

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。

## ●マルウェア「Emotet」感染活動再開か…IPA等注意喚起

<https://internet.watch.impress.co.jp/docs/news/1367367.html>  
<https://www.ipa.go.jp/security/announce/20191202.html#L16>  
[https://www.lac.co.jp/lacwatch/alert/20211119\\_002801.html](https://www.lac.co.jp/lacwatch/alert/20211119_002801.html)  
<https://japan.zdnet.com/article/35179514/>



### このニュースをザックリ言うと…

- 11月16日(日本時間)、IPAより、マルウェア「Emotet」への感染を意図したとみられるメールの拡散が確認されたとして、注意喚起が出されています。
- 2019年~2020年に猛威をふるったEmotetは、今年**1月27日**に欧州刑事警察機構(EUROPOL)による**無力化**が宣言(AUS便り 2021/02/01号参照)、**4月25日**の**機能停止**後は殆ど感染が確認されていませんでしたが、**11月14日頃から活動再開の兆候が確認された**とする情報があったとしています。
- IPAでは添付されているWord・Excelファイルを開いて**マクロを有効化した場合に感染する**といった手口は以前と同様としている一方、11月19日、国内大手セキュリティ企業のラック社からは、新しいEmotetは**指令サーバーとHTTPSによる暗号化通信を行う**等挙動の変化がみられること、**再びボットネットが構築**されていることが発表されています。

### AUS便りからの所感等

- Emotetは、感染したPC上から**実際にやり取りされたメールを奪取、文面を似せたメール**にマルウェアやダウンローダーが含まれる**Officeファイル**を添付して送信する手口により、大きな被害を出してきました。
- Emotet自体が1月に無力化された後も、**類似した手口をとる「loadd」**「Trickbot」等が台頭、特にTrickbotはここ最近大手セキュリティプロダクトによる**検出が最も多いマルウェアの一つ**とされる他、ラック社によれば**Trickbotが感染したPCにEmotetがダウンロードされるケース**も今回確認されているとのこと。
- IPAでは、引き続きEmotetに限らず**一般的なマルウェアへの対策**として、**身に覚えのないメール(あるいは自分が送信したメールへの返信であっても)の添付ファイルを開いたり、本文中のリンクをクリックしたりしないこと**、Office文書ファイルを開いた際に**セキュリティの警告が出た場合、信頼できるものと判断できない限り「編集を有効にする」「コンテンツの有効化」といったボタンをクリックしないこと**を呼び掛けており、こういった慎重な行動に加え、**アンチウイルスやUTMによる防御を確実に**行うことや、**OS・アプリケーションおよびアンチウイルスのパターンファイル等を最新に保つ**ことも重要となります。



#### マルウェア「Emotet」の感染につながる不審なメールが再び出回ったとして、IPAが注意喚起

知人からのメールで感染、情報窃取機能やスパム拡散機能などあり

林 恭平 2021年11月19日 07:15

ツイート リスト BI 32 Pocket 17 いいね! 93 シェア

独立行政法人情報処理推進機構 (IPA) は11月16日、マルウェア「Emotet (エモテット)」の感染につながるメールの配布が再び観測されたとして、注意を呼び掛けた。

Emotetは情報を窃取するだけでなく、感染した端末から窃取した情報を用いて攻撃メールを送信し、さらなる感染拡大を図ることもある。取引先など、一般に信頼できると考えられる相手からのメールに、感染につながるファイルが添付されているなど、感染に気が付きにくい手口となっている。

注意喚起 | 2021年11月19日

#### 【注意喚起】マルウェアEmotetが10カ月ぶりに活動再開、日本も攻撃対象に

サイバー攻撃 セキュリティ

サイバー緊急センター

note

サイバー緊急センターの脅威分析チームです。

日本時間の2021年11月15日、マルウェアEmotetの活動が再開され、11月17日頃から日本組織においても攻撃メールが届き始めていることを当社で確認しています。

これまでEmotetは、その攻撃手口から世界中で大きな被害をもたらし、当社では二度に渡り注意喚起を行いました。現在は検知数が少ない状況ですが、このような背景から今後猛威をふるう可能性が十分考えられます。本注意喚起では、活動を再開したEmotetのポイントをまとめましたので対策にお役立てください。



## ●世界1位「123456」、国内1位「password」…2021年に「最もよく使われた」パスワード発表

<https://www.itmedia.co.jp/news/articles/2111/19/news109.html>  
<https://nordpass.com/most-common-passwords-list/>

### このニュースをザックリ言うと…

- 11月17日(現地時間)、パスワード管理ツール「NordPass」等を提供するNord Security社より、「Top 200 most common passwords of the year 2021(2021年における最もよく使われたパスワードトップ200)」と題した**ランキングが発表**されました。
- ランキングは全世界総合のもの50ヶ国別のもものが挙げられ、**全世界での結果**では1位が「**123456**」、以下5位まで「**123456789**」「**12345**」「**qwerty**」「**password**」となっており、**日本**では1位が「**password**」、以下「**123456**」「**123456789**」「**12345678**」「**1qaz2wsx**」となっています。
- また、**使用されるパスワードの傾向**として、「**ユーザー本人の名前**」や、**アイドル・サッカーチーム・車のブランド名**等「**趣味に関連した単語**」が多く用いられるといった分析結果も出ています。

### AUS便りからの所感

- ランキングはセキュリティインシデント研究者との協力で作成されたもので、同社が2020年に行ったランキングと同様、最もよく「**ユーザーに使用された**」、そして「**流出した**」「**攻撃者によってクラッキングのために試行された**」頻度に基づいたものとみられます。

- 同様のランキングは他のパスワード管理ツールの開発元やセキュリティ企業・機関からも発表されていますが、「**数字の羅列**」「password・iloveyou等**簡単な単語やフレーズ**」「qwerty・asdfghjk・1qaz2wsx等**キーボード上で並んでいる文字列**」が**上位に入る傾向**は、どのランキングでも**何年もの間共通したものと**なっています。

- ランキングに載っている、あるいは上記のパターンに合致するようなパスワードは、**攻撃者がアカウント奪取のため真っ先に試すもの**の心得、Webやそれ以外のサービスで**実際に使っていないか確認**し、より**推測されにくく比較的長いパスワード**を各サービス毎に**使い回すことなく設定**し、所有する**全てのアカウントの保護**に努めることが肝要です。



### 2021年に最も使われたパスワード、世界1位は「123456」 日本の1位は？—Nord Security調べ

© 2021年11月19日 13時22分 公開

[松浦立樹, ITmedia]

パスワード管理ツール「NordPass」を提供するパナマのセキュリティ企業であるNord Securityは11月17日、2021年で最も使われたパスワードのランキングを発表した。その結果、世界50カ国での1位は「123456」であり、日本での1位は「password」であることが分かった。

同社は世界50カ国で使われたパスワードを集計し、全体の合計値と各国でのランキング結果をトップ200まで算出。4TBに及ぶデータベースをサイバーセキュリティ事件の研究者と共同で評価し、リストを作成したという。結果は**公式Webサイト**で公開している。

日本での結果は「password」が1位で最も多く、次点で「123456」「123456789」「12345678」が続き、キーボード左のキーを縦に順番に打った「1qaz2wsx」が5位に入った。世界50カ国には入らず、日本でのみランクインしたのものには「sakura」が15位、「takahiro」が21位、「nekoneko」が35位などがあつた。

## ● Windows 10 バージョン21H2リリース、以降の大型アップデートは年1回に…バージョン2004は12月でサポート終了

<https://pc.watch.impress.co.jp/docs/news/1366953.html>  
<https://pc.watch.impress.co.jp/docs/news/1367207.html>

### このニュースをザックリ言うと…

- 11月17日(日本時間)、マイクロソフト(以下・MS)より、**Windows 10 November 2021 Update(バージョン21H2)が一般ユーザー向けにリリース**されると同時に、**以後の大型アップデートは年2回から年1回に変更**されることが発表されました。
- 10月にリリースされた**Windows 11**については、既に大型アップデートは**年1回となること**が発表されており、**10についてもそれに合わせ、次回の大型アップデートは2022年秋のリリースとなる予定**です。
- なお、2020年5月にリリースされたWindows 10 バージョン**2004**は**2021年12月をもってサポートが終了**するため、以後セキュリティアップデートを受けるためにはバージョン**20H2/21H1/21H2へのバージョンアップが必要**となります。

### AUS便りからの所感

- 21H2は既に**Windows Updateでも配布が開始**されていますが、新しいバージョン固有の不具合が報告されることもあるため、安全を考慮するならば、ISOイメージ等から**手動でバージョンアップ**を行うのは避け、**ダウンロードを促す表示がされるまで待つ**のが良いでしょう。

- 一方で、**2004やそれ以前のバージョンのまま**になっているPCについては、**必ず「更新プログラムのチェック」を実行**し、20H2以降へのバージョンアップも促される様子がない場合に、MSのページから「**Windows 10 更新アシスタント**」をダウンロードして**手動バージョンアップ**を検討すべきです。

- そしてまだ先の話にはなりますが、**Windows 10自体のサポートも2025年10月には終了**となるため、**11のインストールが可能か**、MSが提供する「**PC正常性チェックツール**」または**非公式ツール「WhyNotWin11」**で確認した上で、サポート終了までに**より新しいPCへの置き換えが間に合うよう計画**することを推奨致します。



### Windows 10 November 2021 Update(21H2)が配信開始

関根 慎一 2021年11月17日 10:43

米Microsoftは16日(現地時間)、Windows 10の機能アップデート「Windows 10 November 2021 Update(バージョン21H2)」を配信開始した。Windows Update、Windows 10 更新アシスタント、メディア作成ツールなどを介して更新を適用できる。

Windows 10大型アップデートは今後1年ごとに。サポートは少なくとも2025年10月まで継続

宇都宮 充 2021年11月17日 18:57

Microsoftは16日(現地時間)、これまで半年ごとにWindows 10向けに提供してきた機能更新プログラム(Feature Update)について、今後提供ベースを1年ごとに変更すると発表した。

