問1　スマートフォンを用いた決済に関する次の記述を読んで，設問1～3に答えよ。

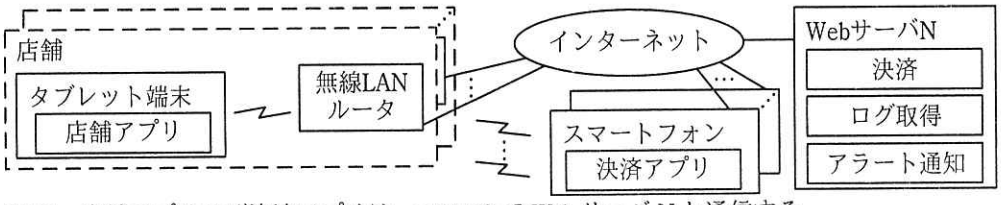
N社は，従業員数10,000名の飲食業者で，全国に500店舗を展開している。

N社では，会員番号をバーコードとして表示するスマートフォン用ポイントアプリケーションプログラム（以下，ポイントアプリという）を使って，ポイントサービスを提供している。店員がバーコードをバーコードリーダで読み取ることによってポイントが付与される仕組みである。

利用者の利便性向上のために，スマートフォンで決済を行う，N社独自のシステム（以下，Nシステムという）を開発することになった。

〔Nシステムの概要〕

Nシステムは，図1に示す構成であり，店舗で店員が利用するタブレット端末用店舗アプリケーションプログラム（以下，店舗アプリという），利用者が利用するスマートフォン用決済アプリケーションプログラム（以下，決済アプリという），及び決済，ログ取得，アラート通知などの機能をもつWebサーバNを用いて決済を実現する。



注記　店舗アプリ及び決済アプリは，HTTPSでWebサーバNと通信する。

図1　Nシステムの構成（概要）

決済アプリの機能の概要を表1に，WebサーバNの機能の概要を表2に，会員登録処理を表3に，決済処理を表4に示す。

表1　決済アプリの機能の概要（抜粋）

機能	概要
会員登録	利用者を会員登録する。ログインIDとして，メールアドレスを登録する。会員登録すると，決済アプリ用の会員番号が自動で発番される。また，パスワードなど他の情報の登録も行う。
ログイン	ログインIDとパスワードを入力して，ログインする。
決済	ポイントアプリの仕組みを利用し，16桁の会員番号をバーコードとして表示する。決済が完了すると，決済完了の画面が表示される。

表2　WebサーバNの機能の概要（抜粋）

機能	概要
決済	決済アプリ及び店舗アプリとのメッセージのやり取り，並びに決済を行う。
ログ取得	次の各種ログを取得する。 ・会員登録 ・ログイン ・決済アプリ及び店舗アプリの起動 ・決済アプリ及び店舗アプリでの決済
アラート通知	次のイベントが検知された場合は，Nシステムの管理者にアラートを通知する。 (i) 同一IPアドレスから，同一のログインIDでのログイン失敗が短時間に連続する。 (ii) 同一IPアドレスから，存在しないログインIDでのログイン試行が短時間に連続する。

表3　会員登録処理（抜粋）

記号	処理
1	利用者は，決済アプリにメールアドレスを入力する。
2-a	【入力されたメールアドレスが会員登録されていない場合】 WebサーバNは，入力されたメールアドレスに詳細登録ページのURLを電子メールで送信する。また，決済アプリは，“電子メールを送信しました。”と表示する。
2-b	【入力されたメールアドレスが会員登録されている場合】 決済アプリは，“既に使用されているメールアドレスです。”とエラー表示する。

表4　決済処理（抜粋）

記号	処理
1	利用者は，事前に決済アプリにログインしておく。
2	店員は，店舗アプリに金額を入力するとともに，利用者に金額を伝える。
3	利用者は，決済アプリにバーコードを表示する。
4	店員は，店舗アプリで，決済アプリに表示されたバーコードを読み取る。
5	バーコードが示す会員番号に対して決済する。
6	決済が完了すると，店舗アプリ及び決済アプリに決済完了が通知される。

各店舗では，決済時に利用者のスマートフォンが確実に通信できるように，Nシステム導入に合わせて，各店舗に導入済みの無線 LAN ルータをインターネットに接続し，利用者に無線LANサービスを提供する予定である。無線LANルータは全て同一の機種である。各店舗で管理者を決めて，管理者が手動で初期設定をしている。表 5 に無線LANルータの管理者機能の設定項目を示す。

表 5　無線LANルータの管理者機能の設定項目（抜粋）

記号	設定項目名	設定内容
あ	管理者機能のパスワード	各設定を変更するための管理者機能のパスワード
い	DNSプロキシ	無線LANルータが参照するDNSサーバのIPアドレス
う	DHCPサーバ	IPアドレス範囲，リース期間
え	パケットフィルタリング	インターネットとの間で送受信されるパケットを通過させるか，破棄するかのフィルタリングルール

Nシステムの開発チームに所属するXさんが検討したNシステムの仕様並びに店舗アプリ及び決済アプリの設計を，セキュリティの観点から情報処理安全確保支援士（登録セキスペ）のYさんがレビューした。レビューでのYさんの指摘を表6に示す。

表 6　Yさんの指摘

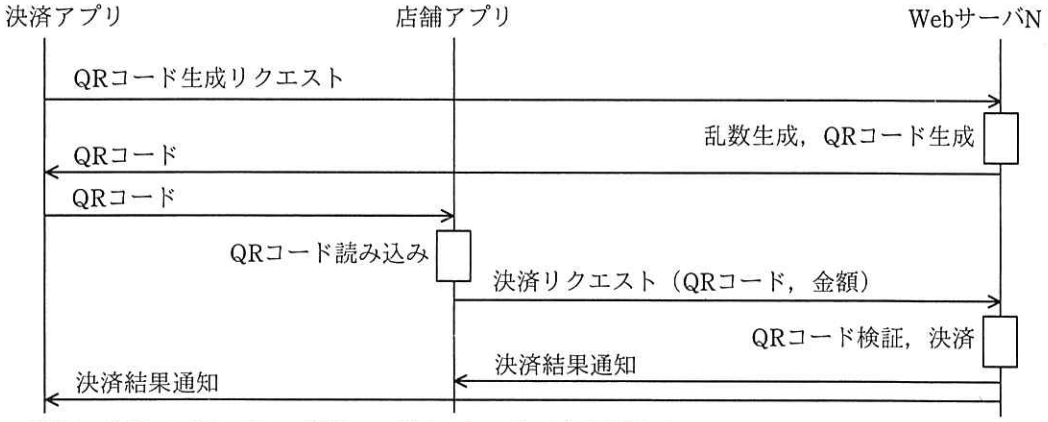
項番	指摘の内容
1	他者になりすまして決済できる。今までポイントアプリでは被害が発生していなかったが，ポイントアプリの仕組みを利用した決済アプリでは金銭を直接扱うので，リスクがより高い。
2	店舗の無線 LAN ルータには既知の脆弱（ぜい）性が存在する。その結果，インターネット側のインタフェースからはアクセスできない仕様のはずが，管理者機能のログイン画面にアクセスできてしまう。
3	管理者機能のパスワードが工場出荷時のパスワードから変更されていない可能性がある。変更されていないと，店舗の無線 LAN ルータに接続している利用者の端末から管理者機能にアクセスできる。
4	決済アプリ及び店舗アプリでのサーバ証明書の検証に不備がある。
5	決済アプリの会員登録機能は，攻撃者が悪用すると，当該機能の挙動からスクリーニング[1]ができてしまう。

注[1]　攻撃者が，攻撃者の手元にあるパスワードリストから無効なものを取り除くこと

Xさんは，指摘について対策を検討した。

〔項番 1 への対策〕

X さんは，表 6 中の項番 1 への対策として，メッセージ認証を用いることにした。具体的には，決済機能利用時に決済アプリに表示する情報として，会員番号，Web サーバ N で生成した乱数，時刻，及びそれら三つの情報を基に生成される HMAC（Hash-based Message Authentication Code）値を含めることにした。バーコードで扱える桁数を超えてしまうので，代わりに QR コードを表示することにした。HMAC 値を含む QR コードを用いた決済フローを図 2 に示す。QR コード生成及び QR コード検証の手順を図 3 に示す。



注記　決済アプリでは，事前にログインしておく必要がある。

図 2　HMAC 値を含む QR コードを用いた決済フロー

QR コード生成

1. Web サーバ N がもつ秘密鍵 K を用いて，会員番号，乱数，時刻を基にした HMAC 値 α を計算する。
2. 会員番号，乱数，時刻及び HMAC 値 α から成る QR コードを生成する。

QR コード検証

1. 秘密鍵 K を用いて，QR コード中の会員番号，乱数及び時刻を基にした HMAC 値 β を計算する。
2. [a]
3. 現在時刻が QR コード中の時刻から 5 分以内であること，及び同じ QR コードが過去に使われていないことを確認する。

図 3　QR コード生成及び QR コード検証の手順

〔項番 2～4 への対策〕

表 6 中の項番 2～4 の指摘を解決せずに無線 LAN サービスを提供し，①攻撃者が無線 LAN ルータの設定を変更すると，攻撃者が用意したサーバに利用者が接続しても気付かないおそれがある。

X さんは，項番 2 については，インターネットから管理者機能のログイン画面にアクセスされないようにするために，無線 LAN ルータのファームウェアを脆弱性が対策された最新のバージョンにアップデートしてもらうことにした。項番 3 については，管理者機能のパスワードを工場出荷時のパスワードから変更するように運用ルールを変更し，まだ変更していない場合は変更してもらうことにした。項番 4 については，サーバ証明書が図 4 に示す条件を満たしているかどうかを検証するように決済アプリ及び店舗アプリを改修した。

・サーバ証明書に [b] の dNSName があれば，アクセス先の Web サーバ N の [c] と合致し，サーバ証明書に [b] の dNSName がなければ，アクセス先の Web サーバ N の [c] が subject の [d] と合致すること
・有効期間内のサーバ証明書であること

図 4　サーバ証明書の検証条件（抜粋）

〔項番 5 への対策〕

攻撃者が，②事前にスクリーニングを実行したパスワードリストを用いて，パスワードリスト攻撃を行うと，Web サーバ N のアラート通知機能では検知されないおそれがある。そこで，X さんは，③表 3 の会員登録処理を修正することにし，さらに，パスワードリスト攻撃への追加対策として 2 段階認証を施し，アラート通知機能も見直すことにした。

N 社は，N システムの試行を幾つかの店舗で実施し，問題がないことを確認した。その後，N システムを全店舗に展開した。

設問１　〔項番１への対策〕について，(1)，(2)に答えよ。

(1)　どのような手段でなりすまして決済ができるのか。想定される手段を 30 字以内で具体的に述べよ。また，その攻撃が成功してしまう決済アプリにおける問題を 25 字以内で，具体的に述べよ。

(2)　図３中の［　a　］に入れる適切な字句を，30 字以内で述べよ。

設問２　〔項番２～４への対策〕について，(1)，(2)に答えよ。

(1)　本文中の下線①について，攻撃者はどの設定項目の内容をどのように変更するか。変更する設定項目を表５の中から選び，記号で答えよ。また，変更後の設定内容を 25 字以内で述べよ。

(2)　図４中の［　b　］～［　d　］に入れる適切な字句を，［　b　］，［　d　］については解答群の中から選び記号で，［　c　］については５字以内で，それぞれ答えよ。

解答群

ア	authorityKeyIdentifier	イ	commonName
ウ	issuer	エ	serialNumber
オ	subjectAltName	カ	subjectPublicKeyInfo

設問３　〔項番５への対策〕について，(1)，(2)に答えよ。

(1)　本文中の下線②について，N システムのどのような挙動を利用してスクリーニングを実行したと考えられるか。利用したと考えられる挙動を 40 字以内で具体的に述べよ。

(2)　本文中の下線③について，表３中の修正すべき処理を記号で答えよ。また，どのように修正すべきか。修正後の処理を，25 字以内で述べよ。