社団法人 情報処理学会　研究報告
IPSJ SIG Technical Report

2004－ＤＰＳ－117　(2)
2004－CSEC－　24　(2)
2004／3／4

セキュアP2Pのためのユーザ主導型コンテンツ交換方式

今本 吉治*　松本 真弥*　重野 寛*　岡田 謙一*

P2P システムはコンテンツが自律的に分散される特徴を持ち, 新しいコンテンツ流通基盤として注目されている. しかし, 現実に使われている P2P では違法コピーなどの著作権問題があり, コンテンツ配信者だけでなく利用者にとっても危険な流通基盤となっている. そこで本稿ではコンテンツにパーミッション情報を付与し, 利用者のポリシーに従って配信を行うコンテンツセキュア P2P システムを提案する. また, 実 P2P ネットワーク上で実装したプロトタイプシステムを動作させ, その有効性を検証する.

A User Initiative Content Exchange Method for Secure Peer-to-Peer System

Yoshiharu IMAMOTO*　Shin-ya MATUMOTO*　Hiroshi SHIGENO*
Kenichi OKADA*

Peer-to-peer systems have the feature that distributes contents autonomously, and be in the spotlight for the new contents distribution system. But for the actual P2P system, there are problems about copyright, illegal copy and so on, so for not only content holders but also P2P users have the risk in the P2P system. Therefore we propose a content secure P2P system in which contents contain the information about the permission and they are distributed according to the poliscy set by P2P users. Moreover we implements the prototype, and evaluate it.

1　はじめに

P2P は, レガシー・システムからクライアント/サーバシステムへ続く分散処理の流れをさらに進めた通信形態であり, 新しい情報配信プラットフォームとして注目を集めている. しかし一方で, Gnutella[1][2][3] や WinMX のようなファイル交換ソフトは, 音楽ファイルや映画の違法コピーを目的として使用されることが多く, 一般的に P2P は違法コピーのネットワーク, 危険なネットワークとして認識されてしまっている. また, 違法コピーを行ないたくない善意のユーザが P2P を使用すると, 違法コピーの仲介をさせられてしまう危険性もある. そのため, P2P はその多大なる検索能力を発揮することが出来ていないのが現状である.

これを解決するための 1 つの手段として, 違法コピーを排除することが考えられる. コピープロテクションや電子透かしを用いた犯人特定技術はこれを目的として開発された技術である. しかし, コピープロテクションは回避する技術がハッカー達によって開発され, 電子透かしを用いた犯人特定は P2P ネットワークの中では困難である. また, 法的に規制を行い違法コピーを減らそうとしても P2P そのものに違法性がないため困難である.

本研究では, 違法コピーの排除を目的とせずにセキュア P2P を実現するために, Content Secure P2P を提案する.

Content Secure P2P ではコンテンツに Permission 情報 (許可情報) を改ざんされないように付与し, ネットワーク中の CS-P2P Node(Content Secure P2P Node) でその情報に基づいてユーザへの転送を決定する. 違法コピーの危険性を回避したいユーザへは, 危険なコンテンツは CS-P2P Node でフィルタリングされ, Permission 情報の付与された安全なコンテンツのみが送信される. これにより利用者は安心し

* 慶應義塾大学 理工学部 情報工学科
Department of Instrumentation(Information), Faculty of Science and Technology, Keio University

て P2P を使うことができる.

以下, 2 章ではデジタル署名や SION などの関連研究について, 3 章では提案システムについて, 4 章で実験・評価を述べ, 5 章でまとめとする.

2 関連研究

2.1 SIONet

SION[4][5] は意味情報用いた配信システムであり利用者がネットワーク中のノードへ意味情報フィルタを登録するネットワーク中のノードはそのフィルタを元にコンテンツのルーティングを決定し利用者の嗜好に応じたコンテンツ配信を実現するシステムである. この意味情報として著作権情報を用いることにより, 本研究で実現しようとしている著作権情報をもとにした配信が可能となるがコンテンツに著作権情報を安全に埋め込む機構がないため悪意のある利用者による著作権情報の改ざんが考えられる.

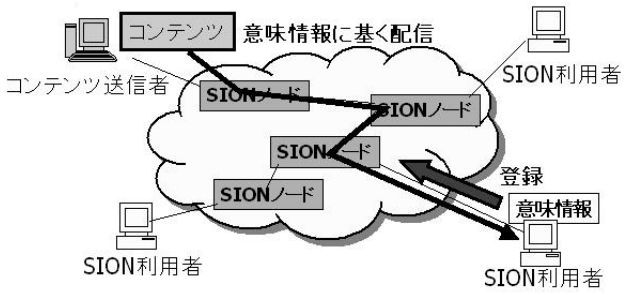

図 1: SIONet

2.2 デジタル署名

デジタル署名は, ハッシュ関数や暗号技術を用いることで, 受信したデータが伝送経路中で改ざんされていないことを保障するための技術である. この技術を用いることで, コンテンツの送信者から受信者までの経路で Permission 情報の改ざんを防ぐことが可能となる. クライアント/サーバ技術を用いた Web システムではコンテンツの著作権者と送信者がほぼ一致するためこの技術で十分であったが, P2P ではコンテンツの受信者が次のフェーズでは送信者にもなり得るため, 単純なデジタル署名の適用では対処できない.

2.3 電子透かし技術

電子透かし技術はコンテンツにひそかに情報を埋め込む技術であり, その使用目的は主に違法コピーの摘発である. つまり, コンテンツの著作権者がコンテンツに自分の情報を埋め込み, 不当に著作権を主張するものが現れた場合に正規の著作権者が著作権を主張するために使われる. 一方, 本研究で提案している電子透かしは, コンテンツの利用者が安心して使用できるようにコンテンツの著作権者が埋め込むものである. ただし, 電子透かしを実現するために用いる信号処理の技術は従来のものと同じである.

3 Content Secure P2P の設計

提案する Content Secure P2P ではコンテンツに Permission 情報（許可情報）を改ざんされないように付与し, ネットワーク中ではその情報にもとづいてユーザへの転送を決定する. 違法コピーの危険性を回避したいユーザへは危険なコンテンツはフィルタリングされ, Permission 情報の付与された安全なコンテンツのみが送信される.

3.1 Permission 情報の定義

本研究では, 安全なコンテンツであることを示すために Permission 情報を作成し, コンテンツにそれを付与する. Permission 情報とは, そのコンテンツを取得した後, 第三者にコピーしても良いか, 改変しても良いか, 画像であればそれを公衆の面前で表示しても良いかなどの使用目的に応じた許可情報であり, XML を用いて定義する. 図 2 に Permission 情報の例を示す.

3.2 コンテンツ ID を用いた認証付き電子透かし手法

本研究では Permission 情報に基くコンテンツフィルタリングを行なうため, Permission 情報とコンテンツの対応付けを行なう必要がある. また Permission 情報が偽造されてしまうとセキュア P2P を実現することが出来ないので, Permission 情報はコンテンツと不可分でなければならない. そこで将来的に全てのコンテンツに付与されるであろうコンテンツ ID を用いて Permission 情報を付与する手法を提案する.

```
<?xml version="1.0" encoding="shift-jis"?>
<!DOCTYPE permissioninfo [
<!ELEMENT permissioninfo (copy, change, use)>
                    ⋮
]>
<permissioninfo>
   <copy value="true" />
   <change value="false" />
   <use value="true" />
</permissioninfo>
```

図 2: Permission 情報の例

本手法ではコンテンツホルダが単独で電子透かしを入れるのではなくネットワーク中の管理サーバと連携して以下の手順で行なう. 本研究ではこの管理サーバを CS-P2P MS(Content Secure P2P Management Server) と呼ぶ. コンテンツホルダによるコンテンツに対する Permission 情報の付与と, ダウンロードユーザによる確認手順を図 3 に示し, 以下に説明する.

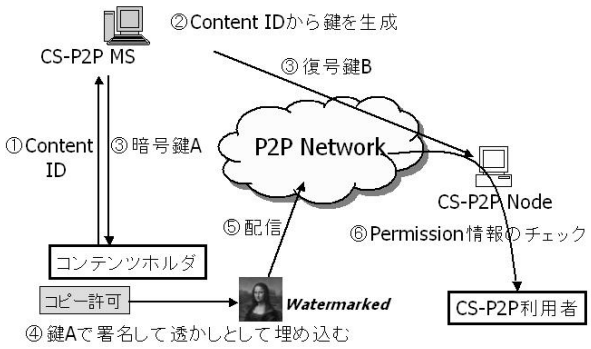

図 3: Permission 情報挿入の流れ

1. コンテンツ ID の登録： コンテンツホルダは電子透かしを挿入したいコンテンツのコンテンツ ID を CS-P2P MS へ登録する. ここで, コンテンツ ID の取得やコンテンツ ID の漏洩による危険性は, Content ID Forum で十分な議論がされており, RA (Registration Authority) と連携して認証を行うことにより安全に登録できると仮定する.

2. 署名用の鍵検証用の鍵の生成： コンテンツ ID を受け取った CS-P2P MS はコンテンツ ID 毎に異なる鍵を生成する.

3. 暗号鍵の送信： CS-P2P MS は作成した鍵のうち, 署名に用いる暗号鍵のみをコンテンツホルダに送信する.

4. Permission 情報へ署名： コンテンツホルダは CS-P2P MS から受信した暗号鍵を用いて Permission 情報を暗号化し, Permission 情報の署名を生成する.

5. 電子透かしの挿入： コンテンツホルダはコンテンツへ Permission 情報とその署名を電子透かしとして挿入し, 透かし付きのコンテンツを生成する.

6. P2P ネットワークを用いた配信： 生成された透かし付きコンテンツを P2P ネットワークを通して配信する.

3.3 ユーザ主導型コンテンツフィルタリング

本研究ではユーザの要求している条件に合うコンテンツのみを取得するために, ユーザ主導型コンテンツフィルタリングを提案する. フィルタリングはネットワーク中にあるフィルタリング用のノードで行いそのノードを CS-P2P Node と呼ぶ. 以下にその手順を示す.

1. Permission 情報の登録： ユーザは自分の欲しいコンテンツの Permission 情報を図 2 に示すフォーマットを用いて CS-P2P Node へ登録する.

2. 検索ダウンロードの開始： P2P プロトコルの検索メッセージを P2P ネットワーク内へ送信するそしてその検索結果から欲しいコンテンツのダウンロードメッセージを送信する.

3. 復号鍵のダウンロード： CS-P2P Node はユーザへ流れるコンテンツをキャプチャしそのコンテンツ ID から対応する復号鍵を CS-P2P MS からダウンロードする.

4. 署名の検証： CS-P2P Node は電子透かしを抽出し取得した復号鍵を用いてその署名を検証する.

5. Permission 情報のチェック： CS-P2P Node はコンテンツに付与されている Permission 情報とユーザが求めている Permission 情報を比較しユーザへの転送の可否を判断する.

4　実験・評価

本研究では提案した Content Secure P2P の実現性を調べるために実 P2P ネットワークと接続しプロトタイプシステムの動作検証を行った．またユーザにおけるコンテンツ取得時間を測定しネットワーク利用の有効性について評価を行った．

4.1　実 P2P ネットワーク上での検証実験

図 4 に示すように, CS-P2P MS, CS-P2P Node を配置し, 検証実験用のネットワークを構築し, 次の 4 通りのポリシーでコンテンツ取得を試みた．そして取得できたコンテンツを付与されている Permission 情報の割合に関して分析を行った．

- 従来の P2P
- 条件 A　コピー, 改変可能なコンテンツのみ取得
- 条件 B　コピーが可能なコンテンツのみ取得
- 条件 C　使用可能なコンテンツのみ取得

図 5 に検証実験の結果を示す．従来の P2P を用いた場合は Permission 情報の付与されていないコンテンツが大量に集まっている．現段階では Permission 情報を付与したコンテンツを扱っているのは筆者のみであるため, 実 P2P ネットワークと接続した場合は必然的に Permission 情報の付与されていないコンテンツが大量に集まってしまう．

一方, Content Secure P2P のを用いた条件 A, B, C ではいずれも Permission 情報の付与されていないコンテンツ, すなわち許可が確認できないコンテンツについては取得すると危険であるため, 取得されていない．また, 全ての条件において, ユーザが設定したポリシーに適合するコンテンツのみが取得されていることが分かる．

以上より, 提案した Content Secure P2P のプロトタイプは実 P2P ネットアークへ接続したときに正常に動作し, 危険なコンテンツを排除することに成功していることが分かる．

4.2　コンテンツ取得時間に関する評価実験

図 6 にこの評価実験で用いたネットワークを示す．CS-P2P MS, CS-P2P Node, ハブ間は 1Gbps の広帯域で接続し, それをコアネットワークと呼ぶ．Content

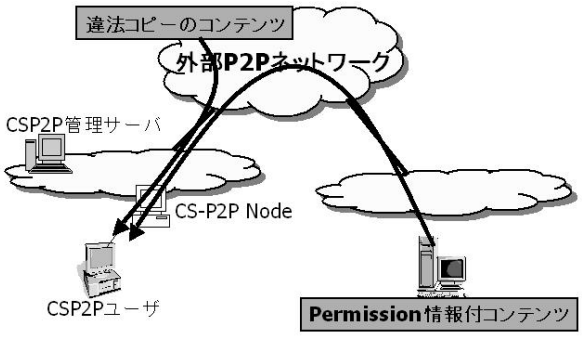

図 4: 実 P2P ネットワーク上での検証実験

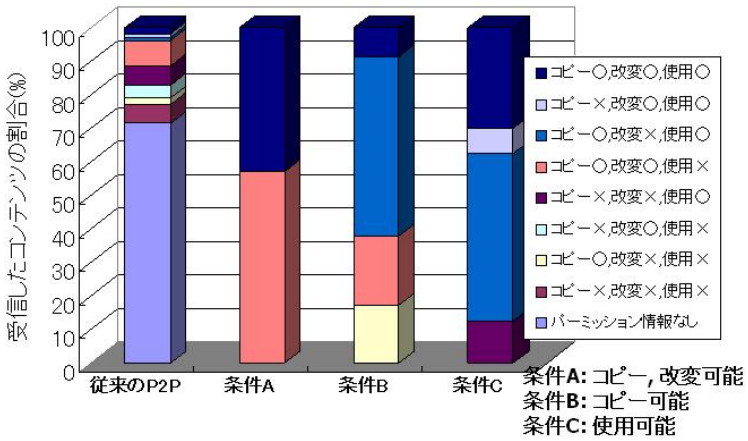

図 5: 受信コンテンツの割合

Secure P2P のユーザの端末とコンテンツを配信する端末は, それぞれコアネットワークと 100Mbps の狭帯域で接続した．インターネットの接続形態は, バックボーンは WDM を用いた高速ネットワークに, アクセス回線は安価な媒体を用いる傾向が強いため, これを模擬するたにこのようにした．

そして, 以下の手順で評価実験を行った．

1. 各コンテンツ配信端末に 200 個のコンテンツを保持させ, それらを共有させる．
2. 受信端末へ, 0Mbps, 50Mbps, 90Mbps のトラヒックによる負荷をかける．
3. コンテンツの検索を行い, 従来方式と Content Secure P2P でコンテンツのダウンロードを行なう．
4. ユーザが欲しているコンテンツを集めるまでの時間を測定する．

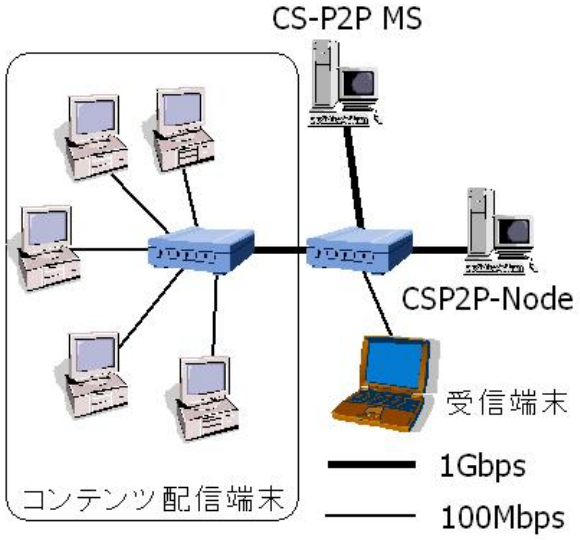

図 6: コンテンツ取得時間に関する評価実験

まず, コンテンツ配信端末および, ユーザ端末間で P2P ネットワークを形成し, コンテンツ配信端末はそれぞれ 200 個のコンテンツを共有した. ユーザ端末は, コンテンツの検索とダウンロードを行い, 自分のポリシーに適合するコンテンツを受信するまでの時間を測定し, 従来方式と提案方式である Content Secure P2P で検索を行った.

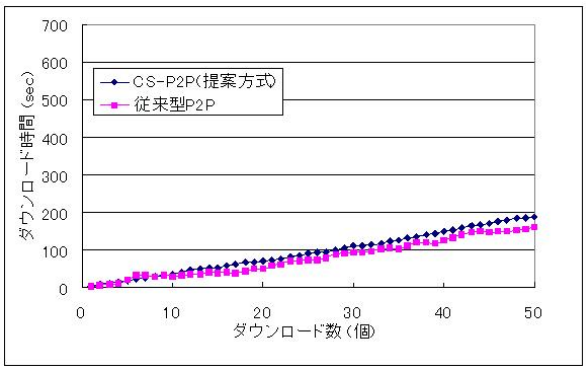

図 7: コンテンツダウンロード時間 (0Mbps)

図 7, 図 8, 図 9 はそれぞれ, ユーザ端末に 0Mbps, 50Mbps, 90Mbps のネットワーク負荷をかけて評価を行ったときの結果のグラフである. 図の横軸はユーザがポリシーに適合するコンテンツを受信した数である。つまり, Content Secure P2P を用いた場合は受信したそうコンテンツ数と一致するが, 従来方式の場合は受信した総コンテンツ数のうち Content Secure P2P を用いたときに設定したポリシーにも適合するコンテンツの数を横軸にしている. 従って, 受信端末で行った場合との比較になる. 縦軸は横軸に示す数のコンテンツを受信するまでにかかった時間を示している.

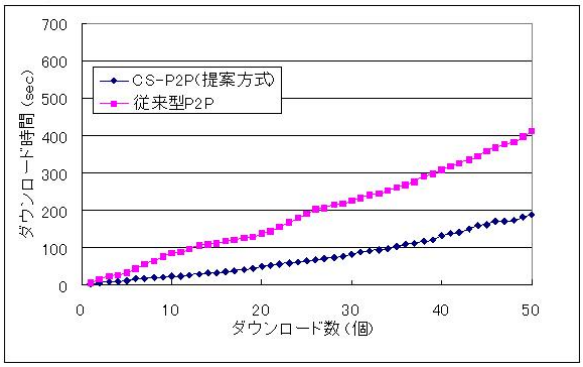

図 8: コンテンツダウンロード時間 (50Mbps)

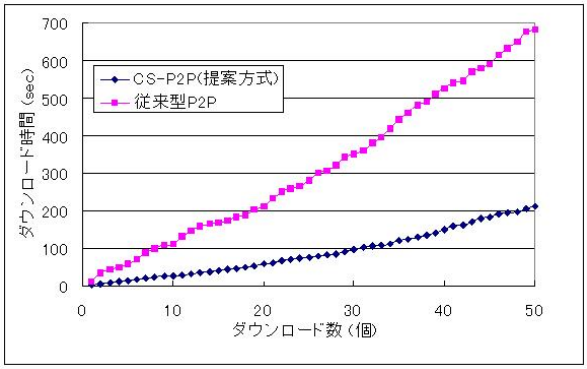

図 9: コンテンツダウンロード時間 (90Mbps)

図 7 より, ユーザ端末に負荷を与えない場合は, CS-P2P Node でコンテンツフィルタリングを行っていることにより, CS-P2P Node での処理がボトルネックとなってしまいスループットが下がってしまっているが, 従来方式との差はほとんど見られない.

一方, 図 8, 図 9 より, ユーザの端末へのネットワーク負荷を増やすとそれに伴って従来方式ではダウンロード時間が増加しているのに対して, 提案方式では増加は見られない. これは提案方式ではユーザ端末に送信されるコンテンツのトラヒックはフィルタリングにより最小に抑えられるため, アクセス回線が狭帯域になっても性能低下を防ぐことができたた

めと考えられる.

5 結論

本稿では, セキュアな P2P 実現のために P2P システムを悪用した違法コンテンツ交換の危険性に着目し, 管理サーバを含む新しい形態の P2P ネットワークを設計することによって, 危険なネットワーク中で安全なコンテンツのみを取得する Content Secure P2P System を提案した. これを実現するためにコンテンツと一体になるように Permission 情報を付与する電子すかし手法を提案した. そして, 提案アーキテクチャを適用したシステムの設計について述べ, この設計にもとづいて構築したプロトタイプシステムをテストベッドに導入して評価実験を行った. この結果から, 実 P2P ネットワーク上で正しく動作することを検証し, また狭帯域の環境ではコンテンツ取得にかかる時間が従来の P2P に比べて有利であることが評価実験より証明さた.

参考文献

[1] 伊藤 直樹: P2P コンピューティング-技術解説とアプリケーション, ソフト・リサーチ・センター (2001).

[2] 井口 圭一: 実験：ネットワーク管理者のための Gnutella 入門, http://www.atmarkit.co.jp/fwin2k/experiments/gnutella_for_admin/gnutella_for_admin_0.html.

[3] 山村 恭平: グヌーテラでいこう!—インターネットの世界に革命を起こす怪物ソフト『Gnutella』, ベストセラーズ (2001).

[4] 星合隆成: 意味情報ネットワーク SIONet におけるエンティティのオンライン増減設機構, 電子情報通信学会論文誌 B, , Vol.J85-B, No.2, pp.180-199.

[5] 星合隆成, 小柳恵一, ビルゲー・スクバタール, 久保田稔, 柴田弘, 酒井隆道: 意味情報ネットワークアーキテクチャ, 電子情報通信学会論文誌 B, Vol.J84-B, No.3, pp.411-424, (2001).