迷惑メールに関する注意事項

1. 迷惑メールを受信した場合の対応

1-1. メールを開かない

迷惑メールを開いてしまうと、ウイルス感染や望まない広告・画像などが表示される恐れがあります。心当たりがないアドレスから送られてきたメールは、開かずに削除してください。

1-2. クリックしない・返信しない

宛先間違いを指摘する、メール本文に書かれた配信停止 （送信拒否） 用の URL をクリックするなど、迷惑メールに対して反応してしまうと、そのアドレスが現在使われているアドレスであることを知らせることになります。また、インターネットバンクや会員専用サイトからの連絡メールを装って、偽の Web ページへ誘導して ID やパスワードなどの入力を促し、個人情報を盗む「フィッシング詐欺」が増えています。見慣れている送信者名やメールアドレスからのメールでも、少しでもおかしいと思った場合はメールの返信や、本文に記載されている URL リンクをクリックしないでください。

1-3. 添付ファイルを開かない

添付の ZIP ファイルを解凍することで感染するウイルスが存在します。ウイルスは、使用しているパソコンに常駐して動作環境を壊すものから、感染者のアドレス帳に登録されているアドレスに自動的にウイルスを送信してしまうものまで、その種類はさまざまです。感染先のアドレスを使って、さらに多数のユーザーへウイルスメールをばら撒くという事例もあり、不用意に添付ファイルを開かないでください。

1-4. メールソフトの迷惑メールフィルタ機能を利用する

メールソフトの機能を利用して、迷惑メールを受信トレイに残さず、自動的に別フォルダに振り分けることができます。必要なメールと迷惑メールの区別が可能です。ご利用中のメールソフトによって操作方法が異なりますので、詳しくはメールソフトのサポートサイトをご覧ください。

例： Microsoft Outlook for Office 365, Outlook 2019, 2016, 2013, 2010 のサポートサイト

https://support.microsoft.com/ja-jp/office/迷惑メール-フィルターの概要-5ae3ea8e-cf41-4fa0-b02a-3b96e21de089?ui=ja-jp&rs=ja-jp&ad=jp

2. 迷惑メールを受信しないようにするための対応

2-1. 自分のメールアドレスを不用意に公開しない

迷惑メール送信者は、WEB ページや掲示板などに公開されているメールアドレスを収集し、迷惑メール送信リストに追加していきます。また、無料のサービスを利用する際の会員登録から情報が漏れる場合もあります。各種サービスを利用する場合にメールアドレスを登録する場合は、フリーメールのメールアドレスを使用するなど、目的別にメールアドレスを使い分けることをおすすめします。

2-2. 怪しげな WEB サイトにアクセスしない

怪しげな WEB サイトへのアクセス、怪しげなバナー広告をクリックすることはウイルスに感染するリスクがあります。スパイウェアに侵入される、パソコンを迷惑メールの踏み台として悪用される、などの危険にさらされることにもなります。有名企業の名を騙ったアンケートサイトや懸賞サイトを装って、個人情報の収集を目的とした悪質なサイトも存在します。業務に関係のない WEB サイトにはアクセスしないでください。

2-3. セキュリティソフトを導入する

セキュリティソフトを導入し、ウイルス対策を行うことをおすすめします。セキュリティソフトの定期的なアップデートを行い、ウイルス定義ファイルを常に最新の状態に保つことで感染の被害を防ぐことが出来ます。