

Windows Server 2003 でのユーザ管理と Unix との連携

鬼頭良彦*、藤原富未治*

*工学研究科・工学部技術部 電子・情報技術系

はじめに

現在我々が行っている依頼業務の中に電子情報システム専攻共通計算機室管理がある。この計算機室の計算機環境としてはワークステーションとパソコンが混在しており、OS も Unix、Windows と異なるものが稼働している。この為、ユーザが計算機を利用するには管理者がそれぞれのサーバにユーザ ID を作成し、サーバ間でユーザ ID とパスワードの統合を常に図る必要があった。また、Windows に関しては脆弱性用の修正更新が頻繁に起こるため、管理サーバでもその更新に対応できるように検討を心掛けておく必要があった。

そこで将来的検討事項として現サーバ OS の Windows 2000 Server (以後 2000 Server という) を Windows Server 2003 (以後 2003 Server という) に移行した場合を想定して、管理方法の習得及び問題点の検証、ユーザデータの移行方法、Unix と Windows のパスワード同期の検証等の研鑽を行ったので報告する。

1. システム構成

システム構成はパソコンを 3 台、ワークステーション 1 台、OS 交換用ハードディスクを 3 台準備し、ディスクには 2000 Server、PC-Solaris8、PC-Solaris9 といった OS をインストールしてディスクを交換することによって構成を変更した。また、検証はルータによってローカルネットワーク環境の中で行った。

- 1) 2003 Server の構築・設定の検証 (図 1. 中①)
- 2) 2000 Server から 2003 Server へのユーザデータ移行の検証 (図 1. 中②)
- 3) 2003 Server と Solaris Server (PC-Solaris 8, 9) とのパスワード同期の検証 (図 1. 中③、図 1. 中④で OS ディスク交換)

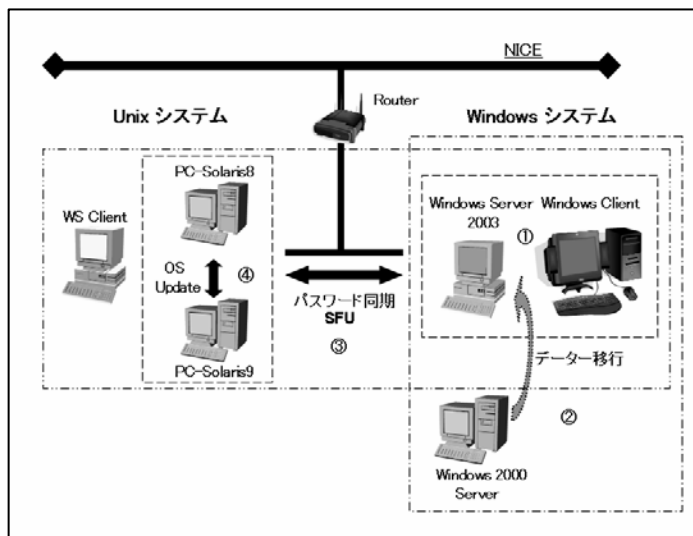


図 1. システム構成図

2. Windows Server 2003 の構築・設定

現システムで利用している 2000 Server ではユーザファイルの共有が目的のため、集中管理を行っていたのはユーザ ID、パスワード、ユーザデータのみでセキュリティアップデートや計算機の環境設定はクライアント側で行ってきた。その為、2003 Server 構築にあたり、クライアントの環境設定等の管理も集中して行うことを前提に構築を行った。今回サーバ構築に使用した OS は


```
net share c:¥ユーザ Dir¥%4¥%1 /delete (共有アクセス権削除)
net share %1=c:¥ユーザ Dir¥%4¥%1 /grant:%1,full (共有アクセス権作成)
cd C:¥バッチファイル Dir (バッチファイルディレクトリへ移動)
```

4. Windows Server 2003 と Unix サーバとのパスワード同期

Unix と Windows が混在した環境でパスワード同期を行うソフトとしては Microsoft Japan から SFU (Service For Unix 3.5) というソフトが提供されており、現在の Sparc Solaris 8 と 2000 Server の環境では既に利用している。但し、SFU はサポートされている環境に制限があり、Unix 環境では Sparc Solaris 7 と 8、HP-UX Ver. 11i、IBM AIX ver. 5L と 5.2、Redhat Ver. 8.0、Windows 環境は Windows 2000 Professional、Windows XP Professional、Windows 2000 Server、Windows Server 2003 のみで、その他の OS で利用する場合予め動作確認をする必要がある。

今回研鑽では将来的に起こりえる機種変更および OS のアップデートを想定し、Unix サーバとして PC-Solaris 8 と 9 を使って検証を行った。

1) 2003 Server の設定

2003 Server の SFU で、パスワード同期の方向、暗号キー、ポート番号等の設定を行う。パスワード同期の方向では Unix サーバの IP アドレスとパスワード変更の際の同期方向の指定を行う。研鑽では Windows から Unix、Unix から Windows の双方向の設定を行った。また、Unix クライアントが増えた場合はその IP アドレス等の設定を行う必要がある。暗号キーは Windows と Unix で同期をとる際の認証用暗号キーで独自に設定する。ポート番号は Windows と Unix で同期をとる際に使用する通信ポートの番号を設定する。

2) Unix サーバの設定

Unix サーバでは Unix システムにあるパスワード認証用ファイル pam.conf ファイルの編集と SFU 付属の pam_sso.so.1、ssod、sso.conf ファイルを Unix システムに追加をする。pam.conf は認証モジュールの設定が記述してあり、パスワード同期の為の pam_sso.so.1 の設定を記述する。ssod はパスワード同期の為のデーモンだが、SFU 付属のファイルは Sparc 版 Solaris 用のため PC-Solaris では動作しなかった。このためアメリカの Microsoft から PC-Solaris 用 ssod をもってくる必要があった。sso.conf はパスワード同期の為の設定ファイルで Windows サーバの IP アドレス、Windows サーバと同じ認証暗号キーとポート番号の記述等の設定を行った。また、パスワード同期の設定に直接関係しないが Unix サーバの再起動時に ssod デーモンが自動的に起動するように設定が必要である。

3) Unix クライアントの設定

Unix クライアントでは Unix サーバと同じ設定で ssod ファイルを除いた pam.conf、pam_sso.so.1、sso.conf ファイルを設定する。

4) パスワード同期

パスワード同期では Unix 側と Windows 側では動作が異なる。Windows クライアントでパスワード変更を行った場合図 2. 中①で示

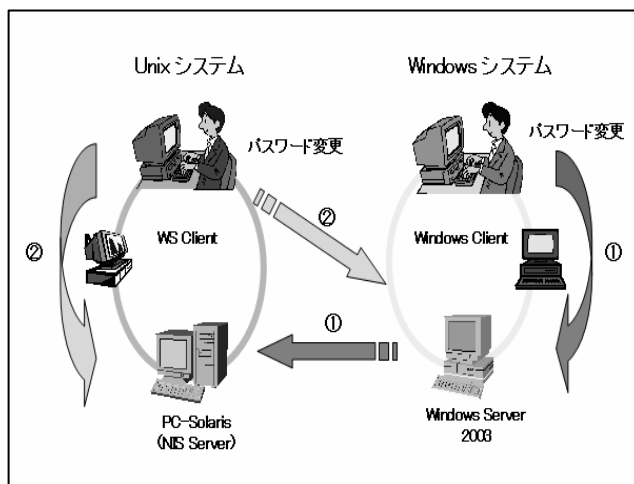


図 2. パスワード同期の流れ

すように 2003 Server に変更情報が送られ、2003 Server から Unix サーバにも変更情報が送られる。一方 Unix クライアントでパスワード変更を行った場合には図 2. 中②で示すように UNIX サーバと Windows サーバ双方に情報が送られることになり、Unix と Windows 双方のパスワードの同期がとられる。

5) PC-Solaris8 と PC-Solaris9 の設定の相違点

UNIX サーバの OS バージョンの違いによる設定の相違点は pam.conf ファイルのモジュール表示形式が異なるので編集の際にはそのバージョンの表示形式に合わせる必要があった。

5. まとめ

Windows Server 2003 のインストールから設定までを行ない、サーバ構築のイメージをとらえる事ができ、集中管理に関しても一部検証を行って技術の習得ができたが、2003 Server にはまだ、様々の集中管理の為の技術が残されているので、今後も継続して検証を行っていく予定である。

Windows 2000 Server から Windows Server 2003 への移行に関しても実際にデータ移行を検証し、注意点の確認やバッチファイルの作成を行い、時間短縮の為の技術も習得できたので依頼があった場合でも対応ができる事を確信した。

将来的な検討として Solaris の OS バージョンの違い、機器の違いによるパスワード同期の検証を行ったが、設定ファイルの修正で対応可能であることの確認が得られた。

参考文献

- ・ Windows Server 2003 実践ガイド, 村嶋修一著, 技術評論社
- ・ Windows Server 2003 必携 Bible, 宋倉幸則著, 技術評論社

検証ソフトダウンロードサイト

- ・ Windows Server 2003 R2, Enterprise Edition 180 日限定評価版 :
<http://www.microsoft.com/japan/windowsserver2003/evaluation/trial/default.msp>
- ・ ファイルサーバ移行ツールキット :
<http://www.microsoft.com/japan/windowsserver2003/upgrading/nt4/tooldocs/msfsc.msp>
- ・ SFU (Service For Unix3.5) :
<http://www.microsoft.com/downloads/details.aspx?displaylang=ja&FamilyID=896C9688-601B-44F1-81A4-02878FF11778>
- ・ PC-Solaris 用 ssod :
<http://www.microsoft.com/downloads/results.aspx?pocId=&freetext=ssod&DisplayLang=en>