

## 第9部

### AAAアーキテクチャの検討およびAAA基盤の構築

寺岡 文男, 厚谷 有輝, Souheil Ben Ayed

---

---

#### 第1章 AAA WG 2011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 EAP Applicationのplug-inとしてのEAP-TTLSの実装

---

---

#### 第2章 Diameter EAP Applicationのplug-inとしてのEAP-TTLSの実装

---

---

EAP-TTLSはネットワークアクセスにおける認証方式の1つで、サーバの認証に電子証明書を、ユーザの認証にTLSトンネルを利用したパスワードベースの認証を行うことで相互認証をサポートする。同じくTLSハンドシェイクを利用するEAP-TLSに比べてユーザに証明書を配布する必要がない分、運用が容易である。2011年度はDiameter EAP Application上にEAP-TTLS認証システムを実装し、EAP-TTLS内部での認証方式には主要な4つの認証方式(PAP、CHAP、MS-CHAP、MS-CHAPv2)をサポートした。検証の結果、Windows7、Linux、Android、iOS(iPad)の

クライアントマシンで正常に認証処理を行うことができることを確認した。認証処理時間も16ms前後であり、実用上問題ないことを確認した。

EAP-TTLSの実装についての詳細は、wide-paper-aa-eapttls-00.txtを参照のこと。