NRA

FreeRADIUS 設定手順

2022年1月14日

Ver. 1.00

改訂履歴

| 版 | 日付 | 内容 | 備考 |
|--------------|-----------|------|----|
| Ver. 1.00 | 2022/1/14 | 初版作成 | |

<目 次>

| 1. 概要 | |
|--------------------|---|
| 2. 事前準備 | 4 |
| 3. 設定手順 | 5 |
| 3.1. AP からのアクセスを許可 | 6 |
| 3.2. 証明書ファイルの配置 | 7 |
| 3.3. 失効リストの設定 | 8 |
| 3.4. EAP-TLS 認証の設定 | 9 |
| 4. appendix | |
| 4.1. PEM 形式のルート証明書 | |
| 4.2. ログの設定 | |

1. 概要

本書ではEAP-TLS認証方式を用いたWi-Fi接続時のクライアント証明書認証の設定手順について説明致します。

説明範囲は認証に必要な FreeRADIUS における設定手順になりますので、その他の設定については割愛させていただきます。

※AWS 上の Linux サーバに FreeRADIUS (Version 3.0.13)をインストールし検証した結果を元に作成して います



【構成と接続イメージ】

2. 事前準備

■ FreeRADIUS をインストール済みのサーバ

■AP(アクセスポイント)

本書では設定手順は割愛させていただきます。

■SSL サーバ証明書

インストールする際には PEM 形式に変換した証明書と秘密鍵のファイルが必要になります。

■ルート証明書

インストールする際には PEM 形式に変換する必要があります。 ※作成方法については、p14「4.1. PEM 形式のルート証明書」をご確認ください

■クライアント証明書

ご利用する端末にインストールしてください。

3. 設定手順

本項から詳細な設定手順に関する説明になります。 流れは次の通りです。

| 6 | 3.1. AP からのアクセスを許可 |
|---|---|
| | AP から RADIUS サーバへのアクセスを許可する設定をします。 |
| 7 | 3.2. 証明書ファイルの配置 |
| | 失効確認をするための失効リストの設定をします。※失効確認をしない場合はスキップ |
| 8 | 3.3. 失効リストの設定 |
| | 失効確認をするための失効リストの設定をします。※失効確認をしない場合はスキップ |
| 9 | 3.4. EAP-TLS 認証の設定 |
| | EAP-TLS 認証の設定をします。 |

項目は以上です。次ページから各項目の説明の記載になります。

3.1. AP からのアクセスを許可

APから RADIUS サーバへのアクセスを許可します。対象のファイルを【設定内容】を参考に変更して下さい。

【対象ファイルパス】

/etc/raddb/clients.conf

【設定内容】

client private-network-1(241 行目付近)の{}内を以下の通り変更

ipaddr = $x.x.x.x/x \approx 1$

secret = xxxx 💥 2

APのIPを指定します

②任意の値を設定します (secret は AP 側でも設定が必要な共有キーになります)

【設定例】

You can now specify one secret for a network of clients.

- # When a client request comes in, the BEST match is chosen.
- # i.e. The entry from the smallest possible network.

#

| client private-network-1 { | —241 行目付近 | | |
|-----------------------------|-----------------|--|--|
| ipaddr | = 0.0.0/0 —1 | | |
| secret | = testing123 —2 | | |
| } | | | |
| | | | |
| #client private-network-2 { | | | |

ipaddr = xxx.xxx.xxx/xx
secret = testing123-2
#}
~~~~ (以下省略)

# 3.2. 証明書ファイルの配置

サーバ証明書、ルート証明書を配置します。ファイル名は任意の値に変更可能です。本書では以下ファイル 名にて説明いたしますが、設定時は任意で設定した値に置き換えてください。

■サーバ証明書ファイル

/etc/raddb/certs/server.pem

■サーバ証明書の秘密鍵ファイル

/etc/raddb/certs/server.key

■ルート証明書ファイル

/etc/raddb/certs/ca.pem

# 3.3. 失効リストの設定

本項目ではクライアント証明書の失効確認を行う失効リスト(CRL)を設置します。

(必要がなければ本項目はスキップしてください)

失効リストは PEM 形式にてルート証明書と結合する必要があり、かつ定期的に更新する必要があるので cron で以下の様なスクリプトを設定してください。

一度実行を試し、/etc/raddb/certs に ca\_crl.pem が作成されている事を確認してください。

【スクリプト例】 #!/bin/sh cd /etc/raddb/certs rm -f cdp.crl rm -f crl.pem wget 'http://mpkicrl.managedpki.ne.jp/mpki/NipponRACertificationAuthority4/cdp.crl' openssl crl -inform der -in cdp.crl -outform pem -out crl.pem cat ca.pem crl.pem > ca\_crl.pem systemctl restart radiusd

## 3.4. EAP-TLS 認証の設定

EAP-TLS 認証の設定をします。

(1)eap ファイルを【設定内容】を参考に変更して下さい。

【ファイルパス】

/etc/raddb/mods-available/eap

【設定内容】

tls-config tls-common (172 行目付近)の{}内を以下の通り変更

-----

private\_key\_file = /etc/raddb/certs/server.key ※2

certificate\_file = /etc/raddb/certs/server.pem X3

ca\_file = /etc/raddb/certs/ca\_crl.pem ※④

check\_crl = yes  $\times$ 5

check\_cert\_issuer = "/C=JP/O=Nippon RA Inc./CN=Nippon RA Certification Authority 4" <u>\*6</u>

①サーバ証明書のパスワード (xxxx の部分は証明書パスワードに置き換えてください)

2秘密鍵のパス (3.3. 証明書ファイルの配置にて配置したパスを記載してください)

③サーバ証明書のパス (3.3. 証明書ファイルの配置にて配置したパスを記載してください)

④ルート証明書+失効リストのパス (失効確認しない場合は、ca\_crl.pem の部分を ca.pem に置き換えて ください)

⑤失効リストのチェック (失効確認をしない場合は no)

6 クライアント証明書発行者のチェック

#### 【設定例】

#### ~~~~(省略)

- # If ca\_file (below) is not used, then the
- # certificate\_file below MUST include not
- #  $\,$  only the server certificate, but ALSO all  $\,$
- # of the CA certificates used to sign the
- # server certificate.

~~~~ (省略)

- # In general, you should use self-signed
- # certificates for 802.1x (EAP) authentication.
- # In that case, this CA file should contain
- # *one* CA certificate.
- #

~~~~ (省略)

- # Check the Certificate Revocation List
- #
- # 1) Copy CA certificates and CRLs to same directory.
- # 2) Execute 'c\_rehash <CA certs&CRLs Directory>'.
- # 'c\_rehash' is OpenSSL's command.
- # 3) uncomment the lines below.
- # 5) Restart radiusd

check\_crl = yes 一⑤ 281 行目付近

~~~~ (省略)

- # In 2.1.10 and later, this check can be done
- # more generally by checking the value of the
- # TLS-Client-Cert-Issuer attribute. This check
- # can be done via any mechanism you choose.

#

```
check_cert_issuer = "/C=JP/O=Nippon RA Inc./CN=Nippon RA Certification Authority 4" 一⑥ 300 行目付近 ~~~~ (以下省略)
```

(2)tls ファイルを【設定内容】を参考に変更して下さい。【ファイルパス】

/etc/raddb/sites-available/tls

【設定内容】

tls (83 行目付近)の{}内を以下の通り変更

private_key_file = /etc/raddb/certs/server.key ※2

certificate_file = /etc/raddb/certs/server.pem X3

ca_file = /etc/raddb/certs/ca_crl.pem ×4

check_crl = yes \times 5

check_cert_issuer = "/C=JP/O=Nippon RA Inc./CN=Nippon RA Certification Authority 4" ×6

①サーバ証明書のパスワード (xxxx の部分は証明書パスワードに置き換えてください)

2秘密鍵のパス (3.3. 証明書ファイルの配置にて配置したパスを記載してください)

③サーバ証明書のパス (3.3. 証明書ファイルの配置にて配置したパスを記載してください)

④ルート証明書+失効リストのパス (失効確認しない場合は、ca_crl.pem の部分を ca.pem に置き換えて ください)

⑤失効リストのチェック (失効確認をしない場合は no)

6 クライアント証明書発行者のチェック

```
【設定例】
```

```
tls {
                                                 —83 行目付近
         private_key_password = 1234 —1
         private key file = /etc/raddb/certs/server.key -2
~~~~ (省略)
# If ca_file (below) is not used, then the
# certificate_file below MUST include not
# only the server certificate, but ALSO all
```

- # of the CA certificates used to sign the
- # server certificate.

~~~~ (省略)

- # This parameter is used only for EAP-TLS,
- # when you issue client certificates. If you do
- # not use client certificates, and you do not want
- # to permit EAP-TLS authentication, then delete
- # this configuration item.

ca file = /etc/raddb/certs/ca crl.pem -④ 114 行目付近

~~~~ (省略)

```
# Check the Certificate Revocation List
```

- #
- # 1) Copy CA certificates and CRLs to same directory.
- # 2) Execute 'c_rehash <CA certs&CRLs Directory>'.
- 'c_rehash' is OpenSSL's command. #
- # 3) uncomment the line below.
- # 5) Restart radiusd

 $check_crl = yes$ —⑤ 162 行目付近

ca_path = \${cadir}

~~~~ (省略)

- # In 2.1.10 and later, this check can be done
- # more generally by checking the value of the
- # TLS-Client-Cert-Issuer attribute. This check
- # can be done via any mechanism you choose.

#

```
check_cert_issuer = "/C=JP/O=Nippon RA Inc./CN=Nippon RA Certification Authority 4" 一⑥ 177 行目付近
~~~~(以下省略)
```

#### ■補足

クライアント証明書認証において会社名英字表記でアクセスを制限をする場合は、tls ファイルと eap ファイルの check\_cert\_issuer =の下に check\_cert\_o =を追加してください。

【設定内容】

check\_cert\_o = "会社名英字表記"

【O(会社名英字表記)の値の確認方法(WindowsPCの場合)】

「certmgr.msc」を実行し、「個人」-「証明書」にて対象の証明書を選択します。

証明書をダブルクリックで開き、詳細タブのサブジェクト欄をご確認ください。

| 😱 証明書 X                                                                                                             |                              |  |  |  |  |
|---------------------------------------------------------------------------------------------------------------------|------------------------------|--|--|--|--|
| 全般詳細証明のパス                                                                                                           |                              |  |  |  |  |
|                                                                                                                     |                              |  |  |  |  |
| 表示(S): <すべて>                                                                                                        | ~                            |  |  |  |  |
| フィールド                                                                                                               | 値 ^                          |  |  |  |  |
| [5] バージョン                                                                                                           | V3                           |  |  |  |  |
| □□ シリアル番号                                                                                                           | 13e59b                       |  |  |  |  |
|                                                                                                                     | sha256RSA                    |  |  |  |  |
| 📴 署名ハッシュ アルゴリズム                                                                                                     | sha256                       |  |  |  |  |
| 2 発行者                                                                                                               | Nippon RA Certification Auth |  |  |  |  |
| [ 有効期間の開始                                                                                                           | 2022年1月6日 11:25:40           |  |  |  |  |
| 📴 有効期間の終了                                                                                                           | 2027年2月6日 11:25:00           |  |  |  |  |
| ■ サブジェクト                                                                                                            | sample-taro@nrapkijp, sam    |  |  |  |  |
| □ 公開キー                                                                                                              | RSA (2048 Bits)              |  |  |  |  |
| E = sample-taro@nrapki.jp<br>CN = sample taro<br>OU = RBSF99E37B650DEF4CEC741C9C5D9D751CA8390E<br>O = NRA<br>C = JP |                              |  |  |  |  |
|                                                                                                                     | プロパティの編集(E) ファイルにコピー(C)      |  |  |  |  |
|                                                                                                                     | ОК                           |  |  |  |  |

#### 【設定例】

~~~~ (省略)

- # In 2.1.10 and later, this check can be done
- # more generally by checking the value of the
- # TLS-Client-Cert-Issuer attribute. This check
- # can be done via any mechanism you choose.

#

check\_cert\_issuer = "/C=JP/O=Nippon RA Inc./CN=Nippon RA Certification Authority 4"

```
check_cert_o = "NRA"
```

```
~~~~(以下省略)
```

# 4. appendix

### 4.1. PEM 形式のルート証明書

以下、弊社 HP のレポジトリにて公開するルート証明書を PEM 形式にした内容です。 テキストファイルヘコピー&ペーストし、本手順を例に、"ca.pem"というファイル名で、 /etc/raddb/certs/に配置します。(ファイル名は任意の値に変更可能です)

----BEGIN CERTIFICATE----

MIIDazCCAlOgAwIBAgIBATANBgkghkiG9w0BAQsFADBXMQswCQYDVQQGEwJKUDEX MBUGA1UEChMOTmlwcG9uIFJBIEluYv4xLzAtBgNVBAMTJk5pcHBvbiBSQSBSb290 IENIcnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTExMDgxNTAyMzAyNloXDTMxMDgx NTAyMjg1NlowVzELMAkGA1UEBhMCSlAxFzAVBgNVBAoTDk5pcHBvbiBSQSBJbmMu MS8wLQYDVQQDEyZ0aXBwb24gUkEgUm9vdCBDZXJ0aWZpY2F0aW9uIEF1dGhvcmI0 eTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPRqqsUWzgB38ZMi7aeT  $Thq\,i\,jKzqBaNOUWL9Czhb30b/L\,i\,5KEQr\,Az2Peg0wZns6b+F/4QE2H2g\,I\,9k4qBe8dh$ Arlns9tSIH6N6/rDg625rCGKj9cAiOizis2gyTptmcgMffENQI6dcDxviuCY98dG 8ITMWxKucza/rCVt5KBC5Uh17AgPA1j5vPgXnDn9vnwV04sYqoXXa7ZRgYFc+g/h pM/lqWFze1gtGLBvEnYIgyd3cbVE0mMwc15NNaCcSFJbr2p/P/KA9xEmot768M5f 5NTIW/Cg6LJ/bm/byu8H2jhjpQEdY35rDS0ip20mqEJy51nWbUMqMV2SesPouVjv x5UCAwEAAaNCMEAwDwYDVROTAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAcYwHQYD VR00BBYEFBmZpk3iL3keW05k2YDn98mwn3I0MA0GCSqGSIb3DQEBCwUAA4IBAQCX Meax614X08HFK/XWmzBmnXbU10XGigNK5CCmVXVM5tdVGSvSW8br9c+ZUGRca4cd 6cUA/4pIUILTqUb5T0w08+pw+egehYWeeVqoF7T5EWLps2HBv8+LoIPnXY/Btp88 teacCIQS5tiSbfuR3UDuCfGWtAUdmyG5jH60se9k/k+zLCvCh0hXGaQXAe0AnEIM n+oKqSQeSTbo7+7KxiqtjyZ2WerBqPgAFpJNu+PCpG1rXaPU87//PKqP9IYqk05h VGMOs8QNnWXVbVT0eJV79Ef5ZfbtWS8x20JYRALzbLKtu9wuFdlocL5dWeVL6QxS uWKINqU/oyG9yDKuoG5I

----END CERTIFICATE-----

# 4.2. ログの設定

RADIUS サーバにユーザからアクセスしたログを残す場合は、以下対象のファイルを【設定内容】を参考に変更して下さい。

【対象ファイルパス】

/etc/raddb/radiusd.conf

【設定内容】

Log (255 行目付近)の{}内を以下の通り変更

-----

\_\_\_\_\_

auth = yes  $\times$  1

auth\_badpass = yes  $\times (2)$ 

auth\_goodpass = yes  $\times$  3

①認証可否のログ出力

2認証失敗のログ出力

3認証成功のログ出力

#### 【設定例】

```
# Log authentication requests to the log file.
#
# allowed values: {no, yes}
#
auth = yes 一①※342 行目付近
# Log passwords with the authentication requests.
```

```
# auth_badpass - logs password if it's rejected
# auth_goodpass - logs password if it's correct
#
# allowed values: {no, yes}
#
auth_badpass = yes -2※350行目付近
auth_goodpass = yes -3
~~~~ (以下省略)
```