論　文　概　要

九州工業大学大学院情報工学府　情報創成工学専攻

学生番号	10675026	氏　名	永田　卓也
論文題目	Cell/B.E. の SPE を利用した安全な OS 監視システム		

1　はじめに

近年は計算機への様々な攻撃に備えて、AntiVirus 等のセキュリティソフトウェアを利用するのが一般的になっている。しかし、セキュリティソフトウェアは OS の機能を利用して監視を行っており、カーネルルートキットを用いた攻撃によって OS が改ざんされてしまった場合、セキュリティソフトウェアの実行結果を信頼することはできなくなる。セキュリティソフトウェアの信頼性を向上させるには、OS が正しく動作していることを保証する必要がある。

本研究では、ヘテロジニアス・マルチコアプロセッサの Cell/B.E. を対象として、SPE と呼ばれるコアを物理的に隔離して OS 監視システムを動作させる SPE Observer を提案する。

2　SPE Observer

SPE Observer は図 1 のように Cell/B.E. の SPE と呼ばれるコアの上で OS 監視システムを安全に動作させるシステムである。Cell/B.E. を用いたシステムでは、OS は PPE と呼ばれるコアで動作している。SPE 上で動く OS 監視システムは、DMA 転送を行う事でカーネルメモリから情報を読み取り、カーネルが改ざんされていないかどうかのチェックを行う。

SPE を Isolation モードで動作させることにより、OS 監視システムの完全性と機密性を保証することができる。OS が動作している PPE からは OS 監視システムを改ざんしたり、内部の情報を盗み見たりすることはできない。ただし、PPE から SPE 上で動く監視システムの実行を停止させることは防げないため、外部のセキュリティプロキシからハートビートを送ることで OS 監視システムの動作状況を監視する。

SPE Observer では監視内容に応じて、OS 監視システムのスケジューリングを行うことができる。SPE を占有して監視を行うとシステム性能に与える影響が大きいが、必要な時だけ監視を行うことで性能低下を抑えることができる。Secure Loader を用いることで、OS が改ざんされた後でも OS 監視システムを安全に起動することができる。OS 監視システムの起動を阻害した場合にはセキュリティプロキシに検出される。

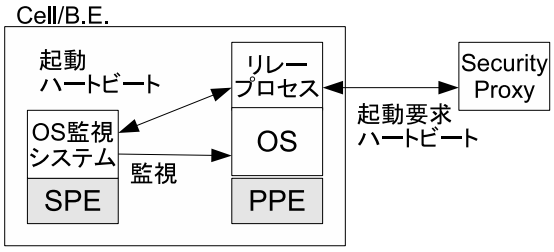

図 1: SPE Observer のシステム構成

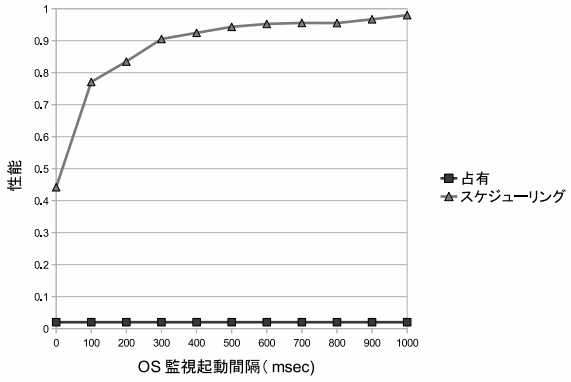

図 2: スケジューリングによる性能改善

3　実験

SPE Observer を PlayStation 3 に実装し、OS 監視システムの起動間隔を変えて、アプリケーションの性能に与える影響を調べた。実験には 6 並列で行列の乗算を行うアプリケーションを用いた。図 2 に OS 監視システムを動作させた時のアプリケーションの性能低下を示す。実験の結果より、OS 監視システムの起動間隔がある程度以上長ければ、性能低下を十分に抑えられることが分かった。

4　おわりに

Cell/B.E. の SPE 上で安全に OS 監視を行うことができる SPE Observer を提案した。SPE Observer は SPE Isolation モードを用いて OS 監視システムを物理的に隔離して動作させる。実験の結果、OS 監視システムをスケジューリングすればアプリケーションの性能低下が抑制できることが分かった。