全問が必須問題です。必ず解答してください。

問1　標的型攻撃メールの脅威と対策に関する次の記述を読んで，設問1，2に答えよ。

Y社は，事務用機器を主力商品とする販売代理店である。従業員数は1,200名であり，本社には営業部，情報システム部，総務部などがある。

〔PCのマルウェア感染〕

ある日，情報システム部は，Y社内の1台のPCが大量の不審なパケットを発信していることをネットワーク監視作業中に発見し，直ちに外部との接続を遮断した。

情報システム部による調査の結果，営業部に所属する若手従業員G君が，受信した電子メール（以下，電子メールをメールという）の添付ファイルを開封したことが原因で，G君のPCがマルウェアに感染し，大量のパケットを発信していたことが判明した。幸いにも，情報システム部の迅速な対処によって，顧客情報の漏えいなどの最悪の事態は防ぐことができた。

〔受信したメール〕

情報システム部のS主任は，営業部の情報セキュリティリーダであるE課長に，今回の事態に関する調査結果を報告した。次は，その時の会話である。

S主任　：G君が受信したメールは，いわゆる標的型攻撃メールと呼ばれるものです。標的型攻撃メールとは，［　a　］の組織や個人を対象として，受信者のPCにマルウェアを送りつけ，情報を窃取することなどを目的とするメールであり，［　b　］の組織や個人を対象として送られるウイルスメールとは異なるものです。

E課長　：最近は国内でも標的型攻撃メールに起因する情報漏えい事故が多数発生しており，大手企業や官公庁以外もターゲットになり得るので，営業部の従業員には十分に注意するよう言っていたのだが。

S主任　：標的型攻撃メールでは，注意していたつもりでも，気付かずにマルウェア感染が起こります。また，受信者が疑いをもたないように，メールの差出人を公的機関などに詐称したり，メールの件名や内容を受信者の業務に関連したものに偽装したりするといった，［　c　］を利用します。

E 課長　：G 君が受信したメールを具体的に説明してくれるかな。

S 主任　：メールの内容を図 1 に示します。この内容から，①受信者の疑いを低減させる手口や，受信者の動作を巧みに誘導する手口などが見受けられます。

S 主任は，②標的型攻撃メールによく見られる注意すべき特徴のうち，G 君が受信したメールに見られる特徴を説明した。

差出人：F <F@zz-freemail.co.jp>　　送信日時：2016/03/18 10:22
宛先　：info@y-sha.com
CC　　：
件名　：Re: Re: 【至急】製品導入に関する問合せ

添付ファイル：質問事項.exe

G様

お世話になっております。
先日，貴社の製品について問合せをしたX社のFです。
これまで，貴社の事務用機器に関する情報を提供していただき，
ありがとうございました。
弊社では，今回，貴社から提案していただいた製品について，
導入する方向で検討を進めております。
その中で，確認したい事項が幾つか出てきました。
つきましては，急なお願いで恐縮ですが，添付ファイルの質問内容を
ご確認の上，本日15時までに回答をいただけないでしょうか。
よろしくお願いいたします。

---
X社　調達部　F
E-mail: F@x-sha.co.jp
URL: http://www.x-sha.co.jp

図 1　G 君が受信したメールの内容

〔ヒアリング〕

S 主任からの調査報告を受けた E 課長は，G 君に対して，このメールを受信した際の状況及び対応に関してヒアリングをした。また，Y 社の情報セキュリティインシデント管理規程（以下，管理規程という）どおりには対応しなかった理由を G 君に確認した。

E課長がまとめたヒアリング結果を図2に，Y社の管理規程を図3に示す。

・X社は過去に取引がある会社であった。
・F氏と直接会ったことは無かったが，10日前から，製品の問合せが3回あり，メールでやり取りをしていた。
・メールの添付ファイルを開封した際は，見慣れないウィンドウが表示されただけでドキュメントは開くことができなかった。そこで，ファイルを再送してほしい旨を先方にメールで返信したが，15時までと急いでいた割にその後の返信が無く不審に思った。再度連絡しようと思っていたが，別件で多忙になり，確認ができなかった。
・その後，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が発生していたが，その都度，PCを再起動するなどして解決を試みた。また，ウイルス対策ソフトが動作し，パターンファイルが最新になっていることを確認できたのでマルウェア感染はあり得ないだろうと考え，誰にも相談せず，報告もしなかった。
・以前に他の部のH君が，顧客から貸与されたUSBメモリをPCに接続してマルウェア感染が起きたことを上司に報告した際に，上司から大変厳しく叱責されたとH君本人から聞いていたので，マルウェア感染と確信できない限りは，報告したくないと思っていた。
・管理規程については，新入社員研修の際に一度見たことがある程度で，重要な規程とは思っていなかった。
・標的型攻撃メールについては，聞いたことはあったが理解はしていなかった。

図2　G君へのヒアリング結果

第1章　情報セキュリティインシデント（以下，インシデントという）の定義
・インシデントとは次のことをいう。
“不正アクセス”，“マルウェア感染”，“情報の漏えい”，“情報の改ざん”，“情報の消失”，
（省略）
第2章　インシデント検知時の報告及び対処
・従業員は，インシデントを発見した際には，速やかに情報セキュリティリーダに報告し，その指示に従うこと。
なお，インシデントであるかどうか判断がつかない疑わしい事象も，自己判断せず同様に報告すること。
・情報セキュリティリーダは，インシデントを認知した場合には，その状況を確認し，情報セキュリティ責任者に速やかに報告するとともに，情報システム部と連携し，被害の拡大防止を図るための応急措置及び復旧に係る指示又は勧告を行うこと。
・従業員は，各自の判断で復旧対応や解決を試みるのではなく，必ず情報セキュリティリーダの指示又は勧告に従うこと。
第3章　インシデントの原因調査及び再発防止
・情報セキュリティリーダは，情報システム部と協力してインシデントの原因を調査するとともに，再発防止策を検討し，報告書にまとめて情報セキュリティ責任者に報告すること。
（省略）

図3　管理規程

〔情報セキュリティ意識向上に向けて〕

次は，ヒアリング実施後のE課長とS主任との会話である。

S主任　：標的型攻撃メールによるマルウェア感染を完全に防ぐことは難しいので，被害を最小化するためには，メールの添付ファイルを開封した後に従業員が適切な対応を取ることが重要になります。

E課長　：そうだね。③今回の初動対応における問題点は二つあったと思う。本来であれば，管理規程に基づき，疑わしい事象を発見した従業員は，［　d　］に報告をしなければならない。また，報告に当たっては，［　e　］報告することも重要だ。

S主任　：おっしゃるとおりです。今回の問題点を解決するには，規程やルールは単に策定しただけでは不十分であり，それらが順守されるように［　f1　］，［　f2　］の2点を行うことが重要だと考えられます。

E課長　：今回のような標的型攻撃メールなどへの対策に当たっては，従業員一人一人の情報セキュリティ意識を向上させる地道な活動が必要だと思う。まずは，④実際に攻撃を受けた場合にも一人一人が適切に対応できるかを定量的に測定し評価できるようにしていきたい。そのための全社的な取組みも情報システム部で実施してもらえないだろうか。

S主任　：承知いたしました。検討し実施したいと思います。

E課長からの提案もあって，Y社では，従業員の情報セキュリティ意識向上に着実に取り組むようになった。

設問1　〔受信したメール〕について，(1)～(4)に答えよ。

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

a，bに関する解答群

| | | |
|---|---|---|
| ア　海外 | イ　架空 | ウ　官界 |
| エ　国内 | オ　大企業 | カ　中小企業 |
| キ　特定 | ク　不特定多数 | ケ　民間 |

(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　AES | イ　ゼロデイ攻撃 |
| ウ　ソーシャルエンジニアリング | エ　トロイの木馬 |
| オ　ヒヤリハット | カ　ブルートフォース攻撃 |

(3)　本文中の下線①について，今回の攻撃者が使った手口として考えられるものを二つ，解答群の中から選べ。

解答群

ア　製品を導入する方向で検討を進めているという趣旨を伝えた上で，質問の回答期限を指定することによって添付ファイルを開くよう誘導している。

イ　メールの本文にY社の従業員しか知り得ない情報を記載することによって疑いを低減している。

ウ　メールの本文に正当なURLを装ったリンクを記載した上で，そのURLリンクをクリックするよう指示し，誘導している。

エ　メールのやり取りを数回行うことによって疑いを低減している。

(4) 本文中の下線 ② について，次の (i) ～ (iii) のうち，G 君が受信したメールに見られる特徴だけを全て挙げた組合せを，解答群の中から選べ。

(i) 差出人のメールアドレスがY社の社内メールアドレスに詐称されている。

(ii) 差出人のメールアドレスと，本文の末尾に記載された署名のメールアドレスが異なる。

(iii) 実行形式ファイルが添付されている。

解答群

| | | |
|---|---|---|
| ア (i) | イ (i), (ii) | ウ (i), (ii), (iii) |
| エ (i), (iii) | オ (ii) | カ (ii), (iii) |
| キ (iii) | | |

設問2 〔情報セキュリティ意識向上に向けて〕について，(1) ～ (5) に答えよ。

(1) 本文中の下線 ③ について，次の (i) ～ (iv) のうち，今回の初動対応における問題点を二つ挙げた組合せを，解答群の中から選べ。

(i) PC の不具合に気付いても直ちに再インストールなどの復旧対応を行わなかった点

(ii) 問合せ対応を行うに当たって，X社との最近の取引記録を確認しなかった点

(iii) 不審な事象が起きたにもかかわらず，情報セキュリティリーダに報告しなかった点

(iv) 不審な事象が起きたにもかかわらず，マルウェアには感染していないと自己判断した点

解答群

| | | |
|---|---|---|
| ア (i), (ii) | イ (i), (iii) | ウ (i), (iv) |
| エ (ii), (iii) | オ (ii), (iv) | カ (iii), (iv) |

(2) 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　インシデントであると判断した後

イ　原因調査後

ウ　再発防止策を検討した後

エ　速やか

(3) 本文中の［ e ］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。

e に関する解答群

ア　誤った報告を行わないよう，事象をインターネットや書籍などで確認して，類似の事例が確認できたものを

イ　判断に迷う事象であっても自己判断せずに

ウ　部内の同僚と相談してから，報告するように勧められた事象を

エ　報告事項がそろうのを待って，レポートにまとめたものを

(4) 本文中の［ f1 ］，［ f2 ］に入れる，次の (i) ～ (iv) 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) 管理規程の内容に関する従業員への周知

(ii) 情報共有や報告が包み隠さず行われるような組織文化の醸成

(iii) 情報セキュリティにおけるクラッキング手法の教育

(iv) マルウェア感染時の迅速な復旧対応方法の指導

f に関する解答群

| | f1 | f2 |
|---|---|---|
| ア | (i) | (ii) |
| イ | (i) | (iii) |
| ウ | (i) | (iv) |
| エ | (ii) | (iii) |
| オ | (ii) | (iv) |
| カ | (iii) | (iv) |

(5) 本文中の下線 ④ について，E 課長の提案に応える取組みはどれか。解答群のうち，最も適切なものを選べ。

解答群

ア 標的型攻撃メールについて，従業員の PC がマルウェア感染しないために注意すべき事項を標語として作成して掲示する。

イ 標的型攻撃メールへの対策を題材とする DVD 上映会を年に 2 回開催し，従業員の出席率を確認する。

ウ 標的型攻撃メールを起因とするインシデントについて，他社で発生した事例を月に 1 回，イントラネット上の掲示板で紹介する。

エ 模擬の標的型攻撃メールを従業員に期間を空けて何回か送付し，添付ファイル開封後の報告完了率，報告完了までに要した時間などの変化を調査する。