— AUS（アルテミス・ユーザ・サポート）便り 2017/05/15号 —
http://www.artemis-jp.com

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

# ●Windows Defender・Microsoft Security Essentials等に脆弱性…パッチ緊急公開

http://internet.watch.impress.co.jp/docs/news/1058644.html
http://forest.watch.impress.co.jp/docs/news/1058674.html

## このニュースをザックリ言うと・・・

- 5月6日（現地時間）、Googleの研究者であるTavis Ormandy氏のTwitterにおいて、マイクロソフトが提供するWindowsのアンチウイルス製品に含まれるマルウェア検索エンジン「Microsoft Malware Protection Engine(MPE, MsMpEng.exe)」に「重大な脆弱性がある」と発表がありました。

- MPEを利用している製品としては「Windows Defender」や「Microsoft Security Essentials」等が挙げられ、発表によれば、細工した不正なファイルをウイルススキャンさせることにより、任意のコードをPCのシステムアカウントの権限で実行され、PCを乗っ取られる等の恐れがあるとされています。

- その後、5月9日にマイクロソフトからMPEの最新バージョン 1.1.13704.0が緊急リリースされ、脆弱性が対策されています。

## AUS便りからの所感等

- 今回の脆弱性の影響範囲は広く、不正なファイルを自ら開いたりするだけでなく、Webサイトの閲覧やファイルが添付されたメールの受信等でウイルススキャンが発生する場合にも攻撃を受ける可能性があった模様です。

- Windows Defender等を利用している場合、MPEは通常自動更新されますが、念の為、エンジンのバージョンが1.1.13704.0以上になっているか確認することを強く推奨致します。

- こういったアンチウイルスソフト自体の脆弱性を攻撃される可能性を引き下げるためにも、UTM等による多層防御を行うことは欠かせません。

INTERNET Watch

**Microsoftのマルウェアスキャンエンジンに最悪な脆弱性、修正パッチが緊急公開**

Windows 10/8.1/8/7やWindows Serverなど広範に影響

岩崎 宰守　2017年5月9日 16:50

ツイート リスト いいね！ 308 シェア B! 58 Pocket 78

Microsoftは9日、「Microsoft Malware Protection Engine（MPE）」の脆弱性「CVE-2017-0290」を修正するセキュリティ更新プログラム（修正パッチ）を緊急公開した。

Microsoft MPEの実行ファイル名は「MsMpEng.exe」で、Windows 10/8.1/8に組み込まれた「Windows Defender」やWindows 7向けの「Microsoft Security Essentials」といったMicrosoftのセキュリティ
けの「Windows Intune Endpoint Protect
Endpoint Protection」などでも利用されて

脆弱性の影響を受けるのは、Microsoft M
前。スクリプトエンジンにメモリ破損の脆弱
ファイルをスキャンした場合に、リモートか
ントのセキュリティコンテキストで実行さ
る。


窓の杜 WINDOWS FOREST

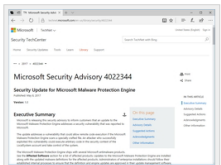
**Windowsのマルウェア対策機能に深刻な脆弱性、スキャンするだけで攻撃を受ける恐れ**

「Windows Defender」などに影響。更新プログラムが配信中

樽井 秀人　2017年5月9日 17:52

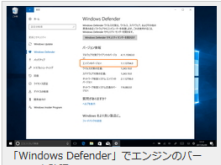
ツイート リスト いいね！ 146 シェア B! 55 Pocket 82

米Microsoft Corporationは8日（現地時間）、マルウェア対策機能「Microsoft Malware Protection Engine」に脆弱性（CVE-2017-0290）が存在することを明らかにした。現在、本脆弱性を修正するセキュリティ更新プログラムが"Windows Update"から入手可能。




脆弱性の内容は、ス
ンのメモリ破損により
イルをスキャンするだ
ドを実行される恐れの
いないとしているが、
れており、Webサイト
メールの受信などでマ
る。この脆弱性を報告
と評しており、なるべ

本脆弱性の影響を受ける製品は「Microsoft Forefront Endpoint Protection 2010」、「Microsoft Endpoint Protection」、「Microsoft Forefront Security for SharePoint」、「Microsoft Security Essentials」、「Windows Defender」（Windows 7/8.1/10、Windows RT 8.1、Windows Server 2016）、「Windows Intune Endpoint Protection」で、エンジンのバージョンがv1.1.13704.0であれば対策済みだ。「Windows Defender」の場合、セキュリティ更新プログラムの適用後に"エンジンのバージョン"が"1.1.13704.0"になっていることを確認しよう。




「Windows Defender」でエンジンのバージョンを確認

# ●auをかたり「緊急速報」メール出回る…「KDDI@ezweb.ne.jp」という送信元でも偽物

http://www.itmedia.co.jp/news/articles/1705/12/news070.html

## このニュースをザックリ言うと・・・

- 5月11日（日本時間）、KDDIのauサポートより、auをかたるスパムメールが拡散されているとして警告が出されています。

- 警告によれば、件名は「緊急速報」、発信元メールアドレスは「KDDI@ezweb.ne.jp」で、本文記載のURLをクリックすることにより、実在するメールアドレスであるかを確認し、さらなるスパムメールの標的にしようとする手口とされています。

- 同様のメールで、速度制限通知を装ったもの等も拡散しているとの情報もあり、メールのURLをクリックしないよう呼びかけられています。

## AUS便りからの所感等

- こういったスパムメールが発信される要因は様々ですが、今日ではPCを「ボット」と呼ばれるマルウェアに感染させてネットワーク（ボットネット）を構成し一斉にメール送信指令を出す形が有力です。

- ある調査では、1台のPCから1ヶ月間に50種類以上・25万通のマルウェア添付メールが送信されていたという報告もあり、万が一感染した場合の影響は所属組織や外部にまで及びます（http://itpro.nikkeibp.co.jp/atcl/column/14/346926/040700924/）。

- UTMを設置し、内部ネットワークのPCから外部への不審なメール送信を検知・遮断する機能を有効にすることにより、万が一内部PCがマルウェアに感染した場合の影響を抑制することが可能となるでしょう。


# ●大手人材派遣会社から1.5万人の個人情報流出…元社員が持ち出し

http://www.nikkei.com/article/DGXLASDG09H64_Z00C17A5000000/

## このニュースをザックリ言うと・・・

- 5月9日（日本時間）、人材派遣大手のスタッフサービス社より、派遣登録者15,368人分の個人情報が同社の元社員によって持ち出されていたことが発表されました。

- 4月19日に同社の利用者から問合せがあったことで発覚したもので、元社員は2015年2月から今年3月の退職までの間、メールでの送信や印刷によって個人情報の持ち出しを行っていたことが判明しています。

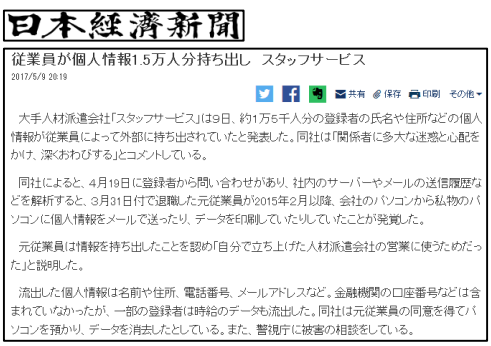
- 持ち出された情報には氏名・住所・電話番号・メールアドレス等の個人情報や時給等のデータが含まれている一方、クレジットカードや金融機関の口座番号といった情報は含まれていなかったとしています。

- 同社では元社員のPCから当該データを回収しており、第三者への流出は確認されていないとのことです。

## AUS便りからの所感等

- 内部からの個人情報持ち出しと言えば、やはり最大3,504万件が持ち出された2014年のベネッセでの事件が思い起こされ、このときは名簿業者への売却のためでしたが、今回は元社員が「自分が立ち上げた人材派遣業の営業のため」としています。

- いくらUTM・ファイアウォールやアンチウイルスによる防御を固めたとしても、外部からの攻撃にのみフォーカスしているのでは、当然ながらこういった内部の悪意を持った人間による不正行為を止めることはできません。




- そういった内部の不正行為の他、特に標的型攻撃によりマルウェアに侵入された場合にも有効な防御策となる「出口対策」のソリューションについても導入を検討し、かつ電子データから紙ベースに至るまであらゆる機密情報の処理について、関係者に対する十分な教育を行うことが改めて重要となります。