計算機センターは今でもユーザのホームディレクトリを預る必要があるのか？
– PICKLES プロジェクトにおける携帯ファイルシステムの試み –

木本雅彦　　大野浩之　　野田明生
東京工業大学大学院 情報理工学研究科

概要

計算機センターのように多数の利用者を扱う環境では、ファイルサーバで集中管理したホームディレクトリをネットワーク経由で共有する手法が従来用いられてきた。この手法ではネットワークやサーバの負荷が増加するだけではなく、利用者の所有物であるホームディレクトリの管理責任が計算機センターに発生するという問題がある。著者らがすすめる PICKLES プロジェクトで提案する手法では、利用者はホームディレクトリを含めた個人情報を小型の記録メディアに記録して携帯し、計算機を利用する場合は「携帯ファイルシステム」を用いてそのメディアを読み書きする。この記録メディアは所有者である利用者の自己責任の下で管理され、その責を計算機センターが負うことはない。本報告では PICKLES プロジェクトで用いられる携帯ファイルシステムの要求仕様と、その実現可能性を示すための実験について述べる。

Why don't computer centers through away responsibility on users' home directories?

Masahiko KIMOTO　Hiroyuki OHNO　Akio NODA
Graduateschool of Information Science and Engineering,Tokyo Institute of Technology

ABSTRACT

Many computer centers construct large scale file servers so that client hosts are able to share applications and home directories. In that case, there are two problems – the heavy network traffic and that computer centers take on the responsibility for management of users' home directories. In the PICKLES project, we propose the following technique. Each user has their personal information including their home directories in a smapp portable disk module and carries it. When he uses a computer, he attach the disk module to the computer, and access to the disk module through a "portable file system." The user owns the disk module and manages it under his own responsibility. The computer centers do not need to take on the responsibility. In this paper, we describe the overview of this technique. From results of some experiments, we show advantages of this technique and specify requirement for the "portable file system."

1　はじめに

計算機センターのように多数の利用者を扱う環境では、ホームディレクトリをファイルサーバに集約し、ネットワークファイルシステムを用いて共有する手法が従来用いられてきた。この手法では、性能がサーバやネットワークの能力に依存するという問題だけでなく、ホームディレクトリの管理責任が計算機センターへ発生するという問題がある。さらに、作業内容を自宅に持ち帰りたいという利用者の要求に応えられない。

これらの問題を解決するために、著者らは、自らがすすめる PICKLESプロジェクトの特徴と運用経験を活用し、「携帯型自己管理ホームディレクトリ」を用いる手法を提案する。利用者はホームディレクトリを含めた個人情報を、携帯可能な小型の記録メディアに記録して携帯する。この記録メディアはハードディスクと同程度のアクセス速度を有し、個人情報を記録するために十分な記憶容量を持つ。利用者が管理すべき情報は、すべてこの記録メディアに記録されており、その管理責任は利用者自身に生じる。

本稿では、まず従来用いられてきた手法を比較するために、研究の背景となっている計算機センターでのファイル管理の現状を述べる。次に携帯型自己

管理ホームディレクトリの概要をのべ、予備調査の内容と結果、および実際にホームディレクトリを持ち歩く際の問題点などについて議論する。

2 研究背景

2.1 計算機センターでのファイル管理の現状

本節では、現在計算機センターで一般的に採用されているシステム設計法について概観し、それらが抱える問題点を列挙する。

大学の計算機センターのように多数の利用者を扱う環境では、ホームディレクトリをファイルサーバに集約し、ネットワークファイルシステムを用いて共有する手法が従来用いられてきた。北陸先端大学院大学では大型サーバを用いた集中管理型ネットワークを構築している [3]。1500 台のクライアントに対して、大型ファイルサーバに利用者のホームディレクトリや共有アプリケーションを集約して管理している。サーバへの依存度が高いため、サーバの 2 重化と定期的バックアップを併用して事故に備えている。高速なネットワークを導入することによって、ファイルサーバの高い応答性を実現している。京都大学では WindowsNT をサーバにしたシステムを構築している [1]。利用者ホームディレクトリの容量制限や、利用者によるアプリケーションのインストールを禁止するようにした点などが苦労した点として挙げられている。九州芸工科大学では PC-UNIX と Windows クライアントが混在した環境を構築している [2]。Windows の起動に時間がかかること、Windows 起動終了時に共有ファイルの読み込み書き戻しに時間がかかることなどが問題の一つとしてあげられている。ファイルの集中管理をすすめたものとして NC [5] や NetPC [6] を用いた環境構築に一時注目が集まったが、これらの方式は共有アプリケーションやホームディレクトリへのアクセスを高速に行うために、高速なネットワークを必要とする。

利用者が扱えるファイル容量を明確にし、かつ自宅などとの情報の移動を容易にするために、大阪大学情報教育センターでは、利用者のホームディレクトリをフロッピーディスクなどの取り外し メディアに保持するという手法をとった [4]。しかしフロッピーディスクでは容量が不十分であり、光磁気ディスクなどの場合は充分な速度が得られない。また、スプールや WWW キャッシュのような情報も利用者の持ち物と考えると、単純にホームディレクトリを保持するだけでは不十分である。

2.2 問題点のまとめ

本節では、計算機センターが抱える問題を整理する。これまでに挙げた事例では、以下の点で問題があった。

- ファイルを共有することにより、高速なサーバやネットワークが必要になる
- 利用者の所有物であるホームディレクトリの管理責任が計算機センターに発生する

ファイルを集中管理することにより、サーバとネットワークへの依存度が増加する。このためサーバの負荷とネットワークトラフィックが増加し、全体としてアクセス速度が低下する。これを解消するために高価な高速バックボーンと高速な大型サーバを導入しなければならない。

集中管理した利用者のホームディレクトリに対しては、バックアップサービスなどを計算機センタが行うことになる。上記の資料ではとり上げられていないが、利用者が休学、退学、死亡した場合などのホームディレクトリの扱いについても、ネットワークの運用規則の中に含めなければならない。企業などと異なり、利用者の著作物は大学の計算機センターが所有権を持つものでないし、多くの場合、所有権を主張する意義もない。利用者のホームディレクトリ管理は、学生の授業ノートの面倒をみるようなものであり、計算機センターにとっては本来の業務の範囲外と考えられる。

また利用者の利便性という点では、自宅の環境との整合性をとりにくいという問題もある。大学の作業結果を自宅の計算機で利用しようとした場合、現状ではフロッピーディスクなどに手作業でファイルを転送して持ち帰るといった方法をとる場合も多い。

3 PICKLESプロジェクト

以下では、計算機センターが抱える問題に対する解決方法として、携帯型自己管理ホームディレクトリを提案する。まず最初に、著者らが 1995 年からすすめる PICKLESプロジェクトについて述べる。自己管理ホームディレクトリの考え方は、PICKLES での情報管理手法に基づいたものになっている。

3.1 PICKLESプロジェクトの目標

最近では「モバイルコンピューティング」という言葉に対して「ノマディック (nomadic – 遊牧民

的) コンピューティング」という言葉が使われることがある。概念的に後者の言葉は「移動した先々で機材を準備してネットワークに接続し、使い終ったら切断して移動する」という現状を正確に表しているといえる。確かに現状ではノートパソコンや携帯電話、モデムカードなどの必要な機材をすべて持ち歩くという、遊牧民スタイルをとらざるを得ない。

しかし移動した先々で必要な機材やネットワークへの接続性がすべて揃っているのであれば、本人は身軽に移動できる。これはテントを始め食糧や衣類まですべて持ち歩かなければならない遊牧民スタイルに対し、クレジットカードだけ持って必要なものがすべて揃っている部屋に宿泊するホテルスタイルといえる。文献 [7] では同様のコンセプトをキャラバン (隊商) とホテルとの比較になぞらえている。

著者らはインターネットの利用者に対してもこのような「行く先々で必要な道具がそろっている環境」を提供する必要があると考え、1995 年から PICKLES プロジェクト [8] [9] [10] をすすめている。著者らが提案する環境は、インターネットにアクセスできる情報キオスクを随所に設置し、利用者向けには最低限の大きさ (カード型) の端末を提供し、両者を連携させた情報サービスを構築するものである。

3.2 PICKLES での情報管理手法

PICKLES が提供する環境では、「情報キオスクが故障したときの復旧をいかに容易かつ迅速に行うか」「分散した多数の情報キオスクをどうやって保守管理するか」「多数の情報キオスク間で同じ環境をどうやって維持するか」といった課題が生じる。故障などの障害時にシステムを迅速に復旧させるためには、故障箇所を迅速に切り分けて代替品と交換する方法が考えられる。しかしハードウェア部品を交換したために、端末の設定情報がすべて消去されてしまい、端末の管理者が復旧作業を行うようでは効率的でない。同様に、OS を更新したために端末の設定情報が消失するのは好ましくない。担当者の責任の範囲を明確にし、管理作業によって互いの責任範疇に影響を及ぼさないような仕組みが必要である。

著者らが採用した方針は、「構成要素を責任の境界によってモジュールに分離し」、「モジュール交換によって保守作業を行う」ものである。まず、ホストの利用者と、管理者、OS 等を保守する人、ハードウェアの販売業者との役割を分離した。ハードウェア販売業者は端末ハードウェアに責任を持つ。最初の 3 者の責任の範囲は、管理する情報で区分けする (図 1)。区分けした情報は、それぞれ異なったモジュールに記録される。

責任者	管理する情報
利用者	個人情報, 認証情報
ホストの管理者	ホストの設定
OS 等の保守管理者	OS, アプリケーション

表 1: モジュールごとの情報の内容

文献 [9] [10] ではホストの管理者と OS 等の保守管理者との責任範疇で情報を分離することによる、システム管理作業の軽減化について述べている。本報告で注目するのは、利用者が管理する情報を分離する手法である。PICKLES で提案する手法では、利用者はホームディレクトリを含めた個人情報をクレジットカード大の記録メディア (以後 携帯メディア) に記録して携帯する。計算機を利用する場合は「携帯ファイルシステム」を用いてそのメディアを読み書きする。この携帯メディアは所有者である利用者の自己責任の下で管理される。その管理責任が計算機センター等にかかることはない。

3.3 PICKLES の現状

PICKLES 情報キオスクのシステムは、現時点では BSD/OS 3.1 を基に機能を追加している。ハードウェアは IBM PC をベースにしており、ディスクモジュールには、着脱可能なケースにいれた IDE ハードディスクを用いている。ホストの管理者の責任範疇の情報を一つのディスクモジュールに記録し、OS やアプリケーションを一つのディスクモジュールに記録する。前者をユーザディスクと呼び、後者をシステムディスクと呼ぶ。通常 PICKLES 情報キオスクは一台のシステムディスクと一台のユーザディスクの組で動作する。ユーザディスクには一般的に /etc 以下に置かれるような設定情報の他、スプール、利用者のホームディレクトリが格納されている (図 1)。

現在 PICKLES は情報キオスクだけでなく、著者らが所属する大野研究室での標準プラットホームとして利用されている。現在約 15 台の利用者端末、3 台のノートブック型端末、3 台のルータ、メールサーバ、WWW サーバ、バックアップサーバが PICKLES に基づいたものになっている。

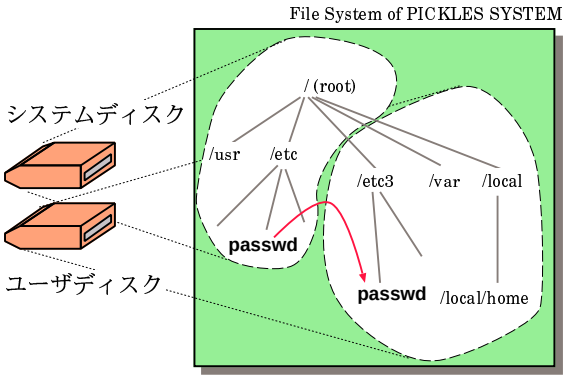

図 1: ディスクの構成

4 携帯型自己管理ホームディレクトリを用いた解決方法の提案

4.1 携帯型自己管理ホームディレクトリ

利用者が管理する情報を分離するために、携帯型自己管理ホームディレクトリを導入する。利用者が所有する情報はすべて携帯メディアに記録する。計算機センタの計算機を利用する場合、自宅の計算機を利用する場合、個人用のノートブックパソコンを利用する場合など、必要に応じてその記録メディアを計算機本体に接続して利用する。これによって、どの計算機を利用しても利用者自身のホームディレクトリを参照できる。

ここで利用者が所有する情報としては、以下が挙げられる。

- 通常ホームディレクトリに保存するファイル
- 一時的な作業ファイル
- プリンタやメールのスプール
- WWW のキャッシュ

計算機を利用し始めるときは、利用者は自分の記録メディアを計算機に接続する。接続を検知した計算機は、まず記録メディアが正当なものであることを検査する。検査の結果正当なものであった場合、記録メディアの内容をファイルシステムの一部として参照できるようにする。次に記録メディアの内容に基づいて利用者を認証する。認証に成功したら、利用者は計算機を利用できるようになる。

携帯メディアとして以下の仕様を想定した。

- クレジットカードと同等の大きさ
- ハードディスクと同程度のアクセス速度
- 数百 MB〜1GB 程度の容量を持つ

すでに IBM 株式会社からコンパクトフラッシュメモリカードと同じ大きさ (43mm × 37mm) のハードディスクユニットが発表されている。このカードは当初 300MB 程度の容量が提供され、1GB を超える容量まで提供されるという発表がなされている。したがってこのような仕様の携帯型ホームディレクトリは充分に実現可能なものであると考えられる。

4.2 予備調査の概要

すでに PICKLES システムでは、すべてのホストに共通な部分と、ホストごとに異なる部分との分離を実現している。後者にはホストのネットワーク設定情報などとスプールや両者のホームディレクトリなどが混在している。例えばネットワーク設定はホストごとの情報だが、PPP アカウントの設定などは利用者が保持する情報になる。携帯型自己管理ホームディレクトリを実現するためには、まず利用者の責任範疇の情報を抜きだす必要がある。

また携帯メディアを計算機に接続した際には、何らかの基準に基づいて、携帯メディアの正当性を検査しなければならない。利用者の携帯メディアが接続されていない場合でも、通常計算機は動作している。携帯メディアが接続された場合は、動作中のプロセスのうちスプールなどの領域を参照しているものを一旦終了させ、携帯メディアをマウントした後に再度起動するという手続きを踏む必要がある。

まず最初に、システム動作にこのような処理を行った場合に正常な動作を続けることが可能か否かを確認する必要がある。これらの処理の実行にどの程度の時間を要するのか把握しておく必要もある。そこで、予備調査として以下を行った。

1. 動作中のシステムに対して、終了させる必要があるプロセスをすべて停止し、利用者の記録メディアをマウントした後、終了させたプロセスを再度起動し、その時間を計測する。
2. ある基準を設けて正当性検査を行い、その時間を計測する。

実験に用いた機材について述べる。携帯メディアには、I/O データ製 520MB PCMCIA TypeIII のハードディスクドライブ (PCHD-520c) を用いた。計算機の性能は、MMX Pentium200MHz, 主記憶 32MB である。上記のドライブを図 2 のパーティションに切った。

調査 1 では 1) 動作中のプロセスを停止し、 2) 携帯メディアの全パーティションをマウントし、3)

パーティション名	マウント先	容量
e	/etc3	8MB
f	/var	64MB
g	/local	430MB

表 2: 利用者用記録メディアのパーティション

再度プロセスを起動する、という一連の処理をシェルスクリプトで行い、全体の時間を計測した。

調査 2 では携帯メディアの正当性の検査を行った。今回は不正な HDD の条件として、setuid 属性が有効になっているファイルが存在していることと、ファイルのユーザ ID、グループ ID が適正な範囲を超えていることとした。正当性の検査として、fsck によるファイルシステムの試験と、すべてのファイルのユーザ ID, グループ ID を調査した。

4.3 予備調査の結果

結果として調査 1 での手続きを実行したあとでもシステムは正常に動作し続けた。また、調査 1 の手続きにかかった時間はおよそ 15 秒であった。正当性検査に要する時間はおよそ 40 秒であった (ホームディレクトリには 100MB 程度分のファイルがあった場合)。利用者が記録メディアを装着してから、計算機を利用できるようになるまでには、最大でおよそ 55 秒程度必要ということになる。文献 [2] では WindowsNT を用いたクライアントの起動時間としてセルフチェックを含めた場合約7 分と述べている。またサーバからのデスクトップの読み込みを含めたログインに要する時間を 15 秒から 2 分 14 秒 (デスクトップに 100MB のファイルがあった場合) と述べている。独自に Windows98 の起動に要する時間を計測したところ、約 50 秒であった。これらの値と比較すると、ほぼ実用になる速度であると考えられる。

5 考察

5.1 携帯型ホームディレクトリを実現する際の問題点

再起動手続き

今回の調査では、動作しているすべてのプロセスを一旦終了させてから、利用者の記録メディアをマウントした。しかし終了する必要があるプロセスは、ユーザディスクのファイルをアクセスしているものだけでよい。再起動するプロセスをより分けて、必要なプロセスだけを再起動するべきである。

SystemV UNIX で用いている実行レベル (run level) と類似の概念を、「携帯メディア接続時に終了させるプロセスとそうでないプロセスの違い」という視点で導入することも考えられる。

携帯メディアを取り外す際の手続き

今回は携帯メディアとして用いた PCMCIA 接続の HDD カードは、動作中に引き抜けるという欠点がある。そこで不必要な抜き差しを物理的に防止する機構が求められる。また利用し終ったら自動的に排出される機構が望ましい。

ノートブック型の計算機の場合は、サスペンド状態の時には携帯メディアを抜き差しできるようにしたい。このためには、サスペンド状態に入る時のイベントを検知して、自動的に不必要なプロセスを停止させて携帯メディアのマウントを解除する機構が必要である。

仮に利用者が強引に携帯メディアを取り外した場合でも、破損するのは利用者の携帯メディアの内容だけにとどめて、計算機側が故障することがあってはならない。

正当性の条件

今回の調査では、setuid 属性や不適切なユーザ ID を不正なものとした。ているか否かを挙げた。setuid 属性についてはマウント時に無効にできるため、今回実質的に調査対象となったのは後者であった。後者の問題はシステムディスク側の UID との衝突が問題になる。仮にファイルシステムの段階で UID を決められた安全な値の範囲に変換すれば、この検査は必要なくなる。場合によっては利用できるサービスを制限するかわりに正当性検査を簡略化する選択肢を提示することも考えられる。しかし厳密には何らかの方法でデータ本体の不正な改善などを検出できなければならない。正当性の条件については、議論の余地がある。

バックアップ

携帯メディアを用いる場合、バックアップ作業は利用者の自己責任のもとで行われる。利用者支援のために、何らかのバックアップサービスを準備する必要はある。また、ホームディレクトリの本体を自宅ないし大学の計算機に置いておき、よく使うファイルだけを自動的に携帯メディアに取り込むような利用方法も考えられる。

ファイルの分類

利用者が持ち歩く携帯メディアには、送信キューに溜っているメールや未処理のプリンタスプールな

ども記録される。これらの情報を保持したまま、携帯メディアを他の計算機に接続したときに、その計算機で送信処理や印刷処理を継続しては困る場合がある。計算機を渡り歩くごとに新規にスプールディレクトリを生成すると共に、以前のスプールディレクトリの処理を続行するか否か利用者が選択できることが望ましい。

また、一部のファイルについては計算機ごとの内容と利用者の携帯メディアの内容とを合成して利用したい場合がある。例えばパスワード情報の場合、管理者パスワードはその計算機のものを用い、利用者のパスワードは携帯メディアのものを用いるような使いかたが考えられる。携帯メディア装着時に自動的にファイルの内容を合成し、実際に参照されるファイルを自動生成する方法や、複数のファイルを合成して単一のファイルとして提示できるファイルシステムを開発する方法が考えられる。

セキュリティ

今回の実験では、正当性の試験のみを行った。実際に安全に使うためには認証機構が必要となる。この場合、1) 携帯メディアの認証、2) 利用者の認証の 2 段階が必要になる。ここで SmartCard 等の技術を応用することを考えると、認証のための計算能力を持った携帯メディアが必要である。

また携帯メディアの紛失等の事故を考えると、携帯メディアの内容はすべて暗号化されている必要がある。暗号化ファイルシステムの導入も検討するべきである。

5.2 携帯ファイルシステムの要求機能

本稿では携帯型自己管理ホームディレクトリの実現可能性についての予備実験を行った。実際に携帯ホームディレクトリを実現するためには、利用者の記録メディアは、何らかの「携帯ファイルシステム」を経由してアクセスする。これまでの考察をまとめると、ここでの携帯ファイルシステムには以下の機能が求められる。

- ファイルのユーザ ID, グループ ID の変換機能
- 情報の暗号化機能
- 複数のファイルを合成して単一のファイルに見せかける機能
- 良く使うファイルだけを自動的に携帯メディアに取り込む機能

これ以外に携帯メディアの記録容量が不足するという問題を解決するため、圧縮機能が望まれる。

6 おわりに

計算機センターでのファイル管理の問題点を挙げ、これを解決するための「携帯型自己管理ホームディレクトリ」を用いた手法を提案した。本手法は、PICKLES プロジェクトでの情報管理手法の特徴を活用することにより、利用者の個人環境の管理責任を分離できる。予備実験を行った結果、この手法は実用可能であるという感触を得られた。今後は携帯すべき情報を整理し、研究室規模での実験をすすめ、本文中で述べた携帯ファイルシステムの開発を検討する。

参考文献

[1] 丸山伸, 辻斉, 藤井康雄, 中村順一, 総合情報メディアセンターにおける WindowsNT による大規模分散システムの管理・運用, Feb. 1999, 情報処理学会, DSM シンポジウム

[2] 藤村直美, 来海義英, 平山善一, 情報処理教育のための共同利用パソコン運用上の問題 Feb. 1999, 情報処理学会, DSM シンポジウム

[3] 敷田幹文, 井口寧, 丹康男, 松澤照男, 大規模分散システムのための集中運用管理における効率化技術の提案, Feb. 1999, 情報処理学会, DSM シンポジウム

[4] 斎藤明紀 他, 多人数教育計算機環境におけるシステム管理の省力化の一方法, Jul. 1997, 情報処理学会, 分散システム運用技術研究会 研究報告

[5] Network Computer Inc., http://www.nc.com/

[6] NetPC Specification, http://web.jf.intel.com/design/netpc/netovr.htm

[7] Frank Stajano and Alan Jones, The Thinnest Of Clients: Controlling It All Via Cellphone, October 1998, MC2R Volume 2 Number 4,, ACM SIGMOBILE,

[8] 木本雅彦, 大野浩之, 街角公衆情報端末計画 ～ PICKLES の概要～, Mar. 1996, 第 52 回全国大会 講演番号 3Y-2

[9] 木本雅彦, 大野浩之, 自律型ネットワーク端末 (PICKLES) を用いたシステム運用技法, Feb. 1998, 情報処理学会,DSM シンポジウム

[10] Masahiko KIMOTO and Hiroyuki OHNO, A way to the ubiquitous computing: Design and implementation of the PICKLES information kiosk, Mar. 1998, Proceedings of IEICE Internet Workshop '98