第 VIII 部

AAA アーキテクチャの検討および AAA 基盤の構築

第 8 部
AAA アーキテクチャの検討および AAA 基盤の構築

AAA（Authentication, Authorization, and Accounting）WG は 2009 年 1 月に設立された新しいワーキンググループである。2009 年は 3 月と 9 月の合宿においてそれぞれ 1 回ずつ BoF を開催した。

第 1 章　AAA WG 設立の背景

ユーザがネットワークからサービスを受ける際、サービス提供者はそのユーザが正当なユーザであるかを確認（authentication: 認証）し、そのユーザが正当なユーザであることが確認できた場合はそのユーザがサービスを受ける権利があるかを確認して権利を委譲（authorization: 権限委譲）し、そのユーザによるサービスの利用状況を記録（accounting: 利用履歴記録）する必要がある。これら一連の処理を、Authentication, Authorization, and Accounting の頭文字を取って AAA（“トリプルエー” と発音）と呼ぶ。AAA 処理に必要となる情報を “AAA 情報” と呼び、AAA 情報を運搬するためのプロトコルを “AAA プロトコル” と呼ぶこととする。

以下、最も基本的なネットワークサービスであるネットワークアクセスを例として挙げる。ユーザは通常 1 つのインターネットサービスプロバイダ（ISP: Internet Service Provider）と契約していると考えられる。このようなプロバイダを “ホームプロバイダ” と呼ぶこととする。ユーザがホームプロバイダを介してインターネットに接続しようとすると、ホームプロバイダはユーザを認証し、ユーザの権限を確認して接続を許可する。ホームプロバイダは当然ユーザの契約情報を保持していると考えられるので、ホームプロバイダはユーザの契約情報にアクセスすることにより、認証処理や権限確認処理を問題なく行うことができる。このような環境で使用される AAA プロトコルとしては、IEEE802.1X[49] + RADIUS（Remote Authentication Dial In User Service）[84] + EAP（Extensible Authentication Protocol）[4] が広く利用されている（図 1.1 参照）。IEEE802.1X は無線 LAN（IEEE802.11）や Ethernet で利用される AAA プロトコルであり、通常はユーザの端末機器と無線 LAN のアクセスポイント間で動作する。RADIUS はアクセスポイントと認証サーバ間で動作するプロトコルであり、UDP 上で動作する。IEEE802.1X も RADIUS も AAA 情報を運搬するためのプロトコルであり、具体的な認証処理は EAP によって行われる。さらに EAP はさまざまな認証方式（EAP methods）をサポートしている。たとえば証明書を用いる EAP-TLS[87] や事前共有鍵を用いる EAP-GPSK（Generalized Pre-Shared Key）[22] などが標準化されている。以上のように、IEEE802.1X + RADIUS + EAP のシステムでは、ユーザの端末機器と認証サーバ間で合意された EAP method のメッセージが IEEE802.1X と RADIUS によって交換され、AAA 処理が行われる。なお、端末機器とアクセスポイント（あるいはアクセスルータ）間の部分を AAA プロトコルにおける “フロン

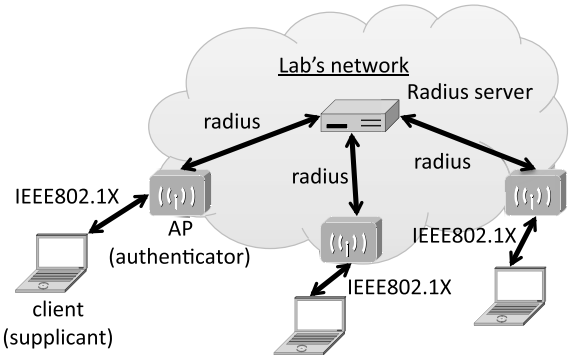

図 1.1.　IEEE802.1X + RADIUS + EAP によるシングル管理ドメインにおける AAA 環境

トエンド” と呼び、アクセスポイント（またはアクセスルータ）と認証サーバ間の部分を “バックエンド” と呼ぶこともある。すなわち、IEEE802.1X はフロントエンド用のプロトコルであり、RADIUS はバックエンド用のプロトコルである。

次にプロバイダ間のローミング契約を考える。ローミング契約とは、あるプロバイダのユーザは、そのプロバイダとローミング契約を結んでいる他のプロバイダにおいてもインターネット接続が許可されるという契約である。ユーザにとってホームプロバイダとローミング契約を結んでいるプロバイダを “訪問先プロバイダ” と呼ぶこととする。ユーザが訪問先プロバイダを介してインターネットに接続しようとしたとき、訪問先プロバイダはそのユーザの契約情報を保持していないため、そのユーザの認証や権限確認を直接行うことはできず、そのユーザのホームプロバイダに問い合わせる必要がある。このような問い合わせは信頼性を保証しかつセキュアに行われなければならない。また、複数のプロバイダ間でローミング契約を結ぶ場合を考えると、プロバイダを越えた AAA 情報の運搬のために標準となるプロトコルが必要となる。すなわち、マルチ管理ドメイン環境において AAA 情報を転送するための標準 AAA プロトコルが必要となると言える。

しかし、マルチ管理ドメイン環境における AAA プロトコルという観点からは IEEE802.1X と RADIUS には以下のような問題点がある。まず IEEE802.1X は IEEE802.11 や Ethernet という特定のリンク層に依存しているため、汎用的ではない。RADIUS は元々シングル管理ドメイン環境における AAA プロトコルとして設計されている。RADIUS を拡張してマルチ管理ドメイン環境に適用させる活動も行われているが、RADIUS は UDP 上で動作するためメッセージの信頼性のある転送は RADIUS 自体で実現しなければならない、RADIUS には failover 機能が定義されていない、サーバ側からの処理の起動ができない、などの問題点がある。

そこで RADIUS の後継となる AAA のバックエンド用プロトコルとして Diameter Base Protocol[19] が標準化された。Diameter は最初からマルチ管理ドメインでの運用を目指して設計されており、RADIUS と比較すると failover 機能が組み込まれている、トランスポートレベルでのメッセージ転送の信頼性やセキュリティを保証している、サーバ側からの処理の起動が可能である、さまざまな機能をもつ agent が導入されている、などの利点を有する。Diameter Base Protocol は拡張性を考慮して設計されており、さまざまなアプリケーションに対応できるようになっている。たとえば EAP を利用した認証のためには Diameter EAP Application[30] が標準化されている。

さらに IEEE802.1X の後継となる AAA のフロントエンド用プロトコルとして PANA（Protocol for Carrying Authentication for Network Access）[32]

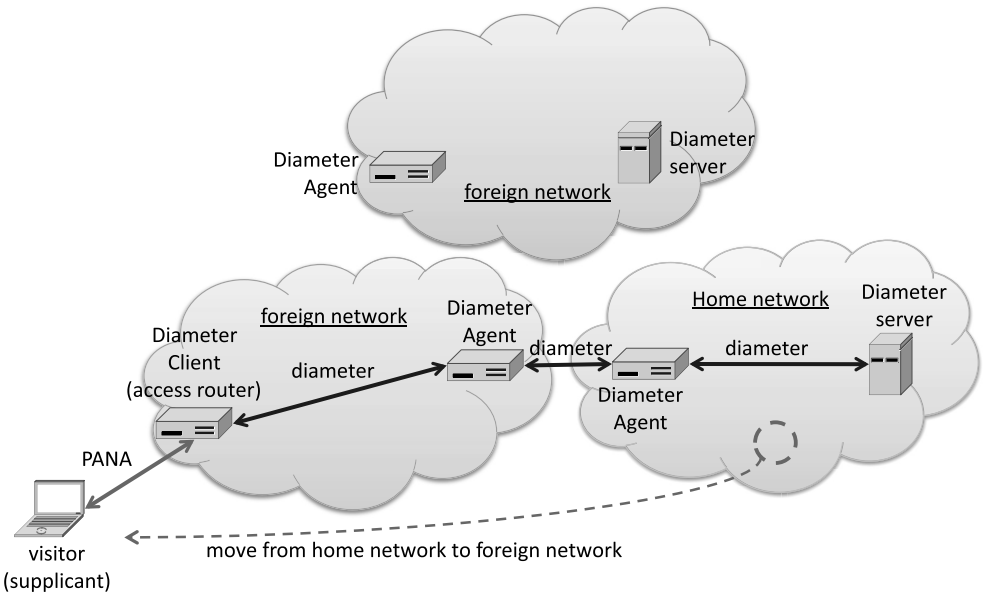

図 1.2.　PANA + Diameter + EAP によるマルチ管理ドメインにおける AAA 環境

が標準化された。PANA + Diameter + EAP によるマルチ管理ドメインにおける AAA 環境を図 1.2 に示す。

第 2 章　AAA WG の活動目標

AAA WG の目標は WIDE インターネット上に AAA 基盤を構築することである。すなわち、ネットワークアクセスに限らずさまざまなネットワークサービスにおいて、サービス提供者およびサービス利用者が安心してサービスを提供/利用できるようにするための汎用 AAA 基盤を構築することである。そのために、以下のようなマイルストーンを設定した。

1. WIDE インターネット上に Diameter を利用した AAA 基盤を構築する。
2. 上記の AAA 基盤を基にして、IETF で標準化されている AAA アーキテクチャや AAA プロトコルが将来のネットワークにとって妥当なものであるかを評価する。
3. もし、Diameter をベースとした IETF の AAA アーキテクチャが不適当であると判断された場合は、新たな AAA アーキテクチャを提案する。

マイルストーン 1 のために、NICT の Sebastien Decugis が Diameter Base Protocol を実装している。この実装は freeDiameter と呼ばれている [33]。さらに他のメンバーが freeDiameter 上への Diameter EAP Application の実装を進めている。なお、フロントエンド用のプロトコルとしては、PANA ではなく引き続き IEEE802.1X + RADIUS を利用する予定である (図 2.1 参照)。IEEE802.1X を利用する理由は、現在多くのオペレーティングシステムに IEEE802.1X が実装されているため、ユーザの機器がそのまま使えるためである。また、RADIUS をフロントエンドの一部として利用する理由は、市販の多くのアクセスポイントが IEEE802.1X と RADIUS の変換機能を有しているためである。IEEE802.1X + RADIUS をフロントエンドとして利用するため、我々は Diameter Agent として RADIUS/Diameter gateway を実装している。図 2.1 に示すように、この方法であればユーザの機器やアクセスポイントを変更することなく、バックエンドに RADIUS/Diameter gateway、Diameter Agent、Diameter Server を設置することによって実験を行うことができる。

マイルストーン 2 のためには、さまざまな Diameter Application を実装し、また WIDE メンバーにも参加してもらって実験を行う必要がある。最初に予定している実験は、Diameter EAP Application を利用したネットワークアクセスの際の AAA 処理である。2010 年 3 月あるいは 9 月の WIDE 合宿において、合宿ネットワークに接続する際の AAA 処理を実験として行いたいと思っている。さらにこの方式

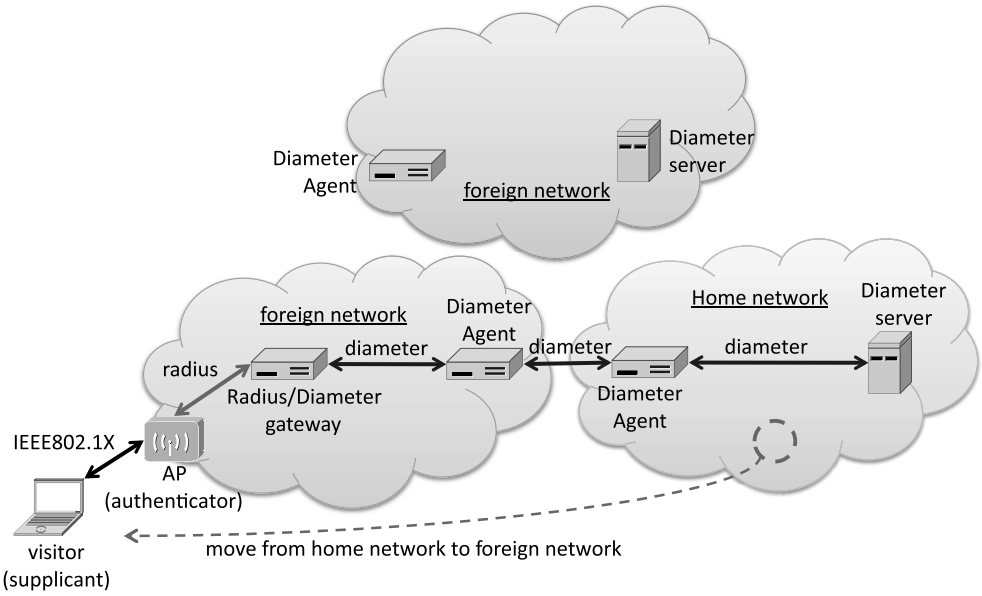

図 2.1.　RADIUS/Diameter Gateway を導入した環境

を通常の WIDE インターネット上でも利用できるように整備していきたいと思っている。以上のような実験を通じて Diameter に基づく IETF の AAA アーキテクチャが将来のネットワークに適しているかを評価したい。

マイルストーン 3 であるが、今までのサーベイや freeDiameter の実装からは、Diameter というプロトコルは複雑すぎるのではないかという感覚を得ている。たとえば、メッセージのトランスポート機能と AAA 機能を分離した方がいいのではないかという意見もある。

第 3 章　おわりに

ネットワークにおける攻撃をいかにして防御するか、また攻撃元をいかにして検知するか、などの研究は盛んであるが、ネットワークを介したサービスを安心・安全に使用するための研究はあまり注目を集めていないようである。しかしネットワークを介したサービスを提供したり利用したりする場合、特に商用の場合は認証、権限委譲、利用履歴記録という AAA 処理は非常に重要な機能となる。AAA WG はこの点に注目し、将来のネットワークのための汎用的な AAA 基盤を構築することを目標として活動を続けていきたい。