問1　Webセキュリティに関する次の記述を読んで，設問に答えよ。

A社グループは，全体で従業員20,000名の製造業グループである。技術開発や新製品の製造・販売を行うA社のほか，特化型の製品の製造・販売を行う複数の子会社（以下，グループ各社という）がある。A社及びグループ各社には，様々なWebサイトがある。A社では，資産管理システムを利用し，IT資産の管理を効率化している。Webサイトの立上げ時は，資産管理システムへのWebサイトの概要，システム構成，IPアドレス，担当者などの登録申請が必要である。

A社には，CISOが率いるセキュリティ推進部がある。セキュリティ推進部の業務は，主に次の三つである。

・A社の情報セキュリティマネジメントを統括する。
・A社のWebサイトの脆弱(ぜい)性診断（以下，脆弱性診断を診断という）を管理する。例えば，A社の会員サイトなど，重要なWebサイトについて，診断を新規リリース前に実施し，その後も年1回実施する。なお，診断は，セキュリティ専門業者のB社に委託している。
・グループ各社に対して，情報セキュリティポリシーやセキュアコーディング規約を配布する。なお，診断の実施有無や内容はグループ各社の判断に任せている。

IoT製品の市場拡大によってグループ各社による新規Webサイト開発の増加が予想されている中，A社の経営陣は，グループ各社のWebサイトのセキュリティが十分かどうかを懸念し始めた。そこで，グループ各社の重要なWebサイトも，A社のセキュリティ推進部がグループ各社と協議しつつ診断を管理することになった。

セキュリティ推進部がB社に診断対象となるWebサイトのリリーススケジュールを伝えたところ，同時期に多数の診断を依頼されても対応することができない可能性があるとのことだった。そこで，グループ各社の一部のWebサイトに対する診断をA社グループ内で実施できるようにするための内製化推進プロジェクト（以下，Sプロジェクトという）を立ち上げた。

セキュリティ推進部のZさんは，Sプロジェクトを担当することになった。Zさんはこれまでも B社への診断の依頼を担当しており，診断の準備から診断結果の報告まで，診断全体をおおむね把握していた。

〔S プロジェクトの進め方〕

S プロジェクトは，B 社の支援を得ながら，表 1 のとおり進めることにした。B 社からは，セキュリティコンサルタントで情報処理安全確保支援士（登録セキスペ）である Y 氏の支援を受けることになった。

表 1　S プロジェクトの進め方

フェーズ	作業内容	説明
フェーズ 1	診断項目の決定	診断項目を決める。
フェーズ 2	診断ツールの選定	診断ツールを選定する。
フェーズ 3	Z さんと B 社での診断の実施と結果比較	A 社グループである K 社の製品のアンケートサイト（以下，サイト M という）について，Z さんと B 社がそれぞれ診断を実施する。Z さんは，B 社の診断結果との差異を評価する。
フェーズ 4	A 社グループの診断手順案の作成	フェーズ 3 の評価を基に，A 社グループの診断手順案を作成する。
フェーズ 5	診断手順案に従った診断の実施	K 社の会員サイト（以下，サイト N という）に対し，A 社グループの診断手順案に従って，診断を実施する。
フェーズ 6	A 社グループの診断手順の制定	フェーズ 5 の診断で残った課題についての対策を検討した上で，A 社グループの診断手順を制定する。

〔フェーズ 1：診断項目の決定〕

S プロジェクトでは，診断項目を決めた。

〔フェーズ 2：診断ツールの選定〕

B 社が Web サイトの診断にツール V を使っていることもあり，A 社はツール V を購入することに決めた。ツール V の仕様を図 1 に示す。

1. 機能概要

Dynamic Application Security Testing (DAST) のツールである。パラメータを初期値から何通りもの値に変更した HTTP リクエストを順に送信し，応答から脆弱性の有無を判定する。

2. 機能

(1) プロジェクト作成機能

(1-1) プロジェクト作成機能：診断対象とする Web サイトの FQDN を登録してプロジェクトを作成する。

(2) 診断対象 URL の登録機能

(2-1) 診断対象 URL の自動登録機能：探査を開始する URL を指定すると，自動探査によって，指定された URL の画面に含まれるリンク，フォームの送信先などをたどり，診断対象 URL を自動的に登録していく。診断対象 URL にひも付くパラメータ [1]とその初期値も自動的に登録される。

(2-2) 診断対象 URL の手動登録機能：診断対象 URL を手動で登録する。診断対象 URL にひも付くパラメータとその初期値は自動的に登録される。

(2-3) 診断対象 URL の拡張機能：診断対象 URL ごとに設定できる。本機能を設定すると，診断対象 URL の応答だけでなく，別の URL の応答も判定対象になる。本機能を設定するには，診断対象 URL の拡張機能設定画面を開き，拡張機能設定に，判定対象に含める URL を登録する。

(3) 拒否回避機能

(3-1) 拒否回避機能：特定のパラメータが同じ値であるリクエストを複数回送信すると拒否されてしまう診断対象 URL については，URL ごとに本機能を設定することで，拒否を回避できる。

(4) URL にひも付くパラメータの設定機能

(4-1) パラメータ手動設定機能：パラメータの初期値を，任意の値に手動で修正して登録する。

(5) 診断項目の設定機能

(5-1) 診断項目設定機能：診断項目を選択して設定する。

(6) アカウント設定機能

(6-1) 利用者 ID とパスワードの設定機能：ログイン機能がある Web サイトの場合は，ログイン後の画面の URL に対して診断するために，診断用のアカウントの利用者 ID とパスワードを設定する。

(6-2) アカウントの拡張機能の設定：診断用のアカウントを複数設定できる。

(7) 診断機能

(7-1) 診断機能：診断項目について診断を行う。診断用のアカウントが設定されている場合は，それらを順番に使う。

(8) レポート出力機能

(8-1) レポート出力機能：診断結果を PDF で出力する。

注 [1] 例えば，検索画面から検索結果が表示される画面に遷移する URL が診断対象 URL の場合，診断時に送信される検索ワードを含むパラメータを指す。

図 1　ツール V の仕様（抜粋）

診断対象 URL の自動登録機能及び手動登録機能の特徴を表 2 に示す。

表 2　診断対象 URL の自動登録機能及び手動登録機能の特徴

自動登録機能の特徴	手動登録機能の特徴
・登録に作業者の工数がほぼ不要である。 ・常に一定の品質で登録できる。 ・Web サイトによっては，登録が漏れる場合がある。例えば，遷移先の URL が JavaScript などで動的に生成されるような場合である。 ・必須入力項目に適切な値を入力できず，正常に遷移できないことがある。	・登録に作業者の工数が必要である。 ・Web ブラウザを使ってトップページから順に手動でたどっても，登録が漏れる場合がある。Web サイトの全ての URL を診断対象とする場合，①診断対象 URL を別の方法で調べる必要がある。

A 社は，診断項目のうち，ツール V では診断ができないものは手動で診断を実施することにした。

〔フェーズ 3：Z さんと B 社での診断の実施と結果比較〕

Z さんと B 社は，サイト M に対して診断を実施した。サイト M の画面遷移を図 2 に示す。

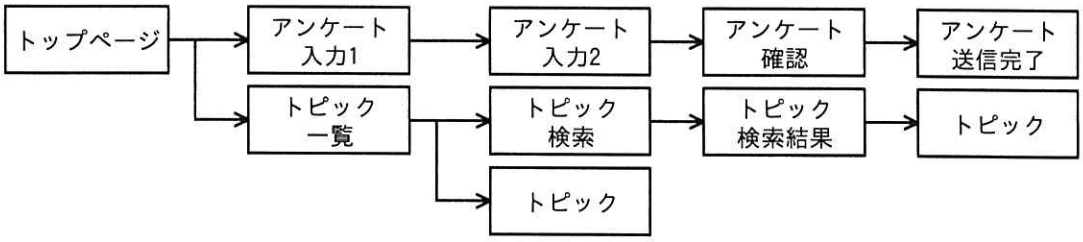
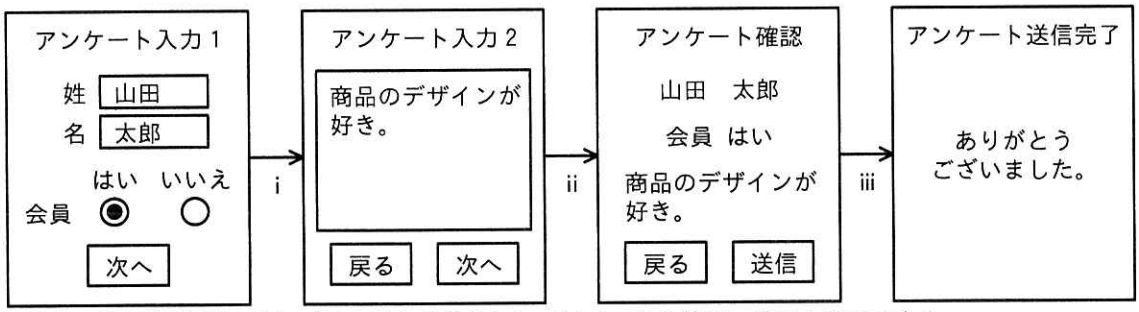


図 2　サイト M の画面遷移（抜粋）

Z さんは，Z さんの診断結果と B 社の診断結果とを比較した。その結果，Z さんは脆弱性の一部を検出できていないことが分かった。検出できなかった脆弱性は，アンケート入力 1 の画面での入力値に起因するクロスサイトスクリプティング（以下，クロスサイトスクリプティングを XSS という）と，トピック検索の画面での入力値に起因する SQL インジェクションであった。サイト M のアンケート入力 1 からの画面遷移を図 3 に示す。



注記　画面遷移時に Web ブラウザから送られたパラメータの値は，次のとおりである。

i : last_name=%E5%B1%B1%E7%94%B0&first_name=%E5%A4%AA%E9%83%8E&member=Y

ii : text=%E5%95%86%E5%93%81%E3%81%AE%E3%83%87%E3%82%B6%E3%82%A4%E3%83%B3%E3%81%8C%E5%A5%BD%E3%81%8D%E3%80%82

iii : submit=Yes

図３　サイト M のアンケート入力１からの画面遷移

トピック検索の画面で検索条件として入力した値の処理に関する診断で，ツール V が送ったパラメータと検索結果の件数を表３に示す。なお，トピック検索の画面で検索条件として入力した値は，パラメータ keyword に格納される。

表３　ツール V が送ったパラメータと検索結果の件数（抜粋）

診断者	送ったパラメータ	検索結果の件数
B 社	keyword=manual	10 件
	keyword=manual’	0 件
	keyword=manual a	10 件
	keyword=manual b	0 件
Z さん	keyword=xyz	0 件
	keyword=xyz’	0 件
	keyword=xyz a	0 件
	keyword=xyz b	0 件

注記１　B 社はパラメータ keyword の初期値を manual としている。

注記２　Z さんはパラメータ keyword の初期値を xyz としている。

ツール V は，B 社の診断では，keyword=manual a と keyword=manual b の検索結果を比較して SQL インジェクションを検出できたが，Z さんの診断では SQL インジェクションを検出できなかった。

Z さんは，検出できなかった二つの脆弱性について，どうすれば検出できるのかをY氏に尋ねた。次は，その際のY氏とZさんの会話である。

Y氏　：XSS については，入力したスクリプトが二つ先の画面でエスケープ処理されずに出力されていました。XSS の検出には，ツール V において図 1 中の［　c　］の②設定が必要でした。SQL インジェクションについては，keyword の値が文字列として扱われる仕様となっており，SQL の構文エラーが発生するような文字列を送ると検索結果が 0 件で返ってくるようです。そこで，③keyword の初期値として SQL インジェクションを検出できる“manual”のような値を設定する必要がありました。

Zさん：なるほど。ツール V は，Web サイトに応じた初期値を設定する必要があるのですね。

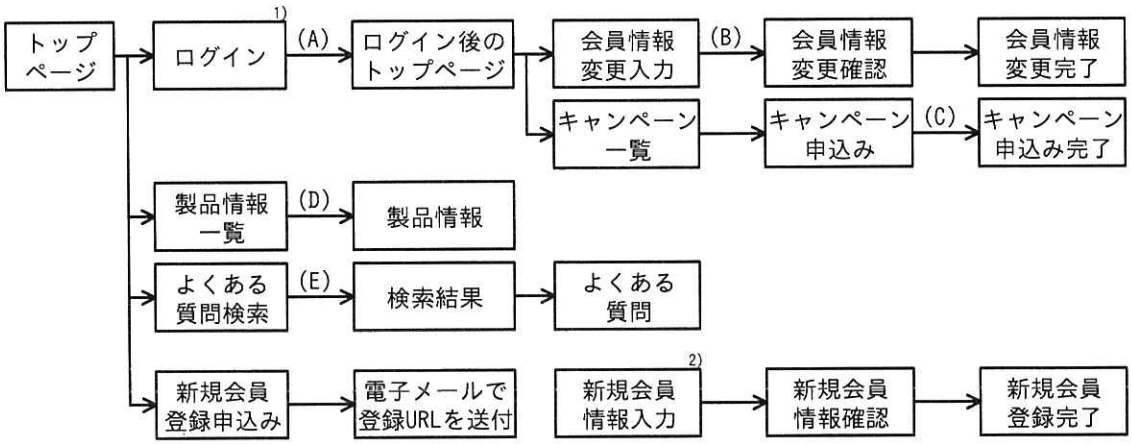
その後，Z さんは，Y 氏とともに，フェーズ 3 での診断結果を分析した。その際，偽陽性を除いてから開発者に報告することは難しいことが問題となった。

そこで，Z さんは，“開発者への報告の際に，診断結果の報告内容が脆弱性なのか偽陽性なのか，その判断を開発者に委ねる。一方，診断結果の報告内容における脆弱性の内容，リスク及び対策について，開発者が B 社に直接問い合わせる。”という案にした。なお，B 社のサポート費用は，問合せ件数に比例するチケット制である。グループ各社がB社とサポート契約を結ぶが，費用は，当面A社がまとめて支払い，後日グループ各社と精算する。

これまでの検討を踏まえて，Z さんは，フェーズ 4 で A 社グループの診断手順案を作成した。

〔フェーズ 5：診断手順案に従った診断の実施〕

Y 氏の協力の下，Z さんは，診断手順案に従ってサイト N の診断を実施することにした。サイト N は既にリリースされている。サイト N の会員（以下，会員 N という）は，幾つかのグループに分けられており，申し込むことができるキャンペーンが会員の所属しているグループによって異なる。サイト N の画面遷移を図 4 に示す。



注記 1　一つのキャンペーンに対して，会員 N は 1 回だけ申込みできる。

注記 2　既に登録されているメールアドレスでは，新規会員登録の申込みはできない。

注記 3　ログインすると，会員 N が所属しているグループを識別するための group_code というパラメータがリクエストに追加される。

注記 4　よくある質問検索の画面で検索する際に，次の画面に遷移する URL が JavaScript で動的に生成される。

注 1)　パスワードを連続 5 回間違えるとアカウントがロックされる。ログイン時に発行されるセッション ID である JSESSIONID は cookie に保持される。ログイン後しばらくアクセスしないとセッション ID は破棄され，再度ログインが必要になる。

注 2)　新規会員登録の申込み時に電子メールで送付された登録 URL にアクセスすると表示される。

図 4　サイト N の画面遷移（抜粋）

まず，Z さんは，診断対象 URL，アカウントなど，診断に必要な情報を K 社に確認した。しかし，サイト N については診断に必要な情報が一元管理されていなかったので，確認の回答までに 1 週間掛かった。診断開始までに要する時間が課題として残った。

次に，Z さんは，アカウントの設定を行った後，④探査を開始する URL に図 4 のトップページを指定してツール V の診断対象 URL の自動登録機能を使用したが，一部の URL は登録されなかった。その後，登録されなかった URL を手動で登録した。診断を実施してもよいか，Y 氏に確認したところ，注意点の指摘を受けた。具体的には，⑤特定のパラメータが同じ値であるリクエストを複数回送信するとエラーになり，遷移できない箇所があることに注意せよとのことであった。適切な診断を行うために，ツール V の拒否回避機能を設定して診断を実施した。診断では，次に示す脆弱性が検出された。

・XSS

・アクセス制御の回避

Z さんは，これらの脆弱性について，サイト N の開発部門（以下，開発部 N という）に通知し，偽陽性かどうかの判断，リスクの評価及び対策の立案を依頼した。

〔XSS〕

XSS の脆弱性は，複数の画面で検出された。開発部 N から，“cookie に HttpOnly 属性が付いていると，［ d ］が禁止される。そのため，cookie が漏えいすることはなく，修正は不要である。”という回答があった。Z さんは，この回答を受けて Y 氏に相談し，“XSS を悪用しても cookie を盗めないのは確かである。しかし，⑥XSS を悪用して cookie 以外の情報を盗む攻撃があるので，修正が必要である。”と開発部 N に伝えた。

〔アクセス制御の回避〕

Z さんは，手動で診断し，アクセス制御の回避の脆弱性を，図 4 中のキャンペーン一覧の画面などで検出した。ある会員 N が⑦アクセス制御を回避するように細工されたリクエストを送ることで，その会員 N が本来閲覧できないはずのキャンペーンへのリンクが表示され，さらに，リンクをたどってそのキャンペーンに申し込むことが可能であった。正常なリクエストとそのレスポンスを図 5 に，脆弱性を検出するのに使ったリクエストとそのレスポンスを図 6 に示す。

```
[リクエスト]
POST /campaignSearch HTTP/1.1
Host: site-n.▲▲▲▲.jp
Cookie: JSESSIONID=KCRQ88ERH2G8MGT319E5OSMOAJFDIVEM

group_code=0001&keyword=new

[レスポンス]
<html>
 (省略)
<h1>申込み可能キャンペーン</h1>
<a href="/a_campaign1">1 A社キャンペーン1</a>
<a href="/a_campaign2">2 A社キャンペーン2</a>

<h1>注意事項</h1>
 (省略)
```

注記 1　リクエストヘッダ部分は，設問に必要なものだけ記載している。
注記 2　レスポンスは，レスポンスボディから記載している。

図 5　正常なリクエストとそのレスポンス

```
[リクエスト]
POST /campaignSearch HTTP/1.1
Host: site-n.▲▲▲▲.jp
Cookie: JSESSIONID=KCRQ88ERH2G8MGT319E50SMOAJFDIVEM

keyword=new

[レスポンス]
<html>
 (省略)
<h1>申込み可能キャンペーン</h1>
<a href="/a_campaign1">1 A社キャンペーン1</a>
<a href="/a_campaign2">2 A社キャンペーン2</a>
<a href="/b_campaign1">3 B社キャンペーン1</a>
<a href="/c_campaign1">4 C社キャンペーン1</a>
 (省略)
<a href="/z_campaign2">30 Z社キャンペーン2</a>

<h1>注意事項</h1>
 (省略)
```

注記１　リクエストヘッダ部分は，設問に必要なものだけ記載している。
注記２　レスポンスは，レスポンスボディから記載している。

図６　脆弱性を検出するのに使ったリクエストとそのレスポンス

開発部Ｎは，サイトＮへ送られてきたリクエスト中の［　e　］から，ログインしている会員Ｎを特定し，その会員Ｎが所属しているグループが［　f　］の値と一致するかを検証するように，ソースコードを修正することにした。

開発部Ｎは，Ｂ社の支援によって対応を終えることができたが，Ｂ社へ頻繁に問い合わせることになった結果，Ｂ社のサポート費用が高額になった。サポート費用をどう抑えるかが課題として残った。

〔フェーズ６：Ａ社グループの診断手順の制定〕

Ｚさんは，フェーズ５の診断で残った二つの課題についての対策を検討し，グループ各社から同意を得た上で，Ａ社グループの診断手順を完成させた。

セキュリティ推進部は，制定したＡ社グループの診断手順をグループ各社に展開した。

設問１　表２中の下線①について，別の方法を，30 字以内で答えよ。

設問２　〔フェーズ３：Z さんと B 社での診断の実施と結果比較〕について答えよ。

(1)　表 3 中及び本文中の［ a ］，［ b ］に入れる適切な字句を，解答群の中から選び，記号で答えよ。

解答群

ア　”　　イ　’ and ’a’=’a　　ウ　’ and ’a’=’b

エ　and 1=0　　オ　and 1=1

(2)　本文中の［ c ］に入れる適切な機能を，図１中の(1-1)～(8-1)から選び答えよ。

(3)　本文中の下線②について，どのような設定が必要か。設定の内容を，図 2 中の画面名を用いて 60 字以内で答えよ。

(4)　本文中の下線③について，keyword の初期値をどのような値に設定する必要があるか。初期値が満たすべき条件を，40 字以内で具体的に答えよ。

設問３　〔フェーズ５：診断手順案に従った診断の実施〕について答えよ。

(1)　本文中の下線④について，URL が登録されなかった画面名を，解答群の中から全て選び，記号で答えよ。

解答群

ア　会員情報変更入力　　イ　キャンペーン申込み

ウ　検索結果　　エ　新規会員情報入力

(2)　本文中の下線⑤について，該当する画面遷移とエラーになってしまう理由を 2 組み挙げ，画面遷移は図 4 中の(A)～(E)から選び，理由は 40 字以内で答えよ。

設問４　〔XSS〕について答えよ。

(1)　本文中の［ d ］に入れる適切な字句を，30 字以内で答えよ。

(2)　本文中の下線⑥について，攻撃の手口を，40 字以内で答えよ。

設問５　〔アクセス制御の回避〕について答えよ。

(1)　本文中の下線⑦について，リクエストの内容を，30 字以内で具体的に答えよ。

(2)　本文中の［ e ］，［ f ］に入れる適切なパラメータ名を，図 5 中から選び，それぞれ 15 字以内で答えよ。

設問６　〔フェーズ６：A 社グループの診断手順の制定〕について答えよ。

(1)　診断開始までに要する時間の課題について，A 社で取り入れている管理策を参考にした対策を，40 字以内で具体的に答えよ。

(2)　B 社のサポート費用の課題について，B 社に対して同じ問合せを行わず，問合せ件数を削減するために，A 社グループではどのような対策を実施すべきか。セキュアコーディング規約の必須化や開発者への教育以外で，実施すべき対策を，50 字以内で具体的に答えよ。