

FreeRADIUS Ver2.1.1 の設定例

エスアイアイ・ネットワーク・システムズ株式会社

FreeRADIUS Ver2.1.1 の設定例を以下に記載します。

この設定例は参考情報としてお取り扱いください。

FreeRADIUS Ver2.1.1 のインストール方法や設定の詳細は FreeRADIUS のドキュメント (<http://freeradius.org/>)をご参照ください。

なお、SmartCS NS2240 シリーズの設定例は取扱説明書「4.8 章 設定事例」に記載しております。そちらもあわせてご参照ください。

■ RADIUS サーバ情報

FreeRADIUS は以下で動作します。

動作 OS	各種 Linux、FreeBSD
設定方法	ファイル編集
Auth ポート番号	UDP 1812 (デフォルト) 変更可
Acct ポート番号	UDP 1813 (デフォルト) 変更可

■ クライアントの登録方法

・クライアント(SmartCS NS2240 シリーズ)とシークレットキーの登録

クライアントの情報を FreeRADIUS のクライアント定義ファイル(`clients.conf`)に登録します。FreeRADIUS の定義ファイルを`/etc/raddb`の下にインストールした場合は、クライアント定義ファイルは`/etc/raddb/clients.conf`となります。

この設定ファイルに SmartCS NS2240 シリーズの IP アドレスとシークレットキー、ショートネーム(装置名)、`nastype` を登録します。`nastype` は `other` を設定します。シークレットキーは SmartCS NS2240 シリーズに登録したキーと同じものを設定します。

```
client 192.168.1.1 {
    secret      = network
    shortname   = SmartCS1
    nastype     = other
}
client 192.168.1.2 {
    secret      = network
    shortname   = SmartCS2
```

```
nastype    = other
}
```

■ 認証ユーザの登録方法

・ユーザの登録

ユーザ情報を FreeRADIUS のユーザ定義ファイル(users)に登録します。

FreeRADIUS を/etc/raddb の下にインストールした場合は、クライアント定義ファイルは/etc/raddb/users となります。

下記はアクセスグループ機能利用時のポートユーザの登録例です。

```
tanaka      Cleartext-Password := "abc"
             Filter-Id = "PortGrp"

suzuki      Cleartext-Password := "def"
             Filter-Id = "PortGrp" ,
```

・複数 Filter-Id アトリビュートの登録

複数の Filter-Id アトリビュートを登録する場合は2行目以降に"+=(追加)"を設定します。

下記はポートユーザと装置管理ユーザの権限を与えた場合の登録例です。

```
sato        Cleartext-Password := "xyz"
             Filter-Id = "PortGrp" ,
             Filter-Id += "admin"
```

■ 設定の反映

登録したクライアントやユーザを反映させるには以下のコマンドを実行して、radiusd を再起動させます。

```
# /etc/init.d/radiusd restart
```

■ 注意

- ・ Linux 上で FreeRADIUS を動作させる場合は FireWall を無効にするか、もしくは、RADIUS で使用するポート番号が通過できるように FireWall の設定を変更してください。

- Linux 上で FreeRADIUS を動作させる場合は SELinux を disable にするか、もしくは、SELinux の設定を変更してください。
- RADIUS の定義ファイル(users)にユーザを登録する場合は DEFAULT 行の前に登録してください。
- FreeRADIUS Ver2.X は Ver1.X と異なり、RADIUS の定義ファイル(users)に登録したユーザと同じ名前のユーザがシステムにも登録されている場合は、users ファイルに登録したパスワードではなく、システムに登録されているパスワードと比較されます。認証の順番は/etc/raddb/sites-available/default で変更することも可能です。詳細は FreeRADIUS のドキュメントを参照してください。

■ 補足情報

- エラーログ

エラーログは/var/log/radius/radius.log に保存されます。

接続ができない場合は上記ファイルを参照してエラーを確認してください。

- アクセスログの保管場所

アカウントログは/var/log/radius/radacct/にクライアント毎に保存されます。

アクセスログを確認する場合は上記ファイルを参照してください。

- デバッグモード

FreeRADIUS はデバッグモードで動作させることもできます。

RADIUS 認証ができない場合は実行モジュールに-X オプションを付けてデバッグモードで起動しトラブルシューティングしてください。

```
# /usr/sbin/radiusd -X
```

なお、SmartCS NS2240 シリーズ上で trace radius level 2 コマンドを実行すると、トラブルシューティングに有用な情報を収集することもできます。

このコマンドの詳細は取扱説明書ならびにコマンドリファレンスを参照してください。

以上