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。

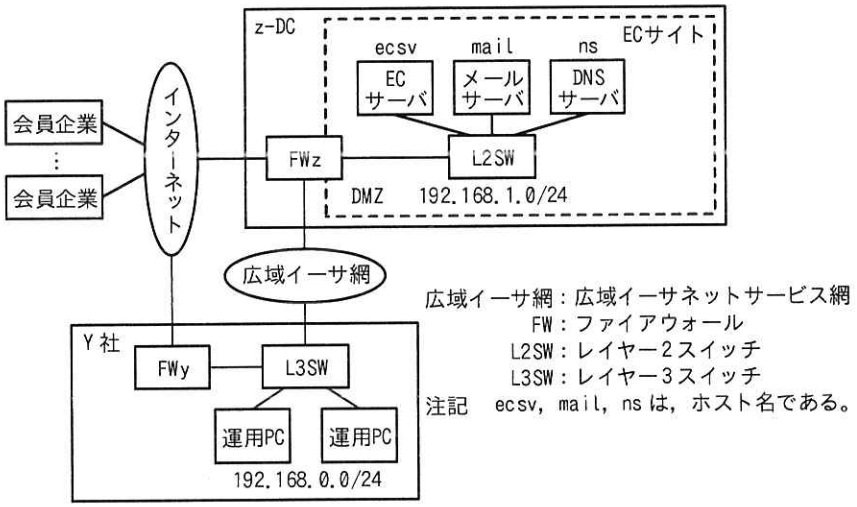


図 1　EC サイトに関連するシステムの構成（抜粋）

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。

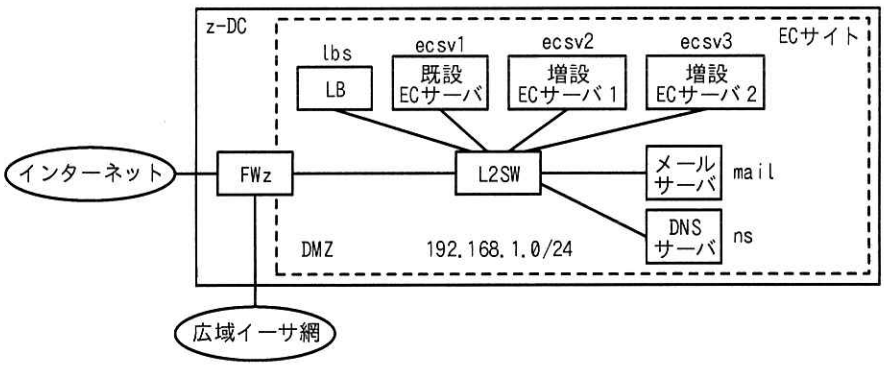
この結果から，X主任は，ECサーバが処理能力不足になったと判断した。

〔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。



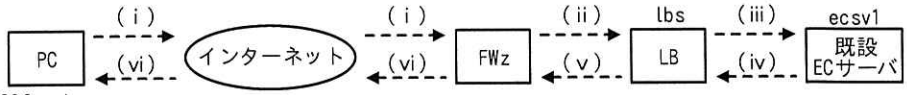
注記 lbsはLBのホスト名であり，ecsv1～ecsv3は増強後のECサーバのホスト名である。

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。

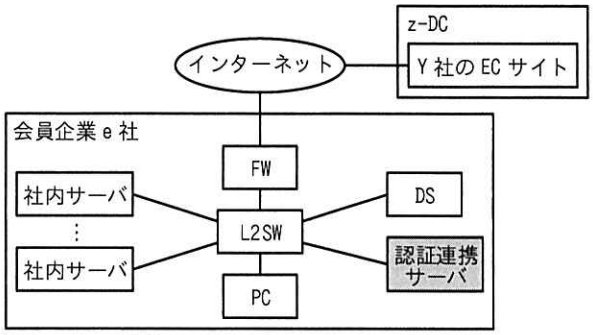
・SP は，IdP から提供された SAML アサーションを基に，利用者にサービスを提供する。

・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。

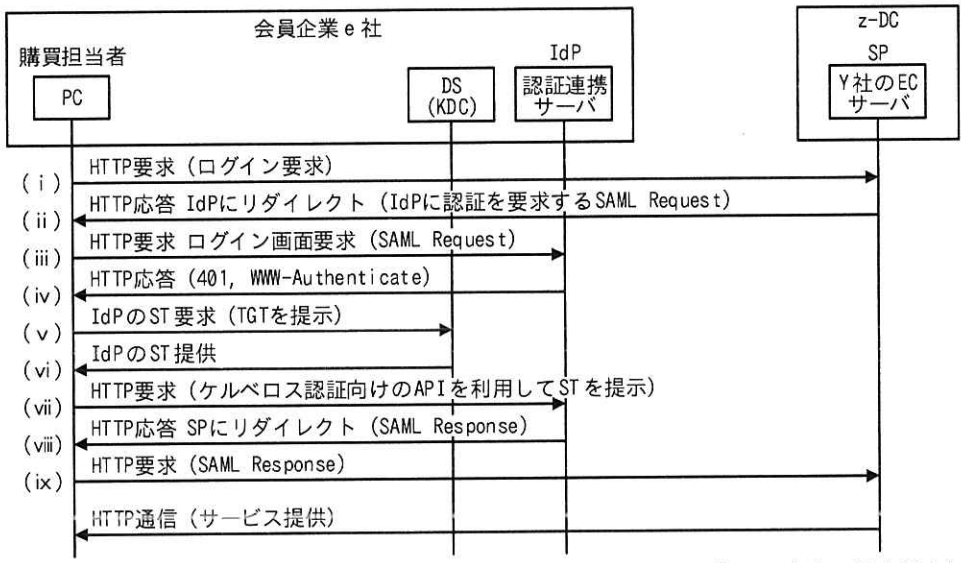
図 6　会員企業 e 社のシステム構成（抜粋）

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。