回　覧 | 印 | 印 | 印 | 印 | 印 | 印 | 印 | 印 | 印 | 印 | 印 | 印

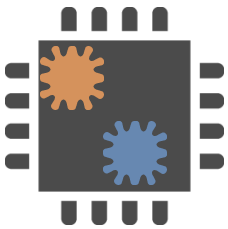
ASAMA Security News Letter Vol.32

あさまセキュリティニュースレター

CPUに脆弱性が！？

(2018年1月16日)

過去のニュースレター（**Vol29 無線LANの脆弱性**、**Vol31 OSやソフトの脆弱性**）で脆弱性についてご紹介してきましたが、今回は**CPU** のパフォーマンス向上のための機能に、**脆弱性**（ **Meltdown/Spectre** ）があると発表されました。



影響を受けるCPU
インテル製CPUの大半、AMD製CPUの一部、アーム製CPUの一部

影響を受けるデバイス
PC、サーバ、スマホ、タブレット（Winに限らず）その他該当のCPUを搭載している機器上で提供されている、クラウドサービスやシステム全体にかかわる問題ともいわれています

今回の脆弱性のパッチに対する偽のサイトと偽のパッチも出現！情報収集も各メーカーサイトから正確な情報を！

今回の脆弱性に関する情報

日々、情報が更新されています。
今回の脆弱性に対するパッチを当てるとPCが遅くなるといった情報も出ておりますが、ご利用のCPUやご利用環境によって異なります。定期的にご利用機種のメーカーのサポートページ等で情報をご確認ください。

被害

個人情報やブラウザに保存された各種ログインやパスワード等の流出の可能性

対策

- **OS・ファームウェア・ソフト等の更新情報の確認、アップデート**
- **正確な情報収集、現状のネットワークの把握、問題点の確認（不明な場合はご相談を）**
- **アップデートのみならず、日ごろからネットワーク全体での対策、バックアップの確認、万が一に備えた、個人での対策ではなく、企業としての対策を考える**
- **PCに限らず、インターネットにつながるモノは脆弱性が発見されると考え、定期的にご利用機器のサポート情報などでサポート情報の確認をしましょう**

情報源

「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 http://www.fmworld.net/biz/common/info/20180109/
セキュリティ TechCenter https://technet.microsoft.com/ja-jp/security/default.aspx

浅間商事株式会社　〒110-0005　東京都台東区上野7-15-70 浅間第一ビル　0120-830-414