SC

令和２年度
情報処理安全確保支援士試験
午後Ⅰ　問題

試験時間	12:30 ～ 14:00（1 時間 30 分）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
4. 問題は，次の表に従って解答してください。

問題番号	問１～問３
選択方法	２問選択

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B 又は HB の黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に**受験番号**を，**生年月日欄**に**受験票の生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **選択した問題**については，次の例に従って，**選択欄**の**問題番号**を**○印**で囲んでください。○印がない場合は，採点されません。3 問とも○印で囲んだ場合は，はじめの 2 問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問１，問３を選択した場合の例〕

選択欄	
２問選択	(問１)
	問２
	(問３)

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

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。

現行システムの説明

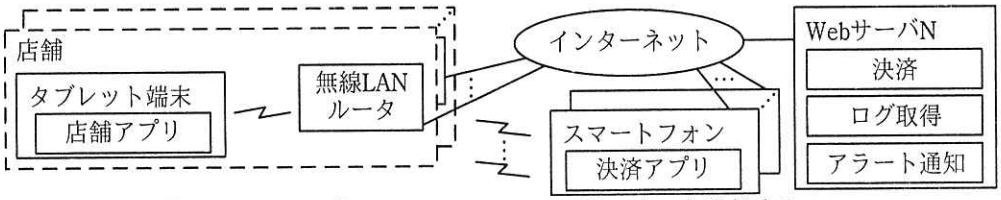
N社は，従業員数10,000名の飲食業者で，全国に500店舗を展開している。

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。

1.1

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。

3.1

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。

ここにテキストを

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。

2.1

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。

1.1

3.1

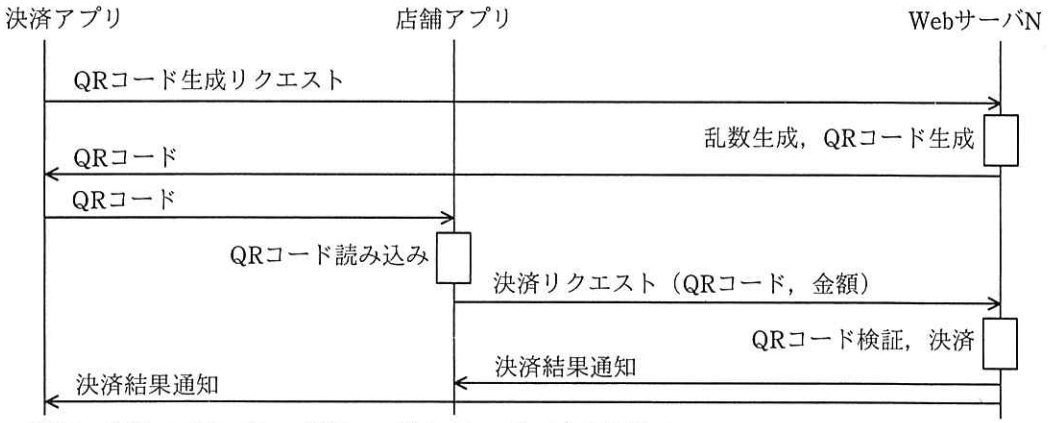
注[1]　攻撃者が，攻撃者の手元にあるパスワードリストから無効なものを取り除くこと

問題の懸念

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。1.2
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。

問2　電子メールのセキュリティ対策に関する次の記述を読んで，設問1～3に答えよ。

現行システムの説明

R社は，従業員数100名のシステム開発会社である。

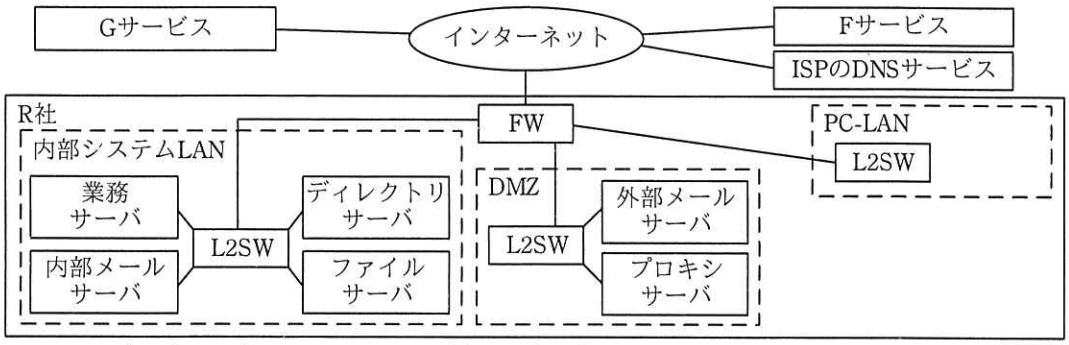
R社では，電子メール（以下，メールという）を利用している。メールアドレスのドメイン名には，r-sha.co.jp（以下，R社ドメイン名という）を使用している。R社では，委託先との設計ドキュメントファイルの交換に当たって，F社のファイル交換サービス（以下，Fサービスという）の利用を推進している。ただし，委託先が社内ルールで外部のファイル交換サービスの利用を禁止している場合は，設計ドキュメントファイルをパスワード付きZIPファイルにし，メールに添付して，メーリングリスト（以下，MLという）のメールアドレス宛てに送信している。ZIPファイルのパスワードは，平文のメールでMLのメールアドレス宛てに送信している。

MLには，G社のMLサービス（以下，Gサービスという）を利用している。MLのメールアドレスのドメイン名は，G社が取得したものである。MLのメールアドレスのローカル部は，プロジェクト名と委託先の会社名を組み合わせている。例えば，Bプロジェクトでの S社との交換では，MLのメールアドレスのローカル部は，*b-project_s-sha* にする。

Gサービスでは，メールをMLのメールアドレス宛てに送信すると，登録されたメンバ（以下，登録メンバという）のメールアドレス宛てに同報される。MLの登録メンバのメールアドレスの管理は，プロジェクトごとにR社のそれぞれのプロジェクト管理者が行う。各プロジェクト管理者は，自身が管理するプロジェクトのMLの登録メンバでもある。

〔R社の情報システム〕

R社の情報システムは，情報システム部が運用している。R社の情報システムのネットワーク構成を図1に示す。



FW：ファイアウォール　　L2SW：レイヤ2スイッチ
注記 1 PC-LAN に接続されている PC の記載は省略している。
注記 2 DMZ 内の各サーバには，グローバル IP アドレスを割り当てている。
注記 3 内部システム LAN 及び PC-LAN には，プライベート IP アドレスを割り当てている。

図 1　R 社の情報システムのネットワーク構成（抜粋）

内部システム LAN のサーバの機能概要を表 1 に示す。

表 1　内部システム LAN のサーバの機能概要（抜粋）

サーバ名	機能名	機能概要
内部メールサーバ	メール転送機能	・外部メールサーバとの間で，SMTP を用いてメールを転送する。
	メールボックス機能	・宛先メールアドレスのドメイン名が R 社ドメイン名であるメールをメールボックスに格納する。 ・POP3 を用いて，PC からメールボックス内のメールにアクセスできるようにする。
	メール受信機能	・SMTP を用いて，PC からメールを受信する。
ディレクトリサーバ	ディレクトリ機能	・X.500 モデルをサポートするディレクトリを管理し，当該ディレクトリへのアクセスを提供する。 ・ディレクトリへのアクセスは，標準で TCP ポートの 389 番を使用する［ a ］を用いる。 ・内部システム LAN のサーバでの認証に用いる。
	DNS 機能	・R 社内のサーバ及び PC のホスト名を管理する。

1.1

内部システム LAN のサーバではサーバ証明書を利用している。それらのサーバ証明書は，ネットワークに接続していない証明書発行専用機器上の R 社認証局（以下，R 社 CA という）で発行している。R 社 CA は情報システム部が運用している。

DMZ のサーバの機能概要を表 2 に示す。

表2　DMZ のサーバの機能概要（抜粋）

サーバ名	機能名	機能概要
外部メールサーバ	メール転送機能	・インターネットとの間で，SMTP を用いてメールを転送する。 ・内部メールサーバとの間で，SMTP を用いてメールを転送する。 ・SMTP over TLS にも対応している。
プロキシサーバ	プロキシ機能	・内部システム LAN 及び PC-LAN からインターネット上の Web サーバへのアクセスだけを中継する。

ISP の DNS サービスを，DNS キャッシュサーバ及び R 社ドメイン名の権威 DNS サーバとして利用している。

R 社では，従業員ごとに 1 台の PC を貸与している。各 PC には，R 社 CA のルート証明書を信頼できる発行元として登録している。

PC の Web ブラウザでは，HTTPS でアクセスする Web サーバのサーバ証明書が失効していないことを，RFC 6960 で規定されている [b] を利用して確認できるようにしている。

1.2

〔要望への対応〕

営業部と開発部から，委託先とのメール利用についての要望が情報システム部の D 部長に提出された。D 部長はその要望を基に，表 3 の要件をまとめた。

表3　委託先とのメール利用についての要件

項番	目的	要件
1	メールの暗号化	送信者から受信者まで暗号化された状態で，メールを送受信する。
2	送信者の検証	委託先とのやり取りのメールがなりすまされたものでないかどうかを確認できるように，送信者を検証する。

D 部長は，部下の E 主任と H さんに表 3 についての対応策の検討を指示した。

H さんは，メールの通信を暗号化することによって，表 3 の二つの要件に対応できるのではないかと E 主任に話した。

それに対して，E 主任は次の指摘をした。

2.1

・①メールの通信を暗号化しただけでは，表 3 の項番 1 を満たせない。

・攻撃者が委託先を装った [c] を用意するようななりすましは，送信元の [c] の真正性を確認して検出できる。一方，送信者メールアドレスとして

2.2

委託先のメールアドレスを使うようななりすましは検出できないので，表 3 の項番 2 を満たせない。

そこで，E 主任と H さんが他の対応策を調査したところ，S/MIME を利用すれば表 3 の要件を実現できることが分かった。E 主任と H さんは，S/MIME の利用を想定した次の方式を考えた。

（あ）R 社 CA で，S/MIME で利用する鍵ペアを生成し，S/MIME に利用可能なクライアント証明書（以下，S/MIME 証明書という）を発行する。

（い）S/MIME 証明書の失効情報を提供する機能をもつサーバ（以下，失効情報サーバという）を導入し，S/MIME 証明書の失効情報を登録する。

（う）S/MIME 証明書が失効していないことをメールクライアントから確認する。

（え）後でも参照する必要があるメールは，2.3 ②復号できなくなる場合に備えて，復号してファイルサーバに保存する。

〔S/MIME 利用に向けた課題と解決策〕

E 主任と H さんは，S/MIME の利用に向けて，解決すべき課題を次のとおりリストアップした。

（ア）R 社 CA のようなプライベート認証局のルート証明書を PC に登録することが，委託先によっては禁止されており，その場合，R 社の従業員が送信したメールの 3 [d] を [e] することができない。

（イ）委託先に事前に S/MIME 証明書を渡す必要があり，その方法を決める必要がある。

（ウ）ML 宛てのメールを暗号化できない。

E 主任と H さんは，（ア）～（ウ）それぞれの解決策を検討した。

（ア）については，認証局サービス事業者が発行する S/MIME 証明書であれば，委託先での R 社 CA のルート証明書を PC に登録しなくてもよいことが分かった。加えて，失効情報サーバの導入も不要であることが分かった。そこで，認証局サービス事業者が発行する S/MIME 証明書を利用することにした。

（イ）については，S/MIME 証明書を外部記憶媒体に保存して手渡す方法と，メー

ルで送信する方法を調査した。調査の結果，S/MIME を用いて［ d ］を付与したメールを送信すれば，受信者は S/MIME 証明書も受け取れるし，送信者が他者になりすましていないことも確認できることが分かり，便利でもあるので，メールで送信する方法にすることにした。

（ウ）については，表 3 の項番 1 を完全に満たすわけではないが，次の案を考えた。

（1）R 社のプロジェクト管理者は，あらかじめ，G サービスに［ f ］のメールアドレスの S/MIME 証明書を登録する。

（2）R 社のプロジェクト管理者は，あらかじめ，［ g ］のメールアドレスの S/MIME 証明書の発行手続を G 社に依頼する。

（3）メール送信者は，［ g ］のメールアドレスの S/MIME 証明書を使って暗号化したメールを送信する。

（4）G サービスは，メールを復号する。

（5）G サービスは，［ f ］のメールアドレスのそれぞれの S/MIME 証明書を使い，受信後にそれぞれが復号できるようにしてメールを暗号化する。

（6）G サービスは，暗号化したメールを送信する。

E 主任が G 社に確認したところ，この案には対応できないと回答があった。そこで，委託先との間で暗号化したメールを送信する場合は，ML を利用せずに委託先担当者の S/MIME 証明書で暗号化し，当該担当者のメールアドレスに送信することにした。

E 主任と H さんは，S/MIME の利用について，D 部長に報告した。D 部長は，S/MIME の利用を営業部長と開発部長に説明し，了承を得た。営業部経由で委託先に S/MIME の利用を打診したところ，S/MIME の利用の内諾が得られた。その後，必要な準備を行い，S/MIME を試行した。その結果，問題ないことが確認でき，S/MIME の利用が始まった。

設問1　〔R社の情報システム〕について，(1)，(2)に答えよ。

(1)　表1中の［　a　］に入れる適切なプロトコル名を，英字5字以内で答えよ。

(2)　本文中の［　b　］に入れる適切なプロトコル名を，英字5字以内で答えよ。

設問2　〔要望への対応〕について，(1)~(3)に答えよ。

(1)　本文中の下線①の理由を，35字以内で述べよ。

(2)　本文中の［　c　］に入れる適切な字句を，10字以内で答えよ。

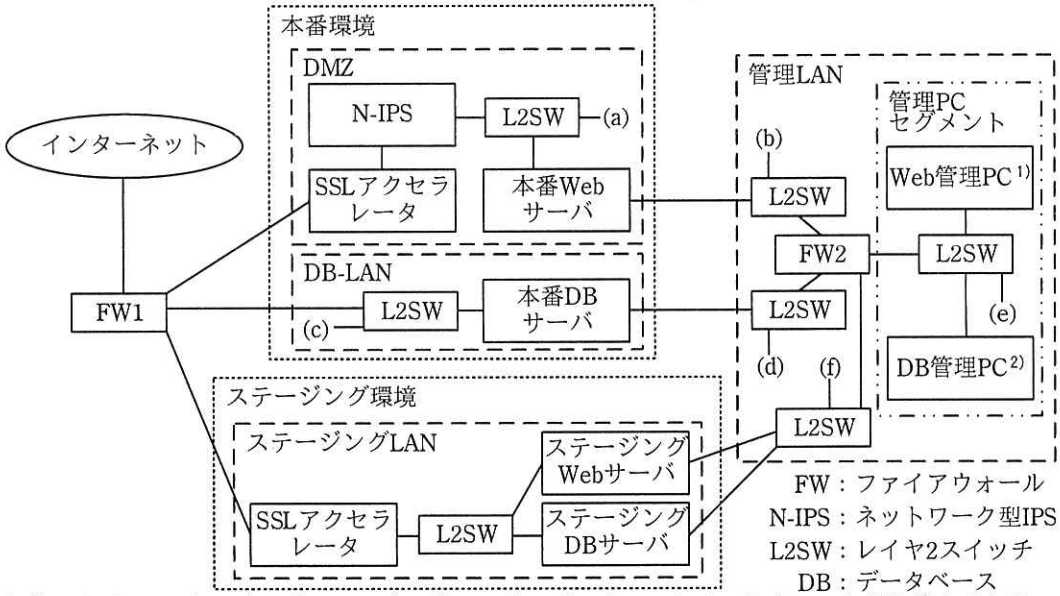
(3)　本文中の下線②について，復号できなくなるのはどのような場合か。25字以内で述べよ。

設問3　本文中の［　d　］～［　g　］に入れる適切な字句を，［　d　］，［　f　］は，それぞれ10字以内で，［　e　］，［　g　］は，それぞれ5字以内で答えよ。

問３　Web システムのセキュリティ診断に関する次の記述を読んで，設問 1，2 に答えよ。

現行システムの説明

L 社は，EC サイトを運営している従業員数 800 名の企業である。L 社のモールの会員は，モールで買物をすると，購入金額に応じて L 社が独自に発行するポイントが得られる。L 社のポイントサービス部が管理するポイントシステム（以下，P システムという）のネットワーク構成を図 1 に示す。



注 1)　本番 Web サーバ及びステージング Web サーバのリモートメンテナンスを行う端末である。

注 2)　本番 DB サーバ及びステージング DB サーバのリモートメンテナンスを行う端末である。このリモートメンテナンスは，DB 管理 PC からだけ行うよう運用ルールが定められている。

注記 1　DMZ から DB-LAN への通信は FW1 を経由する。

注記 2　本番 Web サーバ，本番 DB サーバ，ステージング Web サーバ，ステージング DB サーバはそれぞれ，サービス用と管理用の二つの NIC を備えている。

注記 3　ステージング環境は，主に新しいソフトウェアを本番環境に導入する際の動作確認に利用されている。保存されているデータはテスト用データである。

図 1　P システムのネットワーク構成（概要）

2.2

P システムが受信する 1 日の時間帯別の通信量の比率は，0 時～8 時が 2%，8 時～16 時が 55%，16 時～24 時が 43%である。P システムの機器は全て固定 IP アドレスで運用している。

P システムの機器の概要を表 1 に示す。

表1　P システムの機器の概要（抜粋）

機器名	概要
N-IPS	インターネットから本番 Web サーバへの通信，本番 Web サーバから DB-LAN への通信を監視している。遮断モードと検知モードの 2 種類のモードがあり，通信を脅威と判定したとき，遮断モードでは通信を拒否する。通信が脅威かどうかの判定では，通信ごとに，次の番号の小さい順に，最初に合致したルールが適用される。 1. ホワイトリスト判定：ホワイトリストに登録した IP アドレスからの通信は，脅威ではないと判定する。 2. 脅威通信判定：通信の内容を解析し，脅威レベルが高いと定義しているものは，脅威と判定する。 現在は，遮断モードに設定されており，ホワイトリスト判定と脅威通信判定が有効になっている。ホワイトリストには，現在，IP アドレスは一つも登録されていない。
本番 Web サーバ	会員が利用するポイント照会などの機能をもつ Web サーバである。本番 DB サーバにアクセスする。
本番 DB サーバ	会員のポイント情報や購入履歴などの情報をもつ DB サーバである。ホスト型 IPS が導入されている。本番 DB サーバで利用されているホスト型 IPS の概要を図 2 に示す。
FW1	ステートフルパケットインスペクション型の FW である。インターネットから本番 Web サーバ，本番 Web サーバから本番 DB サーバへの通信のうち必要なものだけを許可している。また，インターネットからステージング Web サーバへの通信は，普段は拒否しているが，ステージング環境利用時だけ必要なものを許可している。DB-LAN から DMZ 及びインターネットへの通信，並びに本番環境とステージング環境の間の通信を拒否している。
FW2	ステートフルパケットインスペクション型の FW である。管理 PC セグメントから，本番 Web サーバ，本番 DB サーバ，ステージング Web サーバ及びステージング DB サーバへの通信を許可し，それ以外の通信は全て拒否している。

通信ごとに，ホワイトリスト設定による判定が行われ，許可された通信は，侵入検知設定による判定が行われる。ホワイトリスト設定や侵入検知設定による判定で通信が拒否されると，ポイントサービス部運用グループの執務室内にある警告灯[1)]を点灯させる。

1. ホワイトリスト設定：登録された IP アドレスからの通信だけを許可し，それ以外を拒否する。ホワイトリストには，現在，本番 Web サーバと DB 管理 PC の IP アドレスだけが登録されている。
2. 侵入検知設定：ホストの通信を監視して，脅威と判定した通信を拒否し，それ以外を許可する。侵入検知設定は無効にもでき，無効にすると，ホストの通信を全て許可する。

注[1)]　警告灯が点灯すると，運用グループは，緊急対応体制をとり，最優先で対処を行う。

図2　ホスト型 IPS の概要

〔P システムの診断計画〕

EC サイトへの情報セキュリティ上の脅威の高まりを受け，L 社は，P システムの脆弱性診断を実施することを決定した。L 社のリスク管理部の T 主任と部下の U さんが，診断計画を策定する担当に任命された。T 主任は，図 3 に示す診断要件を基に診断計画を策定するよう U さんに指示した。

1. 本番環境への影響を最小化すること
2. 診断に当たってネットワーク構成，システム構成，設定及びデータを変更した場合は，診断終了後，診断前の状態に戻し，システムの正常な動作を確認すること

図 3　診断要件

U さんは，専門業者の診断サービスについて調査し，図 4 に示す調査結果を得た。

診断サービスでは，診断 PC で診断対象機器と通信し，レスポンスの内容を評価して脆弱性の有無を確認する。診断 PC は，既存の機器とは別の IP アドレスを設定し，インターネット又は内部のネットワークに接続する。次の 2 種類の診断方法がある。

・プラットフォーム診断（以下，PF 診断という）：サーバやネットワーク機器に対して，全てのポートをスキャンする。開いているポートを発見すると，そのポートを使って検査する。主に OS やミドルウェアの脆弱性を検出できる。
・Web アプリケーション診断（以下，Web 診断という）：Web アプリケーションプログラムを検査することによって，その脆弱性を検出できる。

図 4　診断サービスの調査結果

U さんは，調査結果を基に L 社で実施すべき脆弱性診断の検討に入った。Web 診断については，次のように実施することにした。

2.1 ・診断用の利用者 ID を作成する。その利用者に診断用のポイントを付与し，P システムにログインして診断する。
・ログイン無しでアクセスできるページも診断する。
・診断前の状態に戻せないようなデータの更新が発生する診断は実施しない。

PF 診断については，T 主任から助言を得ることにした。次は，本番 Web サーバがインターネットから攻撃される脅威を想定した時の，PF 診断に関する，U さんと T 主任の会話である。

Uさん： インターネットから診断する場合，調査した幾つかの事例によると，PF診断の実施時だけ，N-IPS の脅威通信判定を無効にすることがあるようです。有効なまま診断するケースと比べ，無効にすると，1.1 ①より多くの脆弱性を検出する可能性があります。

T主任： 無効にすると，PF診断実施時に本物の攻撃を防げないというリスクも生ずる。無効にするのではなく，1.2 ②N-IPS の設定を変更すれば，そのようなリスクは生じない。

Uさん： 分かりました。

T主任： それと，インターネットからの PF 診断の通信経路を考慮すると，インターネットからの PF 診断だけでなく，内部のネットワークからの PF 診断も実施すべきだ。

Uさん： 分かりました。その場合は，想定する脅威を踏まえると，診断 PC を図1中の接続点 1.3 [a] に接続して診断すれば良いでしょうか。

T主任： そのとおりだ。

U さんは T 主任のアドバイスを踏まえ，更に検討を進め，診断計画を表2のとおりにまとめた。

2.2 表2 診断計画（抜粋）

項目	内容
日時	○月×日から○月△日（10 営業日） 9 時～17 時（うち，診断時間は 1 日当たり連続した 5 時間程度）
診断対象	P システムの本番環境
診断内容	次の診断を順に行う。 診断 1：本番 Web サーバの脆弱性診断 攻撃者がインターネットから本番 Web サーバを攻撃し，本番 DB サーバの秘密情報を窃取する脅威を想定し，次の二つの診断を行う。 ・インターネットから，本番 Web サーバに PF 診断，Web 診断を行う。 ・図 1 中の接続点 [a] から，本番 Web サーバに PF 診断，Web 診断を行う。 診断 2：本番 DB サーバの脆弱性診断 1.3 攻撃者が何らかの方法で管理 LAN に侵入し，本番 DB サーバの秘密情報を窃取する脅威を想定し，次の診断を行う。 ・図 1 中の接続点(e)から，本番 DB サーバに PF 診断を行う。
検査項目	診断によってサービスダウンを引き起こす可能性がある項目を含め，使用する商用検査ツールに登録されている全ての検査項目の診断を行う。ただし，診断前の状態に戻せないようなデータの更新が発生する検査項目は除く。

〔P システムの診断計画レビュー〕

診断計画レビューにおいて T 主任は，診断の検査項目の内容は妥当であるとした上で，次の指摘を行った。

指摘 1： Web 診断は本番環境ではなく，ステージング環境で行うべきである。ステージング環境で実施する際，全ての診断の終了後に，担当者が，FW1 の設定を元に戻すこと，及びステージング環境の［ b ］を削除することを，明確に手順書に記載すること

指摘 2： PF 診断は本番環境で実施すべきだが，サーバが異常停止した場合の影響を最小化するために③計画の一部を変更すること

指摘 3： 診断 2 の実施に当たっては，警告灯が点灯することで社内に混乱が起きないよう，運用グループに④機器の設定の変更を依頼すること

その後，指摘 3 に従い，U さんは運用グループに診断計画を説明して設定の変更を依頼した。運用グループから，設定の変更については承諾を得られたが，診断計画について，診断 2 の診断 PC を接続するポイントを，図 1 の(e)から(d)に変更する必要があるという提案があった。

この提案について，運用グループから説明があった。運用グループによれば，最近配属された担当者が，Web 管理 PC から本番 DB サーバにログインを試みた。その結果，警告灯が点灯し，運用グループは緊急対応体制をとることになってしまった。その再発防止策の一つとして，FW2 のルールを修正し，［ c ］宛ての通信については，［ d ］からの通信だけを［ e ］することにした。その影響で，接続ポイントの変更が必要になるとのことだった。

U さんは T 主任の指摘及び運用グループからの提案を踏まえ，診断計画を確定し，診断実施に向けて準備を進めた。

設問1　〔P システムの診断計画〕について，(1)～(3)に答えよ。

(1) 本文中の下線①について，その理由を 35 字以内で述べよ。

(2) 本文中の下線②について，どのような設定変更をすべきか。設定変更の内容を 30 字以内で述べよ。

(3) 本文中及び表 2 中の［ a ］に入れる診断 PC の接続箇所を，図 1 中の接続点(a)～(f)の記号で答えよ。

設問2　〔P システムの診断計画レビュー〕について，(1)～(4)に答えよ。

(1) 本文中の［ b ］に入れる適切な字句を，15 字以内で具体的に答えよ。

(2) 本文中の下線③について，何をどのように変更すべきか。P システムの通信量に着目し，変更する項目を表 2 から選び答えよ。また，変更する内容を 20 字以内で述べよ。

(3) 本文中の下線④について，どの機器に対して，どのように設定を変更すべきか。機器は図 1 中から選び，変更後の設定は 55 字以内で具体的に述べよ。

(4) 本文中の［ c ］，［ d ］に入れる適切な字句を，図 1 中から選び答えよ。また，本文中の［ e ］に入れる適切な字句は，許可又は拒否のいずれか。答案用紙の“許可”，“拒否”のいずれかを○印で囲んで示せ。

6. 退室可能時間中に退室する場合は，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	13:10 ～ 13:50

7. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，次のものに限ります。

   なお，会場での貸出しは行っていません。

   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。
13. 午後Ⅱの試験開始は 14:30 ですので，14:10 までに着席してください。

試験問題に記載されている会社名又は製品名は，それぞれ各社又は各組織の商標又は登録商標です。
なお，試験問題では，™ 及び ® を明記していません。

©2020　独立行政法人情報処理推進機構