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つ基本をしっかり覚えてください。ｐ１～２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。ｐ１～16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。ｐ19～22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。ｐ25～26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。p1～4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。p5～6、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。p45～46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。p43～48を参照