P2P ファイル交換ソフトウェア環境向け 注意喚起メッセージングシステムの提案

寺田真敏[†1] 鬼頭哲郎[†1] 仲小路博史[†1] 甲斐根功[†2] 宮川雄一[†3]
湯川隆司[†3] 松岡正明[†4] 松木隆宏[†4] 鵜飼裕司[†5]

[†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
[†3)] (株)日立情報システムズ 〒141-8672 東京都品川区大崎 1-2-1
[†3)] (株)クロスワープ 〒150-0011 東京都渋谷区東 2-27-10
[†4)] (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
[†5)] (株)フォティーンフォティ技術研究所 〒162-0808 東京都新宿区天神町 8 神楽坂 U ビル 2 階

概要：P2P 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による被害を低減するためには，対策基盤の整備だけではなく，P2P 利用者自身が被害低減に関わることも必要である．本稿では，Winny／Share ネットワーク上に「該当するダウンロードファイル削除のお願い」「ウイルスファイルの可能性あり」など意図するメッセージを直接流すことで，P2P 利用者への注意喚起を図りつつ，ファイルのダウンロード抑止措置を支援する注意喚起メッセージングシステムについて提案する．
キーワード：P2P，セキュリティ，注意喚起

Masato Terada[†1] Tetsuro Kito[†1] Hirofumi Nakakoji[†1] Isao Kaine[†2] Yuichi Miyagawa[†3]
Ryuji Yukawa[†3] Masaaki Matsuoka[†4] Takahiro Matsuki[†4] Yuji Ukai[†5]

[†1)] System Development Lab. Hitachi Ltd. 890 Kashimada, Saiwai-ku, Kawasaki, Kanagawa, 212-8567 Japan
[†2)] Hitachi Information Systems, Ltd. 1-2-1 Osaki, Shinagawa-ku, Tokyo, 141-8672 Japan
[†3)] CROSSWARP Inc. 2-27-10 Higashi, Shubuya-ku, Tokyo, 150-0011 Japan
[†4)] Little eArth Corporation Co., Ltd 1-5-2 Higashi-Shinbashi, Minato-ku,Tokyo, 105-7111 Japan
[†5)] Fourteenforty Research Institute, Inc. 8 Tenzin, Shinjuku-ku,Tokyo, 162-0808 Japan

Abstract: P2P file exchange software is spreading on the Internet. The requirements of investigation reports such as threats about P2P network are increasing. In this paper we describe a message notification approach by index poisoning to improve user awareness. Also, we show overview of a message notification system for Winny and Share.
Key words: P2P, Security, Awareness notification

1 はじめに

P2P 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．本研究では，これら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アーキテクチャとそれをベースにした情報流通対策システムを提案してきた[1][2][3].

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対策にあたっては，対策基盤の整備だけではなく，P2P 利用者自身が被害低減に寄与することも必要である．本稿では，これまで開発してきた情報流通対策システムの部品を応用し，P2P 利用者に「該当するダウンロードファイル削除のお願い」「ウイルスファイルの可能性あり」など意図するメッセージを直接流すことで，P2P 利用者への注意喚起を図りつつ，ファイルのダウンロード抑止措置を支援する注意喚起メッセージングシステムについて提案する．

2 関連技術

P2P モデルで構成されたファイル交換ソフトウェア環境には，Napster[4]のようにノード情報やファイルの所在を中央サーバで管理するハイブリッド型 P2P ファイル交換ソフトウェアと，Winny，Share，Gnutella のように，全ての処理を P2P で行なうピュア型 P2P ファイル交換ソフトウェア環境がある．本章では，ピュア型 P2P ファイル交換ソフトウェア環

境に，不要な情報を流すことでファイルのダウンロード抑止措置を実現するポリューションとインデックスポイズニングについて整理する．

2.1 ポリューション

ポリューションは，ファイル保持ノードからのファイルのダウンロードを抑止するために，ファイル名を変更したファイル(メタポリューション)や，ファイル内容を差し替えたファイル(コンテンツポリューション)をアップロードする手法である(図 1).

ポリューションを利用して P2P ネットワーク上に不要な情報を流した場合の可用性への影響については，eDonkey，FastTrack，Gnutella を対象とした文献5)，KaZaA を対象とした文献6)がある．文献7)では不正なノードを判定し，不正なノードからのダウンロード要求に対しては不要なデータを送付する機能を持たせファイルの流通を抑止する手法を提案している．文献8)では，ファイルにノイズをいれる，品質劣化をさせる，不完全なファイルを構成するなどの操作がユーザ行動に与える影響を調査している．

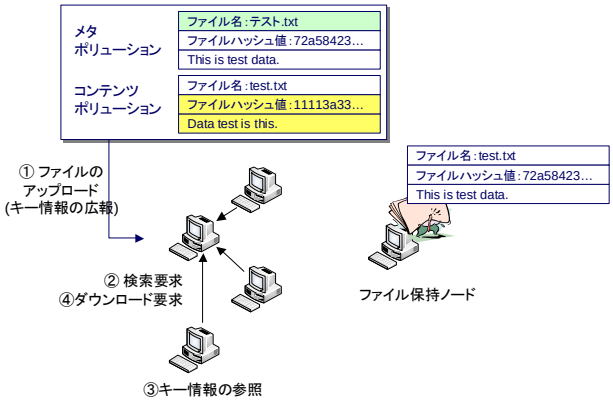


図 1：ポリューション

2.2 インデックスポイズニング

インデックスポイズニングは，ファイル保持ノードからのファイルのダウンロードを抑止するために，実際にはファイルを保持していないノード(IP アドレスやポート番号)を格納した所在情報(インデックス，キーと呼ばれる)を送付する手法である(図 2).

インデックスポイズニングを利用して P2P ネットワーク上に不要な情報を流した場合の可用性への影響については，Winny を対象とした文献9)10)がある．また，2007 年にはインデックスポイズニングを利用したファイルダウンロード抑止サービスが開始されており[11][12]，実環境での公開実験についても報告されている[13].

インデックスポイズニングについては，ファイルのダウンロードを抑止する手法として活用できる反面，P2P ファイル交換ソフトウェアが使用するファイル所在情報に，Web サーバやメールサーバなど P2P ネットワーク外のノードを指定することで，トラフィック誘導に悪用されてしまう可能もある．例えば，図 3のように詐称されたインデックス情報を参照した場合，ファイル保持ノードとして誘導された Web サーバに大量の接続要求を送信することになる．トラフィック誘導によるサービス運用妨害の影響については文献14)～17)で報告されている．

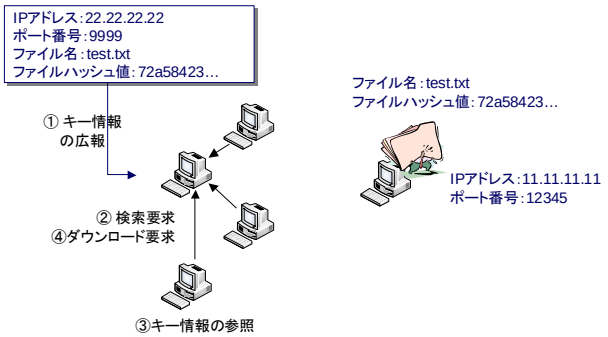


図 2：インデックスポイズニング

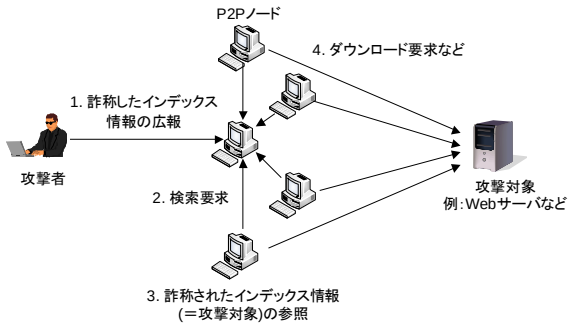


図 3：インデックスポイズニングによる
トラフィック誘導

3 注意喚起メッセージングシステム

本章では，P2P 利用者に「該当するダウンロードファイル削除のお願い」「ウイルスファイルの可能性あり」など意図するメッセージを直接流すことで，P2P 利用者への注意喚起を図りつつ，ファイルのダウンロード抑止措置を支援する注意喚起メッセージングシステムについて提案する．

3.1 解決したい課題

【 課題 1 】ウイルス感染により流出したファイルならびに，著作権上適切ではないファイルのダウンロードを抑止する．

【 課題 2 】 P2P 利用者に対する直接的な注意喚起を通して被害の低減を図る．

課題 1 については，2005 年頃からインデックスポイズニングを利用したファイルダウンロード抑止に

ついて研究がされてきている．また，2007 年にはインデックスポイズニングを利用したファイルダウンロード抑止サービスが開始されている．しかし，課題 2 については，Web サイトでのウイルスファイルである旨の警告掲載など，P2P 利用者に対する間接的な方法での注意喚起に留まっている状況にある．

3.2 提案手法

注意喚起メッセージングシステムでは，インデックスポイズニングの手法を応用し，次のように課題解決を図る．

【 課題 1 】ファイル保持ノードからのファイルダウンロードを抑止するために，実際にはファイルを保持していないノード(IP アドレスやポート番号)を格納した所在情報(以降，キー)を送付する．
【 課題 2 】キーに格納可能な情報のうち，P2P ファイル交換ソフトウェアの GUI に表示可能なフィールドに「該当するダウンロードファイル削除のお願い」「ウイルスファイルの可能性あり」などを意図する注意喚起メッセージを格納する．

Winny／Share を対象とした課題 2 の具体的な注意喚起方法を示す．
(1) Winny
Winny には，トリップと呼ぶ投稿者が自分の投稿であることを提示するためのフィールドが存在する．このトリップフィールドを利用するにあたっては，次に示す文字数と文字種の制約がある(図 4).

- Winny で利用できるトリップの文字数は，0 文字(最初が 00)，10 文字(最後が 00)，11 文字(00 なし)の 3 通りである．
- 使用可能な文字列は‘0’～‘9’，‘A’～‘Z’，‘a’～‘z’のみである．左記以外の文字に変換される数値を入れた場合にはトリップは表示されない．

```
4D  61  6C  77  61  72  65  46  69  6C  65
M   a   l   w   a   r   e   F   i   l   e

44  65  6C  65  74  65  46  69  6C  65  00
D   e   l   e   t   e   F   i   l   e  NULL
```

図 4：トリップで利用可能な文字数と文字種

提案方式では文字数と文字種の制約下で，このトリップフィールドに図 5に示すような“StopFileDL”や”DeleteFile”などの意図するメッセージを書き込むことで，P2P 利用者に対して直接的な注意喚起情報を届ける．

(2) Share
Share の場合にも，Winny と同様の投稿者が自分の投稿であることを提示するための ID フィールドが存在する．この ID フィールドには，次に示す文字数の制約がある．

- Share で利用できる ID の文字数は，8 文字(英数字，日本語文字)である．

提案方式では文字数の制約下で，この ID フィールドに図 6に示すような“StopFile”や”危険なファイル”などの意図するメッセージを書き込むことで，P2P 利用者に対して直接的な注意喚起情報を届ける．

3.3 実現方法

Winny／Share が構成する P2P ネットワークは，ファイルの所在(IP アドレス，ポート番号など)を記載したキーを交換して，ダウンロードしたいファイルの所在を取得している．注意喚起メッセージ送付では，トリップ(あるいは ID)と呼ばれるフィールドに注意喚起メッセージを書き込み，ファイルの所在として，『P2P ネットワークからランダムに選択したノードの所在を記載したキー(以降，注意喚起メッセージキー)』を大量かつ継続的に Winny／Share ネットワーク上に送付する．これにより，注意喚起をしつつ，注意喚起対象となるファイルのダウンロード抑止を実現する．

通常状態において，Winny／Share ネットワークでは，「ファイル X を保有しているのはノード(F)である」というファイルの所在を記載したキーが流通する(図 8(a)). このキーを入手したノードでは，キーに記載されている情報に従い，ノード(F)から「ファイル X」をダウンロードする．注意喚起メッセージングシステムでは，図 8(b)に示すようにランダムに選択したノードの所在を記載した注意喚起メッセージキーを流通させることにより，多くのノードが仮想的に「ファイル X」を持っているような状態に見せかけ，これにより，ノード(F)から「ファイル X」をダウンロードしにくい状態を作り出す．

注意喚起メッセージキー送付を実現する注意喚起メッセージングシステムの構成を図 7に示す．
(1) 送付管理装置
送付管理装置では，注意喚起メッセージキー自身の管理とその送付先管理がある．
(a) 注意喚起メッセージキーの管理
注意喚起対象となるファイル，所在情報やトリップ(あるいは ID)フィールドに格納するメッセージを管理する．
(b) 注意喚起メッセージキーの送付先管理
観測装置からのノード稼動情報に基づき，送信装置に対して，P2P ネットワーク外のノードにトラフィック誘導されることのないよう注意喚起メッセージキーの送信先を指示する．

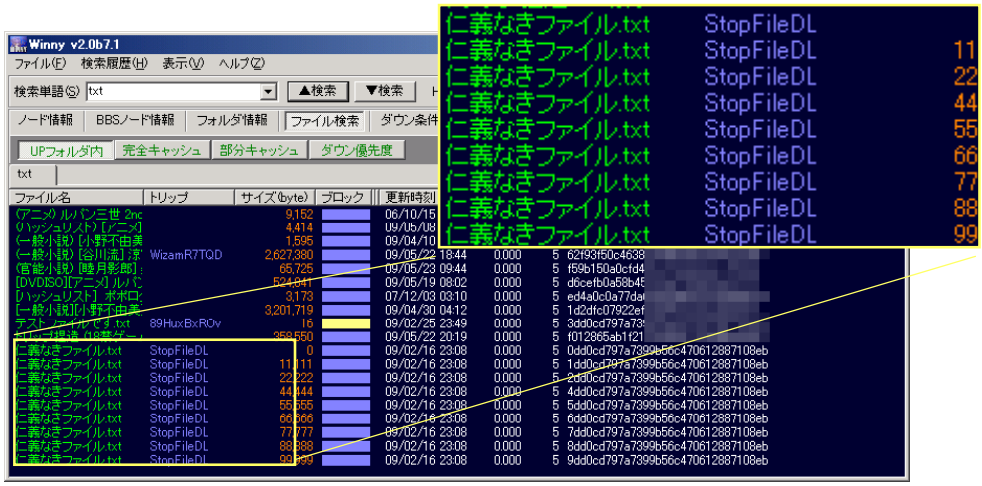


図 5：Winny における注意喚起メッセージ送付

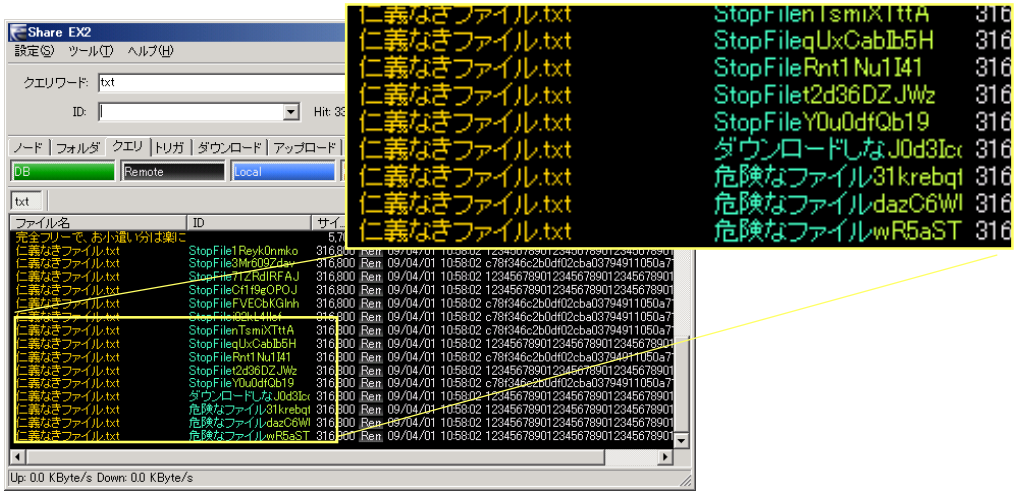


図 6：Share における注意喚起メッセージ送付

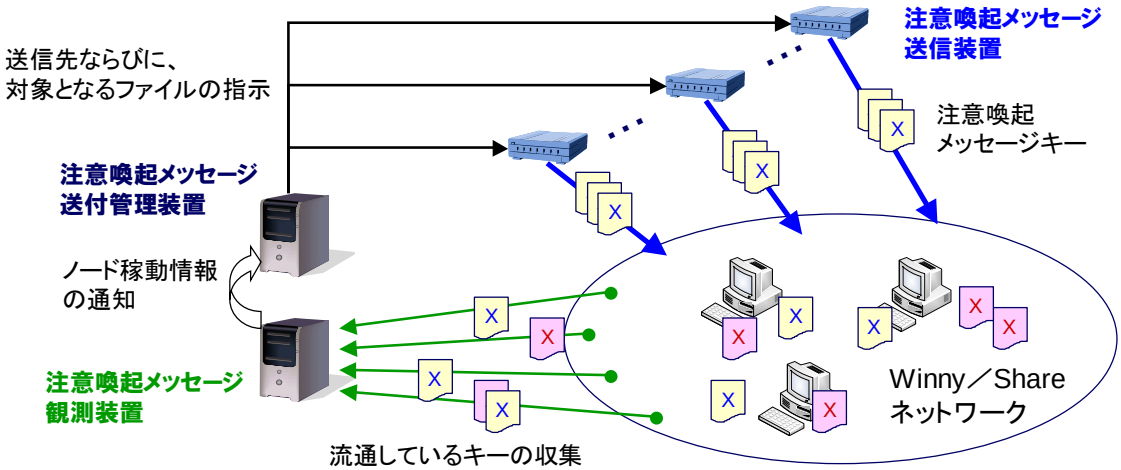
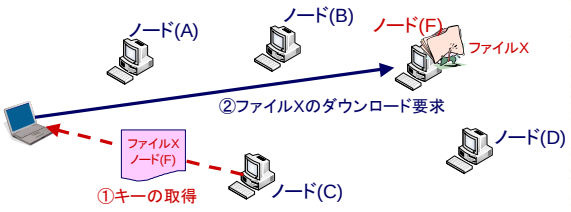
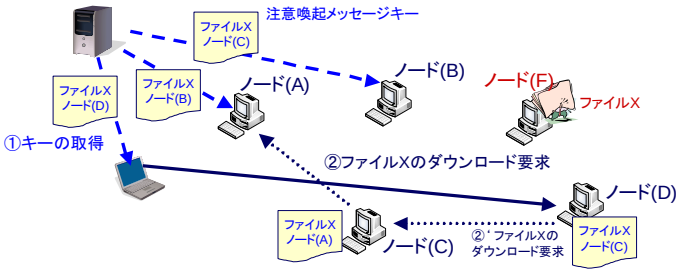


図 7：注意喚起メッセージングシステムの構成

商品名称等に関する表示
Napster は Napster,LLC.の登録商標または商標です.
本稿に記載されている会社名，製品名は，
それぞれの会社の商標もしくは登録商標です.



(a)通常時



(b)注意喚起メッセージキー送付時

図 8：キーの流通状態

(2) 送信装置

送信装置は，送付管理装置の指示に従い，注意喚起メッセージキーを送付する．システム構成を検討するにあたっては，注意喚起メッセージキーのトラフィックが集中しないこと，耐障害性を確保すること，運用コストの低減を図ることを考え，分散型の装置構成としている．

(3) 観測装置

観測装置では，注意喚起対象となるファイルの所在を記載したキーの流通状況を観測する．観測結果の表示については，注意喚起メッセージキーの地域的な拡散状態を可視化する“ハザードマップ(図 9)”，特定の注意喚起メッセージキーの時系列的な拡散状態を可視化する“拡散状態の時系列表示(図 10)”を想定している．

ファイルの所在を記載したキーには，IP アドレス，ポート番号，ファイルサイズ，ファイル名，ハッシュ値，トリップ，更新日などが格納されている．注意喚起メッセージを格納するトリップはファイル発信者を識別する情報で，通常，一般ユーザはこのフィールドに自由な値を設定することはできない．注意喚起メッセージキーでは，トリップに通常キー(既定で流通しているキー)と重複しない，意味ある文字列を設定する．特定の注意喚起メッセージキーの時系列的な拡散状態を可視化にあたっては，注意喚起メッセージキーと通常キーの区別判定にトリップ(あるいは ID)フィールドに格納された値を利用する．

3.4 考察

本節では，注意喚起メッセージキー送付の運用上の課題について考察する．

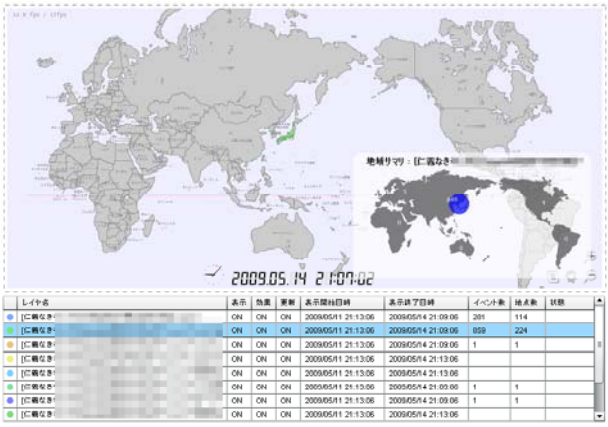


図 9：ハザードマップ

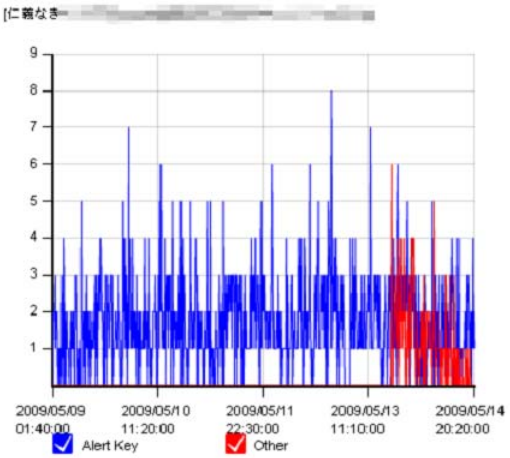


図 10：拡散状態の時系列表示

(1) 注意喚起メッセージキーの除外操作について

注意喚起メッセージキー送付において，P2P 利用者に対する注意喚起とファイルダウンロード抑止を両立させることが難しい状況が発生する場合がある．例えば，ファイルダウンロードを試みる P2P 利用者に注意喚起メッセージキーの特徴が知られてしまうと，その特徴をもつキーを除外することで，ファイルをダウンロードできてしまう可能性は高まってしまう．このような場合には，表 1に示すように注意喚起メッセージキーと抑止キー(トリップに注意喚起メッセージを格納しないキー)を併用するなどの解決策が必要となる．

表 1：注意喚起メッセージキーと抑止シーの役割分担

分類	用途
注意喚起メッセージキー	P2P 利用者への注意喚起を目的としたキーとして利用する．
抑止キー (トリップに注意喚起メッセージを格納しないキー)	ファイルダウンロード抑止を目的としたキーとして利用する．特徴を持たせないことにより，除外するという操作をさせにくい状況を作り出す．

(2) 注意喚起メッセージキーの注目度について

表 2に示すように抑止キーと通常キーには，注意喚起メッセージキーと通常キーのような違いがない．このため，P2P 利用者が抑止キーの流通状況を把握することはできない．一方，注意喚起メッセージキーの場合には，ファイルのダウンロード抑止に加え，注意喚起と対策実施中であることを P2P 利用者に提示できる反面，これが制約となる場合がある．例えば，特定の情報漏えいファイルを注意喚起対象とした場合，ファイルダウンロードを試みる P2P 利用者の興味を引き，かえって偏った注目度を高めてしまう．このような場合には，偏った注目度を高めないよう注意喚起メッセージキーを対象となるファイルならびに関係性のあるファイルに対して一律送付するなどの工夫が必要となる．

表 2：各種キーの比較

項目	注意喚起メッセージキーの場合	通常キーの場合	抑止キーの場合
IPアドレス	133.145.43.13	133.145.43.13	133.145.43.13
ポート番号	3456	3456	3456
ファイルサイズ	1575535	1575535	1575535
ファイル名	[仁義なき…]Admin	[仁義なき…]Admin	[仁義なき…]Admin
ハッシュ値	1096a7984ffd6c…	1096a7984ffd6c…	1096a7984ffd6c…
トリップ	StopFileDL	Kaxm9pWJTh	Kaxm9pWJTh
更新日	2009-01-11 04:24	2009-01-11 04:24	2009-01-11 04:24

4 おわりに

本稿では，P2P 利用者に「該当するダウンロードファイル削除のお願い」「ウイルスファイルの可能性あり」など意図するメッセージを直接流すことで，P2P 利用者への注意喚起を図りつつ，ファイルのダウンロード抑止措置を支援する注意喚起メッセージングシステムについて提案した．

今後は，本提案システムの実装を進め，注意喚起メッセージキー送付の効果測定の実施ならびに，考察で提示した運用上の課題解決を図っていく．さらに，注意喚起メッセージングシステムを情報漏えい対策に応用し，情報漏えいの対策猶予時間に幅を持たせるシステムの実現を検討していく予定である．

謝辞

本研究は総務省から受託した「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」の成果の一部です．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) 寺田真敏 他：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，情報処理学会 CSEC 研究報告 No.21 pp.243-248(2008 年 3 月)
2) 松岡正明 他：P2P ファイル交換ソフトウェア環境におけるノード型情報流出防止機能の提案，情報処理学会 CSEC 研究報告 Vol.2008, No.71, pp.115-122(2008 年 7 月)
3) 松木隆宏 他：IP マーキングによる不正活動ホストの広報機能の開発，情報処理学会 CSEC 研究報告 Vol.2008, No.71, pp.323-328(2008 年 7 月)
4) Napster, http://www.napster.com/
5) N. Christin and et al., "Content Availability, Pollution and Poisoning in Peer-to-Peer File Sharing Networks", ACM E-Commerce Conference (2005). http://p2pecon.berkeley.edu/pub/CWC-EC05.pdf
6) J. Liang and et al., "Pollution in P2P File Sharing Systems", Proc. of IEEE INFOCOM (2005). http://cis.poly.edu/~ross/papers/pollution.pdf
7) Xiaosong Lou and et al., "Proactive Content Poisoning To Prevent Collusive Piracy in P2P File Sharing", IEEE TRANSACTIONS ON COMPUTERS, TC-2007-09-0492R2(2008) http://gridsec.usc.edu/files/publications/IEEE-TC2007-09-0492R2-finalized-April8-2008.pdf
8 Uichin Lee and et al., "Understanding Pollution Dynamics in P2P File Sharing", In Proceedings of the International Workshop on Peer-to-Peer Systems (2006). http://rose.cs.ucla.edu/~cho/papers/lee-iptps.pdf
9) 吉田雅裕，大坐畠智，川島幸之助, "P2P ファイル共有ネットワークにおけるファイル ID 検索に対応したポイゾニング手法の提案"，信学技報, Vol. 108, No.31, NS2008-9, pp.49-54(2008 年 5 月)
10) 吉田雅裕，大坐畠智，中尾彰宏，川島幸之助, "Winny ネットワークにおけるインデックスポイズニングの適用と評価"，信学技報, Vol.108, No.203, NS2008-58, pp.93-98(2008 年 9 月)
11) Winny ファイル拡散防止サービス, http://forensic.netagent.co.jp/winny_kakusan.html
12) 情報拡散対策サービス, http://www.sosus.co.jp/b_expansion.htm
13) Winny ファイル拡散防止サービス公開実験, http://forensic.netagent.co.jp/winny_jikken.html
14) Prolexic Technologies: "P2P DDoS Attacks", (2007-05-14) http://www.prolexic.com/content/moduleId/tPjJLKRF/article/aRQNVcBH.html
15) J. Liang, N. Naoumov and K. Ross, "The index poisoning attack in P2P file-sharing systems", Proc. Infocom (2006). http://cis.poly.edu/~ross/papers/poison.pdf
16) N. Naoumov and K. Ross, "Exploiting P2P Systems for DDoS Attacks", Proc. of INFOSCALE (2006) http://cis.poly.edu/~ross/papers/p2pddos.pdf
17) 寺田真敏 他：P2P ファイル交換ソフトウェア Winny を対象としたオーバーレイネットワークの制御実験，情報処理学会 CSEC 研究報告 Vol.2009-CSEC-45 No.22 (2009 年 5 月)