情報漏洩防止のための出力先毎に制御可能なファイルアクセス制御方式

岩永 真幸† 毛利 公一††
†立命館大学大学院 理工学研究科 ††立命館大学情報理工学部

1 はじめに

近年，情報の漏洩事件が頻繁に発生している．JNSAセキュリティ被害調査ワーキンググループによる個人情報漏洩事件・事故の調査分析 [1] では情報漏洩の原因が，紛失・置忘れ，管理ミス，誤操作が多くを占めていることが示されている．また，この調査結果では，漏洩原因別の一件当たりの漏洩人数は，内部犯罪・内部不正行為によるものが最も多く，他の原因に比べて飛びぬけて多いことがわかる．これは，すなはち，内部の人間による情報漏洩である．そのため，外部からの攻撃からデータを保護することを目的としている認証，暗号化，侵入検知などの従来のセキュリティ技術だけでは，これらの原因による漏洩を防止することができない．

文献 [1] では，情報漏洩の経路についても述べられており，USBメモリやCD-Rなどのリムーバブルメディアと紙媒体が多くを占めており，次いで，ネットワークが挙げられている．リムーバブルメディアは小型で発見が困難であり，大容量であるため利用されやすい．リムーバブルメディアやネットワークなどデジタルデータとして情報が漏洩してしまうと，情報の拡散が極めて速いという特徴があるため，回収することが非常に困難であると同時に被害が大きくなりやすい．文献 [1] では，経路別の一件当たりの漏洩人数は，リムーバブルメディアが圧倒的に多いという結果がでており，デジタルデータによる被害を防止することは重要である．

これらの原因や経路による情報漏洩を防止するためには，情報漏洩を発生させる可能性のある計算機資源へのアクセスを制御する必要がある．このような背景から，我々は，Privacy-aware OS *Salvia*[2] の開発を行っている．Salviaは，ファイルを保護の単位とし，ファイルの出力先ごとに制御を行うことによって，データの伝播範囲を制御する．

2 *Salvia* のデータ保護方式

2.1 システムコール制御

情報漏洩を防止するためには，情報漏洩を発生させる可能性のある計算機資源へのアクセスを制御する必要がある．そのためには，データの出力先である計算機資源ごとに制御を行う必要がある．データの出力先には，大きく以下の3つに分類することが可能である．

- 同一計算機
- 外部計算機
- 外部記憶装置

これらの計算機資源に出力される際に，情報漏洩が発生する可能性がある．同一計算機内への情報漏洩は，ファイル，パイプ，ソケットなどへのデータの出力であり，ファイルのコピーやプロセス間通信によって重要なデータが他プロセスへ漏洩するケースである．外部計算機への情報漏洩は，ネットワークを介した情報漏洩であり，重要なデータがネットワークを通じて外部計算機へ漏洩するケースである．外部記憶装置への情報漏洩は，USBメモリやCD-Rなどのリムーバブルメディアを用いた情報漏洩であり，重要なデータがリムーバブルメディアに書込まれ持出されるケースである．情報漏洩を防止するためには，同一計算機内で利用されることを許可し，外部計算機や外部記憶装置に持出されることを禁止するといったような制御が必要となる．よって，これらの計算機資源アクセスは，情報漏洩の観点から区別して制御する必要がある．

これらの計算機資源への出力は，必ずシステムコールによって行われる．よって，*Salvia* は，システムコールの制御を行うことで，計算機資源へのアクセスを制御する．

2.2 コンテキストとデータ保護ポリシ

Salvia は，ファイルを保護の単位とし，保護が必要なファイルごとに保護ポリシを定義することができる．*Salvia* は，この保護ポリシに基づいてファイルの制御を行う．保護ポリシは，ファイルへの危険な操作を定義するため，コンテキストを用いて記述することが可能である．これにより，データが漏洩する危険性のある状況を記述し，システムコールの制御を計算機の状況に応じて行う．利用可能なコンテキストは，ユーザ，位置，時刻，IPアドレスなどである．コンテキストを利用することにより，管理者のみファイルの編集が可能，社内のみファイルの読込みが可能，会議の時間内でのみファイルを閲覧可能，特定の計算機にのみファイルを送信可能といった記述が可能となる．

ユーザは，保護ポリシをXMLを用いて記述することができる．*Salvia* は，それをバイナリに変換し，保護すべきファイルと対応するiノードの拡張属性領域に格納

File access control based on target devices for preventing data leakage
Masayuki Iwanaga† and Koichi Mouri††
†Graduate school of Science and Engineering, Ritsumeikan University
††College of Information Science and Engineering, Ritsumeikan University

表 1　システムコールの分類

分類名	システムコール
read	read, readv, pread64, mmap, mmap2, readahead
write	write, writev, pwrite64, sendfile, sendfile64, mmap, mmap2, munmap
send_local	write, writev, sendfile, sendfile64, mmap, mmap2, socketcall, ipc, mq_timedsend
send_remote	write, writev, sendfile, sendfile64, socketcall

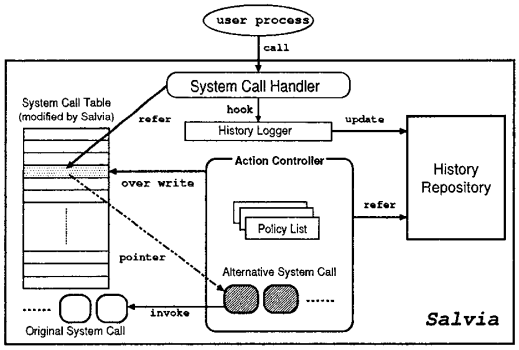

図 1　*Salvia* の構成

して管理している．保護ポリシは，コンテキストを用いてシステムコールごとに制御条件を定義可能であるが，システムコールは多数存在するため，すべてのシステムコールについて，その実行の許可・禁止を定義した場合，ポリシが膨大になり，記述ミスが起こる可能性が高くなる．よって，表 1 に示すように，システムコールを処理内容やデータの伝搬範囲に着目し，read，write，send_local，send_remote に分類している．2.1 節で述べた同一計算機の資源による情報漏洩は，ファイルへのアクセスやプロセス間通信によって発生するため，read，write，send_local によって情報漏洩を防止することが可能である．外部計算機による情報漏洩は，ネットワークを通じた情報漏洩であるため，send_remote によって情報漏洩を防止することができる．外部記憶装置による情報漏洩は，リムーバブルメディアに対する書込みによって情報が漏洩するため，write システムコールによって情報漏洩を防止することが可能である．しかし，write は，同一計算機の情報漏洩を防止する際にも利用されているため，リムーバブルメディアへの書込みであることを区別して保護ポリシに記述することを可能とした．

3　*Salvia* の実装

Salvia は，OS でデータの漏洩を防止する．OS によってデータ漏洩を防止することにより，アプリケーションのセキュリティ機能が不完全であっても情報漏洩を防止することが可能である．プロセスは，ファイルをオープンすることにより，ファイルへのアクセスを開始する．そのため，*Salvia* は，保護ポリシが設定されているファイルがオープンされると，プロセスに対してその保護ポリシを適応する．そして，*Salvia* は，そのプロセスが表 1 のシステムコールを実行すると，コンテキストと保護ポリシを比較し，そのアクセスの可否を決定する．

Salvia の構成を図 1 に示す．*Salvia* は，システムコールの履歴を取得する History Logger，History Logger が取得したシステムコールの履歴をプロセスごとに管理する History Repository，システムコールの可否を決定する Action Controller で構成されている．プロセスが，システムコールを呼び出すと，History Logger によってプロセスの履歴がとられ，History Repository に蓄積される．History Repository には，コンテキストも蓄積されている．そして，呼び出されたシステムコールが，System Call Table を参照し，実行される．システムコールは，Action Controller によって SystemCall Table を書き換えることによって変更されている．これにより，システムコールが実行された際にアクセス制御を行うことが可能である．この書き換えられたシステムコールの中で，出力先を区別する．システムコールの種類，pipe や socket が生成するオブジェクト，ファイルシステムの情報，メジャー番号，マイナー番号を用いることで出力先を判断し，プロセスに付加されている保護ポリシと HistoryRepository を参照することにより，そのシステムコールの可否を判定する．

4　おわりに

情報漏洩事件が今も頻繁に発生しており，それらを防止するためには，データの出力先である計算機資源へのアクセスを制御する必要があることについて述べた．このような背景から，我々は，Privacy-aware OS *Salvia* の開発を行っていることについて述べ，その保護法式と実装方法について述べた．

参考文献

[1] NPO 日本ネットワークセキュリティ協会; JNSA 2007 年情報セキュリティインシデントに関する調査報告書, http://www.jnsa.org/result/2007/pol/ incident/2007incidentsurvey_v1.32.pdf

[2] 鈴来和久，一柳淑美，毛利公一，大久保英嗣 : "Privacy-Aware OS Salvia におけるデータアクセス時のコンテキストに基づく適応的データ保護方式," 情報処理学会論文誌:コンピューティングシステム Vol. 47 No. SIG3, pp. 1-15 2006.