

クイズの答えと解説 【大人用】

答えは一つとは限りません

答え	解説
Q1(全部) 1.2.3.4.5	インターネットは世界中の人と簡単につながる便利な仕組みです。しかし、その中には詐欺の犯人や個人情報を狙う犯人もいます。インターネットでは危険な人物とつながる可能性があることを視野に入れておかなければなりません。
Q2 2.4	パスワードの使い回しは危険です。1つでもパスワードが漏れると他のサービスのアカウントも攻撃されてしまいます。家族の名前や誕生日などの簡単なパスワードは避け、アルファベットの大文字、小文字、数字、記号を組み合わせて、できるだけ長いパスワードを設定しましょう。
Q3 1.2.3.5	最近では、自動車や家電など様々な物がインターネットに接続されています。離れた場所から鍵を開けたり、エアコンや掃除機のスイッチを入れたりすることができ、生活がとても便利になりました。しかし同時に、こうした機器がサイバー攻撃の対象になるケースも増えています。便利さの裏には「ネットにつながる＝狙われる可能性がある」というリスクを意識して使うことが大切です。
Q4 2.3.4	コンピュータウイルスは、スマートフォン等の中に入り込み、個人情報や金銭等を狙うプログラムです。感染すると、遠隔操作されたり、個人情報や写真が盗まれたり、インターネットバンキングでの不正送金等の被害に遭う可能性があります。信頼できないアプリやメールのリンクは開かず、セキュリティ対策ソフトを入れて常に最新の状態を保ちましょう。
Q5(全部) 1.2.3.4	インターネット上には、違法サイトや詐欺サイト、裸等のわいせつ画像、他人の個人情報や名誉を傷つける投稿、デマ情報などがあります。利用する前に内容の正確性や安全性を必ず確認しましょう。また、違法・有害情報を発見した際には警察署やIHC（インターネットホットラインセンター）に通報しましょう。
Q6 1.3.4	写真に位置情報がついていると撮影日時や場所、端末情報などがわかります。SNS等に写真を投稿する際、位置情報がついたまま投稿すると、これらの情報から自宅や職場、学校など個人の生活に関わる場所が特定される危険があります。今は多くのSNSで投稿時に位置情報がついていれば削除してくれますが、一部のSNSやインターネットのブログ等ではそのまま投稿されるため、撮影時に位置情報をオフにしたり、投稿する前に不要な情報を削除するなどの対策が重要です。
Q7 例	SNSに投稿した写真や文章からは、住所や勤務先、行動パターン、名前や名称など、個人の詳細な情報が特定されることがあります。 <ul style="list-style-type: none">○住んでいる地域(車のナンバープレートや周囲の景色から)○写真を撮った日時(SNSにアップした時間から)○写真を撮った場所(店の看板やマンホール、限定商品から)○姿や通っている学校(顔、制服から)○本名や呼び名(ユーザー名「AHIRU」) 等 犯人や悪意ある第三者がこうした情報を利用してストーカーやトラブルを起こす可能性もあります。投稿前には位置情報や個人情報を特定できる情報が含まれていないか確認することが大切です。
Q8 3.4	イベント等の特定のチケットの不正転売、または転売を目的としてチケットを譲り受けた場合は処罰の対象となります。チケットを購入する際は転売条件に関する情報を確認し、公式サイトかリセールサイトから購入しましょう。