

WebSphere Application Server V6.1

自己署名証明書の置き換え手順

<ND 編>

V1.1

2009 年 2 月 20 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	6
4. ノード、セル(マスター)の自己署名証明書の再作成	12
5. 署名者証明書の追加	17
6. Web サーバー・プラグイン用鍵データベースを更新	20
7. 管理セキュリティーの有効化	25
8. 管理クライアント用トラスト・ストアの更新	27
9. 更新履歴	30

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Network Deployment エディション(Deployment Managerを使用する分散アプリケーション・サーバー環境)を対象としています。Baseエディション、およびExpressエディションで、スタンドアロン・アプリケーション・サーバー環境を構成されている場合には、置き換え手順書<Base/Express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、セル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。
- 7章. 管理セキュリティーを有効化します。
- 8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。**

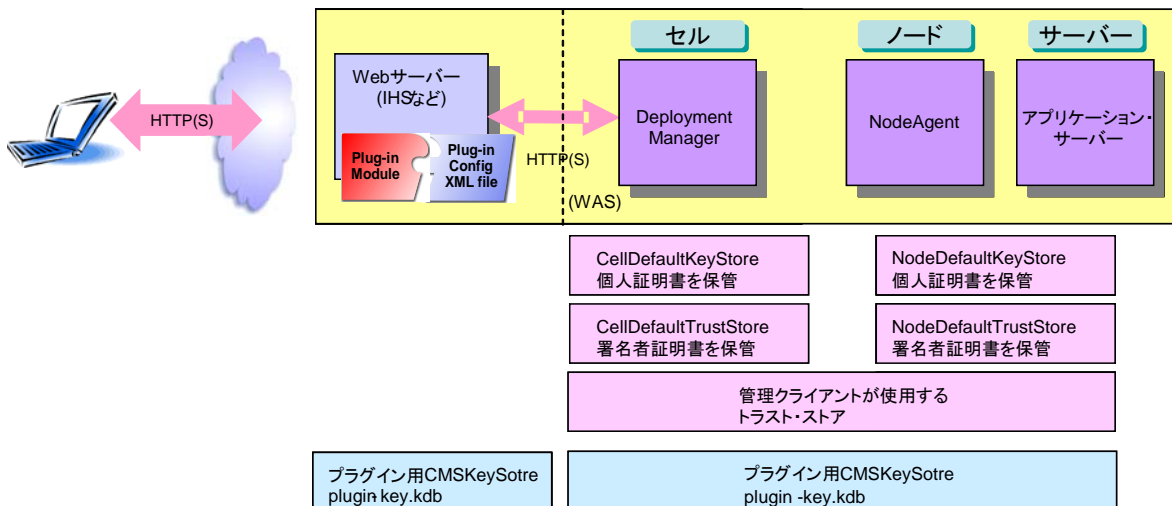
【参考】 証明書を保存する鍵ストアは、デフォルトでは以下の場所にある鍵ストアを使用します。

<WASが導入されているノードの鍵ストア>

- WASが使用するCellDefaultKeyStore (個人証明書を保管)
<WAS_ROOT>/profiles/<DM_profile_name>/config/cells/<cell_name>/key.p12
- WASが使用するCellDefaultTrustStore (署名者証明書を保管)
<WAS_ROOT>/profiles/<DM_profile_name>/config/cells/<cell_name>/trust.p12
- WASが使用するNodeDefaultKeyStore (個人証明書を保管)
<WAS_ROOT>/profiles/<Node_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/<Node_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/<Node_profile_name>/config/cells/<cell_name>/nodes/<node_name>/servers/<webserver_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



CellDefaultKeyStore, CellDefaultTrustStore, 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 通信が使用されます。

ノード

ノード

このページを使用して、アプリケーション・サーバー環境でのノードを管理します。ノードは、固有の IP ホスト・アドレスを持つ物理コンピュータです。以下の表に、このセル内の管理対象および非管理対象ノードがリストされています。最初のノードが「デプロイメント・マネージ追加」をクリックして、セルおよびこのリストに新規ノードを追加します。

設定

ノードの追加 ノードの除去 強制削除 **同期化** 完全な再同期 停止

選択	名前 	バージョン 	ディスカバリー・プロトコル 	状況 
<input type="checkbox"/>	TrustTestDMNode	ND 6.1.0.11	TCP	
<input type="checkbox"/>	TrustTestNode01	ND 6.1.0.11	TCP	
<input type="checkbox"/>	TrustTestNode02	ND 6.1.0.11	TCP	

合計 3

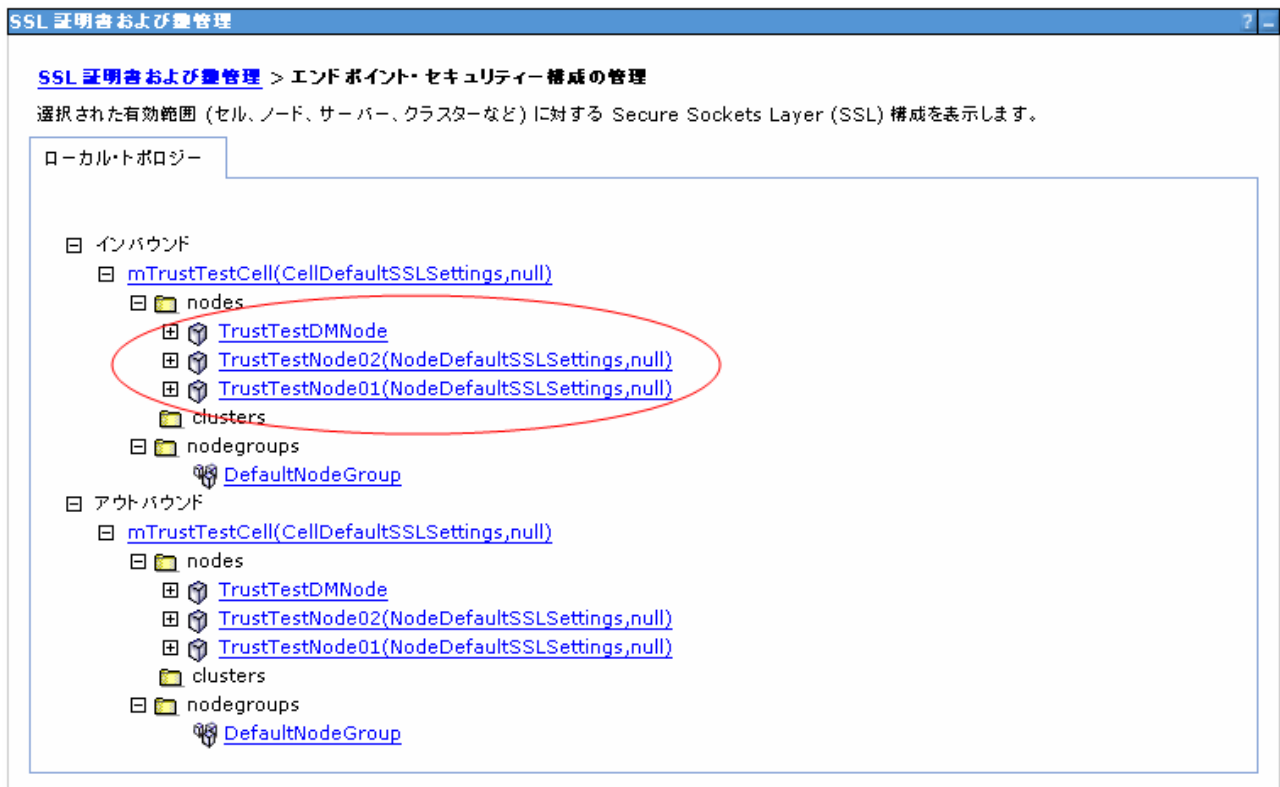
同期されていない場合は、この画面にて、確実に同期化させてください。

3. 自己署名証明書の削除

管理コンソールから、以下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
- セル(マスター)の鍵ストアにある個人証明書
- セル(マスター)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

【注】セル内にDM以外のノードが複数存在する場合には、「ノードの鍵ストアにある個人証明書」と、「ノードのトラスト・ストアにある署名者証明書」の削除は、ノード毎に行ってください。以下の図は、Cell に 2 つのノードが統合されている状態の、「管理コンソール」 → 「セキュリティー」 → 「SSL 証明書および鍵管理」 → 「エンドポイント・セキュリティー構成の管理」で表示される例です。



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、「セキュリティー」 → 「SSL 証明書および鍵管理」 → 「エンドポイント・セキュリティー構成の管理」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、「追加プロパティー」にある「個人証明書」をクリックします。

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 > TrustTestNode02 > 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=minny, O=IBM, C=US	CN=minny, O=IBM, C=US	1203474676	有効期間は 2008/02/20 から 2023/02/16 です。

合計 1

マスター構成に保管後、同期化してください。

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> (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。「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。

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 > TrustTestNode02 > 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	発行先	指紋 (SHA ダイジェスト)	有効期限
<input checked="" type="checkbox"/>	default	CN=minny, O=IBM, C=US	54:EE:C5:1E:82:DC:85:B8:3C:17:93:9A:CB:19:70:7E:08:1F:9A:86	有効期間は 2008/02/20 から 2023/02/16 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"/>	dummyserversigner	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。
<input checked="" type="checkbox"/>	default_1	CN=minny, O=IBM, C=US	89:9E:4F:52:BF:EC:FC:E7:DF:68:94:74:8D:47:A0:DE:BB:DB:EA:20	有効期間は 2008/02/20 から 2023/02/16 です。

合計 4

マスター構成に保管後、同期化してください。

3-3. セル(マスター)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>(CellDefaultSSLSettings,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。「CellDefaultKeyStore」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。

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 > mTrustTestCell > 鍵ストアおよび証明書 > CellDefaultKeyStore > 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
<input checked="" type="checkbox"/>	default	CN=minny, O=IBM, C=US	CN=minny, O=IBM, C=US	1203474089	有効期間は 2008/02/20 から 2023/02/16 です。

合計 1

マスター構成に保管後、同期化してください。

3-4. セル(マスター)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>(CellDefaultSSLSettings,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。「CellDefaultTrustStore」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。

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 > mTrustTestCell > 鍵ストアおよび証明書 > CellDefaultTrustStore > 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	発行先	指紋 (SHA ダイジェスト)	有効期限
<input checked="" type="checkbox"/>	default	CN=minny, O=IBM, C=US	89:9E:4F:52:BF:EC:FC:E7:DF:68:94:74:8D:47:A0:DE:BB:DB:EA:20	有効期間は 2008/02/20 から 2023/02/16 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"/>	dummyserversigner	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。
<input checked="" type="checkbox"/>	default_2	CN=minny, O=IBM, C=US	54:EE:C5:1E:82:DC:85:B8:3C:17:93:9A:CB:19:70:7E:08:1F:9A:86	有効期間は 2008/02/20 から 2023/02/16 です。
<input checked="" type="checkbox"/>	default_1	CN=minny, O=IBM, C=US	D2:CF:8D:7C:BE:A4:E8:07:0D:31:AD:13:4E:A4:89:70:71:9F:C8:BA	有効期間は 2008/02/20 から 2023/02/16 です。

合計 5

マスター構成に保管後、同期化してください。

3-5. Web サーバー・プラグインが使用する鍵データベース CMSKeyStore (plugin-key.kdb) の個人証明書を削除します。

【注】 default という名前で始まる証明書が存在しない場合、3-6 証明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。

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 > webserver01 > 鍵ストアおよび証明書 > CMSKeyStore > 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=minny, O=IBM, C=US	CN=minny, O=IBM, C=US	1203474676	有効期間は 2008/02/20 から 2023/02/16 です。

合計 1

マスター構成に保管後、同期化してください。

3-6. Web サーバー・プラグインが使用する鍵データベース CMSKeyStore (plugin-key.kdb) の署名者証明書を削除します。

【注】 default という名前で始まる署名者証明書が存在しない場合、次の手順に進んでください。

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「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後、同期化してください。

4. ノード、セル(マスター)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。

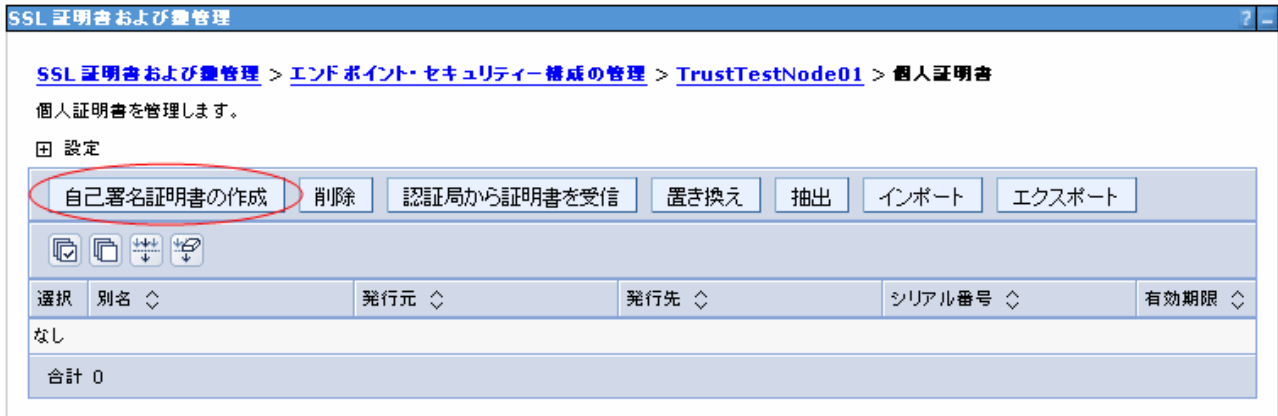
4-1. ノードの自己署名証明書を再作成します。

【注】セル内に DM 以外のノードが複数存在する場合には、「自己署名証明書の再作成」は、ノード毎に行ってください

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> (NodeDefaultSSLSettings,null と書かれているもの) 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。

The screenshot shows a configuration page for a node. The page is titled '構成' (Configuration) and has a sub-section '一般プロパティ' (General Properties). Under this section, there are two input fields: '名前' (Name) with the value 'TrustTestNode01' and '方向' (Direction) with the value 'インバウンド' (Inbound). Below this is a section '継承された SSL 構成' (Inherited SSL Configuration) with two input fields: '継承された SSL 構成名' (Inherited SSL Configuration Name) with the value 'CellDefaultSSLSettings' and '継承された証明書別名' (Inherited Certificate Alias) with the value 'null'. The bottom section is 'このエンドポイントの特定 SSL 構成' (Specific SSL Configuration for this Endpoint). It has a checked checkbox '継承された値のオーバーライド' (Override inherited values). Below this are three dropdown menus: 'SSL 構成' (SSL Configuration) with the value 'NodeDefaultSSLSettings', '証明書別名リストの更新' (Update Certificate Alias List), and '鍵ストアの証明書別名' (Certificate Alias in Key Store) with the value '(なし)' (None). The '証明書別名リストの更新' and '証明書の管理' (Certificate Management) buttons are highlighted with a red circle.

4-2. 「自己署名証明書の作成」ボタンをクリックします。



4-3. 構成のタブで以下の値を入力した後、「OK」ボタンを押し、マスター構成に保管後、同期化してください。

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 日間 (任意の期間で構いませんが、デフォルトが 365 日間 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

バージョン

鍵サイズ
 ビット

* 共通名

* 有効期間
 日間

* 組織

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 > TrustTestNode01 > 個人証明書 > default

個人証明書を管理します。

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

シリアル番号
1203491937

有効期間
有効期間は 2008/02/20 から 2023/02/16 です。

発行先
CN=minny, OU=, O=IBM, L=, ST=, POSTALCODE=, C=US

発行元
CN=minny, OU=, O=IBM, L=, ST=, POSTALCODE=, C=US

指紋 (SHA ダイジェスト)
E5:3E:72:C0:FE:86:25:97:DD:7B:CD:38:26:7E:9D:64:2A:E5:78:FD

署名アルゴリズム
SHA1withRSA(1.2.840.113549.1.1.5)

戻る

作成された証明書の確認画面

4-4. セル(マスター)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>(CellDefaultSSLSettings,null と書かれているもの) 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。

選択された有効範囲（セル、ノード、サーバー、クラスターなど）に対する Secure Sockets Layer (SSL)

構成

一般プロパティ

名前

mTrustTestCell

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

CellDefaultSSLSettings

証明書別名リストの更新

証明書の管理

継ストアの証明書別名

(なし)

4-5. 「自己署名証明書の作成」ボタンをクリックします。

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 ◇

なし

合計 0

4-6. 構成のタブで以下の値を入力した後、「OK」ボタンを押し、マスター構成に保管後、同期化してください。

別名: default（任意の名前で構いません）

共通名: <上記手順 3-3 で CN= としてメモした値>

有効期間: 5475 日間（任意の期間で構いませんが、デフォルトが 365 日間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

バージョン

鍵サイズ
 ビット

* 共通名

* 有効期間
 日間

* 組織

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 > mTrustTestCell > 個人証明書 > default

個人証明書を管理します。

構成

一般プロパティ

別名

バージョン

鍵サイズ
 ビット

シリアル番号

有効期間

発行先

発行元

指紋 (SHA ダイジェスト)

署名アルゴリズム

作成された証明書の確認画面

5. 署名者証明書の追加

NodeDefaultTrustStore、CellDefaultTrustStore に署名者証明書を追加します。

5-1. CellDefaultKeyStore と CellDefaultTrustStore の署名者を交換します。

5-1-1. 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> (CellDefaultSSLSettings,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。「CellDefaultKeyStore」と「CellDefaultTrustStore」を選択し、「署名者の交換...」ボタンをクリックします。



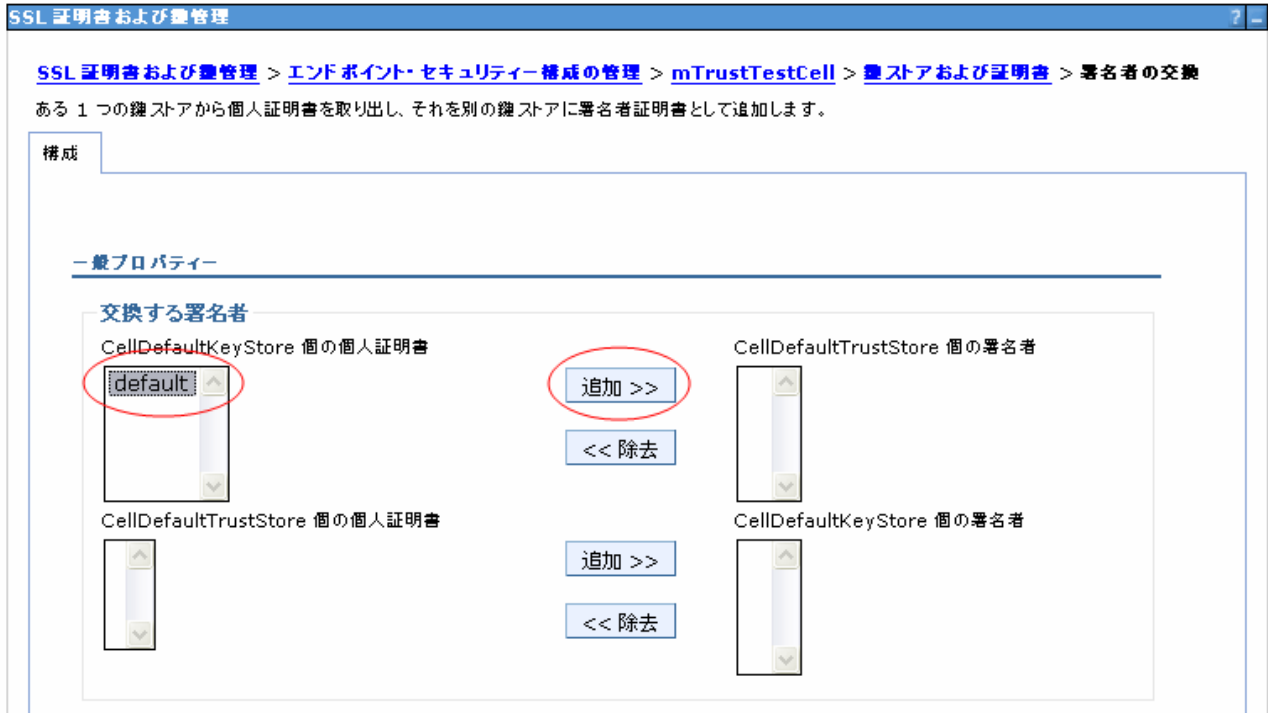
The screenshot shows the 'SSL 証明書および鍵管理' (SSL Certificate and Key Management) console. The breadcrumb navigation is 'SSL 証明書および鍵管理 > エンドポイント・セキュリティ構成の管理 > mTrustTestCell > 鍵ストアおよび証明書'. Below the breadcrumb, there is a description: '暗号方式、RACF(R)、CMS、Java(TM)、およびすべてのトラストストア・タイプを含む、鍵ストア・タイプを定義します。' and a '設定' (Settings) section. The '設定' section contains three buttons: '新規作成' (New), '削除' (Delete), and '署名者の交換...' (Signer Exchange...), with the latter being circled in red. Below the buttons are several icons for file operations. A table lists the key stores:

選択	名前	パス	リモート側で管理	ホスト・リスト
<input checked="" type="checkbox"/>	CellDefaultKeyStore	\${CONFIG_ROOT}/cells/mTrustTestCell/key.p12	false	
<input checked="" type="checkbox"/>	CellDefaultTrustStore	\${CONFIG_ROOT}/cells/mTrustTestCell/trust.p12	false	
<input type="checkbox"/>	CellLTPAKeys	\${CONFIG_ROOT}/cells/mTrustTestCell/ltpa.jceks	false	

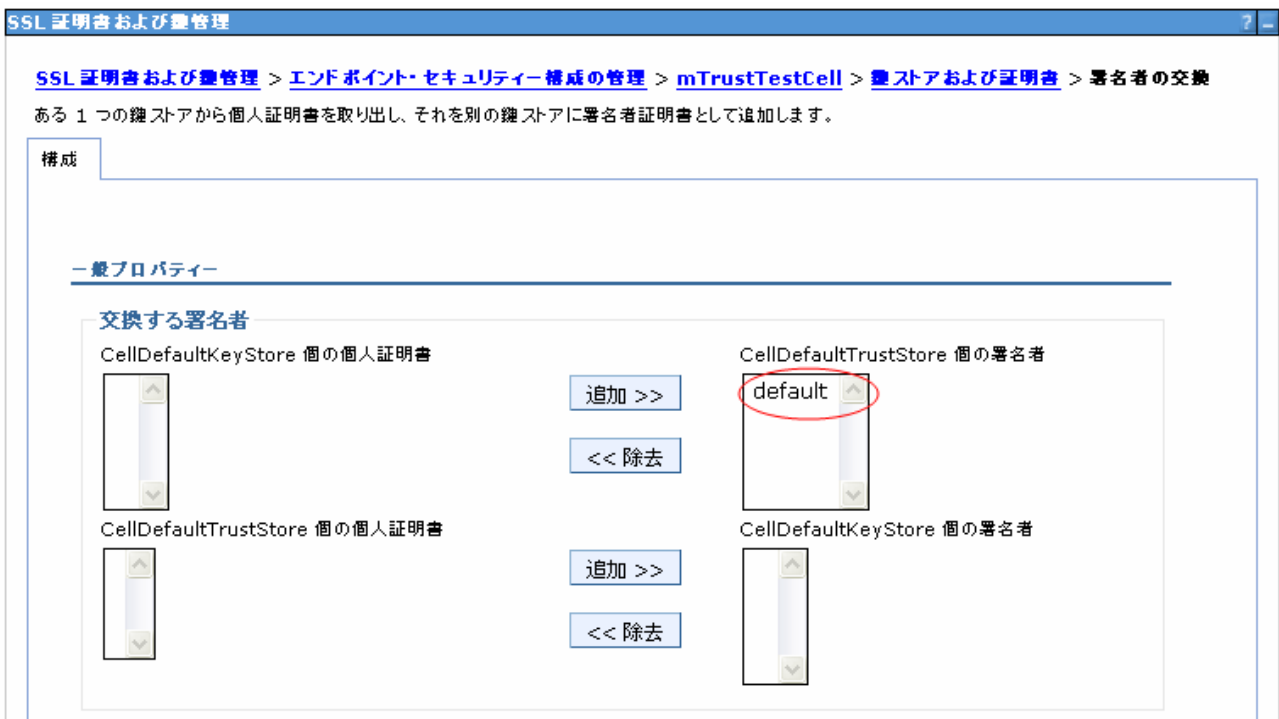
At the bottom of the table, it says '合計 3' (Total 3).

5-1-2. 署名者証明書に追加します。

「CellDefaultKeyStore」の、上記手順 4-4、4-5、4-6 で作成した、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。



5-1-3. 「CellDefaultTrustStore」に、新規作成した自己署名証明書が追加されたら、OK ボタンをクリックし、マスター構成に保管後、同期化してください。



5-2. NodeDefaultKeyStore と NodeDefaultTrustStore の署名者を交換します。

【注】 セル内に DM 以外のノードが複数存在する場合には、「NodeDefaultKeyStore と

NodeDefaultTrustStore の署名者を交換」は、ノード毎に行ってください。

5-2-1. 管理コンソールから「セキュリティー」 → 「SSL 証明書および鍵管理」 → 「エンドポイント・セキュリティー構成の管理」を開きます。ローカル・トポロジーを展開し、「インバウンド」 - <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」と「NodeDefaultTrustStore」を選択し、「署名者の交換...」ボタンをクリックします。

5-2-2. 5-1-2 以降の手順と同様に、署名者証明書の追加を行います。

5-3. CellDefaultKeyStore と NodeDefaultTrustStore の署名者を交換します。

【注】 セル内に DM 以外のノードが複数存在する場合には、「CellDefaultKeyStore と NodeDefaultTrustStore の署名者を交換」は、ノード毎に行ってください。

5-3-1. 管理コンソールから、「セキュリティー」 → 「SSL 証明書および鍵管理」 → 「エンドポイント・セキュリティー構成の管理」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。「CellDefaultKeyStore」と「NodeDefaultTrustStore」を選択し、「署名者の交換...」ボタンをクリックします。

5-3-2. 5-1-2 以降の手順と同様に、署名者証明書の追加を行います。

5-4. NodeDefaultKeyStore と CellDefaultTrustStore の署名者を交換します。

【注】 セル内に DM 以外のノードが複数存在する場合には、「NodeDefaultKeyStore と CellDefaultTrustStore の署名者を交換」は、ノード毎に行ってください。

5-4-1. 管理コンソールから、「セキュリティー」 → 「SSL 証明書および鍵管理」 → 「エンドポイント・セキュリティー構成の管理」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」と「CellDefaultTrustStore」を選択し、「署名者の交換...」ボタンをクリックします。

5-4-2. 5-1-2 以降の手順と同様に、署名者証明書の追加を行います。

6. Web サーバー・プラグイン用鍵データベースを更新

次に、Webサーバー・プラグインが使用する鍵データベースCMSKeyStore (plugin-key.kdb) に署名者証明書を追加します。

Web サーバーを管理しているノードが、管理対象ノードで、そのノードの NodeDefaultKeyStore と、CMSKeyStore の署名者を交換する場合は、6-1 を、

Webサーバーが非管理対象ノードに属している場合など、Webサーバーを管理していないノードとの署名者の交換を行う場合は、手順6-2を行ってください。

【注】 Plugin がアプリケーション・サーバーと SSL 通信を行うためには、割り振り先サーバーの署名者証明書が、CMSKeyStore に含まれている必要がございます。セルが複数のノードで構成されている場合には、すべてのノードの署名者証明書を、CMSKeyStore に取り込んでください。

【注】 CMSKeyStore に、すべてのノードの署名者証明書をとり込み後、手順 6-3 を必ず行ってください。

6-1. Web サーバーを管理しているノードの NodeDefaultKeyStore と Web サーバーが使用する CMSKeyStore の署名者を交換します。

6-1-1. 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 > エンドポイント・セキュリティ構成の管理 > webserver01 > 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

<input type="button" value="新規作成"/> <input type="button" value="削除"/> <input type="button" value="署名者の交換..."/>		
選択	名前	パス
<input checked="" type="checkbox"/>	CMSKeyStore	C:\IBM\WebSphere\AppServer6.1ND\profiles\TrustTestDmgr\config/cells/n
<input type="checkbox"/>	CellDefaultKeyStore	\${CONFIG_ROOT}/cells/mTrustTestCell/key.p12
<input type="checkbox"/>	CellDefaultTrustStore	\${CONFIG_ROOT}/cells/mTrustTestCell/trust.p12
<input type="checkbox"/>	CellLTPAKeys	\${CONFIG_ROOT}/cells/mTrustTestCell/ltpa.jceks
<input checked="" type="checkbox"/>	NodeDefaultKeyStore	\${CONFIG_ROOT}/cells/mTrustTestCell/nodes/TrustTestNode01/key.p12
<input type="checkbox"/>	NodeDefaultTrustStore	\${CONFIG_ROOT}/cells/mTrustTestCell/nodes/TrustTestNode01/trust.p12
合計 6		

6-1-2. CMSKeyStore に署名者証明書を追加します。

「NodeDefaultKeyStore」の、上記手順 4-1、4-2、4-3 で作成した、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。

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 > webserver01 > 鍵ストアおよび証明書 > 署名者の交換

ある 1 つの鍵ストアから個人証明書を取り出し、それを別の鍵ストアに署名者証明書として追加します。

構成

一般プロパティ

交換する署名者

CMSKeyStore 個の個人証明書

追加 >>

<< 除去

NodeDefaultKeyStore 個の署名者

NodeDefaultKeyStore 個の個人証明書

追加 >>

<< 除去

CMSKeyStore 個の署名者

6-1-3. 「CMSKeyStore」に「default」が追加されたら、OK ボタンをクリックし、マスター構成に保管後、同期化してください。

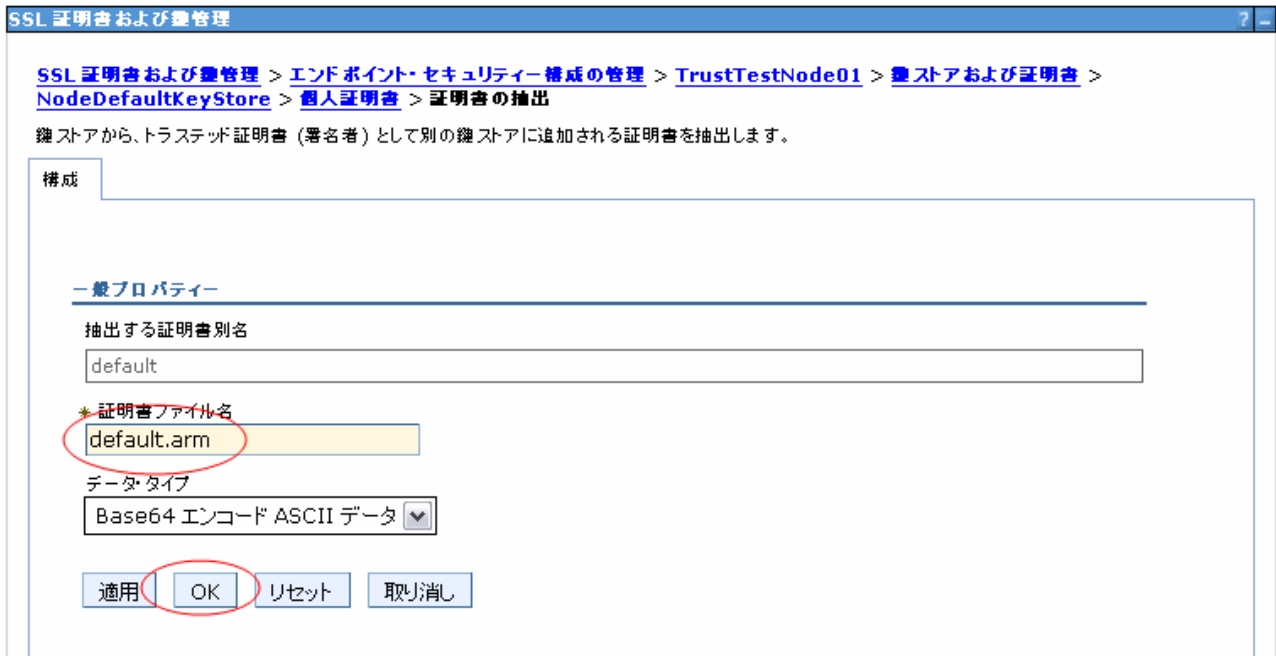


6-2. Web サーバーが非管理対象ノードに属している場合など、Web サーバーを管理していないノードとの署名者の交換を行います。

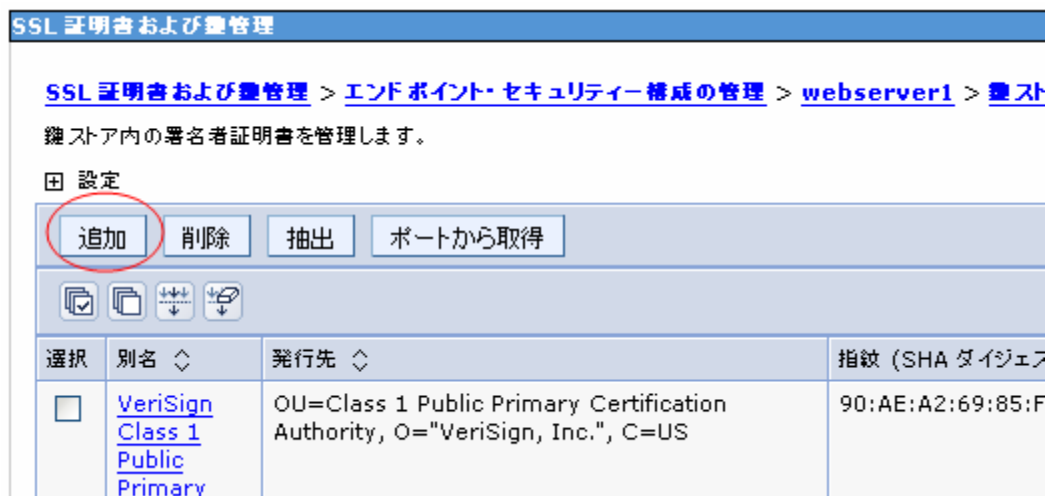
6-2-1. 管理コンソールから「セキュリティ」→「SSL 証明書および鍵管理」→「エンドポイント・セキュリティ構成の管理」を開きます。ローカル・トポロジーを展開し、「インバウンド」 - <Cell 名> - 「nodes」 - <node 名> をクリックします。「関連項目」にある「鍵ストアおよび証明書」をクリックします。「NodeDefaultKeyStore」をクリックし、「追加プロパティ」にある「個人証明書」をクリックします。個人証明書(ここでは「default」)にチェックを入れて、「抽出」ボタンをクリックします。



6-2-2. 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/<DM_profile_name>/etc に default.arm が生成されます。



6-2-3. 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」をクリックします。「CMSKeyStore」をクリックし、「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。



6-2-4. 「別名」に、任意の名前(ここでは「default」)および、「ファイル名」に、先ほどの指定したファイル名(こ

では default.arm))を入力して「OK」ボタンをクリックし、マスター構成に保管後、同期化してください。

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 > 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。

6-3-1. 更新したCMSKeyStore(plugin-key.kdb)を、Webサーバー・プラグイン鍵ストア・ディレクトリーにコピーします。

管理コンソールから「サーバー」 → 「Webサーバー」 → <Webサーバー名> を開き「追加プロパティ」のプラグイン・プロパティをクリックします。

「Web サーバー・プラグイン・ファイルの Web サーバー・コピー」内の「プラグイン鍵ストア・ディレクトリーおよびファイル名」に指定されている、プラグインが導入されているノードのロケーションに、<WAS_ROOT>/profiles/<profile_name>/config/cells/<cell_name>/nodes/<node_name>/servers/<webserver_name>/plugin-key.kdb をコピーします。

Webサーバー・プラグイン・ファイルの Web サーバー・コピー:

* プラグイン構成ディレクトリー およびファイル名
C:\IBM\IHS6.1\Plugin:

* プラグイン鍵ストア・ディレクトリー およびファイル名
C:\IBM\IHS6.1\Plugin:

6-3-2. Webサーバーを再起動します。

7-2. マスター構成に保管後に、各ノードと同期化されていることを確認したら、管理コンソールからログアウトし、DeploymentManager、NodeAgent を停止します。

停止する前に、管理コンソールから、「システム管理」 → 「ノード」画面を開き、各ノードが同期化されている事を確認してください。

ノード

ノード

このページを使用して、アプリケーション・サーバー環境でのノードを管理します。ノードは、固有の IP ホスト・アドレスを持つ物理コンピュータです。以下の表に、このセル内の管理対象および非管理対象ノードがリストされています。最初のノードがデプロイメント・マネージ追加をクリックして、セルおよびこのリストに新規ノードを追加します。

田 設定

ノードの追加 ノードの除去 強制削除 **同期化** 完全な再同期 停止

📄 📄 📄 📄

選択	名前	バージョン	ディスカバリー・プロトコル	状況
<input type="checkbox"/>	TrustTestDMNode	ND 6.1.0.11	TCP	↔
<input type="checkbox"/>	TrustTestNode01	ND 6.1.0.11	TCP	↔
<input type="checkbox"/>	TrustTestNode02	ND 6.1.0.11	TCP	↔

合計 3

同期されていない場合は、この画面にて、確実に同期化させてください。

8. 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。

8-1. DeploymentManager を起動します。NodeAgent が起動している場合、停止してください。

8-2. コマンド・プロンプトを起動し、<WAS_ROOT>/profiles/<DM_profile_name>/bin に移動します。

8-3. serverStatus.sh (.bat) -all コマンドを実行します。

8-4. 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 minny からの SSL 署名者が、トラスト・ストア C:/IBM/WebSphere/
AppServer6.1ND/profiles/TrustTestDmgr/etc/trust.p12 に見つかりません。

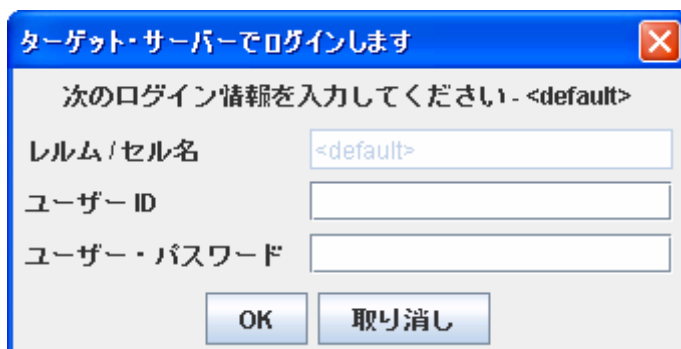
以下に署名者情報を示します（ダイジェスト値が、サーバーに表示された値に一致してい
ることを確認してください）：

対象 DN:      CN=minny, OU=, O=IBM, L=, ST=, POSTALCODE=, C=US
発行者 DN:    CN=minny, OU=, O=IBM, L=, ST=, POSTALCODE=, C=US
シリアル番号: 1203492880
有効期限:     Thu Feb 16 16:34:40 JST 2023
SHA-1 ダイジェスト: 15:95:46:1C:25:EC:F0:32:66:E2:66:85:65:82:DF:66:7E:51:DE:29
MD5 ダイジェスト:  0C:17:AE:69:92:15:CC:AC:77:4B:D3:BA:F6:74:93:DA

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。
```

8-5. 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/<DM_profile_name>/etc/trust.p12に、CellDefaultKeyStoreの必要な署名者証明書が追加されました。

8-6. コマンド・プロンプトを起動し、<WAS_ROOT>/profiles/<Node_profile_name>/bin に移動します。

【注】セル内に DM 以外のノードが複数存在する場合には、8-6～8-9 の作業は、ノード毎に行ってください。

8-7. syncNode.sh (.bat) DM_Host_Name DM_SOAP_PORT コマンドを実行します。

8-8. 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 localhost からの SSL 署名者が、トラスト・ストア C:/IBM/WebSphere/AppServer6.1ND/profiles/TrustTestCustom02/etc/trust.p12 に見つかりません。

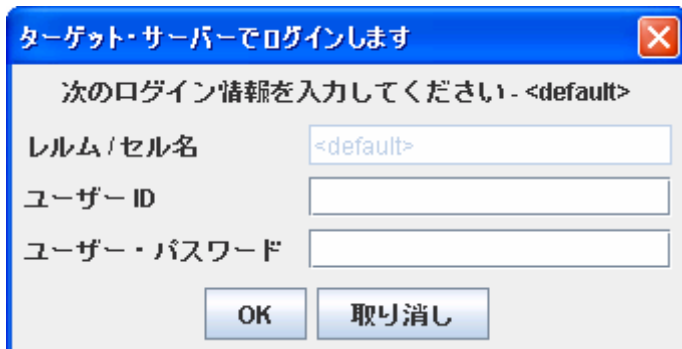
以下に署名者情報を示します（ダイジェスト値が、サーバーに表示された値に一致していることを確認してください）：

対象 DN: CN=minny, OU=, O=IBM, L=, ST=, POSTALCODE=, C=US
発行者 DN: CN=minny, OU=, O=IBM, L=, ST=, POSTALCODE=, C=US
シリアル番号: 1203492880
有効期限: Thu Feb 16 16:34:40 JST 2023
SHA-1 ダイジェスト: 15:95:46:1C:25:EC:F0:32:66:E2:66:85:65:82:DF:66:7E:51:DE:29
MD5 ダイジェスト: 0C:17:AE:69:92:15:CC:AC:77:4B:D3:BA:F6:74:93:DA

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。
```

8-9. 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。

syncNode 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/<Node_profile_name>/etc/trust.p12に、CellDefaultKeyStoreの必要な署名者証明書が追加されました。

8-10. nodeAgent を起動します。

【注】セル内に DM 以外のノードが複数存在する場合には、8-10～8-14 の作業は、ノード毎に行ってください。

8-11. コマンド・プロンプトを起動し、<WAS_ROOT>/profiles/<Node_profile_name>/bin に移動します。

8-12. serverStatus.sh (.bat) -all コマンドを実行します。

8-13. 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。

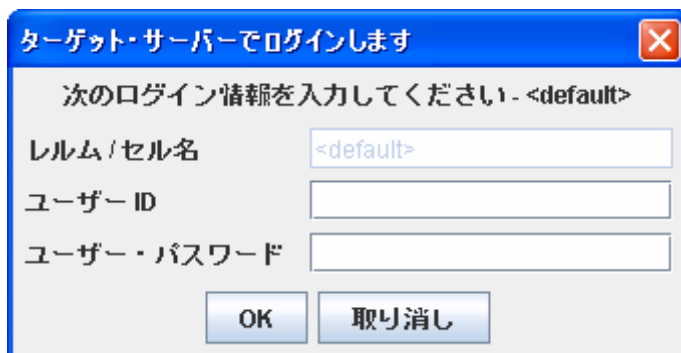
```
*** SSL 署名者交換プロンプト ***
ターゲット・ホスト minny からの SSL 署名者が、トラスト・ストア C:/IBM/WebSphere/
AppServer6.1ND/profiles/TrustTestCustom02/etc/trust.p12 に見つかりません。

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=minny, OU=, O=IBM, L=, ST=, POSTALCODE=, C=US
発行者 DN: CN=minny, OU=, O=IBM, L=, ST=, POSTALCODE=, C=US
シリアル番号: 1203492537
有効期限:   Thu Feb 16 16:28:57 JST 2023
SHA-1 ダイジェスト: 59:E5:5A:08:98:CD:5E:11:49:2E:85:0C:77:20:9F:CE:0E:E8:AA:6D
MD5 ダイジェスト:   E3:5A:8A:0A:87:A0:28:E7:9C:65:81:32:43:97:7D:82

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。
```

8-14. 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/<Node_profile_name>/etc/trust.p12に、NodeDefaultKeyStore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。

9. 更新履歴

・2008/3/3

・初版リリース

・2009/2/20

・手順「5-4」を追加

・タイトル「9.更新履歴」を追加