

eduroam Next Step

国立情報学研究所
オープンフォーラム2019

一步踏み込んだ運用へ

- 認証VLANによる学内無線LAN一元化
- eduroam CATによる、安全な設定の導入
- eduroamアクセスポイントマップ新バージョン

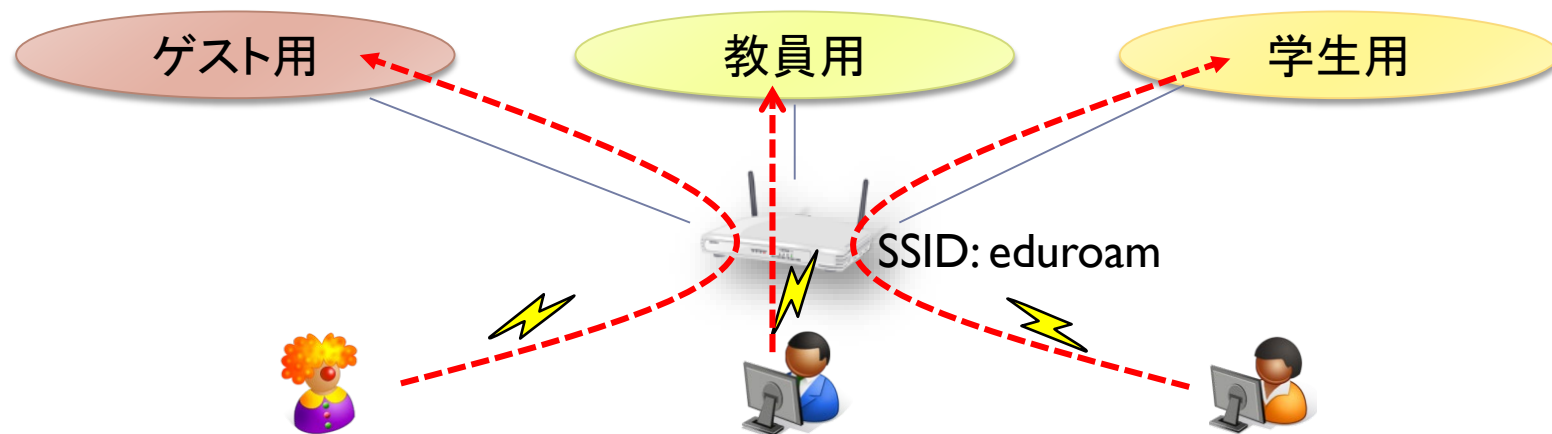
認証VLANのすすめ

eduroamを整備したけど.....

- こんな問題ありませんか？
 - 学生がeduroamばかり使う
 - 学内ネットより制限が緩やかだから.....
 - eduroamに接続していると学内システムが使えないという問い合わせが増えた
 - eduroamと学内ネットはセグメントを分離するのが基本
 - 学内専用のシステムはeduroamからアクセスできない
 - 学内利用者がゲスト用ネットワーク帯域を圧迫して訪問者から不満が.....

認証VLANのすすめ

- 学内無線LANをeduroamに一本化可能！
 - 訪問者と大学関係者をレームで区別
 - 大学関係者の場合は学内ネットワークのVLANに收容
 - 訪問者の場合はeduroam用ゲストネットワークのVLANに
 - 学生用と教職員用をさらに分離することもできる
 - 大学関係者はeduroamの設定だけすればよい
 - 学内では自動で学内ネットにeduroam経由で接続
 - 訪問先では通常のeduroamに接続



認証VLANのメリット

- ユーザが手動で接続先を変更する必要なし
 - 学内で接続すれば自動で学内ネットに！
 - 学内専用ポリシーを適用したネットワークに誘導
- 機関構成員は学内システムを利用できる
- 機関構成員はIPアドレス制限のかかった電子ジャーナル等も閲覧できる
 - 学内用IPアドレスを付与できる
- eduroam用ネットワークの帯域不足も解消
- 学内専用SSIDとeduroamの間で不用意に接続先が変わるトラブルがなくなり、利便性が向上する
- 複数の異なる無線ネットワークを管理運用するコストを削れる

認証VLANの導入

- 導入How Toを公開
 - <https://meatwiki.nii.ac.jp/confluence/x/zQaGAQ>
 - FreeRADIUSを対象
- たとえば学内ネットのVLAN番号が100なら
 - raddb/mods-config/attr_filter/post-proxyに追記

example.ac.jp(自機関のレルム)

Tunnel-Type := 13,

Tunnel-Medium-Type := 6,

Tunnel-Private-Group-Id := 100 (指定したい学内ネットVLAN番号)

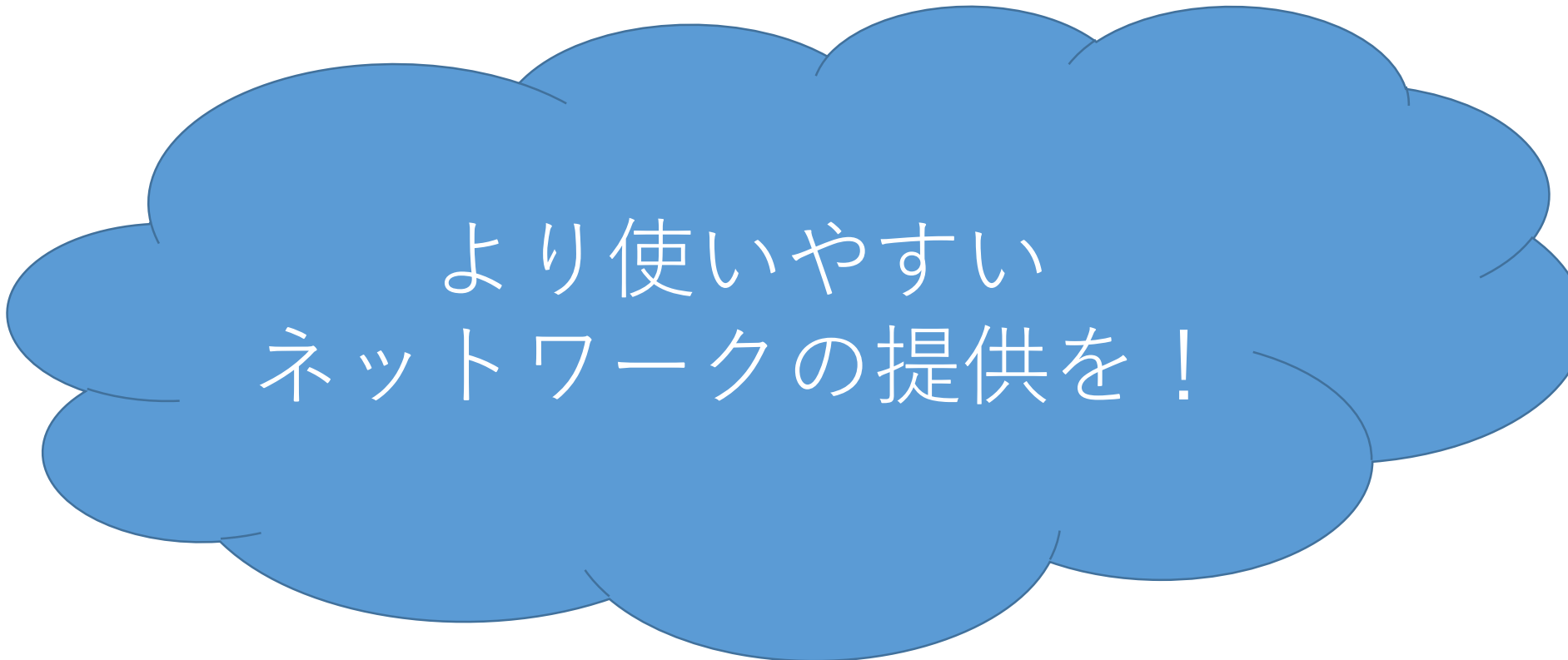
DEFAULT ※ここの定義に追記

(略) 最終行を継続行 (","をつける) にして以下を追加する

Tunnel-Type := 13,

Tunnel-Medium-Type := 6,

Tunnel-Private-Group-Id := 200 (指定したいeduroam用ネットVLAN番号)

A large, irregular blue cloud shape with a thin black outline, serving as a background for the central text.

より使いやすい
ネットワークの提供を！

eduroam CATのすすめ

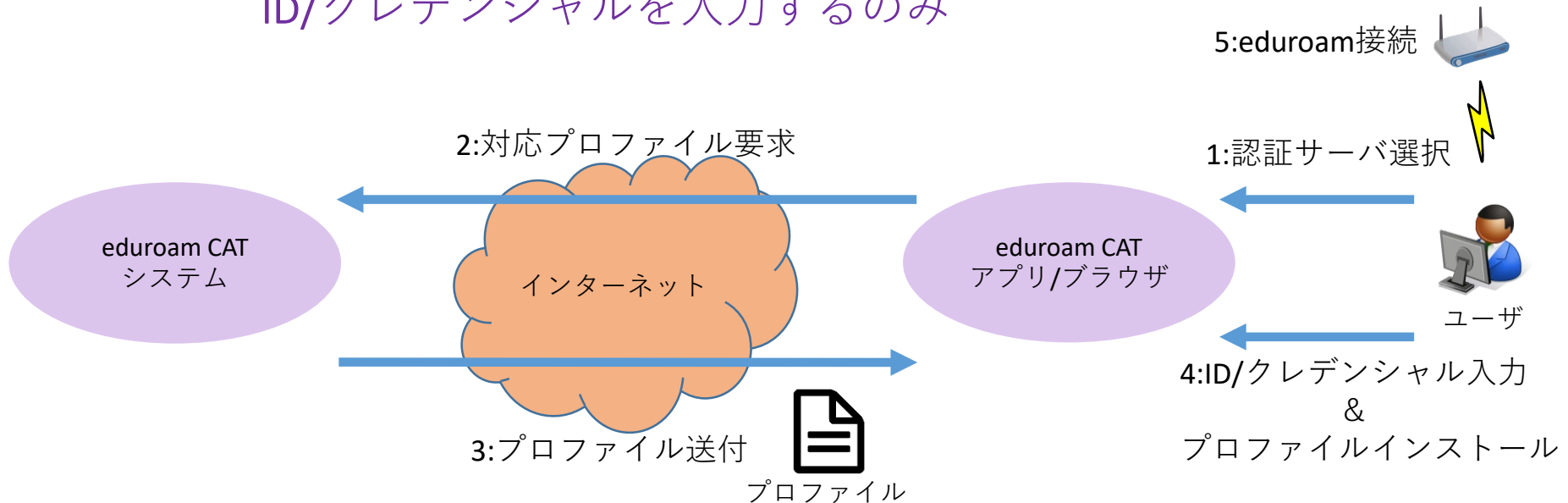
端末へのeduroam接続設定

- うまくつながらないことが.....
 - 認証方式の設定ミス
 - パスワード認証ならPEAP-MSCHAPv2にする必要が.....
 - クライアント証明書認証ならTLS
 - 認証サーバ証明書検証の設定ミス
 - 検証する証明書の設定を間違えた.....
 - 端末によっては証明書の指定ができない
- そもそも技術に明るくない学生や教職員には正確なeduroamの設定は厳しい！
 - 証明書検証を無視するとかならなんとか.....
 - 端末によっては認証方式の選択方法もよくわからない.....

そこで.....

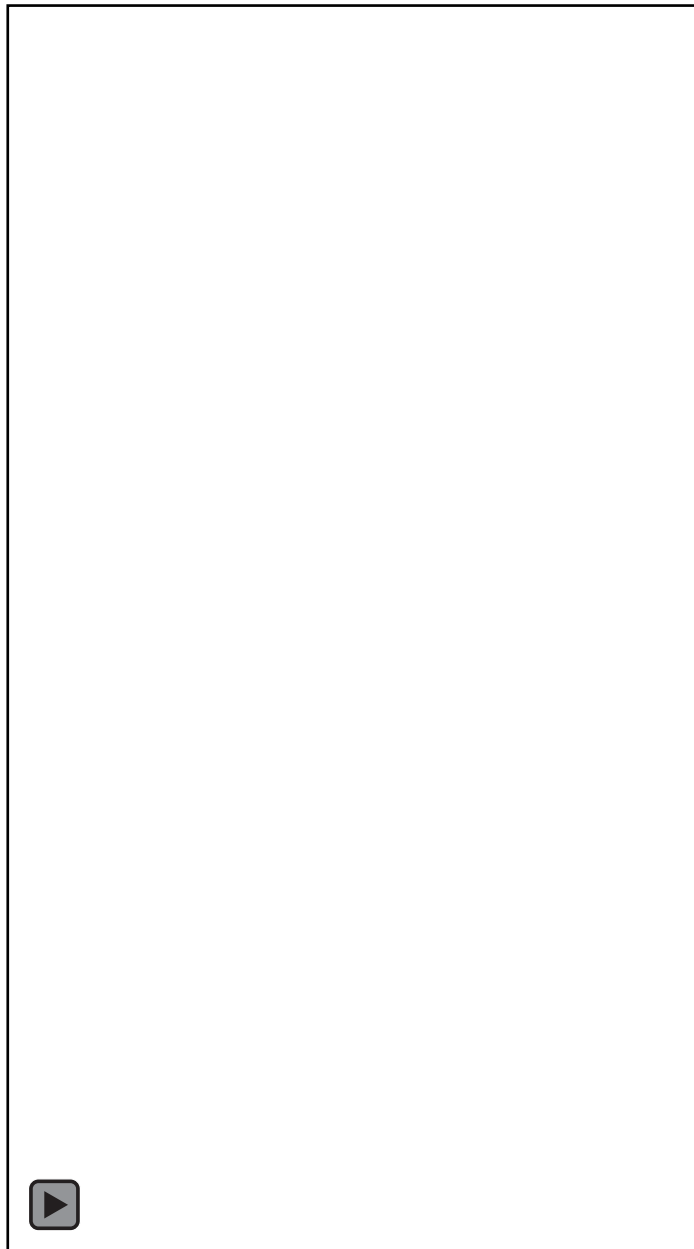
eduroam CAT

- GÉANTが提供するeduroam用設定半自動化ツール
 - CAT = Configuration Assistant Tool
 - 認証サーバごとにプロファイルを作成
 - プロファイル作成は各機関のeduroam運用担当者が行う
 - ユーザは自機関のプロファイルをCAT経由でインストールしてID/クレデンシャルを入力するのみ



eduroam CAT導入のメリット

- 複雑な設定を自動化
 - **技術に詳しくないユーザでも安全な設定に！**
 - 認証サーバの証明書検証をデフォルト化
 - 認証方式をあらかじめ指定
 - 端末によってはユーザの操作では指定できないものも
 - プロファイルとしてインストールすると指定可能
- 偽AP対策に有効
 - 認証サーバの証明書を検証するため偽APと繋がった偽サーバにはつながらない
 - この場合、証明書検証に失敗して切断する



CATのプロファイルを作成するには

- eduroam CATのプロファイル作成はWebで
 - プロファイル管理サイトへの招待が必要
 - eduroam JP担当にご連絡ください
 - 招待メールをお送りします
- eduGAIN(学認)/SNS等のアカウントでアクセス
 - 学認およびeduGAINに参加済み→SPに属性送信を！
entityID:
`https://monitor.eduroam.org/sp/module.php/saml/sp/metadata.php/default-sp`
属性：ePTID(必須), displayName(Optional), mail(Optional)
 - 学認/eduGAIN未参加→GoogleやSNSのアカウントで認証

作成方法は以下に公開中：

https://meatwiki.nii.ac.jp/confluence/x/hx2_AQ

プロフィール作成に必要な情報

- 機関情報
 - 機関英語名称とか所在地とか連絡先など
- プロファイル名の指定
 - プロファイルは複数作成可能
 - パスワード認証と証明書認証ではプロファイルを分ける等
- 認証方式の指定
 - PEAP-MSCHAPv2(パスワード認証)
 - TLS(クライアント証明書認証)
- 証明書検証用情報
 - サーバ証明書を発行したCAの証明書(CA証明書)
 - 認証サーバのCN(証明書記載のホスト名)

General Profile properties

We will now define a profile for your user group(s). You can add as many profiles as you like by choosing the appropriate button on the end of the page. After we are done, the wizard is finished and you will be taken to the main IdP administration page.

Profile Name and RADIUS realm

First of all we need a name for the profile. This will be displayed to end users, so you may want to choose a descriptive name like 'Professors', 'Students of the Faculty of Bioscience', etc.

Optionally, you can provide a longer descriptive text about who this profile is for. If you specify it, it will be displayed on the download page after the user has selected the profile name in the list.

You can also tell us your RADIUS realm. This is useful if you want to use the sanity check module later, which tests reachability of your realm in the eduroam® infrastructure. It is required to enter the realm name if you want to support anonymous outer identities (see below).

Custom Installer Name Suffix	select language		-
Profile Description	select language		-
Profile Display Name	select language		-
Production-Ready		☐	-

[Add new option](#)

Realm:

Realm Options

Some installers support a feature called 'Anonymous outer identity'. If you don't know what this is, please read [this article](#).

On some platforms, the installers can suggest username endings and/or verify the user input to contain the realm suffix.

The realm check feature needs to know an outer ID which actually gets a chance to authenticate. If your RADIUS server lets only select usernames pass, it is useful to supply the information which of those (outer ID) username we can use for testing.

Verify user input to contain realm suffix: ☐ Prefill user input with realm suffix: ☐

Enable Anonymous Outer Identity: ☐ anonymous

Use special Outer Identity for realm checks: ☐ anonymous

Installer Download Location

The CAT has a download area for end users. There, they will, for example, learn about the support pointers you entered earlier. The CAT can also immediately offer the installers for the profile for download. If you don't want that, you can instead enter a web site location where you want your users to be redirected to. You, as the administrator, can still download the profiles to place them on that page (see the 'Compatibility Matrix' button on the dashboard).

Redirect end users to own web page: ☐

Supported EAP types

Now, we need to know which EAP types your IdP supports. If you support multiple EAP types, you can assign every type a priority (1=highest). This tool will always generate an automatic installer for the EAP type with the highest priority; only if the user's device can't use that EAP type, we will use an EAP type further down in the list.

Supported EAP types for this profile	
Unsupported EAP types	FAST-GTC PEAP-MSCHAPv2 EAP-pwd TLS TTLS-GTC TTLS-MSCHAPv2 TTLS-PAP Managed IdP

Use "drag & drop" to mark an EAP method and move it to the supported (green) area. Prioritisation is done automatically, depending on where you "drop" the method.

Helpdesk Details for this profile

The option

• Support: E-Mail

is already defined IdP-wide. If you set it here on profile level, this setting will override the IdP-wide one.

Support: E-Mail	select language		-
Terms of Use	select language		参照...
Support: Phone	select language		-
Support: Web	select language		-

[Add new option](#)

EAP Details for this profile

CA Certificate File		参照...	-
Name (CN) of Authentication Server			-
CA Certificate URL			-

[Add new option](#)

Media Properties for this profile

HS20 Consortium OI		-
Mandatory Content Filtering Proxy		-
Remove/Disable SSID		-
Additional SSID		-

注意：
MS Edgeではうまく
EAP-TYPEの操作が
できないことが
ある模様。
別のブラウザも
試してください。

eduroam CAT利用の注意点

- 初回の接続は所属機関内であらかじめ済ませる
 - CAT利用に限りませんが、訪問先で初めてeduroamにつなげると偽APに騙されるかもしれません
- 所属機関の信頼できるAP下で初回接続を済ませるよう周知を！

是非eduraom CATをご利用ください！

eduroam アクセスマップ 新バージョン

現在のアクセスマップ

- 単一ポイント指定
 - どこまで電波が届いてるかわかりづらい
- 建物単位程度の指定
 - 使える部屋や階がどこかまではわからない



新バージョンマップ

- 高度の概念が追加
 - 緯度、経度、高度のセットで表現可能
 - 高度は省略可
- エリア(範囲)の概念
 - 複数の緯度、経度、高度の座標を組み合わせてエリアを指定可能
 - eduroamの使えるエリアを指定できる
- XMLだけでなくjson形式も利用可能

新バージョンへの切り替え時期

- 2019年11月～12月ごろに切り替え予定
 - グローバルマップ開発担当者からお知らせあり
- 新形式の記述方法についてはできるだけ早く案内できるようにいたします

お寄せいただいた質問への回答

- 駅や空港の公衆無線LANにeduroam出せない？
 - 検討しましたがNIIではコストが.....
 - 各所公衆無線LANに出してくれる事業者さんを募集中です
 - 「セキュア公衆無線LANローミング研究会」が市街地eduroamの構築を推進しているので、ご相談を
<https://nghsig.jp/>
- Windows NPSを使った運用をしたい
 - 本家の英語版マニュアルがあります
 - https://services.geant.net/sites/cbp/Knowledge_Base/Wireless/Documents/CBP-13_Using-Windows-NPS-as-RADIUS-in-eduroam_final.pdf

お寄せいただいた質問への回答

- URLフィルタリングはやっていいの？
 - eduroamは学術研究用に提供されるものですが、原則としてフィルタリングを行わないことが世界的ルールです。
 - 国内機関では過度のフィルタリングが問題となっており、学生の自主的な学習機会を奪っている例が散見されます。
 - eduroamでは不正利用時の利用者追跡が可能なこと、学術研究は本来広範囲に及ぶものであることを念頭に、やむを得ずフィルタリングを行う場合でも極力控え目にしてください。

お寄せいただいた質問への回答

- ポート制限の届け出をまとめてほしい
 - 届け出があればまとめる予定ですが、今のところ届け出が一つ也没有せん
 - もしポート制限が厳しい機関をご存知でしたら、こっそり教えてください。対象機関に確認します。
- 認証連携IDサービスのビジターアカウントは機関管理者が緊急停止できる？
 - できます
- ビジターアカウントの利用開始/終了に時間指定も加えてほしい
 - システム側のアカウント管理の都合上、難しいです

お寄せいただいた質問への回答

- ビジターアカウントによる他機関での認証試行が負荷になりそうだけど、手前で止める方法が必要では？
 - 各機関側RADIUS Proxyサーバで、
 - 自分の機関で発行したビジターアカウントは通す
 - それ以外のv.eduroam.jpはドロップする
- とproxy.confに設定するとよさそうです。

```
home_server jp-top-1 {  
(略)  
}  
home_server jp-top-2 {  
(略)  
}  
home_server_pool jp-top {  
  type = fail-over  
  home_server = jp-top-1  
  home_server = jp-top-2  
}
```

```
realm "~example-u%.v%.eduroam%.jp$" {  
  pool = jp-top  
  nostrip  
}  
realm "~^(.+%.)?v%.eduroam%.jp$" {  
  virtual_server = auth-reject  
}  
realm "~^(.+%.)?example-u%.ac%.jp$" {  
  authhost = LOCAL  
  accthost = LOCAL  
}  
(中略)
```

```
※末尾に追加  
server auth-reject {  
  authorize {  
    suffix  
    update reply {  
      Reply-Message :=  
        "Rejected by Example-U Proxy Server"  
    }  
    reject  
  }  
}
```

お問い合わせ先

eduroam JPの詳細については以下をご覧ください

<https://www.eduroam.jp/>

eduroam全般のお問い合わせ先：
eduroam-office@nii.ac.jp