九州工業大学 情報工学部 情報・通信工学科 2025 年度 卒業論文 概要

コース	ソフトウェアデザイン	指導教員	光來 健一
学生番号	24222205	氏　　名	近藤 瑛

論文題目	ライブラリ OS を用いた異種 TEE 間でのマイグレーションの実現

1　はじめに

近年，クラウドが広く普及し，様々なサービスで利用されるようになっている．一方で，クラウドの内部犯による攻撃によってサービス内の機密情報が盗まれる危険性がある．このような情報漏洩を防ぐために，最近のクラウドでは CPU の隔離実行環境 (TEE) を用いてユーザのアプリケーションや仮想マシン (VM) を安全に実行する機密コンピューティングが活用されている．各 CPU ベンダから様々な TEE が提供されており，プロセス単位で保護を提供する TEE や VM 単位で保護を提供する TEE などがある．同じ種類の TEE 間では，ホストのメンテナンス時などに TEE 内のアプリケーションを別のホストに移動させることを可能にするマイグレーション手法が提案されている．しかし，異なる種類の TEE 間では，TEE ごとにマイグレーション手法が異なることから，マイグレーションを行うことができない．

本研究では，TEE 内で共通のライブラリ OS を用いてアプリケーションを実行することで，異なる種類の TEE 間でもマイグレーションを可能にする MigTEE を提案する．

2　MigTEE

MigTEE はアプリケーションのマイグレーションを可能にするために，異なる種類の TEE 内で共通のライブラリ OS を実行する．ライブラリ OS はアプリケーションに OS の機能をライブラリとして提供する．そのため，汎用 OS を動かせないプロセスベースの TEE でも利用することができ，汎用 OS を動かせる VM ベースの TEE でも汎用 OS の代わりに利用することができる．図 1 のように，移送元 TEE 内でアプリケーションの状態を保存し，移送先ホストに転送して TEE の状態を復元することにより，実行中のアプリケーションを中断することなく移動させることができる．

マイグレーションを行う際には，まず，移送元 TEE の内部で動作するライブラリ OS が自身の状態と実行中のアプリケーションの状態を保存する．ライブラリ OS はプロセスの各メモリ領域について先頭アドレスとサイズおよび，実際に割り当てられたページのメモリデータを保存する．さらに，プロセス ID などの実行時情報，ルートディレクトリやマウント情報などのファイルシステム情報，CPU やメモリ

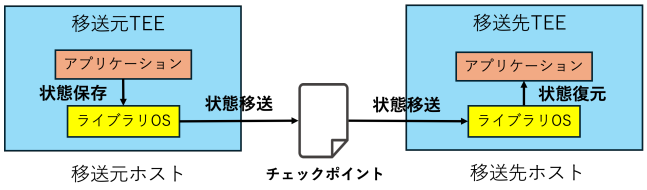

図 1. MigTEE のシステム構成

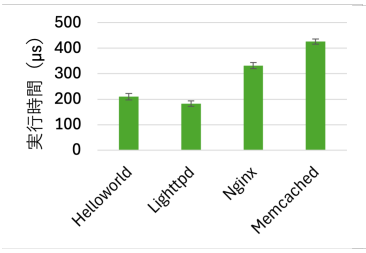

図 2. 保存時間

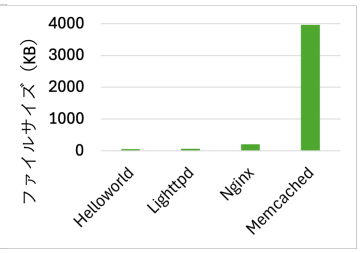

図 3. ファイルサイズ

などのシステム情報をチェックポイントとして保存する．この処理はアプリケーションが save システムコールを実行することによって行い，取得した状態はチェックポイントファイルに保存する．

その後，移送先ホスト上に新たな TEE を作成し，その内部にアプリケーションとライブラリ OS の状態を復元する．ライブラリ OS はチェックポイントファイルに保存された状態を読み込み，新たに作成された TEE 内のアプリケーションに対して設定する．また，移送元と同じメモリ領域を割り当ててメモリデータを書き戻すことでアプリケーションの状態を復元する．

3　実験

MigTEE を用いてアプリケーションをマイグレーションする実験を行った．この実験には，ライブラリ OS として Intel SGX と Intel TDX の両方に対応している Gramine [1] を用いたが，TEE は用いずにアプリケーションの実行を行った．実験の結果，アプリケーションの状態の保存には成功したが，復元には失敗した．これは，復元時に CPU トポロジ情報の取得に失敗したためである．

次に，実行中のアプリケーションの状態保存にかかる時間を測定した．保存時間は図 2 に示すようになり，どのアプリケーションでも十分に短く，ばらつきも小さいことが分かった．また，保存されたチェックポイントのファイルサイズは図 3 に示すようになり，アプリケーションによって大きく異なることが分かった．

4　まとめ

本研究では，TEE 内で共通のライブラリ OS を用いることで，異なる種類の TEE 間においてもアプリケーションのマイグレーションを可能にする MigTEE を提案した．今後の課題は，移送元 TEE で保存した状態を基に移送先 TEE でアプリケーションの復元を行えるようにすることである．

参考文献

[1] C. Tsai, et al.: Graphene-SGX: A Practical Library OS for Unmodified Applications on SGX. ATC 2017.