LDAP サーバを利用した認証システムの一元化

遠山　紗矢香
情報学部技術部

1. 概要

情報学部では、基盤システムの一部として導入した LDAP[1]サーバが稼働している。LDAP サーバは、ユーザのアカウント名・パスワード・氏名・メールアドレス等の個人情報を格納しており、他のシステムやサーバからの要求に応じて個人情報を提供したり、照合したりする。中でも、アカウント名とパスワードの照合によるユーザ認証機構が一般的である。個人認証が必要なシステムを構築する際、ユーザ ID・パスワードのアカウント情報を LDAP サーバへ問い合わせるよう実装することで、既に LDAP サーバへ登録されているアカウント情報をそのまま利用することができる。本稿では、(1) マイクロソフト社のソフトウェアダウンロードサイト (2) 著者が構築したソフトウェアライセンス申請用 CGI の 2 つの異なる web サービスにおける個人認証を、情報学部の LDAP サーバを用いて構築した。そして、ユーザが既存のアカウントで新しいサービスを利用できるようにした。

2. 背景

近年の業務電子化に伴い、ユーザ 1 人が管理するアカウントの数は非常に多くなっている。そして、多くのユーザが感じているように、管理アカウントが多くなればなるほどパスワードの管理はおろそかになりやすい。パスワードが流出すると最悪の場合、悪意ある他者による「なりすまし」によって情報流出やデータ改ざんなどのセキュリティ事故が引き起こされる可能性がある。大学など公共性の高い組織のシステム管理者は特に、ユーザ 1 人のわずかな気の緩みが、組織の社会的信用を失墜させてしまう危険を常に警戒する必要がある。

情報セキュリティへの関心が高まっている昨今では、このような問題を回避するために、一度のログインで組織内の全システムを利用可能にする「シングルサインオン(SSO)」の実現[2]や、LDAP(Lightweight Directory Access Protocol)サーバによるアカウント管理の効率化[3]など、アカウント一元管理化への動きが顕著になりつつある。

著者の所属学部では、学部内基盤システムとして導入した LDAP サーバが稼働している。学部所属の教職員・学生は全員、この LDAP サーバで管理されている自身のアカウントを日々メール送受信等に利用している。本学部内で新しいシステムを構築する場合、この LDAP サーバを用いたユーザ認証機構を実現することで、アカウントの一元管理を実現できる（図 1)。つまり、ユーザは使い慣れたアカウントを用いて、新しいシステムの利用を開始できる。

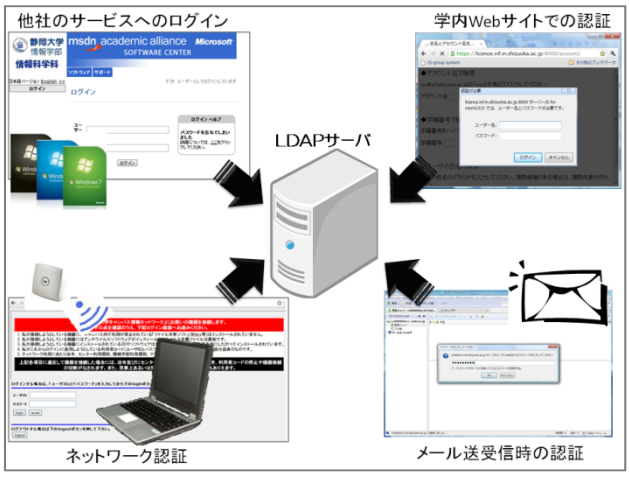

図 1　LDAP サーバを利用した認証の統合

3. LDAP を利用した認証統合の利点

LDAP サーバを利用して認証機構を統合すると、ユーザとシステム管理者の双方に利点がある。

ユーザは、新規アカウント情報を覚える負担から解放されるため、パスワードのメモ書きなど危険なアカウント管理方法が減少すると期待できる。

管理者にとっての利点の 1 つ目は、パスワード忘れに対する再発行の手間や、古いアカウント整理などの管理業務量を従来通りのまま維持できることである。特に、学生用アカウントは、卒業等によりいずれは必ず削除する時が来る。ユーザ不在の古いアカウントは悪用されやすく、また一部システムでは利用者を「在学生」と決めている場合もあるため、利用完了後には可能な限り速やかにアカウントを削除すべきである。削除作業の際、LDAP サーバによってアカウント情報を統合していれば、作業は一度で完了するが、システムごとに別々のアカウントを発行していた場合、全システムのアカウントを個別に削除する手間が生じてしまう。

管理上の利点の 2 点目として、アカウントを統合しておくと、異なるシステム間でのログファイルを確認する手間が少ないことが挙げられる。ユーザの氏名とアカウント名が全てのシステムで一意に対応していれば、異なるシステム間で特定のユーザのログを抽出したり比較したりすることが容易に行える。他方、あるユーザがシステムごとに別々のアカウント名だった場合、本質的な作業に先立って対応付けを行う必要がある。

3. 作業対象

著者の所属する情報学部においてサービスを開始した 2 つの web システムの認証を、既存のユーザアカウントで行えるようにするために、情報学部内に既に設置されている LDAP サーバと連携した認証システムをそれぞれ構築した。web システムはそれぞれ、(1) マイクロソフト社の MSDN アカデミックアライアンスプログラム ソフトウェアダウンロード用の web サービス (2) 著者が情報学部向けに構築したアンチウイルスソフトのライセンス申請用 web サービス である。LDAP サーバ群と(1) (2) のサーバとの関係を図 2 に示す。

(1) MSDNAA ダウンロードサイト

著者の所属学部では「MSDN アカデミックアライアンス(MSDNAA) Developer Edition[4]」を購入している。本学部の教員と学生、一部職員は、MSDNAA のサービスを利用することで、マイクロソフト社の 200 タイトル余りのソフトウェアをインストールすることができる。

本学部でのソフトウェアの提供は、一昨年度まで、ユーザが希望するソフトウェアをメール等で申し込み、DVD とライセンスキーを技術部にて手渡しする方式を採っていた。著者は昨年度、業務負荷低減のため、MSDNAA にて無償提供されている「Hosted ELMS[5]」と呼ばれるクラウド型のサービスへユーザ登録を行い、認証機構を整備して、ユーザ個人が学部のアカウントを用いてログインし必要なソフトウェアを

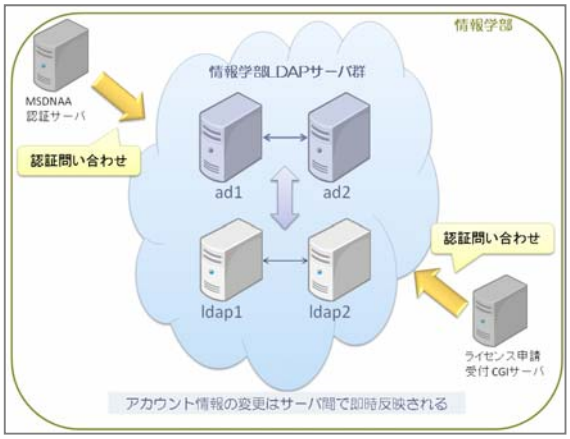

図 2　LDAP サーバ群との通信

自由にダウンロードできる環境を構築した。以降、Hosted ELMS を利用した MSDNAA ソフトウェアをダウンロードするための web サイトを、「MSDNAA ダウンロードサイト」と呼ぶ。

本サイトの整備によって、技術部の仕事は、サイトへログインするためのアカウント管理業務と、サイトそのものの利用方法サポートが中心となった。なお、ユーザ認証方式は、LDAP サーバを利用する方法と、ローカルアカウントを作成する方法の二択から、LDAP サーバの利用を選択した。

(2) 学部内ライセンス申請用サイト

著者の所属学部では、校費で購入された計算機のウイルス感染を防ぐため、アンチウイルスソフトの年間ライセンスを一括購入している。例年、技術部にて、学部の教職員に希望ライセンス数を尋ね、メールの返信を集計して購入ライセンス数を決めている。しかし、メール集計作業が煩雑なため、教職員がライセンス数を登録するための web サイトを perl による CGI として構築した。web サイトには、登録の手違いや無関係な学生による申請を見分けるため、LDAP サーバを利用したユーザ認証を設けた。

4.構築手順

4-1. 認証機構構築の手順

(1) MSDNAA ダウンロードサイト

今回著者が構築したのは、(1) ユーザのアカウント名・パスワードの組み合わせが正しいかを学部内 LDAP サーバへ問い合わせる (2) MSDNAA ダウンロードサイトへユーザ情報と共にログイン要求を送信する という 2 段階の処理である。ユーザから見た全体の流れを図 3 に示す。

① MSDNAA ダウンロードサイトのログイン画面にて「ログイン」を押下する
② 学部内の認証ページが表示されるので、アカウント名とパスワードを入力して「送信」を押下する
③ (入力されたアカウント情報は学部内 LDAP サーバにて照合される)
④-1 アカウント情報が正しければ、MSDNAA ダウンロードサイトにログインする
④-2 アカウント情報が間違っていれば、警告文が表示され③のページに戻る

(2) 学部内ライセンス申請用サイト

ライセンス申請用サイトは全体を構築したため、(1) ユーザのアカウント名・パスワードの組み合わせが正しいかを学部内 LDAP サーバへ問い合わせる (2) ライセンス申請フォームを用意する という 2 つの作業が必要であった。ユーザから見た流れを図 4 に示す。

① 学部内ライセンス申請用サイト URL にアクセスすると、Apache BASIC 認証ダイアログが表示されるので、アカウント名とパスワードを入力し「ログイン」を押下する
② (入力されたアカウント情報は学部内 LDAP サーバにて照合される)
③-1 アカウント情報が正しければ、学部内ライセンス申請用サイトにログインする
③-2 アカウント情報が間違っていれば、再度アカウント情報の入力を求める
④ (ユーザに入力されたライセンス情報の csv バックアップファイルが作成される)

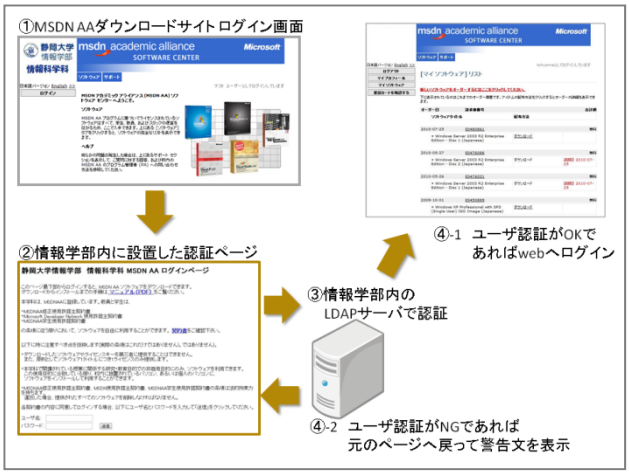

図 3　MSDNAA ログインまでの流れ

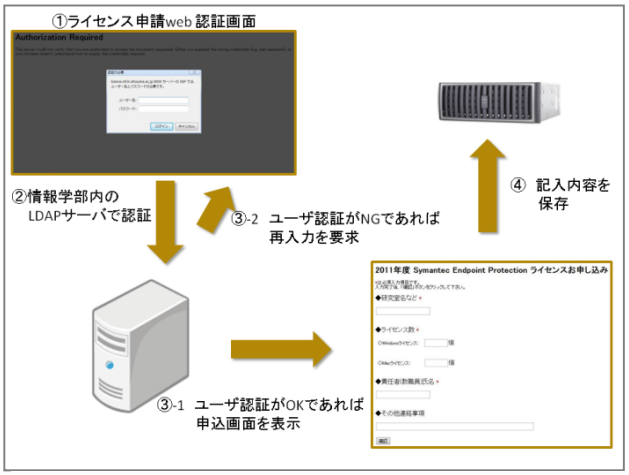

図 4　ライセンス申請ログインまでの流れ

4-2. 内部処理の流れ

学部内 LDAP サーバと連携した認証機構を実現した内部の処理について、以下に記す。

(1) MSDNAA ダウンロードサイト

1. MSDNAA ダウンロードサイトでの設定を行う
   ・「校内認証」を「テストモード」に設定して、サイト管理者のローカルアカウントによるログインと LDAP 連携ログインの両方を併用できるようにした。
   ・校内認証 URL として、3 で作成するプログラムを公開する URL を決めた。
   ・校内用 CGI サーバ IP として上記 URL のグローバル IP アドレスを設定した。
2. 学部内のサーバにて web サーバソフトを稼働させる
   ・3 で作成するプログラムを web で公開するために、web サービスを稼働させた。今回は既に稼働していた Microsoft Internet Information Services 6 を利用した。
3. 学部内 LDAP サーバへ認証を委譲するプログラムを稼働させる
   ・C# (Microsoft .NET) によって開発を行った。
   前任者の参考プログラムが C#で書かれていたこと、公式マニュアル[6]のサンプルコードが C#と同じく.NET Framework の構成要素である VB.NET で記述されていたため、C#を選択した。

(2) 学部内ライセンス申請用サイト

1. 学部内のサーバにて web サーバソフトを稼働させる
   ・2 で作成するプログラムを web で公開するために、web サービスを稼働させた。今回は既に稼働していた Apache2.2 を利用した。
2. 学部内 LDAP サーバへ認証を委譲するための設定を行う
   ・httpd.conf (Apache の設定ファイル) にて、BASIC 認証のユーザ情報の問い合わせ先を、学部内 LDAP サーバに設定した。

5. 結果

(1) MSDNAA ダウンロードサイト

主な成果：

2009/10/23 から 2010/12/16 現在までの 1 年強の運用期間について報告する。調査対象は、

本サイト内部で記録されている管理者用ログ・認証時に情報学部内のサーバへ記録しているログ・IIS のアクセスログの 3 点である。学部全体のユーザ数はおよそ 1,100 名である。

まず、本サイトへのアクセスは、515 件であった。ユーザがダウンロードしたソフトの本数の総計は 238 本であった。なお、利用したユーザは 130 名であった。本サイトの運用開始前は年間 10 件程度の利用に留まっていたことを考えれば、大きな前進だと考えられる。

認証機構そのものへの質問はなかったが、本サイトの URL や、本サイトの使い方についての質問はしばしば寄せられるようになった。しかし、利用率の飛躍的な向上と比較すれば、増加した業務量ははるかに少ないと言える。

付随した成果：

本サイトの運用開始をメーリングリストにて学部全体へ案内したことで、いくつかの研究室では学部で MSDNAA を契約していることを関知しておらず、研究室単位で購入を行っていたことが発覚した。学部全体でのライセンス購入方法の見直しに寄与することができた。

さらに、2010 年度からは、新しい販売形態として、ダウンロードサイトのみ(貸出用 DVD メディアなし)のパッケージを選択可能になった。従来のメディア付きパッケージの半額未満であるため、経費の削減にも貢献することができた。

(2) 学部内ライセンス申請用サイト

2010/10/29 から、2010/11/15 の間に限定して開設された本サイトの利用について報告する。調査対象は、ライセンス申請用サイトにて保存している申請内容のバックアップファイルと、Apache のログファイルである。申請者は最大で約 75 名である。

およそ 60 名が、本サイトを経由してアンチウイルスソフトのライセンス数の申請を問題なく完了できた。本サイトの URL 等など基本的な部分の問い合わせは数件寄せられたが、認証についての問い合わせは寄せられなかった。なお、Apache のログを参照することで、ログインしたユーザをさかのぼることができる。この結果、不明なアカウントからの申請がなかったことも確認できた。

web サーバ等の環境構築は、別目的で稼働中だった既設サーバを利用したため、本サイトの構築とテストは 1 日で完了した。LDAP サーバを利用することで、単体でのアカウント登録や次年度以降のアカウント入れ替えも不要なシステムを短時間で構築することができた。

6. まとめと展望

ユーザ認証が必要な web サービスを新しく構築する際、学部内にて運用されている LDAP サーバにてアカウント情報を照合することで、新しいアカウントを発行することなく 2 つのサービスを開始することができた。ユーザとシステム管理者双方の負担を増すことなく、技術部のサービスを拡充できたことは意義深いと考えられる。

LDAP サーバを利用した認証は、特に突発的なニーズで新設されるサービスにおいて利点が大きいと考えられる。アカウント管理業務を、システム本体の構築とは切り分けて考えることができるためである。Ruby on Rails[7]などのアジャイル型開発手法が一般的となった近年では、管理者が現場の多様なニーズに合わせて、ごく少ないコストでシステム開発を行わなければならないことが多い。ユーザ認証が必要なシステムを構築する場合、LDAP サーバ等既存の認証システムと連携させることで、ユーザ認証機構やアカウント発行などの手間を

省略することができる意味は大きい。

今後は、SSO による学部内認証システム実現を見据えつつ、LDAP サーバをより効率的かつ安全に運用していくための知識と技術を身につけていきたい。

参考文献

[1] Wahl, M., Howes, T., Kille, S. “RFC2251: Lightweight Directory Access Protocol (v3)”, ftp://ftp.rfc-editor.org/in-notes/rfc2251.txt, 参照 Jan. 20, 2011.

[2] 藤村喬寿, 西村浩二, 相原玲二, “大規模キャンパスネットワークにおける SSO 認証の設計と実装”, 電子情報通信学会技術研究報告 IA インターネットアーキテクチャ, vol.109, no.299, pp.13-18, November 2009

[3] データーネット, 入門 LDAP/OpenLDAP ディレクトリサービス導入・運用ガイド, 秀和システム, 東京, 2007.

[4] Microsoft, Inc., “MSDN アカデミックアライアンス“, http://msdn.microsoft.com/ja-jp/academic/,参照 Jan. 20, 2011.

[5] Microsoft, Inc., “MSDN アカデミックアライアンス Hosted ELMS とは”, http://www.microsoft.com/japan/academic/elms/, 参照 Jan. 20, 2011.

[6] e-academy, Inc., “ELMS for MSDNAA Integrated User Verification Customer Implementation Guide”, http://support.e-academy.com/docs/ELMS_IntegratedUserVerification_ImplementationGuide_MSDNAA.pdf, 参照 Jan. 20, 2011.

[7] 前田修吾, Rails によるアジャイル Web アプリケーション開発 第 3 版, オーム社, 東京, 2009.