資料2

WiMAX網を活用し、セキュアに学内LANに接続する取り組み

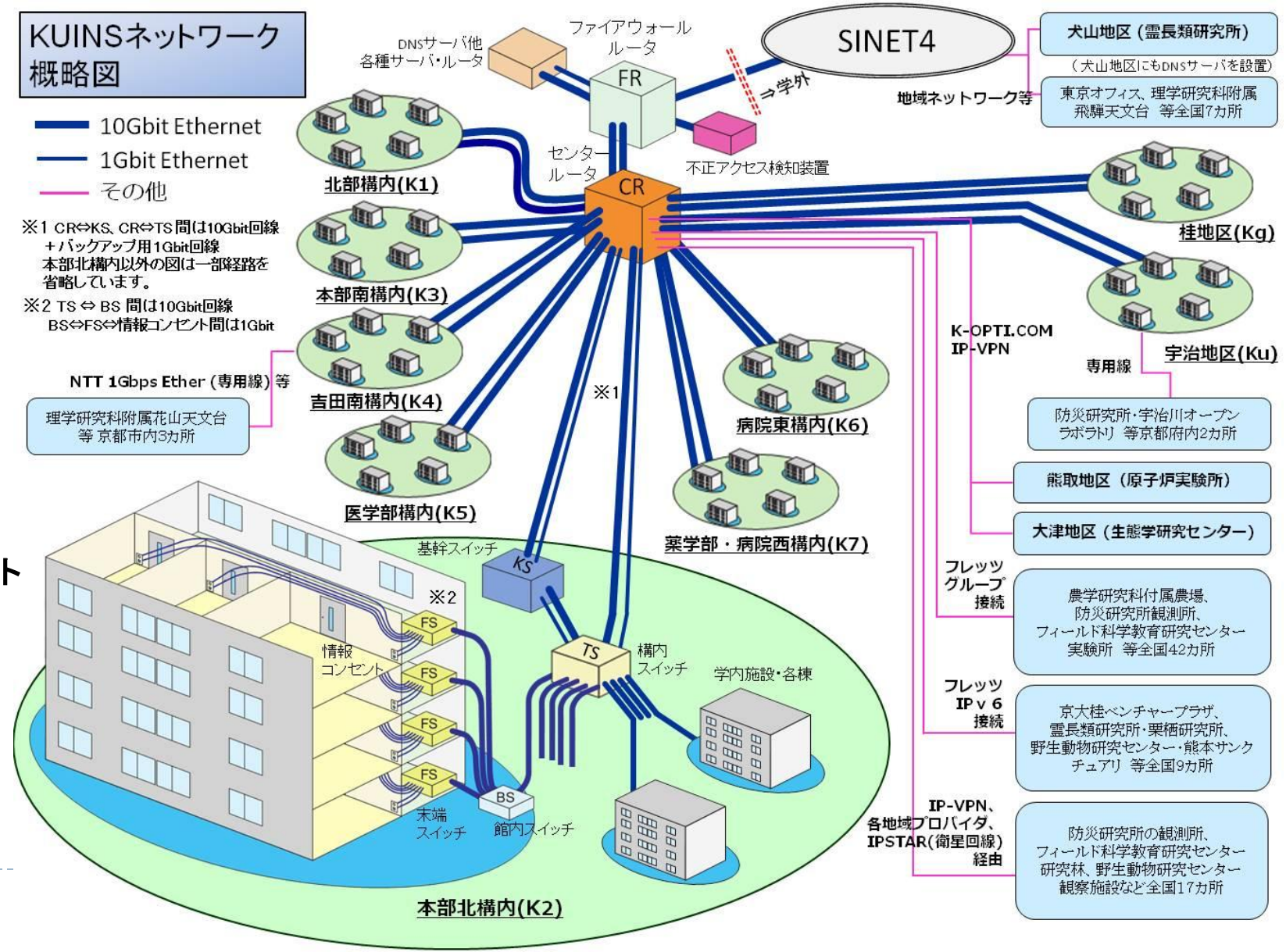
岡部 寿男（京都大学学術情報メディアセンター）

平成24年7月4日
学術情報基盤オープンフォーラム

概要

- 京都大学の学内LANであるKUINSにおいて、UQコミュニケーションズ（株）との提携により、UQ WiMAXを利用し直接イントラネット(KUINS-III)へのアクセスを可能にするサービスを開始（2012年4月1日）
  - 京都大学の構成員（教職員・学生）は、WiMAX仕様のWi-Fiルータ やWiMAX内蔵のPC等から、VPN接続等の設定・操作なしにKUINSに接続可
- UQC社のモバイルWiMAXネットワークとの接続にはSINET4のL2VPNを利用
- 契約時の利用資格（学内構成員であること）の確認には学認を利用

KUINS (Kyoto University Integrated informaiton Network System) 概要



情報コンセント

KUINSの規模

ネットワーク

グローバル IPアドレス	：	約　2,500個
グローバル サブネット	：	約　 500 個
プライベートVLAN	：	約　4,200個
情報コンセント	：	約 21,000 個
遠隔地接続	：	83 箇所

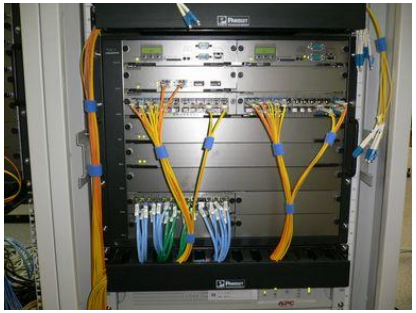
ハードウエア

ルータ、スイッチ等

- メインルータ: 4台
  （対外接続、学内接続）
- 構内スイッチ: 10台
- 基幹スイッチ:　4台
- サーバスイッチ: 3台
- 館内スイッチ: 約　250台
- 末端スイッチ: 約1,200台

サーバ類

- DHCPサーバ: 20台
- DNSサーバ: 4台
- NATサーバ: 10台
- VPNサーバ:1台
- メールー中継サーバ: 16台
- PPTPサーバ: 13台
- SSHポートフォワードサーバ: 1台
- 不正アクセス検知装置　1式
- 電子メールファイアーウオールサーバ: 2台
- SPAMメール検知サーバ: 4台
- ログ収集サーバ: 6台
- WEBプロキシサーバ: 20台



KUINSのサービス（有線系）

- 情報コンセントによる有線接続
  - KUINS-II
    - グローバル固定IPアドレス
    - IPアドレス単位のサービス
      - IPアドレスとMACアドレスの組を登録
    - 月額1,500円（IPアドレス毎に）
  - KUINS-III
    - プライベートIPアドレス、DHCP
    - 学外への接続はproxyを利用
      - POP, IMAPなどだけNAT
    - 情報コンセント単位のサービス
      - VLAN（サブネット）と情報コンセントの対応付け
    - 月額300円（情報コンセントのポート毎に）

KUINSのサービス（無線系）

- 学内の様々な施設（主に公共スペース）に、約1,000台の無線LAN基地局を設置

・みあこネット方式（PPTP接続利用）
教職員用アカウント（SPS-ID）、学生用のアカウント（ECS-ID）、ビジター用アカウントで利用。

・eduroam方式
- eduroamアカウント（大学間連携のアカウント）で利用。
- 他大学のeduroamアカウント保持者も利用できる。
- 上記のビジター用アカウントでも利用可能。
- 学外のアドレスが割り当てられる。

・Livedoor wireless
- 学内の約100か所に、Livedoor Wirelessにも対応した基地局を設置（主に生協食堂や時計台記念館など外部者も出入りする場所）
- 事業者と契約することで構成員以外でも利用可能

KUINSのサービス（学外からのアクセス）

1. PPTP接続

学外（自宅等）にいながら、大学内で利用するのと同様の環境で
ネットワークに接続できるサービス（「SPS-ID」、「ECS-ID」で認証）

- 学内限定のホームページの閲覧
- 学内でしか利用できない電子ジャーナルへのアクセス
- 教職員グループウエアへのログイン

さらに、PPTP-VLAN固定接続サービス（自宅から、研究室のネットワークに繋がる）

単なるPPTP接続に加えて、あたかも研究室内にいるかのように

- 研究室のサーバとのファイル共有
- 研究室のプリンタへの印刷
- リモートデスクトップの利用

なども可能

PCからの利用はよいが、スマートホンなどからの利用に課題

- 端末ごとの差異（特にAndroid）によるサポートコストの増
- 端末が移動するごとにVPNの再接続が必要

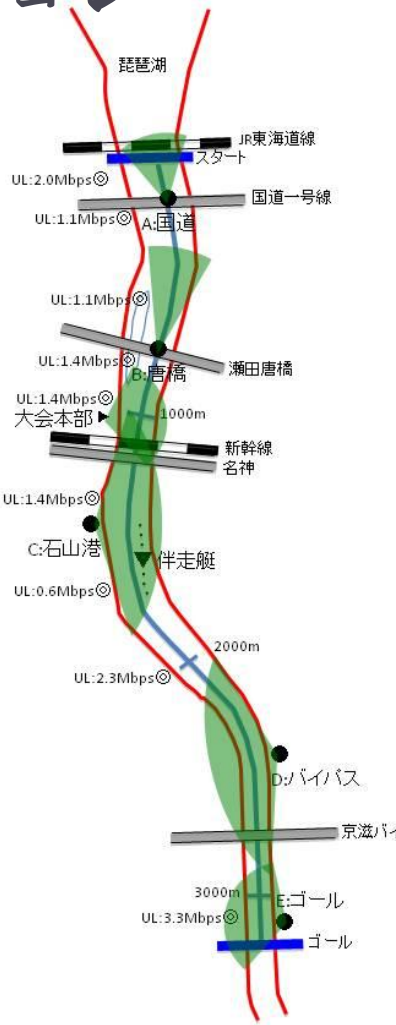
2. その他のVPN接続

SSH Port-forwarding, SSL-VPN
OpenVPN, SSTP（準備中）

3. UQWiMAX

京都大学とUQWiMAXとのコラボレーション

- UQ WiMAXのサービス開始（2009年7月）
  - 吉田キャンパス、宇治キャンパス、桂キャンパスのほぼ全域がカバーエリアに
    - 吉田キャンパス内に四か所（北部構内、本部構内、吉田南構内、薬学部構内）に基地局設備を設置
- 京大・東大対校ボート競漕大会の手作り実況中継（2010年6月）
  - 瀬田川で行われるレースを、SkypeおよびUstreamを用いて中継。回線には主としてWiMAXを利用



UQコミュニケーションズ社からの提案（2011年夏）

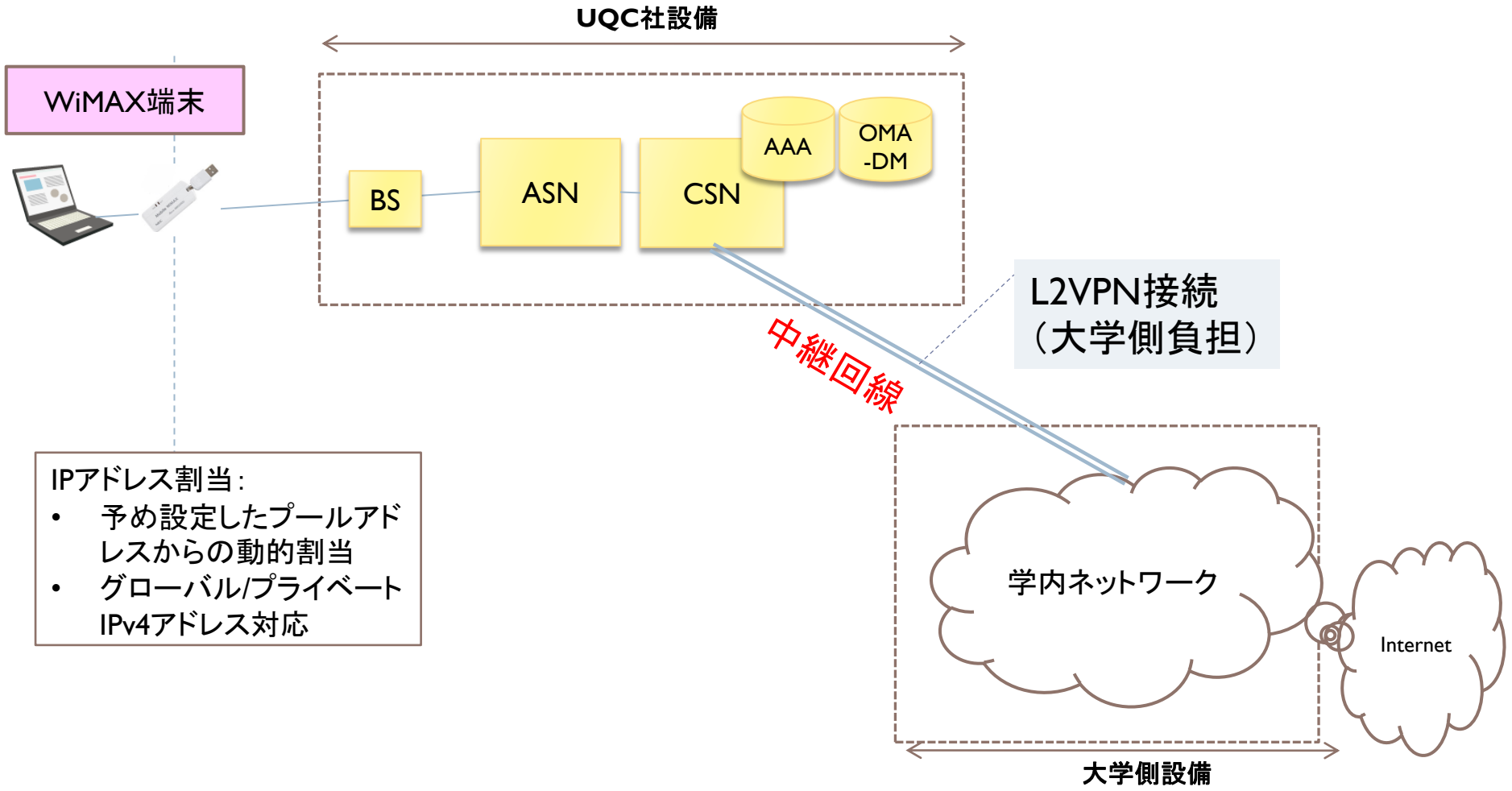
WiMAXによるキャンパスネットワークアクセス

- 同社は2011年4月より慶應義塾大学において「モバイルWiMAXによるキャンパスネットワークアクセス」のサービスを開始
  - 学内ドメインメールアドレスや学生証等を利用して学内ネットワークへのアクセス権を確認
  - 市販のWiMAX製品から接続するだけで学内ネットワークに直接接続
- 同種のサービスを、京都大学においても提供したいとの申し入れ

サービス導入にあたっての検討

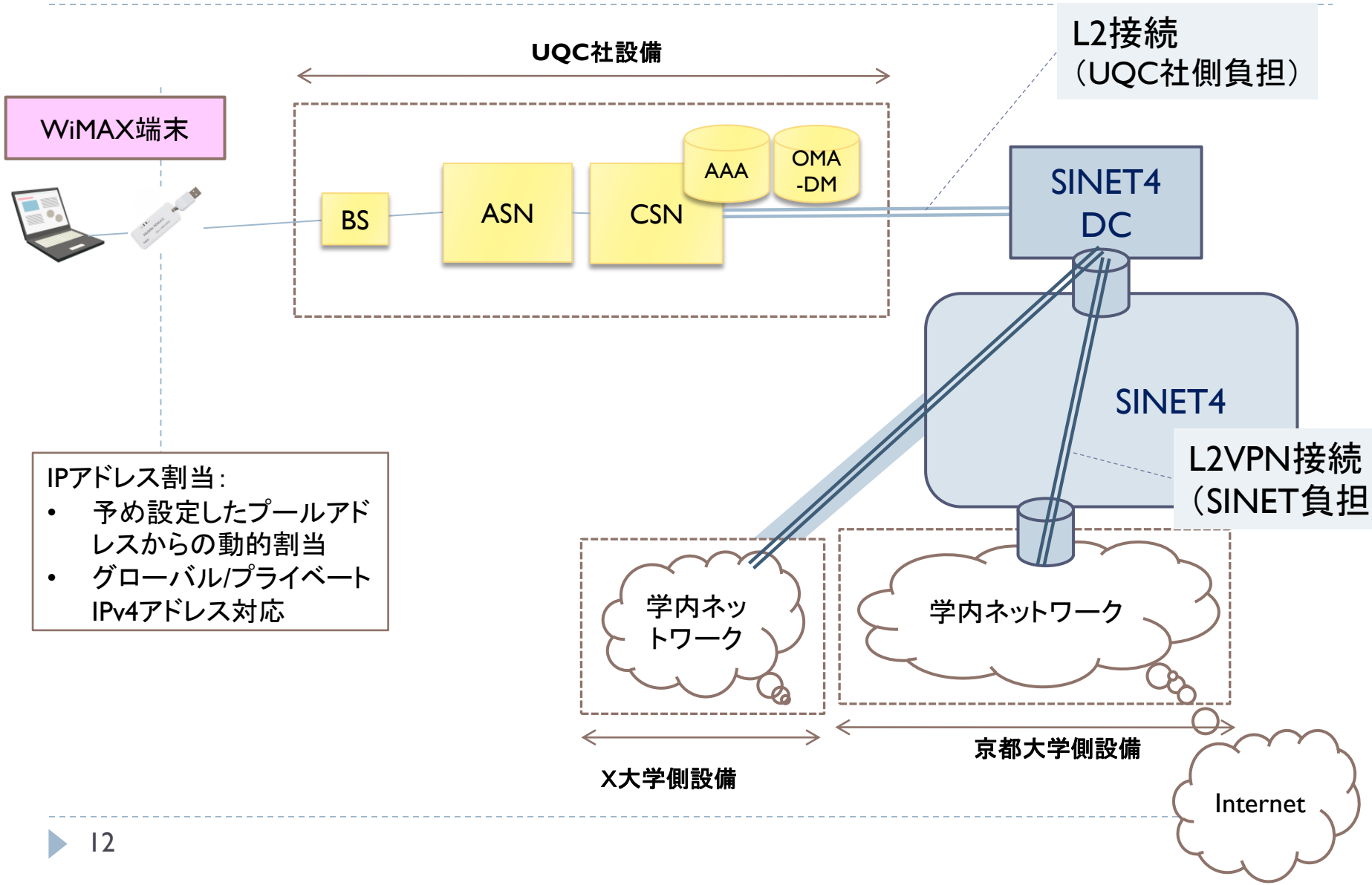
- 京都大学としてのメリット
  - 利用者が学外からKUINSへ接続する際に、VPN設定・操作が不要
    - 設定にかかるサポートコストの削減
    - VPNサーバの負荷軽減
  - 利用者へ、安全なネットワーク環境の提供
  - 料金も若干安い(?)
- UQコミュニケーションズ（UQC）側のメリット
  - モバイルWiMAXサービスの利用拡大
  - 上流ISPへの帯域の削減
  - IPv4アドレスの削減
- 課題
  - 中継回線のコスト負担
  - 契約時の在籍確認における個人情報保護

ネットワーク構成（UQC社の提案）



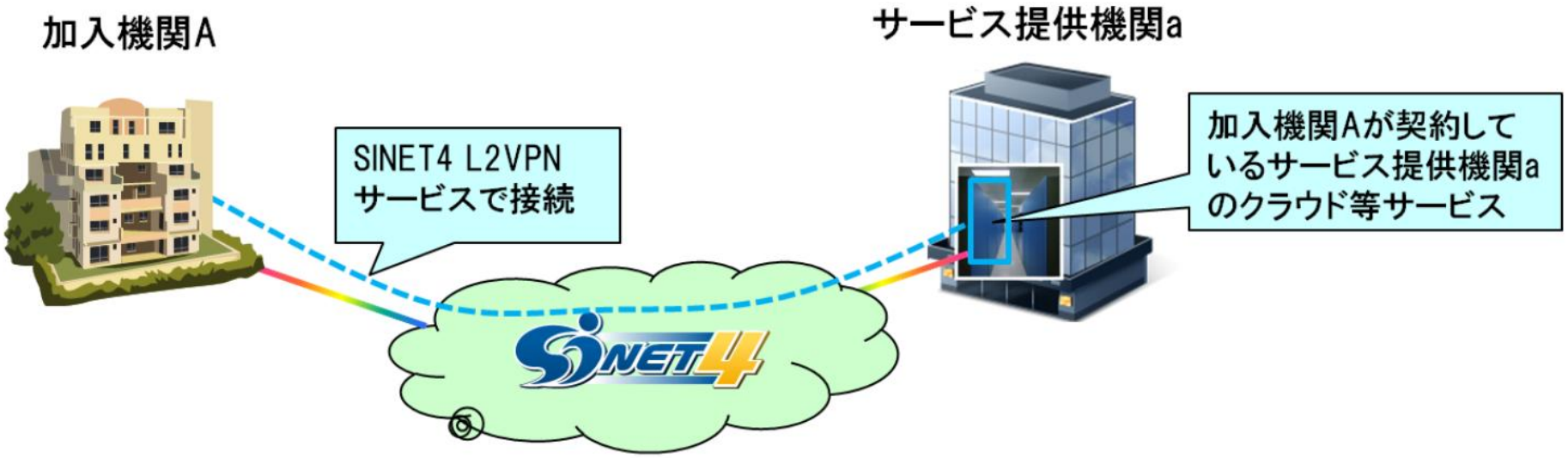
IPアドレス割当：
- 予め設定したプールアドレスからの動的割当
- グローバル/プライベートIPv4アドレス対応

ネットワーク構成（京都大学からの逆提案）



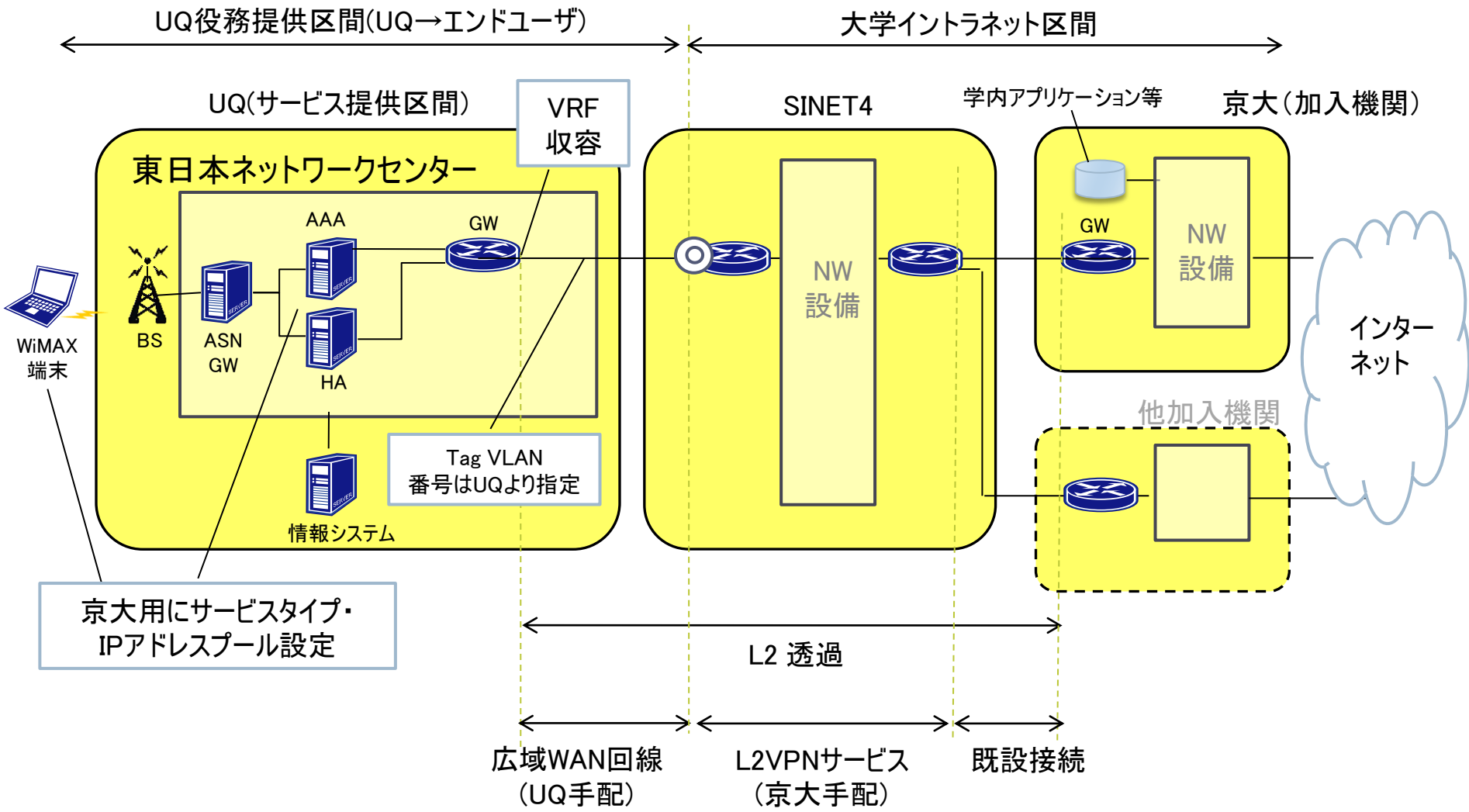
SINET加入機関向けサービス提供機関からの接続

- http://www.sinet.ad.jp/service/other/cloud_services



SINETでは、新たに上位レイヤサービス（ストレージ、メール等）を提供する機関を「サービス提供機関」と位置付け、上位レイヤサービスの利用を希望するSINET加入機関との橋渡しをおこないます。これにより、例えば民間のデータセンターがSINET加入機関向けのサービス提供のために直接SINET4 DCに接続することが可能となります。

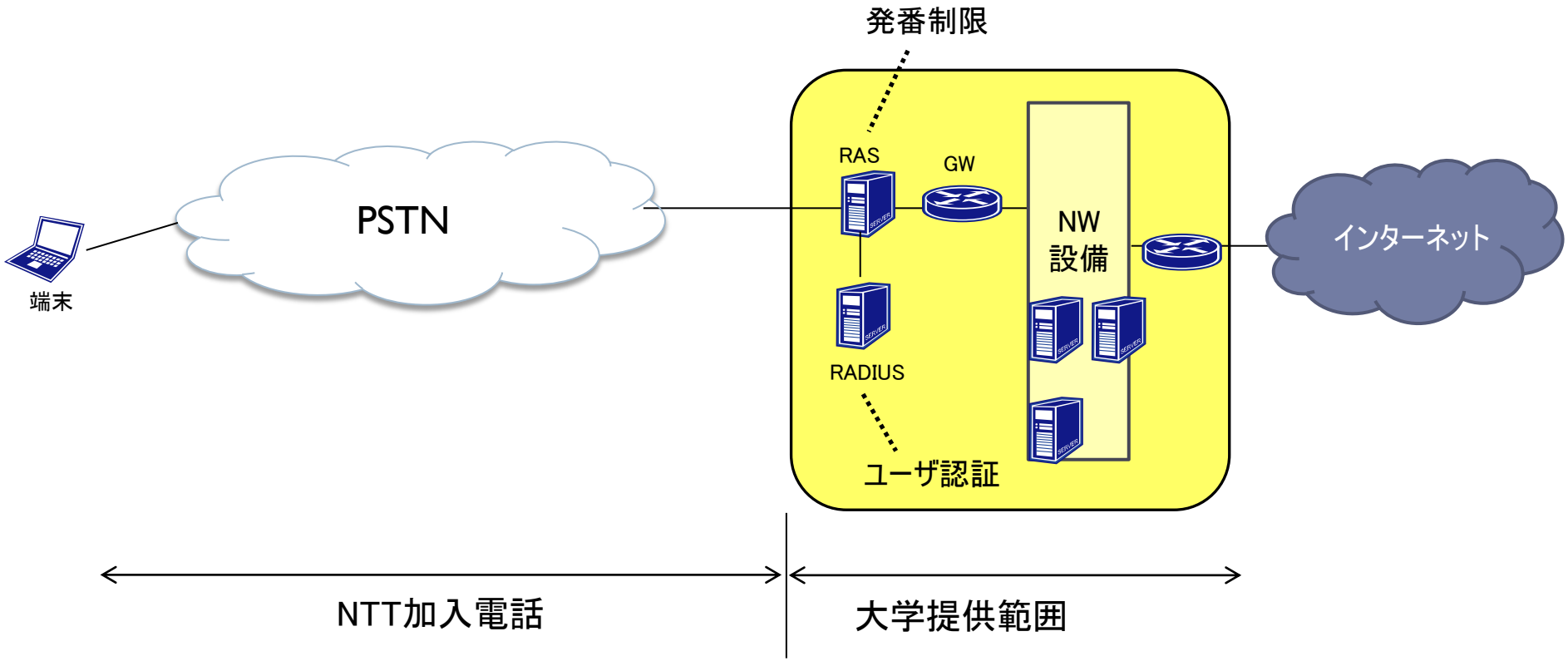
ネットワーク構成（SINETモデル）



疑問

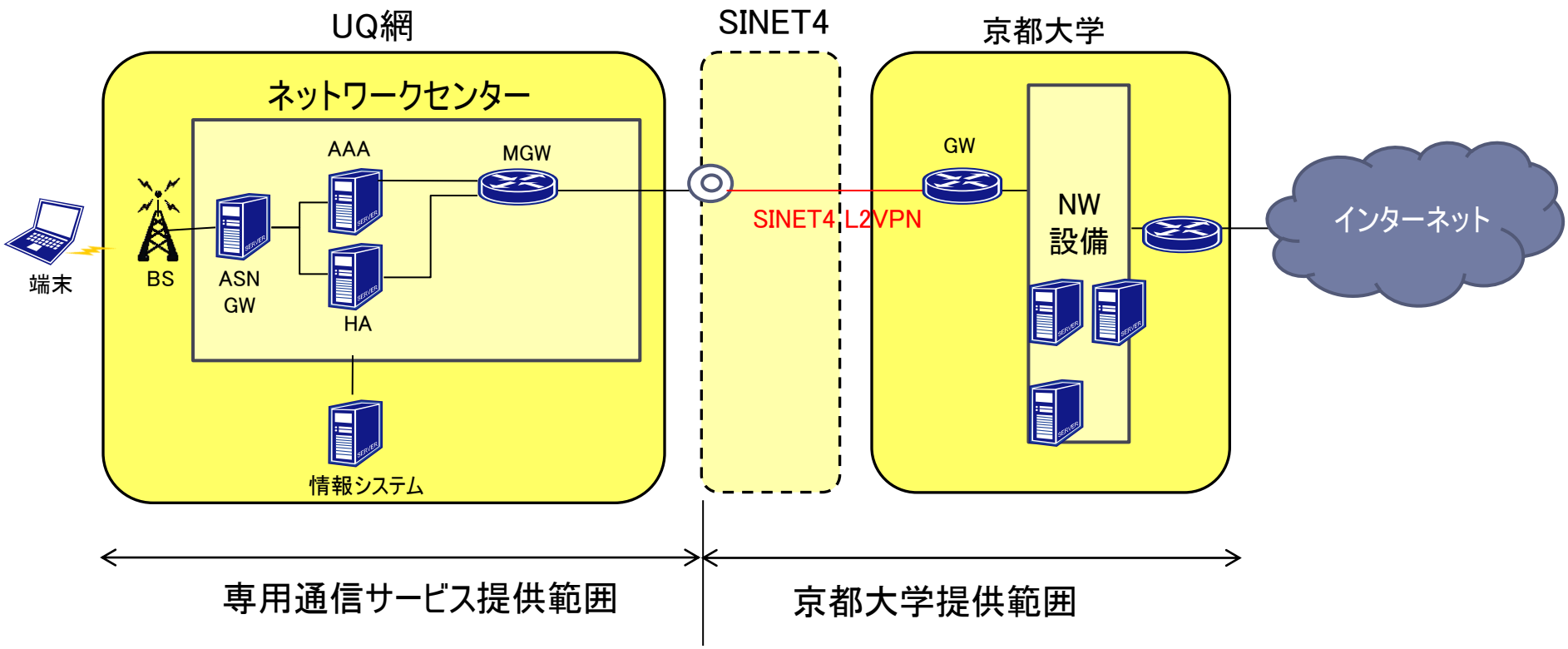
- 大学とUQC社と利用者（個人）との間でどういう契約をすればいいのか？
  - そもそもこのサービスはどう位置づけられるのか？
    - 国立大学がこんなことしていいのか？？
      - 電気通信事業法上の整理は？
        - …

（参考事例）
ダイヤルアップリモートアクセス



・公衆網に接続された組織が自らRASとRADIUSを構築
・アクセス権に基づき認証情報を登録し、利用の都度認証を行うことで組織の構成員へリモートアクセスを提供

SINETモデルWiMAXサービス



- キャリアが専ら特定の接続点に対する通信を提供する閉域サービスである
- 法人向けリモートアクセスサービスでも認証をキャリア設備で行う例はある。但しアクセス回線も同一法人が契約し、構成員へ一体的に提供するため、キャリア自身による識別・承認は発生しない
- 本モデルはUQC社が直接エンドユーザのアクセス権を識別・承認のうえ契約受付し、接続点に対する通信サービスを提供する。その識別と承認に係る業務と責任については規定が必要

京都
大学

イントラネット接続サービスに関する契約書

・UQ～京大間の接続条件
・当該接続を用いた専用通信サービスを申込者に提供するにあたり、
以下の条件を遵守する。
具体的な内容
(a) UQは指定された手段(Shibbolleth)により京都大学へアクセス権の有効性照会を行い、有効であることが応答された場合に限りその申込を承諾すること
(b) 契約後も登録された情報(EPTID)を基に、UQは定期的に京都大学へ有効性照会を行い、失効が確認された場合はその当月末をもって専用通信サービスの提供を終了すること
(c) 京都大学の要請によりePTIDで指定された専用通信サービスの停止を行うこと
・両者間の守秘義務規定

UQ

専用通信サービス契約（附合契約）

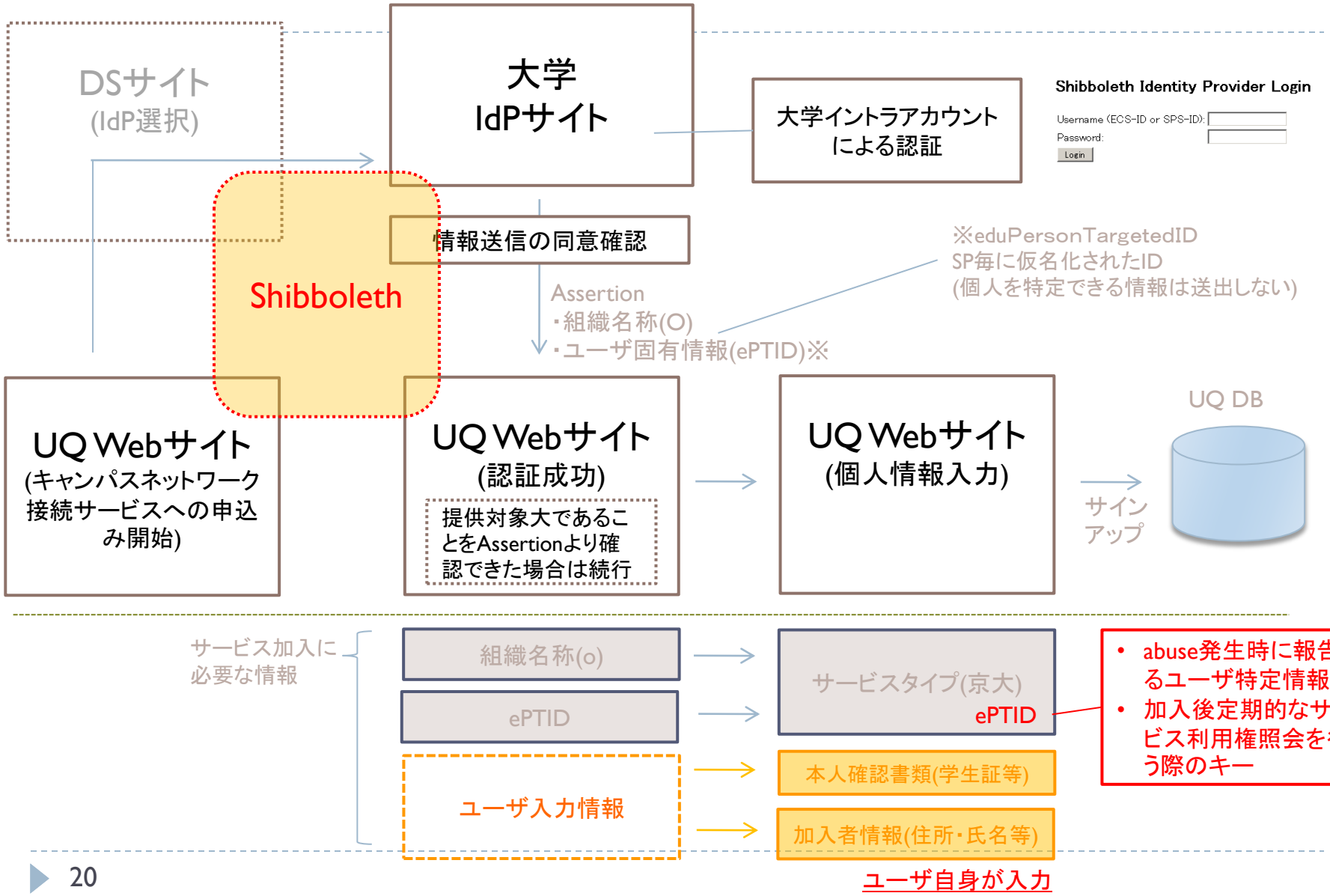
・専用通信サービス提供条件の規定
- 端末から京都大学との接続点までの通信を提供すること
- 加入条件として有効なアクセス権を保有していること
- 加入後にアクセス権が失効が確認された場合は次月より通常の料金種別に変更されること
- 京都大学から要請があった場合に、アクセスログの調査を行い、その結果を回答する場合があること

エンド
ユーザ

契約時の利用資格（実在性・本人性）の確認

- 大学構成員であることをどのように確認するか？
  - メールの到達性を使う?
    - xxx@yyy.kyoto-u.ac.jp の任意のメールアドレス？
    - 全学メール xxx@kyoto-u.ac.jp ？
  - 学内認証基盤にradiusやLDAPで接続する？
    - 学外のシステムを、本学が委託する業務以外の目的で、学内認証基盤に接続してよいのか？？
- こういうときこそ学認を使いましょう！
  - 大学からは組織名称(O)と仮名化されたユーザ固有情報(eduPersonTargetedID; ePTID)のみを送出
  - UQC側は電気通信事業者として契約時に独自に住所、氏名を確認
  - 定期的な在籍確認およびインシデント発生時はePTIDでやりとりする。

加入者オンライン認証の流れ




お申し込み（機種・プラン選択） | UQ WiMAX - ワイヤレスブロードバンドで高速モバイルインターネット - Mozilla Firefox
ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)
uqwimax.jp https://jvr.uqwimax.jp/univ/AgreementAction
kuins
お申し込み（機種・プラン選択） | UQ WiMAX - ワイヤレスブロードバンドで高速モバイルインターネット - Mozilla Firefox
ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)
uqwimax.jp https://jvr.uqwimax.jp/univ/AgreementAction
kuins
お申し込み（機種・プラン選択） | UQ...
3 料金プランの選択
料金プランを1つ選択してください。
KUINS Flat
年間パスポート
月額 3,200円
詳細
4 オプションサービスの選択
UQ Wi-Fi
月額利用料 無料
詳細

インシデント対応手順

1. グローバルIPアドレスをキーにして通報（外部からの場合）
2. ログから対応するプライベートIPアドレスを検索
3. プライベートIPアドレスと時刻をUQC社に通知→
4. UQC社から対応するePTIDの連絡
5. ePTIDから対応する構成員を特定
6. 構成員の所属部局長を通じて調査協力依頼→

まとめ

- UQC社と提携し、WiMAX網に接続された端末が直接学内LANに収容されるサービスを開始
  - VPN接続が不要となり、スマートホン端末での利便性が向上
- 中継線にSINET4　L2VPNサービスとクラウド型接続、認証連携に学認を活用
  - 大学とUQC社の契約関係、個人情報のやり取りなどセキュリティポリシー上の事項を整理
  - SINET4接続機関かつ学認参加機関なら同じモデルでのサービスインが容易

参考文献

- UQコミュニケーションズ（株）：UQコミュニケーションズ 京都大学のキャンパスネットワークへ接続可能なモバイルWiMAXサービスを提供－京都大学の学生・教職員様へ2012年4月1日より提供開始－（ニュースリリース），2012年1月．
  - http://www.uqwimax.jp/annai/news_release/201201303.html
- 堀田功：WiMAXでどこでも学内LANに接続、追加コストをほとんどかけず構築，日経コミュニケーション 2012年5月号 pp.41-44 , 2012年5月．
  - http://itpro.nikkeibp.co.jp/article/JIREI/20120528/399222/
- 蚊野 浩，前川 覚，中村 陽一：高速無線通信を用いた京大・東大対校ボート競漕大会の手作り実況中継放送，KUINSニュース, No.70, 2010年8月．
  - http://www.kuins.kyoto-u.ac.jp/news/70/#boat