〈製品/ハードウェア〉

モバイルIPシステム「UNIVERGE MBシリーズ」

Mobile IP System “ UNIVERGE MB Series ”

吉井浩明* 本吉 彦* 田崎裕美* 西村啓之*
Hiroaki Yoshii Gen Motoyoshi Hiromi Tazaki Hiroyuki Nishimura

要 旨

UNIVERGEソリューションのなかで，IPsecによるセキュリティ機能とモバイルIPv4によるシームレス化サービスを同時に提供するUNIVERGE MBシリーズについてご紹介します。社内外を問わず，移動した場所でグループウェアや共有サーバを自席にいるかのように利用できます。

This paper describes UNIVERGE MB series among UNIVERGE solution, which can offer IPsec for security and mobile IPv4 for seamless handover at the same time. With UNIVERGE MB, you can use groupwares or shared servers from the outside and inside of corporate network in the same manner as you work at your own office desk.

1. まえがき

近年のインターネット社会の本格化に伴い，インターネット上の決済情報，取引情報や機密情報の漏洩を防ぐため，セキュリティ対策が重要になってきています。また，ユビキタスサービスの実現に向けて，企業網，公衆無線LANや3G携帯電話網などの異なるサービスのシームレスなハンドオーバの実現ニーズが高まっており，モバイルIPv4技術は，上位レイヤに依存しないモビリティ機能の提供，端末に対してIP着信が可能なためIP電話システムの実現には欠かせない技術として注目されています。

UNIVERGE MBシリーズは，セキュリティ対策としてIPsec機能，シームレスハンドオーバサービスとしてモバイルIPv4機能を同時に提供可能なシステムで，スウェーデンのipUnplugged社とのソフトウェアアライアンスによる協業により開発を実現しました。本稿にてUNIVERGE MBシリーズの詳細につき紹介します。

2. 概 要

UNIVERGE MBシリーズは現在，ハードウェアIPsecボードを搭載し，大規模ネットワークへの導入に適したMB1500，ならびにIPsec処理をソフトウェアで行い，かつユーザ同時接続数を低く制限することでコスト低減を図り，中小規模ネットワーク構成への導入を容易にしたMB1200の2シリーズを用意しています。表に諸元を示します。

3. 各装置・ソフトウェア機能

MBシリーズで使用する各装置およびソフトウェアの機能並びに動作概要を紹介します。

3.1 ローミングゲートウェイ

ローミングゲートウェイ装置は，モバイルIPにおけるホームエージェント機能およびフォーリンエージェント機能を実装しており，図1のように企業ネットワークに配置されることで，ローミングクライアントソフトウェアがインストールされた移動端末に対してホームエージェントとして動作し，モビリティを実現します。

移動端末側では，移動先ネットワークにフォーリンエージェントが存在する場合はフォーリンエージェント経由で気付アドレスを，ない場合はDHCPなどで自身が取得したIPアドレスを共存気付アドレスとしてホームエージェントに通知します（登録要求メッセージの送信）。ホームエージェント側ではこれを認証し，認証に成功した場合は移動端末に付与されたホームアドレスと呼ばれる固有のIPアドレスと気付アドレスの対応関係（モビリティ・バインディング）を記憶しておきます。

ホームエージェントは，移動端末のホームアドレス宛のトラヒックを代理受信してIPヘッダを付加（カプセル化）し，気付アドレス宛に送信することでトラヒックを移動端末に到達させます。また代理受信を実現するために，ホームエージェントは無償ARPメッセージをブロードキャストし，またホームアドレスへのARP要求に対してARP応答を行います（代理ARP）。またRFC3024で提示されている逆方向トンネリングをサポートしており，移動端末によってカプセル化された通信相手宛のパケットを受信してカプセル化を解除し，通信相手に転送します。

移動端末側の通信メディアはEthernet，無線LAN，ダ

* IPネットワーク事業部
IP Networks Division

表　MBシリーズ諸元
Table　Specifications of MB series.

	MB1500	MB1200
プロトコル機能	IPv4 (RFC791)，IP-IP Tunneling (RFC2003)	
モビリティ機能	Mobile IP HA/FA (RFC3344)，Reverse Tunneling (RFC3024) Mobile IP NATトラバーサル	
ファイアウォール機能	Ingress/Egressフィルタリング機能フルサポート，SRC/DSTポート番号， プロトコルによるフィルタリング，セッションステート管理機能	
NAT機能	NAT/NAPT (RFC3022)	
VPN機能	IPsecトランスポートモード/トンネルモードサポート， IKE (RFC2409)，IPsec (RFC2401～RFC2408)， DES (RFC1829) / 3DES (RFC1851)	
	IPsecハードウェア アクセラレータ搭載	–
同時接続数	100/200/500/1,000ユーザ	100/200ユーザ
処理能力	最大200Mbps	最大20Mbps
インタフェース	10BASE-T/100BASE-TX/ 1000BASE-T (RJ45) : 4ポート	10BASE-T/100BASE-TX (RJ45) : 3ポート

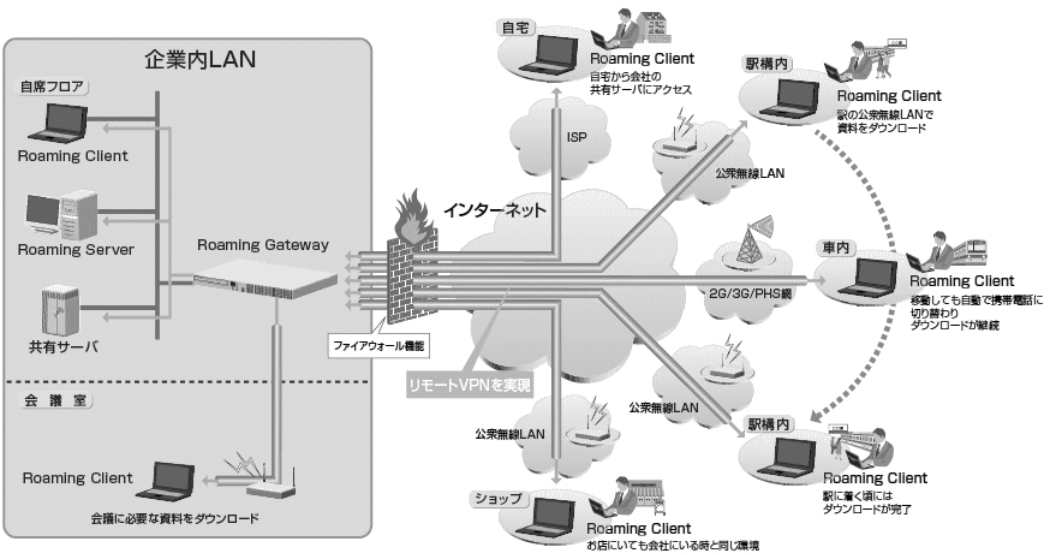

図1　MBシリーズ導入事例
Fig.1　Introduction case of MB series.

イヤルアップなど多岐にわたりますが，通信メディアや接続する無線LAN基地局が切り替わったことで気付アドレスが変更された場合，移動端末は新しく取得した気付アドレスをホームエージェントに通知し，ホームエージェント側ではモビリティ・バインディングを更新して更新後は新たな気付アドレスにトラヒックを送信します。気付アドレスが変更された場合でもホームアドレスは変更されないため，通信セッションは切断されません。

また，ローミングゲートウェイを企業内に導入してセキュアなリモートアクセス・ソリューションを実現するために，移動端末とホームエージェントとの間で送受信されるトラヒックをIPsec暗号化する機能を持っています。図2に，UNIVERGE MBでのリモートアクセス時の動作を示します。また，その他の代表的な機能を下記に示します。

(1) VLAN機能

IEEE802.1Qをサポートし，1つの物理インタフェース上に最大32個の仮想インタフェースを作成することが可能です。

(2) NATトラバーサル

RFC2003で規定された従来のカプセル化ではIP-IPトンネリングが使用されますが，このパケットは一般的なNAPTルータを通過できないため，移動端末がローカルアドレスを取得している環境ではモバイルIPが利用できなくなるという問題があります。UNIVERGE MBではUDPによるパケットトンネリングをサポートすることで，このような環境でのローミングを可能にしています。

3.2　ローミングクライアント

移動端末にモバイルIPクライアント機能を実装するため

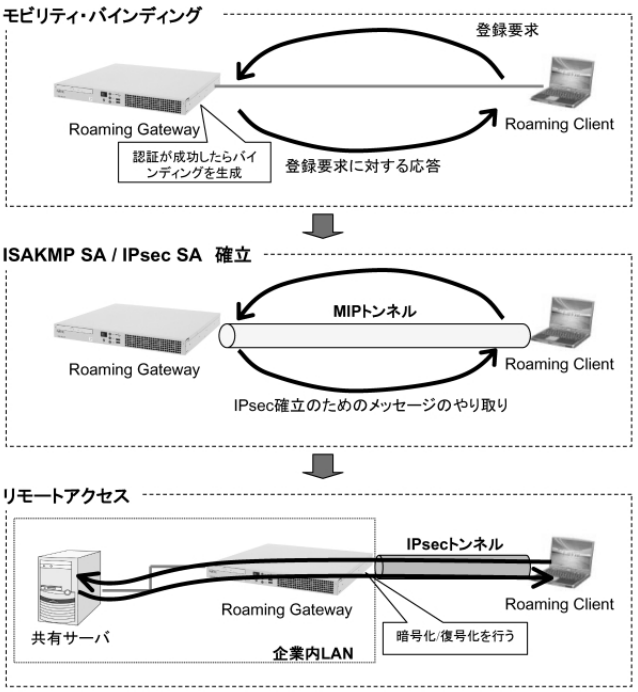

図2　リモートアクセス時の動作
Fig.2　Behavior in remote-access.

にインストールされるソフトウェアで，Windows版ソフトウェアを提供しています。代表的な機能を示します。

(1) モバイルIPによるシームレス通信

モバイルIPを利用することで，通信メディアの変更などに伴ってIPアドレスが変更された場合でもセッションが継続します。またこのシームレス通信の利便性を強化すべく，Ethernet・無線LANのリンクダウン・リンクアップ，もしくは無線LAN電波強度の閾値をトリガとする自動ダイヤルアップおよび自動切断機能を実装しています。またフォーリンエージェントやDHCPサーバの存在を検知して自動的に適切なモードで接続する機能を持ちますので，異なるネットワークに移動した場合に生じるWindows上でのネットワーク設定変更作業が不要になり，ユーザの利便性が向上します。

(2) 暗号化機能

前述のモバイルIP機能の他に，ローミングゲートウェイとの間でISAKMPを利用してIPsec接続を確立し，トラヒックを暗号化してそのパケットをモバイルIPプロトコルで送受信することで，企業内リソースへのインターネット側からのセキュアなアクセスを実現しています。またモバイルIP並びにISAKMPで利用する鍵情報などを後述するローミングサーバからプロファイルの形でダウンロードすることができ，設定の煩わしさを軽減する仕組みを備えています。また複数プロファイルの保有をサポートし，容易に切り替えることが可能です。その他，あらかじめ登録されたフォーリンエージェントやDHCPドメインをトリガとして，接続したネットワークによっては暗号化しない通信を行わせる機能を備えています。

3.3　ローミングサーバ

本製品付属のローミングサーバソフトウェア（Windows版，RedHat Linux版を提供）をインストールしたサーバをネットワークに導入することにより，ローミングゲートウェイの設定，管理ならびに移動端末用プロファイルの配布をGUIベースで行うことができます。また，1台のローミングサーバで複数台のローミングゲートウェイを管理することができるため，大規模ネットワークへの導入を容易にしています。その他の機能について下記に示します。

(1) RADIUS認証・課金機能

モバイルIP登録要求メッセージをホームエージェントが受信した際，メッセージの認証をローミングサーバに担当させることができます。またローミングゲートウェイには移動端末の接続時間や通信量をRADIUS課金プロトコルで送信する機能があり，ローミングサーバはこれらの受信をサポートしています。

(2) IAC（Internet Access Control）機能

UNIVERGE MBはモバイルIPとは独立した機能として，ローミングゲートウェイのファイアウォールルールをWeb認証によって動的に変更し，認証済みユーザについてローミングゲートウェイ経由でのアクセスを許可するというIAC機能を有しています。ローミングサーバは，このプロセスにおいてWebサーバ機能の提供およびローミングゲートウェイのファイアウォールの制御を行います。またユーザ認証に関して，ローカルデータベースによる認証と，外部RADIUSサーバによる認証をサポートしています。

この機能をモバイルIPと組み合わせることで（図3参照），モバイルIP登録要求が認証されたユーザのトラヒックをリダイレクトしてIAC認証画面をブラウザ上に表示させ，Web認証の完了後に社内ネットワークへのアクセスを許可する環境を構築することで，RADIUSをサポートする他の認証サーバとの連携を可能にしています。

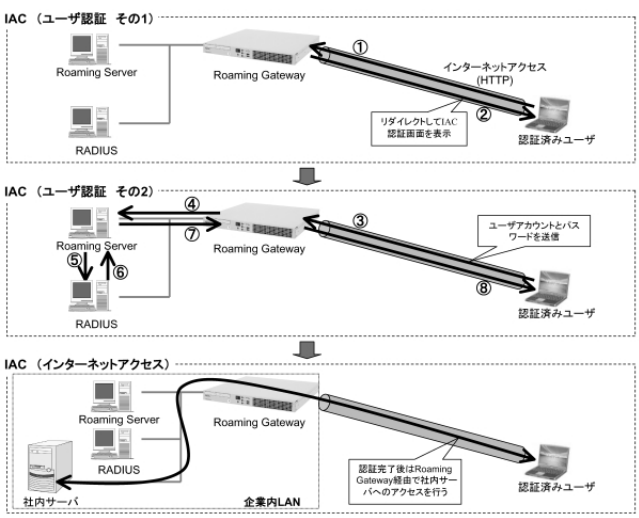

図3　モバイルIP-IAC連携時の動作
Fig.3　Behavior in cooperation between MIP and IAC.

4. むすび

以上UNIVERGE MBシリーズについて紹介しました。

UNIVERGE MBシリーズのモバイルIPv4技術をベースとしたシームレスローミングはユビキタスネットワークを構成する上で重要な技術であると考えており，今後もモバイルIP技術を中心にセキュリティ機能などをさらに充実させ，より充実したユビキタスサービスを提供できる製品として開発していく所存です。

＊ Ethernetは，XEROX社の商標です。

＊ Windowsは米国Microsoft Corporationの，米国およびその他の国における商標または登録商標です。

＊ RedHatは米国Red Hat software. Incの登録商標です。

＊ LinuxはLinus Torvaldsの，米国およびその他の国における商標または登録商標です。

筆者紹介

Hiroaki Yoshii

吉井　浩明　1987年，NEC入社。現在，ブロードバンドネットワーク事業本部IPネットワーク事業部マネージャー。

Gen Motoyoshi

本吉　彦　1995年，NEC入社。現在，ブロードバンドネットワーク事業本部IPネットワーク事業部主任。

Hiromi Tazaki

田崎　裕美　1991年，NEC入社。現在，ブロードバンドネットワーク事業本部IPネットワーク事業部勤務。

Hiroyuki Nishimura

西村　啓之　2002年，NEC入社。現在，ブロードバンドネットワーク事業本部IPネットワーク事業部勤務。