

**SIS** (Secure IP Solution)・**MIP** (Mobile IP Solution)  
についての技術解説

2004年12月

ルート株式会社

## 目次

1. Secure IP Solution の目的
2. Mobile IP Solution の目的
3. SIS のもたらすユビキタス
  - ・ 認証手続き不要の無線 LAN アクセス
  - ・ 再接続作業不要の「移動透過性」
  - ・ 優れた拡張性
4. MIP のもたらすユビキタス
  - ・ 高速移動体からの継続した IP 通信を実現する「高速ハンドオーバー」技術
  - ・ 利用制限のない幅広い応用可能性
  - ・ 優れた通信エリア拡張性
5. SIS・MIP のもたらすセキュア環境
  - ・ LAN 通信のセキュリティを多角的・総合的に向上
  - ・ SIS・MIP のもたらす技術的セキュリティ要素
    - 1) SIS・MIP の通信の機密性(Confidentiality)
    - 2) SIS・MIP の通信の完全性(Integrity)
    - 3) SIS・MIP の通信の可用性(Availability)
  - ・ SIS・MIP のもたらす社会的セキュリティ要素
    - 4) SIS・MIP における責任追跡性 (Accountability)の確保
    - 5) SIS・MIP における真正性 (Authenticity)の確保
    - 6) SIS・MIP における信頼性(Reliability)の確保
6. 関連技術
  - ・ SIS・MIP を構成する技術
  - ・ 無線 IP 通信のセキュリティに関連する技術
  - ・ SIS・MIP の導入と無線 LAN のセキュリティ技術の関連

### 【参考資料】

## 1 . Secure IP Solution の目的

Secure IP Solution (SIS)は、LAN を用いたビジネス IT 環境のコビキタスとセキュリティを同時に実現するトータルシステムです。

SIS は、LAN を用いた組織の IT システム、特に複数拠点を持つ組織について、優れた通信作業性をもたらし、かつ同時にバックグラウンドでの堅牢な通信セキュリティを確保します。LAN を利用するエンドユーザは LAN へのアクセスに関する煩わしい一切の作業から開放され、一方で意識することなく情報通信の高度なセキュリティ保護を受けます。

## 2 . Mobile IP Solution の目的

Mobile IP Solution (MIP)は、高速移動体からの容易な IP 通信というコビキタス環境とセキュリティを同時に実現するトータルシステムです。

MIP は、車両などの移動体と地上とを IP ネットワークとして接続するためのシステムです。移動体上で用いる PC などの端末には特別なハードウェアもソフトウェアも導入する必要はなく、使用するアプリケーションなどにも何の制限もありません。300Km/h に近い高速移動中の車両から、接続する地上無線局を自動的かつスムーズに切り替えながら IP 接続を継続することができます。移動体からの接続対象である地上無線局群が複数のネットワークにまたがっていても、無線局の接続切り替え特性は全く変化しないことから、移動体が広域を移動する場合に対しても適用できます。このような高い利便性を持ちながら、同時に高度なセキュリティ対策を施しており、公道などでの使用で懸念される盗聴などのセキュリティ侵害を完全に防いでいます。

## 3 . SIS のもたらすコビキタス

SIS を用いた LAN を利用しようとするエンドユーザは、煩わしい一切の作業なく、いつでもどこでも LAN に接続できるようになります。

### 認証手続き不要の無線 LAN アクセス

SIS によって無線 LAN 環境が構成され、エンドユーザはその無線 LAN にどこからでもアクセスすることができます。この無線 LAN 環境は高度なアクセス保護が施されているにもかかわらず、エンドユーザはアクセスするたびに認証手続きなどの煩わしさは一切ありません。

エンドユーザは SIS 管理者がユーザ毎に発行する「プロファイル」と呼ばれるファイルをパソコンに保存・登録します。プロファイルの登録されたパソコンは、パスワード入力

などの煩わしい認証手続きをユーザが行うことなく LAN に接続できます。プロファイルを USB フラッシュメモリなどのリムーバブルメディアに入れて持ち運べば、そのメディアを LAN 接続のための「鍵」(トークン)として使用することができ、パソコンを無断借用しての LAN やインターネットへの不正接続などを防止できます。

#### **再接続作業不要の「移動透過性」**

パソコン(端末)をどこへ持っていても再接続することなしに LAN へ接続できます。パソコンの移動によって、接続する無線あるいは有線の接続基地局(アクセスポイント)が変更されても、ユーザはそのことを全く意識する必要がありません。

接続する基地局が変更になると、通常システムでは、再認証手続きが必要になったり、パソコンの IP アドレスが変更されて通信相手との通信が途切れたりします。接続ポイントを変更しても通信が途切れないという特性「移動透過性」を、接続ポイントによらず送信相手からは同じ IP アドレスとして認識されるようにすることによって実現する技術は「Mobile IP」と呼ばれ、その仕様は RFC2002 で規定されています。SIS では、この RFC2002 を満たすよう定められた、モバイルブロードバンド協会(MBA)標準「MIS モバイル IP 仕様書」を実装し、優れた移動透過性を実現しています。

この移動透過性によって、部屋やフロア、あるいは建物間を移動しながら、インターネットから途切れることなくファイルをダウンロードしたり、VoIP 技術を用いた音声通話、動画転送を行ったりすることができます。例え拠点間を移動してもインターネットから見た IP アドレスが変化しないことから、IP アドレスによるアクセス制限に対応でき、あるいは持ち運びを行うノートパソコンでサーバを(無線が届かない所を通過する場合は断続的に)運用することさえも可能にします。

#### **優れた拡張性**

パソコンと基地局との通信方式に MIS プロトコルを用いています。この MIS プロトコルは、MBA 標準として採用されているオープンな通信仕様であるため、同じ通信仕様を採用している他組織の様々なネットワークシステムとの相互接続展開が可能となっています。

ローミング機能を有するため、パソコンを他組織の SIS ネットワークに接続することも容易であり、その際エンドユーザ自身は接続のための面倒な認証手続きを行ったり、設定を変更したりすることなく、自分のデスクにいる時と全く同じように自組織 LAN やインターネットを使用できます。

#### 4 . MIP のもたらすユビキタス

MIP を用いた移動体通信システムを利用するエンドユーザは、移動する車両内からも、地上のデスクトップ環境と同様な継続的で安定・広帯域な IP 通信を行うことができるようになります。

##### 高速移動体からの継続した IP 通信を実現する「高速ハンドオーバー」技術

高速で移動する車両内でパソコン（端末）からインターネットなどへの IP 通信網へ接続できます。時速 300Km/h にもなる高速移動中でも、通信を途切れさせることなく接続先の無線基地局を切り替える「高速ハンドオーバー」が実現されています。

しかもこの高速ハンドオーバーは、Mobile IP による移動透過性を実装した上で実現されていることから、端末とその通信相手の間の通信において、基地局を変更したことに伴う端末の IP アドレス変化などの影響が全くありません。MIP における Mobile IP は、SIS と同様 RFC2002 を満たすよう定められた、モバイルブロードバンド協会（MBA）標準「MIS モバイル IP 仕様書」を実装しています。

Mobile IP 特性を確保した上での優れたハンドオーバーの高速性によって、高速移動中の車両からでも安定した IP 通信を可能にしています。また高速ハンドオーバーによって接続させる無線基地局を複数のネットワークにわたって配置させることができるため、単一ネットワークに接続する端末の集中による情報の輻輳を回避することができ、多数の端末を収容しての広帯域通信を可能にしています。

##### 利用制限のない幅広い応用可能性

高速移動体内で用いる端末には特殊なハードウェアやソフトウェアは全く不要です。端末の通常の LAN 接続機能によって移動体内に設置されたモバイルルータに接続すれば、移動していることを全く意識することなく通常の IP 接続が可能となります。また利用するアプリケーションについても全く制限がありません。このことから、移動車両からの動画配信、車両の内外間での VoIP 技術を用いた音声通話、車内でのストリーミング放送の受信、高速移動物体の制御や移動体からの測定データ送信など、幅広い応用が可能となります。

また、MIP でサポートしている無線カードを Windows 98SE/Me/2000/XP において使用する場合には、端末から、モバイルルータを介さずに直接無線基地局と通信し、高速ハンドオーバーさせながら IP 通信することも可能です。

##### 優れた通信エリア拡張性

複数のネットワークにまたがって無線基地局を配置できるため、広域にわたる無線基地

局の通信エリアを確保できます。また無線基地局へ接続する IP ネットワーク網を選ばないため、容易に通信エリアを拡張できます。

無線基地局の通信エリア拡張の際、新規無線基地局の設置場所と既存 IP ネットワークとの間を直接接続できない場合でも、多段中継が可能な中継専用の無線ルータを間に配置することによって容易に無線基地局と既存 IP ネットワークを結ぶことができるため、場所を選ばず無線基地局を増設することができます。

## 5 . SIS・MIP のもたらすセキュア環境

### LAN 通信のセキュリティを多面的・総合的に向上

SIS・MIP は LAN 通信に関して、IT のセキュリティ 6 要素である機密性、完全性、可用性、責任追跡性、真正性、信頼性の全てを確保することができます。これらのセキュリティ要素は、一般的には互いに相反しトレードオフの関係になりますが、SIS・MIP はこれら全ての要素を向上させるトータルセキュリティシステムです。

### SIS・MIP のもたらす技術的セキュリティ要素

ISMS、ISO17799、BS 7799-2:2002 では、IT セキュリティの要素として CIA：機密性 (Confidentiality)、完全性(Integrity)、可用性(Availability)の 3 つを取り上げており、これらは IT セキュリティを評価する上での技術的要素として常に重視されます。

#### 1) SIS・MIP の通信の機密性(Confidentiality)

機密性とは、「アクセスを認可された (authorized) 者だけが情報にアクセスできることを確実にすること」です。言い換えれば、情報を漏洩や不正アクセスから保護するということです。端末と基地局の間での通信には MIS プロトコルによる堅牢な暗号化を施しており、暗号通信や暗号の鍵情報の漏洩を防いでいます。特に、不正な無線基地局を用いた盗聴を防いでいる点で、他の無線 LAN 通信のセキュリティ方式とは一線を画すセキュアレベルが保証されています。

#### 2) SIS・MIP の通信の完全性(Integrity)

完全性とは、「情報及び処理方法が、正確であること及び完全であることを保護すること」です。言い換えれば、情報の改ざんや間違いから保護するということです。SISでは端末と基地局とのデータ通信にAES-CBCないしはHMAC-MD5による署名を用いてパケットごとの完全性チェックを行っているため、通信内容の改ざん、誤りの危険性が排除され、データ完全性が保証されています。

#### 3) SIS・MIP の通信の可用性(Availability)

可用性とは、「認可された利用者が、必要なときに、情報及び関連する資産にアクセスで

きることを確実にすること」です。言い換えれば、情報の紛失・破損やシステムの停止などから保護するということです。

通信システムにおいて最も重要な可用性とは、通信可能時間に他なりません。LAN などの IP 通信システムにおいて通信可能時間が損なわれる要因には、通信切断、配線作業、(再)接続作業、認証手続きなどがあります。SIS・MIP においては最初のシステム設定さえ行われれば、後は(ハードウェア上の問題を除いて)システム停止をさせることなく、いつでもどこでも接続作業、認証手続きなしに LAN などの IP 通信網へ接続でき、常に安定した継続的な IP 通信環境が得られます。

また、無線基地局や認証サーバを複数用いた場合、これらの機器のいずれかに障害が発生しても、端末の通信が途絶えることなく自動的に使用機器が切り替えられ、通信を続けることができます。

#### **SIS・MIP のもたらす社会的セキュリティ要素**

GMITS (Guidelines for the Management for IT Security : ISO/IEC TR 13335) においては、IT セキュリティに必要な要素として機密性、完全性、可用性の他に責任追跡性 (Accountability)、真正性 (Authenticity)、信頼性 (Reliability) を定義しており、これらはセキュリティの社会的要素と呼ばれています。

#### **4) SIS・MIP における責任追跡性 (Accountability) の確保**

責任追及性とは、責任をとるべき本人を明確にすることです。作業を行っているものが誰であるか明らかにすることができるようにして、問題が発生した場合などには、その責任を追求できるようにすることです。

SIS・MIP において、エンドユーザの全ての通信について認証サーバやホームエージェントサーバで認証が行なわれるため、これらのサーバで適切な認証ログを残すことが可能です。これによって自ネットワークの通信に関する責任追跡性を SIS / MIP 管理者が確保することができます。

#### **5) SIS・MIP における真正性 (Authenticity) の確保**

真正性とは、本人性を確保することです。情報の入力者が間違いなく本人であり、成りすましや情報の改ざんなどがなされていないことを保証することです。

通信システムにおける真正性は I&A (Identification and Authentication : 本人性確認と認証) に依存することになります。

SIS では本人性確認の仕組みとして、「プロファイル」と呼ぶ、SIS 管理者がユーザに発行する特定のファイルを用います。このファイルがユーザに適切に管理されている限り、真正性は保証されます。プロファイルは USB メモリやコンパクトフラッシュなどのリムーバブルメディアに保存し、そのメディアを物理的な「鍵」のように用いるトークンシステムとして管理運用すれば、堅牢な I&A システムとなります。

SIS・MIP において、通信相手との接続に認証手続きや暗号通信を要する真正性の確保が必要な重要なサービスを利用する際、通信途中で接続する無線基地局の切り替えがあっても真正性は継続的に確保されます。通信相手から見て移動体内の端末は継続的に同一の IP アドレスとして認識されるため、再認証手続きが必要になったり、暗号通信が継続できなくなったりする問題は一切発生せず、一方で別人がそのサービスへの接続を乗っ取ることは全く不可能です。

さらに、SIS・MIP では端末（ユーザ）の認証だけでなく、基地局の認証が行われており、偽基地局によるデータ改ざんから起こる真正性の破れを防いでいます。

## 6) SIS・MIP における信頼性(Reliability)の確保

信頼性とは、矛盾のない計画どおりの動作および結果を確保する特性を言います。SIS・MIP はその通信に際してあらゆる不正接続、成りすましを防いでおり、さらにパケット毎の署名確認を行うことによって想定外の通信が行われるあらゆる可能性が排除されています。また、基地局、認証局の冗長化によって、機器障害に起因する通信障害を回避することができます。

## 6 . 関連技術

### SIS・MIP を構成する技術

#### Mobile IP :

Mobile IP とは、IP によるルーティング制御において、ノードが移動した場合にも、接続前と同じ IP アドレスを用いたままルーティング制御するための解決方法です。

パソコンをネットワークの別の場所に接続しなおすと、通常はそのパソコンに割り当てられる IP アドレスが変化してしまうために、

- 1 . 継続中だった通信が途絶えてしまう
- 2 . 他者から見つけてもらえなくなる
- 3 . IP アドレスによる管理（ファイヤーウォールやアクセス制御）が混乱する
- 4 . 暗号通信の鍵が失われてしまい、暗号通信が継続できなくなる

という問題が起こってしまいます。そこで Mobile IP の目的として設定されているのが、別

の場所に移動してネットワークに接続しなおしても以前と同じ IP アドレスで、同じネットワーク環境が継続されるようにすることだと言えます。

Mobile IP の議論は 1997 年頃から始まり、2001 年頃から本格的な議論がなされていて、その基本的な内容は RFC2002 で規定されました（現在は RFC3344）。また、Mobile IP を実現する際に必要となるトンネル通信技術については RFC2003 で規定されています。モバイルブロードバンド協会(MBA)がこの RFC2002 と RFC2003 を包含した標準仕様を「MIS モバイル IP 仕様書」として公開しています。

また IETF Routing AREA の IP Routing for Wireless/Mobile Hosts でさまざまな議論がなされています。Mobile IP は、無線 IP 通信でのネットワーク接続だけを対象とした技術だけではありませんが、IETF でのワーキンググループ名が示すように、その実装として想定されているのは実質上無線 IP 通信を用いたネットワーク接続です。

ここで注意しなければならないのは、RFC や Internet Draft において、Mobile IP の機能を実現するのに足る取り決めについては提案がなされてはいますが、実際に Mobile IP を実現して運用した時に起こりうる脆弱性についてのセキュリティ対策などについては、これら RFC や Internet Draft は何ら規定されないということです。

SIS・MIP は、Mobile IP を実装するにあたり、無線 IP 通信に関して最善のセキュリティを備えた MIS プロトコルを採用しています。SIS・MIP は、単なる Mobile IP ソリューションではなく、どんな場合も安全に使えることを大前提とする Mobile IP ソリューションなのです。

#### **MIS プロトコル：**

無線 IP 通信を用いた LAN 環境は、いつでもどこでも簡単に LAN へ接続できる便利さから急速に利用されるようになってきましたが、一方で、平文でやりとりされる無線通信の盗聴、無線通信の基本的な暗号化手法である WEP の脆弱性などから、セキュリティ面からは大変危険な環境でした。

無線 IP 通信の危険性を防ぐ手法として、SSID や MAC アドレスフィルタなどが用いられてきましたが、泥縄式の感を否めず、設定の苦勞の割にさほどセキュアレベルは上がらない状況が続いてきました。最近ようやく、IEEE802.1x による認証や、TKIP による暗号化、これら二つの技術を合わせた IEEE802.11i など新しい無線 LAN のセキュリティ技術が一部の一般向け製品にも搭載されるようになってきましたが、これら技術においても偽基地局による盗聴やデータ改ざんの可能性などのセキュリティ問題が未だ残っています。

MIS プロトコルは IEEE802.1x が今なおかかえるセキュリティ問題をいち早く克服した、安全性に優れた無線 IP 接続の認証、無線通信の暗号化技術を含んだプロトコルです。MIS プロトコルを用いた SIS による無線 LAN 環境では、どこで LAN 接続しても、いつも自分のデスクと同じネット環境が実現される移動透過性を有しながら、他に類を見ないセキュアな無線 IP 通信環境が得られます。

そして MIS プロトコルについて特筆すべきことは、このプロトコルがモバイルブロードバンド協会(MBA)が定めた標準プロトコルとして採用されているということです。オープンな通信仕様である MIS プロトコルが普及することによって、今後様々な無線 IP 通信網との相互接続が期待されます。

### 無線 IP 通信のセキュリティに関連する技術

#### Service Set Identifier (SSID) :

SSID は、無線 LAN システムにおける、クライアント機器の無線基地局への接続についてのアクセス制御技術の 1 手法です。無線基地局からは定期的に SSID を含んだビーコンというパケットを発信しています。SSID について認証機能という説明がなされることも多いですが、実質的にはその役割を果たしておらず、クライアント側でこの SSID を自らのパケットに設定する機能を有していれば、SSID をあらかじめ知らなくても基地局に接続することができます。また悪意ある基地局が SSID を詐称してクライアントからの誤接続を誘導する危険性があります。また、SSID 自体は特に無線通信の暗号化と関係がありません。

現在市販されている無線 LAN 用機器とそれらの付属ソフトウェアはほとんど SSID に対応しています。

#### MAC アドレスフィルタ :

MAC アドレスフィルタは、無線 LAN システムにおける、クライアント機器の無線基地局への接続についてのアクセス制御技術の 1 手法です。無線基地局で、接続を許可する無線機器を MAC アドレスによって区別するフィルタリング方式です。クライアントが MAC アドレスを詐称して不正に接続してくることを防ぐことはできません。

クライアント側では設定等一切不要です。

#### Authentication Gateway :

Authentication Gateway は、無線 LAN システムにおける、クライアント機器の無線基地局への接続についてのアクセス制御技術の 1 手法です。

その基本的な原理は、ユーザが無線などによって LAN に接続し、その LAN を介してインターネットと通信するためには、認証ゲートウェイサーバによる認証を継続的に受け続ける必要があり、認証を受け続けられない限り、該当 LAN を介しての WAN (インターネット) への接続をさせないというものです。認証時にインターネット使用について許可するプロトコルは、認証ゲートウェイでのファイヤーウォールルールで適宜制御可能です。この Authentication Gateway という技術によって、該当 LAN を発信元とする不正アクセスなどについての責任追跡性を確保することができます。

認証時に SSH を用いて、認証サーバのホスト認証などを使えば、認証サーバの詐称を防ぐこともできます。

Authentication Gateway は、基本的に接続対象となる LAN (とその運用組織) を保護するための技術であり、接続するユーザや、ユーザが行う通信内容を保護する技術ではありません。そのため、LAN に接続したユーザの通信の機密性を保護するための通信暗号化は、Authentication Gateway の目的自体には要請されていないことには注意する必要があります。

Authentication Gateway において、ユーザ側は SSH クライアントなどの継続的な認証を行う特定のアプリケーションを導入するだけで利用可能となり、プラットフォームや機器の制約は小さいです。

なお、Authentication Gateway という用語は、元は Linux における特定のツールを用いた運用方法を指したようですが、上記の基本原理は無線 LAN のセキュリティにおいて重要な概念となるので、本解説書においては、Authentication Gateway という用語を、上記基本原理に基づくセキュリティ手法全てを指すものとします。

参照：「Authentication Gateway HOWTO」

<http://www.linux.or.jp/JF/JFdocs/Authentication-Gateway-HOWTO/index.html>

#### **IEEE802.1x :**

IEEE802.1x は、無線 LAN システムにおける、クライアント機器の無線基地局への接続についてのアクセス制御技術の 1 手法です。IEEE 802.1x では、Authentication Server というユーザ情報を管理し認証を行うサーバが用いられ、無線基地局はユーザから無線 LAN 経由でアクセスがあった場合には Authentication Server での認証を経て後に有線 LAN への中継を行うようにします。

無線 LAN 接続に関して LAN を保護する機構として、Authentication Gateway とよく似たセキュリティポリシーに基づいています。Authentication Gateway との違いは、Authentication Gateway が利用許可する資源がインターネットへの接続であることに対し、IEEE802.1x は有線 LAN であることと、Authentication Gateway がネットワーク層レベルの認証であることに対し、IEEE802.1x がデータリンク層レベルの認証であることです。IEEE802.1x では EAP 認証と呼ばれる認証方式が用いられていますが、EAP 認証には EAP-MD5, Cisco-EAP, EAP-SKE, EAP-SRP などのパスワード交換方式、EAP-TLS, EAP-TTLS, PEAP, EAP-MAKE などの公開鍵暗号方式のものなどがあります。

IEEE802.1x において、ユーザがアクセスポイントにアクセスしようとする時に、ユーザの真正性は認証によって保証されますが、ユーザからみてアクセスポイントの真正性は保証されません。また、データの完全性も保証されません。従って、アクセスポイントの成りすましによってユーザの通信が悪意あるアクセスポイントによって盗聴されたり、改ざんを受けたりすることがあり得ます。従って、IEEE802.1x も、Authentication Gateway と同様の性格を持ち、接続対象となる LAN (とその運用組織) は保護しますが、接続するユーザや、ユーザが行う通信内容の保護する技術としては十分強固ではありません。

EAP データが、アクセスポイントと認証サーバ間でやりとりされる間は、ネットワーク層レベルでデータがやりとりされますが、EAP データは機密性、完全性に欠けていることから、ここから通信遮断などを狙った DoS 攻撃を受ける危険性があります。

クライアント側が IEEE802.1x を使えるかどうかは、クライアント側の OS や使用している無線機器が該当の EAP を使えるかどうか依存します。EAP-TLS (RFC 2716) や EAP-TTLS は、Windows 95/98/ME/NT/2000/XP、Mac OS X、Linux で使用可能です。その他多くの EAP は使用する無線カードのサポート状況に依存します。また、大規模ネットワークでは IEEE802.1x を用いた環境を安定運用させるのが難しいことなども報告されています。

参考： <http://www.isalliance.org/knowledgebase2/80211/Content/TLS-based%20Method%20Comparison.htm>  
<http://www.atmarkit.co.jp/fnetwork/tokusyuu/19wlan/02.html>

#### **Wired Equivalent Privacy (WEP) :**

WEP は無線 LAN システムにおいて広汎に用いられている暗号化技術です。RC4 アルゴリズムをベースにした秘密鍵暗号方式で、IEEE によって標準化されており、IEEE 802.11 に対するセキュリティシステムとして採用されました。直訳すれば「有線と同等のプライバシー」という用語ですが、同じ鍵で通信を続けていると傍受された通信内容が解読可能

であり、通信内容の改ざんもできるという脆弱性が既に明らかとなっており、この脆弱性を回避するためには、頻繁に使用する鍵を変更しなければなりません。

#### **Temporal Key Integrity Protocol (TKIP):**

TKIP は WEP の脆弱性をなくした新しい無線通信の暗号化技術です。暗号鍵をクライアントの MAC アドレスを用いて生成し、それを頻繁に変更する仕組みを採用して暗号解読を防ぎ、また MIC (Message Integrity Code) と呼ばれるメッセージの完全性を保証する機構によって通信内容の改ざんを防いでいます。

#### **IEEE802.11i:**

IEEE802.11i は、IEEE802.1x の認証と TKIP あるいは AES による暗号化を合わせた、新しい無線 LAN の暗号通信である Wi-Fi Protected Access (WPA)を含んだ新しい標準仕様です。

#### **SIS・MIP の導入と無線 LAN のセキュリティ技術の関連**

SIS・MIP で用いられている MIS プロトコルの認証と無線通信の暗号化によって確保しようとするセキュリティは、基本的には IEEE802.1x/EAP の認証と TKIP による暗号化技術と同じです。しかし、MIS プロトコルは IEEE802.1x が未だ残しているセキュリティ上の課題を既に克服しています。さらに、一方多くの EAP 方式に見られるような無線カード毎のサポートではなく、OS 毎のサポートであり、クライアントの OS として Windows 98SE/ME/2000/XP, Mac OS X, Windows CE.NET 4.1(DT5100), Pocket PC 2003 がサポートされているため、SIS・MIP の導入によってクライアントユーザが受ける制約は非常に小さくなっています。

また SIS・MIP は無線 LAN システム全体をトータルにサポートするソリューションなので、IEEE802.1x のように導入後システムが安定しないという心配はありません。

以上

#### **【参考資料】**

MBA 標準仕様 :

MBA 標準 0201 号「MIS プロトコル仕様書」<http://www.mbassoc.org/j-services/mbas0201.pdf>

MBA 標準 0202 号「MIS モバイル IP 仕様書」<http://www.mbassoc.org/j-services/mbas0202.txt>

RFC :

Applicability Statement for IP Mobility Support (RFC 2005)

Copyright©2004 ROOT Inc. All rights reserved.

**Minimal Encapsulation within IP (RFC 2004)**

**IP Encapsulation within IP (RFC 2003)**

**The Definitions of Managed Objects for IP Mobility Support using SMIv2 (RFC 2006)**

**Sun's SKIP Firewall Traversal for Mobile IP (RFC 2356)**

**Mobile IP Network Access Identifier Extension for IPv4 (RFC 2794)**

**Mobile IP Authentication, Authorization, and Accounting Requirements (RFC 2977)**

**Mobile IP Challenge/Response Extensions (RFC 3012)**

**Reverse Tunneling for Mobile IP, revised (RFC 3024)**

**Mobile IP Vendor/Organization-Specific Extensions (RFC 3115)**

**IP Mobility Support for IPv4, revised (RFC 3220)**

**IP Mobility Support for IPv4 (RFC 3344)**

**Mobile IP Traversal of Network Address Translation (NAT) Devices (RFC 3519)**

**Registration Revocation in Mobile IPv4 (RFC 3543)**

**IETF :**

**IP Routing for Wireless/Mobile Hosts (mobile ip)**

<http://www.ietf.org/html.charters/mobileip-charter.html>