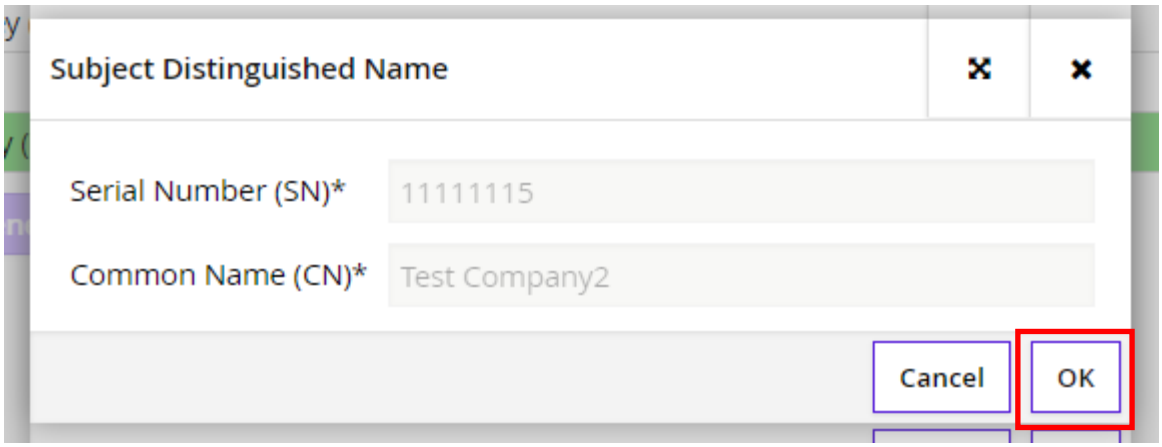
[Certification Service]: 対象の CA※を選択します。

※指定する CA はご利用の環境、用途により異なりますのでご注意願います（本番／検証／PoC 開発）。各 CA はリリースノート別紙（指定事項）に記載しておりますのでご確認願います。不明の場合は Planetway 担当にご確認願います。

[CSR Format]: 「PEM」を選択します。

上記を選択後、[OK]ボタンを押します。

続いて、[OK]ボタンを押します。



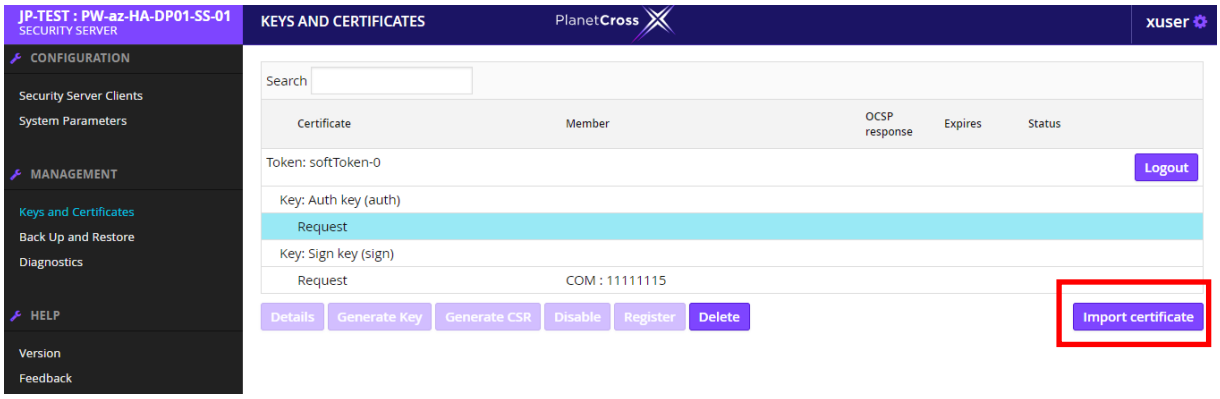
以下の情報を Planetway 社に送付します。

- 認証用の CSR
- 署名用の CSR
- この作業を行った Security Server Code (この例では「PW-az-HA-DP01-SS-01」)

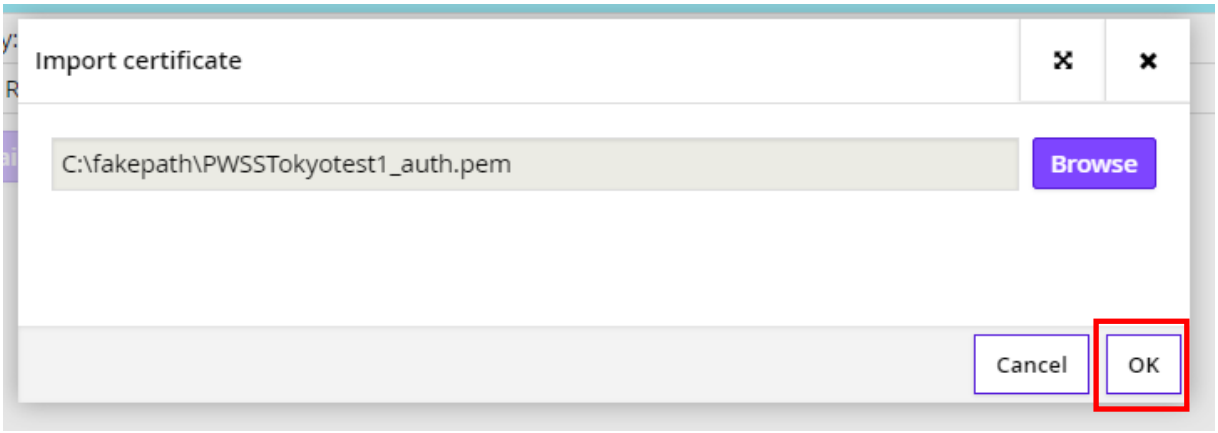
4.9 証明書の登録

Planetway 社から認証用、署名用の証明書を受け取り、Security Server に登録します。

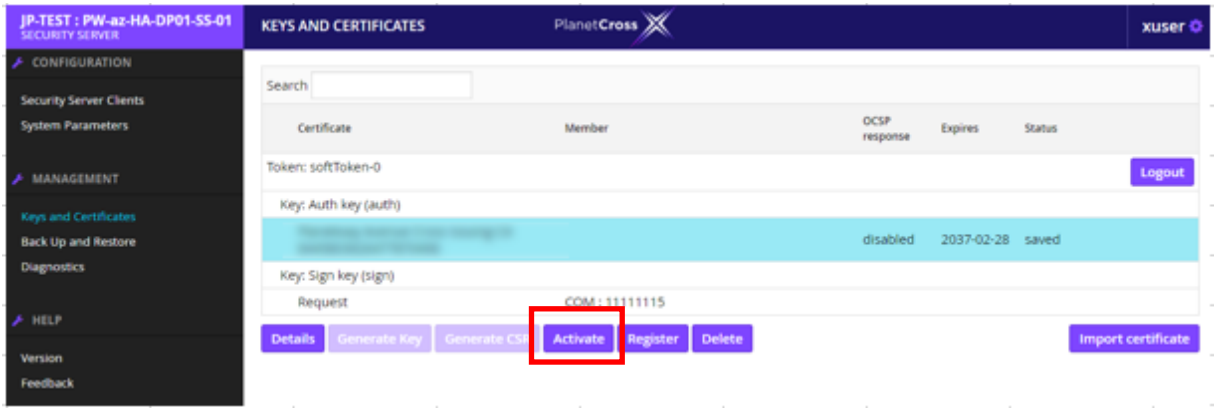
認証用キーを選択し、[Import certificate]ボタンを押します。

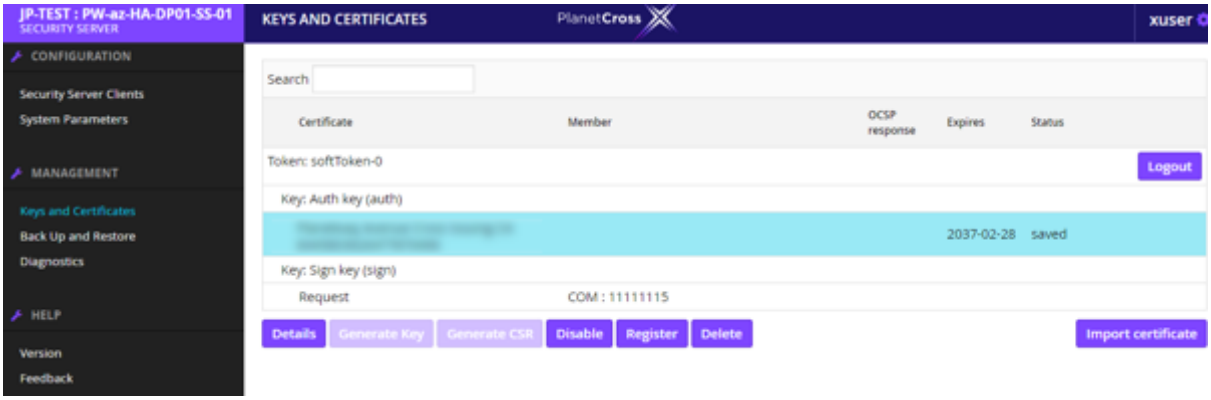


[Browse]ボタンを押して、認証用の証明書を選択し、[OK]ボタンを押します。

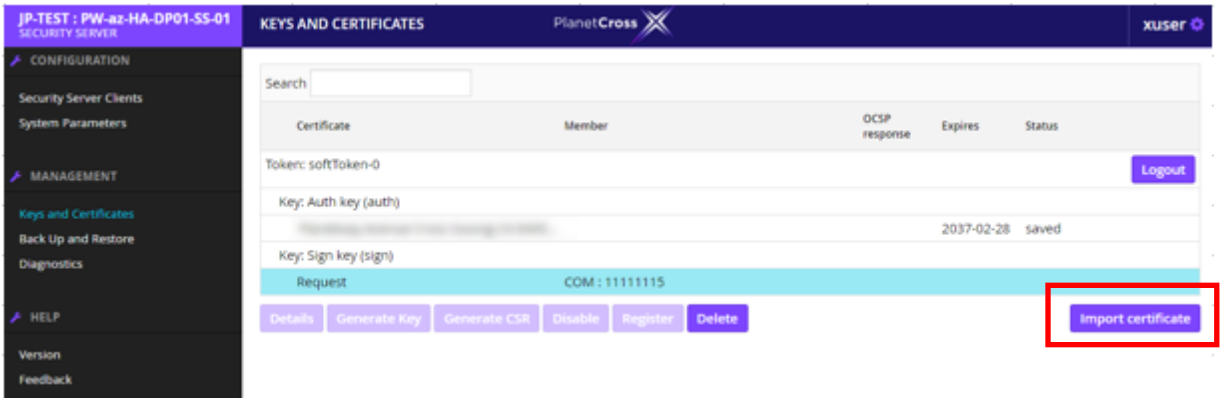


認証用証明書を選択し、[Activate]ボタンをクリックします。

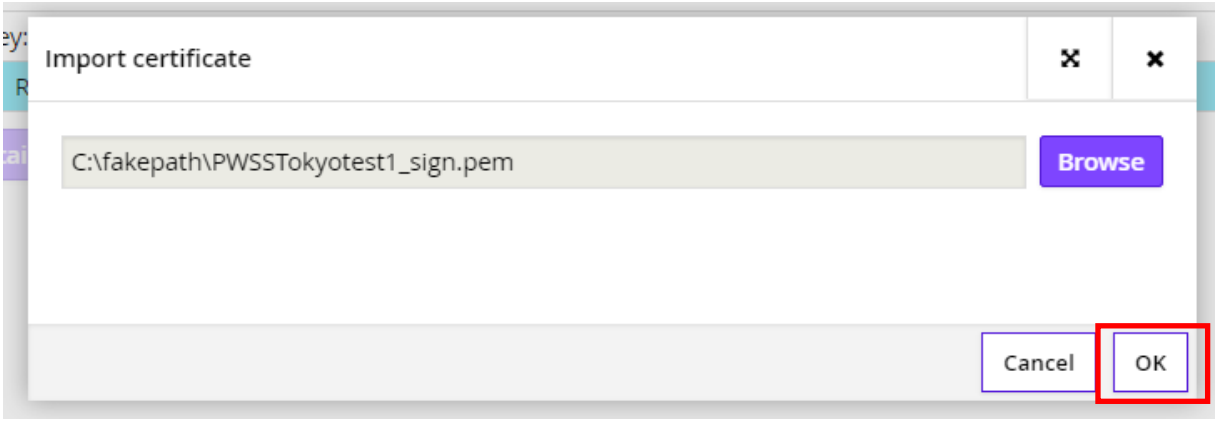


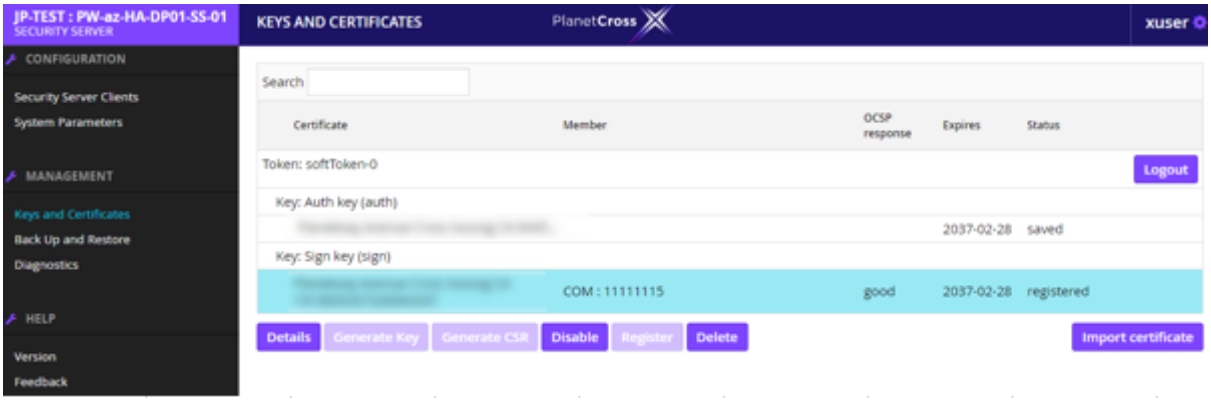


署名用キーも同様に選択し、[Import certificate]ボタンを押します。



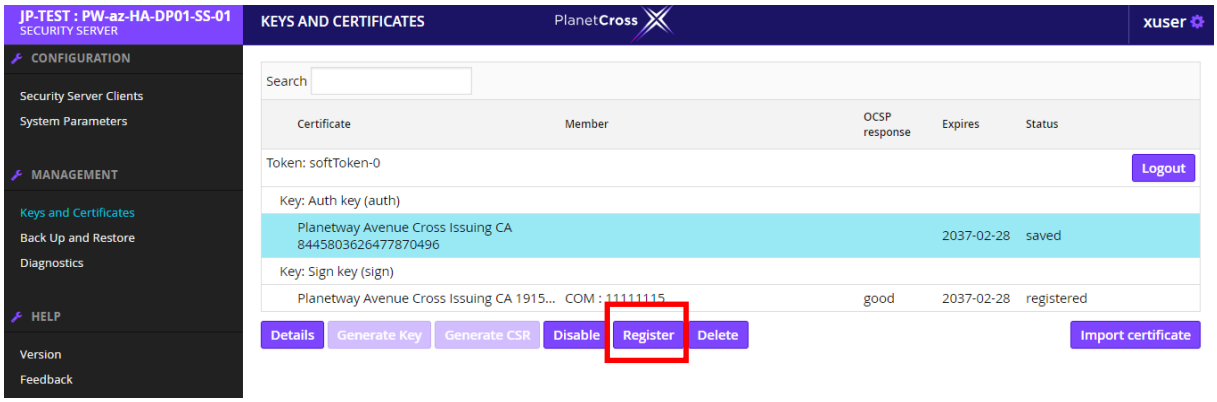
[Browse]ボタンを押して、署名用の証明書を選択し、[OK]ボタンを押します。



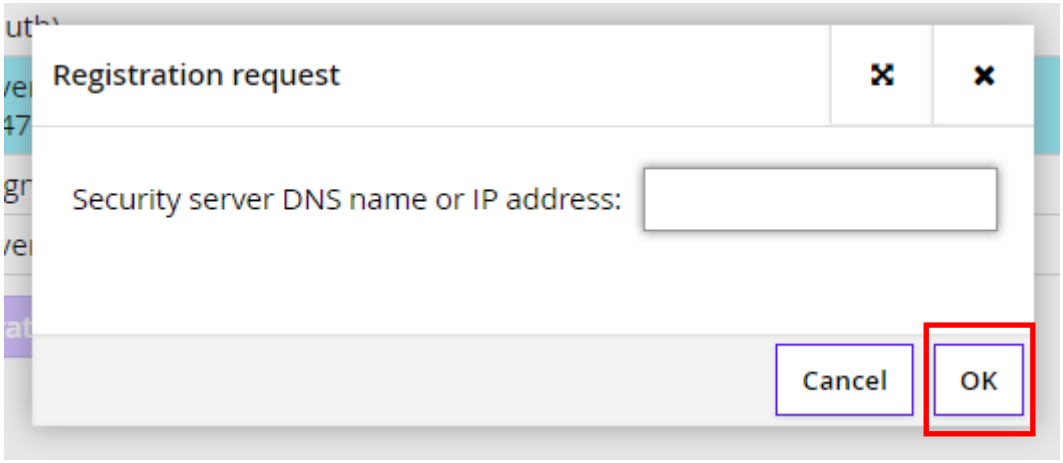


4.10 Security Server の登録

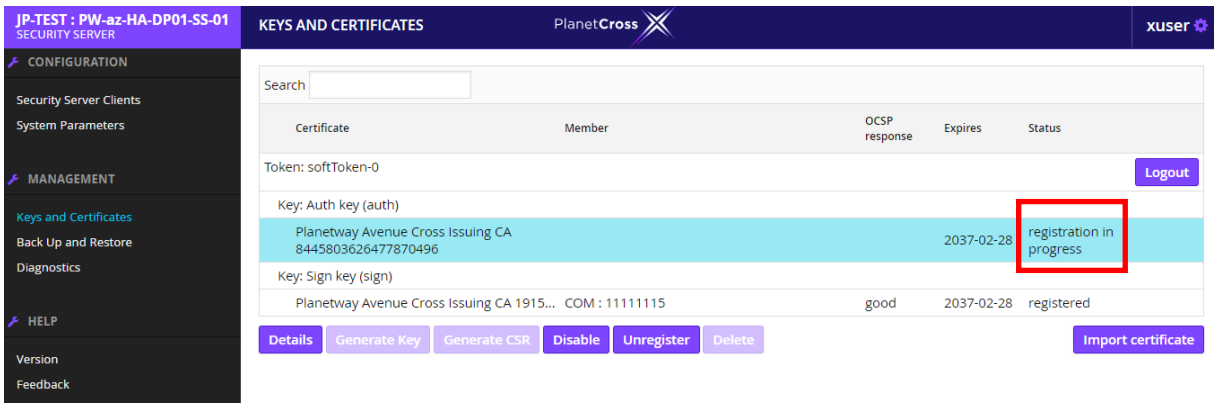
認証用証明書を選択し、[Register]ボタンをクリックします。



Security Server のグローバル IP またはホスト名を入力し、[OK]ボタンを押します。



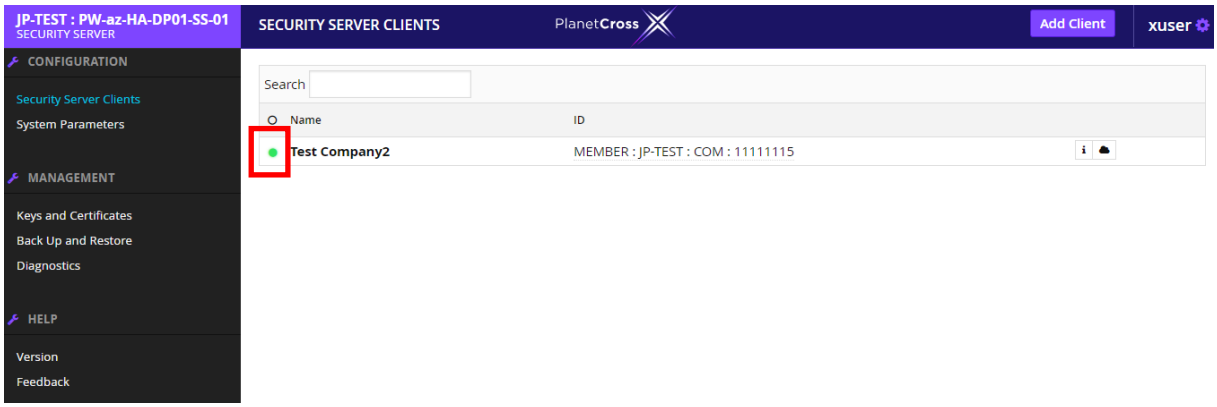
Status の欄が「registration in progress」になります。

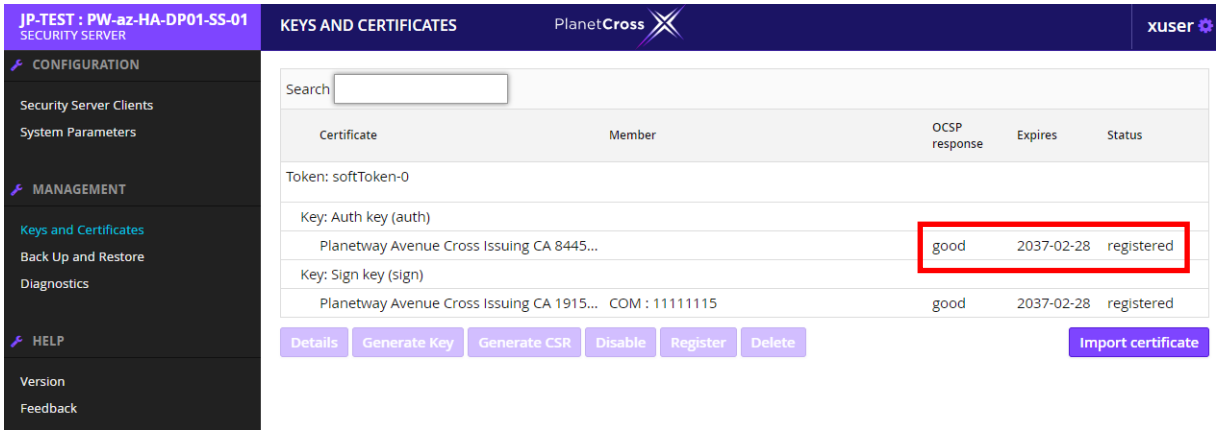


以下の情報を Planetway 社に送付します。

- この作業を行った Security Server Code (この例では「test-ss」)
- 認証用証明書(pem 形式)

Planetway 社の PlanetCross センターの作業が完了してしばらくすると、以下のように「registered」状態になります。

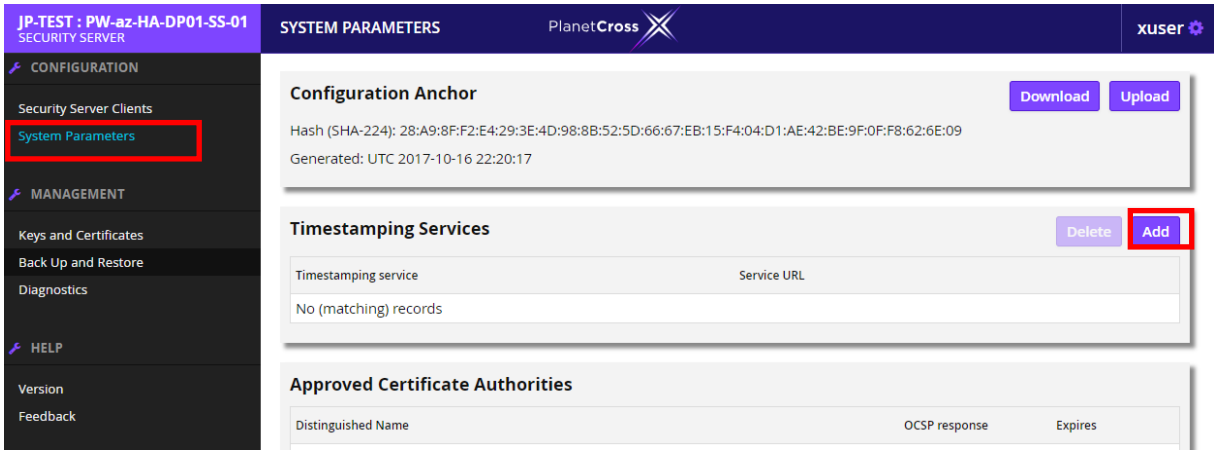




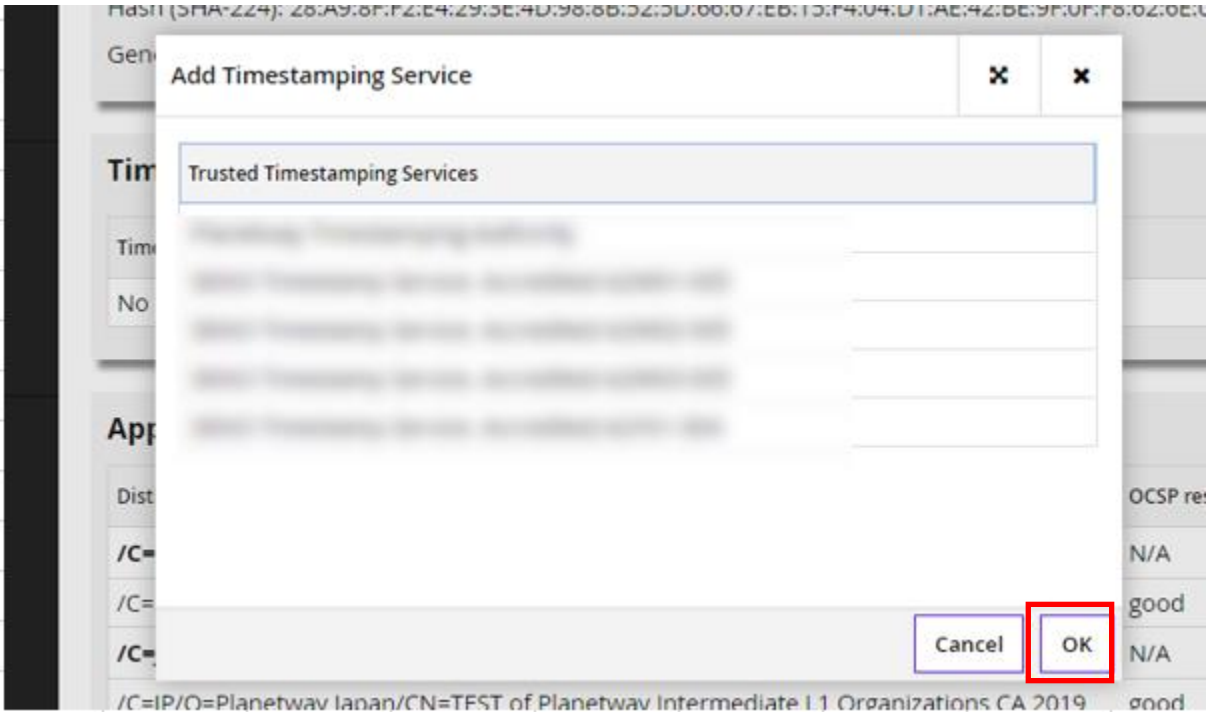
4.11 タイムスタンプサーバーの登録

以下のようにして、タイムスタンプサーバーを登録します。

[System Parameters]を選択し、[Timestamping Services]の[Add]ボタンを押します。



タイムスタンプサーバーを選択し、[OK]ボタンを押します。指定するタイムスタンプサーバーはご利用の環境、用途により異なりますのでご注意願います（本番／検証／PoC 開発）。各タイムスタンプサーバーはリリースノート別紙（指定事項）に記載しておりますのでご確認願います。



以上で、Security Server のインストール後の設定は完了です。

クライアントの追加、データサービスプロバイダーの追加を行うと、他組織とデータ連携が可能になります。詳しくは『Security Server 設定ガイド』を参照してください。

改訂履歴

バージョン	日付	変更履歴
第 1 版	2019 年 2 月 15 日	初版発行
第 1.1 版	2019 年 2 月 28 日	「4. 事前準備」以降の項を追加 ※新構成では「2.2 事前準備」
第 1.2 版	2019 年 3 月 8 日	文書内の画像を更新
		文書内の表現を更新
第 1.3 版	2019 年 3 月 29 日	文書内の表現を更新
		文書の章構成を全体的に更新
		「3.1.2 初期設定」の項を追加
		「7.10 Security Server の登録完了」(旧項目)を「Security Server の登録」(旧 7.9、新 3.10)に統合
第 1.4 版	2019 年 8 月 1 日	3 章に RHEL サポートを追加（これにより旧 3 章（初期設定）が 4 章に移動、システム要件を 1 章に集約）
		パッケージリポジトリサーバーに関する記載を修正
		文書内の表現を更新
第 1.5 版	2020 年 1 月 20 日	パッケージリポジトリサーバーに関する記載を修正
第 1.6 版	2020 年 2 月 5 日	商標についての記載を追加。フッターを更新