NW

令和５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〕

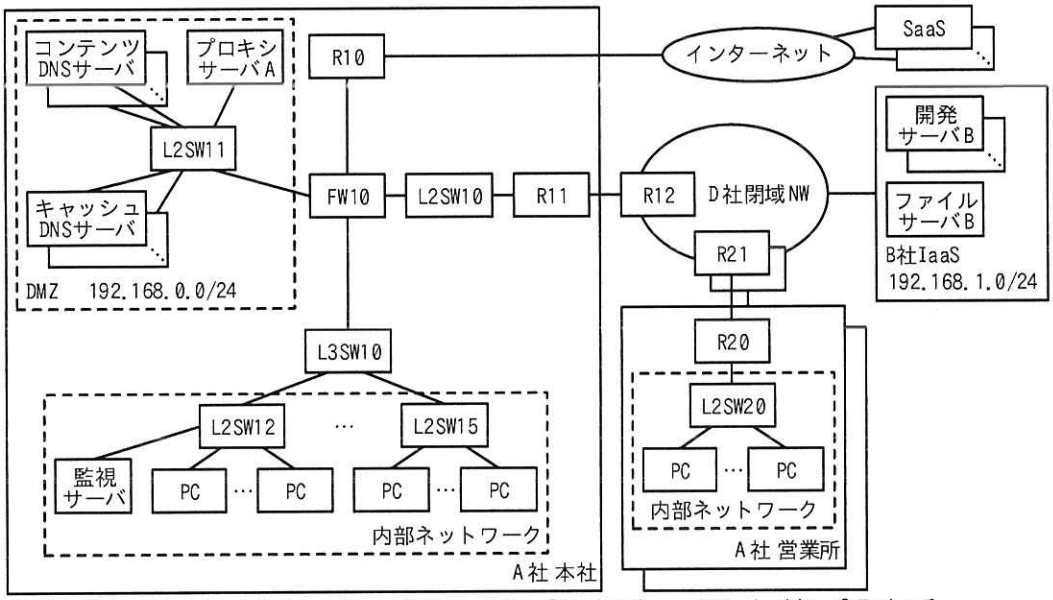
選択欄	
１問選択	問１
	(問２)

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　マルチクラウド利用による可用性向上に関する次の記述を読んで，設問に答えよ。

A 社は，従業員 500 人のシステム開発会社である。A 社では，IaaS を積極的に活用して開発業務を行ってきたが，利用している IaaS 事業者である B 社で大規模な障害が発生し，開発業務に多大な影響を受けた。A 社のシステム部では，利用する IaaS 事業者をもう 1 社追加してマルチクラウド環境にし，本社を中心にネットワーク環境も含めた可用性向上に取り組むことになり，E さんを担当者として任命した。

現在の A 社のネットワーク構成を図 1 に示す。



R：ルータ　FW：ファイアウォール　L2SW：レイヤー２スイッチ　L3SW：レイヤー３スイッチ
D 社閉域 NW：回線事業者である D 社が提供する閉域ネットワークサービス

図 1　現在の A 社のネットワーク構成（抜粋）

図 1 の概要を次に示す。

・A 社は本社と 2 か所の営業所で構成されている。

・D 社閉域 NW を利用して，本社と 2 か所の営業所を接続している。R11 及び R20 といった A 社と D 社閉域 NW とを接続するルータは，D 社からネットワークサービスとして提供されている。

・D 社閉域 NW と B 社 IaaS は相互接続しており，A 社は D 社閉域 NW 経由で B 社 IaaS

を利用している。

・A 社ネットワークでは静的経路制御を利用している。

・B 社からは，Web ブラウザを利用した画面操作によって，IaaS 上に仮想ネットワーク，仮想サーバを簡単に構築できる管理コンソールが提供されている。

・A 社のシステム部は，受託した開発業務ごとに開発サーバ B を構築し，A 社の担当部門に引き渡している。開発サーバ B の運用管理は担当部門で実施する。

・システム部は，共用のファイルサーバ B を構築し，A 社の全部門に提供している。

・A 社の全部門で利用する電子メールやチャット，スケジューラーなどのオフィスアプリケーションソフトウェアはインターネット上の SaaS を利用している。これらの SaaS は HTTPS 通信を用いている。

・A 社の一部の部門では，担当する業務に応じてインターネット上の SaaS を独自に契約し，利用している。これらの SaaS では送信元 IP アドレスによってアクセス制限をしているものもある。これらの SaaS も HTTPS 通信を用いている。

・プロキシサーバ A は，従業員が利用する PC やサーバからインターネット向けの HTTP 通信，HTTPS 通信をそれぞれ中継する。従業員はプロキシサーバとして proxy.a-sha.co.jp を PC の Web ブラウザやサーバに指定している。

・A 社は，本社設置の R10 を経由してインターネットに接続している。FW10 にはグローバル IP アドレスを付与しており，FW10 を経由するインターネット宛ての通信は NAPT 機能によって IP アドレスとポート番号の変換が行われる。

・キャッシュ DNS サーバは，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を応答する。キャッシュ DNS サーバは複数台設置されている。

・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。コンテンツ DNS サーバは複数台設置されている。

・監視サーバは，ICMP を利用する死活監視（以下，ping 監視という）を用いて DMZ や IaaS にあるサーバの監視を行っている。監視サーバで検知された異常はシステム部の担当者に通知され，復旧作業などの必要な対応が行われる。

システム部では，ネットワーク環境の可用性向上の要件を次のとおりまとめた。

・新規に C 社の IaaS を契約し，B 社 IaaS と併せたマルチクラウド環境にし，D 社閉域 NW 経由で利用する。

・A 社本社と D 社閉域 NW との接続回線を追加し，マルチホーム接続とする。

・インターネット接続を本社経由から D 社閉域 NW 経由に切り替える。

可用性向上後の A 社のネットワーク構成を図 2 に示す。

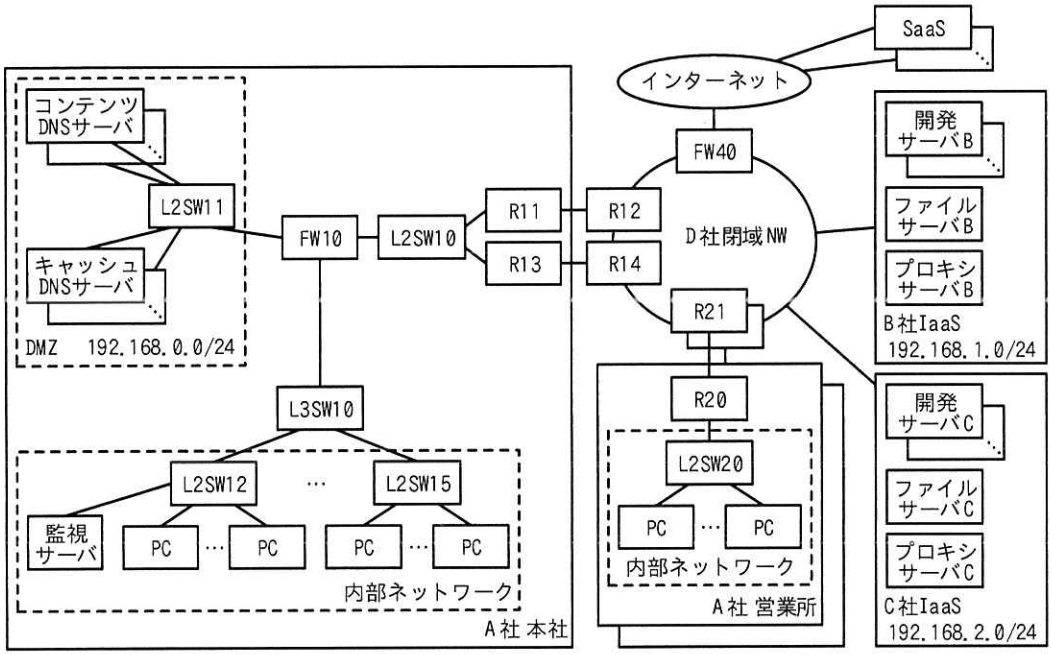


図 2　可用性向上後の A 社のネットワーク構成（抜粋）

〔B 社と C 社の IaaS 利用〕

C 社からも，B 社と同様に管理コンソールが提供されている。B 社 IaaS に構築された仮想ネットワーク，仮想サーバと C 社 IaaS に構築された仮想ネットワーク，仮想サーバは D 社閉域 NW を経由して相互に通信できる。

E さんは，B 社と C 社の IaaS 利用方針を次のとおり策定した。

・C 社 IaaS にファイルサーバ C を新たに構築し，ファイルサーバ B と常に同期をとるように設定する。A 社従業員はファイルサーバ B 又はファイルサーバ C を利用する。

・B 社 IaaS にプロキシサーバ B を，C 社 IaaS にプロキシサーバ C を新たに構築し，プロキシサーバ A から切り替える。

・B 社 IaaS を利用して開発サーバ B を，C 社 IaaS を利用して開発サーバ C を構築し，

A社の担当部門に引き渡す。

〔プロキシサーバの利用方法の検討〕

Eさんは，IaaSに構築するプロキシサーバBとプロキシサーバCの利用方法を検討した。プロキシサーバの利用方法の案を表1に示す。

表1　プロキシサーバの利用方法の案

案	概要
案1	平常時はプロキシサーバBを利用し，プロキシサーバBに障害が発生した際にはプロキシサーバCを利用するように切り替える。
案2	平常時からプロキシサーバB及びプロキシサーバCを利用し，片方に障害が発生した際には正常稼働しているもう片方を利用するように切り替える。

Eさんは，従業員が利用するプロキシサーバを，DNSの機能を利用して制御することを考えた。プロキシサーバに障害が発生した際には，DNSの機能を利用して切り替える。

プロキシサーバに関するDNSゾーンファイルの記述内容を表2に示す。

表2　プロキシサーバに関するDNSゾーンファイルの記述内容

	DNSゾーンファイルの記述内容
現在の設定	proxy.a-sha.co.jp.　IN A　192.168.0.145　；従業員が指定するホスト proxya.a-sha.co.jp.　IN A　192.168.0.145　；プロキシサーバAのホスト
案1の初期設定	proxy.a-sha.co.jp.　IN A　192.168.1.145　；従業員が指定するホスト proxya.a-sha.co.jp.　IN A　192.168.0.145　；プロキシサーバAのホスト proxyb.a-sha.co.jp.　IN A　192.168.1.145　；プロキシサーバBのホスト proxyc.a-sha.co.jp.　IN A　192.168.2.145　；プロキシサーバCのホスト
案2の初期設定	proxy.a-sha.co.jp.　IN A　192.168.1.145　；従業員が指定するホスト proxy.a-sha.co.jp.　IN A　192.168.2.145　；従業員が指定するホスト proxya.a-sha.co.jp.　IN A　192.168.0.145　；プロキシサーバAのホスト proxyb.a-sha.co.jp.　IN A　192.168.1.145　；プロキシサーバBのホスト proxyc.a-sha.co.jp.　IN A　192.168.2.145　；プロキシサーバCのホスト

注記 切替え期間中の設定を含む。

Eさんは，プロキシサーバの監視運用について検討した。監視サーバで利用できる①ping監視では不十分だと考え，新たにTCP監視機能を追加し，プロキシサーバのアプリケーションプロセスが動作するポート番号にTCP接続可能か監視することにし

た。また，監視対象として，従業員がプロキシサーバとして指定するホストに加えて，プロキシサーバ A，プロキシサーバ B，プロキシサーバ C のホストを設定することにした。

次に，監視サーバでプロキシサーバ B の異常を検知した際に，従業員がプロキシサーバの利用を再開できるようにするための復旧方法として，②DNS ゾーンファイルの変更内容を案 1，案 2 それぞれについて検討した。また，③平常時から proxy.a-sha.co.jp に関するリソースレコードの TTL の値を小さくすることにした。

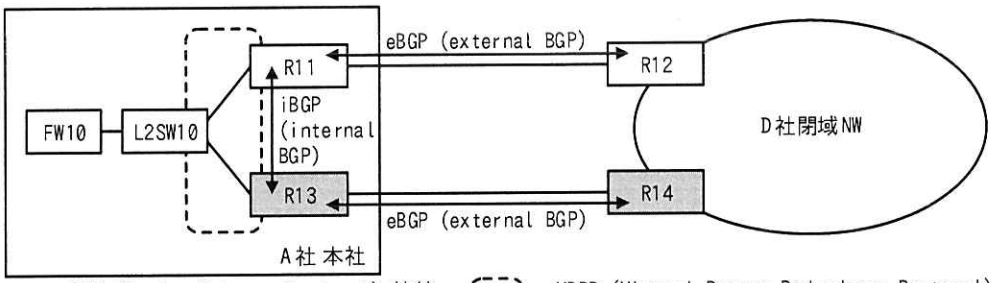
これらの検討の結果，プロキシサーバの負荷分散ができること，及びプロキシサーバの有効活用ができることから案 2 の方が優れていると考え，E さんは案 2 を採用することにした。

さらに，E さんは，自動でプロキシサーバを切り替えるために，④ DNS とは異なる方法で従業員が利用するプロキシサーバを切り替える方法も検討した。プロキシサーバを利用する側の環境に依存することから，DNS ゾーンファイルの書換えによる切替えと併用することにした。

〔マルチホーム接続〕

次に，E さんは D 社閉域 NW とのマルチホーム接続について検討した。A 社本社に増設するルータ及び回線は D 社からネットワークサービスとして提供される。マルチホーム接続の設計について D 社担当者から説明を受けた。

D 社担当者から説明を受けたマルチホーム接続構成を図 3 に示す。



注記　網掛け部分は，追加する機器を示す。

図 3　D 社担当者から説明を受けたマルチホーム接続構成（抜粋）

図3の概要は次のとおりである。

・本社とD社閉域NWとの間で，新たにR13と専用線がD社からネットワークサービスとして提供される。R11とR13とを併せてマルチホーム接続とする。

・増設する専用線の契約帯域幅は既設の専用線と同じにし，平常時は既設の専用線を利用し，障害発生時には増設する専用線を利用する。

・既存のR11とR12は，静的経路制御からBGPによる動的経路制御に変更する。

・R11とR12との間，R13とR14との間はeBGPで接続する。⑤ R11とR13との間はiBGPで接続し，あわせてnext-hop-self設定を行う。

・R11とR13との間ではVRRPを利用する。FW10はVRRPで定義する仮想IPアドレスをネクストホップとして静的経路設定を行う。

D社担当者からの説明を受けたEさんは，BGPについて調査した。

RFC 4271で規定されているBGPは，［ a ］間の経路交換のために作られたプロトコルで，TCPポート179番を利用して接続し，経路交換を行う。経路交換を行う隣接のルータを［ b ］と呼ぶ。BGPで交換されるメッセージは4タイプあり，表3に示す。

表3　BGPで交換されるメッセージ

タイプ	名称	説明
1	OPEN	BGP接続開始時に交換する。 自AS番号，BGPID，バージョンなどの情報を含む。
2	［ c ］	経路情報の交換に利用する。 経路の追加や削除が発生した場合に送信される。
3	NOTIFICATION	エラーを検出した場合に送信される。
4	［ d ］	BGP接続の確立やBGP接続の維持のために交換する。

経路制御は，［ c ］メッセージに含まれるBGPパスアトリビュートの一つであるLOCAL_PREFを利用して行うとの説明をD社担当者から受けた。LOCAL_PREFは，iBGPピアに対して通知する，外部のASに存在する宛先ネットワークアドレスの優先度を定義する。BGPでは，ピアリングで受信した経路情報をBGPテーブルとして構成し，最適経路選択アルゴリズムによって経路情報を一つだけ選択し，ルータの［ e ］に反映する。LOCAL_PREFの場合では，最も［ f ］値をもつ経路情

報が選択される。

また，E さんは，D 社担当者から静的経路制御から BGP による動的経路制御に構成変更する手順の説明を受けた。この時，⑥BGP の導入を行った後に VRRP の導入を行う必要があるとの説明だった。E さんが説明を受けた手順を表 4 に示す。

表 4　E さんが説明を受けた手順

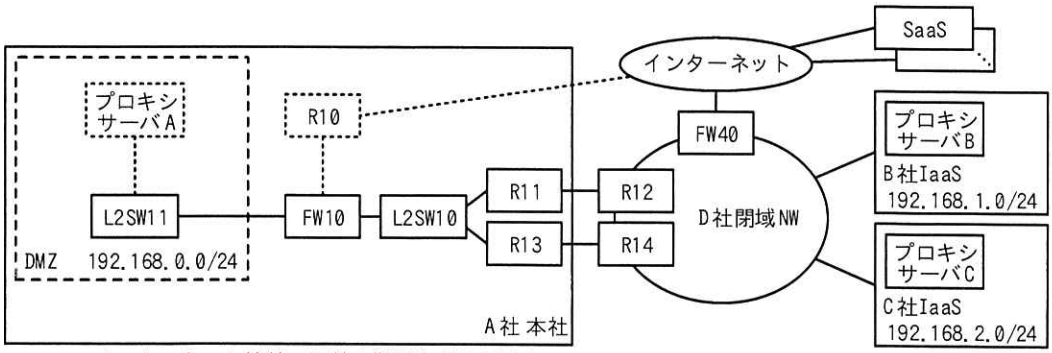
項番	作業内容
1	R13 及び R14 を増設する。
2	R13 と増設する専用線とを接続する。 R14 と増設する専用線とを接続する。 R13 と L2SW10 とを接続する。
3	R13 及び R14 のインタフェースに IP アドレスを設定する。
4	⑦増設した機器や回線に故障がないことを確認するために ping コマンドで試験を行う。
5	R11～R14 に BGP の設定を追加する。ただし，この時点では BGP 接続は確立しない。
6	全ての BGP 接続を確立させ，送受信する経路情報が正しいことを確認する。
7	⑧ R11 及び R12 の不要になる静的経路制御の経路情報を削除する。
8	R11 と R13 との間の VRRP で利用する新しい仮想 IP アドレスを割り当て，VRRP を構成する。
9	FW10 において VRRP で利用する仮想 IP アドレスをネクストホップとする静的経路制御の経路情報を設定する。
10	FW10 で不要になる静的経路制御の経路情報を削除する。

E さんは，設計どおりにマルチホームによる可用性向上が実現できたかどうかを確認するための障害試験を行うことにし，⑨想定する障害の発生箇所と内容を障害一覧としてまとめた。

〔インターネット接続の切替え〕

次に，E さんはインターネット接続を本社経由から D 社閉域 NW 経由へ切り替えることについて検討した。

インターネット接続の切替え期間中の構成を図 4 に示す。



------- ：インターネット接続の切替え期間中だけ利用する。

図4　インターネット接続の切替え期間中の構成（抜粋）

FW40 を使ってインターネット接続する。FW40 は D 社からネットワークサービスとして提供される。FW40 には新たにグローバル IP アドレスが割り当てられる。FW40 を経由するインターネット宛ての通信は NAPT 機能によって IP アドレスとポート番号の変換が行われる。A 社とインターネットとの通信を，R10 経由から FW40 経由になるようにインターネット接続を切り替える。

E さんは，設定変更の作業影響による通信断時間を極力短くするために，⑩ FW10 の設定変更は D 社閉域 NW の設定変更とタイミングを合わせて実施する必要があると考えた。

E さんは，⑪インターネット接続の切替えを行うと一部の部門で業務に影響があると考えた。対策として，全てのインターネット宛ての通信は FW40 経由へと切り替えるが，⑫一定期間，プロキシサーバ A からのインターネット宛ての通信だけは既存の R10 経由になるようにする。あわせて，E さんは，業務に影響がある一部の部門には切替え期間中はプロキシサーバ A が利用可能なことを案内するとともに，⑬恒久対応として設定変更の依頼を事前に行うことにした。

E さんは，プロキシサーバ A のログを定期的に調査し，利用がなくなったことを確認した後に，プロキシサーバ A を廃止することにした。

E さんが検討した可用性向上の検討案は承認され，システム部では可用性向上プロジェクトを開始した。

設問1　〔プロキシサーバの利用方法の検討〕について答えよ。

(1) 表2中の案2の初期設定について，負荷分散を目的として一つのドメイン名に対して複数のIPアドレスを割り当てる方式名を答えよ。

(2) 本文中の下線①について，ping監視では不十分な理由を40字以内で答えよ。

(3) 本文中の下線②について，表2の案1の初期設定を対象に，ドメイン名proxy.a-sha.co.jp.の書換え後のIPアドレスを答えよ。

(4) 本文中の下線③について，TTLの値を小さくする目的を40字以内で答えよ。

(5) 本文中の下線④について，DNSとは異なる方法を20字以内で答えよ。また，その方法の制限事項を，プロキシサーバを利用する側の環境に着目して25字以内で答えよ。

設問2　〔マルチホーム接続〕について答えよ。

(1) 本文中及び表3中の［ a ］～［ f ］に入れる適切な字句を答えよ。

(2) 本文中の下線⑤について，next-hop-self設定を行うと，iBGPで広告する経路情報のネクストホップのIPアドレスには何が設定されるか。15字以内で答えよ。

(3) 表3について，BGPピア間で定期的にやり取りされるメッセージを一つ選び，タイプで答えよ。また，そのメッセージが一定時間受信できなくなるとどのような動作をするか。30字以内で答えよ。

(4) 本文中の下線⑥について，BGPの導入を行った後にVRRPの導入を行うべき理由を，R13が何らかの理由でVRRPマスターになったときのR13の経路情報の状態を想定し，50字以内で答えよ。

(5) 表4中の下線⑦について，pingコマンドの試験で確認すべき内容を20字以内で答えよ。また，pingコマンドの試験で確認すべき送信元と宛先の組合せを二つ挙げ，図3中の機器名で答えよ。

(6) 表4中の下線⑧について，R11及びR12では静的経路制御の経路情報を削除することで同じ宛先ネットワークのBGPの経路情報が有効になる。その理由を40字以内で答えよ。

(7) 本文中の下線⑨について，想定する障害を六つ挙げ，それぞれの障害発生

箇所を答えよ。ただし，R12 と R14 については D 社で障害試験実施済みとする。

設問３　〔インターネット接続の切替え〕について答えよ。

(1)　本文中の下線⑩について，D 社閉域 NW の設定変更より前に FW10 のデフォルトルートの設定変更を行うとどのような状況になるか。25 字以内で答えよ。

(2)　本文中の下線⑪について，業務に影響が発生する理由を 20 字以内で答えよ。

(3)　本文中の下線⑫について，FW10 にどのようなポリシーベースルーティング設定が必要か。70 字以内で答えよ。

(4)　本文中の下線⑬について，どのような設定変更を依頼すればよいか。40 字以内で答えよ。

問2　EC サーバの増強に関する次の記述を読んで，設問に答えよ。

Y 社は，従業員 300 名の事務用品の販売会社であり，会員企業向けにインターネットを利用して通信販売を行っている。EC サイトは，Z 社のデータセンター（以下，z-DC という）に構築されており，Y 社の運用 PC を使用して運用管理を行っている。

EC サイトに関連するシステムの構成を図 1 に示し，DNS サーバに設定されているゾーン情報を図 2 に示す。

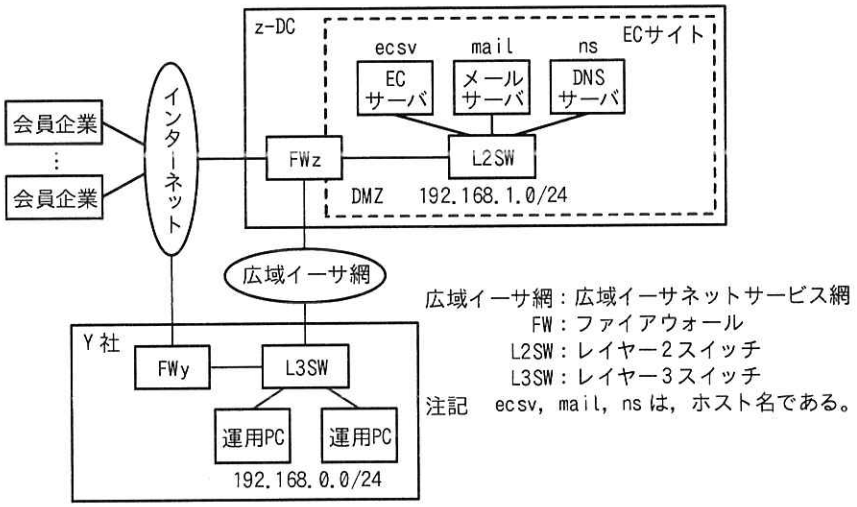


図 1　EC サイトに関連するシステムの構成（抜粋）

項番	ゾーン情報
1	@　IN　SOA　ns.example.jp.　hostmaster.example.jp.（省略）
2	IN　[a]　ns.example.jp.
3	IN　[b]　10　mail.example.jp.
4	ns　IN　A　[c]
5	ecsv　IN　A　（省略）
6	mail　IN　A　[d]
7	@　IN　SOA　ns.y-sha.example.lan.　hostmaster.y-sha.example.lan.（省略）
8	IN　[a]　ns.y-sha.example.lan.
9	IN　[b]　10　mail.y-sha.example.lan.
10	ns　IN　A　[e]
11	ecsv　IN　A　（省略）
12	mail　IN　A　[f]

図 2　DNS サーバに設定されているゾーン情報（抜粋）

〔EC サイトに関連するシステムの構成，運用及びセッション管理方法〕

・会員企業の事務用品購入の担当者（以下，購買担当者という）は，Web ブラウザで https://ecsv.example.jp/ を指定して EC サーバにアクセスする。

・運用担当者は，運用 PC の Web ブラウザで https://ecsv.y-sha.example.lan/ を指定して，広域イーサ網経由で EC サーバにアクセスする。

・EC サーバに登録されているサーバ証明書は一つであり，マルチドメインに対応していない。

・EC サーバは，アクセス元の IP アドレスなどをログとして管理している。

・DMZ の DNS サーバは，EC サイトのインターネット向けドメイン example.jp と，社内向けドメイン y-sha.example.lan の二つのドメインのゾーン情報を管理する。

・L3SW には，DMZ への経路とデフォルトルートが設定されている。

・運用 PC は，DMZ の DNS サーバで名前解決を行う。

・FWz には，表 1 に示す静的 NAT が設定されている。

表 1　FWz に設定されている静的 NAT の内容(抜粋)

変換前 IP アドレス	変換後 IP アドレス	プロトコル／宛先ポート番号
100.α.β.1	192.168.1.1	TCP/53，UDP/53
100.α.β.2	192.168.1.2	TCP/443
100.α.β.3	192.168.1.3	TCP/25

注記　100.α.β.1～100.α.β.3 は，グローバル IP アドレスを示す。

EC サーバは，次の方法でセッション管理を行っている。

・Web ブラウザから最初にアクセスを受けたときに，ランダムな値のセッション ID を生成する。

・Web ブラウザへの応答時に，Cookie にセッション ID を書き込んで送信する。

・Web ブラウザによる EC サーバへのアクセスの開始から終了までの一連の通信を，セッション ID を基に，同一のセッションとして管理する。

〔EC サイトの応答速度の低下〕

最近，購買担当者から，EC サイト利用時の応答が遅くなったというクレームが入るようになった。そこで，Y 社の情報システム部（以下，情シスという）のネットワ

ークチームのX主任は，運用PCを使用して次の手順で原因究明を行った。

(1) 購買担当者と同じURLでアクセスし，応答が遅いことを確認した。

(2) ecsv.example.jp及びecsv.y-sha.example.lan宛てに，それぞれpingコマンドを発行して応答時間を測定したところ，両者の測定結果に大きな違いはなかった。

(3) FWzのログからはサイバー攻撃の兆候は検出されなかった。

(4) sshコマンドで① ecsv.y-sha.example.lanにアクセスしてCPU使用率を調べたところ，設計値を大きく超えていた。

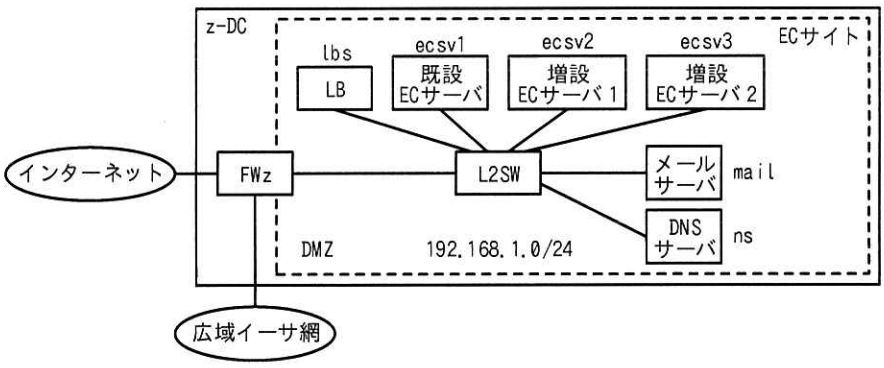
この結果から，X主任は，ECサーバが処理能力不足になったと判断した。

〔ECサーバの増強構成の設計〕

X主任は，ECサーバの増強が必要になったことを上司のW課長に報告し，W課長からECサーバの増強構成の設計指示を受けた。

EC サーバの増強策としてスケール［ g ］方式とスケール［ h ］方式を比較検討し，ECサイトを停止せずにECサーバの増強を行える，スケール［ h ］方式を採用することを考えた。

X主任は，② ECサーバを2台にすればECサイトは十分な処理能力をもつことになるが，2台増設して3台にし，負荷分散装置（以下，LBという）によって処理を振り分ける構成を設計した。ECサーバの増強構成を図3に示し，DNSサーバに追加する社内向けドメインのリソースレコードを図4に示す。



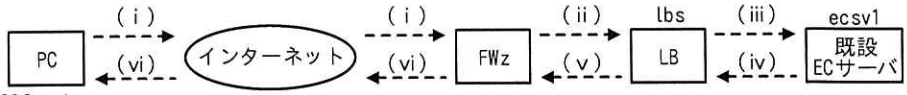
注記 lbsはLBのホスト名であり，ecsv1～ecsv3は増強後のECサーバのホスト名である。

図3 ECサーバの増強構成（抜粋）

lbs	IN	A	192.168.1.4	; LB の物理 IP アドレス
ecsv1	IN	A	192.168.1.5	; 既設 EC サーバの IP アドレス
ecsv2	IN	A	192.168.1.6	; 増設 EC サーバ 1 の IP アドレス
ecsv3	IN	A	192.168.1.7	; 増設 EC サーバ 2 の IP アドレス

図 4　DNS サーバに追加する社内向けドメインのリソースレコード

EC サーバ増強後，購買担当者が Web ブラウザで https://ecsv.example.jp/ を指定して EC サーバにアクセスし，アクセス先が既設 EC サーバに振り分けられたときのパケットの転送経路を図 5 に示す。



----→ : パケットの転送方向

注記　200.a.b.c は，グローバル IP アドレスを示す。

図 5　既設 EC サーバに振り分けられたときのパケットの転送経路

導入する LB には，負荷分散用の IP アドレスである仮想 IP アドレスで受信したパケットを EC サーバに振り分けるとき，送信元 IP アドレスを変換する方式（以下，ソース NAT という）と変換しない方式の二つがある。図 5 中の(i)～(vi)での IP ヘッダーの IP アドレスの内容を表 2 に示す。

表 2　図 5 中の(i)～(vi)での IP ヘッダーの IP アドレスの内容

図 5 中の番号	LB でソース NAT を行わない場合		LB でソース NAT を行う場合	
	送信元 IP アドレス	宛先 IP アドレス	送信元 IP アドレス	宛先 IP アドレス
(i)	200.a.b.c	i	200.a.b.c	i
(ii)	200.a.b.c	j	200.a.b.c	j
(iii)	200.a.b.c	192.168.1.5	k	192.168.1.5
(iv)	192.168.1.5	200.a.b.c	192.168.1.5	k
(v)	j	200.a.b.c	j	200.a.b.c
(vi)	i	200.a.b.c	i	200.a.b.c

〔EC サーバの増強構成と LB の設定〕

X 主任が設計した内容を W 課長に説明したときの，2 人の会話を次に示す。

X 主任 ：LB を利用して EC サーバを増強する構成を考えました。購買担当者が EC サーバにアクセスするときの URL の変更は不要です。

W 課長 ：DNS サーバに対しては，図 4 のレコードを追加するだけで良いのでしょうか。

X 主任 ：そうです。EC サーバの増強後も，図 2 で示したゾーン情報の変更は不要ですが，③図 2 中の項番 5 と項番 11 のリソースレコードは，図 3 の構成では図 1 とは違う機器の特別な IP アドレスを示すことになります。また，④図 4 のリソースレコードの追加に対応して，既設 EC サーバに設定されている二つの情報を変更します。

W 課長 ：分かりました。LB ではソース NAT を行うのでしょうか。

X 主任 ：現在の EC サーバの運用を変更しないために，ソース NAT は行わない予定です。この場合，パケットの転送を図 5 の経路にするために，⑤既設 EC サーバでは，デフォルトゲートウェイの IP アドレスを変更します。

W 課長 ：次に，EC サーバのメンテナンス方法を説明してください。

X 主任 ：はい。まず，メンテナンスを行う EC サーバを負荷分散の対象から外し，その後に，運用 PC から当該 EC サーバにアクセスして，メンテナンス作業を行います。

W 課長 ：X 主任が考えている設定では，運用 PC から EC サーバとは通信できないと思いますが，どうでしょうか。

X 主任 ：うっかりしていました。導入予定の LB はルータとしては動作しませんから，ご指摘の問題が発生してしまいます。対策方法として，EC サーバに設定するデフォルトゲートウェイを図 1 の構成時のままとし，LB ではソース NAT を行うとともに，⑥ EC サーバ宛てに送信する HTTP ヘッダーに X-Forwarded-For フィールドを追加するようにします。

W 課長 ：それで良いでしょう。ところで，図 3 の構成では，増設 EC サーバにもサーバ証明書をインストールすることになるのでしょうか。

X 主任 ：いいえ。増設 EC サーバにはインストールせずに⑦既設 EC サーバ内のサーバ証明書の流用で対応できます。

W 課長 ：分かりました。負荷分散やセッション維持などの方法は設計済みでしょう

か。

X主任：構成が決まりましたので，これからLBの制御方式について検討します。

〔LBの制御方式の検討〕

X主任は，導入予定のLBがもつ負荷分散機能，セッション維持機能，ヘルスチェック機能の三つについて調査し，次の方式を利用することにした。

・負荷分散機能

アクセス元であるクライアントからのリクエストを，負荷分散対象のサーバに振り分ける機能である。Y社のECサーバは，リクエストの内容によってサーバに掛かる負荷が大きく異なるので，ECサーバにエージェントを導入し，エージェントが取得した情報を基に，ECサーバに掛かる負荷の偏りを小さくすることが可能な動的振分け方式を利用する。

・セッション維持機能

同一のアクセス元からのリクエストを，同一セッションの間は同じサーバに転送する機能である。アクセス元の識別は，IPアドレス，IPアドレスとポート番号との組合せ，及びCookieに記録された情報によって行う，三つの方式がある。IPアドレスでアクセス元を識別する場合，インターネットアクセス時に送信元IPアドレスが同じアドレスになる会員企業では，複数の購買担当者がアクセスするECサーバが同一になってしまう問題が発生する。⑧IPアドレスとポート番号との組合せでアクセス元を識別する場合は，TCPコネクションが切断されると再接続時にセッション維持ができなくなる問題が発生する。そこで，⑨Cookie中のセッションIDと振分け先のサーバから構成されるセッション管理テーブルをLBが作成し，このテーブルを使用してセッションを維持する方式を利用する。

・ヘルスチェック機能

振分け先のサーバの稼働状態を定期的に監視し，障害が発生したサーバを負荷分散の対象から外す機能である。⑩ヘルスチェックは，レイヤー3，4及び7の各レイヤーで稼働状態を監視する方式があり，ここではレイヤー7方式を利用する。

X主任が，LBの制御方式の検討結果をW課長に説明した後，W課長から新たな検討事項の指示を受けた。そのときの，2人の会話を次に示す。

W課長 ：運用チームから，EC サイトのアカウント情報の管理負荷が大きくなってきたので，管理負荷の軽減策の検討要望が挙がっています。会員企業からは，自社で管理しているアカウント情報を使って EC サーバにログインできるようにして欲しいとの要望があります。これらの要望に応えるために，EC サーバの SAML2.0（Security Assertion Markup Language 2.0）への対応について検討してください。

X主任 ：分かりました。検討してみます。

〔SAML2.0 の調査と EC サーバへの対応の検討〕

X 主任が SAML2.0 について調査して理解した内容を次に示す。

・SAML は，認証・認可の要求／応答のプロトコルとその情報を表現するための標準規格であり，一度の認証で複数のサービスが利用できるシングルサインオン（以下，SSO という）を実現することができる。

・SAML では，利用者にサービスを提供する SP（Service Provider）と，利用者の認証・認可の情報を SP に提供する IdP（Identity Provider）との間で，情報の交換を行う。

・IdP は，SAML アサーションと呼ばれる XML ドキュメントを作成し，利用者を介して SP に送信する。SAML アサーションには，次の三つの種類がある。

(a) 利用者が IdP にログインした時刻，場所，使用した認証の種類などの情報が記述される。

(b) 利用者の名前，生年月日など利用者を識別する情報が記述される。

(c) 利用者がもつサービスを利用する権限などの情報が記述される。

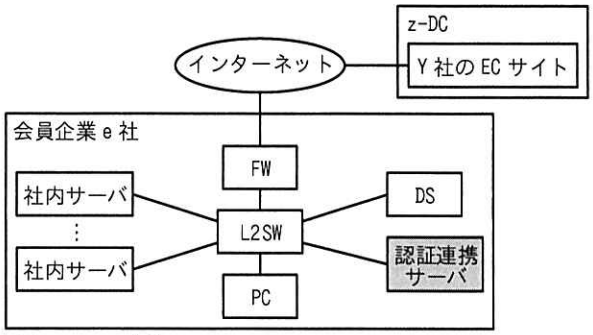
・SP は，IdP から提供された SAML アサーションを基に，利用者にサービスを提供する。

・IdP，SP 及び利用者間の情報の交換方法は，SAML プロトコルとしてまとめられており，メッセージの送受信には HTTP などが使われる。

・z-DC で稼働する Y 社の EC サーバが SAML の SP に対応すれば，購買担当者は，自社内のディレクトリサーバ（以下，DS という）などで管理するアカウント情報を使って，EC サーバに安全に SSO でアクセスできる。

X 主任は，ケルベロス認証を利用して社内のサーバに SSO でアクセスしている会員企業 e 社を例として取り上げ，e 社内の PC が SAML を利用して Y 社の EC サーバにも SSO でアクセスする場合のシステム構成及び通信手順について考えた。

会員企業 e 社のシステム構成を図 6 に示す。



注記　網掛けの認証連携サーバは，SAML を利用するために新たに導入する。

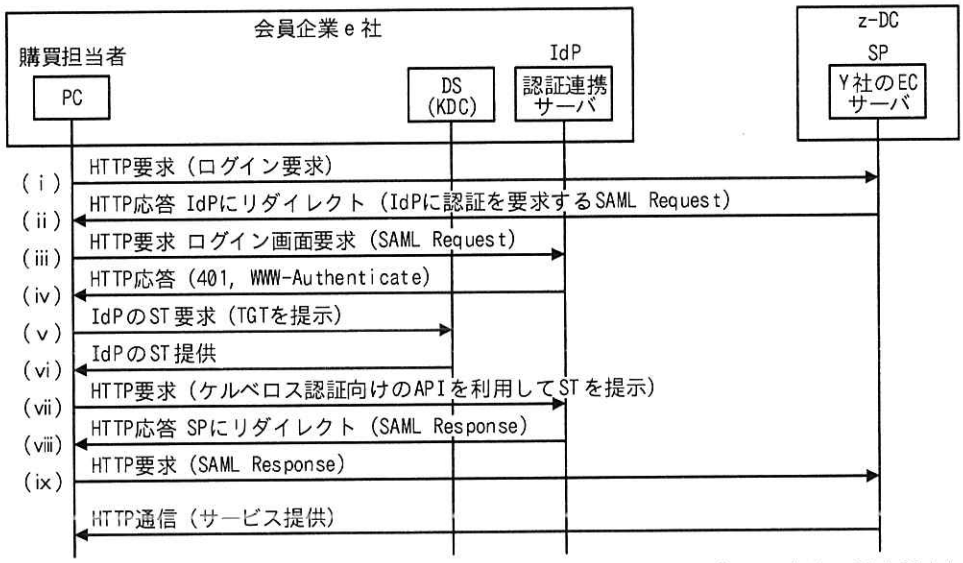
図 6　会員企業 e 社のシステム構成（抜粋）

図 6 で示した会員企業 e 社のシステムの概要を次に示す。

・e 社ではケルベロス認証を利用し，社内サーバに SSO でアクセスしている。
・e 社内の DS は，従業員のアカウント情報を管理している。
・PC 及び社内サーバは，それぞれ自身の共通鍵を保有している。
・DS は，PC 及び社内サーバそれぞれの共通鍵の管理を行うとともに，チケットの発行を行う鍵配布センター（以下，KDC という）機能をもっている。
・KDC が発行するチケットには，PC の利用者の身分証明書に相当するチケット（以下，TGT という）と PC の利用者がアクセスするサーバで認証を受けるためのチケット（以下，ST という）の 2 種類がある。
・認証連携サーバは IdP として働き，ケルベロス認証と SAML との間で認証連携を行う。

X 主任は，e 社内の PC から Y 社の EC サーバに SAML を利用して SSO でアクセスするときの通信手順と処理の概要を，次のようにまとめた。

e 社内の PC から EC サーバに SSO でアクセスするときの通信手順を図 7 に示す。



注記１　本図では，購買担当者はPCにログインしてTGTを取得しているが，IdP向けのSTを所有していない状態での通信手順を示している。

注記２　LBの記述は，図中から省略している。

図７　ｅ社内のPCからECサーバにSSOでアクセスするときの通信手順（抜粋）

図７中の，(ｉ)～(ix)の処理の概要を次に示す。

(ｉ)　購買担当者がPCを使用してECサーバにログイン要求を行う。

(ii)　SPであるECサーバは，⑪SAML認証要求（SAML Request）を作成しIdPである認証連携サーバにリダイレクトを要求する応答を行う。

ここで，ECサーバには，⑫IdPが作成するデジタル署名の検証に必要な情報などが設定され，IdPとの間で信頼関係が構築されている。

(iii)　PCはSAML RequestをIdPに転送する。

(iv)　IdPはPCに認証を求める。

(v)　PCは，KDCにTGTを提示してIdPへのアクセスに必要なSTの発行を要求する。

(vi)　KDCは，TGTを基に，購買担当者の身元情報やセッション鍵が含まれたSTを発行し，IdPの鍵でSTを暗号化する。さらに，KDCは，暗号化したSTにセッション鍵などを付加し，全体をPCの鍵で暗号化した情報をPCに払い出す。

(vii)　PCは，⑬受信した情報の中からSTを取り出し，ケルベロス認証向けのAPIを利用して，STをIdPに提示する。

(viii) IdP は，ST の内容を基に購買担当者を認証し，デジタル署名付きの SAML アサーションを含む SAML 応答（SAML Response）を作成して，SP にリダイレクトを要求する応答を行う。

(ix) PC は，SAML Response を SP に転送する。SP は，SAML Response に含まれる⑭デジタル署名を検証し，検証結果に問題がない場合，SAML アサーションを基に，購買担当者が正当な利用者であることの確認，及び購買担当者に対して提供するサービス範囲を定めた利用権限の付与の，二つの処理を行う。

X 主任は，EC サーバの SAML2.0 対応の検討結果を基に，SAML2.0 に対応する場合の EC サーバプログラムの改修作業の概要を W 課長に説明した。

W 課長は，X 主任の設計した EC サーバの増強案，及び SAML2.0 対応のための EC サーバの改修などについて，経営会議で提案して承認を得ることができた。

設問1　図 2 中の［ a ］，［ b ］に入れる適切なリソースレコード名を，［ c ］～［ f ］に入れる適切な IP アドレスを，それぞれ答えよ。

設問2　〔EC サイトの応答速度の低下〕について答えよ。

(1) URL を https://ecsv.y-sha.example.lan/ に設定して EC サーバにアクセスすると，TLS のハンドシェイク中にエラーメッセージが Web ブラウザに表示される。その理由を，サーバ証明書のコモン名に着目して，25 字以内で答えよ。

(2) 本文中の下線①でアクセスしたとき，運用 PC が送信したパケットが EC サーバに届くまでに経由する機器を，図 1 中の機器名で全て答えよ。

設問3　〔EC サーバの増強構成の設計〕について答えよ。

(1) 本文中の［ g ］，［ h ］に入れる適切な字句を答えよ。

(2) 本文中の下線②について，2 台ではなく 3 台構成にする目的を，35 字以内で答えよ。ここで，将来のアクセス増加については考慮しないものとする。

(3) 表 2 中の［ i ］～［ k ］に入れる適切な IP アドレスを答えよ。

設問4　〔EC サーバの増強構成と LB の設定〕について答えよ。

(1) 本文中の下線③について，どの機器を示すことになるかを，図 3 中の機器名で答えよ。また，下線③の特別な IP アドレスは何と呼ばれるかを，本文中

の字句で答えよ。

(2) 本文中の下線④について，ホスト名のほかに変更する情報を答えよ。

(3) 本文中の下線⑤について，どの機器からどの機器の IP アドレスに変更するのかを，図 3 中の機器名で答えよ。

(4) 本文中の下線⑥について，X-Forwarded-For フィールドを追加する目的を，35 字以内で答えよ。

(5) 本文中の下線⑦について，対応するための作業内容を，50 字以内で答えよ。

設問 5 〔LB の制御方式の検討〕について答えよ。

(1) 本文中の下線⑧について，セッション維持ができなくなる理由を，50 字以内で答えよ。

(2) 本文中の下線⑨について，LB がセッション管理テーブルに新たなレコードを登録するのは，どのような場合か。60 字以内で答えよ。

(3) 本文中の下線⑩について，レイヤー3 及びレイヤー4 方式では適切な監視が行われない。その理由を 25 字以内で答えよ。

設問 6 〔SAML2.0 の調査と EC サーバへの対応の検討〕について答えよ。

(1) 本文中の下線⑪について，ログイン要求を受信した EC サーバがリダイレクト応答を行うために必要とする情報を，購買担当者の認証・認可の情報を提供する IdP が会員企業によって異なることに着目して，30 字以内で答えよ。

(2) 本文中の下線⑫について，図 7 の手順の処理を行うために，EC サーバに登録すべき情報を，15 字以内で答えよ。

(3) 本文中の下線⑬について，取り出した ST を PC は改ざんすることができない。その理由を 20 字以内で答えよ。

(4) 本文中の下線⑭について，受信した SAML アサーションに対して検証できる内容を二つ挙げ，それぞれ 25 字以内で答えよ。

〔 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。