群馬県警察 Gunma Prefectural Police

サイバーポリスニュース

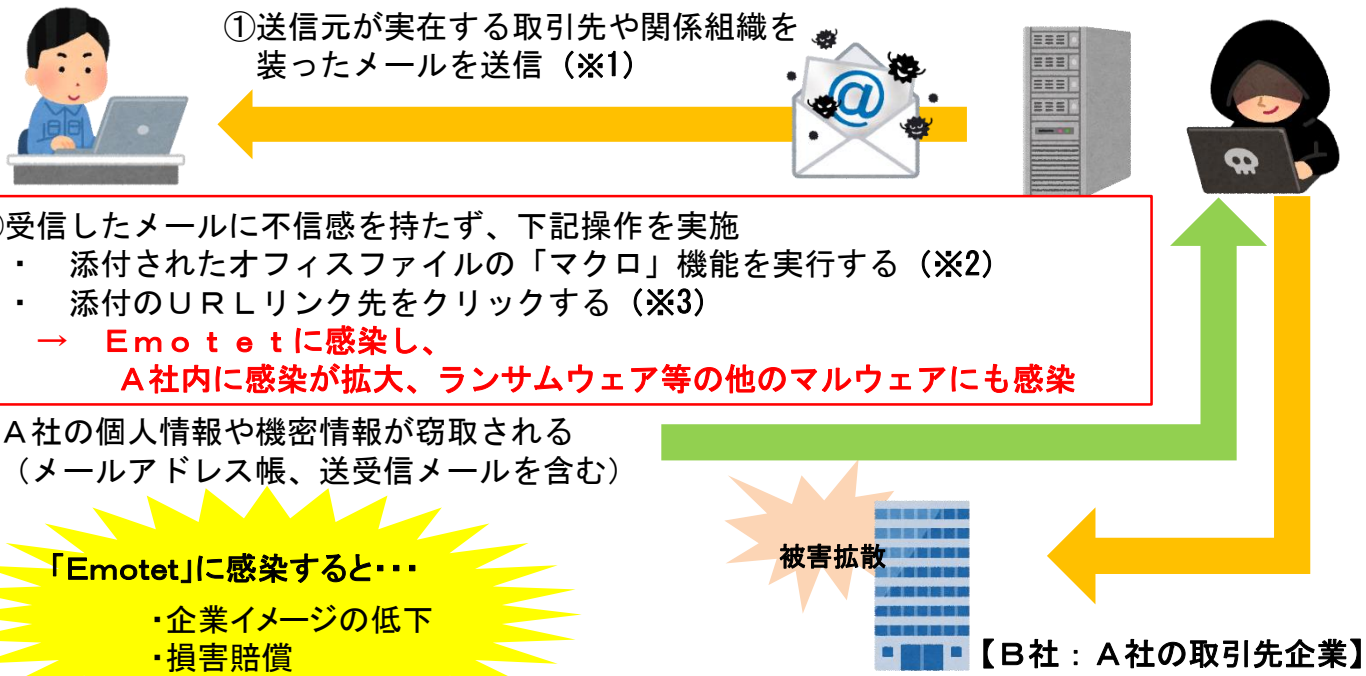
マルウェア「Ｅｍｏｔｅｔ」への注意！

令和４年２月上旬頃から「Ｅｍｏｔｅｔ（エモテット）」と呼ばれるマルウェアによるウイルス感染を狙う攻撃メールの再流行の兆しがあるとの報道があり、県内においても感染が確認されています。

「Ｅｍｏｔｅｔ」に感染すると、様々なマルウェア（「ランサムウェア」や「トロイの木馬」等）をダウンロードするため、情報流出等につながります。また、取引先等に被害を拡散してしまう危険性があります。

【重要：新たな手口】ショートカット（.lnk）ファイルを添付し、これを開くだけで感染させる手口が確認されています。（マクロの実行許可に依存しません！）

【Ｅｍｏｔｅｔ感染イメージ】



「Emotet」に感染すると・・・
- 企業イメージの低下
- 損害賠償
- 取引停止　等

大きなダメージを受けることになります！

送信されるメールの例　（※１）

2022/04/01　12:00

xxxxxxx<xxx@abc.jp>　← 実在する相手の氏名、メールアドレス

Re:請求書送付のお願い　← 正規のメールの返信を装う件名

宛先：zzzzzzz<zzzz@mpp.com>

添付ファイル

202204_御請求書.docm

いつもお世話になります。

御請求書を添付しますので確認ください。
色々とお手数おかけしますが、宜しくお願い致します。

メールだけでは不審点を見破れない場合も・・・

↑　「正規のメールの返信を装う内容」、「業務上開封してしまいそうな内容」

～ 被害に遭わないための注意！ ～

① 添付ファイルに注意（※2）

＜注意＞

- ○ 不用意に**「コンテンツの有効化」をクリックしない**でください。
- ○ マクロ機能により、不正プログラムが実行されてEmotetに感染します。

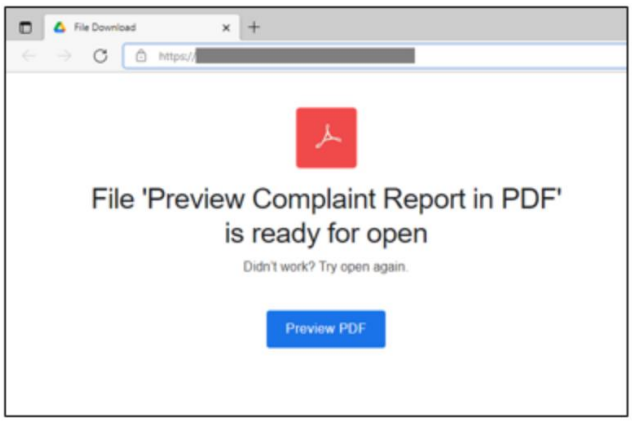
注 ショートカットファイルは、マクロの実行許可に依存しません！

Office 365

Emotet感染を狙う添付ファイルの多くは、マイクロソフト社のオフィスファイルです。

② 添付URLに注意（※3）

2021年11月、添付されたURLリンク先から不正プログラムをダウンロードさせる新たなEmotetの手口が報告されています。URLリンクをクリックするとPDFファイルが存在するかのような画面が表示され、PDFファイルの閲覧ソフトウェアを装ってEmotetをダウンロードさせ、利用者の手で実行させるものです。



← ＵＲＬリンク先の例

＜注意＞

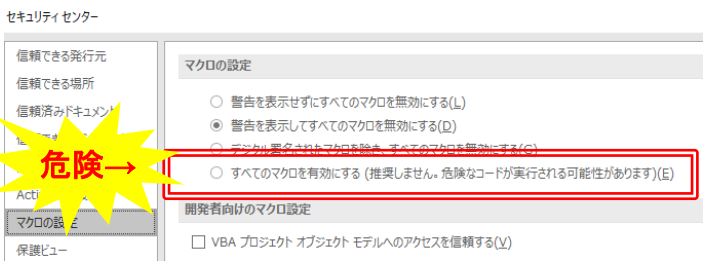
- ○ **添付されたURLリンク先から**不用意に**ソフトウェアをダウンロードしない**でください。
- ○ 今後、URLリンク先の見た目やダウンロードを促すファイルの種類等が変化していくことが予想されます。
- ○ **ソフトウェアのダウンロードは**、提供元の**正規サイトや信頼できるサイトから行って**ください。

引用 IPA情報処理推進機構 「「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」
https://www.ipa.go.jp/security/announce/20191202.html

～ 被害に遭わないための対策！ ～

○ オフィスのマクロ自動化を無効にする

オフィスファイルのマクロ設定が「すべてを有効にする」になっていないか確認しましょう。
（設定箇所 オプション→セキュリティセンター）
また、安易にマクロ機能を実行する「コンテンツの有効化」をクリックしないようにしましょう。



○ Windows Updateの実行

Emotet感染後、組織内のネットワークへ感染を広げる手口として、SMB（Server Message Block）の脆弱性が狙われることがあるため、OSを常に最新の状態にすることで感染リスクを低減しましょう。

○ サイバーセキュリティに関するリテラシーの向上（職員への周知事項）

- ・身に覚えのないメールや添付ファイルを安易に開かない（ショットカットファイルを含む）。
- ・不審な添付ファイルを開いてしまったり、「コンテンツの有効化」をクリックしてしまった場合は、すぐにシステム管理者等に連絡する。

※参考

Emotetの感染チェックに特化したツール「EmoCheck」がJPCERTコーディネーションセンターから無料で配布されています。ただし、感染チェック機能だけですので、駆除等の対応はできません。

＜ 群馬県警察サイバーセンター TEL027-243-0110 ＞