仮想ピアを用いたP2Pネットワークの効率的な共有フィルタ管理手法の提案

佐久間 政碩[1] 喜多 義弘[1] 朴 美娘[1] 岡崎 直宣[2]

近年，コンピュータの高性能化とネットワークの発達により，P2Pネットワークを用いたサービスに注目が集まっている．しかし，P2Pネットワークでは，有害なコンテンツが拡散する問題が従来からあり，解決すべき問題となっている．本研究では，この問題を解決するために，仮想ピアを用いたP2Pネットワークの効率的な共有フィルタ管理手法を提案する．仮想ピアは，クラスタ内の性能の高いピアを複数集合して構築し，フィルタやコンテンツ所持者の情報を管理する．クラスタ内のピア同士でフィルタを共有することによって，フィルタの設定が脆弱なピアでも有害なコンテンツに対して有効なフィルタの設定が可能となる．

A Proposal of Efficient Shared Filter Management Method of P2P Network

Masahiro Sakuma[1] Yoshihiro Kita[1] Mirang Park[1] Naonobu Okazaki[2]

1. はじめに

近年，コンピュータの高性能化とネットワークの発達により，P2Pネットワークモデルを用いたコンテンツ配布サービスに注目が集まっている．P2Pネットワークでは，サーバを必要とせず，各ピアが互いにサービスを提供し合うため，単一障害点が起こりにくい．また，ネットワークの負荷を各ピアに分散させるため，高いスケーラビリティを実現できる［1］．しかし，P2Pネットワークにおける問題の1つに，有害なコンテンツがネットワーク全体に拡散しやすいことがある［2,3,4］．そこで有害なコンテンツへの対策として，ピア間でのフィルタ共有手法［5］が提案されている．この手法では，ネットワーク内の全ピアが有害なコンテンツに有効なフィルタを有するために，有効なフィルタをピア間で管理し共有する手法である．これにより，個別にフィルタを有しないピアにも有効な共有フィルタを持たせることができる．しかし，共有フィルタの管理をピアごとに行っているため，時間がたつことにより各ピアのフィルタにばらつきが生じ，フィルタ管理が不十分なピアを中心に有害なコンテンツが再び拡散しやすくなることが考えられる．

一方，ピュア型P2Pネットワークは，各ピアがコンテンツの配信だけでなく，コンテンツの検索も行うため，検索用のサーバも必要としない．しかし，コンテンツの検索を行う際，任意のピアから発したコンテンツ要求（クエリ）をネットワーク内の全てのピアに伝搬させる必要があり，検索時間が長くなってしまうことが考えられる．そこで，効率的なコンテンツの検索を行うため，類似のピアをグループ化するクラスタリング手法が提案されている［6,7,8］．

このようなクラスタリングを用いたP2Pネットワークにおいては，共通のキーワードをクエリとする類似ピアを1つのクラスタとして論理的に構築することにより，クラスタ内の全ピアの共有フィルタを生成することができ，フィルタのばらつきを低減することができる．

しかし,クラスタ内の共有フィルタの管理者がいないため，フィルタ更新時期が遅れるピアが生じる問題点がある．そこで本研究では，仮想化技術を使ってクラスタ内の共有フィルタを一元管理できる仮想ピア［9］を構築し，その仮想ピアを用いたフィルタ共有手法を提案する．本提案手法では，共有フィルタのばらつきを低減することで，有害なコンテンツのネットワークへの拡散防止対策とクラスタ内の共有フィルタの統一が期待できる．

2. 既存研究

2.1 Winnyのフィルタリング［2］

P2Pファイル共有ソフトの1つであるWinnyでは，コンテンツ取引の際にまず検索条件を設定し上流ノードへ検索要求を行う．この時各ピアは，所持しているファイルを基にしたキーを所持しており，キーを使うことで検索条件と一致するか比較を行う．キーにはファイル名やファイルサイズ，同じファイル名から分割したキャッシュを識別する

†1 神奈川工科大学
Kanagawa Institute of Technology,Atsugi,Kanagawa 243-0292,Japan
†2 宮崎大学
University of Miyazaki,Miyazaki 889-2192,japan

個人フィルタ

対象				対処方法(無視条件)		
ファイル名	ハッシュ値	サイズ上限	サイズ下限	転送拒否	対象の削除	接続の拒否
*.exe	hash	100,000MB	1,000MB	1(拒否)	1(削除)	1(拒否)
お茶				1(拒否)	0(削除無し)	0(許可)

図 1. 個人フィルタ設定例

Fig.1 Example of personal filter

ためのハッシュ値が記録されている．

また，Winny では，無視リストと呼ばれるフィルタリングを採用している．無視リストとは検索要求を行う際に，各利用者がファイル名に対して無視したいキーワードを含むものを取引対象から除外する機能を持つブラックリスト方式のフィルタリングである．

無視条件として設定することができるのは，ファイル名の一部，ハッシュ値，トリップ，ファイルサイズとなっている．無視条件に指定したファイルは，取引の中断だけではなくキャッシュファイルとして所持を破棄することができるようになり，該当するキーを持つピアに対して無視警告を出すことができる．無視リストは，ファイルのダウンロード時に無視条件との照合を行いフィルタリングする．

この無視リストによって有害なコンテンツの拡散を防止することができるようになる．しかし，この無視リストを十分に機能させるためには利用者同士で対象の情報を共有しあい協力を行うことが必要となる．

Winny のフィルタリングの手順は次のようになる．

(1) コンテンツ要求ピアは，キーとハッシュ値を基にフィルタ設定と取引をしたいファイルのキーワードを検索条件に設定する．

(2) コンテンツ要求ピアは，検索条件を基に上流ピアへ検索要求を送信する．

(3) 検索要求を受け取った上流ピアは，検索条件と自身が持つキーを比較する．

(4) 一致するファイル名がキーに存在する場合，コンテンツ要求ピアへキーを送り返し，一致するファイル名がキーに存在しない場合，さらに上流のピアへ検索要求を送信する．

(5) コンテンツ要求ピアは，キーとフィルタ条件を比較し，一致しない場合のみコンテンツ取引対象とする．この時，フィルタ条件にハッシュ値が設定されている場合フィルタ対象となっているファイル名であってもハッシュ値が一致していない場合取引対象とする．

2.2 スーパーノードを用いたコンテンツ検索手法［10］

P2P ネットワークには，効率的にコンテンツ検索を行うために，スーパーノード型と呼ばれるネットワーク手法がある［10］．これは，スーパーノードと呼ぶピアをネットワーク内から選出し，スーパーノードによってコンテンツのインデックス情報を管理するものである．そして，ネットワーク内のピアからクエリを受理した際，目的のコンテンツを保持するピアの情報をそのピアに提供する．クエリの受け渡しによる負荷の集中を考慮し，スーパーノードに性能の高いピアを割り当てたり，複数のスーパーノードに処理を割り振ったりと様々な対策を施しているが，スーパーノードの離脱や障害発生により，所持しているインデックス情報が損なわれてしまう問題点がある［1,10］．

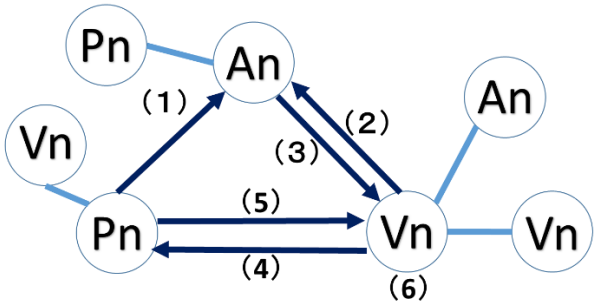

図 2. ハッシュキーを用いたフィルタ共有手法

Fig.2 Filter sharing using hash keys

2.3 ハッシュキーを用いた既存のフィルタ共有手法[5]

一般的に P2P ファイル共有ソフトにおいては，各ピアが個人フィルタを作成している（図 1 に，個人フィルタの設定例を挙げる）．そのため，有害なコンテンツに関する知識が豊富な熟練したピアは，有害なコンテンツを共有しないフィルタの設定ができる．しかし，有害なコンテンツに関した知識が足りない未熟なピアでは，十分な設定が行えずの被害を受け，P2P ネットワーク上に有害なコンテンツを拡散してしまう問題点がある．

このような問題点を解決するために，ハッシュキーを用いたフィルタ共有手法が提案されている［8］．この手法では，有害なコンテンツに対して有効なフィルタ設定情報をピアからピアへ受け渡すことができる．

本手法におけるフィルタ共有の手順を図 2 を用いて説明する．ここでは，次のような記号を用いる．

- Pn (Producing Node): フィルタを作成するピア
- An (Administrator Node): 作成されたフィルタのハッシュキーを管理するピア
- Vn (Void Node): フィルタを要求するピア

(1) Pn → An : Send(*K*fn)

フィルタを作成するピア Pn は，自分が作成したフィルタ fn に対するハッシュキー（Kfn）を作成し，ハッシュキーを管理するピア An へハッシュキーを送信する．

(2) Vn → An : Req(Kfn)

Vn は，ピア Pn のフィルタを設定するために，対応するハッシュキーを An へ要求する．

(3) An → Vn : Send(*K*fn)
An は，要求されたハッシュキーを Vn へ送信する．

(4) Vn → Pn : Req(*E*(fn))
Vn は，ピア Pn へフィルタを要求する．

(5) Pn → Vn : Send(*E*(fn))
Pn は，Vn へ自身が作成した暗号化されたフィルタを送信する．

(6) Vn : *K*fn(*E*(fn)) → fn
ハッシュキーと暗号化されたフィルタを受け取った Vn は，暗号化を解除する．暗号化が解除できない場合，なりすましによる偽装されたフィルタの可能性がある．

(7) Vn は同様に他のピアからフィルタを集め，Pn がフィルタの有効性を記録した有効値と，Vn の Pn に対する信頼値を元に適用するフィルタ設定を選択することによって，自身のフィルタ Pf の設定を行うことができる．以降同様に Vn は，新たな Pn となり他のピアへのフィルタ共有を行う．

この手法では，フィルタ設定が苦手なピアでも他のピアのフィルタを受け取ることにより，一定の強度を持つフィルタ設定を行うことが可能となる．しかし，この手法は，以下の 2 つの問題点がある．

- 各ピア自身がフィルタを管理するため，フィルタの内容や更新時期にばらつきが生じる．
- フィルタの更新情報は，自分から相手に聞く必要があるため，更新が遅れる．

これらの問題点により，P2P ネットワーク上に新たな有害なコンテンツが発生した場合，対応できずに拡散する可能性がある．

3. 提案方式

本研究では，フィルタのばらつきを低減し，有害なコンテンツの拡散を抑制するために，P2P ネットワークのクラスタにおける仮想ピアを用いたフィルタ共有手法を提案する．具体的には，仮想ピアはクラスタ内の各ピアからフィルタを集め，それらを合成し，共有フィルタを作成する．そして，作成した共有フィルタを各ピアに一斉配信することにより，クラスタ内の全てのピアが同じ共有フィルタを有することができる．

以下では，本手法で提案するクラスタ構築方法，仮想ピアとその構築方法，および仮想ピアを用いたフィルタ共有手法について述べる．

3.1 クラスタの構築方法

クラスタリングは，P2P ネットワーク内での効率的なコンテンツ検索を行うために，類似のピアを 1 つのクラスタとしてグループ化する手法である．クラスタを構築する基準は用途や場合によって様々である．各ピアは，求めるコンテンツの検索キーワード（以下メインキーワード）と，より詳細な検索範囲に絞り込むキーワード（サブキーワード）を有しており，本研究では，メインキーワードが共通のピアをクラスタとして構築する．

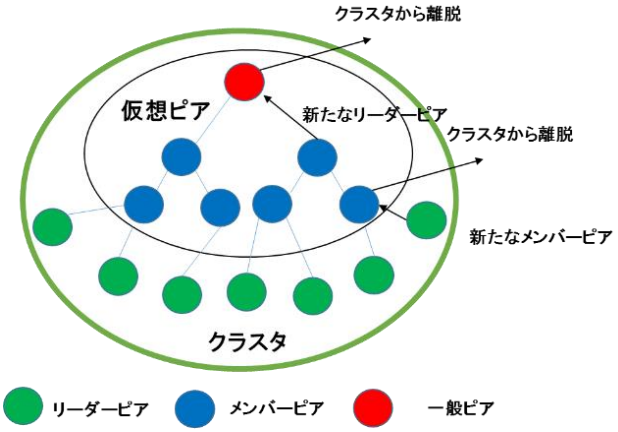

図 3．仮想ピアの維持

Fig.3 Replenishment of a leader peer and member peers

各ピアは，自身のメインキーワードと同じクラスタ 1 つのみに所属し，複数のクラスタに跨って所属することはできない．また，メインキーワードと同じクラスタが存在しない場合は，自ピアを中心として新たにクラスタを構築する．

3.2 仮想ピアの構築方法

一般に仮想ピアは，スーパーノードの代わりとして用いられる．仮想ピアを構成する複数のピアがインデックス情報を共有して管理を行い，ピアの障害によるインデックス情報の損失を防いでいる．そこで本研究では，仮想ピアの耐障害性を利用し，共有フィルタの一元管理を仮想ピアによって行う．

スーパーノードの役割を担うため，仮想ピアは，最も性能が高いピア(リーダーピア)を中心に比較的性能の高いピア(メンバーピア)によって構成する[8]．本研究では，この構成を基に性能だけではなく各ピアが持つ信頼値を用いて仮想ピアを構成するメンバーの決定を行う．信頼値とは，各ピアが通信を行った際の結果を基に設定する値である．各ピアは，相手に対する信頼値を所持する．信頼値の増減する条件は以下の 3 つである．

- コンテンツ取引成功
  コンテンツ取引が成功することにより，信頼値を増加させる．
- 連続したコンテンツ要求
  連続したコンテンツ取引成功による，悪意のあるピアの信頼値増加を防ぐために信頼値を減少させる．

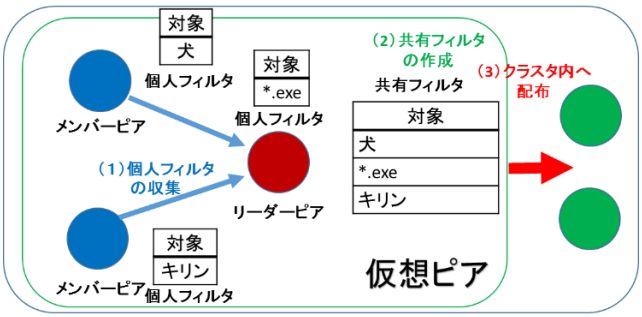

図 4. 共有フィルタの生成と配布

Fig.4 Generation and distribution of a shared filter

● 時間経過

長期間通信を行わないピアの信頼値は，信頼性が欠けるため信頼値を初期値である 0 に戻す．

仮想ピアを構成するメンバーは，自身が所持する信頼値の平均値と個人フィルタを所持していることを条件とする．また，インデックスや共有フィルタの管理にかかる負荷を分散させるために，クラスタの規模に合わせて，仮想ピアを構成するピアの数を調整し，階層化を行う．リーダーピアが離脱または障害が発生した場合は，現在のメンバーピアから新たなリーダーピアを選出する．そして，リーダーピアへの昇格やメンバーピアの離脱または障害の発生によりメンバーピアが減少した場合は，クラスタ内のピアから性能の高い順に選び補充する（図 3 参照）．

3.3 仮想ピアを用いたフィルタ共有手法

従来のフィルタ共有方式では，共有フィルタの管理を各ピアが行っていた．そのため，共有フィルタが統一されず，各ピアでの共有フィルタの更新にばらつきが生じる問題がある．

そこで，仮想ピアが共有フィルタの管理者となり，共有フィルタの一括管理を行う．そこで，仮想ピアが共有フィルタの管理者となり，共有フィルタの一括管理を行う．クラスタは共通のメインキーワードを持つピアの集合体であるため，各ピアの個人フィルタは共有フィルタを作成するための素材として有用であることが考えられる．共有フィルタを作成するために，リーダーピアは，自身の個人フィルタ仮想ピア内の各メンバーピアの個人フィルタを組み合わせることで共有フィルタを作成する（図 4 参照）．

共有フィルタを作成した後，仮想ピアはクラスタ内の全ピアに向けて共有フィルタを配布する．まず，仮想ピアを構成するメンバーピアを通じて，それらに隣接するピアに配布する．そして，共有フィルタを受け取ったピアはさらに自身に隣接するピアに共有フィルタを配布し，全ピアに行き届くまで繰り返す．

各ピアは共有フィルタを受け取った後，共有フィルタと所持している個人フィルタを併せてフィルタリングを行う．構造としては，自身に返ってきた検索クエリの応答をホワイトリストでフィルタリングを行い，通過した応答に許可リストを通じて共有フィルタでフィルタリングを行う，それを通過した応答をさらに個人フィルタがフィルタリングを行う．そして，個人フィルタでブロックした応答を仮想ピアに送信し，仮想ピアはその情報を共有フィルタに組み込み，再配布する．また，悪意のあるピアによって共有フィルタの内容を改ざんされる恐れがある．それを防ぐために，共有フィルタは仮想ピア以外では確認及び編集することができないようにする．これらにより，共有フィルタは常に更新され，クラスタ内の全てのピアで同じ共有フィルタを扱うことができる．また，新規のピアがクラスタに加入した際は，新規のピアは自身に隣接するピアから共有フィルタを受け取り，クラスタから離脱する場合は保持している共有フィルタを破棄する．

共有フィルタの編集を禁止することにより，共有フィルタの安全性を保つことができるが，フィルタ設定に長けているピア（熟練ピア）では，フィルタのカスタマイズができず，P2P ネットワークの利便性が低下することも考えられる．そこで，許可リストの設置を提案する．許可リストとは，各ピアがそれぞれで自由に設定できるホワイトリスト方式のフィルタである．許可リストは共有フィルタと併せて用い，共有フィルタで通過しなかった応答に対し，許可リストに記載されているキーワードを含んでいた場合は通過を許可する．許可リストで共有フィルタのフィルタリングの条件を緩和することにより，熟練ピアの利便性を保つことができる．

また許可リストの導入により，共有フィルタの更新は，個人フィルタでブロックした応答のうち許可リストに記載されていないキーワードを含む応答のみを仮想ピアに送信する（図 5,6 参照）．

各ピアから送信された「ブロックされた応答」を随時共有フィルタに組み込むと，共有フィルタの容量が膨大になる恐れがある．そこで，容量増加を軽減するために，共有フィルタ内の各フィルタ項目にラストフィルタリングタイム（Last Filtering Time: LFT）の記録を導入する．LFT とは，そのフィルタ項目を最後にフィルタリングした時間である．LFT は対象のフィルタ項目においてフィルタリングが行われる度に更新され，LFT から一定の期間を経過したフィルタ項目は自動的に破棄される．これにより，容量増加を抑えつつ，共有フィルタを洗練していく．逆に，フィルタ項目が破棄され続け，共有フィルタを縮小しすぎた場合，仮想ピアは，サブキーワードと同じキーワードをメインキーワードとする他のクラスタから共有フィルタを受け取り，自身の共有フィルタと組み込んだ後，クラスタ内の全ピア

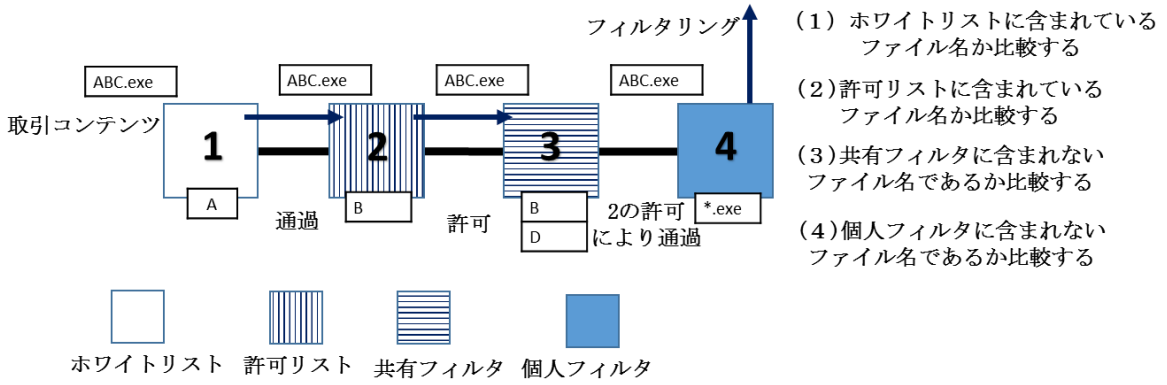

図 5. 取引時のフィルタ運用

Fig.5 Sending of filtering information to the virtual peer

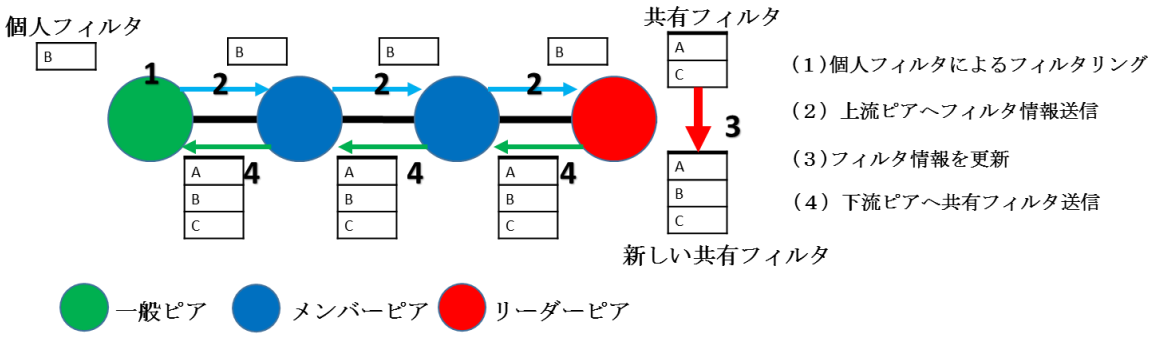

図 6. 共有フィルタの更新

Fig.6 Sending of filtering information to the virtual peer

に再配布する．

これらを踏まえて，個人フィルタ，共有フィルタ，及び許可リストの記述内容と，提案するフィルタ共有手法のアルゴリズムを以下に述べる．

3.4 各フィルタ及び許可リストの記述内容

各フィルタ及び許可リストの記述例を，図 7 に示す．個人フィルタと共有フィルタの記述形式は，既存のフィルタ共有手法［5］に基づいて定義している．

個人フィルタには，対象のキーワード（または条件）と，そのキーワードを含む応答への対処方法について記述する．対処方法は，転送拒否，対象の削除，及び接続の拒否の 3 種類である．それぞれの対処方法についてキーワードごとに許否を示す．

共有フィルタには，対象のキーワード（または条件）と，そのキーワードの LFT について記述する．LFT は年日時について秒単位で記録し，対象のキーワードのフィルタリングの度に，そのときの時刻で LFT を自動的に更新する．このとき LFT の更新は各ピアで行うことになるが，各ピアから LFT の内容を確認することはできない．

許可リストには，対象のキーワード（または条件）のみを記述する．各ピアでは許可したいキーワードをこのリスト内に任意に記述する．

3.5 フィルタ共有手法のアルゴリズム

本研究で提案するフィルタ共有手法のアルゴリズムについて述べる．以下に本提案手法に用いる記号を示す．

- k（Keyword）：
  クラスタ構成の基となるメインキーワード
- C（Cluster）：クラスタ
- N（CS）（Content Trading Success）：
  コンテンツ取引成功
- N（CR）（Continuous Request）：
  連続したコンテンツ要求
- V_c（Confidence Value）：信頼値
- V（PF）（Private Filter）：
  個人フィルタを所持している場合 1，所持していない場合 0 の値となる
- V（VP）（Virtual Peer）：仮想ピアの対象となるピアを判別する値
- LP（Leader Peer）：リーダーピア
- MP（Member Peer）：メンバーピア
- VP（Virtual Peer）：仮想ピア
- PF（Filte）： 個人フィルタ
- SF（Shared Filte）：共有フィルタ

ホワイトリスト

対象			
ファイル名	ハッシュ値	サイズ上限	サイズ下限
*.exe	hash	100,000MB	1,000MB

個人フィルタ

対象				対処方法(無視条件)		
ファイル名	ハッシュ値	サイズ上限	サイズ下限	転送拒否	対象の削除	接続の拒否
*.exe	hash	100,000MB	1,000MB	1(拒否)	1(削除)	1(拒否)
お茶				1(拒否)	0(削除無し)	0(許可)

共有フィルタ

対象	ラストフィルタリングタイム
犬	2013/10/10/12:30:20
*.jpg	2013/10/6/6:21:10
hash	2013/10/8/16:15:24

許可リスト

対象
ファイル名
*.exe

図 7. ホワイトリスト，個人フィルタ，共有フィルタ，許可リストの例

Fig.7 White list,Example of personal filter, shared filter, and permission list

本手法におけるフィルタ共有の手順は以下のようになる．

step1. 仮想ピアの生成

（1-1） 各ピアは，コンテンツの取引を行う際に N(CS)と N(CR)を比較することにより信頼値(V_c)を求める．

（1-2） k を基に存在しているピアを集め，C を形成する．

（1-3） C 加入後各ピアは，以下の式により仮想ピアの基準となる値（V（VP））を求める．

$$V(VP) = V\_c \times V(PF)$$

（1-4） C 内のピアで，最も V（VP）が高いピアを LP とする．

（1-5） LP は，C 内のピアのうち，V（VP）が高い複数のピアを集め，MP とする．

（1-6） LP と MP は互いに C 内の各ピアの情報を共有しあい，VP を構築する．

step2. 仮想ピアによる共有フィルタの生成

（2-1）LP は，MP の PF を収集し，それらの和集合を C の SF とする．

（2-2）SF の生成または更新の後，VP(LP 及び MP) は，隣接するピアに SF を送信する．

（2-3）MP は，C 内の各ピアから送信されてくる，ブロックした応答の情報を受信する．

（2-4）MP は，LP へ受信したフィルタ情報を送信する．この時，階層化により上位の MP が存在する場合，上位の MP へ送信する．

（2-5）LP は，（2-4）の情報を現在の SF に組み込む．

（2-6）もしも SF の容量が一定量よりも下回った場合は，step2．の（2-1）へ戻る．

（2-7）step2．の（2-2）～（2-6）を繰り返す．

step3. 各ピアでの共有フィルタを用いたフィルタリング

（3-1） 変更した場合，各ピアはそれぞれ隣接するピアに SF を送信する．ただし隣接するピアの SF が送信する SF と等しい場合は送信しない．

（3-2）各ピアは自身の許可リストを作成する．

（3-3）各ピアは受信した SF と PF とホワイトリスト及び許可リストを併用してフィルタリングを開始する．

（3-4）許可リストに含まれていないキーワード(または条件)の応答を個人フィルタがブロックした場合，その応答を VP に送信する．

（3-5） C から離脱する場合，SF を破棄する．

（3-6） step3．の（3-1）～（3-5）を繰り返す．

4. 考察と評価

4.1 考察

● 新たな有害なコンテンツが発生した場合の考察

クラスタ内に，新たな有害なコンテンツが存在した場合の共有フィルタの動作について考察する．新たな有害なコンテンツがクラスタ内に存在する場合，このコンテンツをフィルタリングできるピアがあれば，フィルタリングを行うと同時に仮想ピアへフィルタ設定が送られ，新たな共有フィルタをクラスタ内に配布する．これにより，最小限の被害で効率よく有害なコンテンツの拡散抑制が行うことができると考えられる．

● 攻撃者が悪意のあるフィルタを共有させた場合の考察

攻撃者が，P2P ネットワーク上に有害なコンテンツの拡散を目的として，脆弱性のあるフィルタを作成した場合について考察する．クラスタ内のピアから，仮想ピアの共有フィルタに個人フィルタの設定が組み込まれる条件として，フィルタリングが行われることが必要となる．そのため，攻撃者が脆弱性のあるフィルタを共有フィルタに組み込むことは可能であるが，クラスタ内のピアに拡散させたい有害なコンテンツに対応した個人フィルタがあれば，共有フィルタに組み込むため，拡散を防止することができる．

● フィルタリングしてはいけないキーワードをフィルタに組み込まれた場合の考察

正常な通信を妨害しようとする悪意のあるピアが，フィルタにクラスタ構築の基となるメインキーワードや「あ, い, う」などの断片的な単語を登録した場合について考察する．悪意のあるピアが，クラスタ内のやりとりを妨害することを目的として悪意のある個人フィルタを作成する．フィルタリングが行われることで悪意のある個人フィルタが仮想ピアへ送られる．仮想ピアは，悪意のある個人フィルタを組み込んだ共有フィルタをクラスタ内のピアへ配布する．

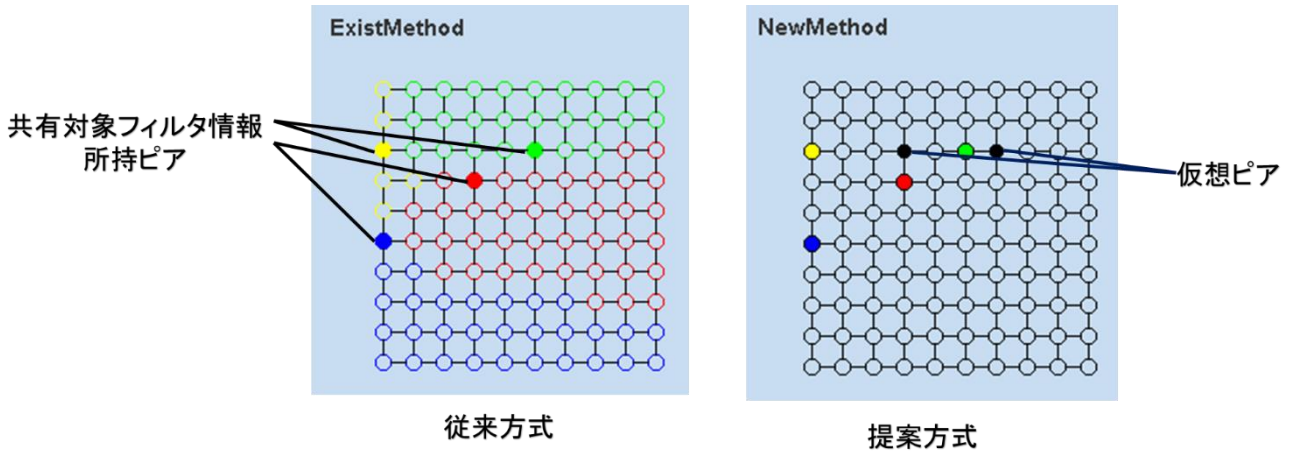

図 8. 共有フィルタのばらつきの比較

Fig.8 Comparison of dispersion of the shared filter

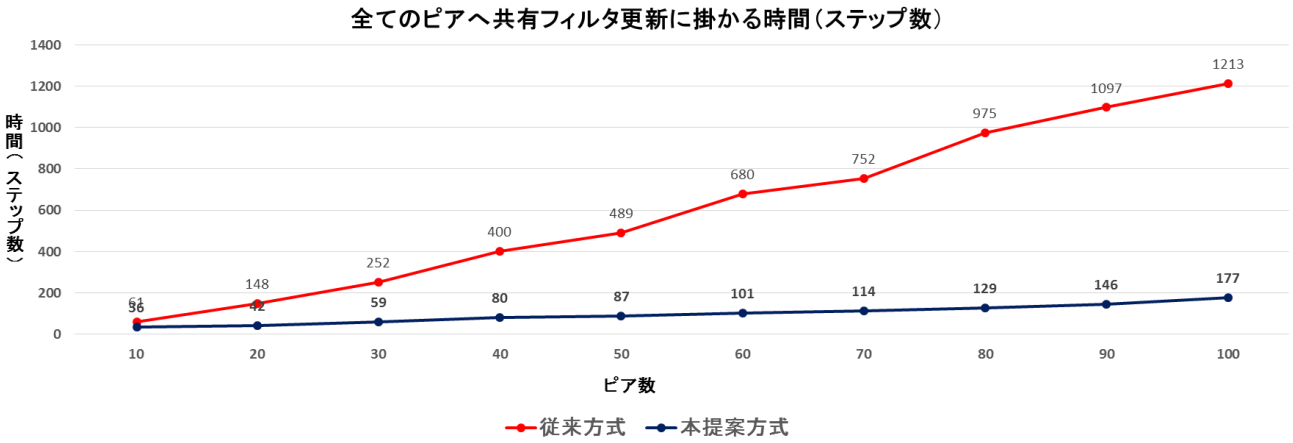

図 9. 共有フィルタ配布時間の比較

Fig.9 Comparison of dispersion shared filter time

この時，悪意のあるピアが作成したフィルタに登録された情報が，メインキーワードやサブキーワードを許可リストに自動で登録されているため，クラスタ内のやりとり妨害を防ぐことができる．しかし，メインキーワードやサブキーワードを含む有害なコンテンツを作成された場合，許可リストを介してフィルタを通過する問題点があると考えられる．

4.2 評価

既存の P2P ネットワークにおけるフィルタ共有手法と本提案の仮想ピアを用いたクラスタリングにおけるフィルタ共有手法における比較を行うため，以下の条件でシミュレーションを行った．

- クラスタ構築した状態で格子状のネットワーク
- 同一のクラスタ規模，フィルタ環境で 20 回繰り返す
- ピア数は 10 ずつ増加させ，最大で 100 ピア
- フィルタを共有したピアは，共有対象フィルタ情報所持ピアと同じ色で表示される．

以上の条件で，クラスタ内の全てのピアへフィルタが統一されるまでの時間を検証する．

既存のフィルタ共有手法では，P2P ネットワーク全体でフィルタの共有を行うため，個人で共有するフィルタを管理する必要がある．そのため，共有対象となるフィルタを持つピアを自身で探し出して，適用するフィルタの選択をする必要があり，ピアごとに所持しているフィルタにばらつきが発生する（図 8 左部参照）．本提案では，類似したコンテンツを求めるピアのクラスタ内の仮想ピアを管理者とすることで，共有対象を共有したいピアが探し出すのではなく，所属しているクラスタ内のフィルタ設定を共有することが可能であり，仮想ピアによって共有フィルタの一括管理を行っているため共有するフィルタの統一が可能となり全体で同一のフィルタを所持していることが確認できる（図 8 右部参照）．また，クラスタ加入時からフィルタの共有を行うことができる．これにより従来のフィルタ共有手

法と比べ，クラスタ全体への素早い統一されたフィルタ共有によって有害なコンテンツの拡散抑制が可能であると考えられる(図 9 参照).

5. おわりに

本論文では，有害なコンテンツの拡散抑制を目的として，従来のフィルタ共有手法をクラスタリングと組み合わせた，仮想ピアを用いたフィルタ共有について提案した．その結果，従来のフィルタ共有の問題点であった新たな有害なコンテンツのネットワークへの拡散防止対策とクラスタ内の共有フィルタの統一が可能になった．以上の結果から有害なコンテンツの拡散抑制の向上が可能となる．

今後の課題として，フィルタ容量を考慮した通信量の確認，脆弱なフィルタへの攻撃成功確率を加えたシミュレーションによる有害なコンテンツへの拡散抑制効果確認が必要であると考えられる．

参考文献

[1] 江崎　浩(監修): P2P 教科書, 株式会社インプレス R&D, (2005).
[2] 金子　勇: Winny の技術,株式会社アスキー.(2005)
[3] 寺田　真敏, 宮川　雄一, 松岡　正明, 松木隆宏, 鬼頭　哲郎, 仲小路　博史: P2P ファイル交換ソフトウェア環境における情報流通対策向けデータベースの検討, 情報処理学会研究報告書, vol.2008, no.71,　pp.123-128, (2008).
[4] 安藤　類央, 外山　英夫, 門林　雄基: DLL injection を用いた P2P ソフトウェアの情報漏洩の追跡と防止, 情報処理学会研究報告, vol.2007, no.16, pp.49-53, (2007).
[5] 伊吹　和也, 川原崎　雅敏: 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, 情報処理学会研究報告, vol.107, no.151, pp.7-12, (2007).
[6] 上田　達也, 安倍　広多, 石橋　勇人, 松浦　敏雄: P2P 手法によるインターネットノードの階層的クラスタリング, 情報処理学会論文誌, Vol.47, No4, (2006).
[7] 川田　量久, 石本　一生, 植田　和憲: P2P ネットワークにおけるクラスタリング手法の提案, 情報処理学会研究報告, Vol.2007, no.38, pp.49-54, (2007).
[8] 横田　健治, 中河　隆二, 磯貝　太喜,　朝香　達也, 高橋　達郎: P2P ファイル共有アプリケーションにおける保持コンテンツの分散のためのクラスタリング手法, 電子情報通信学会論文誌, vol.j95-B, No.2,　pp.178-187, (2012).
[9] 鹿野　将典, 上田　達也, 安倍　広多, 石橋 勇人, 松浦　敏雄: P2P 基盤ソフトウェア musasabi の仮想ピアにおける通信方式,”　電子情報処理学会研究報告, 2009-DPS-139, No.2, pp.1-8, (2009).
[10] R.Venkadeshan, M.Jegatha,: SupeVneer Deployment in Unstructured Peer-to-Peer Networks, International Journal of CoAnuter Networks and Wireless Communications (IJCNWC), Vol.2, No.1, 105-114, (2012).