モバイル企業やサービス・プロバイダ向けにセキュリティを強化したIBMのソリューション
2003年4月

WebSphere Everyplace Connection Manager: モバイル・セキュリティを強化し、ワイヤレス環境のコストを削減

デニス・アンダーソン
フレッド・クリステンセン
IBMパーベイシブ・コンピューティング

business

目次

概要

企業がモバイル環境を拡張するに伴って、経営者は複雑な課題に直面しています。たとえば、ホットスポットの数は2005年までに今の4倍になると予測されており、新世代のモバイル端末が高速データ通信の活用を加速しています。Gartnerは、「音声通信サービスの料金低下にもかかわらず、2003年現在モバイル・アプリケーションを展開している多くの企業で、ワイヤレス・データ通信サービスにかかる月々のコストやモバイル・ソリューションの所有にかかるコストが、予測よりも少なくとも30%超過すると見ている」と報じています[1]。

この問題に対して、帯域幅を最適化してコストを削減し、セキュリティを確保してさまざまなネットワークをシームレスにつなぐローミングを実現するために、IBMではWebSphere Everyplace Connection Managerを開発しました。WebSphere Everyplace Connection Managerは、性能を最適化して通信コストを削減しながらデータを暗号化する仮想プライベート・ネットワーク（VPN）をモバイル環境で実現します。このプラットフォームには、インターネット・プロトコル（IP）と非IPの両方を含む多様なネットワークやサーバーのハードウェア、装置、オペレーティング・システムおよびモバイル環境のセキュリティ機能も統合されています。ここでは、WebSphere Everyplace Connection Managerについて、次の機能に焦点をあてて解説します。

- クロス・ネットワーク・ローミング、データ圧縮と帯域幅の最適化
- モバイルVPN、強力な認証機能と米国政府による証明付き暗号化
- 業界標準のSSL（Secure Sockets Layer）とWTLS（Wireless Transport Layer Security）を使用したセキュアなモバイル・アクセス
- WAP（Wireless Access Protocol）、SMS（Short Message Services）、パケット・ラジオおよびページング・ネットワーク用のプッシュ型および双方向型メッセージング
- ネットワーク接続の検出、選択および優先順位付け
- HACMP（High Availability Cluster Multiprocessing）および分散管理

[1] Gartner, Five Steps to Contain Mobile Data Costs, by William Clark, February, 2003.

WebSphere Everyplace Connection Managerにより、モバイル・ユーザーは事実上あらゆる有線または無線ネットワークの間でローミングを行うことができるようになります。

WebSphere Everyplace Connection Manager — 概要

ワイヤレス・データ・ネットワークの進歩にもかかわらず、管理コストや通信可能なエリア、セキュリティに関する従業員からの要求の高まりに企業は直面しています。WebSphere Everyplace Connection Managerは、デリケートなデータの保護とネットワーク・トラヒックの最適化を行い、ワイヤレス・メッセージングを提供するとともにシームレスなローミングを可能にするように設計されています。分散型の拡張可能な多用途通信プラットフォーム・テクノロジーによって、ワイヤレス・ネットワークやサーバーのハードウェア、モバイル機器、オペレーティング・システムや業界標準の選択肢が広がります。

アーキテクチャの面から見ると、WebSphere Everyplace Connection Managerのプラットフォームは3つのコンポーネントで構成されています。モビリティ・クライアント、接続管理サーバー、分散管理の3つです。これによってユーザーは、コストが低くデータ転送速度の高いさまざまなネットワークを使用して、「いつでもつながっている」ことが可能になります。主な機能には次のようなものがあります。

機能	利点
ワイヤレス・ネットワークのデータ通信の最適化	• データ量とオーバーヘッドを削減し、ワイヤレス環境のVPNネットワークにおけるデータ通信効率を改善
認証	• 強力な二者認証により、サーバーとクライアント双方を確認
暗号化	• 3DESよりも高速な実行が可能な先進の暗号規格
クロスネットワーク・ローミング	• ネットワークが切り替わったときも、一貫したモバイルVPNとアプリケーションの使用が可能
シン・クライアントによるセキュアなアクセス方法	• 電話やIBMクライアント・ソフトウェアを使用していない装置も、HTTPSおよびWTLS業界標準でサポート
SMSゲートウェイおよびプッシュ型サービス	• フル機能のSMSゲートウェイと同様に設定可能 • Java™、C、C++をサポートするメッセージングSDK
サーバーの統合	• Radiusによって既存のAAAを統合し、LDAPおよびODBCデー タベースによってディレクトリを統合
信頼性と拡張性	• スケーラブルな分散設計による24時間常に信頼のおけるサーバー

には、WAPやShort Messaging、単方向および双方向ページング、およびパケット・ラジオ・ネットワークを利用したメッセージングのためのさまざまなメッセージング機能とプッシュ型機能も組み込まれています。プラットフォームは成熟した第五世代のソフトウェアで、負荷分散クラスターの設定、分散管理、ハードウェアのフェールオーバー機能を持ち、世界最大のプロフェッショナルなサービス集団によるサポートを受けることができます。

モバイル環境の一貫性とセキュアなネットワーク・ローミング

基本的な電子メール、SMSおよび個人情報管理（PIM）から移行しようとしている企業では、複数のネットワーク環境に対応するために、セキュリティ権限、接続の頻度、総合的なデータおよびネットワークのコストの条件を満たす必要があります。複数のネットワーク環境を通じて、一貫性や認証および暗号化方式の保守を行うのは大変な作業になります。この環境を単純化するために、WebSphere Everyplace Connection Managerではユーザーにログインを要求するのではなく、ローミングが発生したときにアプリケーションの再初期化を行うことによって生産性を高めています。

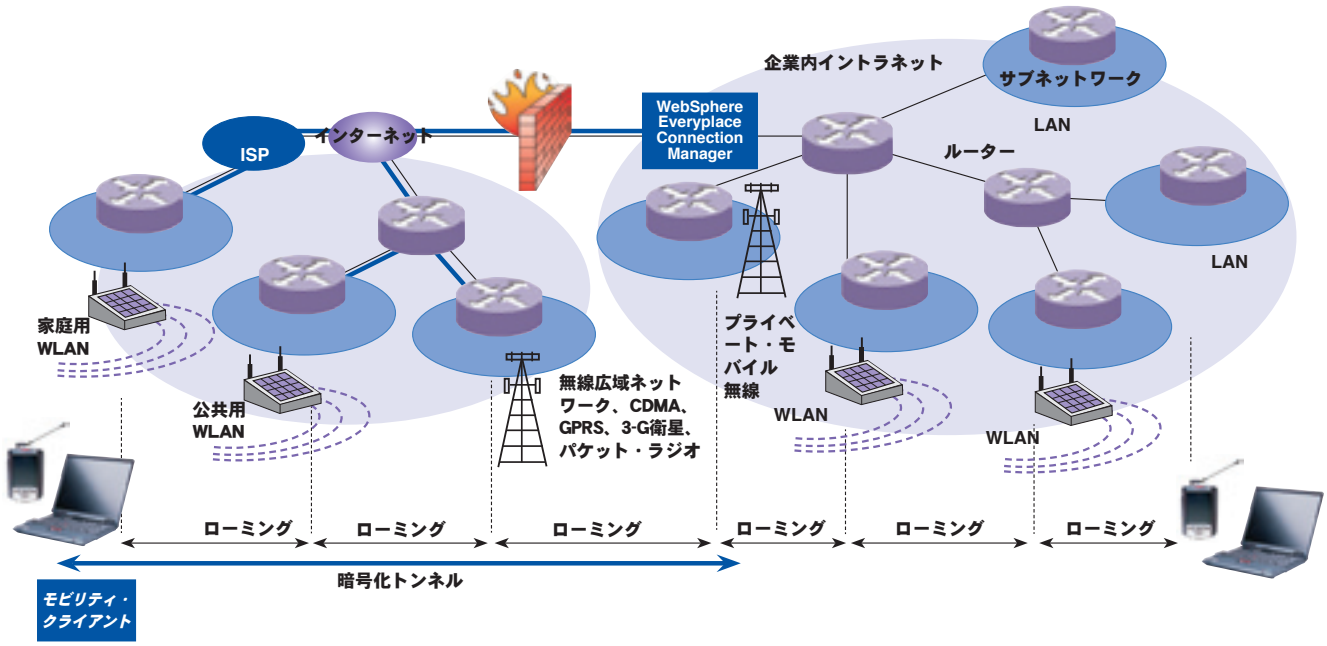
シームレスなローミングによって、モバイル機器が接続するネットワークが変わっても、エンドユーザー・セッションのカレントの状態とセキュリティを維持することができます。

一貫性が保たれることにより、VPN接続とアプリケーションのセッションの両方を維持したままで、物理ネットワークの切り替えが可能になります。デジタル加入者線（DSL）からオフィスのLAN、携帯電話やホットスポットへの移行では、ユーザーの接続は維持されて機器から企業への通信は暗号化されたままになります。ローミングをしない場合、ユーザーのセッションは失われアプリリケーションを再起動しなければならず、ファイアウォールの認証をやり直して新しいIPアドレスを取得し、VPN接続を更新してアプリケーションを再起動しなければなりません。特にこれは、有効な接続が切断されると会話の文字列全体が失われるインスタント・メッセージング・セッションにとっては大きな問題となります

非IPネットワークやパケット・ラジオ・ネットワーク間のローミングは、WebSphere Everyplace Connection Managerの重要な機能のひとつです。

ローミングは、物理的なネットワーク・インターフェイスからアプリケーションを分離したソフトウェア層で行われ、一貫したIPネットワーク・インターフェイスを実現し、新しいインターフェイスを経由するアプリケーションのトラフィックのルーティングを行います。これによって、モビリティ・クライアントVPNが動的にネットワークを選択し、セッションの整合性を損なうことなくスムーズにローミングを行うことができます。

IPおよび非IPネットワークの両方におけるローミングと暗号化



有線および無線ネットワーク間の事実上シームレスなローミングに加えて、WebSphere Everyplace Connection Managerはセキュアな暗号化されたトンネルを実現しています。

ネットワーク接続

携帯電話ネットワーク:
CDMA
TDMA
GSM CSD, SMS
PCS 1900 （日本）
PDC (Japan)
PHS (Japan)
CDMA2000, 1XRTT, eVDO
GPRS (GSM)
UMTS
PDC-P (Japan)
iDEN
DPD および CS-CDPD
AMPS & N-AMPS

SMS-C 接続:
SMPP
SMTP
SNPP
UCP

W-LAN, W-PAN:
802.11b
802.11a
Bluetooth

LAN 接続:
Ethernet
トークン・リング

インターネット接続:
ケーブル・モデム
ADSL/DSL
ISDN
ISP

ダイヤル接続:
DIAL/TCP
ISDN
PPP
PSTN (POTS)

公共非IPラジオ・ネットワーク:
DataTAC 4000 （アメリカ）
DataTAC/IP
DataTAC 5000 （ヨーロッパ）
Modacom （ドイツ）
DataTAC 6000 （アジア）
DataTAC/IP
Mobitex（世界）
Mobitex/IP （アメリカ）

プライベート・パケット・ラジオ・ネットワーク:
Dataradio
Motorola プライベート・ラジオ (DataTAC)

衛星ネットワーク:
Norcom
Wireless Matrix

比類のないモバイル・セキュリティ

WebSphere Everyplace Connection Managerは、複数のレベルからなる認証と暗号化によって、ユーザーの特定を行って認証を受けないアクセスを防止し、データのプライバシーを保護する機能を持っています。モバイルVPNオプションに加えて、Connection Managerにはセキュア・ソケット・レイヤ接続、WTLS（Wireless Transport Layer Security）およびPPPクライアントからのPPPプロトコルによるリモートアクセス規格が組み込まれています。鍵の長さが変化する対称的暗号化鍵をエンコードまたはデコードに使用しており、AES（Advanced Encryption Standard）で使用される256ビットの鍵としては最強となっています。データのプライバシーと保護を確実にするために、お客様はDES（Data Encryption Standard）、Triple DES、RC5、AESおよびその他のアルゴリズムを選択することができます。

WebSphere Everyplace Connection Manager は、米国政府および米国軍用のFIPS承認を受けています。

従来のInternet Protocol Security（IPSec）VPNや専用のモバイル用ミドルウェアと比較して、IBMが採用している方法には他に類を見ない利点があります。

概要の比較

モビリティ・クライアント機能	IBM WebSphere Everyplace Connection Manager	従来のIPSec VPN
エンド・ツー・エンドの暗号化	✔	✔
IPおよび非IPネットワーク間のシームレスなクロスネットワーク・ローミング	✔	
非IPネットワークを経由したセキュアなIPルーティング	✔	
ネットワーク・アドレスのトランスレーション	✔	
双方向の二要素認証	✔	✔
ヘッダの軽減、パケットのオーバーヘッドを軽減するためのIPデータ圧縮およびフィルタリング	✔	
ネットワークの待ち時間によって発生するコストのかかる再伝送を最小化して、TCPプロトコルを最適化	✔	
動的な切断/再接続	✔	
接続技術の違いに対する効率調整プロファイルのカスタマイズ	✔	
Microsoft® CE.Net、Windows®、Pocket PC、Win CE、Palm OSおよびLinuxのサポート		

Connection Managerは、 RADIUS（Remote Authentication Dial-In User Service）に準拠した認証サーバーだけでなく、企業のLDAPディレクトリ・サーバーに対するユーザーの確認も行います。共有秘密鍵の強固さを適切に保つために、Connection Managerでは包括的なパスワード運用規則が適用されます。最新のリリースでは二要素認証が強化されており、ユーザーの証明書とハードウェアのシリアル番号やモデムのネットワーク・アドレス、または通話回線識別名などのハードウェアの識別要素を組み合わせるようになっています。 WebSphere Everyplace Connection Managerは、信頼のおける承認機関に対して証明書の情報を照会して、有効なX.509クライアント証明を確認することもできます。

米国政府や米国軍向けのクライアントについては、WebSphere Everyplace Connection Managerは、米国連邦情報処理規格（FIPS）140-2（審議中）、197、46-3、186-2および180-1の規格について承認を受けています。IBMが使用している暗号ライブラリは、ミッションクリティカルな高度なセキュリティ機能を備えたモバイル・アプリケーションを採用する際に重要な要素であるアメリカ合衆国およびカナダ連邦政府機関による試験を受け、承認を受けています。

WebSphere Everyplace Connection Manager の効率的なデータ圧縮によって、データ転送コストを削減できます。

帯域幅の最適化によるコスト削減

最近のテストでは、WebSphere Everyplace Connection Managerは GPRSネットワーク上の有効スループットを60%以上向上させました。これを実現するために、モビリティ・クライアントとConnection Managerは、高度なデータ圧縮とTCP（Transmission Control Protocol）による再転送のバイト数削減と最小化を実装し、データ負荷を軽減し有効帯域幅を拡大しています。このプラットフォームでは、インスタント・メッセージングや巨大なファイルのダウンロード、Webトランザクションなどのセッションの安定性が改善されることも示されました。GPRSサービスの平均料金が月$50で、年間20%ずつ値下げされるとして、200人のユーザーがそれぞれ毎月40メガバイトの通信を行うとすると、最初の1年だけで$75,000のコスト節減になります。

広範なメッセージング・サービス

WebSphere Everyplace Connection Managerの機能の一つであるMessaging Serviceも、幅広いWAP電話やSMS電話、ページャーをサポートする強力なメッセージング・ゲートウェイが組み込まれています。WebSphere Everyplace Connection Manager Toolkitとアプリケーション・プログラム・インターフェイス（API）を使用して、アドレスのタイプを簡単に指定するだけでプッシュ型アプリケーションを作成することができます。Connection Managerは、各ネットワークにおけるメッセージ・エンコーディング固有のプロトコルの複雑な詳細部分やネットワークへの接続が、開発者からは見えないようにします。

これらのメッセージング・サービスはWebSphere Everyplace Accessと強力に統合された補完製品となっています。このプラットフォームには、メッセージング・サービスを利用してプッシュ型警告を行うINS（Intelligent Notification Services）が含まれています。INSは、さまざまな情報源からの情報を監視し、事件の発生を認識して、携帯電話、ページャー、またはPDA（携帯情報端末）を経由して従業員に通知します。たとえば、INSを利用できるサプライ・チェーン用アプリケーションから「在庫切れ警告」を使用して、在庫が一定の水準以下になったときにメッセージを送信することができます。

GPRSネットワーク上のスループットの最適化

データ・タイプ	ファイル・サイズ Kb	WebSphere Everyplace Connection Manager 導入後のファイル・サイズ	削減率	実際のスループット Kb/S
アプリケーション・ログ・ファイル（小）	14	5	64%	45
アプリケーション・ログ・ファイル（小）	291	119	59%	54
アプリケーション・ログ・ファイル（大）	973	318	67%	61
システム設定ファイル	77	32	58%	44
HTML ファイル	2,660	948	64%	55

従業員200人に対する総節減額 = $75,000（1年目）

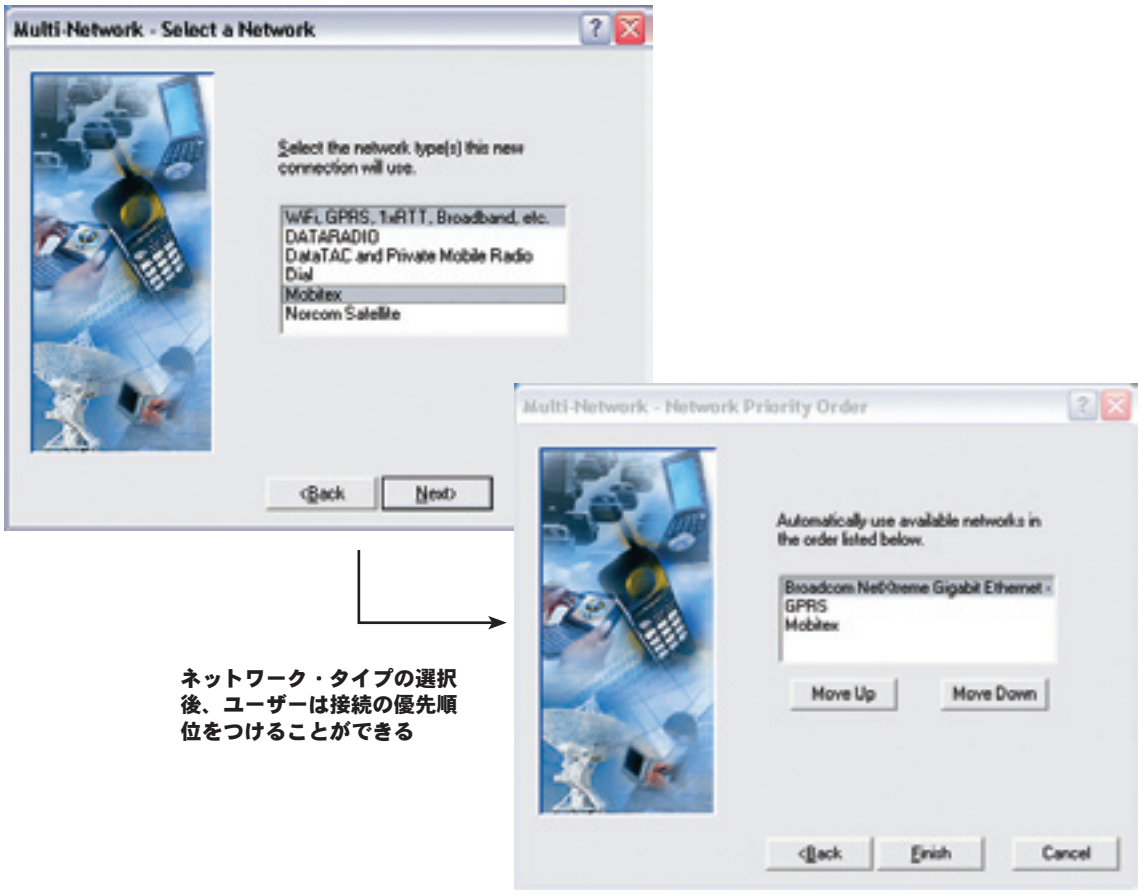
条件	
実際のスループットの平均増加幅	63%
モバイル環境を使用する従業員の数	200
1カ月あたりのモバイル・データ通信量の予測（MB）	40
モバイル・データ通信利用の増加予測	0%
毎月の料金（AT&TワイヤレスGPRS）	$50
年間のデータ通信料金の値下げ幅	20%

WebSphere Everyplace Connection Manager は、連続するワイヤレス・ネットワーク・アクセスによって、途切れない通信とデータの保護、そして生産性の向上をモバイル環境のユーザーにもたらします。

ユーザーの経験の強化

ネットワークの選択を簡単に行うために、WebSphere Everyplace Connection Manager Version 5.0は、優先順位をつけたリストからユーザーが選択を行える強力なグラフィカル・ユーザー・インターフェイス を備えています。優先順位のより高い接続が利用できるようになったときには、WebSphere Everyplace Connection Managerが自動的にそれを検出してネットワークを切り替えます。新しい接続が見つかったときは、モビリティ・クライアントがユーザーに問い合わせを行い、新しいネットワーク・インターフェイスを動的に定義してオプションに加え、優先順位に従ってインターフェイスを開いて接続を切り替えます。

ローミングに使用するネットワークの優先順位付け



ネットワーク・タイプの選択後、ユーザーは接続の優先順位をつけることができる

アーキテクチャ

WebSphere Everyplace Connection Managerは、モバイル環境のユーザーがe-businessソリューション、つまりあらゆるIPベースのアプリケーションを拡張して、安全かつ効率的に使用できるようにする無線および有線によるモバイル・アクセスの完全なプラットフォームです。このアーキテクチャは、複数のベンダーのハードウェアやオペレーティング・システムのプラットフォーム上で動作するようにそれぞれ設計されたConnection Managerサーバー、モビリティ・クライアントおよび分散管理という3個の別個のコンポーネントで構成されています。

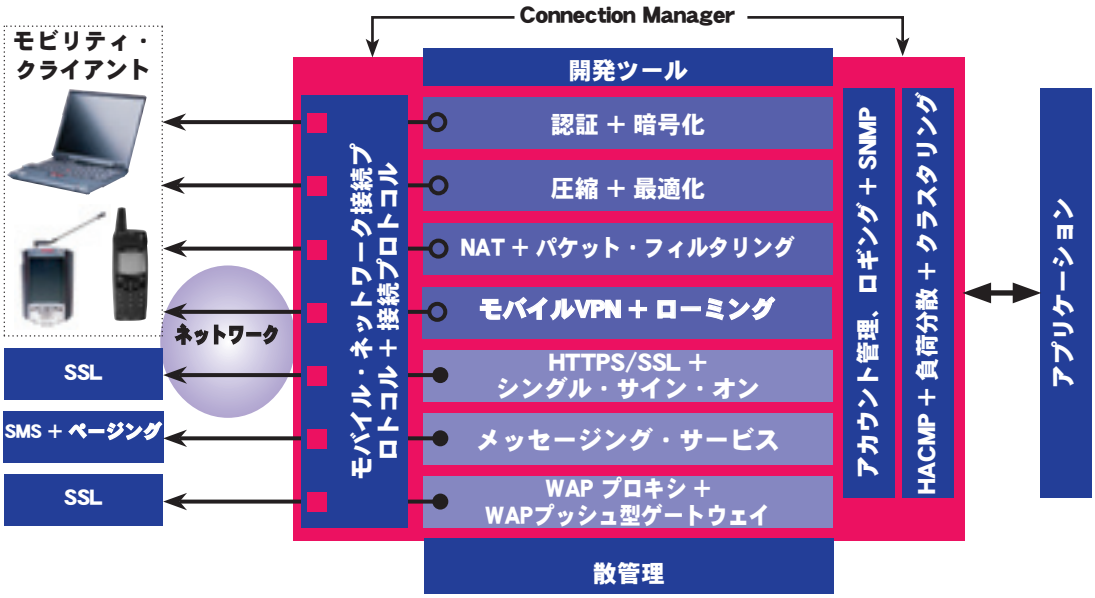
モビリティ・クライアント

モビリティ・クライアントは機器上でローカルに実行され、最適なモバイルVPNを確立してクロスネットワーク・ローミングを可能にします。モビリティ・クライアントがConnection Managerに対して認証されると、VPNが確立され機器は安全に企業のイントラネットに接続されます。

モビリティ・クライアントには、ネットワーク認識アプリケーションを作成するためにツールキットおよびAPIが含まれています。たとえばアプリケーションの1つのタイプとして、接続のタイプやコスト、帯域幅に基づいて転送するデータのタイプを正確に選択するものがあげられます。Wi-Fi信号の強さを監視して、GPRS接続を開始してWi-Fi接続が切断される前にGPRS接続を開始するアプリケーションもあります。

Connection Manager

Connection Manager は、5ページの表にあるように、IPおよび非IPネットワークの両方の通信プロトコルを幅広く包括的にサポートします。パブリックまたはプライベートな物理ネットワークの任意の組み合わせについて複数のモバイル・ネットワーク接続（MNC）の設定を行うことによって、柔軟なコネクティビティを実現しています。従来のVPNと異なり、通信テクノロジによって異なる待ち時間、接続速度やその他の特性を補って最適な性能を実現できるように、各MNCを調整することができます。



モバイル・ネットワーク・インターフェイスとIPアドレス

WebSphere Everyplace Connection Managerは、オペレーティング・システムがサポートされているすべての無線、ダイヤルまたは有線ネットワークとIP層での通信を行うときに使用するモバイル・ネットワーク・インターフェイス（MNI）も実装しています。このプラットフォームは、適切なMNIを経由してトラフィックのルーティングが行われているユーザーの1個以上のIPサブネットをコントロールします。IPアドレスは固定のものが割り当てられるか、動的に割り当てられたアドレス群をサポートする動的ホスト設定プロトコル（DHCP）によって割り当てられます。

WebSphere Everyplace Connection Manager ***の各ネットワーク・インターフェイスは、トラフィックの流れをコントロールするために微調整を行うことができます。***

データのトラフィックを削減してコントロールするために、各MNIをパケット・フィルタリングまたはパケット・マッピングによってカスタマイズすることができます。内蔵のネットワーク・アドレス翻訳機能によって、乏しい企業のIPアドレスを管理し、実際のIPアドレス1個に対して64,000までのモビリティ・クライアントのアドレスを割り当てられるように拡張します。

HTTP/HTTPSアクセス・サービス

SSL機能のあるブラウザを持つ機器については、Connection Managerはセキュアでないハイパーテキスト転送プロトコル（HTTP）と、セキュア・ソケット・レイヤ上で認証を行うハイパーテキスト転送プロトコル（HTTPS）接続の両方をサポートしています。Webサーバーやポータル・サイト上でシングル・サイン・オンを可能にするために、WebSphere Everyplace Connection Manager Version 5.0では軽量なサードパーティの認証トークンのサポートが追加されています。

メッセージング・サービス

Connection Managerには、さまざまなサービス・プロバイダの接続オプションを実現する幅広いメッセージング・サービスが含まれています。多様なプロトコルによって、ショート・メッセージングおよび単方向または双方向メッセージングのニーズが幅広くカバーされています。

- SMPP — X.25およびTCP/IP上のShort Message Peer to Peer
- UCP — X.25およびTCP/IP上のUniversal Computer Protocol
- WCTP — TCP/IP上のWireless Communication Transfer Protocol
- SNPP — TCP/IP上のSimple Network Paging Protocol
- SMTP — TCP/IP上のSimple Mail Transfer Protocol
- WAPプロキシ・サービス

WAP プロキシとプッシュ型プロキシ・ゲートウェイ

オプションとして、WebSphere Everyplace Connection ManagerにはWAP 1.2.x準拠のWAPプロキシおよびプッシュ型プロキシ・ゲートウェイを組み込むことができます。

分散管理

1つまたは複数のConnection Managersの管理は、Javaのリモート・コンソールとIBM WebSphere Portal Serverのポートレットで簡単に行うことができます。複数レベルの管理者権限の委任や個別のアクセスまたは変更に対する許可を定義することができ、組織のニーズに柔軟に対応することができます。

すべての管理および設定データは、共通のLDAP（Lightweight Directory Access Protocol）ディレクトリに保管されます。Remote Gatekeeper管理は、SSL接続上で拡張マークアップ言語（XML）を経由してConnection Managersとセキュアな通信を行います。

推奨事項

データ通信を利用するときには、ネットワークの選択肢とセキュリティの脆弱性が大きくなるため、企業は通信アーキテクチャを単純化して、コストを削減して企業のセキュリティ政策を徹底する必要があります。WebSphere Everyplace Connection Managerのメリットを活用するために、企業はモバイル環境を実現してユーザーの接続を管理する上で、計画について5つの点を考慮する必要があります。

1. 現行の無線接続のセキュリティ・レベル、リスク、接続に関する課題、ユーザーの挙動やモバイル環境にかかるコストに対する評価を実施する
2. 適切なモバイル・アーキテクチャ、セキュリティの原則、コスト目標およびネットワークの選択肢を定義する
3. ネットワーク、機器、アプリケーションおよびユーザーのニーズについて、現行および将来の両方についてモデル化する
4. 展開の方法について、エンド・ツー・エンド通信プラットフォームとパッチワーク・アーキテクチャを比較する
5. 製品の機能、パートナーシップ、将来の見通し、財政面の安定性およびサービスについての技術について、優れたベンダーと手を組む

まとめ

コストを削減しながら生産性を向上させるというプレッシャーの中で、ローミングとセキュリティ、そしてネットワーク間の最適化がコネクティビティの基本的な条件として浮上してきています。IBMのプラットフォームによって、従業員が場所やネットワークを変えたときでも、セキュアで暗号化されたセッションを維持できるシームレスなコネクティビティが実現できます。

ワイヤレス環境によるe-businessのリーダーであり、170カ国に150,000人のグローバル・サービス・プロフェッショナルを持つIBMは、お客様の無線LAN、パブリックWLANおよびシームレスなローミングを支援します。IBMは、サービス・プロバイダだけでなく、企業がワイヤレス・ネットワークを展開してシームレスでセキュアなローミングを従業員や顧客に対して提供する場合にもお手伝いさせていただきます。

詳しくは

IBM パーベイシブ・コンピューティングとWebSphere Everyplace Connection Managerの詳細ついては、次のURLを参照してください: **ibm.com**/software/pervasive/products/mobile_sols/connection_manager.shtml

IBM Corporation
Department LG9A
8051 Congress Avenue
Boca Raton, Florida 33487

Produced in the United States of America
04-03