非構造化P2Pネットワークにおける評価偽造の影響低減を目的とした評価集約手法

武田 苑子[1,a)]　牛窪 洋貴[1,b)]　重野 寛[1,c)]

概要：非構造化 P2P ネットワークにおけるファイル交換のセキュリティ対策として評価集約手法がある．評価集約手法 GossipTrust は，各ピアの信頼度を数値化したグローバル値を算出し，その値を参照することで安全なファイル交換を行っている．また，グローバル値の上位のピアである power node の持つ他ピアに対する評価を各ピアが参照することでより精度の高いグローバル値算出を行っている．しかし，ネットワーク上には正常なファイルを提供し続け高い評価を得ながら他ピアに対する評価を偽造する，評価偽造ピアが存在する．GossipTrust では，評価偽造ピアが存在し power node に選ばれた際の評価偽造の影響を考慮していない問題がある．そこで，各ピアが power node の評価との類似度を用いて評価偽造ピアが power node に選ばれていることを検知する手法 DIF-Trust を提案する．DIF-Trust では，評価偽造ピアが power node に選ばれた際の評価偽造の影響を低減することを目的とする．また，シミュレーション評価により評価偽造ピアによる影響の確認と，GossipTrust との比較を示す．

1. はじめに

現在，P2P ネットワークにおけるアプリケーションの 1 つとしてファイル共有ソフトが利用されている．非構造化 P2P ネットワークにおけるファイル共有では，各ピアはファイルのアップロード, ダウンロードを自由に行うことができる [1][2][3]．しかし，P2P ネットワーク上に存在する悪意あるピアがファイルの捏造やウィルスファイルのばら撒きなどを行った場合，ファイル交換が正常に行われなくなってしまう [4][5]．これに対して，非構造化 P2P ネットワークにおいて悪意あるピアとのファイル交換の回避を目的とした評価集約手法がある．評価集約手法は，各ピアの信頼度を数値化した評価値を算出し，ファイル交換の際に評価値を参照することで安全なファイル交換を行うことを目的としている．この手法により，どのピアが相対的に信頼できるかを判断できる [7][8][9]．

非構造化 P2P ネットワークにおける評価集約手法の 1 つに，GossipTrust が提案されている [7][8]．GossipTrust は，各ピアがランダムに隣接ピアを選択し，自身の持つ他ピアに対する評価と，その隣接ピアが持つ他ピアに対する評価を交換することで，他ピアに対する評価値を算出する．また，各ピアが隣接ピアと評価を交換する際に，評価値が上位数%のピアを power node と設定し，power node の持つ他ピアに対する評価を優先的に取り入れることによってより精度の高い評価値の算出ができ，より安全なファイル交換を行うことができる [6][8]．しかし，ネットワークには，悪意あるファイルは提供せず，正常なファイルを提供し続け高い評価を得ながら他ピアに対する評価を偽造するピア (評価偽造ピア) が存在する．GossipTrust では，評価偽造ピアが power node に選ばれてしまい，評価を偽造した場合の影響が今まで考慮されていなかった．

この問題に対して，本稿では各ピアが power node の評価との類似度を用いて評価偽造ピアが power node に選ばれていることを検知する手法 DIF-Trust を提案する [10]．DIF-Trust では各ピアが power node の評価に対する類似度と，比較スレッショルドを算出する．また，各ピアが power node に選ばれた評価偽造ピアの評価を取り入れず，さらに評価偽造ピアに対する評価を下げることによって，評価偽造ピアが power node に選ばれた際の評価偽造の影響を低減させる．さらに，コンピュータシミュレーションを用いて GossipTrust と提案手法の性能比較を行う．

以下，本稿の構成について述べる．まず第 2 章において関連研究について述べる．第 3 章で提案手法 DIF-Trust を提案し，第 4 章でシミュレーションを用いた評価により，提案手法は既存手法に比べファイル交換成功率が向上していることを確認する．最後に第 5 章で結論を述べる．

[1] 慶應義塾大学大学院理工学研究科
Graduate School of Science and Technology, Keio University
[a)] takeda@mos.ics.keio.ac.jp
[b)] ushikubo@mos.ics.keio.ac.jp
[c)] shigeno@mos.ics.keio.ac.jp

2. 関連研究

関連研究として，評価集約手法，評価の偽造，既存研究である GossipTrust について述べる．

2.1 評価集約手法

評価集約手法とは，P2P ネットワークにおけるファイル共有のためのセキュリティ対策の一つである．評価集約手法では，ウイルスファイルやごみファイルを提供する悪意あるピアとのファイル交換回避のために，評価値と呼ばれる各ピアの信頼度を数値化した値を用いている．評価値は，ローカル値とグローバル値の二つの値に分けられる．まず，ローカル値は，ファイルを受信したピア（受信ピア）がファイルを提供したピア（提供ピア）に対して，ファイルの中身の良し悪しから評価し，各ピアが算出する値である．ローカル値は各受信ピアが提供ピアに対して個別に算出するため，同一の提供ピアに対して各受信ピアが保持するローカル値は異なる．一方，グローバル値は各ピアが保持するローカル値から算出される値であり，各ピアが保持するローカル値を交換し合うことで値が集約され，ネットワーク全体のピア間でほぼ共通の値となる．

つづいて，ファイル交換において評価値がどのように用いられるかについて述べる．ファイル交換の際，各ピアはダウンロードしたいファイルを持つピアの中からグローバル値を参照し，各ピアの信頼度を判断する．このグローバル値の高いピアを選ぶことで，信頼度の高いピアを選ぶことができる．そしてファイル交換相手を決定し，実際に受信したファイルの善悪の結果からローカル値を更新し，そのローカル値を集約することでグローバル値を更新する．このように，ファイル交換の度に評価値を更新する．

2.2 評価の偽造

ネットワーク上には，悪意あるファイルを提供する他に，他ピアに対する評価も偽造する悪意あるピアが存在する．評価の偽造とは，評価を偽造するピアがファイル交換を経て提供ピアに対してローカル値を算出する際に，本来は提供ピアに対してローカル値が高いと評価すべきピアを故意に低いローカル値であると偽り，また逆に本来はローカル値が低いと評価すべきピアを高く偽ることを指す．評価集約手法において，このような評価を偽造するピアがネットワーク上に存在する場合，評価の偽造の影響により評価値算出の精度が低下してしまう．そして，評価値算出の精度が低下することによって，ファイル交換の際に正常なピアが悪意あるピアとファイル交換をしてしまう可能性が高まり，その結果，ネットワーク全体のファイル交換成功率が低下してしまう．

2.3 GossipTrust

非構造化 P2P ネットワークにおける評価集約手法の既存手法として GossipTrust がある．GossipTrust は，悪意あるファイルを提供し，かつ評価も偽造する悪意あるピアが存在する場合でも，評価値算出の精度の低下を抑制することを目的としている．

GossipTrust では，大きく分けて二つのフェーズが存在する．まず一つは，集約フェーズである．集約フェーズでは，各ピアが他ピアに対するローカル値を保持し，そして全てのピアが他ピアに対する評価値をピア間で互いに交換・集約することによってグローバル値を算出する．その際に，グローバル値の高い上位のピアが power node として選ばれる．ローカル値の初期値は，全てのピアが同じ値を保持する．評価値を集約する際に各ピアがより精度の高いグローバル値を算出するために，信頼度の高いピアの持つ評価値は精度が高いため，power node が保持する他ピアに対する評価値を優先的に参照する．

ここで，評価値の集約と power node の利用について，詳しく説明する．GossipTrust では，各ピアがグローバル値を算出する際に，正規化されたローカル値を含む評価データという値を計算し，それを各ピア間で集約することでグローバル値を算出する．各ピアがその評価データを算出する際に，グローバル値の上位のピアである power node の持つ正規化ローカル値を重み付けして各ピア自身の評価データに取り入れる．ここで，power node はグローバル値の上位のピアであり，信頼度の高いピアである．そのため，各ピアが power node の持つ他ピアに対する正規化ローカル値を重み付けして評価データに取り入れることで，精度の高いグローバル値を算出している．

ここで，各ピア i が他ピア（提供ピア）j に対して，t 回目で算出するローカル値を $r_{ij}(t)$ としたとき，正規化ローカル値 $s_{ij}(t)$ は式 1 で表される．

$$s_{ij}(t) = \frac{r_{ij}(t)}{\sum_{j=1}^{n} r_{ij}(t)}, (0 \leq s_{ij}(t) \leq 1) \tag{1}$$

正規化ローカル値 $s_{ij}(t)$ は各ピア $i = 1, 2, \cdots, n.$ に対して $\sum_{j=1}^{n} s_{ij}(t) = 1$ となる．また，各ピア i が他ピア j に対して算出する評価データ x_{ij} は以下の式 2 で表される．

$$x_{ij}(t) = ((1-\alpha)\, s_{ij}(t) + \alpha s_{pj}(t)) \times v_i(t-1) \tag{2}$$

$s_{pj}(t)$ は power node p の持つ他ピア j に対する正規化ローカル値であり，α は power node の持つ他ピアに対する正規化ローカル値の重み付け値を表す．また，$v_i(t-1)$ は 1 試行前の $t-1$ 回目で算出された各ピア i 自身のグローバル値である．式 2 より，t 回目における各ピア i が他ピア j に対して算出する評価データ $x_{ij}(t)$ は，power node の持つ正規化ローカル値 $s_{pj}(t)$ を重み付け値 α でどの程度取り入れるかを重み付けし，さらに，1 つ前のファイル交換で算出された自身のグローバル値を重み付けすることによっ

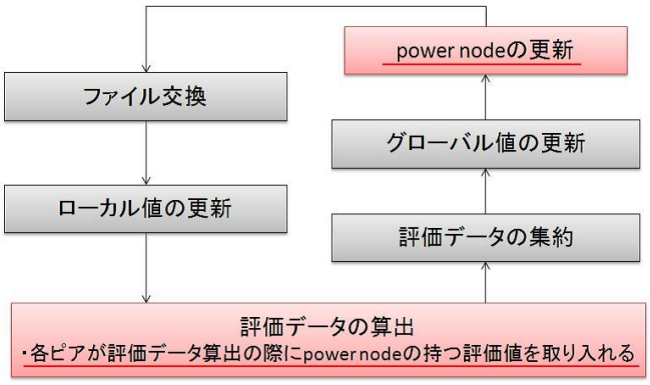

図 1　GossipTrust のサイクル

て表される．

続いて二つ目のフェーズは，交換フェーズである．交換フェーズでは，各ピアが他ピアとファイルを交換する．その際に，要求するファイルを持つピア群のグローバル値を参照し，グローバル値の高いピアをファイル交換相手として選択することで，安全なファイル交換が出来る．このように交換フェーズでファイル交換を行うごとに，各ピアは交換相手に対するローカル値を算出する．

ここで，GossipTrust のサイクルを図 1 に示す．図 1 は GossipTrust がこのサイクルを繰り返すことを表す．

このように，power node は評価値の高い上位のピアであり，正常なファイルや要求通りのファイルを送信し続け，高い評価を得ていれば，power node に選ばれる．よって，power node になる条件は，常に正常なファイルや要求通りのファイルを送信することに依存する．ここで，ネットワーク上における悪意あるピアは，主に 3 種類に分けられる．順に，悪意あるファイルの提供のみを行うピア，悪意あるファイルの提供は行わず他ピアに対する評価の偽造のみを行うピア，悪意あるファイルを提供しかつ他ピアに対する評価の偽造も行う多重の悪意ある攻撃をするピア，である．またこれらを順に，不正ファイル提供ピア，評価偽造ピア，多重攻撃ピアと呼ぶことにする．GossipTrust では，評価偽造ピアが存在する場合，他ピアに対する評価は偽造するが悪意あるファイルを送信しないため，評価偽造ピア自身の評価値は低くならず，power node に選ばれる可能性が高くなる．その結果，各ピアが評価データ算出の際に power node の評価値を参照するため，評価偽造による影響が出てしまうという問題がある．また，悪意あるファイルを提供するピアと結託をした場合，さらに評価偽造による影響が増大してしまい，その結果，正常なピアが悪意あるピアとファイル交換をしてしまう可能性が高くなる．

3. 提案手法

本稿では，非構造化 P2P ネットワークにおいて，各ピアが power node の評価との類似度を用いることで評価偽造ピアが power node に選ばれていることを検知する手法 DIF-Trust (Decreasing the Influence of Forgery) を提案する．DIF-Trust は，評価偽造ピアが power node に選ばれた際の評価偽造の影響を低減させることを目的とし，また，悪意あるファイルを提供するピアとの結託にも対応することで，ネットワーク全体でのファイル交換成功率低下の抑制ができる．DIF-Trust では，各ピアの持つ評価値と power node の持つ評価値の類似度と，比較スレッショルドを算出することで，評価偽造ピアが power node に選ばれていることを各ピアで検知する．さらに，power node に選ばれた評価偽造ピアに対する評価値を意図的に低下させることで，再び評価偽造ピアが power node に選ばれる確率を下げる．また，DIF-Trust では，GossipTrust と同様に評価値を算出している．提案手法 DIF-Trust は，

- 類似度と比較スレッショルドの算出
- 評価データの算出
- 評価偽造ピアに対する評価値の算出

から構成されている．

3.1 類似度算出と比較スレッショルド

各ピアが持つ他ピアに対する評価値と power node の持つ他ピアに対する評価値の類似度と比較スレッショルドを算出することによって，power node に選ばれた評価偽造ピアを各ピアが検知する．

まず，類似度の算出について説明する．各ピアの評価値の類似度は，θ_{ij} で表し，ピア i のピア j に対する評価値の類似度である．類似度の式は以下に示す．

$$\theta_{ij}(t) = \beta \times |s_{ij}(t) - s_{pj}(t)| . \tag{3}$$

式 3 より，各ピア i が持つ他ピア j に対する正規化ローカル値 $s_{ij}(t)$ と，power node が持つ他ピア j に対する正規化ローカル値 $s_{pj}(t)$ の差をとり，重み付け値 β によって重み付けした値である．重み付け値 $\beta(\ 0 \leq s_{ij} \leq 1\ )$ は，各ピアの正規化ローカル値の差をどの程度考慮するかの定数である．類似度 θ_{ij} は，その値が小さければ，各ピアと power node の持つ他ピアに対する評価が近いとなり，値が大きければ，各ピアと power node の持つ他ピアに対する評価は異なると判断している．また，評価値の類似度が比較スレッショルド ψ 以上ならば，power node の持つ正規化ローカル値 $s_{pj}(t)$ が偽造されているとし，評価偽造ピアが power node に選ばれていると判断する．逆に，評価値の類似度が比較スレッショルド ψ 以下ならば，power node の持つ正規化ローカル値 $s_{pj}(t)$ は偽造されていないとし，評価偽造ピアが power node に選ばれていないと判断する指標といえる．その際は，power node の持つ正規化ローカル値は信頼できるため，各ピア自身の評価データに，power node の持つ正規化ローカル値を取り入れる．このときの評価データは式 2 により算出する．

続いて，比較スレッショルド ψ について説明する．比較

スレッショルド ψ は，スレッショルドが小さすぎると，正常なピアが power node に選ばれているにも関わらず，評価偽造ピアが選ばれていると誤ってしまう．逆にスレッショルドが大きすぎると評価偽造を検知できない．そのため，DIF-Trust では，各ピアの，各時間ごとに動的な比較スレッショルドを算出する．その算出式は，以下に示す．

$$\psi_i(t) = s_{iH}(t) - s_{iL}(t) \tag{4}$$

$$s_{iH}(t) = \sum_{k=1}^{Hnum} s_{ih_k}(t)/Hnum \tag{5}$$

$$s_{iL}(t) = \sum_{k=1}^{Lnum} s_{il_k}(t)/Lnum \tag{6}$$

式 4 より，正常なピア数の総数が $Hnum$ であり，悪意あるピア数の総数が $Lnum$ である．また，$s_{ih_k}(t)$ は，各ピア i の正常ピア h_k に対する正規化ローカル値であり，$s_{il_k}(t)$ は各ピア i の悪意あるピア l_k に対する正規化ローカル値である．このとき，$s_{iH}(t)$ は，各ピア i が正常ピアに対して持つ正規化ローカル値の平均であり，$s_{iL}(t)$ は，各ピア i が悪意あるピアに対して持つ正規化ローカル値の平均である．ここで，各ピア i が正常なピアに対して持つローカル値は高く，悪意あるピアに対して持つローカル値は低くなると考えられる．比較スレッショルド $\psi(t)$ は各ピア i が持つ正規化ローカル値の高い平均と正規化ローカル値の低い平均の差から，時間 t ごとに動的に算出する．

3.2 評価データの算出

各ピアは，グローバル値の算出のために，ネットワーク全体でローカル値を含む評価データをピア間で交換・集約し，グローバル値を算出する．そのため，各ピアはローカル値を保持し，グローバル値を算出する際に，評価データを算出する．その際，各ピアは類似度と比較スレッショルドにより，評価データの算出をする．

前述の通り，まず，各ピアの類似度が比較スレッショルド以下ならば，power node の持つ正規化ローカル値 $s_{pj}(t)$ は偽造されていないとし，評価偽造ピアが power node に選ばれていないと判断する．そのとき，各ピアは power node の持つ正規化ローカル値を自身の評価データに取り入れ，式 2 により算出する．次に，各ピアの類似度が比較スレッショルド以上ならば，power node の持つ正規化ローカル値 $s_{pj}(t)$ は偽造されているとするため，評価偽造ピアが power node に選ばれていると判断する．そのときの評価データは以下のように算出する．

$$x_{ij}(t) = s_{ij}(t) \times v_i(t-1) \tag{7}$$

式 7 より，各ピア i の持つ正規化ローカル値 $s_{ij}(t)$ に一つ前のサイクルで算出した各ピア i 自身のグローバル値 $v_i(t-1)$ を重み付けて算出する．こうすることにより，評価偽造の影響を低減させる．

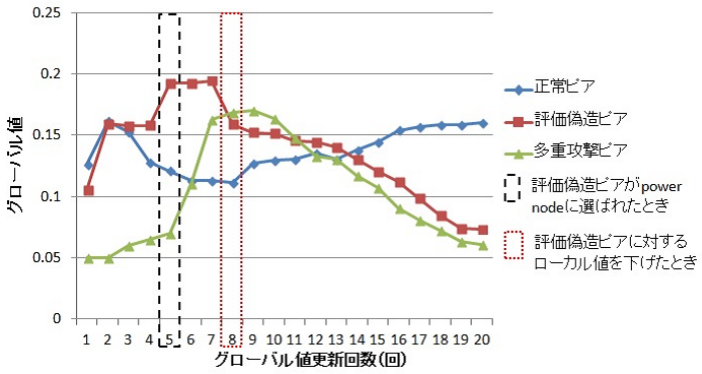

図 2 DIF-Trust におけるグローバル値の推移の例

3.3 評価偽造ピアに対するグローバル値の算出

power node に選ばれた評価偽造ピアを検知した後，その評価偽造ピアに対する評価値を低くしなければ，後に再び power node に選ばれてしまう可能性がある．それは，評価偽造ピアが悪意あるファイルを提供せず，正常なファイルを提供し，評価偽造ピア自身の他ピアからの評価値は低くならないからである．そこで，power node に選ばれた評価偽造ピアの検知後，その評価偽造ピアに対するローカル値を意図的に下げることでグローバル値が下げ，再び power node に選ばれる頻度を少なくする．

各ピア i は，power node に選ばれた評価偽造ピア p を検知した後の次のファイル交換において，自身の持つ評価偽造ピアに対するローカル値を意図的に下げる．このときのローカル値の算出を以下に示す．

$$r_{ip}(t) = r_{ip}(t-1) \times \eta \tag{8}$$

式 8 より，1 試行前にピア i が算出した評価偽造ピアに対するローカル値 $r_{ip}(t-1)$ に定数 η ($0 \leq \eta \leq 1$) を重み付けすることにより，グローバル値を下げる．

ここで，図 2 に，DIF-Trust における各ピアのグローバル値の推移の例を示す．この図は，正常ピアが評価偽造ピアに対するローカル値を下げたときの，正常ピア，評価偽造ピア，多重攻撃ピアのグローバル値の推移の例を表す．横軸がグローバル値更新回数，縦軸がグローバル値である．図 2 では，グローバル値更新回数が 8 回目のときに正常ピアが評価偽造ピアに対するローカル値を下げたとき，徐々に評価偽造ピアのグローバル値が下がる．その結果，評価偽造ピアが再び power node に選ばれなくなり，評価偽造の影響を低減でき，多重攻撃ピアのグローバル値も下がる．また，それに伴って，正常ピアのグローバル値が上がる．

4. シミュレーション結果

提案手法 DIF-Trust の有用性を示すために，既存手法における評価偽造ピアの影響や既存手法との比較評価を行う．本稿では，シミュレーションにより評価し，その結果を考察する．

表 1　シミュレーション条件

ネットワーク上の全ピア数 N	1000
悪意あるピアの割合 γ	0〜50 %
評価偽造ピア数：多重攻撃ピア数 γ_f ： γ_m	1 : 9
1 サイクルあたりの各ピアのファイル交換数 F	100
power node の割合 N_p	0.1
power node の評価値の重み付け値 α	0.3
類似度の重み付け値 β	0.5
評価偽造ピアに対する評価値の重み付け値 η	0.5
グローバル値更新頻度	100

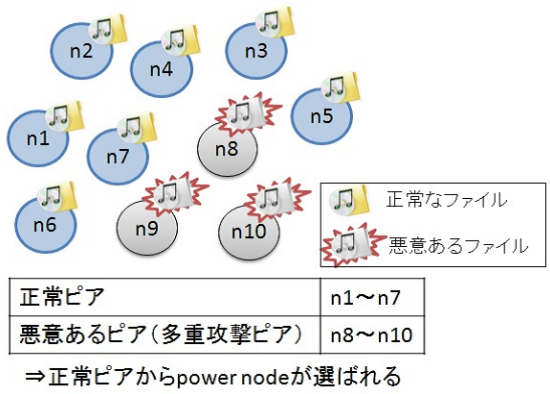

図 3　評価偽造ピアが存在しない場合のピアモデル

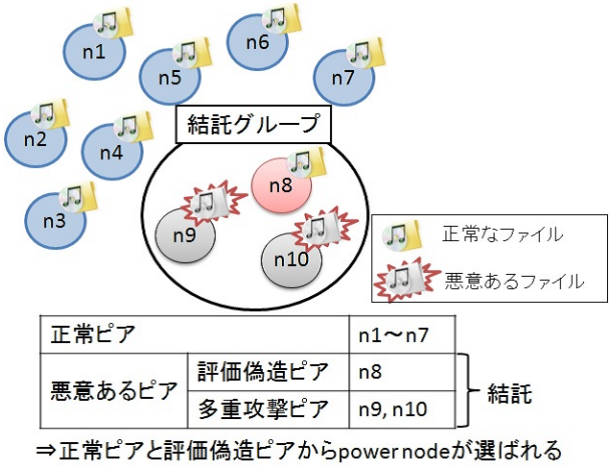

図 4　評価偽造ピアが存在する場合のピアモデル (結託)

4.1　シミュレーション条件

表 1 にシミュレーションで使用した条件を示す．本稿では，1000 ピアが参加する P2P ネットワークにおいて，正常ピアと悪意あるピアの両方が混在するものとする．各ピアは，ファイル交換を 100 回行い，そこから評価値を算出する．これを 1 サイクルとし，全ての評価結果は，100 サイクル行った結果の平均をとっている．

次に，ピアのモデルについて説明する．ピアは正常ピアと悪意あるピアの両方が存在し，悪意あるピアの中で 2 種類のピアが存在する．一つは評価偽造ピアであり，正常なファイルを提供するが，他ピアに対する評価を偽造する行動をとる．一方は多重攻撃ピアであり，悪意あるファイルを提供しかつ他ピアに対する評価も偽造する行動をとる．また，正常なピアが悪意あるファイルを提供する割合を 5 %とする．正常なピアでも意図せず悪意あるファイルを提供してしまうことを考慮している．逆に，悪意あるファイルを提供するピアがまれに正常ファイルを提供する割合も 5 %と考慮している．また評価の偽造は，以下の式のように評価値が偽造される．

$$r'_{ij}(t) = 1 - r_{ij}(t) \tag{9}$$

式 9 より，$r'_{ij}(t)$ は悪意あるピアにより偽造されたローカル値である．

ここで，図 3，4 より評価偽造ピアが存在しない場合と存在する場合のピアのモデルを表す．まず，図 3 は，ネットワークに評価偽造ピアが存在しない場合のピアのモデルを表す．これより，$n1$ 〜 $n7$ が正常ピアで，$n8$ 〜 $n10$ が悪意あるピア（多重攻撃ピア）である．power node は正常ピアの中から選ばれる．次に，図 4 は，ネットワークに評価偽造ピアが存在する場合のピアのモデルを表す．$n1, n2$ 〜 $n7$ が正常ピアで，$n8$ 〜 $n10$ が悪意あるピアである．このとき，悪意あるピアのモデルとして，評価偽造ピアと多重攻撃ピアの結託が想定される．これは，悪意あるピアの行動として，ネットワーク上に悪意あるファイルによる影響が最も大きくなると想定されるためである．悪意あるピアの中で結託することで，悪意あるピアは結託グループ内のピアの評価は高く，結託グループ以外のピアの評価は低く偽造するため，評価偽造ピアから power node が選ばれやすくなり，評価偽造の影響がより大きくなる．

評価項目は，下記項目についてシミュレーションを行った．

- 既存手法における評価偽造ピアによる影響
- 既存手法と提案手法のグローバル値の推移
- ファイル交換成功率の比較
- 既存手法と提案手法のオーバーヘッドの比較

ファイル交換成功率は，各ピアの全ファイル受信数のうちの正常なファイル受信数の割合であり，ファイル交換の安全性を示す指標である．また，提案手法導入における類似度と比較スレッショルドの算出により，提案手法とのオーバーヘッドによる比較評価も行う．ここで述べるオーバーヘッドとは，各ピアの評価データの集約回数を表す．

4.2　既存手法における評価偽造ピアによる影響

図 5 に既存手法 GossipTrust における評価偽造ピアの影響を示す．図 5 より，GossipTrust において評価偽造ピアが存在した場合，存在しない場合に比べてファイル交換成功率が低減している．評価偽造ピアが存在しない場合，悪意あるピアは多重攻撃ピアのみのため，多重攻撃ピアのグローバル値は下がる．そのため，power node は正常ピアから選ばれる．グローバル値算出の際に power node 持つ評価値の影響は大きいため，power node が正常ピアから

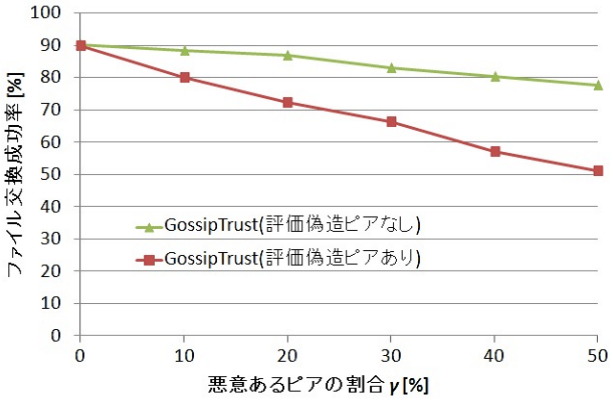

図 5　GossipTrust における評価偽造ピアの影響

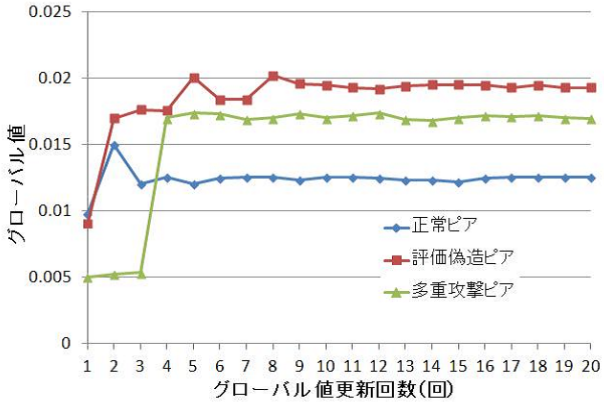

図 6　GossipTrust における各ピアのグローバル値の推移

選ばれることにより理論値に近いグローバル値を算出出来る．一方，評価偽造ピアが存在した場合，評価偽造ピアは悪意あるファイルを提供せずに評価偽造のみを行うため，評価偽造ピアのグローバル値は下がらず，評価偽造ピアが power node に選ばれやすくなる．そして評価偽造ピアは多重攻撃ピアと結託するため，評価偽造ピアによる影響が大きくなる．その結果，正常なピアは悪意あるファイルを交換してしまい，ファイル交換成功率が下がっていると考えられる．

4.3　各ピアのグローバル値の推移

図 6，図 7 に，GossipTrust における各ピアのグローバル値の推移と DIF-Trust における各ピアのグローバル値の推移を示す．図 6 より，グローバル値更新回数が 2 回目以降で評価偽造ピアのグローバル値が上がり，4 回目以降で多重攻撃ピアのグローバル値が上がり，逆に正常ピアのグローバル値が下がっている．GossipTrust において評価偽造ピアが存在したときに power node に選ばれやすくなり，グローバル値更新回数が 2 回目以降で power node に選ばれてしまう．その結果，評価偽造ピアが power node に選ばれた際の評価偽造の影響により，グローバル値更新回数が 4 回目以降で多重攻撃ピアのグローバル値が高くなり，正常ピアのグローバル値が下がってしまったと考えられる．

次に，図 7 より，グローバル値更新回数が 2 回目のときは評価偽造ピアのグローバル値は高いが，3 回目以降で評価偽造ピアのグローバル値が下がり，そのあと多重攻撃ピアのグローバル値も下がっている．このとき，逆に正常ピアのグローバル値が上がっている．また，10 回目以降で再び評価偽造ピアのグローバル値が高くなっているが，11 回目で下がり，それ以降繰り返しになっている．DIF-Trust により，評価偽造ピアが power node に選ばれていると検知した後，評価偽造ピアに対するローカル値を 3 回目以降で下げたことにより，評価偽造ピアのグローバル値が下がったと考えられる．そのため，3 回目から 9 回目は一時的に評価偽造ピアが power node に選ばれない．それによって

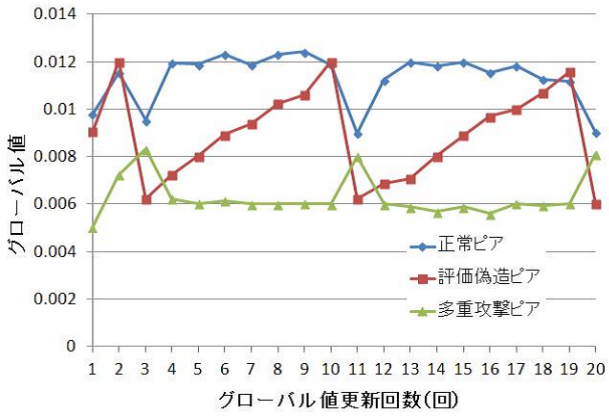

図 7　DIF-Trust における各ピアのグローバル値の推移

評価偽造の影響を低減でき，多重攻撃ピアのグローバル値は下がり，逆に正常ピアのグローバル値は上がったと考えられる．しかし，評価偽造ピアは正常なファイルを提供するため，次第にグローバル値は上がっていく．そのため再び 10 回目で power node に選ばれてしまうが，その都度検知し，ローカル値を下げることによってグローバル値が下がる．図 6 と比較すると，DIF-Trust の導入により，評価偽造ピアから power node に選ばれる頻度が少なくなった．それによって，評価偽造の影響を低減できる．

4.4　ファイル交換成功率

図 8，図 9 に，既存手法 GossipTrust と提案手法 DIF-Trust の比較をファイル交換成功率で示す．図 8 は悪意のあるピアの割合が増加した時のファイル交換成功率を表し，図 9 は，悪意あるピア数が一定の時の，評価偽造ピア数の変化に伴うファイル交換成功率を表す．

まず，図 8 より，提案手法 DIF-Trust の導入により，提案手法 GossipTrust よりも最大約 20 %のファイル交換成功率が向上している．DIF-Trust では，評価値の類似度により評価偽造ピアが power node に選ばれた場合の評価偽造を検知し，偽造された評価値を取り入れなくしたことにより評価偽造の影響を低減させている．また，power node

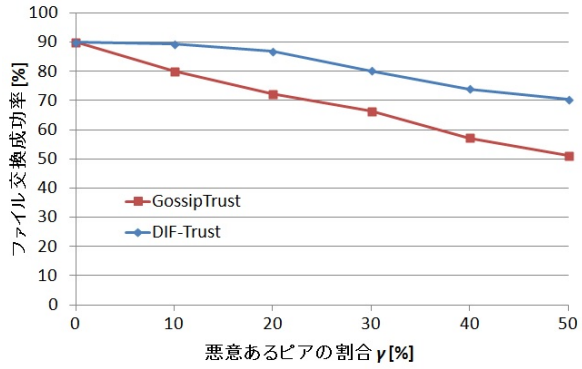

図 8　ファイル交換成功率

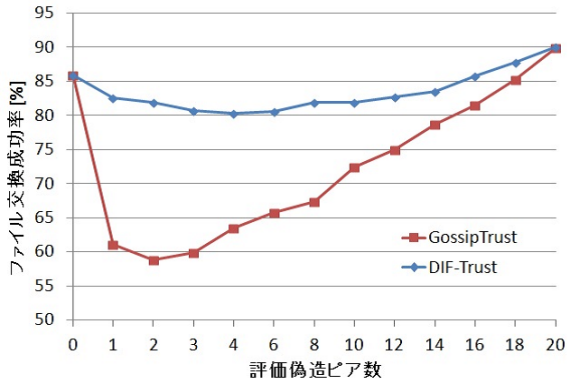

図 9　評価偽造ピア数の変化に伴うファイル交換成功率

に選ばれた評価偽造ピアに対する評価値を下げることにより，結託グループの悪意あるピアのグローバル値が下がり，再び power node に選ばれる頻度を少なくした．その結果，DIF-Trust では悪意あるピアとファイル交換をする可能性が低くなり，GossipTrust におけるネットワーク全体のファイル交換成功率の低減が抑制できたと考えられる．

次に，図 9 より，DIF-Trust の導入により，評価偽造ピア数の増加に対して常に 80 %以上のファイル交換成功率を維持している．ここで，評価偽造ピア数が増えれば増えるほど，多重攻撃ピア数は減っていく．そのため，悪意あるファイルを提供するピア数は減る．GossipTrust では，評価偽造ピア数が存在する限り，各ピアが評価偽造による影響を受けてしまい，結果としてネットワーク全体でのファイル交換成功率は低くなっている．しかし，DIF-Trust では，評価偽造ピア数の変化によらず評価の偽造を検知し，評価偽造の影響を低減できている．その結果，GossipTrust と比較して，ネットワーク全体でのファイル交換成功率は高く維持できている．

4.5　オーバーヘッドの比較

図 10 に，既存手法 GossipTrust と提案手法 DIF-Trust のオーバーヘッドの比較を表す．オーバーヘッドは，各ピアがグローバル値を算出する際の評価データの集約回数である．図 10 より，提案手法 DIF-Trust では，悪意あるピア

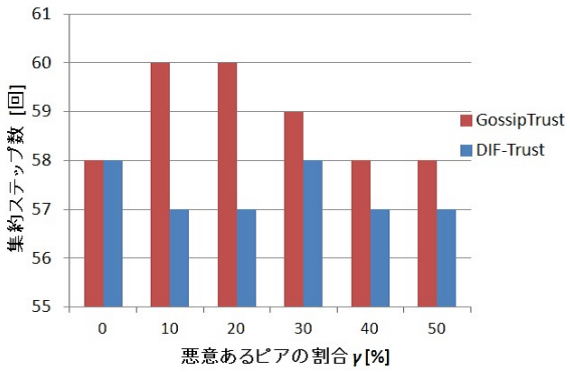

図 10　グローバル値算出のためのオーバーヘッド

の割合が多くなり，評価偽造の影響が大きくなったとしても，既存手法 GossipTrust よりも集約回数が増加しておらず，オーバーヘッドの増加の抑制ができていることが分かる．提案手法 DIF-Trust の導入により，評価偽造の影響を低減でき，さらに評価偽造ピアに対する評価値も下げたことで，本来悪意あるピアが持つ評価値の理論値に近い値を算出できたため，集約回数を抑えられたと考えられる．提案手法 DIF-Trust では，悪意あるピアの割合が増加しても常に既存手法 GossipTrust よりも少ない集約回数でグローバル値が算出出来ているため，グローバル値算出のオーバーヘッドの増加抑制を確認できた．

5.　おわりに

本稿では，各ピアと power node との評価値の類似度と比較スレッショルドを用いて，評価偽造ピアが power node に選ばれた際の評価の偽造を検知する評価集約手法 DIF-Trust を提案した．DIF-Trust では，各ピアの持つ評価データをピア間で交換する際に，各ピアの持つローカル値と power node の持つローカル値の類似度と，比較スレッショルドを動的に算出する．類似度が比較スレッショルド以下の場合，評価偽造ピアが power node に選ばれていると判断する．そして，その power node の持つローカル値を各ピアの評価データに取り入れず，また，グローバル値を下げることで power node に再度選ばれる確率を下げる．こうすることで，評価偽造ピアが power node に選ばれた際の評価偽造の影響を低減し，悪意あるピアとファイル交換する可能性が低くなり，その結果，ネットワーク全体でのファイル交換成功率の低減を抑制する．

さらに，本提案手法をシミュレーションにより既存手法との比較評価を行った．結果として，評価偽造ピアによる評価偽造の影響を低減でき，悪意あるピアの割合を変化させたとき，既存手法と比べネットワーク全体のファイル交換成功率を最大約 23 %改善した．また，評価偽造ピア数が増加したとき，ネットワーク全体のファイル交換成功率を 80 %以上の維持を達成した．

参考文献

[1] J. Erman, A. Mahanti, M. Arlitt, and C. Williamson, “Identifying and discriminating between web and peer-to-peer traffic in the network core,” *16th international conference on World Wide Web ACM New York, NY, USA*, May 2007.

[2] M. Hefeeda and O. Saleh, “Traffic modeling and proportional partial caching for peer-to-peer systems,” *IEEE/ACM TON archive Volume 16 Issue 6 2008*, Dec 2008.

[3] J. Meserve, ”P2P traffic still dominates the Net,” Network World, Aug 2005.

[4] N. Christin, A. Weigend, and J. Chuang, ”Content availability, pollution and poisoning in file sharing peer-to-peer networks,” *ACM Conf. on E-Commerce 2005*, Jun 2005.

[5] J. Mao, Y. Cui, j. Huang, and J. Zhang, ”Modeling and Analysis of Resource’s Load-Scale in P2P Network,” *CMC 2009*, Jan 2009.

[6] R. Zhou, and K. Hwang, ”PowerTrust: A Robust and Scalable Reputation System for Trusted P2P Computing”, *IEEE Trans. on Parallel and Distributed Systems, pp.460-473*, April 2007.

[7] R. Zhou and K. Hwang, ”Gossip-based reputation aggregation for unstructured peer-to-peer networks,” *IEEE International. on Parallel and Distributed Processing Symposium*, Mar 2007.

[8] R. Zhou, K. Hwang, and M. Cai, ”GossipTrust for Fast Reputation Aggregation in Peer-to-Peer Networks,” *IEEE Trans. on Knowledge and Data Engineering, vol. 20, Issue. 9, pp. 1282-1295*, 2008.

[9] Yajima, T.; Matsumoto, A.; Shigeno, H., ”PTrust: Provisional Value based trust for reputation aggregation in peer-to-peer networks,” *1st International Symposium on Access Spaces (IEEE-ISAS 2011), pp. 180-185*, June 2011.

[10] Takeda, S.; Ushikubo, H.; Shigeno, H., ”SPTrust: Reputation Aggregation Method Based on Similarity to Reputation Scores of Power Nodes in Unstructured P2P Networks,” *Eighth Inter National Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA2013)*, October 2013.