［注意喚起］

マルウェアEmotetの感染に関する対応策

2022年5月17日
株式会社フーバーブレイン

Ⅰ． マルウェアEmotet概要

2021年12月9日にIPA（独立行政法人情報処理推進機構）より、Emotet攻撃の再開を観測したと注意喚起がなされ、当社お客様においても、2021年12月からEmotetに関するお問い合わせが増えています。2022年4月26日、IPAでは、**新たな攻撃手口としてファイルを開くだけで感染するショートカットファイル（LNKファイル）による感染手口を公表**し、注意を呼び掛けています。マクロを無効化しても感染するため、今後、再び被害が拡大していく可能性があり、お客様におかれましては、こちらの資料「マルウェアEmotetの感染に関する対応策」をご参照いただき、改めて注意を徹底していただくようお願いします。繰り返しとなりますが、安全であると判断できない「不審なメール」を受信された場合には、「添付ファイルを開かない」、「マクロを有効にしない」、「ダウンロードされたファイルを開いたり実行しない」等、感染防止対策をお願いします。

※2022年4月25日頃より、ショートカットファイル（LNKファイル）を悪用してEmotetへ感染させる手口が観測されています。ショートカットファイルがメールに直接添付されているパターン（図6）と、ショートカットファイルがパスワード付きZIPファイルとして添付されているパターン（図7）の2タイプがあります。このショートカットファイルをダブルクリックなどで開くとEmotetに感染するため、注意が必要です。

※なりすましメールによるマルウエア Emotet の感染被害が、2021年11月以降、国内で確認されており、当社サポートへの感染・被害に関する相談も増加しています。 JPCERT/CCは12月1日付、IPAは12月9日付で情報更新、注意喚起を実施しています。

※2021年11月14日から活動再開が確認されたEmotetでは、メールにdoc、docmファイル、xls、xlsmファイル、パスワード付きZIPファイルが添付されるケースを確認しています。また、メール内のリンクからdoc、docmファイル、xls、xlsmファイルがダウンロードされるケースを確認しています。※「JPCERT/CC マルウエアEmotetへの対応FAQ」、「当社サポート窓口への問い合わせ内容」より

なお、2022年5月9日現在リアルタイム監視とヒューリスティック検知の多層の機能により防護可能と確認しております。

図1:感染から拡散までの概略図

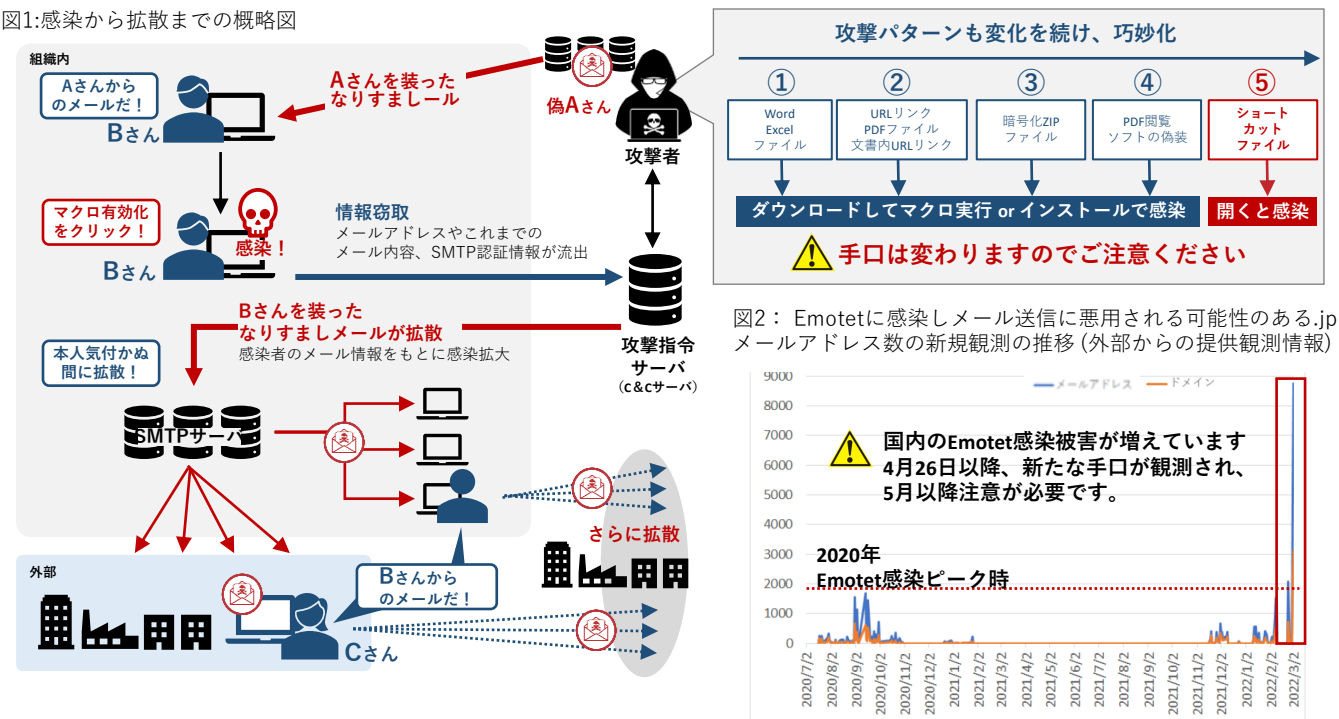
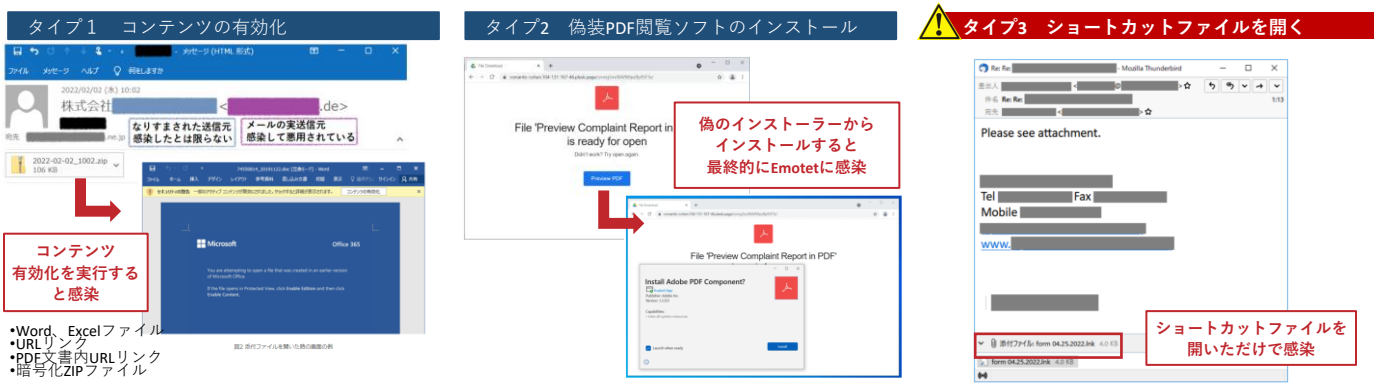


図2： Emotetに感染しメール送信に悪用される可能性のある.jp メールアドレス数の新規観測の推移（外部からの提供観測情報）

図3:確認されているEmotetの特徴／動向



Ⅲ． Emotetの感染経路

※2022年5月17日現在

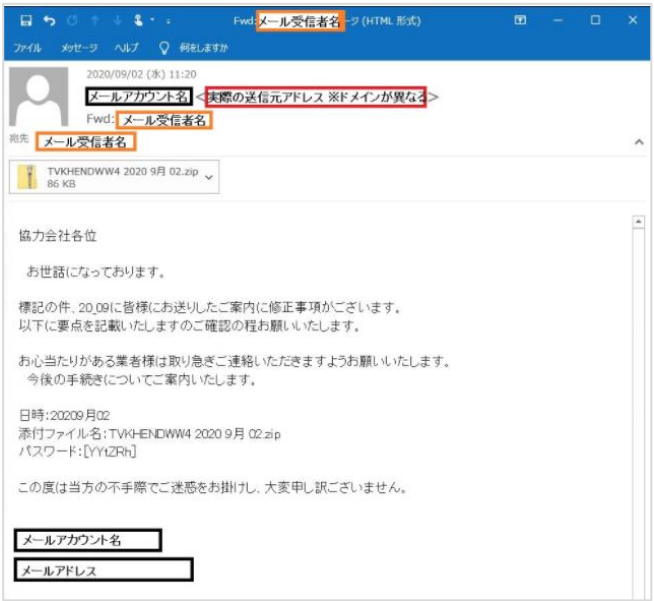
感染経路は、なりすましメールです。

特徴

- **メールアカウントがお取引様（組織内の社員）のメールアドレス**
- **メール本文内に自分が送ったメールが履歴で入っている。**
- **Officeファイルが添付されているか、URLリンクが記載されている。**
- **ショートカットアイコンが添付されている。**

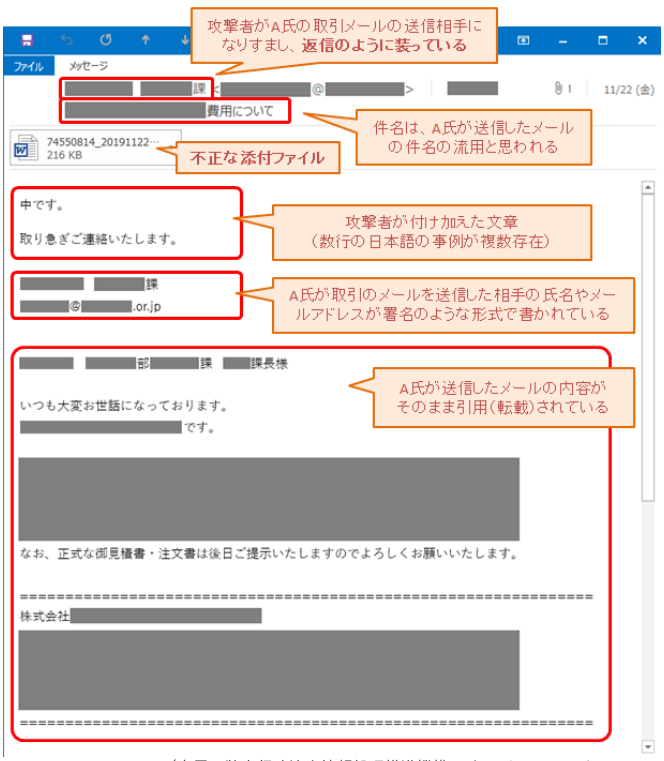
- なりすましメールによるマルウェアEmotetへの感染を狙う攻撃メールには、メール受信者のPCにEmotetを感染させるための悪性の添付ファイルがついています。 添付ファイルはOfficeファイル(Word、Excel）、ZIPファイルです。メールに添付されたOfficeファイルを受信者が開き、 画面に表示される「コンテンツの有効化」を実行することで Emotet への感染が発生します。
- 偽のウェブサイトの見た目や、ダウンロードさせられるファイルの種類など、細かい手口は変化していく可能性があります。
- また、新たな手口として**ファイルを開くだけで感染する「ショートカットファイルを悪用した攻撃」が確認**されています。

図4: 攻撃メール例　暗号化ZIPファイル



（出展：一般社団法人 JPCERT コーディネーションセンター
：パスワード付き ZIP ファイルが添付された Emotet のメール例）

図5: 攻撃メール例　主な特徴



（出展：独立行政法人情報処理推進機構 セキュリティセンター
：「Emotet」と呼ばれるウイルスへの感染を狙うメールについて）

新たな手口
ショートカットファイルを悪用した攻撃

2022年4月25日頃より、Emotetへ感染させる新たな手口として、ショートカットファイル（LNKファイル）の悪用を確認しています。**ファイルを開くだけでEmotetに感染する**ため、添付ファイルの取り扱いに注意が必要です。

（出展：独立行政法人情報処理推進機構 セキュリティセンター
：「Emotet」と呼ばれるウイルスへの感染を狙うメールについて　※最終更新日：2022年4月26日）

図6:ショートカットファイルを悪用する攻撃メールの例（2022年4月）

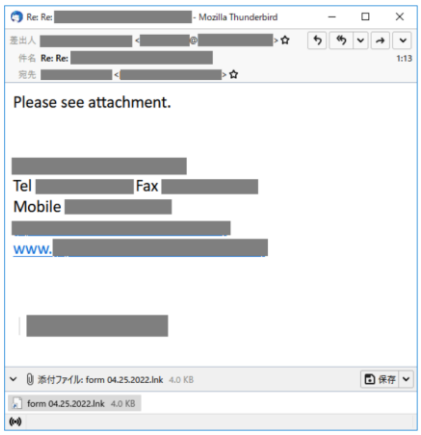
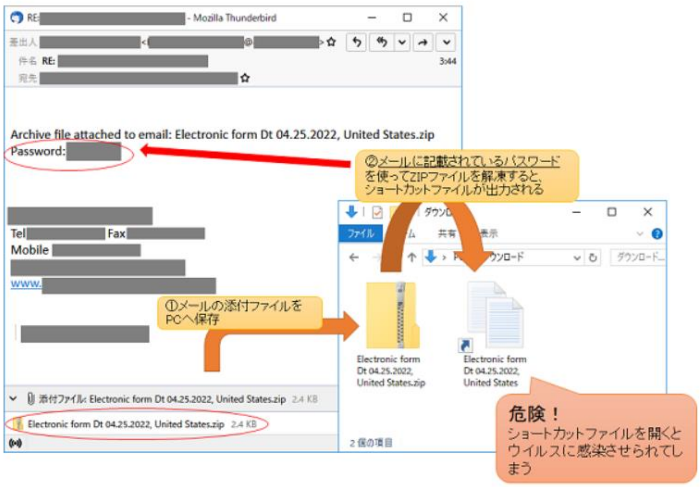


図7:ショートカットファイルが格納されたパスワード付きZIPファイルからEmotet感染までの流れ（2022年4月）



ショートカットファイルは、アイコンが文書ファイルのように偽装されていることや、Windowsの標準設定では拡張子が表示されないといった特徴から、見分けが付きにくい点に注意してください。

Ⅳ. すぐにできるEmotet対策

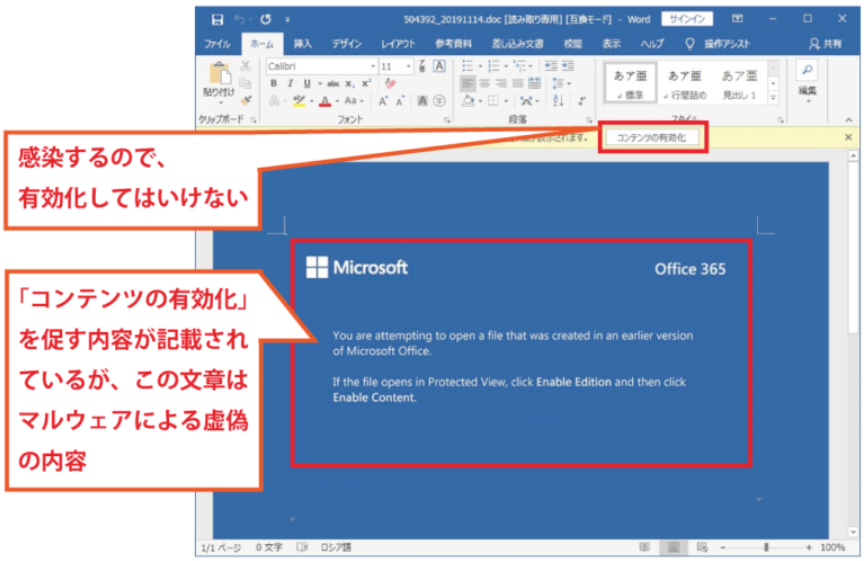
※2022年5月17日現在

［Emotet感染原因］

Officeファイルの添付ファイルを開き、「コンテンツの有効化」をクリックすると感染。

絶対に「コンテンツの有効化」は、クリックしないでください。

※なお、手口がショートカットファイルの場合はマクロ無効化に関係なく、
ファイルを開くと感染しますので添付ファイルの取り扱いには注意が必要です。



[図7: 添付ファイル例]
（出展：JPCERT/CC JPCERT-AT-2019-0044 マルウエア Emotet の感染に関する注意喚起　フーバーブレイン加工）

添付されたファイルには、Officeファイルの「コンテンツの有効化」を実行するように促す内容が記載されている場合がありますが、Emotetがダウンロードされ、感染が発生しますので、「コンテンツの有効化」を実行しないでください。
※Office の設定によっては、有効化の警告が表示されずに Emotet がダウンロードされる場合があります。

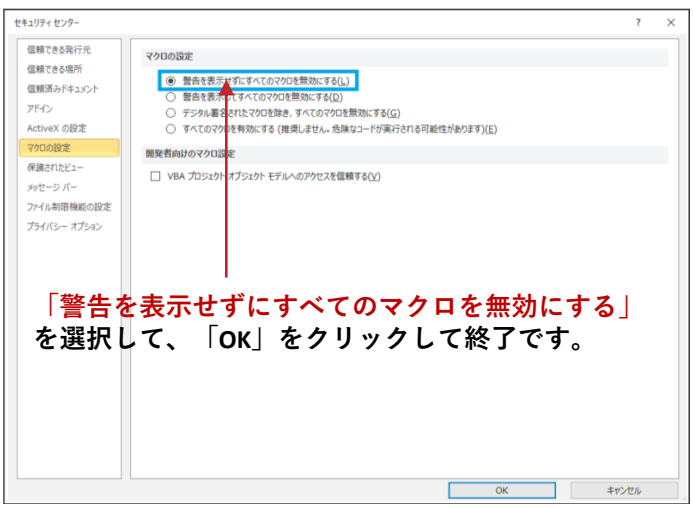
［参考情報］

「Officeマクロの自動実行の無効化」設定方法

1. [ファイル] タブをクリックします。
2. [オプション] をクリックします。
3. [トラストセンター**※1**] をクリックし、[トラストセンターの設定] をクリックします。
4. [トラストセンター] の [マクロの設定] をクリックします。
5. [警告を表示せずにすべてのマクロを無効にする]を選択する。
6. [OK] をクリックします。
7. 右の図は、トラストセンターの [マクロの設定] 領域です。

※1　お使いのOfficeのバージョンにより「トラストセンター」は「セキュリティセンター」の表記になっておりますが、手順は同じです。

[図8: Microsoft Office のトラストセンターのマクロの設定]



「警告を表示せずにすべてのマクロを無効にする」を選択して、「OK」をクリックして終了です。

※なお、MicrosoftはExcelやWordなどのOfficeファイルのマクロをデフォルトで無効にすると発表。（2022年2月7日）
※Office でインターネットから入手したマクロが既定でブロックされ、VBAマクロを含むファイルを開いた際の新たな通知メッセージ。有効にするためのボタンは出てこない仕様に変更される。2022年4月12日以降、プレビュー版を皮切りに順次変更を適用していく予定。（2022年4月27日）
Microsoft https://docs.microsoft.com/ja-jp/deployoffice/security/internet-macros-blocked

日々、気を付けておきたいこと

1. **受信メール・添付ファイルが信用できるものか慎重に判断し、正当性が判断できない場合は、**
   - **Word、Excel等の添付ファイルを開かない**
   - **「編集を有効にする」や「コンテンツの有効化」を実行しない**
2. **脆弱性を突いた攻撃に備え、OS、アプリケーション、セキュリティソフトを最新の状態に保つ**
3. **重要情報の定期的なバックアップ**

といった意識・対策が必要です。

Ⅴ． 2次感染拡大を防ぐために、お客様に実施していただきたいこと

早期対応が二次被害を最大限抑えることができます。

自組織の端末やシステムにおいて Emotet の感染が確認された場合、
被害拡大防止の観点より初期対応として次の対処を行うことを推奨します。

その異変を感じたら、

① まず、感染した（感染が疑われる）端末のネットワークからの隔離（重要）
② 電源は切らない（Windowsをシャットダウンしない）
③ 早急に、社内IT担当者／上司へ電話（口頭）で報告

自己判断はせずに、現状の状態を維持したまま、インフラ、セキュリティ関連窓口へ
ご相談ください。

- ネットワークから隔離した状態
- ウイルスソフトで隔離している際は、隔離している状態（除外・キャンセルはしない）
- 疑わしいメール等の履歴はそのまま残した状態
- 過去に作成したファイル等のデータを残した状態
- PCの設定等を変更しない

なお、必要に応じて、　（社内IT担当者の指示を仰いでください。）

- 感染した端末が利用していたメールアカウントのパスワード変更 **※1**
- 全端末のウイルス対策ソフトによるフルスキャン
- 端末のアカウントのパスワード変更
- ネットバンキング利用PCであればネットバンキングのパスワード変更 **※1**

※1 感染端末以外の「別の端末」でパスワード変更を行ってください。

お問い合わせ窓口

サポートセンターにてすべての初期対処を終了後、
基本的には感染した端末については初期化していただくこととなります。
PCのHDD内の重要なデータのバックアップをしていただくことを推奨します。

FuvaBrain製品　サポートセンター

サポート営業時間：10:00～17:00
（但し、土日祝祭日、夏季および年末年始の特別休暇期間、
止むを得ない事由によるサポート業務停止日/時間を除きます）

サポート電話受付窓口：050-5530-1261
（営業時間外のお問合せは翌営業日の受付・対応）

サポートEメール受付窓口：
support@fuva-brain.co.jp
（但し、時間外のお問合せは翌営業日の受付・対応）

JPCERT/CC、IPAの注意喚起情報

・JPCERT/CC　JPCERT-AT-2019-0044
マルウエア Emotet の感染に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190044.html

マルウエアEmotetへの対応FAQ
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

・IPA 独立行政法人情報処理推進機構
セキュリティセンター
「Emotet」と呼ばれるウイルスへの感染を
狙うメールについて
https://www.ipa.go.jp/security/announce/20191202.html