

エデュローム
eduroam導入のチェックポイント

第2版 (2014.2.23)

後藤英昭

東北大学 / 国立情報学研究所

まえがき

- この資料は、国内の教育・研究機関等において、国際無線LANローミング基盤「eduroam」を導入する際の、技術面および運用面のチェックポイント(要点)をまとめたものです。





内容

1. 設備供用の可否の確認
 2. ゲスト用ネットワークの確保
 3. 認証VLANの導入の選択
 4. 管理・運用体制の検討
 5. アクセスポイントの選定
 6. アカウント管理方法の検討
 7. RADIUSサーバの選択
-
- A1. 認証方式の選択
 - A2. サーバ証明書の利用
 - A3. 公衆無線LANサービスの導入の検討



1. 設備供用の可否の確認

- eduroamでは、機関内の無線LANアクセスポイント(AP)やネットワーク(LAN)を来訪者に利用させることが前提となっています。

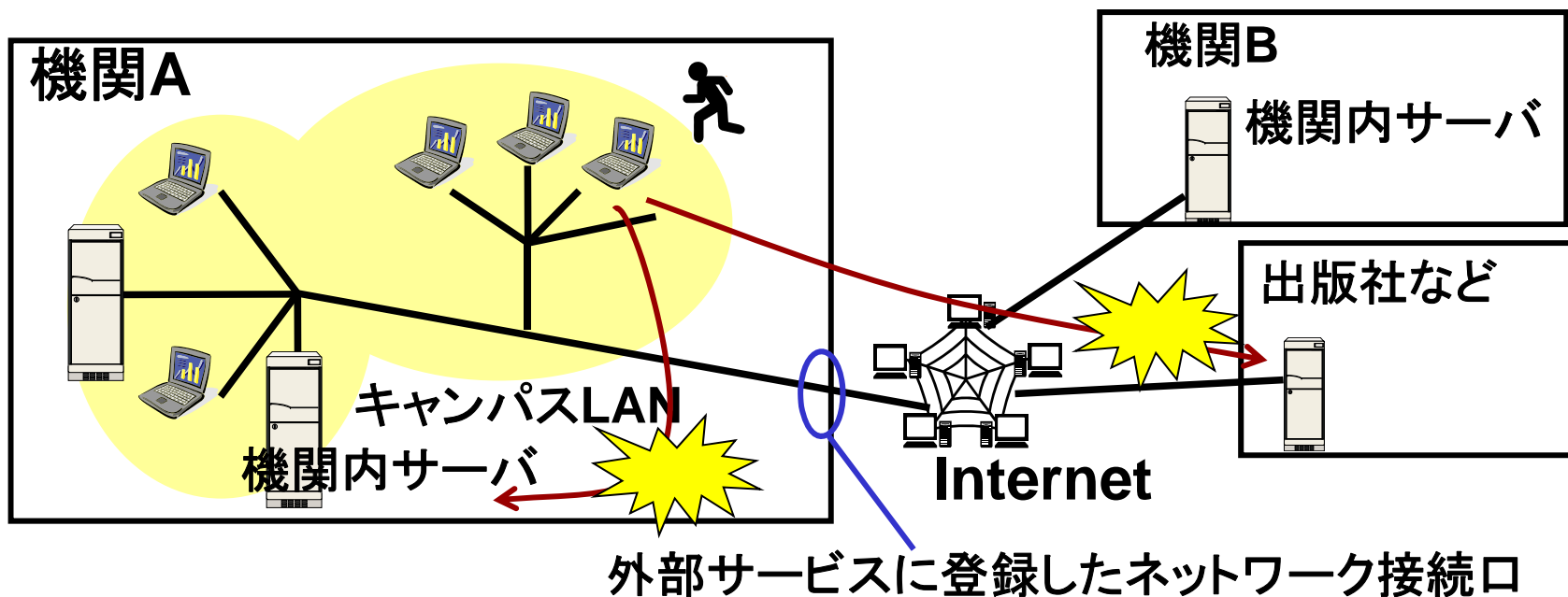
機関内のネットワーク設備を来訪者に利用させられるかどうかは、機関ごとにポリシーが異なるでしょう。設備供用が可能かどうか、機関内で調整および確認が必要です。

- 後述のように、機関内の通信と、訪問者の通信は、物理的または論理的に分離するのが一般的です。

学内通信の盗聴や、機関内限定のサーバなどにアクセスができないように、セキュリティを確保したネットワーク構成が可能です。

2. ゲスト用ネットワークの確保 1/4

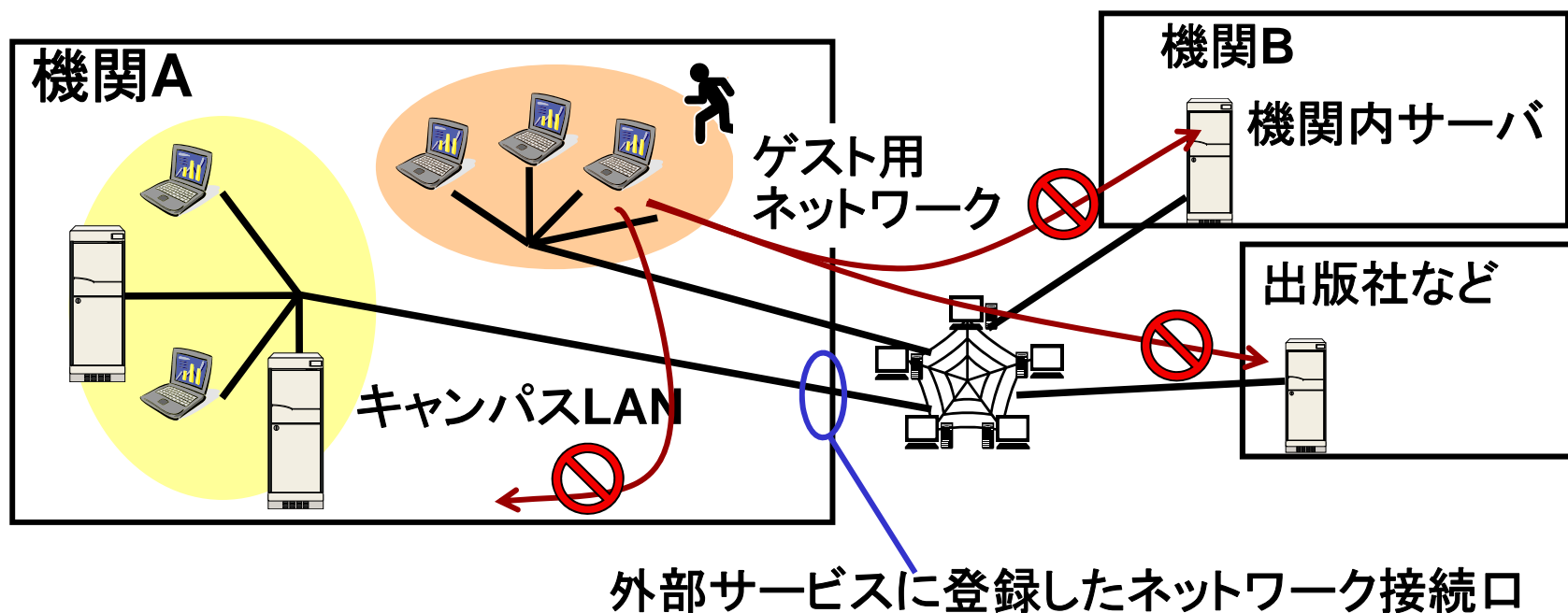
- 無線LAN端末を既存のキャンパスLANに收容すると、部外者が機関内のサーバにアクセスできたり、契約している外部サービス(電子ジャーナルなど)が利用できるという、セキュリティ上および契約上の問題が生じます。



2. ゲスト用ネットワークの確保 2/4

- キャンパスLANとは別に、ゲスト用のネットワークを確保することで、無線LAN利用者を機関外からのアクセスとして扱い、機関内サーバへのアクセスや、外部サービスの不正利用を防ぐことができます。

(自機関の利用者も外部アクセスとなるので、利便性は下がります)





2. ゲスト用ネットワークの確保 3/4

- ゲスト用ネットワークを用意するには、例えば以下の方法があります。
 - 既存のLANを分割してゲスト用のサブネットを切り出す
(外部サービスの登録変更も必要)
 - プロバイダと別途契約する
 - SINETの「eduroamアクセスネットワーク」を利用する
- eduroamアクセスネットワーク
 - SINET4を利用している機関は、申請により、ゲスト用ネットワークのためのサブネットを無償で利用できます。
IPv4は、NAPTの利用を前提として、/30のサブネットが割り当てられます。オプションでIPv6(/64)の利用も可能です。

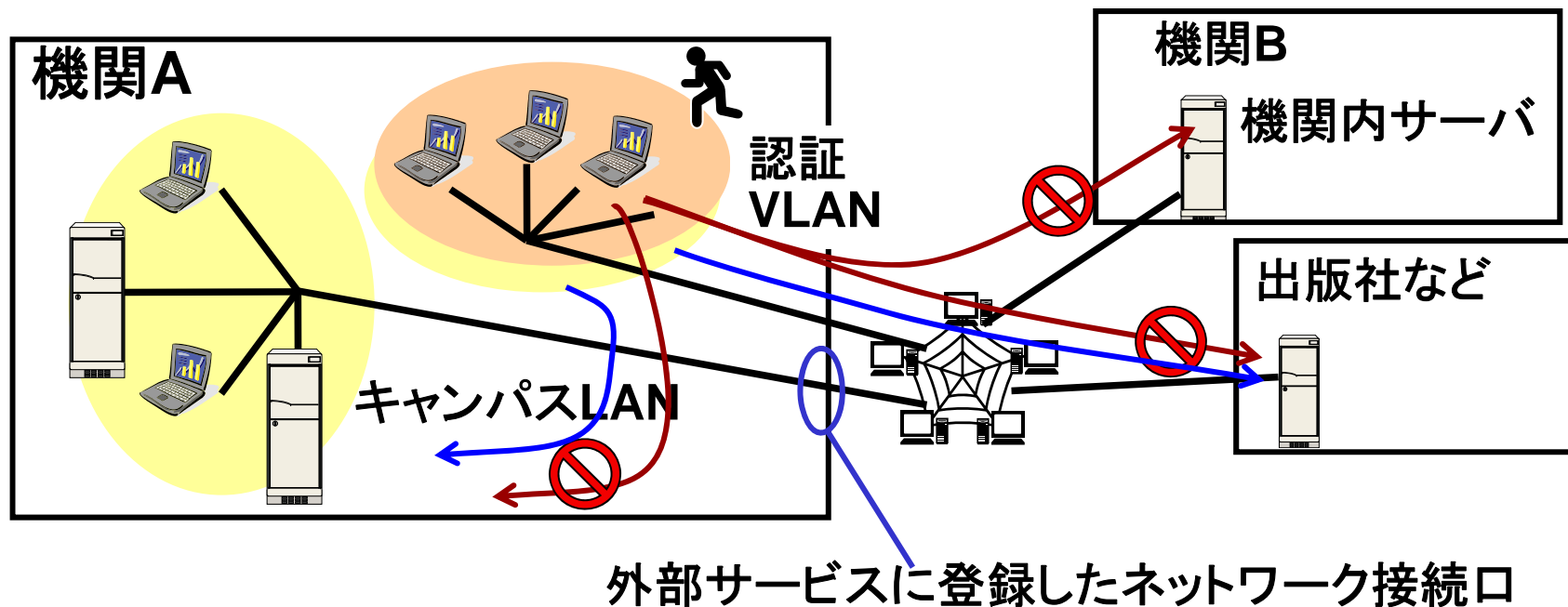


2. ゲスト用ネットワークの確保 4/4

- 機関内LANとゲスト用ネットワークの分離には、以下のような方法があります。
 - アクセスポイントを接続するネットワークを別配線(物理的に分離)として、最寄のスイッチでタグVLANなどを用いて機関内LANと論理的に分離し、センターでゲスト用ネットワークを集約する.
 - コントローラ型のアクセスポイントを導入し、アクセスポイントのトンネル(VPN)機能を利用して、コントローラ側でゲスト用ネットワークを集約する。
(アクセスポイント自体は機関内LANに収容するが、端末のトラフィックはトンネル内を通り、LANのセキュリティは確保される)

3. 認証VLANの導入の選択

- ゲスト用ネットワークでは、利用者が自機関において無線LANを利用する場合でも外部アクセスとみなされ、利便性が若干劣ることになります。認証VLANを導入すれば、自機関の利用者として認証された者の端末をLANに直接収容することができ、利便性が大幅に向上します。





4. 管理・運用体制の検討

- 新規に無線LANシステムを構築する場合は、その運用を機関主導で行うのか、全面的に業者に委託するのかを決める必要があります。
- 業者に管理・運用を委託すると、商用の公衆無線LANサービスの同時整備が容易になるなどのメリットがあります。
- 既存の無線LANシステムにeduroamを追加しようとする場合は、機材の対応状況の確認も含めて、現在の委託業者との調整が必要です。

5. アクセスポイントの選定

- eduroam対応の無線LANシステム構築では、コントローラ型のアクセスポイント(AP)の導入を推奨しています。
 - コントローラ型APでは、集中管理により、多数のAPの設定変更が容易です。集中管理ができない独立したAPを多数導入した場合、管理コストが問題になる場合があります。
 - トンネル機能を有するAPを利用することで、無線LANの通信を容易にコントローラに集約することができ、AP設置場所のネットワーク設計の自由度が高くなります。
- マルチSSID機能を有するAPが必要です。
 - eduroam以外に、機関独自の無線LANシステムや、公衆無線LANサービスを、同一のAPで提供できます。
(独立したAPを多数並べるのは、電波干渉により深刻なサービス障害が生じる恐れがあり、避けるべきです)



6. アカウント管理方法の検討 1/4

- eduroamのアカウント(利用者ID)発行方法には、以下のよう
なものがあります。複数を組み合わせた運用も可能です。
 - 機関にRADIUS IdP (IDプロバイダ)となるサーバを設置し
て、アカウントを発行・管理する。
 - 「eduroam代理認証システム」を利用する。
 - 「eduroam仮名アカウント発行システム」を利用する。
 - その他、業者が提供するアカウントサービス(IdP)などを
利用する。



6. アカウント管理方法の検討 2/4

- 機関にRADIUS IdPを設置する場合
 - 学内のID管理システムと連携させる場合、既存のLDAPやActive Directoryなどと接続できるかどうか、業者に確認が必要です。アカウントのデータ形式によっては、RADIUSと連携できない場合があります。
 - 一台のRADIUSサーバでも運用は可能ですが、サービスの安定性向上のため、二台のサーバによる冗長構成が推奨されます。

6. アカウント管理方法の検討 3/4


■ 「eduroam代理認証システム」

- eduroam JPが提供する、アカウント発行ウェブサービスです。機関のIDデータベースとは連携できませんが、機関のRADIUS IdP設置が不要で、機関管理者のオンラインサインアップのみで利用できるようになります。
(eduroam参加申請が別途必要)
- 機関管理者のウェブ画面上の操作により、eduroamアカウントを必要数だけ随時取得できます。
(利用者へのアカウント配布は機関内で手作業となります)
- 学会や研究会などのゲストアカウント発行にも利用できます。(利用機関の責任と裁量によりゲストアカウント配布)
- 地理的に分散された冗長構成IdPにより、激甚災害などで機関が被災した場合でも、他機関でeduroamの継続利用が可能です。

6. アカウント管理方法の検討 4/4

■ 「仮名アカウント発行システム」

- 学術認証フェデレーション(学認)に対応した、アカウント発行サービスです。学認とeduroamの両方に参加している機関で利用できます。
- 機関のIDデータベースとは連携できませんが、機関のRADIUS IdP設置が不要です。
- 各機関の利用者が、学認のアカウントでログインし、eduroamのアカウント(期限付き)を取得できます。(アカウント発行に際して、機関管理者の操作は不要です)



7. RADIUSサーバの選択

- 機関に設置されるRADIUSサーバには、以下の機能があります。
 - 利用者認証のためのIdP(IDプロバイダ)機能
(外部のアカウントサービスを利用する場合は不要)
 - アクセスポイントからの認証リクエストを中継するproxy機能
- RADIUSサーバには、以下のような種類があります。
 - ソフトウェアによるもの
(FreeRADIUSやRadiator、その他各種製品があります)
 - アプライアンス製品 (ハードウェア)
(2014年現在、国内では数社から販売されています)



- オプションの検討事項

A1. 認証方式の選択

- eduroamでは、一般的なPEAP方式の他に、様々な認証方式を利用することができます。機関でIdPを運用する場合、想定する利用環境に合わせて選択する必要があります。
(サーバの構成によっては併用も可能)
 - 世界のeduroamでは、PEAPによるID/パスワード認証方式が広く用いられています。これは、標準でPEAPをサポートする端末が多く、汎用性・利便性が高いためです。
 - クライアント証明書による認証を行うEAP-TLSを採用することで、より高い安全性が実現されます。ただし、利用できる端末に限られるというデメリットがあります。
(2014年2月現在、Androidでは設定用アプリケーションが別途必要です)

A2. サーバ証明書の利用

- 端末接続時にサーバ証明書(RADIUS IdP)の検証を行うことで、偽のアクセスポイントに誘導、経由させられるリスクを低減できます。利用者端末のサーバ証明書検証機能を有効にする運用が望ましいですが、現状では必ずしも容易ではないことから、推奨の扱いになります。
 - PEAP(MS-CHAPv2)を利用する場合、証明書の検証がOFFであっても、MS-CHAPv2の相互認証のレベルで安全性が確保されます。(ウェブ認証と違い、平文のパスワードがそのまま偽サーバに渡ることはありません)
 - 独自認証局のサーバ証明書を利用すると、利用者がCA証明書を端末に導入する手間が生じます。さらに、CA証明書を追加できない端末が多く市販されており、利用上のトラブルも懸念されます。
 - 「UPKIオープンドメイン証明書自動発行検証プロジェクト」の参加機関は、このサーバ証明書を使用することで、対応端末ならばサーバ証明書の検証が容易になります。



A3. 公衆無線LANサービスの導入の検討

- 新規に無線LANシステムを構築する場合、公衆無線LANサービスを同時整備するか否かを検討しておくといでしょう。
 - 大学・研究所などにおいて学会や研究会が開催される場合、企業の人はもちろん、一般市民も参加することがあります。附属図書館や附属病院には、日常的に市民が訪れます。要所のみ公衆無線LANを導入するという選択もあるでしょう。
- 既設のアクセスポイントの機種とネットワーク構成によっては、後から追加で公衆無線LANサービスを乗せることも可能です。業者への設備提供に関して、機関内で十分な検討・調整が必要です。また、対応できる業者が少ない点にも留意する必要があります。