

シリーズ

シリーズ「電子政府を支える情報通信基盤技術」第5回

電子政府を支えるミドルウェア

日本電気株式会社 インターネットシステム研究所 所長 阪田 史郎

はじめに

インターネットを利用した電子政府システムの構築においては、電子政府の各種サービス（電子申請・帳票発行、電子入札、電子調達、電子決済、各種行政サービス等）を提供するアプリケーションプログラム群を支えるミドルウェア、あるいはネットワークミドルウェアが重要な役割を果たす。

ミドルウェアは、コンピュータにおいて、基本ソフトのOSとアプリケーションプログラム群の間に位置し、インターネットのネットワーク層（第3層）からアプリケーション層（第7層）までのプロトコル処理を実行するソフトウェア群である。これらのソフトウェア群が、電子政府システムのあらゆるサービスの実行・制御を司ることになり、これらのソフトウェア群の構造、機能、動向を理解することは、電子政府の今後を展望する上で重要となる。

電子政府において特に重要となるプロトコルは、プライバシー保護や不正侵入防止、サイバーテロ対策、DDoS（Distributed Denial of Service Attack）対応を含むセキュリティと、将来のブロードバンド&モバイルインターネット環境における情報通信の品質（QoS：Quality of Service。動画や音声による通信を含む）制御に関するものである。さらに、このセキュリティとQoS制御を主対象とする情報通信のためのポリシー管理も今後重

要となる。

本稿では、インターネットにおけるセキュリティプロトコル、QoS制御プロトコル、ポリシー管理プロトコルを中心に、電子政府システム実現において重要となるネットワークミドルウェアの発展経緯、技術動向、標準化動向を解説し、その分析に基づきこれらの技術の電子政府への適用可能性、有効性を展望し、実現に向けての課題等について述べる。

ミドルウェアは一般に、図1のように基本ソフト（OS）とアプリケーションプログラムの間において、基本ソフトのもつ、各種リソースの管理機能やタイミング制御機能を使って、アプリケーションプログラムに対して、要求されるサービスを効率的に提供するソフトと定義される。ネットワーク化の進展やアプリケーションの多様化、特にインターネットが世界の情報インフラとして定着したことに伴い、世界中の多様なコンテンツを安全に効率的に流通させ、アプリケーションの付加価値を生出すミドルウェアは、益々重要な位置を占めるようになってきている。一般には、通信プロトコル処理を司るネットワークソフト、データベースやファイルとのデータの読み書きを制御するデータベースソフト、各種のアプリケーションを支援するソフトなどが該当する。

図1 ミドルウェアの位置付けとプロトコル階層

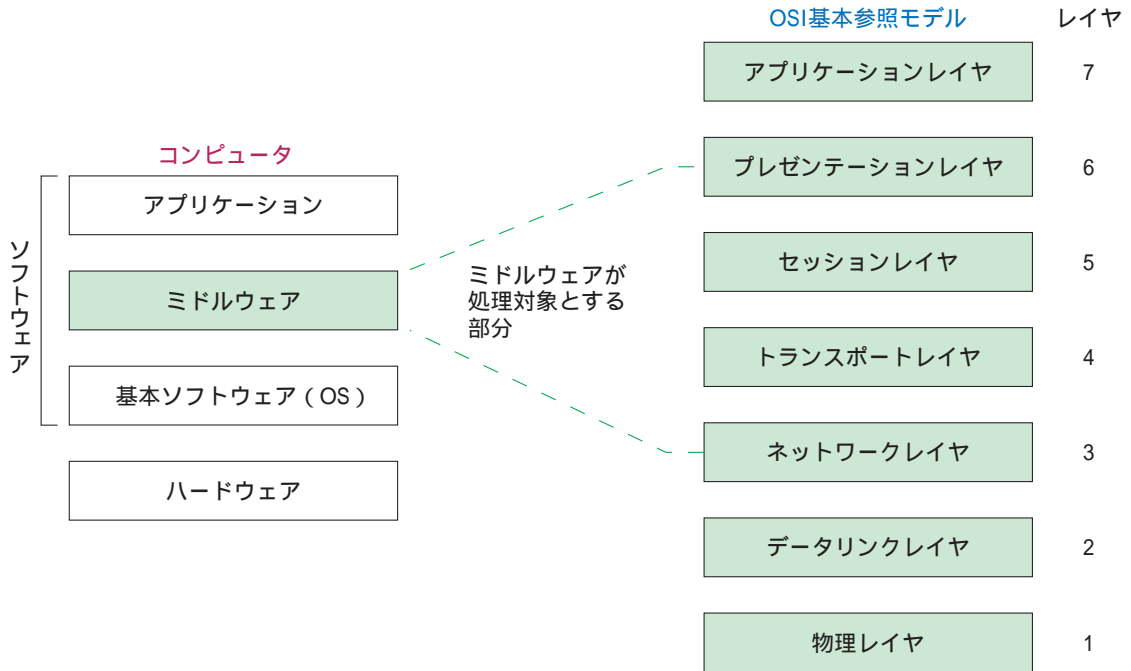
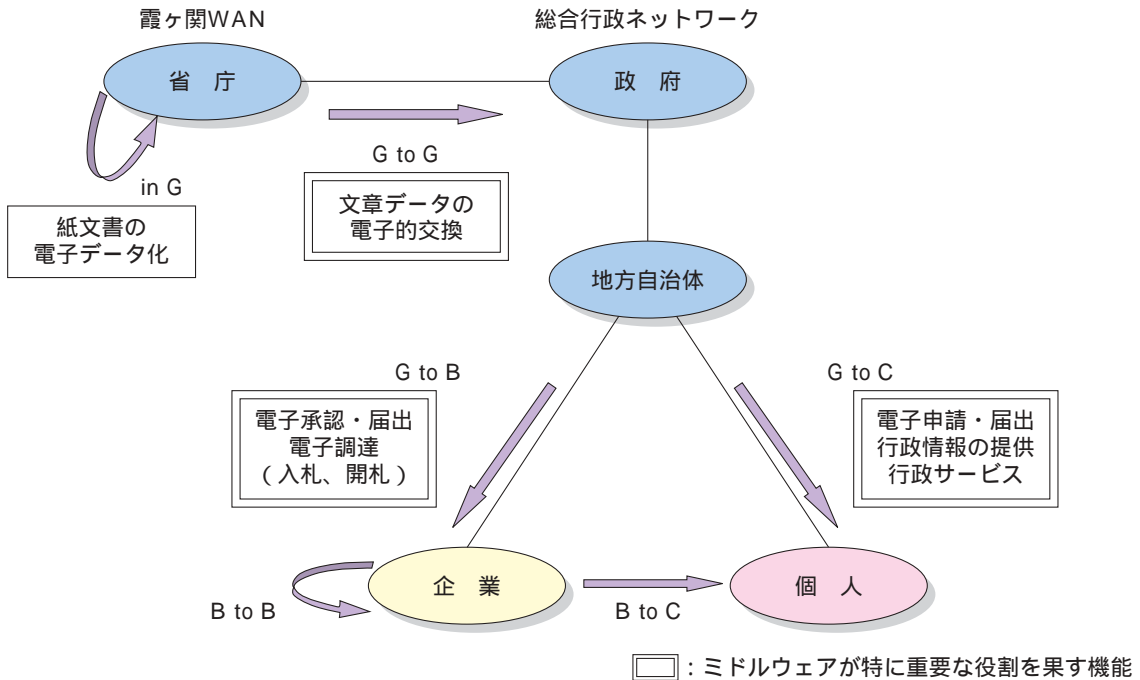


図2 電子政府のイメージ図とミドルウェア



電子政府・電子行政に関連する、

- ・省庁間の文書データの電子的交換
- ・電子申請・届出
- ・行政情報の提供
- ・電子調達（入札・開札）
- ・電子投票
- ・政府認証基盤（GPKI）・電子署名

等のサービス実現においても、ミドルウェアは、これらを直接サポートする基盤として重要な役割を果たす。図2に、電子政府・電子行政サービスのためのシステムの概要とミドルウェアの関係を示す。

ネットワークとの関連に限れば、ISO（International Standardization Organization、国際標準化機構）で標準化された開放型システム相互接続OSI（Open Systems Interconnection）の7層モデルにおける、第3層（ネットワークレイヤ）からその上位、第7層（アプリケーションレイヤ）の一部まで、個別のアプリケーションを支える部分までのプロトコルを処理する部分に相当する。第1層（フィジカルレイヤ）と第2層（データリンク制御レイヤ）については、ミドルウェアというよりも、通信インフラおよびデバイスの組み込みソフトで実行・処理されると考えてよい。

インターネットプロトコルの標準化機関であるIETF（Internet Engineering Task Force）のほぼ全体と、WWW（World Wide Web）に関連する標準化機関であるW3C（WWW Consortium）の大部分の検討対象が、ミドルウェアに相当すると考えてよい。特にIETFではInternet Area、Routing Area、Transport Area、Security Area、Network Management Areaの5つのエリア、W3CではArchitecture DomainとUser Interface Domainの2つのドメインにおける検討が、技術的にミドルウェアとの関係が強い。

1 ミドルウェアの構造

ミドルウェアは、大きく2つの階層に分けられる。下位はアプリケーションを直接意識せずネットワークインフラの機能に直接関係する部分であり、上位はネットワークインフラの機能とは独立してアプリケーションに共通の支援機能を提供する部分である。上位には、各種リソース管理、分散オブジェクト管理、ディレクトリ管理、ネットワーク運用管理、各種ポリシー管理、認証・決済・課金管理、情報や文書の構造・表現、エージェント機能などが含まれ、下位には、QoS（Quality of Service）制御、マルチキャスト通信、セキュリティ基本制御（暗号化、メッセージ認証、鍵管理、アクセス制御など）、データベース管理、エンドトゥエンド転送制御、経路制御などの各機能が該当する。

下位と上位の機能の区別は必ずしも明確には規定できないが、下位の代表的な機能は、経路制御、マルチメディア通信を実現するためのQoS制御、セキュリティ基本制御、データベース管理などであり、上位の代表的な機能がエージェント、課金管理、文書記述・交換などである。

ミドルウェアの中の下位についてはIETF、上位についてはW3Cにおいてそれぞれ検討されている。下位の最も重要な機能は、QoS制御とセキュリティであり、企業を対象とした仮想私設網（VPN：Virtual Private Network）や、キャリア網（公衆網）・企業網の双方で今後重要なネットワークサービスとなるポリシーネットワークングにおいても、この2つが主要な提供機能となる。電子政府・電子行政サービスにおいても、当面はセキュリティ（下位の暗号化、メッセージ認証、鍵管理、アクセス制御など、上位の認証・決済・課金管理）が最も重要なミドルウェアであるが、サービスがある程度普及しより高度なサービスが

要求される2005年頃以降はQoS制御が重要性が高まる。

ミドルウェアの中の上位におけるエージェントについては、いわゆるAPI(Application Programming Interface、ミドルウェアがその上位のアプリケーションに対して提供するプログラムインタフェース)などが、FIPA (Foundation for Intelligent Physical Agents)やOMG MASIF (Object Management Group Mobile Agent System Interoperability Facility) 等において検討されている。たとえば、近年、イントラネットにおいて重要となっている、数理的、確率統計的な手法や学習理論を用いて大量のデータの傾向や特徴を解析するデータマイニングもCRM (Customer Relationship Management) の一環として、ミドルウェアの中の上位に位置づけられる。

90年代になってその重要性が急速に増したグループウェアについては、マルチメディア会議に代表されるリアルタイム通信型のマルチメディアグループウェアは主に下位に相当し、電子メールを利用した非リアルタイム(非同期)通信型は情報共有の基本メカニズムが下位に、ワークフロー管理の部分が上位に相当する。

2 NGIにおけるミドルウェアの役割

ミドルウェアがいかに重要であることを示す一事例として、米国におけるNII (National Information Infrastructure) からNGI (Next Generation Internet) への発展、移行がある。90年代初頭にゴア副大統領によってNIIが提唱され、その一環として官主導の下HPCC (High Performance Computing and Communications) が推進された。HPCCの実証実験の場として、全米にわたって、AURORA、VISTAnet、NECTAR、CASA、BLANCA、MAGICと呼ばれる6つのギガビットネットワーク・テストベッドが構築された。各テ

ストベッドでは、ギガビットが示す通り、光ファイバを用いて数100Mbpsから一部数Gbpsの通信を可能にした。しかし、これらのテストベッド上で実験したアプリケーションとしては、スーパーコンピュータ間を接続した高速シミュレーションが主であった。しかも、各テストベッドは、その中でしか通信ができず、テストベッド間で情報を交換したり、共有したりすることができなかった。

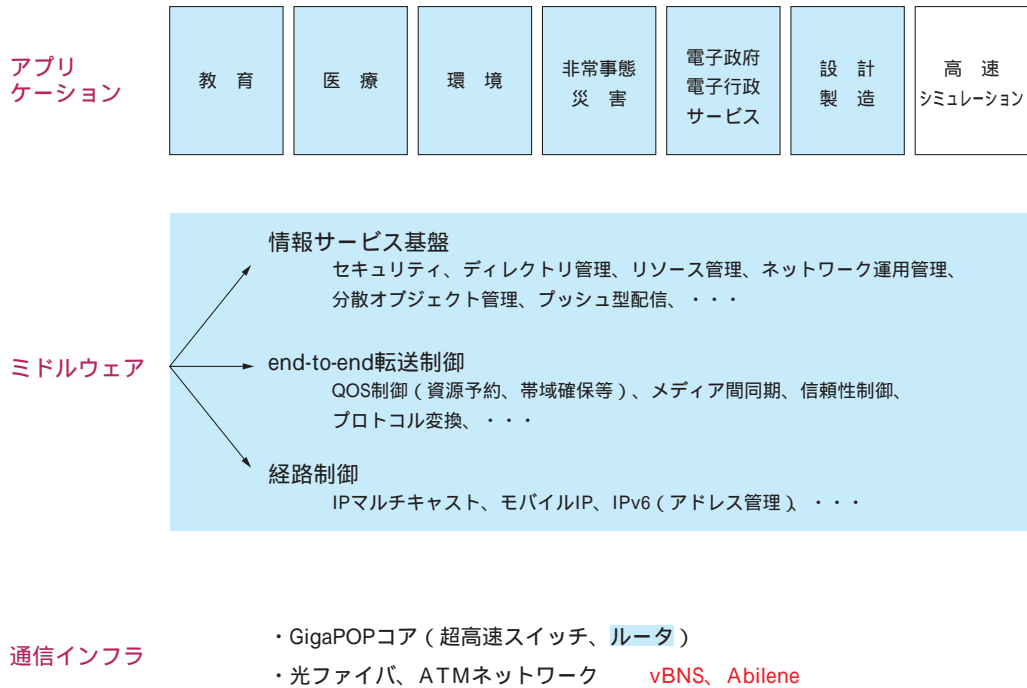
HPCCにおける局所的なHPC (High Performance Computing) とHPC (High Performance Communication) が個別に独立に構築され実験されたが、当初目指したHPCC、すなわち広域ネットワークにおいて多様なアプリケーションを提供するというHPC (High Performance Computing) + HPC (High Performance Communication) (+ は統合の意味を含む) は実現しなかった。

これには、いくつかの理由が考えられる。

- ・当時は未だインターネット (IPプロトコル) のような共通の情報インフラがなく、テストベッド間での相互通信ができなかった。
- ・当時は未だミドルウェアに対する重要性があまり認識されておらず、その技術も未熟で、多様なアプリケーションに対応できるネットワークシステムが構築できる状況ではなかった。

以上のような限界や問題を踏まえて、1998年に開始されたNGIでは、単に通信インフラを高速化するだけでなく、むしろインフラの高速性を生かし、教育、医療、環境、非常事態/災害、電子政府・電子行政サービス、設計/製造、高速科学技術計算/シミュレーションなどの多様なアプリケーションに対応するためには、ミドルウェアが極めて重要な技術と位置づけた。図3にNGIのシステム体系を示す。QoS制御やセキュリティなどについては、最先端技術の標準化を進めているIETFのプロトコルや方式に準拠していくとともに

図3 NGIシステム体系



に、NGIにおける研究成果をIETFに提案していくことを表明している。

ミドルウェアの実現によってはじめて、HPCCが当初目指した、そしてNGIが現在目指している、

- ・多様なサービスの提供
- ・広域でのサービスの利用
- ・高品質なマルチメディア通信

が達成されることになるであろう。

3 マルチメディアアプリケーションとQoS制御

3節と4節では、ミドルウェアの2つの代表的な機能として、QoS制御とセキュリティ制御をとりあげ、その役割について述べる。

QoSが重要となるアプリケーションは、動画と音声を含む通信、いわゆるマルチメディアアプリケーションである。

(1) マルチメディアアプリケーションとその分類

動画と音声を含むマルチメディア通信のアプリ

ケーションは、大きく2つに分けることができる。

一つは、VOD (Video On Demand) に代表されるマルチメディア検索やインターネット放送に代表されるマルチメディア配信 (ストリームメディア配信) であり、広い意味でマルチメディア・オンデマンドといえる。マルチメディア・コンテンツが通信される方向は一方向 (サーバからクライアント端末へ) で、コンテンツの内容そのものがアプリケーションの良否を決定づける重要な要因である。もう一つは、マルチメディア会議に代表されるマルチメディア・グループウェアで、マルチメディア・コンテンツは同時に双方向に通信される。コンテンツは、双方の端末に登場するユーザの表情や音声などが主体となるため、マルチメディア・グループウェア用に新しいコンテンツを特に考える必要はない。

マルチメディア・オンデマンド (電子新聞・ニュース、電子図鑑・百科事典、電子博物館・美術館・図書館、オンラインショッピング・バンキング・決済、チケット予約・発券、ゲームソフト

などのプログラム配信・カラオケ配信、電子行政サービス（住民票や抄本・謄本等の電子申請・届出、行政情報の提供等）、医療画像検索等のデータベース検索ほか）は、コンテンツが重要となる主に家庭向けのサービスに相当する。

マルチメディア・グループウェア（マルチメディア会議・打合せ・フォーラム、遠隔教育・トレーニング、協同デザイン、分散ソフト開発・分散CAD、遠隔保守・点検、遠隔コンサルテーション／悩み相談、遠隔医療、双方向インタラクティブゲームほか）は、効率重視の企業向けがそれぞれ主体となる。

- ・家庭ではある程度の品質が要求されるにもかかわらず現在のインターネットでは高品質の通信ができない（家庭に高品質の動画をオンデマンドに配信するVODは高価格過ぎたため普及に至らなかった）

- ・企業では動画のニーズが現在のところ小さいなどの理由で、マルチメディア・アプリケーションの市場は未だ立ち上がっていない。以下でも述べるように、ブロードバンドインターネットの普及率が20%を超えると予想されている2004年以降のサービス本格化が期待される。

1994年～1998年に京阪奈地方の関西文化学術研究都市において、BBCC（次世代通信網実験協議会）が実施した20近くのマルチメディア実験はすべて、マルチメディア・オンデマンドとマルチメディア・グループウェアのいずれかのカテゴリに属する。インターネットを対象とした動画の符号化・圧縮方式も、マルチメディア・オンデマンドではMPEG4、マルチメディア・グループウェアではH.263（MPEG4はH.263を元としているが）のように別々の標準を規定している。

（2）電子政府・電子行政サービスにおけるマルチメディア通信

マルチメディアオンデマンドに相当するストリーム配信としては、動画を含むマルチメディアで制作された公報やイベント等の自治体情報の住民への配信が考えられる。マルチメディアグループウェアに相当するTV電話としては、住民相談や悩み相談、各種カウンセリング等住民と役所の担当者とのお互いの顔の表情を見ながらの遠隔面談が考えられる。

2001年末現在では、CATVインターネット、ADSL（Asymmetric Digital Subscriber Line）のブロードバンドインターネットの利用世帯数は、それぞれ100万強、50万強で、両者を合わせてもブロードバンドインターネットの普及率はまだ全世帯の4%にも満たない。これらのサービスは、光ファイバを用いたFTTH（Fiber To The Home）を含めたブロードバンドインターネットの利用世帯数が900万世帯、普及率が20%を超えると予想されている2004年ごろから、徐々に本格化するものと思われる。

（3）インターネットにおけるQoS制御

インターネットに限らず一般のネットワークにおいて、動画と音声を品質よく通信するには、

- ・通信帯域の確保
- ・伝送遅延の抑制
- ・遅延のバラツキ（ジッタ）の低減
- ・伝送誤り（パケット／セル損失）の低減
- ・メディア間の同期（会議システムにおける唇の動きと音声との同期など）

などを実現する必要があるが、QoSを保証する上で最も重要かつ基本的な役割を果たすのは、シグナリング制御（論理的なコネクションの設定）時に様々な資源（通信帯域や通信用バッファなど）の予約と、遅延に対する条件が厳しい動画・音声

を文字データなどよりも先んじて送出するような優先制御である。

前者はマルチメディア・コンテンツを通信する前にQoSを保証するための通信路を確保する静的な方法であり、後者はマルチメディア・コンテンツの通信中にその送出タイミングや順序を制御する動的な方法である。すなわち両者は、QoSをそれぞれ静的、動的の両面から相互補完する形で保証するための制御機能である。IETFにおけるQoS制御に関する議論では、資源予約についてはRSVP (Resource reSerVation Protocol)、優先制御についてはDiffServe (Differntiated Services)、パケットスケジューリングなどが代表的なプロトコル・方式である。

通信帯域や通信用バッファに代表される通信品質を保つための各種システム資源の予約については、80年代半ば頃より欧米のインターネットの研究者により、多くのプロトコル・方式が提案され、理論、シミュレーション、実際の各側面から評価が行われた。92年のST (Stream Transport) というプロトコルの提案を経て、インターネットの普及に拍車がかかった94年頃から議論が活発になり、97年にRSVPがRFC (Request For Comments) 化するすなわち標準化がなされた。RSVPは、受信側による制御が基本のためマルチキャストに向いているなどの利点を持つが、

- ①帯域の有効利用 (多くのユーザが品質を要求すると、バックボーン回線の帯域使用効率 (統計多重効果) が低下し、優先度の低いユーザがバックボーン回線の帯域を利用できなくなる。)
- ②ルータの処理負荷 (途中のすべてのルータが下位のレイヤの制御も含めてRSVPに対応する必要があり、その処理負荷はRSVPに対応しない場合の100倍以上といわれている。)
- ③資源予約の単位 (個々のアプリケーション単

位に資源予約ができない。)

- ④プロバイダ間の相互接続 (プロバイダ間のルーティングプロトコルBGP (Border Gateway Protocol) 4がルータを介さない方式をとっており、エンドツーエンドでのRSVPの適用が容易でない。)

などの理由から、多くのISP (Internet Service Provider) が途中に介在する大規模なネットワーク、すなわちインターネット・バックボーンではスケーラビリティの面で利用が難しいことが判明した。

優先制御については、RSVPの検討に押されて90年代半ばはあまり活発に議論されなかったが (RSVPが十分に実現されればQoS制御はほぼ達成されるという向きも多かった、ということに加えて、インターネットが大方の予想を超えてあまりにも急速に普及、すなわち大規模なネットワークとして運用することがこれ程早く必要になるとは思われていなかった)、1997年後半に明白になった上述のRSVPに関するスケーラビリティの問題から、優先制御を実現するDiffServが、QoS保証という面では後退するが、制御が容易でスケーラビリティをもつという利点から急浮上し、1998年中にほぼプロトコルの骨子が固まるという異例の早さで標準化が進展した。

DiffServは、これまで使われなかったIPヘッダの中のTOS (Type Of Service) フィールドを用いて優先度を設定し、IPパケットをその優先度に従って転送制御するもので、回線の使用効率は高くなるが、ネットワークが大規模になるほどその具体的効果は予想しにくく、今後の実装と実ネットワーク上での評価が待たれる。

ATM (Asynchronous Transfer Mode) に対してもスケーラビリティに対応するため、ATM LANを対象としたLANE, NHRP, MPOAなどの方式は殆ど実用化されず、基幹 (バックボーン)

表1 インターネット上のマルチメディア通信制御

マルチメディア通信制御		プロトコル				制御方式			
		RSVP*	RTP/RTCP	RTSP	SDP	DiffServ	IntServ*, ISSLL	MPLS	パケットスケジューリング
伝送レベル	通信帯域保証、予約								
	遅延と揺らぎの検出と補正								
	メディア間同期								
	誤り率の検出と通知								
	優先制御								
	QoS記述								
	転送効率化								
APレベル	QoS指定								

*スケラビリティに問題

図4 レイヤごとのQoS制御プロトコル・方式
(日経コミュニケーションの記事をもとに作成)

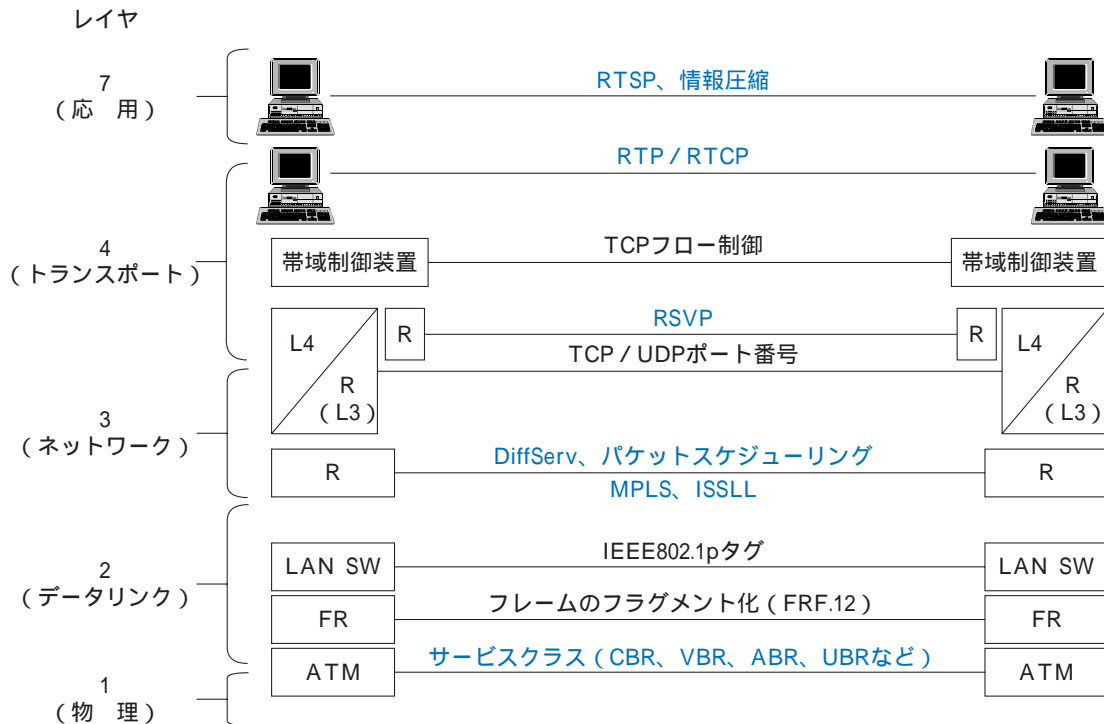
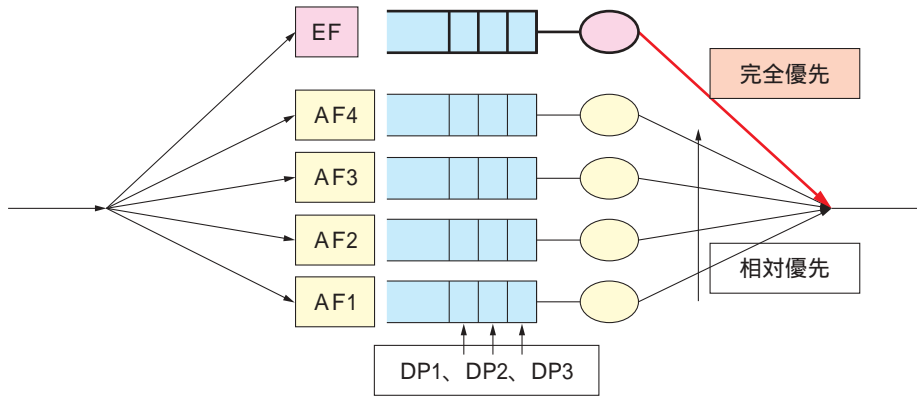


図5 Diffservによる優先制御

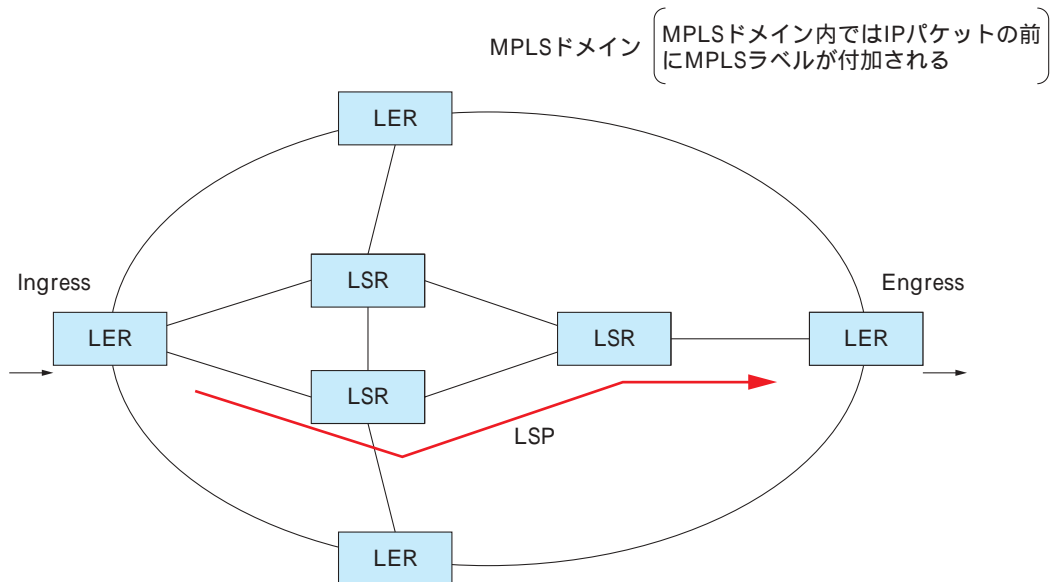
Diffservでは、その実装方式までは規定していないが...

EF : 完全最優先でパケットをフォワードする
 AF : AF4クラスのために、4つのキューを持つ



EF : Expedited Forwarding
 AF ;: Assured Forwarding
 DP : Drop Precedence

図6 MPLSのしくみ



LER : Label Edge Router
 LSR : Label Switching Router

LSP : Label Switching Path

網の転送効率を上げるMPLS (MultiProtocol Label Switching) の検討が活発になっている。表1に、IETFで議論されているQoS制御のためのプロトコル・方式の一覧を示す。図4に、表1に示したQoS制御のためのプロトコル・方式とネットワークの各レイヤとの対応を示す。図5、図6にそれぞれDiffserv, MPLSのしくみを示す。

QoS制御については、表1、図4のように、資源予約と優先制御、転送効率化を中心とした様々なプロトコルと方式が提案されてきた。これらをセキュリティを含めてネットワーク上で‘ポリシー’と呼ぶ統一的な方針に基づきディレクトリを用いて管理しようという概念が98年から叫ばれ、ポリシーネットワークングやポリシー管理の名で盛んに検討されるようになった。ポリシーによって新しいQoS制御やセキュリティの機能を提供するというのではなく、利用者が要求するQoS制御やセキュリティの機能を統一的に記述、登録、管

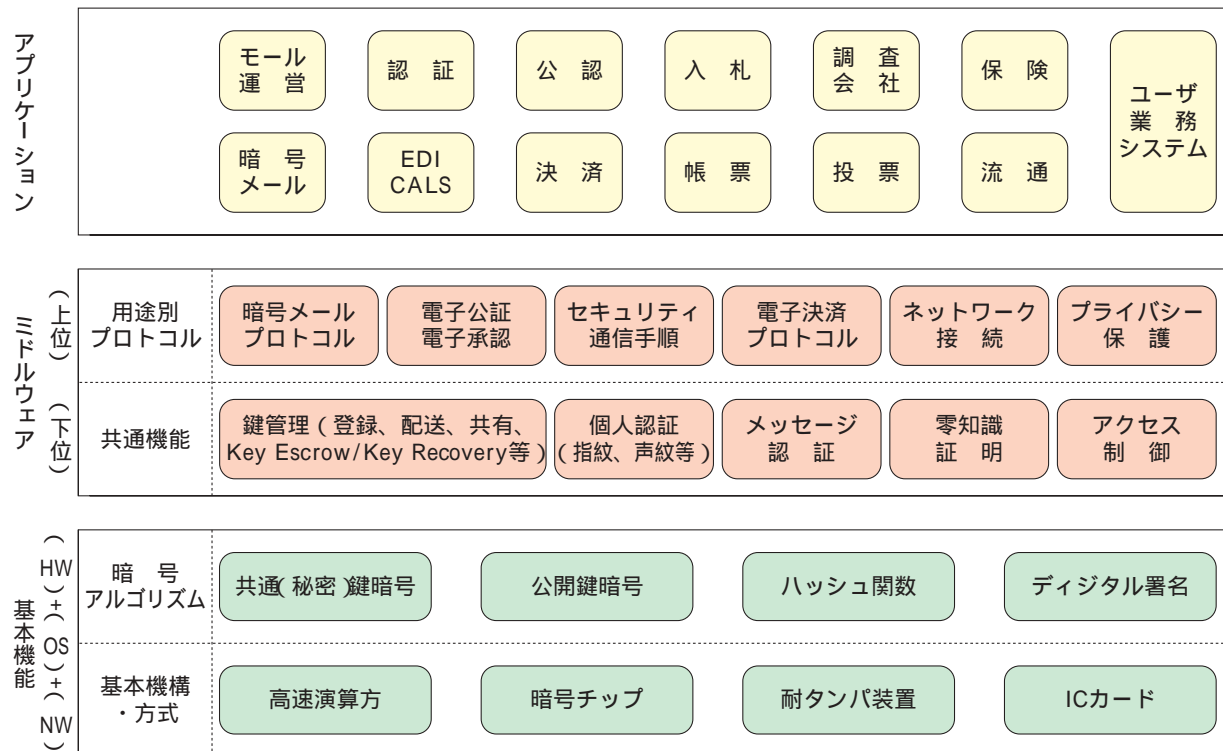
理することによって、あらゆる利用環境において、その要求に応じた各機能を適用しようとするものである。利用者からの申告に応じてディレクトリサーバに格納されたポリシー (PIB: Policy Information Base) を、ポリシーサーバ (PDP: Policy Decision Point) はルータなどのネットワーク制御機器 (PEP: Policy Enforcement Point) に通知し、PEPが実際のQoS制御やセキュリティの機能を実現する。

ポリシーネットワークングは、今後ディレクトリサーバ、ポリシーサーバはじめ各種アプリケーションサーバやルータ、端末までをも含むミドルウェアの基盤技術として重要になると思われる。

4 セキュリティミドルウェア

セキュリティのシステム体系を図7に示す。図7は通常のソフトウェアの階層構造に基づいているが、基本機能の部分には、OSのような基本ソ

図7 セキュリティシステムの階層構造



フトだけでなく、セキュリティ特有の主に暗号処理のためのハード、ネットワーク対応の組み込みソフトも加えている。ミドルウェアの部分についても、アプリケーションに共通な部分(下位)と個々のアプリケーションに依存する部分(上位)に分けている。

暗号アルゴリズムについては、当時盛んに研究された誤り訂正符号の理論を一部応用した研究領域ということもあって、70年代より各国から多くの提案がなされた。しかし、機能の性格上国際標準化を推進しにくい面があり、インターネットが普及した90年代半ばまではそれほど活発には行われなかった。ミドルウェアについては、OSIにおいて認証や決済のプロトコルが80年代半ばに標準化されたが、普及に至らず、結局90年代半ば以降にインターネットを対象とした多くのプロトコル

や方式に関して、IETFを中心に標準化が進められ、2、3年の間に10近くのRFCが発行されている。表2に、電子政府・電子行政サービスにおいて特に重要となる、インターネットで標準化されているプロトコルの一覧を示す。表内の対応レイヤからわかるように、インターネット上で利用されているプロトコルのほぼすべてがミドルウェアで実現される。

セキュリティ技術に関する日本の現状は以下の通りである。クレジットカードやICカードの普及、インターネットの利用面で欧米に遅れをとったこともあり、暗号や個人認証のような個別技術に閉じた部分を除き、技術的に欧米(特に米国)の先行を許している。今後、当面は官(関連省庁)主導の電子マネーやECの実証実験を通してミドルウェアの開発を加速し、2004年頃の民に移行し

表2 インターネットにおける主なセキュリティプロトコル

プロトコル	正式名	主な提案企業	対応するレイヤ	概要
IPSec	IP Security	(IETF標準)	ネットワーク(3)	パケットレベルにおける公開鍵暗号の標準方式。鍵交換プロトコルがIKE(Internet Key Exchange)、インターネットVPNの業界標準となっており、IPv6では実装が必須。
TLS	Transport Layer Security	(IETF標準)	トランスポート(4)	トリプルDES暗号化を必要とし、SSL3.0をより強力にした標準化プロトコル。
PKI	Public Key Infrastructure	特になし	アプリケーション(7)	公開鍵暗号による認証基盤。電子証明、デジタル署名なども提供し不正アクセスを防止。電子政府ではGPKIと呼ばれる。
SSL	Secure Socket Layer	Netscape	トランスポート(4)、セッション(5)	インターネット上でカード番号等をのぞき見できないようにするためのセキュリティ技術。EC関連のプロトコルの業界標準はSET(Secure Electronic Transaction)。
S HTTP	Secure HyperText Transfer Protocol	EIT, Netscape	アプリケーション(7)	インターネット上でカード番号等をのぞき見できないようにするためのセキュリティ技術
SOCKS	SOCKS	NEC	アプリケーション(7)	企業間における情報流出を防ぐ。(自社のWebサーバに接続してホームページを閲覧している相手の企業名、部門名を確認できる)
S/MIME	Secure/Multi purpose Internet Mail Extensions	RSAデータセキュリティ	アプリケーション(7)	公開鍵暗号アルゴリズムを利用した電子メールの認証プロトコル

た実運用のフェーズでは、欧米とも連携を図った情報流通基盤を構築することが肝要である。中でも、電子マネーやECにおいて最も重要な役割を果たす、安全で安心・確実な認証機能と小額を含む決済機能を組合せた課金管理の実現が待たれる。

- 今後、電子政府・電子行政サービス関連では、
- ・プライバシー保護（インフォームドコンセント、匿名性保証）
 - ・不正侵入検知（IDS：Intrusion Detection System）・防止
 - ・ネットワークを通じたサービス停止攻撃・サービス不能化攻撃（DDoS：Distributed Denial of Service attack）検知
 - ・サイバーテロ対策

等が益々重要となり、官と民が効果的に連携した技術開発、法整備が望まれる。

特にIDSとサイバーテロ対策は、従来のファイアウォールよりも攻撃的に踏込んだセキュリティ防御システムとして、電子政府・電子行政サービスのようなGtoB/Cだけでなく、BtoBの電子商取引でも重要なサービス機能になりつつある。IDSはセキュリティエリアや公開エリアを監視し、DDoS攻撃やポートスキャンなどのアタックを受けると、攻撃側のパケットに反撃したり、端末の情報を書き換えて、自動的に自動的に防御・迎撃するシステムである。

5 インターネット・ミドルウェアに関する国際標準化の状況と日本の役割

ミドルウェアは、様々なアプリケーションのプラットフォームとして機能しなければならないので、相互運用の面で重要となるインタフェースについては、世界レベルでの標準化が不可欠である。このことは、世界的に激しいデファクトスタンダード化の競争が展開され、このスタンダードの地位を獲得することが重要な企業戦略、国家戦略

目標となることを意味する。本節では、このインターネット・ミドルウェアに関連する標準化について検討する。

インターネットの中核技術で米国に遅れをとった日本は、未だ国際標準化の中でのプレゼンスは小さいが、今後21世紀に大きなマルチメディア市場を創出すると思われるモバイルコンピューティングやデジタル放送・情報家電・ホームネットワークなどを取込むホームマルチメディアシステム、エージェントアーキテクチャなどのアプリケーション、コンテンツに直結した領域で積極的に提案していくことがまず必要である。特に、2000年12月に開始されたBS（Broadcast Satellite）デジタル放送や2001年10月に開始されたIMT 2000の第3世代移動体通信は、日本が世界に対して先駆けて推進しているものであり、これらの分野で世界をリードしながら、これらの消費者向けECと密接な関係をもつ電子政府・電子行政サービスのためのミドルウェアにおいても世界への提案・発信が重要である。

さらにインターネットミドルウェアの根幹でかつ最重要技術のQoS制御とセキュリティについても、海外企業とも適切に連携し、これまでの遅れを取戻すべく技術コンピタンスを育成することが極めて肝要であることを主張する。

IETFが1984年、W3Cが丁度10年後の1994年に発足している。図8にインターネットミドルウェアの標準化の位置づけを示す。

①IETF

IETFは、年3回の会合で標準化の審議を行うが、1993年頃までは1回の会合に参加者が1000名を超すことはなかったが、WWWの開発によってインターネットへの注目が高まり始めた1994年に1000名を超すようになった。その後、インターネットが全世界の情報インフラとしての地位を築き、大規模網としても検討すべき対象になった

図8 インターネット関連の標準化

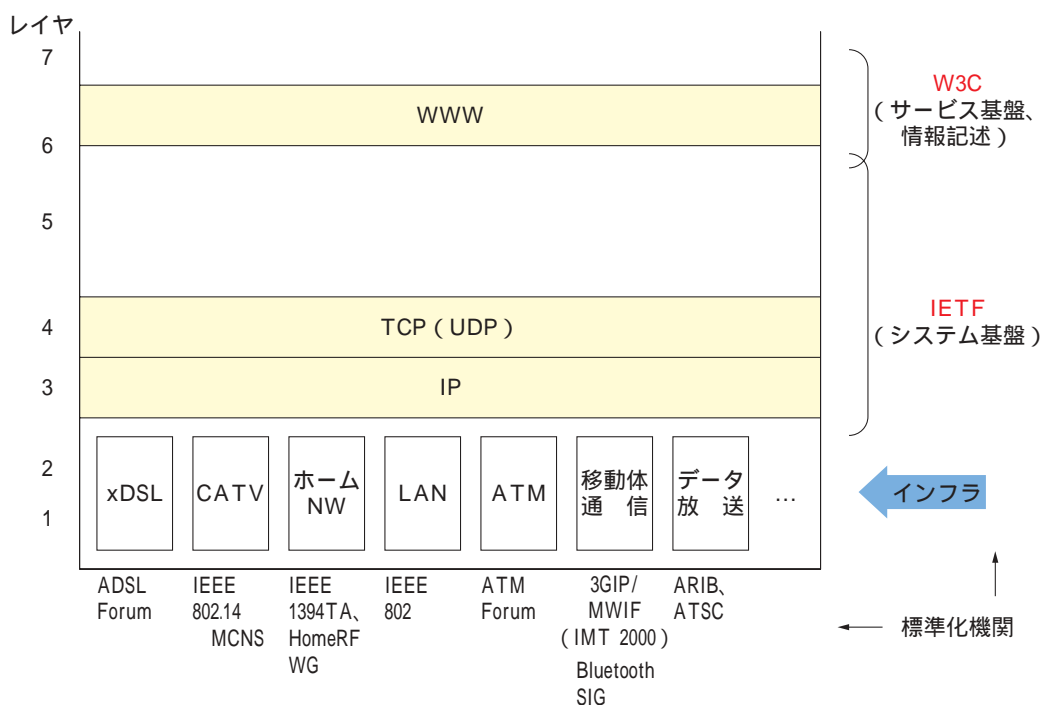


表3 IETFを構成するAreaと主な検討内容

Area名	主な検討内容	主なプロトコル
Genera	標準化のプロセス	
Internet	IP、IPアドレス	IPv6, DHCP, PPP
Routing	ルーティング、モバイルマルチキャスト通信	RIP, OSPF, IP Multicast, Mobile IP, MPLS , QOSPF
Transport	マルチメディア通信、インターネットテレフォニ	RTP/RTCP, SDP, SAP, SIP, IntServ/RSVP, ISLL, RTSP, DiffServ , IPtel/MEGACO
Applications	ディレクトリサービス、アプリケーション	IDS, FTP, HTTP, MIME
User Services	一般社会へのサービス	
Security	ユーザ認証、ファイアウォール	IPsec, TLS, PKI
Operations & Management (O&M)	ネットワーク管理、オペレーション支援	Policy Framework , TE , AAA SNMP, 各種MIB CIDR, MBONE

1997年以降、コモンキャリア（通信業者）からの参加が急増したこともあって、毎回2000名に及ぶ参加者を集めるようになってきている。

IETFは、表3に示すように、General、Internet、Routing、Transport、Security、Applications、User Services、Operations and Manage-

mentの8つのAreaに分かれ、それぞれのAreaの幾つかのWG（Working Group）で実質的な議論がなされる。QoS制御やマルチメディア通信関連はTransport Area、セキュリティ関連はSecurity Areaで検討されている。

IETFへの提案は米国からのものが8割以上を

占め、有名な国際会議や学会で活躍しているコンピュータネットワーク関連の世界トップレベルの研究者も、多くの提案を行っている。IETFに提案された後にその内容が、国際会議や学会で最先端技術の成果として論文発表されることも多くなっている。すなわち、分野によっては（QoS制御やセキュリティなど）、世界の最先端の技術が発表される学会と同じかあるいはそれ以上に、IETFでの議論のレベルの高さが認められている。

日本からの提案は1995年頃までは全体の1%にも満たない状況であったが、日本が世界の市場をほぼ独占しているFAXのインターネット上での通信に関する標準化（インターネットFAX）で1996年から1997年にかけて主導権をとったこともあって、それ以降は日本からの提案が増加している。セキュリティ分野でも日本からの発表も目立つようになってきている。しかし、インターネット技術に関して、セキュリティと並ぶかそれ以上の重要性をもつQoS制御（Transport Area）領域での提案はまだ殆どない。

コンピュータと通信の両技術が効果的に連携して始めて実現されるマルチメディア情報通信の基本であるQoS制御の領域（Transport Area）や電

子政府・電子行政サービスにおいて当面極めて重要となるセキュリティ（Security Area）で提案していくことは、最先端のミドルウェア技術において国際的に貢献していく上で極めて重要である。中でも今後この領域において中核技術となるポリシーネットワークング関連での日本からの活発な提案が期待される。このためには、海外の先端研究者との密な連携、産学での効果的な役割分担と協力が必須である。

②W3C

W3Cは、ヨーロッパ（INRIA、仏）、北米（MIT、米）、アジア（慶大、日）が各地域を代表する管理機関となって運営している。全体としての定期的な会合は総会のような比較的形式的なものに留め、IETFのように定期的な会合で標準化のための深い議論は行っていない。標準化のための技術的な議論は、各Domain（IETFにおけるAreaに相当）の中の各WGで行う。WGの会合の開催はWG毎に任されている。W3Cは、表4に示すように、User Interface, Architecture, Technology and Society, WAI（Web Accessibility Initiative）の4つのDomainから構成され、Web上でのマルチメディア情報の表現やその制御方式については、

表4 W3Cにおける標準化活動

ドメイン	主要項目	プロトコル	情報記述
User Interface	<ul style="list-style-type: none"> ・HTML ・レイアウト設定(CSS/XSL) ・文書モデル(DOM) ・モバイルコンピューティング ・デジタル放送 		
Architecture	<ul style="list-style-type: none"> ・HTTP ・XML ・メディア間同期(SMIL) 		
Technology & Society	<ul style="list-style-type: none"> ・メタ情報(RDF) ・個人情報プロファイル(P3P) ・情報フィルタリング(PICS) 		
Web Accessibility Initiative	<ul style="list-style-type: none"> ・障害者への対応 		

表5 インターネットの課題

第 1 世 代 (60年代末~1995年) 専門家ネットワーク	第 2 世 代 (~2005年) 一般ユーザに普及	第 3 世 代 (2005年~) 生活の隅々まで浸透、ユビキタスに。QoSからQoL(Life) へ
軍 ARPANET 学 CSNET, NSFNET 民 Internet ・ TC/IPベースの商用ネットワークへ ・ WWWにより一般ユーザへの普及が開始	・ 広帯域化 IP over WDM Photonic Network ・ アドレス空間拡大 IPv6 ・ QoS制御 DiffServ, MPLS パケットスケジューリング ・ マルチキャスト IP Multicast 高信頼マルチキャスト ・ モビリティ機能 Mobile IP ・ ルータ性能向上 テラビットルータ ・ セキュリティ 暗号、認証、決済	・ ペタビットルータ ・ PAN (Personal Area Network)、 HAN (Home Area Network) への展開と端末の多様化 家電、車、センサ、ウェアラブル機器、アドホック / 高密度ネットワーク ・ ヘテロジニアス環境 通信媒体、インタフェースの多様化、標準化とシームレス相互接続・運用 ・ 状況適応サービス サービス発見と最適形態での提供、環境情報コンピューティング ・ 一つのパーソナルアドレスによるすべてのサービスの提供 VHE(Virtual Home Environment)からモバイル対応AAAへ ・ 動的資源配分による自己組織型ネットワーク アクティブネットワークなど ・ ネットワーク管理自動化/Plug & Play

User InterfaceとArchitectureの2つのDomainで分担して検討している。

IETFと比較すると相対的には日本からの貢献は大きい。ユーザプロファイル(各利用者の姓名、生年月日、職業などの個人に関する情報)記述のP3P(Platform for Privacy Preferences)や、新しい応用領域で、無線通信と放送というもともと日本が比較的強い技術を保有している、Webへのモバイルアクセス、TV&Web(デジタル放

送とWebとの融合)などでは日本からいくつか提案されている。

中長期先のインターネットの技術課題を表5にまとめて示す。要約すると、ブロードバンド化、ユビキタス/モバイル化、インテリジェント化を進展させるための課題であり、電子政府・電子行政サービスにとっても、その普及、高度化において克服していくことが必須である。

参考文献

- (1) 阪田「マルチメディアネットワーク技術の動向 高品質映像通信からインターネットマルチメディアへ」, bit、1998 .11 .
- (2) 阪田、小林「インターネット上のマルチメディア通信」, bit、1998 .6 .
- (3) 「21世紀デジタル社会の暗号政策への提言 暗号通信のあり方に関する研究会報告書」, 郵政省電気通信局、1999 .6 .
- (4) 阪田編著「モバイルコンピューティング」, アスキー出版、1999 .5 .
- (5) 阪田、田淵「デジタル放送とインターネット」, bit、1999 .5 .
- (6) 阪田他「インターネットとQoS制御」, 裳華房、2001 .6 .
- (7) 阪田他「情報家電とインターネット」, 裳華房、2001 .10 .
- (8) 阪田他「爆発するインターネット」, オーム社、2000 .10 .
- (9) 阪田他「21世紀の技術革新 モバイルインターネット」工業調査会、2000 .11 .
- (10) 阪田「インターネットストリーミング技術」電子情報通信学会講演会資料、2001 .6 .
- (11) 阪田「モバイルインターネットの展望」情報処理学会誌、2001 .12 .
- (12) 阪田「インターネットにおけるQoS制御」電子情報通信学会誌、2002 .5 .