# 異機種間ネットワーク環境におけるユーザ管理

7H-1

琴屋秀平　平沢　裕

(株)　東芝　府中工場

## 1. はじめに

ネットワーク技術の発達により、計算機をLAN(ローカルエリアネットワーク)に接続し複数の計算機間で資源の共有や分散処理を行なうシステムが数多く実現されている。通常、異なった機種の計算機では独自のアクセス法やユーザ管理法を採用しているため、それらの間で資源の共有を行なった時、所有者やアクセス権の混乱などを引き起こす。

本稿では、スーパーマルチプロセッサDS6060上に実装したネットワークファイルシステム(NFS)で採用したユーザ識別子のマッピング方式について紹介する。

## 2. 概要

### 2.1 NFSの概要

NFSはSun Microsystems,inc.によって開発された分散ファイルシステムで、IEEE802.3を用いたLANに接続された計算機間でのファイルの共有を実現する。ファイルの共有は共有したい相手計算機(リモートマシン)上のファイルを自計算機(ローカルマシン)のファイルにマウントする事によって行なわれる。一旦マウントした後は、ユーザからはローカル/リモートの区別なく同じ方法でファイルにアクセスすることが可能になる。

ネットワーク上の計算機に自らの資源を提供する計算機を”サーバ”と呼び、それらが提供する資源をネットワークを通して利用する計算機を”クライアント”と呼ぶ。

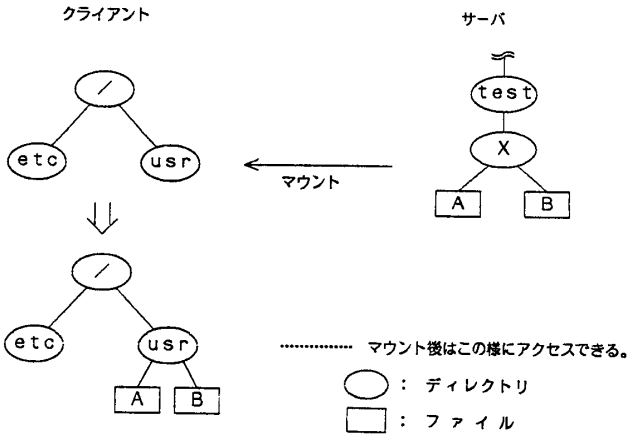


図 1　ファイルシステムのマウント

### 2.2 ユーザ管理法の相違

DS6060のオペレーティングシステムであるVMPでは、ユーザを識別するユーザid(UIC)は2バイトから構成される。ユーザのグループを特定する1バイトのグループid(GID)と、グループ内のメンバを特定する1バイトのメンバid(MID)である。

一方、NFSはUNIX上で開発されており、ユーザを識別するための識別子として、2バイトのユーザid(uid)と、2バイトのグループid(gid)の合計4バイトのデータを使用している。

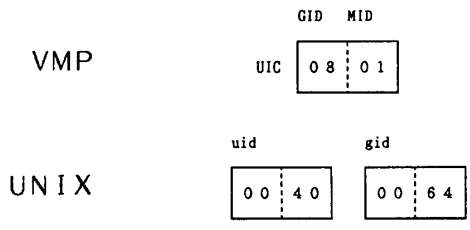


図 2　ユーザidの相違

注)　UNIXはAT&Tが開発し、ライセンスしているオペレーティングシステムです。

NFSはSun microsystems, Inc.の登録商標です。

User management in heterogeneous computing environment

Shuhei KOTOYA, Yutaka HIRASAWA
TOSHIBA CORPORATION

## 3. ユーザｉｄのマッピング

前項で示したようなオペレーティングシステムの相違に基づく差を吸収するために、今回の実装ではマッピングテーブルによるユーザｉｄのマッピング機構を採用した。このマッピング機構は、マッピングテーブルを用いて、VMP上のユーザとＵＮＩＸ上のユーザをそれぞれの名前で１対１に対応付けるという機能を持つ。具体的には、リモート／ローカル間のアクセスにおいて、リモートからの要求ブロック中に記録されているリモートユーザのｉｄ（ｕｉｄ）は対応するローカルユーザのｉｄ（ＵＩＤ）に変換され、ローカルからリモートへの要求ブロック中に記録されているＵＩＤは対応するｕｉｄにそれぞれ変換される。

マッピングテーブルは次に示す３つのファイルから生成される。

- ユーザ名マッピングファイル
  （ｎｆｓ．ｕｓｅｒ）
- VMPでのユーザ定義ファイル
  （／ｓｙｓｍｇｒ／ｕｄｆ）
- ＵＮＩＸでのユーザ定義ファイル
  （／ｅｔｃ／ｐａｓｓｗｄ）

ユーザ名マッピングファイルは以下に示すようなフォーマットを持つテキストファイルである。

```
VMP_username  UNIX_username [ｺﾒﾝﾄ]
```

これらのフィールドは１個以上の空白またはタブで区切られ、第１フィールドはVMP上でのユーザ名を示し、第２フィールドではＵＮＩＸ上でのユーザ名を示している。第３フィールド以降と"#"以降はコメントとみなされる。

これらのファイルからコマンド（mknfsuser）によってユーザｉｄのマッピングテーブル（nfs.umap）を作成し、システムのカーネル部分に組み込む。このテーブルの組み込みはＮＦＳシステムを停止せずに行なうことが可能である。

ＵＮＩＸシステムにおけるスーパーユーザ（root,uid=0）もしくは、テーブル上に存在しないユーザがアクセスしてきた場合は、それらの要求のユーザｉｄはすべて特定のユーザｉｄ（nobody,UIC=0xFFFE）にマッピングされる。

## 4. 効果

ユーザｉｄマッピング機構の採用により、次に示す効果を得ることができた。

（１） トランスペアレントなユーザ管理を実現した。
ローカルとリモートのユーザｉｄはマッピングによって独立に設定でき、それぞれのシステムで提供するユーザ管理に関するサービスを制約なく受けることができる。

（２） セキュリティが向上した。
マッピングテーブル中に存在しないユーザは強制的にデフォルトのユーザｉｄを与えられるため、外部からの侵入に対して強くなった。

（３） ユーザ管理が容易になった。
マッピングテーブルの内容を変更するだけでＮＦＳのサービスを受けることのできるユーザを変更できるため、ユーザｉｄが変更された場合などの処理が容易になる。

（４） よりユーザフレンドリィになった。
ユーザにとってはそれぞれの計算機でユーザ名の対応さえ取っておけば、異機種環境において複数の名前を持つ必要がなくなり、一つの名前で透過的なアクセスを行なうことができるようになった。

## 5. おわりに

今後増加して行く異機種間結合において問題となるユーザ管理について、一つの有効な方式を示した。

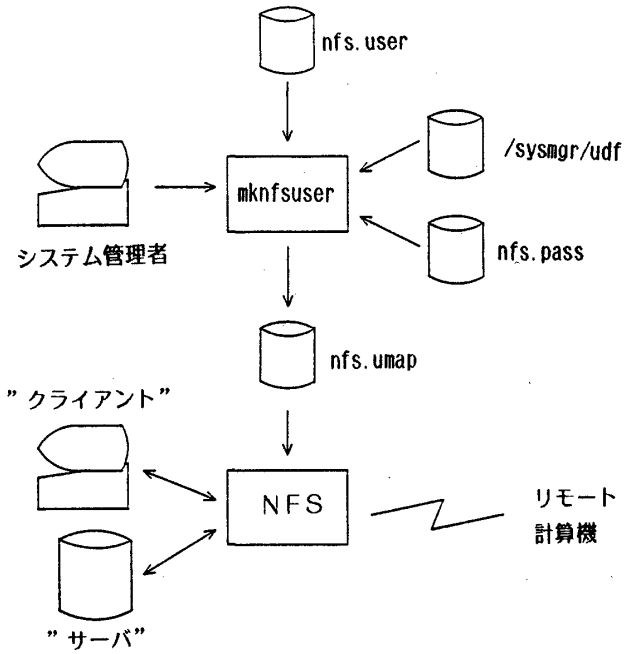


図 3 マッピング機構