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〕

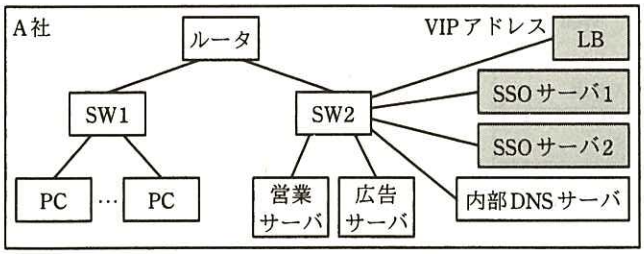
情報システム課は，A 社の全システムに SSO を本格導入する前に，試験的に営業システムと広告システムに SSO を導入することにした。そこで，B 課長が要件をとりまとめ，ネットワーク担当の C 氏に検討を指示した。その指示の内容を次に示す。

・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。

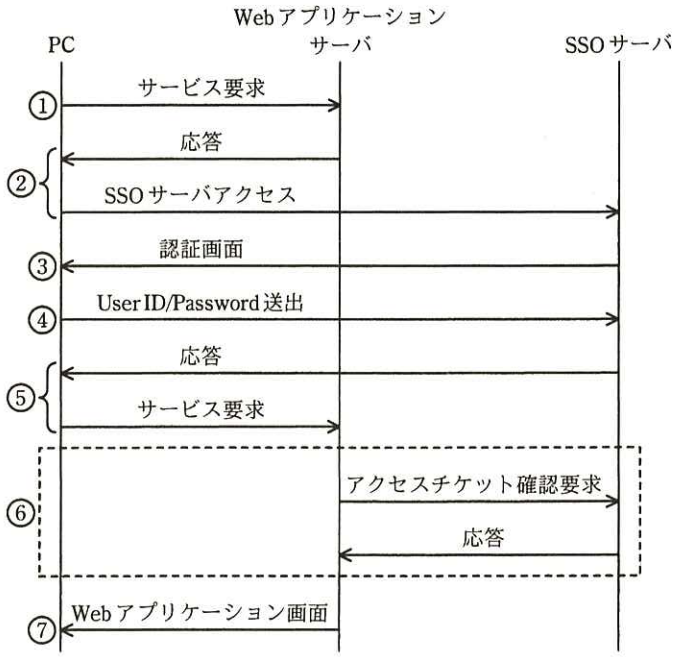


図2　エージェント方式における SSO 認証処理のシーケンス

〔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。