Vol.2010-IOT-11 No.1
2010/10/15

Open Directory と Active Directory を併用したコンピュータ教室運用

中 山 貴 夫[†1]　宮 下 健 輔[†1]

京都女子大学では全学的なユーザ認証システムとして Open Directory を採用しており，コンピュータ教室に設置した Windows XP および Mac OS X でも Open Directory を利用している．平成 22 年 8 月から 9 月にかけてコンピュータ教室の一部設備を更新し，新しい端末では Windows XP を NetBoot することにした．NetBoot には Active Directory によるドメイン運用が必要であるため，既存の認証システムに Active Directory を組み込む必要が生じた．本稿では，Open Directory と Active Directory を併用してコンピュータ教室を運用するために行った仕様の検討および実験とその結果について報告し，さらに導入を予定している Windows 7 への適用の可能性について述べる．

Computer Room Management with Cooperative System of Open Directory and Active Directory

Takao Nakayama[†1] and Kensuke Miyashita[†1]

In Kyoto Women's University, we deploy the user authentication system with Open Directory and it supports Windows XP and Mac OS X clients in our computer rooms. We have restructured a half of computer rooms during the summer of 2010. Windows XP can be NetBooted on the new client. The Windows domain management with Active Directory is needed for NetBoot system. Then, we should cooperative operate an existing authentication system and Active Directory. In this paper, we report a discussion about design requirement of our new system and some experiments for development of cooperative system of Open Directory and Active Directory. And, we describe whether Windows 7 can be applied to the new authentication system.

1. はじめに

京都女子大学（以下本学という）は 4 学部 11 学科からなり，学生数約 6000 名，教職員数約 500 名の中規模私立女子大学である．本学では平成 12 年度に情報教育環境を整備し，KWIINS(Kyoto Women's university Integrated Information Network System) と呼ばれる全学的な情報システムを整備した[1)]．その後平成 17 年度末にサーバ群の大規模な更新[2)]，平成 19 年度にネットワーク機器群を更新した[3)] ことにより KWIINS 2.0 となった．

本学には 10 室のコンピュータ教室があり，内訳は Windows PC 教室が 9 室（うち CALL 教室が 2 室）と Mac 教室が 1 室である．これらの教室を含めて KWIINS 2.0 では Open Directory を用いたユーザ認証を行っており，Windows 教室向けの Windows ドメイン運用も Open Directory を利用している．Open Directory は Mac OS X Server に標準で備わっている機能のひとつで，LDAP や NetInfo，NIS，Active Directory 等に対応するディレクトリサービスと認証システムを提供する．

各コンピュータ教室にはそれぞれ約 60 台のコンピュータが設置されており，その他に教員の各研究室や学生用研究室，学生寮などにそれぞれコンピュータが設置されている．それらを合計して，KWIINS 2.0 には約 1000 台のコンピュータが接続されている．

学術情報システムはサーバ機器やコンピュータ教室端末の老朽化，情報教育環境充実への要求，変化の激しい情報技術へ対応する必要があり，常に更新する必要がある．本学においても例外ではなく，減価償却期間やリース期間を過ぎた端末類の更新が必要となっていた．そのため，平成 21 年度から更新に関するポリシーなどの議論を開始し，平成 22 年 8 月から 9 月にかけて 2 室の CALL 教室と Windows 教室のうちの 3 室の合計 5 教室の機器更新を行った．

本稿では，まずこの機器更新において検討した事項について述べ，次に更新の際必要となったユーザアカウント管理手法の検討について説明する．そして Open Directory と Active Directory を連携して運用するための実証実験と更新後の環境における運用実験について述べる．

†1 京都女子大学 現代社会学部
Faculty for The Study of Contemporary Society, Kyoto Women's University

2. 機器更新における検討事項

機器更新の対象となった 5 教室についてどのような方針で環境整備を行うかについて検討した．ここではその検討事項について述べる．

2.1 OS やソフトウェア環境に関する検討

まず OS 環境に関する検討から行った．現在，CALL 教室を含めた Windows 教室の OS は Windows XP で統一されている．年度途中の更新であり，一部の教室の OS を変更することは授業に重大な影響を及ぼすため，今回も Windows XP を導入するのが妥当だと思われた．一方，本学では今後残り 5 教室の機器更新が想定されているが，その時点で Windows XP という選択肢はほぼあり得ない．現在主力である Windows 7 についてもいつ次期 OS が登場するか予想ができない状況にある．さらに，管理上からも教育上からも利用者環境は統一されていることが望ましい．つまり，OS 環境としては以下に挙げる要素が求められる．

- 全教室を統一した OS 環境で整備する
- 現行の Windows XP も利用可能である
- 数年後に Windows 7 やその次期 OS にも対応可能である

これらを満たす環境として，多くの大学でも導入実績のある[4)5)] クライアント仮想化を採用することとした．クライアント仮想化により，上記の要求を満たすだけでなく次に挙げる利点もある．

- 今後の環境変化に対応可能
  今後の OS 環境がいかに変化しても，仮想化によりその変化を吸収できる．そのため，クライアント PC 自体を更新する必要がなくなる．今後情報システム整備予算の肥大化を防ぐことを考えるとこれは大きな利点といえる．
- 管理工数の削減が可能となる
  現状，コンピュータ教室のソフトウェア環境の整備は半期ごとに人手をかけて行っている．具体的には教室ごとにマスタクライアントで雛型を作成し，それを配布する形で行っている．配布にはある程度時間がかかるため，セメスターの途中でセキュリティ対応の必要性などからソフトウェア環境を変更する必要があった場合に対応が困難である．しかし，クライアントを仮想化すると各クライアントへ配布の必要がなくなるため，サーバ上の起動イメージの変更だけで対応できる．
- 様々な授業形態への対応が可能となる
  現在，Windows OS の種類は複数のものが混在しており，また授業で使用するアプリケーションも多種多様である．クライアントを仮想化し，起動イメージを複数作成することにより，例えばある授業（教室）では Windows 7 を用いた授業を行い，他の授業（教室）では Windows XP で授業を行う，などといったことが可能となる．その他にもバージョンの違う Office がインストールされた起動イメージを作成して授業ごとに異なる Office を利用したり，授業ごとに必要なアプリケーションだけをインストールした起動イメージを用いて学生が授業に集中できる環境を整えることも考えられる．

2.2 仮想化方式に関する検討

次に，クライアント仮想化の方法としてシンクライアント方式と NetBoot 方式を比較した．

シンクライアント方式の場合，クライアント PC は最小限の機能に限定することができ，この点では有利と思われた．しかし，高性能で大規模なサーバ群を設置するためのサーバルームを確保することが困難であり，また本学のコンピュータ教室は物理的に離れたキャンパスに点在しているために広帯域のネットワークを整備することは難しい．一方，NetBoot 方式では各教室に 1 台か 2 台のサーバを設置すればよいのでネットワークの増強なしに対応でき，サーバルームの確保も必要ではなくなる．

両者を予算面から比較した結果，NetBoot 方式のほうが安価であったため今回の更新では NetBoot 方式を採用することとした．

3. ユーザ認証構成の検討

前節での議論により，今回の更新では Windows の NetBoot 方式を採用することとなった．NetBoot システムの構築には Citrix 社の XenDesktop 3.0 Enterprise Edition とパナソニック電工社の DeskWaveNetkaleido を用いた．これらのシステムによる起動イメージ配信には Active Directory サーバが必要となる[⋆1] ．しかし KWIINS2.0 では現在，サーバ群を Mac OS X Server で運用している関係から，ユーザアカウントや Windows ドメインは Open Directory により管理している．そのため，Windows ドメインやユーザアカウント管理を再構成する必要がでてきた．一方で，本学のコンピュータ教室環境には Mac 教室も 1 教室あるため，Open Directory による管理も必要となる．

そこで，既存のドメイン運用やユーザアカウント管理方法をなるべく変更しないような形の再構成案をいくつか検討し，サーバ群および数台のクライアントを用いた予備実験を行っ

⋆1 http://support.citrix.com/servlet/KbServlet/download/19198-102-19661/cds-sys-reqs-bk.pdf

た．ここでは，検討した案とその実験について述べる．

3.1 Active Directory にユーザ管理を移行

まずユーザアカウントを Open Directory から Active Directory に移行し，Windows と Mac 両方の認証を Active Directory で行う方法について検討した．この案については，以下の手順で検証を行った．

(1) ユーザアカウントを Open Directory から Active Directory へ移行する
(2) ホームフォルダとユーザプロファイルを Windows ファイルサーバへ移行する
(3) Windows クライアントでログオンして動作確認する
(4) Mac クライアントで「ディレクトリアクセス」の認証を Active Directory サーバを最優先にし，ログインできるか確認する

その結果，検証中に以下の問題点が明らかとなり，この方法は採用しないこととなった．

- Open Directory から Active Directory へアカウント情報を保持したまま移行する機能がないため，実質的には同じアカウント名のユーザを Active Directory 側に作成する必要がある．そのため全てのユーザに新規のパスワードを発行する必要があり，パスワード発行・交付の事務的手続きの負担が大きい．さらに新規パスワードを発行すれば，当然全てのユーザにパスワードを変更してもらう必要があり，更新時期が夏休みであることも加えると後期の授業開始時に大きな混乱が予想される．
- 本学ではコンピュータ教室以外にメールや LMS (Learning Management System) へのログイン時や，OPAC (Online Public Access Catalog) を利用する図書館の端末などでもユーザ認証を行っている．ユーザアカウント管理を変更する際にはそれらのシステムの認証も Open Directory から Active Directory へ変更する必要がある．しかし，全てのシステムが Active Directory による認証に対応しているか検証するのは時間的に難しく，変更の手間もかかる．
- Mac では Windows ファイルサーバ上にあるホームディレクトリを SMB でマウントすることができない．そのため，現在のように Windows と Mac でホームフォルダを共有する運用が不可能となる．

3.2 Open Directory と Active Directory それぞれでアカウント管理を行う

次に 3.1 と同様の手順で Active Directory 上にユーザアカウントを作成し，互いの連携を取らずに独立して運用する方法を検討した．しかしこの方法は以下に挙げるようにユーザの負担が大きく現実的ではないため，あらゆる連携がうまくいかなかった場合の最悪の案とした．

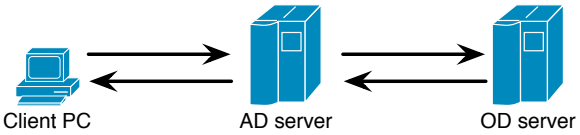

図 1 Open Directory と Active Directory の連携による認証手順

- Mac 教室と Windows 教室でパスワードの連携ができないため，ユーザは二つのパスワードを管理する必要がある．
- ホームフォルダについては，Windows サーバに置いた場合は Mac からホームフォルダにアクセスできない．また，既存のファイルサーバに置いた場合は，ファイルサーバと Windows クライアントとで利用されるアカウントが異なるため，Windows クライアントからアクセスするための適切なアクセス権が設定できない．

以上のように検討した案についてはそれぞれ問題点があり，その案での運用は難しいと分かった．

4. Open Directory と Active Directory の連携

前節で述べた検討結果から，Active Directory 側にユーザアカウントを作成するのは管理者・ユーザともに負荷が高く，ユーザ認証は従来通り Open Directory 側で行うのが望ましいと判断した．そこで，ユーザ認証は Open Directory で行い，NetBoot する Windows クライアントのコンピュータアカウントのみを Active Directory で管理する方法について検証を行った．この方式では，Windows ドメインは Active Directory サーバで管理し，Active Directory と Open Directory の間に信頼関係を構築することで認証のみ Open Directory で行う．クライアントからのユーザ認証要求は，まずドメイン管理をしている Active Directory サーバに送られ，そこから Open Directory サーバに送られることになる（図 1）．ここでは Open Directory と Active Directory の連携に関する実証実験について述べる．

4.1 既存環境を用いた実証実験

4.1.1 実験 1：既存の Open Directory 環境におけるログオン時間計測

平成 22 年 7 月に，Open Directory と Active Directory を連携した新環境との比較を行うため，既存の環境で 1 教室で一斉にログオンおよびシャットダウンを行い，それに要する時間の測定を行った．

実験用にテストアカウントを作成し，Windows 教室 ×1，Windows 教室 ×2，Mac 教室

表 1 実験 1 の結果

対象	1 回目		2 回目		3 回目		平均値	
端末数	ログオン	シャットダウン	ログオン	シャットダウン	ログオン	シャットダウン	ログオン	シャットダウン
Windows×60	1:06	2:26	1:02	1:59	1:05	1:53	1:04	2:06
Windows×120	2:05	2:43	1:52	2:31	1:54	2:17	1:57	2:30
Mac×60	2:21	0:37	1:25	0:46	1:29	0:38	1:45	0:40
Windows×60+ Mac ×60	Win 1:50/Mac 7:10	Win 2:14/Mac 0:54	Win 1:18/Mac 2:28	Win 2:20/Mac 0:45	Win 0:51/Mac 2:25	Win 2:19/Mac 0:43	Win 1:20/Mac 4:01	Win 2:18/Mac 0:47

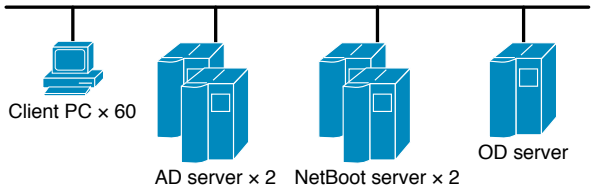

図 2 実験 2-1, 2-2 の環境

×1，Windows 教室 ×1+Mac 教室 ×1 の 4 パターンでそれぞれ 3 回ずつ一斉ログオンおよびシャットダウンを行った（前述の通り 1 教室当たりの端末数は 60 台である）．一斉ログオンはあらかじめログオン画面でユーザ名とパスワードを入力しておき，合図とともに順番に Enter キーを押下していく方法で行った．ログオンについては合図開始から全ての端末がログオン後，ログオンスクリプトによるコマンドプロンプト起動が完了するまでの時間を計測した．シャットダウンについても同様に，全ての端末がシャットダウン完了するまでの時間を計測してある．以降の実験についても同様の方法で計測している．結果を表 1 に示す．

1 教室の場合ログオンには 1 分程度，教室数が増えても 2 分程度でログオンできていることが分かる．1 回目や 2 回目のテストにおいて Mac 端末のログインに時間がかかっていることが分かる．この原因は，テストアカウントを用いてテストしたことによるもので，アカウント作成後の初回ログイン時に個人設定ファイルの雛型を作成するための時間が余計にかかったためである．

4.1.2 実験 2-1：Open Directory と Active Directory の連携テスト

次に，図 2 に示すトポロジを構築して同様の実験を行い，Open Directory と Active Directory の連携が可能かを確認した．実験は運用中のネットワークに影響を与えないよう，学内ネットワークから切り離して行った．Open Directory サーバについては既存の Open Directory サーバのバックアップイメージから復元したものを用い，そこにテスト用のアカウントを作成した．Active Directory サーバと NetBoot サーバは新規に構築し，それぞれ 2 台ずつ用意した．各クライアントは 100BASE-TX で L2 スイッチに集約され，L2 スイッチと各サーバは 1000BASE-TX で接続した．

表 2 実験 2-1 の結果

	1 回目	2 回目
Active Directory サーバ ×1	1:23	1:33
Active Directory サーバ ×2	2:04(15 台エラー)	1:48(17 台エラー)

1 つの Windows 教室で一斉にログオンおよびシャットダウンするテストを 2 回ずつ行い，要する時間を測定した．Active Directory サーバの負荷を確認するため，Active Directory サーバが 1 台の時と 2 台の時の 2 パターンで行った．結果を表 2 に示す．

Active Directory サーバが 1 台の場合はログオンに要する時間が 1 分 30 秒前後と表 1 の結果に比べてが長くなっているが，全ての端末で問題なくログオンできており Active Directory と Open Directory が連携してユーザ認証ができることが確認できた．

しかし，Active Directory サーバが 2 台の場合には 4 分の 1 程度の端末にログオンエラーが発生し，ログオンできた端末についてもサーバが 1 台のときよりも時間がかかっている．負荷分散が働くためサーバ 2 台のほうが時間が短縮されると予想していたが，反する結果となった．ログオンエラーの原因はドメインを利用できないエラーによるものであった．このときの Open Directory サーバのログを確認したところ，ログオンエラーが起きた場合にはサーバからクライアントの NetBIOS 名が逆引きできていないことが分かった．なお，いずれの場合もシャットダウンに要する時間は短くなっているが，この原因は特定できていない．

4.1.3 実験 2-2：hosts ファイル修正後

上記の問題を解決するため，Open Directory サーバの hosts ファイルに各クライアント

表 3 実験 2-2 の結果

	1 回目	2 回目	3 回目
Active Directory サーバ ×1	1:34	1:43	1:48
Active Directory サーバ ×2	1:44(38 台エラー)	1:55(2 台エラー)	1:45(18 台エラー)

の IP アドレスを記述し，逆引きできるようにして再度実験を行った．この結果を表 3 に示す．hosts ファイル修正前と同様，Active Directory サーバ 1 台の場合は問題なくログオンできたが Active Directory サーバ 2 台の場合にログオンエラーとなる端末が見られた．ログオンに要する時間もあまり変わっていないため，hosts ファイル修正ではログオンエラーを解決できないと分かった．

ログオンエラーの原因については特定できていないが，以下のことが予想される．実環境では Open Directory サーバは PDC が 1 台，BDC が 2 台の 3 台構成であるが，機器確保ができなかったためこの実験では PDC のみを用意した．しかし，バックアップから復元したので設定上は BDC が 2 台が存在していたことが判明した．後述するように実環境におけるログオンテストではエラーが発生しなかったため，この実環境と異なっている点が原因ではないかと考えられる．

4.2 実環境における実証実験

次に平成 22 年 8 月に，各教室の端末や新規導入したサーバ群を学内ネットワークに接続した実環境においてログオンテストを行った．今回導入した機器類のうちユーザ認証に関する部分の概略図を図 3 に示す．なお，各教室内の帯域は 100Mbps，サーバセグメントは 1Gbps，ルータ間は 2Gbps である．

4.2.1 実験 3：1 教室でのログオン実験

前節と同様，テストアカウントを作成して 1 教室で一斉ログオンおよびシャットダウンを行い，要する時間を測定した．また，NetBoot サーバが 1 台の場合と 2 台の場合で，クライアントを一斉に電源を入れて全てのクライアントがログオン画面になるまでの時間も測定した．結果を表 4 に示す．

全てのパターンにおいて 1 分以内に全ての端末のログオンが完了しており，既存の Open Directory のみによる認証よりもよい結果が得られた．また，Active Directory サーバの数によらずログオンエラーは見られなかったため，テスト環境でのログオンエラーは Open Directory サーバにおける BDC 関連の設定ミスが原因であると予想される．クライアントの起動時間については，NetBoot サーバが 2 台の場合でおよそ 1 分 30 秒程度，1 台の場合

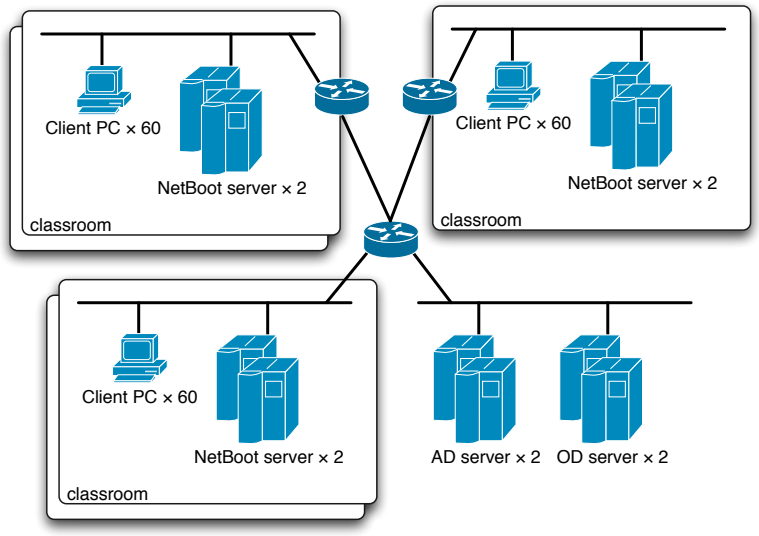

図 3 導入環境

表 4 実験 3 の結果

サーバの台数	起動時間	ログオン	シャットダウン
Active Directory サーバ ×2，NetBoot サーバ ×2	1:25	0:51	1:01
Active Directory サーバ ×1，NetBoot サーバ ×2	2:09	0:56	0:56
Active Directory サーバ ×1，NetBoot サーバ ×1	2:01	0:59	1:01

でも 2 分程度で全てのクライアントが起動している．この値は片方の NetBoot サーバに障害が起こった場合を想定しても許容範囲だと思われる．

4.2.2 実験 4：複数教室でのログオン実験

次に，Active Directory サーバがどれくらいの負荷に耐えることができるかを確認するため，複数の教室で一斉にログオンし，その時間を測定した．結果を表 5 に示す．

Active Directory サーバが 2 台の場合，1 教室の場合に比べて若干時間がかかっている．しかし最大でも 1 分 20 秒程度で全ての端末のログオンが完了しており，実用には十分耐えうると判断した．また，ログオン後にクライアントで用いたログオン先のサーバを確認した

表 5 実験 4 の結果

同時ログオン端末数	ログオン時間
1 教室（60 台）	0:39
3 教室（172 台）	1:11
5 教室（292 台）	1:19
5 教室 (Active Directory サーバ ×1)	1:33(38 台エラー)

ところ，ほぼ均等に割り振られており，適切に負荷分散されていることが確認された．

Active Directory サーバが 1 台の場合はログオンできた端末については 1 分 30 秒程度でログオンが完了したが，全 292 台中 38 台の端末でログオンエラーが発生した．エラーが起きた端末はログオンするタイミングが遅れた端末ばかりであったため，本学の環境では Active Directory サーバ 1 台に対して 250 台程度のクライアントまで同時ログオンに耐えうると考えられる．

4.2.3 パスワード変更と Windows 7 への適応

次に，Open Directory のみで管理されている既存のクライアントと，Open Directory と Active Directory の連携で管理されている新規のクライアントの間でパスワード変更が反映されるかを確認した．その結果，Mac クライアントも含め既存のクライアントでパスワード変更した後新規のクライアントでのログオン・新規のクライアントでパスワード変更した後既存のクライアントでのログオンともに問題なく行えた．

以上の実験結果より，本学で Open Directory と Active Directory を連携したユーザ認証によるコンピュータ教室の運用が可能であると確認できた．

また，来年度以降コンピュータ教室設備を更新する場合，Windows 7 の導入が必須となる．そのための準備として，Windows 7 を NetBoot するための起動イメージを作成してテストを行った．ログオン自体は問題なかったが，Windows XP と Windows 7 ではユーザの移動プロファイルを保存するフォルダが異なるため，アプリケーション設定の引き継ぎやドキュメントの保存場所などの環境が異なる問題が生じることが確認された．

5. おわりに

本稿では，平成 22 年夏に導入した本学コンピュータ教室の改修の設計方針とそれに伴い発生した認証システムの変更およびそのための実験について述べた．Open Directory と Active Directory を連携した認証については一応の動作確認は取れたものの，9 月中旬から実運用に入るため当面は注意深く見守る必要がある．今後は，残り 5 教室の改修に向けたサーバの負荷やネットワーク帯域の利用状況の測定，また Windows 7 とのプロファイル共有の方法に関する検討が必要と考えている．

謝辞 今回の機器更新や認証システム構築に関する実験を進めるにあたり，三谷商事株式会社の岸本邦裕氏に多大なご協力をいただきましたことを付記し，謝意を表します．

参考文献

1) 宮下健輔，水野義之：京都女子大学学内ネットワーク（KWIINS）の構築と運用，平成 14 年度情報処理教育研究集会講演論文集，pp.310–313 (2002)．
2) 宮下健輔，水野義之: 京都女子大学における情報機器更新計画，情報処理学会研究報告，2005-DSM-39 (5)，pp.25–30 (2005)．
3) 宮下健輔：京都女子大学におけるネットワーク機器の更新 —安全・快適なネットワークを目指して—，分散システム／インターネット運用技術シンポジウム 2007 論文集，情報処理学会シンポジウムシリーズ，vol.2007，no.13，pp.59–64 (2007)．
4) 佐々木芳宏，正木忠良，小林俊央，鷲谷貴洋，西田眞，中村雅英：シンクライアントによる教育用端末環境の構築，情報処理学会研究報告，2008-IOT-2，No.12（2008）
5) 奥村勝：教育用 PC システムを用いた大規模分散計算フレームワークの実現に向けて，情報処理学会研究報告，2009-IOT-7，No.2（2009）