

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

甲斐 賢[†] 荒井 正人[†] 永井 康彦[†] 富田 理[‡]

[†] 日立製作所 システム開発研究所 〒212-8567 川崎市幸区鹿島田 890 日立システムプラザ新川崎

[‡] 日立製作所 情報機器事業部

E-mail: kai@sdl.hitachi.co.jp

あらまし 企業ネットワークにおいてはサーバと同様にクライアントにも情報資産がある。これまで報告者らは、サーバへの侵入により引き起こされる問題に着目し、侵入が発生した場合にも情報資産の保護を可能にする耐侵入型アクセス制御システムを開発してきた。一方、クライアントにおいても同様に不正なプログラムがデータ改ざんや情報漏えいを引き起こす脅威がある。しかし、クライアントは多用途であるため適切なアクセス制御ポリシーを定義することが難しく、耐侵入型アクセス制御システムをクライアントに応用することが困難であった。本報告では、多用途なクライアントに適したアクセス制御ポリシーの設計と、そのポリシー設定を簡易化するポリシー設定支援ツールの概要について述べる。

キーワード ファイルアクセス制御, アクセス制御ポリシー, クライアント, ポリシー設定

Configuration Tool of File Access Control Policy for Client

Satoshi KAI[†] Masato ARAI[†] Yasuhiko NAGAI[†] and Satoru TOMIDA[‡]

[†] Hitachi, Ltd., Systems Development Laboratory Hitachi System Plaza Shinkawasaki, 890, Kashimada, Saiwai-ku, Kawasaki-shi, Kanagawaken, 212-8567 Japan

[‡] Hitachi, Ltd., Mechatronics Systems Division

E-mail: kai@sdl.hitachi.co.jp

Abstract In enterprise network, clients as well as servers hold informational assets. We focused on problems caused by intrusion into servers, and proposed the access control system (IRACS: Intrusion Resistant Access Control System) which can protect informational assets even if intrusion occurred. On the other hand, informational assets on clients also can be caused by illegal programs to be altered and leaked. But we use clients for all-round, so it is difficult to define an appropriate access control policy for clients and to apply IRACS to clients. We describe what access control policy is suitable for clients, and the policy configuration tool which simplifies setting of the above-mentioned policy.

Keyword File Access Control, Access Control Policy, Client, Policy Configuration

1. はじめに

企業ネットワークにおいては、サーバと同様にクライアントにも多くの情報資産がある。クライアントでは利用者がメール送受信やダウンロード等のデータ通信を頻繁に行うため、不正なプログラムが混入し利用者の知らない間に動作してしまう可能性も高い。さらに、利用者が OS 管理者権限でクライアントにログインすることも多く、クライアントに混入した不正なプログラムが動作したときのデータ改ざんや情報漏えいはますます深刻なものとなる。そのため、クライアントにおけるセキュリティ対策も重要である。

近年、クライアント向けの主要なセキュリティ技術としてウィルス対策ソフトとパーソナル FW が普及し

てきた。しかし、ウィルス対策ソフトは既知のウィルスの検出や駆除はできても、未知のウィルスに対抗できない。またパーソナル FW は、トロイの木馬による不正な通信を検出し遮断することはできても、データ改ざんや情報漏えいそのものを防止することはできない。今後も新種のウィルスや高度なトロイの木馬が発生することを考えると、脅威から情報資産そのものを保護する技術、すなわちファイルアクセス制御が有効である。

報告者らはこれまで、サーバへの侵入が発生した場合にも情報資産の保護を可能とする耐侵入型ファイルアクセス制御システムを開発してきた[1][2]。今回、耐侵入型ファイルアクセス制御システムをクライアント

へと応用し、クライアント向けアクセス制御ポリシーの設定支援ツールを試作した。以下では、クライアントに応用する際の問題を述べ、クライアント向けのファイルアクセス制御ポリシーと、前記ポリシーの作成と修正を支援するポリシー設定支援ツールについて述べる。

2. クライアント向けファイルアクセス制御の課題

2.1. 従来のアクセス制御技術

汎用 OS における全てのプログラムは、アクセス制御機能を有するファイルシステム上で動作する。本アクセス制御は「任意アクセス制御」と呼ばれ、ファイルの所有者がファイルを共有可能とする範囲を設定できる。しかし、不正なプログラムがユーザ A の権限で動作すればユーザ A の利用可能な全てのファイルが危険にさらされる可能性がある。OS 管理者権限で不正なプログラムが動作すれば全てのファイルが無防備となる。よって、任意アクセス制御では不正なプログラムの動作による被害を防止できない。

一方、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 では、「必須アクセス制御」というアクセス制御が採用される。必須アクセス制御の下では、取り扱い資格を与えられていないプログラムは機密性の高いファイルへのアクセスを制限されるため、不正なプログラムによるファイルへの被害を極小化できる。しかし、Trusted OS のポリシー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[5]。またポリシー設定ができたとしても、従来クライアントで使われることの多い汎用 OS を Trusted OS に変えるとなると AP も変える必要があるが、Trusted OS で利用可能なワープロソフトや表計算ソフトなどの AP の種類が少ないため、クライアントに導入した場合、既存資産を継承して活用することが難しくなる。よって、必須アクセス制御もクライアントのセキュリティ対策には向かない。

報告者らがこれまでに開発してきたファイルアクセス制御システム[1][2]は、報告者らが「耐侵入型アクセス制御」と名付けたアクセス制御機能をもつ。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、汎用 OS にインストールすることで汎用 OS のアクセス権チェックよりも厳密なチェックを実施できることを特徴とする。耐侵入型アクセス制御は、図 2-1 に示すようにユーザ ID だけでなくプログラム ID も含めてファイルへのアクセス権をチェックするといったアクセス制御をおこなう。このため、OS 管理者権限であってもポリシーで許可されたプログラム以外からはファイルにアクセスできない。ファイルへのアクセス手

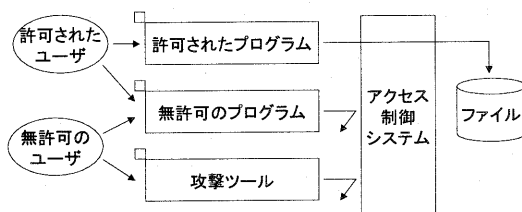


図2-1 耐侵入型アクセス制御システムの概要

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

図2-2 アクセス制御ポリシーの例

段を限定することで、不正プログラムによるファイルの改ざんや漏えいを防止し、情報資産の完全性と機密性を確保する。

例えば、電子商取引の WWW 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 2-2 に示すように、(1)改ざんされては困るカタログ情報のオブジェクト（ファイル、ディレクトリ）には、不正な書き込みを防ぐために Web サーバのプロセスだけが読み込み可となるポリシーを設定し、(2)漏えいしては困る顧客情報のオブジェクトには、不正な読み込みを防ぐために特定の CGI プロセスだけが読み書き可となるポリシーを設定する。このように耐侵入型アクセス制御システムのポリシー設定は理解が容易であり、適切なポリシー設定さえ行えばサーバだけでなくクライアントにも応用できるものである。そこで、クライアントにおいて不正なプログラムから情報資産を保護するために「耐侵入型アクセス制御」を採用することにした。

2.2. クライアント向けポリシー設定の課題

耐侵入型アクセス制御システムの技術をクライアントに適用する上で、次に示す 2 点が課題となる。

（課題 1）正当なアクセスと不正なアクセスとを区別し、適切なアクセス制御ポリシーを策定すること

不正なプログラムの動作から情報資産を守るには、ファイルへの必要最小限のアクセスのみを許可すれば良い。サーバであれば DB サーバや WWW サーバなどの用途に応じて情報資産が明らかになるため、正当なプログラムを定義しやすい。しかし、クライアントは

＊「特徴値」とはプログラムの真正性を確認するためのものであり、プログラムファイルのサイズやハッシュ値などを使う。このため、改ざんされたプログラムからはファイルにアクセスできない。

用途が限定されないことが多く、インストールされる AP も多様であるため、情報資産への必要最小限のアクセスを定義することは複雑なものとなる。そこで、クライアントに適したアクセス制御ポリシーを明確化し、設計する必要がある。

(課題 2)上記のアクセス制御ポリシーを容易に設定できること

総務省の調査報告[6]によると、セキュリティ製品を導入しない理由として「実施するノウハウがない」「手間がかかる」が挙げられている。そのため上記(課題 1)を解決しポリシーが明らかになったとしても、ポリシーを容易に設定できなければアクセス制御システム自体が導入されない。耐侵入型アクセス制御システムをクライアントに導入する場合でも、図 2-3 に示すようにポリシー設定はクライアントの業務利用に必ずついて回るものとなるため、ポリシー作成やポリシー修正の手間を極力少なくし、操作性も含めて利用者の負担にならないツールが必要となる。

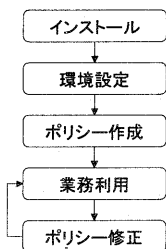


図2-3 アクセス制御システムの導入と運用の流れ

3. クライアント向けポリシーの設計

本章では、前記(課題 1)を解決するため、主要な情報資産に対する正当なアクセスを分析し、クライアント向けポリシーを設計した結果を述べる。

3.1. クライアントにおける情報資産

クライアントには、システムファイルやプログラムファイル、ドキュメントファイルなど多種のファイルが存在する。機密性と完全性の観点からすると、そのうち最も重要な情報資産はドキュメントファイル、すなわち利用者自身の作成するファイルであると言える。利用者の作成するファイルは、利用者が決めたフォルダの下にまとめて置かれることが多い。

3.2. クライアントにおけるファイルアクセスの分析

利用者の作成するファイルにはほとんどの場合何らかの AP と関連付けられている点に着目した。ここで関連付け AP とは、特定の種類のファイルへアクセ

スする際にそのアクセス手段として利用される頻度の高いプログラムのことであり、例えば Windows OS^{***}ではファイルの拡張子ごとに関連付け AP が、レジストリと呼ばれる OS 管理のデータベースにて定められている[3]。しかし、クライアントにおけるファイルアクセスを調査したところ、関連付け AP も含め、図 3-1 に示す 4 種類のアクセスが存在することが分かった。

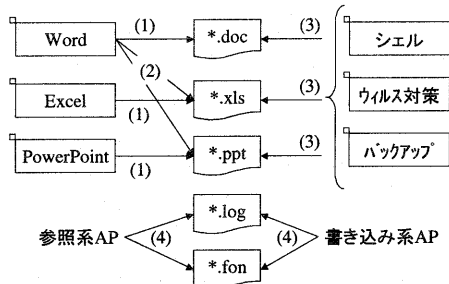


図3-1 クライアントにおけるファイルアクセス^{***}

(1)関連付け AP からのアクセス

同じ種類(拡張子)のファイルであれば、関連付け AP からのアクセスが発生する。例えば、ワープロファイルの場合、ワープロファイルに関連付けられたワープロソフトからのアクセスが発生する。表計算ファイルには表計算ソフトからのアクセスが発生する。

(2)OLE 対応の AP からのアクセス

関連付けられていない AP からのアクセスとして、例えば表計算ファイル中のグラフオブジェクトをワープロファイルに埋め込む場合がある。この時、ワープロソフトから表計算ファイルへのアクセスが発生する。ある AP のデータを別の AP のデータ内部に取り込むことができる技術は、Windows OS では OLE^{****}と呼ばれる。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アクセス

ドキュメントの作成や編集以外にもシステムを利用する上で特定の用途で用いるプログラムがある。表 3-1 に示すような用途別のプログラムからはあらゆる種類のファイルへのアクセスが発生しうる。

^{***} Windows, Windows 2000 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。

^{****} 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。

^{*****} 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 3-1 用途別プログラムの例

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	ウイルス対策ソフト, 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, ファイルサーバ

(4) 関連付けられたファイルへの共有アクセス

ある AP と関連付けられたファイルであっても、不特定多数の AP からアクセスが発生する場合がある。例えば、ログファイルであればログビューアに関連付けられていることが多いが、一方ログファイルへの出力をおこなう各種 AP からアクセスが発生する。また、フォントファイルであれば、関連付けられているフォントビューアだけでなく、各種エディタソフトからのアクセスも発生する。これらのファイルアクセスが制限されるとシステムの動作に支障がでることもあるため、基本的にはアクセスを制限すべきではない。

3.3. クライアント向けアクセス制御ポリシーの設計

クライアント向けポリシーは、3.1節で述べた情報資産に対し3.2節で述べたファイルアクセスだけを許可すれば良く、次に示すものとなる。このようにポリシーを定義すれば、クライアントを利用する上で支障がなく、かつ情報資産に対する不正なプログラムからのアクセスを防止できるようになる。

- ・ 情報資産を、フォルダとそのフォルダ以下に置かれるファイルの種類（拡張子）で指定する
- ・ 同一種類のファイルには、関連付け AP と OLE 対応の AP と用途別プログラムからのアクセスを許可し、それ以外のプログラムからのアクセスを禁止する
- ・ システムの動作に支障がでるファイルの種類にはアクセスを制限しない

4. ポリシー設定支援ツールの開発

本章では、前記(課題 2)を解決するため、試作したポリシー設定支援ツールについて述べる。

4.1. クライアントにおける設定項目

従来のサーバ向けのポリシー設定ツールでは、ポリシー設定時に図 2-2に示す全てのパラメータを設定する必要があった。しかし、クライアント向けポリシーではポリシー設定を極力簡略化するために「オブジェクト」と「プログラム」の対応関係のみを規定するものとし、「ユーザ」と「アクセスタイプ」についてはファイルシステムの ACL 設定に委ねることにした。実際には両者のアクセス権チェックが実施されるため、

表 4-1 アクセス制御ポリシーの設定項目

設定項目	サーバ向け	クライアント向け	ファイルシステムの ACL 設定
オブジェクト	○	○	○
ユーザ	○	×	○
プログラム	○	○	×
特徴値	○	○	×
アクセスタイプ	○	×	○

○: 設定可, ×: 設定不可

表 4-1に示すようにサーバ向けと同様のきめ細かなアクセス制御を実現できる。

また、従来のサーバ向けのポリシー設定ツールでは、オブジェクトとプログラムの対応関係を設定するときに、まずオブジェクトを指定し次にそのオブジェクトへのアクセスを許可するプログラムを指定する必要があった。しかし、クライアント向けポリシーの設計によれば、関連付け AP と OLE 対応の AP のようにファイルの種類が決まればプログラムも決まってくるものがある。さらに用途別プログラムも表 3-1に示した中には、OS が標準で提供するプログラムをユーザがそのまま利用することもある。そこでクライアント向けポリシー設定では、ポリシー設定支援ツールがポリシーの原案を自動生成するようにし、利用者は原案をカスタマイズすれば済むようにする。

4.2. システム構成

クライアントとして Windows 2000 を対象にポリシー設定支援ツールを試作した。図 4-1に示すようにポリシー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、本システムは他に、ポリシー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ーファイルで規定さ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、ポリシー設定支援ツールはポリシーファイルを管理する役割をもつものである。

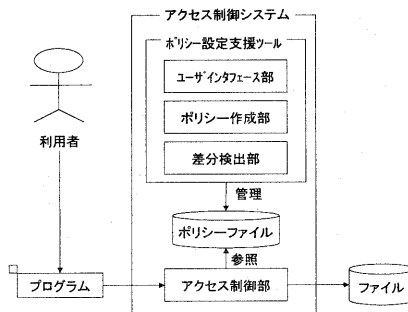


図 4-1 ポリシー設定支援ツールのシステム構成

ポリシー設定支援ツールの各構成要素について以

下述べる。

- ・ユーザインタフェース部

利用者へのポリシーの提示や、利用者からのポリシー編集を実現する。

- ・ポリシー作成部

OS 管理のデータベースなどを参照し、ポリシーの原案を自動生成する。

- ・差分検出部

業務利用中にアプリケーションの追加などが発生した場合でも、現在のポリシーと最新のシステム情報との差異を自動検出し、ポリシーの修正案を提示する役割を持つ。

4.3. ポリシー作成機能

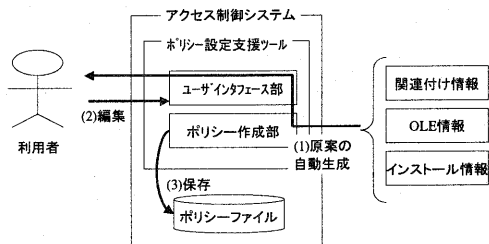


図 4-2 ポリシー作成機能の処理の流れ

ポリシー作成機能は図 4-2に示す流れで処理をおこなない、ポリシー原案を利用者に提示しポリシー編集を可能とする。これにより、クライアントの業務利用を開始するまでのポリシー作成の手間の削減を図る。

(1)ポリシー原案の自動生成

関連付け情報や OLE 情報は、Windows OS のレジストリに保持される[3]。そこで、ポリシー作成部がレジストリを検索し、関連付け情報や OLE 情報から分かるオブジェクトとプログラムの対応関係を導出し、それらのアクセスだけを許可するようなポリシーの原案を自動作成する。また、ユーザインタフェース部を通してポリシー原案を利用者に提示する。

(2)利用者による編集

利用者は、図 4-3に示すユーザインタフェースを通して各種の設定をおこなう。設定項目は次に示すとおりである。

(a)監視対象とするフォルダを指定する (左部)

デフォルトで「マイドキュメント」「デスクトップ」が登録される。利用者は必要に応じてフォルダのチェックボックスを指定/解除する。

(b)保護対象とするファイルの種類を指定する (上部)

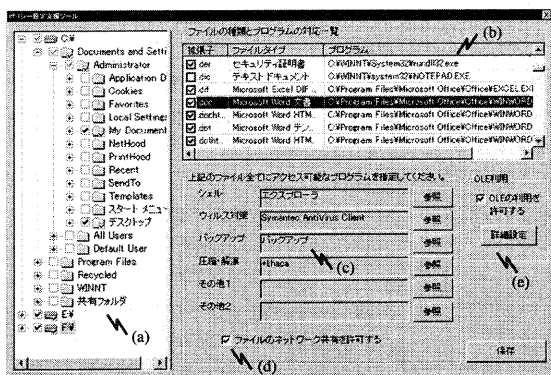


図 4-3 ポリシー作成画面

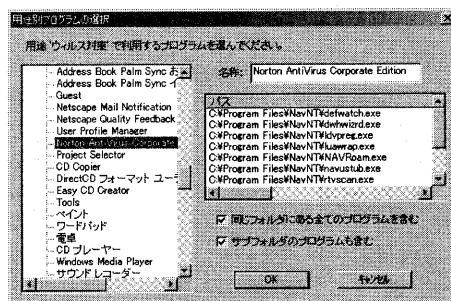


図 4-4 用途別プログラムの選択画面 (ポリシー作成画面で「参照」ボタン押下時に表示)

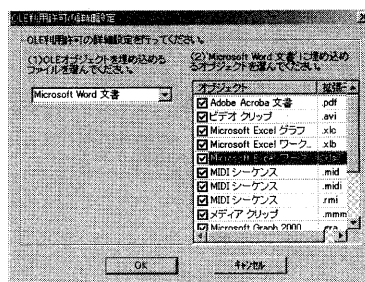


図 4-5 OLE 利用許可の詳細設定画面 (ポリシー作成画面で「詳細設定」ボタン押下時に表示)

デフォルトで、関連付けがありシステムの動作に支障が出ない拡張子すべてにチェックが付けられる。利用者は必要に応じて、拡張子のチェックボックスを指定/解除する。

(c)用途別プログラムを指定する (中央部)

デフォルトで OS 標準のプログラムが登録される。OS 標準でないプログラムは、図 4-4に示す画面から利用者が登録しなければならない。

(d)OLE 利用の許可、詳細設定をおこなう（右部）
デフォルトで全ての OLE 対応の AP からのアクセスが許可される。利用者は必要に応じて、図 4-5 に示す画面から OLE 利用許可のチェックボックスを指定／解除する。

(e)ネットワーク共有の許可をおこなう（下部）
デフォルトで許可される。利用者は必要に応じて、チェックボックスを指定／解除する。

なお(c)用途別プログラムを指定する画面（図 4-4）においては、利用者が容易に指定できるようにするため、インストールされたプログラムの一覧を名称で表示し、その中から利用者が選べるようにすることで、操作性を高めている。インストール情報を得るため、ポリシー作成部は Windows OS の[スタート]-[プログラム]に表示される AP を参照する。

(3)ポリシーファイルへの保存

ポリシーの編集が完了すれば、ポリシー作成部がポリシーファイルへとポリシーを保存する。図 4-6 にクライアント向けポリシーの一部抜粋を示す。

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

図 4-6 クライアント向けポリシーの一例

以上述べてきたポリシー作成機能により、主要な情報資産に対して正当なアクセスのみが許可されるようになるため、ほぼポリシー原案のままでもクライアントの業務利用に使えるようになる。利用者は最低(c)用途別プログラムのうち OS 標準でないプログラムの指定さえすればポリシー設定を完了できる。

4.4. ポリシー修正機能

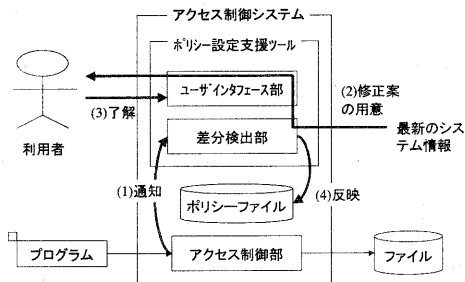


図 4-7 ポリシー修正機能の処理の流れ

ポリシー修正機能は図 4-7 に示す流れで処理をおこない、ポリシー修正案を利用者に提示する。これによ

り、クライアントでの業務利用中に必要となるポリシー修正の手間の削減を図る。

(1)修正トリガの通知

アクセス制御部はポリシーと異なるファイルアクセスを検出したときに当ファイルアクセスを禁止し、さらに差分検出部へと通知する。

(2)ポリシー修正案の用意

差分検出部は前記 OS 管理のデータベースをはじめ最新のシステム情報を参照することで、ポリシーに最新のシステム情報が反映されているかどうかを判断し、未反映であればポリシーの修正案を用意する。修正案の種類を次に示す。

(a)プログラム変更に伴う修正

利用者が了解したときには、該当するプログラムの特徴値を現在のものに更新する。

(b)関連付け情報変更に伴う修正

利用者が了解したときには、現在の関連付け情報をもとに導出したポリシーに修正する。

(c)例外的なアクセス許可と変更

画面例を図 4-8 に示す。「はい」押下時には、アクセスを許可するようポリシーを変更する。

メッセージ:例外的なアクセス許可と変更

未登録のプログラム「neweditor.exe」が、「personal.doc」ファイルにアクセスしようとしています。アクセスを許可しますか？

「はい」を選択すると、以降「neweditor.exe」から全ての「.doc」ファイルへのアクセスが可能となります。
「いいえ」を選択すると、アクセスを禁止します。

はい
いいえ

図 4-8 ポリシー修正画面の一例

(3)利用者による了解

利用者は図 4-8 に示したようなユーザインタフェースを通してポリシー修正案を確認し、了解あるいは却下する。もし利用者が不正アクセスだと判断すれば、修正案を却下すればよい。

(4)ポリシーファイルへの反映

利用者が了解した場合、差分検出部はポリシーファイルへと修正案を反映させる。

以上述べてきたポリシー修正機能により、一旦はファイルアクセスが禁止されるものの、提示される修正案を利用者が了解すれば、以降同じファイルアクセスが発生するときには許可されるようになる。

ところで、レジストリのもつ関連付けの情報が不正

に書き換えられた場合、利用者がレジストリの改変に気付かずに修正案を了解すると、不正なプログラムによるアクセスを許してしまうことになる。これを防ぐために、OS の起動時にレジストリの値を保存し、OS の稼働中はレジストリを常時監視しつつ、レジストリの改変を検出した時には保存していた値に強制的に戻すといった方法が考えられる。

5. ポリシー設定の簡易さの評価

本章では、試作したポリシー設定支援ツールの有効性評価（ポリシー設定の簡易さ）を評価した結果について述べる。

5.1. ポリシー作成の所要時間

ポリシー作成はクライアントの業務利用を開始するまでに必要となる作業であり、利用者にとって許容できる時間内におさまるかどうかのポイントとなる。許容時間の目安を知るために、広く普及したソフトウェアならば一般的な利用者が許容できているものと考え、表 5-1 に示すように製品シェアの高い汎用ソフトウェアの導入時間を調べたところ、10 分という目安が得られた。

また、利用者による操作時間を定量的に図るには実測する方法もあるが、今回、ユーザインタフェースの定量化手法である「GOMS キーストローク・レベル・モデル」[4]という方法を利用した。この GOMS (Goals Operators Methods Selection-Rules) 法とは、ユーザインタフェースが決まった時にそのユーザインタフェースを利用して特定の目標を達成するための所要時間を机上で予測する方法である。具体的には、目標を達成するための操作をキーボードやマウスのオペレーションにまで分解し、オペレーション毎に標準的な時間を当てはめ、時間の総和を予想操作時間とするものである。

本 GOMS 法を、ポリシー作成時に利用する図 4-3 から図 4-5 に示すユーザインタフェースに適用したところ、表 5-2 に示す結果が得られた。

また利用者が必要に応じてポリシー原案をカスタマイズする場合の所要時間を計算した。前提として、利用者がカスタマイズする可能性が高いと考えられる項目以外は、ポリシー原案のまま利用すると仮定した。

- ・監視対象フォルダを Nmon 個選択あるいは解除
- ・保護対象ファイルを Nprt 種選択あるいは解除
- ・OS 標準の用途別プログラムを原案のまま利用
- ・OS 標準でない用途別プログラムを 2 種登録（ウィルス対策、圧縮・解凍）
- ・OLE 利用許可を原案のまま利用
- ・ネットワーク共有許可を原案のまま利用

表 5-1 汎用ソフトウェア製品の導入時間の目安

ソフトウェア名	導入時間	製品シェア
バックアップソフト(V社)	10分	56.0%(世界)
グループウェアソフト(C社)	10分	19.9%(国内)

表 5-2 ポリシー作成時の設定項目と所要時間

#	設定項目	利用者による操作	予想操作時間
a	監視対象フォルダの指定	必要に応じて、フォルダ一覧から選択・解除	26.9秒
b	保護対象ファイルの指定	必要に応じて、拡張子一覧から選択・解除	8.35秒
c	用途別プログラムの指定	OS標準でないプログラムを登録	13.65秒
d	OLE利用許可の指定	必要に応じて、OLE利用一覧から選択・解除	22秒
e	ネットワーク共有の指定	必要に応じて、選択・解除	3.05秒

※予想操作時間は、GOMSモデルにより算出した。

※操作時間は、1つのフォルダ当たり、1つの拡張子当たりなどの単位時間を示す。

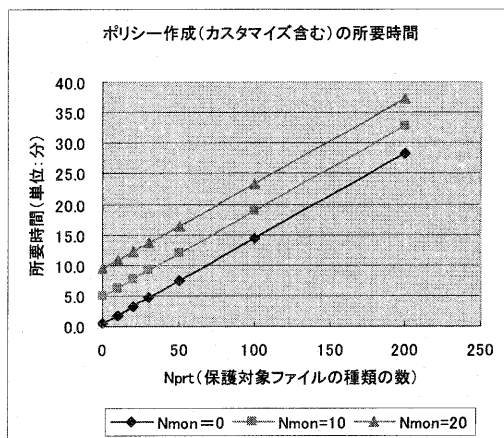


図 5-1 原案カスタマイズを含むポリシー作成の所要時間

このとき、所要時間 = $26.9 \times Nmon + 8.35 \times Nprt + 13.65 \times 2$ (秒) で表され、結果をグラフ化したものを図 5-1 に示す。ここでポリシー原案に含まれる保護対象ファイルの種類は、Windows 2000 をインストールした直後の状態で約 150 種、オフィス系ソフトをインストールした後の状態で約 200 種あるため、Nprt の値を 200 までとして計算した。

以上の結果、10 分という目安の許容時間内では、一例として監視対象フォルダを 10 個まで、保護対象ファイルを 30 種までカスタマイズできることが分かる。平均的な利用者によるカスタマイズを想定すると、監視対象フォルダとして「マイドキュメント」「デスクトップ」以外に指定するフォルダの数は 10 個を超えないものと考えられ、また保護対象ファイルとしてシステムの動作に支障が出る以外の理由でカスタマイズするよ

うなファイルの種類も 30 種を超えないと考えられる。従って、ポリシー作成の所要時間は利用者が許容できる時間内におさまると考える。

5.2. ポリシー修正の所要時間

ポリシー修正はクライアントの業務利用中に必要となる作業であり、修正作業がクライアントの業務利用を妨げないことがポイントとなる。ポリシー修正では、クライアントの業務利用中に表示される図 4-8 に示すようなダイアログから、利用者が 4.4 節の (2) に述べた (a) から (c) のいずれかのメッセージに答えることになる。ポリシー修正項目に対する利用者による操作と GOMS 法による予想操作時間を表 5-3 に示す。いずれの場合もダイアログに表示されるボタンのどれか一つを利用者が押下するという操作となり、GOMS 法による予測値が 3.05 秒であることが分かった。そのため、ポリシー修正の必要があっても業務利用の大きな中断にはならないと考える。

ここで図 4-8 に示すようなダイアログは、クライアントでの業務利用中に利用者の意図しないタイミングで出てくるものであるため、利用者がダイアログの文面を理解し判断するのに手間取ることも考えられる。しかし、怪しいファイルアクセスなら「いいえ」を選ぶことを利用者が徹底すれば、選択に迷う時間もほとんどないと考える。

表 5-3 ポリシー修正時の設定項目と所要時間

#	設定項目	デフォルト内容	利用者による操作	予想操作時間
a	プログラム変更に伴う修正	「いいえ」にフォーカス	「はい」「いいえ」のいずれかを選択	3.05秒
b	関連付け情報変更に伴う修正	「いいえ」にフォーカス	「はい」「いいえ」のいずれかを選択	3.05秒
c	例外的なアクセス許可と変更	「いいえ」にフォーカス	「はい」「いいえ」のいずれかを選択	3.05秒

※予想操作時間は、GOMSモデルにより算出した。

6. おわりに

外部不正である未知ウィルスやトロイの木馬による被害を防止することを目的とし、クライアント向けに耐侵入型アクセス制御システムのポリシー設定支援ツールを試作し、簡易なポリシー作成およびポリシー修正ができること示した。ポリシー設定の簡易さを定量評価したところ、ポリシー作成が利用者の許容時間内におさまり、ポリシー修正がクライアントの業務利用を妨げない程度であることが分かった。そのため試作したポリシー設定支援ツールは有効なものであり、実用に耐えうるものと考えられる。

文 献

- [1] 荒井ほか：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 年 10 月)。
- [2] 荒井ほか：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 Number4，pp.1092-1100(2003 年 4 月)。
- [3] Peter D.Hipson：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)。
- [4] ジェフ・ラスキン：ヒューメイン・インタフェース～人にやさしいシステムへの新たな指針～，ISBN 4-89471-420-5，ピアソン・エデュケーション(2001 年 9 月)。
- [5] 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)。
- [6] 情報セキュリティ対策の状況調査 ～世界的に情報セキュリティ対策の関心が高まる中で～，総務省調査報告書(2002 年 9 月)。