サイエンティフィック・システム研究会 システム技術分科会 (2008年度第2回)
2009年1月29日

キャンパス無線LANにおける認証連携と国際ローミング基盤eduroam

後藤英昭　東北大学サイバーサイエンスセンター

1

講演内容

- キャンパス無線LAN
- 大学間ローミング
  - 国際無線LANローミング基盤 eduroam
  - eduroamのセキュリティ問題
  - ロケーションプライバシー問題とPseudonymous ID
- キャンパス無線LANの構成方法
- 東北大学の無線LANシステム
  - 「どこでもTAINS」方式

2

キャンパス無線LAN

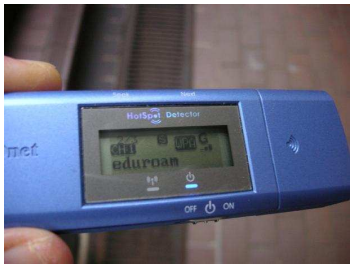
- 国内・国際会議，研究会，集会
  - 教職員、研究者、学生のネットワーク利用環境改善
  - 主催者側の準備負担軽減
- 講義など
  - 講師のネットワーク利用環境の改善
  - ネットワークを利用した新しい授業方法の推進
    - 持ち込みPCによる演習、遠隔講義・プレゼンテーション、VODによる自習、など
  - 単位互換制度による学生移動への対応

3

キャンパス無線LAN

- 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、相互利用システムが必要！

4

キャンパス無線LANの特徴

- 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

5

キャンパス無線LANの特徴 （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
- ゲスト利用に配慮を
  - 最低限、SSIDの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）

6

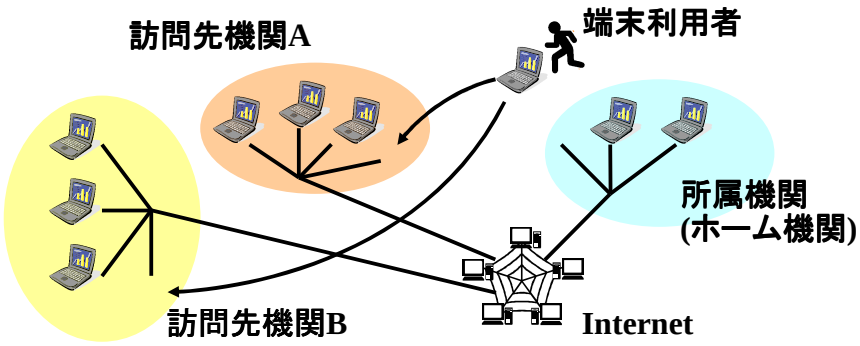
共通無線LANインフラの可能性

- 世界中の機関で共通のシステムを導入できるか?
  - 1ベンダの独占では問題あり
  - 共通仕様にすると、自由度が小さい
  - 相互利用の仕組みは？？？
- 全機関の利用者を統合管理できるか?
  - ユーザアカウントはクリティカルな情報で、一ヶ所に集めるのは難しい
  - セキュリティ的に危ない

7

無線LANローミング

- 認証連携技術により、
  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



8

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
  - 「UPKI共通仕様」の作成と配布
  - NIIによるサーバ証明書の発行
  - 大学間無線LANローミング （eduroam等)
  - コンテンツサービスのシングルサインオンの実現
  - NAREGI-CAを利用した認証局ソフトウェアパッケージの開発
  - S/MIME証明書の運用実験
  - ・・・etc.

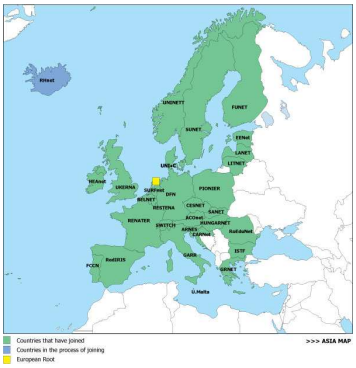
9

エデュローム
eduroamとは

特長： 国際的な無線LANローミング

- 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！



10

エデュローム
eduroamとは

- UPKI構築事業の中で日本に導入
  - 2006年 東北大学が初導入

- セキュリティ上の問題が若干ある（要改良）
- 1X認証のしきいが高い（欠点）

11

eduroam JP

- 国内のeduroam参加機関 (2009.1現在)

eduroam.jp participants map

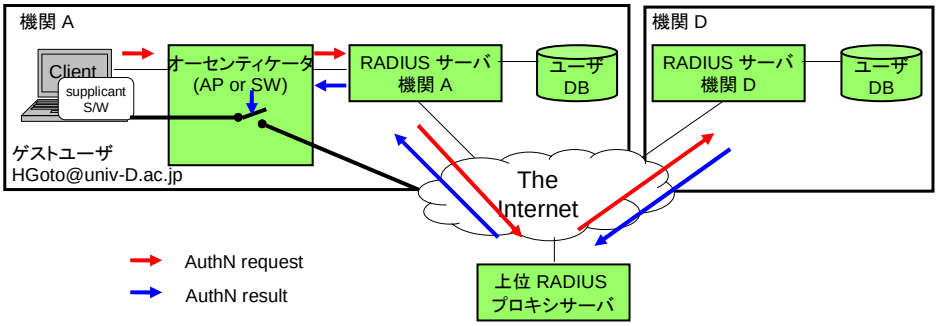
eduroam.jp participants map
1,068 ビュー - 一般公開
5月1日作成 - 1月6日更新
投稿: HIDEAKI
この地図に評価を付ける - コメントを投稿

- 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 サイト情報 map
- eduroam - Osaka University 大阪大学
- eduroam - Shokei Gakuin University 尚絅学院大学

12

eduroamのしくみ

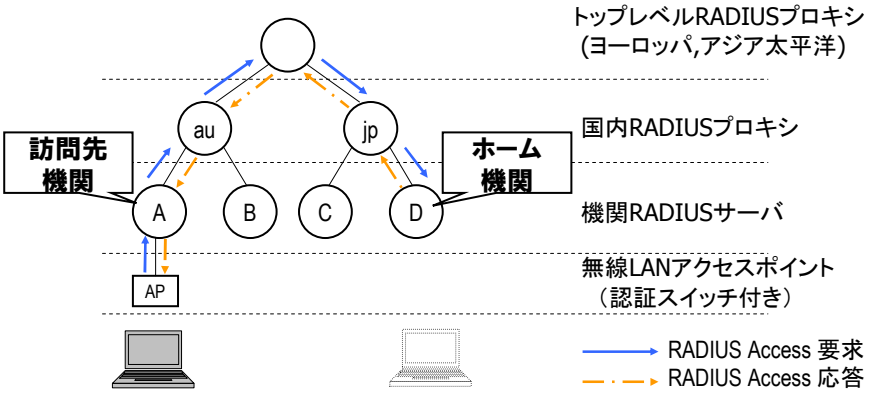
■IEEE802.1x認証に基づいた，ユーザ認証・認可



13

eduroamのしくみ（つづき）

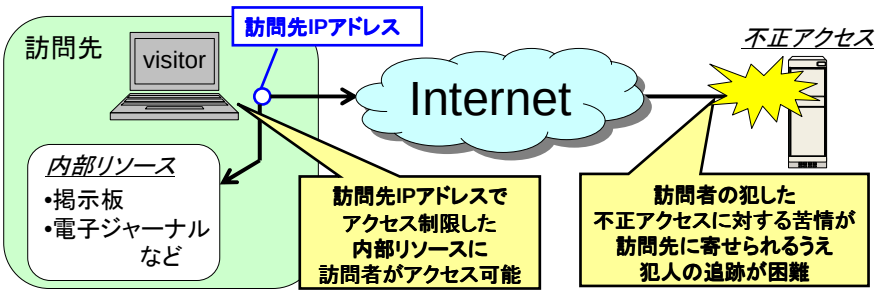
■RADIUSツリーを介して認証情報を相互利用



14

従来のeduroamの問題点(1)

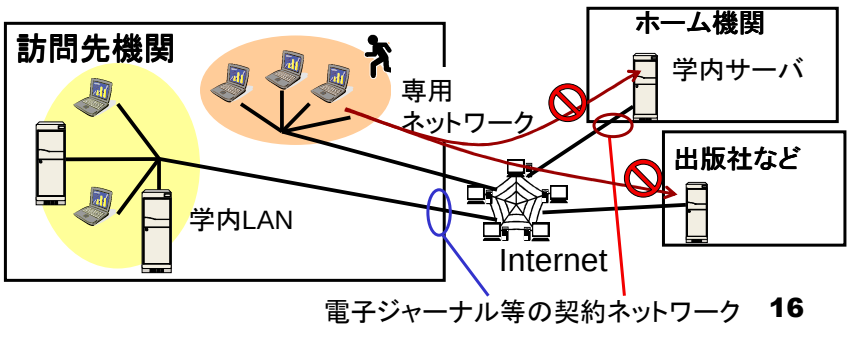
- 訪問先機関のアドレスをゲストに自由に利用させる形態(オープンアクセス)が一般的



15

従来のeduroamの問題点(1) — 解決策1

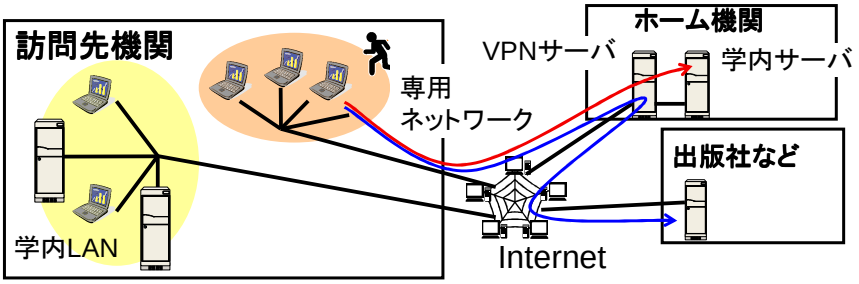
- ゲスト専用ネットワークの利用
  - 責任問題は部分的に解決可能.
  - 不正利用者の追跡はあいかわらず難しい.
  - ホーム機関のローカルリソースに直接アクセス不可.



16

従来のeduroamの問題点(1) ― 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.



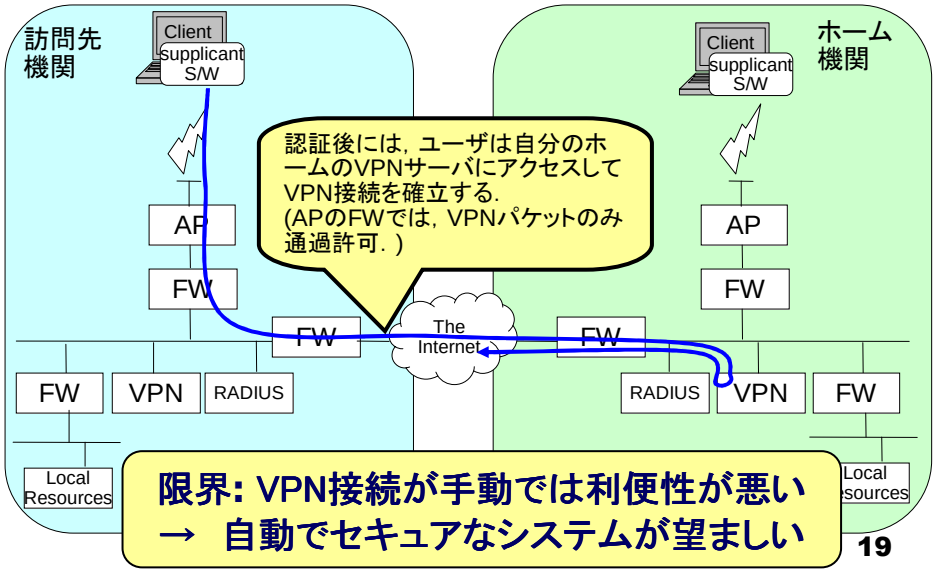
17

従来のeduroamの問題点(1) ― 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.

18

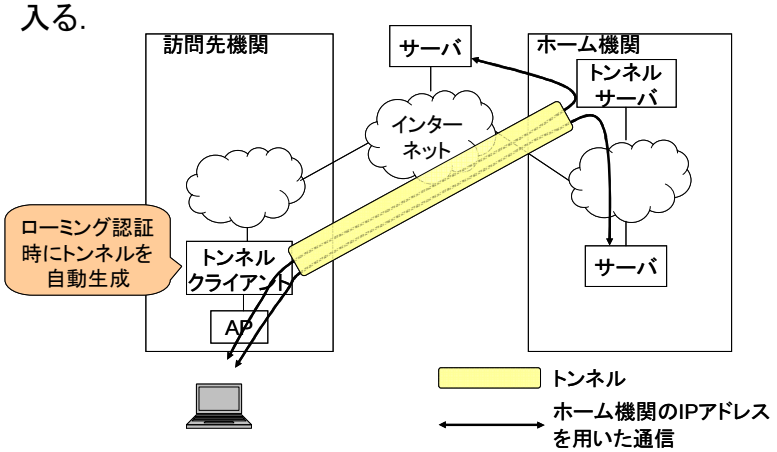
VPN-only ポリシー



19

プロキシVPNによる自動トンネリング方式

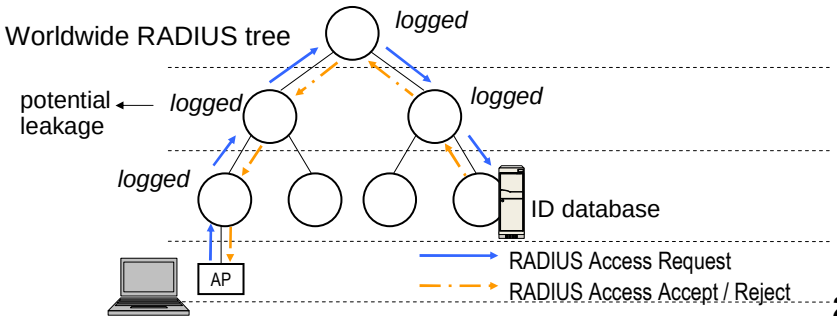
- UPKI事業の中で東北大学が開発中
- 自動トンネリングにより、端末は仮想的にホーム機関の中に入る.



20

従来のeduroamの問題点(2, 3)

- ユーザIDが経路上のRADIUSプロキシのログに残る
  - 利用者が追跡可能 ― ロケーションプライバシー問題
  - ログ採取の是非と併せて問題視され始めた
    （欧州にて，プライバシ保護法とも関係）
- ユーザの不注意により、パスワードがログに残る恐れ
  - パスワード漏洩の危険性



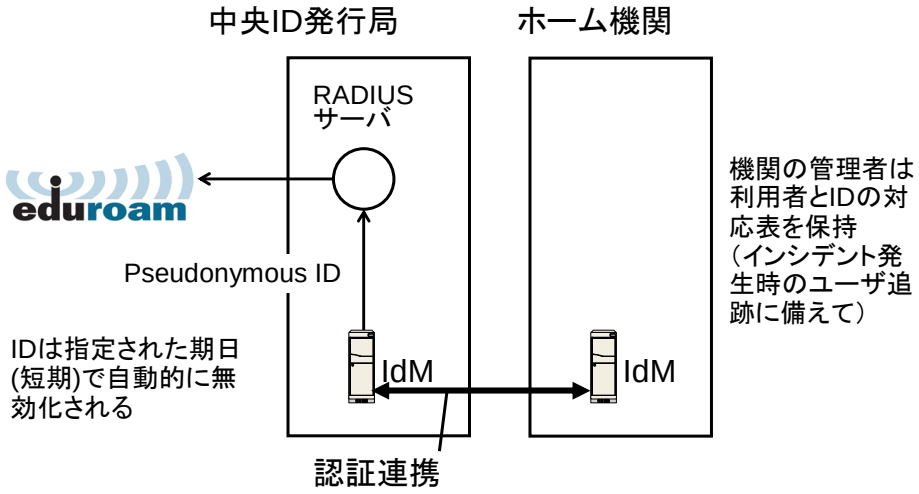
21

Pseudonymous ID の利用

- 通常の利用において、利用者は匿名でいられる
  - ホーム機関以外のプロキシ管理者は、実際に誰が利用しているのかを知ったり予想したりはできない.
- インシデント発生時には、悪意のあるユーザや有害なユーザを追跡可能.
  - Anonymous IDよりも安全で有用.
- 幾つかの国で導入・改定された（されつつある）プライバシー保護法に対応可能か.
  - まだまだ議論の段階…

22

Pseudonymous ID を用いたシステムの例



エンドユーザ自身がIDを請求、取得

23

キャンパス無線LANの構成方法

要望： キャンパスのどこでも同じ使い勝手で
ネットワークに接続したい

- 全学統合の無線LANシステム
  - センターで全学(全キャンパス)にアクセスポイントを設置して，一元管理
- 統一仕様に基づく部局個別システム
  - センターで仕様を提示し，部局ごとに無線LANシステムを構築
  - 認証連携とローミング技術によって，アクセスポイントを相互利用

24

全学統合システム

統一した利用方法を提供できるが、
初期費用・メンテナンス体制・柔軟性が課題

利点

- 統一した利用方法
- 管理・運用等をセンターに一元化

欠点

- 大きな初期導入経費
- 大量APの監視・メンテナンス体制
- 部局からの細かな要望に答えにくい
- センター管理AP用ネットワークを部局の末端(壁コン)まで敷設

25

統一仕様に基づく部局個別システム

スモールスタートができ、柔軟性もあるが、
各部局の負担が大きい

利点

- 小規模な予算でも部分的にシステム構築できる
- 部局内の細かい要望に対応可能
- 学内ローミングも可能

欠点

- 利用方法の統一に要努力
- 各部局がNW設計・管理運用を負担
- ゲスト用NW使用には、センター管理のゲスト用ネットワークが部局の末端(壁コン)に必要

26

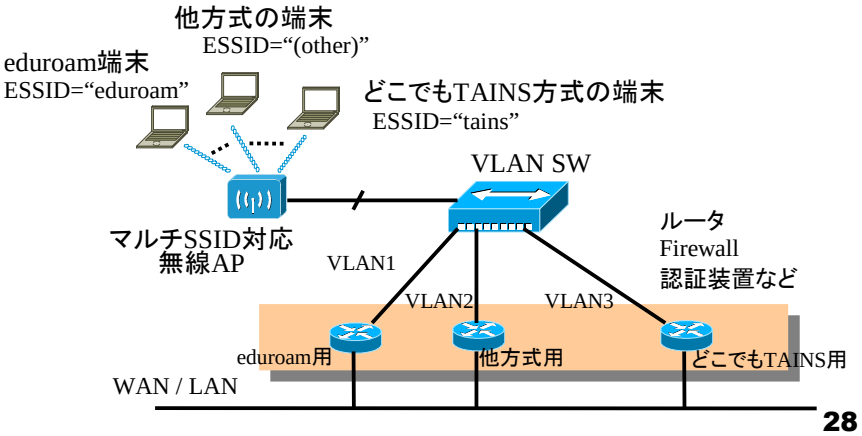
東北大学の無線LANシステム

- 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
  - 「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，学内ローミング方式
  - eduroam
    - 国際ローミング対応
  - 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

27

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ESSIDが同時にブロードキャストできる製品を選ぶこと！



28

「どこでもTAINS」方式

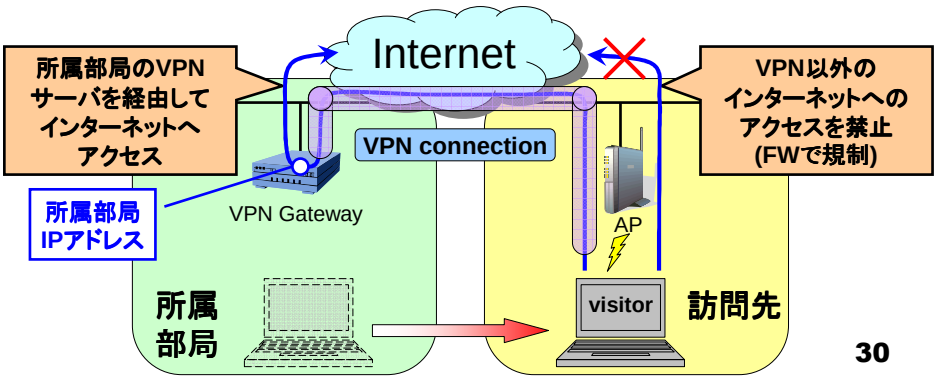
特長： 草の根的なシステム構築

- VPNを利用した学内ローミングシステム
  - センターが共通仕様を開発・提示し，部局ごとに無線LANシステムを構築
  - PPTPだけで接続でき，高い利便性とセキュリティ
  - 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

29

VPNを利用した無線LANローミングシステム

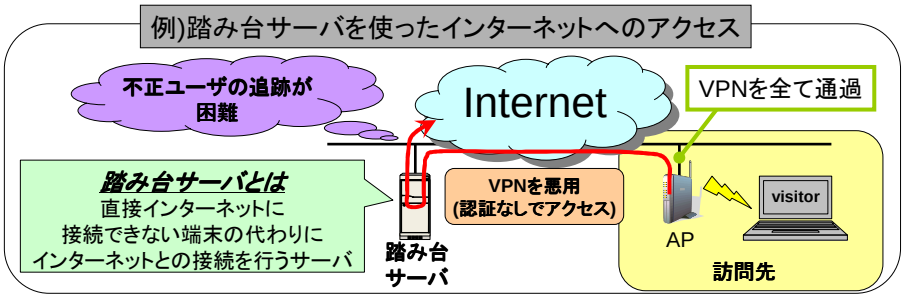
- 訪問者に所属部局のLANへVPNを張らせる
  - ユーザに対する責任の所属が明確になる
  - 訪問先の内部リソースを守る



30

セキュリティ確保のためにVPNを利用したシステム　で要求されること

- VPNを全て通過させてしまうと……
  - VPNのポート番号(プロトコル番号)を悪用される危険性



- 踏み台サーバが存在しない部局（機関）に対して
  VPNの通過のみを許可するアクセス制御が必要

31

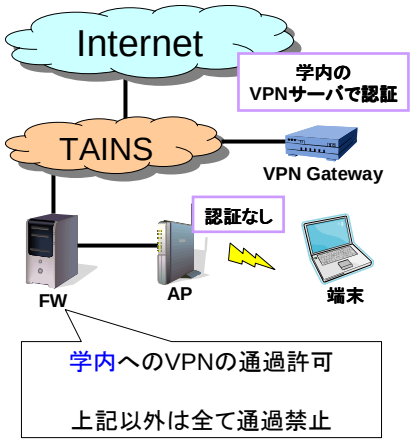
「どこでもTAINS」のしくみ

- 東北大学の学内ネットワーク「TAINS」で展開

TAINSの利用規則
不特定多数が利用可能な
踏み台サーバの設置禁止

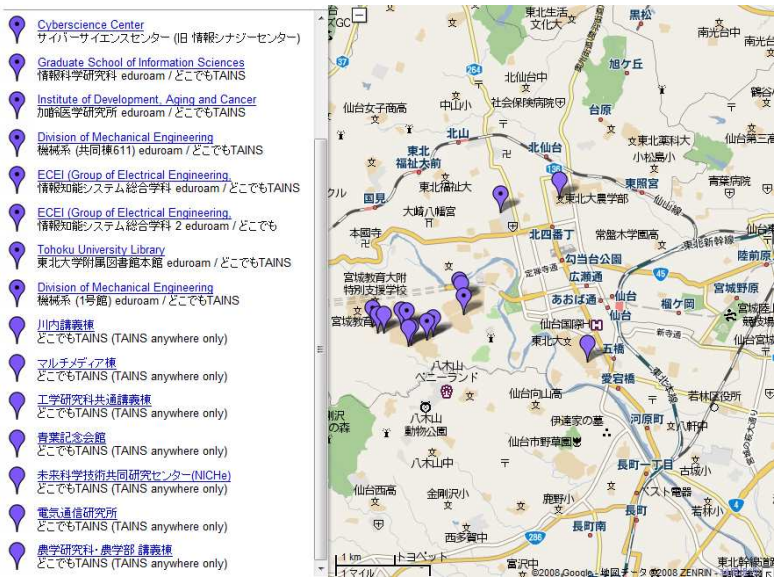
- 踏み台サーバが存在しない学内のみにVPNを通す

利用範囲は学内に限定



32

「どこでもTAINS」アクセスポイントマップ



33

まとめ

- キャンパス無線LANには、商用公衆無線LANと異なる要求がある
- 国際無線LANローミング基盤eduroam
  - ゲストに配るIPアドレスの問題
  - ロケーションプライバシー 問題 / パスワード漏洩問題
    - Pseudonymous IDによる対策
- 東北大学では複数ローミング方式を展開
  - 学内は利便性の高い「どこでもTAINS」
    - 草の根的なローミングシステム構築
  - 学外はスタンダードな「eduroam」

34

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.

35

VPN-onlyポリシー 通過推奨プロトコル (参考)

- 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)