問2　ログ管理システムの設計に関する次の記述を読んで，設問1～4に答えよ。

A社は，従業員数20,000名の製造会社であり，東日本と西日本にそれぞれ10の支社をもっている。A社は，内部統制強化の一環として，システムの運用に関わる内部統制について外部監査人による監査を受けた。監査の結果，システムの特権を与えられた管理者やオペレータなど（以下，特権ID利用者という）の操作（以下，特権操作という）に対する監視について，次の2点が指摘された。

・特権操作のログを取得していないシステムがある。
・どのシステムにおいても特権操作のログに対する分析が行われていない。

これまで，A社情報システム部では，特権操作に対する監視方法をシステムごとに個別に検討，実装してきたことから，特権操作のログを取得，収集保存及び分析（以下，合わせてログ管理という）する方法がシステムごとに異なっていた。情報システム部は，監査における指摘を踏まえ，特権操作に対して全システム共通のログ管理方法を定め，共通のログ管理システムを構築することとし，システムのログ管理について，次のとおり計画した。

・大量の個人情報又は財務データを処理している，本社営業管理システム，会計管理システム，経理システム及び支社営業管理システム（以下，主要4システムという）のログ管理のため，本年度中に，ログ管理システムを稼働させる。
・主要4システムへの適用後の評価に従って，ログ管理システムの設計及び運用の見直しを行い，ログ管理システムを利用してログ管理を行うシステムを順次増やす。

〔A社のシステム環境〕

A社は，東京と大阪に自社のデータセンタ（以下，DCという）を構えており，東京DCでは本社及び東日本の支社における業務処理を，大阪DCでは西日本の支社における業務処理を行っている。両DC間は広域イーサネットで接続されており，本社及び各支社からは広域イーサネットを介して両DCのシステムを利用できる。

各DC内のマシン室には，汎用機が2台ずつ，UNIXサーバが150台ずつ，PCサーバが150台ずつ配置されている（以下，汎用機，UNIXサーバ及びPCサーバを合わせてサーバという）。両DCには，マシン室に隣接してオペレータ室があり，マシン室と

オペレータ室はLANで接続されている。

各DCでは電源設備の定期保守作業のために，半年に1回，4時間程度，DC内の全サーバを停止する。電源設備の保守作業は，東京DCと大阪DCでは異なる日に行われるように調整されている。

〔特権IDの利用〕

特権ID利用者は，各個人に1台ずつ割り当てられた管理端末からネットワークを介して各サーバにアクセスしてシステム管理又は運用の作業を行っている。管理端末は，本社に200台，東京DCと大阪DCのオペレータ室にそれぞれ10台ずつ配置されており，利用者IDとパスワードによる認証機能によって，本人でなければ操作できない仕組みになっている。管理端末のIPアドレスは，東京DC及び大阪DCそれぞれにある［ a ］サーバによって動的に割り当てられる仕組みになっており，同じ管理端末でも割り当てられるIPアドレスが異なることがある。

主要4システムにおいては，A社の情報セキュリティポリシに従い，マシン室の内部・外部間で個人情報又は財務データを通信する場合の暗号化，並びに個人情報又は財務データを外部記憶媒体に保管する場合の暗号化を行っている。特権ID利用者が管理端末から各サーバにアクセスする際の通信においても，暗号化を行っている。

サーバと管理端末の配置場所，時刻設定の方法及び特権ID利用者の利用者IDの割当て方法を表1に，特権ID利用者の役割名称，担当者，作業場所及び作業内容を表2に，それぞれ示す。

表1　サーバと管理端末の配置場所，時刻設定の方法及び特権 ID 利用者の利用者 ID の割当て方法

	配置場所	時刻設定の方法	利用者 ID の割当て方法
汎用機	東京 DC 内のマシン室及び大阪 DC 内のマシン室	オペレータが，起動時に，電話の時報サービスで提供されている時刻を設定する。	OS，DBMS を含むミドルウェア（以下，DBMS を含めてミドルウェアという）及び業務アプリケーションにおいて，統一された ID 体系が定義されており，情報システム部が各特権 ID 利用者個人に各サーバの利用者 ID を割り当てている。
UNIX サーバ及び PC サーバ		社内の［ b ］サーバがインターネットの［ b ］サーバと時刻同期を行い，社内のサーバは社内の［ b ］サーバと時刻同期を行う。	
管理端末	本社，東京 DC 内のオペレータ室及び大阪 DC 内のオペレータ室	各管理端末は，管理端末を管理するドメイン管理サーバと時刻同期されている。ドメイン管理サーバの時刻は，オペレータが，毎週月曜日の朝に，自分の腕時計を基に設定するが，時刻の正確さは重視されていない。	管理端末の利用者 ID 8 桁のうち，上 2 桁が A 社及び役割ごとの委託先各社に割り当てられており，各社の管理責任者が特権 ID 利用者個人に下 6 桁を割り当てている。

表2　特権 ID 利用者の役割名称，担当者，作業場所及び作業内容

役割名称	担当者	作業場所	作業内容
アプリケーション管理者	A 社情報システム部の従業員及び業務アプリケーション保守の委託先である B 社の従業員（担当する業務アプリケーションごとに A 社情報システム部の従業員 2 名以上を含むグループに分かれている。）	本社	業務アプリケーション及び業務データの管理を行う。
インフラ管理者	A 社情報システム部の従業員及びインフラ管理の委託先である C 社の従業員（担当範囲ごとに A 社情報システム部の従業員 2 名以上を含むグループに分かれている。）		ネットワーク機器を含むハードウェア並びに OS 及びミドルウェアの管理（一部，パッチ適用などの定型のシステム運用を含む）を行う。
オペレータ	運用委託先 D 社の従業員	東京 DC 内のオペレータ室及び大阪 DC 内のオペレータ室	定型のシステム運用を行う。

特権 ID 利用者は合計 220 名である。特権 ID 利用者は，定型のシステム運用以外に特権操作を含む作業を行う場合，事前に自分の氏名と所属，作業で使用する利用者 ID，作業開始日時，作業時間，作業目的及び作業の概要を記載した作業申請書を自社の管理責任者に提出する。各社の管理責任者は，作業内容が業務上必要なものであること

を確認し，承認印を押印する。通常時，各社の管理責任者は，担当者に対する作業指示や作業の管理を行っている。何かの事情で担当者の手が足りなくなった場合，各社の管理責任者が特権操作を行うことがあるので，各社の管理責任者は特権 ID 利用者を兼務しており，利用者 ID が割り当てられている。

特権 ID 利用者のうち，情報システム部の従業員は，アプリケーション管理者又はインフラ管理者のどちらか一方を担当しており，自分が所属するグループの作業内容を詳しく理解している。各システムの構築は SI ベンダに委託している。各システムのオペレータが行う運用手順は，手順の概要を記した引継ぎ資料と口頭説明によって委託先の SI ベンダからオペレータに直接引き継がれてきた。さらに，情報システム部の従業員の中にオペレータの役割をもつ者がいないこともあり，オペレータが行うシステム運用の詳細を知っている者はいない。

〔設計の前提条件〕

情報システム部の X 部長は，ログ管理システムの基本設計を Y 主任に指示した。Y 主任がログ管理に関する十分な経験と知識をもっていなかったことから，X 部長は，専門家の参加が必要と判断し，SI ベンダの E 社にログ管理システムの基本設計への参加を依頼した。E 社の情報セキュリティスペシャリストの T 氏は，最初に Y 主任から，ログ管理システムを開発することになった経緯や A 社のシステム環境についての説明を受けた。後日，Y 主任は，T 氏の助言を受けながら，設計の前提条件を次のように整理し，X 部長の承認を得た。

(1) ログ管理システムを次の三つの機能からなるシステムとする。

ログ取得機能：監視の対象とする特権操作について，記録すべきデータをログファイルとして出力する機能

ログ収集保存機能：複数のログファイルを収集し，フォーマットの変更を行って，一つのログデータベースに統合し，ログファイルと併せて保存する機能

ログ分析機能：与えられた条件に従い，ログデータベースから疑わしい特権操作のログを抽出する機能

(2) 監視の対象とする特権操作を，次の3種類とする。

特権操作1：特権ID利用者による各サーバへのログオン及びログオフ

特権操作2：各システムのデータベース（DB）に保管された個人情報及び財務データに対する参照及び更新

特権操作3：各サーバのOS及びミドルウェアのコマンド，スクリプト及びプログラムの実行，並びに設定情報の参照及び更新

主要4システムにおいて監視の対象とする特権操作を表3に示す。

表3　主要4システムにおいて監視の対象とする特権操作

項番	システム名	サーバ種別	特権操作の分類	特権操作の内容	操作インタフェース
1	本社営業管理システム	汎用機	特権操作1	・特権ID利用者による各サーバへのログオン及びログオフ	コマンドライン
			特権操作2	・個人情報及び財務データに対する参照及び更新（管理端末からのデータ参照要求及び更新要求が，DBでSQL文として処理される。）	テキストインタフェース
			特権操作3	・コマンド，スクリプト及びプログラムの実行	コマンドライン
				・設定ファイルの参照及び更新	テキストエディタ
2	会計管理システム	UNIXサーバ	特権操作1	・特権ID利用者による各サーバへのログオン及びログオフ	コマンドライン
			特権操作2	・個人情報及び財務データに対する参照及び更新（管理端末からのデータ参照要求及び更新要求が，DBでSQL文として処理される。）	表形式のGUI
			特権操作3	・コマンド，スクリプト及びプログラムの実行	コマンドライン
				・設定ファイルの参照及び更新	テキストエディタ
				・バッチ処理のスケジュールの参照及び更新	GUI
3	経理システム	UNIXサーバ	特権操作1	・特権ID利用者による各サーバへのログオン及びログオフ	コマンドライン
			特権操作2	・個人情報及び財務データに対する参照及び更新（管理端末からのデータ参照要求及び更新要求が，DBでSQL文として処理される。）	表形式のGUI
			特権操作3	・コマンド，スクリプト及びプログラムの実行	コマンドライン
				・設定ファイルの参照及び更新	テキストエディタ
				・ERP業務パッケージにおける利用者権限の設定情報の参照及び更新	GUI
				・バッチ処理のスケジュールの参照及び更新	GUI
4	支社営業管理システム	PCサーバ	特権操作1	・特権ID利用者による各サーバへのログオン及びログオフ	GUI
			特権操作2	・個人情報及び財務データに対する参照及び更新（管理端末からのデータ参照要求及び更新要求が，DBでSQL文として処理される。）	表形式のGUI
			特権操作3	・コマンド，スクリプト及びプログラムの実行	コマンドライン
				・設定ファイルの参照及び更新	テキストエディタ

(3) 各特権操作に対して記録すべきデータ項目は，次の五つとする。

① 特権操作が行われた日時

② 特権操作に利用された利用者 ID

③ 特権操作が行われたサーバのホスト名又はサーバの IP アドレス

④ 特権操作の内容

⑤ 特権操作の結果（成功又は失敗。エラーメッセージなどの補助的情報で成功と失敗が判別できる場合は，結果が記録されなくてもよい。）

主要 4 システムの各特権操作に対して記録すべき特権操作の内容を表 4 に示す。

表 4　主要 4 システムの各特権操作に対して記録すべき特権操作の内容

特権操作の分類	記録すべき特権操作の内容
特権操作 1	(A) ログオン (B) ログオフ
特権操作 2	(C) 参照要求（又は SQL 文）及び参照されたデータの内容 (D) 更新要求（又は SQL 文）及び更新されたデータの内容
特権操作 3	(E) コマンド，スクリプト又はプログラムの実行文 (F) 参照された設定ファイルの内容又は更新された設定ファイルの内容 (G) 参照された ERP 業務パッケージにおける利用者権限の内容又は更新された ERP 業務パッケージにおける利用者権限の内容 (H) 参照されたバッチ処理のスケジュール又は更新されたバッチ処理のスケジュール

(4) 構築費用を抑えるため，製品の標準機能を最大限に活用する。

〔利用する製品の仕様〕

T 氏は，ログ管理システムに利用できる製品として，次の二つの製品を選んだ。

製品 R ：管理端末でログを取得し，収集保存及び分析を PC サーバで行う製品

製品 S ：各サーバの OS 及びミドルウェアが取得したログを UNIX サーバで収集保存及び分析する製品

T 氏は，OS 及びミドルウェアの標準機能，製品 R の機能並びに製品 S の機能に関する調査を行った。主要 4 システムの OS 及びミドルウェアの標準機能で共通に取得できるログのデータ項目を図 1 に，主要 4 システムの DBMS における DB アクセスに関するログ取得機能を表 5 に，製品 R の仕様を図 2 に，製品 S の仕様を図 3 に，それぞれ示す。

・操作が行われた日時
・操作に利用された利用者 ID
・操作が行われたサーバのホスト名
・次の操作内容
  - サーバに関するログオン及びログオフ
  - ファイルアクセスの内容（ファイル名，並びに作成，参照，更新及び削除の操作種別）
  - コマンド，スクリプト及びプログラムの実行文
・操作の結果（成功又は失敗）

図１　主要４システムの OS 及びミドルウェアの標準機能で共通に取得できるログのデータ項目

表５　主要４システムの DBMS における DB アクセスに関するログ取得機能

システム名	本社営業管理システム	会計管理システム	経理システム	支社営業管理システム
システムが使用している DBMS の製品名	G 社製品 H（汎用機版）	G 社製品 H（UNIX 版）	K 社製品 L（UNIX 版）	K 社製品 L（PC 版）
取得できるログのデータ項目	各 DB アクセスに対して，日時，利用者 ID，実行した SQL 文，SQL 文の実行結果がログファイルに出力される。			
ログ取得機能の設定方法	ログ取得を行うか否かを表ごとに設定する。		各利用者 ID が所属するユーザグループを定義し，ログ取得を行うか否かをユーザグループごとに設定する。	

・管理端末に導入するエージェントプログラム（以下，R エージェントという）と，ログ収集保存及び分析用の PC サーバに導入するサーバプログラム（以下，R サーバという）からなる。
・R エージェントは，キーボード，マウス及びディスプレイのデバイスドライバの動作を監視する。R エージェントは，R サーバ側で設定された，ログ取得開始の事象（管理端末での操作）を検知すると，取得するデータ項目及び取得時間の定義に従い，定期的に画面の画像データ並びにキーボード入力及び画面出力のテキストデータを取得する。複数ウィンドウを使って操作する場合は，取得したキーボード入力及び画面出力のテキストデータがどのウィンドウで入出力されたものか判別できない。
・取得したデータには，管理端末の認証機能で使われる利用者 ID と日時が付加される。
・R エージェントは，取得したログを，リアルタイム又はバッチ処理で R サーバに転送する。ネットワーク障害などで転送が失敗した場合，R エージェントは，ログを管理端末のハードディスクにファイルとして蓄積しておき，転送が可能になった時点で R サーバに転送する。
・R サーバに転送されたログは，毎日，画像データとテキストデータのそれぞれについて，一つずつのファイルとして保存される。ファイル名には日付を含む名前が付けられる。
・R サーバは，利用者 ID，日時及び取得したテキストデータに対する検索画面をもち，検索結果の利用者 ID，日時又はテキストデータをクリックすると対応する画像データが表示される。
・R サーバが提供するコマンドを利用して，利用者 ID，日時及びテキストデータに対する検索条件を指定して，画像データとテキストデータをファイルとして抽出することができる。

図２　製品 R の仕様

・各サーバに導入するエージェントプログラム（以下，S エージェントという）と，ログ収集保存及び分析用の UNIX サーバに導入するサーバプログラム（以下，S サーバという）からなる。
・S エージェントは，各サーバのログファイルにログデータが 1 レコード書き込まれるごとにそのレコードを S サーバに転送することでログの収集を行う。ネットワーク障害などでログデータの転送が失敗した場合，最大 1 時間再送を試行し，再送が成功しない場合は再送エラーとする。
・S サーバに収集されたログデータは，事前定義された変換ロジックに従い，標準のログフォーマットに変換され，ログデータベースに保存される。
・ログデータベースの内容は表形式で表示され，各データ項目に対する整列処理，検索処理を GUI から定義することで分析ロジックを組み立てることができる。
・分析結果のデータをグラフ化して表示したり，ファイルとして保存したりすることができる。

図 3　製品 S の仕様

〔ログ取得機能の設計〕

以上の検討結果に基づき，T 氏は，ログ取得機能の実装方法として，次の二つの案を Y 主任に説明した。

・各サーバの OS 及びミドルウェアの標準機能を利用する。
・製品 R を利用する。

なお，製品 S はログ取得機能をもたないので，ログ取得機能には利用できない。

Y 主任は，T 氏の案以外にも，通信経路でログを取得する，ネットワークフォレンジックと呼ばれている案もあるのではないかと質問した。T 氏は，通信経路でログを取得する案は採用できないことを説明した。

T 氏は，図 1 を基に，主要 4 システムにおける特権操作 1 については，OS 及びミドルウェアの標準機能で必要なログのデータ項目を取得できると判断した。一方，ログオフの操作に，パラメタなしの “exit”，“logoff”，“logout” といったコマンドが使われることから，製品 R では必要なデータ項目が取得できず，分析の際にもそのデータ項目の値を判別できない場合があると判断した。

T 氏は，これらの検討結果から，特権操作 1 について設計の前提条件を満たすためには，製品 R でなく，OS 及びミドルウェアの標準機能を使うべきだと判断した。

次に T 氏は，特権操作 2 に関するログ取得機能の実装方法を検討するために，主要 4 システムの DBMS が稼働している各サーバについて，サーバ資源の利用状況及び DB アクセス数全体に占める特権操作 2 の割合を調査した。T 氏は，サーバ資源の利用状況から，DBMS の標準機能によってログを取得すると，各システムの業務処理への影響が大きいと考えた。また，T 氏は，各システムの DB アクセス数は同程度で，その中での特

権操作の割合が5％だったことから，システムによってはログの保存及び分析のために大量のディスク資源を追加する必要があると考えた。T氏は，これらの検討結果から，特権操作2に対しては，DBMSの標準機能よりも製品Rを使う方が適切と判断した。

さらに，T氏は，図1及び図2を基に，特権操作3に対しては，OS及びミドルウェアの標準機能よりも製品Rを使う方が適切と判断した。

Y主任は，T氏の案をまとめ，X部長の承認を得た。

〔ログ収集保存機能の設計〕

次に，Y主任とT氏は，特権操作1のログに対する収集保存機能の設計を行った。製品Rの収集保存機能は，製品Rで取得したログを対象とした機能である一方，製品Sの収集保存機能は，主要4システムの管理及び運用に使われているOS及びミドルウェアのログ全てに適用できることから，T氏は，製品Sを採用することを提案した。

そこで，Y主任は，東京DCにSサーバを配置し，両DCのログデータを一括して収集する方法（以下，案1という）を考えた。案1の構成を図4に示す。

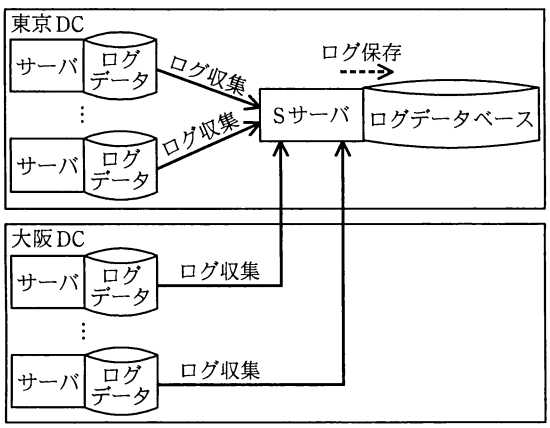

図4　案1の構成

サーバの中には，ログデータに割り当てられたディスク領域が一杯になると，新しいログデータで古いログデータを先頭から上書きするものがある。このことから，T氏は，ログが収集できない時間帯が発生する案1では，特別な運用対策が必要となることを指摘し，そうした対策の必要がないように，DCごとにSサーバを配置してログデータを収集する方法（以下，案2という）を提案した。案2の構成を図5に示す。

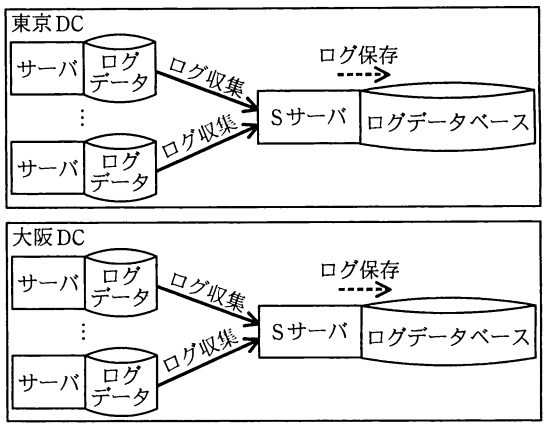

図５　案２の構成

Y 主任は T 氏の指摘を認め，X 部長も案 2 の構成とすることを承認した。

次に，Y 主任と T 氏は，特権操作 2 及び特権操作 3 のログに対する収集保存の方法を検討した。Y 主任は，東京 DC に R サーバを配置してログを収集保存する方法を考えた。図 6 に特権操作 2 及び特権操作 3 のログに対する収集保存の方法案を示す。

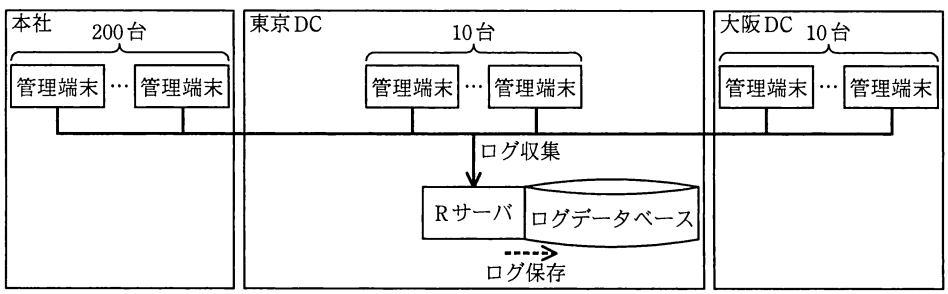

図６　特権操作２及び特権操作３のログに対する収集保存の方法案

T 氏は，収集保存の対象となる特権操作 2 及び特権操作 3 のログが大量になることから，ログの最大データ量とログ収集に必要なネットワークの伝送速度を見積もり，現在のシステム環境への影響を評価することを Y 主任に提案した。Y 主任は，見積りに関する基礎数値を設定し，①A 社全体で発生する特権操作 2 及び特権操作 3 に対する 30 日分のログの最大データ量と②製品 R を使って本社の管理端末 200 台から東京 DC にログを収集するために必要なネットワークの伝送速度を見積もった。見積りに関する基礎数値を図 7 に示す。

・1台の管理端末を8時間使用した場合，その間のログの最大データ量は，画像データとテキストデータを合わせて70Mバイトである。
・各管理端末は，年間を通じて1日平均8時間利用されている。
・製品Rを使って管理端末のログをRサーバに収集した場合，管理端末1台当たりに必要なネットワーク伝送速度は30kビット／秒である。

図7　見積りに関する基礎数値

Y主任とT氏は，見積結果から，現在のシステム環境への影響はないと判断し，東京DCにRサーバを配置してログを収集保存する方法について，X部長の承認を得た。

次に，Y主任は，ログファイル及びログデータベースのバックアップに関する運用規程を定める必要があると考え，現在のシステム運用を考慮して，その案を作成した。図8にログファイル及びログデータベースのバックアップに関する運用規程案を示す。

1. ログを保存する際は，一度データを書き込むと再書込みが不可能な磁気テープ媒体（以下，WORM（Write Once Read Many）テープという）を用い，正副の二つの媒体に保存する。
2. ログの保存期間は1年間とし，保存期間満了後は1週間以内に媒体を物理的に破壊し，廃棄する。
3. WORMテープには通番を付与し，台帳管理を行った上で，正の媒体はオペレータ室内の保管庫で，副の媒体は遠隔地で，それぞれ保管する。
   なお，副の媒体を遠隔地に運搬する際は安全な運搬手段を利用する。

図8　ログファイル及びログデータベースのバックアップに関する運用規程案

T氏は，特権操作2に関するログのデータ項目の内容を考慮し，運用規程案に追加すべき点を指摘した。③Y主任は運用規程案に項目を追加し，これまでの検討結果をまとめ，X部長の承認を得た。

〔ログ分析機能の設計〕

次にY主任とT氏は，ログ分析機能の設計を行った。Y主任は，他社で発生している情報漏えい事件の内容から，業務時間（月曜日から金曜日の9:00から17:00）外に行われた特権操作を優先的に監視する必要があると考えた。Y主任は，毎月第2金曜日に行われる運用報告会議において，前月のログに対する確認作業の結果を，各社の管理責任者がX部長に報告することを考えた。Y主任が考えたログ分析機能及び確認作業の内容は次のとおりである。

ログ分析機能：特権操作1に関するログから，業務時間外に行われた特権操作1のログを抽出する。

確認作業：抽出された特権操作1のログについて，関連する作業申請書と特権操作2及び特権操作3に関するログを基に，操作内容の必要性を確認し，確認者の氏名と確認結果を記録する。

Y主任は，情報システム部の従業員では一部の特権ID利用者について個々の操作内容の必要性を十分に確認できないことから，各社の管理責任者が確認作業を行う案に修正した。しかし，T氏は，その修正案には，特権操作の確認として不十分な点が別にあることを指摘し，改善案を提案した。Y主任は改善案に従って手順を修正し，これまでの検討結果をまとめ，X部長の承認を得た。

Y主任とT氏は引き続きログ分析機能の設計を行い，無事にログ管理システムの基本設計を完了した。

設問1　本文中の［　a　］及び表1中の［　b　］に入れるプロトコル名を，それぞれ英字4字以内で答えよ。

設問2　〔ログ取得機能の設計〕について，(1)～(5)に答えよ。

(1) T氏が，通信経路でログを取得する案を採用しなかった理由を，30字以内で述べよ。

(2) ログオフの操作について記録すべきデータ項目のうち，製品Rでは取得できないデータ項目は何か。25字以内で述べよ。その場合でも，ある条件の下では分析の際にそのデータ項目の値を判別できるが，それはどのような場合か。30字以内で述べよ。その際，判別の根拠となる情報は何か。45字以内で述べよ。

(3) DBMSの標準機能によるログ取得を行った場合，各システムの業務処理への影響が大きいとT氏が考えたのはなぜか。サーバ資源という用語を用いて30字以内で述べよ。

(4) DBMSの標準機能によるログ取得を行った場合，ログの保存及び分析に大量のディスク資源が必要になるシステムを，表3中の項番で二つ答えよ。また，その理由を30字以内で述べよ。

(5) 記録すべき特権操作の内容のうち，特権操作3に対して，主要4システムのOS及びミドルウェアの標準機能では取得できないものは何か。表4中から該当するものを全て挙げ，(A)～(H)の記号で答えよ。

設問3 〔ログ収集保存機能の設計〕について，(1)～(5)に答えよ。

なお，1Gバイト＝1,000Mバイト，1Mビット／秒＝1,000kビット／秒とする。

(1) 案1において，システムの障害発生時以外でログが収集できないのはどのようなときか。20字以内で答えよ。

(2) 本文中の下線①について，見積もった最大データ量（Gバイト）を求めよ。

(3) 本文中の下線②について，見積もった伝送速度（Mビット／秒）を求めよ。

(4) ログの保存にWORMテープを用いる目的を，15字以内で答えよ。

(5) 本文中の下線③について，Y主任が，運用規程案に追加した項目の内容を，20字以内で述べよ。

設問4 〔ログ分析機能の設計〕について，(1)～(3)に答えよ。

(1) 抽出した特権操作1のログに関連する，特権操作2及び特権操作3のログを，自動的に抽出できるようにログ分析機能を強化するためには，〔特権IDの利用〕における，サーバと管理端末の運用や利用の方法に関して変更又は追加が必要である。その内容を二つ挙げ，それぞれ25字以内で述べよ。

(2) 情報システム部の従業員では，どの特権ID利用者についての操作内容の確認が不十分となるか。表2中の役割名称で答えよ。また，その理由を，40字以内で述べよ。

(3) 各社の管理責任者が確認作業を行った場合，どのような特権操作に対する確認が不十分となるか。その操作を20字以内で述べよ。また，T氏が提案した改善案の内容を25字以内で述べよ。