内容

C2Net Stronghold

1. Stronghold Configuration Manager を開きます。
2. **[New Key Generation]** をクリックします。
3. 鍵のサイズ (2048 ビット) を入力し、ランダムデータを生成するための手順に従います。

   注意: < > ~ ! @ # $ % ^ * / ( ) ?. &　は使用しないでください。

   新しい鍵のペアは、strongholdserverroot/private/**your_domain_name**.key　に保存されます。ここで、**your_domain_name**　は、保護するドメイン名および拡張子です (例: yourcompany.com)。

4. ファイル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。
5. AffirmTrust ポータルにログオンし、証明書の発行を行います。

Cisco Adaptive Security Appliance (ASA) 5500

1. Cisco Adaptive Security Device Manager (ASDM) を開き、**[Configuration]** → **[Device Management]** の順にクリックします。
2. **[Certificate Management]** を展開し、**[Identity Certificates]** → **[Add]** の順にクリックします。
3. **[Add a new identity certificate]** を選択し、**[Key Pair]** リストの横にある **[New]** をクリックします。
4. **[Enter new key pair name]** を選択し、鍵のペアの名前を入力します。**[Size]** を 2048 に設定し、**[Usage]** を [General purpose] に設定します。
5. **[Generate Now]** をクリックします。
6. **[Certificate Subject DN]** の右側にある **[Select]** ボタンをクリックします。[Certificate Subject DN] 画面で、DN に関する属性を設定します。そのためには、**[Attribute]** リストから属性の種類を選択し、適切な **[Value]** を入力して **[Add]**をクリックします。
7. [Add Identity Certificate] 画面の **[Advanced]** をクリックします。
8. **[FQDN]** に、デバイスに外部からアクセスする際に使用する完全修飾ドメイン名を入力します (例: vpn.domain.com)。この値は、手順 6 で指定したコモンネームと一致している必要があります。
9. **[OK]** をクリックし、**[Add Certificate]** をクリックします。表示される指示に従って、CSR の情報を .txt ファイルとして保存します。
10. ファイル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。
11. AffirmTrust ポータルにログオンし、証明書の発行を行います。

Cobalt RaQ4/XTR

仮想サイトで SSL を有効にする
CSR を作成する前に、仮想サイトで SSL を有効にする必要があります。

1. **[Server Management]** 画面に移動します。
2. SSL を有効にする仮想サイトの横にある緑色のレンチ (RaQ4) または鉛筆 (XTR) のボタンをクリックします。これで、Site Management UI が表示されます。
3. 左側にある **[Site Settings]** (XTR を使用する場合は **[General]**) をクリックします。
4. **[Enable SSL]** オプションを選択します。
5. **[Save Changes]** をクリックします。

自己署名 SSL 証明書を作成し、CSR を送信する
SSL を有効にしたら、自己署名 SSL 証明書を生成します。この証明書は後から AffirmTrust で署名されます。

1. **[Server Management]** 画面に移動します。
2. SSL を有効にする仮想サイトの横にある緑色のレンチ (RaQ4) または鉛筆 (XTR) のボタンをクリックします。これで、Site Management UI が表示されます。
3. 左側にある **[Site Settings]** (XTR を使用する場合は **[General]**) をクリックします。
4. **[Certificate Subject Information]** テーブルに、次の情報を入力します。
    - **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:** 本社がある都道府県の正式名称。「Tokyo (東京都)」などです。
    - **Locality:** 本社がある地域または市区町村の正式名称。「Shibuya (渋谷区)」などです。
    - **組織:** 会社の正式名称。
5. 画面の一番下にあるリストで、**[Generate self-signed certificate]** を選択します。
6. **[Save Changes]** をクリックします。画面が更新され、**[Certificate Request]** ボックスと **[Certificate]** ボックスに自己署名証明書が表示されます。
7. 開始タグと終了タグを含めて **[Certificate Request]** ボックスの内容をコピーします。
8. AffirmTrust ポータルにログオンし、証明書の発行を行います。

F5 BIG IP (バージョン 9)

1. F5 BIG-IP の Web UI を起動します。
2. **[Local Traffic]→[SSL Certificates]→[Create]** の順にクリックします。
3. **[General Properties]** で、証明書の名前を指定します。
4. **[Certificate Properties]**で、次の情報を指定します。
    - **Issuer:** 証明機関 (AffirmTrust SSL)
    - **Common name:** サーバの完全修飾ドメイン名 (例: www.domain.com、mail.domain.com、*.domain.com)
    - **Division:** 組織内の部門
    - **Organization:** 組織の正式名称
    - **Locality, State or Province, Country:** 組織がある国、都道府県、市区町村
    - **E-mail Address:** メールアドレス
    - **Challenge Password, Confirm Password:** パスワード
5. **[Key Properties]** を 2048 に設定します。
6. **[Finished]** をクリックします。これで、CSR ファイルのテキストが提供されます。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。

F5 BIG IP (バージョン 9 より前のバージョン)

1. ルートユーザとして BIG-IP デバイスにログインし、次のコマンドを実行します。

   # /usr/local/bin/genconf

   会社の詳細情報 (正式名称と住所を含む) の入力を求められます。

2. 次のコマンドを使用して CSR を作成します。

   # /usr/local/bin/genkey www.yoursite.com

3. 表示される指示に従って、会社の詳細情報を入力します。
4. /config/bigconfig/ssl.csr/ で、CSR (www.yoursite.com.csr) を探します。このファイルをワークステーションに転送し、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。
5. AffirmTrust ポータルにログオンし、証明書の発行を行います。

F5 FirePass VPS

1. FirePass の Web 管理 UI にログインします。
2. 管理コンソールで、**[Server]** → **[Security]** → **[Certificates]** の順にクリックします。
3. **[Generate a New Certificate Request]** をクリックします。
4. CSR 生成に関する領域に会社の情報を入力し、**[Generate Request]** をクリックします。
5. ダウンロードする CSR は、CSR ファイルと秘密鍵を含む ZIP ファイルです。秘密鍵は後で証明書をインストールするときに必要になるので、安全な場所に保存してください。
6. CSR ファイル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。

HSphere Web Server

1. コントロールパネルのホームページで、**[SSL]** をクリックし、保護するドメインに対して SSL を有効にします。
2. 次の [SSL Certificate Signing Request Parameters] 画面に移動します。空欄に情報を入力し、**[Submit]** をクリックします。
3. 3 つのファイル (CSR、秘密鍵、一時 SSL 証明書) が生成されます。秘密鍵と CSR を保存します。これらは、テキストファイルとして安全な場所に保存してください。秘密鍵と CSR は SSL 証明書をインストールする場合に必要になります。
4. CSR ファイル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。
5. AffirmTrust ポータルにログオンし、証明書の発行を行います。

IBM HTTP Server

1. IKEYMAN を開き、鍵のペアと証明書要求を鍵データベースに作成します。鍵と要求のセットごとに新しいデータベースを作成することも、すべての鍵と要求を 1 つのデータベースに保存することもできます。
2. 新しいデータベースを作成するには、IKEYMAN を起動して **[鍵データベース・ファイル]** を選択し、**[新規]** をクリックして新しいデータベースの名前を入力します。**[OK]** をクリックします。パスワードを入力し、確認のためにもう一度入力します。**[OK]** をクリックします。
3. 新しい鍵のペアと CSR を作成するには、IKEYMAN でデータベースの名前を指定して開きます。
4. **[作成]** をクリックし、**[新規証明書要求]** をクリックします。フォームに情報を入力します。鍵サイズには、選択可能な最大サイズを使用します。推奨値は 2048 ビットです。**[OK]** をクリックします。
5. CSR ファイル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。

Java ベースの Web サーバ (汎用)

1. 古い KeyStore をバックアップして、Java ベースの Web サーバから削除します。古い KeyStore では新しい SSL 証明書が適切に機能しないため、CSR を作成するには、新しい KeyStore を生成する必要があります。
2. 新しい KeyStore を作成します。
    1. コマンドプロンプトで、次のように入力します。

        keytool -genkey -alias server -keyalg RSA -keysize 2048 ?keystore your_domain_name.jks

    2. 表示される指示に従って、DN 情報を入力します。氏名をドメイン名および拡張子に設定します (例: www.yourcompany.com)。ワイルドカード証明書を要求する場合は、先頭にアスタリスク (*) を付けます (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。
    4. 表示される指示に従って、パスワードを入力します。

3. 新しい KeyStore を使用して CSR を生成します。
    1. コマンドプロンプトで、次のように入力します。

        keytool -certreq -alias server -keyalg RSA -file your_domain.csr -keystore your_domain_name.jks

    2. 表示される指示に従って、KeyStore の作成時に指定した KeyStore のパスワードを入力します。CSR ファイルが作成されます。

4. 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。
5. AffirmTrust ポータルにログオンし、証明書の発行を行います。

Lotus Domino 8.5

1. サーバー証明書管理画面で、**[Create Key Ring]** をクリックします。
2. フォームに必要事項を入力します。**[Key Size]** を 2048 に設定します。
3. 次の画面に進みます。キーリングが作成されたことを確認できます。
4. **[OK]** をクリックしてメイン画面に戻ります。**[Create Certificate Request]** をクリックします。
5. **[Paste into form on CA’s site]** を選択し、**[Create Certificate Request]** をクリックします。
6. CSR フィールドのプロパティと CSR のテキストを示す確認画面が表示されます。開始タグと終了タグを含めて証明書要求をコピーし、**[OK]** をクリックします。
7. AffirmTrust ポータルにログオンし、証明書の発行を行います。

Mirapoint

1. **[Admin]** 画面の **[Security and Certificates]** をクリックします。
2. **[(CSR)]** を選択します。
3. SSL 証明書に表示される詳細 (保護するコモンネーム (例: www.yourdomain.com) を含む) を入力します。
4. [Download] をクリックし、ファイルをテキストファイルとして保存します。
5. CSR をテキストエディタで開き、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。

Nginx

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 と秘密鍵です。秘密鍵は、SSL 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 (ドメイン名) 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を入力します。ワイルドカード証明書を生成する場合、コモンネームはアスタリスクで始まります (例: *.yourcompany.com)。組織情報の入力を求められます。入力すると、CSR ファイルが作成されます。
4. CSR をテキストエディタで開き、開始タグと終了タグを含めてテキストをコピーします。
5. AffirmTrust ポータルにログオンし、証明書の発行を行います。

Oracle Wallet Manager

1. Oracle Wallet Manager で、メニューの **[操作]** をクリックします。**[証明書要求の作成]** を選択して **[証明書要求の作成]** 画面を開きます。
2. 各フィールドに情報を入力します。
3. **[OK]** をクリックします。証明書要求が正常に作成されたことを示す画面が表示されます。もう一度 **[OK]** をクリックしてメイン画面に戻ります。
4. Oracle Wallet Manager で、メニューの **[操作]** をクリックします。**[証明書要求のエクスポート]** を選択します。
5. CSR を保存するディレクトリを入力します。**[ファイル名]** ボックスにファイル名を入力します。
6. **[OK]** をクリックします。
7. CSR をテキストエディタで開き、開始タグと終了タグを含めてテキストをコピーします。
8. AffirmTrust ポータルにログオンし、証明書の発行を行います。

Oracle WebLogic Server 8 または 9

キーストアを作成する
インストール時のエラーを回避するには、新しいキーストアを生成してから CSR を作成します。証明書を再発行または更新する場合でも、新しいキーストアを生成する必要があります。

1. コマンドプロンプトで、次のコマンドを入力します。

   keytool -genkey -alias server -keyalg RSA -keystore your_domain_name.jks

2. 表示される指示に従って、証明書の情報を入力します。
3. 表示される指示に従って、「yes」と入力して確定します。次に、パスワードの入力を求められます。このパスワードは、後で CSR を生成する場合や証明書をインポートする場合に使用する必要があります。

CSR を作成する

1. コマンドプロンプトで、次のコマンドを入力します。

   keytool -certreq -alias server -keyalg RSA -file your_domain.csr -keystore your_domain_name.jks
2. キーストアのパスワードを入力します。
3. your_domain_name.csr ファイルをテキストエディタで開き、開始タグと終了タグを含めてテキストをコピーします。
4. AffirmTrust ポータルにログオンし、証明書の発行を行います。

Plesk

Plesk 10

1. Plesk のコントロールパネルにログインします。
2. **[ツールとユーティリティ]** をクリックします。このオプションは、**[サーバ]** タブまたは左側の列に表示される場合があります。
3. **[SSL 証明書]** をクリックします。
4. **[SSL 証明書の追加]** をクリックします。
5. [SSL 証明書の追加] 画面で設定を入力し、**[リクエスト]** をクリックします。

   注意 : * が付いたすべてのフィールドに情報を入力する必要があります。**[ビット数]** を 2048 に設定します。
6. CSR は証明書リストから取得できます。Plesk の登録時に指定したメールアドレスにも、CSR がメールで送信されます。
7. CSR ファイルをテキストエディタで開き、開始タグと終了タグを含めてテキストをコピーします。
8. AffirmTrust ポータルにログオンし、証明書の発行を行います。

Plesk 9

1. Plesk 9 のコントロールパネルにログインします。
2. 左側のメニューの **[設定]** をクリックします。
3. **[セキュリティ]** の **[SSL 証明書]** をクリックします。
4. [SSL 証明書] メニューの **[SSL 証明書]** をクリックします。
5. 証明書の情報 (CSR) のセクションに適切な情報を入力し、**[リクエスト]** をクリックします。
6. **[SSL 証明書]** に戻り、新しい証明書要求の名前を選択します。
7. CSR はこの画面から取得できます。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。
8. AffirmTrust ポータルにログオンし、証明書の発行を行います。

Plesk 8

1. Plesk のコントロールパネルにログインします。
2. **[ドメイン]** ボタンをクリックします。ドメインリストの画面が表示されます。
3. SSL で保護するドメイン名をクリックします。
4. **[証明書]** ボタンをクリックします。
5. **[証明書を追加]** ボタンをクリックします。SSL 証明書の設定画面が表示されます。
6. **証明書の情報**のセクションに適切な情報を入力します。

   注意: * が付いたすべてのフィールドに情報を入力する必要があります。[ビット数] を 2048 に設定します。

7. 詳細の右側に表示される **[リクエスト]** ボタンをクリックします。
8. Plesk の登録時に指定したメールアドレスに、CSR がメールで送信されます。このメールには秘密鍵と CSR の 2 つのセクションがあります。秘密鍵は後で証明書をインストールするときに必要になるので、なくさないようにしてください。
9. CSR をテキストエディタで開き、開始タグと終了タグを含めて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。

SAP Web Application Server 6.10 以降

サーバ固有の PSE を使用するアプリケーションサーバごとに個別の証明書要求を生成する必要があります。システム全体の SSL サーバ PSE を使用する場合は、証明書要求を 1 つ生成するだけでかまいません。

固有の SSL サーバ PSE を確認するには、トラストマネージャで SSL サーバ PSE ノードを展開し、各アプリケーションサーバをダブルクリックしてサーバの詳細を表示します。サーバの識別名が **[Own certificate]** に表示されます。固有の識別名を持つアプリケーションサーバごとに証明書要求を生成する必要があります。

1. トラストマネージャ画面で、SSL サーバ PSE ノードを展開します。
2. サーバ固有の PSE ごとに、またはシステム全体で単一の PSE について、次の手順を実行します。
    1. アプリケーションサーバを選択します。アプリケーションサーバの証明書が、**[Own certificate]** の **[PSE maintenance]** に表示されます。
    2. **[PSE maintenance]** で、**[Create Certificate Request]** をクリックします。証明書要求が画面に表示されます。
    3. 開始タグと終了タグを含めて証明書要求をコピーします。
    4. AffirmTrust ポータルにログオンし、証明書の発行を行います。

Zeus Web Server

1. Web サーバにログインします。
2. **[SSL Certificates]** を選択します。
3. **[Create]** ボタンをクリックして新しい証明書セットを作成します。
4. **[Buy a certificate from another certifying authority]** を選択し、**[OK]** をクリックします。
5. 適切なフィールドに DN 情報を入力し、**[OK]** をクリックします。
6. 開始タグと終了タグを含めて CSR 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。