問３　標的型メール攻撃への対応訓練に関する次の記述を読んで，設問 1 ～ 4 に答えよ。

X 社は，人材派遣及び転職を支援する会員制のサービス（以下，X サービスという）を提供する従業員数 150 名の人材サービス会社であり，東京と大阪に営業拠点がある。X 社には，営業部，人事総務部，情報システム部などがある。営業部には，100 名の営業部員が所属しており，東京拠点及び大阪拠点にそれぞれ 60 名，40 名に分かれて勤務している。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。

X 社では，最高情報セキュリティ責任者（CISO）を委員長とする情報セキュリティ委員会（以下，X 社委員会という）を設置している。各部の部長は，X 社委員会の委員及び自部における情報セキュリティ責任者を務め，自部の情報セキュリティに関わる実務を担当する情報セキュリティリーダを選任している。

X サービスの会員情報は，会員情報管理システムに保存される。営業部員は，会社から貸与された PC（以下，X-PC という）を使って会員情報管理システムにログインし，会員情報を閲覧する。また，会員から電子メール（以下，電子メールをメールという）に添付されて送られてきた連絡先の電話番号及びメールアドレスを含む履歴書や職務経歴書などを，会員情報管理システムに登録する。X 社は，ドメイン名 x-sha.co.jp（以下，X 社ドメインという）をメールの送受信のために使用している。メールは X 社の従業員にとって日常の業務に欠かせないコミュニケーションツールになっている。

X-PC には，パターンマッチング方式のマルウェア対策ソフトが導入され，マルウェア定義ファイルが常に最新版に更新されている。X-PC のハードディスクは暗号化されている。X-PC で使用するメールソフトは，外部から受信したメールが HTML メールであった場合，自動的にテキストメールに変換するように設定されている。

3 年前に情報システム部は，添付ファイルの開封や URL のクリックを促す不審なメール（以下，不審メールという）に備えて，図 1 の不審メール対応手順を定めた。

メールを受信した従業員（以下，メール受信者という）及び問合せ対応者は，次の手順に従って対応すること。

【メール受信者の手順】

1. メールを受信した時は，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. メールに少しでも不審な点がある場合は，問合せ対応者に次の項目を連絡する。
   （省略）
   その際は，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こと。
   また，問合せ対応者の指示なしに不審メールを転送したりしないこと。
3. 不審メールの添付ファイルを開封したり，不審メールの本文中のURLをクリックしたりした場合は，速やかにX-PCからLANケーブルを抜き，さらに無線LANをオフにする。

【問合せ対応者の手順】

1. 不審メールを受信した従業員（以下，不審メール受信者という）から連絡を受けたときは，不審メール受信者に，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たかを確認する。
2. 不審メール受信者が添付ファイルを開封しておらず，本文中のURLもクリックしていない場合は，不審メールを指定のメールアドレス宛てに転送するように指示する。
3. 不審メール受信者が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ていた場合は，まず，X-PCに不自然な挙動があったかどうかを確認する。次に，不審メール受信者に，X-PCに導入しているマルウェア対策ソフトでフルスキャンを実行し，その結果を報告するように指示する。

（省略）

図1　不審メール対応手順

〔X社のネットワーク構成〕

X社のネットワークは内部ネットワークとDMZで構成されている。インターネットとDMZとの間，及びDMZと内部ネットワークとの間には，それぞれファイアウォールが設置されている。

内部ネットワークには会員情報管理システム，ログサーバ，内部メールサーバなどが設置されている。DMZには外部メールサーバ及びプロキシサーバが設置されている。外部メールサーバでは次の機能を使用している。

・内部メールサーバとインターネットとの間でメールを転送する。
・インターネットから転送されたメールの差出人メールアドレスがX社ドメインである場合，当該メールを破棄する。
・受信したメールの添付ファイルをスキャンし，マルウェアとして検知された場合は，メールを破棄する。

プロキシサーバはインターネットへのアクセスをブラックリスト型の URL フィルタリング機能で制限している。プロキシサーバのログはログサーバに転送され，直近3か月分が保存される。ログはネットワーク障害の場合などに利用する。

〔標的型メール攻撃対策の検討〕

ある日，同業他社の W 社で，標的型メール攻撃によるマルウェア感染が原因で約3 万件の個人情報が漏えいする事故が発生し，大きく報道された。報道によると，メールにマルウェアが添付されていたほか，メールの本文の言い回しが不自然であったり，日本では使用されていない漢字が使用されていたりした。

X 社委員会では W 社の事例を受けて，標的型メール攻撃に対する情報セキュリティ対策について話し合った。営業部の K 部長は，最近多くの企業で実施されているという①標的型メール攻撃への対応訓練（以下，標的型攻撃訓練という）を，自部を対象に実施することを CISO に提案した。CISO は，標的型攻撃訓練の計画をまとめて次回の X 社委員会で報告するよう，K 部長に指示した。K 部長は，営業部の情報セキュリティリーダである Q 課長に標的型攻撃訓練の計画を策定するよう指示した。また，K 部長が，情報システム部にシステム面での協力を依頼したところ，情報システム部の R 主任が協力することになった。

〔標的型攻撃訓練の計画〕

Q 課長は，標的型攻撃訓練の対象者（以下，訓練対象者という），標的型攻撃訓練で用いるメール（以下，訓練メールという）の本文，差出人メールアドレス，添付ファイルなどについて2通りの計画案を表1のとおり作成した。

表1　標的型攻撃訓練の計画案（抜粋）

項目	計画案1	計画案2
訓練対象者	全ての営業部員	
訓練メールの本文	実在する社外の組織を詐称し，メールに添付されている契約書を，至急，確認するように依頼する内容	業務に関連する内容になっており，X社の実在する従業員を詐称し，メールに添付されている履歴書を，至急，確認するように依頼する内容
差出人メールアドレス	実在する社外の組織を詐称したメールアドレス	X社ドメインのメールアドレス
添付ファイルの形式と内容	・PDF形式 ・全文，文字化けしたテキスト	・オフィスソフトの文書ファイル形式 ・架空の履歴書
送信日時	次の日時に分けて，各営業拠点の訓練対象者宛てに送信 ・東京：2018年10月1日10時 ・大阪：2018年10月2日10時	次の日時に，全ての訓練対象者宛てに送信 ・2018年10月1日10時
添付ファイルの開封に関する情報の集計	次の期間に，訓練メールの添付ファイルの開封に関する情報を開封ログとして取得し，集計 ・集計予定期間：2018年10月1日～10月8日	
訓練対象者の対応調査	訓練メールを受信した訓練対象者がどのように対応したかを，問合せ対応者に聞き取り調査 ・調査予定期間：2018年10月9日～10月10日	
結果の報告	X社委員会への報告予定日：2018年10月31日	
備考	標的型攻撃訓練の計画が確定した後，問合せ対応者だけに計画内容を周知	

K部長，Q課長及びR主任は，標的型攻撃訓練の計画案について打合せを行った。次は，そのときの会話である。

K部長：計画案1と計画案2の訓練メールは，どちらも実在する組織や個人を詐称した内容になっていますね。

Q課長：はい。情報セキュリティ機関の注意喚起によると，標的型メール攻撃に用いられるメールの多くは，②実在する組織がメール本文と添付ファイルを作成したかのように装ったり，差出人メールアドレスを詐称して実在する担当業務の関係者になりすましたりしています。その情報を参考にしました。

K部長：計画案1のように，訓練メールの差出人に実在する社外の組織を用いた場合は，実在しない組織を用いた場合と違い，［　a　］，［　b　］することがあるので，この点については再検討が必要です。

Q 課長：分かりました。再検討します。

R 主任：当社には開封ログを取得し，集計するシステムがありません。また，標的型攻撃訓練のノウハウが不足しているので，他社への提供実績が多数ある Y 社の標的型攻撃訓練サービス（以下，訓練サービスという）を利用するのはどうでしょうか。

K 部長：分かりました。Y 社の訓練サービスを候補にして計画案をまとめてください。

〔訓練サービス〕

後日，Y 社のコンサルタントである T 氏が X 社を訪れ，Q 課長，R 主任に訓練サービスの内容を次のように説明した。

・訓練メールを Y 社から訓練対象者宛てに送信し，開封ログを取得し，集計する。

・開封ログの集計結果と Y 社が蓄積してきた人材サービス業界の訓練結果との比較も含めた報告書を X 社に提供する。

T 氏からは，計画案 2 は，③訓練メールを Y 社から送信すると訓練対象者に届かないなどの問題があるので，再検討する必要があるとの助言があった。

Q 課長は，Y 社の人材サービス業界での訓練結果を基に，X 社の訓練では添付ファイルの開封率を 15%程度と予想した。Q 課長は R 主任とともに，計画案 1 及び計画案 2 を再検討し，K 部長に報告した。X 社委員会で二つの計画案を報告したところ計画案 1 が承認され，後日，計画案 1 を基に標的型攻撃訓練が実施された。

〔情報セキュリティ対策の改善〕

標的型攻撃訓練を実施した後，Q 課長と R 主任は，訓練対象者からの問合せ内容について問合せ対応者を対象に調査した。この調査結果及び Y 社からの報告から，幾つかの課題が明らかになった。そこで，Q 課長と R 主任は，課題を表 2 のとおりまとめた。また，課題に対する解決案と，そのうち Q 課長が有効であると判断したものを実施案として表 3 のとおりまとめて，K 部長に報告した。

表 2　課題（抜粋）

課題 No.	課題
課題 1	添付ファイルの開封率が 15%を大幅に超えており，業界平均を上回っている。
課題 2	④不審メールだと気付いた訓練対象者が，注意喚起するために営業部のメーリングリスト宛てに添付ファイルを付けたまま訓練メールを転送しているなど，不審メール対応手順どおりには対応できていない。
課題 3	⑤一部の訓練対象者が，マルウェア検査サイト [1] の無料サービスを使って添付ファイルを検査している。
課題 4	問合せ対応者が不審メールを転送してもらった後，全社に注意喚起するまでの手順が不明確である。

注 [1]　アップロードされたファイルがマルウェアか否かを検査する無料のサービスを提供する外部の Web サイトである。また，無料のサービスを使って検査されたファイルを入手できるという有料のサービスも提供している。

なお，有料のサービスを利用するためには，入手した他人のファイルを悪用しないという規約に同意しなければならない。

表 3　解決案及び実施案（抜粋）

課題 No.	課題に対する解決案	実施案
課題 1	[案 1]　業務でメールを使用してよい従業員の人数を段階的に減らす。 [案 2]　様々なタイプのメール文面や差出人メールアドレスを利用して標的型攻撃訓練を定期的に実施する。 [案 3]　組織再編を定期的に実施する。 [案 4]　他社が受信した実際の不審メールの事例や被害などを基にした e-ラーニングを定期的に実施する。 [案 5]　添付ファイルを開封した従業員が 0 名になるまで，今回と全く同じ標的型攻撃訓練を定期的に実施する。 [案 6]　問合せ対応者の人数を段階的に増やし，対応を強化する。	[案 1]～[案 6]のうち，［ c ］が有効である。
課題 2	（省略）	（省略）
課題 3	[案 7]　不審メール対応手順に，マルウェア検査サイトに添付ファイルをアップロードした後，問合せ対応者に報告するという記述を追加する。 [案 8]　不審メール対応手順に，マルウェア検査サイトに添付ファイルをアップロードすることを禁止するという記述を追加する。 [案 9]　不審メール対応手順に，ファイル名に少しでも不審な点があるファイルは，マルウェア検査サイトにアップロードしてよいという記述を追加する。 [案 10]　プロキシサーバの URL フィルタリング機能において，マルウェア検査サイトの URL をブラックリストに追加する。 [案 11]　ログサーバに保存されているログを定期的に確認する。	再発防止には，[案 7]～[案 11]のうち，［ d ］が有効である。
課題 4	（省略）	（省略）

後日，標的型攻撃訓練の結果並びに表 2 の課題及び表 3 の実施案を X 社委員会で報告したところ，表 3 の実施案が全て承認された。また，訓練対象者を他部にも拡大し，定期的に標的型攻撃訓練を実施することが決まった。これらが実施された後，さらに，標的型メール攻撃に関する技術的セキュリティ対策が導入され，更なるセキュリティ強化へとつながった。

設問 1　本文中の下線①について，W 社での事故を受けて，X 社で標的型攻撃訓練を実施する目的は何か。次の (i) ～ (viii) のうち，該当するものだけを全て挙げた組合せを，解答群の中から選べ。

(i)　X 社を不審メールの宛先にされないようにすること
(ii)　会員が不審メールを受信した場合に備えて，問合せ窓口を設置すること
(iii)　会員に不審メールが送信されないようにすること
(iv)　会員に不審メールを見分けるポイントを周知すること
(v)　問合せ対応者が不審メール対応手順に従って対応できるようにすること
(vi)　不審メール受信者が不審メールの差出人を特定できるようにすること
(vii)　不審メール受信者が不審メールを見分けられるようにすること
(viii)　不審メール受信者が不審メール対応手順に従って対応できるようにすること

解答群

ア　(i)，(ii)，(iv)　　イ　(i)，(iv)　　ウ　(ii)，(iii)，(v)
エ　(ii)，(vii)　　オ　(iii)，(iv)，(vi)　　カ　(iii)，(vi)
キ　(iv)，(v)　　ク　(v)，(vi)，(viii)　　ケ　(v)，(vii)，(viii)
コ　(vi)，(vii)

設問２　〔標的型攻撃訓練の計画〕について，(1)，(2) に答えよ。

(1)　本文中の下線②の目的は何か。解答群のうち，最も適切なものを選べ。

解答群

ア　PC やサーバの脆弱性をメール受信者に気付かれないようにするため

イ　SPF や DKIM などの技術的セキュリティ対策を回避するため

ウ　攻撃者が Bcc に設定した他の標的をメール受信者に気付かれないようにするため

エ　不審メールであるとメール受信者に思われないようにするため

オ　マルウェアの機能が個人情報の窃取なのか，金銭詐欺なのかを解析されないようにするため

カ　メールの添付ファイルがパターンマッチング方式のマルウェア対策ソフトによって，マルウェアとして検知されることを回避するため

(2) 本文中の［ a ］，［ b ］に入れる適切な字句を，解答群の中から選べ。

a，b に関する解答群

ア　会員から当該組織名を使用したことによって，名誉毀損で訴えられたり

イ　会員が当該組織に問い合わせることによって，当該組織からクレームを受けたり

ウ　訓練対象者が注意喚起のためにインターネット上の SNS に訓練メールの内容を投稿することによって，当該組織の風評被害につながったり

エ　訓練対象者が添付ファイルの内容についての確認に追われることによって，日常の業務が遅延したり

オ　訓練対象者が問合せ対応者に連絡することによって，メールを送ったかどうかを問合せ対応者が当該組織に確認するのに追われたり

カ　訓練対象者が問合せ対応者の指示によって X-PC をマルウェア対策ソフトでフルスキャンすることになったり

キ　訓練対象者が当該組織に問い合わせることによって，当該組織からクレームを受けたり

設問3　本文中の下線③の理由について，解答群のうち，最も適切なものを選べ。

解答群

ア　HTML メールはテキストメールに変換されるから

イ　X-PC のハードディスクが暗号化されているから

ウ　大阪拠点の訓練対象者が東京拠点の訓練対象者に標的型攻撃訓練メールを転送できないから

エ　外部メールサーバがインターネットから受信するメールについて送信元ドメインを制限するから

オ　外部メールサーバが添付ファイルをマルウェアとして検知してメールを破棄するから

設問4　〔情報セキュリティ対策の改善〕について，(1) ～ (3) に答えよ。

(1) 表 2 中の下線④について，本物の標的型メール攻撃であった場合，どのような情報セキュリティリスクが想定されるか。次の (i) ～ (iv) のうち，適切なものだけを全て挙げた組合せを，解答群の中から選べ。

(i) 転送された標的型攻撃メールを受信した営業部員が添付ファイルを開封しなくても，その営業部員のメールアカウントの情報が攻撃者に送信される。

(ii) 転送された標的型攻撃メールを受信した営業部員が，添付ファイルを開封することによって，X-PC と攻撃者が用意したサーバとの間で通信が発生する。

(iii) 転送された標的型攻撃メールを受信した営業部員が，当該メールの本文を閲覧するだけで，攻撃者とのコネクトバック通信が発生する。

(iv) 標的型攻撃メールをメーリングリスト宛てに転送した営業部員のメールアカウントの情報が攻撃者に送信される。

解答群

ア (i)　　イ (i), (ii)　　ウ (i), (iii)

エ (ii)　　オ (ii), (iii)　　カ (ii), (iii), (iv)

キ (ii), (iv)　　ク (iii)　　ケ (iii), (iv)

コ (iv)

(2) 表 2 中の下線⑤について，会員からのメールに添付されていたファイルであった場合，どのような被害が予想されるか。次の (i) ～ (iv) のうち，適切なものだけを全て挙げた組合せを，解答群の中から選べ。

(i) 会員の個人情報が有料サービスの利用者に漏えいする。

(ii) 会員のメールアドレス宛てにフィッシングメールが送られる。

(iii) 外部メールサーバによって，X 社ドメイン宛てのメールが拒否される。

(iv) 無料のサービスを利用した訓練対象者の個人情報が漏えいする。

解答群

ア (i), (ii)	イ (i), (ii), (iii)	ウ (i), (iii)
エ (i), (iv)	オ (ii), (iii)	カ (ii), (iii), (iv)
キ (ii), (iv)	ク (iii), (iv)	

(3) 表 3 中の [c] , [d] に入れる適切な字句を，それぞれの解答群の中から選べ。

c に関する解答群

ア [案 1], [案 2]	イ [案 1], [案 2], [案 5]
ウ [案 1], [案 3]	エ [案 2], [案 3], [案 4]
オ [案 2], [案 3], [案 4], [案 6]	カ [案 2], [案 4]
キ [案 3], [案 6]	ク [案 4], [案 5]

d に関する解答群

ア [案 7]	イ [案 7], [案 9], [案 11]
ウ [案 7], [案 11]	エ [案 8], [案 9], [案 10]
オ [案 8], [案 10]	カ [案 9]
キ [案 9], [案 11]	ク [案 11]