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
（L1TF, L1 Terminal Fault）

2018年8月14日にIntel社より以下の脆弱性(L1TF)が公表されました。

INTEL-SA-00161

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00161.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。
なお、UEFI(BIOS),F/W対策についてはINTEL-SA-00115対策と同じですので、「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)」を実施されている場合は必要ありません。
Virtage環境では、UEFI(BIOS)やHVM FWのバージョンに関わらず、【注記】*3の対処でCVE-2018-3646を回避可能です。
HVM FWは、ハイパースレッド(SMT)設定が無効なブレード向けの対策と、有効なブレード向けの対策を順次リリースします。ブレードのハイパースレッド(SMT)設定に合致する版をご適用ください。

1-1 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			ハードウェア対策		
				CVE-2018-3615	CVE-2018-3620	CVE-2018-3646	UEFI(BIOS)	Virtage HVM F/W SMT 無効 *4	Virtage HVM F/W SMT 有効 *5
1	BS1000	Xeon	x1～x4	なし	なし	なし	―	―	―
2		Xeon MP	x2	なし	なし	なし	―	―	―
3	BS320	X86	x1～x3	なし	なし	なし	―	―	―
4		標準 HDD 拡張 SAN 専用 PCI 拡張	x4	なし	**あり**	**あり**	（保守期限終了）	―	―
5			x5	なし	**あり**	**あり**	調整中	調整中	調整中
6			x6	なし	**あり**	**あり**	調整中	（対象外）	（対象外）
7	BS2000	標準	x1	なし	**あり**	**あり**	2019/1/25 リリース [01-67/03-60]*1	2019/2/22 リリース [Ver.59-84]	2019/3/15 リリース [Ver.59-85]
8			x2	なし	**あり**	**あり**	2019/1/25 リリース [03-60]*1		
9			x3	なし	**あり**	**あり**	2018/7/27 リリース [09-64]*1	2018/12/21 リリース [Ver.59-84]	
10			x4	なし	**あり**	**あり**	2018/7/27 リリース [11-56]*1		
11		高性能	x1	なし	**あり**	**あり**	2019/1/25 リリース [03-37]*1	2019/1/25 リリース [Ver.79-84]	2019/3/15 リリース [Ver.79-85]
12			x2	なし	**あり**	**あり**	2018/9/28 リリース [07-74]*1	2018/12/21 リリース [Ver.79-84]	
13	BS500	BS520A	x1	なし	**あり**	**あり**	2018/7/27 リリース [Ver.02-68]	2018/10/26 リリース [Ver.02-64]	2019/2/15 リリース [Ver.02-65]
14		BS520H	x1	なし	**あり**	**あり**	2018/7/27 リリース [Ver.05-12]		
15			x2	なし	**あり**	**あり**	2018/7/27 リリース [Ver.04-55]		
16			x3	なし	**あり**	**あり**	2018/7/6 リリース [Ver.08-93]		
17			x4	なし	**あり**	**あり**	2018/7/6 リリース [Ver.10-24]		
18		BS540A	x1	なし	**あり**	**あり**	2018/7/27 リリース [Ver.03-44]		
19		BS520X	x1	なし	**あり**	**あり**	2018/7/27 リリース [Ver.07-72]		
20			x2	なし	**あり**	**あり**	2018/7/6 リリース [Ver.09-61]		

1-1 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			ハードウェア対策		
				CVE-2018-3615	CVE-2018-3620	CVE-2018-3646	UEFI(BIOS)	Virtage HVM F/W	
								SMT 無効 *4	SMT 有効 *5
21	BS2500	標準	x1	なし	**あり**	**あり**	2018/7/6 リリース [Ver.08-93]	2018/10/26 リリース [Ver.02-64]	2019/2/15 リリース [Ver.02-65]
22			x2	なし	**あり**	**あり**	2018/7/6 リリース [Ver.10-24]		
23		高性能	x1	なし	**あり**	**あり**	2018/7/27 リリース [Ver.07-72]		
24			x2	なし	**あり**	**あり**	2018/7/6 リリース [Ver.09-61]		
25			x3	なし	**あり**	**あり**	2018/7/6 リリース [Ver.11-21]		

1-2 日立アドバンストサーバ HA8000 シリーズ (1/2)

#	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	HA8000	RS110xJ, TS10xJ, RS220xJ, RS210xJ, TS20xJ, RS440xK, RS110xK, TS10xK, SS10xK, RS220xK, RS210xK, TS20xK, RS440xK1, RS110xK1, TS10xK1, SS10xK1	なし	**あり**	**あり**	(保守期限終了)
2		RS220xK1, RS210xK1, TS20xK1	なし	**あり**	**あり**	2019/4/5 リリース [Ver F15]
3		RS110xL, TS10xL, SS10xL, NS110xL, NS10xL, NS10sxL	なし	**あり**	**あり**	2019/1/25 リリース [Ver 1.09]
4		RS440xL	なし	**あり**	**あり**	2019/2/8 リリース [Ver 0041]
5		RS220xL, RS210xL, TS20xL, NS220xL	なし	**あり**	**あり**	2019/4/5 リリース [Ver F15]
6		RS440xL1	なし	**あり**	**あり**	2019/2/8 リリース [Ver 0041]
7		RS110xL1, TS10xL1, SS10xL1, NS110xL1, NS10xL1, NS10sxL1	なし	**あり**	**あり**	2019/1/25 リリース [Ver 1.09]
8		RS440xL2	なし	**あり**	**あり**	2019/2/8 リリース [Ver 0041]
9		RS110xL2, TS10xL2, NS110xL2, NS10xL2, SS10xL2, NS10sxL2	なし	**あり**	**あり**	2019/1/25 リリース [Ver LU.1.03.00]
10		RS440xM	なし	**あり**	**あり**	2018/12/7 リリース [Ver 5.6.0171]
11		RS110xM, TS10xM, NS110xM, NS10xM	なし	**あり**	**あり**	2019/1/25 リリース [Ver M1.1.08.00]
12		RS220-hxM, RS210-hxM	なし	**あり**	**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	なし	**あり**	**あり**	2018/11/30 リリース [Ver M2.1.08]
14		RS110xM1, TS10xM1, NS110xM1, NS10xM1	なし	**あり**	**あり**	2019/1/25 リリース [Ver MD.1.05.00]
15		RS220-hxM1, RS210-hxM1	なし	**あり**	**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	なし	**あり**	**あり**	2018/11/30 リリース [Ver M2.1.08]
17		RS220-hxM2, RS210-hxM2	なし	**あり**	**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	なし	**あり**	**あり**	2019/1/25 リリース [Ver MB.1.08.00]

1-2 日立アドバンストサーバ HA8000 シリーズ (2/2)

#	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)
25	HA8000	RS440xN	なし	**あり**	**あり**	2018/12/7 リリース [Ver 5.6.0273]
26		RS220xN, RS210xN	なし	**あり**	**あり**	2018/11/30 リリース [Ver 5.0.E034]
27		TS20xN	なし	**あり**	**あり**	2019/1/25 リリース [Ver 5.0.8013]
28		RS110xN, TS10xN, NS10xN, NS110xN	なし	**あり**	**あり**	2018/11/30 リリース [Ver 5.0.9017]
29		RS440xN1	なし	**あり**	**あり**	2018/12/7 リリース [Ver 5.6.0383]
30		RS220xN1, RS210xN1, NS220xN1	なし	**あり**	**あり**	2018/11/30 リリース [Ver 5.0.E034]
31		RS110xN1, TS10xN1, NS10xN1, NS110xN1	なし	**あり**	**あり**	2018/10/26 リリース [5.0.4008]
32		RS220xN2, RS210xN2, NS220xN2	なし	**あり**	**あり**	2018/11/30 リリース [Ver 5.0.8023]
33		TS20xN2	なし	**あり**	**あり**	2018/11/30 リリース [Ver 5.0.5010]
34		上記モデル以外 (RS440xJ を含みます)	なし	なし	なし	ー

1-3 日立アドバンストサーバ HA8000V シリーズ

#	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	HA8000V	DL380, DL360, DL580, ML350	なし	**あり**	**あり**	2018/7/13 リリース [Ver.1.42]

1-4 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

1-5 エンタープライズサーバ EP8000 (1/2)

#	装置	モデル	CPU	影響			ハードウェア対策
				CVE-2018-3615	CVE-2018-3620	CVE-2018-3646	F/W *1
1	EP8000	S914, S924	POWER9	なし	**あり**	**あり**	※初回出荷から対策済み
2		S814, S824, E850	POWER8	なし	**あり**	**あり**	2018/2/16 リリース [SV860_138]
3		E870, E880	POWER8	なし	**あり**	**あり**	2018/2/16 リリース [SC860_138]
4		720(E4D), 740(E6D),	POWER7+	なし	**あり**	**あり**	2018/3/23 リリース [AL770_122]
5		770(MMD), 780(MHD)	POWER7+	なし	**あり**	**あり**	2018/3/23 リリース [AM780_096]
6		710(E2B), 720(E4B), 740(E6B), 750(E8B)	POWER7	なし	**あり**	**あり**	2018/3/23 リリース [AL730_157]
7		720(E4C), 740(E6C),	POWER7	なし	**あり**	**あり**	2018/3/23 リリース [AL740_165]
8		770(MMB), 780(MHB)	POWER7	なし	**あり**	**あり**	2018/3/23 リリース [AM780_096]

1-5 エンタープライズサーバ EP8000 (2/2)

#	装置	モデル	CPU	影響			ハードウェア対策
				CVE-2018-3615	CVE-2018-3620	CVE-2018-3646	F/W *1
9	EP8000	770(MMC), 780(MHC)	POWER7	なし	**あり**	**あり**	2018/3/23 リリース [AM770_122]
10		795(FHB)	POWER7	なし	**あり**	**あり**	2018/3/23 リリース [AH780_096]
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。			

1-6 スーパーテクニカルサーバ SR24000

#	装置	モデル	CPU	影響			ハードウェア対策
				CVE-2018-3615	CVE-2018-3620	CVE-2018-3646	F/W *1
1	SR24000	XP1, XP2	POWER8	なし	**あり**	**あり**	2018/2/23 リリース [SV860_138]

1-7 ディープラーニングシステム SR24000

#	装置	モデル	CPU	影響			ハードウェア対策
				CVE-2018-3615	CVE-2018-3620	CVE-2018-3646	
1	SR24000	DL1	POWER9 POWER8	なし	**あり**	**あり**	OS パッチのみで、F/W 更新は不要です

1-8 サーバ・クライアント関連製品

#	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	HA8000-bd シリーズ	x2	なし	**あり**	**あり**	サポート窓口から提供*2
2		x3	なし	なし	なし	ー
3	FLORA bd500 シリーズ	x7	なし	なし	なし	ー
4		x9	なし	**あり**	**あり**	サポート窓口から提供*2

【注記】

*1: 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。

*2: サポート窓口から対策版を提供させて頂きますので、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。

*3: Virtage 環境での回避策
複数ユーザのゲスト OS がブレード内に混在する環境(例:クラウド環境)では、下記の回避策をお願いします。
① ブレードのハイパースレッド(SMT)設定が無効の場合:
下記のいずれかを実施する。
A) 物理プロセッサを占有モードで割り当てる。
B) ユーザ毎のプロセッサグループを作成する。
② ブレードのハイパースレッド(SMT)設定が有効の場合:
下記のいずれかを実施する。
A) コア内の物理プロセッサ(2 つ)を同一ユーザに占有モードで割り当てる。
B) ユーザ毎のプロセッサグループを作成する。

*4: ハイパースレッド(SMT)設定が無効なブレード向け、有効なブレード向け、それぞれの対策版リリース日程を示します。

*5: 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、下記の対処をお願いします。
下記①もしくは②を実施する。
① ハイパースレッド(SMT)が「無効」なブレード向け:
A) 対処は不要です。
② ハイパースレッド(SMT)が「有効」なブレード向け:
A) Hvm 管理コマンド(HvmSh)を用いて下記を実施する。
i. opr HvmScdOptions コマンドを使用して、コアスケジューリングを有効にする。

1-9 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)

1-10 その他サーバ・クライアント・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。

・日立アドバンストサーバ 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
・セキュリティ PC(SPC)FLORA Se210/Se330 の全モデル
・FibreChannel スイッチ装置 FCSW の全モデル
・システム運転支援装置(CSC)(2 形,3 形)
・SVP の全モデル
・UPS の全モデル
・コンソール切替ユニットの全モデル
・テープライブラリ装置 LTO
・プリンタ製品
・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)
・統合データ保護システム DMV(Data Mover for Volume)
・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
・エントリークラスディスクアレイ装置 BR1200, BR1250 の全モデル

1-11 影響調査中の製品

以下の製品については、影響有無を調査中です。

・ロードバランサの全モデル

2. 脆弱性の対策について

仮想化機構をHyperThread有効でご利用されている場合は、UEFI(BIOS),OS,VMM全ての対策版適用に加え、仮想化機構ベンダーが情報を提供している追加策がありますので、必要に応じて対応をご検討ください。

Virtageの追加策については、対策版リリース時に情報提供致します。

3. 対策による性能影響について

Intel社の公表によると、今回の脆弱性の対策によって性能に悪影響が出る場合があります。

対策の適用につきましては、本脆弱性の特徴を踏まえてお客様環境に対する対策をご検討ください。また、お客様環境等で性能影響を見極めた上で、本番対策検討をお願いします。

Intel社公表資料

https://www.intel.com/content/www/us/en/architecture-and-technology/l1tf.html

4. 関連情報

HP 社製 PC https://support.hp.com/jp-ja/document/c06114441

5. 本件に関する問い合せ窓口

各製品サポート窓口にお問合せください。

6. 更新履歴

2019年4月5日：BladeSymphony,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：BladeSymphony,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：BladeSymphony,HA8000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：BladeSymphony,HA8000,EP8000,SR24000の対策情報を更新しました。
2018年10月26日：BladeSymphony,HA8000,EP8000,SR24000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：Virtage環境の回避策を追記しました。BS2000高性能x2の対策情報を更新しました。
周辺機器製品の一部を「影響調査中」から「影響なし」としました。
2018年8月31日：BS500,BS2500のVirtage対策予定を追記しました。EP8000,SR24000の対策日程を延期しました。
2018年8月24日：HA8000の一部対策予定を変更しました。
2018年8月23日：性能影響に関するIntel社公表資料URLを修正しました。
2018年8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。