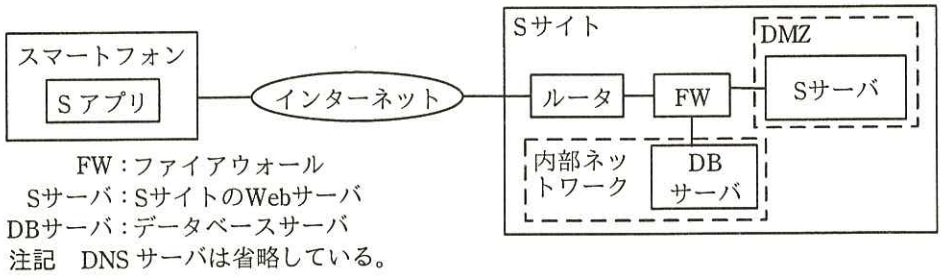
問3　スマートフォンアプリケーションの試験に関する次の記述を読んで，設問 1，2 に答えよ。

S 社は，従業員数 100 名の EC サービス会社である。今回，新たにショッピングサイト（以下，S サイトという）と S サイト専用のスマートフォンアプリケーション（以下，S アプリという）から構成されるシステム（以下，S システムという）の開発プロジェクトを立ち上げた。プロジェクトリーダには，サービス開発部の R さんが任命され，S システムのセキュリティについては，セキュリティ専門業者の A 氏の支援を受けることになった。

〔S システムの概要〕

S システムの構成を図 1 に，S アプリの機能概要を図 2 に示す。



FW：ファイアウォール
Sサーバ：SサイトのWebサーバ
DBサーバ：データベースサーバ
注記　DNS サーバは省略している。

図 1　S システムの構成

・S サーバとの間では HTTP over TLS（以下，HTTPS という）を使って通信を行う。
・S アプリ内に，S サーバの FQDN が組み込まれている。
・スマートフォンに対応している商用認証局から S サーバに対して発行されたサーバ証明書（以下，S サイト用サーバ証明書という）を，S サーバの認証に使用する。
・S サーバと通信ができなかった場合は通信エラー画面を表示し，S サーバを認証できなかった場合はサーバ認証エラー画面を表示する。

図 2　S アプリの機能概要（抜粋）

〔S アプリでのサーバ証明書の検証試験〕

開発がテスト工程に入り，R さんは，A 氏と共同で，S システムのセキュリティに関する試験を検討し，S サーバの認証を行うためのサーバ証明書の検証が S アプリで適切に行われていることの確認を試験に含めた。

Rさんは，図3に示すサーバ証明書の検証試験環境をS社内に設置し，スマートフォンからは無線 LAN 機能でこの検証試験環境に接続することにした。また，サーバ証明書の検証試験環境で用いる機器と設定を表 1 に，不正なサーバ証明書の検出についての試験項目を表2にまとめた。

なお，試験に使うサーバ証明書は，別に用意したプライベート認証局で発行する。

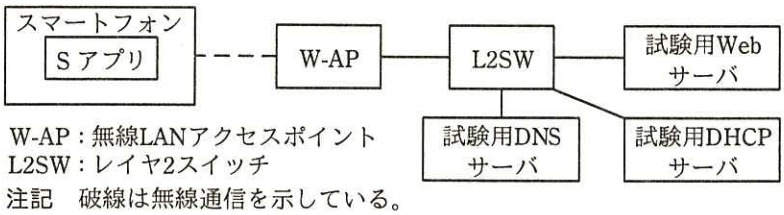


図3　サーバ証明書の検証試験環境

表1 サーバ証明書の検証試験環境で用いる機器と設定（抜粋）

機器名	設定
試験用 Web サーバ	試験用のサーバ証明書を登録する。
試験用 DNS サーバ	[a] の FQDN から [b] の IP アドレスに名前解決するための A レコードを設定する。
試験用 DHCP サーバ	スマートフォン自体の IP アドレス及びサブネットマスク，並びにスマートフォンが参照する DNS サーバの IP アドレスを割り当てる。

表2　不正なサーバ証明書の検出についての試験項目（抜粋）

項番	試験項目	試験方法	期待される結果
1	発行者が不正であることの検出	・試験用 Web サーバに次の値のサーバ証明書を登録する。 サブジェクトのコモンネーム：S サイト用サーバ証明書と同一の値 有効期間の開始と終了：S サイト用サーバ証明書と同一の値 ・スマートフォンにプライベート認証局のルート証明書を登録しない。	[d]
2	有効期間内でないことの検出	・試験用 Web サーバに次の値のサーバ証明書を登録する。 サブジェクトのコモンネーム：S サイト用サーバ証明書と同一の値 有効期間の開始：S サイト用サーバ証明書と同一の値 有効期間の終了：[c] ・スマートフォンにプライベート認証局のルート証明書を登録する。	[d]

表2　不正なサーバ証明書の検出についての試験項目（抜粋）（続き）

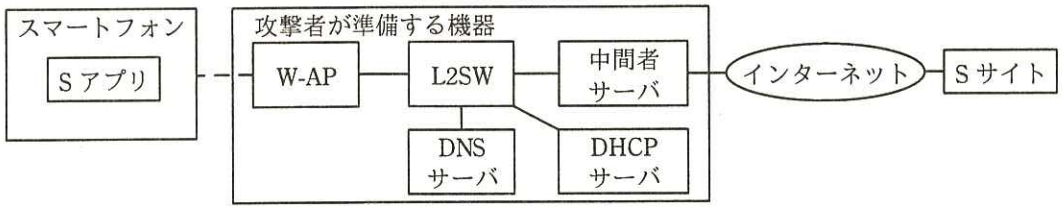
項番	試験項目	試験方法	期待される結果
3	サブジェクトのコモンネームが不正であることの検出	・試験用 Web サーバに次の値のサーバ証明書を登録する。 サブジェクトのコモンネーム：［a］の FQDN とは異なる値 有効期間の開始と終了：S サイト用サーバ証明書と同一の値 ・スマートフォンにプライベート認証局のルート証明書を登録する。	［d］

なお，S アプリと試験用 Web サーバ間で HTTPS 通信が確立することは，サーバ証明書の検証試験を実施する前に，試験用 Web サーバに S サイト用サーバ証明書を登録して確認している。

A 氏は，図 3，表 1 及び表 2 のレビューを行い，問題がないことを確認した。R さんが試験を実施した結果，S アプリでのサーバ証明書の検証に不備は見つからなかった。

〔S アプリでのサーバ証明書の検証不備による影響の検討〕

R さんは，S アプリでのサーバ証明書の検証に不備がある場合に，どのような攻撃が行われると影響を受けるのかを，A 氏に質問した。A 氏は，中間者攻撃に用いられる環境の例を図 4 に示した。



注記　破線は無線通信を示している。

図 4　中間者攻撃に用いられる環境の例

図 4 では，攻撃者が中間者サーバを含む機器を準備し，その先でインターネットを介して S サイトに接続している。中間者サーバは，S アプリとの間，及び S サイトとの間で，独立した二つの HTTPS 通信を確立し，中継する。

R さんは A 氏に，例えば，表 3 に示す攻撃者が準備するサーバ証明書のうち，ど

れを使用すると中間者攻撃が成功するのかを質問した。A氏は，もしSアプリにサーバ証明書の検証不備があると，表4のとおり攻撃が成功すると答えた。

表3　攻撃者が準備するサーバ証明書

証明書番号	発行者	サブジェクトのコモンネーム
1	スマートフォンに対応している商用認証局	攻撃者が所有しているドメインを使用したFQDN
2	攻撃者が準備するプライベート認証局	
3		Sサーバの FQDN
4		上記二つ以外の FQDN

表4　中間者攻撃が成功するサーバ証明書

項番	サーバ証明書の検証状況		中間者攻撃が成功するサーバ証明書
	発行者の検証不備	サブジェクトのコモンネームの検証不備	
1	あり	あり	e
2	あり	なし	f
3	なし	あり	g

A氏は，サーバ証明書の検証不備がある場合に，①Sアプリの利用者が，図4中のW-APに接続すると，中間者攻撃を受けることを説明した。説明を受けたRさんは，表2の試験において，Sアプリに不備が見つからなかったことから，中間者攻撃を受けた場合には利用者が気付くことができると判断した。

その後，残りの工程も完了し，S社ではSシステムを無事リリースした。

設問1　〔Sアプリでのサーバ証明書の検証試験〕について，(1)～(4)に答えよ。

(1) 表1中及び表2中の［ a ］に入れる適切な字句を，図1中又は図3中の構成要素から選び，答えよ。

(2) 表1中の［ b ］に入れる適切な字句を，図1中又は図3中の構成要素から選び，答えよ。

(3) 表2中の［ c ］に入れる適切な字句を，15字以内で答えよ。

(4) 表2の試験で，Sアプリが試験項目どおりに動作している場合に，どのような結果となるか。［ d ］に入れる適切な結果を，本文中又は図表中の字句を用いて，30字以内で具体的に述べよ。

設問2　〔Sアプリでのサーバ証明書の検証不備による影響の検討〕について，(1)，(2)に答えよ。

(1)　表4中の［　e　］～［　g　］に入れるサーバ証明書を，それぞれ表3中から全て選び，証明書番号で答えよ。

(2)　本文中の下線①について，攻撃者が，W-APの設定をどのように細工すると，Sアプリの利用者のうち，公衆無線LANの利用者のスマートフォンを自動的にW-APに接続させることができてしまうか。W-APの設定上の細工を45字以内で具体的に述べよ。