不正プログラムから情報資産を保護するクライアント向けファイルアクセス制御方式の提案

甲斐 賢[†] 荒井正人[†] 永井康彦[†,☆]
冨田 理[††,☆☆] 手塚 悟[†]

コンピュータのネットワーク化が進み社会基盤を担う一方で，ウイルス・ワーム感染は深刻な問題である．とくにウイルス・ワームがコンピュータ上の情報資産を外部に漏えいおよび改ざんした場合の被害は甚大である．このためウイルス対策ソフトの導入やセキュリティパッチ適用が一般に行われているが，ワクチンやパッチが間に合わない時間には情報資産が無防備になるという問題がある．この問題に対処するため筆者らはこれまでサーバ向けに，仮にコンピュータが侵入された場合にも情報資産を保護する耐侵入型アクセス制御を開発してきた．本アクセス制御は，情報資産にアクセスするプログラムを制限することで，情報資産の改ざんと漏えいを防止する．しかし情報資産はネットワークにおいてサーバに限らずクライアントにも多数存在する．そこで本稿では，耐侵入型アクセス制御をクライアントに適用したクライアント向けファイルアクセス制御方式を提案する．クライアントに適用するうえで，多用途なクライアントではポリシの決定に必要な正常アクセスの把握が困難となり，一般利用者でもポリシを設定できるように専門的な知識や煩雑な手間を不要とすることが課題となる．これに対し，正常アクセスの分析から多様なアクセスが代表的なパターンに分類できることを特定し，このパターンに基づくポリシ決定および設定を，OS の持つ構成情報を参照して準自動で行う方式としている．

Proposal of File Access Control Scheme for Client Protecting Information Assets from Illegal Programs

Satoshi Kai,[†] Masato Arai,[†] Yasuhiko Nagai,[†,☆]
Satoru Tomida[††,☆☆] and Satoru Tezuka[†]

The virus worm infection is a serious problem while the computer networking advances. Damage of leaking and falsification are especially extensive. It becomes measures indispensable to protect information assets from the virus worm even if neither the vaccine nor the patch are enough because the virus worm expands rapidly and cleverly more and more in recent years. So authors had developed “Intrusion-Resistant Access Control System (IRACS)” for the server which can prevent the falsification and the leakage even if the computer is invaded. The IRACS controls file access of program to information assets. But such information assets exist in not only the server but also the client in network system. In this paper, we apply the IRACS suitably to the client. In application to the client, first problem is the decision of the access control policy without the excess and deficiency to all-round client, and second problem is the policy setting without special knowledge and complex time. Against this, we analyze normal accesses and classify various accesses into typical patterns. And we make the policy decision based on this pattern and develop a method by a semi-automatic operation referring to configuration information on OS.

† 日立製作所システム開発研究所
Systems Development Laboratory, Hitachi, Ltd.
†† 日立製作所情報機器事業部
Mechatronics Systems Division, Hitachi, Ltd.
☆ 現在，日立製作所プラットフォームソリューション事業部
Presently with Platform Solution Division, Hitachi, Ltd.
☆☆ 現在，日立オムロンターミナルソリューションズ
Presently with Hitachi-Omron Terminal Solutions, Corp.

1. はじめに

コンピュータのネットワーク化が急速に進み社会基盤を担う一方で，コンピュータがウイルス・ワームに感染することは深刻な問題となっている．とくに近年ではウイルス・ワームの感染経路が多様化し急速に感染拡大する傾向があり，ウイルス・ワームの感染はコンピュータの管理者から利用者にいたるまで幅広い者にとって懸念事項となっている．たとえば，総務省が

民間企業・各種団体を対象に行った情報セキュリティ対策の実態調査[5]によると，過去1年間に発生したセキュリティ問題のうちウイルス・ワーム感染が圧倒的に多いと報告されており，今後も継続してウイルス・ワーム対策を強化していくことが重要となる．

ウイルス・ワームに感染したときの被害は多岐にわたり[10)~12)]，システムが起動できなくなることやネットワークトラフィックを著しく増大させるといった可用性の損失をはじめ，ウイルスが機密データを第三者に流出させる機密性の損失や，利用者が知らないうちにウイルスがデータを操作するといった完全性の損失まで広範囲となる．被害額の点からすると2003年の国内のウイルス被害総額は3,025億円と推計され[7]，とくに機密性が損失した場合の被害はたとえ1回でも甚大なものとなる．

一方，これまでクライアント・サーバ型により発展してきた企業のコンピュータネットワークにおいて，情報資産がサーバ側にあることは周知のとおりであるが，実際にはクライアント側にも多くの情報資産が存在する．たとえば文献4)によると企業における情報資産の約6割がクライアントに保護されないまま存在すると指摘されており，先に述べたウイルス・ワーム感染時の機密性や完全性の損失は，サーバよりもクライアントの方がより深刻な問題となっている．

情報資産はコンピュータ上でファイルという形式で存在する．クライアントにあるファイルとは，システムファイル，プログラムファイル，ユーザデータファイルに大きく分類できる．システムファイルやプログラムファイルはたとえ改ざんされてもインストールCDから復旧することができ，また漏えいの対象にはまずなりえない．一方ユーザデータファイルは，具体的にはクライアントで利用者が自ら作成したファイルや，サーバからダウンロードしたファイルなどが相当する．たとえば企業でいうユーザデータファイルは報告書や提案書や顧客情報などのデータを格納し，さらには動画や音声といったデータも格納することが予想される．これらのユーザデータファイルにこそ機密データや重要データが含まれる．過去にこのようなユーザデータファイルを狙うウイルスもいくつか確認されており[8]，今後はウイルス・ワームがユーザデータファイルを狙うことが増加することも推測される．よってユーザデータファイル自体をウイルス・ワームから保護することはますます重要性を増す．

本稿は以上のことから，クライアント上のユーザデータファイルを，ウイルス・ワームをはじめトロイの木馬といった不正プログラムから保護することを目的とした，クライアント向けのファイルアクセス制御方式を提案する．本稿で述べるファイルアクセス制御方式とは，筆者らがこれまでサーバ向けに開発してきた耐侵入型アクセス制御[1),2)]をクライアントに応用したものであり，一般利用者でも容易に使えるようにした次に示す特長を持つ．

- 多用途なクライアントに対して，正常アクセスの分析から多様なアクセスが代表的なパターンに分類できることを特定し，
- 上記正常アクセスを，OSの持つ構成情報を参照して準自動的にポリシ設定するようにした．
- ポリシ設定後の修正を，利用者が対話式な操作で実施できるようにした．

以下，2章で一般的なクライアント向けのセキュリティ対策を，3章で耐侵入型アクセス制御をクライアントに適用するうえでの課題を述べる．4章で課題を解決するためのクライアント向けファイルアクセス制御方式を提案し，5章で試作開発結果とその考察を述べる．

2. 不正プログラムからユーザデータファイルを保護するセキュリティ対策

本章ではまず，クライアントに侵入する不正プログラムからユーザデータファイルを保護する従来のセキュリティ対策を全般的に述べる．

2.1 クライアント向けセキュリティ対策の現状

不正プログラムからユーザデータファイルを保護するには，まずは不正プログラム自体のクライアントへの侵入を防ぐことが第1である．一般的に実施される対策には，次のものがあげられる．

- アンチウイルスソフトの導入
- OSセキュリティパッチをはじめとする各種パッチの適用
- パーソナル・ファイアウォール（FW）の導入

しかし，感染経路が多様化し急速に感染拡大するウイルス・ワームに対してワクチンの更新や最新パッチの適用が間に合わず，ウイルス・ワームに対してクライアントが無防備になるという時間帯が存在する．さらに，パーソナルFWでは利用者が安易なダウンロードを実施したときにトロイの木馬が侵入してくる場合には対応できない．よって，仮に不正プログラムがクライアントに侵入したとしても被害を防ぐ事後防止策も重要となる．こうした事後防止策には，次のものがあげられる．

- 制限付きアカウントの使用
- バックアップの実施

ここで制限付きアカウントの使用とは，利用者が通常は制限付きアカウントを使用し必要なときだけ OS 管理者権限を使用することで不正プログラムが侵入した場合にもコンピュータ全体に被害が及ぶことを防ぐものである．しかし，制限付きアカウントで読み書きするようなユーザデータファイルに対しては改ざん・漏えいの被害が及んでしまう．また，バックアップの実施では，バックアップをとるまでにユーザデータファイルを改ざんされた場合には復旧もできず，漏えいには無効である．よって，これらの事後対策をさらに補完できるような，ユーザデータファイルを直接的かつリアルタイムに保護できる対策が望まれ，この対策を実現する手段としてファイルアクセス制御が考えられる．

2.2 従来のファイルアクセス制御と耐侵入型アクセス制御

ユーザデータファイルを保護するファイルアクセス制御は，クライアントに適用することを考慮すると次の要件を満たすべきだと考える．

要件 1 専門知識を持たない者でも，手間をかけずに容易にアクセス制御の設定を行えること

要件 2 これまで作成・蓄積したユーザデータファイルを継承して利用できること

一般にファイルアクセス制御といえば，汎用 OS 付属のファイルシステムの多くが有する「任意アクセス制御」と，軍事向けなど高度なセキュリティを要する場合に利用される Trusted OS の持つ「必須アクセス制御」があげられる．しかしこれらのファイルアクセス制御には以下のような問題がある．

まず「任意アクセス制御」は，ファイルの所有者がファイルへのアクセス権（ファイルを共有可能とする範囲）を指定できるものである．しかし，2.1 節で制限付きアカウントを使用するときの現状でも述べたように，ユーザ A の権限で不正プログラムが動作した場合，ユーザ A にアクセス権が与えられたファイルはすべて無防備となる．よって不正プログラムからユーザデータファイルを保護することができない．

また「必須アクセス制御」とは，取扱い資格を与えられていないサブジェクト（ユーザやプログラムなど）は，機密性の高いオブジェクト（ファイルやデバイスなど）へのアクセスを制限されるものである．かりに不正プログラムが混入したとしてもユーザデータファイルへの被害を極小化することができる．しかしそもそも Trusted OS を運用するときにサブジェクトとオブジェクトの対応関係を設定すること自体が難しく運用負荷が高いと指摘されている[6]．一方でこうした運用負荷の高い必須アクセス制御のポリシ設定を簡易化するアプローチもある[13),14)]．これらは記述の複雑なポリシを直接編集するのではなく理解を容易にする中間言語を利用して設定簡易化する方式[13)] と，実際にプログラムやサービスを走行させて発生したアクセス履歴をもとに設定簡易化する方式[14)] である．しかし前者の中間言語を利用する簡易化方式では中間言語を理解することが前提であることから専門知識が必要となる．また後者のアクセス履歴をもとにした簡易化方式では多用途なクライアントに適用するにはますます手間がかかってしまう．よって前記（要件 1）を満たせない．またこれまで汎用 OS で作成・蓄積されることの多いユーザデータファイルは，アプリケーションの数の少ない Trusted OS では継承して利用することが難しくなり前記（要件 2）も満たせない．

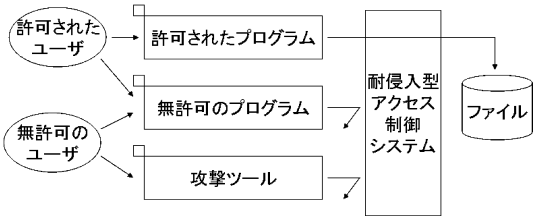

図 1 耐侵入型アクセス制御システムの概要
Fig. 1 The overview of Intrusion Resistant Access Control System.

以上述べた任意アクセス制御と必須アクセス制御とは異なるものとして，筆者らはこれまでに「耐侵入型アクセス制御」と呼ぶファイルアクセス制御を開発してきた[1),2)]．耐侵入型アクセス制御は主にインターネットサーバへの適用を対象としたものであり，**図 1** に示すようにファイルにアクセス可能なプログラムを制限できる．また汎用 OS にアドオン可能である．このため業務で利用するプログラムにあらかじめ限定しておけばユーザデータファイルを不正プログラムから保護することができる．このようなアクセス制御を決めるポリシ設定は，後述する 3.1 節で述べるように分かりやすい．またアプリケーションを継承利用できるため前記（要件 2）を満たす．よって筆者らはユーザデータファイルを保護するために耐侵入型アクセス制御を採用した．本稿では以下，前記（要件 1）を満たすことを目標としたポリシ設定の簡易化について述べる．

オブジェクト	ユーザ	プログラム	特徴値	アクセスタイプ
C:¥www¥catalog.htm	www	C:¥prog¥httpd.exe	0x1234	Read
C:¥www¥customers.txt	www	C:¥prog¥register.exe	0xabcd	Read,Write

図 2 サーバ向けのアクセス制御ポリシの例
Fig. 2 Example of access control policy for server.

3. 耐侵入型アクセス制御をクライアントに適用するうえでの課題

3.1 サーバ向けの耐侵入型アクセス制御

耐侵入型アクセス制御ではホワイトリスト型のポリシをもとに，ファイルアクセスの制御を行う．つまり，あらかじめポリシで許可しておいたアクセスだけを通し，それ以外のアクセスを禁止するというものである．たとえば，電子商取引の Web サーバに耐侵入型アクセス制御システムを適用する場合，**図 2** に示すポリシ例のように，サービス提供に必要最小限となる次のような正常アクセスだけを許可するよう各種パラメータを設定する．

(1) カタログ情報のファイル（catalog.htm）には，Web サーバのプロセス（httpd.exe）だけが読み込み可となるよう各種パラメータを設定する．
(2) 顧客情報のファイル（customers.txt）には，特定の CGI プロセス（register.exe）だけが読み書き可となるよう各種パラメータを設定する．

ここで図 2 に示すポリシ例の中でのパラメータの 1 つである特徴値とは，プログラムの真正性を確認するための情報（たとえば，プログラムのサイズやハッシュ値）を登録したものである．図 2 に示すポリシを設定した Web サーバ上では，保護対象オブジェクトに未許可のプログラムがアクセスしようとしてもブロックされ，さらに不正なプログラムが許可プログラムになりすましてアクセスしようとしてもブロックされる．一般にサーバは用途が限定的であり正常アクセスを特定しやすいため，サーバ向けにホワイトリスト型のポリシを設定することは容易となる．

3.2 課　　題

3.1 節で述べた耐侵入型アクセス制御をクライアントにも適用し，ユーザデータファイルを不正プログラムから保護しようとする場合，サーバに適用するときには問題にならなかったクライアント固有の課題が出てくる．

まずサーバ向けの場合にはサーバの用途が限定されるため，3.1 節で述べたようにサービス提供に必要な正常アクセスを把握しポリシを決めることが容易である．しかし，クライアントは多用途でありインストールされるプログラムも多様であるため，クライアント向けのホワイトリスト型ポリシを決めるのに必要となる正常アクセスの把握が困難となる．

次にポリシの初期設定は，サーバ・クライアントに関係なく耐侵入型アクセス制御を導入するときに必要な操作となる．しかし，クライアントの利用者はサーバの管理者に比べて十分に訓練されているとは限らず，たとえばはじめてポリシ設定を行うような場合には何を設定すればよいか分からないこともありうる．それゆえポリシを初期設定するための前提条件に，専門的な知識を求めることができない．またクライアントにインストールされるアプリケーションは 1 台ずつ異なることが多く個別設定が必要となるため，ポリシを初期設定することは煩雑な作業となる．さらに一度設定したポリシを修正するには，修正対象箇所を特定し適切なパラメータに変更するという手間がかかる．アプリケーションの追加や更新が頻繁に起こりうるクライアントでは，追加や更新のたびにパラメータの変更を余儀なくされ，このようなポリシ修正の手間は利用者にとっての負担となる．

以上をまとめると，耐侵入型アクセス制御をクライアントに適用するうえでの課題は次のとおりとなる．

課題 1 クライアント向けのホワイトリスト型ポリシを決めるのに必要な正常アクセスの把握が困難なこと
課題 2 専門的な知識や煩雑な手間を必要とせずにポリシを設定および修正できること

4. クライアント向けファイルアクセス制御方式の提案

本章では，3 章で述べたクライアントに適用するうえでの課題を解決した，クライアント向けのファイルアクセス制御方式を提案する．3 章で述べた（課題 1）に対して下記（解決策 1）で，（課題 2）に対して下記（解決策 2）（解決策 3）で解決することにした．

解決策 1 正常アクセスの分析によるクライアント向けホワイトリスト型ポリシの決定
解決策 2 OS の持つ構成情報を参照した準自動的なポリシ設定
解決策 3 対話式によるポリシ修正

次節よりそれぞれの解決策について具体的に説明する．

4.1 解決策 1：正常アクセスの分析によるクライアント向けホワイトリスト型ポリシの決定

（課題 1）に対してまず，クライアントで業務を遂行するのに必要なアクセス（以下，正常アクセスと称す）をサンプル収集し，次に収集した正常アクセスの

表 1 クライアントで想定される利用プログラムとその処理
Table 1 List of programs and that processes on clients.

利用プログラム	プログラムの処理
OS	起動，終了，ログイン，セキュリティパッチ適用
管理ツール	ユーザ設定，ディスク設定，ほか各種設定
エクスプローラ	コピー，移動，削除，名称変更，アクセス権変更，ゴミ箱を空にする，ゴミ箱から元に戻す
ウィルス対策ソフト	ファイルをスキャンする，パターンファイルを更新する
バックアップ	バックアップする，復元する
アーカイブソフト	圧縮，解凍
ネットワーク共有	リモートマシンからのファイルアクセス，各種ファイル操作
Web ブラウザ	ページ参照，各種設定変更，ダウンロード・アップロード
電子メール	メール送信・メール受信，添付ファイルの保存，メールへの添付，アドレス帳のインポート・エクスポート
ビジネスソフト（ワープロ，表計算，プレゼンテーション）	文書作成，編集，保存，印刷，OLE オブジェクトの埋め込み・リンク，Web ページとして保存

分析を行うこととした．クライアントで想定される利用プログラムとその処理の一覧を**表 1** に示す．

前記収集した正常アクセスをもとにホワイトリスト型ポリシを設定することも 1 つの方法（前記文献 14)）である．しかし，利用頻度が低いアプリケーションからのアクセスなど収集し忘れた正常アクセスがある場合には，不完全なホワイトリスト型ポリシとなってしまう．そのためクライアントに導入するたびに正常アクセスを収集しなくても済むように，前記収集した正常アクセスを何らかの着眼点からパターン化できないかと考えた．その結果，ユーザデータファイルに対する正常アクセスを**図 3**☆に示す 3 パターンにほぼ分類できることが分かった．

(1) 関連付けアプリケーション（AP）からのファイルアクセス（図 3 (1)）
ユーザデータファイルであればほとんどの場合，特定の AP と関連付けられているという点に着目した．ここで関連付け AP とは，ファイルに対するアクセス手段として利用される頻度の高いプログラムといってもよい．たとえばワープロファイルの場合，それに関連付けされたワープロソフトからのファイルアクセスが発生する．

☆ Microsoft Word, Microsoft Excel は，米国 Microsoft Corporation の商品名称です．Microsoft PowerPoint は，米国 Microsoft Corporation の米国，および，その他の国における商標です．Acrobat，Acrobat Reader は，アドビシステムズ社の登録商標です．

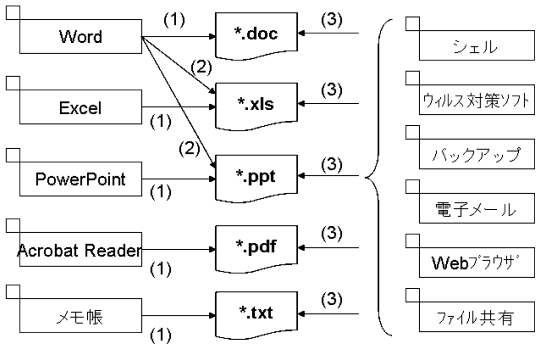

図 3 ユーザデータファイルに対するファイルアクセス
Fig. 3 File accesses against user data files.

表計算ファイルには表計算ソフトからのファイルアクセスが発生する．

(2) OLE 対応の AP からのファイルアクセス（図 3 (2)）
次に前記関連付け AP からは，関連付けされたファイル以外に対してもアクセスが発生する点に着目した．たとえばワープロソフトは，表計算ファイルで作成したグラフオブジェクトをワープロファイルに埋め込むために，表計算ファイルにアクセスする．このようなある AP のデータを別の AP のデータ内部に取り込む技術は Windows☆☆OS では OLE☆☆☆と呼ばれる．関連付けされたファイルには，関連付け AP 以外にも OLE に対応した AP からのアクセスが発生する．

(3) 用途別プログラムからのファイルアクセス（図 3 (3)）
さらに前記 (1)，(2) は主にユーザデータファイルの作成・編集という傾向が強いのに対して，そうした用途とはまったく異なる用途で利用するプログラムからのアクセスもある点に着目した．こうした特定用途のプログラムは**表 2** に示すように数を絞り込むことができるものとなる．この用途別プログラムからはあらゆるユーザデータファイルへのアクセスが発生する．

以上のパターン化によりユーザデータファイルへの多様な正常アクセスをまとめて把握できるようになる．

☆☆ Windows，Windows 2000，Windows XP は，米国 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．

☆☆☆ OLE は Microsoft Corporation が開発したソフトウェア名称です．OLE は Object Linking and Embedding の略です．

表 2 用途別プログラムの例
Table 2 Sample of programs for specified purpose.

用途	プログラム例
ファイル操作	シェル，圧縮・解凍ツール
セキュリティ	ウィルス対策ソフト，バックアップツール
ネットワーク	電子メール，Web ブラウザ，ファイル共有

よって，上記パターンのすべてを許可することを，クライアント向けのホワイトリスト型ポリシとして決定した．なお，上記パターンに分類されない正常アクセスがあったとしても後から容易にポリシに追加可能であることを 4.3 節で述べる．

4.2 解決策 2：OS の持つ構成情報を参照した準自動的なポリシ設定

上記（解決策 1）で述べたパターン化されたものの中には，レジストリといった OS の持つ構成情報を調べることで，ファイルアクセスの内容を具体的に知ることができるものがある．そこで（解決策 2）では，ポリシの初期設定時に OS の持つ構成情報を参照することで下記に示すようにポリシ原案を自動的に生成することにした．その後は利用者がポリシ原案を編集することで設定を完了できるようにする．

解決策 2a 関連付け AP と OLE 対応の AP からのファイルアクセスは，たとえば Windows OS ではレジストリに保持される情報から分かる[9]．ファイルの種類とそれにアクセスするプログラムを調べ，それらのファイルアクセスだけを許可するポリシ原案を自動生成する．

解決策 2b 用途別プログラムからはすべてのファイルの種類へのアクセスを許可するよう，ポリシを自動生成する．このような用途別プログラムのうち OS 標準で提供されるものならば，事前に分かる OS 標準の用途別プログラムをポリシ自動生成時に登録する．

解決策 2c OS 標準でない用途別プログラムは，利用者がクライアントを使い始めてからインストールしたものであると考えられる．OS 標準でない用途別プログラムは，インストールされたアプリケーションの中から利用者が選択できるようにする．

以上のような準自動設定とすることで（課題 2）にあげた専門的な知識や煩雑な手間を低減できる．

4.3 解決策 3：対話式によるポリシ修正

ポリシを初期設定した後に

- アプリケーションが追加や更新された場合，
- ユーザデータファイルへのアクセスが必要にもかかわらず，前記（解決策 2）で自動生成されるポリシではアクセス許可されない場合，

それらのアプリケーションはポリシで許可されていないためにユーザデータファイルにアクセスできない．前記の（課題 2）で述べたように，こうしたアプリケーションをポリシで許可するには，3.1 節で述べたポリシに対してパラメータの変更対象箇所を探す手間などが必要となり，利用者にとって手間がかかる．（解決策 3）では，必要なアクセスを許可したい場合に利用者が対話式にポリシを修正できるようにする．これにより利用者は変更対象箇所を探す手間をかけずにパラメータを変更することができる．

5. クライアント向けのポリシ設定支援ツールの開発

本章では，4 章で述べた方式に基づき試作したクライアント向けのポリシ設定支援ツールについて述べる．

5.1 利用者に要求する前提知識

前述の（解決策 2）ポリシ原案の自動生成によりファイルとプログラムとの対応関係といった専門的な知識はほぼ不要となるが，その一方で自動生成されたポリシ原案の編集のためにはツールの利用者にも多少の知識が必要となる．こうした編集時における前提知識も少なくて済むように，ポリシ設定支援ツールの開発にあたり，利用者が最低限次に示す前提知識を持っていれば原案を編集できるようにツールを設計した．

- ユーザデータファイルを置くフォルダの絶対パスを知っていること
- 重要データや機密データを格納するファイルの種類（拡張子）を知っていること
- クライアントに何のアプリケーションをインストールしたかを名称で知っていること

5.2 システム構成

クライアントとして Windows 2000/XP を対象にポリシ設定支援ツールを試作した．**図 4** に示すようにポリシ設定支援ツールは耐侵入型アクセス制御システムの一部をなし，本システムはほかに，ポリシファイルとアクセス制御部からなる．アクセス制御部はポリシファイルで決められたとおりにファイルアクセスを許可あるいは禁止するものであり，ポリシ設定支援ツールは利用者がポリシファイルを管理できるようにする役割を持つ．

ポリシ設定支援ツールの構成要素と役割は次に示すとおりである．

- ポリシ作成部
  前記（解決策 1）（解決策 2）に基づきポリシ原案を自動生成することや，利用者が編集を完了したポリシをポリシファイルに保存する役割を持つ．

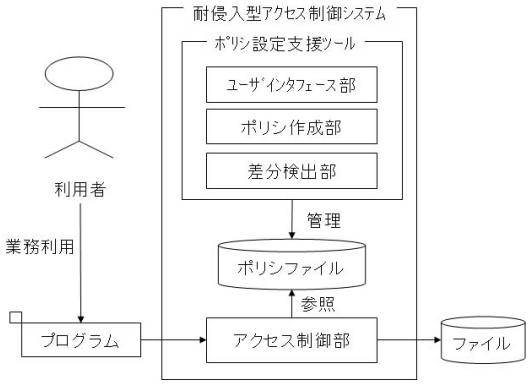

図 4 耐侵入型アクセス制御システムの機能構成
Fig. 4 Functional block diagram of Intrusion Resistant Access Control System.

- 差分検出部
  前記（解決策 3）に基づく対話式のポリシ修正で，利用者にポリシの修正案を提示するとともに，修正案に沿ってポリシファイルのパラメータ変更を行う役割を持つ．
- ユーザインタフェース部
  前記ポリシ作成部が自動生成したポリシ原案の利用者への提示や，利用者による原案の編集を行うためのインタフェースを提供する．また，前記差分検出部が提供する対話式のポリシ修正インタフェースを利用者に提示する．

なおクライアントの利用形態には，1 人 1 台が割り当てられる専用端末と，複数人で 1 台を利用する共用端末が考えられる．専用端末に本アクセス制御システムを導入する場合には，端末の利用者がそのまま本ツールの利用者となる．また共用端末に導入する場合には，管理者の役割を担う者がいると考えられることから，その管理者だけが本ツールの利用者となることとする．端末管理者が設定したポリシに従ってすべての端末利用者はクライアントを利用するものとなり，端末管理者以外はポリシをいっさい変更することはできない．

5.3 ポリシ準自動設定機能

ポリシ準自動設定機能は**図 5** に示す流れで処理を行い，ポリシの初期設定を実現する．処理の流れを下記 (1)〜(3) に示す．

(1) ポリシ原案の自動生成
利用者がポリシ設定支援ツールを起動すると，前記ポリシ作成部が前記（解決策 1）に述べたパターンを許可するように（解決策 2）のもとポリシ原案を自動生成する．

ところで 3.1 節に述べたポリシ設定によると，上記

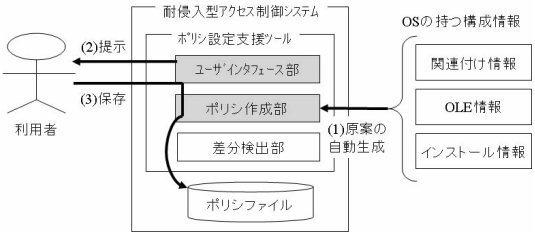

図 5 ポリシ準自動設定機能の処理の流れ
Fig. 5 Flow of processing of semi-automatic policy configuration function.

表 3 アクセス制御ポリシの設定項目
Table 3 Configuration parameter of file access control policy.

設定項目	サーバ向け耐侵入型アクセス制御	クラインアント向け耐侵入型アクセス制御	任意アクセス制御
オブジェクト	○	○	○
ユーザ	○	×	○
プログラム	○	○	×
特徴値	○	○	×
アクセスタイプ	○	×	○

○：設定する，×：設定しない

（解決策 2）だけでは自動生成できない設定項目として，保護対象オブジェクトの絶対パス，ユーザ，アクセスタイプ，特徴値も決めなければならない．これらの設定項目については次のように考え，設定を簡易化するようにした．

(a) ユーザデータファイルは，利用者が決めたフォルダ以下にまとめて置かれることが多い．たとえば Windows OS であれば「マイドキュメント」「デスクトップ」あるいは利用者が自ら定めたデータ用フォルダが考えられる．「マイドキュメント」「デスクトップ」を最初からポリシに登録し，その他のフォルダの追加も容易にする．

(b) ユーザとアクセスタイプは，ポリシ設定簡略化のためクライアント向けには指定しない．ユーザとアクセスタイプの設定は，汎用 OS のファイルシステムの有する任意アクセス制御に委ねる．実際には両者のアクセス権チェックが行われるため，両者を組み合わせることで**表 3** に示すようにサーバ向けと同等のきめ細かなアクセス制御を実現できる．

(c) プログラムの特徴値の検査を行うかどうかを，安全側を見てすべてのプログラムを対象に行うようにする．検査を不要とする場合には，簡略化のため一律に外せるようにする．

(2) ポリシ原案の編集
前記ポリシ作成部が生成したポリシ原案を利用者が確

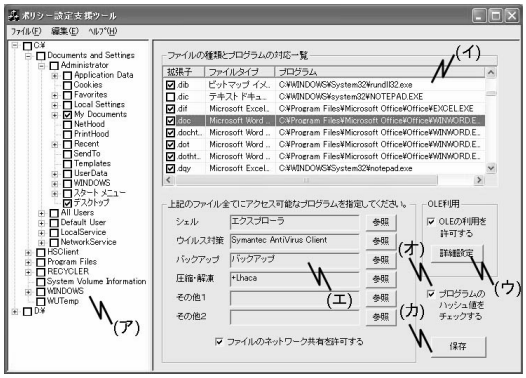

図 6 ポリシ編集画面
Fig. 6 User interface of policy editor.

認し編集できるよう，前記ユーザインタフェース部が**図 6** に示す画面を提供する．利用者は自動生成されたポリシ原案を編集すれば初期設定が完了する．以下に，原案の詳細と，利用者による編集項目を示す．なお前述した (1)(b) に基づき，ユーザおよびアクセスタイプの設定項目はない．

(ア) 監視対象とするフォルダの指定（図 6 (ア)）
原案：前述した (1)(a) のもと，「マイドキュメント」「デスクトップ」を登録．
編集：監視対象とするフォルダをたどってチェックをつける．

(イ) 保護対象とするファイルの指定（図 6 (イ)）
原案：（解決策 2a）のもと，関連付け AP からのアクセスをすべて許可．
編集：保護対象としない拡張子のチェックを外す．

(ウ) OLE 利用の許可と詳細設定（図 6 (ウ)）
原案：（解決策 2a）のもと，OLE 対応の AP からのアクセスをすべて許可．
編集：「詳細設定」ボタンを押下して**図 7** に示す OLE 利用許可の詳細選択ダイアログを開き，OLE 対応の AP の一覧の中からアクセスを許可しない AP のチェックを外す．

(エ) 用途別プログラムの指定（図 6 (エ)）
原案：（解決策 2b）のもと，OS 標準の用途別プログラムを登録．
編集：「参照」ボタンを押下して**図 8** に示す用途別プログラムの選択ダイアログを開き，（解決策 2c）に述べたようにインストールされたプログラムの一覧の中から該当するものを名称で選択する．

(オ) プログラムの特徴値の検査実施の指定（図 6 (オ)）
原案：前述した (1)(c) のもと，プログラムに対して一律に特徴値の検査を行う．
編集：特徴値の検査を行わない場合にチェックを外す．

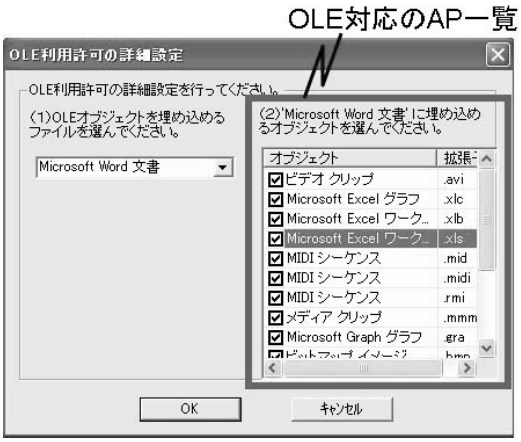

図 7 OLE 利用許可の詳細選択画面
Fig. 7 User interface of selecting program with OLE function.

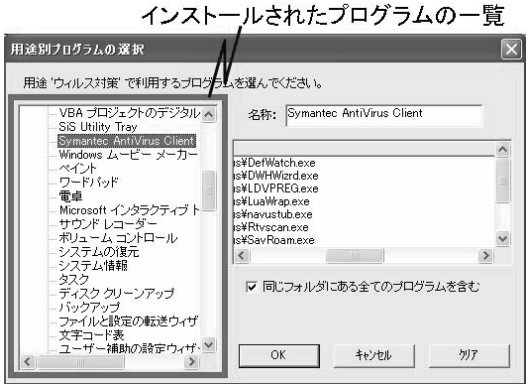

図 8 用途別プログラムの選択画面
Fig. 8 User interface of selecting program for specified purpose.

オブジェクト（フォルダ）
C:¥Admin¥ﾏｲﾄﾞｷｭﾒﾝﾄ¥
C:¥Admin¥ﾃﾞｽｸﾄｯﾌﾟ¥
D:¥Doc¥

オブジェクト（拡張子）	プログラム	特徴値	許可理由
*.doc	C:¥Prog¥Office¥Winword.exe	0x1234	関連付けAP
*.xls	C:¥Prog¥Office¥Excel.exe	0x2345	関連付けAP
*.xls	C:¥Prog¥Office¥Winword.exe	0x1234	OLE対応AP
.	C:¥Prog¥AntiVirus¥Scan.exe	0x3456	用途別-ウィルス対策

図 9 クライアント向けのファイルアクセス制御ポリシの例
Fig. 9 Example of file access control policy for client.

(3) ポリシファイルへの保存
利用者が図 6 の (カ) に示す「保存」ボタンを押下すると，前記ポリシ作成部がポリシを前記ポリシファイルに保存する．**図 9** にポリシの一部抜粋を示す．ポリシファイルへの保存が完了すると，保存したポリシに基づいて前記アクセス制御部がファイルアクセスを許可あるいは禁止する．

5.4 ポリシ対話型修正機能

ポリシ対話型修正機能は**図 10** に示す流れで処理を行い，対話的なポリシの修正を実現する．処理の流れ

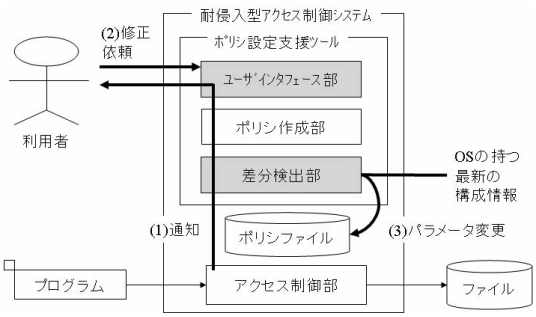

図 10 ポリシ対話型修正機能の処理の流れ
Fig. 10 Flow of processing of dialogical policy modifying function.

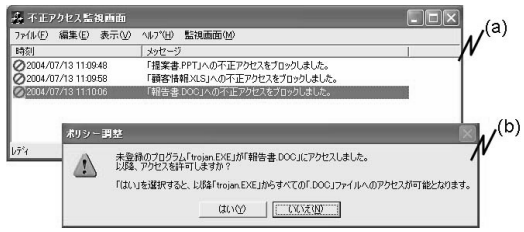

図 11 対話的なポリシ修正画面
Fig. 11 User interface of dialogical policy modifying.

を下記 (1)〜(3) に示す．

(1) ポリシ違反の通知

前記アクセス制御部はポリシと異なるファイルアクセスを検出したときに当該ファイルアクセスを禁止し，さらに前記差分検出部へと通知する．差分検出部は，**図 11** (a) に示す不正アクセス監視画面を提示し，ポリシに違反したアクセスが起きたことを利用者に通知する．

(2) 利用者からの修正依頼の受け付け

利用者は図 11 (a) に示す不正アクセス監視画面に表示される情報をもとに，ポリシを修正する必要性を判断する．ファイルアクセスが禁止されたままでよい項目については，利用者はそれ以上何もしない．必要なのに禁止されてしまっているファイルアクセスについては，利用者が図 11 (a) に示す不正アクセス監視画面上で該当項目をクリック選択することで，前記ユーザインタフェース部が図 11 (b) に示すポリシ調整ダイアログを表示し，そこで利用者は「はい」ボタンを押下してポリシの修正を依頼する．このような修正依頼の種類には，次に示すものがある．

(i) プログラム変更にともなう修正

既存アプリケーションのアップデートを行った場合，プログラムの特徴値がアップデート前と異なる場合がある．プログラムの特徴値を現在のものに修正する．

(ii) 関連付け情報変更にともなう修正

新規アプリケーションを追加するときにはレジストリの関連付け情報が追加・変更される場合がある．現在の関連付け情報をもとに導出したポリシに修正する．

(iii) 例外的なアクセス許可と変更

5.3 節で述べたポリシ準自動設定機能でアクセス許可されたプログラム以外にも，利用者が例外的にファイルアクセスを許可したい場合がある．このような例外的なアクセスを許可するようポリシを修正する．

(3) ポリシファイルに対するパラメータ変更

前記差分検出部は，利用者の修正依頼を受けてから OS の持つ最新の構成情報を参照してポリシの一部を再生成し，図 9 に示したポリシファイル中のパラメータを変更する．変更が完了すると，変更後のポリシに基づいて前記アクセス制御部がファイルアクセスを許可あるいは禁止する．

5.5 開発結果の考察

開発したポリシ設定支援ツールを，ポリシ設定の容易性とポリシ原案の有効性の点から考察する．

ポリシ設定に必要な知識はポリシ原案の編集に必要な 5.1 節に述べた前提知識だけあればよく，クライアントを使いこなせるような利用者にとって妥当なものだと考える．またポリシ設定に必要な手間は，ツールがポリシを準自動で設定するために，利用者はポリシ原案をベースにチェックボックスの付け外しや，候補一覧からの選択といった操作だけでポリシ設定を完了でき，初期設定に大きな手間はかからないと考える．定量的評価を行った文献 3) によるとポリシ設定完了までに 10 分以内の操作時間で済む見通しを得た．さらに対話式のポリシ修正ができるため，ポリシ設定後も利用者が確認をとりながらクリック 2 回で修正することができ，修正にも手間がかからないと考える．

また 5.3 節に述べたポリシ原案によると，レジストリから読み取った拡張子のすべてを対象に，その拡張子を持つファイルに対してアクセス制限を行うポリシとなっている．一般にユーザデータファイルの拡張子は，レジストリに登録される拡張子がほとんどだと考えられるため，ポリシ原案をそのまま使うだけでもユーザデータファイルに対する保護を漏れなく実施することができると考える．

なお本アクセス制御システムでユーザデータファイルを保護していても，ポリシで許可されたプログラム（以下，許可プログラムと称す）を不正プログラムが悪用してユーザデータファイルにアクセスすることも考えられる．このような悪用には，(1) 不正プログラムが許可プログラムの特徴値を変えずに感染する，(2) リモートから操作可能な許可プログラムを不正プログ

表 4 ポリシ自動生成時に参照する OS 上の構成情報
Table 4 Configuration on OS searched during policy semi-automatic generation.

ポリシ準自動生成時に参照する情報	Windows 2000/XP での参照箇所	Linux (Fedora Core 3) での参照箇所
関連付け情報	レジストリ	GNOME デトップの持つ MIME 設定ファイル
OLE 情報	レジストリ	OpenOffice アプリケーションの持つ OLE 設定ファイル
インストール情報	[スタート]-[プログラム] にあるショートカット一覧	「rpm -qa」コマンドの実行結果

ラムが操作する，といった状況がある．このような場合，提案方式では不正プログラムを原因としたアクセスと検知できない．このうち前記（1）は許可プログラムのソフトの脆弱性に起因するものと考えられ，そのため許可プログラムとして脆弱性の少ないプログラムを選定することが重要となる．また前記（2）についても，たとえば P2P ソフトのようにリモートから操作可能なプログラムを選定しないことが重要となる．

6. おわりに

本稿では，クライアント上のユーザデータファイルを不正プログラムから保護することを目的とし，これまで筆者らがサーバ向けに開発してきた耐侵入型アクセス制御をクライアントに応用したクライアント向けファイルアクセス制御方式を提案した．本方式は，多用途なクライアントに対して，正常アクセスの分析から多様なアクセスが代表的なパターンに分類できることを特定し，このパターンに基づくホワイトリスト型ポリシの決定および設定を，OS の持つ構成情報を参照して準自動で行うものである．また本方式に基づくクライアント向けのポリシ設定支援ツールを試作した結果，ユーザデータファイルを漏れなく保護できるポリシを，容易に設定できることを確認した．

また 4.2 節で述べた OS の持つ構成情報を参照したポリシ準自動設定の考え方は Windows OS だけに限らず，下記に示す情報を持つ OS に対してもそれらの情報を参照することでポリシを準自動設定できるものとなる．

- ファイルへのアクセス手段として利用される可能性のあるプログラムの情報（たとえば関連付け情報や OLE 情報）
- 用途別プログラムの情報（たとえばインストール情報）

一例として Linux☆OS の場合には**表 4** に示すように上記の各種情報を保有しており，これらの情報を参照すれば本稿で提案したポリシを準自動設定できる見通しを得た．

☆ Linux の名称は，Linus Torvalds の米国あるいはその他の国における登録商標あるいは商標です．

参考文献

1) 荒井正人ほか：マルチ OS 環境を利用したアクセス制御システム，第 61 回情報処理全国大会論文集（1），pp.45–46 (2000).
2) 荒井正人ほか：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).
3) 甲斐　賢ほか：クライアント向けファイルアクセス制御ポリシーの設計と簡易設定方法，信学技報，Vol.103, No.196, pp.123–130 (2003).
4) IDC: Business Continuity in 2002: It's Not Business as Usual (2002).
5) 総務省：情報セキュリティに関する実態調査 (2004 年 7 月).
http://www.soumu.go.jp/s-news/2004/040705_2.html
6) IPA：セキュアなインターネットサーバ構築に関する調査（トラステッド OS 利用とセキュア Web プログラミング），IPA 調査報告書 (2003 年 5 月).
http://www.ipa.go.jp/security/fy14/contents/trusted-os/guide.html
7) IPA：国内・海外におけるコンピュータウイルス被害状況調査 (2004 年 4 月).
http://www.ipa.go.jp/security/fy15/reports/virus-survey/index.html
8) IPA：「W32/Sircam」に関する情報 (2002 年 1 月).
http://www.ipa.go.jp/security/topics/sircam.html
9) Hipson, P.D.：システム管理者のための Windows 2000 Server レジストリガイド，ISBN 4-7973-1346-3，ソフトバンク (2000 年 9 月).
10) トレンドマイクロ社：用語集—ダメージ度 (2004 年 9 月確認).
http://www.trendmicro.com/jp/security/general/glossary/overview.htm#ダメージ度
11) シマンテック社：危険性の評価 (2004 年 9 月確認).
http://www.symantec.com/region/jp/sarcj/threat.severity_j.html
12) マカフィー社：ウイルスの危険度についての説明 (2004 年 9 月確認).
http://www.mcafeesecurity.com/japan/security/riskassesment.asp

13) 中村雄一ほか：Security-Enhanced Linux のアクセス制御ポリシ設定の簡易化，SCIS 2003 (2003 年 1 月).
14) 原田季栄ほか：プロセス実行履歴に基づくアクセスポリシー自動生成システム，Network Security Forum 2003 (2003 年 10 月).

(平成 16 年 10 月 27 日受付)
(平成 17 年 6 月 9 日採録)

甲斐　賢（正会員）

1996 年京都大学理学部数学科卒業．1998 年同大学大学院理学研究科修士課程修了．同年（株）日立製作所システム開発研究所入所．ネットワークセキュリティ，コンピュータセキュリティ，情報セキュリティ等の研究開発に従事．2000 年情報処理学会第 60 回大会奨励賞受賞．

荒井　正人（正会員）

1990 年日本大学理工学部電子工学科卒業．1992 年同大学大学院理工学研究科修士課程修了．同年（株）日立製作所入社．マイクロエレクトロニクス機器開発研究所を経て，システム開発研究所に勤務．以後，ネットワークシステム，情報セキュリティ等の研究開発に従事し，製品化に貢献．現在，同研究所主任研究員．

永井　康彦（正会員）

1983 年日本大学理工学部航空宇宙工学科卒業．1985 年同大学大学院理工学研究科修士課程修了．同年（株）日立製作所システム開発研究所入所．ネットワーク管理システム，グループウエア，情報セキュリテイ等の研究開発に従事．工学博士．現在，同社プラットホームソリューション事業部セキュリティソリューション部部長．電子情報通信学会，電気学会各会員．

冨田　理

1990 年豊橋技術科学大学情報工学科卒業．1992 年同大学大学院情報工学科修士課程修了．同年（株）日立製作所入社．2004 年日立オムロンターミナルソリューションズ（株）転籍．現在，端末システム事業部第 3 開発部担当課長として，主に金融，交通，自治体向け専用端末システムのミドルソフトウェア，業務アプリケーションソフトウェアの開発を担当．合わせて，ファイルアクセス制御機能を持つ情報セキュリティソフトウェア製品の開発に従事．

手塚　悟（正会員）

1984 年慶應義塾大学工学部数理工学科卒業．同年（株）日立製作所入社．マイクロエレクトロニクス機器開発研究所に勤務し，パーソナルコンピュータのオペレーティング・システム，デバイス・ドライバ，LAN システム等の研究開発に従事．その後，システム開発研究所に勤務．以来，パーソナルコンピュータを中心とした LAN システムの構築・運用管理の研究開発，さらにセキュリティシステムの研究開発に従事，現在に至る．東京工科大学非常勤講師（2005 年）．2004 年度情報処理学会論文賞受賞．工学博士．著書に『Inside CORBA』（共訳，アスキー出版，1998 年），『インターネットコマース—新動向と技術』（共著，共立出版，2000 年），『インターネット時代の情報セキュリティ—暗号と電子透かし』（共著，共立出版，2000 年）．