パソコンやスマホに届く 迷惑メール

効果的な対処方法はこれだ!

日々大量に届く迷惑メールは不快なばかりでなく、業務の妨げにもなりますし、金銭的な被害に直結する危険も潜んでいます。迷惑メールに対処するために、しっかりと対策をしておきましょう。

テクニカルライター
小野　均

金銭的被害に直結するフィッシング詐欺メール

迷惑メールには、比較的実害の少ない広告・宣伝を目的とするものから、個人情報を盗もうとしたり、金銭を目的とするものまで、さまざまな種類があります。

なかでも気を付けたいのが、こ最近、急増している金銭目的のフィッシング詐欺メールです。これには、携帯番号やＬＩＮＥ宛てに送られてくるメッセージもあります。

フィッシング詐欺メールとは、あたかも銀行やクレジットカード会社、ネット通販等からのメールのように装い、偽のウェブページに誘導して口座番号やクレジットカード番号、暗証番号などを入力させて盗もうとするものです。

こうした詐欺メールに騙されると、銀行口座からお金を勝手に送金されたり、クレジットカードを不正利用されることがあります。

フィッシング対策協議会の報告によると、同協議会に寄せられたフィッシング報告件数は２０２２年６月単月で約８万８２５０件。昨年の６月が約３万件だったので、１年で３倍近くに増加していることがわかります。しかも、この件数は報告があったものだけなので、実際にはこれを大幅に上回る詐欺メールが配信されていると予測されます。

また、警察庁の発表では、昨年中におけるインターネットバンキングの不正送金被害は５８４件発生し、被害総額は８億２０００万円にも上るとしています。このように被害金額も大きくなるので、フィッシング詐欺メールには十分に注意する必要があります。

迷惑メールを受信したときにしてはいけないこと

根本的な迷惑メール対策の前に、迷惑メールを受け取ったときにしてはいけないことを理解しておきましょう。

まず、迷惑メールに対して、送信の停止を求めるような返信をしてはいけません。

迷惑メールの宛先のメールアドレスは、インターネット通販サイト等に自分で登録したものやどこかで流出したもののほか、実在するかどうかに関わらずランダムな文字の組合せで送信するものがあります。特にランダムに送りつける場合、返信をすると実在するメールアドレスだとわかり、かえって迷惑メールが増えることになってしまいます。

基本的には削除するか、後述する対策を実践してください。

厄介なのは、迷惑メールなのか正規のものなのかを判別できないケースです。

最近のフィッシング詐欺メールは、手口が著しく巧妙化しています。フィッシング詐欺メール自体、本物か偽物かを判別しづらいものがありますし、リンクをクリックした先にある偽のウェブページも、本物そっくりに作り込まれたものが少なくありません。

また、リンクをクリックするだけでコンピューターウイルスをダ

図表1　フィッシング詐欺メールの例


[アマゾン] 新しい端末でのログイン通知

amazon.co.jp プライム

お客様センターより重要なお知らせ

お客様のアカウントは第三者が不正にログインを試みた可能性がありますので、システム自動的に高リスクのアカウントと判断しました。

お客様の資金や取引安全の為、お客様のアカウントは利用制限されています。以下のリンクから、本人確認手続きをご確認ください。ご確認の上、お客様のアカウント制限を解除します。

24時間以内にご確認がない場合、誠に申し訳ございません、お客様の安全の為、システムによりアカウントをリセットします。

個人情報管理センター

発行元：アマゾングループ株式会社
© Amazon Group, Inc.社

ウンロードさせるものもあります。ですから、メッセージ内のリンクを安易にクリックしてはいけません。まずは、受け取ったメールが本物なのか、疑ってかかることが大切です。

メッセージの内容は、だいたい「あなたのアカウントに不正なアクセスがありました」や「不正な出金が確認されました」など、ユーザーの不安を煽る内容になっています（**図表1**）。

こうした内容は半信半疑でも気になるものなので、その場合はリンクからではなく、日頃使うブックマークなどを使って正規のウェブページにアクセスし、確認をしてください。

こうしたポイントも踏まえ、以下では具体的な迷惑メール対策を紹介します。

パソコンのメールソフトで行なう迷惑メール対策

自分で登録した覚えのない配信元からの迷惑メールに対しては、マイクロソフトの「Ｏｕｔｌｏｏｋ」やグーグルの「Ｇメール」などパソコンで使う主なメールソフトに備わっている迷惑メール対策機能を活用しましょう。

機能の１つは、自動振り分け機能です。この機能を有効にしておくと、受信メールを自動で識別し、迷惑メールと判断したメールを「受信トレイ」ではなく「迷惑メール」フォルダーに保存します。これにより、迷惑メールを目にすることが少なくなります。

ただし、振り分けの精度は１００％ではないので注意が必要です。

必要なメールが迷惑メールと判断されることがありますので、定期的に「迷惑メール」フォルダーを確認してください。

迷惑メールではないメールが見つかったときには、対象のメールを右クリック、あるいは選択して「迷惑メールではない」といった文言の機能を実行します。

「Ｇメール」を例にすると、メールを選択して「迷惑メールではない」をクリックします。

これでメールは「受信トレイ」に移動し、以降は学習して同じ差出人からのメールを「受信トレイ」に保存するようになります。

逆に、迷惑メールが「受信トレイ」に保存された場合は同様の操作で、「迷惑メールにする」といった文言（「Ｇメール」では「迷惑メールを報告」）の機能を実行してください。

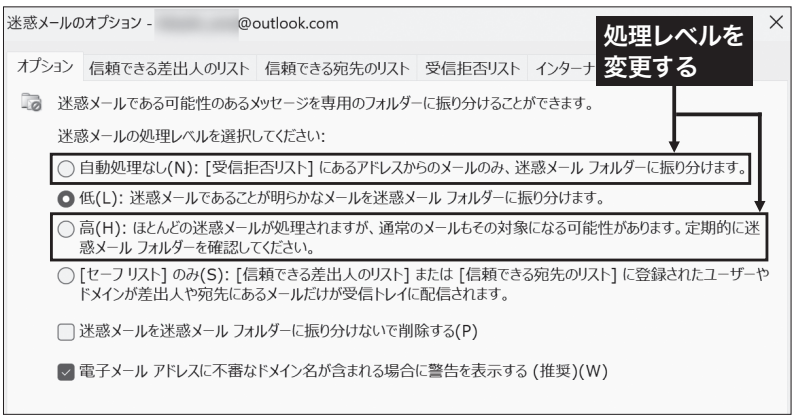
以降、同じ差出人のメールは、「迷惑メール」フォルダーに振り分けられるようになります。

なお、「Ｏｕｔｌｏｏｋ」は、さらに詳細な設定が可能です。

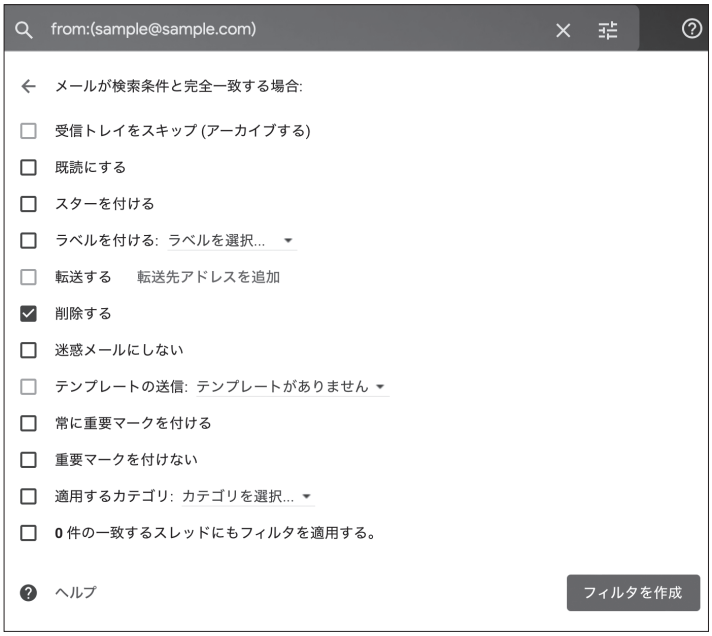
適当なメールを選択して右クリックし、「迷惑メール」→「迷惑メールのオプション」とクリック。開く画面の「オプション」タブで、迷惑メールの処理レベルを設定できます。一般的には標準設定の「低」で問題ありませんが、誤判断が多いときにはここで「自動処理なし」か「高」を選んでみてください（**図表2**）。

さらに同じ画面で、「信頼できる差出人のリスト」「信頼できる宛先のリスト」「受信拒否リスト」の作成も可能

図表2　「Outlook」の「迷惑メールのオプション」では、処理レベルを変更できる



図表3　「Gメール」のフィルタ作成の例



です。振り分けの精度を上げたいときは、これらの機能も使ってみてください。

もう1つは、「Gメール」にあるようなフィルター機能の活用です。これは、あらかじめ設定する条件を満たした対象に対し、特定の操作を自動実行するものです。

たとえば、特定のメールアドレスやドメイン（メールアドレスの@以降）からのメールを受信したときに「削除する」や「迷惑メールにしない」といった動作を設定できます（**図表3**）。

「Gメール」では、「設定」→「すべての設定を表示」→「フィルタとブロック中のアドレス」の画面から作成します。

スマホのメールアプリで行なう迷惑メール対策

スマートフォンのメールアプリにも、同様の迷惑メール対策機能があります。

それでも「受信トレイ」に迷惑メールが保存された場合は、以下の操作を行なってください。

iPhone／iPadの「メール」の場合は、対象のメールを左方向にスワイプして操作ボタンを表示。「その他」→「〝迷惑メール〟に移動」をタップします。

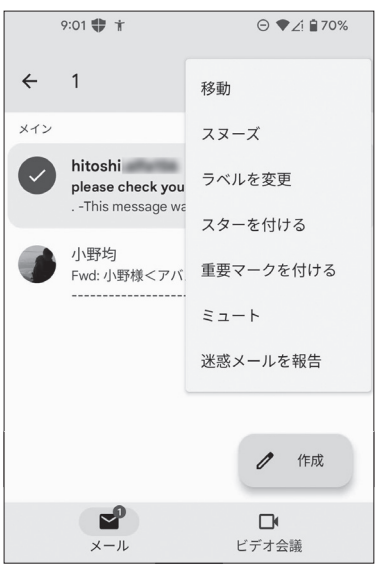
「迷惑メール」から「受信トレイ」に移動させるには、「その他」→「〝受信〟トレイに移動」になります。

「Gメール」アプリの場合は、対象のメールを長押しして選択。右上の三点ボタンをタップして「迷惑メールを報告」、逆のケースでは「迷惑メールではない」となります（**図表4**）。

メッセージアプリで行なう迷惑メール対策

フィッシング詐欺メールは、携帯電話宛てのSMS（ショートメッセージサービス）や、携帯キャリアが提供するメールサービス、LINE宛てにも送られてくるケースが増えています。そのため、スマホの「メッセージ」アプリやLINEでもしっかりと対策をしておく必要があります。

図表4　「Gメール」で迷惑メールを報告する例



iPhone／iPadの「メッセージ」では、「既知の差出人」と「不明な差出人」からのメッセージを分離して別々にリスト表示できます。操作は、「設定」アプリの「メッセージ」で「不明な差出人をフィルタ」を有効にするだけです。

迷惑メッセージのブロックまではできませんが、分離することで注意喚起になります。

Androidの「メッセージ」には、「スパム対策」機能があります（Pixel5／Android12の例）。同機能を有効にすると、不審なメッセージを受信したときに、「スパムとして報告」または「スパムではない」が選択できるようになります。

設定は、「メッセージ」アプリ右上の三点ボタンをタップし、「設定」をタップ。開く画面で「スパム対策」をタップし、次の画面で「スパム対策を有効にする」をオンにします。

さらに強固な対策をするに

は、携帯キャリアが提供するサービスの活用も検討してください。

ドコモは「あんしんセキュリティ」と「迷惑メールおまかせブロック」、ａｕは「迷惑メールフィルター」と「迷惑メッセージ・電話ブロック」、ソフトバンクは「迷惑メールフィルター」です。

詳細は、各キャリアのウェブページ等で確認できます。

ＬＩＮＥには「メッセージ受信拒否」機能が用意されています。これは、「友だち」以外からのメッセージを拒否する機能です。

設定は、「設定」画面を開いて「プライバシー管理」をタップ。開く画面で「メッセージ受信拒否」を有効にすれば完了です。

セキュリティ対策ソフトの活用

冒頭で解説したように、迷惑メールには複数の種類があり、そこには様々な危険が潜んでいます。また、ここまで解説した対策により、ある程度はリスクを低減できるのですが、セキュリティ対策に完全はありません。

そこで最後に、セキュリティ対策ソフトの活用もおすすめしておきます。

多くの人が、パソコンにセキュリティ対策ソフトを導入していると思いますが、同様にスマホやタブレットにも対策が必要です。

現在、パソコンで使っているセキュリティ対策ソフトが、スマホやタブレットにもインストールできるマルチプラットフォーム版であれば、ぜひインストールして活用してください。

これから導入を検討するのなら、「ウイルスバスタークラウド」（トレンドマイクロ）や、「ノートン３６０」（ノートン）、「マカフィーリブセーフ」（マカフィー）といったマルチプラットフォームに対応する有料版ソフトがよいでしょう。

ウイルス対策のほか、個人情報の漏えいをブロックする機能など機能が豊富で、万一のときにしっかりとしたサポートを受けられるのもおすすめの理由の１つです。

無料版になると機能がやや制限されてしまいますが、マイクロソフトが提供する「Microsoft Defender」はマルチプラットフォーム対応で、Ｗｉｎｄｏｗｓ、Ｍａｃのパソコン、ｉＰｈｏｎｅ、ｉＰａｄ、Ａｎｄｒｏｉｄのスマホ・タブレットにインストールして利用できます（**図表５**）。

いずれにせよ、セキュリティ対策ソフトは各機器を総合的に守るものなので、活用を真剣に検討してください。

加えて、パソコンやスマホなど端末自体のセキュリティレベルの向上も忘れてはいけません。

そのためには、ＯＳを常に最新の状態にアップデートしておくことが重要です。ＯＳのアップデートには最新のセキュリティ対策が含まれていますので、アップデートすることで見つかったセキュリティの脆弱性をカバーすることになるのです。

＊　＊　＊

ここまで解説した対策を実践すれば、迷惑メールを目にする機会は減り、被害も少なくなることでしょう。しかし、送られてくる迷惑メールがなくなるわけではありません。また、今後はさらに手口が巧妙化することも考えられます。

そのため、最も大切なことは、常に危機意識を持って対処することです。安易にクリックさえしなければ被害は避けられるので、不審なメールではないかと疑ってかかることを忘れないでください。

図表５　セキュリティ対策ソフトを活用する

おの　ひとし　編集プロダクション勤務を経て、フリーライターとして独立。現在は、パソコン、インターネット、スマホ、タブレット操作の解説記事を中心に、様々なメディアで幅広く執筆活動を行なう。