京都大学の無線ネットワーク環境とVPNの概要

古村　隆明*
京都大学情報環境機構IT企画室

Ⅰ．はじめに

スマートフォンやタブレットの普及により，無線LANの重要性が高まっている。

京都大学では学内の有線ネットワークおよび無線ネットワーク環境の管理・運用をKUINS（Kyoto University Integrated Information Network System）が行なっている。KUINSは学内の無線ネットワーク環境の実験的な提供を2002年から開始した。現在，KUINSが学内に設置している無線基地局は約1,000局を数え，全ての無線基地局で「MIAKOネット」と「eduroam」と呼ぶ二つの利用方式を提供している。いずれの利用方法でも利用者は認証したうえで無線LANからインターネットへ通信を行なうことになるが，二方式で認証の方法は大きく異なる。それぞれの方式についてⅡ章で概要を説明する。京都大学では，eduroamを「仮名アカウント」で利用する方法を推奨している。その理由と仮名アカウント発行の仕組みをⅢ章で述べる。VPN（Virtual Private Network）はMIAKOネット方式を利用するために必要不可欠なサービスであるだけでなく，学外や無線ネットワークから学内限定コンテンツへアクセスするためにも必要となる重要なネットワークサービスである。Ⅳ章でKUINSが提供しているVPNについて説明を行なう。

Ⅱ．京都大学の無線LAN環境

京都大学ではKUINSが全学的な有線ネットワークと無線ネットワークの環境整備・管理・運用を行なっている。有線ネットワークは，グローバルアドレスはIPアドレスごとに，プライベートアドレスはサブネットごとに管理者を置き学内で課金を行なうなど特徴的な管理を実施しているが本稿では詳細は省略し，無線ネットワークについて説明を行なう。

セキュリティの観点からKUINSで提供する無線ネットワークは以下の2つの要件を満たす必要がある。

－無線区間の通信が利用者ごとに個別に暗号化され，利用者が安全に通信を行えること
－不正アクセス発生時には利用者を特定できること

KUINSが設置している無線基地局は約1,000局に達している。利用している無線基地局は，複数のSSID（Service Set Identifier；無線LANにおける基地局の識別子）に対応し，それぞれのSSIDで異なる認証方式を利用できる。また，SSIDごとに有線LANの異なるVLANに繋ぎ込むことができる。この機能を利用して，上記の二つの要件を満たす「MIAKOネット」と「eduroam」と呼ぶ二つの通信方式を同時に提供している。

いずれの方式も，学内の構成員だけでなく，学会や打合せなどで本学を訪れる学外からの訪問者らの利用も想定している。訪問者が学内ネットワークを利用するのは好ましくないため，**図1**のように両方式とも無線接続時に端末に割り当てるIPアドレスは，学内の有線ネットワークで利用しているのとは異なるアドレス空間から払い出す設計とした。

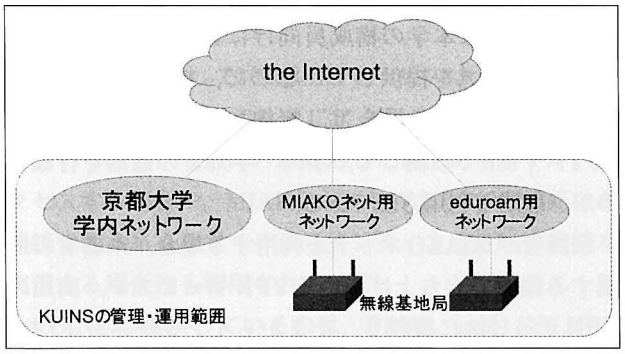

図1．KUINSの管理する学内ネットワークと無線ネットワーク

1．MIAKOネット

MIAKOネットは，2002年から京都大学，特定非営利活動法人日本サスティナブル・コミュニティ・センター，財団法人京都高度技術研究所などが共同で開発した方式

*Takaaki KOMURA：〒606-8501 京都府京都市左京区吉田本町.
komura@media.kyoto-u.ac.jp
（2012年8月21日　受理）

である[1]。MIAKOネット方式では，無線LANへの接続時には認証を行なわないが，インターネットとの通信はパケットフィルタによりVPNしか通さないという制限を設けた通信方式である。ここで我々が想定しているVPNとは，ユーザ認証を行なったうえで，通信を暗号化する機能を有する通信方式のことであり，通信相手のVPNサーバはインターネット上のどこに存在しても構わない。

VPNを利用することで，端末からVPNサーバまでの通信区間が暗号化されるため，無線区間も暗号化される。また，不正アクセス発生時にはVPNサーバでの認証ログから利用者を特定することもできる。よって，2章で挙げた二つの要件を満たすことができる。利用者は，**図2**のようにVPNが接続できればMIAKOネットによる通信制限からは開放され，VPNサーバ側が許す通信を行なうことができる。

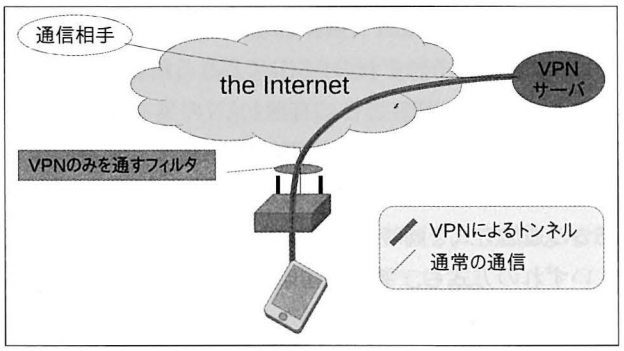

図2．MIAKOネットでVPNを利用した通信

本学のMIAKOネット環境から通信を許可しているのは，PPTP（Point-to-Point Tunneling Protocol），IPsec，ssh，OpenVPN，imap4／ssl，pop3／ssl，smtp／sslなどの通信方式である。

KUINSでは本学の構成員向けにPPTPやsshによるVPNサービスを提供しているので，構成員がMIAKOネットを利用する場合は，無線LANに接続したあとPPTPやsshで接続して，学内・学外との通信を行なうのが一般的な利用方法である。

来訪者がMIAKOネットを利用する場合，来訪者の所属する機関で立ち上げているVPNサービスや，商用のVPNサービスに接続し，そこからインターネットへの通信を行なう。

接続できるVPNサーバを持たない利用者用に，KUINSではビジター用PPTPサーバも準備している。このビジター用PPTPサーバは，本学の構成員の操作でビジター用アカウントを即座に発行できる。発行したIDとパスワードを来訪者等に渡す際には，来訪者の氏名や連絡先を記録するよう利用規約で定めている。

なお，一般的なVPNの定義からは外れるが，ユーザ認証と通信の暗号化を行なうという点で要件を満たしているimap4／ssl，pop3／ssl，smtp／sslもMIAKOネットからの通信を許可しており，一般的なVPN接続をすることなくメールの送受信は可能である。

2．eduroam

eduroam[2]はTERENA（欧州研究教育ネットワーク協会）で開発された無線LANローミング基盤で，50カ国以上の大学等教育研究機関の間で無線LANの相互利用を実現している。日本では国立情報学研究所（NII）と東北大学が中心となり導入が進められており，35以上の機関が参加している。

eduroamでは無線LAN接続時に802.1xに基き，IDとパスワードの組や電子証明書で認証を行なう。利用者は一度eduroam用のアカウントを取得しておけば，世界中のeduroam対応基地局を利用できる。多くのPCやスマートフォンなどで，無線LAN接続用のアカウントを登録しておけば，同じ条件で接続できる電波を見付けると自動的に再接続する機能がある。eduroamではこの機能により，自組織のeduroam基地局に接続する場合だけでなく，出張先などでもeduroam対応基地局があれば，国内・国外を問わずに自動的に無線LANに接続されることが多く，利便性が高い。

eduroamでは，各参加機関に設置されているRADIUSと呼ばれる認証サービスが，RADIUSプロキシを利用して機関や国を越えて連携することでローミングを実現している。利用者自身が所属する機関でeduroamを利用するときは**図3**のように無線基地局からRADIUSサーバに認証要求が送信され認証処理が進む。

eduroam参加機関のRADIUSサーバは，**図4**のようにトップレベルRADIUSプロキシ，国内RADIUSプロキシ，機関RADIUSサーバの三階層で相互に認証連携できるよ

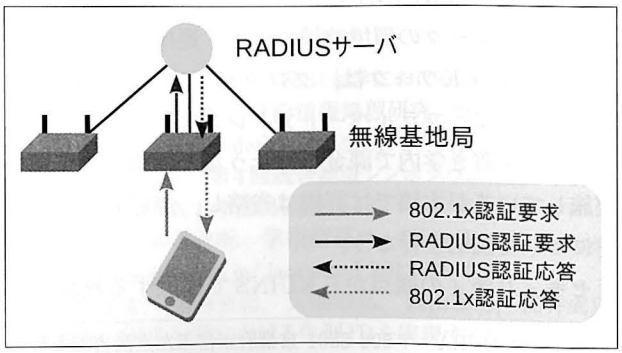

図3．自機関でeduroamを利用する際の認証

うに接続されている。eduroam接続用のアカウントには，本学が発行するIDであれば“@kyoto-u.ac.jp”のような発行機関を示すレルムと呼ばれる文字列を付加する規則になっている。他機関を訪問してeduroamを利用する際は，**図4**中の矢印のように，レルム情報を利用して訪問先機関のRADIUSサーバからホーム機関のRADIUSサーバまでRADIUSプロキシが認証要求を中継する。認証応答は逆向きに中継され，認証成功の応答であれば訪問先機関が提供する無線ネットワークに接続される。

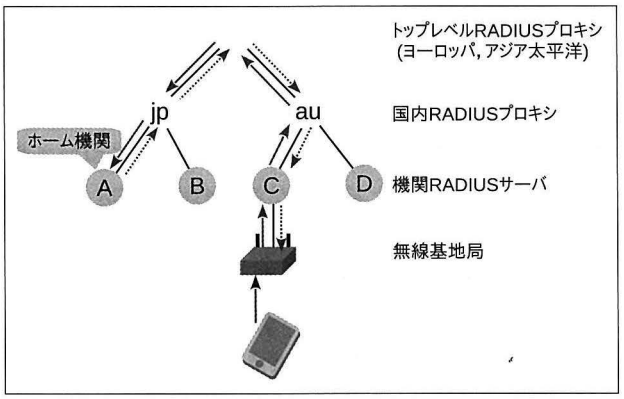

図4. 他機関でeduroamを利用する際の認証

Ⅲ. eduroam仮名アカウント

Ⅱ章2節での説明の通り，他機関でeduroamを利用する場合は，RADIUSプロキシで認証要求やその応答が中継される。このとき，RADIUSサーバやプロキシには利用者のIDがログとして記録されている。不正アクセスが発生したときに利用者を特定するためには，IDをログに記録しておく必要があるが，一方で，利用者に紐付くID情報があちこちのRADIUSサーバやRADIUSプロキシに記録される事は利用者のロケーションプライバシを侵害する問題となり得る。IDの文字列中に利用者の氏名などが含まれている場合は，問題は更に大きくなる。また，機関内で認証に利用しているIDのセキュリティレベルと，eduroamのセキュリティレベルが必ずしも一致しているとは限らないため，機関内のIDをそのままeduroam認証に利用するのは問題となる場合もある。

こうした問題を解決するため，NIIと京都大学が共同で**図5**のような学認フェデレーション参加機関向けにeduroam接続用の「仮名アカウント発行システム[3]」を提供している。仮名アカウント発行システムは，学認[4),5)]のShibboleth連携により，IdP（Identity Provider）での認証を経て，ユーザ名は利用者と直接紐付かない文字列で，レルムは“@upki.eduroam.jp”となる仮名アカウントを発行するSP（Service Provider）として動作する。

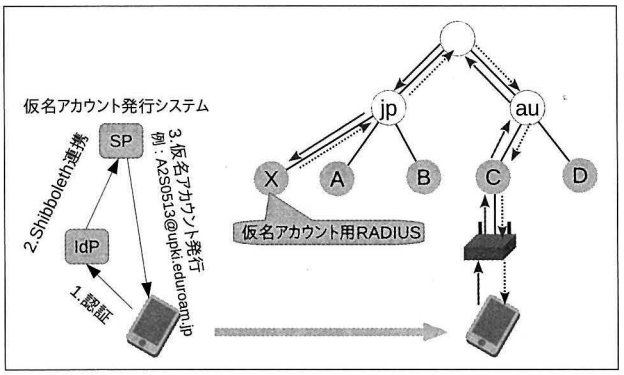

図5. 仮名アカウント発行システムとその利用

アカウントの仮名性により，各機関のRADIUSにIDが記録されたり，通信経路上でIDを盗み見られることがあっても，個人を特定することはできない。また，複数の仮名アカウントを短期間で使い捨てて利用することで，複数のRADIUSサーバのログを長期間寄せ集めることで個人を特定しようとする攻撃に対する耐性を持たせることもできる。そして，機関内での認証に利用するIDとは全く異なる体系のアカウントを利用することで，機関内のIDを不要な危険にさらす必要がなくなる。Ⅳ章でも述べるように，eduroamの認証プロトコルとして利用しているMS-CHAPv2の欠陥[6)]が指摘されたが，仮名アカウントを利用することでこの問題の影響を最小限にとどめることができる。

仮名アカウントの利用中に不正アクセスが発生してしまった場合は，仮名アカウント発行システムのSPとIdPのログを照合することで，仮名アカウントを取得した利用者を特定することができる。

Ⅳ. VPN接続

KUINSで提供しているVPNサービスは，自宅や出張先から学内限定コンテンツにアクセスする場合の他に，学内からのアクセスにのみ対応した電子ジャーナルへアクセスする場合や，MIAKOネットのようにVPNだけが接続できるネットワークからインターネットへの接続を実現する場合にも利用されている。

KUINSで提供しているのは，PPTP，ssh，SSLVPNの三種類のVPN接続サービスだが，安全性向上や利便性向上の目的で，新たにSSTP（Secure Socket Tunneling Protocol）とOpenVPNの二種類のVPNサービスを提供する準備を行なっている。VPNの種類によって，利用できるOSの種類，設定の容易さ，利用できるネットワーク環境の制限，安全性の違いなど，一長一短がある。

1．KUINSが提供しているVPN

PPTPはWindows，MacOS X，Linux，iOS，Androidなどの幅広いOSから利用できるVPNであり，KUINSの提供するVPNサービスの中でも利用頻度が最も高い。しかしPPTPには，NAT（Network Address Translation；ネットワークアドレス変換）を介したネットワークから接続できない場合がある事や，認証プロトコルとして利用されているMS-CHAPv2の欠陥[6]が指摘されている。MS-CHAPv2問題は重大であり，PPTPでより安全な認証方式への移行や，NAT越えの問題も解決できてより安全な別のVPN方式の導入を進めてゆく必要があると認識している。

sshは一般的には安全にリモートコンピュータにログインしてコマンドライン等で操作を行なうために利用されるが，KUINSではsshのポートフォワード機能に着目してVPN的な利用方法を提供している。ポートフォワード機能とは，接続元ホストのTCPの特定のポート番号宛ての通信を，ssh接続先ホストから任意のホストの任意のポート番号に向けて中継する機能である。設定にはネットワークに関する知識が必要とされるが，PPTPが利用できない環境からでも利用できる場合も多く，PPTPが接続できない環境からどうしても学内限定コンテンツにアクセスしたい利用者などから一定数の利用が有る。

SSLVPNは，SSLを用いたVPNに対する総称で様々な実装が存在するが，本学では，端末側に専用のクライアントソフトをインストールして，HTTPSを用いてVPNを張る方式のものを導入した。KUINSで導入した三つのVPNサービスの中で，導入が一番最後であったこととWindows専用のクライアントソフトをインストールする必要があることなどから利用者数は少ないが，KUINSが提供している三つのVPNの中では，最も利用者側のネットワーク環境の制限を受けにくく，様々な環境から接続できる可能性の高いVPNである。

2．導入を検討中のVPN

KUINSで新たに対応を検討しているVPNはSSTPとOpenVPN[7]である。

SSTPはMicrosoftが開発した方式で，Windows Vista SP1以降には標準で組込まれており利用が容易な点と，通信方式としてhttpsを利用しているため多くのネットワーク環境から接続できる可能性が高いことが利点となる。

OpenVPNはオープンソースとして公開されており，各自インストールが必要にはなるもののWindows，MacOS X，Linux，Androidなどの複数の環境から接続できることが利点となる。

両VPNとも，IDとパスワードでのユーザ認証に代わり，より安全性の高い電子証明書（クライアント証明書）を利用してユーザ認証を行なう。VPN用の電子証明書は，ICカードに格納して教職員に配布済みのクライアント証明書を利用するか，Shibboleth認証連携に対応した学内限定サービスとしてVPN接続専用のクライアント証明書発行システムを立ち上げて配布する予定である。なお，SSTPとOpenVPNとは，共通のクライアント証明書で接続できるように設計を行なっている。

V．おわりに

京都大学で提供している二種類の無線ネットワーク接続方式の「MIAKOネット」と「eduroam」について紹介した。認証の手順などは異なるものの，二方式とも，無線区間を暗号化して安全に通信を行なえる事と，不正アクセス発生時などに利用者を特定できる方式となっている。本学では，eduroamはロケーションプライバシの保護とIDを必要以上に危険にさらす事が無いよう，「仮名アカウント」での利用を推奨しており，仮名アカウントの仕組みについて紹介した。VPN接続サービスはMIAKOネットと密接に関わりがあり，また，eduroam等からも学内へのアクセスに必要になる。現在対応しているVPNと今後対応予定のVPNサービスを紹介した。

参考文献

1）大平健司，隅岡敦史，北岡有喜，古村隆明，藤川賢治，岡部寿男．公衆無線インターネット接続サービス「みあこネット」の設計と運用．電子情報通信学会論文誌．2010;J93-B(5):759-68.

2）L. Florio, K. Wierenga. Eduroam, Providing Mobility for Roaming Users. Proceedings of 11th International Conference EUNIS2005: 21st-24th June 2005; Manchester UK, 2005.

3）古村隆明，岡部寿男，中村素典．SAML連携を用いてロケーションプライバシを守るeduroamアカウント利用方式．電子情報通信学会技術研究報告．IA，インターネットアーキテクチャ．2010;109(438):153-8.

4）阿蘇品治夫．学認-gakunin（学術認証フェデレーション）の概要（第12回図書館総合展）．薬学図書館．2011;56(2):166-74.

5）阿蘇品治夫．シボレス認証で広がる便利な世界：学認（gakunin：学術認証フェデレーション）（特集情報環境の新しい流れ）．ほすぴたるらいぶらりあん．2011;36(4):189-93.

6）Divide and conquer: Cracking MS-CHAPv2 with a 100% Success Rate[internet]. https://www.cloudcracker.com/blog/2012/07/29/cracking-ms-chap-v2/ [accessed 2012-09-01]

7）Open Source VPN[internet]. http://openvpn.net [accessed 2012-09-01]