問 11　コンピュータウイルス対策の監査に関する次の記述を読んで，設問 1～4 に答えよ。

S 社は，広告業を営む中堅企業である。S 社では，最近，ある従業員が顧客に渡した USB メモリがコンピュータウイルス（以下，ウイルスという）に感染していたということが，顧客からのクレームによって分かった。S 社で調査した結果，当該従業員は，“委託先事業者にデータ加工を依頼するために，当該データを会社支給の USB メモリに入れて渡した。その後，委託先事業者から USB メモリを受け取り，データの内容を確認した後，当該 USB メモリを顧客に渡した”とのことであった。

S 社では，この事故を重く受け止めて，情報システム部門が中心になって事故の再発防止策の策定及び現状のウイルス対策の見直しを行うことになった。また，監査部においても，事故原因，ウイルス対策の状況などについて確認し，その結果を情報システム部門が行う再発防止策の策定及び現状のウイルス対策の見直しの検討に役立てることになった。監査部長は，U 君をリーダとする監査チームを編成した。

〔予備調査での判明事項（抜粋）〕

(1) S 社で使用しているウイルス対策ソフトの機能は，次のとおりである。

① サーバのウイルス対策ソフト及びそのパターンファイルは，設定した時刻に自動的に更新されるようになっている。また，PC のウイルス対策ソフト及びそのパターンファイルについては，PC を社内 LAN に接続した時点で自動的に更新される。ウイルス対策ソフトには管理ツールが提供されており，ウイルス対策管理サーバ内に蓄積される情報をウイルス対策管理者用 PC から検索して，サーバ，PC のウイルス対策ソフト及びパターンファイルのバージョンを確認することができる。

② ウイルス対策ソフトは，サーバ，PC のメモリ上に常駐し，リアルタイムでウイルススキャンを行うとともに，ハードディスクのウイルススキャン（以下，ハードディスクスキャンという）を自動又は手動で行うことができる。

なお，ハードディスクスキャンの自動実行日時は，PC 設置時に，毎週月曜日の正午に設定されており，利用者は変更できないようになっている。ただし，その日時に起動されていないサーバ，PC では，ハードディスクスキャンは実行されない。

③ サーバ，PC には，ウイルス検知の状況，ハードディスクスキャンの実行日時などがログとして記録される。これらのログは，ウイルス対策管理サーバ内にも蓄積されており，管理ツールを利用して，ウイルス対策管理者用 PC から条件を設定して検索することができる。また，利用者も自身の PC のログを確認することができる。

④ メールサーバでは，送受信される電子メール（以下，メールという）についてウイルススキャンを実施している。メール受信時にウイルスを検知した場合には，感染した添付ファイルを取り除いた後，そのメールにウイルスを検知した旨の通知文を添えて受信者に送信する。メール送信時にウイルスを検知した場合には，メールの送信は行わず，送信者にその旨を連絡する。

(2) S 社のセキュリティポリシには，ウイルス対策として次の事項が義務付けられている。

① ウイルススキャンによって添付ファイルがウイルスに感染していることが検知された場合，又は不審なメールを受信した場合には，ウイルス対策管理者にメールで通知すること。また，サーバ又は PC がウイルスに感染した場合には，当該機器を LAN から切り離した上で，ウイルス対策管理者に電話で連絡すること。

② ハードディスクスキャンの実行日時を定期的に確認し，ハードディスクスキャンが自動で実行されていない場合には手動で実行すること。

(3) ウイルス対策管理者が実施している主なウイルス対策管理は，次のとおりである。

① サーバについては，ウイルス対策ソフト及びパターンファイルの更新状況，ハードディスクスキャンの実行状況，並びにウイルス検知の状況について週次でログを確認している。PC については，ベンダからウイルス感染について重大な注意喚起があった際などに同様の事項を確認している。

② 利用者からウイルスの検知，感染などの連絡を受けた場合には，報告日，ウイルスの種類，報告元，感染源，被害状況などを記録簿に記載している。

(4) その他，ウイルス対策管理者などにインタビューを実施して把握できた事項は，次のとおりである。

① 利用者は，配布されている PC を外出先，自宅などに持ち出すことができる。社外からは，PC を社内 LAN に接続することはできないが，自身のスマートフ

ォンから社内メールを送受信したり，社内掲示版を閲覧したりすることができる。

② まれに利用者から“社内 LAN にログインしてもウイルス対策ソフト，パターンファイルが正常に更新されない”との問合せがある。しかし，発生頻度が低く，ほとんどの場合，次にログインしたときに更新されるようなので，今のところ特に対応は行っていない。

③ ハードディスクスキャンが自動で実行されている途中で，手動でスキャンを中止する利用者もいる。

(5) 今回の事故の状況を把握するために，事故を起こした従業員，ウイルス対策管理者などにインタビューを行った。その結果は次のとおりである。

① 業務で USB メモリなどの外部記憶媒体を利用せざるを得ない場合が多く，セキュリティポリシでも外部記憶媒体の利用は禁止されていない。

② 当該従業員が，委託先事業者から USB メモリを受け取って顧客に渡すまでの間に最新のパターンファイルで USB メモリのスキャンを実施していれば，ウイルスを検知できたとのことであった。しかし，当該従業員は，その期間は出張中で，PC を社内 LAN に接続しておらず，パターンファイルは更新されていなかった。

〔監査の実施〕

監査チームは，ウイルス対策の実施状況を確認するために，表 1 のような監査要点及び監査手続を設定し，監査を実施した。

表1　監査要点及び監査手続（抜粋）

項番	監査要点	監査手続
1	ウイルス対策ソフト及びパターンファイルが［ a ］こと	管理ツールを利用し，ウイルス対策ソフト及びパターンファイルのバージョンが最新バージョンと異なっているという条件でサーバ，PCを抽出する。抽出されたサーバ，PCのバージョンが最新でない理由をウイルス対策管理者などにインタビューして確認する。
2	サーバ，PCのハードディスクスキャンが，適切に実施されていること	管理ツールを利用し，“ログに記録された［ b ］がログの確認日よりも前の日付になっている”という条件でサーバ，PCを抽出する。抽出されたサーバ，PCのハードディスクスキャンが適切に実行されていない理由をウイルス対策管理者，利用者などにインタビューして確認する。なお，ログの確認は月曜日の夕方に実施する。
3	ウイルス対策ソフトによってウイルスが検知された場合に，従業員がウイルス対策管理者に通知を行っており，ウイルス対策管理者が通知を適切に記録していること	ウイルス対策管理者が作成している記録簿とログの［ c ］を行う。

〔情報システム部門に助言すべき事項（抜粋）〕

監査チームは，情報システム部門の再発防止策の策定及び現状のウイルス対策の見直しの検討のために，助言内容を次のようにまとめた。

(1) ［ d ］を利用する場合は，最新の［ e ］によってウイルススキャンを実施することをセキュリティポリシに追加すること。また，情報システム部門は，［ e ］が最新かどうかを利用者が確認できる手段を提供すること。

（以下，省略）

設問1　表1中の［ a ］に入れる適切な字句を20字以内で述べよ。

設問2　表1中の［ b ］に入れる適切な字句を20字以内で述べよ。

設問3　表1中の［ c ］に入れる適切な監査技法を解答群の中から選び，記号で答えよ。

解答群

ア　観察　　イ　結合　　ウ　調整　　エ　突合せ

設問4　監査チームが，情報システム部門に助言すべき事項について，本文中の［ d ］，［ e ］に入れる適切な字句をそれぞれ10字以内で答えよ。