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　情報・通信工学分野

学生番号	226E0102	氏　名	安東 尚哉
論文題目	AMD SEV とネストした仮想化を用いた安全な通信の追跡・制御		

1　はじめに

クラウドで大量のデータが扱われるようになるにつれて，クラウドからのパーソナルデータの漏洩が問題となっている．その原因の一つとして，クラウドのサービスが年々複雑化していることが挙げられる．一般的に，クラウド内のデータの流れはユーザに公開されていないため，ユーザは自分のデータが漏洩したり，意図しないサービスに転送されたりしていてもそのことを把握することができない．この問題を解決するには，ユーザが自分のデータを追跡・制御するためのプライバシ制御機構がクラウド内に必要となる．しかし，ユーザはクラウドの提供するプライバシ制御機構を完全に信頼することはできない．

本研究では，AMD SEV とネストした仮想化を用い，クラウド内の通信の安全な追跡・制御を行うシステム SEV-tracker を提案する．

2　SEV-tracker

SEV-tracker では図 1 のようにユーザが送り込んだ仮想化ソフトウェア（ユーザ・ハイパーバイザ）をクラウドの仮想マシン（VM）内で実行し，プライバシ制御機構を動作させる．ユーザ・ハイパーバイザ上にユーザ VM を作成し，その中でユーザ用のクラウドサービスを動作させる．そのサービスが他のクラウドサービスを利用する場合には，再帰的にユーザ・ハイパーバイザを送り込む．ユーザ・ハイパーバイザはユーザ VM のすべての通信を捕捉して解析し，通信情報をユーザ用のログサーバに送信する．ユーザはログサーバから通信履歴を取得し，視覚的に表示することでデータ流を把握する．

ユーザ・ハイパーバイザをクラウド内で安全に実行できるようにするために，SEV-tracker はユーザ・ハイパーバイザとクラウドを相互に保護する．そのために，AMD SEV と呼ばれる CPU のセキュリティ機能を用いてクラウド VM のメモリを暗号化し，Nested SEV [1] を用いてクラウド VM 内のユーザ VM のメモリを別の鍵で暗号化する．これにより，クラウドがユーザ・ハイパーバイザ内のプライバシ制御機構を無効化することや，ユーザ・ハイパーバイザがクラウドサービスへの攻撃を行うことを防ぐ．

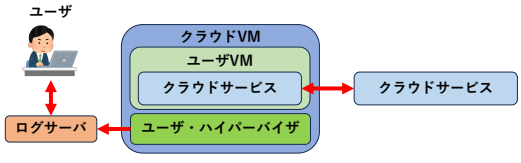

図 1: SEV-tracker のシステム構成

SEV-tracker はネストした仮想化を用いてクラウド VM 内にユーザ VM を作成するため，より多くのリソースを必要とし，クラウドサービスの性能も低下する．この影響を抑えるために，SEV-tracker は最小限の仮想化のみを行う軽量なハイパーバイザの BitVisor をユーザ・ハイパーバイザとして用いる．さらに，ユーザ VM 内のクラウドサービスには Unikernel と呼ばれる軽量なライブラリ OS を提供し，サービスが必要とするな最小限の OS の機能のみをリンクする．

3　実験

SEV-tracker を用いて 2 つのクラウドサービスを実行し，取得した通信履歴を可視化した結果を図 2 に示す．ユーザがサービス 1 にアクセスした時に，サービス 2 経由で監視対象外の外部サービスにアクセスしていることがわかる．また，クラウド VM 内で汎用の KVM と Linux を用いた場合と性能を比較した結果を図 3 に示す．HTTP サーバが使用するメモリが増えると SEV-tracker の方が性能がよくなることがわかった．

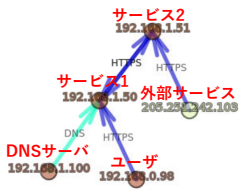

図 2: 通信履歴

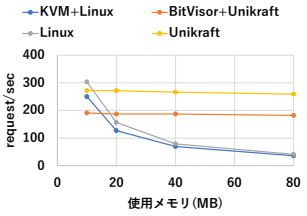

図 3: サービスの性能

4　おわりに

本研究では，AMD SEV とネストした仮想化を用いてユーザがクラウド内のデータ流を安全に追跡・制御することを可能にするシステム SEV-tracker を提案した．今後の課題はクラウド VM とユーザ VM に SEV を適用して性能を測定することである．

参考文献

[1] 瀧口ら: Nested SEV: ネストした仮想化への AMD SEV の適用. ComSys2022.