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

近年，不正アクセスや設定の不備によるクラウドからのデータ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考えられる．一方，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．このようなプライバシ制御機構があれば，自分のデータの保存先や流通範囲を知ることができたり，データの流通範囲を制限することで情報漏洩を防いだりすることができる．しかし，クラウドの提供するプライバシ制御機構をユーザが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，通信の安全な追跡・制御を行うシステムである SEV-tracker を提案する．

2　SEV-tracker

SEV-tracker ではユーザが仮想化ソフトウェア（ユーザ・ハイパーバイザ）を含んだディスクを作成してクラウドに送り込む．クラウドがユーザのディスクを用いて仮想マシン（VM）を起動すると，図 1 のようにユーザ・ハイパーバイザが起動されてユーザ VM が作成される．最後に，ユーザ VM 上ではクラウドのディスクからクラウドサービスを動作させる．

このユーザ・ハイパーバイザとクラウドサービスを相互に保護するために，SEV-tracker は 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 とユーザ VM のメモリを個別に暗号化する．これによって，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の情報を盗むことを防ぐ．

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，クラウドサービスの性能が低下する．このオーバヘッドを削減するために，SEV-tracker は軽量なハイパーバイザである BitVisor をユーザ・ハイパーバイザとして用いる．BitVisor は VM を 1 つだけサポートし，最小限のデバイスのみを仮想化する．さらに，ユーザ VM 内のクラウドサービスには Unikraft と呼ばれる軽量なライブラリ OS を提供する．Unikraft はサービスが必要な最小限の OS の機能をアプリにリンクする．

SEV-tracker はユーザのすべての通信を監視することにより，データ流の追跡・制御を可能にする．そのために，ユーザ・ハイパーバイザはユーザ VM の通信を捕捉して解析し，通信情報をログサーバに送信する．ユーザがログサーバに要求を送ると，クラウドサービスの通信履歴を返す．

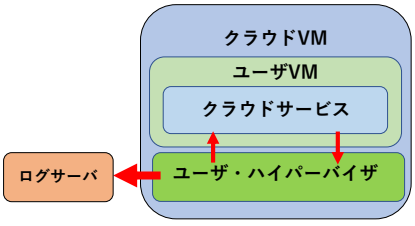

図 1: SEV-tracker のシステム構成

3　実験

SEV-tracker を用いて動作させたサービスの性能測定を行った．

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．今後の課題は取得した通信履歴を視覚的にわかりやすく表示するツールの開発である．