Vol.2011-IOT-15 No.2
2011/10/7

組織連携による整備環境非依存のキャンパス無線LANサービスの構築

藤枝俊輔[†1]　小川剛史[†2]　石原知洋[†3]
下見淳一郎[†4]　中村誠[†5]

キャンパスネットワークを学内の部局が分割運用している場合，キャンパスのあらゆる場所で利用可能な無線 LAN サービスを提供するには，部局ネットワークの連携が必要である．しかし，部局が整備している無線 LAN 環境が大きく異なる，学内者の情報が複数のデータベースに分散している，といった事情が実際の連携を妨げている．そうした環境に適合し，部局連携による全学無線 LAN サービスを実現する効率的な運用方式を考案し，本学において実験サービスを行った．

Wireless LAN service on campus by cooperation in divisions over multiple network environment

Shunsuke Fujieda,[†1] Takefumi Ogawa,[†2]
Tomohiro Ishihara,[†3] Junichiro Shitami[†4]
and Makoto Nakamura[†5]

In cases that the operation of a campus network is devided to some devisions of the university, a cooperation between sub network systems is necessary for providing campus-wide wireless network service. But in fact, differences of network environments, and decentralizations of user database make it hard. We considerd an efficient operation scheme that adapts to such environments and realize a campus-wide wireless network service in cooperation with many divisions over varied network systems.

1. はじめに

大学のキャンパスにおいて，無線 LAN はあらゆる教育・研究の基盤として必須のサービスとなっている．情報通信は多くの教職員・学生があらゆる場所で恒常的に必要としており，キャンパス全体に大規模な無線 LAN サービスが提供されている場合も多い．大規模な無線 LAN システムを効率的に管理する製品も数多く提供されている．

一方，キャンパスネットワークは複数の部門が分割運用している場合がある．東京大学のキャンパスは，学部，大学院，研究センター，本部事務といった組織（以下，部局と呼ぶ）と，様々な学術分野が集合している．部局毎に情報通信への要求が異なるため，本学ではキャンパスネットワーク (以下 UTnet) を部局毎に分割運用している．このように運用が細分化されているため，キャンパス全体を対象とした無線 LAN サービスを提供できていない．

本学では，キャンパスネットワークを特定の部門が集中管理する体制に移行することは，大幅なシステム変更と組織変更が必要であり，早期の実現は困難である．また，部局内の無線 LAN は 802.1X のダイナミック VLAN[1)] などにより部局の有線 VLAN と結合している場合もあるため，無線 LAN だけを切り離して全学的に集中管理することもできない．そうした状況で，無線 LAN の整備環境が異なる複数の部局が連携し，全学共通の無線 LAN サービスを提供する仕組みを検討した．

2. 対象とするネットワーク

2.1 UTnet

東京大学には学部 10，大学院 15，研究所・センター 32，病院 2 の部局が存在し，学部生約 14,000 人，大学院生約 14,000 人，教職員約 9,700 人が所属する．キャンパスは本郷、駒場、柏を軸に，それ以外にも多くの遠隔キャンパス・遠隔施設が存在する．本学では，情

†1 東京大学新領域創成科学研究科
Graduate School of Frontier Sciences, The University of Tokyo
†2 東京大学情報基盤センター
Information Technology Center, The University of Tokyo
†3 東京大学総合文化研究科
Graduate School of Arts and Sciences, The University of Tokyo
†4 東京大学理学系研究科
School of Science, The University of Tokyo
†5 東京大学情報システム本部
Division for Information and Communication Systems, The University of Tokyo

報基盤センターが部局間および学外インターネットをつなぐ基幹ネットワークを，各部局が自部局内の研究室や各施設を繋ぐ支線ネットワークを運用管理している．部局の規模，情報システムに対する要望，運用ポリシ，管理体制には大きな差があり、そのためネットワークの整備状況は非常に多様である．ファイヤウォール，無線 LAN，認証システム，各種サーバ等，多くのネットワークコンポーネントは部局が独自に導入している．

2.2 無線 LAN 環境

キャンパスに設置されている無線 LAN 基地局には，以下の種類がある．

(1) 講義室など主要なエリアに部局が設置したもの
(2) 大講堂や端末室などに情報基盤センターが特定用途向けに設置したもの
(3) 研究室など末端利用者が設置したもの
(4) 公衆無線 LAN 事業者が設置したもの

(1) は，少数の家庭用基地局を設置している部局から，多数の基地局によって建物全館をカバーする無線 LAN システムを構築している部局まで様々である．基地局の機種も多様であり，基地局が独立して動作する FAT 型基地局と，コントローラによる集中制御を受ける Thin 型基地局の両方が利用されている．(2) は，本学の教育用計算機システム (Educational Campuswide Computing System, 以下 ECCS) の利用者を対象とした演習・自習用の無線サービスと，大講堂のシンポジウム等に利用するゲスト用無線サービスである．大学院の多くの研究室が (3) を利用し，少数ではあるが (4) も存在する．

現在，本学は無線 LAN 環境に関して下記の問題を抱えている．

(1) 利用者が特定のエリアでしか無線 LAN を利用できない．特に他部局が管理する建物における活動が不便である．
(2) 部局が自部局の所属者以外に無線 LAN を提供する場合に労力がかかる．
(3) 一部のエリアでは，部局や用途毎に基地局が設置されており無駄である．
(4) 一部のエリアでは，基地局数が多すぎることや周波数割り当ての調整不足ため電波干渉が生じている．

2.3 認証環境

本学では，全構成員が登録された共通認証システムが存在しない．現時点で利用できるのは，サービス単位または部局単位で構築された認証システムだけである．部局では，他機関に所属する人物が学内者と同様に活動している場合もあり，部局の事情を含んだ最終的な人員情報は部局にのみ存在する．

3. 検討項目

3.1 システム要件

本研究では，2.2 で示した基地局のうち管理元が明確な (1)，(2) の連携による全学共通無線 LAN サービスを検討する．そのシステム要件を表 1 に示す．サービスを広範囲に展開するには，専門的な管理者が存在しない部局も参加でき，参加した部局に負担が発生せず，可能な限り既設機器を流用できることが望ましい．また，全学内者からの問い合わせを受ける窓口は設置できないため，ユーザサポートを極力行わずに運用できる必要がある．一方，多様な機能を持つ基地局を利用する以上，サービス品質の確保は困難であり除外した．

表 1 システム要求
Table 1 System requirement

利用の容易性	利用者が簡単に設定できること 可能な限り多くの学内者が利用できること 利用開始までのオーバヘッドが小さいこと
導入の容易性	幅広い種類の基地局に対応できること 既存のサービスと衝突しないこと 専門的な管理者が存在しない部局でも導入できること
管理の容易性	トラブル時に問題切り分けを簡単に進められること 基地局をこれまで通り部局が分散管理できること
認証セキュリティ	接続できる者を学内者に限定すること 利用者の認証情報が漏洩しないこと
LAN セキュリティ	無線の盗聴に対応できること 無線内部からの攻撃に対応できること 不適切な利用を制限したり事後調査できること

3.2 認証方式

キャンパス無線 LAN の運用において主流である WEB 認証，802.1X，VPN の 3 方式を，3.1 の要件から比較した．これを表 2 に示す．

WEB 認証は，利用者とサービス提供者の双方に導入が容易な方式である．しかし，認証情報を毎回入力する点は煩雑であり，スマートフォンなどの小型デバイスではストレスがある．また，スマートフォンは，データオフロードのため携帯電話回線より無線 LAN を優先する．このため，無線 LAN の上流で通信がフィルタされていると電話以外のアプリケーションが動作しなくなる問題もある．また，WEB 認証の大きな課題はセキュリティの確保である．悪意を持った人間が，偽の基地局と偽の認証画面を学内に設置することが可能で

表 2 認証方式の比較
Table 2 Comparison of authentication methods

	WEB 認証	802.1X	VPN の併用
利用の容易性	○直観的 ×毎回の認証が面倒	×端末の設定がやや複雑 △一部の端末が未対応	×無線と VPN 両方の設定が必要 ×無線接続後に VPN 接続するのは煩雑
導入の容易性	○認証ゲートウェイを上流に設置すれば部局の対応は不要	×全基地局が認証サーバと通信する必要がある	× VPN システムが必要
管理の容易性	○認証画面が閲覧できるか否かにより問題の切り分けが可能	×問題の切り分けに基地局や認証サーバの情報が必要 ○情報が揃えばおよその問題解決が可能	× VPN の障害もトラブルの可能性になる
認証セキュリティ	×攻撃者による偽の認証画面への誘導が簡単	○安全な方式が存在	○安全な方式が存在
LAN セキュリティ	×未認証の端末からオンリンクの攻撃が可能	○無線への接続前に攻撃者をブロック可能	×未認証の端末からオンリンクへの攻撃が可能

あり，利用者の認証情報が盗まれる危険がある (ただし，地理的に学内から攻撃することは攻撃者側のリスクも高いと思われる)．LAN セキュリティにおいては，未認証の端末によるウィルス活動，スキャン，不正な DHCP サーバの設置による間違った IP アドレスの配布などが懸念される．

802.1X は，認証が完了した後に端末が無線に接続する．利用者と認証サーバが相互に認証する方式[2)3)4)] を利用すれば，安全な認証が可能である．接続した全ての端末は認証済であるため，仮に LAN セキュリティの問題が発生しても，問題のある端末の接続者を特定できる．一方，802.1X の問題は利用・導入・管理の労力である．802.1X は RADIUS 認証を前提としており，基地局は NAS(Network Access Server) として RADIUS サーバと通信する[1)]．NAS と RADIUS サーバ間の接続は双方の機器に個別に登録が必要であるため，基地局数が増えると設定維持する接続数も増大する．基地局を集中管理する無線 LAN システムでは，その労力を大幅に削減できるが，本サービスが利用するのは部局が個別に導入した基地局であり，そうした効率化は困難である．また，802.1X 環境では，接続問題が生じた場合，端末と基地局間の問題か，基地局と Radius サーバ間の問題か，Radius サーバ上の問題かなど，問題の切り分けに NAS である基地局や RADIUS サーバのログデータを照合する必要がある．機器のログデータは部局が個別に蓄積しており，トラブル解決時にそれらを照会するのは部局の負担が大きい．ログデータを一か所に収集する仕組みを構築したとしても，大量のログデータの管理や，出力される情報の違いを運用者が吸収するのは労力が高い．

VPN は，セキュリティが確保されない無線 LAN において，VPN 機能によって学内者を認証するためや[5)]，通信の暗号化を行うためや[5)]，利用者の通信トラフィックを所属組織にトンネルするために利用されている[6)]．これらの利点が存在する一方，VPN を利用すること自体が利用者とサービス提供者の双方に負担となる．本学では VPN 設備を保持しない部局も多いため，VPN の利用を前提としたサービス設計は適切ではない．また，WEB 認証の利用時と同様，VPN を利用する場合も，未認証の端末が無線 LAN に接続したうえで VPN サーバと通信する必要があるため，ウィルス活動，スキャン，不正な DHCP サーバ等の LAN セキュリティの問題が発生し得る．

3.3 サブネット構成

無線 LAN に接続した端末を，どのような IP サブネットに収容するか検討が必要である．ネットワークの管理責任は各部局にあるため，802.1X のダイナミック VLAN などによって，利用者を所属部局のサブネットに収容する方式が理想的だが，本学では部局同士の VLAN 番号が競合しているため，全学規模のダイナミック VLAN は利用できない．そのため，無線端末を収容する特定の部局に所属しないサブネットが別途必要である．このサブネットは，SSID との対応，オンリンク通信の規模性，基地局間ローミングへの影響を考慮して設計する必要がある．

表 3 に SSID と IP サブネットの関連付け方式を示す．方式 1 は，全ての基地局と端末を単一のサブネットに収容する．この方式はキャンパスに一つの共通 VLAN を作成すればよく，トポロジが単純であり基地局の追加が容易である．しかし，端末の数が増加するとブロードキャストドメインとしての規模性が障害になる．一方，現在の基地局は，無線の帯域を有効利用するため，代理 ARP や DHCP リレー等の機能によって，ブロードキャストパケットを無線へ中継しない機能が備わっている場合も多い．そのため，方式 1 の規模性は検証の余地がある．次に，方式 2 は規模性の問題を回避できるが，端末が接続先の基地局を変更した場合に IP アドレスの再取得が必要である．しかし，端末は同一 SSID が設定された基地局間を移動した場合，レイヤ 3 のハンドオーバが生じたことを検知する方法がない[7)]．このため，端末が移動先で正しく IP アドレスを再取得しない可能性がある．方式 3 は既に

述べたように本学のキャンパス環境の制約により 802.1X のダイナミック VLAN が利用できないため今回は利用できない，方式 4 は全学共通サービスの目的に合わない．

表 3 SSID と IP サブネットの関連付け方式
Table 3 Conbination patterns of IP subnet and SSID

方式	SSID	サブネット	規模性	可用性	実現例
1	単一	単一	△	○	キャンパス共通 VLAN
2	単一	複数	○	△	基地局を異なる VLAN に収容
3	単一	動的	○	○	802.1X ダイナミック VLAN
4	複数	複数	○	×	マルチ SSID+マルチ VLAN

4. utroam

4.1 設　　計

3 の検討をもとに，全学共通無線 LAN サービス”utroam”を設計した．認証方式には，利用・導入・管理の容易性を重視し，WEB 認証を採用した．サブネット構成は表 3 の方式 1(単一 SSID+単一サブネット) を採用した．端末が基地局間をシームレスに移動する可能性があるのは同一キャンパス内だけであるため，1 つのキャンパスに 1 つのサブネットを設置した．サブネットはキャンパス内の部局を横断する VLAN であり，utroam に参加する基地局を全て接続する．全基地局が同一の SSID”utroam”を広告し，同一の WPA2 共有鍵が設定されている．WPA2 は AES による暗号化のみを目的に利用し，実際の認証には WEB 認証を用いる．utroam の VLAN は基幹ネットワーク上で認証ゲートウェイに接続され，利用者が端末でブラウザを立ち上げると自動的に認証画面へリダイレクトされる．本システムの概要を図 1 に示す．

認証ゲートウェイは Radius ツリーに問い合わせを行う．2.3 で述べたように，本学には全構成員が登録された認証システムが存在しない．そこで，可能な限り多くの学内者にサービスを提供するため，新たに Radius ツリーを構築し，そこに登録された認証システムの何れかに許可を受けることを学内者の証明とした．本論文の執筆時点で，Radius ツリーにはテスト段階の事務用認証システム，ECCS 認証システム，3 つの部局認証システムが接続されている．これによって構成員の 8 割以上が利用可能である．

3.2 で述べたオンリンクの攻撃については，システム側では未対応である．端末の大半は個人 PC であるため，最低限のセキュリティ対策は個人が行うことを前提としている．

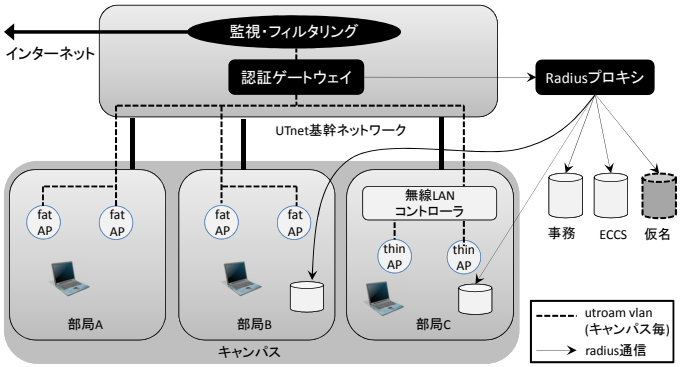

図 1 utroam のシステム構成
Fig. 1 System architecture of utroam

4.2 実　　装

図 1 のように，Thin 型基地局はコントローラを通じて utroam のキャンパス共通 VLAN に接続される．複数のキャンパスに基地局を持ち，それらを CAPWAP[8] 等により単一のコントローラに収容している部局は，基地局を各キャンパスに対応した VLAN に接続する必要がある．本学で使用されているコントローラでは，特定の SSID を広告する基地局を複数のグループに分け，異なる VLAN に接続する機能が利用可能であった．

認証ゲートウェイには Aruba 社の Aruba 3400 を用いた．本機は無線 LAN コントローラであるが，有線の認証ゲートウェイとして稼働させている．本機のカタログスペックは Gigabit Ethernet ポート 4 個，最大利用者数 4096，最大 MAC アドレス数 64000，ファイアウォールセッション数最大 128000，ファイアウォールスループット 4Gbps となっている．本機はレイヤ 2 で動作するため，トポロジを維持したまま増設することも可能である．

Radius ツリーの根となる Radius プロキシは，freeradius[9] にて構築した．LDAP 機能しか持たない認証サーバを Radius ツリーに接続する場合，freeradius の仮想サーバ機能を用いて，LDAP 認証サーバの Radius フロントエンドを Radius プロキシと同一サーバ上で提供した．Radius へのブルートフォースアタックを防止するため，認証ゲートウェイにおいて，一定回数連続して認証に失敗すると，その端末による WEB 認証を自動的に一定時間拒否する機能を利用した．認証情報の漏洩防止に関する，その他の検討は 5.1 で述べる．

認証ゲートウェイの上流では，utroam サブネット内の監視と通信フィルタを行っている．

本学では既に基幹ネットワーク上でトラフィックの監視を行い，当該 IP アドレスを利用している部局に不審な通信や P2P 型アプリケーションの活動をインシデントや参考情報として通知している．utroam では Radius の認証ログから利用者情報を抽出し，それを付与したうえで部局へ通知する．こうした監視と通知の労力を軽減するため，インシデントを減らす目的で，外部へ接続可能な TCP ポートを制限し，標準利用できるアプリケーションをウェブ，メール，SSH，FTP，VPN 等に限定している[*1]．繰り返し不正トラフィックが検知される端末は MAC アドレスのブラックリストにより全通信をフィルタする予定であるが，現在までその事例はない．

4.3 試験運用

2011 年 3 月 2 日より，utroam を試験サービスとして全学的に稼働させている．現在，utroam には情報基盤センター，新領域創成科学研究科，工学系研究科，理学系研究科，総合文化研究科，情報学環・学際情報学府，生産技術研究所，東京大学本部の 8 部局が参加している．基地局数は合計 854 台である．その内訳は本郷キャンパス 489 台，駒場キャンパス 261 台，柏キャンパス 83 台，遠隔地 21 台である．

2011 年 3 月 1 日から 2011 年 8 月 31 日までに利用された総アカウント数は約 2200 であった．接続した端末数は約 3700 であった．図 2 に，最大同時接続端末数の推移を示す．サービス開始から夏季休業直前まで，ほぼ単調に増加しており，部局外における無線 LAN 利用の需要が伺える結果となった．

図 3 は，利用者数が多かった 7 月期における外部から utroam への受信 (Inbound) と，外部への送信 (Outbound) のピークトラフィックである．データは 5 分毎に取得した．802.11n の普及により無線 LAN の通信速度は向上を続けており，本システムは全端末のトラフィックを認証ゲートウェイに集約しているため，サービスが拡大すると今後相応の通信量が予想される．ただし，サービス開始直後であるため，ベンチマーク等により故意に急激なトラフィックを発生させる利用者も散見された．

本サービスは，WEB サイトによる接続方法の告知以外はユーザサポートを行わずに運用している．要望と障害報告を受けとる電子メール窓口だけを設けている．現在まで，大きな障害は生じておらず，接続できないといった報告も僅かである．運用と利用の両面において，本方式の負荷は大変小さいと考えられる．

⋆1 利用できる VPN 方式は eduroam[10] 仕様を参考にした

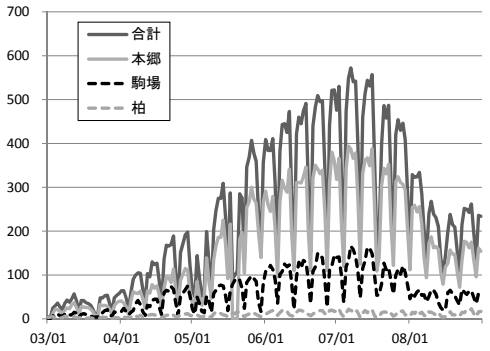

図 2 最大同時接続端末数
Fig. 2 Number of devices on peak time

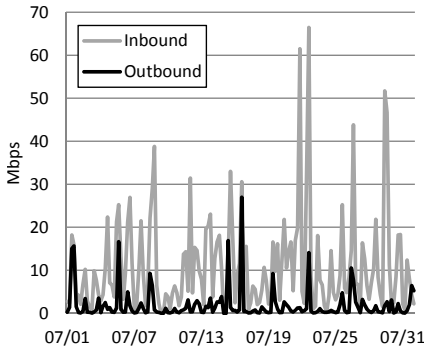

図 3 ピークトラフィック
Fig. 3 Peak traffic

5. 考　　察

5.1 認証情報の漏洩防止

無線 LAN で WEB 認証を用いた場合，偽基地局を設置することで，攻撃者が利用者を偽の認証ページに誘導する可能性がある．utroam では，認証ゲートウェイが表示する WEB 認証ページにおいて，NII より配布されてるサーバ証明書を提示し，利用者に認証ページの正当性を確認するように指示している．しかし，全ての利用者が注意深く認証ページを確認することは期待できない．最近のブラウザはサーバ証明書のチェックを厳しく行うものが多いが，攻撃者は http の認証ページを表示することも可能である．偽基地局による学内アカウントの盗難を防ぐため，近日中に仮名認証システムを導入する予定である．しかし，仮名アカウントが漏洩した場合も，その有効期間は攻撃者に不正なネットワーク接続を許すことになるため，仮名認証は完全な解決方法ではない．

パスワードを利用する認証方式のうち，802.1X の EAP-PEAP[7] や EAP-TTLS[3] のように，認証サーバをサーバ証明書によって端末が検証する方式では，偽の認証サーバによる認証情報の盗難を防止できる．ただし，端末が正しく設定されないと認証サーバの検証を行わない可能性があるため，安全性の確保には利用者の教育とサポートが必要と思われる．根本的には，攻撃者が介入する余地のある環境でパスワード認証を行う点に危険があり，固定のシステムパスワードを利用しない認証方式への移行が望ましい．本研究では，今後 802.1X の EAP-TLS[4] や，ワンタイムパスワードの利用を検討していく予定である．ク

ライアント証明書を利用した WEB 認証方式[11] も提案されている．

5.2 既存の連携手法との比較

組織連携によって互いに無線 LAN を提供しあう取り組みに，eduroam[10] がある．eduroam 参加組織の所属者は，他の参加組織を訪問した際，自分の所属組織が発行したアカウントを使って訪問先の eduroam 無線 LAN に接続できる．参加組織の間で認証連携を実現するため，世界規模の RADIUS ツリーが構築されている．eduroam 無線 LAN において許可されている通信は基地局の設置組織に依存し，一般的なインターネット接続が許可されている場合や，VPN だけが許可されている場合などがある．

一方，utroam は大学の部局という地理的に密な組織の連携を目的としている．利用者は，異なる組織間の基地局をシームレスに移動できる必要がある．また，どの基地局に接続しても同じようにアプリケーション利用できる必要がある．そのため，3.3 で検討したように，論理的に近い環境を提供するシステム構成が必要であった．

5.3 今後の課題

実験サービスの開始以降，utroam の利用者は増加を続けている．同時接続端末数の増加に対して，無線基地局を収容したブロードキャストドメインの規模性を継続的に検討していく必要がある．無線へのフィルタリング機能を持たない基地局や，無線帯域が混雑している基地局では，そうでない基地局よりも早く限界が訪れる可能性が高い．また，ウィルス活動など LAN セキュリティの問題についても，運用から対応策を講じていく必要がある．状況に応じて検疫システムも検討を考えている．

現在の認証方式が，スマートフォンなど小型デバイスからの利用しずらい点は大きな課題である．インターネットには認証サーバを検証せずに WEB 画面に認証情報を自動入力するツールも存在しており，不用意に利用されると非常に危険である．同様の問題を抱える公衆無線 LAN サービス業者は，ブラウザの Cookie 機能に対応した安全性が高い自動入力プログラムを提供したり，802.1X の利用を薦めている．本学では，802.1X に対応できる部局で WEB 認証と 802.1X のサービスを二面展開することを検討している．

6. おわりに

本稿では，大学の部局という地理的に密な組織が連携し，幅広い構成員に共通の無線 LAN サービスを提供する方式を述べた．キャンパスネットワークを部局が分割して運用管理している場合，組織連携によって大学全体の利便性と効率性を向上させる必要があり，それを実現する運用技術は重要である．本方式により，本学では 2.2 で述べた利便性の問題を大きく改善した．共通エリアに設置された基地局の無駄や電波干渉の問題も，間接的に軽減できると期待している．また，utroam で構築した Radius ツリーによって，今後は eduroam など他機関との連携や，学内における無線 LAN 以外の部局連携も促進していきたいと考えている．

謝辞 utroam 実験サービスと本論文作成に御協力頂いた，全学共通無線 LAN 作業分科会と ICT インフラ整備専門部会の皆様に感謝致します．

参 考 文 献

1) Congdon, P., Aboba, B., Smith, A., Zorn, G. and Roese, J.: IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines, RFC 3580 (Informational) (2003).
2) AshwinPalekar, DanSimon, J. S. G.Z. and Josefsson, S.: Protected EAP protocol (PEAP) version 2, Internet-Draft (work in progress), draft-josefsson-pppext-eap-tls-eap-10.txt (2004).
3) Funk, P. and Blake-Wilson, S.: Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0), RFC 5281 (Informational) (2008).
4) Simon, D., Aboba, B. and Hurst, R.: The EAP-TLS Authentication Protocol, RFC 5216 (Proposed Standard) (2008).
5) 篠宮俊輔，萩原洋一：大学キャンパス無線アクセスシステムの構築，情報処理学会研究報告，Vol.2001, No.50, pp.7–12 (2001).
6) 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. B, 通信， Vol.93, No.5, pp.759–768 (2010).
7) Forte, A.G., Shin, S. and Schulzrinne, H.: Improving layer 3 handoff delay in IEEE 802.11 wireless networks, *Proceedings of the 2nd annual international workshop on Wireless internet*, WICON '06, New York, NY, USA, (2006).
8) Calhoun, P., Montemurro, M. and Stanley, D.: Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification, RFC 5415 (Proposed Standard) (2009).
9) The FreeRADIUS Server Project, http://freeradius.org/ (accessed 2011-09-11).
10) eduroam JP, http://www.eduroam.jp (accessed 2011-09-11).
11) 藤澤 優，大谷 誠，渡辺健次：PKI 対応ネットワーク利用者認証システム Opengate-PKI の開発と試験運用，電子情報通信学会技術研究報告，Vol.108, No.459, pp.149–154 (2009).