



オペレーティングシステム(OS)や仮想化技術を中心とした システムソフトウェアの研究をしています。

■ システムソフトウェア研究の特徴と魅力

OSや仮想化ソフトウェアといった低レイヤのシステムソフトウェアは、CPUの特権命令の実行や、全ての物理メモリへのアクセス、各種デバイスの直接制御が可能な特別な権限を持ったソフトウェアであり、システム全体の性能や安全性を左右する重要な研究対象です。

システムソフトウェア研究には、コンピュータの原理・本質を捉えた適切な抽象概念をアプリケーションに提供するという「理学的」な側面と、実際のハードウェアで設計・実装・評価することで有効性を検証する「工学的」な側面があります。さらに、OSのアーキテクチャの選択や設計思想には、開発者のセンスや美学が色濃く表れるなど「アート的」な要素もあります。例えば、モノリシックカーネルかマイクロカーネルかという議論は、単なる性能比較にとどまらず、設計哲学の対立でもあります。

このように、理・工・芸の要素が融合するシステムソフトウェア研究は、深い知的探究と創造性を求められる、奥行きのある研究分野です。

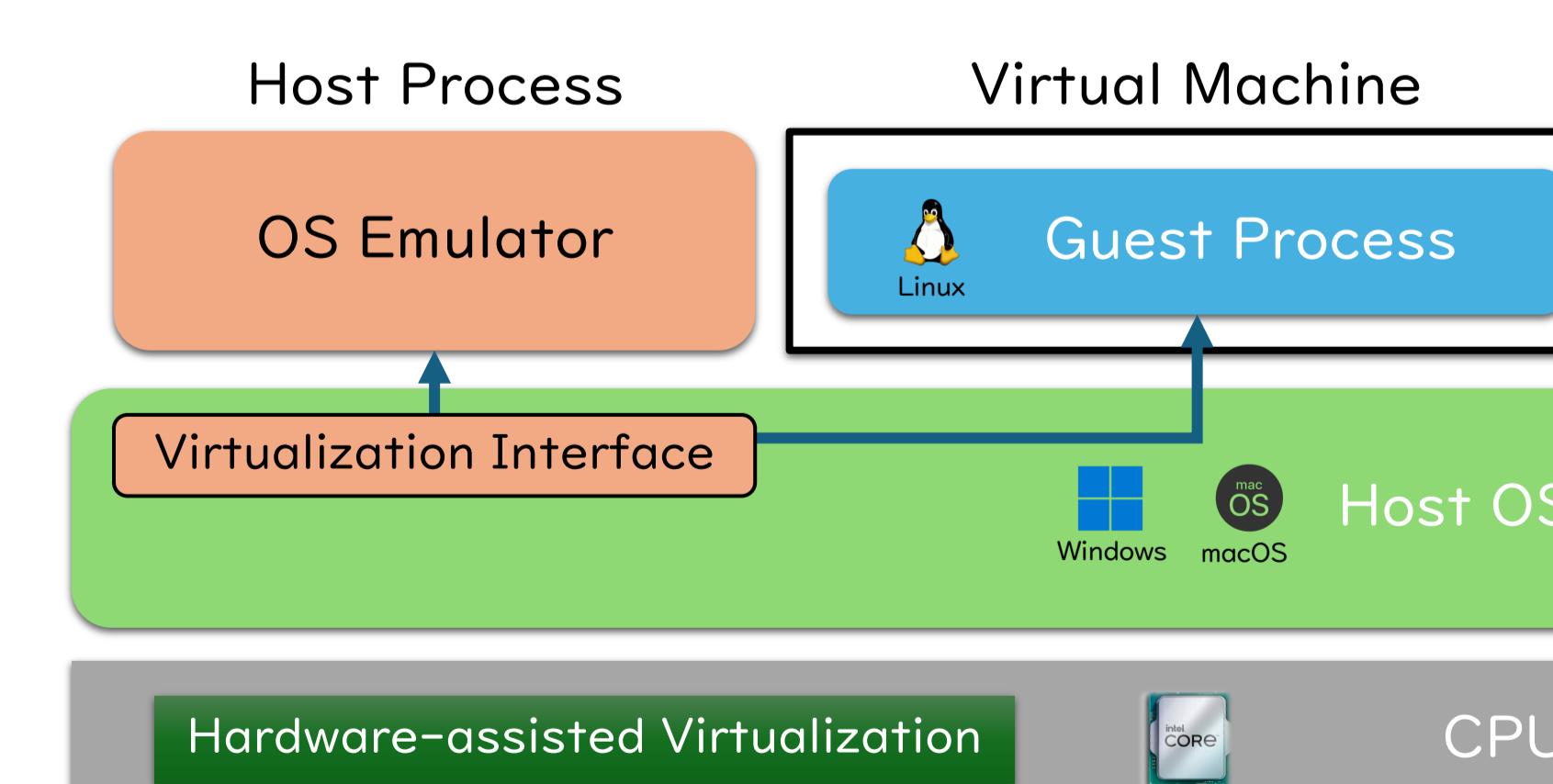
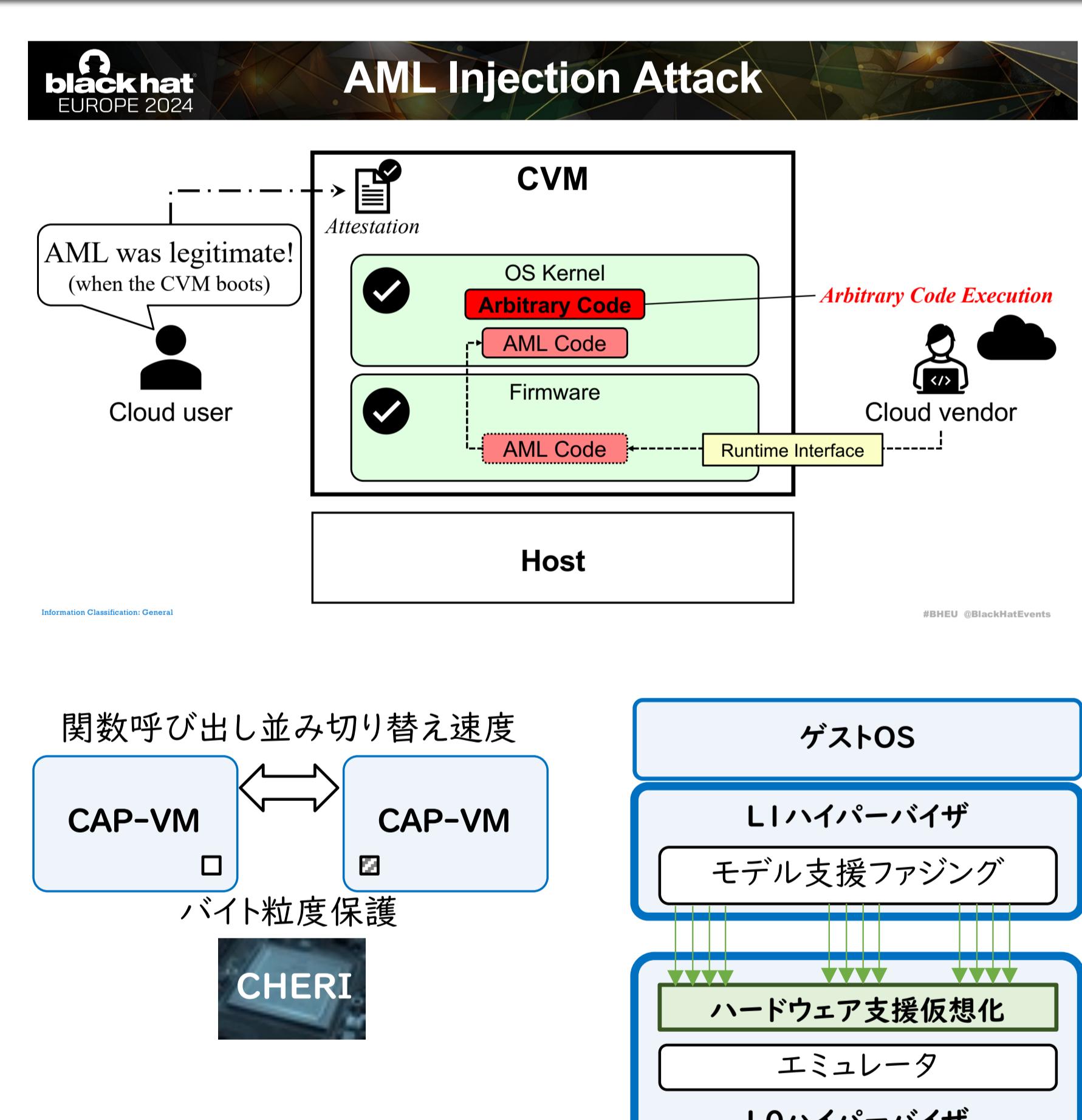
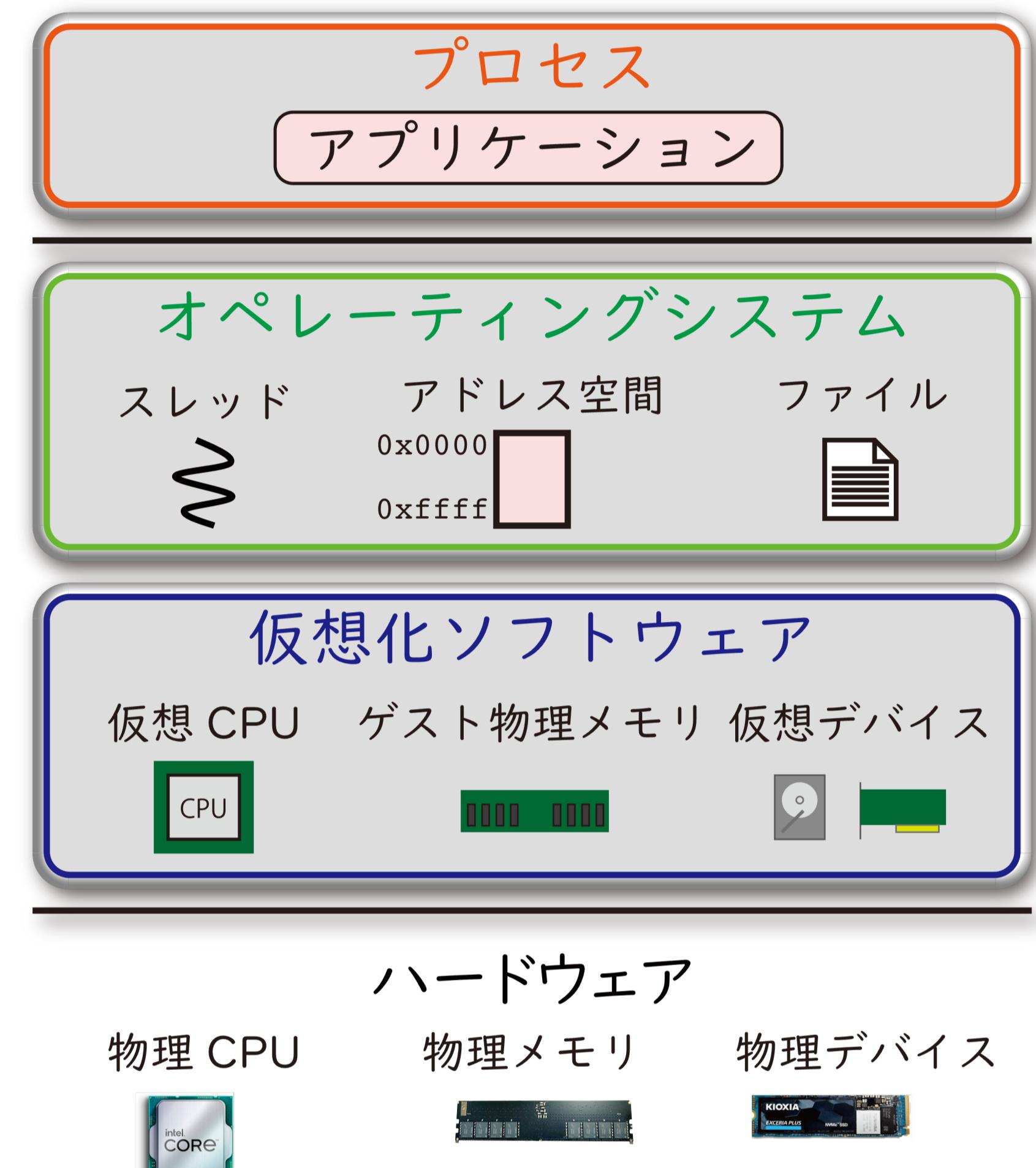
■ 研究紹介1: システムソフトウェアのセキュリティ研究

品川研究室での最新の研究として、機密仮想マシン(CVM)があります。CVMはCPUベースの暗号化・検証機能を利用して、クラウドベンダーを信用することなく、ユーザの機密性の高いデータを安心してクラウド上で処理できるようにするための仕組みです。しかし、我々の研究によって一般に広く使われているCVMには、クラウドベンダーがCVM内で任意コード実行できる欠陥があることを発見し、Black Hat Europe 2024で発表しました。

また、仮想マシンの中で仮想マシンを動作させられるネストッド仮想化の脆弱性をファジングで発見する研究や、国産ハイパーバイザであるBitVisorを用いた研究などもしています。他にも、ケンブリッジ大学が研究開発したCHERIと呼ばれるCPUアーキテクチャを活用した、バイト粒度で高速かつ柔軟な保護ができるケーパビリティ仮想マシン(CAP-VM)の仕組みの研究をImperial College Londonと共同で行なっています。

■ 研究紹介2: システムソフトウェアによる性能・機能向上の研究

品川研究室では、セキュリティに限らずシステムソフトウェアによる性能向上や機能向上のための研究を幅広く手掛けています。例えば、FPGAによるメモリ操作高速化、新しいOS開発のためのデバイスドライバ再利用、コンテナ起動時のレイヤ取得高速化、不揮発メモリ向けファイルシステム、低遅延のクラスタスケジューラ、macOSやWindows上でLinuxバイナリを動作させるOSエミュレータなど、幅広い対象・目的で研究を行なっています。



品川研究室では学生の皆さんのが興味を持って楽しく研究することを目指しています。低レイヤのシステムソフトウェア(Linux, KVM, BitVisorなど)やシステムプログラミング(C, C++, Rustなど)が好き and/or 得意な学生さんは特に歓迎しますが、システムソフトウェアに興味があればどのレイヤでも楽しく研究ができると思います。