NW

令和４年度　春期
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. **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。**
4. 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

5. 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，**生年月日欄**に**受験票の生年月日**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。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **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。○印がない場合は，採点されません。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。
   (4) 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。
   (5) 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。

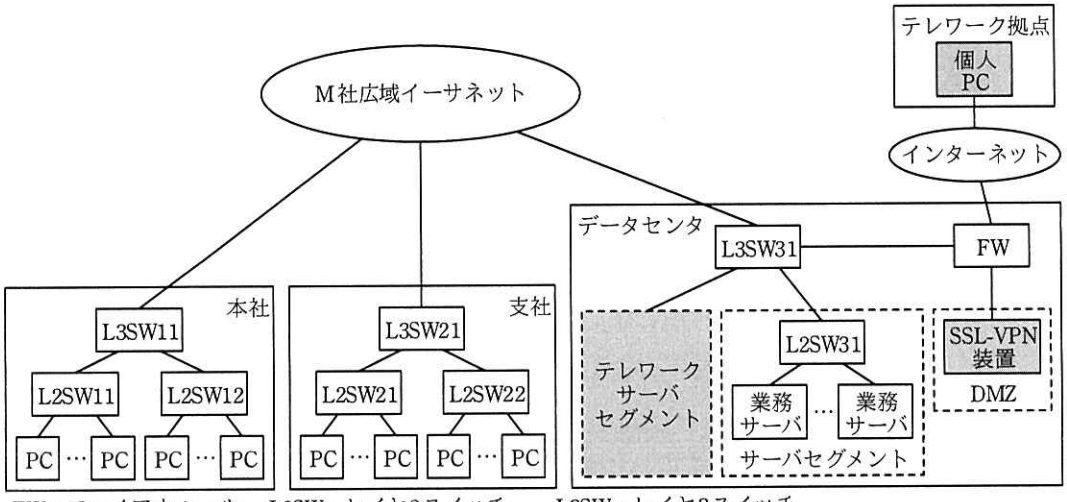
〔問２を選択した場合の例〕

選択欄	
１問選択	問１
	問２（○）

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　テレワーク環境の導入に関する次の記述を読んで，設問1～5に答えよ。

K社は，東京に本社を構える中堅の製造業者である。東京の本社のほかに，大阪の支社，及び関東圏内のデータセンタがある。このたびK社では，テレワーク環境を導入し，K社社員が自宅などをテレワーク拠点として，個人所有のPC（以下，個人PCという）を利用して業務を行う方針を立てた。また，業務の重要性から，ネットワークの冗長化を行うことにした。これらの要件に対応するために，情報システム部のP主任が任命された。K社の現行のネットワーク及び導入予定の機器を図1に示す。



FW：ファイアウォール　L2SW：レイヤ2スイッチ　L3SW：レイヤ3スイッチ
広域イーサネット：広域イーサネットサービス網　業務サーバ：業務アプリケーションサーバ
テレワークサーバセグメント：テレワークのための機器で構成するセグメント
注記　網掛け部分は，テレワーク環境として導入予定の機器を示す。

図1　K社の現行のネットワーク及び導入予定の機器（抜粋）

〔現行のネットワーク構成〕

図1の概要を次に示す。

・本社，支社，データセンタはM社の広域イーサネットで接続されている。
・サーバセグメントに設置された業務サーバに，社内のPCからアクセスして各種業務を行っている。
・FWは，社内からインターネットへのアクセスのためにアドレス変換（NAPT）を行っている。

・FW で DMZ を構成し，DMZ にはグローバル IP アドレスが割り当てられている。
・DMZ 以外の社内の全てのセグメントは，プライベート IP アドレスが割り当てられている。
・経路制御の方式は，OSPF が用いられている。
・本社のネットワークアドレスには，172.16.1.0/24 を割り当てている。
・支社のネットワークアドレスには，172.16.2.0/24 を割り当てている。
・データセンタのネットワークアドレスには，172.17.0.0/16 を割り当てている。

〔テレワーク環境導入方針〕

P 主任は，テレワーク環境構築に当たって，導入方針を次のように定め，技術検討を進めることにした。

・テレワーク拠点の個人 PC には業務上のデータを一切置かない運用とするために，仮想デスクトップ基盤（以下，VDI という）の技術を採用する。
・データセンタのテレワークサーバセグメントに VDI サーバを導入する。VDI サーバでは，個人ごとの仮想化された PC（以下，仮想 PC という）を稼働させ，個人 PC から遠隔で仮想 PC を利用可能にする。
・個人 PC には，仮想 PC の画面を操作するソフトウェア（以下，VDI クライアントという）を導入する。
・仮想 PC から，業務サーバへアクセスして業務を行う。社内の PC からは直接業務サーバへアクセスできるので，社内の PC から仮想 PC は利用しない。
・DMZ に SSL-VPN 装置を導入して，テレワーク拠点の個人 PC からデータセンタのテレワークサーバセグメントへのアクセスを実現する。
・情報セキュリティの観点から，SSL-VPN アクセスのための認証は，個人ごとに事前に発行したクライアント証明書を用いて行う。
・SSL-VPN 装置は，個人 PC からの接続時の認証に応じて適切な仮想 PC を特定する。そして，個人 PC からその仮想 PC への VDI の通信を中継する。このような機能をもつ SSL-VPN 装置を選定する。
・テレワークを行う利用者は最大 200 人とする。

〔SSL-VPN 技術調査とテレワーク環境への適用〕

P 主任は，テレワーク拠点からインターネットを介した社内へのアクセスを想定し

て，SSL-VPN の技術について調査を行い，結果を次のようにまとめた。

・SSL-VPN は，TLS プロトコルを利用した VPN 技術である。

・TLS プロトコルは，HTTPS（HTTP over TLS）通信で用いられる暗号化プロトコルであり，インターネットのような公開ネットワーク上などで安全な通信を可能にする。

・TLS プロトコルのセキュリティ機能は，暗号化，通信相手の認証，及び［　ア　］である。

・SSL-VPN は，リバースプロキシ方式，ポートフォワーディング方式，［　イ　］方式の 3 方式がある。

・リバースプロキシ方式の SSL-VPN は，インターネットからアクセスできない社内の Web アプリケーションへのアクセスを可能にする。

・ポートフォワーディング方式の SSL-VPN は，社内のノードに対して TCP 又は UDP の任意の［　ウ　］へのアクセスを可能にする。

・［　イ　］方式の SSL-VPN は，動的にポート番号が変わるアプリケーションプログラムでも社内のノードへのアクセスを可能にする。

・リバースプロキシ方式以外の SSL-VPN を利用するためには，SSL-VPN 接続を開始するテレワーク拠点の PC に，SSL-VPN 接続を行うためのクライアントソフトウェアモジュール（以下，SSL-VPN クライアントという）が必要である。

・TLS プロトコルは，複数のバージョンが存在するが，TLS1.3 は TLS1.2 よりも安全性が高められている。一例を挙げると，TLS1.3 では AEAD（Authenticated Encryption with Associated Data）暗号利用モードの利用が必須となっており，①セキュリティに関する二つの処理が同時に行われる。

・TLS プロトコルで用いられる電子証明書の形式は，X.509 によって定められている。

・認証局（以下，CA という）によって発行された電子証明書には，②証明対象を識別する情報，有効期限，［　エ　］鍵，シリアル番号，CA のデジタル署名といった情報が含まれる。

P 主任は，SSL-VPN の技術調査結果を踏まえ，テレワーク環境への適用を次のとおり定めた。

・SSL-VPN クライアント，クライアント証明書，及び VDI クライアントを，あらか

じめ個人 PC に導入する。

・SSL-VPN 装置へのアクセスポートは，TCP の 443 番ポートとする。

・SSL-VPN 装置で利用する TLS プロトコルのバージョンは，TLS1.3 を用い，それ以外のバージョンが使われないようにする。

・仮想 PC へのアクセスのプロトコルは RDP とし，TCP の 3389 番ポートを利用する。

・SSL-VPN 装置が RDP だけで利用されることを踏まえ，SSL-VPN の接続方式は［ オ ］方式とする。

〔SSL-VPN クライアント認証方式の検討〕

P 主任は，個人 PC から SSL-VPN 装置に接続する際のクライアント認証の利用について整理した。

・個人 PC から SSL-VPN 装置に接続を行う時に利用者のクライアント証明書が SSL-VPN 装置に送られ，③SSL-VPN 装置はクライアント証明書を基にして接続元の身元特定を行う。K 社においては，社員番号を利用者 ID としてクライアント証明書に含めることにする。

・TLS プロトコルのネゴシエーション中に，④クライアント証明書が SSL-VPN 装置に送信され，SSL-VPN 装置で検証される。

・⑤SSL-VPN 装置からサーバ証明書が個人 PC に送られ，個人 PC で検証される。

TLS プロトコルにおける鍵交換の方式には，クライアント側でランダムなプリマスタシークレットを生成して，サーバの RSA［ エ ］鍵で暗号化してサーバに送付することで共通鍵の共有を実現する，RSA 鍵交換方式がある。また，Diffie-Hellman アルゴリズムを利用する鍵交換方式で，DH 公開鍵を静的に用いる方式もある。これらの方式は，⑥秘密鍵が漏えいしてしまったときに不正に復号されてしまう通信のデータの範囲が大きいという問題があり，TLS1.3 以降では利用できなくなっている。TLS1.3 で規定されている鍵交換方式は，［ カ ］，ECDHE，PSK の 3 方式である。

さらに P 主任は，クライアント証明書の発行に関して次のように検討した。

・クライアント証明書の発行に必要な CA を自社で構築して運用するのは手間が掛か

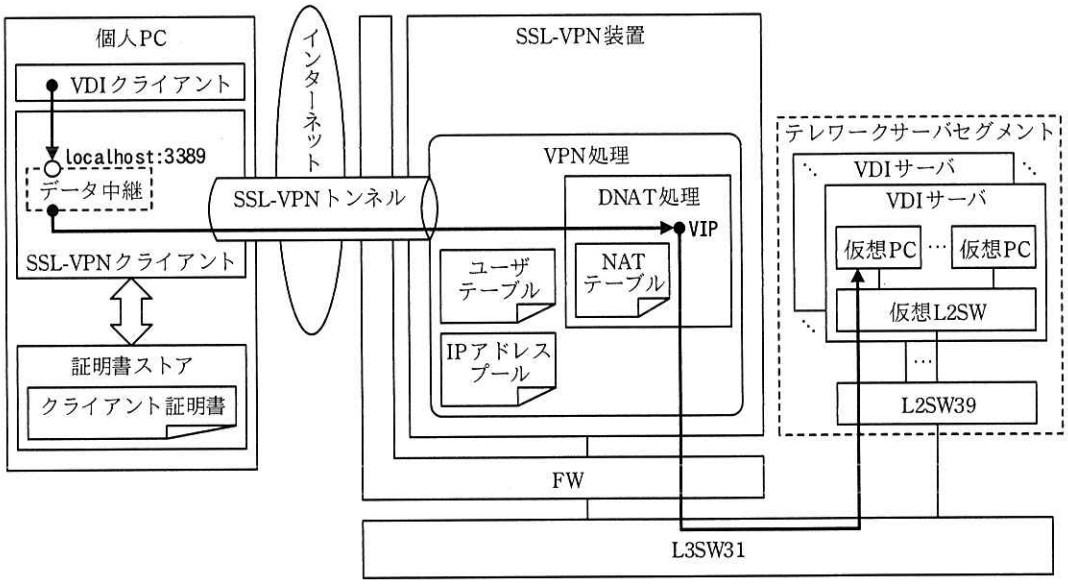
るので，セキュリティ会社である S 社が SaaS として提供する第三者認証局サービス（以下，CA サービスという）を利用する。

・新しいクライアント証明書が必要なときは，利用者の公開鍵と秘密鍵を生成し，公開鍵から証明書署名要求（CSR）を作成して，CA サービスへ提出する。CA サービスは，クライアント証明書を発行してよいかどうかを K 社の管理者に確認するとともに，⑦CSR の署名を検証して，クライアント証明書を発行する。

・クライアント証明書の失効が必要なときは，S 社の CA サービスによって証明書失効手続を行うことによって，CA の証明書失効リストが更新される。証明書失効リストは，失効した日時と⑧クライアント証明書を一意に示す情報のリストになっている。

〔テレワーク環境構成の検討〕

P 主任は，ネットワーク構築ベンダ Q 社の担当者に相談して，Q 社の製品を利用したテレワーク環境の構成を検討した。P 主任が考えたテレワーク環境を図 2 に示す。また，図 2 の主要な構成要素の説明を表 1 に示す。



VIP：仮想IPアドレス　　DNAT：Destination NAT
注記 1　localhost:3389 は，localhost の TCP の 3389 番待受けポートを示す。
注記 2　●→ は，パケットの送信元と宛先を示す。
注記 3　○ は，待受けポートを示す。

図 2　P 主任が考えたテレワーク環境

表1　図2の主要な構成要素

名称	説明
仮想 PC	利用者の業務で利用するための仮想化された PC である。利用者ごとに仮想 PC があらかじめ割り当てられており，IP アドレスは静的に割り当てられている。それぞれの仮想 PC は RDP 接続を TCP の 3389 番ポートで待ち受けている。
VDI サーバ	仮想 PC を稼働させるためのサーバである。複数の VDI サーバで，全利用者分の仮想 PC を収容する。システム立上げ時に全仮想 PC が起動される。 VDI サーバ内の仮想 PC は仮想 L2SW に接続される。仮想 L2SW は VDI サーバの物理インタフェースを通じて L2SW39 に接続される。
L2SW39	複数の VDI サーバを収容する L2SW である。
SSL-VPN 装置	SSL-VPN 接続要求を受けて SSL-VPN トンネルの処理を行い，仮想 PC へ RDP 接続を中継する。この一連の処理を VPN 処理という。VPN 処理はユーザテーブルと NAT テーブルの二つのテーブルを利用する。DNAT 処理のための仮想的な宛先 IP アドレスである VIP が設定される。
VDI クライアント	個人 PC で，仮想 PC の画面を操作するクライアントソフトウェア
SSL-VPN クライアント	SSL-VPN を利用するために個人 PC にインストールされたソフトウェアモジュールである。証明書ストアに格納されたクライアント証明書を用いて処理を行う。VDI クライアントから localhost の TCP の 3389 番ポートへの接続を受け付け，SSL-VPN 装置にその通信を中継する。

SSL-VPN 装置の⑨ユーザテーブルは，SSL-VPN 接続時の処理に必要な情報が含まれるテーブルであり，仮想 PC の起動時に自動設定される。

SSL-VPN 装置の NAT テーブルは，SSL-VPN クライアントからの通信を適切な仮想 PC に振り向けるためのテーブルである。SSL-VPN 装置が SSL-VPN トンネルから VIP 宛てのパケットを受けると，適切な仮想 PC の IP アドレスに DNAT 処理して送る。この処理のために NAT テーブルがあり，SSL-VPN で認証処理中にエントリが作成される。

IP アドレスプールは，SSL-VPN クライアントに付与する IP アドレスのためのアドレスプールであり，172.16.3.1～172.16.3.254 を設定する。

P 主任が考えた，図 2 のテレワーク環境の VDI クライアントから仮想 PC までの接続シーケンスを図 3 に示す。

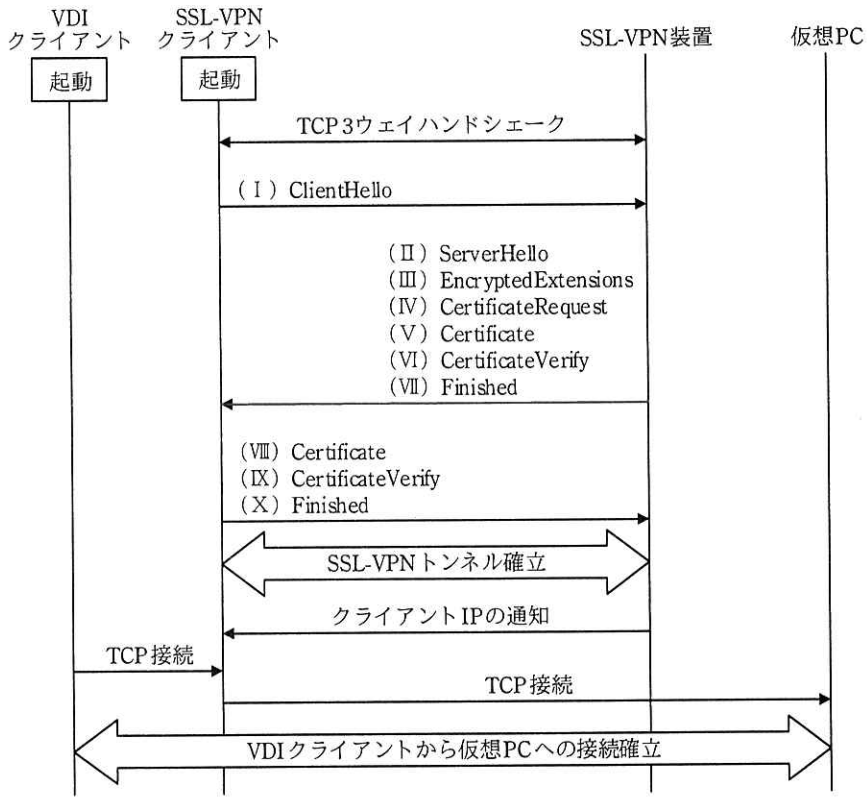


図 3　VDI クライアントから仮想 PC までの接続シーケンス（抜粋）

図 3 の動作の概要を次に示す。

(1) 個人 PC で SSL-VPN クライアントと VDI クライアントを起動する。

(2) SSL-VPN クライアントは，SSL-VPN 装置に対するアクセスを開始する。

(3) SSL-VPN 装置は，クライアント証明書による認証を行う。

(4) SSL-VPN クライアントと SSL-VPN 装置間に，TLS セッションが確立される。この TLS セッションは SSL-VPN トンネルとして利用する。

(5) SSL-VPN 装置は，SSL-VPN クライアントに割り当てる IP アドレスを管理するための IP アドレスプールから IP アドレスを割り当て，SSL-VPN クライアントに通知する。この割り当てられた IP アドレスを，クライアント IP という。

(6) SSL-VPN 装置は，⑩ユーザテーブルを検索して得られる IP アドレスを用いて，NAT テーブルのエントリを作成する。

(7) SSL-VPN クライアントは，localhost:3389 の待ち受けを開始する。

(8) VDI クライアントは，localhost:3389 へ TCP 接続を行う。

(9) SSL-VPN クライアントは，SSL-VPN トンネルを通じて，VIP の 3389 番ポートへ向けての TCP 接続を開始する。

(10) SSL-VPN 装置は，VIP に届いた一連のパケットを DNAT 処理して仮想 PC に転送する。これによって，SSL-VPN クライアントと仮想 PC の間に TCP 接続が確立する（以下，この接続をリモート接続という）。

(11) SSL-VPN クライアントは，localhost:3389 とリモート接続の間のデータ中継を行う。

上記の (1)〜(11) によって，VDI クライアントから仮想 PC までの接続が確立し，個人 PC から仮想 PC のデスクトップ環境が利用可能になる。

〔ネットワーク冗長化の検討〕

次に P 主任は，次のようにネットワークの冗長化を考えた。P 主任が考えた新たな冗長化構成を図 4 に示す。

・PC と業務サーバの間のネットワーク機器のうち，PC を収容する L2SW 以外の機器障害時に，PC から業務サーバの利用に影響がないようにする。

・拠点間接続の冗長化のために，新たに N 社の広域イーサネットを契約する。その回線速度と接続トポロジは現行の M 社広域イーサネットと同等とする。

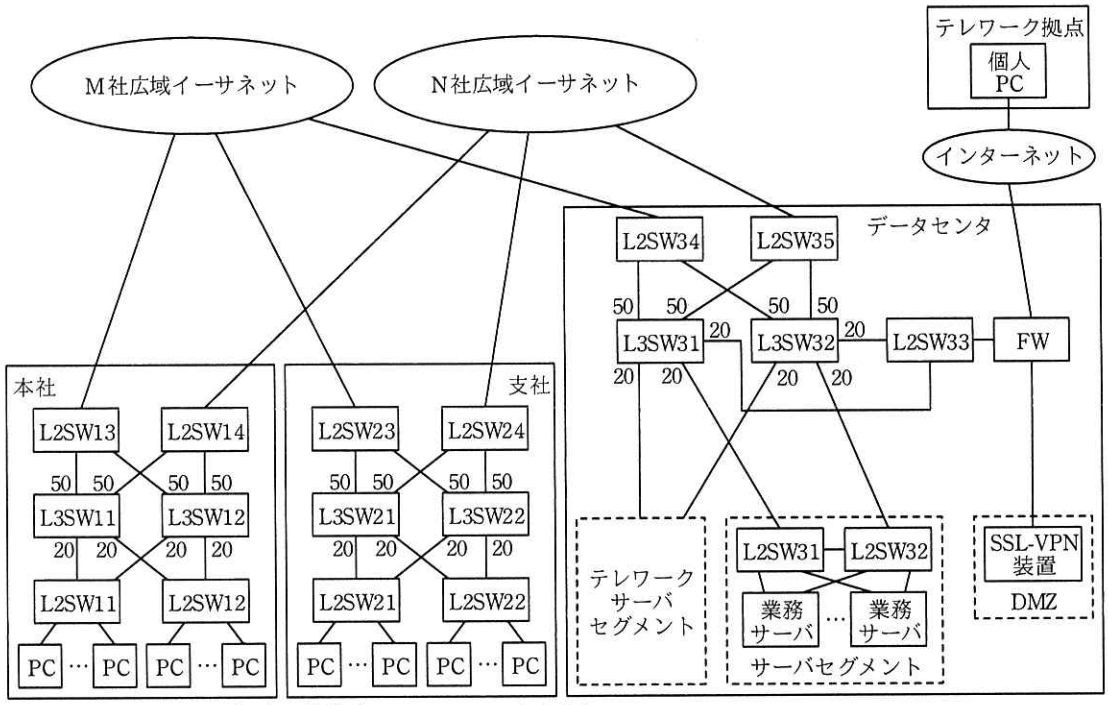
・通常は，M 社と N 社の広域イーサネットの両方を利用する。

・本社に L2SW13，L2SW14，L3SW12，支社に L2SW23，L2SW24，L3SW22，データセンタに L2SW32〜L2SW35，L3SW32 を新たに導入する。

・業務サーバの NIC はチーミングを行う。

・サーバセグメントに接続されている L3SW は VRRP によって冗長化を行う。

・ネットワーク全体の経路制御はこれまでどおり，OSPF を利用し，OSPF エリアは全体でエリア 0 とする。



注記　図中の L3SW のポートの数値は，OSPF のコストを示す。

図 4　P 主任が考えた新たな冗長化構成（抜粋）

全ての L3SW で OSPF を動作させ，冗長経路の OSPF のコストを適切に設定することによって，⑪ OSPF の Equal Cost Multi-path 機能（以下，ECMP という）が利用できると考え，図 4 に示すコスト設定を行うことにした。その場合，例えば⑫ L3SW11 のルーティングテーブル上には，サーバセグメントへの同一コストの複数の経路が確認できる。

K 社で利用している L3SW のベンダに ECMP の経路選択の仕様を問い合わせたところ，次の仕様であることが分かった。

・最大で四つの同一コストルートまでサポートする。
・動作モードとして，パケットモードとフローモードがある。
・パケットモードの場合，パケットごとにランダムに経路を選択し，フローモードの場合は，送信元 IP アドレスと宛先 IP アドレスからハッシュ値を計算して経路選択を行う。

P 主任は，K 社の社内の PC と業務サーバ間の通信における⑬通信品質への影響を考慮して，フローモードを選択することにした。また，フローモードでも⑭複数回

線の利用率がほぼ均等になると判断した。

次に，P 主任は，サーバセグメントに接続されている L3SW の冗長化について，図5のように行うことにした。

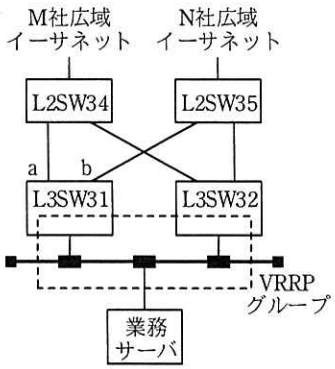


図5　サーバセグメントに接続されている L3SW の冗長化

図5において，L3SW31 と L3SW32 で VRRP を構成し，L3SW31 が VRRP マスタとなるように優先度を設定する。また，L3SW31 において，⑮図5中の a 又は b での障害をトラッキングするように VRRP の設定を行う。これによって，a 又は b のインタフェースでリンク障害が発生した場合でも，業務サーバから PC へのトラフィックの分散が損なわれないと考えた。

P 主任は，以上の技術項目の検討結果について情報システム部長に報告し，SSL-VPN 導入，N 社と S 社サービス利用及びネットワーク冗長化について承認された。

設問1　本文中の［　ア　］～［　カ　］に入れる適切な字句を答えよ。

設問2　〔SSL-VPN 技術調査とテレワーク環境への適用〕について，(1)，(2) に答えよ。

(1) 本文中の下線①について，同時に行われる二つのセキュリティ処理を答えよ。

(2) 本文中の下線②について，電子証明書において識別用情報を示すフィールドは何か。フィールド名を答えよ。

設問3　〔SSL-VPN クライアント認証方式の検討〕について，(1)～(6) に答えよ。

(1) 本文中の下線③について，クライアント証明書で送信元の身元を一意に特

定できる理由を，“秘密鍵”という用語を用いて 40 字以内で述べよ。

(2) 本文中の下線④について，クライアント証明書の検証のために，あらかじめ SSL-VPN 装置にインストールしておくべき情報を答えよ。

(3) 本文中の下線⑤について，検証によって低減できるリスクを，35 字以内で答えよ。

(4) 本文中の下線⑥について，TLS1.3 で規定されている鍵交換方式に比べて，広く復号されてしまう通信の範囲に含まれるデータは何か。“秘密鍵”と“漏えい”という用語を用いて，25 字以内で答えよ。

(5) 本文中の下線⑦について，利用者が CA サービスに CSR を提出するときに署名に用いる鍵は何か。また，CA サービスが CSR の署名の検証に用いる鍵は何か。本文中の用語を用いてそれぞれ答えよ。

(6) 本文中の下線⑧について，証明書失効リストに含まれる，証明書を一意に識別することができる情報は何か。その名称を答えよ。

設問 4 〔テレワーク環境構成の検討〕について，(1)，(2) に答えよ。

(1) 本文中の下線⑨について，ユーザテーブルに含まれる情報を 40 字以内で答えよ。

(2) 本文中の下線⑩について，検索のキーとなる情報はどこから得られるどの情報か。25 字以内で答えよ。また，SSL-VPN 装置は，その情報をどのタイミングで得るか。図 3 中の (I)～(X) の記号で答えよ。

設問 5 〔ネットワーク冗長化の検討〕について，(1)～(5) に答えよ。

(1) 本文中の下線⑪について，P 主任が ECMP の利用を前提にしたコスト設定を行う目的を，30 字以内で答えよ。

(2) 本文中の下線⑫について，経路数とそのコストをそれぞれ答えよ。

(3) 本文中の下線⑬について，フローモードの方が通信品質への影響が少ないと判断した理由を 35 字以内で述べよ。

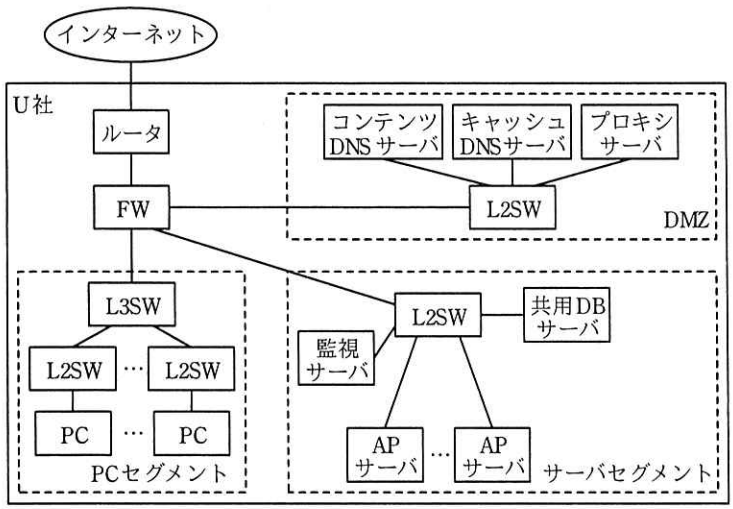
(4) 本文中の下線⑭について，利用率がほぼ均等になると判断した理由を L3SW の ECMP の経路選択の仕様に照らして，45 字以内で述べよ。

(5) 本文中の下線⑮について，この設定による VRRP の動作を“優先度”という用語を用いて 40 字以内で述べよ。

問2　仮想化技術の導入に関する次の記述を読んで，設問1～5に答えよ。

U社は社員3,000人の総合商社である。U社では多くの商材を取り扱っており，商材ごとに様々なアプリケーションシステム（以下，APという）を構築している。APは個別の物理サーバ（以下，APサーバという）上で動作している。U社の事業拡大に伴ってAPの数が増えており，主管部署であるシステム開発部はサーバの台数を減らすなど運用改善をしたいと考えていた。そこで，システム開発部では，仮想化技術を用いてサーバの台数を減らすことにし，Rさんを担当者として任命した。

現在のU社ネットワーク構成を図1に示す。



FW：ファイアウォール　L2SW：レイヤ2スイッチ　L3SW：レイヤ3スイッチ
DB：データベース
注記　ルータ，FW，L2SW，L3SW，コンテンツDNSサーバ，キャッシュDNSサーバ，プロキシサーバ，共用DBサーバ，監視サーバは冗長構成であるが，図では省略している。

図1　現在のU社ネットワーク構成（抜粋）

現在のU社ネットワーク構成の概要を次に示す。

・DMZ，サーバセグメント，PCセグメントにはプライベートIPアドレスを付与している。

・キャッシュDNSサーバは，社員が利用するPCやサーバからの問合せを受け，ほかのDNSサーバへ問い合わせた結果，得られた情報を応答する。

・コンテンツDNSサーバは，PCやサーバのホスト名などを管理し，PCやサーバな

どに関する情報を応答する。

・プロキシサーバは，PC からインターネット向けの HTTP 通信及び HTTPS（HTTP over TLS）通信をそれぞれ中継する。

・AP は，共用 DB サーバにデータを保管している。共用 DB サーバは，事業拡大に必要な容量と性能を確保している。

・AP ごとに 2 台の AP サーバで冗長構成としている。

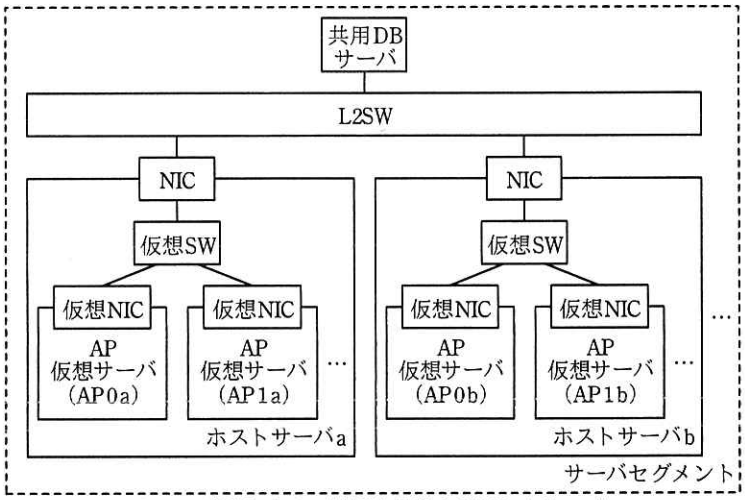
・AP サーバ上で動作する多くの AP は，HTTP 通信を利用して PC からアクセスされる AP（以下，WebAP という）であるが，TCP/IP を使った独自のプロトコルを利用して PC からアクセスされる AP（以下，専用 AP という）もある。

・監視サーバは，DMZ やサーバセグメントにあるサーバの監視を行っている。

〔サーバ仮想化技術を利用した AP の構成〕

R さんは，WebAP と専用 AP の 2 種類の AP について，サーバ仮想化技術の利用を検討した。サーバ仮想化技術では，物理サーバ上で複数の仮想的なサーバを動作させることができる。

R さんが考えたサーバ仮想化技術を利用した AP の構成を図 2 に示す。



AP仮想サーバ：APが動作する，仮想化技術を利用したサーバ
ホストサーバ：複数のAP仮想サーバを収容する物理サーバ
仮想SW：仮想L2SW　　NIC：ネットワークインタフェースカード
注記　（ ）内はAP仮想サーバ名を示し，AP名とそのAP仮想サーバが動作するホストサーバの識別子で構成する。一例として，AP0a は，AP 名がAP0 の AP が動作する，ホストサーバ a 上の AP 仮想サーバ名である。

図 2　サーバ仮想化技術を利用した AP の構成

ホストサーバでは，サーバ仮想化を実現するためのソフトウェアである［　ア　］が動作する。ホストサーバは仮想 SW をもち，NIC を経由して L2SW と接続する。

AP 仮想サーバは，ホストサーバ上で動作する仮想サーバとして構成する。AP 仮想サーバの仮想 NIC は仮想 SW と接続する。

一つの AP は 2 台の AP 仮想サーバで構成する。2 台の AP 仮想サーバでは，冗長構成をとるために VRRP バージョン 3 を動作させる。サーバセグメントでは複数の AP が動作するので，VRRP の識別子として AP ごとに異なる［　イ　］を割り当てる。①可用性を確保するために，VRRP を構成する 2 台の AP 仮想サーバは，異なるホストサーバに収容するように設計する。

VRRP の規格では，最大［　ウ　］組の仮想ルータを構成することができる。また，②マスタとして動作している AP 仮想サーバが停止すると，バックアップとして動作している AP 仮想サーバがマスタに切り替わる。

一例として，AP 仮想サーバ（AP0a）と AP 仮想サーバ（AP0b）とで構成される，AP 名が AP0 の IP アドレス割当表を表 1 に示す。

表 1　AP0 の IP アドレス割当表

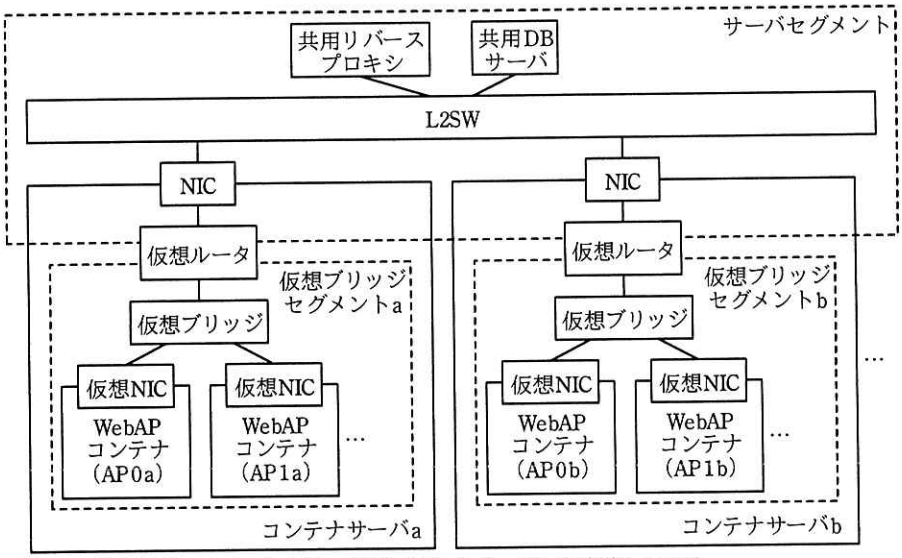
割当対象	IP アドレス
AP0a と AP0b の VRRP 仮想ルータ	192.168.0.16/22
AP0a の仮想 NIC	192.168.0.17/22
AP0b の仮想 NIC	192.168.0.18/22

AP ごとに，AP 仮想サーバの仮想 NIC で利用する二つの IP アドレスと VRRP 仮想ルータで利用する仮想 IP アドレスの計三つの IP アドレスの割当てと，一つの FQDN の割当てを行う。AP ごとに，コンテンツ DNS サーバにリソースレコードの一つである［　エ　］レコードとして VRRP で利用する仮想 IP アドレスを登録し，FQDN と IP アドレスの紐付(ひも)けを定義する。PC にインストールされている Web ブラウザ及び専用クライアントソフトウェアは，DNS の［　エ　］レコードを参照して接続する AP の IP アドレスを決定する。

〔コンテナ仮想化技術を利用した WebAP の構成〕

次に，R さんはコンテナ仮想化技術の利用を検討した。WebAP と専用 AP に分け，まずは WebAP について利用を検討した。コンテナ仮想化技術では，ある OS 上で仮想的に分離された複数のアプリケーションプログラム実行環境を用意し，複数の AP を動作させることができる。

R さんが考えた，コンテナ仮想化技術を利用した WebAP（以下，WebAP コンテナという）の構成を図 3 に示す。



注記 1　共用リバースプロキシは冗長構成であるが，図では省略している。
注記 2　（ ）内は WebAP コンテナ名を示し，AP 名とその WebAP コンテナが動作するコンテナサーバの識別子で構成する。一例として，AP0a は，AP 名が AP0 の AP が動作する，コンテナサーバ a 上の WebAP コンテナ名である。

図 3　WebAP コンテナの構成

コンテナサーバでは，コンテナ仮想化技術を実現するためのソフトウェアが動作する。コンテナサーバは仮想ブリッジ，仮想ルータをもち，NIC を経由して L2SW と接続する。WebAP コンテナの仮想 NIC は仮想ブリッジと接続する。

WebAP コンテナは，仮想ルータの上で動作する NAPT 機能と TCP や UDP のポートフォワード機能を利用して，PC や共用 DB サーバなどといった外部のホストと通信する。コンテナサーバ内の仮想ブリッジセグメントには，新たに IP アドレスを付与する必要があるので，プライベート IP アドレスの未使用空間から割り当てる。ま

た，③複数ある全ての仮想ブリッジセグメントには，同じ IP アドレスを割り当てる。

WebAP コンテナには，AP ごとに一つの FQDN を割り当て，コンテンツ DNS サーバに登録する。

WebAP コンテナでは，AP の可用性を確保するために，共用リバースプロキシを新たに構築して利用する。共用リバースプロキシは負荷分散機能をもつ HTTP リバースプロキシとして動作し，クライアントからの HTTP リクエストを受け，④ヘッダフィールド情報から WebAP を識別し，WebAP が動作する WebAP コンテナへ HTTP リクエストを振り分ける。振り分け先である WebAP コンテナは複数指定することができる。振り分け先を増やすことによって，WebAP の処理能力を向上させることができ，また，個々の WebAP コンテナの処理量を減らして負荷を軽減できる。

共用リバースプロキシ，コンテナサーバには，サーバセグメントの未使用のプライベート IP アドレスを割り当てる。共用リバースプロキシ，コンテナサーバの IP アドレス割当表を表 2 に，コンテナサーバ a で動作する仮想ブリッジセグメント a の IP アドレス割当表を表 3 に示す。

表 2　共用リバースプロキシ，コンテナサーバの IP アドレス割当表（抜粋）

割当対象	IP アドレス
共用リバースプロキシ	192.168.0.98/22
コンテナサーバ a	192.168.0.112/22
コンテナサーバ b	192.168.0.113/22

表 3　仮想ブリッジセグメント a の IP アドレス割当表（抜粋）

割当対象	IP アドレス
仮想ルータ	172.16.0.1/24
WebAP コンテナ（AP0a）	172.16.0.16/24
WebAP コンテナ（AP1a）	172.16.0.17/24

共用リバースプロキシは，振り分け先である WebAP コンテナが正常に稼働しているかどうかを確認するためにヘルスチェックを行う。ヘルスチェックの結果，正常な WebAP コンテナは振り分け先として利用され，異常がある WebAP コンテナは振り分け先から外される。振り分けルールの例を表 4 に示す。

表 4　振り分けルールの例（抜粋）

AP 名	（設問のため省略）	WebAP コンテナ名	振り分け先
AP0	ap0.u-sha.com	AP0a	192.168.0.112:8000
		AP0b	192.168.0.113:8000
AP1	ap1.u-sha.com	AP1a	192.168.0.112:8001
		AP1b	192.168.0.113:8001

PC が，表 4 中の AP0 と行う通信の例を次に示す。

(1) PC の Web ブラウザは，http://ap0.u-sha.com/へのアクセスを開始する。

(2) PC は DNS を参照して，ap0.u-sha.com の接続先 IP アドレスとして［　オ　］を取得する。

(3) PC は宛先 IP アドレスが［　オ　］，宛先ポート番号が 80 番宛てへ通信を開始する。

(4) PC からのリクエストを受けた共用リバースプロキシは振り分けルールに従って振り分け先を決定する。

(5) 共用リバースプロキシは宛先 IP アドレスが 192.168.0.112，宛先ポート番号が［　カ　］番宛てへ通信を開始する。

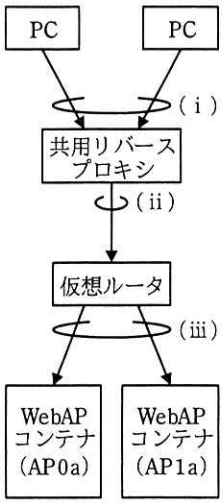
(6) 仮想ルータは宛先 IP アドレスが 192.168.0.112，宛先ポート番号が［　カ　］番宛てへの通信について，⑤ポートフォワードの処理によって宛先 IP アドレスと宛先ポート番号を変換する。

(7) WebAP コンテナ AP0a はコンテンツ要求を受け付け，対応するコンテンツを応答する。

(8) 共用リバースプロキシはコンテンツ応答を受け，PC に対応するコンテンツを応答する。

(9) PC はコンテンツ応答を受ける。

WebAP コンテナである AP0a と AP1a に対する PC からの HTTP 接続要求パケットの例を図 4 に示す。



（i）の箇所で通信が確認できるHTTP接続要求パケット

送信元IPアドレス	送信元ポート番号	宛先IPアドレス	宛先ポート番号
192.168.145.68	30472	192.168.0.98	80
192.168.145.154	31293	192.168.0.98	80

（ii）の箇所で通信が確認できるHTTP接続要求パケット

送信元IPアドレス	送信元ポート番号	宛先IPアドレス	宛先ポート番号
192.168.0.98	54382	192.168.0.112	8000
192.168.0.98	34953	192.168.0.112	8001

（iii）の箇所で通信が確認できるHTTP接続要求パケット

送信元IPアドレス	送信元ポート番号	宛先IPアドレス	宛先ポート番号
192.168.0.98	54382	172.16.0.16	80
192.168.0.98	34953	172.16.0.17	80

注記 ⟶ は，通信の方向を示す。

図4　AP0a と AP1a に対する PC からの HTTP 接続要求パケットの例

〔コンテナ仮想化技術を利用した専用 AP の構成〕

R さんは，専用 AP は TCP/IP を使った独自のプロトコルを利用するので，HTTP 通信を利用する WebAP と比較して，通信の仕方に不明な点が多いと感じた。そこで，コンテナ仮想化技術を導入した際の懸念点について上司の O 課長に相談した。次は，コンテナ仮想化技術を利用した専用 AP（以下，専用 AP コンテナという）に関する，R さんと O 課長の会話である。

R さん：専用 AP ですが，AP サーバ上で動作する専用 AP と同じように，専用 AP コンテナとして動作させることができたとしても，⑥PC や共用 DB サーバなどといった外部のホストとの通信の際に，仮想ルータのネットワーク機能を使用しても専用 AP が正常に動作することを確認する必要があると考えています。

O 課長：そうですね。専用 AP は AP ごとに通信の仕方が違う可能性があります。AP サーバと専用 AP コンテナの構成の違いによる影響を受けないことを確認する必要がありますね。それと，⑦同じポート番号を使用する専用 AP が幾つかあるので，これらの専用 AP に対応できる負荷分散機能をもつ製品が必要になります。

R さん：分かりました。

R さんは専用 AP で利用可能な負荷分散機能をもつ製品の調査をし，WebAP と併せて検討結果を取りまとめ，O 課長に報告した。

R さんが，サーバの台数を減らすなど運用改善のために検討したまとめを次に示す。

・第一に，リソースの無駄が少ないことやアプリケーションプログラムの起動に要する時間を短くできる特長を生かすために，コンテナ仮想化技術の利用を進め，順次移行する。
・第二に，コンテナ仮想化技術の利用が適さない AP については，サーバ仮想化技術の利用を進め，順次移行する。
・第三に，移行が完了したら AP サーバは廃止する。

〔監視の検討〕

次に，R さんが考えた，監視サーバによる図 3 中の機器の監視方法を表 5 に示す。

表 5　図 3 中の機器の監視方法（抜粋）

項番	監視種別	監視対象	設定値
1	ping 監視	共用リバースプロキシ	192.168.0.98
2		コンテナサーバ a	192.168.0.112
3		コンテナサーバ b	192.168.0.113
4	TCP 接続監視	WebAP コンテナ（AP0a）	192.168.0.112:8000
5		WebAP コンテナ（AP0b）	192.168.0.113:8000
6	URL 接続監視	共用リバースプロキシ	http://ap0.u-sha.com:80/index.html
7		WebAP コンテナ（AP0a）	http://192.168.0.112:8000/index.html
8		WebAP コンテナ（AP0b）	http://192.168.0.113:8000/index.html

監視サーバは 3 種類の監視を行うことができる。ping 監視は，監視サーバが監視対象の機器に対して ICMP のエコー要求を送信し，一定時間以内に［　キ　］を受信するかどうかで，IP パケットの到達性があるかどうかを確認する。TCP 接続監視では，監視サーバが監視対象の機器に対して SYN パケットを送信し，一定時間以内に［　ク　］パケットを受信するかどうかで，TCP で通信ができるかどうかを確認す

る。URL 接続監視では，監視サーバが監視対象の機器に対して HTTP［　ケ　］メソッドでリソースを要求し，一定時間以内にリソースを取得できるかどうかで HTTP サーバが正常稼働しているかどうかを確認する。ping 監視で WebAP コンテナの稼働状態を監視することはできない。⑧表 5 のように複数の監視を組み合わせることによって，監視サーバによる障害検知時に，監視対象の状態を推測することができる。

〔移行手順の検討〕

R さんは，コンテナ仮想化技術を利用した WebAP の移行手順を検討した。

2 台の AP サーバで構成する AP0 を，WebAP コンテナ（AP0a）と WebAP コンテナ（AP0b）へ移行することを例として，WebAP の移行途中の構成を図 5 に，WebAP の移行手順を表 6 に示す。

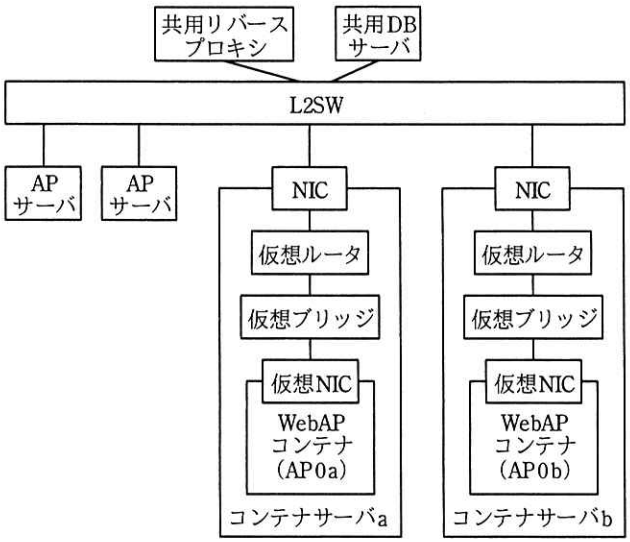


図 5　WebAP の移行途中の構成（抜粋）

表 6　WebAP の移行手順

項番	概要	内容
1	WebAP コンテナの構築	コンテナサーバ上に WebAP コンテナを構築する。
2	共用リバースプロキシの設定	WebAP コンテナに合わせて振り分けルールの設定を行う。
3	WebAP コンテナ監視登録	監視サーバに WebAP コンテナの監視を登録する。
4	動作確認	⑨テスト用の PC を用いて動作確認を行う。
5	DNS 切替え	DNS レコードを書き換え，AP サーバから WebAP コンテナへ切り替える。
6	AP サーバ監視削除	監視サーバから AP サーバの監視を削除する。
7	AP サーバの停止	⑩停止して問題ないことを確認した後に AP サーバを停止する。

R さんは表 6 の WebAP の移行手順を O 課長に報告した。次は，WebAP の移行手順に関する，O 課長と R さんの会話である。

O 課長：今回の移行は AP サーバと WebAP コンテナを並行稼働させて DNS レコードの書換えによって切り替えるのだね。

R さん：そうです。同じ動作をするので，DNS レコードの書換えが反映されるまでの並行稼働期間中，AP サーバと WebAP コンテナ，どちらにアクセスが行われても問題ありません。

O 課長：分かりました。並行稼働期間を短くするために DNS 切替えの事前準備は何があるかな。

R さん：はい。⑪あらかじめ，DNS の TTL を短くしておく方が良いですね。

O 課長：そうですね。移行手順に記載をお願いします。

R さん：分かりました。

O 課長：動作確認はどのようなことを行うか詳しく教えてください。

R さん：はい。WebAP コンテナ 2 台で構成する場合は，⑫次の 3 パターンそれぞれで AP の動作確認を行います。一つ目は，全ての WebAP コンテナが正常に動作している場合，二つ目は，2 台のうち 1 台目だけ WebAP コンテナが停止している場合，最後は，2 台目だけ WebAP コンテナが停止している場合です。また，障害検知の結果から，正しく監視登録されたことの確認も行います。

O 課長：分かりました。良さそうですね。

AP を，仮想化技術を利用したコンテナサーバやホストサーバに移行することによって期待どおりにサーバの台数を減らせる目途が立ち，システム開発部では仮想化技術の導入プロジェクトを開始した。

設問１　〔サーバ仮想化技術を利用した AP の構成〕について，(1)～(3) に答えよ。

(1) 本文中の［　ア　］～［　エ　］に入れる適切な字句又は数値を答えよ。

(2) 本文中の下線①について，2 台の AP 仮想サーバを同じホストサーバに収容した場合に起きる問題を可用性確保の観点から 40 字以内で述べよ。

(3) 本文中の下線②について，マスタが停止したとバックアップが判定する条件を 50 字以内で述べよ。

設問２　〔コンテナ仮想化技術を利用した WebAP の構成〕について，(1)～(4) に答えよ。

(1) 本文中の下線③について，複数ある全ての仮想ブリッジセグメントで同じ IP アドレスを利用して問題ない理由を 40 字以内で述べよ。

(2) 本文中の下線④について，共用リバースプロキシはどのヘッダフィールド情報から WebAP を識別するか。15 字以内で答えよ。

(3) 本文中の［　オ　］に入れる適切な IP アドレス，及び［　カ　］に入れる適切なポート番号を答えよ。

(4) 本文中の下線⑤について，変換後の宛先 IP アドレスと宛先ポート番号を答えよ。

設問３　〔コンテナ仮想化技術を利用した専用 AP の構成〕について，(1)，(2) に答えよ。

(1) 本文中の下線⑥について，専用 AP ごとに確認が必要な仮想ルータのネットワーク機能を二つ答えよ。

(2) 本文中の下線⑦について，どのような仕組みが必要か。40 字以内で答えよ。

設問４　〔監視の検討〕について，(1)～(3) に答えよ。

(1) 本文中の［　キ　］～［　ケ　］に入れる適切な字句を答えよ。

(2) 本文中の下線⑧について，表 5 中の項番 2，項番 4，項番 7 で障害検知し，それ以外は正常の場合，どこに障害が発生していると考えられるか。表 5 中の字句を用いて障害箇所を答えよ。

(3) 本文中の下線⑧について，表5中の項番4，項番7で障害検知し，それ以外は正常の場合，どこに障害が発生していると考えられるか。表5中の字句を用いて障害箇所を答えよ。

設問5　〔移行手順の検討〕について，(1)～(4)に答えよ。

(1) 表6中の下線⑨について，WebAPコンテナで動作するAPの動作確認を行うために必要になる，テスト用のPCの設定内容を，DNS切替えに着目して40字以内で述べよ。

(2) 表6中の下線⑩について，APサーバ停止前に確認する内容を40字以内で述べよ。

(3) 本文中の下線⑪について，TTLを短くすることによって何がどのように変化するか。40字以内で述べよ。

(4) 本文中の下線⑫について，3パターンそれぞれでAPの動作確認を行う目的を二つ挙げ，それぞれ35字以内で述べよ。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 退室可能時間中に退室する場合は，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

7. **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。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，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，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 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。
12. 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。