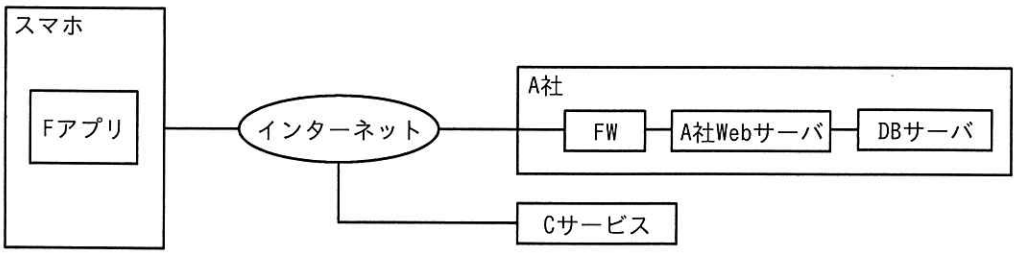
問３　スマートフォン用アプリケーションプログラムの開発に関する次の記述を読んで，設問に答えよ。

A 社は，撮影機器の販売や写真のプリントサービスを全国に 200 店舗で展開する従業員 2,000 名の企業である。実店舗の運営に加え，インターネットを介して撮影機器の販売を行う EC サイト事業を有している。このたび，会員がスマートフォン（以下，スマホという）用アプリケーションプログラム（以下，スマホ用アプリケーションプログラムをスマホアプリという）を通じて，写真入りのカレンダーなどのグッズ（以下，フォトグッズという）を注文できるサービス（以下，E サービスという）を新規に開始することになった。E サービス用スマホアプリ（以下，F アプリという）は国内で流通する主要なスマホ OS である OS-α と OS-β の過去 5 年以内に正式リリースされたバージョンをサポートする。

〔E サービスの説明〕

E サービスは，F アプリとサーバサイドのシステム群で構成される。F アプリは，インターネットを介して E サービス用 Web サーバ（以下，A 社 Web サーバといい，FQDN は www.a-sha.co.jp とする）及び大手クラウドサービスプロバイダ C 社のクラウドストレージサービス（以下，C サービスという）との間で HTTPS を使用して通信する。フォトグッズの作成に使う写真は，F アプリから C サービスにアップロードする。E サービスのネットワーク構成を図 1 に，機能概要を図 2 に，F アプリの画面構成を図 3 に，フォトグッズの注文処理の流れを図 4 に，C サービスの仕様を図 5 に示す。



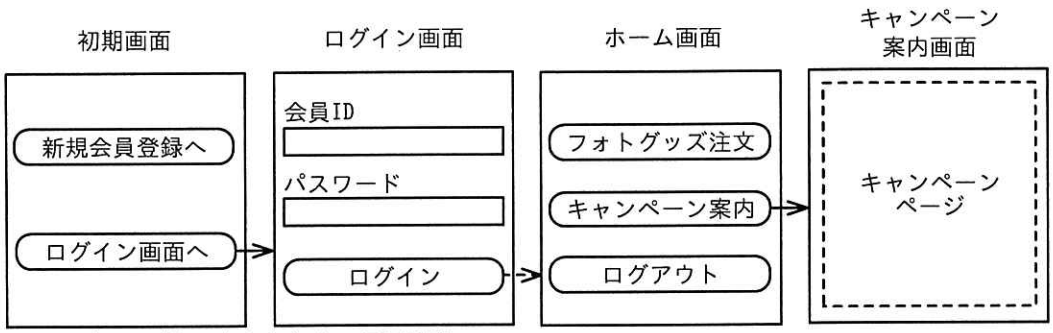
FW：ファイアウォール　　DBサーバ：データベースサーバ

図 1　E サービスのネットワーク構成（概要）

1. 新規会員登録機能
   E サービスを利用するための新規会員登録を行う。
2. ログイン機能
   会員 ID とパスワードでログインする。ログインした会員には，認証トークン [1] が払い出され，ログアウトするまでの間，F アプリに保存される。認証トークンは，A 社 Web サーバ上で会員のセッションを識別するために使用する推測困難な値である。
3. フォトグッズ注文機能
   F アプリ上でフォトグッズを注文する。ログイン済み会員だけが利用できる。
   なお，フォトグッズは，指定した A 社の実店舗で受け取ることができる。
4. キャンペーン案内機能
   キャンペーンの Web ページ（以下，キャンペーンページという）を表示する。ログイン済み会員だけが利用できる。
   なお，キャンペーンに応募することによって，フォトグッズの割引などに利用可能なクーポンを入手できる。会員には，電子メール（以下，メールという）などを通じて，期間限定のキャンペーンを案内する。キャンペーンの内容は，2 週間ごとに更新される。

注 [1] 認証トークンは，ログイン後に F アプリが A 社 Web サーバに HTTP リクエストを送信する際，Authorization ヘッダーに指定される。

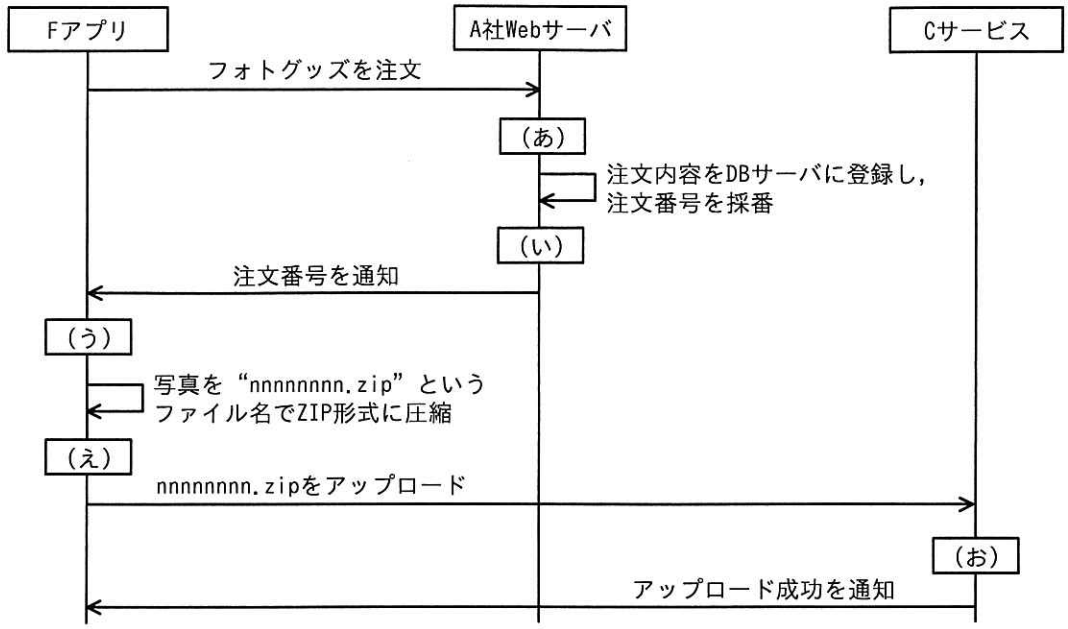
図 2　E サービスの機能概要（抜粋）



→：ボタンが押下されたときの画面遷移
-→：適切な値を入力してボタンが押下されたときの画面遷移

注記　キャンペーンページは HTML 形式で作成し，A 社 Web サーバにアップロードしておく。

図 3　F アプリの画面構成（抜粋）



注記　“nnnnnnnn”は注文番号であり，00000001から始まる十進数の連番である。

図4　フォトグッズの注文処理の流れ

1. サービスの概要

(1) Cサービスはマルチテナントのストレージサービスである。テナントの管理権限をもつ利用者（以下，管理者という）が作成したストレージに対し，テナントの作成したシステム（以下，利用システムという）からファイルのアップロードやダウンロード（以下，アップロード，ダウンロードを併せてファイル操作という）を行う。

(2) 管理者は，ストレージの作成時に任意のストレージ名を設定する。ストレージを作成すると，Cサービスからアクセスキーが発行される。アクセスキーはストレージごとに異なる40字の英数字である。

(3) 利用システムは，ストレージ上のファイルをURLのパスで指定する。例えば，ストレージ“●●●”上のファイル“▲▲▲”をファイル操作する際は，“/●●●/▲▲▲”を指定する。ファイルのアップロードにはHTTPのPUTメソッドを，ファイルのダウンロードにはGETメソッドを用いる。

(4) 利用システムは，次の方式a又は方式bでファイル操作を行う。

2. 方式a

(1) 説明

アクセスキーをHTTPリクエストのAuthorizationヘッダーに指定する方式である。利用システムは，Cサービスから発行されたアクセスキーを用いることによって，アクセスキーに対応するストレージに格納された全てのファイルに対するファイル操作が可能となる。

Authorizationヘッダーに正しいアクセスキーが指定されていない場合，ファイル操作は拒否される。

図5　Cサービスの仕様（抜粋）

(2) 使用例

アクセスキー“○○○”を指定して，ストレージ“abc”上のファイル“xyz”をダウンロードする際に送信するHTTPリクエストの例を次に示す。

リクエストライン　：GET /abc/xyz HTTP/1.1

ヘッダーフィールド：Host: storage.c-sha.jp

Authorization: Bearer ○○○

3. 方式b

(1) 説明

有効期限（Expires）と署名値（Signature）をクエリパラメータとして付加したURL（以下，署名付きURLという）を用いて，特定のファイルに対するファイル操作を一時的に可能とする方式である。ここで，Expiresパラメータに指定する有効期限はUNIXタイムスタンプ形式である。署名値の生成は次のように行う。

（i）GET又はPUTから始まり，パス中の“/●●●/▲▲▲?Expires=【有効期限】”で終わる文字列を署名対象文字列とする。

（ii）アクセスキーを秘密鍵とする。

（iii）署名対象文字列と秘密鍵からHMAC-SHA256値を求める。

（iv）（iii）で求めた値をbase64urlエンコードする。

利用システムは，署名付きURLを生成し，ファイル操作を許可する利用者に伝える。伝えられた利用者は，署名付きURLを指定してHTTPリクエストを送ることによって，ファイル操作ができる。有効期限が切れた場合やサーバ側で署名値の検証が失敗した場合は，ファイル操作が拒否される。

(2) 使用例

ストレージ“abc”上のファイル“xyz”をダウンロードする場合で，かつ，署名値が“△△△”の場合のHTTPリクエストの例を次に示す。xyzは，日本時間の2025年5月30日0時0分0秒，つまりUNIXタイムスタンプで1748530800までの間，ダウンロードが許可されている。

リクエストライン　：GET /abc/xyz?Expires=1748530800&Signature=△△△ HTTP/1.1

ヘッダーフィールド：Host: storage.c-sha.jp

図5　Cサービスの仕様（抜粋）（続き）

Eサービスで使うCサービスのストレージ名は，e-serviceである。Fアプリでは，方式aを利用する。アクセスキーは，鍵長256ビットの共通鍵とAES-CBCアルゴリズムで暗号化し，Fアプリ内にリソースとして保存する。Cサービスのストレージ名並びにAES-CBCの共通鍵及び初期ベクトルは，Fアプリのコード中に定数として定義する。

〔キャンペーン案内機能の実装方法〕

Fアプリでのキャンペーンページの表示には，WebViewという仕組みを用いる。WebViewは，スマホOSの提供する仕組みであり，スマホアプリの画面の一部にWebペ

ージを表示させることができる。キャンペーンページのHTMLは，WebViewを用いて，Fアプリの画面上に表示させる。

会員に送るキャンペーン案内のメール本文中には，F アプリでキャンペーンページを表示するための URL（以下，F-URL という）を含める。会員がメールアプリから F-URL を開くと，F アプリが起動し，WebView 上にキャンペーンページが表示される。キャンペーンページからキャンペーンに応募する際の会員のセッションの識別には，F アプリに保存されている認証トークンを用いる。OS-αでは，キャンペーンページが表示された後に，WebView の機能によってキャンペーンページ上の ECMAScript コードが F アプリの getToken 関数を呼び出す。これによって，認証トークンが F アプリからキャンペーンページに引き渡される。OS-βでは別の方式で同様の機能を実現する。キャンペーンページ上の ECMAScript コードを図 6 に示す。

```
const token = f_app.getToken();
```

図 6　キャンペーンページ上の ECMAScript コード

キャンペーンページ以外から getToken 関数を悪用されないように，getToken 関数の内部では，図 7 のように呼出し元の Web ページの URL を確認する。

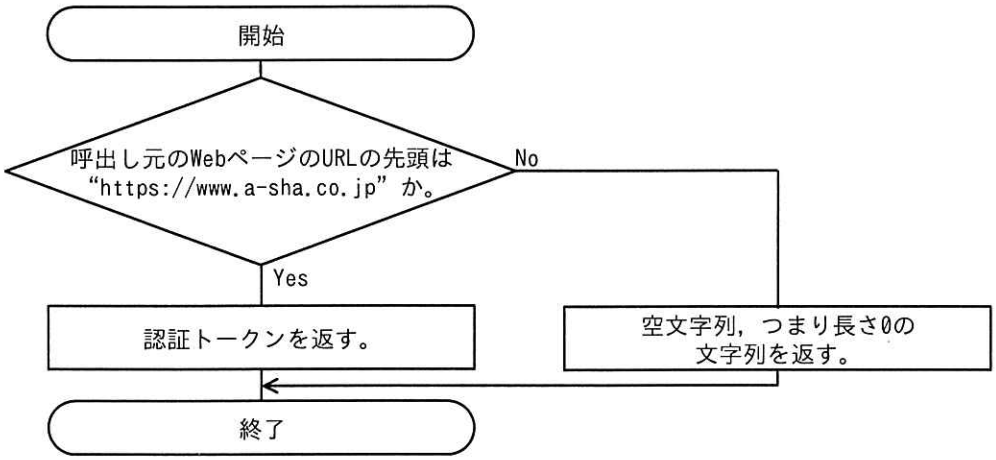


図 7　getToken 関数の処理の流れ

F-URL の例を図 8 に示す。

```
f-app://campaign?url=https://www.a-sha.co.jp/campaign/□□□
```

注記1　“f-app”はカスタムURLスキームである。
注記2　“□□□”はキャンペーンページのURLのパスである。

図8　F-URLの例

〔Fアプリの脆弱性診断結果〕

A社は，セキュリティ専門会社のD社に依頼してFアプリの脆弱性診断を実施した。その結果，表1に示す脆弱性が検出された。

表1　脆弱性診断結果（抜粋）

脆弱性	脆弱性の概要	解説
1	サーバ証明書の検証不備がある。	Fアプリは，HTTPSでサーバと接続する際，サーバ証明書の検証エラーがあっても無視し，通信を続行する。そのため，HTTPS通信の内容が盗聴されたり，改ざんされたりするおそれがある。盗聴されると，①盗聴した内容からアクセスキーとストレージ名を攻撃者が取得するおそれがある。 （省略）
2	Cサービスのアクセスキーの保護に不備がある。	②攻撃者がFアプリから平文のアクセスキーとストレージ名を取得できる。そのアクセスキーを用いて，③攻撃者がEサービスの全利用者の写真を不正にダウンロードするおそれがある。 （省略）
3	F-URLの処理にアクセス制御の不備がある。	F-URLのurlクエリパラメータに，④細工したURLが指定されることによって，攻撃者のWebサイトにアクセスしてしまうおそれがある。また，攻撃者が会員の認証トークンを取得するおそれがある。 （省略）

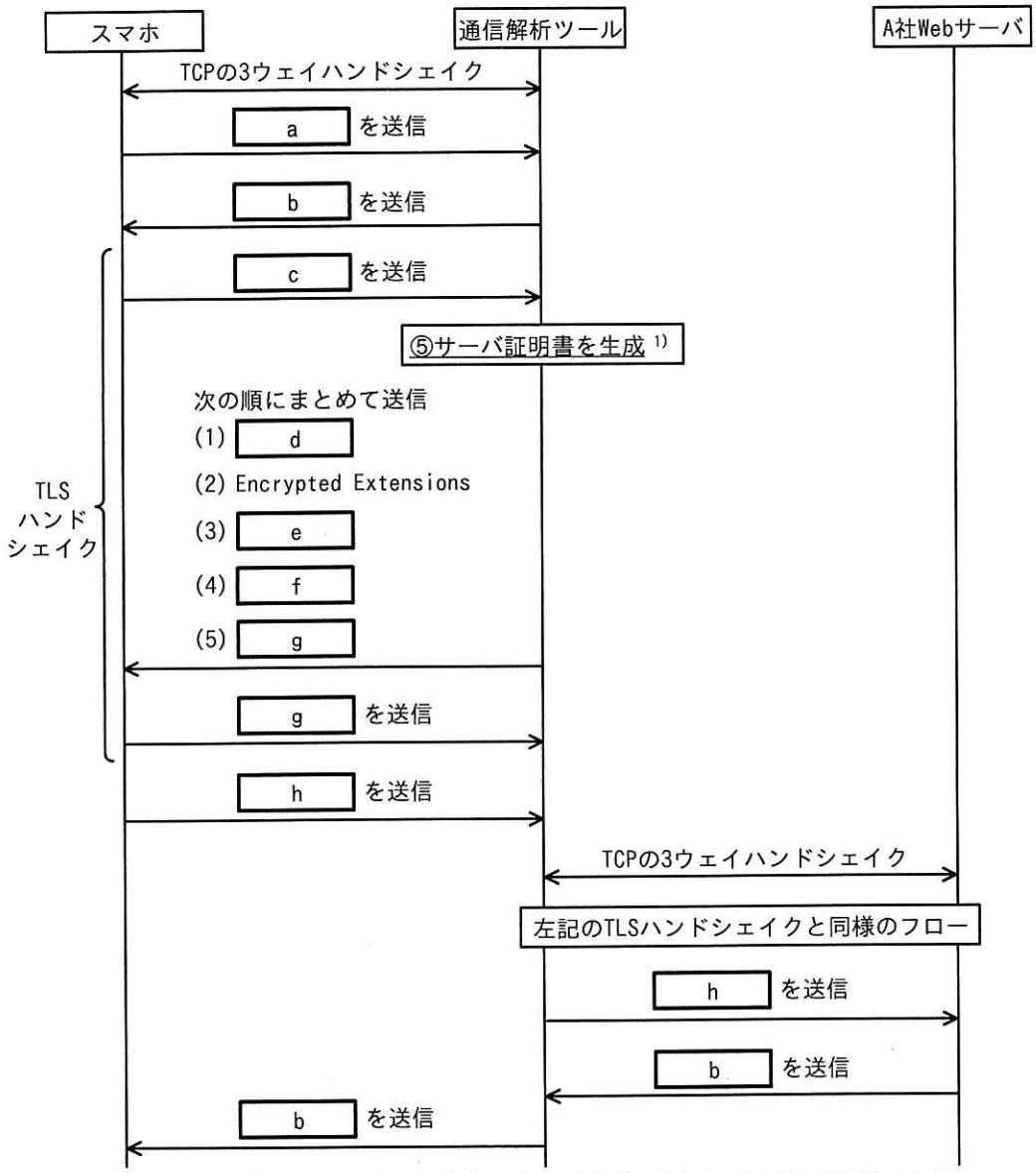
〔脆弱性1〕

Fアプリの開発チームに所属するUさんは，D社のSさんが開催する診断結果報告会に参加した。

Uさんは，脆弱性1が作り込まれた経緯を説明した。Uさんによると，FアプリとA社Webサーバとの間の通信内容に異常がないかどうかを調査するために，開発用PCで通信解析ツールを利用した。この通信解析ツールはプロキシサーバとして動作する。このツールを利用すると，Fアプリでは，サーバ証明書の検証エラーが発生し，FアプリとA社Webサーバとの間の通信が中断されてしまった。そこで，インターネット上のある記事でエラーが発生しても通信を続行する方法が紹介されていたのを

参考にして，F アプリのコードを変更したということであった。

この通信解析ツールを利用し，“https://www.a-sha.co.jp/campaign/□□□”にアクセスした際のレイヤー4～7 の通信フローの例を図 9 に示す。



注記　通信解析ツールのプライベート IP アドレスは，○○○.○○○.○○○.○○○とする。
注 1)　通信解析ツールは，自身のプライベート認証局機能を用いる。

図 9　通信解析ツールを利用した際の通信フローの例（抜粋）

U さんは，通信解析ツールを利用してテストを行う際も通信を正常に続行させる方

法をチーム内で話し合った。その結果，今後，開発用のスマホに⑥必要な設定を行うことにした。加えて，OS-αではテストを行う際だけその設定を有効化するように，Fアプリの中にも設定を追加した。

〔脆弱性2〕

脆弱性2への対応について，Sさんからは方式bを利用し，その際に署名付きURLの生成を図4中の［　i　］の時点で行ってはどうかとの提案があった。Uさんは Sさんの提案を了承した。

〔脆弱性3〕

次は，脆弱性3についてのUさんとSさんの会話である。

Uさん：対策として，図7の処理を修正します。

Sさん：図7の処理を修正すれば，認証トークンを盗まれるリスクは回避できます。しかし，Web ブラウザと比べると，⑦フィッシングサイトにアクセスしてしまっても気付くことができないというFアプリの仕様上の問題点が残ります。フィッシングサイトに気付くことができるようにするための機能か，そもそもフィッシングサイトにアクセスできないようにする機能が必要です。

Uさん：はい。図7の処理の修正に加えて，⑧フィッシングサイトにアクセスできないようにする機能を実装します。

A社は，検出された脆弱性を修正し，Eサービスの提供を開始した。

設問1　〔Fアプリの脆弱性診断結果〕について答えよ。

(1)　表1中の下線①について，アクセスキーを取得する方法を，具体的に答えよ。

(2)　表1中の下線②について，アクセスキーを取得する方法を，具体的に答えよ。

(3)　表1中の下線③について，ダウンロードする方法を，具体的に答えよ。

(4) 表 1 中の下線④について，攻撃者の Web サイトにアクセスさせることができるように細工した URL の例を，攻撃者が取得したドメイン名を k-sha.co.jp とした場合で答えよ。

設問２ 〔脆弱性 1〕について答えよ。

(1) 図 9 中の下線⑤について，サーバ証明書の Subject Alternative Name の値を，具体的に答えよ。

(2) 図 9 中の［ a ］～［ h ］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 Certificate

イ Certificate Verify

ウ Client Hello

エ CONNECT ○○○.○○○.○○○.○○○:443 HTTP/1.1

オ CONNECT www.a-sha.co.jp:443 HTTP/1.1

カ Finished

キ GET /campaign/□□□ HTTP/1.1

ク HTTP ステータスコード 101 (Switching Protocols)

ケ HTTP ステータスコード 200 (OK)

コ Server Hello

(3) 本文中の下線⑥について，設定の内容を，具体的に答えよ。

設問３ 本文中の［ i ］に入れる記号を，図 4 中の(あ)～(お)から選び，答えよ。

設問４ 〔脆弱性 3〕について答えよ。

(1) 本文中の下線⑦について，問題点を，20 字以内で答えよ。

(2) 本文中の下線⑧について，実装する機能を，具体的に答えよ。