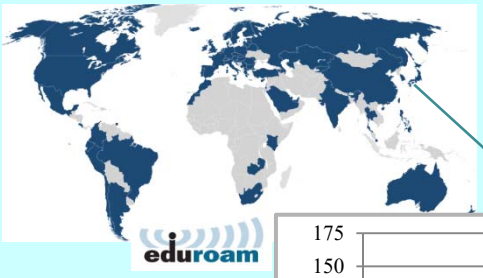
国際学術無線LANローミング基盤「eduroam」

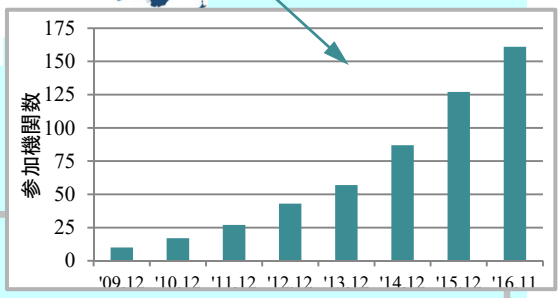
http://www.eduroam.jp/

eduroam（エデュローム）は，欧州のGÉANT(旧TERENA)で開発された学術無線LANローミング基盤です．日本を含む世界80か国・地域で，キャンパス無線LANのデファクト・スタンダードになっています．

eduroamは2006年に国立情報学研究所の全国大学共同電子認証基盤構築事業の一環として日本に導入され，「eduroam JP」の名称でNIIと東北大学が共同で国内における運用とサポート，および技術開発などを行っています．

2016年11月時点で，国内161機関がeduroam JPに参加しています．新時代の教育・研究をサポートする情報インフラの一つとして，多くの機関の参加をお待ちしています．





eduroamで何ができるの？

■ 自機関はもちろん，国内外の訪問先機関の無線LANが利用できます

- ✓ 自機関の教職員・学生に，訪問先での無線LAN利用手段を提供し，教育・研究を強力にサポート．
- ✓ 認証連携により，所属機関で発行されたIDがそのまま使えます．
- ✓ 接続設定が共通なので，訪問先ごとに設定を変更する必要がありません(共通ESSID: eduroam)．

■ ユーザ認証および通信内容の高いセキュリティが確保できます

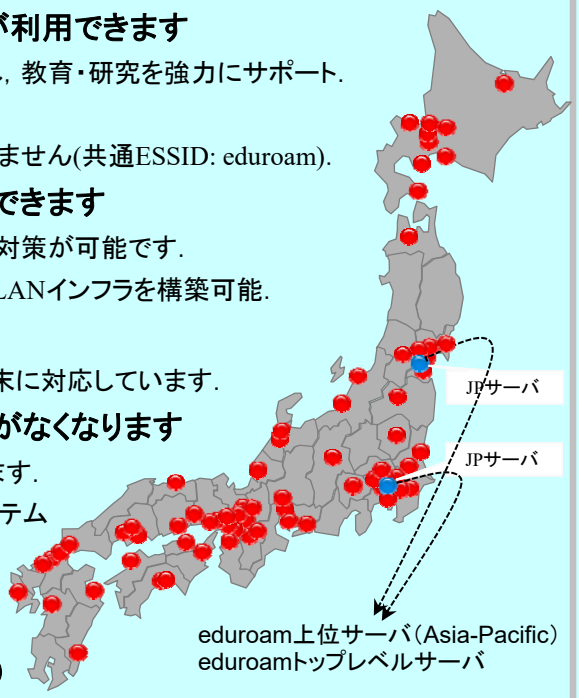
- ✓ 802.1X方式による安全なユーザ認証を利用しており，偽基地局の対策が可能です．
- ✓ WPA2/AESによる強力な暗号通信による，安全なキャンパス無線LANインフラを構築可能．

■ 様々な端末が使えます

- ✓ WindowsやMacはもちろんのこと，iPhoneやAndroidなど様々な端末に対応しています．

■ 訪問者のためのネットワーク環境を毎回準備する必要がなくなります

- ✓ 学会等で訪問者が来るたびに基地局を設置・変更しなくても済みます．
- ✓ eduroam用のネットワークを分離しておくことで，訪問者が学内システムに不正にアクセスすることを防止できます．
- ✓ SINET接続機関はeduroam用アドレスの割り当てが受けられます．（詳細: http://www.eduroam.jp/docs/SINET-eduroam.pdf）



■ 学術認証フェデレーションとも連携できます（オプション）

- ✓ NIIが運用している「学術認証フェデレーション(学認)」に機関が参加することにより，RADIUSサーバを用意しなくとも，機関のアカウントを用いてeduroam用アカウントの発行が可能です．

どこで使えるの？

- ✓ 参加機関のアクセスポイントが利用できます．
- ✓ 関東地区の貸会議室，カフェ等の公衆無線LANのアクセスポイント（約130か所）でも利用できます．
- ✓ GÉANTのウェブサイトに参加国・機関リストやマップがあります． https://www.eduroam.org/

どうすれば利用できるの？

- ✓ 機関で認証サーバ（RADIUS）や基地局を用意してeduroam JP のRADIUSサーバ網に接続します（要参加申請，無償）．
- ✓ 機関の認証サーバが不要な代理認証システム（アカウントサービス）も提供されています．
- ✓ 利用者は，自分の所属機関でIDが取得できます．

情報・システム研究機構 国立情報学研究所 National Institute of Informatics

学術基盤推進部 学術基盤課 総括・連携基盤チーム

TEL:03-4212-2218　FAX:03-4212-2230

e-mail: tech@eduroam.jp

（2016年11月）

eduroamの参加と運用について

● 参加について

- ✓ ウェブサイトにある申請フォームに記入し、電子メールにてご提出ください。参加に費用はかかりません。
- ✓ 参加にあたって、SINETや学認への加入の有無は不問ですが、原則として高等教育機関および学術研究機関からの参加を受け付けます。(SINETの加入基準に準じます)
- ✓ 互恵精神によるサービス提供の枠組みですので、原則として、機関内または最寄にeduroam対応基地局の提供が必要です。参加に際しては、来客が利用しやすい所に一基以上の基地局を設置してください。

● 認証サーバについて

- ✓ RADIUSプロトコルによる認証サーバを使用します。(学認で用いるSAMLの認証サーバとは異なります)
- ✓ eduroamのアカウントでは、IDとして電子メールアドレスに類似のものを利用します。例えば UserID@大学名.ac.jp のようになり、@以降の部分はレルム(realm)と呼ばれ、所属機関を表します。
- ✓ 認証の安全性を高めるために、認証サーバにはサーバ証明書のインストールが必要です。利便性を確保するため、いわゆる「オレオレ証明書」ではなく、公正な証明書の利用を推奨します。この目的のために、NIIが提供するUPKIオープンドメインサーバ証明書も利用可能です。(自機関のユーザが訪問先でeduroamを利用する場合も、訪問先ではなく所属機関のサーバ証明書で検証が行われます)
- ✓ 認証には、IDとパスワードを利用するPEAP方式が一般的ですが、クライアント証明書を用いたEAP-TLS認証を利用することも可能です。(証明書のCNにレルムのついたIDが入っていると、端末での設定が容易になります)
- ✓ 現在、認証サーバを準備する主な方法には、以下の3通りがあります。
  1. 機関内に自前でRADIUSサーバを構築する
     - FreeRADIUSや、eduroam対応アプライアンスなどを利用。学内の電子認証システムと連携することで、共通のIDとパスワードを利用した認証も可能です。また、教育機関向けクラウドサービスで実現することも可能です。
     - 参加申請時に、希望のレルムを指定してください。機関のDNSドメイン名と合せるのが基本です。
     - 部局ごとに認証サーバを構築してサブドメイン階層構造を持ったレルムを利用することも可能です。この場合でも、認証サーバの学外との接続は、機関を代表するプロキシサーバに集約してください。
     - 冗長化のために、同一レルムに対して複数のサーバを用意しても構いません。
  2. 代理認証システムを利用 (eduroam JPのサーバでアカウントを発行し、配布する形態です)
     - 利用申請時にレルムの一部となる機関名を指定してください。機関で保有しているDNSドメイン名と同一の名前を使用するのが一般的です。
  3. 仮名アカウント発行システムを利用 (学認に参加している場合に、利用者自身が学認用のアカウントを利用してeduroam用のアカウントを取得できます)

● 無線ネットワークについて

- ✓ 原則として、eduroam用のESSIDは「eduroam」に統一し、ビーコンを出してください。
- ✓ 無線基地局からの認証要求を集約するためのRADIUSプロキシの設置をお願いします。冗長化のために複数のプロキシを接続することも可能です。
- ✓ ゲスト用に割り当てるIPアドレスとして、キャンパス内の通常利用のIPアドレスと異なるものを利用するには、次の方法があります。
  - 自機関が保有する別IPアドレスブロックを利用する。(電子ジャーナルなどの契約と分離が必要)
  - 商用回線を導入し、その回線に付随するIPアドレスを利用する。
  - SINETからeduroam用アドレスの割り当てを受ける。(SINETとの接続が必要、VLAN接続になる)
- ✓ 認証時のレルムを見て、自機関のユーザである場合に自機関ユーザ向けネットワークに振り分ける仕組み(認証VLAN)を導入すると 、ユーザが接続先のESSIDを切り替える必要がなくなり、大変便利です。
- ✓ 不正アクセス対応のために、認証ログ(RADIUS認証、MACアドレス)の取得が義務付けられています。これに加えて、IPアドレス(DHCP)、NATなどの情報も取得しておくことが推奨されます。(プロバイダ責任制限法等に基づき、3～6か月程度)
- ✓ ゲスト用に提供するネットワークでは、原則としてFirewallの設定を行わないこととなっていますが、必ずしもFirewallの設定を禁止するものではありません。ただしhttp(s)と各種VPNプロトコルの通過は必要です。
- ✓ 民間サービスプロバイダが提供するキャンパス無線ネットワーク構築・運用サービスの中には、eduroamに対応しているものもあります。公衆無線LANサービスと同時整備が可能なところもあります。

情報・システム研究機構 国立情報学研究所 National Institute of Informatics
学術基盤推進部 学術基盤課 総括・連携基盤チーム
TEL:03-4212-2218　FAX:03-4212-2230　e-mail: tech@eduroam.jp