「シン・テレワークシステム HTML5 版 Web クライアント用 Web サーバー」における SSL クライアント証明書認証で OU 値条件を設定する方法のサンプルメモ

作成: 2021/09/22 登

- 概要
  - ある 1 つの CA (認証局) によって、多数のクライアント証明書が発行されているとする。これらは、色々な組織向けに発行されているが、すべて単一の CA によって発行されているとする。
  - それらのクライアント証明書の Subject フィールドの「OU」の値によって、組織を識別することが意図されているとする。
  - この場合において、シン・テレワークシステム HTML5 版 Web クライアント用 Web サーバーでは、クライアントが提示した証明書が、以下の条件に「すべて」合致する場合にのみ、認証に成功させたい、という需要がある。
    - 上記の CA によって、そのクライアント証明書が発行 (署名) されていること。
    - **クライアント証明書の Subject フィールドの「OU」の値が、例: OU=Neko, OU=ABC, OU=DEF, ... のようになっており、2 つ目の OU の値と 3 つ目の OU の値の文字列がそれぞれ "ABC", "DEF" に完全一致すること。**
    - クライアント証明書の期限が有効期限内であること。
  - そこで、本メモでは、上記を実現する条件式を記載する方法について述べる。

- 実装方法
  1. ここでは、例として、ある 1 つの商用認証局の CA「CN = Cybertrust DeviceiD Public CA G3isr, O = Cybertrust Japan Co.,Ltd., C = JP」によって発行された証明書を例にとって議論する。
  2. まず、上記 CA の証明書ファイルを、HTML5 版 Web サーバーをインストールした場所において、「IPA-DN-ThinApps-Private/Vars/VarResources/VarResources/ThinWebClient_ClientCertAuth_SampleCerts/210921_CyberTrust_Device_ID_Public_CA_G3isr_Root_Cert/210921_CyberTrust_Device_ID_Public_CA_G3isr_Root_Cert.cer」
というファイル名で保存する。
なお、上記 CA の証明書ファイルは、その名の通り、「公開鍵」であり、秘密情報を含まないことから、「210921_CyberTrust_Device_ID_Public_CA_G3isr_Root_Cert.cer」という名前で、この PPT が置いてある「210922_ThinTelework_CertAuth_with_Subject_OU_Values」ディレクトリの「Files」サブディレクトリに置いておいた。
  3. 次に、マニュアル「9-12」および右記の cs ファイルのコメントを参考にして、この PPT ファイルが置いてある「210922_ThinTelework_CertAuth_with_Subject_OU_Values」ディレクトリの「Configs/README.md」ファイルのとおりに、Vars.cs ファイルを編集し、前頁の条件を定義する条件式を、Vars.cs にスクリプトとして記述する。
  4. マニュアル「3B-6」、「4B-6」に従い、ソースコードを改変した後のリビルドを実施する。
  5. HTML5 版 Web クライアント用 Web サーバーが再始動したら、意図した挙動になっていることを確認する。