NW

平成27年度　秋期
ネットワークスペシャリスト試験
午後Ⅰ　問題

試験時間	12:30 ～ 14:00（1時間30分）

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3
選択方法	2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。3問とも○印で囲んだ場合は，はじめの2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1，問3を選択した場合の例〕

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　シングルサインオンの導入に関する次の記述を読んで，設問1～4に答えよ。

A 社は，新興の広告代理店である。A 社ではここ数年，業務の拡大傾向が続き，営業システムや広告システムなど，PC の Web ブラウザからアクセスされる Web アプリケーションを導入してきた。これらの Web アプリケーションの利用者認証は，それぞれ個別に行っている。しかし，この方法は利用者の利便性が低いことから，情報システム課に改善の要望が出されていた。

そこで，情報システム課の B 課長は利用者からの改善要望を踏まえ，全ての社内 Web アプリケーションの認証を共通化するために，シングルサインオン（以下，SSO という）の導入を考えた。SSO を導入すると，利用者は一度の認証操作で複数のシステムの利用が可能となる。

〔SSO の導入〕

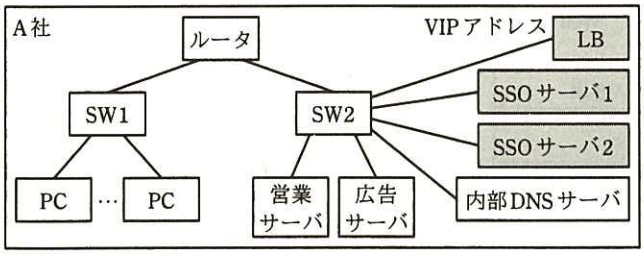
情報システム課は，A 社の全システムに SSO を本格導入する前に，試験的に営業システムと広告システムに SSO を導入することにした。そこで，B 課長が要件をとりまとめ，ネットワーク担当の C 氏に検討を指示した。その指示の内容を次に示す。

・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

C 氏が検討した A 社のシステム構成を，図1に示す。



SW1，SW2：レイヤ2スイッチ
VIPアドレス：仮想IPアドレス

注記　網掛け部分は，導入検討中の機器を示す。

図1　C氏が検討したA社のシステム構成（抜粋）

〔SSOについての検討〕

C氏はHTTPを用いたSSOの方式と認証処理シーケンスについて検討した。SSOの方式を分類すると，SSO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。C氏は，エージェント方式の検討を行い，エージェント方式を採用することにした。

エージェント方式におけるSSO認証処理のシーケンスは，次のとおりである。

① PCからWebアプリケーションサーバに，サービス要求を行う。

② 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。

③ SSOサーバからPCに，認証画面を送る。

④ PCからSSOサーバに，UserIDとPasswordを送出する。

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。サービス要求は，Webアプリケーションサーバへ［　イ　］される。

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。

⑦ Webアプリケーションサーバは，⑥の応答によって利用者のアクセスの正当性が確認できた場合，Webアプリケーション画面を送出する。

エージェント方式におけるSSO認証処理のシーケンスの①～⑦を図示すると，図2のようになる。

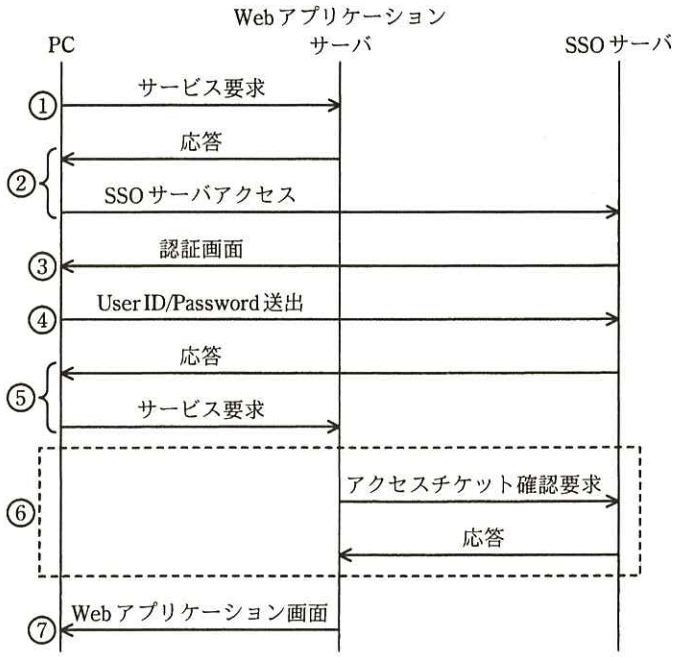


図2　エージェント方式における SSO 認証処理のシーケンス

〔SSO サーバの動作確認〕

C 氏は，図 1 と同等構成の検証環境を本番環境とは別に用意し，SSO サーバを構築した。また，営業サーバと広告サーバには，エージェントのインストールを行った。

検証環境を構築した後，動作確認として営業システムへのアクセスを行ったところ，認証画面が表示されるところまでは想定どおり動作したが，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。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。そこで，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。

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を流れないよう，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。

〔負荷分散に関する設定と動作確認〕

C 氏は，検証環境において，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するとともに，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。SSO サーバを DSR 方式で負荷分散するときの LB の動作の要点を次に示す。

(1) 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，LB は当該リクエストを負荷分散ポリシに従って，SSO サーバ 1 又は SSO サーバ 2 に転送する。

(2) 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。

(3) 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。

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ことに注意する必要がある。

要点 (3) の動作から，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。

C 氏が［オ］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，（Ⅳ）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，想定どおりに動作することが確認された。

その後，A 社は，営業システムと広告システムを対象範囲とする SSO システムを正式に導入することにした。

設問1　本文中の［　ア　］～［　オ　］に入れる適切な字句を答えよ。

設問2　図 2 中の ⑥ で確認が行われるアクセスチケットは，PC に対して発行されたものである。PC はどの時点でアクセスチケットを得るかを，図 2 中の ① ～⑦ の番号で答えよ。

設問3　〔SSO サーバの動作確認〕について，(1)，(2) に答えよ。

(1) 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。

(2) 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，25 字以内で述べよ。

設問4　〔負荷分散に関する設定と動作確認〕について，(1) ～ (3) に答えよ。

(1) 本文中の下線（Ⅲ）の理由を，30 字以内で述べよ。

(2) 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。

(3) 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。40 字以内で述べよ。

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。

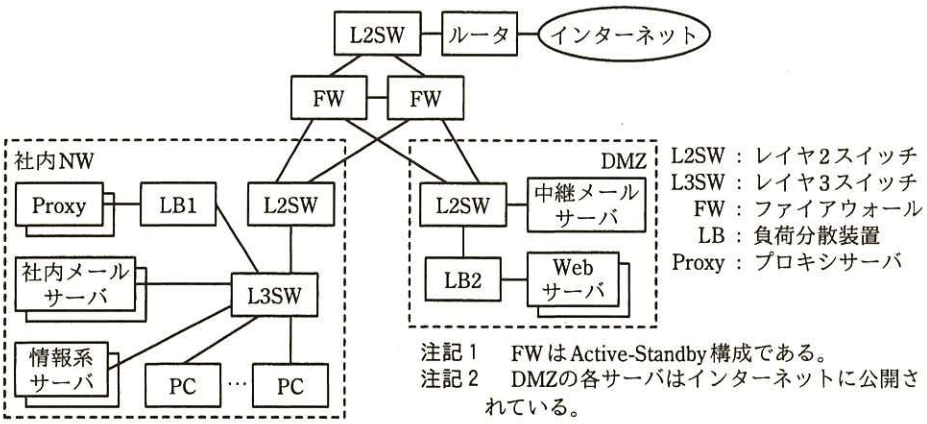


図1　D 社の現行の NW 構成（抜粋）

〔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。

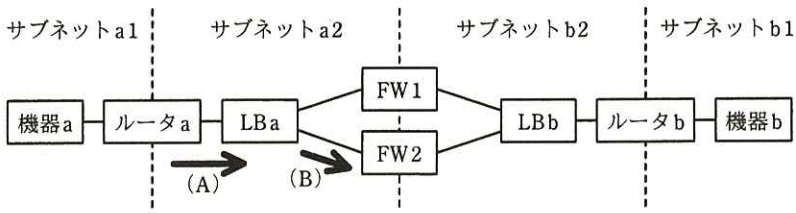
NW の移行を担当する D 社情報システム部の W 氏は，移行後の新 NW におけるイ

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。

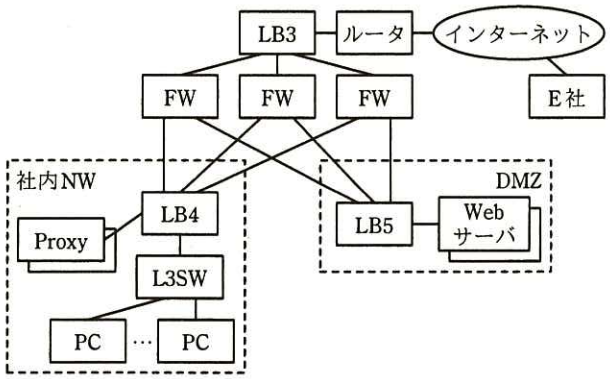


図3　新NW構成案（抜粋）

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。

問３　侵入検知・防御システムの導入に関する次の記述を読んで，設問 1～3 に答えよ。

F 社は，中堅の輸入食品卸売会社であり，自社で営業支援システムを運用している。

現在の営業支援システムのネットワーク構成を，図 1 に示す。

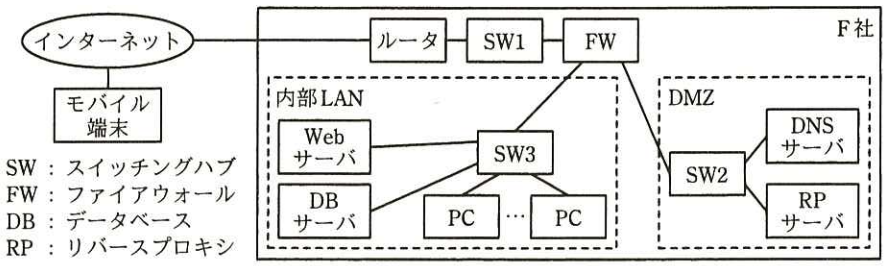


図 1　現在の営業支援システムのネットワーク構成（抜粋）

F 社の営業部員は，社内で営業支援システムにアクセスする場合には，自席の PC を使い，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。社内の PC からインターネットへのアクセスは，RP サーバを経由しない。

F 社では数年前にネットワーク構成を見直し，侵入検知システム（IDS）の機能をもった FW を導入した。最近になって営業部員から，インターネットを通じたサービスのレスポンスがしばしば悪化していると，苦情が寄せられるようになった。F 社の情報システム部が調査した結果，現在の FW は IDS としての性能の限界に近づいており，これがレスポンス悪化の原因となっていると考えられた。IDS 機能を使わなければ FW は負荷が軽減され，今後も継続して利用できることが分かった。

また，最近発見された一部のサーバのミドルウェアの脆弱性を悪用する攻撃は，FW の IDS 機能では検出できないものであった。このときは，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。

F 社の情報システム部は，インターネットを通じた様々なサイバー攻撃の増大が頻繁に報道されていることも考慮し，営業支援システムのセキュリティレベルを向

上させるために，プロジェクトを立ち上げた。プロジェクトのリーダには H 君が任命された。まず H 君は，IDS の見直しを開始した。

〔IDS の見直し〕

侵入検知の仕組みとしては，次の 2 種類がある。

一方はシグネチャ型と呼ばれ，不正なパケットに関する一定のルールやパターンを使う。原則として未知の攻撃には対応できないが，あらかじめ様々な種類のシグネチャが登録されている。

他方の［　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。H 君は，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。

次に，H 君は，IDS のネットワークへの接続について検討した。

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。また，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。

検出可能な通信は，IDS の接続箇所によって異なる。例えば，インターネットと DMZ 間の通信は，IDS を SW1 又は SW2 に接続した場合は検出可能だが，SW3 に接続した場合は検出できない。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。

表 1　IDS で検出可能な通信（接続箇所別）

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	×	×	○
（設問のため，省略）			

○：検出可　　×：検出不可

H 君が調査した 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。

また，IDS が不正な TCP コネクションを検知した場合に，該当する通信を強制的に切断する目的で，送信元と宛先の双方の IP アドレス宛てに，TCP の RST フラグをオンにしたパケットを送る機能があった。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。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。

これまでの検討結果から，H 君は，より高度な侵入防御の仕組みが必要であると考え，ネットワークの重要な部分へは侵入防止システム（IPS）を追加することを検討した。

〔IPS の追加〕

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。しかし，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。

また，高度な機能をもつ IPS には高い負荷が掛かることが予想される。ネットワークの通信量が急激に増えた場合でも，営業支援システムのレスポンス悪化を避け，継続して利用できる状態にすることが重要であることから，H 君は IPS の障害対策について検討した。

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，④IPS 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，H 君は IPS を冗長化しないことにした。

以上の検討の結果，H 君は営業支援システムのネットワークに，IDS と IPS の両方を追加し，管理用 PC を接続した管理用 LAN を設けることを考えた。

H 君による，見直し後の営業支援システムのネットワーク構成案を，図 2 に示す。

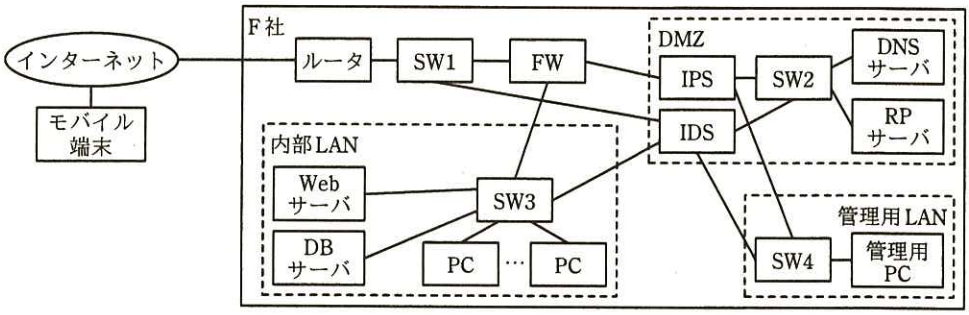


図 2　見直し後の営業支援システムのネットワーク構成案（抜粋）

H 君が考えたネットワーク構成案は承認され，営業支援システムの見直しプロジェクトが開始された。

設問 1　本文中の［　ア　］～［　オ　］に入れる適切な字句を答えよ。

設問 2　〔IDS の見直し〕について，(1) ～ (3) に答えよ。

(1) 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。

(2) 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。40 字以内で具体的に述べよ。

(3) H 君が，本文中の下線 ② のように考えたのはなぜか。35 字以内で述べよ。

設問 3　〔IPS の追加〕について，(1) ～ (3) に答えよ。

(1) 本文中の下線③で可能としている，一時的な運用を 50 字以内で述べよ。

(2) 本文中の下線 ④ の，IPS が実装している機能とは何か。25 字以内で述べよ。

(3) 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。35 字以内で具体的に述べよ。

6. 退室可能時間に途中で退室する場合には，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	13:10 ～ 13:50

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。
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。
13. 午後Ⅱの試験開始は **14:30** ですので，**14:10** までに着席してください。