仮想計算機技術のセキュリティ技術への応用

佐藤 将也　　山内 利宏

岡山大学大学院自然科学研究科

〔受賞論文〕
ログの改ざんと喪失を防止するシステムの仮想計算機モニタによる実現
佐藤将也，山内利宏（岡山大学大学院自然科学研究科）
情報処理学会論文誌，Vol.53, No.2, pp.847-856（2012）

このたび，標記の論文で本会論文賞という名誉ある賞をいただくことになり，大変光栄です．今後も，この受賞を励みに，精進していきたいと思います．

受賞論文は，仮想計算機技術の基盤ソフトウェアである仮想計算機モニタを用い，仮想計算機上におけるログの改ざんと喪失を防止するシステムを提案しています．計算機の動作を把握するためには，計算機上のログが重要になります．しかし，攻撃や問題の発生によりログの改ざんや喪失が起こる可能性があります．このため，ログの保護に関する研究が数多く提案されています．しかし，既存研究は，主に外部記憶装置に書き出された後のログファイルの保護を目的としており，ログの書き出しプログラムが攻撃されるなど，ファイルへログが書き出される前に攻撃を受けた場合には対処できないものが多いです．

そこで，受賞論文では，ファイルへ書き出される前のログに着目し，仮想計算機モニタにより，ログの改ざんと喪失を防止するシステムを提案しています．提案システムでは，仮想計算機上において，ユーザプロセスとOSが出力するログを，OSのソースコードの修正なしに仮想計算機モニタにより取得し，ログの取得元の仮想計算機から隔離された仮想計算機に保存します．提案システムは，仮想計算機上のログ出力を検知することで，ログの生成直後にログを取得するため，ファイルの編集やログの書き出しプログラムへの攻撃によるログの改ざんの影響を一切受けません．

受賞論文における研究内容は，仮想計算機技術のセキュリティ技術への応用です．仮想計算機技術は，計算機をより効率的に利用するための技術として広く利用されています．仮想計算機モニタは，仮想的な計算機資源をそれぞれの仮想計算機へ提供するため，それぞれの仮想計算機の状態を容易に把握できます．このため，状態監視などへ容易に応用できます．また，仮想計算機モニタは，仮想計算機から独立しているため，セキュリティ機構を仮想計算機モニタへ導入することにより，より堅牢な機構を実現できます．受賞論文における研究内容は，これらの利点をログの保護へ応用したものです．仮想計算機技術を応用したセキュリティ機構はこれまでにも提案されています．しかし，ログの安全性に着目した研究は少なく，ファイルに書き出される前のログに着目した研究にいち早く着手し，仮想計算機技術を応用できたことは，幸いです．ログに関する研究は，そのセキュリティ面での重要性にもかかわらず，運用管理に重点を置いた研究が多く，安全性への考慮が十分とは言えず，今後のさらなる発展が期待されます．

最後に，受賞論文に関して助言をくださった多くの皆様に感謝いたします．特に，査読者の皆様に，心より感謝を申し上げます．

（2013年5月13日受付）

佐藤 将也（学生会員）　m-sato@swlab.cs.okayama-u.ac.jp
2010年岡山大学工学部情報工学科卒業．2012年同大大学院自然科学研究科博士前期課程修了．同年同大学院博士後期課程入学．現在，在学中．日本学術振興会特別研究員（DC2）．コンピュータセキュリティ，仮想化技術に興味を持つ．

山内 利宏（正会員）　yamauchi@cs.okayama-u.ac.jp
1998年九州大学工学部情報工学科卒業．2002年同大大学院システム情報科学府博士後期課程修了．九州大学大学院システム情報科学研究院助手を経て，現在，岡山大学大学院自然科学研究科，准教授．博士（工学）．OS，コンピュータセキュリティに興味を持つ．