

# スパム

スパム (spam) とは受信者の意向を無視して、無差別かつ大量に一括してばらまかれる、電子メールや SNS 上のメッセージのことです。電子メールで送られてくることが多く、迷惑メールと呼ばれるものはスパムの典型的なものです。Twitter や Facebook などの SNS 上にも登場し、今では、インターネット上での迷惑行為全般を指すようになりました。

## スパムとハム

### 【便利知識】

スパムという用語は、豚肉の缶詰の「スパム (SPAM)」に由来しています。イギリスのコメディ集団モンティパイソンの「スパム」というコントがきっかけで、スパムという用語が使われるようになりました。このコントは、スパムが嫌いな夫婦がレストランでメニューを開くと、すべてスパムのメニュー、店員にスパムと連呼され、スパム嫌いな夫婦でも仕方なくスパムを注文してしまった、という話です。相手の迷惑を考えずにしつこく何度も繰り返されることから、迷惑メールの語源としてスパムが使われたようです。

この言葉は 40 年も前にある商品の広告宣伝のために使われ始めました。大量発信可能な迷惑メールは、やがて爆発的に広がり一般化して行きました。今も廃れていないことが、新しい宣伝・広告手法としてスパムが有用であった証明です。

### 【便利知識】

スパム (spam) メールに対して、スパムではないメールのことを、スパムになぞらえてハム (ham) メールと呼びます。一看するとスパム (自分が承諾していないのに送られてくる広告メッセージなど) に見えるメールが、よくよく考えてみると、実は自分が意識的・無意識的に関わらず、メールを受け取ることを承諾していた、というようなものがあります。

オンラインで物を買ったり、予約したりする際に、サービス提供者から、情報や案内の配信を「同意する」に予めチェックが入っている場合も少なくありません。

ハムメールも数多いと、受信リストの中で本当に必要なメールが埋もれてしまい見落としてしまう、というようなことが起こりがちです。時々受信リストをチェックして、不要なハムメールを「購読停止」することをお勧めします。

## 代表的なスパムの例

### スパムの内容と現れ方

- 出会い系・アダルトサイトなどへ誘導する「スパムメール・LINE スпам」
- 金をだまし取ろうとする架空請求やフィッシング詐欺などの「スパムメール」
- ブログのコメント欄で宣伝したりサイトへ誘導する「コメントスパム」
- ブログ記事に多量のトラックバックを送り付ける「トラックバックスパム」
- サイトやサービスの宣伝を行う「ブログコメント・Facebook スпам」
- ページの拡散力を高めたり個人情報の獲得を狙う「Facebook・Twitter スпам」

### スパムメールの具体例

- ID・パスワードなどの個人情報の入力を要求してくるメール
- 「すぐにアクセスしてください」などと焦らせるメール
- 「ウイルスに感染しています」などと脅迫しているメール
- 「稼ぐコツ 懸賞当選」などのもうけ話を語るメール
- 知らない異性が甘く誘惑してくるメール
- 「・・・から紹介を受けた」などと、知らない人からのメール

## スパムメールへの対処法

### 迷惑メールは開かない、リンクにアクセスしない、返信しない

まずは、メールのタイトルを見て、「お得です！」「危険性があります。安全を確認しましょう！」的に人の気を惹こうというようなメールは、開かないことをお勧めします。メールを開いただけでウイルスなどに感染する場合がありますからです。

また本文の中で同様に人の気を惹こうとしているメールも、不用意にメール内にあるリンクにアクセスする、メール返信で連絡するなどを控えるべきです。

スパムメールの中には、著名な企業や組織からのメールを装いユーザの油断を誘う「騙りメール(なりすましメール)」もあります。

「本人確認のため、ID とパスワードを入力してください」という類のメールでうっかりその入力をしてしまうと、その ID、パスワードで様々なサービスのアカウントを乗っ取られて、財産を失いかねません。気をつけましょう。正規の企業から ID、パスワードなどの個人情報を求めるメールが届くことはまずありません。

楽天グループの事例をご紹介します。

＜楽天の FAQ「[【ご注意ください】楽天を装った不正関連の事例一覧](#)」より抜粋＞

- 楽天を装った不審なメール(会員情報変更メール)
- 楽天カードを装った不審なメール(カード利用お知らせメール)
- 楽天市場を装った不審なメール(アカウント確認メール)
- 楽天を装った不審なメール(ログイン通知)
- 楽天を装った不審なメール(自動配信メール)
- 楽天を装った不審なメール(注意喚起を装ったメール)
- 楽天を装った不審なメール(年次本人確認メール)

### 迷惑メールフィルターを設定する

Gmail などの Web メールサービスや、outlook などのメールソフトの多くは、迷惑メールフィルター設定機能を備えています。

初期設定を変更しなければ、迷惑メールと判断されるものは、自動的に「迷惑メール」フォルダーへ移動するように設定されているものがほとんどです。迷惑メールフィルターが無効になっているようであれば、有効に戻すことをお勧めします。

なお、迷惑メールフィルターが完璧ということはありません。スパムメールが見逃されることはまだしも、正しいメールを迷惑メールと見誤って「迷惑メール」フォルダーに移されてしまうこともおきます。Web メールサービスの迷惑メールフィルターで引っかかった場合、いつまでたってもメールが届かず、重要な連絡を受け取れないということもあり得ます。時々、Web メールサーバ上の「迷惑メール」フォルダーをチェックして、そのようなことが起きていないかを確認しましょう。特定の送り主からのメールがいつも迷惑メールと判断されているようならば、迷惑メールフィルターの設定を手動で調整しましょう。(具体的な設定の仕方は各 Web メールサービスのマニュアルを参照してください。)

### SNS スパムの事例と対策

スパムメールが依然として存在する中、最近ではスパム行為に Twitter や Facebook、LINE といった人気 SNS やコミュニケーションアプリを悪用するケースが目立っています。「インスタ映え」の流行語に象徴される写真投稿主体の Instagram でも発生しています。スマホやタブレットの普及を背景に、多くの利用者を抱える人気の SNS やアプリが、攻撃者の格好の標的になっているのです。

不正な Web サイトへ誘導するスパムツイートやメッセージ、想定外の個人情報にアクセスするスパムアプリなどがその例です。スパムアプリの誘導先でアプリ連携を承認すると自身のアカウントをアプリ開発元にコントロールされてしまう恐れがあります。

例えば Twitter では、「あなたの写真が載っているよ」などと書き込んだリンク付きのダイレクトメッセージから Twitter の偽ログインページへ誘導し、そこに入力されたアカウント情報を盗み出す手口があります。Facebook では、見知らぬ美男・美女の写真付きスパムアカウントが多数作成されており、彼らからの友達申請を承認すると、個人情報を悪用されたり、悪質な出会い系サイトへの登録を促されたりします。LINE でも、芸能人のマネージャーを装ったメッセージで出会い系サイトへ誘導し、情報や金銭をだまし取る手口が確認されています。

Instagram では、特に人気「女性」芸能人や読者モデルの方の投稿に対してコメントの形で書き込まれるものが多いようです。

攻撃者は人気の SNS やアプリに便乗し、あらゆる手段でユーザを罠にかけようとし、つい返信したくなるようなメッセージが送られてきても、無視するのが鉄則です。あまり度が過ぎるようなら、それぞれの SNS の FAQ を参照して、SNS 運営者にスパム報告をしましょう。

### アプリ連携による個人情報の漏えい

最近、注目を集めているのが、SNS 上でのアプリ連携をきっかけにプライバシー情報を漏えいさせてしまうリスクです。

例えば、Twitter では、昨年末から「Plays Now」と呼ばれるスパムアプリが流行しています。タイムラインに流れてきた動画のリンク、あるいは再生ボタンを押すと表示されるページ上で「Plays Now があなたのアカウントを利用することを許可しますか？」と尋ねられた経験はありませんか。そこで許可ボタンを押すとアプリ連携を承認したことになり、移動先の動画サイトで再生した動画のタイトルとリンクを勝手にツイートされ、フォロワーに動画の視聴状況が筒抜けになってしまいます。

Facebook では、「●●診断●●鑑定」といったアプリをリンク付きで紹介する投稿に注意が必要です。個人情報へ必要以上にアクセスしようとするスパムアプリの可能性があります。

アプリ連携へ誘導するリンク付きの投稿には、ついクリックしたくなるような表題が付けられています。リンク先の情報を見たいがあまり、表示されるアプリ連携の確認画面をよく見ず安易にクリックすることのないよう注意が必要です。

実際、リンク先でアプリ連携を許可すると、そのアプリにプロフィールや友達リスト、メールアドレス、位置データへのアクセスや、メール送信、投稿の権限などを与えることがあります。