問2　ファイアウォールの負荷分散に関する次の記述を読んで，設問1～3に答えよ。

D 社は，営業活動に関わる情報の共有・活用を強化するために，情報系サービス基盤を再構築することになった。新たな情報系サービス基盤には，アプリケーションサービスプロバイダの E 社を利用することが決まった。E 社のサービスは，インターネット上で Web サービスとして提供されている。

D 社の現行のネットワーク（以下，NW という）構成を図1に示す。

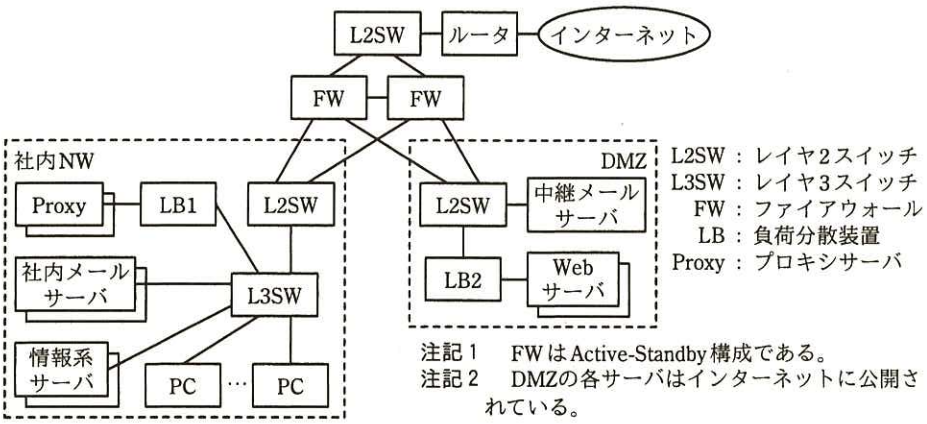


図1　D 社の現行の NW 構成（抜粋）

〔現行 NW の移行〕

D 社の情報系サービス基盤再構築の概要は，次のとおりである。

・現行 NW の情報系サーバ上で稼働しているアプリケーションは，E 社のグループウェアサービスに置き換える。

・社内メールサーバと中継メールサーバは，E 社の電子メールサービスに置き換える。

・Web サーバは，現行のままとする。

・FW では，現行どおりレイヤ 4 までの動的フィルタリングを行う。

・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。

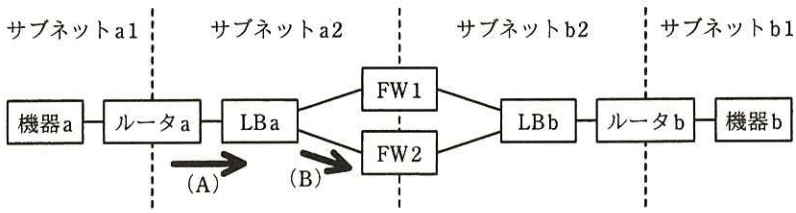
NW の移行を担当する D 社情報システム部の W 氏は，移行後の新 NW におけるイ

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 と Proxy 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 W 氏は，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。

〔FW の負荷分散〕

D 社の FW には，相互に負荷分散する機能がないので，LB を使用する必要がある。W 氏が現行 NW の LB の仕様を調査したところ，透過モードという機能によって，FW の負荷分散が可能であることが分かった。

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。

(2) ②LBa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。

・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。

〔新NW構成の設計〕

現行LBは，透過モードとサーバに対する負荷分散のモードとの併用が可能である。そこでW氏は，次の方針の下で新NW構成を設計した。

・現行NWにFWを1台追加し，③3台構成とする。

・現行NWのLBを，可能な限り新NWに転用する。

・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。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。

・新NWに必要な性能を満たすために，Proxyは台数を増設する。

W氏が設計した新NW構成案を図3に示す。

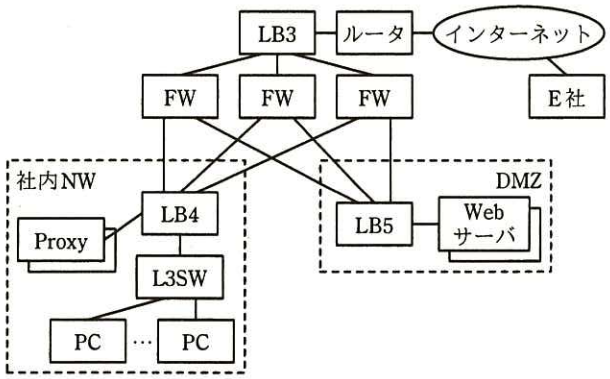


図3　新NW構成案（抜粋）

新NW構成の設計に当たってW氏が主に検討した課題は，次の2点である。

(1) LB の転送データ量の見積り

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。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［ ア ］は転送パケット長によって変化する。そこで W 氏は，インターネットのトラフィックをシミュレートして測定した LB の性能値を用いることにした。

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。また，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。

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 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

この見積りに基づいて W 氏は，次のように決定した。

・現行 NW の 2 台の LB を LB3 と LB5 に転用する。

・LB4 には上位機種を新規に導入する。

(2) FW の故障対策

FW の故障対策として，LB に用意されている次の二つの機能を使用する。

・FW の故障検出機能

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。

・FW の故障発生時の影響軽減機能

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。この影響を軽減するために，故障検出時に，⑤FW 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。

W 氏が設計した新 NW 構成案は，プロジェクト推進会議で承認され，再構築が進められることになった。

設問 1　本文中の［ ア ］～［ ウ ］に入れる適切な字句を答えよ。

設問 2　〔FW の負荷分散〕について，(1)～(3)に答えよ。

(1) 図 2 中の（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を表し，矢印はその転送方向を表す。また，この TCP コネクション上のパケットは FW2 を経由する。（A），（B）の宛先 IP アドレスと宛先 MAC アドレスを，図 2 中の機器名を用いて答えよ。

(2) 本文中の下線 ① はどのような制約か。20 字以内で述べよ。

(3) 本文中の下線 ② では，LB a のパケット振り分け動作と LB b 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，30 字以内で述べよ。

設問 3　〔新 NW 構成の設計〕について，(1)～(4)に答えよ。

(1) 本文中の下線 ③ で，FW を 3 台構成とする目的を 20 字以内で述べよ。

(2) 表 2 中の［ あ ］，［ い ］に入れる適切な数値を答えよ。

(3) 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。30 字以内で述べよ。

(4) 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のノードにどのような利点を与えるか。30 字以内で述べよ。