個人用コンピュータのための直感的なセキュリティ管理機構*

品川 高廣

東京農工大学工学部情報コミュニケーション工学科
E-mail: shina@cs.tuat.ac.jp

1 概要

近年のインターネット接続環境の普及にともない，一般の個人が使用するコンピュータがウィルスなどによる不正アクセスに巻き込まれるケースが急増している．しかし，従来のオペレーティングシステムが提供するセキュリティ機能は，その概念やメカニズムに関する専門的知識が必要であり、コンピュータの専門家ではない一般の個人には正しく管理することが困難である．

本研究の目的は，個人用コンピュータを対象として，専門的知識がないユーザでも容易にセキュリティを維持できるようにするための，オペレーティングシステムによる新しいセキュリティ機構を開発することである．本研究では，セキュリティ管理に関する機能を可能な限り自動化して管理の負担を減らすとともに，シンプルかつ直感的な管理システムを提供することで，一般の個人でも容易に管理できるシステムの実現を目指す．

2 従来の OS の問題点

従来のオペレーティングシステムは，もともと軍や企業など大規模な組織で使用することを想定して設計されている．そのため，一般の個人が占有して使用するコンピュータで利用した場合，そのセキュリティ管理機能には様々な問題が生じる．

ユーザ単位の保護　従来のオペレーティングシステムのセキュリティモデルは，主に共有して利用する複数のユーザ間の保護を目的としている．従って，保護の単位は「ユーザ」であり,「ユーザ」より細かい単位での保護はあまり提供されていない．例えば UNIX では,「ユーザ」毎に割り当てられたユーザ ID に基づいてファイルのアクセス制御などを行なっている．また，管理作業は root と呼ばれる特別なユーザ（管理者）が行なうことになっている．

しかし個人用コンピュータでは，一般にそのコンピュータを使用するのは一人のユーザであり，ユーザ間の保護はあまり必要ではない．また，管理者と使用者は同一人物になるため，その区別が曖昧になっている．従って，ユーザ単位の保護は，個人用コンピュータでの利用形態にそぐわないモデルになっている．

複雑なセキュリティ管理作業　従来のオペレーティングシステムは，一般に専門の管理者の存在を仮定しているため，管理作業が専門的で複雑になっている．また，管理作業を行なうためには，オペレーティングシステムが提供しているセキュリティモデルに関する専門的知識が必要である．例えば UNIX におけるファイル管理では，chmod コマンドを用いてファイルのアクセス権（パーミッション）を設定するが，アクセスする主体を所有者 (owner)，所属グループ (group)，その他 (other) の 3 つに分けて，それぞれに対して読み込み (read)，書き込み (write)，実行 (exec) という 3 つの権限を与えるかどうかを指定することになる．このような設定には，所有者や所属グループといった概念を理解している必要があり，コンピュータの専門的知識を持たない一般の個人には難しい作業である．

閉じた環境の想定　従来のオペレーティングシステムのセキュリティモデルは，基本的に LAN のような閉じた環境で使用することを想定して設計されている．従って，インターネットのように，システムの外から入手したファイルなどに対してアクセス制御を行なう仕組みが備わっていない．例えば，ユーザがインターネットからダウンロードしたファイルは，所有者がそのユーザとなり，もともとユーザが所有していたファイルと区別がつかなくなる．このように，その安全性・信頼度や責任の所在が異なるファイルを同じように管理してしまうために，ウィルスなど悪意を持ったプログラムを一般のプログラムから区別することが難しくなっている．

3 PeSeMo の機能

本研究では，個人用コンピュータでの使用を想定した新しいセキュリティ機構を備えるオペレーティングシステム PeSeMo[1]（仮称）を開発する．PeSeMo では，専門的知識のない一般の個人でも管理できるような直感的な

*第 15 回コンピュータシステム・シンポジウム
ポスターセッションアブストラクト（2003 年 12 月 12 日）

[1] Personal Security Manager in the operating system

セキュリティ管理機構を実現を目指す．また，オペレーティングシステムのレベルで情報の流れを把握することにより，従来は把握していなかった作者や入手元などの情報を管理することにより，管理作業を可能な限り自動化することを目指す．

3.1 直感的アクセス制御

PeSeMo では，アクセス制御を個々の資源ごとに直接設定する代わりに，同じようなアクセス制御が適用される資源をグループ化して，ラベルとしてわかりやすい名前を付けて管理する．ラベルのついたファイルに対して，どのプログラムがどのようなアクセスを許可するかといったアクセス制御の設定は，システムであらかじめ定義したものを用意しておく．これによって，ユーザはアクセス制御機構に関する詳しい知識がなくても，ラベルを張り替えるといった直感的な作業だけでアクセス権を管理出来るようになる．従って，個々のユーザは自分でアクセス制御の設定を考える必要がなくなり，管理を容易にすることができる．

例えば，ユーザのメールの内容が格納されたファイルに対しては,「メール」というラベルを付けられるようにする．ラベルの設定はユーザもしくはメールソフトが行なう．これによって，例えばメールのファイルはメールソフトだけが読み書きできるといったアクセス制御を比較的容易に実現できる．また，メールで送られてきたファイルを Web で公開したくなった場合には，ファイルについたラベルを「Web 文書」などに張り替えることによって，例えば FTP プログラムから読み込んで，Web サーバにアップロードすることができるようになる．

このようにファイル毎にラベルをつけることによって,「ユーザ」より細かい単位での保護を可能にしつつ，同じアクセス制御が適用されるファイルをグループ化してまとめて管理することにより，記述しなければならないアクセス制御の量を減らして管理が複雑になるのを防いでいる．また，アクセス制御の記述を個々のファイルから分離することにより，様々な状況で用いることができる一般的なラベルをあらかじめテンプレートとして定義しておくことを可能にする．これによって，アクセス制御を設定するという作業をユーザから隠蔽して，専門的な知識がなくても直感的に管理することが可能になる．

3.2 出所追随管理機構

一般のユーザに対するセキュリティ管理の負担をできるだけ減らすために，従来は管理者が行っていたような作業を可能な限りシステムソフトウェアのレベルで自動化する．例えば，インターネット上の信頼できないサイトからダウンロードしたプログラムは，自動的にアクセス権を制限して実行することにより，不正アクセスを防止するなどの機能を実現する．

これを実現するために，本研究では，ファイルなどの資源の出所を把握・管理するための機構をオペレーティングシステムに組み込む．従来のオペレーティングシステムでは，例えば，ネットワーク経由でやり取りされるデータの所有者や作者などに関する情報は把握されておらず，どのようなデータが入っているのか全く分からなくなっている．これに対して本研究では，送信元 IP アドレスやデジタル署名などの情報を元に，カーネルやオペレーティングシステム内で流れるデータの出所に関するデータを把握・管理する．

このファイルの出所に関する情報を前述のラベルに基づくセキュリティ機能と組み合わせることで，自動的かつ柔軟な保護を実現することができる．例えば，未知のサイトから送られてきたメールの添付ファイルを閲覧するときは,「未知のサイト：添付ファイル」といったラベルが付けられ，自動的に他のメールファイルへのアクセスは禁止したサンドボックス内で実行するなどの保護ポリシーが実現できる．

また，この機能を利用することによって，ソフトウェアの自動更新システムを安全に実行する枠組みを構築する．セキュリティを向上させるための基本的な管理作業として，WindowsUpdate のような機能でセキュリティ上の欠陥があるソフトウェアを更新する作業があるが，闇雲に様々なソフトで自動更新を許可すると，かえってウィルスなどが侵入する手段となる危険性がある．そこで，この出所を管理する機能を利用して，自動更新プログラムで更新可能なファイルは，同じサイトからダウンロードしたファイルに限る，等といった保護ポリシーを適用することにより，ソフトウェアの自動更新を安全に行うことができる．

4 まとめと今後の課題

本稿では，個人用コンピュータのための新しいセキュリティ機構についての提案を行なった．ファイル毎に分かりやすいラベルをつけることによって，一般の個人でも容易にアクセス制御を管理できるようになる．また，オペレーティングシステムのレベルで出所を管理することで，適切なラベル設定をするための情報を確保し，できるだけ管理作業を自動化出来るようにする．

今後の課題としては，具体的に用意すべきラベルの種類をリストアップし，それぞれのアクセス制御をどのように記述すればよいか考察することや，ラベルの数が増えた時にどのように管理するかなどについて考察することなどが挙げられる．