

❖ IPA、『Emotetの攻撃活動再開について』追記 ❖

Emotet（エモテット）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、感染の拡大が試みられています。

Emotetへの感染を狙う攻撃メールの中には、正規のメールへの返信を装う手口が使われている場合があります。これは、攻撃対象者（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流用された、あたかもその相手からの返信メールであるかのように攻撃メールです。このようなメールは、Emotetに感染してしまった組織から窃取された、正規のメール文面やメールアドレス等の情報が使われていると考えられます。すなわち、Emotetへの感染被害による情報窃取が、他社に対する新たな攻撃メールの材料とされてしまう悪循環が発生しているおそれがあります。

なお、正規のメールへの返信を装う手口の事例はこの他にもあり、例えば2018年11月、Emotetとは異なるウイルスへの感染を狙う日本語の攻撃メールでも悪用されたことを確認しています。今後もこの手口は常套手段となりうることから、注意が必要です。

■ Emotetの攻撃活動再開について（2021年11月16日 追記）

2021年11月14日頃から、Emotetの攻撃活動再開の兆候が確認されたという情報があります。また、Emotetへの感染を狙う攻撃メール（Emotetの攻撃メール）が着信しているという情報も複数観測している状況です。

IPAでは、攻撃メールに添付されていたと思われるWord文書ファイルとExcelファイルを入手し、確認しています。これらは悪意のあるマクロ（プログラム）が仕込まれたもので、今年1月までの攻撃と同様の手口です。引き続き、特にメールを経由して入手したOffice文書ファイルについて、信用できると判断できる場合でなければ、「編集を有効にする」「コンテンツの有効化」というボタンはクリックしないよう注意してください。

今後、攻撃メールの大規模なばらまきに発展する可能性もあります。2019年から2020年にかけて、多くの企業・組織が被害に遭いました。念のため、警戒を尾お願いします。

- 「IPA（独立行政法人 情報処理推進機構）ホームページ」より-

＊今月の豆知識＊

～「おせち料理」の具材のそれぞれの意味～

新型コロナウイルスが拡大し、昨年のお正月は自宅で過ごす人が増えたこともあり、「おせち料理」を利用する人が増加したそうです。今年は昨年以上に好調とも言われています。おせち料理の具材の種類は、全部で20～30種類あり、それぞれにおめでたい意味やいわれがあります。いくつかの具材の意味をご紹介します。

- ＊ 鯛・・・「めでたい」の語呂合わせ
- ＊ 黒豆・・・邪気払い
- ＊ 数の子・・・子孫繁栄
- ＊ 田作り・・・五穀豊穡
- ＊ 鱈の照り焼き・・・立身出世
- ＊ 海老・・・長寿
- ＊ 昆布巻き・・・「よろこぶ」に通ずるとされており、縁起が良いもの
- ＊ 栗きんとん・・・勝負運、金運、商売繁盛をもたらす縁起物
- ＊ 伊達巻き・・・巻物に似ていることから、知識が豊富になるようにとの願いが込められています
- ＊ 紅白かまぼこ・・・日の出を象徴する色と形。紅白の紅は魔除けや喜び、白は神聖な意味があります





赤松事務機株式会社
代表取締役 片松 保佳

『社長のつぶやき』

12月になりました。早いですね～。もう一年が終わろうとしています。10月から色々な制限が緩和されてから一気にスピード感が増した気がします。皆様いかがお過ごしでしょうか？

2021年も色々なことがありました。昨年に引き続きのコロナ禍・東京オリンピック・政権交代……。社会活動は制限が多くかかっていましたが世の中はどんどん変わっていきました。何にも行動を起こさないとすぐに置いていかれるような一年でした。その中でも2年にわたるコロナ禍が日本においては沈静化し始めたのは良いニュースでした。会食や人の往来の制限も緩和され、12月は忙しくされている方も多いと思います。今まで大変な思いをされておりました飲食業や旅行・宿泊業の皆様におかれましても例年までとはいかないまでも回復の兆しが見え始めているのではないのでしょうか？そんなこんなで私も久しぶりに東京出張に行って参りました。

12月7日(火) 情報セキュリティ企業様訪問 今後の事業展開についてのミーティング @東京

訪問先の社長様とは数年来のお付き合いがあり、情報セキュリティ対策に関しては書籍の出版・コメンテーターとしてのTV出演・コラムの執筆など幅広く活躍されている方です。その社長様は「Emotetをはじめとする暗号化ウイルスに感染してデータを読み取れなくなったとの相談を毎日のようにいただいております」とおっしゃっていました。日頃から最新の情報セキュリティに対しての情報収集と対策の意識を持ち続けることが大切とも指摘されておりました。そして移転されたばかりのオフィスもご案内いただき（最新の都会のシェアオフィスでした!!!カッコいい!!!）、オフィス家具提案のヒントになるようなレイアウトも勉強させていただきました。・・・やっぱり東京の最先端オフィスは違います。

久しぶりに出張に行って感じたことは「やっぱり直接対面で会うと話の広がりやオンラインと全然違う」「やっぱり現場に行かないと雰囲気は分からない」の2点です。実際にお会いすると雰囲気・表情・声のトーンで感じ取れることが違います。やっぱり人間は意識なくとも五感をフルに使って置かれた状況を理解し、最適な判断をする動物なんだと再認識しました。やっぱりリアルは良いです。今後はリアルとバーチャルの使い分けが大事ですね。何かとバタバタする年末ですが、皆様が大過なく新しい年を迎えられますようご祈念申し上げます。

IT用語

知っておいて損はしない！かも・・・

■ リカバリ ■

「リカバリ」とは、PCを工場出荷時の初期状態に戻すことや、障害が発生したコンピュータ・システムなどを復旧、回復、修復することです。

OSやソフトウェアなどをアンインストールして、再度インストールし直したり破損したハードディスクを入替えたり、データを取り出したりします。

リカバリを行うと、PC内のテキストデータ・写真・動画など全てのデータが消去されるため、外付けのハードディスクなどに、必要なデータのバックアップを取る必要があります。

リカバリ作業でかかる時間は、リカバリ作業の内容や進行の度合いなどにもよりますが、2時間～数時間、それ以上時間がかかることもあります。

リカバリが完了したPCに、バックアップしておいたデータを入れ直す場合、その設定などに時間がかかります。

弊社では、情報セキュリティ対策商品、UTM(統合脅威管理)等の取扱いをしております！
HPでも紹介しておりますのでぜひご覧頂ければと思います!!!
対策は早目にしましょう！

