L-076

P2P アプリケーショントラヒックの検出・ユーザ管理支援システムの試作

A Prototype System for P2P Application Traffic Detection and User Management Support

笹本 知将† 伊藤 洋† 大坐畠 智† 川島 幸之助†
Toshimasa Sasamoto Hiroshi Ito Satoshi Ohzahata Konosuke Kawashima

1. はじめに

近年，ADSL や FTTH の普及に伴い，P2P アプリケーションによるトラヒックが急増し，負荷が多大なものとなっている．また，これらの P2P アプリケーションにより，社内から個人情報が流出する事件も後を絶たず，ネットワーク管理者としては P2P ユーザを把握することは不可欠である．これまでポート番号[1]やシグニチャマッチング[2]によるトラヒック検出が行われてきたが，管理者が暗号化された P2P トラヒックを検出，管理することは難しかった．本稿では，Linux に標準で搭載されている tcpdump のパケットスニファ機能と iptables のパケットフィルタリング機能を併用して Firewall を構築することで，WinMX[3]，Winny[4]，および Share[5]のトラヒック検出し，P2P アプリケーションのユーザを GUI で管理する支援システムを実装した．その結果，管理者が P2P アプリケーションユーザに対し，容易にネットワークの使用を制限することが可能であることを確認した．

2. 提案方式

2.1 P2P トラヒック特定方式

P2P アプリケーションには大きく分けて，ハイブリッド P2P，ピュア P2P の 2 つの種類が存在する．WinMX はハイブリッド P2P であるため，既存の方式でトラヒック制御が可能である[6]．Winny と Share はピュア P2P であり，一般に検出が困難であるが，本稿では P2P アプリケーショントラヒックを識別する方式として，図 1，2 のパケットシーケンスを用いた．パケットサイズと TCP の PUSH フラグに着目して識別を行った．今回の実験の結果，図 1，2 に示すパケットシーケンスが，Winny，Share 特有のトラヒックパターン（バージョンに依存する可能性がある）であるということを確認した．

2.2 P2P ユーザ管理支援システムの概要

提案システムの概要を図 3 に示す．tcpdump を用い，パケットすべてをキャプチャし，ログを出力させる．Perl で記述したスクリプトで前述のトラヒックパターンが検出された場合，Web ベースの CGI で情報を表示させる．P2P アプリケーションユーザに対してインターネット使用拒否を行いたい場合は，GUI による操作で iptables のルールに P2P アプリケーションユーザの IP アドレスを追加することにより，トラヒック制御を行う管理システムを構築する．Web ベースのユーザ管理システムでは，P2P ユーザの IP，各アプリケーションの利用回数，最終使用時刻を表示し，その情報に応じてチェックボックスを用いたネットワーク接続制限を行えるようにした．接続不可能に設定したホストについては，DHCP による IP アドレス

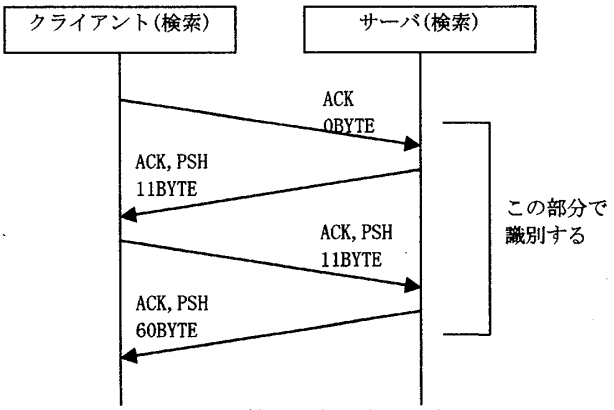


図 1 Winny トラヒック検出パケットシーケンス．

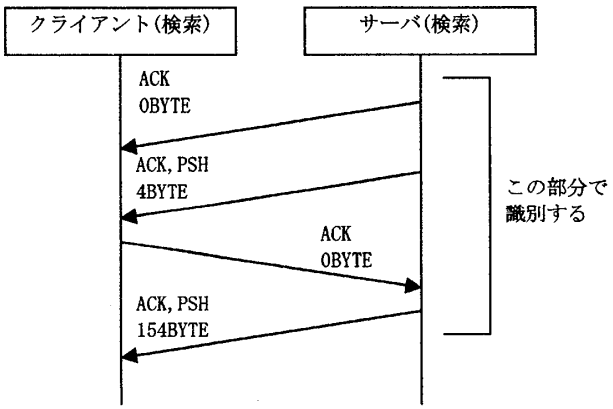


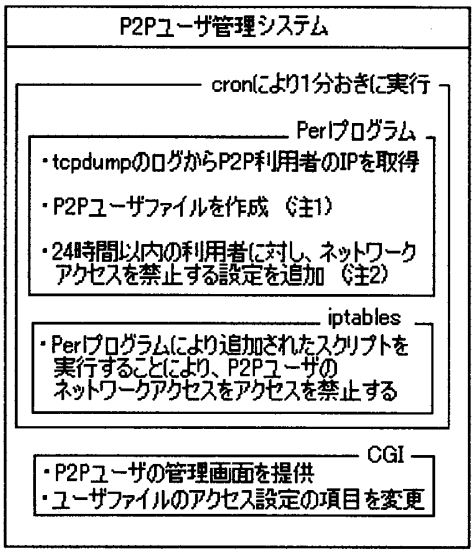
図 2 Share トラヒック検出パケットシーケンス．

再割り当てを考慮し，24 時間で制限を自動的に解除するようにした．P2P ユーザ管理支援システムの動作流れを図 3 に示す．

1. tcpdump のログより，WinMX，Winny，Share を利用したホストの IP を取得．
2. アクセス許可/禁止，IP，WinMX 利用回数，Winny 利用回数，Share 利用回数，最終の P2P 利用時刻の 6 項目でユーザファイルを作成．
3. アクセス禁止されたユーザに対し，(現在の時刻 − 最終の P2P 利用時刻 < 24(h))を満たすものについて，該当 IP によるネットワーク利用を禁止する設定を加える．
4. root 権限下のユーザファイルを GUI でアクセスするユーザファイルにコピーする．
5. iptables スクリプトファイルを実行する．

1−5 を 1 分間隔で繰り返すことで，P2P ユーザの割り出しを行う．

†東京農工大学
Tokyo University of Agriculture and Technology.



注1:（アクセス許可/禁止, IP, WinMX利用回数, Winny利用回数, Share利用回数, 最終のP2P利用時刻）の項目で作成
注2: 設定例, iptables -A FORWARD -s $IP_data -j DROP

図 3　P2P ユーザ管理支援システム構成図.

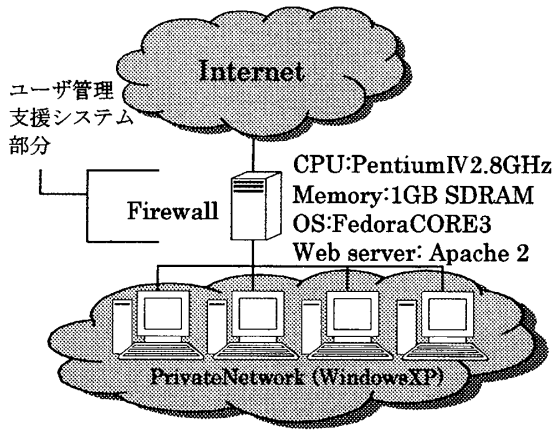


図 4　構築したネットワーク環境.

3 実験

3.1 実験の概要

図 4 のネットワーク環境において，Windows マシンで WinMX，Winny，Share をそれぞれ起動し，インターネット上の他のピアと通信を行わせた．P2P ユーザ管理支援システムを動作させ，Windows マシンにおいて，トラヒックが正しく制御できているかの確認を行った．

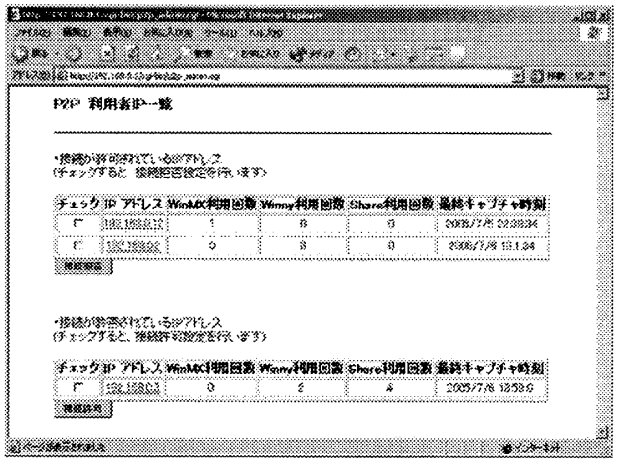


図 5　P2P ユーザ管理画面.

3.2 実験結果

各 P2P アプリケーションを起動し，管理画面（図 5）を Web ブラウザから呼び出した結果，P2P アプリケーションのユーザ情報が表示された．さらに，P2P ユーザ管理画面からユーザのネットワーク接続不可能設定を行い，Windows マシンでネットワーク接続の確認を行った．結果，接続不可能にしたホストは，Firewall でパケットをドロップしているため P2P アプリケーションの接続を含め，一切のネットワーク接続が不可能であることを確認した．その後，接続不可能にしたホストに対して接続許可処理を行った場合，正常にネットワーク接続が行えるようになることを確認した．

4 おわりに

本稿では，P2P アプリケーショントラヒック検出・ユーザ管理支援システムを提案し，実装した．今後は，IP アドレス以外の情報などを表示し，より一層ユーザを検出しやすくするなどの管理面での改善を行う予定である．

参考文献

[1] M. St. Johns and G. Huston, "Considerations on the use of a Service Identifier in Packet Headers," RFC 3639, 2003.
[2] S. Sen, O. Spatscheck and D. Wang, "Accurate, Scalable In-Network Identification of P2P Traffic Using Application Signatures," Proc. of ACM WWW'04, 2004.
[3] WinMX, http:/www.winmx.com/.
[4] Winny, http://www.nynode.info/.
[5] Share, http://www.stereoz.net/next/.
[6] 伊藤洋，貫名東，大坐畠智，川島幸之助，ハイブリッド型 P2P アプリケーショントラヒック制御方式の一考察，情報処理学会 第 67 回全国大会，6W-7，2005.