SC

令和４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サイトのセキュリティに関する次の記述を読んで，設問1～6に答えよ。

A社は，従業員1,500名の中堅システム開発会社である。A社では，セキュリティ品質の高いWebサイトを開発するために，表1に示すWebセキュリティ管理基準を定めて運用している。

表1　Webセキュリティ管理基準（抜粋）

項番	管理策	概要
1	セキュリティ要件レビュー	・概要設計，基本設計，詳細設計それぞれの設計レビューにおいて，Webサイトに関するセキュリティ要件をレビューする。
2	ツールによるソースコードレビュー	・Webサイトのリリースまでに実施する。 ・期間は，3日間くらいが目安である。 ・開発環境の特性などが原因で実施できない場合，項番3を行う。 ・ツールが検出した指摘事項について，開発担当者は，脆弱性かどうか，対策が必要かどうかを判断する。 ・セッション管理の脆弱性は，一部だけが対象である。 ・認可・アクセス制御の脆弱性は，対象外である。
3	プロジェクトメンバによるソースコードレビュー	・項番2が実施できない場合，Webサイトのリリースまでに実施する。 ・期間は，10日間くらいが目安である。 ・A社の指定した既知の脆弱なコードパターンを見つける。 ・レビューでの指摘事項について，開発担当者は，脆弱性かどうか，対策が必要かどうかを判断する。 ・セッション管理の脆弱性は，一部だけが対象である。 ・認可・アクセス制御の脆弱性は，対象外である。
4	ツールによる脆弱性診断	・Webサイトのリリースまでに実施する。 ・期間は，3日間くらいが目安である。 ・Webサイトをテスト環境で稼働させ，ツールでWebサイトに様々なHTTPリクエストを送り，その応答を評価する。 ・ツールが検出した指摘事項について，開発担当者は，脆弱性かどうか，対策が必要かどうかを判断する。 ・セッション管理の脆弱性は，一部だけが対象である。 ・認可・アクセス制御の脆弱性は，対象外である。
5	専門技術者による脆弱性診断	・Webサイトのリリースまでに実施する。 ・期間は，10日間くらいが目安である。 ・専門会社[1]に委託する。 ・Webサイトをテスト環境で稼働させ，Webサイトに様々なHTTPリクエストを送り，その応答を評価する。 ・診断による指摘事項について，専門技術者と開発担当者は，対策が必要かどうかを協議して判断する。 ・セッション管理の脆弱性は，対象である。 ・認可・アクセス制御の脆弱性は，対象である。

注[1]　脆弱性診断サービスを提供しているD社に委託している。

〔A 社による B 社の子会社化〕

B 社は，従業員 200 名の新興の IT サービス会社であり，各種 SaaS を提供している。アジャイル開発の能力が高く，機能の追加や性能の改善を頻繁に行っている。B 社と A 社とは協業関係にあったが，両社の経営陣は，双方の強みを生かせると判断し，A 社による B 社の子会社化について合意した。

B 社のクラウド環境には，コーポレートサイト（以下，サイト B という），及び B 社が提供中の三つの SaaS それぞれの Web サイト（以下，サイト X，サイト Y，サイト Z という）がある。それらの概要を表 2 に示す。

表 2　B 社の Web サイトの概要

サイト名及び URL	概要	システム構成
サイト B https://www.b-sha.co.jp/	・B 社に関する情報を発信している。 ・コンテンツマネジメントシステム（CMS）を導入し，運用している。	IaaS 上の Web サーバで構成されている。
サイト X https://x.b-sha.co.jp/	・会社又は組織向けのコミュニケーションサービスであり，利用する会社間又は組織間で，情報共有やチャットが行える。 ・利用する会社又は組織は，B 社の提携企業の新商品のモニターになると，“キャンペーン応募”をサイト X で行える。	IaaS 上の Web サーバ及びデータベースサーバ 1)（以下，DB サーバという）で構成されている。
サイト Y https://y.b-sha.co.jp/	・個人向けのブログサイトであり，利用者が情報を発信できる。 ・“A 社のニューストピック”を表示できる。	
サイト Z https://z.b-sha.co.jp/	・ソフトウェア開発企業向けの Web サービスである。利用者はグループを作ることができ，そのグループ内で，スケジュール，タスク，ソースコードなどのプロジェクト情報を共有できる。 ・外部の Web サイトと連携して，経費精算，出張申請などの業務手続を行う機能を提供予定である。	

注 1)　DB サーバには，B 社のシステム担当者と，それぞれのサイトの Web サーバとがアクセスできる。各 DB サーバには，レコードの更新や削除が簡単にできるメンテナンス用の Web インタフェースがある。その URL を次に示す。

・サイト X の DB サーバ：https://db-x.b-sha.co.jp/
・サイト Y の DB サーバ：https://db-y.b-sha.co.jp/
・サイト Z の DB サーバ：https://db-z.b-sha.co.jp/

子会社化に当たって，B 社の Web サイトのセキュリティ水準を確認することになり，A 社の品質管理部でセキュリティ技術を担当している R さんが対応することになった。

〔B 社の Web サイトのセキュリティ水準の確認〕

R さんは，サイト B，サイト X，サイト Y 及びサイト Z に対する脆弱性診断を D 社に依頼した。診断の結果，検出された脆弱性を表 3 に示す。

表 3　検出された脆弱性（抜粋）

サイト名	脆弱性名
サイト B	・クロスサイトスクリプティング（以下，XSS という）脆弱性
サイト X	・XSS 脆弱性 ・クロスサイトリクエストフォージェリ（以下，CSRF という）脆弱性 ・クリックジャッキング脆弱性
サイト Y	・XSS 脆弱性 ・サーバサイドリクエストフォージェリ（以下，SSRF という）脆弱性
サイト Z	・XSS 脆弱性 ・SSRF 脆弱性

〔サイト B の XSS 脆弱性〕

D 社は，サイト B に①診断用リクエストを送ることで，XSS 脆弱性があることを確認した。このリクエストは，ライブラリ M を使ってプログラム C が処理する。ライブラリ M のコードを図 1 に示す。

```
   (省略)
1:  out.println("<meta property=\"og:url\" content=\"https://"+serverName+"/"
   +scriptName+"?"+queryString+"\">");
   (省略)
```

注記　serverName には，リクエストの URL のホスト名が格納されている。scriptName には，URL のパス名が格納されている。queryString には，URL のクエリ文字列以降の値が URL デコードされて格納されている。

図 1　ライブラリ M のコード

ライブラリ M は，SEO のためのライブラリである。

B 社では，開発部のメンバそれぞれが，開発時に利用可能なライブラリを収集している。使用するライブラリは，マルウェアが含まれていない，既知の脆弱性が修正された，安全性が確認できているライブラリを公開している Web サイトから，ファイルサーバにダウンロードし，利用している。ファイルサーバは，開発部のメンバであればアクセス可能である。

今回使われていたライブラリ M は，既知の XSS 脆弱性の対策をしていないバージョンであった。その結果，ライブラリ M を使っているサイト B，サイト X，サイト Y 及びサイト Z において，同じ XSS 脆弱性が検出された。

これを受けて，B 社における②再発防止策について検討した。

〔サイト X の CSRF 脆弱性〕

サイト X は，セッション ID を JSESSIONID という cookie に格納している。D 社は，サイト X のキャンペーン応募ページで CSRF 脆弱性を検出した。

CSRF 脆弱性を確認した手順は，次のとおりであった。

(1) 診断用利用者（以下，利用者 A という）の利用者 ID でサイト X にログインし，キャンペーン応募ページで送信されるリクエストの内容をツールを使って確認した。リクエストの内容を図 2 に示す。

```
POST /campaign HTTP/1.1
Host: x.b-sha.co.jp
Cookie: JSESSIONID=KCRQ88ERH2G8MGT319E5OSMOAJFDIVEM

csrftoken=3f4aee446f680df6e0842d7179fcefd00fe5b232
```

注記 1 リクエストヘッダ部分は，設問に必要なものだけを記載している。
注記 2 JSESSIONID について，SameSite 属性は指定されていない。
注記 3 csrftoken の値は，サーバが発行する推測困難な値であり，ほかの利用者の利用時には別の値が発行される。
注記 4 リクエストを送るとトークンが破棄される可能性があるので，リクエストの内容は，ツールで確認しただけであり，実際にはサイト X に届いていない。

図 2　リクエストの内容

リクエストの内容を確認後，csrftoken を CSRF 対策用のパラメタと考え，リクエスト中の csrftoken の値を削除して送信した場合と 1 文字変更して送信した場合を試したところ，どちらもエラーになった。

(2) 利用者 A とは別の診断用利用者（以下，利用者 B という）の利用者 ID でサイト X にログインし，キャンペーン応募ページで送信されるリクエスト中の csrftoken の値に，図 2 の csrftoken の値を設定して送信したところ，利用者 B として処理された。

この結果から，csrftoken と［ a ］又は［ b ］とをひも付けるという対策ができていないことが分かった。

〔サイトXのクリックジャッキング脆弱性〕

サイトXでは，クリックジャッキングによって，利用者が気付かずに利用者情報の公開範囲を変更させられてしまう脆弱性が検出された。攻撃者が図3の画面を用いてクリックジャッキングを行う場合を仮定してみる。このとき，クリックイベントは，利用者から見て手前にある画面上で発生するものとする。

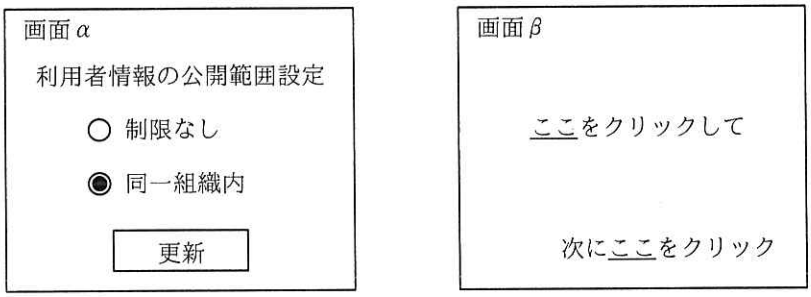


図3　攻撃者が用いる画面

攻撃者は，画面［ c ］を利用者から見て［ d ］に［ e ］状態で罠（わな）サイトに公開し，サイト X の画面［ f ］を利用者から見て［ g ］に［ h ］状態で重ねて表示する。この状態のサイトにアクセスした利用者は，意図せず利用者情報の公開範囲を変更させられてしまう可能性がある。

クリックジャッキング脆弱性の対策には，レスポンスヘッダに［ i ］を含める方法と［ j ］を含める方法がある。後者は標準化されている。

〔サイトYのSSRF脆弱性〕

サイトYでは，例えば，図4のリクエストを受け取ると，A社のニューストピックを取得し，表示するようになっている。

```
GET /news?topic=https://www.a-sha.co.jp/news/20220417.html HTTP/1.1
（省略）
```

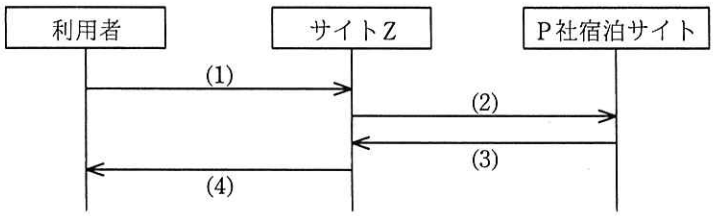
注記　topic パラメタに A 社のニューストピックの URL を指定している。

図4　A社のニューストピックを取得するリクエスト

この処理にSSRF脆弱性があった。D社は，③図4のリクエスト中の値を変更してサイトYに送り，サイトYのDBサーバのメンテナンス用のWebインタフェースにアクセスできることを確認した。

〔サイトZのSSRF脆弱性〕

サイトZでは，最近，新機能が開発された。新機能の一つである，旅行会社P社の宿泊サイト（以下，P社宿泊サイトという）との連携機能でSSRF脆弱性が検出された。その機能は，駅名を入力すると，その駅近辺のホテルの割引クーポンなどの“お得情報”を表示できるというものである。利用者が，P社宿泊サイトに登録されている駅名の一つ，“東京”を入力したときの流れを図5に，登録されていない架空の駅名である“abc”を入力したときの流れを図6に，D社の専門技術者V氏がSSRF脆弱性を検出した手順を表4に示す。



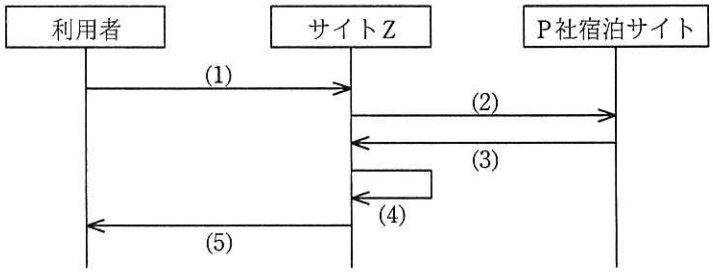
番号	送信されるデータ
(1)	“東京”駅近辺の“お得情報”を取得するリクエスト[1)] GET /station/%E6%9D%B1%E4%BA%AC HTTP/1.1 Host: z.b-sha.co.jp
(2)	“東京”駅近辺の“お得情報”を取得するリクエスト[1) 2)] GET /station/%E6%9D%B1%E4%BA%AC?returnURL=https://z.b-sha.co.jp/error HTTP/1.1 Authorization: Basic （省略）
(3)	“東京”駅近辺の“お得情報”
(4)	“東京”駅近辺の“お得情報”を含むページ

注記　送信されるデータのリクエストヘッダ部分は，一部省略している。

注[1)]　リクエストURIには，“/station/▲▲▲▲▲”の形式で，▲▲▲▲▲に駅名をURLエンコードした値を指定する。

注[2)]　returnURLには，登録されていない駅名が入力されたときに利用されるURLを指定する。サイトZは，(1)のHostヘッダの値を，returnURL中のホスト名として指定する。

図5　登録されている駅名である“東京”を入力したときの流れ



番号	送信されるデータ
(1)	“abc”駅近辺の“お得情報”を取得するリクエスト GET /station/abc HTTP/1.1 Host: z.b-sha.co.jp
(2)	“abc”駅近辺の“お得情報”を取得するリクエスト GET /station/abc?returnURL=https://z.b-sha.co.jp/error HTTP/1.1 Authorization: Basic （省略）
(3)	“abc”駅が登録されていなかったことを知らせるレスポンス HTTP/1.1 301 MOVED PERMANENTLY
(4)	サーバ上にあるエラーページのテンプレート情報 GET /error HTTP/1.1
(5)	登録されていない駅名が入力されたことを示すエラーページ

注記　送信されるデータのリクエストヘッダ部分は，一部省略している。

図6　登録されていない駅名である“abc”を入力したときの流れ

表4　SSRF 脆弱性を検出した手順

順序	手順
1	P社宿泊サイトに登録されていない駅名，例えば，“abc”を入力し，Host ヘッダの値を，V氏が用意したサイトの FQDN に変更して，サイト Z にリクエストを送る。
2	サイト Z は，P 社宿泊サイトに，“/station/abc”をリクエスト URI に指定したリクエストを送る。
3	P 社宿泊サイトは，Location ヘッダに［　k　］の URL を含めたレスポンスをサイト Z に返す。
4	サイト Z は，受け取ったレスポンスを基に，［　k　］にリクエストを送る。

表4の手順によって，V氏は，Authorization ヘッダの値を受け取ることができた。P社の協力の下，この値を用いることで，本来許可なしではアクセスできないP社宿泊サイトや同じ Authorization ヘッダの値を利用する P 社保有のサーバへのアクセスが可能になることを確認した。

D 社からは，P 社宿泊サイトからのレスポンスに含まれる URL が想定されたもの

かを調べて想定外の値の場合はその URL にはアクセスしないようにするという，SSRF 脆弱性への対策が提案された。加えて，④別の対策も実施することが望ましいとのことであった。

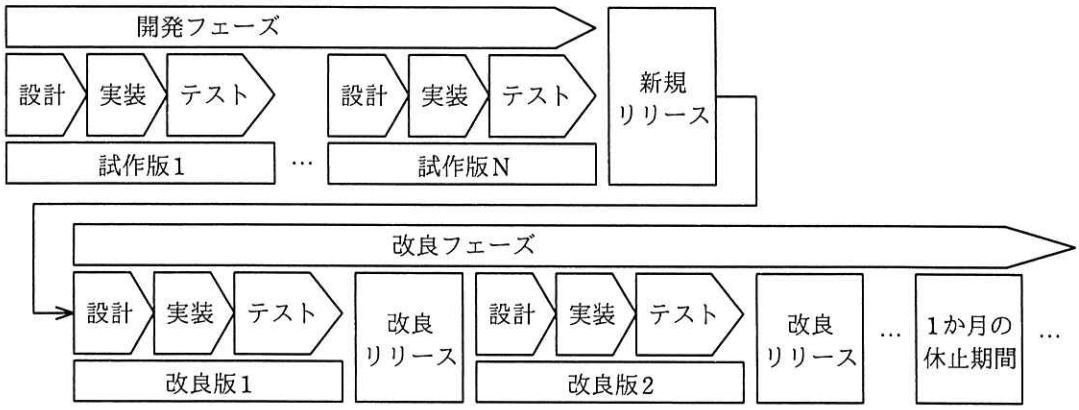
R さんは，D 社の脆弱性診断で検出された脆弱性について，B 社の開発部の E 課長に報告した。その後，B 社の開発部によって対策が実施され，D 社による再度の脆弱性診断で問題が修正されたことが確認された。

〔開発プロセスの見直し〕

B 社の Web サイトのセキュリティ水準について，R さんは，開発プロセスの観点からも調査を進めた。

B 社では，顧客に機能の追加要望や性能の改善要望をヒアリングしながら，開発部内で目標を設定し，アジャイル開発を行っている。また，社外の研修などでセキュアプログラミングの知識を習得し，その知識を生かして Web サイトを開発している。

B 社の開発プロセスの概要を図 7 に示す。



注記 1 ライブラリの活用などで 2 週間周期での改良リリースを実現しているが，およそ 20 回に 1 回は大規模な改修があり，改良リリース間隔を 1 か月とすることがある。

注記 2 改良フェーズにおいて，半年に 1 回，1 か月の休止期間を設けている。その間，開発部のメンバは，長期休暇の取得，長期研修の受講，Web サイトの点検などを実施している。

図 7　B 社の開発プロセスの概要

Rさんは，B社のWebサイトのセキュリティ水準を十分なものにするためには，A社のようなWebセキュリティ管理基準をB社に導入する必要があると考えた。次は，B社の開発プロセスについてのRさんとE課長の会話である。

Rさん：B社でも表1のとおりに実施できますか。

E課長：開発フェーズにおいてはできると思います。しかし，改良リリースの周期は2週間程度です。専門技術者による脆弱性診断には，その周期の大半を費やしてしまうので，省略できないでしょうか。

Rさん：⑤ソースコードレビューやツールによる脆弱性診断では発見できないが，専門技術者による脆弱性診断では発見できる脆弱性が多くあります。専門技術者による脆弱性診断を改良リリースにおいて毎回実施できない場合でも，当該診断が長期間行われないことを避けるために，⑥時期を決めて実施することや，⑦開発プロセスを見直すことを検討してみてください。

E課長：分かりました。そのほかに，アジャイル開発に合った脆弱性対策はないでしょうか。

Rさん：Webサイトの実装に必要となる一般的な機能や定型コードを，ライブラリとしてあらかじめ用意したフレームワークには，⑧脆弱性対策が組み込まれていて，それがデフォルトで有効になっているものもあるので，利用を検討してみてください。

その後，B社は，セキュリティを考慮したアジャイル開発を行うことになった。

設問1　〔サイトBのXSS脆弱性〕について，(1)，(2)に答えよ。

(1) 本文中の下線①における診断用リクエストの構成要素を，解答群の中から選び，記号で答えよ。

解答群

ア　リクエストライン：GET /confirm?"><img src=1 onerror=alert(1)><"

イ　リクエストライン：GET /confirm?><img src=1 onerror=alert(1)><"

ウ　リクエストライン：POST /confirm

　　リクエストボディ："><img src=1 onerror=alert(1)><"

エ　リクエストライン：POST /confirm

　　リクエストボディ：><img src=1 onerror=alert(1)><"

(2) 本文中の下線②について，考えられる再発防止策を，35字以内で述べよ。

設問2　本文中の［　a　］，［　b　］に入れる適切な字句を答えよ。

設問3　〔サイトXのクリックジャッキング脆弱性〕について，(1)，(2)に答えよ。

(1) 本文中の［　c　］～［　h　］に入れる適切な字句を，それぞれの解答群の中から選び，記号で答えよ。

c，fに関する解答群

ア　α　　イ　β

d，gに関する解答群

ア　奥　　イ　手前

e，hに関する解答群

ア　可視の　　イ　透明な

(2) 本文中の［　i　］，［　j　］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　Content-Disposition　　イ　Content-Security-Policy

ウ　X-Content-Type-Options　　エ　X-Frame-Options

設問4　本文中の下線③について，図4のリクエスト中のどの値をどのような値に変更したか。45字以内で具体的に述べよ。

設問5　〔サイトZのSSRF脆弱性〕について，(1)，(2)に答えよ。

(1) 表4中の［　k　］に入れる適切な字句を，15字以内で答えよ。

(2) 本文中の下線④について，別の対策とは何か。B社で実施することが望ましい対策を，25字以内で述べよ。

設問6　〔開発プロセスの見直し〕について，(1)～(4)に答えよ。

(1) 本文中の下線⑤について，該当する脆弱性を二つ挙げ，それぞれ15字以内で答えよ。

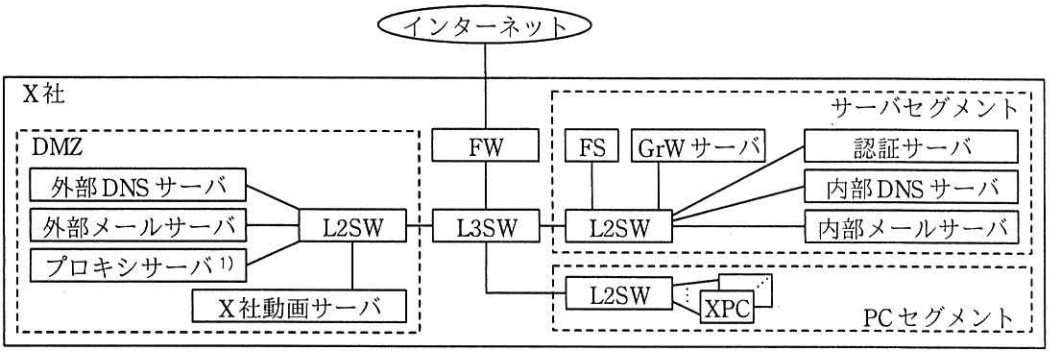
(2) 本文中の下線⑥について，専門技術者による脆弱性診断が長期間行われないことを避けるためには，どのような時期に実施すればよいか。改良リリースの実施に影響を与えないことを前提に，20字以内で答えよ。

(3) 本文中の下線⑦について，専門技術者による脆弱性診断が長期間行われないことを避けるためには，開発プロセスをどのように見直せばよいか。アジャイル開発の継続を前提に，40字以内で述べよ。

(4) 本文中の下線⑧について，CSRF脆弱性の場合では，どのような処理を行う機能が考えられるか。その処理を，55字以内で具体的に述べよ。

問2　クラウドサービスへの移行に関する次の記述を読んで，設問1～5に答えよ。

X社は，従業員500名の情報サービス会社であり，5年前から動画投稿配信サービス（以下，動画サービスという）を提供している。動画サービスは，アカウント登録した会員が動画を投稿したり，投稿された動画を閲覧して評価したりすることができるサービスである。動画サービスは，Webサーバ（以下，動画サービスを提供するWebサーバをX社動画サーバという）を用いて提供されている。X社のシステム部は，X社のシステム全てを管理している。X社のシステム構成を図1に示す。



FW：ファイアウォール　　L2SW：レイヤ2スイッチ　　GrW：グループウェア
FS：ファイルサーバ　　L3SW：レイヤ3スイッチ　　XPC：会社貸与の業務PC
注1)　拒否リストに登録したFQDNを宛先とする通信を遮断する機能がある。

図1　X社のシステム構成

XPCには，Webブラウザ，電子メール（以下，メールという）ソフト，GrW用クライアントソフトなどが導入されている。X社の従業員の認証は，認証サーバで行われており，XPC，GrWサーバ，FS，内部メールサーバへのシングルサインオン（以下，シングルサインオンをSSOという）を実現している。

X社のシステムでは，動画サービスの人気上昇による会員の増加に伴い，X社動画サーバの負荷が高くなっており，インターネット回線もひっ迫している。

X社の経営陣は，この問題への対策と併せて，セキュリティを強化するための抜本的な対策を検討するようシステム部に指示した。システム部のCさんが担当に指名され，セキュリティサービスを提供するW社から情報処理安全確保支援士（登録セキスペ）のF氏を招き，助言を受けることになった。

〔抜本的な対策の検討〕

F 氏は，X 社動画サーバをクラウドサービスへ移行し，さらに，Content Delivery Network（CDN）を利用する案を図 2 のように提案した。

1　X 社動画サーバのクラウドサービスへの移行
　コンピュータリソースを柔軟に増強できるようにするため，X 社動画サーバをクラウドサービス事業者の IaaS に移行する。クラウドサービス事業者が提供する FW 及び IPS の利用を検討する。
2　CDN の利用
　X 社動画サーバの可用性を高めるため，CDN を利用する。CDN の利用によって，セキュリティ対策の効果も期待できる。

図 2　X 社動画サーバのクラウドサービスへの移行及び CDN の利用案（抜粋）

次は，図 2 の 2 についての C さんと F 氏の会話である。

C さん：X 社動画サーバでの動画配信に CDN を利用すると，どのように動画が配信されるようになりますか。

F 氏　：CDN では，インターネット上に［　a　］サーバというサーバを分散配置して，動画配信を要求した端末に最も近い［　a　］サーバから動画を配信するようにします。［　a　］サーバは，動画配信を要求されたとき，要求された動画を保持していれば代理応答し，保持していなければ動画を保持している X 社動画サーバにアクセスして動画を取得し，応答します。多くの動画配信が代理応答されるので，X 社動画サーバの負荷が軽減されます。

C さん：その仕組みによって，［　b　］攻撃への耐性も向上しますね。X 社動画サーバでの動画配信に CDN を利用するには，どのようにすればよいでしょうか。

F 氏　：例えば，M 社が提供している CDN を採用した場合の利用手順は図 3 のようになり，動画配信時の動作は図 4 のようになります。

(1)　M 社 CDN から X 社動画サーバ用に割り当てられた FQDN（以下，X-CDN-M-FQDN という）が発行される。
(2)　X 社の外部 DNS サーバの CNAME レコードで，X 社動画サーバの FQDN（以下，X-FQDN という）と X-CDN-M-FQDN とをひも付ける。

図 3　M 社 CDN の利用手順（抜粋）

(1) 会員が端末から X 社動画サーバに動画配信を要求すると，X 社の外部 DNS サーバに問合せが届く。X 社の外部 DNS サーバは，図 3 の設定に基づいて，X-CDN-M-FQDN を返す。
(2) 会員の端末は，M 社の DNS サーバに問い合わせて，X-CDN-M-FQDN の名前解決を行う。
(3) 会員の端末は，X-CDN-M-FQDN を名前解決した IP アドレスのサーバとの HTTPS 通信を行うため，TLS 接続を確立する。
(4) 会員の端末は，動画配信を要求する HTTP リクエストを送信する。TLS の接続先サーバ名には RFC 6066 に基づいて，HTTP リクエストの［ c ］ヘッダには RFC 7230 に基づいて，X-FQDN が指定される。要求された動画を M 社 CDN が保持していない場合，M 社 CDN は，HTTP リクエストの［ c ］ヘッダから X 社動画サーバを特定し，HTTP リクエストを転送する。

図 4　動画配信時の動作（抜粋）

C さん：理解しました。CDN を悪用する攻撃というのはあるのでしょうか。

F 氏　：X 社動画サーバの CDN 利用に関するものではありませんが，CDN を悪用する攻撃の一つにドメインフロンティング攻撃があります。X 社内のインターネット利用者を FW とプロキシサーバで保護するセキュリティ対策では，注意が必要です。どのようにして攻撃が成功するか，その例を図 5 に示します。

(1) ある CDN（以下，CDN-U という）が，X 社内から頻繁にアクセスする他社の Web サイトの複数で利用されているとする。それらの Web サイトの一つを Y 社 Web サイトとする（以下，Y 社 Web サイトの FQDN を Y-FQDN といい，CDN-U から Y 社 Web サイト用に割り当てられた FQDN を Y-CDN-U-FQDN という）。また，CDN-U は攻撃者サーバも利用しているとする（以下，攻撃者サーバの FQDN を Z-FQDN といい，CDN-U から攻撃者サーバ用に割り当てられた FQDN を Z-CDN-U-FQDN という）。
(2) この状況で XPC の 1 台がマルウェアに感染すると，次のような攻撃が行われることがある。
(3) 当該マルウェアは，Y 社 Web サイトとの HTTPS 通信を行うため，Y-FQDN の名前解決を行うと，まず Y-CDN-U-FQDN が返される。次に，Y-CDN-U-FQDN の名前解決を行い，Y-CDN-U-FQDN を名前解決した IP アドレスのサーバとの HTTPS 通信を行うため，TLS 接続を確立する。
(4) 当該マルウェアは，HTTP リクエストを送信する際，［ c ］ヘッダに Z-FQDN を指定する。CDN-U は，攻撃者サーバに HTTP リクエストを転送することになる。
(5) 結果として，当該マルウェアと攻撃者サーバとの間の通信が CDN 経由でできてしまう。

図 5　ドメインフロンティング攻撃が成功する例

C さん：何か対策はあるのでしょうか。

F 氏　：攻撃者サーバに割り当てられた IP アドレスを宛先とする通信を FW で拒否しても，Z-FQDN をプロキシサーバの拒否リストに登録しても，図 5 の(5)の

通信は遮断できません。①Y-CDN-U-FQDN を名前解決した IP アドレスを宛先とする通信を FW で拒否すると，複数の Web サイトが閲覧できなくなる影響があります。通信内容を監視して遮断するなどセキュリティ強化を進めている CDN 事業者もありますが，進めていない事業者もあります。X 社では，FW 又はプロキシサーバを，アウトバウンド通信の復号及び高機能な通信解析ができるものに替え，［ d ］と HTTP リクエスト中の［ c ］ヘッダの値が一致していることを検証して，一致していなければ遮断するという対策を検討してもよいでしょう。

C さん：分かりました。

システム部は，X 社動画サーバのクラウドサービスへの移行及び CDN の利用案について経営陣に報告した。この案は経営陣に承認され，X 社動画サーバの移行が開始された。

〔他のサーバのクラウドサービスへの移行案〕

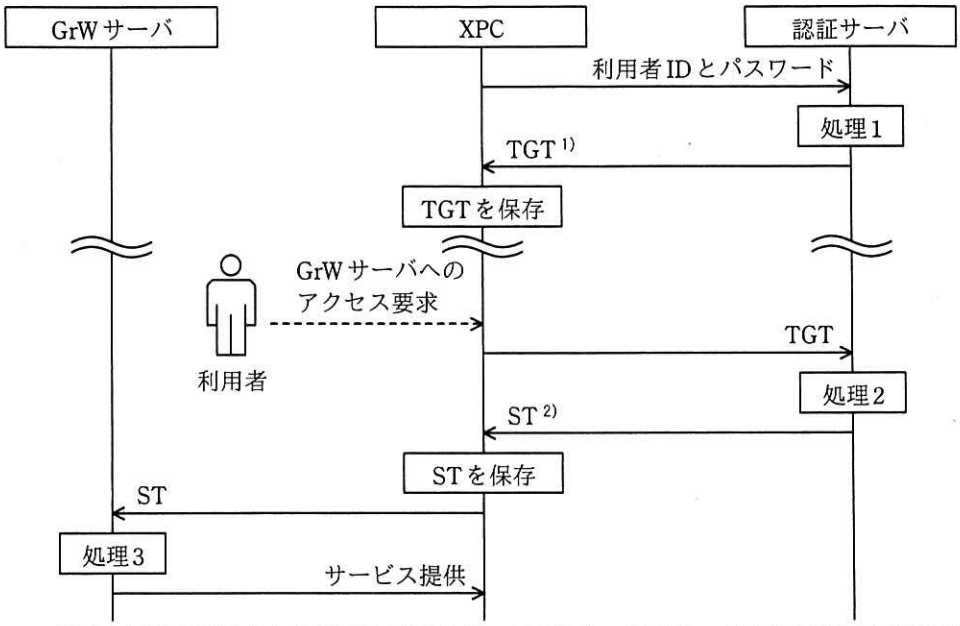
X社動画サーバの移行が完了し，CDNの利用も開始された。X社動画サーバに関する課題が解決されると，経営陣は，自社が保有する他のサーバについてもクラウドサービスへの移行を検討するようシステム部に指示した。システム部では，図6に示すクラウドサービスへの移行案を作成した。

・GrW 及びメールを SaaS に移行する。SaaS に切り替え後，GrW サーバ，外部メールサーバ及び内部メールサーバは，廃止する。
・従業員の利便性を確保するために，移行後の SaaS でも SSO を実現する。

図6　他のサーバのクラウドサービスへの移行案（抜粋）

〔SSO の現状〕

X社では，Kerberos 認証で SSO が実現されている。XPC から GrW サーバにアクセスする場合の Kerberos 認証の流れを図7に，図7中の各処理の概要を表1に示す。



注1) 利用者のアクセス権限を示すチケットである。認証サーバに登録されたTGT発行用アカウントのパスワードハッシュ値を鍵として暗号化されている。

注2) アクセス対象のサーバごとに発行されるチケットである。アクセス対象のサーバの管理者アカウント（以下，サーバ管理者アカウントという）のパスワードハッシュ値を鍵として暗号化されている。

図7　XPCからGrWサーバにアクセスする場合のKerberos認証の流れ

表1　図7中の各処理の概要

処理名	処理内容
処理1	利用者IDとパスワードが正しければ，TGTを発行する。
処理2	TGTを復号して検証し，問題なければ，STを発行する。
処理3	STを復号して検証し，問題なければ，アクセスを許可する。

次は，図7についてのCさんとF氏の会話である。

Cさん：Kerberos認証に対する攻撃はあるのでしょうか。

F氏　：幾つかあります。二つ説明しましょう。一つ目は，TGT，ST の偽造攻撃です。TGT又はSTが偽造されると，サーバが不正アクセスされて危険です。現在，TGT の偽造については，認証サーバ側での対策が進んでいます。一方，②STの偽造については，認証サーバ側で検知することができません。

Cさん：リスクがありますね。

F氏　：二つ目は，サーバ管理者アカウントのパスワードを解読して不正にログインする攻撃です。XPC から ST が奪取され，不正アクセスに悪用されても，不正アクセスされる範囲は限定されます。しかし，奪取された ST に対してサーバ管理者アカウントのパスワードの総当たり攻撃が行われ，それが成功すると，当該サーバ管理者アカウントでアクセスできるサーバが乗っ取られてしまいます。この総当たり攻撃は，③サーバ側でログイン連続失敗時のアカウントロックを有効にしていても対策になりません。

C さん：分かりました。

〔SaaS での SSO の実現〕

C さんは，GrW 及びメールの SaaS への移行後の SSO の実現方法を F 氏に尋ねた。次は，その際の F 氏と C さんの会話である。

F氏　：IDaaS の利用を提案します。多くの IDaaS では，Kerberos 認証ではなく SAML 認証をサポートしています。SaaS 側が SAML 認証をサポートしていれば，SAML 認証を用いた SSO が可能です。SAML 認証の流れを図 8 に，図 8 中の各処理の概要を表 2 に示します。

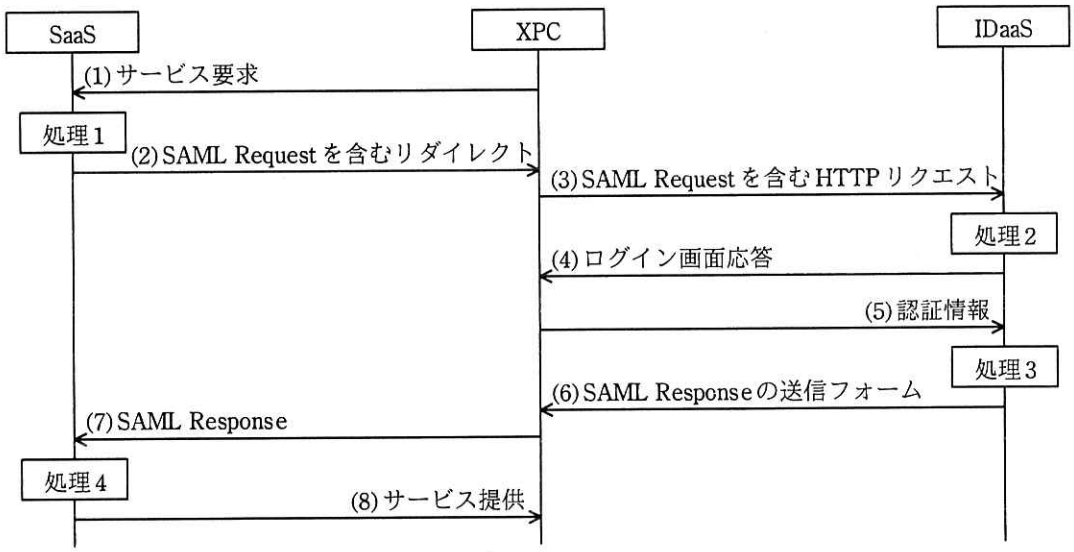


図 8　SAML 認証の流れ

表2　図8中の各処理の概要

処理名	処理内容
処理1	・IDaaSに認証を要求するSAML Requestを生成し，エンコードする。 ・エンコード結果とIDaaSのログイン画面のURLを組み合わせて，リダイレクト先URLを生成する。
処理2	・図8中の(3)のHTTPリクエスト中の［　e　］からSAML Requestを取得する。 ・信頼関係が構築されたSaaSからの認証要求であることを検証する。
処理3	・認証処理を行う。利用者の認証が成功した場合，処理4で用いるSAMLアサーションと，それに対するデジタル署名を含めたSAML Responseの送信フォームを生成する。
処理4	・SAML Responseに含まれるデジタル署名を検証することで，デジタル署名が［　f　］のものであること，及びSAMLアサーションの［　g　］がないことを確認する。 ・SAMLアサーションの内容を検証し，サービス提供すべきかどうかを決定する。

Cさん：事前の準備はありますか。

F氏　：IDaaSとSaaSとの間で事前に情報を共有しておく必要があります。事前に共有する情報は，SAMLアサーションで用いる属性，図8中の処理［　h　］で用いるURL，図8中の処理［　i　］及び処理［　j　］において必要なデジタル証明書などがあります。

Cさんは，F氏の提案を受け，SAML認証をサポートしているIDaaSを調査した。同時に，GrWサービス及びメールサービスを提供し，かつ，SAML認証をサポートしているSaaSを調査した。調査の結果，G社のSaaSとIDaaS（以下，G社のGrWサービスをGrW-G，メールサービスをメール-G，IDaaSをIDaaS-Gという）に移行することを経営陣に提案した。この案は経営陣に承認され，GrW-G及びメール-Gへの移行並びにIDaaS-GでのSSOの準備が開始された。

〔従業員からの要望〕

GrW-G，メール-G 及び IDaaS-G への移行及び SSO の準備が完了し，利用が開始された 3 か月後に，システム部は，X 社の従業員に対して，GrW-G 及びメール-G についてのヒアリングを実施した。その回答に，GrW-G でスケジュールを管理しているが，会議の主催者が会議日程の調整をもっと簡単にできるようにしてほしいという要望があった。C さんは，S 社が提供しているスケジュール調整サービス（以下，S サービスという）を導入し，GrW-G と連携させることで，その要望に応えることができると考えた。S サービスの内容を表 3 に示す。

表 3　S サービスの内容（抜粋）

項番	項目	内容
1	概要	SaaS で提供されており，S サービスのスマートフォン用アプリケーションプログラム（以下，スマートフォン用アプリケーションプログラムをスマホアプリという）又は PC の Web ブラウザから利用できる。
2	利用手順	(1)　主催者は，S サービスにアクセスする。 (2)　S サービスは，GrW-G から主催者のスケジュールを取得し，空き時間を表示する。 (3)　主催者は，空き時間の中から会議日程の候補を複数選ぶ。 (4)　S サービスは，会議の参加予定者に，各候補に対する参加可否の回答を依頼するメールを送信する。 (5)　会議の参加予定者は，可否を回答する。 (6)　S サービスは，会議の参加予定者の各候補に対する参加可否の一覧表を主催者に示す。 (7)　主催者は，一覧表を見て会議日程を決定する。 (8)　S サービスは，会議の参加予定者に招待メールを送付し，会議日程を GrW-G の主催者のスケジュールに登録する。

C さんは，S サービスの導入検討を進める中で，S サービス，GrW-G 及び IDaaS-G の間の連携について F 氏に相談した。次は，その際の F 氏と C さんの会話である。

F 氏　：S サービス，GrW-G 及び IDaaS-G は，OAuth 2.0 をサポートしています。OAuth 2.0 を利用したサービス要求からスケジュール情報の取得までの流れは，図 9 のようになります。

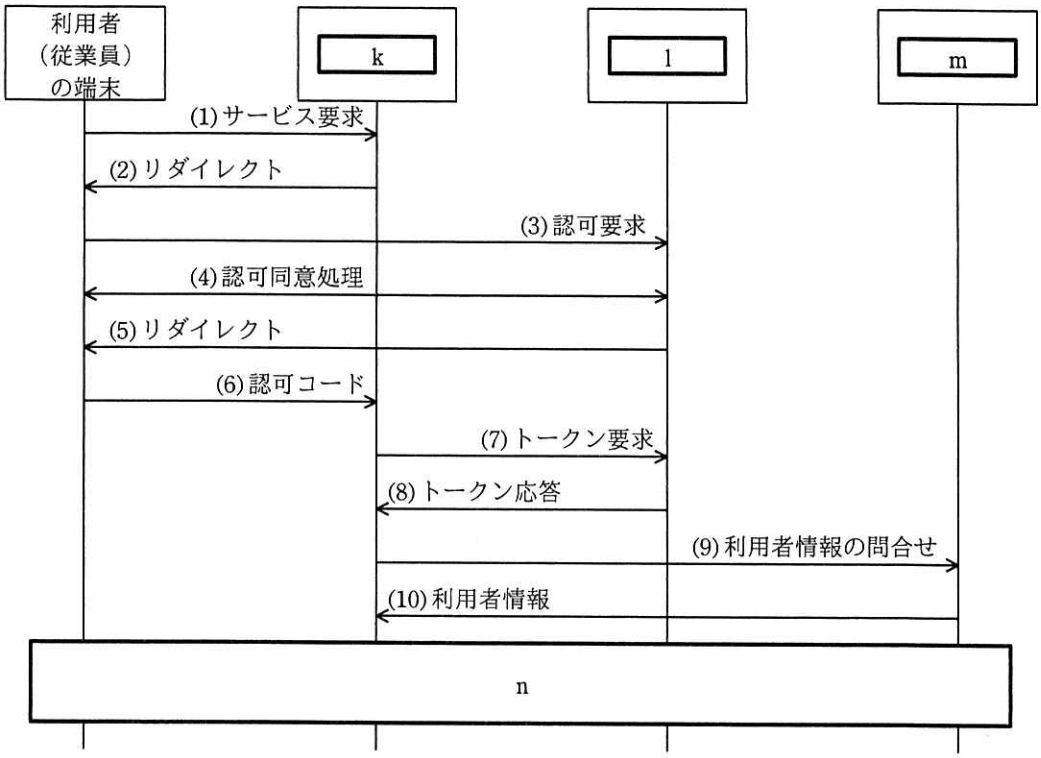


図 9　OAuth 2.0 を利用したサービス要求からスケジュール情報の取得までの流れ

C さん：セキュリティ対策について確認すべきことはありますか。

F 氏　：二つあります。一つ目は，クロスサイトリクエストフォージェリ（以下，CSRF という）攻撃についてです。標的となる利用者が重要な秘密を扱う会議の主催者として日程を決定する場合を考えてみましょう。攻撃者は，GrW-G に攻撃者のアカウントを登録し，当該 GrW-G にアクセスするための認可コードを利用者に送付します。そのときに，図 9 の実装に CSRF脆弱性があり，かつ，利用者の Web ブラウザが攻撃者によって生成された認可コードを受け付けてしまう実装となっている場合，利用者が気付かないうちに攻撃者のアカウントで会議日程が登録されてしまいます。対策として，state パラメタの実装が求められています。適切な実装であれば，図 9 中の［ o ］において，state パラメタを付与して送信し，図 9 中の［ p ］で送られてきたものと比較することで，攻撃を検知しているはずです。

二つ目は，利用者が S サービスへのアクセスに S サービスのスマホアプリを

使う場合についてです。S サービスのスマホアプリをインストールしたスマートフォンに，攻撃者が用意した不正なスマホアプリをインストールしてしまうと，GrW-G にアクセスするための認可コードを，攻撃者のスマホアプリが横取りしてしまうという攻撃があります。

C さん：二つ目の攻撃への対策にはどのようなものがありますか。

F 氏　：S サービスのスマホアプリでランダムな検証コードとその値を基にしたチャレンジコードを作成して，そのチャレンジコードを認可要求に追加し，検証コードをトークン要求に追加します。二つのコードを検証することで，検証コードを知らない攻撃者からのトークン要求を排除できます。この仕組みは，［　q　］として標準化されています。

C さん：分かりました。

〔企画チームからの要望〕

C さんは，企画チームから要望を受けた。要望は，T 社が運営しているメッセージ投稿サイト（以下，T 社投稿サイトという）と X 社動画サーバとを連携させ，T 社投稿サイトの認証サーバを用いた認証機能，及び T 社投稿サイトの投稿サーバへの自動投稿機能を X 社動画サーバに追加したいというものだった。この要望に対応することで，T 社投稿サイトのアカウントをもつ動画サービスの会員は，T 社投稿サイトにログインすれば X 社動画サーバも利用できる。また，X 社動画サーバに動画を投稿すると，“動画の概要”が T 社投稿サイトに自動で投稿されるようにもできる。C さんは，T 社投稿サイトと X 社動画サーバの連携方法について，F 氏に助言を求めた。次は，その際の F 氏と C さんの会話である。

F 氏　：OpenID Connect（以下，OIDC という）を用いれば，T 社投稿サイトと X 社動画サーバを連携できます。例えば，図 10 のような流れです。

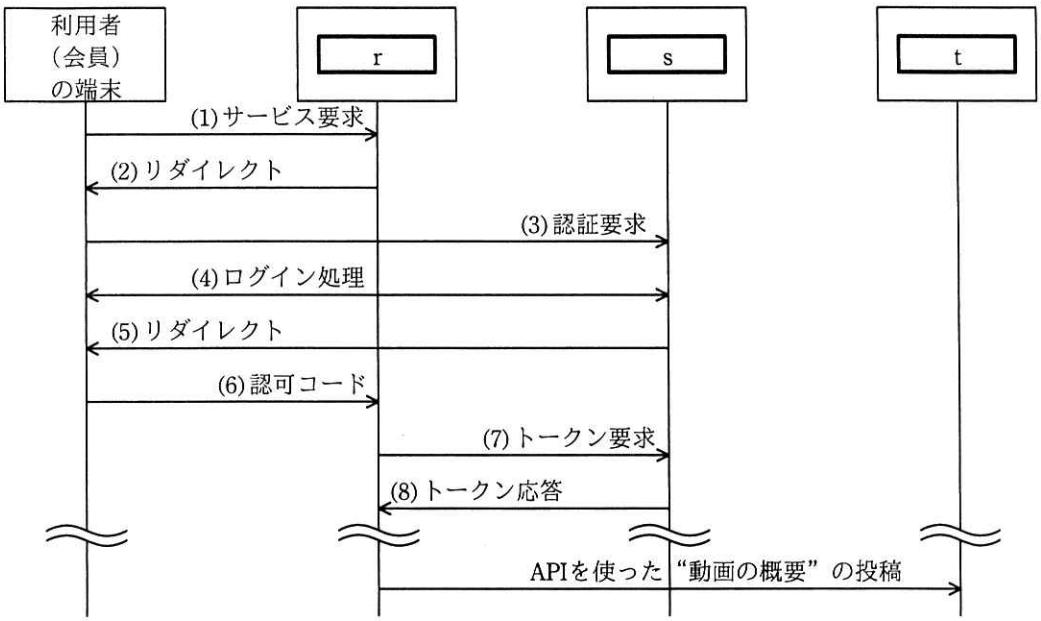


図 10　OIDC を用いた T 社投稿サイトと X 社動画サーバの連携の流れ

F 氏　：認可コードフローの場合，ID トークンは，図 10 中の［　u　］で送付されます。ID トークンは，JSON Web Token 形式で表現され，ヘッダ，ペイロード，署名の三つの部分で構成されます。署名は，ヘッダとペイロードに対して，T 社投稿サイトの認証サーバの秘密鍵を使って作成します。署名アルゴリズムは，ヘッダにおいて指定します。ヘッダ，ペイロード，署名は，それぞれ［　v　］でエンコードされます。

C さん：T 社投稿サイトでのセキュリティ対策について確認することはありますか。

F 氏　：ハイブリッドフローを用いる場合，state パラメタのほか，nonce 値を実装しているかを確認すべきです。まず，nonce 値を生成し，［　w　］に含めて送信します。次に，送られてきた［　x　］に含まれる nonce 値を検証することで，攻撃者による ID トークンの不正利用を防ぐことができます。

C さん：分かりました。

システム部は，T 社投稿サイトと動画サービスとを，OIDC で連携することに決め，X 社動画サーバの改修に着手した。

設問1　〔抜本的な対策の検討〕について，(1)～(5)に答えよ。

(1) 本文中の［ a ］に入れる適切な字句を，5字以内で答えよ。

(2) 本文中の［ b ］に入れる適切な字句を，英字5字以内で答えよ。

(3) 図4中，図5中及び本文中の［ c ］に入れる適切な字句を，英字5字以内で答えよ。

(4) 本文中の下線①について，Y-CDN-U-FQDNを名前解決したIPアドレスを宛先とする通信をFWで拒否した場合に閲覧できなくなるWebサイトの範囲を，60字以内で具体的に述べよ。

(5) 本文中の［ d ］に入れる適切な字句を，20字以内で答えよ。

設問2　〔SSOの現状〕について，(1)，(2)に答えよ。

(1) 本文中の下線②について，認証サーバ側では検知することができない理由を，30字以内で述べよ。

(2) 本文中の下線③について，対策にならない理由を，35字以内で述べよ。

設問3　〔SaaSでのSSOの実現〕について，(1)～(4)に答えよ。

(1) 表2中の［ e ］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　cookie　　イ　HTML　　ウ　クエリ文字列

エ　ボディ　　オ　リファラ

(2) 表2中の［ f ］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　IDaaS　　イ　SaaS　　ウ　XPC

(3) 表2中の［ g ］に入れる適切な字句を，5字以内で答えよ。

(4) 本文中の［ h ］～［ j ］に入れる適切な数字を，それぞれ答えよ。

設問4　〔従業員からの要望〕について，(1)～(4)に答えよ。

(1) 図9中の［ k ］～［ m ］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　GrW-G　　イ　IDaaS-G　　ウ　Sサービス

(2) 図9中の［ n ］に入れる適切な流れを解答群の中から選び，記号で答えよ。

解答群

(3) 本文中の［ o ］，［ p ］に入れる適切な通信を，図9中の(1)～(10)から選び，番号で答えよ。

(4) 本文中の［ q ］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　ASLR（Address Space Layout Randomization）

イ　EIAM（Enterprise Identity and Access Management）

ウ　PKCE（Proof Key for Code Exchange）

エ　SCIM（System for Cross-domain Identity Management）

設問5　〔企画チームからの要望〕について，(1)～(4)に答えよ。

(1) 図 10 中の［ r ］～［ t ］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　IDaaS-G　　イ　S サービス

ウ　T 社投稿サイトの投稿サーバ　　エ　T 社投稿サイトの認証サーバ

オ　X 社動画サーバ

(2) 本文中の［ u ］に入れる適切な通信を，図 10 中の(1)～(8)から選び，番号で答えよ。

(3) 本文中の［ v ］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　base32　　イ　base64url

ウ　ROT13　　エ　UTF-8

(4) 本文中の［ w ］，［ x ］に入れる適切な字句を，それぞれ 10 字以内で答えよ。

〔 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。