# 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 | 16675036 | 氏　名 | 松井　尚督 |
|---|---|---|---|
| 論文題目 | GPU を用いた安全で高速な OS 監視システム | | |

## 1　はじめに

近年，ネットワークを経由した計算機への攻撃が増加している．従来，計算機内部にセキュリティソフトウェアをインストールして攻撃を検知するという対策がとられてきた．しかし，OS 自体を書き換えるカーネルルートキットを用いた攻撃が増えてきており，OS 上で動作する従来のセキュリティソフトウェアでは攻撃を検知できない．そこで，OS の状態を常に監視するシステムが必要となってくるが，OS 内部で監視システムを動作させると OS への攻撃時に無力化されてしまう可能性がある．

本研究では，多くの計算機に標準的に搭載されているデバイスである GPU に着目し，GPU 上で OS の監視を行う GPUsec を提案する．GPUsec では，OS が動作する CPU やメインメモリから物理的に隔離された GPU 上で OS 監視システムを実行させることにより，安全に OS の監視を行う．また，GPU は多数の演算コアを有しており，監視システムの並列化を行うことで高速に処理を行うことができる．

## 2　GPUsec

GPUsec のシステム構成は図 1 のようになる．GPU 上の OS 監視システムは監視対象ホストの起動時に実行を開始され，常に GPU を占有して動作し続ける．定期的に OS の監視を行うために，外部の監視ホストから監視対象ホストの GPU 上の OS 監視システムに監視コマンドを送信する．監視コマンドを受信した OS 監視システムはメインメモリからデータを取得して攻撃の検知を行う．その結果を監視ホストに送信し，監視ホストは必要に応じて管理者への通知を行う．

GPUsec は OS のコード領域とデータ領域の改ざんを検知することができる．コード領域の改ざんを検知するために，OS 監視システムはメインメモリ上の OS のコードを取得し，そのハッシュ値が変化していないかどうかを調べる．メインメモリのアクセスとハッシュ値計算を並列化するために，コード領域を分割してハッシュ値を計算する．一方，データ領域の改ざん検知のために，OS 監視システムは OS のシステムコールテーブルと割り込みテーブルのハッシュ値を調べる．

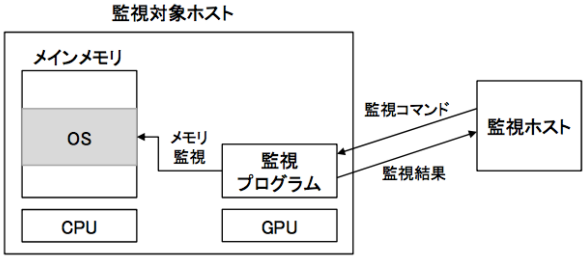


図 1. GPUsec のシステム構成

## 3　実験

GPUsec を用いた OS 監視システムの有効性を調べる実験を行った．実験には NVIDIA GeForce GTX 960 の GPU，GPUsec 用に修正した Linux 3.16.7 と GPU ドライバを使用した．

まず，コンフィグを変更してコンパイルした OS をインストールし，インストール前後の OS コード領域のハッシュ値を比較した．その結果，ハッシュ値が変化したため，GPUsec を用いて OS の整合性を検査できることが確認できた．

次に，この OS 監視システムの実行にかかる時間を測定した．図 2 に実験結果を示す．スレッド数が 1 の時，GPU からメインメモリへのアクセスに 98%の時間がかかっていることがわかった．スレッド数を増やしたところ，大幅な実行時間の改善がみられた．

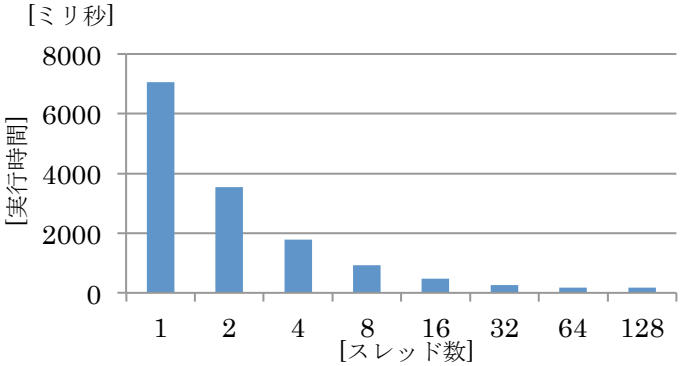


図 2. OS 監視システムの実行時間

## 4　まとめ

本研究では，GPU を用いて OS 監視システムを動作させることを可能にする GPUsec を提案した．今後の課題は OS の様々なデータを用いて改ざんを検知できるようにすることである．