

WebSphere Application Server V6.1

自己署名証明書の置き換え手順

<Base / Express 編>

V1.1

2008 年 3 月 10 日
日本アイ・ビー・エム株式会社
ソフトウェア事業

目次

1. はじめに	2
2. 証明書更新の準備(セキュリティーを無効化)	4
3. 自己署名証明書の削除	5
4. ノードの自己署名証明書の再作成	10
5. 署名者証明書の追加	12
6. Web サーバー・プラグイン用鍵データベースを更新(ローカル構成)	14
7. Web サーバー・プラグイン用鍵データベースを更新(リモート構成)	16
8. 管理セキュリティーの有効化	19
9. 管理クライアント用トラスト・ストアの更新	20

1. はじめに

WebSphere Application Server(以下WAS) では、V6.1で新しく追加された自己署名証明書の自動更新機能について、幾つかの重要な考慮事項がございます。詳細については、以下の文書をご参照ください。

<http://www.ibm.com/jp/domino01/mkt/websphere.nsf/doc/0033ED2E>

本ガイドでは、WAS V6.1導入後のプロファイル作成時に自動で作成される自己署名証明書(有効期限1年)を、より長い有効期限を持つ自己署名証明書で置き換える手順をご紹介します。ただし、WAS V6.1.0.7以降(Fix Pack 7適用以降)の環境で新しく作成されたプロファイルについては、自己署名証明書の有効期限は15年となっていますので、このガイドで紹介する対応は不要となります。

このガイドは、WAS V6.1のBaseエディション、Expressエディション、およびNetwork Deploymentエディションのスタンドアロンのアプリケーション・サーバー環境を対象としています。Network DeploymentエディションでDeployment Managerを使用したセル環境を構成している場合には、置き換え手順書<ND編>をご参照ください。

以下の章では、次の手順を実施します。

- 2章. 証明書更新のために、管理セキュリティーを無効化します。
- 3章. 有効期限が1年で作成された自己署名証明書を削除します。
- 4章. 有効期限のより長い自己署名証明書を作成します。
- 5章. ノードが使用するトラスト・ストアに署名者証明書を追加します。
- 6章. Webサーバー・プラグイン用鍵データベースに署名者証明書を追加します。(ローカル構成の場合)
- 7章. Webサーバー・プラグイン用鍵データベースに署名者証明書を追加します。(リモート構成の場合)
- 8章. 管理セキュリティーを有効化します。
- 9章. 管理クライアント用のトラスト・ストアに署名者証明書を追加します。

<注意>

- **できる限り最新の FixPack を適用した状態で、作業を実施してください。**
- **これからの先のステップを実行する前に、必ずバックアップを取得しておいてください。**

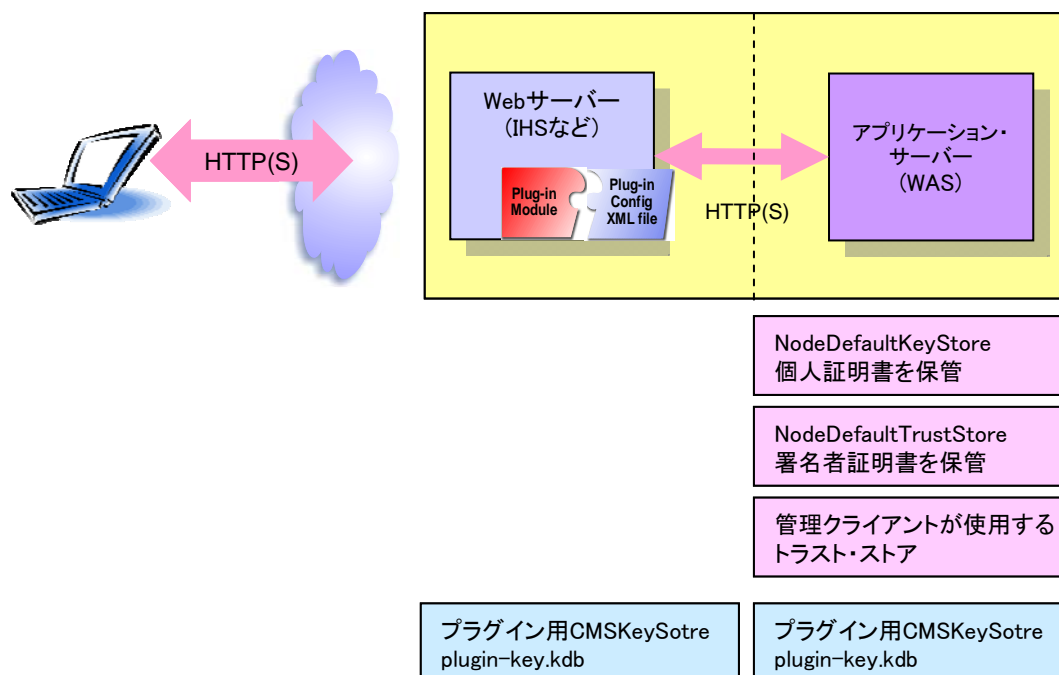
【参考】 証明書を保存する鍵ストアは、デフォルトでは以下の場所にある鍵ストアを使用します。

<WASが導入されているノードの鍵ストア>

- WASが使用するNodeDefaultKeyStore (個人証明書を保管)
<WAS_ROOT>/profiles/<profile_name>/config/cells/<cell_name>/nodes/<node_name>/key.p12
- WASが使用するNodeDefaultTrustStore (署名者証明書を保管)
<WAS_ROOT>/profiles/<profile_name>/config/cells/<cell_name>/nodes/<node_name>/trust.p12
- 管理クライアントが使用するトラスト・ストア
<WAS_ROOT>/profiles/<profile_name>/etc/trust.p12
- Webサーバーが使用するための鍵データベース
<WAS_ROOT>/profiles/<profile_name>/config/cells/<cell_name>/nodes/<node_name>/servers/<wobserver_name>/plugin-key.kdb

<Webサーバーが導入されているノードの鍵ストア>

- Webサーバー・プラグインが使用する鍵データベース
<plugin_install_root>/config/<web_server_name>/plugin-key.kdb



NodeDefaultKeyStore, NodeDefaultTrustStore, 管理クライアント用トラスト・ストアは、WAS の管理セキュリティを使用可能に設定した場合に使用されます。

plugin-key.kdb は、Web サーバー・プラグインと WAS 間が SSL 通信を行う場合に使用されます。ブラウザと Web サーバー間で SSL 通信を行う場合は、デフォルトで Web サーバー・プラグインと WAS 間も SSL 通信が行われます。

2. 証明書更新の準備(セキュリティーを無効化)

管理セキュリティーを使用している場合は無効化します。管理セキュリティーが既に無効になっている場合は、次の3章に進みます。

2-1. 管理セキュリティーを無効化します。

管理コンソールから、「セキュリティー」 → 「管理、アプリケーション、およびインフラストラクチャーの保護」画面を開き、「管理セキュリティー」と「Java 2 セキュリティー」が有効になっている場合は、チェックボックスをはずし、「適用」ボタンをクリックします。(もともとチェックがついていないものについては変更しません。また、管理セキュリティーを無効にした場合、アプリケーション・セキュリティーも自動的に無効となります。)

管理セキュリティー、アプリケーション・セキュリティー、Java 2 セキュリティーのどれが有効になっているか、必ずメモしておいてください。 このガイドの最後で、元のセキュリティー設定に戻す必要があります。

管理、アプリケーション、およびインフラストラクチャーの保護

管理、アプリケーション、およびインフラストラクチャーの保護

管理、アプリケーション、およびインフラストラクチャーの保護

アプリケーションにサービス提供している環境は、管理が制限されている場合、完全に保護されます。あるインフラストラクチャーも保護されます。

構成

セキュリティー構成ウィザード

セキュリティー構成報告書

管理セキュリティー

- 管理セキュリティーを使用可能にする
- [管理ユーザー・ロール](#)
 - [管理グループ・ロール](#)

アプリケーション・セキュリティー

- アプリケーション・セキュリティーを使用可能にする

Java 2 セキュリティー

- Java 2 セキュリティーを使用してアプリケーションのアクセスをローカル・リソースに制限する
- アプリケーションがカスタム許可を認可されたときに警告する
 - リソース認証データへのアクセスを制限する

2-2. マスター構成に保管し、WAS を再起動します。

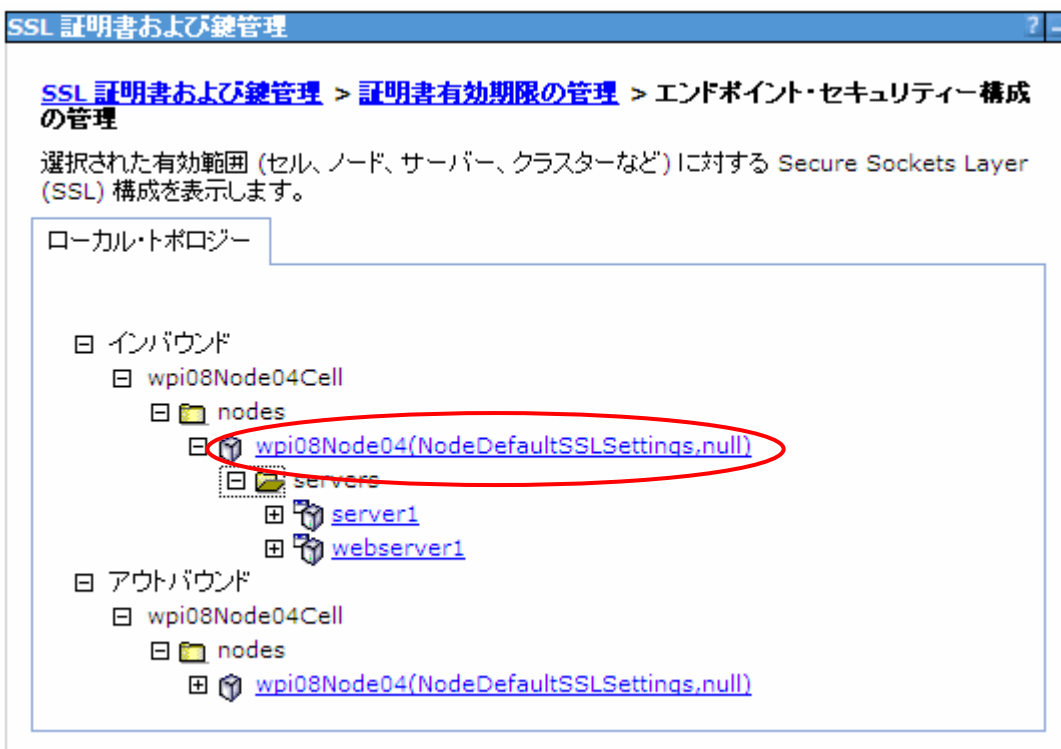
3. 自己署名証明書の削除

管理コンソールから、以下の 3 箇所に存在する自己署名証明書(default)を全て削除します。

- ノードの鍵ストアにある個人証明書
- ノードのトラスト・ストアにある署名者証明書
- CMSKeyStore にある個人証明書、署名者証明書

3-1. ノードの個人証明書を削除します。

管理コンソールから、「セキュリティ」 → 「SSL 証明書および鍵管理」 → 「エンドポイント・セキュリティ構成の管理」を開きます。ローカル・トポロジーにある「インバウンド」- <Cell 名> - 「nodes」 - <node 名> の図から、<node 名> (NodeDefaultSSLSettings,null と書かれているもの)をクリックします。



「関連項目」にある「鍵ストアおよび証明書」をクリックします。「NodeDefaultKeyStore」をクリックし、「追加プロパティ」にある「個人証明書」をクリックします。

SSL 証明書および鍵管理

SSL 証明書および鍵管理 > エンドポイント・セキュリティ構成の管理 > wpi08Node04 > 鍵ストアおよび証明書

暗号方式、RACF(R)、CMS、Java(TM)、およびすべてのトラストストア・タイプを含む、鍵ストア・タイプを定義します。

田 設定

新規作成 削除 署名者の交換...

選択	名前	パス
<input type="checkbox"/>	NodeDefaultKeyStore	\${CONFIG_ROOT}/cells/wpi08Node04Cell/nodes/wpi08Node04/key.p12
<input type="checkbox"/>	NodeDefaultTrustStore	\${CONFIG_ROOT}/cells/wpi08Node04Cell/nodes/wpi08Node04/trust.p12
<input type="checkbox"/>	NodeLTPAKeys	\${CONFIG_ROOT}/cells/wpi08Node04Cell/nodes/wpi08Node04/ltpa.jceks

合計 3

自己署名証明書(発行元と発行先が IBM のもの)のCN= をメモした上で、全て選択し、「削除」ボタンをクリックします。

SSL 証明書および鍵管理

SSL 証明書および鍵管理 > エンドポイント・セキュリティ構成の管理 > wpi08Node04 > 鍵ストアおよび証明書 > NodeDefaultKeyStore > 個人証明書

個人証明書を管理します。

田 設定

自己署名証明書の作成 削除 認証局から証明書を受信 置き換え 抽出 インポート エクスポート

選択	別名	発行元	発行先	シリアル番号	有効期限
<input checked="" type="checkbox"/>	default	CN=wpi08, O=IBM, C=US	CN=wpi08, O=IBM, C=US	1179670660	有効期間は 2007/05/20 から 2008/05/19 です。

合計 1

マスター構成に保管します。

3-2. ノードの署名者証明書を削除します。

管理コンソールから「セキュリティ」→「SSL 証明書および鍵管理」→「エンドポイント・セキュリティ構成の管理」を開きます。ローカル・トポロジーにある「インバウンド」 - <Cell 名> - 「nodes」 - <node 名> の図から、<node 名>をクリックします。「関連項目」にある「鍵ストアおよび証明書」をクリックします。「NodeDefaultTrustStore」をクリックし、「追加プロパティ」にある「署名者証明書」をクリックします。

SSL 証明書および鍵管理

SSL 証明書および鍵管理 > エンドポイント・セキュリティ構成の管理 > wpi08Node04 > 鍵ストアおよび証明書

暗号方式、RACF(R)、CMS、Java(TM)、およびすべてのトラストストア・タイプを含む、鍵ストア・タイプを定義します。

田 設定

新規作成 削除 署名者の交換...

選択	名前	パス
<input type="checkbox"/>	NodeDefaultKeyStore	\${CONFIG_ROOT}/cells/wpi08Node04Cell/nodes/wpi08Node04/key.p12
<input type="checkbox"/>	NodeDefaultTrustStore	\${CONFIG_ROOT}/cells/wpi08Node04Cell/nodes/wpi08Node04/trust.p12
<input type="checkbox"/>	NodeLTPAKeys	\${CONFIG_ROOT}/cells/wpi08Node04Cell/nodes/wpi08Node04/ltpa.jceks

合計 3

default という名前で始まる証明書を全て選択し、「削除」ボタンをクリックします。

SSL 証明書および鍵管理

SSL 証明書および鍵管理 > エンドポイント・セキュリティ構成の管理 > wpi08Node04 > 鍵ストアおよび証明書 > NodeDefaultTrustStore > 署名者証明書

鍵ストア内の署名者証明書を管理します。

田 設定

追加 削除 抽出 ポートから取得

選択	別名	行先	指紋 (SHA ダイジェスト)	有効期限
<input checked="" type="checkbox"/>	default	CN=wpi08, O=IBM, C=US	4D:40:DE:E7:70:73:C1:3C:09:6F:EB:F3:76:E9:C7:C6:A3:2C:91:01	有効期間は 2007/05/20 から 2008/05/19 です。
<input type="checkbox"/>	dummyclientsigner	CN=jclient, OU=SWG, O=IBM, C=US	0B:3F:C9:E0:70:54:58:F7:FD:81:80:70:83:A6:D0:92:38:7A:54:CD	有効期間は 2003/07/31 から 2021/10/14 です。
<input type="checkbox"/>	dummyserver signer	CN=jserver, OU=SWG, O=IBM, C=US	FB:38:FE:E6:CF:89:BA:01:67:8F:C2:30:74:84:E2:40:2C:B4:B5:65	有効期間は 2003/07/31 から 2021/10/14 です。

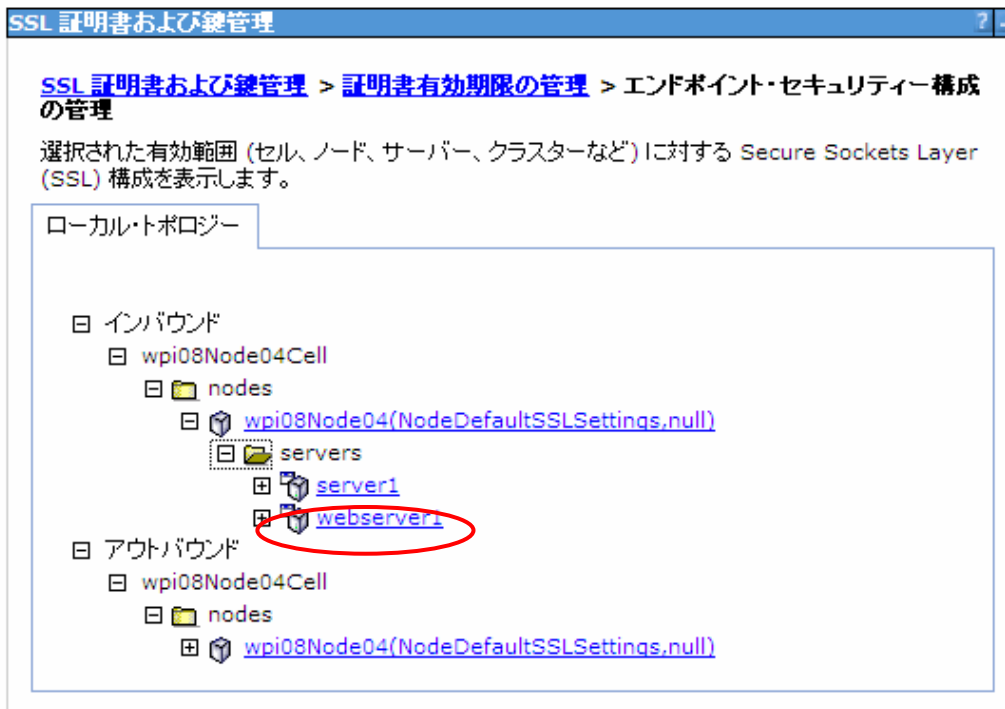
合計 3

マスター構成に保管します。

3-3 CMSKeyStore の個人証明書を削除します。

【注】 Web サーバー・プラグインをリモート構成にした場合は、個人証明書が存在しない場合があります。その場合は、3-4 署名者証明書の削除を実施してください。

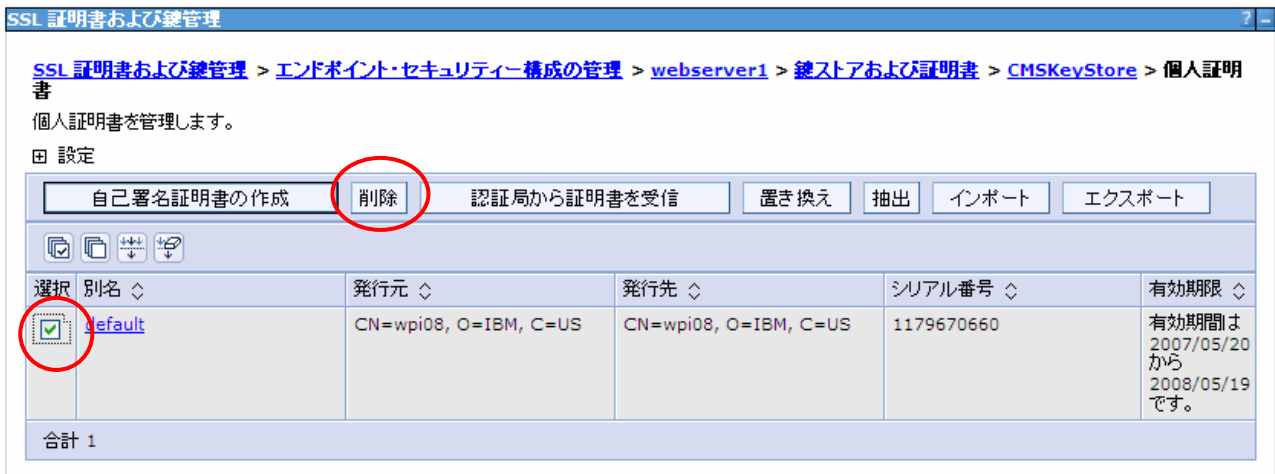
管理コンソールから「セキュリティ」 → 「SSL 証明書および鍵管理」 → 「エンドポイント・セキュリティ構成の管理」を開きます。ローカル・トポロジーを展開し、「インバウンド」 - <Cell 名> - 「nodes」 - <node 名> - 「servers」 - <webserver 名> をクリックします。



「関連項目」にある「鍵ストアおよび証明書」をクリックします。「CMSKeyStore」をクリックし、「追加プロパティ」にある「個人証明書」をクリックします。



default という名前で始まる証明書を全て選択し、「削除」ボタンをクリックします。



マスター構成に保管します。

3-4 CMSKeyStore の署名者証明書を削除します。

【注】 Web サーバー・プラグインをローカル構成にした場合は、CMSKeyStore に default という名前の署名者証明書が存在しません。3-3 にて個人証明書の削除を実施していれば問題ありません。

管理コンソールから「セキュリティ」 → 「SSL 証明書および鍵管理」 → 「エンドポイント・セキュリティ構成の管理」を開きます。ローカル・トポロジーを展開し、「インバウンド」 - <Cell 名> - 「nodes」 - <node 名> - 「servers」 - <webserver 名> をクリックします。「関連項目」にある「鍵ストアおよび証明書」をクリックします。「CMSKeyStore」をクリックし、「追加プロパティ」にある「署名者証明書」をクリックします。

default という名前で始まる証明書を全て選択し、「削除」ボタンをクリックします。
(VeriSign など IBM 以外のものを削除する必要はありません。)

マスター構成に保管します。

4. ノードの自己署名証明書の再作成

有効期限が長い(このガイドでは 15 年)自己署名証明書を作成します。

4-1. ノードの自己署名証明書を再作成します。

管理コンソールから「セキュリティ」→「SSL 証明書および鍵管理」→「エンドポイント・セキュリティ構成の管理」を開きます。ローカル・トポロジーを展開し、「インバウンド」 - <Cell 名> - 「nodes」 - <node 名>をクリックします。「このエンドポイントの特定 SSL 構成」にある「証明書の管理」ボタンをクリックします。

一般プロパティ

名前
wpi08Node04

方向
インバウンド

このエンドポイントの特定 SSL 構成

SSL 構成
NodeDefaultSSLSettings

証明書別名リストの更新

証明書の管理

鍵ストアの証明書別名
(なし)

4-2. 「自己署名証明書の作成」ボタンをクリックします。

SSL 証明書および鍵管理

SSL 証明書および鍵管理 > エンドポイント・セキュリティ構成の管理 > wpi08Node04 > 個人証明書

個人証明書を管理します。

設定

自己署名証明書の作成

削除

認証局から証明書を受信

置き換え

抽出

インポート

エクスポート

選択	別名	発行元	発行先	シリアル番号	有効期限
	なし				
合計 0					

4-3. 構成のタブで以下の値を入力した後、「適用」ボタンを押します。

別名: default (任意の名前で構いません)

共通名: <上記手順 3-1 で CN= としてメモした値>

有効期間: 5475 (任意の期間で構いませんが、デフォルトが 365 に設定されているため、1 年で有効期限が切れます。ここでは、約 15 年とした設定例を示しています。)

組織: IBM

構成

一般プロパティ

* 別名
default

バージョン
X509 V3

鍵サイズ
1024 ビット

* 共通名
wpi08

* 有効期間
5475 日間

* 組織
IBM

4-4. 以下の確認画面が出ますので、有効期間を確認し、マスター構成に保管します。

一般プロパティ

別名
default

バージョン
X509 V3

鍵サイズ
1024 ビット

シリアル番号
1204178985

有効期間
有効期間は 2008/02/28 から 2023/02/24 です。

発行先
CN=wpi08, O=IBM, C=US

発行元
CN=wpi08, O=IBM, C=US

指紋 (SHA ダイジェスト)
E0:C1:C8:CB:1A:86:51:9D:A3:BE:EE:47:D9:00:AB:2F:8F:C7:04:1C

署名アルゴリズム
SHA1withRSA(1.2.840.113549.1.1.5)

5. 署名者証明書の追加

NodeDefaultTrustStore に署名者証明書を追加します。

5-1. NodeDefaultKeyStore と NodeDefaultTrustStore の署名者を交換します。

管理コンソールから「セキュリティ」→「SSL 証明書および鍵管理」→「エンドポイント・セキュリティ構成の管理」を開きます。ローカル・トポロジーを展開し、「インバウンド」 - <Cell名> - 「nodes」 - <node 名> をクリックします。「関連項目」にある「鍵ストアおよび証明書」をクリックします。「NodeDefaultKeyStore」と「NodeDefaultTrustStore」を選択し、「署名者の交換...」ボタンをクリックします。



The screenshot shows the 'SSL 証明書および鍵管理' (SSL Certificate and Key Management) console. The breadcrumb path is 'SSL 証明書および鍵管理 > エンドポイント・セキュリティ構成の管理 > wpi08Node04 > 鍵ストアおよび証明書'. Below the breadcrumb, there is a description: '暗号方式、RACF(R)、CMS、Java(TM)、およびすべてのトラストストア・タイプを含む、鍵ストア・タイプを定義します。' and a '設定' (Settings) section. In the settings bar, the '署名者の交換...' (Signer Exchange...) button is circled in red. Below this is a table with three rows:

選択	名前	パス
<input checked="" type="checkbox"/>	NodeDefaultKeyStore	\${CONFIG_ROOT}/cells/wpi08Node04Cell/nodes/wpi08Node04/key.p12
<input checked="" type="checkbox"/>	NodeDefaultTrustStore	\${CONFIG_ROOT}/cells/wpi08Node04Cell/nodes/wpi08Node04/trust.p12
<input type="checkbox"/>	NodeLTPAKeys	\${CONFIG_ROOT}/cells/wpi08Node04Cell/nodes/wpi08Node04/ltpa.jceks

At the bottom of the table, it says '合計 3' (Total 3).

5-2. 署名者証明書を追加します。

「NodeDefaultKeyStore」の自己署名証明書(ここでは「default」)を選択し、「追加>>」ボタンをクリックします。

一般プロパティ

交換する署名者

NodeDefaultKeyStore 個の個人証明書 default	追加 >>	NodeDefaultTrustStore 個の署名者
	<< 除去	
NodeDefaultTrustStore 個の個人証明書	追加 >>	NodeDefaultKeyStore 個の署名者
	<< 除去	

適用 OK リセット 取り消し

5-3. 「NodeDefaultTrustStore」に署名者(ここでは「default」)が追加されたら、「OK」ボタンをクリックします。

一般プロパティ

交換する署名者

NodeDefaultKeyStore 個の個人証明書	追加 >>	NodeDefaultTrustStore 個の署名者 default
	<< 除去	
NodeDefaultTrustStore 個の個人証明書	追加 >>	NodeDefaultKeyStore 個の署名者
	<< 除去	

適用 OK リセット 取り消し

5-4. マスター構成に保管します。

6. Web サーバー・プラグイン用鍵データベースを更新(ローカル構成)

次に、Webサーバー・プラグインが使用する鍵データベース(plugin-key.kdb)に署名者証明書を追加します。Webサーバー・プラグインをリモート構成にしている場合は、次の7章に進んでください。

6-1. NodeDefaultKeyStore と Web サーバーが使用する CMSKeyStore の署名者を交換します。

管理コンソールから「セキュリティ」 → 「SSL 証明書および鍵管理」 → 「エンドポイント・セキュリティ構成の管理」を開きます。ローカル・トポロジーを展開し、「インバウンド」 - <Cell 名> - 「nodes」 - <node 名> - 「servers」 - <Web サーバー名> をクリックします。「関連項目」にある「鍵ストアおよび証明書」をクリックします。「CMSKeyStore」と「NodeDefaultKeyStore」を選択し、「署名者の交換...」ボタンをクリックします。



SSL 証明書および鍵管理

SSL 証明書および鍵管理 > エンドポイント・セキュリティ構成の管理 > webserver1 > 鍵ストアおよび証明書

暗号方式、RACF(R)、CMS、Java(TM)、およびすべてのトラストストア・タイプを含む、鍵ストア・タイプを定義します。

田 設定

新規作成 削除 **署名者の交換...**

選択	名前	パス
<input checked="" type="checkbox"/>	CMSKeyStore	c:\\Program Files\\IBM\\WebSphere\\AppServer\\profiles\\HaraSingle\\config\\cells\\wpi08Nokey.kdb
<input checked="" type="checkbox"/>	NodeDefaultKeyStore	\${CONFIG_ROOT}/cells/wpi08Node04Cell/nodes/wpi08Node04/key.p12
<input type="checkbox"/>	NodeDefaultTrustStore	\${CONFIG_ROOT}/cells/wpi08Node04Cell/nodes/wpi08Node04/trust.p12
<input type="checkbox"/>	NodeLTPAKeys	\${CONFIG_ROOT}/cells/wpi08Node04Cell/nodes/wpi08Node04/ltpa.jceks

合計 4

6-2. CMSKeyStore に署名者証明書を追加します。

「NodeDefaultKeyStore」の自己署名証明書(ここでは「default」)を選択し、「追加>>」ボタンをクリックします。

一般プロパティ

交換する署名者

CMSKeyStore 個の個人証明書	追加 >>	NodeDefaultKeyStore 個の署名者
	<< 除去	
NodeDefaultKeyStore 個の個人証明書	追加 >>	CMSKeyStore 個の署名者
default	<< 除去	

適用 OK リセット 取り消し

6-3. 「CMSKeyStore」に署名者(ここでは「default」)が追加されたら、「OK」ボタンをクリックします。

一般プロパティ

交換する署名者

CMSKeyStore 個の個人証明書	追加 >>	NodeDefaultKeyStore 個の署名者
	<< 除去	
NodeDefaultKeyStore 個の個人証明書	追加 >>	CMSKeyStore 個の署名者
	<< 除去	default

適用 OK リセット 取り消し

6-4. マスター構成に保管します。

6-5. 更新したCMSKeyStore (plugin-key.kdb)の内容を、Webサーバー・プラグイン側の鍵データベースにコピーします。

<WAS_ROOT>/profiles/<profile_name>/config/cells/<cell_name>/nodes/<node_name>/servers/<webserver_name>/plugin-key.kdb を、Webサーバー・プラグインがあるノードの <plugin_install_root>/config/<web_server_name>/plugin-key.kdb にコピーします。

6-5. Webサーバーを再起動します。その後、8章に進みます。

7. Web サーバー・プラグイン用鍵データベースを更新(リモート構成)

Webサーバー・プラグインが使用する鍵データベース(plugin-key.kdb)に署名者証明書を追加します。ここではWebサーバーをリモート構成にしている環境が対象です。ローカル構成の場合は、8章に進みます。

7-1. 署名者証明書を抽出します。

管理コンソールから、「セキュリティ」 → 「SSL 証明書および鍵管理」 → 「エンドポイント・セキュリティ構成の管理」を開きます。ローカル・トポロジーにある「インバウンド」-<Cell 名>-「nodes」-<node 名> の図から、<node 名>をクリックします。「関連項目」にある「鍵ストアおよび証明書」をクリックします。「NodeDefaultKeyStore」をクリックし、「追加プロパティ」にある「個人証明書」をクリックします。

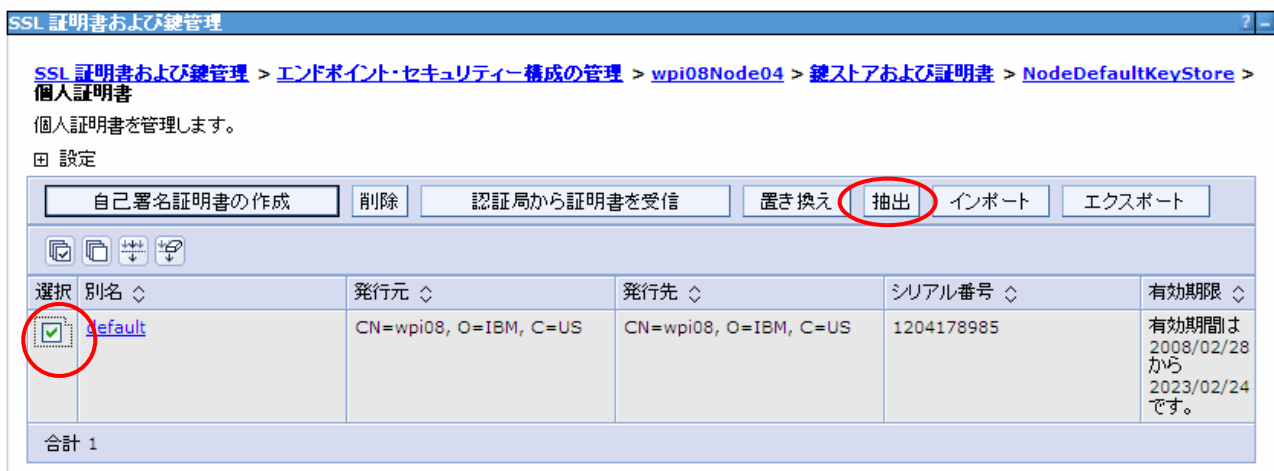


The screenshot shows the 'SSL 証明書および鍵管理' console. The breadcrumb path is: SSL 証明書および鍵管理 > エンドポイント・セキュリティ構成の管理 > wpi08Node04 > 鍵ストアおよび証明書. Below the breadcrumb, there is a description: '暗号方式、RACF(R)、CMS、Java(TM)、およびすべてのトラストストア・タイプを含む、鍵ストア・タイプを定義します。' and a '設定' button. There are three buttons: '新規作成', '削除', and '署名者の交換...'. Below these are icons for copy, paste, and refresh. A table lists three key stores:

選択	名前	パス
<input type="checkbox"/>	NodeDefaultKeyStore	\${CONFIG_ROOT}/cells/wpi08Node04Cell/nodes/wpi08Node04/key.p12
<input type="checkbox"/>	NodeDefaultTrustStore	\${CONFIG_ROOT}/cells/wpi08Node04Cell/nodes/wpi08Node04/trust.p12
<input type="checkbox"/>	NodeLTPAKeys	\${CONFIG_ROOT}/cells/wpi08Node04Cell/nodes/wpi08Node04/ltpa.jceks

At the bottom, it says '合計 3'. The 'NodeDefaultKeyStore' row is circled in red.

7-2. 個人証明書(ここでは「default」)にチェックを入れて、「抽出」ボタンをクリックします。



The screenshot shows the 'SSL 証明書および鍵管理' console. The breadcrumb path is: SSL 証明書および鍵管理 > エンドポイント・セキュリティ構成の管理 > wpi08Node04 > 鍵ストアおよび証明書 > NodeDefaultKeyStore > 個人証明書. Below the breadcrumb, there is a description: '個人証明書を管理します。' and a '設定' button. There are several buttons: '自己署名証明書の作成', '削除', '認証局から証明書を受信', '置き換え', '抽出', 'インポート', and 'エクスポート'. Below these are icons for copy, paste, and refresh. A table lists one certificate:

選択	別名	発行元	発行先	シリアル番号	有効期限
<input checked="" type="checkbox"/>	default	CN=wpi08, O=IBM, C=US	CN=wpi08, O=IBM, C=US	1204178985	有効期間は 2008/02/28 から 2023/02/24 です。

At the bottom, it says '合計 1'. The '抽出' button and the 'default' row are circled in red.

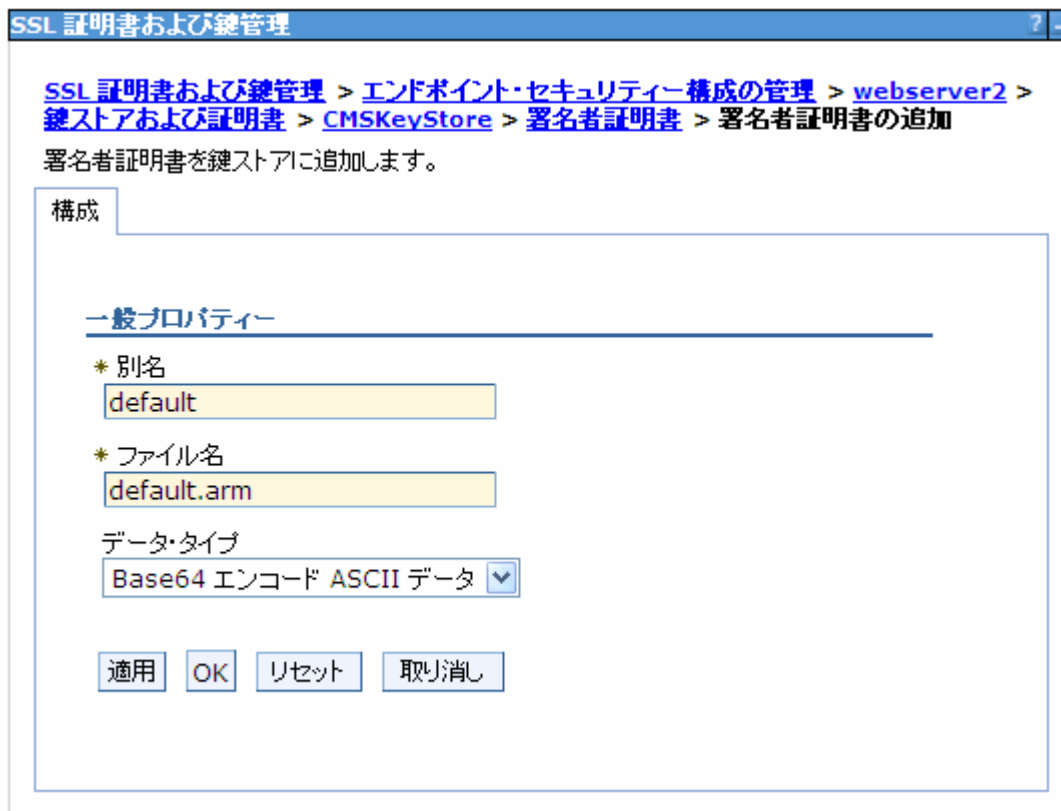
7-3. 証明書の抽出画面で、「証明書ファイル名」に任意のファイル名を指定し(ここでは「default.arm」)、「OK」ボタンをクリックします。これで<WAS_ROOT>/profiles/<profile_name>/etc に default.arm が生成されます。

7-4. 次に、取り出した署名者証明書を CMSKeyStore に追加します。

管理コンソールから「セキュリティ」→「SSL 証明書および鍵管理」→「エンドポイント・セキュリティ構成の管理」を開きます。ローカル・トポロジーを展開し、「インバウンド」- <Cell 名> - 「nodes」- <node 名> - 「servers」- <Web サーバー名> をクリックします。「関連項目」にある「鍵ストアおよび証明書」をクリックし、「CMSKeyStore」をクリックします。「追加プロパティ」から「署名者証明書」を選択し、「追加」ボタンをクリックします。

選択	別名	発行先	指紋 (SHA ダイジェスト)	有効期限
<input type="checkbox"/>	VeriSign Class 1 Public Primary Certification Authority	OU=Class 1 Public Primary Certification Authority, O="VeriSign, Inc.", C=US	90:AE:A2:69:85:FF:14:80:4C:43:49:52:EC:E9:60:84:77:AF:55:6F	有効期間は 1996/01/29 から 2028/08/02 です。
<input type="checkbox"/>	VeriSign Class 2 Public Primary Certification Authority	OU=Class 2 Public Primary Certification Authority, O="VeriSign, Inc.", C=US	67:82:AA:E0:ED:EE:E2:1A:58:39:D3:C0:CD:14:68:0A:4F:60:14:2A	有効期間は 1996/01/29 から 2028/08/02 です。

7-5. 「別名」に任意の名前(ここでは「default」)および「ファイル名」にソ先ほどの指定したファイル名(ここでは「default.arm」)を入力して「OK」ボタンをクリックします。



SSL 証明書および鍵管理 > エンドポイント・セキュリティ構成の管理 > webserver2 > 鍵ストアおよび証明書 > CMSKeyStore > 署名者証明書 > 署名者証明書の追加

署名者証明書を鍵ストアに追加します。

構成

一般プロパティ

* 別名
default

* ファイル名
default.arm

データタイプ
Base64 エンコード ASCII データ

適用 OK リセット 取り消し

これで CMSKeyStore に署名者証明書が追加されました。

7-6. 更新したCMSKeyStore (plugin-key.kdb)の内容を、Webサーバー・プラグイン側の鍵データベースにコピーします。

<WAS_ROOT>/profiles/<profile_name>/config/cells/<cell_name>/nodes/<node_name>/servers/<webserver_name>/plugin-key.kdb を、Webサーバー・プラグインがあるノードの <plugin_install_root>/config/<web_server_name>/plugin-key.kdb にコピーします。

7-7. Webサーバーを再起動します。

8. 管理セキュリティの有効化

8-1. 2章のステップにて、管理コンソールから管理セキュリティを無効にした場合は、元の設定に戻します。初めから管理セキュリティが無効になっている場合には、以下の作業は必要ありません。ここで終了となります。

管理コンソールから、「セキュリティ」→「管理、アプリケーション、およびインフラストラクチャーの保護」画面を開きます。「管理セキュリティ」のチェックボックスにチェックします。「アプリケーション・セキュリティ」「Java 2 セキュリティ」についても元の状態に戻してください。「適用」ボタンをクリックします。

セキュリティ構成ウィザード セキュリティ構成報告書

管理セキュリティ

管理セキュリティを使用可能にする

- [管理ユーザー・ロール](#)
- [管理グループ・ロール](#)

アプリケーション・セキュリティ

アプリケーション・セキュリティを使用可能にする

Java 2 セキュリティ

Java 2 セキュリティを使用してアプリケーションのアクセスをローカル・リソースに制限する

- アプリケーションがカスタム許可を認可されたときに警告する
- リソース認証データへのアクセスを制限する

ユーザー・アカウント・リポジトリ

現在のレルム定義
ローカル・オペレーティング・システム

使用可能なレルム定義
ローカル・オペレーティング・システム ▼ 構成 現在値として設定

適用

リセット

8-2. マスター構成に保管し、WAS を再起動します。

9. 管理クライアント用トラスト・ストアの更新

この手順は、管理セキュリティーを有効にしている場合にのみ必要です。

ここでは、管理クライアントが使用するトラスト・ストアに署名者証明書を追加します。

9-1. コマンド・プロンプトを起動し、<WAS_ROOT>/profiles/<profile_name>/bin に移動します。

9-2. serverStatus.sh (.bat) -all コマンドを実行します。

9-3. トラスト・ストアに署名者を追加しますか？(y/n) と聞かれるので、y を入力します。

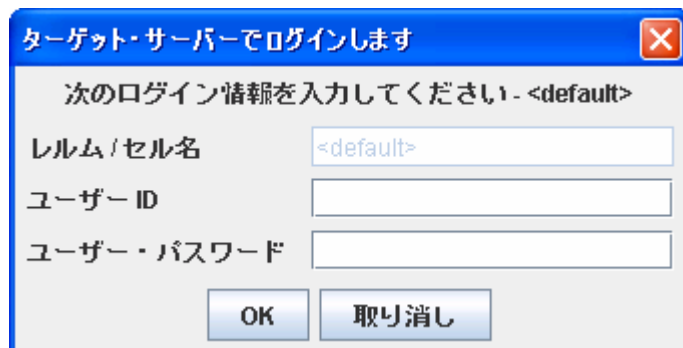
```
*** SSL 署名者交換プロンプト ***
ターゲット・ホスト wpi08 からの SSL 署名者が、トラスト・ストア c:/WebSphere/
AppServer/profiles/HaraSingle/etc/trust.p12 に見つかりません。

以下に署名者情報を示します（ダイジェスト値が、サーバーに表示された値に一致してい
ることを確認してください）：

対象 DN:    CN=wpi08, O=IBM, C=US
発行者 DN:  CN=wpi08, O=IBM, C=US
シリアル番号: 1204178985
有効期限:    Fri Feb 24 15:09:45 JST 2023
SHA-1 ダイジェスト:  E0:C1:C8:CB:1A:86:51:9D:A3:BE:EE:47:D9:00:AB:2F:8F:C7:04:1
MD5 ダイジェスト:    F7:CC:6F:69:B2:E6:12:B6:05:79:6B:40:C2:02:B2:DD

ここでトラスト・ストアに署名者を追加しますか？ (y/n) y
プロンプトの応答の待機中にソケットがタイムアウトになると、要求の再試行が必要な場
合があります。再試行が必要なときに、(y) を入力した場合、プロンプトが再表示されな
いことに注意してください。これは、署名者がすでにトラスト・ストアに追加されている
ことを示します。
```

9-4. 管理セキュリティーを有効にした場合は、コマンドの実行にユーザーID とパスワードが必要になります。serverStatus コマンドの実行時に以下のプロンプトが表示されましたら、ユーザーID とパスワードを入力してOK をクリックします。



この作業で、<WAS_ROOT>/profiles/<profile_name>/etc/trust.p12に、必要な署名者証明書が追加されまし
た。

以上で全ての作業が終了となります。正しくWebサーバーや管理クライアントと接続できるか確認してください。

<更新履歴>

- 2007年3月5日 V1.0公開
- 2007年3月10日 V1.1公開 手順6-1の誤字を修正(「NodeDefaultTrustStore」を「NodeDefaultKeyStore」に修正)