問2　スマートフォンアプリケーションに関する次の記述を読んで，設問1～3に答えよ。

R 社は，従業員数 1,000 名の飲食店情報提供サービス会社である。R 社では，会員制 Web サイトで飲食店情報や割引クーポンを提供してきた。今回，会員数を更に増やすために，新たに R 社スマートフォンアプリケーション（以下，スマホアプリという）を利用したサービスを提供することを決め，プロジェクトを立ち上げた。プロジェクトリーダには，会員制 Web サイトの運用チームのメンバである B さんが任命された。

〔スマホアプリの概要〕

スマホアプリは，専用 Web サーバに設置する Web アプリケーション（以下，WebAP という）と通信する。WebAP は各飲食店の予約システムと通信して，予約を行う。スマホアプリを利用したサービスのシステム構成を図 1 に，スマホアプリと WebAP の動作概要（案）を表 1 に示す。

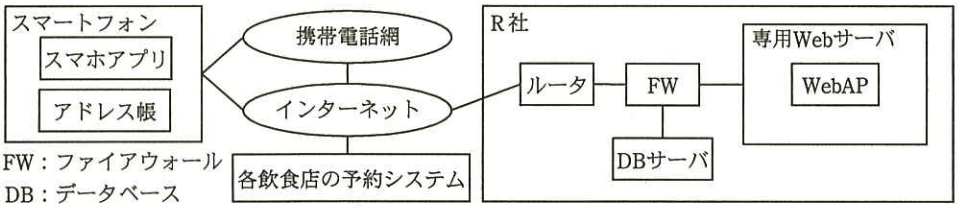

図 1　スマホアプリを利用したサービスのシステム構成

表 1　スマホアプリと WebAP の動作概要（案）

サービス	スマホアプリ	WebAP
(1) 情報配信	新しい飲食店情報を WebAP に定期的に確認し，受信	新しい飲食店情報を送信
(2) 飲食店検索	地域，料理ジャンル，その他条件を選択して WebAP に送信し，検索結果を受信	検索条件に合致する飲食店情報を送信
(3) 予約確認	会員が予約した情報（以下，予約情報という）を WebAP から受信し，表示	予約情報を送信
(4) 予約案内	パーティ開催のために会員が予約した日時，店舗情報をパーティ参加予定者に案内するために，スマートフォン内のアドレス帳の全件データを WebAP に送信	アドレス帳の全件データの中からパーティ参加予定者を選択して，そのメールアドレスに予約情報を記載した電子メール（以下，メールという）を送信
(5) 新規予約	WebAP に予約要求を送信し，予約結果を WebAP から受信	スマホアプリからの予約要求を飲食店の予約システムに送信し，予約結果をスマホアプリに送信
(6) 会員管理	会員情報を受信して表示し，変更情報を WebAP に送信	DB に登録している会員情報を送信し，変更情報を受信

〔スマホアプリの利用者認証〕

B さんは，スマホアプリを開発するに当たり，利用者認証について情報システム部のC課長に相談した。次は，そのときの会話である。

Bさん：スマホアプリを繰返し利用してもらうために，面倒なログイン操作は初回だけにして，2回目以降は自動的に利用者が認証されるようにしたいと考えています。

C課長：2回目以降はどんな情報を用いて利用者を認証するのかね。

Bさん：スマートフォンには，IMEI（International Mobile Equipment Identity）などの固有の端末識別番号が付与されていますので，これを用いて利用者を認証することを考えています。

C課長：確かに端末識別番号は端末の固有コードにはなるね。しかし，端末識別番号の特性を考えると，自分の端末識別番号を別の端末で利用されて，サービスを不正利用されるおそれがあるから，①端末識別番号の値をそのまま利用者認証に使うわけにはいかないな。

Bさん：そのまま使うのが問題であれば，端末識別番号を基にスマホアプリ内で②鍵付きハッシュ関数で算出したハッシュ値を使うという方法はどうでしょう。このスマホアプリ専用の鍵を一つ用意して，スマホアプリ内に格納しておけば，不正利用を防ぐことができるのではないかと思います。

C課長：しかし，③鍵を秘密にしておくことが難しいので，その方法を採用してはいけないと思うよ。スマートフォンサイトでの利用者認証は，一般的な PC サイトと同じように考えた方がいいのではないかな。

Bさん：分かりました。

〔予約案内サービスの問題〕

予約案内サービスは，利用者がパーティの参加予定者を利用者のスマートフォンのアドレス帳から選択すると，予約した日時，店舗の情報が参加予定者にメールで通知されるサービスである。具体的には次のような手順で行われる。

(1) 利用者が，スマホアプリの画面で“友達に案内する”ボタンを選択すると，図 2 のような予約案内の確認画面が表示される。

(2) 確認画面の“はい”ボタンを選択すると，WebAP にアドレス帳の全件データが送信され，友達の選択画面が表示される。

(3) 選択画面で参加予定者を選択すると，WebAP から参加予定者宛てにメールが送信される。

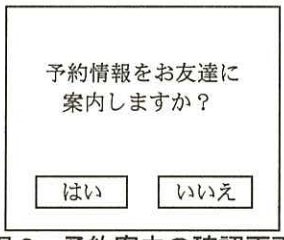

図２　予約案内の確認画面

予約案内サービスについてプロジェクトのメンバが検討している際に，“図２の確認画面は，メールで予約情報を案内することについて同意確認を行っているが，アドレス帳の全件データが R 社に送信されることについては利用者に説明していないので問題である”という意見が多くのメンバから出た。

この意見に対して，“アドレス帳の全件データが送信されることについて確認画面で明確に説明し，同意確認を行う”という改善案が出た。しかし，説明しただけでは不十分であるとして，“アドレス帳の全件データの送信”が行われない別の案（以下，A 案という）が提示され，A 案を採用することになった。

B さんは A 案に基づき，仕様を策定した。また，スマホアプリの機能や動作を利用者に理解してもらえるよう，スマホアプリの導入時に表示される利用規約に，サービスについて詳細に記述することにした。B さんは仕様書を渡して開発業者にスマホアプリと WebAP の実装を依頼した。

〔WebAP の問題〕

開発後，スマホアプリと WebAP に関して第三者のセキュリティ評価を受けることが決定された。そこで B さんは，この分野で実績がある S 社を選んでセキュリティ評価を受けることにした。S 社によるセキュリティ評価の結果，WebAP の予約確認サービスには他人の予約情報を取得できてしまうという問題があるとの指摘を受けた。予約確認サービスのリクエストに含まれるパラメタの概要と，WebAP の予約確認サービスの動作概要を図３に示す。

この問題は，ある利用者（以下，利用者 V という）が，数日前に自分が発した予約確認のリクエスト中に含まれるパラメタのうちの二つのパラメタの値を変更して送信することによって，別の利用者（以下，利用者 W という）の予約情報を取得することができるというものであった。つまり，④利用者 V が予約情報を表示した際のリクエストである図 4 で使われるパラメタのうちの二つの値を変更して送信すると，利用者 W が予約情報を表示した際のリクエストである図 5 に対する応答を得られるというも

のである。セキュリティ評価では，仕様書などを参考にして，図 4 のリクエストに操作を加えた上で，WebAP に送信し，その応答を確認した。予約確認サービスについて，図 4 のリクエストに対して行った操作内容，及びリクエストに対して WebAP から受信した応答を表 2 に示す。

1. 予約確認サービスのリクエスト中のパラメタの概要
 ・LANG：言語を指定する値
 ・AppID：アプリケーション名
 ・AuthKey：初回ログイン時に発行される利用者認証用のキー
 ・YoyakuCode：年月と予約番号で構成された予約明細コード（予約番号は月ごとに全利用者の予約を 000001 から順番に割り振る）
 ・DateTime：スマートフォンの年月日及び時刻

2. WebAP の予約確認サービスの動作概要
 (a) LANG の値が条件に含まれる文字以外の場合はアプリケーションエラーを返し，ja の場合は日本語，en の場合は英語で該当するコンテンツを返す。
 (b) AppID の値が URL に含まれていなければアプリケーションエラーを返す。
 (c) AuthKey の値が WebAP に保持されている利用者認証用の値と一致しない場合は認証エラーを返す。
 (d) YoyakuCode の値が DB サーバに保持されている予約明細コードと一致しない場合はアプリケーションエラーを返す。
 (e) DateTime の値とサーバ側の時刻とのずれが 5 分以上の場合はアプリケーションエラーを返す。
 (f) (a)～(e)でエラーを返さない場合は該当の予約情報を返す。

図 3　WebAP の予約確認サービスのパラメタと動作概要

表 2　リクエストに対して行った操作内容，及び WebAP から受信した応答（抜粋）

リクエストに対して行った操作内容	WebAP から受信した応答
LANG パラメタを削除	アプリケーションエラー
LANG パラメタの値を削除	アプリケーションエラー
LANG パラメタの値を 0 に変更	アプリケーションエラー
AppID パラメタを削除	アプリケーションエラー
AppID パラメタの値を新規予約サービス（ShinkiYoyaku）に変更	アプリケーションエラー
AuthKey パラメタを削除	認証エラー
AuthKey パラメタの値を削除	認証エラー
AuthKey パラメタの値を別利用者の値に変更	YoyakuCode が 201310000034 の予約情報の表示
YoyakuCode パラメタを削除	アプリケーションエラー
YoyakuCode パラメタの値を 201310000071 に変更	YoyakuCode が 201310000071 の予約情報の表示
DateTime パラメタを削除	アプリケーションエラー
DateTime パラメタの値を現在から 4 分前の時刻に変更	YoyakuCode の値に該当する予約情報の表示
DateTime パラメタの値を現在から 5 分前の時刻に変更	アプリケーションエラー

注記　操作するパラメタ以外の値はエラーにならない値を送るものとする。

```
POST /coupon/YoyakuKakunin HTTP/1.0
Host: www.r-sha.jp
Content-Type: text/xml
Content-length: 254

<?xml version="1.0" encoding="utf-8"?>
<XML>
    <LANG>ja</LANG>
    <AppID>YoyakuKakunin</AppID>
    <AuthKey>f3c7b48aac2da10596271a460fb317ac</AuthKey>
    <YoyakuCode>201310000034</YoyakuCode>
    <DateTime>2013 10 16 18:08:10</DateTime>
</XML>
```

図４　利用者Ｖが予約情報を表示した際のリクエスト

```
POST /coupon/YoyakuKakunin HTTP/1.0
Host: www.r-sha.jp
Content-Type: text/xml
Content-length: 254

<?xml version="1.0" encoding="utf-8"?>
<XML>
    <LANG>ja</LANG>
    <AppID>YoyakuKakunin</AppID>
    <AuthKey>6h4Y4io98Uy3q2rfbghyy45ecRyH44po</AuthKey>
    <YoyakuCode>201310000071</YoyakuCode>
    <DateTime>2013 10 16 20:17:14</DateTime>
</XML>
```

図５　利用者Ｗが予約情報を表示した際のリクエスト

〔指摘された問題への対応〕

Ｂさんは Ｓ 社から指摘された問題について対応を検討し，開発業者に依頼して必要な修正を行った後，再度 Ｓ 社のセキュリティ評価を受けた。その結果，問題が解消されていることが確認できたので，スマホアプリを利用したサービスの提供を開始した。

設問１　〔スマホアプリの利用者認証〕について，(1)～(3)に答えよ。

(1)　Ｃ 課長が本文中の下線①のように判断したのは，端末識別番号のどのような特性からか。20 字以内で述べよ。

(2)　本文中の下線②の鍵付きハッシュ関数を解答群の中から選び，記号で答えよ。

解答群

ア　AES　　イ　HMAC　　ウ　RIPEMD　　エ　SHA-256

(3) 本文中の下線③について，どのような手法で鍵を知られてしまうか。30 字以内で述べよ。

設問 2 〔予約案内サービスの問題〕について，A 案の実現方法を，40 字以内で述べよ。

設問 3 〔WebAP の問題〕について，(1)，(2)に答えよ。

(1) 本文中の下線④について，利用者 V はどのパラメタの値を変更することによって利用者 W の予約情報を取得できたか。値を変更したパラメタを，図 4 から選び，二つ答えよ。また，それぞれ，どのような値にすることで予約情報を取得できたか。予約情報を取得できたパラメタの内容を答えよ。

(2) 他人の予約情報を取得できてしまう問題の対策として，図 3 の 2.にどのような仕様を追加すればよいか。追加する仕様を 55 字以内で述べよ。