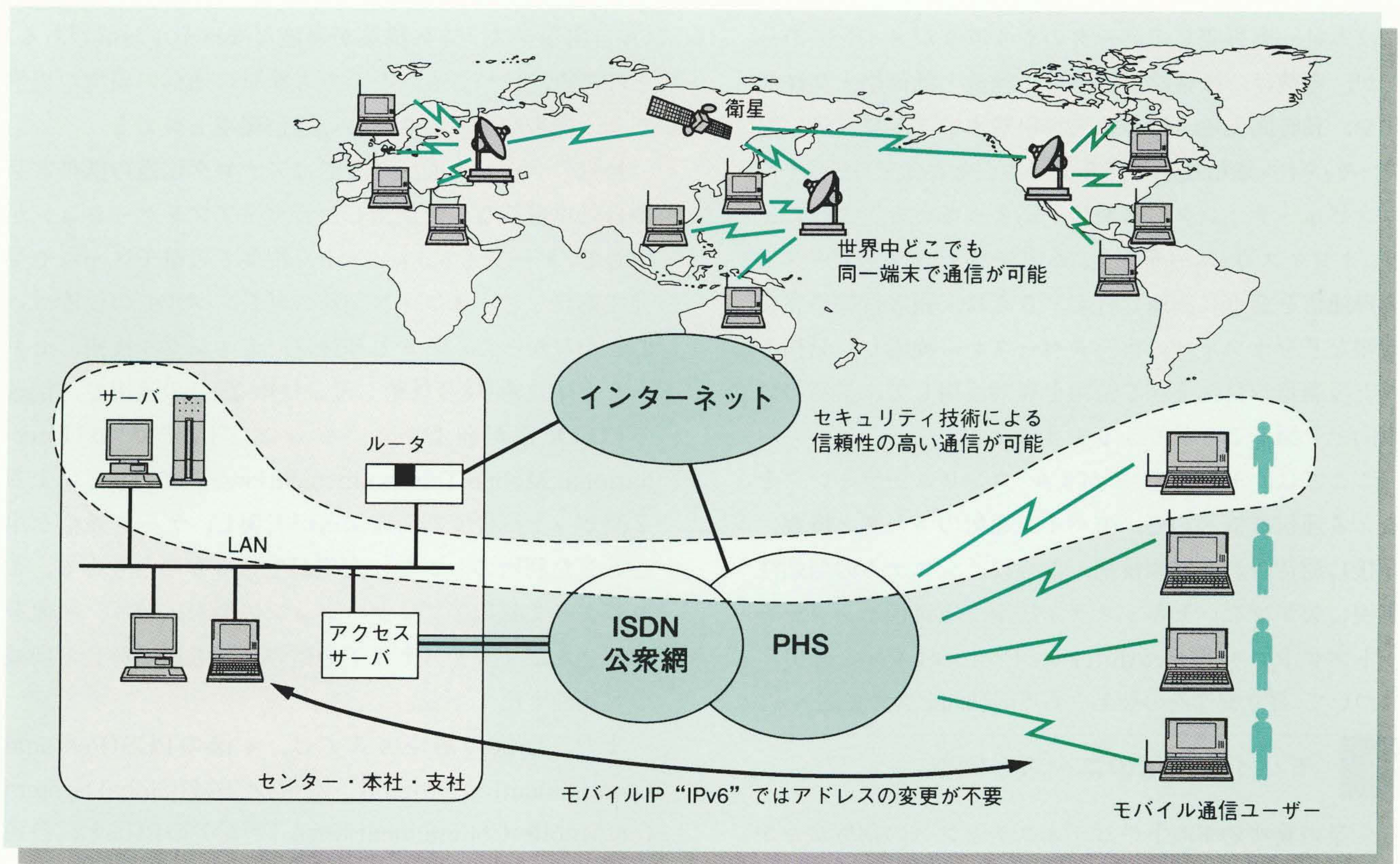


セキュア モバイル コンピューティングを支える通信基盤

Secure Communication Infrastructure for Mobile Computing

河野哲也 Tetsuya Kawano 安江利一 Toshikazu Yasue
松井 進 Susumu Matsui 金野千里 Chisato Konno



注：略語説明 ISDN (Integrated Services Digital Network), IP (Internet Protocol), PHS (Personal Handyphone System)

モバイル通信のイメージ

国内はもちろんのこと、海外を含めたグローバルなビジネス展開を推進し、業務のいっそうの効率向上を目指す企業では、今、正にセキュアモバイルコンピューティングが注目されている。

情報化社会の進展に伴い、情報システムもネットワークを中心とした業務の展開を見せている。ユーザーの要求は、従来のオフィス中心の業務から、さらにリモートでの業務にも広がってきている。例えば、(1)顧客情報や在庫情報を得るために、外出先からのデータベースへのアクセスを、(2)電子メール、状況報告などを行うために、自宅からのアクセスをそれぞれスピーディーに実現したいという要求がある。またその実現に向けて、小型・軽量・高性能な携帯端末の開発、携帯端末向けの基本ソフトウェアやアプリケーションソフトウェアの提供、さらにモバイル通信技術の確立が推進されており、ビジネス分野でモバイルコンピューティングがますます注目されてきている。

一方、モバイルコンピューティングを利用し、シームレスなコンピューティングシステム環境の構築を可能とするためには、モバイル環境でもオフィス内のLAN環境と遜色のない環境を構築する必要がある。そのためには、(1)伝送速度、(2)セキュリティ、(3)移動によるアドレス確保などの問題を解決しなければならない。

日立製作所は、このような問題を解決し、最適なセキュアモバイルコンピューティングの環境を提案するために、携帯端末などのハードウェアや、ソフトウェア製品はもとより、セキュアモバイルコンピューティングを支える通信基盤として、通信技術、セキュリティ技術も取り込んだシステムを開発していく。

1 はじめに

インターネットの急速な普及と、企業でのイントラネットの構築が、大企業だけでなく中小企業にまで展開されようとしている。このような中で、ビジネス形態も変わろうとしている。今までは、単に本社・支社内、さらには本社一支社間でのデータのやり取りがメインであったが、今後は、携帯端末の小型・軽量・低価格・高性能化や、長時間充電、携帯端末専用基本ソフトウェアの開発、モバイル通信技術の進歩により、セキュア モバイル コンピューティングへの期待が高まっている。これにより、オフィス外(ユーザー先、外出先など)でも、データ・音声通信を簡単に高速で行え、さらに、顧客情報や在庫情報などをオフィスのデータベースから検索し、見積もり支援業務や発注業務で情報を有効活用して、業務の効率向上を図ることができるようになる。

ここでは、セキュア モバイル コンピューティングを支える通信基盤として、モバイル通信のニーズと概要、今後に期待される無線技術、さらに、システムの信頼性実現に欠かせないセキュリティ技術、次世代インターネットプロトコル“IPv6(Internet Protocol Version 6)”について、日立製作所の製品や業界の動向を含めて述べる。

2 モバイル通信のニーズと概要

企業の業務効率向上やビジネスチャンスの期待がかかるモバイルコンピューティングと、これを支えるモバイル通信に対する企業ユーザーのニーズを図1に示す。

ネットワークの通信媒体は、有線と無線に大別できる。有線には、日本電信電話株式会社が提供している公衆網、ISDN(Integrated Services Digital Network)網、専用線

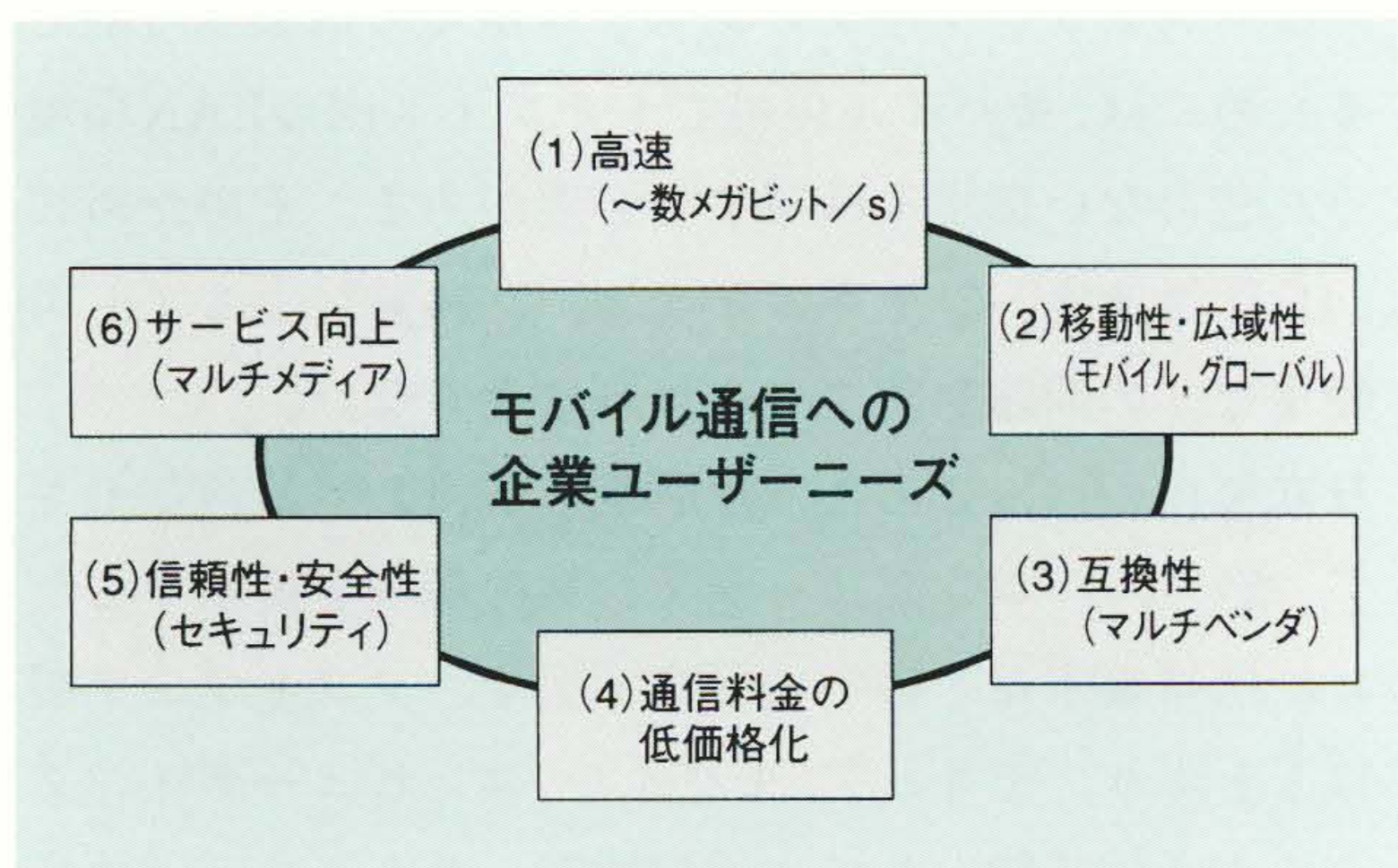


図1 モバイル通信に対する企業ユーザーのニーズ

モバイル通信に対する企業ユーザーのニーズは、主に六つのキーワードに要約できる。

などのサービスが含まれる。これらは、銅線と光ファイバケーブルを通信媒体としており、高速で、信頼性の高い通信サービスを提供している。反面、発信・着信ポイントが固定化されるため、携帯端末などを使用した移動業務には適していない。無線は、物理的にケーブルを使用しない通信サービスであり、通信配線には拘束されない、自由なシステムの構築が可能なモバイル通信である。そのため、いつでも、どこでも簡単に通信の環境が提供でき、携帯端末にふさわしい通信環境と言える。

無線のサービスも、今まではアナログ伝送の携帯電話や自動車電話などを使用した音声系アプリケーションが中心で、データも2.4 kビット/s程度での電子メールや受発注業務など、オフィス業務の延長レベルでの位置づけでしかなかった。しかし今後は、デジタル技術、セキュリティ技術(暗号技術、認証技術など)の適用で、伝送での信頼性が向上する。さらに、“IMT-2000(International Mobile Telecommunications-2000)”などによる2 Mビット/s程度の高速伝送が実現し、データ通信を中心とした利用のしかたに変化が生じるものと考ええる。これによって利用アプリケーションの幅が広がり、画像を取り込んだマルチメディア通信の実現と通信料金の削減の可能性も出てくる。

また、現状の無線方式では、米国のPCS(Personal Communication System)、欧州のGSM(Global System for Mobile Communications)、アジアのPHSと、各通信事業者、国・地域などの独自のサポートが展開されている。しかし現在、無線方式でも国際標準化が検討されており、近い将来地球上のどこでも同一の携帯端末で通信が可能となる。ITU(国際電気通信連合)で検討されている標準化方式として、「IMT-2000プロジェクト」が推進されている。これは、2000年をめどに低軌道周回衛星(LEO)を利用した衛星データ通信である。モバイルコンピューティングは、グローバルなビジネス展開としてもこれからますます期待できる。

日立製作所は、このような市場の動向をすばやくキャッチアップし、ユーザーのニーズにこたえたさまざまな製品と最適なソリューションサービスを提案していく考えである。

3 システム構築技術

モバイルコンピューティングを支える通信基盤である無線データ通信技術の現状と将来動向について以下に述べる。

表1 PDCシステムとPHSの仕様

データ通信速度ではPHSが、移動速度の限界ではPDCシステムがそれぞれ優れている。

項 目	PDCシステム	PHS
周波数帯	800 MHz/1.5 GHz	1.9 GHz
多重化方式	TDMA	
チャンネル帯域	14 kビット/s	32 kビット/s
セル半径	数キロメートル	数百メートル
出 力	800 mW	10 mW
移動速度の限界	約80 km/h	約20 km/h
データ通信速度	9.6 kビット/s	29.2 kビット/s

注：略語説明 TDMA(Time-Division Multiple Access；時分割多元接続)

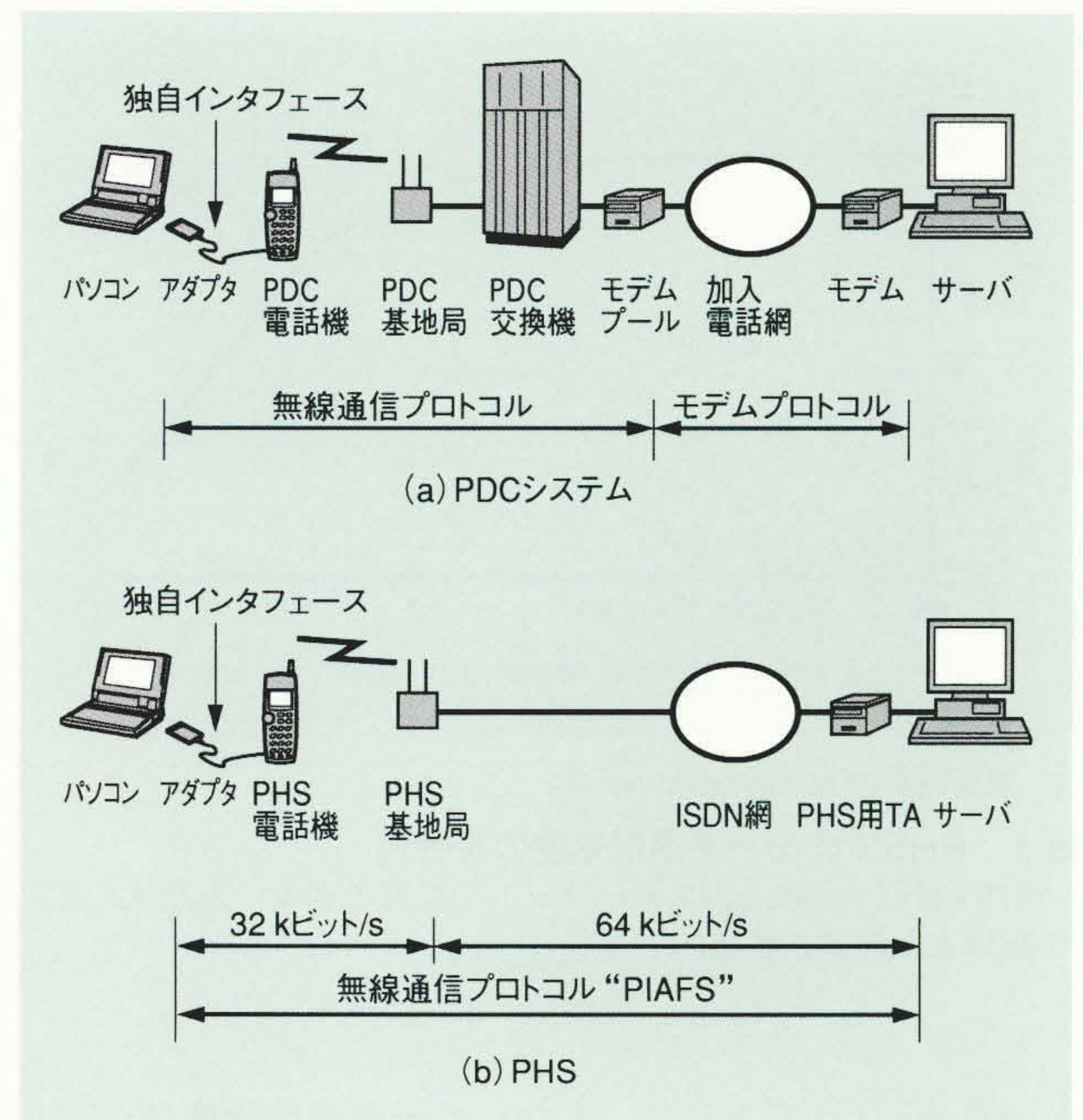
3.1 無線データ通信技術の現状

現在、全国規模で使用が可能な無線データ通信基盤としては、PDC(Personal Digital Cellular)システムとPHSがある。PDCシステムとPHSの仕様を表1に示す。

PDCシステムとPHSの大きな違いは、そのセル(一つの無線基地局がカバーする範囲)の大きさにある。PDCシステムでは、数キロメートルオーダ、PHSでは数百メートルオーダである。この違いが、PDCシステムとPHSとの使用可能時間や端末移動速度に影響している。PDCシステムではPHSに比べてセルが大きいので、無線基地局と通信するためには大きな電力が必要であり、同一のバッテリー容量では使用可能時間が短くなる。また、端末がセル範囲を越えて移動する場合、その切換(ハンドオーバー)には処理オーバーヘッドがかかり、通信は瞬断を起こす。PHSではPDCシステムに比べてセルが小さいため、同一速度で移動した場合、セルの切換が頻繁に起き、処理オーバーヘッドが大きくなって通信ができなくなる。つまり、端末移動速度がPDCシステムに比べて遅くなる。現状では、PDCシステムで約80 km/h、PHSで約20 km/h程度が限界と言われている。

一方、無線データ通信速度を比較すると、PDCシステムでは9.6 kビット/s、PHSでは29.2 kビット/sのデータ通信がそれぞれ可能である。この違いは、チャンネル帯域、つまり、一つの呼が占有する帯域に依存している(表1参照)。

PDCシステムとPHSのデータ通信構成を図2に示す。どちらの場合も、PDCシステムや、PHS電話機とクライアント端末をアダプタで接続する構成である。アダプタとクライアント端末の接続には、RS-232Cパソコンによるものと、PCMCIA(Personal Computer Memory Card International Association)によるものがある。また、アダプタと電話機には、16ピンの独自デジタルインタフェース(PDCシステムとPHSで異なる。)を用いている。網側の構成は、PDCシステムが網内にモデムプールを持



注：略語説明 TA(Terminal Adapter)

PIAFS(PHS Internet Access Forum Standard)

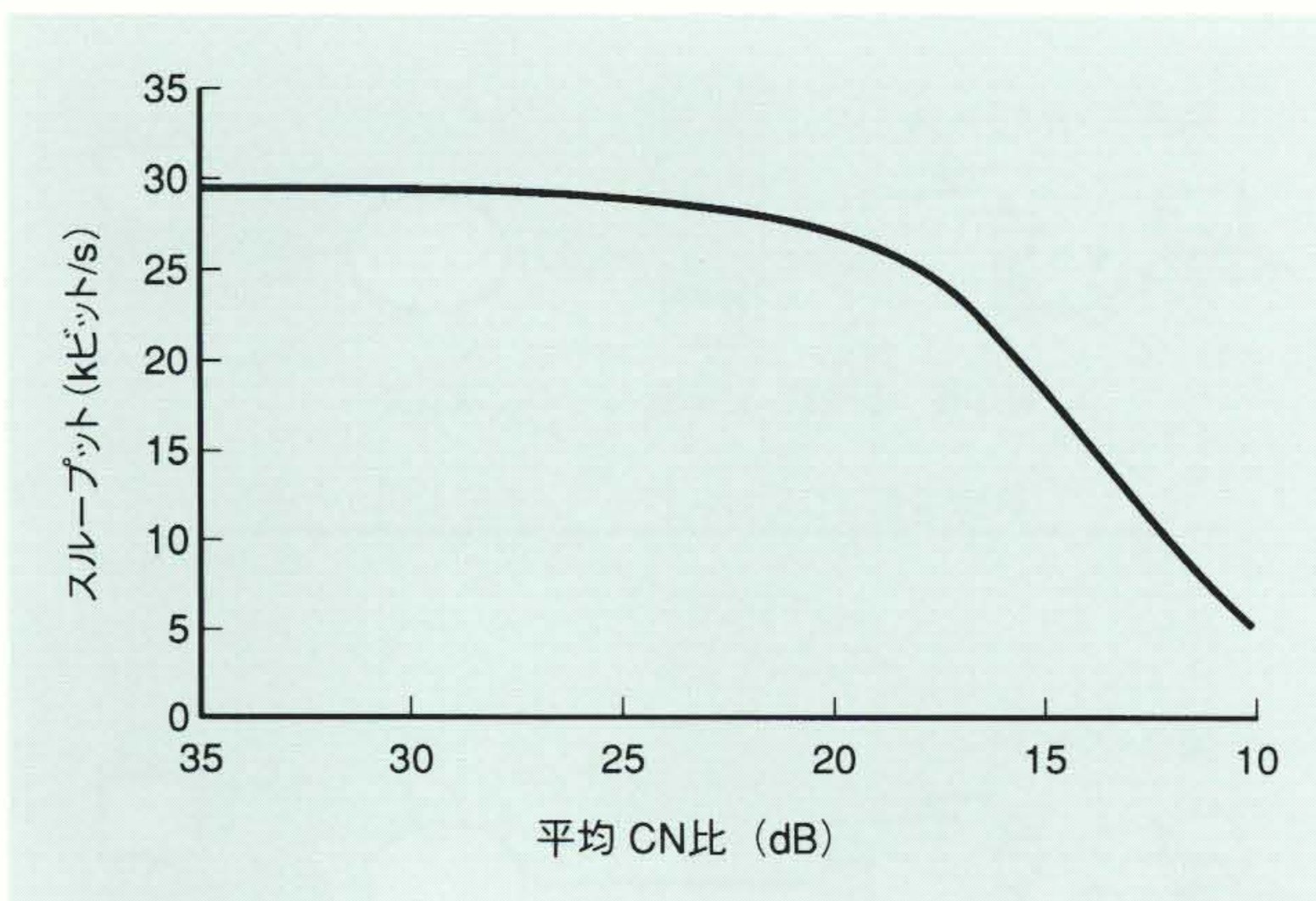
図2 PDCシステムとPHSのデータ通信構成

PDCシステムでは網内にモデムプールを用意し、サーバ側は一般モデムで通信が可能であるのに対し、PHSではサーバ側にもPHS専用のTAが必要である。

ち、アダプタとの間のPDC無線通信プロトコルをモデムプロトコルに変換しているのに対し、PHSでは、網側はISDNに接続されたサーバとの間に32 kビット/sのベアラチャネルを提供している。つまり、PDCシステムでは、サーバ側は通常のもデムによって通信が可能であるのに対し、PHSではサーバ側にPHS用のTA(Terminal Adapter)、通称“TAP”が必要となる。クライアント側のアダプタとTAP間で、PHS用の無線通信プロトコル“PIAFS(PHS Internet Access Forum Standard)”によって通信する構成である。PDCシステムとPHSの無線通信プロトコルは詳細では異なっているが、再送による誤り制御を行うプロトコルである。PHSでのデータ通信速度の特性例を図3に示す。また、双方とも“V.42bis”によるデータ圧縮をサポートしており、データ種別によっては、実効スループットがそれぞれ9.6 kビット/s、29.2 kビット/sを超える場合がある。

3.2 無線データ通信の将来動向

PDCシステムやPHSなどの現在の無線通信網は、デジタル化を特徴とする第2世代通信と呼ばれている。第2世代では、システム内の端末移動(ローミング)は可能であるが、異なるシステムをまたがる端末移動(例えば日



注：略語説明 CN (Carrier-to-Noise)

図3 PHSでのデータ通信速度の特性例

約25 kビット/s以上のスループットが期待できる。CN比は、通常20 dB以上と想定される。

本一欧州間)はできない。また、データ通信速度は、32 kビット/s足らずである。これに対して、“IMT-2000”と呼ばれる、2000年のサービス開始を目標とした第3世代の無線通信網の標準化が推進されている。IMT-2000の目標は、グローバルローミング(全世界にまたがる端末移動)と、384 kビット/sから2 Mビット/sの高速マルチメディア通信の実現である。高速マルチメディア通信実現のため、無線伝送方式としては、可変速度通信に適したCDMA (Code Division Multiple Access) 方式が、無線基地局と移動交換機間の網としては、ATM (Asynchronous Transfer Mode) 網がそれぞれ採用されている。

IMT-2000の時代には、インターネットとのシームレスな接続が必須である。すなわち、無線通信網上にIP (Internet Protocol) パケットを効率よく運ぶためのパケットルーティング機能や、IPレベルでの端末移動を実現するモバイルIP機能をサポートしたモバイルインターネットが構築される。これにより、有線・無線を問わない、真のモバイルコンピューティング通信基盤が現実のものになると考える。

4

セキュア モバイル コンピューティングを支える技術

セキュア モバイル コンピューティングを構築するにあたって必要な二つの技術、つまり次世代インターネットプロトコル“IPv6”をはじめとするインターネット関連技術と情報セキュリティ技術について以下に述べる。

4.1 インターネット関連技術^{1), 2)}

インターネットはサブネットワークの集まりで構成

し、他のサブネットワークとはルータで接続する。インターネットにつながるすべての機器には、ネットワークアドレスを付ける。インターネットの場合、これを「IPアドレス」と呼ぶ。IPアドレスは、サブネットワークアドレスと機器固有のアドレスの組合せで表現する。

移動するインターネット環境での携帯端末も、IPアドレスを使って通信する。サブネットワークを越えて移動した場合、サブネットワークアドレスが変わるため、IPアドレスも変える必要がある。インターネットでのモバイルコンピューティングの課題は、このIPアドレスを自動的に解決することにある。IPアドレスを解決する三つの方法を表2に示す。

これらは、利用形態に応じて使い分ける。HTTP (Hypertext Transfer Protocol) サーバや電子メールサーバなどへのアクセスはクライアント-サーバ型アクセスであり、自動配布、自動生成方法を用いる。一方、インターネット電話のような「Peer-to-Peer^{※1)}通信」の場合は、相手をアドレスで直接呼び出す必要があり、不変な固定方法を用いる。

次世代インターネットプロトコル“IPv6”では、現行のインターネットプロトコル“IPv4”が抱えるIPアドレス不足の問題を解決するとともに、移動端末自身でIPアドレスを自動生成することができる。

日立製作所が業界に先駆けて製品化したIPv6ルータ“NR60”(図4参照)は、固定、自動生成方法を支援する。

今後、IPv6の固定、自動配布機能を搭載するとともに、より快適に安心して使えるように、認証機構やセキュリティを強化する考えである。

※1) Peer(ピア)：ネットワークで他のステーションと同等の資格を持つステーション

表2 IPアドレスの解決方法

利用形態によって使い分ける。IPv4の自動配布機能はWindows 95/Windows NT^{*}が、白地部分はNR60がそれぞれサポートしている。

バージョン 方法	現行インターネット “IPv4”	次世代インターネット “IPv6”	設備
自動配布	○	△	中
固定	○	△	大
自動生成	—	○	小

注：記号説明ほか

○ [IETF (Internet Engineering Task Force) 標準仕様], △ (IETFで審議中), — (機能なし)

* WindowsおよびWindows NTは、米国およびその他の国における米国Microsoft Corp.の登録商標である。

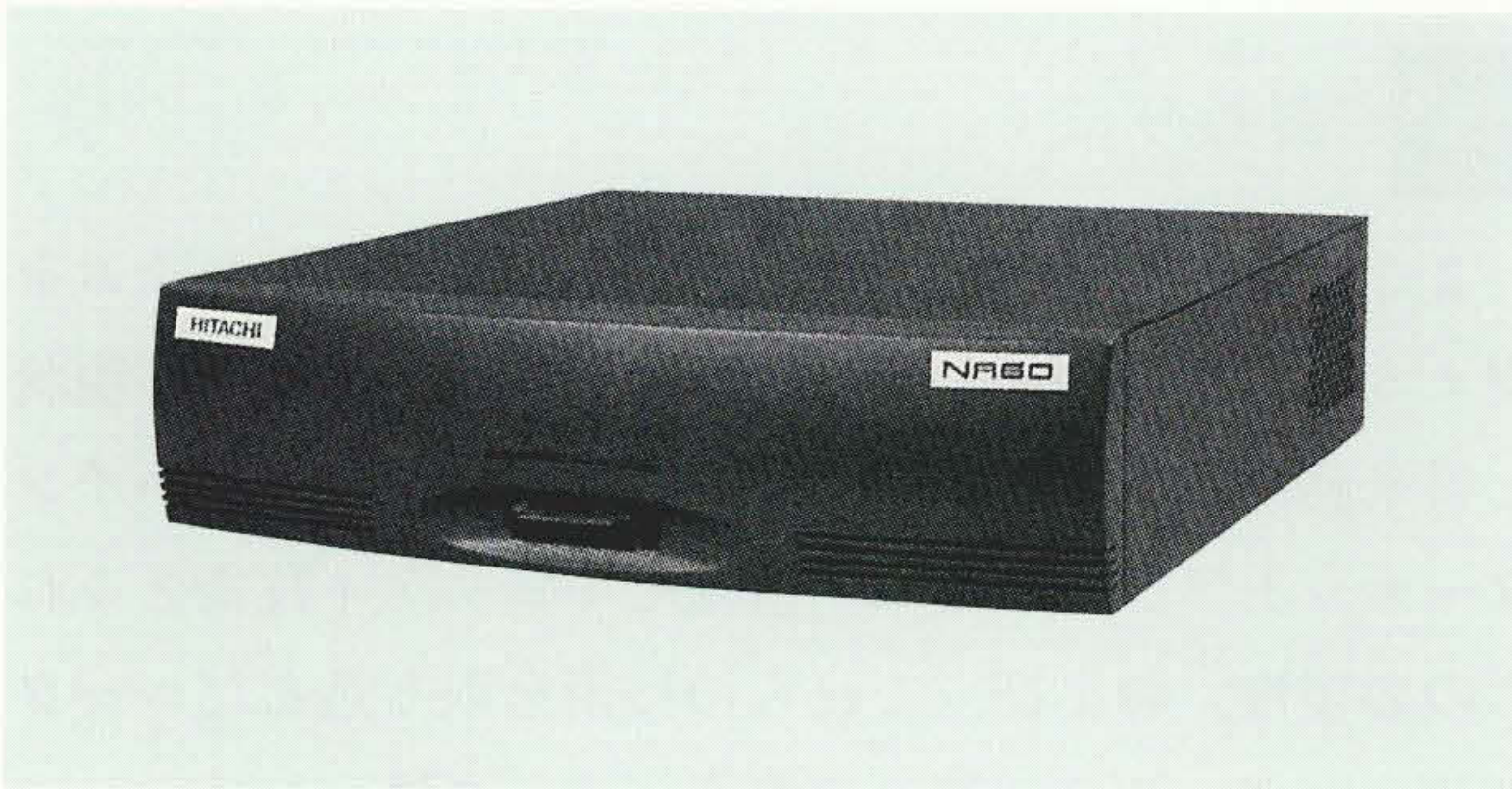


図4 IPv6ルータ“NR60”

インターネット端末の移動をサポートする機能を用意している。

(1) 自動配布方法

DHCP (Dynamic Host Configuration Protocol) サーバを用意し、ネットワーク管理者が事前に割り当て用IPアドレス群を設定する。移動端末を接続したとき、IPアドレスが自動的に割り当てられる。すでに、Windows 95/Windows NTがサポートしている。

(2) 固定方法

移動元と移動先のサブネットワークに、モバイルIPエージェントを搭載したルータまたはゲートウェイを用意する。モバイルIP機能を持った端末が移動すると、移動元と移動先のモバイルIPエージェントとが連携し、移動

端末あてにきたデータを自動的に移動先に届ける。

(3) 自動生成方法

IPv6ルータは、マルチキャストを使ってサブネットワークのアドレスを定期的にそのサブネットワーク内に配信する。ネットワークに接続した端末は、このアドレスの受信を行うと同時に、自分が持っている機器アドレスと組み合わせてIPアドレスを自動生成する。

4.2 情報セキュリティ技術³⁾

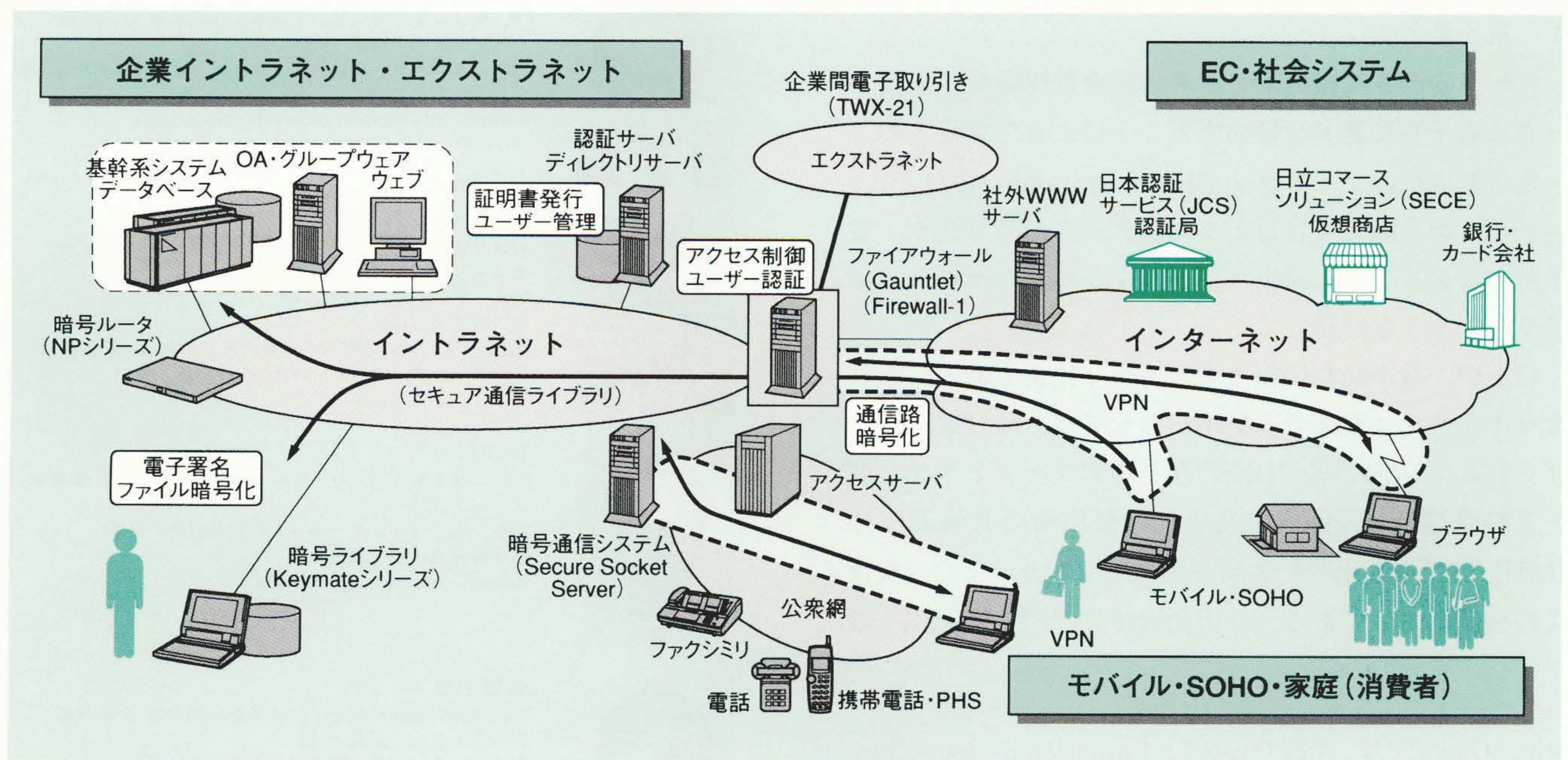
公衆網のような社外のオープンなネットワークから企業内情報システムへのアクセスを可能とするSOHO (Small Office, Home Office)・モバイルシステムでは、情報セキュリティが非常に重要となる。

実現したい利用形態は、ネットワークを介して、(1) 正当なユーザーだけが正当な相手にアクセスできること (成り済まし防止)、(2) 必要な情報の入手や発信をする際にネットワークを経由するデータの盗聴を防止できること、(3) 交信されたデータの改ざんの検出や交信事実の否認を防止できることなどである。情報セキュリティの全体概要を図5に示す。

その主要な考慮点と対策について以下に述べる。

(1) アクセス制御

許可されたユーザーだけのシステムアクセスを許容するために、LANからオープンなネットワークへの出入口



注：略語説明ほか EC (Electronic Commerce), WWW (World Wide Web), ←→ (通信路暗号化範囲)

図5 情報セキュリティの全体概要

モバイル環境でのセキュリティの考慮個所と対策の対応を示す。

にファイアウォールを設定することによって実現する。ファイアウォールは許容するプロトコル種別やIPアドレス、ポート番号やユーザー認証などによってLANへの進入を制御する。

“Gauntlet^{※2)}”と“FireWall-1^{※3)}”という2種類のファイアウォール製品を提供している。

(2) データ保護・通信路暗号化

データの流出やネットワーク上を流れるデータの盗聴を防止するため、データの暗号化が行われる。ネットワーク上を暗号化することにより、一般の回線を仮想的な専用線“VPN(Virtual Private Network)”として用いることが可能となる。これを、上述のファイアウォールへの付加機能や、専用のサブシステムによって実現する。

日立製作所は現在、Gauntletにアドオンする“VPN for Gauntlet”と、公衆網経由のモバイルアクセスを対象とした「Secure Socket Serverシステム」の2形態のVPN製品を開発している。

(3) 認 証

交信相手や組織の身元保証を行うために、認証サーバが発行する電子的な証明書を利用する。認証サーバでは証明書単位に認証を行うため、クライアントを操作しているユーザーが本人かどうかを正確に認証できる。

国際標準である“X.509”に準拠した証明書を発行、管理する認証サーバを開発している。この証明書は、ICカードなどに格納して携帯することも可能である。

(4) 電子署名

データの改ざん検出やデータの完全性保証を、送信データに電子的な署名を付加することによって実現する。

電子署名用のライブラリ“Keymate/sign”のほかに、ユーザーが意識せずに行える交信データの暗号化や、電子署名による改ざん検出ができるようにしたセキュア通信ライブラリを開発している。

以上が、基本的な情報セキュリティ技術である。これらセキュリティ製品の基盤技術としては、暗号技術があげられる。“RSA”や“DES”などのデファクトスタンダード暗号以外に、強度の高い日立製作所の共通鍵暗号“MULTI2”を適用した製品も開発しており、また、次世代の公開鍵暗号である、だ円曲線暗号“ELCURVE”の

適用も予定している。

5 おわりに

ここでは、モバイル コンピューティング システムを支える通信基盤技術から見た無線データ通信技術の現状と将来動向、さらに、モバイル通信には欠かせないインターネットアドレス技術・情報セキュリティ技術とこれらの必要性、および、これらの技術を取り込んだルータ製品、セキュリティ製品の概要について述べた。

今後は、これら先行技術の標準化活動に貢献するとともに、ユーザー要求を先取りした製品とソリューションを提案していく考えである。

参考文献

- 1) S. Thomson, et al.: IPv6 Stateless Address Autoconfiguration. RFC 1971(1996-8)
- 2) C. Perkins: IP Mobility Support, RFC 2002(1996-10)
- 3) 佐々木, 外: インターネットセキュリティ, オーム社(1996)

執筆者紹介



河野 哲也

1978年日立製作所入社, 情報事業企画本部 企画本部
システム製品企画部 所属
現在, ネットワーク製品, ネットワークサービス商品企画に
従事
E-mail: t-kawano@comp.hitachi.co.jp



松井 進

1980年日立製作所入社, システム開発研究所 第4部
ネットワーク基盤センタ 403研究ユニット 所属
現在, モバイルコンピューティング・コミュニケーション
の研究開発に従事
IEEE会員, 情報処理学会会員, 電子情報通信学会会員
E-mail: matsui@sdl.hitachi.co.jp



安江 利一

1970年日立製作所入社, サーバ開発本部 開発部 開発第二
グループ 所属
現在, 次世代インターネットの製品開発に従事
電子情報通信学会会員
E-mail: yasuye@isrd.hitachi.co.jp



金野 千里

1977年日立製作所入社, 情報事業企画本部 企画本部
システム製品企画部 所属
現在, セキュリティ関連製品の企画に従事
理学博士
情報処理学会会員, 日本応用数理学会会員
E-mail: c-konno@comp.hitachi.co.jp

※2) Gauntletは, 米国Trusted Information Systems, Inc.の商品名称である。

※3) FireWall-1は, Check Point Software Technology Ltd.の商品名称である。