Development Reports

「IPルータ網」の構成技術
－L2/L3統合VPNバックボーンの概要－

IMT-2000方式（FOMA）や公衆無線LANのサービス（Mzone）開始に伴いデータ通信需要が高まる中，低コストで多種多様なシステムからの接続要望に応えられる通信網基盤の構築が急務となってきた．

「IPルータ網」は，上記要望を満たすことをねらいに導入された基幹データ通信網であり，広域イーサネットとIP-VPNサービスの特徴を併せ持つVPNバックボーンである．

大崎 憲嗣（おおさき けんじ） 前田 吉功（まえだ よしのり）
守屋 裕三（もりや ひろみつ） 下川 真由子（しもかわ まゆこ）

1. まえがき

公衆無線LAN（Local Area Network）サービスMzoneの開始やFOMA（Freedom Of Mobile multimedia Access）の普及に伴い，データ通信需要が高まる中，FOMAパケットトラヒックやMzoneのトラヒックを始めとする多種多様なデータ系トラヒックの増大に対応可能な，低コストでより高速・大容量の通信網基盤の構築が要望されている．

上記要望を満たすIP（Internet Protocol）ルータ網の構築には，主として以下の条件が要求される．

(1) IPトラヒック転送

増大するIPトラヒックを高速に，しかも安価に転送できること．

(2) 論理網分離重畳

FOMAパケットトラヒックやMzoneトラヒックなどの異なるネットワークを収容するため，またセキュリティやユーザの利便性を確保するため，本ネットワークにおいて閉域性を担保しつつユーザごとの論理網を1つの物理網上に多重できること．

(3) 重要トラヒックの品質保証

iモードサービスなどの重要トラヒックを伝送するため，帯域保証などによる伝送品質の保証ができること．

(4) 信頼性確保

サービス停止時間の短縮化のため，網内が冗長化構成されていること．

(5) 非IPトラヒックのレイヤ2転送

広域イーサネットサービス，非同期転送モード（ATM：Asynchronous Transfer Mode）などが提供できること．

● Development Reports ●

(6) 多様な接続形態

ギガビットイーサネット（GbE：Gigabit Ethernet），ファスト・イーサネット（FE：Fast Ethernet），POS（PPP Over SONET），ATMなどの接続インタフェースが提供できること．

また，IPルータ網の構築設計においては，市販製品の活用による低コスト化，およびインターネットに見られるようなIP技術の急速な進歩への迅速かつ柔軟な対応が重要となるため，標準的な技術の適用を基本方針とした．本稿では，IPルータ網の構成技術について概説する．

2. 要求条件に対する検討結果

2.1 伝送網条件

今後予測されるデータトラヒック需要の増加に対応するため，物理伝送路網は光ファイバの利用を前提とする．ドコモの伝送路の主流であったマイクロ波伝送から光伝送への転換により，劇的な大容量化と低コスト化が実現可能となる．

2.2 物理網条件（物理トポロジ）

検討段階で考慮したIPルータ網の物理構成（トポロジ）を**図1**に示す．図1の各トポロジに対してコスト，信頼性などの検討を行った結果，信頼性においては各トポロジ間で大差がなく，FOMAパケットトラヒックおよびMzoneのトラヒックが東京に集中することを考慮した場合に，最もコストメリットのあるトポロジが各地域会社から東京に接続されるトポロジ（中央集中スター型トポロジ）であることが明らかとなり，この網構成を採用することとした．

3. 網構成技術の概要

3.1 基本網方式

IPルータ網内では，仮想閉域網（VPN：Virtual Private Network）により，複数ユーザ／システム間を論理的に分離する構成とした．IPルータ網には，複数ユーザ／システムを重畳して効率的に収容することが求められるが，その際，同じIPアドレスを使用する可能性のある複数ユーザを重畳して収容すること，重畳して収容した複数ユーザの通信データのセキュリティを確保すること，などが必要になるためである．

また，IPルータ網は，さまざまなユーザが収容されるネットワークであり，高い可用性の確保が要求されるため，ネットワークを構成する装置や伝送路に障害が発生した場合の迂回路を確保し，サービスが継続できるようにすることが必要である．そこで，ネットワークのコア部分では冗長構成を取ることとした．

ネットワークの基本構成および動作概要を**図2**に示す．ユーザ網はエッジルータ（ER：Edge Router）あるいは集約スイッチ（ISW：Intensive SWitch）と呼ばれる装置に収容される．ユーザトラヒックはネットワーク内をVPN経路に従って伝達され，再びエッジルータあるいは集約スイッチ装置からユーザ網へ出力される．

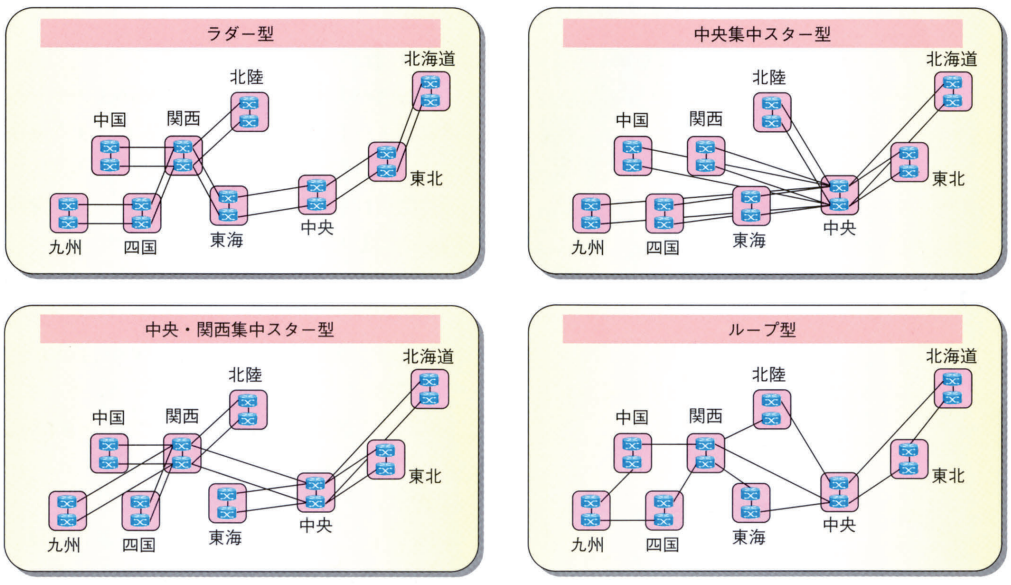
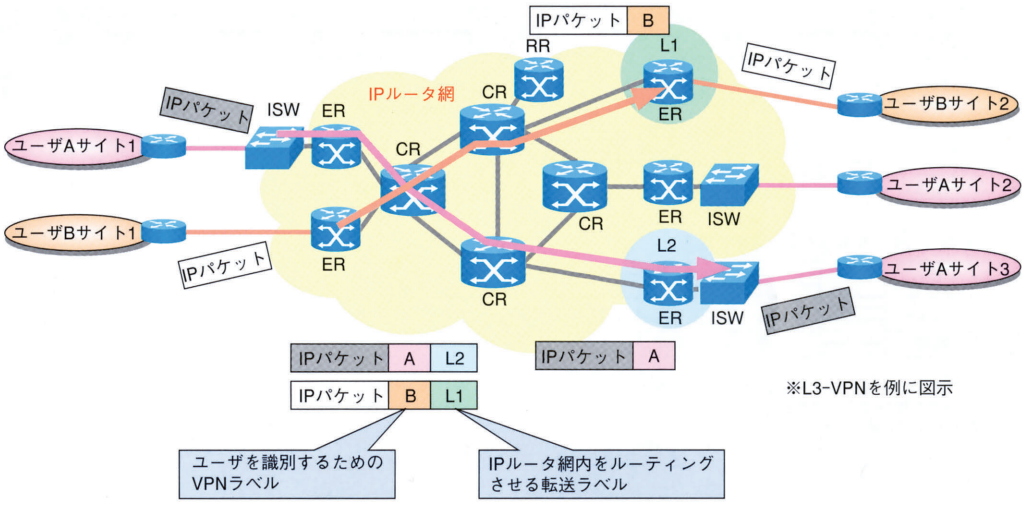


図1 物理トポロジの例



CR（Core Router，コアルータ）：MPLS高速ラベル転送を実行
ER（Edge Router，エッジルータ）：ユーザ宛先アドレスとラベルの対応付け，L2-VPN，L3-VPN収容を実行
ISW（Intensive SWitch，集約スイッチ）：低速回線を集約し高速のアップリンクにまとめてエッジルータに収容
RR（Route Reflector，ルートリフレクタ）：L3-VPNユーザ経路を一元管理

図2 ネットワーク構成および動作概要図

3.2 MPLSの適用

VPNの実現方式としてMPLS仮想閉域網（MPLS-VPN：Multi-Protocol Label Switching-Virtual Private Network）方式を採用した．MPLSは，通常のIPルーティングとは異なり，ラベルと呼ばれる付加情報でデータパケットをカプセル化して伝達するため，ユーザデータ間をセキュアに分離できる（図2）．また，3.3節で述べるレイヤ2仮想閉域網（L2-VPN：Layer 2 VPN）とレイヤ3仮想閉域網（L3-VPN：Layer 3 VPN）の両方のサービスが同じ物理網で提供できる．現在MPLSに関しては，トラヒックエンジニアリング，マルチなサービス品質（QoS：Quality of Service），IPv6（Internet Protocol version 6）対応，マルチキャスト，保守運用（OAM：Operation And Maintenance），さらにはGMPLS（Generalized Multi-Protocol Label Switching）などの検討が進められており，ネットワークへの適用に向けたMPLSの技術拡張[1]が期待できる．

3.3 VPN方式

VPNには用途に応じて以下に述べる2通りの方式がある．

(1) L2-VPN

L2-VPNは，ユーザサイト間をポイント・ツー・ポイント（P-P：Point to Point）形態で接続する仮想専用線サービスの提供に対応する．

イーサネットの場合のプロトコルスタックを図3に示す．

L2-VPNは，地理的に離れたユーザサイト間をあたかも1つのLANであるかのように接続するものである．この方式では，IPプロトコル以外のデータ通信が可能である．また，IPプロトコルの場合でもユーザ経路情報は網内透過転送されるため，ユーザはルーティングプロトコルなどを自由に設計することができる．

(2) L3-VPN

L3-VPNは，ユーザサイト間をポイント・ツー・マルチポイント（P-MP：Point to Multi Point）形態で接続する網加入型サービスの提供に対応する．

イーサネットの場合のプロトコルスタックを図3に示す．

L3-VPNは，地理的に離れたユーザサイト間をIPルーティングにより接続するものである．BGP（Border Gateway Protocol）/MPLSによる方式では，ユーザ側に特別なVPN機器を必要としない．また，IPルータ網ではユーザ側IPアドレスはユーザごとに分離管理されるため，プライベートアドレスも使用可能である．VPN（ユーザ）間の通信はルータ装置内および網内で分離され，ATMやフレームリレーと同様のセキュリティが確保できる．

また，ユーザ網同士を接続する際のルーティングはIPルータ網が行うため，ユーザはIPルータ網にユーザ網を接続するだけで，複数のユーザ網を結ぶネットワークを構築することができる．ユーザ網とIPルータ網とのルーティング情報のやりとりは，BGP4（Border Gateway Protocol version 4）やオープンSPFプロトコル（OSPF：Open Shortest Path First）のように動的に，あるいは固定

● Development Reports ●

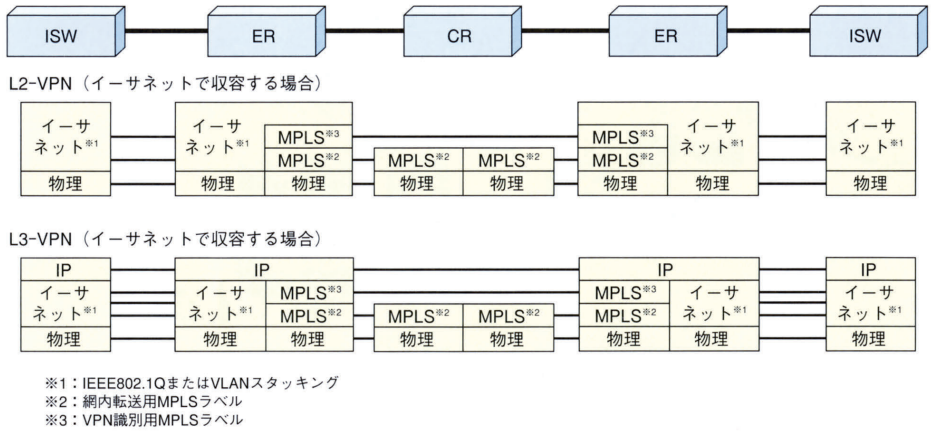


図3 L2/L3-VPNプロトコルスタック

的に行うことも可能である．

IPルータ網内では，ユーザパケットはVPNごとのMPLSラベルによってカプセル化され，VPNごとの経路情報はエッジルータ内で分離して管理される．

3.4 ユーザ網収容例

ユーザ網収容方式の決定にあたり，IPプロトコル以外のデータ通信の要否やサイト間の通信形態（P-P型通信／P-MP型通信），既存システムからの移行の場合には，新規にIPアドレス体系の設計し直しが許容されるか否か，などのさまざまな条件を考慮し，最適なVPN方式を決定する必要がある．

(1) L2-VPNの適用例

・xGSN～EMS回線（**図4**）

既設のネットワーク設備（NE：Network Element）の管理システム（EMS（network Element Management System））側には，ベンダ独自ルーティングプロトコルのEIGRP（Enhanced Interior Gateway Routing Protocol）を運用している．これをIPルータ網内透過転送するため，VPN方式はL2-VPNとする必要がある．また，第3世代移動通信（IMT-2000：International Mobile Telecommunications-2000）用パケット処理装置のxGSN（Serving/Gateway GPRS Support Node）への監視制御回線には，信頼性が要求される一方で，帯域はそれ程必要とされない．そのため，中低速回線をISWにて集約しIPルータ網へ接続する形態が適している．

・xGSN～企業LAN回線（**図5**）

一般的に企業LAN内のアドレス体系の見直しは許容されないため，VPN方式はL2-VPNとする必要がある．また，L2-VPNの場合は，ISW収容形態であってもユーザ付与の仮想LAN（VLAN：Virtual LAN）タグ

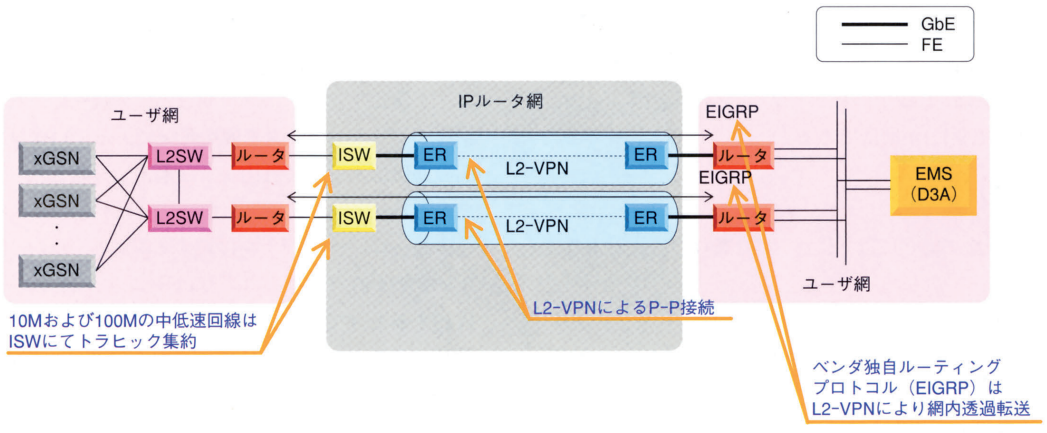


図4 xGSN～EMS回線

を網内透過転送する機能を有しており，各企業LANからの回線をIPルータ網の手前にて集約する形態が適している．

(2) L3-VPNの適用例（図6）

xGSN間の通信は一対多型の通信形態となるため，P-MP型のフルメッシュ構成とする必要がある．また，新規システムであり既存IPアドレス体系を見直す必要もないため，L3-VPNが適している．

また，IPルータ網の持つ網内冗長化構成と障害時自動迂回機能に加え，IPルータ網へマルチホーミング接続し，動的ルーティングプロトコル（BGP4）を適用することで，信頼性の向上を図っている．

4. 網管理装置の概要

IPルータ網を効率的に運用するための網管理として，以下に示す機能要件を満たす必要がある．

①保守者がIPルータ網のIP機器が故障した時に発するALM（ALarM）を把握できること．さらに，故障したIP機器が収容しているユーザごとのサービス影響を把握できること．

②IP機器の使用状況を把握するため，IP機器単位にトラヒック管理ができること．さらに，サービス品質管理という観点で，サービスごと，遅延時間，揺らぎなどのトラヒックも管理できること．

③IP機器に登録されている構成情報（config）の管理が

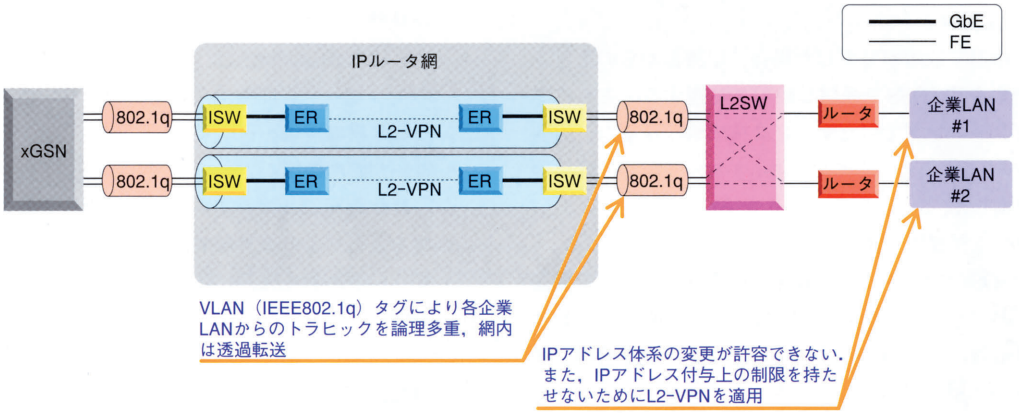


図5 xGSN～企業LAN回線

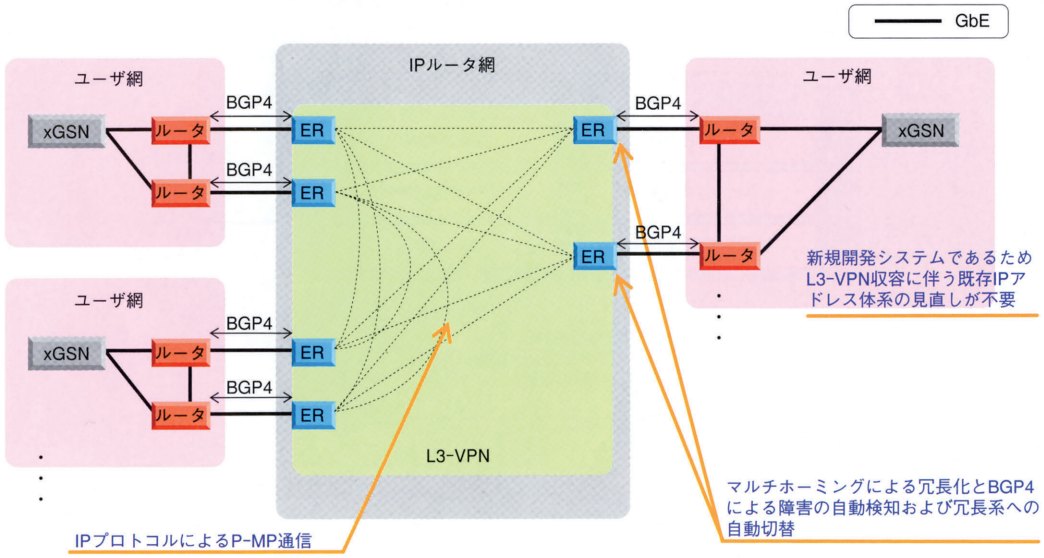


図6 xGSN～xGSN回線

● Development Reports ●

できること．

④保守センタから，遠隔でIP機器を制御できること．

⑤VPN網設計において，収容ユーザシステムにより異なるL2-VPN，L3-VPNのプロビジョニングが容易であること．

⑥計画・建設・保全業務を効率化するため，網構成情報，configデータなどの各種情報を一元管理する必要があるが，作業者による，情報設定／変更操作に対し，誤操作防止が図られていること．

⑦コストの低減，市販機能の有効利用が図れること．

以上の機能要件を満足する網管理装置のIP-OSS（IP-Operation Support System）（**図7**）の開発を行った．以下にIP-OSSの機能概要を示す．

①ALM監視機能：

IP機器で故障が発生した場合，IP機器からのトラップ情報をIP-OSSで受信し故障を監視する．さらにプロビジョニングで得たサービス構成情報を基に，VPN単位の故障状況を保守者へ通知するサービス故障管理を具備した．

②トラヒック収集機能：

IP-OSSでIP機器のMIBを収集することで，IP機器個々のトラヒックを収集・管理する．さらにサービス構成情報によりVPN単位のトラヒック状況を管理，またIP-OSSからルータに対し，エンド・ツー・エンド（E2E：End to End）の試験を実施することで，遅延時間，揺らぎなどのトラヒックも管理可能とした．

③設備構成管理：

IP-OSSに登録したIP機器ごとのconfigを原本とし，configを変更する場合はIP-OSSからデータをIP機器に投入する方式にすることで，configの一元管理を具現化した．

④遠隔制御機能：

IP機器へのアクセスはIP-OSSからのみを許容させることにより，セキュリティを強化した．

⑤VPN網設計機能：

プロビジョニングは，個々のIP機器に直接コマンドを投入することはせず，トポロジマップ上でのグラフィカルユーザインタフェース（GUI：Graphical User Interface）で設定できる機能を実現することで，誤操作防止を図るとともに，操作性を向上させた．また，構成情報を基にVPNサービスごとに冗長化された経路の状態を管理および表示することを可能とした．また，VPN網設計機能は，サービス監視機能，VPN単位のトラヒック管理機能などを実現するために必要なサービス構成情報を管理する．

⑥ユーザ管理機能：

操作画面ごとに，業務に応じた操作権限を設定管理することにより，外部者による誤操作，誤設定による網への悪影響を未然に防止するとともにセキュリティを強化した．

IP-OSSの管理対象装置は，市販品ベースのIP機器である．IP機器とのインタフェースを業界標準（SNMP，FTPなど）で実現することで，市販製品が有効利用できるとともにIP-OSS上のアプリケーションも市販製品をベースと

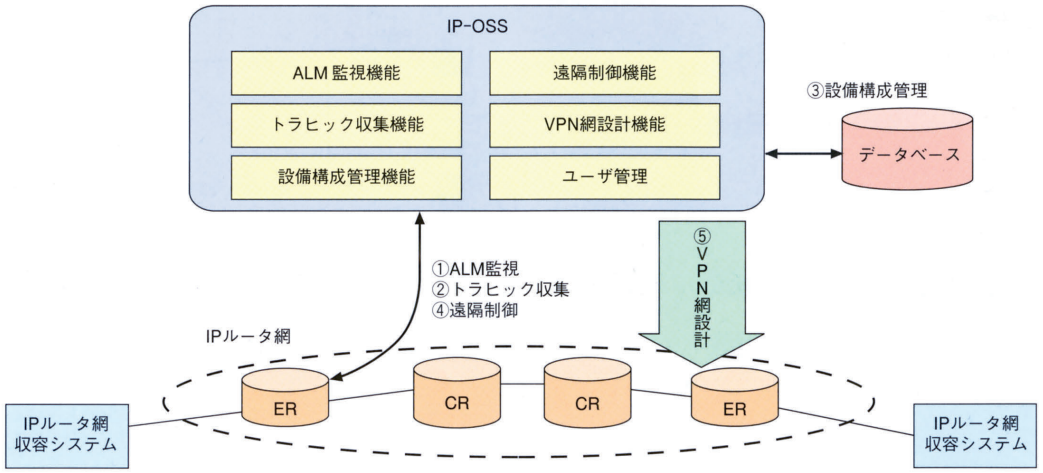


図7 IPルータ網管理装置（IP-OSS）概要図

してドコモの網管理のための差分機能のみを開発することにより，開発規模削減および開発期間の大幅な短縮を可能とした．また，ドコモ開発機能も市販ソフトに直接プログラムを書き込むのではなく，市販ソフトのアドオンソフトとして開発することで，今後の標準化動向により新しい管理機能が必要になったとき，市販製品を利用した柔軟な機能盛り込みを可能とした．

5. あとがき

本稿では，IPルータ網構築の背景，網管理装置を含めた網構成技術の概要を述べた．今後は，移動通信網のIP化に向け，データのみならず音声を含めたマルチメディア系トラヒック需要に対応するため，高可用性のさらなる追及とQoS機能の強化・本格運用の検討を進める．また，キャリアの通信網基盤としてふさわしいIPネットワークを構築すべく，IP^2 (IP based IMT network Platform) [2]の転送網への展開も視野に入れた検討を進めていく予定である．

文　献

[1] IETF MPLS (Multiprotocol Label Switching) Working Group: http://www.ietf.org/html.charters/mpls-charter.html
[2] 今井，ほか：“モバイルネットワークALL-IP化特集，”本誌，Vol. 10，No. 4，pp. 6-34，Jan. 2003.

用 語 一 覧

ALM：ALarM
ATM：Asynchronous Transfer Mode（非同期転送モード）
BGP：Border Gateway Protocol
BGP4：Border Gateway Protocol version 4
CR：Core Router（コアルータ）
EIGRP：Enhanced Interior Gateway Routing Protocol
EMS：network Element Management System
ER：Edge Router（エッジルータ）
FE：Fast Ethernet（ファースト・イーサネット）
FOMA：Freedom Of Mobile multimedia Access
FTP：File Transfer Protocol（ファイル転送プロトコル）
GbE：Gigabit Ethernet（ギガビットイーサネット）
GMPLS：Generalized Multi-Protocol Label Switching
GPRS：General Packet Radio Service
GUI：Graphical User Interface（グラフィカルユーザインタフェース）
IMT-2000：International Mobile Telecommunications-2000（第3世代移動通信）
IP：Internet Protocol
IP^2：IP based IMT network Platform（読み：アイピースクエア）
IP-OSS：IP-Operation Support System
IPv6：Internet Protocol version 6
IP-VPN：IP-Virtual Private Network（IP仮想閉域網）
ISW：Intensive SWitch（集約スイッチ）
L2-VPN：Layer 2 VPN（レイヤ2仮想閉域網）
L3-VPN：Layer 3 VPN（レイヤ3仮想閉域網）
LAN：Local Area Network
MIB：Management Information Base
MPLS：MultiProtocol Label Switching（マルチプロトコル・ラベルスイッチング）
MPLS-VPN：MPLS-Virtual Private Network（MPLS仮想閉域網）
NE：Network Element（ネットワーク設備）
OAM：Operation and Maintenance（保守運用）
OSPF：Open Shortest Path First（オープンSPFプロトコル）
P-MP：Point to MultiPoint（ポイント・ツー・マルチポイント）
POS：PPP Over SONET
P-P：Point to Point（ポイント・ツー・ポイント）
PPP：Point to Point Protocol
QoS：Quality of Service（サービス品質）
RR：Route Reflector（ルートリフレクター）
SNMP：Simple Network Management Protocol（簡易ネットワーク管理プロトコル）
SONET：Synchronous Optical NETwork
VLAN：Virtual LAN（仮想LAN）
VPN：Virtual Private Network（仮想閉域網）
xGSN：Serving/Gateway GPRS Support Node