作成　令和３年１月１４日

【F-CSNET 通信かわら版】
【表題：新型コロナウイルス感染症に関連した標的型メール攻撃に注意】

中小事業者の皆様へ
攻撃者がマルウェアに感染させる代表的な手口が「メール」です。
そして、攻撃者はメールを受け取った受信者がそのメールを開封し、添付されたファイルや URL リンクに誘導するために「不安感」等の人心を巧みに突いてきます。

１　コロナ禍に関連した不審なメール（国内確認事例）

○　国立感染症研究所に類似した架空の団体名を称したメール
新型コロナウイルス感染症の注意喚起とともに、不審な URL へのリンクが付いたメールが、「国立感染症予防センター」という実在しない組織名義で個人宛に送信されていることを確認されています。

○　保健所を騙ったマルウェア「Emotet」に感染させるメール
メールの情報を盗む機能等を有するマルウェア「Emotet」への感染を目的としたメールについて、昨年、実在の保健所を騙り、新型コロナウイルスの予防対策を要請する内容のものが確認されています。
Emotet は、「給与」「賞与」「クリスマス」等時期によって題材が変化しており、引き続き警戒が必要です。

○　総務省を騙った特別定額給付金に関するフィッシングメール
2021 年 1 月 7 日、総務省を騙るメールが確認されました。
攻撃者は、個人情報や金融機関等の情報窃取を狙い、政府による緊急事態宣言の再発令にあわせて、総務省を騙るフィッシングサイトを立ち上げているとみられます。

２　被害に遭わないために

○　心当たりのないメールや SMS は開かない
○　メールや SMS の内容は安易に信用しない
○　メールや SMS に添付されたファイルや URL は安易に開封しない、接続しない

★　突然受信した添付ファイル付きメール…送信元に「電話で」確認するとより安全。
メール返信による問い合わせやメールに記載された電話番号から問い合わせは厳禁。あらかじめ把握している電話番号や、信頼できる Web サイト（企業公式サイト）から確認をしましょう。

★　マルウェア「Emotet」付きのメールは、過去実際にやり取りのあった人物を騙って送信されています。送信者名と送信元のメールアドレスの確認をしましょう。

★　「Emotet」は、マクロの有効化によって感染します。マクロの有効化（コンテンツの有効化）やマクロの自動実行は避けましょう。

★　F-CSNET は、公的機関（九州経済産業局地域経済部情報政策課、福岡県警察本部生活安全部サイバー犯罪対策課、福岡県商工部中小企業振興課）と、４つの中小事業者支援団体とが連携し、県内中小事業者を対象に、サイバー犯罪の被害防止等に的確に対応することを目的として発足したネットワークです。

★　福岡県警察サイバー犯罪対策課では、随時情報をホームページに掲載していますので、是非ご覧ください。

https://www.police.pref.fukuoka.jp/seian/cyber/index.html