**2019年度未踏IT人材発掘・育成事業**
**プロセッサートレースを用いた組み込みデバイス向けファザーの開発**
**高速なARM向けファザー**

**大塚　馨**


# ZeroSight

**ZeroSightで脆弱性発見を自動化**

ZeroSightは、ARMの
システムコンポーネント向けファザー。

ARMのプロセッサー支援機能CoreSightを用いた
ハードウェアモードとソフトウェアモードを開発。

**Linux kernel 4.4.0では、9日間で**
**Linuxカーネルのバグを326,681回観測。**

**ハードウェアモード**

ARMのホスト上のCoreSightと
Virtualization Extensionを用いて
高速にカーネルファジングを可能にする。

**ソフトウェアモード**

QEMU上で実装されたソフトウェアモードはx86
のホストでファジングが可能。

**見つかったカーネルクラッシュのリスト**
**https://github.com/roppinhoppin/kernel_crashes**