信頼連鎖による P2P コンテンツ流通システムの提案と評価

Evaluation of P2P Contents Distribution System with Cryptographic Trust Chains

伊藤 洋輔♥ 河野 浩之♦

Yosuke ITO Hiroyuki KAWANO

P2P ネットワークにおけるコンテンツ流通の安全性や信頼性の確保が重要な課題となっている．本論文では，P2P 環境下の信頼性を保証するために，システム内の各ピアの信頼するホストの連鎖を用いるアルゴリズムを提案する．加えて，提案アルゴリズムによりシステム上のピアの公平性が保証できることを，各ピアのインセンティブと評判(reputation)に基づく格差サービスの評価モデルにより簡単に示す．

In P2P network, safety and reliability of the contents distribution are becoming important. In this paper, we propose a novel P2P reputation algorithm based on trust chain mechanism to guarantee good reliability. By using our algorithm, we construct trust networks of peers by using the cryptographic trust chains. Furthermore, we shortly evaluate performance model of our mechanism, which provides fairness by differential-based service depending on amount of incentive and reputation values.

1. はじめに

広帯域な高速通信基盤が整備されるにつれて，ネットワーク上に分散する情報源の効率的な統合管理技術の重要性が高まっている．中でも，P2Pコンテンツ流通システムは，接続ホスト数の拡張性の高さ，耐故障性の高いシステム構築が可能性の点から，精力的に研究が進められている[1,2]．しかし，中央管理サーバをもたないP2Pシステムにおける匿名性の高いファイル共有では，コンテンツ流通の信頼性に関わるさまざまな課題がある[3,4]．

一方，Webシステムでは，未知の取引相手に対する信頼性を高め脅威を減らす方法として，認証局(CA)による本人性確認技術が用いられている．例えば，eBayのオンライン取引では，認証局と評判(reputation)に基づく信頼性評価が重要な役割を果たす．その他，PGP(Pretty Good Privacy)による信頼の輪が，電子メールシステムで利用されており，信頼性を高めるネットワーク技術は着実に浸透しつつある．

もっとも，この種のシステムの信頼性は，システム形態，システム可用性，ファイルやリソースに対するアクセス制御，提供されたデータ自身の信頼性，取引相手の本人性確認など様々な要素技術と関係する[4,5]．加えて，社会制度に関わる要素も，信頼の形成に大きな影響を与える．

♥ 学生会員 南山大学大学院数理情報研究科博士前期課程修了 m05mm010@msie.nanzan-u.ac.jp

♦ 正会員 南山大学数理情報学部情報通信学科 kawano@it.nanzan-u.ac.jp

そこで，本研究では，P2Pの本質である分散制御に注意しながら，取引相手ならびにコンテンツの状態に基づく各ピアから信頼するピアへの複合的な信頼連鎖に基づく信頼性保証アルゴリズムを提案する．分散型のコンテンツ配布・管理を円滑に行いながら，悪意ピアの盗聴や改ざんなどの脅威を防ぐため，公開鍵を利用した取引相手の信頼性確認，第三者からの公開鍵に対する署名を用いる．また，信頼性評価アルゴリズムの性能を簡単な評価モデルにより示す．

2. ピアの信頼性に関する関連研究

ウィルスなどに汚染されたり，改ざんや盗聴などのリスク回避，さらに，選好基準[1]に合致しないコンテンツの受信拒否のために，P2Pコンテンツ流通は高い信頼性が求められる．

表１に，通信相手のプロファイル提示，他ピアによる推薦に基づく信頼形成，コミュニティ内の評判に基づく信頼性評価など，P2P 環境下の信頼性評価手法を示す．特に，評判に基づく信頼性評価手法は，社会システムにおける信頼形成に密接に関係するため，評判値の単純平均，確率モデルの導入，信頼の輪に基づく評価，システム内の高次構造に基づく評価など多数の研究がある．

表 1 信頼評価手法

Table 1 Trust evaluation methods

手法		方法
プロファイル情報		ホスト自身の提示情報に基づく[6]
推薦		他ホストへの推薦情報を利用[3]
評判	単純平均	過去の振舞いへの評判値の平均化
	確率モデル	ベイズモデルによる確率的構造の利用[7]
	信頼の輪	信頼できるホストの連鎖を利用[8]
	フローモデル	システム全体の評判の流れを利用[9]

表１の「プロファイル情報」による評価は，社会的に信用された第三者による保証がない状態での信頼性確保が困難であり，コミュニティ内の全ピアに対する集中型の認証局を必要とする．また，中央サーバの必要性は P2P の分散制御の特質を失う問題でもある．「推薦」に基づく手法も提供者の信頼性を必要とし，同様の問題を引き起こす．次に，最近注目されている「評判」に基づく信頼性評価手法として，例えば，過去のピアの振舞いの平均値やベイズモデルの応用が提案されている[5]．eBay のオンライン取引は集中型システムであり，P2P システムへの応用には工夫を要するが，Web 上の評判に基づく信頼モデルの好例である．また，信頼の輪を用いる手法として対象の信頼情報の伝播時に，信頼性の低い構造を同時に伝播させることが考えられている[8]．さらに，過去の履歴によるローカルな信頼値とシステム中の評判の構造を利用し，各ピアのローカルな信頼値を基にした固有値計算を行うグローバルな信頼値計算手法がある[9]．取引の成功・失敗以外の複数要因に注目し，フィードバック結果，トランザクション量，フィードバックの信頼性，トランザクション背景，コミュニティ背景の 5 種に基づく信頼評価方法が提案されている[10]．その他，信頼値問合せピアと信頼値情報を保持するピアの両方の匿名性保持のため，多数の異なる公開鍵とネットワーク参加に用いるブートストラップサーバの利用なども研究されている．

[1] 本稿では，利用者のコンテンツに対する条件，例えば，興味，コンテンツ品質，メディアタイプ，ファイル転送待ち時間等を選好基準とする．

しかしながら，様々な信頼評価手法では，保持する信頼情報のサイズや，P2P のネットワーク接続の特徴である参加率の変動を考慮しておらず，実際の P2P 環境下を考慮した評価とは言い難い．そこで，本研究では，P2P システム特有のネットワーク参加率の変化による信頼の連鎖構造への影響を考慮し，表 1 における信頼の輪の構成手法の拡張を試みる．以下，各ピアが保持する信頼情報のサイズや，ネットワーク参加率を考慮したアルゴリズムを提案し，信頼性保証の向上などを考察する．

3. 信頼の連鎖機能の提案

3.1 公開鍵配布モデル

公開鍵暗号は，秘密鍵を保持する相手への安全な情報提供を可能とするが，互いの公開鍵を確実に手渡す必要性があり，公開鍵の入手者はその鍵の作成者の本人性を検証しなければならない．そこで，公開鍵配布方法として，PKI(Public Key Infrastructure)や PGP が用いられる(表 2)．また，本研究の P2P コンテンツ流通でも，認証局を必要としない分散制御に基づくコンテンツ管理が重要であるため，信頼の連鎖を用いる公開鍵配布モデル利用が妥当であると考えられる．

表 2 PGP と PKI の比較
Table 2 Difference between PGP and PKI

	PKI	PGP
信頼モデル	信頼の輪	第三者信頼
信頼の起点	個人	認証局
信頼の連鎖	個人	認証局
公開鍵の信憑性	個人責任	認証局による保証

3.2 システム概要と連鎖を用いた評判値導出方法

我々が提案する信頼の連鎖構造を用いたコンテンツ流通システムの概要を図 1 に示す．コンテンツ要求ピア A は，システム参加ピアに対し，目的サービスの提供が可能なピアを問合せる．その応答を用いて，コンテンツ提供ピア B を取引ピアとして選択しサービス要求を行う．このとき，選好基準を満たすコンテンツ入手の信頼性を高め，盗聴や改ざんの脅威を回避するために，ピアの公開鍵の入手と，公開鍵に施された署名に基づく信頼連鎖の検証するアルゴリズムを提案する．

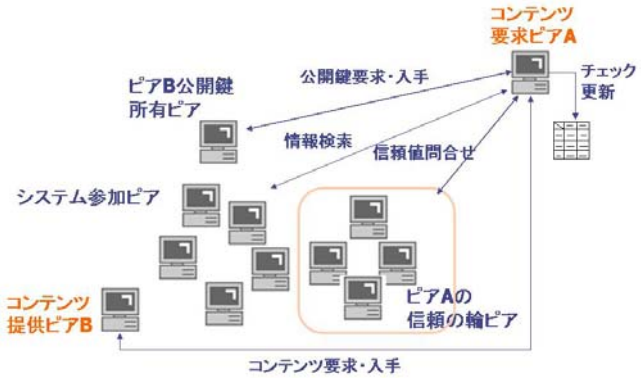

図 1 信頼の連鎖を考慮したコンテンツ流通システム
Fig.1 Contents distribution system with trust chain

すなわち，サービス提供ピア B は，過去にピア A から提供されたサービス量情報や既に自身が保持しているピア A に対する評判情報，後述する信頼の連鎖構造を用いて求めた評判を利用し，ピア A に対するサービス提供量を決定し，サービスを提供する．また，ピア B からサービスを入手したピア A は，今回のサービス情報を以降サービス提供のために記録し，サービス結果からピア B に対する評判を更新する．なお，評判値を管理するテーブルサイズに制限があるものとし，LRU に基づいて最も古い評判値情報を削除し，対応する公開鍵を削除することにする．

次に，信頼の連鎖構造を用いた評判値導出方法を示す．図 2 は，あるピアが未知のピアと取引を行うために用いる評判の導出例であり，説明番号は図 2 に対応する．問合せ元のピアは，対象ピアに至る信頼の連鎖構造を検証するため，(1) 自身が直接信頼する全ピアに対し，対象ピアの評判問合せを行う．評判問合せメッセージを受け取ったピアは，(2) 自身の信頼するピア中に対象ピアが存在しなければ自身が信頼する全ピアに対して再帰的に評判問合せを行う．(3) (4) 対象ピアが存在すれば対象の評判値情報，経由したピアの評判値情報を追加し，問合せメッセージ転送ピアへと返送する．

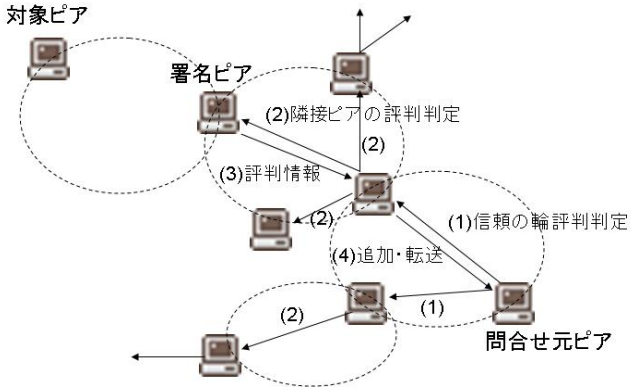

図 2 信頼の連鎖を用いた評判導出例
Fig.2 Example of finding trust chain

以上の処理を繰り返し行うことで，問合せピアは対象ピアに至る複数の信頼の連鎖構造情報を入手する．その後，問合せピアはあらかじめ保持している評判値，入手した信頼の連鎖情報に基づいて対象ピアの評判値を求める．(1)式により，ピア i からピア j に対する評判値を与える．

$$R_{ij}^{P}(t) = \max(m * R_{ik}^{P}(t) * chainR_{kj}^{P}(t), R_{ij}^{P}(t-1)) \quad (1)$$

ここで，$chainR_{ij}^{P}(t)$ は評判問合せにより求めた i のピア j に対する信頼値である．(1)式は，ピア i からピア j に対する評判値を求める信頼の連鎖情報を用い，ピア j の直前ピア k に対する評判値，ピア k のピア j に対する評判値，自身からの信頼の連鎖数に応じた係数の積である．なお，ピア i からピア j に対する評判値を既に保持する場合，大きい値を新たなピア評判値とする．この式を再帰的に適用し，自身からコンテンツ提供ピアまでの信頼の連鎖構造を利用した評判値計算を実行する．複数の信頼の連鎖が存在する場合，対象ピアに至る評判値の最大値に基づいて求め，ピア A における $chainR_{AB}^{K}(t)$ は，ピア B の公開鍵に署名したピアの評判値の最大値となる．複数の連鎖構造における初期評判値計算の中で最大値を用いることにより，大量の連鎖情報による不必要な初期評判値の低下を防ぐ．

なお，新規にネットワークに参加した際，評判値テーブル中に情報を持っていないことがあるため，このような場合は，あらかじめ信頼可能であると知られているピアや P2P ネットワークでの隣接ピア，隣接ピアの評判値テーブルを利用するなど，別の方法を必要とする[9].

3.3 サービス入手ピアの選択

システムにおける公平性を確保するためには，信頼できるピアからサービスを入手するだけでなく，システム中におけるピアの利己的な振舞いを抑制する方法を導入する必要がある．このとき，P2P システム上での適用が比較的容易な格差サービスにより，ピアの協調参加を促すインセンティブとする[11]．格差サービスはピアがシステムに対して提供した貢献量に応じて入手サービス量が変化する機構である．

これらを考慮し，サービスを入手するピアの選択戦略について，過去の対象へのサービス量と，対象の評判を用い，確率的に選択する．時刻 t にピア i がピア j を取引相手として選択する確率 $P_{ij}(t)$ を求める(2)式を与える．

$$S_{ij}(t) = k * \frac{u_{ij}(t)}{\max(u_j(t))} + (1-k) * R_{ij}^{P}(t)$$

$$P_{ij}(t) = \frac{S_{ij}(t)}{\sum_j S_{ij}(t)} \qquad (2)$$

ここで，k は過去の取引量と取引相手の評判における重みを決定する変数であり，$0 \le k \le 1$ である．また，$u_{ij}(t)$ はピア j によって提供されたサービス量，$\max(u_j(t))$ はサービス要求に対して応答をしてきたピアにおける $u_{ij}(t)$ の最大値であり，$\sum_j S_{ij}(t)$ は要求に応答したピアにおける $S_{ij}(t)$ の和である．

(2)式を用いて，入手先のピアを確率的に選択する．その結果，特定ピアからのみサービスを入手することがなくなり，広範囲のピアと取引を行う機会を与え，スケーラビリティを高めることができる．

3.4 信頼値更新と公開鍵に対する署名

履歴を反映し次回のサービス提供につなげるため，サービス授受を行ったピアはサービス結果にともない対象ピアの評判値を更新する．評判値更新の判断基準を表 3 にまとめる．

評判値の増加に関して，サービス要求ピアでは今回の入手サービス量 $d_{ij}(t)$ が現在まで自身が対象ピアに提供したサービス量 $u_{ij}(t)$ より少しでも多い場合とする．また，自身の限界サービス入手容量のサービスを入手できた場合も増加させる．一方，サービス提供ピアではサービス提供によって対象ピアの評判が上昇することはない．次に，サービス要求ピアにおける評判値を下落させる要因として偽サービスの入手が挙げられる．また，過去に自身が提供したサービス量よりも少ない量が提供された際，相手の限界サービス提供容量でない場合についても同様に評判値を減少させる．サービス提供ピアについては，サービスを入手することが困難なピアから何度もサービス要求が行われる場合に減少させる．最後に，サービス要求ピアでは自身が提供したサービス量と同量のサービスを入手したとしても，自身が提供した量は返してくるのが当然であるため，評判値は変化させないものとする．

表 3 要求・提供ピアの評判値更新判断基準
Table 3 Criteria for reconfiguring reputation value

	増加	変化なし	減少
要求ピア	$d_{ij}(t) > u_{ij}(t)$ $d_{ij}(t) = D_{\max}$	$d_{ij}(t) = u_{ij}(t)$ $d_{ij}(t) = U_{\max}$	$d_{ij}(t) < u_{ij}(t)$ 選好基準を満たさないサービス
提供ピア	—	—	$d_{ji}(t) < 0$

次に，(3)式～(6)式で評判値更新式を与える．ここで，(a, b, c, d) はサービス結果に伴い評判値更新率を決定する任意の値，(K, L, M, N) は[0, 1]の値を取る評判値の正規化パラメータ，過去の通信成功・失敗の連続回数 x である．

評判値増加

$$R_{ij}^{K}(t+1) = R_{ij}^{K}(t) + Ka^{x} \qquad (3)$$

$$R_{ij}^{P}(t+1) = R_{ij}^{P}(t) + Lb \qquad (4)$$

評判値減少

$$R_{ij}^{K}(t+1) = R_{ij}^{K}(t) - Mc^{x} \qquad (5)$$

$$R_{ij}^{P}(t+1) = R_{ij}^{P}(t) + Nd^{x} \qquad (6)$$

ここで，評判は直近の振舞いを反映することの必要性により連続回履歴に基づき更新する一方，ピアに対する評判は徐々に確立させる必要性により，取引成功時に評判値を一定量増加する．また，取引失敗によるサービス入手者のコストを考慮し，評判値は取引成功時の上昇値に比べ取引失敗時の減少値を大きく取りペナルティを与える．

なお，取引失敗の原因が特定可能である場合は，その原因である評判値のみを更新するが，特定が不可能であった場合は，どちらの評判値も更新する必要がある．

4. 性能評価

前章で提案した信頼の連鎖構造を用いたアルゴリズムによるサービス入手ピアの選択により，悪意ピアとの取引抑制が可能なことを示す．また，ピアから提供されるサービス量の動的変化に対し，供給するサービス量を柔軟に対応させる格差サービスに用いるパラメータは，[12]に基づいて与える．

最大信頼連鎖数を 6，評判値 0.97 以上の 1,000 ピアに対して評判問合せを評価する．初期信頼ネットワークはランダムなピア間で形成し，悪意ピア間で共謀を行うとし，悪意ピアでは通常ピアの信頼値を 0，悪意ピア同士の評判値を 1 に設定する．また，通常ピアが提供可能なコンテンツ種別には制限を与え，悪意ピアは全コンテンツの提供を試みるとする．すなわち，通常ピアは，適切でないコンテンツを確率的に提供するとし，95%の確率で適切なコンテンツを提供する．他方，悪意ピアは，必ず偽コンテンツを提供するとする．ピア評判値は，通信成功時に $R^{P}(t)+0.02$，通信失敗時に $R^{P}(t)-0.01*10^{x}$ で更新する．また，取引可能なピアの内，実際に取引するピアを選択する方法は，取引可能なピアの評判値に基づいて決定する．このとき，システム中の悪意ピアの割合を 1%から 10%まで変更し，システム内の通常のピアがコ

ンテンツ要求を行うことを 500,000 回繰り返した際に，システム中のピアと悪意ピアとの 5,000 回毎における取引回数は図 3 で示すグラフのように変化する．

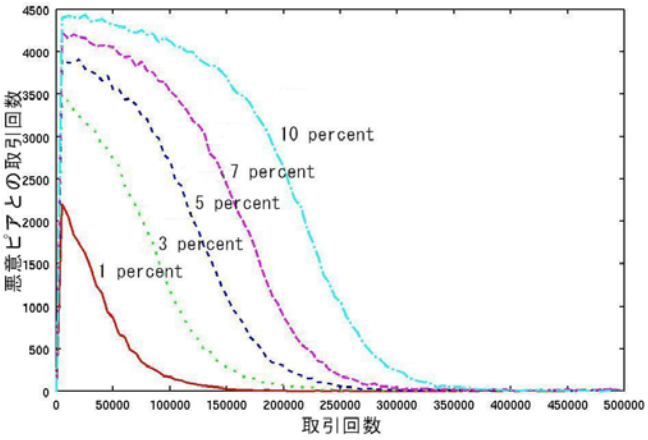

図 3　悪意ピアとの取引回数の変化
Fig.3 Transaction times from malicious peers

グラフの初期状態においては，任意のピア間にランダムな信頼ネットワークを形成するため，通常ピアは悪意ピアを認識できない．そのため，悪意ピアに対する取引回数が取引開始直後に急増している．しかし，悪意ピアの割合に関わらず，信頼の連鎖構造が徐々に確立されるにしたがい，悪意ピアとの取引回数が減少する．そして，取引回数の増加につれ，最終的に信頼の連鎖構造が完成すると，全ての通常ピアにおいて悪意ピアに対する連鎖構造を排除するため，悪意ピアとの取引がなくなる．その結果，悪意ピアをネットワークから締め出すことが可能となり，本研究で提案した信頼の連鎖構造を用いた評判問合せが有効に動作していることが明らかになった．

5. むすび

本研究では，P2P ネットワーク環境下における情報資源の流通を行う上で重要な課題となるコンテンツ流通の信頼性に焦点を当てた．そして，各ピアから信頼するピアへの多重の信頼の連鎖構造に着目し，公開鍵暗号と鍵に対する署名を利用した評判値計算アルゴリズムを提案した．さらに，公平性を保証するため，システム貢献量とピアの評判にしたがいサービス提供を行う格差サービスの導入を行った．また，シミュレーション実験の結果，悪意ピアとの取引は信頼の連鎖構造が確立されるにつれ減少することを明らかにした．

今後，複数の信頼性向上技術の融合，攻撃を想定したシミュレーション実験など，信頼性要因に対する幅広い評価を必要とする．また，信頼性低下や通信障害など失敗時の原因に応じた信頼値更新を行うアルゴリズム拡張も必要とする．

[謝辞]

本稿は，文部省科学研究費(19500098)ならびに「2007 年度南山大学パッヘ研究奨励金」(Pache Research Subsidy) I-A-2 の研究支援を受けている．また，田島道彦君(卒業生)との研究成果を発展させたものである．

[文献]

[1] 伊藤洋輔，河野浩之: “信頼の連鎖機能を用いたピアコンテンツ流通システム”，データベースと Web 情報システムに関するシンポジウム, pp.133-140 (2005).
[2] 中辻真，川原稔，河野浩之: “トピック主導型 P2P 情報検索システムの提案と評価”，電子情報通信学会論文誌, vol.J87-D1, no.2, pp.126-136 (2004).
[3] Chopra, K. and Wallace, W.: “Trust in Electronic Environments”, Proceedings of 36th Annual Hawaii International Conference on System Sciences, pp.331-340 (2003).
[4] Daswani, N., Garcia-Molina, H., and Yang, B.: “Open Problems in Data-Sharing Peer-to-Peer Systems”, Proceedings of the 9th International Conference on Database Theory, pp.1-15 (2003).
[5] Josang, A., Ismail, R., and Boyd, C.: “A Survey of Trust and Reputation Systems for Online Service Provision”, Decision Support Systems, vol.43, issue 2, pp.618-644 (2007).
[6] Stakhanova, N., Basu, S., Wong, J., and Stakhanov, O.: “Trust Framework for P2P Networks using Peer-Profile based Anomaly Technique”, Proceedings of the 2nd International Workshop on Security in Distributed Computing Systems, pp.203-209 (2005).
[7] Withby, A., Josang, A., and Indulska, J.: “Filtering Out Unfair Ratings in Bayesian reputation Systems”, Proceedings of the 3rd International Joint Conference on Autonomous Agents and Multi Agent Systems (2004).
[8] Guha, R., Kumar, R., Raghavan, P., and Tomkins, A.: “Propagation of Trust and Distrust”, Proceedings of the 13th International Conference on World Wide Web, pp.403-412 (2004).
[9] Kamvar, S., Schlosser, M., and Garcia-Molina, H.: “The EigenTrust Algorithm for Reputation Management in P2P Networks”, Proceedings of the 12th International Conference on World Wide Web, pp.640-651 (2003).
[10] Xiong, L. and Liu, L. “PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities”, IEEE Transaction on Knowledge and Data Engeneering, vol.16, no.7, pp.843-857 (2004).
[11] Buragohain, C., Agrawal, D., and Suri, S.: “A Game Theoretic Framework for Incentives in P2P Systems”, Proceedings of the 3rd International IEEE Conference on Peer-to-Peer Computing, pp.48-56 (2003).
[12] 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 第 18 回データ工学ワークショップ (2007).

伊藤 洋輔　Yosuke ITO
1982 年 11 月 24 日生．2005 年 3 月南山大学数理情報学部情報通信学科卒業．2007 年 4 月 4 日 3 月，同大学院数字情報研究科数理情報専攻修了．P2P の研究に興味をもつ．

河野 浩之　Hiroyuki KAWANO
1962 年 6 月 27 日生．昭 60 京都大・工・数理卒．平 2 年 4 月同大学工学部数理工学教室助手．平 9 年同大学院工学研究科応用システム科学専攻助教授．平 16 年 4 月南山大学数理情報学部情報通信学科教授，現在に至る．工博．情報伝送システムの研究に興味を持つ．ACM，IEEE，AAAI，電子情報通信学会，情報処理学会，人工知能学会等会員．