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

2008－ＤＰＳ－134　(42)
2008－CSEC－ 40　(42)
2008／3／7

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アーキテクチャの検討

寺田真敏[†1]　鬼頭哲郎[†1]　仲小路博史[†1]
松木隆宏[†2]　松岡正明[†2]

[†1)] (株)日立製作所　システム開発研究所
〒212-8567 神奈川県川崎市幸区鹿島田 890
[†2)] (株)ラック
〒105-7111 東京都港区東新橋 1-5-2 汐留シティセンター11 階

概要：ファイル交換ソフトウェア環境において，ウイルス感染によるファイルの流出，著作権上適切ではないファイル交換などの問題が深刻になっている．本稿では，ファイル交換ソフトウェア環境において，意図しないファイルの流出を防ぎ，持ち込まれたくないファイルの流入を防ぐ情報流通対策を検討した．また，検討に基づきファイル交換ソフトウェア向けの情報流通対策として，意図しないファイルアップロードの防止，暴露型ウイルスへの感染通知，著作権上適切ではないファイルのダウンロードの抑止，不正活動ホストの広報機能を備えたシステムを提案する．
キーワード：P2P，情報流出，ウイルス，著作権

Information Sharing Architecture for P2P File Exchange Environment

Masato Terada[†1]　Tetsuro Kito[†1]　Hirofumi Nakakoji[†1]
Takahiro Matsuki[†2]　Masaaki Matsuoka[†2]

[†1)] System Development Lab. Hitachi Ltd.
890 Kashimada, Saiwai-ku, Kawasaki, Kanagawa, 212-8567 Japan
[†2)] Little eArth Corporation Co., Ltd
1-5-2 Higashi-Shinbashi, Minato,Tokyo, 105-7111 Japan.

Abstract: Recently, there are many problems regarding the P2P file exchange environment on the Internet. The need to reconsider the current P2P file exchange environment for information leak and copyright is obvious. In this paper, we examine the countermeasure architecture when applying the present P2P file exchange environment to the Internet. And, we show the Information Sharing Architecture for P2P File Exchange Environment that includes the prevention of the file upload, the prevention of circulation of copyright violation file, the infection notice to the exposure type virus, and the notice of illegal activities of host.
Key words: P2P, Information Leak, Virus, Copyright

1　はじめに

社会インフラとして，IT システムやインターネット利用が拡大する一方で，P2P ファイル交換ソフトウェア環境においては、ウイルス感染によるファイルの流出，著作権上適切ではないファイル交換などの問題が深刻化している．

IPA の 2006 年調査レポートによれば，P2P ファイル交換ソフトウェアのウイルス感染によって情報が流出した際の復旧作業の延べ人日は，ウイルス感染全般の復旧作業よりも多く，被害経験率は低いもののいったん被害に遭うと対応の負荷が大きいと報告している[1]．また，社団法人コンピュータソフトウェア著作権協会の調査レポートによれば，著作権上適切ではないファイル交換による被害相当額は約 100 億円の規模と報告している[2]．文献 3)では，アンケート調査より，多くのユーザが P2P ファイル交換ソフトウェアによる情報流出に対して不安を持っており，利用をやめた理由として情報流出への懸念が最も多いことを指摘している．

本稿では，上記の課題を解決するため，P2P ファイル交換ソフトウェア環境において，意図しないファイルの流出を防ぎ，持ち込まれたくないファイルの流入を防ぐ情報流通対策を検討した．また，検討に基づきファイル交換ソフトウェア向けの情報流通対策として，意図しないファイルアップロードの防止，暴露型ウイルスへの感染通知，不正活動ホストの広報，ファイルの流入防止機能を備えたシステムを提案する．

2　関連研究

本章では，P2P ファイル交換ソフトウェア関連研

究として，トラフィック／稼動ノード数／ファイル流通量の把握，意図しないファイル流出の防止，著作権上適切ではないファイル交換の抑止の視点から整理する．

2.1 トラフィック／稼動ノード数／ファイル流通量の把握

(1) トラフィック

文献 4) 5) 6) 7)では，トラフィックが P2P であることを判定するため，トラフィックの特徴量やピア間通信のサーバ／クライアント関係を用いたトラフィックの特定方法を提案している．この他に，トラフィックの可視化を通して P2P トラフィックの管理支援する研究も行われている[8][9]. ネットワークの実計測を通して，Web 及び P2P トラフィックのフロー分析を行った報告としては，文献 10) 11) 12)がある．文献 12)では，NetFlow を用いて一日当たりのユーザの送受信トラフィック量を測定しており(調査時期：2004 年 4，5，10 月，2005 年 2，7 月)，1 日当たり 2.5GB 以上のトラフィックを発生させているヘビーユーザは一定割合で存在し，トラフィックの流量と方向から P2P による帯域占有の可能性を示唆している．

(2) 稼動ノード数

稼動ノード数については，全ノード数把握が困難な Winny ネットワークの規模を推定するため，文献 13) では，実測定によって得られた Winny の通信データをもとにコンピュータシミュレーション実験を行い，Winny ネットワークの規模推定する方法を提案している．文献 14) 15)では，Winnybot／Sharebot と呼ぶツールを用いて収集したデータを元に Winny／Share 稼動ノード数, ファイルのプロパティが格納されている Winny／Share のキー流通量について報告している．

(3) ファイル流通量

文献 16)(調査時期：2003 年 4 月)では，WinMX, Gnutella, Winny を対象としたコンテンツ分析を行っており，Winny では，全ファイル数が 23 万，ファイルサイズが約 63MB，avi や mpg などの動画像，zip や rar といった圧縮ファイルが流通していることを報告している. 文献 17)では(調査時期:2007 年 9 月), Winny 上のファイルは約 484 万 6 千件存在し，流通するファイル全体の 51.4%が著作物と推定している．

2.2 意図しないファイル流出の防止

事前措置として，すべてのファイルアクセスを監視し，未知のプログラムからのファイルアクセスを禁止することでファイル流出を防止する方式[18], 一般情報と機密情報を区別して，機密情報を含むファイルのみ暗号化し，かつ機密情報が平文のまま一般ファイルに混入しないよう強制アクセス制御を行う方式[19]などが提案されている．

事後措置としては，P2P ファイル交換ソフトウェア環境に，不要あるいは，おとりの情報を流す技術は，流出した情報を取得しにくくする技術としての利用側面がある．このような不要あるいは，おとりの情報を流した場合の影響を検討した研究として文献 20)，21)がある．

実フィールドでの対策アプローチとしては，(1) 個人／機密情報を持ち出さない／データを暗号化するなどコンピュータへのファイル格納に関する制限, (2) Winny／Share など流出ファイルを伝搬する P2P ファイル交換ソフトウェアの除去，または，P2P ファイル交換ソフトウェアトラフィックの遮断，(3) Antinny など意図しないファイル伝搬を助長するマルウェアの除去，(4) 事後措置としての情報漏えい調査，風評被害対策などがある．

2.3 著作権上適切ではないファイル交換の抑止

ファイルの流通を管理する方式として，文献 22) は有害コンテンツの拡散を抑制するフィルタを共有する方式，文献 23)では，不正変更の検出，著作権情報の取得，転送ルートの記録など，すべての共有ファイルの交換履歴を管理する方式，文献 24)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方式を提案している．文献 25)ではコンテンツ自身の管理と保護に注目し，コンテンツ識別のための CoFIP(Content FInger Printing)技術を提案している．また，文献 26)では，適用先を Web サイトとしているが，著作者から管理の依頼があったデジタルコンテンツの不正利用を一般ユーザの協力により発見する仕組みを提案している．法的側面での研究については，文献 27)が現行著作権制度をインターネットに適用した場合の問題点について言及している．

実フィールドでの対策アプローチとしては，著作権上適切ではないと思われるファイルのハッシュ値を Web サイトで掲載するという方法が取られている．

3 情報流通対策アーキテクチャの検討

本章では，P2P ファイル交換ソフトウェア環境の課題を整理した後，検討した情報流通対策アーキテクチャについて述べる．

3.1 課題整理

関連研究を調査した結果から，これまでの研究や対策は，トラフィック／稼動ノード数／ファイル流通量の把握，意図しないファイル流出の防止，著作権上適切ではないファイル交換の抑止をそれぞれの事象として取り扱っている。しかし，これら 3 つの視点を組み合わせることにより，情報流通対策としての相乗効果を期待できる．

(1) トラフィック／稼動ノード数／ファイル流通量の把握

国内で比較的良く利用されている P2P ファイル交換ソフトウェアや新たに開発される P2P ファイル交換ソフトウェアを対象に，該当トラフィック量，稼動ノード数，ファイル流通量とコンテンツ傾向とを短期ならびに長期的に調査した結果は，流出したファイルや適切ではないファイルのダウンロードを遮断するための基礎データとしての活用や，情報流通対策実施後の効果測定として利用できる．

(2) 意図しないファイル流出の防止

意図しないファイル流出などのインシデント発生を，近傍のネットワークに広報することにより，端末だけでは解決できない問題を協調により解決できる．具体的には，ネットワークから該当するトラフィックを抽出すれば，意図しないファイル流出の遮断をネットワーク側で対処可能となる．

(3) 著作権上適切ではないファイル交換の抑止

流出したファイルを，適切ではないファイル交換の一部と考えることにより，著作権上適切ではないファイル交換の抑止機能を適用できる．

3.2 情報流通対策アーキテクチャ

図 1を用いて，整理した課題を解決する情報流通対策アーキテクチャの機能部品について述べる．

①トラフィック検出と制御

ネットワーク側で，意図しないファイル流出や著作権上適切ではないファイル交換を検出し，必要に応じて遮断を行う．検出方法としては，プロトコルおよびコネクション特徴に基づき該当トラフィックを抽出する方法や広報されたインシデント発生の検知する方法がある．

②クローリング調査／ダウンロード調査

クローリング調査は，ノードが保持する他ノード情報を取得するという操作を繰り返していく事で，P2P ファイル交換ソフトウェアが稼動するノードを網羅的に調査する方法である．稼動ノード数，ファイル流通量の長期的な調査，情報流通対策の効果測定として利用する．

ダウンロード調査は，P2P ファイル交換ソフトウェアで流通するコンテンツを収集し，ウイルス混入有無，著作権上の適切性を判定する．

③ファイル属性情報を格納したデータベース (P2PDB)

ダウンロード調査の結果として，ファイルを一意に識別する情報を，ウイルス混入有無，著作権上の適切性などのファイル属性情報と共に格納する．流出したファイルや適切ではないファイルのダウンロードを遮断するための基礎データとして利用する．

④ファイル流出の防止

端末側で意図しないファイル流出を検出し，必要に応じて遮断やインシデント発生の広報を行う．流出の防止方法については項番4.2で述べる．

⑤ファイル流入の抑止

端末側で著作権上適切ではないファイルダウンロードを検出し，必要に応じて遮断やインシデント発生の広報を行う．流入の抑止方法については項番4.4で述べる．

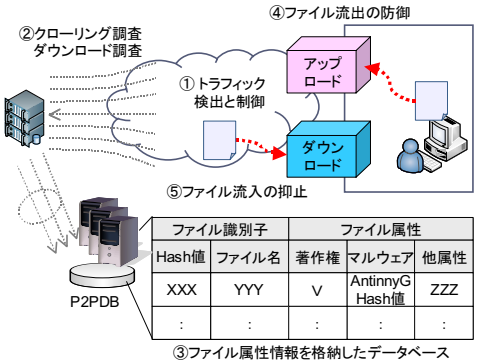

図 1：情報流通対策アーキテクチャの機能部品

4 情報流通対策システムの提案

本章では，前章の情報流通対策アーキテクチャをベースとした情報流通対策システムを提案する．

4.1 方針

実フィールドでの対策アプローチである，ファイル格納に関する制限や，P2P ファイル交換ソフトウェアの除去は，団体組織を対象とする対策としては有効である．ところが，個人が保有する端末を対象とした場合には，必ずしも適用できるとは限らない．そこで，情報流通対策システムでは，P2P ファイル交換ソフトウェアの利用を促進しつつ，インターネット利用者(または事業者)が安全に，安心して P2P ファイル交換ソフトウェアを利用できる環境を提供することを目的とする．

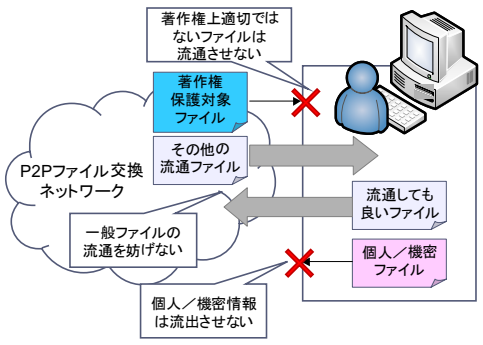

図 2：情報流通対策システムの設計方針

具体的には，端末に格納されている流通しても良いファイルのアップロードや著作権保護対象になっ

ていないファイルのダウンロードを妨げない．個人／機密情報のアップロードはさせず，著作権保護対象となっている著作権上適切ではないファイルのダウンロードもさせないシステムを実現することにある．

次節以降，情報流通対策システムを実現する 4 つの機能について述べる．

(1) 意図しないファイルアップロードの防止機能
(2) 暴露ウイルス感染通知機能
(3) 著作権上適切ではないファイルのダウンロードの抑止機能
(4) 不正活動ホストの広報機能

4.2 意図しないファイルアップロードの防止機能

誤操作，ウイルスなどによる本人の意図しない情報漏えいを防止するための機能である．個人／機密情報ファイルが，Winny／Share などの P2P ファイル交換ソフトウェアに対してアップロードされるのを検知した場合，該当ファイルを隔離することで問題を回避する．

本機能の実現にあたっては，次のようなアプローチをとることで利便性の向上を図る予定である．

- 端末上に存在するすべてのファイルに対して機密情報であるという保護マークをデフォルトで付与する．
- 一方，Winny／Share などの P2P ファイル交換ソフトウェア環境上で流通させたいファイルに対しては付与されている保護マークをはずした後，アップロード操作を行う．

ファイルのアップロード操作が行われたときの動作概要を図 3に示す．「個人／機密ファイル」は保護マークが付いているため隔離フォルダに収納されてしまう．一方，保護マークのはずされた「流通しても良いファイル」は P2P ファイル交換ソフトウェアのアップロードフォルダに格納され，流通することになる．

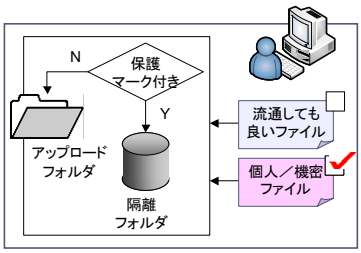

図 3：ファイルアップロードの防止機能

4.3 暴露ウイルス感染通知機能

ウイルスなどによる本人の意図しない情報漏えいを抑止するための補助機能である．P2P ファイル交換ソフトウェアを対象とした暴露型ウイルスは，スクリーンショットを取得した後にアップロード操作を行う，P2P ファイル交換ソフトウェアの設定ファイルを書き換えるなどの特有動作がある．

本機能の実現にあたっては，ウイルス対策ソフトウェアとの併用を想定し，ウイルス対策ソフトウェアを補助することで，安全性の向上を図る予定である．

暴露型ウイルスの活動の特徴を検出したときの動作概要を図 4に示す．「画面キャプチャファイル」は隔離フォルダに収納され，暴露型ウイルスに感染した可能性のあることを，利用者に通知する．

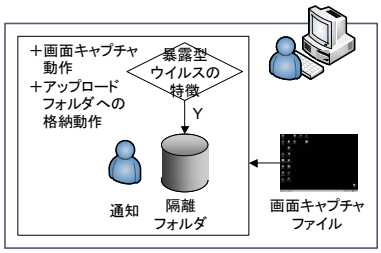

図 4：暴露ウイルス感染通知機能

4.4 著作権上適切ではないファイルのダウンロードの抑止機能

ダウンロードしたファイルが著作権上適切ではない場合，ファイルの流入を抑止するための機能である．Winny／Share などの P2P ファイル交換ソフトウェア環境からダウンロードしたファイルが，著作権上適切ではないと判断された場合，該当ファイルを隔離する．

本機能の実現にあたっては，次のようなアプローチをとることで拡張性の向上を図る予定である．

- 利用者端末単独で，ダウンロードしたファイルを隔離する．この場合，利用者端末に事前に格納した定義を使い判定し，ファイルを隔離する．
- ファイル属性情報を格納したデータベース(P2PDB)と連携して，ダウンロードしたファイルを隔離する．この場合，利用者端末上の情報流通対策システムから P2PDB に問合せを行い，該当ファイルの属性情報が著作権上適切ではないファイルか否かを確認する．適切ではないと判断された場合には，ファイルを隔離する．

ファイルのダウンロード操作が行われたときの動作概要を図 5に示す．ダウンロードファイルが P2PDB からの情報により著作権上適切ではないファイルと判断された場合には隔離フォルダに収納する．「その他の流通ファイル」は P2P ファイル交換ソフトウェアのダウンロードフォルダに格納され，流通することになる．

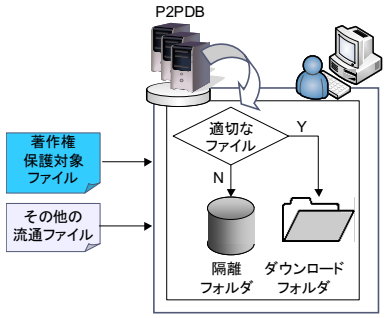

図 5：ファイルのダウンロードの抑止機能

4.5 不正活動ホストの広報機能

報告されている個人／機密情報の漏えい問題の多くは，表面化しにくい事象であること，問題が発生した後の対処にあたっては，近傍のネットワーク装置や事業者と協調して解決した方が良い場合がある．

本機能の目的は，利用者端末から，近傍のネットワークにインシデント発生あるいは，発生の可能性を通知することにより，ネットワーク側で情報流出に伴う拡散抑止につなげることにある．

本機能の実現にあたっては，次のような事象を捉えた場合，端末が送信する TCP/IP パケットに「端末が不審あるいは不正な活動をしている」ことを表す事象フラグを格納する．

- 個人／機密情報ファイルが P2P ファイル交換ソフトウェアに対してアップロードされるのを検知した場合
- 暴露型ウイルス感染を検知した場合

上述の広報対象となる事象を検出したときの動作概要を図 6に示す．事象フラグは，IP ヘッダあるいは，TCP ヘッダに格納することができ，目的にあわせて選択できることが拡張性を持たせることができると考えている．

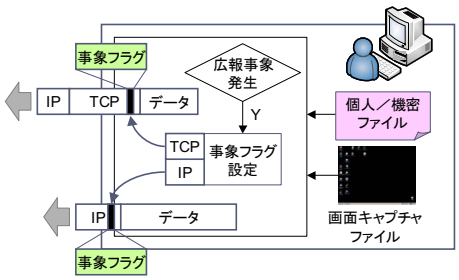

図 6：不正活動ホストの広報機能

また，このような「端末が不審あるいは不正な活動をしている」ことを表す事象フラグを格納した TCP/IP パケットを送信することにより，受信した中継装置や端末は，関連する通信を遮断する，関連する組織に通知する，あるいは他の信頼できる装置に TCP/IP パケットを転送するなどの対処が可能となる(図 7)．さらに，事象フラグには，発生の事象によって異なる値を付与し広報することでネットワーク側との対策連携の選択肢が増えると考えている．

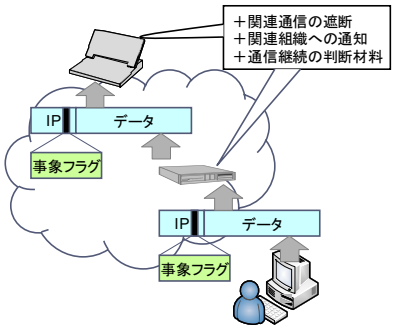

図 7：不正活動ホストの広報の受信

5 おわりに

本稿では，トラフィック／稼動ノード数／ファイル流通量の把握，意図しないファイル流出の防止，著作権上適切ではないファイル交換の抑止を組み合わせることにより，情報流通対策としての相乗効果を期待できることを示した．次に，P2P ファイル交換ソフトウェア環境において，意図しないファイルの流出を防ぎ，持ち込まれたくないファイルの流入を防ぐ情報流通対策システムを提案した．提案したシステムは，意図しないファイルアップロードの防止，暴露ウイルスへの感染通知，不正活動ホストの広報，ファイルの流入防止機能を備えている．

今後の課題は，情報流通対策アーキテクチャの機能部品の具体的な手法と相互連携手法の検討，さらに，その実現形態のひとつである情報流通対策システムの開発と有効性の検証などが挙げられる．

謝辞

本研究は総務省から委託を受けた「ネットワークを通じた情報流出の検知及び漏出情報の自動流通停止のための技術開発」の支援を受け実施している．本研究を進めるにあたって有益な助言と協力を頂いた関係者各位に深く感謝致します．

参考文献

1) (独)情報処理推進機構：2006 年 国内における情報セキュリティ事象被害状況調査(2007 年 8 月)
2) 社団法人コンピュータソフトウェア著作権協会：「Winny」ネットワーク上の無許諾流通コンテンツ実態調査(2006 年 11 月),
http://www2.accsjp.or.jp/news/release061128.html
3) 日立製作所：2007 年ファイル交換ソフトによる情

報漏えいに関する調査結果(2007 年 12 月),
http://www.hitachi.co.jp/hirt/publications/hirt-pub07012/index.html
4) 大坐畠智 他：パッシブ/アクティブ検知を用いた P2P トラフィック特定法, 情報処理学会 DSM 研究報告 No.31 pp.79-84(2005 年 3 月)
5) 松田崇 他：P2P 弁別のためのトラフィック特徴量の提案，電子情報通信学会技術研究報告 Vol.105 No.12 pp.5-8(2005 年 4 月)
6) 松田崇 他：通信の相互性に着目した PureP2P トラフィック弁別手法，電子情報通信学会技術研究報告 Vol.106, No.355 pp.61-66(2006 年 11 月)
7) 松田崇：PureP2P ファイル共有トラフィックの特性解析，電子情報通信学会技術研究報告 Vol.105 No.627 pp.133-136(2006 年 2 月)
8) 戸川聡 他：トラフィック傾向可視化による P2P ファイル共有通信検出支援モデルの提案，情報処理学会 DSM 研究報告 No.118 pp.19-24(2003 年 11 月)
9) 戸川聡 他：トラフィックマイニングと可視化による Peer-to-Peer ファイル共有検出支援システムの構築，電子情報通信学会技術研究報告 Vol.107 No.30 pp.99-104(2007 年 5 月)
10) 川島幸之助 他：ピアツーピア(P2P)トラフィックの現状，電子情報通信学会技術研究報告 Vol.103 No.492 pp.37-42(2003 年 12 月)
11) 森達哉 他：インターネットトラフィックのフロー分析 ：web と P2P の特性比較，電子情報通信学会論文誌 Vol.J87_D_I No.5 pp.561-571(2004 年 5 月)
[12] 福田健介：ブロードバンドトラフィック分析, http://www.ndrc.kyutech.ac.jp/interop06/
13) 蜂須賀大紀 他, ピュア P2P ネットワーク構成ピア数推定法の一検討，電子情報通信学会技術研究報告 Vol.105 No.12 pp. 1-4（2005 年 4 月）
14) 寺田真敏，鵜飼裕司 他：P2P ファイル交換ソフトウェア環境を対象とした観測に関する一考察, SCIS2007(2007 年 1 月)
15) 寺田真敏，鵜飼裕司 他：クローリング手法を用いた P2P ネットワークの観測，情報処理学会 CSEC 研究報告 No.48 pp. 51-56(2007 年 5 月)
16) 大井恵太 他：P2P ファイル共有におけるコンテンツ分析，情報処理学会 DPS 研究報告 No.87 pp.17-24(2003 年 8 月)
17) 社団法人コンピュータソフトウェア著作権協会：利用実態のアンケート調査，クローリング調査の結果(2007 年 12 月),
http://www2.accsjp.or.jp/news/release071221.html
18) 喜田弘司 他：ファイルアクセス制御エージェントの提案：P2P 型ファイル共有システムのセキュアな利用を目指して，情報処理学会論文誌 Vol.48 No.1 pp.200-212(2007 年 1 月)
19) 荒井正人 他：情報漏洩防止システムの提案，情報処理学会 CSEC 研究報告 No.22 pp.61-67(20040304)
20) N. Christin, A. Weigend, and J. Chuang, "Content Availability, Pollution and Poisoning in Peer-to-Peer File Sharing Networks," ACM E-Commerce Conference (2005)
21) J. Liang, R. Kumar, Y. Xi, and K. Ross. “Pollution in P2P file sharing systems.” Proc. IEEE INFOCOM’05(2005)
22) 伊吹和也 他：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 DSM 研究報告 No.72 pp.7-12 (2007 年 7 月)
23) 任光輝 他：P2P ネットワークにおける著作権管理手法の提案と実装，電子情報通信学会技術研究報告 Vol.104 No.568 pp.55-60(2005 年 1 月)
24) 今本吉治 他：セキュア P2P のためのユーザ主導型コンテンツ交換方式，情報処理学会 DPS 研究報告 No.22 pp.7-12(2004 年 3 月)
25) 青木 輝勝 他：コンテンツフィンガープリントを用いたコンテンツ管理方式，情報処理学会 AVM 研究報告 No.25 pp. 61-66(20040304)
26) 松下哲也 他：賞金稼ぎの仕組みを利用したディジタルコンテンツの監視方式，情報処理学会論文誌 Vol.44 No.8 pp.1970-1982(2003 年 8 月)
27) 近藤佐保子 他：ネットワークにおける現行著作権制度の問題と検討 ： ファイル共有ソフト(Winny 事件)を中心として，電子情報通信学会技術研究報告 Vol.106 No.526 pp.39-46 (2007 年 1 月)