

## 次世代 WAP(WAP 2.0)特集

## プロトコル技術

ドコモは、iモードの経験を踏まえ、インターネット標準との融合を図った次世代WAP (WAP 2.0) の標準化を WAP フォーラムに提案した。本提案は WAP フォーラム内で広く受け入れられ、WAP 2.0 が 2001 年 7 月に公開された。

本稿では、WAP2.0 のプロトコル技術について解説する。

いしかわ のりひろ	いなむら ひろし
石川 憲洋	稲村 浩
みうら ふみあき	うえの ひでとし
三浦 史光	上野 英俊

## 1. まえがき

携帯電話や PDA (Personal Digital Assistant) などから、ニュース、天気予報、モバイルバンキングなどのインターネット上のコンテンツにアクセスするサービスが非常に注目を集めている。WAP (Wireless Application Protocol) は、携帯電話などのモバイル端末からインターネットのコンテンツへのアクセスを実現することを主な目的に、WAP フォーラムで仕様開発が進められているプロトコルおよびアプリケーション環境である。WAP フォーラムは 1997 年 6 月に設立されて以来、世界の主要なオペレータ、メーカ、コンテンツプロバイダが参加し、2001 年 4 月時点で参加メンバー数は 600 社を超えている。

WAP フォーラムでは、一般に帯域が狭く遅延が大きい無線ネットワーク上で使用するために最適化された、WAP 1.X プロトコルを標準化した (最新仕様は 2000 年 6 月に公開された WAP 1.2.1)。WAP 1.X プロトコルは、低速、高遅延である第 2 世代の移動通信網では有効であった。しかし、2001 年 5 月からドコモが試験サービスを開始した次世代移動通信 (IMT-2000: International Mobile Telecommunications-2000) 方式のネットワークでは、開始時に最大 384kbit/s と、第 2 世代方式の約 40 倍の速度でサービスが提供される。第 3 世代方式などの高速無線ネットワークでは、WAP 1.X のように無線に最適化されたプロトコルではなく、TCP (Transmission Control Protocol) などの標準的なインターネットプロトコルでも十分な性能を得ることができる [1]。モバイルインターネットを発展させるためには、急速に進展するインターネット技術をタイムリーに取り込むこ

とが必要であり、そのためには、WAPとインターネット標準との、より一層の融合を図ることが望ましい。

以上を踏まえて、ドコモは、エリクソンなどの協力を得て、IETF (Internet Engineering Task Force) およびW3C (World Wide Web Consortium) で規定された標準に基づいて次世代WAP (WAP 2.0) の標準化を行うことをWAPフォーラムに提案した。本提案はWAPフォーラム内で広く受け入れられ、WAP 2.0仕様が2001年7月に公開された。

本稿では、WAP 2.0の protocols 技術について解説する。

## 2. WAP 2.0のアーキテクチャ

WAP 2.0のアーキテクチャは、WAP 1.Xと同様に、WAPクライアント、WAPゲートウェイ、オリジンサーバから構成される(図1)。WAPクライアントは、携帯電話などの小さい画面のモバイル端末である。WAPアーキテクチャは、基本的にインターネットのWWWアーキテクチャを無線ネットワーク向けに拡張したものであり、WAPゲートウェイが無線ネットワークとインターネットの間のゲートウェイの役割を果たしている。本アーキテクチャは、IMT-2000におけるiモードシステムのアーキテクチャとほぼ同じである。

WAPクライアントとWAPゲートウェイの間は、ワイヤレス向けTCPプロファイルを使用して通信する。ワイヤレス向けTCPプロファイルは、遅延が大きく誤り率が高い無線ネットワーク上で使用するために最適化されたプロトコルである。WAPゲートウェイとオリジンサーバの間は、TCP/IP (Internet Protocol), HTTP (HyperText Transfer Protocol) 1.1などの標準的なインターネットプロトコルを

使用して通信する。したがって、オリジンサーバとして既存のWWWサーバをそのまま使用することができる。

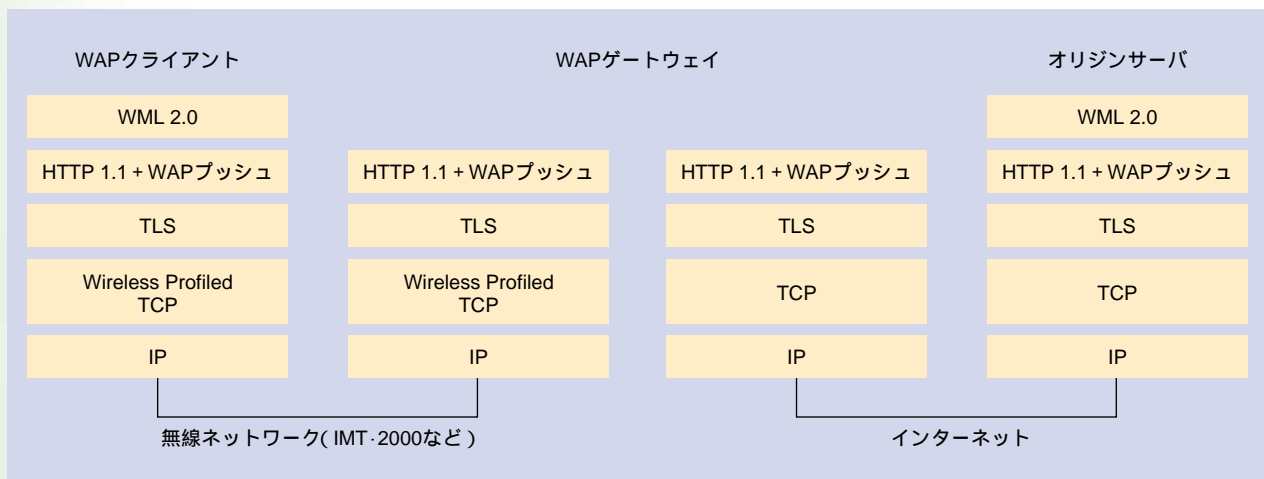
## 3. ワイヤレス向けTCPプロファイル

ワイヤレス向けTCPプロファイル (WAP仕様名: Wireless Profiled TCP) は、WAPクライアントとWAPゲートウェイの間で信頼性のあるバイトストリーム転送機能を提供している。ワイヤレス向けTCPプロファイルでは、遅延が大きく誤り率の高い無線ネットワークにTCPを適用するために以下の最適化を図っている。

### 3.1 無線ネットワークへのTCPの適用

TCPは、その開発の経緯からLAN (Local Area Network) のような高速、低遅延で誤り率の低いネットワークで利用され、発展してきた。したがって、無線区間を含む伝送路に対してTCPが適しているかどうかについて従来から議論があった。IMT-2000のような符号分割多元接続方式 (CDMA: Code Division Multiple Access) 技術に基づく第3世代方式におけるネットワークでは、無線区間再送方式 (ARQ: Automatic Repeat reQuest) や誤り訂正符号化 (FEC: Forward Error Correction) 方式の適用によってパケット誤り率を低く押さえることが可能である一方、その結果として生じる広い帯域幅に対する比較的長い遅延時間が問題になった。

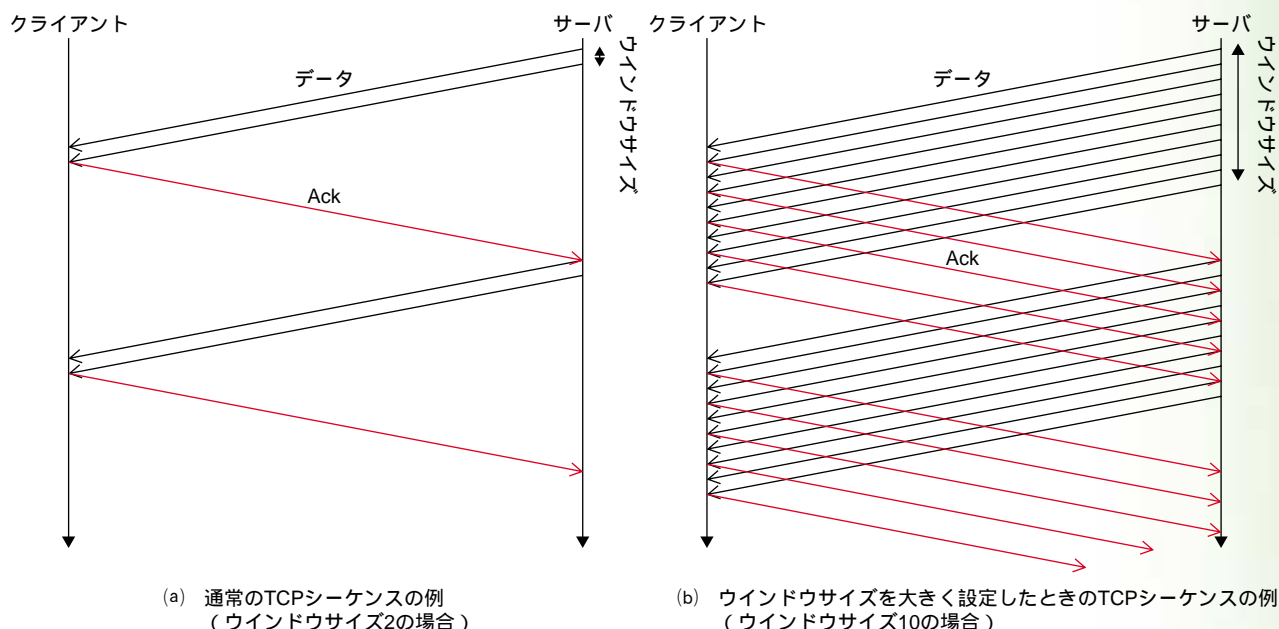
一例として、遅延時間によって生じる回線利用効率上の問題について説明する。図2は遅延の長いネットワークでのTCPの振舞いである。サーバからクライアントに向けてデータが転送され、クライアントはサーバに送達確認



HTTP: HyperText Transfer Protocol  
 IMT-2000: International Mobile Telecommunications-2000  
 (次世代移動通信)  
 IP: Internet Protocol

TCP: Transmission Control Protocol  
 TLS: Transport Layer Security  
 WAP: Wireless Application Protocol  
 WML: Wireless Markup Language

図1 WAP 2.0のアーキテクチャ



TCP : Transmission Control Protocol

図2 TCPシーケンス

(Ack)を送出している。クライアントでデータあふれを起さないために、サーバはAckを待たずに転送できるデータ量に上限値を設けている。この値は、TCP接続時にクライアントとサーバの間で行われる3ウェイハンドシェイクというネゴシエーションで交換される。この上限値をウィンドウサイズと呼ぶ。

図2(a)はウィンドウサイズが2の場合、図2(b)はウィンドウサイズが10の場合である。これらの図から、ウィンドウサイズを変化させるとサーバ・クライアント間の回線において転送間隔が変わり、その結果、回線の利用効率が異なることが分かる。すなわち、遅延時間が長いネットワークでTCPを利用すると回線利用効率の低下の可能性があるが、ウィンドウサイズというパラメータを適切に設定することで効率低下を回避できる。

TCPを無線ネットワークに適用する際に著者らが提案したアプローチは、インターネット標準準拠の観点からTCPそのものは変えず、その柔軟性を活かして適切なパラメータやオプションを定めることで問題解決を図ることである[2]。言い換えれば、既存のオプションの中から無線向けに有効なものを選択し、プロファイル化することである。これによって、通常のTCPとの相互接続性を確保することが可能となる。

### 3.2 プロファイル概要

ワイヤレス向けTCPプロファイルでは、通常のTCPに加えて以下の4つのオプションを採用する。

無線遅延を考慮してウィンドウサイズを適切に設定することで、回線利用効率を向上させる。

初期伝送流量を大きく（一般のTCP実装との比で1.5～2倍）設定することで、iモードのような小容量コンテンツを伝送するときの応答時間を向上させる。本機能は、RFC (Request for Comment) 2414 [3]で規定されている。

TCPは、自律的に回線帯域に適應する機能としてスロースタートを備えている。その適應速度の向上のため伝送するIPパケット長を長く（1500バイトなど）設定する。

パケットロスからの回復性能を向上させるため、選択再送機能 (Sack : Selective acknowledgement) を用いる。本機能は、RFC 2018 [4]で規定されている。

### 3.3 効果とサービス展開

IMT-2000におけるiモード端末には、本プロファイルが搭載されている。iモードコンテンツのWebページは、そのほとんどが数KB程度の小さなデータ容量であり、上記のによって通常のTCPに比べiモード接続時の応答時間が数秒程度短縮されている。mopera (Mobile OPERATION Radio Assistant) などのコンテンツサービスでは、最高384kbit/sの高速性を活かすためにやが有効である。moperaの利用者はラップトップPCを使う場合も多く、ラップトップPCの主要OSであるWindowsのTCPパラメータ設定変更によって上記プロファイルに適合させるツールが提供されて

いる。また、上記プロファイルはサーバOSなどで広く支持されることが望ましいため、IETFにて標準化活動を並行して行っている。

## 4. ワイヤレス向けHTTPプロファイル

ワイヤレス向けHTTPプロファイル（WAP仕様名：Wireless Profiled HTTP）は、WAPクライアントとWAPゲートウェイ間のリクエスト/レスポンス型通信を行うための機能を提供している。HTTP1.1 [5]をコア仕様として採用し、ワイヤレス向けHTTPプロファイルとして以下のように規定している。

### 4.1 使用するHTTPメソッド

WAPクライアントでは、コンテンツの取得のために必要なGET、POSTメソッドのサポートが必須であり、その他のメソッドのサポートはオプションである。

また、エンド・エンドセキュリティ（TLS（Transport Layer Security）を用いたHTTPトンネリング）を実現するために、WAPクライアントがTLSを実装する場合は、HTTPトンネリングを実現するために必要なCONNECTメソッドのサポートが必須となっている。

WAPゲートウェイでは、WAPクライアントとの相互接続性を確保するために、GET、HEAD、POST、CONNECTのメソッドのサポートが必須であり、その他のメソッドのサポートはオプションである。

### 4.2 HTTPレスポンスメッセージ中のコンテンツ圧縮

無線区間を流れるデータ量を削減することを目的に、HTTPレスポンスメッセージ中のコンテンツ圧縮機能がオプションとして定められている。WAPゲートウェイにてコンテンツ圧縮機能をサポートする場合には、可逆圧縮フォーマットであるdeflateエンコーディング[6]をサポートする必要がある。しかし、JPEG（Joint Photographic Experts Group）画像などのあらかじめ圧縮されているコンテンツに対しては、deflateエンコーディングによって大幅な圧縮効果が見込めないため、WAPゲートウェイにおいてdeflateエンコーディングのサポートは必須ではない。

## 5. ワイヤレス向けTLSプロファイル

ワイヤレス向けTLSプロファイル（WAP仕様名：WAP TLS Profile and Tunneling）は、TLS[7]をコア仕様として採用し、携帯電話に適用を図るために以下のプロファイルを規定している。

### 5.1 エンド・エンドセキュリティ

やりとりを行う2者だけで実現されるセキュリティをエンド・エンドセキュリティと呼ぶ。エンド・エンドセキュリティは、どこにどのような悪意の第3者がいてもセキュリティを確保できるメカニズムである。現代のセキュリティは、エンド・エンドで行うことが基本となっている。

### 5.2 TLSの機能

TLSは、通信を行うときに用いられるエンド・エンドセキュリティメカニズムの1つで、SSL（Secure Sockets Layer）[8]を改良し、標準化したものである。したがって、TLSはSSLと同様に以下の機能を備えている。

通信相手の認証

通信内容の秘匿

届いた情報が、送信元が送ったとおりであることの確認（改ざん防止）

TLSは、この3つの機能によって安心できる通信路を作り出すことができる。TLSはHTTPに使われることが多いが、その他のさまざまな用途にも使える。なお、TLSはSSLから無理なく移行できるように設計されている。

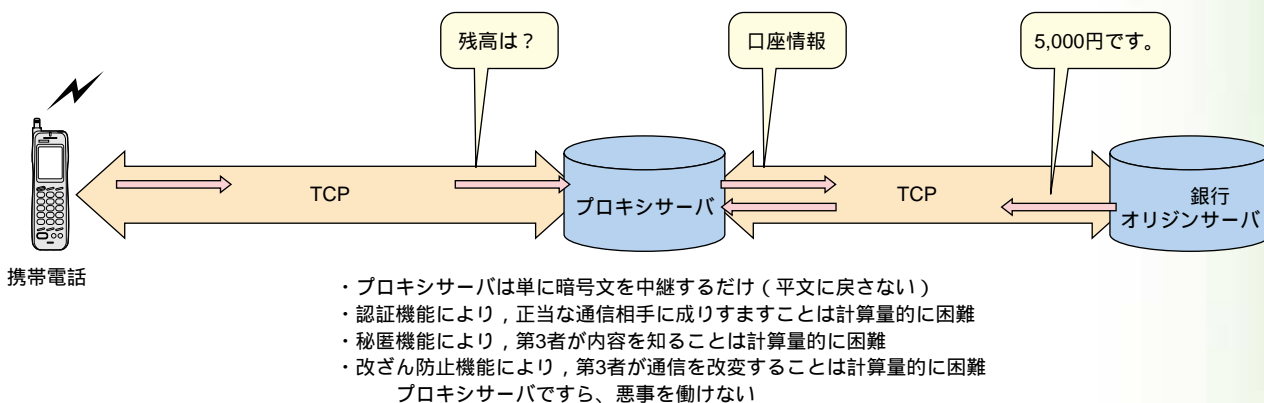
### 5.3 TLSの概要

TLSでの通信相手の認証には、公開鍵証明書を用いる。公開鍵には対応する秘密鍵が存在する。その秘密鍵を保持している者の情報を保証するのが公開鍵証明書である。電子証明書に含まれる電子署名は演算によって検証できるので、正しい証明書であることを確認できる。さらに、秘密鍵を保持していないと計算量的に困難な演算を要求し、正しい答えが返ったことを確認すれば、秘密鍵の所持していることが判明するので認証が完了したことになる。ここで述べた検証には公開鍵暗号を用いる。秘匿には対称鍵暗号を、改ざん防止には一方向性ハッシュ関数を用いる。

また、プロキシサーバ（WAPの場合はWAPゲートウェイ）を経由する場合でもエンド・エンドセキュリティが実現できる（図3）。プロキシサーバは通信の仲介をするが、通信内容の理解および改ざんは計算量的に不可能である。また、要求と異なるオリジンサーバに接続した場合は認証が成立しない。つまり、悪意のあるプロキシサーバにも対抗できる。

### 5.4 TLSのワイヤレス向けプロファイル

このように優れた性質を持つTLSであるが、実装するのは容易ではない。TLSの開設には電子証明書をデコードして内容を理解し、公開鍵暗号を使ったさまざまな演算を行



TCP : Transmission Control Protocol

図3 プロキシサーバを経由する場合のエンド・エンドセキュリティの利用例

う必要がある。また、対称鍵暗号の演算を高速に行わないと、通信速度が遅くなってしまふ。そこで、これらの実装にアセンブラを用いて性能を出すことが現在でも行われている。しかし、このような重い処理を、演算能力やメモリの制限が大きい携帯電話へ実装することは困難である。

この問題に対処するために、WAP フォーラムでは TLS のワイヤレス向けプロファイルを作成した。このプロファイルは、実装しなければならない機能をなるべく減らしてはいるものの、ほとんどの通信には支障がないように設計してある。一例を挙げると、TLS は認証などで用いる方式として DSA (Digital Signature Algorithm) や DH (Diffie Hellman) というほとんど使用されていない方式の実装を必須としているが、実際に利用されている方式は RSA (Rivest Shamir Adleman) が多い。この理由は、RSA の特許がすでに切れていることによる。本プロファイルではこの現状に対応し、必須として実装すべき方式として RSA のみが採用された。

## 6. WAP 2.0 プッシュ技術

WAP の特徴的な機能の 1 つとしてプッシュ機能がある。WAP プッシュでは、メール着信通知やコンテンツプッシュを実現するためのプッシュプロトコルが規定されている。

### 6.1 プッシュアーキテクチャ

WAP プッシュは、PI (Push Initiator)、PPG (Push Proxy Gateway)、WAP クライアントから構成される (図 4)。PI はプッシュコンテンツとプッシュ制御情報を PPG に送信し、PPG は、PI から送られてきたプッシュ制御情報を基に WAP クライアントに対しコンテンツをプッシュする。PPG は WAP クライアントへプッシュを行うために、無線ネットワークのアドレッシング方式に基づいてアドレス解決を行

うことを主な役割とする。その他にも、WAP クライアントの能力情報に応じたコンテンツ変換やプッシュの結果を PI に通知する機能も備える。

### 6.2 プッシュプロトコル

PI と PPG の間の通信には PAP (Push Access Protocol) が用いられ、PPG と WAP クライアントの間の通信には、PushOTA (Over The Air) プロトコルが用いられる (図 5)。

PAP は、プッシュ制御情報の転送と、任意の MIME コンテンツタイプのプッシュを行う。PAP のオペレーションには、プッシュの実行、プッシュのキャンセル、プッシュメッセージの置換、状態問い合わせ、PPG から PI へのプッシュ結果通知機能などがある。PAP の転送プロトコルとして、インターネット標準である HTTP または SMTP (Simple Mail Transfer Protocol) を使用する。

PushOTA には、コネクションレス型 (必須) とコネクション型 (オプション) がある。コネクションレス型プッシュのプロトコルとしては WAP 1.X の WSP (Wireless Session Protocol) が、コネクション型のプロトコルとしては HTTP がそれぞれ用いられる。

コネクションレス型プッシュでは、トランスポート層としてさまざまなベアラ上で動作する WAP 1.X の WDP (Wireless Datagram Protocol) を用いるため、GPRS (General Packet Radio Service) などの IP ベアラのほか、SMS (Short Message Service) などの非 IP ベアラ上におけるプッシュも実現可能である。

コネクション型プッシュでは、HTTP POST メソッドを用いたプッシュ機能を提供する。つまり PPG が HTTP クライアントとなり、WAP クライアントがコンパクト HTTP サーバとして動作する。

プッシュを行う際にあらかじめプッシュセッションおよ

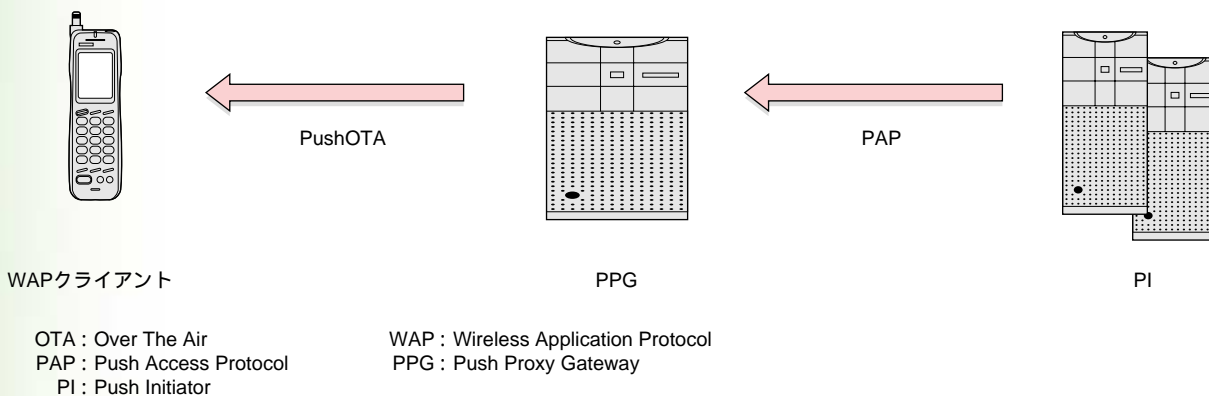


図4 WAP プッシュアーキテクチャ

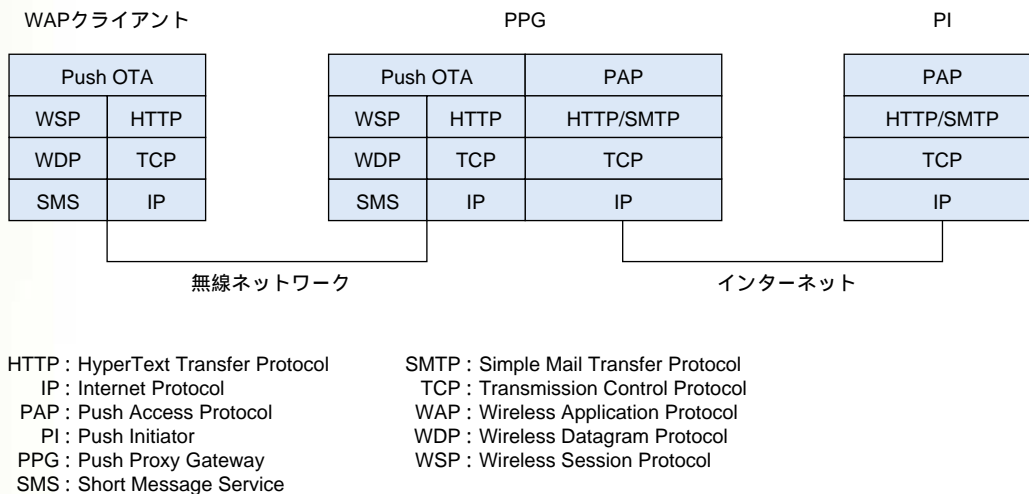


図5 WAP プッシュプロトコルスタック

びペアラが開設されていない場合には、ネットワーク側からこれらの開設をWAPクライアントに要求することが必要となる。このための仕組みとして、SIR (Session Initiation Request) が規定されている。SIRでは、SMSを用いてSIA (Session Initiation Application) メッセージをプッシュすることにより、ネットワーク側からプッシュセッションおよびペアラの開設をWAPクライアントに要求することができる。

### 6.3 スマートプル (擬似プッシュ)

WAPプッシュでは、スマートプル (擬似プッシュ) を実現するSI (Service Indication) とSL (Service Loading) を規定している。SLのプッシュを受けたWAPクライアントは、プル型によりそのURLで記述されたコンテンツの取得を行い、擬似的にプッシュを行うスマートプルを実現する。

### 6.4 プッシュ実現例

プッシュの実現例を以下に示す。なお説明中の番号は、図中の番号に対応している。

#### (1) SLを用いたスマートプルの例 (図6)

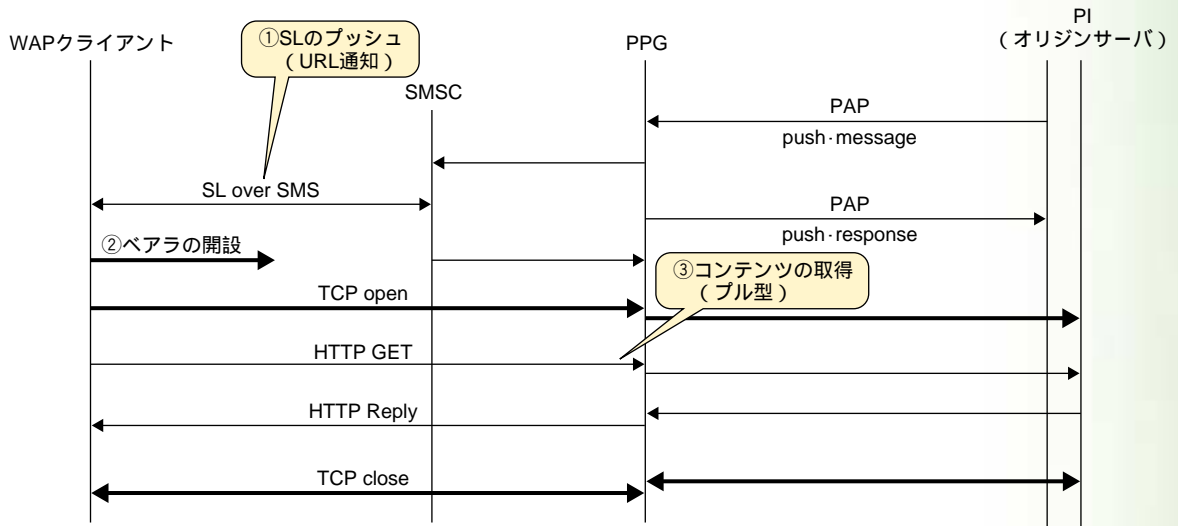
SMS上のコネクションレス型プッシュにてSLをプッシュし、WAPクライアントからペアラを開設後、プル型にてコンテンツを取得する。

#### (2) HTTPを用いたコンテンツプッシュの例 (図7)

SMS上のコネクションレス型プッシュにてSIAをプッシュし、WAPクライアントからペアラの開設およびプッシュセッション (TCPコネクション) の開設を行った後、HTTP POSTを用いたコンテンツプッシュを行う。その際PPGは、そのWAPクライアントから開設されたTCPコネクション上でプッシュする方式、またはPPGから新たにTCPコネクションを開設する方式のいずれかを選択する。

## 7. あとがき

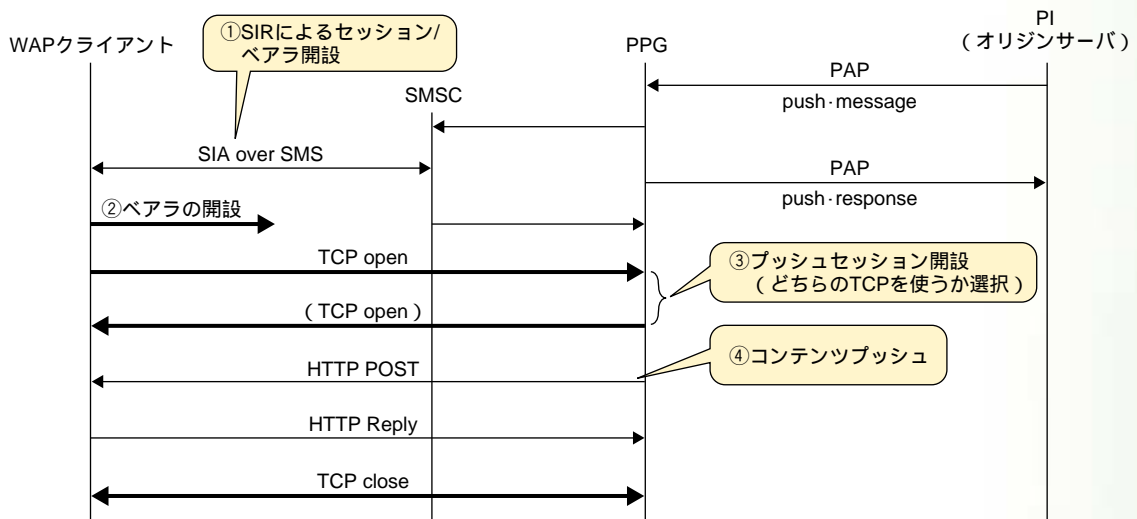
WAP 2.0のプロトコル技術について解説した。今後は、iモードなどのドコモが提供するサービスへのWAP 2.0の適用について検討を進める予定である。



HTTP : HyperText Transfer Protocol  
 PAP : Push Access Protocol  
 PI : Push Initiator  
 PPG : Push Proxy Gateway  
 SL : Service Loading

SMS : Short Message Service  
 SMSC : Short Message Service Center  
 TCP : Transmission Control Protocol  
 WAP : Wireless Application Protocol

図6 SLを用いたスマートプルの例



HTTP : HyperText Transfer Protocol  
 PAP : Push Access Protocol  
 PI : Push Initiator  
 PPG : Push Proxy Gateway  
 SIA : Session Initiation Application

SIR : Session Initiation Request  
 SMS : Short Message Service  
 SMSC : Short Message Service Center  
 TCP : Transmission Control Protocol  
 WAP : Wireless Application Protocol

図7 HTTP POSTを用いたコンテンツプッシュの例

文 献

[1] Ishikawa, et al. : “ Considerations on the Mobile Internet Architecture for High - Speed Wireless Networks ”, INET 2001 ( 2001 ).

[2] 石川, ほか : “ W - CDMA 向け TCP プロファイル ”, 情報処理学会 MBL/ITS 合同研究会報告 ( 2000 ).

[3] Allman, et al. : “ Increasing TCP’s Initial Window ”, RFC 2414 ( 1996 ).

[4] Mathis, et al. : “ TCP Selective Acknowledgement Options ”, RFC 2018 ( 1996 ).

[5] Fielding, et al. : “ Hypertext Transfer Protocol - HTTP/1.1 ”, RFC 2616 ( 1999 ).

[6] Deutsch : “ DEFLATE Compressed Data Format Specification Version 1.3 ”, RFC 1951 ( 1996 ).

[7] Dierks, et al. : “ The TLS Protocol Version 1.0 ”, RFC 2246 ( 1999 ).

[8] 大井, ほか : “ 高機能iモード携帯機特集, iモードにおけるセキュリティ - SSL (Secure Sockets Layer) - ”, 本誌, Vol.9, No.1, pp.22 - 26 Apr, 2001 .

## 用語一覧

ARQ : Automatic Repeat reQuest  
 CDMA : Code Division Multiple Access (符号分割多元接続方式)  
 DH : Diffie Hellman  
 DSA : Digital Signature Algorithm  
 FEC : Forward Error Correction (誤り訂正符号化)  
 GPRS : General Packet Radio Service  
 HTTP : HyperText Transfer Protocol  
 IETF : Internet Engineering Task Force  
 IMT - 2000 : International Mobile Telecommunications - 2000  
 (次世代移動通信)  
 IP : Internet Protocol  
 JPEG : Joint Photographic Experts Group  
 LAN : Local Area Network  
 mopera : Mobile OPEration Radio Assistant  
 OTA : Over The Air  
 PAP : Push Access Protocol  
 PDA : Personal Digital Assistant  
 PI : Push Initiator  
 PPG : Push Proxy Gateway

RFC : Request for Comment  
 RSA : Rivest Shamir Adleman  
 Sack : Selective acknowledgement (選択再送機能)  
 SI : Service Indication  
 SIA : Session Initiation Application  
 SIR : Session Initiation Request  
 SL : Service Loading  
 SMS : Short Message Service  
 SMSC : Short Message Service Center  
 SMTP : Simple Mail Transfer Protocol  
 SSL : Secure Sockets Layer  
 TCP : Transmission Control Protocol  
 TLS : Transport Layer Security  
 W3C : World Wide Web Consortium  
 WAP : Wireless Application Protocol  
 WDP : Wireless Datagram Protocol  
 WML : Wireless Markup Language  
 WSP : Wireless Session Protocol