

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。

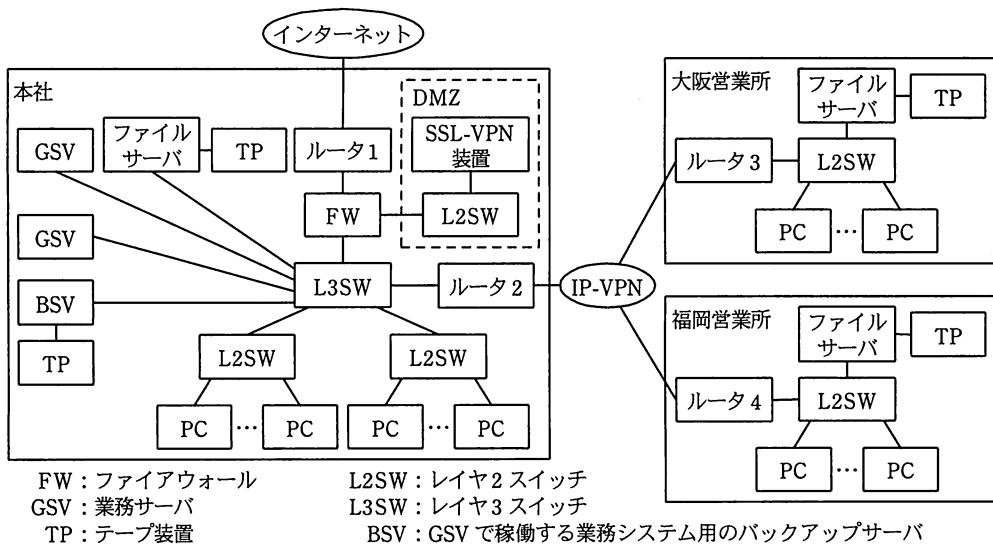


図1 現在のネットワークシステム構成（抜粋）

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、商品マスターを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]

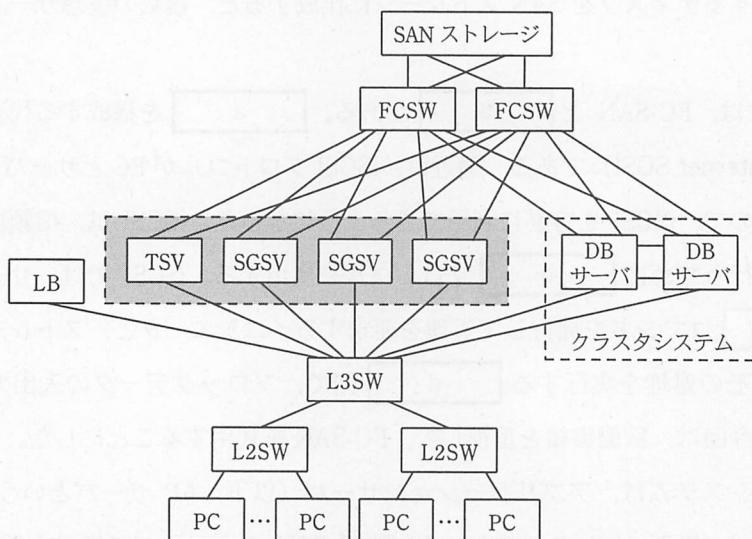
サーバの仮想化を実現させる仕組み（以下、仮想化機構という）を動作させるサーバのことを、物理サーバという。仮想化機構によって、物理サーバ上に作成されるサーバ機能を、仮想サーバという。仮想サーバは、物理サーバ上に複数作成できる。仮想サーバが使用するディスクは、物理サーバのローカルディスクと SAN に接続されたディスク装置（以下、SAN ストレージという）に作成することができる。仮想サーバが使用するディスクを SAN ストレージに作成すると、複数の仮想サーバで共用できる。

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 を経由することにする。

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するために、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、データ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、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。

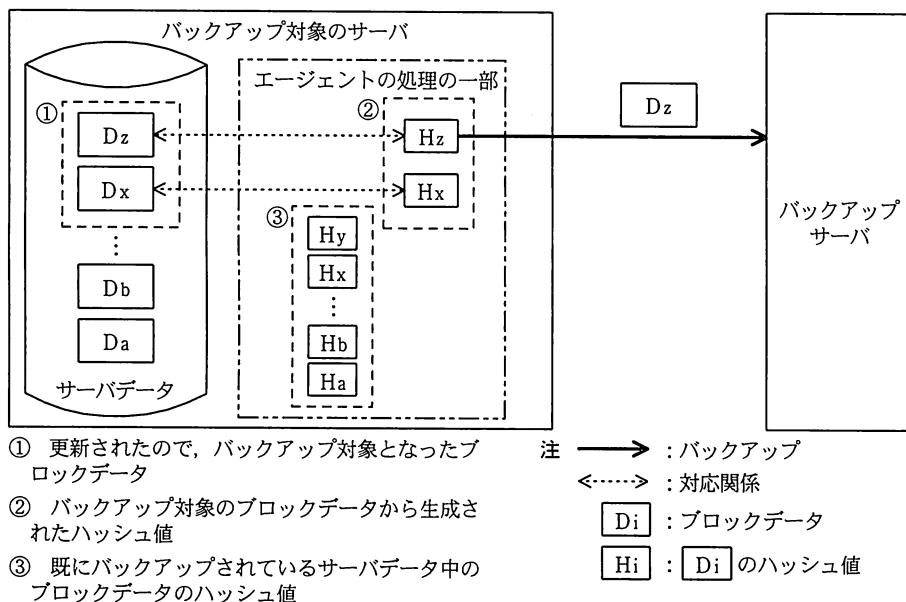


図3 バックアップ対象のサーバでの重複除外処理の概要

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 H_x と H_z のうち、 H_x は、③のハッシュ値の中に存在するので、 D_x はバックアップされない。 H_z は、③のハッシュ値の中に存在しないので、 D_z 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 H_x と H_z 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、 D_x と D_z が、既

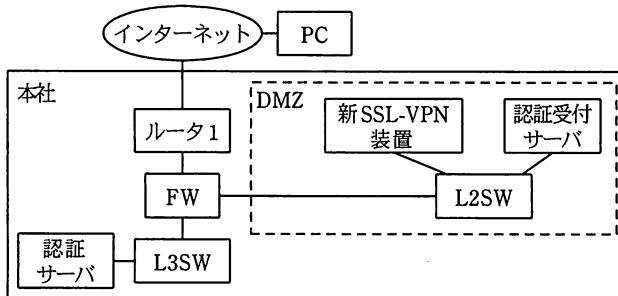
にバックアップされたブロックデータと重複しているかどうか判断される。

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。

(I) 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。

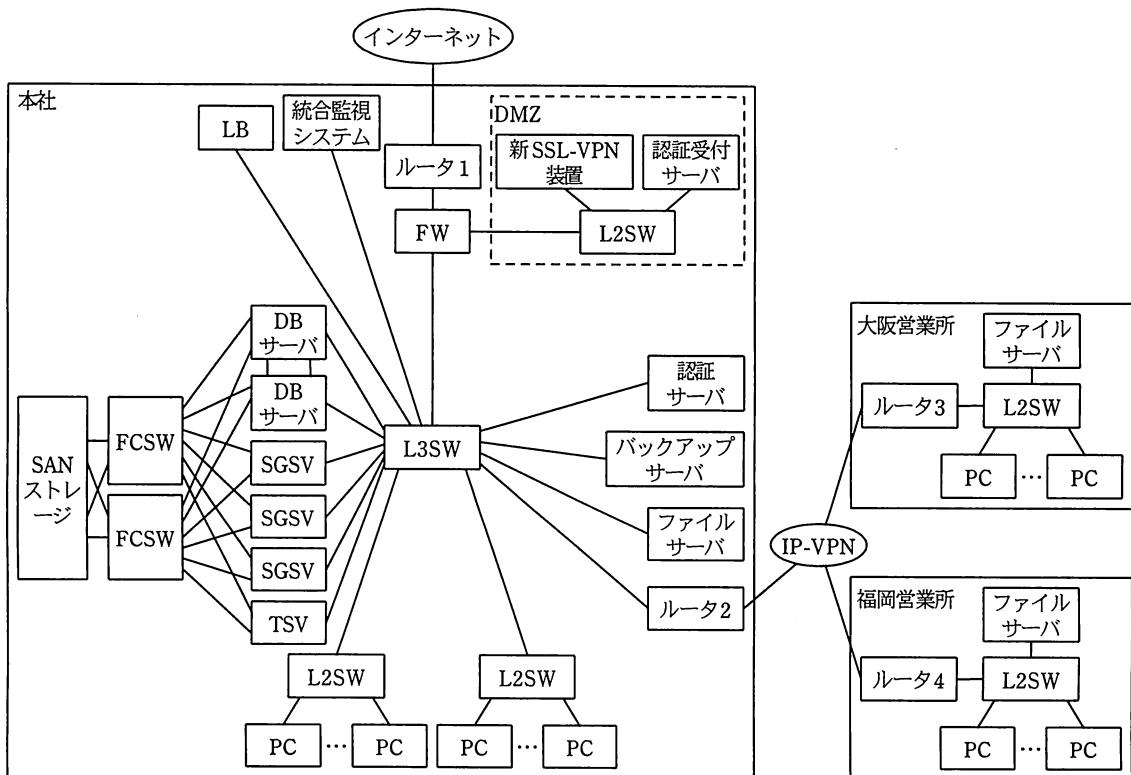


図 5 新業務システム構築後のネットワークシステム構成（抜粋）

[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

測定項目	単位 %					
	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ー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

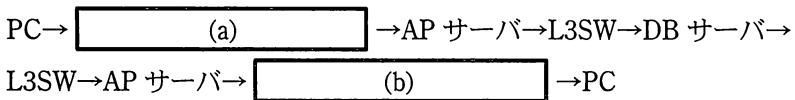
システムの切替えは、月末の金曜日から 3 日間かけて実施した。金曜日の業務終了後に、月末の締め処理を行い、その後にデータ移行作業を開始した。移行データの確認後、月曜日の業務開始のための準備作業を行い、システム切替作業を終了した。データ移行作業の途中で問題が幾つか発生したが、必要な対応措置をとり、無事に新業務システムを稼働させることができた。

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】



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。