

マイクロアーキテクチャ攻撃

九州大学 サイバーセキュリティセンター
谷本 輝夫

講義予定

講義資料-1（マイクロアーキテクチャ攻撃 1）

- ▶ マイクロアーキテクチャ攻撃とは
- ▶ CPU を対する攻撃

講義資料-2（マイクロアーキテクチャ攻撃 2）

- ▶ メモリに対する攻撃
- ▶ マイクロアーキテクチャ攻撃の影響と対応

演習資料-1

- ▶ 実習（準備）

演習資料-2

- ▶ 実習（攻撃の再現実験）

レポート課題

- ▶ 講義資料を理解したうえで、演習資料に従って Spectre の再現実験を行ってください。
- ▶ 以下をレポートにまとめ、MLS に提出してください

1. Spectre 演習

- ▶ 攻撃が成立する様子のパイプラインを、命令列を対応させて説明する
- ▶ Spectre を回避するための変更を加えたプログラムを作成し、1) そのプログラムと、2) 回避できる理由、3) 回避できていることを示すパイプラインの様子をまとめる
- ▶ 実施した回避策の性能への影響を命令列もしくはそれを実行した際のパイプラインの様子と関連付けて考察する

2. Spectre や Meltdown などのマイクロアーキテクチャ攻撃について、自分が計算機を使用するシーンの中でこれらの攻撃の影響を受けるものを挙げ、それに誰がどのような対策をしているか／するべきか論じてください