3ZB-5

条件に基づく認可を実現するシングルサインオンシステム

田中 美里 ‡　廣安 知之 †　三木 光範 †
‡同志社大学工学部学生　†同志社大学工学部

1　はじめに

コンピュータシステムにおける認証は，ユーザ，サービス，およびパケットが正規のものであるか確認する行為を意味する．システムにログインしようとするユーザが認証に成功すると，システムからユーザに対して，相応の権限が付与される．例えばユーザに対して与えられたのがゲスト権限であれば利用できるサービスが限定されるのに対し，システム管理者の権限であればシステムの設定を変更することもできる．このように，認証されたユーザがアクセス可能な情報資源を制御することを認可という．

通常，特定の情報資源へのユーザのアクセス権は，管理側のポリシに基づいて，ユーザへと固定的に付与されることが多い．これに対し，本研究ではユーザのアクセス権を動的に変更させるシステムについて検討する．具体的には，ユーザは管理者によって条件を与えられ，それに対する自身の状態について応答する事で，各情報資源へのアクセス権が決定される．ここで言う条件とは，それに対するユーザの状態が変化しうるものであり，たとえばタスクの処理中や済みといった，ユーザ自身が変更可能な条件を含む．

本報告では，提案システムの実現方法と有効性を検討するために，条件の具体例としてタスクの管理を用い，システムを実装した．また，認証を一元的に管理するシングルサインオンシステムを構築し，各情報資源に対する認証と同時に，ユーザの状態に基づく認可を行った．

2　システムの概要

2.1　条件に基づく認可

一般に，ユーザの認可即ちアクセス制御はセキュリティポリシに基づいて行われる．ポリシに従って一度決定された認可が，頻繁に変更されることはない．また，認可を変更するにはシステム管理者やサービス提供者など，アクセス制御をかける対象に対して広範な権限を持つ者である必要がある．

これに対し，管理者がユーザに対して与えた条件をユーザが満たすか否かをポリシとして採用したものが，本システムの実現する条件に基づく認可である．もし，条件に対するユーザの応答が固定的であれば，管理者による設定で済む．しかし，タスクの処理中や済み，ユーザのシステムの使用頻度，出勤状況など様々に変化し得るユーザの状態に対し，認可を制御する場合，管理者の手によってだけでは難しい．本システムでは，管理者等がユーザに対して条件を与え，その条件に対するユーザの状態によって，管理者を通さない頻繁な認可の変更を可能としている．認可の条件やユーザの状態は，ユーザに対して条件を付加するシステム上に保存される．これらのシステムはユーザの状態の変化を受けると，各サービスへの認証，認可を一元的に管理する認証システムへとアクセスを行い，認可の設定を変更する．

例えばタスク管理の場合，認証，認可を終えたユーザがシステムにアクセスしていたとしても，タスク管理システムに新たなタスクが投入されると，ユーザのアクセス権限が変更され，ユーザはシステムへのアクセスが制限されることとなる．

2.2　SSO(Single Sign-On)

SSO とは一回の認証によって，許可された複数のシステムへのアクセスを許可する技術，システムである．

SSO の実現には，主に 2 つの手法がある．一方は，各サービスサーバにインストールされたエージェントモジュールが，認証サーバへとユーザの認証状態を問い合わせるエージェント型．もう一方は，各サービスサーバへのアクセスを認証サーバが代理 (proxy) するリバースプロキシ型である．本システムでは，エージェント型を用いた SSO を提供する．エージェント型はサービスサーバ毎にエージェントモジュールを導入しなければならないが，拡張性が高く，認証システムへの負荷も少ない．

3　認証システム

3.1　構成

本システムは，認証サーバと，各サービスサーバに導入されるエージェントモジュール，認証サーバに認可の変更を求める認可変更システムの三つによって構成される．認証サーバ上に，条件に基づく認可に利用

Single Sign-on system that authorizes user based on the condition

‡ Misato TANAKA(mtanaka@mikilab.doshisha.ac.jp)
† Tomoyuki HIROYASU(tomo@is.doshisha.ac.jp)
† Mitsunori MIKI(mmiki@mail.doshisha.ac.jp)
Undergraduate Student (‡)
Department of Knowledge Engineering and Computer Science, Doshisha University (†)
1-3 Miyakodani, Tatara, Kyotanabe, Kyoto 610-0321, Japan

するルールベースが格納されており，これについては 3.3 節にて詳述する．また，ユーザ情報を一元的に管理するバックエンドデータベースとして LDAP を利用している．

エージェントとしてはプログラムから呼び出すプラグイン型の認証モジュールと，Apache のモジュールを利用したディレクトリ型の認証手法の 2 つがある．後者は，Apache の Basic 認証機能を利用してきたため，プログラム中に認証機能が存在しない既存サービスへの対応を目的としている．

3.2 認証と認可の流れ

認証は認証システムへのログイン時のみ行われる．その後，ユーザが各サービスにアクセスする場合，認可の確認のみ行われる．

認証前のユーザは，認証システムに参加するサービスにアクセスする場合，認証システムに ID とパスワードを送信する必要がある．以下にこのケースにおける認証，認可の流れを示した．

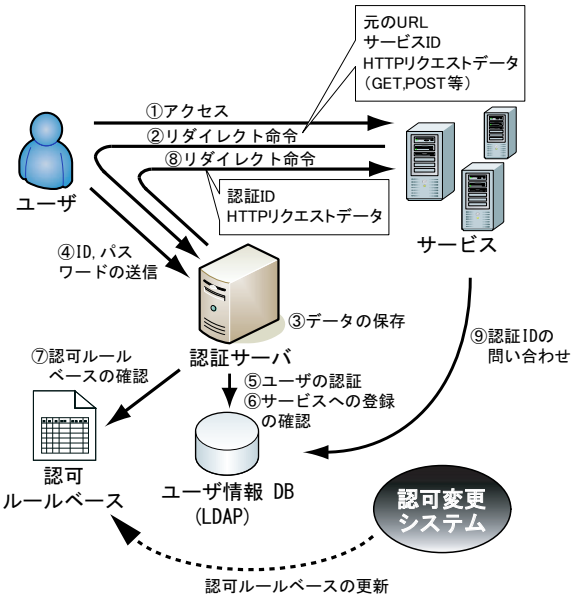

図 1: 認証，認可の流れ

1. 認証システムに認証されていないユーザがサービスにアクセスする
2. サービスは現在の URL とサービス ID，HTTP リクエストのコンテンツの情報を付加し，ユーザを認証システムへリダイレクトする．
3. 認証システムはアクセスしてきたユーザから，2 で付加されたデータを DB に保存する．
4. ユーザは認証システムに対し，ID とパスワードを送信する．
5. 認証システムはユーザの認証を行う．
6. ユーザが認証されると，認証システムはユーザのサービスに対するアクセス権限を確認する．
7. 6 で権限が認められると，次に認可ルールベースを確認する．
8. 6，7 で認可されると，ユーザは認証システムから一時的な認証 ID とアクセス時に渡したデータを与えられ，元のサービスへとリダイレクトさせられる．認可されなかった場合，認証システムのポータルサイトが表示される．
9. サービスはアクセスしてきたユーザから一時的な認証 ID を受け取り，これの有効性を認証システムに問い合わせる．
10. 一時的な認証 ID が有効な場合，サービスはユーザのログインを許可する．

以前のシステム [1] では，認証サーバはサービスの稼動するサーバに対して HTTP COOKIE を発行することで，認証用のトークンを共有していた．しかし，クロスドメインにおける COOKIE の共有にはセキュリティ上の問題がある．本システムはリダイレクト時に，HTTP リクエストデータに認証 ID を含める事で，安全性の向上を図った．

3.3 認可

本システムにおける認可は二段階に分けて行われる．各サービスに対するユーザの登録の確認と，条件に基づく認可によるアクセス制御である．前者はシステムの管理者，サービス提供者等がポリシに従って特定のユーザを許可するという，従来通りの固定的な認可である．これを実行した後，後者の条件に基づく認可を行う．

条件に基づく認可では，認証サーバ上の認可ルールベースを利用する．これは，タスク管理システム等の各認可変更システムから認証サーバに送られてきた認可情報が，フィルタとして格納されている．

以下にフィルタに格納される情報を示す．

表 1: 認可ルールベースのフィルタ

内容	備考
番号	一意な ID
ユーザ ID	アクセスを拒否 (または許可) するユーザ
サービス名	アクセス先サービス名
開始時刻	拒否 (または許可) の開始時間
終了時刻	拒否 (または許可) の終了時間
認可	拒否または許可

これらのフィルタが認可ルールベース上に複数登録され，認証システムはユーザのサービスへのアクセス要求に対しこれを検索する．

フィルタには，ユーザのアクセスを拒否するフィルタと，特例的に許可するフィルタの二種類がある．このルールベースによって行われるフィルタリングはルータ等のフィルタリングとは異なり，原則許可となる．つまり，ユーザのアクセスを拒否するフィルタがない場合，基本的にユーザのアクセスが許可される．例外は，アクセス許可フィルタが存在する場合である．これは，サービスへのアクセスが必要とされる場合に，一時的にアクセス禁止を解除するため用いられ，同時刻に存在するアクセス拒否フィルタに対して優越する．

参考文献

[1] 牧野 浩之，廣安 知之，三木 光範．認可を必要とするシングルサインオンシステム，情報科学技術フォーラム JST 資料番号：L4664A，Vol.FIT 2007 一般講演論文集 第 4 分冊，pp.121-122，2007.