# 分散処理環境におけるネットワークアクセス制限の実現法

7D−7

大西 淑雅　中山　仁
九州工業大学 情報科学センター

## 1　はじめに

現在，大学や企業で広く普及している分散処理環境において，ネットワークの利用がますます重要視されている．特に，ネットワークの拡張により，電子メイルや電子ニュースによる情報交換も活発に行なわれている．しかし，分散処理環境の規模が大きくなるにつれて，ネットワークの利用をどのように管理するかが問題となってきている．

九州工業大学では，教育用ワークステーション[1]からの広域ネットワークのアクセスを禁止している．これは，ネットワークの利用マナーを教育する前に，広域ネットワークを利用させるべきではないという判断からである．しかし，専門教育用ワークステーションにおいては，広域ネットワークの利用を認めている．

現状では，ネットワークのアクセス範囲は，利用者毎に制限できるわけではなく，利用するワークステーションごとに決めざるをえない．このことは，広域ネットワークの利用権利を持った利用者であっても，利用するワークステーションによっては，ネットワークを利用できないという不便さを招いている．

本論文では，従来，ハードウェアごとに管理されていたネットワークのアクセス範囲を利用者毎に設定できる方法について述べる．この方法により，管理者はネットワークの形態による管理からより自由度の高いネットワークアクセスの管理を行なうことができる．

## 2　ネットワークのアクセス制限

ネットワークのアクセスを管理するには，ネットワークのセグメント単位で管理する方法とパケット送信段階において管理する方法の2つが考えられる．

An Approach to Realize Network Access Restriction in a Distributed Enviroment ; Yoshimasa Ohnishi, Hitoshi Nakayama (Kyushu Institute of Technology)

### 2.1　ゲートウェイでのアクセス管理

図1にネットワークのモデルを示す．セグメントAのネットワークとセグメントBのネットワークがゲートウェイで接続されているとする．セグメントBのネットワークの利用権利を持ったuser1がセグメントBに向かってパケットを送信した場合，ゲートウェイは問題なくパケットをセグメントBに送信する．しかし，権利を持たない user2 がパケットを送信した場合は，ゲートウェイでこのパケットを抹消してしまう方法である．

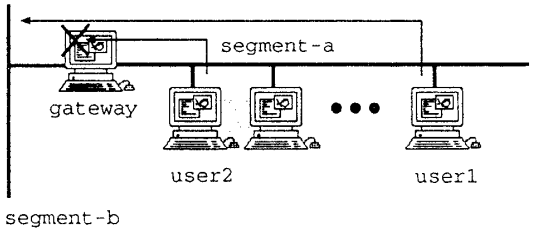


図 1: ゲートウェイで管理する場合

この方法では，ゲートウェイに利用者のアクセス管理ファイルを用意することで実現できる．しかし，ゲートウェイが受信するパケットには利用者を特定する情報が含まれていない．この問題を解決するには，パケットに利用者の認識を可能にするUIDもしくは新たなアクセス情報を加える必要があるが，一般性を考慮すると望ましい方法ではない．また，専用のゲートウェイ機器を利用している場合に対応できないという問題もある．

### 2.2　発信元でのアクセス管理

各ワークステーション(発信元)がネットワークに対しパケットを送信する前にネットワークの利用権利を判断する方法も考えられる．図2に示すように，セグメントBの利用権利を持たない user2 がパケットをセグメントBに送信する段階において，パケットを破棄してしまい，セグメントAにもそのパケットを送信しない方法である．

この方法においては，利用者のアクセス管理ファイルを各ワークステーションで保持する必要がある．しかし，ゲートウェイ方式で必要とされるパケットに新たな情報を加える必要がない．また，アクセス管理ファイルについては，Network Information Service(NIS) を活用することで一貫性を保つことができる．

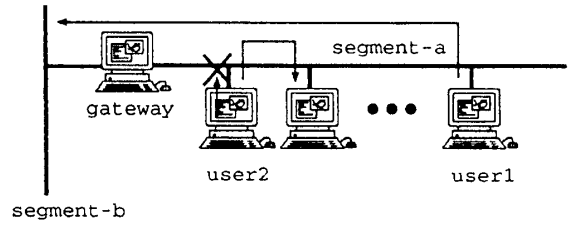


図 2: 発信元で管理する場合

## 3 発信元方式の実現

以上の結果から，発信元で管理する方式による基本設計を試みた．以下，ワークステーションとしてSparc Station (Sun Microsystems) をモデルに，オペレーティングシステムを BSD 系としている．

### 3.1 アクセス情報の管理

実現には利用者とアクセス範囲との対応を付けるアクセス情報が必要である．このアクセス情報は /etc/passwd ファイルに追加する形がもっとも望ましいが，アクセス制限を行なわない分散処理環境も考慮にいれて，別ファイルを作成することにした．ファイルは2つ用意する．1つ目はネットワークのアクセス可能範囲を定義したファイル (/etc/netaccgroup) で，次に示すような記述を行なう．

```
12:131.206.3,131.206.4
15:131.206.51
```

ネットワークアクセスグループ番号 (Network Access Group ID，以下 NAGID とする) とアクセス可能なネットワークアドレスを : で区切って指定する．この場合，NAGID が 12 の利用者は 131.206.3.xxx のネットワークと 131.206.4.xxx のネットワークにアクセス可能であることを示している．

2つ目のファイル (/etc/netaccess) は，利用者の UID と NAGID の対応を定義するファイルである．初めのフィールドが UID であり，次のフィールドが NAGID である．ここで，NAGID が 0 の場合は，その利用者がすべてのネットワークをアクセスできることを示している．

```
1003:12
1004:0
1005:15
```

### 3.2 制御方法

パケットの送信は図 3に示すように，socket 層のプロトコル切替えテーブルを通して tcp_usrreq() もしくは udp _usrreq() が呼び出される．パケットを送信すべきかどうかの判定をこの部分に埋め込む．これは，usrreq(tcp_usrreq() と udp_usrreq()) 関数において各種情報の接続が行なわれるため，アクセス管理に必要な UID や送信先アドレスを簡単に得ることができるからである．

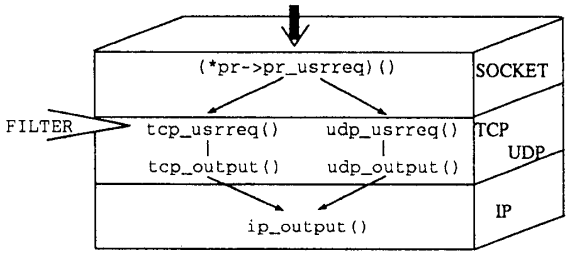


図 3: パケット制限

## 4 おわりに

本論文では，分散処理環境におけるネットワークのアクセス制限を行なう方法について述べた．この方法を用いることにより，ネットワークのアクセス管理を利用者毎に設定することができるようになる．このことは，さまざまな利用者 (学部学生，教職員，事務職員，大学院生) が存在する分散処理環境において，ネットワークの利用範囲をきめ細かく設定できる点において優れている．

一方，管理情報が新たに増えることのオーバヘッドも無視できるものではないと思われる．現在，このシステムを開発中であるので，早急にシステムを完成し，効率上の諸問題も今後研究していく予定である．

## 参考文献

[1] 中山他: 大学における大規模分散システムの構築 , 九州大学 計算機科学研究報告 第 9 号