問2　Web サービスでの Web アプリケーションソフトウェア開発委託に関する次の記述を読んで，設問1～4に答えよ。

P 社は，従業員数 1,200 名の大学受験及び高校受験のための大手予備校である。先日開催した経営会議において，次年度から中学受験向けコースの事業部（以下，C 事業部という）を新たに立ち上げることが決まり，現在，開講に向けた準備作業を進めている。C 事業部は，教務部，営業部，総務部，マーケティング部の計 4 部で構成され，マーケティング部は，市場調査，広報活動，外部公開の Web サービスの企画，導入，運用などを担当している。

〔情報セキュリティ管理規程〕

P 社の情報セキュリティ管理規程では，次を規定している。

・情報セキュリティ委員会は，最高情報セキュリティ責任者（CISO）と各事業部の事業部長，各部の部長によって構成される。
・情報セキュリティ委員会は，P 社の情報セキュリティに関する意思決定を行う。
・上記の意思決定には，“暫定策を適用する際のリスク評価結果や残留リスクの承認”，“リスク評価結果などを踏まえた，新規事業又はサービスの開始の可否判断”などを含む。
・各部には，情報セキュリティの推進者として情報セキュリティリーダを配置する。

〔情報セキュリティの重点方針〕

現在，P 社の CISO は，情報セキュリティ活動を推進し情報を守ることと，情報を活用しビジネスを成長させることの両立が必要不可欠であると考えている。そこで，P 社の情報セキュリティの重点方針として，“個人情報の漏えい防止”と“Web サービスの継続性確保”の 2 点を定めて，情報セキュリティ委員会のメンバに通知している。

〔Web サービスの仕様〕

C 事業部のマーケティング部では，模擬試験の結果速報，成績推移などを，P 社の中学受験向けコースに通う児童（以下，児童という），及び児童の保護者（以下，保

護者という）が閲覧できるように，ログイン機能を有した Web サービス（以下，W サービスという）を Web アプリケーションソフトウェア（以下，Web アプリという）として開発し，提供することを検討している。マーケティング部の N さんは，W サービスの企画を担当している。図 1 は，N さんが作成した W サービスの仕様案である。

1. サービスメニューの概要
(1) 模擬試験の結果速報
(2) 成績推移
(3) 料金の自動引落し明細
2. 認証機能
(1) ログイン
　任意に設定できる英数字の利用者 ID と数字 4 桁の児童用パスワードを使用してログインする。
(2) アカウントロック
　5 回連続してログインに失敗すると，1 分間，アカウントをロックする。
(3) 保護者用パスワードによる追加ログイン
　料金の自動引落し明細メニューにアクセスするためには英数記号 8 文字以上の保護者用パスワードによる追加ログインを必要とする。
(4) ログアウト
　“ログアウト”ボタンをクリックするとログアウトする。“ログアウト”ボタンを押さない限り，ログインしたままとする。
(5) パスワードの表示
　児童用パスワードも保護者用パスワードも，パスワード入力内容の表示，非表示を切り替えられるようにする。初期状態は，非表示とする。

図 1　W サービスの仕様案（抜粋）

マーケティング部の情報セキュリティリーダである S 主任は，N さんが作成した W サービスの仕様案を情報セキュリティの観点からレビューした。

次は，S 主任と N さんとの会話である。

S 主任 ：模擬試験の結果などが児童本人及びその保護者以外に閲覧されるリスク（以下，閲覧リスクという）を減らすために，W サービスはログイン機能を実装することになっていたね。

N さん：はい。児童でも覚えやすい数字 4 桁のパスワードを用いる仕様です。

S 主任 ：料金の自動引落し明細メニューのログインについても教えてくれないか。

Nさん：こちらは，保護者がアクセスします。児童が閲覧する必要はないことから，英数記号 8 文字以上の保護者用パスワードで追加ログインする仕様です。また，パスワードの入力間違いを減らすために，保護者がパスワード入力内容を表示に切り替えて，入力内容を確認することができます。

S主任：よく分かった。この仕様案では，ブルートフォース攻撃のリスクが大きいね。また，児童の場合，自分専用の PC をもっているケースは少ないと思うよ。図書館，学校などの共用 PC を利用することが多く，そこでログアウトを忘れることもあるので，閲覧リスクが大きいね。

S主任は，レビュー後に，次の2点の変更，追加をNさんに指示した。

・①ブルートフォース攻撃のリスクを低減するために認証機能の仕様を変更する。

・②共用 PC における閲覧リスクを低減するために機能を追加する。

〔委託仕様書の検討〕

近年，Web アプリの脆弱性を悪用した攻撃が増えている。脆弱性の代表的な例としては，SQL インジェクションやクロスサイトスクリプティングが知られている。

S 主任は，Web アプリの開発を外部に委託するに当たり，情報システム部の U 課長に相談し，委託仕様書は IPA が公開している“ウェブ健康診断仕様”を参考にすることにした。また，検収の際はセキュリティ専門会社の Y 社に脆弱性診断を依頼することにした。“ウェブ健康診断仕様”とは，元々は地方公共団体が運営する Web サイトの基本的な対策状況を診断するための仕様であり，低コストで診断できるように，必要かつ最小限の診断項目，検査パターンを採用している。したがって，Web アプリの一般的な脆弱性診断サービスと比較すると簡素な診断項目となっている。

“ウェブ健康診断仕様”の診断項目を表1に示す。

表1　“ウェブ健康診断仕様”の診断項目（抜粋）

項番	診断項目（脆弱性名など）	危険度	受動的攻撃[1]／能動的攻撃[2]	攻撃によって影響を受ける特性[3]		
				機密性	完全性	可用性
1	SQL インジェクション	高	a1	○	○	○
2	クロスサイトスクリプティング	中	a2	○	○	
3	クロスサイトリクエストフォージェリ	中	受動的	○	○	○
4	OS コマンドインジェクション	高	能動的	○	○	○
5	意図しないリダイレクト	中	受動的	○		
6	HTTP ヘッダインジェクション	中	受動的	○	○	
7	b	低～中	能動的			○

注記　本表は，P 社の情報セキュリティ委員会が“ウェブ健康診断仕様”の内容，表現を自社向けに一部変更したものである。

注[1]　脆弱性を悪用する攻撃の成功には，攻撃者の用意した不正なリンクをクリックするなどの被害者の操作が必要である。

注[2]　脆弱性を悪用する攻撃の成功には，被害者の操作なしに，攻撃者が Web アプリに対して攻撃するだけでよい。

注[3]　○は影響を受けることを示す。

S 主任は，表 1 を基に対処の必要な脆弱性を委託仕様書に列挙した。また，③情報セキュリティを向上させる上で有効かつ適切な他の事項についても，委託仕様書に盛り込み，情報システム部のレビューを受けてから，開発会社の Z 社に Web アプリの開発を委託した。

〔脆弱性診断結果〕

3 か月後，S 主任は，Z 社が開発した Web アプリの検収に当たって，Y 社に脆弱性診断を依頼した。Y 社の脆弱性診断では，情報処理安全確保支援士が，“ウェブ健康診断仕様”に比べて診断項目が多い詳細な診断を実施する。

Y 社の診断での“危険度基準”を表 2 に，“総合判定基準”を表 3 に示す。

表2　危険度基準

危険度	内容
高	能動的攻撃が成功する可能性が高く，機密性や完全性の被害につながりやすい脆弱性がある。
中	受動的攻撃が成功する可能性が高い脆弱性がある。 又は，機密性や完全性の被害にはつながりにくいものの，能動的攻撃が成功する可能性が高い脆弱性がある。
低	攻撃成功の可能性が低い脆弱性がある。 又は，攻撃が成功しても被害が軽微であると考えられる脆弱性がある。

注記　本表は，“ウェブ健康診断仕様”を基に，Y社が脆弱性診断の評価基準として作成した。

表3　総合判定基準

総合判定所見	説明
要治療・精密検査（優先度：高）	危険度が“高”の脆弱性が検出された。直ちに Web アプリの改修などの措置を講じる必要がある。
要治療・精密検査（優先度：通常）	危険度が“中”の脆弱性が検出された。Web アプリの改修などの措置を講じる必要がある。
差し支えない	危険度が“低”の脆弱性が検出された。Web アプリの改修などの措置を講じることが望ましい。
異常検出なし	脆弱性は検出されなかった。

注記　本表は，“ウェブ健康診断仕様”を基に，Y社が脆弱性診断の評価基準として作成した。

Y社が Web アプリの脆弱性診断を行ったところ，［　c　］検出されたので，総合判定所見は，“要治療・精密検査（優先度：高）”であった。

次は，診断報告会でのS主任とY社の診断担当T氏との会話である。

S主任：脆弱性診断で脆弱性が検出された場合，Web アプリを改修する以外の代替手段はあるのですか。

T氏　：WAF を導入することによって，パラメタ操作による攻撃などを防御することができます。ただし，認証やセッション管理の不備を悪用する攻撃の中には，防御できない攻撃もあるので，WAF は，Web アプリに対する攻撃によるリスクを低減するための対策と考えてください。

S主任：なるほど，対策として不十分なので，Web アプリを改修するよりも残留リスクが大きくなるのですね。それでは，Web アプリを改修する場合であれば，WAF の導入は不要ですか。

T氏　：いいえ，そうとも限りません。Webアプリの改修が完了するまでの間，Webサービスを停止する代わりに，④WAF を暫定策として活用することも可能です。

S主任：分かりました。Webアプリの情報セキュリティ対策では他にも注意すべきことはありますか。

T氏　：Webアプリの脆弱性を突く攻撃とは別に，パスワードリスト攻撃のような利用者側の管理面の脆弱性を突く攻撃が，最近，増えています。

S主任は，今回の脆弱性診断で検出された脆弱性については，Z社に対してWebアプリの改修を求めることにした。また，パスワードリスト攻撃については，⑤児童や保護者に対する注意喚起を行うために，児童にも分かりやすい情報セキュリティのしおりを作成し，配布することにした。

Z社は，Webアプリを改修した上でP社に納品した。数日後，S主任は，Wサービス開始に向けて情報セキュリティ委員会に報告した。

〔Wサービス開始とその後〕

情報セキュリティ委員会には，脆弱性診断結果と，その後のWebアプリの改修対応が報告され，Wサービス開始に向けて問題ないと判断された。情報セキュリティ委員会の終了後，S主任は，情報システム部に対して，Wサービス提供開始後に新たな脆弱性が発見される可能性，及び，⑥P社の情報セキュリティの重点方針を実現する上でWAF導入によって期待できるメリットを説明した。情報システム部は，WAFを導入することを決定し，その後，C事業部のWサービスは，予定どおりサービス提供を開始した。

Wサービスの提供開始から数か月後，S主任は，Z社に対して，⑦パスワードリスト攻撃などによる不正ログインの発生状況に利用者側でも気付くための機能などの追加を依頼した。

その結果，P社はWサービスをより安全に提供することができるようになった。

設問1　〔Webサービスの仕様〕について，(1)，(2)に答えよ。

(1)　本文中の下線①の仕様変更について，Wサービスの仕様案よりもリスクを低減できる変更内容を，解答群の中から二つ選べ。

解答群

ア　児童用パスワード及び保護者用パスワードの入力内容を，常に非表示にするように変更する。

イ　児童用パスワードを，数字4桁から英数記号8文字以上に変更する。

ウ　保護者用パスワードを，英数記号8文字以上から数字9桁に変更する。

エ　ログイン失敗回数によるアカウントロックのしきい値を，5回から8回に変更する。

オ　ログイン失敗時のアカウントロック時間を，1分間から60分間に変更する。

(2)　本文中の下線②について，追加すべき機能はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　アカウントロックを利用者が自ら解除できる機能の追加

イ　定期的なパスワード変更を利用者に促すメッセージ機能の追加

ウ　パスワード強度をチェックする機能の追加

エ　パスワードを忘れた際に使う利用者への“秘密の質問”機能の追加

オ　マルウェア検知機能の追加

カ　ログイン状態をタイムアウトさせる機能の追加

設問2　〔委託仕様書の検討〕について，(1) ～ (3) に答えよ。

(1)　表 1 中の［ a1 ］，［ a2 ］に入れる字句はどれか。a に関する解答群のうち，最も適切なものを選べ。

a に関する解答群

	a1	a2
ア	受動的	受動的
イ	受動的	能動的
ウ	能動的	受動的
エ	能動的	能動的

(2)　表 1 中の［ b ］に入れる字句を，解答群の中から選べ。

b に関する解答群

ア　クローラへの耐性

イ　セッション管理の不備

ウ　ディレクトリトラバーサル

エ　ディレクトリリスティング

オ　認可制御の不備，欠落

(3) 本文中の下線 ③ について，次の (i) ～ (v) のうち，有効かつ適切な事項だけを全て挙げた組合せを，解答群の中から選べ。

(i) 開発を進めていくうちに，追加のセキュリティ対策が必要なものが発生した場合，委託元に提案すること

(ii) 再委託先も含めたセキュアな開発体制を，委託元に説明すること

(iii) 脆弱性観点からのセキュリティ試験結果を，委託元に成果物として納品すること

(iv) 他社のセキュリティ開発案件で顧客から受領した委託仕様書を，委託元に開示すること

(v) 納品後のセキュリティに関するサポート方法と費用負担を，委託元に説明すること

解答群

ア (i), (ii), (iii), (iv)

イ (i), (ii), (iii), (iv), (v)

ウ (i), (ii), (iii), (v)

エ (i), (ii), (iv), (v)

オ (i), (ii), (v)

カ (i), (iii), (iv), (v)

キ (i), (iv), (v)

ク (ii), (iii), (iv)

ケ (ii), (iii), (iv), (v)

コ (iii), (iv), (v)

設問3　〔脆弱性診断結果〕について，(1)～(3)に答えよ。

(1)　本文中の［　c　］に入れる字句はどれか。解答群のうち，最も適切なものを選べ。

cに関する解答群

ア　“HTTPヘッダインジェクション”の脆弱性が，1件

イ　“OSコマンドインジェクション”の脆弱性が，1件

ウ　“クロスサイトリクエストフォージェリ”の脆弱性が，1件

エ　“クロスサイトリクエストフォージェリ”の脆弱性と“意図しないリダイレクト”の脆弱性が，それぞれ1件

オ　攻撃が成功しても被害が軽微であると考えられる脆弱性が，3件

カ　攻撃成功の可能性が低い脆弱性が，1件

(2)　本文中の下線④について，P社の情報セキュリティ管理規程と照らし合わせると，どのような対応が必要になるか。解答群のうち，最も適切なものを選べ。

解答群

ア　C事業部の営業部による，Wサービスを停止させるかどうかという業務観点からの判断

イ　WAF提供元による，リスク回避の観点からのWAF設定などの技術的なアドバイス

ウ　情報セキュリティ委員会による，リスク対応の観点からの承認

エ　使いやすさや画面の見やすさの観点からの児童の意見の聴取

オ　保護者による，個人の権利利益保護の観点からの同意

(3) 本文中の下線⑤について，注意喚起すべき内容はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア 他のWebサイトと同じ利用者IDとパスワードを使わないこと

イ パスワードを定期的に変更すること

ウ パスワードを変更した直後に再変更はしないこと

エ パスワードを忘れた場合に備えて，周りの友達とパスワードを共用すること

オ パスワードを忘れないように，パスワードをメモして安全な場所に保管すること

カ 利用できる全ての文字種を組み合わせ，可能な限り複雑なパスワードを設定すること

設問4 〔Wサービス開始とその後〕について，(1)，(2)に答えよ。

(1) 本文中の下線⑥のメリットはどれか。解答群のうち，最も適切なものを選べ。

解答群

ア Webアプリ改修期間中のサービス中断を回避することができる。

イ Webアプリの改修を一切不要にすることができる。

ウ 保護者などに対外的なアピールをすることができる。

エ マルウェアによる個人情報の漏えいを防止することができる。

オ レスポンスを向上させることができる。

(2) 本文中の下線⑦について，追加すべき機能はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア 2要素認証

イ 休眠アカウントの無効化

ウ 推測可能なパスワードの設定禁止

エ 特定のIPアドレスからの通信遮断

オ 認証エラーに対するアカウントロック

カ パスワードの有効期間設定

キ パスワード履歴保存と現在と同じパスワードの再設定禁止

ク 普段と異なるIPアドレスからの通信遮断

ケ ログイン履歴の表示