NW

平成22年度　秋期
ネットワークスペシャリスト試験
午後Ⅱ　問題

試験時間	14:30 ～ 16:30（2時間）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. この注意事項は，問題冊子の裏表紙に続きます。必ず読んでください。
4. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
5. 問題は，次の表に従って解答してください。

問題番号	問1，問2
選択方法	1問選択

6. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B又はHBの黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に，**受験番号**を記入してください。正しく記入されていない場合は，採点されません。
   (3) **生年月日欄**に，受験票に印字されているとおりの**生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。
   (4) **選択した問題**については，次の例に従って，**選択欄の問題番号**を**○印**で囲んでください。

   なお，○印がない場合は，採点の対象になりません。2問とも○印で囲んだ場合は，はじめの1問について採点します。

   〔問2を選択した場合の例〕

選択欄	
1問選択	問1
	○問2

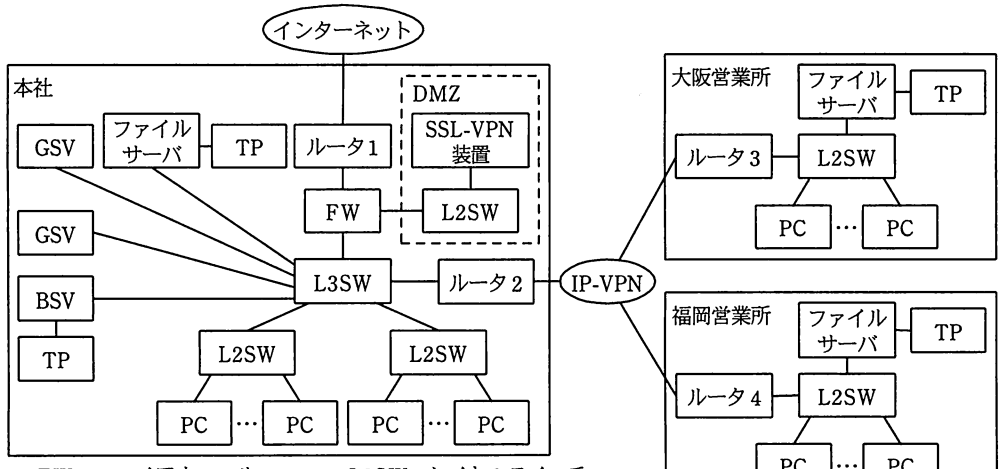
   (5) 解答は，問題番号ごとに指定された枠内に記入してください。
   (6) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問1　業務システムの再構築に関する次の記述を読んで，設問1～6に答えよ。

T社は，コンピュータ関連製品の卸売会社である。従業員数は400名で，東京に本社が，大阪，福岡に営業所がある。T社の営業員200名及び技術員100名は，外出先で活動することが多い。営業員は，担当する販売代理店への営業活動を行い，技術員は，自社の取扱商品の技術サポートを行っている。営業員と技術員は，外出先にデータ通信カードを装着したPCを携帯し，インターネット経由でSSL-VPN装置に接続して，T社内のシステムを利用している。

T社では，販売，購買，会計などの業務システムを運用している。現在のネットワークシステム構成を，図1に示す。



FW：ファイアウォール　　L2SW：レイヤ2スイッチ
GSV：業務サーバ　　L3SW：レイヤ3スイッチ
TP：テープ装置　　BSV：GSVで稼働する業務システム用のバックアップサーバ

注　IP-VPNの回線速度は，すべて10Mビット／秒である。

図1　現在のネットワークシステム構成（抜粋）

T社では，業務システムの機能強化を目的に，システムの再構築を行うことにした。機能強化策の一つとして，取扱商品を大幅に増やすために，商品マスタを50万レコードに拡大する。併せて，以前から改善が求められていた，ファイルサーバのデータバックアップの見直しも行う。これらを推進するためのプロジェクトマネージャとして，情報システム部のW部長が任命された。W部長は，販売，購買，会計などの業務の責任者及びシステム基盤設計，構築，運用の責任者を選出して，新業務システム開発プロジェクトを発足させた。

新業務システムの概要設計完了後，W 部長は，部下の Y 課長に対してシステム基盤と運用管理方式の設計を指示した。Y 課長は，環境の変化に柔軟に対応できるようにすることと，運用負荷を抑えるために，新業務システムを稼働させるシステム基盤に，サーバ仮想化技術を活用することにした。

〔システム基盤の設計〕

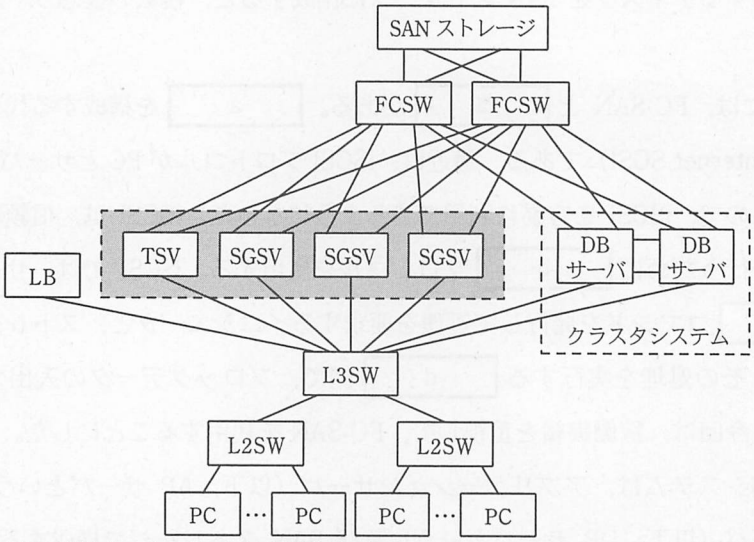
サーバの仮想化を実現させる仕組み（以下，仮想化機構という）を動作させるサーバのことを，物理サーバという。仮想化機構によって，物理サーバ上に作成されるサーバ機能を，仮想サーバという。仮想サーバは，物理サーバ上に複数作成できる。仮想サーバが使用するディスクは，物理サーバのローカルディスク と SAN に接続されたディスク装置（以下，SAN ストレージという）に作成することができる。仮想サーバが使用するディスクを SAN ストレージに作成すると，複数の仮想サーバで共用できる。

SAN には，FC-SAN と［ a ］がある。［ a ］を構成する代表的な技術が iSCSI（internet SCSI）である。最近は，iSCSI プロトコルが PC とサーバ OS に実装されているので，iSCSI を容易に利用できるようになった。iSCSI は，信頼性のあるデータ通信を行うために［ b ］プロトコルを使用する。iSCSI では，サーバで稼働し，［ c ］コマンドを発行して処理を要求するイニシエータと，ストレージ装置で稼働して，その処理を実行する［ d ］間で，ブロックデータの入出力を実現させている。今回は，稼働実績を重視して，FC-SAN を利用することにした。

新業務システムは，アプリケーションサーバ（以下，AP サーバという），データベースサーバ（以下，DB サーバという）及び SAN ストレージで構成する。AP サーバは，仮想サーバで稼働させる。DB サーバは，AP サーバのアプリケーションプログラムから使用される。T 社では，仮想化機構を活用したシステム構築は初めての経験だったので，DB サーバは，2 台でアクティブスタンバイ型のクラスタシステムを構成し，仮想化機構を利用しないことにした。クラスタシステムでは，ハートビートパケットで各サーバの生存を確認するが，①各サーバが稼働しているにもかかわらず，ハートビートパケットを受信できなくなると，サービスを正常に提供できなくなる危険性がある。この障害を避けるために，②各サーバの生存確認を確実に行うための対応策を実施する。

仮想化機構には，物理サーバの障害時や負荷増大時の対策機能が備わっている。しかし，この機能だけでは不十分なので，負荷分散装置（以下，LB という）を利用して，AP サーバの冗長性を高めるとともに，［　e　］も向上させることにした。利用する LB には，負荷分散時に送信元 IP アドレスを LB のものに付け替えるソース NAT 機能があるが，AP サーバを使用する PC を特定するために，この機能は利用しない。また，LB による AP サーバの稼働状態管理を確実に行うために，AP サーバからの返送パケットは，LB を経由させることにする。

AP サーバを稼働させる物理サーバ（以下，SGSV という）は，障害時の影響を低減させるために，3 台構成にする。各 SGSV では，AP サーバを 2 台ずつ，全体で 6 台を稼働させて，能力面で余裕をもった構成にする。そのほかに，テスト用の物理サーバ（以下，TSV という）も用意する。新業務システムの構成を，図 2 に示す。



注1　網掛け中の物理サーバでは，仮想化機構が稼働する。　　FCSW：ファイバチャネルスイッチ
注2　各 SGSV では，2 台の AP サーバが稼働する。
注3　LB は，SGSV で稼働する AP サーバの負荷分散だけを行う。
注4　TSV では，テスト用の AP サーバと DB サーバが稼働する。

図 2　新業務システムの構成

〔データバックアップの検討〕

現在，営業所ごとにファイルサーバのデータを TP にバックアップしており，テープの管理やエラー時の対応などで，営業所員に負担を強いている。この問題を解決するために，TP へのバックアップを止め，すべての営業所のバックアップデータを本社に集めて，新業務システムのデータバックアップと統合するのが効果的と判断した。

遠隔地にバックアップする場合は，バックアップとリストアを高速化するために，通信帯域の確保が必要になる。そこで，通信帯域をあまり必要としないバックアップ方式を調査したところ，重複除外機能をもつバックアップシステムを利用すれば，バックアップデータ量を飛躍的に削減できることが分かった。

重複除外機能は，サーバデータをブロックに分割し（以下，ブロックデータという），更新されたブロックデータが既にバックアップサーバに存在した場合，そのブロックデータをバックアップしない働きをもつ。重複除外機能をもつバックアップシステムは，バックアップ対象のデータをもつサーバに導入されるエージェントと，バックアップデータを保存するバックアップサーバから構成される。バックアップ対象のサーバでの重複除外処理の概要を，図3に示す。

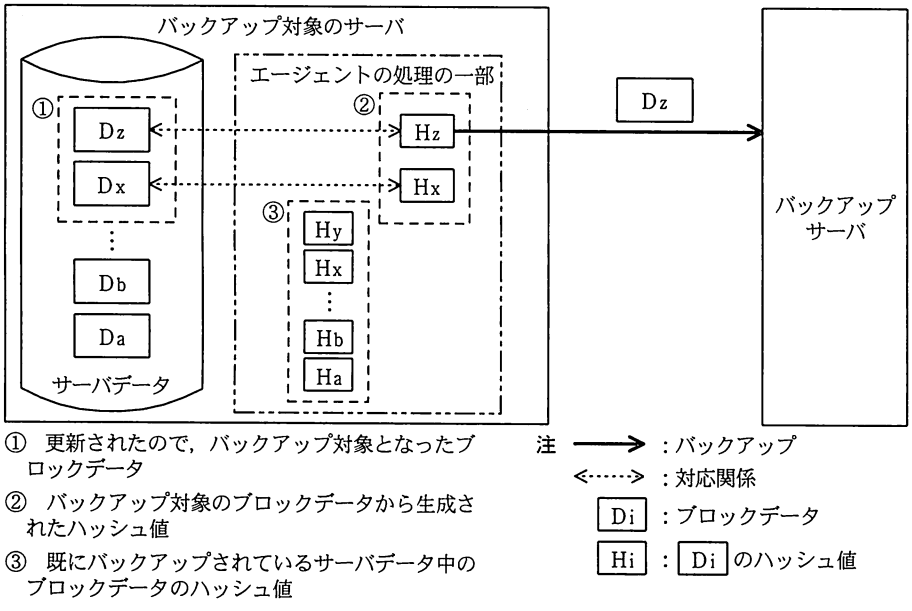


図3　バックアップ対象のサーバでの重複除外処理の概要

エージェントは，ハッシュ値同士の比較によって，更新されたブロックデータがバックアップ済かどうかをチェックする。図3中に示した②のHxとHzのうち，Hxは，③のハッシュ値の中に存在するので，Dxはバックアップされない。Hzは，③のハッシュ値の中に存在しないので，Dzがバックアップサーバに送られて，バックアップされる。このように，更新されたブロックデータから生成されたHxとHzが，③のサーバデータのハッシュ値に存在するかどうかをチェックすることで，DxとDzが，既

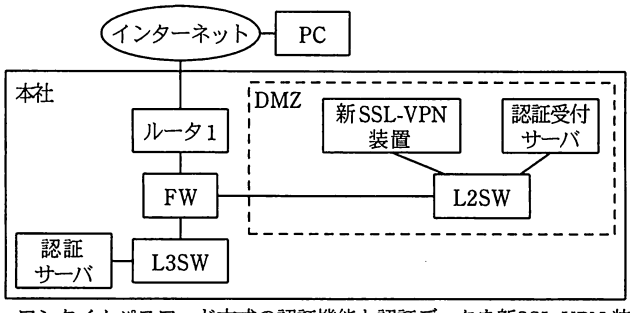
にバックアップされたブロックデータと重複しているかどうか判断される。

ハッシュ値は，低い確率ではあるが，③ハッシュ値の衝突が発生するので，発生確率を更に低くするために，様々な対応策が考えられている。今回使用する重複除外機能をもつバックアップシステムでは，独自の対応策が実施されている。

〔セキュリティ強化策と回線の検討〕

外出先から T 社内のシステムを利用するときの認証は，ログイン ID と固定パスワードだけで行われているので，セキュリティ上の問題を洗い出し，強化策を検討することにした。

調査した結果，ワンタイムパスワード方式の認証システムを導入し，既設の SSL-VPN 装置の代わりに，PC のセキュリティチェック機能をもち，認証システムと連携も可能な SSL-VPN 装置（以下，新 SSL-VPN 装置という）を導入すれば，少ない変更でセキュリティを強化できることが分かった。認証システムは，認証受付サーバと認証サーバで構成される。認証システムと新 SSL-VPN 装置の構成を，図 4 に示す。



注1 認証受付サーバは，ワンタイムパスワード方式の認証機能と認証データを新SSL-VPN 装置に引き渡す連携機能をもつ。
注2 認証サーバは，ランダムな数表の発行や認証処理を行う。RADIUS サーバ機能ももつ。

図 4　認証システムと新 SSL-VPN 装置の構成

新 SSL-VPN 装置と認証システムとの連携処理手順を，次に示す。

（ｉ） 利用者は，PC のブラウザで，新 SSL-VPN 装置に接続する。

（ii） 新 SSL-VPN 装置は，セキュリティポリシに従って，PC をチェックする。

チェック項目には，セキュリティパッチ，稼働プロセス，ウイルス対策ソフトなどが設定できる。チェック結果が正常のときには，認証受付サーバにリダイレクトされる。チェック結果が異常のときには，PC との接続が切断される。

（iii） 認証受付サーバによって，ログイン ID 入力画面が PC に表示される。

利用者が，ログイン ID を入力すると，認証受付サーバは，ログイン ID を基に，ランダムな数表を取得し，次の処理に移る。

(iv) 認証受付サーバによって，認証画面が表示される。

利用者は，PC に表示されたランダムな数値で構成される数表から，事前に決めた数表の位置に表示されている数値をパスワードとして入力する。入力された数値がチェックされ，正しければ，新 SSL-VPN 装置にリダイレクトされ，ログイン ID とパスワードが，新 SSL-VPN 装置に送信される。

(v) 新 SSL-VPN 装置は，受信したログイン ID とパスワードを基に，RADIUS プロトコルで，認証サーバに対し認証を要求する。

認証後，接続可能なサーバ一覧などを PC に表示する。

(vi) 利用者が，サーバ一覧の中から接続したいサーバを指定すると，PC と新 SSL-VPN 装置間で VPN が設定され，本社のサーバに接続できる。

次に，本社と各営業所間の回線が，継続して利用できるかどうかを検討した。

ルータ 2 のログから送受信データ量を確認したところ，本社と営業所間で発生するトラフィックは，日中最大となり，7M ビット／秒であった。このうち，既存の業務システム利用のトラフィックが 40%である。このトラフィックは，新業務システムの利用で，1.3 倍になることが見込まれる。これらの条件から，本社と営業所間の最大トラフィックは，［ ア ］M ビット／秒であり，増加量は少ないことが判明した。

各営業所のデータバックアップは，夜間に行う。各営業所のファイルサーバのデータ量は 1T バイトである。2 回目以降のバックアップデータ量は，ベンダの情報によれば，重複除外機能によって全体の 0.5%以下に削減される。これらの条件から，許容時間内にバックアップを完了できる見込みである。

以上の検討によって，本社と各営業所間の回線が，継続して利用可能と判断した。

〔システムの運用管理方式の設計〕

新業務システムでは，統合監視システムを利用して，ネットワーク機器とサーバの稼働状態の監視を行う。

(1) ネットワーク機器の監視

統合監視システムには，④監視対象機器を発見して，接続構成図を自動作図する

機能があるので，管理者は，接続構成図の中から，監視するネットワーク機器を選択することができる。ネットワーク機器の監視は SNMP で行われ，ネットワーク機器の稼働状態を，MIB 情報の定期的な収集によって監視するとともに，Trap の受信によって異常を検知する。

(2) サーバの監視

サーバの監視は，あらかじめ設定された間隔で，各サーバから監視対象の情報を収集して行う。収集した情報の中に異常が発見されたときには，その内容がメッセージ表示画面に表示される。監視項目には，CPU，メモリなどの使用率，サービスとプロセスの稼働状態及びイベントログの内容がある。仮想サーバを活用したシステムでは，仮想サーバの稼働状態監視だけでは十分でないので，⑤通常のサーバ監視よりも複雑な監視が必要になる。イベントログの監視では，フィルタ機能の活用が必要になり，フィルタの条件設定には，⑥運用後のチューニングが必要になる。

新業務システム構築後のネットワークシステム構成を，図5に示す。

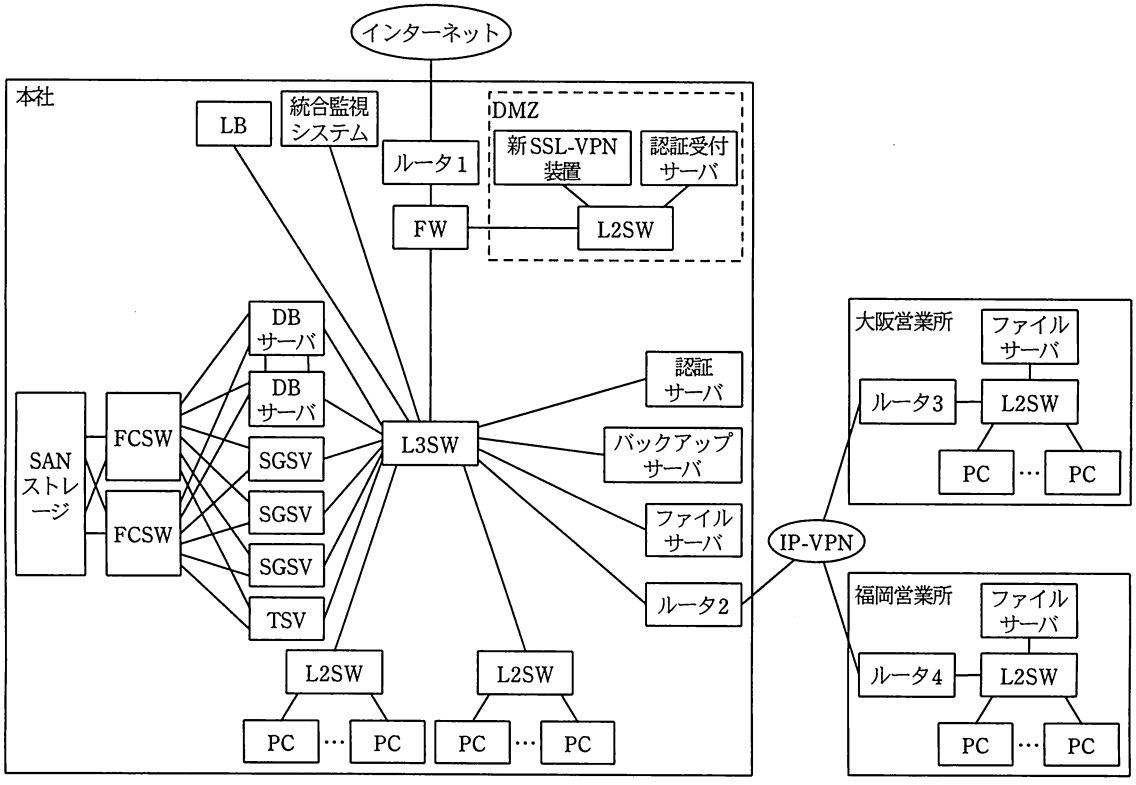


図5　新業務システム構築後のネットワークシステム構成（抜粋）

〔システムの切替え〕

W 部長は，プロジェクトメンバと共同で，システム切替えまでの準備作業のスケジュールと，切替時の作業スケジュール（以下，システム切替スケジュールという）を立案した。そして，W 部長は，プロジェクトメンバを各作業の責任者として，システム切替えまでの準備作業を実施させた。

各種テストの終了後，受注から代金回収までの，一連の業務の流れに沿って処理を進める方式で，総合テストを実施し，問題なく完了した。

負荷テストは，Y 課長が担当した。負荷テストでは，新業務システムの処理能力を確認するために，本番と同じ 6 台の AP サーバを稼働させて実施した。LB には，処理を平均的に分散させるために，ラウンドロビン方式が設定されている。

負荷テストは，11：00 から 12：00 までの間に，主要業務の販売と購買のシステムを利用する社員に，日常的に行われる業務を処理してもらって行った。負荷テストは順調に進み，ほぼ期待どおりの結果が得られ完了した。負荷テストにおける，ある時間内での CPU 使用率を，表に示す。

表　負荷テストにおける，ある時間内での CPU 使用率

単位　%

測定項目	物理サーバ 1		物理サーバ 2		物理サーバ 3	
	仮想サーバ 1	仮想サーバ 2	仮想サーバ 3	仮想サーバ 4	仮想サーバ 5	仮想サーバ 6
CPU 使用率	10～40	20～60	50～100	60～100	20～50	10～50

負荷テストで，6 台の仮想サーバに処理が振り分けられたことを確認できた。しかし，CPU 使用率の高い状態が続いた仮想サーバが存在していた。振り分けられた処理との関係を調べたところ，メモリに読み込んだ商品マスタの大量のデータに対して，検索を伴う処理を実行した仮想サーバが，高負荷になることが判明した。新業務システムの中には，仮想サーバに大きな負荷を与えるプログラムがあるので，このようなプログラムを実行するサーバに負荷を集中させることなく，負荷を平準化するために，負荷分散方式の見直しを行うことにした。

データ移行テストでは，既存の業務システムから新業務システムへのトランザクションデータの移行が，正しく行えるかどうかを確認する。データ移行は，移行データの作成，移行データの取込み，及び移行データの確認の 3 段階で行われる。移行デー

タは，既存の業務システムからトランザクションデータを抽出し，各種マスタとテーブルを参照して，加工処理が施されて作成される。移行データの取込みでは，取込みプログラムで，移行データを新業務システムに取り込む。移行データの確認では，新業務システムに取り込まれたデータの正当性を，新業務システムのプログラムでチェックする。データ移行テストを何回か繰り返した結果，問題なくデータ移行を行えることが確認できた。

以上の準備作業を行った後，システム切替え当日，システム切替スケジュールに従って，作業を実施した。システム切替スケジュールを，図6に示す。

作業内容	月末（金曜）	稼働2日前（土曜）	稼働1日前（日曜）
月締め処理	→		
移行データの作成	——→	——→	
移行データの取込み	——→	——→	——→
移行データの確認			——→
業務開始準備			——→

図6　システム切替スケジュール

システムの切替えは，月末の金曜日から 3 日間掛けて実施した。金曜日の業務終了後に，月末の締め処理を行い，その後にデータ移行作業を開始した。移行データの確認後，月曜日の業務開始のための準備作業を行い，システム切替作業を終了した。データ移行作業の途中で問題が幾つか発生したが，必要な対応措置をとり，無事に新業務システムを稼働させることができた。

設問1　本文中の［ a ］～［ e ］に入れる適切な字句を答えよ。

設問2　〔システム基盤の設計〕について，(1)，(2)に答えよ。

(1) 本文中の下線①の状況の発生で，サービスが正常に提供できなくなる DB サーバの状態を，40 字以内で述べよ。また，下線②の対応策の内容を，25 字以内で述べよ。

(2) 図2で，PC からの処理要求が AP サーバと DB サーバで処理されて，処理結果が PC に転送されてくる経路を，次の【転送経路】に示す。(a)，(b)に入れるサーバと機器を，図2中の名称を用いて，【転送経路】の表記方法に従い，すべて記述せよ。

【転送経路】

PC→［　(a)　］→AP サーバ→L3SW→DB サーバ→
L3SW→AP サーバ→［　(b)　］→PC

設問 3　〔データバックアップの検討〕について，(1) ～ (3) に答えよ。

(1) 重複除外処理にハッシュ関数を利用する利点を，30 字以内で述べよ。

(2) 本文中の下線③の衝突によって引き起こされる問題を，30 字以内で述べよ。

(3) 上記 (2) の問題の発生確率を更に低くする方法について，考えられる方法を，50 字以内で述べよ。

設問 4　〔セキュリティ強化策と回線の検討〕について，(1) ～ (4) に答えよ。

(1) 手順 (ii) の PC のチェックは，すべての PC に対して行われる。新 SSL-VPN 装置が PC に対して行う処理を，25 字以内で述べよ。また，認証受付サーバと認証サーバ間の通信が発生する箇所を，連携処理手順 (i) ～ (vi) の中から，すべて選んで答えよ。

(2) セキュリティ強化策によって，セキュリティ面で改善される点を二つ挙げ，それぞれ 25 字以内で述べよ。

(3) 認証システムを導入したときに，FW に新たに許可設定すべき通信を二つ挙げ，それぞれ送信元とあて先を明確にして，25 字以内で答えよ。

(4) 本文中の［　ア　］に入れる数値を求めよ。答えは，小数点以下を切り上げて整数で求めよ。

設問 5　〔システムの運用管理方式の設計〕について，(1) ～ (3) に答えよ。

(1) 本文中の下線④の発見方法を，50 字以内で述べよ。

(2) 本文中の下線⑤の監視では，性能管理を効果的に行うために，どのような監視方法が必要か。50 字以内で述べよ。

(3) 本文中の下線⑥のチューニング内容を，25 字以内で述べよ。

設問 6　〔システムの切替え〕について，(1) ～ (3) に答えよ。

(1) 負荷テストで判明した状況を基に，負荷分散効果をより高められる負荷分散方式を，30 字以内で答えよ。

(2) データ移行テストの目的を，25 字以内で述べよ。

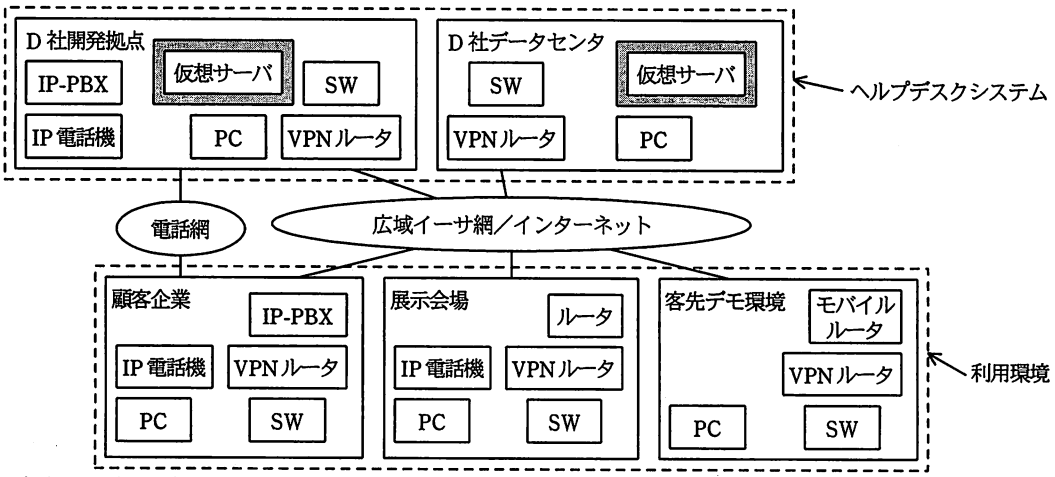
(3) システム切替スケジュールの立案において明確にすべき事項を，問題発生時の措置の面から二つ挙げ，それぞれ 40 字以内で述べよ。

問2　ヘルプデスクシステムの構築に関する次の記述を読んで，設問1～4に答えよ。

D 社は，システム構築ベンダである。顧客企業のシステム開発を受託する以外に，自社で所有するデータセンタを活用したサービス事業も展開している。最近，D 社のアプリケーション開発部門が，新しいヘルプデスクソフトを開発した。D 社は，このソフトウェアの販売に当たり，顧客企業にとって導入期間の短縮及び初期コストの低減が可能なサービス型で提供できないか，検討することになった。その担当者として，データセンタサービス部門のサーバ技術者である S 君とネットワーク技術者である N 君が指名された。

S 君は，“比較的小規模で，多くの顧客企業にサービスを提供する場合は，サーバの仮想化を行って，複数企業でサーバを共用すれば，投資の削減，サービス立上げの迅速化，運用効率の向上などが可能になる”と考えた。サーバの仮想化では，仮想化を行う仕組み（以下，仮想化機構という）を動作させるサーバのことを物理サーバという。仮想化機構によって，物理サーバ上に複数の OS 実行環境（以下，仮想サーバという）を作成することができる。

D 社の仮想サーバを採用したヘルプデスクシステム及び利用環境での機器の種類と設置場所を図1に示す。



広域イーサ網　：広域イーサネットサービス網
SW：レイヤ2 スイッチ又はレイヤ3 スイッチ
IP-PBX：VoIP 対応PBX
注　網掛けは物理サーバを示す。

図1　ヘルプデスクシステム及び利用環境での機器の種類と設置場所

D 社のヘルプデスクシステムは，電話システムとの連携機能である CTI（Computer Telephony Integration）機能も利用できるように作られているのが特長で，コールセンタでの顧客サポート業務に利用すると効果的である。その連携のための構成機器が，図 1 に示した IP-PBX と IP 電話機である。ヘルプデスクソフトと IP-PBX の制御を行う CTI 制御ソフトは，それぞれ仮想サーバ上で動作させる。

図 1 のヘルプデスクシステムで実現したいことは，次の 2 点である。

(1) D 社データセンタの仮想サーバでホスティングしたヘルプデスクシステムを，インターネットを介して顧客企業が利用できるようにする。

(2) マーケティング部門から要望が出されていた，展示会や客先でのデモができるようにする。

N 君と S 君は，仮想サーバを使ったシステムの技術的特徴を整理した上で，まず，サーバ仮想化の検討を行った。

〔サーバ仮想化の検討〕

物理サーバ上に，仮想化機構を動作させるための OS を必要としない，［ア］方式と呼ばれる方式は，仮想サーバの動作の安定性，仮想化を支援するハードウェアによる性能向上などを背景に普及しつつある。仮想化機構は，仮想サーバの実行制御，及び仮想サーバと外部のネットワークやストレージデバイスとの接続制御を行う。

仮想サーバを使用したシステムでは，1 台の物理サーバ内で，多数の仮想サーバを動作させることができる。N 君によると，“仮想化を行った場合は，仮想化を行わずに物理的に独立したサーバだけでシステムを構成する場合と比較すると，NIC などの外部接続用ハードウェアを複数の仮想サーバで共有するので，［イ］と［ウ］の面でより注意が必要である”ということであった。

仮想サーバと，ほかの仮想サーバや外部のスイッチとの接続は，ソフトウェアで実現する仮想的なスイッチ（以下，仮想 SW という）が行う。今回採用予定の仮想 SW はレイヤ 2 スイッチであり，その使用構成を，図 2 に示す。

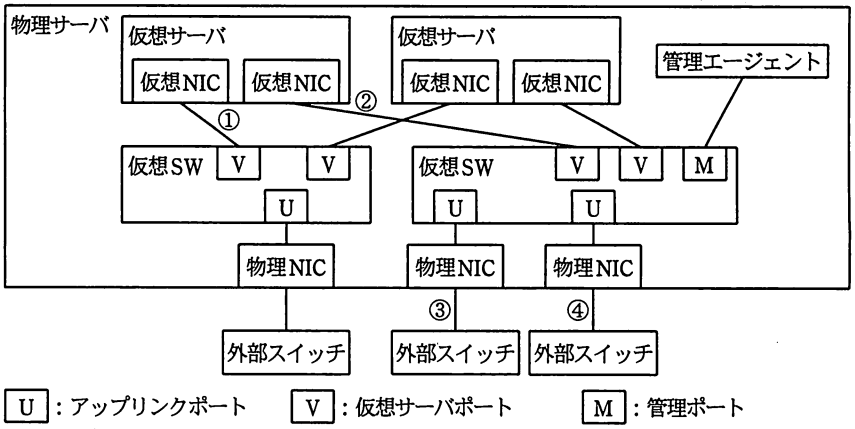


図2　仮想SWの使用構成

物理サーバのNICを物理NICという。仮想サーバのNICに相当する機能部分を仮想NICという。

仮想SWは用途別に3種類のポートを備えることができる。

仮想サーバポート（V）は，仮想サーバの仮想NICを接続するためのポートである。

アップリンクポート（U）は，物理NICと1対1で対応し，仮想SWを外部のネットワークに接続するためのポートである。（i）仮想SWにとって，物理NICは外部スイッチに接続するためのケーブルと見なせる。

管理ポート（M）は，仮想化機構と物理サーバの外部との通信を仲介する管理エージェントが，後述する管理システムと通信するために接続するポートである。

仮想化機構は仮想SWも管理しており，送信元仮想NICのMACアドレスを把握しているので，仮想SWは通過するパケットからMACアドレスを学習する動作を行わない仕様になっている。また，仮想SW間の接続はできないという仕様になっているが，仮想SWに接続する仮想サーバの接続数には物理的な制限がないので，構成上の制約とはならない。加えて，アップリンクポート間ではパケットを転送することはできない仕様になっているが，アップリンクポートを通過するパケットは基本的に仮想サーバ及び管理エージェントを送信元かあて先とするパケットなので，これも構成上の制約とはならない。

次は，検討を開始したS君とN君の会話である。

S君：物理サーバ上で多くの仮想サーバを動作させようとすると，物理サーバだけでシステムを構築する場合とは違った配慮が必要になりそうですね。

N 君：外部のネットワークに接続する部分についても，信頼性や通信帯域の確保についてよく考えておく必要があります。それには，外部接続のかなめである物理 NIC の使い方が重要です。このため（ii）NIC を論理的に束ねて一つに見せる［　エ　］技術を活用する必要があります。この技術によって冗長化と負荷分散が実現できます。

S 君：仮想 SW と外部スイッチとの接続の障害検知は，どのようにしているのですか。

N 君：スイッチ間の［　オ　］状態を監視することで，仮想 SW は障害を認識できます。

以上の検討から，N 君の提案した技術を使うことにし，次に仮想サーバの外部ネットワーク接続方式について検討することにした。

〔仮想サーバの外部ネットワーク接続方式の検討〕

論理的に束ねた複数の物理 NIC の，どの NIC を通して外部ネットワークとパケットを送受するかについての方式の検討が必要になった。

D 社で採用予定の仮想 SW では，外部接続に使用する物理 NIC を選択する方式（以下，物理 NIC 選択方式という）として，次の(1)～(4)の 4 種類がある。(2) と (3) の方式では，選択のために使用する値からハッシュ値を求め，そのハッシュ値を基に物理 NIC を選択する。

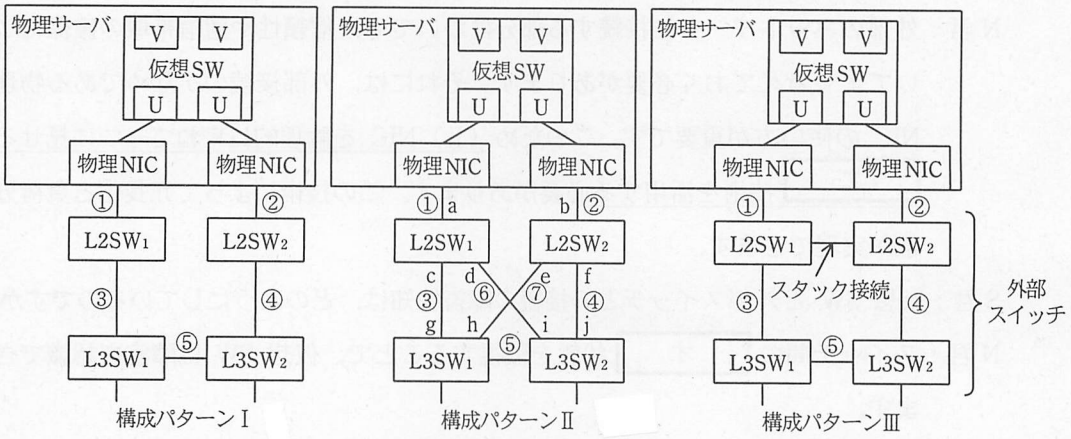
(1) 仮想 NIC が接続されている仮想 SW のポート ID を使用する（以下，ポート ID ベース方式という）。

(2) 仮想 NIC の MAC アドレスを使用する（以下，MAC ベース方式という）。

(3) パケットの送信元とあて先の IP アドレスを使用する（以下，IP ベース方式という）。

(4) 仮想 NIC ごとに使用する物理 NIC を明示的に指定する（以下，明示的選択方式という）。

N 君は，仮想 SW の物理 NIC 選択方式と外部スイッチの構成パターンについては，組み合わせる上で注意が必要と考え，S 君に説明するために，図 3 の外部スイッチの構成パターンを示した。



L2SW：レイヤ2 スイッチ　　L3SW：レイヤ3 スイッチ　　①～⑦ ：リンク番号

a ～j ：L2SW とL3SW のポート識別記号

図３　外部スイッチの構成パターン

構成パターンⅠは 2 台の L2SW を独立させる構成，構成パターンⅡは L2SW と L3SW 間のリンクを冗長化させる構成，構成パターンⅢはスタック接続によって 2 台の外部スイッチを 1 台に見せる構成である。図 3 中の③～⑦のリンクは，$L3SW_1$ と $L3SW_2$ のレイヤ 2 機能によって同一 VLAN となっている。また，$L3SW_1$ と $L3SW_2$ は，VRRP による冗長化構成を採っている。N 君は，表の物理 NIC 選択方式と外部スイッチの構成パターンとの組合せ検討表を S 君に示した。

表　物理 NIC 選択方式と外部スイッチの構成パターンとの組合せ検討表

物理 NIC 選択方式	外部スイッチの構成パターン		
	Ⅰ	Ⅱ	Ⅲ
ポート ID ベース方式			
MAC ベース方式			
IP ベース方式	×	×	
明示的選択方式	△	○	○

○：接続上，問題のない構成　　△：信頼性の観点から対策が必要な構成　　×：接続できない構成

注　網掛けは設問の都合上省略していることを示す。

（iii）構成パターンⅠで物理 NIC と外部スイッチとを接続した場合，冗長化ができていない部分があるので，外部スイッチへの対策が必要である。構成パターンⅡとⅢでは，（iv）適切な場所にループを回避するための設定が必要になる。構成パターンⅠ～Ⅲのうち，物理 NIC 選択方式によっては，組合せが不可能なものがある。IP ベース

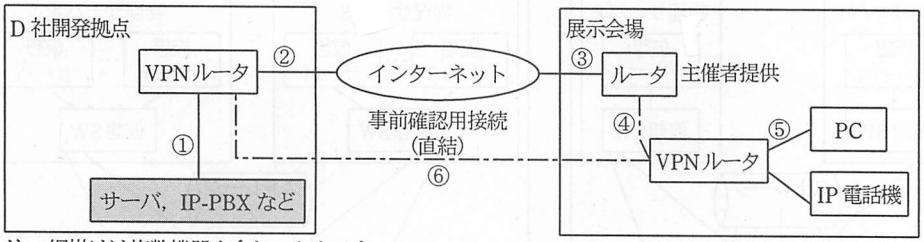
方式では，構成パターンⅠ及びⅡとは組み合わせられない。

N 君は図 3 と表を用いて，S 君に各組合せの優劣を説明し，IP ベース方式と構成パターンⅢの組合せを提案した。S 君は N 君の説明に納得し，提案に同意した。

〔デモシステムの構築〕

マーケティング部門は，各種広告媒体に加え，展示会，客先でのデモが有効と考え，コールセンタでの利用を想定したデモを見せたいと N 君に要請した。デモ内容について検討した結果，展示会場から，D 社開発拠点の IP-PBX を通して展示会場の IP 電話機に電話を掛けると，PC にヘルプデスクソフトの問合せ対応画面をポップアップ表示する連係動作を見せることになった。そこで N 君は，D 社開発拠点と展示会場をインターネット VPN で接続するネットワーク構成を検討した。

N 君が検討した D 社開発拠点と展示会場間のネットワーク接続構成を，図 4 に示す。展示会場側のインターネット接続については，主催者がルータまで準備し，出展者に対して動的なグローバル IP アドレスでの接続を提供する（図 4 中の④の部分）。N 君は，これらの要件から，インターネット VPN の構築には IPsec-VPN 方式のトンネルモードとアグレッシブモードを使わなければいけないと考えた。



注　網掛けは複数機器を含むことを示す。

図 4　D 社開発拠点と展示会場間のネットワーク接続構成

展示会場での準備には，開催前日の限られた時間しかないので，D 社内で事前確認を行うことにした。会場に機器を持ち込んでも，サーバ，IP-PBX，IP 電話機及び PC の IP アドレスなどの設定を変更しなくても済むように，事前確認用接続を行って動作確認を行う。会場に機器を持ち込むときは，ネットワーク接続用機器の設定変更だけで済むようにする。併せて，接続要件を示して主催者側に確認する。N 君は，実際の事前確認では，あらかじめ開発拠点内で，図 4 中の④の代わりに⑥の接続を使って確

認してから，展示会場に持ち込んだ。VPN ルータの設定は，多少変更が必要だったが，無事にデモを行うことができ，来場者にも好評であった。

続いて，客先でのデモ実現方式の検討に入った。まず，N 君はルータの代わりに，通信事業者が提供する，無線によるインターネット接続サービスに対応したモバイルルータを使えないか検討した。この場合，モバイルルータの配下の NAT 環境に VPN ルータを接続するので，帯域不足・遅延で通話は難しいものの，アプリケーションの画面を表示するには十分な帯域であり，ヘルプデスクシステムの特長を PR できることを確認した。

販売促進の結果，J 社から最初の受注をし，D 社データセンタにあるサービス提供用システム内に，J 社向けサービス提供用ヘルプデスクシステム（以下，J 社向けサービス提供用システムという）の構築に着手した。

〔J 社向けサービス提供用システムの構築〕

D 社が J 社にサービスを提供するための，J 社向けサービス提供用システムと開発システムを図 5 に示す。

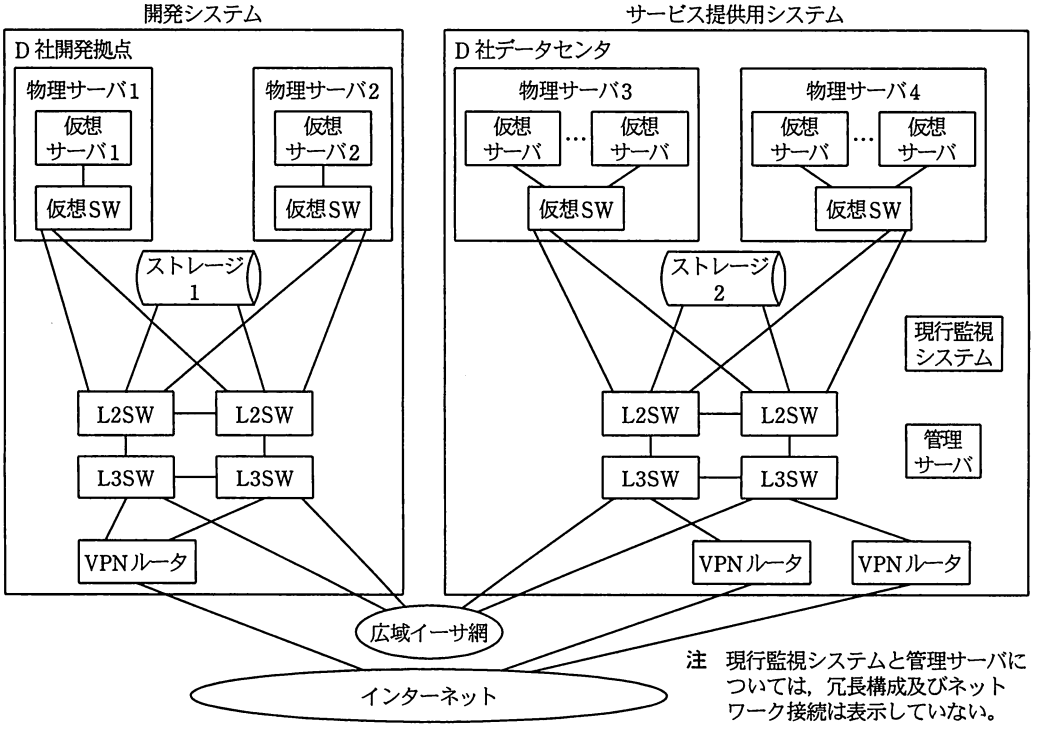


図 5　J 社向けサービス提供用システムと開発システム（抜粋）

開発システムは，J社向けサービス提供用システムとできるだけ同一の構成とするため，冗長化構成とした。

J社向けサービス提供用システムは，次の手順で構築することにした。

(1) D 社開発拠点で作成したヘルプデスクシステム用仮想サーバを基に，構成情報をカスタマイズできる形式に変換したもの（以下，テンプレートという）を作成し，ストレージ1に格納しておく。

(2) テンプレートを基に仮想サーバ1を作成し，J社向けのカスタマイズを加えて必要な機能を確認する。

(3) 確認を終えた J 社向け仮想サーバを，D 社データセンタの仮想環境に移動し，本番のサービスを提供する。

また，障害が発生したときに代替サーバに速やかに切り替えて運用できるようにするため，仮想サーバ 1 を動作させている物理サーバ 1 に障害が発生した場合の代替サーバは，物理サーバ 2 とする。同様に，データセンタの物理サーバ 3 に障害が発生した場合の代替サーバは，物理サーバ 4 とする。このとき，速やかな自動切替えを実現するために必要なストレージ 1 とストレージ 2 は，コストパフォーマンスの良い iSCSI（internet SCSI）タイプを使用することにした。

J社では社員の負担を軽減するために，導入システムの運用を極力，外部に委託したいと考えていた。そこで，D 社ではヘルプデスクシステムの監視に当たって，D 社データセンタ内の現行監視システムの監視対象に，今回新規に導入する仮想サーバを追加することにした。仮想サーバ上で動作するアプリケーションの状態監視については，これまで D 社が導入してきた手法と同様に，各仮想サーバの OS 上に監視エージェントを導入し，必要なプロセスの動作確認，イベントログの監視及びソフトウェアリソースの状態把握を行うことにした。

加えて，S 君は，仮想サーバと仮想 SW の接続設定，ポートの属性設定，動作モード設定などの構成制御のため，ベンダが提供する管理システムを導入することにした。管理システムは，図 5 中の管理サーバ上で動作し，図 2 に示した管理エージェントに接続して，各種管理を行う。この管理システムは，システムの構成制御に不可欠なものであり，可用性の確保が重要であった。

そこで N 君は，（v）管理システムの可用性に配慮した設計を行い，ヘルプデスクシステム用の監視機能を実現した。さらに，物理サーバに障害が発生したときに，代替の別の物理サーバ上の仮想サーバに処理を移行する際に，ネットワーク情報を継承させる必要があることをS君にアドバイスした。

このようにして，D社は，J社向けのサービスを，開始できるようになった。今後は，新たな顧客企業のシステムを受注した場合に備え，仮想サーバを作成する際の基になるテンプレートを，D 社データセンタに用意しておいて，データセンタで短時間に顧客用仮想サーバが生成できるようにするなど，J社向けヘルプデスクシステム構築の実績を生かしてデータセンタの提供機能を拡充し，効率よくシステム展開できるように準備を整えた。

設問1　〔サーバ仮想化の検討〕について，(1)～(3)に答えよ。

(1) 本文中の［　ア　］～［　オ　］に入れる適切な字句を答えよ。

(2) 本文中の下線（i）について，物理 NIC から外部スイッチに送信されるパケットの送信元 MAC アドレスは，どこのアドレスとなっているか。10 字以内で答えよ。

(3) 本文中の下線（ii）について，この技術の適用部分を，図 2 中の番号で，すべて答えよ。

設問2　〔仮想サーバの外部ネットワーク接続方式の検討〕について，(1)～(5)に答えよ。

(1) 4 種類の物理 NIC 選択方式のうち，動作させる仮想サーバが 1 台でも物理 NIC の負荷分散効果が得られる方式はどれか。方式名を答えよ。また，その理由を 40 字以内で述べよ。

(2) 本文中の下線（iii）について，冗長化できていない部分を図 3 中のリンク番号で，すべて答えよ。また，そのための対策として，外部スイッチにもたせるべき機能を，45 字以内で述べよ。

(3) 本文中の下線（iv）について，必要な設定を，15 字以内で答えよ。また，構成パターンⅡでループを回避する設定が不要なポートを，図 3 中のポート識別記号 a～j で，すべて答えよ。

(4) IP ベース方式では，構成パターンⅠ及びⅡとは組み合わせられない理由を 65

字以内で述べよ。

(5) IP ベース方式で構成パターンⅢを組み合わせる場合，どの外部スイッチにどのような設定が必要か。45 字以内で述べよ。

設問 3 〔デモシステムの構築〕について，(1) ～ (4) に答えよ。

(1) N 君が，D 社開発拠点と展示会場間のインターネット VPN の構築に，IPsec-VPN 方式のトンネルモードとアグレッシブモードを使用することにした理由を，それぞれ 30 字以内で述べよ。

(2) 主催者が準備する展示会場側ルータと持ち込む VPN ルータの接続に関し，N 君は，アドレス上の観点でルータのどのポートに，どのような設定で接続することを想定したと考えられるか。50 字以内で述べよ。

(3) 事前確認のための接続で，D 社開発拠点の VPN ルータの配下に接続する展示会場用の VPN ルータには，どのような設定が必要か。55 字以内で述べよ。

(4) モバイルルータを使用した構成では，VPN 接続のために展示会場で使用した VPN ルータには必要でない設定が，モバイルルータには必要であった。その設定を 15 字以内で答えよ。

設問 4 〔J 社向けサービス提供用システムの構築〕について，(1) ～ (3)に答えよ。

(1) 物理サーバに障害が発生したときに，速やかに自動切替えを行うためのストレージ 1 及び 2 の使い方を，35 字以内で述べよ。

(2) ストレージに iSCSI を利用することで，ネットワーク環境から考えられる利点を，35 字以内で述べよ。

(3) 本文中の下線（ｖ）について，N 君のネットワーク設計上の具体的な対策を，35 字以内で述べよ。

〔メ モ 用 紙〕

〔 メ モ 用 紙 〕

7. 途中で退室する場合には，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	15:10 ～ 16:20

8. **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。
9. 問題冊子の余白などは，適宜利用して構いません。
10. 試験時間中，机上に置けるもの及び使用できるものは，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，B 又は HB の黒鉛筆又はシャープペンシル，鉛筆削り，消しゴム，定規，時計（アラームなど時計以外の機能は使用不可），ハンカチ，ティッシュ
これら以外は机上に置けません。使用もできません。
11. 試験終了後，この問題冊子は持ち帰ることができます。
12. 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。
13. 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。

午

お知らせ

1. システムの構築や試験会場の確保などの諸準備が整えば，平成 23 年 11 月から IT パスポート試験において CBT※方式による試験を実施する予定です。
2. CBT 方式による試験の実施に伴い，現行の筆記による試験は，廃止する予定です。
3. 詳細が決定しましたら，ホームページなどでお知らせします。

※CBT（Computer Based Testing）：コンピュータを使用して実施する試験。