群馬県警察 Gunma.Pref.Police
部外用

サイバーセキュリティ対策通信 令和２年度 第３号

ウィルスへの感染を狙うメールが急増！

「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が、日本国内の企業や組織へ広く送りつけられています。

特に、攻撃メールの受信者が過去に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

業務上開封してしまいそうな巧妙な文面

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。

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

2020/09/01(火)11:30

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

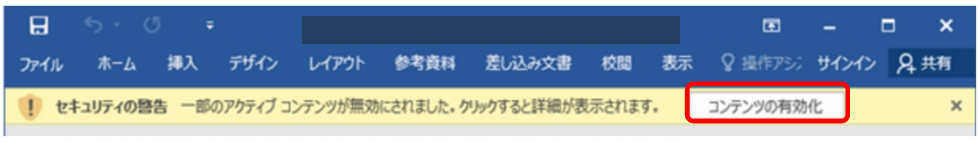
2020090_御請求書.doc

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！

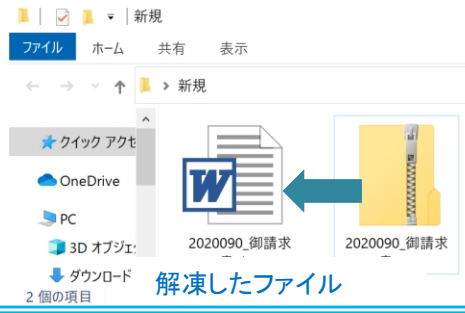
注意

WordやExcel等のマイクロソフトのオフィスファイルにマクロ（プログラム）が埋め込まれていた場合、ファイルを開くと「**セキュリティの警告**」がメニューバーの下に表示されます。

表示される「**コンテンツの有効化**」をクリックすると、マクロの実行を許可することになり、悪意のあるプログラムが動作し、ウィルスに感染してしまいます。

増加中！ また、最近増加している手口は、マイクロソフトのオフィスファイルが直接添付されているのではなく、パスワード付きZIPファイルが添付されているものです。

2020/09/01(火)11:30
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
添付ファイル
宛先：zzzzzzz<zzzz@mpp.com> 2020090_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：2020090_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マイクロソフトのオフィスファイルが直接添付されている場合、メール送信経路上にあるセキュリティ製品で検知・検疫されることがありますが**ZIPファイルは検知等されず、受信者に届いてしまう場合が多いので、取扱いには注意が必要**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、パソコンがウィルス感染し、下記のとおり、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流出
- ・ウィルス感染が自組織内へ広がる
- ・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）

情報流出・組織の信用低下

対策

- ・組織内で添付ファイルのマクロを安易に実行しないように注意喚起しましょう。
  （他組織へマクロを埋め込んだファイルを送信することは稀ですので、セキュリティの警告が表示された場合、送信先にマクロの有無を問い合わせましょう。）
- ・マイクロソフトのオフィスファイル設定で、マクロの設定を無効にしましょう。
- ・最新のセキュリティパッチを適用したり、ウイルス対策ソフトにも最新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。

＜群馬県警察本部警務課サイバーセキュリティ対策係 TEL027-243-0110 ＞