

技術ノート KGTN 2013072501

現象

[SSL] SSL サーバ証明書に中間 CA 証明書が必要な場合、その中間 CA 証明書はどうやってインストールするのか？

説明

SSL サーバ証明書のファイルを **server.crt** , 1つ上の中間 CA 証明書のファイルを **ica1.crt** , さらにその上の中間 CA 証明書のファイルを **ica2.crt** とします. この条件で, 以下の手順で新たな SSL サーバ証明書を作成して下さい.

- 1) SSL サーバ証明書 **server.crt** をコピーし **server-org.crt** を作る (元の証明書の保存) .
- 2) メモ帳で **server.crt** を開く.
- 3) 新たなメモ帳で1つ上の中間 CA 証明書 **ica1.crt** を開く.
- 4) メモ帳で開いた **ica1.crt** の内容を, 上記 2 のメモ帳の末尾にペーストする.
- 5) 上記 3 のメモ帳を「保存しない」で閉じる.
- 6) 新たなメモ帳でさらにその上の中間 CA 証明書 **ica2.crt** を開く.
- 7) メモ帳で開いた **ica2.crt** の内容を, 上記 2 のメモ帳の末尾にペーストする.
- 8) 上記 6 のメモ帳を「保存しない」で閉じる.
- 9) 上記 3 のメモ帳を「保存する」で閉じる (上書き保存) .

この手順で作成した (新しい) SSL サーバ証明書のファイル **server.crt** をクラスタマネージャで指定して下さい. なお, ファイルの **COPY** コマンドでも同じことが出来ませんが, 改行コードの問題等が未然に分かるように, メモ帳での作成をお勧めします.

補足1

簡単に言えば, 以下のように SSL サーバ証明書, 1つ上の中間 CA 証明書, さらにその上の中間 CA 証明書を (テキストとして) 結合し保存して下さい.

```
-----BEGIN CERTIFICATE-----  
SSL サーバ証明書の内容  
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----  
1つ上の中間 CA 証明書の内容  
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----  
さらにその上の中間 CA 証明書の内容  
-----END CERTIFICATE-----
```

補足2

iOS Client および Android Client を使用する場合は、中間証明書だけでなくルート証明書も結合して下さい (つまり全ての証明書を、サーバ証明書 → 中間 CA 証明書 → ルート証明書の順に結合する)。これに加え、初回 iOS Client または Android Client から接続する時に表示される SSL の警告ダイアログで、先ず **View Certificate** ボタンをクリックし、次に **Install Certificate** ボタンをクリックして下さい。これで SSL の環境が整い、2 回目の接続から SSL の警告ダイアログが表示されなくなります。

The image shows a screenshot of an SSL warning dialog box. The dialog is split into two main sections. The left section contains a warning message and three status indicators. The right section displays certificate details and buttons for installation and confirmation.

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

- The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
- The security certificate date is valid.
- The security certificate matches the name of the page you are trying to view.

Do you want to proceed?

Yes **No** **View Certificate**

Issued to: ██████████.jp
Issued by: Cybertrust Japan Public CA G2
Valid from: Jul 22 07:09:48 2013 GMT
Valid to: Aug 22 14:59:00 2013 GMT

Certificate
Data
Version
Serial Number
Signature Algorithm

Install Certificate **OK**

Last reviewed: Aug 22, 2013
Status: DRAFT
Ref: CASE#37808
Copyright © 2013 kitASP Corporation