問1　インターネット Web サイトの刷新に関する次の記述を読んで，設問 1～4 に答えよ。

A 社は，従業員数 700 名の外食サービス会社であり，地方都市で事業を展開している。A 社グループ傘下には，レストラン，ピザ店及びハンバーガー店がある。A 社では，これまで，様々な業務のシステム化を行ってきたが，今年末の宅配すし事業の立上げを契機に，販売促進システムの一部であるインターネット Web サイトにおけるサービス向上を検討することになった。

〔A 社のインターネット Web サイトの概要〕

A 社のインターネット Web サイトには，一般公開用のもの（以下，一般サイトという。ドメインは a-sha.co.jp）と，事前に登録した会員向けのもの（以下，会員サイトという。ドメインは a-sha-kaiin.com）がある。

一般サイトでは，会社情報及び商品情報を提供しており，誰でも閲覧できる。一般サイトは，コンテンツの更新も含めて B 社に運用管理を委託している。会員サイトは，一般サイトにあるリンクで示された Web ページでログインでき，登録した届け先住所を用いた手軽な注文が可能で，注文履歴に基づいてお勧め商品に関する情報を表示するといったサービスを提供している。会員の誕生日には割引券も発行しており，評判が良い。

会員サイトは個人情報を扱うことから，①サーバ認証による HTTPS を採用し，その上でのフォームを用いた利用者認証を行っている。例えば，ある会員がブラウザで会員サイトにアクセスしようとすると，利用者 ID とパスワードによる利用者認証が求められ，認証に成功すると，会員サイトにアクセスできるようになる。クッキーの有効期限が切れるか，利用者がログアウトした後は，当該ブラウザから会員サイトにアクセスできなくなり，再び利用者認証を求められる。

会員サイトは，D 社に運用管理を委託しており，A 社情報セキュリティポリシ上，個人情報を扱う会員サイトから一般サイトへのデータの転送といった機密データの連携は一切行わないことになっている。

〔インターネット Web サイトのサービス向上策の検討〕

会員が一般サイトにアクセスした際に，当該会員の獲得ポイント状況，最近の注文

状況のほか，近隣のグループ店からのお知らせなどの情報を表示するサービス（以下，ターゲット型広告サービスという）を検討することにした。そこで，最近話題になっているマッシュアップ技術を有効活用したサービス（以下，マッシュアップサービスという）が実現可能かどうかを調査することになった。

マッシュアップサービスの実現に関しては，まず，Ajax（Asynchronous JavaScript + XML）という技術を用いることを検討した。

Ajax を用いると，Web ページ全体を再描画することなく，現在表示されている Web ページの表示の一部だけを更新することができる。例えば，［ a ］を利用する HTML ファイル群をブラウザがダウンロードして実行すると，非同期的又は同期的に Web サーバにアクセスし，そのレスポンスデータを用いて Web ページを更新することができる。

しかし，通常，ブラウザではセキュリティ確保のための［ b ］ポリシが採用されているので，［ a ］を利用する HTML ファイル群をダウンロードして実行する際，FQDN，プロトコル又はポート番号のいずれかが，ダウンロードしたものと異なる URI にはアクセスできず，A 社が想定するターゲット型広告サービスを実現できない。そこで，次に，JSONP（JavaScript Object Notation with Padding）という技術を用いて，マッシュアップサービスを実現することを検討した。JSONP を用いて上記の 3 要素のいずれかが異なる URI からでもデータを取得することが可能な JavaScript（以下，JSONP 呼出しスクリプトという）を記述できる。

A 社では JSONP を用いてターゲット型広告サービスを実現する仕組みを検討した。図 1 はその案である。この案では，会員のポイントの獲得状況を表示するサービス（以下，ポイント表示サービスという）用の JSONP 呼出しスクリプト（図 2）を呼び出すページを，一般サイトのトップページに用意しておく。例えば，利用者 ID を user1 としてログインした会員が，一般サイトのトップページを閲覧した際，会員サイトから送られてくる図 3 に例示したような JSONP 型データを用いて，その月の獲得ポイントとトータルの獲得ポイントを表示する。

A 社ではポイント表示サービスのほかにも，会員の誕生月にポイントを 2 倍付与するサービスと，会員が住む地域のグループ店からのお得情報を提供するサービスを検討している。

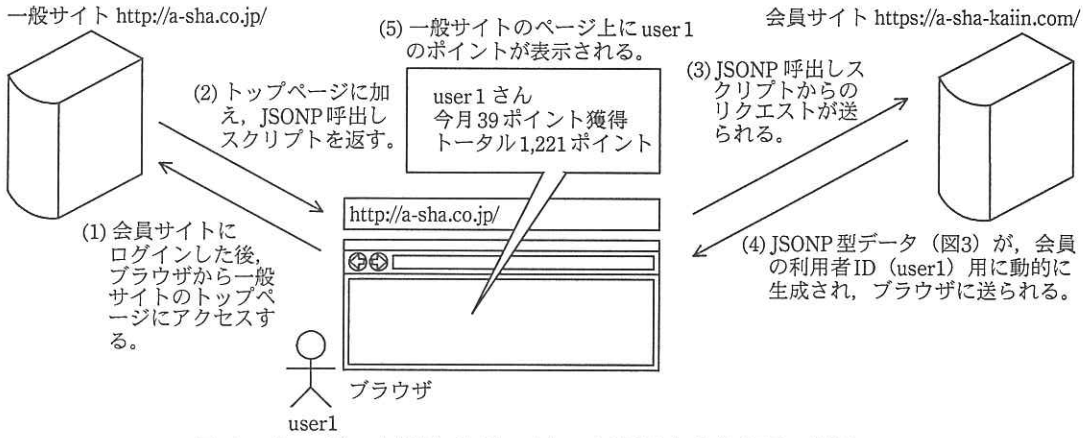

図１　ターゲット型広告サービスを実現する仕組み（案）

```
function putUserData(data) {
    dispUserPoint(data.name, data.thisMonthPoint, data.totalPoint);
}
// データ提供用に用意された会員サイトのURL
var url = "https://a-sha-kaiin.com/callback.json";
// 動的にSCRIPTタグを生成
var script = document.createElement("script");
script.setAttribute("src", url);
```

注記　dispUserPointは，ブラウザに表示をするために別途用意された関数である。

図２　ポイント表示サービス用のJSONP呼出しスクリプト（抜粋）

```
putUserData({name:"user1", thisMonthPoint:39, totalPoint:1221,
birth:"1978/3/15", address:"user1の住所", telephone:"029-xxx-yyyy"});
```

図３　会員サイトから送られてくるJSONP型データの例

〔セキュリティに関する検討〕

A社では，マッシュアップサービスを初めて導入することもあり，ターゲット型広告サービスの仕組みについて，セキュリティ専門家のZ氏にレビューを受けた。すると，ポイント表示サービスの仕組みには，次に示すようにJSONP呼出しスクリプトを悪用する攻撃で会員の個人情報が漏えいする可能性があるとの指摘を受けた。

A社のポイント表示サービスの仕組みの場合，［c］から送られる［d］が，会員の個人情報を含む。しかし，②ある条件が成立しているとき，悪意あるWebサイトにアクセスし，図4のように動作するJSONP呼出しスクリプトを［e］が実行すると，［d］に含まれる会員の個人情報を奪われる可能性がある。

ステップ1)　[c] にアクセスし，目的とする [d] を取得する。
ステップ2)　取得した [d] から会員の個人情報を抽出して，悪意あるWebサイトに転送する。

図4　悪意あるJSONP呼出しスクリプトの動作概要

Z氏からは，このような攻撃に対する一般的な対策として図5が示され，対応をA社関係者で検討した。

JSONP型データをブラウザに送信する前に，そのリクエストが正規のものであることを確認し，確認できた場合にだけJSONP型データをレスポンスで返す。この確認の実現方法には次の二つがある。
(1)　認証情報を用いた確認
　リクエストのHTTPヘッダに埋め込んである認証情報を確認する。認証情報とは，そのリクエストが [f] からのアクセスであることを確認できるものである。(以下，省略)
(2)　Refererヘッダによる参照元の確認
　JSONP型データをリクエストする直前に特定のページにアクセスしていたことをRefererヘッダで確認する。(以下，省略)

図5　JSONP呼出しスクリプトを悪用しようとする攻撃への一般的な対策

ポイント表示サービスの実現においては，会員が一般サイトのトップページにアクセスした際，JSONP呼出しスクリプトが会員サイトにアクセスする。そのため，図5の(1)の対策をとるには，一般サイトで“トップページへのアクセスのリクエストが [f] からのアクセス”という情報が必要になる。しかし，一般サイトと会員サイトの運用管理会社が違うこともあり実現方法の検討に期間を要してしまうので，この対策方法は見送ることにした。

図5の(2)の対策については，A社のWebサイトは様々な環境の利用者を想定していることから，Refererヘッダの情報がサーバに [g] というケースもあり得るので，Refererヘッダの情報の利用を前提としてポイント表示サービスを実現すると，正規のリクエストか否かを区別できないケースがある。そのため，この対策方法も見送ることにした。

Z氏との検討の結果，ポイント表示サービスを含むターゲット型広告サービスは，将来普及が見込まれる [a] の新規格を用いることも含めて検討課題とし，最終的には，ターゲット型広告サービスを除いてA社のWebサイトを刷新することとした。

設問 1　本文中の［　a　］，［　b　］に入れる適切な字句を解答群の中から選び，記号で答えよ。

解答群

ア　APT　　イ　ATM　　ウ　Same-Origin

エ　XMLHttpRequest　　オ　アノニマス　　カ　プライバシ

設問 2　本文中の下線①について，SSL のクライアント認証と比較した場合の，サーバ認証による HTTPS 通信上でフォームを用いた利用者認証を行う利点を，25 字以内で述べよ。

設問 3　悪意ある JSONP 呼出しスクリプトについて，(1)～(3)に答えよ。

(1)　本文及び図 4 中の［　c　］並びに本文中の［　e　］に入れる適切な字句を答えよ。

(2)　本文中の下線②における条件を，本文に即して，50 字以内で述べよ。

(3)　本文及び図 4 中の［　d　］に入れる適切な字句を，10 字以内で具体的に答えよ。

設問 4　JSONP を用いて，個人情報を扱う際の対策の検討について，(1)，(2) に答えよ。

(1)　本文及び図 5 中の［　f　］に入れる適切な字句を，10 字以内で答えよ。

(2)　本文中の［　g　］に入れる適切な字句を，10 字以内で答えよ。