

P2Pファイル共有の実態と課題

～トラフィック測定・設計・制御・管理法の確立に向けて～

2003/11/06

NTTサービスインテグレーション基盤研究所

亀井聡 / 森達哉

NTT情報流通プラットフォーム研究所

大井恵太

➤ 研究の背景

- ネットワーク利用の変遷とP2Pトラヒックの増加

➤ 研究の目的

➤ P2Pファイル共有アプリケーション

➤ ネットワークレイヤ測定 / アプリケーションレイヤ測定 / マルチレイヤ測定

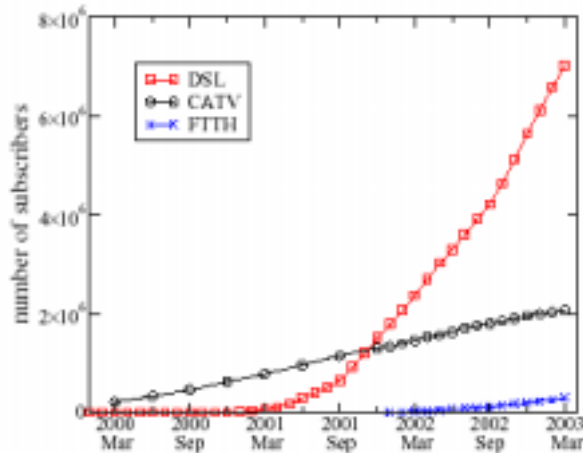
- 測定手法
- 測定結果の分析～フロー分析, 規模, 流通ファイル, ポート番号 etc...

➤ 考察

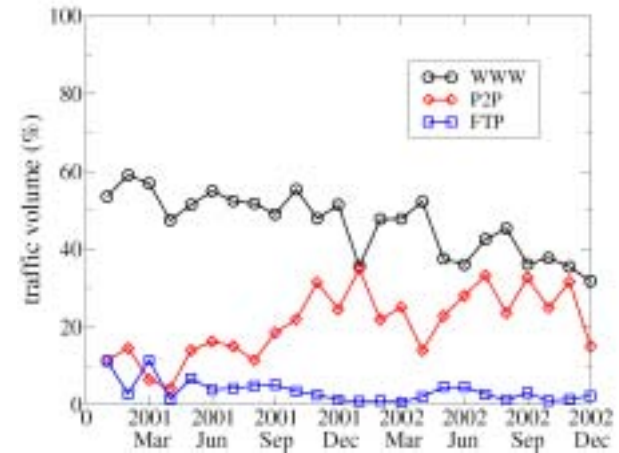
- P2Pトラヒックの現状
- 対策と課題

➤ まとめ

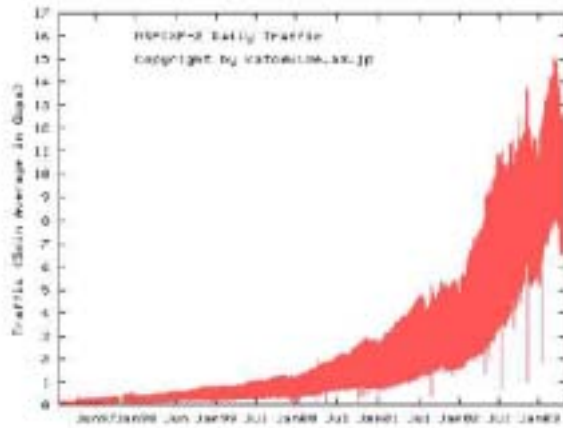
背景 ~ ネットワーク利用の変遷とP2Pトラフィック



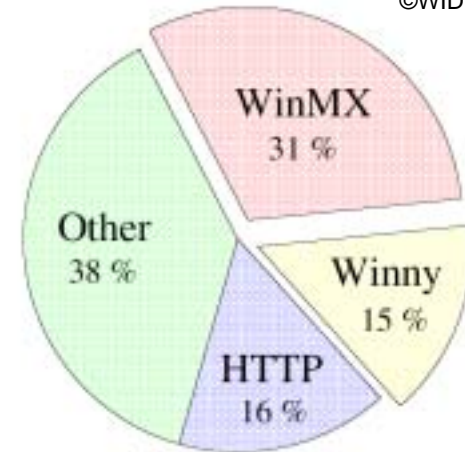
ブロードバンド環境の急激な普及
©総務省



バックボーントラフィックのアプリケーション比率
(ポート番号識別)
©WIDE mawi Project



バックボーン (IX) トラフィックの増加
©NSPIX2



ISP内トラフィックのアプリケーション比率
(ポート番号識別)

- P2Pファイル共有アプリケーションのトラフィック増が著しい.
- 既存の測定法で確認できるトラフィックは極一部. 全貌把握が困難.



- アプリケーション / ネットワーク両レイヤからの測定.
- ターゲットアプリケーションは WinMX/Winny/Gnutella



P2Pネットワークの**現状把握**に有効なマルチレイヤ測定を提案
P2Pトラフィックに関する**課題と対策**を考察

P2Pファイル共有アプリケーション

➤ P2Pファイル共有アプリケーション

Napster/Gnutellaをその起源とするアプリケーション群

- 参加ユーザのディスク上にあるファイルを**検索**する機構
- 検索によって各ユーザが発見したファイルを自ノードへ**転送**する機構をその特徴とする。

➤ トラフィックパターンが大きく変化

- スケーラビリティの向上, ボトルネック回避等による限界解除
- 距離(ホップ数など)を考慮せずに接続先を選択
- アプリケーションレイヤでのマルチホップ
- トラフィックソースのエッジ側への移行
- 上りトラフィックの増加

➤ C/S型のWebと比較して全貌把握が非常に困難

既存のP2Pトラフィック識別手法

➤ トラフィック識別手法

a. ポート番号による識別

- TCPのポート番号を利用してアプリケーションを識別

b. セッション追跡

- 中央サーバへの検索パケットをトリガーとして、以降の通信を追跡

c. ペイロード監視通信, パターン認識

- ペイロード中の文字列やパケット長等の特徴を利用

d. アプリケーションレイヤ解析

- アプリケーションレイヤでプロトコルを解析

市販装置:

c. P-Cube/Ellacoya

d. SandVine/CacheLogic

The diagram illustrates traffic flow with red highlights and labels a, b, c, and d. The traffic flow is as follows:

```
src-addr.sport > dst-addr.dport flag seq/size payload
src-addr.sport > dst-addr.dport flag seq/size payload
src-addr.sport > dst-addr.dport flag seq/size payload
src-addr.sport > dst-addr.dport flag seq/size payload
src-addr.sport > dst-addr.dport flag seq/size payload
src-addr.sport > dst-addr.dport flag seq/size payload
src-addr.sport > dst-addr.dport flag seq/size payload
src-addr.sport > dst-addr.dport flag seq/size payload
src-addr.sport > dst-addr.dport flag seq/size payload
src-addr.sport > dst-addr.dport flag seq/size payload
```

Labels and highlights:

- a.** points to the `dport` field in the first line.
- b.** points to the `flag` field in the fourth line.
- c.** points to the `payload` field in the first line.
- d.** points to the `payload` field in the last line.

既存のP2Pトラフィック測定手法 ~ 問題点

a. ポート番号による識別

- ポート番号可変, well-known-portを使うアプリケーションの存在.

b. セッション追跡

- 中央サーバが存在しないアプリケーションへの適用困難.
- プロトコルの解析が必要.

c. ペイロード監視, 通信パターン認識

- 誤認識の危険性
- プロトコルの解析, もしくはパターン分析がアプリケーション毎に必要.
- 大量のパケット監視, 通信内容(一部)の取得が必要, スケールしない.

d. アプリケーションレイヤ解析

- パケット監視, 組立が必要でスケーラビリティが低い.
- プロトコルが既知である必要がある.

主にネットワークレイヤでの分離を目的としている.

スケーラビリティ, アプリケーション依存の問題が大きい. また, 最近のP2Pアプリケーションは通信の暗号化や, ポート番号のランダム設定等, 隠蔽機能の高度化が進む.

今回実施した測定

➤ ネットワークレイヤ測定

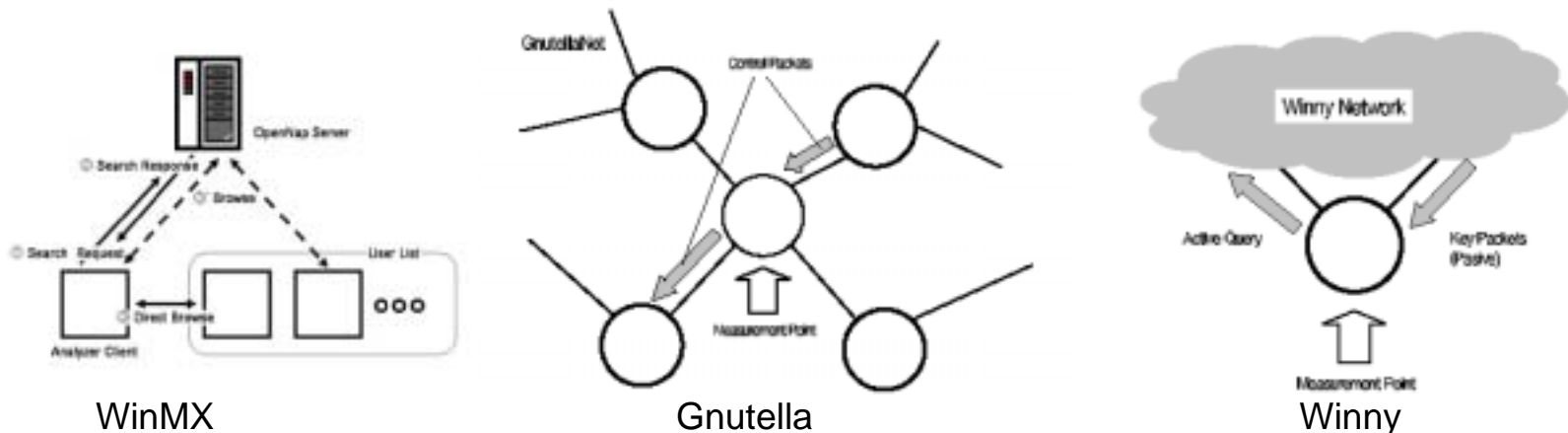
- P2P通信が含まれるバックボーン回線でのパケットキャプチャー

➤ アプリケーションレイヤ測定

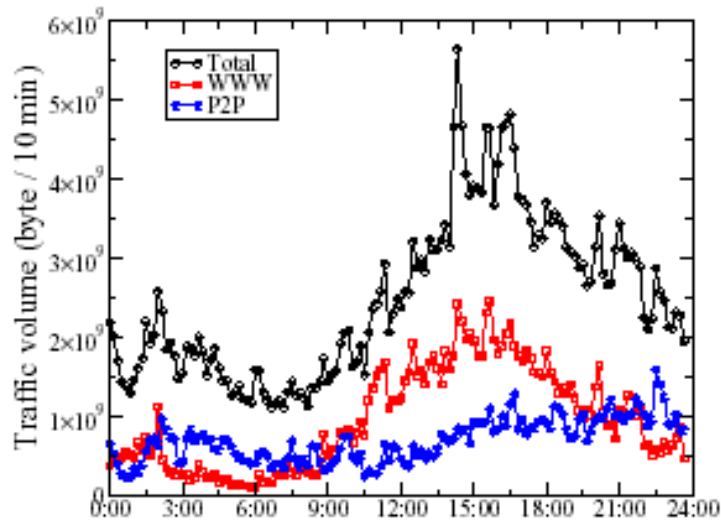
- アプリケーション毎にヒューリスティックな手法が必要
ファイル名, ファイルサイズ, 共有数等の情報を収集

➤ マルチレイヤ測定

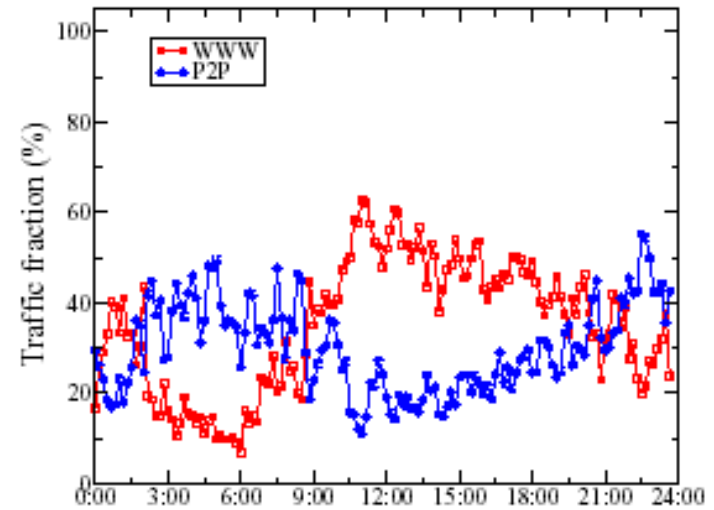
- アプリケーション動作ノードの隣接ノードでネットワークレイヤでの測定を実施
IPアドレス, 利用ポートを収集
- アプリケーションへの依存度が低い
- クライアント権限での測定が可能



ネットワークレイヤ測定 ～ トラフィックの日変動



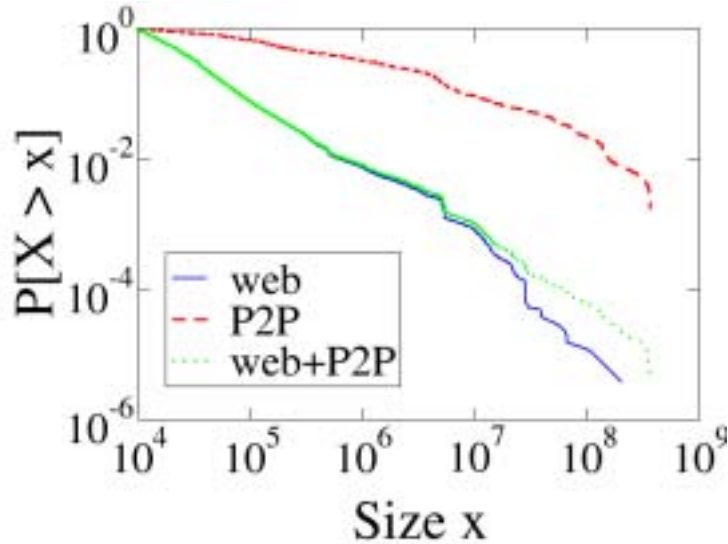
トラフィック流量



トラフィック占有率

- インターネットへのuplinkの10分単位の日変動(ポート番号識別)
- オフィスアワーのピークを示すウェブトラフィック
- P2PとWebでは正反対の傾向

ネットワークレイヤ測定 ~ フロー分析



フローサイズ統計

	フロー数 (#/3時間)	トラフィック総量 (Gbyte/3時間)
全体	1223735 (100%)	37.72 (100%)
Web	810418 (66.2%)	17.52 (46.4%)
P2P	12405 (1.0%)	10.25 (27.2%)

	上位1%フロー 数 (#/3時間)	トラフィック総量 (Gbyte/3時間)
Web	8104	9.53 (25.40%)
P2P	124	9.32 (24.71%)

フロー数とトラフィック総量

- フロー分布はパレート分布 $P[X > x] = k$ で近似可能
- **P2P**は**Web**と比較してフロー数は少ないが、フローあたりでは多くのトラフィックを占有。
- **P2P**の上位1% (全体の0.01%) のフローが全体の1/4のトラフィックを占める。

アプリケーションレイヤ測定 ~ ファイルサイズ

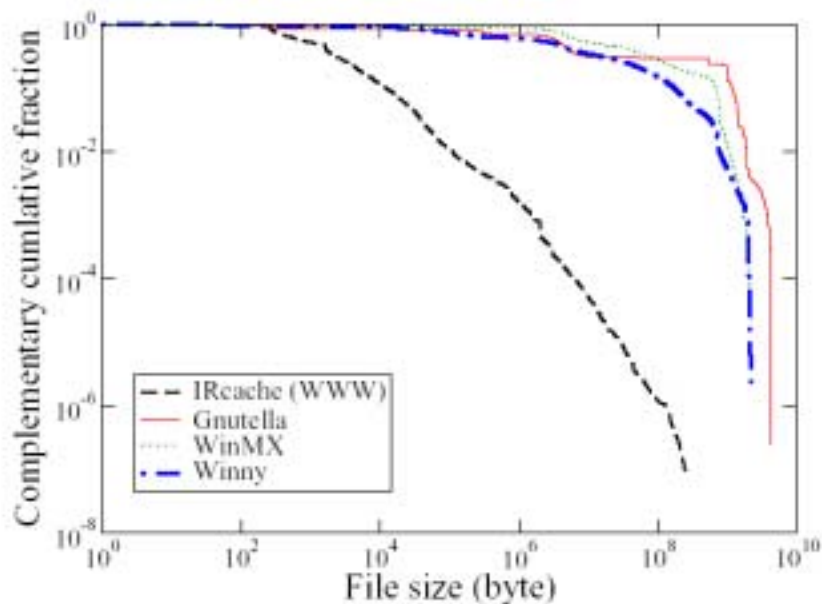
➤ ファイルサイズ分布

- WinMXは中央サーバ経由で取得したクライアントのファイル
- GnutellaはQueryHit上のファイル
- Winnyは繰り返し検索を実施して取得したファイル

条件がそろっていないので単純には比較できないが、傾向として

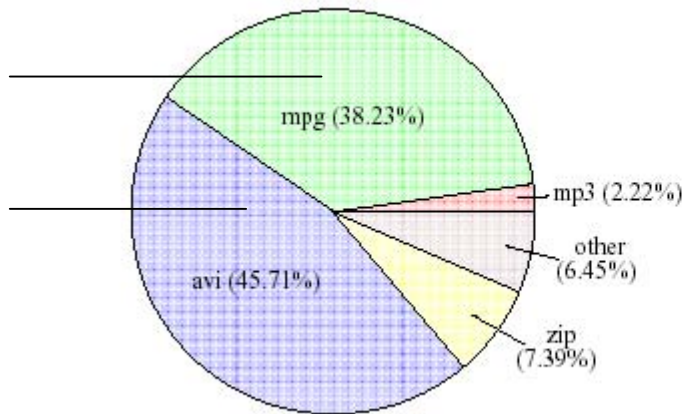
➤ ウェブと比較してかなり大きいサイズのファイル分布

➤ 10^9 付近(1Gbyte)での急激な落ち込み ファイルシステムの限界？

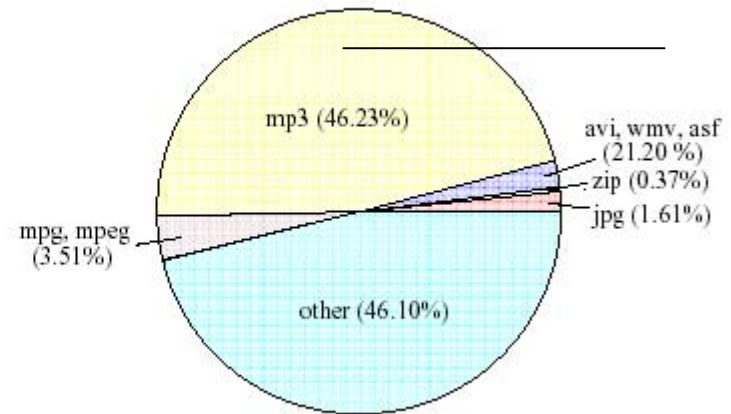


アプリケーションレイヤ測定 ~ 拡張子分布

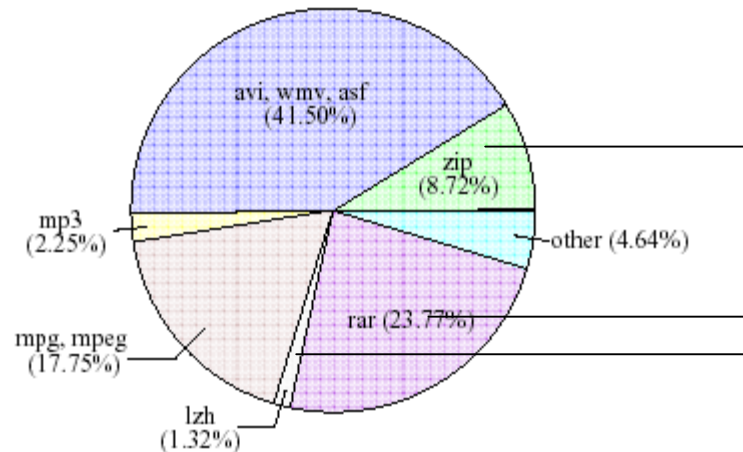
➤ アプリケーション毎に異なる特性



WinMX:動画中心



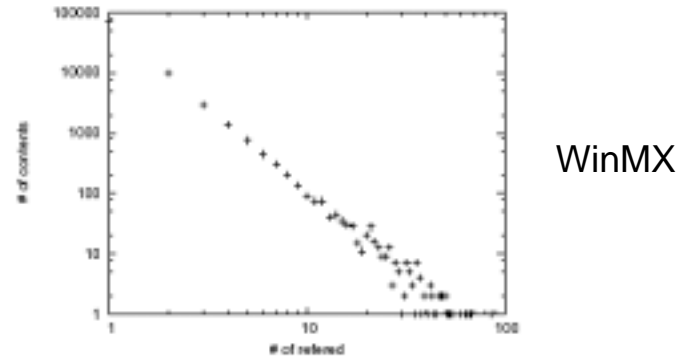
Gnutella:音楽中心



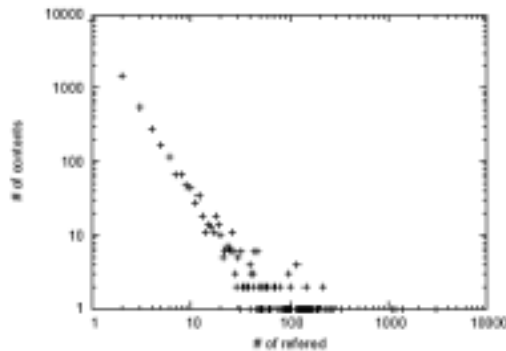
Winny:圧縮ファイルが相対的に多い

アプリケーションレイヤ測定 ~ コンテンツ分布

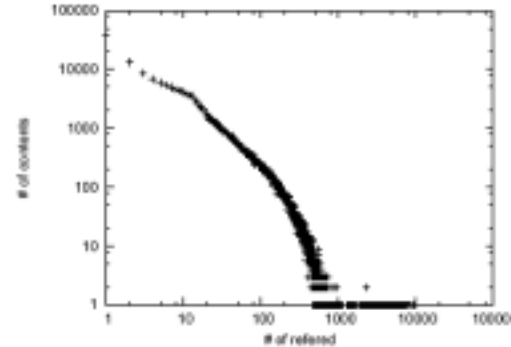
➤ x/y : コンテンツ被共有数 n / n 人に共有されたコンテンツ数



Gnutella



Winny



➤ Lotokaの法則 (Zipfの第二法則) による直線性

- コンテンツが足りない場合に左上で曲線化 (マイナーコンテンツが不足) することが知られている
- ファイル数が万のオーダーにもかかわらず、直線性を保っているのは驚異的

マルチレイヤ測定 ~ ネットワーク規模

➤ ネットワーク規模(ユニークアドレスetc)

収集データ

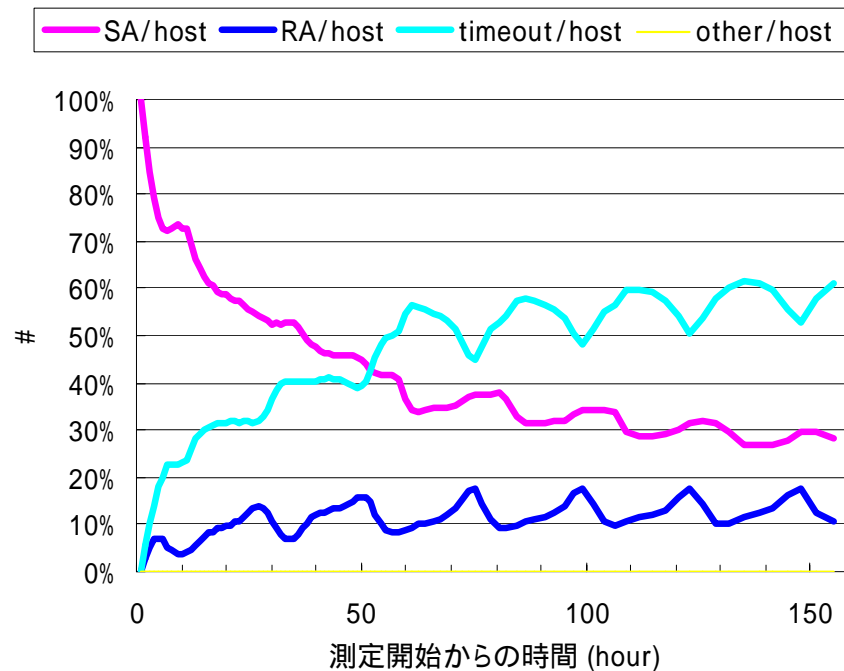
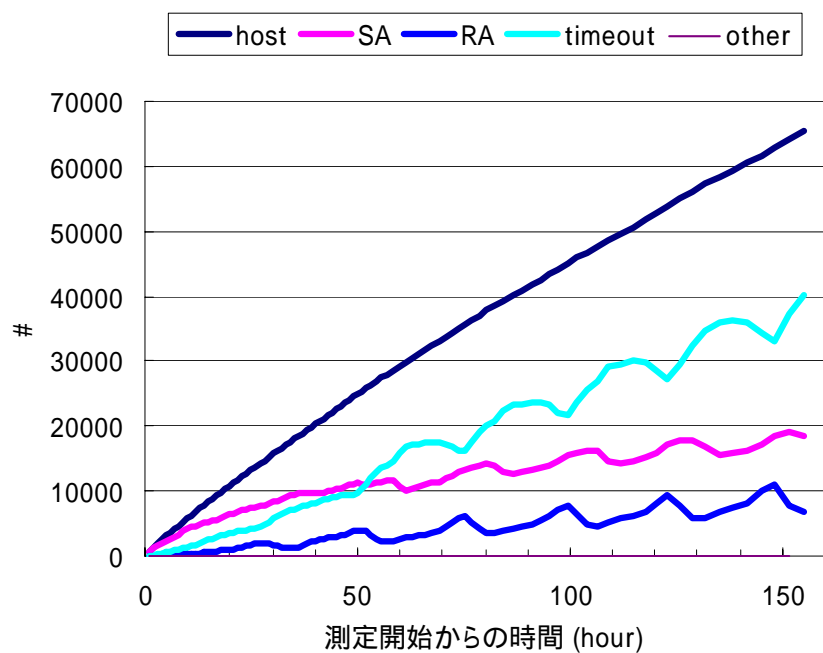
種別	固有 IP 数	固有ファイル数	合計ファイル容量	平均ファイル容量
WinMX	350	165,933	25TB	150MB
Gnutella	30,052 135,291 (P2P)	3,883,752	1.3PB	330MB
Winny	39,123	235,423	27TB 6.4PB (share)	63MB

- WinMXはサンプル測定 , Gnutella/Winnyは68時間連続測定
- ほぼ10万とされるGnutellaをP2Pレイヤでは捉えられている
- IPレイヤでは3万程度
- Winnyについても同様の傾向があるとするれば , 10万程度?
 - Winnyはリンクを頻繁に張り直す特性があるので単純には比較できない
 - アプリケーションの特性 , ネットワークのサイズ等の要素も考慮する必要

マルチレイヤ測定 ~ アクティブノード

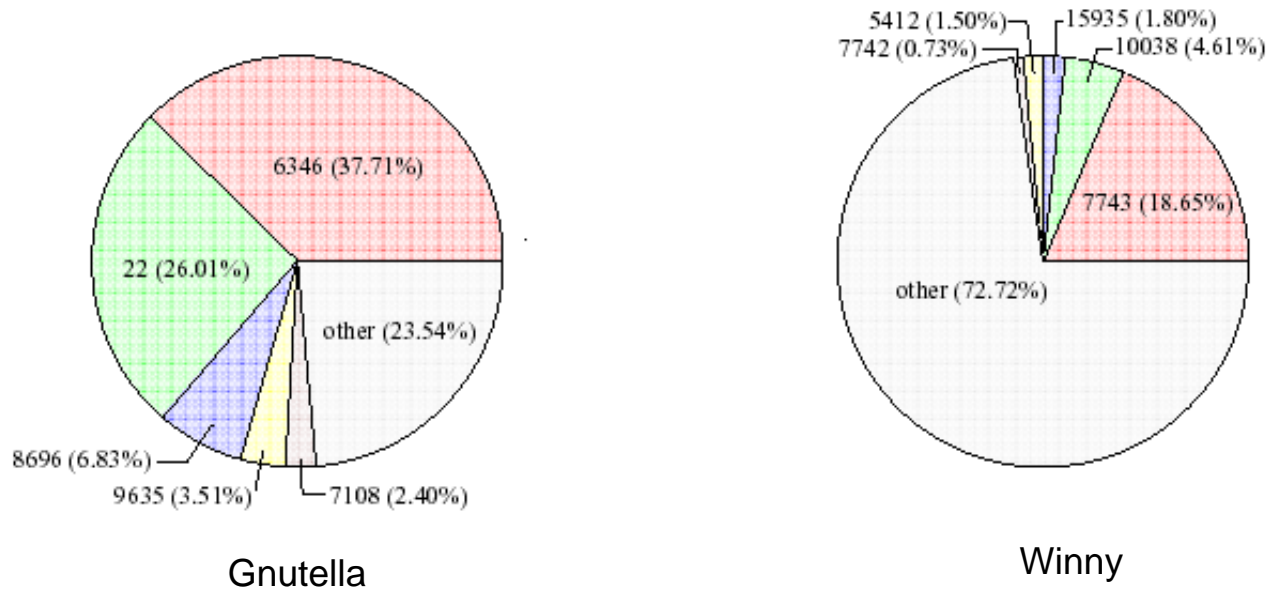
Winny2についてhpingにより生存確認
Null 接続によって確かにWinnyであると確認することもできる

(*)NetAgent, P2P検知技術



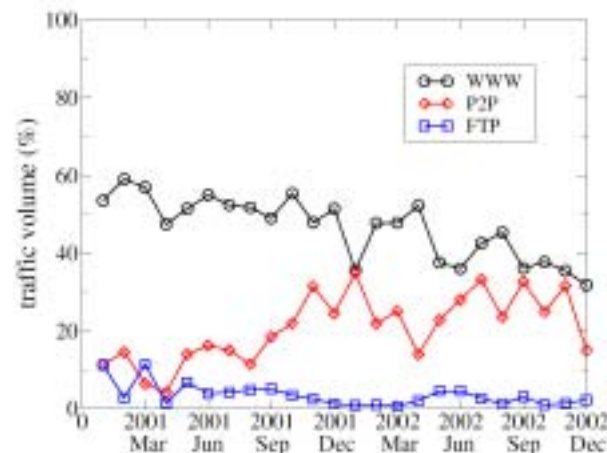
マルチレイヤ測定 ~ ポート番号分布

➤ デフォルトポートの使用率(パケット数)



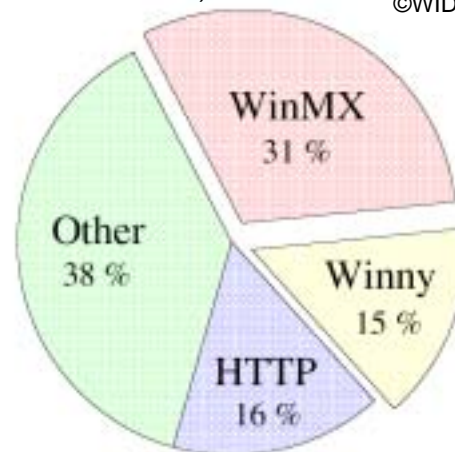
- **デフォルトポート**利用はGnutellaで38% , Winnyで19%
- ポート番号による統計値の2 ~ 5倍の潜在P2Pトラフィックの存在

背景 ~ ネットワーク利用の変遷とP2Pトラフィック



バックボーントラフィックのアプリケーション比率
(ポート番号識別)

©WIDE mawi Project



ISP内トラフィックのアプリケーション比率
(ポート番号識別)

考察 ~ P2Pトラフィックの現状

➤ ネットワークレイヤとアプリケーションレイヤより俯瞰

– トラフィック量

- バックボーンで20% , Webの40%に迫る
- ISPではWebの3倍にも

通信ポートによる識別なのでさらにこの2 ~ 5倍の可能性

- 少数ユーザの占有率が高い(0.1%が1/4等)

– 流通ファイル

- 平均でWebの5000 ~ 13000倍
- コンテンツの供給も充分 まだまだ規模は拡大



Webを上回る規模 , 主要アプリケーションに比肩



ネットワーク設計 , 制御 , ビジネスモデルへのインパクト大

➤ トラヒック増加への対策

- 回線増強/トラヒック制御, 制限/網設計, 運用での回避

➤ 課題

- P2Pトラヒック識別法

- 現行方式ではスケールせず, クローズドアプリへの対応困難
- スケーラブルで高精度かつ柔軟な手法c

- P2Pトラヒックの制御

- 単純に帯域を絞ると影響大
- P2Pの中のヘビーユーザを絞ったり, 要求品質差に着目した制御
- **影響範囲**を見極め, **要求品質**を考慮した共存可能な方式

- P2Pトラヒックを考慮した網設計法 / 管理法

- トラヒックマトリクスの変化に対しては, 少数箇所の厳密な管理から多数箇所のゆるやかな管理への移行
- ネットワークモデルの見直し
 - 幅広いNW/Applicationのレイヤーをまたがった測定, 分析により
 - P2Pの特性を考慮したトラヒック / ネットワークモデルの考案
 - シミュレーション等の手法により効率的ネットワーク設計, 管理法確立

- 普及がめざましいP2Pアプリケーションの実態解明のため、WinMX/Gnutella/Winnyについてネットワークレイヤとアプリケーションレイヤ双方にまたがる測定と分析を実施

その結果、

- 現在P2Pアプリケーションはトラフィック量でWebの数倍
- ユーザ規模でも国内だけで数万人以上の規模のアプリケーションが存在
- 少数ユーザによる帯域占有

といった実態を定量的に示した。

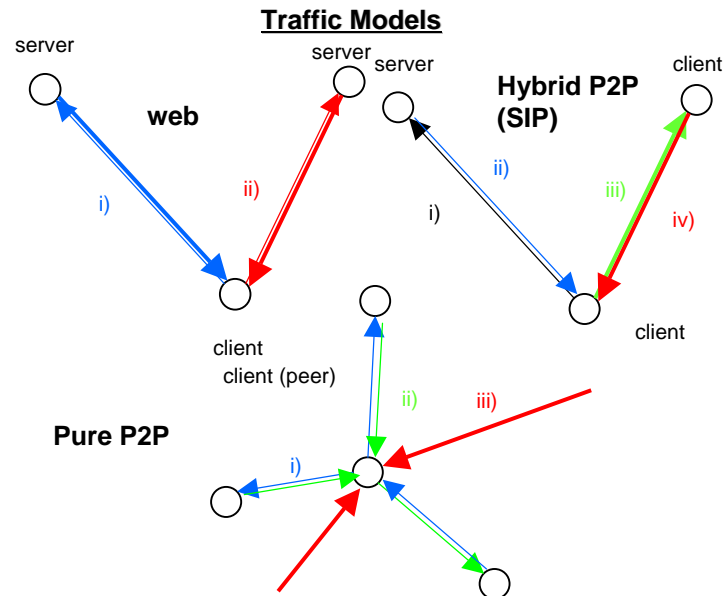
- 分析結果よりトラヒック的課題を抽出、今後の研究領域を示した
 - トラヒック測定、トラヒック制御、ネットワーク設計/管理法についてそれぞれ対策と課題を示した。

- 亀井聡, 森達哉, 大井恵太, “P2Pファイル共有の実態と課題”, 信学技報, CQ-2003-40, July 2003.
- 亀井聡, 森達哉, 木村卓巳, “P2Pトラヒック分離法とその評価”, 信学ソ大, B-7-19, September 2003.
- 森達哉, 亀井聡, 大井恵太, “P2Pトラヒックの測定と特性評価”, 信学ソ大, SB-3-1, September 2003.
- 岡田昭宏, 川原亮一, “IP網におけるトラヒック特性分析の一考察”, 信学技報, NS2003-5, April 2003.
- WIDE Project, “Measurement and analysis on the WIDE internet”, <http://www.wide.ad.jp/wg/mawi/>, 1988.
- Netarc, “P2P Finder”, <http://www.netarc.jp/p2pfinder.html>, July 2003.
- NetAgent, “P2P検知技術”, <http://www.netagent.co.jp/ppt/p2p.ppt>, ACCSセミナー, October 2003.



トラフィック分離, 識別技術 ~ 提案方式

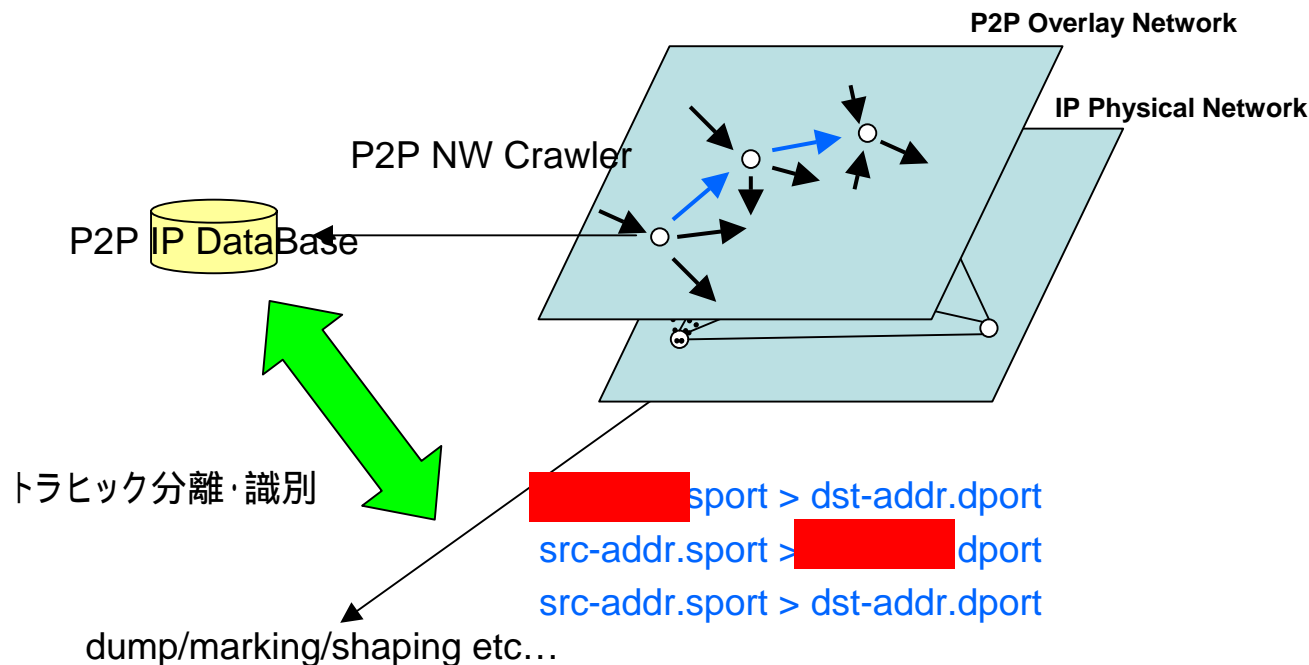
- 不特定の複数ノードと常にセッションを張りながらP2Pネットワーク上を移動する, P2Pアプリケーションの挙動に着目
- P2Pアプリケーションを通常の手続きで動作させ, 隣接ノードとの通信をネットワークレイヤで測定できれば実施可能.
汎用性が高く, アプリケーションの内部構造に依存しない
- トラフィックに対するマッチングは, 送受信アドレスのみ
スケーラビリティに優れる



トラフィック分離, 識別技術 ~ アルゴリズム

アルゴリズム

1. 任意の場所においてP2Pネットワークに接続したノードを設置, IPレイヤでの通信相手(P2Pレイヤでの隣接ノードのIPアドレス)を記録
2. 収集したアドレス情報に有効期限を設定し, P2P IPデータベースに登録
3. P2Pトラフィック識別対象の通信において送受信アドレスをデータベースに問合せ
4. 問い合わせ適合時にこれを P2P 通信と識別



トラフィック分離, 識別技術 ~ 実測に基づく評価

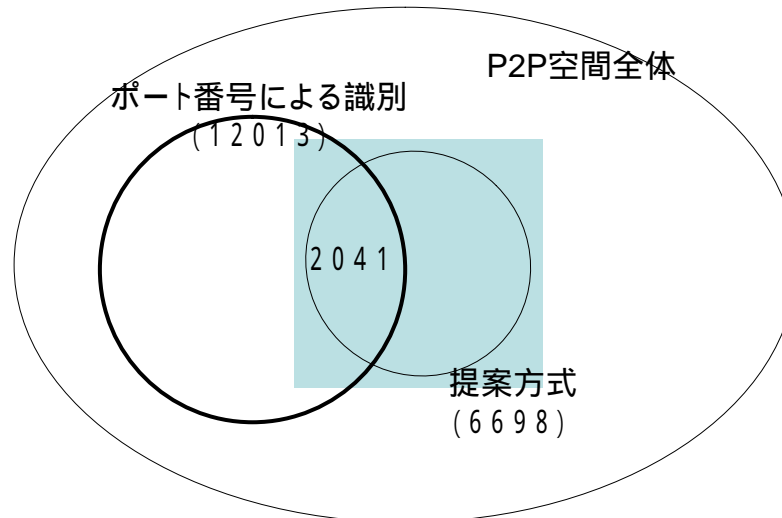
➤ 評価に用いたデータ

- ある組織のバックボーントラフィックの24時間分の送受信アドレスの組(100万アドレス)
- Winny, GnutellaでそれぞれIPレイヤでの収集アドレス(それぞれ1万5千, 1万6百)
- 比較のためにGnutellaのアプリケーションレイヤでの収集アドレス(19万)

➤ トラフィック分離結果

	ポート番号	提案方式	合計
Winny	12,013	6,698	16,670
Gnutella	951	212	1,129

➤ Winnyにおける識別空間



トラヒック分離, 識別技術 ~ 考察

➤ 考察

- ポート番号識別との併用で, Winnyで40%弱, Gnutellaで20%弱のノードを新たに発見

本トラヒック分離方式の有効性が示された

- 提案方式でカバーできないアドレスがそれぞれ60%, 95%存在

アドレスの収集が不十分である可能性

- Gnutellaのアプリケーションレイヤでの取得アドレスを使うと, 2800アドレスを新たに識別可能(ポート番号方式の3倍)

アドレスの収集方式改善が今後の課題

