

# サーバ・ホスト製品 「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

各脆弱性に対するファームウェア(F/W)、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	F/W 対策版適用*2	Virtual I/O Server 対策版適用	AIX 対策版適用
2017-5715	Spectre	要*1	不要	不要
2017-5753			要(入手可能)	要(入手可能)
2017-5754	Meltdown		要(入手可能)	要(入手可能)

\*1 ハードウェア管理コンソール(HWMC)が接続されている場合は、ファームウェア更新の前提として、HWMCコードの更新が必要となる場合があります。

\*2 IBM社公開情報に基づくものです (<https://www.ibm.com/blogs/psirt/potential-impact-processors-power-family/>)

## 2. 製品の該非情報、対応方法

当該脆弱性によるサーバ・ホスト製品への影響は以下の通りです。

なお、Virtual I/O Server、AIX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。

### エンタープライズサーバ EP8000 (1/2)

EP8000 の F/W、Virtual I/O Server 対策版及び AIX 対策版の全ての適用が必要です。

#	装置	モデル	CPU	影響	F/W 対策適用	F/W 対策バージョン	備考
1	EP8000	S814	POWER8	あり	要 *1 2/16 リリース	SV860_138	
2		S824	POWER8	あり		SV860_138	
3		E850	POWER8	あり		SV860_138	
4		E870	POWER8	あり		SC860_138	
5		E880	POWER8	あり		SC860_138	
6		720	POWER7+	あり	要 *1 3/23 リリース	AL770_122	E4D
7		740	POWER7+	あり		AL770_122	E6D
8		770	POWER7+	あり		AM780_096	MMD
9		780	POWER7+	あり		AM780_096	MHD
10		710	POWER7	あり	要 *1 3/23 リリース	AL730_157	E2B
11		720	POWER7	あり		AL730_157	E4B
						AL740_165	E4C
12		740	POWER7	あり		AL730_157	E6B
						AL740_165	E6C
13	750	POWER7	あり	AL730_157		E8B	
14	770	POWER7	あり	AM780_096		MMB	
				AM770_122	MMC		

## エンタープライズサーバ EP8000 (2/2)

EP8000 の F/W、Virtual I/O Server 対策版及び AIX 対策版の全ての適用が必要です。

#	装置	モデル	CPU	影響	F/W 対策適用	F/W 対策バージョン	備考
15	EP8000	780	POWER7	あり	要 *1 3/23 リリース	AM780_096	MHB
						AM770_122	MHC
16		795	POWER7	あり		AH780_096	FHB
17		-	POWER6 POWER5 POWER4	POWER6、POWER5、POWER4 については個別にお問合せください。			

## スーパーテクニカルサーバ SR24000/SR16000

SR24000/SR16000 の F/W 及び AIX 対策版の両方の適用が必要です。

#	装置	モデル	CPU	影響	F/W 対策適用	F/W 対策バージョン	備考
1	SR24000	XP1	POWER8	あり	要 *1 2/23 リリース	SV860_138	
2		XP2	POWER8	あり		SV860_138	
3	SR16000	M1	POWER7	あり	要 *1 3/23 リリース	AL730_157	
4		XM1	POWER7	あり		AL730_157	
5		VM1	POWER7	あり		AL730_157	

## ディープラーニングシステム SR24000

#	装置	モデル	CPU	影響	F/W 対策適用	F/W 対策バージョン	備考
1	SR24000	DL1	POWER8	あり	要 *1 2/23 リリース	OP820.21	

### 【注記】:

\*1:お客様装置への適用作業につきましては、サポートサービス窓口までご連絡をお願い致します。

### その他のサーバ・ホスト製品

以下の機種は、影響を受けないため、F/Wの対策適用は不要です。

- ・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
- ・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-6355 FEP-4V サーバ(E2,E3,E4,E4 エンハンス)

### 3. 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>

### 4. 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。

## 5. 更新履歴

2018年4月20日:EP8000 POWER6,5,4 モデルの対応について追記しました。

2018年3月23日:EP8000,SR16000 のリリース日程を更新し、対策バージョンを追記しました。

2018年2月28日:EP8000 に注記を追加しました。

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ました。

SR24000(XP1,XP2,DL1) F/W リリース日程を更新し、対策バージョンを追記しました。

2018年2月16日:EP8000 F/W リリース日程を更新し、F/W 対策バージョンを追記しました。

2018年2月8日:2. 製品の該非情報、対応方法 EP8000/SR24000/SR16000 F/W リリース日程を更新しました。

2018年2月7日:2. 製品の該非情報、対応方法[その他のサーバ・ホスト製品]に対する OS 対応方法の誤記削除しました。

2018年2月6日:1. 脆弱性の対策についてを追記。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。

2018年1月31日:EP8000 の対応情報を更新しました。

2018年1月23日:CSC の影響情報を更新しました。

2018年1月19日:AP8000/AP8800,SGW,FEP-4V の影響情報を更新しました。

2018年1月16日:EP8000,SR16000 の影響情報を更新しました。

2018年1月12日:EP8000 のモデル追加、SR16000,HA8500,AP8000,AP8800,CSC,SGW,H-6355 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に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。