

問3 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。

D社は、従業員1,000名の小売業である。自社のホームページやECサイトなどのWebサイトについては、Webアプリケーションプログラム（以下、Webアプリという）に対する診断（以下、Webアプリ診断という）を専門会社のZ社に委託して実施している。Webアプリ診断は、Webサイトのリリース前だけではなく、リリース後も定期的に実施している。Z社のWebアプリ診断は、脆弱性診断ツールによるスキャンだけではなく、手動による高度な分析も行う。

[新たなWebサイトの構築]

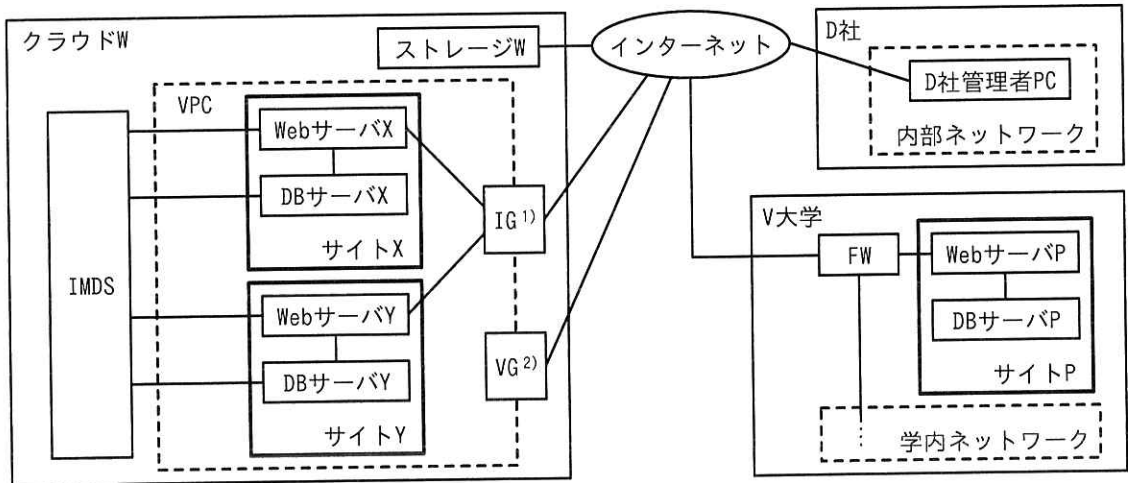
D社では、新たにECサイトX（以下、サイトXという）と商品企画サイトY（以下、サイトYという）をW社が提供するクラウドサービス（以下、クラウドWという）上に構築することになった。

サイトXでは、D社が取り扱う商品をインターネットを介して会員に販売する予定である。取引は毎月10,000件ほどを見込んでいる。サイトYでは、サイトXで販売する新商品の企画・開発を顧客参加型で行う。サイトXとサイトYは、いずれもWebサーバとデータベースサーバ（以下、DBサーバという）で構成する。WebサーバについてはクラウドWの仮想Webサーバサービスを利用し、DBサーバについてはクラウドWのリレーショナルデータベースサービスを利用する。サイトXとサイトYはいずれも、コンテンツマネジメントシステム（以下、CMSという）を使って構築される。サイトXとサイトYにはいずれも、Webアプリ、HTMLによる静的コンテンツ、DBサーバに格納したデータを使った動的コンテンツなどを用意する。

D社は、V大学と新商品開発の共同研究を行っている。新商品開発の共同研究では、V大学が運用する情報交換サイト（以下、サイトPという）を利用している。サイトYは、サイトPで取り扱っている情報などを表示する。

D社は、Webサイト構築に関連するデータやドキュメントの保存場所として、クラウドWのストレージサービス（以下、ストレージWという）を利用する。

D社は、サイトX及びサイトYの設計書を作成した。設計書のうち、サイトX、サイトY及びサイトPのネットワーク構成を図1に、サーバやサービスの説明を図2に示す。



FW : ファイアウォール

IG : インターネットゲートウェイ

IMDS : インスタンスメタデータサービス VG : VPNゲートウェイ VPC : 仮想プライベートクラウド

注¹) VPC とインターネットとの間の通信を可能にする。

注²) VPC と D 社の内部ネットワークとの間の VPN 通信を可能にする。

図 1 サイト X, サイト Y 及びサイト P のネットワーク構成

[クラウド W にあるサーバ及びストレージ W について]

クラウド W 上のサービスの管理のためのアクセスの際は、クラウド W 用の利用者 ID、アクセスキーなどのクレデンシャル情報をリクエストに含める必要がある。D 社が利用するクラウド W 上のサービスには、D 社用に発行されたクレデンシャル情報でアクセスでき、全ての操作ができる。

[IMDS について]

IMDS は、VPC の各サーバから特定の URL にアクセスされると特定の情報を返す。例えば、<https://000.000.000.000/meta-data/credential> に GET メソッドでアクセスされると、クラウド W 上のサービスのクレデンシャル情報を返す。IMDS には、インターネットから直接アクセスできないプライベート IP アドレス (000.000.000.000) が設定されている。

IMDS にアクセスする方式は、次のいずれかを採用する必要がある。D 社では、方式 1 を採用する。
 方式 1 : 特定の URL にアクセスするだけで情報を取得できる。

方式 2 : トークンを発行する URL に PUT メソッドでアクセスし、レスポンスボディに含まれるトークンを入手してから、そのトークンをリクエストヘッダに含めて特定の URL にアクセスすると情報を取得できる。

[CMS について]

Web サーバ X の <https://□□□.jp/admin> 又は Web サーバ Y の <https://■■■.jp/admin> にアクセスすると、それぞれのサーバの CMS の管理ログイン画面にアクセスできる。ログインは、POST メソッドでは許可されるが、GET メソッドでは許可されない。各 CMS の管理ログイン画面へのアクセスは、VPN 接続された D 社管理者 PC、又は VPC 内からのアクセスだけに制限される。D 社では、各 CMS の管理者アカウントは初期パスワードのまま運用する。

図 2 サーバやサービスの説明

[サイト X]

サイト X には、会員用の利用者アカウントと D 社管理者用の利用者アカウントがある。サイト X のログインセッション管理は、cookie パラメータの SESSIONID で行う。SESSIONID には、値と Secure 属性だけがセットされる。なお、サーバ側のセッションの有効期間は 24 時間である。設計書のうち、サイト X の機能一覧を表 1 に示す。

表 1 サイト X の機能一覧 (抜粋)

項番	機能	詳細機能	機能概要
1	ログイン機能	ログイン機能	利用者 ID とパスワードを入力し、ログインに成功すると利用できる機能が表示されるページに遷移する。
2	利用者機能 (ログイン前)	会員機能 (登録)	登録画面では最初にメールアドレスを入力する。そのメールアドレス宛てに送られた電子メールに記載された URL にアクセスして利用者情報を入力し、登録する。
3	利用者機能 (ログイン後)	注文機能 (商品検索, 注文, 注文履歴閲覧)	商品には商品コードが付与されており、商品検索画面で検索できる。注文履歴は、注文年月である数字 6 桁とランダムな英大文字 6 桁の値をハイフンでつないだ注文管理番号で管理される。注文履歴を閲覧する際は、注文管理番号を基に検索する。
4		会員機能 (編集)	登録した利用者情報を編集できる。
5		問合せ機能	問合せ情報を入力できる。入力した問合せ情報は、数字 10 桁の管理番号が発番され、管理される。
6	サイト管理機能 (ログイン後)	商品管理機能 (登録, 編集, 削除)	商品情報を登録, 編集, 削除できる。商品情報が登録されると、数字 10 桁の商品コードが割り当てられ、その商品を会員が注文できるようになる。
7		売上管理機能 (売上情報閲覧, 検索)	商品の売上情報を閲覧できる。また、条件を指定して検索することができる。
8		会員管理機能 (閲覧, 変更, 削除)	登録された会員の利用者情報を閲覧, 変更, 削除できる。
9		問合せ管理機能	問合せ機能で入力された問合せ情報が閲覧できる。

サイト管理機能は、D 社の内部ネットワーク以外からも利用する可能性があり、サイト X では、接続元の制限は行わない。

サイト X とサイト Y の構築は順調に進み、D 社はリリース前の Web アプリ診断を Z 社に委託した。Z 社は、サイト X とサイト Y それぞれに対して Web アプリ診断を実施した。

[サイト X に対する Web アプリ診断]

サイト X に対する Web アプリ診断では、次の三つの脆弱性が検出された。

- ・クロスサイトスクリプティング（以下、XSS という）
- ・クロスサイトリクエストフォージェリ（以下、CSRF という）
- ・認可制御の不備

[XSS について]

Z 社が XSS を検出した経緯は、次のとおりであった。

- (1) 問合せ機能で、脆弱性診断ツールによるリクエストとレスポンスを確認した。

このときのリクエストとレスポンスは、図 3 のとおりであった。

[リクエスト]

POST /shop/contact HTTP/1.1

Host: (省略)

(省略)

Content-Type: application/x-www-form-urlencoded

Content-Length: (省略)

Cookie: SESSIONID=nt1t3dmxmlmwuicyiz3h4nq1

subject_id=004&name=%22%3e%3cscript%3ealert%281%29%3c%2fscript%3e%3c%22&tel=(省略) &mail=(省略) &mail2=(省略) &comment=(省略)

[レスポンス]

(省略)

<h1>問合せを受け付けました。</h1>

(省略)

注記 パラメータ name の値は ”<script>alert(1)</script>” を URL エンコードした値である。

図 3 問合せ機能のリクエストとレスポンス

(2) 図 3 中のレスポンスボディには、問合せ機能で入力した値は出力されていない。しかし、Z 社は、①設計書を調査した上で手動による分析を行い、図 3 中のリクエスト内のスクリプトが別の機能の画面に出力されることを確認した。

Z 社は、②攻撃者がこの XSS を悪用してサイト X 内の全会員の利用者情報を取得する可能性があると説明した。

[CSRF について]

Z 社が CSRF を検出した経緯は、次のとおりであった。

(1) 会員機能（編集）において、図 4 に示すリクエストを送ってその応答を確認した。リクエストは正常に処理された。

```
POST /shop/editmember HTTP/1.1
Host: (省略)
(省略)
Content-Type: application/x-www-form-urlencoded
Content-Length: (省略)
Cookie: SESSIONID=b9y33f89umt6uua1pe4j4jn7

sei=sato&mei=taro&mail=aaa%40example.jp&csrf_token=KCRQ88ERH2G8MGT319E50SMOAJFDIVEM
```

図 4 会員機能（編集）のリクエスト

(2) リクエスト内のメッセージボディの一部を変更して送り、その応答を確認した。リクエスト内のメッセージボディと応答は表 2 のとおりであった。

表 2 リクエスト内のメッセージボディと応答

手順	リクエスト内のメッセージボディ	応答
1	sei=sato&mei=taro&mail=aaa%40example.jp&csrf_token=	エラー
2	sei=sato&mei=taro&mail=aaa%40example.jp	エラー
3	sei=sato&mei=taro&mail=aaa%40example.jp&csrf_token=（異なる利用者アカウントで取得した csrf_token の値）	正常に処理

- (3) Z社は、手順1, 2の応答が“エラー”であることから一定のCSRF対策ができて
いるが、手順3の応答が“正常に処理”であることから③利用者に被害を与える
可能性がある」と判断した。

Z社は、対策には二つの方法があることを説明した。

- ・ csrf_token の処理の修正
- ・ cookie への SameSite 属性の追加

サイトXの構成次第では、SameSite属性をcookieに付与することも有効な対策と
なり得る。SameSite属性は、Strict, Lax, Noneの三つの値のうちのいずれかを取る。
サイトXにログインした利用者のWebブラウザにおいて、サイトX内で遷移する場合
と外部WebサイトからサイトXに遷移する場合は、SameSite属性の値によってサイ
トXのcookie送信の有無が表3のように異なる。

表3 SameSite属性の値の違いによるcookie送信の有無

SameSite 属性の値	サイトX内で遷移		外部WebサイトからサイトXに遷移	
	GET	POST	GET	POST
Strict	○	○	a	b
Lax	○	○	c	d
None	○	○	(省略)	(省略)

注記 “○”はcookieが送られることを示す。“×”はcookieが送られないことを示す。

〔認可制御の不備について〕

Z社が認可制御の不備を検出した経緯は、次のとおりであった。

- (1) Z社は、利用者 α 、利用者 β という二つの利用者アカウントを用いて、注文履
歴を閲覧した際のリクエストを確認した。注文履歴を閲覧した際のリクエストを
図5及び図6に示す。

```
POST /shop/order-history HTTP/1.1
Host: (省略)
(省略)
Content-Type: application/x-www-form-urlencoded
Content-Length: (省略)
Cookie: SESSIONID=ac9t66bxlxmwuiiki53h4nq3

order-code=202404-AHUJKI 1)
```

注 ¹⁾ 表 1 の注文管理番号のことである。値から利用者を特定することができる。

図 5 利用者 α で注文履歴を閲覧した際のリクエスト

```
POST /shop/order-history HTTP/1.1
Host: (省略)
(省略)
Content-Type: application/x-www-form-urlencoded
Content-Length: (省略)
Cookie: SESSIONID=k1ctghbxbx5wuj3ki33hlnq5

order-code=202404-BAKCXW
```

図 6 利用者 β で注文履歴を閲覧した際のリクエスト

- (2) 図 5 のリクエストのパラメータ order-code の値を図 6 中の値に改変してリクエストを送った。
- (3) 利用者 α が、本来は閲覧できないはずの利用者 β の注文履歴を閲覧できるという攻撃が成功することを確認した。
- (4) さらに、ある利用者がほかの利用者が注文した際の order-code を知らなくても、④ある攻撃手法を用いれば攻撃が成功することを確認した。

Z 社は、⑤サイト X の Web アプリに追加すべき処理を説明した。

[サイト Y に対する Web アプリ診断]

サイト Y に対する Web アプリ診断では、次の脆弱性が検出された。

- ・サーバサイドリクエストフォージェリ (以下、SSRF という)

[SSRF について]

Z 社が SSRF を検出した経緯は、次のとおりであった。

- (1) サイト P の新着情報を取得する際に、利用者の Web ブラウザが Web サーバ Y に送るリクエストを確認したところ、図 7 のとおりであった。

```
GET /top?page=https://△△△.jp/topic/202404.html HTTP/1.1
Host: (省略)
(省略)
Cookie: SESSIONID=pq4ikd31op215jebter41sae
```

注記 △△△.jp はサイト P の FQDN である。

図 7 利用者の Web ブラウザが Web サーバ Y に送るリクエスト

- (2) ⑥図 7 のリクエストのパラメータの値を Web サーバ Y の CMS の管理ログイン画面の URL に変更することで、その画面にアクセスできるが、ログインはできないことを確認した。
- (3) ⑦図 7 のリクエストのパラメータの値を別の URL に変更するという方法（以下、方法 F という）で SSRF を悪用して、クレデンシャル情報を取得し、ストレージ W から情報を盗み出すことができることを確認した。
- (4) IMDS にアクセスする方式を方式 1 から方式 2 に変更すると、方法 F ではクレデンシャル情報を取得できないので、ストレージ W から情報を盗み出すことができない。しかし、図 7 のリクエストのパラメータの値を変更することで、Web サーバ Y から送られるリクエストに任意のメソッドの指定及び任意のヘッダの追加ができる方法（以下、方法 G という）がある。方法 G を用いれば、方式 2 に変更しても、⑧クレデンシャル情報を取得し、ストレージ W から情報を盗み出すことができることを確認した。

Z 社は、クラウド W 上のネットワークでのアクセス制御の設定、及び⑨サイト Y の Web アプリに追加すべき処理を提案した。

リリース前の脆弱性診断で検出された脆弱性の対策が全て完了し、サイト X とサイト Y は稼働を開始した。

設問1 [XSS について] について答えよ。

- (1) 本文中の下線①について、図 3 中のリクエスト内のスクリプトが出力されるのはどの機能か。表 1 の詳細機能に対する項番を選び答えよ。
- (2) 本文中の下線②について、攻撃者はどのような手順で利用者情報を取得するか。具体的に答えよ。

設問2 [CSRF について] について答えよ。

- (1) 本文中の下線③について、被害を与える攻撃の手順を、具体的に答えよ。
- (2) 表 3 中の ~ に入れる適切な内容を、“○” 又は “×” から選び答えよ。

設問3 [認可制御の不備について] について答えよ。

- (1) 本文中の下線④について、どのような攻撃手法を用いれば攻撃が成功するか。30 字以内で答えよ。
- (2) 本文中の下線⑤について、サイト X の Web アプリに追加すべき処理を、60 字以内で具体的に答えよ。

設問4 [SSRF について] について答えよ。

- (1) 本文中の下線⑥について、ログインができないのはなぜか。SSRF 攻撃の特徴を基に、35 字以内で答えよ。
- (2) 本文中の下線⑦について、クレデンシャル情報を取得する方法を、具体的に答えよ。
- (3) 本文中の下線⑧について、方法 G を用いてクレデンシャル情報を取得する方法を、具体的に答えよ。
- (4) 本文中の下線⑨について、サイト Y の Web アプリに追加すべき処理を、35 字以内で具体的に答えよ。