**********
Hitachi Cloud「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
エンタープライズクラウドサービス
**********

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)]
弊社サービスを安全にご利用頂くため、サービス提供基盤への対策の実施状況をご報告するとともに、お手数をおかけいたしますがお客様にて下記に記載するセキュリティアップデート作業を実施願います。

－ 記 －

1. 脆弱性の概要

投機的実行機能を持つ CPU に対して、サイドチャネル攻撃が行われる脆弱性が報告されております。

本脆弱性の対策は、"サービス提供基盤"と"ご利用中の仮想サーバ"の両方の対策が必要となり、サービス提供基盤における対策状況と、お客様側の対策作業をお知らせしております。

2. サービス提供基盤の対策

2. 1 対象サービス

このお知らせは、エンタープライズクラウドサービスのサーバサービス、オンデマンドサーバサービスをご利用のお客様を対象としています。

2. 2 対象状況

前回のお知らせ以降、本脆弱性に関するハードウェア、ソフトウェア各ベンダより各種アップデートが提供されております。

これらの適用を含めたサービス提供基盤の対策作業については、適宜、影響のあるお客様へのメンテナンス通知にてご連絡を差し上げておりましたが、2018 年 7 月 6 日(金)に作業を完了しております。

3. ご利用中の仮想サーバの対策

お客様のご利用中の仮想サーバへの脆弱性対策版のセキュリティパッチの適用をお願いします。

OS ごとの対応を下記に記載しますので、お客様ご利用中の OS に合わせた対応をお願いします。

３．１　WindowsOS の場合

Microsoft 社から公開されている以下の情報を元に OS におけるパッチ適用等の対策を実施願います。

※参考情報

″Windows Server を投機的実行のサイドチャネルの脆弱性から保護するためのガイダンス″

参考 URL: https://support.microsoft.com/ja-jp/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution

なお、WindowsOS とウィルス監視オプションの現行ソフトウェアバージョン Symantec Endpoint Protection(以下、SEP)の組み合わせにおいて、本脆弱性に対する OS パッチ適用後に仮想サーバが停止する事象が報告されています。

ウィルス監視オプションをご利用のお客様には、別途、個別に対応方法のご案内を行なっておりますので、事前に SEP のバージョンアップのご対応をお願いいたします。

３．２　Red Hat Enterprise Linux の場合

Red Hat 社から公開されている以下の情報を元に OS におけるセキュリティパッチ適用等の対策を実施願います。

※参考情報

″カーネル のサイドチャネル攻撃- CVE-2017-5754 CVE-2017-5753 CVE2017-5715″

参考 URL: https://access.redhat.com/ja/security/vulnerabilities/3311961

なお、上記のセキュリティパッチ対策はバージョンの変更が前提となっております。サービス基盤のサポート OS の制限により、Red Hat Enterprise Linux のバージョンは、現在 6.x の仮想サーバは 6.9、7.x の仮想サーバは 7.4 へのアップデートをお願いします。

また、ウィルス監視オプションをご利用の場合、上記セキュリティパッチ適用により、現行 SEP バージョンのサポート対象外となる場合があります。ウィルス監視オプションをご利用のお客様には、別途、個別に対応方法のご案内を行なっておりますので、事前に SEP のバージョンアップのご対応をお願いいたします。

4. ご利用中の仮想サーバの対策の影響

セキュリティパッチ適用等に伴い、仮想サーバの再起動が必要となる可能性がございます。

また、本脆弱性に対するセキュリティパッチ適用に起因し、アプリケーションによっては性能が劣化する場合があるとの報告がございます。セキュリティパッチ適用にあたっては業務影響をご検討の上、実施願います。

※参考情報

"Windows システム上の Spectre および Meltdown に対する緩和策のパフォーマンスへの影響について"

参考 URL：https://blogs.technet.microsoft.com/jpsecurity/2018/01/23/understanding-the-performance-impact-of-spectre-and-meltdown-mitigations-on-windows-systems/

"投機的実行の脆弱性によるパフォーマンスへの影響: CVE-2017-5754、CVE-2017-5753、および CVE-2017-5715 に対するセキュリティーパッチによるパフォーマンスへの影響"

参考 URL：https://access.redhat.com/ja/articles/3315851

5. 今後のご連絡について

今後、ハードウェア、ソフトウェア ベンダから追加の対策版が発行された場合、適宜、対策に関するご案内をさせていただきます。

ご理解・ご協力のほどよろしくお願いいたします。

6. お問い合わせ先

本件に関するお問い合わせは、日立クラウドサポートデスクまでお願い致します。

●更新履歴

2018 年 8 月 3 日　サービス基盤に関する追加の対策状況と、ご利用中の仮想サーバの対策に関して更新しました。

2018 年 1 月 19 日　サービス基盤の対策完了に関して更新しました。

2018 年 1 月 16 日　このセキュリティ情報ページを一般向けに発信を開始しました。

・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。

**********
Hitachi Cloud「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
プラットフォームリソース提供サービス
**********

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)]
弊社サービスを安全にご利用頂くため、サービス提供基盤への対策の実施状況をご報告するとともに、お手数をおかけいたしますがお客様にて下記に記載するセキュリティアップデート作業を実施願います。

－ 記 －

1. 脆弱性の概要

投機的実行機能を持つ CPU に対して、サイドチャネル攻撃が行われる脆弱性が報告されております。

本脆弱性の対策は、"サービス提供基盤"と"ご利用中の仮想サーバ"の両方の対策が必要となり、サービス提供基盤における対策状況と、お客様側の対策作業をお知らせしております。

f

2. サービス提供基盤の対策

2. 1 対象サービス

このお知らせは、プラットフォームリソース提供サービスをご利用のお客様を対象としています。

Customize-Pro モデル等の一部サービス提供基盤については、個別の対応を取っているため、対象のお客様には、別途ご案内を差し上げます。

2. 2 対象状況

前回のお知らせ以降、本脆弱性に関するハードウェア、ソフトウェア各ベンダより各種アップデートが提供されております。

これらの適用を含めたサービス提供基盤の対策作業については、適宜、影響のあるお客様へのメンテナンス通知にてご連絡を差し上げておりましたが、2018/7/6(金)に作業を完了しております。

3. ご利用中の仮想サーバの対策

お客様のご利用中の仮想サーバへの脆弱性対策版のセキュリティパッチの適用をお願いします。

OS ごとの対応を下記に記載しますので、お客様ご利用中の OS に合わせた対応をお願いします。

## 3．1　WindowsOS の場合

Microsoft 社から公開されている以下の情報を元に OS におけるパッチ適用等の対策を実施願います。

※参考情報

"Windows Server を投機的実行のサイドチャネルの脆弱性から保護するためのガイダンス"

参考 URL: https://support.microsoft.com/ja-jp/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution

なお、WindowsOS とウィルス監視オプションの現行ソフトウェアバージョン Symantec Endpoint Protection(以下、SEP)の組み合わせにおいて、本脆弱性に対する OS パッチ適用後に仮想サーバが停止する事象が報告されています。

ウィルス監視オプションをご利用のお客様には、別途、個別に対応方法のご案内を行なっておりますので、事前に SEP のバージョンアップのご対応をお願いいたします。

## 3．2　Red Hat Enterprise Linux の場合

Red Hat 社から公開されている以下の情報を元に OS におけるセキュリティパッチ適用等の対策を実施願います。

※参考情報

"カーネル のサイドチャネル攻撃- CVE-2017-5754 CVE-2017-5753 CVE2017-5715"

参考 URL: https://access.redhat.com/ja/security/vulnerabilities/3311961

なお、上記のセキュリティパッチ対策はバージョンの変更が前提となっております。サービス基盤のサポート OS の制限により、Red Hat Enterprise Linux のバージョンは、現在 6.x の仮想サーバは 6.9 へのアップデートをお願いします。

また、ウィルス監視オプションをご利用の場合、上記セキュリティパッチ適用により、現行 SEP バージョンのサポート対象外となる場合があります。ウィルス監視オプションをご利用のお客様には、別途、個別に対応方法のご案内を行なっておりますので、事前に SEP のバージョンアップのご対応をお願いいたします。

4. ご利用中の仮想サーバの対策の影響

セキュリティパッチ適用等に伴い、仮想サーバの再起動が必要となる可能性がございます。

また、本脆弱性に対するセキュリティパッチ適用に起因し、アプリケーションによっては性能が劣化する場合があるとの報告がございます。適用にあたっては業務影響をご検討の上、実施願います。

※参考情報

"Windows システム上の Spectre および Meltdown に対する緩和策のパフォーマンスへの影響について"

参考 URL：https://blogs.technet.microsoft.com/jpsecurity/2018/01/23/understanding-the-performance-impact-of-spectre-and-meltdown-mitigations-on-windows-systems/

"投機的実行の脆弱性によるパフォーマンスへの影響: CVE-2017-5754、CVE-2017-5753、および CVE-2017-5715 に対するセキュリティーパッチによるパフォーマンスへの影響"

参考 URL：https://access.redhat.com/ja/articles/3315851

5. 今後のご連絡について

今後、ハードウェア、ソフトウェア ベンダから追加の対策版が発行された場合、適宜、対策に関するご案内をさせていただきます。

ご理解・ご協力のほどよろしくお願いいたします。

6. お問い合わせ先

本件に関するお問い合わせは、日立クラウドサポートデスクまでお願い致します。

●更新履歴

2018 年 8 月 3 日　サービス基盤に関する追加の対策状況と、ご利用中の仮想サーバの対策に関して更新しました。

2018 年 1 月 16 日　このセキュリティ情報ページを一般向けに発信を開始しました。

・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。