社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＤＳＭ－46／2007－ＱＡＩ－24（２）
2007／7／19

フィルタ共有によるP2Pネットワーク上の有害コンテンツ拡散抑制

伊吹和也† 川原崎雅敏†

†筑波大学図書館情報メディア研究科 〒305-8550 茨城県つくば市春日 1-2
E-mail: †{ ibuki, mkawa} @slis.tsukuba.ac.jp

あらまし 近年，P2P ファイル共有ソフトの使用による著作権の侵害や，ウィルス感染による情報漏洩などがメディアで取り上げられ，大きな問題となっている．今後想定される，様々な分野での P2P ネットワークのビジネス利用に向けては，ネットワーク全体の更なる安全性，信頼性が求められ，著作権侵害や情報漏洩などの原因となる有害なコンテンツをフィルタリングする技術が重要になりつつある．

本稿では，スキルの高いピアが作成するフィルタを，そのピアと信頼関係を持つ全てのピアが共有することにより，様々な有害コンテンツの拡散を抑制すると共に，有害で悪意あるピアをネットワークから隔離することを可能にする方式を提案する．また，その基盤技術として，スキルの高いピアを本人特定することなく認証する方法として，P2P ネットワークに参加する各ピアに対して，匿名性を保持した本人証明を行う技術について述べる．

キーワード インターネット，P2P，フィルタリング，認証技術

Suppression of Harmful Content Diffusion over P2P Network Using Filter Sharing

Kazuya IBUKI† and Masatoshi KAWARASAKI†

† Information and Media Studies, University of Tsukuba 1-2 Kasuga, Tsukuba-shi, Ibaraki, 305-8550 Japan
E-mail: †{ ibuki, mkawa} @slis.tsukuba.ac.jp

Abstract Recently, mass-media points out that the use of P2P file sharing software is inviting copyright invasions and/or virus based information leakages. Towards expected business use of P2P network, more secure and reliable network is pursuit and technologies to filter harmful contents that may cause copyright invasion and information leakage. This paper proposes a filter sharing method that suppresses the diffusion of various harmful contents and isolates malicious peers from the network. It also discusses basic technology that authenticates high-skill peer without revealing his/her name to other participating peers of a P2P network.

Keyword Internet, peer to peer, filtering, Certification

1. はじめに

パソコンの高性能化とブロードバンドの普及に伴い，インターネットの利用者数や情報量は爆発的に増大している．このような背景において，管理コストの削減やスケーラビリティ，耐障害性に優れた Peer-to-Peer（以降 P2P と呼ぶ）ネットワークが注目され，ビジネス利用への期待が高まっている．しかし，P2P による従来とは異なる事業モデルの形成や新規市場の創出が期待される一方で，ファイル共有ソフトを利用した不法コンテンツの流通や個人情報の漏洩，無効トラフィックによる回線帯域圧迫など，危惧すべき問題も指摘されている．メディアの P2P に対する一連の報道は，権利を侵害する不法なコンテンツと情報漏洩事件に焦点が当てられ，P2P 技術全般に対する悪印象を与える原因となっていることも否定できない．事実，現在ファイル共有ソフトが形成する P2P ネットワーク上には，不法なコンテンツや有害なコンテンツが多数存在しており，このような状況を改善するために早急な対策が求められている．

総務省は，ネットワークの中立性に関する懇談会，P2P ネットワークの在り方に関する作業部会にて，P2P を用いた新トランジットモデルやコンテンツ配信などの実証実験を行っており，いずれは大規模なユーザ発信型サービスも生まれてくると予想される．しかし，現在の P2P ファイル共有ネットワークの状況を見ても明らかなように，ネットワークを中正に維持するためには，著作権管理やユーザ，コンテンツ管理を可能にし，ネットワーク全体に対する統一的な基準を設けなければならない．そこで，現在のファイル共有ソフトが抱える問題への改善，解決策を示すことで，P2P を利用する他のサービスやソフトウェア，プラットフォーム，ユーザ発信型の次世代 P2P サービスモデルで生じる課題の解決に繋がると考えられる．

本稿では，ピア間でのフィルタ共有を用い，現在のファイル共有ソフトが抱える問題点のひとつである権利侵害コンテンツ，ウィルスなどの有害コンテンツの拡散抑制を可能にし，情報漏洩などの二次的な被害への解決策を提示する．知識共有による柔軟で信頼性の高いフィルタを適用することで，安全性の向上と，有害コンテンツの効率的な拡散抑制，有害コンテンツをばら撒くピアの判別，隔離が期待できる．また，匿名性を維持した認証方式についても触れ，ピア間の信頼関係を利用したP2Pネットワークの自律的な調整の可能性について論じる．

2. P2Pファイル共有ソフトの現状

現在，ファイル共有ソフトが形成するネットワーク上には，著作権を侵害するコンテンツや広告目的のスパムコンテンツ,名称と実体が一致しない詐称(贋物)コンテンツ，P2Pネットワーク独特のウィルスなど，ネットワーク全体にとって有害なコンテンツが蔓延しており，ファイル共有ソフトを介したウィルス感染による情報漏洩などの二次的被害も増加している.更に，最近では漏洩した情報と実名 SNS とを組み合わせた名寄せにより被害が拡大する傾向にある．

2.1. 現在のファイル共有ソフトの問題

ネットワーク上での有害なコンテンツの氾濫，ウィルス感染による情報漏洩が後を絶たない原因として，P2Pは管理者が居ないために，一度ネットワーク上に公開されたものを回収，削除する事が非常に困難であることが挙げられる．更に，有害なコンテンツをネットワークにばら撒くピアの存在や，有害なコンテンツに対する知識や経験が乏しいピアが大多数であることも問題である．

2.2. 何故問題が起こるのか

現状，有害なコンテンツへの対策は，各ピアがファイル共有ソフトの機能として実装されているフィルタを利用，ウィルスに対してはアンチウィルスソフトの導入などで対応する他ないが，新種のウィルスが発見されてからアンチウィルスソフトが対応するまでの期間は事実上無防備な状態であり，最終的には各ピアの判断でそれぞれの状況に対応しなければならない．

将来的には変化する可能性もあるが，現在ファイル共有ソフトが形成するネットワーク上に存在するウィルスの殆どは，権利を侵害する不法なコンテンツと密接な関わりがあり，それらのコンテンツを求めるピアの不注意による感染を狙ったものであるため，ウィルスに感染するかどうかは各ピアのスキルレベルに大きく依存する．

スキルレベルの高いピアには，ウィルスの驚異度は比較的低いと言えるが,そうではない大多数のピアは，ウィルスに対して適切な対処が出来ず，結果P2Pネットワーク上で更にウィルスが蔓延し，その拡散を抑制が出来ないために情報漏洩などの二次的被害の増加を助長することになる．

3. 既存システム

本稿で提案するフィルタ共有について述べる前に，P2Pを対象としたものに限定せず，フィルタリング関連の既存技術を幾つか挙げ，P2Pネットワークへの親和度，不足している条件を考察する．

3.1. ファイル共有ソフトが実装しているフィルタ

現存P2Pファイル共有ソフトもフィルタ機能を実装していることが多いが，その多くは，各ピアが個別に条件を設定し，フィルタリングを行うものである．しかし，各ピアが個別に条件設定を行うため，ネットワーク全体での統一的な対応は難しい．権利を侵害する不法なコンテンツや，ウィルスなどの各種有害コンテンツに対して適切に対処出来るスキルの高いピア，及びP2Pネットワーク外での知識共有による情報蓄積を実現しているピア以外，特に，メディアの報道や雑誌の紹介記事などでファイル共有ソフトの存在を知ったばかりのスキルの低いピアは,フィルタの設定が適切，または充分ではないことが多く，ウィルス感染などの危険に晒されやすい．また，有害コンテンツのキャッシュを保持することにより，更なる拡散，被害の拡大を助長している．

3.2. ファイアウォール

ある特定のコンピュータネットワークとその外部との通信を制御し，内部のコンピュータネットワークの安全を維持することを目的としたソフトウェア，あるいはそのソフトウェアを搭載したハードウェアを指す．レイヤ3のIPパケットを監視するもの，レイヤ4で通信を代替し制御するもの，レイヤ7のプロトコルレベルで制御するものなど様々であるが，P2Pで遣り取りされるパケット制御が可能な反面，その内容を意識して選択的なフィルタリングを行うことは不可能である．

3.3. スパムフィルタ

サーバ上でメールの文脈や特定単語，特徴を判断し，フィルタリングを行う．代表的な方式として多重フィルタやベイジアンフィルタを用いたものを挙げることができるが，日々進化を遂げるスパムメールへの対応が追い付かない場合があることや，意図的な誤記など

によるフィルタの無効化が可能である．変わって，それらの問題に対応可能なコラボレーション型フィルタ（Collaboration based Filter）に注目する．この方式は，DNSBL（DNS-based Blackhole List）のように多くのユーザからのインプットをベースにフィルタを作成する方式である．DNSBL との違いは，IP アドレス以外の部分にも注目し，属性分割しそれぞれに信用度を紐付け，信用度判定による悪意の登録者の排除を可能にしているなどの点である．ユーザの知識を利用するという点では，P2P ネットワークへの親和度は高いと推察するが，特定のサーバを持たないピュア型の P2P ネットワークに適用するためには，何らかの工夫が必要である．

3.4. 要求される機能など

上述のように，現状では，統一的な基準の下 P2P ネットワーク上の有害なコンテンツのみを選択的にフィルタリングする事は非常に難しい．日々増え続ける有害なコンテンツに柔軟に対応し，統一的な基準の下にその拡散を抑制するためには，有害コンテンツに対する知識や経験を共有することが得策であろう．そのためには，

1. 各ピアが作成したフィルタを，ネットワーク上に公開可能にする
2. フィルタ作成においてスキルレベル（信頼度）の高いピアを評価可能とする
3. スキルレベルの高いピアに対する成りすましを排除する
4. 出来る限り煩雑な操作を必要とせず公開されたフィルタを共有可能にする
5. 嗜好性を考慮し，信頼できる複数のピアが公開したフィルタを組み合わせ，自身に適用可能にする

などの条件を満たす必要がある．

4. 要件

本章では，提案するフィルタ共有方式のモデル概要と，各部の具体的な内容について述べる．

4.1. フィルタ共有の基本モデル(三者モデル)

本稿で提案するモデルは，3.3 節で触れたコラボレーション型スパムフィルタに類する情報の共有と活用，それによるネットワーク全体での統一的な基準作成を目的としたフィルタの共有である．本モデルは，

- フィルタを作成，公開するピア
- フィルタのハッシュキーを保有するピア
- フィルタを取得，共有するピア

の三者で構成される．ネットワークはピュア型 P2P，検索アルゴリズムは Chord を想定している．

フィルタを作成するピアを Pn，キー保有ピアを An，共有ピアを Vn，Pn が作成するフィルタを F(Pn)と定義する．

DHT において，Pn が作成した F(Pn)のハッシュキーを保有する An がネットワーク全体に向けて公開し，Pn を信頼した Vn が Pn(もしくは F(Pn)を既に共有している他のピア)と通信し F(Pn)を取得，共有する．

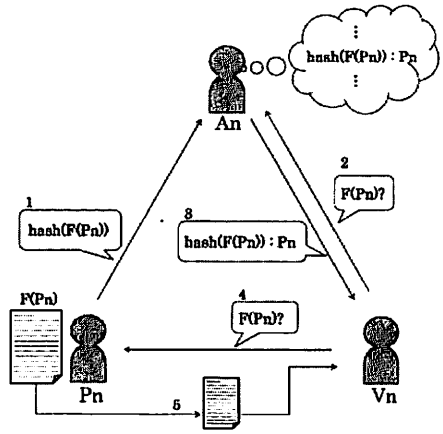

図 1 フィルタ共有モデル

4.2. フィルタリング方式

フィルタリングを行うにあたり，その方式としてブラックリストとホワイトリストの二通りのアプローチが考えられるが，許可された条件以外を全てフィルタリングするホワイトリスト方式を採った場合，P2P ネットワークの利点である負荷分散や有益なコンテンツに対する冗長性が生かせなくなってしまう可能性が高いため，今回の提案では，基本的にブラックリスト方式のフィルタ共有を行う．

各ピアは検索クエリ，キー，転送パケット，キャッシュを監視し，自身が適用したフィルタの条件に一致したものに対し，転送遮断やキー及びキャッシュの削除，転送元のピアとの一定時間の接続遮断などを実行する．これにより，同じフィルタを共有する全てのピア間でネットワーク全体に対して有害なコンテンツへの対処基準が統一され，有害なコンテンツの P2P ネットワーク全体への拡散抑制を実現する．

4.3. フィルタの適用方法

あるピアが，全ての有害なコンテンツについての情報を把握しているとは考えられないため，所有する情報に嗜好性や偏りがある事も考慮し，複数のフィルタを組み合わせ，補いあう形をとる．ウィルスなどのように，ネットワーク全体にとって確実に有害であると判断されるコンテンツ以外に，あるピアにはフィルタ

リングしたいと思われているが，別のピアにはそう思われていないコンテンツも存在する．ピアによりその基準は様々であるため，各ピアは，共有する複数のフィルタを組み合わせ，カテゴリ単位，ルール単位でカスタマイズし，それを自身の適用フィルタとして新たに出力し，適用する．

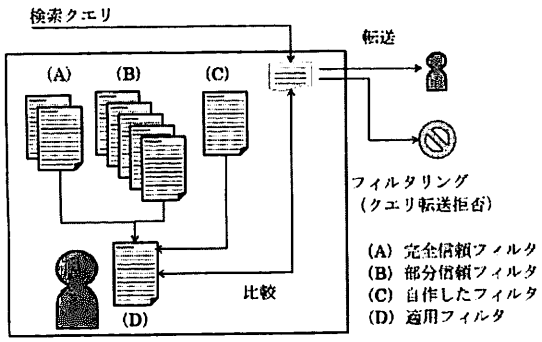

図 2 フィルタの統合と適用

4.4. フィルタの内容

各ピアが作成するフィルタは，RFC4180 に従う CSV 形式で記述する．まずフィルタリング条件に指定した理由毎（ex.ウィルス，詐称，権利侵害，など）にカテゴリを別け，条件毎に詳細を記述していく．条件は，キーワード（単語），拡張子，任意のハッシュ，コンテンツサイズ範囲などで指定する．条件毎に，対処方法（検索クエリ転送拒否の有効/無効，キャッシュの削除，コネクション切断の有効/無効など），有効期限，条件指定者などを指定する．各ピアが定めた有効値 E 以上（ex:E=5）のフィルタ作成ピアによりフィルタリング指定された条件を有効にし，適用フィルタへ反映させる．条件指定者にはその条件をフィルタリング対象として指定したピアを，有効期限は条件を有効状態に保つ期限（最後にその条件が働いた日時を基準）．各ピアは，フィルタ毎に信頼度（=そのフィルタを作成したピアに対する信頼度）を設定する（完全信頼/部分信頼）．部分信頼したピアのフィルタ項目の有効/無効判定は有効値 E に従い，E を超えた条件のみ有効にする．完全信頼したピアのフィルタに記述された条件に関しては，E に関わらず有効にする．自身が作成したフィルタの信頼度は任意で調整可能にし（完全信頼/部分信頼），必要があれば，フィルタリング除外条件の指定も行う．ある条件に対する対処方法が信頼したフィルタ間で異なる場合，信頼度が高いフィルタを優先する．これにより，ピア間での所有情報の差異を考慮しつつ，多くのフィルタ作成者がフィルタ指定した条件ほどネットワーク全体で統一的にフィルタリングされる確率が上がり，効率的な拡散抑制が期待できると推測する．

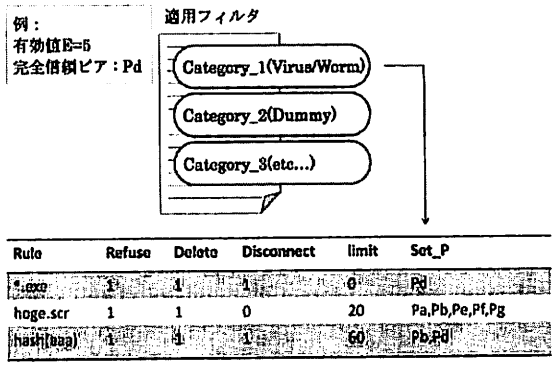

図 3 フィルタ記述方式

5. 評価

本稿で提案したフィルタ共有モデルを評価するため，以下の条件でシミュレーションを行った．

- 一台の物理 PC 上に，1000 ノードからなる仮想 P2P ネットワークを構築
- ハッシュキー空間は 128 ビットとする
- 検索アルゴリズムには Chord を使用
- 初期段階で，有害なコンテンツ Cx の完全キャッシュを保持するピア P(Cx)を全体の 1%と仮定
- P(Cx)は Cx の拡散アップロードを行うと仮定
- Cx を検索するピア群 Ps を全体の 10%と仮定
- 全てのピアは，一定時間毎にランダムでネットワークから一時離脱する可能性がある
- 一定時間 Q(Cx)への応答がない場合，Ps はランダムでネットワークからの一時離脱と再接続を試行する
- Ps は Cx の完全なキャッシュを得た段階で，ネットワークから離脱する可能性がある
- Pf は，Q(Cx)拒否，Cx キャッシュ削除，Cx キャッシュ転送元ピアとの接続を遮断する

以上の条件で，Pf の存在率の差異(5%/10%/30%/50%)による Q(Cx)，Ps，P(Cx)，Cx 拡散抑制への影響を検証する．

使用言語 C#

使用機器 CPU : AMD Athlon XP 2500+
メモリ : DDR333 512Mx2
OS : Windows XP SP2

図 4,5 より，ネットワーク全体に対し 30%程度の Pf が存在すれば，Q(Cx)を 60%以上無効化している．図 5 において Pf3-Pf4 間の差が僅かであり，Pf4 以降も Cx 拡散抑制率が向上しない原因としては，Q(Cx)を拒否された Ps，及び Pf からの接続遮断によりネットワークから隔離状態となった P(Cx)の再接続，各ピアのランダムな一時離脱などによるネットワーク状態の変化と，新たな Q(Cx)の発生が影響したものと推測する．

現実の P2P ネットワークにおいても，常時接続ピアは全体からみれば少数に過ぎず，大多数のピアは特定の時間帯にのみネットワークに参加していることから，共有フィルタ適用による効果も今回のシミュレーション結果に近いものになると予測する．

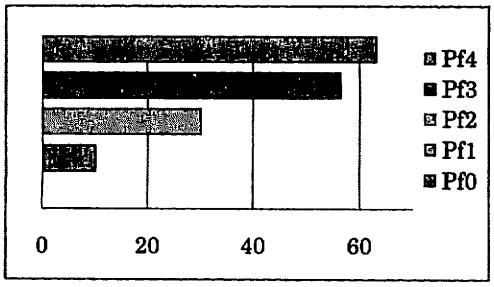

図 4 Q(Cx)のフィルタリング成功率比較

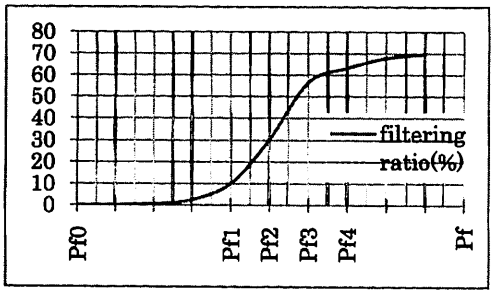

図 5 Cx の拡散抑制率

次に，フィルタ非共有時を基準とした，Ps が P(Cx)とのコネクションを確立するまでに要する平均時間比率を示す．

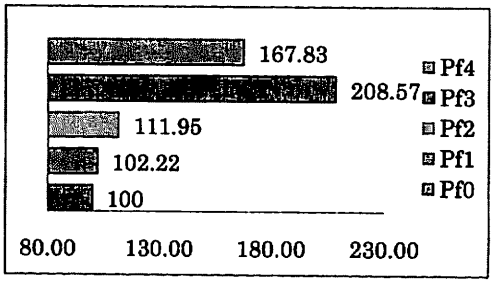

図 6 Ps/P(Cx)間通信実行までの平均時間比率

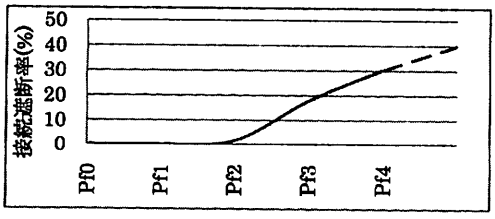

図 7 Pf の P(Cx)接続遮断率

図 6 において Pf4<Pf3 となるのは，Pf により隔離状態にされた P(Cx)が増加し，Ps/P(Cx)間のコネクション確立自体が難しくなることに起因すると思われる．Pf3 での P(Cx)との接続遮断が 17.85%であったのに対し，Pf4 では，ピアの離脱，再接続が頻繁に起こり得る状況下であるにも関わらず，30.232%の接続遮断を実現した．また，DHT と違い，flooding 方式のネットワークでは偏りが生じるため，近傍ピアに Pf が固まっていた場合，Q(Cx)が P(Cx)にまで辿りつく確率は限りなく低くなる事を追記しておく．

6. 本人証明

信頼性確保，及び成りすましを排除するためにも，Pn と F(Pn)の正統性を保証する仕組みが必要である．提案する方式では，図 1 の三者間モデルに幾つかの工程を追加することで実現できる．

まず，フィルタ作成ピア Pn はネットワーク参加前に公開鍵 e と秘密鍵 d のペアを生成すると共に，任意の文字列 W と，d で W を暗号化し得た dW を連結し(ex : "W@dW")，自身のエイリアス Al(Pn)とする．また，F(Pn)内に宣言用のカテゴリを設け，自身が得意としているカテゴリなどを含むプロフィール，自身が信用しているピア（エイリアス）リストなどと共に Al(Pn)を記述する．また，F(Pn)のファイル名には作成日時やリビジョンなどフィルタの新旧が比較できる情報を含める．

ネットワーク参加後は，hash(F(Pn))を An に通知すると同時に，e を公開する．そして，図 1 の第 5 工程で，Pn は Vn へ F(Pn)と共に，hash(F(Pn))を d で暗号化した d(hash(F(Pn)))を渡す．Vp は，公開されている e を用い d(hash(F(Pn)))を復号化し，計算によって求めた F(Pn)のハッシュと比較することで改竄がないことを確認する．そして，F(Pn)内に記述された Al(Pn)の dW 部を e により復号化した edW が W と等しいか確認することで，e が F(Pn)作成者の公開鍵であることも確認できる．

この時点で，e と hash(F(Pn))と F(Pn)により e が Pn の鍵であること，e と Al(Pn)と F(Pn)により d の所有者が Pn であること，及び Pn が F(Pn)作成者であることが証明された．よって，Vn は，以降 Al(Pn)が F(Pn)作成者であると信用しても良いということになる．

一連の工程を終えた後，Vn は An に向けて，F(Pn)に対する評価を d(AL(Vn))と共に渡し，An が F(Pn)に対する評価を集計し，公開することで，フィルタ内に記述されたエイリアスリストと照らし合わせることで，他のピアが F(Pn)，及び Pn が信用するピアの作成したフィルタを共有するかどうかの有効な判断基準なると予測する．

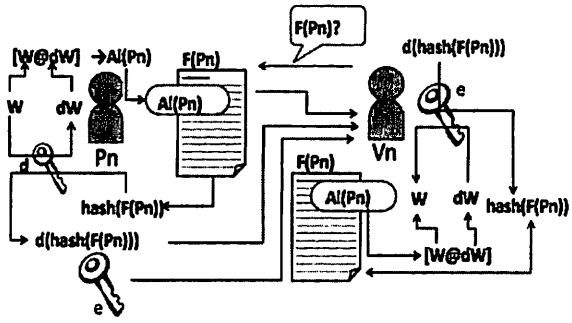

図 8 Pn/Vn 間でのやり取り（図 1-工程 4,5）

7. おわりに

今回提案したフィルタの共有により，ウィルスなどの有害なコンテンツを P2P ネットワーク上に蔓延させる主な原因となるスキルレベルの低いピアと悪意あるピア双方への対処が可能となり，柔軟な拡散抑制，ネットワークからの隔離を可能にした．しかし，本システムには，いくつかの課題が残っている．まず，本モデルは，ウィルスなどのネットワーク全体が有害と判断するファイルに対しては有効だと証明されたが，個人情報など，多くのピアが興味を持つコンテンツであるほど抑制が難しい点，より信頼性の高い認証システムとの導入という点で更なる改良の余地が見受けられる．機能的には等価なサービスが提供可能であると考えているが，サービス性や法制度，適用領域などを分析，評価し，より望ましい形態を明らかにする必要があると考える．

文　献

[1] Gnutella. http://gnutella.wego.com/.

[2] Ion Stoica, Robert Morris, David Liben-Nowell,David R. Karger, M. Frans Kaashoek, Frank Dabek, Hari Balakrishnan, "Chord: A Scalable Peer-to-peer Lookup Protocol for Internet Applications, "In Proceedings of ACM SIGCOMM, San Diego, August.2001. http://www.pdos.lcs.mit.edu/chord.

[3] Ian Clarke, Oskar Sandberg, Brandon Wiley, and Theodore Hong. "Freenet: A distribuited anonymous information storage and retrieval system, "In In Proc. of Workshop on Design Issues in Anonimity and Unobservability, pp.311-320, July.2000. http://freenet.sourceforge.net.

[4] PLAXTON, C., RAJARAMAN, R., AND RICHA, A. "Accessing nearby copies of replicated objects in a distributed environment, "In Proceedings of the ACM SPAA, pp.311-320, Newport, Rhode Island, June.1997.

[5] Michelle Anderson, Marcel Ball, Harold Boley, Stephen Greene, Nancy Howse, Daniel Lemire, Sean McGrath, "RACOFI: A Rule-Applying Collaborative Filtering System, "In Proc. IEEE/WIC COLA'03, Halifax, Canada, October.2003. http://www.daniel-lemire.com/fr/abstracts/COLA2003.html

[6] RFC4180, http://www.ietf.org/rfc/rfc4180.txt

[7] RFC2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, http://www.ietf.org/rfc/rfc2459.txt

[8] 平野基孝，首藤一幸，田中良夫，佐藤三久，"匿名相互証明書と P2P 通信を用いる認証方式，"IPSJ SIG Notes, Vol.2005, No.79(20050803) pp.17-24, Oct.2005.

[9] 伊藤洋輔，河野浩之，"P2P 環境下の評判モデルによる公平性保証，"電子情報通信学会 DEWS2007, Feb.2007.