NTT DATA
Trusted Global Innovator

注目されているセキュリティ事故・事件に関する情報 ＜2018年3月版 (第24号) ＞(選り抜き版)

2018年3月30日
ＮＴＴデータ先端技術株式会社
セキュリティ事業部

今回のサマリー

CPUの脆弱性「Meltdown」と「Spectre」が登場
2018年1月初旬から今日にかけて、CPUの脆弱性「Meltdown」と「Spectre」がネット上で話題となっています。本記事では、これらの脆弱性の詳細や想定される影響を述べるとともに、企業の取るべき対策について解説します。

CPUの脆弱性「Meltdown」と「Spectre」が登場

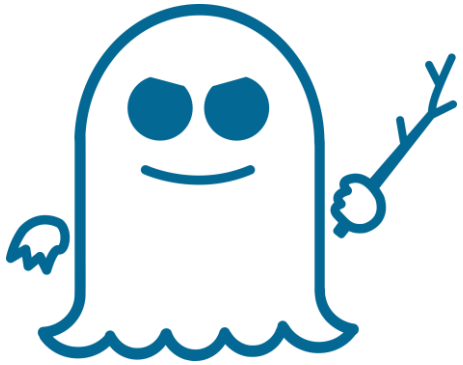
1. はじめに

「Meltdown」と「Spectre」は、2018年1月初旬からネット上で話題になり始めたCPUに関する脆弱性です。

この脆弱性は、CPU内部に備えられたキャッシュと「投機的実行」と呼ばれる機能を悪用することにより、アクセスが許可されていないメモリ領域の情報を窃取することが可能になるものです。

これらの脆弱性に対し、1月初旬にOSやCPUの開発ベンダなどから対策パッチが提供されましたが、端末のパフォーマンス低下や不具合が発生するなど、混乱が続いています。

Meltdown



Spectre

引用: https://meltdownattack.com/

2. MeltdownとSpectreの概要

MeltdownとSpectreの概要をまとめると、以下の通りとなります。

	Meltdown	Spectre
CVE番号	CVE-2017-5754 （Variant 3: Rogue data cache load）	• CVE-2017-5753 （Variant 1: Bounds Check Bypass） • CVE-2017-5715 （Variant 2: Branch Target Injection）
CVSSv3 基本値	4.7（JPCERT/CC） 5.6（NIST）	
脆弱性の対象CPU	• Intel製（※1） • ARM製 Cortex-A75（※3）	• Intel製（※1） • AMD製（※2） • ARM製（※3）
脆弱性による影響	カーネルメモリ領域の情報が窃取される	他のアプリケーションが利用している メモリ領域の情報が窃取される
脆弱性による 被害状況	現時点ではなし （ただし、これらの脆弱性を悪用したマルウェアサンプルが発見されている）	
対策方法	OS / アプリケーション / BIOSのアップデート	

※1 1995年以降に製造されたCPUのほとんどが影響を受けるとされている
https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr
※2 AMD Radeon GPUアーキテクチャは対象外
https://www.amd.com/en/corporate/speculative-execution
※3 Cortex-R7/R8/A8/A9/A15/A17/A57/A72/A73/A75がSpectreの影響を受ける
このうち、Cortex-A75はMeltdownの影響も受ける
https://developer.arm.com/support/security-update

3. CPUのキャッシュと投機的実行

近年のCPUは処理効率を高めるために、CPU内部に高速な読み書きができるキャッシュと、「投機的実行（Speculative Execution）」と呼ばれる機能を備えています。

MeltdownとSpectreはこれらを悪用し、通常ではアクセスできないメモリ領域の情報を窃取します。

■ CPUの「投機的実行」について

CPUの投機的実行は大きく2種類に分類できます。

- **アウトオブオーダー（Out of Order）**

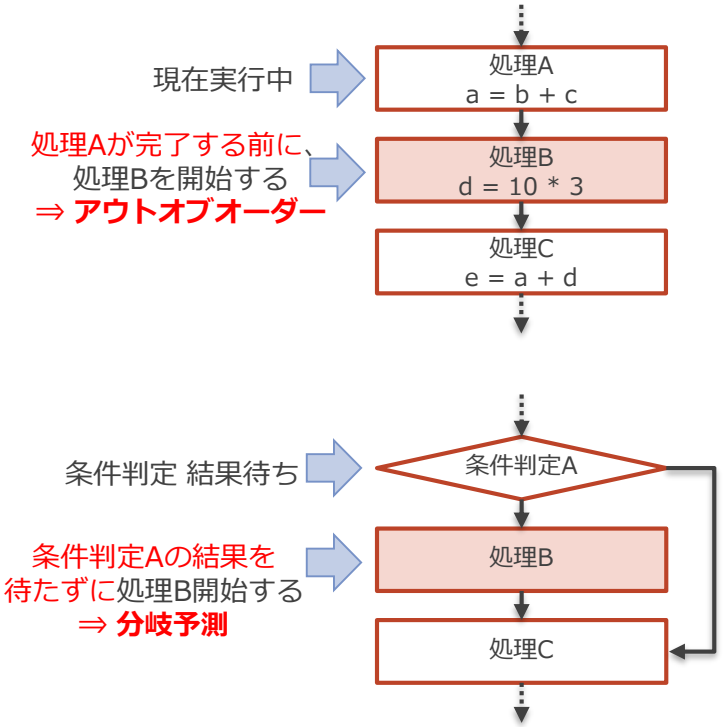
  プログラム中の命令の並び順に依らず、データなどの依存関係を見て処理可能な命令を順次実行する機能です。

  右の図において、処理Bは処理Aに依存していないため、処理Aの完了を待たずに処理Bを実行させることができます。このように、CPUの待機時間を減らして処理効率を向上させることができます。

- **分岐予測（Branch Prediction）**

  今までの条件分岐結果の傾向から、次の条件分岐結果を予測してその先の処理を事前に実行する機能です。

  予測結果が外れた場合は、事前に実行した結果を破棄します。

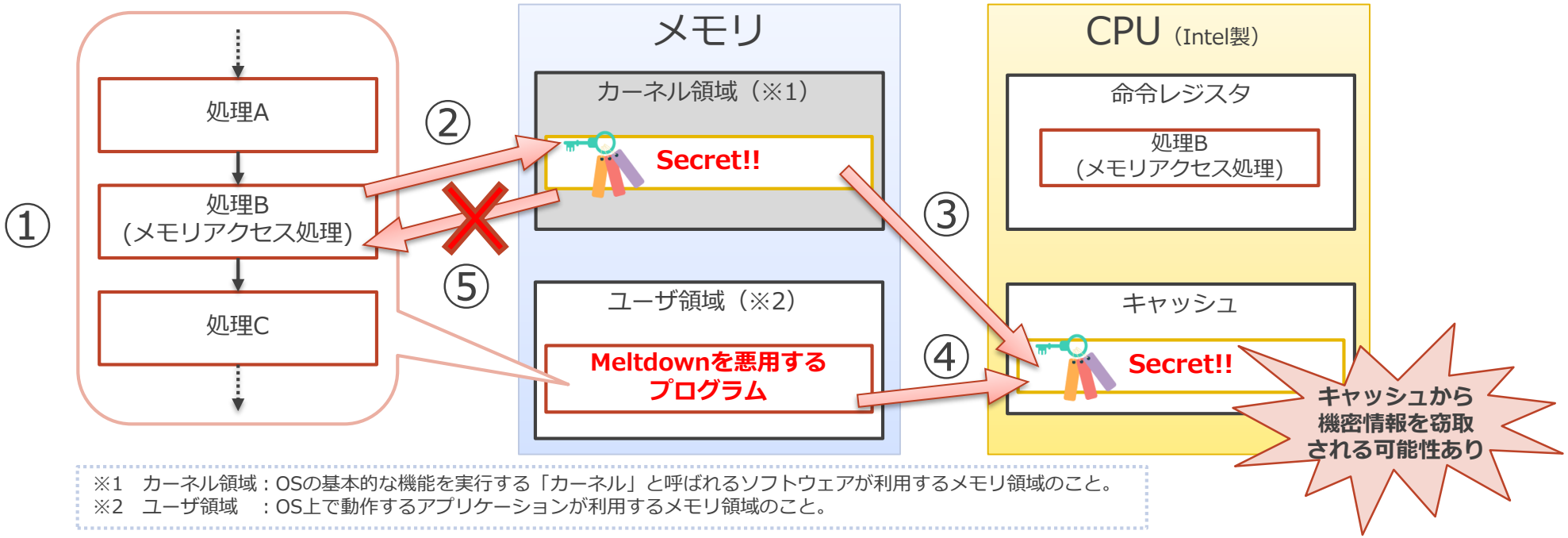


4. Meltdownの攻撃手法（概要図）

Meltdownによる攻撃フローの概要図を以下に示します。Meltdownはメモリ内のカーネル領域にある情報を窃取しようと試みます。

■ 攻撃フロー

① 「アウトオブオーダー」により、CPUは「処理A」が完了する前に「処理B(メモリアクセス処理)」や「処理C」を実行する
② 「処理B」の実行により、プログラムがカーネル領域の情報にアクセスする
③ CPUのキャッシュ機能により、手順②でアクセスした情報がCPUのキャッシュに一時保存される
④ CPUのキャッシュにアクセスすることで、カーネル領域の情報を窃取
⑤ 「メモリアクセス違反」により手順②の処理がエラーとなり、実行結果は破棄される



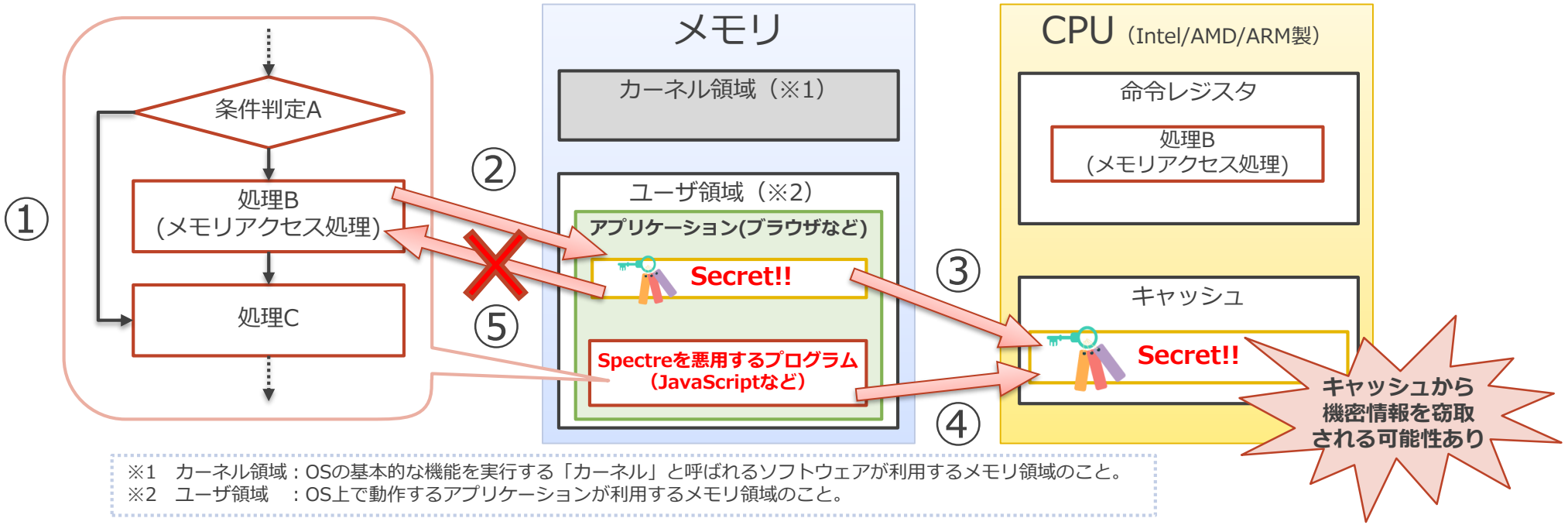
※1　カーネル領域：OSの基本的な機能を実行する「カーネル」と呼ばれるソフトウェアが利用するメモリ領域のこと。
※2　ユーザ領域　：OS上で動作するアプリケーションが利用するメモリ領域のこと。

5. Spectreの攻撃手法（概要図）

Spectreによる攻撃フローの概要図を以下に示します。Spectreはメモリ内のユーザ領域にある情報を窃取しようと試みます。

■ 攻撃フロー

① 「分岐予測」により、CPUは「条件判定A」の結果を待たずに、「処理B(メモリアクセス処理)」を実行する
② 「処理B」の実行により、プログラムがユーザ領域の情報にアクセスする
③ CPUのキャッシュ機能により、手順②でアクセスした情報がCPUのキャッシュに一時保存される
④ CPUのキャッシュにアクセスすることで、ユーザ領域の情報を窃取
⑤ 「メモリアクセス違反」により手順②の処理がエラーとなり、実行結果は破棄される



※1　カーネル領域：OSの基本的な機能を実行する「カーネル」と呼ばれるソフトウェアが利用するメモリ領域のこと。
※2　ユーザ領域　：OS上で動作するアプリケーションが利用するメモリ領域のこと。

6. 想定される影響

MeltdownとSpectreはCPUの脆弱性であることから、OSやアプリケーションの垣根を越えて、幅広い機器が影響を受ける可能性があります。

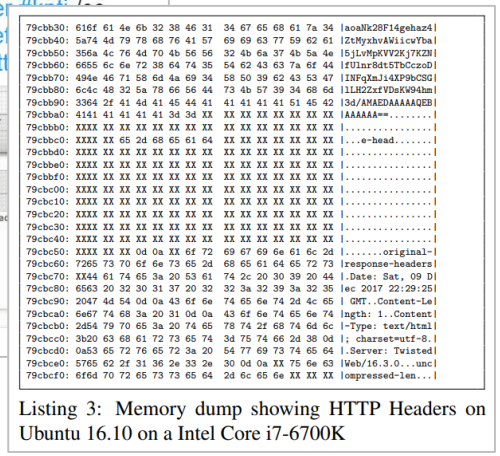
■ MeltdownやSpectreによる主な影響

- パスワードや通信内容の窃取

  Twitter（※1）や論文では、Meltdownを悪用して、メモリに記録されたパスワードや通信内容の窃取ができることが明らかになっています。

  また、ブラウザ上でSpectreを悪用したJavaScriptを実行させることにより、ブラウザに保存されたユーザIDやパスワードが窃取できるとされています。

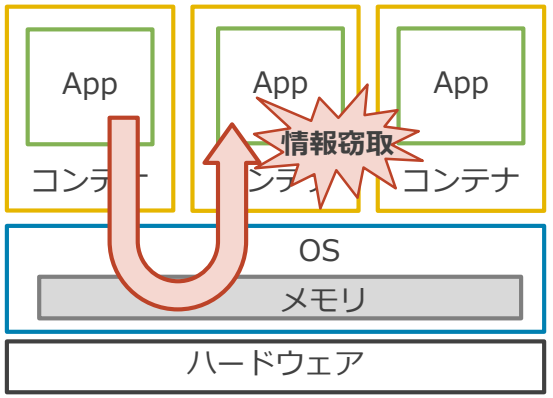
  ※1 https://twitter.com/misc0110/status/948706387491786752


Listing 3: Memory dump showing HTTP Headers on Ubuntu 16.10 on a Intel Core i7-6700K

- 同一ホストにある仮想マシン間の情報窃取

  Docker, LXC, OpenVZのようなコンテナ型仮想化技術はホストOSのメモリを共有しています。このため、あるコンテナから他のコンテナの情報をメモリから窃取される可能性があります。

  また、VMware社のESXiや、Citrix社のXen Server等のハイパーバイザ型仮想化技術を利用している環境下でも、ある仮想マシンから他の仮想マシンの情報を窃取される可能性があります。なお、完全仮想化された環境であれば、他の仮想マシンの情報窃取はできないとされています。



7. パッチ提供状況 (1/3)

MeltdownとSpectreの発見を受けて、OSやCPUの開発ベンダなどから対策パッチが提供されています。一方で、対策パッチを適用すると端末の不具合やパフォーマンス低下が発生する事象も確認されています。

日時	ベンダ	出来事
2017年12月6日	Apple	Appleが脆弱性（Meltdown）に対応したmacOS High Sierra 10.13.2を公開
2018年1月3日	Google	Google Project Zeroが脆弱性の詳細情報を公開
2018年1月3日	Intel	IntelがCPUバグの存在を正式に認め、脆弱性に対する見解を発表
2018年1月4日	Microsoft	Microsoftが緊急の更新プログラムを公開。Win10が自動アップデート。Edge,IE11が脆弱性に対応
2018年1月5日	Mozilla	Mozillaが脆弱性に対応したFirefox 57.0.4を公開
2018年1月9日	Apple	AppleがmacOS Sierra/El Capitan等に脆弱性（Spectre）に対応した最新版を公開
2018年1月9日	Microsoft	MicrosoftがAMD製CPU搭載モデルでの不具合を受け、更新プログラムの公開を一時停止
2018年1月10日	Microsoft	MicrosoftがWin7、Win8.1等への月例のアップデートを公開
2018年1月11日	Microsoft	MicrosoftがAMD製CPUの不具合に対応した更新プログラムを再公開
2018年1月12日	Intel	Intelがマイクロコードに不具合が確認されたとして一部の顧客へ忠告していると報道
2018年1月17日	Intel	Intelがマイクロコードの不具合の続報として複数のCPUで同問題が確認されていることを報告
2018年1月22日	Intel	Intelがマイクロコードの不具合の調査が終わるまでアップデートを見送るよう推奨
2018年1月23日	Apple	AppleがiOS,macOS Sierra/ElCapitanのMeltdownに対応した最新版を公開
2018年1月24日	Google	Googleが脆弱性(Spectre)に対応したChromeを公開
2018年1月25日	Microsoft	Microsoftが緩和策を無効化するアップデート（KB4078130）を公開
2018年2月7日	Intel	Intelがマイクロコードの不具合を修正したアップデートを公開
2018年2月20日	Intel	Intelが第6～第8世代向けのマイクロコードの不具合を修正したアップデートを公開

7. パッチ提供状況 (2/3)

■ Intel

IntelはMeltdown/Spectre対策として、修正版マイクロコードをPC製造ベンダに提供しています。PC製造ベンダからは「BIOSアップデート」として提供されています。BIOSアップデートを適用すると、端末起動時にCPUが修正版マイクロコードを読み込み、Meltdown/Spectreの悪用を防ぐことができます。

なお、この対応に関し、1月中旬から末にかけてBIOSアップデート後に端末が再起動を繰り返すなどの不具合が確認されました。その後、2月7日と2月20日にIntelから不具合を修正したマイクロコードが公開されています。

■ Microsoft

1月4日に、Meltdown/Spectreの緩和策としてMicrosoftから緊急パッチが公開（※1）されました。WindowsやMicrosoft Edge、Internet Explorer 11に対して、メモリ管理方法などの修正が行われています。

この緊急パッチを適用する際に、古いバージョンのウイルス対策ソフトを利用していると、互換性の問題によりブルースクリーンが発生する場合があります。2018年3月時点で、主なウイルス対策ソフト（※2）がこの互換性問題を解消しており、ソフトを最新版にすることで正常に緊急パッチを適用できます。

※1： https://portal.msrc.microsoft.com/ja-jp/security-guidance/advisory/ADV180002
※2： TrendMicro, McAfee, Symantec, Kaspersky, Nortonはすでに互換性問題を解消済み

7. パッチ提供状況 (3/3)

■ その他

製品/アプリケーション		状況	参考URL
CPU	AMD製	1月11日からOS/PCベンダと連携してパッチ提供中	https://www.amd.com/ja/corporate/speculative-execution
	ARM製	OSのアップデートや、特定の命令を実行させるといった対策を公開中	https://developer.arm.com/support/security-update
OS	macOS	• High Sierra：v10.13.2で対策済み • Sierra / OS X El Capitan： セキュリティアップデート 2018-001で対策済み	https://support.apple.com/ja-jp/HT208394
	iOS	v11.2で対策済み	https://support.apple.com/ja-jp/HT208394
	Android	1月5日以降のパッチで対策済み	https://source.android.com/security/bulletin/2018-01-01
	CentOS	• CentOS7：kernel-3.10.0-693.11.6で対策済み • CentOS6：kernel-2.6.32-696.18.7で対策済み	• https://lists.centos.org/pipermail/centos-announce/2018-January/022696.html • https://lists.centos.org/pipermail/centos-announce/2018-January/022701.html
ブラウザ	Microsoft Edge / Internet Explorer 11	1月4日 緊急アップデートで対策済み	https://portal.msrc.microsoft.com/ja-jp/security-guidance/advisory/ADV180002
	Google Chrome	• Meltdown：v63で対策済み • Spectre：v64で対策済み	https://support.google.com/faqs/answ
	Firefox	v57で対策済み	https://blog.mozilla.org/security/2018/01/03/mitigations-landing-new-class-timing-attack/er/7622138?hl=en
	Safari	v11.0.2で対策済み	https://support.apple.com/ja-jp/HT208394

8. パフォーマンス低下問題

Meltdown/Spectreの対策パッチを適用すると、若干のパフォーマンス低下が発生することが確認されています。

■ Intel

Intelは検証したパフォーマンスのベンチマーク結果を公開しています。これによると、オフィス用途を想定したベンチマークでは、パフォーマンス低下は概ね5%程度にとどまっています。しかし、一部環境（Windows10/第6世代CPUを使用）では、パフォーマンスが約21%低下する結果が出ています。

参照: https://newsroom.intel.com/wp-content/uploads/sites/11/2018/01/Blog-Benchmark-Table.pdf

■ Microsoft

Intel製の第6世代以降のCPUを搭載している端末では、パフォーマンスの低下はほぼ発生しないとしています。一方で、第4世代以前のCPUを搭載したWindows7/8/10端末では、ユーザがパフォーマンス低下に気づくとしています。

■ Apple

Spectre対策を行ったSafariのパフォーマンス低下については、JetStreamによるベンチマークで2.5%未満の影響しかないとしています。

9. 対策方法

1月3日にMeltdown/Spectreの詳細が公開されてから、OSやCPU開発ベンダなどから対策パッチの提供が行われています。パフォーマンスへの影響が許容範囲内であるかどうか、十分に検証を行ったうえで対策パッチを適用することを推奨します。

また攻撃者が本脆弱性を悪用するためには、端末上で不正なプログラムを実行する必要があります。そのため、従来のマルウェアを検知するための対策も有効です。シグネチャの更新頻度や検知時の報告ルールの見直しなど、運用面も含めて対策を見直されることを推奨します。

■ 推奨する対策

- 本脆弱性に対処したパッチを適用する

  OS/アプリケーション/BIOSのそれぞれに対して、対策パッチを適用することを推奨します。一方で、先述のとおりパフォーマンスの低下や端末の不具合が発生する可能性もあります。業務継続の観点からパッチ適用が困難な場合は、以下の低減策の実施を検討ください。

■ 低減策

- マルウェア感染防止のための対策
  - OSやアプリケーションを最新の状態に保つ
  - 不審なメールに添付されたファイルやURLを開かない

10. まとめ

本記事では、2018年1月初旬からネット上で話題になり始めたCPUの脆弱性「Meltdown」と「Spectre」について紹介しました。

Meltdown/Spectreは、CPUのキャッシュ機能と「投機的実行」と呼ばれる機能を悪用し、アクセス許可されていないメモリ領域の情報を窃取できる脆弱性です。

CPUの脆弱性のため、OSやアプリケーションなどの垣根を越えて、多くの端末が影響を受けます。Meltdown/Spectreによる攻撃を防ぐためには、OSやCPU開発ベンダなどから提供されている対策パッチを適用するほか、OSやアプリケーションを常に最新の状態に保つといったマルウェア感染防止のための基本的な対策が有効です。

現時点ではこの脆弱性による被害は確認されていませんが、この脆弱性を悪用したマルウェアがすでに発見されているなど、今後の動向が注目されます。

11. 参考URL

- Meltdown and Spectre
  https://meltdownattack.com/
- Meltdown(論文)
  https://meltdownattack.com/meltdown.pdf
- Spectre Attacks: Exploiting Speculative Execution
  https://spectreattack.com/spectre.pdf
- Reading privileged memory with a side-channel
  https://googleprojectzero.blogspot.jp/2018/01/reading-privileged-memory-with-side.html
- Microsoftが1月の月例パッチ公開、“緊急”はMicrosoft Edge/IE11など
  https://internet.watch.impress.co.jp/docs/news/1100228.html
- Apple、プロセッサ脆弱性「Meltdown」と「Spectre」の対策について説明
  http://www.itmedia.co.jp/enterprise/articles/1801/05/news035.html
- 脆弱性対策パッチの導入中止を――「リブート問題」でIntelが呼び掛け
  http://www.itmedia.co.jp/enterprise/articles/1801/23/news057.html
- Windowsの臨時アップデート公開、「Spectre」の脆弱性緩和策を無効に
  http://www.itmedia.co.jp/enterprise/articles/1801/30/news061.html
- 「プロセッサ脆弱性」公表から1カ月　アップデートの不具合がさらなる混乱を招く
  http://www.itmedia.co.jp/pcuser/articles/1802/08/news039.html
- Spectre/Meltdown脆弱性を利用したマルウェアが発見
  https://pc.watch.impress.co.jp/docs/news/1104573.html
- CPUの脆弱性 MeltdownとSpectreについてまとめてみた
  http://d.hatena.ne.jp/Kango/20180104/1515094046
- 【図解】CPUの脆弱性 [Spectre] [Meltdown] は具体的にどのような仕組みで攻撃する？影響範囲は？
  http://milestone-of-se.nesuke.com/nw-advanced/nw-security/meltdown-spectre/

NTT DATA

Trusted Global Innovator