NRA

FreeRADIUS 設定手順

2025 年 01 月 22 日

Ver. 2.00

改訂履歴

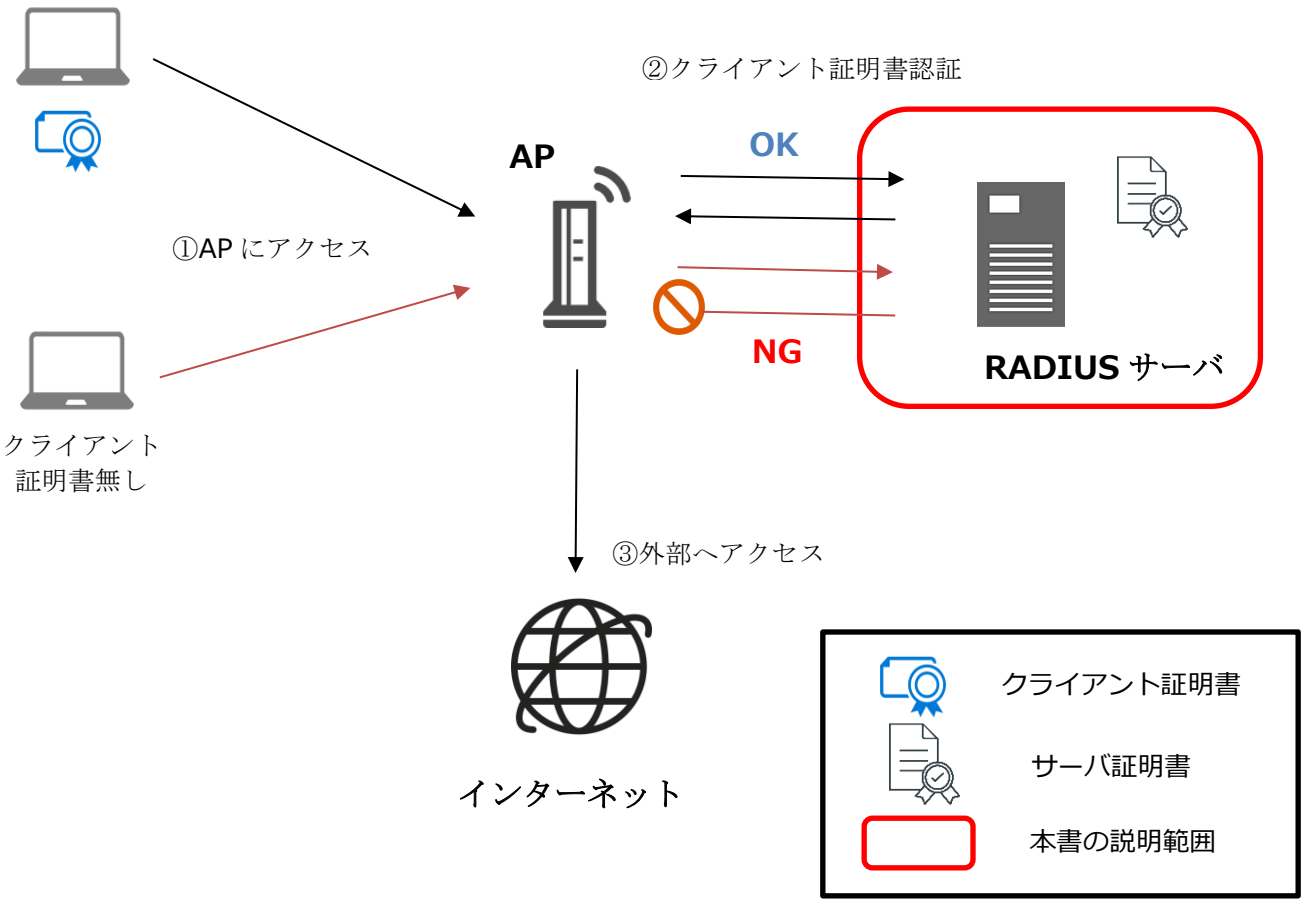
版	日　付	内　容	備　考
Ver. 1.00	2022/1/14	初版作成	
Ver. 2.00	2025/1/22	ルート、中間証明書および CRL を新認証局(G2)に変更	

<目　次>

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。

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　※①

secret = xxxx　※②

---

①AP 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                  = 0.0.0.0/0   —①
        secret                  = testing123   —②
}

#client private-network-2 {
#       ipaddr                  = xxx.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/NipponRACertificationAuthority4G2/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。

⑴eap 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_password = xxxx　※①

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

certificate_file = /etc/raddb/certs/server.pem　※③

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

check_crl = yes　※⑤

check_cert_issuer = "/C=JP/O=Nippon RA Inc./CN=Nippon RA Certification Authority 4 G2"　※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】

```
~~~~（省略）
tls-config tls-common {      ―172 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.
certificate_file = /etc/raddb/certs/server.pem      ―③ 186 行目付近

~~~~（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.
#
ca_file = /etc/raddb/certs/ca_crl.pem      ―④ 198 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 lines below.
#   5) Restart radiusd
check_crl = yes      ―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 G2"    ―⑥ 300 行目付近
~~~~（以下省略）
```

⑵tls 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_password = xxxx　※①

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

certificate_file = /etc/raddb/certs/server.pem　※③

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

check_crl = yes　※⑤

check_cert_issuer =　"/C=JP/O=Nippon RA Inc./CN=Nippon RA Certification Authority 4 G2"　※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.
certificate_file = /etc/raddb/certs/server.pem        —③ 97 行目付近

~~~~（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 G2"    —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。

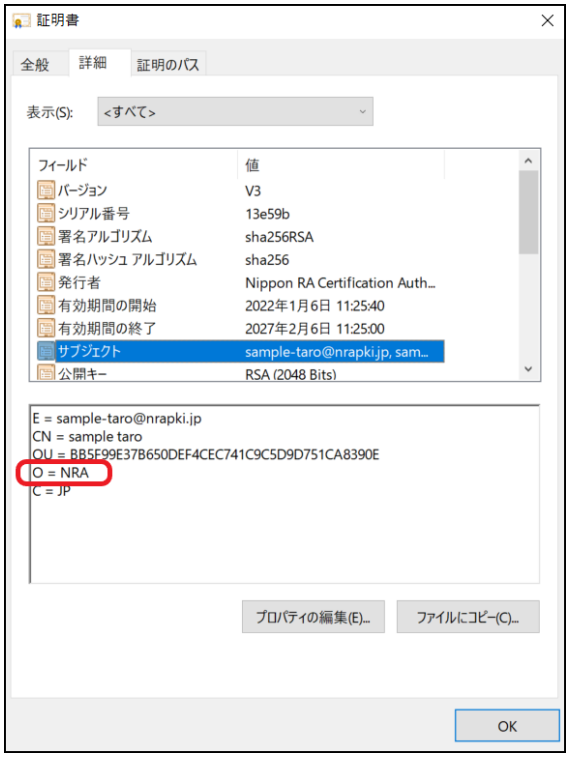
【設定内容】

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。



【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 G2"

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。
テキストファイルへコピー＆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-----
MIIFcTCCA1mgAwIBAgIBATANBgkqhkiG9w0BAQsFADBaMQswCQYDVQQGEwJKUDEX
MBUGA1UEChMOTmlwcG9uIFJBIEluYy4xMjAwBgNVBAMTKU5pcHBvbiBSQSBSb290
IENlcnRpZmljYXRpb24gQXV0aG9yaXR5IEcyMB4XDTI0MDgwMjAyMzMzOFoXDTQ0
MDkwMjAyMzMzOFowWjELMAkGA1UEBhMCSlAxFzAVBgNVBAoTDk5pcHBvbiBSQSBJ
bmMuMTIwMAYDVQQDEylOaXBwb24gUkEgUm9vdCBDZXJ0aWZpY2F0aW9uIEF1dGhv
cmlOeSBHMjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBALh9x9q92LDN
WhqWCqPtTgNLWgCWbOEnZXt4YY9oMBbxzKU6lpMixuHxdCv5Fcct+gNWE98VmRVz
7NjBzlOpUyzasjzWZLCIxacSJpxKKn3lIQorHsFKdEgYoelEbom/duj81c7r2ftP
9S3LpX776DQI6FeEvWfNkqdCcUBm79Geounn8mIH5Ub1JtBLRRHFiVcvKoq8UQQk
pdrRY22Nh3pOXqkOMRt/sVCLA9seZyaRm/aSALTK3OGMyN782H7dWHyhaZOed/cw
qKd5yBzWzCeBKLEz8xkoF3oztMArPdGpQr+tzlSpOeRuNuQP9POpxgPD3egbX+D/
GXQaQsaa+54yxjCIr/kAUi7273DooyAFGXnheRG7EsRu8mX5vRiJZPt1YZw2lCXu
sQmyWqOFch6Ve2jD9kc4IdoLezIz1/nwJu4jZaiWIyk7pIsT9jyL99kQhCfOQjAQ
wr+oxVafpAt7ejZcwOM8IH7KDQ32iCUCMWnFiaiyyhbRkuqEjtoOIXNN6dOBKmBx
bWOJJH2FBKHt6XhfDaGeDDiiE/iCnpSIf1UDjXkJvOI+rLWgg1PrpuOTgyJj7Rn7
X2RNRr2WE9bt1Db68RvMEzwWBEfJxZaQwYtaOWOf6iG+Ssr5deefoppyfhOOesrx
Bei2nkhlUG//TqkcBMMaFuox3ROJPwRFAgMBAAGjQjBAMA8GA1UdEwEB/wQFMAMB
Af8wDgYDVR0PAQH/BAQDAgHGMB0GA1UdDgQWBBQTrjzkvfDAcNazgpqjawHolkx2
fjANBgkqhkiG9w0BAQsFAAOCAgEAQithspZyjJ6jS8tZbVEQtMxS9dx8tHUfKb3l
N+P2D2KkLgF+lVKX2MY/+8/VhzYAIO/4kvHNbXFMco7Obtw37bumkCeCT4B8pZZe
Ao7ixh9m4OXBYWn7APvwXiBFOG4YEwmhS98jNxzOMj6GhuCOGeKbkUWbZxbNH9av
WGPHgFPQ5lqPBqW5glaOmLDPd+aInciJCtfNiB+cVqhrCs3OOuMsBPsLQeaoVFSc
6Apk1vOAjWArg1PFtvRfFalEzGLzdsxT/PYtX/5elxAlYbeBUF7GLyOSXtTG+P8V
DbpF7b9OKmvEx42b7ocOppWiIgZG76XtWuWFQ3Zo8Jzvt7plsPdO432EJSa+QmHB
xtph2Qv7L6jhM5ChVxifsLYu4F6n9Oij/ivwN5s+eo5okIel5CITUOgsd+mkiPdD
5eQgSExJpJ8F9kdtBXzozG9sczaSktr2xVYOsvgtMjIBdqyMU2bGwUpIrKn8IUwW
NphrJaTxAuQKF9qiFOvXTU/4igBHfkxOKO5JosJlvC1pkODOqAm9c34wV2bskOIx
tRyxgrZa4ley7y1Qa8eg5wwKbUik5Yj9rIEZ8/32nE7JBIOHSpOevXFA4cmg9oUX
Dzj3RXMYtDaemGZ6gTCxdV7Hi4L/OP+Zop99zY9aNAzQW2Msvizj2BrJTs7LpOKw
Vw8mcPU=
-----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　※①

auth_badpass = yes　※②

auth_goodpass = yes　※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   —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）
```