2008－IOT－2 (5)
2008／7／24

ゆるやかに結合したLDAPツリーを用いた統合認証システムに関する研究

土屋 英亮† 丸山 一貴‡ 高田 昌之†

電気通信大学 情報基盤センター† 東京大学 情報基盤センター‡

要 旨

現在、組織内に複数存在する認証システムを一つにまとめ、統合認証システムを構築することがよく行なわれている。統合認証システムは内部統制に必要であったり、組織内の人員を一元管理するのに利用されたり、あるいはパスワードポリシーを統一運用するために利用される。

今まで利用されてきた複数の認証データベースをまとめ、統合認証システムを構築することは、各システムで利用されてきた各個人のアカウントやパスワードを一つに統合する作業が必要となる。この作業は、アカウントの変更を必要とすることが多く、管理者及び利用者に多大な負担を強いる。

本稿では、電気通信大学情報基盤センターで運用中であるゆるやかに結合したLDAPツリーを用いた統合認証システムを紹介する。この統合認証システムは完全な統合を行なう前の前段階のシステムとして理解することができる。このシステムにより完全な統合認証までの移行をよりスムーズに行なうことが可能となる。

A study of the Integrated Authentication System with the loose coupled LDAP trees

Hideaki Tsuchiya† Kazutaka Maruyama‡ Masayuki Takata†

Information Technology Center, The University of Electro-Communications†
Information Technology Center, The University of Tokyo‡

Abstract

Today, the integrated authentication systems are used instead of the existing two or more independent authentication systems in the organisation. The integrated authentication systems are necessary to enforce the internal controls and the password policy.

For the construction of the integrated authentication system, it is necessary to integrate the authentication databases that are used by each systems. The integration of authentication databases is difficult process.

We introduce the integrated authentication system with the loose coupled LDAP trees, which is working in Information Technology Center of The University of Electro-Communications. This integrated authentication system can be understood as the system for the phased conversion to the complete integrated authentication system.

1 はじめに

大学をはじめ多くの組織で、ユーザーの利便性を向上するために、組織内に複数存在する認証システムを一本化し、統合認証システムを構築することが行なわれるようになっている [1]。統合認証システムにより、ユーザーはIDとパスワードの組を一つだけ記憶及び管理するだけで済むようになる。また、組織内で異なるポリシーで管理されていたIDとパスワードを単一のポリシーで運用できるようになる。これは各組織での情報セキュリティポリシーの運用を容易にする。さらに、統合認証システムに様々な属性値を付加することにより、一元的にユーザー毎に利用可能な情報システムを分類することが可能となる [2]。統合認証システムのアクセスログを保存しそれを解析することにより、いつ誰が何のシステムを利用しているかを一括して監視できるようになる。これは内部統制の実行に欠くべかざる要素の一つであるといえる。

しかしながら、統合認証システムを構築することは非常に困難である [3]。第一に、統合認証システムを構築し、運用することに関して組織全体の同意を得なければならない。同意を得ないで統合認証システムを構築したとしてもそれはどこからも利用されないシステムになってしまう。第二に、今までは組織内のそれぞれの部局で発行していたIDを統一しなければならない。今まで、各部局の独自性に任されていたIDの発行基準やその形式を統一するのは非常に困難な仕事である。特に、組織の構成員全てに一意にIDを割り当てることと、そのIDの形式が長期間にわたって有効に機能することが求められる [4, 5]。第三に、組織が保有する複数の情報システムが統合認証システムを利用するようにしなければならない。この作業は、今までローカルデータベースでIDとパスワードを管理していた情報システムの認証システムのソフトウェアを変更することと、その情報システムに蓄積されているデータの中でIDに関連する箇所を全て変更することの二つからなる。前者は比較的容易であるが、後者は注意を要する。最後は、更なる利便性の向上を期待して、各情報システム間でのログイン情報の共有、すなわちシングルサインオンシステムの導入を行なうことができれば、統合認証システムとしてはほぼ完全なものになったといえる。これらを全て行なうには、作業量やコスト、さらには組織内の政治的な問題までを解決する必要がある。

著者の所属する電気通信大学 情報基盤センターでは、2007年2月にシステム更新を行なった。更新の対象は、情報基盤センターで運用する教育系システム及び研究系システム、教育支援システム、学内ネットワーク機器である。今回の更新では、新たな試みとして今まで独立して管理していた教育系システムと研究系システム、教育支援システムの認証システムを統一した。本稿では、その際に開発し現在も運用を行なっている統合認証システムについて述べる。認証システムへの要求事項と、その解決方法について述べる。最後に運用時の問題点について述べる。

2 システムの概要

電気通信大学 情報基盤センター（以下、本センターと記す）では、今まで、主に一部の研究者や学生が利用する課金制の研究系システムと、全学の構成員が利用可能で無課金制の教育系システム、教育系システムを用いて講義を行なう教員のための教育支援システムの三つのシステムを運用している。研究系システムは高速計算サーバとその上で動作する科学技術計算用アプリケーションからなり、教育系システムは計算機リテラシー教育に利用する端末とそれらに接続された中規模サーバからなり、教育支援システムは教材提示用ウェブサーバからなる。本稿では、主に研究系システムと教育系システムの統合認証について記述する。

現在は、2007年2月に更新を行なったシステムが稼動している。中核となるのは大型サーバのSun Fire E25Kであり、このサーバをドメイン分割して、研究系システムと教育系システム、教育支援システムのサーバを構築している。教育系端末にはリッチクライアントとしてiMacを採用している。そのため教育系サーバへの依存は減少している。

今回の更新では、この大型サーバとは別個に認証用システムを用意した。LDAP[6] サーバとしてSun One Directory Server 5.2[7] が動作するSun Solaris 9サーバが2台と、その前段に設置されているL7スイッチである (図1)。これらは非常用発電器が接続された無停電区画に設置され、一日一回のバックアップが行なわれている。LDAPサーバはデュアルマスターとして構成されている。無停電化されてい

ることと、2台のサーバをデュアルマスター構成にしたことより、耐障害性は十分に確保されていると考えている。

今回の更新以前のシステムでは、ユーザーの認証情報は各システム毎に独立したNISによって管理されていた。研究系システムのユーザーアカウントはユーザーの希望するアカウントを自由に選択できるようになっていた。教育系システムでは、ユーザーに自由に選択させることなしに学籍番号や職員番号を元にして生成したアカウントを強制的に割り当てていた[1]。メールアドレスはというと、UNIXシステムのMTAをそのまま利用しているために、アカウントがメールアドレスになる。研究系システムは自由にメールアドレスを選択できるが、教育系システムは学籍番号や職員番号を元にしたものが利用される。このように研究系システムと教育系システムでは、ユーザーIDそのものに差別化が行なわれている。しかしながら、教育系システムのユーザーからは、自由にIDが選択できない、メールアドレスが選択できない等の不満が聞こえてくることがある。

研究系システムのアカウントは、申請書の提出により生成され、一年毎に更新申請を行なってもらうことで、ユーザーの存在確認を行なっている。教育系システムのアカウントは、入学や就職と同時に生成され、卒業や退学及び退職と同時に削除される。

パスワードの有効期限は、本センターのポリシーとして二つのシステムとも90日となっており、それを過ぎても変更されない場合は、自動的にロックされるようになっている。ロックの解除は身分証明書と解除申請書の提出によってのみ行なっている。

3 統合認証システムの構築

3.1 本センターにて必要とされる統合認証システムの要件

前節にて説明したように、本センターでは以前よりNISを利用して認証システムを構築していた。NISによる認証システムは運用実績があり、また自作の管理ツールも充実していたのだが、NISでは性能が不足していて制限のある運用しか行なえなかった。特に利用者が一斉にパスワードを変更したとき

[1]講義を担当する教員には希望するアカウントを割り当てている。これは受講する学生に対して教員が誰であるかをわかりやすくするための措置である

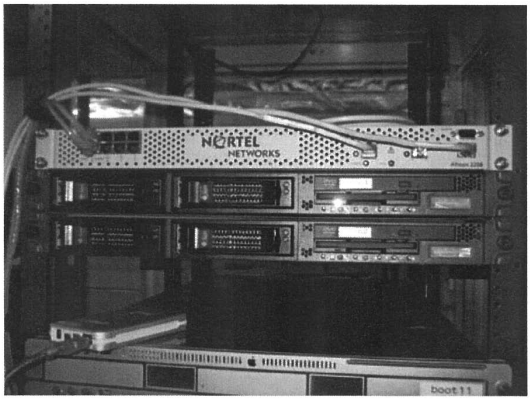

図 1: LDAPサーバとL7スイッチ

に、マスターサーバからセカンダリサーバへのパスワードファイルの配信が不安定になることが判明したため、マスタサーバからセカンダリサーバへの情報配信は15分おきに行なうようにしていた。そのため、パスワードを変更してすぐに、その変更が有効であるかを確認することができず、コンピュータリテラシーを教育している教員からは不評であった。

今回のシステム更新にて、信頼性の高いLDAPサーバを導入することができたので、本センターではこれを認証システムの中核にすることにした。

LDAPは木構造によって階層的に構造化されたディレクトリをアクセスするためのプロトコルである。ディレクトリの各ノードには認証情報だけではなく、メールアドレスや電話帳等を格納することが可能であり、認証システムだけではなく、多機能データベースとしても利用可能である。しかしながら本センターでは、認証システムとしてのみLDAPサーバを利用することとし、それ以外の情報をLDAPサーバで管理することは将来の課題とした。

研究系システムと教育系システムの認証システムを一つのLDAPサーバ上で構築する場合の選択肢として、本センターでは三つの方式を検討した。それぞれの方式とその欠点を以下に示す。

1. 研究系システムと教育系システムの二つの認証システムを構築する。基本的に今まで運用していたそれぞれのNISサーバの情報をLDAPサーバに転送して運用すればよい。

2. 研究系システムのアカウントを教育系システムのそれに統一して運用を行なう。研究系システムの自由に選択できるアカウントという差別化された特長は失われるが、パスワードが共通化されるので、ユーザーに取ってみれば管理しなければならないパスワードが減ることとなり、利便性は向上する。しかしながら、研究系システムに教育系システムのユーザーがログインできないようにアクセス権限を定義して参照する仕組みを仕込まなければならない。
3. 教育系システムのアカウントを研究系システムのように自由に選択できるようにして、統一運用を行なう。しかしこれは非常に難しい。本学の全構成員全員の希望アカウントを調査し、一意になるようにアカウントを割り当て現在利用しているアカウントから移行することは困難である。新入生から順次移行するにしても、計算機システムの専門的教育を受けていない入学直後にアカウントを生成しなければならないことので、時間的な制約も含めて難しい。また、2と同様にアクセス権限の問題も発生する。

このようにアカウントとパスワードの統合は、パスワード管理の利便性を向上させるが、本センターの統合認証システムの運用における作業量の増加や今まで利点としていた各システムの差別化された特長が失われることがわかった。二つのシステムの認証情報の統合を行ないたいのならば、研究系システムのアカウントを教育系システムのそれに合わせる2の方法が最も合理的である。ユーザ数は圧倒的に研究系システムのほうが少なく、それのアカウント名とユーザID、グループIDを統一することは不可能ではない。しかし、課金制である研究系システムのアカウントを変更することに対する反発は当然予想された。

これらを総合的に考え、本センターではアカウントそのものの統合は断念し、二つのシステムのパスワードの共通化を目標とすることにした。これにより90日に一回強制されるパスワードの変更の作業回数が減ることでユーザーへの利便性が向上することが予想された。それと同時に、最終的な目標であるアカウント統合を行なう統合認証システムの導入の準備段階の一つとして運用経験を積むことができると考えた。

3.2 パスワードの同期システム

研究系システムの各ユーザーのパスワードとそれに対応する教育系システムのパスワードを共通化するということは、LDAPのディレクトリ情報ツリー上の異なる識別名を持つ二つのノードのposixaccountスキーマのuserPassword属性の属性値を常に同一にするようにすることで実現できる。

それには二つの方法が考えられた。最も優れている手法は片方のシステムのノードのuserPassword属性の属性値の変更を行なうときに、対応するノードのuserPassword属性の属性値を同時に変更することである。これを実現するためには、Sun Java Directory Serverのプラグインを開発する必要がある。

次善の手法として、定期的にuserPassword属性の属性値に変更があったかを調べ、変更があったら対応するノードのuserPassword属性の属性値を変更する方法である。この手法ではパスワードの変更は即時に反映されないという欠点があるが、十分に短い時間間隔で動作させることにより欠点を補うことができると考えられる。

本センターでは検討の結果、開発コストと開発時間を考慮して後者の方法を採用することとした。定期的に行なわれるuserPassword属性の属性値の共通化をパスワードの同期処理と呼ぶこととする。

最初に、教育系システムと研究系システムのノードを対応づける必要がある。教育系システムはその目的上、本学の全構成員のアカウントが用意されている。従って、教育系システムのツリーをマスターデーターベースと考え、参照先とする。それぞれのノードにedunameなる属性を付加した。属性値には対応する教育系システムのノードのuid属性の属性値と同一とする。このようにすることで、研究系システムのアカウントは一対一で教育系システムのアカウントと対応づけられる(図2)。

パスワードの変更を検出するために pwdChangedTime属性[8]を用いる。前回のパスワード同期処理が行なわれた時刻とこの属性値を比較することで、前回のパスワード同期処理後に変更されたパスワードのエントリを検索することができる。研究系システムのノードにてuserPassword属性の属性値に変更があった場合は、そのノードのedunameの属性より、対応する教育系システムのノードのpwdChangedTime属性を比較し、最も新しい

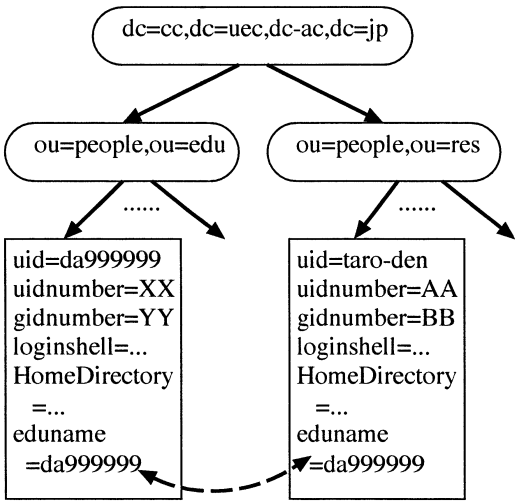

図 2: eduname 属性によるノードの対応付け

userPassword の属性値をそれぞれのノードの userPassword 属性に代入する。教育系システムのノードにて userPassword 属性値の変更が行なわれた場合は、研究系システムのノードにて uid 属性値と一致する eduname 属性を検索し、一致するノードが存在したときのみ userPassword 属性値の共通化を行なう。

このように eduname 属性を用いた研究系システム LDAP データベースの参照は、片方向のリンクしか用意していない。そのため、逆方向への参照を行なうときに eduname 属性を検索しなければならないというオーバーヘッドが生ずる。双方向のリンクを用いればオーバーヘッドは発生しないが、Sun Java Directory Server での ldapsearch の実行速度が非常に高速なこと、管理しなければならない属性を最小限にとどめたいこと、将来はさらに異なるシステムに対して認証情報を提供したいことを考慮し、あえて片方向のリンクを利用することとした。

パスワード同期処理を行なうスクリプトは Perl5 で実装されている。パスワード同期処理スクリプトは各サーバ上で 30 分間隔で cron より交互に実行される。従ってユーザーにとって待ち時間はサーバに障害が発生し 1 台で動作した場合に最長の 30 分となる。1 台の LDAP サーバで行なわれた同期処理は、デュアルマスター構成を取っているので自動的

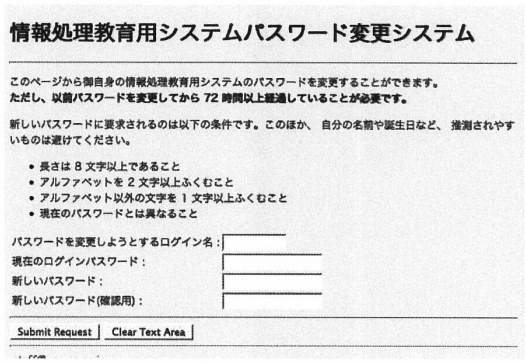

図 3: パスワード変更ウェブページ

にもう片方のサーバの LDAP データベースに反映される。

パスワードの変更後、15 分は再びパスワードを変更することができないように設定されている。これは同期処理における混乱を排除するための制限である。

ユーザーはパスワードの変更は Solaris サーバから passwd コマンドを利用して行なうことができるが、専用ウェブページからも変更が可能である (図 3)。このウェブページのパスワード変更 CGI はパスワードの強度や同一のパスワードを利用していないか等を確認しているので、ユーザーに対しより強度のあるパスワードの利用を強制することが可能となっている。

3.3 運用状況

パスワード同期スクリプトを、研究系システム及び教育系システム、教育支援システムの計 3 システムに対し適用し、2007 年 3 月より運用を開始した。

運用開始前にダミーアカウントを用いて負荷テストを実施した。全演習端末からユーザーが一斉にパスワードを変更した場合を想定して負荷テストを行なったが、パスワード同期スクリプトは瞬時に同期を行なった。これによりどのような場合でも運用が可能であると判断し、実運用を開始した。

運用当初は、eduname 属性によるノードの参照のための情報が未入力のままでパスワードの同期が行なわれないという苦情が多かったが、eduname 属性の未入力がなくなった現在ではパスワード同期処

理システムはメンテナンスなしに稼動している。

LDAP サーバも含めた障害としては、パスワード同期スクリプトのログを全て残していたために/var パーティションが溢れ、2 台の LDAP サーバのうち、1 台がヘルスチェックには反応するが LDAP サーバとしては機能しなくなる障害が発生した。障害が発生した LDAP サーバの/var/log 以下のログファイルを整理することが回復した。現在では/var/log 以下のログファイルの容量が増えすぎないように常時チェックを行ない、再発を防止している。

本統合認証システムの評価であるが、教育系システムと教育支援システムを同時に用いる講義担当教員と TA から高評価を得ている。これは利用頻度の高い 2 系統のシステムのパスワードの変更を一括してかつ共通に行なうことができるからである。研究系システムのユーザーからはそれほどの評価を得ていない。これは研究系システムを利用するユーザーは、学部 4 年生以上の研究室に所属している学生と教員に限られ、計算機教育を目的とする教育系システムをほとんど利用しないためである。

4 最後に

本稿にて，電気通信大学情報基盤センターにて開発した LDAP を用いた複数の UNIX システム間のパスワードに共通化よる統合認証システムについて述べた。このシステムは、複数の系統の UNIX システムのアカウントのパスワードを共通化することでユーザーの利便を確保するものである。

本システムの欠点は、パスワードの同期に一定の待ち時間が必要なことと、データ構造として片方向のリンクを用いているために同期の際にオーバーヘッドが存在することである。前者に関してはユーザーの利便性を考えると実時間で同期することが望ましい。後者に関しては LDAP サーバのディレクトリ情報ツリー上の情報の管理のための作業量とパスワード同期スクリプトの実行時間とのバランスが問題となる。

統合認証は原則的に、シングルアカウント・シングルパスワードを実現することが望ましい。それを踏まえると本統合認証システムは、シングルアカウント・シングルパスワードを実現する一歩前の、マルチアカウント・シングルパスワード統合認証システムである。

本システムは、それぞれの命名規則で作成されたアカウントを持つ複数の情報システムに対して、シングルアカウント・シングルパスワードへのゆるやかな移行を行なうための道具として利用することが可能と考えられる。まずは、複数の情報システムのパスワードを統一することで、ユーザーへの利便性を向上させる。新規に作成されるアカウントよりシングルアカウントへ移行する、あるいはシングルパスワードの利便性を体験してもらうことにより、シングルアカウント採用への同意を得やすくする等の活用が可能である。

Acknowledgement

本研究に関し、電気通信大学 情報基盤センタースタッフの岡野豊氏、才木良治氏、大西邦弘氏、石井和広氏、ならびにキヤノン IT ソリューションズ株式会社の村山輝氏、下村健氏に深謝致します。彼らとのブレインストーミングとご尽力により、本統合認証システムの開発と実運用が可能となりました。

参考文献

[1] 江藤博文, 渡辺健次, 只木進一, 渡辺義明, 全学的な共通情報アクセス環境のための統合認証システム, 情報処理学会研究報告 2002-DSM-27, pp.31–36 (2002).

[2] 梶田将司, 内藤久資, 小尻智子, 平野靖, 間瀬健二, CAS によるセキュアな全学認証基盤の構築, 情報処理学会研究報告 2005-DSM-37, pp.35–40 (2005).

[3] 奥村勝, 本山聡, 三河邦夫, 福岡大学における統合認証システムの構築と運用について, 情報処理学会研究報告 2006-DSM-40, pp.7–12 (2006).

[4] 平塚紘一郎, 大垣内多徳, 田中光也, 長期運用を考慮した認証システムの設計と運用, 情報処理学会研究報告 2007-DSM-47, pp.13–17 (2007).

[5] 梶田将司, 太田芳博, 田島嘉則, 田島尚得, 平野靖, 内藤久資, 間瀬健二, 生涯利用可能な名古屋大学 ID の導入に伴う名寄せ問題とその解決法, 情報処理学会研究報告 2008-DSM-48, pp.73–78 (2008).

[6] RFC 1777, 1778, 1779, 1959, 1960, 1823 (LDAP v2). RFC 2251, 2252, 2253, 2254, 2255, 2256 (LDAP v3).

[7] Sun ONE Directory Server 5.2, *http://docs.sun.com/source/816-6880-10/*.

[8] J. Sermersheimm, L. Poitou, Password Policy for LDAP Directories, *http://tools.ietf.org/html/draft-behera-ldap-password-policy-09*.