事務所ニュースNews
2022.4
K-032
発行：税理士法人　行本事務所

経営バイタルの強化書 KEIEI VITAL

Emotetに気をつけましょう!

情報セキュリティ10大脅威とEmotet対策

3月に入り「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被害が急増しています。「Emotet」の被害を拡大しないためにも、添付ファイルの開封には十分注意しましょう。

情報セキュリティ10大脅威の内容とEmotetへの対応ついて理解しましょう!

1 情報セキュリティ10大脅威

IPA（独立行政法人情報処理推進機構）は、2022年1月27日「情報セキュリティ10大脅威2022」を公開し、2月28日に個人編の解説書を公開しました。「情報セキュリティ10大脅威2022」は情報セキュリティ対策の普及を目的として、2006年から前年に発生した情報セキュリティ事故や攻撃の状況等から脅威を選出し、上位10位を公表しているものです。「個人」の立場と「組織」の立場でのランキングはそれぞれ【図1】のようになっています。

個人の順位では、順位の変動はあるものの、脅威の内容は昨年、一昨年と全て同じとなっています。2019年から2年連続2位にランクインしていた「フィッシングによる個人情報等の詐取」が今回初めて1位になりました。フィッシング詐欺は、実在する公的機関や有名企業を騙ったメールやショートメッセージサービス（SMS）等を送信し、正規のウェブサイトを模倣したフィッシングサイト（偽のウェブサイト）へ誘導することで、個人情報や認証情報等を入力させる詐欺です。また、大手ECサイトや金融機関などを騙った手口が多く確認されました。

一般社団法人フィッシング対策協議会が3月3日に公開した2022年2月のフィッシング報告状況によれば、Amazonを騙るフィッシングは報告数全体の約39.2%を占めており、次いで報告数が多かったメルカリ、JCBを騙るフィッシングの報告も含めた上位3ブランドで、報告数全体の約56.6%を占めています。また1,000件以上の大量の報告を受領したブランドは10ブランドあり、これら上位10ブランドでは全体の約74.2%を占めています。最近では、NTTドコモやえきねっと（JR東日本）を騙るフィッシングについても報告されています。

フィッシングに悪用された87ブランドのうち、クレジット・信販系は21ブランドとなり、前月に引き続きクレジットカードブランドを騙るフィッシングが多く、都市銀行やネット銀行など金融系ブランドは5ブランドとなっています。ISPやホスティング事業者、メールサービスについては15ブランドと増えており、詐取されたアカウント情報が不正なメール配信等に使われている可能性があります。また、1月と比較してキャッシュレス決済サービスを騙るフィッシングの報告は約1.6倍、モバイルキャリアを騙るフィッシングの報告は約3倍となっています※2。

3月より感染被害が急拡大しているEmotetと呼ばれるウイルスに感染すると、上記のような被害にあう恐れがあります。安易にURLをクリック・タップしない、サービスを利用する際は自身のブックマークや公式アプリからアクセスするなど、利用者は日ごろから注意が必要です。

【図1】情報セキュリティ10大脅威 2022※1

昨年順位	「個人」向け脅威	順位	「組織」向け脅威	昨年順位
2	フィッシングによる個人情報等の詐取	1	ランサムウェアによる被害	1
3	ネット上の誹謗・中傷・デマ	2	標的型攻撃による機密情報の窃取	2
4	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3	サプライチェーンの弱点を悪用した攻撃	4
5	クレジットカード情報の不正利用	4	テレワーク等のニューノーマルな働き方を狙った攻撃	3
1	スマホ決済の不正利用	5	内部不正による情報漏えい	6
8	偽警告によるインターネット詐欺	6	脆弱性対策情報の公開に伴う悪用増加	10
9	不正アプリによるスマートフォン利用者への被害	7	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
7	インターネット上のサービスからの個人情報の窃取	8	ビジネスメール詐欺による金銭被害	5
6	インターネットバンキングの不正利用	9	予期せぬIT基盤の障害に伴う業務停止	7
10	インターネット上のサービスへの不正ログイン	10	不注意による情報漏えい等の被害	9

NEW：初めてランクインした脅威

2 Emotetとは

Emotetは情報の窃取に加え、更に他のウイルスへの感染のために悪用されるウイルスであり、悪意のある者によって、不正なメール（攻撃メール）に添付される等して、感染の拡大を試みます。

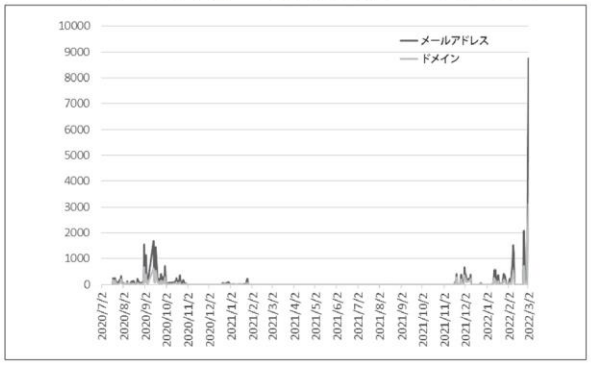
Emotetは2021年1月27日、EUROPOL（欧州刑事警察機構）が、欧米８カ国の法執行機関・司法当局の協力により、Emotetの攻撃基盤（ウイルスメールをばらまいたり、感染したマシンを操作するための機器等）をテイクダウンした（停止させた）と発表し、その攻撃や被害が停止あるいは大幅に減少していましたが、2021年11月後半から、Emotetの攻撃活動再開の兆候が確認されたという相談がJPCERT/CC（JPCERTコーディネーションセンター）に寄せられており、IPA（独立行政法人情報

裏面へ続く→

処理推進機構）や警視庁サイバーセキュリティ対策本部からも注意喚起が出されていました。

沖縄県や日本気象協会、東北海道いすゞ自動車、リコー傘下のリコーリース（東京都千代田区）、教育系NPOのアスクネット（名古屋市）、韓国食品の農心ジャパン（千代田区）、業務用調理機器のフクシマガリレイ（大阪市）など多岐にわたる組織がEmotet感染についてのプレスリリースを出しています。

【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）（2022年3月3日更新）※3



3 Emotetに感染した場合の影響

Emotetに感染した場合、次のような影響が発生する可能性があります。

- コンピュータ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
- 窃取されたパスワードを悪用されネットワーク内に感染が広がる
- メールアカウントとパスワードが窃取される
- メール本文とアドレス帳の情報が窃取される
- 窃取されたメールアカウントや本文などが悪用され、Emotetの感染を広げるメールが送信される

このようにEmotetに感染してしまうと、感染したコンピュータから情報が窃取された後、攻撃者側から取引先や顧客に対して感染を広げるメールが配信されてしまう恐れがあります。また、感染したままのコンピュータが組織内に残留すると、感染を広げるメールの配信元として攻撃者に利用され、外部に大量の不審メールを送信することになります。

Emotetに感染したコンピュータが別のウイルスをダウンロードし、結果としてランサムウエアに感染してデータが暗号化されるなどの被害に繋がるケースも報告されています。

Emotetへの感染を防止するためには、下記のような一般的なウイルス対策の徹底が必要となります。

- 身に覚えのないメールの添付ファイルは開かない。メール本文中のURLリンクはクリックしない。
- 自分が送信したメールへの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かない。
- OSやアプリケーション、セキュリティソフトを常に最新の状態にする。
- 信頼できないメールに添付されたWord文書やExcelファイルを開いた時に、マクロやセキュリティに関する警告が表示された場合、「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない。
- メールや文書ファイルの閲覧中、身に覚えのない警告ウインドウが表示された際、その警告の意味が分からない場合は、操作を中断する。

4 Emotetの対策

Emotetに感染しているかどうかを確認するために、JPCERT/CCでは、EmoCheckというツールを公開しています※4。

感染が疑われるコンピュータ上でEmoCheckツールを実行し、「Emotetは検知されませんでした」と表示されていた場合には、Emotetに感染していません【図3】。「Emotetのプロセスが見つかりました」と表示されていた場合には、Emotetに感染していますので、JPCERT/CCに掲載されている「感染時の対応」により対応を行うことが必要です。感染が確認された場合には、以下の対応が必要となります※5。

【図3】EmoCheckによりEmotetが検知されなかった例※5

①感染端末の隔離、証拠保全、および被害範囲の調査

感染した端末を証拠保全します。端末に保存されていた対象メール、およびアドレス帳に含まれていたメールアドレスを確認します（端末に保存されていたこれらの情報が漏えいした可能性があるため）。

②感染した端末が利用していたメールアカウントなどのパスワード変更

OutlookやThunderbirdなどのメールアカウント、Webブラウザに保存されていた認証情報などを変更します。

③感染端末が接続していた組織内ネットワーク内の全てのコンピュータを調査

横断的侵害で組織内に感染を広げる能力を持っているため、添付ファイルを開いたコンピュータだけでなく、ネットワークに接続している他のコンピュータも併せて調査を実施します。

④ネットワークトラフィックログの監視

感染したコンピュータを隔離できているか、他の感染コンピュータがないかを確認します。

⑤他のウイルスへの感染有無の確認

Emotetは別のウイルスに感染させる機能を持っているため、Emotet以外にも感染していたかどうかを調査します。もし、別のウイルスに感染していた場合には、更なる調査・対応が必要となります。日本では、Ursnif、Trickbot、Qbot、ZLoaderなどの不正送金マルウエアの追加感染の事例があり、海外では、標的型ランサムウエアの感染などの事例あります。

⑥被害を受ける（攻撃者に窃取されたメールアドレス）可能性のある関係者への注意喚起

①の調査で確認した対象メール、およびアドレス帳に含まれていたメールアドレスを対象にして関係者へ注意喚起と上述EmoCheckを利用した感染確認と対応を行います。不特定多数の場合は、プレスリリースなどでの掲載が必要です。

⑦感染した端末の初期化

感染したコンピュータの初期化を行います。

※1 情報処理推進機構「情報セキュリティ10大脅威 2022」（URL：https://www.ipa.go.jp/security/vuln/10threats2022.html）
※2 フィッシング対策協議会「2022/02 フィッシング報告状況」（URL：https://www.antiphishing.jp/report/monthly/202202.html）
※3 JPCERT/CC「マルウェアEmotetの感染再拡大に関する注意喚起」（URL：https://www.jpcert.or.jp/at/2022/at220006.html）
※4 「EmoCheck」（URL：https://github.com/JPCERTCC/EmoCheck/releases）
※5 JPCERT/CC 公式ブログ「マルウエアEmotetへの対応FAQ」（URL：https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html）