熊本大学公式 Web サイト更新に伴う認証システムの構築

谷口 勝紀[1], 永井 孝幸[2], 杉谷 賢一[2], 林 恵里[2], 松葉 龍一[3], 河津 秀利[4], 岩永 菜穂子[5]

熊本大学 工学部技術部[1], 熊本大学 情報基盤センター[2]

熊本大学 E-learning 推進機構[3], 熊本大学 運営基盤管理部情報企画ユニット[4]

熊本大学 マーケティング推進部広報戦略ユニット[5]

katunori@tech.eng.kumamoto-u.ac.jp[1]

概要：熊本大学では、2010 年度下半期より公式 Web サイトのリニューアルに取りかかり、2012 年度に公開を行った。旧システムでは、学内教職員向けの情報等を提供するサイトは個別運用しており、管理者不在のページが発生する事態の発生や、サイト毎に更新手段が異なる等業務の混乱を招く事もあった。新システムでは、これらサイトの CMS 化を図り更新業務内容の統合を図った。 本講演では、新たに認証システムの構築が必要となった背景・構築・運営等について述べる。

1 はじめに

熊本大学では、WEB への情報発信業務フローとコンテンツ管理業務の改善に向け、2010 年度より学内職員のみで構成されるスタッフで大学公式 WEB サイトのリニューアルへの取り組みを行い、2012 年 3 月末に公開を行った。[1]

これまで、大学公式 WEB サイトや教職員向け WEB サイトやその他のコンテンツは、ばらばらに管理され、各システム毎に CMS の導入状況や、利用 CMS の相違があり、情報の更新作業などにおいて混乱を招く要因となっていた。

本リニューアルでは、コンテンツを新たに構築した CMS へ集約し、記事公開への編集フローを構築し導入する事で、これらの問題解決を図り現在に至る。[2]　CMS については、編集フローの構築が可能であることや、熊本大学で導入している CAS 認証に対応可能であること、コンテンツ毎に編集/閲覧権限を設定できること、CSS によるデザインのカスタマイズができること等を考慮して、Plone 4 を使用してシステム構築を行った。[3][4]

ここで、CAS 認証にはユーザ ID とパスワードの検証のみしか行われないので、ユーザ ID に対する編集/閲覧等の権限情報の管理は別途行う必要がある。 本稿では、CAS 認証と連携する権限情報管理を行う認証構築について述べる。

2 認証システムの構築

想定する運用では、数千のユーザ登録と、組織毎に権限レベルの異なるグループの設定を準備することで、数百グループの登録が必要であり、人事異動等で定期的に発生する情報更新を Plone 自体の管理画面で直接行うことは容易ではない。そこでユーザとグループ情報は LDAP 上で管理を行い、Plone は LDAP を参照する方式を採用した。

Plone4 はユーザ認証、権限管理、グループ管理にそれぞれ別のプラグインを利用することが可能である。　グループ管理と権限管理に LDAP プラグインを、ユーザの認証には CAS プラグインを指定することで、LDAP によるユーザ・グループ管理と CAS 統合認証を連携させることができた。

2.1 LDAP システム構成

導入時現在での OpenLDAP リリースバージョンは 2.4 系である。　設定やトラブルの情報で主にネット上で情報は、slapd.conf ファイルを編集して設定する 2.2 系のものが殆どで、ldapmodify コマンド等で LDIF を追加変更することで設定を行う slapd-config 方式に替わった 2.4 系の情報は少なく、構築には手間がかかってしまった。

大学 WEB システム構成を図 1 に示す。

ユーザ・グループの更新は LDAP マスター上で行い、LDAP スレーブは、レプリケーション機能を用いて、LDAP マスター上のデータの保持を行う。　このようにデータの更新系と参照系を分離することで、セキュリティの向上を図った。

LDAP のレプリケーションには、refreshOnly と refreshAndPersist の 2 つのモードがある。

refreshAndPersist モードは、初期動機完了後も接続を保持し、データ更新を素早く反映させることができるが、その分負荷が高くなってしまう。本システムは、頻繁にユーザ・グループの変更が

発生することはない事を考慮し、refreshOnly モードを採用した。

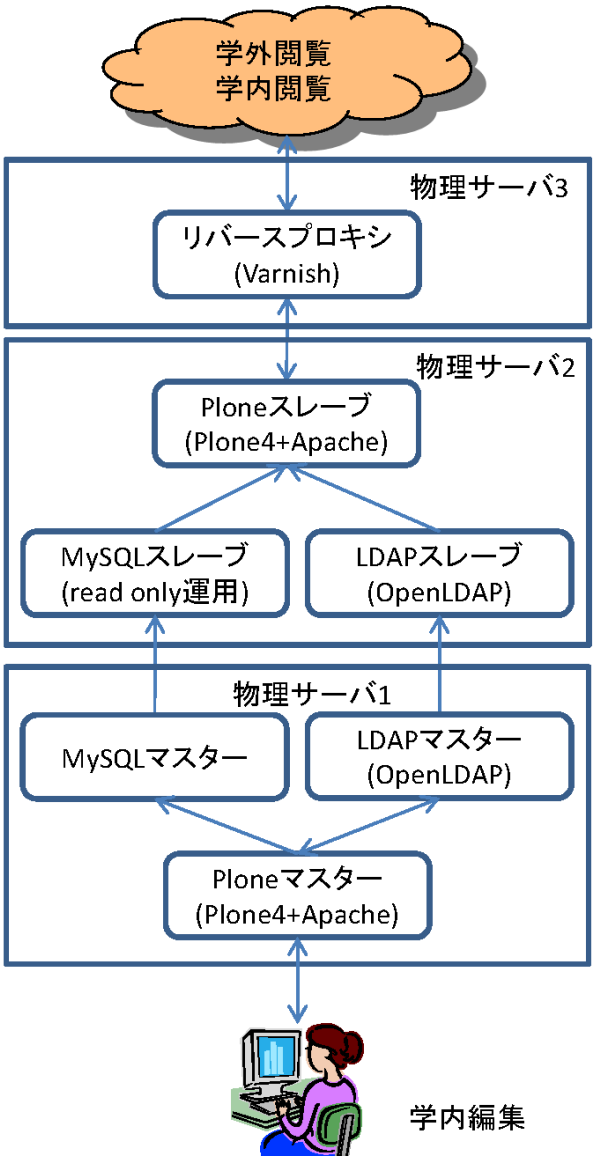

図 1 熊本大学 Web システムの構成 [1]

図２に、LDAP マスターを provider として、LDAP スレーブを consumer として、設定を行った設定用 LDIF ファイルの一部を紹介する。

provider では index の追加と syncprov モジュールのロード、consumer では、index の追加と olcSyncRepl・olcUpdateRef 項目の追加と設定が必要となる。

```
●LDAP マスター (provider)
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryCSN eq
-
add: olcDbIndex
olcDbIndex: entryUUID eq

dn:olcOverlay=syncprov,olcDatabase={1}hdb,
cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpNoPresent: TRUE

●LDAP スレーブ (consumer)
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: entryUUID eq
-
add: olcSyncRepl
olcSyncRepl: rid=0 provider=ldap://プロバイダ
を指定　binddn="接続 DN"
bindmethod=simple credentials=パスワ
ード　searchbase="検索 DN"
logbase="cn=accesslog"
logfilter="(&(objectClass=auditWriteObject)
(reqResult=0))" schemachecking=on
type=refreshOnly interval=00:00:05:00
syncdata=accesslog
-
add: olcUpdateRef
olcUpdateRef: ldap://プロバイダを指定
```

図２ LDAP 設定 LDIF ファイル(抜粋)

2.2 ユーザ・グループの設計

今回のシステムでは、学外に公開するコンテンツについては全て広報戦略ユニットのチェックを得た後に公開する。　また編集ワークフローとして、「制作者」「承認者」「総合管理者」の３種類のユーザ区分を設けた。

「制作者」は各部局でホームページ用コンテンツの作成を行うスタッフに対応し、「承認者」は各部局の記事への決済を行う課長等に相当する。

「総合管理者」は広報戦略ユニットの学外ホームページ責任者に対応し，コンテンツ公開に関する最終権限を持っている。

公開コンテンツは、各部局の「制作者」が作成

し、「制作者」はコンテンツ作成後に同部局「承認者」へ承認の依頼を行う。　もしコンテンツに不備があれば「制作者」に差し戻しを行い、なければ「承認者」はコンテンツの「公開依頼」を「総合管理者」に対して行う。　「総合管理者」は「公開依頼」のあったコンテンツの内容を確認し，問題がなければコンテンツの「公開」を行う。

権限付与については、LDAP 上で、部局毎に「一般グループ」「制作者グループ」「承認者グループ」を作成し、Plone サイドで各グループに権限を設定する事で実現している。

ユーザ情報は、”メールアドレス”・”氏名”、”CAS 認証 ID” 情報を持つため、inetOrgPerson オブジェクトクラスの mail 属性・cn 属性・uid 属性を利用し作成した。

Plone では LDAP 上に登録されたグループ情報を取り扱うには、メンバー情報を uniqueMember 属性または member 属性で複数登録が可能なスキーマで定義されたオブジェクトクラスである必要がある。　本システムでは、メンバー情報を取り扱うだけで良かったので、uniqueMember 属性を複数持つ事ができる groupOfUniqueNames オブジェクトクラスを利用し作成した。

図３にユーザ DN・グループの設計観念を紹介する。

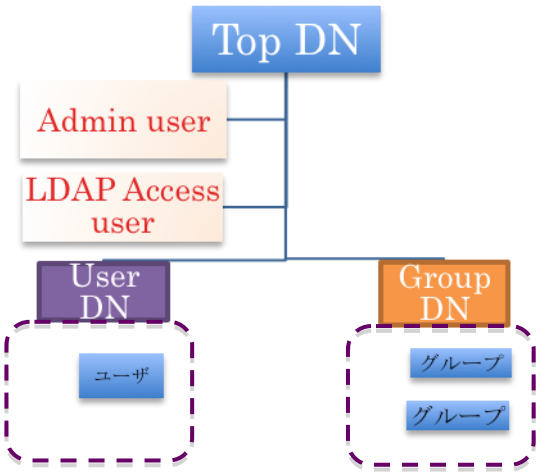

図３　設計した LDAP ディレクトリ構造

次に図４に設計すた LDIF の例を紹介する。

●Top DN
dn: dc=kuweb,dc=kumamoto-u,dc=ac,dc=jp
objectClass:　top
objectClass:　dcObject
objectClass:　organization
o:　kuweb
dc:　kuweb
description:　KUWEB LDAP

●Admin user
dn:　cn=admin,dc=kuweb,
dc=kumamoto-u,dc=ac,dc=jp
objectClass:　simpleSecurityObject
objectClass:　organizationalRole
cn:　admin
description: KUWEB LDAP administrator
userPassword:　xxxxxxxxxxxxx

●User DN
dn:　ou=KUWEB-User,dc=kuweb,
dc=kumamoto-u,dc=ac,dc=jp
objectClass:　organizationalUnit
ou:　KUWEB-User

●Group DN
dn:　ou=KUWEB-Group,dc=kuweb,
dc=kumamoto-u,dc=ac,dc=jp
objectClass:　organizationalUnit
ou:　KUWEB-Group

●ユーザ例
dn:　uid= abcdxxxxx,ou=KUWEB-User,
dc=kuweb,dc=kumamoto-u,dc=ac,dc=jp
objectClass:　inetOrgPerson
objectClass:　top
uid:　abcdxxxxx
cn:　帆下　歩毛男
sn:　abcdxxxxx
mail:　hoge-hoge@tmp.kumamoto-u.ac.jp

●グループ例
dn:cn=WRITER-Kansa,ou=KUWEB-Group,
dc=kuweb,dc=kumamoto-u,dc=ac,dc=jp
objectClass:　top
objectClass:　groupOfUniqueNames
uniqueMember:　uid= abcdxxxxx,
ou=KUWEB-User,dc=kuweb,
dc=kumamoto-u,dc=ac,dc=jp

図４　設計した LDIF の例

3 運用事例の紹介

3.1 ユーザ・グループ情報の更新

主な人事異動時期は、4 月と１０月の年 2 回であるが、教員の異動等全学での異動状況は毎月発生する事になる。　本システムは、全学教職員用サイトでもある為、人事異動状況似合わせて速やかにユーザの登録、権限情報の設定を行わねばならない。　また LDAP は、ldapmodify コマンドで、現在の登録内容との差分 LDIF を用いて、登録内容の追加/修正/削除処理を行う事ができるが、LDIF ファイルに間違いが発生したり、更新作業中にLDAPのトラブルが発生してしまった場合には、トラブル発生直前の更新までは完了してしまうが、残りの更新は実行されず、データのロールバックも出来ない。　一旦このような状況になると、どこまで更新が実行されたかを突き止め、新たな更新作業の為の LDIF の作成から行わなければならなくなり、時間手間を取られてしまう羽目になる。　また、更新中でのLDAP参照には不整合が発生してしまうケースも考えられる。様々な状況を考慮して、ユーザ・グループ情報の更新作業は、毎回新たな User DN、Group DN を作成し、登録時時点のデータを全て新規データとして登録するように取り決めた。　データ更新完了後に、Plone 側でユーザ情報およびグループ情報の参照先を、新規作成した User DN、Group DN へ変更する事で、データ追加時のトラブルをさける事だけでなく、旧データへのロールバックも参照先を元に戻すだけで可能になる。　ユーザ情報となる、”CAS 認証 ID”・”氏名”・”メールアドレス”については、人事労務ユニットより情報企画ユニットへ連絡があり、情報基盤センターにて CAS 認証サーバへ登録されるデータを利用する。　また、グループ情報については、広報戦略ユニットが取り纏めを行い、LDIF の基となるデーラをエクセルに作成する。　この２つのデータをマージして LDIF ファイルを生成するスクリプトを作成する事で、業務の簡略化を行った。

4 まとめ

今回の公式/教職員 Web サイトリニューアル プロジェクトは、学内教職員のみから構成されるチームで導入から運用まで実施されている非常に革新的な取り組みであると考えている。　私も含めこの様な大規模なシステムを構築するプロジェクトの経験がないメンバーが殆どであった。

LDAP の導入にしても、想定されるデータ件数を見積もり、データ登録のテストを行い、登録にかかる時間測定や、負荷確認、データバックアップとレルトア手法の確立など、様々な検証を行い運用までたどり着いたが、実運用でのユーザ更新作業を行った際にログインに不具合がおこるトラブルが発生した。　当初 LDAP の不具合も考えられたが、原因を究明した結果、コンテンツを作成した事があるユーザを削除してしまうと発現する不具合である事がわかった。　事前にこの様な状況も確認できるような経験を積む事は非常に大切な事であると共に、運用面での体制等様々な面で重要課題がある事を学ぶ機会となった。

参考文献

[1] 永井孝幸、杉谷賢一、久保田真一郎、木田健、松葉龍一、坂本瑞穂、伊澤睦、岩永菜穂子、中村直美、谷口勝紀、上田誠、後藤正三、河津秀利、Plone4 による熊本大学公式 Web サイトの構築、大学 ICT 推進協議会 年次大会 2011 予稿集、pp268-275、2011

[2] 岩永菜穂子、松葉龍一、中村直美、河津秀利、坂本瑞穂、伊澤睦、木田健、林恵里、谷口勝紀、青木敏裕、竹本浩、野口緑、久保田真一郎、永井孝幸、宇佐川毅、中野裕司、杉谷賢一、熊本大学 公式/教職員 Web サイトリニューアル プロジェクト、大学 ICT 推進協議会 年次大会 2012 予稿集

[3] 坂本瑞穂、伊澤睦、久保田真一郎、永井孝幸、松葉龍一、熊本大学公式 Web サイトの構築ー CSS 等のカスタマイズによる Web サイトデザインー、大学 ICT 推進協議会 年次大会 2011 予稿集、pp499-502、2011

[4] 坂本瑞穂、伊澤睦、木田健、川津秀利、久保田真一郎、永井孝幸、松葉龍一、利用者のためのウェブサイトデザイン-公式ウェブサイトと教職員向け情報サイトのシステム統合-、大学 ICT 推進協議会 年次大会 2012 予稿集