第○○回　チェックテスト内容

2021年9月　IT部

IT Professor

チェックテスト（1/5）

Q1　BECに該当するものはどれですか。

① ウイルスプログラムが添付されたメールを、不特定多数に送りつけること。

② 第三者が取引先の担当者になりすまして偽のビジネスメールを送り、金銭をだまし取ること。

③ サーバーに大量のデータを送り付けて、サーバーを停止させること。

④ 使用しているコンピュータを強制的にロックして、もとに戻すことと引き換えに身代金を要求してくること。

【答え：②】
　BEC(Business E-mail Compromise)は、ビジネスメール詐欺と訳されます。巧妙なだましの手口を駆使して、偽の電子メールを組織・企業に送り付け、架空の送金取引などを通じて金銭をだまし取るサイバー攻撃です。人の心理的な隙に付け込んだ攻撃であり、技術的対策で排除することが難しいので、攻撃の手口を周知しておくことが必要となります。
　直接的に金銭的被害が生じている「①」だけがBECの事例となります。①ウイルス攻撃、③DDOS攻撃、④ランサムウェア

チェックテスト（2/5）

Q2　取引先から口座変更を知らせるメールを受信しました。
その後の対応として『間違っている』行動を選んでください。

① メールに記載の電話番号に、電話して口座変更は本当か確かめる

② ビジネスメールのパスワードを変更する

③ メール送信者のアドレスが正しいか確認する

④ 正しいメールアドレス宛に、新規作成したメールを送り確認する

【答え：①】
　ビジネスメール詐欺（BEC）では、業務用メールを盗み見した攻撃者は、なりすましのメールを作成しターゲットの企業の従業員を巧みな方法でだまします。送信者のメールアドレスが正しいかをチェックするだけでなく、メール・電話など複数の手段で事実確認することが重要です。
　メールに記載している署名欄は攻撃者によって偽装されている可能性があるため、「メール記載の電話番号」ではなく、正しい電話番号を調べて連絡しましょう。

チェックテスト（3/5）

Q3　PCのデータのバックアップについて、『間違っている』ものを選択してください。

① 共有のファイルサーバーにデータを保存しておく

② よく使うデータはUSBメモリや外付けハードディスクに保存する

③ バックアップを取ったUSBメモリは、施錠できる引き出しやキャビネット等に保管しておく

④ 大切なデータはPCの中にだけ保存しておく

【答え：④】

　データをPCの中にだけ保存しておくと、PCが故障した場合などにデータが消失する恐れがあります。

　大切なデータのバックアップを怠ると、万が一データが使用できなくなった場合に業務がストップしてしまい、仕事に支障をきたしてしまいます。

　そうなる前に、会社の共有のファイルサーバを利用したり、USBメモリにデータを保存するなど、バックアップをとることを徹底しましょう。

チェックテスト（4/5）

Q4　記憶媒体（USBメモリなど）の扱いについて『間違っているもの』を選択して下さい。

① 直射日光・強い磁気に当てない

② 施錠可能な場所に保管する

③ 自宅PCで使用した個人所有のUSBメモリを社用PCに接続して使用する

④ 廃棄する場合、媒体を初期化したうえで、破砕してから廃棄する

【答え：③】
自宅で使用している個人所有のUSBメモリが万が一ウイルスに感染していた場合、社用PCに接続したことで社内ネットワークを通じてすべてのパソコンがウイルスの脅威にさらされてしまいます。
私用のUSBメモリを業務で使用しないようにしましょう。

チェックテスト（5/5）

Q5　機密区分が「秘」のデータの情報漏えいを防ぐ方法として、適切なものを選んでください。

① データのバックアップをセキュリティ機能のないUSBメモリーに保存して、持ち歩く。

② データをサーバーの共有フォルダーに保存する。

③ データを添付したメール本文に、パスワードを記載する。

④ データにパスワードを設定して保存する。

【答え：④】
　組織の情報資産のうち、業務情報に関しては暗号化することが望まれます。データにパスワードを設定（暗号化）することにより、万一、それらのデータを格納した電子媒体（パソコン本体/CD/DVD/HD/USBメモリー等）を盗まれたり紛失したりしても、パスワードを知られなければ、大切なデータをある程度、情報漏えい事故から保護することができるからです。
　管理しているデータの漏えいを防ぐには暗号化が最善かつ唯一の策です。したがって④が正解です。