最所研究室 研究紹介
コンテナ型仮想環境のセキュリティ研究

20G451 飯國 隆志

研究分野

OS, システムソフトウェア, 仮想化, コンテナ, クラウドコンピューティング

一言で言えばアプリケーション実行基盤について研究
(例: OS, VM, コンテナ)

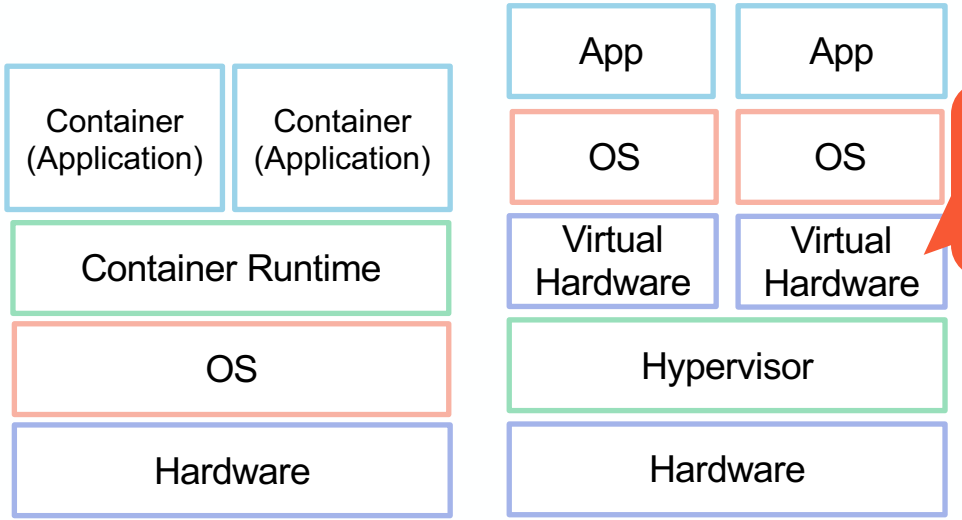
目的: 安全かつ高速なアプリケーション実行基盤の開発

近年のクラウドコンピューティングの需要から
コンテナ型仮想化について研究

コンテナ型仮想化(Containerization)

クラウドコンピューティングを実現する1要素

コンテナ型仮想化(通称: コンテナ)とは
- **OS上で様々なリソースを分離したプロセス**
- あたかも複数のOSが動いているように見える
- VMと比べ**低容量、高速起動**
- Docker, Kubernetesなどのソフトウェアが有名



コンテナの導入事例

コンテナは生活基盤の裏で既に動いている

- Cloud: Amazon, Google, Microsoft, IBM, Oracle
- 金融: PayPay, merpay
- ゲーム:ドラゴンクエストウォーク
- 飲食: Pizza Hut

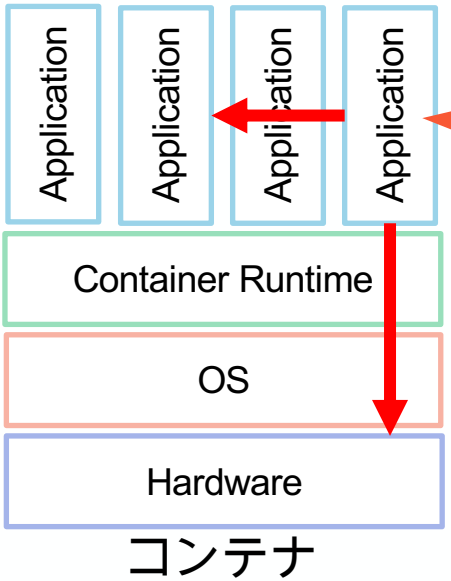
様々な企業のシステムがコンテナ上で実行される用になった

企業がコンテナ(Docker, Kubernetes)を導入する利点

- 軽量なので、オートスケール(自動でサーバを増やす)が高速
- ハード、ホストOSの違いを抽象化 → **移植性が高い**
- インフラを宣言的に定義できる → **インフラのバージョン管理**
- 障害時の切り戻しが高速 → **高速な障害対応**

コンテナのセキュリティ的課題

コンテナは軽量だがコンテナ間で共有された**OS, コンテナランタイムの脆弱性を用いて攻撃されるリスク**が存在



コンテナ内から
ハードウェア、
他ユーザのコンテナ
を攻撃される

1台のサーバで
複数のユーザのコンテナが実行
されるサービスだと致命的

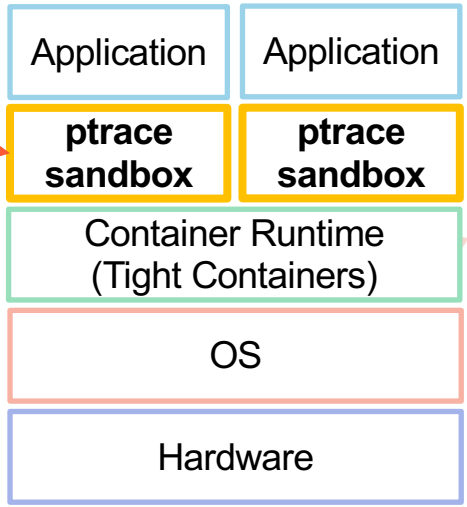
Tight-Containersの開発

コンテナを強力に隔離するコンテナランタイム

防壁(ptrace sandbox)を追加

- システムコールを制限
- root権限不要で実行可能

- コンテナ内の危険な命令をフィルタ
- コンテナに不要な権限を与えない



Tight-Containers

共同研究者募集中

一緒に研究したい人
- **新しい技術**に興味がある人
- **コンピュータの仕組み**に興味がある人
- **プログラミング**が苦手でない人
- (Optional) **英語**ができる人

GoogleやAmazon、多くの大学が取り組んでいるホットな分野なので、やりがいのある研究だと思います！
一緒に研究しましょう！！

質問等はTeamsや s20g451@stu.kagawa-u.ac.jp まで