

Mac OS X Serverを利用したWindowsドメイン運用

宮下 健輔

京都女子大学 現代社会学部

E-mail: miyasita@cs.kyoto-wu.ac.jp

あらまし 京都女子大学ではコンピュータ教室などに設置された合計約600台のWindows端末を1つのドメインで管理運用している。このWindowsドメインのコントローラとして平成12年度から平成17年度末まではWindows NT Serverを設置していたが、平成18年度にこれに代わってMac OS X Serverを設置した。本報告では、このような運用形態を計画してから運用開始するまでの経過を報告する。

キーワード 情報教育環境, ネットワーク環境, Windows, Mac OS X Server, クライアント運用管理

Mac OS X Server can Manage Windows Domain

Kensuke MIYASHITA

Faculty for the Study of Contemporary Society, Kyoto Women's University

E-mail: miyasita@cs.kyoto-wu.ac.jp

Abstract Kyoto Women's University has about 600 Windows PCs in computer rooms and these PCs are managed in 1 windows domain. From April 2000 to March 2006, the Primary Domain Controller of this domain was Windows NT Server, but it was replaced with Mac OS X Server in this April. In this paper, I report how things developed from when this plan has been made.

Keywords Computer Education, Computer Network, Windows, Mac OS X Server, Client Management

1.はじめに

京都女子大学（以下、本学という）は学生約6000名、教職員約500名の中規模文系女子大学である。本学は平成12年度に情報教育環境を刷新し、7室のWindows PC教室と1室のMac教室および30台のサーバ群によるKWIINS (Kyoto Women's university Integrated Information Network System) を構築した。その後、このシステムには適時に改良が加えられてきたが、平成17年度末にサーバ群の大規模な更改が行われ、平成18年度より7室のWindows PC教室と2室のCALL教室 (Windows PC) および1室のMac教室を約20台のサーバ群で運営する新ネットワークシステムが運用開始した。

平成12年度当初より、Windows PC（主にコンピュータ教室に設置されたもの）は1つのWindowsドメインとして運用されており、そのPDC (Primary Domain Controller) およびBDC (Backup Domain Controller) としてCompaq社製サーバ上で動作するWindows NT Serverを利用していた。このドメインには教職員が利用する各研究室のWindows

PCや学生研究室のPCが参加することも可能であり、ドメイン参加クライアント数は約500台であった。

その後、平成16年度にWindows PCを利用するCALL教室が増設され、これもドメインに参加する形態で運用されることになったため、クライアント数は約600台となった。

平成17年度末から平成18年度にかけて行われた更新により、学内のWindows PCを1つのドメインで管理する方針には変化はなかった。しかし、新規サーバ群の構築にあたっては、できるだけ多くのサーバで同一の機種およびOSを利用することでサーバ管理工数の削減を目指すことや、費用対効果の面で優れていることなどから、ほぼすべてのサーバをアップル社製のXserve G5 (OSはMac OS X Server) で構築することになり、WindowsドメインのPDCとBDCも同じくMac OS X Serverにて運用することとなった。

以下では、まず平成12年度から運用してきた旧サーバ群でのWindowsドメイン運用について述べる。その後、新ネットワークシステムへの移行に際して平成17年度に行なった運用試験について説明し、新システムの運用開始から

運用が安定するまでに生じた問題点とその対策について報告する。

2.旧サーバ群でのWindowsドメイン運用

平成12年度に運用を開始したKWIINSにおけるWindowsドメイン運用に関わる部分を図1に示す。

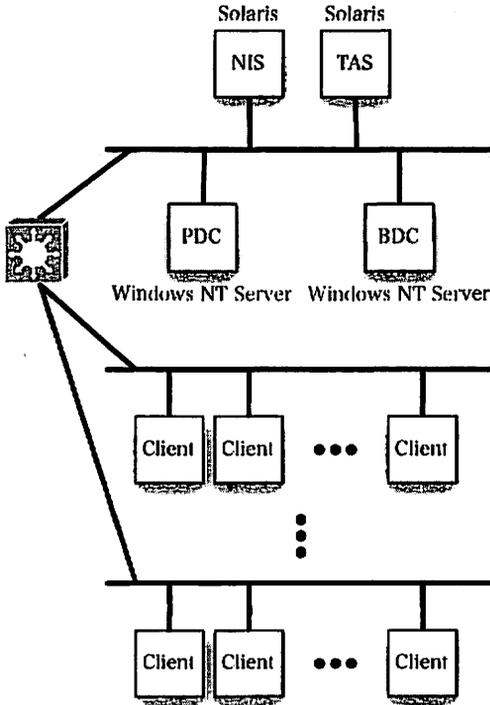


図1. 旧サーバ群でのWindowsドメイン運用

前述の通りWindowsドメインを運用するためのPDCとBDCはWindows NT Serverで構築されており、L3スイッチを隔てていくつかのサブネットに個々のコンピュータ教室等が配置されている。ユーザのアカウント情報はNISで管理されており、PDCがSFU¹を利用してNISサーバ（Solaris上に構築）とアカウント情報の同期を行なっている。またドメイン上の共有ファイルサービスはSolaris上のTAS²を利用したが、応答速度の面で問題があったため、移動プロファイルはPDC上に格納するようになっている。

この環境下では、数十台一斉ログオン時のサーバ応答時間計測などの性能実験は行なっていないが、通常の授業時にはほぼ問題なく利用されていた。ただし、クライアントPCがより速度の大きいものに更新されていくうちに、それに比較してサーバ性能が見劣りするようになり、平成17年度にはコンピュータ教室8室で一斉に行われる授業でクライアント

利用に支障が出るようになっていた。

3.新サーバ群でのWindowsドメイン運用

本学では平成18年度運用開始を目指してKWIINSを更新する計画を立て、16年度に予備調査と予算化を行ない、17年度に構築業者の決定と実際のシステム更新を行なった[1]。この節で、計画時の機器構成とそれを元にした運用試験の詳細、および実運用に至るまでに生じた問題点とその対策について述べる。

3.1.計画時の機器構成

平成17年10月の時点で計画されていた、新サーバ群でのWindowsドメイン運用に関わる部分を図2に示す（クライアント部分は図1と同様なので省略）。

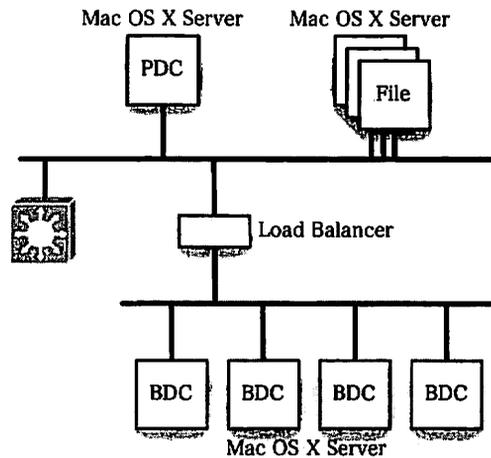


図2. 新KWIINS計画時の機器構成

新サーバ群では、ほぼすべてのサーバがMac OS X Serverにて構築され、Windowsドメインに関わる部分もほとんどがMac OS X Serverとなった。

まずアカウント情報はすべてOpen Directoryで管理することとした。このことにより、Windowsドメインとその他のサーバ群（メールサーバ等）の間でのアカウント情報を共有することができる。PDCがOpen Directoryのマスタになり、BDCはレプリカサーバとした。

BDCは4台存在し、それぞれクライアントとは負荷分散装置を介して通信することとした。ここで負荷分散装置は、各BDCの負荷状況をパケットの応答時間と維持しているセッションの数とで判断し、それぞれの負荷を均等化するものである。

Windowsドメイン上での共有ファイルサービスは、サーバに接続できるディスク容量の上限と負荷分散との両立のた

¹ Microsoft Services for UNIX (<http://www.microsoft.com/japan/windows/sfu/>)

² TotalNET Advanced Server (<http://www.engenio.com/tas/>)

め、3台のファイルサーバでそれぞれ行なうこととした。

3.2.運用試験1

まず、図2に準じた構成でクライアント数十台規模での一斉ログオンに 대응できるかどうか、実験を行なった。

実験は平成17年10月に行ない、図2の構成のうち負荷分散装置とその配下のBDCを省略し、ファイルサーバも1台にして行なった。クライアントとして、Windows XP Pro. SP2が稼働するPCが56台設置された教室を2室利用した。これらの教室はKWIINSから切り離して実験に必要なトラヒックのみが観測できるようにした。サーバはXserve G5 (2GHz/2GB/400GB)の上でMac OS X Server 10.4.4を利用し、共有ファイルサービス用のディスクもこの内蔵ディスクを利用した。アカウントとしてテストユーザ400名分を用意した。

認証方式としてWindows XP標準のNTLMv2とLM (LAN Manager)の2種類を用い、112台のクライアントで一斉にログオンとログオフを行なった。また、各ユーザの個人プロフィールを移動式としてサーバに保持させる場合とクライアントに固定する場合との比較も行なった³。

実験結果は表1の通りである。それぞれの認証方式およびプロフィール格納方式について、NTLMv2では3回、LMでは2回の試行を行ない、表1にその平均値を示している。移動プロフィールの大きさは約10MBであり、固定式プロフィールではプロフィールの保存失敗が生じないので空欄となっている。

また、DELL Power Edge 600SC (Celeron 2GHz/1GB)の上でMiracle Linux 3を動作させ、この上でOpen LDAP 2.1とSamba 3.0.14を稼働させたサーバで同条件の実験を行なったところ、固定式プロフィールでのログオンが20.5秒、ログオフが16秒と、表1に記載した結果とはあまりにもかけ離れた結果となった。

3.3.運用試験2

次に、平成18年2月に図2の構成での実験を行なった。前回の実験結果(表1)を受けて認証方式はLM、プロフィール格納方式は固定式のみとし、BDCの数を1台、2台、4台と3通りで試行し、更に負荷分散の方法として次の3種類を試した。

・パターン1

BDCはすべて負荷分散装置下に配置し、各クライアントにはWINSサーバとして負荷分散装置のもつIPアドレスを与えておく。するとクライアントからのWINS問い合わせに対して負荷分散が可能になる。ここで認証サーバを探す問い合わせに対してBDCが自IPアドレスを答える。以降の認証は各クライアントがBDCと直接行なう。

利点として、WINSの一斉問い合わせが分散されること、分散が1回のみなので障害発生時の問題切り分けがパターン2より容易なことが挙げられる。欠点として、負荷分散装置故障時にはWindowsドメインがまったく機能しないことが挙げられる。

・パターン2

BDCはすべて負荷分散装置下に配置し、各クライアントにはWINSサーバとして負荷分散装置のもつIPアドレスを与えておく。クライアントからのWINS問い合わせに対して負荷分散を行ない、認証サーバを探す問い合わせに対してもBDCが負荷分散装置のIPアドレスを答えることで以降の認証も負荷分散される。

利点として、パターン1よりも更に効果的に負荷が分散されることが挙げられるが、欠点としてパターン1同様負荷分散装置故障時にはWindowsドメインがまったく機能しないことや、分散が複数回にわたるので障害発生時の問題切り分けがパターン1よりも困難になることが挙げられる。

・パターン3

負荷分散装置を利用せず、クライアントごとに特定のBDCをWINSサーバとして指定しておくことで、BDCが各クライアントとそれぞれ通信を行なう。このときはBDCの数を4台固定とする。

この方式の利点として負荷分散装置を利用しないので負荷分散装置故障時にもWindowsドメインへの影響がないことや、分散されないので障害発生時の問題切り分けが容易であることなどが挙げられる。欠点として、クライアントごとにWINS設定を変更する必要があることや、クライアントの利用のされ方によって特定のBDCに負荷が集中する可能性があることなどが挙げられる。

上記のどのパターンでも、ユーザの認証はBDCでのみ行

表1.平成17年10月の実験結果(112台一斉)

	ログオン	ログオフ	\$HOMEマウント失敗	プロフィール保存失敗
NTLMv2, 移動プロフィール	261.0秒	220.7秒	30.3台	33.0台
NTLMv2, 固定プロフィール	181.7秒	68.7秒	33.0台	
LM, 移動プロフィール	200.5秒	571.0秒	1.0台	0.0台
LM, 固定プロフィール	116.0秒	22.0秒	0.0台	

³ KWIINSでは移動プロフィールを利用していた。

表2. 平成18年2月の実験結果 (56台一斉)

パターン	BDC数	ログオン	ログオフ	BDC数	ログオン	ログオフ	BDC数	ログオン	ログオフ
1	1	33.1秒	12.1秒	2	19.8秒	13.2秒	4	19.1秒	13.2秒
2	1	35.2秒	12.5秒	2	27.0秒	12.4秒	4	18.1秒	13.2秒
3	1			2			4	15.6秒	13.0秒

表3. 平成18年2月の実験結果 (112台一斉)

パターン	BDC数	ログオン	ログオフ	BDC数	ログオン	ログオフ	BDC数	ログオン	ログオフ
1	1	80.7秒	22.7秒	2	40.4秒	14.0秒	4	27.9秒	14.4秒
2	1	72.5秒	16.2秒	2	39.2秒	15.4秒	4	31.1秒	17.3秒
3	1			2			4	31.3秒	14.6秒

なうこととし、PDCはOpen Directoryのマスクとしてのみ動作するようにした。アカウントは前回同様、テストユーザ400名分を用意した。

実験結果を表2と表3に示す。パターン1, 2, 3の間に大きな差異は確認できなかった。また、パターン1, 2においてはそれぞれBDCの数が増えるにしたがってログオンに要する時間が短くなっている。BDCの数はログオフに要する時間にはあまり影響していないように思われる。

表には載せていないが、各BDCのCPU負荷はほぼ均等であり、ログオン開始後5秒ほどで約100%に達し後は緩やかに降下していた。これはPDCのCPU負荷についても同様であったが、ログオフ時にはPDCのCPUのみ高い負荷となっていた。またディスクおよびネットワークのI/Oについては非常に小さなものであった。

更に、移動プロファイルを利用した場合のログオンとログオフについて実験した結果を表4に示す。このときはファイルサーバもBDCとして振舞うよう設定した（ただし表中のBDC数には含めていない）。これはホームディレクトリマウント時や移動プロファイル操作時のユーザ認証をファイルサーバのみで行なえるようにすることで、他の認証サーバの負荷を増やさないようにするためである。ただしこうすることによって、Open Directoryのレプリカが増える（BDCはレプリカでなければならない）ので、アカウント情報の同期がマスクにかける負荷を考慮しなければならない。

表4. 移動プロファイル方式 (56台一斉)

BDC数	ログオン	ログオフ
2	31.0秒	51.0秒
4	38.5秒	53.6秒

以上の結果より、負荷分散装置の故障は減多に起こらないであろうことと障害発生時の問題切り分けはできるだけ容易な方がよいことから、負荷分散方式はパターン1を採用した。また、移動プロファイルを利用することによるユーザ

のメリットは非常に大きいので、表4の結果を踏まえてできるだけ移動プロファイルを利用する方針をとることとした。

3.4. 実環境での運用試験

平成18年3月よりサーバ群の新旧更改が行われ、同時に実際のコンピュータ教室環境を利用してのWindowsドメイン運用試験を開始した。

2月の実験後にMac OS X Server 10.4.5がリリースされたので、3月に導入されたサーバではこのバージョンのOSが稼働していた。また、実環境ではユーザ数が約6500名となり、これに実験のためのテストユーザを合わせて約7000名分のアカウント情報をPDCに持たせることになった。

このような状況の下、一斉ログオン・ログオフ実験を行なったところ、2月の実験結果（表4）の2倍以上の時間がかかり、しかもログオンに失敗するクライアントが複数台発生する（60台一斉ログオンに対して10台以上）という結果が得られた。また、本来は認証サーバとして動作しないはずのPDCで認証を行なったクライアントが存在した。更に、ログオフ時にPDCの負荷が非常に高い（100%）まま数十秒間が経過し、その間に新たなログオン等のイベントが発生すると、認証にそれだけ余計に時間がかかるようになっていた。負荷の原因はslapd（LDAPサーバ）がCPUをほぼ占有していることだった。

これらの結果は、まずOSのバージョンが2月実験時と異なることが原因と考えられ、バージョンを10.4.4へ戻して再び実験を行なった。すると、ログオンに失敗するクライアントの数は減ったものの、処理時間は依然として前回実験時を上回っていた。また、PDCの負荷も解消されなかった。

次に、ユーザ数の違いも原因であると考え、ユーザ数400名と7000名とで実験したところ、クライアント19台での一斉ログオンに対して20.0秒（400名）と38.5秒（7000名）という結果が得られた。また、ユーザ数が400名のときにはログオフ後のPDCのCPU負荷の高い状態は数秒で終了した

のに対して7000名の場合は数十秒間持続していた。これらのことから、ユーザ数の差異がサーバでの処理に大きな影響を与えていることがわかった。

これらを少しでも緩和するために、PDCとBDCにはデュアルプロセッサのサーバを用いることにした。しかしslapdが一方のCPUを占有している間に他のジョブがもう一方のCPUで動作することで少しは処理全体が早く進むようにはなったが、当然ながらslapdのCPU占有時間には変化がなかった。

実験時のクライアントとBDCの挙動を分析することにより、以下のことも判明した。すなわち、負荷分散装置配下にあるBDCは、PDCとは別のサブネットに属しているの、必然的にそのうち1台がマスタブラウザの役目をするようになる。そのマスタブラウザとなったBDCが、自分を認証サーバとしたクライアントに対して、自分がマスタブラウザであるという情報も渡してしまう。この事実から、この情報がクライアントを混乱させているのではないかという仮説を立てたが、検証はできていない。

同様に、なぜ認証しないはずのPDCを認証サーバとするクライアントが存在するのかについても、安定稼働させることを優先したため時間的余裕がなく解析し切れなかった。

3.5. 設計変更

上述した実験結果とその分析・考察により、図2の機器およびネットワーク構成を図3のように変更した。PDCとBDCは引き続きデュアルプロセッサのサーバを用いた。大きな変更点とその理由は以下の通りである。

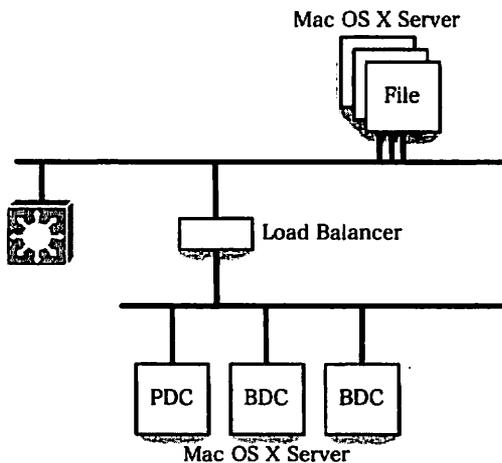


図3. 変更された機器構成

・PDCとBDCを負荷分散装置配下とした

PDCとBDCが同じサブネットに存在すれば、前述したマスタブラウザはPDCに固定されるので、認証サーバ(BDC)を通じてクライアントにその情報が伝えられる可能性がなくなる。このとき、PDCは認証を行わないので、PDCの

IPアドレスを認証サーバとしてクライアントに渡すことはしないように負荷分散装置を設定した。

・BDCの数を減らした

BDCはOpen Directoryのレプリカであるので、前述のようにアカウント情報の同期を必要とする。新しいサーバ群においては図3に示されたサーバの他にもレプリカが存在するので、その数はできるだけ減らした方がよい。しかしBDCを減らすことはログオン・ログオフの時間を増加させることになる。これはこの設計に変更した後にログオン実験を行なってBDCの台数を調整する目的で、最初は2台から始めることにした。

・認証方式をNTLMv2にした

前述の実験結果からLM方式の方が速度の面で勝ることがわかっているが、2月以降の実験に対して根本的に設計変更を行なったので、より困難であると考えられるNTLMv2方式での認証から実験を始めることにした。実験結果によっては再度LM方式に変更することもある。

図3のように設計変更した後、PDC上でログを解析することにより、ログオフ後にslapdがCPUを占有する原因が判明した。これは、LDAP上にsambaPrimaryGroupSIDというレコードが存在しないために、BDCからその値の問い合わせがPDCに集中していたせいで、その問い合わせを処理するslapdが長時間CPUを占有していた。このレコードは、Open Directoryでは標準的に各ユーザについて設定されるSMBPrimaryGroupSIDと実質同じ値でよいので、これをコピーすることで各ユーザにレコードを作成したところ、BDC内部で問い合わせが解決できることになり、BDCがPDCへの問い合わせを行わなくなった。そのため、一斉ログオフ後のPDCのCPU負荷が著しく減少した。

その後、一斉ログオン・ログオフ実験を行なった。その結果を表5に示す。これは56台のクライアントで一斉にログオンとログオフを2回行ない、その結果を平均したものである。移動プロファイルを利用した実験では1回目にログオンしたユーザのプロファイルがクライアントにキャッシュとして残るので、これを再利用することで処理が速く行われたように見えるのを避けるために、1回目と2回目で同じクライアントに異なるユーザがログオンするようにした。移動プロファイルのサイズは前回同様ほぼ10MBである。固定プロファイルでの一斉ログオフは計測していないが、各クライアントでローカル認証でログオフしたときと変わらないほどの処理時間(十数秒)だった。

表5. 設計変更後の実験結果 (56台一斉)

プロファイル	ログオン	ログオフ
固定	38.0秒	
移動	40.5秒	60.5秒

この実験結果より、移動プロファイルの利用は問題ないと判断し、またNTLMv2方式による認証も実用に耐えると判断した。

この実験の後、BDCの台数を増減して何度か実験を行なった。3台以上のBDCを用いると、BDCが増えることによってログオン・ログオフのための処理時間が減少することは確認できた。しかしOpen Directoryのレプリカが増えることによりアカウント情報同期が頻繁に発生し、そのためマスタの負荷が高いという状態がよく観測された。これは上記処理時間の減少による恩恵を上回ると判断し、結局BDCは2台ということにした。BDCを追加する手間は小さいので、実運用開始後に上記処理時間が著しく増大するなどの現象が見られれば追加して様子を観察することができるだろうと思われる。

また、各BDCのメモリには余裕があったので、smbdcが内部に持つBerkeley DBのキャッシュサイズをできるだけ大きくした。これは各ユーザの1回目のログオンには影響しなかったが、2回目以降のログオンに際してはユーザ情報がメモリ上に存在することで処理時間短縮につながった。

4.実運用開始

前述したような実験結果をもって、図3の機器構成で4月1日からの実運用開始に臨んだ。

しかし4月7日の授業開始時には早くもログオフに数分程度の時間がかかるといふ不具合が発生した。授業開始および終了時の一斉ログオンとログオフはせいぜい2教室分と見積もって最大112台程度での実験を行なったが、実際に2教室を越えるコンピュータ教室で授業が行なわれた際には開始時のログオンは一斉に行われなく（授業開始前から三々五々ログオンする）ても、終了時のログオフは各教室一斉に行われる（授業終了の合図とともに各教室で一斉にログオフする）ことがあることがわかった。

具体的には、ログオフ時のユーザ認証が終了した後、移動プロファイルを保存するために多くの時間が費やされていることが観測されている。これは現在原因究明中である。

5.おわりに

本報告では、Mac OS X ServerによるWindowsドメイン運用について、いくつかの実験とその結果によるシステムの改良とを行なって実運用を開始するまでの経緯について報告した。上述のように未だ安定運用には至っていないが、複数教室での一斉ログオン・ログオフ時以外にはほぼ実用的な安定度を得られたと考えている。

約600台のクライアントからなるWindowsドメインをMac OS X Serverで運用するという事例は世界最大規模である。そのためMac OS X Serverの開発元であるアップル社にも他のSI業者にも未だ確立したノウハウが存在しないらしい。本報告がそのような場合に役立てば幸いである。

謝辞

今回のシステム更改全体および本稿で報告した実験を進めるにあたり三谷商事株式会社（プロジェクトマネージャ：山本茂裕氏）にはシステム導入業者として多大なご協力をいただいたのでここに記して感謝いたします。

また、実験全般の進行にあたりキヤノン・スーパーコンピュータ・エスアイ株式会社（プロジェクトマネージャ：中尾良介氏）には実験現場でのサーバ設定に関する重要な示唆や実際のサーバの操作などをしていただいたのでここに記して感謝いたします。

参考文献

[1] 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,” 分散システム/インターネット運用技術研究会研究報告, vol. 2005, no. 101, pp. 25-30, 2005年10月.