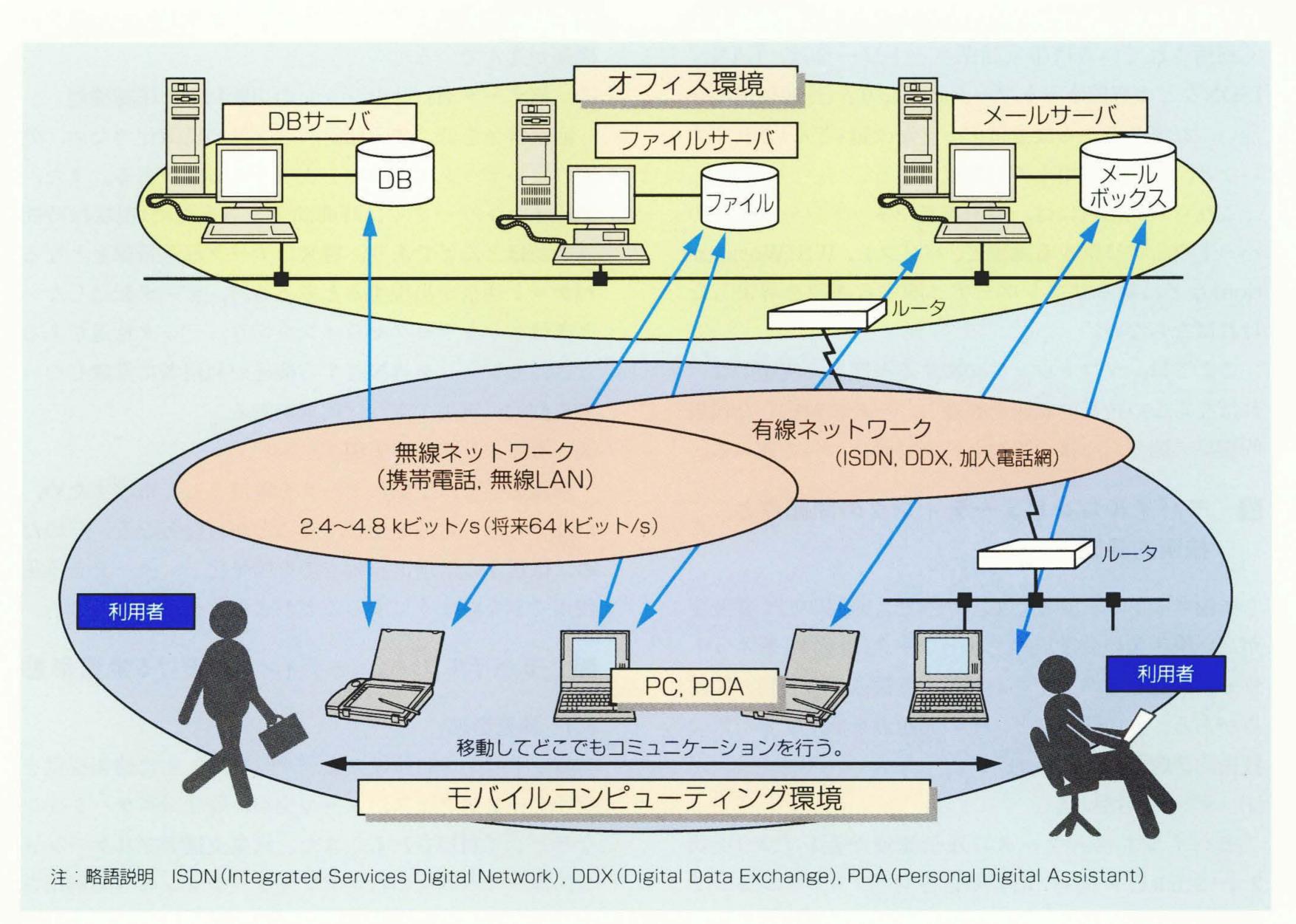
# モバイルコンピューティング環境におけるソフトウェア製品の開発

Software Products and Examples of Application in Mobile Environment

松崎高典\* Takanori Matsuzaki 池田 裕\*\*\* Yutaka Ikeda 橋本 尚\*\* Hisashi Hashimoto 斉藤太朗\*\* Tarô Saitô



# モバイルコンピューティング環境

モバイルコンピューティング環境では、サブノートパソコン、PDAを持ち運び、どこからでも無線、有線ネットワークを使ってオフィス環境内の各種サーバにあるデータを利用することができる。

携帯電話のネットワーク、サブノートパソコン、 およびPDA (Personal Digital Assistant)の普及に より、移動してどこからでもパソコン、PDAを使用 したデータ通信が行えるモバイルコンピューティン グ環境が急速に広がっている。

一方,モバイルコンピューティングの実現のためには,データのセキュリティや回線料金の低減化,携帯型新端末の利用など,システム構築上考慮しなければならない問題点が多数ある。

モバイルコンピューティングの実現のため、検討対象のモデル化と利用上の問題点の把握および必要技術を整理して、非同期アプリケーションを実現する製品やデータの圧縮・暗号化、および認証を実現する製品を開発した。この製品は、統合型グループウェア "Groupmax" とPDAとを接続し、モバイル環境でのメール交換を実現するとともに、既存のアプリケーションの改造なしにセキュリティを実現するものである。

<sup>\*</sup> 日立製作所 情報システム事業部 \*\* 日立製作所 ソフトウェア開発本部 \*\*\* 日立製作所 ソフトウェア開発本部 技術士(情報処理分野)

#### 1 はじめに

モバイルコンピューティングの実現に利用される広域ネットワークは、有線ネットワークと無線ネットワークに大別される。無線系のネットワークとして現在最もよく利用されている携帯電話系ネットワークは、LAN、ISDNなどの有線ネットワークと異なり、(1)通信速度が遅い、(2)第3者から故意にデータが改竄(ざん)されやすいなど、種々の利用上の問題点がある。

これらの問題点には、端末機器やネットワークなどのハードウェアに関する課題と、パソコン、WS(Workstation)などに載るソフトウェアに関する課題を解決しなければならない。

ここでは、ソフトウェアに関する課題と、実現しなければならない技術的課題を整理し、それに対応した代表的製品の紹介、今後の課題と将来計画について述べる。

# 2 モバイルコンピューティングの問題点と 技術的課題

無線ネットワークとして、サービス範囲が広く普及度が高い携帯系の公衆無線ネットワークには、有線ネットワークに比べてユーザーが利用する観点から各種の問題点がある。その問題点と、その問題点を解決するための技術的課題を表1に示す。

#### (1) データー括転送

モバイルネットワークの通信速度が遅いため(現状 2.4~9.6 kビット/s), 問合せ応答型アプリケーションでは応答性や使い勝手が悪い。この問題点を解消する, リアルタイム処理が必要なアプリケーションのほかに, データアクセス要求後しばらくたってから情報を取り出してもよいアプリケーションがある。このアプリケーショ

表 | 無線ネットワークの問題点と技術的課題

応答性や使い勝手を向上するには,技術的課題で示す対応を図らなければならない。

問 題 点	技術的課題	
通信速度が9.6, 4.8 kビット/sと 低速なので、問合せ応答アプリ ケーションには向かない。	データー括転送などの低速度通 信に耐えられるアプリケーション	
回線料金が高い。 ● ディジタル携帯電話系: 10円/7秒 ● PHS: 40円/3分	無データ通信時セションの切断 制御とデータ圧縮機能	
無線通信なのでセキュリティ機 能が必要である。	暗号化機能	

ンは非同期アプリケーションと呼ばれ(反対に問合せ応答型は同期アプリケーションと呼ぶ。),通信速度が遅くてもあまり問題とならない。このアプリケーションを実現する技術としてメッセージキュー機能があり、メッセージキュー対応ミドルソフトウェアを使用したシステム構築が進んでいる<sup>1)</sup>。

#### (2) 無データ通信時セションの切断制御と圧縮機能

回線料金を低くする伝送データ量の低減化のため,効率の良いデータ圧縮機能を実現する必要がある。また,無線ネットワークでは時間課金であるため(現状は時間課金がほとんどであり,将来はデータ転送量課金となるパケット通信が出現すると考える。),データ転送しないときはネットワークセションを切り,データ転送があるときはセションを再接続する機能が利用者に意識しないで自動的に実現できれば便利である。

## (3) セキュリティの実現

無線通信では空間にデータを電波として飛ばすため、 だれでもその電波を受信することが可能となる。そのため、伝送するデータそのものを暗号化し、データを不正 使用できないようにすることが必要となる。

# **3** モバイルコンピューティングにおける業務形態

# 3.1 業務形態

ネットワークに接続するパソコンは、主に情報提供を 行うデータアクセス、メール交換、コミュニケーション などとして利用される。また、営業支援アプリケーショ ン、ユーザー固有の特定アプリケーションとして利用さ れたり、商品のプレゼンテーション、個人のスケジュー ラ管理としても活用されている。

PDAは手帳機能として利用され始めたが、最近はメールや営業支援・特定アプリケーションとして利用されるようになっている。このように利用されるアプリケーションから想定したモバイルコンピューティングの業務形態例を表2に示す。同表で示すように、モバイルコンピューティングで利用されるアプリケーションを整理すると、サーバクライアント型での適用が多い。モバイル環境の端末からオフィス内にある各種データベース、ファイルへの必要な情報のアクセス、オフィス内システムとのメール交換などのサーバクライアント型アプリケーションである。

#### 3.2 サーバクライアントモデル

データアクセス,メール交換などを実現するサーバ クライアント モデルを定義した。この場合,2章で述べた

表 2 モバイルコンピューティングの業務形態

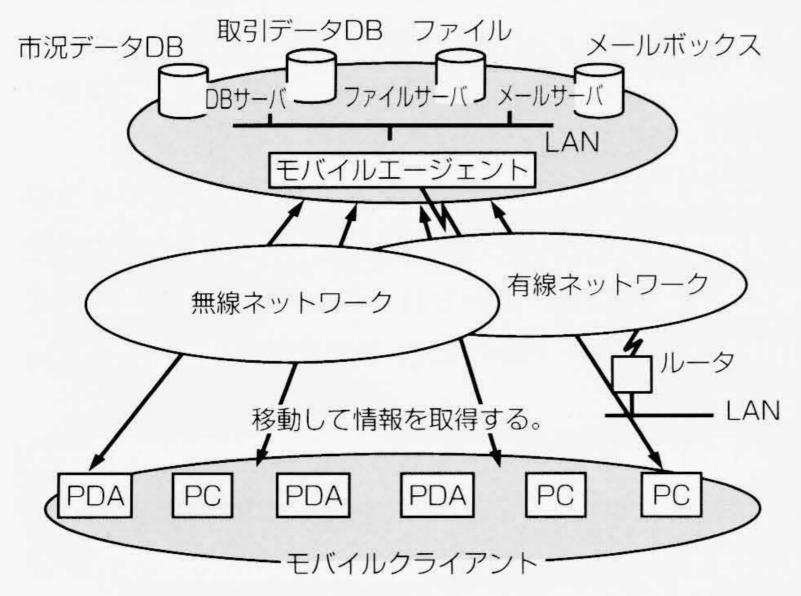
手帳機能として利用され始めたPDAは、メールや営業支援・特定 アプリケーションとしても利用されるようになってきた。

適用 分野	業務概要	適用業務	アプリケーション
営業分野	顧客先での迅速な 情報の入手による 的確な営業活動の 促進	<ul><li>●発注・見積支援</li><li>●プレゼンテーション</li></ul>	<ul><li>●DBアクセス</li><li>●電子メール</li><li>●受発注・見積支援</li><li>ソフトウェア</li></ul>
分 オ フィ 野 ス	出先でのメール, グループウェアに よるオフィス業務 との連携	● グループウェア ● データファイル 共有	<ul><li>グループウェア</li><li>リモートファイルアクセス</li></ul>
サービス分野	現場情報を迅速にかつ的確に把握し、業務システムへのスピーディな 反映を実現	<ul><li>●売上・生産管理</li><li>●診療支援システム</li><li>●チケットなどの 情報サービス</li></ul>	<ul><li>●DBアクセス</li><li>●電子メール</li><li>●リモートファイルアクセス</li></ul>

技術課題を解決する接続構成とすることが必要である。

最近、米国では、勘によるユーザーへの製品セールス ではなく, オフィス外でもユーザー情報を見て適切なセ ールス活動ができる、営業員の情報武装化を目的とした 環境開発が話題になっている<sup>2)</sup>。この環境にも適合する サーバクライアントモデルを図1に示す。このモデルで は、サーバをモバイルエージェント、クライアントをモ バイルクライアントと定義する。

オフィス内のLANの環境には、データベースサーバや ファイルサーバおよびメール交換を実現するメールサー バなどがある。これらのシステムでは、既存の資産を使 用してモバイルに適用させることがユーザーニーズ上必



モバイルコンピューティング適用のサーバクライアン トモデルー営業員支援システムー

モバイルクライアントからモバイルエージェントに各種サーバ 上の情報検索を依頼する。

要である。そのため、2章で述べた技術課題をモバイル エージェントとモバイルクライアント間で実現し, LAN 環境の既存の資産をそのまま利用できるようにする。

また、2章で述べた非同期アプリケーションとして、 メッセージキュー機能を使用したシステム構築も必要と なる。モバイルクライアントからデータアクセス命令を モバイルエージェント上のキューに蓄積することによ り、モバイルエージェント上のアプリケーションが命令 の実行を行い、必要な情報をLAN上の各種サーバから取 り出し、まとめることができる。このシステムでは、モ バイルエージェントはクライアントの秘書的な存在とな り、クライアント端末を持ち歩く営業員にとって情報武 装化の重要なシステムとなる。

# **4** モバイルコンピューティング環境を実現する ソフトウェア製品

2章で述べたモバイルコンピューティングに必要な技 術課題に対応し、3章で述べた業務形態を実現するソフ トウェア製品を開発した。この章では、製品紹介と機能 および具体的実現方式について述べる。

#### 4.1 非同期アプリケーションの実現

2章で述べた技術課題の中のデーター括転送を実現す るMobile Message Queueと、この製品を使用してデー タベースアクセスを実現するDBPARTNER Mobileを 開発した。

#### 4.1.1 開発のねらい

#### (1) Mobile Message Queue

非同期アプリケーションを実現するメッセージキュー 機能を提供するミドルソフトである。開発のねらいを次 に示す。

- (a) 従来の基幹業務システムで活用しているオンライ ントランザクション処理(OpenTP1)との連携を実現
- (b) DBPARTNERとの連携によるデータベースアク セスの実現
- (c) メッセージキューAPIを提供して利用者独自のア プリケーションの構築を実現

## (2) DBPARTNER

メインフレームからPC, UNIX\*1)サーバのリレーショ ナルデータベースを容易に検索して更新するアプリケー ションソフトである。開発のねらいを次に示す。

UNIXは、X/Open Company Limitedがライセンスし ている米国ならびに他の国における登録商標である。

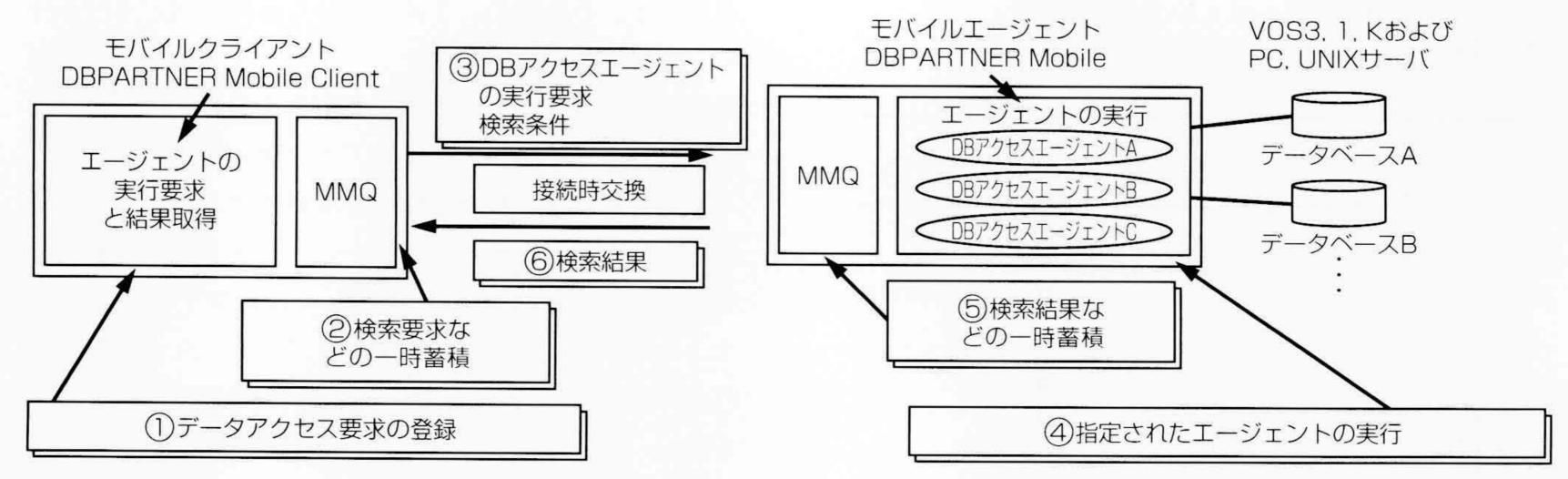


図 2 メッセージキュー機能によるデータベースアクセス DBPARTNERとMMQ(Mobile Message Queue)による非同期データベースアクセスを実現する。

- (a) Mobile Message Queueと連携して非同期による データベースアクセスを実現する。
- (b) 既存のメインフレームのデータベースもアクセス する。

#### 4.1.2 実現方式

MMQ(Mobile Message Queue)と DBPARTER Mobleでデータベースアクセスを実現する処理手順を **図 2** に示す。

- (a) DBPARTNER Mobile Clientからデータベース アクセスを実行するエージェントの指定と検索条件な どのデータアクセス要求を登録する(図2の①)。
- (b) 上記アクセス要求をモバイルクライアント側の MMQに一時蓄積する(**図2**の②)。
- (c) モバイルクライアントとモバイルエージェントが接続時データを一括転送する。転送後はいったん切断し,別作業が可能になる(図2の③)。
- (d) モバイルエージェント側では、指定したデータベースアクセスエージェントが受信したデータアクセス 要求を実行する(図 2 の④)。
- (e) 実行結果はモバイルエージェント側MMQに蓄積 する(**図2**の⑤)。
- (f) モバイルクライアントとモバイルエージェントの接続時に, MMQの中に検索結果があればモバイルクライアントへデータを一括ダウンロードする(図2の⑥)。

# 4.2 圧縮・暗号機能の実現

2章で述べた技術課題の中の圧縮・暗号化を実現する SecureSocketを開発した。

#### 4.2.1 圧縮・暗号化実現のための要件

圧縮・暗号化の実現要件を以下に示す。

(1) 効率の良いデータ圧縮暗号化機能の開発

- (2) 通信異常時でもエンドシステム間の圧縮辞書情報を 一致させる内部フレーミング機能の開発
- (3) 本機能を持たない通信相手との接続
- (4) マスタ鍵とセション鍵による高セキュリティの実現
- (5) アプリケーションごとの圧縮, 暗号化方式の指定による柔軟なセキュリティの設定
- (6) 既存アプリケーションの改造なしにセキュリティ環 境を実現

#### 4.2.2 セキュリティ要件

必要なセキュリティ要件は,暗号鍵,認証,データの 完全性保証である。

#### (1) 暗号鍵

暗号鍵は、セション鍵とマスタ鍵から成る。セション 鍵は個々の通信データの暗号化に用いる。セションごと に異なる鍵を接続要求側が生成する。セション開始時に、 接続要求側が接続受け付け側にセション鍵を伝える。マ スタ鍵は、セション鍵を相手に伝える際に、そのセション鍵を暗号化するのに用いる。マスタ鍵は、事前に各パ ソコンに設定しておく。

マスタ鍵は2種類まで設定することができる。ネットワーク内に特定の相手どうしだけと通信するグループを設定したい場合には、ほかとは異なるマスタ鍵を設定しておけばよい。マスタ鍵の設定、切り替えは自由にできる。(2) 認 証

通信相手が正しい相手であることを確証する機能である。接続時に異なるパスワードを用いて相手確認を行う。 毎回異なるパスワードは本製品内部で自動生成され、接続時に自動確認が行われる。

アプリケーションが同時に複数のコネクションを張る 場合があっても,本製品内部で自動的に確認が行われる ため、ユーザーが煩わしい操作をする必要がない。

## (3) データの完全性

第三者が通信経路の途中で, データを改ざんしていな いかどうかを検知する機能である。通信データに、独自 のハッシュコード(パリティ チェック コード)を付与す ることにより、改ざんの有無をチェックする。 第三者へ の対策である。

#### 4.2.3 圧縮・暗号機能

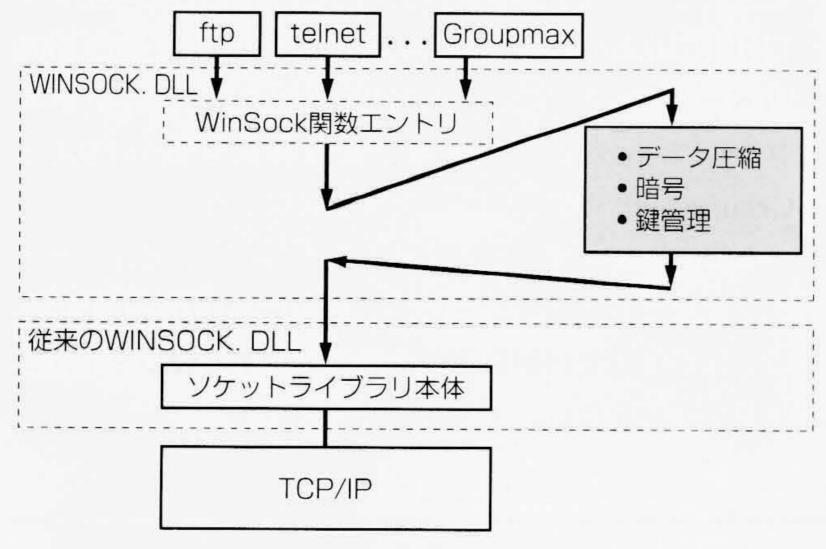
#### (1) 圧縮・暗号化

アプリケーションとTCP/IP(Transmission Control Protocol/Internet Protocol)プログラムとの間で、送受 信データの授受を行うソケットAPI(Application Programming Interface)を通して圧縮・暗号処理を行う。送 信処理で圧縮および暗号化を, 受信処理で伸長および復 号化を行う。圧縮率では最高50%の圧縮が可能である。 (2) ソケット関数フックによるAP(Application Process) 非依存型圧縮・暗号化

圧縮・暗号化の処理では、アプリケーションがTCP/IP プログラムにコールするソケット関数をフックすること によって実現する。アプリケーションおよびTCP/IPプ ログラムの改造なしに圧縮・暗号化機能が利用できる。 ソケット関数のフック処理の概念を図3に示す。

#### (3) セキュアポートによる圧縮暗号処理

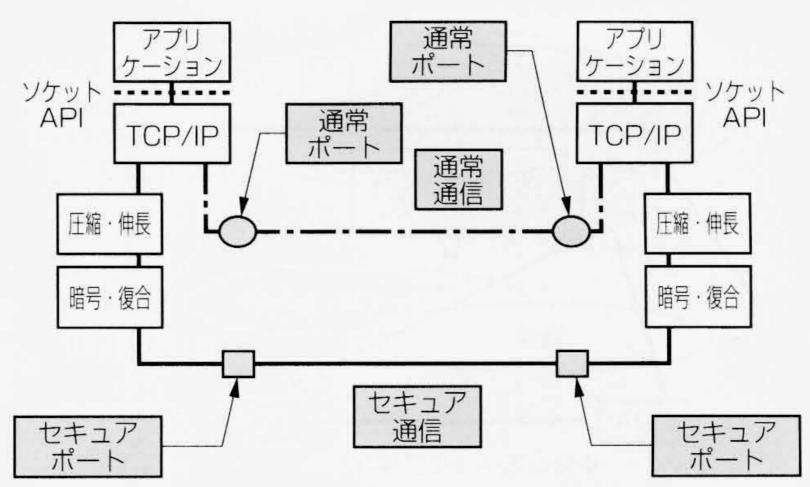
アプリケーションが指定したポートを、図4に示すよ うにセキュアポートと呼ぶ特別なポートに置き換えて, 自動的に圧縮・暗号化を行う。アプリケーションが送信



注:略語説明 ftp(ファイル転送), telnet(仮想端末) WINSOCK. DLL(WINSOCK(WindowsでのTCP/IP用 アプリケーション インタフェースを提供するインタフェ ース)を実現するライブラリ]

# 図3 フック処理

ソケット関数のフック処理により,従来のアプリケーションの変 更無しにデータの圧縮・暗号処理を実現する。



注:略語説明 API(Application Programming Interface)

図 4 セキュアポートによるセキュア通信 特別なセキュアポートを設定し, 圧縮・暗号を実現する。

依頼を出してきたデータを圧縮・暗号化処理し、セキュ アポート経由で送信する。受信処理でも同様に、セキュ アポートからの受信結果を伸長復号化して, アプリケー ションに渡す。

#### (4) 圧縮方式,暗号処理方式の選択

圧縮・暗号化処理では、複数の圧縮方式、暗号化方式 に対応するため、アプリケーションに対して、X/Open\*2)で 定められている暗号化の標準的なインタフェース"GSS-API (Generic Secure Service Application Programming Interface)"を提供する。

# 4.3 グループウェアでの対応

統合型グループウェア製品"Groupmax"は、顧客ニー ズの多様化,変化に対応する企業活動を支援するため, 企業のBPR (Business Process Re-engineerig)を支援す る基本機能を提供する。今回、モバイルコンピューティ ングの対応として、メール機能製品"GroupmaxMail"が メールサーバとなり、PDAとのメール交換を実現した。

#### 4.3.1 GroupmaxMailのPDA対応

GroupmaxMailのサーバでは、TCP/IPをサポートし ていないクライアント端末からもメールの送受信ができ るように、「リモートパソコン」という機能を提供してい る。この機能は、TCP/IPによる通信手順をパソコン通信 で使用されている無手順プロトコルに変換し、端末側か らはパソコン通信のメールのようなイメージで使えるよ うにするためのものである。このため、パソコン通信機 能だけに対応するPDAなどの端末は、このリモートパソ コン機能を使ってGroupmaxMailとメールの送受信を

X/Openは、X/Open Company Limitedの英国ならび に他の国における登録商標である。

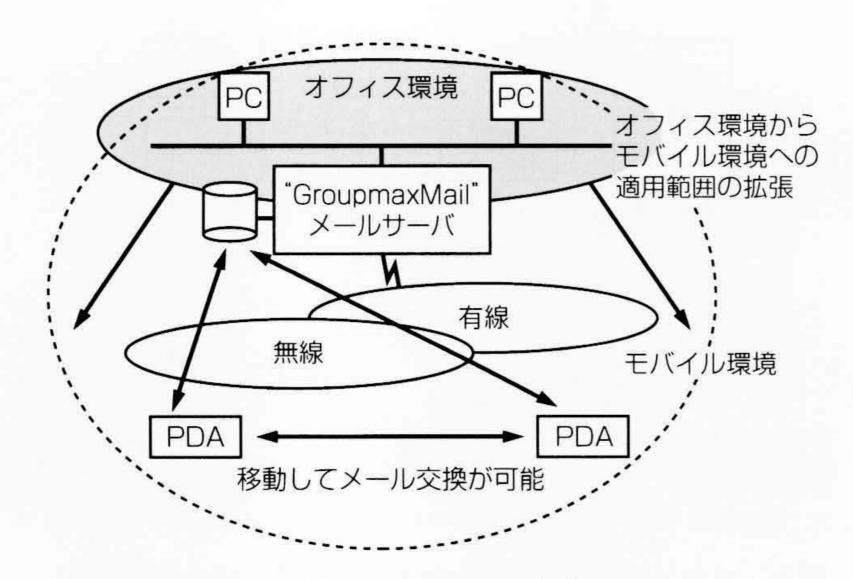


図 5 GroupmaxMailとPDAとのメール交換 GroupmaxMailサーバによってPDAとのメール交換を実現する。

行うことが可能となる。PDAとのメール交換の概念を 図5に示す。

さらに、日立のPDAである"NomadicPad"、"Possible" には、GroupmaxMail専用のGUI(Graphical User Interface)上から容易にメールの送受信ができるようにした。 また、今後は他社のPDAとの連携も行うほか、メール 以外のワークフロー、スケジューラでのPDA連携も進めていく考えである。

# 4.3.2 GroupmaxMailのセキュリティ

GroupmaxMailでは、パソコン間およびパソコン・メインフレーム間で、Keymate/Multiの暗号化ライブラリと連携し、GroupmaxMailの画面から簡単にメール本文と添付ファイルデータの暗号化が行える。これにより、アプリケーションレベルでの1対1の暗号化通信が実現でき、機密を保つことができる。また、SecureSocketを使用した圧縮・暗号機能をパソコン間で実現することもできる。

#### 5 今後の展開

現状では、2章で述べた技術課題の圧縮・暗号機能およびデーター括転送に対応している。今後は、機能の拡張を図っていく考えである。

また、これ以外にもモバイルコンピューティングの利 便性を追求するため、検討していかなければならない事 項が多数ある。

#### (1) Groupmaxの拡張

GroupmaxとPDAとの接続では、ワークフローやスケジュール管理の対応が必要となる。また、パソコンとPDAとの接続時のセキュリティ確保も必要であり、それぞれ対応を図っている。

#### (2) インターネット接続

最近のインターネットの利用促進にかんがみ、モバイルネットワークとインターネット相互接続サービスが増えることが予想される。モバイル環境でのインターネット利用形態とファイアウォールを含めたセキュリティ実現の検討を進めている。

#### (3) モバイルIP

TCP/IP通信で、あるサブネットワークに接続していた端末をサブネットワークアドレスが異なる別のネットワークに接続するためには、IPアドレスの再登録が必要となり、端末を移動しながらでは容易に通信が行えない。これを解決するために、IETF(Internet Engineering Task Force)でモバイルIPの標準化が検討されている3。今後、このモバイルIPをサポートしていく考えである。

#### 6 おわりに

ここでは、モバイルネットワークの中で、携帯電話ネットワークの問題点とその問題点を解決する技術の整理、およびその技術を実現した製品の概要について述べた。

SecureSoketにより、既存システムでもプログラムの変更なしに、セキュリティシステムが構築でき、DBPAR-TNER MobileとMobile Message Queueによって非同期データベースアクセスが実現できる。また、モバイルコンピューティング環境で使用頻度が高いPDAとGroupmaxとの間でメール交換を実現した。

今後は、ユーザーが要求するモバイルコンピューティング環境でのアプリケーション構築と利便性の実現を目指し、最優先で必要となる機能を実現する製品を早期に開発していきたい。

# 参考文献

- 1) 快適になるモーバイル環境 データベースも社外で検索, 日経コンピュータ, 1995年10月16日号
- 2) 日経情報ストラテジー:特集 営業のリエンジニアリング, SFA, セールスマンA氏社長賞もらう
- 3) 石井,外:移動するネットワークのための透過的な通信機構の設計,情報処理学会,マルチメディア通信と分散処理ワークショップ論文集(1995-10)