cybertrust

中間CA証明書　設定変更手順書(Microsoft IIS)

はじめに

【！】本手順書をご利用の前に必ずお読みください

1. 本ドキュメントは、「Microsoft IIS 6.0～8.5」の環境下で**「SureServer[SHA-2]」をクロスルート設定でご利用いただいており、3階層設定へ変更する手順について解説するドキュメント**です。
2. 実際の手順はお客様の環境により異なる場合があり、Microsoft IISの動作を保証するものではございません。あらかじめご了承ください。
3. このドキュメントは予告なく変更される場合があり、サイバートラスト株式会社はその内容に対して責任を負うものではありません。また、このドキュメント内に誤りがあった場合、サイバートラスト株式会社は一切の責任を負いません。
4. このドキュメントで説明するソフトウェアはライセンスに基づいて配布されるものであり、ライセンスの条項に従った使用のみ許可されます。このドキュメントは、本来の使用目的のために発行され、公に発行されるものではありません。
5. このドキュメントの一部または全部を複製することは禁じられており、提供または製造を目的として使用することはできません。ただし、サイバートラスト株式会社との契約または同意文書で定められている場合に限り、この注記の添付を条件として複製することができます。
6. サイバートラスト株式会社から事前に書面による合意を得ない限り、このドキュメントまたはその一部から直接的または間接的に知り得た内容または主題に関して、個々の企業やその従業員などの第三者に対し、口頭、文書、またはその他のいかなる手段によっても伝達することはできません。

クロスルート証明書の削除手順（Microsoft IIS）

1. **Microsoft IISが稼働しているWindows Server上で「Microsoft 管理コンソール (MMC)」を起動します。**

A) スタートメニュー（Windowsボタン）から【ファイル名を指定して実行】をクリックします。

B) 【名前】へ「mmc」と入力して【OK】をクリックし、MMC を開きます。

C) MMC 画面左上の【ファイル】メニューをクリックし、【スナップインの追加と削除】をクリックします。

D) **[IIS6.0の場合のみ]**：【追加】ボタンをクリックします。

E) 【利用できるスナップイン】から【証明書】を選択し、【追加】をクリックします。

F) 【コンピュータアカウント】を選択し、【次へ】をクリックします。

G) 【ローカルコンピュータ（このコンソールを実行しているコンピュータ）】を選択し、【完了】をクリックします。

H) 【選択されたスナップイン】に【証明書（ローカルコンピュータ）】が追加されていることを確認し、【OK】をクリックします。

I) コンソールルートへ【証明書（ローカルコンピュータ）】が追加されたことを確認します。

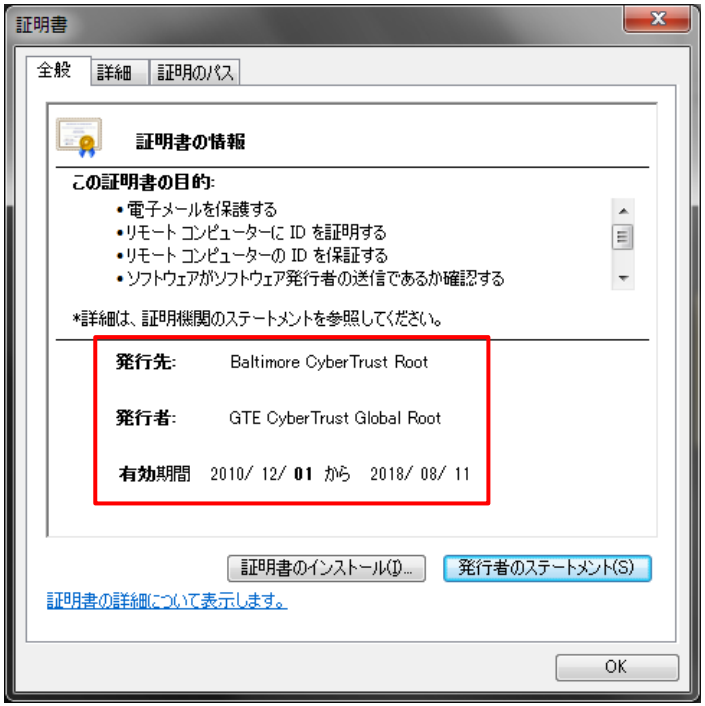
クロスルート証明書の削除手順（Microsoft IIS）

2. クロスルート証明書を削除します。

A) 【証明書(ローカルコンピュータ)】→【中間証明機関】→【証明書】の順にクリックします。

B) 発行先が「Baltimore CyberTrust Root」の証明書をダブルクリックして、以下の内容であることを確認します。

・発行先：Baltimore CyberTrust Root
・発行者：GTE CyberTrust Global Root
・有効期間：2010/ 12/ 01 から 2018/ 08/ 11



C) 右記のクロスルート証明書を右クリックして、【削除】を選択します。

D) 証明書削除に関するメッセージが表示されますので、【はい】をクリックします。

E) 削除が完了しますので、MMCの画面を閉じます。

3. 以下の手順で設定を反映させます。

・IIS6.0

WEBサイトの再起動(起動/停止)を行ってください。

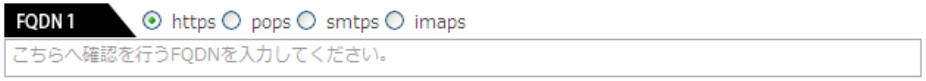
・IIS7.0～

証明書のバインド設定で現在設定されている証明書を再選択します。
※反映されない場合はWEBサイトの再起動(起動/停止)を行ってください。

クロスルート証明書の削除手順（Microsoft IIS）

4. 下記「SSLサーバ証明書　導入サポートツール」のURLへ接続します。
   https://sstool.cybertrust.ne.jp/support_tool/index01.php

5. 設定確認を行うFQDNを以下の欄へ入力して、「設定を確認する」ボタンをクリックします。



6. 下記メッセージと情報が表示されることを確認してください。

■確認項目

1. 「SureServer[SHA-2]が従来方式（3階層）で正しく設定されています。」というメッセージが表示されることを確認します。

2. 中間CA証明書1の「署名アルゴリズム」が「sha256WithRSAEncryption」と表示されていることを確認します。

確認は以上となります。

エラーメッセージが表示された場合は、表示されたメッセージに従い、再設定を行ってください。