情報処理学会論文誌　Vol. 51　No. 9　1645–1658 (Sep. 2010)

P2P ファイル交換ソフトウェア環境における クライアント型情報流通対策システムの提案

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]

P2P ファイル交換ソフトウェアから構成される P2P ネットワークにおいて，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．P2P ファイル交換ソフトウェアの利用を促進しつつ，利用者が安全にファイル交換ソフトウェアを利用できる環境を実現するためには，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必要がある．本論文では，P2P ネットワークにおいて，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 P2P ファイル交換ソフトウェア向けのクライアント型情報流通対策システムを提案する．提案する方式は，P2P ファイル交換ソフトウェアのアップロードならびにダウンロード用フォルダを常時自動監視し，保護マークの付いていないファイルのみアップロード用フォルダに格納可能とし，ファイル属性情報を格納したデータベースに登録されていないファイルのみダウンロード用フォルダに格納可能する方式である．さらに，実装したプロトタイプの評価を通して提案方式の有効性を示す．

Information Distribution Control System of Host Based for P2P File Sharing Environment

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

Recently, problems regarding the P2P file sharing on the Internet are growing. To promote the safe use of P2P file sharing network while preventing information leak through virus infection and circulation of copyrighted materials, we should reconsider the way of the current P2P file sharing. In this paper, we propose the information distribution control system of host based for P2P file sharing environment, a client-based security measure that monitors the specific file folders used in P2P file sharing and prevents upload and download of copyrighted materials and malicious files by inspecting and filtering what can be put in the folders. The effectiveness of the approach obtained with the prototype system is also presented.

1. はじめに

P2P（Peer to Peer）ファイル交換ソフトウェア利用が広がるなか，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流通による著作権侵害は続いており，その被害が顕在化している状況にある．独立行政法人情報処理推進機構の 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を悪用する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)]．文献 2) では，アンケート調査より，多くの利用者が 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．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[3)]．

本論文では，情報流出の懸念を解消し，利用者が安全に，安心して P2P ファイル交換ソフトウェアから構成されるネットワーク（以降，P2P ファイル交換ソフトウェア環境）を利用できるよう，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 P2P ファイル交換ソフトウェア向けのクライアント型情報流通対策システムを提案する．さらに，プロトタイプの評価を通して提案方式の有効性を示す．提案する方式は，P2P ファイル交換ソフトウェアの特定フォルダ，具体的にはアップロードならびにダウンロード用フォルダを常時自動監視する．アップロード用フォルダについては，自動監視により，保護マークの付いていないファイルのみ格納可能とする．また，ダウンロード用フォルダについては，ファイル属性情報を格納したデータベースに登録されていないファイルのみ格納可能とする方式である．

本論文の構成について述べる．2 章で P2P ファイル交換ソフトウェア環境における被害

†1 株式会社ラック
Little eArth Corporation Co., Ltd.
†2 株式会社日立製作所システム開発研究所
Systems Development Lab., Hitachi Ltd.

状況と，既存方式の概要と課題を示す．3 章で意図しないファイルの流出を防ぐための「マルウェアや利用者の誤操作によるファイルのアップロードの防止機能」と，持ち込まれたくないファイルの流入を防ぐための「不適切なファイルのダウンロードの抑止機能」を提案する．4 章で提案方式の実現方法を述べ，5 章で提案方式の有効性を示す．

2. 関 連 研 究

P2P 通信技術については，ネットワーク上のトラフィック分散を実現する技術として期待されている一方，国内で普及している P2P ファイル交換ソフトウェア環境は，著作権上適切ではないファイルやマルウェアファイルなどの流通基盤として利用されている状況にある．本章では，国内における P2P ファイル交換ソフトウェアの利用状況と，P2P ファイル交換ソフトウェア環境を対象とした意図しないファイルの流出や著作物流通に関する既存対策方式について述べる．

2.1 P2P ファイル交換ソフトウェア環境の利用状況

(1) P2P 利用者数と稼動ノード数

文献 4)（調査時期：2008 年 9 月）では，約 2 万名を対象としたアンケート調査結果から，ファイル交換ソフトウェアの利用者がインターネット利用者の 10.3%（2007 年 9 月の調査では 9.6%）となり，利用者増加を報告している．また，クローリング手法を用いて収集したデータをもとに Winny 稼動ノード数 18 万台以上（/日），Share 稼動ノード数約 20 万台以上（/日）と推定しており，それぞれ 9 割以上が日本からのアクセスであるとしている．

(2) ファイル流通状況

(a) 著作権侵害ファイル

文献 4)（調査時期：2008 年 9 月）では，Winny ネットワーク上のファイルは約 531 万 6 千件（/日）存在し，流通するファイル全体の約 50%が著作物，Share ネットワーク上のファイルは約 71 万 2 千件（/日）存在し，流通するファイル全体の約 56%が著作物と推定している．また，文献 5)（調査時期：2008 年 1〜2 月）では，Winny ネットワーク上に流通しているファイルの約 6 割強が著作物と推測されるファイルであることと，映像系ファイル（64%）が多く流通しており，そのほとんどが許諾がないと推測されることを報告している．

(b) マルウェアファイル

文献 5) では，Winny ネットワーク上ではマルウェア単体での流通は稀であり，9 割以上がアーカイブファイル（zip，lzh など）に混入して流通していること，収集したすべての zip，lzh，rar コンテンツ中，19.0%がマルウェアを含むコンテンツであることを報告している．

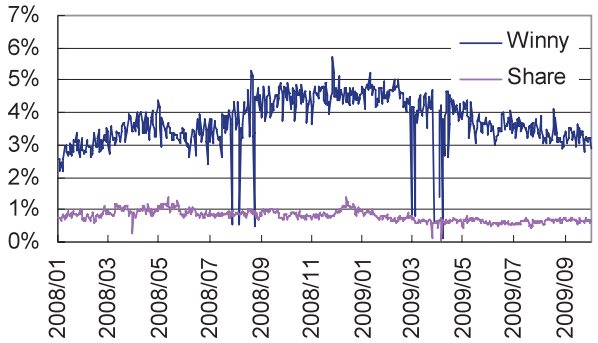


図 1　漏えいファイルの流通比率
Fig. 1　Ratio of the outflow file on Winny/Share network.

(c) 漏えいファイル

著者らのサンプリングによるクローリング調査によれば，マルウェア感染により発生した意図しない流出に見られる特徴的なファイル名のみを抽出した場合，Winny ネットワーク上には約 3.7%（/日），Share ネットワーク上には約 0.8%（/日）の漏えいファイルが流通していると推定される（**図 1**）．

2.2 既存対策方式

(1) 意図しないファイル流出の防止

事前措置としては，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[6]，一般情報と機密情報とを区別して，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[7] 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ことで，流出した情報を取得しにくくする方式がある．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 8)，9) がある．

実フィールドでの対策アプローチとしては，(a) 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，(b) 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，(c) 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，(d) 事後措置としての漏えい調査，風評被害対策などがある．

(2)　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 10) 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 11) 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 12) では，コンテンツにパーミッション情報を付与し，利用者のポリシに従って配信を行う方式を提案している．文献 13) 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 14) 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利用者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 15) 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，(a) ファイル自体を暗号化して，特定のデバイスやソフトウェアでのみファイルを利用できるように制限をかけるデジタル著作権管理，(b) 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とられている．

2.3　解決したい課題

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．著作権管理が必要となるファイルにはデジタル著作権管理，マルウェアファイルにはウイルス対策ソフトウェアの導入が流入抑止に有効ではあるが，いずれも，漏えいファイルの流入抑止までを適用範囲にしていない．また，デジタル著作権管理などによる方式は，事前措置として導入した場合には有効であるが，P2P ファイル交換ソフトウェア環境にすでに流通しているファイルに対しては，必ずしも適用できない．ウイルス対策ソフトウェアも，パターンとしてウイルス定義ファイルに登録されていない，P2P ファイル交換ソフトウェア環境への情報流出を引き起こす新たなマルウェアに対しては改善の余地がある．さらに，実用を考えた場合，情報流出を引き起こすウイルスがダウンロード時のチェックをすり抜けて端末内に入ってきたとしても，アップロード時のチェックで情報流出を防ぐなどの多重防御機構の導入は必須である．

本論文で提案するクライアント型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，主として情報流出の懸念と流出情報の拡散を解消し，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ため，次の 2 つの課題を解決することにある．

【課題 1】　意図しないファイルの流出の防止

【課題 2】　持ち込まれたくないファイルの流入の抑止

3.　クライアント型情報流通対策システムの提案

本章では，2 章で示した課題を解決するためのクライアント型情報流通対策システムについて述べる．提案方式は，**【課題 1】**の意図しないファイルの流出を防ぐための「マルウェアや利用者の誤操作によるファイルのアップロードの防止機能」と，**【課題 2】**の持ち込まれたくないファイルの流入を防ぐための「不適切なファイルのダウンロードの抑止機能」により課題解決を図る．

3.1　システム概要

(1)　前提とする P2P ファイル交換ソフトウェア

国内で普及している P2P ファイル交換ソフトウェアは，P2P ノード間の通信プロトコルは異なるが，ファイルのアップロードと，ファイルのダウンロードに関する実装には類似性がある．具体的には，P2P ファイル交換ソフトウェア環境にファイルをアップロードする際には，アップロード用フォルダ（以降，アップロードフォルダ）にファイルを格納する．ファイルをダウンロードする際には，ダウンロード用フォルダ（以降，ダウンロードフォルダ）にファイルを格納するという処理の流れがある．

提案方式は，この実装上の特徴に着目し，上述のフォルダを常時自動監視するというアプローチをとる．このため，アップロードするファイルを格納するためのアップロードフォルダと，ダウンロードするファイルを格納するためのダウンロードフォルダを有する P2P ファイル交換ソフトウェアを前提としている．

(2)　システムコンセプト

P2P ファイル交換ソフトウェア環境においては，マルウェア感染がファイル流出の主な原因となっている．このため，意図しないファイルの流出を防ぐには，アップロード時のファイルチェックに加え，ダウンロード時のファイルチェックによってファイルの流出を引き起こすマルウェアの侵入を阻止することが効果的である．すなわち，ダウンロード時とアップロード時のダブルチェックというチェックポイントの組合せによる多重防御が有効であると考える．また，端末に持ち込まれたくないファイルとしては，マルウェアだけでなく，著作権侵害ファイルや，他の端末から漏えいした機密ファイルなどがある．同様に，これらのファイルは端末からの流出を防ぐべきファイルでもあり，端末から外に出すべきではない．

このため，ダウンロード時およびアップロード時のファイルチェックは，既存のウイルス対策ソフトウェアによる単なるマルウェアチェックだけでは不十分であり，著作権侵害，情報漏えいなどとも組み合わせた多面的なコンテンツチェックが必須となる．すなわち，ウイルス対策ソフトウェア，デジタル著作権管理アプリケーションなどを連携させ，それぞれが独自に整備しているファイルチェック用データベース，たとえば，ウイルス対策ソフトウェアにおけるウイルス定義ファイルなどをすべて活用した形でファイルチェックを行わなければならない．

そこで，本論文で提案するクライアント型情報流通対策システムでは，アップロードならびにダウンロード用フォルダを常時自動監視するというチェックポイントの組合せを実装するとともに，これらのチェックポイントにおいては，コンテンツの種別ごとに管理されているファイルチェック用データベースとを連携させることによって，著作権侵害，マルウェア，情報漏えいなどの多面的なコンテンツチェックを実現していく．

次節以降，上述のシステムコンセプトに基づき，マルウェアや利用者の誤操作によるファイルのアップロードの防止機能を実現するアップロードフォルダ監視と，不適切なファイルのダウンロードの抑止機能を実現するダウンロードフォルダ監視について述べる（**図 2**）．

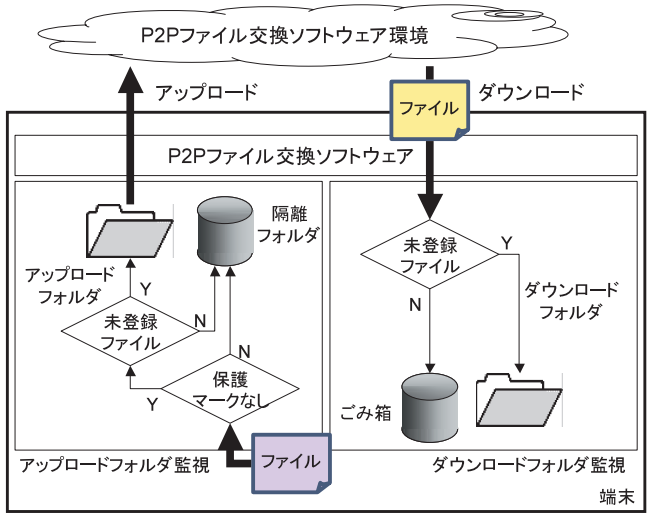


図 2　P2P ファイル交換ソフトウェアにおける情報流通対策システムの概要
Fig. 2　Overview of proposal P2P file exchange control system.

3.2　アップロードフォルダ監視

アップロードフォルダ監視は，端末内において，利用者が P2P ファイル交換ソフトウェア環境への流通を許可したファイルのみをアップロード可能とし，**【課題 1】**の意図しないファイルの流出を防ぐ．ここで，アップロードフォルダとは，P2P ファイル交換ソフトウェア Winny，Share，Cabos，LimeWire で利用するアップロード用のフォルダのことを指す．

(1)　機能要件

マルウェアや利用者の誤操作によるファイルのアップロード防止を実現するためにアップロードフォルダ監視に求められる機能要件は次のとおりである．

【機能要件 1-1】　端末から P2P ファイル交換ソフトウェア環境にファイルが流通する前に，アップロードフォルダに格納されたファイルを自動検出すること．次に，マルウェアの活動や利用者の誤操作によってアップロードフォルダに格納されたファイルか，利用者によって事前に公開を許可されたファイルであるか否かを判定すること．

【機能要件 1-2】　アップロードフォルダに格納されたファイルが，マルウェアや利用者の誤操作によるファイルであると判断した場合には，意図しないファイルの流出を防ぎ，利用者自身がファイルの内容を確認可能とするため，ファイルを一次退避させること．

(2)　機能概要

提案方式では，端末内に格納されているすべてのファイルを P2P ファイル交換ソフトウェア環境に流通してはならない保護マーク付きファイルとして取り扱う．このため，利用者が，該当ファイルを P2P ファイル交換ソフトウェア環境に流通させるためには，事前に該当ファイルを公開許可ファイルリストに登録し，保護マークをはずす．万が一，保護マーク付きファイルがアップロードフォルダに格納された場合には，マルウェア感染もしくは，利用者の誤操作で格納されたファイルであると判断し，ファイルをアップロードフォルダから一次退避させる．

(a) ファイル検出と判定

アップロードフォルダ監視のファイル検出と判定では，【機能要件 1-1】を満たすために，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ファイルが格納される操作を自動検出する．

次に，利用者が公開を許可したファイル（以降，保護マークなしファイル）であるか否かを公開許可ファイルリストと比較照会する．比較にあたっては，ファイルの内容を要約して算出するファイルのハッシュ値を使用する．具体的には，検出したファイルと，事前に公開許可ファイルリストに登録した保護マークなしファイルのハッシュ値とを比較することで，保護マークなしファイルか保護マーク付きファイルかを判定する．保護マーク付きファイ

表 1　P2PDB に登録されているファイルの属性情報
Table 1　Stored file profile in P2PDB.

ファイル属性	概要	保持に伴う問題点
著作権侵害ファイル	著作権利を持つ者の許諾を得ずアップロードされたファイル． 例：音楽，映像，ソフトウェア，書籍，画像など	利用者は当該ファイルを知らずに違法利用．第三者による利用されることで著作権利者の利益を害する．
マルウェアが混入するファイル	ファイルにマルウェアを含む，もしくはファイル自体がマルウェア． 例：Antinny	Antinny の場合，感染すると，利用者の個人情報漏えいに繋がる可能性がある．
情報漏えいの可能性があるファイル	マルウェアの活動や，利用者による誤操作によって流出した機密情報の可能性があるファイル． 例：個人情報，機密情報	第三者による機密情報の悪用や，個人のプライバシー侵害に繋がる可能性がある．

ルと判定した場合には，利用者が意図して格納したファイルでなく，マルウェア感染もしくは，利用者の誤操作で格納されたファイルであると判断する．

また，保護マークなしファイルについては，ファイルの属性情報を格納したデータベース（以降，P2PDB）[5] にコンテンツが公開にあたり適切か否かを照会する．なお，P2PDB には，**表 1** に示す属性情報のいずれかを有するファイル（以降，登録ファイル）が登録されており，これらのファイルは公開するのに不適切なファイルと判断する．

(b) ファイル退避

アップロードフォルダ監視のファイル退避では，【機能要件 1-2】を満たすために，ファイルが P2P ファイル交換ソフトウェア環境に送出される前に，ファイルをアップロードフォルダ以外に移動させる．具体的には，保護マーク付きファイルがアップロードフォルダに格納される操作を検出した場合，保護マークなしファイルが P2PDB に登録されていた場合には，該当ファイルをアップロードフォルダではなく，隔離フォルダに格納先を変更することで一次退避を実現する．これにより，意図しないファイルの流出を防ぎ，利用者自身がファイルの内容を確認可能とする．

3.3　ダウンロードフォルダ監視

ダウンロードフォルダ監視は，**【課題 2】**の持ち込まれたくないファイルの流入を抑止する．ここで，ダウンロードフォルダとは，P2P ファイル交換ソフトウェア Winny，Share，Cabos，LimeWire で利用するダウンロード用のフォルダのことを指す．

(1)　機能要件

無許諾な著作物，マルウェア，漏えいファイルなど，不適切なファイルのダウンロードの抑止を実現するためにダウンロードフォルダ監視に求められる機能要件は次のとおりである．

【機能要件 2-1】 P2P ファイル交換ソフトウェア環境から端末にファイルがダウンロードされたことを判定するために，ダウンロードフォルダに格納されたファイルを自動検出すること．次に，無許諾な著作物など所持するのに適切か否かを判定すること．

【機能要件 2-2】 ダウンロードフォルダに格納されたファイルが，所持するのに不適切であった場合には，利用者に警告をあげた後，削除すること．

(2)　機能概要

提案方式では，ファイルがダウンロードフォルダに格納される際に，ファイルの属性情報を格納したデータベースを活用して，所持するのに適切か否かを判定する．所持が不適切であった場合には，利用者に通知し，ファイルを削除する．

(a) ファイル検出と判定

ダウンロードフォルダ監視のファイル検出と判定では，【機能要件 2-1】を満たすために，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ファイルが格納される操作を自動検出する．次に，ファイルの属性情報を格納したデータベース P2PDB に所持するのに適切か否かを照会する．なお，P2PDB には，表 1 に示す属性情報のいずれかを有するファイルが登録されており，これらのファイルを所持するのに不適切なファイルとした．

(b) ファイル削除

ダウンロードフォルダ監視のファイル削除では，【機能要件 2-2】を満たすために，検出したファイルが登録ファイルであると判定した場合，ファイル削除確認を兼ね，取得したファイルの属性情報を利用者に通知する．利用者が削除確認した後，ファイルを削除する．これにより，ダウンロードの抑止の理由提示とともに，利用者自身がファイルの属性情報を確認可能とする．

4.　クライアント型情報流通対策システムの実装

本章では，Microsoft Windows XP 上に実装したアップロードフォルダ監視とダウンロードフォルダ監視機能のプロトタイプについて述べる．なお，今回はプロトタイプのため，P2PDB への照会は，ダウンロードフォルダ監視にのみ実装することとした．

4.1　アップロードフォルダ監視

(1)　実装要件

アップロードフォルダ監視に求められる実装要件は次のとおりである．

●提案方式を実現するための要件

【実装要件 1-1】 アップロードフォルダへのファイル格納操作を自動検出した後，ファイルを退避させること

【実装要件 1-2】 退避させたファイルの保護マーク有無を判定すること

【実装要件 1-3】 退避させたファイルが保護マークなしの場合は，アップロードフォルダにファイルを戻すこと

●提案方式の安全性を確保するための要件

【実装要件 1-4】 退避させたファイルをマルウェアや利用者から隔離すること

(2) 実装

プロトタイプの動作概要を**図 3** に示す．

(a) ファイル格納要求操作モジュール

ファイルの格納要求操作モジュールは，アップロードフォルダ内にファイルの作成や移動を検知した直後に，該当ファイルの格納先を隔離フォルダに切り替える（図 3 の ①②）．プロトタイプでは，フィルタドライバによる I/O 要求パケット（IRP: IO Request Packet）の監視と，監視対象の IRP を操作する実装とした．

マルウェア感染や利用者の誤操作などによるファイル操作は，ユーザモードからファイル操作に関連する CreateFile や MoveFile などの API 関数の呼び出しが行われる．これにともない，カーネルモードでは，NtReadFile や NtWriteFile などの対応するシステムコールが呼び出される．続いて，ファイル操作要求を受けた I/O マネージャが要求にあった IRP を発行する．ここで，IRP には，作成先，移動先，削除対象などのファイルパスが格納されており，この IRP をファイルシステムのドライバが処理することでファイル操作が実行される．ファイルの格納要求操作モジュールは，IRP がファイルシステムによって処理される前に FPFLT_PRE_OPERATION_CALLBACK 関数で，作成や移動先のファイルパスをフックする．

このファイルパスが，事前に登録された監視フォルダ設定のアップロード用フォルダ（**図 4**）に一致する場合には，IRP に格納されたファイルパスや属性などを変更する FltSetInformationFile 関数を使って，ファイル格納先をアップロードフォルダから隔離フォルダに変

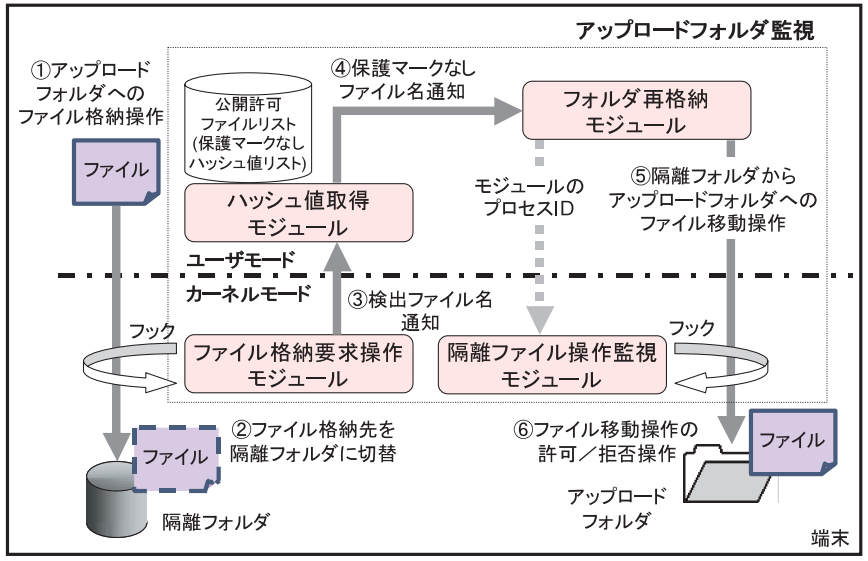


図 3 アップロードフォルダ監視の実装と IRP のフック概要
Fig. 3 Overview of upload folder monitoring and IPR hook.

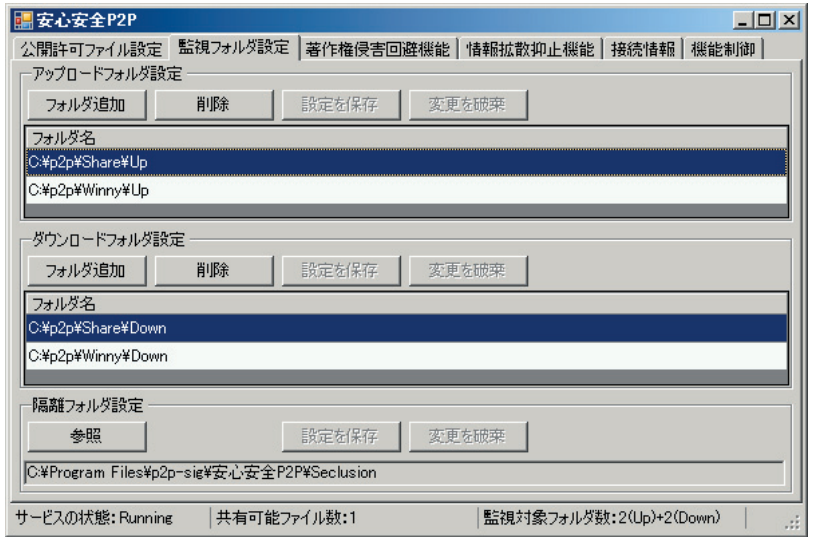


図 4 アップロードとダウンロードフォルダの設定画面
Fig. 4 Configuration of upload and download folder.

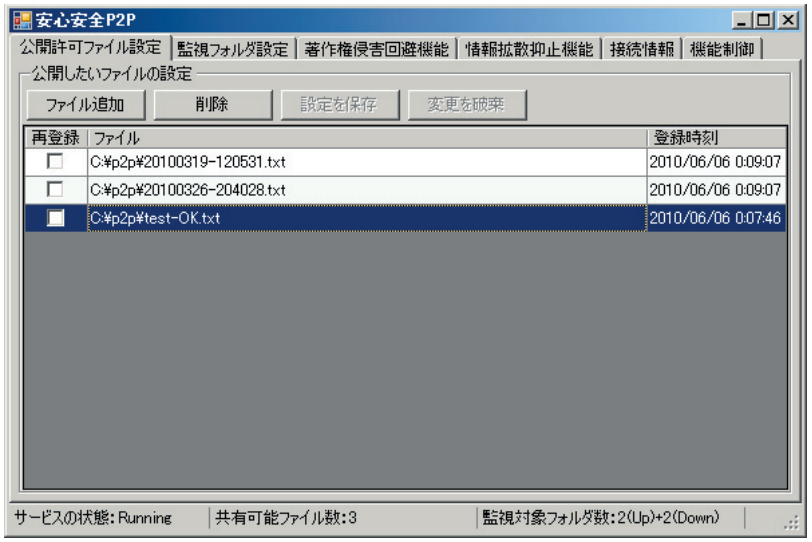


図 5　公開許可ファイルの設定画面
Fig. 5　Configuration of the public permission file.

更する．これにより，【実装要件 1-1】のアップロードフォルダの常時自動監視とファイル退避を実現した．

(b) ハッシュ値取得モジュール

ハッシュ値取得モジュールは，検出したファイルと，公開許可ファイルリストとして事前に登録した保護マークなしファイルのハッシュ値とを比較することで，保護マークの有無を判定する（図 3 の ③④）．P2P ファイル交換ソフトウェア環境に流通させたいファイルを公開許可ファイルリストに登録する画面を**図 5** に示す．利用者は，公開許可ファイル設定のファイル追加で該当ファイルを公開許可ファイルリストに登録することで，保護マークをはずすことができる．

本モジュールでは，ファイル格納要求操作モジュールが退避させたファイルに対して，ハッシュ値を算出する関数（Cryptography->ComputeHash）をかけた後，ハッシュ値を公開許可ファイルリスト，すなわち，保護マークなしファイルのハッシュ値リストと照会する．一致した場合は保護マークなしファイル，一致しなかった場合には保護マーク付きファイルと判定することで【実装要件 1-2】を実現した．

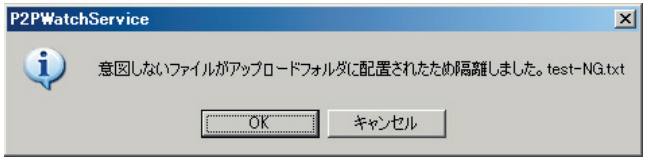


図 6　アップロードフォルダ監視ダイアログ
Fig. 6　The dialog of upload folder monitoring.

(c) フォルダ再格納モジュール

フォルダ再格納モジュールは，保護マークなしファイルと判定したファイルをアップロードフォルダに再格納する（図 3 の ⑤）．実装では，ハッシュ値取得モジュールが保護マークなしファイルと判定したファイルを，隔離フォルダからアップロードフォルダに移動することで【実装要件 1-3】を実現した．また，保護マーク付きファイルと判定した場合には，利用者に**図 6** に示すダイアログボックスで通知し，該当ファイルは，隔離フォルダに保持したままとする．

(d) 隔離フォルダ監視モジュール

隔離フォルダ監視モジュールは，ファイル格納要求操作モジュールが退避させたファイルに対するアクセス制限機構である（図 3 の ⑥）．隔離フォルダに退避させたファイルに対してファイル操作を信頼する本プロトタイプのプロセスからのみアクセス可能とすることで，退避させたファイルを安全に隔離する．実装では，FPFLT_PRE_OPERATION_CALLBACK 関数で取得した IRP のファイルパスが監視フォルダ設定の隔離フォルダ配下（図 4）にあるか否かを判定する．隔離フォルダ配下の場合には，次に，ファイル操作を要求するプロセス ID とプロトタイプのプロセス ID を照合し，合致すれば要求するファイル操作の IRP を処理完了させる．合致しない場合には，IRP を変更しファイルの操作要求を拒否することで【実装要件 1-4】を実現した．

4.2　ダウンロードフォルダ監視機能の要件と実装

(1)　実装要件

ダウンロードフォルダ監視に求められる実装要件は次のとおりである．

● 提案方式を実現するための要件

【実装要件 2-1】　ダウンロードフォルダへのファイル格納操作を自動検出すること
【実装要件 2-2】　検出したファイルの属性情報を P2PDB に照会すること
【実装要件 2-3】　登録ファイルである場合には利用者に通知すること

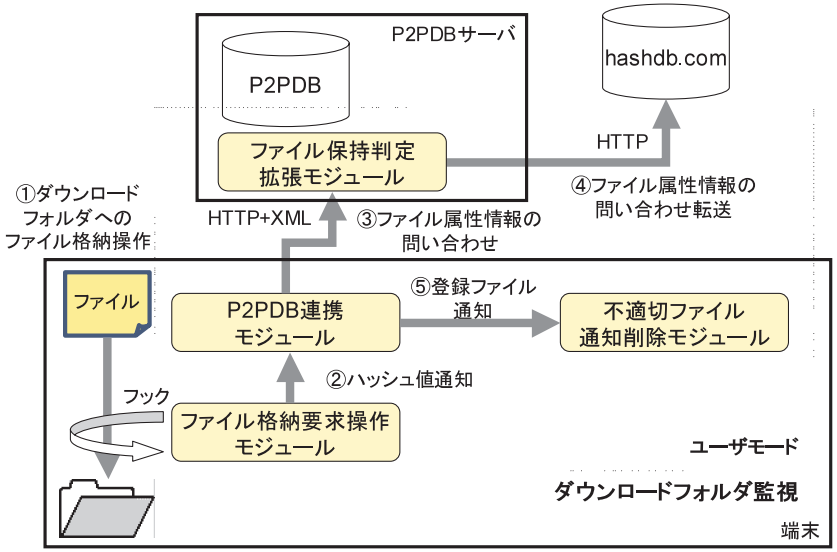


図 7　ダウンロードフォルダ監視の概要
Fig. 7　Overview of download folder monitoring.

● 提案方式の拡張性を確保するための要件

【実装要件 2-4】 検出したファイルの属性情報を P2PDB 以外の外部データベースに照会するよう拡張すること

(2)　実装

プロトタイプの動作概要を**図 7** に示す.

(a) ファイル格納操作検出モジュール

ファイル格納操作検出モジュールは，ダウンロードフォルダ内でのファイル作成を検知することで，P2P ファイル交換ソフトウェア環境から端末にファイルがダウンロードされたことを判定する（図 7 の ①）．実装には，フォルダ内のファイルの変化をイベントとしてあげる FileSystemWatcher クラスを使い，事前に登録された監視フォルダ設定のダウンロードフォルダ（図 4）に格納されたファイルを検出することで【実装要件 2-1】を満たした.

(b) P2PDB 連携モジュール

P2PDB 連携モジュールは，検出したファイルの属性情報を P2PDB に照会する（図 7 の ②③）．実装では，検知したファイルのハッシュ値を SHA-1 か MD5 で算出した後，**表 2** に示す要求形式で HTTP による P2PDB への問合せを行い，XML による応答形式でファイルの属性情報を受信することで【実装要件 2-2】を実現した.

表 2　P2PDB への要求/応答形式
Table 2　P2PDB request/response format.

要求形式	
URL	http://<Server>/p2pdb/getfileinformation.ashx? type=<hashtype>&hash=<hash value>
メソッド	Get
応答形式	
形式	XML
内容例	<?xml version="1.0" encoding="utf-8"?> <Resultset> <errorcode>0</errorcode>P2PDB エラーコード <mal_flg>1</mal_flg>マルウェア混入フラグ <rights_flg>0</rights_flg>無許諾著作物フラグ <leak_flg>1<leak_flg/>情報漏えい可能性フラグ <entry_date>yyyy/mm/dd</entry_date>登録年月日 </Resultset>

(c) ファイル所持判定拡張モジュール

ファイル所持判定拡張モジュールは，検出したファイルの属性情報を P2PDB 以外の外部データベースに照会するための拡張機構である（図 7 の ④）．プロトタイプで独自実装した P2PDB には，ファイル属性情報として約 2 万件保持している．しかしながら，P2P ファイル交換ソフトウェア環境で流通するファイルは，Winny ネットワークで約 530 万，Share ネットワークで約 70 万と推定され，P2PDB のみの情報量では持ち込まれたくないファイルの流入の抑止には不十分である．そこで，本モジュールでは，インターネット上の P2PDB 以外の外部データベースを活用しながら検知精度の向上を可能とする実装としている．なお，プロトタイプでは，P2PDB 以外の外部データベースとして，P2P ファイル交換ソフトウェア環境で違法なファイルの流通を抑止するためのデータベースである hashdb.com を参照することとした.

実装にあたっては，P2PDB にファイルが登録されていなかった場合には hashdb.com へ HTTP 通信で照会すること，P2PDB や hashdb.com 以外のデータベースへの照会を想定し，ファイルのハッシュ値アルゴリズムとして SHA-1 と MD5 を採用することで【実装要件 2-4】を実現している.

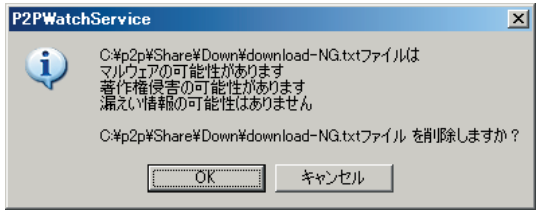


図 8　ダウンロードフォルダ監視ダイアログ
Fig. 8　The dialog of download folder monitoring.

(d) 不適切ファイル通知削除モジュール

不適切ファイル通知削除モジュールは，P2PDB 連携ならびにファイル所持判定拡張モジュールがダウンロードフォルダに格納されたファイルを登録ファイルとして判定した場合に，ファイル削除確認を兼ね，取得したファイルの属性情報を利用者に通知する（図 7 の⑤）．実装では，利用者に**図 8** に示すダイアログボックスで通知し，ファイル削除確認を促すことで【実装要件 2-3】を実現した．

5. 評価と考察

本章では，4 章で提示したプロトタイプを用いて，特定のフォルダを常時自動監視するというアプローチの有効性を検証する．

5.1 評価内容と評価環境

評価にあたっては，機能検証，マルウェア検体を用いた機能検証，ウイルス対策ソフトウェアとの共存性検証の 3 つの視点から実施した．

(1) 機能検証

プロトタイプで実装したアップロードフォルダ監視とダウンロードフォルダ監視が，機能要件ならびに実装要件を満たすかの検証（**表 3**）を通して，特定のフォルダを常時自動監視するというアプローチが P2P ファイル交換ソフトウェアに依存しない汎用的な方式であることを確認する．

評価環境では，検証用ファイルとして，保護マークなしファイル，保護マーク付きファイル，登録ファイル各 5 ファイルを用い，インターネットに接続した端末に OS として Windows XP Professional SP2，P2P ファイル交換ソフトウェア Winny v2.0b7.1，Winnyp 7.28 と Share EX2 による環境を構築した．

表 3　検証項目と結果
Table 3　Functional evaluation and result list.

#	検証項目	検証操作	確認要件		結果
1	利用者の正常操作を想定したアップロードフォルダへのファイル格納	保護マークなしファイルをアップロードフォルダに格納する．	【機能要件 1-1】	【実装要件 1-1】 【実装要件 1-2】 【実装要件 1-3】	○
2	利用者の誤操作を想定したアップロードフォルダへのファイル格納	保護マーク付きファイルをアップロードフォルダに格納する．	【機能要件 1-1】 【機能要件 1-2】	【実装要件 1-1】 【実装要件 1-2】 【実装要件 1-4】	○
3	不適切なファイルの取得を想定したダウンロードフォルダへのファイル格納	P2P ファイル交換ソフトウェア環境から登録ファイルを取得する．	【機能要件 2-1】 【機能要件 2-2】	【実装要件 2-1】 【実装要件 2-2】 【実装要件 2-3】 【実装要件 2-4】	○

(2) マルウェア検体を用いた機能検証

プロトタイプで実装したアップロードフォルダ監視が，既存のマルウェア検体によってアップロードされたファイルに対して機能要件ならびに実装要件を満たすかの検証（**表 4**）を通して，P2P ファイル交換ソフトウェア環境への情報流出を引き起こす新たなマルウェアへの対応性を確認する．

評価環境には，VMware Server を用いた仮想環境上に，ゲスト OS として Windows XP Professional SP2，P2P ファイル交換ソフトウェアとして Winny v2.0b7.1 を稼動させる環境を構築した．検証に使用したマルウェア検体は計 217 件で，2008 年 1 月から 2 月にかけ，Winny ネットワークに流通していたファイルから収集した検体である．その内訳は**表 5** のとおりである．いずれも検体実行後の動作は，アップロードフォルダに自身のコピーを格納する．なお，検証にあたっては，各マルウェアの実行ごとに，仮想環境をマルウェア実行前のクリーンな環境に復元した．

表 4　検証項目と結果
Table 4　Functional evaluation and result list.

#	検証項目	検証操作	確認要件		結果
1	マルウェア感染を想定したアップロードフォルダへのファイル格納	保護マーク付きファイルをアップロードフォルダに格納する．	【機能要件 1-1】 【機能要件 1-2】	【実装要件 1-1】 【実装要件 1-2】 【実装要件 1-4】	○

表 5　検証に使用したマルウェア検体
Table 5　Malware samples in evaluation.

マルウェア検体名	ファイル数
WORM_ANTINNY.JB	184
PE_PARITE.A	15
WORM_ANTINNY.BB	8
WORM_ANTINNY.JA	8
PE_BOBAX.AH	1
PE_FUNLOVE.4099	1

(3)　ウイルス対策ソフトウェアとの共存性検証

プロトタイプは，カーネルモードでファイル操作をフックするアップロードフォルダ監視，ユーザモードでファイル操作をフックするダウンロードフォルダ監視を実装している．ウイルス対策ソフトウェアは，プロトタイプと同様に，ファイル操作をフックすることで，ファイル検査を行っている．ウイルス対策ソフトウェアとの共存性検証では，プロトタイプで採用した実装が，既存のウイルス対策ソフトウェアと競合しないことを確認する．

評価環境には，VMware Server を用いた仮想環境上に，ゲスト OS として Windows XP Professional SP2，P2P ファイル交換ソフトウェアとして Winny v2.0b7.1，ウイルス対策ソフトウェアとして，ウイルスバスター 2008，Norton Internet Security 2008，Kaspersky Internet Security 7.0 を稼動させる環境を構築した．

5.2　検 証 結 果

(1)　機能検証

機能検証の結果を表 3 に示す．いずれの検証項目についても，機能要件，実装要件を満たし，アップロードフォルダとダウンロードフォルダを有する P2P ファイル交換ソフトウェア Winny v2.0b7.1，Winnyp 7.28 と Share EX2 に対して有効であった．

(a) 利用者の正常操作を想定したアップロードフォルダへのファイル格納

アップロードフォルダに格納された保護マークなしファイルをファイル格納操作モジュール（【実装要件 1-1】）が自動検出し，隔離フォルダに退避させた（【機能要件 1-1】）．また，ハッシュ値取得モジュール（【実装要件 1-2】）が保護マークなしファイルと判定して，フォルダ再格納モジュール（【実装要件 1-3】）が隔離フォルダからアップロードフォルダに該当ファイルを移動させた．

(b) 利用者の誤操作を想定したアップロードフォルダへのファイル格納

ファイル格納操作モジュール（【実装要件 1-1】）が，アップロードフォルダに格納された保護マーク付きファイルを自動検出し，隔離フォルダに退避させた（【機能要件 1-1】）．ハッシュ値取得モジュール（【実装要件 1-2】）が保護マーク付きと判定したファイルを隔離フォルダ内に隔離維持した（【機能要件 1-2】）．さらに，隔離フォルダ内のファイルに対しては，隔離フォルダ監視モジュール（【実装要件 1-4】）が，プロトタイプのプロセスからのみファイルへのアクセス（閲覧，移動，削除）を許可し，その他のプロセスからのファイルへのアクセスを拒否することを確認した．

(c) 不適切なファイルの取得を想定したダウンロードフォルダへのファイル格納

ファイル格納操作モジュール（【実装要件 2-1】）がダウンロードフォルダに格納されたファイルを自動検出した．次に P2PDB 連携モジュール（【実装要件 2-2】）が検出したファイルの属性情報を P2PDB に問合せを行った（【機能要件 2-1】）．また，ファイル属性情報に基づき，通知削除モジュール（【実装要件 2-3】）が，利用者にダイアログボックスで，マルウェアファイルの可能性，著作権侵害ファイルの可能性，漏えいファイルの可能性を通知した（【機能要件 2-2】）．

(2)　マルウェア検体を用いた機能検証

マルウェア検体を用いた機能検証の結果を表 4 に示す．ファイル格納操作モジュール（【実装要件 1-1】）が，マルウェア感染によってアップロードフォルダに格納された保護マーク付きファイル（マルウェア自身がコピーしたファイル）を自動検出し，隔離フォルダに退避させた．また，ハッシュ値取得モジュール（【実装要件 1-2】）が保護マーク付きファイルと判定して，隔離フォルダ内に該当ファイルを隔離維持した．

隔離フォルダ監視モジュール（【実装要件 1-4】）が，プロトタイプのプロセスからのみファイルへのアクセス（閲覧，移動，削除）を許可し，その他のプロセスからのファイルへのアクセスを拒否した．マルウェア検体 217 件すべてにおいて，機能要件，実装要件を満たすことを確認した．

(3)　ウイルス対策ソフトウェアとの共存性検証

(a) アップロードフォルダ監視

検証には，保護マーク付きファイルに該当する，誤操作を想定したファイルとマルウェア検体を用いた．アップロードフォルダ監視は表 3 の#2，表 4 に示す機能要件，実装要件を満たすことを確認した．また，いずれのウイルス対策ソフトウェアにおいても，検証の範囲では，端末での障害発生はなかった．

(b) ダウンロードフォルダ監視

検証には，登録ファイルに該当する，著作物を想定したファイルと，マルウェア検体を用いた．ダウンロードフォルダ監視は表 3 の#3 に示す機能要件，実装要件を満たすことを確認した．ただし，著作物を想定したファイルについては本機能が検出し削除した．マルウェア検体については，ダウンロードフォルダにマルウェア検体が格納された時点で，ウイルス対策ソフトウェアが削除したため，本機能ではダウンロードフォルダにマルウェア検体が格納されたことを検出しなかった．また，いずれのウイルス対策ソフトウェアにおいても，検証の範囲では，端末での障害発生はなかった．

5.3 考　　察

本節では，プロトタイプの機能検証，マルウェア検体を用いた機能検証，ウイルス対策ソフトウェアとの共存性検証の 3 つの視点から検証結果を考察する．

(1)　機能検証

機能検証を通して，特定のフォルダを常時自動監視するという実装が，国内で利用されている主要な P2P ファイル交換ソフトウェア Winny，Share に適用可能であることを確認するとともに，汎用的な方式としての可能性を示したと考える．

(a) アップロードフォルダ監視について

プロトタイプのアップロードフォルダ監視では，利用者の誤操作によるアップロードフォルダへのファイル格納を中心に機能検証を行った．ウイルス対策ソフトウェアの場合には，マルウェア感染以外には対応できず，デジタル著作権管理技術の場合には，著作権侵害ファイルのアップロード以外に対応できない．このことから，提案方式の有効性の 1 つに，利用者の誤操作によるアップロードフォルダへの機密情報や個人情報のファイル格納を回避できることにあるといえる．また，公開許可ファイルリストに 1 万件の保護マークなしファイルを登録した場合にも，アップロードフォルダへのファイル格納操作から 1 秒以内には，図 6 に示すダイアログボックスが表示されたことから，プロトタイプで実装したアップロードフォルダ監視は実用に耐えうると考える．

(b) ダウンロードフォルダ監視について

プロトタイプのダウンロードフォルダ監視では，著作権侵害ファイルの可能性，マルウェアファイルの可能性，漏えいファイルの可能性を想定して機能検証を行った．文献 7) に示すような一般的なファイルアクセス制御方式の場合には，これらの不適切なファイルのダウンロードに対応できず，ウイルス対策ソフトウェアやデジタル著作権管理技術の場合には，漏えいファイルのダウンロードには対応できない．このことから，提案方式の有効性の 1 つに，漏えいファイルを含む不適切なファイルのダウンロード，すなわち，ダウンロードフォルダへのファイル格納を回避できることにあるといえる．ただし，漏えいファイルの可能性を利用者にダイアログボックス通知することは，ファイルのダウンロード抑止に加え，注意喚起を促すことができる反面，ファイルダウンロードを試みる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可能性がある．このような場合には，偏った注目度を高めないようダイアログボックスの通知には表示しないなどの工夫が必要となる．

また，マルウェアの場合には亜種ごとにハッシュ値が異なり，著作権侵害ファイルの場合には符号化を変更するだけでハッシュ値が異なることになる．このため，本来であればハッシュ値の一致判定だけでは不十分であることが分かる．さらに，著作権侵害ファイルおよびマルウェアファイルに対する検知精度は P2PDB に登録するファイル属性情報の保守，ファイル所持判定拡張モジュールが参照する外部データベースの保守の状態にも大きく左右されてしまうことになる．しかし，判定アルゴリズムの改良およびファイル属性情報の保守には，たとえば現在のウイルス対策ソフトウェアベンダが行っている業務レベルの運用であるウイルス検知アルゴリズムの改善およびウイルス定義ファイルの定期更新が必要となる．このため，今回の機能検証では，そこまでの評価は行っていない．

(c) P2PDB 連携モジュールについて

P2PDB 連携モジュールを用いた P2PDB からの応答時間は数秒であり，P2P ファイル交換ソフトウェアによるファイルのダウンロードには少なくとも数分から数時間かかること，P2P ファイル交換ソフトウェアがダウンロードフォルダにファイルを格納する際に P2PDB 連携モジュールが自動実行されることから，プロトタイプで実装したダウンロードフォルダ監視は性能面では実用に耐えうると考える．ただし，ダウンロードフォルダ監視において，不適切なファイルを判定するための P2PDB 連携モジュールの精度向上については，P2PDB に登録されている属性情報件数を増やすだけではなく，ファイル所持判定拡張モジュールを用いた外部データベース連携を進めるなどの検討が必要となる．筆者らの調査では，Winny ネットワークで流通するファイル 100 件を任意抽出して hashdb.com に照会し

た結果，27%がデータベースに登録されていたことから，外部データベース連携は有効な解決方法の 1 つと考える．

また，今回はプロトタイプのため，不適切なファイルのアップロードを抑止する機能を実装していないが，アップロードフォルダ監視に P2PDB 連携モジュールを組み込むことにより実現可能である．今後，P2PDB の拡充ならびに，インターネット上の P2PDB 以外の外部データベース活用を含め検討していきたいと考えている．

(2)　マルウェア検体を用いた機能検証

マルウェア検体を用いた機能検証では，P2P ファイル交換ソフトウェア環境への情報流出を引き起こす新たなマルウェアを想定し，既存のマルウェア検体を用いた機能検証を行った．

提案方式は，端末内に格納されているすべてのファイルを P2P ファイル交換ソフトウェア環境に流通してはならない保護マーク付きファイルとして取り扱い，保護マーク付きファイルが 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た場合には，マルウェア感染もしくは，利用者の誤操作で格納されたファイルと判定している．動作による検知方式を採用しているため，既存ウイルス対策ソフトウェアと組み合わせて使うことで，P2P ファイル交換ソフトウェア環境への情報流出を引き起こす新たなマルウェアによる対処の改善につながると考える．ただし，プロトタイプでは，監視対象となるアップロードフォルダを図 4 に示すとおり手動で登録している．このため，利用者がアップロードフォルダを新規に作成した場合には，作成のたびに追加登録が必要となる．また，マルウェアによっては，情報流出用のアップロードフォルダを新規に作成する場合もある．アップロードフォルダ監視の有効性を高めるためには，今後，P2P ファイル交換ソフトウェアが使用するアップロードフォルダの自動監視ならびに登録機能の実装などが必要となる．

(3)　ウイルス対策ソフトウェアとの共存性検証

ウイルス対策ソフトウェアとの共存性検証を通して，検証の範囲では，プロトタイプで採用した実装が，既存のウイルス対策ソフトウェアと競合しないことを示した．このことから，プロトタイプで採用した実装が，既存ウイルス対策ソフトウェアと組み合わせて使用できること，さらに，P2P ファイル交換ソフトウェア環境への情報流出を引き起こす新たなマルウェアへの対処改善方法としての実現可能性を示したと考える．

6. おわりに

本論文では，P2P ファイル交換ソフトウェアで発生した被害状況や，既存の対策から解決したい課題を示し，課題解決するための方式である「マルウェアや利用者の誤操作によるファイルのアップロードの防止機能」と「不適切なファイルのダウンロードの抑止機能」を有するクライアント型情報流通対策システムを提案した．

提案方式は，P2P ファイル交換ソフトウェアのアップロードフォルダとダウンロードフォルダという実装上の特徴に着目した．これらのフォルダを常時自動監視し，保護マークなしのファイルのみアップロードフォルダに格納可能とし，ファイル属性情報を格納したデータベースに登録されていないファイルのみダウンロードフォルダに格納可能とする方式である．また，提案方式に基づきアップロードフォルダ監視とダウンロードフォルダ監視をプロトタイプ実装した．評価を通して，アップロードフォルダ監視とダウンロードフォルダ監視による提案方式の有効性を示した．今後も提案方式のさらなる実用化を目指してゆきたいと考えている．

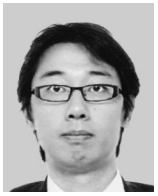
謝辞　本研究は総務省から委託を受けた「ネットワークを通じた情報流出の検知及び漏出情報の自動流通停止のための技術開発」の支援を受け実施している．本研究を進めるにあたって有益な助言と協力をいただいた関係者各位に深く感謝いたします．

参考文献

1) 独立行政法人情報処理推進機構：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) 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
3) 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
4) 社団法人コンピュータソフトウェア著作権協会：第 7 回「ファイル共有ソフト利用実態調査」（2008 年 12 月 12 日）．
http://www2.accsjp.or.jp/research/research08.php
5) 寺田真敏ほか：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の検討，情報処理学会 CSEC 研究報告，Vol.2008, No.71, pp.123–128 (2008).
6) 喜田弘司ほか：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).
7) 荒井正人ほか：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 (2004).
8) Christin, N., Weigend, A. and Chuang, J.: Content Availability, Pollution and Poisoning in Peer-to-Peer File Sharing Networks, *ACM E-Commerce Conference* (2005).

9) Liang, J., Kumar, R., Xi, Y. and Ross, K.: Pollution in P2P file sharing systems, *Proc. IEEE INFOCOM'05* (2005).
10) 伊吹和也ほか：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).
11) 任　光輝ほか：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).
12) 今本吉治ほか：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).
13) 青木輝勝ほか：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 (2004).
14) 松下哲也ほか：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).
15) 近藤佐保子ほか：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).

(平成 21 年 12 月 1 日受付)
(平成 22 年　6　月 3 日採録)



松岡　正明

2003 年日本高信頼システム入社．セキュア OS のアプライアンスサーバ開発や，キャリアサービスのリリース管理およびシステムテストに SE として従事．2007 年（株）ラック入社．現在，セキュリティ事業部セキュリティエキスパートセンター所属．マルウェアの調査研究，マルウェア対策技術の研究開発に従事．2007 年から安心・安全インターネット推進協議会 P2P 研究会構成員．

松木　隆宏（正会員）

2005 年岡山大学工学部通信ネットワーク工学科卒業．同年（株）ラック入社．現在，サイバーリスク総合研究所研究員．ネットワークセキュリティ脅威分析等のセキュリティコンサルティング部門を経て，マルウェアの調査研究，マルウェア対策技術の研究開発に従事．2006 年より，サイバークリーンセンターによるボット対策プロジェクトに参画し，調査研究，ハニーポットの開発，運用支援に従事．2007 年から安心・安全インターネット推進協議会 P2P 研究会構成員．2008 年情報処理学会コンピュータセキュリティ研究会専門委員．CISSP．

寺田　真敏（正会員）

1986 年千葉大学大学院工学研究科写真工学専攻修士課程修了．同年（株）日立製作所入社．博士（工学）．現在，システム開発研究所にてネットワークセキュリティの研究に従事．2004 年から Hitachi Incident Response Team チーフコーディネーションデザイナー，2004 年 4 月から JPCERT コーディネーションセンター専門委員，2004 年 4 月から 2007 年まで中央大学研究開発機構客員研究員，2004 年 8 月から情報処理推進機構セキュリティセンター研究員．2008 年から中央大学大学院客員講師を兼務．

鬼頭　哲郎（正会員）

2005 年東京大学大学院情報理工学系研究科電子情報学専攻修士課程修了．同年（株）日立製作所システム開発研究所に入所．現在，ネットワークセキュリティ技術に関する研究開発に従事．

仲小路博史（正会員）

2001 年東京理科大学大学院理工学研究科情報科学科修士課程修了．同年（株）日立製作所システム開発研究所入所．PKI ならびに X.509 属性証明書の研究開発に従事．現在はネットワークセキュリティ技術に関する研究開発に従事．