SG

平成30年度　秋期
情報セキュリティマネジメント試験
午後　問題

試験時間	12:30 ～ 14:00（1時間30分）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
4. 問題は，次の表に従って解答してください。

問題番号	問1 ～ 問3
選択方法	全問必須

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) 答案用紙は光学式読取り装置で読み取った上で採点しますので，B 又は HB の黒鉛筆で答案用紙の**マークの記入方法**のとおりマークしてください。マークの濃度がうすいなど，**マークの記入方法**のとおり正しくマークされていない場合は読み取れないことがあります。特にシャープペンシルを使用する際には，マークの濃度に十分注意してください。訂正の場合は，あとが残らないように消しゴムできれいに消し，消しくずを残さないでください。
   (2) **受験番号欄**に**受験番号**を，**生年月日欄**に**受験票の生年月日**を記入及びマークしてください。答案用紙の**マークの記入方法**のとおり記入及びマークされていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入及びマークしてください。
   (3) **解答**は，次の例題にならって，**解答欄**にマークしてください。答案用紙の**マークの記入方法**のとおりマークされていない場合は，採点されません。

〔例題〕　次の［　　］に入れる適切な字句を，解答群の中から選べ。

秋の情報処理技術者試験は，［ a ］月に実施される。

解答群　ア 8　　イ 9　　ウ 10　　エ 11

適切な字句は“ウ 10”ですから，次のようにマークしてください。

例題	a	ア	イ	●	エ	オ	カ	キ	ク	ケ	コ

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

全問が必須問題です。必ず解答してください。

問1　インターネットを利用した振込業務の情報セキュリティリスクに関する次の記述を読んで，設問1～5に答えよ。

F社は，従業員数70名の商社であり，主にインテリアやギフト用品の仕入れ，販売を行っている。F社には，総務部，企画管理部，商品部，営業部がある。

F社では，3年前に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を設置し，情報セキュリティポリシ及び情報セキュリティ関連規程を整備した。CISOは社長が兼務しており，情報セキュリティ委員会の事務局は，総務部が担当している。また，各部の部長は，情報セキュリティ委員会の委員，及び自部における情報セキュリティ責任者を務めている。各情報セキュリティ責任者は，自部の情報セキュリティを確保，維持及び改善する役割を担っており，さらに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。F社の企画管理部には，経営企画課及び経理課がある。経営企画課のS主任は，企画管理部全体の情報セキュリティリーダである。

〔インターネットバンキングサービスの利用〕

F社は，C銀行に口座をもち，C銀行が提供する法人向けインターネットバンキングサービス（以下，IBサービスという）を次の目的で利用している。

・自社の口座の残高及び入出金明細の照会
・取引先への商品代金の振込，運送業者への輸送費の振込，従業員への給与振込など

F社でIBサービスを利用しているのは，経理課のL課長，M主任及びNさんの3名（以下，経理担当者という）である。振込に関する取引先との電子メール（以下，電子メールをメールという）連絡などは各自の会社貸与のPCで行い，IBサービスの利用はIBサービス専用のPC（以下，IB専用PCという）1台で行っている。

IBサービスにおける情報セキュリティに関する仕様を図1に示す。

(a) IB サービスの利用者登録申請及びログイン

IB サービスを利用する法人は，法人内で IB サービスを利用した事務処理を行う者（以下，利用者という）を書面で C 銀行に登録申請する。利用者は，ログインするとき，利用者ごとに発行された利用者 ID 及びパスワードを入力する。利用者は，IB サービスのパスワード管理メニューでパスワードを変更することができる。

(b) ディジタル証明書

利用者は，ログインするとき，利用者 ID 及びパスワードに加えて，ディジタル証明書を利用する。ディジタル証明書は，C 銀行によって IB サービス利用法人の口座ごとに発行される。

IB サービス利用法人には，C 銀行から，①ディジタル証明書と秘密鍵を格納した耐タンパ性をもつ IC カード 1 枚，USB 接続式 IC カードリーダ 1 台及び PC 用 IC カードドライバが，提供される。

なお，PC に接続した IC カードリーダに IC カードを挿入したとき，IC カード利用のための暗証番号を入力する必要がある。暗証番号は IB サービス利用申込時に書面で登録申請する。

(c) 承認ワークフロー

振込の操作は，承認依頼と承認の 2 回の操作に分かれている。承認は承認依頼とは別の利用者でなければ実行できない。ただし，承認依頼の操作で入力された情報は，承認の操作の時に修正できる。

(d) ワンタイムパスワード

利用者は，振込の承認依頼を実行するとき，C 銀行が利用者ごとに提供するワンタイムパスワード生成器（以下，トークンという）が生成するワンタイムパスワードを IB サービスの操作画面に入力する必要がある。

トークンは，トークンごとの秘密情報と時刻情報を基にして，あるアルゴリズムによってワンタイムパスワードを生成しており，IB サービスのサーバも同じ情報とアルゴリズムを使うことによってトークンと同期したワンタイムパスワードを生成する。IB サービスのサーバは，利用者が入力したワンタイムパスワードと，サーバで生成されたワンタイムパスワードを比較して認証する。ワンタイムパスワードは 1 分ごとに更新され，生成された後 2 分間有効である。

(e) トランザクション認証

利用者は，振込の承認を実行するとき，振込先の口座番号をトークンに入力する。トークンは，トークンごとの秘密情報，振込先の口座番号及び時刻情報を基にしてあるアルゴリズムによってワンタイムパスワードを生成する。利用者はそのワンタイムパスワードを IB サービスの操作画面に入力して振込を承認する。

(f) 振込の操作を知らせるメール

(e)の振込の承認が実行されると，振込の承認が実行されたことを知らせるメールが，あらかじめ IB サービスに登録されたメールアドレスに送信される。メールには，振込の承認を実行した利用者 ID，日時などが記載されている。

(g) 履歴の照会

利用者は，IB サービスの履歴照会メニューで，振込内容，承認依頼及び承認を実行した利用者 ID，日時などの履歴を照会することができる。

(h) EV-SSL

IB サービスでは EV-SSL サーバ証明書を採用している。

図 1　IB サービスにおける情報セキュリティに関する仕様（抜粋）

F 社では，経理担当者それぞれに，IB サービスの利用者 ID 及びパスワードが発行され，トークンが提供されている。IC カードは 1 枚を 3 名で共用している。

〔F 社における標準的な振込手続〕

F 社では，自社のサーバで稼働している会計システム（以下，F 社会計システムという）の取引先口座マスタの登録，変更，削除の操作は M 主任が担当している。取引先口座マスタには，取引先の口座情報（金融機関名，支店名，口座種別，口座番号，口座名義人など）が登録されている。F 社における標準的な振込手続を図 2 に示す。

1. 振込依頼情報作成及び依頼書・データ出力

M 主任は，取引先への支払のために振込を行う場合，F 社会計システムを操作して，振込先名，振込先口座情報，振込金額及び振込指定日の情報（以下，この四つの情報を振込依頼情報という）を作成し，振込依頼書として紙に出力する。このとき，取引先口座マスタに登録されている口座情報を利用する。

また，M 主任は，振込依頼情報を C 銀行指定の“振込依頼データ”の形式で出力し，企画管理部の共有フォルダに保存する。

2. 振込依頼書の承認（書類に押印）

L 課長は，請求書など，振込の根拠となる証憑（ショウヒョウ）と振込依頼書を突き合わせて振込依頼情報を確認の上，承認印を押して N さんに回付する。

3. IB サービスでの振込（承認依頼）

N さんは，振込依頼書の記載に従い，IB サービスの操作画面で振込承認依頼を入力する。件数が多い場合は，共有フォルダ上の“振込依頼データ”を IB サービスにアップロードし，振込依頼書の内容と突き合わせて確認する。N さんが承認依頼を実行する。

4. IB サービスでの振込（承認）

M 主任は，IB サービスの操作画面で，振込承認依頼の内容と振込依頼書を突き合わせて確認し，誤りがなければ承認を実行する。これで IB サービスでの振込手続が完了する。振込承認依頼の内容に誤りなどがあれば N さんに差し戻す。又は，M 主任が，②内容を修正して承認を実行することもできる。

5. 振込の記録及び振込依頼書の保管

M 主任は，振込の承認を実行した日付を F 社会計システムの振込依頼情報に追記する。また，振込依頼書を共用キャビネットに保管する。

（“6. 振込完了の確認及び記録”は省略）

図 2　F 社における標準的な振込手続

〔F 社における IB サービス利用時の情報セキュリティリスク及びその対策〕

F 社では，IB サービス利用時の情報セキュリティリスクを想定し，表 1 に示す対策を実施している。

表1　IBサービス利用時の情報セキュリティリスク及びその対策

情報セキュリティリスク	対策
IB専用PCへの不正アクセス	（省略）
IB専用PCのマルウェア感染	・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化する。 ・［a1］ ・［a2］ ・［a3］
ICカードの盗難，紛失	・利用時以外は，ICカードを経理担当者用の共用キャビネットに施錠保管する。
［b1］	・ICカードの暗証番号を推測されにくいものにする。 ・IBサービスのパスワードを推測されにくいものにする。
［b2］	・トークンを各自のロッカーに施錠保管する。 ・振込の操作を知らせるメールの宛先として，経理担当者3名のメールアドレスを登録する。
［b3］	・振込の操作を知らせるメールの宛先として，経理担当者3名のメールアドレスを登録する。

〔B社からの問合せ〕

10月2日の朝，取引先であるB社の営業担当者から，先月末までに入金予定の商品代金800万円がまだ入金されていないとの電話が入った。応対したL課長は，折返しの返答を約束して電話を切り，Nさんに F 社会計システムの記録を確認させたところ，当該代金は振込済であることが分かった。あいにく M 主任は外出しており不在だったので，L課長は，Nさんに振込の詳細を確認した。次は，Nさんと L 課長との会話である。

Nさん　：IBサービスの履歴も確認しましたが，先月28日に振り込んでいます。

L課長　：振込先誤りの可能性はありませんか。

Nさん　：振込先は振込依頼書どおりでしたが，8月まで利用していた B 社の口座とは違っていました。振込時は L 課長が出張中だったので，振込依頼書の承認は受けずに振込の承認依頼を実行するよう M 主任から直接指示を受けました。IBサービスで私が振込の承認依頼を実行した後，M 主任がそのまま承認しています。

L課長　：M 主任に経緯を確認しましょう。IB専用PCのマルウェア感染も心配です。③振込の操作画面上は正しく操作しているように見えても，銀行との間で

送受信される振込先口座情報をマルウェアが書き換えていたという報道記事を以前読んだことがあります。

夕方，M 主任が外出先から戻ると，L 課長は，B 社から受けた問合せと，振込の詳細について確認した内容を伝えた。

M 主任にも，B 社に入金されていない理由は分からなかった。M 主任によれば，先月末，B 社の経理部長との間で請求書の発行時期や振込期限などについてメールでやり取りをしており，口座変更の連絡と改訂された請求書を受信し，了解の旨を返信した後，お礼を受信してメールのやり取りを終えていた。

M 主任が口座変更の根拠として保管していた B 社の経理部長からのメールを図 3 に示す。

日時　：2018 年 9 月 27 日　16:36
差出人：YYYY <YYYY@interiar-bsha.com>
宛先　：M@f-sha.com
CC　　：ZZZZ@interiar-bsha.com
件名　：Re: Re: 【ご相談】支払条件の件
添付ファイル：　請求書.pdf

M 様
諸々お気遣いいただきありがとうございます。
追加のお願いで申し訳ないのですが，この度，弊社の銀行口座を下記のとおり変更いたしました。月末の急な連絡で誠に恐縮ですが，今月末の入金から，新口座宛てにお振込いただけますでしょうか。
不都合，不明点などありましたらご連絡いただきたくよろしくお願いします。
　新口座
　●●●銀行●●●支店
　普通預金　XXXXXXX
　名義　　ビーシャ
改訂した請求書の写しを添付します。添付ファイルを開封するためのパスワードは前回と同じです。
B 社経理部 YYYY

図 3　B 社の経理部長からのメール

B 社の経理部長からのメールに表示されていたメールアドレスを表 2 に示す。

表２　Ｂ社の経理部長からのメールに表示されていたメールアドレス

役職	最後の２通のメールに表示されていたメールアドレス	普段使われているメールアドレス
Ｂ社の経理部長	YYYY@interiar-bsha.com	YYYY@interior-bsha.com
Ｂ社の社長	ZZZZ@interiar-bsha.com	ZZZZ@interior-bsha.com

早速，Ｍ主任からＢ社の経理部長に確認したところ，Ｂ社は口座を変更しておらず，変更を伝えるメールは送っていないということだった。Ｆ社から第三者の口座に商品代金を振り込んだことが分かったので，Ｆ社は，振込先の銀行に連絡し，事実関係を整理して警察に被害届を提出した。

〔手口と対策〕

後日，警察から，９月末にＢ社を退職した元従業員を被疑者として逮捕し，犯行手口に関する供述を得たとの連絡があった。被疑者の指定した口座に振り込ませるよう，偽メールを送信したとのことであった。被疑者は８月にＢ社の経理部長の手帳からメール受信のためのパスワードを盗み見て以来，職場の自分のＰＣで経理部長のメールを不正に閲覧していた。④Ｂ社の情報システム部が自社のログ収集システムに保管していたログからこのことが分かり，被疑者特定の手掛かりになった。

なお，被疑者は，［　c　］，メールを送っていた。

Ｌ課長は，今回の出来事を教訓としてＦ社で改善すべき点がないか，情報セキュリティリーダであるＳ主任と話し合った。そのときの会話を次に示す。

Ｌ課長　：今後，我が社が偽メールにだまされないための対策はありますか。

Ｓ主任　：第三者によるメールの不正な閲覧への対策にもなるので，できれば取引先に［　d　］を使ってもらいたいと思いますが，同意を得て準備する手間も掛かります。偽メールにだまされないための対策のうち確実であり，かつ，すぐできるものとして，振込に関わるメールのやり取りの際は，［　e1　］のがよいと考えます。そのためには，［　e2　］ことも必要です。

Ｌ課長　：我が社の取引先口座マスタの変更手続と，標準的な振込手続には問題はありませんか。

Ｓ主任　：振込依頼情報の作成前に，Ｍ主任が自分一人の判断で取引先口座マスタ中

の B 社の口座情報を変更できたという問題があります。対策として，［ f1 ］ことを進めます。振込依頼書の承認が省略できたという問題については，［ f2 ］ことを進めます。これによって，振込依頼書の書類を廃止でき，操作結果が社内システムに自動的に記録できるようにもなります。

S 主任は，これらの対策を情報セキュリティ委員会に提案し，対策を実施した。

設問 1　図 1 中の下線①について，C 銀行が，利用者にディジタル証明書と秘密鍵を IB サービスを利用する PC 内のハードディスクに格納させるのではなく，IC カードに格納して提供する目的はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　IB サービスを利用する PC のマルウェア感染による秘密鍵の漏えいリスクを低減するため

イ　ディジタル証明書の更新を不要にするため

ウ　複数枚のディジタル証明書を格納できるようにするため

エ　利用者が，IB サービスの利用者 ID とパスワードを知らなくても，IC カードで IB サービスにログインできるようにするため

オ　利用者が，IB サービスを利用する PC を，複数人で共用できるようにするため

設問2　図2中の下線②について，この段階でM主任が内部不正を働くおそれに対して，内部不正を思いとどまらせるために有効な牽制手段はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　IB専用PCを共用キャビネットに施錠保管し，必要なときだけ取り出して使うルールとする。

イ　L課長が，IBサービスの履歴と振込依頼書を突き合わせて点検し，差があればM主任に理由を聞くルールとする。

ウ　承認の操作の際，急がない修正は，修正して承認を実行する機能を利用せず，差し戻すルールとする。

エ　トークンを共用キャビネットに施錠保管し，使うときだけ貸し出すルールとする。Nさんが共用キャビネットの鍵を管理して貸出記録をつける。

オ　振込先の口座情報はIBサービス画面で手入力せず，“振込依頼データ”をIBサービスにアップロードするルールとする。

設問３　〔F 社における IB サービス利用時の情報セキュリティリスク及びその対策〕について，(1)，(2) に答えよ。

(1)　表 1 中の［ a1 ］～［ a3 ］に入れる，次の (i) ～ (vi) の組合せはどれか。a に関する解答群のうち，最も適切なものを選べ。

(i)　IB 専用 PC では，メール利用を禁止する。

(ii)　IB 専用 PC の OS にログインするには，経理担当者専用の共有アカウントを使う。

(iii)　IB 専用 PC は，社内ネットワークには接続せず，インターネットに直接接続する。

(iv)　IB 専用 PC から社内のファイルサーバへのアクセスは，企画管理部の共有フォルダへのアクセスだけを許可する。

(v)　IB 専用 PC では，使用していない USB ポートを物理的に閉鎖する。

(vi)　プロキシで，社外サイトへのアクセスは OS アップデートとマルウェア定義ファイルのアップデートだけを許可するように設定する。

a に関する解答群

	a1	a2	a3
ア	(i)	(ii)	(iii)
イ	(i)	(ii)	(iv)
ウ	(i)	(ii)	(v)
エ	(i)	(iii)	(iv)
オ	(i)	(iv)	(v)
カ	(i)	(iv)	(vi)
キ	(ii)	(iii)	(v)
ク	(ii)	(iv)	(v)
ケ	(ii)	(v)	(vi)
コ	(iv)	(v)	(vi)

(2) 表1中の [b1] ～ [b3] に入れる，次の (i) ～ (vi) の組合せはどれか。b に関する解答群のうち，最も適切なものを選べ。

(i) 経理担当者以外の者による，IB サービスへの不正なログイン操作

(ii) 経理担当者が操作を誤ることによる，振込金額や振込先の誤り

(iii) 経理担当者がフィッシングサイトに誘導されることによる，パスワード及び IC カード中の秘密鍵の盗難

(iv) 経理担当者による，自身の利用者 ID を使った不正な振込の承認

(v) 経理担当者の他の経理担当者へのなりすましによる，IB サービスへの不正なログイン操作

(vi) 経理担当者の他の経理担当者へのなりすましによる，又は経理担当者以外の者による，不正な振込の操作

b に関する解答群

	b1	b2	b3
ア	(i)	(iv)	(ii)
イ	(i)	(iv)	(v)
ウ	(i)	(vi)	(iv)
エ	(i)	(vi)	(v)
オ	(iii)	(i)	(iv)
カ	(iii)	(iv)	(v)
キ	(iii)	(vi)	(iv)
ク	(v)	(i)	(iv)
ケ	(v)	(iv)	(ii)
コ	(v)	(vi)	(ii)

設問4　〔B社からの問合せ〕について，(1)，(2)に答えよ。

(1)　本文中の下線③について，このようなサイバー攻撃手法の名称を，解答群の中から選べ。

解答群

ア　CSRF　　イ　DDoS

ウ　MITB　　エ　クリックジャッキング

オ　クロスサイトスクリプティング　　カ　フィッシング

(2)　本文中の下線③について，このようなサイバー攻撃手法への対策として，図1に示す情報セキュリティに関する仕様のうち，最も有効なものを解答群の中から選べ。

解答群

ア　(a)　　イ　(b)　　ウ　(c)　　エ　(d)

オ　(e)　　カ　(f)　　キ　(g)　　ク　(h)

設問5　〔手口と対策〕について，(1)～(5)に答えよ。

(1)　本文中の下線④について，被疑者を特定するために最も有効だったと考えられるものを，解答群の中から選べ。

解答群

ア　B社の経理部長が使っているPCで記録されたメール送受信ログ

イ　B社のメールサーバで記録されたメールクライアントソフトからの大量のログイン失敗ログ

ウ　B社のメールサーバで記録されたメールクライアントソフトからのメール受信要求ログ

エ　B社のメールサーバで記録されたメールクライアントソフトからのメール送信ログ

オ　被疑者が自宅で使っていた個人所有のPCで記録された操作ログ

(2) 本文中の［ c ］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。

c に関する解答群

ア　B 社から貸与された PC を使い，B 社の経理部長のアカウントを盗用して

イ　B 社から貸与された PC を使い，メールクライアントソフトの設定で差出人メールアドレスを B 社のドメイン名とよく似た実在しないドメイン名に詐称して

ウ　B 社の経理部長が席を外した隙に，B 社の経理部長が使っている PC のメールクライアントソフトを使って

エ　B 社のドメイン名とよく似たドメイン名を取得し，個人所有の PC でメールサーバを立ち上げて

(3) 本文中の［ d ］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。

d に関する解答群

ア　HTTP over TLS 利用の Web メール

イ　POP before SMTP

ウ　S/MIME によるディジタル署名付き暗号メール

エ　SMTP-AUTH

オ　SPF（Sender Policy Framework）

カ　パスワード付き ZIP ファイル

(4) 本文中の［ e1 ］，［ e2 ］に入れる字句の組合せはどれか。e に関する解答群のうち，最も適切なものを選べ。

e に関する解答群

	e1	e2
ア	受信メールの差出人メールアドレスと文面を慎重にチェックする	受信メールを印刷して情報セキュリティリーダを含め複数人でチェックする
イ	受信メールの差出人メールアドレスと文面を慎重にチェックする	情報セキュリティリーダに受信メールの写しを転送する
ウ	メールの内容について電話をかけて確認する	振込に関する詐欺事例と振込時の注意事項を経理担当者に教育する
エ	メールの内容について電話をかけて確認する	メールには必ず差出人の電話番号を記載してもらう
オ	メールをサーバに保存しておく	保存用のメールアドレスにもメールを同報する
カ	メールをサーバに保存しておく	保存用のメールアドレスにもメールを同報するとともに，情報セキュリティリーダが必要に応じてメールの内容を確認できる仕組みを作る

(5) 本文中の [f1] , [f2] に入れる，次の (i) ～ (vi) の組合せはどれか。f に関する解答群のうち，最も適切なものを選べ。

(i) F 社会計システムから共有フォルダに出力した後の振込依頼データは L 課長がディジタル署名を付与してから保管する

(ii) F 社会計システムの取引先口座マスタの登録及び変更のワークフローシステムを導入し，その申請権限と承認権限を分離する

(iii) IB サービスでの振込（承認）の承認者を，振込依頼書の承認者と同一人物にする

(iv) IB サービスでの振込の承認を実行する時に，もう一度，取引先の口座情報の変更の証憑と突き合わせて確認する

(v) 取引先口座マスタを登録，変更するときに取引先から入手すべき証憑の種類をマニュアルに明記する

(vi) 振込依頼情報を申請するワークフローシステムを F 社会計システムに導入し，かつ，振込依頼情報の申請権限と承認権限を分離する

f に関する解答群

	f1	f2
ア	(ii)	(i)
イ	(ii)	(iii)
ウ	(ii)	(vi)
エ	(iv)	(i)
オ	(iv)	(iii)
カ	(iv)	(vi)
キ	(v)	(i)
ク	(v)	(iii)
ケ	(v)	(vi)

問2　リスク対応策の検討に関する次の記述を読んで，設問1に答えよ。

A社は，ECサイトで旅行商品を販売している，資本金1億円，従業員数80名の会社である。もともとA社は旅行商品を店舗で販売していたが，2014年にECサイト（以下，A社ECサイトという）での販売を開始し，3年後の現在はA社ECサイトでの販売だけを行っている。A社ECサイトでの販売になってから旅行商品の販売のほとんどはクレジットカード決済である。A社には，総務部，人事部，旅行企画部，旅行営業部の四つの部がある。A社ECサイトは旅行営業部が管理，開発及び保守を行っており，A社ECサイトのシステム管理者も旅行営業部に所属している。A社ECサイトを除くA社の情報システムのシステム管理者は総務部に所属している。

A社全体の情報セキュリティ責任者は旅行営業部長である。旅行営業部に所属するEさんは，A社全体の情報セキュリティ推進を担う情報セキュリティリーダに任命されている。A社には，社長，総務部長，人事部長，旅行企画部長，旅行営業部長及びEさんが参加する情報セキュリティ委員会があり，Eさんは事務局を務めている。

〔A社における情報セキュリティ対策〕

A社で最も情報セキュリティが必要とされる情報は，顧客のクレジットカード情報である。このクレジットカード情報には，クレジットカード番号，クレジットカード会員名などが含まれている。A社が保有するクレジットカード情報及び販売履歴は，A社ECサイトのデータベースサーバ1台とファイルサーバ1台に保存されている。データベースサーバとファイルサーバは，A社の社内LANに接続されている。ファイルサーバには，テープバックアップ装置が接続され，クレジットカード情報などを含む特定のフォルダにある全てのファイルを毎週バックアップするように設定されている。バックアップは2世代分保存されている。バックアップテープは，テープバックアップ装置の隣にあるキャビネットに保管されている。また，A社で使われている全てのPCにはマルウェア対策ソフト（以下，対策ソフトという）が導入されており，マルウェア定義ファイルを自動的に最新版に更新するように設定されている。対策ソフトの設定は，対策ソフトの管理サーバによって一元的に管理されている。A社が使用している対策ソフトには，PCでのソフトウェアの起動可否をホワイトリスト

又はブラックリストで制御する機能がある。これらのリストを管理サーバで変更すると，A 社の全ての PC に自動的にそのリストが反映される。ブラックリストには，次の機能がある。

・制御する対象のソフトウェアを，個別のソフトウェア単位及びソフトウェアのカテゴリ単位で指定できる。
・指定したソフトウェアに対して，許可モード，禁止モード又は監視モードのいずれかを選択できる。監視モードを選択した場合は，指定したソフトウェアの起動を許可するが，実行されたソフトウェアの実行履歴を管理サーバのログに記録する。

A 社は，業務マニュアルなどの有用な情報を大量に蓄積した掲示板システムを保有している。当該システムは社内 LAN だけからアクセスが可能であり，多くの従業員がほぼ毎日アクセスしている。当該システムが使用しているソフトウェアパッケージ（以下，現行パッケージという）は，最新バージョンの OS をサポートしていない。また，当該システムには，個人情報は保存されていない。

A 社では，毎年 10 名ほどの従業員が退職し，ほぼ同数の従業員が採用されている。入社時には雇用契約書及び秘密保持契約書を含む複数の契約書に署名させている。署名が済むと，システム管理者が，各情報システムに共通の利用者 ID（以下，従業員 ID という）を所属部に応じて，必要な情報システムに登録する。従業員 ID を登録する際には，従業員の氏名及び所属部も一緒に各情報システムへ登録する（以下，従業員 ID，従業員の氏名及び所属部を併せて ID 情報という）。従業員の退職時には，雇用期間中に知り得た秘密を守るという誓約書（以下，退職時誓約書という）への署名を依頼することになっている。

〔情報セキュリティ委員会の開催〕

A 社では，情報セキュリティ委員会を毎月開催している。2017 年 12 月に開催された情報セキュリティ委員会において，同業他社の EC サイトでの大規模なクレジットカード情報の漏えい事件が報告された。そこで情報セキュリティ委員会では，情報セキュリティ点検と，その結果に基づく改善を行うことを決め，その評価基準と情報セキュリティ点検の外部委託先の選定を E さんに指示した。A 社は 10 年前に情報セキュリティポリシ及び関連規程類（以下，A 社規程類という）を策定しているが，これ

までほとんど見直しを行っていない。E さんは，A 社規程類は情報セキュリティ点検の評価基準として適切ではないと考え，JIS Q 27002:2014 の管理策を基に新たに評価基準を作成した。さらに，外部委託先として幾つかの候補を比較検討した。その結果は翌月の情報セキュリティ委員会で審議され，情報セキュリティ点検の実施，及びそこでの指摘事項について A 社が作成する対応方針のレビューを，情報セキュリティ専門会社 U 社に依頼することになった。U 社では情報処理安全確保支援士（登録セキスペ）の P 氏が担当することになった。

〔対応方針の検討〕

情報セキュリティ点検が完了し，P 氏は，図 1 に示す指摘事項を報告した。

指摘事項 1：	掲示板システムが使用しているバージョンの OS は，標準サポート契約期限が切れている。延長サポートサービスが提供されているが，A 社は契約していないので，OS ベンダからパッチが提供されない。そのため既知の脆弱性があり，対応が必要である。
指摘事項 2：	（省略）
指摘事項 3：	幾つかの情報システムで退職者の従業員 ID 及び業務上アクセスが不要になった従業員 ID が有効なままである。
指摘事項 4：	脆弱性を悪用した攻撃を行う機能があり，不正アクセスにも悪用される危険性の高いソフトウェア（以下，高リスクソフトという）が，A 社 EC サイトの脆弱性を検査するために使用されている。
指摘事項 5：	ファイルサーバ用のバックアップテープが劣化してエラーが起き，バックアップが 3 週間取得されていなかった。
指摘事項 6：	A 社 EC サイトではクレジットカード決済を行っているので，クレジットカード情報を保持している。そのため PCI DSS への準拠が必要だが，準拠に必要な要件を満たしているかどうかを確認していない。

図 1　指摘事項（抜粋）

まず E さんは指摘事項 1 について，対応方針を検討することにした。最新バージョンの OS を導入すれば OS の既知の脆弱性はなくなるが，現行パッケージの動作が保証されないこと，また，同等の機能をもつ他製品のソフトウェアパッケージであれば最新バージョンの OS での動作が保証されるが，掲示板システムのデータは，手動で個別に再入力しなければならないことが分かった。E さんは，掲示板システムの利用状況を踏まえて対応方針を検討し，P 氏にその対応方針が適切かを聞いた。P 氏からは，E さんの対応方針は適切であるとの回答が得られた。E さんは，①この対応方

針について情報セキュリティ委員会の承認を得てから，総務部に提示し，対応を指示した。

次に E さんは②指摘事項 2 について，対応方針を検討することにした。その際の P 氏からの助言は，従業員の入社時に締結する秘密保持契約書に，退職後も一定期間は秘密を守るという条項を追加するのがよいというものであった。人事部もその助言に同意し，従業員の入社時に締結する秘密保持契約書に追加することにした。

次に E さんは指摘事項 3 について，対応方針を検討することにした。A 社規程類では，従業員が退職した際，又は各情報システムに業務上アクセスする必要がなくなった際には，当該従業員の従業員 ID の無効化を上司が各情報システムの管理者に申請するように定められているが，申請を忘れてしまうことがあった。E さんは，A 社の管理職全員に，従業員 ID 無効化の申請を忘れずに行うよう注意喚起した。更にリスクを低減するためには，過去，一度だけ実施したことのある従業員 ID の棚卸を定期的に実施することが効果的だと考えた。E さんは P 氏及び社内の関係者と相談の上，従業員 ID の棚卸手順を図 2 のとおり整備した。

手順 1：人事部から前回棚卸以後に退職した従業員一覧（以下，退職者一覧という）を入手する。
手順 2：［ a ］
手順 3：［ b ］
手順 4：不要な従業員 ID の無効化を各システム管理者に申請する。

図 2　従業員 ID の棚卸手順

次に E さんは指摘事項 4 について，対応方針を検討することにした。E さんは，指摘されたソフトウェアを使っていた従業員をよく知っていたので聞いてみたところ，そのソフトウェアである必要はなく，広く一般的に使用されている安全性の高い他のソフトウェアでも十分に検査はできるという報告を受けた。そこで E さんは，高リスクソフトの使用を禁止することにした。

E さんは，インターネットで高リスクソフトを調査して一覧を作成し，対策ソフトのブラックリストに登録することによって高リスクソフトの起動を制限する案を考え，P 氏にレビューを依頼した。P 氏は，③この案の問題点を指摘した。

問題点を指摘された E さんは，代替案として，従業員から利用申請があったソフトウェアが高リスクソフトではないと判断できた場合に，ホワイトリストに登録する案を考え，P 氏にレビューを依頼した。P 氏は，④この案の問題点を指摘した。代替案として，P 氏は，高リスクソフトが含まれているカテゴリをブラックリストに指定することによって，高リスクソフトの起動を禁止する案を提案した。

そこで E さんは，ブラックリストでの制御を有効にする際に旅行営業部の業務に影響が出ないようにする方針を検討し，P 氏の案と併せて情報セキュリティ委員会に提案して承認を受け，総務部に指示した。

次に E さんは指摘事項 5 について，対応方針を検討することにした。ファイルサーバ及びバックアップテープにはクレジットカード情報などの重要な情報が格納されていることから，E さんは，P 氏の助言を得ながら，ファイルサーバとそのデータのバックアップに関するリスクと対策を検討して表 1 にまとめた。

表 1　ファイルサーバとそのデータのバックアップに関するリスクと対策(抜粋)

No.	ファイルサーバとそのデータのバックアップに関するリスク	対策
1	ファイルサーバ上のデータを誤操作で消したり，ランサムウェアによって暗号化されたりした結果，データを利用できなくなるリスク	c
2	ファイルサーバ周辺で火災が発生した結果，データを利用できなくなるリスク	d
3	バックアップの取得が失敗していることに気付かないリスク	e
4	バックアップ対象の設定を誤り，必要なデータのバックアップが取得されないリスク	f

次に E さんは指摘事項 6 について，対応方針を検討することにした。E さんが P 氏に相談したところ，PCI DSS への準拠には多額の費用が掛かるが，［　g　］という方法だと費用が少額で済み，2018 年 6 月の改正割賦販売法の施行にも間に合うのでその方法で対応するとよいと助言された。

E さんは，指摘事項 5 及び指摘事項 6 の対応方針について情報セキュリティ委員会で承認を得た。その後，旅行営業部でその方法を実施することとした。

E さんは，他の指摘事項についても P 氏の助言を得ながら対応方針を検討して対策を実施し，A 社規程類も見直されて，A 社の情報セキュリティは大きく改善した。

設問1　〔対応方針の検討〕について，(1)～(7)に答えよ。

(1)　本文中の下線①について，対応方針として最も適切なものを解答群の中から選べ。

解答群

ア　OS の延長サポートサービスを契約してパッチを入手し，検証用のシステムにパッチを適用し，稼働を検証してから本番システムにパッチを適用する。

イ　速やかに情報システムを停止し，OS ベンダからパッチが提供されるのを待って，提供されたら適用し，稼働を検証する。

ウ　速やかに情報システムを停止し，最新バージョンの OS，及び現行パッケージと同等の他製品のソフトウェアパッケージを導入し，データを移行する。

エ　速やかにデータをバックアップし，最新バージョンの OS を導入した上で現行パッケージを再インストールし，バックアップしたデータをリストアする。

(2)　本文中の下線②について，P 氏の指摘事項はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　退職時誓約書に，秘密を開示した際に A 社が損害賠償を請求するという条項が含まれていない。

イ　退職時誓約書に，不正競争防止法に関する説明が含まれていない。

ウ　退職時誓約書に，有効とは思えないような競業避止条項が含まれている。

エ　退職者から退職時誓約書への署名を拒否されることがあった。

オ　退職者に署名後の退職時誓約書を渡していない。

(3) 図 2 中の［ a ］，［ b ］に入れる字句はどれか。解答群のうち，最も適切なものをそれぞれ選べ。

a，b に関する解答群

ア　ID 情報の一覧の出力を，各システム管理者に依頼する。

イ　ID 情報の一覧の出力を，人事部に依頼する。

ウ　ID 情報の一覧を，在籍する全従業員を登録した名簿から作成する。

エ　ID 情報の一覧を，前回の従業員 ID の棚卸結果から作成する。

オ　退職者一覧及び ID 情報の一覧を P 氏に渡し，無効化すべき従業員 ID が存在していないかの確認を依頼する。

カ　退職者一覧及び ID 情報の一覧を各システム管理者に渡し，無効化すべき従業員 ID が存在していないかの確認を依頼する。

キ　退職者一覧及び ID 情報の一覧を各情報システムを用いる業務の責任者に渡し，無効化すべき従業員 ID が存在していないかの確認を依頼する。

ク　退職者一覧及び ID 情報の一覧を人事部に渡し，無効化すべき従業員 ID が存在していないかの確認を依頼する。

(4) 本文中の下線③について，P 氏が指摘した問題点を二つ，解答群の中から選べ。

解答群

ア　調査から漏れた高リスクソフトが使われてしまう可能性がある。

イ　高リスクソフトの使用はライセンス違反になる可能性がある。

ウ　高リスクソフトを継続的に調査して登録し続けることは工数が掛かりすぎる。

エ　ブラックリストを利用して高リスクソフトの使用を禁止するとマルウェアを検知できなくなる。

オ　ブラックリストを利用すると PC が A 社 EC サイトにアクセスできなくなる可能性がある。

(5) 本文中の下線④について，P 氏が指摘した問題点を三つ，解答群の中から選べ。

解答群

ア　申請されたソフトウェアが高リスクソフトではないことの判断が難しい場合がある。

イ　申請されたソフトウェアが高リスクソフトではないことを確認し，検証する工数が掛かりすぎる場合がある。

ウ　ソフトウェアの利用申請から，実際に利用できるようになるまで時間が掛かるので，業務に影響が出る場合がある。

エ　ソフトウェアをホワイトリストに登録すると，そのソフトウェアのライセンス違反になる場合がある。

オ　対策ソフトには，従業員がソフトウェアの利用を申請する機能がない場合がある。

(6) 表1中の [c] ～ [f] に入れる字句はどれか。解答群のうち，最も適切なものをそれぞれ選べ。

c ～ f に関する解答群

ア　一時的に構築した情報システムに，バックアップテープの全ファイルをリストアし，ファイル比較ツールを使用してファイルサーバのバックアップ対象ファイルと比較し，ファイルが減っていないことを確認する。

イ　現在のバックアップに加え，日次で増分バックアップを行い，増分バックアップを6世代分取得し，世代ごとに別のバックアップテープに保存する。

ウ　テープバックアップ装置を，より高速な製品に交換する。

エ　バックアップ先の媒体をバックアップテープからハードディスクに変更する。

オ　バックアップ中にエラーが発生したら電子メールでシステム管理者に通知するツールを導入する。

カ　バックアップテープをエラーの起きにくい信頼性の高い製品に変更する。

キ　バックアップを2組み取得し，うち1組みを遠隔地に保管する。

ク　ファイルサーバに対策ソフトを導入する。

ケ　ファイルサーバのファイル一覧を出力した後，ファイルを全て消去し，バックアップテープのデータをファイルサーバにリストアして出力したファイル一覧と照合し，ファイルが減っていないことを確認する。

(7) 本文中の［ g ］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。

g に関する解答群

ア　A 社 EC サイトに対して ASV（認定スキャニングベンダ）による脆弱性スキャンを実施し，発見された全ての脆弱性に対応する

イ　A 社 EC サイトの決済機能を変更することによって，クレジットカード情報の非保持化を実現する

ウ　A 社 EC サイトのシステム運用業務を外部業者に委託する

エ　A 社 EC サイトのペネトレーションテストを外部業者に委託し，指摘された内容を全て修正する

オ　ISO/IEC 27001:2013 又は JIS Q 27001:2014 認証，及び ISO/IEC 27017:2015 に基づく認証を取得している組織のクラウドサービスを利用して A 社 EC サイトを再構築する

カ　クレジットカードの取扱いをやめることによって，クレジットカード情報漏えいのリスクを回避する

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，<u>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</u>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]

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 退室可能時間中に退室する場合は，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	13:10 ～ 13:50

7. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，次のものに限ります。

   なお，会場での貸出しは行っていません。

   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。

試験問題に記載されている会社名又は製品名は，それぞれ各社又は各組織の商標又は登録商標です。なお，試験問題では，™ 及び ® を明記していません。

©2018　独立行政法人情報処理推進機構