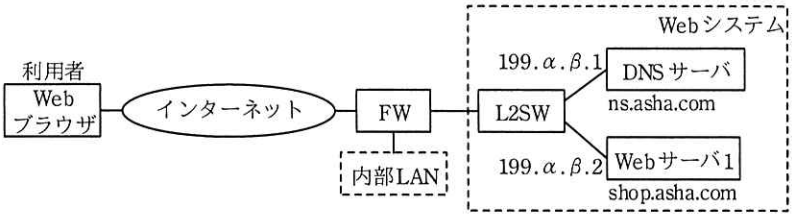
問2　Webシステムの構成変更に関する次の記述を読んで，設問1～3に答えよ。

A社は，中堅の菓子メーカであり，自社で製造する商品を，店舗とオンラインショップで販売している。オンラインショップの利用者は，Webブラウザを使ってWebシステムにアクセスする。A社のオンラインショップを構成する，現行のWebシステムを図1に示す。



L2SW：レイヤ2スイッチ　　FW：ファイアウォール
注記1　199.α.β.1及び199.α.β.2は，グローバルIPアドレスを示す。
注記2　インターネットからWebシステムへの通信について，DNSとHTTPSだけを許可するアクセス制御を，FWに設定している。

図1　現行のWebシステム（抜粋）

A社では，Webシステムのアクセス数の増加に対応するために，Webサーバの増設と負荷分散装置（以下，LBという）の導入を決めた。また，昨今，Webアプリケーションプログラム（以下，WebAPという）の脆弱(ぜい)性を悪用したサイバー攻撃が報告されていることから，WAF（Web Application Firewall）サービスの導入を検討することになった。そのための事前調査から設計までを情報システム部のUさんが担当することになった。

〔WAFサービス導入の検討〕

Uさんは，SaaS事業者のT社が提供するWAFサービスを調査した。T社によるWAFサービスの説明は，次のとおりである。

・WAFサービスは，利用者のWebブラウザとWebシステム間のHTTPS通信を中継する。利用者のWebブラウザは，WAFサービスにアクセスするためのIPアドレス（以下，IP-w1という）宛てにHTTPリクエストを送信する。
・WAFサービスは，HTTPS通信を復号してHTTPリクエストを検査する。そのた

めに，A 社は，現行と同じコモンネームのサーバ証明書と秘密鍵を，WAF サービスに提供する必要がある。

・WAF サービスは，WebAP へのサイバー攻撃が疑われる通信を検知し，Web システムへのアクセスを制御する。

・WAF サービスは，アクセスを許可した HTTP リクエストの送信元 IP アドレスを，HTTP ヘッダの X-Forwarded-For ヘッダフィールド（以下，XFF ヘッダという）に追加する。XFF ヘッダへの追加後に，HTTP リクエストの送信元 IP アドレスを，HTTP レスポンスが WAF サービスに送られるようにするための IP アドレス（以下，IP-w2 という）に変更する。

・WAF サービスは，HTTP リクエストを再度 HTTPS で暗号化して，Web システムにアクセスするための IP アドレスである 199.α.β.2 宛てに転送する。

・WAF サービスは，HTTP レスポンスを検査する。HTTP レスポンスに対する処理の説明は省略する。

U さんは，Web ブラウザから送信される HTTP リクエストを，WAF サービス宛てに変える方法について，T 社に確認した。T 社からの回答は，次のとおりである。

・A 社 DNS サーバに，RDATA に IP-w1 を設定した A レコードを登録する方式と，RDATA に T 社 WAF サービスの FQDN を設定した CNAME レコードを登録する方式がある。

・T 社は，IP-w1 を変更する場合があるので，<u>① CNAME レコードを登録する方式を推奨している</u>。

T 社からの説明を踏まえて，U さんが検討した A 社 DNS サーバのゾーンファイルを，図 2 に示す。

```
$ORIGIN     asha.com.
$TTL        3600
（省略）
            IN    NS        ns
ns          IN    A         199.α.β.1
shop        IN    CNAME     waf-asha.tsha.net.
（省略）
```

注記　“waf-asha.tsha.net.”は，A社WebシステムでWAFサービスを利用するために，T社から割り当てられたFQDNである。

図2　A社DNSサーバのゾーンファイル（抜粋）

現行のWebAPでは，Webシステムへのアクセス時の送信元IPアドレスをアクセスログに記録している。Uさんは，送信元IPアドレスの代わりにXFFヘッダの情報を記録するように，WebAPの設定を変更することにした。

Uさんは，FWに設定しているWebシステムへのアクセス制御について，IP-w2を送信元とする通信だけを許可するように，設定を変更することにした。

〔LBに関する検討〕

A社が導入するLBは，HTTPリクエストの振分け機能，死活監視機能，セッション維持機能，TLSアクセラレーション機能，HTTPヘッダの編集（追加，変更，削除）機能をもっている。

HTTPリクエストの振分け機能について，Uさんは，HTTPリクエストをWebサーバに［　ア　］に振り分けるラウンドロビン方式を採用することにした。

死活監視機能について，Uさんは，WebAPの稼働状況を監視するために，レイヤ7方式を利用することにした。死活監視に用いるメッセージの設定を表1に示す。

表1　メッセージの設定（抜粋）

メッセージ	項目	設定値
HTTPリクエスト	宛先IPアドレス	WebサーバのIPアドレス
	ポート番号	［　イ　］
	メソッド	GET
	パス名	/index.php
成功時のHTTPレスポンス	ステータスコード	［　ウ　］

セッション維持機能には，HTTP リクエストの送信元 IP アドレスに基づいて行う方式と，LB によって生成されるセッション ID に基づいて行う方式がある。セッション ID に基づいて行う方式では，Web サーバと Web ブラウザ間で状態を管理するために用いられる Cookie を利用する。LB は，HTTP レスポンスの［　エ　］ヘッダフィールドにセッション ID を追加する。HTTP レスポンスを受け取った利用者の Web ブラウザは，［　エ　］ヘッダフィールドにあるセッション ID を，次に送信する HTTP リクエストの［　オ　］ヘッダフィールドに追加する。HTTP リクエストを受け取った LB は，［　オ　］ヘッダフィールドのセッション ID に基づいて，セッション維持を行う。U さんは，② WAF サービスの利用を考慮し，セッション ID に基づいて行う方式を採用した。

TLS アクセラレーション機能は，TLS の暗号化・復号処理を専用ハードウェアで高速に処理する機能である。U さんは，TLS の暗号化・復号処理の性能向上の目的と，③ LB が行うある処理のために，TLS アクセラレーション機能を利用することにした。U さんは，LB と Web サーバ間の通信に HTTP を用い，ポート番号に HTTP のウェルノウンポート番号を用いることにした。

構成変更後の Web システムを図 3 に示す。

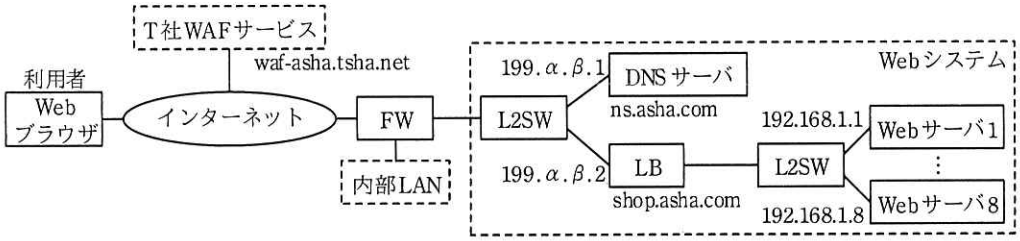


図 3　構成変更後の Web システム（抜粋）

〔WAF サービス停止時の対応検討〕

U さんは，障害などで WAF サービスを 1 日以上利用できなくなった場合に備え，対応を検討した。WAF サービス停止期間中も，オンラインショップでの商品販売を継続させたい。U さんは，WAF サービスを経由せずに，利用者の Web ブラウザと Web システム間で直接通信させるために，WAF サービス導入時に設定変更を予定している［　カ　］の④設定を変更することと，図 2 中の⑤資源レコードの 1 行を書

き換えることで対応できると考えた。

U さんは，WebAP のアクセスログについて，WAF サービスの有無にかかわらず，XFF ヘッダの情報から Web システムへのアクセス時の送信元 IP アドレスを記録することとし，⑥LB に設定を追加した。

その後，Web システムの構成変更に関する U さんの報告書は経営会議で承認され，導入の準備を開始した。

設問1　本文中の下線①について，A 社にとっての利点を 45 字以内で述べよ。

設問2　〔LB に関する検討〕について，(1)～(3) に答えよ。

(1) 本文及び表 1 中の［　ア　］～［　オ　］に入れる適切な字句又は数値を答えよ。

(2) 本文中の下線②について，送信元 IP アドレスに基づいて行う方式を採用した場合に発生するおそれがある問題を，10 字以内で述べよ。

(3) 本文中の下線③の処理の内容を，20 字以内で答えよ。

設問3　〔WAF サービス停止時の対応検討〕について，(1)～(3) に答えよ。

(1) 本文中の［　カ　］に入れる機器を，図 3 中の DNS サーバ以外の機器名で答えよ。また，本文中の下線④の変更内容を 35 字以内で述べよ。

(2) 本文中の下線⑤について，書換え後の資源レコードを答えよ。

(3) 本文中の下線⑥の設定内容を，30 字以内で答えよ。