第5章 IMSにおけるセッション制御

4.1節では、一般のインターネット上でSIPがどのように使われているかを解説した。また、SIPのコアの機能やSIP UAでサポート可能な、いくつかの重要な拡張機能についても詳しく見てきた。個々のSIPは、アプリケーションからの要求に応じて、これらの各オプションや拡張機能を選んで実装することになる。

3GPP（Third Generation Partnership Project）のシステムは、SIPを無線環境下で利用するという条件のSIPアプリケーションの1つである。3GPPでは、SIPは様々な制約条件を課されたパケット網で動作することになる。無線環境でSIPを利用するための検討の結果、SIPを3GPPネットワークに適用するのに必要な条件が明らかになった。この条件に対する解決策を実装するために、3GPPでは、SIPおよびその他のいくつかのプロトコルに対して、多くのオプション選択と拡張機能を必ず利用することになっている。3GPPの役割は、IMSにおけるSIPおよびその他関連プロトコルの利用方法に関するプロファイルを定めることだと考えてよい。IMSのための3GPP SIPプロファイルは、3GPP TS24.229 [37] で規定されている。SIPを利用するという点では、パブリックなインターネットで使う場合と違いはないので、この規定を「プロファイル」と呼ぶことができる。しかし一方、3GPPはIMSのネットワークノードと端末の双方に対して、多くのオプション選択と拡張機能の実装要求を課している。本章では、SIPがIMSにおいてはどのように使われているのかについて焦点を当て、一般のインターネットで使われるSIPの用法とどう違うのかを明らかにしていく。

3GPPでIMSのためのセッション制御の開発が開始されたとき、SIPがそのセッション制御プロトコルとして選択された。同じ時期にIETFでは、SIPの改版作業が行われ、RFC 2543 [161] からRFC 3261 [286] およびその他のRFC文書への移行と拡張が行われた。それ以前には、無線環境におけるSIPの検討は行われてはいなかった。

無線環境では、SIPのようなセッション制御プロトコルに対して、多くの厳しい要求条件が求められる。これらの要求条件は、セキュリティ上の要求条件から、ユーザがホームネットワークかローミング先のネットワークのどこでも同じようなサービスを受けることができること、というような要求条件まであって幅広い。IETFは、これらの要求条件を検討し、ほとんどのものをIETFでの検討対象とした。その結果として、多くのSIPによる解決策の提案が行われ、RFC 3261 [286] のコアのSIP仕様に含められるか、あるいはSIPの拡張機能とし

て別の文書で定められた。これらの拡張機能について、本章でIMSでのセッション制御を詳しく説明する際に分析することにしよう。

5.1 IMSにおける処理動作の前提条件

IMS端末がIMSの利用を始める前に、満たしておかなければならない多くの前提条件がある。**図 5.1**は、要求される前提条件について大まかな全体像を示したものである。

まず初めに、IMSサービス事業者は、エンドユーザのIMSサービス利用を認可する（Authorize）必要がある。これには通常、IMSネットワークの運用管理者とユーザとの間で登録や契約を交わしておくことが必要となる。この契約は、従来の携帯電話ユーザが使えるようにするために事業者との間で交わす加入契約と同等のものである。

次にIMS端末は、GPRS（General Packet Radio Service）[※1]、ADSL、WLANなどのIP-CAN（IP Connectivity Access Network：IP接続アクセスネットワーク）にアクセスすることが必要となる。IP-CANは、IMSのホームネットワークやローミング先ネットワークへのアクセス手段を提供するものである。IMSの前提条件の1つとして、IMS端末はIPアドレスを取得することが必要となる（GPRSアクセスでの手続きは、3GPP TS 23.060［35］）。通常、端末のIPアドレスは、IP-CANの事業者によってある一定期限の下で動的に割り当てられる。

これらの2つの前提条件が揃うと、IMS端末は、アウトバウンドおよびインバウンドのプロキ

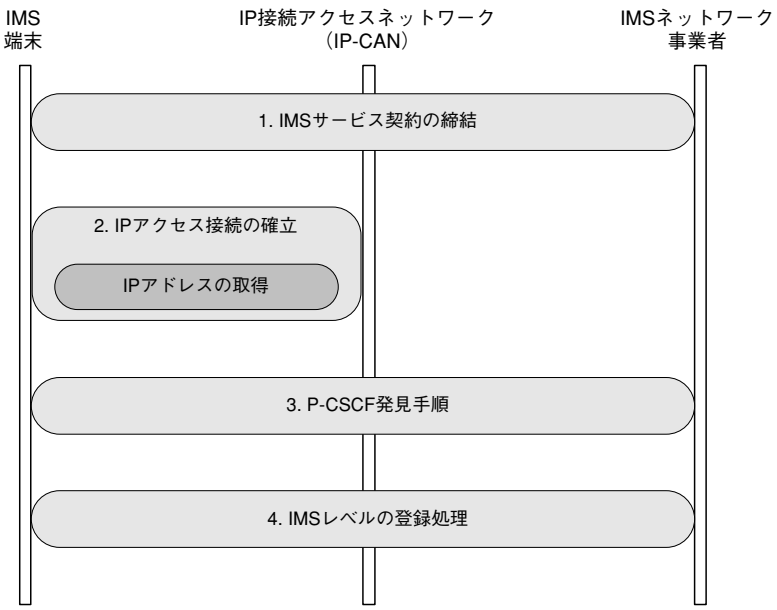

図 5.1　IMSサービスを利用するための前提条件

※1［訳註］GSM網/UMTS網で用いられるパケットデータ伝送技術。

シサーバとして動作するP-CSCF（Proxy Call/Session Control Function）のIPアドレスを知る必要がある。IMS端末によって送信されるSIPメッセージは全て、このP-CSCFを経由して送信される。P-CSCF発見手順が完了すると、IMS端末はP-CSCFとの間でSIPメッセージの送受信が可能となる。通常は、IMS端末の電源オンから電源オフまでの間の、ロケーション登録が有効な間は、P-CSCFは固定的に割り当てられることになる。

P-CSCF発見手順は、利用されるIP-CANの種類によって、IP-CANへの接続を確立する手順の中で行われる場合もあるし、IP-CANへの接続手順とは別の手順として行われる場合もある。独立して行われる場合のP-CSCF発見手順では、DHCP（Dynamic Host Configuration Protocol、RFC 2131［123］）もしくはDHCPv6（DHCP for IPv6、RFC 3315［124］）が用いられる。

ここまでの前提条件が満たされると、IMS端末はSIPのアプリケーションレベルでIMSネットワークにロケーション登録を行う。登録処理は通常のSIPの処理手順に沿って行われる。IMS端末は、全てのSIP信号手順の開始および受信処理に先立って、ネットワークへの登録処理を行う必要がある。IMSはいくつかのレイヤ構成に沿ってモデル化されており、IP-CANのレイヤはIMSのアプリケーションレイヤ（すなわちSIP）とは独立している。そのため、IMSレベルでの登録処理は、IP-CANへの登録処理（例えばGPRSへのアタッチメント処理）とは独立したものである。IMSの登録処理により、IMSネットワークではユーザの位置を知ることができる（つまり、IMSネットワークは端末のIPアドレス知ることができる）。またこれにより、IMSネットワークはユーザを認証し、セキュリティアソシエーション（SA）を確立し、セッションの確立を認可することができる。IMSのセキュリティ機能については12章で説明する。

5.2 IMSにおけるIPv4とIPv6

3GPPでIMSが設計されたとき、IPv6がIETFで標準化されつつあった。3GPPはIMSへのIPv6の適用を検討し、IMSが最初に運用されるときまでにはIPv6がインターネットで最も一般的なIPバージョンになっているだろうと結論付けた。IPv4の大規模な導入にはプライベートIPアドレスの割当てが必要になり、通信経路上で何らかの形でのNATが必要となる。

SIPとその関連プロトコル（SDP、RTP、RTCPなど）は、NATを越える場合に問題が生じるプロトコルの例として知られていた。IMSでIPv4を許容するためには、NAT越えの技術に関して相当な議論が必要になると考えられた。

これらの理由をもって、3GPPはIPv6をIMS接続のための唯一のIPバージョンとすることを選択した。

しかし不幸にも、初期のIMS製品が市場に現れたときの状況は、その数年前に予測した状況とはまったく異なっていた。IPv6は広まっておらず、IPv4とNATがいたるところに存在しており、SIPとその関連プロトコルが簡単にNAT越えできるようにするための研究が行われていた。

2004年6月に3GPPは、IPv4とIPv6のジレンマについて再度検討した。その時点では、IPv6はまだまだ主流にはなっていない、ということがマーケットの答えであった。インターネットの

ほとんどは、まだIPv4で動作しており、2〜3の移動体網だけがIMSで要求されるような大規模IPv6を導入する準備をしているだけであった。一方、SIPのNAT越えの研究が大きく進展し、SIPはNAT越え可能なプロトコルとなった。つまり、IPv4をサポートするための特に余計な機能追加が必要なかったため、IPv4は初期のIMS製品のほとんどで実装されていた。

これら全ての状況を踏まえ、3GPPはIMSの最初の版である3GPPリリース5の段階からIPv4の初期実装を許容することを決定した。IMSでIPv4をサポートするための検討は、3GPP TR 23.981［16］にまとめられた。3GPPの主要アーキテクチャ文書である3GPP TS 23.221［30］には、IPv4をサポートするIMS実装のための、3GPP TR 23.981［16］への参照が追加された。

単一のIPバージョンの実装と同様に、今ではIMS端末とネットワークノードの双方で、IPv4とIPv6のデュアルスタックの実装が許容されている。このため、IMS-ALG（Application Layer Gateway）とTrGW（Transition Gateway）と呼ばれる2つの新しいノードがIMSアーキテクチャに加えられた。IMS-ALGはSIPのIPv4とIPv6間のインタワークを扱うものであり、TrGWはRTPのIPv4とIPv6間のインタワークを扱うものである。

IPv4をIMSに追加した結果として、パブリックなインターネットでのIPv6の導入が遅れることになった。IMSがIPv6普及の主たる推進力となっていれば、インターネットにおけるIPv6の導入を後押ししていたはずである。IPv6が将来的にインターネットにおける共通バージョンとなることには、ほとんど全ての人が賛成するものの、それはまだ先のことであり、IMSは現実とともに進んでいかなくてはならない。

なお本章以降、本書では、IPv4とIPv6の両方のIMSに考慮しつつ、IPv6の例を優先している。私たち著者としては、IPv6が将来を約束されたプロトコルであると信じており、より多くの分析をIPv6のIMSに加えることに対して、ほとんどの読者が賛同してくれるものと信じている。

5.3 IP接続アクセスネットワーク（IP-CAN）

IP-CANには、様々な種類がある。例えば、固定通信環境でのIP-CANの例としては、DSL、ダイヤルアップ、企業LANなどが挙げられる。無線通信環境では、GPRSや無線LANなどのようなパケット・データアクセスが挙げられる。いずれも登録とIPアドレス取得の手順は、IP-CANの種類によって異なる。

例えばGPRSにおいては、IMS端末はまず、GPRSアタッチ手順（GPRS Attach Procedure）という一定の手順を踏む。この手順の処理では、SGSNからHLR、GGSNまで複数のノードが関係する。**図 5.2**に、この手順を示す。この手順がいったん完了すると、端末はPDPコンテキスト※2の起動要求（Activate PDP Context Request）メッセージをSGSNに対して送信し、IPv4もしくはIPv6網への接続を要求する。このメッセージには、特定のAPN（Access Point Name：アクセ

※2［訳註］ PDPコンテキスト（Packet Data Protocol Context）とは、3GPPのパケットデータ・ネットワークにおいて、端末からGGSNまでの論理的なパケット転送パスもしくは各エンティティ（端末-SGSN-GGSN）でのパス設定の状態情報を指す。

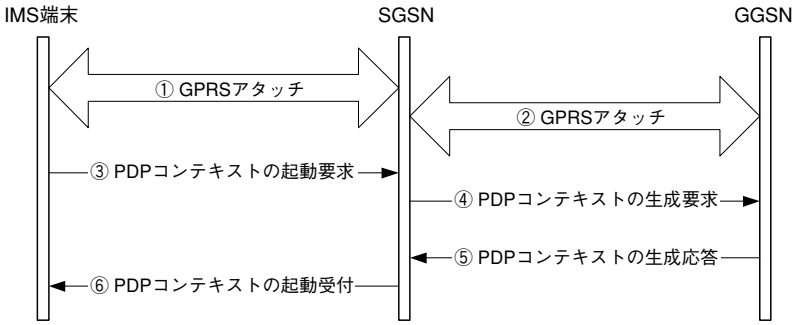

図 5.2　GPRSにおけるIPアドレス取得

スポイント名）への接続要求とパケット接続タイプの情報が含まれており、APNによって接続先のネットワークとIPアドレスが属するアドレス空間を特定することができる。IMS端末の場合、APNには要求する接続ネットワークはIMSネットワーク、接続タイプはIPv4もしくはIPv6が指定されることになる。SGSNは、APNと接続タイプに応じて、適切なGGSNを選択し、PDPコンテキストの生成要求（Create PDP Context Request）メッセージをそのGGSNに対して送信する。メッセージを受信したGGSNは、責任を持ってIPアドレスの割当てを行う。

IMS端末がIPv6を要求した場合、GGSNは端末に対してIMSアドレス空間に属している特定の1つのIPv6アドレスの割当てを行うわけではない。GGSNは、端末に対して、特定の128ビットのアドレスではなく、64ビットのIPv6プリフィックスを割り当て、その内容をPDPコンテキストの生成応答（Create PDP Context Response）メッセージに含めて送信する。SGSNは、このIPv6プリフィックスをPDPコンテキストの起動受付（Activate PDP Context Accept）メッセージに透過的に設定して端末に転送する。したがって、GPRSアタッチ手順が完了したとき、IMS端末は64ビットのIPv6プリフィックスを取得していることになる。端末は、任意のIPv6サフィックス（後位の64ビット）を選択することができ、これにより、128ビットのIPv6アドレス（すなわち、端末がIMSトラフィックのために使うアドレス）が構成される。

これに対し、IMS端末がIPv4を要求した場合は、GGSNは端末で利用するIPv4アドレスを直接割り当てる。

IP-CANがGPRSでなかった場合、IMS端末を設定するために、DHCP（RFC 2131［123］）かDHCPv6（RFC 3315［124］）が使われる可能性が高い。DHCPは、設定パラメータを端末に伝えるときに使われるプロトコルである。DHCPの主な目的はIPアドレスの付与だが、それに加えて端末が要求すれば、DHCPサーバはアウトバウンド・プロキシサーバのアドレスやHTTPプロキシサーバのアドレスなど、他の種類の設定データについても端末に伝えることができるようになっている。

IP-CANへの接続において、ユーザは何らかの利用登録と利用料金の支払いを必要とすることがある。現在、空港やホテルなどでは、Hot Spotを利用した無線LANアクセス環境が増えてきている。通常、このようなHot Spotへのアクセスのためには、何らかの形のサービスへの申込みと、何らかの形の料金支払いが必要となる。例えば、サイトにログインしてユーザ名とパス

ワードを入力することが必要だったり、サービス利用料を支払うためのクレジットカード情報の入力が必要であったりする。また他のIP-CANの形態としては、3GPPの無線LANアクセス網も挙げることができる。

5.4 P-CSCF発見手順

P-CSCF発見手順（P-CSCF Discovery）は、IMS端末がP-CSCFのIPアドレスを取得する手順である。P-CSCFは、IMS端末に対してアウトバウンドおよびインバウンド・プロキシサーバとして動作する。つまり、全てのIMS端末から送信されるSIPメッセージおよびIMS端末へ送信されるSIPメッセージは、P-CSCFを通ることになる。

P-CSCF発見手順は、幾つかの方式がある。

●IP-CANへのアクセスを獲得する手順に統合された手順
●独立した手順

統合型のP-CSCF発見手順は、IP-CANの種類によって異なる。IP-CANがGPRSである場合、GPRSアタッチ手順が完了したときには、端末はGPRSネットワークの利用が認可されている。その後、IMS端末は、いわゆるPDPコンテキスト起動手順と呼ばれる処理を行う。この手順の主な目的はIMS端末のIPアドレス※3を設定することだが、この場合IMS端末は、SIPリクエストを送信してきたP-CSCFのIPアドレスも同時に知ることになる。

一方、独立型のP-CSCF発見手順は、DHCPあるいはDHCPv6と、DNS（Domain Name System：RFC 1034［217］）に基づいて行われる。

DHCPv6では、端末は予約されたマルチキャストアドレスに対してDHCPメッセージを送信するため、DHCPサーバのアドレスを知っている必要はない。DHCP（IPv4）が利用される場合、端末はローカルな物理的サブネットに対してdiscoverメッセージをブロードキャストする。構成によっては、端末は意識する必要はないが、DHCPメッセージを適切なネットワークに中継するためにDHCPリレーが必要となることがある。

図 5.3のステップ①と②に、この手順を示す。IMS端末がいったんIP-CANへ接続できるようになると、IMS端末は、DHCPサーバに対して、SIPサーバのためのDHCPv6オプション（RFC 3319［305］）を要求するDHCPv6 Information-Requestを送信する（①）。IMSの場合、P-CSCFはアウトバウンドおよびインバウンド・プロキシサーバとしての役割を持つので、DHCPサーバは、1つ以上のドメイン名あるいは1つ以上のP-CSCFのIPアドレス（もしくはその両方）を含むDHCP Replyメッセージを返送する（②）。

※3 IPv6が利用される場合、実際のIMS端末では64ビットのIPv6プリフィックスが設定される。IMS端末は、任意の64ビットのサフィックスを選んで、128ビットのIPv6アドレスを完成することになる。

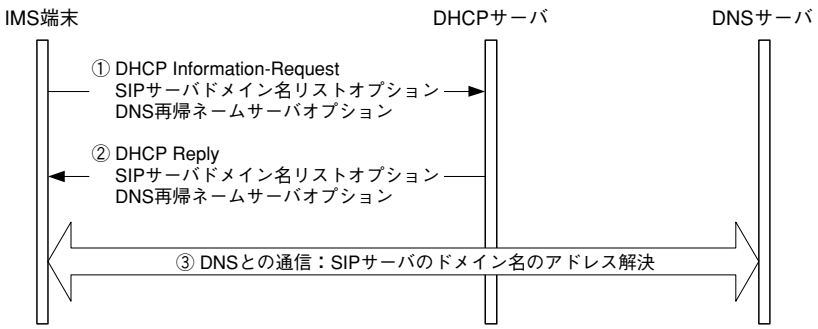

図 5.3　DHCPとDNSに基づくP-CSCF発見手順

IMS端末が、SIPサーバのためのDHCPv6オプションを要求する方法は2つあり、IMS端末の実装により自由に選択することができる。

- IMS端末がDHCPv6 Information-Requestメッセージ※4で**SIPサーバドメイン名リストオプション**を要求する。DHCPv6 Replyメッセージには、P-CSCFのドメイン名の候補リストが含まれる。IMS端末は、これらのドメイン名中の少なくとも1つについてアドレス解決を行い、IPv6アドレスを得る必要がある。このP-CSCFのドメイン名の解決はDNSへの問合せによって行われるが、そのためには、事前にIMS端末はDNSメッセージを送信するDNSサーバのアドレスを少なくとも1つ以上は知っている必要がある。この問題を解決するために、図 5.3の①のDHCP Information-Requestメッセージには、SIPサーバオプションだけでなく、**DNS再帰ネームサーバ・オプション**が含められている。DHCPv6 Replyメッセージ②には、P-CSCFのドメイン名に加えてDNSサーバのIPv6アドレスのリストが含まれる。そしてIMS端末は、②のメッセージによって通知されたばかりのDNSサーバに、P-CSCFのドメイン名から1つ以上のIPv6アドレスを得るための問合せを行う。SIPサーバ名から複数のIPアドレスを得る手順は、RFC 3263［285］によって標準化されている。
- もう１つの方法は、IMS端末がDHCPv6 Information-Requestメッセージで**SIPサーバIPv6アドレス・リストオプション**を要求する方法である。DHCPサーバは、IMS端末に割り当てられるP-CSCFのIPv6アドレスのリストを含むDHCP Replyメッセージを返送する。この場合、IMS端末は、1つ以上のIPv6アドレスを直接知ることができるため、DNSとのやり取りは必要ない。

これらの2つの方法は、互いに排他的であるわけではない。IMS端末が**SIPサーバドメイン名**

※4　SIPサーバDHCPv6オプションは、DHCPv4の同様のオプションとは異なる。DHCPv6では、ドメイン名かSIPサーバのIPアドレスかの２つの異なるオプションコードが存在する。DHCPv4では、２つの違う答え、ドメイン名かIPv4アドレスが返ってくる可能性がある１つのオプションコードが存在する。DHCPv4のオプション数は最大256に制限されており、これに対してDHCPv6では最大65,535である。このためDHCPv6では、必要な２つのオプションコードを割り当てるための十分な空間が存在している。

リストオプションと**SIPサーバIPv6アドレス・リストオプション**の両方を要求することは必ずしも必要ではないが可能である。ただしDHCPサーバは、このような要求に対して両方のオプションではなく、片方のオプションの回答のみを返送する可能性はある。もしDHCPサーバが両方のリストの応答を返す場合、IMS端末側ではSIPサーバドメイン名リストの方を優先して処理するべきである。両方式で得られた結果を処理する方法は、RFC 3263［285］に記述されている。

P-CSCFのアドレスを取得する他の方法は、何らかの別のやり方で事前設定を行うことである。例えば、端末に送信するSMS（Short Message Service）のメッセージによって設定を行ったり、OMA（Open Mobile Alliance）で規定されているクライアント・プロビジョニング［227］やデバイス管理［231］などがその設定方法の例として挙げられる。

最終的にIMS端末は、P-CSCFのIPアドレスを知り、SIPメッセージを自分に割り当てられたP-CSCFに対して送信することができるようになる。P-CSCFは、SIP上の次ホップに向けて受信したSIPメッセージの転送処理を行う。IMS端末に割り当てられたP-CSCFは、再度P-CSCF発見手順が行われない限り変更されない。通常、P-CSCF発見手順は、端末に電源を入れたときか、激しいエラー状態が起きた後にだけ実行される。ここで重要な点は、P-CSCFのアドレスが固定的であるので、IMS端末はその変更の可能性について心配する必要がないということである。

5.5 IMSレベル登録処理

IMS端末がIP-CANへのアクセスを確保する手順を終え、IPv6アドレスを取得もしくは構成し、P-CSCFのIPv4アドレスもしくはIPv6アドレスを知ると、端末はIMSレベルでの登録処理を行うことができるようになる。

IMSレベルの登録処理は、IMSユーザがIMSネットワークにおけるIMSサービスの利用の認可を要求する手順でもある。このときIMSネットワークは、ネットワークへアクセスするユーザを認証し、利用認可を行う。

IMSレベルの登録処理は、REGISTERリクエストによって実現される。4.1.4項で、SIP登録処理はユーザの**パブリックURI**をログインする端末のホスト名もしくはIPアドレスを含むURIに結び付ける処理である、と説明した。通常のSIPとは異なり、IMSでの登録処理は、IMSがセッションを確立する前に必ず実施しておく必要がある。

IMSでの登録処理では、REGISTERリクエストが利用される。しかし、メッセージ往復回数を最小限にしたいという3GPPの要求を満たすために、この処理には単なる登録処理に加えて、非常に多くの処理内容が含まれている。**図 5.4**※5に示す通り、この処理は2往復のメッセージ交換で手順が完了するようになっており、3GPPの意図は反映させられている。

※5 簡略化のため、図 5.4にはSLF（Subscriber Location Function）を含めていない。ホームネットワークにHSSが1つ以上存在する場合には、SLFが必要となる。

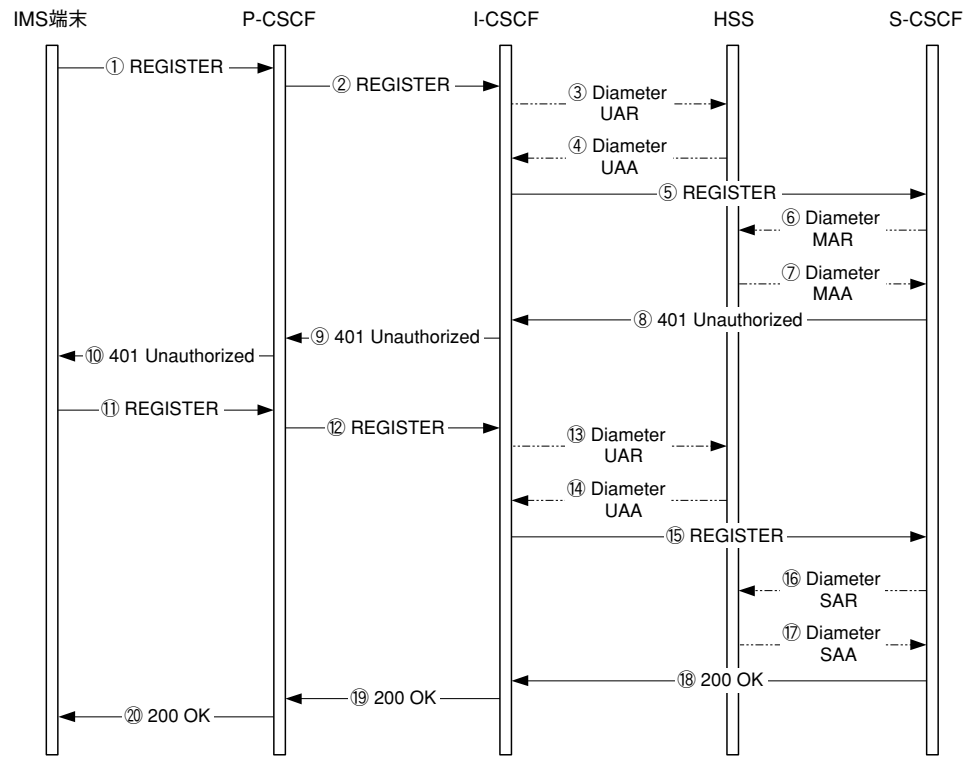

図 5.4　IMSレベルでの登録処理

5.5.1　ISIMによるIMS登録処理

ユーザがIMSネットワークにアクセスするときに、そのユーザを認証するためにIMS端末はUICC（Universal Integrated Circuit Card）を有している必要がある。このことについては3.6節で説明した。UICCは、ISIM（IP multimedia Service Identity Module）アプリケーションかUSIM（Universal Subscriber Identity Module）アプリケーション、もしくはその両方を含むことができる。ISIMは、IMS特有のものであり、またUSIMはIMSが設計される前の回線交換網およびパケット交換網で既に利用されてきた規格であるため、双方のアプリケーションで保持されているパラメータは全く異なっている。登録処理自体はISIMやUSIMとは独立しており、互いに非常に似た処理を行うが、実際には細かい点において違いがある。本節では、ISIMアプリケーションを用いたIMSアクセスについて記述する。UICCがUSIMだけを持っている場合の登録処理については、5.5.2項で説明する。

IMS登録処理では、必要となる次に挙げる各処理を2往復のメッセージ交換で実現している。

- ユーザがパブリックユーザIDをコンタクトアドレスにバインドする。：REGISTERリクエストの主目的。
- ホームネットワークがユーザを認証する。
- ユーザがホームネットワークを認証する。