RADIUSクライアント証明書認証

RADIUSサーバにおいてクライアント証明書を用いた認証を行う設定のサンプルです。

FreeRADIUS自体にもクライアント証明書を用いた認証を行う機能がありますが、特定のCAから発行された証明書であるかどうかを確認する程度で、証明書の細かな情報に基づいた認証可否の制御を行うためには、外部スクリプトで認証判断を実現する必要があります。ここでは、その例を紹介します。

あくまでもサンプルであり、実際に意図通り動作するかどうか、各自で検証を行ってから運用に投入してください。

設定例

認証スクリプトの呼び出し

raddb/mods-enabled/eapファイル中の外部プログラム呼び出しの記載を以下のようにします。

```
client = "/usr/local/etc/raddb/CA/VERIFY.sh %{TLS-Client-Cert-Filename}"
```

証明書はテンポラリファイルの形でスクリプトに渡されます。

認証スクリプトの記述

VERIFY.shの中身は以下のような内容になります。

```
#! /bin/sh

CRL_URI=http://repo1.secomtrust.net/sppca/nii/odca3/fullcrlg4.crl
CRL_FILE=fullcrlg4.crl
CRL_DIR=/tmp

# Subject matching
openssl x509 -subject -noout -in ${1} |\
grep -q '^subject= /C=JP/L=Academe/O=National Institute of Informatics/' || exit 1

# Issuer matching
openssl x509 -issuer -noout -in ${1} |\
grep -q '^issuer= /C=JP/L=Academe/O=National Institute of Informatics/CN=NII Open Domain CA - G4' || exit 1

# Purpose matching
openssl x509 -purpose -noout -in ${1} |\
grep -q 'SSL client : Yes' || exit 1

# Downloading CRL should be done by CRON daily or weekly
#wget -q -P $CRL_DIR -N $CRL_URI

# CRL lookup
SERIAL=`openssl x509 -serial -noout -in ${1} | sed 's/serial=//'`
openssl crl -inform der -in $CRL_DIR/$CRL_FILE -text | grep 'Serial Number:' |\
grep -q $SERIAL && exit 1

exit 0
```

実際に証明書にどのように記載されているか、openssslがどのような出力を生成するかを確認しながら、記述を修正してください。

CA証明書の厳密な確認や証明書の有効期限切れのチェックも追加する必要があるでしょう。