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	21675017	氏　名	古賀　吉道
論文題目	Intel SGX と SMM を組み合わせた安全なホストベース IDS の実行		

1　はじめに

近年，インターネットに接続された情報システムへの攻撃が数多く報告されている．攻撃の糸口となるシステムの脆弱性を完全に取り除くことは困難であるため，侵入検知システム（IDS）を用いて対象システムを監視し，管理者に攻撃を通知する必要がある．しかし，システムの異常を検知するホストベース IDS は監視対象システム上で動作するため，安全に実行することが難しい．例えば，システムが改ざんされると IDS はシステムから正確な情報を取得することができなくなる．これまで，汎用 CPU の機能を用いて安全に IDS を実行する様々な手法が提案されてきたが，安全性や柔軟性の面で課題があった．

本研究では Intel 製 CPU の隔離実行環境である SGX とシステムマネジメントモード（SMM）を組み合わせることで，より安全かつ柔軟に IDS を実行することが可能な機構 SSdetector を提案する．

2　SSdetector

SSdetector は図 1 のように，IDS が SGX と SMM を用いてメモリ上の OS データを取得できるようにすることにより，システムの安全な監視を可能にする．IDS を保護するために，SSdetector は SGX が提供するエンクレイヴ内で IDS を実行する．エンクレイヴは通常のアプリケーション内に作成される保護領域であり，CPU によるメモリの暗号化および整合性検査により IDS の盗聴や改ざんを防ぐことができる．一方，エンクレイヴ内ではシステムのメモリデータを安全に取得することができないため，SMM で動作する BIOS 内のプログラムを用いてメモリデータを取得する．この SMM プログラムは独立した実行環境で安全に動作し，様々な IDS に共通で用いられる．

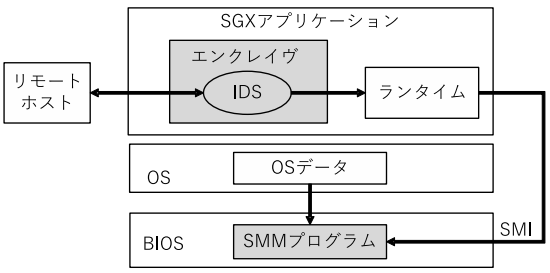

図 1: SSdetector のシステム構成

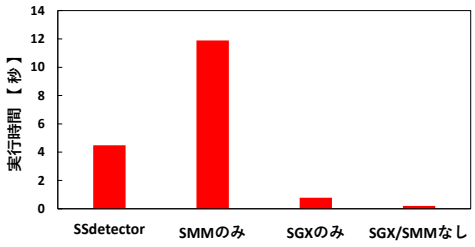

図 2: システム情報の取得時間

エンクレイヴ内の IDS が OS データを必要とした際には，SGX の機構を用いてエンクレイヴの外部で動作する SSdetector ランタイムを呼び出す．そして，SMI と呼ばれるソフトウェア割り込みを発生させて SMM で動作するプログラムを呼び出す．SMM プログラムは取得したデータを SSdetector ランタイム経由でエンクレイヴ内の IDS に返す．SSdetector ランタイムは攻撃を受ける可能性があるため，暗号化および整合性検査により転送中のメモリデータの盗聴および改ざんを防ぐ．暗号化に用いる鍵は公開鍵暗号を用いて IDS から SMM プログラムに安全に受け渡す．

3　実験

ホストベース IDS の多くが監視に用いる proc ファイルシステムに必要なシステム情報を取得するのにかかる時間を測定した．実機の BIOS を変更するのは難しいため，本実験は仮想マシン（VM）を用いて行った．図 2 に示すように，SGX と SMM を用いることにより，22 倍の実行時間がかかることが分かった．ただし，VM 内での SMM プログラムの呼び出しは実機よりも 0.5 ミリ秒遅いため，実機では高速化できる可能性がある．

4　まとめ

本研究では SGX と SMM を組み合わせることで，IDS をより安全に実行可能にするシステム SSdetector を提案した．今後の課題は，様々なホストベース IDS を実行できるようにすることである．