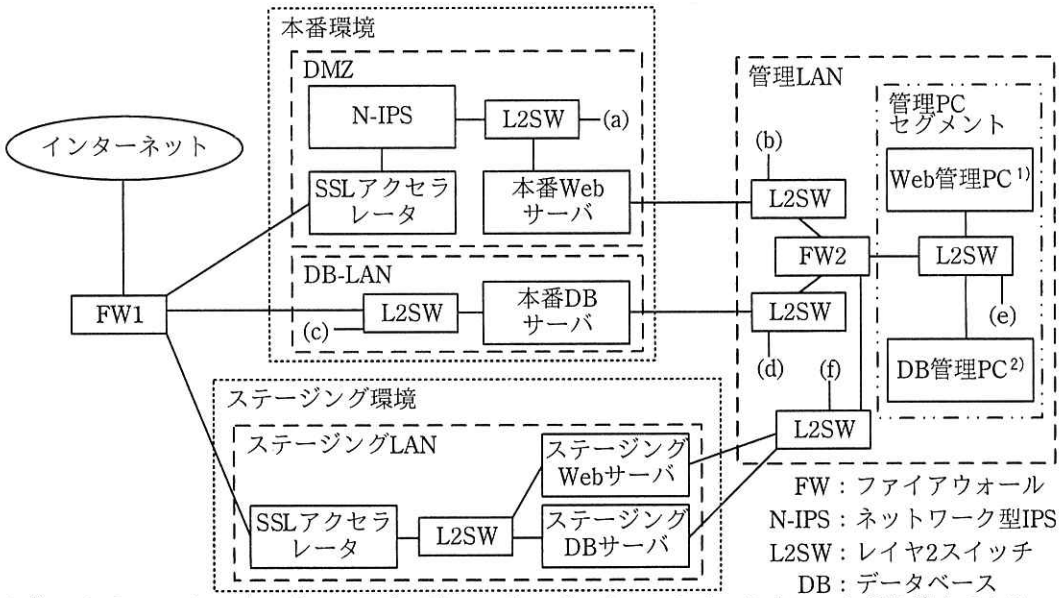
問３　Web システムのセキュリティ診断に関する次の記述を読んで，設問 1，2 に答えよ。

L 社は，EC サイトを運営している従業員数 800 名の企業である。L 社のモールの会員は，モールで買物をすると，購入金額に応じて L 社が独自に発行するポイントが得られる。L 社のポイントサービス部が管理するポイントシステム（以下，P システムという）のネットワーク構成を図 1 に示す。



注 1)　本番 Web サーバ及びステージング Web サーバのリモートメンテナンスを行う端末である。

注 2)　本番 DB サーバ及びステージング DB サーバのリモートメンテナンスを行う端末である。このリモートメンテナンスは，DB 管理 PC からだけ行うよう運用ルールが定められている。

注記 1　DMZ から DB-LAN への通信は FW1 を経由する。

注記 2　本番 Web サーバ，本番 DB サーバ，ステージング Web サーバ，ステージング DB サーバはそれぞれ，サービス用と管理用の二つの NIC を備えている。

注記 3　ステージング環境は，主に新しいソフトウェアを本番環境に導入する際の動作確認に利用されている。保存されているデータはテスト用データである。

図 1　P システムのネットワーク構成（概要）

P システムが受信する 1 日の時間帯別の通信量の比率は，0 時～8 時が 2%，8 時～16 時が 55%，16 時～24 時が 43%である。P システムの機器は全て固定 IP アドレスで運用している。

P システムの機器の概要を表 1 に示す。

表1　Pシステムの機器の概要（抜粋）

機器名	概要
N-IPS	インターネットから本番 Web サーバへの通信，本番 Web サーバから DB-LAN への通信を監視している。遮断モードと検知モードの 2 種類のモードがあり，通信を脅威と判定したとき，遮断モードでは通信を拒否する。通信が脅威かどうかの判定では，通信ごとに，次の番号の小さい順に，最初に合致したルールが適用される。 1. ホワイトリスト判定：ホワイトリストに登録した IP アドレスからの通信は，脅威ではないと判定する。 2. 脅威通信判定：通信の内容を解析し，脅威レベルが高いと定義しているものは，脅威と判定する。 現在は，遮断モードに設定されており，ホワイトリスト判定と脅威通信判定が有効になっている。ホワイトリストには，現在，IP アドレスは一つも登録されていない。
本番 Web サーバ	会員が利用するポイント照会などの機能をもつ Web サーバである。本番 DB サーバにアクセスする。
本番 DB サーバ	会員のポイント情報や購入履歴などの情報をもつ DB サーバである。ホスト型 IPS が導入されている。本番 DB サーバで利用されているホスト型 IPS の概要を図 2 に示す。
FW1	ステートフルパケットインスペクション型の FW である。インターネットから本番 Web サーバ，本番 Web サーバから本番 DB サーバへの通信のうち必要なものだけを許可している。また，インターネットからステージング Web サーバへの通信は，普段は拒否しているが，ステージング環境利用時だけ必要なものを許可している。DB-LAN から DMZ 及びインターネットへの通信，並びに本番環境とステージング環境の間の通信を拒否している。
FW2	ステートフルパケットインスペクション型の FW である。管理 PC セグメントから，本番 Web サーバ，本番 DB サーバ，ステージング Web サーバ及びステージング DB サーバへの通信を許可し，それ以外の通信は全て拒否している。

通信ごとに，ホワイトリスト設定による判定が行われ，許可された通信は，侵入検知設定による判定が行われる。ホワイトリスト設定や侵入検知設定による判定で通信が拒否されると，ポイントサービス部運用グループの執務室内にある警告灯[1)]を点灯させる。

1. ホワイトリスト設定：登録された IP アドレスからの通信だけを許可し，それ以外を拒否する。ホワイトリストには，現在，本番 Web サーバと DB 管理 PC の IP アドレスだけが登録されている。
2. 侵入検知設定：ホストの通信を監視して，脅威と判定した通信を拒否し，それ以外を許可する。侵入検知設定は無効にもでき，無効にすると，ホストの通信を全て許可する。

注[1)]　警告灯が点灯すると，運用グループは，緊急対応体制をとり，最優先で対処を行う。

図2　ホスト型 IPS の概要

〔P システムの診断計画〕

EC サイトへの情報セキュリティ上の脅威の高まりを受け，L 社は，P システムの脆弱性診断を実施することを決定した。L 社のリスク管理部の T 主任と部下の U さんが，診断計画を策定する担当に任命された。T 主任は，図 3 に示す診断要件を基に診断計画を策定するよう U さんに指示した。

1. 本番環境への影響を最小化すること
2. 診断に当たってネットワーク構成，システム構成，設定及びデータを変更した場合は，診断終了後，診断前の状態に戻し，システムの正常な動作を確認すること

図 3　診断要件

U さんは，専門業者の診断サービスについて調査し，図 4 に示す調査結果を得た。

診断サービスでは，診断 PC で診断対象機器と通信し，レスポンスの内容を評価して脆弱性の有無を確認する。診断 PC は，既存の機器とは別の IP アドレスを設定し，インターネット又は内部のネットワークに接続する。次の 2 種類の診断方法がある。

・プラットフォーム診断（以下，PF 診断という）：サーバやネットワーク機器に対して，全てのポートをスキャンする。開いているポートを発見すると，そのポートを使って検査する。主に OS やミドルウェアの脆弱性を検出できる。
・Web アプリケーション診断（以下，Web 診断という）：Web アプリケーションプログラムを検査することによって，その脆弱性を検出できる。

図 4　診断サービスの調査結果

U さんは，調査結果を基に L 社で実施すべき脆弱性診断の検討に入った。Web 診断については，次のように実施することにした。

・診断用の利用者 ID を作成する。その利用者に診断用のポイントを付与し，P システムにログインして診断する。
・ログイン無しでアクセスできるページも診断する。
・診断前の状態に戻せないようなデータの更新が発生する診断は実施しない。

PF 診断については，T 主任から助言を得ることにした。次は，本番 Web サーバがインターネットから攻撃される脅威を想定した時の，PF 診断に関する，U さんと T 主任の会話である。

Uさん： インターネットから診断する場合，調査した幾つかの事例によると，PF診断の実施時だけ，N-IPS の脅威通信判定を無効にすることがあるようです。有効なまま診断するケースと比べ，無効にすると，①より多くの脆弱性を検出する可能性があります。

T主任： 無効にすると，PF診断実施時に本物の攻撃を防げないというリスクも生ずる。無効にするのではなく，②N-IPS の設定を変更すれば，そのようなリスクは生じない。

Uさん： 分かりました。

T主任： それと，インターネットからの PF 診断の通信経路を考慮すると，インターネットからのPF診断だけでなく，内部のネットワークからのPF診断も実施すべきだ。

Uさん： 分かりました。その場合は，想定する脅威を踏まえると，診断 PC を図1中の接続点［ a ］に接続して診断すれば良いでしょうか。

T主任： そのとおりだ。

U さんは T 主任のアドバイスを踏まえ，更に検討を進め，診断計画を表2のとおりにまとめた。

表2 診断計画（抜粋）

項目	内容
日時	○月×日から○月△日（10 営業日） 9 時～17 時（うち，診断時間は 1 日当たり連続した 5 時間程度）
診断対象	P システムの本番環境
診断内容	次の診断を順に行う。 診断 1：本番 Web サーバの脆弱性診断 攻撃者がインターネットから本番 Web サーバを攻撃し，本番 DB サーバの秘密情報を窃取する脅威を想定し，次の二つの診断を行う。 ・インターネットから，本番 Web サーバに PF 診断，Web 診断を行う。 ・図 1 中の接続点［ a ］から，本番 Web サーバに PF 診断，Web 診断を行う。 診断 2：本番 DB サーバの脆弱性診断 攻撃者が何らかの方法で管理 LAN に侵入し，本番 DB サーバの秘密情報を窃取する脅威を想定し，次の診断を行う。 ・図 1 中の接続点(e)から，本番 DB サーバに PF 診断を行う。
検査項目	診断によってサービスダウンを引き起こす可能性がある項目を含め，使用する商用検査ツールに登録されている全ての検査項目の診断を行う。ただし，診断前の状態に戻せないようなデータの更新が発生する検査項目は除く。

〔P システムの診断計画レビュー〕

診断計画レビューにおいて T 主任は，診断の検査項目の内容は妥当であるとした上で，次の指摘を行った。

指摘 1： Web 診断は本番環境ではなく，ステージング環境で行うべきである。ステージング環境で実施する際，全ての診断の終了後に，担当者が，FW1 の設定を元に戻すこと，及びステージング環境の［ b ］を削除することを，明確に手順書に記載すること

指摘 2： PF 診断は本番環境で実施すべきだが，サーバが異常停止した場合の影響を最小化するために③計画の一部を変更すること

指摘 3： 診断 2 の実施に当たっては，警告灯が点灯することで社内に混乱が起きないよう，運用グループに④機器の設定の変更を依頼すること

その後，指摘 3 に従い，U さんは運用グループに診断計画を説明して設定の変更を依頼した。運用グループから，設定の変更については承諾を得られたが，診断計画について，診断 2 の診断 PC を接続するポイントを，図 1 の(e)から(d)に変更する必要があるという提案があった。

この提案について，運用グループから説明があった。運用グループによれば，最近配属された担当者が，Web 管理 PC から本番 DB サーバにログインを試みた。その結果，警告灯が点灯し，運用グループは緊急対応体制をとることになってしまった。その再発防止策の一つとして，FW2 のルールを修正し，［ c ］宛ての通信については，［ d ］からの通信だけを［ e ］することにした。その影響で，接続ポイントの変更が必要になるとのことだった。

U さんは T 主任の指摘及び運用グループからの提案を踏まえ，診断計画を確定し，診断実施に向けて準備を進めた。

設問1　〔P システムの診断計画〕について，(1)～(3)に答えよ。

(1) 本文中の下線①について，その理由を 35 字以内で述べよ。

(2) 本文中の下線②について，どのような設定変更をすべきか。設定変更の内容を 30 字以内で述べよ。

(3) 本文中及び表 2 中の［ a ］に入れる診断 PC の接続箇所を，図 1 中の接続点(a)～(f)の記号で答えよ。

設問2　〔P システムの診断計画レビュー〕について，(1)～(4)に答えよ。

(1) 本文中の［ b ］に入れる適切な字句を，15 字以内で具体的に答えよ。

(2) 本文中の下線③について，何をどのように変更すべきか。P システムの通信量に着目し，変更する項目を表 2 から選び答えよ。また，変更する内容を 20 字以内で述べよ。

(3) 本文中の下線④について，どの機器に対して，どのように設定を変更すべきか。機器は図 1 中から選び，変更後の設定は 55 字以内で具体的に述べよ。

(4) 本文中の［ c ］，［ d ］に入れる適切な字句を，図 1 中から選び答えよ。また，本文中の［ e ］に入れる適切な字句は，許可又は拒否のいずれか。答案用紙の“許可”，“拒否”のいずれかを○印で囲んで示せ。

6. 退室可能時間中に退室する場合は，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	13:10 ～ 13:50

7. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，次のものに限ります。

   なお，会場での貸出しは行っていません。

   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。
13. 午後Ⅱの試験開始は 14:30 ですので，14:10 までに着席してください。