組織連携によるキャンパス無線LANサービス utroamの展開と統計的評価

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

本学では，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。このため、ネットワークサービスが部局内に閉じており，学内者のユーザ情報は複数のデータベースに分散管理されている．このような環境で全学共通の無線 LAN サービスを実現するため，多様な無線 LAN システムと複数のユーザデータベースを連携させる運用方式を検討し，実験サービス”utroam”として学内に広く実験展開している．本稿では，本方式の仕組みと利用動向に関する評価を述べる．

The Deployment Report and Statistical Evaluation of ”utroam” the Wireless LAN service on Campus by Cooperation in Divisions

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

In our campus, the operation of the campus network is devided to many devisions. Thereby network services are only for internal users on each devision, and user information is decentralized to some databases. To realize an university common wireless LAN service on such environment, we considerd an operation scheme combining varied wireless LAN systems and multiple user databases, and we started a trial service. In this paper, we describe our architecture and statistical evaluation of our service from real usages.

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 サービスを提供している大学も多い．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．

†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

一方，東京大学は学部，大学院，研究センター，本部事務といった部局に分かれており，様々な学術分野と目的を持つ組織の集合である．部局毎に情報通信に対する要求が異なるため，本学ではキャンパスネットワークを各部局が分割運用している．これにより，部局の要望に沿った整備や運用が行いやすい反面，他部局の所属者にはサービスを提供することが困難であり，これまで全学内者を対象とした無線 LAN サービスを提供できていなかった．

本学では，ネットワーク運用を部局分割から特定部門による集中管理体制に移行するには，既存の体制から大幅にポリシ・組織・システムを変更する必要があり非常に困難である．また，もし無線 LAN だけを切り離して全学的に集中管理した場合，逆に部局内では無線 LAN の利便性やセキュリティが低下する可能性がある．例えば，幾つかの部局では無線 LAN を 802.1X のダイナミック VLAN[1)] や複数 SSID などにより有線 LAN と結合しているが，このように有線と無線に同じネットワーク環境が実現することが困難になる．

そこで，部局に分かれた運用体制を維持したまま，各部局の多様な無線 LAN システムを連携させ，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・施設が存在する．本学では，情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違いがあり，そのためネットワークの整備状況も非常に多様である．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構成要素を部局が独自に導入している．

2.2 無線 LAN 環境

本学の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) 講義室など主要エリアを中心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) 研究室など一般の学内者が設置したもの
(4) 公衆無線 LAN 事業者が設置したもの

(1) は，コンシューマ向けの基地局を最低限必要な場所にだけ設置している部局から，エンタープライズ向けの基地局を多数設置し，建物全館をカバーする大規模無線 LAN システムを構築している部局まで様々である．すなわち，基地局が独立して動作する FAT 型基地局と，無線 LAN 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．基地局のメーカ・機種・保持する機能も多様である．(2) は，本学の教育用計算機システムのユーザを対象とした演習・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に利用している．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．

このように多数の基地局が設置されている一方，本学は無線 LAN 環境に関して以下の問題を抱えている．

(1) 学内者であっても自部局や自研究室外では無線 LAN を利用できない場合が多く不便である．
(2) 部局が自部局の所属者以外に無線 LAN を提供する場合，その都度ゲストアカウントの発行など労力がかかる．
(3) 部局に属さない公共的なエリアでは，部局や用途毎に複数の基地局が設置され設備投資に無駄があったり，逆に全くネットワークサービスが利用できない場合がある．
(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，全構成員を登録する共通認証システムを構築途上であり，現時点ではサービス単位や部局単位で構築された認証システムのみ利用可能である．また，部局には他機関に所属する人物が学内者に近いかたちで活動しているなど個別の事情があるため，最終的なユーザ情報は部局内にのみ存在する．

3. 検討項目

3.1 システム要件

本学では，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 サービスを検討した．そのシステム要件を表 1 に示す．全学内者を対象としたユーザサポートは大きな労力がかかるため，一般ユーザによる利用の容易性を確保し，極力サポートを行わずに提供できる必要がある．サービスを広範囲に展開するためには，部局によるサービス導入も容易であることが望ましい．また，部局間の連携作業は時間がかかり各管理者の負担になるため，トラブル解決や構成変更の際に必要な連携を最小限に留め，容易に管理できる必要がある．また，サービス提供の大前提として，認証と無線 LAN 通信のセキュリティ確保が必要である．一方，多様な基地局を利用する以上，特定のサービス品質の確保は困難であり，その点はシステム要件から除外している．

表 1 システム要件
Table 1 System requirements

利用の容易性	ユーザ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 利用申請や端末の設定など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 既存の無線 LAN サービスと共存できること 専門的な知識を有する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	トラブル時に部局内・外など問題の切り分けを簡単に進められること 基地局を従来通り部局が分散管理でき，部局内のシステム変更が他部局に影響しないこと
認証セキュリティ	接続できる者を学内者に限定できること 認証情報の漏洩を防ぐこと
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

認証方式を検討するため，既存のキャンパス無線 LAN で主要である WEB 認証，802.1X 認証，VPN による認証の 3 方式を，3.1 の要件から比較した．こ

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

	WEB 認証	802.1X	VPN による認証
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 接続作業が必要
導入の容易性	○認証ゲートウェイを上流に設置すれば基地局の対応は不要	×全基地局が認証サーバと通信する必要がある	△既に VPN が導入されている場合を除き，接続先の VPN サーバが必要
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ログが必要 ○ログが揃えば問題の特定が正確	○ VPN 機能に依存するため無線のサービスは簡略化できる × VPN の障害が無線に影響
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可能	○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への不正アクセスが可能	○悪意を持った接続者を無線への接続前にブロック可能	×未認証の端末からオンリンクへの不正アクセスが可能

れを表 2 に示す．

WEB 認証は，ユーザ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入力にストレスがある．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 の上流で通信をフィルタしていると未認証の端末でアプリケーションが動作しなくなる問題もある．さらに，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，偽の基地局や認証ゲートウェイを設置して偽の認証画面にユーザを誘導することが理論上可能であり，それによって認証情報が盗まれる危険がある (ただし，学内で攻撃活動を行うことは攻撃者側のリスクも非常に高い)．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，アタック，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 を利用すると，認証が完了した後に端末が無線に接続する．ユーザ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 セキュリティ上の問題が発生しても，問題を起こしてい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，効率化が困難な部局も多数存在する．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 サーバのログを照合する必要がある．機器のログ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，大量のログ管理や，出力されるログフォーマットの違いを運用者が吸収するのは労力が高い．

VPN は，無線 LAN において VPN 機能により学内者を認証するためや[5)]，無線 LAN 通信を暗号化するためや[5)]，ユーザ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，既に VPN を利用している場合を除き，無線 LAN のために同時に VPN を導入することはユーザとサービス提供者の双方に大きな負担である．本学では VPN 設備を保持しない部局も多いため，VPN 設備を前提としたサービス設計は適切ではない．また，WEB 認証と同様に，この方式では未認証の端末を無線 LAN に接続させたうえで認証を行うため，未認証の端末による LAN セキュリティ上の問題が発生する危険がある．

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．本学ではネットワークの管理責任は部局にあるため，802.1X のダイナミック VLAN などによって，ユーザを所属部局のネットワークに収容できることが理想的だが，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 が構築困難である．そのため，無線端末を収容するサブネットが新たに必要である．このサブネットは，SSID との対応，ブロードキャストドメインとしての規模性，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キャンパスで単一のサブネットに収容する．この方式は部局を横断する一つの共通 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問題になる．ただし，基地局によっては，ARP や DHCP 等のブロードキャストを利用する機能を，無

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

線 LAN 上のブロードキャストを利用せずに動作させる機能や，ブロードキャストパケットを全般的にフィルタする機能など，無線の帯域を有効利用する機能を保持している．特定のブロードキャストパケットしか許可しないといった設定を VLAN の中間スイッチに設定することも可能である．したがって，方式 1 の規模性は検討の余地がある．

方式 2 は，ブロードキャストドメインの規模性に関する問題を回避できる．しかし，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．端末は同一 SSID が設定された基地局間を移動した場合にレイヤ 3 のハンドオーバが生じたことを検知する方法がない問題が指摘されており[7]，移動先で IP アドレスを再取得しないために長時間の通信断が発生する可能性がある．

方式 3 は，ユーザを論理的に所属部局に収容できる点や，ブロードキャストドメインの規模性の点から理想的であるが，802.1X のダイナミック VLAN が必要であり，既に述べたとおり本学には適用できない．方式 4 は，全学共通無線 LAN サービスの目的自体に合わない．

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．認証方式は，3.2 で述べたように，利用・導入・管理が容易であり，サービスの実現性が高いことから，WEB 認証を採用した．サブネット構成は，端末が複数部局が管理する基地局間を継ぎ目なく移動する可能性があるため，長時間の通信断が発生しないように，表 3 の方式 1(単一サブネット) とした．キャンパス間は離れているため，本郷・駒場・柏キャンパスに各 1 のサブネットを設置した．各サブネットはキャンパス内の複数の部局を横断する VLAN であり，utroam に参加する基地局全てに接続される．多くの基地局は複数 SSID と複数 VLAN が設定可能であるため，部局は既存の無線サービスを維持したまま utroam を追加提供できる．utroam に参加する全基地局は同一の SSID”utroam”を広告し，同一の WPA2 共有鍵を設定する．WPA2 は AES による暗号化のみを目的に利用し，学内者の認証には WEB 認証を利用する．utroam のサブネット上流に全部局共有の認証ゲートウェイを設置しており，ユーザ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．

認証先のユーザデータベースに関しては，2.3 で述べたように，本学には全構成員が登録されたデータベースが存在しない問題がある．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，部局が管理するデータベースを接続する学内の RADIUS ツリーを構築した．そして，utroam では登録されたデータベースの何れかに有効アカウントが存在することを学内者の証明とした．2011 年 11 月時点で，学内 RADIUS ツリーには 2 つの学内サービス部門と 3 つの部局によるユーザデータベースが接続されている．これにより全構成員の約 8 割が利用可能となっている．このほか，有効アカウントを RADIUS で確認できるユーザに対し，utroam 接続用の仮名アカウントを WEB 上で配布しており，仮名アカウントのデータベースも RADIUS ツリーに接続している．学内アカウントの漏洩防止のため，ユーザには仮名アカウントへの移行を促している．

4.2 実　　装

本システムの WEB 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．端末は無線に接続すると DHCP によって IP アドレスを取得できるが，認証が行われるまで，認証ゲートウェイは DHCP と DNS 以外のパケットをサブネット外へ転送しない．端末からサブネット外への HTTP または HTTPS 通信が開始されると，認証ゲートウェイはそのコネクションを奪い取り，HTTP リダイレクトによってユーザのブラウザに認証ページを表示する．認証が成功すると，認証ゲートウェイは端末の IP アドレスと MAC アドレスを認証済端末エントリとして記憶する．エントリはその端末による通信が 30 分間検出されないと自動的にタイムアウトする．タイムアウト後に利用する場合は再認証が必要である．utroam は共有端末でなく個人端末を想定しており，アカウントを切り替えて利用する必要性がほぼないことや，後述のとおり 1 アカウントにつき 2 台の同時接続が可能であるため，ユーザ自身によるログアウトページは表示しない設定にしている．また，認証システムへのブルートフォースアタックを防止するため，認証ゲートウェイでは，一定回数連続して認証に失敗すると，その端末による通信を自動的に一定時間フィルタする．

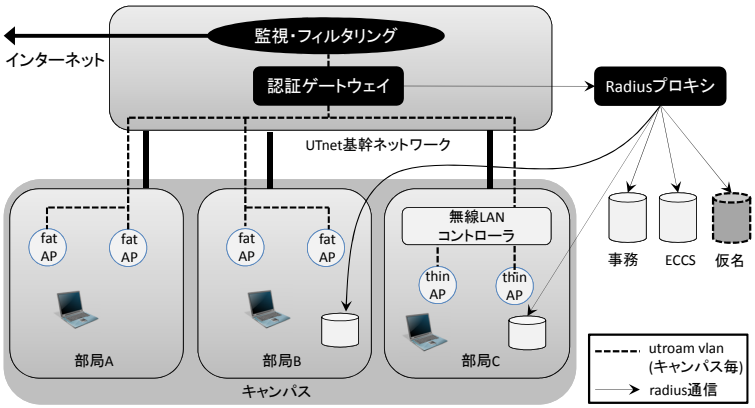

図 1 utroam のシステム構成
Fig. 1 System architecture of utroam

認証ゲートウェイの上流では，utroam サブネット内の監視とアプリケーション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，不審な通信や P2P 型アプリケーションの活動を検知した場合は，当該 IP アドレスを利用している部局に情報を通知している．utroam では RADIUS の認証ログからアカウント情報を抽出し，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，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]通信先の学内・学外は区別せず，同じポリシを適用している．現在は機材の理由でポート番号によるフィルタを行っており，そのため上記のように最低限の通信だけ許可しているが，これに不便を感じているユーザも多数存在するため，プロファイルにより柔軟にアプリケーションを識別・制限できるファイヤウォールを導入し，ユーザの自由度を確保することを検討している．なお，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が，現在までその事例はない．

RADIUS ツリーの中心となる RADIUS プロキシは，freeradius[9] にて構築した．freeradius では仮想サーバ機能が利用できるため，接続するユーザデータベースが LDAP 機能しかサポートしていない場合，LDAP サーバに RADIUS フロントエンドを提供する仮想サーバをプロキシ上に作成することで，最小限のマシン構成で RADIUS ツリーを構築できた．ユーザは RADIUS 上のレルムによってユーザデータベースを指定するが，レルムの末尾に u-tokyo.ac.jp を付与するフル表記と，それを省略した短縮形により，見かけのうえで 2 つのアカウントと考え，各アカウントにつき 1 台（合計 2 台）を接続可能とした．

⋆1 利用できる VPN 方式は eduroam[8] 仕様を参考にした．

部局では，無線 LAN コントローラを利用する場合に下記の対応が必要になった．図 1 のように，Thin 型基地局の通信を CAPWAP[10] 等により単一のコントローラに収容している部局では，基地局はコントローラを通じて utroam の VLAN に接続する．そのため，Thin 型基地局が複数のキャンパスに分散しており，それを特定キャンパスのコントローラに収容している場合，基地局全てをコントローラが存在するキャンパスの VLAN に接続すると，他キャンパスの基地局は間違ったキャンパスの VLAN に接続してしまう．今回，本学で使用したコントローラでは，特定の SSID を広告する基地局を複数のグループに分け，グループ毎に異なる VLAN に接続する機能により問題が解決したが，今後部局が無線 LAN システムを導入する場合に注意が必要である．

5. 統 計 評 価

本学では，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 865 台（本郷キャンパス 518 台，駒場キャンパス 261 台，柏キャンパス 86 台）である．基地局の分布を図 2 に示す．

5.1 利 用 数

2011 年 3 月 2 日から 2011 年 10 月 31 日までに利用された総アカウント数は約 2900 であった．認証された端末数は約 3600 であった．図 3 に最大同時接続端末数の推移を示す[⋆1]．サービス開始から夏期休暇を挟ん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．柏キャンパス

⋆1 グラフは DHCP のログから作成しており，認証前の端末も含む．DHCP のリースタイムは 30 分と短く設定している

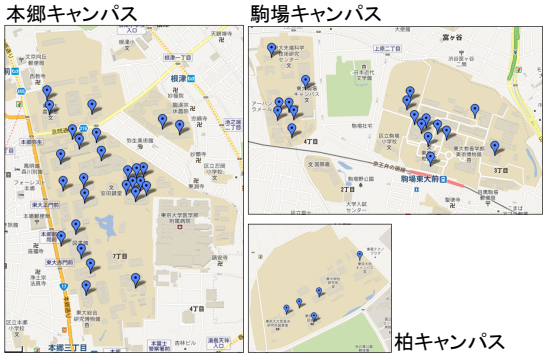

図 2 基地局の分布（建物にのみポイント）
Fig. 2 Distribution of APs（Only buildings are pointed）

の変化が少ないのは，既に部局が独自に学内者向けにサービスを公開しているためであるが，近く utroam への統合を検討している．

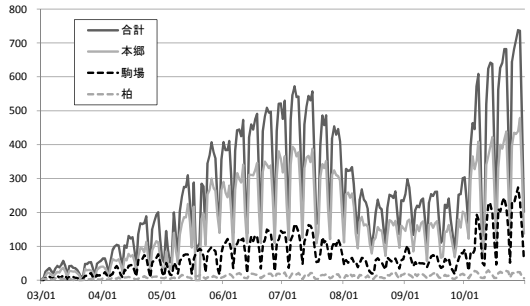

図 3 最大同時接続端末数
Fig. 3 Peak numbers of connected devices per days

4.2 に述べたように，認証ゲートウェイの端末エントリは 30 分間その端末の通信を検知しないとタイムアウトするため，再度利用する場合に再認証が必要である．再認証がユーザの負担になっていないか検討するため，アカウント毎の 1 日の認証回数を図 4 に示す．多くのアカウントは 1 回のみ認証しているが，2 回，3 回，4 回以上と認証を行っているアカウント数も無視できない数である．PC 端末では，ユーザが意図的な通信を行っていない時間帯にもバックグラウンドプロセスによる通信が継続的に発生すると考えられ，タイムアウトは利用終了か完全な圏外で生じると考えられる．しかし，タブレット端末やスマートフォンは頻繁に電源オフとなり，バックグランドの動作頻度も少ないと考えられ，頻繁な再認証がユーザの負担になっていたり，利用が見送られている可能性がある．PC 以外の端末の割合としては，DHCP のログからマシン名を取得できた端末 3269 台のうち，751 台 (約 23.0%) はスマートフォンやタブレットマシンと思われるマシン名が付与されていた．その内訳を表 4 に示す．

端末の種類による利用日数を比較したものが図 5 で

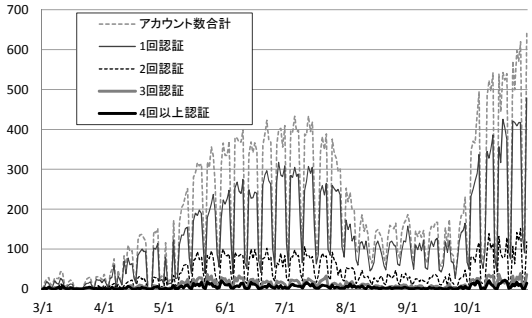

図 4 日毎の認証回数
Fig. 4 Times of authentication per accounts per days

表 4 PC 以外の接続台数
Table 4 Number of non-PC-nodes

iphone	232
Android	199
ipad	128
ipod	192

ある．さらに利用日数を詳細に示したものが図 6 である．全端末と PC 以外の端末とで，利用頻度の分布は類似しているが，PC 以外の端末は 1 日のみ利用された割合が高い．これらの端末では前述のタイムアウトと，ブラウザの認証画面への入力が煩雑であるため，継続的な利用を見送ったユーザ存在したと推察される．さらにスマートフォンに絞ると，無線 LAN よりも低速であるが携帯電話網による通信が可能であるため，全般的に利用頻度が低下している．しかし，iphone では 1 日のみ利用した割合が高いと同時に，多くの日数利用している端末の割合も高い．これは，携帯電話網の通信環境など，外的な要因が利用頻度に影響していると考えられる．なお，全般的に利用日数はそれほど多くないが，本サービスは所属部局によって無線 LAN が提供されていない場所で利用するために設置しており，さらにサービスが認知されるまでの期間を差し引くと，十分継続的に活用されている．

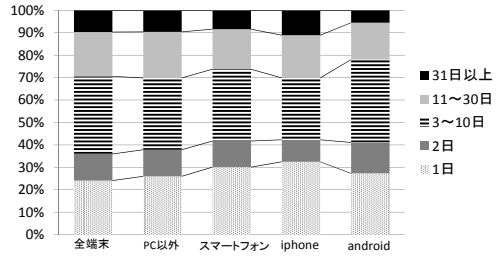

図 5 端末の種類による利用日数の比較
Fig. 5 Comparison of numbers of use days per device types

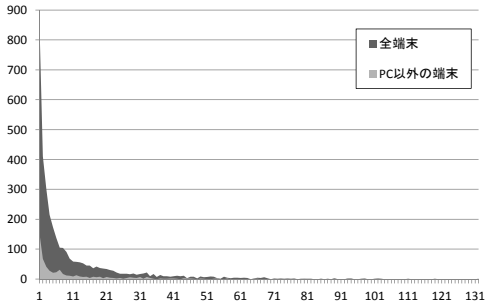

図 6 アカウント毎の総利用日数
Fig. 6 Number of days of usage per accouts

5.2 トラフィック量

図 7 は，2011 年 6 月 10 日から 2011 年 10 月 31 日までの 5 分平均によるピークトラフィックである．Inbound は無線端末の受信，Outbound は無線端末からの送信である．収容しているのは全て無線端末であるが，ピーク時には受信が 70Mbps 近くに達している．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，本システムのように全トラフィックを認証ゲートウェイに集約すると，今後も相当の通信量が生じると予想される．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ユーザも散見された．

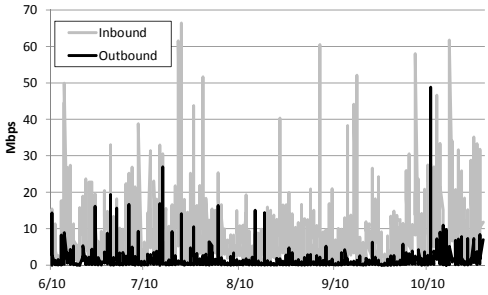

図 7 ピークトラフィック
Fig. 7 Peak traffic

6. 考　　察

6.1 運 用 負 荷

本サービスは，現在のところ 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．

6.2 アカウント情報の漏洩防止

3.2 で述べたように，無線 LAN で WEB 認証を利用すると，攻撃者がユーザを偽の認証ページに誘導する可能性がある．utroam では，認証ページにおいて NII より配布されている正規のサーバ証明書[11] を提示し，ユーザに認証ページの正当性を確認するように指示しているが，全てのユーザが注意深くこの作業を行うことは期待できない．現在の WEB 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り，ブラウザのチェックによる効果も低いと考えられる．そこで，学内アカウントの盗難被害を防ぐため，4.2 で述べたように，utroam 接続専用の仮名アカウントを配布している．しかし，仮名アカウントの取得や維持はユーザの負担が増すことや，仮名アカウントが漏洩した場合，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から，短期的な解決法と考えている．

パスワードを利用する認証方式のうち，802.1X の EAP-PEAP[2] 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，偽の基地局と認証サーバによって認証情報を盗まれる危険が少ない．ただし，端末を正しく設定しないと認証サーバの検証を行わない可能性があるため，安全性の確保にはユーザの教育とサポートが必要である．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，固定のパスワードを利用しない認証方式への移行が望ましい．その点では，802.1X の EAP-TLS[4] や，ワンタイムパスワードの利用が望ましい．クライアント証明書を利用した WEB 認証方式[12] も提案されている．今後，段階的に認証方式の強化を行っていく予定である．

6.3 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[8] 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，接続場所によって異なる．

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．ユーザは，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アプリケーションを利用できる必要がある．そのため，3.3 で検討したように，論理的に同じ環境を提供するシステム構成が必要であった．

6.4 今後の課題

今後の接続端末数増加に対応するため，キャンパス毎に設置したサブネットについてブロードキャストド

メインとしての規模性を検証していく必要がある．有線から無線へのフィルタ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の利用も検討したい．

5 で述べたように，WEB 認証方式が，スマートフォンやタブレット端末から利用しずらい点は利便性の問題である．スマートフォン用のツールの中には，認証サーバを検証せずにブラウザに認証情報を自動入力するものも存在しており，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商用公衆無線 LAN サービスでは，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 に対応できる部局において，WEB 認証と 802.1X を二面展開することを検討している．

また，utroam と同様の認証を，学内の講義室や会議室の卓上情報コンセントでも利用したいという要望がある．しかし，有線 LAN ではループ結線などにより異常トラフィックが発生する危険が高いため，無線と同様にキャンパス共通のサブネットを部局を跨いで設置することは適さない．このため，異なるネットワーク構成による実現を検討している．

7. おわりに

大規模な無線 LAN を運用する場合，基地局と無線 LAN コントローラを特定のベンダに統一して行うことが一般的である．集中制御による管理労力の軽減や高機能化は大きなメリットであるが，無線 LAN コントローラやシステム全体の肥大化，単一障害点になること，トラフィックや負荷の集中，システム移行の困難性といったデメリットも存在する．また，本学のように，歴史的，組織的な理由や，または予算的な理由により，大規模な集中管理体制が構築できない場合も存在する．その問題を解決するのが無線 LAN システム間のローミング技術や運用における連携技術である．本稿では，本学の部局という，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．これにより本学では，部局による分割運用と部局内ネットワークの最適構成を維持したまま，大学全体の利便性を大きく向上させることができた．今後は，本運用方式の評価を継続すると共に，セキュリティ強化・安定性向上・利便性向上を目指して，運用強化と要素技術の開発を行っていきたい．また，無線 LAN 以外での部局連携への応用や，eduroam など他機関との連携を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，東京大学全学共通無線 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) P. Congdon and B. Aboba and A. Smith and G. Zorn and J. Roese: IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines, RFC 3580 (Informational)(2003)
2) Ashwin Palekar, Dan Simon, Joe Salowey, Glen Zorn and S. Josefsson: Protected EAP protocol (PEAP) version 2, Internet-Draft (work in progress), draft-josefsson-pppext-eap-tls-eap-10.txt(2004)
3) P. Funk and S. Blake-Wilson: Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0), RFC 5281 (Informational)(2008)
4) D. Simon and B. Aboba and R. Hurst: 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 分散システム/インターネット運用技術, No50, 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, Vol.93, No.5, pp.759-768(2010)
7) Forte, Andrea G. and Shin, Sangho and Schulzrinne, Henning: Improving layer 3 handoff delay in IEEE 802.11 wireless networks, WICON '06 Proceedings of the 2nd annual international workshop on Wireless internet, ACM, New York(2006)
8) 国立情報学研究所: eduroam JP, http://www.eduroam.jp/
9) The FreeRADIUS Server Project, http://freeradius.org/
10) P. Calhoun and M. Montemurro and D. Stanley: Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification, RFC 5415 (Proposed Standard)(2009)
11) 国立情報学研究所: UPKI イニシアティブ, https://upki-portal.nii.ac.jp/
12) 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)