平成１４年度　秋期　ﾃｸﾆｶﾙｴﾝｼﾞﾆｱ（ネットワーク）　午後Ⅱ問題

問１　セキュリティを重視したLANの構築に関する次の記述を読んで，設問１～５に答えよ。

D社は，法人を主な顧客とする中規模な電子部品販売会社である。最近では，個人に対してもパソコン部品の通信販売を行っている。業務の効率化を目的として，インターネットを利用した受注システムを開発することにした。受注システムの開発は，情報システム部が担当する。

受注システムでは，顧客の利便性の向上や開発コストの抑制を目的として，Webや電子メール（以下，メールという）の仕組みを利用する。また，開発コストの抑制以外に，適切なサービス応答時間の確保やインターネットを利用する際のセキュリティ確保も必要である。

〔業務要件〕

D社は，インターネットを利用した受注システムでも従来と同様に，事前に顧客登録を行っている法人と個人を会員として管理し，会員以外には商品を販売しない。法人の顧客登録はD社の営業員が行い，個人の顧客登録は本人がWebサーバを利用して行う。会員の氏名や住所などの会員情報は，プライバシ保護の観点からも非常に重要な情報であり，情報漏えいの脅威から保護しなければならない。

会員は，D社から商品紹介を受けたり，商品の仕様を確認したりするために，Webの仕組みを用いた電子カタログを利用する。新商品のお知らせは，メールを利用して会員に通知する。このメールを受け取った会員は，電子カタログを参照することで，詳細な新商品情報を入手できる。

会員が注文する場合には，定められた注文フォームに必要事項を入力し，Webサーバに見積りを要求する。Webサーバは，要求した会員に関する過去の購入明細を基に見積りを行い，回答する。会員は，見積価格を確認して商品を発注する。

会員からD社への問合せには，メールを利用してもらうため，専用のメールアドレスが設けられている。このメールは，内容に従って担当者に転送され，その担当者が回答する。

〔ネットワーク構成の検討〕

受注システムは，小規模なシステム構成でサービスを開始し，将来の需要に応じて拡張が可能なシステム構成にする。

受注システムの開発担当である情報システム部のU君は，D社で保有しているスイッチングハブの利用を予定している。表１にレイヤ2スイッチングハブ(以下，L2スイッチという)の仕様を，表2にレイヤ3スイッチングハブ(以下，L3スイッチという)の仕様を示す。

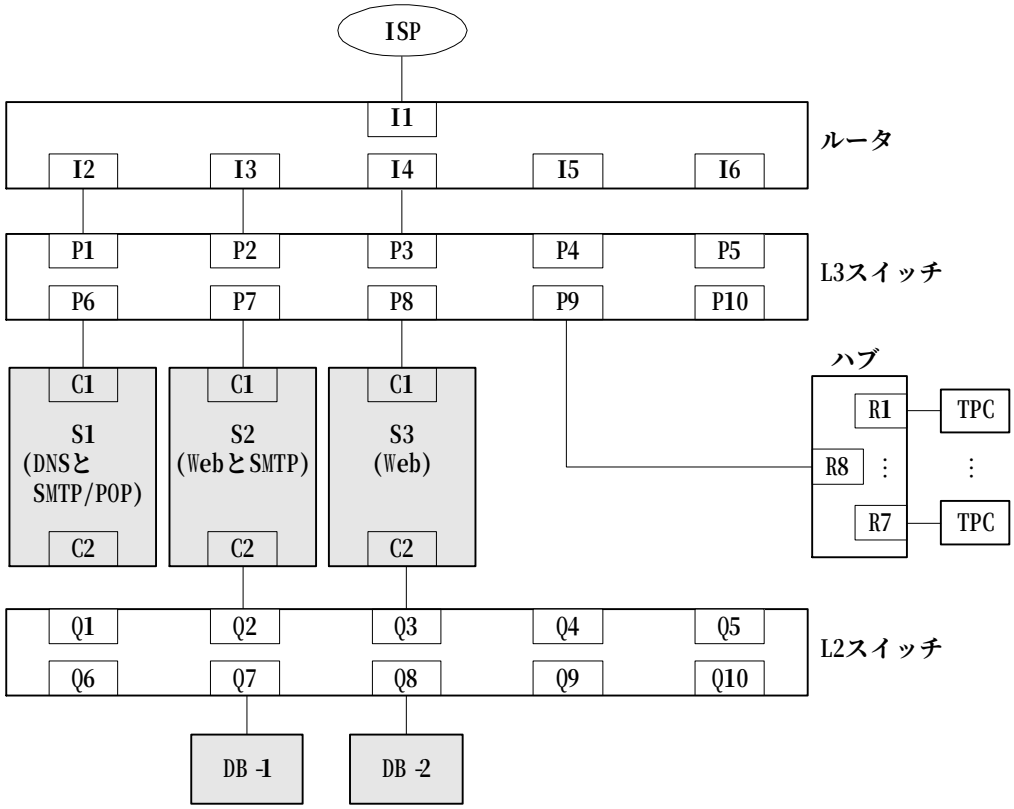
表１　L2 スイッチの仕様(抜粋)

ポート構成	100BASE-TX：10 ポート
スイッチング容量	5G ビット／秒
スイッチング方式	ストアアンドフォワード
VLAN	ポートベース VLAN
フィルタリング機能	なし
ルーティング機能	なし
ネットワーク管理	SNMP

表２　L3 スイッチの仕様（抜粋）

ポート構成	100BASE-TX：10 ポート
スイッチング容量	9G ビット／秒
スイッチング方式	ストアアンドフォワード
VLAN	ポートベース VLAN
フィルタリング機能	次の条件を組み合わせて，IP パケットを通過，又は破棄 (1) 送信元及びあて先 IP アドレス (2) TCP ヘッダの送信元及びあて先ポート番号 (3) TCP ヘッダの SYN，ACK，FIN の各ビット
ルーティング機能	静的及び動的ルーティング
ネットワーク管理	SNMP

U君は，SI 業者のT氏に受注システムの設計を依頼した。T氏は，受注システムに対する設計要件を確認するため，図１に示す受注システムのネットワーク構成の予備検討案を示して，U君と検討を行った。



TPC ： テスト用パソコン

注　“I番号”は，インタフェース番号を示す。
“P番号”，“Q番号”及び“R番号”は，ポート番号を示す。
“C番号”は，LANカード番号を示す。
　　は，サーバを示す。

図１　受注システムのネットワーク構成の予備検討案

T氏：S1 は受注システムの DNS と問合せメール用の SMTP/POP の兼用サーバです。このサーバは，SMTP を用いてメールの送受信を行います。S2 は，電子カタログ機能を実現する Web と SMTP の兼用サーバです。このサーバは，会員に電子カタログの情報を提供したり，新商品情報のお知らせをメールで送信したりします。しかし，メールは受信しません。DB-1 は，電子カタログの情報を格納しているデータベースサーバで，S2 から参照されます。S3 は，受注機能を実現する Web サーバです。このサーバは，会員からの注文内容の受信と，会員への見積回答の送信を行います。DB-2 は，会員情報，過去の購入実績及び商品価格を格納しているデータベースサーバです。S3 は，会員の識別のために，DB-2 を利用します。TPC は，受注システムの開発において，システムの初期設定やテストを行うために使用します。

U君：受注システムの機能を S1，S2 及び S3 に分割しているのですね。

T氏：はい。三つのサーバに分割することでセキュリティを確保することが目的です。仮に，一つのサーバに不正侵入されても，ほかのサーバへの影響を回避するためです。

U君：DB-1 は S2 とだけ通信し，DB-2 は S3 とだけ通信するということで，どちらのデータベースサーバも定められたサーバ以外とは通信しないのですね。

T氏：はい。特に，DB-2 には会員情報が格納されていますので，情報の漏えいには万全の対策を

講じたいと思います。サーバの静的ルーティング機能とサブネット分割を利用する方法では，不正侵入に対応できないと考えて，L2 スイッチを利用した VLAN を構成することにしました。一つの VLAN に DB-1 と S2，ほかの VLAN に DB-2 と S3 を収容したいと思います。

U君：ところで，受注システムの各サーバにプライベート IP アドレスを割り当てるかと思いますが，公開用のグローバル IP アドレスとの変換方法について教えてください。

T氏：グローバル IP アドレスは，S1，S2 及び S3 の各サーバを，インターネット経由でアクセスするために利用されます。これらは，S1 の DNS に登録します。各サーバのプライベート IP アドレスとグローバル IP アドレスの変換は静的に 1 対 1 に対応する NAT 機能を利用します。この機能は，ルータで実現しています。

U君：例えばあて先 IP アドレスが S1 のグローバル IP アドレスの場合ルータで S1 のプライベート IP アドレスに必ず変換されるのですね。

T氏：はい。さらに，IP パケットのヘッダ部だけでなく，FTP や DNS などのプロトコルでは，IP パケットのデータ部に含まれる IP アドレスに対しても同様な変換が行われます。

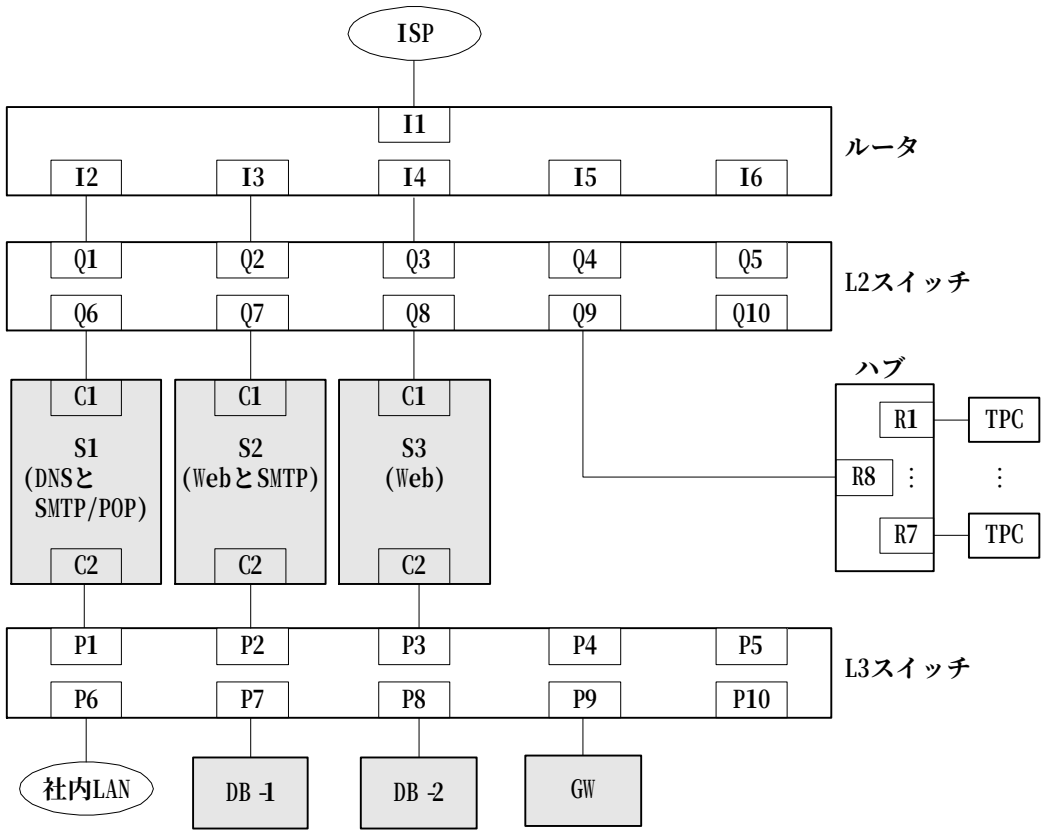
U君：部内での検討の結果，問合せメールの受信や各サーバのメンテナンスは，既存の社内 LAN を経由して社員のパソコンから実施する予定です。このため，社内 LAN の接続方法に関しても検討してください。

T氏：はい。更に設計を進めます。

〔ネットワーク構成の再提案〕

T氏は，社内 LAN の接続を考慮し，受注システムのネットワーク構成に関して，再提案を行った。

T氏：社内 LAN の接続も含めて設計しました。システム監視を行う監視サーバの設置方法については，ほぼ検討が終わっていますが，運用方法が明確になった後で提案させてください。図２に，受注システムのネットワーク構成を示します。



GW ： ゲートウェイサーバ

図２　受注システムのネットワーク構成

U君：予備検討案との大きな違いは，GW の追加や L2 スイッチと L3 スイッチの使い方ですね。

T氏：はい。十分なセキュリティの確保と社内 LAN の接続方法を検討した結果です。GW は，S3 と DB-2 の通信だけを中継します。VLAN 機能は L2 スイッチだけで利用し，L3 スイッチではフィルタリング機能を利用します。VLAN は，三つのグループにします。それぞれの VLAN は，独立したサブネットにし，ホスト部を 8 ビットにします。具体的には，“ Q1 と Q6 と Q9 ”，“ Q2 と Q7 ”，“ Q3 と Q8 ”で三つの VLAN を構成し，S1，S2 及び S3 の IP アドレスには，それぞれ，“ 10.10.30.10 ”，“ 10.10.40.10 ”及び“ 10.10.60.10 ”を静的に割り当てます。表 3 に，各サーバの IP アドレスを示します。

表３　各サーバの IP アドレス(抜粋)

サーバ	IP アドレス
S1 の C1	10.10.30.10
S1 の C2	10.10.50.10
S2 の C1	a .10
S2 の C2	b .20
S3 の C1	10.10.60.10
S3 の C2	10.10.50.30
DB-1	10.10.50.40
DB-2	10.10.50.45
GW	10.10.50.50

U君：DB-1，DB-2 及び GW の環境構築のために，TPC から telnet を用いてアクセスする必要があると思います。このアクセスは，提案された VLAN の設定で，問題なく行うことができるのでしょうか。

T氏：はい。できます。各サブネットに収容されているサーバのデフォルトゲートウェイには，それぞれ，ルータの IP アドレスを設定します。また，受注システムの開発時に限っては，ルータを用いて VLAN 間の通信を行います。このため，DB-1，DB-2 及び GW に対しては，アクセス可能な S2 と S3 のサーバにログインした後，そのサーバから telnet を利用してアクセスします。繰り返しになりますが，これらのアクセスは開発時だけ許可し，サービス開始以降は禁止する必要があります。

U君：はい。サービス開始時には十分注意します。ところで，GW の必要性を教えてください。

T氏：DB-2 の情報を外部から守るため，GW を新たに設置しました。GW は，S3 と DB-2 間の通信を定められたルールに基づいて中継します。仮に，S3 からパスワードに対する取得命令が発せられても，GW はこれを排除します。S3 は，会員認証のため，GW を介して DB-2 に会員が入力した ID やパスワードなどの認証識別情報を転送します。その認証結果は，GW を介して DB-2 から S3 に回答されます。

U君：DB-2 に格納されている商品価格の情報は，社内 LAN を通じて設定されますが，この構成であれば，社内 LAN への不正侵入対策も十分だと思います。

〔受注システムのテスト〕

受注システムのテストが始まって間もなく，U君は，情報システム部の後輩であるK君から，サーバに接続できないので助けてほしいとの相談を受けた。ほかの TPC からは接続できるので，U君は，K君の使用している TPC における TCP/IP の設定を確認させた。

K君の使用した TPC の IP アドレスは正しかったが，そのほかの設定に間違いがあったので修正した。その結果，S1 にはアクセスすることができたが，S2 にはアクセスすることができなかった。その後，別の設定の間違いに気付いて，それを修正したところ，S2 へのアクセスも可能になった。K君は，これらをU君に報告した。

K君：［ c ］の設定をしたところ，S1 だけにはアクセスできましたが，S2 にもアクセスするためには，［ d ］の設定の修正が必要でした。
U君：TPC と S1 は，同一の VLAN に収容されています。しかし，TPC は，［ c ］の設定が正しくないので，S1 が同一の［ e ］ドメインに存在しないと判断し，誤った［ d ］への通信を試みます。
K君：［ d ］を間違えても，S1 へのアクセスは可能でした。なぜでしょうか。
U君：［ c ］の設定が正しく修正されたので，K君のパソコンが ARP を利用して［ f ］の［ g ］を取得できたからです。
K君：分かりました。ありがとうございました。

内部に閉じたテストが完了したので，外部からのアクセスに関してテストを行った。内部に閉じたテストの段階では，S2 にプライベート IP アドレスを回答する DNS を構築し，各 TPC やサーバが DNS サーバとして S2 を指定していた。外部からのアクセスを確認するために，グローバル IP アドレスを回答する DNS を S1 に構築した。D社は，S1 の DNS 設定が正しいことを確認し，利用している ISP に対して，受注システムのゾーン情報のコピーを保有するような設定を依頼した。

翌日，K君は，TPC が参照する DNS サーバを S2 から ISP の DNS サーバに変更し，S3 の名前解決を試みた。その結果，TPC には，S3 のプライベート IP アドレスが回答された。次に，K君は，TPC の設定を変更せずに，ISP にダイアルアップ接続して，S3 の名前解決を試みた。今度は，S3 のグローバル IP アドレスが回答された。K君は，U君から，ISP の DNS がフルサービスリゾルバ用の DNS として機能したので，この動作には問題がないと説明され，納得した。

U君は，テストの終盤に，社内のセキュリティポリシに従い，チェックツールを用いて SMTP に関する設定を確認した。その結果，S1 は，メールの不正中継が可能であることが判明した。このため，U君は，T氏に対策を相談した。

U君：S1 の設定を見直し，メールの不正中継対策を行いたいと思います。
T氏：メールの不正中継対策を行うには，SMTP に関する設定を適切に行う必要があります。図３に，メールの不正中継の代表例を示します。

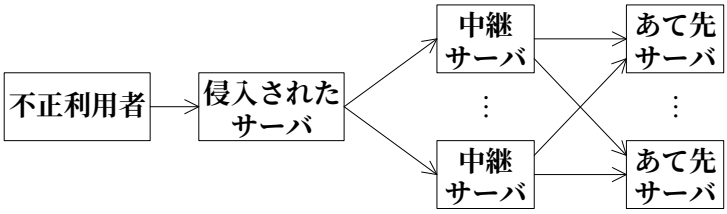


図３　メールの不正中継の代表例

U君：不正利用者は，侵入したサーバからメールを自由に送信できるのに，なぜ，中継サーバを利用するのでしょうか。
T氏：不正利用者の目的は，複数の相手に対して大量にメールを送信することです。メールの送信

処理では，あて先サーバへのデータ転送に要する時間以外にも，必要な処理に多くの時間が費やされます。この時間は，複数の異なるあて先に対してメールを送信する場合，より多く必要になります。そのため，不正利用者は，これらの処理を図３の複数の中継サーバで並列に実行させます。

U君：SMTP に関する設定がぜい弱だと，S1 が図３の中継サーバとして利用されてしまうのですね。具体的な不正中継対策の方法を教えてください。

T氏：メールを中継する条件として，あて先か送信元のアドレスにD社のドメインが含まれている場合で，かつ，D社内から発信したメールに限定します。さらに，ルータの設定も確認してください。

U君は，S1 の SMTP に関する設定を変更した。また，ルータの設定も確認し，メールの不正中継ができないことを確認した。

〔監視サーバの運用方法〕

社内 LAN に接続されたパソコンには，商品価格や電子カタログの更新など，業務上必要なアクセスだけを許可し，ルータやスイッチングハブなどのネットワーク機器とサーバの監視を禁止する。監視サーバは，SNMP を利用して，サーバやネットワーク機器の動作状態やトラフィックを監視する。各サーバにおけるサービスプロセスの状態監視は，監視サーバからサービスプロセスに定期的に自動接続して確認する。

監視サーバは，2 枚の LAN カードを搭載する。一方の LAN カードは，［　h　］と接続し，もう一方の LAN カードは，［　i　］と接続する。また，今後のサーバ増設を考慮して，静的なルーティング機能は使用しない。

監視サーバが障害を検知した場合，S2 を介したメールで，定められた運用担当者に障害情報を通知する。障害情報を受け取った運用担当者は，監視サーバから状況を確認する。障害の状況に応じて，サーバやネットワーク機器を操作し，障害からの復旧を行う。

監視サーバを用いた運用方法も確立できたので，D社は，受注システムのサービスを開始した。

設問１　IP アドレス計画に関する次の問いに答えよ。

(1) 表 3 中の［　a　］，［　b　］について，表 3 のほかの項目表記に従って答えよ。

(2) 各サーバで使用しているサブネットマスクを答えよ。

設問２テスト期間中に発生した事象に関する次の問いに答えよ。

(1) TPC における TCP/IP の設定に関して，本文中の［　c　］～［　g　］に入れる適切な字句を答えよ。

(2) TPC が参照する DNS サーバを S2 から ISP の DNS サーバに変更し，S3 の名前解決を試みた結果，S3 のプライベート IP アドレスが回答された理由を，70 字以内で述べよ。

設問３　図 1 の受注システムのネットワーク構成の予備検討案に関する次の問いに答えよ。

(1) T氏がサーバの静的ルーティング機能とサブネット分割を利用する方法では，不正侵入に対応できないと考えて，L2 スイッチを利用した VLAN を構成することにした理由を，60 字以内で述べよ。

(2) 図 1 に示したネットワーク構成のままで，L2 スイッチの一つのポートを利用して社内 LAN を収容した場合に生じる不具合とその発生理由を，50 字以内で述べよ。

設問４　メールの不正中継に関する次の問いに答えよ。

(1) T氏が述べた中継サーバを利用して並列に実行する処理に関して，中継サーバとあて先サーバのデータ転送以外の処理を，40 字以内で述べよ。

(2) T氏が指示した，D社内から発信したメールに限定するためのルータの設定に関する確認事項を，40 字以内で述べよ。

設問５　図２の受注システムのネットワーク構成に関する次の問いに答えよ。

(1) 監視サーバの接続方法に関して，本文中の［　h　］～［　i　］に入れる適切なネットワーク機器名を，図２から選び答えよ。

(2) 監視サーバが設置され，サービスを開始したときのルータのルーティング処理に関して，開発時との変更点を，60 字以内で述べよ。

(3) 予備検討案に社内 LAN や GW を付加したので，L2 スイッチと L3 スイッチを入れ替えている。DB-2 と GW を目的どおりに機能させるため，L3 スイッチで利用する機能とその設定すべき内容を，80 字以内で述べよ。

問２　システムの災害対策に関する次の記述を読んで，設問１～５に答えよ。

A社は，中小企業向けに業務アプリケーション提供サービス（以下，ASP という）を実施している。契約企業(以下，ユーザという)は，インターネットを経由して，パソコンのブラウザから利用している。ASP 事業のためのシステム（以下，ASP システムという）は，B社の首都圏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し，運用もアウトソーシングしている。図１に，現在の ASP システムの構成を示す。

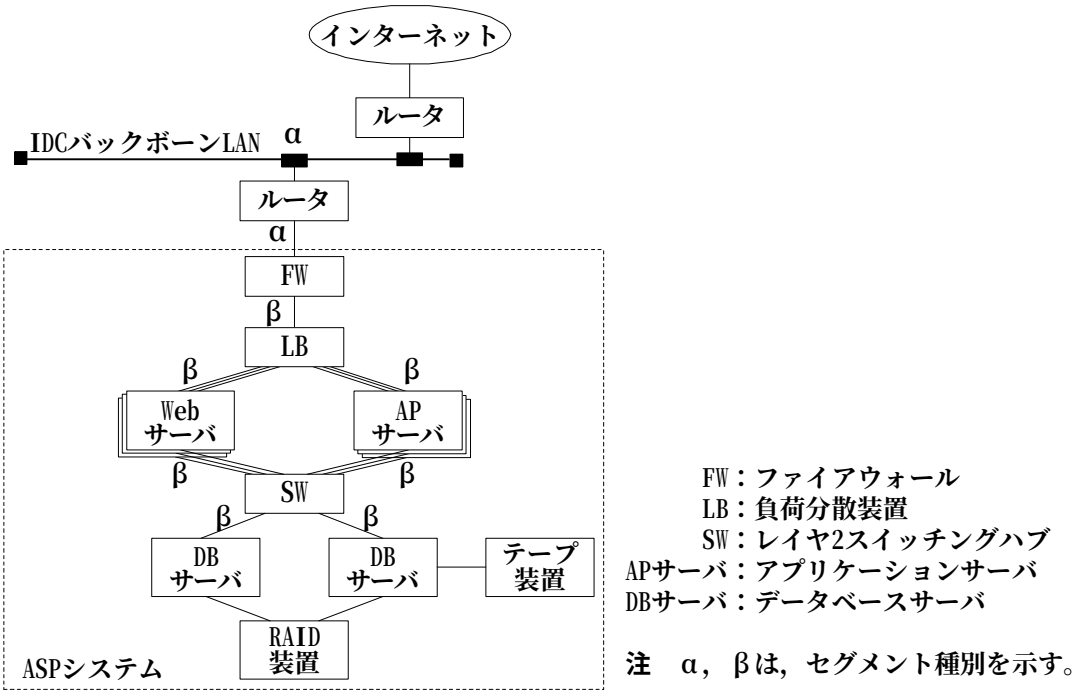


図１　ASP システムの構成

Web サーバは，ユーザが接続する ASP システムの公開サーバであり，αで示されるセグメントはグローバル IP アドレス，βで示されるセグメントはプライベート IP アドレスを使用している。ASP システムのための DNS サーバは，B社の首都圏 IDC が運用管理しているものを利用している。DNS サーバは，プライマリとセカンダリの 2 台とも首都圏 IDC に設置されている。

現在，ASP 事業のユーザは，約 300 社になっている。事業が軌道に乗るにつれて，システム停止による被害が，事業経営に大きな影響を及ぼすことが想定されるようになったので，A社は，システム停止を避けるための対策とデータ破壊や消失を防ぐ対策を積極的に実施してきた。現在では，図 1 に示すとおり，Web サーバと AP サーバを 3 台構成にし，DB サーバを 2 台でクラスタ構成にしている。LB，SW 及び FW などのネットワーク機器は，故障率が低いことと交換作業が容易であることから，代替機を確保して障害に対応している。DB サーバには，光ファイバケーブルで RAID 装置を直結している。テープ装置は，片方の DB サーバに接続している。データのバックアップは，土曜日の深夜に DB 全体をバックアップするフルバックアップ方式で行っている。また，ユーザとの間で締結しているサービス契約に従い，月次更新前にフルバックアップを実施し，バックアップテープ（以下，テープという）を 1 年間保管している。表 1 に，現在利用している RAID 装置とテープ装置の仕様を示す。

表１　RAID 装置とテープ装置の仕様

装置名	仕様	備考
RAID 装置	有効容量　　：120G バイト 構成　　：RAID5 ハードディスク数：10 台 きょう体増設　：不可	4 台のハードディスクで RAID5 を構成し，ミラーリングを行う。2 台はホットスペアとする。 1 台当たりのハードディスク容量は，40G バイトである。
テープ装置	ドライブ数　　：1 収納テープ本数　：5 本 テープ容量　　：40G バイト／本 転送速度　　：6M バイト／秒	

注：G バイトは 10^9 バイト。M バイトは 10^6 バイト。

ASP システムの運用責任者であるＡ社のＦ課長は，これまで，システムの増強を積極的に実施してきた。現在，システムは，安定して稼働しているが，月に約 10 社ずつユーザが増加している。Ｆ課長は，担当者のＥ君に現状の運用を継続したときに顕在化しそうな問題点の洗い出しを指示した。Ｅ君は，Ｆ課長に次の 3 点の懸念事項を説明した。

① テープ装置を接続している DB サーバに障害が発生したとき，バックアップができなくなる。
② バックアップが週 1 回なので，1 週間分の変更データが失われる危険性がある。
③ ユーザは，10 か月後に 400 社を超えることが予想されるので，ディスク容量の拡大が必要になる。

説明を受けたＦ課長は，Ｅ君に対策案の検討を指示した。Ｅ君は，対策案を立案するために，RAID 装置の使用状況とデータの更新状況を調査し，表２にまとめた。

表２　RAID 装置の使用状況とデータの更新状況

項目	内容	備考
DB 容量	90G バイト	ユーザ 400 社分の容量を確保
1 日の変更量	1.5G バイト	1 ユーザ当たり，平均 5M バイト

〔ストレージシステムの見直し〕

Ｅ君は，調査結果を基に，①，②及び③の懸念事項を解決するとともに，運用が容易なバックアップ方式を検討することにした。

(1) バックアップ運用の検討

②の懸念事項を解決するためのバックアップ方式を検討した。

データのバックアップ方式には，フルバックアップと変化分バックアップがある。変化分バックアップは，変化したデータブロックだけをバックアップする方法である。変化分バックアップには，差分バックアップと増分バックアップとがある。差分バックアップは，フルバックアップを行ったときから変更された部分をバックアップする方法である。一方，増分バックアップは，前回のバックアップからの変更部分だけをバックアップする方法である。

障害が発生した場合に，前日のデータ内容に復旧するためのバックアップ運用を次のとおりにし

た。

・月～金曜日は，差分バックアップを行う。テープは，曜日ごとに固定し，毎週同じものを使用する。
・土曜日は，フルバックアップを行う。テープは，2 セット用意して，毎週交互に使用する。
・日曜日は，ASP システムのサービスを停止するので，バックアップを行わない。

これらをまとめると，表3のとおりになる。

表３　バックアップ運用

単位　本

バックアップタイミング	月曜	火曜	水曜	木曜	金曜	土曜	月末
バックアップ方式	差分	差分	差分	差分	差分	フル	フル
テープ本数	1	1	1	1	1	a ×2	a

注　差分は差分バックアップ，フルはフルバックアップを示す。月末は，最終営業日のことである。
土曜日は，“2 セット用意したテープを，毎週交互に使用する”ことを示している。

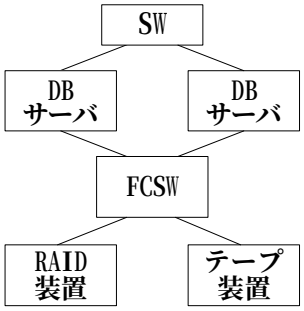
月～土曜日のバックアップはテープ交換も含めて自動で行い，月末はオペレータの操作で行う。月末のバックアップ後，月末用テープは手作業で入れ替え，1 年間保管する。このような運用でバックアップを行った場合，テープの破損がなければ，月末用テープも合わせて，月当たり b 本のテープが使用される。表３のスケジュールでバックアップを行った場合，表１，２の条件下では，月曜日のバックアップ時間は c 分になり，土曜日のバックアップ時間は d 分になる。

(2) ストレージシステム構成の見直し

①，③の懸念事項を解決するために，次の 3 点を考慮して，RAID 装置とテープ装置を使ったストレージシステム構成の見直しを行った。

(ⅰ) DB サーバの二重化にテープ装置も対応させる。
(ⅱ) 表３のバックアップ運用を，月末以外は自動で行うことができるようにする。
(ⅲ) RAID 装置の増設が簡単に実施できるようにする。

見直しの結果，(ⅱ)の課題は収納可能なテープ本数が b 本以上のテープ装置に交換することで解決でき，(ⅰ)，(ⅲ)の課題は SAN(Storage Area Network)を導入して，図２の構成にすることで解決できることが分かった。



FCSW：ファイバチャネルスイッチ

図２　SAN の導入による構成案

E君は，ユーザ数の増加と拡張性を考慮した対策案をまとめ，F課長に説明した。F課長は，対策案の有効性を理解し，実施のためのりん議書を提出して承認を得た。ストレージシステムにSANを導入した後，ASPシステムは，順調に稼働を続けた。

〔システムの災害対策方式の検討〕

その後，社長から，災害によるシステム破壊のリスクに対する対策の必要性が指摘された。F課長は，E君とASPシステムの災害対策方式の検討を行った。

災害対策としては，遠隔地バックアップが効果的であると考えられる。幾つかの遠隔地バックアップ方式の中でも，同一システムを遠隔地に設置してシステム全体をバックアップする方法が，サービス停止を短時間に抑えることができるので，投資金額は大きいが最も効果的であると考えられた。遠隔地にバックアップシステムを設置する場合には，データの整合性の維持が課題になる。そのための方法は幾つか考えられたが，WAN回線を使用したデータの複製(以下，レプリケーションという)による整合性の維持が，最も費用対効果が高い方法であると判断された。

レプリケーションにおいて，最初の同期化が済んだ後は，実際に変更のあったデータブロックだけを複製することによって，WANのトラフィックを最小限に抑える工夫が施されている。レプリケーションのパフォーマンスは，使用可能な帯域幅，ネットワークの構成及び複製するデータ量に影響される。また，レプリケーション方式には，同期レプリケーションと非同期レプリケーションがある。

同期レプリケーションでは，データの複製元になるサーバ（以下，プライマリサーバという）のアプリケーション処理によって更新されたデータが，データの複製先になるサーバ(以下，セカンダリサーバという)に転送され，セカンダリサーバでの更新処理が終了した時点で，アプリケーション処理が次のステップに進むことができる。このように，同期レプリケーションでは，完全なデータの整合性が常に確保されているが，更新が多いときや帯域幅に制約があるときなどは，(a)提供するサービスに影響を与える場合がある。

非同期レプリケーションでは，プライマリサーバで書き込まれた更新データが，いったんキューに登録され，ネットワーク帯域幅に余裕があるときにセカンダリサーバに転送される。(b)そのため，セカンダリサーバに切り替えるときには，データの整合性を確保するための対応処置が必要になる。非同期レプリケーションでは，レプリケーションがアプリケーション処理と独立して行われるので，アプリケーション処理には影響を与えない。

B社は，全国3か所でIDCを運営しているISPである。B社のIDCは，広帯域の専用線で接続されており，インターネットサービスのためのバックボーンを構成している。図3に，B社のバックボーン回線の構成を示す。バックボーン回線は，東京の首都圏IDCと大阪の関西地区IDCからIX(Internet eXchange)に接続されているので，バックアップシステムは，関西地区IDCに設置するのが適切と判断された。

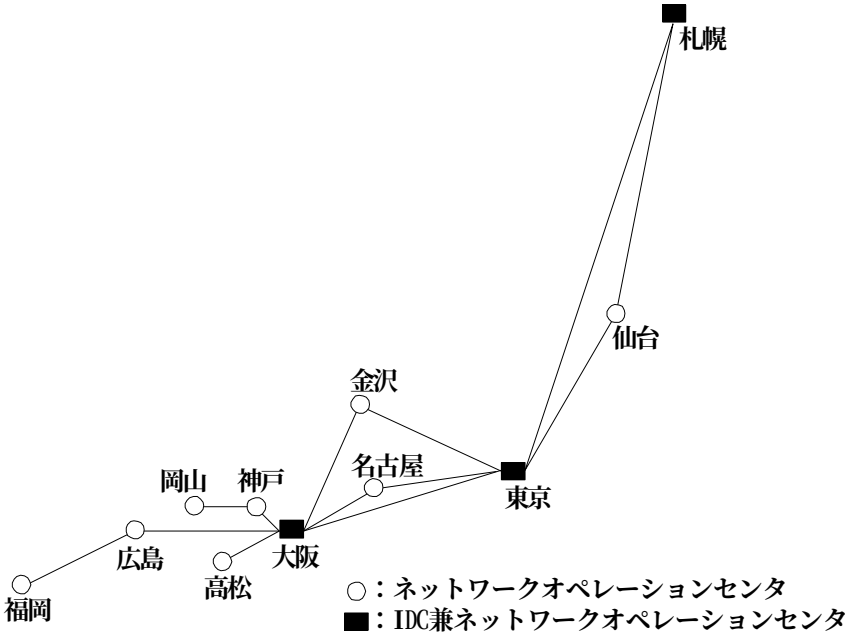


図３　Ｂ社のバックボーン回線の構成

Ａ社は，IDC バックボーン LAN に 10M ビット／秒で全二重接続する，帯域占有方式でのハウジングサービス契約を行っている。ASP システムが発生するトラフィックを調査した結果は，次のとおりである。1 分間隔で測定したトラフィックを 30 分単位で平均化すると，最繁時で，ASP システムに転送されるトラフィックは 2.5M ビット／秒，ASP システムから転送されるトラフィックは 3M ビット／秒であった。Ｂ社の説明によると，IDC バックボーン LAN 及び IDC 間を接続するバックボーン回線の帯域には，まだ十分余裕があるとのことである。そのため，バックボーン回線を利用した通信では，利用可能な帯域を狭く見積もっても，ユーザ数が倍増した時点で片側 2M ビット／秒の帯域がレプリケーションのために使えることが予想できた。

IDC 間でのレプリケーションのための通信で，2M ビット／秒の帯域が利用される場合，レプリケーション処理の伝送効率が 80%であれば，表 2 に示した 1 日の変更量のレプリケーション時間は，システム運用上，問題ない範囲に抑えられる。また，インターネットを利用したデータ転送では，セキュリティの問題があるが，VPN を利用することで解決できる。

以上の検討から，バックアップシステムを関西地区 IDC に設置し，Ｂ社のバックボーン回線を利用してレプリケーションを行うことで，ASP システムの災害対策が実施できると判断できた。Ｂ社のバックボーン回線では，帯域の保証が行われないので，トラフィック混雑時のサービスへの影響を避けるために，レプリケーション方式として，非同期レプリケーションを採用する。非同期レプリケーションのプライマリサーバを運用系システムの DB サーバ，セカンダリサーバを待機系システムの DB サーバとして，レプリケーションのためのプログラムを運用系及び待機系システムの DB サーバで稼働させる。図４に，レプリケーションを利用した ASP システムの災害対策システムの構成案を示す。

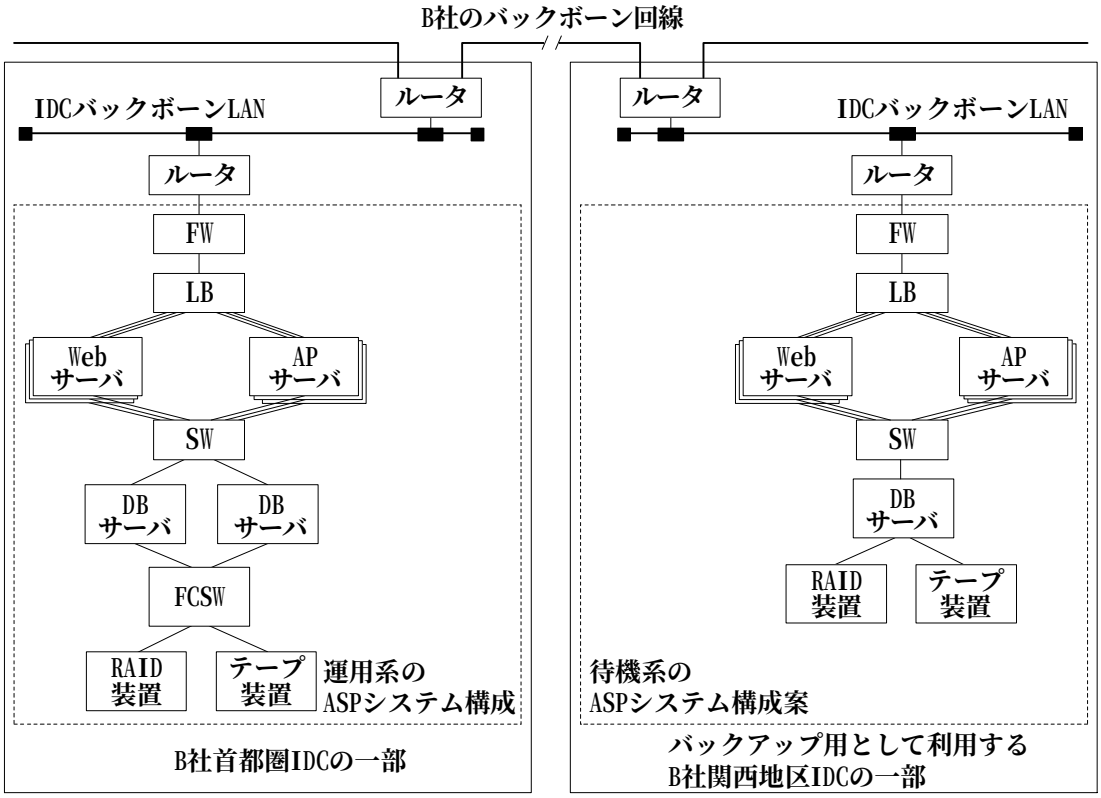
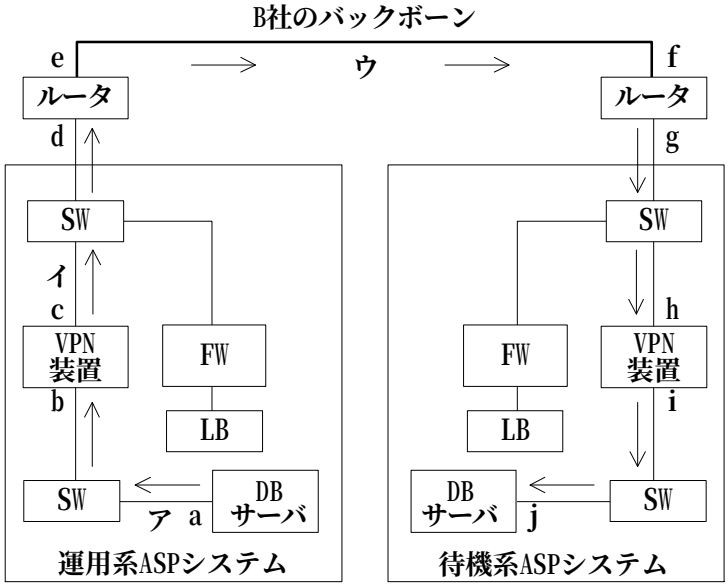


図４　ASP システムの災害対策システムの構成案

〔VPN の検討〕

VPN は，暗号化と認証機能をもつ暗号技術を利用すれば実現できる。暗号化の方法は複数あり，暗号化処理をどの層で行うかによって分類できる。例えば，SSH はアプリケーション層，SSL はソケット層，IPsec は［　e　］層での暗号化が行われ，それぞれ，異なった特徴をもっている。今回のレプリケーションでは，インターネット VPN で広く利用されている IPsec を利用することにした。IPsec では，暗号ペイロード(以下，ESP(Encapsulating Security Payload)という)と認証ヘッダによって，IP パケットの機密性を保障する仕組みをもっている。ESP では，IP パケットの暗号化で盗聴を防ぐことができ，また，認証ヘッダ中の認証データでパケットの［　f　］を検出することができる。

IPsec には，トンネルモードとトランスポートモードがある。トンネルモードは，IP パケット全体を暗号化する方式である。トランスポートモードは，IP ヘッダを暗号化せず，IP データだけを暗号化する方式である。運用系と待機系の ASP システム間での VPN は，FW の負荷の増加を抑えるために，VPN 装置を導入してレプリケーションデータが FW を通過しないように設定する。VPN 装置では NAT が実装されていないので，この構成ではトランスポートモードが利用できない。そのため，トンネルモードを利用する。図５に，IPsec を利用したときのレプリケーションデータの流れを示す。



注　a～jは，IPアドレスを示す．

図５　IPsec を利用したときのレプリケーションデータの流れ

VPN は，VPN 装置間で設定される。このとき，図５のア，イ，ウの位置における IP パケット構成を，それぞれ，図６，７に示す。図６，７の①，③は送信元 IP アドレス，②，④はあて先 IP アドレスを示す。

IPヘッダ ①，②	IPデータ

図６　アの位置における IP パケット構成

IPヘッダ ③，④	認証ヘッダ	ESPヘッダ	暗号化データ	ESP 認証データ

図７　イとウの位置における IP パケット構成

〔災害時のシステム切替方法の検討〕

待機系システムのハードウェア構成は，冗長化せずに運用系システムよりも簡略化する。しかし，アプリケーションプログラムや DB は，同一のものにして，同等の機能をもたせる。災害などによって，運用系システムや設置した環境のどこかに大きな障害が発生して，運用系システムでサービスの提供ができなくなったときには，待機系システムに切り替えることでサービスが継続できるようにする。

ユーザパソコンの設定変更を行うことなく待機系システムに切り替えるためには，DNS への登録データの変更が必要である。しかし，この変更を行ってもユーザパソコンのブラウザの接続先が，(c)すぐには待機系システムに切り替わらない場合がある。さらに，待機系システムを稼働させ，サ

ービスの提供を再開するときには，ユーザへの影響を最小限に抑えるために，適切な通知が必要になる。

以上の検討を基に，F課長は，B社のバックボーン回線を利用した非同期レプリケーションによるASPシステムの災害対策方式をまとめた。

設問１　バックアップと暗号化処理に関する次の問いに答えよ。

(1) 表３中及び本文中の［ a ］～［ d ］に入れる適切な数値を答えよ。答えは，小数点以下を切り上げて整数で答えよ。

(2) 本文中の［ e ］，［ f ］に入れる適切な字句を答えよ。

設問２　データバックアップに関する次の問いに答えよ。

(1) 変化分バックアップの方法として差分バックアップを行うことにした理由を，30字以内で述べよ。

(2) 遠隔地バックアップを行った場合も，テープへのデータのバックアップを継続する。その理由を，データ保護の観点から50字以内で述べよ。

設問３　レプリケーションによる災害対策に関する次の問いに答えよ。

(1) 本文中の下線(a)の影響とは何か。具体的な内容を，35字以内で述べよ。

(2) 本文中の下線(b)の対応処置がなぜ必要か。40字以内で述べよ。

(3) 本文中の記述において，1日の変更量のレプリケーション時間が何分になるかを求めよ。

設問４　VPNに関する次の問いに答えよ。

(1) 図５の構成では，VPN装置にNATが実装されていないと，トランスポートモードが利用できない。その理由を，30字以内で述べよ。

(2) 図６，７中の①～④に対応するIPアドレスを，図５中のa～jの中から答えよ。

設問５　災害時における，システム切替方法と課題に関する次の問いに答えよ。

(1) 本文中の記述以外に，DNSの構成に関して，B社に依頼しておかなければならない対策内容は何か。40字以内で述べよ。

(2) 待機系システムへの切替えのために，変更しなければならないDNSの登録データは何か。60字以内で述べよ。

(3) 本文中の下線(c)の原因は何か。40字以内で述べよ。

(4) 待機系システムへの切替えを円滑に行うために，A社とB社が協力して実施しておくべきことは何か。20字以内で述べよ。

(5) 本文中で採用した非同期レプリケーション方式の特徴から，待機系システムへの切替えをユーザに通知するとき，ユーザの業務で問題を発生させないためにユーザに依頼すべき作業内容は何か。60字以内で述べよ。