## Apache 2.x (Open SSL)

1. AffirmTrust ポータルからサーバ証明書と CA 証明書のバンドルをダウンロードします。Apache サーバには、CSR の生成時に作成されたキーファイルがあります。キーファイルが保存されているディレクトリに証明書を配置し、その証明書をルートからのみ読み取れるようにします。
2. Apache 設定ファイルを探します。通常、このファイルは /etc/httpd/httpd.conf ですが、ファイルの場所と名前はサーバによって異なる場合があります。正しいファイルには、Apache の設定を含む＜VirtualHost＞ブロックが存在します。
3. セキュリティで保護されている https 接続と保護されていない http 接続の両方を通じてアクセスできる Web サイトの場合、これらの接続ごとに仮想ホストが必要です。セキュリティで保護されていない既存の仮想ホストのコピーを作成し、次の手順に従ってセキュリティで保護します。https 接続を通じてのみアクセスできる Web サイトの場合は、既存の仮想ホストのコピーを作成せずに、次の手順に従って仮想ホストをセキュリティ保護してください。
4. 次の例のように ＜VirtualHost＞ブロックを編集します。太字の要素は SSL 設定に必要な部分を示しています。

```
＜VirtualHost 192.168.0.1:443
DocumentRoot /var/www/html2
ServerName www.yourdomain.com
SSLEngine on
SSLCertificateFile [サーバ証明書ファイルのパス]
SSLCertificateKeyFile [秘密鍵のパス]
SSLCertificateChainFile [CA 証明書のバンドルのパス]
＜/VirtualHost＞
```

※ 各項目の詳細は次のとおりです。

- SSLCertificateFile : サーバ証明書ファイル (例: your_domain_name.crt)
- SSLCertificateKeyFile : CSR の生成時に作成されたキーファイル
- SSLCertificateChainFile : CA 証明書のバンドル (SSLCertificateChainFile ディレクティブが機能しない場合は、代わりに SSLCACertificateFile ディレクティブを使用してください)

5. 次のコマンドを実行して、Apache 設定ファイルの構文エラーを確認します。

   apachectl configtest (※ 一部のサーバでは、apache2ctl configtest コマンドを使用します)

6. 次のコマンドを実行して、SSL サポートを含む Apache を再起動します。

   apachectl stop
   apachectl start

※SSL サポートを含む Apache が起動しない場合は、apachectl start コマンドの代わりに apachectl startssl コマンドを使用してください。apachectl startssl コマンドを使用したときにしか SSL サポートがロードされない場合は、通常の apachectl start コマンドに SSL サポートを含めるように Apache のスタートアップ設定を実行してください。通常は、SSL 設定を囲むタグとタグを削除します。それ以外の場合は、サーバが再起動されるたびに、apachectl startssl コマンドを使用して Apache を手動で再起動しなければならないことがあります。

## Apache cPanel

**注意 :** 本手順は cPanel 11 のものです。別のバージョンの cPanel を使用している場合もプロセスは同様ですが、特定の手順を Web ホストに依頼しなければならない可能性があります。

1. AffirmTrust からサーバ証明書と CA 証明書のバンドルをダウンロードします。
2. WebHost Manager を開きます。[SSL/TLS] メニューの **[Activate your SSL Certificate]** をクリックします。
3. 表示される画面には 3 つのボックスが含まれています。最初のボックスには、サーバ証明書ファイルの内容を貼り付けます。証明書ファイルがサーバ上にある場合は、**[Fetch]** ボタンをクリックしてファイルの内容をコピーできます。2 番目のボックスには、CSR の生成時に作成された秘密鍵を貼り付けます。3 番目のボックスには CA 証明書のバンドルを貼り付けます。
4. 画面の上部にある **[Do it]** をクリックします。

## Apache Ensim Web Server

**サーバ証明書をインストールする**

1. SSL 証明書を格納するディレクトリ （例: /etc/ssl/crt/）にサーバ証明書を保存します。このディレクトリをルートからのみ読み取れるようにします。また、公開鍵ファイルと秘密鍵ファイルもこのディレクトリに保存します。
2. 管理者コンソールにログインし、保護する Web サイトを選択します。
3. **[Services]** をクリックします。
4. Apache Web Server の横にある **[Actions]** アイコンをクリックします。

5. [Apache Web Server Manager] 画面で、[SSL Settings] をクリックします。自己署名証明書がすでに保存されています。
6. [Import] をクリックします。開始タグと終了タグを含めて証明書をコピーし、[Save SSL Certificate] の下にあるボックスに貼り付けます。
7. 証明書を保存してからログアウトします。

### CA 証明書のバンドルをインストールする

証明書を信頼する前に、中間証明書とルート証明書を含む CA のバンドルをサーバにインストールする必要があります。

1. Ensim サーバで、/etc/httpd/conf/virtual ディレクトリに移動します。このディレクトリには、Ensim サーバでホストする各仮想サイトのファイルが保存されています。

   例:
   site1
   site2
   site3

2. 編集する必要のある仮想サイトのファイルを探します。HTML エディタまたはテキストエディタを使用してサイトのファイルを開き、その内容を表示することができます。各ファイルの先頭には、次のような情報が保存されています。

   ＜VirtualHost 000.00.00.000:80＞
   ServerName www.yourdomain.com

3. エディタでサイトのファイルを開き、次に示す太字の行を追加します。

   ＜/Directory＞
   SetEnv SITE_ROOT /home/virtual/site#/fst SetEnv SITE_HTMLROOT /home/virtual/site#/fst/var/www/html Include /etc/httpd/conf/site# SSLEngine on
   SSLCertificateFile /home/virtual/site#/fst/etc/httpd/conf/ssl.crt/server.crt
   SSLCertificateKeyFile /home/virtual/site#/fst/etc/httpd/conf/ssl.key/server.key
   **SSLCACertificateFile /home/virtual/site#/fst/etc/httpd/conf/ssl.crt/cabundle.crt**
   ＜/VirtualHost＞
   ＜/IfDefine＞

   ※ site# は仮想サイトの番号（例: site1）を、server はサーバ証明書の名前を示しています。

4. サーバ証明書の保存ディレクトリに、CA 証明書のバンドルファイルをコピーします。

   /home/virtual/site#/fst/etc/httpd/conf/ssl.crt/cabundle.crt

5. 現在のサイトのファイルのバックアップコピーを作成します。
6. 編集したサイトのファイルを保存します。
7. Apache を再起動します。

**注意 ：** 上記の手順は、Ensim を使用して管理するサイトに証明書をインストールするためのものです。Ensim 自体に SSL 証明書をインストールする場合、ホストの設定は同じですが、Ensim インタフェースのホストの設定ファイルは /usr/lib/opcenter/fastcgi/httpd-templ.conf になります。

## Apache Tomcat

1. ダウンロード画面から、KeyStore があるディレクトリに<サーバ名>.p7b ファイルをダウンロードします。

   **注意 ：** 証明書は、CSR の生成に使用したのと同じ KeyStore にインストールする必要があります。別の KeyStore にインストールしようとしても、機能しません。

2. 次のコマンドを入力して証明書をインストールします。

   keytool -import -trustcacerts -alias tomcat -file <server.name>.p7b -keystore <yourkeystorename>.jks

3. 証明書を信頼するかどうかを尋ねるプロンプトが表示されたら、「yes」と入力します。証明書が正しくインストールされると、「Certificate reply was installed in keystore」というメッセージが表示されます。