事務所News ニュース
2021.10
K-026
発行：佐園達哉税理士事務所

経営バイタルの強化書 KEIEI VITAL

コロナ禍を悪用する詐欺メール被害が広がっています

新型コロナウイルスを題材とした攻撃メール

新型コロナウイルス感染症は新規感染者数が減少してきているものの、先の見えない状況が続いています。また、通販や宅配利用などの新しい生活様式が定着しつつあります。こうした中で、新型コロナウイルス感染症に関連したワクチン接種予約や国立感染症研究所に類似した機関による、新型コロナウイルス感染症の注意喚起を装うメール、通信販売をめぐるトラブル、クレジットカードブランドをかたるフィッシング、宅配業者を装った偽のSMS等の被害が多発しています。このような被害にあわないように不審なメールや電話には十分な注意を払いましょう。

ワクチン接種情報や特別定額給付金等の偽メールが増加しています

1 新型コロナウイルス感染症対策に直接関係する詐欺メール

新型コロナウイルス感染症に対応するため、ワクチン接種や感染防止対策を行い、三密を避けるため外出機会を減らし、通信販売を利用するなどいわゆる新しい生活様式が励行されています。このような状況に乗じて、ワクチン接種やコロナウイルスに対する注意喚起、支援金・給付金等新型コロナウイルスに直接関係する詐欺メールや通信販売や宅配業者を装った詐欺メールが横行しています。

詐欺メールは、フィッシング詐欺、クリック詐欺、なりすましメール等とも言われますが、偽のウェブサイトに誘導し、IDやパスワード、クレジットカード番号等の個人情報を盗み取り不当な請求等を行うことを目的としています。

金銭的な被害にあわない場合でも、IDやパスワードを盗まれてしまうと、今まで使用していたウェブ上のサービスの利用ができなくなり、再び利用ができるようになるまでにかなりの時間を要する場合もあり、その間通常利用していたサービスが利用できなくなる等の大きな不利益を被ることになります（例えばAppleIDを盗まれてしまうと、場合によっては復旧までに数か月を要することがあり、復旧までの間は利用していたサービスが全て使えなくなってしまいます）。AppleIDやGoogle、Facebookアカウント等最近では複数のサービスと紐づいたID、アカウントがあり、一度盗まれてしまうと紐づいているサービスの利用を全て停止しなければならなくなり多大な不利益を被ります。

フィッシング詐欺とは、国や地方公共団体、ネットバンキングやクレジットカード会社、有名企業になりすまして個人情報をだましとる詐欺の手口で、企業等からのお知らせメールを装い、本物そっくりに偽装したホームページへ誘導し、ログインID、パスワード、クレジットカード番号などの個人情報を入力させます。情報をだましとられてしまうと、いつものサイトにログインしたつもりで、後日オンラインバンクの預金残高がなくなっていたり、ログインパスワードが勝手に変更されるなどの状況になってから、はじめて被害に気づく場合が多いとされています。通常は、国や地方公共団体、企業がメールでIDやパスワードなどの個人情報を求めることはありません。もし、そのようなメールを受け取った場合は、まず、その団体のウェブサイトで問い合わせ先を確認し、窓口に直接確認するなどの慎重な対応が必要です。以前は、見た目が本物と異なるウェブサイトや日本語表記が怪しいウェブサイト等が大半でよく観察することで被害を防ぐことができましたが、最近では本物とそっくりでかなり注意しないと偽サイトであることがわからないものが増えてきています【図1】※1。

【図1】佐川急便「佐川急便を装った迷惑メールにご注意ください」※1

フィッシング詐欺は当初、主に海外で被害が急増していましたが、国内でも2009年以降、銀行を装ったフィッシングメールによる被害が報告されました。以後メールを利用した詐欺の手法として目立つようになってきたことを背景に、他人のIDやパスワードの使用などを規制する不正アクセス禁止法において、フィッシング詐欺の処罰化などを盛り込んだ改正案が2012年3月30日に可決、成立しました。しかし法規制だけではフィッシング詐欺の抑止となっても、すべての根絶はむずかしいため、自分の個人情報を守るためには自衛の意識が必要です。

クリック詐欺とは、広告宣伝メール等に記載されたURLをクリックすると過大な料金請求などを行う手法です。迷惑メールのURLをクリックしただけでいきなり「会員登録が完了しました」「入会金○○円です」などと記載された画面が表示され、驚いた閲覧者から金銭を振込ませ、だまし取るというものです。最近はより手口が巧妙になり、1度のクリックではなく4回程クリックさせページを変えていく中に、こっそり規約へのリンクを表示させて、規約に料金が発生することはきちんと書いてあったと一方的に主張するようなものもあります。ウェブサイトを利用する際は、あらかじめ利用規約をしっかり探し、「有料なのか、無料なのか」「あやしい表示がないか」を確認しておきましょう。

裏面へ続く→

パソコンメールは、メールソフトで送信者アドレスを自由に設定できるので、知り合いや有名企業などを装った「なりすましメール」が可能です。そのため、送信者アドレスが、自分のアドレスになっている迷惑メールがあり、受け取った人は驚いてメールを確認してしまったということがよくあります。まさか自分のアドレスで迷惑メールを送られているのでは？と心配になる人もいるかもしれませんが、あなたのアドレスで迷惑メールが大量に送信されている訳ではないので、安心してください。これは迷惑メールを送信する際に、送信者アドレス（Fromアドレス）が宛先アドレス（Toアドレス）と同一となるソフトを使用して送られたもので、受け取った人の気を引いてメールを確認させるためや送信者の身元をわかりづらくしてアドレスによるフィルタリングを回避するためと思われます※2。

2 詐欺メールの事例

フィッシング詐欺、クリック詐欺、なりすましメールは複数を組み合わせて行われることも多く、件名や内容によく注意を行うと同時にURLをクリックする前に内容をよく確認し、よく流行している詐欺メール等のニュースにも注意を払うことが重要です。

新型コロナウイルスに直接関係する詐欺メールとしては、ワクチン接種 医療機関等の注意喚起、支援金、給付金等があり、厚生労働省、総務省から注意喚起のお知らせが出されています。

ワクチン接種についての詐欺メールの例としては、差出人の名称が「自衛隊大規模接種センター」と表示されるコロナワクチン接種の予約サイトを案内するメールの例があります。これは、同じメールが何通も届き、記載されているURLをクリックすると厚生労働省のマークが記載されたコロナワクチン接種に関するポータルサイトによく似た画面が表示され、画面をクリックすると、氏名や住所といった個人情報を入力する画面となり、次のページではクレジットカードの情報を入力する画面となるものです【図2】※3。

医療機関等の注意喚起の例としては、「国立感染症予防センター」から「新型コロナウイルスの感染予防策について」の件名で、「新型コロナウイルス関連肺炎については、中国武漢市を中心に患者が報告され、国内でも多数患者が報告されています。つきましては、以下通知をご確認いただき、感染予防策についてよろしくお願いします。〈対策はこちら〉」というメールが届き、〈対策はこちら〉の部分をクリックすると不審なURLへ誘導されるというものです※4。

支援金、給付金等の例としては、「【特別定額給付金】二回目特別定額給付金の特設サイトを開設しました。」等の件名で以下のような内容のメールが届く事例が報告されています。

「令和2年8月15日、「新型コロナウイルス感染症緊急経済対策」が閣議決定され、感染拡大に留意しつつ、簡素な仕組みで迅速かつ的確に家庭への支援を行うため、二回目特別定額給付金事業が実施されることになり、総務省に特別定額給付金実施本部を設置いたしました。」

本文内にあるURLのクリックにより、特別定額給付金のオンライン申請を装った偽のサイトに誘導され、サイト内の「オンライン申請」を押すと、氏名、国籍、生年月日等の個人情報のほか、クレジットカード情報の入力が求められ、情報が盗まれてしまうことになります【図3】※5。

【図2】フィッシング対策協議会「厚生労働省をかたるフィッシング（2021/08/30）」※3

【図3】フィッシング対策協議会特別定額給付金に関する通知を装うフィッシング（2021/08/24）」※5

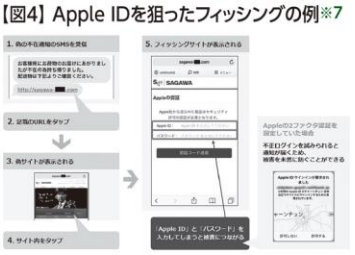
3 新しい生活様式に関係する詐欺メール

通信販売の利用の増加に伴って宅配便業者をかたる偽ショートメッセージや決済のためのクレジットカード会社をかたるフィッシングメールが増加しており、フィッシング被害状況を毎月報告しているフィッシング対策協議会の2021年8月の報告書によると、20021年8月のフィッシング報告件数は53,177件となり、7月と比較すると18,390件増加し、フィッシングに悪用されたブランド数も増加しています※6。

ショートメッセージ（SMS）から誘導されるフィッシングについては通常のメールと比較すると、本物と誤認したり、ついアクセスしてしまう傾向があるため、特に注意が必要となります。

宅配業者の不在通知を装ったSMSについても多くの報告が寄せられており、不正なアプリ（マルウェア等）のインストールへ誘導されたり、AppleやLINE、ドコモなどのフィッシングサイトへ誘導されるケースが確認されています。このSMSの送信元の電話番号は、同様のSMSから不正なアプリ（マルウェア等）のインストールを行ってしまった被害者のものである可能性が高いため、返信したり電話をかけないよう、注意することが必要です。Android端末とiPhoneでは、誘導の方法が異なりますが、iPhoneでは【図4】のような誘導サイトにIDやパスワードを入力してしまうと被害につながってしまうのでよく注意をすることが必要です。

【図4】Apple IDを狙ったフィッシングの例※7



※1 佐川急便「佐川急便を装った迷惑メールにご注意ください」（URL:https://www2.sagawa-exp.co.jp/whatsnew/detail/721/）
※2 参考：一般社団法人日本データ通信協会 迷惑メール対策（URL:https://www.dekyo.or.jp/soudan/contents/taisaku/1-1-3.html）
※3 フィッシング対策協議会「厚生労働省をかたるフィッシング（2021/08/30）」（URL:https://www.antiphishing.jp/news/alert/mhlw_20210830.html#）
※4 国立感染症研究所「当研究所に類似した機関による新型コロナウイルス感染症の注意喚起を装うメール攻撃にご注意ください」（URL:https://www.niid.go.jp/niid/ja/others/9432-warning200226.html）
※5 フィッシング対策協議会「特別定額給付金に関する通知を装うフィッシング（2021/08/24）」（URL:https://www.antiphishing.jp/news/alert/kyufukin_20210824.html）
※6 フィッシング対策協議会「2021/08 フィッシング報告状況」（URL:https://www.antiphishing.jp/report/monthly/202108.html）
※7 情報処理推進機構「情報セキュリティ 安心相談窓口だより」（URL:https://www.ipa.go.jp/security/anshin/mgdayori20181129.html）