
Kousec Server Certificate Manager

Oracle WebLogic Server への証明書インストール方法

Copyright 2009 Kousec Software, Inc. All rights reserved.

Kousec and Kousec Server Certificate Manager are trademarks of Kousec Software, Inc.
WebLogic and BEA WebLogic Server are registered trademarks of BEA Systems, Inc, a
subsidiary of Oracle Corporation.

All company names and product names are trademarks of their respective holders.

r3

Table of Contents

はじめに	4
対象製品	4
証明書申請・取得時の操作	5
証明書の配備時の操作	5
(A) 証明書の新規インストール	6
サーバーコンピューター上での準備	6
CertMgr 上での操作	6
サーバーコンピューター上での証明書のインストール	7
WebLogic Server の Keystore と SSL 設定の変更	8
(B) 証明書の更新	9
CertMgr 上での操作	9
WebLogic Server 9 以降での手順	9
WebLogic Server 9 以前での手順	10

はじめに

WebLogic Server において通常の SSL 証明書の取得は、まず証明書用の鍵と CSR(Certificate Signing Request)をサーバー内の keystore 内で生成するところから始まります。

Kousec Server Certificate Manager を使用した場合は、証明書用の鍵は Kousec Server Certificate Manager 内で生成しそこで一元的に管理します。そして証明書と秘密鍵の両方を、WebLogic サーバー内の keystore にインポートする方法を取っています。したがって、WebLogic サーバー上で CSR の生成することはありません。証明書を CA に申請する際は Apache2 の形式を指定して証明書を取得し、Kousec Server Certificate Manager に登録します。

本文書では、Kousec Server Certificate Manager に登録された証明書と秘密鍵を WebLogic Server にインストールする手順を説明します。

なお、本ドキュメント内では、Kousec Server Certificate Manager を Kousec CertMgr または CertMgr と省略表記します。

対象製品

Kousec Server Certificate Manager Beta-2

Oracle WebLogic Server (formerly known as BEA WebLogic Server)

本ドキュメントでは下記製品の Windows 版を使用した場合の手順を掲載しています。

BEA WebLogic Server® 9.2

また内容の大部分は下記製品にも適用可能です。

BEA WebLogic Server® 8.1

証明書申請・取得時の操作

WebLogic Server 用の SSL 証明書は CertMgr の通常の操作で取得します。CA には常に **Apache2** 用証明書と指定してください(WebLogic や Java アプリケーションサーバーではない)。Kousec CertMgr が Apache 用の証明書を JKS ベースサーバー(すなわち WebLogic Server)用に変換・パッケージします。

証明書のインストール先サーバーの設定は、証明書定義の作成時や次に説明する配備プロセス実行時のどちらでも指定できます。

証明書定義作成時に指定する場合、サーバーソフトウェアタイプの指定は **Java(generic)** を選択します。サーバーソフトウェアオプションについては、以下の「証明書の配備時の操作」を参照してください。

証明書の配備時の操作

SSL 証明書の新規インストールと更新

2つのケースに分けて説明します。

A) 現在 Demo Identity JKS を使用している。または、現在既に商用 CA からの証明書を使っているが今回 CertMgr 導入にあたり ID キーストアファイルを規則性のあるパスとファイル名に変更したい。もしくはストアパスワードなどが分からない。

B) 現在既に商用 CA からの証明書を使っておりその ID キーストアの名前は server.jks である。今回 CertMgr 導入してもその JKS ファイル名や alias 名、ストアパスワードなどは現在のまま使用したい。

ここでは A)を証明書の新規インストール、B)を証明書の更新と呼びます。

A)の場合、対象 WebLogic サーバーの SSL 設定変更を伴います。

1. CertMgr からの証明書パッケージで新規に ID キーストア(JKS ファイル)を作成
2. 対象 WebLogic サーバーの Keystore 設定と SSL 設定を行う
3. 対象 WebLogic サーバーを立ち上げなおす

B)の場合は、対象 WebLogic サーバーの設定変更は伴いません。

1. 対象 WebLogic サーバーを停止する
2. CertMgr からの証明書パッケージで ID キーストア (JKS ファイル) を変更
3. 対象 WebLogic サーバーを開始する

当然 alias 名、ストアパスワード、キーパスワードは知っておかなければなりません。

WebLogic Server 9 以降では、対象 WebLogic サーバー自体の再起動は必要なく、SSL だけを再起動できます。その場合は以下のような流れになります。

1. CertMgr からの証明書パッケージで ID キーストア (JKS ファイル) を変更
2. Administration Console から対象サーバーを選択し、SSL の再起動を行う

(A) 証明書の新規インストール

サーバーコンピューター上での準備

ID キーストアの JKS ファイルは WL_HOME¥server¥ssl-private というディレクトリを作成しそこに配置します。サーバーマシン上で ssl-private ディレクトリを作成しておきます。

コマンドラインを立ち上げて サーバー証明書用のディレクトリを作成します

```
>cd C:¥bea¥weblogic92¥server
```

```
>mkdir ssl-private
```

CertMgr 上での操作

JKS ファイル名は<コモンネーム>.jks と命名します。配備する証明書のコモンネームが www2.example.com の場合、www2.example.com.jks とします。

配備情報の入力画面の Server Software Type に JKS(generic)を選択します。Server Name には対象 WebLogic サーバーコンピューターのホスト名を入力します。

そして Server Software Options には以下を設定します。

```
JKS File Path: C:¥bea¥weblogic92¥server¥ssl-private¥www2.example.com.jks
```

Alias in Keystore: wlserver (任意)
Keystore Password: changeit (任意)

最後に[Set]を押して確定します。

サーバーコンピュータ上での証明書のインストール

証明書インストールパッケージ(cert.zip)を unzip し中の jks_inst.bat を実行します。

```
C:¥work¥cert¥cert>jks_inst.bat
Kousec Certmgr Cert Installer for JKS 0.1.5a
successfully read parameter file
Creating new keyStore file : C:¥bea¥weblogic92¥server¥ssl-private¥www2.example.com.jks
Certificate chain length: 2
Subject: CN=www2.example.com
Validity Period: 2009/10/08 22:53:39 to 2010/10/08 22:53:39
Intermediate CA Certificates
Subject: CN=Kousec CertMgr Auto-Generated CA 20090715215939
SUCCESS:A new key store with private key and certificate is created.
Alias and key password are set as follows:
    Alias:wlserver Password:changeit
You can change them using one of the commands below:
keytool -keypasswd -alias wlserver -keystore
"C:¥bea¥weblogic92¥server¥ssl-private¥www2.example.com.jks"
keytool -changealias -alias wlserver -keystore
"C:¥bea¥weblogic92¥server¥ssl-private¥www2.example.com.jks"
Enter 'y' or 'n' to end this program(y/n)y
Press any key to continue . . .
```

これで、C:¥bea¥weblogic92¥server¥ssl-private に www2.example.com.jks という ID キーストアファイルが作成されました。

WebLogic Server の Keystore と SSL 設定の変更

次に、WebLogic サーバーがこの ID キーストアファイルを使うように設定します。

ここでは、WebLogic Server 9.2 での手順を示します。

- Administration Console にログインします。
- Environment > Servers > 該当サーバーを選択し、Configuration タブを開きます。
- Keystores タブを開きます。
- Keystores のリストボックスで、デフォルトでは Demo Identity and Demo Trust が選択されています。これを別の値に変更し新たな ID キーストアとトラストキーストアを作るのですがその参考にするために、現在の画面のコピーを取って置きます。
- Keystores のリストボックスで、Custom Identity and Java Standard Trust を選択する。そして以下を入力します。

Custom Identity Keystore: **C:\bea\weblogic92\server\ssl-private\www2.example.com.jks**

Custom Identity Keystore Type: **jks**

Custom Identity Keystore Passphrase: **changeit**

Confirm Custom Identity Keystore Passphrase: **changeit**

Java Standard Trust Keystore の方は変更しません。

- [Save] ボタンをクリックして保存します。
- SSL タブを開きます。
- Identity and Trust Locations のリストボックスで Keystores が選択されていることを確認します。
- 下記を入力します。

Private Key Location: **from Custom Identity Keystore** になっていることを確認

Private Key Alias: **wlserver**

Private Key Passphrase: **changeit**

Confirm Private Key Passphrase: **changeit**

Certificate Location: **from Custom Identity Keystore** になっていることを確認

Trusted Certificate Authorities: **from Java Standard Trust Keystore** になっていることを確認

- [Save]ボタンをクリックして保存する

- 最後に左側にある[Activate Changes]をクリックすると対象サーバーで SSL 証明書が有効になります。

WebLogic Server 8.1 を使用している場合、手順の多くは同様です。ただし新しい ID キーストアを有効にするために対象サーバーを再起動する必要があります。

(B) 証明書の更新

CertMgr 上での操作

現在 WebLogic で使用中の ID キーストアファイルに合わせて設定します。

例

JKS File Path: C:\bea\weblogic92\server\lib\server.jks

Alias in Keystore: wl_server

Keystore Password: Something

最後に[Set]を押して確定します。

注意: 現バージョンの CertMgr では Keystore Password と Key Password は同一である必要があります。

WebLogic Server 9 以降での手順

- 証明書インストールパッケージをサーバーマシン上で実行します。

cert.zip を unzip し中の jks_inst.bat を実行します。

- Administration Console から対象サーバーを選択し、SSL の再起動を行います。

WebLogic Server 9.2 での手順を示します。

- ・ 左ペインの Environment > Servers ノードをクリックし、右側で対象サーバーを選択
- ・ Control - Start/Stop タブをクリック
- ・ ページ下部の Server Status 表に行き、対象サーバーのチェックボックスを選択。
- ・ Restart SSL ボタンをクリックする

WebLogic Server 9 以前での手順

SSL の単独再起動ができない WebLogic Server 製品では（例えば WebLogic Server 8.1）、jks_inst.bat の実行中は対象の WebLogic サーバーを停止しておきます。

対象の WebLogic サーバーを shutdown します

jks_inst.bat を実行

対象の WebLogic サーバーを起動します