

CASによる Django, Plone間での シングルサインオン

佐古田 純哉

シングルサインオン (Single Sign On - SSO) とは

一度の認証処理によって
複数のコンピュータ上の
リソースが利用可能に
なる認証機能である。

(Wikipediaより)

Central Authentication Service(CAS)とは

<http://www.ja-sig.org/products/cas/index.html>

各種Webサービスの認証
機能を担い、SSOを実現
する。Servletとして稼動

対応クライアント

Java, Perl, PHP, .NET,
RoR, Zopeなど多数。
Apacheのモジュール
もある。

CASに必要なもの

- Servlet環境
- ユーザ情報を管理する
データソース(LDAP他)

インストールの ポイント (CAS 3.0.7 + LDAP)

必要プラグイン

- `cas-server-ldap-3.0.7.jar` (1)
- `ldapbp-1.0.jar` (2)
- `spring-ldap-1.1.2.jar` (3)

(1) 付属 (targetディレクトリ内)

(2) <https://svn.sourceforge.net/svnroot/springframework/repos/repo-ext/com/sun/ldapbp/1.0/ldapbp-1.0.jar>

(3) <http://www.springframework.org/ldap> (バージョンに注意)

インストール

- localPlugins/libにプラグインを配置
- webapp/WEB-INF/classes内の
deployerConfigContext.xml修正*
- localPluginsでant war実行
- 作成したwarファイルをデプロイ

* <http://www.ja-sig.org/products/cas/server/ldapauthhandler/index.html>

その他

デフォルトではSSL環境が要求されるのでApacheとの組み合わせが一般的。non-SSL環境で使いたい場合はcas-servlet.xmlを以下のようにする。

```
<property name="cookieSecure" value="true" />
```

Plone と Django の 認証機能にCAS を導入する

Plone + CAS

Plone-2.5.x

必要パッケージ

- Plone CAS Login 2.5.0 (1)
- CAS4PAS (2)

(1) <http://plone.org/products/plonecaslogin/releases/2.5.0>

(2) <http://www.zope.org/Members/mrlex/ACUF>

Root Folder

- [-] Catalog
- [-] CatalogOld1
- [-] Control_Panel
 - Lib
- [-] Plone
- [-] Team
- [-] TeamOld1
- [-] Test
- [-] Test2
- [-] acl_users
 - temp_folder

© Zope Corporation
Refresh

Contents | **Search** | **Properties** | **Security** | **Undo** | **Ownership** | **Interfaces** | **Find** | **Cache**

Pluggable Auth Service at /Plone/acl_users Help

CAS Auth Helper ▼ Add

Type	Name	Size	Last Modified
<input type="checkbox"/>	chooser		2006-11-19 16:32
<input type="checkbox"/>	credentials_basic_auth (HTTP Basic Auth)		2006-11-19 16:32
<input type="checkbox"/>	credentials_cookie_auth		2006-11-19 16:32
<input type="checkbox"/>	local_roles		2006-11-19 16:32
<input type="checkbox"/>	mutable_properties		2006-11-19 16:32
<input type="checkbox"/>	plonecaslogin (PloneCASLogin Installation)		2007-05-21 16:19
<input type="checkbox"/>	plugins		2006-11-19 16:32
<input type="checkbox"/>	portal_role_manager		2006-11-19 16:32
<input type="checkbox"/>	sniffer		2006-11-19 16:32
<input type="checkbox"/>	source_groups		2006-11-19 16:32
<input type="checkbox"/>	source_users		2006-11-19 16:32
<input type="checkbox"/>	user_factory (Plone User Factory)		2006-11-19 16:32

Rename Cut Copy Delete Import/Export Select All

- Root Folder
 - Catalog
 - CatalogOld1
 - Control_Panel
 - Lib
 - Plone
 - Team
 - TeamOld1
 - Test
 - Test2
 - acl_users
 - temp_folder
- © Zope Corporation
Refresh

Activate

Properties

Ownership

Interfaces

Security

Properties

CAS Auth Helper at /Plone/acl_users/plonecaslogin

Help!

Properties allow you to assign simple values to Zope objects. To change property values, edit the values and click "Save Changes".

Name	Value	Type
Title	<input type="text" value="PloneCASLogin Installation"/>	string
CAS Login URL	<input type="text" value="https://localhost/cas/login"/>	string
CAS Logout URL	<input type="text" value="https://localhost/cas/logout"/>	string
Ticket validation URL	<input type="text" value="https://localhost/cas/validate"/>	string
Session credentials id	<input type="text" value="_ac"/>	string
Use ACTUAL_URL instead of URL	<input checked="" type="checkbox"/>	boolean

To add a new property, enter a name, type and value for the new property and click the "Add" button.

Name Type

Value

Plone-2.1.x

必要パッケージ

- Plone CAS Login 2.0.1 (1)
- ACASUserFolder \geq 2.0.0b2 (2)

(1) <http://plone.org/products/plonecaslogin/releases/2.0.1>

(2) <http://www.zope.org/Members/regebro/CAS4PAS>

- Root Folder
- Control_Panel
- Main
- Plone
- Test
- acl_users
- temp_folder
- © Zope Corporation
- Refresh

Contents Properties Test Undo Ownership Security

ACAS User Folder at /Plone/acl_users/Users/acl_users Help!

ACASUserFolder Objects are User Folder capable of CAS Authentication (<http://www.yale.edu/tp/auth/>) Users are generated "on the fly" and they have no way to authenticate otherwise than with a CAS ticket within this folder (no password support).

This User Folder needs to add a custom button to your site for logins if **login redirect** is NOT activated.
More details in [CAS usage scenarios](#)

GRUF Tip: Within a Group User Folder, put this user source **LAST** AND activate user persistence.

CAS Server

CAS Ticket Validation URL

CAS Login (interactive) URL

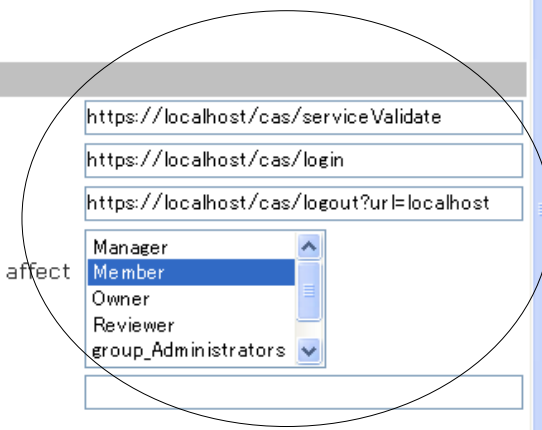
CAS Logout URL

Default User Roles
With persistent users this setting is used only once at 1st login. Subsequent changes of this setting won't affect previously stored roles, unless you reset all users.

Default User Domains
Same behaviour as for default user roles.

Retain POST data on session timeout
Warning! read [help](#) if you need high security.
It prevents data loss but enables session exhausting DoS !

Activate CAS login auto-redirect
Warning! read [help](#) before activating.
It disable UserFolder recursion!
In other words, login is mandatory.



User Persistence

Activate User Persistence

Users are kept upon Zope restart or session timeout.
This setting allow to manage **local roles** and is mandatory within a GRUF (Plone) to support groups.

Warning! Changing this setting **discards** locally stored user roles.

Fine Tuning

Validate Tickets with ACTUAL_URL

Django + CAS

cas-middleware

Djangoの認証システムを Middleware化したもの

パッケージ http://exogen.case.edu/cas_middleware.tar.gz

解説 http://blog.case.edu/bmb12/2006/12/cas_for_django_part_2

スクリーンショット

現在の場所: ホーム

ナビゲーション

- ホーム
- Members
- News
- Events

ログイン (cas)

ログイン

Welcome to Plone

作成者 toyoake - 最終変更日時 2007年05月21日 13時30分

Congratulations! You have successfully installed Plone.

If you're seeing this instead of the web site you were expecting, the owner of this web site has just installed Plone. Do not contact the Plone Team or the Plone mailing lists about this.

The first thing you should do is to set up your site by visiting the [site setup area](#). Become familiar with Plone by getting one of the [Plone books](#), and make sure you look at the available [add-on products](#) and [online documentation](#).

Quick Start

Some useful hints if you are new to Plone:

- Access key + 4 focuses the LiveSearch field - you can start writing your search terms straight away, and have all your information at your fingertips without leaving the keyboard. For information about how to use access keys in your particular browser, see the [accessibility page](#).
- Plone will automatically be displayed in the language your browser asks for. If you need more control over languages in Plone, install Plone Language Tool from the [site setup](#). If you need to maintain your content in multiple languages, download [LinguaPlone](#).
- Workflow states are color coded if you are logged in, so it is easy to keep track of content security and visibility. Try the site map with color coding for a visual security inspection of your site!
- If you prefer working with pure HTML, Structured Text or ReStructured Text markup instead of using a visual editor, you can disable it in [your preferences](#).

More information

For more information on Plone:

- [The Plone Open Source Content Management System website](#)
- [What's new in Plone 2.1](#)
- [Plone documentation](#)
- [Plone add-on products](#)
- [Plone mailing lists and support forums](#)
- [Available Plone books \(recommended!\)](#)
- [Server recommendations for Plone](#)

Plone is based on the Zope application server, and uses the Python programming language. More about these technologies:

- [Zope community](#)

2007年 5月						
日	月	火	水	木	金	土
			1	2	3	4 5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		



Central Authentication Service

Single Sign-on for the Web

CASオンライン認証サービスへようこそ！ デフォルトの設定ではユーザ名とパスワードは同じです。どうぞ試してみてください。

セキュリティ上の理由のためユーザ認証が必要なサービスへの接続が終了した際にはログアウトし、ブラウザを閉じてください！

NetIDとパスワードを入力して下さい。

NetID:

パスワード:

他のサイトへログインする前に警告する。

Languages: [English](#) | [Español](#) | [Français](#) | [Russian](#) | [Nederlands](#) | [Svenskt](#) | [Italiano](#) | [Urdu](#)

Copyright © 2005-2006 JA-SIG. All rights reserved.
XHTML, CSS

Powered by JA-SIG CAS 3.0.5

CASの認証サーバへ推移



Central Authentication Service

Single Sign-on for the Web

CASオンライン認証サービスへようこそ！ デフォルトの設定ではユーザ名とパスワードは同じです。どうぞ試してみてください。

セキュリティ上の理由のためユーザ認証が必要なサービスへの接続が終了した際にはログアウトし、ブラウザを閉じてください！

NetIDとパスワードを入力して下さい。

NetID:

パスワード:

他のサイトへログインする前に警告する。

Languages: [English](#) | [Español](#) | [Français](#) | [Russian](#) | [Nederlands](#) | [Svenskt](#) | [Italiano](#) | [Urdu](#)

Copyright © 2005-2006 JA-SIG. All rights reserved.
XHTML, CSS

Powered by JA-SIG CAS 3.0.5

IDとパスワードを入力

現在の場所: ホーム

ナビゲーション

- ホーム
- Members
- News
- Events

最近の変更

- sakoda
2007年05月21日
- amano
2007年05月21日
- Past Events
2007年05月21日
- Events
2007年05月21日
- News
2007年05月21日
- 最近すべての変更

Welcome to Plone

作成者 [toyoake](#) - 最終変更日時 2007年05月21日 13時30分

Congratulations! You have successfully installed Plone.

If you're seeing this instead of the web site you were expecting, the owner of this web site has just installed Plone. Do not contact the Plone Team or the Plone mailing lists about this.

The first thing you should do is to set up your site by visiting the [site setup area](#). Become familiar with Plone by getting one of the [Plone books](#), and make sure you look at the available [add-on products](#) and [online documentation](#).

Quick Start

Some useful hints if you are new to Plone:

- Access key + 4 focuses the LiveSearch field - you can start writing your search terms straight away, and have all your information at your fingertips without leaving the keyboard. For information about how to use access keys in your particular browser, see the [accessibility page](#).
- Plone will automatically be displayed in the language your browser asks for. If you need more control over languages in Plone, install Plone Language Tool from the [site setup](#). If you need to maintain your content in multiple languages, download [LinguaPlone](#).
- Workflow states are color coded if you are logged in, so it is easy to keep track of content security and visibility. Try the site map with color coding for a visual security inspection of your site!
- If you prefer working with pure HTML, Structured Text or ReStructured Text markup instead of using a visual editor, you can disable it in [your preferences](#).

More information

For more information on Plone:

- [The Plone Open Source Content Management System website](#)
- [What's new in Plone 2.1](#)
- [Plone documentation](#)
- [Plone add-on products](#)
- [Plone mailing lists and support forums](#)
- [Available Plone books \(recommended!\)](#)
- [Server recommendations for Plone](#)

Plone is based on the Zope application server, and uses the Python programming language. More about these technologies:

- [Zope community](#)

2007年 5月						
日	月	火	水	木	金	土
			1	2	3	4 5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

ログインした状態で Djangoの管理画面へ

✔ Login succeeded. Welcome, sakoda.

サイト管理

Auth	
グループ	+ 追加 ✎ 変更
ユーザ	+ 追加 ✎ 変更
Sites	
サイト	+ 追加 ✎ 変更

最近行った操作
操作
利用不可

そのままログイン可能

DjangoでのCAS認証 機能をカスタマイズ

ユーザ情報の付加

settings.py内の環境変数
CAS_POPULATE_USERに定義
したモジュール名を設定する
ことで拡張可能。

```
CAS_POPULATE_USER = 'mysite.utils.populate_user'
```

とした場合はプロジェクト内のutils.pyにpopulate_userを
定義する

例1) ログインユーザに無条件で
スタッフ権限を与える

```
def populate_user(user):  
    user.is_staff = True
```

例2)あらかじめパーミッション等を登録済みのeditorグループに設定

```
from django.contrib.auth.models import Group
def populate_user(user):
    user.is_staff = True
    try:
        group = Group.objects.get(name='editor')
        user.groups.add(group)
    except:
        pass
```

CASには最低限の認証機能だけをもたせ、そのほかの情報はLDAPやデータベースから取得することが可能

シングルサインオブ

CASサーバのログアウト
画面へリダイレクトする
ことによりなんちゃって
なシングルサインオフを
実現する

オリジナルのviews.pyの logoutメソッド

```
def logout(request, next_page=None):  
    from django.contrib.auth import logout  
    logout(request)  
    if not next_page:  
        last_page = request.META.get('HTTP_REFERER')  
        next_page = last_page or settings.CAS_REDIRECT_URL  
    return HttpResponseRedirect(next_page)
```

強引にCAS_REDIRECT_URLへ

```
def logout(request, next_page=None):  
    from django.contrib.auth import logout  
    logout(request)  
    if not next_page:  
        next_page = settings.CAS_REDIRECT_URL  
    return HttpResponseRedirect(next_page)
```

setcfg.pyのCAS_REDIRECT_URL はこんな感じ

```
SITE_URL = "http://mydjango/mysite/"  
CAS_SERVICE_URL = 'https://casserver/cas/'  
CAS_REDIRECT_URL = "%slogout?%s" % (  
    CAS_SERVICE_URL,  
    urllib.urlencode({'url':SITE_URL}))
```

CASの感想

選択できるデータソース
やCAS化クライアントの
多さが魅力。

ただし、それが逆に導入
をやや難解にさせてしま
っている。

mod_casを用いることで
Apacheの認証も統合可能。
適用範囲がかなり広まる。
今後tracなどでも試して
みたい。

以上