

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。

●新たなEmotetはOffice既定の「信頼できる場所」にファイルを置くよう指示…IPA等が注意喚起を更新



<https://scan.netsecurity.ne.jp/article/2022/11/07/48444.html>
<https://www.ipcert.or.jp/at/2022/at220006.html>
<https://www.ipa.go.jp/security/announce/20191202.html#L22>

このニュースをザックリ言うと…

- 11月4日(日本時間)、IPAおよびJPCERT/CCより、マルウェア「Emotet」の活動が同2日から再び確認されたとして、相次いで注意喚起が出されています。
- IPAの情報によれば、Emotetの活動は7月13日頃より確認されていませんでしたが、新たな傾向として、添付された.xlsファイルをOffice既定の「信頼できる場所」に設定されているTemplatesディレクトリに配置した上で開くような指示が書かれているとのことです。
- 指示に従った場合、従来のような「コンテンツの自動化」のクリックを経ずにマクロ等が実行される恐れがあるため、決して不審なファイルをTemplatesディレクトリに保存等しないよう呼び掛けられています。

AUS便りからの所感等

- 現時点での指示は英語で記載されていますが、Emotetのこれまでの傾向から、程なく指示文が日本語化されることが予想されます。
- 現在指定されているTemplatesディレクトリもシステム全体に関わるディレクトリで、通常ファイルの保存時にはUACによる事前の警告が表示されますが、ユーザーディレクトリ以下にも同様のTemplatesディレクトリが設定されており、UACの警告を回避するためにこちらにファイルを保存するよう指示が変更されることも考えられます。
- IPA・JPCERT/CCともEmotetに関する注意喚起を更新し続けていますので、随時情報を確認し、使われている手口を十分に把握した上で、アンチウイルス・UTMによる防御も確実に実行しつつ、慎重に行動することが肝要です。

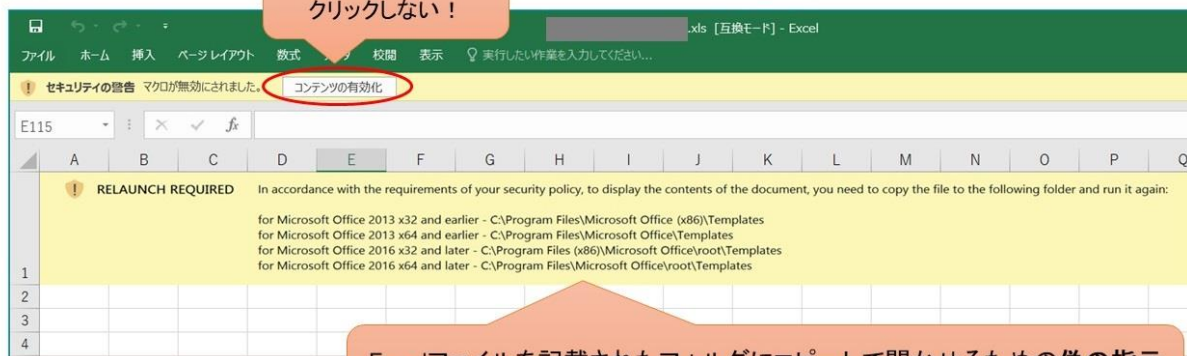
IPA

Emotet (エモテット) と呼ばれるウイルスへの感染を狙うメールについて

(2022年11月4日)

2022年7月13日頃より、Emotetの攻撃メールの配信が観測されない状態が続いていましたが、2022年11月2日から再開されたことを観測しました。攻撃の手口はこれまでと大きくは変わっていませんが、攻撃メールに添付されたExcelファイル内に書かれている偽の指示が、特定のフォルダにExcelファイルをコピーして開かせるように促す内容に変化しています。

危険！
クリックしない！



Excelファイルを記載されたフォルダにコピーして開かせるための偽の指示 (危険！指示どおりに操作するとマクロが強制的に実行されてしまう)

●10月フィッシング報告件数は78,126件…先月より23,899件減少

<https://www.antiphishing.jp/report/monthly/202210.html>



このニュースをザックリ言うと…

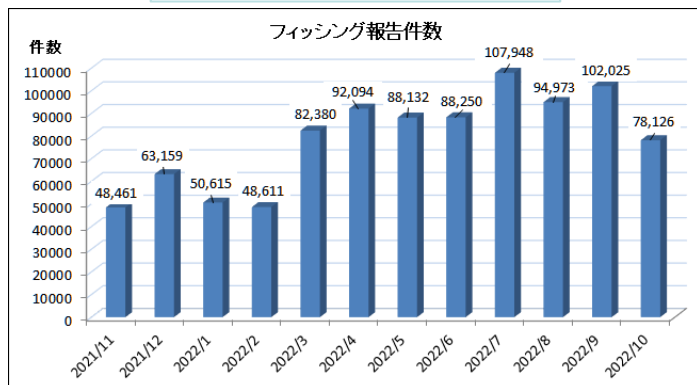
- 11月4日(日本時間)、[フィッシング対策協議会](#)より、[10月に寄せられたフィッシング報告状況](#)が発表されました。
- 10月度の報告件数は78,126件で、9月度(<https://www.antiphishing.jp/report/monthly/202209.html>)の102,025件から23,899件減少しています。
- [フィッシングサイトのURL件数](#)も29,604件と、9月度(53,612件)から24,008件の減少、フィッシングに悪用されたブランド数は89件で9月度(94件)から5件減少となっています。
- [Amazonを騙るフィッシング](#)が全体の約20.9%の他、[えきねっと](#)を騙るものも目立ち約20.4%となっており、以下イオンカード・三井住友カード・国税庁およびJCBを騙るものと合わせて全体の約74.3%を占めたとのこと。

AUS便りからの所感

- 7~9月度の急増傾向からは一旦落ち着いたものの、[年末年始\(12月あるいは1月\)には急増する傾向が過去に見られており](#)、くれぐれも油断せず警戒を続けるべきでしょう。

- フィッシングサイトで使用されるTLD(トップレベルドメイン)の割合は、[topが約65.1%](#)でトップ、以下.ly、.org、.com、.cn、.icu、.shopが上位に挙げられています。

- 前述したえきねっとのフィッシング等で、メールやSMSのみならず、[Google検索結果の上位に広告として偽サイトが表示される事象](#)も確認されており(AUS便り 2022/10/25号)、[利用しているWebサイトへのアクセスは事前に登録したブックマークや公式のモバイルアプリからアクセスするよう心掛けることにより](#)、フィッシングからの確実な回避を行うことを推奨致します。



●Windows 10 22H2リリース、IE11は2023年2月に完全無効化

<https://forest.watch.impress.co.jp/docs/news/1448628.html>

<https://forest.watch.impress.co.jp/docs/news/1451366.html>



このニュースをザックリ言うと…

- 10月19日(日本時間・以下同様)、Microsoftより、[Windows 10バージョン22H2がリリース](#)されました。
- 既にWindows 11がリリースされており、10については21H2以来1年ぶりのバージョンアップながら、[更新内容は小規模](#)とされています。
- また同28日、[Windows 10上のIE11デスクトップアプリ](#)について、[2023年2月15日のセキュリティアップデートにより完全無効化](#)されることが発表されています。

AUS便りからの所感

- Windows 10 [21H1](#)については12月、[21H2は2023年6月にサポート終了](#)となるため、[引き続きセキュリティアップデートを受けるために確実に適用することが推奨](#)されます。

- また10上のIE11のサポートは6月に終了しており、代わりにEdge内で実行されるIEモードが2029年まで提供されます(AUS便り 2022/06/14号参照)が、万が一今までIEでのみ動いていたようなWebアプリケーションが残っていたとしても、Edge・Chrome・Firefox(あるいはSafari)に対応するよう改修を行うよう努めましょう。



「Windows 10 2022 Update」(バージョン 22H2)の一般提供が開始

年1回の大型アップデート。3つの方法でアップグレードが可能

梶井 秀人 2022年10月19日 06:00

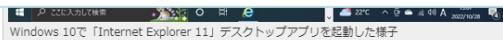
Windows 10 2022 更新 | バージョン 22H2

Microsoft、「Windows 10 2022 Update」(バージョン 22H2)を一般公開

米Microsoftは10月18日(現地時間)、Windows 10の新しい機能アップデート「Windows 10 2022 Update」(バージョン 22H2)を一般公開した。「Windows Insider Program」に加入していないユーザーに対しても、段階的な配信が開始される。

「Internet Explorer 11」は2023年2月のパッチで完全無効化 ~Microsoftがアナウンス

梶井 秀人 2022年10月28日 13:22



米Microsoftは10月27日(現地時間、以下同)、「Internet Explorer 11」(IE11)デスクトップアプリを完全に無効化すると発表した。Windows 10環境のIE11デスクトップアプリは6月15日にすでに廃止され、「Microsoft Edge」へのリダイレクト(振り替え)が開始されているが、2023年2月14日に予定されている月例のセキュリティ更新プログラムでとうとう無効化されるといふ。