修 士 論 文 の 和 文 要 旨

大学院情報システム学研究科	博士前期課程	情報システム設計学 専 攻
氏 名	崔 哲浩	学籍番号 0350022
論 文 題 目	仮想マシン技術を用いて隔離された プロセス監視制御システム	

要 旨

近年、コンピュータ産業は急速に発展し、社会の様々の分野にコンピュータが普及している。それに伴い、コンピュータシステムに対する不正侵入が増加し、被害も拡大している。

本研究では、仮想マシン技術を利用した侵入検知システムの提案を行う。この侵入検知システムはホストOS上で動作し、ゲストOS上で提供される計算機サービスを監視する。ゲストOSからはホストOSの資源の参照、操作が不可能であり、侵入者がゲストOSに攻撃を加えたとしてもその影響は侵入検知システムに及ばない。そのため、侵入者からの発見と破壊に対し堅牢な侵入検知システムになる。

今現在、侵入検知システムには、おもにネットワークベースとホストベースの2種類がある。ネットワークベースの侵入検知システムはネットワーク上のパケットを調査することで、ネットワークレベルでの侵入検知を行う。つまり侵入者がネットワーク上から侵入を試みた時点での検知が可能という利点がある。しかし、パケットの内容や送受信元、流量、頻度などの限られた情報をもとにしか分析できず、侵入を許した後の検知が困難であるという欠点がある。

一方、ホストベースの侵入検知システムは侵入対象の計算機上で動作するため、その内部を全面的に監視制御でき、侵入の発見精度を高めることができる利点がある。しかし、侵入者にシステムの管理者権限を奪われてしまうと、侵入検知システム自体の改ざんや破壊をされてしまうという脆弱性を欠点に持つ。

本研究では、ホストベース侵入検知システムの利点を生かしたまま、上述の欠点を克服する方法としてHostedアーキテクチャ仮想マシンに着目した。Hostedアーキテクチャ仮想マシンとは、実計算機上で動作するOS(ホストOS)上に仮想的に構築された計算機である。この仮想的な計算機の上で動作するOS(ゲストOS)は完全にホストOSの支配下にあり、ゲストOSからはホストOSの資源の参照や操作を自由にはできないという特徴がある。この特徴を利用し、侵入検知システムをホストOSで、計算機サービスをゲストOSで動作させる手法を提案する。この手法を使えば、ホストOS上の侵入検知システムはゲストOSの全体を監視できる一方で、ゲストOSからは侵入検知システムの改ざんや破壊が不可能になる。

本論文では、ホストOS側からゲストOSのプロセスを監視制御する隔離されたプロセス監視制御システムを実装し、評価を行った。評価の結果、ゲストOSの動作に10%-15%のオーバヘッドを与えることで、ゲストOSのユーザ操作から影響を受けないまま、ゲストOSのプロセス操作が可能であると確認された。