SC

令和５年度　春期
情報処理安全確保支援士試験
午後Ⅱ　問題

試験時間	14:30 ～ 16:30（２時間）

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２
選択方法	１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。２問とも○印で囲んだ場合は，はじめの１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２を選択した場合の例〕

選択欄	
１問選択	問１
	(問２)

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　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。

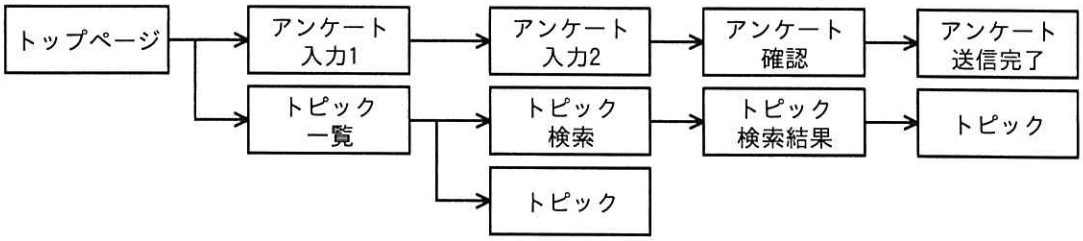
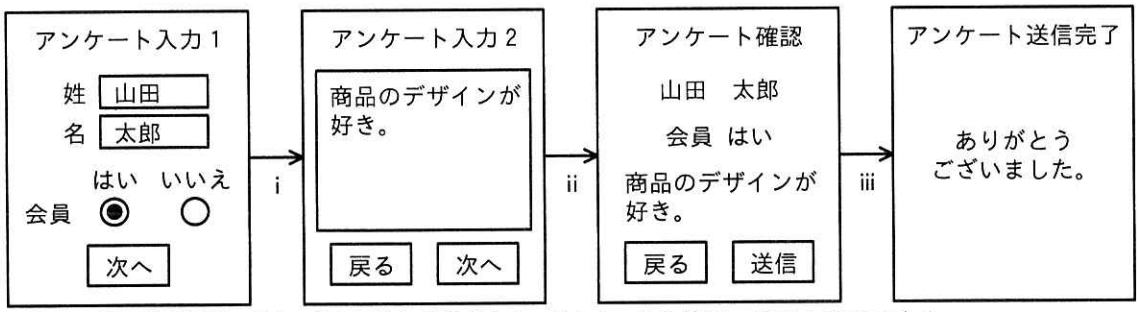


図 2　サイト M の画面遷移（抜粋）

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。

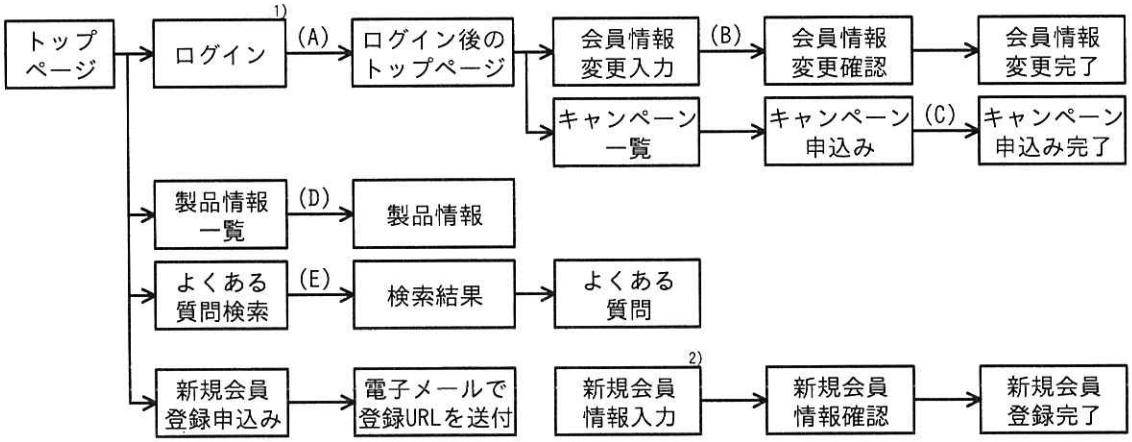
その後，Z さんは，Y 氏とともに，フェーズ 3 での診断結果を分析した。その際，偽陽性を除いてから開発者に報告することは難しいことが問題となった。

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=KCRQ88ERH2G8MGT319E5OSMOAJFDIVEM

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。

問２　Web サイトのクラウドサービスへの移行と機能拡張に関する次の記述を読んで，設問に答えよ。

W 社は，従業員 100 名のブログサービス会社であり，日記サービスという Web サービスを 10 年前から提供している。日記サービスの会員は，自分の食事に関する記事の投稿及び摂取カロリーの管理ができる。

日記サービスは，W 社のデータセンター内で稼働している。ハードウェアの調達には 1 か月程度を要する。W 社は，日記サービスが稼働している各機器の運用を D 社に委託している。D 社に委託している運用を表 1 に示す。

表 1　D 社に委託している運用（概要）

項番	運用	運用内容
1	ログ保全	・定期的に，日記サービスが稼働している各機器の全てのログを外部メディアにバックアップする。 ・外部メディアにバックアップする前に，ログを一時的に D 社作業用端末にダウンロードする。 ・D 社作業用端末でのバックアップ作業後に，D 社作業用端末からログを削除する。なお，各機器からログを削除する作業は W 社が行う。
2	障害監視	・アプリケーションプログラム（以下，アプリという）の問題の一次切分けを行う。アプリの問題は，ログを監視しているソフトウェアによって検知される。 ・ログを確認して一次切分けを行う。その際に，サーバの一覧を参照する。 ・W 社への連絡は，電子メール（以下，メールという）と電話で行う。
3	性能監視	・W 社が定めた，CPU 稼働率，処理性能及び応答時間に関わる指標（以下，性能指標という）を監視する。 ・異常を検知すると，一次切分けを行う。その際に，サーバの一覧を参照する。 ・必要に応じて，W 社への連絡をメールと電話で行う。
4	機器故障対応	・交換対象のハードウェアの発注を行う。 ・故障機器のハードウェア交換作業を行う。

この 2，3 年，会員が急増しているので，W 社は，日記サービスをクラウドサービスに移行することにした。

〔移行先のクラウドサービス選定〕

W 社は，クラウドサービスへの移行時及び移行後の管理，運用について，検討を開始した。

まず，クラウドサービスへの移行時及び移行後に，W 社が何を管理，運用する必要があるかを調べたところ，表 2 のとおりであった。

表 2　W 社が管理，運用する必要のある範囲

構成要素	クラウドサービスの分類		
	IaaS	PaaS	SaaS
ハードウェア，ネットワーク	×	×	×
OS，ミドルウェア	a	b	c
アプリ	d	e	f
アプリに登録されたデータ	g	h	i

注記　“○”は W 社が管理，運用する必要があるものを示し，“×”は必要がないものを示す。

クラウドサービスへの移行及びクラウドサービスの設定は W 社が行い，移行後，表 1 の項番 1～項番 3 の運用を D 社に委託する計画にした。

移行先のクラウドサービスとして，L 社のクラウドサービスを選定した。L 社が提供しているクラウドサービスを表 3 に示す。

表 3　L 社が提供しているクラウドサービス

クラウドサービス名	説明
仮想マシンサービス	・利用者が OS やアプリを配備することによって，物理サーバと同じ機能を実行するための仮想化基盤である。
データベース（以下，DB という）サービス	・関係 DB である。 ・容量の拡張，バックアップなどは，自動で実行される。
ブロックストレージサービス	・固定長のブロックという論理単位で管理できるストレージである。仮想マシンサービスのファイルシステムとして割り当てることが可能である。
オブジェクトストレージサービス	・データをオブジェクトとして扱い，各オブジェクトをメタデータで管理できるストレージである。 ・オブジェクトの保存のために必要なサーバの資源管理，容量の拡張などは，自動で実行される。
モニタリングサービス	・利用者が利用している L 社の各クラウドサービスについて，性能指標を監視する。

表３　Ｌ社が提供しているクラウドサービス（続き）

クラウドサービス名	説明
アラートサービス	・Ｌ社のクラウドサービスの環境[1)]でイベント[2)]が発生したときに，そのイベントを検知してアラートをメールで通知する。
仮想ネットワークサービス	・レイヤー2 スイッチ（以下，L2SW という），ファイアウォール（以下，FW という），ルータなどのネットワーク機器を含むネットワークを仮想的に構成でき，インターネットとの接続を可能にする。

注[1)]　Ｌ社の各クラウドサービスを利用して構築したシステム及びネットワークを指す。
注[2)]　特定の利用者による操作，システム構成の変更，設定変更などである。

イベント検知のルールは JSON 形式で記述する。そのパラメータを表４に示す。

表４　イベント検知のルールに記述するパラメータ

パラメータ	内容	取り得る値
system	検知対象とするシステム ID	・0000 ～ 9999
account	検知対象とする利用者 ID	・0000 ～ 9999
service	検知対象とするクラウドサービス名	・仮想マシンサービス ・オブジェクトストレージサービス ・モニタリングサービス
event	検知対象とするイベント	event の取り得る値は，service の値によって異なる。 ・仮想マシンサービスの場合 - 仮想マシンの起動 - 仮想マシンの停止 - 仮想マシンの削除 ・オブジェクトストレージサービスの場合 - オブジェクトの作成 - オブジェクトの編集 - オブジェクトの削除 - オブジェクトの閲覧 - オブジェクトのダウンロード ・モニタリングサービスの場合 - 監視する性能指標の追加 - 監視する性能指標の削除

注記　system と account の取り得る値には正規表現を利用できる。正規表現は次の規則に従う。
[012] は，0，1 又は 2 のいずれか数字 1 文字を表す。
[0-9] は，0 から 9 までの連続する数字のうち，いずれか数字 1 文字を表す。
* は，直前の正規表現の 0 回以上の繰返しを表す。
+ は，直前の正規表現の 1 回以上の繰返しを表す。

仮想マシンサービスを利用して構築した，システム ID が 0001 のシステムにおいて，

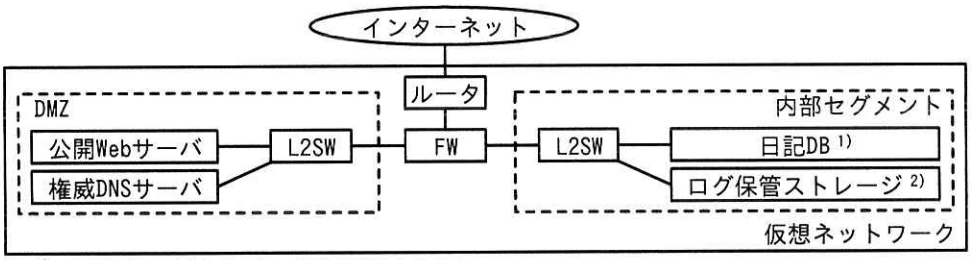
利用者 ID が 1000 である利用者が仮想マシンを停止させた場合の，イベント検知のルールの例を図 1 に示す。

```
1: {
2:  "system": "0001",
3:  "account": "1000",
4:  "service": "仮想マシンサービス",
5:  "event": "仮想マシンの停止"
6: }
```

図 1　イベント検知のルールの例

〔日記サービスの L 社のクラウドサービスへの移行〕

移行後の日記サービスの仮想ネットワーク構成を図 2 に，図 2 中の主な構成要素を表 5 に示す。



注 1)　日記サービスのデータを管理する DB
注 2)　日記サービスのログを保管するストレージ

図 2　移行後の日記サービスの仮想ネットワーク構成

表 5　図 2 中の主な構成要素

システム ID	構成要素	利用する L 社のクラウドサービス
1000	公開 Web サーバ	・仮想マシンサービス ・ブロックストレージサービス
2000	権威 DNS サーバ	・仮想マシンサービス ・ブロックストレージサービス
3000	日記 DB	・DB サービス
4000	ログ保管ストレージ	・オブジェクトストレージサービス
5000	仮想ネットワーク	・仮想ネットワークサービス

注記　日記サービスでは，モニタリングサービスとアラートサービスを利用する。

W 社は，L 社のクラウドサービスにおける，D 社に付与する権限の検討を開始した。

〔L 社のクラウドサービスにおける権限設計〕

L 社の各クラウドサービスにおける権限ごとに可能な操作を表 6 に示す。

表 6　L 社の各クラウドサービスにおける権限ごとに可能な操作（抜粋）

クラウドサービス名	一覧の閲覧権限	閲覧権限	編集権限
仮想マシンサービス	仮想マシン一覧の閲覧	仮想マシンに割り当てたファイルシステム上のファイルの閲覧	・仮想マシンの起動，停止，削除 ・仮想マシンへのファイルシステムの割当て ・仮想マシンに割り当てたファイルシステム上のファイルの作成，編集，削除 ・仮想マシンの性能の指定
DB サービス	スキーマ一覧及びテーブル一覧の閲覧	テーブルに含まれるデータの閲覧	・テーブルの作成，編集，削除 ・テーブルに含まれるデータの追加，編集，削除
ブロックストレージサービス	生成したストレージ一覧の閲覧	ストレージの使用済み容量及び空き容量の閲覧	・ストレージの生成 ・ストレージの容量の指定
オブジェクトストレージサービス	オブジェクト一覧の閲覧	オブジェクトの閲覧	・オブジェクトの作成，編集，削除 ・オブジェクトのダウンロード
モニタリングサービス	監視している性能指標一覧の閲覧	過去から現在までの性能指標の値の閲覧	・監視する性能指標の追加，削除

W 社は，D 社に付与する権限が必要最小限となるように，表 7 に示す D 社向けの権限のセットを作成した。

表 7　D 社向けの権限のセット（抜粋）

クラウドサービス名	D 社に付与する権限
仮想マシンサービス	j
DB サービス	k
オブジェクトストレージサービス	一覧の閲覧権限，閲覧権限，編集権限
モニタリングサービス	l

さらに，W 社は，①D 社の運用者がシステムから日記サービスのログを削除したときに，そのイベントを検知してアラートをメールで通知するための検知ルールを作成した。

W 社は，L 社とクラウドサービスの利用契約を締結して，日記サービスを L 社のクラウドサービスに移行し，運用を開始した。

〔機能拡張の計画開始〕

W 社は，サービス拡大のために，機能を拡張した日記サービス（以下，新日記サービスという）の計画を開始した。新日記サービスの要件は次のとおりである。

要件 1：会員が記事を投稿する際，他社の SNS にも同時に投稿できること

要件 2：スマートフォン用のアプリ（以下，スマホアプリという）を提供すること

W 社は，要件 1 を実装した後で要件 2 に取り組むことに決めた。その上で，要件 1 を実現するために，T 社の SNS（以下，サービス T という）と連携することにした。

〔サービス T との連携の検討〕

OAuth 2.0 を利用してサービス T と連携した場合のサービス要求から記事投稿結果取得までの流れを図 3 に，送信されるデータを表 8 に示す。

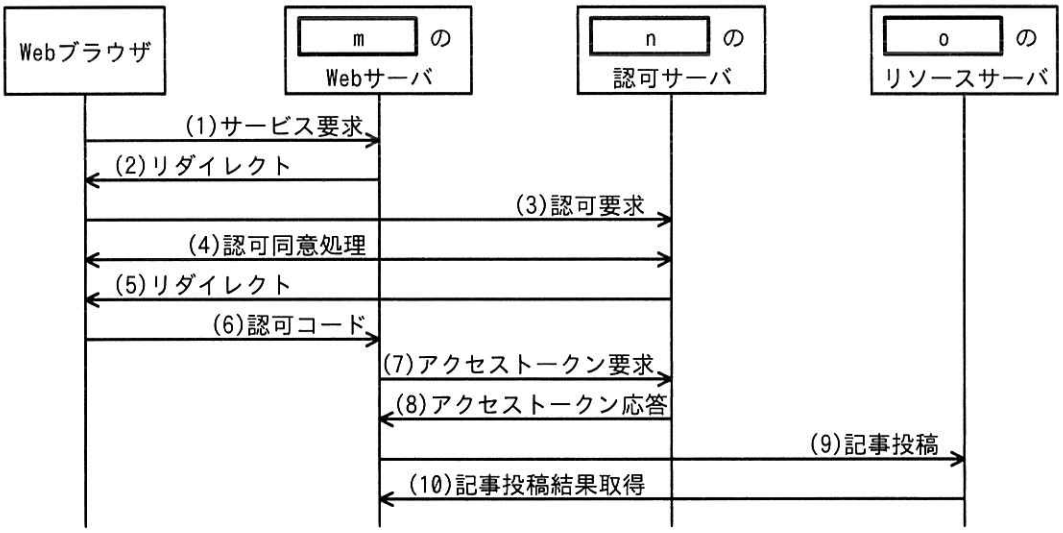


図 3　サービス要求から記事投稿結果取得までの流れ

表8　送信されるデータ（抜粋）

番号	送信されるデータ
p	GET /authorize?response_type=code&client_id=abcd1234&redirect_uri=https://△△△.com/callback HTTP/1.1 [1]
q	POST /oauth/token HTTP/1.1 Authorization: Basic YWJjZDEyMzQ6UEBzc3dvcmQ= [2] grant_type=authorization_code&code=5810f68ad195469d85f59a6d06e51e90&redirect_uri=https://△△△.com/callback

注記　△△△.com は，新日記サービスのドメイン名である。

注 [1]　クエリ文字列中の“abcd1234”は，英数字で構成された文字列であるクライアント ID を示す。

注 [2]　“YWJjZDEyMzQ6UEBzc3dvcmQ=”は，クライアント ID と，英数字と記号で構成された文字列であるクライアントシークレットとを，“:”で連結して base64 でエンコードした値（以下，エンコード値 G という）である。

各リクエストの通信で TLS 1.2 及び TLS 1.3 を利用可能とするために，②暗号スイートの設定をどのようにすればよいかを検討した。また，サービス T との連携のためのモジュール（以下，R モジュールという）の実装から単体テストまでを F 社に委託することにした。F 社は，新技術を積極的に活用している IT 企業である。

〔F 社の開発環境〕

F 社では，R モジュールの開発は，取りまとめる開発リーダー1 名と，実装から単体テストまでを行う開発者 3 名のチームで行う。システム開発において，顧客から開発を委託されたプログラムのソースコードのリポジトリと外部に公開されている OSS リポジトリを利用している。二つのリポジトリは，サービス E というソースコードリポジトリサービスを利用して管理している。

サービス E の仕様と，R モジュールについての F 社のソースコード管理プロセスは，表 9 のとおりである。

表9　サービスEの仕様とF社のソースコード管理プロセス

機能	サービスEの仕様	F社のソースコード管理プロセス
利用者認証及びアクセス制御	・利用者IDとパスワードによる認証，及び他のIdPと連携したSAML認証が可能である。 ・リポジトリごとに，利用者認証の要・不要を設定できる。 ・サービスEは外部に公開されている。 ・IPアドレスなどで接続元を制限する機能はない。	・利用者認証には，F社内で運用している認証サーバと連携した，SAML認証を利用する。 ・Rモジュール開発向けのリポジトリ（以下，リポジトリWという）には，利用者認証を“要”に設定する。
バージョン管理	・ソースコードのアップロード[1)]，承認，ダウンロード，変更履歴のダウンロード，削除が可能である。 ・新規作成，変更，削除の前後の差分をソースコードの変更履歴として記録する。 ・ソースコードがアップロードされ，承認されると，対象のソースコードが新バージョンとして記録され，変更履歴のダウンロードが可能になる。	・開発者は，静的解析と単体テストを実施する。開発者が，それら二つの結果とソースコードをアップロードして，開発リーダーに承認を依頼するルールとする。ただし，静的解析と単体テストについてリスクが少ないと開発者が判断した場合は，開発者自身がソースコードのアップロードとその承認の両方を実施できるルールとする。
権限管理	・設定できる権限には，ソースコードのダウンロード権限，ソースコードのアップロード権限，アップロードされたソースコードを承認する承認権限がある。 ・利用者ごとに，個別のリポジトリの権限を設定することが可能である。 ・変更履歴のダウンロードには，ソースコードのダウンロード権限が必要である。 ・変更履歴の削除には，アップロードされたソースコードを承認する承認権限が必要である。 ・外部のX社が提供している継続的インテグレーションサービス[2)]（以下，X社CIという）と連携するには，ソースコードのダウンロード権限をX社CIに付与する必要がある。	・開発者，開発リーダーなど全ての利用者に対して，設定できる権限全てを与える。
サービス連携	・別のクラウドサービスと連携する際に，権限を付与するトークン（以下，Eトークンという）を，リポジトリへアクセスしてきた連携先に発行することができる。 ・Eトークンの有効期間は1か月である。Eトークンの発行形式や有効期間の変更はできない。	・X社CIと連携する。 ・X社CIに発行するEトークン（以下，Xトークンという）には，リポジトリWの全ての権限が付与されている。

注記　OSSリポジトリには，利用者認証を“不要”に設定している。また，OSSリポジトリのソースコードと変更履歴のダウンロードは誰でも可能である。

注[1)]　ソースコードのアップロードには，関連するファイルの新規作成，変更，削除の操作が含まれる。

注[2)]　アップロードされたソースコードが承認されると，ビルドと単体テストを自動実行するサービスである。

〔悪意のある不正なプログラムコードの混入〕

F 社は，R モジュールの実装について単体テストまでを完了して，ソースコードを W 社に納品した。その後，W 社と T 社は結合テストを開始した。

結合テスト時，外部のホストに対する通信が R モジュールから発生していることが分かった。調べたところ，不正なプログラムコード（以下，不正コード M という）がソースコードに含まれていたことが分かった。不正コード M は，OS の環境変数の一覧を取得し，外部のホストに送信する。新日記サービスでは，エンコード値 G が OS の環境変数に設定されていたので，その値が外部のホストに送信されていた。

W 社は，漏えいした情報が悪用されるリスクの分析と評価を行うことにした。それと並行して，不正コード M の混入の原因調査と，プログラムの修正を F 社に依頼した。

〔W 社によるリスク評価〕

W 社は，リスクを分析し，評価した。評価結果は次のとおりであった。

・エンコード値 G を攻撃者が入手した場合，［ m ］の Web サーバであると偽ってリクエストを送信できる。しかし，図 3 のシーケンスでは，③攻撃者が特定の会員のアクセストークンを取得するリクエストを送信し，アクセストークンの取得に成功することは困難である。

次に，W 社は，近い将来に要件 2 を実装する場合におけるリスクについても，リスクへの対応を検討した。

そのリスクのうちの一つは，スマホアプリのリダイレクトにカスタム URL スキームを利用する場合に発生する可能性がある。W 社が提供するスマホアプリと攻撃者が用意した偽のスマホアプリの両方を会員が自分の端末にインストールしてしまうと，正規のスマホアプリとサーバとのやり取りが偽のスマホアプリに横取りされ，攻撃者がアクセストークンを不正に取得できるというものである。この対策として，PKCE（Proof Key for Code Exchange）を利用すると，偽のスマホアプリにやり取りが横取りされても，アクセストークンの取得を防ぐことができる。

要件 2 を実装する場合のサービス要求から記事投稿結果取得までの流れを図 4 に示す。

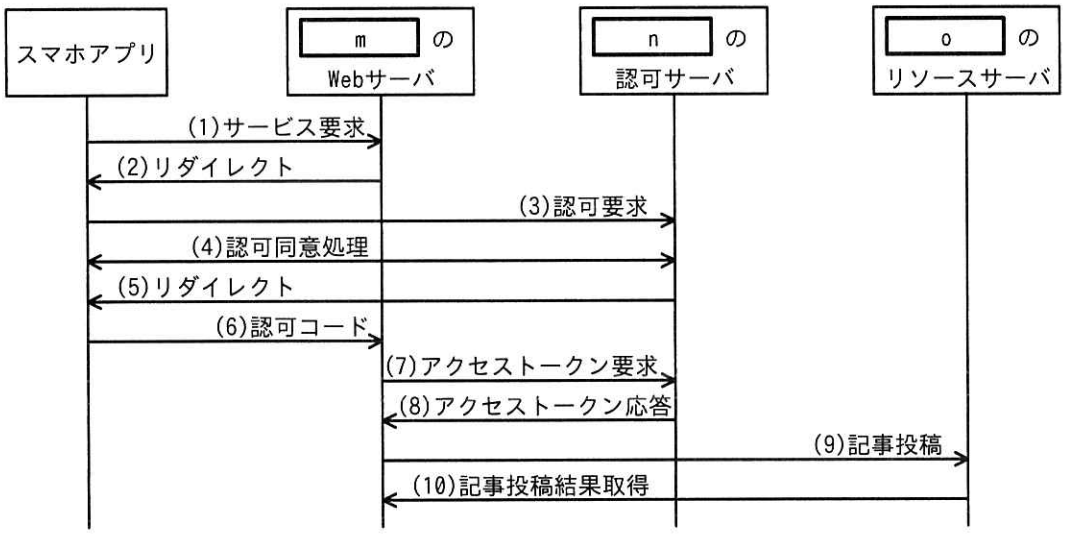


図4　要件2を実装する場合のサービス要求から記事投稿結果取得までの流れ

PKCE の実装では，乱数を基に，チャレンジコードと検証コードを生成する。(3)のリクエストにチャレンジコードと code_challenge_method パラメータを追加し，(7)のリクエストに検証コードパラメータを追加する。最後に，④認可サーバが二つのコードの関係を検証することで，攻撃者からのアクセストークン要求を排除できる。

〔F 社による原因調査〕

F 社は，不正コード M が混入した原因を調査した。調査の結果，サービス E の OSS リポジトリ上に，X トークンなどの情報が含まれるファイル（以下，ファイル Z という）がアップロードされた後に削除されていたことが分かった。

F 社の開発者の 1 人が，ファイル Z を誤ってアップロードし，承認した後，誤ってアップロードしたことに気付き，ファイル Z を削除した上で開発リーダーに連絡していた。開発リーダーは，ファイル Z が OSS リポジトリから削除されていること，ファイル Z がアップロードされてから削除されるまでの間にダウンロードされていなかったことを確認して，問題なしと判断していた。

F 社では，⑤第三者が X トークンを不正に取得して，リポジトリ W に不正アクセスし，不正コード M をソースコードに追加したと推測した。そこで，F 社では，X トークンを無効化し，次の再発防止策を実施した。

・表 9 中のバージョン管理に関わる見直しと⑥表 9 中の権限管理についての変更

・X トークンが漏えいしても不正にプログラムが登録されないようにするための，⑦表 9 中のサービス連携に関わる見直し

ソースコードには他の不正な変更は見つからなかったので，不正コード M が含まれる箇所だけを不正コード M が追加される前のバージョンに復元した。

W 社は，F 社が改めて納品した R モジュールに問題がないことを確認し，新日記サービスの提供を開始した。

設問 1　表 2 中の［ a ］～［ i ］に入れる適切な内容を，“○”又は“×”から選び答えよ。

設問 2　〔L 社のクラウドサービスにおける権限設計〕について答えよ。

(1)　表 7 中の［ j ］～［ l ］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　一覧の閲覧権限，閲覧権限，編集権限

イ　一覧の閲覧権限，閲覧権限

ウ　一覧の閲覧権限

エ　なし

(2)　本文中の下線①のイベント検知のルールを，JSON 形式で答えよ。ここで，D 社の利用者 ID は，1110～1199 とする。

設問 3　〔サービス T との連携の検討〕について答えよ。

(1)　本文中，図 3 中及び図 4 中の［ m ］～［ o ］に入れる適切な字句を，“新日記サービス”又は“サービス T”から選び答えよ。

(2)　表 8 中の［ p ］，［ q ］に入れる適切な番号を，図 3 中の番号から選び答えよ。

(3) 本文中の下線②について，CRYPTREC の“電子政府推奨暗号リスト（令和 4 年 3 月 30 日版)”では利用を推奨していない暗号技術が含まれる TLS 1.2 の暗号スイートを，解答群の中から全て選び，記号で答えよ。

解答群

ア TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

イ TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

ウ TLS_RSA_WITH_3DES_EDE_CBC_SHA

エ TLS_RSA_WITH_RC4_128_MD5

設問４ 〔W 社によるリスク評価〕について答えよ。

(1) 本文中の下線③について，アクセストークンの取得に成功することが困難である理由を，表 8 中のパラメータ名を含めて，40 字以内で具体的に答えよ。

(2) 本文中の下線④について，認可サーバがチャレンジコードと検証コードの関係を検証する方法を，“ハッシュ値を base64url エンコードした値”という字句を含めて，70 字以内で具体的に答えよ。ここで，code_challenge_method の値は S256 とする。

設問５ 〔F 社による原因調査〕について答えよ。

(1) 本文中の下線⑤について，第三者が X トークンを取得するための操作を，40 字以内で答えよ。

(2) 本文中の下線⑥について，権限管理の変更内容を，50 字以内で答えよ。

(3) 本文中の下線⑦について，見直し後の設定を，40 字以内で答えよ。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

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	15:10 ～ 16:20

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。