# 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 | 18675026 | 氏　名 | 中野　智晴 |
|---|---|---|---|
| 論文題目 | Intel SGX を用いた安全な VM 監視手法 | | |

## 1　はじめに

近年，仮想マシン（VM）を提供する IaaS 型クラウドの普及が進んでいる．クラウド内の VM のセキュリティを向上させるには，侵入検知システム（IDS）を用いて監視を行う必要がある．VM を安全に監視するために，IDS を監視対象 VM の外側で実行する IDS オフロードと呼ばれる手法が提案されている．しかし，クラウドの管理者は必ずしも信頼できるとは限らず，管理者によってオフロードした IDS が攻撃される恐れがある．これまでに，IDS を保護するための様々なシステムが提案されてきたが，クラウド内で高度な IDS を安全に実行し，かつ，システム性能に対する影響を小さくするのは難しかった．

本研究では，Intel SGX を用いてクラウド内で IDS を安全かつ軽量に実行し，情報漏洩を防ぎつつ VM の監視を行うことができるシステム SGmonitor を提案する．

## 2　SGmonitor

SGmonitor は Intel SGX を用いてクラウド内の IDS を保護することにより，IDS の安全な実行を保証する．SGX はエンクレイヴと呼ばれる保護領域を提供する CPU 機構である．図 1 のようにエンクレイヴ内で IDS を実行することにより，IDS の改ざんや情報漏洩などの攻撃を防ぐことができる．ただし，IDS の実行を停止することは防げないため，SGmonitor では VM ユーザのホストから定期的に暗号化ハートビートを送ることで IDS が正常に動作していることを確認する．エンクレイヴはアプリケーションの一部として実行されるため，システム性能に大きな影響を与える恐れはなく，高度な IDS を比較的容易に開発することができる．

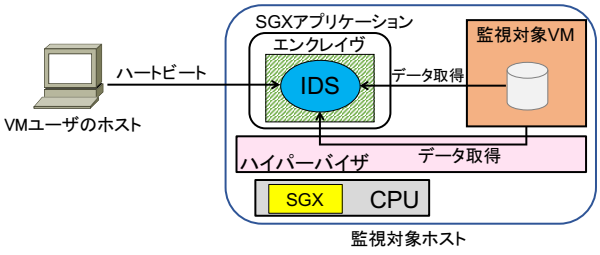
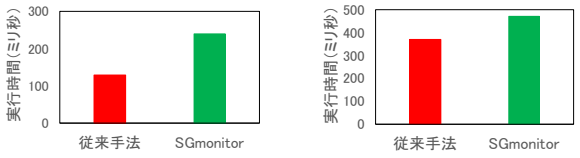



図 1: SGmonitor のシステム構成

エンクレイヴ内の IDS は VM のメモリデータやディスクデータを安全に取得して監視を行う．エンクレイヴは VM のメモリに直接アクセスできないため，メモリ上の OS データは信頼できるハイパーバイザを介して取得する．その際に，ハイパーバイザで OS データのハッシュ値を計算して暗号化し，エンクレイヴ内で復号およびハッシュ値の検証を行うことで情報漏洩や改ざんを防ぐ．また，エンクレイヴ内のファイルシステムを用いて，暗号化された VM の仮想ディスク上のファイルにアクセスする．情報漏洩を防ぐためにディスクデータはエンクレイヴ内で復号する．これらの機能を用いて，SGmonitor は IDS を OS の一部であるかのように記述することを可能にする．

## 3　実験

SGmonitor を用いて動作させた IDS の実行時間を測定した．実行時間は VM のメモリ上の OS データを監視する場合とディスクを監視する場合についてそれぞれ測定した．比較として，従来手法を用いてオフロードした IDS の実行時間も測定した．実験結果を図 2 に示す．メモリ監視の実行時間は，SGX や暗号化・整合性検査により従来手法と比較して 1.9 倍に増加した．ディスク監視の実行時間は，SGX や暗号化，ネットワーク共有のオーバヘッドのために 1.3 倍に増加した．




（a）メモリ監視　　（b）ディスク監視

図 2: IDS の実行時間

## 4　まとめ

本研究では，Intel SGX を用いてクラウド内の IDS を保護することにより，安全かつ軽量に VM を監視することができるシステム SGmonitor を提案した．今後の課題は，IDS が情報を取得できる VM を限定するための仕組みを実装することである．