■5 群（放送・通信）－ 9 編（ネットワーク管理）

4 章 個別ネットワークの管理

（執筆者：吉原貴仁）［2011 年 6 月 受領］

■概要■

電気通信事業者が管理するような大規模なコアネットワークと，個人のお客様の宅内に敷設される小規模なホームネットワークとでは，提供するサービスや機能要件が異なる．結果として，機能要件を満足するために配備される設備や構成，その上でのネットワークの管理手法も異なる．このため，ネットワーク管理の実践では，管理の対象となるネットワークに固有の設備や構成と管理手法を加味し，本編第 2 章で解説した「ネットワーク管理アーキテクチャ」や，本編第 3 章で解説した「ネットワーク管理の共通機能」といった概念や手法，ツールを取捨選択し，具現，適用することになる．ただし，管理対象となるネットワークの種別ごとにも区々の管理条件を加味しなければならないこともまた事実である．

そこで本章では，コアネットワーク，アクセスネットワーク，ユビキタスネットワーク，FMC ネットワーク，カスタマネットワーク／ホームネットワークなどの個別のネットワークを取り上げ，これらネットワークを管理するための個別の課題，対処技術，標準化や関連技術の動向などについて見ていく．また，実用されているコアネットワークやアクセスネットワークでは運用管理の実際についても触れていく．

【本章の構成】

本章では，コアネットワーク管理（4-1 節），アクセスネットワーク管理（4-2 節），ユビキタスネットワーク管理（4-3 節），FMC ネットワーク管理（4-4 節），カスタマネットワーク管理／ホーム NW 管理（4-5 節）について解説する．

■5 群－9 編－4 章

4-1 コアネットワーク管理

（執筆者：馬島宗平）［2008 年 10 月 受領］

コアネットワーク管理は，キャリアにおける加入者終端装置，ゲートウェイ装置，トランスポートネットワーク，及び，ネットワークを制御するシグナリングネットワークから構成されるネットワークを管理の対象とする．**図 4･1** にキャリアのネットワーク構成におけるコアネットワーク管理が管理対象とする範囲を示す．

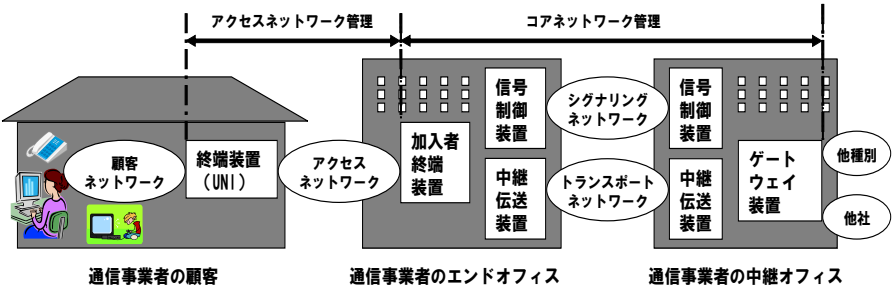


図 4･1　ネットワーク管理の種別と管理対象ネットワーク

コアネットワーク管理に必要とされる要件は，(1)ネットワーク管理一般に求められる要件，(2)キャリアのネットワーク管理に求められる要件，(3)それぞれのネットワークプロトコルに基づく要件の 3 種類の要件から構成される．以下の節で，それぞれの管理要件を示す．

4-1-1 キャリアのコアネットワーク管理に求められる要件

ネットワーク管理一般に求められる機能要件は，3-1-3 節で示した FCAPS で示せる．

キャリアのコアネットワークは，管理一般に求められる機能要件に加えて，(1)信頼性（無停止性），(2)スケーラビリティ要件，(3)網構成変更に対する柔軟性要件，(4)加入者ごとに異なる多様な用途を同一ネットワークに共用することを考慮した保守グレードとコスト要件，(5)他キャリアや ISP との接続を考慮した要件が必要となる．

(1)　信頼性

キャリアのコアネットワークは，前段のアクセスネットワークで多くの加入者の情報を集約しており，一つの設備で多量のトラヒックを扱う．このため，装置故障による通信断が生じた場合に影響を受ける加入者の範囲が大きく，場合によっては県や国単位の通信が影響を受ける．キャリア用のコアネットワーク装置は信頼性を向上させるために，装置や伝送路を二重化しているが，二重化の仕組みをいつでも正常作動させるための予防保全（定期的に予備系装置の試験を行って二重故障を防ぐ，統計的な故障率を把握して事前に交換など）やソフトウェアの更改時における無停止性（通信中サービスの継承），24 時間体制での監視を行うことが求められる．

ネットワーク管理としては，二重化された装置やネットワークを対象とした設備管理，構

成管理，故障管理（すなわち，装置が運用状態か，予備系としてのスタンバイ状態か，故障中かなどの装置状態の正確な把握とそれらの正確な接続関係の把握）が必要とされる．

保守用装置（OSS：Operation Support System）と通信装置を接続する DCN（Data Communication Network）に対しても，警報欠落や非監視状態の発生を確実に識別できることなどの高い信頼性が求められる．DCN については，アクセス系の装置ではそれぞれごとに別網を敷設するとコスト高になるために通信装置が伝送を行っている信号の中に含めるインチャネル方式が使われることが多いが，コアネットワークでは，監視を行っている装置自身を使った警報転送を行うと，当該装置が故障すると DCN が使えなくなってしまうために，通信装置が伝送を行っているネットワークとは別のネットワークを使って構築されるアウトチャネル方式を使うことが多い．

(2) スケーラビリティ

電話や電報はサービス開始からピーク時まで 50 年近くの年月をかけて普及してきたが，1990 年後半あたりからの ISDN や ATM，インターネット接続サービスなどは，サービス開始からピーク時までの期間は数年から 10 年程度と短くなっており，新たなコアネットワークを構築する場合に大規模な初期投資を行うことは難しくなった．また，通信市場の競争の激化やサービスの多様化により需要が読みにくくなったことから，設備投資も以前は 2 年程度先の需要を見た設計を行ってきたが，新たなサービスでは半年とか数か月先の需要を見て設備投資を計画し，急速な需要増が見極められてからこまめに増設を行う必要が出てきた．

ネットワーク管理の要件としては，設備設計（必要設備数の算出）や設備の調達期間の短縮化，増設工事の簡易化が必要となっている．しかし，設備設計の基礎データとなる，サービスごとのトラヒックデータやサービス品質データを収集するには，ネットワーク設備に基礎的なデータを測定する機能が必要となりコストがかかるため，効率良く必要な情報を収集・分析する技術の開発が課題となっている．また，より本質的な需要の要因となる，販売促進キャンペーンやキラーアプリの出現，大規模な社会インフラのリニューアルなどと，トラヒックとの関連性を定量的に把握する技術を実用レベルにすることが期待されている．

(3) 構成変更に対する柔軟性

キャリアのネットワークは，規模が大きいために，ほぼ毎日，同時並行的にネットワークの増設や変更・ソフトウェアの更改などの工事が実施されている．また，加入者が新たなサービスに加入する，廃止するといった変更も，サービスの加入者数にもよるが，1000 万加入規模のネットワークの展開期には数万件/日といった数の申込み（SO：Service Order）を設定する必要がある．

ネットワーク管理としては，これらの多量の工事や SO を間違いなく，迅速かつ，セキュア（特に個人情報が漏えいしないよう）に実行する必要がある．特に工事や増設・ソフトウェアの更改は，失敗をすると大規模な影響を与えるために，工事手順を事前に確認し，手順を自動的に実行できる仕組み（スクリプト）でヒューマンエラーのなくす方法が一般化している．また，SO については，複数の装置間で整合をとった設定を，間違いなく多量に実施する必要があるため，設備の現況情報や利用可能リソースの管理を徹底させる必要がある．また，SO の内容により異なる装置ごとの設定内容を適切な装置管理権限をもつ OSS へ配信し，

その結果を確認する（一部でも失敗したら成功した他の装置への設定も元へ戻すか，成功した他の装置の設定の有効化を遅らせて，失敗要因を除去してから継続実行する）技術が必要となる．この技術は，トランザクション処理のコミットロールバックと対応付けて提案されることが多いが，所謂データベース処理における分散トランザクションと，ネットワーク管理における上記要件は，ネットワーク装置に実装される情報の書き込み，コミットロールバックのモデルが異なることから，その差異を吸収する方式が実装上の課題となる．

SO は，加入者からの申込み時に発生し，工事の伴わない内容なら即日実施が可能であるが，工事を伴うものは，数日後に開通する．このような SO は，申込み受付け時に，設備状況（空き端子の有無）や工事要員の手配可能日時が即答できると，加入者にとって利便が良くなる．すなわち，SO の加入者対応をするには，設備の現況だけではなく，将来の装置増設計画を反映した設備予約ができ（これを将来在庫の管理と呼ぶ），工事要員のスケジュールが参照・予約できることが望まれる．

現状ではテレビ放送用の中継ネットワーク管理で，予約に基づいた回線の切替えなどを実現しているが，緊急放送などの予約の変更などがあり，処理の論理が複雑になる．このような処理を実現する設備管理には，現在という「動く時間」を含めた時間概念のあるデータを容易に扱える技術が必要とされる．

(4) 保守グレードとコスト

キャリアネットワークは，警察・消防への緊急通話や地震や津波の警報など，人の生死にかかわる内容から，迷惑電話や間違い電話などの通話中切断が発生しても，ほぼ社会的な影響はない内容まで様々である．キャリアは，これを音声・データ・映像などのメディア種別や専用サービスでは帯域や可用性などで，用途の多い組合せに対してタリフ（サービスの料金表）単位で提供してきた．

しかし，高い可用性，故障の即時通知，故障時駆けつけ時間の短縮，といった保守グレードは，サービスを提供する設備の冗長化費用やプローブや監視装置などの設置費用が，コスト的には，その設備を利用するすべてのサービスに一律にかかってくるために，高い保守グレードを必要とせず，料金の安さで勝負する設定のサービスは，高い保守グレードを必要とするサービスと設備共用をすることはできない．

2000 年半ばからキャリアが構築を行っているオール IP ネットワークや NGN（Next Generation Network）では，電話サービスや映像配信サービスとベストエフォートベースのインターネット接続サービスを一つのネットワークに重畳させることにより，サービス需要の変動に強く設備利用率を高めることによって，安価なネットワークサービスが提供されることが期待されている．しかし，これらのネットワークは，割り当て帯域や転送の優先順序が異なる論理的に分割したネットワークを提供できるが，可用性や継続性は高い信頼性を求められるサービスに合わす必要がある．従来，高い可用性を提供してきた電話サービスや映像配信サービスで必要とされる信頼性を実現する設備構成で，ベストエフォート型の通信サービスで必要となる，低コスト・低料金を実現することは難しく，信頼性要件の異なるサービスの共用技術の実現は課題となっており，各キャリアでネットワークの構成方法やサービス提供条件の工夫により，市場に受け入れられる保守グレードとコストを工夫している．

(5) 他事業会社との接続

インターネットの普及や携帯電話網の発達により，キャリアの扱うトラヒックの半分以上は,自社ネットワーク内には閉じずに,複数のキャリアを介して行われるようになっている．また，インターネットでは多様なサービスがキャリアとは別の事業会社により展開されており，同様に NGN でも，サービス提供事業社とキャリアを区別して，それぞれ独立の展開できるようにインタフェース ANI（Application Network Interface）を規定している [2].

他キャリアとの管理情報連携は，上記のようなキャリア連携の広がりと連携形態の多様化により，交換すべき情報の項目定義について以下のような検討が行われている．

(a) 加入者ごとの課金・キャリア間での精算

キャリア間での課金・精算は，電話時代から実施されており，その情報交換フォーマットも，電話を継承するネットワークでは，CDR（Call Data Record）に基づき実施されることが多い．しかし，CDR では，呼情報ベースのレコードが記録されるために，より柔軟な課金情報の交換を実現すべく，IPDR（Internet Protocol Detail Record）の標準化が進められている．

(b) 故障・回復通知

故障やその回復の他事業社への通知は，故障を起こしたキャリアからの通知と，利用している他事業会社やお客様からの問合せによる通知がある．標準化については，tML（Telecom Markup Language : ITU-T M.3030）により，ルールやガイドラインが規定されているが，詳細情報の構造は，欧州や米国の標準化機関で規定している．

(c) サービスオーダ

サービスオーダは，各国のキャリアが受け持つ事業範囲により，多様な組合せが生じる．先に述べたように多様なサービスが複数の事業会社により提供されると，加入者自身がそれぞれの事業会社に申込みを行うことは利便性が悪いため，顧客からの申込みを受け付けた会社が主体となり，関連する事業会社へ一元的にサービスオーダを展開する（ワンストップ）を実現することが望まれている．

(d) トラヒックレポート

キャリアと上位サービスの提供事業社間では，サービス品質におけるネットワーク品質の影響や利用度合いを分析するために，故障情報だけではなくトラヒック情報の提供を行う場合がある．

4-1-3 ネットワークプロトコルに基づく要件

コアネットワークをプロトコルの観点から分類すると，シグナリングネットワークとトランスポートネットワークに大別できる．以下にシグナリングネットワークとトランスポートネットワークの管理要件を示す.

(1) シグナリングネットワークの管理

シグナリングネットワークとは，電話網では，No.7 共通線信号方式（Common Channel Signaling System No.7 : SS 7）に代表される通信制御のためのネットワークであり，SS 7 のほかにも VoIP（Voice over IP）で使われ，NGN でも基本的な制御プロトコルである SIP（Session Initiation Protocol）や音声・動画を 1 対 1 で送受信するために音声・映像方式，データ圧縮伸長方式などを定めた H.323 などがある．これらのシグナリングネットワークは，端末とネッ

トワーク装置間での通信制御を行い，発着信の制御のみならず，サービス番号（E.164 : ITU-T で規定される国際的に一意な電話番号の勧告）による経路制御や Megaco（Media Gateway Control：H.248）によるメディアコントロール（メディア変換）を行う．

また，本節では，IP（Internet Protocol）における加入者への IP アドレスの払い出しを行う DHCP（Dynamic Host Configuration Protocol）や加入者からの接続要求を認証する Radius（Remote Authentication Dial In User Service），ホスト名から IP アドレスへ変換する DNS（Domain Name System）もシグナリングプロトコルと考える．

シグナリングネットワークの管理には，この機能が停止するとネットワーク全体に影響が及び通信ができなくなるために特に高い信頼性が求められる．

シグナリングプロトコルは，加入者の設備である端末と網内設備が通信を行うために，シグナリングを扱う装置（SIP サーバ，加入者収容エッジルータ，認証サーバなど）には，加入者情報の設定を行う必要がある．加入者情報の設定には，加入者へのサービス番号の付与，どの設備に加入者を収容する（割り付ける）かの設備選定，加入者の申し込んだサービス属性の設定，従量制の場合は加入者ごとの課金情報の測定開始と作成，設備増設や変更に伴う加入者の収容変更などの管理機能が必要となる．

(2) ルーティングプロトコルの管理

「ルーティング」という用語は，E.164 番号から着信先ネットワークと端末を求め，接続先回線を決める「電話番号の解決」と IP（Internet Protocol）において，IP アドレスから着信先端末と接続先回線を決める「パケットの転送経路を解決」という場合に使われる．

「電話番号の解決」では，番号帯が国や通信事業社と加入者の利用する地域に割り当てられ，政府管理の基にキャリアが加入者に番号を払い出すため，電話交換機の時代にはオンラインで修正が可能なデータとして各装置に設定してきた．このため，設備設計や工事と連動した保守運用システムにより一元的な供給が可能であった．しかし，キャリアが競争の時代に入り，電話番号を変えずにキャリアを変更可能とする番号ポータビリティが固定電話にも携帯電話にも IP 電話にも導入されると，電話番号でキャリアや地域を示すことはできない．このことは，電話番号の割付け方法（他社に割り当てられていた番号を利用可能とする）や番号が地域（装置）と対応付いていることに基礎をおいていた輻輳制御といった管理機能に影響を与える．IP 電話同士の異なるキャリア間の接続で一旦は電話ネットワークに接続してから他キャリアの IP 電話に接続する形態を取らざるを得なかったのも，この番号解決を電話ネットワークで実施してきたからであるが，NGN や ALL-IP ネットワークの時代を迎えるにあたっては，電話ネットワークに依存しない効率的な電話番号の解決の方式を実用化することが必要である．

「パケットの転送経路を解決」では，OSPF（Open Shortest Path First）といったキャリア内での番号解決を図るレイヤ（IGP：Interior Gateway Protocol）と，キャリア間やインターネットの AS（Autonomous System）間で使われる BGP 4（Border Gateway Protocol 4）がある．

OSPF の管理では，IP アドレスの番号帯（サブネットマスク）によりエリアという論理ネットワークを管理し，ルータに Config 情報として設定することで，ルータ間でのルーティング情報はプロトコルで整合させる．ネットワーク管理としては，プロトコルに依らずに設定する（Static Route）区間と，OSPF を用いる区間を区別して管理することと，OSPF で用い

るエリアに対してルータを収容すること，コストと呼ばれる経路を決定するためのパラメータを与えることが必要となる．

BGP 4 の管理では，AS（キャリア）間でのルーティング情報の交換であるため，ネットワーク全体としての管理はできない．すなわち，各 AS は，性善説に立ってルーティング情報を広告し，他 AS から広告された情報をフィルタする必要がある．しかし，AS 番号を取得するキャリア以外の企業や大学は年々増加しており，BGP の運用に不慣れな参加者が増えてきており，全世界的な接続不能を引き起こすなどの障害事例が増えている．このため，BGP の管理技術や障害の診断・回復・予防に対する検討が進められている [3)].

(3) トランスポートネットワークの管理

トランスポートネットワークとは，加入者終端装置を含まない中継伝送装置間のネットワークを示し，WDM（Wavelength Division Multiplexing）/ OTN（Optical Transport Network：ITU-T G.709）/SDH（Synchronous Digital Hierarchy）/ IP（Internet Protocol）といったトランスポートプロトコルがある．

中継ネットワークの管理機能要件では，電話サービスや ISP 接続サービスなどの網加入型のサービスの場合は加入者ごとに行う業務はないため，故障対応以外は計画的に業務を実施することができる．一方，専用サービスや VPN サービスのような End-End 型のサービスの場合には，中継ネットワーク区間も加入者ごとの設備（パスや VLAN などの論理回線）を割り付ける必要があるために，加入者対応の設計や事業社間での開通といったシグナリングネットワークと同様の業務が必要となる．

また，中継ネットワークは，それぞれのネットワークプロトコルに多重のパス網が構成され，更に OTN のチャネルの上に SDH のパスが収容されるといったレイヤ構造をとることから，その収容関係を管理することが必要となる．ネットワークレイヤ 1 では，物理的には，ケーブルが装置間に接続されており，ケーブルには複数のファイバが収容されている．また，WDM では，ファイバに複数の波長ネットワークが収容されている．波長ネットワークは，論理的には OTN に対応し，その内部構造として，OTS（Optical Transmission Section），OMS（Optical Multiplex Section），Och（Optical Channel）が階層構造として定義されている．ネットワークレイヤ 2 以上も同様に，SDH，ATM（Asynchronous Transfer Mode），MPLS（Multi-Protocol Label Switching）といったプロトコルのパスが用途に応じてネットワークを形成している．

それぞれのパスは，プロトコルごとに終端点が定義されており，それぞれの終端点が装置内で上位のパスと関係付けられる．この収容関係管理の難しさは，上位レイヤでパスの冗長構成を構築しても，運用中に発生した収容ケーブルの変更により，運用系と予備系が同じケーブルに収容されてしまい，ケーブル切断といった故障の発生時は通常ケーブル単位に切断されてしまうので，ネットワークの二重故障が発生してしまう，といった問題を引き起こすことにある．また，レイヤごとに独立にネットワーク設計を行うと，下位レイヤで冗長化構成をとり，上位レイヤでも冗長化構成をとることで，故障発生時に双方のレイヤで切替えを発生させ，実際の通信がどのルートに切り替わったかを分かりにくくする場合もある．このような二重故障となる状態がないかを確認する技術を分散評価と呼ぶ．

これまで開発されてきた多くのネットワーク管理システムは，SDH や ATM，IP といった

単一ネットワークレイヤを管理の対象としているため，分散評価は保守者が行うか，分散評価用の収容設計システムを別途用意してきた．GMPLS（Generalized Multi-Protocol Label Switching）では，このような単一故障要因で二重故障が発生する単位を SRLG（Shared Risk Link Group）としてプロトコル上で定義されており，パスの切替え時に二重故障とならない仕組みが用意されている．ただし，SRLG は，プロトコル上パスの切替えを行う場合の代替パスの選定に使われる用途が規定されているだけであり，ファイバケーブルの包含関係をグループにするなどの例示はあるが，どのような値を設定して運用するかは，それぞれの実装で検討しなければならない [4)].

■参考文献

1) ITU-T Recommendation M.3400（2000）, “TMN management functions”.
2) ETSI Advanced ES 282 001, V1.1.1, “Telecommunications and Internet Converged Services and Protocols for Networking（TISPAN）; NGN Functional Architecture Release 1,” Jun. 2005.
3) 田原光穂, 大島利充, 草場　律, 馬島宗平, 田島悟志, 川村宜伯, 成田亮介, “経路ハイジャックに伴う通信障害の回復方式の検討,” 信学技報, vol.106, no.600, pp.53-58, Mar. 2007.
4) 柿沼英樹, 小内伸夫, 小池和郎 “GMPLS に対応したリスク情報管理方法,” 信学総全大, 2005 年通信, no.2, p.501, Mar. 2005.
5) “オペレーションの技術,” http://www.hct.ecl.ntt.co.jp/exhibit/technologies/technologies_3.html
6) 大貫雅史, 谷川延広, 原　和彦, “ドコモにおけるオペレーションシステムの開発動向,” NTT DoCoMo テクニカルジャーナル, vol.8. no.1, Apr. 2000.
7) 清水孝男, “新ノードオペレーション技術の実用,” 信学総全大, 1998 年通信, pp.769-770, Mar. 2008.

■5群－9編－4章

4-2 アクセスネットワーク管理 [1)]

（執筆者：宇野浩司）［2008年7月 受領］

4-2-1 まえがき

一般に，通信は2者がそれぞれ同じ機能を有して対向する対称な構成である．しかし，アクセスネットワーク（AN：Access Network）は，後述する理由により，多くの機能が非対称な構成をしているため，その管理機能も非対称である．本節では，それらの特徴に着眼し，AN管理の課題とその解決技術を解説する．

4-2-2 アクセスネットワークの特徴と運用管理の課題

本節は，ANの特徴と運用管理の課題について解説する．

(1) 上り下り伝送の多重化

中継ネットワークは，装置間で伝送する情報量が多いとともに距離が長い．したがって，双方向の伝送のためには，二つの伝送媒体が利用される．一方，ANは，ユーザ当たりの情報量が少ないとともに距離が短い．このような場合は，上り（ユーザ側装置から事業者側装置方向）と下り（事業者側装置からユーザ側装置方向）の伝送を，一つの伝送媒体に多重化することが有利である．双方向多重のための機能が必要であるが，情報量が少なく距離が短いために比較的簡易に実現できる．伝送媒体が一つであるため，媒体コストを低減できるだけでなく，運用が簡易になる利点がある．**図4･2**に，その例を示す．電話の場合は，ハイブリッド回路によって，一対のメタリック線で，アナログ音声信号を双方向に伝送する．ADSL（Asymmetric Digital Subscriber Line）の場合は，周波数分割により，ディジタル信号を双方向に伝送する．PON（Passive Optical Network）の場合は，波長多重により，1心の光ファイバで，ディジタル信号を双方向に伝送する．FWA（Fixed Wireless Access）の場合は，TDD（Time Division Duplex）により，単一周波数で，ディジタル信号を双方向に伝送する．ADSLやPON，FWAの場合，これらの方式以外の双方向多重化方式もある．また，適用領域によっては，ANでも二つの伝送媒体を用いる．上り下り多重化の特徴を活用した，試験・監視方式が必要である．

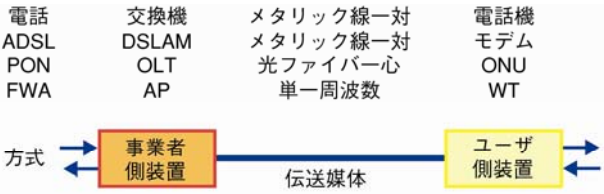


図4･2 アクセス線の双方向伝送方式

(2) 非対称なネットワーク構成

電話機などのユーザ側機器相互間，あるいは交換機などの事業者側装置相互間は，同じ機能同士が対向している．したがって，主信号機能や運用管理機能の形態は対象である．中継

ネットワークを構成する中継装置間も同様である．それに対して，ユーザ側装置と事業者側装置間は，異なる機能が対向しており，非対象な形態である．**図 4･3** に示すように，AN は，一つの事業者側装置に複数のユーザ側装置が接続される．電話の場合は，1 台の交換機に最大数万台の電話機を接続する．ADSL の場合は，1 台の DSLAM（Digital Subscriber Line Access Multiplexer）に，数百のモデムと接続する．PON の場合は，1 台の OLT（Optical Line Terminal）に数百台以上の ONU（Optical Network Unit）を接続する．FWA の場合は，1 台の AP（Access Point）に数百台の WT（Wireless Terminal）を接続する．このような非対称な接続構成においては，数量の多いユーザ側機器の機能を簡易化すること，数量の少ない事業者側装置の機能を高めることが全体最適である．それに適した試験・監視方式が必要である．

なお，電話機や ONU は機能や位置付けの異なる機器であるが，図 4･3 ではネットワークのトポロジを説明するため平素に記述した．

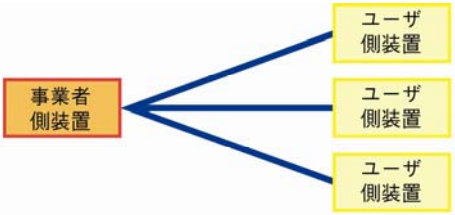


図 4･3　アクセスネットワークの接続構成

(3)　多様な責任分界点

旧来，電話機は通信事業者の資産であり，ユーザは通信事業者から電話機を借用していたが，制度の改正により，ユーザは自由に電話機を入手して取り付けることが可能となった．更に，宅内配線を，ユーザ自身が保守可能となった．ユーザは，通信事業者に支払う借用費や保守費を，自己負担とする選択が可能となった．これらの責任分界点の多様化により，故障の切り分けが必要となった．故障した設備の責任が，ユーザなのか通信事業者なのかを切り分けられないと，ユーザは不必要な故障修理依頼を通信事業者にしてしまう可能性がある．

(4)　制御監視情報のユーザ情報への重畳

ネットワークが取り扱う情報は，ユーザ情報と制御監視情報の二つである．前者は，ユーザ相互間で授受する情報である．後者は，ユーザ情報が正しく授受されるための運用管理情報である．中継ネットワークは，多くのユーザ情報を扱うため，制御監視情報量が多いとともに，その重要性が高い．そのため，中継ネットワークでは，ユーザ情報の伝送路と，制御監視情報の伝送路とを独立に設ける．これにより，ユーザ情報伝送路が故障した場合でも，制御や監視を継続できる．中継ネットワークを構成する装置やケーブルは，通信事業者ビルに集中して設置されているため，制御監視伝送路の構築は比較的容易である．一方，AN は制御情報が少なく，監視の必要性が相対的に低い．また，AN は地理的に各ユーザ宅まで分散しているため，ユーザ情報伝送路と制御監視伝送路を独立に構築することが困難である．そのため制御監視情報はユーザ情報伝送路に重畳して伝送する．**図 4･4** に構成例を示す．AN

ではユーザ情報伝送路が故障した場合，制御監視ができなくなる．

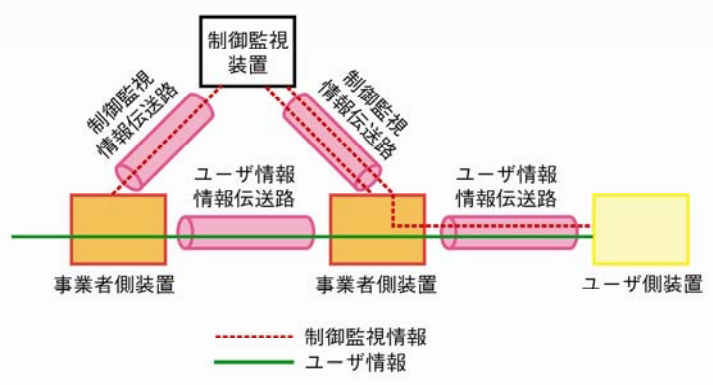


図 4･4　制御監視情報の流れ

(5)　ユーザの利用状況に依存した機器の状態

ユーザ側機器を駆動するための電力は，事業者側装置からアクセス線を介して給電する方法と，ユーザ構内の電源を利用する方法の二つがある．電話のように消費電力が少ないとともに緊急時や災害時でも動作が必要な場合は前者の方式が用いられる．例えば，多機能電話機は，親機の音声通話などの基本機能は前者の方式で，内線子機やディスプレイ機能などの付加機能は後者の方式で動作する．光ファイバはメタリック線と異なり電力の搬送ができない．したがって，光アクセス方式の場合は必ず後者の方式となる．ユーザ電源を利用する方式はユーザの都合により電源を切る場合があり，その間は通信が途絶える．通信事業者は，通信途絶が発生した場合，機器の故障によるものかユーザ電源の都合によるものかを識別する必要がある．

(6)　多くの受動的設備

交換機や OLT などの能動的設備は，自ら電子的に制御，検索，監視することができる．したがって，設備運用者は制御監視装置から遠隔通信によってその管理を行うことができる．一方，ケーブル，電柱，地下管路などの設備は受動的である．AN では，この受動設備の割合が高い．受動設備は自ら電子的に制御，検索，監視することができないため，人手により制御管理する必要がある．その人手作業を迅速かつ正確に行う必要がある．特に，ケーブルは収容している心線数が多いとともに，その接続構成や使用状態の変化が多いのでより迅速性，正確性が要求される．

(7)　地理情報との連携

ケーブルや電柱など，多くの AN 設備は屋外に設置される．また，各ユーザは地理的に分散している．これらを管理するためには地理情報との連携が必要である．設備の設置位置は，地図上に示すことが良い．ユーザ最寄りの電柱を選定することやケーブル配線ルートの設計には道路や建築物の情報が必要である．また，配線区画の設計には鉄道，河川，更には行政

区画などの情報を参照する必要がある．

FWA の場合は，電波の伝搬品質を保つために地形のみならず建築物や構造物も考慮した置局設計が必要である．

4-2-3 基本的な課題解決技術

本節及び次節では，前節で述べた AN の課題を解決するための技術について述べる．

(1) 折り返し試験・監視方式

4-2-2 項(1)で述べたように，AN は上りと下りの伝送媒体を共用するため，上りと下りの伝送特性を独立して試験・監視する必要性は低い．そのため，AN は試験・監視形態として折り返し方式を採用する．**図 4･5**(a)に折り返し方式による試験･監視形態を示す．本方式は，試験・監視信号の生成・挿入機能，検出・測定機能を一方の装置のみに具備する．他方の装置には折り返し機能のみ具備する．試験・監視機能を一方だけに具備すればよいので，機能数を削減できる．

図 4･5(b)には対向方式による試験・監視形態を示す．本方式は事業者側装置間，ユーザ側機器間及び中継装置間など，機能が対象な装置間で用いられる．本方式は片方向ごとの特性や機能を試験・監視できるが，試験・監視信号の生成・挿入機能，検出・測定機能が両装置に必要となる．

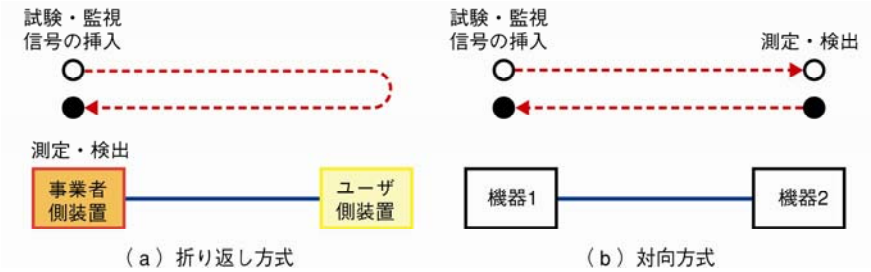


図 4･5 試験・監視形態

(2) 試験機能の共用

メタリック線や光ファイバなどを試験するためには，アナログ特性を測定する必要がある．例えば，メタリック線の場合は，線路抵抗，線間容量などである．光ファイバの場合は，光減衰特性，反射特性などである．これらの測定には精密な測定回路が必要であり，メタリック線一対ごと，光ファイバ 1 心ごとに用意することは，コスト的，スペース的に困難である．そのため，4-2-2 項(2)で述べたネットワーク構成の非対称性を利用して一つの測定回路を多くのメタリック線や光ファイバで共用する．アナログ特性測定はサービス開通時や故障時のみ行われるため，輻輳なく共用することが可能である．

共用試験装置を各伝送媒体に接続するためには媒体の接続換えが必要である．接続換えを人手で行うことは緩慢であるとともに誤りを生じる可能性があるが，切替機能の設置が不要である．迅速化，正確化のためには切替機能を設置して遠隔で媒体の接続換えを行う．試験

の頻度や初期コスト，運用コストなどを考慮して採用方式を選定する必要がある．

遠隔制御による試験機能の共用法を**図 4･6** に示す．屋外メタリック線は，通信時はメタリック通信回路と接続される（図 4･6(a)の 1 の接続）．試験時にはメタリック試験回路に接続される（図(a)の 2 の接続）．メタリック線通信回路側の試験も可能である（図(a)の 3 の接続）．本接続換えを行う試験線接続回路はメタリック線一対ごとに設ける．メタリック線試験回路を共用するために試験線切替回路を用いる．

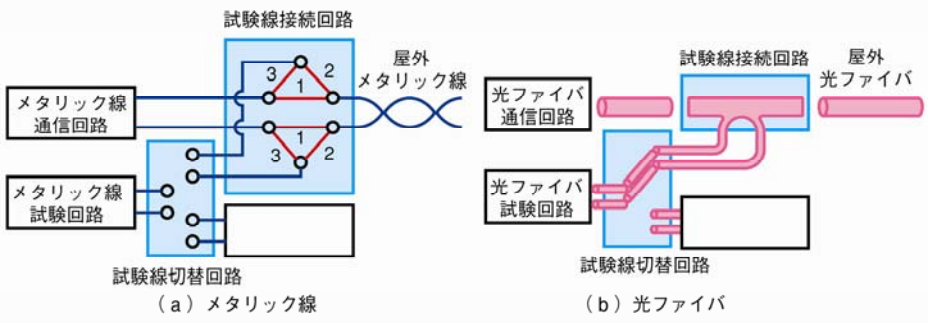


図 4･6　試験機能の共用

光ファイバの場合，試験線接続回路内にある光スイッチの特性により屋外光ファイバや光ファイバ通信回路を常に試験線切替回路側に接続する．通信中でもある程度の光電力が試験線切替回路側に流れるが，量が少ないため通信に影響はない．また，試験線切替回路を接続しなければ試験信号が挿入されることはない．試験線切替回路には光スイッチを設け，試験機の共用を図る．本方式では，通信用波長と異なる試験用波長を利用すれば，通信中でも試験が可能である．

(3)　故障点切り分け方式

4-2-2 項(3)に述べた多様な分界点に対応するために切り分け機能を設置する．**図 4･7** に故障点切り分け方式を示す．メタリック線の場合は，屋外アクセス線と宅内線とを切り分ける機能を保安器に内蔵する．また，宅内線と端末線を切り分ける機能をモジュラージャックに内蔵する．これらの試験は事業者側装置側より遠隔で行われる．これにより故障修理が迅速化されるとともに，故障箇所の責任者が通信事業者かユーザかが明確化される．

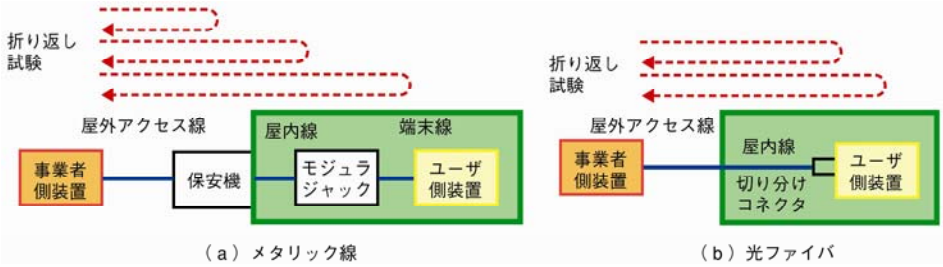


図 4･7　故障点切り分け方式

光ファイバの場合は，ユーザ側機器直前の光ファイバに切り分け機能付きコネクタを用いる．これにより媒体区間の故障か装置の故障かを遠隔折り返し試験により切り分けることができる．今後，光ファイバにおいても宅内線やユーザ側機器の解放やユーザ保守を行うためにはより細かい切り分け機能の検討が必要である．

(4)　警報転送方式

故障点の切り分けは，試験と警報を組み合わせて行う．AN の代表的な警報を**図 4･8** に示す．以下では，発生確率が非常に低いので，二重故障は対象外として説明する．

上り故障は，上りアクセス線故障，ユーザ側機器送信異常，及び事業者側装置受信異常の三つの原因が考えられる．警報を正常に検出している場合，事業者側装置受信は正常と判断できる．したがって，上りアクセス線故障か，ユーザ側機器送信異常が類推される．4-2-3 項(2)で述べた媒体試験を行い，異常ならばアクセス線故障，正常ならばユーザ側機器送信故障と特定できる．

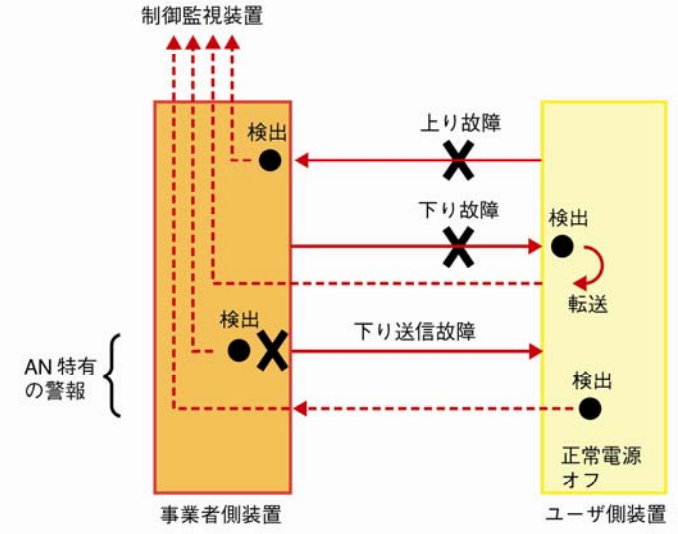


図 4･8　警報転送

下り故障は，下りアクセス線故障，事業者側装置送信異常，及びユーザ側機器受信異常の三つの原因が考えられる．下りアクセス線故障は，上りアクセス線故障と同様に，媒体試験により判別できるため，事業者側装置送信異常とユーザ側機器受信異常の切り分けが課題となる．4-2-2 項(4)で述べたとおり，ユーザ側機器で検出した運用管理情報は，制御監視装置に通知できない場合がある．そのため，AN 特有の機能として，事業者側装置に送信異常の検出機能を設ける．本警報が検出されれば事業者側装置送信異常であり，検出されなければユーザ側機器受信異常と特定できる．

更に，4-2-2 項(5)で述べたとおり，ユーザは自分の意志でユーザ側機器の電源を切る場合がある．この場合は，通信断が検出されても故障ではない．それを識別するために AN 特有

の機能としてユーザによる正常な電源オフを通知する機能を設ける．

これらに加えてユーザ側機器の正常・異常をより詳細に確認するために，バッテリーの充電状態，温度などの設置環境など多くの警報が定義される場合がある．

4-2-4 最新の課題解決技術

4-2-2 項(6)及び 4-2-2 項(7)の課題に対しては，これまでは人手による対応が行われてきた．例えば，配線の識別管理には色や文字による識別や荷札などの添付が行われていた．また，地理情報の管理は，紙ベースの原情報に対して人手による加筆修正を行ってきた．近年の情報技術の発達により，これらの管理方法が大きく変化している．

(1) タグの活用

メタリック線や光ファイバは，細径であり実装密度が高い．したがって，それらを管理するための識別子には小型であることが要求される．また，コンピュータへ電子的に情報を送れることが望まれる．近年，2 次元コードや IC タグ技術の利用が進められている．これらは荷札などと比較して情報量が多く小型であるため配線管理に最適である．**図 4･9** は光ファイバコネクタに 2 次元コードを添付した例である．実装密度の高いところでは，誤読み取り，誤書き込みの可能性があるため無線タグより 2 次元コードが適している．

図 4･9　光ファイバへの 2 次元コードの適用例

(2) GIS（Geographical Information System）の活用

GIS は，山や河川などの地形情報，道路や家屋などの情報などの上に，電柱や地下管路，ケーブルなどの情報を登録可能である．すべての情報をコンピュータで管理できるので，迅速性や正確性に優れる．これにより，形式や製造年などの設備情報と，位置や環境などの設置情報との連携が図れる．**図 4･10** は GIS によるケーブルルートの管理例である．道路上での位置関係を明確に表示できる．電柱へのケーブルの取付け状況などの写真との連携を行えばより一層の管理の向上が図れ，現地状況調査などの稼働を削減できる．

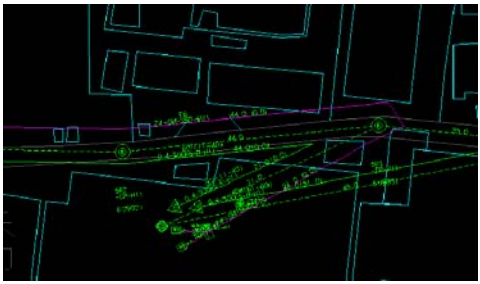


図 4･10　GIS を用いた屋外設備管理例

(3)　FWA 管理

ルーラルエリアのディジタルデバイドを早期，安価に解決する方法として，FWA は有力な手段であり，導入が進んでいる．FWA では，AP と WT を対象として，それらの回線開通業務及び保守・切り分け業務を達成するために，装置監視，設備管理，折り返し試験などの機能が必要である [2]．更に，無線特有の条件として，AP と WT 間の見通し率計算，干渉計算，回線品質計算などが必要である．それらを簡易な操作で高速に実現するためには，地形や建物，構造物などの情報を有し，伝搬特性を計算可能な置局設計用システムが必要である [3]．

4-2-5 まとめ

信号を単純に伝送するだけならば，中継ネットワーク技術や構内ネットワーク技術をそのまま AN に流用可能である．しかし，本章で説明したとおり，AN は，運用管理の面で非対称な構成とすることが必要である．中継用や構内用の運用管理機能をそのまま適用した場合は，試験や監視などのために非効率な設備構成，運用稼働が生じる．本章では，それらの課題や解決法を基本的な課題を中心に説明した．

AN は，ユーザと通信事業者とを接続するため，ユーザの利便性向上や通信事業者の事業運営向上のために，非常に重要である．特に，サービス開通や故障修理の迅速化や正確化などの運用管理向上の必要性が高い．光伝送技術や DSL 技術とともに，情報処理技術を活用することにより，利便性の高い AN を構築することが必要である．

更に，サービスの広帯域化に伴い光ファイバの利用が増加している．そのため，光ファイバなどの光設備に対してその管理技術高度化の要求が高まっている [4]．

■参考文献

1)　宇野浩司, 松雪康巳, “アクセスネットワーク管理,” 信学誌, vol.87, no.12, pp.1016-1021, 2004.
2)　市川敬章, 根元能成, 田中逸清, 渡邊和ニ, “ワイヤレス IP アクセスシステムのオペレーションシステムの構成と技術,” NTT R&D, vol.51, no.11, pp.959-967, 2002.
3)　丸山秀幸, 吉江智孝, “ワイヤレス IP アクセスシステム用置局設計システム,” NTT R&D, vol.51, no.11, pp.952-968, 2002.
4)　宇野浩司, “光設備管理,” 信学誌, vol.91, no.8, pp.706-713, 2008.

■5 群－9 編－4 章

4-3 ユビキタスネットワーク管理

（執筆者：堀内浩規）［2011 年 5 月 受領］

4-3-1 まえがき

「ユビキタス」はラテン語で「遍在する（いたるところに存在する）」の意味である．1980 年代後半に M. Weiser により「ユビキタスコンピューティング（遍在するコンピュータ）」が提唱され [1]，主に情報処理の分野で研究開発が開始された．近年，次世代情報通信ネットワークのあるべき姿として，いたるところにネットワークが存在し，いつでも，どこでも，情報機器がネットワークに接続され，様々な情報やコンテンツが利用可能となる「ユビキタスネットワーク（以下，ユビキタス NW と呼ぶ）」が注目されている．総務省の重点施策としてユビキタスネット社会（u-Japan）の実現が取り上げられており，産学連携によるユビキタス NW の研究開発プロジェクトなどが活発に進められている [2].

一方，携帯電話の加入者は国内で 1 億人を超え（2009 年 1 月），インターネット接続サービス（所謂，モバイルインターネット）の契約者は加入者の 8 割以上となっている．携帯電話ネットワークは重要な社会インフラとして発展するとともに，第 3 世代から第 4 世代へと更に進化が見込まれる．これらの携帯電話ネットワークや，無線 LAN を用いたホットスポットなども含めたモバイルネットワークは，ユビキタス NW を支える基盤ネットワークとして重要な役割を果たす.

本章では，まず，ユビキタス NW の概要を述べ，それを支えるモバイルネットワークの管理，更に，ユビキタス NW の運用と利用の効率化を行う Zero Administration 技術の動向や課題を述べる.

4-3-2 ユビキタスネットワークとは

(1) ユビキタスネットワークの概要

いつでも，どこでも，あらゆるものがネットワークに接続され，自由自在に映像や情報のやり取りを可能とするユビキタス NW は, 2010 年以降に成熟期を迎えると予測されている [3]. このユビキタス NW は**図 4･11** の概念図にも示される下記の特徴を持つ.

① 携帯電話端末，パソコン，PDA やカーナビなどの情報端末は既にネットワークに接続されているが，更に家庭のエアコン，電子レンジなどの情報家電やロボット，センサなどの多種多様な端末がネットワークに接続される．これにより，外出先からの携帯電話を用いた情報家電の操作など，ネットワークと連携した便利なサービスが可能となる.

② 非接触型 IC チップ（非接触型 IC カード，RFID など）が膨大な数の機器や商品に組込まれ，装置を介してネットワークに接続される．機器や商品の管理などの生産・流通の効率化にとどまらず，様々な応用サービスへの適用が期待されている.

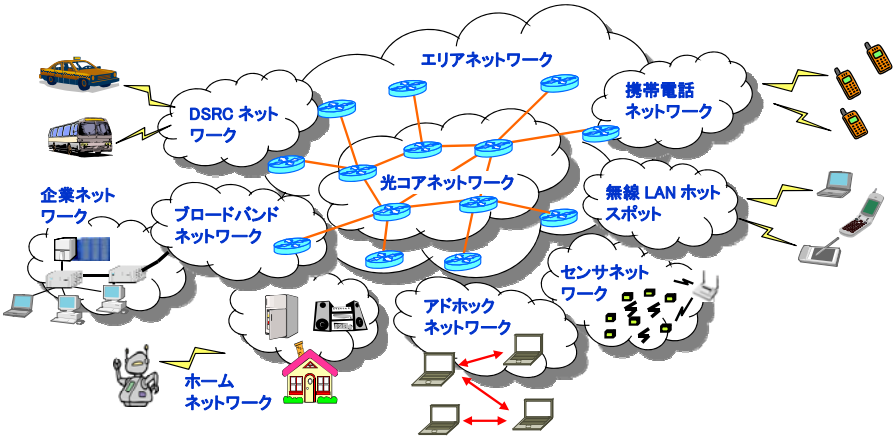
③ 多様なアクセスネットワーク経由で端末がネットワークに接続される．具体的には，FTTH（Fiber To The Home）などのブロードバンドネットワーク，情報家電が接続されるホームネットワークなどの固定系ネットワークに加え, 携帯電話ネットワーク, 無線 LAN, DSRC（専用狭域通信），アドホックネットワークなどからなるモバイルネットワークが想定され，これらのネットワークがシームレスに接続される．ここで，アドホックネッ

トワークとは，ネットワークインフラに依存することなく，中継機能を搭載した移動端末だけから構成する一時的なネットワークである．

④　ユビキタス NW ではインターネットが引き続き主要な役割を果たすが，膨大な数の端末がネットワークに接続されるため，従来の IPv4 からアドレス空間が広い IPv6 の適用が有望となる．

⑤　大量のトラヒックがバックボーンを流れるため，コアネットワークはテラビット級の光ネットワークで構成される．

⑥　ユビキタス NW ではインターネットにおける仮想空間の情報のみならず，位置や周辺環境などのユーザの状況を示す実空間の情報がセンサなどを介して取得可能になる．仮想空間と実空間との融合により，ユーザの状況に応じた最適なサービス（いわゆる，Context-aware サービス）の提供が期待されている．



※どこにいてもストレスなく，あらゆるサービスを自在に利用できるネットワーク．様々なものに通信機能付きチップが埋め込まれ，情報のやり取りが行われる．

図 4･11　ユビキタスネットワークの概念図

(2)　ユビキタスネットワークの管理

ユビキタス NW は多種多様な機能を持つ端末が多数収容され，大規模で複雑なネットワークとなる．このため，サービスの利用や運用管理の効率化が重要となり，ユーザや運用者に複雑な設定を強いることなく，簡便かつ安全にネットワークに接続し，サービスを利用可能とする技術が必要となる．本技術については 4-3-4 節で述べる．

また，ユビキタス NW では，固定系ネットワークとモバイルネットワークが混在した多様なアクセスネットワークを利用する．このため，異なるアクセスネットワークをまたがって移動する際にも，切り替えをユーザが意識せずに継続的に通信をサポートする移動管理技術も重要となる．これらの技術に関連する「FMC ネットワーク管理」は，本知識ベースの 4-4 節に記述されている．更に，ユーザからの多様なサービス要求やネットワークの状況に応じ

た最適なサービスを提供するためには，大規模ネットワークにおける経路制御や品質管理技術などを高度化する必要があり，これらの核となる技術も本編第 3 章に記述されている．

4-3-3 モバイルネットワーク管理

(1) 携帯電話の高度化

2000 年頃の携帯電話加入者のうちモバイルインターネットの加入者は 2 割程度であったが，その後，その割合は急増し，8 割以上となった．このように，携帯電話ネットワークは，人と人の通信から，人と物，更には物と物の通信へと適用領域が広がっていき，高速大容量伝送を実現する第 3 世代携帯電話の導入が進んだ．第 3 世代携帯電話の方式は，北米系 3GPP2[4] による cdma2000，欧州系の 3GPP [5]による W-CDMA の二つがあり，国内では，前者を KDDI，後者を NTT ドコモやソフトバンクが採用してサービスを提供，1x EV-DO や WiMAX，更には LTE（Long Term Evolution）など，ALL IP（4-3-3 節(2)で説明）への流れをかんがみ，データ通信の性能を高めたシステムの導入も進んでいる．更に，カメラ付き，ムービー撮影，ワンセグやお財布機能などの機能面の充実や，スマートフォンやタブレット端末など新しい端末の市場投入など，量的成長とともに質的な成長も見られる．

第 3 世代のネットワーク構成は，**図 4･12** に示すように一つの無線インタフェースが，音声通信のための回線交換ネットワークとデータ通信のためのパケット交換ネットワークとが別々のドメインを構成する．このため，携帯端末や加入者情報の管理は共有化されているが，端末の移動管理やサービス提供機能は音声通信とデータ通信で個別に実装されていることが多い．

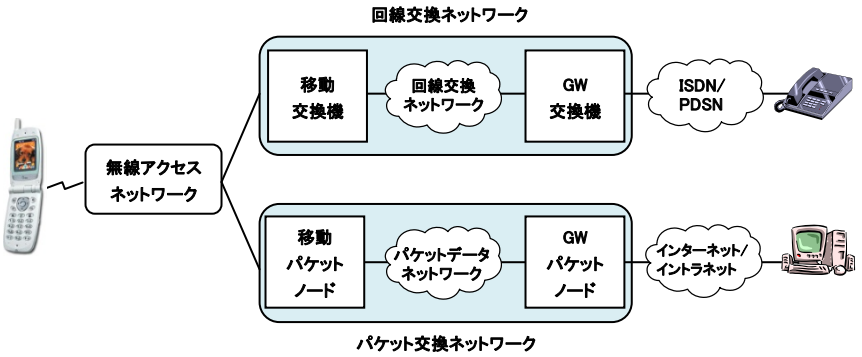


図 4･12　携帯電話ネットワークの基本構成

(2) ALL IP と新世代モバイル通信

LTE をはじめ，第 3 世代の後半（3.9 世代）には，これまで回線交換で提供された音声通信もパケット交換の IP 上で運ぶ，いわゆる ALL IP への移行が見込まれる [4), 5)]．ALL IP では，音声通信とデータ通信が統合され，マルチメディア情報としてすべて IP にカプセル化され，その呼制御プロトコルとして SIP（Session Initiation Protocol）[6)]（用語）を用いる．また，モ

バイル IP[7]を用いて，無線 LAN などと異なるアクセスシステムの間でも移動性を確保する汎用的な移動管理機能を提供する．本知識ベースの 4-4 節「FMC ネットワーク管理」の各技術の適用も見込まれる．

更に，次の世代として新世代モバイル通信システム（第 4 世代　IMT-Advanced）の検討や研究開発もある．第 4 世代では 2015 年頃モバイル環境で 50 Mbps-1Gbps の超高速大容量通信が研究開発の目標値とされている．第 4 世代のサービス実用化を目指し活動していた国内フォーラム mITF（mobile IT Forum）[8]が策定した新世代モバイル通信の参照モデルを**図 4･13** に示す．本参照モデルは以下の機能を持つ．

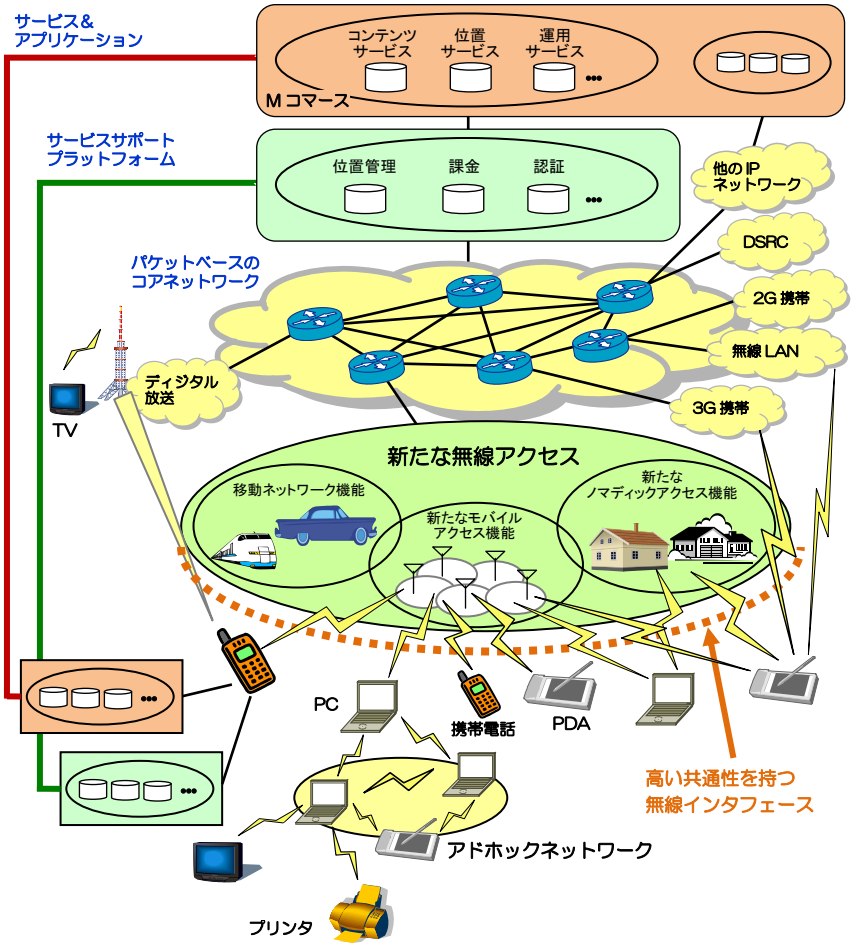


図 4･13　新世代モバイル通信（第 4 世代）のシステム参照モデル（mITF による）

- 携帯電話ネットワークや無線 LAN などの既存のモバイルアクセスを収容するとともに，高い共通性を有する無線インタフェースを持つ新たなモバイルアクセスが導入され，第 3 世代を含む統合発展型のネットワークを構成する．
- コアネットワークはパケットベースとする．
- 多様なサービスを提供するためのサーバ群は 2 層構成となる．すなわち，位置管理，課金，認証などの各種サポートプラットフォームと，ユーザの所望するコンテンツサービス，位置サービスならびに運用サービスなどのアプリケーションとサービスを提供するサーバ群からなる．
- ローカルな無線インタフェースを介し，アドホックネットワークなどで数多くの機器が協調して，単一の端末だけでは十分でなかったサービスをユーザは享受できる．
- 車両や電車などに収容される端末から構成されるネットワークの移動性をサポートする．

上述した様々な無線アクセスを包含するパケットベースの新世代モバイル通信のシステム構成は，ユビキタス NW の基本構成要素となると考えられる．このシステムの NW 管理としては，NW，サーバや端末自体に対する一般的な障害，構成，性能の管理は必須となる．それらに加え，端末が最適な NW を選択するため，接続可能な NW の種類，状態や接続の優先度などの管理，発着呼や場所に応じた Context-aware サービスの提供などのため，位置情報や所有者のプロファイルの管理なども必要となる．また，サービスの利用やトラフィックの計測値に応じた課金やユーザや端末認証などのセキュリティ管理も重要となる．

(3) 携帯端末を対象とするデバイス管理

様々な国や地域で提供される携帯端末向けサービスの相互運用性向上を目的に，プロトコル仕様を策定する標準化団体 OMA（Open Mobile Alliance）[9]が組織されている．OMA の標準化活動の一つとして，携帯端末を対象とするデバイス管理のプロトコル仕様策定がデバイス管理作業部会で進められている．ここでは，80 を超える仕様が公開されており，仕様準拠の製品も 40 を超えている（2011 年 4 月現在）．管理モデルと管理プロトコルは OMA の前身の一つである SyncML Initiative が策定した SyncML[10]を基にしている．SyncML は携帯端末と他情報通信機器とのデータ同期や携帯端末のデバイス管理を目的に策定された XML（eXtensible Markup Language）を基本とするプロトコル仕様である．

SyncML デバイス管理プロトコルでは，管理情報の最小単位はノードと呼ばれ，複数のノードが木構造で管理される．ノードは URI（Uniform Resource Identifiers）を使って一意に識別，操作される．インターネットの管理プロトコルとして広く普及する SNMP（Simple Network Management Protocol）[23]では管理情報がテーブル構造で，オブジェクト識別子で一意に識別する点で異なる．管理操作については，ほとんどの携帯端末に装備されるディスプレイから操作することを想定し，操作内容の表示や操作の実行確認入力など，ディスプレイ入出力のための操作（User interaction alert）をはじめ，SNMP には見られない操作が定義されている．また，携帯端末向けサービスで重要となる位置情報は，SyncML デバイス管理プロトコル同様，OMA では XML を基本に記述されている．今後，位置情報が管理情報としても利活用で

ければ「いつでも，どこでも，ネットワークに接続できる情報端末」の管理に一層有効となろう．

4-3-4 ユビキタスネットワークにおける Zero Administration 技術

(1) Zero Administration 技術とその必要性

4-3-2 節で述べたように，ユビキタス NW は多種多様な機能を持つ端末が多数収容される大規模で複雑なネットワークとなることが予想される．ユビキタス NW の中核をなすと考えられるインターネットは，当初，学術目的で研究開発された経緯がある．例えば，国内で契約 1,977 万回線（2010 年 12 月末現在）を超える FTTH（Fiber To The Home）インターネット接続サービスの利用にはインターネットに関する高度な専門知識や経験が必要であり，これら知識や経験を持たないユーザにとっては利用に至るまでの妨げとなっている（**図 4･14** 左下）．また一方で，ネットワークは日々大規模化し，高度な専門知識や経験を持つ限られた数のネットワーク運用者だけでは，近い将来，運用管理が手に負えなくなってしまう（図 4･14 右中）．このため，ユーザや運用者に煩わしい設定を強いることなく，端末やネットワーク機器などをネットワークに簡便に接続し，サービスを利用，制御する技術（以下，Zero Administration 技術と呼ぶ）がユビキタス NW の運用管理においては必要となる．

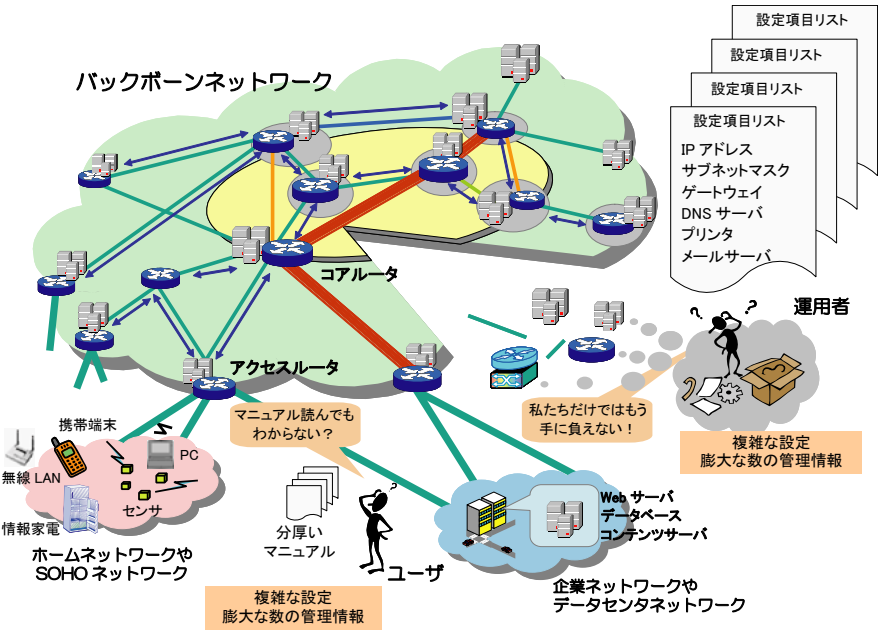


図 4･14 Zero Administration 技術の必要性

(2)　Zero Administration 技術実現に向けた取り組み

Zero Administration 技術の実現に最も有効な手段の一つは自動設定であるが，これは次の二つに分類できる．

(a)　集中型自動設定

端末やセンサ，ネットワーク機器などの設定対象に対し，これら対象に設定するアドレスなどの管理情報の値を限られた数のサーバなどに運用者があらかじめ投入，一括管理する．端末やセンサ，ネットワーク機器がネットワークに接続する際，サーバから管理情報の値を設定対象に自動設定し，サービスを利用，制御可能とする．

(b)　分散型自動設定

多数の端末やセンサ，ネットワーク機器が集まって一つのネットワークを構成する際，あるいは既存のネットワークに接続する際，ネットワークを構成する端末やセンサ，ネットワーク機器が自律分散協調して管理情報の値を矛盾のないように決定する．決定した管理情報を自身やほかに自動設定し，サービスを利用，制御可能とする．

集中型自動設定は，「Zero」ではないものの，管理対象を少数のサーバなどに限定することで，高度な専門知識や経験を持つ運用者が運用管理する端末やセンサの数を少なくすることを狙う．一方，分散型自動設定は，今後も継続的に高機能化する端末やセンサを想定し，ユーザや運用者による手動設定を理想的には文字通り「Zero」にすることを狙う．

これまでに多数の自動設定方式が知られており，いくつかは実用化されている．IP ネットワークやリンクにおける代表的な自動設定方式を対象に，上述した「分類」と「各方式が自動設定の対象とする管理情報」の点から整理した結果を**図 4･15** とともに以下に示す．

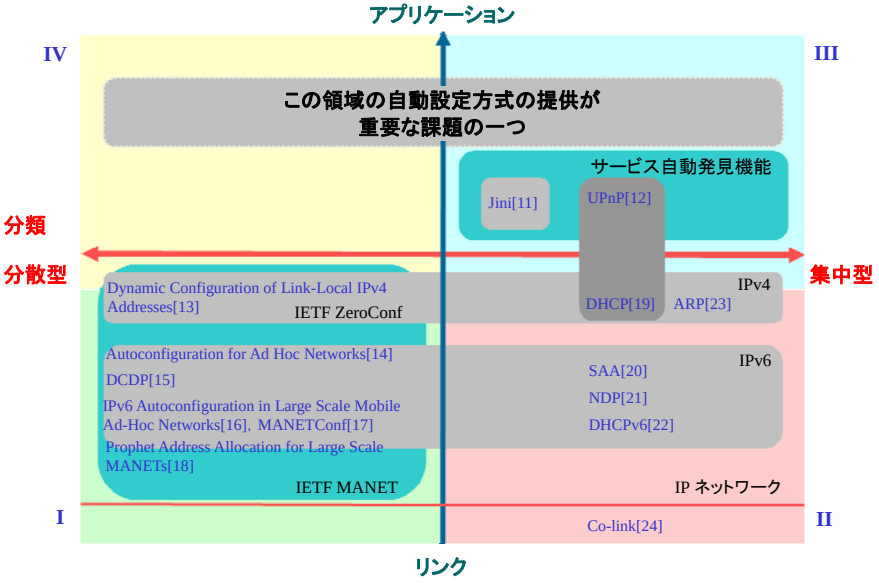


図 4･15　代表的な自動設定方式

［I の領域］

モバイルアドホックネットワークやセンサネットワークを対象に，IP ネットワークやリンクに関する管理情報を自動設定する方式が該当する．これまでのところ IP ネットワークを対象とする研究開発[11)−16)]が盛んである．IPv4 のリンクローカルアドレスを対象に IETF ZeroConf が標準化[13)]を進めている．また，モバイルアドホックネットワークを対象に IETF MANET Working Group がいくつかの方式[12)−16)]の標準化を進めている．

［II の領域］

IP ネットワークやリンクに関する管理情報を自動設定する方式が該当する．DHCP（Dynamic Host Configuration Protocol）[17)]はホームネットワークをはじめ現在広く利活用されている．IPv6 に関しても SAA（Stateless Address Autoconfiguration）[18)]や NDP（Neighbor Discovery Protocol）[19)]，DHCPv6[20)]などの自動設定方式が次第に実用化されつつある．また，DHCP サーバと RAP（Router Autoconfiguration Protocol）[21)]サーバと呼ばれるサーバが協調動作し，ルータを数珠繋ぎに自動設定する方式が研究開発されている．更に，赤外線などを無線 LAN リンクの自動設定に使う方式も提案されている[22)]．

［III の領域］

IP ネットワークに関する管理情報に加え，プリンタなどを自動発見し，印刷サービスを自動設定する方式が該当する．Sun Microsystems による Jini[23)]や UPnP Forum による UPnP（Universal Plug and Play）[24)]が広く知られる代表的な方式である．Jini では，lookup サービスとしてサービスの発見や発見したサービスの利用，制御に必要な手段を集中管理し，サービスを利用する端末などにそれらを提供する．なお，UPnP などのホームネットワークで使用されるプロトコルは，本編第 5 章「ホームネットワーク管理」に詳述されている．

［IV の領域］

IP ネットワークに関する管理情報に加え，TV 会議などの多地点 P2P（Peer to Peer）アプリケーションなどを対象とする自動設定方式が該当する．広く知られた代表的な方式は少なく，今後の研究開発が期待される．

(3) Zero Administration 技術実現の課題

多くのユーザにとって有用な技術となるためには，ネットワークに加え，ネットワークを使って実現されるサービスやアプリケーションに関する煩わしい設定からもユーザや運用者を解放することが必要である．特定のサービスやアプリケーションのみに対応した自動設定技術は多数あるものの，4-3-4 節(2)で概観したように，（図 4･15 の III と IV の領域に含まれる）ネットワークからアプリケーションまでを一括して自動設定する技術は今のところ少なく，その研究開発[25)−30)]が今後も期待される．この一例として，ADSL 常時接続環境のホームネットワークを対象に，IP ネットワークとともに，無線 LAN，E-mail，ならびに VoIP などのアプリケーションの管理情報を一括して自動設定するシステム[25)]が開発されている．

また，Zero Administration 技術は所望のセキュリティを保つことと表裏一体の関係にある．Zero Administration 技術を一方的に押し進めてしまうと，セキュリティを保つことが難しくなる場面がしばしば生じる．例えば，無線 LAN などで利用される暗号化鍵が該当する．Zero

Administration 技術実現の点では，強引ではあるが，すべてのユーザに共通の鍵を設定することが容易である．しかしながら，それでは明らかに所望のセキュリティを保てない．このため，今後は所望のセキュリティを保ちながら目的を達成できる Zero Administration 技術の研究開発が課題になる．

4-3-5 まとめ

本章では，いつでも，どこでも，あらゆるものがネットワークに接続され，様々な情報やコンテンツが利用可能となるユビキタスネットワーク，その基盤となるモバイルネットワーク，ならびに，運用や利用の効率化のキーとなる Zero Administration 技術についてネットワーク管理の観点から述べた．本章では触れられなかったが，ユビキタスネットワークの普及のためにはセキュリティ，プライバシー，著作権なども重要な課題である．ユビキタスネットワークが人々の社会生活に浸透していくためには更なる研究開発が必要と考えられるが，通信サービスの基盤として早期の実現を期待したい．

■参考文献

1) M. Weiser, “Some computer science issues in ubiquitous computing,” Commun. ACM, vol.36, no.7, pp.75-84, 1993.
2) ユビキタスネットワーキングフォーラム, “ユビキタスネットワーク戦略,” クリエート・クルーズ, Dec. 2002.
3) “小特集「ユビキタスネットワーク技術開発プロジェクト」,” 信学誌, vol.91, no.7, pp.562-603, 2008.
4) 3GPP2: http://www.3gpp2.org/
5) 3GPP: http://www.3gpp.org/
6) J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, “SIP: session initiation protocol,” IETF RFC 3261, 2002.
7) C. Perkins, IP Mobility Support for IPv4, IETFRFC3220, Jan, 2002.
8) 中西, “モバイル・コンテンツ・サービスの可能性,” 情報処理学会研究報告, 2005-AVM-49, pp.1-6, Jul, 2005.
9) OMA: http://www.openmobilealliance.org/
10) J. Case, M. Fedor, M. Schoffstall, and J. Davin, “A Simple Network Management Protocol (SNMP),” IETF RFC 1157, 1990.
11) S. Cheshire, B. Aboba, and E. Guttman, “Dynamic Configuration of Link-Local IPv4 Addresses,” Internet Draft: draft-ietf-zeroconf-ipv4-linklocal-14.txt, March, 2004.
12) C.E. Perkins, J. Malinen, R. Wakikawa, E. Belding-Royer, and Y. Sun, “Autoconfiguration for Ad Hoc Networks,” Internet Draft: draft-ietf-manet-autoconf-01.txt, November, 2001.
13) A. Misra, S. Das, and A. McAuley, “Autoconfiguration, Registration, and Mobility Management for Pervasive Computing,” IEEE Personal Commun., vol.8, no.4, pp.24-31, August, 2001.
14) K. Weniger and M. Zitterbart, “IPv6 Autoconfiguration in Large Scale Mobile Ad-Hoc Networks,” In Proc. of European Wireless 2002, pp.142-148, February, 2002.
15) Nesargi and R. Prakash, “MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network,” In Proc. of IEEE INFOCOM 2002, pp.1059-1068, June, 2002.
16) H. Zhou, L.M. Ni, and M.W. Mutka, “Prophet Address Allocation for Large Scale MANETs,” In Proc. of IEEE INFOCOM 2003, pp.1304-1311, April, 2003.
17) R. Droms, “Dynamic Host Configuration Protocol,” RFC 2131, March, 1997.
18) S. Thomson and T. Narten, “IPv6 Stateless Address Autoconfiguration,” RFC2462, December, 1998.
19) T. Narten, E. Nordmark, and W. Simpson, “Neighbor Discovery for IP version 6 (IPv6),” IETF RFC2461, 1998.

20) “Dynamic Host Configuration Protocol for IPv6 (DHCPv6),” ed. by R. Droms, IETF RFC3315, July, 2003.
21) K. Hori, K. Yoshihara, and H. Horiuchi, “Automatic Configuration of IP Networks and Routers,” in Proc. of APNOMS2003, pp.248-259, October, 2003.
22) J. Tourrilhes and V. Krishnan, “Co-Link configuration: Using Wireless Diversity for More Than Just Connectivity,” Tech. Rep. of Hewlett Packard Laboratories, HPL-2002-258, 2002.
23) Sun Microsystems, “JiniPTMP Architecture Specification Version 2.0,” June, 2003.
24) UPnP Forum, “Universal Plug and PlayPTMP Device Architecture 1.0,” June, 2000.
25) K. Yoshihara, T. Kouyama, M. Nishikawa, and H. Horiuchi, “Server Support Approach to Zero Configuration In-Home Networking,” in Proc. of DSOM2004, pp.232-234, November, 2004.
26) S. Motegi, K. Yoshihara, and H. Horiuchi, “Address Autoconfiguration for Event-Driven Sensor Network,” IEICE Trans. Commun., vol.E-88B, no.3, pp.950-957, March, 2005.
27) 堀 他, “動的なサブネット構成により管理作業を削減した IP ルータ自動設定方式,” 信学 B, vol.J88-B, no.7, pp.1213-1226, 2005
28) 吉原 他, “構成情報の照合による宅内通信機器予備診断方式,” 信学誌 B, vol.J89-B, no.4, pp.507-518, 2006.
29) 堀 他, “Auto-configuration Method of Provisioning System for Internet VPNs,” IEICE Trans. Commun., vol.E89-B, no.9, pp.2424-2433, 2006.
30) D. Arai, K. Yoshihara, A. Idoue, and H. Horiuchi, “Server Support Approach to Zero Configuration of Power Line Communication Modems and Coaxial Cable Modems,” in Proc. of APNOMS2007, pp.92-101, October, 2007.

■5 群－9 編－4 章

4-4 FMC ネットワーク管理

（執筆者：高橋和秀）［2008 年 8 月 受領］

4-4-1 FMC を実現する技術

FMC（Fixed Mobile Convergence）とは，無線通信と有線通信を連携させる通信サービスやこれを実現する技術の総称である．FMC 通信サービスの代表例としては，家の中において携帯端末を IP 電話の端末として使用できる通信サービス（One Phone/One Number サービス）があげられる．BT（British Telecommunications）は，2005 年 6 月より，本サービス（BT Fusion）を提供している．FMC 通信サービスが対象とする通信ネットワークとその通信端末は，802 系ネットワーク，3GPP/3GPP2 系ネットワーク，FTTH，CATV，ADSL など，多種多様である．このため，ユーザに対して，これらの通信ネットワークの存在や通信端末の差異を意識させない，シームレスな通信サービスを提供するために，デバイスの切替えや，ヘテロジニアスな通信ネットワーク間にて移動時においてもサービスの継続性の保証や，デバイスやネットワーク状況に適した End-to-End での QoS 制御が課題となる．そこで，課題解決に必要なネットワーク管理技術を**図 4･16** に示す．

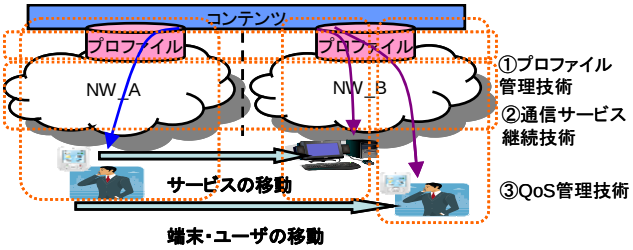
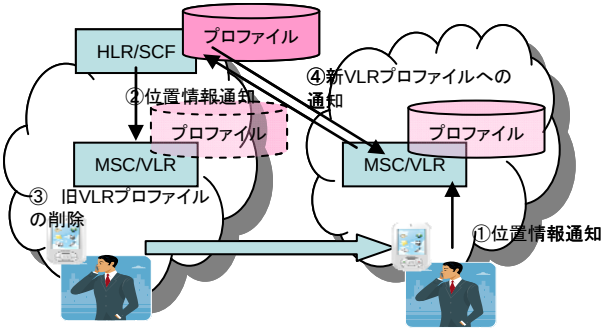


図 4･16　FMC サービス概要

携帯電話の電話番号や機体番号，PC 端末の IP アドレス，ユーザの位置情報やサービス状態などの，ユーザや通信端末の属性を表現する情報はプロファイルと呼ばれる．このプロファイルは，通信ネットワークや通信キャリアごとに異なる．ヘテロジニアスな通信ネットワークや通信キャリア間で，これらを一元的に管理する，または流通する技術がプロファイル管理技術である（①）．また，ユーザや通信端末がヘテロジニアスな通信ネットワーク間を移動（ローミング）した場合に，通信サービスやそのアプリケーションを継続させる技術が，通信サービス継続技術である（②）．また，ヘテロジニアスな通信ネットワーク間の通信サービスにおいて，ネットワークの帯域を管理し，端末やコンテンツなどの特性に応じて最適な帯域を提供する技術が QoS 管理技術である（③）．その他の技術として，ローミング先の通信ネットワークの候補が複数存在する場合，ユーザの位置，コンテンツ，帯域，料金などのコンテクストに応じて，最適な通信ネットワークに自動的にローミングさせるコンテクストアウェア技術がある．これらのネットワーク管理技術のサーベイ論文に文献 1), 2) がある．

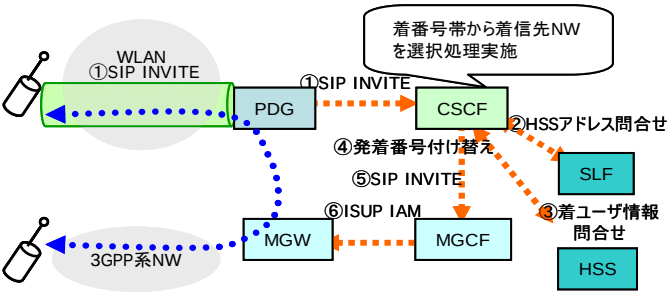
4-4-2 プロファイル管理技術

IMT-2000 ネットワークのローミングサービスにおけるプロファイル管理について，3GPP（3rd Generation Partnership Project）[3] が標準化している VHE（Virtual Home Environment）方式 [4] を**図 4･17** に示す．ここで，SCF（Service Control Function）は，プロファイルを管理するエンティティである．本方式においては，通信端末が異なる通信キャリアの通信ネットワークにローミングアウトした場合，移動元ネットワークの SCF から，移動先ネットワークの MSC へプロファイルを流通させる．



HLR ： Home Location Register
VLR ： Virtual Location Register
SCF ： Service Control Function
MSC ： Mobile Switching Centre

図 4･17 VHE でのローミングアウト処理



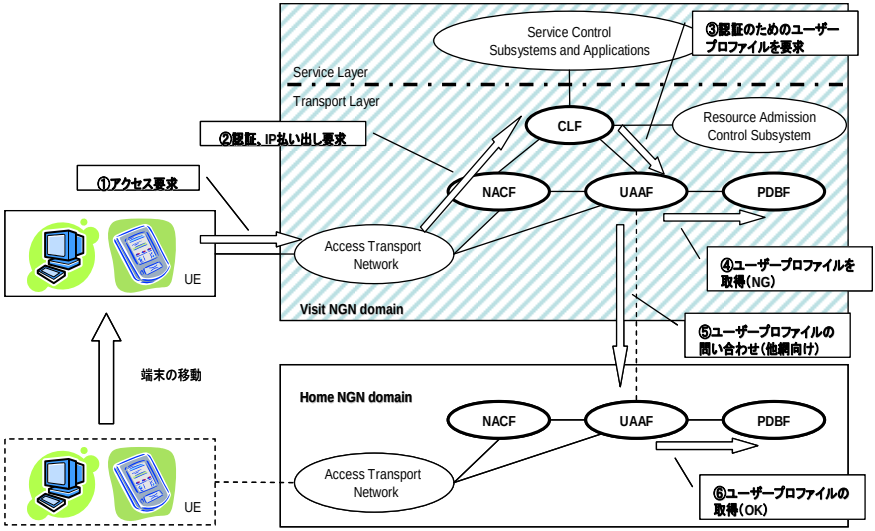
PDG ： Packet Data Gateway
CSCF ： Call Session Control Function
MGCF ： Media Gateway Control Function
MGW ： Media Gateway Function
SLF ： Subscription Locator Function
HSS ： Home Subscriber Server

図 4･18 3GPP での One Phone/One Number サービス

3GPP 系 NW と WLAN 間の通信サービスの連携におけるプロファイル管理について，3GPP が標準化している方式 [5] を**図 4･18** に示す．ここで，HSS（Home Subscriber Server）は，プロファイルを管理するエンティティである．本方式においては，3GPP 系ネットワークの電話

番号と WLAN の IP 電話番号の対応関係を HSS で管理している．本方式により，3GPP 系ネットワークの電話番号を用いて，WLAN に位置する携帯端末と 3GPP 系ネットワークに位置する携帯端末間の発着信が可能となる．3GPP での One Phone/One Number サービスについては，2008 年 10 月よりサービス展開されている．

NGN（Next Generation Network）におけるプロファイル管理について，TISPAN（Telecoms & Internet converged Services & Protocols for Advanced Networks）[6] が標準化を進めている NASS（Network Attachment Sub-System）[7), 8)] を**図 4･19** に示す．NASS においては，PDBF（Profile DataBase Function）がプロファイルを管理する．通信端末が，Home NGN Access Network から Visit NGN Access Network にローミングした場合，Visit NGN Access Network の UAAF（User Authentication and Authorization Function）は当該通信端末のプロファイルを管理している Home NGN Access Network の UAAF に認証情報の問合せを行う．この認証が完了すると，Visit NGN Access Network の NACF（Network Access Configuration Function）から通信端末に IP アドレスなどの情報を割り当て，CLF（Connectivity session Location and repository Function）において通信端末の位置情報を管理する．なお，もうひとつの NGN 標準化団体である ITU-T（International Telecommunication Union Telecommunication standardization sector）では，本処理を実現する機能を NACF（Network Attachment Control Function）として規定している．NGN 方式については，2008 年 3 月より商用でのサービス展開がなされている．



NASS : Network Attachment Sub-System, NACF : Network Access Configuration Function、CLF : Connectivity session Location and repository Function, UAAF : User Authentication and Authorization Function, PDBF : Profile DataBase Functiorn、UE : User Equipment

図 4･19　TISPAN NGN NASS アーキテクチャ及びローミング時の動作

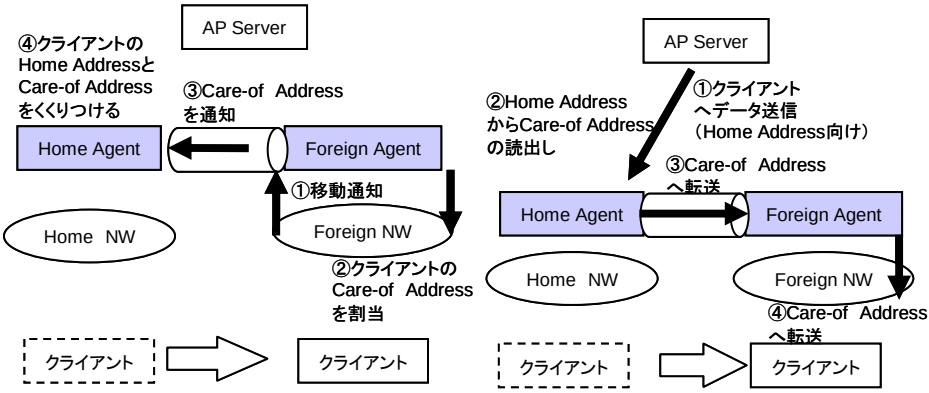
WWW を利用するユーザのプロファイル（認証情報）を一元管理する技術に SSO（Single Sign On）がある．SSO によれば，複数サービスの利用について，アクセス権限を有するユーザが一度の認証を受けるのみで，すべてのサービスの利用を許可することが可能である．現

在，利用可能な SSO としては，Microsoft[9] が主導する Windows Live ID と Sun Microsystems[10] が主導する Liberty Alliance が有名である．

4-4-3 通信サービス継続技術

通信サービス継続技術について，通信プロトコル階層ごとに説明する．データリンク層において通信を継続する方式に，IEEE 802.21 規格において検討されている MIHF（Media Independent Handover Function）[11] がある．IEEE 802.21 規格においては，802 系ネットワークと非 802 系ネットワーク（3GPP/3GPP2 系ネットワークなど）間でシームレスなハンドオーバを実現するために，MIHF（Media Independent Handover Function）がレイヤ 2 の状態をレイヤ 3 以上に伝えることより，最適な無線通信ネットワークへ短時間にハンドオーバすることが可能となる．MIHF については，3G 網と LTE 網間などの異なる無線通信ネットワーク間ハンドオーバについて検証を進めている．

ネットワーク層において通信を継続する方式に，RFC 3344 において定義されている Mobile IP（IPv4）[12] がある．本方式を**図 4･20** に示す．通信端末が外部ネットワーク（Foreign Network）へ移動した場合は，通信端末は外部エージェント（Foreign Agent）が広告している気付きアドレス（Care-of-Address）を取得し，このアドレスを外部エージェント経由でホームエージェント（Home Agent）に登録する．ホームエージェントは，外部エージェント経由で通信端末宛のパケットを移動先の通信端末へ転送する．



(a) 端末移動時のシーケンス　　(b) 端末移動後の着信シーケンス

図 4･20　Mobile IP での端末移動

セッション層において通信を継続する方式に，RFC 3261 で定義されている SIP（Session Initiation Protocol）[13] を用いた Call Transfer[14] と 3PCC（3rd Party Call Control）[15] の二つの方式がある．Call Transfer はインターネットドラフト，3PCC は RFC 3725 で定義されている．Call Transfer 方式を**図 4･21** に，3PCC 方式を**図 4･22** に示す．Call Transfer は，移動する通信端末に対する通信先が SIP コントローラとなり，移動先の通信端末にセッション状態を転送する方式である．また，3PCC は，移動元の通信端末が SIP コントローラとなり，移動先の

通信端末にセッション状態を転送する方式である．また，SIP によるセッションを記述する言語として，RFC 4566 で定義されている SDP（Session Description Protocol）[16] がある．セッション状態，トランスポートプロトコル（RTP，RSTP など），メディア種別（音声，映像，画像など），メディア形式（H.261 ビデオ，MPEG ビデオなど），タイムスタンプなどのメディアネゴシエーションを行うための情報要素は，この SDP を用いて記述する．これらの情報要素は，SIP 基本メソッドである INVITE/200/ACK のメッセージボディ部に組み込まれ，SIP セッションを確立する際に，通信端末の間でネゴシエーションされる．Mobile IP や SIP については様々なネットワーク機器へ機能実装されている．

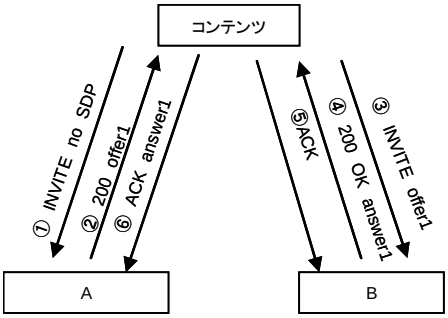


図 4･21　Call Transfer でのサービス移動

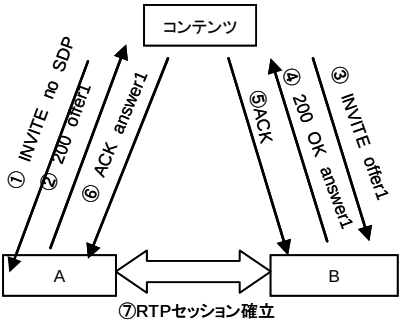


図 4･22　3PCC でのサービス移動

4-4-4 QoS 管理技術

3GPP は，UMTS（Universal Mobile Telecommunications System）Forum [17] において規格化された QoS 制御方式 [18] を採用している．C-Plane においては，ネットワークエンティティごとに存在する BS マネージャが，そのリソース管理を行い，サービスに対してリソースの割当てを行う．U-Plane においては，MT（Mobile Terminal）及び CNGW（Core Network GateWay）に存在するクラシフィケーション機能がパケットのクラスに応じて優先制御を行う（Diffserv）．優先制御クラスには，会話クラス，ストリーミングクラス，インタラクティブクラス（WWW やメールなど），及びバックグランドクラス（ftp によるファイル転送など）の四つが定義されており，この順に優先度が高い．ただし，ヘテロジニアスな通信ネットワークにまたがる QoS 制御に関する規定はない. ヘテロジニアスな通信ネットワークにまたがる QoS 制御に関する研究に，QoS Broker [19]，DRM [20]，効用関数を用いる手法などがある．

NGN における QoS 管理について, TISAPN が標準化している RACS（Resource and Admission Control Sub-System）[21), 22)] を**図 4･23** に示す．RACS は，リソース割当てやパケット遅延のゆらぎの制御などを行う．SPDF（Service Policy Decision Function）は，アプリケーションサーバからの要求を契機に, プロバイダのサービスポリシーに対応したリソース割当てを決定し，リソース割当て要求を RACF に転送する. この要求を受信した RACF（Resource and Admission Control Function）は，NASS からリソース使用状況を取得し，割当て可能なリソースを割り当てる．ローミングの場合は，移動元の SPDF がローミング先の SPDF に要求を転送する．

なお，ITU-T では，本処理を実現する機能を RACF（TISPAN の RACF と同名称）として規定している．

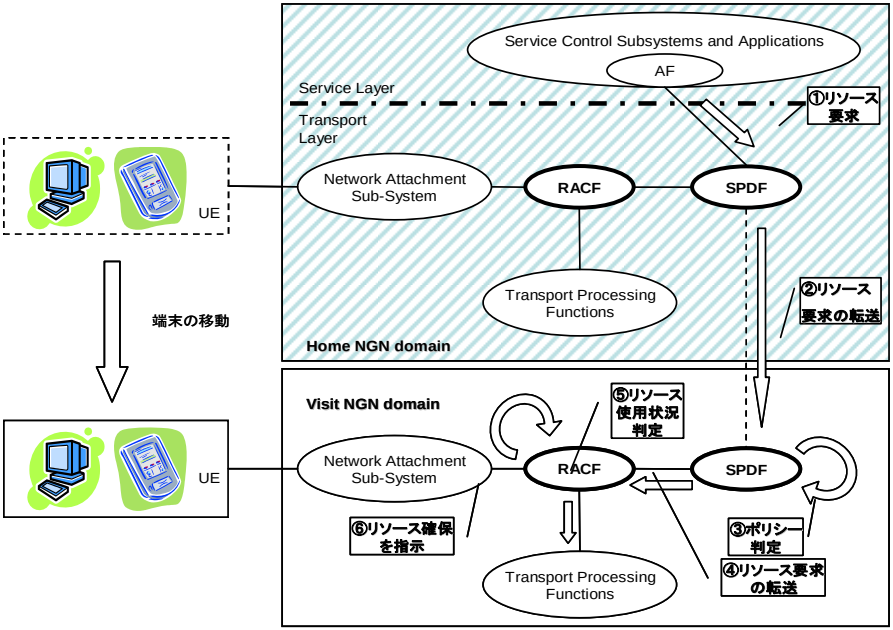
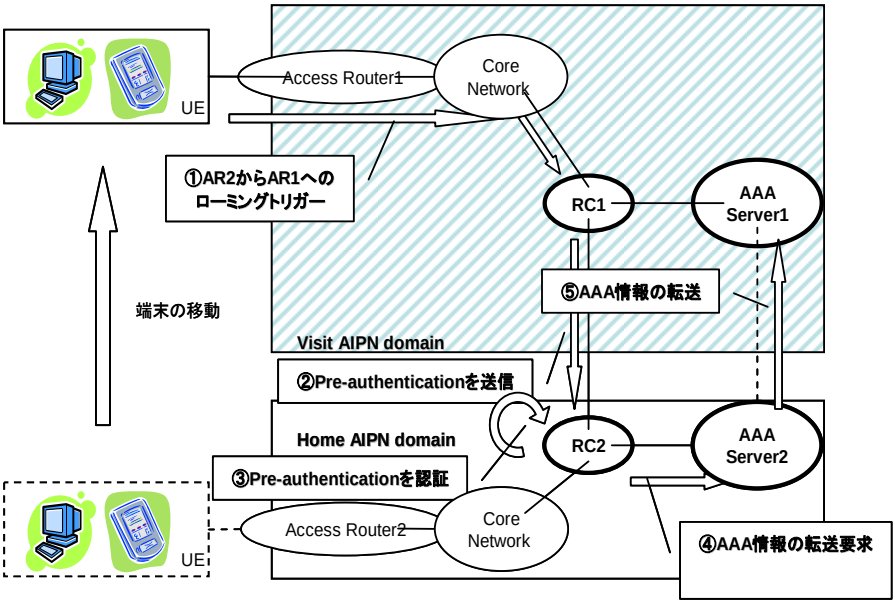


図 4･23　TISPAN NGN RACS アーキテクチャ及びローミング時の動作

4-4-5 その他の技術

4G に向けたコンテクストアウェア技術について提案を行っている研究に，RC（Roaming Coordinator）[23] がある．本提案方式を**図 4･24** に示す．本方式においては，Visited Network の RC は，Home Network のアクセスルータが管理対象ドメイン内に存在していないことを検知すると，Home Network の RC に Pre-authentication（認証済みを示すセットアップ情報）を送信する．この Home Network の RC が Visited Network の RC から送信された Pre-authentication を承認できた場合，Home Network の AAA から Visited Network の AAA にプロファイル（認証情報）を転送する．コンテクストアウェア技術については研究段階である．



AIPN : All IP Network, AAA : Authentication Authorization Accounting

図 4･24　4G Network RC アーキテクチャ及びローミング時の動作

■参考文献

1) 今井和雄, 山崎憲一, 中村　寛, ヴォルフガング ケレラー, 倉掛正治, “シームレス通信サービスとその研究開発の動向,” 信学論 B, vol.J89-B, no.8, pp.1347-1356, Aug. 2006.
2) 宇野新太郎, “ユビキタス環境におけるシームレス通信サービスとその実現技術,” 信学論 B, vol.J89-B, no.8, pp.1334-1346, Aug. 2006.
3) “3GPP,” http://www.3gpp.org/
4) 3GPP TR 22.121, “The Virtual Home Environment,” Jun 2002. http://www.quintillion.co.jp/3GPP/Specs/22121-531.pdf
5) 3GPP TS 22.234, “Requiements on 3GPP system to Wireless Local Area Network (WLAN) interworking (Release6),” v8.1.0, Jun. 2007, http://www.quintillion.co.jp/3GPP/Specs/22234-810.pdf
6) “TISPAN,” http://www.etsi.org/tispan/
7) ETSI ES 282 001 v2.0.0, “NGN Functional Architecture,” Mar. 2008.
8) ETSI ES 282 004 v2.0.0, “NGN Functional Architecture - Network Attachment Sub-System (NASS),” Feb. 2008.
9) “Microsoft,” http://www.microsoft.com/ja/jp/default.aspx
10) “Sun Microsystems,” http://jp.sun.com/
11) “IEEE 802.21,” http://ieee802.org/21
12) C. Perkins, “IP Mobility Support for IPv4,” RFC3344, Aug. 2002.
13) J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, “SIP: Session Initiation Protocol”, RFC3261, Jun. 2002.
14) R. Sparks, “The Session Initiation Protocol (SIP) Refer Method,” Apl. 2003.
15) J. Rosenberg, J. Peterson, H. Schulzrinne, G. Camarillo, “Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP),” RFC 3725, Apr. 2004.
16) M. Handley, V. Jacobson, C. Perkins, “SDP: Session Description Protocol,” Jul. 2006.

17) “UMTS Forum,” http://www.umts-forum.org/
18) 3GPP TR 23.802, “Architectural enhancements for end-to-end Quality of Service (QoS) (Release 7),” v7.0.0, http://www.quintillion.co.jp/3GPP/Specs/23802-700.pdf, Sep. 2005.
19) V. Mrgues, R. Aguiar, C. Garia, J. Moreno, C. Beaujean, E. Melin, and M. Liebsch, “An IP-Based QoS architecture for 4G operator scenarios,” IEEE Wireless Commun., vol.10, no.3, pp.54-62, Jun. 2003.
20) J. Hillebrand, C. Prehofer, R. Bless, and M. Zitterbart, “Quality-of service signaling for next generation IP-based mobile networks,” IEEE Commun. Mag., vol.42, no.8, pp.72-79, Jun. 2004.
21) ETSI ES 282 001 v2.0.0, “NGN Functional Architecture,” Mar. 2008.
22) ETSI ES 282 003 v2.0.0, “Resource and Admission Control Sub-System (RACS): Functional Architecture,” May 2008.
23) M, Lee and S, Park, “A Context-Aware Seamless Interoperator Roaming Management Framework in 4G Networks,” IEICE TRANSACTIONS on Communications vol.E90-B, no.11, p.3015-3023, Nov. 2007.

■5 群－9 編－4 章

4-5 カスタマネットワーク管理/ホームネットワーク管理

（執筆者：登内敏夫）［2008 年 8 月 受領］

4-5-1 カスタマネットワーク管理

(1) 背 景

カスタマネットワーク管理（CMN：Customer Network Management）とは，事業者から提供されているサービスに関する情報に，ネットワークを通して顧客がアクセスすることを可能にするサービスである [1].

企業が拠点間接続のため，キャリアから専用線サービスを受ける場合，専用線と拠点内の LAN が接続されている状況を考える．その場合，企業側のシステム管理者は拠点内 LAN だけではなく，専用線の状態も統合的に管理する必要がでてくる．例えば，トラヒックの増大によりシステム設計を見直す際，ボトルネックが LAN 側にあるのか，専用線側にあるのか検討する必要がある．そのために，専用線側のトラヒックも把握する必要がある．このように，キャリア側が所有・管理する専用線の情報を顧客である企業側に提示する CMN が求められるようになってきた．

また，1990 年後半には，サービスレベルアグリメント（SLA：Service Level Agreement）の概念が出現してきた．SLA とは事業者と顧客間で締結する，サービス品質の保証する契約である．例えば，インターネットサービスで，月平均パケットロス率の最大値を契約に盛り込む．もし，月平均パケットロス率が契約値より大きければ，事業者は顧客に違約金として利用料を割り引く．このような場合，事業者側からでなく，顧客からもサービス品質を監視し，SLA 違反が起きていないことを確認する手段が重要になる．このような要求を満たすために，顧客が自網だけではなく，事業者網も監視する CNM が重要視されてきた．

(2) 動 向

ATM フォーラムでは，公衆網管理（Public Network manager）と専用線管理（Private Network Manager）の間に，CNM 用インタフェースとして，SNMP を用いた M 3 インタフェース [8] が定義された．

また，ITU-T では，Telecommunications Management Network（TMN）のフレームワークに従い，X.160 [1] で CNM の標準アーキテクチャを，X.161 [2] では CNM が CNM インタフェースで提供する管理サービスを定義している．**図 4･25** にカスタマネットワーク管理の概要を示す．図の下半分は事業者システムを表し，上半分は顧客システムを現す．顧客側サービス管理システムと CNM システムをつなぐインタフェースが CNM インタフェースである．事業者側と顧客側はそれぞれでサービスの品質などの監視やサービス提供システムの設定などを行っている．CNM Application は，X.161 [2] で定義されている CNM 管理サービスを実現する．CNM Information は CNM 管理情報であり，顧客から見える管理イメージが格納されている．事業者は多数の顧客をかかえている．それぞれの顧客はほかの顧客のデータや関係ないデータにアクセスできないよう，Access Control が設けられている．

X.160 [1] では，CNM インタフェースとしては，CNMC インタフェース [3] もしくは CNME インタフェース [4] のいずれかを使うことを定義している．すなわち，管理プロトコルとしては，CNMC インタフェースでは CMIP [5]，CNME では EDI [6] を使用することが定義されてい

る．前者は OSI 管理プロトコルであり，リアルタイム・インタラクティブに管理情報にアクセスするのに適している．一方，後者はサービス提供者と顧客の契約関係などの情報にアクセスするのに適している．X.161[2] で提供する管理サービスを CNMC 及び CNME でどう実装するかは，それぞれ X.162[3] 及び X.163[4] で定義されている．このような TMN フレームワークをもとに，CMN 管理システムを実装した研究[8),9)] が行われてきた．

近年では，顧客側サービス管理システムとして，Web システムを採用することが多くなってきた[12)]．これにより，特別な管理コンソールを置かなくても，顧客はサービスプロバイダ側情報にアクセスすることができるようになってきた．また，PC や携帯電話によるインターネットアクセスが一般家庭に普及した現在，e ビリングサービスのように一般家庭から随時，キャリア側の課金情報にアクセスできるようになってきた．

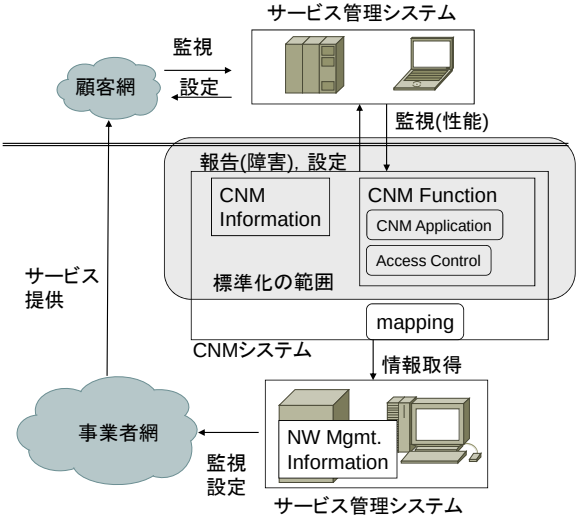


図 4･25　カスタマネットワーク管理 [1)]

4-5-2 ホームネットワーク管理

(1)　背　景

光ファイバや DSL により，ホームとサービスプロバイダを結ぶアクセス網は，高帯域化が進んできた．また，宅内網も無線 LAN の高帯域化が進んできた．そのため，映像配信などホーム向けに多様なサービスが出現してきた．例えば，IP-TV など宅外ネットワークから宅内への映像配信や，DLNA による宅内での映像配信などである．文献 13) によると，以下の 4 領域において，ホームネットワークに関する標準化が活発に行われている．

- **ホームネットワークアーキテクチャ**：Broadband Forum[14)] においてアクセス網の物理レイヤや，IPTV の機能や管理などが検討されている．また，ITU-T の Study Group（SG）では，SG-9（CATV），SG-13（NGN），SG-15（光アクセス網），SG-16（マルチメディアシステム）の観点から検討さている．

- **ホームゲートウェイ**：Home Gateway Initiative[15] がホームゲートウェイの要件を検討，OSGi は，ホームゲートウェイ用 Java 基盤の仕様を標準化．
- **ホーム端末**：UPnP による設定の自働化や，DLNA による宅内コンテンツ流通が一般化してきた．また，Echonet では，家電ネットワークを検討している．
- **宅内伝送網**：Ethernet，Wifi，PLC，Bluetooth，ZigBee など多様化な網が実現されている．

ホームネットワーク管理上の課題として，ホーム内では網管理の専門家が不在のため，システム設定や障害対応が困難な点があげられる．例えば，インターネットサービスプロバイダは，宅内に終端装置（Terminal Adapter）を設置するが，その終端装置のソフトウェアアップデートや障害時対応が必要になる．そこで，ホームネットワーク機器の自動設定や，サービスプロバイダ側からの端末機器のモニタリングや，ソフトウェアアップデートなどの管理機能が必要となる．

そこで，このような課題を解決するためのホームネットワークの管理機能として，機器自動設定として UPnP，機器のソフトウェアアップデート機能として OSGi，そして，サービスプロバイダからの機器管理を可能とするブロードバンドフォーラム TR-069 について説明する．

(2) 技術紹介

(a) Universal Plug & Play (UPnP)

1999 年に Microsoft が提唱．端末が自身の IP ネットワーク設定を行うプロトコル．UPnP フォーラムで標準化提案を行っている．UPnP は HTTP を通信プロトコルとし，伝送構文としては XML を使用している．

UPnP は以下の機能を有する．

1. **IP アドレスの設定**

   IP ネットワークに接続するには情報家電自身に適切な IP アドレスを割り当てる必要がある．通常 DHCP を利用する．UPnP でも DHCP サーバが存在する場合には，DHCP を利用する．存在しない場合には，使用していないプライベートアドレスを調査し，それを利用する．

2. **サービス発見**

   UPnP ではネットワーク機器が機能を提供するデバイスと，それを操作するコントロールポイントの二つに分類される．デバイスがネットワークに接続されると，デバイスが提供するサービスの仕様をネットワークに広告する．コントロールポイントは広告されたデバイスのサービスを発見する．本動作は Simple Service Discovery Protocol（SSDP）で定義されている．また，サービス状況の変更のために，通知プロトコルとして，General Event Notification Architecture（GENA）を採用している．

通常 UPnP とは，UPnP Device Architecture，及び，その上位の UPnP DCP（UPnP Device Control Protocol）が定義されている．その他にメディアサーバと端末とのメディア再生制御を定義した UPnP/AV もある．また，NAT トラバース機能も提供しており，UPnP IGD（Internet Gateway Device）規格に従ったルータでは，UPnP ソフトウェア側からポート制御を行い，NAT トラバースを実現可能である．UPnP 対応のホームルータも多数販売されている．

(b) TR-069 CWMP（CPE WAN Management Protocol）

TR-069 は，ブロードバンドフォーラム（旧 DSL フォーラム）が規定している宅内装置（CPE：Customer Premises Equipment）向け管理プロトコル CWMP（CPE WAN Management Protocol）を定義している．CWPE は，CPE と，自動設定サーバ（ACS：Auto Configuration Server）間の SOAP/HTTP に基づく双方プロトコルであり，CPE の自動設定を行うことを目指している（**図 4･26**）．HTTP を使用しているため，ホームネットワークなどに設けているファイアウォールも一般的な設定であれば，通過可能である．TR-069 は，DSL における端末自動設定における標準となっている．また，ホームゲートウェイイニシアティブ（HGI：Home Gateway Initiative）や DVB（Digital Video Broadcasting Project）などでも採用の動きがある．CPE の自動設定や遠隔設定，ファームウェアのバージョン管理・更新，CPE の状態のモニタリングやサービスの制御が可能である．

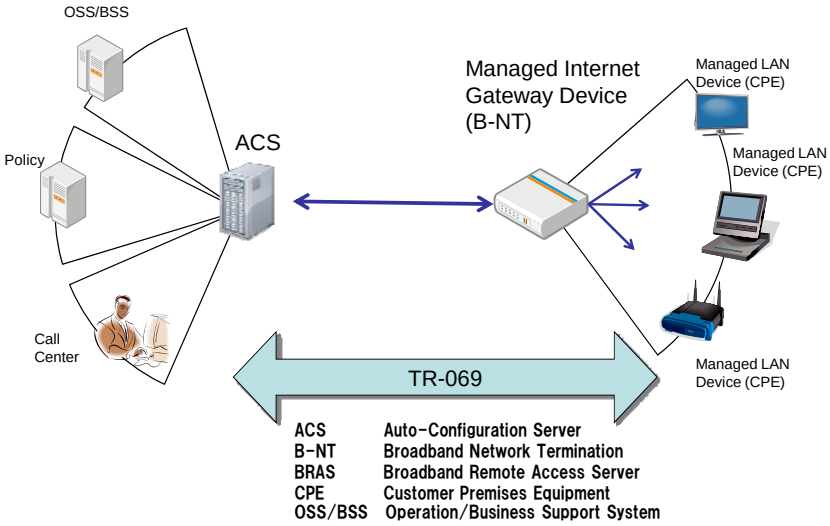


図 4･26　TR-069 想定環境 [16)]

表 4･1 は，CWMP が提供するメソッドの一覧表である．表を見ると分かるとおり CPE や ACS がどのようなメソッドやパラメータを有するかを得る手続き（GetRPCMethod，GetParameterNames），パラメータ値の取得・設定（Set/Get Parameter Value，Set/Get Parameter Attributes），管理対象オブジェクトの追加・削除（Add/Delete Object），ファームウェアなどのダウンロード（Download）がある．Inform は，CPE から ACS にセッションを張る手続きである．Inform の Direction を見れば分かるとおり，CWMP では，CPE 側からコネクションを張るため，管理権限のない ACS から CPE が設定されることを防止する．また，通信は HTTPS を使用することも可能なため，サーバ詐称や盗聴を防止することができる．

CMWP における管理対象として，共通管理モデル [17)]，ホームゲートウェイ（RG：Residential Gateway）[18)]，VoIP 端末 [19)]，セットトップボックス [20)]，NAS [21)] などの管理モデルが標準化されている．

表 4･1 CWMP RPC メソッド [13)]

メソッド	方　向	説　　明
Inform	CPE→ACS	管理セッションを開始する.
GetRPC	CPE→ACS ACS→CPE	遠隔手続き呼び出し（RPC）の一覧を返す．ベンダ特有の RPC が含まれているかもしれない.
GetParameter-Names	ACS→CPE	CPE のパラメータのリストの一覧を返す．ベンダ特有の管理オブジェクトやパラメータが含まれているかもしれない.
Get/Set-Parameter-Values	ACS→CPE	CPE のパラメータの値を得たり，値を設定する．パラメータ名の Prefix を与えると，それを含むパラメータのすべての値を得ることができる.
Get/Set-Parameter-Attributes	ACS→CPE	CPE のパラメータの属性（値変更時の通知の有無など）の読み出しや設定をする.
Add/Delete Object	ACS→CPE	複数のパラメータを包含するオブジェクト型のパラメータを生成・削除する.
Download	ACS→CPE	ファイル（例：ファームウェア）を CPE にダウンロードする.

(c) OSGi

OSGi [22)] は，ホームや小規模オフィス用のゲートウェイに対して，ネットワークを介して必要なサービスを追加・更新・削除可能にするための，Java 上で稼働するソフトウェアプラットフォームである.

ホームに対して多様なサービスが展開される可能性がある．しかし，サービスごとにホームゲートウェイを用意することは現実的ではない. 予め，トリプルプレイ（インターネット，CATV，電話）のように複数のサービスをまとめて提供可能なホームゲートウェイを用意する方法もある．しかし，新たなサービスには，対応が困難である．そこで，動作中のシステムを停止することなく，新たなソフトウェア（バンドルと呼ぶ）を修正・更新・追加する必要ための仕組みとして, OSGi が提案された. OSGi は, OSGi Alliance が標準化を行っている. ホームゲートウェイだけではなく，自動車メーカの車載情報機器や携帯電話に搭載される事例も現れた．更に，Eclipse 3.0 が OSGi を採用，Eclipse のプラグインによる機能拡張を実現した．当初，OSGi は，Open Service Gateway initiative の略称であったが，このようにゲートウェイ以外にも適用範囲が広がっているため，2003 年から OSGi が正式名称である.

OSGi では，Java プログラムのメタ情報を格納したマニフェストファイルに，依存関係情報を記述する．依存関係を管理しているため，あるバンドルを更新するさいに，依存関係のないバンドルを停止させる必要はない．このため，ホームにおけるサービスを停止させることなく，家庭内情報機器のバグ修正，機能追加が可能になる.

■参考文献

1) ITU-T Recommendation X.160, “Architecture for customer network management service for public data networks,” 1994.
2) ITU-T Recommendation X.161, “Definition of customer network management services for public data networks,” 1997
3) ITU-T Recommendation X.162, “Definition of management information for customer network management service for public data networks to be used with the CNMc interface,” 2000
4) ITU-T Recommendation X.163, “Definition of management information for customer network management service for public data networks to be used with the CNMe interface,” 2000

5) CCITT Recommendation X.711, “Common management information protocol specification for CCITT applications,” 1991
6) X.400 (1996), “Message Handling: System and service overview”.
7) ISO/IEC 10021-1, “Information technology − Message Handling Systems (MHS) − Part 1: System and Service Overview,” 1997
8) T. Yamamura, T. Tanahashi, M. Hanaki, N. Fujii, “TMN-based customer network management for ATM networks,” Communications Magazine, IEEE, vol.35, Issue 10, pp.46-52, Oct. 1997.
9) H. Sunaga, Y. Yoshida, K. Murata, T. Nishitani, “Customer network management system for NTT's data communication service,” GLOBECOM’96, vol.1, 18-22, pp.173-178, Nov. 1996.
10) ATM Forum Technical Committee, af-nm-019.000, “Customer Network Management (CNM) for ATM Public Network service (M3 specification),” Oct. 1994.
11) H. Sunaga, Y. Yoshida, K. Murata, and T. Nishitani, “Customer Network Management System For NTT's Communication Service”.
12) Hyun-Chul Kang, Jae-Wook Lee, and Gil-Haeng Lee, “Customer Network Management of VPN Services,” in Proceedings of the 2005 International Conference on Computational Intelligence for Modelling, Control and Automation, and International Conference on Intelligent Agents, Web Technologies and Internet Commerce (CIMCA-IAWTIC’05), 2005.
13) 鹿田　實, “次世代ホームネットワーク管理に向けた技術動向,” TM ワークショップ, Mar. 2008.
14) Broadband Forum, http://www.broadband-forum.org/
15) Home Gateway Initiative, http://www.homegatewayinitiative.org/
16) TR-069 Amendment 2, “CPE WAN Management Protcol,” DSL Forum, Dec. 2007.
17) TR-106 Amendment 1, “Data Model Template for TR-069 Enabled Devices,” DSL Forum, Dec. 2006.
18) TR-098 Amendment 1, “Internet Gateway Device Data Model for TR-069,” DSL Forum, Dec. 2006.
19) TR-104, “DSLHomeTM Provisioning Parameters for VoIP CPE,” DSL Forum, Nov. 2008.
20) TR-135, “Data Model for TR-069 Enabled STB,” DSL Forum, Dec. 2007.
21) TR-140 Issue 1.1 TR-069, “Data Model for Storage Service Enabled Devices,” DSL Forum, Dec. 2007.
22) OSGi Alliance, “OSGi Service Platform Release 4,” Oct. 2005.