2019年度未踏IT人材発掘・育成事業

高速なVMI機構を実装したバイナリ解析基盤
― FastVMIX / Fast VMI on Intel VT-X ―

森瑞穂（電気通信大学）

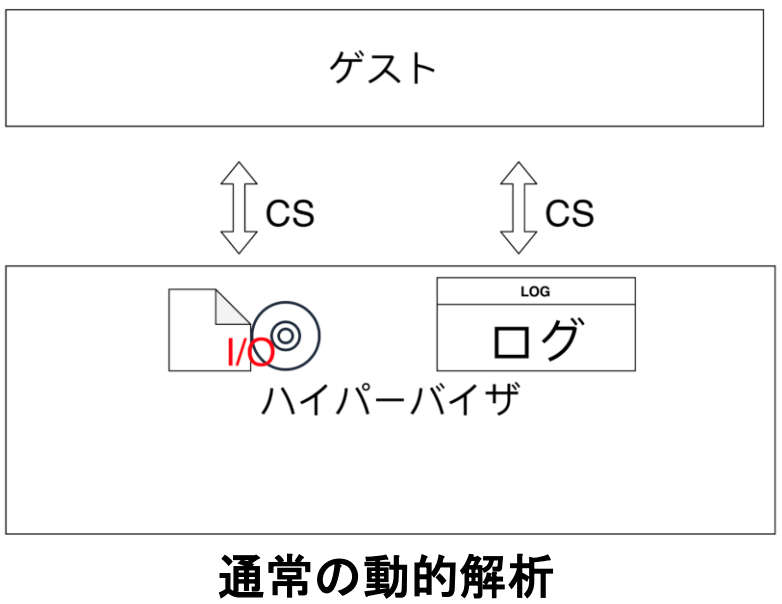
なぜ動的解析？

マルウェアの挙動を早く明らかにするために実際にマルウェアを動作させる

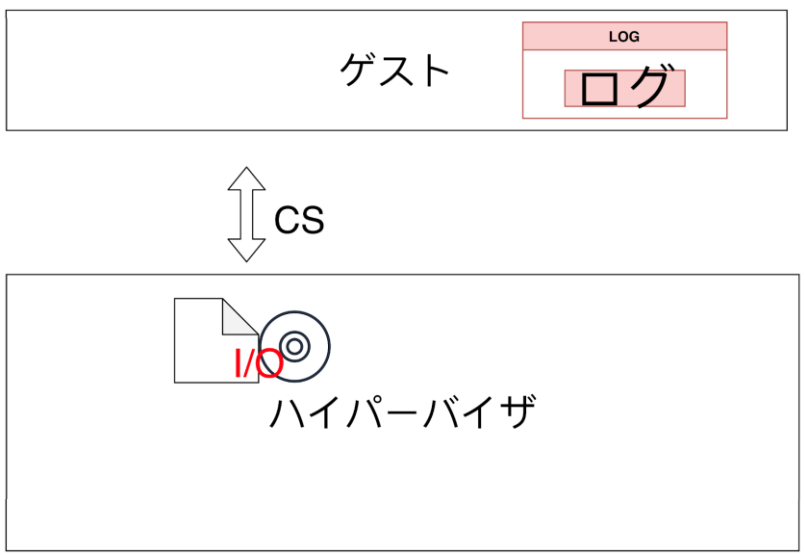
なぜFastVMIX?

マルウェアの動的解析を高速に安全に効率よく行うため

システムはなるべくコンテキストスイッチを廃したデザインになっている



通常の動的解析



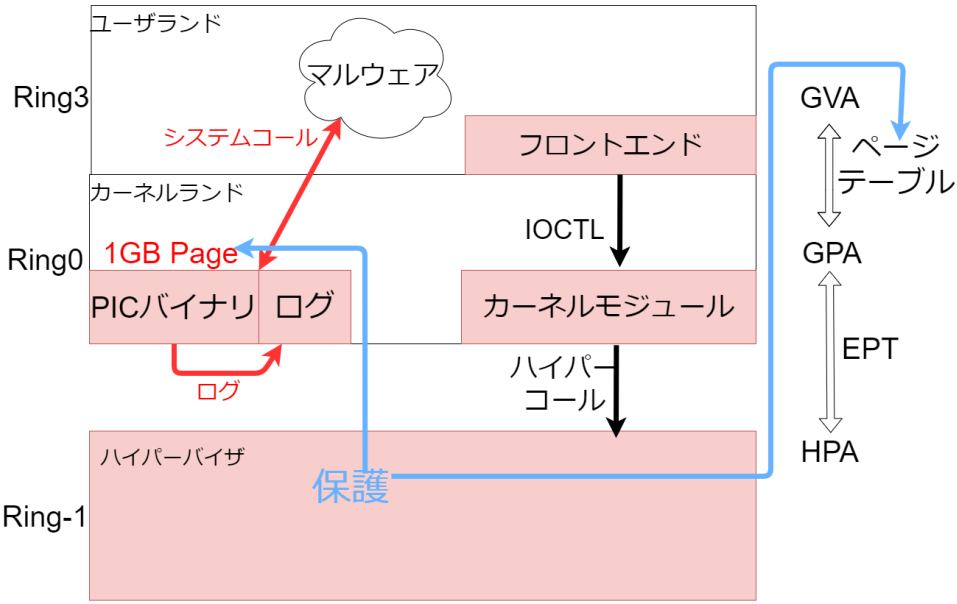
FastVMIX

FastVMIXの特徴

高性能

独自のベンチマークにより

- DRAKVUF™の306倍高速
- ネイティブより5.3倍遅い



対解析妨害機能

マルウェアの小賢しい振舞を防ぐ

- CPU時間の偽装を実装

拡張はPICバイナリで

1GB Huge Pageで動くバイナリを拡張するだけでよい