cybertrust

SureServer/SureServer EV

Oracle iPlanet Web Server 6.1

CSR 作成/証明書インストール手順書

（新規・更新用）

Version 1.7

PUBLIC RELEASE

2017/04/28

改訂履歴

日付	バージョン	内容
2012/06/22	1.0	初版リリース
2012/08/27	1.1	「OU」に関する記述内容を修正
2013/06/26	1.2	SureServer(1024bit)の受付終了に伴う修正
2013/08/02	1.3	Cybertrust Japan Public CA G3 の提供開始に伴う修正
2014/01/06	1.4	SureServer(1024bit)の終了に伴う修正
2015/02/09	1.5	クロスルート証明書の変更に伴う修正
2016/12/15	1.6	「はじめに」の記述内容を修正
2017/04/28	1.7	「OU」に関する記述内容を修正

目次

はじめに

【！】本手順書をご利用の前に必ずお読みください

本ドキュメントは、「Oracle iPlanet Web Server 6.1(旧 Sun ONE Web Server)」の環境下でサイバートラストのサーバ証明書をご利用いただく際の CSR 作成とサーバ証明書のインストールについて解説するドキュメントです。

本手順は、「Oracle iPlanet Web Server 6.1 SP12」の環境下で動作確認をしております。

「Oracle iPlanet Web Server 6.1」がすでに設定されており、「Oracle iPlanet Web Server 6.1」単独での動作確認ができている事を前提としております。

実際の手順はお客様の環境により異なる場合があり、「Oracle iPlanet Web Server 6.1」の動作を保証するものではございません。あらかじめご了承ください。

なお、このドキュメントは予告なく変更される場合があり、サイバートラスト株式会社はその内容に対して責任を負うものではありません。

また、このドキュメント内に誤りがあった場合、サイバートラスト株式会社は一切の責任を負いません。

サーバ証明書お申込みフロー

サーバ証明書のご購入については、以下のお申込みフローをご確認ください。

本手順では、赤枠で囲まれた部分のフローをご案内しています。

STEP1	お申込み前の確認	お申込み前の確認
	CSR の作成　P6～	
STEP2	WEB からのお申し込み(SureBoard / SureHandsOn)	
STEP3	必要書類送付/申請の意思確認(電話) 証明書の発行	
STEP4	証明書のダウンロード　P18～	
STEP5	証明書のインストール　P19～	
STEP6	SSL 通信の確認　P31～	

CSR の作成

1. CSR 作成前のご確認事項

CSR 作成前に以下についてご確認ください。

1.1. 公開鍵長のご指定について

公開鍵長は「2048bit」をご指定ください。

※クラウド商品(for クラウド)、マルチドメイン商品(SureServer MD など)を含みます。

1.2. CSR 作成時に指定する項目(DN)について

詳細は以下をご確認ください。

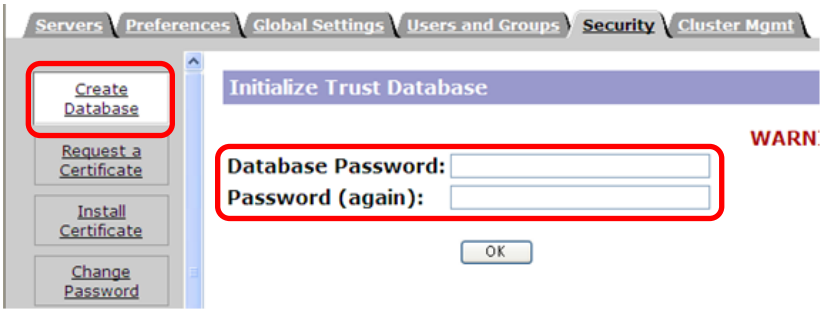
≫CSR 作成時に指定する項目について

1.3. キーデータベースファイルについて

CSR を作成する場合、キーデータベースファイルが事前に作成されている必要があります。

キーデータベースファイルがない場合は、管理コンソールへログイン後、所定のサーバ上で【Security】タブをクリックし、【Create Database】でインスタンス用データベースへのアクセスパスワードを設定して作成します。

※サーバ証明書のインストールや SSL 通信を行うサーバの起動の際などに、キーデータベースファイルのパスワードが必要です。



2. キーペア・CSR の作成

2.1. CSR の作成方法

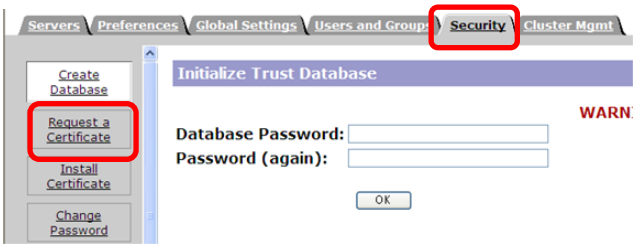
「Oracle iPlanet Web Server 6.1」では、ご利用のバージョンにより CSR の作成方法が異なります。

バージョン	CSR 作成方法
SP13 以降	管理コンソールから作成します
SP13 未満	付属のユーティリティ(certutil)コマンドを使用し、CSR を作成します。

2.2. バージョン SP13 以降の CSR 作成方法

A) 管理コンソールへログインし、【Manage Severs】の【Select a Server】項目で CSR を作成するサーバ名を指定して、【Manage】ボタンをクリックします。

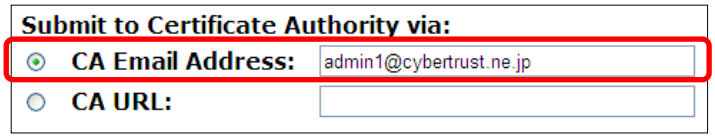
B) 【Security】タブをクリックし、【Request a Certificate】をクリックします。



C) CSR 作成に必要な項目を設定します。

- 新規の場合:【New Certificate】を選択してください。
- 更新の場合:【Certificate renewal】を選択してください。

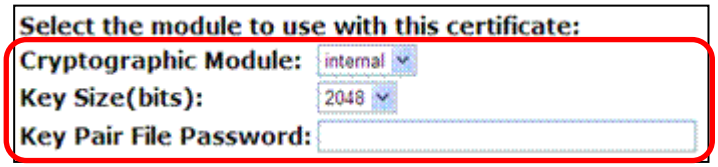
D) Submit to Certificate Authority via



- 【CA Email Address】を選択し、任意の E メールアドレスを入力してください。

  ※入力内容は申請や発行される証明書に影響ありません。

E) Select the module to use with this certificate

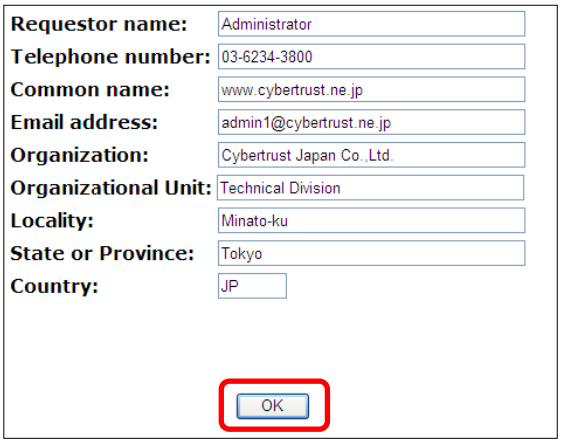


- 【Cryptographic Module】:【internal】を選択します。

  ※外部トークンを使用する場合は、ドロップダウンリストから外部トークンの名前を選択してください。

- 【Key Size(bits)】:【2048】を選択します。
- 【Key Pair File Password】:キーデータベースファイルのパスワードを入力します。

F) CSR 作成に必要な DN 情報を入力して、【OK】ボタンをクリックします。(全て必須入力項目です。)



入力内容については以下の表をご参照ください。

※●印の付いている項目は、証明書の DN 情報(識別名)記載項目で、CSR に含まれる値です。

	入力項目	必須/任意	内容	入力例
	Requestor name	必須	任意の氏名	Administrator
	Telephone number	必須	任意の電話番号	03-6234-3800
●	Common name	必須	完全なドメイン名(FQDN)	www.cybertrust.ne.jp
	Email address	必須	任意の E メールアドレス	admin1@cybertrust.ne.jp
●	Organization	必須	申請組織の名称(英語)	Cybertrust Japan Co.,Ltd.
●	Organizational Unit	任意	「部署名」(※)	Technical Division
●	Locality	必須	申請組織の事業所住所の「市町村名」(英語) ※東京は 23 区	Minato-ku
●	State or Province	必須	申請組織の事業所住所の「都道府県名」(英語)	Tokyo
●	Country	必須	申請組織の国名	JP

※指定可能な値については、「組織単位名(OU)について」をご覧ください。

G)「Certificate request has been generated.」と表示され、CSR が作成されます。

表示された内容に誤りがないことを確認のうえ、「-----BEGIN NEW CERTIFICATE REQUEST----」から、「----- END NEW CERTIFICATE REQUEST-----」の部分までをコピーし、任意の名前でテキストファイルなどに保存してください。

※上記画面で指定されている「The mail that you should is in the fie ＜保存先ディレクトリ＞」のディレクトリに CSR が保存されております。

以上で、CSR の作成は完了です。

※「3. 鍵ペアファイルのバックアップ」へお進みください。

2.3. バージョン SP13 未満の CSR 作成方法

管理コンソールで公開鍵長 2048bit の選択ができないため、Oracle iPlanet Web Server 付属のユーティリティ(certutil)を使用して CSR を作成します。

A) 以下のコマンドを入力して CSR を作成します。

<サーバルート>¥bin¥https¥admin¥bin¥certutil -R -s <DN 情報> -p <電話番号> -o <出力ファイル名指定> -d <alias> -a -t "u,u,u" -g <公開鍵長> -P <データベースファイル名>

■ 入力例

※以下の環境で実行した例です。

OS: Windows OS
サーバルート: C:¥Sun¥WebServer6.1
インスタンス名: instance
ホスト名: host

C:¥Sun¥WebServer6.1¥bin¥https¥admin¥bin¥certutil -R -s "C=JP, ST=Tokyo, L=Minato-ku, O=Cybertrust Japan Co.¥,Ltd., OU=Technical Division CN=www.cybertrust.ne.jp" -p "03-6234-3800" -o server.csr -d C:¥Sun¥WebServer6.1¥alias -a -t "u,u,u" -g 2048 -P https-instance-host-

■ コマンドで指定する内容

項目	内容	入力例
-R	CSR 作成	
-s	DN 情報を入力	(※2)
-p	任意の電話番号を入力	03-6234-3800
-o	任意の出力ファイル名を指定。	server.csr
-d	alias フォルダ名を指定	C:¥Sun¥WebServer6.1¥alias
-a	ASCII での出力を指定	
-t	証明書の属性を指定	"u,u,u"
-g	公開鍵長を指定	2048
-P	データベースファイル名を指定 (インスタンス名-ホスト名-)(※1)	https-instance-host-

※1　インスタンス名、および、ホスト名が不明な場合は、alias フォルダ内の「cert8.db」、もしくは、「key3.db」ファイル名の「https-インスタンス名-ホスト名-」部分をご確認ください。

※2　入力内容の詳細については以下の表をご参照ください。

項目	内容	入力例
C	申請する組織の国名を選択してください。	JP
ST	申請組織の事業所住所の「都道府県名」を英語で入力してください。	Tokyo
L	申請組織の事業所住所の「市町村名」(東京は 23 区)を英語で入力してください。	Minato-ku
O	申請組織の名称を英語で入力してください。	Cybertrust Japan Co.,Ltd.
OU	必要に応じて、「部署名」を入力してください。(※)	Technical Division
CN	完全なドメイン名(FQDN)を入力してください。	www.cybertrust.ne.jp

※指定可能な値については、「組織単位名(OU)について」をご覧ください。

■ DN 情報中の文字列に「,」(カンマ)を含める方法

DN 情報中の文字列に「,」(カンマ)を含める方法はお使いの OS ごとに指定方法が異なります。

- **Windows の場合**

  DN 情報全体を「″」ダブルクォーテーションで囲み、【,】(カンマ)文字の前に「¥」エスケープ文字を置く

  【入力例】

  ″C=JP, ST=Tokyo, L=Minato-ku, O=Cybertrust Japan Co.¥,Ltd., OU=Technical Division, CN=www.cybertrust.ne.jp″

- **SUN Solaris SPARC 版 の場合**

  DN 情報全体を「'」シングルクォーテーションで囲み、各 DN の項目を「″」ダブルクォーテーションで囲む

  【入力例】

  'C=″JP″, ST=″Tokyo″, L=″Minato-ku″, O=″Cybertrust Japan Co.,Ltd.″, OU=″Technical Division″, CN=″www.cybertrust.ne.jp″'

B) キーデータベースファイルのパスワードを入力します。

```
Enter Password or Pin for "NSS Certificate DB":
```

C) プログレスメーターが埋まるまで任意のキーを入力し、【Finished.】と表示されたら、Enter キーを押します。

```
A random seed must be generated that will be used in the
creation of your key.  One of the easiest ways to create a
random seed is to use the timing of keystrokes on a keyboard.

To begin, type keys on the keyboard until this progress meter
is full.  DO NOT USE THE AUTOREPEAT FUNCTION ON YOUR KEYBOARD!


Continue typing until the progress meter is full:

|**********************************************************|

Finished.  Press enter to continue:
```

D) 指定した出力先に CSR が作成されます。

```
Generating key.  This may take a few moments...
```

以上で、CSR の作成は完了です。

3. 鍵ペアファイルのバックアップ

鍵ペアファイルは証明書のインストール時に必要となります。

万が一に備えて、必ず別のメディア(CD や USB 等)にコピーして安全な場所に保管してください。

なお、弊社がお客様の鍵ペアファイルの情報を受け取ることはございません。あらかじめご了承ください。

※デフォルトでは、以下のディレクトリに鍵ペアファイルが保存されています。

<サーバルート>/alias/https-<サーバインスタンス名>-key3.db

<サーバルート>/alias/https-<サーバインスタンス名>-cert8.db

4. 証明書のお申し込み

作成した CSR をテキストエディタで開いて内容をコピーし、WEB の申請サイト(SureBoard / SureHandsOn)の申請フォームへ貼り付けて、弊社へお申し込みください。

＜CSR サンプル＞ ※申請にはご利用いただけません。

```
-----BEGIN NEW CERTIFICATE REQUEST-----
・・・・・
MIIEhDCCA2wCAQAwgYkxCzAJBgNVBAYTAkpQMQ4wDAYDVQQIDAVUb2t5bzESMBAG
A1UEBwwJTWluYXRvLWt1MSIwIAYDVQQKDBlDeWJlcnRydXN0IEphcGFuIENvLixM
dGQuMRIwEAYDVQQLDAlUZXN0IFVuaXQxHjAcBgNVBAMMFXRlc3QuY3liZXJOcnVz
2t/rD9fTPgo7u4aYzw4BpnAqLmGgy3XpsvCo6f4ROcFsgrkO5FgeUCaeDFyllEST
・・・・・
-----END NEW CERTIFICATE REQUEST-----
```

「-----BEGIN NEW CERTIFICATE REQUEST-----」から、「-----END NEW CERTIFICATE REQUEST-----」までをハイフンを含め、すべてコピーし申請画面に貼り付けてください。

1 文字でも欠けるとフォーマットエラーとなりますのでご注意ください。

証明書のインストール

【！】本手順はサーバ証明書の発行後に行います。

5. 証明書のダウンロード

インストールが必要となる中間 CA 証明書・SSL サーバ証明書を事前にダウンロードします。

5.1. 中間 CA 証明書のダウンロード

サーバ証明書をご利用の際、お使いの機器へ中間 CA 証明書のインストールが必要となります。

ご選択いただいた商品により必要な証明書が異なりますので、証明書の種類をご確認のうえ、以下弊社ホームページからダウンロードしてください。

≫ ルート・中間 CA 証明書のダウンロード

また、ご利用商品や必要な証明書の種類がご不明の場合は、以下をご覧ください。

≫どの中間 CA 証明書をダウンロードすればよいですか？

5.2. SSL サーバ証明書のダウンロード

SSL サーバ証明書が発行されましたら、証明書発行のお知らせのメール内リンクより事前にダウンロードし、【.cer】や【.txt】などの拡張子で保存してください。

≫ SSL サーバ証明書のダウンロードについて

6. 証明書のインストール

中間 CA 証明書とサーバ証明書のインストールを行います。

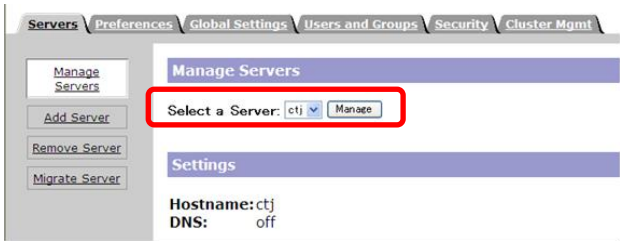
6.1. 中間 CA 証明書のインストール

中間 CA 証明書のインストールを行います。

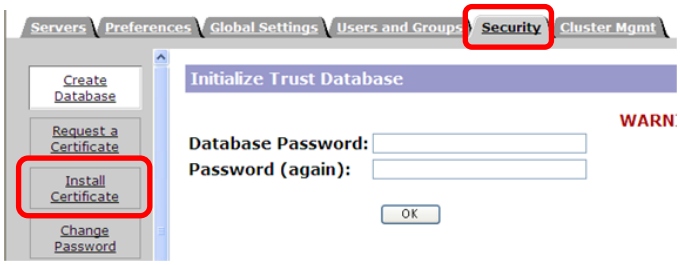
※更新の際、必要な中間 CA 証明書が既にインストールされている場合は、本手順をスキップしてください。

※SureServer EV[2048bit]・SureServer EV[SHA-2]、および、SureServer[2048bit]用クロスルート方式では、同様の手順で「クロスルート用中間 CA 証明書」と「中間 CA 証明書」をインストールしてください。

A) 管理コンソールへログインし、【Manage Servers】の【Select a Server】項目で中間 CA 証明書をインストールするサーバ名を指定して、【Manage】ボタンをクリックします。



B) 【Security】タブをクリックし、【Install Certificate】をクリックします。

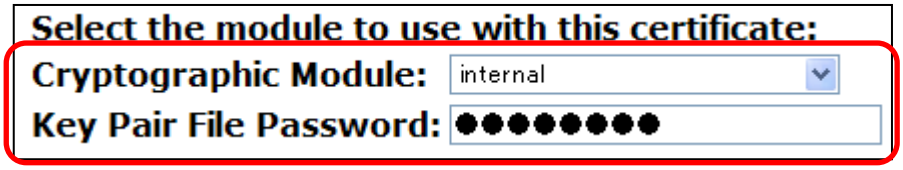


C) インストールに必要な項目を設定します。

■ Certificate For

- 【Server Certificate Chain】を選択してください。

■ Select the module to use with this certificate

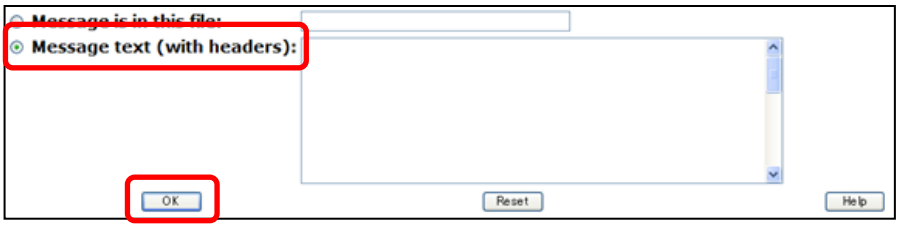


- 【Cryptographic Module】:【internal】を選択します。

  ※外部トークンを使用する場合は、ドロップダウンリストから外部トークンの名前を選択してください。

- 【Key Pair File Password】:キーデータベースファイルのパスワードを入力します。

■ Enter Certificate Name ONLY if certificate is not for 'This Server'.

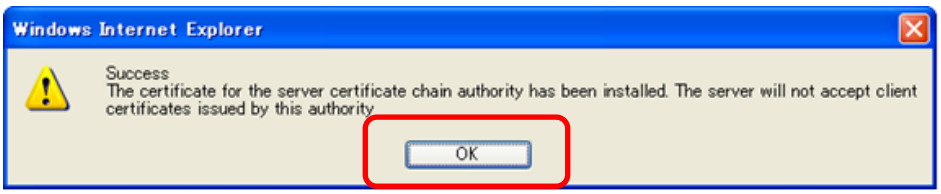


- 【Message text(with headers)】にチェックを入れます。
- 入力欄へ中間 CA 証明書ファイルの「-----BEGIN CERTIFICATE-----」から「-----END CERTIFICATE-----」までをハイフンを含め、すべてコピーして貼り付けて、【次へ】ボタンをクリックします。

D) インストールする中間 CA 証明書の内容を確認し、【Add Server Certificate】ボタンをクリックします。

E) 【OK】をクリックします。

F) 証明書のインストールが成功した旨が表示されますので、【OK】をクリックします。



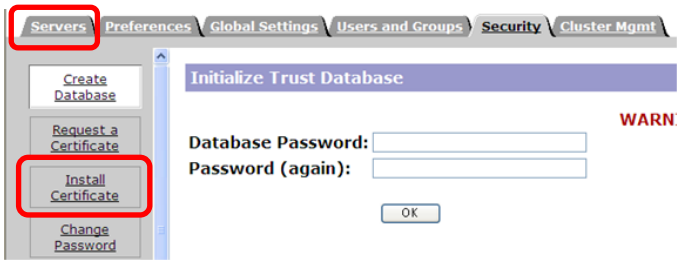
以上で中間CA証明書のインストールが完了します。

6.2. SSL サーバ証明書のインストール

SSL サーバ証明書のインストールを行います。

A) 管理コンソールへログインし、【Manage Servers】の【Select a Server】項目で SSL サーバ証明書をインストールするサーバ名を指定して、【Manage】ボタンをクリックします。

B) 【Security】タブをクリックし、【Install Certificate】をクリックします。

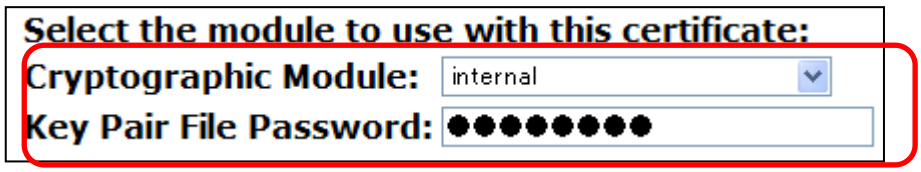


C) インストールに必要な項目を設定します。

■ Certificate For

- 【This Server】を選択してください。

■ Select the module to use with this certificate



- 【Cryptographic Module】:【internal】を選択します。

  ※外部トークンを使用する場合は、ドロップダウンリストから外部トークンの名前を選択してください。

- 【Key Pair File Password】:キーデータベースファイルのパスワードを入力します。

■ Enter Certificate Name ONLY if certificate is not for 'This Server'.

・【Certificate Name】: 入力不要です。

・【Message text(with headers)】にチェックを入れます。

・入力欄へ SSL サーバ証明書ファイルの「-----BEGIN CERTIFICATE-----」から「-----END CERTIFICATE-----」までをハイフンを含め、すべてコピーして貼り付けて、【次へ】ボタンをクリックします。

D) インストールするサーバ証明書の内容を確認して、次へ進みます。

■ 新規の場合

・【Add Server Certificate】ボタンをクリックします。

■ 更新の場合

- 【Replace Certificate】ボタンをクリックします。

E) サーバの再起動後に設定が反映される旨が表示されますので、【OK】ボタンをクリックします。

F) 証明書のインストールが成功した旨が表示されますので、【OK】ボタンをクリックします。

■ 新規の場合

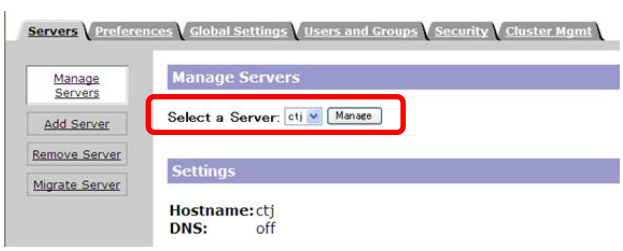
■ 更新の場合

以上でサーバ証明書のインストールが完了します。

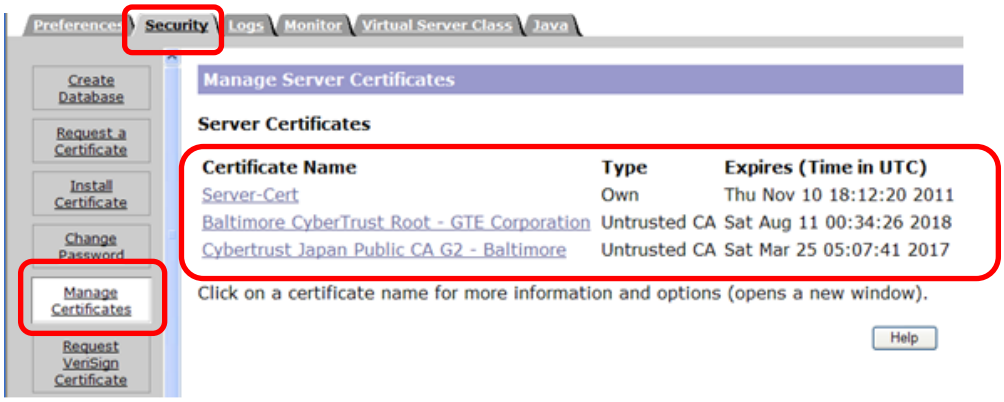
6.3. 証明書のインストール確認

証明書が正しくインストールされたか確認します。

A) 管理コンソールへログインし、【Manage Servers】の【Select a Server】項目で証明書をインストールするサーバ名を指定して、【Manage】ボタンをクリックします。



B) 【Security】タブをクリックし、【Manage Certificates】をクリックして、キーデータベースファイルに登録されている証明書の一覧の中に登録した証明書が含まれているか確認します。



※証明書の削除は、【Certificate Name】に表示されている各証明書名をクリックし、遷移後の画面の【Delete Certificate】ボタンから削除可能です。
※【Type】が「Untrusted CA」と表示されていても SSL 通信に問題はありません。

7. SSL 通信の有効化

SSL 通信を有効化します。

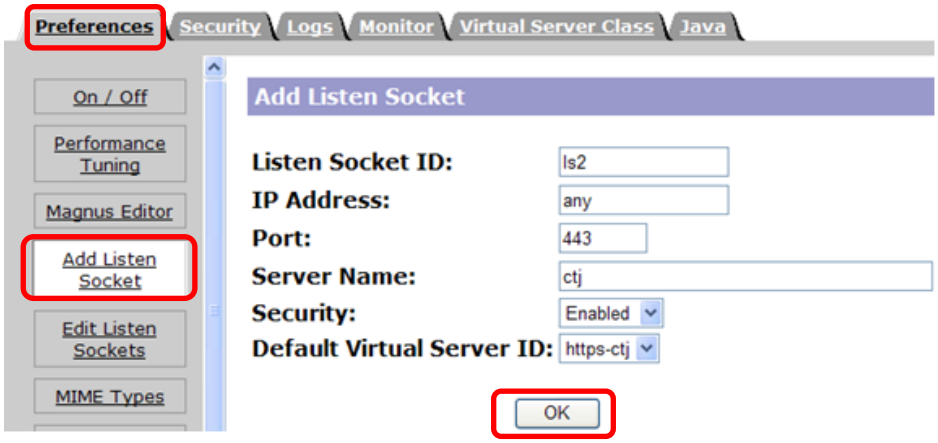
7.1. Listen Socket の追加

SSL 通信を行う Listen Socketを追加します。

※更新時において、必要な Listen Socket が既に追加されている場合は、本手順をスキップしてください。

A) 管理コンソールへログインし、【Manage Servers】の【Select a Server】項目で証明書をインストールするサーバ名を指定して、【Manage】ボタンをクリックします。

B) 【Preferences】タブの【Add Listen Socket】をクリックして、入力項目を設定し、【OK】ボタンをクリックします。



入力項目の詳細は以下です。

■ Listen Socket ID:

任意の Socket ID 名を入力します。

■ IP Address:

使用する IP アドレスを指定します。

■ Port:

SSL 通信を行うポート番号を指定します。

※通常は「443」ポートをご指定ください。

■ Server Name:

サーバ証明書をインストールしたサーバ名を指定します。

■ Security:

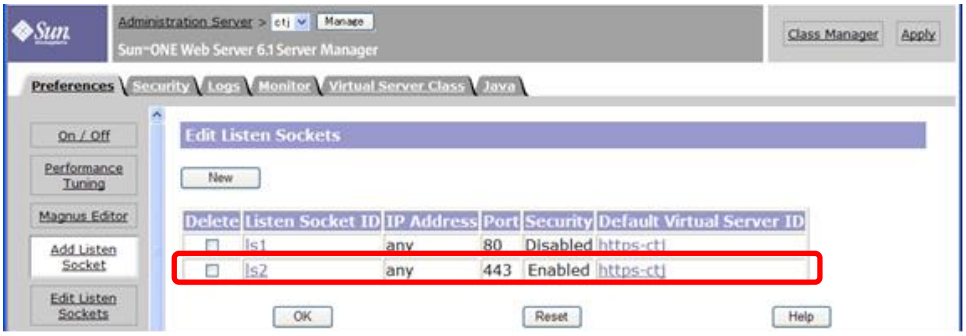
「Enabled」を選択します。

■ Default Virtual Server ID:

インスタンス名を指定します。

C) 【OK】ボタンをクリックします。

D) Listen Socket が追加されていることを確認します。

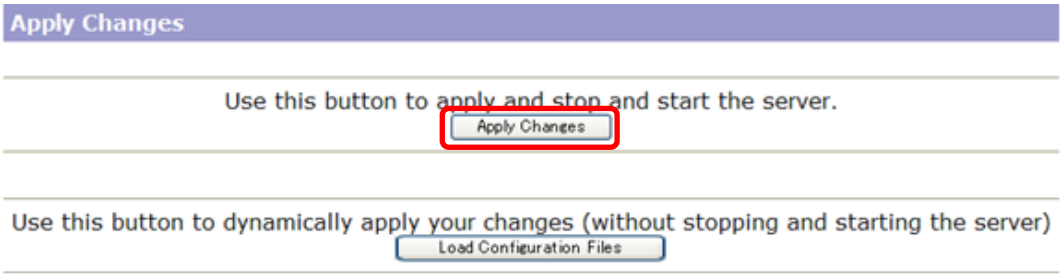


7.2. 設定の反映

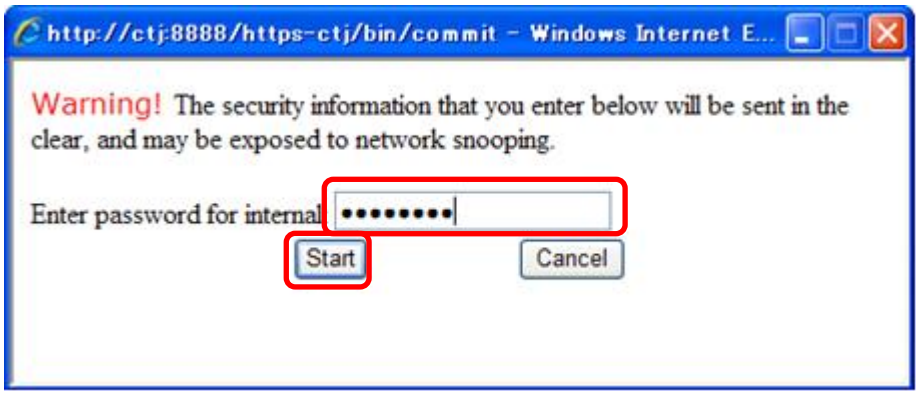
これまで行った設定を反映します。

A) 画面右上の【Apply】をクリックします。

B) 【Apply Changes】ボタンをクリックして、サーバの再起動を行います。



C) キーデータベースのパスワードを入力し、【Start】ボタンをクリックします。



D) 以下が表示されますので、【OK】ボタンをクリックします。

以上で SSL 通信が有効となります。

SSL 通信の確認

8. SSL 通信の確認

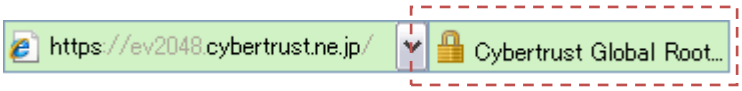
サーバ証明書が正しくインストールされ、エラーやセキュリティ警告が表示されず、正常に SSL 通信が可能であることを確認します。

SSL 通信の確認は設定を行っているサーバ以外の Web ブラウザや携帯電話、スマートフォンなどの携帯端末、「サーバ証明書の設定確認」から行うことを推奨します。

■ 設定確認例

- Internet Explorer 8

＜SureServer EV[2048bit]＞



＜SureServer[2048bit](クロスルート方式を含む)＞

- Firefox 12.0

＜SureServer EV[2048bit]＞

＜SureServer[2048bit](クロスルート方式を含む)＞

なお、接続時にセキュリティ警告やエラーが表示される場合は、以下よくある質問の「SSL 通信時のセキュリティ警告やエラーについて」をご参照ください。

≫ SSL 通信時のセキュリティ警告やエラーについて