問 11　情報システムのアクセス管理状況の点検に関する監査について，次の記述を読んで，設問に答えよ。

P 社グループは，持株会社 P 社，小売業 Q 社，金融業 R 社，人材派遣業 S 社（以下，グループ各社という）から構成される企業グループであり，様々な情報システムを利用している。P 社システム統括部は，P 社グループ全体のシステムリスク管理を所管し，グループ各社におけるアクセス管理状況に関する自主点検（以下，点検という）などを主導している。一方，P 社グループでは，アクセス管理策の不備に起因する情報漏えい事案などが発生していた。

P 社内部監査部は，このような状況を踏まえて，グループ各社を対象として，点検の実効性が確保されているかどうか，監査を実施することにした。システム監査チームは，予備調査を実施して，P 社グループの情報システムの運用状況及び点検の概要を次のとおり把握し，本調査での監査要点案を作成した。

〔情報システムの運用状況〕

(1) P 社システム統括部は，グループ各社のシステム部からの報告内容に基づき，IT 機器管理表及びアプリケーションソフトウェア管理表（以下，各管理表という）を更新している。

(2) IT 機器管理表には，グループ各社が管理するサーバ，PC などの識別番号，OS，業務委託の有無などが記載されている。また，アプリケーションソフトウェア管理表には，グループ各社が利用するアプリケーションソフトウェア名，取り扱う情報の内容，業務委託の有無などが記載されている。

(3) P 社のアクセス管理規程に定められた管理策は，原則としてグループ各社に適用される。当該規程では，例えば，グループ各社に配置された PC は，利用者ごとの ID 及びパスワードでログインすることが定められている。

(4) グループ各社においてアクセス管理規程に定められた管理策を適用できない場合には，グループ各社のシステム部が代替の管理策を申請し，P 社システム統括部長の承認を受ける。

(5) P 社は，グループ各社が共同利用するグループウェア，経理システム，人材管理システムなどのほか，グループ各社の営業情報などを収集，モニタリングする

経営情報システムを保有しており，T 社に運用，保守を業務委託している。

(6) Q 社は，R 社発行のクレジットカードを利用した顧客の購買履歴などを分析する顧客管理システムを保有しており，U 社に運用，保守を業務委託している。

(7) Q 社の店舗には，複数の従業員が共用する PC が配置されており，顧客対応上の必要性を考慮して，共用の ID 及びパスワードでログインする。店舗のシステム管理者は当該パスワードを 10 営業日ごとに変更し，店舗の従業員に連絡する。P 社システム統括部長は，当該管理策を承認している。

(8) S 社は，派遣スタッフの氏名，派遣先，時間単価などを派遣システムで管理している。予備調査の 1 か月前には，派遣システムのアクセス管理策の運用状況に関する不備に起因して，派遣スタッフの個人情報が漏えいする事案（以下，情報漏えい事案という）が発生していた。

〔点検の概要〕

(1) 点検プロセスの概要は，次のとおりである。

① P 社システム統括部は，アクセス管理規程，各管理表などに基づき，点検のポイント，対象などを設定し，グループ各社の点検表を作成して，グループ各社のシステム部に半年ごとに点検を指示する。

② グループ各社のシステム部は，点検表に基づき点検を実施し，当該点検の結果，不備についての是正状況などを P 社システム統括部に報告する。

③ P 社システム統括部は，点検に関する報告内容を確認し，必要に応じて，不備について是正を進めるよう指導，支援する。

④ P 社システム統括部は，グループ各社のシステム部からの点検に関する報告内容などを踏まえて，点検のポイント，対象などを見直す。

(2) P 社システム統括部の担当者は，各管理表に点検の対象かどうかを記載し，1 か月ごとに更新している。システム統括部長は，担当者から更新の内容及び理由について説明を受け，各管理表に承認したことを記録する。

(3) グループ各社のシステム部は，顧客情報，営業情報などを取り扱う情報システムの運用，保守を業務委託する場合，点検の一環として，委託先のアクセス管理状況を確認し，P 社システム統括部に報告することになっている。Q 社のシステム部からは当該点検の都度，U 社におけるアクセス管理策の不備が報告されていた。

(4) 予備調査までに S 社以外のグループ各社で実施された点検では，何らかの不備が発見されていた。一方，S 社で情報漏えい事案の発生時までに実施された点検では，派遣システムのアクセス管理策の運用状況を点検していたものの，不備は全く発見されていなかった。

(5) P 社システム統括部が作成した点検表の例（抜粋）を表 1 に示す。

表 1 点検表の例（抜粋）

会社名	（省略）		
点検の項番	点検のポイント	点検の対象	点検の結果
1	PC にログインする際に，利用者ごとの ID 及びパスワードを用いているか。	（省略）	（省略）
2	委託先におけるアクセス管理状況の不備について，是正状況を確認しているか。	（省略）	（省略）

〔監査要点案の作成〕

システム監査チームが予備調査の結果を踏まえて作成した本調査での監査要点案（抜粋）を表 2 に示す。

表 2 監査要点案（抜粋）

項番	監査要点
1	点検のポイントは，適切に設定されているか。
2	点検の結果は，実態と整合しているか。
3	点検で発見された不備は，適切に是正されているか。
4	点検の対象は，適切に見直されているか。

〔内部監査部長の指示〕

内部監査部長は，本調査での監査要点案をレビューして，次のとおり指示した。

(1) 表 2 項番 1 の監査要点に関して，グループ各社においてアクセス管理規程に定められた管理策が適用できない場合の［ a ］も考慮して，点検のポイントを適切に設定しているか，確認すること。

(2) 表 2 項番 2 の監査要点に関して，効率よく監査を実施するために監査対象をサ

ンプリングする場合には，［ b ］が形骸化しているおそれが大きいと想定されるS社を含めること。

(3) 表2項番3の監査要点に関して，グループ各社及び［ c ］における不備についての是正状況を確認するだけではなく，［ d ］がQ社のシステム部に対して，［ e ］しているか，確認すること。

(4) 表2項番4の監査要点に関して，点検の対象が記載されている各管理表の更新について，P社システム統括部長の［ f ］を確認するだけではなく，P社システム統括部長が［ g ］を把握しているか，インタビューによって確認すること。

(5) 表2項番1～4の監査要点に加えて，点検の対象を見直した結果に基づき，グループ各社に点検が指示されているか，［ h ］と［ i ］とを照合して，確認すること。

設問1 〔内部監査部長の指示〕(1)の［ a ］に入れる適切な字句を，10字以内で答えよ。

設問2 〔内部監査部長の指示〕(2)の［ b ］に入れる適切な字句を解答群の中から選び，記号で答えよ。

解答群

ア 監査	イ 承認	ウ 情報漏えい事案
エ 点検	オ 派遣システム	カ 予備調査

設問3 〔内部監査部長の指示〕(3)について答えよ。

(1) 本文中の［ c ］に入れる適切な字句を，5字以内で答えよ。

(2) 本文中の［ d ］に入れる適切な字句を，10字以内で答えよ。

(3) 本文中の［ e ］に入れる適切な字句を，15字以内で答えよ。

設問4 〔内部監査部長の指示〕(4)について答えよ。

(1) 本文中の［ f ］に入れる適切な字句を，5字以内で答えよ。

(2) 本文中の［ g ］に入れる適切な字句を，10字以内で答えよ。

設問5 〔内部監査部長の指示〕(5)の［ h ］，［ i ］に入れる適切な字句を，それぞれ5字以内で答えよ。