L-027

Shibboleth を応用した認可管理機構の一検討
Disccusion about authorization function based on Shibboleth

宇野 槙祐† 松浦 健二‡ 佐野 雅彦‡ 上田 哲史‡ ボロルツェツェグ・ガンバト†
Shinsuke Uno Kenji Matsuura Masahiko Sano Tetsushi Ueta Bolortsetseg Ganbat

1. はじめに

高等教育機関など多くの組織では統合的な認証基盤を実装した Web システムが導入され,組織内の認証管理を統一化している.こうした組織では異なる組織との協働を目的に,各組織が保有する情報資源の共用を図るなど組織間の連携に対する関心が高まっている.しかし,組織間で連携を行なうには,単一組織に向けたシングルサインオンの枠組みでは実現困難な問題もある.その技術的な問題として,複数組織間における組織構造の違いが挙げられる.ユーザ管理上の組織体系は組織毎に固有のものであり,構成員の所属を表す名称といった属性情報は共通化されている部分もあるが,多くは独自のものである.このため,認証を通じた属性情報は認証機構によって異なる.さらに,多様な情報システムの中にはユーザによって動作を変える動的なコンテンツも存在し,それを利用する範囲や必要な属性は予め定めた運用ポリシによって決定される.従って,各組織が保有する情報資源を組織間で流通させるには,共通的な運用ポリシと運用ポリシに対応できる柔軟性,高度なセキュリティ水準を持った機構が必要である.

本研究は組織間認証連携における個人単位での小規模連携を視野に入れた,各組織特有の認証管理機構に対して柔軟に対応可能な,オンライン組織活動を支援する組織間認可基盤の構築を行なう事が目的である.また,我々が想定する連携には高等教育機関における共同研究プロジェクトのような形態も含み,数名程度で協働を行なう場合から一定の大きさまで幅広く対応する.

2. 組織間の連携

2.1 問題点

異なる複数の組織が連携動作を行なう上で,各組織が保有する既存のシステムで利用する属性情報と組織間で利用する属性情報との運用ポリシの違いが課題となる.各組織が保有する既存のシステムは組織内に向けて設計・開発されたものであり,運用ポリシも予め定められたものが多い.そのため各組織で運用されているシステムは組織間の連携には対応しておらず,属性情報の不一致や不足のために十分に機能しない.従って,各組織が保有するリソースを組織間で応用するには,属性共有の技術が必要である.この問題に対しては,次節以降の Shibboleth で解決できる部分がある.

2.2 Shibboleth

本研究は,組織間に渡るシングルサインオンおよび認可のための属性共有の技術として米国 Internet2 が開発した Shibboleth を用いる.Shibboleth は ID 連携によるプライバシー保護を考慮した認証・認可の統合フレームワークを実現する.これらの機能は共通の認証基盤として利用する事により,複数の組織を信頼関係で結びつける組織間連携だけでなく,組織間での認可制御を可能にするものである.

3. 設計・実装

3.1 Shibboleth の動作概要

Shibboleth を構成する主体はアイデンティティプロバイダー(IdP)とサービスプロバイダー(SP),複数の認証基盤を含む連携組織で利用するディスカバリーサービス(DS)の 3 つである.IdP ではユーザ認証機能とともにバックエンドにあるデータベースから属性情報を取得し,SP に渡す属性の定義・制御が可能である.DS は IdP が複数存在する場合に使用するオプションであり,ユーザに対して IdP を選択可能とする機能を提供する.SP は組織が管理する情報サービスや研究資料等の情報資源のアクセスを管理し,ユーザに提供するプロバイダーである.Shibboleth の枠組みの中ではアプリケーションやコンテンツリソースは SP によって保護・管理されている.ユーザがそれらを利用するには本人性を証明する必要があり,未認証の場合にユーザからのアクセスは IdP または DS へとリダイレクトされる.ユーザは指定された認証方式に従って認証を行い,認証に成功すると結果を基に認可判断が行なわれ,SP はユーザに対してリソースへのアクセスを行なわせる.

3.2 属性情報に基づいた認可制御

Shibboleth ではサービスを提供する側が属性情報を保持する必要はなく,IdP のバックエンドにある認証管理機構などから必要な属性情報を取得する.例えば高等教育機関における部局間の包有関係を表現しやすい LDAP を導入し,ユーザの属性情報を格納している.取得した属性情報は SP がユーザに対してリソースへのアクセス権限を与えるかどうかの判断に利用される.特定のディレクトリ下に置かれているリソースにアクセスするには SP 側で指定した属性値が必要となる.下記の図は,実世界上の組織に属する人物が我々の提案する組織間認可基盤を用いてサービスを利用する体系を示したものである.

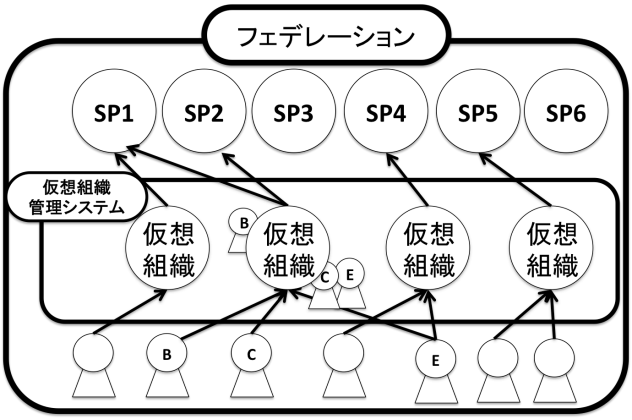

図 1 仮想組織におけるサービス利用体系

図中の上層と下層は実世界のサービス及びユーザーである.例えば,図中に記述されている人物は実組織上は異なる組織に属する人物となる.また,中層は仮想組織管理システムによって仮想的に存在する仮想組織である.すなわち,本

研究ではこの層を前述の Shibboleth を用いて設計および実装を行なう.ここで,例えば,当該仮想組織に着目すると人物 B がグループを作成した管理者であり,人物 C,E は一般のユーザとして SP1 と SP2 が利用可能である.人物 B は当該仮想組織の管理者であるが,SP1,P2 の管理者である必要は無い.人物 C,E は異なる実組織に所属する人物であり,仮想組織に所属する以前にはアクセスする権限を持たないため,SP1 と SP2 のサービスを受ける事はできない.しかし,SP1 と SP2 を利用可能な人物 B が当該仮想組織を構築し,同じグループに所属する事により人物 B のアクセス権が反映され,利用可能となる.このように,仮想組織はグループを作成した人物のアクセス権がグループ全体のアクセス権として反映され,自身とは異なるアクセス権を持った人物が構築したグループに参加する事により利用できるサービスの範囲を拡張することができる.

仮想組織管理システムはフェデレーションの中の SP として構築される.そのデータベースは各組織の IdP から参照可能なようにデータの共有化を図る.利用するデータ自身は一時的なものであり,ダイナミックに生成される.すなわち,個人情報は含まない暗号化データとする.本提案のモデルではこの暗号化データを鍵として各 SP 側で認可制御を行なう.

3.3 属性情報の管理

前節の認可制御を実現するための属性情報の渡し方について,本研究では検討を行なった.一般には Shibboleth では,任意の属性情報を,認証後に必要に応じて SP 毎に流通させることもできるが,この属性情報は,DataConnector と呼ばれる機構によって属性源を指定する事が出来る.指定された属性源を使って属性を定義できる.この属性の定義に Simple(単純)な Mapped(マッピング),Script(ECMAScript)などが実装される.これらの実現手法によって,属性情報(名前,値)を扱えるが,ここではその値の定義方法について検討する.すなわち,異なる実組織に跨がる仮想組織の構成員共通の属性を暗号化し,その運用フローを検討する.

実際には,認可制御を行なうにはこの特殊な属性情報を事前に設定しておかねばならない.また,それに対して認可制御情報として渡ってくる属性情報の値の照合が必要となる.

4. 考察

Shibboleth を用いた組織間連携に関する先行研究[1],[2][3],[4]は数多く報告されている.例えば GakuNin mAP[5]あがある.GakuNin mAP は学認で用いる SP であり,学術認証フェデレーションの認証フレームワークを利用して大学の学部や研究室,共同研究プロジェクトといった様々な所属レベルで仮想的なグループを作成および管理する機能を持ったグループ管理システムである.mAP 上において,利用者はグループ単位で活動を行い,アクセス制御をかける事で柔軟なサービス提供を受ける事ができる.mAP の特徴としてグループ構造を階層化して管理する事が挙げられる.すなわち,下位に位置するグループは上位に位置するグループに含まれるという包有関係を表したグループ管理構造である.

本研究が提案するシステムはユーザ認証,属性提供を行なう IdP と動的仮想組織を構築するシステムを管理する SP,構築した仮想組織でアクセスした場合のみサービスを提供する SP によって構成されている.設計としては動的に構築される仮想組織にサービス利用権限の付加を行なえるよう属性認可による実現を試みたものである.本研究における仮想組織とは所属する各メンバーがそれぞれ自立した主体として相互に連携し,活動を自主展開していくネットワーク型の組織である.実組織に属する人物が自由に参加でき,システム上は仮想組織を識別する属性と仮想組織管理者の属性などがある.構成員は管理者と一般ユーザであり,管理者は仮想組織を作成した人物,一般ユーザは既存の仮想組織に参加した人物である.特定の権限情報を持った人物が管理者として活動する仮想組織に所属することで自身の権限では利用できなかったサービスが利用可能となる.従って,グループ同士の関連性は無く,それぞれが独立している.本研究が提供する組織間連携の枠組みにおいては,サービスやリソースを提供する SP の利用には仮想組織を構築あるいは既存の仮想組織に所属していない場合にアクセスを仮想組織登録システムへとリンクする必要がある.

5. まとめ

本稿では,Shibboleth を用いた組織間認証連携におけるオンライン組織活動を支援する組織間認可基盤の構築を行なう一検討を行なった.Shibboleth は認証・認可のフレームワークと属性交換による組織間シングルサインオンを実現する技術であり,先行研究の事例も数多く報告されている.しかし,それらの事例は組織間認証連携を行なうには認可の機能を充実させる必要がある. 既存のシステムと協調する機能が不足するため属性が不足,または一致しない場合があった.本提案によって,例えば同じ実組織内でも異なる認可ポリシにも対応できる事になる.例えば,A 学部の教授会コンテンツサーバ(ファイル)には職名としての教授のみとし,B 学部の教授会コンテンツには B 学部所属の教員全員がアクセスできるような枠組みが容易に実現できる.

これらの事例を踏まえ,本研究は Shibboleth の枠組みの中でユーザの属性情報を基にサービスの提供者が認可判断する実装を行った.その結果,ユーザが認証を行なうと属性値によって特定のディレクトリ下のリソースを取得できるかどうかの判断を行なう事ができた.

参考文献

[1] 金西 計英, 松浦 健二, 三好 康夫, 高木 知弘, 嵯峨山 和美, 矢野米雄：「大学間 Web サービス連携のための Shibboleth を用いた認可管理機能の実現」日本教育工学会論文誌 32(Suppl.), 93-96, 2008

[2] 松浦 健二：「ek4 を支える認証基盤」情報知識学会誌 21(2), 309-312,2011

[3] 伊藤 栄典, 片岡 真, 牧瀬 ゆかり：「Shibboleth 認証基盤構築と学術認証フェデレーションへの参加 –今後の e-リソースサービス基盤にむけて-」九州大学付属図書館研究開発年俸 2009, 11-15, 2009.

[4] 伊藤 栄典：「九州大学の取り組み」,UPKI シンポジウム 2010, パネルディスカッション, 2010.

[5] GakuNin mAP https://map.gakunin.nii.ac.jp, 2012 年 6 月 20 日 参照

† 徳島大学先端科学技術教育部

‡ 徳島大学情報化推進センター