2ZA-06

KVMにおける機密情報の拡散追跡機能を支援する可視化機構の検討

本田 匠† 森山 英明† 山内 利宏‡

†有明工業高等専門学校 電子情報工学科 ‡岡山大学大学院自然科学研究科

1. はじめに

近年，計算機上で会社や個人の機密情報を扱う機会が増加しており，これに伴い，外部からの不正アクセスや利用者の誤操作による機密情報の漏えいが増加している．この問題に対処するために，KVM(Kernel-based Virtual Machine)によって仮想化された計算機を用いた，拡散追跡機能を実現している[1]．この機能では，仮想計算機の VMM(Virtual Machine Monitor)上から機密情報を操作するシステムコールをフックし，機密情報のファイルを操作したプロセスの情報や，機密情報のデータを書き込んだファイルの情報を取得することで，機密情報の拡散経路を追跡する．この機能の問題点として，拡散経路を表すログをテキスト形式で出力しているため，利用者が機密情報の拡散経路を確認する際に把握が難しいことがある．

本稿では，機密情報の拡散経路を表すログを可視化する機構について，検討した結果を報告する．

2. KVMにおける機密情報の拡散追跡機能

2.1 機能の概要

計算機内の機密情報の利用状況を把握するために，仮想計算機モニタにおける機密情報の拡散追跡機能(以降，拡散追跡機能と略す)を提案し，KVM 上に実現している[1]．機密情報の拡散追跡機能は，機密情報を有する可能性のあるファイル(以降，管理対象ファイルと略す)とプロセス(以降，管理対象プロセスと略す)を拡散情報として記録し，追跡する．この機能を，VMM 上に実装することにより，オペレーティングシステムよりも攻撃が困難である VMM で機密情報を管理できる．VMM における機密情報の拡散追跡機能の処理の流れを，以下に示す．

(1) ゲスト OS 上でユーザープロセスがシステムコールを発行
(2) VMM でシステムコールの発行を検知し，発行されたシステムコールを判定後，以下の処理を実行
  (A) 機密情報の拡散に関係しないシステムコールの場合，制御をゲスト OS へ戻し，システムコール処理を続行
  (B) 機密情報の拡散に関係するシステムコール処理の場合，機密情報の拡散追跡に必要な情報を取得
(3) (2-B)で取得した情報をもとに機密情報の拡散を追跡し，拡散情報を更新
(4) 制御をゲスト OS へ戻し，システムコール処理を続行

これにより，ゲスト OS を改変することなく，拡散追跡機能を提供できる．

2.2 機密情報の拡散経路ログ

機密情報の拡散追跡機能では，管理対象プロセスと管理対象ファイルから，機密情報の拡散追跡に関わるシステムコールが発行される際に，/var/log/messages のシステムログへ，機密情報の拡散経路を表すログ(以降，拡散経路ログと略す)を出力する．機密情報の拡散追跡機能により出力されるログの例を，図 1 に示す．拡散経路ログは，テキスト形式で 1 行ごとに記録される．ここで，利用者が機密情報の拡散経路を把握するには，var/log/messages 上の拡散経路ログを検索し，管理対象プロセスと管理対象ファイルの依存関係を確認する必要がある．このため，拡散経路ログから機密情報の拡散する流れを即座に把握することは困難であり，特に拡散経路ログが増加した際は，管理対象プロセスと管理対象ファイルの依存関係の把握が困難となる．この結果，機密情報の漏えいが起こった際に，拡散経路の把握に時間を要してしまう．

この問題を解決するために，拡散経路ログから機密情報の拡散する様子を，視覚的に把握可能とする可視化機構(以降，可視化機構と略す)が必要となる．以降では，可視化機構について説明する．

3. 機密情報の拡散経路の可視化機構

3.1 可視化に必要な情報

2.2 節で述べたように，利用者が機密情報の拡散経路を迅速に把握可能な形で提供する必要がある．そこで，機密情報の拡散経路の可視化機構では，拡散追跡情報を有向グラフ形式の図(以降，拡散経路図と略す)として表示する．有

Consideration of Visualization Mechanism to Support Diffusion Tracing Function of Classified Information on KVM
† National Institute of Technology, Ariake College
‡ Graduate School of Natural Science and Technology, Okayama University

```
[463961.356076] read_ino:915716
[463961.356077] --------trace process list--------
[463961.356079]   782
[463961.356102] ----------------------------------
[463961.356142] sensitive data is diffused to "secret/copy-secret.txt"(inode number: 915715) by "cp" (pid: 782)
[463961.356143] --------------------trace file list--------------------
[463961.356144]  no.: inode number, file path
[463961.356145]    0:       915716, /secret/secretfile.txt
[463961.356146]    1:       915715, secret/copy-secret.txt
[463961.356147] ---------------------------------------------------
```

図 1 拡散経路ログの出力例

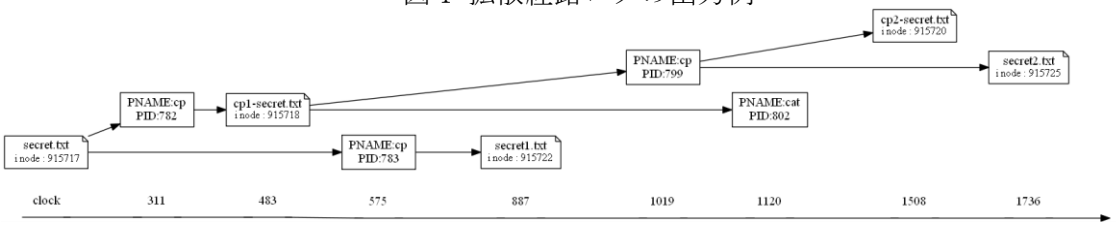

図 2 拡散経路図の出力例

効グラフを用いた拡散経路図の例を図 2 に示す．拡散経路図では，操作が行われた管理対象ファイル，操作を行った管理対象プロセスをノードとし，管理対象プロセスが管理対象ファイルに対してシステムコールによるアクセスを行った際に，管理対象ファイルノードから管理対象プロセスノードに向かってエッジを結ぶ．また，拡散経路を時系列順に表現するために，横軸としてクロック軸を表示する．クロック軸は各管理対象ファイルと管理対象プロセスのクロック数を表示したノードをクロック数をもとに整列させて表示する．管理対象ファイルノード，管理対象プロセスノードをクロック数に応じたクロック軸上に配置することにより，機密情報の利用状況を時系列順に表示する．以下に，拡散経路図に表示する情報について述べる．

(1) 管理対象ファイルノードに表示する情報:
ノード内には，ファイルを識別する情報として，ファイル名とファイルの inode 番号を表示する．ノードの形はノート形で表示する．

(2) エッジに表示する情報:
エッジに，管理対象ファイルの操作を行ったプロセスを識別する情報として，プロセス名とプロセス ID を表示する．

(3) クロック軸に表示する情報:
クロック軸には，下線ノード内に，単位を示す clock と，各管理対象ファイル，管理対象プロセスが管理対象と登録されたクロック数を表示する．

3.2 基本機構

表示する管理対象ファイルノードの数や図の大きさ，関係性によって各ノードの配置を変える必要がある可視化機構では，表示する管理対象ファイルノードの関係性を細かく指定できる Graphviz を使用する．Graphviz は，AT&T が開発したオープンソースのツールパッケージである．DOT 言語と呼ばれる言語を用い，テキスト形式で記述されたソースコードを読み込んでグラフを作成できる．これにより，図 2 に示すようなグラフを出力する．

可視化機構による拡散経路図出力までの流れを以下で説明する．

(1) 可視化機構を起動する．

(2) /var/log/messages 上にある拡散経路ログを集約し，管理対象ファイル，管理対象プロセス，およびこれらの依存関係を抽出する．

(3) 機密情報の拡散経路情報から，DOT 言語形式のソースコードを作成する．

(4) DOT 言語形式のソースコードを入力とし，Graphviz により拡散経路図を出力する．

4. おわりに

本稿では，拡散追跡機能を支援する可視化機構の実現方式を検討した．今後は，可視化機構の実装について検討する．

謝辞 本研究の一部は JSPS 科研費 16H02829（基盤研究(B)）の助成を受けたものです．

参考文献

[1] Fujii, S., Sato, M., Yamauchi, T., and Taniguchi, H.: Evaluation and Design of Function for Tracing Diffusion of Classified Information for File Operations with KVM, The Journal of Supercomputing, Vol.72, Issue 5, pp.1841-1861, (2016).