ネットワークアクセス認証プロトコル PANA

Protocol for Carrying Authentication for Network Access (PANA)

大場　義洋　　勝部　泰弘

■OHBA Yoshihiro　■KATSUBE Yasuhiro

ユーザーがネットワークに接続する場合には，ユーザーとネットワークの間でユーザー認証のためのネットワークアクセス認証プロトコルが使用される。

東芝は，次世代のネットワークアクセス認証プロトコルであるPANA（Protocol for carrying Authentication for Network Access）の研究開発を，IETF（Internet Engineering Task Force）での標準化，及びPANAプロトコルソフトウェアのオープンソース形態の開発を主体として行ってきた。これらの活動により，ネットワークアクセスを安全に行うための要素技術の普及に貢献している。

A network access authentication protocol is required before a user connects to a secure network.

Toshiba's research and development activities in this area are focused on the Protocol for carrying Authentication for Network Access (PANA), which is a next-generation network access authentication protocol. These activities are based on standardization of the PANA protocol by the Internet Engineering Task Force (IETF) and open-source development of PANA protocol software to contribute to deployment of the fundamental technologies required for providing secure network access.

1 まえがき

ユーザーがインターネットやイントラネットに接続するときは，通常，ユーザー名とパスワードを入力するなどの認証手続きが必要となる。このような接続の例として，ダイヤルアップ接続，無線LAN接続などがある。ネットワークアクセス時に実行される，ユーザー（以下，クライアントという）とクライアントを認証するネットワーク内のエンティティ（以下，認証エージェントという）との間の認証をネットワークアクセス認証（以下，アクセス認証という）と呼ぶ。

従来のアクセス認証プロトコルは，一部の例外を除き，データリンク層で定義されてきたが，DSL（Digital Subscriber Line），無線LAN，携帯電話などの様々なネットワークの普及に伴い，その問題点が顕著化している。これに対し，東芝は，次世代のアクセス認証プロトコルである，PANA（Protocol for carrying Authentication for Network Access）の研究開発を，IETF（Internet Engineering Task Force）でのプロトコル標準化，及びPANAプロトコルソフトウェアのオープンソース形態の開発を主体に進めてきた。

ここでは，従来のアクセス認証プロトコルの問題点，PANAの概要，及びオープンソースのPANA実装について述べる。

2 従来のアクセス認証プロトコルの問題点

従来のアクセス認証プロトコルは，無線LANホットスポット接続などで使用されている，HTTP（HyperText Transfer Protocol）を用いたアプリケーション層での認証を除き，データリンク層で定義されている。PPP（Point-to-Point Protocol）[(1)]の認証フェーズや，IEEE 802（米国電気電子技術者協会規格802）で規定されたLAN用にポートアクセス制御を定義した802.1X[(2)]がその一例である。

近年のアクセス認証プロトコルに必要とされる機能として，EAP（Extensible Authentication Protocol）[(3)]がある。EAPは，パスワード認証やデジタル証明書認証など，様々な認証メソッドに対応する認証プロトコルである。

アクセス認証プロトコルがEAPメッセージを運ぶことにより，アクセス認証プロトコルと認証メソッドを分離して扱うことができ，その結果，認証メソッドの追加や変更が容易にできる。PPPの認証フェーズやIEEE 802.1XはEAPをサポートするが，これらの既存のアクセス認証プロトコルはデータリンク層で定義されるため，データリンクプロトコルの多様性に対応するのが難しい。

特に，DSLのように，プロバイダーやベンダーによって，Ethernetであったり，PPP over Ethernetであったりなど，データリンク層の構成がまちまちなアクセスネットワークでこの問題が顕著になっている。こうした問題に加え，様々な無線インタフェースを持つ端末が普及しつつある現在，多様な

データリンク層に対応し，かつEAPをサポートするアクセス認証プロトコルの必要性が高まっている。

3 PANAの概要

先に述べたような従来のアクセス認証プロトコルの問題を解決するために，ネットワーク層で動作する新しいアクセス認証プロトコルを標準化するためのワーキンググループ（WG）がIETFに2001年12月に設立された。その標準化対象となるプロトコルがPANA[(4)]であり，現在，東芝，サムスン電子社，ノキア社，シーメンス社が主体となってIETFのPANA WGで標準化が進められている。

PANAはUDP/IP（User Datagram Protocol/Internet Protocol）の上でEAPメッセージを運ぶ，クライアント／サーバ型のアクセス認証プロトコルである。PANAのクライアント及びサーバを，それぞれ，PaC（PANA Client）及びPAA（PANA Authentication Agent）と呼ぶ。PANAのプロトコルスタックを**図1**に示す。

認証メソッドをPAAとは別の認証サーバ上に実装することもできる。この場合，PAAはPaCと認証サーバとの間でEAPメッセージを中継する。PAAと認証サーバとの間のEAPメッセージ転送には，RADIUS（Remote Authentication Dial-In User Service）[(5)]やDiameter[(6)]などのAAA（Authentication, Authorization and Accounting）プロトコルを使用する（**図2**）。

PANAのメッセージ交換にはかかわらないがPANAと密接な関連を持つ重要な機能要素として，EP（Enforcement Point）がある（**図3**）。EPは，PANAを用いて認証されたPaCについて，パケット単位のアクセス制御を実行する機能要素であり，EPの機能を持つ機器の例として無線LANアクセスポイントやアクセスルータがある。EPへのアクセス制御パラメータの設定はPAAが行う。EPはまた，PaCの存在を検出しPAAに通知するPaCプレゼンス通知機能も持つ。これにより，PaCからPAAに対してだけでなく，PAAからPaCに対してもPANA認証を起動でき，その結果，そのネットワークで認証が必要かどうかをクライアントはあらかじめ知っておく必要がない。PAAとEPは同一の機器にも異なる機器にも実装することができる。後者の場合には，PAAはSNMP（Simple Network Management Protocol）を用いてEPと通信する。

EPが暗号化と認証を伴うパケット単位のアクセス制御を行う場合（この場合PaCとEPの間でパケットの暗号化と認証が行われる）には，PaCとEPとの間でSecure Association Protocolと呼ばれる，パケットの暗号化と認証を行うために必要な暗号鍵などのパラメータを設定するための鍵交換プロトコルが実行される。パケットの暗号化と認証にIPsec（IPセキュリティ）を用いる場合にはIKE（Internet Key Exchange）[(7)]を，また，IEEE 802.11i[(8)]を用いる場合に

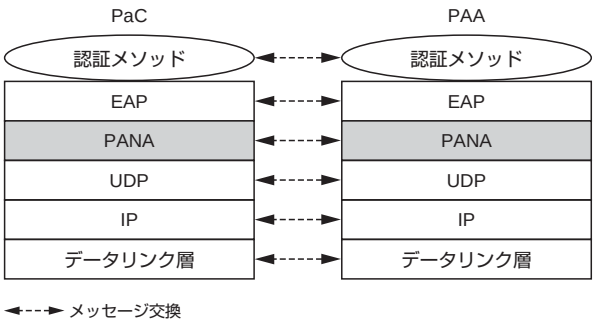


図1．PANAのプロトコルスタック — PANAはUDP/IPの上でEAPメッセージを運ぶ。

Protocol stack of PANA

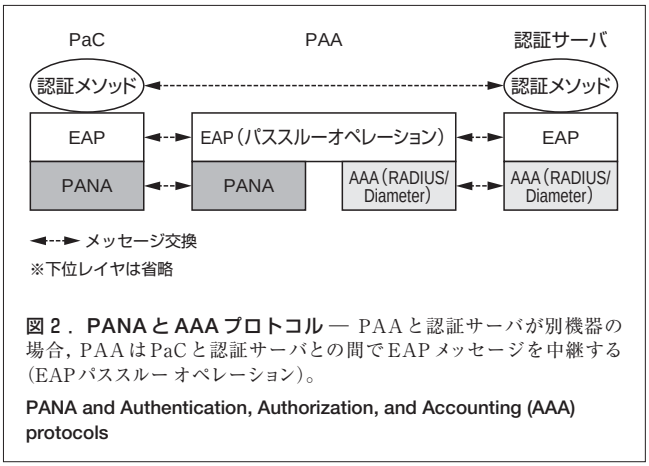


図2．PANAとAAAプロトコル — PAAと認証サーバが別機器の場合，PAAはPaCと認証サーバとの間でEAPメッセージを中継する（EAPパススルー オペレーション）。

PANA and Authentication, Authorization, and Accounting (AAA) protocols

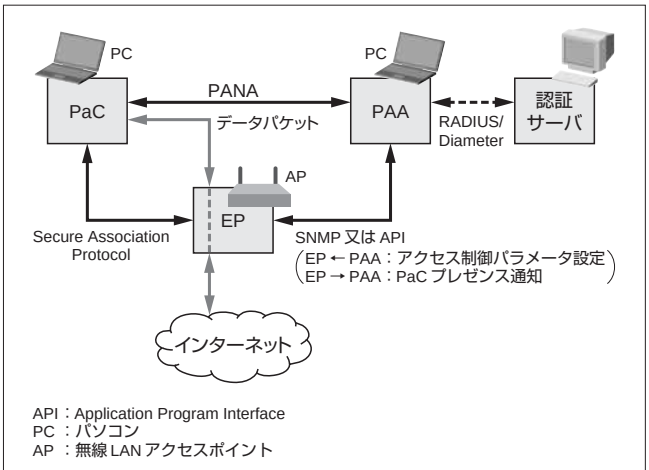


図3．PANAモデル — PAAはPaCの認証結果に応じて，パケットフィルタリング情報をEP（この場合，無線LANアクセスポイント）に動的に設定する。

PANA model

はIEEE 802.11iの4ウェイハンドシェイク手順を，Secure Association Protocolとしてそれぞれ使用する。後者は無線LANアクセスポイントがEPの場合に必要となる。

3.1 特長

PANAの特長は，従来のアクセス認証プロトコルでは実現できなかった，次に示すようなフレキシビリティにある。

⑴ 対象データリンクのフレキシビリティ　任意のデータリンクプロトコル上でEAPを用いたアクセス認証を一元的に行える。

⑵ サービスのフレキシビリティ　従来のアクセス認証プロトコルでは実現が困難であった新しいサービスを提供できる。例えば，複数のISP（Internet Service Provider）から一つのISPを選択することができる。

⑶ 管理のフレキシビリティ　PANAにより，無線LANアクセスポイントと認証エージェントを物理的に分離することができる。その結果，例えば，IT（情報技術）部門は認証エージェントだけを管理し，追加や置換えが比較的頻繁に起こりえる無線LANアクセスポイントは各部署で管理する，といった管理の切分けが可能になり，IT部門のネットワーク管理の負担を軽減することができる。

3.2 動作

PANAはUDP/IPの上で定義されるため，PaCはPANAを起動する前に何らかのIPアドレスを取得する必要がある。このIPアドレスをPRPA（Pre-PANA Address）と呼ぶ。PRPAとしてIPv6（version 6）ではリンクローカルアドレスが使用され，IPv4ではリンクローカルアドレス，プライベートアドレス，グローバルアドレスのいずれも使用できる。PANAが動作するためにデータリンク層に最低限必要なことは，アクセスをまだ承認されていないPaCに対し，DHCP（Dynamic Host Configuration Protocol）などのPRPAを取得するためのプロトコルメッセージ及びPANAのメッセージを，EPでフィルタリングしないように設定しておくことである。

PANAのプロトコルシーケンスは，次の五つのフェーズから成り，それぞれフェーズは**図4**に示すタイミングで実行される。

⑴ Discovery and handshake phase　PaC（又はPAA）がPAA（又はPaC）に対してPANA認証を起動する。3.1節で述べたISPの選択もこのフェーズで行われる。

⑵ Authentication and authorization phase　EAPメッセージがPaCとPAAとの間でやり取りされる。EAPの認証結果に基づいてPaCのアクセスが承認されると，承認されたアクセス制御パラメータがEPに設定されるとともに，PANAセッションと呼ばれる論理コネクションがPaCとPAAの間に確立する。認証メソッドが認証機能に加え，EAPの二つのエンドポイント間で一時的に共有される鍵（セッション鍵）を生成する機能を持つ場合，セッション鍵を用いて，PANAプロトコル自身のセキュリティに関するPaCとPAAの間の関係（セキュリティ アソシエーション）も確立される。セキュリティ アソシエーション確立後に交換されるPANAメッセージには認証情報が付加され，攻撃者によるPANAメッセージの改ざんを防止することができる。

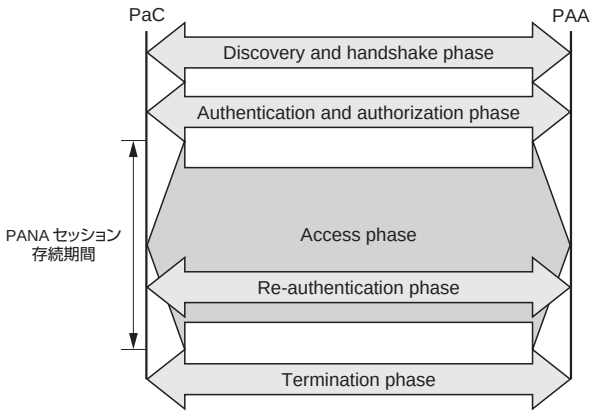


図4．PANAのプロトコルシーケンス ― PANAは，5フェーズから成るプロトコルである。
Protocol sequence of PANA

⑶ Access phase　Authentication and authorization phaseにおいて確立されたPANAセッションは，このフェーズにおいてPaCのアクセスが承認されている間維持され，PaCはEPを通してネットワークとの間のデータパケットのやり取りができる。

⑷ Re-authentication phase　このフェーズにおいて，確立されたPANAセッションの存続期間延長のための再認証が行われる。

⑸ Termination phase　PANAセッションを終了する。PANAセッションが終了すると，これまで承認されていたPaCに対するアクセス制御パラメータがEPから削除される。

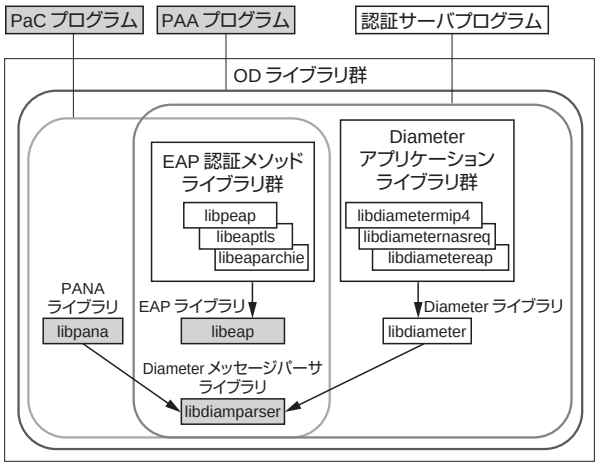
4 PANAのオープンソース実装

PANAの実装はいくつかのベンダーで既に行われている。当社のPANA実装は，OD（Open Diameter）[9]というプロジェクトで行われており，ODのPANAソースコードは無償で公開される。ODが提供するソフトウェアにはPANAだけでなく，EAPやDiameterなど，PANAに密接に関連するプロトコルの実装も含まれる。現在，日本，米国，欧州をはじめ

とする数多くのプロバイダーやベンダー，及び大学が，新しいセキュアネットワークのプロトタイプを構築するツールとしてODのソフトウェアを使用している。

ODのソースコードは，プログラミング言語C++で記述されており，GPL（GNU Public License）及びLGPL（Lesser GPL）の複合ライセンスの下で提供される。ODのソフトウェアアーキテクチャは，オペレーティングシステム（OS）への依存性を最小限に抑えるように設計されており，Linux(注1)，FreeBSD，Windows® 2000/XP(注2)のOSをサポートする。

ODのソフトウェア構成を**図5**に示す。ODソフトウェアは，ライブラリ群と，このライブラリ群を用いて実装された三つのアプリケーションプログラム（PaCプログラム，PAAプログラム，認証サーバプログラム）で構成される。PaCプログラムとPAAプログラムが，それぞれPaCとPAAの機能を実現する。認証サーバ（図2）を用いて認証を行う場合には，認証サーバプログラムも必要となる。これらのアプリケーションプログラムは起動時に，XML（eXtensible Markup Language）形式の設定ファイルから設定パラメータを読み込む。



A→B：AはBに依存していることを表す。

図5．Open Diameterソフトウェアの構成 ― 網掛けされたライブラリ及びアプリケーションプログラムがPANAの動作環境に必須である。

Open Diameter software components

5 あとがき

当社は，次世代ネットワークアクセス認証プロトコルであるPANAの研究開発を，IETFでの標準化，及びオープンソース形態のソースコード開発を主体に行ってきた。PANAは，既存のアクセス認証プロトコルでは困難であった，データリンクプロトコルの多様性に対応可能であり，PANAを用いることでISP選択などの新しいサービスを提供することができ，ネットワーク管理のコストを低減できる。

PANAは，現在，米国の携帯電話網の標準化団体である3GPP2（3rd Generation Partnership Project 2）の次期規格のアクセス認証プロトコルとして提案されている。DSLの標準化団体であるDSL Forumも，次世代DSLのアクセス認証プロトコルとしてPANAに注目している。また，PANAの今後の展開として，検疫ネットワークへの適用や，無線LANシステムにおけるセキュアシームレス ハンドオーバの実現にPANAを使用することなど，幅広い応用が期待される。

(注1) Linuxは，Linus Torvalds氏の米国及びその他の国における登録商標。

(注2) Windows2000及びWindowsXPは，米国Microsoft Corporationの米国及びその他の国における登録商標。

文 献

(1) Simpson, W.“The Point-to-Point Protocol（PPP）”. STD 0051, RFC 1661, July 1994.

(2) The IEEE LAN MAN Standards Committee.“Standard for Port based Network Access Control”. Std 802.1X-2001, 2001.

(3) Aboba, B., et al.“Extensible Authentication Protocol（EAP）”. RFC 3748, June 2004.

(4) Forsberg, D., Ohba, Y., et al.“Protocol for Carrying Authentication for Network Access（PANA）”. Internet-Draft, work in progress, 2005.

(5) Rigney, C., Simpson, W., et al.“Remote Authentication Dial In User Service（RADIUS）”. RFC 2865, June 2000.

(6) Calhoun, P., Loughney, J., et al.“Diameter Base Protocol”. RFC 3588, September 2003.

(7) Harkins, D. and Carrel, D.“The Internet Key Exchange（IKE）”. RFC 2409, November 1998.

(8) The IEEE LAN MAN Standards Committee.“Draft supplement to standard for wireless MAC and PHY specifications, specification for enhanced security”. IEEE 802.11i/D10.0, 2004.

(9) Open Diameter Project（accessed 2005-3-28）. <http://www.opendiameter.org/>.

大場 義洋 OHBA Yoshihiro, Ph.D.

東芝アメリカ研究所リサーチディレクター，工博。
ネットワークセキュリティ プロトコルの研究・開発に従事。
IEEE会員。
Toshiba America Research, Inc.

勝部 泰弘 KATSUBE Yasuhiro

研究開発センター 通信プラットホームラボラトリー主任研究員。
ラボラトリーの研究管理全般，及びグローバルR&D連携支援に従事。IEEE，電子情報通信学会会員。
Communication Platform Lab.