

# PCサーバ・クライアント製品 「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

投機的実行機能を持つ CPU に対してサイドチャネル攻撃を行う手法が複数の研究者によって報告されています。

[JVNVU#93823979(CVE-2017-5715、CVE-2017-5753、CVE-2017-5754)]

## 1. 脆弱性の対策について

各脆弱性に対するUEFI(BIOS)、仮想化機構、OS対策版の適用の要／不要は以下の通りです。

「表1. 脆弱性の対策」の太枠で示した部分の対応方法を「2. 製品の該非情報、対応方法」に示します。

表1. 脆弱性の対策

CVE	脆弱性	UEFI(BIOS) 対策版適用 *3	Virtage HVM F/W 対策版適用	VMware vSphere ESXi対策版適用	Red Hat Enterprise Linux対策版適用	Windows Server / Client対策版適用
2017-5715	Spectre	要	要*2	要*2	要*1 (入手可能)*4	要*1 (入手可能)
2017-5753		不要	不要			
2017-5754	Meltdown	不要	不要	不要	要*1 (入手可能)*4	要*1 (入手可能)

\*1 ベアメタル環境、KVMホスト環境/Hyper-Vホスト環境、仮想ゲストOS環境(ハイパーバイザに依存しない)何れの場合も適用が必要です。

\*2 使用している場合は適用が必要です。

\*3 Intel社公開情報に基づくものです ([https://s21.q4cdn.com/600692695/files/doc\\_presentations/2018/Side-Channel-Analysis-Security.pdf](https://s21.q4cdn.com/600692695/files/doc_presentations/2018/Side-Channel-Analysis-Security.pdf))

\*4 対策版の提供に関してはサポートサービス窓口にお問合せください。

## 2. 製品の該非情報、対応方法

CVE-2017-5715脆弱性によるPCサーバ・クライアント製品への影響は以下の通りです。対策バージョンをクリックするとダウンロードサイトにリンクします。

なお、VMware vSphere ESXi、Red Hat Enterprise Linux、Windows Server / Clientの対応方法はソフトウェア製品の「[投機的実行機能を持つ CPU に対するサイドチャネル攻撃](#)」についてをご確認ください。

### 統合サービスプラットフォーム BladeSymphony (1/2)

#	装置	サーバブレード種類	モデル	影響	UEFI(BIOS)対策版		Virtage HVM F/W 対策版	
					適用	対策バージョン	適用	対策バージョン
1	BS1000	Xeon	x1~x4	なし	—	—	—	—
2		Xeon MP	x2	なし	—	—	—	—
3	BS320	X86	x1~x3	なし	—	—	—	—
4		標準	x4	あり	(保守期限終了)	—	(保守期限終了)	—
5		HDD 拡張 SAN 専用 PCI 拡張	x5	あり	要 *3 3/30 リリース	G29 *3	要 4/27 リリース 適用後に*4 実施要 (PCI 拡張サーバブレードのみ対象)	<a href="#">17-95</a>
6			x6	あり	要 *3 3/16 リリース	F11 *3	(対象外)	—
7	BS2000	標準	x1	あり	要 *3 3/30 リリース	01-66/02-66 *3 03-59/04-59 *3	要 4/13 リリース 適用後に*4 実施要	<a href="#">59-82</a>
8			x2	あり	要 *3 3/30 リリース	03-59/04-59 *3		
9			x3	あり	要 *3 3/16 リリース	09-63/10-63 *3		
10			x4	あり	要 *3 3/16 リリース	11-55/12-55 *3		
11		高性能	x1	あり	要 *3 3/30 リリース	03-35/04-35 *3	要 4/27 リリース 適用後に*4 実施要	<a href="#">79-82</a>
12		x2	あり	要 *3 3/30 リリース	07-73/08-73 *3			

## 統合サービスプラットフォーム BladeSymphony (2/2)

#	装置	サーバブレード種類	モデル	影響	UEFI(BIOS)対策版		Virtage HVM F/W 対策版				
					適用	対策バージョン	適用	対策バージョン			
13	BS500	BS520A	x1	あり	要 3/16 リリース	<a href="#">02-66</a>	要 3/30 リリース 適用後に*4 実施要	<a href="#">02-62</a>			
14			x1	あり	要 3/16 リリース	<a href="#">05-10</a>					
15			x2	あり	要 3/16 リリース	<a href="#">04-53</a>					
16			x3	あり	要 3/9 リリース	<a href="#">08-90</a>					
17			x4	あり	要 3/9 リリース	<a href="#">10-20</a>					
18		BS540A	x1	あり	要 3/16 リリース	<a href="#">03-42</a>					
19		BS520X	x1	あり	要 3/16 リリース	<a href="#">07-70</a>					
20			x2	あり	要 3/16 リリース	<a href="#">09-59</a>					
21		BS2500	標準	x1	あり	要 3/9 リリース			<a href="#">08-90</a>	要 3/30 リリース 適用後に*4 実施要	<a href="#">02-62</a>
22				x2	あり	要 3/9 リリース			<a href="#">10-20</a>		
23	高性能		x1	あり	要 3/16 リリース	<a href="#">07-70</a>					
24			x2	あり	要 3/16 リリース	<a href="#">09-59</a>					
25			x3	あり	要 3/16 リリース	<a href="#">11-18</a>					

BS320/BS2000/BS500 では、対策版リリース以降はサーバブレード保守交換時に対策版 UEFI(BIOS)が適用されます。

## 日立アドバンスサーバ HA8000V シリーズ

#	装置	モデル	影響	UEFI(BIOS) 対策版適用	UEFI(BIOS) 対策バージョン
1	HA8000V	DL380, DL360, DL580, ML350	あり	要 2/28 リリース	<a href="#">1.32</a>

対策版リリース以降は、マザーボード保守交換時に対策版 UEFI(BIOS)が適用されます。

プレインストールモデルについて、対策版 Windows セキュリティ更新プログラムの適用は 2018 年 6 月頃の予定です。

日立アドバンスサーバ HA8000 シリーズ (1/2)

#	装置	モデル	影響	UEFI(BIOS) 対策版適用	UEFI(BIOS) 対策バージョン
1	HA8000	RS110xJ, TS10xJ	あり	(保守期限終了)	—
2		RS220xJ, RS210xJ, TS20xJ	あり	要 4/16 リリース	<a href="#">F14</a>
3		RS110xK, TS10xK, SS10xK	あり	(保守期限終了)	—
4		RS440xK	あり	要 4/20 リリース	<a href="#">0040</a>
5		RS220xK, RS210xK, TS20xK	あり	要 4/16 リリース	<a href="#">F14</a>
6		SS10xK1	あり	(保守期限終了)	—
7		RS440xK1	あり	要 4/20 リリース	<a href="#">0040</a>
8		RS220xK1, RS210xK1, TS20xK1	あり	要 4/16 リリース	<a href="#">F14</a>
9		RS110xK1, TS10xK1	あり	要 4/16 リリース	<a href="#">F7</a>
10		RS110xL, TS10xL, SS10xL, NS110xL, NS10xL, NS10sxL	あり	要 3/23 リリース	<a href="#">1.08</a>
11		RS440xL	あり	要 4/20 リリース	<a href="#">0040</a>
12		RS220xL, RS210xL, TS20xL, NS220xL	あり	要 4/16 リリース	<a href="#">F14</a>
13		RS440xL1	あり	要 4/20 リリース	<a href="#">0040</a>
14		RS110xL1, TS10xL1, SS10xL1, NS110xL1, NS10xL1, NS10sxL1	あり	要 3/23 リリース	<a href="#">1.08</a>
15		RS440xL2	あり	要 4/20 リリース	<a href="#">0040</a>
16		RS110xL2, TS10xL2, NS110xL2, NS10xL2, SS10xL2, NS10sxL2	あり	要 3/23 リリース	<a href="#">LU.1.02</a>
17		RS440xM	あり	要 5/23 リリース	<a href="#">5.6.0170</a>
18		RS110xM, TS10xM, NS110xM, NS10xM	あり	要 3/9 リリース	<a href="#">M1.1.07.00</a>
19		RS220-hxM, RS210-hxM	あり	要 3/23 リリース	<a href="#">MH.1.07</a>
20		RS220xM, RS220-sxM, RS210xM, TS20xM, RS110-hxM, TS10-hxM, NS220xM, NS220-sxM	あり	要 3/23 リリース	<a href="#">M2.1.07</a>
21		RS110xM1, TS10xM1, NS110xM1, NS10xM1	あり	要 3/9 リリース	<a href="#">MD.1.04.00</a>
22		RS220-hxM1, RS210-hxM1	あり	要 3/23 リリース	<a href="#">MH.1.07</a>
23		RS220xM1, RS220-sxM1, RS210xM1, TS20xM1, RS110-hxM1, TS10-hxM1, NS220xM1, NS220-sxM1	あり	要 3/23 リリース	<a href="#">M2.1.07</a>
24		RS220-hxM2, RS210-hxM2	あり	要 3/23 リリース	<a href="#">MA.1.07</a>
25		RS220xM2, RS220-sxM2, RS210xM2, TS20xM2, RS110-hxM2, TS10-hxM2, NS220xM2, NS220-sxM2	あり	要 3/23 リリース	<a href="#">MB.1.07</a>
26		RS440xN	あり	要 5/23 リリース	<a href="#">5.6.0272</a>
27		RS220xN, RS210xN	あり	要 4/16 リリース	<a href="#">5.0.D032</a>
28		TS20xN	あり	要 5/11 リリース	<a href="#">5.0.7012</a>
29		RS110xN, TS10xN, NS10xN, NS110xN	あり	要 5/18 リリース	<a href="#">5.0.8016</a>

## 日立アドバンスサーバ HA8000 シリーズ (2/2)

#	装置	モデル	影響	UEFI(BIOS) 対策版適用	UEFI(BIOS) 対策バージョン
30	HA8000	RS440xN1	あり	要 5/23 リリース	<a href="#">5.6.0382</a>
31		RS220xN1, RS210xN1, NS220xN1	あり	要 4/16 リリース	<a href="#">5.0.D032</a>
32		RS110xN1, TS10xN1, NS10xN1, NS110xN1	あり	要 5/18 リリース	<a href="#">5.0.3006</a>
33		RS220xN2, RS210xN2, NS220xN2	あり	要 4/27 リリース	<a href="#">5.0.7021</a>
34		TS20xN2	あり	要 5/25 リリース	<a href="#">5.0.4009</a>
35		上記モデル以外 (RS440xJ を含みます)	なし	—	—

対策版リリース以降は、保守交換時に対策版 UEFI(BIOS)が適用される場合があります。

## その他サーバ・クライアント関連製品

#	装置	モデル	影響	UEFI(BIOS) 対策版適用	UEFI(BIOS) 対策バージョン	備考
1	HA8000-bd シリーズ	x1	あり	(保守期限終了)	—	装置形名により UEFI が異なります。ダウンロードサイトからご利用の装置形名に合った UEFI アップデートツールを選択してください。
2		x2	あり	要 5/11 リリース	<a href="#">1000.023W</a> <a href="#">1000.023</a> <a href="#">6000.011</a> <a href="#">2000.006W</a> <a href="#">2000.006</a> <a href="#">5000.011</a>	
3		x3	あり	要 5/11 リリース	<a href="#">P1.10</a> <a href="#">P2.10</a>	
4	FLORA bd500 シリーズ**	x9	あり	要 5/11 リリース	<a href="#">3000.007W</a> <a href="#">3000.007</a>	Windows OS の対応が必要です。 *1 手順は管理者ガイドを参照ください。
5	セキュリティ PC(SPC) FLORA Se210/Se330	全モデル	あり	不要	—	
6	テープライブラリ装置 LTO	全モデル	なし	—	—	HA8000 OS の対応が必要です。  *1,*2
7	統合データ保護システム DMV(Data Mover for Volume)	全モデル	なし	—	—	

対策版リリース以降は、マザーボード保守交換時に対策版 UEFI(BIOS)が適用されます。

\*\* : 表記以外のモデルについては個別にお問合せください。

## 【注記】

Intel-SA-00088の情報に基づいた見解です。Intel社からの情報更新があった場合、随時アップデートを行う予定です。

\*1: Windows Server / Clientの対応方法はソフトウェア製品の「投機的実行機能を持つ CPU に対するサイドチャネル攻撃」についてをご確認ください。

\*2: LTO装置およびDMVは影響ありませんが、アプリケーションが動作するOSの対応は必要です。

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

\*4: 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 LparIBRS コマンドを使用して、IBRS(Indirect Branch Restricted Speculation)およびIBPB(Indirect Branch Predictor Barrier)機能をLPARで利用できるようにする。
  - ii. set LparPCID コマンドを使用して、PCID(Process Context ID)機能をLPARで利用できるようにする。  
※本手順が不要な構成ではエラーコード 0x10080001 または 0x1008002 が表示されます。
2. HVMの構成情報を保存する。

以下の機種については、影響を受けないため、UEFI(BIOS)対策適用は不要です。

- ・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
- ・ロードバランサの全モデル
- ・UPS の全モデル

### **3. 対策版適用による性能への影響**

Intel社の下記サイト(英文)にて、対策版マイクロコード適用による性能影響の記載があります。

<https://newsroom.intel.com/news/firmware-updates-and-initial-performance-data-for-data-center-systems/>

### **4. 関連情報**

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5715>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5753>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5754>

<https://jvn.jp/vu/JVNVU93823979>

HP 社製 PC <https://support.hp.com/jp-ja/document/c05872418>

### **5. 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。

## 6. 更新履歴

2018年5月25日: HA8000のリリース日程を更新しました。

2018年5月23日: HA8000Vのプレインストールモデル対応、およびHA8000のリリース日程を更新しました。

2018年5月18日: HA8000のリリース日程を更新しました。

2018年5月11日: HA8000, HA8000-bd, FLORA bd500のリリース日程を更新しました。

2018年4月27日: Virtage HVM F/W, HA8000, HA8000-bd, FLORA bd500のリリース日程を更新しました。

2018年4月23日: HA8000のリリース日程を更新しました。

2018年4月20日: HA8000-bd, FLORA bd500のリリース予定日を更新しました。FLORA bd500に注記を追加しました。

2018年4月16日: HA8000のリリース日を更新しました。

2018年4月13日: BS2000(Virtage)のリリース日を更新しました。

2018年4月6日: HA8000, HA8000-bdのリリース予定を更新しました。注記\*3の記載を変更しました。

2018年3月30日: BladeSymphony, HA8000, HA8000-bd, FLORA bd500のリリース日、リリース予定を更新しました。注記\*4を追加しました。

2018年3月23日: BladeSymphony, HA8000, HA8000-bdのリリース日、リリース予定を更新しました。

2018年3月16日: BladeSymphony, HA8000, HA8000-bdのリリース日、リリース予定を更新しました。

2018年3月9日: BladeSymphony, HA8000のリリース日、リリース予定を更新しました。

2018年3月2日: BladeSymphony, HA8000のリリース予定を更新しました。

2018年2月28日: 2. 製品の該非情報、対応方法の表フォーマット変更し、HA8000V, HA8000リリース日程を更新しました。

2018年2月23日: 表1. 脆弱性の対策の対応状況表記を変更し\*4を追加、HA8000Vのリリース日程を更新しました。

2018年2月16日: 表1. 脆弱性の対策に適用可否の情報を追記しました。

2018年2月6日: 1. 脆弱性の対策についてを追加、2. 製品の該非情報、対応方法のフォーマットを変更しました。

FLORA Se210/Se330, LTO, DMVのOS対応方法の詳細を追加しました。

2018年1月26日: BS320iにHDD拡張サーバブレード, SAN専用サーバブレード, PCI拡張サーバブレードを追記しました。

2018年1月24日: FLORA Se210/Se330の影響情報を更新しました。

関連情報のHP社製PCリンク先を日本語サイトに変更しました。

2018年1月18日: BS500/BS2500, HA8000のUEFI(BIOS)リリース日程を調整中に変更しました。

HA8000 N1モデルに2モデル(NS10xN1, NS110xN1)を追加しました。

その他サーバ・クライアント関連機器にDMVを追加しました。

対策版適用による性能への影響の情報を追加しました。

2018年1月16日: HVM F/W, HA8000リリース日程、およびその他4製品の影響情報を更新しました。

2018年1月12日: BS500/BS2500のUEFI(BIOS)リリース日程、および保守期限終了への対応を追記しました。

その他サーバ・クライアント関連機器に装置を追加しました。

2018年1月11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でき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。