情報処理安全確保支援士試験

科目 B のサンプル問題

情報処理安全確保支援士試験の科目 B は，次の出題構成を予定しています。
・1 問 1 答（1 設問）の問題を，計 8 問出題
・1 問 3 答（3 設問，全ての設問が必須解答）の問題を，計 4 問出題

1 問 1 答のサンプル問題

問 1　A 社は住宅設備機器の設計販売を行う従業員 2,000 名の上場企業である。内部監査で，情報資産が適切に把握できておらず情報セキュリティリスクのアセスメントが困難との指摘があり，表 1 の記載項目をもつ情報資産台帳を，総務部が整備することになった。

表 1　A 社の情報資産台帳の記載項目（抜粋）

項目名	説明
情報資産名	情報資産の名称を記載する。
情報資産の内容	情報資産の内容を簡潔に記載する。
利用部署	情報資産を利用可能な部署名を記載する。
管理部署	情報資産を管理する部署名を記載する。
機密性の評価値	評価値を 0～2 の 3 段階で記載する。 評価値 2：漏えいすると事業に深刻な影響がある。 評価値 1：漏えいすると事業に影響がある。 評価値 0：漏えいしても事業にほとんど影響がない。
完全性の評価値	評価値を 0～2 の 3 段階で記載する。 （省略）
可用性の評価値	評価値を 0～2 の 3 段階で記載する。 （省略）
重要度	情報資産の機密性，完全性，可用性の評価値の最大値を，その情報資産の重要度として記載する。
保存期限	法定文書は定められた保存期限を記載する。それ以外の文書は利用できる期限を記載する。

注記　管理方法や機密性，完全性，可用性の評価値が全て同じ情報資産は一つの情報資産としてまとめて記載してもよい。

情報セキュリティ部に所属し，情報処理安全確保支援士（登録セキスペ）でもある B さんは，各部署に情報資産台帳を作成するように依頼したところ，経理部の担当者から表 2 の質問を受けた。

表 2　経理部担当者からの質問

項番	質問内容
1	投資家に開示済の過年度の決算短信資料と，作成中の決算短信資料を一つの情報資産としてまとめて記載してもよいか。
2	情報システム部が管理するファイルサーバに債権管理情報を保存しているが，債権管理情報の管理部署にはどの部署を記載すればよいか。
3	情報資産の機密性，完全性，可用性の評価値が，それぞれ，0，1，2 の場合の重要度はどのようにすればよいか。

設問　表 2 の項番 1 から 3 の質問に対する B さんの回答の組合せはどれか。解答群のうち，最も適切なものを選べ。

解答群

	項番 1 への回答	項番 2 への回答	項番 3 への回答
ア	してもよい	経理部	2
イ	してもよい	経理部	0
ウ	してもよい	情報システム部	2
エ	してもよい	情報システム部	0
オ	してはいけない	経理部	2
カ	してはいけない	経理部	0
キ	してはいけない	情報システム部	2
ク	してはいけない	情報システム部	0

1問3答のサンプル問題

問２　B 社は，セキュリティ診断サービスを提供している会社である。このたび，転職支援サービスを提供している M 社から，転職支援 Web サイト（以下，M サイトという）のセキュリティ診断を受注した。

M サイトを利用する求職者は，氏名，自宅住所，電話番号，勤務先などの求職者属性情報と，希望職種，希望条件などの求職情報を入力する。求人企業は，会社情報，求人情報，求人担当者の氏名，所属部署などの情報を入力する。

M サイトは，機能を追加した新しいバージョンの Web アプリケーションプログラム（以下，M サイトの Web アプリケーションプログラムを Web アプリという）の開発が完了したところであり，リリース前である。

〔セキュリティ診断の診断対象と診断方法〕

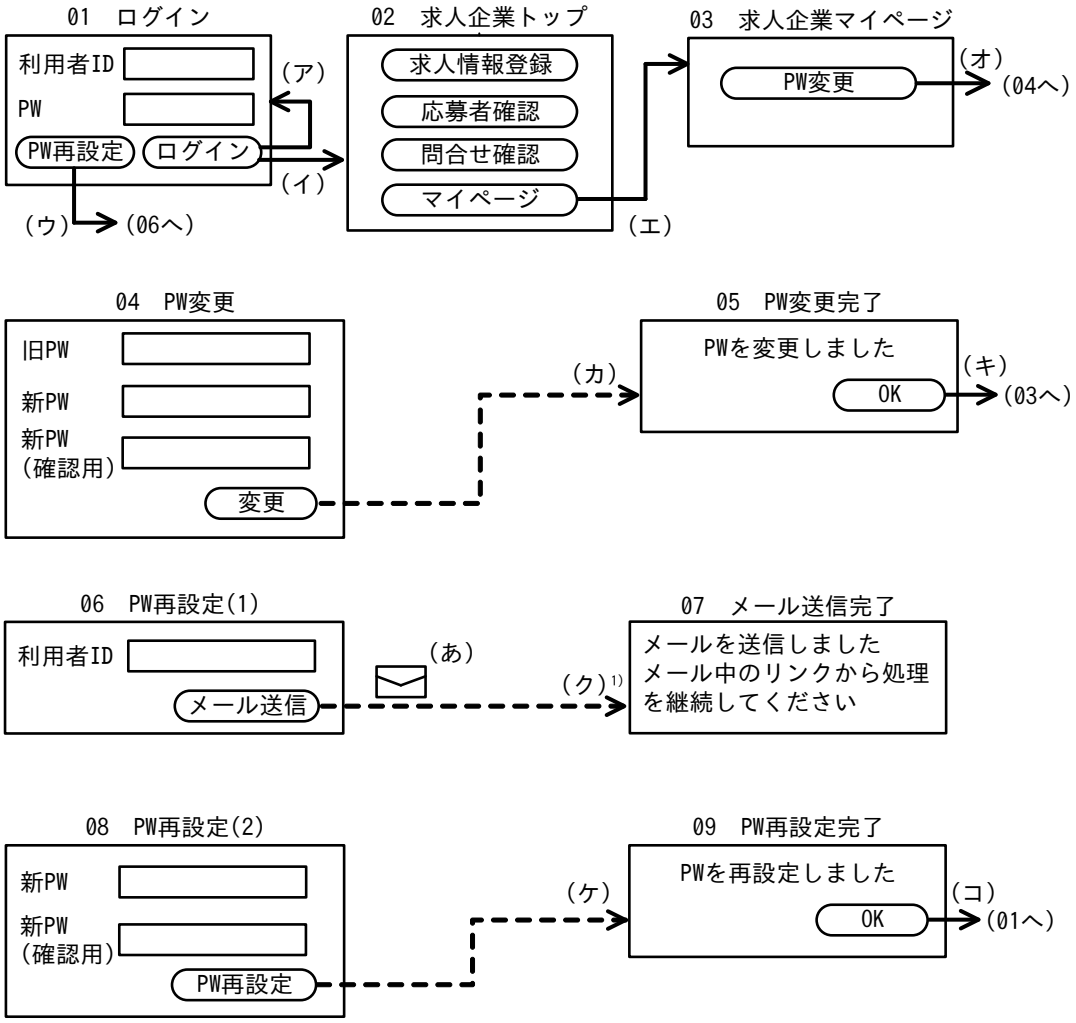
今回のセキュリティ診断の診断対象と診断方法は，図 1 のとおりである。

【診断対象】
・M サイトには本番用サイトと検証用サイトがあり，診断対象は M サイトの検証用サイトとする。検証用サイトには，開発が完了した新しいバージョンの Web アプリが導入されている。なお，本番用サイトと検証用サイトは，同一の構成である。
・検証用サイトでは，アクセス元の IP アドレスを制限している。診断に当たり，B 社からも検証用サイトにアクセスできるように，検証用サイトの設定を変更する。
・検証用サイトには，テスト用疑似データが投入されている。

【診断方法】
・B 社の社内にある診断用 PC からインターネットを経由して診断を行う。
・Web アプリの脆弱(ぜい)性の検出を行う。
・Web アプリの脆弱性の検出は，診断ツールと診断員の手作業で行う。
・診断に当たり，必要に応じて M サイトの設計書を参照する。

図 1　診断対象と診断方法

診断の際に参照した，M サイトの設計書中の画面遷移図を図 2 に，各画面の URL を表 1 に示す。



PW：パスワード　　メール：電子メール　　：メール

：クロスサイトリクエストフォージェリ（CSRF）対策が施されていない画面遷移

：CSRF対策が施された画面遷移

注記 1 ログインしていない状態で，02～05 の画面にアクセスした場合，エラー画面が表示される。

注記 2 設問に関係しない画面，ボタン及び画面遷移は省略している。

注 1)　画面遷移の際，M サイトから，登録しているメールアドレスに，PW 再設定用 URL が記載されたメール(あ)を送信する。利用者がメール(あ)に記載された PW 再設定用 URL にアクセスすると，画面 08 を表示する。

図 2　画面遷移図（抜粋）

表 1　各画面の URL

画面番号	URL
01, 02	https://test.△△△.jp/
03	https://test.△△△.jp/mypage
04, 05	https://test.△△△.jp/pwchange
06, 07	https://test.△△△.jp/pwreset
08, 09	https://test.△△△.jp/pwreset/x [1)]

注 [1)]　x は，PW 再設定を行う都度生成されるランダムな英数字 32 字の文字列である。

〔セキュリティ診断報告書〕

B 社は，セキュリティ診断を実施し，図 3 の診断報告書を作成した。

診断報告書

1 章　診断結果概要

（省略）

2 章　Web アプリケーションプログラムの診断結果

2.1　検出した脆弱性の概要

検出した脆弱性は，表 A のとおりである。

表 A　検出した Web アプリケーションプログラムの脆弱性の一覧

項番	重要度	脆弱性の種類	検出箇所
1	（省略）	セッションフィクセーション	画面遷移 a1
2	（省略）	メールヘッダーインジェクション	（省略）
3	（省略）	HTTP ヘッダーの不備	全ての画面遷移

2.2　検出した脆弱性の説明

2.2.1 セッションフィクセーション

(1) 脆弱性の内容

M サイトでは form 内の hidden フィールドである sessionID の値だけでセッション管理を実施していた。しかし，表 B のいずれの画面遷移においても，HTTP レスポンス中の sessionID の値が同一であった。

図 3　診断報告書

表 B　セッションフィクセーション脆弱性の確認

画面遷移	HTTP レスポンス中の sessionID
Web ブラウザに直接 URL を入力して，画面 01 を表示したとき	<input type="hidden" id="sessionID" name="sessionID" value="764b2ac2-0452-49e4-92a7-0914fa005011">
画面遷移(ア)	<input type="hidden" id="sessionID" name="sessionID" value="764b2ac2-0452-49e4-92a7-0914fa005011">
画面遷移(イ)	<input type="hidden" id="sessionID" name="sessionID" value="764b2ac2-0452-49e4-92a7-0914fa005011">
画面遷移(エ)	<input type="hidden" id="sessionID" name="sessionID" value="764b2ac2-0452-49e4-92a7-0914fa005011">

攻撃者が図 A の手順でこの脆弱性を悪用すると，M サイトに不正にログインすることができる。

手順 1：求人企業への問合せ先として登録したメールアドレスを，何らかの方法で入手する。
手順 2：URL “ a2 ” にアクセスして，sessionID を入手する。
手順 3：次の二つの要素を含む HTML を作成する。
- 手順 2 で入手した sessionID を記述したフォーム
- 当該 HTML が Web ブラウザに読み込まれた直後に，上記のフォームを URL “ a2 ” に POST メソッドで送信するスクリプト

手順 4：手順 3 で作成した HTML を，罠(わな)サイトに置く。
手順 5：手順 4 の HTML へのリンクを含むメールを作成し，手順 1 で入手したメールアドレスに送信する。
手順 6：手順 5 のメールがメール受信者に届き，罠サイトにアクセスするのを待つ。
手順 7：罠サイトへのアクセスを検知後， b が完了することを期待して数分間待ち，手順 2 で入手した sessionID を指定した状態で，URL “ a2 ” にアクセスする。

図 A　セッションフィクセーション脆弱性を悪用して不正ログインする手順

攻撃者が，セッションフィクセーション脆弱性を悪用して不正ログインに成功し，画面 02 で応募者確認ボタンをクリックして，当該企業の求人に応募した求職者の求職者属性情報と求職情報を閲覧できる。また，同じ画面 02 で問合せ確認ボタンをクリックして，当該企業に問合せを行った求職者の求職者属性情報と問合せ内容を閲覧できる。

(2) 脆弱性の修正方法

a1 の画面遷移の際に実行されるコードにおいて， c ことを推奨する。

(省略)

図 3　診断報告書（続き）

B 社は，M 社に診断報告書を提出し，セキュリティ診断を完了した。

設問１　図３中の表Ａ中の［　a1　］に入れる図２中の画面遷移の記号と，図３中の図Ａ中の［　a2　］に入れる表１中のURLの組みはどれか。解答群のうち，最も適切なものを選べ。

解答群

	a1	a2
ア	（ア）	https://test.△△△.jp/
イ	（ア）	https://test.△△△.jp/mypage
ウ	（イ）	https://test.△△△.jp/
エ	（イ）	https://test.△△△.jp/mypage
オ	（エ）	https://test.△△△.jp/
カ	（エ）	https://test.△△△.jp/mypage

設問２　次の動作のうち，図Ａ中の［　b　］に入れるものはどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　メール受信者によるＭサイトへのログイン

イ　メール受信者によるパスワードの再設定

ウ　メール受信者による罠サイトへのログイン

設問３　次の修正方法のうち，図 3 中の［　c　］に入れるものはどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　Cookie に HttpOnly 属性を設定する

イ　Cookie に Secure 属性を設定する

ウ　Cookie に SameSite 属性を設定する

エ　使用した sessionID を GET パラメータで渡す

オ　使用した sessionID を URL パラメータで渡す

カ　使用した sessionID を暗号化して，ローカルストレージに保存する

キ　使用した sessionID を無効化して，新しい sessionID を発行する

情報処理安全確保支援士試験
科目 B のサンプル問題　解答例・出題趣旨

問番号		正解
問 1		オ
問 2	設問 1	ウ
	設問 2	ア
	設問 3	キ

問番号	出題趣旨
問 1	情報資産台帳を作成することは，リスクアセスメントを行う上で重要な要素である。本問では，新たに情報資産台帳を整備する上場企業を題材に，情報資産台帳の様式を理解し，各部署からの質問に的確に助言できる能力を問う。
問 2	個人情報を取り扱う Web サイトに対するセキュリティ診断を題材に，検出された脆弱性について，脆弱性の内容を理解する能力及び脆弱性の修正方法を立案する能力を問う。