syslog-ng Agent for Windows 暗号化通信設定

Rev.1.0

BALABIT

CONTEXTUAL SECURITY INTELLIGENCE

2017.7.4

JTC-i ジュピターテクノロジー

目次

まえがき 1
1 syslog-ng Agent for Windows 暗号化通信設定 1
1.1 SSB の自己証明書のダウンロード 2
1.2 Windows クライアントに証明書をインポートする 3
1.3 syslog-ng Agent for Windows の暗号化を有効にする 10

変更履歴

版	発行日	変更内容
Rev. 1.0	2017/7/4	新規作成

お問合せ先とカスタマーポータル

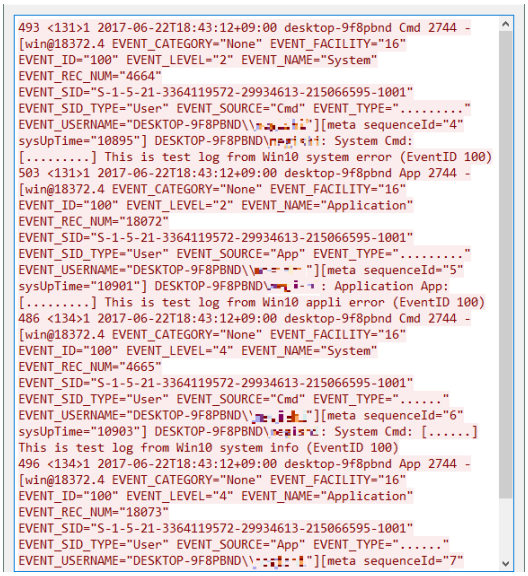
ジュピターテクノロジー株式会社（Jupiter Technology Corp.）

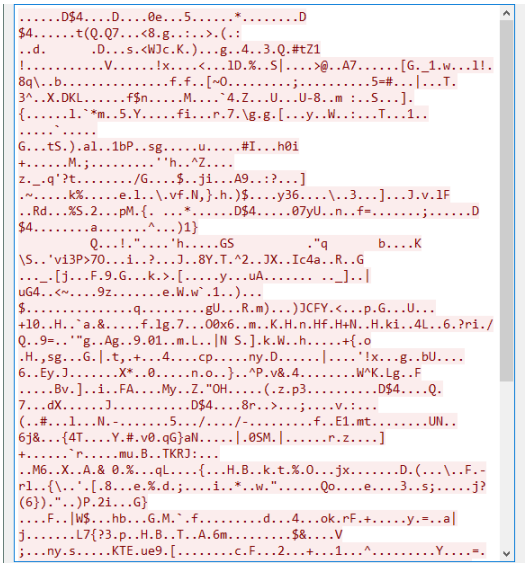
住所: 〒183-0023 東京都府中市宮町 2-15-13 第 15 三ツ木ビル 8F
URL: http://www.jtc-i.co.jp/
電話番号: 042-358-1250
FAX 番号: 042-360-6221
ご購入のお問い合わせ:
お問い合わせフォーム https://www.jtc-i.co.jp/contact/scontact.php
メール sales@jtc-i.co.jp
製品サポートのお問い合わせ:
カスタマーポータル https://www.jtc-i.co.jp/support/customerportal/
評価版のダウンロード:
https://www.jtc-i.co.jp/support/download/

まえがき

暗号化されていない通信では通信途中でデータの盗聴や改ざんが行われる可能性があります。ログの転送についても同じで、ログの内容がパケットキャプチャツールなどで簡単に読めてしまいます。その為、通信の暗号化は PCI DSS の要件の中にも含まれています。ここでは、SSB の自己証明書を使用して、SSB と syslog-ng Agent for Windows との間で、(Windows イベント) ログの転送時に TLS 暗号化して通信する手順を説明します。

この手順書では、syslog-ng Agent for Windows と SSB の間で、(Windows イベント)ログを転送時に暗号化して通信する方法をご紹介いたします。





1 syslog-ng Agent for Windows暗号化通信設定

syslog-ng Agent for Windows と SSB の間で、(Windows イベント)ログを転送時に暗号化して通信するには以下の手順を実行します。

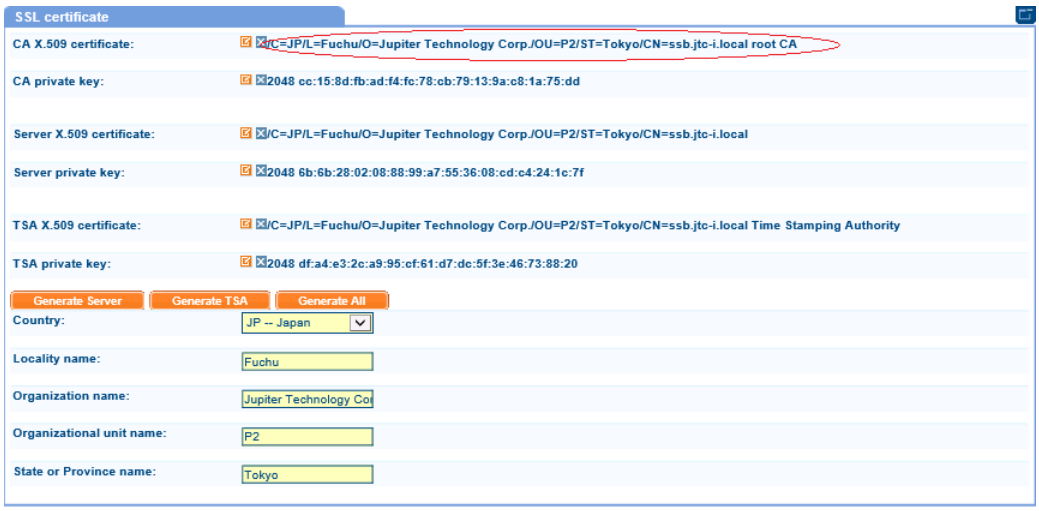
- 1.1 SSB の自己証明書のダウンロード
- 1.2 Windows クライアントに証明書をインポートする
- 1.3 syslog-ng Agent for Windows の暗号化を有効にする

より、詳しい内容については「syslog-ng Agent for Windows 6LTS 管理者ガイド」および「syslog-ng Store Box (SSB) 4LTS 管理者ガイド」をご参照ください。

1.1 SSBの自己証明書のダウンロード

1. SSB の Web I/F にアクセスします。
2. [Basic Settings]>[Management]>[SSL certificate]に移動します。
3. [CA X.509 certificate]フィールドの識別名(DN)をクリックします。

Figure 1 SSL certificate



注意:
この証明書(サーバーの CACert とも呼ばれます)は、サーバー証明書(Server X.509 certificate)ではなく、サーバー証明書に署名した CA の証明書(CA X.509 certificate)になります。

4. 証明書の内容が表示されるので、[Download]横の[DER]をクリックして証明書をダウンロードします。

Figure 2 certificate

注意:

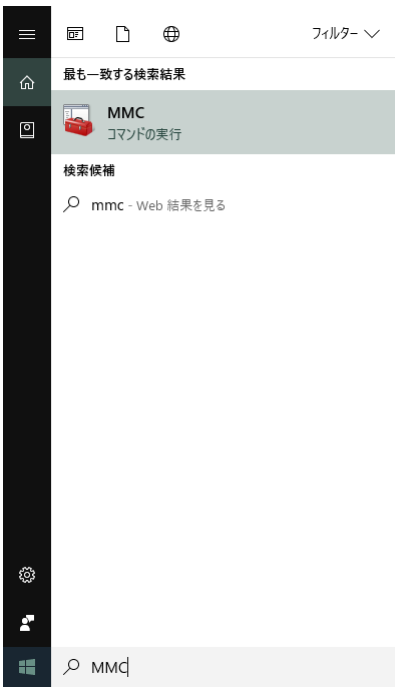
認証局で発行されたサーバー証明書を利用する 場合は、SSB の [Log]>[Options]>[TLS settings]セクションで、サーバー証明書をアップロードします。

1.2 Windowsクライアントに証明書をインポートする

TLS 暗号化通信させたい、syslog-ng Agent for Windows が動作している Windows クライアントに証明書をインポートします。

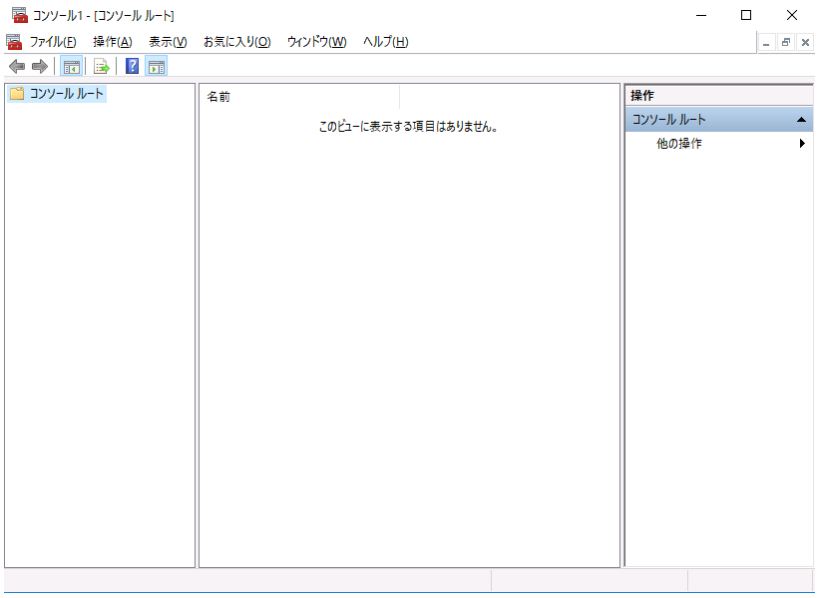
1. MMCコンソールを開きます。(Windows10では、タスクバーの検索ボックス、または、[スタートメニュー]>[ファイル名を指定して実行]で"MMC /a"と入力します。)

Figure 3 検索ボックス



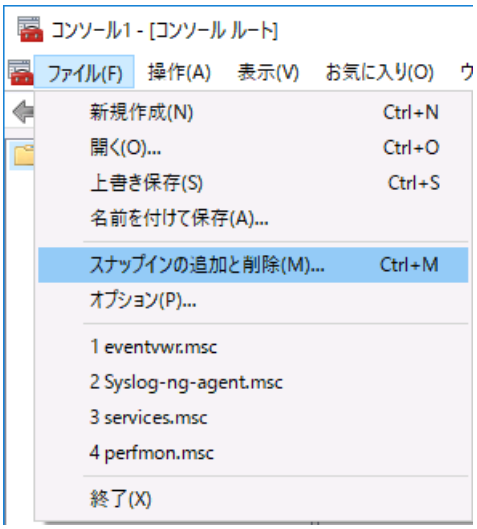
2. MMC コンソールウィンドウが開きます。

Figure 4 MMC コンソールウィンドウ



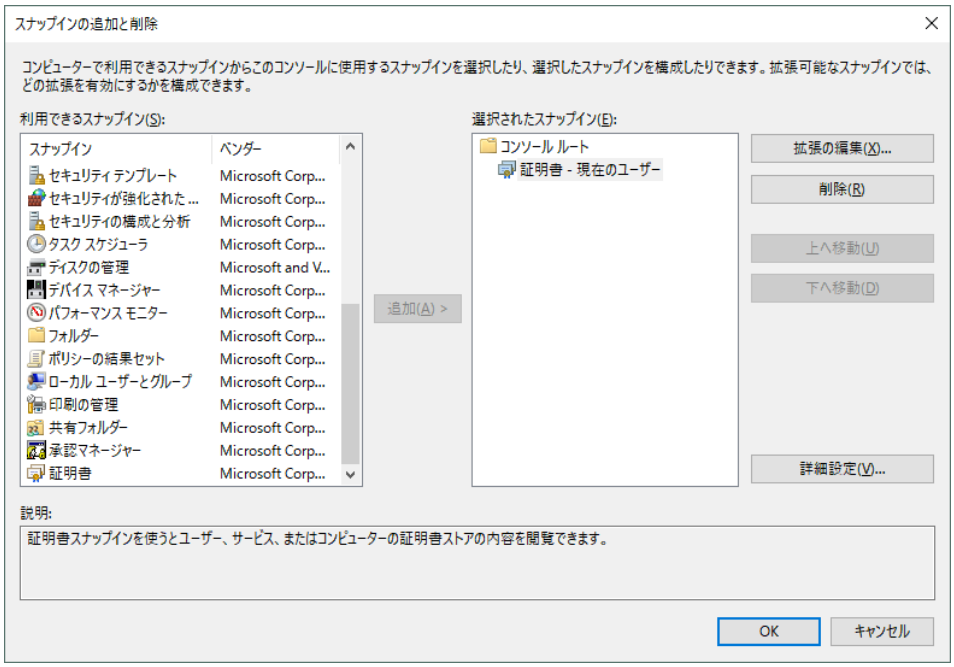
3. メニューから[ファイル]>[スナップインの追加と削除]を選択します。

Figure 5 メニュー[スナップインの追加と削除]



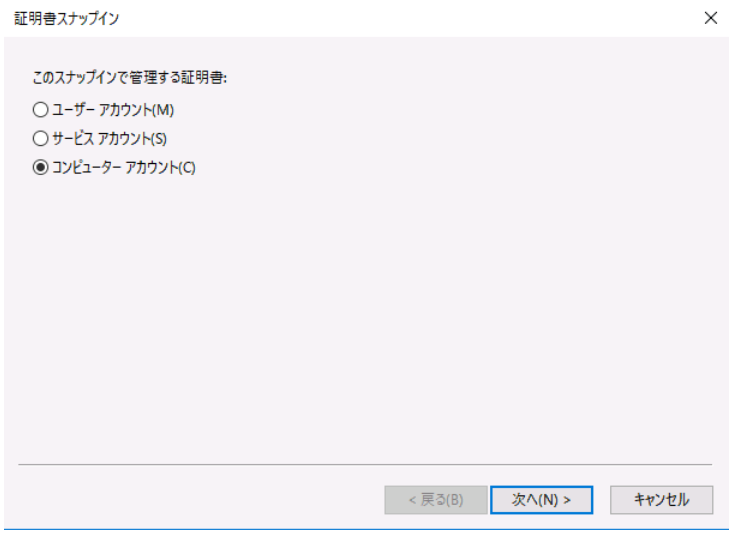
4. [スナップインの追加と削除]ウィンドウで[証明書]を選んで、[追加]ボタンをクリックします。

Figure 6 スナップインの追加と削除ウィンドウ



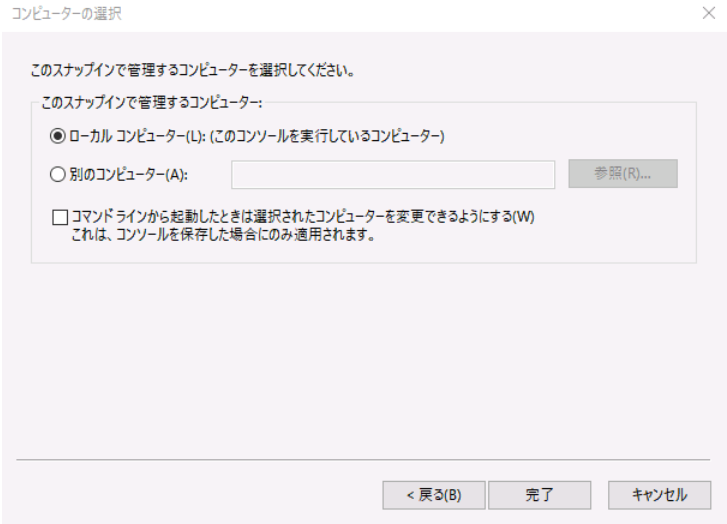
5. 証明書スナップインで[コンピュータアカウント]を選んで、[次へ]をクリックします。

Figure 7 証明書スナップイン画面



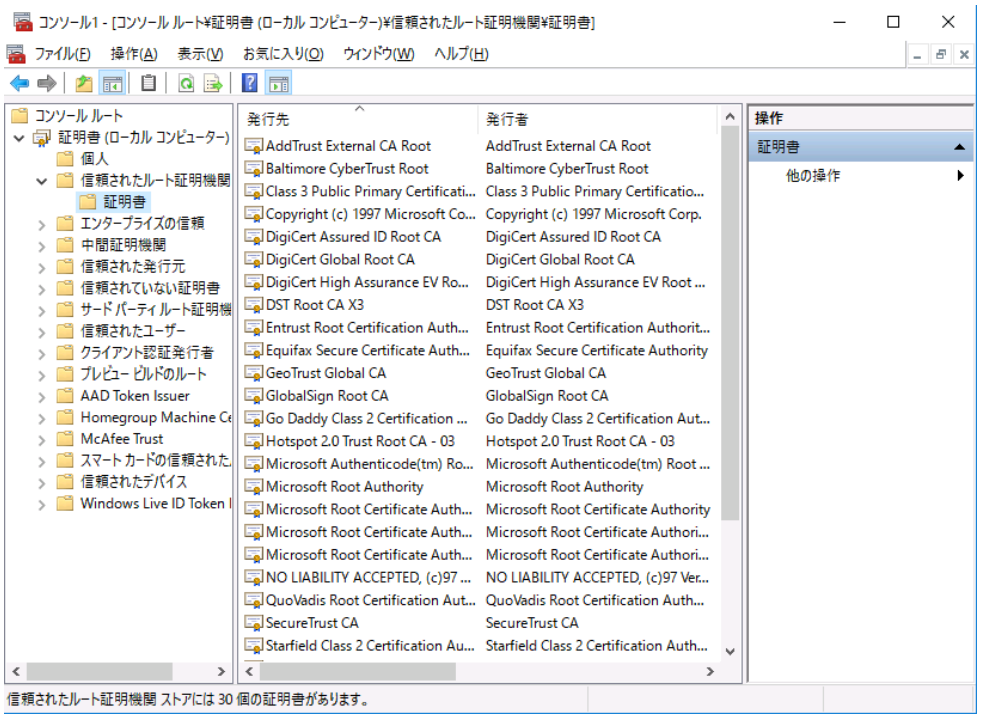
6. コンピューターの選択で[ローカルコンピューター]を選択して、[完了]をクリックします。

Figure 8 コンピューターの選択画面



7. コンソールウィンドウに証明書がリストされますので、[証明書(ローカルコンピューター)]>[信頼されたルート証明機関]>[証明書]と展開して、選択します。

Figure 9 MMC コンソールの証明書リスト

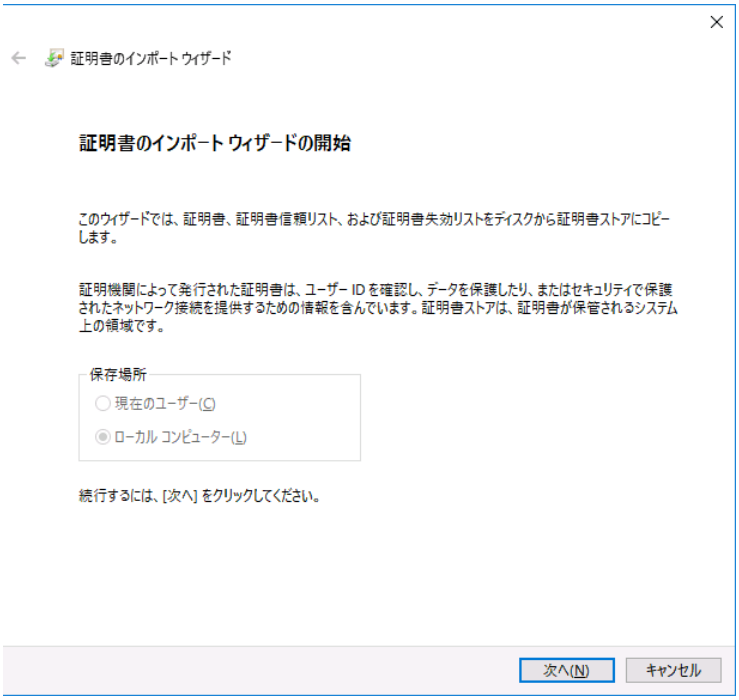


8. 右クリックしてコンテキストメニューを表示し、[すべてのタスク]>[インポート]を選びます。

Figure 10 証明書インポート

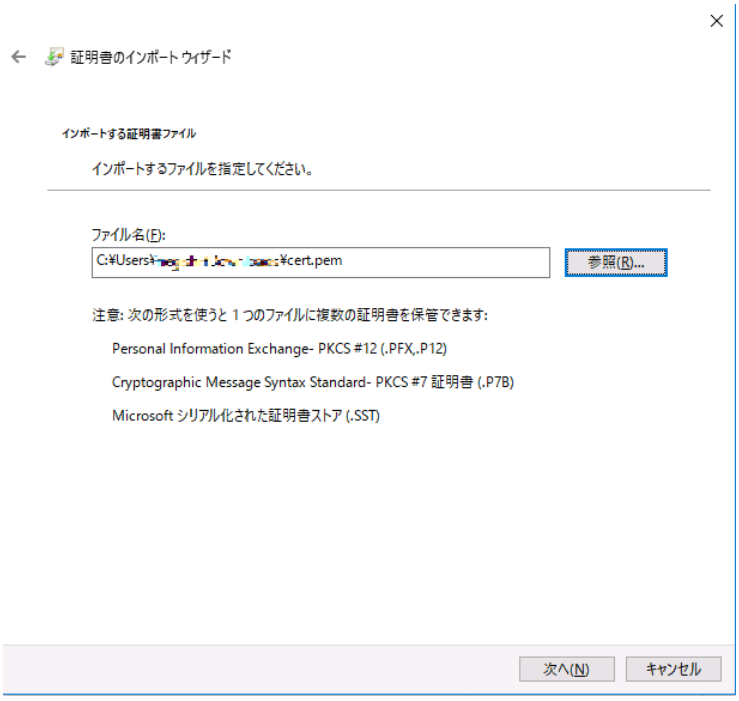
9. 証明書のインポートウィザードが表示されますので、[次へ]をクリックします。

Figure 11 証明書のインポートウィザード



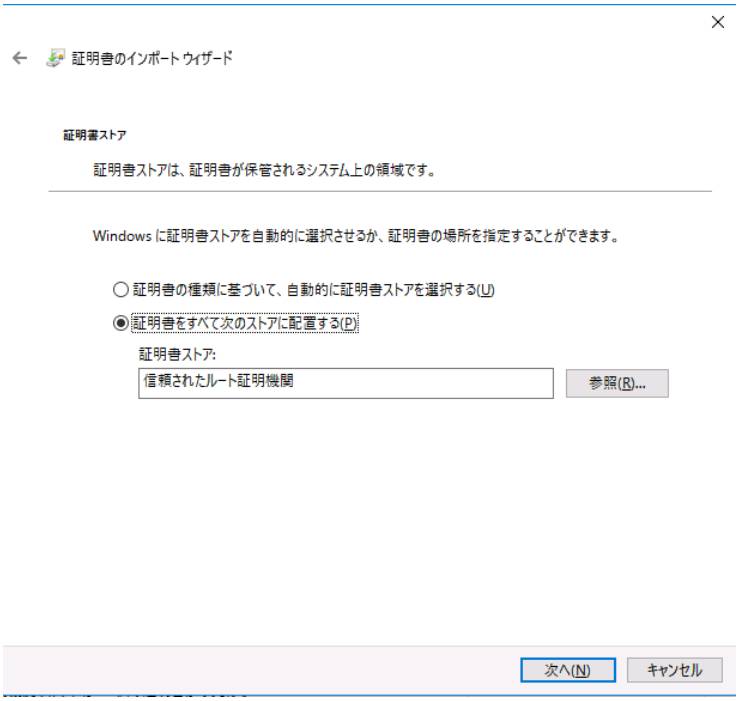
10. インポートする証明書ファイルに、「1.1 SSB の自己証明書のダウンロード」でダウンロードした証明書を選択します。

Figure 12 インポートする証明書ファイル



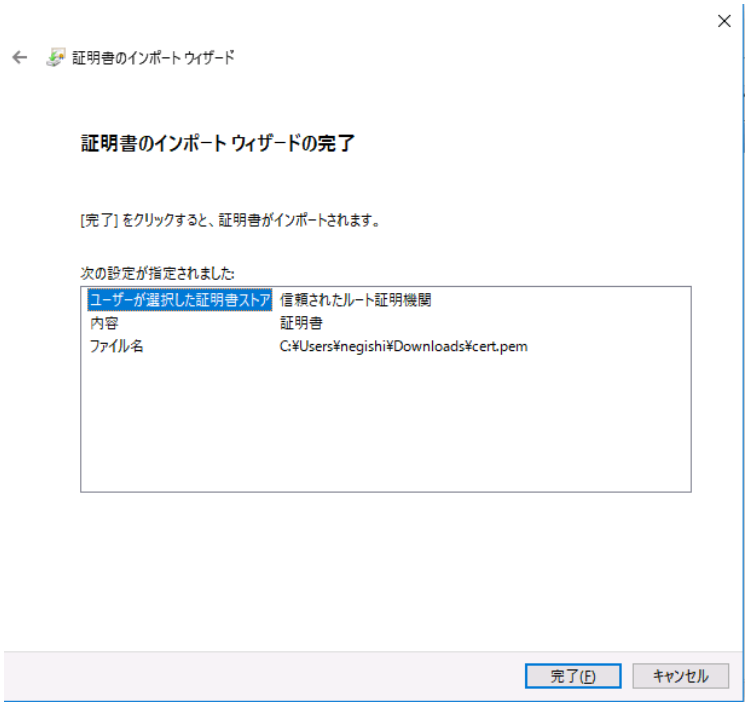
11. 証明書のストア先はデフォルトのまま、[次へ]をクリックします。

Figure 13 証明書ストア



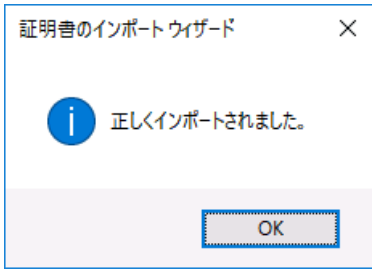
12. 証明書のインポートウィザードが完了しましたので、[完了]クリックします。

Figure 14 証明書のインポートウィザードの完了



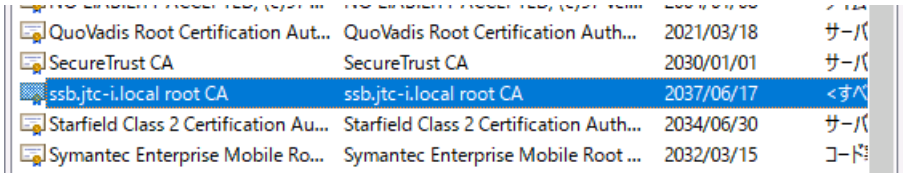
13. 正しく、証明書がインポートされると次のメッセージが表示されますので、[OK]をクリックします。

Figure 15 インポートメッセージ



14. コンソールウィンドウで証明書がリストされていることを確認します。

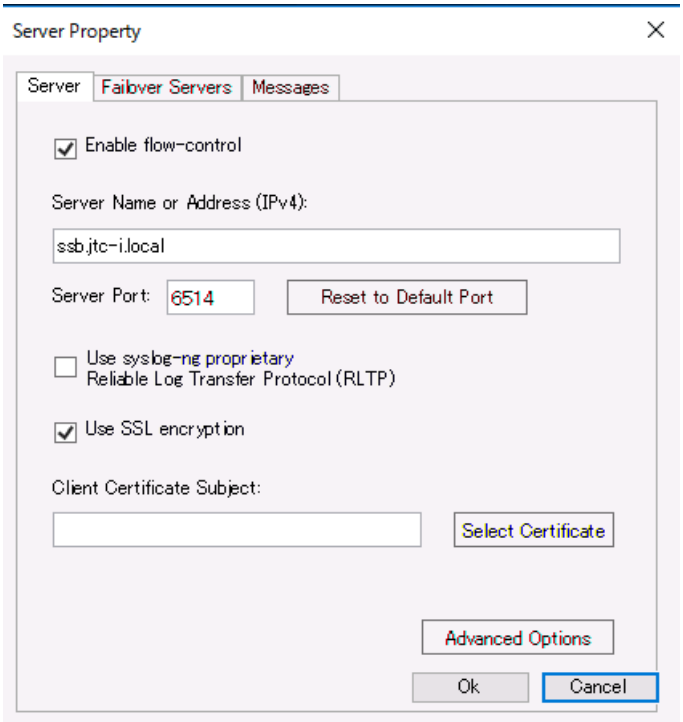
Figure 16 インポートされた証明書



1.3 syslog-ng Agent for Windowsの暗号化を有効にする

1. syslog-ng Agent for Windows コンフィグレーションインターフェイスを開きます。
2. [Destinations]に移動し、宛先ログサーバーの[Properties]をダブルクリックして、サーバープロパティーを開きます。
3. [Server]タブの[Use SSL encryption]にチェックし、[Server Port]を”6514”に変更します。

Figure 17 Server Property



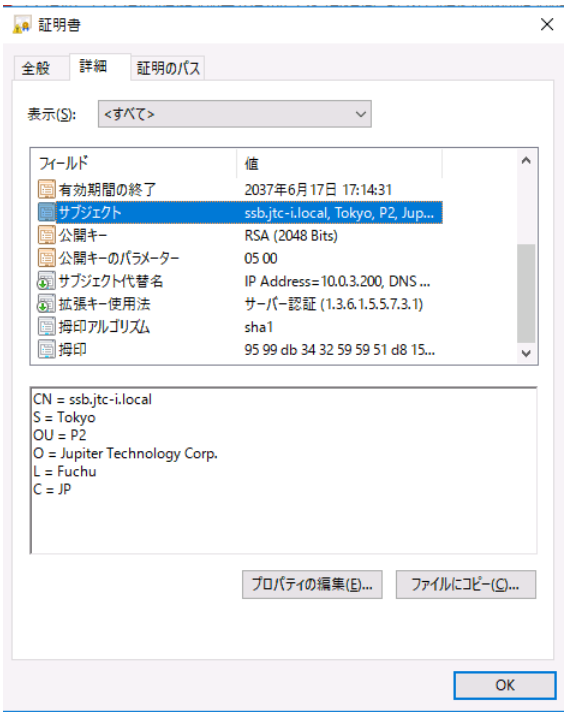
注意:

サーバー証明書の CN(Common Name)を[Server Name or Address(IPv4)]フィールドに設定します。

CN(Common Name)と[Server Name or Address(IPv4)]の値が一致してなければなりません。異なる場合、syslog-ng Agent for Windows はサーバー証明書が不正と認識し、通信を切断します。

また、[Server Name or Address(IPv4)]に設定した値が、サーバー名の場合は、Windows クライアントが IP アドレスを DNS または hosts ファイルで名前解決できている必要があります。

Figure 18 サーバー証明書の CN



4. （オプション手順：）必要に応じて、[Advanced Options]のオプションを設定します。
5. [OK]をクリックします。
6. syslog-ng Agent for Windows のサービスを再起動します。

日本語マニュアル発行日　2017 年 7 月 4 日

ジュピターテクノロジー株式会社 技術グループ