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

2008－CSEC－42（17）
2008 / 7 / 24

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

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

[†1)] （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
[†2)] （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

概要：近年，P2P ファイル交換ソフトウェア環境を悪用したマルウェアなどにより，個人あるいは組織の機密情報が流出する事象が続発し，社会へ悪影響を与えている．本稿では，P2P ファイル交換ソフトウェア環境において，マルウェアによる感染ノードの活動や利用者の誤った操作によって，ノードから機密情報が流出する課題を考察する．次に，P2P ファイル交換ソフトウェア環境のノードを介して，機密情報が流出することを防ぐ対策として，アップロード用フォルダを常時監視して格納されたファイルが流通可能な情報か判定することで，意図しないファイルアップロードを防ぐ方式を提案する．また，提案手法を実装したプロトタイプシステムの評価を通して提案方式の有効性を示す．
キーワード：P2P，情報流出，マルウェア

Information Leakage Prevention Function of host based for P2P File Exchange Environment

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

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

Abstract: Recently, there are many incidents to which the classified information of the individual or the organization flows out in succession with the malware on the P2P file exchange software environment, and the society is affected negatively.In this paper we propose the information leakage prevention function which resolves the problem to which the classified information leaks by the malawre infection activity or the operational error of user.Our proposal is the permission mark method which allows the file circulation on the P2P file exchange software environment, and detects the files without permission.Also we implemented a prototype system to show the validity of our approach.
Key words: P2P, Information Leak, Malware

1　はじめに

人々が生活する上で利便性を向上するため，IT やインターネットは広く深く社会へ行き渡り，今も進化を続けている．それに伴い近年は情報流出事件が数多く発生している．例えば，新聞やインターネットニュースで報道された個人情報流出インシデントがまとめられた文献1）では，2005 年の個人情報流出インシデントの発生件数が 993 件，その中で P2P ファイル交換ソフトウェアによるインシデントが 178 件と 2005 年に発生した個人情報流出インシデントの約 18%を占めていたと報告している．本稿では，P2P ファイル交換ソフトウェア環境で個人／機密情報流出の発生を防ぎ，さらに，安心して利用できるようにするためのノード型の情報流出防止機能を提案する．提案方式は，アップロード用フォルダを常時監視して格納されたファイルが流通可能な情報か判定することで，意図しないファイルアップロードを防ぐ方式である．また，提案手法を実装したプロトタイプシステムの評価を通して提案方式の有効性を示す．

2　関連研究

本章では，P2P ファイル交換ソフトウェアに関する状況把握のため被害原因の調査研究，被害原因の整理，近年の情報流通対策を述べる．

2.1　被害原因に関する調査研究

(1) P2P ファイル交換ソフトウェアの利用状況

2007 年 9 月にインターネットユーザに対して Web アンケートを実施した文献2) では，利用されているファイル交換ソフトとして「Winny」や「LimeWire」など，多数のソフトが存在することを報告している（表 1）．

表1 ファイル交換ソフトの利用状況

ファイル交換ソフト名	利用率（%）
Winny	27.0
LimeWire	18.8
WinMX	15.0
Cabos	13.1
Share	11.0
BitTorrent	7.4
Freenet	2.8
Kazaa	0.5
PerfectDark	0.4
その他	4.1

また，P2P ファイル交換ソフトウェアを利用してファイルをダウンロードした経験のあるファイルのジャンルの中で情報流出ファイルとして 5.8 ファイル，更に共有経験のあるファイルとして情報流出ファイルが 3.7 ファイルという数値も出ている．これらアンケートの結果は，少なからず，個人／機密情報の収集や流通を目的とした利用者が存在することを示している．

(2) 流出する情報

文献3)（調査対象期間：2007 年 1 月～12 月）では，国内の企業／自治体に対して郵送調査法を用いた情報セキュリティ事象被害状況の調査が行われており，ファイル交換ソフトを介して流出した情報が「社内の業務情報」および「顧客（個人）情報」いずれも約半数，自治体では約 7 割が「顧客（個人）情報」であると報告している（図 1，図 2）．

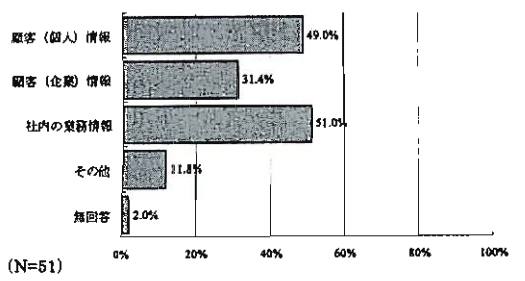

図1：流出情報の種類　（出典：（独）情報処理推進機構）

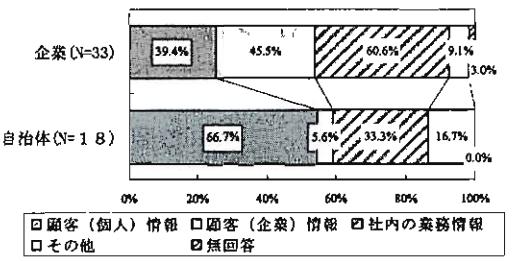

図2：流出情報の種類 企業／自治体別　（出典：（独）情報処理推進機構）

(3) ウイルス感染経験と感染手法

2007 年 9 月にインターネットユーザに対して Web アンケートを実施した文献4) では，ファイル交換ソフトウェアによるウイルスダウンロード・感染経験として，ウイルスをダウンロードしたことがあるが 44%，ウイルスに感染したことがあるが 15%と報告している（図 3）．これらファイル交換ソフト利用者の半数弱がなんらかの形でウイルスの流通に関与していることになり，感染したウイルスによる情報流出が決して稀な事象ではないと推測できる．ウイルスを実行される手法について報告している文献5) によれば，自爆型や求めたファイルかを確認するため exe 拡張子ファイルを実行してしまう形態だけではなく，アイコンを偽装する，RLO（Right to Left Override）を利用して exe 拡張子を視覚的に偽装する，ISO ファイル（CD／DVD）に埋め込んでおくなど感染させるための様々な手段が講じられていると述べており，ウイルス感染の回避が困難になってきている．

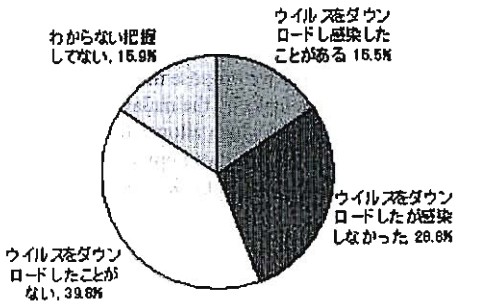

図3：ファイル交換ソフトによるウイルスダウンロード・感染経験 全体

(4) 暴露型ウイルス

文献6) 7) 8) 9) では，P2P ファイル交換ソフトウェアを媒介して，ノードに感染し，情報流出を引き起こす暴露型ウイルス Antinny について報告している．

Antinnyの主な発症活動は，次の通りである．

- 自己複製およびアップロード

自己（Antinny）と同一の機能を持ったファイルを複製し，自ノード内のファイル交換ソフトのアップロード用フォルダに，当該ファイルを格納することで自己を拡散させる．

- 個人デスクトップ画像のアップロード

自ノードのデスクトップ画面を画像キャプチャし人気のオーディオソフトなどのファイル名をつけてファイル交換ソフトのアップロード用フォルダに格納する．結果として，個人情報の流出につながっている．

- 個人／組織資料のアップロード

自ノードのハードディスク内からWindows用オフィスソフトウェアのファイルを収集してファイル交換ソフトのアップロード用フォルダに格納する．流出対象となるファイル拡張子は表2の通りであり，個人情報や組織の機密情報の流出につながっている．

表2 流出対象となるファイルの拡張子

拡張子名	概要
doc	文書ファイル
xls	表計算ファイル
ppt	プレゼンテーションファイル
mdb	データベースファイル
eml	メールファイル
dbx	メールファイル

2.2 被害原因の整理

被害原因に関する調査研究に基づき，P2Pファイル交換ソフトウェア環境を対象に，情報流出の被害原因の整理する．

(1) 情報流出の要因（何が）

「ウイルス感染経験と感染手法」の調査結果から，P2Pファイル交換ソフトウェア利用者が，巧妙かつ様々な手法により暴露ウイルスAntinnyに感染するに至ったことが，情報流出の最大の要因と考えられる．

(2) 流出の対象となる情報（何を）

「暴露型ウイルス」の調査結果から，Antinnyによる不正な動作が，個人や組織の機密資料やデスクトップ画像ファイルを流出させていること，さらに，情報流出の対象は特定の拡張子ファイルだけではないと言える．

2.3 近年の情報流出対策

P2Pファイル交換ソフトウェア環境を介して他ノードに流出拡散した情報を完全に削除するのはファイル交換ソフトの機能的および物理的にもほぼ不可能である．このため，ネットワーク，ノード，ユーザという各レベルでの予防的な情報流出対策が取られている．

(1) ネットワークレベルでの対策

ネットワークレベルでの対策としては，UTM[10]やIDP[11]などのネットワーク機器を用いてファイル交換ソフトの通信を検知し遮断する方法がある．

(2) ノードレベルでの対策

ノードレベルでの対策はAntinnyの削除対策であると言え，ファイル交換ソフトを媒介とするAntinny専用に検知・削除をするツールやアンチウイルスソフトでの検知・削除による対策が主流となっている[12][13][14][15]．

(3) ユーザレベルでの対策

ユーザレベルでの対策は，組織内や社内でのファイル交換ソフトの利用やインストールを禁止する方法であり，近年多くの組織がユーザレベルでの対策を推進している．

上述した対策は，情報を流出させないという点で有効な手段に成り得る．しかし，本研究の目的は，P2Pファイル交換ソフトウェアの利用を促進しつつ，利用者が安全に，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にある．次章以降，目的を達成するための方式として，ノードレベルの対策であり，流出対象となる情報に着目したノード型情報流出防止機能について述べる．

3 情報流通対策アーキテクチャ

本章では，提案するノード型情報流出防止機能が前提とする情報流通対策アーキテクチャ[16]について概説する．

情報流通対策アーキテクチャは，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統合的に推進するための枠組みであり，次に示す5つの機能部品から構成されている(図4)．

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．

②クローリング調査／ダウンロード調査

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．

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．

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．

本稿で提案するノード型情報流出防止機能は，④項のファイル流出の防止のうち，端末側で意図しないファイル流出を検出し，遮断する役割を担う．

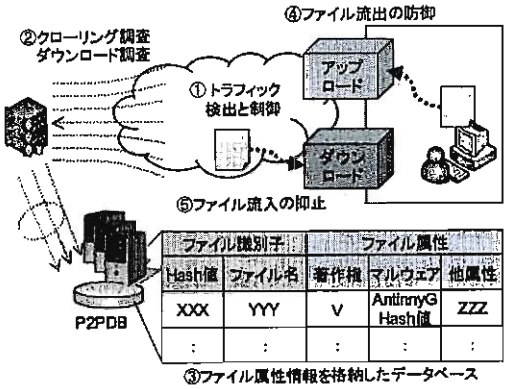

図4：情報流通対策アーキテクチャの機能部品

4 ファイル流出の防止

本章では，ファイル流出の防止を実現にあたっての機能要件と，実現方式について述べる．

4.1 機能要件

調査結果と被害原因に基づき，機能要件を整理すると次の通りとなる．

要件1：個人／機密ファイルの検知
P2Pファイル交換ソフトウェアによって，個人／機密情報ファイルがアップロードされる兆候を検知した場合，当該ファイルを隔離してファイルの流出を回避すること．
要件2：個人／機密ファイルの保護
隔離したファイルは不正なプロセスから操作できないように保護すること．
要件3：汎用性のあるツール
一つのP2Pファイル交換ソフトウェアに特化した流出防止機能として限定せず汎用性を持った設計にすること．

要件1は被害原因の整理に挙げた情報流出の要因を解決し，要件2は被害原因の整理に挙げた流出の対象となる情報に対処するための要件である．要件3はWinnyやShareなど特定のファイル交換ソフトに依存することなく，汎用性を高めるための要件である．

4.2 実現方式

要件1～3を満たす実現方式として，P2Pファイル交換ソフトウェアのアップロード用フォルダを常時監視し，格納されたファイルが流通可能な情報か判定する方式を採用した．また，格納されたファイルが流通可能な情報かの判定にあたっては，ファイルにマークを付与すると共に，流通させたいファイルのマークを管理する方式とした．

(1) マークの付与方式
マークの付与方式として，事前にファイルの要約をマークとして扱い，別途管理ツールで記録し，ファイル流通処理前にファイルと記録した要約を照合して流通の可否を判定する．これにより，既存ファイルに変更を加えることなく流通の可否判定が可能となる．

(2) マークの管理方式
付与したマークの管理方式としては，P2Pファイル交換ソフトウェア環境に流通させたくないファイルを管理するブラックリスト方式と，流通させたいファイルを管理し，それ以外を流通させたくないファイルとするホワイトリスト方式が考えられる．この2案を比較した結果，意図しない動作により生成されたファイルも流通させたくないファイルとして保護でき，結果として意図しないファイルアップロードを実現できることから流通させたいファイルを管理するホワイトリスト方式を採用した．

4.3 情報流出防止の処理の流れ

本節では，ファイルにマークを付与すると共に，流通させたいファイルのマークを管理することで情報流出防止を実現する処理について述べる（表3）．

表3 情報流出防止の実現方式

(1) アップロードフォルダの監視
↓
(2) ファイルの流通判定
↓
(3) 流出ファイル検知の通知

(1) アップロードフォルダの監視
アップロードフォルダの監視は，流通させたくないファイルがファイル交換ソフト固有のフォーマットに変換され，P2Pファイル交換ソフトウェア環境で拡散する前に保護することにある．このために，まずファイル交換ソフトのアップロードフォルダをファイルシステムフィルタドライバによって監視し，当該フォルダ内にファイルが新規作成または移動されたことを検知する．さらに，流通させたくないファイルがファイル交換ソフトにより，固有のフォーマットに変換されないよう別フォルダへ移動して，ウイルスなど不正なプロセスからファイルを保護す

る．

(2) ファイルの流通判定

ファイルの流通判定は，流通させたいファイルと，それ以外とを区別することにある．処理の流れは次の通りである．

- 事前に流通させたいファイルからファイル内容の要約を算出して流通許可リストとして記録する．
- 項番 (1) により隔離されたファイルからファイル内容の要約を算出し流通許可リストと照合する．なお，ファイルの識別方法は，ファイル内容の要約としてファイルハッシュ値を利用する．「ハッシュ値」とは，ドキュメントや数字などの文字列から一定長のデータに要約するための関数・手順を用いて算出した値で，本実装では「SHA-1」ハッシュ関数を利用して「ファイルハッシュ値」を算出する．
- 隔離されたファイルからファイルハッシュ値を算出し流通許可リストと照合して流通可能かを判定する．流通許可リストにファイルハッシュ値が存在しない場合は「流通拒否」と判定し隔離フォルダ内のファイルは保護したままとする．逆にファイルハッシュ値が存在した場合は「流通許可」と判定し隔離フォルダからアップロードフォルダへファイルを再配置する．

(3) 流出ファイル検知の通知

ファイルの流通判定により，流通させたくないファイルとして判定した場合は利用者へ意図しない情報流出の危険性がある旨を通知して，利用者に警告および対処を促す．

5 実装

本章では，実現方式で述べた処理のポイントとなるアップロードフォルダ監視機能およびファイル隔離機能の実装について述べる．

アップロードフォルダ監視機能とファイル隔離機能の実装に際して，IFS (Installable File System) Kit を活用し，minifilter タイプのドライバとすることでファイル入出力 (I/O) 要求のフィルタリングを可能とした (図 5)．

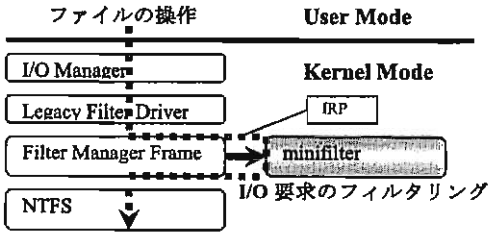

図5 実装の機能ブロック図

商品名称等に関する表示
IFSKit および minifilter は Microsoft Corporation の米国およびその他の国における登録商標または商標です．

5.1 アップロードフォルダ監視機能

アップロードフォルダ監視機能の役割は，アップロード用フォルダ内にファイルが移動／作成された直後に，当該ファイルを隔離フォルダ内に移動することにある．この役割を実現するために，コールバック関数に I/O 要求を登録し (表 4)，ファイルシステムが処理する前に I/O 要求をフィルタリングする仕組みとした．

表4コールバック関数に登録する IRP

IRP:I/O Request Packet	監視対象処理
IRP_MJ_CREATE	ファイルの新規作成を監視
IRP_MJ_SET_INFORMATION	ファイルの移動を監視
IRP_MJ_CLEANUP	ファイルのクローズを監視

具体的には，アプリケーションからファイル I/O 要求が生じた際に発行される I/O 要求パケット (IRP:I/O Request Packet) がファイルシステムによって処理される前にコールバック関数で，新規作成や移動先のファイルパスをフックする．ファイルパスがアップロードフォルダ以下の場合，IRP を変更するコールバック関数を呼ぶ設定をする．

IRP を変更するコールバック関数は，表 5に示す条件が満たすとファイル移動する関数を利用してファイルを隔離フォルダへ移動する処理を行う．ファイル移動する処理は，隔離フォルダパスと I/O 対象のファイル名を連結した移動先パスへファイルを移動する．

表5 ファイル移動処理を行う条件

IRP	条件
IRP_MJ_CREATE	ファイルシステムによるファイルの新規作成
IRP_MJ_SET_INFORMATION	ファイルシステムによるファイルの移動処理

5.2 ファイル隔離機能

ファイル隔離機能の役割は，隔離フォルダに対する読み書きを許可された信頼するクライアントプロセスのみに制限し，隔離されたファイルを保護することにある．

具体的には，コールバック関数で取得した I/O 要求の対象ファイルパスが隔離フォルダ以下であるかを判定する．I/O 要求を出しているプロセス ID と，信頼されたクライアントプログラムのプロセス ID を取得して，信頼するプロセスか照合し判定する．信頼するクライアントプログラムからの I/O 要求であれば処理を完了する．信頼するクライアントプログラムでない場合は，IRP を変更するコールバック

関数を呼び I/O 要求を拒否することで，隔離フォルダ以下のファイル保護を可能とした．

6 検証

本章では，提案方式およびその実装の有効性を情報流出の防止機能に焦点をあてた要件 1 ならびに 2 について実施した．なお，要件 3 の検証については今後の課題である．

6.1 検証内容

本節では，各要件に対する検証方法を述べる．

検証①（要件 1 の確認）

ノード上で Winny を起動し，アップロード用フォルダを登録する．同一ノード上でアップロードフォルダ監視機能を利用して当該フォルダを監視しつつ検体を実行する．利用する検体は，特定のアップロードフォルダ内に自身と同じ機能を持った exe 拡張子ファイルを生成しアップロード用フォルダに配置する動作を行う．本機能が監視するアップロード用フォルダ内に検体がファイルを配置したことを検知して隔離することでファイル流出の防止が実現可能かを検証する．なお，プロトタイプでは，検体によって追加されたアップロード用フォルダの監視機能は実装していないため検証の対象外である．

検証②（要件 2 の確認）

(1) 不正なプロセス

通常のログインユーザを不正なプロセスとして，フォルダ表示用の GUI 操作により隔離フォルダ内の閲覧する．さらに当該フォルダ内のファイルの移動や削除などの操作を試み，ファイル操作が拒否されることを確認する．

(2) 信頼するプロセス

情報流出防止機能のクライアントプログラムを信頼するクライアントプログラムとして，隔離フォルダ内のファイルを操作し，ファイル操作が行えることを確認する．

(1)，(2) により信頼するプロセス以外からファイルを保護することが実現可能かを検証する．

6.2 検証環境

検証には，Windows XP Proffessional SP2 が稼動する仮想マシン環境を準備した．

(1) プラットフォーム

- VMware Server
- OS:Windows XP Proffessional SP2

(2) P2P ファイル交換ソフトウェア

- ソフトウェア名：Winny v2.0b7.1 (03/11/16)
- アップロード用フォルダ：C:¥Winny2¥Up

(3) 情報流出対策ソフトウェア

- ソフトウェア名：情報流出対策ソフトウェア
- アップロード用フォルダ：C:¥ Winny2¥Up
- 隔離用フォルダ：本ソフトのインストールフォルダ内に設置

(4) 検体

検証①で使用した検体は次の通りである．

- 検体数：217 ファイル
- 1 検体の実行時間は 3 分間
- 各検体を実行する毎に VMware のスナップショット機能を利用して，検体に感染していないノードを準備する
- 検体の提供元：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向けデータベースに携わる調査組織の協力により，2008 年 1 月～2 月の間に収集した検体の提供を受けた．

6.3 結果

(1) 検証①

アップロードフォルダ監視機能は，検体によって生成された exe 拡張子ファイルを検知および隔離フォルダに移動してファイルのキャッシュファイル化を防ぐ効果があった．本検証の集計で，217 検体の全てに対して本機能の効果があった．

(2) 検証②

ファイル隔離機能は，不正なプロセスによるファイル操作および隔離フォルダ内の閲覧を拒否した．また，信頼するクライアントプロセスによって，隔離フォルダ内のファイル操作が可能であることを確認した．

6.4 考察

検証結果①からファイル流出の防止が実現可能であり，要件 1 を満したと考える．また，検体をトレンドマイクロ社のオンラインスキャンを利用しウイルス名別に分類した結果を（表 6）に示す．内訳は Antinny 系ウイルスが 92.2%，ついで PE_PARITE.A が 6.9%であった．Antinny 系ウイルスの中でも WORM_ANTINNY.JB が 90%を占めており，WORM_ANTINNY.JB に対しての情報流出防止の高い効果が確認できた．PE_PARITE.A について文献 17）では，ファイル感染型とされ分類されており，文献18）では，PE_PARITE.A が Antinny に感染している検体を別のマルウェアに書き換える構造があると述べられている．このことから，Antinny の動作をする検体に対して感染したため，オンラインスキャンによって PE_PARITE.A として判定されたと推測する．

表6 同一効果の検体

検体のウイルス名	検体数
WORM_ANTINNY.JB	184
PE_PARITE.A	15
WORM_ANTINNY.BB	8
WORM_ANTINNY.JA	8
PE_BOBAX.AH	1
PE_FUNLOVE.4099	1

また，検証結果②から，信頼するクライアントプロセスのみが隔離フォルダ内の閲覧などの操作が可能であることから，要件2を満した．以上の2つの検証を通して，アップロード用フォルダを常時監視して格納されたファイルが流通可能な情報か判定することで，意図しないファイルアップロードを防ぐ方式の有効性を示したと考える．

7 おわりに

本稿では，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として，関連研究では，流出情報を利用目的としてダウンロードしている人が存在しており，企業や自治体から流出した情報の大半が顧客情報や社内の業務情報であったことが分かった．被害原因の整理では，情報流出の要因として暴露型ウイルスのAntinnyが影響として大きく，流出の対象となるファイルの特定が困難なことが判明した．近年の情報流出対策としてネットワークやノード内のAntinnyなどの対策が主流となっており，情報流通対策アーキテクチャにある，流出の対象となるファイルに視点を置いた「ファイル流出の防止」を採用し，個人／機密ファイルの検知，個人／機密ファイルの保護，汎用性のあるツールの3点を機能要件と定義した．実現方式には，アップロードフォルダの監視，ファイルの流通判定，流出ファイル検知の通知を処理の流れとして，アップロードフォルダ監視機能およびファイル隔離機能を実現するべくファイルシステムフィルタドライバで実装し，I/O要求のフィルタリングをする仕組みとした．要件1・2を満たす確認のため，検体を用いた検証を実施して，「ノード型情報流出防止機能」の有効性を確認した．現在のネットワークやノード内のAntinny対策と本機能を組み合わせることで，より高い情報流出対策が施せると考える．

今後の課題は，P2Pファイル交換ソフトウェア環境において，ファイル流入の抑止機能の実現および有効性の検証がある．

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) NPO 日本ネットワークセキュリティ協会：2006年 情報セキュリティインシデントに関する調査報告書 Ver. 02.1 付録3.Winnyインシデント解説(2007年10月)
2) 社団法人コンピュータソフトウェア著作権協会：第6回「ファイル交換ソフト利用実態調査」 アンケート調査実施時期：2007年9月14日～9月25日クローリング調査実施時期：2007年9月28日17:00～29日17:00(24時間)（2007年12月）
3) (独)情報処理推進機構：2007 年 国内における情報セキュリティ事象被害状況調査(2008年4月)
4) 株式会社 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（2008年1月）
5) 小山覚：Winnyネットワークはやっぱり真っ黒，NTTコミュニケーションズの小山氏に聞く(2007年4月)
http://itpro.nikkeibp.co.jp/article/Interview/20070413/268234/?P=1&ST=security
6) マイクロソフト株式会社：Winnyによる情報漏えいへの対策
http://www.microsoft.com/japan/business/industry/gov/register.mspx
7) トレンドマイクロ株式会社：WORM_ANTINNY.G
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?VName=WORM%5FANTINNY%2EG
8) 株式会社シマンテック： W32.Antinny.BF
http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2006-041916-3437-99&tabid=2
9) マカフィー株式会社：W32/Antinny.worm
http://www.mcafee.com/japan/security/virA2003.asp?v=W32/Antinny.worm
10) シスコシステムズ合同会社：Cisco ASA 5500 シリーズ対応 UTM 24+
http://www.cisco.com/web/JP/event/campaign/fy07q1jsoc/index.html
11) ジュニパーネットワークス株式会社：ジュニパーネットワークスのWinny・Share対策ソリューション
http://juniper.co.jp/support/winny
12) 財団法人日本データ通信協会テレコム・アイザック推進会議
https://www.telecom-isac.jp/antinny/measure/index.html
13) トレンドマイクロ株式会社：Winnyによる情報漏えい対策
http://jp.trendmicro.com/jp/threat/solutions/winny/
14) 株式会社シマンテック：Winnyによる情報漏えいについて
http://www.symantec.com/region/jp/winny/winny_tools.html
15) マイクロソフト株式会社：悪意のあるソフトウェアの削除ツール

http://www.microsoft.com/japan/security/malwareremove/default.mspx
16) 寺田真敏，鬼頭哲郎，仲小路博史，松木隆宏，松岡正明：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（2008 年 3 月）
17) トレンドマイクロ株式会社：PE_PARITE.A 概要
http://www.trendmicro.co.jp/vinfo/virusencyclo/default5.asp?Vname=PE_PARITE.A
18) ITmedia エンタープライズ：プロが語るボットネット対策の特効薬は「情報共有」(3/3)
http://www.itmedia.co.jp/enterprise/articles/0704/29/news002_3.html