

クイズ

で学ぶ

情報 セキュリティ

問1

平成30年度に、全国の学校で最も多く発生した「個人情報漏えい事故」は次のうちどれでしょうか？

- ①盗難
- ②紛失・置き忘れ
- ③誤配布
- ④不正アクセス

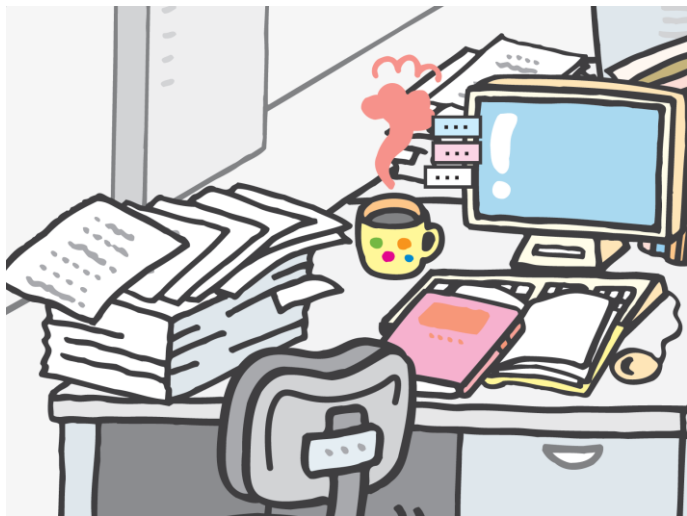
問2

USBメモリを自宅へ持ち帰って利用する際に、避けるべき行動は次のうちどれでしょうか？

- ①管理職に校外持ち出しの許可を得る
- ②データの暗号化やパスワードの設定をする
- ③自宅のパソコンにデータをコピーしてから作業する
- ④不要になったデータはすぐにUSBメモリから削除する

問3

下のイラストの中には、情報セキュリティ上、危険な部分があります。どのような部分に危険が潜んでいるのでしょうか？



© ISEN イラストで学ぶ 日常に潜む危険チェックシート
第一回 学期末の職員室

問4

近年、「ランサムウェア」というマルウェアによる被害が多数報告されています。語源になっている「ランサム」とは、どのような意味でしょうか？

- ①強盗
- ②誘拐
- ③身代金
- ④なりすまし

問5

次のうち、「標的型攻撃メール」の特徴として当てはまらないものはどれでしょうか？

- ①攻撃対象を管理職や情報担当者に絞っている
- ②知り合いや関係者を偽ってメールを送る
- ③添付ファイルからウイルスに感染させる
- ④メール内のリンクから不正なサイトへ誘導する

問6

パソコンがウイルスに感染した疑いがある場合、最優先で行うべき行動は次のうちどれでしょうか？

- ①パソコンを強制シャットダウンする
- ②ウイルス対策ソフトでウイルスチェックを行う
- ③重要なデータをUSBメモリにコピーする
- ④パソコンをネットワークから切り離す

問7

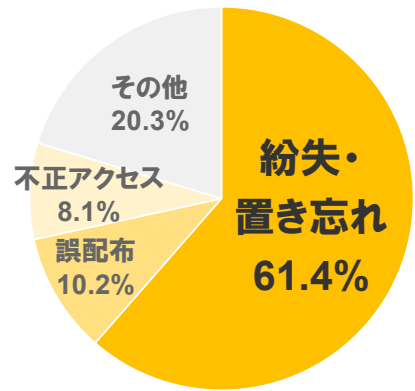
校務用端末のセキュリティを強化するために、文部科学省は「二要素認証」の導入を推奨しています。「二要素認証」に該当する組み合わせは、次のうちどれでしょうか？

- ①ID＋パスワード認証
- ②パスワード認証＋秘密の合言葉
- ③顔認証＋指紋認証
- ④USBキー＋暗証番号

問1の答え. ②紛失・置き忘れ

平成30年度に、全国の学校で最も多く発生した個人情報漏えい事故は「紛失・置き忘れ」です。書類などをなくしてしまわないよう整理整頓を心がけたり、外出時は荷物を肌身離さず持つたりするようにしましょう。

個人情報漏えい事故 発生比率



問2の答え. ③自宅のパソコンにデータをコピーしてから作業する

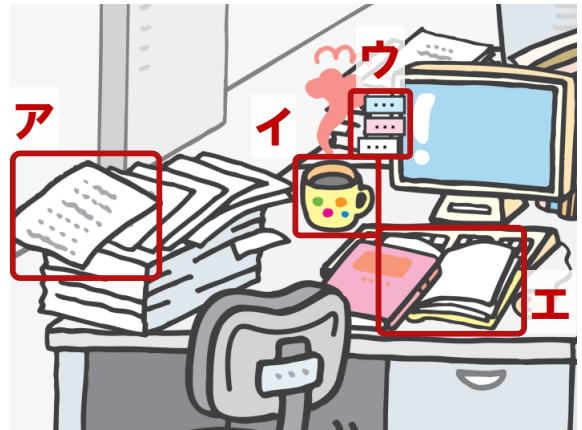
データをコピーすることで、情報漏えいのリスクが高まります。自宅のパソコンが盗難や不正アクセスに遭う可能性も考え、不用意にデータをコピーすることは避けましょう。データ暗号化やパスワード設定、不要なファイルの削除は、紛失や盗難時の被害を最小限に抑えるのに有効です。

© 2019 ISEN

平成30年度 学校・教育機関における個人情報漏えい事故の発生状況 調査報告書(第1版)をもとに作成

問3の答え. (ア)落ちそうな書類 (イ)飲み物の放置 (ウ)画面に貼った付箋 (エ)開いたままのノート

(ア)書類の山から落ちて紛失する恐れがあります
(イ)万が一こぼれたら書類や機器が使えなくなってしまう
(ウ)はがれてなくなったり部外者に見られたりする可能性も
(エ)部外者や子供たちに見られてしまう危険性があります



© ISEN イラストで学ぶ 日常に潜む危険チェックシート 第一回 学期末の職員室

問4の答え. ③身代金

「ランサムウェア」は、身代金要求型の不正プログラムです。パソコンなどの機器を不正にロックしたりファイルを暗号化したりした後、使用可能な状態に戻すことを引き換えに金銭を要求してきます。

問5の答え. ①攻撃対象を管理職や情報担当者に絞っている

「標的型攻撃メール」は、知り合いや関係者を装ったメールで不正なプログラムを送りつける手法です。添付ファイルからウイルスに感染させたり、リンクから不正なサイトへ誘導したりすることで、組織のシステムに侵入したり、情報を盗んだり、改ざんしたりします。誰もが攻撃の対象になり得るため、一人ひとりが注意する必要があります。内容やタイミングが不自然なメールは、添付ファイルやリンクを不用意に開かないようにしましょう。

問6の答え. ④パソコンをネットワークから切り離す

ウイルスの感染拡大や情報漏えいを防ぐために、パソコンをネットワークから切り離すことが最優先です。ウイルスの種類によっては、一度パソコンの電源を切るとパソコンが再起動できなくなる可能性もあります。ウイルス感染したパソコンにUSBメモリを接続すると、USBメモリもウイルスに感染する場合があります。ウイルス感染の疑いがある場合は、有線LANケーブルを抜いたり、Wi-Fiをオフにしたりしてからウイルスチェックをするようにしましょう。

問7の答え. ④USBキー+暗証番号

二要素認証は、「知識認証」「物理認証」「生体認証」のうち、異なる二つの認証方式を組み合わせた認証方法です。「①ID+パスワード認証」「②パスワード認証+秘密の合言葉」はどれも「知識認証」、「③顔認証+指紋認証」は両方とも「生体認証」です。「④USBキー+暗証番号」は「物理認証」と「知識認証」を組み合わせ、セキュリティが強固な認証方法と言えます。