論文概要

学科	情報・通信工学科	指導教員	光来健一
学生番号	１８２Ｃ１００５	氏名	安東尚哉
題目	AMD SEV を用いたクラウド内データ流の安全な追跡・制御		

1　はじめに

クラウドの使用率は年々上昇しており，それに伴ってユーザのパーソナルデータを扱うことも増えている．それに加えて，近年のクラウドでは複雑なサービスを提供するために，マイクロサービスなどのように複数のサービスを連携させることが一般的になっている．そのため，パーソナルデータが様々なサービスに転送されていく可能性がある．しかし，クラウド内でのデータの流れは基本的に非公開であるため，ユーザは自分のデータがどのように扱われているかを知ることができない．

本研究では，ユーザがクラウド内のデータ流を安全に追跡・制御することによりプライバシ制御を可能にするシステム SEV-tracker を提案する．

2　SEV-tracker

SEV-tracker は図 1 のように，ユーザが送り込んだハイパーバイザをクラウドの VM 内で実行する．そして，その上で動作するユーザの VM 内でクラウドサービスを実行する．ユーザ・ハイパーバイザをクラウドから保護するために，AMD SEV と呼ばれる CPU の機能を用いてクラウド VM のメモリを暗号化する．同様に，ユーザ VM のメモリも暗号化してクラウドサービスをユーザから保護する．

クラウド VM 内でユーザ VM を実行する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 を用いる．また，ユーザ VM 内では必要最小限の機能のみを提供するライブラリ OS である Unikraft を用いる．SEV を用いるために Unikraft には UEFI 対応を行った．

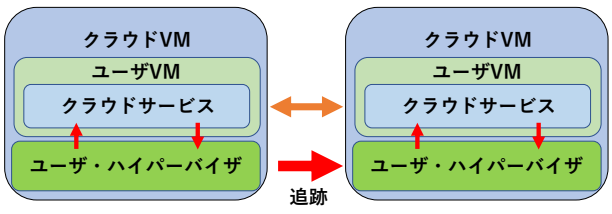
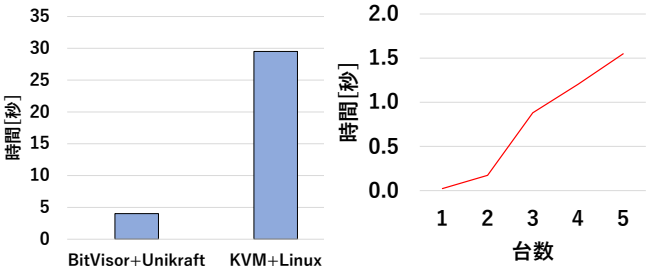


図 1: SEV-tracker のシステム構成



(a) 起動時間　　**(b)** 履歴取得時間

図 2: 実験結果

クラウド内のデータ流を追跡可能にするために，SEV-tracker はユーザ・ハイパーバイザにおいてクラウドサービスの通信を記録する．ユーザがユーザ・ハイパーバイザに要求を送ると，その上で実行されているクラウドサービスの通信履歴を返す．通信先でもユーザ・ハイパーバイザが動作している場合には再帰的に要求を送って通信履歴を取得する．

3　実験

クラウド VM 内で BitVisor と Unikraft を起動する時間を測定した．その結果，図 2(a) に示すように標準的な KVM と Linux を起動する場合に比べて約 6 倍高速であることが分かった．また，図 2(b) はユーザ・ハイパーバイザから通信履歴を取得するのにかかった時間である．再帰的に取得すると台数に応じた時間がかかることが分かった．

4　まとめ

本研究では，AMD SEV 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．今後の課題は様々なクラウドサービスを動作させてデータ流の追跡・制御を行えるようにすることである．