# 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 | 246E0120 | 氏　名 | 佐藤 太陽 |
|---|---|---|---|
| 論文題目 | Arm TrustZone を用いた<br>クラウドアプリケーションの安全かつ柔軟な協調実行 | | |

## 1　はじめに

クラウドアプリケーションをユーザの近くで実行し，サービス品質を向上させるエッジコンピューティングが普及してきている．エッジデバイスは信頼できない場合があるが，CPU が提供する隔離実行環境を用いることで安全に実行を行うことができる．例えば，Arm TrustZone は実行環境を 2 つのワールドに分割し，セキュアワールドで隔離実行するアプリケーション (TA)，ノーマルワールドでそれ以外のアプリケーション (CA) を動作させる．セキュアワールドでクラウドアプリケーションを実行することが考えられるが，セキュアワールドは高い権限を持っているため，クラウドアプリケーションに脆弱性があるとエッジデバイス全体に影響が及ぶ．そのため，TA として実行する部分をできるだけ小さくし，CA と連携しながら実行することが望ましい．しかし，CA との連携には専用 API を用いる必要があり，柔軟な協調は容易ではない．

本研究では，2 つのワールドに分割されたクラウドアプリケーションに対して，OS 標準の POSIX API を用いた協調実行を可能にする TZmediator を提案する．

## 2　TZmediator

TZmediator は図 1 のように，クラウドアプリケーションの中の保護する必要がある処理のみをセキュアワールドで TA として実行し，それ以外の処理はノーマルワールドで CA として実行する．さらに安全性を高める必要がある場合には，セキュアワールドの処理を WebAssembly (Wasm) を用いて安全に実行することもできる．CA と TA は並列に実行され，ワールド間にまたがってパイプやソケット，シグナル，共有メモリなどの POSIX API を用いて協調動作する．

TZmediator はノーマルワールド内に TA に対応するシャドウプロセスを作成し，CA と TA はシャドウプロセスを介して通信を行う．TA は TZmediator が提供する TZm-TA ライブラリ経由で POSIX API を利用する．

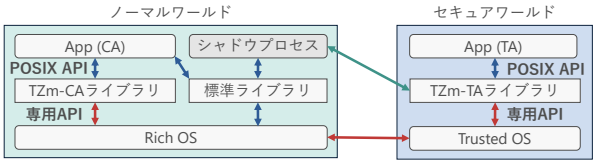


図 1. TZmediator のシステム構成

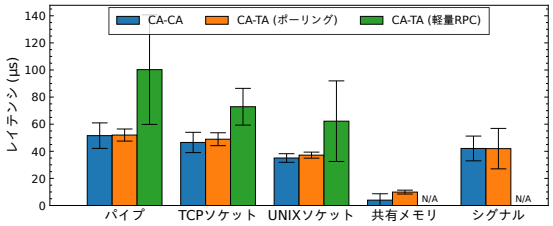


図 2. 通信のレイテンシ

このライブラリがシャドウプロセスを呼び出すと，シャドウプロセスは指定された POSIX API を代理実行し，実行結果を TA に返送する．この時，事前に確保した共有メモリを用いることで，シャドウプロセスの呼び出しを高速化する．一方，CA は標準ライブラリによって提供される POSIX API を利用してシャドウプロセスと通信し，シャドウプロセスが TA との通信を行う．

TZmediator は CA と TA を用いることを意識せずにクラウドアプリケーションを開発することを可能にする．そのために，CA に TZm-CA ライブラリを提供し，POSIX API を利用して TA を実行することで，TA 関連の複雑な処理を CA から隠蔽する．同様に，TA に提供される TZm-TA ライブラリにおいても専用 API を用いた複雑な処理を TA から隠蔽する．

## 3　実験

TZmediator における CA と TA 間の通信性能を IPC-Bench を用いて測定した．シャドウプロセスの呼び出し方式として軽量 RPC とポーリングの 2 種類を用い，ノーマルワールド内の CA 間の通信性能と比較した．図 2 に示すように，TZmediator は CA 間での通信よりも，ポーリングで 1.0〜2.5 倍，軽量 RPC で 1.6〜1.9 倍のレイテンシとなることが分かった．

また，深層学習を行う DarkneTZ をいくつかの POSIX API を用いるように修正し，推論を行った．その結果，実行時間が最大 15%増加するものの，正しく推論を行えることが確認できた．

## 4　まとめ

本研究では，TrustZone の 2 つのワールドに分割されたクラウドアプリケーションに対して，POSIX API を用いた協調実行を可能にする TZmediator を提案した．今後の課題は，TZmediator を活用した様々なクラウドアプリケーションを開発することである．