情報セキュリティマネジメント試験　科目 B のサンプル問題

問 1　A 社は，スマートフォン用のアプリケーションソフトウェアを開発・販売する従業員 100 名の IT 会社である。A 社には，営業部，開発部，情報システム部などがある。情報システム部には，従業員からの情報セキュリティに関わる問合せに対応する者（以下，問合せ対応者という）が所属している。

A 社は，社内の無線 LAN だけに接続できるノート PC（以下，NPC という）を従業員に貸与している。A 社の従業員は，NPC から社内ネットワーク上の共有ファイルサーバ，メールサーバなどを利用している。A 社の従業員は，ファイル共有には，共有ファイルサーバ及び SaaS 型のチャットサービスを利用している。

A 社は，不審な点がある電子メール（以下，電子メールをメールといい，不審な点があるメールを不審メールという）を受信した場合に備えて，図 1 の不審メール対応手順を定めている。

【メール受信者の手順】
1 メールを受信した場合は，差出人や宛先のメールアドレス，件名，本文などを確認する。
2 少しでも不審メールの可能性がある場合は，添付ファイルを開封したり，本文中の URL をクリックしたりしない。
3 少しでも不審メールの可能性がある場合は，問合せ対応者に連絡する。

【問合せ対応者の手順】
（省略）

図 1　不審メール対応手順

ある日，不審メール対応手順が十分であるかどうかを検証することを目的とした，標的型攻撃メールへの対応訓練（以下，A 訓練という）を，営業部を対象に実施することが A 社の経営会議で検討された。営業部の情報セキュリティリーダである B 主任が，マルウェア感染を想定した A 訓練の計画を策定し，計画は経営会議で承認された。

今回の A 訓練では，PDF ファイルを装ったファイルをメールに添付して，営業部員 1 人ずつに送信する。このファイルを開くと PC が擬似マルウェアに感染し，全文が文字化けしたテキストが表示される。B 主任は，A 訓練を実施した後，表 1 に課題と解決案をまとめて，後日，経営会議で報告した。

表 1　課題と解決案（抜粋）

課題 No.	課題	解決案
課題 1	不審メールだと気付いた営業部員が，注意喚起するために部内の連絡用のメーリングリスト宛てに添付ファイルを付けたまま転送している。	不審メール対応手順の【メール受信者の手順】の 3 を，“少しでも不審メールの可能性がある場合は，問合せ対応者に連絡した上で，［　a　］”に修正する。
課題 2	（省略）	（省略）

設問　表 1 中の［　a　］に入れる字句はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　注意喚起するために，同じ部の全従業員のメールアドレスを宛先として，添付ファイルを付けたまま，又は本文中の URL を記載したまま不審メールを転送する。

イ　注意喚起するために，全従業員への連絡用のメーリングリスト宛てに添付ファイルを付けたまま，又は本文中の URL を記載したまま不審メールを転送する。

ウ　添付ファイルを付けたまま，又は本文中の URL を記載したまま不審メールを共有ファイルサーバに保存して，同じ部の全従業員がアクセスできるようにし，メールは使わずに口答，チャット，電話などで同じ部の全従業員に注意喚起する。

エ　問合せ対応者の指示がなくても，不審メールを問合せ対応者に転送する。

オ　問合せ対応者の指示に従い，不審メールを問合せ対応者に転送する。

問２　国内外に複数の子会社をもつA社では，インターネットに公開するWebサイトについて，A社グループの脆弱性診断基準（以下，A社グループ基準という）を設けている。A社の子会社であるB社は，会員向けに製品を販売するWebサイト（以下，B社サイトという）を運営している。会員が2回目以降の配達先の入力を省略できるように，今年の8月，B社サイトにログイン機能を追加した。B社サイトは，会員の氏名，住所，電話番号，メールアドレスなどの会員情報も管理することになった。

B社では，11月に情報セキュリティ活動の一環として，A社グループ基準を基に自己点検を実施し，その結果を表1のとおりまとめた。

表1　B社自己点検結果（抜粋）

項番	点検項目	A社グループ基準	点検結果
(一)	Webアプリケーションプログラム（以下，Webアプリという）に対する脆弱性診断の実施	・インターネットに公開しているWebサイトについて，Webアプリの新規開発時，及び機能追加時に行う。 ・機能追加などの変更がない場合でも，年1回以上行う。	・毎年6月に，Webアプリに対する脆弱性診断を外部セキュリティベンダに依頼し，実施している。 ・今年は6月に脆弱性診断を実施し，脆弱性が2件検出された。
(二)	OS及びミドルウェアに対する脆弱性診断の実施	・インターネットに公開しているWebサイトについて，年1回以上行う。	・毎年10月に，B社サイトに対して行っている。 ・今年10月の脆弱性診断では，軽微な脆弱性が4件検出された。
(三)	脆弱性診断結果の報告	・Webアプリ，OS及びミドルウェアに対する脆弱性診断を行った場合，その結果を，診断後2か月以内に各社の情報セキュリティ委員会に報告する。	・Webアプリに対する診断の結果は，6月末の情報セキュリティ委員会に報告した。 ・OS及びミドルウェアに対する診断の結果は，脆弱性が軽微であることを考慮し，情報システム部内での共有にとどめた。
(四)	脆弱性診断結果の対応	・Webアプリ，OS及びミドルウェアに対する脆弱性診断で，脆弱性が発見された場合，緊急を要する脆弱性については，速やかに対応し，その他の脆弱性については，診断後，1か月以内に対応する。指定された期限までの対応が困難な場合，対応の時期を明確にし，最高情報セキュリティ責任者（CISO）の承認を得る。	・今年6月に検出したWebアプリの脆弱性2件について，1週間後に対応した。 ・今年10月に検出したOS及びミドルウェアの脆弱性4件について，2週間後に対応した。

設問　表1中の自己点検の結果のうち，A社グループ基準を満たす項番だけを全て挙げた組合せを，解答群の中から選べ。

解答群

ア　(一)　　イ　(一)，(二)

ウ　(一)，(二)，(三)　　エ　(一)，(三)

オ　(一)，(四)　　カ　(二)，(三)，(四)

キ　(二)，(四)　　ク　(三)

ケ　(三)，(四)

問３　消費者向けの化粧品販売を行うA社では，電子メール（以下，メールという）の送受信にクラウドサービスプロバイダB社が提供するメールサービス（以下，Bサービスという）を利用している。A社が利用するBサービスのアカウントは，A社の情報システム部が管理している。

〔Bサービスでの認証〕

Bサービスでの認証は，利用者IDとパスワードに加え，あらかじめ登録しておいたスマートフォンの認証アプリを利用した2要素認証である。入力された利用者IDとパスワードが正しかったときは，スマートフォンに承認のリクエストが来る。リクエストを1分以内に承認した場合は，Bサービスにログインできる。

〔社外のネットワークからの利用〕

社外のネットワークから社内システム又はファイルサーバを利用する場合，従業員は貸与されたPCから社内ネットワークにVPN接続する。

〔PCでのマルウェア対策〕

従業員に貸与されたPCには，マルウェア対策ソフトが導入されており，マルウェア定義ファイルを毎日16時に更新するように設定されている。マルウェア対策ソフトは，毎日17時に，各PCのマルウェア定義ファイルが更新されたかどうかをチェックし，更新されていない場合は情報システム部のセキュリティ担当者に更新されていないことをメールで知らせる。

ある日の15時頃，販売促進部の情報セキュリティリーダであるC課長は，在宅で勤務していた部下のDさんから，メールに関する報告を受けた。報告を図1に示す。

・販売促進キャンペーンを委託しているE社のFさんから9時30分にメールが届いた。
・Fさんとは直接会ったことがある。この数か月頻繁にやり取りもしていた。
・そのメールは，これまでのメールに返信する形で作成されており，メールの本文には販売キャンペーンの内容やFさんがよく利用する挨拶文が記載されていた。
・急ぎの対応を求める旨が記載されていたので，メールに添付されていたファイルを開いた。
・メールの添付ファイルを開いた際，特に見慣れないエラーなどは発生せず，ファイルの内容も閲覧できた。
・ファイルの内容を確認した後，返信した。
・11時頃，Dさんのスマートフォンに，承認のリクエストが来たが，Bサービスにログインしたタイミングではなかったので，リクエストを承認しなかった。
・12時までと急いでいた割にその後の返信がなく不審に思ったので，14時50分にFさんに電話で確認したところ，今日はメールを送っていないと言われた。
・現在までのところ，PCの処理速度が遅くなったり，見慣れないウィンドウが表示されたりするなどの不具合や不審な事象は発生していない。
・現在，PCは，インターネットには接続しているが，社内ネットワークへのVPN接続は切断している。
・Dさんはすぐに会社に向かうことは可能で，Dさんの自宅から会社までは1時間掛かる。

図1　Dさんからの報告

C課長は，Dさんの PC がマルウェアに感染した可能性もあると考え，マルウェア感染による被害の拡大を防止するためにDさんに二つ指示をした。

設問　次の(一)～(五)のうち，D さんへの指示として適切なものを二つ挙げた組合せを，解答群の中から選べ。

(一)　B サービスのパスワードを変更するように情報システム部に依頼する。

(二)　PC のネットワーク接続を切断し，PC のフルバックアップを実施する。

(三)　PC を会社に持参し，オフラインでマルウェア対策ソフトのマルウェア定義ファイルを最新に更新した後，フルスキャンを実施し，結果を C 課長に報告する。

(四)　社内ネットワークに VPN 接続した上で，ファイルサーバに添付ファイルをコピーする。

(五)　メールに添付されていたファイルを再度開き，警告が表示されたり，PC に異常がみられたりするかどうかを確認し，結果を C 課長に報告する。

解答群

ア　(一)，(二)	イ　(一)，(三)
ウ　(一)，(四)	エ　(一)，(五)
オ　(二)，(三)	カ　(二)，(四)
キ　(二)，(五)	ク　(三)，(四)
ケ　(三)，(五)	コ　(四)，(五)

情報セキュリティマネジメント試験　科目 B のサンプル問題　解答例・出題趣旨

問番号	正解
問１	オ
問２	キ
問３	イ

問番号	出題趣旨
問１	標的型攻撃メールへの対応訓練を題材にして，不審なメールを受信した従業員が順守すべき対応手順が十分であるかどうかを検証し，その際に発見された課題を解決する能力を問う。
問２	インターネットに公開している Web サイトの脆弱(ぜい)性診断を題材にして，情報セキュリティ活動の一環である自己点検の実施状況が，順守を求められている基準を満たしているか否かを判断する能力を問う。
問３	マルウェア EMOTET は，2021 年 11 月から活動を再開し，多くの企業に被害をもたらしている。本問では，マルウェア感染被害の拡大を防ぐために実施すべき事項を題材にして，情報セキュリティインシデント発生時の初動対応を判断する能力を問う。