

4. 教育用計算機環境の TCO 削減にむけて

3. NetBoot for Mac OS X



アップルコンピュータ (株)
広報部長

竹林 賢

takashi.takebayashi@asia.apple.com

学生や職員が利用する大量のクライアントをかかえる機関では、その管理・運用コストの削減が常に求められている。Apple の Macintosh で利用できる NetBoot を使えば、起動するためのシステムはクライアントではなくサーバ側に一元化できる。個別のクライアントを管理するという仕事から解放され、システムのメンテナンスはサーバにあるシステムのイメージに対して行うことになる。結果的にクライアントの不具合によって「システムが壊れる」ということは皆無に等しくなり、システムのアップデートやパッチの適用もサーバ上にあるイメージに対してのみ行えばよくなり、管理のためのコストは大幅に低減されることが期待できる。

教育用計算機システムの現状

大学などの教育機関における計算機教育は、理科系や文系を問わずに必要とされるようになった。多数の計算機科目の履修生やあるいは電子メール環境を必要とする学生などが毎日滞りなく利用できるようにし、学校全体として計算機の利用環境を整えるという課題は年々大きな問題となってきている。多くの教育機関で、全校的に計算機利用環境を整えるといったことがミッションとなっており、効率よく快適な環境をなるべく管理コストがかからない形式で導入するということへの要求は次第に高くなっている。

一部の教育機関では、学生1人にコンピュータを1台貸与するといった環境を実現しているが、多くの教育機関はコンピュータの台数よりも学生や職員数の方が多いのが一般的だ。したがって、コンピュータを独占的に利用するのではなく、共通に利用できなければならない。また、運用上、どのコンピュータを使っても各人の作業

環境が呼び出せるようになっていないといけない。

個別のコンピュータに個人のデータなどを残すような形式だと、特定のマシンを必ず使わないと何もできないといったことになって運用はスムーズにはできない。そのような運用のやり方では、セキュリティ面を確保することはかなり難しいだろう。管理が行き届かないコンピュータが学内にたくさん散らばっているという状況は管理者にとっては背筋を凍らせるものかもしれない。

もともと、今時セキュリティ機能のない OS は存在しないので、何らかのかたちで安全に運用することは可能となっている。しかしながら、パソコンシステムは成り立ちから、ハードディスクにシステムをインストールして使うという使い方が基本にあったため、そうした使い方が多いのが現状だ。もちろん、利用者に対してシステムの変更権限を与えなければ理論的にはシステムは安全に保全される。しかしながら、セキュリティホールが見つかったりなどといったアップデートは頻繁に行われる現在、キャンパスのあちこちに散らばったコンピュータをその都度アップデートするというのは大掛かりな管理作業をとまなうものであり、結果的にコストに大きく跳ね返ると言っても過言ではない。Apple の NetBoot という仕組みはそうした管理のやり方を大きく変えるものである。

NetBoot による起動システム運用

通常のコンピュータシステムは、ハードディスクにカーネルやシステムあるいはその他のアプリケーションなどをインストールして運用する。もちろん、個人だとクライアントのハードディスクにデータを残すといった使

単体で稼働するコンピュータ



NetBootをベースに稼働するコンピュータ

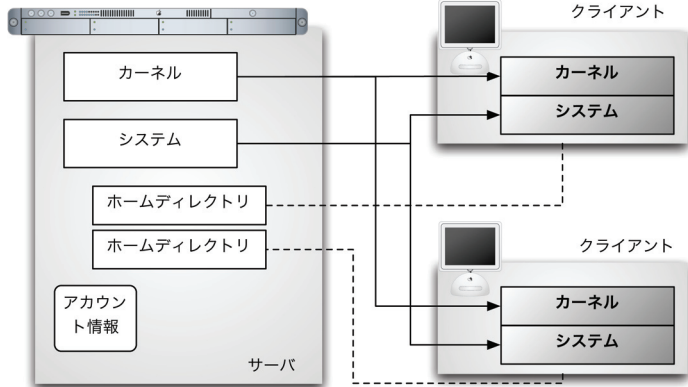


図-1 通常の起動と NetBoot の起動の違い

い方をするが、教育機関での利用ではデータ領域は一般にはネットワーク上に確保して、どのコンピュータを使っても自分のデータと呼び出せるという環境を作っているだろう。

一方、NetBoot を使った場合には、サーバ上に、カーネルやシステムを配置する。そして、クライアントのコンピュータの電源を入れると、サーバからカーネルやシステムをネットワーク経由で取り込んで、自分のマシンのメモリに展開するなどして、起動することができる(図-1)。つまり、各クライアントにシステムをインストールする必要がない。データ領域をネットワーク上のホームディレクトリに確保しておけば、クライアントマシンはハードディスクをはずしても運用が可能である。システムがサーバの1カ所にあり、そのシステムの情報にはクライアントから一切書き込みができないため、偶発的にシステムが壊れることはあり得ない。クライアントからの書き込みはすべてシステムとは別のところで受け付けるため、壊れようがないのである。

さらに、システムのアップデートが必要な場合には、サーバ上において共通に使っているシステムやカーネルなどを更新しておけばよい。夜中にサーバのシステムを入れ替えておけば、翌日からはすべてのクライアントが新しいシステムで運用できる。ファイルサーバやデータベースサーバでデータを一元化することでさまざまな業

NetBootの起動に対応した機種	PowerPC G3搭載iMac*1 PowerPC G4搭載iMac iBook eMac Power Mac G5 Power Mac G4 Power Mac G4 Cube PowerBook G3(FireWire) PowerBook G4 Xserve
本体に必要なメモリ	128MB (Mac OS Xの場合)
ネットワーク環境	100MbpsのEthernet (10台未満のクライアント) スイッチを利用する100MbpsのEthernet (10~50台のクライアント) Gigabit Ethernet (50を超えるクライアント)

*1スロットローディング式に限る

表-1 NetBoot の動作環境

務の効率化が可能になるが、NetBoot はその意味ではシステムそのものをサーバで一元化することで管理の手間を大きく削減させることを実現する。

NetBoot の仕組み

NetBoot を実行するための環境を表-1にまとめておいた。起動可能なシステムは、Mac OS X および Mac OS 9であるが、もちろん最近では Mac OS 9での起動ができない機種もあり、それらの機種では Mac OS 9でのNetBoot はできない。システムそのものを NFS で供給する場合には、Mac OS X Server 以外のサーバでも利用できる。サーバ上のシステムを負荷分散することもできる。

クライアントが NetBoot によってシステムが起動するまでを図-2にまとめた。Macintosh のシステム ROM には NetBoot のための機能が組み込まれており、起動時に NetBoot サーバを検索させることができる。そしてシステムが見つかったら、ハードディスクのシステムではなく、ネットワーク上にあるシステムで起動を行う。TFTP でカーネルを送り込み、システム自体は NFS ないしは HTTP でクライアントに供給される。ここで、システム自体はあたかもディスクボリュームのようにクライアント側では見えている。書き込み可能な部分には書き込みができるのであるが、実はクライアントごとにシャドウファイルをサーバ側で確保して、そのログインセッションの間だけの読み書きを可能にしている。だから、シャドウの領域に書き込んだものはその直後には読み取ることもできるが、改めて再起動したらなくなっている。こうした仕組みを拡張して、記憶領域のページングの処理

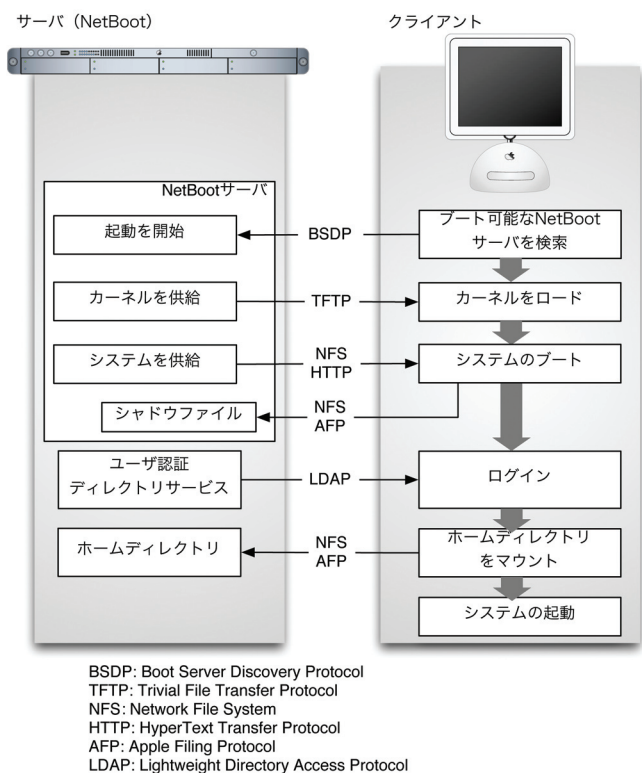


図-2 NetBoot の流れ

もネットワークの先のサーバを使うことが可能となる。だから、ハードディスクすら不要になるわけだ。

システムの起動後はログインパネルが出てくるが、ログインの認証はLDAPサーバを使って可能である。そして、ネットワーク上にあるホームディレクトリを利用するが、たとえば、自動的にNFSのエクスポートされたディレクトリをマウントして、そこにホームを確保するといったことも可能だ。

システムイメージとその管理

NetBootで起動するシステムを作るためのユーティリティ「ネットワークイメージユーティリティ」がMac OS X Serverに付属している(図-3)。CD-ROMで供給されるMac OS Xのシステムから起動イメージを作成することだけでなく、ハードディスク上にある特定のパーティションをそのまま起動用のイメージにすることもできる。たとえば、外付けのFireWireハードディスクにちょうどいいサイズのパーティションを作っておき、そのパーティションで起動して必要な設定やあるいは追加ソフトウェアをインストールし、そのシステムパーティションをNetBootの起動ディスクにすることができる。特殊な設定が必要な場合も、普通に作業をしてシステムを作

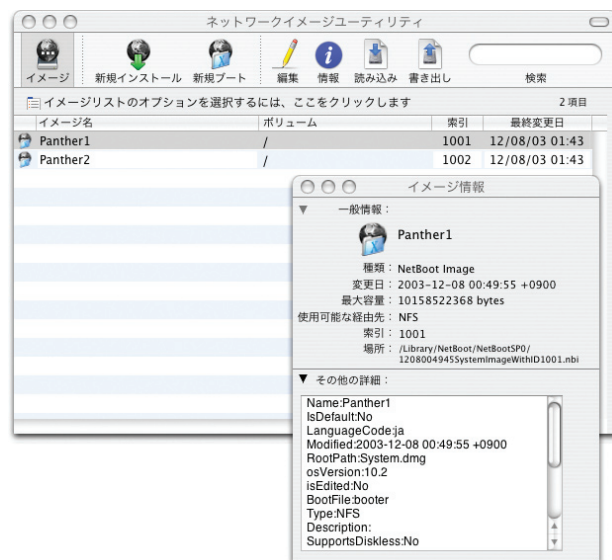


図-3 ネットワークイメージユーティリティ

ればよい。さらに、まとまったシステムに対して追加のセキュリティパッチなどを独立して適用するようなシステムイメージを作成することも可能である。

いずれにしても、こうした仕組みでシステムは一元化されるため、1つのシステムイメージをアップデートすれば、たくさんのクライアントのシステムが一気にアップデートされるのと同じことだ。仮にシステムを供給するサーバを分散化していたとしても、バッチ等で一気に配布するにすればいいだろう。クライアント1台ずつをアップデートすることを考えれば桁違いに管理は容易になる。

また、「ネットワークイメージユーティリティ」はsftpを使って、別のサーバからイメージをもらったリ、あるいはイメージを配布するような機能もある。NetBootサーバそのものが分散している場合でも対処できるような機能が用意されている。

NetBootを運用するためのサーバ

NetBootを運用するには、NetBootサーバが必要になる。ネットワークのパフォーマンスを考慮し、クライアントの台数に応じてNetBootサーバを用意しなければならない。また、EthernetでしかNetBootは利用できない。つまりワイヤレスLANなどは使えないので、基本的にはコンピュータを固定的に設置することになる。

1台のサーバで、NetBootからシステムの供給、さらにはLDAPサーバ、ホームディレクトリの運用までは可能であるが、これらの仕組みはもちろんすべて分散させることも可能である。アクセスの集中をうまく平準化さ

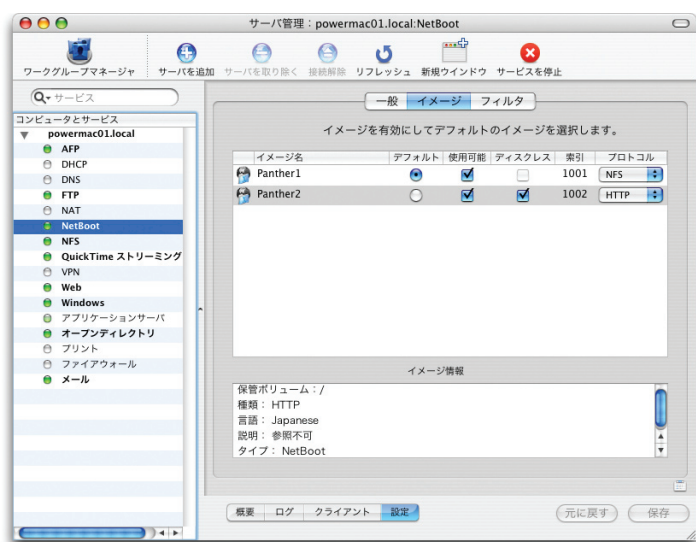


図-4 サーバ管理の「NetBoot」の設定

れるようなネットワーク設計が必要になる。

NetBoot サーバの管理は、Mac OS X Server の「サーバ管理」アプリケーションで行うのが基本である(図-4)。システムのイメージファイルはもちろんだが、シャドーファイルもクライアントに比例して作られる。こうしたファイルの置き場所を任意のボリュームに設定できるなど、運用がやりやすい機能になっている。また、システムのイメージは複数おいておくことが可能である。ある講義と別の講義で違うバージョンのシステムを使わないといけない場合、あるいは場所によって異なるシステムイメージを使うといった運用にも対応は可能である。利用するシステムイメージなどもサーバ管理アプリケーションで選択をすればよい。プロトコルやディスクレスで使うかどうかといった設定もそこで可能である。

起動後のホームディレクトリ運用

起動後、ログインパネルが表示されるが、Mac OS X Server で運用する Open Directory サーバはもちろん、Active Directory、LDAP サーバにあるユーザ情報を用いて認証をすることができる。ディレクトリサービスから得られた情報をもとに、NFS ないしは AFP のサーバをマウントしてそこにホームディレクトリを確保し、ユーザごとのデータを保存しておくことが可能である。また、クライアント側にスタティックなマウントポイントを設定することもできる。クライアントに設定を加えるということは、たくさんのコンピュータにあるシステムを管理する場合には後から変更がないように慎重にした

としても不安は残る。だが、NetBoot だと起動ディスクイメージ自身にスタティックなマウントポイントを設定して運用するというのも、サーバ上にある起動システムに対してだけ行えばいいのである。

Mac OS X では環境設定として、起動したクライアントに対してのさまざまな管理が可能である。項目はたくさんあり、たとえば、CD や書き込み可能ディスク、あるいは外付けディスクの利用を制限したり、利用可能なプリンタを制限したりといったことができる。もちろん、ネットワーク設定などの基本的な設定を一般ユーザは変えられないようになっている。Mac OS X の Dock に登録する項目を強制的に設定できるので、演習科目をスムーズに運用するためにあらかじめ学生のデスクトップに必要なアイコンを並べておくということもできる。

こうした環境設定は、ユーザだけでなく、グループ、あるいは MAC アドレスで識別されるコンピュータのグループに対して適用できる。学生と先生といった区分も可能だが、特定の教室で適用される設定ということも可能なのである。Mac OS X Server を使ってディレクトリサービスを運用した場合には、「ワークグループマネージャ」で環境設定の詳細な設定ができて手軽だが、LDAP 等のディレクトリサービスに該当する属性を定義しておけば、ログイン後に Mac OS X は認識するようになっている。

NetBoot での TCO 削減効果

NetBoot を利用することで、大量のクライアントのシステムをサーバで一元管理することが可能となる。管理者にとってはシステムの調子が悪くなったクライアントのケアをするといったタスクはなくなり、一元化されたシステムのイメージを管理しておけばよい。システムのアップデートやあるいは基本的な設定の変更も、個別のクライアントにインストールしたシステムを管理することに比べれば遥かに少ない労力で行える。クライアントが各所に分散しているとなると、管理にかかる時間は膨れ上がり、結果的には運用コストに跳ね上がるが、NetBoot はシステム自体をサーバに集中させることによる管理コストの低減を実現するのである。

不特定多数が利用するクライアントを大量にかかえる教育機関では、NetBoot によるシステム運用を行うことで、コスト削減につなげることができるといえるだろう。

(平成 16 年 2 月 2 日受付)