

2022年3月4日
一般社団法人シルバーサービス振興会

不審メール マルウェア『Emotet (エモテット)』に関するお知らせ【情報提供】

平素よりお世話になっております。

独立行政法人情報処理推進機構 (IPA) 等の注意喚起情報によりますと、最近、マルウェア「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、国内の組織へ広く着信しており、国内の組織等における感染が増加し、警戒が必要な状況であるとのことでございます。

最近、弊会においても、「弊会から送信していない不審なメールが届く」という事案が発生しておりますため、本件に関する情報提供をさせていただきます。

具体的には、差出人、件名、本文などに「介護技能実習評価試験」「キャリア段位」といった文字のみが入り、ZIP ファイルなどが添付されている不審なメールが出回っているようです。

このようなメールを受信された場合には、メールを開封せず、必ず削除してください。

また、添付ファイルは絶対に開かないようにしてください。

○ Emotet (エモテット) とは

感染した端末のメールの情報を窃取し、それを悪用してメール経由で感染を拡大していくマルウェアです。

主に実在の組織や人物になりすましたメールにファイルを添付する手口で、感染を拡大させる特徴を持ち、正当なメールと見分けがつきにくい特徴があります。

不審メールの見分け方として、送信者の氏名表示とメールアドレスが異なっている特徴があります。

弊会からのメールは「*****@espa.or.jp」を使用しておりますので、弊会名義の不審メールを受信された場合には、送信者アドレスのご確認をいただいた上で、@マーク以下が

「@espa.or.jp」以外の場合には添付ファイルを開封したり、URL をクリックせずにメールごと削除をお願い申し上げます。

また、弊会からメール送信をする際には、添付ファイルの開封パスワードを文面に記載することはしておらず、必ず開封パスワードは別送しておりますのでご確認下さい。

<なりすましメールの例>



○ ご参考

Emotet（エモテット）の詳細については、独立行政法人情報処理推進機構（IPA）並びに警視庁の下記サイトをご参照ください。

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>

ここからセキュリティ！～ウイルス(マルウェア)に感染したら～

<https://www.ipa.go.jp/security/kokokara/accident/index.html>

警視庁サイバーセキュリティ ad 資料

https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/CS_ad.html

以上