平成 27 年度 秋期 午後Ⅰ問題の解答・解説

注：試験センターが公表している出題趣旨・採点講評・解答例を転載している。

問 1

出題趣旨

シングルサインオンは，大規模な Web システム構築で用いられることが多くなってきた技術であるが，この技術を活用したシステム構築においては，アプリケーション技術者，サーバ技術者，ネットワーク技術者が協力して取り組むことが必要である。本問のように，負荷分散装置でシングルサインオンサーバを冗長化したシステムを安定して構築するためには，パケットレベルの詳細な流れが理解できるスキルが必要である。

本問では，Cookie を利用したシングルサインオンについての基本的な仕組みの理解と，DSR 方式ロードバランサを用いたシングルサインオンサービス負荷分散について，実務上必要となる技術の理解を問う。

採点講評

問 1 では，Web アプリケーションにおけるシングルサインオン認証と，負荷分散装置を用いた負荷分散を題材とし，HTTP プロトコル上での Cookie を前提とした認証連携の動作と，DSR を用いるときに必要となる基本的知識について出題した。全体として，正答率は低かった。

設問 1 では，ウの正答率が低かった。HTTP プロトコルにおける重要なヘッダの一つなので，Cookie のやり取りを含め，正しく把握しておいてほしい。

設問 3 では，(2) の正答率が低かった。サーバ側で発行されてクライアントに送られた Cookie が再びサーバに送り返されるという場面を頭に描くところまで至らず，単に通信経路や Cookie を暗号化するといったような解答が散見された。Cookie の Secure 属性については，単にキーワードとしてとらえるのではなく，なぜそれによって安全になるのか，その動作や仕組みについて，しっかりと理解をしてほしい。

設問 4 は，DSR 方式の負荷分散装置の動作に関して問うたものであるが，アドレス重複についての検知の仕組みと対処について，正しく理解していない解答が散見された。アドレス重複検知については，トラブル対応の基本スキルの一つとして，身に付けておくことが必要である。

設問		解答例・解答の要点		備考
設問 1		ア	リバースプロキシ	
		イ	リダイレクト	
		ウ	Set-Cookie	
		エ	内部 DNS	
		オ	ループバック	
設問 2		⑤		
設問 3	(1)	a-sha.example.jp		
	(2)	Cookie に Secure 属性を付ける。		
設問 4	(1)	SYN パケットにはレイヤ 7 情報が含まれていないから		
	(2)	Gratuitous ARP　又は　GARP		
	(3)	VIP アドレスに対する ARP リクエストに応答しないように設定する。		

本問は，SSO（シングルサインオン）の導入をテーマに，SSO の認証処理シーケンス，負荷分散装置を用いた SSO サーバの二重化について問うている。

現在，A 社には営業システムや広告システムなど複数の Web アプリケーションが存在し，利用者認証をそれぞれ個別に行っている。この方法は利用者の利便性が低いため，改善の要望が出されていた。そこで，Web アプリケーションの認証を共通化するために，SSO の導入を考えた。

本格導入する前に，試験的に SSO サーバを設置することとした。〔SSO の導入〕の第 1 段落の中で，試験導入の要件について，次のように記述されている。本問全体に関わるものなので，最初に頭に入れておこう。

- PC からアクセスされる，営業システムと広告システムを対象範囲として，SSO を可能にする。
- SSO サーバは，障害に備えて負荷分散装置（以下，LB という）によって二重化を行う。
- LB は，DSR（Direct Server Return）方式を使用する。
- 関連するシステムの URL を，表 1 のように設定する。

表 1　関連するシステムの URL

システム名称	サーバ名称	URL	備考
SSO システム	SSO サーバ	http://sso.a-sha.example.jp	新規
営業システム	営業サーバ	http://eigyou.a-sha.example.jp	現状のまま
広告システム	広告サーバ	http://koukoku.a-sha.example.jp	現状のまま

本問を首尾よく解くには，SSO の認証処理の仕組みを理解しておく必要がある。そこで，解説に先立ち，SSO について概要を押さえておこう。

なお，本文の中で SSO の認証動作について説明しているので，その内容を理解できれば解を導けるように配慮されている。

● SSO の概要

利用者認証を行うとき，PC は SSO サーバにアクセスする。

利用者認証に成功すると，SSO サーバは，PC に Cookie を送信する。この Cookie には，認証済資格情報（以下，アクセスチケットと称する）が含まれている。アクセスチケットをひとたび取得した後は，認証操作を行わずに Web アプリケーションサーバにアクセスする仕組みになっている。

SSO の方式は，エージェント方式とリバースプロキシ方式の二つに大別される。

両者のどちらも，前述のとおり，Cookie を用いて，SSO サーバでの利用者認証が済んでいるか否かを判別している。

両者で大きく異なっている点は，PC が接続するサーバである。

以下，エージェント方式とリバースプロキシ方式の概要を解説する。本問ではエージェント方式が登場するので，後ほどより詳しく解説する。

●エージェント方式の概要

エージェント方式では，PC は Web アプリケーションサーバに接続する。

Web アプリケーションには，SSO の認証処理を行うソフトウェアモジュールがインストールされている。このソフトウェアモジュールをエージェントという。

［1］PC：サービス要求を送信

PC は Web アプリケーションサーバへのサービス要求を格納した HTTP 要求パケットを送信する。サービス要求の URL は，Web アプリケーションサーバで稼働している業務システムのページである。

［2］エージェント：アクセスチケットの有無を調査

Web アプリケーションが受信すると，エージェントがフックし，Cookie ヘッダフィールドにアクセスチケットが含まれているか否かを調べる。

アクセスチケットがなければ，認証処理を行う必要があるため，項番［3］へ進む。

アクセスチケットがあれば，項番［6］へ進む。

［3］Web アプリケーション：SSO サーバに認証要求をリダイレクト

PC から SSO サーバに接続し，利用者認証を行わせる必要がある。これを実現するため，認証要求を格納した HTTP 応答パケットを PC に送信する。このパケットに，リダイレクトを設定しておく。リダイレクト先は SSO サーバである。これを受け取った PC は，認証要求を SSO サーバに送信する。

［4］SSO サーバ：認証処理を実行

SSO サーバは PC に認証画面を送信し，認証処理を実行する。

［5］SSO サーバ：Web アプリケーションサーバにサービス要求をリダイレクト

認証に成功したため，PC から Web アプリケーションサーバに接続し，当初の業務処理を行わせる必要がある。これを実現するため，SSO サーバはアクセスチケットを発行する。そして，サービス要求を格納した HTTP 応答パケットを PC に送信する。このパケットにアクセスチケットを格納し，かつ，リダイレク

トを設定しておく。リダイレクト先は Web アプリケーションサーバ（［1］で指定した URL）である。

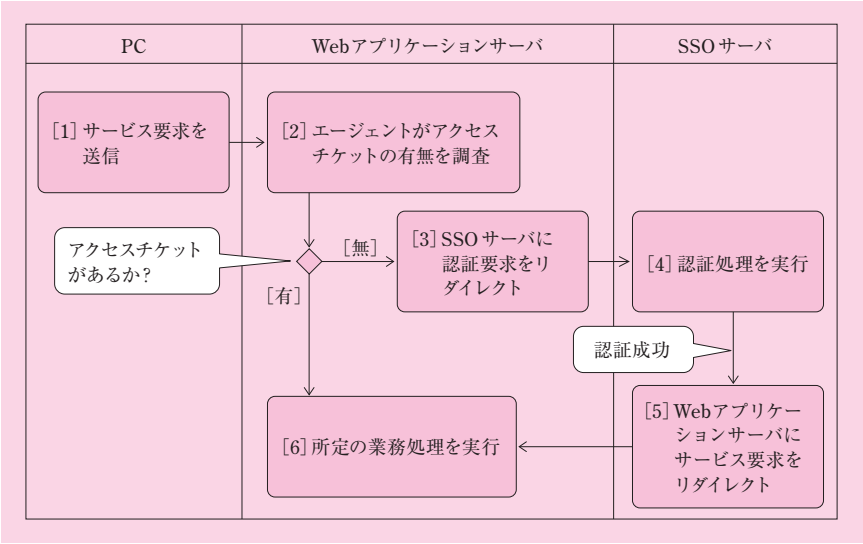
これを受け取った PC は，項番［1］と同様，サービス要求を Web アプリケーションサーバに送信する（リダイレクト設定に従って送信する）。PC には先ほど発行されたアクセスチケットが保存されているので，サービス要求を送信する際，Cookie ヘッダフィールドにアクセスチケットを格納する。

［6］Web アプリケーション：所定の業務処理を実行

エージェントは，アクセスチケットの正当性を確認するため，SSO サーバに問い合わせる。正当性が確認できた場合，エージェントは，サービス要求をそのまま Web アプリケーションに渡す。Web アプリケーションは所定の業務処理を実行する。

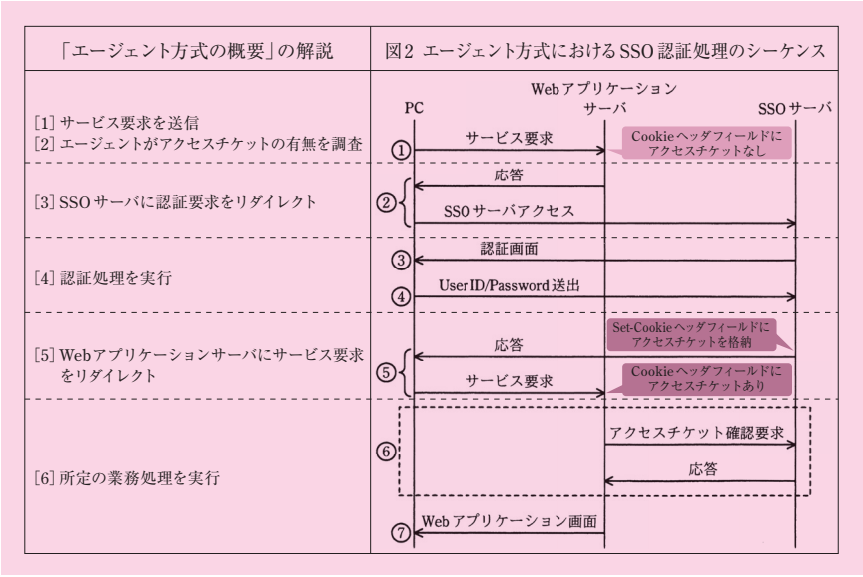
参考までに，項番［5］でリダイレクトする際，SSO サーバはアクセスチケットを Set-Cookie フィールドに格納し，PC に HTTP 応答パケットを返信する。このアクセスチケットは PC に保存される。

したがって，次に項番［1］から実行したときは，HTTP 要求パケットの Cookie フィールドにアクセスチケットが格納されているため，項番［2］→項番［6］のフローをたどる。こうして，SSO を実現している。



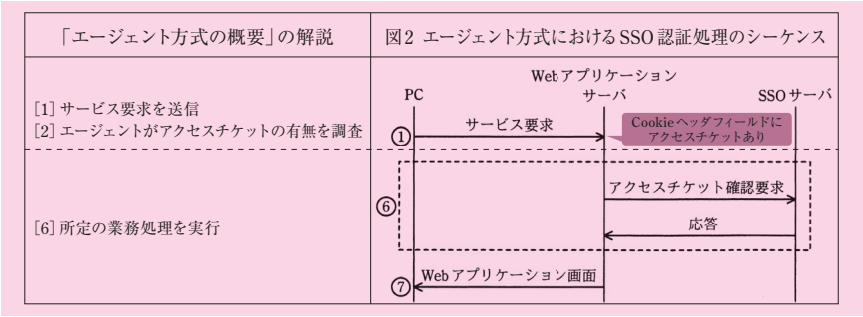
図：エージェント方式の認証動作の概要

本事例では，エージェント方式が採用されている。本文の図 2 には，エージェント方式の認証処理シーケンスが記されている。前述の解説がこれとどのように対応しているか，次の図に示しておく。



図：「エージェント方式の概要」で解説した認証処理と，図 2 との対応（最初にアクセスチケットがない場合）

最初の項番［1］の時点からアクセスチケットがある場合はどうなるか，次の図に示しておく。



図：「エージェント方式の概要」で解説した認証処理と，図 2 との対応（最初からアクセスチケットがある場合）

●リバースプロキシ方式の概要

リバースプロキシ方式は本事例で採用されていないが，関連知識の習得のため，これについても解説しておこう。

リバースプロキシ方式では，SSO サーバは Web アプリケーションサーバのリバースプロキシとして振る舞い，PC と Web アプリケーションサーバ間の通信を全て中継する。

PC に公開された Web アプリケーションサーバの IP アドレスは，実際には，リバースプロキシである SSO サーバの IP アドレスになっている。それゆえ，PC はまず SSO サーバに接続し，これを経由して Web アプリケーションサーバに接続する構成になっている。

［1］PC：サービス要求を送信

PC は Web アプリケーションサーバへのサービス要求を格納した HTTP 要求パケットを送信する。このとき，パケットは，実際には SSO サーバに送信されている。

［2］SSO サーバ：アクセスチケットの有無を調査

SSO サーバはリバースプロキシとして HTTP 要求パケットを受け付け，Cookie ヘッダフィールドにアクセスチケットが含まれているか否かを調べる。

アクセスチケットがなければ，認証処理を行う必要があるため，項番［3］へ進む。

アクセスチケットがあれば，項番［4］へ進む。

［3］SSO サーバ：認証処理を実行

SSO サーバは PC に認証画面を送信し，認証処理を実行する。

［4］SSO サーバ：Web アプリケーションサーバにサービス要求を中継

SSO サーバは，アクセスチケットの正当性を確認する。

その後，SSO サーバは，Web アプリケーションサーバにサービス要求を中継する。

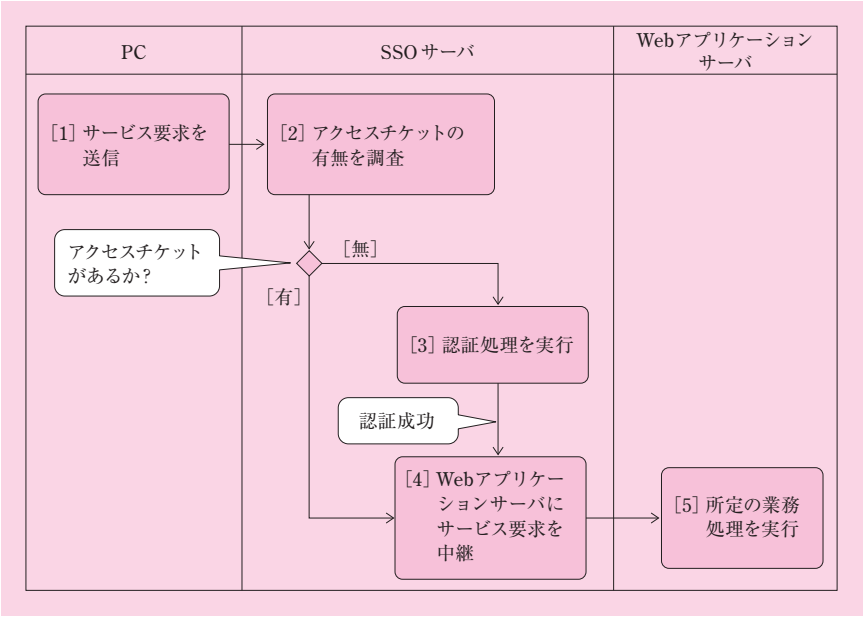
［5］Web アプリケーション：所定の業務処理を実行

Web アプリケーションは所定の業務処理を実行する。

参考までに，認証処理を行うフローにおいて SSO サーバが中継するとき（項番［4］），Web アプリケーションサーバから HTTP 応答パケットを受け取ると，今度は Web アプリケーションサーバの代理となり，これを PC に中継する。PC に HTTP 応答パケットを送信する際，Set-Cookie ヘッダフィールドにアクセスチケットを格納する。この

アクセスチケットは PC に保存される。

したがって，次に項番［1］から実行したときは，HTTP 要求パケットの Cookie フィールドにアクセスチケットが格納されているため，項番［2］→項番［4］→項番［5］のフローをたどる。こうして，SSO を実現している。



図：リバースプロキシ方式の認証動作の概要

SSO について概要を理解できたので，いよいよ設問の解説に移ろう。

■設問 1

解答例

ア：リバースプロキシ
イ：リダイレクト
ウ：Set-Cookie
エ：内部 DNS
オ：ループバック

ア

空欄アを含む文章は，〔SSO についての検討〕の第 1 段落の中にある。そこには「SSO の方式を分類すると，SSO サーバで利用したいサーバにエージェントと呼ばれるソフトウェアモジュールをインストールして実現するエージェント方式と，SSO サーバにおいて全ての通信の中継を行う［ア］方式がある」と記述されている。

冒頭で解説したとおり，SSO の方式は，エージェント方式とリバースプロキシ方式の二つがある。SSO サーバにおいて全ての通信の中継を行うのはリバースプロキシ方式である。

よって，空欄アに該当する字句は，「**リバースプロキシ**」である。

イ

空欄イを含む文章は，〔SSO についての検討〕の第 2 段落，項番②と項番⑤の 2 か所にある。

項番②には「Web アプリケーションサーバ内のエージェントは，サービス要求中の Cookie に認証済資格情報（以下，アクセスチケットという）が含まれているか確認する。含まれていなければ，サービス要求は SSO サーバへ［イ］される」と記述されている。

項番⑤には「SSO サーバは，……利用者のアクセスの正当性を確認したら，アクセスチケットを発行して，Cookie に含めて応答を返す。サービス要求は，Web アプリケーションサーバへ［イ］される」と記述されている。

第 2 段落の項番①～⑦は，エージェント方式における SSO 認証のシーケンスである。

本文の項番②は，PC からのサービス要求をエージェントがフックした後の動作について述べている。エージェントはアクセスチケットの有無を調べ，これがなければ，SSO サーバに認証要求をリダイレクトする。

本文の項番⑤は，SSO サーバが認証処理を行った後の動作について述べている。認証に成功したら，SSO サーバは，Web アプリケーションサーバにサービス要求をリダイレクトする。

よって，空欄イに該当する字句は，「**リダイレクト**」である。

ウ

空欄ウを含む文章は，〔SSO サーバの動作確認〕の第 2 段落の中にある。

「UserID と Password を正しく入力しても，営業システムの画面に遷移せず，SSO として正しく動作しなかった」とあるので，〔SSO についての検討〕の第 2 段落にあ

る認証処理シーケンスの項番⑤に不具合が発生していることが分かる。

その上で，「原因を調査したところ，SSO サーバから送出される HTTP 応答パケットの［ウ］ヘッダフィールドに，Domain 属性が付与されていないからであった」と記述されている。

アクセスチケットは，SSO サーバから PC への HTTP 応答パケットの Cookie に格納される。このとき用いられるヘッダフィールドは，「Set-Cookie」である。

よって，空欄ウに該当する字句は，「**Set-Cookie**」である。

なお，空欄ウを含む文の中で「Domain 属性」が登場する。続く文は，これを正しく設定することで不具合が解消した旨，記されている。この点について設問 3（1）で問われているので，詳しくはそこで解説する。

［エ］

空欄エの解説に入る前に，本問の流れを確認しておこう。

本事例では，図 1 と同等の検証環境を本番環境とは別に用意している。検証環境を用いた動作確認は，二つの段階を踏んでいることに注目できる。

第 1 段階は，SSO サーバの動作確認である。この内容は，〔SSO サーバの動作確認〕の中に記されている。

第 2 段階は，負荷分散の動作確認である。この内容は，〔負荷分散に関する設定と動作確認〕の中に記されている。冒頭で解説したとおり，負荷分散は，今回の SSO 導入の要件に挙げられている。

LB の接続と設定は，第 2 段階で行っている。これは，〔負荷分散に関する設定と動作確認〕の第 1 段落にある，「図 1 と同じように，LB を SW2 に接続して VIP アドレスと負荷分散ポリシを設定（した）」という記述から分かる。

この点を踏まえて，空欄エを解いてみよう。

空欄エを含む文章は，〔負荷分散に関する設定と動作確認〕の第 1 段落の中にある。そこには，「PC から sso.a-sha.example.jp への認証リクエストの宛先がこの VIP アドレスとなるように，［エ］サーバに設定を行った」と記述されている。

ホスト名 sso.a-sha.example.jp は，表 1「関連するシステムの URL」によれば，SSO サーバのものである。それゆえ，「PC から sso.a-sha.example.jp への認証リクエスト」とは，SSO サーバへリダイレクトされた認証要求を指していると言える。

とはいえ，SSO サーバの負荷分散を LB で行うので，ホスト名 sso.a-sha.example.jp に対応する IP アドレスは，LB になっている。この点について，本文の記述から確認しておこう。第 1 段落の中に，「SSO サーバを DSR 方式で負荷分散するときの LB の

動作の要点」が述べられている。その要点（1）の動作は，「PC から SSO サーバへのリクエストは，LB に設定された VIP アドレスに送られ（る）」と記述されている。したがって，ホスト名 sso.a-sha.example.jp に対応する IP アドレスは，LB に設定された VIP アドレスとなる。

ここで，LB の接続と設定を第 2 段階で初めて行ったことを思い起こそう。

第 1 段階は，LB を用いることなく，PC から SSO サーバに直接接続して動作確認を行った。このとき，ホスト名 sso.a-sha.example.jp に対応する IP アドレスは，検証環境にある SSO サーバの実 IP アドレスになっていた。

第 2 段階で LB を用いるので，ホスト名 sso.a-sha.example.jp に対応する IP アドレスを，VIP アドレスに変更する必要がある。これが，「PC から sso.a-sha.example.jp への認証リクエストの宛先がこの VIP アドレスとなるように……設定を行った」という記述の意味するところである。

このホスト名と IP アドレスの対応付けは，図 1 中の内部 DNS サーバ，又は，PC の hosts ファイルのいずれかで行うことができる。この点，空欄エを含む文章は，サーバで設定を行う旨，記されている。よって，空欄エに該当する字句は，「**内部 DNS**」である。

オ

空欄オを含む文章は，〔負荷分散に関する設定と動作確認〕の第 3 段落と第 4 段落の 2 か所にある。

第 3 段落には，「SSO サーバは，自 IP アドレスと異なる VIP アドレス宛てのパケットを受信しなければならない。そこで，VIP アドレスを付与した［　オ　］インタフェースを SSO サーバに設定することにした」と記述されている。

この記述から，SSO サーバは，自 IP アドレスと VIP アドレスの二つのアドレスをもつことが分かる。

自 IP アドレスと異なる VIP アドレス宛てのパケットを受信するには，ループバックインタフェースに VIP アドレスを設定すればよい。

よって，空欄オに該当する字句は，「**ループバック**」である。

●ループバックインタフェース

ループバックインタフェースは，サーバがもつ仮想的なネットワークインタフェースである。これは UNIX の呼称であり，Windows はループバックアダプタと呼称する。

UNIX では，ループバックインタフェースに IP アドレス 127.0.0.1 が事前に割り当てられているが，通常のネットワークインタフェースと同様に IP エイリアスの設定が可

能である（つまり，複数の IP アドレスを設定できる）。Windows では，任意の IP アドレスを自由に割り当てることができる。

なお，Linux では，ループバックインタフェースを使用せずとも，iptables を設定すれば VIP アドレス宛てパケットを受信できる。

■設問 2

解答例

⑤

本問は，図 2 中の⑥で確認が行われるアクセスチケットを，PC がどの時点で得るのかを問うている。図 2 の項番は，〔SSO についての検討〕の第 2 段落にある認証処理シーケンスの項番を図示したものである

項番⑥の動作について，第 2 段落には，「⑥ Web アプリケーションサーバ内のエージェントは，SSO サーバにアクセスチケット確認要求を送り，SSO サーバは，確認して応答を返す」と記述されている。項番⑥は，サービス要求に基づく業務処理を実行する直前に，Cookie に含まれているアクセスチケットの正当性を確認する目的で行っている。

〔SSO についての検討〕の第 2 段落の中で，項番⑥以外にアクセスチケットに言及している箇所は，項番②と項番⑤である。

項番②には，Cookie にアクセスチケットが含まれていなければ，SSO サーバで認証処理を行うために項番③以降の処理を行う旨，記されている。したがって，この時点ではアクセスチケットはもらっていない。

項番⑤には，「⑤ SSO サーバは，UserID と Password から利用者のアクセスの正当性を確認したら，アクセスチケットを発行して，Cookie に含めて応答を返す」と記述されている。したがって，この時点で認証に成功し，SSO サーバからアクセスチケットをもらっていることが分かる。

よって，正解は「⑤」となる。

■設問 3
(1)

解答例

a-sha.example.jp

問題文は，「本文中の下線（Ⅰ）で，Cookie の Domain 属性として設定した具体的なドメイン名を答えよ」と記述されている。

下線（Ⅰ）は，〔SSO サーバの動作確認〕の第 2 段落にある。そこには，「表 1 中の URL 情報を参照して，SSO サーバの設定項目中の（Ⅰ）Cookie の Domain 属性を設定した。その結果，営業システムと広告システムにおいて SSO が正しく動作するようになった」と記述されている。

したがって，本問は，営業システムと広告システムにおいて SSO が正しく動作するために必要な，Cookie の Domain 属性の設定を問うている。

本問を解くには，Cookie の Domain 属性に関する一般的な知識が必要である。そこで，まずはその点について解説する。それを踏まえて，解を導こう。

● Cookie の Domain 属性

Web アプリケーションサーバからクライアント端末に HTTP 応答パケットを返信する際，ブラウザに Cookie を送出することができる。このとき，Cookie は，Set-Cookie ヘッダフィールドに格納されている。

それ以降，クライアント端末が HTTP 要求パケットを送信するとき，渡された Cookie をサーバに送出する仕様になっている。このとき，Cookie は，Cookie ヘッダフィールドに格納されている。

Cookie を渡す宛先となるサーバは，Domain 属性の有無により異なってくる。この Domain 属性は，サーバが Cookie を送出するときに指定する。

表：Domain 属性の有無による Cookie を渡す宛先

Domain 属性の有無	Cookie を渡す宛先
無	Cookie を渡したサーバ（これが既定値になる）
有	Domain 属性に指定された文字列パターンと後方一致したホスト名をもつサーバ

例えば，サーバからクライアント端末に HTTP 応答パケットを返信するとき，パケットの Set-Cookie ヘッダフィールドが次のように設定されているとしよう。

```
Set-Cookie: SID=31d4d96e407aad42; Domain=a-sha.example.jp
```

この例において，Cookie の値は「SID=31d4d96e407aad42」であり，Domain 属性の値は「a-sha.example.jp」である。この Cookie を渡す宛先となるサーバは，ホスト名が「a-sha.example.jp」と後方一致するものとなる。例えば，「eigyou.a-sha.example.jp」や「koukoku.a-sha.example.jp」などが宛先となり得る。

このサーバに対し，クライアント端末が HTTP 要求パケットを送信すると，Cookie ヘッダフィールドは次のように設定される。

```
Cookie: SID=31d4d96e407aad42
```

以上，Cookie の Domain 属性について解説した。Cookie には，他にも様々な属性が定義されている。Cookie の属性について，詳しくは《基礎編》の第 4 章「4.4.2　Web アプリケーション」を参照していただきたい。

●解の導出

アクセスチケットは，Cookie に含まれている。

図 2 のシーケンスにおいて，アクセスチケットはどの時点で Cookie に格納されるのだろうか。

最初は，SSO サーバから PC への送出であり，項番⑤「応答」である。

それ以降は，PC からサーバへの送出であり，二つのケースが考えられる。一つ目は，項番⑤「サービス要求」である。二つ目は，SSO 認証が済んでいる PC による，項番①「サービス要求」である（このときは，項番①→項番⑥→項番⑦というフローをたどる）。

ここで注目できるのは，Cookie の宛先となるサーバが，どちらのケースも「Web アプリケーションサーバ」であることだ。すなわち，Cookie の生成元であるサーバ（SSO サーバ）と，PC が Cookie を送出する宛先となるサーバ（Web アプリケーションサーバ）が異なっているわけだ。

したがって，SSO サーバが PC に Cookie を送出する際，Domain 属性を用いて，Cookie の宛先となるサーバに Web アプリケーションサーバが含まれるようにしなければならない。

図 2 は，一般的なエージェント方式のシーケンスである。これを本事例に適用すると，Web アプリケーションサーバに該当するものは，営業システムのサーバ（営業サーバ）と広告システムのサーバ（広告サーバ）である。

表 1「関連するシステムの URL」を見ると，営業サーバのホスト名は「eigyou.a-sha.example.jp」であり，広告サーバのホスト名は「koukoku.a-sha.example.jp」である。

システム名称	サーバ名称	URL	備考
SSO システム	SSO サーバ	http://sso.a-sha.example.jp	新規
営業システム	営業サーバ	http://eigyou.a-sha.example.jp	現状のまま
広告システム	広告サーバ	http://koukoku.a-sha.example.jp	現状のまま

図：本文の表 1 に記された，営業サーバと広告サーバのホスト名

これら 2 台のサーバを Cookie 送出の宛先とするには，両者が所属している A 社のドメイン名，すなわち「a-sha.example.jp」を Domain 属性に指定すればよい。

よって，正解は，「**a-sha.example.jp**」となる。

(2)

解答例

Cookie に Secure 属性を付ける。（20 字）

問題文は，「本文中の下線（Ⅱ）について，その対策を行っても，予期しなかったコネクションを介して，Web ブラウザから Cookie が平文で，ネットワーク上に意図せず流れてしまう可能性がある。これを防ぐために，SSO サーバが Cookie を発行するときに実施すべき方策を……述べよ」と記述されている。

下線（Ⅱ）は，〔SSO サーバの動作確認〕の第 3 段落にある。そこには，「SSO で Cookie を用いる場合，Cookie が漏えいしたときにセキュリティの問題が生じる。そこで，（Ⅱ）Cookie が平文でネットワークに流れないよう，表 1 中のサーバから返される全てのページを SSL/TLS 対応ページに変更した」と記述されている。

下線（Ⅱ）と照らし合わせるなら，問題文が言わんとしていることは，次のようになる。

「表 1 中のサーバから返される全てのページを SSL/TLS 対応ページに変更したつも

りでいても，予期せずに，SSL/TLS 非対応のページにリンクが貼られており，それを取得するコネクションを介して，Cookie がネットワーク上に流れてしまう可能性がある。これを防ぐために，SSO サーバが Cookie を発行するときに実施すべき方策を（述べよ）」。

そのような SSL/TLS 非対応のページの例として，「A 社のドメイン内に存在するが，表 1 には記載されていないサーバのページ」等が考えられる。設問 3（1）で解説したとおり，A 社のドメイン名が Domain 属性に設定されているので，アクセスチケットを含む Cookie を送出できるからだ。

したがって，本問は，そのような SSL/TLS 非対応のページを取得する HTTP 要求パケットによって，アクセスチケットを含む Cookie が漏えいすることを防ぐため，「SSO サーバが Cookie を発行するときに実施すべき方策」を問うている。

本問は，Cookie に関する一般的な知識から解を導く。

サーバがクライアント端末に Cookie を渡すときに Cookie に付与できる属性の一つに，Secure 属性がある。これを付与すると，HTTPS（SSL/TLS）で通信しているときだけ，クライアント端末は Cookie を送出するようになる。

したがって，SSO サーバが PC にアクセスチケットを発行する際に Secure 属性を付与すれば，予期せずに SSL/TLS 非対応のページを取得したときでも，アクセスチケットを含む Cookie がネットワーク上に流れることはない。

よって，正解は，「**Cookie に Secure 属性を付ける**」となる。

■設問 4

設問 4 の解説に入る前に，DSR 方式の負荷分散について解説する。

● DSR（Direct Server Return）方式とは

LB を用いてサーバを冗長化した場合，クライアント端末からサーバに送信するとき，そのパケットは LB を経由する。

サーバからクライアント端末に返信するとき，DSR 方式を用いなければ，そのパケットは，送信時と同じ経路を逆方向にたどる。一方，DSR 方式を用いると，LB を経由せずに，クライアント端末に直接返信される。DSR（Direct Server Return）という呼称は，返信（Return）がサーバ（Server）から直接（Direct）行われるという本方式の特徴をうまく表現している。

DSR 方式を用いることで，LB のパケット転送にかかる負荷を軽減することや，LB とそれを収容しているネットワーク機器間のトラフィックを緩和することなどの効果を期待できる。

●本事例における DSR（Direct Server Return）の構成

本事例では，SSO サーバを DSR 方式で負荷分散する。そのときの LB の動作が，〔負荷分散に関する設定と動作確認〕の第 1 段落の要点（1）～（3）に記述されている。その内容をまとめると，次のようになる。

表：SSO サーバを DSR 方式で負荷分散するときの LB の動作

設定する項目	具体的な値	本文中の記述箇所
振り分け先の SSO サーバ（2 台）	SSO サーバ 1 SSO サーバ 2	要点（1）
クライアント端末から見た，SSO サーバの IP アドレス	VIP アドレス	要点（1）
LB に設定する仮想 IP アドレス	VIP アドレス	要点（1）
SSO サーバに設定する仮想 IP アドレス	VIP アドレス	要点（3）

本事例では，振り分け先となるサーバは，SSO サーバ 1 及び SSO サーバ 2 である。

クライアント端末は，図 2 のシーケンスの項番②と④においては PC であり，項番⑥においては Web アプリケーションサーバ（営業サーバ又は広告サーバ）である。

クライアント端末から見た，SSO サーバの IP アドレスは，VIP アドレスとなる。その点は，要点（1）に「PC から SSO サーバへのリクエストは，LB に設定された VIP アドレスに送られ（る）」と記述されていることから分かる。ここで，VIP アドレスとは，LB や SSO サーバのインタフェースに設定された実 IP アドレスではなく，DSR 方式で用いる仮想 IP アドレスのことである。

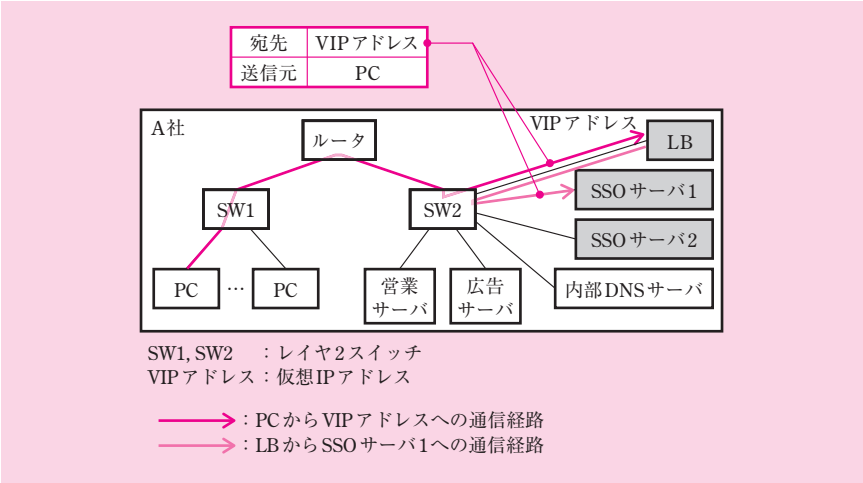
この VIP アドレスを，LB に設定する。その結果，SSO サーバ宛てのパケットを LB が受け取って，配下の SSO サーバ（2 台）へパケットを振り分けることができる。この設定は，通常の負荷分散で行われていることだ。

更に，この VIP アドレスを，振り分け先となる 2 台の SSO サーバに，それぞれ設定する。その点は，要点（3）に「振り分け先として決定された SSO サーバにリクエストパケットが転送されるが，このリクエストパケットの宛先アドレスは VIP アドレスのままである」と記述されていることから分かる。

VIP アドレスを SSO サーバにも設定するのはなぜだろうか。

結論から言うと，DSR 方式の特徴である，「サーバからクライアント端末への直接返信」を実現するためだ。

クライアント端末から見た，SSO サーバへのリクエストの宛先は，VIP アドレスである。このパケットを送信するときの通信経路は，振り分け先として SSO サーバ 1 が選択された場合，次の図のとおりとなる。



図：DSR 方式において，PC から SSO サーバ 1 へ送信するときの通信経路

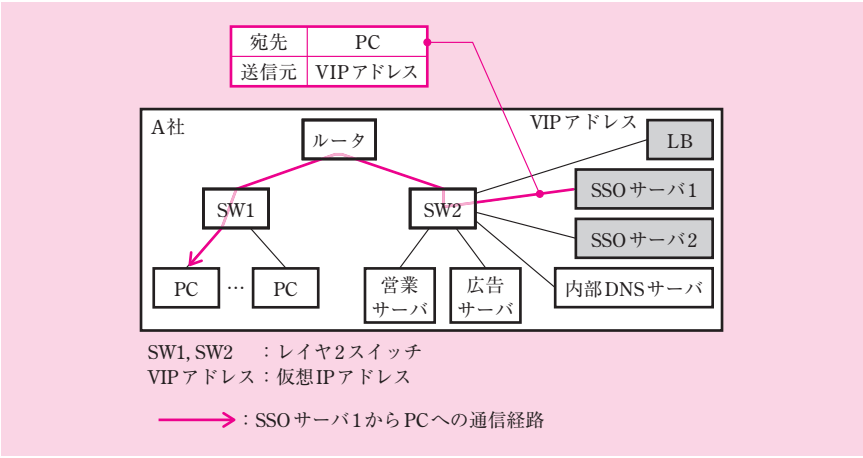
クライアント端末から送信された IP パケットが SSO サーバ 1 に到達するまでの間に，IP パケットの宛先は VIP のまま，送信元は PC のまま，変化しない（もちろん，IP ペイロードも変化しない）。

この間，IP パケットは，ルータ，LB を経由する。

ルータは，この IP パケットをルーティングするとき，VIP を目標とする ARP 要求を送信する。これに LB だけが ARP 応答を返信する。SSO サーバは ARP 応答を返信しないように設定する。この結果，ルータは，LB に IP パケットを転送する。この IP パケットをペイロードに収めたイーサネットフレームは，宛先 MAC アドレスが LB となる。

LB は，振り分け先を SSO サーバ 1 に決定した後，これに IP パケットを転送する。LB は SSO サーバの MAC アドレスをあらかじめ知っているため，この転送時に ARP のやり取りは行われない。この IP パケットをペイロードに収めたイーサネットフレームは，宛先 MAC アドレスが SSO サーバ 1 となる。

これに対する返信は，SSO サーバ 1 から直接行われる。このパケットを返信するときの通信経路は，次の図のとおりとなる。



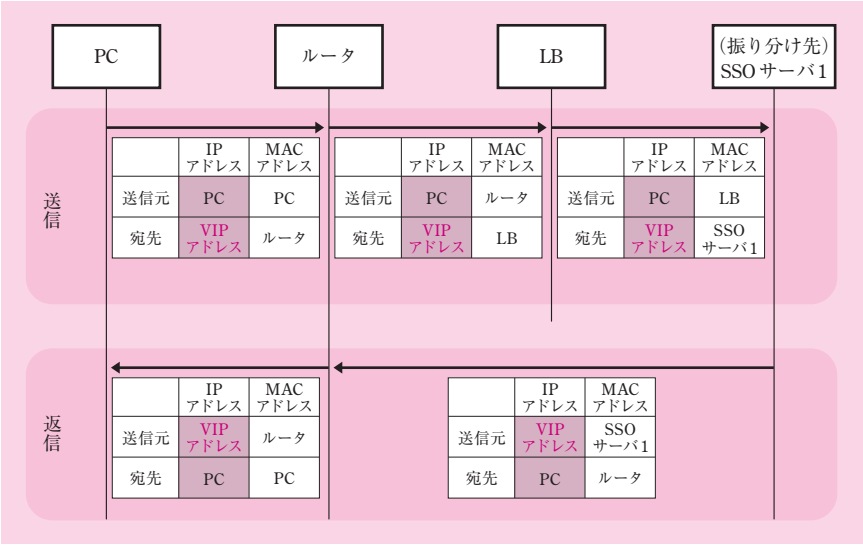
図：DSR 方式において，SSO サーバ 1 から PC へ返信するときの通信経路

返信パケットの送信元 IP アドレスは，送信時の宛先である，VIP アドレスになっていなければならない。さもないと，クライアント端末は，先ほどの VIP アドレス宛ての送信に対応する返信であるとは認識してくれないからだ。

このように，DSR 方式では，振り分け先サーバが返信パケットの送信元となるため，LB に設定した VIP アドレスを振り分け先サーバにも設定する必要があるわけだ。

ついでながら，LB から SSO サーバに転送されるリクエストパケットは，送信元が PC になっている。つまり，LB は，リクエストパケットを受け取ると，送信元／宛先 IP アドレスを変更せずに，そのまま SSO サーバに転送している。なぜならば，SSO サーバから PC に直接返信するので，SSO サーバが受け取るリクエストパケットの送信元は，PC でなければならないからだ。

以上をまとめると，PC が SSO サーバにアクセスするときの送信パケットは，宛先が VIP アドレス，送信元が PC のアドレスとなる。返信パケットは，その宛先と送信元が入れ替わったものとなる。



図：DSR 方式において，PC から SSO サーバにアクセスするときのパケット

参考までに，DSR は平成 21 年午後 I 問 3 で出題されたことがある。DSR の基本的な動作を出題しているので，本書の解説を後ほど確認しておくとよいだろう。

ここまで理解できれば，設問 4 を解く準備は整った。それでは，いよいよ小問の解説に移ろう。

(1)

解答例

SYN パケットには レイヤ 7 情報が含まれていないから （25字）

問題文は，「本文中の下線（Ⅲ）の理由を……述べよ」と記述されている。

下線（Ⅲ）は，〔負荷分散に関する設定と動作確認〕の第 2 段落にある。そこには，「要点（2）の動作から，DSR 方式の LB は（Ⅲ）Cookie などのレイヤ 7 の情報を基にして振り分け先サーバを選定するような方式には対応できない」と記述されている。

その要点（2）は，「振り分け先については，TCP コネクション確立のための SYN パケットが PC から届いた時点で，決定される」と記述されている。

したがって，本問は，SYN パケットが届いた時点では，レイヤ 7 の情報に基づいた

振り分け先を決定できない理由を問うている。

これは一般的な知識から解を導く。

Cookie などのレイヤ 7 の情報は，SYN パケットには含まれていない。レイヤ 7 の情報は，コネクション確立後のデータ通信フェーズでやり取りされるが，SYN パケットはコネクション確立フェーズの最初に送られるパケットであるからだ。

したがって，SYN パケットにはレイヤ 7 の情報が含まれていない以上，この情報に基づいて振り分け先を決定することはできない。よって，正解は解答例に示したとおりとなる。

参考までに，仮にレイヤ 7 の情報に基づいた負荷分散を行いたいのであれば，PC と LB 間のコネクションをいったん確立し，データ通信フェーズに入ってレイヤ 7 の情報が送られてから，振り分け先を決定すればよい。

(2)

解答例

Gratuitous ARP　又は　GARP

問題文は，「本文中の下線（Ⅳ）で，IP アドレス重複エラー検知に用いられる ARP の名称を答えよ」と記述されている。

下線（Ⅳ）は，〔負荷分散に関する設定と動作確認〕の第 4 段落にある。そこには，「(Ⅳ) IP アドレス重複エラーが検知された」と記述されているだけである。それゆえ，本問は，「IP アドレス重複エラー検知に用いられる ARP の名称」を問うているに過ぎない。

これは一般的な知識から解を導く。

IP アドレスの重複検知に用いられる ARP は，Gratuitous ARP である。これは，自 IP アドレスとの重複を検知したい IP ノードによって送信される ARP 要求であり，自 IP アドレスを目標アドレスに指定したものである。自 IP アドレスと同じアドレスをもつ IP ノードが存在しているならば，この ARP 要求に対して ARP 応答を返すので，自 IP アドレスの重複を検知することができる。

よって，正解は，「**Gratuitous ARP**」となる。又は，この略称である「**GARP**」も正解である。

Gratuitous ARP について，詳しくは《基礎編》の第 3 章「3.4.2　特殊な用途の ARP」を参照していただきたい。

(3)

解答例

VIPアドレスに対するARPリクエストに応答しないように設定する。（33字）

問題文は，「本文中の下線（V）の対処について，SSO サーバに対してどのような設定を行ったか」と記述されている。

下線（V）は，〔負荷分散に関する設定と動作確認〕の第 4 段落にある。そこには，「ループバックインタフェースを SSO サーバに設定した後に LB を再起動したところ，IP アドレス重複エラーが検知された。そこで，このエラーの原因を調査し，（V）SSO サーバに ARP 関連の設定を加えて対処した。この対処によってエラーが解消され(た)」と記述されている。

したがって，本問は，IP アドレス重複エラーが検知されることがないよう，SSO サーバに対して行った ARP 関連の設定について，問うている。

まず，この見出し全体の流れを確認しておこう。

第 1 段落から，LB に VIP アドレスを設定している。第 3 段落から，SSO サーバ（SSO サーバ 1 及び SSO サーバ 2）のループバックインタフェースに，それぞれ VIP アドレスを設定している。この状況で第 4 段落に至り，LB を再起動したとき，IP アドレスの重複が検知されたわけだ。

それでは，いよいよ解を導こう。

通常，IP ノードは，起動時に Gratuitous ARP を送信し，自 IP アドレスとの重複検知を行う。それゆえ，LB を起動すると，LB に設定された VIP アドレスの重複検知を行う。この ARP 要求に対し，同じく VIP アドレスをもつ SSO サーバが ARP 応答を返してしまう。この結果，IP アドレス重複エラーが検知されたのである。

これに対処するには，ループバックインタフェースに対し，VIP アドレスを目標とする ARP 要求に応答しないよう，設定する必要がある。

よって，正解は解答例に示したとおりとなる。

●参考：LB を経由した SSO サーバへのアクセスを実現するために必要な措置

この設定は，IP アドレス重複エラーを防ぐだけでなく，LB を経由した SSO サーバへのアクセスを実現するために必要な措置でもある。

図 1 を見ると，PC から VIP アドレスを宛先とする通信は，ルータを経由している

ことが分かる。ルータは，VIP アドレス（すなわ LB）にイーサネットフレームを送出するために，VIP アドレスを目標とする ARP 要求を送信する。

更に，図 2 中の Web アプリケーションサーバ（営業サーバ，広告サーバ）は，SSO サーバと通信している。PC と同様，SSO サーバへのアクセスは LB を経由するので，VIP アドレスを宛先とする通信を行う。図 1 を見ると，営業サーバと広告サーバは，LB と同じサブネットに収容されていることが分かる。それゆえ，同サーバも，VIP アドレスを目標とする ARP 要求を送信する。

この ARP 要求に対し，LB だけが ARP 応答を返すようにしておくことで，LB を経由した通信を実現できる。そのため，ここで出題された設定を SSO サーバにする必要があるわけだ。

さもないと，もしも LB の後に SSO サーバが ARP 応答を返すなら，こちらが ARP キャッシュに残ってしまうため，LB を経由した通信を阻害してしまう。

ARP の仕組みや ARP キャッシュについて，詳しくは《基礎編》の第 3 章「3.4.1 ARP の仕組み」を参照していただきたい。

問 2

出題趣旨

SaaS，PaaS などの利用が拡大しているが，これらを利用する企業ではインターネットとの通信量が格段に増加する。そのため，接続回線の増速，ファイアウォールやルータなどのネットワーク機器の性能拡張などが必要になる場合もある。また，社内のトラフィックに変化が生じることによって，改めて社内ネットワークの検証が必要となることもある。

負荷分散装置は，ネットワーク機器の性能拡張にも用いることができる。その場合は，一般に透過型負荷分散を用いる。これは，FW の他，IDS/IPS，ルータ，接続回線などの負荷分散にも応用可能であり，ネットワーク技術者として理解しておきたい技術である。

本問では，透過型負荷分散を題材として，TCP/IP の各レイヤの動作に関する理解と，性能設計，信頼性設計に関する基礎的な能力を問う。

採点講評

問 2 では，ファイアウォール（以下，FW という）に対する透過型の負荷分散を題材として，TCP/IP の各レイヤの動作，性能設計及び信頼性設計について出題した。全体として，正答率は高かった。

設問 2 は，End to End の通信における，レイヤ 2（データリンク層）～レイヤ 4（トランスポート層）に対する各種ネットワーク機器の動作に関する設問である。レイヤ 2 を中継するブリッジの動作，レイヤ 3 を中継するルータの動作，レイヤ 3・レイヤ 4 の情報に基づいてフィルタリングする FW の動作を正確に理解していれば，本文中の透過型 LB の動作は理解できるので，透過型 LB を知らなくても解答できるはずである。

設問 2（1）では，四つのアドレスが全て正しい解答は少なかった。（1）を一つでも間違えた人は，ブリッジ・L2SW やルータ・L3SW の動作をよく復習してほしい。

設問 3 は，信頼性設計と性能設計における，基本的な考え方や発想を問う設問であるが，（2）“い”では，本文中に示されている要件や条件を見落としたと推測される誤った解答が多く見受けられた。（社内 NW）⇔（インターネット・DMZ）の通信は全て Proxy を経由する，LB4 は FW 負荷分散と Proxy 負荷分散を併用している，という二つの条件が念頭にあれば，図 3 から，LB4 の負荷が最も高そうだ（ボトルネックになりそうだ）という見当がつくはずである。トラフィックモデルなどの要件・条件を正確に把握することは，信頼性設計・性能設計の基礎である。限られた時間で本文を丁寧に読み解き，正確に理解することを心掛けてほしい。

設問			解答例・解答の要点		備考
設問 1		ア	スループット		
		イ	パケット		
		ウ	維持		
設問 2	(1)	(A)	宛先 IP アドレス	機器 b	
			宛先 MAC アドレス	FW1	
		(B)	宛先 IP アドレス	機器 b	
			宛先 MAC アドレス	FW2	
	(2)	宛先 IP アドレスを書き換えられない。			
	(3)	セッション単位に，2 台の LB が同じ FW を選択する。			

（表は次ページに続く）

設問		解答例・解答の要点		備考
設問 3	(1)	故障発生時の性能を不足させないため		
	(2)	あ	99	
		い	180	
	(3)	FW を経由する LB 間の経路の障害を検出できる。		
	(4)	リトライアウトを待たずにコネクションの切断を検知できる。		

本問は，ファイアウォール（以下，FW と称する）の負荷分散をテーマに，負荷分散装置（以下，LB と称する）を用いた故障対策，LB の性能拡張策（転送データ量の見積り），等を問うている。

本事例に登場する LB は，「透過モード」と呼ばれる機能をもっており，FW の負荷分散を実現するために用いられている。

本問を首尾よく解くには，本文に説明されている透過モードの仕組みを理解しておく必要がある。通常のサーバ負荷分散の仕組みとどのように異なるのか，両者を比較しながら，その概要を押さえておこう。

以降の説明で，サーバ負荷分散に用いるモードを「サーバ負荷分散モード」と称することにする。

●サーバ負荷分散モードの動作

サーバ負荷分散モードで動作する LB は，その内部がルータと L2SW で構成されている。このルータと L2SW を，それぞれ「内部ルータ」「内部 SW」と称することにする。

負荷分散の対象となるサーバを「SV」と称する。外部に公開する SV の IP アドレスは，仮想 IP アドレス（以下，「VIP」と称する）である。

LB は，SV に対するアクセスを物理サーバに振り分ける。これら振り分け先の物理サーバは，LB に 2 台以上接続できるが，ここの解説では 2 台あるものとしよう。SV と区別するため，物理サーバを「SV1」「SV2」と称する。

サーバ負荷分散モードでは，内部ルータのポートに VIP を設定し，これをクライアント側のネットワークに接続する。内部 SW のポートに SV1 と SV2 を接続する。

クライアント端末は，SV にアクセスするとき，VIP を宛先とする IP パケットを送信する。

これが内部ルータに到達すると，振り分け先が決定され，宛先 IP アドレスが変換される。変換先の IP アドレスは，振り分け先サーバ（SV1 又は SV2）の実 IP アドレスになる。

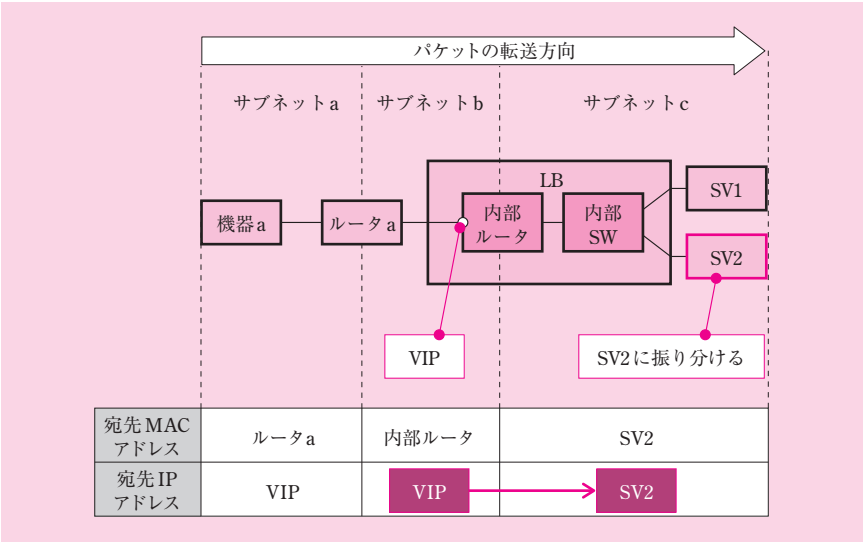
このアドレス変換の様子を，図「サーバ負荷分散モードの LB を使用したときのパケットの転送」に示す。この図では，クライアント端末は「機器 a」である。

SV2 が振り分け先に決定された場合，機器 a から SV2 に至る経路は，

機器 a → ルータ a → LB の内部ルータ → LB の内部 SW → SV2

となる。

図の中で，宛先 IP アドレスは，内部ルータを転送するときに「VIP」から「SV2 の実 IP アドレス」に変換されている。



図：サーバ負荷分散モードの LB を使用したときのパケットの転送

●透過モードの動作

あらかじめ断っておくが，「透過モード」はベンダ依存の技術なので，その動作は様々である。ここでは，あくまで本文の説明に基づいて解説することにしよう。

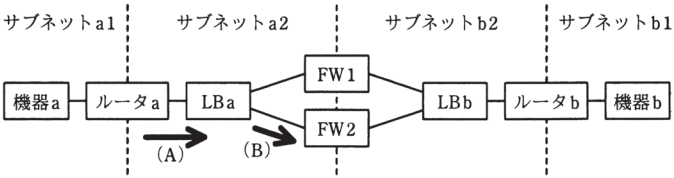
透過モードで動作する LB は，その内部が L2SW だけで構成されている。

透過モードは，サーバ負荷分散モードとは異なり，VIP を設定したり，振り分け時に宛先 IP アドレスを変換したりしない。その代わり，宛先 MAC アドレスを変換する。

その具体的な動作は，〔FW の負荷分散〕の第 2 ～第 3 段落の中に詳しく記されている。

まずは，その箇所を抜粋して掲載しよう。設問の都合上，あえて本文では詳しく書かれていない動作もあるが，適宜補足していく。

LB を使用した FW の負荷分散の基本構成を図 2 に示す。



注記 1　(A)，(B) は設問 2 (1) で使用する。
注記 2　各ルータのルーティング情報は次のとおりである。

ルータ名	宛先	ゲートウェイ
ルータa	サブネットb1	FW1
ルータb	サブネットa1	FW1

図 2　FW の負荷分散の基本構成

図 2 における LB の動作は次のとおりである。

(1) ①FW はセッションの終端ノードではないので，FW の負荷分散では，パケットに対して行える操作に制約があり，サーバ負荷分散で使われる仮想 IP アドレスを用いる方式は使えない。そこで，図 2 の LB によるパケット転送の動作は，次のとおりとなる。

・FW1，FW2 の MAC アドレスは，LB にあらかじめ登録してある。
・LB は，FW 宛てのイーサネットフレームに対し，宛先 MAC アドレスを振り分け先 FW のものに書き換えて転送する。
・その他のイーサネットフレームの転送は，ブリッジと同じ動作となる。

本事例では，FW の負荷分散を実現するために透過モードを用いる。

本文の図 2 は，FW の負荷分散の基本構成を示している。

機器 a と機器 b 間の通信は，FW を経由している。振り分け先となる物理 FW は，FW1 と FW2 の 2 台がある。ここの解説では，送信側（クライアント端末）を「機器 a」，受信側（サーバ）を「機器 b」と便宜上解釈することにしよう。なお，両者の役割を入れ替えても，LB の仕組みは変わらない。

機器 a は，機器 b にアクセスするとき，機器 b を宛先とする IP パケットを送信する。

ルータ a は，これを受け取ると図 2 のルーティングテーブルに従って転送する。機器 b はサブネット b1 に収容されているので，ネクストホップは FW1 となる。それゆえ，ルータ a は，FW1 を宛先 MAC アドレスとするイーサネットフレームを送出する。

LBa は，これを受け取ると，〔FW の負荷分散〕の第 3 段落（1）に記された，透過モードに特有の動作を行う。そこには，「FW1，FW2 の MAC アドレスは，LB にあらかじめ登録してある。LB は，FW 宛てのイーサネットフレームに対し，宛先 MAC アドレスを振り分け先 FW のものに書き換えて転送する」と記述されている。

LBa は，まず，振り分け先の FW を決定する。次いで，振り分け先が FW1 の場合，FW1 が接続されているポートにイーサネットフレームを転送する。一方，振り分け先が FW2 の場合，イーサネットフレームの宛先を FW2 に変換し，FW2 が接続されているポートに転送するのである。この仕組みにより，FW の負荷分散を実現している。

振り分け先の FW は，これを受け取ると，ネクストホップであるルータ b に転送する。この宛先 MAC アドレスは，ルータ b となる。

FW とルータ b の間に LBb があるが，LBb は宛先 MAC アドレスを変換しない。そのことは，「その他のイーサネットフレーム（つまり，FW 以外のものを宛先とするイーサネットフレーム）の転送は，ブリッジと同じ動作となる」と記述されていることから分かる。

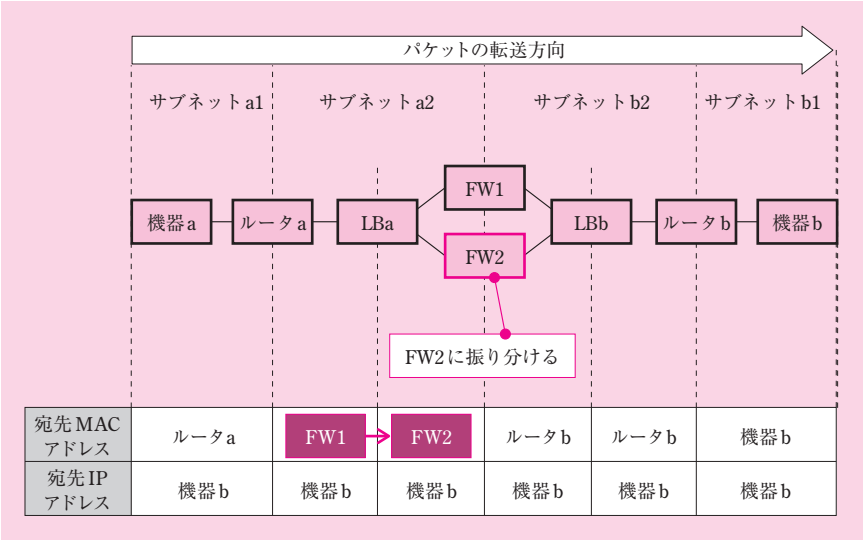
このアドレス変換の様子を，図「透過モードの LB を使用したときのパケットの転送」に示す。

FW2 が振り分け先に決定された場合，機器 a から機器 b に至る経路は，

機器 a → ルータ a → LBa → FW2 → LBb → ルータ b → 機器 b

となる。

図の中で，宛先 MAC アドレスは，LBa を通過するときに「FW1」から「FW2」に変換されている。



図：透過モードの LB を使用したときのパケットの転送

サーバ負荷分散モード，透過モード，それぞれの LB の動作について理解できたので，いよいよ設問の解説に移ろう。

■設問 1

解答例

ア：スループット
イ：パケット
ウ：維持

ア

空欄アを含む文章は，〔新 NW 構成の検討〕「(1) LB 転送データ量の見積り」の第 1 段落の中にある。そこには「LB の仕様には，1 秒当たりの転送データ量である［ア］が記載されている」と記述されている。

もし「LB の仕様……に記載されている」という文脈を考慮せず，「1 秒当たりの転送データ量である［ア］」とだけ書いてあったならば，空欄アに該当する字句は複数思い浮かぶ。

例えば，「1 秒当たりの転送データ量」をそのまま置き換えた技術用語である「転送速度」，あるいは，これによく似た「伝送速度」「帯域」などが，空欄アの候補に思えるだろう。

更には，「1 秒当たりの転送データ量」を包含する技術用語である，「スループット」も候補に思いつくだろう。包含する技術用語としては「性能」もあるが，さすがにこれは意味が広すぎるので，他に適切な語がない限り候補から外しておく。

そこで，ここに挙げた用語のうち，転送速度，伝送速度，帯域，スループットについて，それぞれ解説しよう。その上で，「LB の仕様……に記載されている」という文脈を考慮に入れた場合，最も適切なものはどれかを考察しよう。

●転送速度，伝送速度，帯域

転送速度（transfer rate）という語は，「デジタルデータが 1 秒当たり何ビット転送されるか」を意味している。デジタルデータであれば，ネットワーク回線を流れるデータであっても，コンピュータと周辺機器でやり取りされるデータであってもよい。

伝送速度という語は，転送速度と同義であるが，主に，ネットワーク回線を流れるデータを対象とする。

帯域（bandwidth）という語は，「周波数の幅」を意味している。ここで言う「周波数の幅」とは，通信が関係する様々な周波数の幅（例えば，アナログ信号の搬送波の変調に用いる周波数の幅，光ファイバのような物理媒体が伝送できる周波数の幅，等）を指す。

帯域が広ければ，単位時間当たりの通信量が多くなる。ここから転じ，搬送波をもたないデジタル信号の通信においても，1 秒当たりの通信量（転送ビット量）の意味でこの語が慣用的に使われている。すなわち，伝送速度と同じ意味で用いられている。ただ，「帯域を割り当てる」「帯域を制御する」といった用例から分かるとおり，1 本の物理回線を複数の通信チャネルで多重化したとき，通信チャネルの伝送速度を指して帯域という語を用いることがある。

●スループット

スループットという語は，単位時間当たりの処理量を意味している。

この処理量については，明確な定義が存在していないが，一般的に言って，単位時間当たりに「めいっぱい行った」量を指すことが多い。

スループットの代表例は，サーバが 1 秒当たりに処理するトランザクション数である。

スループットという語をネットワーク機器が行う処理に適用する場合，フレーム転

送以外の複雑な制御を含む何らかの処理を，めいっぱい行っている状況で用いられることが多い。

この説明は，RFC1242 が述べるスループットの定義と合致している。ここには，「機器による損失がなく，受け渡されたフレームを処理する最大の速度（The maximum rate at which none of the offered frames are dropped by the device）」と記述されている。ここで，「機器による損失がなく」とわざわざ断り書きを述べていることから，スループットは，ネットワーク回線のワイヤスピードを下回ることが示唆されている。その処理の複雑さゆえに，ワイヤスピードでパケットが受け渡されたら，損失しかねないわけだ。

この説明と調和する「スループット」の用例は，ネットワーク機器のデータシートに見ることができる。「1 秒当たりの転送データ量」という指標を表す語として，振り分け処理を行う LB や，セキュリティ処理を行う FW のデータシートでは，「スループット」が用いられるのである（例：F5 Networks 社の BIG-IP，Cisco Systems 社の Cisco Application Control Engine）。一方，ワイヤスピードで転送する L2SW のデータシートでは，「転送レート」及びそれに類する語が用いられている（例：I-O DATA 社のスイッチ，等）。つまり，ネットワーク機器のデータシートに「転送速度」ではなく「スループット」と書いてあったら，当該機器の 1 秒当たりのデータ転送量がワイヤスピードではないことを示唆しているわけだ。

以上をまとめると，スループットという語が適用される「処理量」には，明確な定義が存在していない。とはいえ，（RFC1242 は数ある定義の一つに過ぎないが，）損失しないぎりぎりのところまで，めいっぱい最大速度で行ったときの，実際の「処理量」というニュアンスが込められているのである。

それでは，転送速度，伝送速度，帯域，スループットの意味や用例が理解できたところで，いよいよ解を導こう。

●解の導出

「1 秒当たりの転送データ量」は「LB の仕様」に記載されたものである。この点を踏まえ，転送速度，伝送速度，帯域，スループットのうち，空欄アに当てはまる最も適切な字句はどれだろうか。

LB がデータを転送するときは，パケットをただ転送するだけでなく，振り分け処理という複雑な制御が伴っている。それゆえ，LB を収容しているネットワークのワイヤスピードに追いつかないことがある。それゆえ，「LB の仕様」としてデータシートに記載されるべき，最も適切な技術用語は，「**スループット**」である。

よって，これが空欄アに該当する字句となる。

イ

空欄イを含む文章は，〔新 NW 構成の検討〕(1) LB の転送データ量の見積りの第 1 段落にある。そこには，「LB の仕様には，1 秒当たりの転送データ量であるスループットが記載されている。しかし，LB には，1 秒当たりの転送［イ］数に上限があるので，実際の最大スループットは転送パケット長によって変化する」と記述されている。

「転送パケット長」は，1 パケット当たりの転送データ量のことである。この値は，1 秒当たりの転送データ量に影響を与える。両者の関係は次の式となる。

1 秒当たりの転送データ量＝ 1 秒当たりの転送パケット数
× 1 パケット当たりの転送データ量

したがって，1 秒当たりの転送パケット数が上限値に達すると，最大スループット（1 秒当たりの転送データ量の最大値）は，転送パケット長によって定まる。

よって，空欄イに該当する字句は，「**パケット**」である。

ウ

空欄ウを含む文章は，〔新 NW 構成の設計〕(2) FW の故障対策の「・FW の故障発生時の影響軽減機能」にある。そこには，「現行 NW の Active-Standby 構成と異なり，新 NW では，FW の故障発生時にセッション［ウ］ができない」と記述されている。

新 NW では，〔現行 NW の移行〕の第 2 段落にあるとおり，FW を「Active-Active 構成」で負荷分散する。

要するに，空欄ウの文脈が言わんとしているのは，「現行 NW の Active-Standby 構成で使用していた故障対策の機能が，新 NW の Active-Active 構成では使用できない」ということだ。その機能は，故障発生時のセッションの扱いに関わるものである。

さて，本事例に登場する FW の機能について，〔現行 NW の移行〕の第 1 段落の中に，「FW では，……レイヤ 4 までの動的フィルタリングを行う」と記述されている。したがって，FW はステートフルインスペクション機能をもつことが分かる。本文全体を通じ，「セッション」という語が使用されているが，これは，ステートフルインスペクション機能によって動的に許可された通信のことを指している。

一般的に言って，ステートフルインスペクション機能を有する多くの商用 FW は，Active-Standby 構成下でステートフルフェールオーバを実現することもできる。ステートフルフェールオーバとは，障害発生時に Active 側から Standby 側にフェール

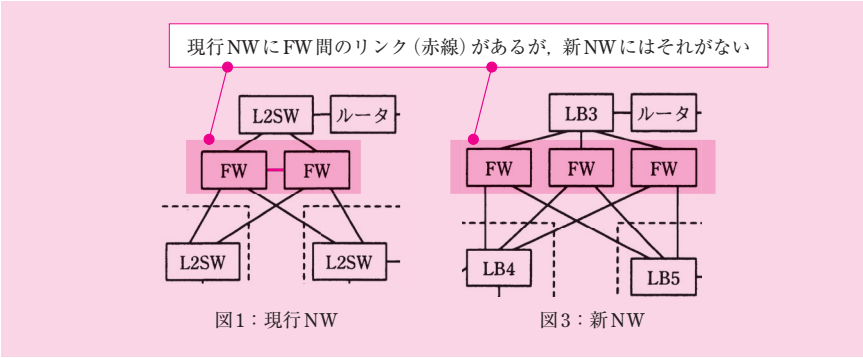
オーバする際，Standby 側がセッションを引き継ぐ機能である。このセッション維持を実現するため，2 台の FW 間をフェールオーバリンクで接続し，Active 側が動的に許可したセッション情報を Standby 側に常時転送して，両者で同期を取っている。

ステートフルフェールオーバ機能は，一般的には Active-Standby 構成で使用している。Active-Active 構成では，使用できない製品があったり，使用時の制約を設けている製品があったりする。その制約とは，例えば，「2 台の FW の合計トラフィック量が，各 FW のトラフィック容量に収まっていること」などである。

ここで，空欄ウの文脈と照らし合わせて，「現行 NW で使用していたが，新 NW では使用できなくなった故障対策の機能は，ステートフルフェールオーバである」という仮説を立ててみよう。

すると，空欄ウを含む文は，「現行 NW の Active-Standby 構成と異なり，新 NW では，FW の故障発生時にセッション維持ができない」となる。

仮説が正しければ，現行 NW の FW 間にはフェールオーバリンクが存在し，かつ，新 NW にはそれが存在しないはずだ。その点，現行 NW のネットワーク構成を記した図 1 を見ると，Active-Standby 構成の FW 同士が接続されている。一方，新 NW のネットワーク構成を記した図 3 を見ると，Active-Active 構成の FW 間は接続されていない。したがって，この仮説は，本文の記述と合致している。



図：FW 間のリンクの有無に関する，現行 NW（図 1）と新 NW（図 3）の比較

更に，先ほど解説したとおり，ステートフルフェールオーバ機能は，多くの場合，Active-Standby 構成で使用している。Active-Active 構成では使用できなかったり，使用できたとしても何らかの制約が設けられていたりする。したがって，現行 NW で使用していたが新 NW では使用できなくなった故障対策機能がステートフルフェールオーバであるという仮説は，一般的な知識とも調和していると言えよう。

以上より，この仮説は，検証に耐え得る確かなものであることが分かる。したがって，ここから解を導くことが妥当である。

よって，空欄ウに該当する字句は，「**維持**」である。

■設問 2

(1)

解答例

(A) 宛先 IP アドレス：機器 b
宛先 MAC アドレス：FW1
(B) 宛先 IP アドレス：機器 b
宛先 MAC アドレス：FW2

本問は，図 2「FW の負荷分散の基本構成」の（A），（B）が示すパケットの，宛先 IP アドレスと宛先 MAC アドレスを問うている。解答に際し，アドレスは図 2 中の機器名を用いる。

図 2 の（A），（B）について，問題文は，「機器 a と機器 b との間の TCP コネクション上のパケットを表し，矢印はその転送方向を表す」と記述されている。

図 2 は，FW の負荷分散の基本構成を示したものである。LB は透過モードを使用しており，LBa による振り分け先は FW2 になっている。

●（A），（B）の宛先 IP アドレス

先ほど述べたとおり，（A），（B）は，「機器 a と機器 b との間の TCP コネクション上のパケット」である。その矢印は，機器 a から機器 b に向かっている。したがって，IP パケットの宛先は，どちらも「**機器 b**」となる。

●（A）の宛先 MAC アドレス

イーサネットフレームの宛先は，同一サブネットワークにおいてイーサネットフレームの転送先となる IP ノードだ。そのため，（A），（B）それぞれのパケットが，どのノードに転送されているかに基づいて解を導く必要がある。

パケット（A）は，ルータ a から LBa に転送されるパケットである。

冒頭の「●透過モードの動作」で解説したとおり，透過モードの LB は，その内部が L2SW になっている。したがって，ルータ a から見た，イーサネットフレームの転

送先となる IP ノードは LB ではない。

ルータ a は，宛先 IP アドレスが機器 b である IP パケットを受け取ると，ルーティングテーブルに従って，ネクストホップを決定する。このネクストホップが，イーサネットフレームの転送先となる。

図 2 の中に，ルータ a のルーティング情報が記されている。機器 b はサブネット b1 に収容されている。宛先がサブネット b1 であるとき，ネクストホップは FW1 である。なお，図 2 には「ゲートウェイ」と書かれているが，このゲートウェイはネクストホップと同義である。

したがって，パケット（A）の宛先 MAC アドレスは，「**FW1**」となる。

●（B）の宛先 MAC アドレス

〔FW の負荷分散〕の第 3 段落（1）の中に，透過モードの LB に関する説明がある。そこには，「FW1，FW2 の MAC アドレスは，LB にあらかじめ登録してある。LB は，FW 宛てのイーサネットフレームに対し，宛先 MAC アドレスを振り分け先 FW のものに書き換えて転送する」と記述されている。

パケット（A）を受け取った LBa は，まず，振り分け先の FW を決定する。図 2 では，振り分け先を FW2 としている。

次いで LBa は，宛先 MAC アドレスを，本文の記述どおり，振り分け先の FW2 のものに書き換えて転送する。

したがって，パケット（B）の宛先 MAC アドレスは，「**FW2**」となる。

●解の導出

以上をまとめると，パケット（A），（B）の，宛先 IP アドレスと宛先 MAC アドレスは次のようになる。よって，これが求める解となる。

（A）	宛先 IP アドレス	機器 b
	宛先 MAC アドレス	FW1
（B）	宛先 IP アドレス	機器 b
	宛先 MAC アドレス	FW2

(2)

解答例

宛先IPアドレスを書き換えられない。（18字）

問題文は，「本文中の下線①はどのような制約か」と記述されている。

下線①は，〔FW の負荷分散〕の第 3 段落（1）の中にある。そこには，「① FW はセッションの終端ノードではないので，FW の負荷分散では，パケットに対して行える操作に制約があり，サーバの負荷分散で使われる仮想 IP アドレスを用いる方式は使えない」と記述されている。

「サーバの負荷分散で使われる仮想 IP アドレスを用いる方式」とは，冒頭で解説した，サーバ負荷分散モードによる振り分け方式のことである。

下線①を考察するに当たり，まずは，下線①のすぐ後にある，「サーバの負荷分散で使われる仮想 IP アドレスを用いる方式は使えない」という記述に着目してみよう。

冒頭で解説したとおり，サーバ負荷分散モードは，負荷分散に仮想 IP アドレスを用いる。外部に公開するサーバの IP アドレスを仮想 IP アドレスとし，LB に仮想 IP アドレスを設定する。つまり，仮想 IP アドレスを宛先とするセッションでは，終端ノードが LB になっている。クライアント端末からサーバにアクセスするとき，実際には，クライアント端末から LB に接続しているわけだ。

このセッションにおいて，LB は，クライアント端末から送信されたパケットを受け取ると，その宛先 IP アドレスを振り分け先のサーバの実 IP アドレスに書き換えて転送する。こうして，サーバの負荷分散を実現している。

セッションの通信経路上にある FW は，果たして，この方式で負荷分散できるだろうか。

クライアント端末からサーバにアクセスするセッションにおいて，宛先 IP アドレスは，送信時はサーバとなり，返信時はクライアント端末となる。言うまでもなく，宛先 IP アドレスが FW になることはない。それゆえ，サーバ負荷分散モードでは，FW の負荷分散を行えないことが分かる。

それでは，これまでの考察を踏まえ，いよいよ下線①の「制約」を導いてみよう。

サーバ負荷分散モードの特徴は，LB が宛先 IP アドレスを書き換えることだ。そこで，「サーバ負荷分散モードを使用して宛先 IP アドレスを書き換えてしまうなら，どうなるだろうか」と発想を転換してみよう。宛先 IP アドレスを書き換えることでかえって不都合が生じるのであれば，「宛先 IP アドレスを書き換えてはならない」とい

う制約があると結論付けることができる。よって，これが求める解となるわけだ。

パケットの宛先 IP アドレスを変更する操作を行えば，当然ながら，終端ノードが変化してしまう。そのままでは本来意図した通信を行えないことは明らかである。それゆえ，元の終端ノードに戻すために，宛先をもう一度変更する操作も必要となる。つまり，クライアント端末とサーバ間の通信経路上に，2 台の LB が必要となる。1 台目を通過したときに宛先 IP アドレスを何らかの値に変更し，かつ，2 台目を通過したときに元に戻すわけだ。

宛先 IP アドレスはルータの経路制御で用いられているので，パケットの宛先 IP アドレスを変更すると，経路を変化させることができる。その特徴を生かし，「1 台目の LB で宛先 IP アドレスを変更し，振り分け先の FW を経由するように経路制御する」という素朴なアイデアを思いつくかもしれない。しかしながら，2 台目の LB で，パケットの宛先 IP アドレスを元に戻す必要があることを忘れてはならない。

例えば，インターネット上の任意のサーバ宛てに，社内のクライアント端末から，FW を経由してアクセスするケースを考えてみよう。サーバの IP アドレスは一つに定まっていない。1 台目の LB で宛先 IP アドレスを変更した場合，2 台目の LB は本来のアドレスをどのようにして知り得るのだろうか。宛先 IP アドレスを書き換えるだけの単純な仕組みでは，不可能だ。

したがって，終端ノードではない FW を負荷分散しようとするあまり，通信経路上の LB で宛先 IP アドレスをむやみに書き換えるなら，任意のサーバとの通信が成り立たなくなってしまう。このような不都合が生じる以上，「宛先 IP アドレスを書き換えられない」という制約が存在すると言えよう。

よって，正解は，「**宛先 IP アドレスを書き換えられない**」となる。

(3)

解答例

セ	ッ	シ	ョ	ン	単	位	に	,	2	台	の	L	B	が	同	じ	F	W	を	選	択	す	る	。

（25 字）

問題文は，「本文中の下線②では，LBa のパケット振り分け動作と LBb のパケット振り分け動作との関係について，ある条件が成立しなければならない。その条件を……述べよ」と記述されている。

下線②は，〔FW の負荷分散〕の第 3 段落（2）の中にある。そこには，「② LBa と LBb によるパケットの振り分けは，FW での動的フィルタリングが正しく行われるよ

うに実行される必要がある。LB は，次のように振り分け先を管理する」と記述されている。この振り分け動作の仕様は二つあり，

- LB は，セッション単位で振り分け先 FW を決定する。
- セッションと振り分け先 FW との対応は，セッションの生成・消滅に合わせて動的に管理される。

と記述されている。

本文に記された振り分け動作は，振り分け先を決定する LB に当てはまるものである。その LB とは，具体的に言うと，パケットを送信した側に位置する LB である。

図 2 の構成を例にすると，機器 a から機器 b 宛てに転送するパケットについては，LBa が振り分け先を決定する。一方，それとは逆方向に転送するパケットについては，LBb が振り分け先を決定する。つまり，行きと帰りで別々の LB が振り分け先を決定しているわけだ。

下線②は「FW での動的フィルタリング」に言及している。設問 1 で解説したとおり，本事例に登場する FW は，ステートフルインスペクション機能をもつ。FW は，レイヤ 4 までの情報に基づき，セッションの生成から消滅までの間，行きと帰りの双方向のやり取りで，状態遷移が適切に行われているかを監視している。許可されたセッションに合致しないパケットは，全て遮断する。

したがって，FW の動的フィルタリングが正しく動作するには，2 台の LB が，行きと帰りのそれぞれで，セッション単位に同じ FW を選択する必要がある。セッションの途中で異なる FW にパケットを振り分けてしまうと，新たな振り分け先となった FW が「受け取ったパケットは，これまで自分の許可したセッションに合致しない」と判断し，これを破棄してしまうからだ。

よって，正解は，「**セッション単位に，2 台の LB が同じ FW を選択する**」となる。

■設問 3

(1)

解答例

故障発生時の性能を不足させないため（17字）

問題文は，「本文中の下線③で，FW を 3 台構成とする目的を……述べよ」と記述さ

れている。

下線③は，〔新 NW 構成の設計〕の第 1 段落にある。そこには，「現行 NW に FW を 1 台追加し，③3 台構成とする」と記述されている。

現行 NW から新 NW への移行のうち，FW に関する記述が，〔現行 NW の移行〕の第 2 段落の中にある。そこには，「移行後の新 NW におけるインターネットアクセスの通信量を見積もった。その結果，インターネットとの通信量の増加によって，FW ……は，現状の 1.4 倍以上の処理能力が必要であることが判明した。そこで……，FW の性能拡張策として，現行 NW での Active-Standby 構成から Active-Active 構成に変更する案を検討することにした」と記述されている。

1 台の FW に求められる処理能力について，現行 NW と新 NW とを比較してみよう。

現行 NW における，1 台当たりの FW の処理量を 1 とする。現行 NW は Active-Standby 構成なので，FW 経由の通信は，1 台の FW だけで処理している。

新 NW の通信量は，現行の 1.4 倍になる。現行のままだと，1.4 倍以上の処理能力が必要となるため，性能拡張策が求められている。

本文の記述どおり，3 台からなる Active-Active 構成に変更した場合，1 台当たりの FW の処理量はどうなるだろうか。各 FW に負荷が平準化される場合，

$$1.4 \div 3 \fallingdotseq 0.47$$（小数点第 2 位を四捨五入）

となる。こうしてみると，FW 全体として見れば，処理能力に結構余裕があることが分かる。

単純に考えれば，新 NW の通信量が現行の 1.4 倍になり，FW を Active-Active 構成にするわけなので，FW の台数は 2 台で済むはずだ。2 台からなる Active-Active 構成に変更した場合，1 台当たりの FW の処理量は，

$$1.4 \div 2 = 0.7$$

となるからだ。

したがって，本問の解を「新 NW の通信量が現行の 1.4 倍になるため」としてはならない。通信量の増加に対処する性能拡張だけが目的であれば 2 台で済むのに，なぜ 3 台にしたのか，この解では説明できていないからだ。

ここで，第 3 段落の「新 NW 構成の設計に当たって……検討した課題」という記述に着目してみよう。2 つ目の課題は，「(2) FW の故障対策」である。本文の「(2) FW の故障対策」の中には，FW を 3 台にした理由が述べられてはいない。とはいえ，少

なくとも，「FW の故障」を念頭に置いていることは分かる（もし書いてあったら，この設問はそれを転記するだけとなり，そもそも出題に値しないだろう）。

これをヒントにして，「2 台だけで Active-Active 構成にするとしたら，どのようなことが懸念されるか」を考えてみよう。

2 台のうち 1 台が故障すると，1.4 倍以上の処理量を 1 台でまかなうことになる。この状態では性能不足に陥ってしまう。

その懸念は，3 台の Active-Active 構成にすれば解消される。3 台のうち 1 台が故障しても，残り 2 台で Active-Active 構成になるので，前述のとおり，1 台当たりの FW の処理量はまだ 0.7 に留まるからだ。したがって，3 台構成にする目的は，1 台の故障発生時でも性能不足に陥らないようにするためであることが分かる。

よって，正解は解答例に示したとおりとなる。

(2)

解答例

あ：99
い：180

本問は，表 2「各 LB の転送データ量」の［　あ　］，［　い　］に入れる適切な数値を問うている。

なお，表の注記から分かるように，表 2 に記載された転送データ量は，「FW 全体の転送データ量を 100 としたときの値」である。「FW 全体の転送データ量」とは，Active-Active 構成をとる 3 台の FW の転送データ量の合計である。

表 2　各 LB の転送データ量

LB	転送データ量 1)	転送データ量に対する現行 LB の性能
LB3	あ	充足
LB4	い	不足
LB5	11	充足

注 1)　FW 全体の転送データ量を 100 としたときの値

表 2 の数値をどのように見積もったのかについて，〔新 NW 構成の設計〕(1) LB の転送データ量の見積りの第 2 段落の中で，「Proxy のキャッシュ効果，及び FW でのパケット破棄を無視し，表 1 に基づいて計算した各 LB の転送データ量は，表 2 のよう

になる」と記述されている。

したがって，表 2 の空欄を埋めるには，表 1「通信区間ごとの FW の転送データ量」を用いる必要がある。

なお，表の注記から分かるように，表 1 に記載された転送データ量も，「FW 全体の転送データ量を 100 としたときの値」である。

表 1　通信区間ごとの FW の転送データ量

通信区間	転送データ量 1)
インターネット ⇔ 社内 NW	89
インターネット ⇔ DMZ	10
社内 NW ⇔ DMZ	1

注 1)　FW 全体の転送データ量を 100 としたときの値

表 1 について，同段落の中で，「新 NW における通信量の見積りによる，通信区間ごとの FW の転送データ量は，表 1 のとおりである」と記述されている。したがって，表 1 は，新 NW の構成と照らし合わせながら理解する必要がある。その構成は，図 3「新 NW 構成案（抜粋）」に示されている。

図 3 を見ると，1 台の LB は，一つ以上の通信区間のトラフィックを転送していることが分かる。LB の転送データ量は，転送している通信区間のデータ量を合計した値となる。

そこで，次の手順に従って，解を導くことにしよう。まず，表 1 に基づき，通信区間ごとに，転送データ量を新 NW の構成図に展開する。次いで，LB ごとに，LB が転送している通信区間のデータ量を合計すれば，解が求まる。

解の導出に先立ち，表 2 の見積りに関し，「Proxy のキャッシュ効果……を無視（する）」と述べられている点を補足しておこう。クライアント端末とサーバ間のトラフィックが Proxy を経由する場合，「クライアント端末と Proxy 間のデータ転送量と，Proxy とサーバ間のデータ転送量が同じである」と仮定して見積もっていることが，この記述から分かる。

同様に，「FW でのパケット破棄を無視（する）」と述べられている。クライアント端末とサーバ間のトラフィックが FW を経由する場合，「クライアント端末と FW 間のデータ転送量と，FW とサーバ間のデータ転送量が同じである」と仮定して見積もっていることが分かる。

要するに，Proxy と FW を経由する場合，転送データ量がその前後で変化しないものとして見積もっている。

●通信区間：インターネット⇔社内 NW

新 NW における，社内 NW の PC からインターネットへの通信経路について，〔現行 NW の移行〕の第 1 段落の中で，「PC からインターネット及び DMZ 上の Web サーバへの通信は，現行どおり全て Proxy を経由する」と記述されている。

LB を用いた負荷分散について，〔新 NW 構成の設計〕の第 1 段落の中で，「新 NW において，社内 NW に配置する LB には，Proxy の負荷分散と FW の負荷分散とを併用させる」と記述されている。「社内 NW に配置する LB」は，図 3 中の LB4 を指している。

したがって，PC からインターネットへの通信経路は，

PC → L3SW → LB4 → Proxy → LB4 → FW → LB3 → ルータ → インターネット

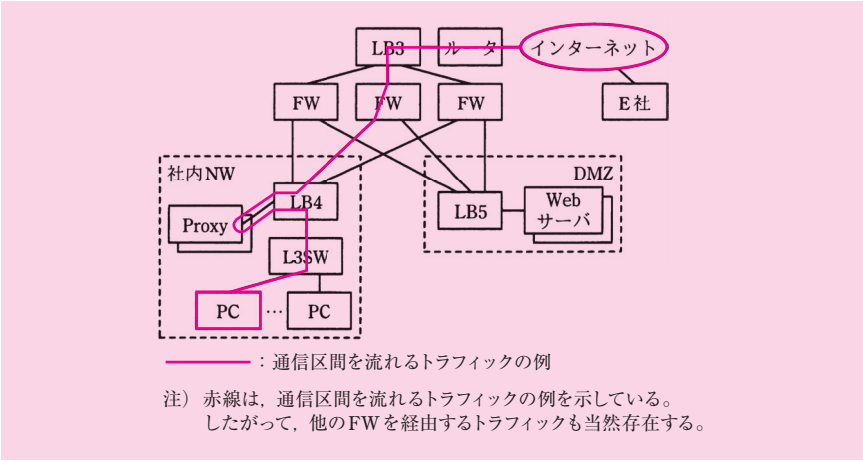
となる。

注目すべきは，この通信経路に，LB4 が 2 回登場することだ。

1 回目は「LB4 → Proxy」の区間である。ここで，LB4 は Proxy の負荷分散を行っている。すなわち，LB4 は PC からパケットを受け取り，Proxy に振り分けている。

2 回目は「LB4 → FW」の区間である。ここで，LB4 は FW の負荷分散を行っている。すなわち，LB4 は Proxy からパケットを受け取り，セッション単位で FW に振り分けている。

このトラフィックを新 NW の構成図に展開したものを次の図に示す。



図：「通信区間：インターネット⇔社内 NW」のトラフィック

この通信経路上に，FW が 1 回登場する。それは，「FW → LB3」の区間である。FW が転送するデータ量は，表 1 によれば，「89」である。

この通信経路上に，LB3 が 1 回登場する。それは，「LB3 →ルータ」の区間である。LB3 が転送するデータ量は，FW と同じく「89」となる。

この通信経路上に，LB4 が 2 回登場する。それは，「LB4 → Proxy」と「LB4 → FW」の区間である。LB4 が転送するデータ量は，2 回登場することを考慮し，「178」（= 89 × 2）となる。

●通信区間：インターネット⇔ DMZ

新 NW の DMZ には，Web サーバが現行のまま据え置かれる。

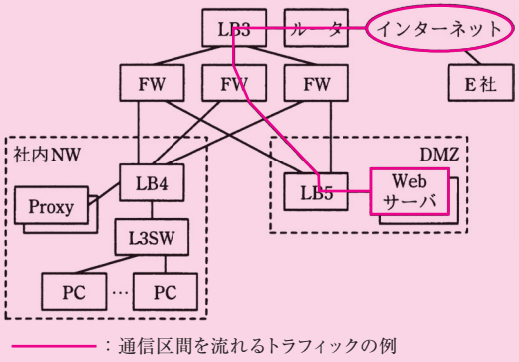
LB を用いた負荷分散について，〔新 NW 構成の設計〕の第 1 段落の中で，「新 NW において，……DMZ に配置する LB には，Web サーバの負荷分散と FW の負荷分散とを併用させる」と記述されている。「DMZ に配置する LB」は，図 3 中の LB5 を指している。

したがって，インターネットから Web サーバへの通信経路は，

インターネット → ルータ → LB3 → FW → LB5 → Web サーバ

となる。

このトラフィックを新 NW の構成図に展開したものを次の図に示す。



注）赤線は，通信区間を流れるトラフィックの例を示している。
したがって，他の FW を経由するトラフィックも当然存在する。

図：「通信区間：インターネット⇔ DMZ」のトラフィック

この通信経路上に，FW が 1 回登場する。それは，「FW → LB5」の区間である。FW が転送するデータ量は，表 1 によれば，「10」である。

この通信経路上に，LB3 が 1 回登場する。それは，「LB3 → FW」の区間である。LB3 が転送するデータ量は，FW と同じく「10」となる。

この通信経路上に，LB5 が 1 回登場する。それは，「LB5 → Web サーバ」の区間である。LB5 が転送するデータ量は，FW と同じく「10」となる。

●通信区間：社内 NW ⇔ DMZ

新 NW における，社内 NW の PC から DMZ 上の Web サーバへの通信経路について，〔現行 NW の移行〕の第 1 段落の中で，「PC からインターネット及び DMZ 上の Web サーバへの通信は，現行どおり全て Proxy を経由する」と記述されている。

LB を用いた負荷分散は，前述のとおり，社内 NW の LB4 と DMZ の LB5 で行っている。

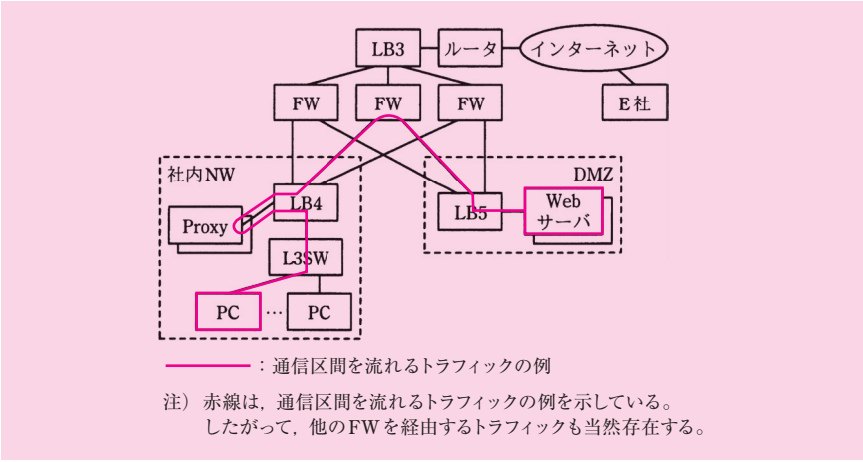
したがって，PC から Web サーバへの通信経路は，

PC → L3SW → LB4 → Proxy → LB4 → FW → LB5 → Web サーバ

となる。

注目すべきは，この通信経路にも LB4 が 2 回登場することである。前述のとおり，LB4 は，Proxy の負荷分散と FW の負荷分散とを行っているからだ。

このトラフィックを新 NW の構成図に展開したものを次の図に示す。



図：「通信区間：社内 NW ⇔ DMZ」のトラフィック

この通信経路上に，FW が 1 回登場する。それは，「FW → LB5」の区間である。FW が転送するデータ量は，表 1 によれば，「1」である。

この通信経路上に，LB5 が 1 回登場する。それは，「LB5 → Web サーバ」の区間である。LB5 が転送するデータ量は，FW と同じく「1」となる。

この通信経路上に，LB4 が 2 回登場する。それは，「LB4 → Proxy」と「LB4 → FW」の区間である。LB4 が転送するデータ量は，2 回登場することを考慮し，「2」（= 1 × 2）となる。

●解の導出

これまで考察した内容をまとめると，各 LB の通信区間ごとのデータ転送量，及び，各 LB のデータ転送量の合計は，次のとおりである。

表：LB の転送データ量

通信区間	転送データ量		
	LB3	LB4	LB5
インターネット⇔社内 NW	89	178	—
インターネット⇔ DMZ	10	—	10
社内 NW ⇔ DMZ	—	2	1
合計	99	180	11

LB3 の転送データ量は「99」となる。よって，これが空欄あの解となる。

LB4 の転送データ量は「180」となる。よって，これが空欄いの解となる。

参考までに，表 2 中の「転送データ量に対する現行 LB の性能」の欄を見ると，LB3 の「99」については「充足」であるが，LB4 の「180」については「不足」と評価されている。

この点を踏まえ，本事例では，LB4 には上位機種を新規に導入することにした。

空欄いの正解である「180」を得るには，LB4 が転送を 2 回行っていることに着目する必要があり，空欄あより難易度が高かった。転送を 1 回だけと考えてしまうと，「90」という数値を導いてしまったはずだ。

とはいえ，「転送データ量に対する現行 LB の性能」に着目するなら，LB3 が 99 で「充足」しているのに，LB4 が 90 で「不足」しているのは，明らかに不自然である。もしかすると，受験者の中には，これを手掛かりにして，LB4 の転送が 1 回だけではないことに気がついた人がいたかもしれない。

(3)

解答例

F	W	を	経	由	す	る	L	B	間	の	経	路	の	障	害	を	検	出	で	き	る	。

（23 字）

問題文は，「本文中の下線④は，LB が故障検出対象である FW に対してヘルスチェック用パケットを送信する方法と比較して，どのような利点があるか」と記述されている。

下線④は，〔新 NW 構成の設計〕(2) FW の故障対策の「・FW の故障検出機能」の中にある。そこには，「④対向する LB との間で，経由する FW を変化させながら，相互にヘルスチェック用パケットを送受信する」と記述されている。

したがって，本問は，問題文の方法と下線④の方法を比較し，下線④の方法の利点を解答することを求めている。

LB が FW の死活監視を行う目的は，FW の故障を検知したときに当該 FW に振り分けないようにするためだ。その点を考慮に入れると，両者の相違点が浮き彫りになる。

ヘルスチェック用パケットの仕様は本文中に記されていない。手掛かりとなるのは下線④の方法だ。FW を経由することから，FW でルーティングできるパケット，つまり，レイヤ 3 が IP のパケットだと考えられる。透過モードを使用するとき LB はブリッジとして動作するが，サーバ負荷分散モードの機能をもつ以上，LB には IP ノー

ドがもともと内蔵されている。それゆえ，その内部の IP ノードでヘルスチェック用パケットの送受信を行っていると考えられる。

ヘルスチェック用パケットを用いた死活監視の具体的な方法は明記されていないが，ping 等によるノード監視と似たようなものだと考えれば，次に示す方法が採られているはずだ。

- 監視対象ノード（下線④の方法では対向 LB）に対し，ヘルスチェック用パケットを送信する
- 監視対象ノードから，ヘルスチェック用パケットの応答（以下，確認パケットと称する）が返信される
- 確認パケットの受信により，自ノードと監視対象ノード間の区間には，障害が発生していないと判断する

それでは，これより，二つの方法を比較してみよう。

●問題文にある，故障検出対象である FW に対してヘルスチェック用パケットを送信する方法

この方法を用いると，死活監視を行える範囲は，「自 LB と FW 間の経路」となる。具体的に言うと，

- 自 LB と FW 間のケーブル
- FW のインタフェース（自 LB の側）
- FW 本体

となる。

したがって，「対向 LB と FW 間の経路」は，死活監視の範囲外となる。

この方法では，「自 LB と FW 間の経路」さえ問題なければ，その FW を振り分け対象にしてよいと判断してしまう。「対向 LB と FW 間の経路」の障害を検知できないが，そのどこかが故障していたならば，その FW を経由する通信は途絶えてしまうので，そこに振り分けてはならない。したがって，この死活監視には致命的欠陥がある。

これまでの解説から，振り分け先 FW を死活監視に当たって，ある重要な結論を導くことができる。それは，「対向 LB と FW 間の経路を含めた，自 LB と対向 LB 間の経路全体を監視しなければならない」という点である。

●下線④にある，対向する LB との間で，相互にヘルスチェック用パケットを送受信する方法

この方法を用いると，死活監視を行える範囲は，「FW を経由する LB 間の経路」となる。具体的に言うと，

- 自 LB と FW 間のケーブル
- FW のインタフェース（自 LB の側）
- FW 本体
- FW のインタフェース（対向 LB の側）
- 対向 LB と FW 間のケーブル

となる。

前述のとおり，FW を振り分け先として選択するには，その FW を経由する LB 間の経路全体を死活監視の範囲としなければならない。この方法では，それが達成できる。

下線④の方法は，「経由する FW を変化させながら」実施している。言い換えると，経由先となる FW を交代しながら，定期的に死活監視を行っていることが分かる。

●解の導出

両者を比較すると，死活監視の範囲に相違があった。問題文の方法とは異なり，下線④の方法は，「FW を経由する LB 間の経路全体」が範囲となる。それが本来あるべき姿であり，むしろ問題文の方法に欠陥があったわけだ。

本問は，問題文の方法と比較した，下線④の利点を問うている。よって，「FW を経由する LB 間の経路の障害を検出できる」旨を解答すればよい。

●参考：解答に詰まったときに役立つ試験テクニック

本問を解く鍵となるのは，前述のとおり，FW の死活監視を行う目的に照らして考察することだ。

この点を考慮せず，死活監視している部位を列挙するならば，問題文の方法と，下線④の方法には差がないように見えるので，解を導くのが困難になる。

この点をかみ砕いて説明しよう。

問題文の方法は「自 LB と FW 間の経路」を死活監視の範囲としているが，言うまでもなく，対向 LB も同様の方法で死活監視を実施している。その結果，両 LB の死活監視の範囲を単純に合算すると，自 LB と FW 間のリンク，FW のインタフェース（両

側），FW 本体，FW と対向 LB 間のリンク，となる。つまり，下線④の方法と同じように見える。

もしも，本問を解いているとき，問題文の方法と下線④の方法に差がないように思えたなら，「出題の意図」を汲み取れていないことになる。その際，次の試験テクニックが役に立つと思う。

序章「0.3.6　問題を解く②：応用テクニック」
4. 出題の意図を汲み取れないときは，出題分野の重要トピックを思い巡らしてみる

解答に詰まったら，その問題から一歩引いて，一般論を思い巡らしてみよう。そのとき，「LB が死活監視を行う目的は，振り分け対象とすべきか否かを判定するためだ」という一般論を思い起こすことができれば，正解に至るはずだ。

(4)

解答例

リトライアウトを待たずにコネクションの切断を検知できる。
（28字）

問題文は，「本文中の下線⑤の動作は，この動作を行わない場合と比べて，TCP コネクションの両端ノードにどのような利点を与えるか」と記述されている。

下線⑤は，〔新 NW 構成の設計〕（2）FW の故障対策の「・FW の故障発生時の影響軽減機能」の中にある。そこには，「現行 NW の Active-Standby 構成と異なり，新 NW では，FW の故障発生時にセッション維持ができない。この影響を軽減するために，故障検出時に，⑤ FW をはさんでいる両 LB が，RST フラグをオンにしたパケットを TCP コネクションの両端に送信する」と記述されている。

設問 1 空欄ウで解説したとおり，本事例の FW は，Active-Active 構成ではステートフルフェールオーバを行わない。したがって，問題文にあるように，FW が故障するとセッションを維持できない。

FW の故障発生時に，下線⑤の動作を行わないならば，TCP コネクションの終端ノードは，どのように振る舞うだろうか。

終端ノードは，直前に送ったパケットに対する確認応答パケットを待ち続け，やがてタイムアウトに至る。そのタイムアウト値は，当該コネクションの接続中に計測さ

れた RTT（Round Trip Time：往復時間）に基づいて決定される（OS のパラメータを調整し，固定値に設定することも可能）。

その後，終端ノードは当該パケットを再送する。FW が故障しているので，当然ながら，その再送もタイムアウトに至る。再送するとき，このタイムアウト値が 2 倍ずつ増えていく。一定回数の再送を試行し，その全てがタイムアウトに至ったとき，ようやく TCP コネクションが切断したと判断する。参考までに，Windows 7 の場合，再送回数の既定値は 5 である。

一方，下線⑤の動作を行うと，TCP コネクションの終端ノードは，FW が故障すると RST フラグをオンにしたパケットを受信する。その結果，ただちに，当該コネクションをリセットして切断する。

したがって，下線⑤の動作によって，再送の試行に費やす時間を待たずに，コネクションの切断を検知することができる。

よって，正解は解答例に示したとおりとなる。

問 3

出題趣旨
近年インターネットのセキュリティ対策の重要性が増大し，その対策として侵入検知システム（IDS）や侵入防止システム（IPS）の導入が一般的となってきている。導入に当たっては，それぞれの機能と特徴を正しく理解し，不正アクセスに対して最適に対応できるように設計し，導入後も継続的にメンテナンスしていく必要がある。IDS と IPS はネットワークを構成する重要な機器であり，ネットワークエンジニアには，関連する知識が求められる。 本問では，ネットワークのセキュリティ対策向上を題材に，IDS と IPS の機能と特徴について，基本的な知識と理解力を問う。

採点講評
問 3 では，ネットワークのセキュリティ向上のための侵入検知・防御システムの導入を題材に，侵入検知システム（IDS）と侵入防止システム（IPS）に関わる基本的な知識と，それぞれの特長を生かしたネットワークの設計について出題した。全体として正答率は高く，ネットワークのセキュリティに関して，受験者の関心は高く，よく学習されていることがうかがえた。 設問 1 は，ネットワークを監視するための IDS のポート設定や，ICMP を使ったコネクション切断の設定などの専門用語の正答率が低かった。用語は正確に覚えておいてほしい。 設問 2（1），（3）は，IDS に関する基本的な知識を踏まえ，ネットワーク上の接続箇所と検出可能な通信の範囲や，攻撃抑止の注意点を解答するものであり，比較的正答率は高かったが，それに比べて（2）では，ファイアウォールとの連携について正確に記述できていない解答が散見された。セキュリティ対策のためにネットワーク機器を連携させることについても，理解を深めておいてほしい。 設問 3（1），（2）は，IPS の機能に関する知識を問うたものであるが，IDS に比べて正答率は低かった。IDS と IPS の違いをよく把握しておいてほしい。（3）は，導入した機器の運用方法を問うたものであり，ネットワーク技術者として，継続的な運用メンテナンスがセキュリティレベルの維持・向上のために必要であることを，理解しておくことが重要である。

<table>
<tr><th>設問</th><th colspan="2">解答例・解答の要点</th><th>備考</th></tr>
<tr><td rowspan="5">設問 1</td><td>ア</td><td>アノマリ　又は　異常検知</td><td></td></tr>
<tr><td>イ</td><td>ミラー　又は　ミラーリング</td><td></td></tr>
<tr><td>ウ</td><td>プロミスキャス</td><td></td></tr>
<tr><td>エ</td><td>IP</td><td></td></tr>
<tr><td>オ</td><td>unreachable</td><td></td></tr>
<tr><td rowspan="3">設問 2</td><td>(1)</td><td><table><tr><td rowspan="2">通信の範囲</td><td colspan="3">IDS の接続箇所</td></tr><tr><td>SW1</td><td>SW2</td><td>SW3</td></tr><tr><td>インターネット⇔内部 LAN</td><td>○</td><td>×</td><td>○</td></tr></table></td><td></td></tr>
<tr><td>(2)</td><td>FW の ACL を動的に変更して，遮断の対象とする送信元アドレスを追加する。</td><td></td></tr>
<tr><td>(3)</td><td>不正アクセスの送信元アドレスが偽装されている可能性があるから</td><td></td></tr>
</table>

（表は次ページに続く）

設問		解答例・解答の要点	備考
設問 3	(1)	保護する機器にセキュリティパッチを適用するまでの間，脆弱性を悪用する攻撃の通信を遮断する。	
	(2)	通信をそのまま通過させ，遮断しない機能	
	(3)	不正アクセスへの対応を最適化するために，ログを取得して解析する。	

本問は，侵入検知･防御システムの導入をテーマに，侵入検知システム（以下，IDS と称する）の機能，侵入防止システム（以下，IPS と称する）の機能，及び，それらを導入した後の運用について問うている。

■設問 1

解答例

ア：アノマリ　又は　異常検知
イ：ミラー　又は　ミラーリング
ウ：プロミスキャス
エ：IP
オ：unreachable

ア

空欄アを含む文章は，〔IDS の見直し〕の中にある。

第 1 段落から第 3 段落は，IDS がもつ侵入検知の仕組みを 2 種類述べている。第 2 段落は，その一つ目として，シグネチャ型の仕組みを説明している。

続く第 3 段落は，二つ目の仕組みに関する説明であり，その中に空欄アが登場する。そこには「［　ア　］型は，定義されたプロトコルの仕様などから逸脱したアクセスがあった場合に不正とみなす。シグネチャ型と比べて，未知の攻撃に対しては柔軟に対応できるが，正常と判断する基準によっては，正常なパケットを異常とみなすこともある」と記述されている。

IDS の侵入検知の仕組みは，シグネチャ型とアノマリ型の 2 種類に大別できる。

シグネチャ型は，第 2 段落にあるとおり，「不正なパケットに関する一定のルールやパターン」に合致したものを不正とみなす。

アノマリ型は，第 3 段落に記述されたとおり，「定義されたプロトコルの仕様などから逸脱したアクセス」を不正とみなす。したがって，第 3 段落は，アノマリ型に関する説明であると結論できる。

よって，空欄アに該当する字句は「**アノマリ**」となる。又は，アノマリ型は，異常検知型とも呼ばれているので，「**異常検知**」も正解である。

イ，ウ

空欄イ，ウを含む文章は，〔IDS の見直し〕の第 5 段落の中にある。そこには，「IDS は，監視対象のネットワークにある SW の［　イ　］ポートに接続し，IDS 側のネットワークポートを［　ウ　］モードにすることで，IDS 以外を宛先とする通信も取り込むことができる」と記述されている。

つまり，ここでは「IDS 以外を宛先とする通信も取り込むこと」を実現するには，次の二つのことが必要であると記されている。

［1］監視対象ネットワークにある SW の［　イ　］ポートに接続する

［2］IDS 側のネットワークポートを［　ウ　］モードにする

ここまで整理できたところで，空欄イ，ウの順に解を導こう。

●空欄イ

SW は，MAC アドレステーブルをもつ。ここには，どのポートの先にどの端末があるかを示す，ポートと MAC アドレスとの対応付けが登録されている。

通常，SW は，イーサネットフレームを転送する際，MAC アドレステーブルを参照し，宛先となる MAC アドレスが存在するポートから，イーサネットフレームを送出する。

それゆえ，通常の設定のまま IDS を SW に接続すると，SW は，IDS を宛先とするイーサネットフレームだけを，IDS が接続されたポートに転送してしまう。

しかし，ポートのミラーリング機能を動作させると，SW が受信したイーサネットフレームを全て，「ミラーポート」と呼ばれる特別なポートから送出する。SW は，任意のポートをミラーポートに指定することができる。

したがって，IDS が接続する SW のポートをミラーポートに設定すれば，SW が転送する全てのイーサネットフレームを IDS に送出することができる。こうして，前述の項番［1］が達成される。

よって，空欄イに該当する字句は，「**ミラー**」となる。又は，「ミラーポート」は「ミラーリングポート」とも呼ぶので，「**ミラーリング**」も正解である。

●空欄ウ

通常，NIC がイーサネットフレームを受信する条件は，宛先 MAC アドレスが自 MAC アドレスと同一であるか，マルチキャストアドレスであるか，又はブロードキャスト

アドレスであるか，のいずれかに合致した場合である。

しかし，NIC をプロミスキャスモードに設定すると，全てのイーサネットフレームを受信することができる。

したがって，IDS のポートをプロミスキャスモードに設定すれば，SW のミラーポートから送出された，様々な宛先 MAC アドレスをもつイーサネットフレームを，IDS に取り込むことができる。こうして，前述の項番［2］が達成される。

よって，空欄ウに該当する字句は，「**プロミスキャス**」となる。

参考までに，平成 26 年午後Ⅱ問 2 の設問 3（1）では，SW 側からポートミラーリング機能を用いてフレームを送出し，端末側でプロミスキャスモードによるフレームを取り込む仕組みについて出題している。類題を解くと理解が深まることがあるので，後ほど確認しておくとよいだろう。

エ

空欄エを含む文章は，〔IDS の見直し〕の第 5 段落の中にある。そこには「IDS 側のネットワークポートに［　エ　］アドレスを割り当てなければ，IDS 自体が OSI 基本参照モデルの第 3 層レベルの攻撃を受けることを回避できる」と記述されている。

図 1 のネットワークはインターネットにつながっているので，IP ネットワークであることが分かる。IP は，OSI 基本参照モデルの第 3 層（ネットワーク層）に位置するプロトコルである。したがって，IDS 側のネットワークポートに IP アドレスを割り当てなければ，IDS 自体がネットワーク層レベルの攻撃を受けることを回避できる。

よって，空欄エに該当する字句は「**IP**」となる。

オ

空欄オを含む文章は，〔IDS の見直し〕の第 8 段落の中にある。そこには「検知した不正パケットが UDP の場合には，該当するパケットの送信元に，ICMP ヘッダのコードに port［　オ　］を設定したパケットを送って，更なる攻撃の抑止を試みることができる」と記述されている。

IP ノードは，UDP パケットを受信すると，宛先ポート番号に対応するアプリケーションが自ノードで稼働しているか否かを調べる。もし稼働していない場合，当該パケットの送信元に対し，「宛先に指定されたポートが開いていない」旨を通知することができる。その通知に用いられるのが，ICMP パケット（タイプ：destination unreachable，コード：port unreachable）である。

よって，空欄オに該当する字句は「**unreachable**」となる。

■設問 2
(1)

解答例

通信の範囲	IDS の接続箇所		
	SW1	SW2	SW3
インターネット⇔内部 LAN	○	×	○

問題文は，「IDS で検出可能な通信の範囲を追加して，表 1 を完成させよ」と記述されている。

表 1 は〔IDS の見直し〕の第 6 段落の下に記載されており，同段落の中にその説明がある。そこには，「図 1 中の SW1 ～ SW3 にそれぞれ IDS を接続した場合に，IDS で検出可能な通信を表 1 に示す」と記述されている。

図 1 は，現在の営業支援システムのネットワーク構成が記されている。SW1 はインターネットと FW の間，SW2 は DMZ の中，SW3 は内部 LAN の中に，それぞれ設置されている。

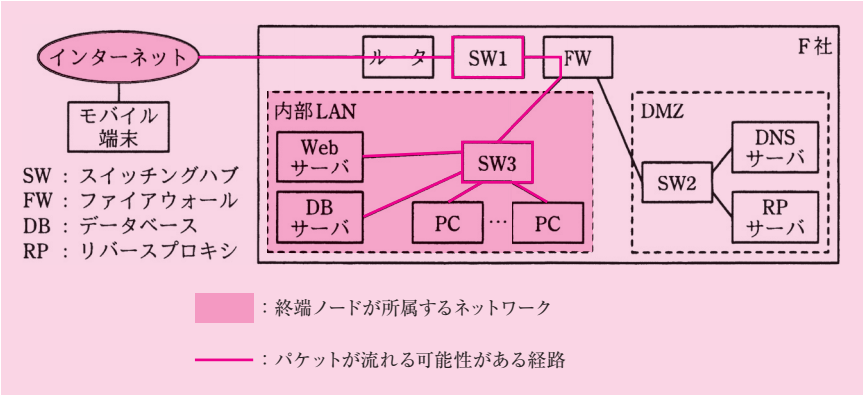
表 1 は，通信の範囲ごとに，IDS が当該通信を検出可能か否かが記されている。IDS をどの SW に接続するかによって，通信の範囲ごとの検出可否は異なってくる。

通信の範囲は，終端ノードが所属するネットワークの組によって定義されている。ネットワークの種類は，「インターネット」「DMZ」「内部 LAN」の 3 種類がある。その組（通信の範囲）は，表 1 によると空欄になっているものを含めて全部で 5 種類がある。表 1 に記載済みの通信の範囲は，「インターネット⇔ DMZ」「DMZ ⇔ DMZ」「DMZ ⇔内部 LAN」「内部 LAN ⇔内部 LAN」の 4 種類だ。

本問が求めていることは，残った通信の範囲を明らかにすること，かつ，SW1 ～ SW3 のそれぞれに IDS を接続したときの検出可否を明らかにすることである。

ネットワークが 3 種類あることから，残った組合せとして考えられるのは，「インターネット⇔内部 LAN」「インターネット⇔インターネット」である。このうち，SW1 ～ SW3 のいずれかに IDS を接続したときに検出可能なものは，「インターネット⇔内部 LAN」だけである。「インターネット⇔インターネット」の通信は SW1 ～ SW3 を流れることがないからだ。

インターネット⇔内部 LAN の通信の範囲を，次の図に示す。



図：インターネット⇔内部 LAN の通信の範囲

この通信の範囲を流れるパケットを，SW1 と SW3 は全て転送する。一方，SW2 は決して転送しない。したがって，SW1 又は SW3 に IDS を接続すれば，この範囲の通信を検出できる。一方，SW2 に IDS を接続しても検出できない。

したがって，表 1 の空欄を埋めると次のようになる。よって，正解は解答例に示したとおりとなる。

表：IDS で検出可能な通信（表 1 を完成させたもの）

通信の範囲	IDS の接続箇所		
	SW1	SW2	SW3
インターネット⇔ DMZ	○	○	×
DMZ ⇔ DMZ	×	○	×
DMZ ⇔内部 LAN	×	○	○
内部 LAN ⇔内部 LAN	×	×	○
インターネット⇔内部 LAN	○	×	○

○：検出可　　×：検出不可

(2)

解答例

F W の A C L を 動 的 に 変 更 し て ， 遮 断 の 対 象 と す る 送 信 元 ア ド レ ス を 追 加 す る 。（36字）

問題文は，「本文中の下線①で，IDS と FW が連携することで不正な接続を遮断する仕組みとは，どのようなものか」と記述されている。

下線①は，〔IDS の見直し〕の第 7 段落の中にある。そこには，「IDS には，検知した攻撃を遮断する機能を実装している機種があった。遮断機能のうちの一つは，①IDS と FW が連携することで，検知した送信元アドレスからの不正な接続を遮断するというものであった」と記述されている。

本事例で導入を検討している IDS は，SW のミラーポートに接続することで，当該 SW が転送しているパケットを取り込んで，不正を検知する。とはいえ，検知対象の通信は，IDS を直接経由するわけではないので，IDS 自体は不正な通信を遮断することができない。

通信を遮断するのに適しているのは，通信経路上にインラインに設置された機器である。パケットがその機器を経由するとき，不正なものを転送しないように制御できるからだ。FW はまさにその役割をもつ機器の代表格である。

その点を踏まえ，あとは一般的な知識から解を導こう。

一般的に言って，商用 FW の中には，外部の IDS と連携して不正な通信を遮断する機能をもつものがある。その仕組みは次のようなものである。

- IDS は，不正な通信を検知したら，ただちに FW に通知する
- FW は，ACL（Access Control List：アクセス制御リスト）を動的に変更し，不正な通信を遮断するルールを追加する

この動的なルールの追加が正常な通信を阻害してはならないので，ピンポイントにフィルタリングすることが求められている。そこで，遮断用のルールとして，不正とみなした通信の送信元 IP アドレスを用いることができる。つまり，特定のホストからの通信だけを遮断するわけだ。

ここまで解説した内容は，FW と IDS の連携による遮断機能としてごく一般的なものであり，下線①が指す遮断機能の最有力候補と言える。これ以外には思い当たるものがないと言っても過言ではない。したがって，ここで解説した内容に基づいて解を導けばよい。

なお，本問は「下線①で……不正な接続を遮断する仕組み」を問うている。下線①には「検知した送信元アドレスからの不正な接続を遮断する」とあるので，遮断するルールの条件として，検知した送信元 IP アドレスを用いることを解答に含めるとよい。

よって，正解は，「**FW の ACL を動的に変更して，遮断の対象とする送信元アドレ**

スを追加する」などとなる。

(3)

解答例

不正アクセスの送信元アドレスが偽装されている可能性があるから（30字）

問題文は，「H 君が，本文中の下線②のように考えたのはなぜか」と記述されている。

下線②は，〔IDS の見直し〕の第 8 段落の中にある。そこには，「検知した不正パケットが UDP の場合には，該当するパケットの送信元に，ICMP ヘッダのコードに port unreachable を設定したパケットを送って，更なる攻撃の抑止を試みることができる。しかし，H 君は，②この ICMP を使った攻撃抑止のためのパケットが，実際は攻撃者に届かないことがあること，又はこのパケット自体が他のサイトへの攻撃となることもあると考えた」と記述されている。

設問 1 空欄オで解説したとおり，IP ノードは，UDP パケットを受信すると，宛先ポート番号に対応するアプリケーションが自ノードで稼働しているか否かを調べる。もし稼働していない場合，当該パケットの送信元に対し，ICMP パケット（port unreachable）を送信する。

このパケットは，「更なる攻撃の抑止を試みる」とある。その理由は，この ICMP パケットの受信は，その直前に送った UDP パケットの宛先ポートが開かれていないこと，すなわち，当該ポートで待ち受けているサーバアプリケーションが稼働していないことを意味しているからである。それゆえ，そのアプリケーション宛ての更なる送信を控えるべきだと考えられるからだ。

しかし，UDP がコネクションレス型であるという特徴を悪用した攻撃を行う場合は，この限りではない。コネクションレス型通信は，通信相手とコネクションを確立することがないため，いわば一方的に，パケットを送信することが可能だ。この特徴を悪用し，送信元 IP アドレスを偽装した上で，不正な UDP パケットを標的サイトに意図的に送り付けるわけだ。

不正な UDP パケットに対する ICMP パケットの通知先は，当該 UDP パケットの送信元であるため，当該 UDP パケットの送信元 IP アドレスが偽装されていれば，ICMP パケットは攻撃者には届かない。それどころか，当該 UDP パケットの送信元が，実

存する他のサイトを詐称していた場合には，そのサイトに届いてしまうため，かえって攻撃の加害者にさえなってしまう。

コネクションレス型である UDP の特徴を悪用した攻撃として，よく知られているものの一つが，UDP フラッド攻撃である。

攻撃者は，標的ノードに UDP パケットを送信する際，宛先ポート番号として，対応するアプリケーションが到底存在しないような，不正なポート番号を指定する。加えて，送信元 IP アドレスを偽装する。

標的ノードは，これを受信すると，ICMP パケットを送信元に返信する。その分だけ，標的のネットワーク帯域や CPU 時間が無駄に消費させられる。送信元が実存する他サイトのノードを詐称していた場合には，そのサイトのリソースも消費させられる。その一方で，送信元を偽装している以上，攻撃者は ICMP パケットを受信することはなく，その分のリソース消費は免れているわけだ。

UDP フラッド攻撃とは，このような UDP パケットを大量に送り付けることによって，サービス妨害をもたらす攻撃である。

このように，UDP は一方的にパケットを送ることができ，しかも送信元の偽装が容易であるため，これを悪用した攻撃が現に存在する。この点を念頭に置いて，改めて下線②を含む文を見てみよう。

そこには，「②この ICMP を使った攻撃抑止のためのパケットが，実際には攻撃者に届かないことがある」「このパケット自体が他のサイトへの攻撃となることもある」と記述されている。

この記述から，送信元 IP アドレスを偽装した，不正な UDP パケットを用いた攻撃を懸念していることが分かる。なお，「大量に送り付ける」というサービス妨害の特徴については特に言及がないので，UDP フラッド攻撃を具体的に考えていたとまでは言い切れない。攻撃と言うからには，相手にダメージを与え得る行為を想定しているはずだが，試験の答案としては，深読みし過ぎるのは危険だろう。

以上より，下線②の部分について，少なくとも H 君が考えていたことは，「不正な UDP パケットの送信元 IP アドレスが偽装されている」となる。

よって，正解は解答例に示したとおりとなる。

■設問 3
(1)

解答例

保護する機器にセキュリティパッチを適用するまでの間，脆弱性を悪用する攻撃の通信を遮断する。（45字）

問題文は，「本文中の下線③で可能としている，一時的な運用を……述べよ」と記述されている。

下線③は，〔IPS の追加〕の第 1 段落の中にある。そこには，「IPS は，不正アクセスを監視するだけでなく，遮断する機能を強化したネットワーク機器である。例えば，SQL インジェクションのような，Web アプリケーションの脆弱性に対応する機能をもつもの，及び③防御対象のサーバに新たな脆弱性が発見された場合の一時的な運用に対応できるものがある」と記述されている。

一般的に言って，防御対象のサーバに新たな脆弱性が発見された場合，どのように対応すればよいだろうか。

脆弱性の情報が公表されると，それはハッカーにも知れ渡ることになる。それを悪用した攻撃を仕掛けてくる可能性があるので，脆弱性の情報と併せてセキュリティパッチも公開されるのが通例となっている。したがって，脆弱性が発見された場合，セキュリティパッチを適用して脆弱性を塞ぐことが求められる。

それでは，これが，下線③の中で言及され，かつ，ここで問われている「一時的な運用」なのだろうか。いや，そうではない。

「一時的な」を別の言葉に置き換えると，「臨時の」「そのとき限りの」などとなる。「一時的な運用」という言葉には，「本来行うべきことは別にあるのだが，それには時間がかかる。しかし，一刻を争う事態なので，応急措置を行う」という意味が込められている。

そのように考えると，「セキュリティパッチを適用して脆弱性を塞ぐ」ことは，二つの観点から，一時的な運用とは言えない。

一つ目の理由は，これ以外に有効な対策がないからだ。脆弱性をもたない完全なシステムが存在しない限り（無論，これは期待できない），又は，保護対象のサービスの使用を永久に停止しない限り（無論，これは経営者が判断すべきものだ），今あるシステムを運用する前提で考え得る最善の現実解は，「脆弱性が見つかったら塞ぐこと」である。つまり，「本来行うべきことは別にある」というわけではない。他に有効な手立

てがない以上，これは「本格的な運用」に位置付けられる。したがって，「一時的な運用」という言葉を当てはめることはできない。

二つ目の理由は，「セキュリティパッチの適用」を実施するのは，相応の工数がかかるからだ。つまり，すぐさま実施できないので，「一時的な運用」という言葉を当てはめることはできない。

セキュリティパッチを適用するには，まず，バージョン等をチェックした上で，正しいファイル群を過不足なく入手しなければならない。必要に応じ，稼働環境とは別に検証環境を用意して，パッチ適用の影響を確認するテストを実施する。こうして，いよいよパッチ適用に着手するわけだが，適用すべきノードが多数ある場合，作業自体に長時間を費やす。最後に，パッチが正しく適用されたことを確認するテストも必要である。

実際，本文中に，パッチ適用には時間がかかるという記述がある。序文の第 5 段落に，「アプリケーションへの影響確認テストに時間が掛かり，当該サーバにセキュリティパッチを適用するまで，営業支援システムを数日間休止せざるを得なかった」とある。

このようにパッチ適用には一定の工数がかかるわけだが，それが完了するまでの間，サイトは危険な状態にさらされている。その間に行うことが，「一時的な運用」である。その目的は，パッチ適用が完了するまでの間，サイトを攻撃から守ることにある。

一般的に言って，「一時的な運用」の具体例で即座に思いつくのは，パッチ適用までの間，一時的にサービスを休止することである。しかし，これは本問の求める解ではない。そのように言える理由は，IDS の見直しに至った経緯を見れば分かる。序文の第 4 段落で，レスポンス悪化を指摘し，第 5 段落で，パッチ適用までサービス休止でしのぐという一時的な運用の問題を指摘している。それを受けて，第 6 段落では，「インターネットを通じた様々なサイバー攻撃の増大」を考慮して「IDS の見直しを開始した」という流れになっている。それゆえ，従来では成し得なかった一時的な運用を，新規に導入する IPS の機能で実施することが，下線③の言わんとする内容である。

下線③は，IPS がもつ遮断機能を列挙した文脈にある。つまり，ここで述べられているのは，「防御対象のサーバに新たな脆弱性が発見された場合の一時的な運用に対応できる」遮断機能である。それゆえ，下線③の中で言及された「一時的な運用」とは，「防御対象のサーバに新たな脆弱性が発見された場合，セキュリティパッチを適用するまでの間，IPS がもつ遮断機能を動作させること」を指しているに違いない。

ここまで整理できたところで，あとは一般的な知識から解を導こう。

IPS の中には，公表された脆弱性にベンダがいち早く対応することで，それを悪用する攻撃の通信を遮断する機能をもつようにアップデートできるものがある。その機

能を利用すれば，外部からの攻撃を防ぎ，その間にセキュリティパッチを適用して脆弱性を塞ぐことができる(もちろん，このようなアップデートが可能である場合に限った話だ。さもなければ，従来と同様，パッチ適用までの間，一時的にサービスを休止するしかない)。

したがって，下線③にある「一時的な運用」とは，その遮断機能を動作させること，つまり，「防御対象のサーバに新たな脆弱性が発見された場合に，セキュリティパッチを適用するまでの間，IPS を用いて脆弱性を悪用する攻撃の通信を遮断すること」である。

よって，その旨を指定字数に収まるように解答すればよい。

(2)

解答例

通信をそのまま通過させ，遮断しない機能 (19字)

問題文は，「本文中の下線④の，IPS が実装している機能とは何か」と記述されている。

下線④は，〔IPS の追加〕の第 3 段落の中にある。そこには，「IPS の障害対策には，並列に複数台導入する冗長化が考えられる。しかし，導入候補の IPS には，④ IPS の機能の一部が故障した場合に備えた機能があった。費用対効果の観点と，IDS が併設されていることや，営業支援システムの継続利用を優先することから，……IPS を冗長化しないことにした」と記述されている。

この記述から，下線④の機能を用いた障害対策について，二つの特徴をもつことが読み取れる。

- IPS のもつセキュリティ機能の喪失を許容すること
- 営業支援システムの継続利用を実現できること

以下，この二つの特徴について解説する。それを踏まえて，解を導こう。

● IPS のもつセキュリティ機能の喪失を許容すること

この点は，「冗長化しない」と記されていることから分かる。冗長化しない以上，IPS が故障したときに別の IPS に切り替わることはないからだ。

これを許容できると判断した理由について，下線④に続く文に「IDS が併設されている」と記述されている。ここから，IPS が故障した場合，代替機の IPS に交換するまでの間，併設した IDS でセキュリティを守ることが分かる。

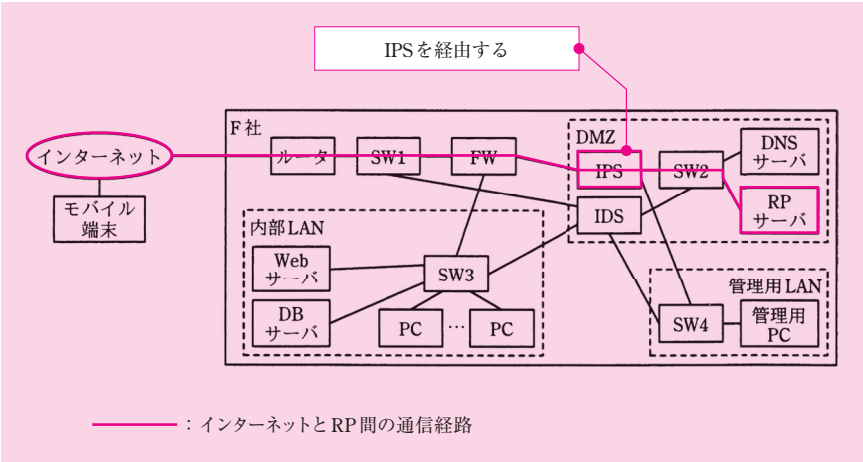
おそらく，設問 2（2）で解説した，FW と連携した遮断機能を導入することで，ある程度は侵入を防御できると考えたのだろう。ただし，IPS ほど高度な仕組みではないため，「交換するまでの間だけ縮退運転を許容する」との判断を下したに違いない。

●営業支援システムの継続利用を実現できること

この点は，下線④に続く文に，「営業支援システムの継続利用を優先する」と記述されているので，明白である。

具体的に言って，営業支援システムは，IPS の故障によってどのような影響を受けるのだろうか。

図 2「見直し後の営業支援システムのネットワーク構成案（抜粋）」は，IPS を導入した場合のネットワーク構成を示している。図 2 を見ると，IPS は FW と SW2 間にインラインに接続されている。SW2 には RP サーバ（リバースプロキシサーバ）が接続されているので，インターネットと RP サーバ間の通信は，IPS を経由する。



図：インターネットと RP サーバ間の通信経路

営業支援システムへのアクセスについて，序文の第 3 段落には，「F 社の営業部員は，……社外からは，モバイル端末を使って営業支援システムにアクセスする。営業支援システムで主なサービスを提供している Web サーバを社外から利用するには，SSL/TLS を実装した RP サーバを経由してアクセスする」と記述されている。つまり，

インターネットから営業支援システムにアクセスするには，RP サーバを経由する。それゆえ，図 2 の構成において，IPS を経由することが分かる。

したがって，IPS が故障した場合，故障対策を何ら講じていなかったなら（つまり，下線④の機能がなかったとしたら），インターネットから営業支援システムにアクセスできなくなってしまう。

この点から，次のように推論することができる。「IPS が故障した場合でも，営業支援システムを継続利用するためには，IPS を経由する通信が遮断されてはならない。それゆえ，下線④の機能とは，故障時に本体がケーブル接続と同等の状態となり，通信をそのまま通過させることではないだろうか」と。

そこで，「下線④の機能は，故障時に通信をそのまま通過させることである」との仮説を立て，これを検証してみよう。

先ほど，本文の記述に基づき，「下線④の機能を用いた障害対策は，IPS のセキュリティ機能の喪失を許容している」旨を解説した。この仮説によれば，故障時には通信を通過させることしか行わないので，本文の記述と合致している。

更に，この仮説は，一般的な知識とも調和している。一般的に言って，IPS をはじめとするインライン接続された機器は，故障時でも本体が通信をそのまま通過させる機能をもつものがある。実際，ネットワークスペシャリスト試験で出題されたことがあるので（平成 23 年午後 I 問 1 設問 2（4），平成 20 年午後 I 問 3 設問 4），後ほど確認しておくとよいだろう。

以上より，この仮説は，検証に耐え得る確かなものであることが分かる。

これ以降は，この仮説に基づき，「故障時に本体が通信を通過させる機能を用いて，営業支援システムの継続利用を実現している」と考えることにする。

●解の導出

本問は，下線④の機能を問うている。

その機能とは，故障時に通信をそのまま通過させることであった。よって，その旨を解答すればよいので，正解は解答例に示したとおりとなる。

(3)

解答例

不	正	ア	ク	セ	ス	へ	の	対	応	を	最	適	化	す	る	た	め	に	，	ロ	グ	を	取	得
し	て	解	析	す	る	。																		

（32 字）

問題文は，「IDS と IPS の導入後に，セキュリティレベルの継続的な向上のために，管理用 PC を使ってどのようなことを行うか」と記述されている。

「管理用 PC を使（う）」とあるので，ここで問われているのは，IDS と IPS を導入した F 社自らが行うことである。

新規に導入する IDS について，〔IDS の見直し〕の第 3 段落の中で，「（シグネチャ型，アノマリ型の）それぞれの仕組みの特長を生かすために，両方の機能をもった IDS を採用することにした」と記述されている。更に，同段落の中で，アノマリ型機能による不正アクセス対応について，「正常と判断する基準によっては，正常なパケットを異常とみなすこともある」という懸念が指摘されている。

したがって，IDS の導入後に F 社が行うべきことは，アノマリ型機能の判断基準を最適化していくことである。正常か否かの判断は，営業支援システムでどのような通信が行われているかを踏まえ，適宜調整していくことが求められる。それゆえ，ログを取得してアクセスを解析することが求められる。

一方，IPS について，〔IPS の追加〕の第 1 段落の中で，「IPS は正常な通信を誤って不正と検知してしまうこと（フォールスポジティブ），又は不正な通信を見逃してしまうこと（フォールスネガティブ）があり，双方のバランスをとって効果的な侵入防御を実現することが重要である」と記述されている。

したがって，IPS の導入後に F 社が行うべきことは，IPS が実施する侵入防御を最適化していくことである。「双方のバランスをとる」には，営業支援システムでどのような通信が行われているかを踏まえ，適宜調整していくことが求められる。それゆえ，IDS と同様に，ログを取得してアクセスを解析することが求められる。

以上より，IDS と IPS の導入後に F 社が行うことは，IDS と IPS が実施する不正アクセス対応を最適化していくことである。そのためには，ログを取得して解析することが求められている。

よって，正解は，「**不正アクセスへの対応を最適化するために，ログを取得して解析する**」となる。