

Apache 2.x (Open SSL)

1. ターミナルクライアント (ssh) を使用してサーバにログインします。プロンプトで、次のように入力します。

```
openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr
```

2. 2つのファイルが生成されます。CSR と秘密鍵ファイルです。秘密鍵は、証明書のインストール時に必要になります。
3. コモンネームの入力を求められたら、保護するサイトの完全修飾ドメイン名を入力します。ワイルドカード証明書の CSR を生成する場合、コモンネームは * で始まります (例: *.yourcompany.com)。
4. 表示される指示に従って、組織情報を入力します。CSR が作成されます。
5. CSR をテキストエディタで開きます。開始タグと終了タグを含めてテキストをコピーします。
6. AffirmTrust ポータルにログオンし、証明書の発行を行います。

Apache cPanel

注意: ここに示す手順は 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. cPanel のコントロールパネルにログインします。
2. **[SSL/TLS Manager]** をクリックします。
3. **[Generate, view, upload, or delete your private keys]** をクリックします。
4. **[Generate a New Key]** までスクロールします。保護するドメインを **[Host]** に入力するか、リストから選択します。これは、証明書にアクセスする際に使用する名前 (通常は、www.domain.com や mail.domain.com などの完全修飾ドメイン名) にする必要があります。 **[Generate]** をクリックします。
5. **[Return to SSL Manager]** をクリックします。
6. **[Generate, view, or delete SSL certificate signing requests]** をクリックします。
7. **[Generate a New Certificate Signing Request]** で、次の情報を入力します。
 - **Host:** 個人キーの生成時に入力または選択したドメイン。
 - **Country:** 2文字の ISO 3166 国コード。たとえば、日本のコードは「JP」です。その他の国については、[ISO の国コードのリスト](#)を参照してください。
 - **State:** 組織がある都道府県。略称は使用しないでください。
 - **City:** 組織がある市区町村。
 - **Company:** 組織/会社の正式名称。
 - **Email:** CSR の送信先となるメールアドレス。
 - **Pass Phrase:** 証明書に関連付けられたパスワード。このパスワードは後で使用するため、忘れないようにしてください。

8. **[Generate]** ボタンをクリックします。画面に CSR が表示されます。
9. 開始タグと終了タグを含めて CSR のテキストをコピーします。
10. AffirmTrust ポータルにログオンし、証明書の発行を行います。

Apache Ensim Web Server

1. Site Administrator にログインし、管理対象のサイトを選択します。
2. **[Services]** をクリックします。
3. Apache Web Server の横 ([ServiceList] の上部または近く) にある **[Actions]** アイコンをクリックします。
4. [Apache Web Server Manager] 画面で、**[SSL Settings]** をクリックします。
5. **[Generate]** をクリックします。組織およびサーバに関する情報を入力します。コモンネームは自動的に設定されます。**[Save]** をクリックします。CSR と RSA 鍵が生成されます。証明書をインストールするには、この 2 つが必要です。
6. CSR をテキストエディタで開きます。開始タグと終了タグを含めてテキストをコピーします。
7. AffirmTrust ポータルにログオンし、証明書の発行を行います。

Apache Tomcat

1. KeyStore と証明書を管理するディレクトリに移動します。次のコマンドを入力します。

```
keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore サイト名.jks
```

注意: keytool コマンドが認識されるようにするには、パスに java/bin/ ディレクトリを追加する必要がある場合があります。

2. 表示される指示に従って、KeyStore のパスワードと組織情報を指定します。**注意:** 氏名の入力を求められたら、保護するサイトの完全修飾ドメイン名 (例: www.yourcompany.com) を入力してください。ワイルドカード証明書を要求する場合、FQDN は文字*で始まります (例: *.yourcompany.com)。
3. 表示される指示に従って、情報が正しいことを確認し、「yes」と入力します。続いて、パスワードを確認します。
4. これで、現在の作業ディレクトリに KeyStore ファイル (サイト名.jks) が作成されます。KeyStore ファイルを保存します。このファイルには、後から証明書がインストールされます。
5. KeyStore から CSR を生成するには、次のコマンドを入力します。

```
keytool -certreq -alias server -file csr.txt -keystore サイト名.jks
```

6. 前の手順で選択した KeyStore のパスワードを入力し、キーを押します。

7. 現在のディレクトリに CSR (csr.txt) が作成されます。
8. 開始タグと終了タグを含めて CSR のテキストをコピーします。
9. AffirmTrust ポータルにログオンし、証明書の発行を行います。