

第14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

第1章 AAA WG 2013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。

- ・ヤマタノオロチ:インターネットサービスのための認証認可基盤

第2章 ヤマタノオロチ:インターネットサービスのための認証認可基盤

ヤマタノオロチは、インターネットを通して提供される様々なサービスに対し、統一的な認証認可の仕組みを実現する汎用認証認可基盤である。汎用の認証認可基盤には“マルチドメイン環境で多様な認証方式をサポートすること”、“サービスによらないアクセス制御を実現すること”、“基盤の負荷を少なくしてスケーラビリティを確保すること”の3つが要求事項として挙げられる。ヤマタノオロチはこれらの要求事項を満たすような認証と認可の機能を提供するシステムである。AAAプロトコルのDiameterと認証フレームワークのEAPを利用することで、ユーザ情報の一元化とマルチドメイン認証を可能とした。またKerberosやXACMLを参考にしたチケットシステムを設計し、サービスによらないアクセス制御とスケーラビリティの確保を実現した。これらの設計に基づいて実装したシステムが複数のインターネットサービスにおいて正しく動作することを検証し、認証および認可の処理時間も実用上問題ない時間で処理が完了することも確認した。

詳細は、wide-paper-aaa-wg-orocho-00.txtを参照のこと。