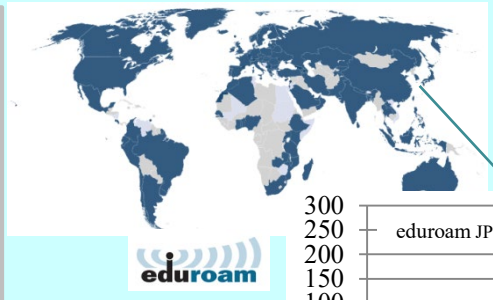
国際学術無線LANローミング基盤「eduroam」

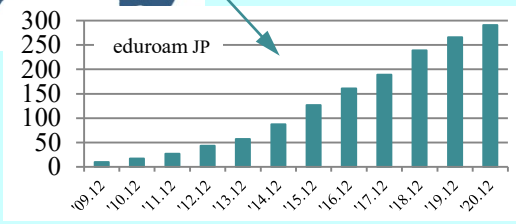
https://www.eduroam.jp/

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．世界106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が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．

2021年3月時点で，国内299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，学習・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．
- ✓ 訪問先ごとに設定変更する必要がなく，所属機関の設定のままで，自動接続できます．

■ 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

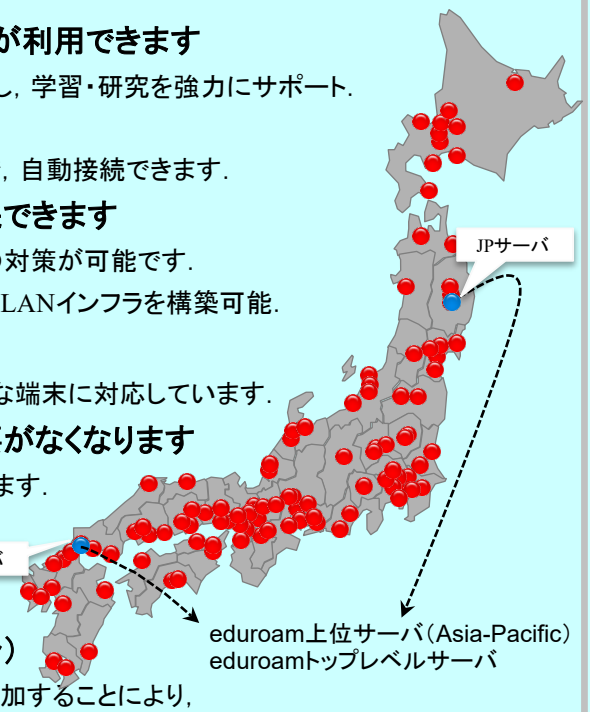
- ✓ WindowsやMac，iPhone，iPad，Android，Chromebookなど，様々な端末に対応しています．

■ 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．
- ✓ 構成員用・訪問者用のネットワークを分離できる仕組みがあり，訪問者が学内システムにアクセスすることを防止できます．
- ✓ SINET接続機関はeduroam用回線の割り当てが受けられます．

■ 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．
- ✓ 国内外の貸会議室・会議施設，カフェ等店舗，商業施設(モール)，図書館，博物館，病院，市街地の公衆無線LANなどでも，利用できるところがあります．
- ✓ 空港や駅で利用できる国々もあります．
- ✓ 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 の認証連携ネットワークに接続します（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

https://www.eduroam.jp/for_admin/contact

（2021年3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「eduroam JP申請システム」よりご申請ください。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。参加要件については、ウェブサイトにある「学術無線LANローミング基盤サービス加入規程」をご覧ください。
- ✓ 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も基地局を設置するようにしてください。
- ✓ 参加機関は、訪問者の利用に供する基地局について、位置情報の提供・更新が必要です。

● 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。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方式を利用することも可能です。
- ✓ 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。
2. 認証連携IDサービスを利用する
   - 学認に参加している場合、機関にRADIUSサーバを設置しない構成です。
   - 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る仕組みです。
3. 代理認証システムを利用する
   - eduroam JPのサーバでアカウントを発行し、構成員に配布する利用形態の、アカウント発行サービスです。
   - 学認に未参加でも、機関の管理者を登録するだけで、eduroamアカウントの一括発行が可能となります。

● 無線ネットワークについて

- ✓ eduroamでは、共通のSSIDである “eduroam” を使用し、ビーコンを出すことが規定されています。
- ✓ 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。
- ✓ 訪問者用に割り当てる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な場合など)
  - 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参加機関のみ。SINET のVLANを利用)
- ✓ 認証時のレルムを見て、自機関の利用者と訪問者でネットワークを自動切替する仕組み(認証VLAN)を導入すると 、利用者が手動でSSIDを切り替える必要がなくなり、利便性と安定性が向上します。
- ✓ 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)
- ✓ 訪問者用に提供するネットワークでは、原則としてアクセス制限を行わないこととなっています(基本的なセキュリティ対策を除く)。特に、http(s)と各種VPNプロトコルの通過は必須です。
- ✓ 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　eduroam JP担当
https://www.eduroam.jp/for_admin/contact