問4　情報システムの特権管理に関する次の記述を読んで，設問1，2に答えよ。

E 社は，従業員数 2,000 名の上場している運輸会社である。E 社の情報システム部では 80 台のサーバを管理しており，複数種の OS と，複数の DBMS 及びアプリケーション（以下，AP という）が稼働している。

インストールされたそれぞれの OS，DBMS，AP に対して，システム管理特権が付与された利用者 ID（以下，特権 ID という）が一つずつ登録されており，情報システム部内のシステム管理チームに所属するシステム管理者 10 名がすべての特権 ID とパスワードを共用している。例えば，OS，DBMS，AP がそれぞれ一つずつ稼働しているサーバでは，OS に一つ，DBMS に一つ，AP に一つの特権 ID が登録されており，システム管理者 10 名がこれらの特権 ID を共用している。特権 ID の使用は，基本的にはネットワーク経由で行われているが，コンソールからでないと行えない特定の作業については，サーバが保管されているラック内に設置されたコンソールから行われている。

E 社は，システム運用の安全性を確認するために，セキュリティ専門会社の F 社に，サーバの設定や運用に関するセキュリティ診断を依頼した。診断の結果，情報システムの特権 ID 管理が十分でないとの指摘を受けたことから，経営陣は情報システム部に対して特権 ID の管理を改善するように指示した。

〔特権 ID 管理の要件〕

F 社による指摘は，“特権 ID の使用において，内部者の不正使用を防止及び発見する仕組みが構築されていない”というものであった。システム管理チームの N 課長と M 君は，この指摘に基づき，必要な管理要件を明確にすることにした。

N 課長：M 君，現状の特権 ID 管理において必要な管理要件とは具体的に何だろう。

M 君　：現在の当社のシステムでは，特権 ID を使用したときのログがほとんど取得されていないので，不正使用があったとしても発見できないおそれがあります。ログインやログアウトなどの基本的なイベントと，システムの設定変更や利用者 ID 登録などの重要な操作については，ログを取得する必要があると思います。当社の全システムが，特権 ID に関するこれらのログを取得する機

能をもっていることは確認できています。

N課長：なるほど。それらのログを取得することにしよう。

M君　：ただし，今の状態では，ログを取得したとしても［　a　］をやめないと，ログからはだれが不正使用を行ったのかを特定できないので意味がありません。

N課長：なるほど。それは①上場企業に求められる内部統制の観点からも改善が必要だな。近々内部統制を評価するための内部監査が行われることになっているが，今回の診断はその準備にもなっている。早速すべての OS，DBMS，AP で改善してくれ。

M君　：分かりました。すぐに改善することにします。

N課長：F 社からは，内部不正を発見する仕組みも必要と言われているが，これはどう考えるかね。

M君　：はい。特権 ID の使用が業務目的であることを確認するために，使用目的，使用者，使用する特権 ID を記入した特権 ID 利用申請書を使用日ごとに課長に提出し，事前に承認していただくという運用にします。その上で，月に 1 回程度［　b　］を実施して不正な使用がなかったことを確認します。この［　b　］が，内部不正を発見する仕組みに当たります。

N課長：よし，ではそれで試験的に運用してみよう。

新たな特権 ID 管理の仕組みが試験的に運用され，1か月が経過した。

〔特権 ID 管理の運用〕

N課長：先月の［　b　］の結果はどうだったかね。

M君　：ある DBMS に利用申請のない特権 ID の使用がありました。OS，DBMS，AP の特権 ID を必要に応じて追加作成し，一つの特権 ID は 1 人のシステム管理者だけが使用する環境を実現できましたので，だれが使ったのかすぐ分かりました。その特権 ID を使った者に確認したところ，状況監視のために毎日使用していました。しかし，一般権限でも問題ないということでしたので，②データの参照だけを行うことができる，状況監視用の利用者 ID を作成し，それを使用させることにしました。また，あるサーバの OS では，特権 ID の

利用申請があったのに，ログが残っていないものがありました。チーム全員に確認してみたところ，ある従業員が誤ってシステムのリストアの際にログファイルを上書きしてしまったということでした。

N課長：ログがちゃんと保存されないのは問題だな。

M君　：そう思います。追記型記憶装置を使えばログが消えてしまうことを防止できるのですが，すべてのサーバに導入するとコストが掛かりすぎます。実はUNIX でログを収集，転送する方式として一般的に使われている［　c　］を使ったログサーバについて調査していました。これを導入して，ログサーバで追記型記憶装置を使用し，OS，DBMS，AP のログを保存するというのはどうでしょう。

N課長：なるほど。しかし，今年度の予算では，ログサーバを購入できたとしても，追記型記憶装置までは購入できないな。そこまでしなくても，もっと簡単な方法でログサーバのログは保護できるのではないだろうか。例えば，［　d　］することにすれば，ログサーバの中にログが保存された状態であっても，ほかのサーバ管理者による故意のログ削除を防止できるし，誤操作によるログ喪失の可能性も低下させることができるだろう。

M君　：そうですね。そうすれば大丈夫だと思います。

N課長：では，ログサーバだけを導入することにしよう。ログは，当社の情報セキュリティ規程に従って，2 年間保存するようにしておいてくれ。しかし，問題の発見に最悪で 1 か月も掛かるというのは遅すぎるな。ほかに方法はないのかね。

M君　：例えば，不正の可能性が考えられる特権 ID の使用が発見されたときにだけアラートを発生させ，それを電子メール（以下，メールという）で通知する仕組みをログサーバに導入すれば，もっと早期に発見することができると思います。例えば，サーバへのログイン回数が多かった場合にアラートを発生させればよいかもしれません。

N課長：しかし，サーバへのログイン回数が多かったからといって不正使用というわけではないだろう。

M君　：はい，そのとおりです。アラートが発生したからといって特権 ID の不正使用があったとは断言できないので，特権 ID 利用申請書などを基に確認を行う

必要がある，という意味です。

N課長：なるほど。では，どのようなアラートの発生条件を設定するか，案を作ってくれ。

M君　：分かりました。

数日後，M 君から特権 ID の使用に関するアラートの発生条件案（表）が提出された。

表　特権 ID の使用に関するアラートの発生条件案

項番	アラートの発生条件
1	一つのサーバにおいて，過去 1 か月間ログインしたことがない特権 ID によるログインが行われたとき（普段使わない特権 ID の使用）
2	全サーバ累計で，1 人が 1 日で 10 回以上のログインを行ったとき（頻繁な使用）
3	ログアウト（又はタイムアウト）時に，ログインからの時間が 2 時間を超えているとき（長時間のログイン）
4	特権 ID の追加が行われたとき
5	システム設定が変更されたとき
6	DBMS に対して SQL 文を実行したとき (1)

注(1)　アプリケーションから DBMS へのアクセスでは，DBMS の特権 ID は使用していない。

N課長：これらの条件だけでは，本人に割り当てられている特権 ID を使用したときにしか検出できないな。③特権 ID をもっていない人が特権 ID を使用しようとする行為があったときにも検出できるようにしてくれないか。それから，アラートを通知するメールは管理職の私が受け取って確認しよう。ところで，④アラートを設定していることはシステム管理者に周知してほしいが，⑤具体的なアラートの発生条件は伝えないようにしておいてもらえるかね。

M君　：分かりました。アラートを通知するメールへの対応はよろしくお願いします。

M君の案に基づき，アラートを発生させる仕組みが導入され，1 週間が経過した。

N課長：M 君，アラートを通知するメールが多くて確認が大変だよ。特に，表の項番

6の条件のときに発生させるアラートの通知メールが必ず毎日届くんだ。

M君　：すみません。どうも最近，DBMSに対して特権IDを使用してSQL文を実行する運用作業が増えたことが原因のようです。アラートの数を減らす方法として，SQL文の中身を解釈し，その内容に応じてアラートを発生させることができるツールを使うことも考えているのですが，まだ調査中で導入にはしばらく時間が掛かりそうです。

N課長：これではほかの仕事ができないな。この条件はそのツールを導入するまでいったん外してくれないか。

M君　：分かりました。当面，特権IDを使用したSQL文の実行に関するログの取得はやめましょう。

N課長：M君，それは駄目だよ。⑥データベース（以下，DBという）では当社の財務にかかわる重要なデータが管理されているから，財務報告の信頼性を担保するためにも，特権IDを使用してDBを操作したログを取得して保存することは重要なんだ。

M君　：なるほど，分かりました。アラートの発生条件からは外しますが，ログは取得するようにしておきます。

N課長：よし，ではこの状態でしばらく運用することにしよう。

その後，SQL文の中身を解釈してアラートを発生させるツールが導入され，再度の試験運用が行われた。その1か月後，アラート発生の設定が適切であることが確認され，本格運用が開始された。これによって，E社システムの特権ID管理が改善され，より安全なシステム運用が実現された。

設問1　〔特権ID管理の要件〕について，(1)～(3)に答えよ。

(1) 本文中の下線①で，上場企業を対象に，内部統制の評価及び報告を求める法律（又はその通称）を解答群の中から選び，記号で答えよ。

解答群

ア　割賦販売法　　イ　金融商品取引法

ウ　個人情報保護法　　エ　不正アクセス禁止法

(2) 本文中の［ a ］に入れる適切な字句を，10字以内で答えよ。

(3) 本文中の［ b ］に入れる適切な字句を，10字以内で答えよ。

設問2 〔特権ID管理の運用〕について，(1)～(6)に答えよ。

(1) 本文中の下線②を実施するに当たって適用した考え方を，解答群の中から選び，記号で答えよ。

解答群

ア 最小権限の原則　　イ 職務の分掌

ウ 多層防御　　エ 要さい化

(2) 本文中の［ c ］に入れる方式を，英文字10字以内で答えよ。

(3) 本文中の［ d ］に入れる，N課長がログサーバに対して実施しようとしている対策を，40字以内で述べよ。

(4) 本文中の下線③を検出するために，表に項番7を追加したい。このとき，アラートの発生条件として何を設定すべきか。20字以内で述べよ。

(5) 本文中の下線④及び下線⑤の指示のセキュリティ上の目的を，それぞれ35字以内で述べよ。

(6) 本文中の下線⑥において，財務報告の信頼性を担保するために，特権IDに関するDBのログの個々の記録について何を確認し，全体として何を立証しようとしているか。特権IDに関するDBのログの個々の記録に対して確認する内容を50字以内で，立証しようとしていることを35字以内で述べよ。