

第 IX 部

AAA アーキテクチャの検討および AAA 基盤の構築

第9部

AAA アーキテクチャの検討および AAA 基盤の構築

第1章 AAA WG 2010 年度の活動

ユーザがネットワークからサービスを受けるとき、サービス提供者はユーザを認証 (authentication) し、権限を委譲 (authorization) し、資源の利用状況を記録 (accounting) する。これらの機能をまとめて AAA と呼ぶ。AAA WG は Diameter による AAA 基盤を WIDE インターネットに構築し、Diameter が AAA アーキテクチャとして相応しいかを検証し、さらに将来のネットワークにおける AAA アーキテクチャはどうあるべきかを検討することを目的とする。今年度の主な活動内容は以下のとおりである。

- Diameter Base Protocol の実装と配布 (freeDiameter)
- Diameter EAP Application の実装と配布 (DiamEAP)
- 2010 年 9 月の WIDE 合宿での運用実験

第2章 Diameter Base Protocol の実装と配布

Diameter Base Protocol [RFC 3588] に完全に準拠した世界最初のオープンソースである freeDiameter を実装し、公開した。Diameter Base Protocol は Diameter ノード間で AAA 情報を安全かつ信頼性をもって配送するプロトコルである。現在、AAA プロトコルとしては RADIUS [RFC 2865] が広く使用されているが、マルチドメインのサポート、信頼性を持ったメッセージ配信、耐故障性、拡張性などに問題がある。Diameter Base Protocol は RADIUS の後継プロトコルとして設計され、これらの問題点を解決している。Diameter Base Protocol は AAA 情報を配送するプロトコルであり、具体的な機能は個別の Diameter Application として定義されている。たと

えば、ネットワークアクセス制御のための Diameter EAP Application [RFC 4072]、SIP ユーザの認証や権限委譲のための Diameter SIP Application [RFC 4740] などが定義されている。freeDiameter はさまざまな Diameter Application を plug-in として動的に組み込めるように設計されている。freeDiameter は以下の URL から入手可能である。

<http://www.freedometer.net/>

第3章 Diameter EAP Application の実装と配布

Diameter EAP Application [RFC 4072] の世界最初のオープンソースである DiamEAP を実装し、公開した。Diameter EAP Application はネットワークアクセス制御を目的とした Diameter Application であり、認証プロトコルである EAP [RFC 3748] を Diameter Base Protocol で運搬するためのプロトコルである。EAP 自体には認証機能はなく、具体的な認証機能は EAP methods として EAP 上に実装される。DiamEAP は EAP methods として EAP-TLS [RFC 5216] と EAP-MD5 を含んでいる。EAP-TLS は X.509 証明書 (certificate) を利用した認証方式であり、強固な認証機能を提供する。また、DiamEAP 自体はさまざまな EAP method を plug-in として動的に組み込めるように設計されている。DiamEAP は以下の URL から入手可能である。

<http://diameap.yagami.freedometer.net/>
DiamEAP の詳細については、文献 [14] を参照のこと。

第4章 2010 年 9 月の WIDE 合宿での運用実験

2010 年 9 月の WIDE 合宿において、freeDiameter と DiamEAP を用いた WiFi アクセス制御の運用実

WiFi Access Control by Diameter and EAP

sdecugis@nict.go.jp, {souheil, nobushi, dolin, atie}@tera.ics.keio.ac.jp, tera@ics.keio.ac.jp

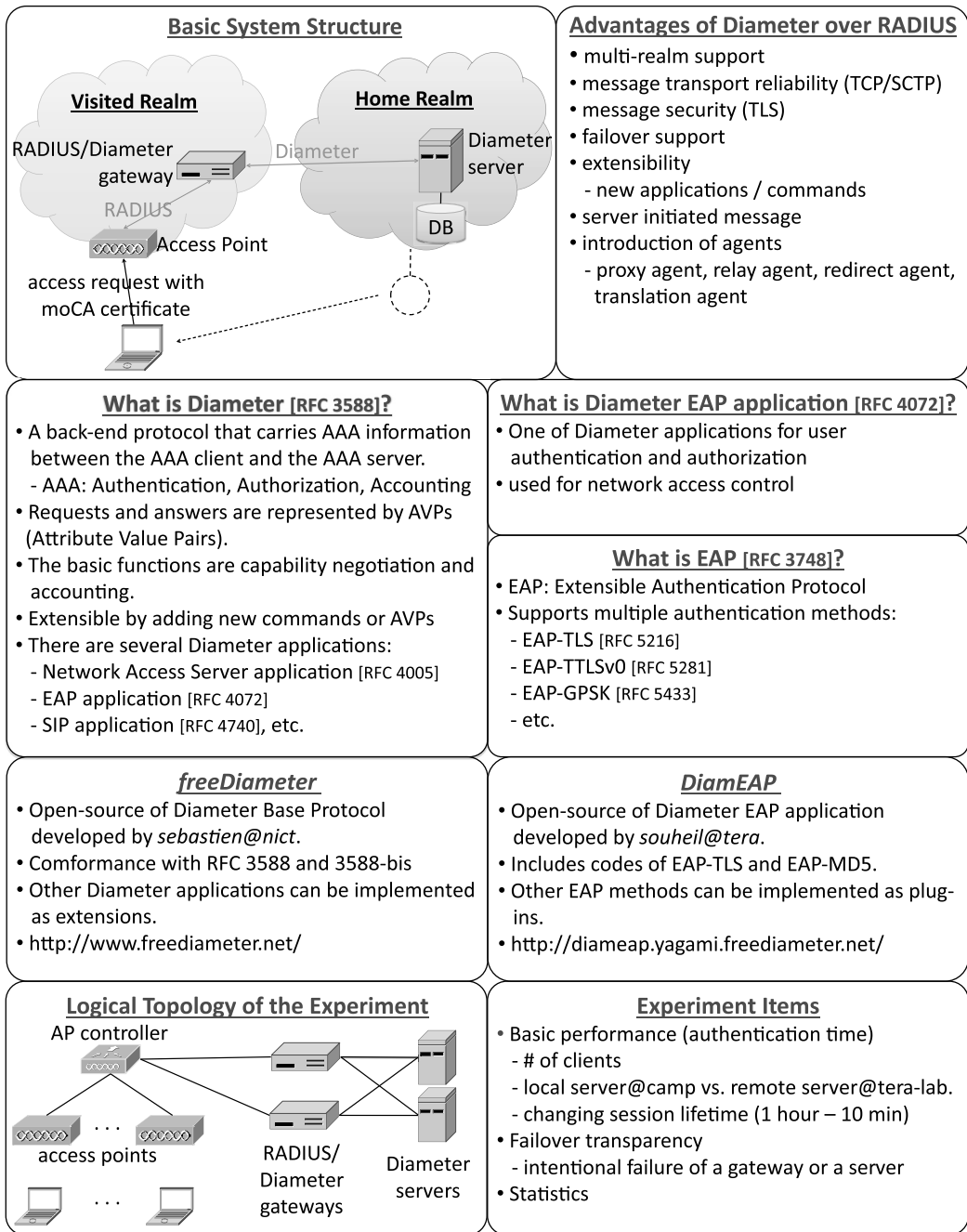


図 4.1. 2010 年 9 月合宿における Diameter と EAP による WiFi アクセス制御の運用実験の概要

験を行った。この合宿には約 200 人が参加しており、4 日間の合宿の全期間を通して運用した。認証のライフタイムは、1 日目は 1 時間、2 日目は 30 分、3 日目と 4 日目は 10 分と設定した。合宿期間中、本シ

ステムに関して参加者からの苦情はなく、安定したサービスを提供できたと言える。

本システムの構成については、図 4.1 を参照のこと。