

# 投機的実行機能を持つ CPU に対するサイドチャネル攻撃について (SSB,RSRE)

2018年5月21日にIntel社より以下の脆弱性(SSB,RSRE)が公表されました。

INTEL-SA-00115

<https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00115.html>

## 1. 製品の該非情報、対策情報

今回の脆弱性について、影響を受ける製品は以下の通りです。

### 1-1 統合サービスプラットフォーム BladeSymphony

#	装置	サーバブレード種類	モデル	影響	UEFI(BIOS)対策	Virtage HVM F/W 対策	
1	BS1000	Xeon	x1~x4	なし	—	—	
2		Xeon MP	x2	なし	—	—	
3	BS320	X86	x1~x3	なし	—	—	
4		標準 HDD 拡張 SAN 専用 PCI 拡張	x4	あり	(保守期限終了)	—	
5			x5	あり	調整中	調整中	
6			x6	あり	調整中	(対象外)	
7	BS2000	標準	x1	あり	2019/1/25 リリース [01-67/03-60]*3	2019/2/22 リリース <a href="#">[Ver.59-84]</a> 適用後に*1 要	
8			x2	あり	2019/1/25 リリース [03-60]*3	2019/2/22 リリース <a href="#">[Ver.59-84]</a> 適用後に*1 要	
9			x3	あり	2018/7/27 リリース [09-64]*3	2018/8/24 リリース <a href="#">[Ver.59-83]</a> 適用後に*1 要	
10			x4	あり	2018/7/27 リリース [11-56]*3	2018/8/24 リリース <a href="#">[Ver.59-83]</a> 適用後に*1 要	
11		高性能	x1	あり	2019/1/25 リリース [03-37]*3	2019/1/25 リリース <a href="#">[Ver.79-84]</a> 適用後に*1 要	
12			x2	あり	2018/9/28 リリース [07-74]*3	2018/12/21 リリース <a href="#">[Ver.79-84]</a> 適用後に*1 要	
13	BS500	BS520A	x1	あり	2018/7/27 リリース <a href="#">[Ver.02-68]</a>	2018/8/31 リリース <a href="#">[Ver.02-63]</a> 適用後に*1 要	
14			BS520H	x1	あり	2018/7/27 リリース <a href="#">[Ver.05-12]</a>	2018/8/31 リリース <a href="#">[Ver.02-63]</a> 適用後に*1 要
15				x2	あり	2018/7/27 リリース <a href="#">[Ver.04-55]</a>	2018/8/31 リリース <a href="#">[Ver.02-63]</a> 適用後に*1 要
16				x3	あり	2018/7/6 リリース <a href="#">[Ver.08-93]</a>	2018/7/13 リリース <a href="#">[Ver.02-63]</a> 適用後に*1 要
17		x4	あり	2018/7/6 リリース <a href="#">[Ver.10-24]</a>	2018/7/6 リリース <a href="#">[Ver.02-63]</a> 適用後に*1 要		
18		BS540A	x1	あり	2018/7/27 リリース <a href="#">[Ver.03-44]</a>	2018/8/31 リリース <a href="#">[Ver.02-63]</a> 適用後に*1 要	
19		BS520X	x1	あり	2018/7/27 リリース <a href="#">[Ver.07-72]</a>	2018/8/31 リリース <a href="#">[Ver.02-63]</a> 適用後に*1 要	
20			x2	あり	2018/7/6 リリース <a href="#">[Ver.09-61]</a>	2018/7/13 リリース <a href="#">[Ver.02-63]</a> 適用後に*1 要	
21			BS2500	標準	x1	あり	2018/7/6 リリース <a href="#">[Ver.08-93]</a>
22		x2			あり	2018/7/6 リリース <a href="#">[Ver.10-24]</a>	2018/7/6 リリース <a href="#">[Ver.02-63]</a> 適用後に*1 要
23	高性能	x1		あり	2018/7/27 リリース <a href="#">[Ver.07-72]</a>	2018/8/31 リリース <a href="#">[Ver.02-63]</a> 適用後に*1 要	
24		x2		あり	2018/7/6 リリース <a href="#">[Ver.09-61]</a>	2018/7/13 リリース <a href="#">[Ver.02-63]</a> 適用後に*1 要	
25		x3		あり	2018/7/6 リリース <a href="#">[Ver.11-21]</a>	2018/7/6 リリース <a href="#">[Ver.02-63]</a> 適用後に*1 要	

## 1-2 日立アドバンスサーバ HA8500 シリーズ

#	装置	モデル	影響	F/W 対策
1	HA8500	F8, F7, E6, D5	なし	—

## 1-3 日立アドバンスサーバ HA8000 シリーズ

#	装置	モデル	影響	UEFI(BIOS)対策
1	HA8000	RS110xJ, TS10xJ, RS220xJ, RS210xJ, TS20xJ, RS440xK, RS110xK, TS10xK, SS10xK, RS220xK, RS210xK, TS20xK, RS440xK1, RS110xK1, TS10xK1, SS10xK1	あり	(保守期限終了)
2		RS220xK1, RS210xK1, TS20xK1	あり	2019/4/5 リリース [ Ver F15]
3		RS110xL, TS10xL, SS10xL, NS110xL, NS10xL, NS10sxL	あり	2019/1/25 リリース [ Ver 1.09]
4		RS440xL	あり	2019/2/8 リリース [ Ver 0041]
5		RS220xL, RS210xL, TS20xL, NS220xL	あり	2019/4/5 リリース [ Ver F15]
6		RS440xL1	あり	2019/2/8 リリース [ Ver 0041]
7		RS110xL1, TS10xL1, SS10xL1, NS110xL1, NS10xL1, NS10sxL1	あり	2019/1/25 リリース [ Ver 1.09]
8		RS440xL2	あり	2019/2/8 リリース [ Ver 0041]
9		RS110xL2, TS10xL2, NS110xL2, NS10xL2, SS10xL2, NS10sxL2	あり	2019/1/25 リリース [ Ver LU.1.03.00]
10		RS440xM	あり	2018/12/7 リリース [ Ver 5.6.0171]
11		RS110xM, TS10xM, NS110xM, NS10xM	あり	2019/1/25 リリース [ Ver M1.1.08.00]
12		RS220-hxM, RS210-hxM	あり	2018/11/30 リリース [ Ver MH.1.08]
13		RS220xM, RS220-sxM, RS210xM, TS20xM, RS110-hxM, TS10-hxM, NS220xM, NS220-sxM	あり	2018/11/30 リリース [ Ver M2.1.08]
14		RS110xM1, TS10xM1, NS110xM1, NS10xM1	あり	2019/1/25 リリース [ Ver MD.1.05.00]
15		RS220-hxM1, RS210-hxM1	あり	2018/11/30 リリース [ Ver MH.1.08]
16		RS220xM1, RS220-sxM1, RS210xM1, TS20xM1, RS110-hxM1, TS10-hxM1, NS220xM1, NS220-sxM1	あり	2018/11/30 リリース [ Ver M2.1.08]
17		RS220-hxM2, RS210-hxM2	あり	2019/1/25 リリース [ Ver MA.1.08.00]
18		RS220xM2, RS220-sxM2, RS210xM2, TS20xM2, RS110-hxM2, TS10-hxM2, NS220xM2, NS220-sxM2	あり	2019/1/25 リリース [ Ver MB.1.08.00]
19		RS440xN	あり	2018/12/7 リリース [ Ver 5.6.0273]
20		RS220xN, RS210xN	あり	2018/11/30 リリース [ Ver 5.0.E034]
21		TS20xN	あり	2019/1/25 リリース [ Ver 5.0.8013]
22		RS110xN, TS10xN, NS10xN, NS110xN	あり	2018/11/30 リリース [ Ver 5.0.9017]
23		RS440xN1	あり	2018/12/7 リリース [ Ver 5.6.0383]
24		RS220xN1, RS210xN1, NS220xN1	あり	2018/11/30 リリース [ Ver 5.0.E034]
25		RS110xN1, TS10xN1, NS10xN1, NS110xN1	あり	2018/10/26 リリース [ 5.0.4008]
26		RS220xN2, RS210xN2, NS220xN2	あり	2018/11/30 リリース [ Ver 5.0.8023]
27		TS20xN2	あり	2018/11/30 リリース [ Ver 5.0.5010]
28		上記モデル以外 (RS440xJ を含みます)	なし	—

#### 1-4 日立アドバンストサーバ HA8000V シリーズ

#	装置	モデル	影響	UEFI(BIOS)対策
1	HA8000V	DL380, DL360, DL580, ML350	あり	2018/7/13 リリース <a href="#">[Ver.1.42]</a>

#### 1-5 高信頼サーバ RV3000

#	装置	モデル	影響			ハードウェア対策
			CVE-2018-3615	CVE-2018-3620	CVE-2018-3646	UEFI(BIOS)
1	RV3000	A1	なし	なし※	なし※	※初回出荷から対策済み

#### 1-6 エンタープライズサーバ EP8000

#	装置	モデル	CPU	影響	F/W 対策 *3
1	EP8000	S914, S924	POWER9	あり	※初回出荷から対策済み
2		S814, S824, E850	POWER8	あり	2018/11/22 リリース [SV860_165]
3		E870, E880	POWER8	あり	2018/11/22 リリース [SC860_165]
4		720(E4D), 740(E6D)	POWER7+	あり	2018/11/22 リリース [AL770_126]
5		770(MMD), 780(MHD)	POWER7+	あり	2018/11/22 リリース [AM780_100]
6		710(E2B), 720(E4B), 740(E6B)	POWER7	あり	2018/11/22 リリース [AL730_159]
7		720(E4C), 740(E6C)	POWER7	あり	2018/11/22 リリース [AL740_167]
8		750(E8B)	POWER7	あり	2018/12/22 リリース [AL730_160]
9		770(MMC), 780(MHC)	POWER7	あり	2018/11/22 リリース [AL770_126]
10		770(MMB), 780(MHB)	POWER7	あり	2018/11/22 リリース [AM780_100]
11		-	POWER6 POWER5 POWER4 POWER3	POWER6、POWER5、POWER4、POWER3 については個別にお問合せください。	

#### 1-7 スーパーテクニカルサーバ SR24000

#	装置	モデル	CPU	影響	F/W 対策 *3
1	SR24000	XP1, XP2	POWER8	あり	2018/11/22 リリース [SV860_165]

#### 1-8 ディープラーニングシステム SR24000

#	装置	モデル	CPU	影響	F/W 対策
1	SR24000	DL1	POWER9 POWER8	あり	OS パッチのみで、 F/W 更新は不要です

## 1-9 サーバ・クライアント関連製品

#	装置	モデル	影響	UEFI(BIOS)対策
1	HA8000-bd シリーズ	x2	あり	サポート窓口から提供*4
2		x3	なし	—
3	FLORA bd500 シリーズ	x7	なし	—
4		x9	あり	サポート窓口から提供*4
5	セキュリティ PC(SPC) FLORA Se210/Se330	全モデル	あり*2	不要 (Windows OS の対応が必要です。 適用手順は管理者ガイドを参照ください。)

### 【注記】

\*1: UEFI(BIOS)およびHVM F/Wを対策バージョンにアップデート後に下記に示す対処を実施してください。

1. HVM管理コマンド(HvmSh)を用いて下記を実施する。
  - i. set LparSSBD コマンドを使用して、SSBD(Speculative Store Bypass Disable)機能をLPARで利用できるようにする。
  - ii. set LparCpuFeatures コマンドを使用して、他のCPU拡張機能もLPARで利用できるようにする。
2. HVM の構成情報を保存する。

\*2: CVE-2018-3640の影響はありませんが、CVE-2018-3639の影響があります。

\*3: お客様装置への適用につきましては、準備が整いしだい保守員から連絡さしあげます。

\*4: サポート窓口から対策版を提供させていただきますので、各製品のサポート窓口にお問合せください。  
ただし、ご提供までにお時間を頂く場合がございます。

## 1-10 その他サーバ・周辺機器製品

以下のサーバ・周辺機器製品については、影響がありません。

- ・日立アドバンスサーバ HA8500(F8,F7,E6,D5)
- ・エンタープライズサーバ AP7000 の全モデル
- ・エンタープライズサーバ AP8000/AP8800 シリーズの全モデル
- ・エントリークラスディスクアレイ装置 BR1200, BR1250 の全モデル
- ・LAN スイッチ装置 LANSW の全モデル
- ・DCB スイッチ装置 DCBSW の全モデル
- ・FibreChannel スイッチ装置 FCSW の全モデル
- ・SVP の全モデル
- ・コンソール切替ユニットの全モデル
- ・UPS の全モデル
- ・テープライブラリ装置 LTO
- ・統合データ保護システム DMV(Data Mover for Volume)
- ・システム運転支援装置(CSC)(2形,3形)
- ・H-634A 入出力制御装置 SGW(SCSI Gateway 装置)(30D,30DF,30E,30EX)
- ・H-6355FEP-4V サーバ(E2,E3,E4,E4 エンハンス)
- ・プリンタ製品

## 1-11 ストレージ製品

以下のストレージ製品については、影響がありません。

- ・Hitachi Universal Storage Platform
- ・Hitachi Universal Storage Platform V/VM
- ・Hitachi Universal Storage Platform H12000/H20000/H24000
- ・Hitachi Virtual Storage Platform
- ・Hitachi Virtual Storage Platform G100,G200,G400,G600,G800,F400,F600,F800
- ・Hitachi Virtual Storage Platform F350,F370,F700,F900,G130,G150,G350,G370,G700,G900
- ・Hitachi Virtual Storage Platform G1000,G1500,F1500
- ・Hitachi Virtual Storage Platform VP9500
- ・Hitachi Virtual Storage Platform VX7
- ・Hitachi Network storage Controller
- ・Hitachi Network storage Controller H10000
- ・Hitachi Unified Storage VM
- ・Hitachi Unified Storage 100 シリーズ
- ・Adaptable Modular Storage 2000 シリーズ
- ・BR1600/BR1650 シリーズ
- ・Hitachi Virtual File Platform
- ・Hitachi Data Ingestor
- ・Hitachi NAS Platform
- ・Hitachi Content Platform
- ・Hitachi Content Platform Anywhere
- ・Hitachi Capacity Optimization
- ・ファイバチャネルスイッチ(HT-4990-SWxxxx)
- ・バックアップストレージ(TFxxxx)

## 1-12 影響調整中の製品

以下の製品については、影響有無を調整中です。

- ・ロードバランサの全モデル

## 2. 関連情報

HP 社製 PC <https://support.hp.com/jp-ja/document/c06001809>

## 3. 本件に関する問い合わせ窓口

各製品サポート窓口にお問合せください。

## 4. 更新履歴

**2019年4月5日: HA8000の対策情報を更新しました。**

2019年2月28日: BladeSymphony, HA8000の対策情報を更新しました。

2019年2月15日: HA8000の対策情報を更新しました。

2019年1月31日: BladeSymphony, HA8000の対策情報を更新しました。

2018年12月25日: BS2000, HA8000, EP8000の対策情報を更新しました。

2018年12月7日: HA8000の対策情報を更新しました。

2018年11月30日: BS2000, HA8000, EP8000, SR24000の対策情報を更新しました。

2018年10月26日: BS2000, HA8000, EP8000, SR24000, SR16000の対策情報を更新しました。

2018年10月5日: RV3000の影響情報を追加しました。

2018年9月28日: BS2000の対策情報を更新しました。

2018年8月31日: BS500, BS2500のVirtage対策版をリリースしました。EP8000, SR24000, SR16000の対策日程を延期しました。

2018年8月24日: BS2000(Virtage)のリリース日を更新しました。

BladeSymphony, HA8000の対策計画見直しのため調整中としました。

2018年8月2日: EP8000, SR24000の対策版提供を延期しました。

2018年7月31日: BS2000(Virtage), EP8000のリリース日を更新しました。サポート窓口からの提供を追記しました。

2018年7月27日: BS2000, BS500, BS2500のリリース日を更新しました。

2018年7月13日: BS500, BS2500, HA8000V, EP8000, SR24000, SR16000のリリース日を更新しました。

2018年7月6日: BS500, BS2500の一部対策版リリース日を更新しました。HA8000, HA8000Vの一部対策予定を更新しました。

項番1-8にSPCの影響を追記しました。

2018年6月26日: BS500, BS2500, HA8000Vの対策版リリース予定日を更新しました。

2018年6月12日: 項番1-1にVirtage HVM F/W対策予定を追記しました。

項番1-5にPOWER9、および対策予定を追記しました。項番1-7にPOWER9を追記しました。

2018年6月5日: 項番1「対応方法」を「UEFI(BIOS)対策」に表記を変更し、一部対策予定日を記載しました。

項番1-10 Hitachi Virtual Storage Platformのモデルを追記しました。

項番2 HP社製PCの情報を英語サイトから日本語サイトに変更しました。

2018年5月29日: 周辺機器の影響情報を更新しました。

2018年5月23日: EP8000, SR24000, SR16000, HA8500, AP7000, AP8000, AP8800の影響情報を更新しました。

2018年5月22日: このセキュリティ情報ページを新規作成および発信しました。

- ・弊社では、セキュリティ対応に関して正確な情報を提供するよう努力しておりますが、セキュリティ問題に関する情報は変化しており、当ホームページで記載している内容を予告なく変更することがありますので、あらかじめご了承ください。情報ご参照の際には、常に最新の情報をご確認いただくようお願いいたします。
- ・当ホームページに記載されている製品には、他社開発製品が含まれております。これらのセキュリティ情報については他社から提供、または公開された情報を基にしております。弊社では、情報の正確性および完全性について注意を払っておりますが、開発元の状況変化に伴い、当ホームページの記載内容に変更が生じることがあります。
- ・当ホームページはセキュリティ情報の提供を目的としたものであり、法律上の責任を負うものではありません。お客様が独自に行なった(あるいは行なわなかった)セキュリティ対応その他のご行為の結果につきまして、弊社では責任を負いかねます。
- ・当ホームページから他サイトのページへのリンクアドレスは情報発信時のものです。他サイトでの変更などを発見した場合には、リンク切れ等にならないよう努力はいたしますが、永続的にリンク先を保証するものではありません。
- ・記載の会社名、製品名などは、それぞれの会社の商標もしくは登録商標です。