# 2-2.　セキュア Web サーバー

# 1. 基本設定

ここではセキュア Web サーバーの基本的な設定を行います。

## ■ 基本設定

適切な「サーバー名」「ポート番号」「管理者メールアドレス」「ドキュメントルート」の各項目を正しく入力します。

### ● サーバー名

外部に公開するサーバー名を入力します。(この例では www.example.com と指定)

### ● ポート番号

通常は 443 です。

変更した場合は、このサーバーにアクセスするための URL が https://www.example.com:443/のように、「:」の後に指定したポート番号を入力する必要が出てきます。

### ● 管理者メールアドレス

管理者メールアドレスには、Web 管理者のメールアドレスを入力します。多くの場合、ここには個人のアドレスではなく「webmaster@example.com」などのような管理者用のアドレスを入力します。(これらのアドレスは最終的にはメ

ールサーバーの設定や、メーリングリストを使用して管理者に届くように設定します。）

- ドキュメントルート

  Web サーバーとして公開したいディレクトリを指定します。

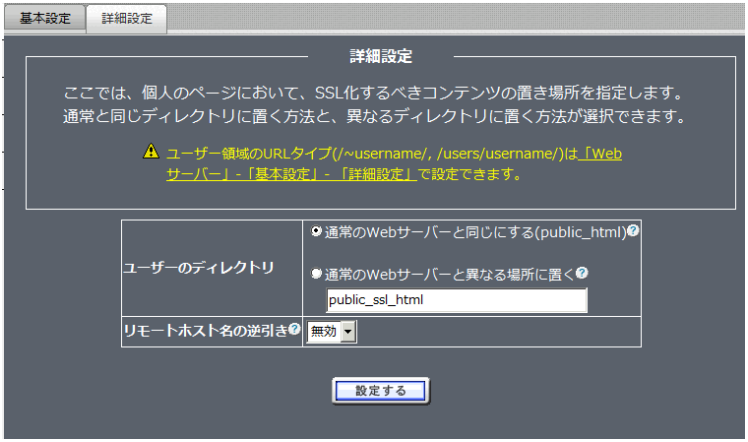
  ドキュメントルートを管理するユーザーのホームディレクトリにディレクトリを作成し、そのディレクトリをドキュメントルートとすれば、FTP でファイルをアップロードすることができます。

「ポート番号」、「ドキュメントルート」は通常は変更する必要はありませんが、Web サイトの管理者とサーバー管理者が異なる場合は、ドキュメントルートを Web サイト管理者のホームディレクトリに変更すると便利です。

「設定する」ボタンをクリックし、設定を完了します。

## ■ 詳細設定

セキュア Web サーバーを通して公開する、ユーザーのディレクトリを設定します。




通常の Web サーバーと同じ設定(public_html)にする場合は、「通常の Web サーバーと同じにする」を選択します。

通常の Web サーバーと異なるディレクトリを指定する場合は、「通常の Web サーバーと異なる場所に置く」を選択します。（フォルダは作成されないので、手動で作成してください。）

異なるディレクトリを選択した場合は、ディレクトリ名を入力します。

正しければ「設定する」ボタンをクリックして、設定を終了します。

## 2. ディレクトリ管理

セキュア Web サーバーのディレクトリについて個別に管理・設定します。

「

2-1. Web サーバー」の「2.ディレクトリ管理」をご参照ください。

## 3. ディレクトリ追加

セキュア Web サーバーのディレクトリを追加します。

「

2-1. Web サーバー」の「3.ディレクトリ追加」をご参照ください。

# 4. ディレクトリ認証設定

Web サーバーで公開するディレクトリの、認証設定を行います。

「

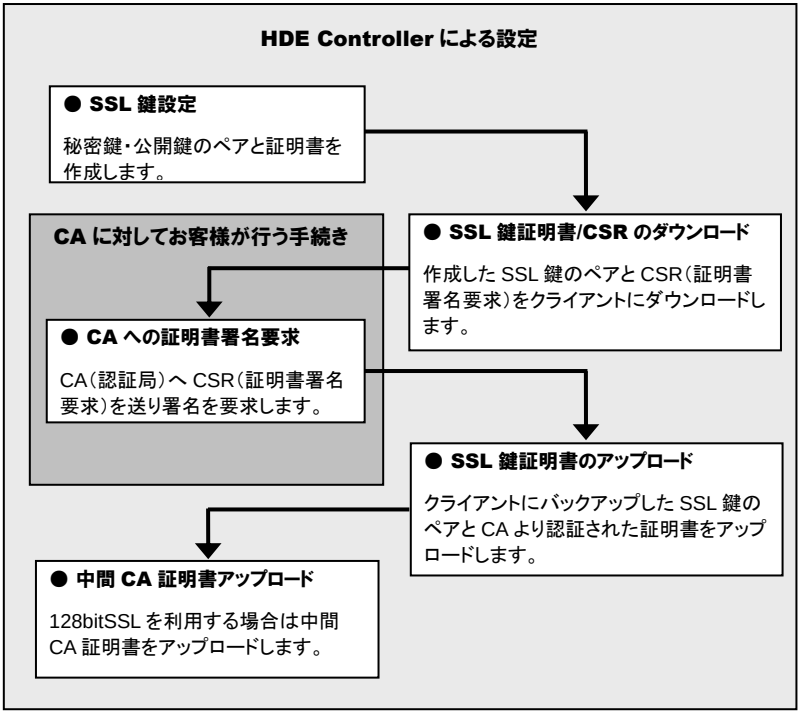
2-1. Web サーバー」の「4.ディレクトリ認証設定」をご参照ください。

# 5. 鍵と証明書の設定

ここではセキュア Web サーバーの暗号化(SSL)の為の秘密鍵・公開鍵の設定を行います。

## ■ 設定の流れ

鍵と証明書の設定の流れは以下のようになります。

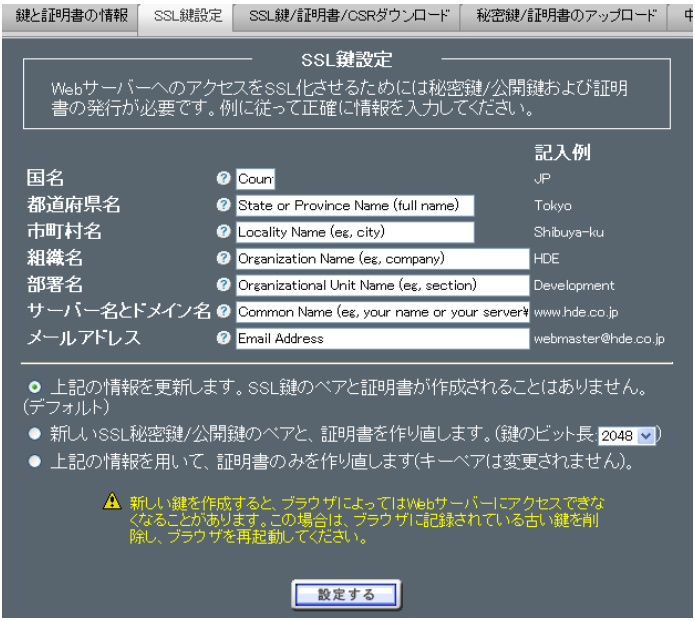


## ■ 鍵と証明書の情報

現在設定されている証明書の情報が表示されます。

## ■ SSL 鍵設定

セキュア Web サーバー用の SSL 鍵を設定します。




Web サーバーへのアクセスを暗号化させるためこの設定により秘密鍵/公開鍵および証明書の発行が必要です。

「国名/都道府県名/市町村名/組織名/サーバー名とドメイン名/E-mail アドレス」を正しく入力します。

> ⚠ 国名/都道府県名/市町村名/組織名/サーバー名とドメイン名/E-mail アドレスなどの情報が正しく入力されていないと、CA にて受け付けられないことがあるので注意してください。

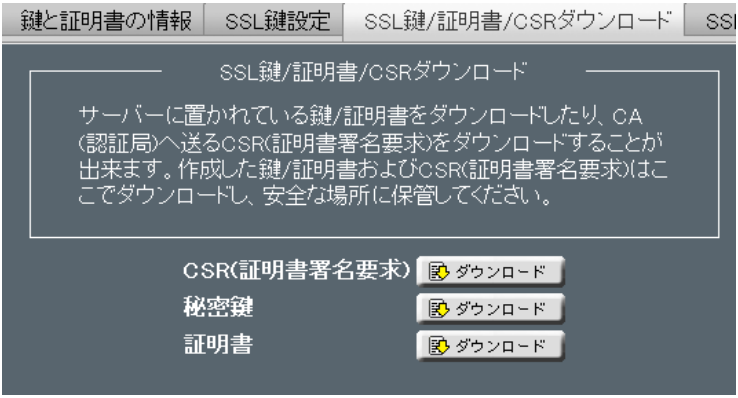
SSL 鍵の設定方法として、下表にあるように複数の方法があります。

| | |
|---|---|
| 上記の情報を更新します。SSL 鍵のペアと証明書が作成されることはありません。 | 既に設定されている証明書の情報のみを更新します。 |
| 新しい SSL 秘密鍵／公開鍵のペアと、証明書を作り直します。 | 新規に SSL 秘密鍵／公開鍵、証明書を作成します。初めて設定する場合や証明書を変更する場合は必ず行います。 |
| 上記の情報を用いて、証明書のみを作り直します。 | 既に設定されている鍵／証明書情報を元に、証明書のみを作り直します。 |

正しければ「設定する」ボタンをクリックして設定を終了します。

## ■ SSL 鍵/証明書/CSR ダウンロード

SSL 鍵・証明書・CSR(証明書署名要求)をクライアントにダウンロードすることができます。



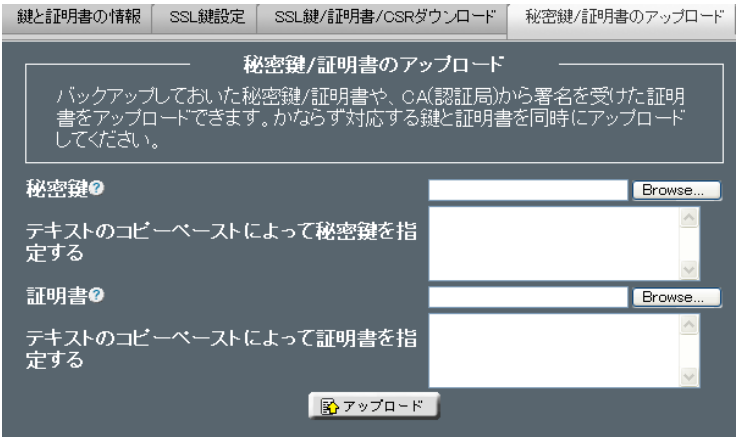

CSR は CA(認証局)へ送付するためにダウンロードを行います。

秘密鍵・公開鍵ペア、および、証明書はバックアップのためにダウンロードすることができます。

「ダウンロード」ボタンをクリックするとファイルをダウンロードすることができます。

## ■ SSL 鍵/証明書のアップロード

SSL 鍵・証明書をクライアントからアップロードすることができます。




アップロードする鍵、証明書は必ず対になっているものを同時にアップロードします。

ファイルの保存されているパスを、「秘密鍵」「証明書」それぞれに入力するか「参照」ボタンをクリックし直接ファイルが存在するディレクトリを指定します。

テキストを直接入力することも可能です。

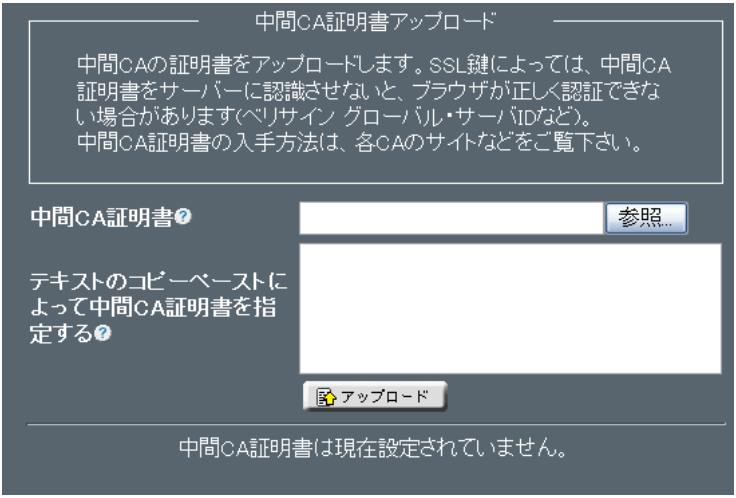
> アップロードする鍵、証明書は必ず対になっているものを同時にアップロードしてください。

> ファイルを指定する方法と、直接入力する方法を同時に行うことはできません。

> パスフレーズ付きの秘密鍵はご利用になれません。

## ■ 中間 CA 証明書アップロード

中間 CA 証明書をアップロードします。




中間 CA の証明書をアップロードします。SSL 鍵によっては、中間 CA 証明書をサーバーに認識させないと、ブラウザが正しく認証できない場合があります (128bit SSL を利用する場合に必要になります。ベリサイン　グローバル・サーバーID など)

中間 CA 証明書の入手方法は、各 CA のサイトなどをご覧下さい。