# 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

喜田弘司[†,†††] 坂本久[††]
島津秀雄[††] 垂水浩幸[†††]

近年，個人情報が P2P ファイル共有システムによって流出したというニュースが連日報道されており社会問題になっている．この対策として P2P ファイル共有システムの使用を禁止するシステムが多く提案されている．しかしながら，ユビキタス時代の社会システムを考えると，ファイル共有ソフトウェアは利用禁止にはできない．そこで我々はファイル共有システムをセキュアに利用する環境を提供する「ファイルアクセス制御エージェント」を開発した．このエージェントは PC に常駐し，すべてのファイルアクセスを監視して，未知のプログラムからのファイルアクセスに対してはアクセスを禁止する．たとえば，あるワープロで作成したファイルは，そのワープロやファイル管理ツールなどからしかアクセスできない環境を提供する．アクセスしているファイルから見て未知のプログラムであるか既知のプログラムであるかは，今回開発した「ファイル利用コンテキストベースアクセス許可判定技術」を使って自動判定する．この技術は，ユーザの GUI 操作やプロセスの親子関係，必要があればユーザとの対話でアクセス権を判断する．これによりユーザが知らないタイミングで知らないプログラムから情報漏えいすることを防止することができる．実験により，本エージェント動作環境下で，これまでと同様に P2P ファイル共有システムとアプリケーションの両方を利用することができた．さらに，ウィルスによる情報漏えいも防止できることを確認した．

# A Proposal of File Access Control Software Agent Toward Using P2P File Sharing System in Safet

Koji Kida,[†,†††] Hisashi Sakamoto,[††] Hideo Shimazu[††]
and Hiroyuki Tarumi[†††]

In recent years information leakage problems via P2P (peer-to-peer) file sharing systems, such as Winny, emerge as a social issue. Countermeasure systems that prohibit the use of P2P file sharing systems have been launched. However, we consider the solutions are NOT feasible according to analysis of the use of P2P file sharing systems. In this paper we propose a file access control software agent that provides users to use P2P file sharing software in safety. The agent is installed on each PC including those for private use. It monitors all file accesses and blocks them from unauthorized applications. For example, ONLY Microsoft Word and Explorer are allowed to access *.doc files. Users have been sharing files such as MP3 files, AVI files and so on using a P2P file sharing system. On the other hand, users have confidential files that should not be shared on P2P file sharing system. We can avoid such inappropriate sharing by blocking accesses to confidential files. The agent monitors GUI operations and analyzes process behaviors to detect such critical accesses. We have experimented and confirmed that the agent can detect illegal accesses to confidential files without inhibiting P2P file sharing systems for their private use.

## 1. はじめに

近年，Winny などのファイル共有ソフトを使った情報漏えい事件が相次ぎ，社会問題になっている[1)]．政府からは「情報漏えいを防ぐ最も確実な対策は，パーソナルコンピュータ（以下 PC と略記）で Winny を使わないことである」との発表があった[2)]．これを受けて，多くのベンダは，Winny などの P2P 型ファイ

† NEC インターネットシステム研究所
NEC Internet Systems Research Laboratories
†† NEC システムテクノロジー
NEC System Technologies, Ltd.
††† 香川大学
Kagawa University

ル共有システムがインストールされている PC を検出し，起動させない，あるいはアンインストールさせる製品を発表している[3]．

ところが我々は，P2P 型ファイル共有システムを利用しないという対策は，以下の点から，本質を見誤った対策であると考える．

(1) ユビキタス時代の社会システムとしてファイル共有ソフトウェアは利用禁止にはできない：ユビキタス時代の社会システムは，商用のコンテンツだけではなく個人が発信するコンテンツや，カメラや各種センサからの情報を効率良く共有，検索できる必要がある．このネットワーク基盤として P2P 型のファイル共有システム[4),5)] は重要であり，利用を禁止することは得策ではない．

(2) ユビキタス時代の仕事スタイルとして企業内の PC だけをセキュアにしても不十分である：従来の対策は，企業内の PC だけを対象にしている．ところが実際に情報が漏れているのは個人の自宅の PC からである．つまり，ユビキタス時代の仕事スタイルは，いつでもどこでも仕事ができる環境であり，企業内の PC だけをセキュアにしても不十分である．問題の本質は，企業ネットだけではなく，社員の自宅の PC や外部リソースも対象としたリスク管理の方法を考えることである．

以上の理由から，我々は，P2P 型ファイル共有システムの利用を禁止するのではなく，セキュアに利用するための方法を提案することを研究目的とする．特に，企業から管理方法や運用方法の指示を受けない個人の PC を対象にする．アプローチとしては，個人の PC のファイルのアクセス権を管理するエージェントを提案する．情報漏えいにつながるアクセスかどうかをエージェントが判断し，アクセスの許可を与えることで，セキュアに P2P 型ファイル共有システムが利用できる．

本研究は，自宅の PC において，P2P 型ファイル共有システムの利用と会社から持ち帰った仕事の遂行が両立できかつ，情報が漏れない社会システム環境を構築することが目標である．

なお，本システムは P2P 型ファイル共有システムを悪用した情報漏えいを完全に防ぐことができるわけではない．本システムの設定ミスや故意にユーザが情報を漏らそうとした場合には防御しきれない場合がある．政府の発表のように P2P 型ファイル共有システムと機密情報を共存させない利用方法の方がセキュリティ強度は高い．

## 2. P2P 型ファイル共有システムによる情報漏えいの分析

### 2.1 P2P 型ファイル共有システムによる情報漏えいモデル

P2P 型ファイル共有システムでの情報漏えいは，P2P 型ファイル共有システムを媒介にしたコンピュータウィルス（以降ウィルス）が，ファイル共有機能を悪用して巧みな手段で重要なファイルを流出させることが原因で発生する．まず，本稿では，ウィルスの動作および状態を以下のように分類する（**図 1**）．ただし，この分類は本稿での説明のための分類であり，分類方法や用語の定義はいろいろな考え方がある[6]．

**侵入** ネットワークなど外部リソースから PC 内部へウィルスのプログラムが入り込む動作のこと

**感染** 侵入したウィルスがメモリや，ディスクにデータとして存在する状態のこと

**潜伏** 侵入したウィルスがメモリ上でプロセスとして存在しているがまだ被害が出ていない状態．すなわち情報が外部へ漏れやすい状態ではあるが，まだ情報が外部へ漏れていない状態のこと

**発病** 潜伏しているウィルスが活動し，情報が外部に漏れてしまった状態

次に，ウィルスの動作パターンを分析すると，P2P 型ファイル共有システムの悪用方法の観点から**図 2** のように 4 つのタイプに分類できる．

**TypeA** ウィルスが PC へ侵入し感染状態にするためだけに P2P 型ファイル共有システムを利用するタイプ．ウィルスの感染状態から，潜伏，発病はウィルス自身が行う．情報の漏えいには直接 P2P 型ファイル共有システムは利用しない．

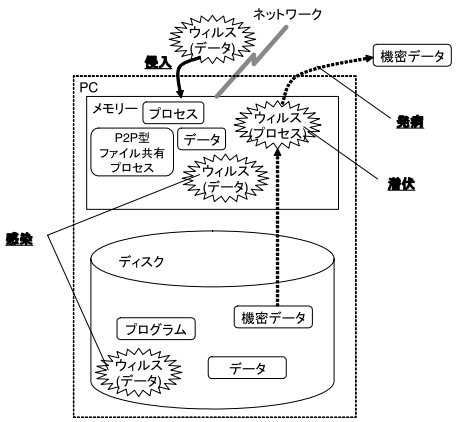


**図 1** ウィルスの状態図
Fig. 1 State transition of computer viruses.

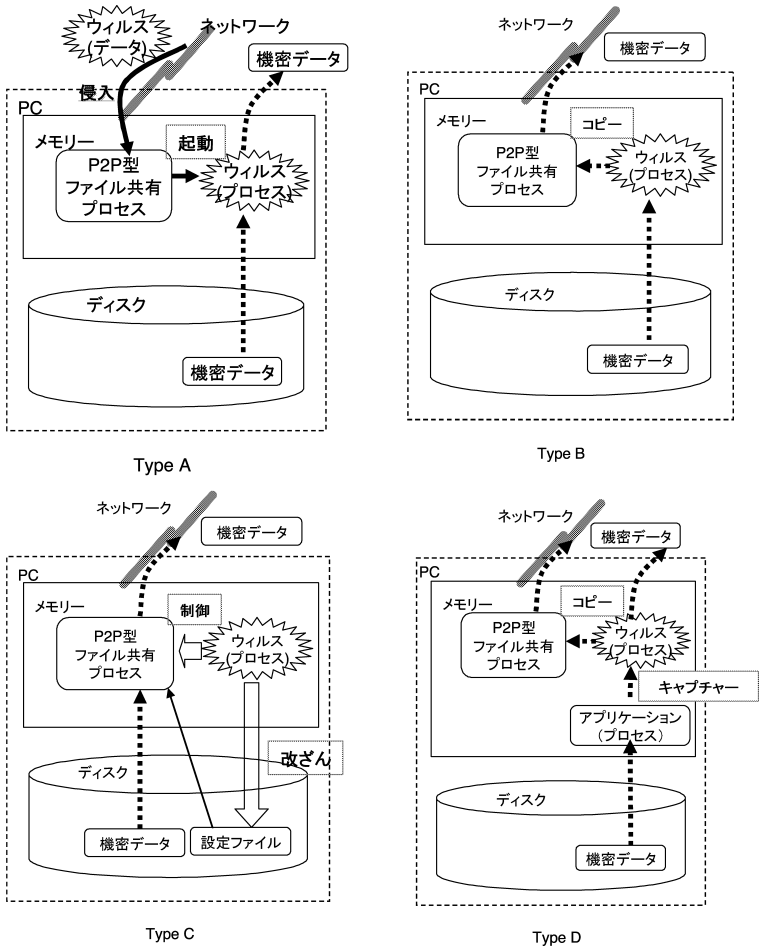


**図 2** P2P 型ファイル共有ソフトウェアの悪用パターン
Fig. 2 Types of computer viruses attacking P2P file sharing system.

**TypeB** 潜伏しているウィルスプロセスが機密データを読み込み，これを P2P 型ファイル共有システムへコピーすることで，この機密データが P2P 型ファイル共有システムのネットワーク（以下 P2P ネットワーク）に漏れてしまうタイプ．P2P 型ファイル共有システムへの機密データのコピーは，P2P 型ファイル共有システムの共有フォルダへ機密データをコピーする方法が一般的であり，現在発見されているウィルスは，このタイプのウィルスが最も多い．

**TypeC** P2P 型ファイル共有システムを制御して，P2P 型ファイル共有システムに機密データを読み込ませ情報漏えいさせるタイプ．P2P 型ファイル共有システムの設定ファイルを改ざんし，P2P ネットワークで共有していないフォルダを，共有する設定にかえる方法が一般的である．

**TypeD** ウィルスは，直接的に機密データを読み込むのではなく，他のアプリケーションで利用している状態を画面キャプチャなどで取得して，P2P ネットワークに漏らしたり，あるいは直接ウィルスのプロセスがサーバとなって，情報を外部に漏えいさせたりする．このウィルスはいわゆる「山田オールタナティブ」と呼ばれており，自分自身が WEB サーバとなって画面キャプチャした情報をインターネットに公開する方法が一般的である．

### 2.2 P2P 型ファイル共有システムによる情報漏えい対策の難しさ

P2P 型ファイル共有システムでは，いったん情報が漏れてしまうとその追跡と回収は不可能である．これはキャッシュを使った匿名ネットワークで実現されたファイル共有ソフトウェアに共通の特徴である[7]．つまり漏れなくすることが対策の基本である．

漏れる原因は，P2P 型ファイル共有システム，仕事のファイル，ウィルスが 1 台の PC に共存しているからである．ところがこれらが共存しない状況を維持す

ることは，非常に難しい．

**（難しさ 1）** P2P 型ファイル共有システムと仕事のファイルは共存について：まず自営業の場合，自宅の PC を仕事にもプライベートにも利用している人が多いため，プライベートで P2P 型ファイル共有システムを使うと，仕事のファイルと共存してしまうことになる．一方，会社と自宅の両方で PC を利用している人は，大容量の USB メモリや，ファイルサイズの大きな添付メールを使って気軽に自宅の PC へ仕事のファイルを転送して自宅で仕事をしている．仕事が完了した際に，そのファイルを削除すればよいが，この削除操作をし忘れることが多い．たとえば，電子メールの添付ファイルで機密情報を受け取った場合，電子メールのメッセージ自体を削除するユーザは少ない．

また，家族で自宅の PC を共有していることも P2P 型ファイル共有システムと仕事のファイルが共存する原因の 1 つである．自分が P2P 型ファイル共有システムをインストールしていなくても他のだれかがインストールしている可能性がある．アクセス権の設定などである程度の対策は可能であるが，現実的にこういった設定をすることはまれである．家族全員が Administrator（管理者）の権限を持っている場合も多く，アクセス制限をかけることができない．

さらに 1 章で述べたとおり，ユビキタス時代には，仕事とプライベートの境界はよりあいまいになり，今後はますます共存していくことが予想される．

このように，P2P 型ファイル共有システムと仕事のファイルは現実的には共存せざるをえない．

**（難しさ 2）** ウィルスの感染について：以下の要因から P2P 型ファイル共有システムのユーザはウィルスに感染する確率が高い．

- P2P 型ファイル共有システムの駆除が間に合わない：アンチウィルスソフトのウィルス定義ファイルの更新が P2P 型ファイル共有システムをターゲットにした最新のウィルスに間に合わないことが多い．他のウィルスでも同様の難しさを持っているが，P2P 型ネットワークを介して感染するウィルスは，非常に感染の速度が速く，この問題がより深刻になる．
- アンチウィルスソフトの常駐を停止する：多くのユーザが P2P 型ファイル共有システムの利用中はアンチウィルスソフトを一時停止している．これは P2P 型ファイル共有システムのダウンロードとウィルスのチェック機能の相性が悪いことが多く，より確実にダウンロードさせるためである．
- ウィルスと気がつかない：スパムメールのように一方的に相手側から送られてきた情報に対しては警戒心が強いが，自分が検索してダウンロードしたファイルは無警戒で実行してしまう．

### 2.3 従来の情報漏えい対策の限界

前記の P2P 型ファイル共有システム利用環境下特有の情報漏えい対策の難しさをふまえ，従来の情報漏えい対策（**図 3**）の限界についてまとめる．

**侵入の防止**：ポートの設定を制御することで外部からのデータの侵入や，内部からの情報の漏えいを防ぐ方法であり，パーソナルファイアウォールの利用が一般的である．ただし，P2P 型ファイル共有システム利用環境では，P2P ネットワークのためのポートは開けられているために，このポートからのウィルスの侵入および，情報の漏えいは防ぐことができない．

**感染・潜伏の防止**：侵入してきたウィルスが発病するまでの間に，メモリやディスクのデータをスキャンして駆除する方法であり，アンチウィルスソフトウェアの利用が一般的である．ただし，P2P 型ファイル共有システム利用環境では，ウィルスの流通速度が非常に速いために，未知のウィルスが侵入しやすく，アンチウィルスソフトウェアで駆除できないことが多い．

以上のように，従来の対策ソフトウェアは，ウィルスの侵入，感染，潜伏を防止することが中心である．発病の防止に関しては，専用の対策ソフトウェアがあるのではなく，以下に説明する運用方法による対策が考えられる．

**発病の防止**：潜伏してしまっているウィルスの発病を防止するためには，ウィルスと機密データを完全に分離することである．したがって，1 台の PC にマルチアカウントでログインする方法や，仮想環境を入れてマルチ OS にする運用方法が考えられる．しかしなが

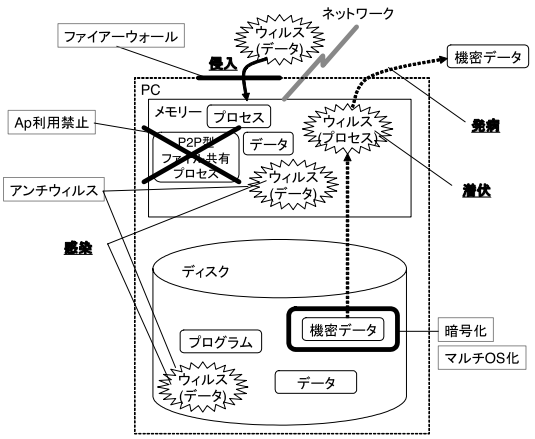


**図 3** 従来の情報漏えい対策図
Fig. 3 Countermeasures for information leakage.

らこれらの方法は個人の PC での利用では非現実的と考える．前者は，アカウントの権限管理を厳密にする必要があり，管理者権限を全員が持っていることが多い個人の PC では運用形態が大きく異なってしまう．後者は，PC の高いスキルが必要でありこの対策の普及は難しい．また別の対策方法として，発病を防止するのではなく，機密データを暗号化することで発病しても被害がないようにする対策が考えられる．ただし，データの暗号化は，保存時に暗号化し利用時に復号化する必要があり，大きく PC の使い勝手を悪くする．たとえば，すでに文書をファイル単位に暗号化するソフトウェアは多く存在するが一般オフィスではほとんど使われていないのが現状である．

以上のように，従来の対策および運用の変更では，P2P 型ファイル共有システムを安全に利用することは難しいといえる．

## 3. 対策の考え方

### 3.1 基本方針

これまでの分析をふまえ，我々は，従来の対策の考え方とは逆の発想で，「ウィルスに感染・潜伏した P2P 型ファイル共有システムと，仕事のファイルを 1 台の PC で共存した環境において，情報漏えいが発生しない，すなわちウィルスが発病しない方法」を提案する．ユーザは，これまでどおり P2P 型ファイル共有システムを使うことができ，仕事も行えることを目指す．

### 3.2 ターゲット

本研究では，以下のような情報漏えい，ユーザ，PC の利用方法を想定する．

**想定情報漏えい**：PC のディスクに，機密情報がファイルの形式で存在する．たとえば，ワープロで作成した資料などである．このファイルが，ユーザが意図しない外部にコピーされることを本研究では情報漏えいと呼ぶ．したがって，ウィルスによるユーザの入力や画面キャプチャデータの漏えい，ウィルス自身の他の PC への増殖，ファイルや装置の破壊活動といった，機密ファイルの流出ではないウィルスの活動に関しては，本研究の対象外とする．すなわち，前章で説明した情報漏えいモデルでいうと，タイプ A，タイプ B，タイプ C を対象とする．タイプ D に関して対象とはぜず，最後に考察するにとどめる．さらに，本システムは，故意による（未必の故意も含む）情報漏えいを防ぐのではなく，過失による情報漏えいを防ぐことを目標とする．

**想定ユーザ**：スキルと利用方法は以下を想定．

- 情報漏えいさせる気はない．
- 機密情報と，機密ではない情報の区別がつく．
- P2P 型ファイル共有システムを利用する．ただし，共有するファイルの種類はファイルの拡張子で区別できるものとする．たとえば，AVI ファイルや，MP3 ファイルなどである．
- 機密情報は P2P 型ファイル共有システムでは利用しない．つまり，機密情報の拡張子は，共有するファイルの拡張子とは異なる．
- ワープロなどの P2P 型ファイル共有システム以外のアプリケーションを利用する．このアプリケーションでは，機密情報も利用する．
- PC で利用するアプリケーションを知っている．たとえば，アプリケーション名から，使ったことがあるか，使ったことがないか判断がつく．
- ソフトウェアのインストール，設定ができる．いずれも画面の指示に従って操作できるレベルでよい．

**想定 PC の利用方法**：

- ファイアウォール，アンチウィルスソフトウェアの従来の対策ソフトウェアも利用している．
- PC に 1 つの OS がインストールされている．なお，本技術は OS の種類は特に問わないが，本稿では，マイクロソフト社のウインドウズ XP で試作した例で説明する．
- PC に複数アカウントが存在してもかまわない．
- 本ソフトウェア導入時は安全であるとする．すなわち，本ソフトウェア導入以前にウィルスに感染していた場合は対象外とする．

### 3.3 対策のアイデア

P2P 型ファイル共有システムを利用した情報漏えいを分析すると，どのタイプも不正なファイルアクセスが存在することが分かる．タイプ A，タイプ B は，直接ウィルスのプロセスが機密データにアクセスしている．タイプ C は，機密データへは直接アクセスしていないが P2P 型ファイル共有システムの設定ファイルを改ざんするという不正アクセスをしている．

これに対し，我々は，ファイルのアクセス権の管理が脆弱であることが原因の 1 つであると考えた．つまり，従来のファイルシステムでは，ユーザの所属グループと，ファイルあるいはファイルが置かれてあるフォルダとの対応に対して，ファイルのアクセス権（読み込み権限，書き込み権限，実行権限）を設定する仕組みである．このために，管理者権限で動作するプログラムからはすべてのアクセス権が与えられてしまう．PC の多くのアカウントは管理者権限が与えられていることから，ウィルスも管理者権限で動作することが多く，このために，ウィルスはどのファイルにも自由

にアクセスができてしまい情報漏えいが発生すると考えられる．

そこで，我々のアイデアは，プログラムとファイルの対応に対して，アクセス権を適切に設定できればPCは，よりセキュアになると考えた，つまり，ファイルごとにアクセスを許可するプログラム（以下「許可プログラム」）と禁止するプログラム（以下「禁止プログラム」）を対応付け，この対応を基に，すべてのファイルアクセスを制御することで情報漏えいを防止する．たとえば，あるワープロのファイルへのアクセスは，以下のようにすれば情報漏えいは防げる．

**「許可プログラム」**：そのワープロのプログラム，ファイル管理ツール，メーラ，圧縮プログラム，アンチウィルスソフトウェア，ファイル高速検索用インデックスプログラムなどのO3サービス．

**「禁止プログラム」**：ウィルスプログラム．一般に，何がウィルスのプログラムかは判断がつかない．したがって，より安全にするために，許可プログラムとして登録されていないプログラムはすべて禁止プログラムとする．つまり，ユーザは許可プログラムだけを登録する，いわゆる「ホワイトリスト」方式とする．一般的にこの設定は，各ファイル形式に対応した通常使うアプリケーション，O3のサービス，ファイル管理ツールは許可プログラムと考えられる．これ以外はユーザの利用方法に依存する．

### 3.4 アイデアの検証

前記のファイルアクセス制御機能により，情報漏えいを防止できることと，P2P型ファイル共有システムやその他の一般アプリケーションがこれまでどおり利用できることを検証する．

**情報漏えいを防止できること**：タイプA，タイプBはウィルスが直接機密データへアクセスしている．このため，ホワイトリストに，ウィルスと機密データの対応が登録されていない限り，アクセスはブロックされ安全であるといえる．すなわち，機密データに関するホワイトリストの設定を，この機密データを編集するアプリケーション，圧縮ツール，ファイラなどの共通アプリケーションだけからなるように維持できれば安全といえる．

次にタイプCは，ホワイトリストに，ウィルスとP2P型ファイル共有システムの設定ファイルとの対応が登録されていない限り，アクセスはブロックされ安全であるといえる．つまり，P2P型ファイル共有システムの設定ファイルが，P2P型ファイル共有システム以外のプログラムからアクセスされないようにホワイトリストを維持できれば安全といえる．ところが，一般的に設定ファイルはそのアプリケーション用に独立した専用のファイルとは限らない．マイクロソフト社のウインドウズの場合，多くのアプリケーションはレジストリと呼ばれるOSの管理の共有設定ファイルに書かれてあり，このファイルにアクセス制限をかけるわけにはいかない．したがって，設定ファイルにアクセス制限をかけるのではなく，P2P型ファイル共有システムが，機密データにアクセスできないように設定すべきである．つまり，P2P型ファイル共有システムと機密データの対応がホワイトリストに登録されないように維持できれば，情報漏えいは防げる．本稿では，3.2節で説明したように，ファイルの拡張子をベースにP2P型ファイル共有ソフトウェアで利用しないソフトウェアを決定できることを前提にしており，このホワイトリストの維持は可能である．

**P2P型ファイル共有システムがこれまでどおり利用できること**：P2P型ファイル共有システムで共有したいファイルはP2P型ファイル共有システムを許可プログラムと設定すれば通常どおり利用可能になる．たとえば，MP3ファイルや，AVIファイルなど共有したいファイルはP2P型ファイル共有システムを許可プログラムと設定すれば，アクセス制限はかからず，通常どおりファイル共有できることになる．

**一般アプリケーションが利用できること**：許可プログラムの設定をユーザごとに行えば問題なく利用できる．3.3節で説明したデフォルトの設定に加えユーザのアプリケーションの利用形態にあわせて設定すればよい．ただし，この登録手間は課題である．

以上のように，理論上は，情報漏えいを防止しながら，P2P型ファイル共有システムや一般のアプリケーションがこれまでどおりに利用できる．実際のユーザでの評価結果や，前記の仮説の検証は5章で示す．

## 4. ファイルアクセス制御エージェント

### 4.1 機 能 定 義

まず，機能ブロック図（**図4**）を基に，本システムの基本的な動作を説明する．本システムは，アプリケーションからのファイルシステムへのアクセスをフックして，ホワイトリストに従ってこのアクセスの許可および禁止を判断する（アクセス制御）．ホワイトリストはアクセスを許可するポリシが書かれてあり，本システムで自動的に生成し（ホワイトリスト半自動生成），これをユーザが設定画面でカスタマイズする（ホワイトリスト設定ツール）．

次に機能ブロックそれぞれの外部仕様を説明する．

**アプリケーション**：実行ファイル単位に管理する．つ

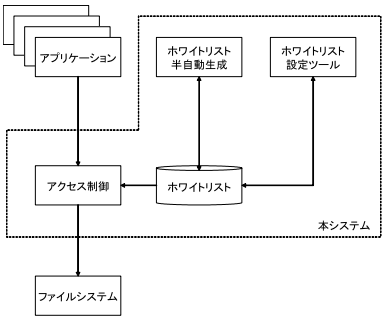


**図 4** 機能ブロック図
Fig. 4 Functional blocks.

まり，ファイルのフルパス名とそのダイジェストで区別する．ダイジェストは MD5[8] を利用した．またアプリケーションは「既知のアプリケーション」と「未知のアプリケーション」の 2 種類に分類する．既知のアプリケーションはホワイトリストを使ってアクセス権を管理している状態であり，未知のアプリケーションとはまだアクセス権を管理していない状態を意味する．さらに既知のアプリケーションは「OS 管理のアプリケーション」と「ユーザ管理のアプリケーション」に分類する（**図 5**）．

**アクセス制御**：アプリケーションとファイルの対応に対して，リード，ライト，実行の権限を制御する．この制御は，既知のアプリケーションの場合には，ホワイトリストを基に許可および禁止を判断し，未知のアプリケーションの場合には，リード，ライトをブロックする．実行権限は基本的にはすべてのアプリケーションで許可するが，未知のアプリケーションが実行された場合は，アクセス権の設定をするかどうかをユーザへ問い合わせる．ここで設定をすると，ホワイトリストへエントリされ以後既知のアプリケーションとして管理する．これにより，たとえば，P2P ファイル共有システムからウィルスが侵入しユーザが誤ってこのファイルを実行した場合には，このファイルのアクセス権を設定をするまでは，すべてのアクセスがブロックされウィルスは発病せず情報漏えいしない．既知のアプリケーションのリードとライトの権限についてはリードの権限だけを管理し，ライトの権限はすでにあるファイルへの上書きはそのファイルのリードのアクセス権に従い，新規のファイルへの書き込みは書き込み先のフォルダの権限に従う．

**ホワイトリスト**：アプリケーションごとにアクセスの許可を与えるポリシを記述する．ポリシは，アクセス可能な対象ファイルをファイル名や拡張子で指定したものや，ファイル名を直接指定したものである（**図 6**）．

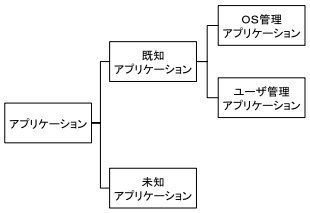


**図 5** アプリケーションの分類
Fig. 5 Classification of application software.

| ダイジェスト | 実行ファイル | 関連ファイル |
|---|---|---|
| 12345 | C:¥Program Files¥Office¥WordPro.exe | *.doc |
| 67890 | C:¥Program Files¥Mail¥WinMail.exe | |
| | | |

| アクセス許可ファイルリスト | ユーザGUI操作中のアクセスを許可 | 実行ファイルのフォルダー以下のファイルのアクセスを許可 |
|---|---|---|
| | True | True |
| C:¥Program Files¥Mail¥WinMail.ini;<br>C:¥Program Files¥Mail¥WinMail.idx; | True | False |
| | | |

**図 6** ホワイトリストの例
Fig. 6 An example of the white-list.

ホワイトリストはこれに加え，ユーザがより設定を簡単にするためにいくつかのアクセスルールが記述できるようになっている（詳細は 4.4 節，4.5 節）．

### 4.2 要　　件

本システムは，ホワイトリストさえ適切に設定できれば，セキュアなファイルアクセス環境が維持できる．ところが一般に，PC はサーバと異なり利用目的が明確ではないことが多く，正常アクセスを事前に定義しにくい．また，個々で利用方法が異なるために，設定ファイルをいっせいに配布するといったことも難しい．すなわち，PC の一般ユーザが，簡単にホワイトリストを設定運用できるようにすることが要件である．

### 4.3 正常アクセスの分析

我々は前記要件を満たすために，自動的にホワイトリストを作成しユーザがカスタマイズする仕組みを考える．まず PC における正常なアクセスを分析した結果，以下のパターンに分類できることが分かった．

(1) 関連づけアプリケーションからのファイルアクセス：アプリケーションごとにそのアプリケーションで利用するデータファイルが対応づけられている．

(2) プログラム実行のためのファイルアクセス：そのプログラム実行のための設定ファイルやライブラリ，データの一時ファイルなどである．

(3) アプリケーション連携によるファイルアクセス：複数のアプリケーションが連携して 1 つのアプリケー

ションのように動作できる．たとえば，ワープロに表計算のデータを貼り付けると，ワープロプログラムから表計算ファイルへのアクセスが発生する．
(4) 特定用途プログラムによるファイルアクセス：そのアプリケーションで利用するデータの形式が決まっているわけではなく，あくまでもデータとして処理するアクセスである．たとえば，メーラで添付メールを作成する際には，ファイルの形式によらず，メーラから添付ファイルへアクセスが発生する．

### 4.4 自動ホワイトリスト生成の検討

正常アクセスのパターンを分析して，自動的にホワイトリストを生成する方法を検討する．

前記の（1）のタイプのアクセスを自動設定するためには，関連アプリケーションからのアクセスを許可すればよい．関連アプリケーションの情報は，O3 の管理ファイル（レジストリ）に拡張子の設定として記憶されておりこれを利用すればよい．(2) のタイプのファイルアクセスの多くは，そのアプリケーションの実行ファイルがあるフォルダ以下へのアクセスであることに注目し，これらのファイルへのアクセスを許可すればよい．ただし，この (1)，(2) の設定は，セキュリティ強度を低下させることになる．たとえば，(2) の場合，あるワープロのデータファイルと同じフォルダにウィルスの実行ファイルを置くと，このウィルスは，そのワープロのファイルへアクセスが許可されてしまう．そこで，本システムでは，3.2 節で説明した，「本ソフトウェア導入時は安全であるとする」という前提の下で，本システム導入時にこれら (1)，(2) の手法で自動的にホワイトリストを設定し，これ以降は，このルールを適用するかどうかをユーザへ問い合わせて設定する．これにより，セキュリティ強度と設定の煩雑さのバランスをとる．

(3) のタイプ，(4) のタイプに関しては，(1)，(2) のような共通ルールがなく，個別に設定する必要がある．この解決をめざし，次章でファイル利用コンテキストベースアクセス許可判定技術を提案する．

### 4.5 ファイル利用コンテキストベースアクセス許可判定技術

我々は，(3)，(4) の場合のホワイトリストの自動作成のためには，ユーザのアプリケーション利用コンテキストを認識する必要があると考えた．ユーザが知らない間に知らないプログラムからのアクセスで情報が漏えいすることが問題なのである．つまり，ユーザがアプリケーションを使って意識的にファイルをアクセスした場合には，このアクセスは禁止する必要はない．許可プログラムを判定することは，ユーザが操作しているプログラムであるのか，ウィルスが利用しているプログラムであるのかを判定することである．

この判定技術を我々は「ファイル利用コンテキストベースアクセス許可判定技術」と呼ぶ．判定方法は，まず，GUI を持ったプログラムは，GUI の利用を監視することでユーザが利用しているかどうかを判定する．たとえば，マウスによりメニューが選択され，キーボードから入力されたのであれば，ユーザが利用していると考えられる．GUI を持たないプログラムの場合は，プロセスの親子関係を見て，O3 が親であるものは O3 のサービスであるとしてすべて許可する．それ以外のものは，はじめてのアクセスの際にユーザに問い合わせ設定する．これらのプログラムはアンチウィルスソフトや，Google Desktop[9] のようにファイルのインデックスを作成するソフトウェアであり多くはない．

この技術により前記の (3)，(4) のアクセスパターンの自動設定の可能性を検証する．まず，(3) のアクセスパターンの多くは，オフィス系のアプリケーションがマイクロソフト社の OLE という機能を使って，複数のファイル形式からなる 1 つの文書をユーザが操作しているときにアクセスが発生する．一方，ウィルスが OLE を使って悪さをした場合には，ユーザは GUI で操作をしていない．このため，GUI の操作による判定で，正規のアクセスを判断できる．(4) に関しては，GUI を持たないアプリケーションの多くは OS のサービスであり，また GUI を持つアプリケーションはメーラなどのユーザのアプリケーションであることが多い．したがって，GUI 操作による判定と，OS が親であるかどうかの判定で自動設定が可能である．GUI を持たないユーザアプリケーションに関してのみ個別に設定する必要があるがその数は少ない．

ところで，この機能は，信頼できないアプリケーションに対して適用するとセキュリティ強度を低下させる恐れがある．そこで本システムでは，以下の 2 つのタイプの信頼できるアプリケーションに対してファイル利用コンテキストベースアクセス許可判定技術を使ったアクセス制御を行う．

【信頼できるアプリケーション】

- 本システム導入時にすでにインストールされていたアプリケーション：3.2 節で説明した「本ソフトウェア導入時は安全である」という前提から，この条件のアプリケーションは信用できると考える．
- ユーザが信用できると設定したアプリケーション

### 4.6 利 用 方 法

インストールは，ファイルアクセス制御エージェン

トを一度起動するだけである．以後常駐する．ユーザはこれまでと変わらない方法で PC を利用する．1 回目の起動時に，OS の管理情報を基に拡張子が登録されているアプリケーションに関して，ホワイトリストの構築を行う．この段階で登録されているアプリケーションは正常であるとして，以下の 2 つのルールをデフォルトの設定として登録する．

- 関連づけられているアプリケーションからのアクセスは正常アクセスである．
- アプリケーションの実行フォルダ以下のファイルからのアクセスは正常アクセスである．

以降のホワイトリストの管理は，そのつど，アクセス制限がかかった際にユーザが設定する．**図 7** にアクセスが制限されたときの画面例を示す．図のようにタスクトレイに吹き出しが表示される．図の例では，「Antinny.exe」というテスト用の GUI を持たないコマンドを作成し，「契約書.DOC」というファイルをコピーしようとした場合を示している．ここで何もせずに放置しておくと，吹き出しは閉じられアクセスが禁止されたことになる．もしアクセス権を変更したい場合には，吹き出しをクリックするとアクセス許可設定のダイアログが表示される（図 7 下）．このダイアログでは，このファイルのアクセス権の設定と，このファイルと同じ拡張子のファイルのアクセス権の設定をすることができる．また，今回のアクセスだけ許可することもできる．

### 4.7 システム構成

**図 8** にシステム構成を示す．「イベントフック部」は，アプリケーションと O3 の間に入り，GUI 操作で発生するイベントやファイルアクセスのシステムコールの呼び出しを横取り（フック）するモジュールである[10]．「GUI 操作監視部」[11),12)] は，マウス，キーボードなどの入力を検知するモジュールである．どのプロセスのどの GUI 部品が利用されたかが分かる．「ファイルアクセス監視部」[11),12)] は，Open，Close，Read，Write などのアクセスの種類やそのパラメータであるファイル名を検知するモジュールである．「アクセス許可判定部」は，ファイルアクセスがあったプロセスに対して許可と禁止の判断を行うモジュールであり，監視結果をホワイトリストにマッチさせて判定する．「ホワイトリスト」は，アプリケーションごとに許可するファイルアクセスを設定したものである．

アクセスの禁止があった場合，このことが O3 のイベントログに登録される．これにより，どんなプログラムが禁止のアクセスを行ったかが一覧でき，ウィルスの発見に役立つ．


**図 7** アクセス制限時画面例
Fig. 7 Screen shots at illegal file access detection.

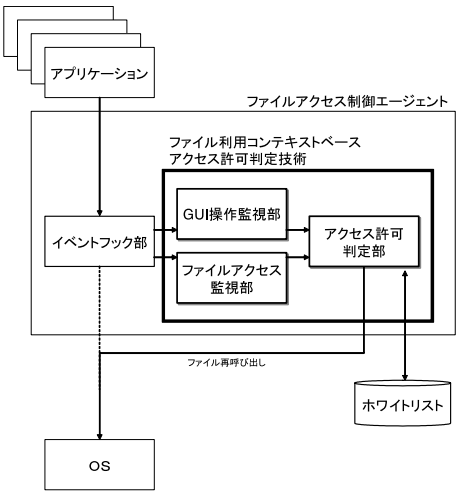


**図 8** システム構成図
Fig. 8 System architecture.

## 5. 評　　価

### 5.1 評価方法

以下のユーザに約 1 カ月間試用してもらった．

**被験者**：Winny ユーザ 3 名：自宅の PC で本ソフトウェアと Winny を利用してもらう．

非 Winny ユーザ 2 名：会社の PC で本ソフトウェアを利用し通常の業務を遂行してもらう．

なお，被験者はいずれもソフトウェアの研究開発者で MS-Office，ブラウザ，メール，プログラミングソフトを主に利用．Winny でダウンロードするコンテンツはユーザごとに異なるが，使い方は同じであり，ユーザの分類は必要ないと考える．使用した Winny は 2006 年 5 月現在の最新版（2.0Beta7.1）である．

**評価の目的と評価方法**：

**（評価項目 1）** Winny がこれまでと変わらず利用できるかどうかを以下の観点から Winny 被験者へヒアリングして評価する．

- 利用データの種類
- ダウンロードの成功確率の変化
- アップロードの成功確率の変化
- ダウンロード，アップロードの速度

**（評価項目 2）** 通常の業務がこれまでと変わらず遂行できるかどうかを被験者全員へ印象のヒアリングと，本システムのログにより評価する．

**（評価項目 3）** 情報漏えい対策の効果ついて，典型的な以下の 2 つのウィルスのパターンで評価する．

パターン 1：Winny の設定ファイルを書き換えて，共有フォルダを書き換える．

パターン 2：Winny 共有フォルダへファイルをコピーするプログラムを実行する．

**（評価項目 4）** 設定などの使い勝手について，被験者全員へ印象をヒアリングすることで評価する．

### 5.2 評 価 結 果

**（評価項目 1）** 利用データの種類：3 名ともに AVI，MP3 などのメディア系のファイル，および画像などの複数ファイルを zip などでアーカイブしたファイルを交換していた．メディア系ファイルは，まったくこれまでと同じように利用できたが，zip ファイルだけは，アクセスコントロールがかかり，エージェントからの問合せに対して毎回，「このファイルを許可」を選択して利用する必要があった．これは，機密情報が zip ファイルで圧縮されている可能性があるため，Winny からの zip ファイルのアクセスを許可することはできないことが原因である．少し面倒ではあるが，ファイル単位にユーザが確認して許可する必要がある．

ダウンロードの成功確率の変化：ダウンロードに失敗した場合に，本システムを起動せずに再ダウンロードをしてもらった．その結果，9 ファイル中 8 ファイルが再ダウンロードできなかったため，本システムが原因ではなく，ネットワークなどの他の要因でダウンロードできなかったと考えられる．被験者全員のアンケート結果からも，ダウンロードの成功確率は変わらないとの印象であった．

アップロードの成功確率の変化：Winny の共有フォルダへファイルを追加し，被験者全員がアップロードされたことを確認した．

ダウンロード，アップロードの速度：正確には測定できないが，被験者全員のアンケートによると変わらないとの印象であった．

以上の結果から，Winny がこれまでと変わらず利用できると考えられる．

**（評価項目 2）** アプリケーションの速度，安定性に変化がないか被験者全員へアンケートを行った結果，被験者全員が特に変化はないと回答があった．本システムの設定の手間に関しては，平均すると，6.2 個の設定をする必要があった．設定の回数を導入日数別にカウントすると（**図 9**），試用期間の初日に半分程度の設定が完了し，最初の 4 日間で全被験者はほとんどの設定を終えていた．

以上のことから，設定全体のコストはそれほど高くなく，また，一度設定が完了するとほとんど保守することなく運用できると考えられる．ただし，今回の試用期間中には OS のセキュリティパッチを適用する必要がなく，被験者はだれも新たなソフトウェアをインストールしていない．こういった状況ではある程度の再設定は必要になるが，更新されたアプリケーションに関する設定のみであることから，それほど煩雑な設定にはならないと考えられる．

**（評価項目 3）** パターン 1 は，Winny の設定ファイルはテキストファイルであるためテキストエディタで変更したところ，適切にアクセス制限がかかりファイルがアップロードされないことを被験者全員が確認した．

パターン 2 は，ファイルのコピーの方法として，以下の 3 種類を調査した．

- エクスプローラでコピー
- コマンドプロンプトの Copy コマンドでコピー
- 低レベルリード，ライトの API（NtCreateFile）を使ってコピーする自作プログラムでコピー

被験者全員がどの方法においても，コピーの制限がかかることを確認した．

以上のように，本システムでは，Winny を媒介とし

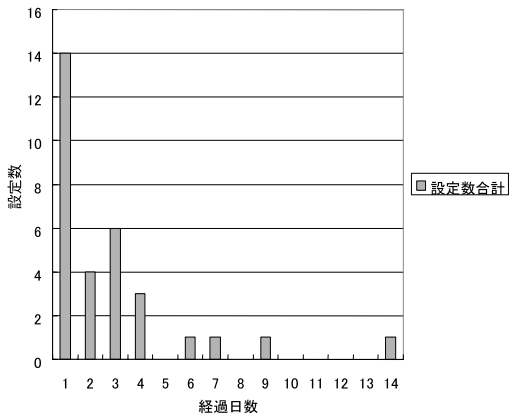


**図 9** 導入日別設定回数
Fig. 9 Number of configuration operations.

たウィルスの典型的動作において，正しくアクセス制限がかかることが確認できた．

**（評価項目 4）** 煩雑に感じたユーザは 1 名もいなかった．使い勝手のコメントとしては，アクセス制御の通知の仕方はタスクトレイの吹き出しのユーザインタフェースを利用しているが，気がつきにくいという意見があった．確かに，アクセス制限がかかっていることに気がつかなければ，アプリケーションがフリーズしているように見える可能性がある．現状のユーザインタフェースでも問題ではないが，こういった細かなユーザビリティに関しても今後工夫していきたい．

## 6. 考　　察

### 6.1 Winny ユーザによる本エージェントの導入

PC の自宅での利用が，企業内での利用と本質的に違うのは運用を強制できないところである．したがって，利用したいと思わせることが重要である．

Winny ユーザは，セキュリティのモラルは低くなく[13]，故意に漏えいさせているわけではない．アンチウィルスやファイアウォールは導入しており，Winny の設定も間違っていない．ただし，Winny の利用を優先しているために Winny の利用ポートはオープンになっており，より確実にダウンロードするためにアンチウィルスソフトを一時停止しているユーザもいる．

評価実験の結果，本エージェントは，Winny を通常どおりに利用できるソフトウェアであり，使い勝手も良く，導入されると考える．

### 6.2 従来のファイルアクセス制御技術との比較

ファイルアクセス制御技術は，マイクロソフト社のウインドウズや UNIX などの広く普及している汎用的な OS に付属の「任意アクセス制御」と，国防などの非常に高度なセキュリティを要する場合に利用される Trusted OS に付属の「強制アクセス制御」があげられる．しかしこれらの方式には，以下の問題がある．

「任意アクセス制御」では，ファイルの所有者が，だれからのアクセスを許可するのかを設定することが基本である．したがって，あるプログラムがファイルにアクセスできるかどうかは，そのプログラムがだれの権限で動作しているかで決定される．すでに述べたように，PC ではほとんどのユーザは管理者権限を持って利用しており，この利用で感染したウィルスは簡単に管理者権限で動作できてしまう．よって，不正なプログラムからのアクセスを保護することは難しい．

「強制アクセス制御」では，取扱い資格のレベルをプログラム，ファイル，デバイスなどに設定でき，レベルの低いオブジェクトからレベルの高いオブジェクトへのアクセスに制限を加えることができる．しかしこういったレベル管理は，Trusted OS を運用するプロの技術者でさえ負荷が高いことが指摘されており[14]，PC のユーザが管理できるものではない．

研究レベルでは，こういった設定を簡易化するアプローチもある[15),16)]．文献 15) は，任意アクセス制御のファイルシステムのサーバに，強制アクセス制御のアイデアを部分的に導入している．つまり，プログラムとファイルのアクセス許可の対応関係をポリシで設定できる．しかしながらこれは，WEB サーバなど用途がすでに分かっている場合にポリシが記述できるのであり，PC での一般での利用には適用できない．文献 16) の方式はポリシを簡単に書くための手法が提案されている．しかし設定の中間言語を覚える必要があり，やはり PC のユーザがターゲットではなく，専門の技術者のための運用コストの削減が目的である．

以上のように，アプリケーションの利用が明確に定義できずユーザのスキルも低い PC 環境のファイルアクセス制御方式としては，ポリシの設定を半自動で生成する本方式が有効である．

### 6.3 従来の P2P ファイル共有システム対策システムとの比較

セキュリティベンダ各社から P2P ファイル共有システム対策システムが多く発売されている[3)]．いずれも「P2P ファイル共有システムを利用させない」ことが基本方針である．ところが，オフィスの PC で P2P ファイル共有システムを利用している例は少ない．P2P ネットワークにあるコンテンツは音楽や映像のファイルが中心であり，個人の自宅の PC での利用がほとんどと考えられる．自宅の PC での P2P ファイル共有システムのユーザは，P2P ファイル共有システムを利用できなくするソフトウェアを導入する動機はうすく，本提案のようにセキュアに利用する方法を考えることが現実解である．

### 6.4 DRM システムとの比較

漏れては困るファイルを DRM システムでカプセル化する解決策も考えられる[17)]．カプセル化されたファイルは認証を受けない限り利用することはできないため，たとえ漏れたとしても安全である．ところが，漏れては困るファイルは，オフィスの文章，設計書，ソフトウェアプログラムなど編集，二次利用が頻繁に行われるデータであり，これらをすべてカプセル化する運用は難しい．また，持ち出す際にだけカプセル化する方法も考えられるが，カプセル化のし忘れと，自宅 PC からオフィスに認証を受ける必要があり，この運用も難しい．やはり DRM は，音楽や映像などのリー

ドオンリーのコンテンツの権利保護のための利用が適しており，頻繁に更新されるオフィス機密文書は，ファイルアクセスを制御して漏えいを防止する本稿の手法の適用が適している．

### 6.5 テレワークシステムとの比較

オフィス以外で仕事をするいわゆるテレワークシステムの研究において，在宅勤務のセキュリティが問題にあげられている[18),19)]．ところが提案されている解決策は，VPN などで企業 LAN に接続しリモートデスクトップで利用することが基本であり，いったん自宅の PC へコピーした瞬間に情報漏えいの可能性がある．本研究で対象にした，企業ネットだけではなく，社員の自宅の PC や外部リソースのリスク管理に関しては解決できていない．現段階でも，オフィスのサーバからのデータ持ち出しは禁止の方向に動いているが，本方式は，万一持ち出された場合にも，ある程度の抑止効果が期待できる．

### 6.6 ファイルアクセス制御エージェントの汎用性

本方式は基本的には，(1) OS などの計算機プラットフォームと，(2) Winny などのアプリケーションに依存していない汎用的な技術である．

(1) について，試作したファイルアクセス制御エージェントは Microsoft の Windows 上で Microsoft の C++ を使って実装したが，この環境でのみ有効なソフトウェアではない．ファイルアクセスなど OS からのプリミティブなイベントをフックするイベントフック部は OS に依存せざるをえないが，ファイルアクセスを制御するコア技術であるファイル利用コンテキストベースアクセス許可判定技術は Windows OS に依存しない汎用的な技術である．なお，イベントフック部の実現は本エージェントでは API フックという手法[8)] を使ったが，UNIX の場合は，フィルタドライバなどを利用すればイベントのフックやアクセス禁止機能は実現できる．

(2) については，本方式は，Winny 特有のファイルアクセスや，ネットワークポート，設定ファイルなどを利用しておらず様々な P2P ファイル共有システムに対応できる．

### 6.7 Winny 自身の改造による対策ついて

もともと Winny は情報漏えいが今のように注目される時代の前に設計されたものであり，その脆弱性をウィルスに利用されている．たとえば，公開フォルダの設定を外部のプログラムから参照・変更できる部分を改造するだけで Winny のウィルス Antinny はうまく動作しない．ところが，Antinny のターゲットは Winny だけではない．すでに，トレンドマイクロの発表によれば，別の P2P ファイル共有ソフト Share の Antinny 型のウィルスが報告されている[20)]．つまり，P2P 型のソフトウェアはウィルスのターゲットになりやすく，本研究のように，特定のソフトウェアを改修するのではなく包括的な対策を考えるべきである．

## 7. おわりに

本稿では，ファイルアクセスを制御するエージェントソフトウェアを提案した．これにより，Winny のようなファイル共有ソフトをこれまでどおり利用しながら情報漏えいを防ぐことができることを評価実験により明らかにした．本研究は，企業ネットだけではなく，社員の自宅の PC などの外部リソースを対象としたリスク管理の方法をターゲットにしているところが従来研究との違いであり，ユビキタス時代の社会システムのセキュリティを考えるうえで重要である．

## 参考文献


1) 日経 BP 社：記事「Winny を介した情報流出事件」論．http://www.nikkeibp.co.jp/style/biz/associe/winny/060511_1st/index2.html
2) 官房長官記者発表，平成 18 年 3 月 15 日．http://www.kantei.go.jp/jp/tyoukanpress/rireki/2006/03/15_a.html
3) NEC：製品紹介ホームページ CapsSuite. http://www.sw.nec.co.jp/cced/capssuite/
4) 何書，木俵，田中：P2P カメラネットワークによる利用者の行動と体験の共有，情報処理学会 DBS 研究会（DBWS2005），2005-DBS-137, No.68, pp.485–490 (2005).
5) 岐部，中村，須永：メタデータキャッシングによる P2P 型検索手法，信学会技術報告，Vol.104, No.690 (NS2004 243-340), pp.299–302 (2005).
6) 通商産業省告示第 952 号，コンピュータウイルス対策基準．http://www.ipa.go.jp/security/antivirus/kijun952.html
7) 金子：Winny の技術，アスキー出版 (2005).
8) RFC1321, The MD5 Message-Digest Algorithm. http://www.ietf.org/rfc/rfc1321.txt
9) Google デスクトップホームページ．http://desktop.google.co.jp/
10) ジェフリー・リッチャー：Advanced Windows 改訂第 4 版，アスキー出版 (2001).
11) 喜田，坂本，高橋：CyberTrace：機密情報を高精度に保護・監視・追跡する企業内情報漏えい対策ソフトウェアの提案，情報処理学会第 68 回全国大会，分冊 3，pp.37–38 (2006).
12) 坂本，高橋，喜田：CyberTrace：OS イベントリアルタイム解析による高精度文書監視方式の提案，情報処理学会第 68 回全国大会，分冊 3，pp.33–34 (2006).

13) ネットアンドセキュリティ総研株式会社：ビジネスユーザの Winny 等の P2P ファイル共有/交換ソフト利用状況調査結果. https://www.netsecurity.ne.jp/3_6308.html
14) IPA：セキュアなインターネットサーバ構築に関する調査，IPA 調査報告書.
15) 荒井，佐々木，梅都，永井：マルチ OS 環境を利用したアクセス制御システムの実装と性能評価，情報処理学会論文誌，Vol.44, No.4, pp.1092–1100 (2003).
16) 中村，鮫島：Security-Enhanced Linux のアクセス制御ポリシ設定の簡易化，暗号と情報，セキュリティシンポジウム，CIS2003 (2003).
17) マイクロソフトデジタル情報保護ソリューション. http://www.microsoft.com/japan/office/business/irm/solution.mspx
18) 飯塚，小川，中島：セキュアなテレワーク支援システムとシステム利用時の安心感についての考察，情報処理学会研究報告，Vol.2004, No.88 (IS-89), pp.31–38 (2004).
19) 力武，菊地，永田，浅見：テレワーク勤務環境での情報セキュリティ管理，情報処理学会第 63 回全国大会，2B-2, pp.625–628 (2001).
20) トレンドマイクロウィルスニュース 2006/4/24. http://www.trendmicro.com/jp/security/report/news/archive/2006/vnews060424.htm

(平成 18 年 5 月 29 日受付)
(平成 18 年 11 月 2 日採録)

**喜田　弘司**（正会員）

1993 年岡山大学大学院工学研究科修士課程修了．同年日本電気（株）入社．グループウェア，エージェント，ナレッジマネージメント，モバイルサーチエンジン等の研究に取り組む．2003 年より NEC システムテクノロジー（株）システムテクノロジーラボラトリにて情報セキュリティ技術（本研究）に取り組む．現在，日本電気（株）インターネットシステム研究所勤務および，香川大学工学研究科博士課程在学中．ネットワークコミュニティ，ヒューマンインタフェース等に興味を持つ．

**坂本　　久**

1992 年大阪電気通信大学経営工学科卒業．同年 NEC 技術情報システム開発（現 NEC 情報システムズ）入社．現在，NEC システムテクノロジー（株）システムテクノロジーラボラトリ勤務．情報セキュリティ技術に取り組む．

**島津　秀雄**

1982 年慶応義塾大学大学院（修士）卒業後，日本電気（株）入社．大規模コールセンター部門の情報武装化と知識武装化を推進．同社インターネットシステム研究所研究部長を経たあと，NEC システムテクノロジー（株）システムテクノロジーラボラトリ所長．博士（政策・メディア）．2005 年人工知能学会功労賞受賞．

**垂水　浩幸**（正会員）

1988 年京都大学大学院工学研究科博士後期課程情報工学専攻修了．同年日本電気（株）入社．1997 年より京都大学助教授．2001 年香川大学工学部教授．2002 年（株）スペースタグ取締役を兼業．モバイル情報サービス，グループウェア，ネットワークコミュニティ，ヒューマンインタフェース等に興味を持つ．ACM，IEEE-CS 等会員．工学博士．