問2　インターネット販売を行う企業の情報セキュリティ管理に関する次の記述を読んで，設問1～5に答えよ。

P社は従業員数500名の衣料小売業者であり，店頭販売やカタログ販売を行っている。これに加え，5年前からは社内に業務システム（以下，販売システムという）を構築し，一般消費者に対してクレジットカード決済を利用したインターネット販売を行っている。P社では情報セキュリティを確保するための取組を進めており，インターネット販売事業に関してISO/IEC 27001（JIS Q 27001）の認証（以下，ISMS認証という）を2年前に取得している。

P社は先ごろISMS認証の維持審査に合格したが，この審査において四つの観察事項を指摘された。ISMS認証機関から提示された維持審査結果報告書を図1に示す。

維持審査結果報告書

ISMS認証機関　X株式会社

（省略）

[不適合]
ISO/IEC 27001:2005の要求事項に対する重大な不適合や軽微な不適合は特に認められませんでした。

[観察事項]　()内はISO/IEC 27001:2005の箇条を示す。
1. ISMSの適用範囲を定義する文書において社内組織の変更点が反映されていない部分がありますので，現行の組織体系に合わせた記述に修正することが望まれます。(4.2.1a，4.3.1b)
2. 販売システムの各サーバで利用している管理者パスワードの利用は適切なセキュリティ慣行に従うことが望まれます。(A.11.3.1，A.11.5.3)
3. Webアプリケーションの開発委託におけるセキュリティ要件を明確にすることが望まれます。(A.12.5.5)
4. 法的要求事項に関しては文書化されていますが，これを最新に保つための手法をご検討ください。(A.15.1.1)

（以下，省略）

図1　維持審査結果報告書

〔観察事項への対応〕

維持審査の結果を受け，P社では，情報セキュリティ責任者を兼務している情報システム部のG部長と，その部下で販売システムの管理を担当しているFさんが観察事項への対応に当たることになった。

次は，G部長とFさんの会話である。

Fさん：維持審査での観察事項への対応ですが，どのように進めていきましょうか。

G部長：不適合はなかったが，四つの観察事項への対応策を検討しよう。1.については適用範囲の定義文書を修正することで対応しよう。2.と3.は情報セキュリティポリシ（以下，ポリシという）の修正に加え，技術的な対応も必要になりそうだ。具体的にどの程度まで実施するのかが難しいね。

Fさん：4.については，新たな法律の制定や業界の動向を踏まえて社内のISMS運営事務局で法的要求事項の改訂案を検討し，［　a　］の場で承認を得るというルールを作るとよいと思います。クレジットカード業界に関しては新たな動きがありますね。

G部長：審査が終わってから聞いた話では，2008年6月に公布された改正割賦販売法が施行されると，クレジットカードの発行会社にはクレジットカード番号（以下，カード番号という）を含むカード会員データの保護が義務付けられるそうだ。当社のようなカードの加盟店を直接規制する法律ではないが，当社にもカード発行会社から何らかの対策が求められるかもしれない。

Fさん：カード番号の不正な取得や有償での提供を行った個人も処罰されるということでしたね。カード番号を悪用されると影響が大きいですからね。
そういえば，クレジットカード業界では加盟店に対して技術的な対応を含めた自主基準を定めていたようです。観察事項の2.と3.への対応のヒントになるかもしれませんので，調べてみます。

数日後，Fさんは G部長に調査の結果を報告した。

Fさん：先日の話ですが，国際クレジットカードブランド5社が共同で設立したPCI SSC（Payment Card Industry Security Standards Council, LLC）という国際協議会が，PCIデータセキュリティ基準（Payment Card Industry Data Security Standard，以下，PCI DSSという）という業界基準を設けています。この基準を参考にして対応を考えてはどうでしょうか。

Fさんは図2に示すPCI DSS（バージョン1.2）の要件をG部長に提示した。

安全なネットワークの構築と維持
　要件1　：カード会員データ(1)を保護するために，ファイアウォールをインストールして構成を維持すること
　要件2　：システムパスワードおよび他のセキュリティパラメータにベンダ提供のデフォルト値を使用しないこと
カード会員データの保護
　要件3　：保存されたカード会員データを保護すること
　要件4　：オープンな公共ネットワーク経由でカード会員データを伝送する場合，暗号化すること
脆弱性管理プログラムの整備
　要件5　：アンチウィルスソフトウェア(2)またはプログラムを使用し，定期的に更新すること
　要件6　：安全性の高いシステムとアプリケーションを開発し，保守すること
強固なアクセス制御手法の導入
　要件7　：カード会員データへのアクセスを，業務上必要な範囲内に制限すること
　要件8　：コンピュータにアクセスできる各ユーザ(3)に一意のIDを割り当てる。
　要件9　：カード会員データへの物理アクセスを制限する。
ネットワークの定期的な監視およびテスト
　要件10：ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する。
　要件11：セキュリティシステムおよびプロセスを定期的にテストする。
情報セキュリティポリシー(4)の整備
　要件12：従業員および派遣社員向けの情報セキュリティポリシーを整備する。

出典：PCI Security Standards Council LLC, “Payment Card Industry（PCI）データセキュリティ基準 要件とセキュリティ評価手順 バージョン1.2”, 1ページ
（URL：https://www.pcisecuritystandards.org/pdfs/pci_dss_japanese.pdf（平成21年3月1日アクセス））

注(1)　カード会員データとは，カード番号，カード会員名，有効期限などを指す。
(2)　“アンチウィルスソフトウェア”は，問題文中の“ウイルス対策ソフト”と同じである。
(3)　“ユーザ”は，問題文中の“利用者”と同じである。
(4)　“情報セキュリティポリシー”は，問題文中の“ポリシ”と同じである。

図2　PCI DSS（バージョン1.2）の要件

G部長：全部で12個の要件があるのか。観察事項に対応する要件は要件6，8辺りかな。これらの要件が更に細かく分かれているわけだね。

Fさん：そうです。例えば，観察事項として指摘されたパスワード管理に関しては，要件8の中に，図3に示すような詳細要件が定められています。

要件 8：コンピュータにアクセスできる各ユーザ(1)に一意の ID を割り当てる。
（省略）
8.5 すべてのシステムコンポーネントで，以下のように，消費者以外のユーザおよび管理者に対して適切なユーザ認証とパスワード管理を確実に行う。
8.5.1 ユーザ ID，資格情報，およびその他の識別子オブジェクトの追加，削除，変更を管理する。
8.5.2 パスワードのリセットを実行する前にユーザ ID を確認する。
8.5.3 初期パスワードをユーザごとに一意の値に設定し，初回使用後に直ちに変更する。
（省略）
8.5.9 少なくとも 90 日ごとにユーザパスワードを変更する。
8.5.10 パスワードに 7 文字以上が含まれることを要求する。
8.5.11 数字と英文字の両方を含むパスワードを使用する。
8.5.12 ユーザが新しいパスワードを送信する際，最後に使用した 4 つのパスワードと同じものを使用できないようにする。
（省略）

出典：PCI Security Standards Council LLC，“Payment Card Industry（PCI）データセキュリティ基準 要件とセキュリティ評価手順 バージョン 1.2”，37～40 ページ
（URL：https://www.pcisecuritystandards.org/pdfs/pci_dss_japanese.pdf（平成 21 年 3 月 1 日アクセス））
注(1) “ユーザ”は，問題文中の“利用者”と同じである。

図 3 パスワード管理に関する PCI DSS の詳細要件

G 部長：クレジットカード加盟店では，今後このレベルの管理が求められるということか。当社の現状からみるとかなり厳しい要件もあるが，クレジットカード決済を利用していくのであれば実施する方がいいのだろうね。
Web アプリケーションの開発時におけるセキュリティ要件については何か参考になりそうなものはあったかな。

F さん：Web アプリケーションの開発では，クロスサイトスクリプティングや SQL インジェクションなど，広く知られた脆弱性について対処する必要があります。そのため，詳細要件 6.5 では，安全なコーディングのためのガイドラインに従うことを推奨しています。PCI DSS では，その代表的なものとして，米国の団体が策定したガイドラインを挙げています。今後はこのガイドラインに沿って具体的なセキュリティ要件を発注の際の仕様に含めるとよいのではないでしょうか。

G 部長：そうだね。詳細については検討する必要があるが，今後 Web アプリケーションの改修を行うときや新規の開発を行うときには，①委託先に具体的なセキュリティ要件を提示することにしよう。

これらの検討を踏まえ，G 部長と F さんは観察事項への対応計画を作成した。この

対応計画は経営陣の承認を経て実行に移されることになった。

〔PCI DSS を参考にした ISMS の継続的改善〕

その後，G 部長が対応計画の完了を経営陣に報告したところ，PCI DSS で求められる要件をベースラインとして ISMS における技術面及び管理面の改善を図るようにとの指示が出た。そこで，G 部長と F さんは PCI DSS の要件に沿って販売システムの管理状況を確認することにした。次は，G 部長と F さんの会話である。

F さん：PCI DSS の各要件への対応状況ですが，私の考えで 12 個の要件ごとに現在の状況を表 1 のようにまとめてみました。

表 1　F さんによる PCI DSS の対応状況のまとめ

要件	対応状況 (1)	今後必要な対策
要件 1	○	ファイアウォール，ルータのルールセットのレビュー
要件 2	△	システム上での不要なサービスや機能の無効化，停止
要件 3	○	システム外でのカード情報の暗号化と難読化
要件 4	◎	対応済（SSL の導入）
要件 5	◎	対応済（ウイルス対策ソフトの導入）
要件 6	△	パッチ適用体制の見直し，既知の攻撃からの Web アプリケーションの防護
要件 7	◎	対応済（ポリシ，システムによるアクセス制限の実施）
要件 8	◎	対応済（パスワードポリシの修正，システムでの対応）
要件 9	△	カメラなどによるサーバ室の監視，安全なバックアップ媒体の保管
要件 10	×	監査証跡の自動取得と保護，ログの確認
要件 11	△	システムへの脆弱性スキャン，ペネトレーションテスト
要件 12	○	PCI DSS への対応に伴うポリシの見直し，インシデント対応計画の立案とテスト及び見直し

注(1)　対応状況は次の例による。
◎：各要件に含まれる詳細要件をすべて満たしている
○：詳細要件の一部について実施状況の見直しや確認が必要
△：詳細要件の一部について未実施
×：詳細要件の多くが未実施

G 部長：今の時点で対応できている要件はどれかな。

F さん：要件 4，5，7，8 は対応できていると思います。要件 4 はインターネットや無線 LAN などの公衆ネットワーク上でのカード会員データの暗号化を求めてい

ますが，販売システムでは無線 LAN は使用していませんし，インターネット経由でカード会員データを送受信する部分はすべて SSL で暗号化されています。要件 5 はシステムへのウイルス対策ソフトの導入ですが，ウイルス対策ソフトは販売システムに含まれるすべての PC とサーバに導入済です。

G 部長：②ウイルス定義ファイルの自動更新と定期スキャンも実施しているし，問題なさそうだ。

F さん：要件 7 はカード会員データへのアクセスを業務上必要な範囲内に制限するということですが，販売システムにはポリシ上も機能上も職責に応じて権限を与えられた担当者だけがアクセスできるようになっているので問題はありません。要件 8 は利用者ごとに個別の利用者 ID を割り当てるという要件で，パスワードポリシについては ISMS の観察事項に基づいて対応しました。それ以外の部分は以前から実施済です。

G 部長：この四つの要件に関しては対策が実施されているということだね。次に，要件 1，3，12 については見直しや確認が必要なところだね。

F さん：はい。要件 1 ではファイアウォールの設置を求めていますが，詳細要件 1.1.6 の，少なくとも 6 か月ごとに，ファイアウォール及びルータに関するルールセットのレビューを実施するという要件が現状では満たされていません。それ以外の詳細要件はすべて対応できています。

G 部長：ファイアウォールもルータも，設定についてのレビューは実施していなかったな。今の運用手順を改訂してレビューを行う必要があるね。

F さん：要件 3 はカード会員データの保護についてです。カード番号は販売システムのデータベースサーバ（以下，DB サーバという）の中では暗号化されていますが，詳細要件 3.4 によるとバックアップやログの中にカード番号が含まれている場合にはカード番号の一部を削除するか，あるいは暗号化やハッシュによって読めないようにする必要があります。

G 部長：販売システム以外にもカード番号が存在するかどうかだね。具体的にカード番号がどの情報資産に含まれているか，それがどこに保管されているかについては，先日の維持審査の前に実施したリスク分析で明確にされているから対応はそれほど難しくはないだろう。

Fさん：要件12はポリシの整備が中心になっていますが，ここで対応すべき詳細要件としてはインシデント対応計画があります。PCI DSS では少なくとも年に一度のテストと見直しを求めていますが，インシデント対応計画についてはこれまでにテストも見直しも行ったことがありません。

G部長：この辺までは今までの対策の延長で対応できそうだが，更に修正が必要になるのが要件2，6，9，10，11だね。

Fさん：要件2は，システムのデフォルト設定を使ってはいけないという要件です。

G部長：サーバについては受入れ検査のときに③ポートスキャンツールを使って不要なサービスの有無を確認しているが，その後システムを変更しているからもう一度確認が必要だ。

Fさん：要件6は後回しにして，要件9は物理的アクセスの制限や媒体の取扱いについてです。詳細要件9.1.1では機密エリアはビデオカメラやその他のアクセス管理機器で監視し，少なくとも3か月間は監視データを保管することが求められていますが，現状では保管していません。

G部長：サーバ室とコールセンタはカメラで監視しているが，監視映像は保管していないから，追加投資が必要になりそうだ。

Fさん：ほかにはバックアップ媒体の保管の話があります。今は媒体を④サーバ室に保管していますが，外部の施設への保管も検討する必要があります。

G部長：これについては，先ほどのインシデント対応計画と同様に，ISO/IEC 27001の［　b　］計画でも対応すべきだろうね。

Fさん：要件11に移りましょうか。詳細要件11.2では，少なくとも四半期に一度，そのほかにネットワークに大きな変更があったときにシステムへの脆弱性スキャンを行うことが求められています。また，詳細要件11.3では，少なくとも年に一度と，そのほかにインフラやアプリケーションを大幅に変更した後にペネトレーションテスト（以下，Pテストという）を実施することが求められています。

G部長：Pテストは外部にお願いする必要があるのかな。Fさんに Pテストのスキルを身につけてもらった上で実施するのはどうだろう。

Fさん：社内で実施することは要件上認められていますが，私に Pテストのスキルがあったとしても，⑤私がPテストを実施するのは望ましくないですね。

G部長：そうだね。内部で実施するか外部で実施するかは別途考えよう。

Fさん：残っているのは要件6，10ですね。まず，要件10はアクセスの追跡と監視についてです。具体的には，各システム上でログを取得するだけではなく，改ざんされないように保護した上で少なくとも日に一度は確認することが求められます。

G部長：Web コンテンツへのアクセス状況は解析しているけれども，セキュリティ上のイベントについては特に何もしていない。日に一度の確認となるとかなり大変だから，今後は何らかの対応が必要だ。

Fさん：ほかにはシステムクロックを正確な時刻に保つことが求められていますが，社内のすべての機器は販売システム上の時刻サーバを介してインターネット上の標準時サーバと時刻を同期させています。これには通信の遅延を補正できる［　c　］というプロトコルを使っています。

〔Webアプリケーションの保護の手法〕

Fさん：技術的に最も対応が難しそうな要件6の対応状況は表2のとおりです。詳細要件6.2から6.5までは対応済ですが，残りの二つに関しては対応が必要になりそうです。特に詳細要件6.6ではWebアプリケーションの見直し又はWebアプリケーションファイアウォール（以下，WAFという）の導入が求められています。

表2　要件6の対応状況

詳細要件	対応状況(1)	今後必要な対策
6.1	○	最新セキュリティパッチのリリース後1か月以内の適用
6.2	◎	対応済（ベンダ，各種団体からの脆弱性情報入手）
6.3	◎	対応済（開発，テスト，本番環境の分離など）
6.4	◎	対応済（変更管理手順に基づくシステム変更の実施）
6.5	◎	対応済（コーディングガイドラインの導入）
6.6	×	Webアプリケーションの見直し又はWAFの導入

注(1)　詳細要件の対応状況は表1の注を参照。

G部長：詳細要件6.1はセキュリティパッチ（以下，パッチという）のリリース後1か月以内の適用ということだね。システムを停止できない場合も多いが，パ

ッチの運用体制を見直して対応するしかないね。

F さん：パッチの適用についてはリスクに応じて優先度をつけることも認められていますので，重大なものを優先させ，軽微なものは 3 か月以内に適用することができます。

G 部長：詳細要件 6.6 の Web アプリケーションの見直しというのはどんな方法で行うのかな。

F さん：Web アプリケーションの脆弱性を手動又は自動で評価するツール又は手法によって，Web アプリケーションをレビューすることが求められています。脆弱性はすべて修正し，修正後に再評価する必要があります。

G 部長：実施の頻度はどれくらいなのかな。

F さん：少なくとも年に一度実施することが求められています。そのほかに何らかの変更があった場合にも実施する必要があります。

G 部長：Web アプリケーションの見直し以外には WAF の導入も選択肢としてあるということだが，今導入している侵入防止システム（以下，IPS という）では対応できないのかな。

F さん：今使っている IPS はシグネチャベースの製品で，ネットワーク層に対する既知の攻撃を防御することに主眼を置いています。Web アプリケーションの脆弱性に対する攻撃にはそれほど効果はありません。

G 部長：WAF では Web アプリケーションへの攻撃をどうやって防ぐのだろう。

F さん：これには二つの考え方があるようです。一つはポジティブセキュリティモデルといって，正常な通信として定義されたもの以外の通信をすべて遮断するものです。どういった通信が正常なのかを定義するために個々の Web アプリケーションに対して細かい設定が必要になり，導入にも手間が掛かります。もう一つはネガティブセキュリティモデルといって，シグネチャや特定のパターンに合致した通信をアプリケーション層で遮断するものです。Web アプリケーションの脆弱性の性質から，⑥個々の攻撃に対してシグネチャを作成することが難しいというデメリットがありますが，特定の情報の漏えいを防ぐ観点からは，こちらのモデルの方が有効な場合があります。このため，PCI DSS では，この二つのセキュリティモデルを WAF に実装することが推奨されています。

G 部長：状況によっては両方のモデルを実装した WAF が必要ということか。

F さん：WAF には攻撃を検知する機能があるので，当社の対策に欠けている PCI DSS の要件を満たせるというメリットもあります。

G 部長：なるほど。ただ，⑦Web アプリケーションの見直しをせずに WAF を導入することには問題があるのではないかな。コスト面での制約はあるが，できるだけ併用する方向で検討しよう。

〔トランザクションログに対する代替管理策〕

その後，P 社では PCI DSS を参考に販売システムの改善を図っていったが，システムの制約上，対応が困難な詳細要件が存在することが分かった。次は，G 部長と F さんの会話である。

G 部長：ベンダに問い合わせてみたところ，DBMS が作成するトランザクションログについては暗号化を施してカード番号を判読困難にすることは難しいようだ。既存のログからカード番号を除去するのも現実的ではない。そうなると，詳細要件 3.4 を満たすことができない。できるだけ追加投資を必要とせずに対応する方法はないだろうか。

F さん：要件を満たせない場合でも，関連するリスクをほかの手段を適用することで［ d ］できる場合には，その手段を代替管理策とすることで，要件の目的を実現することが可能です。PCI DSS では，表 3 に示すようなワークシートを使って，要件が満たされないことに対するリスクを管理するそうです。まだ検討の途中ですが，このような形になるかと思います。

表3　詳細要件 3.4 に対する代替管理策のワークシート

必要な情報		P 社での状況
1. 制約	元の要件への準拠を不可能にする制約を列挙する。	DBMS が出力するトランザクションログの中にカード番号が含まれているが，ソフトウェアの制約によってトランザクションログを暗号化することができない。
2. 目的	元のコントロール(1)の目的を定義し，代替コントロールによって満たされる目的を特定する。	トランザクションログに含まれるカード番号を判読困難にすることによって，カード番号の露呈を防ぐ。
3. 特定されるリスク	元のコントロールの不足によって生じる追加リスクを特定する。	DB サーバにアクセス可能な従業員に対してトランザクションログに含まれるカード番号が露呈するリスクがある。
4. 代替コントロールの定義	代替コントロールを定義し，元のコントロールの目的および追加リスク（ある場合）にどのように対応するかを説明する。	[e]。 これによって，トランザクションログに含まれるカード番号の露呈を防ぐ。
5. 代替コントロールの検証	代替コントロールの検証およびテスト方法を定義する。	（未検討）
6. 維持	代替コントロールを維持するためのプロセスおよび管理を定義する。	（未検討）

太枠部分の出典：PCI Security Standards Council LLC, “Payment Card Industry（PCI）データセキュリティ基準 要件とセキュリティ評価手順 バージョン 1.2”, 62 ページ
（URL：https://www.pcisecuritystandards.org/pdfs/pci_dss_japanese.pdf（平成 21 年 3 月 1 日アクセス））

注(1)　“コントロール”は，問題文中の“管理策”と同じである。

G 部長：なるほど，表 3 の代替管理策を実施すれば詳細要件 3.4 の目的は実現できそうだ。残りの 5. と 6. についても検討してみてくれないかな。

F さん：分かりました。残りの部分についてもこれから検討します。

その後，P 社は PCI DSS を参考にして ISMS の取組を進め，技術面でのセキュリティ向上とポリシ面での継続的改善を図ることができた。

設問 1　〔観察事項への対応〕について，(1)，(2) に答えよ。

(1) 本文中の [a] に入れる適切な字句を，15 字以内で答えよ。

(2) 本文中の下線①について，Web アプリケーションの開発委託先に対してセキュリティ要件を提示していなかった場合，受入れ検査時に脆弱性の存在が判明したときにどのような問題が発生するか。60 字以内で述べよ。

設問2　〔PCI DSSを参考にしたISMSの継続的改善〕について，(1)～(5)に答えよ。

(1) 本文中の［ b ］，［ c ］に入れる適切な字句を，それぞれ5字以内で答えよ。ただし，［ b ］は漢字とし，［ c ］は英字の略称とする。

(2) 本文中の下線②について，自動更新と定期スキャンが確実に実施されていることをどのように確認するべきか。30字以内で述べよ。

(3) 本文中の下線③について，検査対象と同一のネットワークセグメントからポートスキャンツールを利用して検査を行う場合，不要なサービスがあるかどうかをどのような基準で判断するか。50字以内で述べよ。

(4) 本文中の下線④について，現状のままバックアップ媒体をサーバ室に保管する場合のリスクを，50字以内で述べよ。

(5) 本文中の下線⑤について，F さんが自身で P テストを実施することは望ましくないとした理由を，30字以内で述べよ。

設問3　〔Webアプリケーションの保護の手法〕について，(1)，(2)に答えよ。

(1) 本文中の下線⑥について，シグネチャを作成することが難しい理由を，50字以内で述べよ。

(2) 本文中の下線⑦について，Web アプリケーションの見直しをせずに WAF を導入することによって発生するセキュリティ上の問題点を，60字以内で述べよ。

設問4　〔トランザクションログに対する代替管理策〕について，(1)，(2)に答えよ。

(1) 本文中の［ d ］に入れる適切な語句を解答群の中から選び，記号で答えよ。

解答群

ア　移転　　イ　回避　　ウ　受容　　エ　低減

(2) 表3中の［ e ］に入れる代替管理策を，40字以内で述べよ。

設問5　PCI DSS を参考として技術面で新たな対策を追加していった P 社が，ISMS の活動として次回の審査に向けて実施すべき作業を，50字以内で述べよ。