



ネット・メールトラブル防止 理解度チェック

● **問題** 復習も兼ねて理解度をチェックしましょう

No.	問題	回答
Q01	迷惑メールにダマされないための3つの基本にないものを選んでください。 1 メールは開かない 2 リンクをタップ（クリック）しない 3 個人情報を入力しない 4 疑わない	
Q02	いつも利用しているネットショッピングの会社から緊急のメールがきて、IDやパスワードなどの情報の入力を求められた場合の対応で、最も不適切なものを選んでください。 1 緊急なのでその通りに入力した 2 本当かどうか、その会社のホームページで確認した 3 本当かどうか、その会社のサポートセンターに確認した 4 消費生活センターに相談した	
Q03	身に覚えがないのに「あなたがアダルトサイトを閲覧している動画を入手したとして、公開回避のための金銭支払いを求めるメール」を受け取った場合の対応として、最も不適切なものを選んでください。 1 身に覚えはなくても、本当だったら怖いのですぐに払う 2 消費生活センターに相談した 3 メールは無視して払わない 4 同じようなメールを受信しないように迷惑メールフィルターを設定した	
Q04	献血をよびかけるチェーンメールを受け取った場合の対応として、最も適切なものを選んでください。 1 コメントを付け加えて転送する 2 献血のお願いだったので人助けのために転送する 3 記載された内容が本当か、メールに記載された病院へ確認の連絡をする 4 メールは無視して何も対応しない	

No.	問題	回答
Q05	迷惑メールにダマされないための対応には、「3つの基本」のほかに、「日頃の備え」があります。日頃の備えに含まれていないものを選んでください。 1 迷惑メールフィルターを利用する 2 セキュリティソフトを利用する 3 最新のOSに更新する 4 メールに記載されているサイトにアクセスする場合には、いつもと同じサイトかよく確認してから行う	
Q06	SMSを受信した場合の対応として最も適切なものを選んでください。 1 SMSにサイトへのリンクが設定されていたが、タップ（クリック）しなかった 2 送信者名が普段利用しているサービスだったので、サイトにアクセスした 3 宅配便業者からのSMSだったので、指示に従いアクセスした 4 料金未納の連絡だったので、すぐに電話した	
Q07	インターネットで写真を公開する場合に、最も不適切なものを選んでください。 1 スマートフォンカメラアプリの位置情報利用をOFFにして撮影した 2 写真に場所が特定できる情報が写っていないか確認した 3 記念に、校門の前で撮影した入学式の写真を投稿した 4 学校の制服で撮った写真だったので、インターネットへ掲載するのをやめた	
Q08	SNSを利用する際の注意点として、最も不適切なものを選んでください。 1 掲載する内容に個人情報が含まれていないか確認する 2 公開範囲を制限しない設定のまま利用する 3 写真を掲載するとき、自宅周辺は避ける 4 親しい友人や家族であってもログイン情報を共有しない	

正解と解説は次のページをご覧ください。



ネット・メールトラブル防止 理解度チェック

●正解と解説

No.	正解	解説
Q01	4	いきなりメールが来たら「詐欺かもしれない」と疑うクセをつけましょう。ゼロトラスト①メールを開かない②リンクをタップ（クリック）しない③入力しないの3つ基本をしっかりと覚えてください。p 1～2を参照
Q02	1	緊急性を強調して受信者をあわてさせ、アカウント情報をだましとろうとする手口のフィッシング詐欺メールが送られています。メールで個人情報やアカウント情報の入力を求められたら、詐欺を疑ってください。金融機関や企業などに問い合わせるときは、メールに記載されたアドレスや電話番号ではなく、必ずWebページなどの他の方法で調べて問い合わせをしてください。p 1～16を参照
Q03	1	「ハッキングした」と記載されていることもありますが、不特定多数の方あてに一斉送信しているメールと思われます。無視して決して支払ってはいけません。心配な場合は、ひとりで悩まずに消費生活センターなどへ相談してください。p 19～22を参照
Q04	4	誰かに転送を促すメールは、チェーンメールです。チェーンメールは、出所も、真偽もわからない情報です。途中で簡単に書き換えることもできます。それは、善意を装うメールであっても変わりません。伝言ゲームのような不確かな情報には反応しないで無視するようにしましょう。また、確認のためメールやメッセージに記載された電話番号へ問い合わせすることもやめてください。相手先の業務を妨害する可能性があります。p 25～26を参照

問題	正解	解説
Q05	4	どれだけ注意していても、迷惑メールや詐欺メールにダマされる可能性は残ります。そのため、少しでもそのリスクを抑えておくための日頃の備えもとても重要になります。詐欺メールは本物とニセモノを見分けるのは困難です。企業へ問い合わせをする必要がある場合には、普段使用しているブックマークやアプリからアクセスするか、公式サイトで確認したヘルプデスクへ連絡するようにしましょう。p 1～4を参照
Q06	1	SMSは、受信者がメッセージに気づきやすく、自分の電話番号を知っている相手からのメッセージだと思い込みやすいためか有名企業やブランドを装った詐欺メールが増えています。送信者表示の偽装が可能ですから普段利用しているブランド名だからといって安心はできません。SMSを利用した詐欺メールが数多く送信されていることを常に意識しておいてください。SMSに表示されたURLは安易にタップ（クリック）しないようにしましょう。p 5～6、9～10を参照
Q07	3	スマートフォンのカメラアプリで位置情報を利用していると撮影した写真に撮影場所の位置情報が記録されます。位置情報を利用したまま自宅で撮った写真を公開した場合には自宅の場所が特定されてしまうおそれがあります。また、撮影した写真に写り込む情報から個人や場所が特定できてしまう可能性もあります。写真をインターネットで公開するときは、事前によく確認するようにしましょう。p 45～46を参照
Q08	2	SNSは、元々利用者なら誰でも投稿の閲覧ができて、コメントをつけられるサービスですから、誰でも投稿を見ることができるのが基本です。一方、インターネットには悪意を持った人間が潜んでいますので、プライバシー設定が不十分だと、投稿内容や写真などから個人が特定されてしまう可能性もあります。また、アカウント情報の管理が不十分だとSNSアカウントが乗っ取られてしまう危険すらあります。SNSを楽しく安全に利用するため公開範囲などの設定を見直しましょう。p 43～48を参照