CAS を用いた SNS 間のシングルサインオンに関する研究

渡辺研究室　　会田拓也　人見直樹

1.　はじめに

シングルサインオンとは，一度の認証を行うだけで多数のサイトに ID とパスワードを入力せずにアクセスする仕組みである．シングルサインオンを用いれば，渡辺研究室で管理運営している帝京 SNS~試験運用版~[1]とうつのみやバンバ情報館[2]でも一度の認証だけで相互利用できると考えた．

本研究では，CAS を用いて SNS 間のシングルサインオンを実現することを目的とする．

2.　シングルサインオンと CAS

2.1.　シングルサインオンとは

シングルサインオンとは一度の認証を行うだけで多数のサイトに ID とパスワードを入力せずにアクセスする仕組みである．シングルサインオンを実現する認証機構として代表的なものは OpenID[3], CAS などが挙げられる．

2.2.　CAS とは

CAS とは Central Authentication Service の略で，米 Yale 大学によって開発された Web ベースのアプリケーションであり，シングルサインオンを実現するための認証機構である．現在は，JA-SIG[4]のプロジェクトとして継続的な開発が進められている．

CAS の特徴としては，TGC や ST などの標準的な Web 技術を利用しており処理が極めて軽く，インストールが容易という点である．また，CAS はユーザ管理ができるため学内などの組織内でシングルサインオンを行うのに向いている．そのため米をはじめとする 30 を超える大学で用いられており，日本では名古屋大学[5]などで用いられている．

CAS で認証を行う際に，重要な役割を果たしている TGC と ST について，以下に述べる．

・Ticket Granting Cookie(TGC) : TGC とは CAS サーバからブラウザに与えられるクッキーであり，ブラウザが認証済みかどうか判断するための物である．

・Service Ticket(ST) :　ブラウザが CAS 認証を利用する Web アプリケーションへアクセスする際に，ワンタイムチケットの役割を果たす URL パラメータであり，ブラウザが CAS 認証をすることで得られる．

TGC と ST は，ログアウトおよび，ブラウザを終了した際に破棄される．

3.　システムの構成

図 1 は，本研究で作成するシステムの構成図および，認証処理の流れである．シングルサインオンを行う認証機構として CAS を使用し，認証元に OpenLDAP を使用した．以下に認証処理の流れを示す．

(1)ブラウザから SNS にアクセスを行う．

(2)SNS 内の CAS クライアント(以下, クライアント)が CAS サーバへのリダイレクションと同時に TGC と ST の情報を送信する．

(3)未認証の状態では，TGC と ST がないので CAS サーバは Web ブラウザにログインウィンドウを渡す．

(4)ユーザは ID とパスワードを入力する．

(5)CAS サーバは，入力された ID とパスワードの検証要請を LDAP サーバへ行う．

(6)LDAP サーバは検証結果を CAS サーバに送り，検証結果が正しければ認証され, ブラウザに TGC と ST を発行する．

(7)TGC と ST を発行された状態のブラウザが SNS へアクセスを行うと，(2)が再度行われ，CAS サーバは TGC と ST の検証を行う．検証結果が正しければ SNS 内のクライアントに検証結果を送り, SNS はログインを行いブラウザにコンテンツを表示させる．

これらにより，一度の認証で CAS 対応の SNS に ID とパスワードの入力なしでログインが行える．

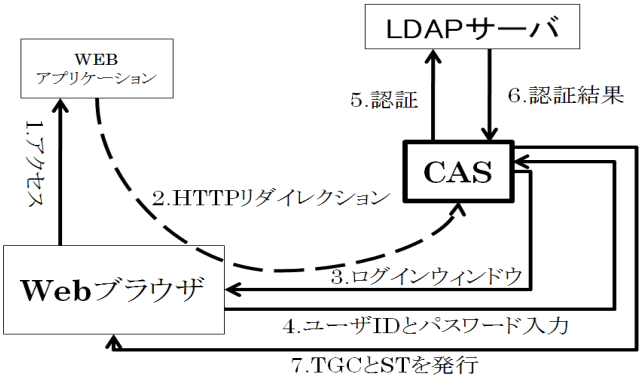

図 1 システム構成図，認証処理の流れ

4. システムの構築

以下に，本研究に使用したシステム環境を示す.

・稼動サーバの OS：FedoraCore6

・使用ソフトウェア：Apache2.0，Tomcat5.5，JDK5.0，OpenLDAP2.3.30，PHP5.1.6

構築手順を以下に示す.

(1)Apache のインストールおよび, 設定を行い, Web サーバを構築.

(2)Tomcat のインストールおよび，設定.

(3)Apache のモジュールである mod_jk2 を利用して, Apache と Tomcat の連携を設定.

連携を行うのは, CAS サーバが SSL を使用するので，Tomcat のポートが邪魔になる為である.

(4)Tomcat にバーチャルホストでアクセスできるように設定.

本研究のシステム構築では，バーチャルホスト名は casls.ics.teikyo-u.ac.jp とした.

(5)(4)で設定したバーチャルホストの SSL の設定.

(6)LDAP サーバの導入.

DB には，BerkreyDataBase を利用した.

(7)CAS サーバの導入.

CAS サーバは，バージョン 3.2.1 を使用した.

(8)CAS サーバの認証元を LDAP サーバに設定.

(9)SNS の構築後、CAS 対応の為に認証部を改造.

(10)SNS にクライアントの配置.

クライアントは，phpCAS を使用した．これは本研究で使用した SNS エンジンの OpenPNE が PHP で構成されている為である.

(11)SNS の config.php に CAS 認証に必要な情報を記述.

5. 動作確認

我々は，CAS 対応した 2 つの OpenPNE(以下, OpenPNE1 号･2 号)を利用して以下のように動作確認を行った.

(1)CAS のログインページから CAS にログイン.

(2)ログイン後のページのリンクから我々が作成した OpenPNE 1 号にアクセス.

(3)OpenPNE 1 号に ID とパスワードを入力することなくログインできることを確認.

(CAS によるシングルサインオンの成功)

(4)OpenPNE1 号内のリンクから OpenPNE2 号にアクセス.

(5)OpenPNE2 号に ID とパスワードの入力なしでログインできることを確認.

以上の手順により，CAS を用いた SNS 間のシングルサインオンが動作したことを確認した.

6. おわりに

本研究では，我々は OpenPNE を CAS に対応させることでシングルサインオンを行った．シングルサインオンを行うことで, 一度の認証で他の ID とパスワードを入力せずにログインを行えることは有用であると考える.

今後の課題としては以下のことがあげられる.

・認証の為のデータと，既存の日記などのデータとの照合.

・上記の場合のユーザ個人情報管理の問題

謝辞　OpenPNE の CAS 対応についてはエミットジャパンが試験的に構築した際のソースリストを参考にさせていただきました.

参考文献

[1]中嶋克寿, 高山裕伴: 「大学におけるソーシャル・ネットワーキング･サービス(SNS)の活用に関する研究」，帝京大学 理工学部 情報科学科　卒業論文 (2007 年)

[2] 澤﨑博志，山崎友之:「商店街に特化した SNS(ソーシャル・ネットワーキング・サイト)の構築と活用に関する研究」，帝京大学 情報科学科 卒業研究 (2008 年)

[3]OpenID　Wikipedia http://ja.wikipedia.org/wiki/OpenID (2009 年 1 月アクセス)

[4] JA-SIG http://www.ja-sig.org/products/cas/ (2009 年 1 月アクセス)

[5] 小村道昭，福山貴幸，梶田将司，山里敬也 :「名古屋大学における WebCT の CAS 化による認証統合」第 3 回 WebCT 研究会予稿集，pp.53-57，(2005)