

問2 ヘルプデスクシステム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ーである。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、仮想サーバといふ）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。

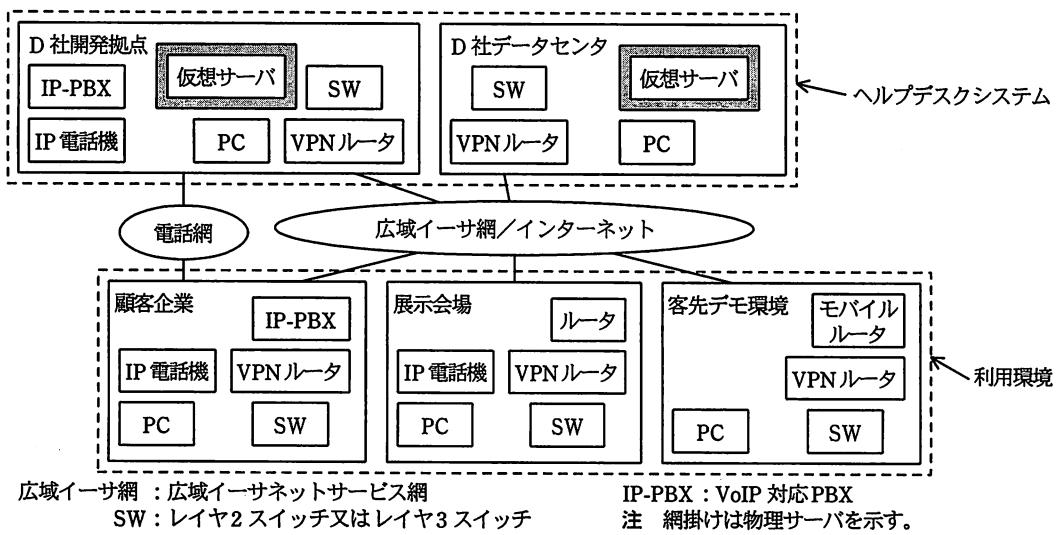


図1 ヘルプデスクシステム及び利用環境での機器の種類と設置場所

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。

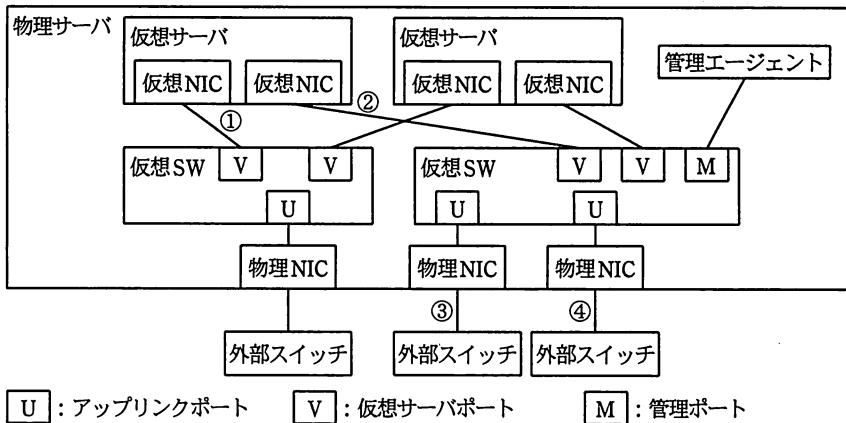


図2 仮想 SW の使用構成

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
工 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。

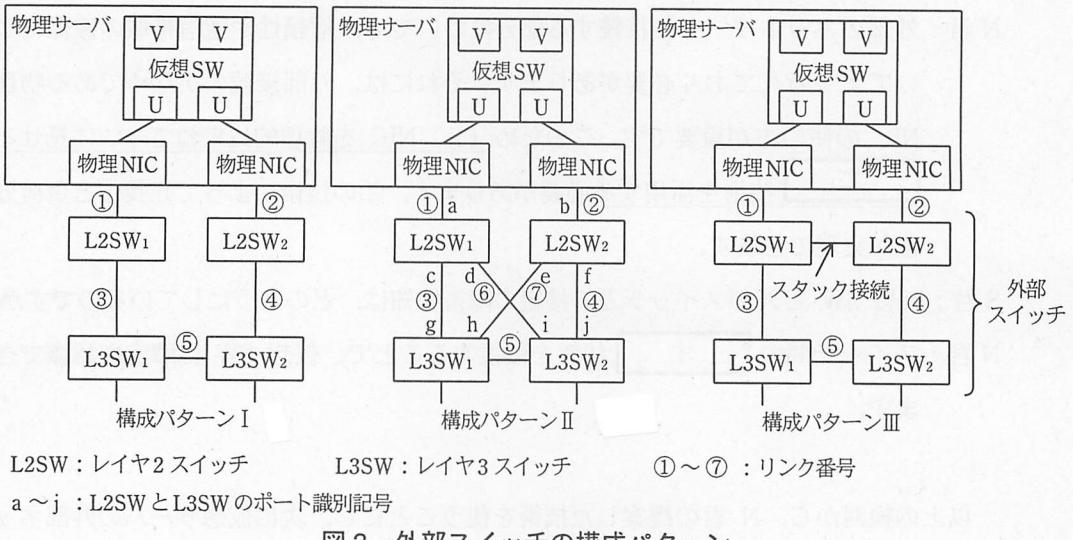


図3 外部スイッチの構成パターン

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、L3SW₁とL3SW₂のレイヤ2機能によって同一VLANとなっている。また、L3SW₁とL3SW₂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。

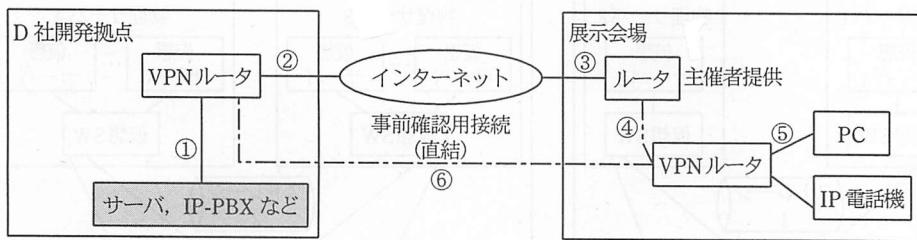


図4 D社開発拠点と展示会場間のネットワーク接続構成

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なる。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。

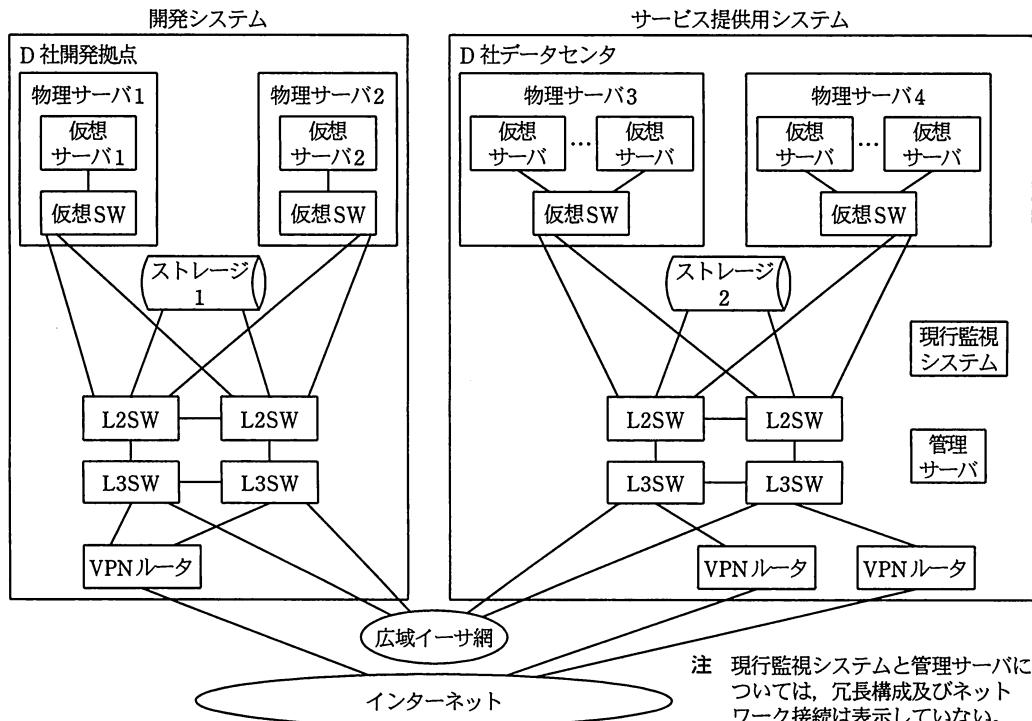


図 5 J 社向けサービス提供用システムと開発システム（抜粋）

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。