信頼の連鎖機能を用いた高信頼性なピアコンテンツ共有システム

2000MT090 田島 道彦　　2001MT041 伊藤 洋輔
指導教員　河野 浩之

1　はじめに

従来のクライアント/サーバモデル (以下 C/S) のネットワークではサーバがサービスを提供する．それゆえ，サーバの信頼性を高めることがネットワークの信頼性を高めることになる．一方，ピアツーピア (以下 P2P) は全てのピアが直接相手と接続して通信し，対等にサービスを提供し合うことでサーバに集中する負荷を分散することができる [1]．しかし，そのことでウィルスや不正アクセスなどのセキュリティ問題が以前より重要視されることとなった．P2P では中央集中型ではなく分散型でのネットワークのセキュリティが求められる．

本研究では P2P コンテンツ共有におけるセキュリティを，既存の C/S で用いられるセキュリティの適用の可能性を考えつつ，JXTA 上で実現する方法を示す．

2　認証モデルと P2P での問題点

2.1　P2P での脅威

セキュリティの問題は大きく以下の 2 種類に分類することができる．

- 能動的ネットワーク攻撃：攻撃者が積極的に仕掛けてくる攻撃．なりすまし，man-in-the-middle 攻撃，反射攻撃など
- 受動的ネットワーク攻撃：攻撃者が直接的に仕掛けてくるのではなく主に盗聴によって情報を手に入れるもの

通常，受動的攻撃は能動的攻撃の前兆となるので先にこちらを注意する必要がある．この盗聴は通信の暗号化によって防ぐことができる．

2.2　公開鍵配布のモデル

公開鍵を用いて通信することによって特定の秘密鍵を保持している相手のみに情報を公開することが出来るようになる．しかしそれには送信者の公開鍵を相手に手渡す必要がある．また，受信者はその鍵がはたして本当に通信したい相手なのかどうかを証明する必要がある．その証明に対し，誰を信頼するかということによって直接信頼モデル，間接信頼モデルに分けることが出来る．

公開鍵の配布の方法としてそれぞれ暗号化方式で知られている Pretty Good Privacy(PGP)，Public Key Infrastructure(PKI) を例にし，その特徴を表 1 で示す [2]．

本研究では P2P ネットワークの本来の形はピアだけで独立して成り立っているもので，認証局といった中央化したものの存在は取り除くものと考える．ゆえに直接信頼モデルを採用して公開鍵を配布するものとする．

表 1　PGP と PKI の違い

\	PGP	PKI
信頼モデル	直接	間接 (第三者信頼)
信頼の基点	個人	認証者
信頼の連鎖	個人責任	認証者
公開鍵の信憑性	個人責任	認証者による保証
拡張性	拡張しづらい	拡張が容易

3　P2P ファイル共有を実現するためのツール

この研究では JXTA 上でセキュリティを実現するための手段と方法を示す．

JXTA は Sun Microsystems で開発された P2P アプリケーションを作成するための標準プロトコル群である [3]．

ピア間で交換されるデータの基本単位であるアドバタイズメントは XML ドキュメントである．アドバタイズメントには，利用可能なサービス，ピア，ピアグループ，パイプ，エンドポイントに関する情報が記載されている．JXTA でピアや各種のリソースを探したい場合は，目的のピアやリソースが記載されたアドバタイズメントを探せばよい．

JXTA プロトコルは，発見，組織化，監視，ピア間の通信を行うための 6 つのプロトコルから成る．

4　直接信頼モデルにおける流れ

4.1　システム概要

図 1 は本研究で提案するシステムの概要図である．図中の番号は処理の流れである．コンテンツをピア間で共有するために，それぞれのピアは公開鍵を入手し，自身の信頼できるピアに対して公開鍵の信頼性を検証するために問合せを行う．

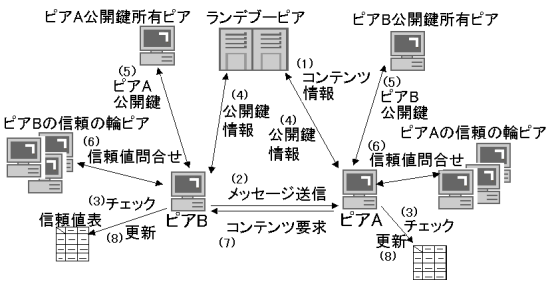

図 1　システム概要図

4.2 メッセージ形式

コンテンツ共有のための JXTA メッセージとして，共有要求メッセージ，共有応答メッセージを定義する．

- 共有要求メッセージ
  コンテンツ保持ピアにコンテンツを要求するためのメッセージ，公開鍵を入手するのにも使用
- 共有応答メッセージ
  コンテンツ要求ピアに公開鍵またはコンテンツを渡すためのメッセージ

信頼値入手のための JXTA メッセージとして，信頼値問合せメッセージ，信頼値応答メッセージを定義する．

- 信頼値問合せメッセージ
  信頼の輪の連鎖上に存在するピアに公開鍵署名ピア，コンテンツ保持ピアを問合せるためのメッセージ
- 信頼値応答メッセージ
  信頼の輪の連鎖上で公開鍵署名ピア，コンテンツ保持ピアまでに存在するピア間の信頼値を返すメッセージ

4.3 信頼値問合せの流れ

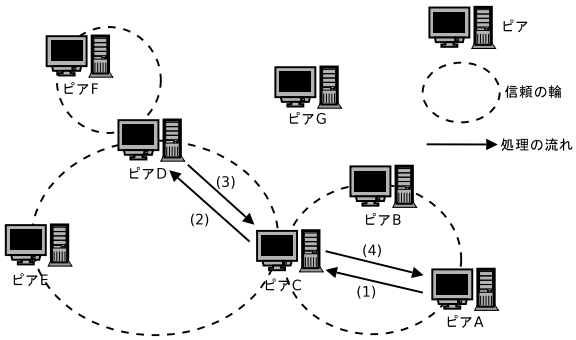

図 2　具体的なネットワーク上での処理の流れ

図 2 のネットワークで，ピア A はピア F に対して，共有要求メッセージを出したものとする．またピア A はピア D の署名がされたピア F の公開鍵を入手したものとする．図中の番号は処理の流れである．(1) ピア A はピア F の公開鍵が確かにピア F が作成した鍵であることを検証するために，自身の信頼の輪の全てのピアに問合せる．(2) 問合せを受けたピアは自身の信頼の輪の中に署名者 D がいればそのピアに，いなければ信頼の輪の全てのピアに再帰的に問合せる．(3) 署名者のもとに問合せが届いたら，署名ピア D の鍵の作成ピア F に対する信頼値を問合せ先 C に返す．(4) ピア C はピア D から受け取った情報にピア C のピア D に対する信頼値を追加して，ピア A に返す．ピア A は入手した情報を元にピア F の鍵の信頼値を計算し，その鍵で通信を行うかどうかを決定する．公開鍵の信頼値が高いとき，または署名ピアのピア信頼値が高いときはピア S は信頼値の問合せをせずに，公開鍵を使用できることとする．

4.4 信頼値テーブル

信頼値テーブルは，表 2 で示す様にピア ID，ピア信頼値，公開鍵信頼値の要素を持つ．信頼値は小数で保持し，信頼値の上限は 1，下限は 0 とする．信頼値テーブルのサイズは限られており，新たに通信相手の公開鍵を入手した際に，署名ピアの信頼値が信頼値テーブルに存在しない，また，存在しても信頼性が低い可能性がある．そのとき信頼値問合せを行い，公開鍵信頼値を求め，信頼性を確認した後に，信頼値テーブルの更新をする．その際，信頼値テーブルのサイズが限界になり，新たに要素を追加するときには，信頼値テーブルにおいて LRU アルゴリズム (Least Recently Used algorithm) を使用し，最も古いピア ID，ピア信頼値，公開鍵信頼値を削除すると共に対応する公開鍵を破棄する．

表 2　ピアが所有する信頼値テーブルの例

ピア ID	ピア信頼値	公開鍵信頼値
A	0.90	1.00
B	0.80	0.98
…		

4.5 信頼値計算

ここでピア A からピア B に対する信頼値を $peer\_conf(A,B)$ と定義し，ピア A のピア B の公開鍵に対する信頼値を $key\_conf(A,B)$ と定義する．

初期信頼値は式 (1) で与える．

$$peer\_conf(s,j) = max((peer\_conf(s,i) * peer\_conf(i,j) \\ *\text{ホップ数に応じた係数}), \\ (\text{現在の } peer\_conf(s,j))) \qquad (1)$$

また，通信を重ねる毎に，公開鍵信頼値，ピア信頼値を更新する．通信が成功したとき，信頼値を上げ，通信が失敗したとき，信頼値を下げる．信頼値は公開鍵の使用，公開鍵に対しての署名のための判断材料となる．更新式は式 (2)，(3) で与える．

■通信成功 (x:連続回数，更新後の上限:1)

$$\text{鍵更新値} : Ka^x,\ \text{ピア更新値} : Lb \qquad (2)$$

■通信失敗 (x:連続回数，更新後の下限:0)

$$\text{鍵更新値} : -Mc^x,\ \text{ピア信頼値} : -Nd^x \qquad (3)$$

a，b，c，d は任意の自然数である．また，K，L，M，N は信頼値を 0 から 1 に正規化するパラメータである．

5　シミュレーションによる実験

テーブルサイズの変化による問合せ割合の変化をシミュレーションした．問合せがあったピアを問合せ割合で昇順に並べたと仮定した際，以下の 3 種類に分類する．

- Core(問合せ割合の上位 1%)
  嗜好がとてもよく似ている
- Normal(問合せ割合の上位 10%)
  嗜好が似ていないが，少し興味がある
- Other(残りの全てのピア)
  ほとんど似ていない

このように分類した際に，一定の範囲における問合せの割合を以下のものについて調べる．

- Found
  問合せのあったピアの信頼値が，信頼値テーブルの中に存在する割合
- Core_again
  テーブル中に存在しなかったうち，上位 1% のピアで 1 回以上信頼値テーブルから消されたことのある割合
- Normal_again
  テーブル中に存在しなかったうち，上位 10% のピアで 1 回以上信頼値テーブルから消されたことのある割合

テーブルサイズや接続ピア数，それぞれのピアの問合せ割合を変化させ，これらの要素を検証するためにシミュレーションプログラムを作成した．

5.1 テーブルサイズ変更時の結果

接続ピア数を 100000 ピア，試行回数を 100000 回，全問合せ中の Core の問合せ割合を 40%，Normal の問合せ割合を 20% としてテーブルサイズを 1%，3%，5%，7.5%，10%，15%，20%，30%，50% と変化させた際の Found，Normal_again，Core_again の結果は図 3 で示すグラフになった．

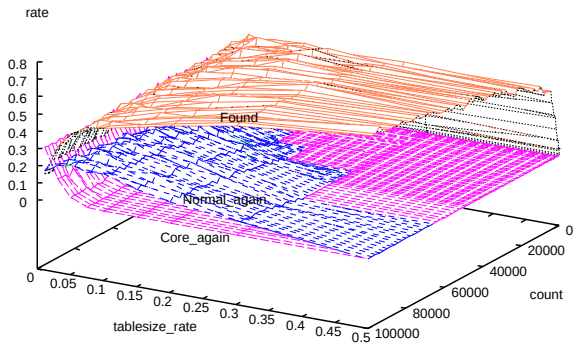

図 3　テーブルサイズを変更した際の結果

グラフよりテーブルサイズが接続ピア数の 5% あたりのところで Found の傾きが減少していることがわかる．また，この 5% 付近のところで Core グループの再問合せ割合がほぼ 0 となっている．

このシミュレーションの結果より接続ピア数の 5% あたりがテーブルサイズの一応の目安となることが分かった．

5.2 各グループの問合せ割合を変更させた際の結果

ピアに対する共有問合せ割合は，自身の所持しているコンテンツの一般への人気によって大きく異なる．

そこで次に接続ピア数を 100000 ピア，試行回数を 200000 回，テーブルサイズの割合を前節の結果より 5% から 15% まで変化させて，各グループの問合せ割合を変更させた際における発見割合，再問合せ割合を調べた．まずは前節の割合よりも人気のあるコンテンツとして，Core グループの問合せ割合が 25%，Normal グループの問合せ割合が 25% としてシミュレーションを行った．結果は図 4 に示すグラフになった．

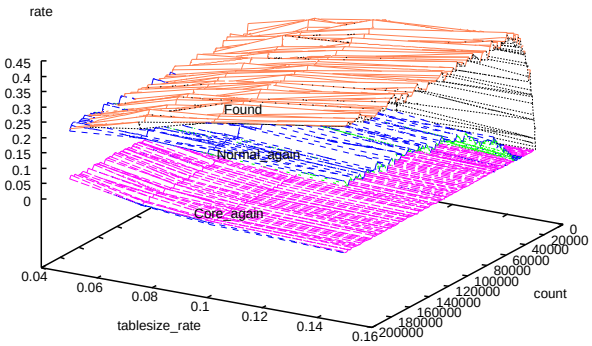

図 4　人気のあるコンテンツ所有時の結果

次に前節の割合よりも人気のないコンテンツとして，Core グループの問合せ割合が 0.5，Normal グループの問合せ割合が 0.2 としてシミュレーションを行った．結果は図 5 に示すグラフになった．

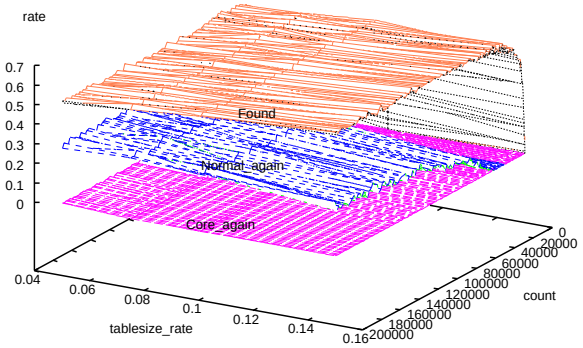

図 5　人気のないコンテンツ所有時の結果

図 4 のグラフより人気のあるコンテンツの場合では，テーブルサイズの違いは発見割合に影響を与えるが，図 5 の人気のないコンテンツの場合では，テーブルサイズの違いが発見割合の上昇に対してさほど影響を与えないということが分かった．

5.3 通信成功確率を変動させた際の評価

次に，通信を重ねるにつれての信頼値テーブル中の信頼値の変化の様子を調べた．ここで通信成功として，ピ

ア間の通信の際，相手の公開鍵を使用して復号化することができ，また共有したいコンテンツの本物を送信してきたものとする．

ピア信頼値の初期値を 0.3 として，特定のピアに対して 1000 回通信を行った際の信頼値の変化を調べた．通信成功確率を 0 から 1 まで 0.02 刻みで変更させ，通信成功時のピア信頼値更新を 0.02，通信失敗時のピア信頼値更新を $-0.01 * 10^x$ とした．x は成功や失敗の連続回数である．また，信頼値の上限は 1 であり，下限は 0 である．シミュレーションの結果，図 6 示すようなグラフとなった．

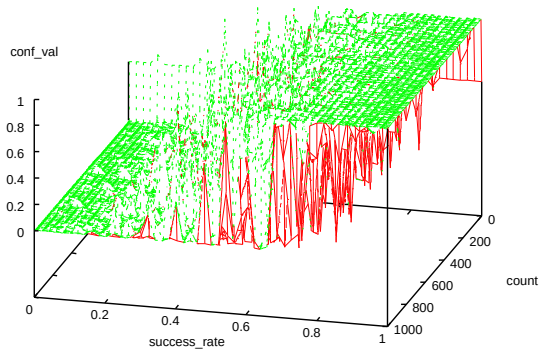

図 6　通信成功確率を変更した際のピア信頼値の変化

グラフより通信成功確率が 0.9 付近以上でないと信頼値テーブル中のピア信頼値が 0 に達してしまうことがわかった．ここで，信頼値が 0 に達した際にブラックリストを作成し，以後の通信を行わないとすると信頼の出来ないピアをネットワークから排除することが可能となり，信頼性の高いシステムを構築することが可能となる．

6　なりすまし問題

本研究で考えたシステムにおけるなりすまし問題について考えてみる．コンテンツ共有要求メッセージの中には電子署名の要素があり，要求を受け取ったピアは対象の公開鍵を用いて署名を検証する．そうすることでなりすましをある程度防ぐことが可能であると思われる．

しかし，この方法では man-in-the-middle 攻撃が可能となる．図 7 は攻撃の流れである．本研究のシステムで当てはめると，(1) ピア B はピア A に対して共有要求メッセージを送信したとする．(2, 3) その際，中間者は電子署名の部分を偽りの公開鍵で署名し直し，送信する．(4) メッセージを受信したピアは公開鍵を入手しようと問合せを行う．また，メッセージ送信者も相手の公開鍵を入手しようとする．(5〜10) ここで両者に偽りの公開鍵を手渡すことができれば，中間者は両者に気づかれることなくメッセージを盗聴，改ざんできてしまう．

本研究では公開鍵を入手した際に信頼値問合せを行う．偽造された鍵に対して，あるピアが本物と信じて署名をしてしまうと，以降その公開鍵に対して信頼の連鎖

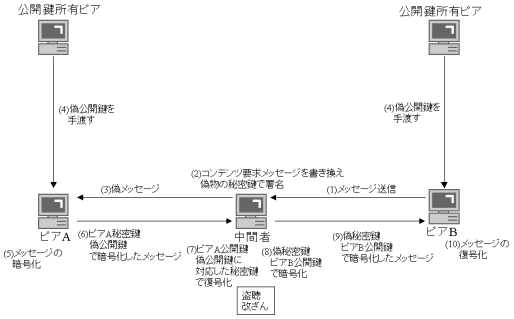

図 7　本システムの中間一致攻撃の様子

を求めることができてしまうために他の入手したピアも信用してしまう．また，信頼の連鎖が求められなくても，その公開鍵の使用は個人の責任となってしまうのでセキュリティに関心のないユーザはそのまま使用してしまうということにもなりかねない．

このような問題に対して別の方法を用いて認証する必要があり，今後の研究課題となるであろう．

7　おわりに

本研究では P2P システム上で通信を行う際に起こるであろうセキュリティ問題について，直接信頼モデルで公開鍵を配布し，暗号化通信をすることで，リスクを軽減しようとした．

提案に対してシミュレーションを行った結果，頻繁に問合せを行ってくるピアに対してピアの信頼性を検証するためには，どのようにテーブルサイズを決定すればよいのかということが分かった．また，高信頼性な通信を実現するためには，どのようにピアの信頼値が振舞えばよいのかということが分かった．

一方で，なりすましといった信頼性に対して重要な問題点を本研究で提案した方法では防ぐことができないので，本研究に対応した別の認証方法の研究が今後の課題として残る．

謝辞

本研究を進めるにあたり，御指導をいただいた河野浩之教授に深く感謝致します．

参考文献

[1] Michael Miller, トップスタジオ: P2P コンピューティング入門, 翔泳社, (2002).

[2] @IT: “PKI 再入門”, (online), available from <http://www.atmarkit.co.jp/fsecurity/rensai/re_pki03/re_pki01.html>, (accessed 2004-08-25).

[3] Bill Yeager: “Enterprise Strength Security on a JXTA P2P Network”, Proceeding of the Third International Conference on Peer-to-Peer Computing. (2003), pp.7-8.