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