問4　セキュリティ診断に関する次の記述を読んで，設問に答えよ。

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。これらの情報は，M サイトのデータベースに保存される。M サイトでは，入力された情報に基づいて，求職者と求人企業のマッチングを行っている。求職者は，マッチングで提案された企業に問合せや応募をすることができる。

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）と，求人企業がアプリケーションプログラムから HTTPS で呼び出すことを想定したインタフェース（以下，このインタフェースを WebAPI 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 アプリの脆弱性の検出と，Web サーバのプラットフォームの脆弱性の検出を行う。
・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。
・Web サーバのプラットフォームの脆弱性の検出は，診断ツールで行う。
・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

Mサイトの設計書の中で参照した部分を，図2，図3及び表1に示す。

1.プロトコルは，HTTPSとする。
2.RESTful APIによって，次の機能を求人企業に提供する。
(1) 日時の範囲を指定して，当該企業宛てに問合せがあった求職者の求職者ID[1)]を取得する。
(2) 日時の範囲を指定して，当該企業宛てに応募があった求職者の求職者IDを取得する。
(3) 任意の求職者IDを指定して，求職者属性情報を取得する。
3.求人企業の認証方式は次のとおりとする。
(1) WebAPIを利用する際の利用者認証のために，Mサイトの利用者ID[2)]と紐付けられたAPIkeyを発行する。APIkeyの有効期間は，発行後14日間とする。
(2) WebAPIを利用する際のHTTP Request内のAPIkeyが，発行済みのものであり，かつ，有効期間内であるか確認することで，正規利用者であるかどうかを確認する。
4. APIkeyについては，次のとおりとする。
(1) 求人企業のうち，WebAPIの利用契約を締結済みの企業だけにAPIkeyを発行する。利用契約で認めている求職者属性情報の利用範囲は，当該企業への問合せ又は当該企業への応募それぞれに関する対応だけである。
(2) 一つの利用者IDに対して複数のAPIkeyを発行できる。
(3) 求職者には，APIkeyを発行しない。

注[1)] 求職者がMサイトに利用者登録をした年月日の8桁の数字の後ろに，日ごとに000001から登録順に割り当てられる6桁の数字を加えた数字14桁の文字列である。
注[2)] Mサイトを利用する求職者及び求人企業の担当者ごとに発行される。

図2 WebAPIの仕様

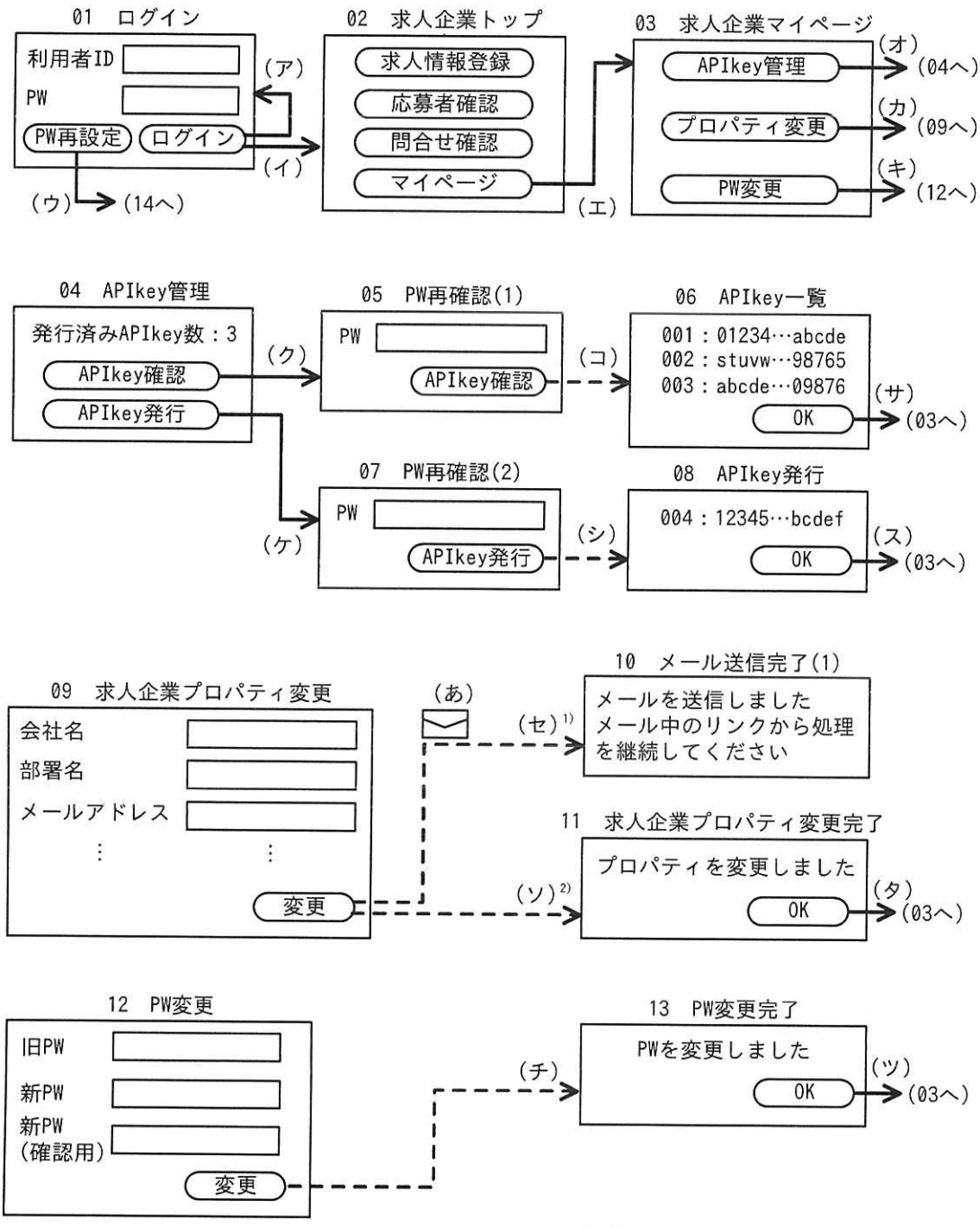
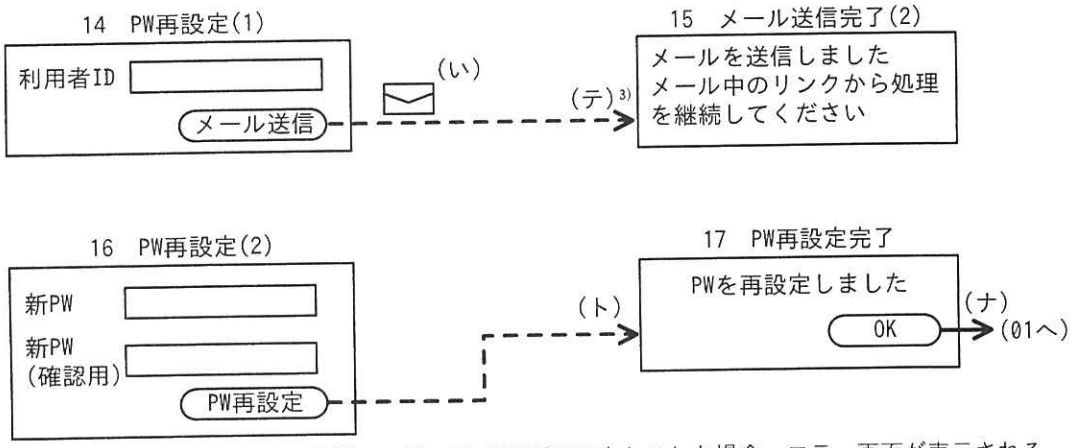

01 ログイン
利用者ID
PW
PW再設定
ログイン
(ア)
(イ)
(ウ)
(14へ)
02 求人企業トップ
求人情報登録
応募者確認
問合せ確認
マイページ
(エ)
03 求人企業マイページ
APIkey管理
プロパティ変更
PW変更
(オ)
(04へ)
(カ)
(09へ)
(キ)
(12へ)
04 APIkey管理
発行済みAPIkey数：3
APIkey確認
APIkey発行
(ク)
(ケ)
05 PW再確認(1)
PW
APIkey確認
(コ)
06 APIkey一覧
001：01234…abcde
002：stuvw…98765
003：abcde…09876
OK
(サ)
(03へ)
07 PW再確認(2)
PW
APIkey発行
(シ)
08 APIkey発行
004：12345…bcdef
OK
(ス)
(03へ)
09 求人企業プロパティ変更
会社名
部署名
メールアドレス
変更
(あ)
(セ)1)
10 メール送信完了(1)
メールを送信しました
メール中のリンクから処理
を継続してください
(ソ)2)
11 求人企業プロパティ変更完了
プロパティを変更しました
OK
(タ)
(03へ)
12 PW変更
旧PW
新PW
新PW
(確認用)
変更
(チ)
13 PW変更完了
PWを変更しました
OK
(ツ)
(03へ)
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

図3　画面遷移図（抜粋）



注記 1　ログインしていない状態で，02～13 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 09 でメールアドレスを変更した場合の画面遷移である。画面遷移の際，M サイトから，変更前のメールアドレスに，確認用 URL が記載されたメール(あ)を送信する。利用者がメール(あ)に記載された確認用 URL にアクセスすると，変更を反映し，画面 11 を表示するとともに，M サイトから，変更前及び変更後のメールアドレスに，変更内容が記載されたメールを送信する。

注 2)　画面 09 でメールアドレス以外だけを変更した場合の画面遷移である。

注 3)　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(い)を送信する。利用者がメール(い)に記載された PW 再設定用 URL にアクセスすると，画面 16 を表示する。

図 3　画面遷移図（抜粋）（続き）

表 1　各画面の URL

画面番号	URL
01, 02	https://test.△△△.jp/
03	https://test.△△△.jp/mypage
04	https://test.△△△.jp/apikey
05, 06	https://test.△△△.jp/keylist
07, 08	https://test.△△△.jp/keynew
09, 10, 11	https://test.△△△.jp/property
12, 13	https://test.△△△.jp/pwchange
14, 15	https://test.△△△.jp/pwreset
16, 17	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 4 の診断報告書を作成した。

診断報告書

1 章　診断結果概要

1.1　診断結果要約

M サイトで，脆弱性を検出した。

（省略）

1.2 検出した脆弱性の件数

（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 a
2	（省略）	メールヘッダーインジェクション	メール(あ)の送信
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。

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">

図 4　診断報告書

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：求人企業の登録メールアドレスを，何らかの方法で入手する。
手順 2：URL “ b ” 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 “ b ” 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， c 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 “ b ” 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

a の画面遷移の際に実行されるコードにおいて，d することを推奨する。

2.2.2 メールヘッダーインジェクション

この脆弱性は，メール(あ)について検出された。なお，メール(い)では，この脆弱性は検出されなかった。

(1) 脆弱性の内容

図 B の手順で操作を行ったところ，メール(あ)が abc@example.com だけに送信され，本来の宛先である変更前のメールアドレスには送信されなかった。abc@example.com に送信されたメール(あ)の内容を表 C に示す。

手順 1：画面 09 の会社名に図 C の検査文字列を入力して変更ボタンをクリックする。
手順 2：画面 11 で OK ボタンをクリックする。
手順 3：画面 03 でプロパティ変更ボタンをクリックして，再度，画面 09 を表示する。
手順 4：画面 09 でメールアドレスに xyz@example.com を入力して変更ボタンをクリックする。

図 B　メールヘッダーインジェクション脆弱性を検出した手順

図 4　診断報告書（続き）

●●株式会社%0D%0ATo:abc@example.com%0D%0A%0D%0A

図C　メールヘッダーインジェクションの検査文字列

表C　メール(あ)の内容

位置	内容
メール(あ)のヘッダー部の末尾	Subject: ●●株式会社 To:abc@example.com
メール(あ)のボディ部の冒頭	様のメールアドレス変更のお知らせ To: 〈本来の宛先〉[1)]

注[1)] 〈本来の宛先〉には，変更前のメールアドレスが入っていた。

攻撃者がこの脆弱性を悪用するには，求人企業として M サイトにログインする必要がある。求人企業としての登録には審査が必要であり，この脆弱性だけを利用して攻撃が行われるおそれは小さい。

(2) 脆弱性の修正方法
（省略）

2.2.3 HTTP ヘッダーの不備
(1) 脆弱性の内容
表 D の HTTP ヘッダーは，出力するよう推奨されているが，いずれの画面遷移の HTTP レスポンスにおいても出力されなかった。

表D　出力されなかった HTTP ヘッダー

HTTP ヘッダー名	設定した場合の主な効果
Content-Security-Policy	Web ブラウザが実行可能なスクリプトの有効なソースとなるドメインを，M サイトで必要なものだけに限定することができる。
Strict-Transport-Security	e
X-Content-Type-Options	f

これらの HTTP ヘッダーを設定することで他の脆弱性による被害を軽減することができる。

(2) 脆弱性の修正方法
（省略）

図4　診断報告書（続き）

3章　プラットフォームの診断結果

3.1　検出した脆弱性の概要

検出した脆弱性は，表Eのとおりである。

表E　検出したプラットフォームの脆弱性の一覧

項番	重要度	脆弱性の種類
1	(省略)	TLS 1.1 が利用可能
2	(省略)	HTTP サーバのバージョンの露出

3.2　検出した脆弱性の説明

3.2.1 TLS 1.1 が利用可能

(省略)

3.2.2 HTTP サーバのバージョンの露出

HTTP レスポンスのヘッダーに，HTTP サーバのバージョンが出力されている。

(省略)

4章　総合評価

4.1　想定される攻撃と被害

攻撃者が，セッションフィクセーション脆弱性を悪用するだけでも求職者属性情報を窃取することができるが，図 D の順序で攻撃をした場合，不審なメールが求人企業に届かないので，攻撃に気付かれることなく，WebAPI を悪用して，より多くの求職者属性情報を窃取することができる。

(1) 図Aの手順で，Mサイトに不正にログインする。ただし，図Aの手順1で入手するメールアドレスは，WebAPI の利用権限をもつ求人企業のものである。
(2) [g]
(3) 画面 09 で，メールアドレスに攻撃者のメールアドレスを入力して，変更ボタンをクリックする。
(4) 別の端末から，画面 01 で PW 再設定ボタンをクリックし，(1)で不正にログインした利用者 ID に対する一連のパスワード再設定処理を行う。
(5) 再設定後のパスワードでログインする。
(6) [h]
(7) WebAPI の機能を利用して，多数の求職者属性情報を窃取する。

図D　より多くの求職者属性情報の窃取につながる攻撃

(省略)

図4　診断報告書（続き）

5章　参考意見

本章は，弊社の知見に基づく参考意見である。

5.1　Mサイトの仕様についての意見

今回の診断の過程で，M サイトの仕様の一部を把握することができた。弊社が把握できた範囲内でも，M サイトの仕様には幾つかの問題点があり，表 A と表 E の脆弱性を修正したとしても，インターネットからの攻撃によって被害が発生するおそれがある。

5.1.1 WebAPI の仕様の改善

WebAPI に関して，仕様の改善の方針案と改善すべき理由を表 F に示す。改善によって，攻撃による被害を未然に防止すること，又は被害を軽減することができる。

表 F　WebAPI の仕様の改善の方針案

項番	仕様の改善の方針案	改善すべき理由
1	i	j
⋮	⋮	⋮

5.1.2 Web アプリケーションプログラムの求職者向け機能の仕様の改善

（省略）

5.1.3 Web アプリケーションプログラムの求人企業向け機能の仕様の改善

Web アプリケーションプログラムの求人企業向け機能に関して，仕様の改善の方針案と改善すべき理由を表 G に示す。改善によって，攻撃による被害を未然に防止すること，又は被害を軽減することができる。

表 G　Web アプリケーションプログラムの求人企業向け機能の仕様の改善の方針案

項番	仕様の改善の方針案	改善すべき理由
1	k	ℓ
⋮	⋮	⋮

（省略）

図 4　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４中の２章について答えよ。

(1)　表 A 中及び 2.2.1(2)中の [a] に入れる適切な記号を，図 3 中の画面遷移の記号(ア)～(ナ)から選び，答えよ。

(2)　図 A 中の [b] に入れる適切な URL を，表 1 から選び答えよ。

(3)　図 A 中の [c] に入れる適切な操作を答えよ。

(4)　2.2.1(2) 中の [d] に入れる適切な修正方法を具体的に答えよ。

(5)　表 D 中の [e]，[f] に入れる適切な効果を答えよ。

設問２　図 4 中の 4 章にある図 D 中の [g]，[h] に入れる攻撃手順を答えよ。

設問３　あなたがこの診断を担当したとして，図 4 中の 5 章の表 F 中の [i]，[j] 及び表 G 中の [k]，[ℓ] に記述する内容を答えよ。なお，複数の改善の方針案がある場合は，被害を防ぐ効果が最も高いものを答えよ。