第13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、Souheil Ben Ayed、厚谷 有輝

第１章　AAA WG 2012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．

- マルチドメインクラウドコンピューティング環境における協調的なアクセス制御

第２章　マルチドメインクラウドコンピューティング環境における協調的なアクセス制御

ユーザがサービス利用を要求したとき，サービス事業者はユーザが真のユーザであるかを認証(authentication)し，次にユーザの属性を確認してユーザにサービス利用の権限を委譲(authorization)する必要がある．ユーザがクラウドコンピューティング事業者(CCP)を利用する際，通常は契約しているCCP(home CCP)が提供するサービスしか利用できないが，契約関係のないCCP(visited CCP)のサービスを一時的に利用したい場合がある．home CCPとvisited CCP間にそれぞれの契約ユーザに関するサービス相互利用契約があれば問題ないが，本論文ではそのような契約が無い場合のアクセス制御方式を提案している．提案方式では，まずvisited CCPはユーザがhome CCPと契約しているユーザであるかを認証し(マルチドメインにおけるユーザ認証)，次に相互利用契約のある他のCCPを経由することによってhome CCPとvisited CCP間に“権限委譲のチェイン”を構築することにより，ユーザはvisited CCPから権限委譲を受け，visited CCPが提供するサービスを利用できるようになる．具体的には，シングルドメインにおける権限委譲のためのアーキテクチャであるXACMLに新たにDVP(Delegation Validation Point)と呼ばれるモジュールを加えることにより，visited CCPとhome CCP間に権限委譲のチェインを構築する．

詳細は，wide-paper-aaa-wg-collaborative-access-control-00.txtを参照のこと．