群馬県警察 Gunma Prefectural Police サイバーポリスニュース

ウイルス感染を狙うメールに注意！

令和４年２月上旬頃から「Emotet」（エモテット）と呼ばれるウイルスへの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おります。この攻撃メールは、過去に受信者がメールのやり取りをしたことのある

実在の相手の氏名、メールアドレス、メールの内容等の一部が、攻撃メールに流用され「正規のメールへの返信を装う」内容

となっている場合や

業務上の連絡と錯覚するおそれのある巧妙な文面

となっている場合がありますので、受信したメールの取扱いには注意してください。

対策

Check!

- **メールに添付されたファイルやURLリンクを安易に実行しない**
- **安易にコンテンツの有効化を実行しない**
- **身に覚えのない警告画面が表示された場合、その警告の意味が分からない場合は操作を中断する**

感染が疑われる場合

- **取引先等への速やかな連絡**
- **メールアカウントのパスワード変更**

Emotetの手口

① **取引先の企業等を装った業務に関係あるようなメールを受信**

2022/4/1(金)10:00

xxxxxxx<xxx@abc.jp> ← 実在の相手の氏名、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

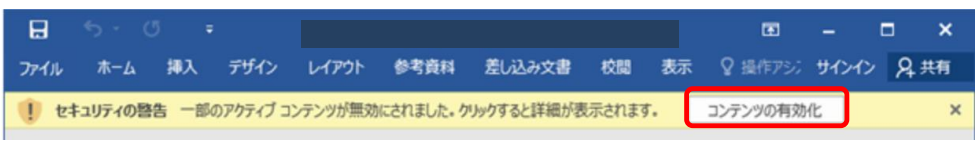
202204_御請求書.docx

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。

↑「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」

② **添付ファイルを開く（Wordファイルの場合）**



絶対にクリックしない！

増加中

パスワード付きZIPファイルに注意

2022/4/1(金)10:00

xxxxxxx<xxx@abc.jp>　← 実在の相手の氏名、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

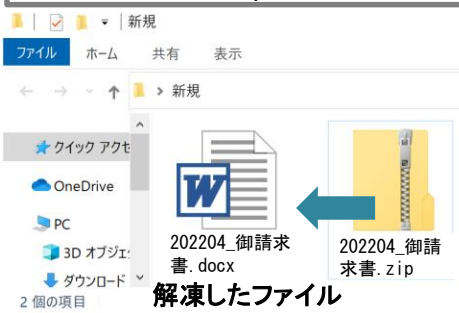
宛先：zzzzzzz<zzzz@mpp.com>

添付ファイル

202204_御請求書.zip

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。
ファイル名：202204_御請求書.zip
パスワード：zaq12wsx　← 「ZIPファイルのパスワードを本文に記載」



解凍したファイル

解凍したWordファイルを開くと、前頁のセキュリティの警告画面が表示されます。

ウィルスが仕込まれているOffice文書ファイルが直接添付されている場合、ウイルス対策ソフト等で検知されることがありますが、**パスワード付きZIPファイルは検知されないため、ZIPファイル内のファイルの取扱いには十分な注意が必要**です。

③ 不正なマクロ（プログラム）を実行してしまうと・・・

不正なマクロを実行すると、パソコンがウイルスに感染し、自組織だけでなく、関係各所にも影響を及ぼす可能性があります。

＜影響＞

- メールアカウント情報、送受信メール内容、アドレス帳等の情報が流出
- パソコンやブラウザに保存されたパスワード等の認証情報が窃取される。
- ウイルス感染が自組織内（端末、スマートフォン、USB等の機器）へ広がる。
- Emotetのメールをばらまくための踏み台にされる。
  （アドレス帳等の情報から関係先にEmotetのメールを送信され、被害が拡大）
- 別のマルウェアに感染する。

情報流出・組織の信用低下

- ＯＳやソフトウェア、アプリケーションを常に最新の状態へアップデートしましょう。
- 最新のセキュリティパッチを適用したり、ウイルス対策（セキュリティ）ソフトに最新の定義（パターン）ファイルを適用しましょう。
- 管理者権限以外でのＷｉｎｄｏｗｓＰｏｗｅｒＳｈｅｌｌを無効化にしましょう。

＜ 群馬県警察サイバーセンター TEL027-243-0110 ＞