

[研究論文] **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の提案**

佐久間政碩<sup>1</sup>・喜多義弘<sup>2</sup>・岡崎美蘭<sup>3</sup>

1 博士前期課程 情報工学専攻

2 セキュリティー研究センター

3 情報ネットワーク・コミュニケーション学科

**A Proposal of Filter Sharing Method Using Virtual peer for Cluster of P2P Network**

Masahiro Sakuma<sup>1</sup>, Yoshihiro Kita<sup>2</sup>, Mirang Okazaki<sup>3</sup>

**Abstract**

In the P2P network, clustering method is used for search of contents efficiency. The clustering method has a problem which is the diffusion of various harmful contents, as same as the problem of P2P network. In this paper, we propose the shared filtering method using virtual peers for clustering. The virtual peers which is the gathering high-spec peers in a cluster, manages the information of filter and content owners. The vulnerable peers can suppress the diffusion of various harmful contents by the shared information filter.

**Keywords:** P2P Network, Shared Filters, Clustering Method, Virtual Peer

**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<sup>1)</sup>。特に、ピア型 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<sup>2,3,4)</sup>。

一方、P2P ネットワークにおける問題の 1 つに、ウィルスを有する悪意のある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<sup>5,6)</sup>。悪意のあるコンテンツへ

の既存対策として、ピア間でのフィルタ共有手法<sup>7)</sup>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悪意のある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悪意のあるコンテンツが拡散することが考えられる。

クラスタリングを用いた P2P ネットワーク手法においても、悪意のあるコンテンツの拡散問題は例外ではない。しかし、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も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を一元管理できる仮想ピア<sup>8)</sup>を構築し、その仮想ピアを

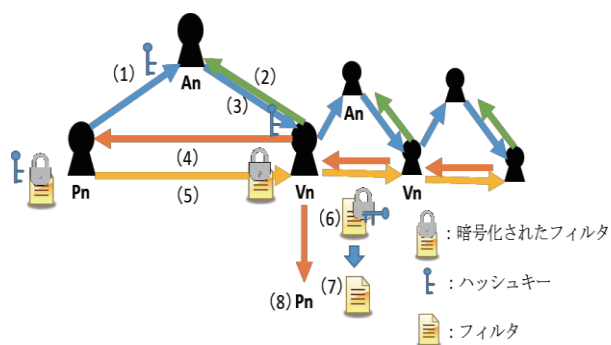


Fig. 1 Filter sharing using hash keys

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、新たな悪意のある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。また、仮想ピアを用いることにより、クラスタ内のピア同士のフィルタ共有だけではなく、他クラスタともフィルタを共有することが期待できる。

## 2. 既存研究

### 2.1 スーパーノードを用いたコンテンツ検索手法

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<sup>9)</sup>。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。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<sup>19)</sup>。

### 2.2 ハッシュキーを用いた既存のフィルタ共有手法

一般的に P2P ファイル共有ソフトにおいては、各ピアがフィルタを作成している。そのため、悪意のあるコンテンツに関する知識が豊富な熟練したピアは、悪意のある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、悪意のあるコンテンツに関する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 ネットワーク上に悪意のある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、フィルタ共有手

法が提案されている<sup>7)</sup>。

Fig.1 にて用いる記号を以下に示す。

- 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

この手法では、悪意のあるコンテンツに対して有効なフィルタ設定をピアからピアへ受け渡す。

この手法におけるフィルタ共有の手順は以下のようになる。

- (1) Pn は、自分が作成したフィルタに対するハッシュキーを作成し、An へハッシュキーを送信する。
- (2) 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 は、要求されたハッシュキーを Vn へ送信する。
- (4) Vn は、ピア Pn へフィルタを要求する。
- (5) 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) 暗号化されたフィルタとハッシュキーを受け取った Vn は、フィルタを解除する。フィルタ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もある。
- (7) Vn はフィルタを集め、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、自身のフィルタの設定を行うことができる。
- (8) 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有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リング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悪意のある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、悪意のあるコンテンツの拡散を抑制するために、P2P ネットワー

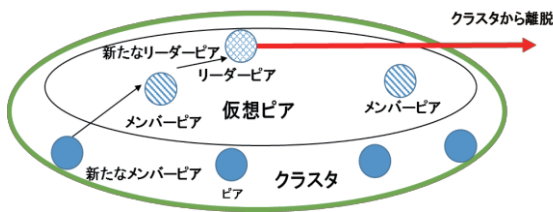


Fig.2 Replenishment of a leader peer and member peers

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や他のクラスタからフィルタを集め、それらを合成し、ブラックリスト方式の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。

以下では、クラスタとその構築方法、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（メインキーワード）と、より詳細な検索範囲に絞込むキーワード（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。

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 仮想ピアとその構築方法

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ではなく各ピアが持つ信頼値を利用することで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行動を基に増減する数値である。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。

フィルタリング発生

フィルタリングが発生することにより信頼値を減少させる。

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。

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、その数を一定に保つ。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 (Fig.2 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。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。また、キーワードが類似したクラスタ同士の共有フィルタも類似したものであると考えられる。これらを踏まえ、共有フィルタを作成するために、自クラスタ内の各ピアの個人フィルタと、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クラスタの共有フィルタを集め、それらを融合する (Fig.3 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

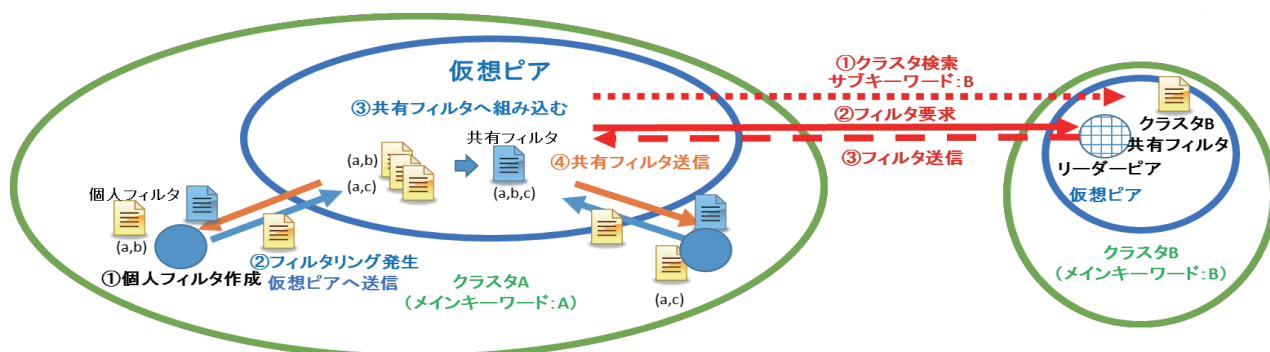


Fig.3 Generation and distribution of a shared filter

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共有フィルタでフィルタリングを行い、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あると考えられる。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 (Fig.4 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、Fig.5 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<sup>7)</sup>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可を示す。

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 は年月日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



## 個人フィルタ

対象	対処方法		
	転送拒否	対象の削除	接続の拒否
犬(単語)	1(拒否)	1(削除)	1(拒否)
*.exe(拡張子)	1(拒否)	1(削除)	0(許可)
hash(saa) (ハッシュ)	1(拒否)	1(削除)	1(拒否)
10GB以上 (コンテンツ容量)	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(単語)	2013/10/10/12:30:20
*.jpg(拡張子)	2013/10/6/6:21:10
hash(cba) (ハッシュ)	2013/10/8/16:15:24

## 許可リスト

対象
犬(メインキーワード)
白い(サブキーワード)
hash(cbb)
骨

Fig. 4 Sending of filtering information to the virtual peer

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
- $k_{sub}$  (Sub Keyword) : サブキーワード
- $C$  (Cluster) : クラスタ
- $C_k$  (Cluster Keyword) :  $k$  を基に構成したクラスタ
- $N(CS)$  (Content Trading Success) : 通信相手のコンテンツ取引成功数
- $N(F)$  (Filtering) : 通信相手へのフィルタリング発生回数
- $N(CR)$  (Continuous Request) : 通信相手からの連続したコンテンツ要求回数
- $V_c$  (Confidence Value) : 通信相手の信頼値
- $AV_c$  (Average of Confidence Values) : 自身の所持する信頼値の合計と数を割った平均値
- $V(PF)$  (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) : 仮想ピアの基準となる値
- $LP$  (Leader Peer) : クラスタ内のリーダーピア
- $MP$  (Member Peer) : クラスタ内のメンバーピア
- $VP$  (Virtual Peer) : クラスタ内の仮想ピア

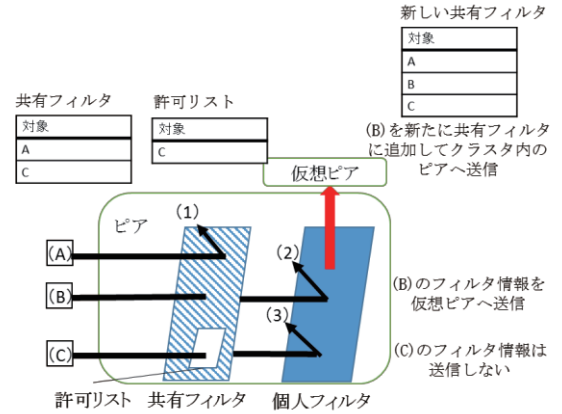


Fig. 5 Example of personal filter, shared filter, and permission list

- $SF$  (Shared Filte) : クラスタ内の共有フィルタ

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以下の式により通信相手の信頼値 ( $V_c$ ) を求める。

$$V_c = N(CS) - N(F) - N(CR)$$

- (1-2)  $k$  をメインキーワードとするピアを集め、 $C_k$  を形成する。
- (1-3)  $C_k$  クラスタ加入後各ピアは、以下の式により仮想ピアの基準となる値 ( $V(VP)$ ) を求める。

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

- (1-4)  $C_k$  内のピアで、最も  $V(VP)$  が高いピアを  $LP$  とする。
- (1-5)  $LP$  は、 $C_k$  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  $MP_{Ck}$  は互いに  $C_k$  内の各ピアの情報を共有しあい、 $VP$  を構築する。

## step2. 共有フィルタの生成

- (2-1)  $VP$  は  $C_k$  内の全ピアからサブキーワードを集計し、最も多いキーワードを  $C_k$  のサブキーワード  $k_{sub}$  とする。
- (2-2)  $VP$  は  $k_{sub}$  をメインキーワードとするクラスタ  $C_{k_{sub}}$  を検索し、そのクラスタの共有フィルタ  $SF_{sub}$  を取得する。
- (2-3)  $VP$  は  $C_k$  内の全ピアから個人フィルタを収集し、それらと  $SF_{sub}$  の和集合を  $C_k$  の共有フィルタ  $SF_{Ck}$  とする。

## step3. 仮想ピアによる共有フィルタの運用

- (3-1)  $SF_{Ck}$  の生成または更新の後、 $VP(LP$  及び  $MP)$  は、隣接するピアに  $SF_{Ck}$  を送信する。
- (3-2)  $VP$  は、 $C_k$  内の各ピアから送信されてくる、プロ

ックした応答の情報を受信する。

- (3-3)  $VP$  は, (3-2) の情報を現在の  $SF_{ck}$  に組み込む。
- (3-4) もしも  $SF_{ck}$  の容量が一定量よりも下回った場合は, step2. へ戻る。
- (3-5) step3. の (3-1) ~ (3-4) を繰り返す。

#### step4. 各ピアでの共有フィルタを用いたフィルタリング

- (4-1) 変更した場合, 各ピアはそれぞれ隣接するピアに  $SF_{ck}$  を送信する。ただし隣接するピアの  $SF_{ck}$  が送信する  $SF_{ck}$  と等しい場合は送信しない。
- (4-2) 各ピアは自身の許可リストを作成する。
- (4-3) 各ピアは受信した  $SF_{ck}$  と自身の個人フィルタと許可リストを併用してフィルタリングを開始する。
- (4-4) 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。
- (4-5)  $C_k$  から離脱する場合,  $SF_{ck}$  を破棄する。
- (4-6) step4. の (4-1) ~ (4-5) を繰り返す。

## 4. 考察と評価

### 4.1 考察

#### ● 新たな悪意のあるコンテンツが発生した場合の考察

クラスタ内に, 新たな悪意のある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。新たな悪意のある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悪意のある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 ネットワーク上に悪意のある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悪意のある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。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悪意のある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の比較を行う。

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, ピアごとにばらつきが発生する。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や類似したクラスタ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る。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, 統一されたフィルタ共有によって悪意のあるコンテンツの拡散抑制が可能であると考えられる。

## 5. おわりに

本論文では, 悪意のある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

た新たな悪意のある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。また、仮想ピアを用いることで、クラスタ内のピア同士のフィルタ共有だけではなく、他クラスタともフィルタ共有をすることが可能になった。以上の結果から悪意のある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、許可リストを通過する悪意のあるコンテンツの対策や、クラスタの規模に応じて仮想ピアを構築するピア数の増加、及びフィルタ有効期限の基準が必要である。

## 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] 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, No.4, (2006).
- [3] 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).
- [4] 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).
- [5] 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).
- [6] 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).
- [7] 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).
- [8] 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).
- [9] R.Venkateshan, 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).