

WebSphere Application Server V7.0 Network Deployment

チェーン証明書の置き換え手順

V1.4

2009 年 10 月
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. 既存のチェーン証明書の確認	6
4. ノード、セル(マスター)のチェーン証明書の作成	9
5. 古い証明書の削除	17
6. 署名者証明書の追加	23
7. Web サーバー・プラグイン用鍵データベースを更新	30
8. 管理セキュリティーの有効化	35

1. はじめに

WAS V7.0では、製品導入後のプロファイル作成時に自動的に個人証明書(チェーン証明書)が作成され、管理セキュリティを有効にした場合に使用されます。このチェーン証明書は、デフォルトでは1年の有効期限を持ちますが、プロファイル作成時に管理者が1年～15年の有効期限を指定することができます。

WAS V7.0では、証明書の有効期限をモニターし、期限が切れる証明書を自動的に新しい証明書で上書きする機能を提供しています。ただし、Network Deployment エディションのセル環境で、Deployment ManagerとNode Agent間の自動同期を無効にした環境では(デフォルト有効)、Node Agent側のチェーン証明書が更新されず、有効期限が切れた後に、Deployment ManagerとNode Agentが通信できなくなる問題が発生します。この問題の発生条件および回避策・対応策については、以下の技術速報(フラッシュ)をご参照ください。

【考慮事項】WAS ND V7.0 証明書自動更新機能について (WAS-09-024)

<http://www.ibm.com/jp/domino01/mkt/cnpages1.nsf/page/default-0007F8D1>

本ガイドでは、この問題の回避策の1つである、より長い有効期限を持つチェーン証明書を作成し、置き換える手順をご紹介します。

本ガイドは、WAS V7.0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。

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、管理セキュリティを無効化します。
- 3章. 有効期限が1年で作成されたチェーン証明書を確認します。
- 4章. 有効期限のより長いチェーン証明書を作成します。
- 5章. 有効期限が1年で作成された証明書を削除します。
- 6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。
- 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。
- 8章. 管理セキュリティを有効化します。

<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。**

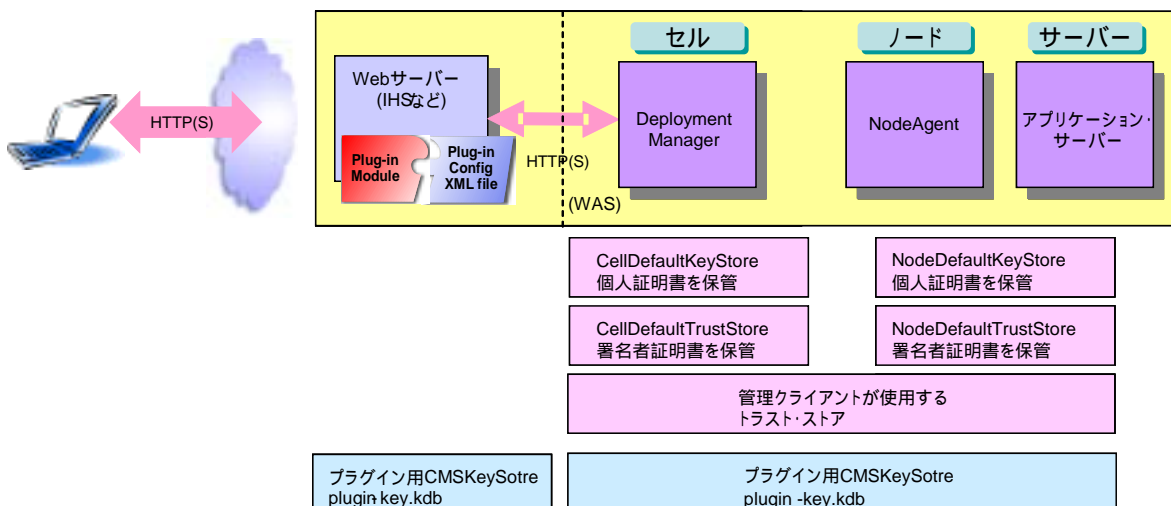
【参考】 証明書を保存する鍵ストアは、デフォルトでは以下の場所にある鍵ストアを使用します。

< 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。

2. 証明書更新の準備(セキュリティを無効化)

管理セキュリティを使用している場合は無効化します。管理セキュリティ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. 管理セキュリティを無効化します。

管理コンソールから、「セキュリティ」 「グローバル・セキュリティ」画面を開き、「管理セキュリティ」と「Java 2 セキュリティ」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、管理セキュリティを無効にした場合、アプリケーション・セキュリティも自動的に無効となります。)

管理セキュリティ、アプリケーション・セキュリティ、Java 2 セキュリティ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、元のセキュリティ設定に戻す必要があります。

グローバル・セキュリティ

グローバル・セキュリティ

このパネルを使用して、管理およびデフォルト・アプリケーション・セキュリティ・ポリシーを構成します。機能のセキュリティ・ポリシーに適用され、ユーザー・アプリケーションのデフォルト・セキュリティ・ドメインを定義して、ユーザー・アプリケーションのセキュリティ・ポリシーをオーバーライドしてカスタム

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
- 管理認証

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

2-2. 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、ApplicationServer を停止し、DeploymentManager、NodeAgent を再起動します。

ApplicationServer は、作業中は停止し、更新作業が終わりましたら、必要に応じて再起動してください。また、再起動を行う前に、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

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 アドレスを持つ物理コンピュータシステムに対応します。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ャーです。「ノードの追加」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 詳細削除 **同期化** 完全な再同期 停止

選択	名前	ホスト名	バージョン	ディスクリムーブプロトコル	状況
	NOGU061CellManager01	NOGU061.dhcp.makuhari.japan.ibm.com	ND 7.0.0.1	TCP	🔄
<input type="checkbox"/>	NOGU061Node01	NOGU061.dhcp.makuhari.japan.ibm.com	ND 7.0.0.1	TCP	🔄
<input type="checkbox"/>	NOGU061Node02	NOGU061.dhcp.makuhari.japan.ibm.com	ND 7.0.0.1	TCP	🔄

合計 3

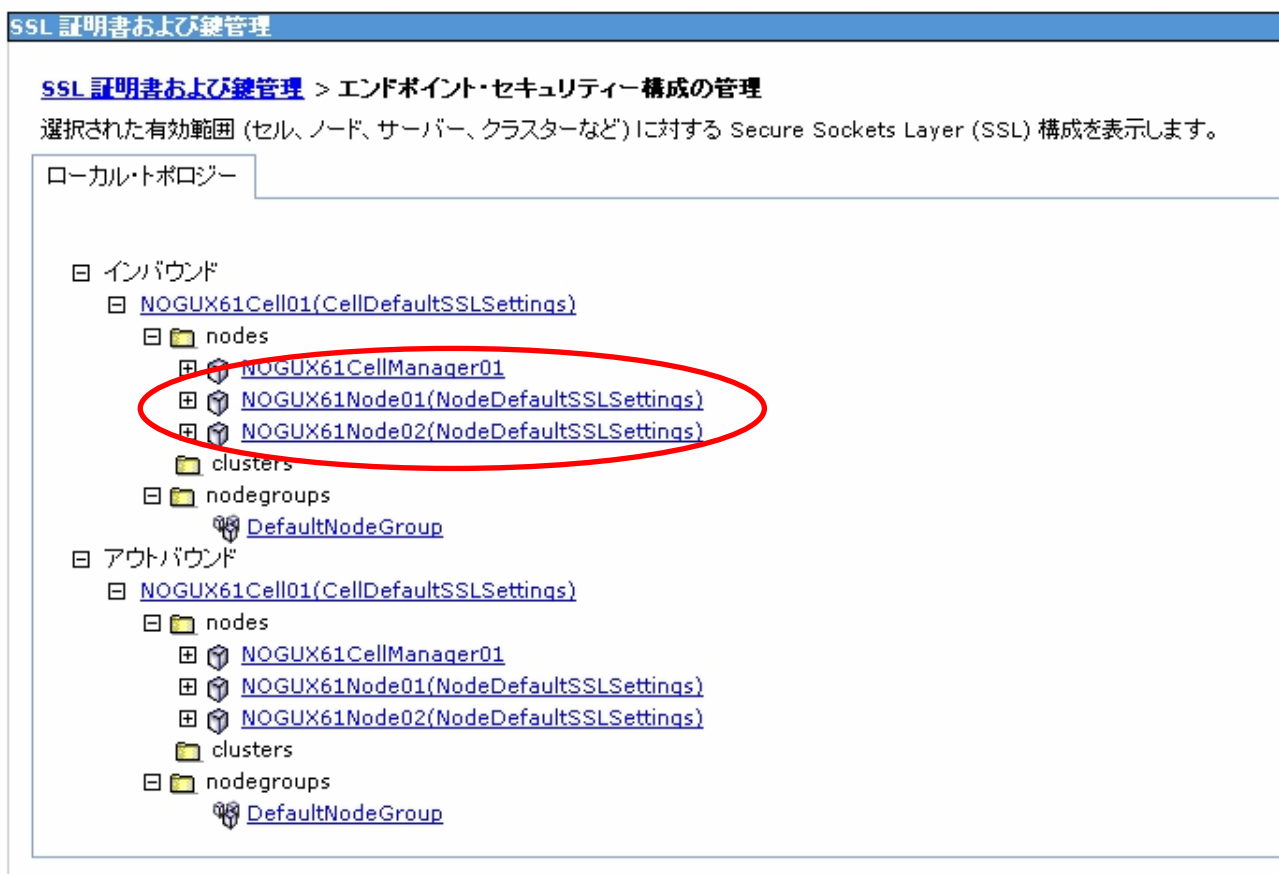
同期されていない場合は、この画面にて、確実に同期化させてください。

3. 既存のチェーン証明書の確認

管理コンソールから、以下に存在するチェーン証明書(default)の発行先とシリアル番号を確認します。

- セル(マスター)の鍵ストアにある個人証明書
- ノードの鍵ストアにある個人証明書

[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」の確認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」 「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」 で表示される例です。



3-1. ノードの個人証明書を確認します。

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。ローカルトポロジにある「インバウンド」-<Cell名>-「nodes」-<node名>の図から、<node名>(NodeDefaultSSLSettings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。

チェーン証明書(「default」などの別名を持つもの)の CN=, OU=, O=, C=の各値をメモします。また、シリアル番号もメモしておきます。

NodeDefaultKeyStore の例1

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 > NOGUX61Node01 > 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

作成... 削除... 証明書から受け取る... 置換... 抽出... インポート... エクスポート... 失効... 更新

選択	別名	発行先	発行元	シリアル番号	有効期限
<input type="checkbox"/>	default	CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US	CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US	186939013524903	有効期限: 2009/07/15 - 2024/07/15
<input type="checkbox"/>		CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US	CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US	186936213061995	有効期限: 2009/07/15 - 2024/07/11

合計 2

NodeDefaultKeyStore の例2

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 > NOGUX61Node02 > 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

作成... 削除... 証明書から受け取る... 置換... 抽出... インポート... エクスポート... 失効... 更新

選択	別名	発行先	発行元	シリアル番号	有効期限
<input type="checkbox"/>	default	CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=NOGUX61Cell01, OU=NOGUX61Node02, O=IBM, C=US	CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61Node02, O=IBM, C=US	534890446317618	有効期限: 2009/07/20 - 2024/07/20
<input type="checkbox"/>		CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61Node02, O=IBM, C=US	CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61Node02, O=IBM, C=US	534887921943152	有効期限: 2009/07/20 - 2024/07/16

合計 2

3-2. セル(マスター)の個人証明書を確認します。

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 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。

チェーン証明書(「default」などの別名を持つもの)の CN=, OU=, O=, C=の各値をメモします。また、シリアル番号もメモしておきます。

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 > NOGUX61Cell01 > 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。

田 設定

作成... 削除... 証明書から受け取る... 置換... 抽出... インポート... エクスポート... 失効... 更新

選択	別名	発行先	発行元	シリアル番号	有効期限
<input type="checkbox"/>	default	CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US	CN=NOGUX61.dhcp.makuhari.japan.ibm.com, O=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US	186939013524903	有効期限: 2019/07/15 - 2024/07/15
<input type="checkbox"/>		CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US	CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US	186936213061995	有効期限: 2009/07/15 - 2024/07/11

合計 2

3-3. ノードのチェーン証明書の置き換え計画を立てます。

各ノードの個人証明書がセル(マスター)の個人証明書と同じかどうかをチェックします。セル(マスター)のシリアル番号と同じであれば、同じ個人証明書です。上記の例では、「NodeDefaultKeyStore の例1」はセル(マスター)と同じですので、同じ個人証明書であることが分かります。また、「NodeDefaultKeyStore の例2」はセル(マスター)とは異なるので、別の個人証明書であることが分かります。

セル(マスター)と同じ個人証明書を持つノード(A)については、次の手順になります。

- セル(マスター)で個人証明書を作成する。
- これをノードの個人証明書(鍵ストア)へエクスポートする。

セル(マスター)と異なる個人証明書を持つノード(B)については、次の手順になります。

- セル(マスター)で個人証明書を作成する。
- ノードで個人証明書を作成する。

【注】

次章以降の手順をよく読んで、上記の(A)、(B)どちらのノードに対する作業かを確認しながら進んでください。

4. ノード、セル(マスター)のチェーン証明書の作成

有効期限が長い(このガイドでは 15 年)のチェーン証明書を作成します。

4-1. セル(マスター)のチェーン証明書を作成します。

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 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。



4-2. 「作成」>「チェーン証明書」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: default2 (任意の名前で構いませんが、「default」は既存の名前のため、使えません。)

証明書に署名するために使用するルート証明書: root (デフォルト値)

鍵サイズ: 1024 ビット(デフォルト値)

共通名: <上記手順 3-2 でメモした CN= の値>

有効期間: 5475 日間 (* 1)

組織: <上記手順 3-2 でメモした O= の値>

組織単位: <上記手順 3-2 でメモした OU= の値> (* 2)

国または地域: <上記手順 3-2 でメモした C= の値>

(* 1) 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せん。ここでは、約 15 年とした設定例を示しています。

(* 2) メモした値が"OU=A, OU=B"のように複数の場合には、初めの"OU="だけを省略して、"A, OU=B"のように入力します。

一般プロパティ

* 別名

default2

証明書に署名するために使用するルート証明書

root

鍵サイズ

1024 ビット

* 共通名

NOGUX61.dhcp.makuhari.jpapar

* 有効期間

5475 日間

組織

IBM

組織単位

NOGUX61Cell01, OU=NOGUX61

市町村

都道府県

郵便番号

国または地域

US

適用

OK

リセット

取り消し

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 > NOGUX61Cell01 > 個人証明書 > default2

個人証明書を管理します。

一般プロパティ

別名
default2

バージョン
X509 V3

鍵サイズ
1024 ビット

シリアル番号
545302087836023

有効期間
有効期間: 2009/07/20 - 2024/07/16

発行先
CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US

発行元
CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US

指紋 (SHA ダイジェスト)
2A:ED:74:B9:28:B1:01:C1:27:68:64:1A:B3:FB:6C:98:03:A2:E6:E3

署名アルゴリズム
SHA1withRSA(1.2.840.113549.1.1.5)

戻る

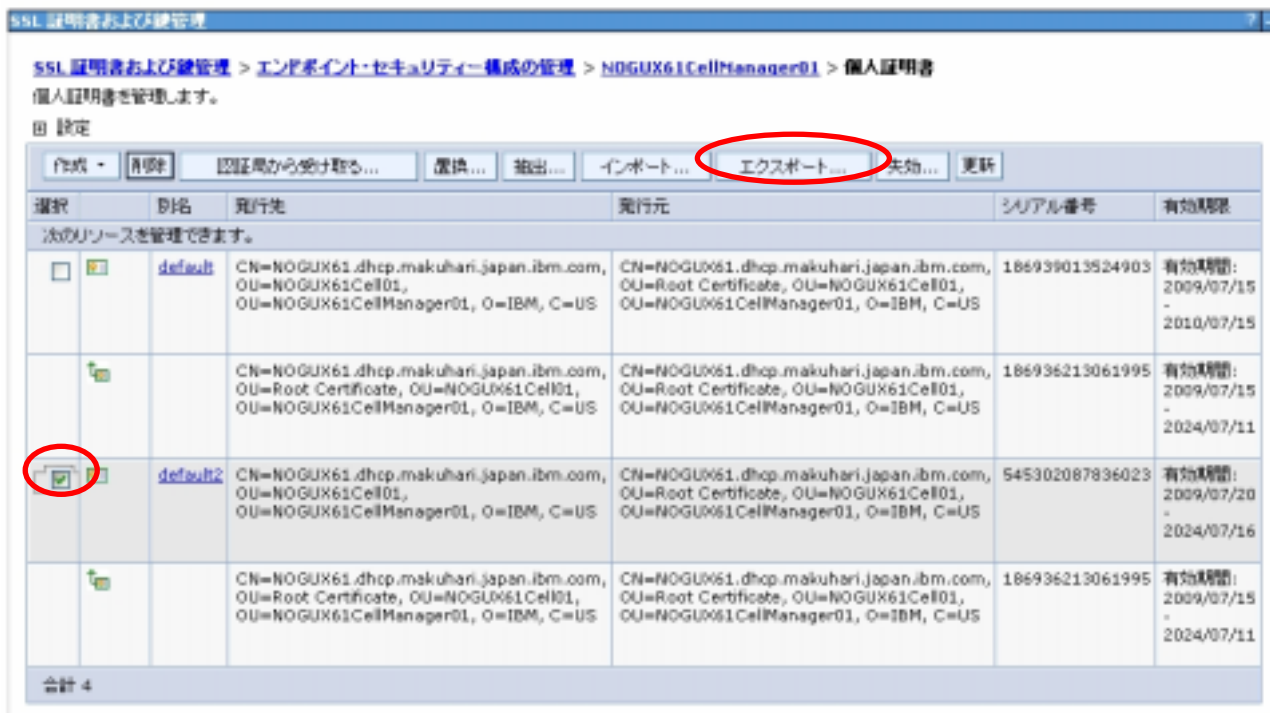
作成された証明書の確認画面

4-4. セル(マスター)と同じ個人証明書を持つノードの場合には、これをエクスポート(コピー)します。

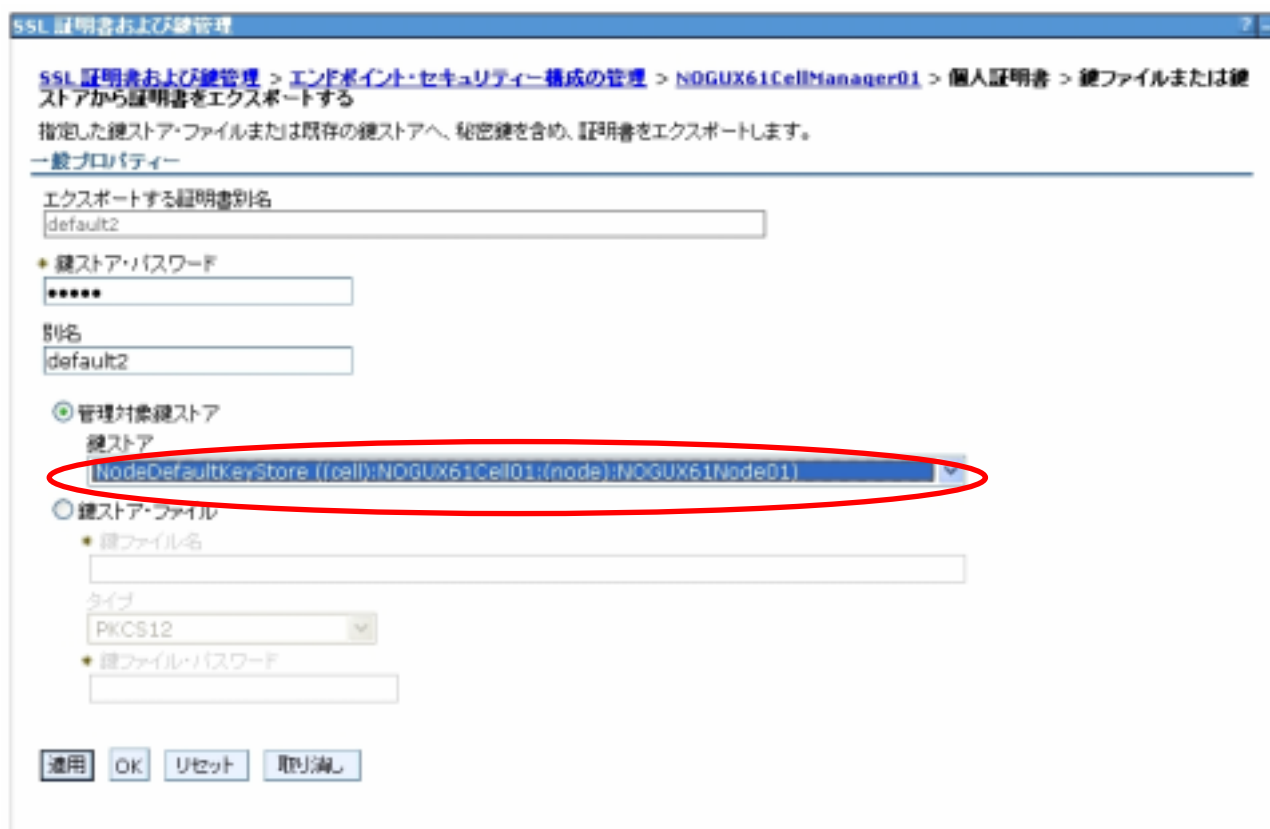
【注】セル内に同様のノードが複数存在する場合には、エクスポートは、ノード毎に行ってください

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>(CellDefaultSSLSettings 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。

上記(4-1 ~ 4-3)で作成した個人証明書(ここでは「default2」)を選択して、「エクスポート」ボタンをクリックします。



鍵ストア・パスワード(デフォルトは「WebAS」と、別名(ここでは「default2」とする)を入力します。「管理対象鍵ストア」を選択して、鍵ストアのドロップダウンから「NodeDefaultKeyStore(セル名:ノード名)」を選択します。




「適用」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。

4-5. エクスポートされた個人証明書を確認します。

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。ローカルトポロジにある「インバウンド」- <Cell 名> - 「nodes」 - <node 名> の図から、<node 名> (NodeDefaultSSLSettings 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。

エクスポートした個人証明書(ここでは「default2」)があることを確認します。



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 > NOGUX61Node@1 > 個人証明書'. Below the breadcrumb, there are buttons for '作成', '削除', '証明書から鍵取得...', '置換...', '抽出...', 'インポート...', 'エクスポート...', '失効...', and '更新'. A table lists certificates with columns for '選択' (Select), '別名' (Alias), '発行先' (Issued To), '発行元' (Issued By), 'シリアル番号' (Serial Number), and '有効期限' (Validity Period). The 'default2' certificate is circled in red.

選択	別名	発行先	発行元	シリアル番号	有効期限
<input type="checkbox"/>	default	CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US	CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US	186939013524903	有効期限: 2009/07/15 - 2016/07/15
<input type="checkbox"/>		CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US	CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US	186936213061995	有効期限: 2009/07/15 - 2024/07/11
<input type="checkbox"/>	default2	CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US	CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US	545302087836023	有効期限: 2009/07/20 - 2024/07/16
<input type="checkbox"/>		CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US	CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US	186936213061995	有効期限: 2009/07/15 - 2024/07/11

合計 4

4-6. セル(マスター)とは異なる個人証明書を持つノードのチェーン証明書を再作成します。

[注] セル内に同様のノードが複数存在する場合には、「チェーン証明書の再作成」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・ポロジを展開し、「インバウンド」 - <Cell 名> - 「nodes」 - <node 名> (NodeDefaultSSLSettings 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。

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・セキュリティー構成の管理](#) > NOGUX61Node02

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
NOGUX61Node02

方向
インバウンド

継承された SSL 構成

継承された SSL 構成名
CellDefaultSSLSettings

継承された証明書別名
null

このエンドポイントの特定 SSL 構成

継承された値のオーバーライド

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) ▼

適用 OK リセット 取り消し

4-7. 「作成」 - 「チェーン証明書」ボタンをクリックします。



4-8. 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: default3 (任意の名前で構いませんが、「default」は既存の名前のため、使えません。)

証明書に署名するために使用するルート証明書: root (デフォルト値) (* 3)

鍵サイズ: 1024 ビット(デフォルト値)

共通名: <上記手順 3-1 でメモした CN= の値>

有効期間: 5475 日間 (* 1)

組織: <上記手順 3-1 でメモした O= の値>

組織単位: <上記手順 3-1 でメモした OU= の値> (* 2)

国または地域: <上記手順 3-1 でメモした C= の値>

(* 1) 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。

(* 2) メモした値が OU=A, OU=B のように複数の場合には、初めの"OU="だけを省略して、"A, OU=B"のように入力します。

(* 3) この手順書では、セル内のルート証明書を Deployment Manager の利用するルート証明書と同じもので統一する方法をガイドしています。もし、別のルート証明書を利用する場合には、このドロップダウンメニューで他のルート証明書を選択します。この場合には、5 章(5-4, 5-6)で署名者証明書を削除するときに、有効期限が 15 年のものは削除しないでください。

一般プロパティ

+ 別名

default3

証明書に署名するために使用するルート証明書

root

鍵サイズ

1024 ビット

+ 共通名

NOGUX61.dhcp.makuhari.jpapar

+ 有効期間

5475 日数

組織

IBM

組織単位

1Cell01, OU=NOGUX61Node02

市町村

都道府県

郵便番号

国または地域

US

適用

OK

リセット

取り消し

SSL 証明書および鍵管理

SSL 証明書および鍵管理 > エンポイントセキュリティ構成の管理 > NOGUX61Node02 > 個人証明書 > default3

個人証明書を管理します。

一般プロパティ

別名

default3

バージョン

X509 V3

鍵サイズ

1024 ビット

シリアル番号

546000156747296

有効期間

有効期間: 2009/07/20 - 2024/07/16

発行先

CN=NOGUX61.dhcp.makuhari.jpapar.ibm.com, OU=NOGUX61Cell01, OU=NOGUX61Node02, O=IBM, C=US

発行元

CN=NOGUX61.dhcp.makuhari.jpapar.ibm.com, OU=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US

指紋 (SHA ダイジェスト)

FB:11C:CA:11:76:37:CB:13:FF:A6:21:98:5D:E6:0A:AF:44:95:B6:BF

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

5. 古い証明書の削除

管理コンソールから、以下に存在する古い証明書(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。

The screenshot shows the 'SSL 証明書および鍵管理' (SSL Certificate and Key Management) console. The breadcrumb is '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'. Below the breadcrumb, it says '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) 構成を表示します。' (Display the Secure Sockets Layer (SSL) configuration for the selected effective scope (cell, node, server, cluster, etc.)).

The main content area is titled 'ローカル・トポロジー' (Local Topology) and shows a tree view of the configuration. Under 'インバウンド' (Inbound), there is a folder 'NOGUX61Cell01(CellDefaultSSLSettings)'. Inside this folder, there is a 'nodes' folder. Under 'nodes', there are two nodes: 'NOGUX61CellManager01' and 'NOGUX61Node01(NodeDefaultSSLSettings)'. The two nodes are circled in red. Below the nodes, there is a 'clusters' folder and a 'nodegroups' folder containing 'DefaultNodeGroup'. The same structure is repeated under 'アウトバウンド' (Outbound).

5-1. 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。

古いチェーン証明書(別名が「default」のもの)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後、同期化してください。

5-2. ノードのトラスト・ストアにある署名者証明書を削除します。

【注】

この節の作業は、セル(マスター)と異なる個人証明書を持つノードの場合(3-3 でノード(B)の場合)のみ、行います。セル(マスター)と同じ個人証明書を持つノードの場合(3-3 でノード(A)の場合)には、削除対象となる署名者証明書は存在しません。

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・トポロジーにある「インバウンド」-<Cell名>-「nodes」-<node名>の図から、<node名>(NodeDefaultSSLSettings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。

古い署名者証明書(別名が「default」のもの)を選択し、「削除」ボタンをクリックします。



マスター構成に保管後、同期化してください。

5-3. 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 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。

古いチェーン証明書(別名が”default”などのもの)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後、同期化してください。

5-4. 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>(CellDefaultSSLSettings 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署名者証明書を全て選択し、「削除」 ボタンをクリックします。

[注] 4-8 で、Deployment Manager のルート証明書以外を指定した場合は、“default”のみを削除します。“default”で始まる他の証明書で、(下図の場合は、“default_1”のように)有効期間が 15 年のものは、Deployment Manager 以外のノードのルート証明書ですので、削除せずに残す必要があります。



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・セキュリティー構成の管理 > NOGUX61Cell01 > 鍵ストアおよび証明書 > CellDefaultTrustStore > 署名者証明書. Below the breadcrumb, there is a text box: '鍵ストア内の署名者証明書を管理します。' (Manage certificates in the key store). There are buttons for '追加' (Add), '削除' (Delete), and 'ポートから取得' (Get from port). Below these are icons for refresh, search, and help. A table lists certificates with columns: '選択' (Select), '別名' (Alias), '発行先' (Issued to), '指紋 (SHA ダイジェスト)' (Fingerprint (SHA Digest)), and '有効期限' (Validity Period). The 'default' and 'default_1' certificates are selected, and the '削除' button is circled in red.

選択	別名	発行先	指紋 (SHA ダイジェスト)	有効期限
<input type="checkbox"/>	datapower	OU=Root CA, O="DataPower Technology, Inc.", C=US	A9:BA:A4:B5:BC:26:2F:5D:2A:8D:93:CA:BA:F4:31:05:F2:54:14:17	有効期限: 2003/06/12 - 2023/06/07
<input checked="" type="checkbox"/>	default	CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US	67:A3:4A:C8:E1:4A:9D:EF:F3:AD:35:BE:4B:6F:51:EF:EA:4F:BF:C3	有効期限: 2009/07/15 - 2010/07/15
<input checked="" type="checkbox"/>	default_1	CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61Node02, O=IBM, C=US	5E:74:8D:D6:8D:44:19:26:E0:C8:0B:C8:FE:6F:E3:8B:F5:98:E1:32	有効期限: 2009/07/20 - 2024/07/16
<input type="checkbox"/>	root	CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US	3C:34:BE:6F:1A:72:D2:AC:CE:2C:2D:B6:BE:2F:4D:DC:03:CD:78:68	有効期限: 2009/07/15 - 2024/07/11

合計 4

マスター構成に保管後、同期化してください。

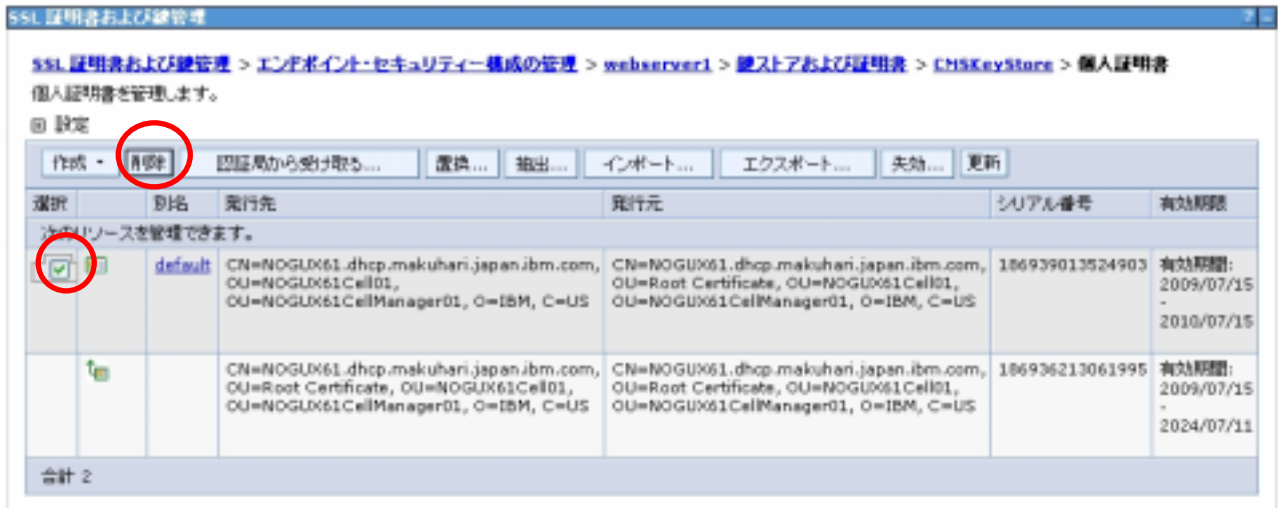
5-5. Web サーバー・プラグインが使用する鍵データベース CMSKeyStore (plugin-key.kdb) の個人証明書を削除します。

[注] default という名前で始まる証明書が存在しない場合、5-6 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」 - <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後、同期化してください。

5-6. 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。

[注] 4-8 で、Deployment Manager のルート証明書以外を指定した場合は、「default」のみを削除します。「default」で始まる他の証明書で、(下図の場合は、「default_1」のように)有効期間が 15 年のものは、Deployment Manager 以外のノードのルート証明書ですので、削除せずに残す必要があります。

SSL 証明書および鍵管理 > エンジン/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

鍵ストア内の署名者証明書を管理します。

設定

追加 削除 抽出 ポートから取得

選択	名前	発行先	指紋 (SHA ダイジェスト)	有効期限
<input type="checkbox"/>	datapower	OU=Root CA, O="DataPower Technology, Inc.", C=US	A9:BA:A4:B5:BC:26:2F:5D:2A:8D:93:CA:BA:F4:31:05:F2:54:14:17	有効期限: 2003/06/12 - 2023/06/07
<input checked="" type="checkbox"/>	default_1	CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61Node02, O=IBM, C=US	5E:74:8D:D6:8D:44:19:26:E0:C8:0B:C8:FE:0F:E3:8B:F5:98:E1:32	有効期限: 2009/07/20 - 2024/07/16
<input type="checkbox"/>	root	CN=NOGUX61.dhcp.makuhari.japan.ibm.com, OU=Root Certificate, OU=NOGUX61Cell01, OU=NOGUX61CellManager01, O=IBM, C=US	3C:34:BE:6F:1A:72:D2:AC:CE:2C:20:B6:BE:2F:4D:DC:83:CD:78:68	有効期限: 2009/07/15 - 2024/07/11

合計 3

マスター構成に保管後、同期化してください。

6. 署名者証明書の追加

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

6-1. CellDefaultKeyStore と CellDefaultTrustStore 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> (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。



6-1-2. 署名者証明書に追加します。

「CellDefaultKeyStore」の、上記手順 4-1、4-2、4-3 で作成した、チェーン証明書(ここでは「default2」)を選択し、「追加 > >」ボタンをクリックします。



6-1-3. 「CellDefaultTrustStore」に、新規作成したチェーン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。



6-2. 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。

[注] セル(マスター)と同じ個人証明書を持つノードの場合でも、異なる個人証明書を持つノードの場合でも、ノード事に行ってください。

6-2-1. 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にある「インバウンド」- <Cell 名> - 「nodes」 - <node 名> の図から、<node 名> (NodeDefaultSSLSettings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。



6-2-2. 署名者証明書に追加します。

「CellDefaultKeyStore」の、上記手順 4-1、4-2、4-3 で作成した(4-5 でエクスポートされた)チェーン証明書(ここでは「default2」)を選択し、「追加 >>」ボタンをクリックします。



6-2-3. 「NodeDefaultTrustStore」に、新規作成したチェーン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。



6-3. NodeDefaultTrustStore と CellDefaultTrustStore の署名者を交換します。

[注] セル(マスター)と異なる個人証明書を持つノードの場合のみ行ってください。セル(マスター)と同じ個人証明書を持つノードの場合は行う必要がありません。

[注] セル内に同様のノードが複数存在する場合には、「NodeDefaultTrustStore と CellDefaultTrustStore の署名者を交換」は、ノード毎に行ってください。

6-3-1. 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。「NodeDefaultTrustStore」と「CellDefaultTrustStore」を選択し、「署名者の交換...」ボタンをクリックします。



6-3-2. 署名者証明書に追加します。

「CellDefaultTrustStore」の、上記手順 4-1、4-2、4-3 で作成した、チェーン証明書(ここでは「default2」)を選択し、「追加 > >」ボタンをクリックします。



6-3-3. 「NodeDefaultTrustStore」に、新規作成したチェーン証明書が追加されたことを確認します。



6-3-4. 「NodeDefaultTrustStore」の、上記手順 4-6、4-7、4-8 で作成した、チェーン証明書(ここでは「default3」)を選択し、「追加 >>」ボタンをクリックします。

【注】 上記手順 4-6、4-7、4-8 を行っていない場合は、「default3」はありませんので、6-3-4、6-3-5 を行う必要はありません。ここまでの操作を 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。



6-3-5. 「CellDefaultTrustStore」に、新規作成したチェーン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。



7. 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 CellDefaultKeyStore と、CMSKeyStoreの署名者を交換する場合は7-1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7-2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7-3を必ず行ってください。

7-1. Webサーバーを管理しているノードの CellDefaultKeyStore と Webサーバーが使用する CMSKeyStore の署名者を交換します。

7-1-1. 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「CellDefaultTrustStore」を選択し、「署名者の交換...」ボタンをクリックします。



7-1-2. CMSKeyStore に署名者証明書を追加します。

「CellDefaultTrustStore」の、上記手順 4-6、4-7、4-8 で作成した、チェーン証明書(ここでは「default2」や「default3」)を選択し、「追加 >>」ボタンをクリックします。



7-1-3. 「CMSKeyStore」にチェーン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。



7-2. 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。

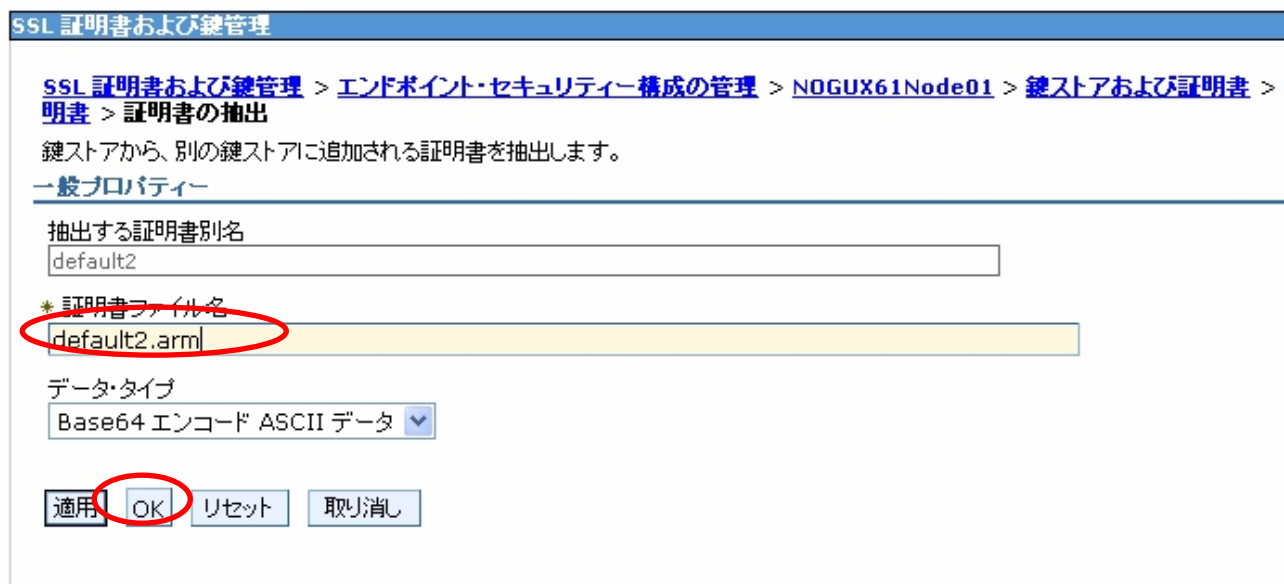
7-2-1. 管理コンソールから「セキュリティ」 「SSL 証明書および鍵管理」 「エンドポイント・セキュリティ構成の管理」を開きます。ローカル・ポロジを展開し、「インバウンド」 - <Cell 名> - 「nodes」 - <node 名> - 「servers」 - <Web サーバー名> をクリックします。「関連項目」にある「鍵ストアおよび証明書」をクリックします。「CellDefaultKeyStore」をクリックし、「追加プロパティ」にある「個人証明書」をクリックします。

個人証明書(ここでは「default2」)にチェックを入れて、「抽出」ボタンをクリックします。



[注] 7-2-1, 7-2-2, 7-2-3, 7-2-4の操作は、同様に”default3”に対しても行う必要があります。上図の画面では、複数選択で「抽出」を行うことができませんので、一つずつ行ってください。

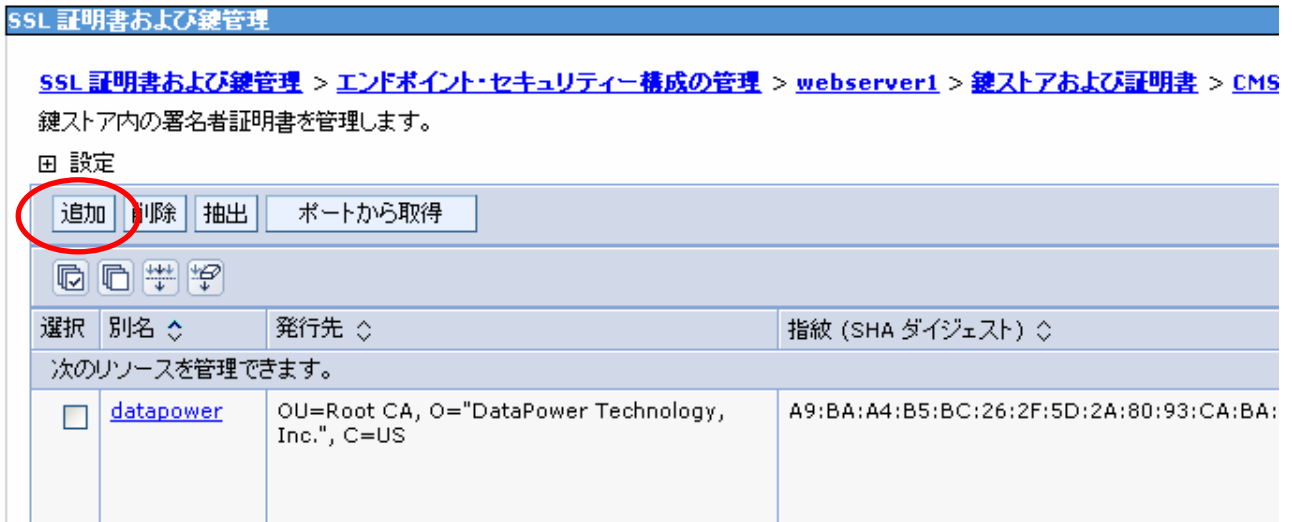
7-2-2. 証明書の抽出画面で、「証明書ファイル名」に任意のファイル名を指定し(ここでは「default2.arm」)、「OK」ボタンをクリックします。これで <WAS_ROOT>/profiles/<DM_profile_name>/etc に default2.arm が生成されます。



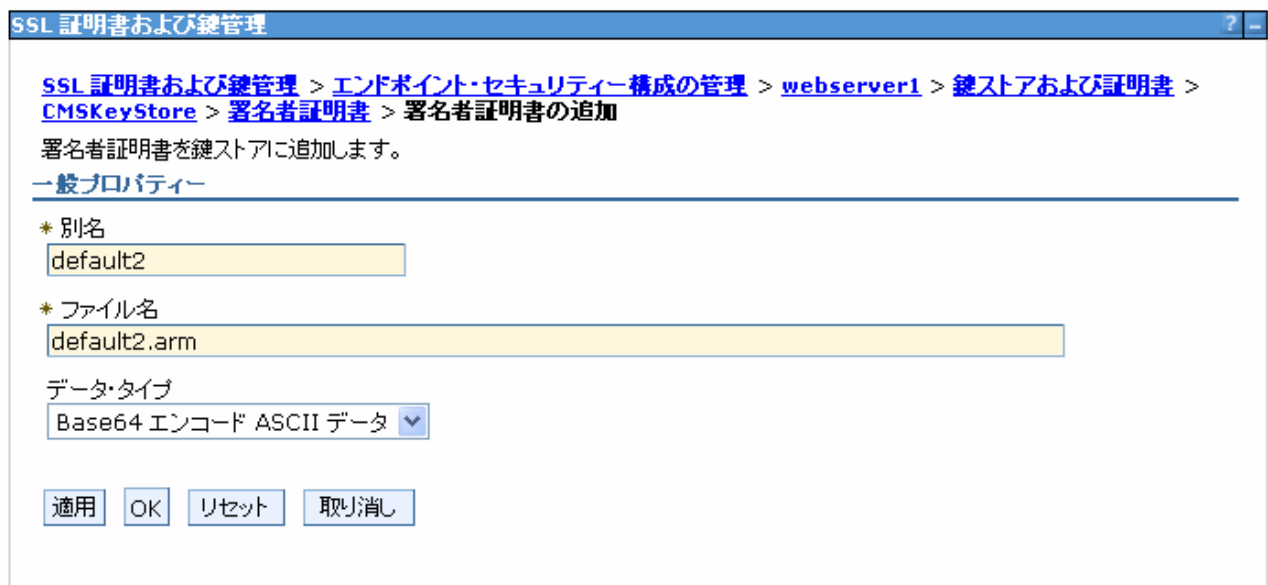
7-2-3. 次に、取り出した署名者証明書を CMSKeyStore に追加します。

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。



7-2-4. 「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(ここでは default2.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。



これでCMSKeyStoreに署名者証明書が追加されました。

7-3. 更新されたCMSKeyStoreファイルをWebサーバー・プラグインに読み込ませます。

7-3-1. 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」 「サーバー・タイプ」 「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/<webse
rver_name>/plugin-key.kdb をコピーします。

Web server plug-in 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およびファイル名

c:\Program Files\IBM\HTTPServer\Plugins\config\webserver1\plugin-cfg.xml

* プラグイン鍵ストア・ディレクトリおよびファイル名

c:\Program Files\IBM\HTTPServer\Plugins\config\webserver1\plugin-key.kdb

7-3-2. 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」 「グローバル・セキュリティ」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。

グローバル・セキュリティ

グローバル・セキュリティ

このパネルを使用して、管理およびデフォルト・アプリケーション・セキュリティ・ポリシーを構成します。ユーザー・アプリケーションのデフォルト・セキュリティ・ポリシーとして使用されます。セキュリティでカスタマイズすることができます。

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](#)
- [管理認証](#)

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。



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。

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。

【注】

WAS V6.1では、<WAS_ROOT>/profiles/<Node_profile_name>/etc/trust.p12に新しい署名者証明書を取り込むための作業が必要でしたが、V7.0ではルート証明書を利用しているため、必要なくなりました。

更新履歴

- 2009/08/21 P31の図(7-1-2)の囲み線を修正
- 2009/08/27 P18に5-2を追加
 - P26の文言を一部補足修正
 - P31の画面と文言の相違を修正
 - P35の管理コンソール画面の用語を修正
 - P36の節番号を修正
- 2009/09/03 P19 5-2に文言(保管と同期)追加
 - P30 7-1-1の文言一部修正
 - P31 7-1-2の文言一部修正
- 2009/10/05 P30 7,7-1の文言一部修正