

平成 13 年度 秋期 テクニカルエンジニア（ネットワーク） 午後 問題

問 1 IP-VPN サービスを用いたネットワークの再構築に関する次の記述を読んで、設問 1 ～ 5 に答えよ。

A 社は、主に、法人向けにカスタマイズしたパソコン(以下、PC という)を販売している。営業範囲が比較的広いので、各地域を担当する地域営業所と、これらを統括する営業支社(以下、支社という)を置いている。法人顧客は、自社の営業員やデザイナー向けに、それぞれの業務に最適な仕様の PC を注文してくる。受注した営業員は、法人顧客の要求したカスタマイズ仕様を工場へ送る。工場では、そのカスタマイズ仕様に従った PC を組み立てる。組み立てられた PC は、物流センターへ送られ、注文した法人顧客が指定した納入日に配送される。

〔これまでのシステムの概要〕

A 社は、支社や工場などに分散配置されていた各サーバを使用して、個別の業務アプリケーションプログラム(以下、分散業務 AP という)を稼働させていた。各サーバの分散業務 AP は、それぞれ専用のクライアント側アプリケーションプログラム(以下、端末 AP という)を使い、PC から TCP/IP を用いて利用されていた。

支社の分散業務 AP はオーダエントリや営業活動報告に利用され、工場の分散業務 AP は生産管理に利用されていた。また、営業員が使用する営業活動報告用の端末 AP は、FTP を用いて支社のサーバで稼働する営業活動報告用の分散業務 AP にアクセスしていた。

〔現在のシステムの開発背景〕

A 社は、1 年前から本社の企画部が中心となり、本社に設置した Web サーバを用いた無店舗販売システムを利用して、PC の個人向け販売も始めた。この個人向け販売の PC も、個人顧客の要望に沿ってカスタマイズして販売する機会が多かった。

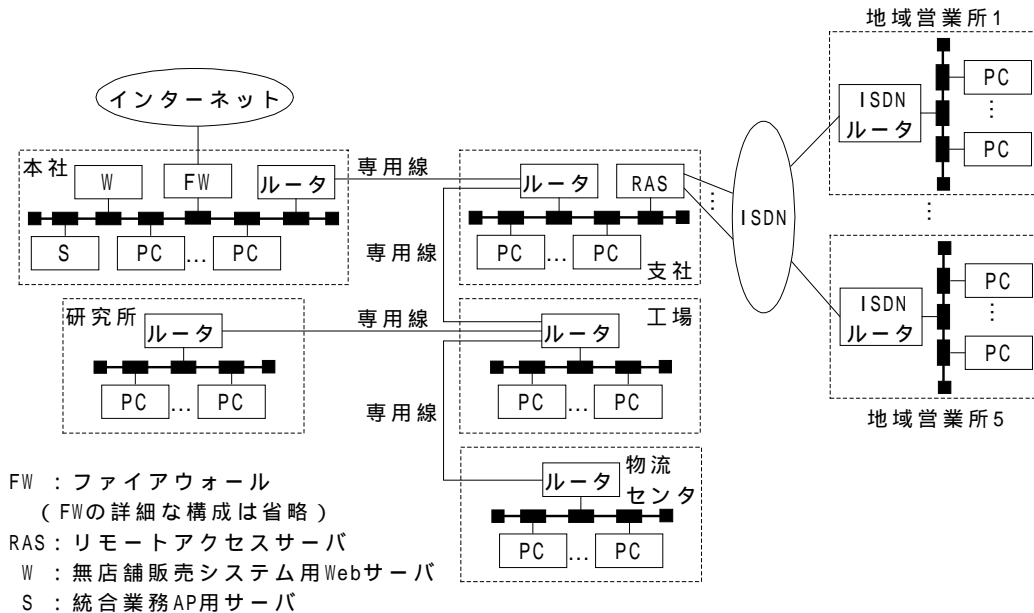
個人向け販売では、注文してから手元に届くまでの状況を顧客が随時参照可能とするサービス(以下、トラッキングサービスという)が求められていた。また、法人顧客からの納入問合せなどへ迅速に対応するために、営業員からもこのサービスが求められていた。

分散業務 AP は、本社の情報システム部が開発したが、機能の追加を繰り返してきたので、トラブルが多かった。トラブル対応は、支社や工場などの保守要員が行うことになっていたが、対応できない場合が多く、情報システム部が対応してきた。このため、情報システム部の開発業務にも支障が出ていた。

〔現在のシステムの概要〕

A 社は、半年前に、それまでの分散業務 AP と分散配置されていたサーバを廃止し、新しく本社に設置したサーバで、新規開発した業務アプリケーションプログラム(以下、統合業務 AP という)を稼働させた。統合業務 AP は、無店舗販売システムとの連携機能、及びトラッキングサービスの機能を含め、分散業務 AP の業務をすべて実現しており、PC から TCP/IP を用いて利用される。

現在のシステムでは、迅速な開発を目指し、これまでのネットワークを継続して使用することにした。現在のシステムのネットワーク（以下、現ネットワークという）構成を図 1 に示す。



注 点線内は、拠点を示す。

図 1 現ネットワークの構成

地域営業所では営業員の希望もあり、営業活動報告は、従来の営業活動報告用の端末 AP を用いて統合業務 AP を利用している。このほかの端末 AP は、統合業務 AP の稼働に合わせて廃止し、PC のブラウザを用いて統合業務 AP を利用することにした。営業員は、このブラウザを用いて、受注した PC が顧客へ届くまでのすべての状況を常に把握できる。

〔現ネットワークの再構築〕

A 社の業績は、統合業務 AP を利用して順調に伸びた。これに伴い、仕様書や設計書の参照などを伴う業務量が増大し、特に工場と本社間のトラフィックが急激に増加した。このため、複数の拠点で応答時間が長くなり、業務に支障が出てきた。しかし、本社と支社間の通信帯域は十分であり、ここに問題はなかった。

情報システム部では、トラフィックの増加や将来の拠点追加に対する拡張性、及び信頼性確保のために、現ネットワークの再構築を検討することになった。

情報システム部では T 君が中心となり、再構築するネットワーク(以下、新ネットワークという)の要求条件を取りまとめて通信サービス事業者へ提示した。その結果、MPLS(Multi-Protocol Label Switching)による IP-VPN サービスを提案してきた通信サービス事業者の技術者である K 氏と、新ネットワークに対する IP-VPN サービスの適用に関して検討することになった。

K 氏が提案する、IP-VPN サービスを用いた新ネットワークの構成を図 2 に示す。

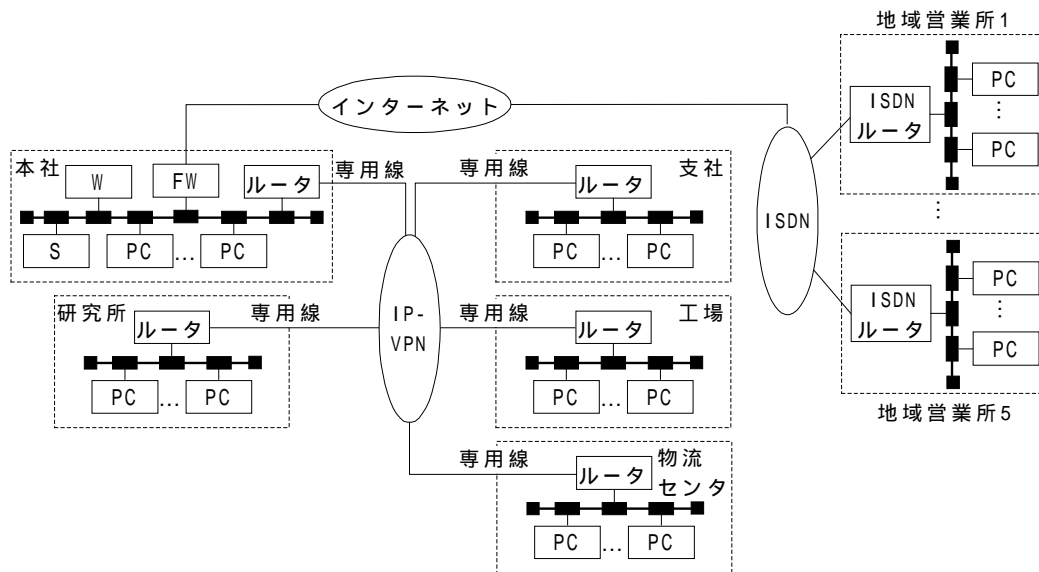


図 2 新ネットワークの構成

T 君：まず，IP-VPN のパケット転送方法について教えてください。

K 氏：図 2 の専用線で接続されたルータをカスタマイズルータ(以下，CER という)といいます。

IP-VPN サービスは，通信サービス事業者のプロパイダエッジルータ(以下，PER という)と，顧客の CER との間を必要な帯域の専用線で接続する形態で提供されます。この専用線を“アクセス回線”といいます。CER から PER へ届いた IP パケットには，PER において，あて先に応じた **a** が付与されます。送信元 PER とあて先 PER の間の IP-VPN 内部では，**a** に基づいてルーティングを行います。転送先の **b** では **a** を外し，通常の **c** に戻して **d** へ転送します。

T 君：IP-VPN 内部では，IP パケットと異なる形式のパケットが転送されるのですか。

K 氏：はい。そうです。

T 君：IP-VPN サービスを利用すれば，セキュリティも確保できるのですか。

K 氏：もちろんです。送信元 PER ではどこの顧客からの IP パケットかの判別が可能であり，ほかの顧客の CER へ届けることはありません。つまり，送信元 PER は送信元の顧客を識別し，届いた IP パケットのあて先 IP アドレスと合わせて，あて先の PER を決定します。送信元の顧客が異なれば，送信元 PER に顧客から届いた IP パケットのあて先 IP アドレスが等しくても，その IP パケットは，**e** CER へ転送されます。これによって，従来の専用線を使った通信と同等のセキュリティが確保されるのです。

T 君：提案資料にある，今後の拡張が容易だという点についても教えてください。

K 氏：例えば，物流センターを新設する場合を考えます。現ネットワークでは，新しい物流センターは専用線を利用して工場と接続されることとなります。この場合，**f** と **g** 間，及び **g** と **h** 間の既存専用線の帯域も検討する必要があります。これに対して，新ネットワークでは，**f** と IP-VPN 間の既存アクセス回線の帯域を検討する程度で，拠点追加による既存ネットワークへの影響を **i** できる

ので、拡張が容易になります。

T 君は、通信のセキュリティが確保され、費用が少なくてすむ IP-VPN サービスを利用した新ネットワークの構築を前提として、更に検討を進めることにした。

〔地域営業所と本社の接続〕

K 氏の提案は、インターネットを介して、地域営業所と本社を接続する形態であった。T 君は、その接続方法に関して K 氏と検討した。

K 氏：地域営業所との接続は、情報システム部のある本社とします。さらに、本社と各地域営業所は離れているので、現ネットワークの ISDN を用いた接続からインターネットを利用した接続にしました。

T 君：地域営業所から本社へ接続するのは妥当だと思いますが、ほかの通信サービス事業者の提案では地域営業所も IP-VPN サービスを利用しています。なぜ、御社の提案では IP-VPN サービスを利用しないのですか。

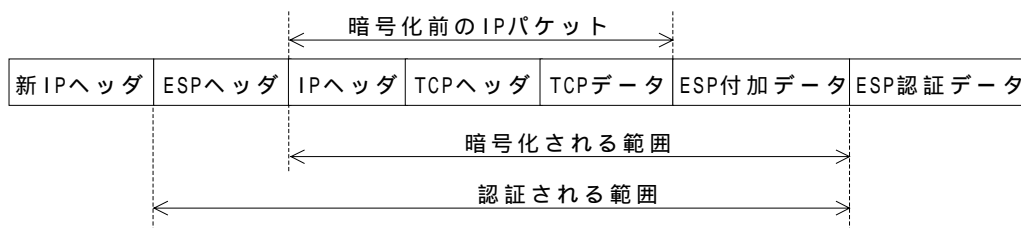
K 氏：地域営業所からのネットワークの利用頻度は少ないと考えられます。したがって、地域営業所とのアクセス回線に専用線を適用するのは、コスト的に見合わないので IP-VPN サービスは不適切だと考えました。

T 君：アクセス回線に専用線以外は適用できないのですか。

K 氏：はい、現時点では専用線しか適用できません。

T 君：IP-VPN は、セキュリティが確保されていますが、インターネットを介した通信の場合、セキュリティが非常に心配です。何か対策はありますか。

K 氏：地域営業所と本社間のインターネットを介した通信は、IP 層でセキュリティを確保する手段の一つである IPsec を用いて、安全に IP パケットを転送します。IPsec は、送信元で IP パケットを暗号化して、受信先で暗号化された IP パケットを復号します。今回提案する IPsec パケットの概要を図 3 に示します。



ESP : Encapsulating Security Payload

図 3 A 社で利用する IPsec パケットの概要

K 氏：暗号化前の IP パケット及び新たに追加される ESP 付加データは、暗号化されます。TCP ヘッダとは異なる ESP ヘッダと暗号化されたデータが改ざん検出の対象です。

T 君：IPsec を用いた場合、暗号化処理のオーバーヘッドやインターネットの輻輳などによる通信スループットの低下は、問題ないでしょうか。

K 氏：地域営業所から行う主な業務は、営業活動報告です。営業活動報告用の端末 AP は、FTP を

用いて統合業務 AP から報告用のテンプレートをダウンロードし、営業員が作成した報告データを統合業務 AP へ送ります。FTP で転送されるデータは少ないので、大きな問題にはならないと考えております。

T 君は、IPsec と FTP を使ってインターネットを介したファイル転送試験を行うことにした。

〔地域営業所と本社の接続試験〕

T 君は、まず最初に、各地域営業所と本社間のインターネットを介した FTP による接続試験を行うための準備を進めた。試験のために用意した FTP サーバは、IPsec 機能を有しているが、トラブル解析に備えて IPsec 機能を用いないことにした。

A 社は、社内でプライベート IP アドレスを使用している。T 君は、インターネット接続のために、現ネットワークで利用している ISDN ルータに、インターネット接続を考慮したパケットフィルタを設定した。接続試験で用いた ISDN ルータにおけるパケットフィルタの内容の抜粋を表に示す。

表 接続試験で用いた ISDN ルータのパケットフィルタの内容(抜粋)

方向	送信元 IP アドレス	あて先 IP アドレス	SYN ビット	ACK ビット	送信元 ポート番号	あて先 ポート番号	通信動作
外向き	内部	外部	オン	オフ	1,024 以上	25	接続
外向き	内部	外部	オン	オフ	1,024 以上	110	接続
内向き	外部	内部	オン	オフ	任意	任意	切断
内向き	外部	内部	オフ	オン	80	1,024 以上	接続
外向き	内部	内部	オン	オフ	任意	任意	切断

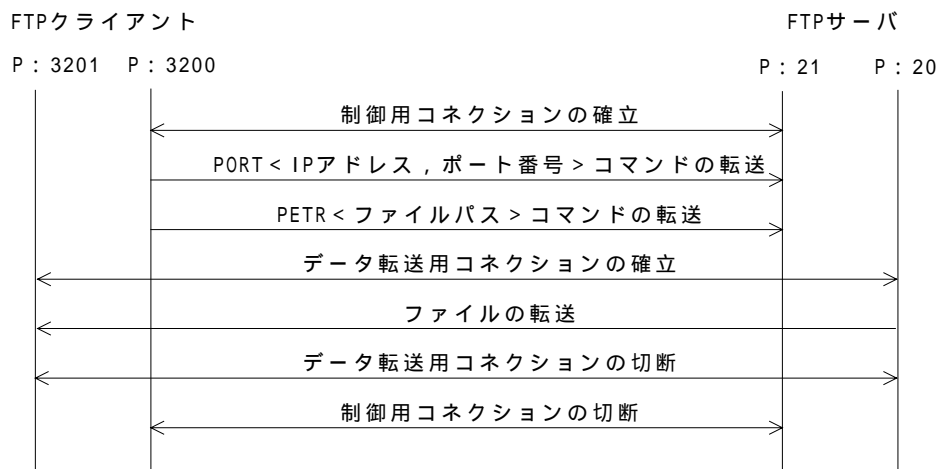
また、試験で用いる ISDN ルータごとに一つのグローバル IP アドレスを与えることによって、プライベート IP アドレスを有する複数の PC からインターネットが利用できる。

T 君は、ある地域営業所からブラウザを使って、FW の DMZ に設置した FTP サーバからファイルをダウンロードした。次に、営業活動報告用の端末 AP を利用して、同様にファイルのダウンロードを試みた。しかし、営業活動報告用の端末 AP では、この FTP サーバからファイルのダウンロードができなかった。T 君は、今回の試験結果を K 氏に伝えて、原因究明と対策を検討することにした。

T 君：ある地域営業所においてブラウザを用いた場合は、ファイルのダウンロードに成功しました。

これに対して、営業活動報告用の端末 AP を用いると失敗してしまいます。ここに FW の DMZ で取得した、FTP サーバと FTP クライアント間のパケットモニタリングデータがあります。このデータを見ると、地域営業所側から TCP コネクションを切断していますが、この原因が分かりません。

K 氏：このモニタリング結果から判断すると、TCP コネクションを切断しているのは、ISDN ルータです。FTP アクティブモードの概要を図 4 に示して説明します。



注 Pは、ポート番号を示す。

図4 FTP アクティブモードの概要

K氏：まず，FTP クライアント側から制御用コネクションの確立が要求されます。制御用コネクションを使って PORT コマンドで，FTP クライアントの IP アドレスとポート番号を FTP サーバへ通知します。これらはデータ転送用コネクションの確立に使います。データ転送用コネクションの確立は，j 側から要求されます。営業活動報告用の端末 AP は，パケットモニタリングデータから判断して，FTP アクティブモードを利用しています。

T君：営業活動報告用の端末 AP が FTP アクティブモードを利用していると，なぜファイル転送ができないのでしょうか。

K氏：ISDN ルータのパケットフィルタリング設定が FTP アクティブモードに対応していないためです。しかし，現状の ISDN ルータを FTP アクティブモードに対応させると，地域営業所のセキュリティが低下する可能性があります。

T君：試験環境では，現ネットワークから FTP クライアントを切り離しているので，自社のセキュリティには問題ないと思います。ISDN ルータの設定を変更して接続試験を行います。

T君は，営業活動報告用の端末 AP を用いたファイルのダウンロードが，IPsec 機能を利用しない環境で行えることを確認した。

K氏の提案によれば，既存の ISDN ルータを IPsec 機能が付いた機種へ変更することになっている。T君は，この IPsec 機能が付いた ISDN ルータを用いて，IPsec 機能を使った環境で，営業活動報告用の端末 AP を用いたファイルのダウンロードが行えることを確認した。また，IPsec 機能を追加した場合も通信スループットは低下しないことを確認した。

〔IPsec の検討〕

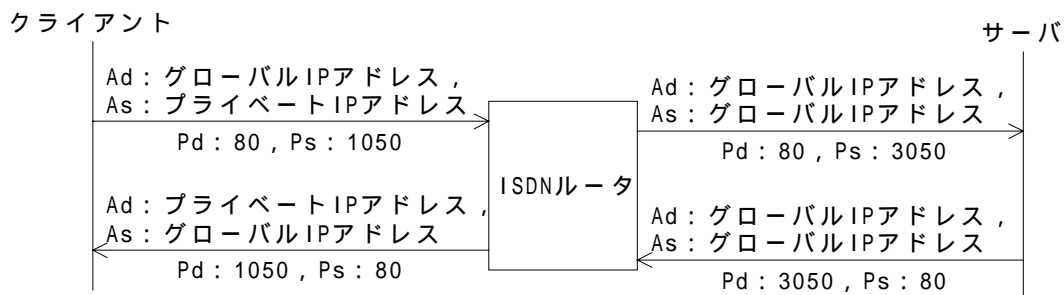
T君は，コスト削減のため，既存の ISDN ルータを IPsec 機能が付いた機種へ変更するのではなく，地域営業所に設置した PC のソフトウェア処理による IPsec 機能の利用について提案し，その実現の可能性を K氏と検討した。

T 君：ISDN ルータを IPsec 機能付きに変更する予定ですが，最近の PC は，ソフトウェア処理による IPsec 機能をもっていますので，こちらの適用も検討したいと思います。

K 氏：ポイントは，社内で利用しているプライベート IP アドレスから地域営業所におけるグローバル IP アドレスへの変換方法です。インターネットヘダイアルアップ接続した場合に割り振られるグローバル IP アドレスは一つです。

T 君：IP アドレスの変換機能は，ISDN ルータが有していますね。

K 氏：はい，そのとおりです。その IP アドレス変換方式は，IP マスカレードと呼ばれるものです。機能概要を図 5 に示します。



注 Adはあて先IPアドレスを示し，Asは送信元IPアドレスを示す。
Pdはあて先ポート番号を示し，Psは送信元ポート番号を示す。

図 5 IP マスカレードの機能概要

K 氏：IP マスカレードは，クライアントから届いた IP パケットのプライベート IP アドレスを，ISDN ルータのグローバル IP アドレスへ変換します。このとき，送信元ポート番号も ISDN ルータが選択した番号に変換されます。サーバ側からは，変換されたグローバル IP アドレスとポート番号あてに IP パケットが送信されます。ISDN ルータは，サーバ側から受信した IP パケットのあて先 IP アドレスを元のプライベート IP アドレスに変換し，ポート番号も元に戻します。このため，IP マスカレード機能と IPsec 機能を適用する順序が問題となり，PC の IPsec 機能を利用することは，困難だと思えます。

T 君：分かりました。今回は，IPsec 機能付き ISDN ルータを利用することにします。

A 社は，これまでの検討結果に基づいて，新ネットワークへ移行することにし，具体的な移行計画の作成を進めた。

設問 1 新ネットワークで利用する IP-VPN サービスに関する次の問いに答えよ。

- (1) 本文中の ~ に入れる適切な字句を答えよ。
- (2) アクセス回線に専用線を用いている理由を，PER でのセキュリティの観点から 30 字以内で述べよ。

設問 2 現ネットワークと新ネットワークの拡張性に関する次の問いに答えよ。

- (1) 本文中の ~ に入れる拠点名を答えよ。
- (2) 本文中の に入れる適切な字句を答えよ。

設問 3 統合業務 AP 用のサーバと現ネットワークに関する次の問いに答えよ。

- (1) 分散業務 AP 用の各サーバを廃止し、統合業務 AP 用のサーバを本社に設置することによって解消する問題点を、20 字以内で述べよ。
- (2) 工場と本社間のトラフィック増加が、ほかの拠点に影響を与えた理由を 35 字以内で述べよ。ただし、影響があった拠点名を含めてネットワーク構成の観点から述べること。

設問 4 地域営業所と本社の接続試験に関する次の問いに答えよ。

- (1) 本文中の に入れる適切な字句を答えよ。
- (2) 図 4 における の PORT コマンドで通知されるポート番号を答えよ。
- (3) ISDN ルータは、IP ヘッダのほかにも IP アドレスの変換を行う。何をどのように変換するのか、具体的に 70 字以内で述べよ。
- (4) ISDN ルータが表の設定に従って通信を切断した理由を 40 字以内で述べよ。
- (5) パケットモニタリングデータにおいて、IPsec 機能を利用しなかったために、トラブル解析に役立った情報を 15 字以内で述べよ。

設問 5 新ネットワークに関する次の問いに答えよ。

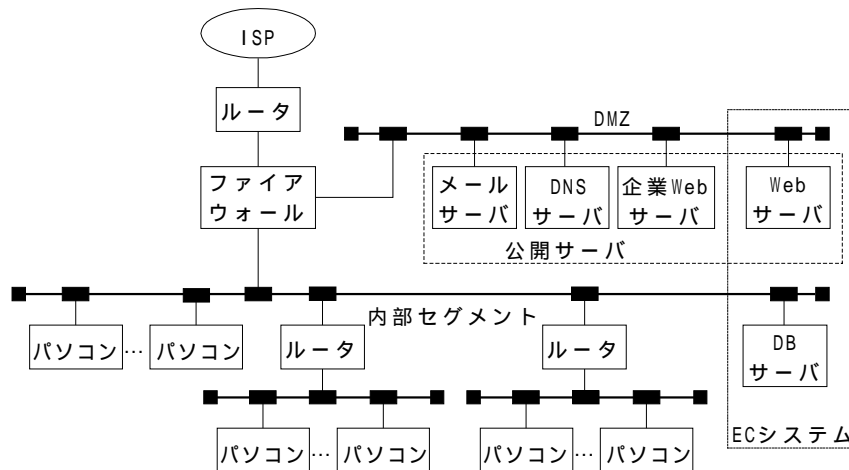
- (1) 現ネットワークでは、地域営業所を除いた通信に関して信頼性に問題があるが、新ネットワークへ移行すれば解消される。ネットワーク構成の観点から、この解消される問題を 50 字以内で述べよ。
- (2) T 君の提案に従って、地域営業所の PC で IPsec 機能を実現すると、現在の ISDN ルータ経由では本社と通信ができない。その理由を 60 字以内で述べよ。
- (3) 現ネットワークから新ネットワークへの移行において、IP-VPN サービスを利用することによって得られる、IP アドレス計画における特長とその理由を 70 字以内で具体的に述べよ。

問 2 インターネット接続システムの安全対策に関する次の記述を読んで、設問 1 ～ 5 に答えよ。

Y 社は、東京に本社を置き全国に 10 か所の営業所をもつ、大手のオフィス用品販売会社である。Y 社では、インターネットの急速な普及に合わせ、1 年前に Web サーバによる契約企業向けのインターネット通信販売(以下、ネット通販という)システムを試験稼働させた。ネット通販での売上は急激な増加を示し、現在では月間 1 億円の売上を達成するようになった。その結果、ネット通販が事業として有望な分野であると判断し、専任組織を作り本格的に取り組むことに決定した。

ネット通販事業の責任者になった H 部長は、事業計画作りに取り掛かった。インターネット利用料金の低下やインターネット利用人口の急増から、Y 社の顧客層においてもインターネット利用の障壁は低くなり、利用環境は早期に整備されることが予想できた。また、ネット通販の利便性と、価格面でのメリットなどを訴求することによって、新規の顧客獲得も十分に可能であると考え、3 年後の月間売上を現在の 10 倍に拡大させる目標を設定し、事業計画を策定した。H 部長は策定した事業計画を基に、月間売上 10 億円の電子商取引（以下、EC という）に耐えられるシステムの検討を情報システム部に依頼した。情報システム部の G 課長は、インターネットインフラ担当の F 君に検討を指示した。

現在、Y 社の本社 LAN は、図 1 の構成になっている。



DBサーバ：データベースサーバ

図 1 本社 LAN の構成

EC システムは、Web サーバと DB サーバから構成されている。EC システムの Web サーバは、電子メール(以下、メールという)サーバ、DNS サーバ、企業 Web サーバなど、Y 社が社外に公開しているサーバと同じく DMZ に設置してある(以下、これらのサーバをまとめて公開サーバという)。DB サーバには、顧客データ、受注データ、商品データなどが蓄積されている。試験システムのため、負荷対策や障害対策は施していない。

Y 社では、この半年間にインターネットに関連する次の四つの問題を経験した。

- (1) ISP が原因でインターネット接続が中断した。
- (2) EC システムの Web サーバ障害によって、サービスが停止した。

(3) メールサービスの停止とメールの紛失事故が発生した。

(4) メールを原因とするウイルスによる被害が発生した。

F 君は、上記の(1)～(4)の問題対策も併せて実施することにし、システムの高信頼化、高性能化などの安全対策として、次の 4 点を骨子とした改善案をまとめ、G 課長に報告した。

〔システムの改善案〕

(1) 二つの ISP と接続(以下、ISP の二重化という)する。

(2) EC システムのサーバやメールサーバなど、主要なサーバに安全対策を施す。

(3) EC システムは、負荷の急増に耐えられる構成にする。

(4) メールのウイルスチェックを行う。

改善案の説明を受けた G 課長は、F 君の提案の必要性を理解し、具体的なシステム構成の設計を指示した。F 君は、システム構築を委託している SI 業者の B 氏に、システム改善案を説明し、その具体的な提案を求めた。

〔B 氏の提案〕

(1) ISP の二重化

B 氏：ISP を二重化する方法は二つあります。それらは、自律システムを運営する方法と、今までどおりの静的経路制御によって二つの ISP と接続する方法です。しかし、前者の運営は技術的に難しい上に、社会的責任も発生しますので、避けたいですね。

F 君：それでは、後者はどんな方法ですか。

B 氏：公開サーバごとに、送受信されるパケットが経由する を分ける方法です。インターネットから転送されてくるパケットは、アクセス先の公開サーバの IP アドレスによって配送ルートが決まります。一方、 から ISP に向けて発信するパケットは、負荷分散装置(以下、LB という)によって振り分けることができます。LB は、送信元の IP アドレスなどトランスポート層以下の情報を基に振り分け先を制御します。負荷分散処理は、振り分け先を均等にするなどの振り分けアルゴリズムに基づいて行われます。LB は、ping による定期的な応答チェックを行い、転送先の障害を検出して転送先を切り替えることができます。LB のこの機能を利用すれば、ISP を二重化することもできます。この方法では、図 2 の構成になります。

F 君：図 2 で、ISP からのパケットはどのように転送されてくるのか、具体的に説明してください。

B 氏：DMZ-1 で公開する IP アドレスを から貸与されたものとし、DMZ-2 で公開する IP アドレスを から貸与されたものとします。そうしますと、社外から DMZ 上の公開サーバへのアクセスは、サーバごとに ISP-1 か ISP-2 のどちらかの経路に固定されますので、トラフィックを二つの ISP に分散させることができます。

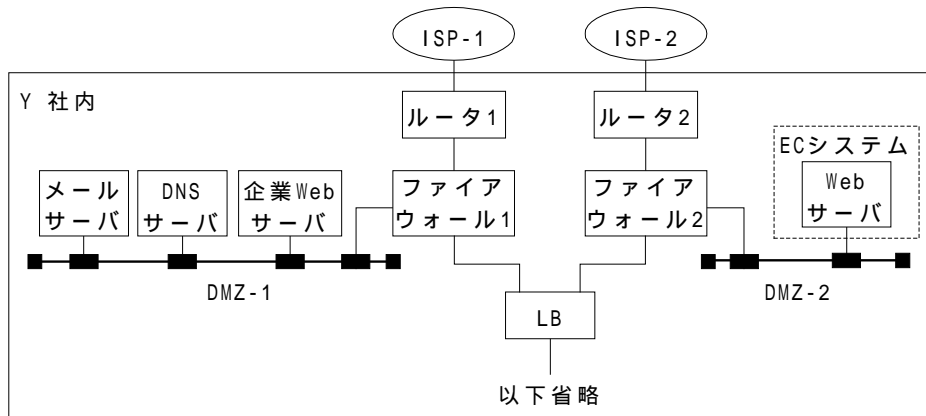


図 2 ISP の二重化構成

F 君：社内から ISP へのパケットは、どのように転送されますか。

B 氏：LB の設定によって、ISP-1 と ISP-2 へ均等に分散させることや、通常は ISP-1 に転送し、ISP-1 へのルートに障害が発生した場合だけ、ISP-2 に転送させることもできます。このとき、NAT をファイアウォールで行えば、(a)リプライパケットは同一の ISP 経由で同一のファイアウォールに戻ってきます。

F 君：分かりました。図 2 の方法でよさそうですね。

(2) EC システムと DNS サーバの安全対策

B 氏：EC システムは今後の負荷増大に対応させるため、アプリケーションサーバ(以下、AP サーバという)を追加して 3 層構造とします。セッション管理、画面制御、業務選択などを行う Web サーバは 2 台構成とし、LB がもつ負荷分散機能を利用して拡張性と可用性を高めます。業務処理を実行する AP サーバも 2 台構成とし、振り分けサーバを利用して負荷分散を行います。振り分けサーバは、CPU 性能と稼働状況を基に CPU の負荷率を検出し、最も負荷の低いサーバを選んで処理を実行させる機能をもちます。DB サーバは、クラスタリング構成とします。ディスク装置は RAID0+1 の構成として、高速化と可用性を高めます。RAID0 は、記録データを複数の磁気ディスク装置に分散させる方式で、RAID1 は、磁気ディスク装置の を行う方式です。RAID0+1 とは、この両方を行う方式です。

F 君：そのほかのサーバに対してはどのような対策を考えていますか。

B 氏：DNS サーバは、社外向けと社内向けに分けます。(b)社外向け DNS サーバは、ISP の障害を考慮して、ISP ごとに分けて設置します。社内向け DNS サーバは、プライマリ、セカンダリの 2 台構成を考えています。

(3) メールサーバの安全対策とウイルス対策

F 君：メールサーバは、どのような対策になりますか。

B 氏：メールシステムは、安全対策のために複数のサーバで構成します。サーバ上でのメール配送定義と、DNS サーバの MX レコード設定情報によってサーバの二重化を図ります。また、併せてウイルスのチェックと駆除も行います。具体的には、図 3 の構成になります。

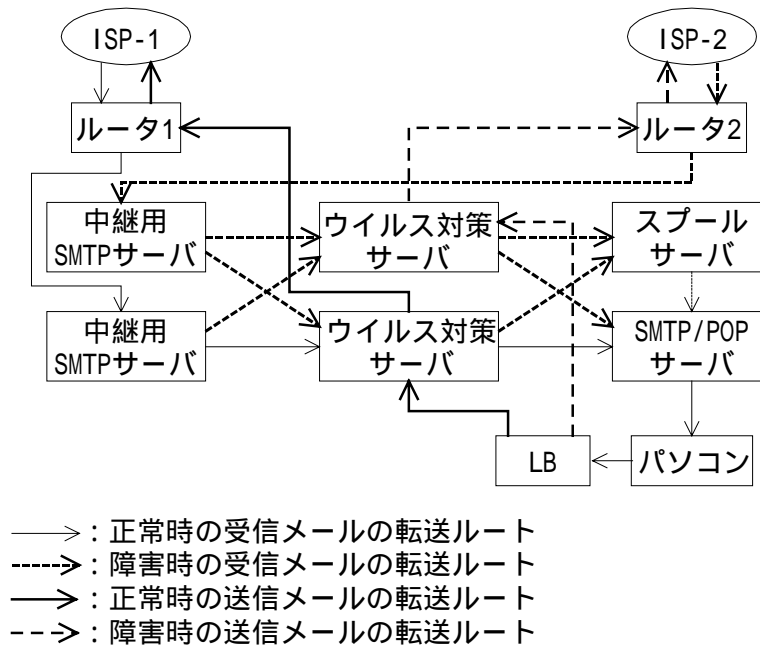


図3 メールシステムの二重化構成

F 君：社外からのメールは，どのように転送されてきますか。

B 氏：社外からのメールは，いったん中継用 SMTP サーバに転送されます。2 台の中継用 SMTP サーバのホスト名は，社外向け DNS サーバに 値を変えて登録します。そうすると，通常では ISP-1 経由でメールが転送されますが，ISP-1 又は中継用 SMTP サーバなどに障害が発生したときには，ISP-2 経由でもう一方の中継用 SMTP サーバに転送されるようにします。中継用 SMTP サーバでは，受信したメールをメール配送定義に従って に転送するようにします。このメール配送定義には，バックアップ用サーバの設定を含めます。

では社内向けの DNS サーバを参照して に転送するようにします。社内向け DNS サーバには，MX レコードとして と の 2 台のサーバのホスト名を登録し，それらには異なる 値を与えることによって， の障害時にバックアップが行われるようにします。一方，パソコンからのメール送信は，LB に設定した仮想 IP アドレスあてに行うようにします。LB では，仮想 IP アドレスあてのメールを正常時の転送ルートに転送するよう設定します。パソコンからのメール送信では，LB を利用してウイルス対策サーバの障害対策を行います。

F 君：メールの不正中継対策も行えますか。

B 氏：社内に転送されてくるメールは，必ず中継用 SMTP サーバを経由しますから，中継用 SMTP サーバで容易に対策を実施することができます。

F 君：十分な対策ですね。これなら安心です。

(4) システム全体構成

B 氏：これらすべてをまとめると，図 4 の構成になります。要求条件に従い，主要なサーバには安全対策を施します。LB，スイッチングハブ，ルータなどのネットワーク機器と振分けサーバ及びファイアウォールは，比較的速やかに交換作業が実施できますので，二重化はコールドスタンバイ方式としています。

F 君：分かりました。この構成で課長に提案してみます。

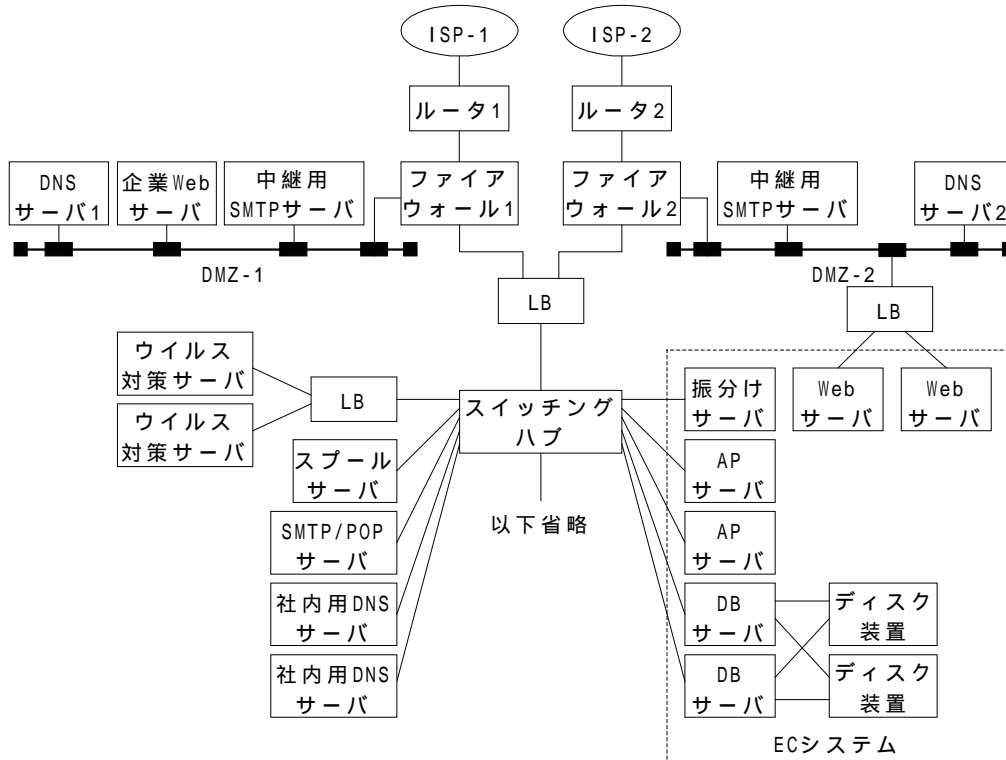


図 4 本社新 LAN の構成

B 氏の提案を基に，F 君が G 課長にインターネットに関連するシステムの安全対策の提案を行ったところ，EC システムの運用に関して，次の五つの課題を検討するよう指示があった。

〔 EC システムの運用に関する課題 〕

- ISP-2 に障害が発生した場合も停止させないための対策
- 停電時や電気設備の法定点検による電源断のときも停止させないための対策
- システムを 24 時間 365 日稼働させるための運用体制
- トラフィックの急増に柔軟に対応するための対策
- 夜間バックアップ作業のための運用体制

F 君は，これらの課題を解決するには，社内のシステム運用では困難なので，インターネットデータセンタ（以下，IDC という）のハウジングサービスを利用するのがよいと考えた。そこで，F 君は，IDC 業者の C 氏に，EC システムのハウジングサービス利用について相談することにした。

〔IDCのハウジングサービス〕

F君: インターネットに関連するシステムの安全対策のために, 図4のシステムを考えていますが, 運用面で幾つかの課題があり, ハウジングサービスの利用を検討することにしました。ECシステムのDBとアプリケーションプログラムのメンテナンスや, 受注データ処理などのサービスの運用は, 今までどおり社内で実施します。しかし, 夜間や休祭日に対応できる体制はとも作れません。ハウジングサービスを利用すると, どの課題が解決できそうですか。

C氏: ECシステム全体及びDMZ-2に関連する機器をハウジング(以下, 案1という)すれば, すべての課題の解決が期待できます。ただ, DMZ-2に関連する機器だけをハウジング(以下, 案2という)する場合は, 幾つかの問題が残ります。

F君: しかし, 案1の場合は, 図4のシステム構成を変更する必要がありますね。

C氏: そうですね。図5のように多少の構成変更が伴います。

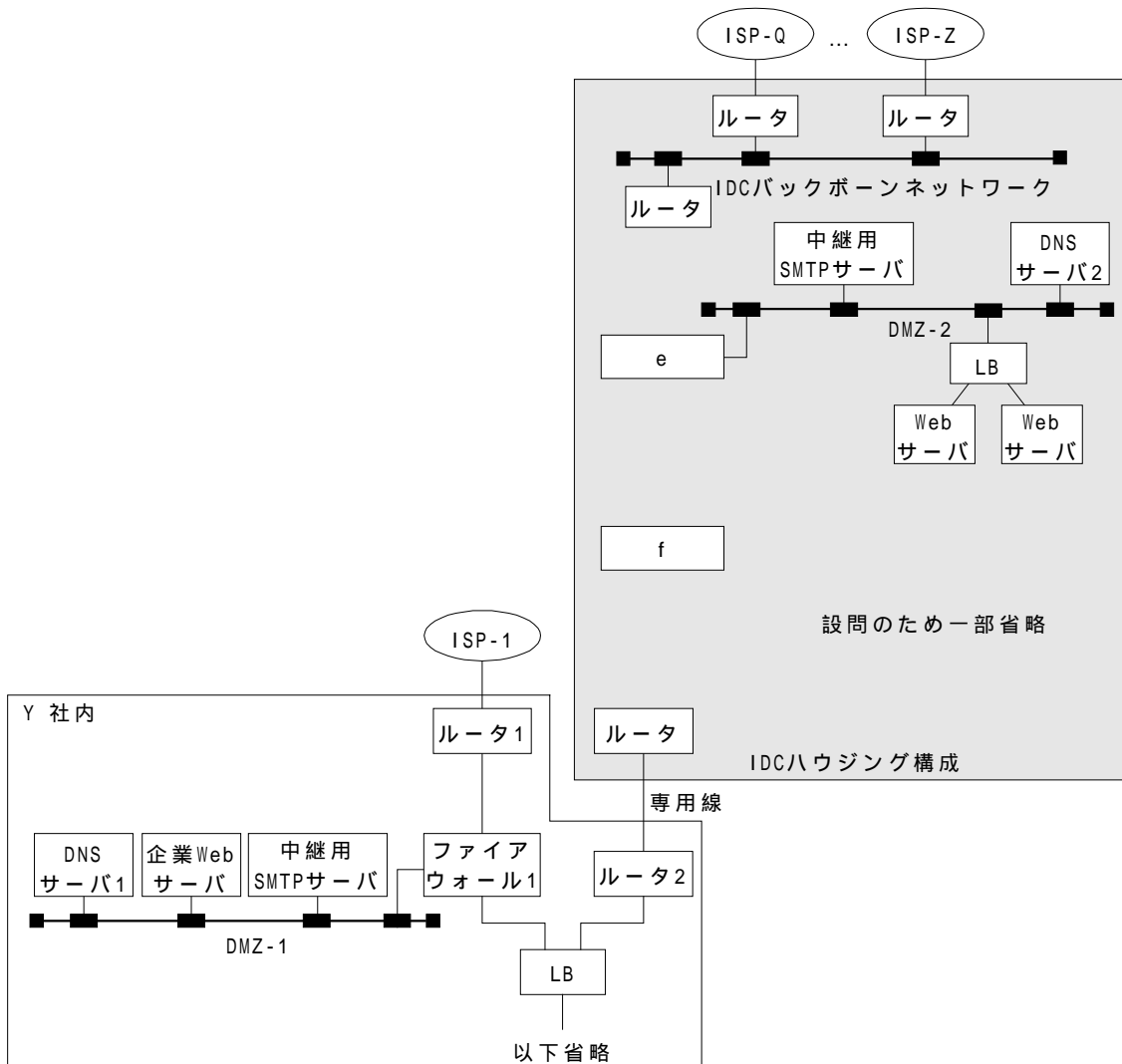


図5 IDCのハウジングサービス利用におけるECシステムの構成(案1)

F 君：案 2 では，G 課長が指摘した EC システムの運用に関する課題の ， が残りますね。そのほか，どんな問題がありますか。

C 氏： と に関連する課題も残ります。

F 君：それでは，案 1 で進める必要がありますね。この場合の の対策を具体的に説明してください。

C 氏：弊社の IDC の設備とサービス概要は，表のとおりになっています。弊社の IDC は，10 社の ISP (ISP-Q ~ ISP-Z) と直接接続（以下，ピアリングという）していますので，ISP の障害による EC システムの停止は避けられます。

表 IDC の設備とサービスの概要

設備及びサービス	概要
耐震	耐震強度を考慮して設計された建物，フロアは免震構造
消火	消火ガスを利用した消火設備
電源	商用電源 2 系統，自家発電設備，UPS 設備
ISP とのピアリング	10 社
標準サービス	ping による監視
オプションサービス	SNMP による監視，障害対応，運用管理など

F 君：自家発電設備があるのに，UPS 設備をもつ理由は何ですか。

C 氏：商用電源の瞬断からコンピュータシステムを守るためです。また，停電時には自家発電装置が稼働しますが，自家発電に切り替わるときの対策も兼ねています。

F 君：すごい設備ですね。システムの障害対応や運用管理は，どのような方法で実施していただけるのですか。

C 氏：24 時間 365 日のシステムの監視と障害対応及び運用管理などを行います。監視によって障害を発見した場合には，オプションサービスとして障害対応を実施します。実施する作業は，障害対応マニュアルに従って行います。また，運用管理マニュアルに従って行う運用管理も，オプションサービスとして用意しております。

F 君：障害対応マニュアルや運用管理マニュアルは，だれが作成することになりますか。

C 氏：それらはシステムの構成や内容，運用方法に関係しますので，お客様に作成していただきます。

G 課長から指摘された課題は，C 氏の説明から IDC のハウジングサービスを利用することで解決できることが分かった。そこで，F 君は IDC のハウジングサービス利用も盛り込んだ新システムへの移行計画をまとめることにした。

設問 1 本文中の ~ に入れる適切な字句を答えよ。

設問 2 図 2 の ISP の二重化に関する次の問いに答えよ。

- (1) 本文中の下線(a)となる理由は何か。75 字以内で述べよ。
- (2) LB で ISP までのルート障害を検出するためには、どの機器に対して ping チェックを行えばよいか。20 字以内で述べよ。

設問 3 図 3 のメールシステムに関する次の問いに答えよ。

- (1) ~ に入れる適切な字句を答えよ。
- (2) 中継用 SMTP サーバでは、なぜ不正中継防止処理を容易に実施できるか。その理由を 40 字以内で述べよ。

設問 4 EC システムの安全対策に関する次の問いに答えよ。

- (1) に入れる適切な字句を答えよ。
- (2) AP サーバへの処理の振分けのために、LB を利用しない理由は何か。55 字以内で述べよ。
- (3) 本文中の下線(b)に従って DNS サーバを設定するが、図 4 の DNS サーバ 2 が管理するゾーン情報は何か。20 字以内で述べよ。

設問 5 IDC のハウジングサービス利用に関する次の問いに答えよ。

- (1) 図 5 中の , に入れる適切な機器の名称を答えよ。また、解答欄に本文中の表記に従って必要な機器及び接続関係を図示し、図 5 を完成させよ。
- (2) 自家発電に切り替わるときの UPS の役割は何か。40 字以内で述べよ。
- (3) 「EC システムの運用に関する課題」の , に対応するために、運用管理マニュアルで指示すべき具体的な作業内容を二つ挙げ、それぞれ 40 字以内で述べよ。
- (4) IDC のハウジングサービス利用によって、EC システムの運用は、Y 社内で行うものと IDC 業者に委託するものに分けられる。Y 社が新たに考慮しなければならない障害対策上の課題は何か。80 字以内で述べよ。