New Technology Report

移動通信網へのIP技術とOpenAPI技術の適用評価 ～All-IP実験結果～

移動通信網のIP化に関する技術的実現性を評価するため，コアネットワーク部分に最新IPネットワーク機器を適用したシステム実験（All-IP実験）を実施した．

本稿では，実験における主要な3つの技術分野，すなわちMobile IP技術，IP呼制御/IP-QoS技術，Open API技術に関する評価結果の概要を報告する．

石井 健司　岡川 隆俊　佐藤 恭
大迫 陽二　檜山 聡

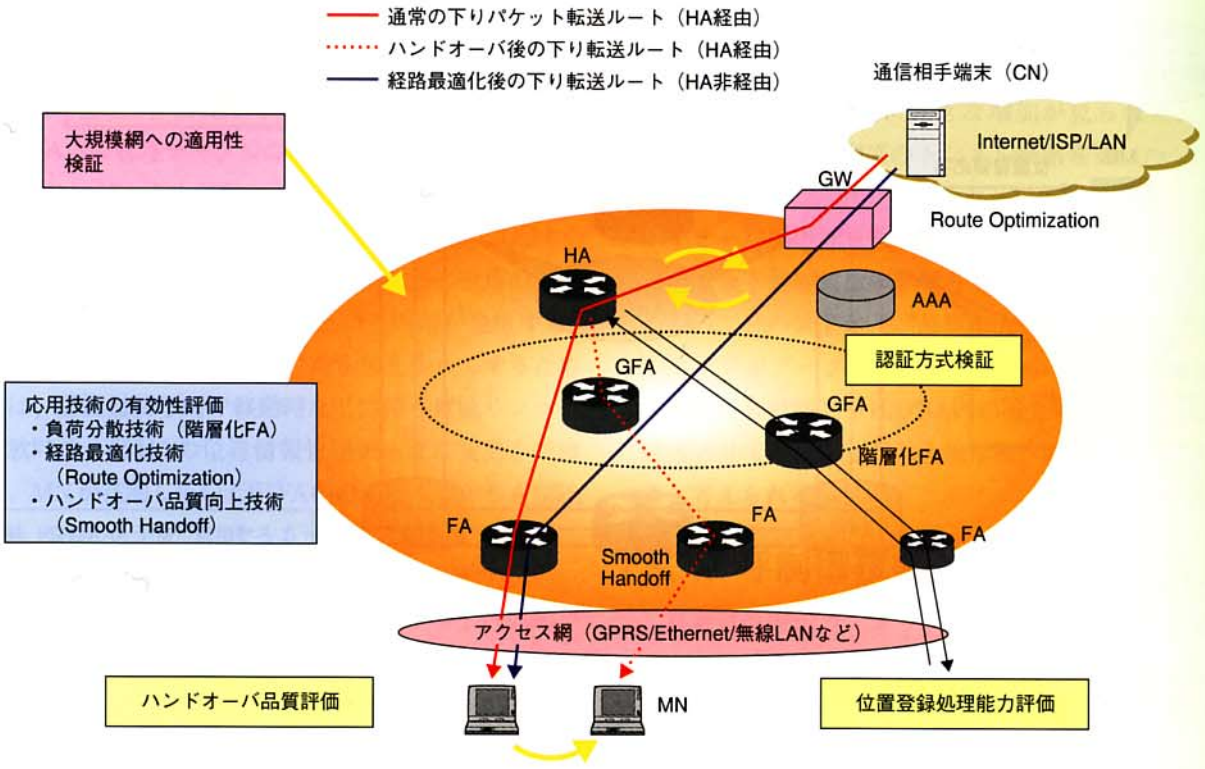
1. まえがき

移動通信網において，iモードなどのインターネットアクセスサービスの爆発的普及によりIPトラヒックが急激に増加しており，IP技術をベースとした新たな通信方式の検討が急務となってきている．3GPPなどの標準化団体において，ネットワークのIP化を目指した検討が積極的に進められているが，まだ多くの課題がある．特に移動通信網においては，次のような技術を評価することがIP系技術の適用性や有効性を検証するうえで重要と考えられる．①移動時の加入者認証や移動追跡といったモビリティ制御をIPレイヤで実現するMobile IP技術，②音声通信を含むIPマルチメディア通信サービスを実現するためのIP呼制御技術とIP-QoS技術，および③サービス制御インタフェースをオープンにすることでネットワーク機能を活用した各種付加サービス開発を迅速化するOpen API（Open Application Programming Interface）技術．これらの主要技術の検証を目的として，コアネットワーク部分に最新のIPネットワーク機器を用いた実験システムを構築し，各種の評価実験を実施した[1]．なお，本実験は日本電信電話㈱ネットワークサービスシステム研究所の協力を得て共同で行った．

本稿では，この実験結果の概要を報告するとともに，各分野における技術完成度の考察や今後の課題について述べる．

2. Mobile IP技術

IP技術をベースとした移動通信網を検討するにあたり，



AAA：Authentication Authorization Accounting
CN：Correspondent Node
FA：Foreign Agent
GFA：Gateway Foreign Agent
GPRS：General Packet Radio Service
HA：Home Agent
ISP：Internet Service Provider
LAN：Local Area Network
MN：Mobile Node

図1　Mobile IP技術における検証のポイント

従来の移動通信網における移動端末の電話番号を用いたHLR（Home Location Register）による移動管理ではなく，移動端末のIPアドレスを用いた位置情報管理や，移動時にも通信を継続させるためのハンドオーバ制御および加入者認証／アクセス認証などを実現するためのIPモビリティ制御方式の確立が重要となる．IPモビリティ制御を実現する技術の候補として，IETF（Internet Engineering Task Force）で提案されているMobile IP技術がある[2]．Mobile IPを用いることにより，移動端末のIPアドレスを保存したままでの移動が実現でき，移動通信網内のモビリティ制御への適用だけではなく，無線LAN（Local Area Network）などの異なるアクセス網間のローミングサービスの提供も期待できる．

今回の実験では，

① Mobile IP技術を用いた認証方式の検証

② Mobile IPの大規模網への適用性の検証
（位置登録処理能力評価／ハンドオーバ品質評価）

③ Mobile IP応用技術の有効性評価

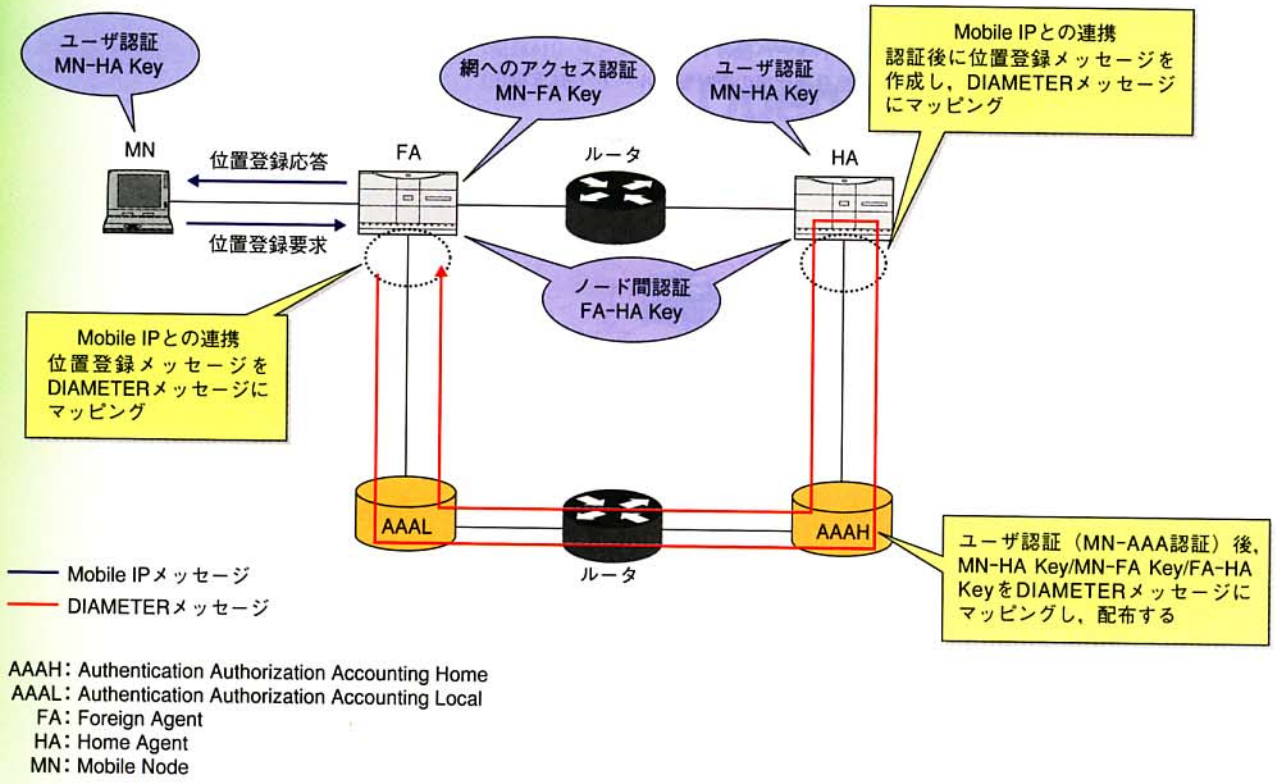
の3つの観点から検証実験を行った（図1）．

本稿では，上記のうち①と②についてその評価ポイントおよび結果を紹介する．

2.1　Mobile IP技術を用いた認証方式の検証

(1)　実験内容と評価ポイント

Mobile IPでは，本来オープンなインターネットでの適用を想定しているため，Mobile IP端末であるMN（Mobile Node），MNの位置情報を管理するHA（Home Agent），移動先でのMNを管理するFA（Foreign Agent）との間で位置登録などの制御メッセージの送受信を行う際に，各ノード（MN/HA/FA）の成り済ましおよびメッセージの改ざん防止のための認証方法が規定されている[2]．その方法では認証を行うノード間で認証鍵を共有し，この鍵を用いて暗号／復号化した演算値を互いに照合することにより，認証を行う．ところが，移動通信網では端末が移動することが前提となるため，網が大規模になるとMNを認証する可能性のあるすべてのノードに対して，あらかじめ共有鍵を設定するのは運用上困難となる．その解決方法として，加入



AAAH：Authentication Authorization Accounting Home
AAAL：Authentication Authorization Accounting Local
FA：Foreign Agent
HA：Home Agent
MN：Mobile Node

図2　位置登録手順と連携させた認証Keyの配布方法

者情報などの管理を司るAAA（Authentication Authorization Accounting）で認証鍵を管理し，位置登録手順とAAAによる加入者認証（MN-AAA認証），および認証が必要なノードへの認証鍵配布処理を連携させる方法が検討されている（**図2**）[3][4]．実験では，認証鍵の配布処理やHA/FA/AAA内における認証処理，認証鍵管理のための処理負荷増に起因する位置登録処理能力への影響を検証した．

(2)　結果と結論

実験では，次世代移動通信（IMT-2000：International Mobile Telecommunications-2000）規模の位置登録頻度に対する位置登録応答時間を測定した．その結果，位置登録処理とAAAによる認証処理の連携時において，HA/FA/AAA内の認証処理負荷により，登録応答時間は著しく増加した．その原因として各ノード内における鍵管理テーブルの検索方法に問題があることが分かった．その改善方法としてはハッシュ関数などを用いたテーブル検索の高速化や認証鍵のライフタイム減算周期の見直しなどにより，位置登録時間を大幅に短縮させる方法が考えられる．

2.2　Mobile IPの大規模網への適用性の検証

(1)　実験内容と評価ポイント

IMT-2000パケット網におけるコアネットワーク程度の大規模網にMobile IPを適用することを想定し，以下に示すMobile IP処理能力評価の実験結果を考察することにより，Mobile IPにおける方式上／実装上の処理ネックの明確化およびその改善方法の提言を行った．

(2)　結果と結論

①　位置登録処理能力の評価

位置登録処理に関しては，現状のFA/HA内の実装技術改善により，IMT-2000規模の大規模トラヒックを処理することが可能であることが分かった．Mobile IPを移動通信網へ適用した場合の方式上の問題点と，その解決案および位置登録時間を削減させるための実装技術の改善方法を以下に述べる．

・Mobile IP方式上の問題点とその解決方法

Mobile IPでは，位置情報を管理しているHAに対してMNが在圏位置を登録することにより移動追跡を実現している．位置登録メッセージを受信したHA/FAでは，それぞれ保持している位置情報管理テーブルにMNの在圏情報の追加／変更を行う．テーブルに追加されたMNの位置情報はライフタイムと呼ばれるタイマーによって管理されており，タイマーが満了するとMNの情報は消去される（ソフトステート管理）．そのため，MNはタイマーが満了する前にHA/FAに対し周期的に位置登録を行うことにより，位置情報のライフタイム更新を行っている．この周期登録を頻繁に行う

と無線リソースの圧迫やHA/FAに対する処理負荷が増加する問題が発生することが予想されるため，周期登録をなるべく行わないようにライフタイム値を長く（ほぼ無限大で）設定する方法が考えられる．この場合，FA内の管理テーブルのライフタイムが長くなるため，MNがFA間を移動した後に旧FA内に不要なMNの情報（以後，不要エントリと呼ぶ）が残ってしまい，FA内のテーブル検索処理やソフトステート管理のための処理負荷が増加してしまうという問題が発生する．FA内に残された不要エントリの影響を少なくするためには，①通信終了時や移動時などに伴う無線リンクの解放時や，②HAの位置情報管理テーブル変更を契機に，MNが在圏していた旧FA内の不要エントリを削除するメッセージを追加する方法が考えられる．

・位置登録時間を削減するための実装上の改善方法

位置登録時間を削減するためには，ノード内処理であるHA/FA/AAA内で保持している管理テーブルの検索方法の高速化や，ソフトステート管理のためのライフタイムの減算方法，登録リストの並び替え方法などを改善し，位置登録時の処理負荷を軽減する必要がある．

② ハンドオーバ品質評価

ハンドオーバの実験として，HA/FAにおけるデータパケット負荷を増加させたときの，ハンドオーバ処理時間（MNがFAを移動した後に通信相手であるCN（Correspondent Node）からのデータパケットを受信するまでの時間）および，パケット廃棄数を測定した．

その結果，CNが送出するデータパケットによる負荷が，ある一定以上大きくなるのに伴い，ハンドオーバ切替時間／パケット廃棄数に大きな増加が見られた．これは，HA/FA内で新FA宛てのトンネル経路変更（ハンドオーバ処理）のための位置登録メッセージ処理（Mobile IPではハンドオーバ用のメッセージは定義されていない）が，データパケット処理負荷の影響を受けてしまうためである．したがって，ハンドオーバ品質を大きく左右する位置登録メッセージがデータパケット処理の影響を受けないように，IP網内の輻輳回避やHA/FA内の優先処理をIP-QoS技術と連携させて行うことが，大規模網への適用時には必須になると考えられる．

3. IP呼制御技術とIP-QoS技術

移動通信用IPコアネットワーク上で，音声を含むマルチメディアサービスを提供することをねらいとし，IP網上の呼制御技術とサービス品質（QoS：Quality of Service）技術の検証実験を行った．本稿で紹介する検証ポイントを**図3**に示す．

3.1 IP呼制御技術

(1) 実験内容と評価ポイント

電話サービスのようなコネクション型通信をコネクションレス型のIP網上で実現するために必要となる呼制御プロ

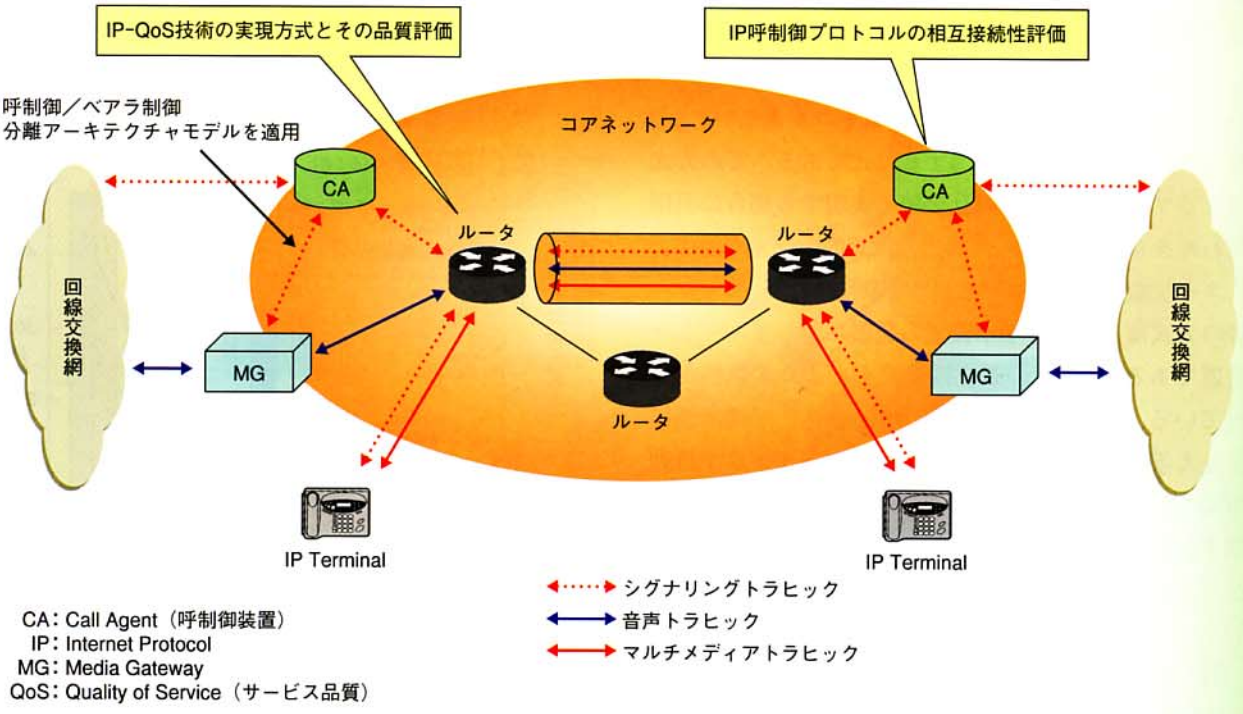


図3 IP呼制御技術とIP-QoS技術における検証ポイント

トコルとして，移動通信関連の標準化団体で採用が決定したSIP（Session Initiation Protocol）[5]と，固定IP網を中心に利用されているH.323[6]がある．また，IP網上の通話と回線交換網の通話を相互接続するためには，呼制御装置（CA：Call Agent）において制御信号間の相互変換機能が必要となる．

本実験では，SIP，H.323およびISUP（ISDN User Part）信号の相互変換機能に関して，実装方式の比較と考察を行い，移動通信網に相応しい変換方式を見出すことを目的とする．

(2) 結果と結論

今回評価を行った各実験システムのCAでは，独自実装の変換機能を提供しており，通話の相互接続を実現している．これは，各プロトコルで用意している呼制御用メッセージ群の間で機能的に類似性を持つものが多く，メッセージ間の関連づけが可能であることによる．ただし，一部のメッセージについては，その変換のタイミングが合わない場合があることが明らかになった．すなわち，現在一般的に使用されているH.323ver.1仕様においては，端末間情報交換のタイミングが呼の接続後となっており，他のプロトコルにおける接続前のタイミングと一致しない．

本問題への対処として，2種類の実装方式が存在する．1つは，双方向の端末間情報交換のタイミングのずれを許容し，H.323側の端末情報については接続後の応答メッセージにて相手に通知する方法である．IETFで検討が進められている方式をベースとしたものであり，後述の方法に比べて端末情報の交換を本来の目的どおりに端末間で実現している．

もう1つは，発側と着側の呼制御プロトコルをCAで完全に分離し，それぞれ独立に終端する方式である．この方式は，異なるプロトコル間の相互接続を実現する場合に汎用的に使われる方法であるが，CA内の仮想的な端末機能によって，ユーザ端末側の機能や接続性が制限される．

前者の方式は，ユーザ端末機能の発展に対してネットワーク装置であるCAからの独立性が高く，より柔軟性が確保されている．一方，後者はCAの機能がユーザ端末側に制限を与える．IP技術の導入によって，今後ますます移動通信用端末の機能向上が促進されることを考慮すれば，ユーザ端末機能の柔軟な発展性は非常に重要な要素であり，したがって前者がより望ましい方式であると判断できる．

3.2 IP-QoS技術

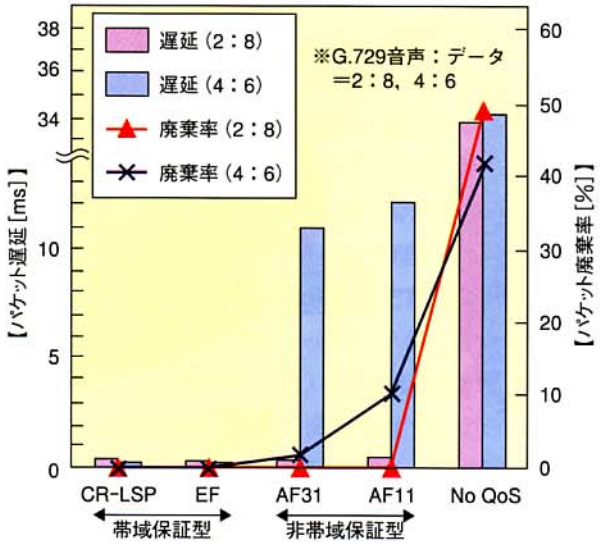
(1) 実験内容と評価ポイント

音声やデータをはじめ，マルチメディア通信を輻輳するIP網上で提供するには，帯域保証や優先制御などを行うことを可能とするDiff-serv（Differentiated Services）[7]やMPLS（Multi Protocol Label Switching）[8]などのIP-QoS技術を導入して各メディアの異なるQoS要求を満たすことが必要である．リアルタイム性を要求する音声トラヒックや確実性を要求するシグナリングトラヒックに対して，どのようなIP-QoS技術を適用するかによって，ユーザが感じ取るサービス品質に大きく影響を与えるにもかかわらず，各トラヒックに適用すべきIP-QoS技術が規定されていないため，実験による検証を行うことは非常に重要である．

本実験は，トラヒック変動などに起因する輻輳状態を想定したIPコアネットワーク環境下において，IP（SIP/H.323）端末または回線交換網からの音声トラヒックと呼制御シグナリングトラヒックに対し，帯域保証型のDiff-serv（EF：Expedited Forwarding），非帯域保証型で相対的な優先制御を行うDiff-serv（AF：Assured Forwarding），帯域保証型のMPLS（Multi Protocol Label Switching）によるIP-QoS制御を適用した場合のIPパケット転送品質と音声品質を評価し，各トラヒックに適用すべきIP-QoS技術を見出すことが目的である．

(2) 結果と結論

図4は，各IP-QoS技術を音声に適用した場合のパケット廃棄率およびパケット遅延である．IP-QoS制御を全く行わない（No QoS）場合は，パケット廃棄率や遅延が大きく，音声通話として成り立たないが，Diff-serv（EF/AF31/AF11）またはMPLS（CR-LSP）によるIP-QoS制御を行う場合は，

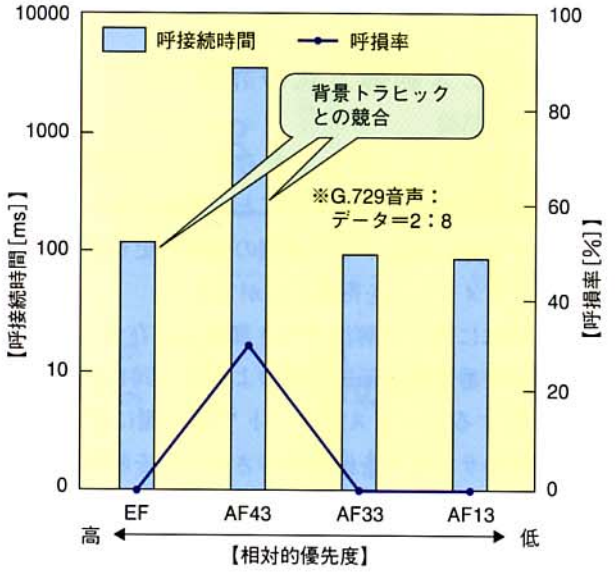


AF：Assured Forwarding
CR-LSP：Constraint-based Routing Label Switched Path
EF：Expedited Forwarding
QoS：Quality of Service（サービス品質）

図4 各IP-QoS技術を音声に適用した場合

パケット廃棄率や遅延が大幅に改善されていることが分かる．しかし，非帯域保証型のDiff-serv（AF31/AF11）では，音声トラヒック比率が増加するとパケット廃棄率や遅延が劣化してしまうため，低遅延／低ジッタ品質を必要とする音声トラヒックには，帯域保証型のIP-QoS技術（CR-LSP/EF）を適用することで，音声品質を保つ必要があると判断できる．

図5は，各IP-QoS技術をSIPシグナルに適用した場合の呼接続時間および呼損率である．背景トラヒックと同一のIP-QoS技術にSIPシグナルが割り当てられている場合，たとえ相対的優先度が高いDiff-serv（AF43）であっても呼損率や呼接続時間が劣化し，呼接続の品質に影響が出てしまうことが分かる．一方，背景トラヒックと異なるIP-QoS技術のDiff-serv（AF33/AF13）にSIPシグナルを割り当てた場合は，帯域保証型のDiff-serv（EF）とほぼ同等の呼損率と呼接続時間が得られることが分かる．しかし，非帯域保証型のDiff-servの場合は，自身よりも相対的優先度が高いトラヒックの影響による品質劣化が実験によって確認された．したがって，バースト性を有するがその絶対量が少なく，遅延品質の条件がゆるいシグナリングトラヒックには，有限な帯域を保証しなくても相対的優先度が高いDiff-servの1つを専用的に割り当てれば，呼接続の品質に影響はないと結論づけられる．

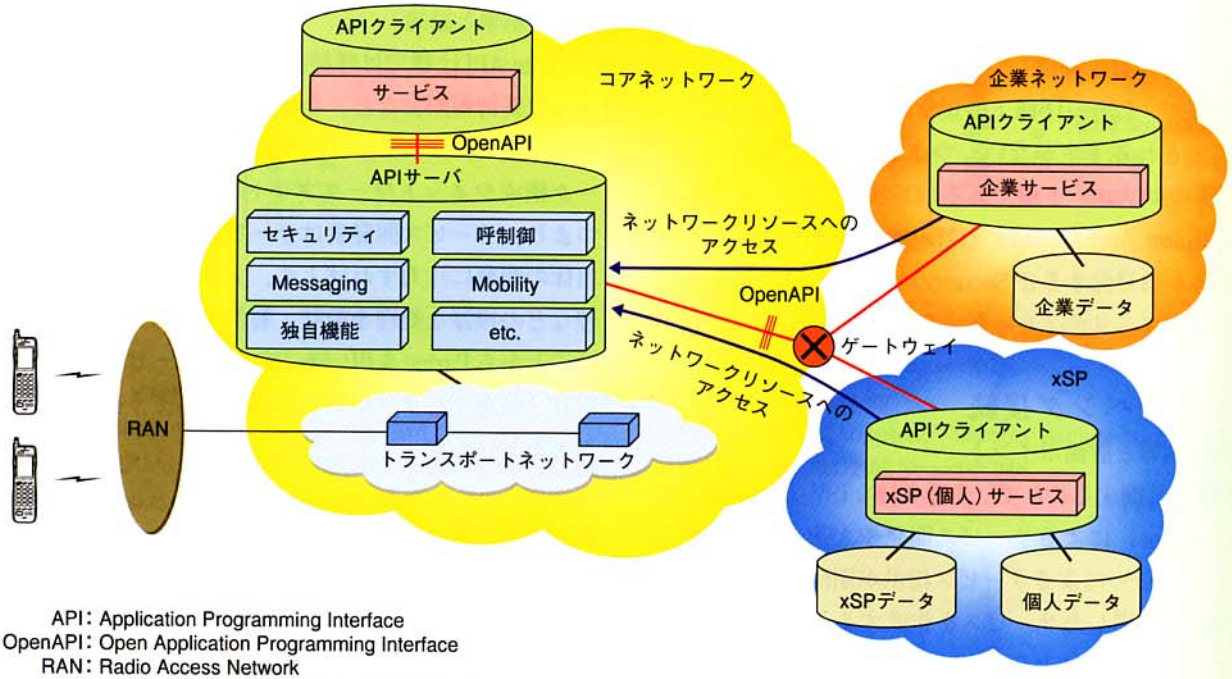


AF：Assured Forwarding
EF：Expedited Forwarding

図5　各IP-QoS技術をSIPシグナルに適用した場合

4. OpenAPI技術

これまでのサービスは通話接続機能を制御するものが大半であったが，通話制御機能に加えてセキュリティ機能，メールサーバ制御や位置情報参照機能などの情報系サービス機能などの機能インタフェースが公開された．これによりサービス開発者を幅広く求め，サービス開発の容易化と高度化を目的としたOpenAPIの議論がParlay [9]，JAIN（Java API for Integrated Network）[10]など各種標準化団体において進められている．このOpenAPI技術を移動通信網



API：Application Programming Interface
OpenAPI：Open Application Programming Interface
RAN：Radio Access Network
xSP：Internet/Application/Content Service Provider

図6　OpenAPIを利用したサービス構成

に適用することで，図6のようにメール機能やユーザのロケーション情報などを活かしたサービスの高度化が可能と考えられる．本稿では，OpenAPIとして最も標準化の検討が進んでいると考えられるParlay2.1を評価した実験の結果について述べる．

4.1 セキュリティ機能

(1) 実験内容と評価ポイント

コアネットワーク機能をAPIを介して外部へ公開する場合には，サービスアプリケーション（以下サービスと称す）とネットワークの双方の安全性を確保する必要がある．そのため，サービスとネットワークノード間で相互確認を行う認証機能，途中経路でのAPIの改ざんによる成り済ましを防ぐ署名機能，APIでやりとりされる情報漏洩を防ぐ守秘機能が必要となる．これらの点を実際にサービスを開発することで検証を行った．

(2) 結果と結論

認証機能はDES（Data Encryption Standard）もしくはRSA（Rivest Shamir Adeleman）による暗号化を用いたCHAP（Challenge Handshake Authentication Protocol）[11]が規定されており，相手の正当性確認と相互に持ち合う公開鍵・秘密鍵の合致が双方向で確認可能である．しかし，認証結果がNGであってもサービスからコアネットワークへのアクセスが可能となってしまう仕様上の問題を発見した．この問題は，Parlay仕様を策定するParlayグループへ問題提起を行い，Parlay3.0仕様において改善する予定である．次にAPIの署名機能・守秘機能については，認証手順で確認した暗号鍵を利用し，API自体を暗号化することで達成できるが，Parlay仕様上の規定はなく，Parlay3.0においても規定される予定がない．つまり現時点では，APIから見ればトランスポート層であるCORBA（Common Object Request Broker Architecture）[12]が持つ暗号化機能やIPパケット自体を暗号化するIP Security Protocol [13]などを適用することでセキュリティを確保する必要がある．

4.2 マルチベンダ接続

(1) 実験内容と評価ポイント

API仕様を公開することで，多種多様なISV（Independent Service Vendor）によるサービス開発やASP（Application Service Provider）によるサービス提供が期待できるが，一方API規定に準拠したサービスを作成することで，アクセスするネットワークによらず，サービスが設計者の意図したとおりに動作することが要求される．そこで，さまざまなベンダの作成したParlayアプリケーションがParlayの仕様どおりに動作するかについて，実際にParlayアプリケーションを作成し，検証を行った．

(2) 結果と結論

結果としては「APIパラメータの具体的定義値が未定義である」「ネットワーク動作との関係が不明確である」といった実装を進めるうえで仕様にあいまいな点があり，サービスとネットワーク間で調整を取る必要があることが明らかとなった．これらの問題点はParlayグループへ問題提起を行い，Parlay3.0仕様において改善していく予定である．

4.3 サービス制御方式の評価

(1) 結果と結論

Parlayを用いると，サービスからサービス起動条件をネットワーク側に動的に設定することが可能であり，サービスを追加する際にネットワーク側の処理変更が不要になるという大きなメリットを得ることができる．

一方，それによって解決すべき課題も存在する（図7）．例えば，留守番電話と転送電話のように，同じサービス起動条件を有するサービスをネットワーク側に設定した場合，いずれのサービスを優先動作させるかを制御する仕組みがParlay2.1では提供されず，Parlay3.0においても提供される予定がない．このサービス間の優先起動制御の実現方法については，前述のメリットを活かしながら解決を行うことが今後の課題となる．

4.4 ParlayAPIの機能評価

(1) 結果と結論

ParlayAPI仕様では呼接続，ガイダンス，メールサービス，位置情報照会など，さまざまな機能を提供することが可能である．これらのAPIを利用するにあたり，ネットワーク構成やネットワークプロトコルの知識は不要である．つまり，サービス開発者はサービスで実現すべきロジック自体の開発に注力すればよく，プロトコル制御や呼状態管理などの複雑な処理を設計・製作する必要がない．これらのことからParlayを用いることで，サービス開発が容易になり，開発するサービスの範囲がいっそう拡大する可能性があるといえる．

4.5 Parlay2.1の実用性評価

Parlay2.1の現時点での実用性を評価すると，「仕様不備を独自仕様にて補足すること」「サービスとネットワーク間で実装のあいまい部分の調整を行うこと」「サービスをセキュリティの確保されたネットワーク内に配置すること」「複数サービス間の優先制御が必要な場合には独自実装を行うこ

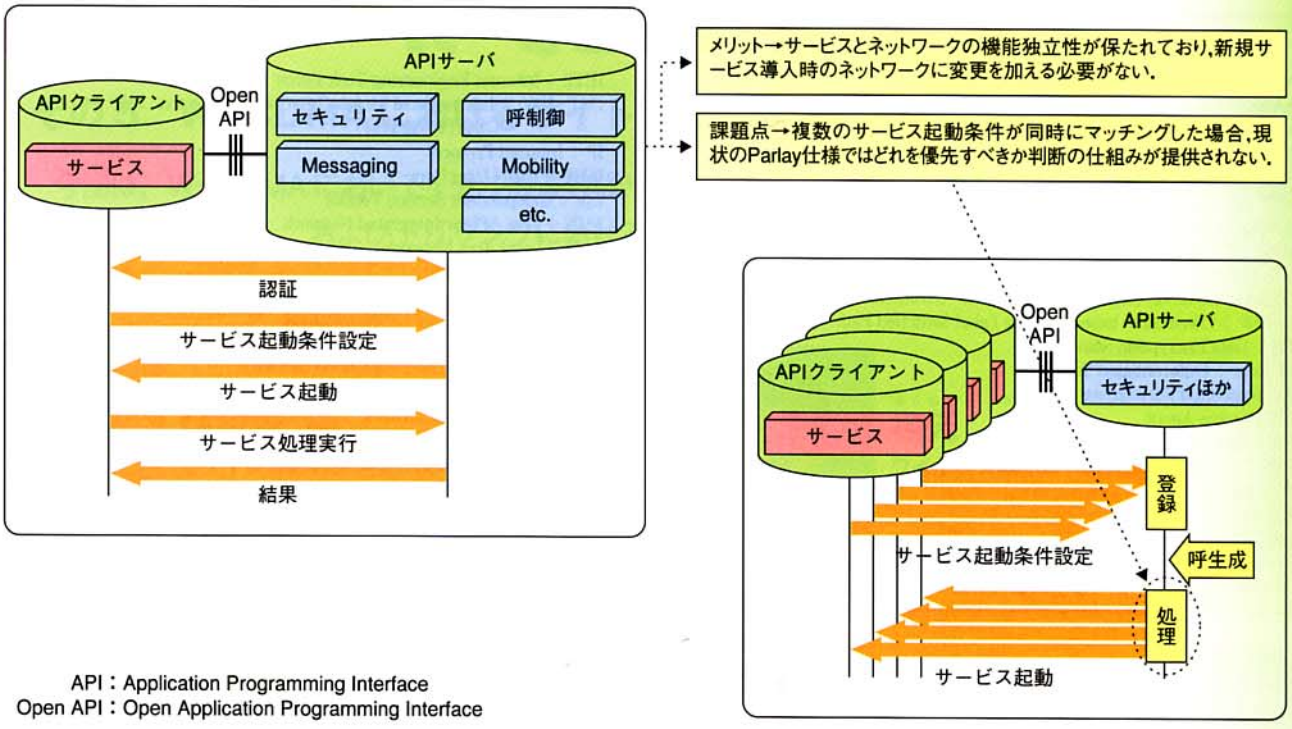


図7　サービス起動方式と問題点

と」という条件つきで適用が可能であると考える．今後は，サービス競合問題の解決，大規模網への適用性，サービス開発環境について検討を行う予定である．

5. あとがき

Mobile IP技術，IP呼制御技術とIP-QoS技術，Open API技術のそれぞれについて，システム実験により移動通信網のコアネットワークへの適用性，有効性を評価し，現時点の技術の到達度や課題を明らかにした．今後は，本実験結果に基づき，未完成技術の改良や新方式の提案，ネットワーク運用面からの課題検討を行うほか，経済性の評価やサービス面でのIP化の有効性を明らかにし，新たなネットワーク展開へ向けた検討を推進する．

文　献

[1] 今井，ほか：“移動通信ネットワークのIP化の検討－ALL-IP実験の概要－”，本誌，Vol.9，No1，pp.38-44，2001.
[2] C. Perkins, “IP Mobility Support”, RFC2002, October 1996/C. Perkins, “IP Encapsulation within IP”, RFC2003, October 1996/D. Cong, M. Hamlen, C. Perkins, “The Definitions of Managed Objects for IP Mobility Support using SMIv2”, RFC2006, October 1996.
[3] Allan Rubens, Glen Zorn, Erik Guttman, Pat Calhoun, Jari Arkko, Haseeb Akhtar, “Diameter Base Protocol”, draft-ietf-aaa-diameter-06.txt, 06/19/2001.
[4] C Perkins, Pat Calhoun, “Diameter Mobile IPv4 Application”, draft-ietf-aaa-diameter-mobileip-06.txt, 06/19/2001.
[5] M.Handley, et al.: “SIP: Session Initiation Protocol”, RFC2543, Mar.1999.
[6] TTC標準 JT-H323 パケットに基づくマルチメディア通信システム 第2版，電信電話技術委員会，Nov.1998.
[7] K.Nichols, et al.: “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers”, RFC2474, Dec.1998.
[8] B.Jamoussi, et al.: “Constraint-Based LSP Setup using LDP”, draft-ietf-mpls-cr-ldp-04.txt, Jul.2000.
[9] http://www.parlay.org
[10] http://java.sun.com/products/jain
[11] W. Simpson, “PPP Challenge Handshake Authentication Protocol (CHAP)”, RFC1994, August 1996.
[12] http://www.omg.org
[13] S. Kent, R. Atkinson, “Security Architecture for the Internet Protocol”, RFC 2401, November 1998.

用 語 一 覧

AAA：Authentication Authorization Accounting
AAAH：Authentication Authorization Accounting Home
AAAL：Authentication Authorization Accounting Local
AF：Assured Forwarding
API：Application Programming Interface
ASP：Application Service Provider
CA：Call Agent（呼制御装置）
CHAP：Challenge Handshake Authentication Protocol
CN：Correspondent Node
CORBA：Common Object Request Broker Architecture
CR-LSP：Constraint-based Routing Label Switched Path
DES：Data Encryption Standard
Diff-serv：Differentiated Services
EF：Expedited Forwarding
FA：Foreign Agent
GFA：Gateway Foreign Agent
GPRS：General Packet Radio Service
GW：GateWay
HA：Home Agent
HLR：Home Location Register
IETF：Internet Engineering Task Force
IMT-2000：International Mobile Telecommunications-2000（次世代移動通信）
IP：Internet Protocol
ISUP：ISDN User Part
ISV：Independent Service Vendor
JAIN：Java API for Integrated Network
LAN：Local Area Network
MG：Media Gateway
MN：Mobile Node
MPLS：Multi Protocol Label Switching
OpenAPI：Open Application Programming Interface
PSTN：Public Switched Telephone Network
QoS：Quality of Service（サービス品質）
RAN：Radio Access Network
RSA：Rivest Shamir Adeleman
SIP：Session Initiation Protocol
VoIP：Voice over IP
WAN：Wide Area Network
xSP：Internet/Application/Content Service Provider