問1　ERP パッケージの監査に関する次の記述を読んで，設問1～4に答えよ。

Z 社は，日用品の卸売業者であり，財務管理，購買管理，会計などの業務システムを ERP パッケージで再構築した。

〔ERP パッケージの概要〕

Z 社が導入した ERP パッケージ及び周辺システムの構成は，図のとおりである。

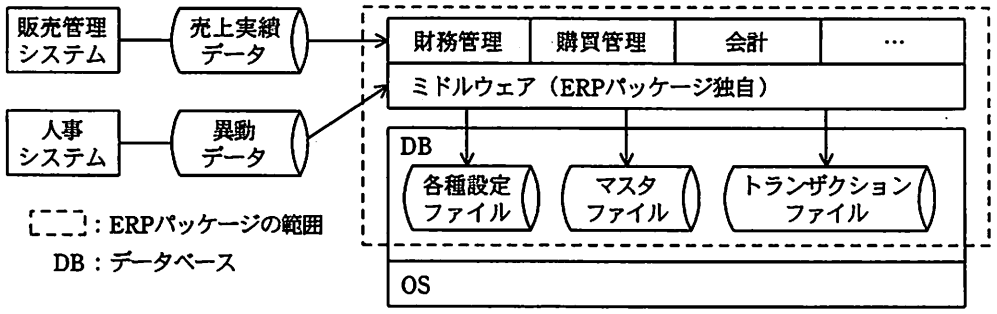

図　ERP パッケージ及び周辺システムの構成

(1)　OS 及び DB には，汎用の製品が採用されている。DB へのアクセスは，初期インストールのときを除いて，DB 用 ID を使用しなくてもよいようになっている。

(2)　財務管理，購買管理，会計などの業務システムは，ミドルウェアを経由して，マスタファイル及びトランザクションファイルを共有している。利用者は，ユーザ ID を使用して業務システムにアクセスする。

(3)　ミドルウェアの主な役割は，業務システムが基盤のアーキテクチャに依存しないで処理できるようにすることである。また，業務システムの安定運用を支援するための機能やセキュリティのレベルを設定する機能として，例えば，次のような機能が搭載されている。

・パスワードの最少けた数の設定機能
・多重ログイン（同一ユーザ ID による同時・複数のログイン）禁止の設定機能
・業務システムへのアクセス，ログインの失敗，マスタデータの変更などにおけるログ採取の設定機能

(4)　ERP パッケージの管理者用の機能を使用するためには，専用の管理者用 ID（以

下，管理者用 ID という）が必要である。管理者用 ID は，情報システム部のシステム管理担当者（以下，担当者という）3 名だけが使用を許可されている。管理者用 ID は，1 ライセンス（1 ユーザ）の契約で使用している。同時に 1 ユーザしか使用できないので，3 名の担当者は，パスワードを共有している。パスワードは，暗号化してファイルサーバのフォルダに保存されている。そのフォルダには担当者以外はアクセスできないように制限されている。

(5) ERP パッケージの DB には，各種設定ファイルのほかに，商品マスタや取引先マスタなどのマスタファイルと，仕入実績などのトランザクションファイルがある。

〔周辺システムとの連携〕

販売管理システムは，ERP パッケージとは別に構築・運用されている。ERP パッケージは，販売管理システムから日次で売上実績データを受け取る。受け取った売上実績データは，会計システムに自動連携され，店舗別，商品分類別に集計される。

人事システムは，ERP パッケージとは別のシステムであり，人事システムから ERP パッケージに，異動データが送られる。異動データには，所属部署及び役職の情報が含まれており，所属部署と役職に応じた利用権限が，ユーザ ID に自動的に設定される。

ただし，この権限については，異動データで自動削除されないようになっている。その理由は，人事異動などに伴う業務引継期間中に元の部署の権限が使用できなくなると，業務に支障を来すからである。業務の引継ぎが完了したら，異動者は元の部署の権限を削除してもらうための申請を速やかに提出し，担当者が申請に従って管理者用画面で削除する。

管理者用画面で権限が付与された場合には，ミドルウェアの機能によってログが採取される。

〔システム監査の実施〕

監査部では，Z 社のビジネスの中核を担う ERP パッケージを対象としたシステム監査を，毎年実施している。既に，業務面や機能面の監査は実施しているので，今年度は，アクセス管理及びバックアップリカバリの適切性を確認するシステム監査を実施することになった。担当するのは，監査部の T 氏である。

(1) アクセス管理の状況

T氏は，アクセス管理に関するリスク及びコントロールを表1のようにまとめた。

表1 アクセス管理に関するリスク及びコントロール（抜粋）

項番	リスク	コントロール
①	・ERPパッケージのDBに直接ログインされ，重要データが改ざんされたり，破壊されたりする。	・初期インストール後，DB用IDのパスワードが変更されていることを確認する。
②	・ユーザIDとパスワードが不正に取得され，業務システムが使用される。 ・ユーザIDの権限が不正に設定され，データが更新される。	・業務システムにログインしたユーザIDのログをモニタリングして，不正なアクセスが行われていないことを確認する。 ・ユーザIDと権限設定のリストを定期的に出力し，不要な権限が設定されていないことを確認する。
③	a	・業務の引継ぎが完了したら，異動者は元の部署の権限を削除してもらうための申請を速やかに提出する。

(2) バックアップリカバリの状況

ERPパッケージには標準で，データのバックアップのスケジュール管理機能が備わっている。担当者は，管理者用画面を使用して，バックアップの実行スケジュール，バックアップデータの記録装置，バックアップの種類（全件か差分か）などを設定する。T氏は，アクセス管理と同様に，バックアップリカバリについても，リスク及びコントロールを抽出して表2のようにまとめた。

項番①のコントロールについて，管理者用画面を確認し，バックアップデータが日次で取得されていることを確かめた。また，取得されたバックアップデータはすべて外部の保管業者に週次で送付し，保管していることを確認した。さらに，バックアップ媒体が読取り可能かどうかを定期的に確認していることを確かめた。

項番②のコントロールについて，障害発生時のリカバリ手順書及びリカバリ訓練の実施記録を閲覧し，問題がないことを確認した。しかし，災害発生時のリカバリについては手順書が作成されていないので，ERPパッケージのDBのバックアップが取得されていてもリカバリできないリスクがあると考えた。そこで，コントロール項目を追加して，更に詳しい調査を行うことにした。

表2　バックアップリカバリに関するリスク及びコントロール（抜粋）

項番	リスク	コントロール
①	・障害が発生した場合に，リカバリに必要なバックアップデータが使用できない。	・バックアップ媒体が，読取り可能であることを定期的に確認する。 ・バックアップ処理がスケジュールどおりに実行されていることをモニタリングする。
②	・障害が発生したときに，SLA に記載された時間内にリカバリできない。 ・災害が発生したときに，外部に保管されているバックアップデータからリカバリできない。	・リカバリ手順を文書化する。 ・リカバリ訓練を定期的に実施する。

設問1　〔ERP パッケージの概要〕の(4)について，管理者用 ID のライセンス契約に違反していないことを確認するための監査手続を，45 字以内で述べよ。

設問2　表1中の項番①のコントロールが有効でも，リスクが十分に軽減されているとは言えない。T 氏が本調査で更に確認すべきコントロールを，40 字以内で述べよ。

設問3　表1中の［ a ］に入れるリスクを，40 字以内で述べよ。また，異動者の申請による削除よりも確実にリスクを低減できるコントロールを，45 字以内で述べよ。

設問4　表2中の項番②について，災害が発生したときのリスクに対して追加すべきコントロールを，45 字以内で述べよ。