NII ネットワークセキュリティ技術研修 (大阪)
2008年11月13日

キャンパス無線LANのユーザ認証と国際無線LANローミング基盤eduroam

後藤英昭　東北大学サイバーサイエンスセンター

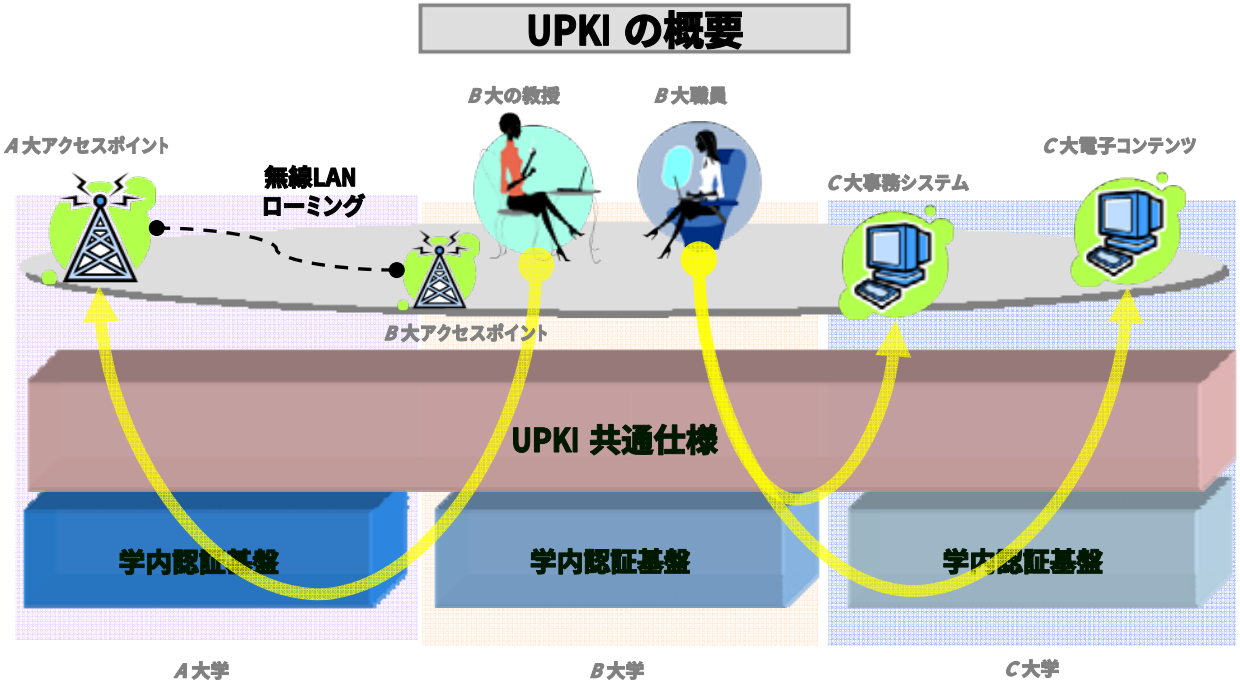
内容

- UPKI構築事業について
- キャンパス無線LANのセキュリティ
- キャンパスユビキタスネットワーク
- 無線LANローミング
  - 国際無線LANローミング基盤 eduroam
- eduroam JP
  - 日本におけるeduroam
  - 参加方法　と　利用方法
- 従来のeduroamの問題と解決策
- 学内ネットワークの構成例

UPKI構築事業

UPKI：大学間連携のための全国共同電子認証基盤

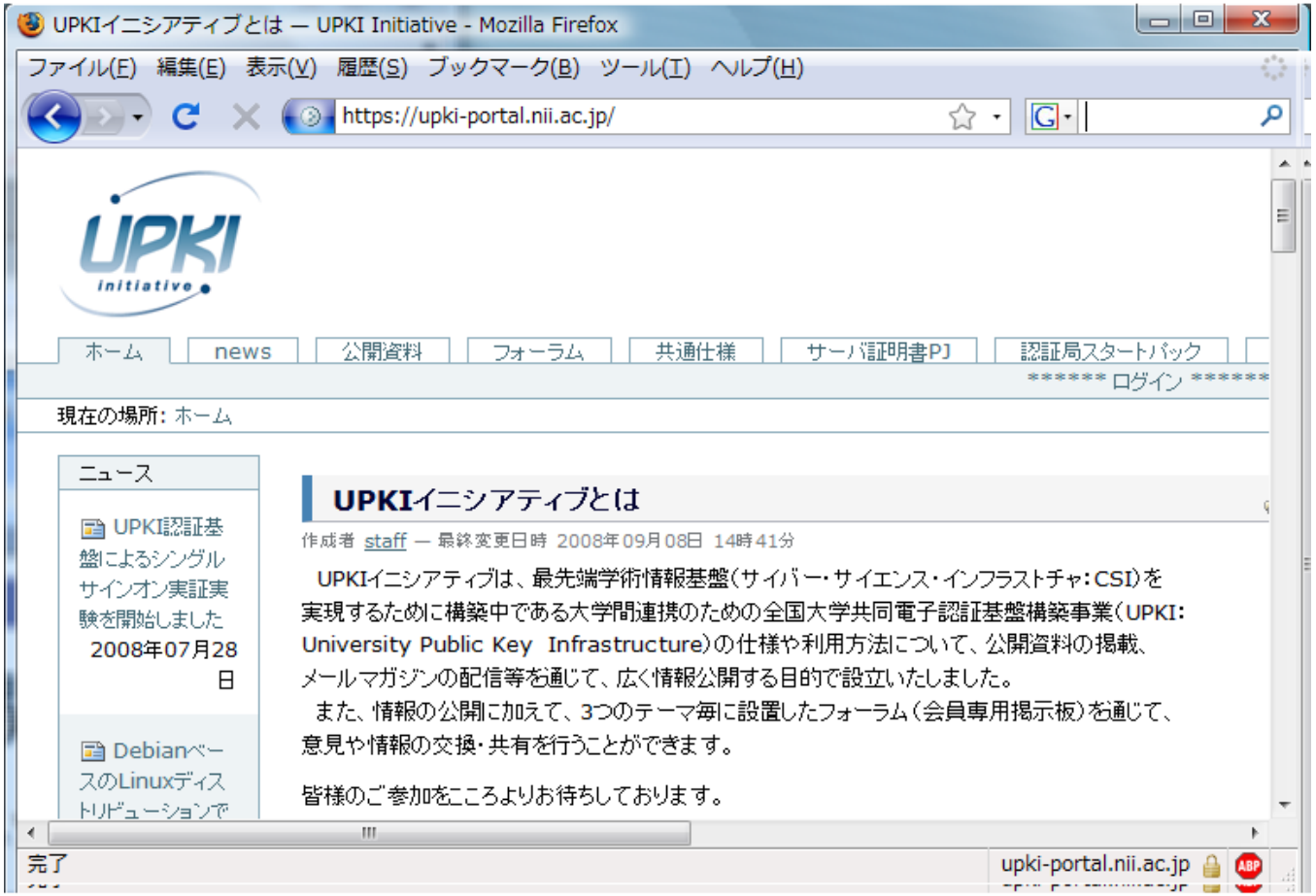
- **最先端学術情報基盤** (Cyber Science Infrastructure) **実現のため，大学等が保有する教育･研究用計算機，電子コンテンツ，ネットワークおよび事務システムなどの学術情報を，安心･安全かつ有効に活用するための電子認証基盤**
- PKI (**公開鍵認証基盤**) **を活用**



UPKIに関する情報

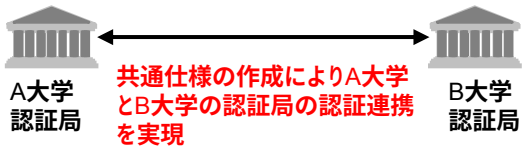
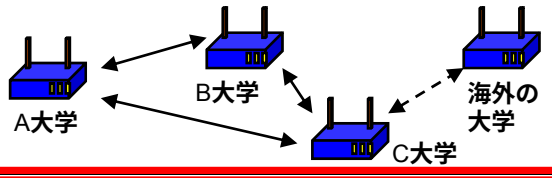
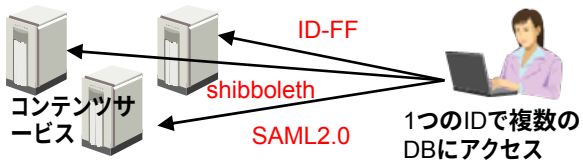
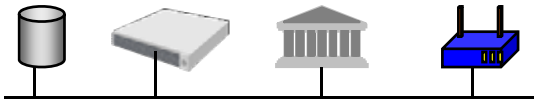
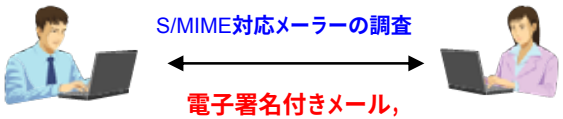
- 「UPKIイニシアティブ」 ウェブサイト

  https://upki-portal.nii.ac.jp/



UPKIのこれまでの成果

(TOPIC講演会資料より)

項番	事項	内容
1	「UPKI共通仕様」の作成と配布	 「UPKI共通仕様」の利用により大学での ・学内認証局の構築 ・CP/CPS等の規程の整備 が容易に実現可能に
2	オープンドメイン認証局の構築とサーバ証明書の発行	 オープンドメイン認証局の構築により，全世界に通用するサーバ証明書を発行し，大学のWebサーバの実在性証明と通信の暗号化を実現
3	大学間無線LANローミングの実現	 eduroamによる大学間無線LANローミングを実現。海外のeduroam参加機関との連携も実現
4	コンテンツサービスのシングルサインオン実験	 各種データベースサーバへのシングルサインオンを実現するため，shibboleth，SAML2.0等の仕様を調査し，UPKIにふさわしい方式を検討
5	NAREGI-CAを利用した認証局ソフトウェアパッケージの開発	 オープンソースの認証局ソフトウェアあるNAREGI-CAを用いて，認証局を簡単に構築し，無線LAN認証を容易に実現できるソフトウェアを開発 これにより，大学の認証局構築を促進する
6	S/MIME証明書の試験利用	 S/MIME証明書を，認証関係者間で試験利用するとともに，対応メーラーの調査，WebメールでのS/MIME利用の調査研究を実施

キャンパス無線LANのセキュリティ

- 有線接続
  - イーサネットジャックや部屋を物理的に施錠できる
  - ポート単位で端末･ユーザ認証が可能
  - 機材を物理的に挟まない限り，盗聴は難しい
- 無線接続
  - 電波の到達範囲が制限できない
    - 誰がどこから接続しているかわかりにくい
    - 部外者でも容易に電波を掴まえられる
  - 電波を掴まえるだけで，盗聴が容易
    - 盗聴は避けようがないので，内容が漏洩するか否かが問題

無線LANのセキュリティ対策

- 利用資格のある人だけに使わせる
  - ハードウェア (端末) 認証　(盗難も考えると，やや不十分)
  - ユーザ認証
  - ゲスト向けには，利用できるサービスを限定
- 盗聴による情報漏洩の防止
  - 利用者の教育　(セキュリティ意識を高める)
  - 通信の暗号化
    - 教育は重要だが，完全ではない．
      ユーザが意識しなくても，自動的かつ安全に暗号化される仕組みが必要．

キャンパスユビキタスネットワーク (CUN)

- **ユビキタスネットワーク：**
  「『いつでも、どこでも、何でも、誰でもアクセスが可能』なネットワーク環境」 (**総務省・情報通信白書** H16)
  - **ユビキタスコンピューティングの実現.**
  - **様々な機器による通信** (PC, **家電**, **乗り物**, …)
  - **様々な通信環境、サービス、物、情報、人を結びつけ、生活や経済を円滑にするもの.**

キャンパスユビキタスネットワーク (CUN)

- **キャンパス～　：**
  - **教育･研究機関におけるユビキタスネットワークの実現.**
  - **特に、新しい研究環境や教育方法の創造･支援.**
  - **まずは、ネットワークの接続性確保が必要.**
    - **イーサネットジャック**
    - **無線LAN**
    - PHS･3G

キャンパスネットワークの現状

多くの教育・研究機関において、

- 幹線ネットワークはよく整備されていても、
  端末接続ポートが少ない、または特定の部屋に限定.
- ユーザ認証機構のないシステム
  - 部外者による不正利用
  - 故意または無意識の加害に対して責任が曖昧
- 部局ごとに異なるシステム
  - 低い利便性
- 他部局の人は自由に使えない
  - 会議などで非常に不便

無線LANシステムに対する要求

- 国内･国際会議，研究会，集会
  - 教職員、研究者、学生のネットワーク利用環境改善
  - 主催者側の準備負担軽減
- 講義など
  - 講師のネットワーク利用環境の改善
  - ネットワークを利用した新しい授業方法の推進
    - 持ち込みPCによる演習、遠隔講義･プレゼンテーション、VODによる自習、など
  - 単位互換制度による学生移動への対応

無線LANシステムに対する要求

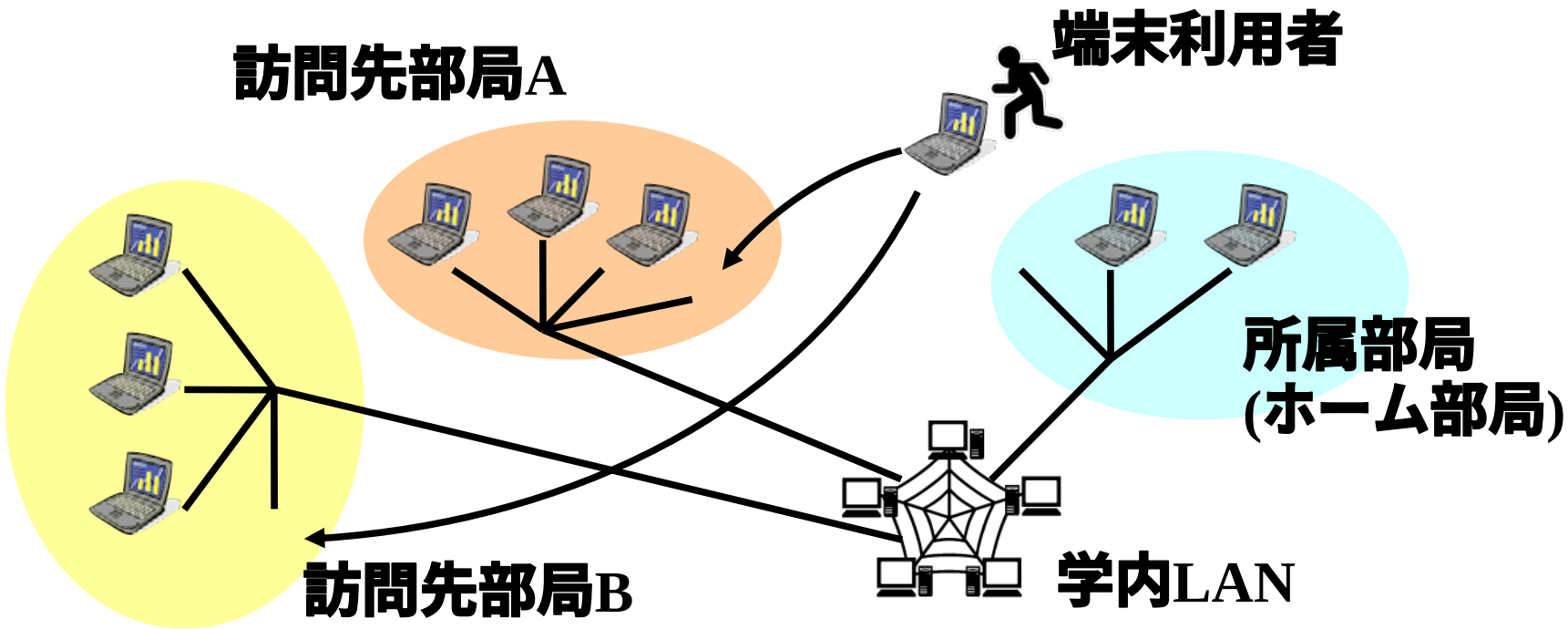
- その他
  - 海外出張中など，商用ブロードバンドサービスが利用しにくい地域におけるネットワーク利用手段の確保




安全性と利便性を兼ね備えたシステムが必要！

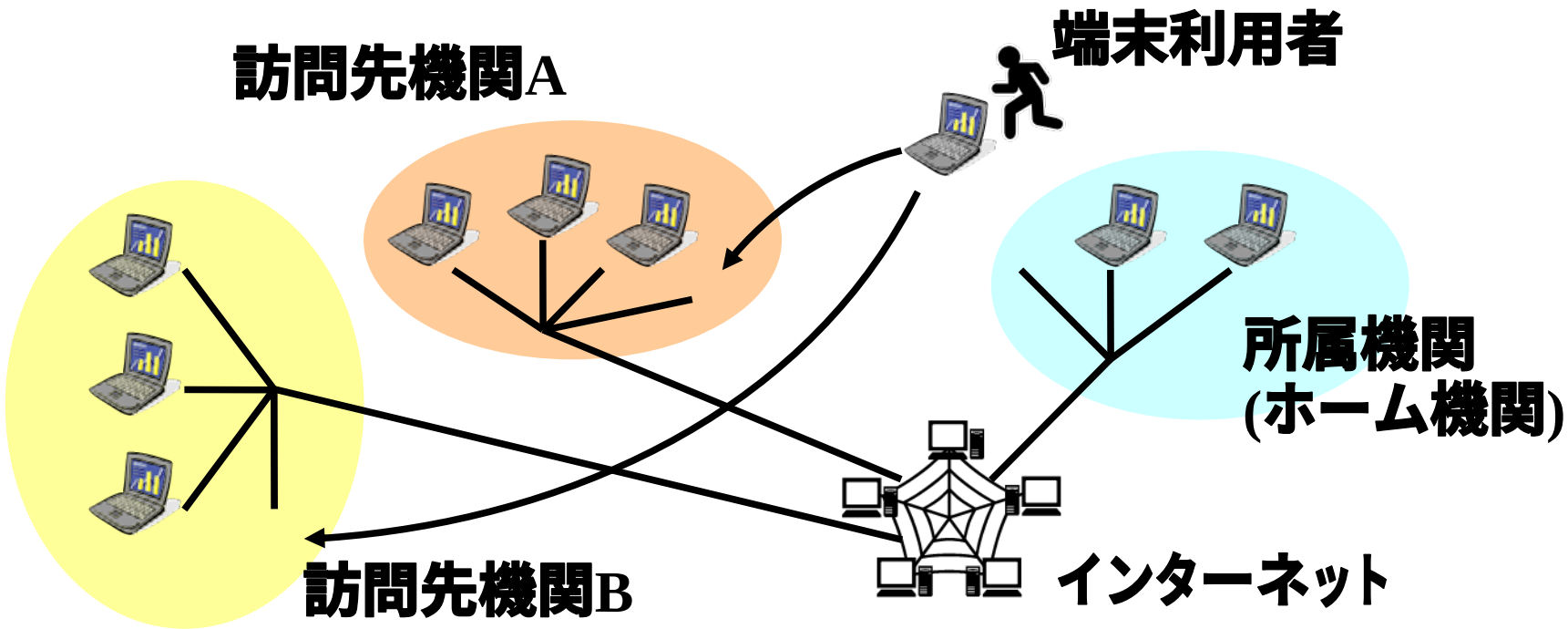
学内無線LANローミング

- 認証連携技術により、利用者が所属部局のアカウントを使って他部局の無線LANインフラを利用できる仕組み



機関間無線LANローミング

- 利用者が所属機関のアカウントを使って他機関の無線LANインフラを利用できる仕組み



エデュローム
eduroamとは

- ヨーロッパのTERENAで開発された、無線LANローミング基盤
  http://www.eduroam.org/
- ヨーロッパ約30ヶ国の他、アジア太平洋地域ではオーストラリア、中国、台湾、香港、日本、NZ、フィリピン、カナダが参加

  世界的なデファクトスタンダードに！

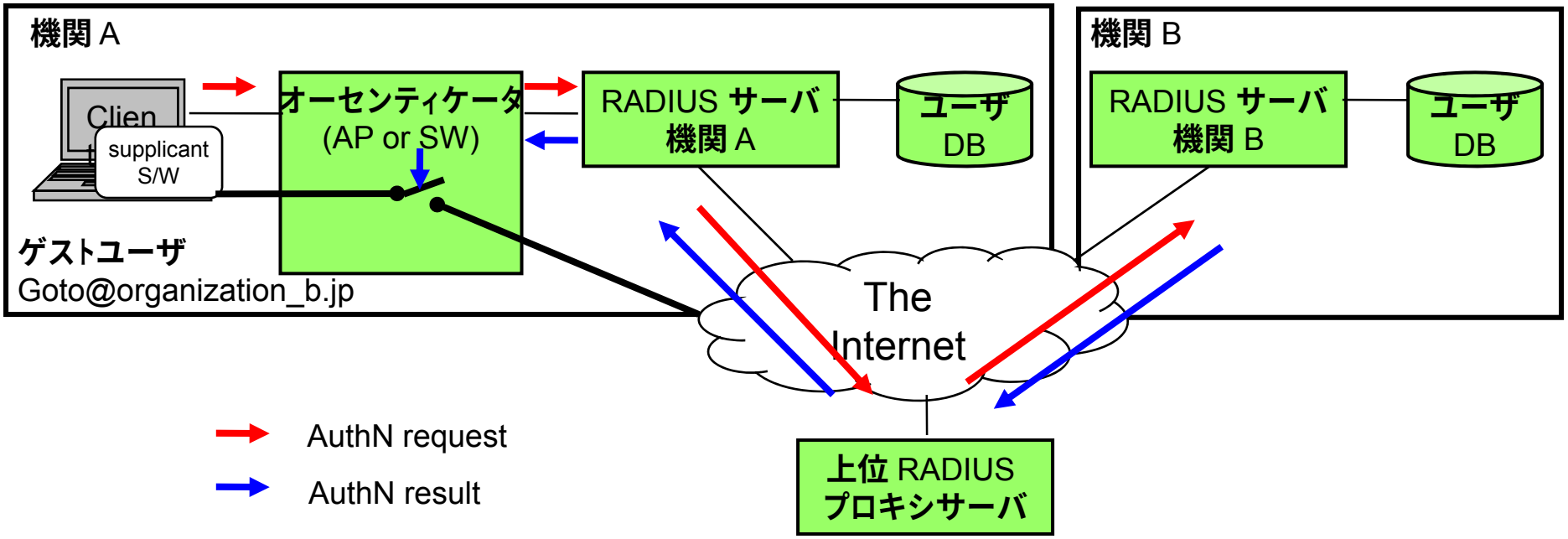
TERENA

- Trans-European Research and Education Networking Association

Amsterdam, Netherland

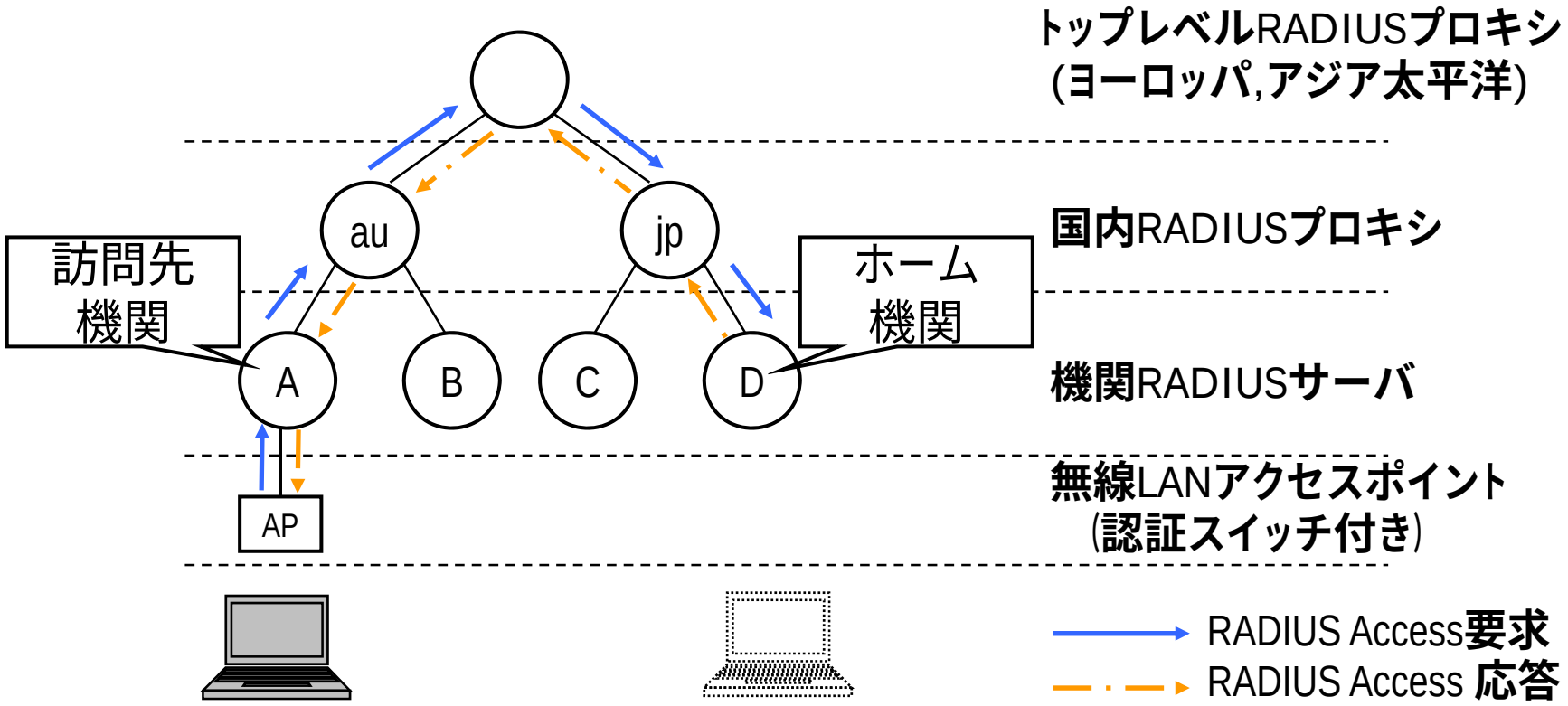
eduroamのしくみ

- IEEE802.1x認証に基づいた，ユーザ認証・認可



eduroamのしくみ　(つづき)

- RADIUSツリーを介して認証情報を相互利用



日本へのeduroam導入

- 2006.8.31 : **東北大学情報シナジーセンターが先行して** eduroam (Asia-Pacific) **に接続**
- 2006.9.28 : eduroam JP **ウェブサイト開設**
- 2006.12 : AP**セカンダリサーバ(香港)と接続**
- 2006.12 : **国情研, 北大, 京大, 高エネ研が接続**
- 2007.6 : **九大が接続**
- 2008 : **名古屋大, 阪大, 山形大が接続**

他機関も常時募集中!

eduroam JP

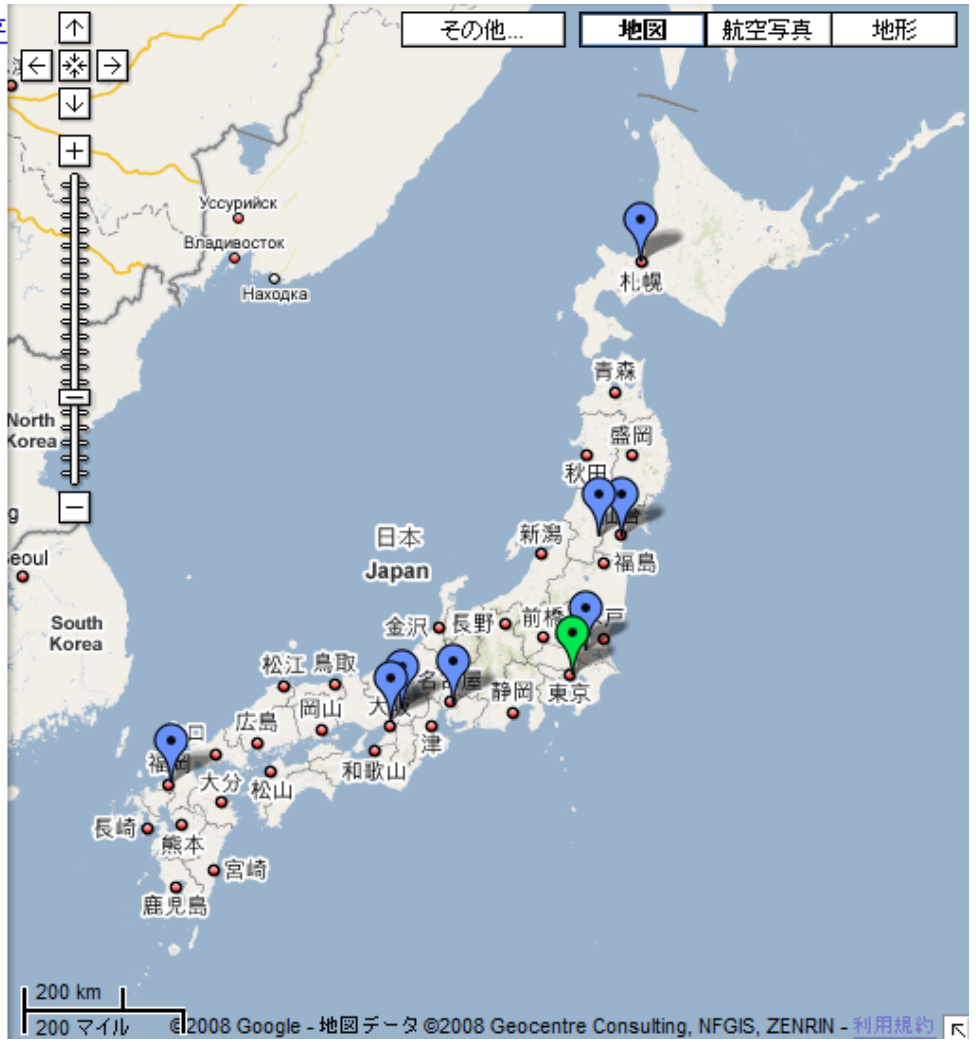
- **国内のeduroam参加機関** (2008.11**現在**)

マイマップに保存

eduroam.jp participants map

eduroam.jp participants map
718ビュー - 一般公開
5月1日作成 - 昨日更新
投稿: HIDEAKI
この地図に評価を付ける - コメントを投稿

- eduroam - Tohoku University
  東北大学 サイト情報 map
- eduroam - Hokkaido University
  北海道大学
- eduroam - Kyoto University
  京都大学
- eduroam - KEK (High Energy Accelerator Research
  高エネルギー加速器研究機構
- eudroam - Nagoya University
  名古屋大学
- eduroam - Kyushu University
  九州大学
- eduroam - National Institute of Informatics
  国立情報学研究所
- eduroam - Yamagata University
  山形大学 (under development)
- eduroam - Osaka University
  大阪大学



eduroam JPのネットワーク構成

国内第一号の
アクセスポイント

プレスリリース (2007.2.22)

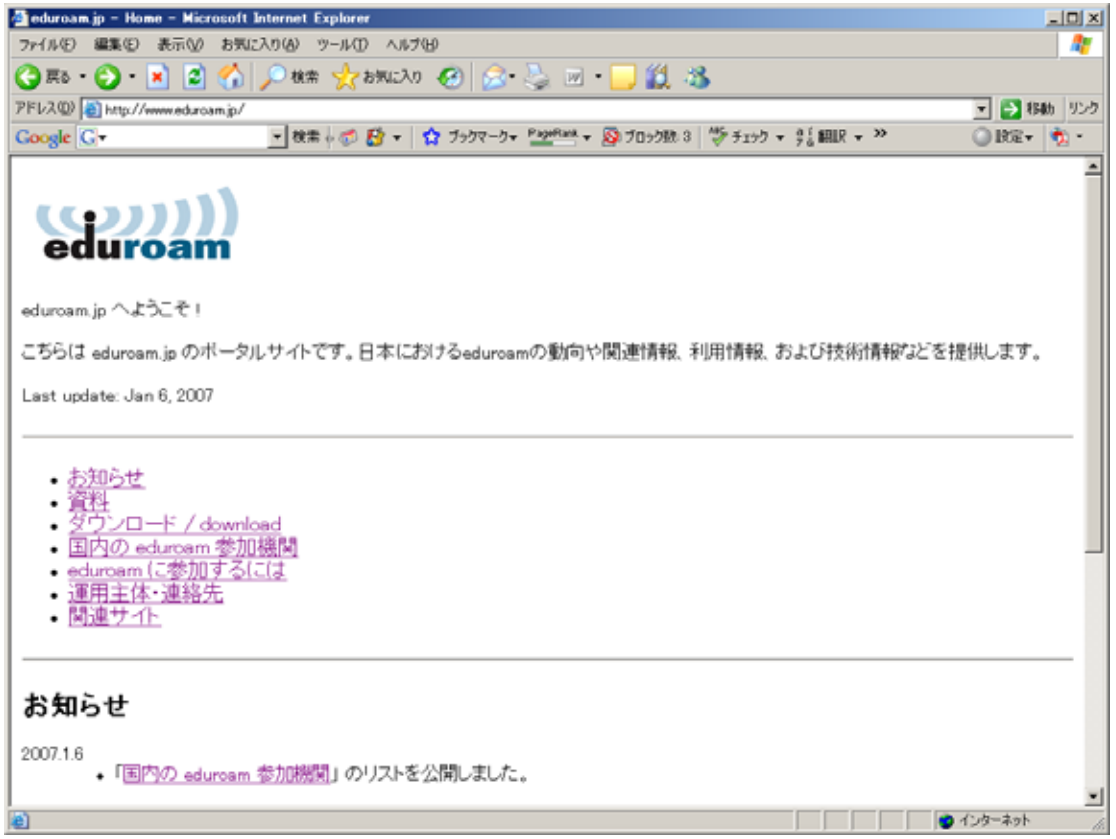
- 「東北大と国情研が国際的な大学間無線ネットワーク相互利用を開始
  – 訪問先の大学でネット利用が可能に・他大学へ普及推進 –」

eduroam JPポータルサイト

参加機関向けの情報提供

http://www.eduroam.jp/

- ニュース
- 参加機関リスト
- 参加サポート
- ソフトウェア提供



eduroam JPに参加するには (機関として)

- **必要な設備**
  - 機関トップレベルRADIUSサーバ
  - 無線LANアクセスポイント
  - ファイアウォール
  - VPNサーバ
- **運用体制**
  - 責任者，最低二名の技術担当者
- **申請方法**
  - 国立情報学研究所 認証作業部会　eduroamグループ　に連絡　(www.eduroam.jp参照)

設備が一切要らない
トライアル環境も準備中！

eduroamを利用するには (エンドユーザ)

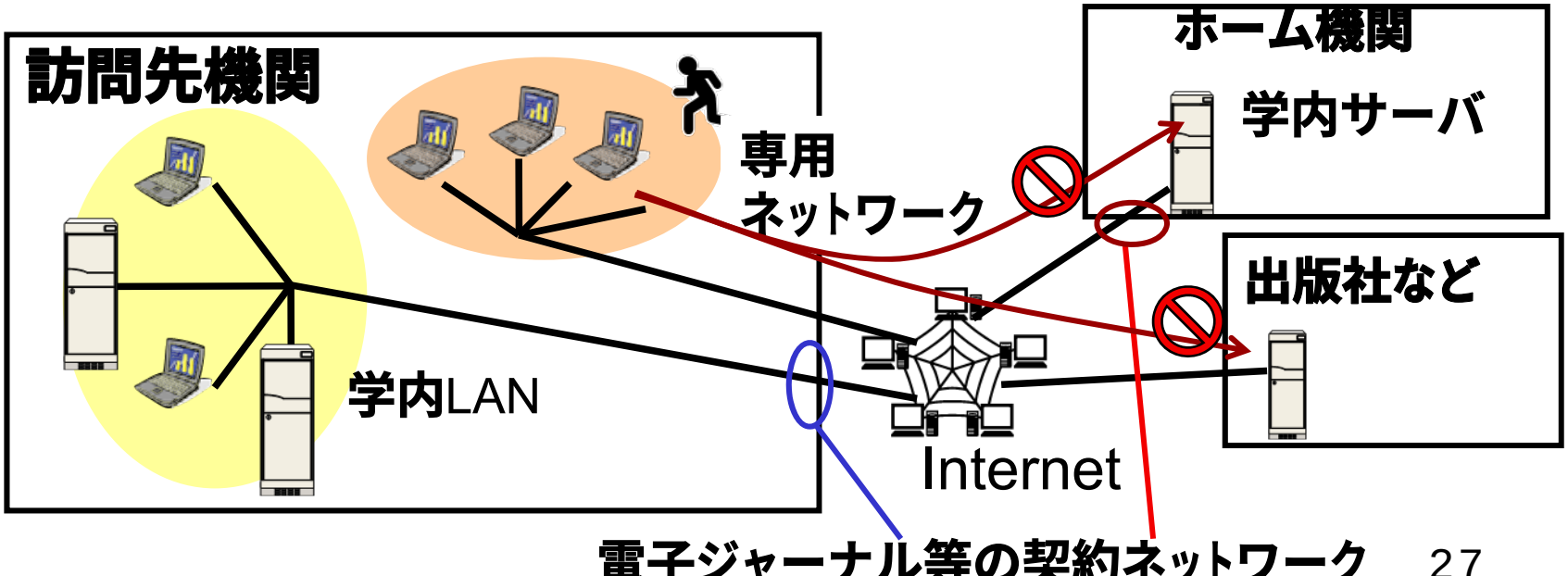
- 所属機関のRADIUSサーバにアカウントが必要
  - 所属機関・部局に申請
- 端末にサプリカントソフトウェアを導入
  - 所属機関で採用している方式 (EAP-TTLS, PEAPなど) のもの
  - PEAPの場合、Windowsならサプリカント不要
- 端末にVPNクライアントソフトウェアを導入
  - PPTPはWindowsで標準対応

従来のeduroamの問題点

- 訪問先機関のアドレスをゲストに自由に利用させる形態(オープンアクセス)が一般的
  - 故意または無意識のネットワーク不正利用における責任の所在が不明確
  - 不正利用者の追跡が困難
  - 電子ジャーナル等の利用規約違反の恐れ
  - 通信制限/監視 (HTTP,SMTP) は運用が困難

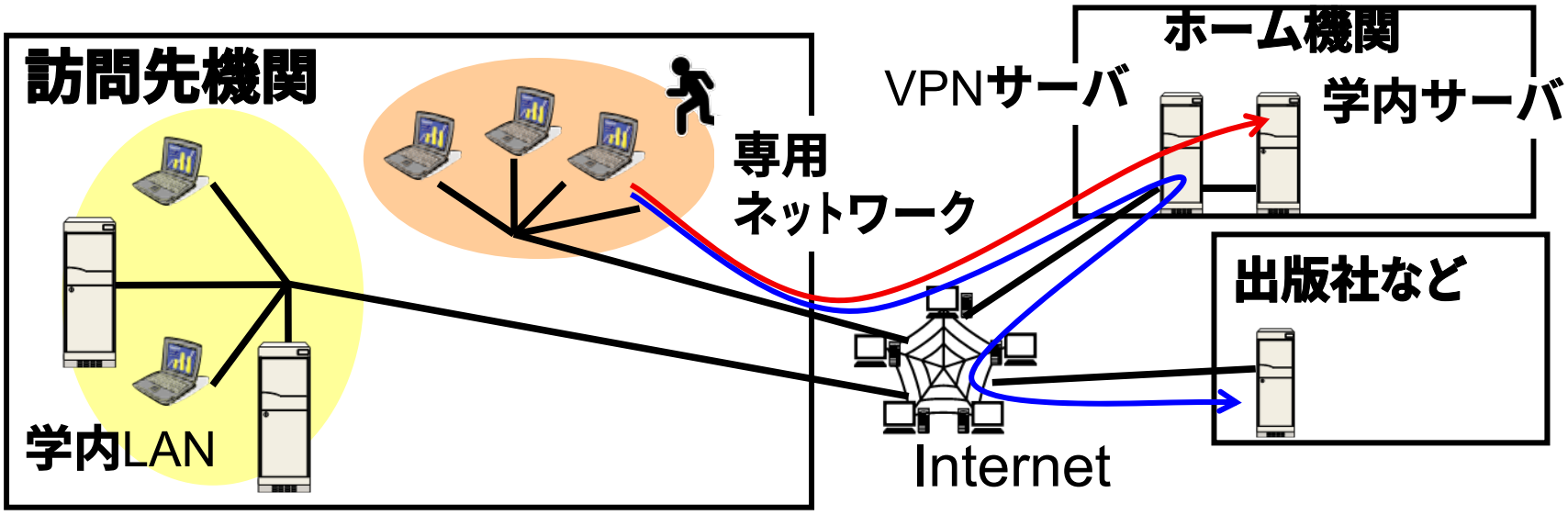
従来のeduroamの問題点 — 解決策1

- ゲスト専用ネットワークの利用
  - 責任問題は部分的に解決可能.
  - 不正利用者の追跡はあいかわらず難しい.
  - ホーム機関のローカルリソースに直接アクセス不可.



従来のeduroamの問題点 ― 解決策1 (つづき)

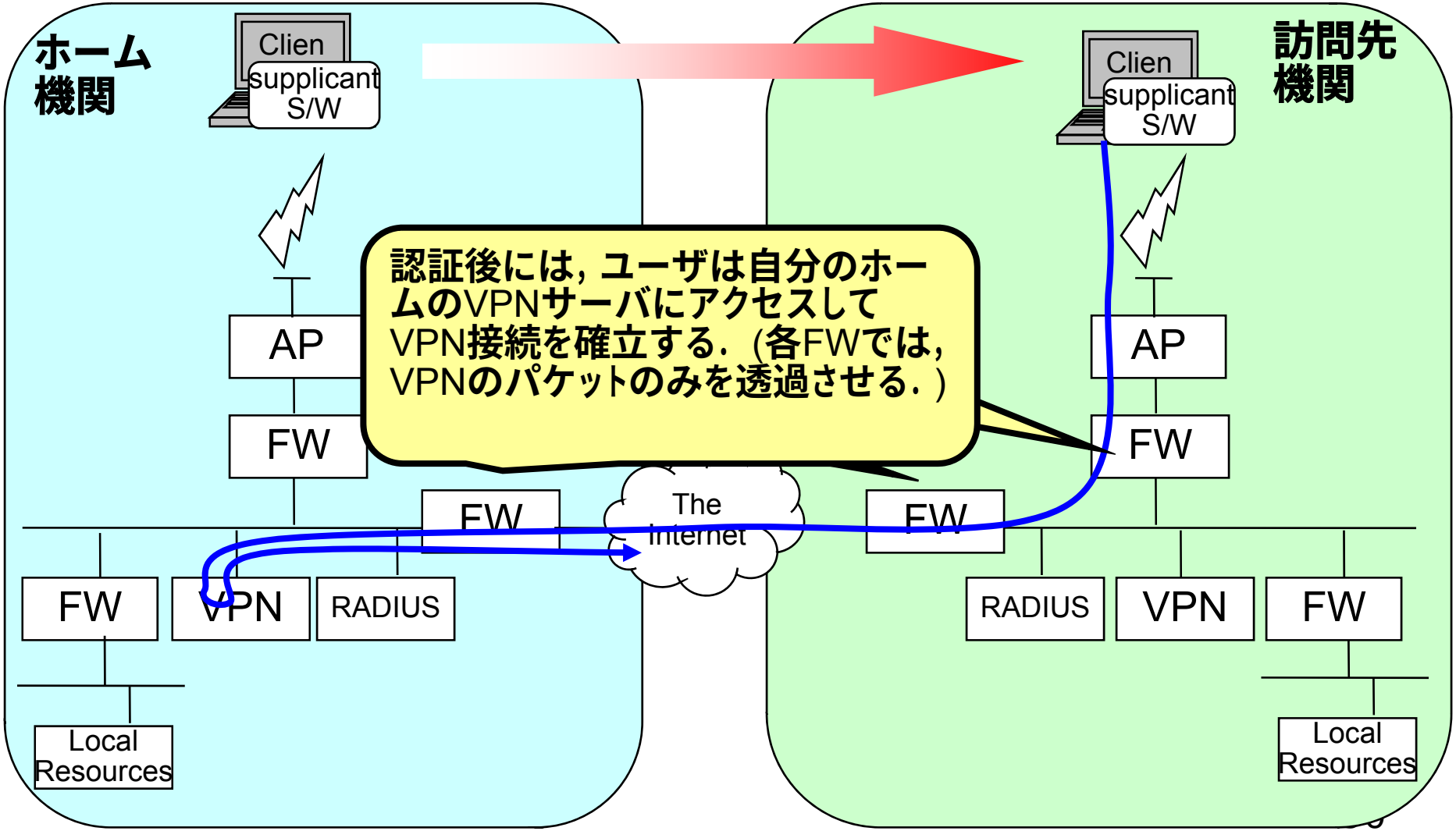
- VPNを併用すると便利に
  - ホーム機関のローカルリソースにアクセス可能.
  - 機関で購読している電子ジャーナルにアクセス可能.



従来のeduroamの問題点 — 解決策2

- VPN接続のみを許す運用
  = VPN-only ポリシーの適用
  - 国内外多くの機関で採用.
    - オーストラリア, 英国, 日本, スイスなど
  - 不正利用者の所属機関がわかりやすい.
  - ホーム機関のローカルリソースが利用可能.

VPN-only ポリシー



VPN-onlyポリシー　通過推奨プロトコル

- PPTP (GRE protocol(47), 1723/tcp)
- OpenVPN (1194/udp, 1194/tcp)
- SSH (22/tcp)
- IPsec NAT-traversal (4500/udp, 4500/tcp, 500/udp)
- L2TP (1701/udp, 1701/tcp)

- pop3 (110/tcp)
- pop3s (995/tcp)
- imap4 (143/tcp)
- imaps (993/tcp)
- ssmtp (465/tcp)
- msa (587/tcp)

eduroam対応システムの構築

- キャンパス利用に合ったセキュリティ対策が必要
  - 大学は教育・研究の場
    - 街の公衆無線LANとは違う
    - 使いやすくて安定なものが必要
    - いざという時のユーザ追跡と教育(指導)の手段を確保
  - 強固すぎて使いにくいシステムではいけない
    - 企業向けのセキュリティ対策は、公衆利用には向かないものが多い
    - やや利便性サイドに倒さないと、ユーザはついてこない

eduroam対応システムの構築 (つづき)

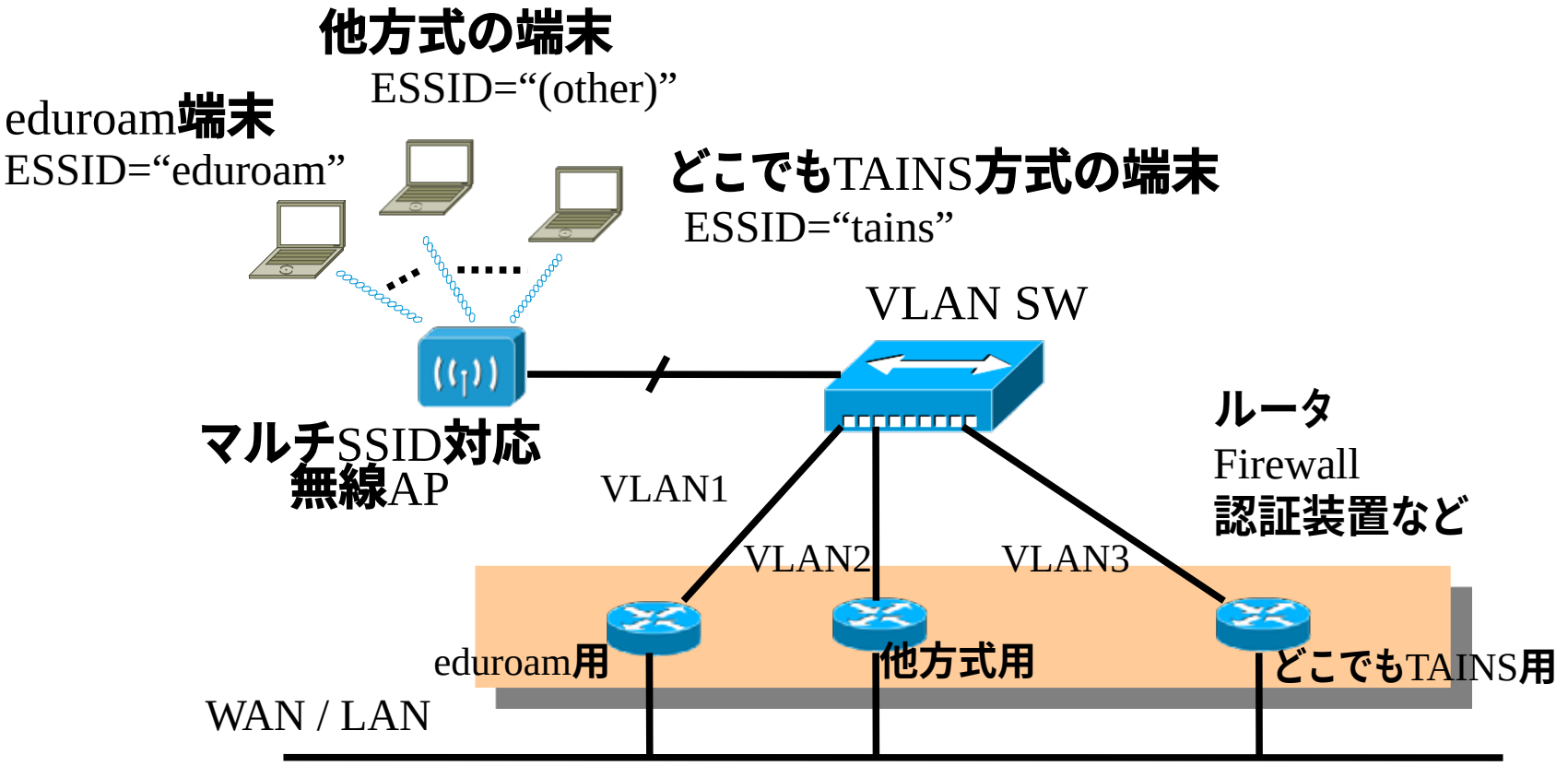
- 大人数のユーザのサポートが必要
  - 学生・教職員で数百～数万人にも！
  - なるべくサポートの手間がかからない方式を選択
- 教育ですべてをカバーしようと思わない
  - ユーザが意識せずとも十分なセキュリティが確保できるようなシステムにする
- ゲスト利用に配慮を
  - 最低限、“eduroam” のSSIDはビーコンを出しておく
  - ロゴの掲示やアクセスポイントマップは有用
  - VPN-only ならば、その旨が分かるように工夫を (例えばキャプティブポータルを利用)

事例紹介： 東北大学における無線LAN

- センターで全学のAP設置などはしない
- 部局ごとに2～3方式の混在システムを自由に構築
  - eduroam
    - 国際ローミング対応
  - 「どこでもTAINS」方式
    - 学内ネットワークTAINSで開発・推奨している，VPNベースの学内ローミング方式
    - PPTPだけで接続できる，高い利便性
    - 家庭用のブロードバンドルータでも構成可能で，導入が極めて容易なシステム
  - 各部局の独自の方式
    - あまり薦められないが，「ウェブ認証方式」など

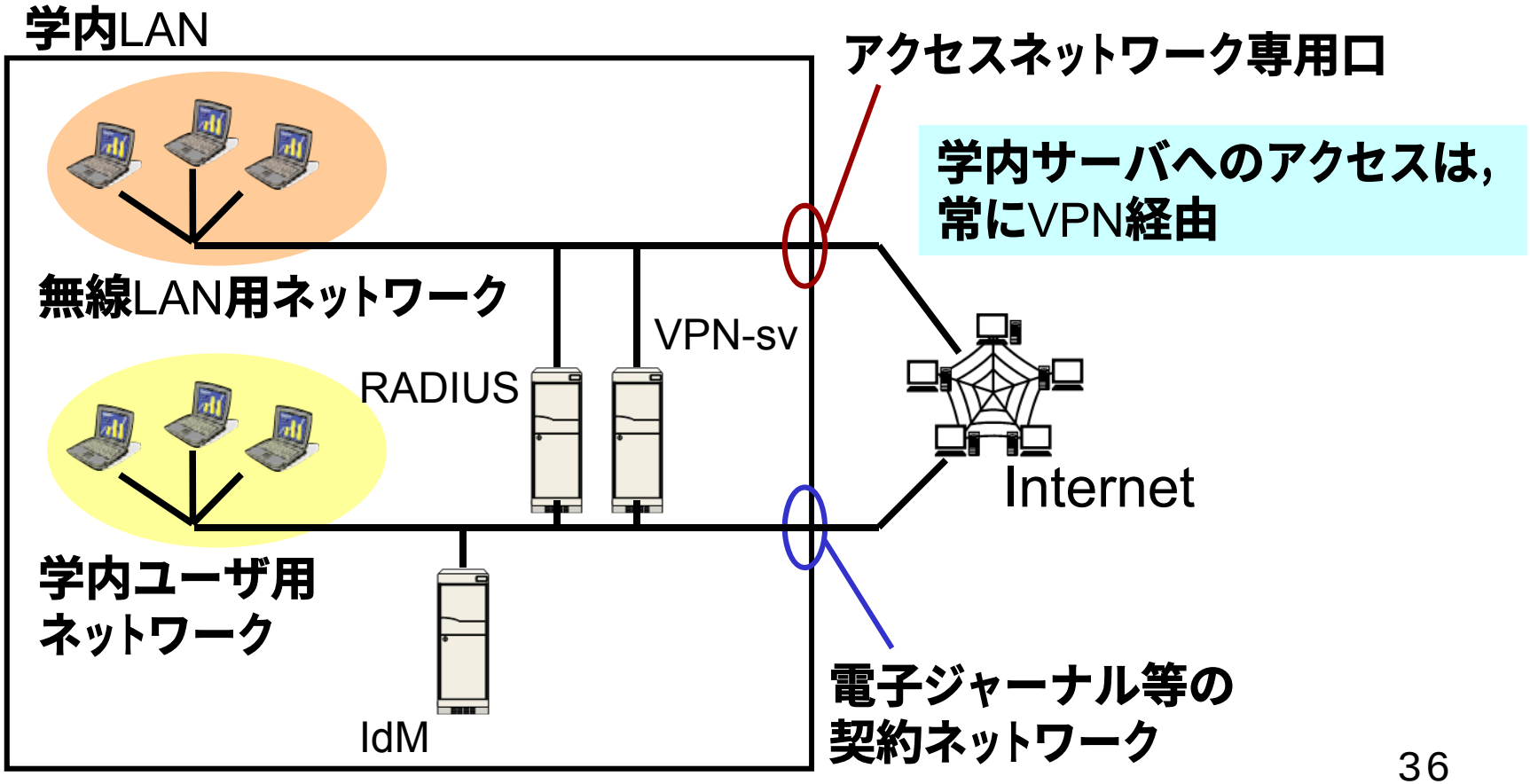
複数方式の同時サービス

- マルチSSID対応の無線LAN機器を利用
  - 複数SSIDが同時にブロードキャストできる製品を選ぶこと！



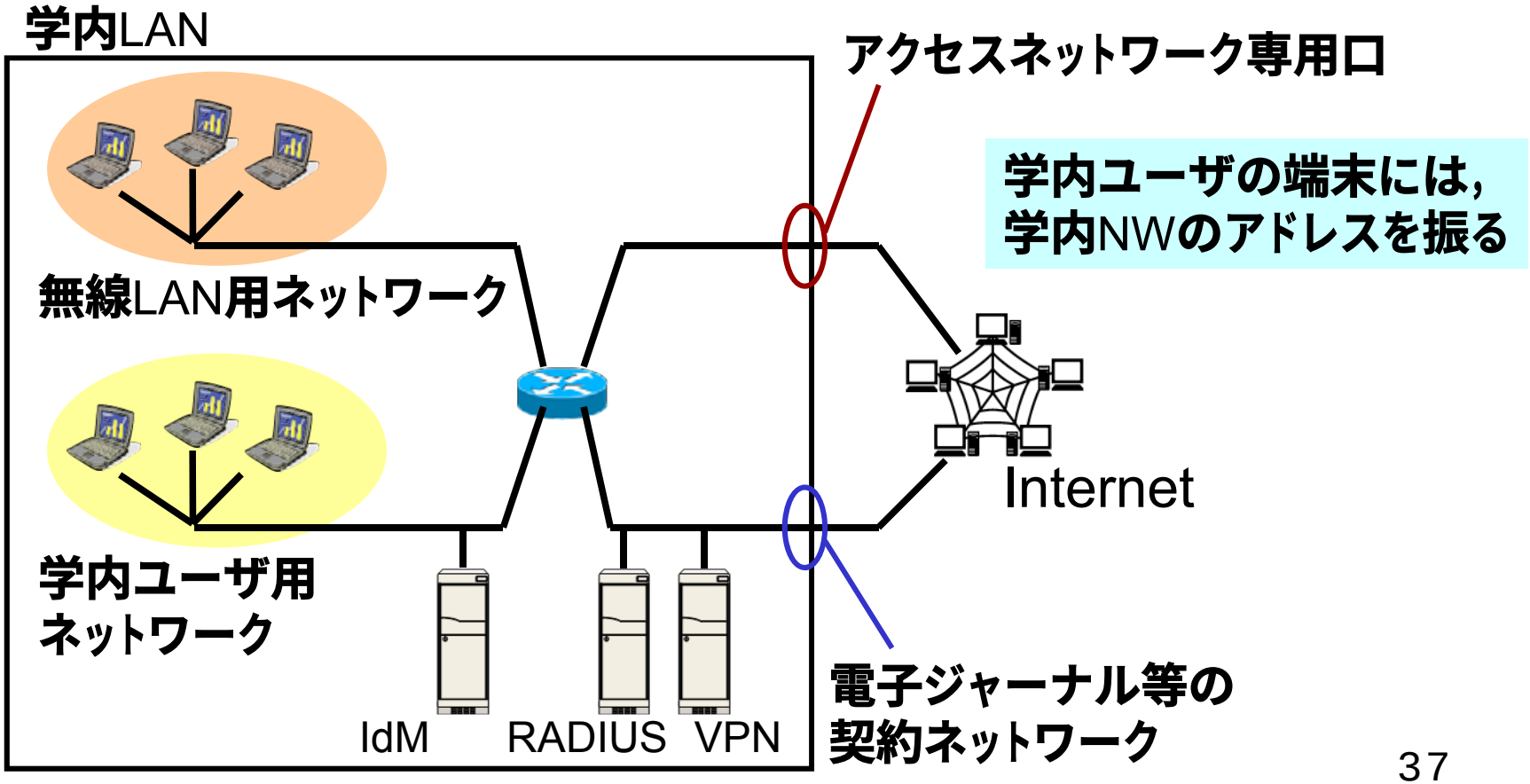
学内ネットワークの構成例 ― その1

- 物理的にNWを分離
- VLANで論理的にNWを分離



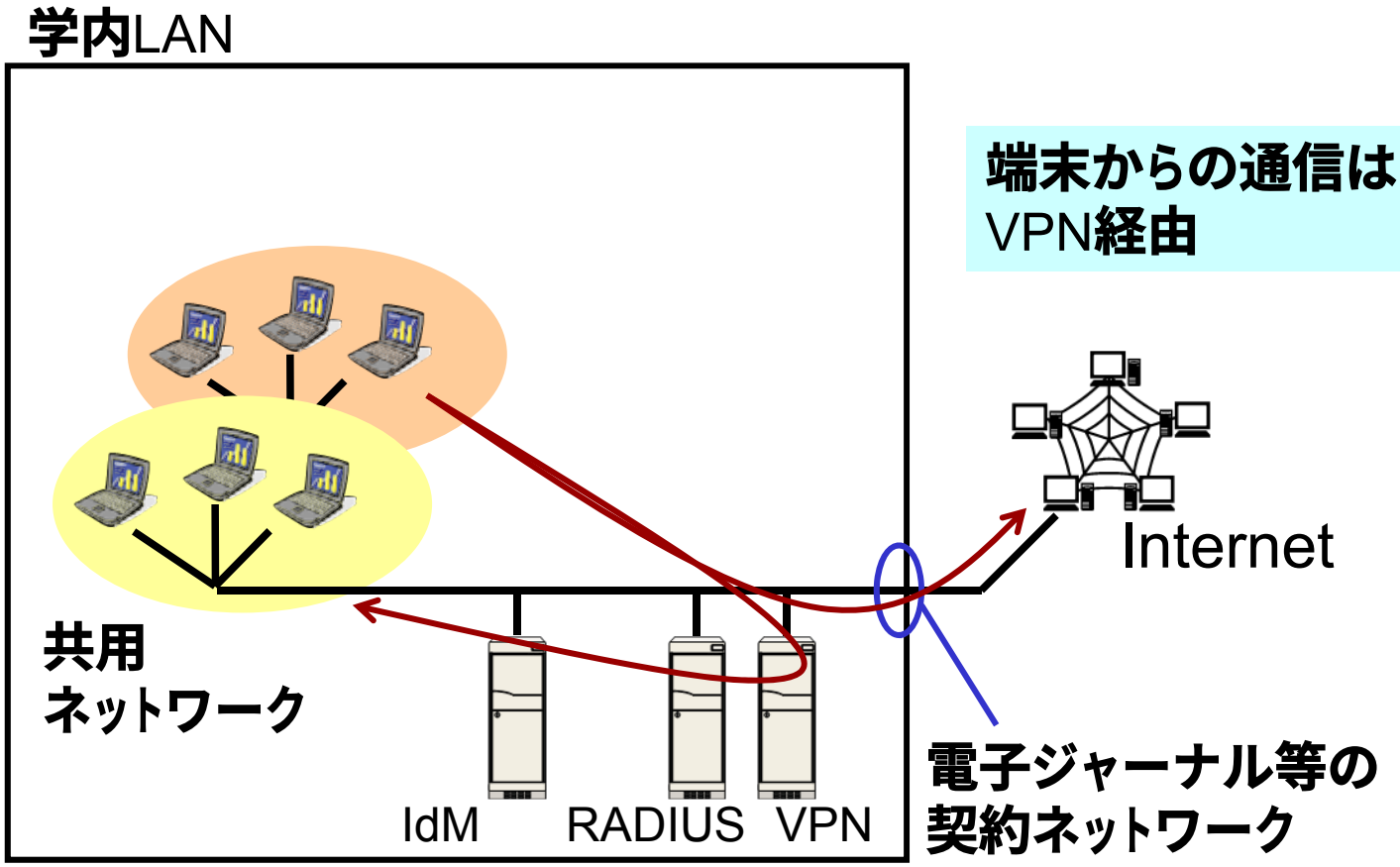
学内ネットワークの構成例 ― その2

- 認証VLANを使い，APの所で論理的にNWを分離
- VPN-onlyのサイトからの利用に備えて，VPNサーバも必要



学内ネットワークの構成例 ― その3

- **無線端末の通信をVPNプロトコルに限定**
  = VPN-only**ポリシーの適用**



デモンストレーション

- eduroamによるユーザ認証
  - Windows XPのサプリカントの設定
  - ログイン操作
- VPN-only環境におけるVPN接続
- 東北大学「どこでもTAINS」によるユーザ認証 (参考)

まとめ

- UPKIによる認証連携
- キャンパスユビキタスネットワークによる、新しい研究環境や教育方法の創造・支援
- eduroamによる無線LANローミング
  - UPKI構築事業で運用中
  - 参加機関を募集中
- eduroam対応システムの構築
  - キャンパス利用に合ったセキュリティ対策が必要
  - 利便性と安全性を両立

参考文献

- UPKIイニシアティブ: https://upki-portal.nii.ac.jp/
- eduroam JP: http://www.eduroam.jp/
- eduroam (Europe): http://www.eduroam.org/
- TERENA: http://www.terena.org/
- **東北大学　AP相互利用システム「どこでもTAINS」:**
  http://www.rd.isc.tohoku.ac.jp/tains-ap/
- **東北大学サイバーサイエンスセンター:**
  http://www.isc.tohoku.ac.jp/
  - **広報誌の中に，学内で構築されたローミング対応無線LANシステムに関する記事があります．**