機密情報の拡散追跡機能の研究開発

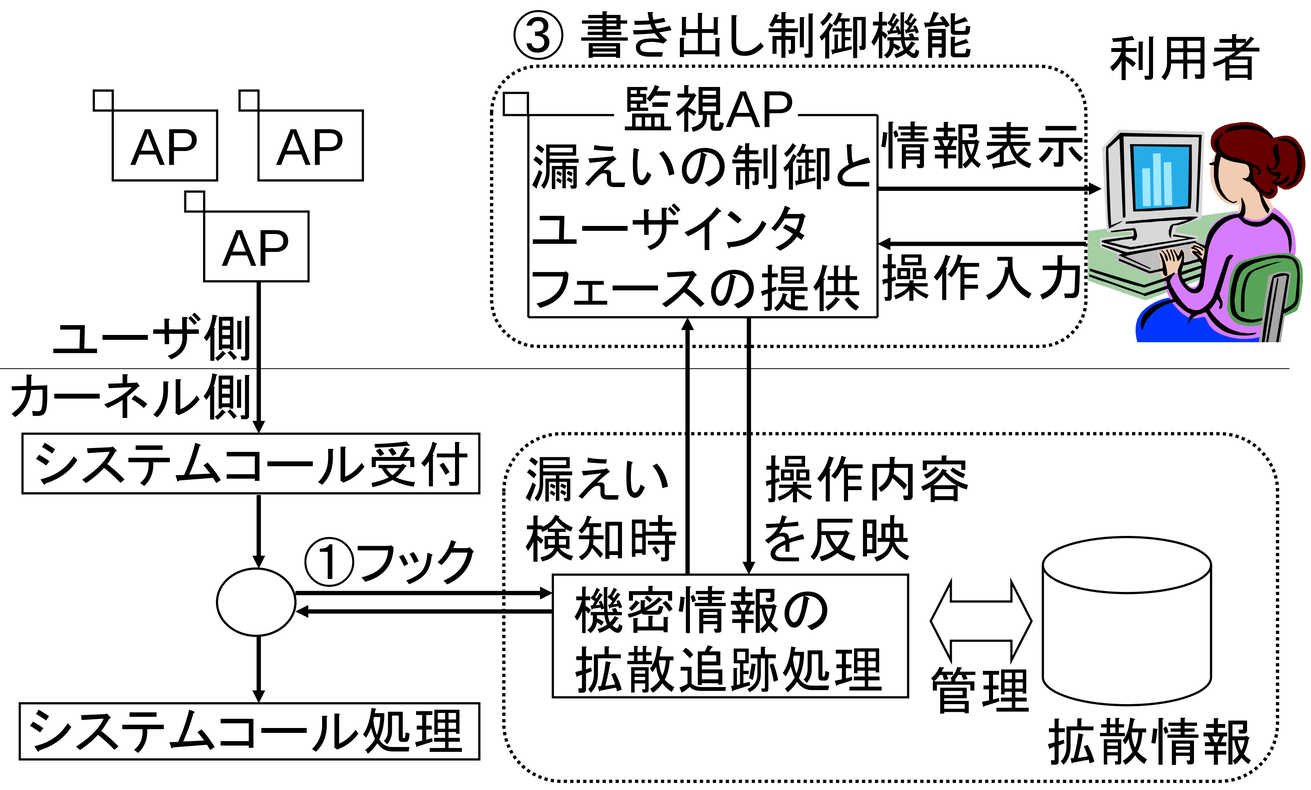
岡山大学大学院自然科学研究科　山内研究室

1.はじめに

近年，計算機で機密性の高い情報を扱う機会の増加
➡ 機密情報漏えい事例の増加
情報漏えいの主な原因は計算機の誤操作や管理ミス
情報漏えい防止のためには，機密情報がシステム上のどこにあるかを把握することが重要

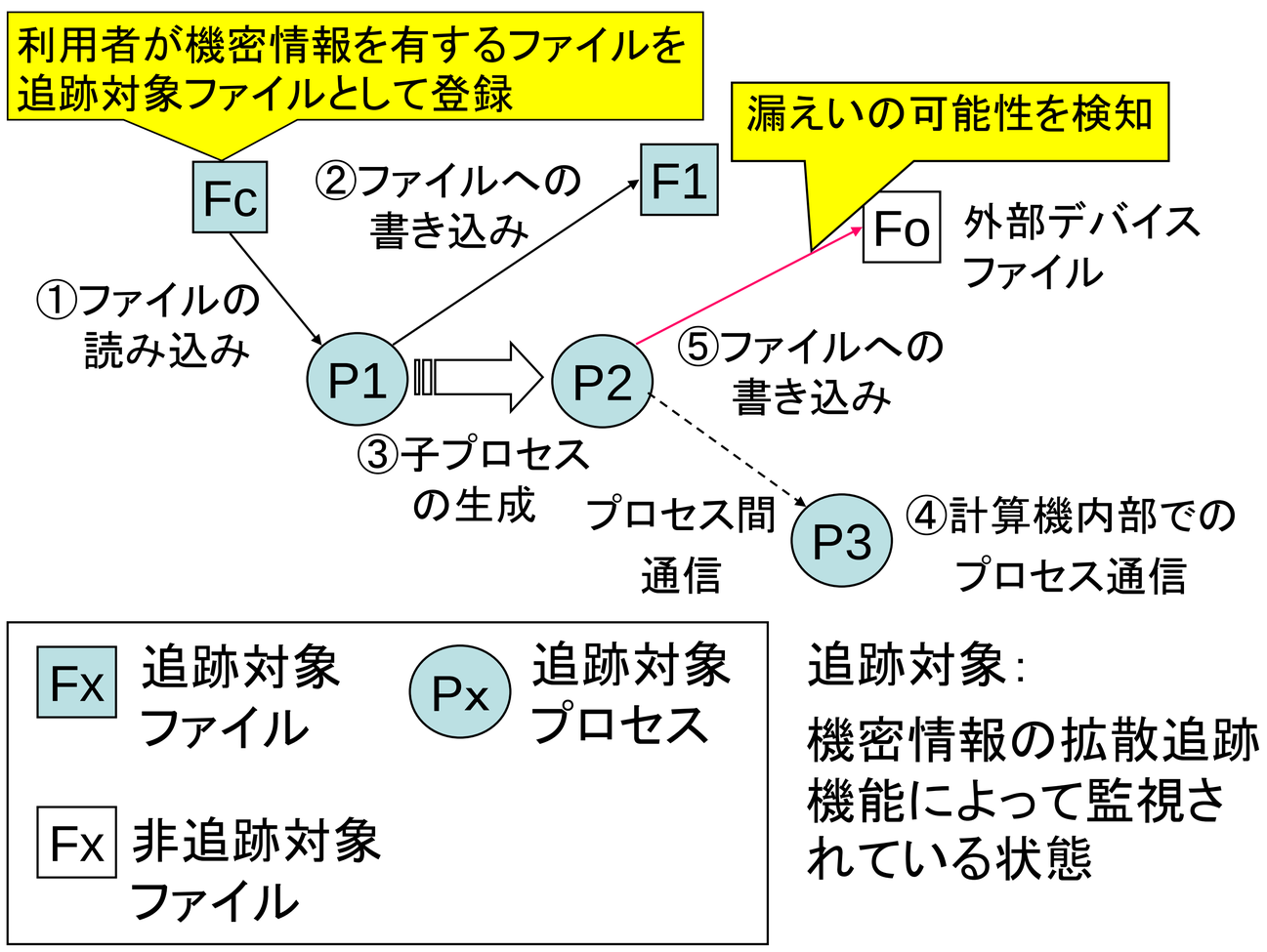
計算機内部における機密情報の拡散追跡機能を提案
(1) オペレーティングシステム（OS）レベルで機密情報の拡散を追跡し，機密情報を有するファイルやプロセスを管理
(2) 情報漏えいの可能性を検知し，書き出しを制御

2.機密情報の拡散追跡機能



3.機密情報の拡散追跡機能の動作

機密情報が伝搬するシステムコールをフックし，追跡と漏えい可能性検知を行う



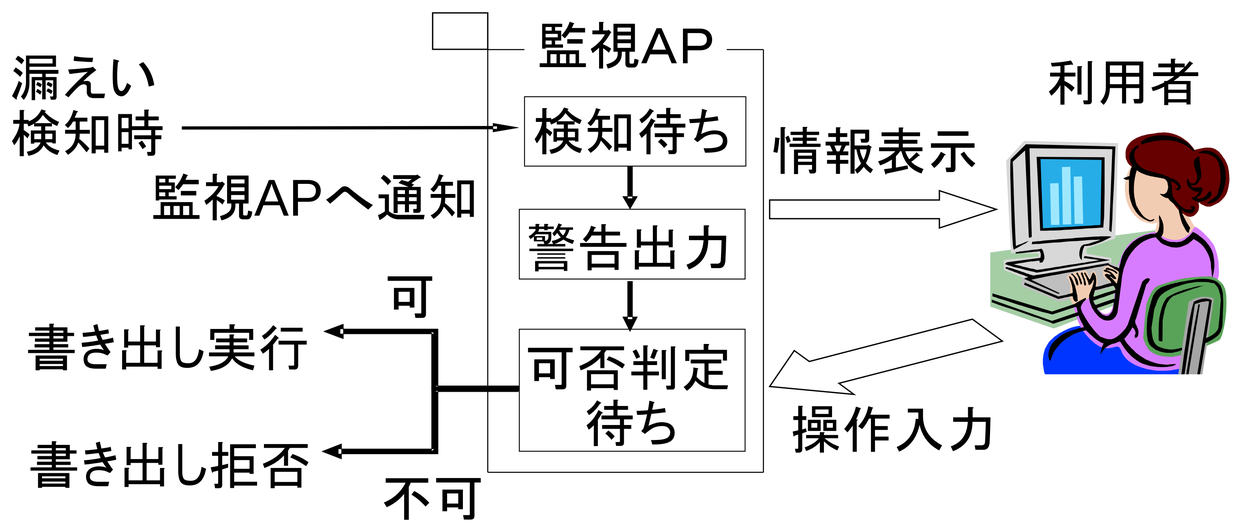
追跡対象：
機密情報の拡散追跡機能によって監視されている状態

4.書き出し制御機能

ユーザの誤操作により，機密情報を有するファイルが漏えいする可能性がある
➡ 漏えい防止の手段として，書き出し制御機能を実現

(1) カーネル上の動作
　(A) 漏えいの可能性を検知後，書き出しプロセスを休止状態とし，書き出し処理を一時停止
　(B) 利用者からの入力を契機に休止プロセスを再開させ，可否に基づき，書き出しを制御
(2) 監視APの動作
　(A) 警告の出力，利用者の書き出し可否判定待ち
　(B) GUIによる警告ダイアログを表示

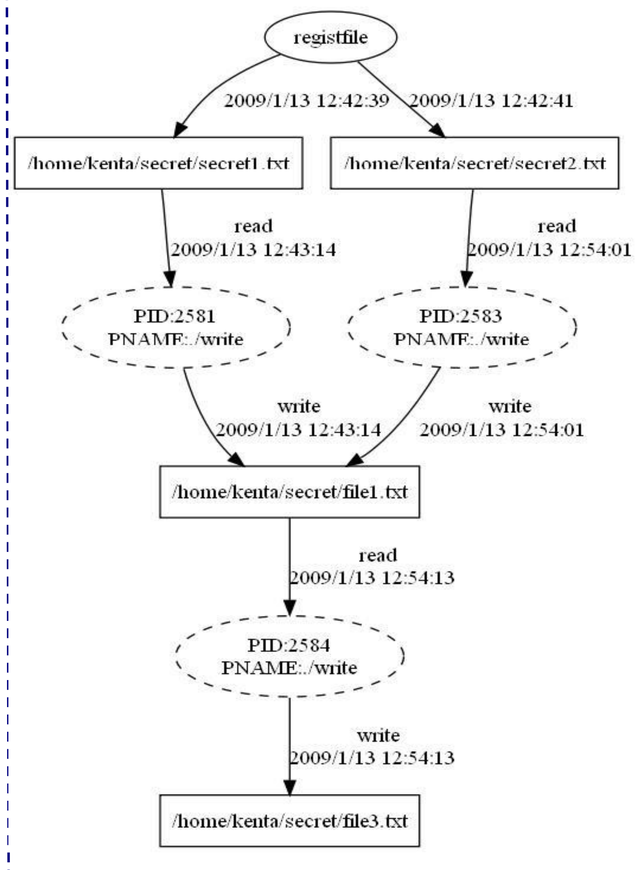
5.書き出し制御機能の処理の流れ



漏えい検知時の動作として，
利用者の判断でその書き出しを制御

利用者の不注意，もしくは不正なプログラムにより知らない間に起こる機密情報の漏えいを防止

6.可視化機能



(1) 可視化機能
　(A) 機密情報の拡散経路図を表示
　(B) 利用者が指定したファイルに関連する情報のみ表示可能

(2) 可視化機能のメリット
　(A) 表示する情報が簡潔
　(B) 拡散経路図から追跡対象のプロセスとファイル間の機密情報の拡散関係を容易に把握可能