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

○鬼頭良彦 A)、藤原冨未治 A)

A) 部局系技術支援室　工学技術系第１技術課（情報通信）

はじめに

現在行っている依頼業務の中に専攻共通計算機室の管理がある。この計算機室の計算機環境はワークステーションとパソコンの２種類の機器が設置されているため、ユーザー管理は Unix と Windows それぞれのサーバで管理を行ってきた。そのため、ユーザーが計算機を利用するためには、Unix と Windows の二つのパスワードを各自で管理する必要があった。

そこで、その不便さを解消するために Microsoft Japan から提供されている SFU(Service For Unix)を利用し、Unix と Windows のどちらの計算機でパスワード変更を行ってもサーバ間でパスワードの同期を行うことによって一つのユーザーID とパスワードで双方の計算機が利用できる環境を整備したので紹介する。

1　共通計算機室のシステム状況

共通計算機室のシステム状況を紹介する。

Unix システムの OS はサーバ、クライアント共に Solaris8、クライアント数 27 台、ユーザーID 管理はサーバに NIS と NFS によって一元管理を行っている。そしてクライアントの１台で Samba を立ち上げ Windows システムとのファイル共有を行っている。

Windows システムの OS はクライアントに WindowsXP、サーバに Windows Server 2003 を利用してユーザーID の一元管理を行っている。クライアント数は 28 台である。

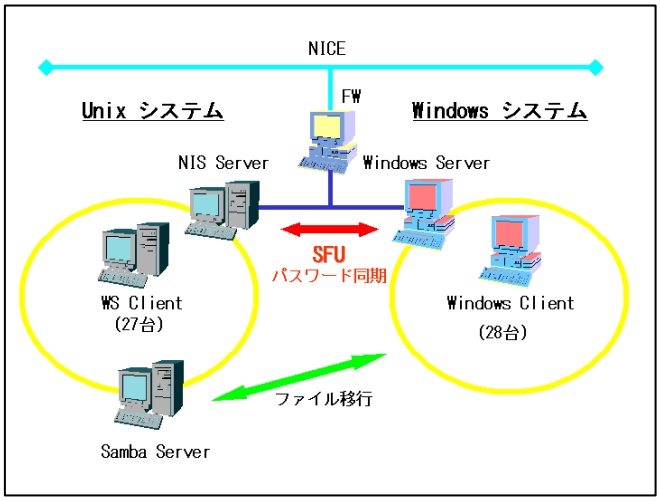

図１．共通計算機室システム

システムの利便性のために以前より SFU を使ってパスワードの一元管理を検討していたが、初期の頃は有償であったため利用を見送っていた。しかし、現在は無償で利用ができるため、SFU の導入によってパスワードの一元管理を行うことにした。

2　ＳＦＵ(Service For Unix)

SFU は Unix と Windows 間でパスワード同期を行うソフトで現在のバージョンは 3.5 である。SFU はサポートしている OS に制限があり、Unix では Sparc Solaris 7 と 8、HP-UX Ver.11i、IBM AIX ver.5L と 5.2、Redhat Ver.8.0、Windows では 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行う必要がある。

SFU は Windows サーバにインストールを行い、Unix 側も認証関連ファイルの修正を行う。

3　Windows Server 2003 の設定

図２と３が Windows サーバにインストールした SFU の設定画面である。この画面ではパスワード同期の方向、セキュリティの構成、ポートの構成、パスワード同期の再試行回数、ログの作成の設定を行う。

パスワード同期の方向では Unix と Windows のシステムでパスワード変更を行った際にもう一方のシステムに同期を行うかどうかを選択する。

セキュリティの構成では同期を行うサーバ同士のセキュリティ確認のため、暗号キーを生成し、Unix と Windows のサーバ双方に同じ暗号キーをセットし、認証を行う。

ポートの構成では同期を行う場合のポート番号の設定を行う。

パスワード同期の再試行回数は同期に失敗した場合の再試行回数と再試行までの時間の設定を行う。

ログの作成はログを記録するかどうかの設定を行う。

ローカルコンピュータ上のパスワード同期では同期を行う 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。

図 2.　SFU 設定画面 1

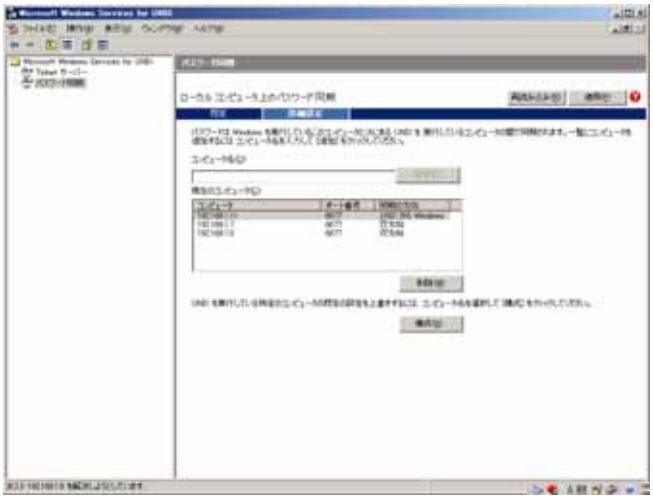

図 3. SFU 設定画面 2

4　Unix システムの設定

4.1　Unix（NIS）サーバの設定

Unix サーバーには SFU 付属の pam_sso.so.1、ssod、sso.conf ファイルを次のディレクトリにコピーをし、属性の変更を行う。

・/usr/lib/security/pam_sso.so.1　属性：755

・/usr/local/bin/ssod　属性：744

・/etc/sso.conf　属性：600

Windows との同期設定の為に SFU で設定した項目を/etc/sso.conf でも設定を行う。

・ENCRYPT_KEY=XXXXXXXXXX　（SFU で生成した暗号コード）

・PORT_NUMBER=6677

・SYNC_USERS=all

・SYNC_HOSTS=(192.168.xxx.xxx)

・USE_SHADOW=1

・FILE_PATH=/etc/shadow

・USE_NIS=1

・NIS_UPDATE_PATH=/var/yp/Makefile

・TEMP_FILE_PATH=/etc

・CASE_IGNORE_NAME=1

・IGNORE_PROPAGATION_ERRORS=1

・SYNC_RETRIES=3

・SYNC_DELAY=30

/etc/pam.conf に次の追加を行う。

Other　password required　pam_unix.so.1　の後に

Other　password required　pam_sso.so.1　を追加する。

Unix サーバの再起動時に ssod デーモンが自動起動するように設定を行う。

4.2　Unix クライアントの設定

Unix クライアントにも Unix サーバで使用している pam.conf、pam_sso.so.1、sso.conf ファイルのコピーを行う。

5　パスワード同期の流れ

パスワード変更を行った場合、同期の流れが Unix 側と Windows 側で動作が異なる。

5.1　Windows でパスワード変更を行った場合

図 4.の①で示すように Windows クライアントでパスワード変更を行った情報が Windows Server に送られ、Windows Server から UFS によって Unix サーバに変更情報が送られる。

5.2　Unix でパスワード変更を行った場合

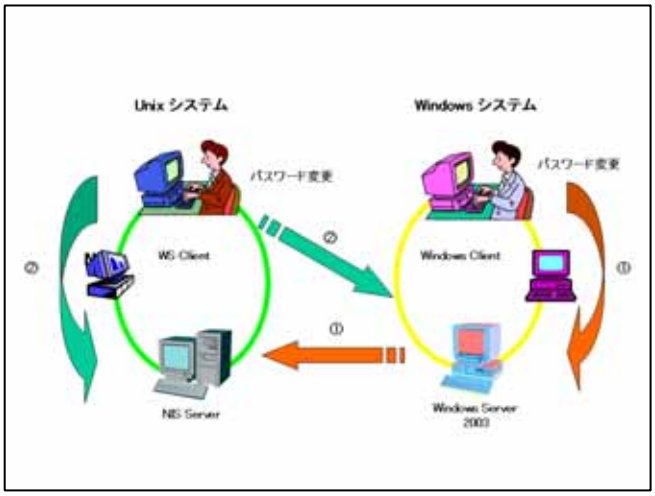

図 4..　パスワード同期の流れ

図 4.の②で示すように Unix クライアントでパスワード変更を行った場合はその情報が Unix サーバと Windows サーバ双方に送られ、Unix と Windows のパスワード同期がとられる。

6　まとめ

Unix システムは主にメールや学生実験､Windows システムはレポートの作成等で学生に利用されているが、これまでは各自で 2 種類のパスワードを管理しなくてならないため、利用率の少ないシステムのパスワードを忘れるといったことがおきていた。しかし、UFS の導入によって一つのパスワードで双方のシステムが利用できるため、パスワード忘れの減少や Windows システムでメールのパスワード変更もできるようになったため、セキュリティの面でも有意義であると思われる。

参考文献及び URL

[1]　Windows Server 2003 実践ガイド，村嶋修一著，技術評論社

[2]　Windows Server 2003 必携 Bible，宍倉幸則著，技術評論社

[3]　SFU
http://www.microsoft.com/downloads/details.aspx?displaylang=ja&FamilyID=896C9688-601B-44F1-81A4-02878FF11778