RISC-VのSpectre脆弱性と対処法

陳拓, 須崎有康（情報セキュリティ大学院大学）

Spectre亜種の一覧（2017~2023）

RISC-Vボードで確認したSpectre脆弱性

Spectre-*	CVE	脆弱性の名称	関連仕組み	出典
v1	2017-5753	BCB: Bounds Check Bypass	PHT: Pattern History Table BTB: Branch Target Buffer	Kocher et al, IEEE S&P 19
v1.1	2018-3693	BCBS: Bounds Check Bypass Store	Speculative buffer overflows	V. Kiriansky et al, arXiv 18
v1.2	未採番	RPB: Read-only protection bypass	Lazy PTE enforcement (similar to Meltdown)	V. Kiriansky et al, arXiv 18
v2	2017-5715	BTI: Branch Target Injection	BTB: Branch Target Buffer	Kocher et al, IEEE S&P 19
v3 (Meltdown)	2017-5754	RDCL: Rogue Data Cache Load	“Exception handling”, or “exception suppression”	M. Lipp et al, USENIX Sec 18
v3a	2018-3640	RSRR: Rogue System Register Read	Counters, debug registers, control registers, others	INTEL-SA-00115 18
v4	2018-3639	SSB: Speculative Store Bypass	STL: Store-To-Load	Kocher et al, IEEE S&P 19
v5	未採番	ret2spec: Return Mispredict	RSB: Return Stack Buffer	Koruyeh et al, USENIX Sec 18
Lazy FP	2018-3665	Lazy FP State Restore	Lazy FPU context switching	Stecklina et al, arXiv 18
BHI	2022-0001 2022-0002 2022-23960	BHI: Branch History Injection	BHB: Branch History Buffer	Barberis et al, USENIX Sec 22
v6	未採番	SRV: Speculative Vectorization Exploit	Leakage from Higher Dimensional Speculation	S. Karuppanan et al, arXiv 23
LAM	未採番	SLAM: Spectre based on Linear Address Masking	LAM: Linear Address Masking	Hertogh et al, IEEE S&P 24（予定）

Spectre対処法の一覧（2017~2023） → 継続調査中

RISC-Vボードで有効性の調査中

提案手法	簡単説明	分類	対象亜種	出典
(総論)	1. 投機的実行を停止する. 2. 秘密データへのアクセスを防ぐ. 3. データが隠れチャネルに入るのを防止する. 4. 隠れチャネルからのデータ抽出を制限する. 5. 分岐予測器へ予測の誤りをさせる企みを阻む.	All	v1, v2, v4	P. Kocher et al IEEE S&P 19 (「Spectreの白書」)
Retpoline	RSBはソフトウェアで制御可能とし, コンパイラは RSB へ lfence/pause loop へのアドレッシング命令を追加する.	SW	v2	Google Project Zero
間接的な命令	Retpoline を RISC-V 環境へ導入し, 間接的なジャンプと間接的なカール命令の使用する.	SW	v1	R. Bălucea and P. Irofti arXiv, Jun. 09, 2022
条件分岐命令変換, 他	1. 秘密データにある分岐出力の依存性をアルゴリズム的に除く. 2. 条件分岐を同等の非条件命令に変える. 3. ハードウェアに支援されるSW防御.	SW + HW	v1, v2, v4, v5	D. Evtyushkin et al ACM, Mar. 2018
SpecBuf	ある形の”投機専用バッファ”の増設を提案. 投機的実行で扱われるデータはそれらに保持 (hold)させるのが共通点である. InvisiSpec では, 途中で暫くサイドチャネルでも見えないようにし, データが安全な状態になっていることを確認できてから, そのデータをシステムの他の部分でも観測可能なように開放する. メモリー貫性を破るデータを識別して検認をさせることも可能である. SpecBuf では, 投機的実行の失敗したときに flush 命令でデータを消すことにより , CPU キャッシュへの影響を防ぐ.	HW	v1, v2, v5	Gonzalez et al U. C. Berkeley, 2018
SafeSpec				Khasawneh et al arXiv, Jun. 15, 2018
InvisiSpec				M. Yan, J. Choi et al IEEE, Oct. 2018
SSE-RV	投機的実行にてロードされたデータに伴い, 行き先レジスタに痕跡 (taint) を付ける. 次の投機的実行は, もしそのレジスタで保存されている痕跡付き (tainted) の番地を再度使うと , LSU からメモリ保護用 fence 命令でブロックされる.	HW	v1, v2, v5	M. Sabbagh et al CARRV 2021