氏　　名	佐藤　将也
授与した学位	博　士
専攻分野の名称	工　学
学位授与番号	博甲第５０４４号
学位授与の日付	平成２６年　９月３０日
学位授与の要件	自然科学研究科　産業創成工学専攻 （学位規則第５条第１項該当）
学位論文の題目	ログ保全と攻撃難化によるセキュリティ向上技術に関する研究
論文審査委員	准教授　山内　利宏　　教授　谷口　秀夫　　教授　名古屋　彰

学位論文内容の要旨

サイバー攻撃による被害の抑制において，計算機利用者の不注意や脆弱性を利用した攻撃を防止するためにどれだけ対策をしても十分なことはなく，侵入や情報の取得などが行われることを前提とした対策が必要不可欠になっている．このため，攻撃者の活動の痕跡であるログの保全を確実にすることが重要である．また，攻撃による被害を抑制するために，攻撃の検知や防止を行うソフトウェア（以降，セキュリティソフトウェア）を攻撃から保護することが重要である．また，仮想化技術は，より多くの環境で利用され，仮想計算機（Virtual Machine，以降，VM）の利用を前提としたソフトウェア構成が一般的になることが予想される．このような環境において，利用者が計算機を安全に利用するためのソフトウェア実行基盤の構築が重要となる．

そこで，ログの改ざんや消失を仮想計算機モニタにより防止するシステムは，ログを生成されてできるだけ早い段階で取得し，VM 外部へ転送することで，攻撃者によるログ改ざんやプログラムの問題によるログの消失の可能性を低減できる．評価結果より，本システムにより，ログファイルの改ざん検出やログの消失防止が可能であることを示した．

また，ログ保全の信頼性を向上しつつ，ログ保全の処理性能を向上する手法として，ライブラリの置き換えによる VM 外部への低オーバヘッドなログ転送手法を提案した．本手法について，評価結果より，本手法の適用による性能低下は非常に小さいことを示した．また，複数 VM が走行する環境における性能評価の結果より，VM 数の増加による性能低下への本手法の影響は小さいことを示した．

さらに，セキュリティソフトウェアの改変なしの保護を実現するために，プロセス情報の不可視化によりプロセスの特定を困難にする攻撃回避手法を提案した．本手法は，不可視化対象プロセスのプロセス情報を偽の情報に置換することで攻撃を回避する．これにより，OS レベルで動作するマルウェアからの攻撃にも耐性のある実行環境の提供を目指す．評価結果より，不可視化対象のプロセスの走行中は，そのプロセスのプロセス情報は偽の情報に置換できていることを確認した．

以上より，将来的に更なる普及が予想される仮想化技術の利用により，攻撃の痕跡の削除を困難にし，かつセキュリティソフトウェアへの攻撃を回避することで，計算機利用環境の安全性を向上できることを示した．

論文審査結果の要旨

計算機は様々な場面で利用され，計算機が重要な情報を扱う機会が増えていることから，ネットワークに接続された計算機が悪意のあるソフトウェアを用いた攻撃や大量のデータを送りつけるサービス不能攻撃に代表されるサイバー攻撃にさらされている．このため，サイバー攻撃による被害を抑制することは重要な課題となっている．

論文提出者は，サイバー攻撃による被害の抑制において，サイバー攻撃による被害が出ることを前提とした証拠保全が必要不可欠であること，及び攻撃者による攻撃対象ソフトウェアの識別を困難にできれば，被害を抑制できる可能性が高いことに着目し，今後ますます普及が見込まれる仮想化技術を用いたログ保全手法と攻撃難化手法を提案した．特に，仮想化技術を用いて保護対象のゲストオペレーティングシステムのログを保護する研究は行われておらず，いち早くこの手法に着目し，ログ保全手法を確立した点が高く評価できる．

まず，ログ保全の信頼性を向上するために，ログの改ざんや消失を仮想計算機モニタにより防止するシステムの構成法を明らかにした．このシステムは，攻撃者に機構自体を攻撃される可能性を低減し，かつ多種のオペレーティングシステムが動作する仮想計算機環境へも適用できることを明らかにした．次に，ログ保全の適用環境によっては，ログ保全の処理オーバヘッドを低減する必要があることに着目し，ログ保全の信頼性を向上しつつ，ログ保全の処理オーバヘッドを抑制する手法を提案した．さらに，プロセス情報の不可視化によりプロセスの特定を困難にする攻撃回避手法を提案した．

以上のように本論文は，サイバー攻撃による被害を抑制できる手法として，仮想化技術を用いてログ保全と攻撃難化を実現する手法を確立しており，情報工学に寄与するところが大きい．よって，本論文は博士（工学）の学位論文に値すると認める．

なお，論文発表会では，適切な説明が行われ，質疑に対する応答も適切であった．これにより，十分な学力を有することが確認でき，自立した研究者として活動を行う能力を有することも認められた．