問３　業務用 PC での Web サイト閲覧に関する次の記述を読んで，設問１～３に答えよ。

P 社は，従業員数 1,000 名の消費者向け健康食品製造会社であり，経営方針として自社のブランドイメージを重視している。P 社のマーケティング部では，社外向け Web サイトのコンテンツのうち，製品紹介情報，IR 情報，CSR 情報などの管理を行っている。マーケティング部には 20 名が在籍し，二つの課がある。マーケティング 1 課は，ブランドマーケティング戦略を担当している。マーケティング部では，情報セキュリティ責任者を A 部長が，情報セキュリティリーダをマーケティング 1 課の B 課長が務めている。

P 社では全従業員が基盤情報システムを利用して日々の業務を行っている。基盤情報システムは，会社貸与の業務用 PC（以下，PC という），LAN 及びインターネット接続から成るネットワークサービス，ディレクトリサービス，社内ファイル共有サービス，電子メールサービスなどから構成されている。P 社従業員は，LAN に接続された各自の PC から各サービスを利用している。また，LAN からのプロキシサーバを経由しないインターネット接続はファイアウォールによって遮断されている。

P 社には，基盤情報システム以外にも勤怠管理システム，交通費精算管理システム及び人事管理システムがある。P 社従業員は，出勤時と退勤時に各自の磁気ストライプカード型の従業員証をタイムレコーダに通すことになっており，出退勤時刻が勤怠管理システムに記録される。P 社の課長以上の職位の者は，直属の部下について，勤怠管理システムを用いて出退勤時刻などの勤怠管理情報を，交通費精算管理システムを用いて交通費精算情報を，人事管理システムを用いて人事評価情報を確認できる。

基盤情報システム，勤怠管理システム，交通費精算管理システム及び人事管理システムは同じタイムサーバに基づいて時刻同期がなされている。それらの情報システム及び自社 Web サイトの構築と運用管理は，情報システム部が行っている。

情報システム部の C 部長が，P 社の最高情報セキュリティ責任者（CISO）を務めている。情報システム部には運用管理課があり，基盤情報システムに対して図 1 に示す設定と運用管理を行っている。また，利用については図 2 に示す P 社基盤情報システム利用規程（以下，利用規程という）を整備している。

1. 設定
・PC 上のハードディスクドライブ（以下，HDD という）全体を暗号化
・PC 上の Web ブラウザで，プロキシサーバを利用するように設定
・社内ファイル共有サービスでの共有フォルダの設定は，次のとおり
　- ディレクトリサービスを利用してアクセス権の設定を管理
　- アクセス権は，各利用部門からの申請に応じて設定単位を変更可能
　- アクセス権の設定単位は，次のいずれか一つを選択
　　部単位：特定の部に属する従業員だけがアクセス可能
　　課単位：特定の課に属する従業員だけがアクセス可能
　　職位単位：特定の部に属する部長，課長，主任のいずれかの職位以上の従業員だけがアクセス可能
　　従業員単位：特定の従業員だけがアクセス可能
　- デフォルトのアクセス権は，課単位
2. 運用管理
・PC 上の OS，オフィスソフト，Web ブラウザ，ウイルス対策ソフトなどのソフトウェアのインストール，パッチ適用及びアップデートを一括で運用管理
・一括運用管理対象のソフトウェアのパッチ及びアップデートがベンダからリリースされた場合は，適用要否の確認を速やかに行い，適用が必要と判断したものを適用
・PC の管理者権限は，PC 運用管理担当者だけに付与
・各利用部門からの情報システム利用に関する各種申請について，利用規程にのっとった承認を得たものだけを受理

図 1　P 社基盤情報システムにおける設定と運用管理（抜粋）

1. パスワードは，使用できる文字種（大小英字，数字，記号）全てを組み合わせて 8 文字以上，かつ，他人に推測されにくいものとし，他人に知られないよう適切に管理すること。
2. 機密性が高い電子データには，暗号化を施し，適切なアクセス権を設定すること。
3. 各利用部門から情報システム部への情報システム利用に関する各種申請については，所属部門長及び情報セキュリティリーダの承認を得ること。
　なお，機密性が高い情報の取扱いに関連する申請内容については，CISO の承認を得ること。
4. 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）の発生時には，その対応として第一に被害拡大防止に努め，第二に証拠保全に努めること。
　なお，所属部門の情報セキュリティリーダ又は情報システム部からの指示があった場合には，その指示に従うこと。

図 2　利用規程（抜粋）

〔インシデントの発見と初動対応〕

9 月 26 日（月）10 時，運用管理課の H さんが基盤情報システムを運用監視していたところ，9 月 23 日（金）20 時から 25 日（日）にかけての社内からインターネットへの通信量が前週の金曜日から日曜日にかけてのものと比較して大幅に増えていることを発見し，直ちに運用管理課の D 課長に報告した。D 課長は不審に思い，プ

ロキシサーバのログを調査するよう H さんに指示した。その結果，図 3 に示すことが判明した。

・大量の通信は，同一の社外 IP アドレス（以下，アドレス Y という）へのアクセスであった。
・POST メソッドから始まって CONNECT メソッドが連続した HTTP over TLS（HTTPS）通信であった。
・発信元はマーケティング 1 課に所属する入社 2 年目の E さんの PC（以下，E-PC という）であった。

図 3　プロキシサーバのログの調査結果

D 課長はその旨を C 部長に報告の上，B 課長に連絡した。連絡を受けた B 課長は利用規程にのっとり，①E さんに初動対応を指示し，併せて A 部長に報告した。

B 課長は，自席の PC を利用して E さんの［ a1 ］を調査した。E さんは市場調査業務を担当しているので，P 社の競合情報，消費者動向などについての様々なインターネット上の Web サイトを日々閲覧している。次に情報システム部の協力の下，B 課長による調査結果と E-PC から［ a2 ］へのアクセスログとを突き合わせたところ，大量の通信が記録されていた時刻の中には，E さんが［ a3 ］時刻が含まれていた。さらに，E さんへの聞き取り調査を行ったところ，E さんは，P 社が入居するオフィスビルの法定点検に基づく停電時以外は離席，外出又は帰宅の際，E-PC にログインしたままにしていたことが判明した。これらのことから，今回の不審なアクセスは，E さん自身によるものではないと推定された。

B 課長と D 課長による協議の結果，同日 15 時に，情報システム部による調査及び対応が開始された。情報システム部における調査の結果を図 4 に，各事象の発生日時を表 1 に示す。

・E-PC は，不正プログラム V に感染していた。
・不正プログラム V は，E-PC にインストールされていたソフトウェア Z（以下，ソフト Z という）の脆弱性 M を突いて侵入するものであった。ソフト Z は，インストールされて以来，パッチが適用されていなかった。
・E-PC 上では，ウイルス対策ソフトが起動しないように管理者権限を用いて設定されていた。

図 4　情報システム部における調査の結果（抜粋）

表1　各事象の発生日時

日付	時刻	事象
7月4日	11:00	E さんが，業務の都合から，しばらくの間，E-PC 上のウイルス対策ソフトが起動しないように設定してほしいと H さんに依頼
	11:30	H さんが，E-PC 上のウイルス対策ソフトが起動しないように管理者権限で設定
8月2日	15:00	ソフト Z の開発元が脆弱性 M の対策パッチをリリース
8月4日	10:00	ウイルス対策ソフトの開発元が，不正プログラム V に対応するパターンファイルをリリース
9月23日	20:00	E-PC がアドレス Y に向けた通信を開始
9月26日	10:00	H さんが通信量の大幅増加を発見，D 課長に報告 H さんがプロキシサーバのログを調査開始
	13:30	H さんがプロキシサーバのログの調査結果を D 課長に報告 D 課長が C 部長に報告，B 課長に連絡
	13:45	B 課長が E さんに初動対応を指示，A 部長に報告後，E さんへの聞き取り調査などを開始
	14:30	B 課長と D 課長が協議
	15:00	②情報システム部が，次に示す調査及び対応を開始 ・社内からアドレス Y への通信を遮断 ・E-PC の HDD 内のデータを証拠保全 ・E-PC からの大量の通信の原因の把握

注記　日付は全て同年のものである。

〔情報システム部による調査結果の中間報告〕

情報システム部による E-PC の調査結果の中間報告が，9 月 27 日（火）13 時から行われた。次は，その時の D 課長と B 課長の会話である。

D 課長 ：マーケティング部と情報システム部の間では，ソフト Z に対するパッチ適用を含めた運用管理について何も取決めがない状態でした。マーケティング部からのソフトウェアインストール申請書には，パッチ適用などの運用管理についての依頼は記載されていませんでした。

B 課長 ：すみません，依頼内容が不十分でしたね。

D 課長 ：他にもこれらと同じようなことがあったら問題なので，引き続き調査をします。ところで，7 月 4 日から昨日までのログ中の通信先を解析したところ，ウイルス対策ソフトの開発元などによって悪意ある Web サイトと判断された URL 又は IP アドレスに該当するものはありませんでした。感染原因は，電子メールの添付ファイルや USB メモリからと考えられますが，も

し，感染原因がインターネット上の Web サイトへのアクセスだとしたら，E さんがアクセスしたのは，閲覧するだけで不正プログラムに感染するように，企業の［ b ］の公開 Web サイトが［ c ］されたものだったとも考えられます。

B 課長 ：［ b ］の URL ということであれば，悪意ある Web サイトだとは思わないので，防ぎようがないですね。Web サイトが［ c ］されたことによって，その Web サイトの所有者たる企業は［ d ］となるだけでなく，Web サイト閲覧者に対しても不正プログラムによる被害が及ぶので，［ e ］の立場になってしまうおそれがあり，非常に怖いですね。③私自身の職務からも人ごとではないので，すぐに対策を検討しましょう。D 課長，協力をお願いします。

〔課題の改善〕

内容が不明なデータが E-PC から社外に大量に送信されたことから，［ f ］が起きたおそれもあると B 課長は考えた。そこで E さんにヒアリングした。その結果，マーケティング 2 課へのヒアリングも必要と考えられたので，マーケティング 2 課のプレゼントキャンペーン担当を務めている G 主任にもヒアリングを行った。それらの結果を図 5 に示す。

1. E さんへのヒアリング結果
・マーケティング 2 課が 8 月に募集した，P 社製品購入者向けプレゼントキャンペーンの匿名アンケート結果に関するファイル（以下，アンケートファイルという）を，9 月 8 日（木）頃，社内共有フォルダ N 内で発見した。
・④いつか業務に役立つかもしれないと考え，アンケートファイルを社内共有フォルダ N から E-PC 内にコピーした。
・E-PC 内には，暗号化されたアンケートファイルを復号したものはなかった。また，アンケートファイル以外には機密性が高い情報を含んだファイルはなかった。
2. G 主任へのヒアリング結果
・アンケートファイルの暗号化には，マーケティング部内の共有パスワードを利用していた。
・アンケートファイルは，G 主任を含めたマーケティング 2 課のプレゼントキャンペーン担当者 3 名が共同作業できるように，社内共有フォルダ N に保存していた。
・アンケート結果には，P 社製品の味や食感，健康食品としての有用性などへの批評や競合会社製品との比較による辛らつな意見が書かれていた。

図 5　B 課長による，E さん及び G 主任へのヒアリング結果

B 課長は，A 部長にこれまでの調査結果の報告を行うとともに，図 6 に示す項目の検討が必要であると進言した。

1. 調査結果から発見された，改善すべき課題
 1-1 ソフト Z の運用管理についてマーケティング部と情報システム部の間で取決めがなかった。
 1-2 E さんと H さんの当事者間だけで E-PC 上のウイルス対策ソフトの停止を決めていた。
 1-3 H さんが E-PC 上のウイルス対策ソフトを起動するように設定を戻すのを忘れていた。
 1-4 E さんが業務と直接関係ないマーケティング 2 課の管理下のアンケートファイルを E-PC 上に保存していた。
 1-5 アンケートファイルの暗号化のパスワードが，部内の共有パスワードであった。
2. 情報システム部の調査から［ f ］が発生したことが確かになった場合の対処
 2-1 P 社所在地管轄の警察署や関係機関への届出又は報告
 2-2 アンケートファイルの関係者へのおわびと説明，社外への公表

図 6　検討が必要な項目

B 課長は，社内関係者の協力を得て課題の改善を実施した。また，中間報告以降の情報システム部の調査結果から［ f ］が発生したおそれは低いことが分かった。

B 課長は，改善すべき課題が図 6 の 1-1 から 1-5 の他にもないかの確認を A 部長に提案し，了承を得た。

B 課長は，改善すべき課題が他にもないか，［ g ］を実施した。その結果，他の課題が発見され，マーケティング部内で改善策の検討が開始された。

A 部長は，マーケティング部内での他の課題の発見に至った B 課長の提案を高く評価した。発見された課題とその改善策を A 部長が P 社経営陣に報告したところ，これらの提案は，全社的な改善活動に発展した。

設問1　〔インシデントの発見と初動対応〕について，(1) ～ (3) に答えよ。

(1) 本文中の下線①について，次の (i) ～ (v) のうち，B 課長が E さんに指示すべき初動対応だけを全て挙げた組合せを，解答群の中から選べ。

(i) E-PC の HDD 内のフォルダとファイルに対して何も操作をしない。

(ii) E-PC の電源を強制切断し，かつ，電源ケーブルを電源コンセントから外す。

(iii) E-PC を LAN から切り離す。

(iv) E-PC を再起動する。

(v) E-PC を使って E さんの基盤情報システムへのログインパスワードを変更する。

解答群

ア (i)　　イ (i)，(iii)　　ウ (i)，(iv)，(v)

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

キ (iii)，(v)　　ク (iv)，(v)

(2) 本文中の［ a1 ］～［ a3 ］に入れる字句の組合せはどれか。a に関する解答群のうち，最も適切なものを選べ。

a に関する解答群

	a1	a2	a3
ア	勤怠管理情報	インターネット	退勤していた
イ	勤怠管理情報	ディレクトリサービス	休暇を取得していた日の
ウ	交通費精算情報	社内ファイル共有サービス	外出していた
エ	交通費精算情報	ディレクトリサービス	出張していた日の
オ	人事評価情報	インターネット	無断欠勤していた日の
カ	人事評価情報	社内ファイル共有サービス	残業していた

(3) 表1中の下線②について，次の(i)～(v)のうち，該当する作業だけを全て挙げた組合せを，解答群の中から選べ。

(i) E-PCのHDDを別のHDDにフルコピーし，その別のHDDを“秘密”とラベルに書いた資料保存用紙封筒に入れ，封印し，Eさんが管理するマーケティング部の鍵付きロッカーに保管

(ii) E-PCのHDDを別のHDDにフルコピーした上で，最新のパターンファイルを搭載した別のPCに，その別のHDDを接続してフルスキャンを実施

(iii) アドレスYへの通信をプロキシサーバで遮断し，ファイアウォールではインターネットへの通信のうち，プロキシサーバを経由しないものだけを許可

(iv) 他の作業に先駆けて最初にE-PCにOS及びアプリケーションのクリーンインストールを実施した上で，E-PCをEさんに返却

(v) プロキシサーバなどのネットワーク機器上のログとE-PC上のイベントログなどを時系列に沿って整理及び分析

解答群

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

設問2 〔情報システム部による調査結果の中間報告〕について，(1)，(2)に答えよ。

(1) 本文中の［ b ］～［ 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。

b，cに関する解答群

ア 改ざん	イ 偽装	ウ 正規
エ 設計	オ 非正規	カ ボット化

d，eに関する解答群

ア 加害者	イ 首謀者	ウ 助言者
エ 扇動者	オ 第三者	カ 被害者

(2) 本文中の下線③について，B課長とD課長はどのような対策を検討したか。解答群のうち，最も適切なものを選べ。

解答群

ア 自社Webサイトのアクセシビリティを見直し，自社Webサイトの閲覧者に対する利便性と安全性を確保することによって，自社のブランドイメージの向上を図る。

イ 自社Webサイトの改ざんを防ぐために，自社Webサーバを情報システム部に依頼して速やかに停止させ，自社 Web サーバを社外のパブリッククラウド上に移行し，他者とのリスク共有（リスク移転）を図る。

ウ 自社 Web サイトの脆弱性検査を定期的に実施して，問題があれば修正する。また，新たな脆弱性が発見された場合にも必要な対応をとる。

エ 自社 Web サイトのトップページ上において，重要なお知らせとして，自社 Web サイトにドライブバイダウンロードが仕掛けられた可能性があると公表し，自社Webサイトの閲覧者に対して注意を喚起する。

設問3 〔課題の改善〕について，(1)～(3)に答えよ。

(1) 本文中及び図6中の［ f ］に入れる字句はどれか。解答群のうち，最も適切なものを選べ。

fに関する解答群

ア E-PC への DDoS 攻撃　　イ E-PC への辞書攻撃

ウ E-PC への総当たり攻撃　　エ 情報改ざん

オ 情報破壊　　カ 情報漏えい

(2) 図5中の下線④について，社内共有フォルダNのアクセス権の設定単位はどのようになっていたと考えられるか。解答群のうち，最も適切なものを選べ。

解答群

ア 課単位　　イ 従業員単位　　ウ 職位単位　　エ 部単位

(3) 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　情報システムのうち，マーケティング部内の従業員が利用しているものに対し，脆弱性検査

イ　マーケティング部内で取り扱っている全ての情報資産とその取扱い状況を可視化した上で，リスクアセスメント

ウ　マーケティング部内で取り扱っている全てのファイルの所在と所有者を洗い出し，各ファイルのアクセス権限の見直し

エ　マーケティング部における，E-PC 以外でのウイルス対策ソフトを停止させたままの PC 又はパッチ適用並びにアップデートが行われていない PC の有無の確認

オ　マーケティング部における，E-PC 以外でのソフト Z がインストールされた PC の有無と利用状況の確認