2003－DSM－31　(3)
2003／11／26

グループ利用に対応したファイル操作インタフェース

岸場清悟　西村浩二　田島浩一　相原玲二

広島大学 情報メディア教育研究センター

大学などで運用される共同利用サーバにおいて，サーバ上で公開しているWebページを協同して保守する場合などにグループ利用を行いたいことがある．しかしUNIXファイルシステムのグループ機能ではいくつか問題点があり運用しにくい．いっぽう大多数の利用者にとってはサーバ機能を従来のシェルコマンドでなくWebブラウザインタフェースで利用することがいまや必須の要件となりはじめている．これらの要求に応えるため，Webベースのサーバ利用ツールusermin にグループ利用に対応する認証機能の実装を行い，運用の効果を評価する．

File Operation Interface for User Group

Seigo Kishiba　Kouji Nishimura　Kouichi Tashima　Reiji Aibara

Information Media Center,　Hiroshima University

In running Web servers for organizations such as universities, users need to use servers as users' group, such as purpose for corporate maintenance of Web pages. But it is difficult to use function of group in UNIX file system because of some administrative problems. By the way, most of users want to use function of server with GUI such as Web browser, not with CUI shell commands. To satisfy these requests, we installed authorization function for group usage to Web based server access tool *usermin,* and evaluate the tool.

1. はじめに

広島大学情報メディア教育研究センター（以下センター）では，大学構成員全員にセンター利用アカウントの取得権限を与えており，これによって取得される「個人アカウント」を使って大学構成員全員が各個人の権限によって電子メールやＷｅｂページ公開，演算サーバ利用といったセンターサービスを受けることができる．

いっぽうこのような個人の資格ではなく，複数人からなるグループでセンターサービスを利用する要求がある．たとえば部局や研究室のＷｅｂページやメールアドレスの利用が考えられる．センターではこのような要求に答えるために，UNIX のアカウント管理機能・グループ管理機能とそれらを制御するよう構築した利用者管理システムを用いて実装した独自のアカウント体系「グループアカウント」を現行センターサービスの開始時（２０００年４月）より導入した[1]．これはセンターの共同利用サーバ上で該当アカウントに提供されるサービスの複数人による共同利用とシステム上の利用者個人の認証とを両立させるもので，実運用としては他に例を見ない．

しかし実際にグループアカウントを運用するなかで，このサービスに利用者にとって使いにくい部分があることが明らかになった．授業利用や事務組織での業務形態との齟齬が大きかった[2]のと同時

に，アプリケーションプロトコルの独自拡張によってグループアカウントを実装したためにクライアントアプリケーションによっては利用ができない状態をひきおこした．

従来から汎用的に使われているアプリケーションの利用を継続して提供しながらこの問題を解決し，利用者が使いやすいＧＵＩベースでのグループ利用を実現する手段として，この報告では Web ブラウザを用いたファイル操作ツールのグループ利用対応を提供する方法を提案する．

２．グループアカウント

２．１　グループアカウントの実装と運用

「グループアカウント」の基本アイデアは次のようなものである．全ての利用者はセンターのサーバに「個人アカウント」を持っており，そのアカウントを使ってサーバを利用できる．この前提のもとに「グループアカウント」を作成し１名の課題管理者を置く．課題管理者がグループメンバーの個人アカウントを登録することにより，グループメンバーはそれぞれ個人アカウントでの認証を経て「グループアカウント」の機能を使うことができる（表１）．

表１　グループアカウントで提供される機能

利用者種別	グループアカウントで提供する機能
課題管理者	グループメンバーの登録・変更（センター利用者管理システムによる） グループアカウント保守のための sudo によるサーバ利用機能 グループアカウント宛の電子メールを転送して個人アカウントで受け取る
グループメンバー	FTP によるファイル転送機能 newgrp によるグループアクセス機能 Web ページの協同での保守

サーバ上の実装としては該当アカウントのプライマリグループをそのアカウントに固有のグループとし，セカンダリグループとしてグループメンバーの個人アカウントをそのグループに登録することにより，「複数の個人アカウントが利用可能なグループアカウントのホームディレクトリ」を実現する．ただしセンター利用の公平性と安全性を確保するために，さらに若干の作りこみを行なっている．

UNIX ファイルシステムでグループへのファイルパーミッション許可をグループアカウントのホームディレクトリに与えてグループに所属する個人アカウントからファイルを作成すると，作成したファイルのオーナーは作成者のアカウントになる．センターのサーバは quota 管理をアカウント単位で行うシステムであるため，この方法ではグループアカウントに対する管理が正しく行えない．したがってグループアカウントの属するファイル操作をグループアカウント権限で行う必要がある．

いっぽうネットワークに繋がる共同利用サーバは万一の abuse に備え，システムの利用ログから利用者個人を特定する機能を持たせることが望ましい．このためサーバ利用は常に個人アカウントの認証を経て行う必要がある．

これらの要件を両立するため，グループアカウントを次のように運用している．

- パスワードを所属者が共有できなくなるようグループアカウントにはログインパスワードを付与しない．グループアカウントへの直接ログインサービスは提供しない．
- メール受信は .forward による個人アカウントへの転送で対応する．
- Web ページ保守に必要なサーバへのファイル転送には FTP サービスを提供する．この FTP サービスは個人アカウントの認証でできるよう作りこみを行う．

２．２　グループアカウント利用上の問題点

グループアカウント導入の主なターゲットである協同での Web ページ保守を実現するために，FTP サーバについては認証部分のユーザ名を「個人アカウント名@グループアカウント名」とする拡張形式を導入し，個人アカウントとそのパスワードの認証によってグループアカウントの権限を与えることで FTP を用いたグループアカウント対応のファイル転送を実現した．ところが FTP クライアントアプリケーションによってはこのユーザ名形式がクライアント側で「アカウント名@ホスト名」と解釈され，結果としてそのクライアントでは FTP が利用できなくなる事態を引き起こした．

また .forward による個人アカウントへの転送では，多くの利用者が「個人アカウント宛とグループアカウント宛のメールを手元で区別して扱えない」という不満を抱えていることがセンターへの問い合わせ数の増加により判明している．

このように「グループアカウントが使いにくい」という印象を利用者に与えるそもそも原因として，

- FTP 等ネットワークアプリケーションの認証部プロトコルへの独自拡張を安易に付加した
- sudo 等のコマンドラインインタフェースを使用できない利用者層を想定しているのに，サーバ利用のための適切なユーザインタフェースが提供されていなかった

ことがあげられる．

グループアカウントに全くパスワードを発行しないのではなくグループアカウントの管理責任者１名だけにパスワードを渡し，POP によるメール受信などパスワードを必要とする作業は管理責任者のみが行う運用とすることも考えられる．それでも主なアプリケーションについてグループ所属者が利用できる仕組みは必要である．アプリケーション毎に上記 FTP と同様の仕組みを作りこむのはコストがかかりすぎ，運用上の問題を引き起こしやすい．

これらを解決する手段として，グループ利用に対応したファイル操作のためのＧＵＩをＷｅｂブラウザ上で提供することが考えられる．共同利用サーバに対して多様な利用者が使うものであることも考慮すると，求められる要件は次のとおりである．

- あるグループに所属する利用者が, 個人アカウントでの認証を経てグループアカウントのホームディレクトリ上のファイルを扱えること．
- クライアント PC とサーバとのあいだでファイル転送ができること．
- ファイルパーミッションを利用者が自分の意思で変更できること．
- 利用者の操作説明が使用時に提示されること．
- パスワードをやりとりするので，サーバとの通信経路が暗号化されること．

３　グループ利用対応ファイル操作インタフェースの実装

３．１　WebDAV のグループ利用対応

WebDAV[4]は Web 上での文書共有のために作られた http をサーバ上のファイル操作を行えるように拡張したプロトコルである．利用者認証やファイル操作のための権限委譲については WebDAV 自体は機能を持たず，WebDAV を実装する http サーバの機能に依存している．

UNIX システム上でアカウントごとのホームディレクトリに対するファイル操作を提供する仕組みとして, Apache+mod_DAV+mod_auth_userdir を用いる実装がある[5]. これは URL から利用するアカウント名を導き，そのアカウントに関する認証を経て該当するホームディレクトリへのアクセスを提供するものである．これをグループ利用に対応させるには，URL から導かれるサーバ上のファイル操作先がグループアカウントのホームディレクトリである場合に，個人アカウントによる適切な認証を経てグループアカウントの権限でファイル操作を行うようにすることが必要である．mod_auth_userdir を修正して, Basic 認証でＷｅｂブラウザから渡される個人アカウントとパスワー

ドの組の認証とその個人アカウントがグループアカウントに所属することの認証を経てグループアカウントへ権限委譲することによって実現できる（図１）.

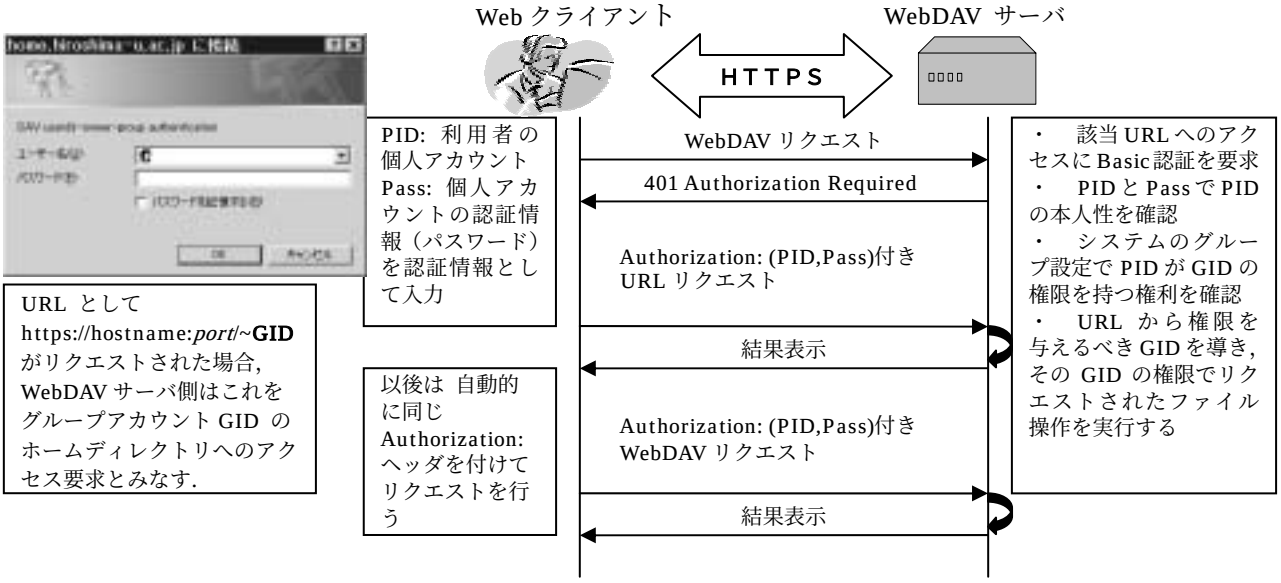

図１．WebDAV のグループ対応実装概要

クライアントとして Windows XP のエクスプローラを使ったところ，初期設定はやや難しく思われるところがあったが，ネットワークプレースとして設定が終わればその後はほとんどローカルファイルを扱うのと同様の良好な操作感が得られた.

WebDAV プロトコルは RFC として規定されている[6][7]などインターネットでの標準性が高く, 広範なクライアントで利用可能であることが期待できる．しかし WebDAV はもともと文書の共有とバージョン管理のためのプロトコルであるため，ファイル操作に関してはファイルアップロード，リネーム，削除のファイル操作とそれに必要なファイルロックなど最低限の機能しかない．ファイルパーミッションの利用者による設定はできないなど，FTP をこれで置き換えてしまうには機能が不足している.

３．２　usermin のグループ利用対応

usermin はもともとサーバ管理 Web インタフェースとして作られた webmin[3]から派生したツールで，Web ブラウザを用いたサーバへの接続を利用者に提供する．この中で JAVA アプレットモジュールとして提供されているファイルマネージャは，ファイルの双方向転送のほか，リネームやパーミッション変更，ファイル内容の編集も可能で，一般のファイルマネージャに要求される機能を十分に備えている（ただし編集についてはマルチバイト言語対応が未だ施されていない）.

usermin の利用者認証には Cookie を用いたセッション認証が標準的であり, セッション開始時にアカウントとパスワードの組を入力して認証を得る．これをグループアカウント対応とするために，個人アカウントとパスワードの組のほかに「ログインするアカウント」の入力を求めるようセッション開始画面を修正した（図２）．サーバ側ではこの入力に対し個人アカウントとパスワードの組から本人性を確認し，その個人アカウントでのログインアカウント利用の正当性を認証する．認証が通ったセッションに対して指定されたログインアカウントの権限を与えることによってグループアカウントでの利用が可能となる.

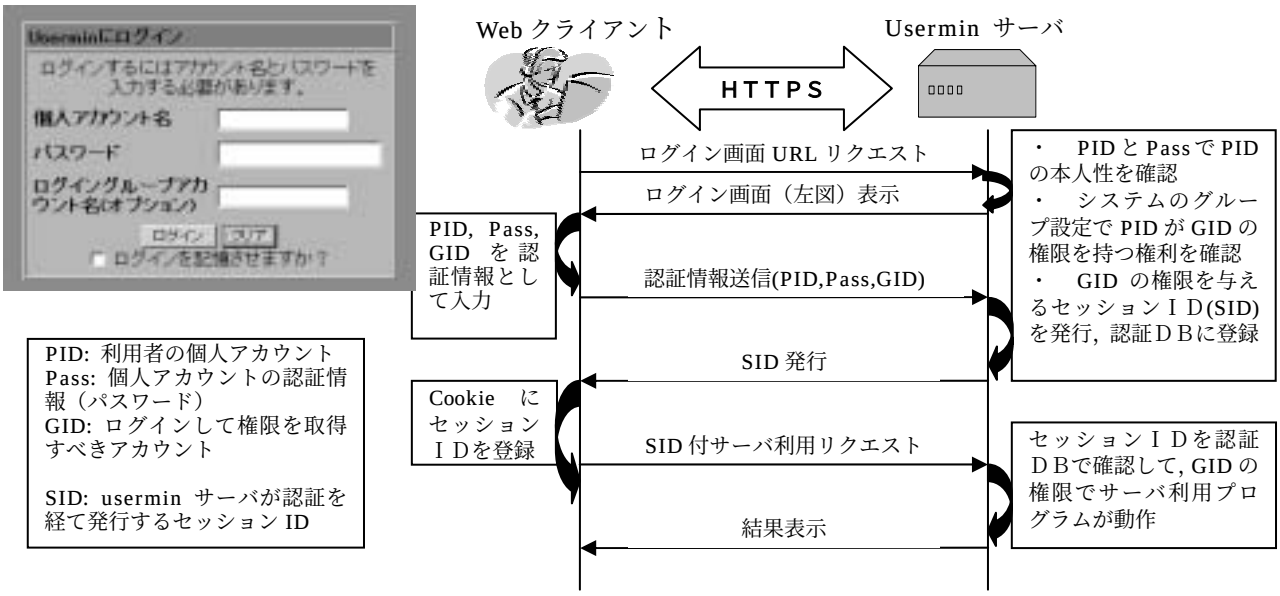

図２．Usermin のグループ対応実装概要

usermin のグループ対応の使用感は良好で，ログイン画面の誘導による自然な認証を経た後は違和感なくグループアカウントのホームディレクトリを操作できる. ただしファイルマネージャは Java アプレットであるため，使用できるクライアントに制限が生じる難点がある．メニュー表示の日本語対応はできているが，ファイル名やファイル内容については未対応の部分が多く，編集機能については２バイト文字が入ると使いものにならない．いっぽう CGI だけで実装したファイル転送モジュールもあるが，これはサーバへファイルを転送する最低限の機能しか持っていない.

usermin モジュールはそのセッションで認証されたアカウントの権限で CGI と同様に実行するので, 利用者がサーバにシェルログインしてコマンドを実行するのとほぼ同等の機能を Web ブラウザからの操作で実現できる．今回使用してみたファイル操作ばかりでなく，サーバ上の各種アプリケーションの利用や利用者環境設定のためのＧＵＩとして使用できるだろう.

４．おわりに

「グループアカウント」の運用上の問題を解決する手段の手がかりとして，グループ利用に対応したファイル操作インタフェースを usermin と WebDAV(apache+mod_dav)をベースに実装し, それぞれの機能を評価した．従来行っていた FTP サーバの作りこみも含め３つのグループ利用対応手法について要件を比較すると表２のようになる．特に usermin を使うことによって従来の手法に比べ多くの点で改善がみられることがわかる.

WebDAV, usermin ともまだできて間が無く，特に日本語対応の点については未実装の部分が多く残っているので，従来のアプリケーションを完全に置き換えて運用するにはまだ時間がかかるように思われる．しかし個人アカウントによる認証を経たグループ利用への対応という点については良好な結果を得た．認証部分は正しく動作することが確認できたので，次は実際に運用を行う中で問題点を洗い出すとともに機能性能について定量的に評価したい.

従来からある個人での利用とグループ利用をひとつのサーバで両立させるには，サーバの提供するアプリケーション全体で一貫した認証の仕組みの検討とともに共同利用サーバの運用，特にホームディレクトリを持つファイルシステムの構成についてさらに検討を進める必要がある.

表２　グループ利用要件に関する実装間の比較

	FTP サーバ	WebDAV	usermin
利用者認証のグループ利用への対応	△	○	○
クライアントソフトウェアの普及	○	○	○
ファイル転送機能	○	○	○
ファイルパーミッションの利用者による変更	○	×	○
グループ対応操作説明を利用時に表示	×	○	○
通信経路の暗号化	×	○	○
ファイル名の日本語対応	○	△	△
ファイル転送以外のサーバ利用への拡張	×	×	○

（△は機能としては対応しているが問題があるもの）

謝辞

「グループアカウント」および本システムの開発・支援・運営は広島大学情報メディア教育研究センターのスタッフの協力を得ています．ここに記して謝意を表します．

参考文献

[1] 岩沢和男，津久間秀彦，新畑道江,岸場清悟，入江治行，稲垣知宏，隅谷孝洋，秋元志美，勇木義則，大学情報サービス基盤としてのアカウント体系，学術情報処理研究 No.4, pp63-72, 2000
[2] 岩沢和男，津久間秀彦，岸場清悟，隅谷孝洋，アカウント体系再編の評価，学術情報処理研究 No.5, pp43-48, 2001
[3] webmin http://www.webmin.com/
[4] WebDAV http://www.webdav.org/
[5] mod_auth_userdir http://www.sera.desuyo.net/apache/mod_auth_userdir
[6] RFC2518 http://www.ietf.org/rfc/rfc2518.txt
[7] RFC3253 http://www.ietf.org/rfc/rfc3253.txt