様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月　 ９ 日現在

機関番号：１７１０４
研究種目：基盤研究(C)（一般）
研究期間：2019～2021
課題番号：１９Ｋ１１９０２

研究課題名（和文）Intel SGXを用いた安全かつ容易な侵入検知システムの構築

研究課題名（英文）Secure and Easy Deployment of Intrusion Detection Systems with Intel SGX

研究代表者
光来　健一（Kourai, Kenichi）

九州工業大学・大学院情報工学研究院・教授

研究者番号：６０３７２４６３

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：本研究では、Intel SGXと呼ばれるCPUの新しいセキュリティ機構を用いて、仮想マシン（VM）の外側に侵入検知システム（IDS）をオフロードして安全に動作させられるようにした。そのために、SGX保護領域からVMのメモリやストレージ、ネットワークの情報を取得することを可能にする機構を開発した。また、SGX保護領域内で軽量OSであるライブラリOSを用いることにより、高度なIDSも実行できるようにした。

研究成果の学術的意義や社会的意義
本研究の学術的意義は、Intel SGXを用いてVMを監視する様々な種類のIDSが安全に実行できるようになったことである。これにより、SGXの新たな活用方法が確立され、IDSだけでなく他の処理を安全にVMの外側にオフロードするという応用にも道が開けた。
本研究の社会的意義は、実際のクラウドに対してIDSオフロードが導入しやすくなったことにより、ユーザがより安全にクラウドを利用できるようになることである。

研究成果の概要（英文）：This project enabled securely offloading intrusion detection systems (IDS) to the outside of virtual machines (VMs) with a new CPU security feature called Intel SGX. We have developed various mechanisms to obtain information on the memory, storage, and networks of VMs from an SGX protection domain. In addition, we supported advanced IDS by using lightweight operating systems (OSes) called library OSes in an SGX protection domain.

研究分野：ソフトウェア

キーワード：仮想マシン　保護領域　侵入検知　監視　クラウド

１．研究開始当初の背景

侵入検知システム（IDS）はホストへの侵入を早期に検知し、被害を最小限に抑えるために必要不可欠である。IDS を監視対象ホスト上で動作させると侵入者によってすぐに無力化されてしまうため、クラウドにおいては仮想マシン（VM）を用いた安全な監視手法が提案されている。この手法は、VM の外側に IDS をオフロードし、VM のメモリ、ストレージ、ネットワークを解析・監視することにより、侵入者による IDS への攻撃を防ぐ（図 1）。我々はこのような IDS オフロードの研究を長年にわたって行っており、多数の顕著な成果が出ている。

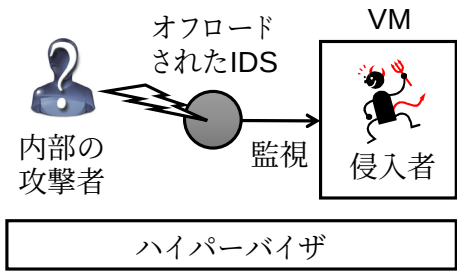

図 1　従来の IDS オフロード

しかし、VM の外側に IDS をオフロードしたとしてもまだ攻撃を受ける危険性がある。クラウドのセキュリティ対策は万全であるが、それでも攻撃者の侵入を完全に防ぐのは難しい。また、クラウドには信頼できない管理者が存在する可能性もある。実際に、2010 年には Google の管理者がユーザのプライバシ侵害を起こしている。サイバー犯罪の 28%は内部犯行であり、IT 管理者の 35%は社内の機密情報に無断でアクセスしたことがあるという報告もある。

そこで、クラウド内部の攻撃者に対して安全な IDS オフロードを行えるようにするために様々な手法が提案されてきた。例えば、仮想化システムの基盤となるハイパーバイザ内で IDS を動作させる手法や、システム管理用の特殊な CPU 実行モードを用いて IDS を実行する手法などがある。我々も IDS をクラウド外部のリモートホストにオフロードして VM を安全に監視する手法や、監視対象 VM が動作している仮想化システム全体をさらに仮想化し、その外側で IDS を安全に動作させる手法などを開発してきた。

これまでの研究では、IDS オフロードのセキュリティを向上させることに主眼が置かれていた。しかし、IDS を保護するためにシステムが大幅に複雑になったり、IDS の追加・更新を行うのが難しかったりすると、実際のクラウドに導入する際には大きな障害となる。また、クラウド外部に IDS を動かすためのホストを用意する必要があると、ユーザの負担が大きくなる。当初の IDS オフロード手法と同程度の労力でクラウドに適用できなければ、安全な IDS オフロードを実用的に利用できるようにはならない。

２．研究の目的

本研究の目的は、Intel SGX と呼ばれる CPU の新しいセキュリティ機構に着目して、安全な IDS オフロードをクラウドに容易に適用できるシステムを開発することである。SGX はアプリケーション内部に保護領域を作成し、その中でプログラムを安全に実行するための仕組みである。この SGX 保護領域が通常のアプリケーションの一部として動作するという特徴を活かして、複雑な仕組みを導入することなく、IDS を安全にオフロードできるようにする（図 2）。その際に、IDS の従来のオフロード先と異なり、SGX 保護領域は高い権限を持っているわけではないため、安全に VM の監視を行える仕組みを考案する。

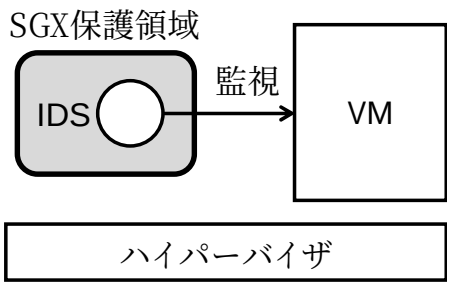

図 2　SGX を用いた安全な IDS オフロード

SGX を用いて IDS オフロードを容易に行えるようにするために、本研究では以下の 3 つの課題に取り組む。

(1) SGX 保護領域からの VM 監視

オフロードした IDS を SGX 保護領域で動作させられるようにする。そのために、VM のメモリやストレージ、ネットワークから安全に情報を取得できるようにする。

(2) SGX 保護領域での高度な IDS 実行

SGX 保護領域で既存の高機能な IDS を実行できるようにする。そのために、ライブラリ OS と呼ばれる小さな OS を用いて、IDS に対して透過的に VM 内の OS の情報を提供できるよう

にする。通常の OS と比べて複数プロセスの協調動作などの機能が不十分であるため、既存の様々な IDS の実行形態に対応できるようにする。

(3) 複数の SGX 保護領域を用いた監視機能の分割

IDS オフロードをさらに一歩進め、ユーザが自身の VM 内で SGX 保護領域を用いて IDS を安全に動作させられるようにする。ただし、VM 内で取得した情報は改ざんされている恐れがあるため、情報取得だけは VM の外部で安全に行う。さらには、より柔軟な運用を可能にするために、IDS をクラウド内の別のホストにもオフロード可能にする。

３．研究の方法

本研究では以下の手順で研究を進めた。

(1) SGX 保護領域からの VM 監視

SGX 保護領域から VM のメモリを監視できるようにする（図 3）。安全にメモリ監視を行えるようにするために、IDS が要求した VM のメモリ上のデータをハイパーバイザが取得・暗号化し、SGX 保護領域で復号を行う。この機構を既存のハイパーバイザの自然な拡張として追加することにより、システムが複雑にならないように留意する。

次に、SGX 保護領域で動作する IDS の開発を支援するツールを開発する。このツールを用いて、オフロードした IDS を OS のカーネルモジュールのように記述できるようにする。その上で、既存のいくつかの IDS を調査し、VM 内の OS 情報を用いた監視を SGX 保護領域において実現する。そのために、我々が GPU 用に開発している OS 監視基盤を SGX 向けに移植する。

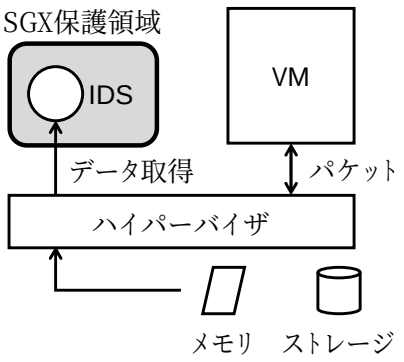

図 3　VM のリソース監視

また、SGX 保護領域から VM のストレージを監視できるようにする。安全にストレージ監視を行えるようにするために、ストレージ全体を暗号化しておき、SGX 保護領域で復号する。SGX 保護領域では、監視対象 VM と同じファイルシステムを動作させられるようにすることで、ファイル単位でのアクセスを実現する。また、通常通りに VM によるストレージアクセスを可能にするために、ハイパーバイザにおいて透過的に暗号化・復号化を行う機構を開発する。この機構もシステムの複雑さを増大させないように実装する。

さらに、SGX 保護領域から VM のネットワークの監視を行えるようにする。VM が送受信するパケットは必ずハイパーバイザを経由するため、ハイパーバイザにおいてパケットを取得し、SGX 保護領域に転送する機構を開発する。

(2) SGX 保護領域での高度な IDS 実行

SGX 保護領域で動作するライブラリ OS の調査を行う。Linux 互換の Graphene-SGX を用いることを考えているが、他のライブラリ OS や独自実装も検討する。既存の IDS を動作させるために必要な機能が提供されているかを調査し、不足している機能についての設計を行う。また、既存のライブラリ OS は実行されている環境の情報を返すため、VM 内の OS 情報を返すべき箇所を特定する。

次に、VM 内の OS 情報を返すライブラリ OS を開発する（図 4）。調査結果に基づいて、ライブラリ OS の必要な箇所で VM 内の OS 情報を取得できるようにする。その際に、課題(1)で開発したメモリ監視機構を用いて VM 内の情報を取得し、開発したツールを用いてライブラリ OS の拡張を支援する。また、クラウド外部のユーザが IDS の実行結果を確認できるようにするために、ライブラリ OS において暗号化を行うことにより安全な通信を実現する。

課題(1)で開発したファイルシステムをライブラリ OS に統合する。その上で、ライブラリ OS 上で既存の様々な IDS を動作させられるようにする。必要に応じて、ライブラリ OS に不足している機能を追加する。

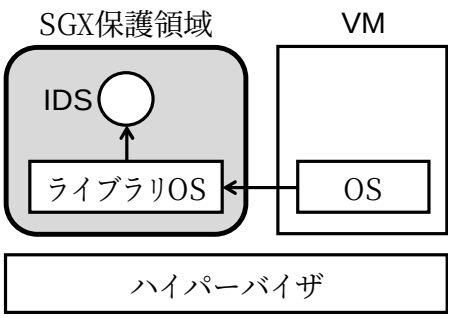

図 4　ライブラリ OS の利用

(3) 複数の SGX 保護領域を用いた監視機能の分割

オフロードした IDS をどのように VM の内部と外部に分割するのが最適かを検討する。SGX 保護領域とその外部とのインタフェースについては様々な研究が行われており、セキュリティや性能のトレードオフがあるため、それらの研究を参考にしながら設計を行う。

次に、ユーザの VM 内で SGX 保護領域を用いて IDS を動作させられるようにする（図 5）。そのために、VM 外部で SGX 保護領域を用いて IDS ヘルパを動作させ、VM 内の情報を取得して IDS に安全に転送できるようにする。さらに、この機構を応用して、IDS をクラウド内の別のホスト上でも動作させられるようにする。

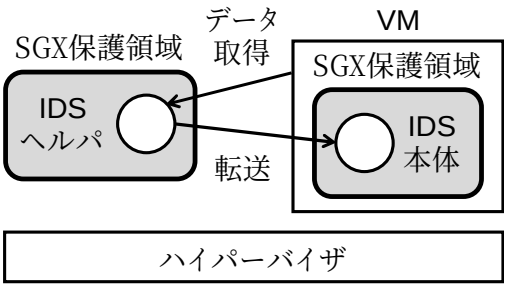

図 5　監視機能の分割

４．研究成果

(1) SGX 保護領域からの VM 監視

オフロードした IDS を SGX 保護領域で動作させられるようにするために、SGX 保護領域から VM のメモリを監視する機構を開発した。IDS が VM 内の OS データにアクセスする時には保護領域外のプログラムを呼び出し、そこからハイパーバイザを呼び出すことで要求された VM のメモリデータを取得する。この処理を IDS の開発者から隠蔽するためのツールを開発し、IDS を OS のカーネルモジュールのように記述できるようにした。

IDS が安全に VM のメモリを監視できるようにするために、IDS とハイパーバイザの間のやり取りを暗号化し、整合性を検査する機構を開発した。IDS が保護領域外のプログラムを実行する際には要求する仮想アドレスを暗号化し、ハッシュ値を付加する。要求を受け取ったハイパーバイザはハッシュ値を検証して、改ざんされていなければ仮想アドレスを復号して VM のメモリデータを取得する。同様に、ハイパーバイザは取得したメモリデータを暗号化してハッシュ値を付加し、IDS はハッシュ値を検証してからメモリデータを復号する。

また、SGX 保護領域内から VM のストレージを安全に監視する機構を開発した。クラウド内部の攻撃者による盗聴を防ぐために、ストレージ全体を暗号化して SGX 保護領域で復号する。そのために、SGX 保護領域内で動作するファイルシステムを開発した。その上で、chkrootkit と呼ばれる IDS と同等の機能を SGX 保護領域内で実現した。具体的には、VM のメモリ監視機構を用いて 9 種類、VM のストレージ監視機構を用いて 57 種類の攻撃を検知できるようにした。

これらの成果をまとめて論文を執筆し、クラウドに関する国際会議で発表を行った。

(2) SGX 保護領域での高度な IDS 実行

SGX 保護領域内で既存の高度な IDS を実行させられるようにするために、ライブラリ OS を用いて IDS が透過的に VM 内の OS 情報を取得できるようにした。既存の IDS は proc ファイルシステムを用いて OS 情報を取得することが多いため、VM 内の OS 情報を返せるように Graphene-SGX の proc ファイルシステムを改造した。しかし、調査の結果、Graphene-SGX では既存の IDS を動かすのが容易ではないことが分かった。

そこで、別のライブラリ OS である SCONE を用いて、SGX 保護領域内で既存の IDS を実行可能なシステムを開発した。SCONE は Graphene-SGX よりも軽量なライブラリ OS であり、OS 情報を返す proc ファイルシステムは提供されていなかったため、IDS に対して VM 内の OS 情報を返す proc ファイルシステムを新たに開発した。このシステムを用いて、既存の netstat を実行して VM のネットワーク情報が取得できることを確認した。

一方、SCONE を用いると IDS が複数のプロセスを実行する際のオーバヘッドが大きいことが判明した。そこで、Occlum と呼ばれるライブラリ OS を用いて SGX 保護領域内で既存の IDS を実行するシステムも並行して開発した。Occlum は複数プロセスの実行を軽量に行うことを可能にする機能を提供しているため、開発したシステムで動作する IDS のオーバヘッドを大幅に削減することができた。SCONE と Occlum を用いたシステムについて機能および性能の評価を行い、それぞれのトレードオフを明らかにした。

これらの成果をまとめて論文を執筆し、クラウドに関する国際会議に採択された。

(3) 複数の SGX 保護領域を用いた監視機能の分割

IDS を複数の SGX 保護領域に分割する計画であったが、システム管理モード（SMM）と呼ばれる安全な実行環境と SGX 保護領域に分割するシステムを開発した。これにより、ハイパーバイザに依存せずにより安全に IDS をオフロードすることが可能になった。さらに、課題(1)で開発した SGX 保護領域で動作する IDS のプログラムを自動変換するツールを SMM に対応させ、複雑な OS 情報を取得できるようになった。

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計9件（うち招待講演　0件／うち国際学会　3件）

１．発表者名 古賀吉道，光来健一
２．発表標題 Intel SGXとSMMの組み合わせによるIDSの安全な実行機構
３．学会等名 SWoPP 2021
４．発表年 2021年

１．発表者名 Tomoharu Nakano and Kenichi Kourai
２．発表標題 Secure Offloading of Intrusion Detection Systems from VMs with Intel SGX
３．学会等名 14th IEEE International Conference on Cloud Computing (CLOUD 2021)（国際学会）
４．発表年 2021年

１．発表者名 古賀吉道，光来健一
２．発表標題 Intel SGXとSMMを用いたIDSの安全な実行機構
３．学会等名 第33回コンピュータシステム・シンポジウム（ComSys 2021）
４．発表年 2021年

１．発表者名 河村拓実，光来健一
２．発表標題 SGX向け実行環境OcclumとSCONEを用いたVMの安全な監視手法
３．学会等名 情報処理学会 第154回OS研究会
４．発表年 2022年

１．発表者名
河村拓実，光来健一

２．発表標題
SGX向け実行環境SCONEを用いたVMの安全な監視機構

３．学会等名
情報処理学会 第149回OS研究会

４．発表年
2020年

１．発表者名
Kouki Yamato, Kenichi Kourai, Tarek Saadawi

２．発表標題
Transparent IDS Offloading for Split-memory Virtual Machines

３．学会等名
44th IEEE Computers, Software, and Applications Conference (COMPSAC 2020)（国際学会）

４．発表年
2020年

１．発表者名
河村拓実，光来健一

２．発表標題
Intel SGXとSCONEを用いた既存IDSの安全なオフロード

３．学会等名
第32回コンピュータシステム・シンポジウム (ComSys 2020)

４．発表年
2020年

１．発表者名
中野智晴，光来健一

２．発表標題
Intel SGXを用いたVMのメモリとディスクの安全な監視

３．学会等名
コンピュータセキュリティシンポジウム2019 (CSS 2019)

４．発表年
2019年

１．発表者名 Tomoharu Nakano and Kenichi Kourai
２．発表標題 Secure Offloading of Intrusion Detection Systems with Intel SGX in Clouds
３．学会等名 The 7th International Symposium on Applied Engineering and Sciences (SAES 2019)（国際学会）
４．発表年 2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関			
米国	CCNY			