

SecureVisit

インストール マニュアル



Webシステムのセキュリティ向上の為に



飛天ジャパン株式会社

著作権と保証について

Copyright© Feitian Japan Co., Ltd. All Rights Reserved.

CD-ROM に含まれているプログラムおよびマニュアルなどの著作権は飛天ジャパン株式会社に帰属します。

本書のどの部分も、いかなる形態または手段（電子的または機械的）によっても、目的を問わず、飛天ジャパン株式会社の許可なしに複製することはできません。

- SecureVisit は飛天ジャパン株式会社の登録商標です。
- Microsoft, Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- Java およびすべての Java 関連の商標は米国およびその他の国における米国 Oracle, Inc.商標または登録商標です。
- Adobe, Adobe ロゴ, Adobe Acrobat は Adobe Systems Incorporated の商標です。
- UNIX は米国ならびに他の国における The Open Group の登録商標です。
- Linux は Linus Torvalds 氏の商標です。
- Red Hat は米国 Red Hat Software, Inc.の登録商標です。
- Ubuntu は Canonical 社の登録商標です。
- その他記載の会社名, 製品名はそれぞれの会社の商標もしくは登録商標です。

飛天ジャパン株式会社では、本書中の情報の正確さに万全の努力を払っておりますが、情報の誤りがあってもいかなる種類の直接あるいは間接的な損失、損害にも責任を負いません。本書に記載されている仕様などは予告なしに変更されることがあります。本書に例として記載されている名称はすべて架空であり、事実とは関係ありません。

更新履歴

日付	リビジョン	変更内容
2008 年 8 月	1.0	新規作成
2011 年 6 月	1.1	機能追加
2013 年 1 月	1.2	内容修正
2021 年 4 月	1.3	内容修正
2021 年 11 月	1.4	内容修正
2024 年 04 月	1.5	Ubuntu 対応
2024 年 10 月	1.6	内容修正

- 目次 -

はじめに	2
本マニュアルの構成について	2
マニュアルで使用している用語	2
SecureVisit インストール CD の構成	3
SecureVisit のインストール	4
1.1 インストール前の準備	4
1.1.1 システム要件	4
1.1.2 ポート番号の確認	4
1.1.3 ファイアウォールの設定	5
1.2 インストール	6
1.2.1 SecureVisit の deb パッケージの命名規則	6
1.2.2 インストール手順	6
1.3 アンインストール	13
1.4 ライセンス パッケージのインストール	13
1.5 管理画面用の証明書の発行と交換	16

はじめに

このマニュアルは、SecureVisit Web 認証システムを導入する企業や組織のシステム管理者を対象に、SecureVisit Web 認証システムのインストール方法などについて説明します。インストール作業の前に、SecureVisit Web 認証システムを理解するために『SecureVisitAdminGuide』の「第 1 章 システム概要」と「第 2 章 認証システムの導入」をご参照ください。

本マニュアルの構成について

このマニュアルには、次の内容が含まれています。

- ❖ **SecureVisit インストール CD の構成**

SecureVisit インストール CD 媒体の構成内容について説明します。

- ❖ **SecureVisit のインストール**

SecureVisit Web 認証システムのインストール手順、注意点などを説明します。

マニュアルで使用している用語

このマニュアルで使用している用語：

- ❖ **Web 管理画面**

SecureVisit Web 認証システムの Web 管理コンソールのことです。Edge/Chrome ブラウザからアクセスする事で様々な設定を行う事ができます。

- ❖ **SecureVisit インストール パッケージ**

SecureVisit 認証サーバプログラムのインストール用 deb パッケージです。

- ❖ **SecureVisit ライセンス パッケージ**

SecureVisit 認証サーバのライセンスファイルをインストールするソフトウェアパッケージです。

- ❖ **deb パッケージ**

Ubuntu は Debian ベースの Linux ディストリビューションであり、Deb パッケージを採用しています。そのため、Ubuntu でも Deb パッケージを使用してソフトウェアをインストール、管理、アンインストールします。

SecureVisit インストール CD の構成

SecureVisit インストール CD は、以下の内容を含む構成となっています。

SecureVisit Ubuntu Setup CD

docs/	SecureVisit 各種マニュアル
Ubuntu/	SecureVisit インストール パッケージ(Ubuntu 系 Linux 用)
win32/	管理者用トークンのドライバ セットアップ プログラム、トークン一括登録ツールなど
管理画面証明書	管理画面の証明書とパスワード
SecureVisit リリースノート.pdf	リリースノート

SecureVisit 製品を新規購入または追加購入する場合は、SecureVisit ライセンス パッケージが発行されます。

SecureVisit Ubuntu License CD

svcert.bin	SecureVisit ライセンス パッケージ
svisit.lcn	ライセンス詳細 (スタンドアロンサーバー)
svisitc-1.lcn	ライセンス詳細 (マスタサーバー)
svisitc-2.lcn	ライセンス詳細 (スレーブサーバー1)
svisitc-3.lcn	ライセンス詳細 (スレーブサーバー2)
svisitc-4.lcn	ライセンス詳細 (スレーブサーバー3)
ca.crt	ルート証明書
admin.p12	PKCS#12 形式の証明書
administrator.p12	PKCS#12 形式の証明書
server.crt	サーバーのデジタル証明書
server.key	サーバーの秘密鍵

注：SecureVisit ライセンス パッケージのファイル名は「svcert.bin」以外の場合もあります。
CD 中の readme.txt に記録しています。ご参照ください。

SecureVisit のインストール

1.1 インストール前の準備

1.1.1 システム要件

SecureVisit Web 認証システムを運用するための必要な動作環境は以下のようになっています。

サーバーOS 要件：

OS	Ubuntu Sever 22.04.4 LTS
----	--------------------------

サーバー ハードウェア要件：

CPU	Intel Celeron 1.7GHz 以上(2.06Hz 以上推奨)
メモリ	1GB 以上
HDD	50GB 以上
ネットワーク	1Gbps イーサネット 1 枚 (2 枚構成推奨)

参考：500 ユーザーでの利用を想定した場合の目安

CPU	Intel Dual-Core Xeon 2GHz(4 コア数)以上
メモリ	4GB 以上
HDD	100GB 以上
ネットワーク	1Gbps イーサネット 2 枚構成推奨

管理用クライアント PC の要件：

OS	Windows10/Windows11
ブラウザ	Edge(92 以降)、Chrome(92 以降)
その他	USB1.1/2.0/3.0 空きポートは 2 つ以上

1.1.2 ポート番号の確認

SecureVisit インストール パッケージの中では、認証サーバー プログラム以外に、認証サーバーの動作に必要なデータベース サーバーやウェブ サーバーのプログラムも含まれているため、デフォルトでは以下のような定められたポート番号を利用しています。

ポート 80/443	認証サーバーが利用するポート番号です。サーバーの設定によりませんが、デフォルトでは、HTTP を利用する場合は 80 に、HTTPS を利用する場合は 443 に設定することが多いです。
ポート 8888	SecureVisit の Web 管理画面が動作するウェブ サーバーに利用されるポート番号です。
ポート 5432	SecureVisit のデータベース サーバーに利用されるポート番号です。
ポート 1237	Edge または Chrome を使用する際、SecureVisit クライアントとサーバーとの通信ポートです。

SecureVisit をインストールする前に、以上のポート番号が、ほかのプログラムに利用されていると、インストールに失敗します。SecureVisit をインストールするために、これらのポートを利用しないように調整してください。

1.1.3 ファイアウォールの設定

SecureVisit を運用する際、リモートから認証サーバーと Web 管理画面が動作するウェブ サーバーにアクセスする必要があるため、これらのポートを開放していることを確認してください。

1.2 インストール

1.2.1 SecureVisit の deb パッケージの命名規則

SecureVisit インストール CD には、Ubuntu を対応する deb パッケージがありますが、間違った deb ファイルを使用してしまうと、インストールに失敗することもありますので、正しい deb パッケージを選択して、インストールしてください。

SecureVisit の deb パッケージの命名規則

SecureVisit の deb パッケージのファイル名は、次のようなフォーマットになっています。

svisitc_[version]_x64.deb

version は SecureVisit のバージョンです。

1.2.2 インストール手順

1. WinSCP を使用して Ubuntu サーバーにログインします。
2. サーバーのルートディレクトリ直下に「Ubuntu」フォルダを新規作成します。
3. ¥SecureVisit Ubuntu Setup CD¥Ubuntu 直下の svisitc_3.1.0_x64.deb ファイルをサーバーの「Ubuntu」フォルダにコピーします。
¥SecureVisit Ubuntu License CD 直下の以下の内容をサーバーの「Ubuntu」フォルダにコピーします。
 - etc フォルダ
 - share フォルダ
 - svcert.bin
 - copy_script.sh
4. インストールするマシンに root ユーザーとしてログインします。
5. Ubuntu ディレクトリに移動し、必要なプログラム（dialog、zip、cron、rsyslog）をインストールし、また、deb パッケージもインストールします。

```
#cd /Ubuntu/  
#apt-get install dialog  
#apt install zip  
#apt install cron  
#apt install rsyslog  
#apt install ./svisitc_3.1.0_x64.deb
```

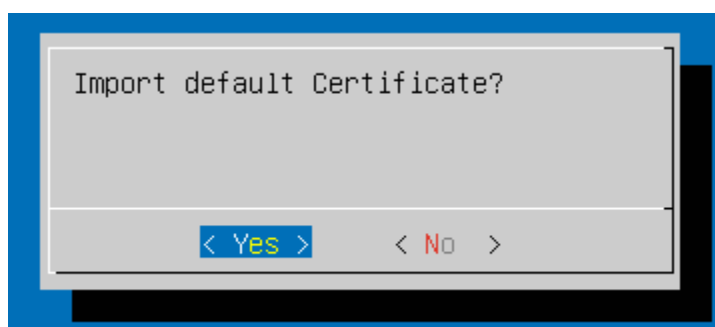

6. ライセンスファイルをインポートする前の準備及びライセンスファイルのインポートを行います。

```
chmod +x copy_script.sh
./copy_script.sh
sh svcert.bin
```

※アクセス分散処理を行いたい場合：

マスターサーバー：sh svcert.bin master

スレーブサーバー：sh svcert.bin slave1



「Yes」をクリックします。

※以下の情報を無視してください。

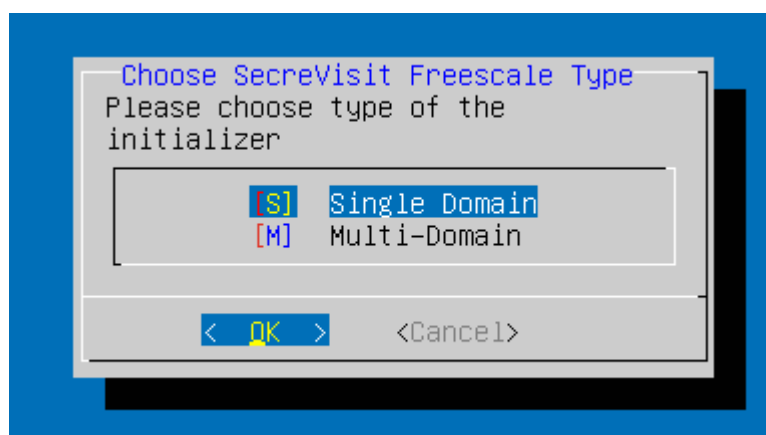
```
/usr/bin/install: cannot stat '/tmp/svtmp/server.key': No such file or directory
/usr/bin/install: cannot stat '/tmp/svtmp/server.crt': No such file or directory
/usr/bin/install: cannot stat '/tmp/svtmp/ca.crt': No such file or directory
/usr/bin/install: cannot stat '/tmp/svtmp/svisit.lcn': No such file or directory
```

7. 次のコマンドを実行し、初期化設定を行います。

※Slave サーバーでも、当該コマンドを実行し、初期化設定を行う必要があります。

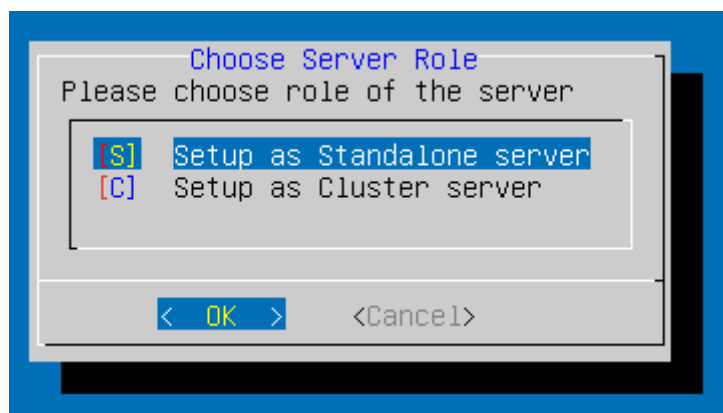
```
#/svisit/sbin/sv_init
```

8. SecureVisit 製品のタイプを選択します。



9. 保護されたいウェブサービスが一つのドメインの場合、「Single Domain」を選択してください、

続いてスタンドアロンまたはクラスタ構成を選択できます。

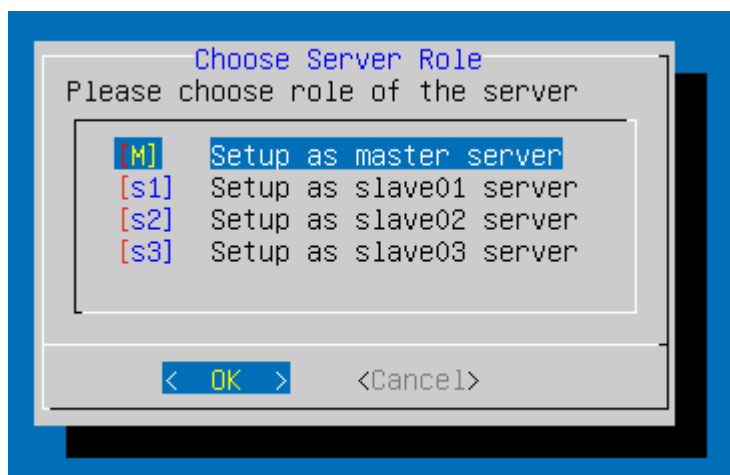


- (ア) 保護されたいウェブサービスにアクセス分散処理を追加する必要がない場合、「Setup as Standalone server」を選択してください。スタンドアロンサーバーとして初期化されます。

※以下のコマンドで SecureVisit サーバーを再起動します。

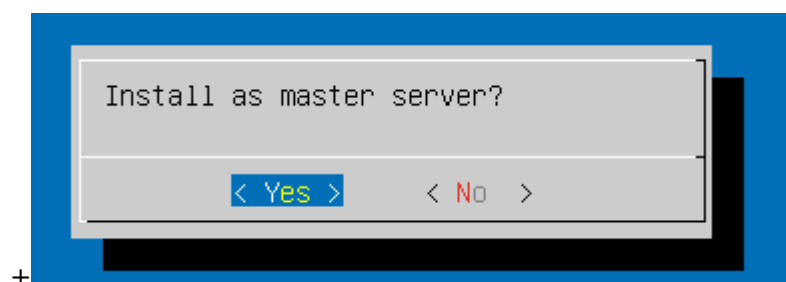
```
#service svisitd restart
```

- (イ) アクセス分散処理を行いたい場合は、「Setup as Cluster server」を選択してください。2種類のサーバーの役割を選択できます。

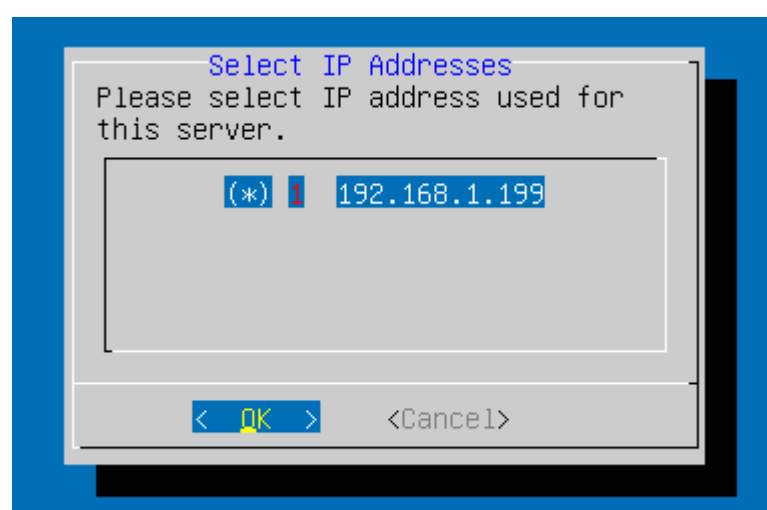


```
クライアント > ロードバラン > SecureVisit master server > 保護されたウェブサービス
SecureVisit slave server >
. >
. >
```

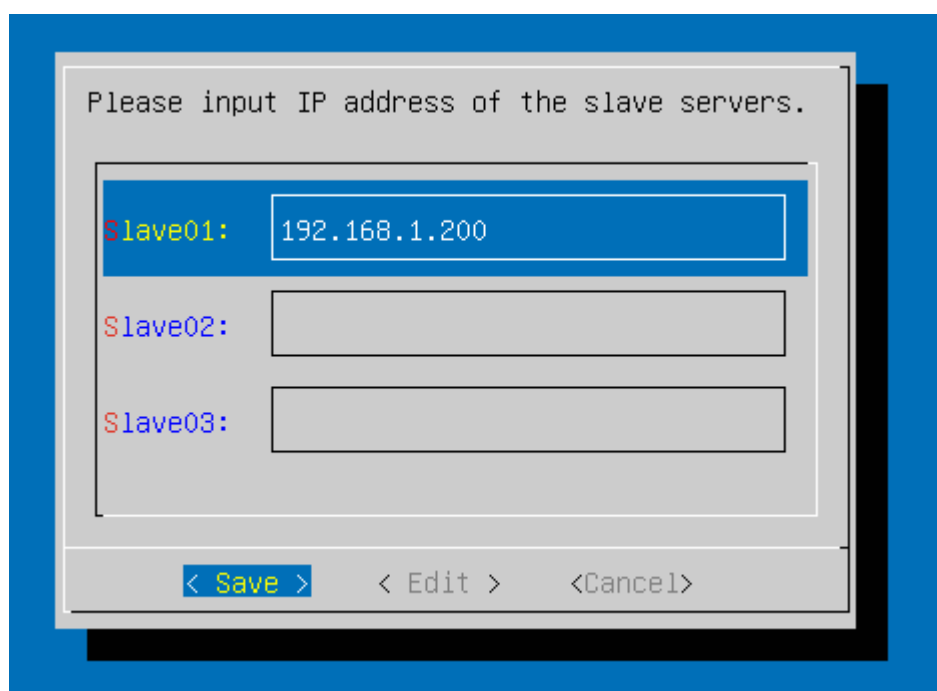
- ①.「Setup as master server」を選択する場合：



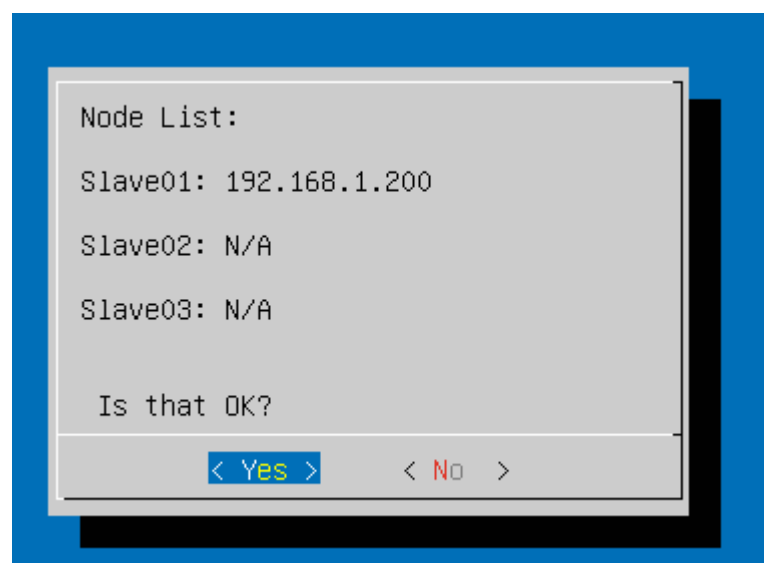
「Master サーバー」の IP アドレスを確認します。



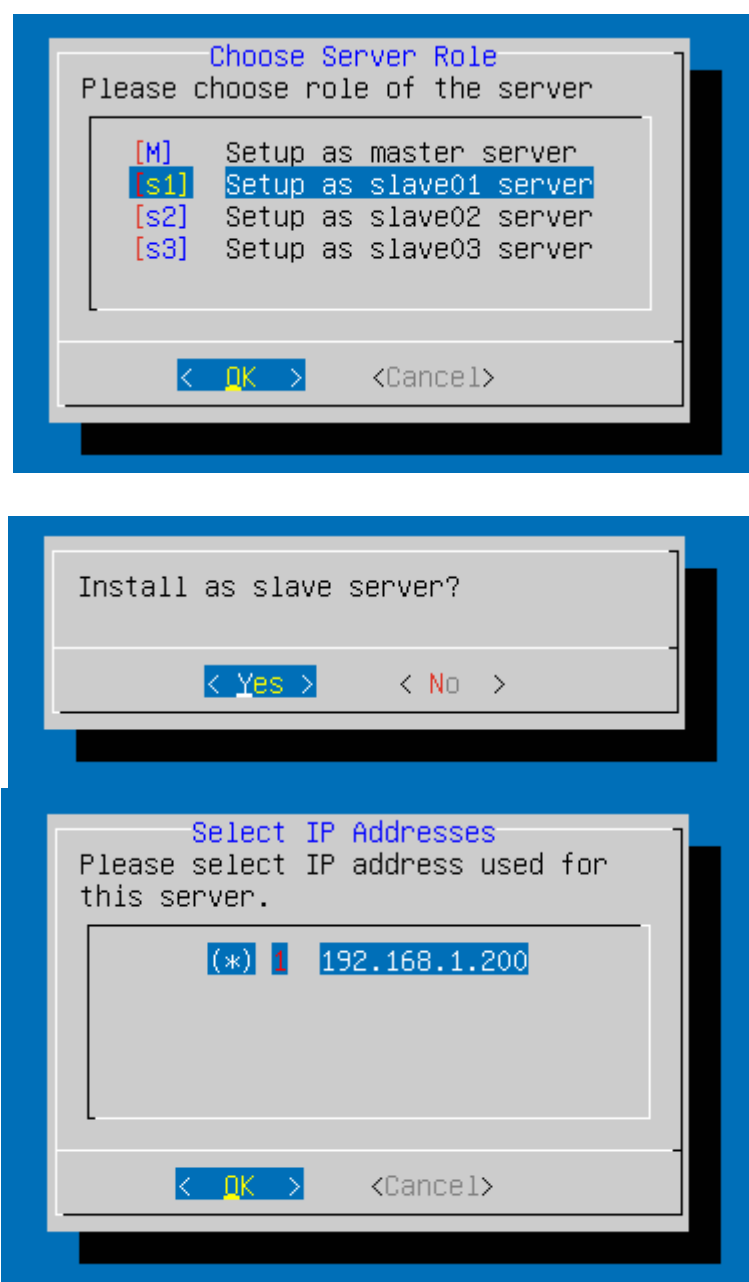
「Slave サーバー」の IP アドレスを設定します。



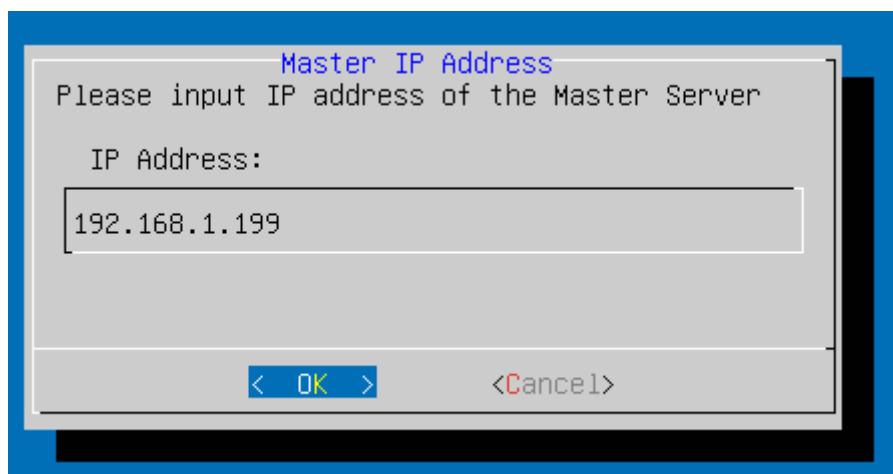
「Yes」をクリックすると、SecureVisit が起動されます。



②.「Setup as slave server」を選択する場合：



「Master サーバー」の IP アドレスを入力します。



「OK」をクリックすると、インストールが完了となります。

※以下のコマンドで SecureVisit サーバーを再起動します。

```
#service svisitd restart
```

10. 保護されたいウェブサービスが複数ドメインの場合、「Multi-Domain」を選択することで2種類のサーバーの役割を選択できます。

※現状、「Multi-Domain」をインストールする際、既知の問題が発生しているため、使用することができません。

1.3 アンインストール

以下の手順で、SecureVisit をアンインストールすることができます。アンインストールする前に、インストールするマシンに root ユーザーとしてログインしてから、アンインストールをしてください。

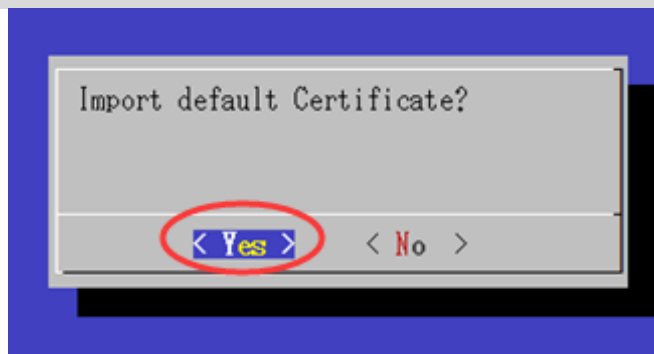
```
#service svisitd stop
#apt remove svisitc -y
```

1.4 ライセンス パッケージのインストール

SecureVisit のライセンス パッケージは、「Standalone server」と「Cluster server」の二種類があります。シェルスクリプトで作成されたものなので、シェルスクリプトとして実行すれば、インストールできます。インストールする前に、インストールするマシンに root ユーザーとしてログインしてから、インストールをしてください。

SecureVisit のライセンス パッケージが「Standalone server」である場合：

```
#service svisitd stop
#sh svcert.bin
```

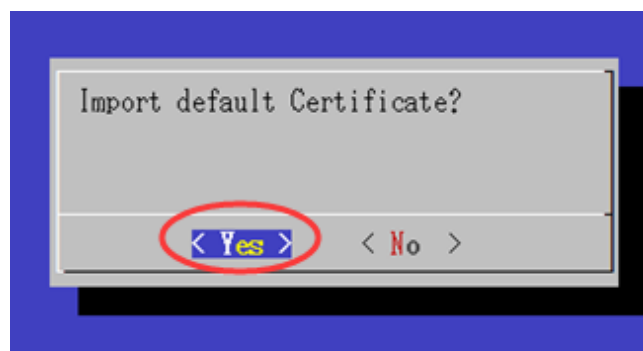


```
#service svisitd start
```

SecureVisit のライセンス パッケージが「Cluster server」である場合：

① master server の場合：

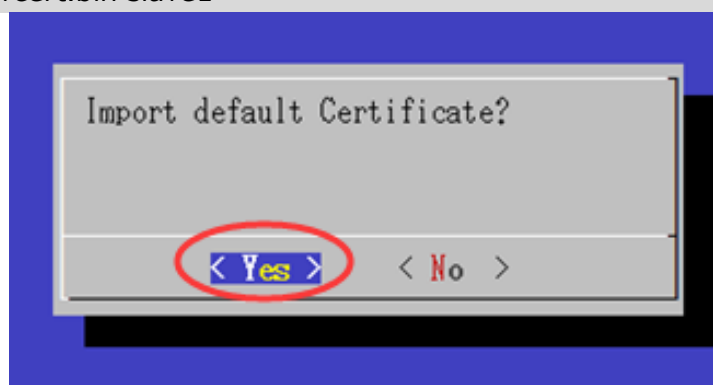
```
#service svisitd stop
#sh svcert.bin master
```



```
#service svisitd start
```

② slave01 server の場合 :

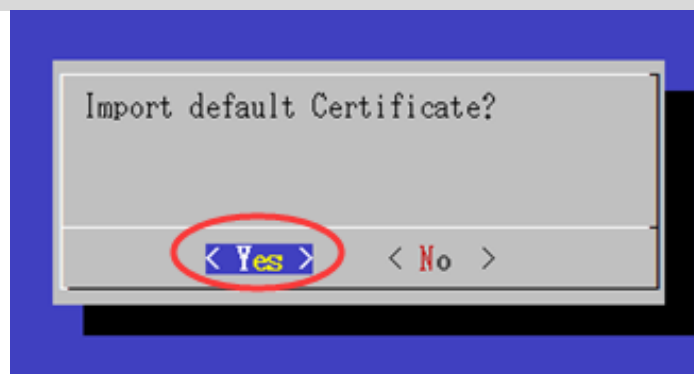
```
#service svisitd stop  
#sh svcert.bin slave1
```



```
#service svisitd start
```

③ slave02 server の場合 :

```
#service svisitd stop  
#sh svcert.bin slave2
```



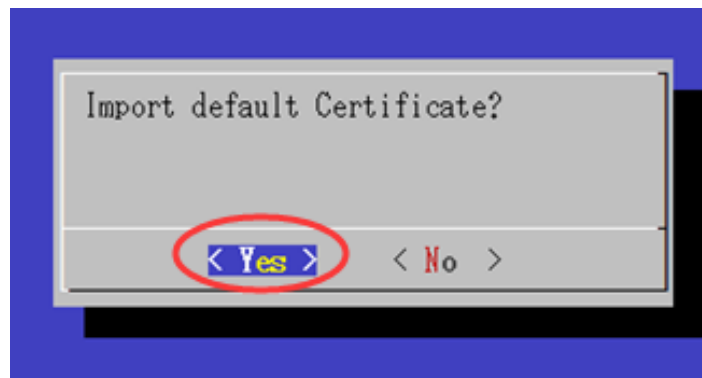
```
#service svisitd start
```

④ slave03 server の場合 :

```
#service svisitd stop
```



```
#sh svcert.bin slave3
```



```
#service svisitd start
```

ライセンスパッケージには、管理画面の SSL サーバー証明書が含まれています。「Yes」を選択した場合は、ライセンスパッケージにある SSL サーバー証明書がインストールされます。ライセンスパッケージのインストールが完了しましたら、必ずライセンスパッケージと一緒に発行された管理者用証明書を使用して Web 管理画面にアクセスしてご確認ください。「No」を選択した場合、SecureVisit インストールパッケージにある評価用の SSL サーバー証明書は引き続き使えます。インストールされたライセンスの内容は、Web 管理画面の「サーバー設定」の「ライセンス」画面で確認できます。

1.5 管理画面用の証明書の発行と交換

SecureVisit 管理画面は SSL を利用しています。SecureVisit 管理画面へアクセスするには管理者用クライアント証明書が必要です。「1.4」でライセンスパッケージをインストールするときに、出荷時に発行された証明書または評価用の証明書がインストールされますが、その後に利用者独自の証明書に取り換えることも可能です。利用者は、信頼する第三者証明書発行機関から発行された証明書または自署名証明書も利用できます。

以下は自署名証明書の交換方法について説明します。

例：

1. openssl の設定

```
#vi /usr/lib/ssl/openssl.cnf
```

「CA_default」下のパスや有効期間を設定してください。

例えば `dir=/svisit/CA`、`default_days=3650` とします。

2. CA(認証局)の構築

```
#/svisit/sbin/sv_create_ca
```

```
root@ip-192-168-0-214:/home/ubuntu# /svisit/sbin/sv_create_ca
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:JP
State or Province Name (full name) [Some-State]:Tokyo
Locality Name (eg, city) []:Tokyo
Organization Name (eg, company) [Internet Widdits Pty Ltd]:FTSAFE
Organizational Unit Name (eg, section) []:FTSAFE
Common Name (e.g. server FQDN or YOUR name) []:SecureVisit
Email Address []:support@ftsafeco.jp
```

赤色の部分は、各環境によって変更してください。実行が終了すると、「/svisit/CA」の下に「cacert.pem」が生成されます。

3. サーバー証明書の作成

```
#/svisit/sbin/sv_create_srv_cert server
```

```

root@ip-192-168-0-214:/home/ubuntu# /svisit/sbin/sv_create_srv_cert server
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:JP
State or Province Name (full name) [Some-State] Tokyo
Locality Name (eg, city) [] Tokyo
Organization Name (eg, company) [Internet Widgits Pty Ltd] FTSAFE
Organizational Unit Name (eg, section) [] FTSAFE
Common Name (e.g. server FQDN or YOUR name) [] SecureVisit
Email Address [] support@ftsafeco.jp

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /usr/lib/ssl/openssl.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 1 (0x1)
    Validity
        Not Before: Oct 10 07:52:09 2024 GMT
        Not After : Oct  8 07:52:09 2034 GMT
    Subject:
        countryName           = JP
        stateOrProvinceName    = Tokyo
        organizationName       = FTSAFE
        organizationalUnitName = FTSAFE
        commonName             = SecureVisit
        emailAddress           = support@ftsafeco.jp
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        X509v3 Subject Key Identifier:
            78:6C:FD:34:44:A2:0B:58:9A:80:C3:25:69:0B:A0:8E:D9:FD:A2:22
        X509v3 Authority Key Identifier:
            17:94:4C:E9:2F:FF:BF:C5:1B:B1:EC:C1:17:71:63:9B:65:24:63:BD
Certificate is to be certified until Oct  8 07:52:09 2034 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated

```

赤色の部分は、各環境によって変更してください。実行が終了すると、「/svisit/CA/private/」の下に server.key が生成されます、「/svisit/CA/certs/」の下に、server.crt が生成されます。

4. クライアント証明書の作成

```

root@ip-192-168-0-214:/home/ubuntu# /svisit/sbin/sv_create_cli_cert client
Enter PEM pass phrase: 
Verifying - Enter PEM pass phrase: 
Enter pass phrase for client.key: 
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU] JP
State or Province Name (full name) [Some-State] Tokyo
Locality Name (eg, city) [] Tokyo
Organization Name (eg, company) [Internet Widgits Pty Ltd] FTSAFE
Organizational Unit Name (eg, section) [] FTSAFE
Common Name (e.g. server FQDN or YOUR name) [] admin
Email Address [] support@ftsafeco.jp

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:
Using configuration from /usr/lib/ssl/openssl.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 2 (0x2)
    Validity
        Not Before: Oct 10 08:18:09 2024 GMT
        Not After : Oct  8 08:18:09 2034 GMT
    Subject:
        countryName             = JP
        stateOrProvinceName     = Tokyo
        organizationName        = FTSAFE
        organizationalUnitName  = FTSAFE
        commonName              = admin
        emailAddress            = support@ftsafeco.jp
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        X509v3 Subject Key Identifier:
            96:2F:B7:15:BA:91:D7:5B:52:64:0D:43:8F:19:0A:EA:56:99:02:0E
        X509v3 Authority Key Identifier:
            17:94:4C:E9:2F:FF:BF:C5:1B:B1:EC:C1:17:71:63:9B:65:24:63:BD
Certificate is to be certified until Oct  8 08:18:09 2034 GMT (3650 days)
Sign the certificate? [y/n] y

1 out of 1 certificate requests certified, commit? [y/n] y
Write out database with 1 new entries
Data Base Updated
Warning: -clcerts option ignored with -export
Enter pass phrase for client.key: 
Enter Export Password: 

```

赤色の部分とパスワードは、各環境によって変更してください。実行が終了すると、
「/svisit/CA/」の下に client.pfx が作成されます。

5. SecureVisit 証明書の交換

「1.」と「3.」で作成されたファイル「cacert.pem」、「server.crt」、「server.key」を SecureVisit の/svisit/etc/下にコピーしてください。SecureVisit を再起動してください。

```
#service svisitd restart
```

6. SecureVisit 管理者用クライアント証明書の導入

「4.」で作成された「client.pfx」ファイルを、管理者用の PC にインストールしてください。