■3 群（コンピュータネットワーク）－ 6 編（ネットワークコンピューティング）

1 章 ディレクトリサービス

（執筆者：江崎　浩）［2010 年 4 月 受領］

■概要■

ディレクトリサービスとは，コンピュータネットワーク上にあるコンピュータシステム名やユーザ情報等の資源を記憶し，検索するためのサービスである．例えば，これによって，人間にとってわかりやすい文字列を用いてコンピュータシステムへアクセスすることが可能となる．ディレクトリサービスの具体的な例としては，インターネットで分散的に運用されている DNS（Domain Name System）や次世代ネットワークとされている NGN（Next Generation Network）で導入される SIP（Session Initiation Protocol）システムがある．

ディレクトリサービスを用いたデータ通信回線（チャネル）を確立するために存在する制御手順であるシグナリングの概念を解説する．シグナリングには，アウトバンドシグナリングとインバンドシグナリングとが存在し，それぞれに技術的特徴と運用面での利点と欠点をもつ．

シグナリングには，広域網におけるデータフローの管理･制御を行う機能を実現するもの，広域網上にオーバーレイとして構築される仮想網を含む私設網におけるデータフローの管理制御を行う機能を実現するもの，さらに，広域網および私設網をまたがって機能を実現するものが存在する．

【本章の構成】

本章では，ディレクトリサービスの概要と DNS システムのアーキテクチャ構造（1-1 節），シグナリングの概念と具体例としての電話網シグナリング，MPLS，IMS，モバイルシグナリング，仮想私設網シグナリング（1-2 節）に関して，システムアーキテクチャの整理，各サービスのシステム概要とその技術要素と技術的な特徴を述べる．

■3 群 － 6 編 － 1 章

1-1 ディレクトリサービス

（執筆者：永見健一）［2009 年 3 月 受領］

ディレクトリサービスとは，コンピュータネットワーク上にあるコンピュータシステム名やユーザ情報などの資源を記憶し，検索するためのサービスである．例えば，これによって，人間にとってわかりやすい文字列を用いてコンピュータシステムへアクセスすることが可能となる．ディレクトリサービスの具体的な例としては，インターネットで分散的に運用されている DNS（Domain Name System）や次世代ネットワークとされている NGN（Next Generation Network）で導入される SIP（Session Initiation Protocol）システムがある．

本節では，これらのシステムを解説し，更に，ディレクトリサービスを用いたデータ通信回線（チャネル）を確立するために存在する制御手順であるシグナリングの概念を解説する．

1-1-1 ディレクトリサービスの概念

人間がコンピュータを利用する場合に，IP アドレスのような数字の列を直接用いるのは容易ではない．人間が覚えやすくわかりやすい文字列を用いてコンピュータをアクセスすることができるようにディレクトリサービスが提供されなければ，コンピュータネットワークの利用の利便性を向上することが難しい．

広義のディレクトリサービスは，あるデータやキーワードから，それに関連するデータを検索し，検索結果を提示するシステムのことを意味する．Google.com や Yahoo.com などのような検索エンジンによるキーワード検索システムなどがその典型例である．インターネットシステムでは，IP アドレスとノードの論理名との対応関係を検索・解決するドメインネームシステム（DNS）がグローバル規模で運用されている．また，近年急速に普及してきている IP 電話サービスで導入されている SIP もディレクトリサービスの一つであると解釈される．

インターネットには，主に四つの識別子が存在する．データリンクアドレス（データリンク層），IP アドレス（インターネット層），ポート番号（トランスポート層），そして，FQDN（Fully Qualified Domain Name；絶対ドメイン名 = ドメイン名＋ホスト名）である．ポート番号を除いた三つの識別子は，互いに対応関係をもっており，対応関係を検索・解決するためのプロトコルと機能が提供されている．

IP アドレスは 32 ビット（IPv4）あるいは 128 ビット（IPv6）のビット列であり，普通のユーザは，各宛先コンピュータのインタフェースの IP アドレスを記憶することは困難である．特に，インターネットを用いたアクセスがグローバル化し，動的に変化していくなかで，個別の IP アドレス情報を各コンピュータに保存・記憶させることは事実上不可能となった．ユーザは，ビット列を記憶することは容易ではないが，論理的な名前であれば比較的容易に理解・記憶することが可能である．インターネットにおける論理的な名前である FQDN と IP アドレスとの対応関係を検索し解決するシステムが DNS である．DNS を用いて，FQDN に対応する IP アドレスの解決を行うことを「正引き」，逆に IP アドレスから FQDN を検索することを「逆引き」と呼ぶ．データリンクアドレスと IP アドレスの間の関係を解決するプロトコルとしては，IPv4 の場合には，ARP（Address Resolution Protocol）が用いられ，IPv6 では，近隣探索（Neighbor Discovery）が用いられている．しかし，本機能はグローバル規模での動

作は不要でありローカルセグメント内でのみ動作すればよい．このような観点から考えれば，ARP／近隣探索はディレクトリサービスとはいえない．

FQDN は，階層的に定義されたドメイン名と，ドメイン内の運用者によって自律的に定義可能なホスト名との組合せで表現される．これは，IP アドレスのネットワーク部（= ドメイン名）と，ホスト部（= ホスト名）に対応する．ドメイン名は階層的に定義することが可能で，これは IP アドレスにおけるサブネッティングとほぼ同じ概念である．このような階層構造をもつことによって，名前空間での規模性を実現している．

1-1-2 DNS

IP アドレスと FQDN の変換サービスを提供するために，全世界で分散的にかつ階層的に協調動作する DNS が構築・運用されている．DNS は，13 個のルートサーバ（A～M）をもつ分散階層化ディレクトリシステムである．欧州に 2 個（K と I），北米に 11 個，アジア地区には，WIDE プロジェクトが管理する M ルートサーバが 1 個存在している．ルート DNS サーバは，初期は物理的な 13 台のサーバ計算機であったが，近年ではその処理負荷の分散と信頼性向上を実現するために，エニキャスト（Anycast）技術を利用して，複数のサーバを物理的に分散させ同一のサーバとしてサービス提供を行っている．

図 1･1 に FQDN のグローバルな名前空間，**図 1･2** に DNS システムの動作例を示した．FQDN は“.”（dot）をルートとし，“jp”や“com”などの TLD（Top Level Domain）を辿り，目的の FQDN の情報を格納している DNS サーバに辿り着く．

DNS の仕様は，RFC 1034 及び RFC 1035 に記述されている．DNS サーバの UNIX 用のプログラムは“named”と呼ばれ，BIND（Berkeley Internet Name Domain）としてソースコードが公開されている．DNS のクライアントソフトウェアは“resolver”と呼ばれている．

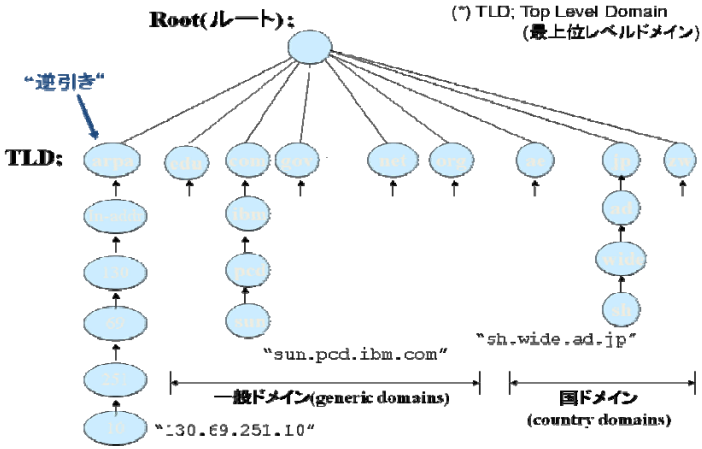

図 1・1　FQDN のグローバルな名前空間

FQDN は階層的にその名前空間が定義されており，ルート“.”のすぐ下の名前空間を TLD（Top Level Domain）と呼んでいる．主な TLD として，“arpa”（逆引き用ドメイン），“gTLD”

（Generic TLD），“ccTLD”（Country Code TLD）が定義されている．gTLD は長い間 3 文字であったが，ICANN により 3 文字の制限が外され，現在では，“.name”や“.info”などの 4 文字以上の gTLD が定義可能となっている．

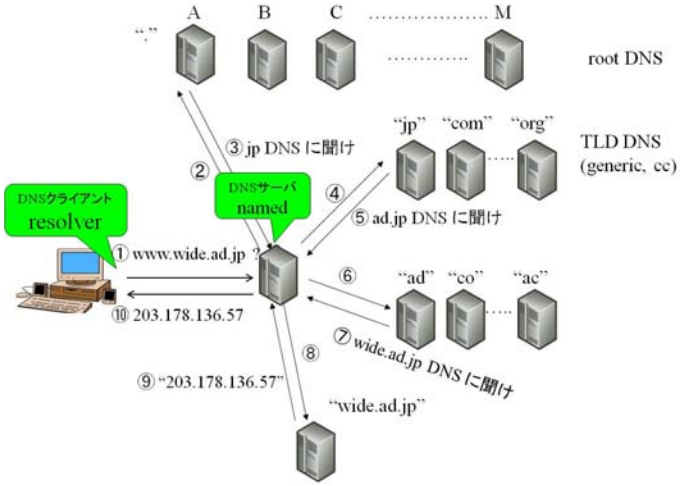

図 1・2　DNS の動作例

また，gTLD よりも下位の階層のサブドメイン名として，従来は，ASCII 文字のみが使われていたが，ACSII コード以外の文字，すなわち，多言語ドメイン名の定義を行うことも可能となった．これを iDN（internationalized Domain Name）と呼んでいる．

FQDN の管理を行っているネットワークの単位（DNS ドメイン）を，“ゾーン”と呼ぶ．“ゾーン”には，一般的に，プライマリサーバとセカンダリサーバが存在し，DNS サービスの信頼性の向上を図っている．プライマリサーバからセカンダリサーバへのディレクトリ情報の更新を，“ゾーン転送”と呼ぶ．FQDN は階層的に定義することが可能である．すなわち，経路制御の構造と同じく，DNS サーバシステムも階層的にかつ回帰的に配置運用することで，大規模化への対応を可能としている．実際に，DNS システムは分散ディレクトリシステムとして，グローバルスケールで定常的に運用されているシステムととらえることができる．

FQDN の種類, すなわち DNS サーバに格納される各ノードの論理的な名前の定義としては，以下のようなものが存在する．

タイプ 1：　A レコード（IPv4 アドレス）
タイプ 2：　NS レコード（DNS サーバ）
タイプ 5：　CNAME（エイリアス，ローカルな名前）
タイプ 6：　SOI（Start of Authority）
タイプ 11：　WKS（Well-Known Service）
タイプ 12：　PTR（arpa，逆引き用アドレス）
タイプ 15：　MX（メールサーバ）
タイプ 28：　AAAA レコード（IPv6 アドレス）

タイプ 35： NAPTR レコード

なお，インターネット上に存在するコンピュータの数が少なかった頃は，DNS の必要性はなく，UNIX システムでは /etc/hosts にノードの論理名と IP アドレスの対応関係を記述していた．その後，SUN OS では LAN エリアでのディレクトリサービスとして yp（Yellow Page）や NIS（Network Information System）が実装運用された．その後，DNS システムが実装運用されるに至った．

DNS が早急に解決しなければならない課題は，以下の二つである．

(1) DNS セキュリティ

DNS に関するセキュリティ機能（DNS-Sec）の実装は重要な課題である．DNS のなりすましにより，容易にインターネットシステム全体あるいは大部分を機能不全に陥れることが可能である．特に，ルート DNS サーバのなりすましが行われた場合を考えると，その影響の大きさは容易に想像できる．

DNS 同士の信頼関係を確実なものにするためのセキュリティ機能（IPSec でも規定されている公開鍵暗号方式を用いた認証機能）の研究開発と展開が推進されている．基本的には，IKE（Internet Key Exchange）と呼ばれるインターネットを用いた鍵配布を実現するためのプロトコルを用いて，DNS サーバに相互認証のために必要な鍵を配布し，IPSec で規定されている AH（Authentication Header，認証ヘッダ）を用いて DNS サーバ同士での相互認証を行うというものである．

(2) IP バージョン 6 への対応

DNS システムが IP バージョン 6 に対応しないと，IPv4 から IPv6 への移行は現実には実現することが不可能である．したがって，各 DNS サーバの IPv6 への対応を推進しなければならない. DNS サーバの参照ソフトウェアとして広く流通し利用されている “bind” は，バージョン 9（bind 9）より，既に IPv6 への対応を行っている．

1-1-3 SIP システムと IP 電話サービス

SIP（Session Initiation Protocol）は，IP 電話サービスを提供するための通信プロトコルとして広く利用されているが，もともとは IP 電話以外の様々な通信サービス（例えば，映像やプレゼンス（Presence）情報などのコミュニケーションをエンド・エンドに提供するための，(i)ディレクトリサービスと，(ii)エンド・エンドで動作するセッション管理プロトコルとして設計された．前者(i)は，電子メールアドレスの形式で表現される SIP のサービスアクセスポイント（SAP：Service Access Point）を解決する機能である．SIP サーバに対して，SIP クライアントは，ネットワークに接続した際に，自ノードの IP アドレス情報を登録する．SIP クライアントは，目的のノードへ（マルチメディア）セッションの設定を行う際には，SIP サーバへのアクセスを行い（= シグナリング手順），通信相手の IP アドレスなどのセッションの確立に必要な情報（例えば，相手先ノードの IP アドレスとポート番号など）を獲得する．獲得した情報をもとに宛先ノードへのアクセスを行い，セッションパラメータのネゴシエーションがエンド・ノード間で行われ，実際のデータ交換が実行される. IP 電話サービスでは，伝送・交換されるユーザ情報が音声であり，SIP サーバにより宛先ノードの IP アドレス情報が解決される．

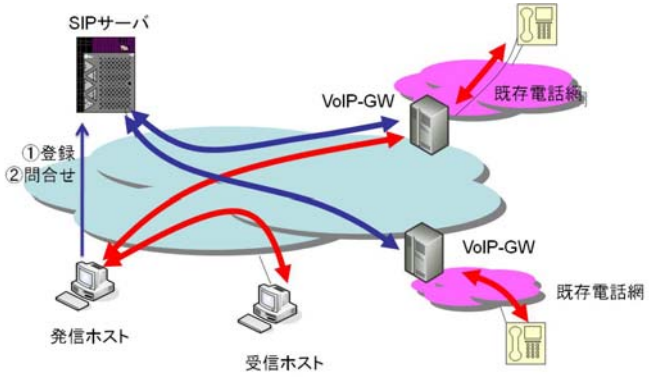

図 1・3　IP 電話システムの動作概念

すなわち SIP ネットワークは, ほぼ DNS と同等のディレクトリサービスを提供していることがわかる. すなわち, 宛先ノードを電子メールの形式で表現し（DNS では FQDN で表現）, これに対応する IP アドレスの情報を提供（= 解決）するサービスを提供している．なお, SIP に類似したアーキテクチャとして ENUM が存在する．ENUM は，電話番号からサービスの URI を検索するディレクトリサービスである. ENUM は, DNS の NAPTR（Naming Authority Pointer）エントリーを利用して，サービスを構築している．NAPTR リソースレコードは, DDDS（Dynamic Delegation Discovery System）という体系のなかで定義された DNS のリソースレコードで，以下の二つの機能をもつ．(1)ドメイン名に URI を登録する機能，(2) SRV（Server）リソースレコードと組み合わせて電子メールの配送に用いる MX リソースレコードの考え方を一般化し多くのアプリケーションを提供するサーバをその URI 用いて指定する機能である．

SIP サーバも ENUM サーバも，通常の DNS サーバと同様にディレクトリサービスを提供している．すなわち，SIP クライアント（ENUM クライアント）は，SIP サーバ（ENUM サーバ）に接続し，通信相手へのアクセスに必要な情報を獲得する．

■3 群 － 6 編 － 1 章

1-2 シグナリング

（執筆者：永見健一）［2009 年 3 月 受領］

1-2-1 シグナリングの概念

電話回線や TCP コネクションは，複数の交換機／ルータと，交換機／ルータを結ぶケーブルを用いて提供される仮想的な回線の代表例である．電話線に接続された情報通信機器（電話機やコンピュータ）は，電話番号を入力し，宛先の情報通信機器への透過的な（= データ加工が行われない）仮想回線の確立を要求する．この仮想回線は，複数の電話交換機と通信回線を介して確立される．一方，TCP コネクションにおいては，エンド・ノードは，DNS を用いて宛先ノードへ IP パケットを転送するために必要な宛先 IP アドレスの情報を解決し，TCP で規定されているコネクション確立手順を実行し，仮想的なコネクションをエンド・ノード間に確立する．このような，仮想回線を確立するための手続きがシグナリング手順（Signaling Procedure）である．

シグナリングには，アウトバンドシグナリングとインバンドシグナリングとが存在する．電話回線の確立はアウトバンドシグナリングの典型例であり，TCP コネクションの確立はインバンドシグナリングの典型例である．一般的に，インターネットにおいてはインバンドシグナリングが用いられ，一方，電話系のシステムにおいてはアウトバンドシグナリングが用いられることが多い．後述する，SIP（インバンドシグナリング）と IMS（アウトバンドシグナリング，及び MPLS（インバンドシグナリング）と GMPLS（アウトバンドシグナリング）が，その具体例としてあげられる．

1-2-2 電話システムにおけるシグナリング

電話網におけるシグナリング手順は，旧来のディジタル交換網においては SS No.7 が存在し，BISDN（Broadband ISDN）網においては B-ISUP が標準化されている．B-ISUP は，ISDN の広帯域版でありマルチメディア統合サービス網として設計された ATM システムにおけるシグナリングとしてその仕様が ITU-T によって標準化された．

SS No.7 手順及び B-ISUP 手順を実行するための専用のネットワーク（これをコントロールプレーンとも呼ぶ）が構築・運用されている．B-ISUP は，技術の標準化と実装は行われたが，広域広帯域有線網での展開は行われず，第 3 世代携帯電話網の有線ネットワークにおいて展開されている．SS No.7 及び B-ISUP は，実際のユーザのデータパケットの転送を行うネットワーク（これをデータプレーンと呼ぶ）とは独立したネットワーク（= シグナリングネットワーク）を形成しており，データプレーンに存在する交換機の制御を，コントロールプレーンに存在する装置が行う構成となっている．

このように，コントロールプレーンからの指示によって，その構成・運用に必要な設定を変更する交換装置をソフトスイッチと呼んでいる．後述する GMPLS システムは，SS No.7 や B-ISUP 網と同じく，コントロールプレーン網とデータプレーン網が独立に定義され，コントロールプレーンのノードがデータプレーンのノードの制御を行うアーキテクチャとなっている．

ここで，インターネット基盤の上での電話サービスの提供と，IP 技術を用いた電話サービ

スの実現を目的とした，SIP と IMS（IP Multimedia Subsystem）の比較を行う．SIP は，インターネット上での，ピア・ツー・ピアでのセッション確立に必要な情報の提供を行うプロトコルとして，IETF において技術標準化が推進された．電子メールアドレスと同等の表記で表現される SIP クライアントノードの情報から，その SIP クライアントにアクセスを行うための必要な情報を提供するのが SIP の基本機能である．このような観点で考えれば，SIP は DNS とほぼ同等の機能（= ディレクトリサービス）を提供しているととらえることができる．実際，SIP は DNS システムを利用しており，具体的には NAPTAR レコードを用いて，通信相手のノードへの（仮想）コネクションの設立に必要な情報（プロトコル，IP アドレスなど）を提供する．すなわち，SIP は，インバンドシグナリング型のシステムアーキテクチャで，中継ノードへの制御は特には行わない．

一方，SIP の発展型と位置づけられている IMS は，SIP パケットは独立に運用される（アウトバンド）シグナリング網で転送される．IMS の技術仕様は SIP を基盤としているが，アーキテクチャとしては，全く異なるシステムアーキテクチャを用いて実現されることになる．すなわち，IMS では，SIP 網とは異なり，SS No.7 や B-ISUP と同様に独立なシグナリング網の存在が前提となっている．IMS を適用したシグナリング網は，Data-Plane 網内の IP パケット交換機（機能的には IP ルータに酷似）の管理・制御を司るシステム構成となっている．

シグナリングに関するネットワークアーキテクチャという観点で比較すると，SIP 網と IMS 網は，エンド・ノードが実装すべきプロトコルは類似したもの（ほぼ，IMS は SIP を包含したスーパーセットのプロトコルとなっている）となるが，全く異なるネットワークアーキテクチャとなる．

1-2-3 MPLS/GMPLS

MPLS 技術は，当初，ATM スイッチを高速大容量のスイッチエンジンとして用いるアーキテクチャとして提案されたが，IETF においてデータリンクに依存しない形に拡張された．任意の粒度のパケット流に対して固定長のラベルを割り当て，このラベル情報を用いて IP パケットの転送を行う．MPLS システムを構成するルータを LSR（Label Switching Router），LSR によって形成される経路を LSP（Label Switched Path）と呼ぶ．LSR は，IP アドレスを用いて転送するインターネット層の転送機能と，ラベルを用いて転送するレイヤ 2.5 スイッチング機能とを併せもっている．

LSP の設定は LDP（Label Distribution Protocol）や MPLS 拡張を施した RSVP などを用いて行われる．LDP 及び拡張された RSVP がシグナリング手順に対応する．

図 1･4 に示す例では，上流側エッジ LSR から LSP の設定を要求するメッセージを送信すると，これを受信した最下流のエッジ LSR から順に隣接 LSR 間で LSP を設定し，これを識別するためのラベル情報が上流に向けて送られる．エッジ LSR 間に LSP が設定されると，その上をパケット流が転送される．

MPLS 技術は一種のトンネリング技術ととらえることも可能であり，インターネット層の経路制御によって形成される経路とは独立に，任意の LSR 間で自由に LSP を設定できるとみることもできる．すなわち，ネットワーク運用者のポリシーによって自由に経路を設定することが可能になる．これをトラヒックエンジニアリング技術と呼ぶ．

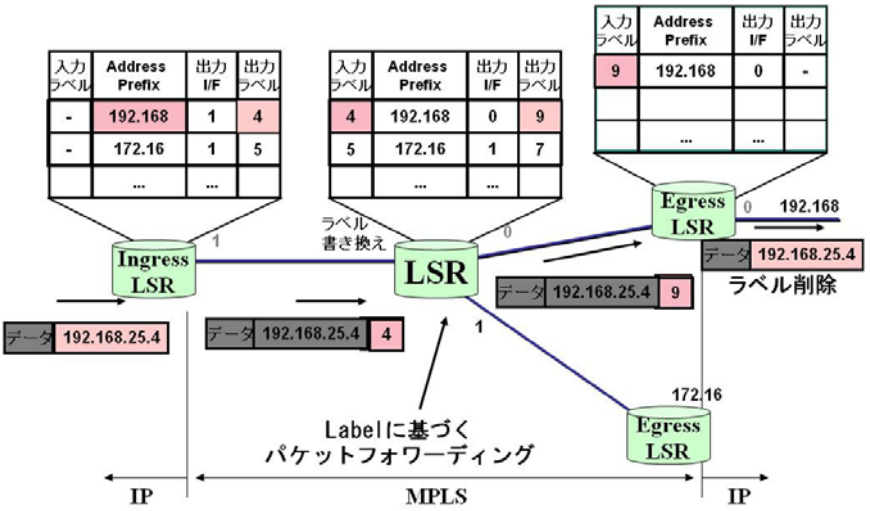

図 1・4　MPLS の動作概念

また，WDM 技術と MPLS 技術及びトラヒックエンジニアリング技術を組み合わせることによって，MPλS 技術（Multi-Protocol Lambda Switch）が実現される．MPλS 技術は，QoS/CoS サービスへの適用，ポリシー制御，トラヒック分散を実現させつつ，高速広帯域な IP パケット交換サービスを提供する技術として，今後の導入と普及が期待されている．MPλS サービスを実現するために定義されたシグナリングプロトコルを GMPLS（Generalized MPLS）と呼び，MPLS におけるラベルの概念を拡張し光多重伝送において利用される波長（λ）情報もラベルとして定義することが可能となっている．なお，GMPLS のシグナリングプロトコルは，MPLS とは LSP の設定・管理手順が同一ではなく，むしろ大きく異なる設計思想で設計されている．

MPLS と GMPLS とをシグナリングのアーキテクチャという観点で整理すると，全く異なるシステムアーキテクチャであることが明らかとなる．MPLS は，MPLS の運用に必要な LDP（あるいは拡張版 RSVP）を，インバンドシグナリングで実現している．一方，GMPLS は，光スイッチ網の技術的な制限もあって，アウトバンド型のシグナリングアーキテクチャとなっている．すなわち，GMPLS 網の運用と管理のために専用のネットワークを構築し，この GMPLS シグナリングネットワークが，データプレーン網のノードの管理・制御を行うという構成になっている．

1-2-4 IMS

固定電話網と移動体通信網とを統合し，これまで電話ディジタル交換機とも，IP ルータを基盤としたインターネットとも異なったアーキテクチャを用いて構築される IP 技術を用いた携帯電話系ネットワークのアーキテクチャである．公衆通信サービス網（無線と有線）を IP 技術と SIP（Session Initiation Protocol）技術で統合し，マルチメディアサービスを実現させ

る．FMC（Fixed and Mobile Convergence）という無線と有線の統合サービスがゴールとされており，各国の大手通信事業者が次世代の公衆通信網として導入を計画している．

IMS を用いた通信サービスは，IP 技術を用いた電話サービスの基盤プロトコルである SIP（Session Initiation Protocol）をもとにしたものとなっており，また，その他の IP ベースのマルチメディアサービスについても，運用／課金などのデータベース機能，セキュリティゲートウェイなどを搭載するとされている．Push-to-Talk やテレビ電話などのほか，スケジューラやクレジットカード決済などの個人データ管理やセキュリティ機能の統合も，サービスプロバイダのサービス機能として提供されることが計画されている．

IMS のコア技術仕様は，第 3 世代携帯電話の規格標準化を行っている団体である「3GPP」と「3GPP 2」によって，それぞれ「3GPP TS 23.228」「3GPP 2 XP 0013.2」として標準化されている．

IMS をもとにしたシステムアーキテクチャは，IP 技術をデータプレーンにおけるデータ伝送・交換フォーマットとしているが，そのアーキテクチャは TCP/IP 網すなわちインターネットとは，異なっていることに注意が必要である．IMS はセッションベースで通信が行われ，エッジノードにおける Admission Control や Shaping/Policing Control の適用が規定されている．

1-2-5 モバイルシグナリング（RADIUS）

RADIUS（Remote Authentication Dial In User Service）は，多数の分散した情報通信サービスプロバイダのアクセスポイント（これを POP：Point of Presence と呼ぶ）にアクセスするユーザに対して，ネットワーク資源の利用可否の判断（認証）と利用事実の記録（アカウンティング）を，自ネットワーク上の特定のサーバコンピュータに一元化管理させることを目的とした，IP 上のプロトコルである．名称に「ダイヤルイン」という言葉があるように，元来はダイヤルアップインターネット接続サービスを実現することを目的として開発された．すなわち，ダイヤルアップ PPP（Point-to-Point Protocol）接続ユーザに対する認証やアカウンティング記録を維持する仕組みである．

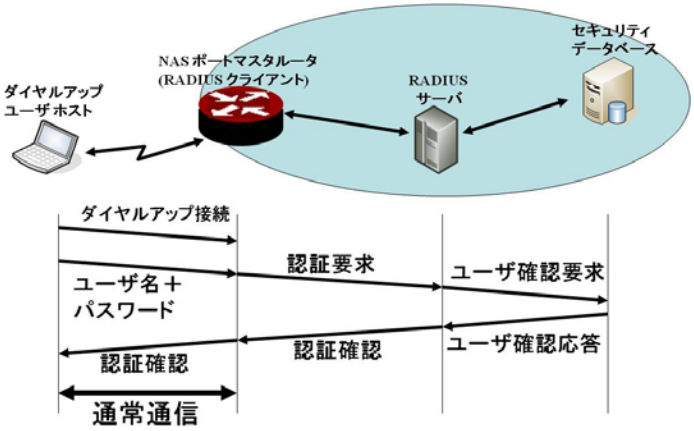

図 1・5　RADIUS システムの構成と動作概要

RADIUS を適用してシステムにおいて，ユーザは，データネットワークエッジにあるいずれかの NAS（Network Access Server）のポートに対応付けられた電話番号をダイヤルする．ユーザ ID とパスワードが設定されている場合は，サーバは NAS データベースをローカルに検索するか，あるいは設定済みの RADIUS サーバに問合せを送り，ネットワークへのアクセスを許可するか拒否するかを判断する．許可されたユーザであれば，通常，RADIUS サーバは設定値を NAS に送信する．これにより，このユーザに許可されているサービスタイプが確認され，それに応じた NAS での設定が行われる（**図 1･5**）．

Point-to-Point Protocol（PPP）は，2 点間を（レイヤ 2 で直接）接続してデータ通信を行うための通信プロトコルである．PPP は，SLIP（Serial Line Internet Protocol）の後継として，1992 年にその技術仕様が標準化された．PPP は SLIP と異なり，TCP/IP 以外のプロトコル（例えば NetBEUI，AppleTalk など）とも接続可能に設計されているのが特長である．ダイヤルアップ PPP は，PPP にダイヤル発信や着信の機能を追加したもので，電話回線を通じて遠隔地にあるネットワークにコンピュータを接続するためのプロトコルとして一般に広く利用されている．

PPP の通信は LCP（Link Control Protocol）と NCP（Network Control Protocol）という二つのプロトコルを使用している．LCP で PAP（Password Authentication Protocol）や CHAP（Challenge Handshake Authentication Protocol）を使ってユーザ認証を行い，リンク確立後，NCP がそれぞれのプロトコルに必要な設定を行い，接続を確立する．また，複数の PPP 回線を束ねることによりスループットの向上を図ることが可能であり，マルチリンク PPP と呼ばれ，ISDN や PHS などで利用されている．また，イーサネットを通じて PPP と同等の機能を提供するプロトコルとして PPPoE 及び，PPPoA（PPP over ATM）があり，ADSL サービスや広域イーサーネットサービスにおいて広く利用されている．

更に，PP Extensible Authentication Protocol（PPP 拡張認証プロトコル：EAP）は，PPP 用の認証プロトコルの一つであり，各種の拡張認証方式を利用するための手続き統合化したものである．実際に利用する認証方式については極めて多岐にわたり，各ベンダによる独自拡張も許されている．

1-2-6 VPN (Virtual Private Network)

企業網のような私的と閉域ネットワークは，公衆ネットワークインフラを利用して構築・運用する形態は，常に，公衆プロバイダによるサービスとある意味競合しながら，サービスの創造と展開を行ってきた．公衆ネットワークインフラの整備と拡充は，私的閉域ネットワークのユーザ，特に企業や組織のキャンパスに存在しないとき（自宅や出張先，あるいは移動中）に，必要なアクセスポイントまでの接続性を，ユーザが存在する場所に依存せずに，かつリーズナブルなコストで提供することを可能とした．

このように，電話回線やインターネットアクセスなどの公衆ネットワークサービスを用いて，ユーザのコンピュータを私的閉域ネットワークに接続する（狭義のリモートアクセス）ことで，所属する組織のキャンパスネットワーク内に存在するコンピュータに，ユーザのコンピュータがキャンパスネットワーク内に存在するときと同じように直接アクセスすることが可能となる．このように，公衆ネットワークサービスを用いて私的閉域ネットワークにリモートアクセスし，仮想的に遠隔地から私的閉域ネットワークに参加して構成されるネット

ワークをリモートアクセス VPN（Virtual Private Network）と呼ぶ．また，特に，電話回線ではなく,公衆インターネットサービスを用いて利用者が暗号化装置を用いて VPN 接続を構築するものをインターネット VPN と呼ぶ．

インターネット VPN のほかには，プロバイダが MPLS を用いて提供する IP-VPN や，透過的なレイヤ 2 サービスを提供する広域イーサーネットサービスなども存在する．プロバイダが提供する VPN を利用する場合には,すべてのキャンパスネットワークと遠隔で接続するユーザ端末／ユーザサイトが，同一のプロバイダに接続されていなければならないという制約が発生する．一方，前者（ユーザ端末・ユーザサイトが自立的に VPN 機能を実現する）の場合には，このような制限はなくなり，ユーザ端末及びユーザサイトは任意のプロバイダに接続されていてもインターネット VPN に接続可能となる．

以下では，典型的な（私的）閉域ネットワークの構成法の例を解説する．

電話網が提供するダイヤルアップ接続機能を用いて，レイヤ 2 でのポイント・ツー・ポイント通信チャネルを，ユーザ端末／ユーザサイトとキャンパスのアクセスルータの間に確立して，ユーザ端末／ユーザサイトを VPN に参加させる方式である．PPP や PPPoE など，レイヤ 2 回線上での接続ノードの認証を行い，適切な通信プロトコルを用いて，データ通信を行う．アナログの音声チャネル上でモデム技術を用いてディジタル通信を行う．

今日の多くの電話網はディジタル交換を行っているが，ダイヤルアップ方式では，ディジタル技術で伝送されるアナログ（音声）伝送信号にモデム技術を適用し，ディジタル信号を伝送するという非効率なデータ伝送となっている．ISDN における D チャネルを用いたディジタル情報の伝送は，この非効率性を改善することを可能とするものであったが，DSL（Digital Subscriber Line）技術の登場により，本格的な普及にはいたらなかった．

インターネット VPN には，アプリケーションレベルでの VPN と，IP レベルでの VPN の二つが存在する．

(1) アプリケーションレベル VPN（例；SSL-VPN）

SSL（Secure Sockets Layer）とは，Netscape Communications 社によって開発されたトランスポート層に位置する通信プロトコルで，暗号化と認証によりセキュリティを要求される通信を提供することができる．一般的に，クレジットカード情報や個人情報を伝送する際に，インターネット上に存在する第 3 者による盗聴を防止するために開発された．暗号化には共通鍵暗号が使われ，認証局（CA：Certification Authority）を用いたサーバ認証を行うのが一般的な運用方法である．

ユーザ端末・サイトとキャンパスネットワークのサーバとの間でのすべてのデータ通信に SSL を適用すれば，安全なデータ通信を行うことが可能となる．このように，SSL 技術のような，TCP/IP レイヤ以上のレイヤ，すなわちアプリケーションレイヤでの暗号化と認証機能を用いて，VPN を構成する手法をアプリケーションレベル VPN と呼ぶ．

(2) レイヤ 3 VPN

レイヤ 3 VPN の構築に利用されるプロトコルとしては，IPSec，MPLS 及び MIP（Mobile IP）の三つがその代表例としてあげられる．

IPsec は，IP パケット自体を保護（暗号化と改竄チェック）するので，暗号化機能をもた

ないアプリケーションでもセキュリティの確保が可能になる．一方で，ユーザがどのような上位アプリケーションプロトコルで通信を行っているかを知ることができない．そのため，トンネルモードと呼ばれるキャンパスネットワークのアクセスポイントで，暗号化を解く運用形態が適用されている場合が多い．

MPLS（MultiProtocol Label Switching）技術は，キャンパス間を結ぶ仮想的通信回線（これを LSP；Label Switching Path と呼ぶ）をレイヤ 3 のネットワーク上に提供する技術である．IP 通信のための LSP だけではなく，任意のプロトコル通信（イーサーネットや SNA など）のための LSP を提供することが可能である．複数のプロバイダにまたがって LSP を提供することは，プロバイダの運用ポリシー上容易ではなく，LSP で相互接続されるキャンパスが同一のプロバイダに接続されていなければならない．また，高機能ルータにのみ具備されている機能であるため，ユーザ端末やユーザサイトのような SOHO（Small Office Home Office）環境において利用することは事実上不可能である．

(3) レイヤ 2 VPN

L2TP（Layer 2 Tunneling Protocol）が，レイヤ 2 VPN の構築で利用される代表的プロトコルである．L2TP は，レイヤ 3 のネットワーク上に，レイヤ 2 のトンネリングパスを提供するプロトコルの一つである．すなわち，公衆インターネット上に仮想的にトンネルを生成し，ユーザ端末／サイトとキャンパスネットワークのアクセスポイントとの間に PPP 接続を確立することにより VPN を構築する．なお，L2TP 自体にはセキュリティ保護機能が具備されていないため，IPsec などと組み合わせることによってセキュリティを確保する必要がある．

L2TP は複数のトンネルを同時に作成することが可能であり，NTT 東西の「フレッツ・サービス」が代表的な例としてあげられる．