

「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)]

当該脆弱性による日立ストレージサービス基盤・SAP HANA クラウドサービス基盤への影響は、以下の通りです。

#	提供サービス	影響	対応	備考
1	<u>コンテンツマネージドサービス</u> (1) 日立 ファイルストレージ アーカイブ マネージドサービス (2) 日立 ファイルストレージ システムバック アップ マネージドサービス (3) 日立 ファイルストレージ アーカイブ/ システムバックアップ マネージドサービス (4) クラウドストレージサービス (5) Cloud on-Ramp	なし	本サービスは任意の外部プログラムを実行できないため、影響はありません。	
2	<u>Storage Utility Management Service (SUMS)</u>	なし	ストレージサービスは任意の外部プログラムを実行できないため、影響はありません。	
3	<u>かんたん Private DaaS</u>	なし	<u>ストレージ</u> 任意の外部プログラムを実行できないため、影響はありません。	
		あり	<u>サーバ/ソフトウェア</u> お客様にて、該当するサーバ、ソフトウェア製品の対処方法をご覧ください、ご対応をお願いいたします。	
4	<u>Cloud Delivered Service for SAP Solutions</u> ・クラウドサービス基盤	あり	弊社にて、 クラウドサービス基盤の対策を順次実施しております。	

●本件に関する問い合わせ窓口

各サービスのサポート窓口にお問い合わせください。

●更新履歴

2018年2月19日：クラウドサービス基盤の対応を更新しました。

2018年1月17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に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。