

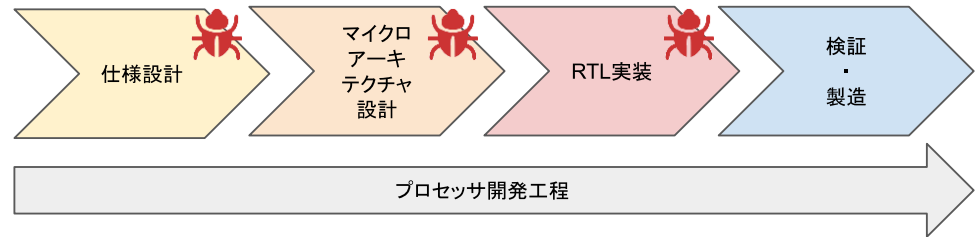
ハードウェアセキュリティ検査システムの開発

— MicroFuzz: RISC-Vプロセッサ向けファuzzer —

杉山 優一

開発動機

- プロセッサの実装にはバグが多い
- 既存のRISC-V用検査システムでは不十分



MicroFuzzの特徴

RISC-Vプロセッサ向けの

- 変異アルゴリズム
- 実行時情報のフィードバック
- 入力評価アルゴリズム

を実装したファuzzer

各プロセッサのマイクロアーキテクチャ
実装に合わせた検査

既存ツールでは発見が難しい
プロセッサのバグ・脆弱性を検出可能

検出したバグ

<https://github.com/lowRISC/ibex/issues/1277>
<https://github.com/lowRISC/ibex/issues/1282>
<https://github.com/rsd-devel/rsd/issues/37>
<https://github.com/rsd-devel/rsd/issues/38>
<https://github.com/rsd-devel/rsd/issues/39>

