4　無線セキュリティ技術
4　Wireless Security Technologies

4-1　モバイルイーサネットとそのセキュリティ
4-1 Mobile Ethernet and its Security toward Ubiquitous Network

宮本　剛　　黒田正博
MIYAMOTO Goh and KURODA Masahiro

要旨

ユビキタス環境とは、3G、WLAN、無線 MAN などの無線システムがシームレスに統合された環境をいい、小型無線装置と合わせて近い将来の普及が期待されている。モバイルイーサネットは異種無線システムを統合するアーキテクチャの一つであり、いつでもどこでもネットワークにアクセスできる環境を実現する。本稿では将来のユビキタス環境を視野に入れたモバイルイーサネットアーキテクチャを 3GPP と IEEE802LMSC の観点から解説する。次に、モバイルイーサネットのセキュリティについて取り上げる。これはアプリケーションとネットワークの両方の認証に対応したセキュリティ方式である。続いて無線セキュリティの課題について論じる。一つは、無線システム間で機密を保持するための共通メカニズムを備えること。もう一つは、アベイラビリティ（可用性）を維持する機能を備えることである。無線セキュリティの議論はまだ途上であり、今後のユビキタスネットワークに向けてプライバシー問題に関する研究を進める必要がある。

The ubiquitous environment is a seamless integration of radio systems, such as the 3G, WLAN and wireless MANs, and is expected popular in near future combined with small RF devices. The Mobile Ethernet is an architecture to integrate different types of radio systems and provide transparent network access anytime anywhere. We explain the Mobile Ethernet architecture for future ubiquitous environment from the viewpoint of 3GPP and IEEE802 LMSC. We, then, talk the Mobile Ethernet Security which is the security framework to accommodate both application and network authentications. We, then, discuss wireless security issues. One is to have a common mechanism to keep confidentiality among radio systems. The other is to provide functions to maintain availability. The wireless security discussion is still on the way and we need to investigate privacy issues for security of future ubiquitous network.

[キーワード]
セキュリティ、モビリティ、DoS 攻撃、ユビキタス無線ネットワーク、無線セキュリティ
Security, Mobility, DoS attack, Ubiquitous wireless network, Wireless security

1　はじめに

ユビキタス環境においては、ネットワークに常時接続されることが期待される。「Beyond 3G」と呼ばれる次世代無線ネットワークは、3G、WLAN、無線 MAN といった異種無線システムを統合し、ユビキタス環境の一候補となっている。Beyond 3G は各無線システムの長所を生かしながら、IP サービスに対してオール IP の無線ソリューションを提供する。

無線ネットワークを IP 技術によって一つのオール IP 網に統合するための作業が現在実施されている[1]－[3]。その基本的な考え方は、無線に依存する機能をできるだけ局所化し、モビリティ、認証、信号制御を共通の IP レイヤによって提供するというものである。IP 網のインフラは IEEE 802 の無線技術と合わせて都市圏ネットワークに普及しつつあり、今後は 3G システムを収容することが期待されている。

3G をベースにした IP 網が無線ネットワークとして徐々に普及する一方、IEEE802.11 に基づくネットワークはその費用対効果の高さによって急速な広がりをみせている。3GPP（3rd Generation Partnership Project：3G システムの標準化団体）では、IP より下のレイヤで行われる RAN（無線アクセスネットワーク）の無線システム間のモビリティ管理とハンドオーバ管理を Beyond 3G に向けて改善するための議論が行われている[4]。IEEE802LMSC[5] も、無線システムの統合について活動している。IEEE802.16[6] ワーキンググループは、固定網と移動網を無線 MAN 環境に混在させる固定広帯域無線アクセスシステム（Fixed Broadband Wireless Access System）の仕様策定に取り組んでいる。また IEEE802.21[7] ワーキンググループは、IEEE802.11、802.16、3G などの無線方式をまたぐ際のシームレスなハンドオーバインタフェースを策定中である。IEEE802LMSC に基づく無線システムはユビキタス環境における重要要素になりつつあり、MIMO システムを用いたソフトウェア無線技術[8] を用いることで共通の IEEE802MAC 層に収束するものと期待されている。共通の IEEE802MAC 層に収束するに当たっては、複雑な IP パケット転送や非効率な再認証などを必要としないことが期待される。

モビリティ管理には 2 種類ある。一つはマクロモビリティで、データ紛失は許されないがリアルタイム性が要求されないもの。もう一つはマイクロモビリティで、VoIP やテレビ会議のようなリアルタイムアプリケーションに対して高い応答性が要求されるものである。統合無線システムではマクロモビリティはモバイル IP[9] によって実現される。モバイル IP の改良作業では、階層的なネットワーク管理[11] による効率的なルート最適化、高速ハンドオーバ[10] 及び制御パケット数の低減が盛り込まれている。これらの改良を実現するには、カプセル化のほか、ルータ間の端末移動時に Binding Update など多くのメッセージ交換が必要となる。また、Binding Update 情報の有効性を確認するための Return Routability も必要になる。カプセル化は処理負荷を高める上、都市圏では頻繁なハンドオーバが起こるため上記のメッセージ交換によってシグナリングの負荷が高まる。この方式は、二つの異種サービスネットワークの間で行われるマクロハンドオーバに適している。一方、マイクロモビリティでは、リアルタイムアプリケーションに対してシームレスな無線統合が要求される。音声通信では一つのパケット紛失でもノイズや切断の原因となる。ユビキタス環境では、公共利用の規格に従ったマクロモビリティとマイクロモビリティが共に期待される。

ユビキタス環境のセキュリティ管理には、ネットワークアクセス認証、無線アクセスセキュリティ、無線プライバシーなどの側面がある。統合無線ネットワークでモバイル端末をあるシステムから別のシステムにハンドオーバするときには、ネットワークは、そのネットワーク内の認証サーバに問い合わせを行うことによってその無線アクセスが許容されるかどうかを確認する。ネットワークアクセス認証は個々の無線システムとは独立していることが期待される。また、ネットワークは攻撃を受けない安全な無線アクセスを提供する必要がある。無線システムが空中を飛ぶコンテキスト情報を用いた DoS（サービス妨害）攻撃を受けると、そのネットワークは正常に機能しなくなる。DoS 攻撃だけでなく、無線妨害、無線セッションの乗っ取り、無線でのフラッド攻撃を防止するには、コンテキスト情報を使って端末を追跡不能にする必要がある。

本稿では、ユビキタスネットワークを対象としたモバイルイーサネット（Mobile Ethernet）とそのセキュリティについて論じる。**2** ではモバイルイーサネットのアーキテクチャ、Beyond 3G 及びそのマイクロモビリティ対策について説明する。**3** ではアプリケーションレベルの認証と同様の形で実施されるネットワークアクセス認証の方式について取り上げ、ハンドオーバ認証について論じる。**4** では無線セキュリティについて説明する。そこではモバイル端末の位置情報を用いた鍵管理

方法を提唱する。その方法は無線システムに依存しない。続いてモバイルイーサネットの無線インタフェースを DoS 攻撃から守る機能について論じる。最後に今後の課題について**5**で触れる。

2　ユビキタスネットワーク：モバイルイーサネット

ユビキタスネットワークでは、ネットワーク及び無線システムのシームレスな統合が期待される。モバイル IP ソリューションを備えたモバイルイーサネットは、マクロモビリティとマイクロモビリティの両方を実現する。本章では現在のモバイルイーサネットとその将来的な描像について説明する。

2.1　3GPP エボリューションにおけるモバイルイーサネット

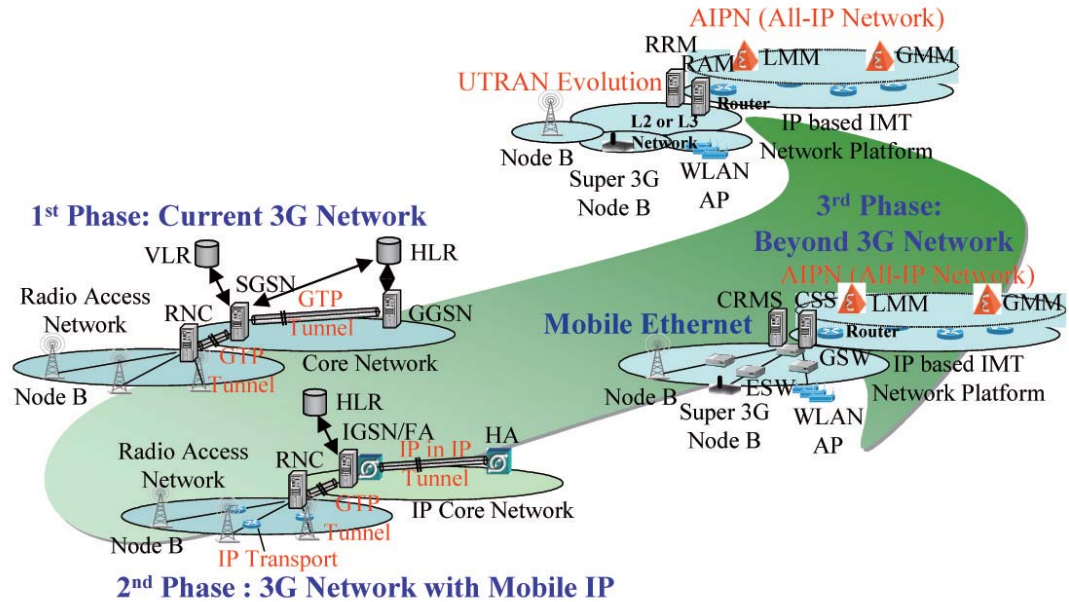
3G の方向性については幾つかの議論がある。図 1 に、3GPP で議論されている 3G の発展形態（3GPP evolution）を示す。

第 1 段階として描かれているのは、日本で現在行われている 3G の携帯電話サービスである。第 2 段階は、基幹網に IETF のモバイル IP を導入してモバイル管理を向上させる試みである。ただし、将来の 3G として使えるかどうかの実証は済んでいない。このアーキテクチャではモバイル IP のモビリティ処理が GSM に盛り込まれる[12]。第 3 段階では基幹網のモビリティ管理の向上が図られ、高度なルータネットワークが形成される[13]。UTRAN の発展形についても動的なリソース割当てとスケジューリングの最適化が議論されている。また、異種無線システム間で効率的なハンドオーバを可能にするようなトラフィック管理ないしモビリティ管理と MAC インタフェースの改善についても議題となっている[14]。モバイルイーサネットは、UTRAN の発展形で用いられる RAN 技術の一候補である。

2.2　モバイルイーサネットのアーキテクチャ

モバイルイーサネットはレイヤ 2 をベースとする都市圏ネットワークであり、各種の無線システムを収容する。このときデータとシグナリングに対して共通のインタフェースが提供される。モバイルイーサネットは Provider Bridge[15] などの別技術を用いることでサポートエリアを拡張できる上、ルータを介してインターネットにも接続できる。図 2 にその様子を示す。

モバイルイーサネットでは基幹網においてすべてのメッセージが固有の MAC アドレスを用いて



GTP: GPRS Tunneling Protocol (GPRS: General Packet Radio Service), RNC: Radio Network Control, HLR: Home Location Register, VLR: Visitor Location Register,
SGSN: Serving GPRS Support Node, GGSN: Gateway GPRS Support Node, IGSN: Internet GPRS Support Node, HA: Home Agent, FA: Foreign Agent,
UTRAN: UMTS Terrestrial Radio Access Network (UMTS: Universal Mobile Telecommunications System), GMM: Global Mobility Manager, LMM: Local Mobility Manage,
RAM: Radio Access Manager, CRMS: Common Resource Management Server, CSS: Common Signaling Server, GSW: Gateway Switch, ESW: Edge Switch

図 1　3GPP エボリューション

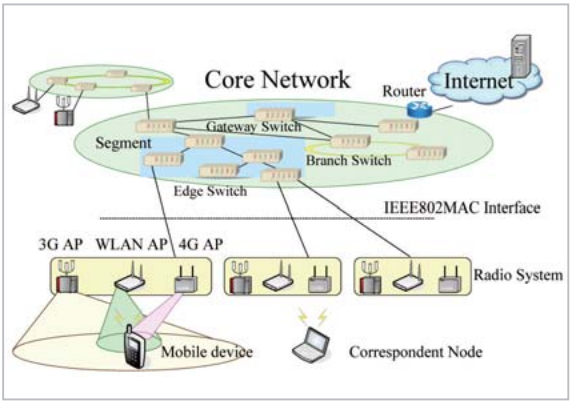


図2 モバイルイーサネット

実質的にブロードキャストされ、共通の MAC インタフェースの先にある 3G、WLAN、無線 MAN、4G などの各種無線システムに送られる。スケーラビリティを確保するため、経路学習機能キャッシュを備えたレイヤ 2 スイッチをネットワーク全体に配置する。あて先 MAC アドレスまでの経路はその経路上にあるすべてのスイッチが学習し、それによって無用なブロードキャストの送信がなくなる[16][17]。

モバイルイーサネットは、レイヤ 2 スイッチアーキテクチャによるリアルタイムハンドオーバ機能と、シームレスなハンドオーバを実現する予測メカニズムを備えることにより、リアルタイムアプリケーションに対応することができる。さらにスイッチの経路学習機能キャッシュを動的に更新するシグナリング機構を備え、ブロードキャストされるシグナリングパケットを抑止する。

モバイルイーサネットはレイヤ 2 スイッチ、共通シグナリングサーバ（CSS）、バッファリングサーバで構成される。レイヤ 2 スイッチにはゲートウェイスイッチ（GSW）、ブランチスイッチ（BSW）、エッジスイッチ（ESW）の 3 種類がある。GSW は基本的なモビリティ機能を備える。これには例えば、レイヤ 2 のモビリティ管理フレームを交換する MAC アドレス学習、フラッディングを不要とする IPv6 マルチキャストトラフィック制御、MAC アドレスの付け替え及び共通シグナリングサーバの MAC アドレステーブル設定に対応したインタフェースなどがある。BSW は GSW と ESW の間に介在する中継スイッチであり、基本的なモビリティ機能を備えている。ESW は MAC フレームの転送を実行する。基本機能以外にも、例えばモバイル端末と CSS の間で共通の無線シグナリングメッセージを中継する。

CSS はメッセージを処理し、モバイル端末と無線システムの制御を行う。CSS はネットワークアクセスポイントを検知できるようモバイル端末に隣接 AP のリストを通知するほか、ハンドオーバ要求などのモビリティ管理指示を与える[18]。一方、モバイル端末はスリープモード中のモビリティ管理に用いられる Location Area Update メッセージ[19]や、ネットワーク主導ハンドオーバにおいてトリガ時に使用される受信信号長の測定データ[20]など、様々な共通無線シグナリングメッセージを発信する。バッファリングサーバは、モバイル端末の呼出しのためにユーザデータフレームを蓄積する。ネットワーク機器とインタフェースの概略を図 3 に示す。

2.3 将来のモバイルイーサネット

上述したモバイルイーサネットのアーキテクチャには、ネットワーク機器と仕様がすべて規定されている。我々は、W-CDMA（3G）及び IEEE 802.11b という異種無線システムから成るモバイルイーサネットシステム[21]を用いて検証実験を行い、ロスレスかつリアルタイムのハンドオーバが共通 MAC インタフェース及びネットワーク機器の下で提供できることを検証する。

各ネットワーク機器の仕様とインタフェースについて確認と標準化作業が完了した場合、将来のモバイルイーサネットではネットワークのどこかにモバイルイーサネットスイッチが導入されることが期待される。この装置は、GSW／BSW／ESW のいずれかと CSS ／バッファリングサーバの機能を併せ持つ装置である。また、このネットワークでは、あらゆる場所のアクセスポイントす

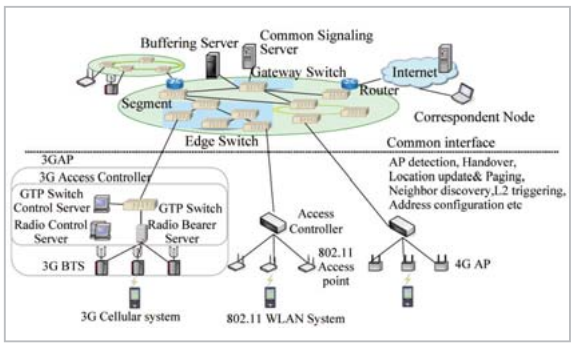


図3 ネットワーク機器とインタフェースの概略

べてにおいてユーザが常時無線アクセスできることが期待される。将来のモバイルイーサネットでは、無線システムの種類に依存しないユビキタス無線ネットワークが実現するものと期待される。その概略を図4に示す。

近い将来、モバイル端末の中には無線の設定を変更することにより、ユーザ位置で使える無線システムやサービスにその場で同調できるものが現れると推測される。そのようなモバイル端末は無線設定をシームレスに変更できる上、サービスの連続性を効率よく実現するためにIPアドレスなど一意のアドレスを使用するものと期待される。モバイルイーサネットには、IPアドレスを変えることなくすべての無線システムにアクセスできる機能が備わっている。

3 モバイルイーサネットのセキュリティ

モバイルイーサネットではユーザが移動中でも、無線システムから別の無線システムにシームレスにハンドオーバすることができる。例えリアルタイムアプリケーションであってもユーザは中断なくサービスが継続されることを期待する。本章では、アプリケーションレベルの認証と同様の形で実施されるネットワークアクセス認証の方式について説明したあと、垂直ハンドオーバの認証について論じる。

3.1 ネットワークアクセス認証方式

我々はモバイルイーサネットを対象に、アプリケーションレベル認証、ネットワークアクセス認証及びこの二つの認証をつなぐセキュリティリンクからなるセキュリティ方式を提唱した[22]。この方式は、ユーザデバイスが個人識別カード(PIC)とモバイル端末という二つの部分に分かれることを前提としている。PICは、無線アクセス／ISP証明書など何らかの証明書をセキュアな形で格納する。モバイル端末はネットワークアクセス認証／アプリケーションレベル認証に用いる委譲証明書を保持する。ここで規定されるPICとモバイル端末間の相互認証では、バイオメトリクス(生体認証)などの方法によってPIC内部で認証処理が実施される。

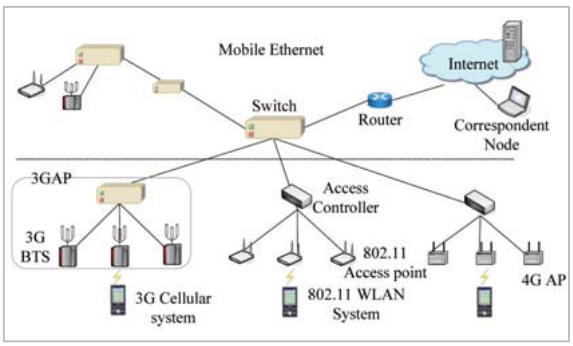


図4 将来のモバイルイーサネット

アプリケーションレベル認証は、委譲証明書を持つモバイル端末とサービスプロバイダ(ISPなど)の間の相互認証である。ネットワークアクセス認証も、モバイル端末と無線ネットワークの間の相互認証である。モバイル端末は無線ネットワークにつながるときにその認証を行う。ネットワーク側も、その端末がネットワークに対するアクセス権を持っているかどうかをチェックする。

図5に、アプリケーションレベル認証とネットワークアクセス認証の両方に対応できる方式を示す。

3.2 ハンドオーバ認証と AAA

モバイル端末が同一セグメント内の別の無線システムに移動する場合(セグメント内ハンドオーバ)、端末はUpdate Entry Request(UER)をAPに送出したあと、上の階層に上がってUERがAAAサーバに届くのを待つ。その様子を示したのが図6である。ネットワークアクセス認証は、モバイル端末とAAAサーバの双方向ハンドシェイクによって行われる。モバイル端末が別のセグメントの無線システムに移動する場合にはAAA

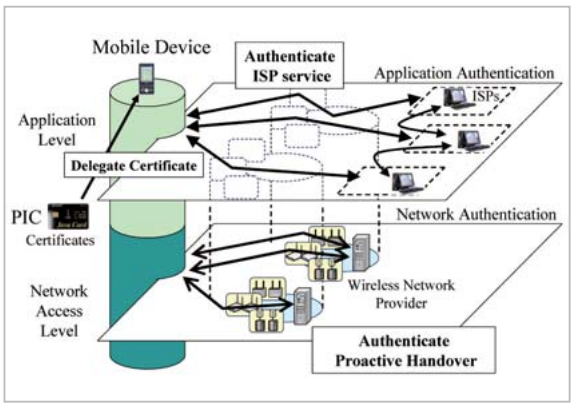


図5 アプリケーションとネットワークの認証の方式

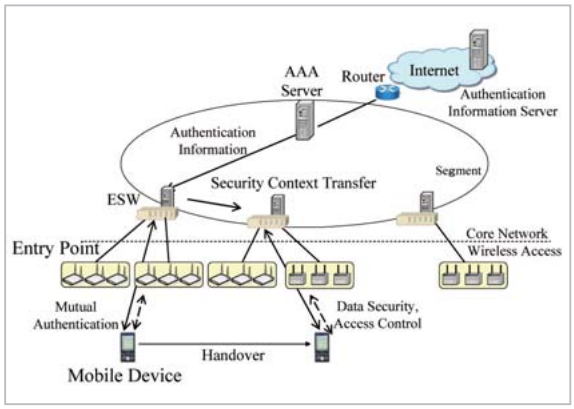


図6 予測型ネットワークアクセス認証

サーバの階層まで上がる。

リアルタイムアプリケーションの場合、ハンドオーバの認証処理はサービス中に実施する必要がある。モバイルイーサネットではネットワーク主導ハンドオーバの利点を生かした事前認証が期待される。モバイル端末が現在の通信エリアを離れるとき、ネットワークはどの無線システムを使うのが適切であるかということを知っている。ネットワークはモバイル機器が属する ESW から新しい ESW へセキュリティコンテキストを転送し、事前認証を行うため、改めて要求を送出しなくて済む。

この認証方式は、多くのサービスプロバイダ(アプリケーションや無線アクセスなど)と多くのユーザを前提にしている。そのようなシステムでは、ユーザが移動するたびに秘密鍵を共有して認証を行うとすれば、ユーザは多量の計算を事前に行う必要が生じる。それよりもチケット認可サービスを利用し、セグメント内の各 AAA サーバに各プロバイダを登録するほうが好ましい。チケット認可認証の方式はユビキタス環境に適用されるが、その場合、すべてのユーザがすべてのサービスに対して PIC を使用できることが前提となる。

4 ユビキタスネットワークに向けた無線セキュリティ

無線セキュリティをめぐって二つの議論がある。一つは、無線システム間で機密を保持するための共通メカニズムを備えること。もう一つは、アベイラビリティ(可用性)を維持する機能を備えることである。

モバイルイーサネットでは各種無線システムの統合が期待される。各無線システムには独自の認証方式があり、なかには互いに相いれない方式もある。以下では、モバイル端末の位置情報を用いたセキュリティ鍵管理方法を導入する[23]。これは無線システムに依存しない。次にモバイルイーサネットの無線インタフェースを DoS 攻撃から守る機能について論じる。

4.1 無線システムに依存しない認証

この節では、位置情報を用いる、無線システムに依存しない無線セキュリティについて説明する。この方式を使用することで、モバイル端末とネットワークの間で低負荷の認証処理が実現する[24]。

(1) 鍵素材としての位置情報

移動環境において位置情報は認証素材の候補の一つである。認証には、モバイル端末と AP が共有するコンテキストとしてモバイル端末の位置リストが使用される。モバイル端末の位置はユーザの移動に従って変化する。位置の情報はユーザが通信を開始した時点で端末と AP によって共有される[25]-[27]。位置情報のリスト(モバイル端末に関する一種の足跡)は、端末と AP の共有コンテキストとみなされる。

一方、ネットワークの AP はモバイル端末から受け取る信号強度を基に位置を計算する[28]。この位置情報は送信によって端末と AP の間で共有される。この情報は GPS(全地球測位システム)よりも粗いが、端末がつながっている AP が持つ一意の ID も端末の位置を表すと考えられる。モバイル端末とネットワークが共有する位置情報は、端末及び相互認証を行う AP の対称鍵を生成する種として使用される。

(2) 移動履歴:共有位置情報

移動履歴(track)とはモバイル端末の位置情報のリストである。位置情報とは、例えば無線システムの ID である。移動履歴が作成されると、リストはモバイル端末とネットワークとで別々に更新されたのち、両者に矛盾がないように管理される。最新の位置はリストの一番上に表示される。一番下に記載されていた一番古い情報は削除されるため、全体の長さは維持される。

移動履歴は端末と AP の相互認証の共有コンテ

キストとして以下の課題の解決に使用される：a) 盗聴と予測、b) セキュリティ侵害、c) 競合。

a）盗聴と予測

モバイル端末のトラフィックを誰かがある場所で調べている場合、端末の位置情報が攻撃者に漏れる恐れがある。しかし、攻撃者が手元の位置情報から、端末のすべての移動履歴を予測することは困難である。十分に強力な鍵の個数が 2128 だとすると、推定される移動履歴の最小長は 40 以上となり、これはモバイル端末に実際に実装される場合の現実的な値だと思われる。

b）セキュリティ侵害

移動履歴を長期に使用することによるセキュリティ侵害は決して発生しない。これは、モバイル端末の移動に伴って移動履歴が頻繁に書き換えられることによる。ただし、モバイル端末が十分に堅牢であり、物理的な攻撃によって移動履歴が外部に漏れないことを前提とする。

c）競合

モバイル端末の移動履歴が他の端末の移動履歴とまったく同一の場合、移動履歴の競合が生じる。ネットワークは競合の起こりやすさを検出することによって競合を回避する。それによって、例えば 1 人のユーザがモバイル端末を 2 台持ち歩いても移動履歴の競合が発生しなくなる。

4.2　追跡不能

無線セキュリティは有線ネットワークが持つセキュリティの延長として扱われ、アクセス制御と機密保持を中心課題としているが、無線ネットワークの中心機能はアベイラビリティにある。モバイルイーサネットの無線部分に生じるセキュリティの脅威について、我々はイーサネットフレームが空中を飛ぶことの公開性に原因があると考えている。電波中のコンテンツは確実な暗号によって保護されるが、ヘッダを含むコンテキストは空中においてオープンである。悪意ある者がモバイル端末の MAC アドレスを追跡すればこれを攻撃できる。そのため DoS 攻撃だけでなく、無線妨害、無線セッションの乗っ取り、無線でのフラッド攻撃を防止するためにもモバイル端末を追跡不能にすることが重要になる。

我々は可変 MAC アドレス方式（TMAC：Transient MAC Address）という方式を提唱している。これを用いればモバイル端末は MAC アドレスが動的に変更できるため、追跡を逃れることができる[29][30]。TMAC の更新は一方向の鍵付きハッシュ関数によって行われるため、MAC アドレスの変遷を記憶できるのは当のモバイル端末とそれがつながっている AP だけである。TMAC 鍵を持たない攻撃者は、現在の TMAC を基に次の TMAC を予測することができない。

5　まとめと今後の課題

本稿では、モバイルイーサネットのアーキテクチャと今後の方向性について 3GPP と IEEE 802 LMSC の観点から論じた。また、モバイルイーサネットのセキュリティについても取り上げた。はじめに、アプリケーションとネットワークの認証に対応できるセキュリティ方式について説明した。次に無線セキュリティの課題について触れた。一つは、無線システム間で機密を保持するための共通メカニズムを備えること。もう一つは、アベイラビリティを維持する機能を備えることである。

無線セキュリティの議論はまだ途上であり、今後のユビキタス無線ネットワークに向けてプライバシー課題に関する研究を進める必要がある。

6　謝辞

モバイルイーサネットの開発に際しては三菱電機株式会社の方々に大変お世話になった。また、次世代無線ネットワークの無線 DoS 攻撃に関して Wade Trappe 教授と有意義な意見交換を行うことができた。この場をお借りして感謝申し上げたい。

参考文献

1 H.Lach, C.Janneteau, and A.Petrescu, "Network Mobility in Beyond-3G Systems", IEEE Communication Magazine, pp.52-57, Jul. 2003.

2 H.Yumiba, K.Imai, and M.Yabusaki, "IP-Based IMT Network Platform", IEEE Personal Communication Magazine, Vol.8, No.5, pp.18-23, Oct. 2001.

3 T.Otsu, I,Okajima, N,Umeda, and Y.Yamao, "Network Architecture for Mobile Communication Systems Beyond IMT-2000", IEEE Personal Communication Magazine, Vol.8, No.5, pp.31-37, Oct. 2001.

4 http://www.3gpp.org/specs/specs.htm

5 http://www.ieee802.org/

6 http://www.ieee802.org/16/

7 http://www.ieee802.org/21/

8 H. Harada and R. Prasad, "Simulation and Software Radio for Mobile Communications", Artech House, 2002.

9 D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6", Internet-Draft, draft-ietf-mobileip-ipv6-24.txt, Jun. 2003.

10 R.Koodli, "Fast Handovers for Mobile IPv6", http://www.ietf.org/internet-drafts/draft-ietf-mobileip-fastmipv6-06.txt, Internet-Draft, Mar. 2003.

11 Hesham Soliman, Claude Castelluccia, Karim El-Malki, and Ludovic Bellier, "Hierarchical Mobile IPv6 mobility management (HMIPv6)", Internet-Draft, draft-ietf-mipshophmipv6-00.txt, Jun. 2003.

12 "Combined GSM and Mobile IP Mobility Handling in UMTS IP CN", 3GPP TR23.923 V3.0.0

13 "All-IP Network (AIPN) feasibility study", 3GPP TR22.978 V7.0.0

14 Compendium of Abstract, 3GPP TSG RAN Future Evolution Work Shop, 2-3 Nov. 2004, Toronto, Canada.

15 "Virtual Bridge Local Area Networks - Amendment 4: Provider Bridge", IEEE P802.1ad/D2.0 Dec. 2003.

16 M. Kuroda, M. Inoue, A. Okubo, T. Sakakura, K. Shimizu, and F. Adachi, "Scalable Mobile Ethernet and Fast Vertical Handover", IEEE Wireless Communications and Networking Conference (WCNC) 2004, Mar. 2004.

17 A. Okubo, M. Tsuzuki, Y. Hirano, K. Shimizu, and M. Kuroda, "Evaluation of Mobile Ethernet Switch on Network Processor", Workshop on High Performance Switching and Routing (HPSR) 2004, Mar. 2004.

18 M. Kuroda, K. Ishizu, Y. Saito, and G. Miyamoto, "Empirical Evaluation of Real-Time Vertical Handover for Beyond 3G Wireless Network", WPMC'05, Sep. 2005.

19 Z. Lan and M. Kuroda, "A Load Balancing Proposal for Beyond 3G Wireless Network", WPMC'05, Sep. 2005.

20 Y. Saito, K. Ishizu, M. Kuroda, and T. Mizuno, "A Study of Media Independent Paging Mechanism for Beyond 3G Wireless Network", WPMC'05, Sep. 2005.

21 K. Ishizu, Y. Saito, and M. Kuroda, "Design of Media Independent Handover Interface for Beyond3G Terminal", WPMC'05, Sep. 2005.

22 M. Kuroda, M. Yoshida, and R. Ono, "Double Stuff Security for the Beyond 3G Wireless Network", WPMC'03, Oct. 2003.

23 R. Nomura, M. Kuroda, and D. Inoue, "Location-based Key Management for Ubiquitous Wireless Network", WPMC'05, Sep. 2005.

24 M.Kuroda and R. Nomura, "Radio-independent Mobile Authentication Protocol for Ubiquitous Network", WPMC'05, Sep. 2005.

25 I. F. Akyildiz, J. S.M. Ho, and Y. Lin, "Movement-Based Location Update and Selective Paging for PCS networks", IEEE Personal Communication Magazine, Vol.8, No.5, pp.18-23, 2001.
26 J. Li, Y. Pan, and X. Jia, "Analysis of Dynamic Location Management for PCS Networks", IEEE Trans. on Vehicular Technology, Vol. 51, No. 5, pp.1109-1119, 2002.
27 Y. Lin, "Reducing Location Update Cost in a PCS Network", IEEE/ACM Trans. on Networking, 1997.
28 T. Aono, S. Tawara, T. Ohira, B. Komiyama, A. Kitaura, H. Mori, and H. Sasaoka., "Secret Common Key Generation Method Exploiting the Fluctuation of Communication Channels Using an Espar Antenna", Proc. of the 2004 IEICE General Conference, 2004.
29 D. Inoue, R. Nomura, and M. Kuroda, "Transient MAC Address Scheme for Untraceability and DoS Attack Resiliency on Wireless Network", WTS2004, Apr. 2004.
30 D. Inoue, M. Kuroda, and K.Ishizu, "FAST Transient MAC Address Scheme Based on Prearranged Update", WPMC'05, Sep. 2005.

宮本　剛（みやもと　ごう）
新世代ワイヤレス研究センターユビキタスモバイルグループ研究員（旧無線通信部門ワイヤレスアプリケーショングループ研究員）
無線通信

黒田正博（くろだ　まさひろ）
新世代ワイヤレス研究センターユビキタスモバイルグループ主任研究員（旧無線通信部門ワイヤレスアプリケーショングループリーダー）　工学博士
ユビキタスモバイルネットワークとその無線セキュリティ