内容

C2Net Stronghold 2
Cisco Adaptive Security Appliance (ASA) 5500 3
Cobalt RaQ4/XTR 4
F5 BIG-IP (バージョン 9) 5
F5 BIG-IP (バージョン 9 より前のバージョン) 6
F5 FirePass VPS 7
HSphere Web Server 8
IBM HTTP Server 9
Java ベースの Web サーバ (汎用) 10
Lotus Domino 8.5 11
Mirapoint 12
Nginx 13
Oracle Wallet Manager 14
Oracle WebLogic Server 8 または 9 15
Plesk 16
SAP Web Application Server 6.10 以降 18
Zeus Web Server 20

C2Net Stronghold

サーバ証明書をインストールする

1. /ServerRoot/ssl/certs/ ディレクトリに一時 SSL 証明書がある場合は、その証明書を移動するか、削除します。
2. 次のコマンドを実行します。

   getca your_domain_name
3. サーバ証明書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。
4. getca ターミナル画面に証明書の内容を貼り付けて、Ctrl-D または適切な EOF 文字を入力します。

CA 証明書のバンドルの証明書をインストールする

1. サーバの /ssl/certs/ ディレクトリに CA 証明書のバンドルをコピーします。
2. テキストエディタで、httpd.conf ファイル (通常は /conf/ ディレクトリにあります) を開きます。次に示すように、SSLCACertificateFile エントリが CA 証明書のバンドルファイルを参照するように編集します。

   SSLCACertificateFile ssl/certs/cabundle.crt
3. サーバを再起動します。

Cisco Adaptive Security Appliance (ASA) 5500

Adaptive Security Device Manager（ASDM）に証明書をインストールする

1. 証明書ファイルを保存するディレクトリに、CA 証明書のバンドルファイルとサーバ証明書ファイルをダウンロードします。
2. ASDM で、**[Configuration]** → **[Device Management]** の順にクリックします。
3. **[Certificate Management]** を展開し、**[CA Certificate]** を選択します。**[Add]** をクリックします。
4. **[Install from a file]** オプションを選択し、CA 証明書のバンドルファイルを参照して、[Install Certificate] 画面の一番下にある **[Install Certificate]** ボタンをクリックします。これで、中間証明書がインストールされます。
5. ASDM で、**[Configuration]** → **[Device Management]** の順にクリックします。
6. **[Certificate Management]** を展開し、**[Identity Certificates]** を選択します。
7. CSR の生成時に作成された適切な ID 証明書を選択し、**[Install]** ボタンをクリックします。
8. 適切な ID を参照し、**[Install Certificate]** をクリックします。証明書のインストールが成功したことを示す確認メッセージが表示されます。

ASDM を使用して新しい証明書を使用するように WebVPN を設定する

1. ASDM で、[Configuration] → [Device Management] の順にクリックします。
2. [Advanced] → [SSL Settings] の順にクリックします。
3. [Certificates] で、WebVPN セッションを終了するために使用するインタフェースを選択し、[Edit] をクリックします。
4. [Certificate] リストで、新しくインストールされた証明書を選択し、[OK] をクリックします。次に、[Apply] をクリックします。

Cobalt RaQ4/XTR

サーバ証明書をインストールする

1. [Server Management] 画面に移動します。
2. 保護する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。
3. **[SSL settings]** をクリックします。
4. 開始タグと終了タグを含めてサーバ証明書 (your_domain_name.crt) をフォームにコピーします。
5. 画面の一番下にあるリストで、**[Use manually entered certificate]** を選択し、**[Save Changes]** をクリックします。

CA 証明書のバンドルをインストールする

1. CA 証明書のバンドルファイルをサーバにコピーします。
2. httpd.conf ファイルを開き、SSL セクションに次の行を追加します。

   SSLCACertificateFile /your_directory_path/cabundle.crt
3. ファイルを保存して Apache を再起動します。

F5 BIG-IP (バージョン 9)

サーバ証明書をインストールする

1. BIG-IP の WebUI を起動します。
2. **[Local Traffic]** → **[SSL Certificates]** の順にクリックします。
3. CSR の作成時に証明書に割り当てた名前をクリックします。
4. ダウンロードした your_domain_name.crt ファイルを参照します。
5. **[Open]** → **[Import]** の順にクリックします。

中間証明書を有効にする

1. AffirmTrust ポータルから cabundle.crt ファイルをダウンロードします。
2. WebUI で、**[Local Traffic]** → **[SSL Certificates]** → **[Import]** の順にクリックします。
3. **[Import Type]** → **[Certificate]** → **[Create New]** の順にクリックします。
4. 証明書名を指定します。
5. cabundle.crt ファイルを参照し、**[Open]** → **[Import]** の順にクリックします。

SSL 用にサーバを設定する

1. この証明書で使用する SSL プロファイルを作成するか、開きます。
2. **[SSL]** メニューで、Configuration Utility にログインし、 **[Local Traffic]** → **[Profiles]** → **[Client]** の順にクリックします。設定するクライアントを選択し、**[Configuration]** メニューの **[Advanced]** をクリックします。
3. この手順の最初にインストールした SSL 証明書 (公開鍵と秘密鍵のペア) を選択します。
4. **[Chain]** で、前の手順でインポートした証明書ファイルを参照し、設定を保存して終了します。

F5 BIG-IP (バージョン 9 より前のバージョン)

1. FTP を使用して、BIG-IP デバイスにサーバ証明書と中間証明書をコピーします。
2. サーバ証明書の名前を your_domain_name.crt から your.domain.name.crt に変更し、/config/bigconfig/ssl.crt/ フォルダにコピーします。
3. 中間証明書を /config/bigconfig/ssl.crt/ フォルダにコピーします。
4. 次のコマンドを実行して、プロキシを再起動します。

   # bigpipe proxy ＜IP アドレス＞:443 disable
   # bigpipe proxy ＜IP アドレス＞:443 enable

F5 FirePass VPS

1. 管理コンソールで、**[Server]** → **[Security]** → **[Certificates]** の順にクリックします。
2. **[Install]** をクリックします。
3. 画面の下部にある **[Add New Certificate]** をクリックします。
4. 証明書ファイルとキーファイルをコピーして、対応するフィールドに貼り付けます。
5. **[Go!]** をクリックして証明書ファイルとキーファイルをインストールします。

HSphere Web Server

サーバ証明書をインストールする

1. 証明書ファイルとキーファイルを保存したディレクトリに、CA 証明書のバンドルファイルとサーバ証明書ファイルをダウンロードします。
2. コントロールパネルホームページで、**[SSL]** をクリックします。
3. **[Web Service]** 領域で、**[SSL]** の下にある **[Edit]** ボタンをクリックします。アップロードフォームが開きます。
4. **[Install Certificate based on previously]** ボックスに、開始タグと終了タグを含めてサーバ証明書ファイルの内容を貼り付けます。証明書はテキストエディタで開くことができます。**[Upload]** をクリックします。

CA 証明書のバンドルをインストールする

1. サーバ証明書のインストール手順と同様に、CA 証明書のバンドルファイルの内容を **[Certificate Chain File]** ボックスに貼り付けます。一部のバージョンの HSphere では、このボックスの名前が **[Certificate Authority File]** になっています。
2. **[Install]** をクリックします。これで、証明書が適切にインストールされます。
3. すべてのキーファイルおよび証明書ファイルのバックアップコピーを安全な場所に保管します。これにより、サーバがクラッシュした場合でも、再び簡単にサーバをセキュリティで保護できます。
4. セキュリティで保護された接続をテストするには、Web ブラウザを開き、https を使用するサイトにアクセスします。ブラウザのエラーや警告は表示されないはずです。Internet Explorer と Firefox の両方でテストを実施してください。これは、中間証明書がインストールされていない場合に Firefox で警告が表示されるためです。サイトを利用できないことを示すメッセージがブラウザに表示される場合は、サーバがポート 443 で待機していない可能性があります。Web 要求がタイムアウトする場合は、Web サーバへのトラフィックが TCP ポート 443 でファイアウォールによってブロックされている可能性があります。

IBM HTTP Server

中間証明書とルート証明書をインストールする

1. ルート証明書と中間証明書、およびサーバ証明書をダウンロードします。
2. **UNIX :** コマンドプロンプトで、「IKEYMAN」と入力します。
   Windows : IBM HTTP Server フォルダにある鍵管理ユーティリティを起動します。
3. メインユーザインタフェースで、**[鍵データベース・ファイル]** をクリックし、**[オープン]** をクリックします。
4. 鍵データベースを選択し、**[OK]** をクリックします。
5. パスワードを入力し、**[OK]** をクリックします。
6. [鍵データベース] 画面で、**[署名者の証明書]** をクリックし、**[追加]** をクリックします。
7. ルート証明書を参照し、**[OK]** をクリックします。このファイルがすでにインストールされていることを示すメッセージが表示された場合は、次に進むように選択します。中間証明書について、上記の手順を繰り返します。

サーバ証明書をインストールする

1. IKEYMAN の [鍵データベース] で、**[個人証明書]** をクリックし、**[受信]** をクリックします。
2. [ファイルから証明書を受信] 画面でサーバ証明書を選択し、**[OK]** をクリックします。

Java ベースの Web サーバ (汎用)

1. KeyStore (domain.jks) が保存されているフォルダに、.p7b 形式のサーバ証明書をダウンロードします。

   注意 : CSR の生成に使用したのと同じ KeyStore に証明書をインストールする必要があります。
2. コマンドプロンプトで、次のように入力します。

   keytool -import -trustcacerts -alias server -file your_domain_name.p7b -keystore filename.jks

   ※ **your_domain_name** は、保護するドメインの名前です。ワイルドカード証明書を要求する場合は、ファイル名の先頭にアスタリスク (*) を付けないでください。これは、アスタリスクがファイル名では無効な文字であるためです。
3. 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。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。

   ※ SSL を使用するようにサーバを設定する手順については、Web サーバのドキュメントを参照してください。

Lotus Domino 8.5

1. サーバー証明書管理画面で、**[Install Trusted Root Certificate into Key Ring]** をクリックします。
2. **[Merge Trusted Root Certificate into Key Ring]** をクリックします。インポートする証明書の概要が表示されます。**[OK]** をクリックします。
3. インポートが成功したことを示す確認メッセージが表示されます。**[OK]** をクリックします。
4. このプロセスを、ルート証明書、中間証明書、サーバ証明書の順序で繰り返します。
5. **[Install Certificate into Key Ring]** をクリックします。
6. **[Merge Certificate into Key Ring]** をクリックします。インポートが成功したことを示す確認メッセージが表示されます。

中間証明書をインストールする

1. 中間証明書をダウンロードしてサーバに保存します。
2. Web サーバの [Admin] 画面で、**[Security]** → **[Certificates]** → **[Intermediate CA Certificate]** の順にクリックします。
3. **[Browse]** をクリックし、サーバに保存したいずれかの中間証明書を探します。**[OK]** をクリックし、**[Install]** をクリックします。次の証明書について、上記の手順を繰り返します。

サーバ証明書をインストールする

1. サーバ証明書のテキストをコピーしてファイルに貼り付け、.crt ファイルとして保存します (例: ssl_cert.crt)。
2. Web サーバの [Admin] 画面で、**[Security]**→**[Certificates]** の順にクリックします。
3. **[Browse]** をクリックし、保存した SSL 証明書を探して **[OK]** をクリックします。
4. **[Install]** をクリックします。これで、Web サーバに証明書がインストールされました。

SSL 接続を選択する

1. **[Security]** → **[SSL]** の順にクリックします。
2. SSL を使用するように設定する接続のチェックボックスをオンにして、**[Apply]** をクリックします。

証明書インタフェースを選択する

1. Web サーバの [Admin] 画面で、**[Security]** → **[Certificates]** → **[Interfaces]** の順にクリックします。
2. **[Interface]** ボックスに、SSL 証明書を使用するインタフェースを入力します。完全修飾ドメイン名 (FQDN) または IP アドレスを指定できます。空白のままにすると、証明書がプライマリシステムインタフェースで使用されます。
3. **[Set]** をクリックします。

Nginx

1. サーバ SSL 証明書と証明書のバンドルファイルを Nginx サーバにダウンロードします。Nginx サーバには、証明書要求の生成時に作成されたキーファイルがあります。
2. 証明書ファイルとキーファイルを参照するように Nginx の設定を編集します。編集する設定ファイルは Nginx のバージョン、使用する OS、および Nginx のインストール方法によって異なります。

Nginx サーバの設定方法の詳細については、

http://nginx.org/en/docs/http/configuring_https_servers.html#chains を参照してください。

Oracle Wallet Manager

1. AffirmTrust ポータルからダウンロードした SSL 証明書をコピーします。
2. Oracle Wallet Manager を開き、メインパネルに移動します。
3. メニューバーで、**[操作]→[信頼できる証明書のインポート]** の順にクリックします。[信頼できる証明書のインポート] 画面が表示されます。
4. **[証明書の貼付け]** を選択し、**[OK]** をクリックします。次のメッセージを表示する、もう 1 つの [信頼できる証明書のインポート] 画面が表示されます。証明書をその下に貼り付けます。
5. 画面に証明書を貼り付けたら、**[OK]** をクリックします。信頼できる証明書が正常にインストールされたことを示すメッセージが画面の最下部に表示されます。
6. **[OK]** をクリックします。Oracle Wallet Manager のメインパネルに戻ります。信頼できる証明書が **[信頼できる証明書]** ツリーの最下部に表示されます。

Oracle WebLogic Server 8 または 9

WebLogic にサーバ証明書をインストールする

この手順では、必要なすべての証明書をキーストアにロードします。

1. AffirmTrust ポータルから your_domain_com.p7b 証明書ファイルをダウンロードします。
2. 次のコマンドを実行して、キーストアに証明書をインストールします。

   keytool -import -trustcacerts -alias server -file your_domain_com.p7b -keystore your_domain_name.jks

   「Certificate reply was installed in keystore」という確認メッセージが表示されます。証明書を信頼するよう求められたら、「yes」と入力します。

次に、キーストアを使用するようにサーバを設定する必要があります。

WebLogic で使用するようにキーストアを設定する

1. WebLogic Server で、**[サーバ]** ノードを展開し、設定するサーバを選択します。
2. **[コンフィグレーション]** → **[キーストア & SSL]** の順にクリックします。**[キーストア コンフィグレーション]** の下には、初期設定またはインストール済みのキーストアがいくつか表示される場合があります。
3. 新しいキーストアを有効にするには、**[キーストア コンフィグレーション]** の **[変更]** をクリックします。
4. キーストアの設定タイプとして **[カスタム ID と Java 標準信頼]** を選択し、**[続行]** をクリックします。
5. **[カスタム ID キーストア]** に、サーバ上の your_domain_name.jks ファイルの完全なパスを入力します。
6. **[カスタム ID キーストアの種類]** を「jks」に設定します。
7. **[カスタム ID キーストアのパスフレーズ]** を、キーストアの作成時に指定したパスワードに設定します。パスワードを忘れた場合は、もう一度キーストアの作成から始めて、このプロセス全体をやり直す必要があります。
8. 表示される指示に従って、確認のためにキーストアのパスワードをもう一度入力します。
9. **[続行]** をクリックし、**[完了]** をクリックします。
10. **[サーバ]** ノードに戻り、設定するサーバを選択します。
11. **[コンフィグレーション]** → **[キーストア & SSL]** の順にクリックし、**[キーストア コンフィグレーション]** の **[変更]** をクリックします。
12. SSL の設定画面で、WebLogic Server の ID と信頼を保存する方法として **[キーストア]** を選択します。
13. キーストアの作成時に使用した **[プライベート キーのエイリアス]** と **[パスフレーズ]** を指定します。エイリアスは「server」で、パスフレーズはキーストアのパスワードです。
14. **[続行]** をクリックし、**[完了]** をクリックします。
15. WebLogic Server を再起動します。これで、キーストアのインストールが完了し、キーストアが有効になります。

Plesk

Plesk 10

1. サーバ証明書、中間証明書、および CA 証明書のバンドルをダウンロードします。
2. Parallels Plesk Panel にログインします。
3. **[ホスティングサービス]** メニューの **[ドメイン]** をクリックします。
4. 使用するドメイン名の横にある **[コントロールパネルで開く]** をクリックします。
5. **[ウェブサイトとドメイン]** タブを開き、**[サイトをセキュリティ保護する]** をクリックします。
6. **[証明書の名前]** で、使用する証明書をクリックします。
7. **[証明書]** の横にある **[ブラウズ]** をクリックします。
8. サーバ証明書ファイルを探して、**[開く]** をクリックします。
9. **[CA 証明書]** の横にある **[ブラウズ]** をクリックします。
10. 証明書のバンドルファイルを探して、**[開く]** をクリックします。
11. **[ファイル送信]** をクリックします。
12. サーバで Linux を実行している場合は、Apache プロセスを停止して、再び開始します。サーバで Windows を実行している場合は、DNS サービスを停止して、再び開始します。

Plesk 9

1. サーバ証明書、中間証明書、および CA 証明書のバンドルをダウンロードします。
2. Parallels Plesk Panel にログインします。
3. 左側にあるメニューで、**[ドメイン]** を選択します。
4. 証明書を発行する対象となるドメイン名をクリックします。
5. **[証明書]** メニュー項目をクリックします。
6. **[参照]** をクリックして署名済みの SSL 証明書を探します。
7. 証明書ファイルを選択し、**[ファイル送信]** をクリックします。
8. サーバ SSL 証明書の場所に移動します。サーバ SSL 証明書を選択し、**[ファイル送信]** をクリックします。対応する秘密鍵に対して証明書がアップロードおよびインストールされます。
9. 表示されるリストで、証明書の名前をクリックします。
10. 証明書のバンドルファイルをテキストエディタで開き、ファイルの内容をコピーして、**[CA 証明書]** ボックスに貼り付けます。
11. **[テキスト送信]** をクリックします。
12. **[上へ]** をクリックし、もう一度 **[上へ]** をクリックします。
13. **[Web ホスティング設定]** を選択します。
14. 画面の上部にある **[SSL 証明書]** を、インストールした証明書に変更し、**[OK]** をクリックします。
15. **[ホーム]** をクリックし、**[サービス管理]** をクリックします。
16. サーバで Linux を実行している場合は、Apache プロセスを停止して、再び開始します。サーバで Windows を実行している場合は、DNS サービスを停止して、再び開始します。

Plesk 8

1. サーバ証明書、中間証明書、および CA 証明書のバンドルをダウンロードします。
2. Parallels Plesk Panel にログインします。
3. 左側にあるメニューで、**[ドメイン]** をクリックします。
4. 証明書を発行する対象となるドメイン名をクリックします。
5. **[SSL 証明書]** メニュー項目をクリックします。
6. **[参照]** をクリックしてサーバ SSL 証明書を探します。
7. 証明書ファイルを選択し、**[ファイル送信]** をクリックします。対応する秘密鍵に対して証明書がアップロードおよびインストールされます。
8. 表示されるリストで、証明書の名前をクリックします。
9. 証明書のバンドルファイルをテキストエディタで開き、ファイルの内容をコピーして、**[CA 証明書]** ボックスに貼り付けます。
10. **[テキスト送信]** をクリックします。
11. **[上へ]** をクリックし、**[設定]** をクリックします。
12. 画面の上部にある **[SSL 証明書]** ドロップダウンメニューで、インストールした証明書に変更します。
13. 左側にあるメニューで、**[サーバ]** をクリックします。
14. **[サービス管理]** をクリックします。
15. サーバで Linux を実行している場合は、Apache プロセスを停止して、再び開始します。サーバで Windows を実行している場合は、DNS サービスを停止して、再び開始します。

注意 ： 単に Apache を再起動するだけでは不十分です。インストールを完了するには、サービスを停止してから再び開始してください。

SAP Web Application Server 6.10 以降

サーバ証明書をインストールする

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. 署名済みの証明書を格納する各アプリケーションサーバについて、次の手順を実行します。
    1. 適切なアプリケーションサーバをダブルクリックして選択します。アプリケーションサーバの SSL サーバ PSE が **[PSE maintenance]** に表示されます。
    2. **[PSE maintenance]** で、**[Import Cert. Response]** を選択します。証明書要求が画面に表示されます。証明書要求応答をコピーします。
    3. 証明書要求応答を画面内のテキストボックスに貼り付けます。署名済みの公開鍵証明書がサーバの SSL サーバ PSE にインポートされ、[PSE maintenance] に表示されます。証明書をダブルクリックすると、その証明書の情報を確認できます。
    4. データを保存します。

次に、CA のルート証明書をインポートする必要があります。インポート手順は、証明書がある場所によって異なります。

証明書データベースにあるルート証明書をインポートする

1. [certificate] で、**[Import certificate]** をクリックします。
2. [Import Certificate] 画面が表示されます。**[Database]** タブストリップを選択します。
3. 証明書データベースから証明書を選択し、**[Enter]** を選択します。証明書が [certificate] に表示されます。
4. **[Add to Certificate List]** をクリックします。[PSE maintenance] に表示される PSE の証明書リストに証明書が追加されます。
5. データを保存します。

ファイルシステムにある CA ルート証明書をインポートする

1. [certificate] で、[Import certificate] を選択します。
2. [Import Certificate] 画面が表示されます。
3. ファイルシステムの対応するファイル名を入力します。
4. 証明書のファイル形式 (Base64) を選択します。[Enter] を選択します。
5. 証明書が [certificate maintenance] に表示されます。
6. [Add to Certificate List] を選択します。
7. [PSE maintenance] に表示される PSE の証明書リストに証明書が追加されます。
8. データを保存します。

別の PSE にある CA ルート証明書をインポートする

1. 証明書を含む PSE のノードを展開し、いずれかのアプリケーションサーバをダブルクリックして選択します。
2. PSE とその証明書リストが **[PSE maintenance]** に表示されます。
3. 証明書をダブルクリックして選択します。

4. 証明書が **[certificate maintenance]** に表示されます。
5. **[SSL server PSE]** ノードで、いずれかのアプリケーションサーバをダブルクリックして選択します。
6. **[Add to Certificate List]** をクリックします。
7. [PSE maintenance] に表示される PSE の証明書リストに証明書が追加されます。
8. データを保存します。
9. すべての証明書について、上記の手順を繰り返します。

Zeus Web Server

1. SSL 証明書ファイルをテキストエディタで開き、サーバ証明書、中間証明書、ルート証明書の順序で内容を貼り付けます。

   ——BEGIN CERTIFICATE——
   (サーバ証明書: your_domain_name.crt)
   ——END CERTIFICATE——
   ——BEGIN CERTIFICATE——
   (中間証明書: AffirmTrust_Certificate_Authority–OV1.crt)
   ——END CERTIFICATE——
   ——BEGIN CERTIFICATE——
   (クロスルート証明書: AffirmTrust_Networking.crt)
   ——END CERTIFICATE——
   ——BEGIN CERTIFICATE——
   (ルート証明書: root_certificate.crt)
   ——END CERTIFICATE——

2. Web サーバで、**[SSL certificates]** を選択します。
3. この証明書の **[Generate CSR]** (**[Replace Certificate]** の場合もある) をクリックします。
4. 新しく連結された証明書を **[Signed Certificate]** ボックスに貼り付けて、**[OK]** をクリックします。
5. この証明書を受け入れます。
6. **[Home]** をクリックし、保護するドメインの横にあるチェックボックスをオンにします。**[Configure]** をクリックします。
7. **[SSL enabled]** に移動します。**[SSL is enabled]** をクリックして証明書を選択します。
8. 変更を保存してサーバを再起動します。