SC

平成31年度　春期
情報処理安全確保支援士試験
午後Ⅰ　問題

試験時間	12:30 ～ 14:00（1時間30分）

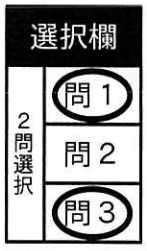
注意事項

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3
選択方法	2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。3問とも○印で囲んだ場合は，はじめの2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1，問3を選択した場合の例〕



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1～3に答えよ。

M社は，従業員数200名の小売業である。コーポレートサイトであるWebサイトA（URLは，https://site-a.m-sha.co.jp/）と，自社の特定のブランドを取り扱うECサイト（以下，ブランドサイトという）を複数運営している。現在運営しているブランドサイトは，WebサイトBからWebサイトFの五つである。Webサイトの開発や運用は自社の開発部で行っている。

Webサイト Aは，ブランドサイト全体のポータルサイトでもあり，各ブランドのキャンペーン情報などを掲載している。会員専用の機能は有していない。

Webサイト B（URLは，https://site-b.m-sha.co.jp/）は，ブランド Bの商品を扱うECサイトで，会員数は10万名である。WebサイトBでは，Cookieを利用したセッション管理を行っている。

会員情報は，各ブランドサイトで個別に管理している。

〔各ブランドサイトからWebサイトAへの情報連携〕

今回，各ブランドサイトの売上数を基にした，ブランド別の売れ筋商品情報を，Webサイト A上で表示するとともに，希望があれば，各ブランドサイトの会員に電子メールでも定期的に配信することにし，そのために売れ筋商品情報及び会員情報を取得する機能（以下，情報連携機能という）を実装することにした。具体的な機能は次のとおりである。

機能1　WebサイトAが各ブランドサイトの売れ筋商品情報を取得する。

機能2　希望する会員に電子メールを配信するために，Webサイト Aは，当該会員の会員情報を取得する。

なお，配信の申込みは，Webサイト A上で行う。

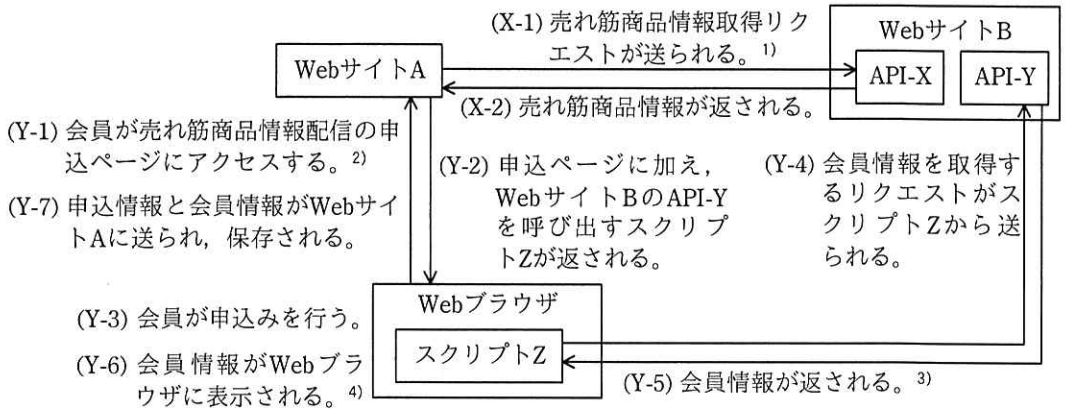
情報連携機能の実装は，開発部の C さんが中心になって進めることになった。まず初めに Webサイト B から Webサイト A への情報連携を行うために，次の二つの Web API を Webサイト B に実装することにした。

・Webサイト Bの売れ筋商品情報を取得可能とするための Web API（以下，API-X という）

・Webサイト Bの会員情報を取得可能とするための Web API（以下，API-Y という）

なお，Web API で受け渡されるデータは，JSON（JavaScript Object Notation）形式にする。C さんは，API-Y からブランドサイトの会員情報を取得する際，配信を希望する会員の同意を得たいと考えた。そこで，会員情報の取得には，会員の Web ブラウザを経由して行う方式を採用することにした。

Web サイト B から Web サイト A への情報連携機能を図 1 に示す。



注 1) API-X では，Web サイト A からだけアクセスできるように，接続元の IP アドレスを制限する。

2) 会員が Web サイト B にログインした状態のときにアクセスする。

3) 会員情報が得られない場合，エラーを返す。

4) （Y-5）でエラーが返ってきた場合，Web サイト B にログイン後再度操作を行うよう促す。

図 1　Web サイト B から Web サイト A への情報連携機能

〔情報連携機能の実装についての検討〕

スクリプト Z は，［ a ］ポリシによって，［ b ］，［ c ］，［ d ］のいずれかが異なるリソースへのアクセスが制限される。そこで，C さんは，この制限をう回するために JSONP（JavaScript Object Notation with Padding）を用いることを開発部の D 課長に提案した。次は，その時の会話である。

C さん：API-Y からの会員情報の取得に JSONP を用いるつもりです。

D 課長：JSONP は，アクセス先を制限する機能をもたないので，その実装では問題がある。例えば，まず，会員情報を窃取するように攻撃者がスクリプト Z を変更して，攻撃者の Web サイトのページに置く。次に，被害者に①特定の操作をさせた上で，そのページにアクセスさせると，攻撃者が被害者の

会員情報を窃取できてしまう。

C さん：JSONP の代わりに何の技術を用いればよいでしょうか。

D 課長：CORS（Cross-Origin Resource Sharing）を用いるのがよいだろう。

〔CORS の概要〕

CORS とは，ある Web サイトから他の Web サイトへのアクセスを制御することができる仕組みである。XMLHttpRequest を使って“https://test2.example.com/test”にリクエストを送るスクリプトの例を図 2 に示す。

```
var xhr = new XMLHttpRequest();
xhr.open('GET', 'https://test2.example.com/test', true);
xhr.setRequestHeader('X-Requested-With', 'XMLHttpRequest');
xhr.send(null);
```

図 2　XMLHttpRequest を使ったスクリプトの例

Web ブラウザが“https://test1.example.com/”にアクセスし，図 2 のスクリプトを含むページを読み込んだとする。図 2 のスクリプトが実行されると，最初に Web ブラウザは“https://test2.example.com/test”にプリフライトリクエストと呼ばれるリクエストを送る。そうすると，実際のリクエスト（以下，メインリクエストという）で許可されるメソッド名やヘッダフィールド名などがレスポンスとして返る。その後，メインリクエストを送り，レスポンスが返る。この一連の動作を図 3 に，また，図 3 中の（iii）～（vi）のリクエストとレスポンスの先頭部分の例を図 4～図 7 に示す。

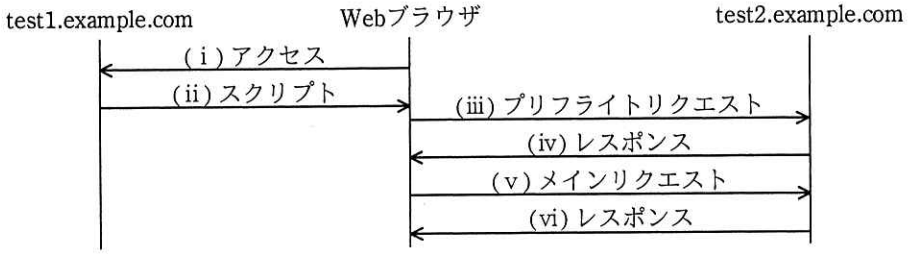


図 3　一連の動作

```
OPTIONS /test HTTP/1.1
Host: test2.example.com
Access-Control-Request-Method: GET [1)]
Access-Control-Request-Headers: x-requested-with [2)]
Origin: https://test1.example.com [3)]
```

注 1) Access-Control-Request-Method には，メインリクエストで利用したいメソッド名を指定する。
2) Access-Control-Request-Headers には，メインリクエストで利用したいヘッダフィールド名を指定する。
3) Origin は，スクリプトを含むページのオリジンであり，Web ブラウザが付与している。

図 4 （iii）のリクエストの先頭部分の例（抜粋）

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: https://test1.example.com [1)]
Access-Control-Allow-Methods: GET, POST, OPTIONS [2)]
Access-Control-Allow-Headers: x-requested-with [3)]
```

注 1) Access-Control-Allow-Origin には，Web サイトが許可するオリジンが返される。
2) Access-Control-Allow-Methods には，Web サイトが許可するメソッド名が返される。
3) Access-Control-Allow-Headers には，Web サイトが許可するヘッダフィールド名が返される。

図 5 （iv）のレスポンスの先頭部分の例（抜粋）

```
GET /test HTTP/1.1
Host: test2.example.com
X-Requested-With: XMLHttpRequest
Origin: https://test1.example.com
```

図 6 （v）のリクエストの先頭部分の例（抜粋）

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: https://test1.example.com
```

図 7 （vi）のレスポンスの先頭部分の例（抜粋）

また，CORS では通常，Web ブラウザは，スクリプトを読み込んだページのオリジンだけに Cookie や，ベーシック認証の情報を送る。図 2 では設定していないが，XMLHttpRequest のプロパティの withCredentials の値が true に設定されている場合，図 3 であれば，［ e ］の動作の際に，test2.example.com から発行された Cookie が送られる。

〔CORS を利用した実装〕

C さんは，スクリプト Z の実装に CORS を用いたときの一連の動作を検討し，表 1 にまとめた。

表 1　スクリプト Z の実装に CORS を用いたときの一連の動作

No.	内容
1	Web ブラウザは，Web サイト A の売れ筋商品情報配信の申込ページにアクセスする。
2	Web サイト A は，Web サイト B の API-Y を呼び出すスクリプト Z を含むページをレスポンスとして返す。
3	Web ブラウザは，会員が申込みを行うと，Web サイト B にプリフライトリクエストを送信する。プリフライトリクエストは，OPTIONS メソッドの呼出しであり，Origin ヘッダフィールドには“https://site-a.m-sha.co.jp”が設定されている。
4	API-Y は，送られてきたリクエストに Origin ヘッダフィールドが存在する場合，Access-Control-Allow-Origin ヘッダフィールドを付加し，レスポンスを返す。Access-Control-Allow-Origin ヘッダフィールドの値は，“ f ”である。Origin ヘッダフィールドが存在しない場合，エラーを返す。
5	Web ブラウザは， g と Access-Control-Allow-Origin ヘッダフィールドの値を照合し，アクセスが許可されていることを確認する。許可されている場合は，次の処理に進む。確認できない場合は，メインリクエストを送らずに終了する。
⋮	⋮
9	スクリプト Z は，受け取った JSON 形式の値を変数に格納し，表示する。さらに，受け取った値は Web サイト A に送られ，保存される。

C さんは，表 1 について D 課長に確認した。次は，その時の D 課長と C さんの会話である。

D 課長：今後，他のシステムでも CORS を利用することが考えられるので，コーディング規約も併せてまとめておきたい。Access-Control-Allow-Origin ヘッダフィールドに指定できるオリジンは一つだけなので，複数のオリジンからのアクセスを許可するような仕様であった場合に，No. 4 の内容では不十分である。Web API のプログラム内に，許可するオリジンのリストを用意しておく必要がある。プリフライトリクエスト又はメインリクエストが Web API に送られてきたときに，そのリクエスト中の h を， i と突合し， j した値があればその値を Access-Control-Allow-Origin ヘッダフィールドに設定するという内容もコーディング規約に含めればよ

いだろう。

C さん：分かりました。

C さんは，CORS の利用に関するコーディング規約をまとめ，表 1 をこれに合うように修正し，D 課長に再度確認した。修正後の内容で問題ないということだったので，C さんは実装を行った。

その後，セキュリティ専門業者に脆弱性診断を依頼し，脆弱性が検出されないことを確認した上で，情報連携機能をリリースした。その後，同様に残り四つのブランドサイトから Web サイト A への情報連携機能も実装した。

設問 1　〔情報連携機能の実装についての検討〕について，(1)～(3)に答えよ。

(1) 本文中の［ a ］に入れる適切な字句を答えよ。

(2) 本文中の［ b ］～［ d ］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 FQDN
ウ Location ヘッダフィールド	エ Referer ヘッダフィールド
オ User-Agent ヘッダフィールド	カ 時刻
キ スキーム	ク ポート番号

(3) 本文中の下線①について，操作の具体的な内容を，20 字以内で答えよ。

設問 2　本文中の［ e ］に入れる適切な記号を，(iii)～(vi)の中から選び，答えよ。

設問 3　〔CORS を利用した実装〕について，(1)～(3)に答えよ。

(1) 表 1 中の［ f ］に入れる適切な URL を答えよ。

(2) 表 1 中の［ g ］に入れる適切な字句を，30 字以内で答えよ。

(3) 本文中の［ h ］，［ i ］に入れる適切な字句を，それぞれ 20 字以内で，本文中の［ j ］に入れる適切な字句を，5 字以内で答えよ。

〔 メ モ 用 紙 〕

問2　クラウドサービスのセキュリティに関する次の記述を読んで，設問 1，2 に答えよ。

U 社は，東京に本社をもつ従業員数 1,000 名の商社である。複数の海外拠点を設置し，海外向けに営業展開している。海外拠点の従業員数は 1 拠点当たり十数名ほどである。

本社の情報システムは，本社の情報システム部が管理しており，各海外拠点の情報システムは，現地の情報システム担当者が管理している。電子メール（以下，メールという）の送受信には，本社ではオンプレミス環境を導入しているが，海外拠点では，P 社が提供するクラウドサービス型 Web メールサービス（以下，メールサービス P という）を利用している。海外拠点では，全ての従業員にスマートフォンとノート PC を貸与している。

〔セキュリティインシデント発生〕

1 月 10 日，送信者が海外拠点 Q の従業員 S さんのメールアドレスである不審なメールを受け取ったという連絡が，S さんとやり取りのあった本社の従業員から情報システム部にあった。情報システム部では，情報処理安全確保支援士（登録セキスペ）である T さんが，調査を担当することになった。T さんが当該メールのヘッダ情報を確認したところ，メールサービス P から送信されたものであった。

海外拠点 Q の情報システム担当者である Y さんによれば，1 月 10 日に S さんのアカウントからの不審なメール送信と考えられる履歴が複数残っているとのことであった。そこで，T さんは，Y さんにメールサービス P の S さんのアカウントを一時的に無効化するよう依頼した。また，会社から貸与された S さんのスマートフォン及びノート PC 並びに S さんのメールボックスには重要情報がなかったことを確認した。T さんが，海外拠点 Q の全従業員のアカウントについて，メールサービス P に残っていた全てのメール送信履歴を Y さんに確認してもらったところ，S さんのアカウント以外に不審なメールの送信履歴はないとのことであった。

〔経緯の調査〕

T さんは，メールサービス P に残っていた海外拠点 Q の全従業員のアカウントのメール送信履歴及び監査ログ，並びに S さんへのヒアリングの結果を Y さんから送付

してもらい，調査した。調査結果を図1に示す。

・1月10日は，Sさんはアジアの Z 国に出張中だった。
・U 社には，会社から貸与されたノート PC を U 社以外の無線 LAN に接続してはならないというルールがあるが，S さんはそのルールを知らず，その日，出張先のホテルで宿泊客用の無線 LAN（以下，ホテル Wi-Fi という）を利用していた。
・ホテル Wi-Fi の SSID は，宿泊客で共通であり，その SSID と事前共有鍵はロビーなどの共有スペースに張り出されていた。
・S さんのノート PC（以下，PC-S という）は，IP アドレス及び DNS サーバの情報を DHCP で自動取得する設定になっていた。
・S さんは，その日，メールサービス P を利用するために，Web ブラウザのアドレスバーにメールサービス P の FQDN を手入力し，ログインページに利用者 ID とパスワードを入力した。
・S さんがメールサービス P にアクセスした時，サーバ証明書が信頼できない旨のエラーは Web ブラウザ上に表示されなかった。
・メールサービス P の監査ログに記録されていた S さんの利用者 ID によるログイン記録のうち不審メールが送信されていた時間帯のものは，Z 国，及び S さんが出張していない南米の W 国の IP アドレスからのものだった。

図1　調査結果（抜粋）

T さんが調べたところ，メールサービス P は HTTP over TLS でサービスが提供されている。HTTP でアクセスした場合は HTTP over TLS の URL にリダイレクトされる仕様になっており，HSTS（HTTP Strict Transport Security）は実装されていない。

こうしたことから，T さんは S さんが不正アクセスを受けたと確信し，図2に示す手口（以下，手口 G という）を使って，攻撃者がメールサービス P の S さんの利用者 ID で不正アクセスしたと推測した。

・攻撃者は，①無線 LAN アクセスポイント，DNS サーバ及び Web サーバを用意した。その DNS サーバには［ a ］の FQDN と［ b ］の IP アドレスとを関連付ける A レコードが設定されていた。
・S さんは，PC-S をホテル Wi-Fi に接続しようとして，攻撃者が用意した無線 LAN アクセスポイントに接続してしまった。
・その結果，PC-S に攻撃者が用意した DNS サーバの情報が設定された。
・S さんは，Web ブラウザからメールサービス P にアクセスしたつもりだったが，実際には Web ブラウザは②攻撃者が用意した Web サーバに接続していた。S さんは，サーバ証明書が信頼できない旨のエラーが表示されなかったので，その Web サーバに対して，利用者 ID 及びパスワードを入力してしまった。
・攻撃者は盗んだ S さんの利用者 ID 及びパスワードを使ってメールサービス P に不正アクセスした。

図2　手口 G

Tさんは，今回のセキュリティインシデントの調査結果を情報システム部長に報告した。情報システム部長は，会社から貸与されたノートPCをU社以外の無線LANに接続してはならないというルールの全社への周知及びメールサービスPの認証方式の強化をTさんに指示した。

〔認証方式の強化〕

情報システム部長からメールサービスPの認証方式の強化について，次の2点が要求された。

要求1　U社以外の無線LANに接続したとしても手口Gを防ぐこと

要求2　手口Gに限らず，偽サイトにアクセスしてしまったときにフィッシングの手口によるメールサービスPへの不正アクセスを防ぐこと

Tさんが調査したところ，メールサービスPは，単体ではパスワード認証にしか対応していないが，認証連携の機能があることが分かった。認証連携機能を使えば，メールサービスPにアクセスしようとしたときに，他のID管理サービスにリダイレクトされ，そこで認証が行われ，認証に成功すると，メールサービスPにアクセスできるようになる。そこで，X社が提供するクラウドサービス型ID管理サービス（以下，IDaaS-Xという）が対応している，より強力な認証方式を利用することにした。IDaaS-Xでは，認証サーバXを使って利用者を認証する。

IDaaS-Xが対応している，より強力な認証方式には，次の2種類がある。

・ワンタイムパスワード（以下，OTPという）認証方式

TOTP（Time-based One-Time Password algorithm）用のスマートフォンアプリケーションプログラム（以下，TOTPアプリという）を利用した認証方式

・パスワードレス認証方式

WebAuthn（Web Authentication API）対応のWebブラウザ及び生体認証対応のオーセンティケータを搭載したデバイスを利用した認証方式

Tさんは二つの認証方式について，要求1及び要求2を満たすことができるかを検討した。

T さんは，まず OTP 認証方式を検討した。IDaaS-X における TOTP アプリ登録処理を図 3 に，OTP 認証方式の認証処理を図 4 に示す。

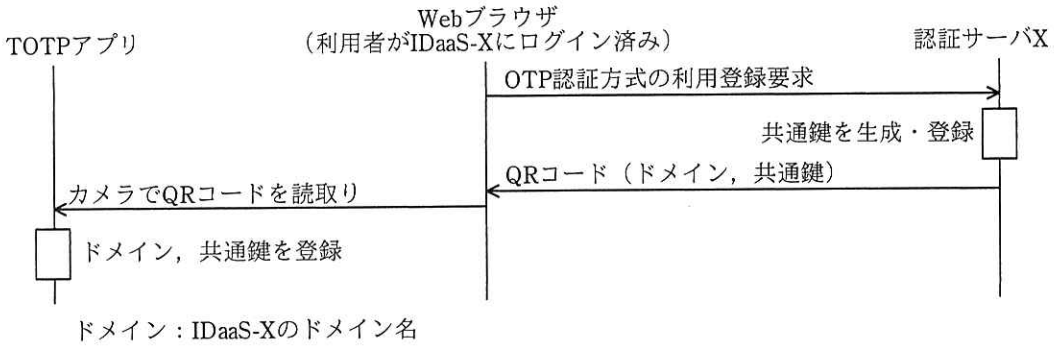


図 3　IDaaS-X における TOTP アプリ登録処理

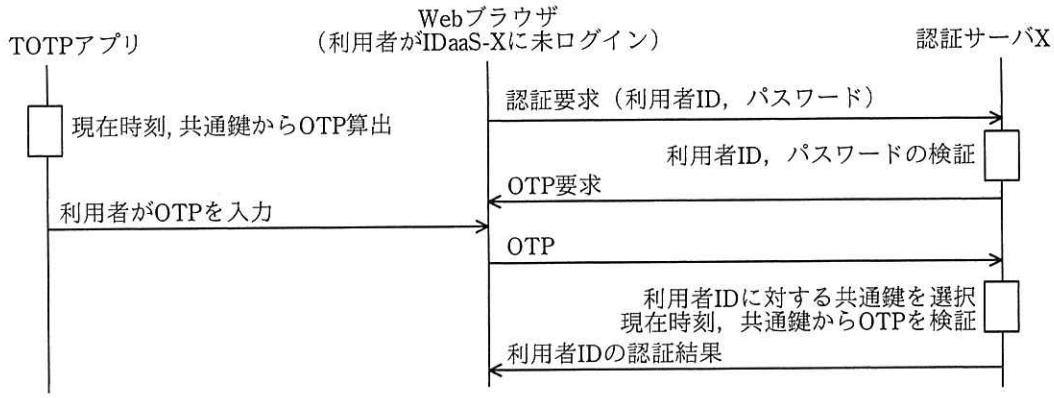
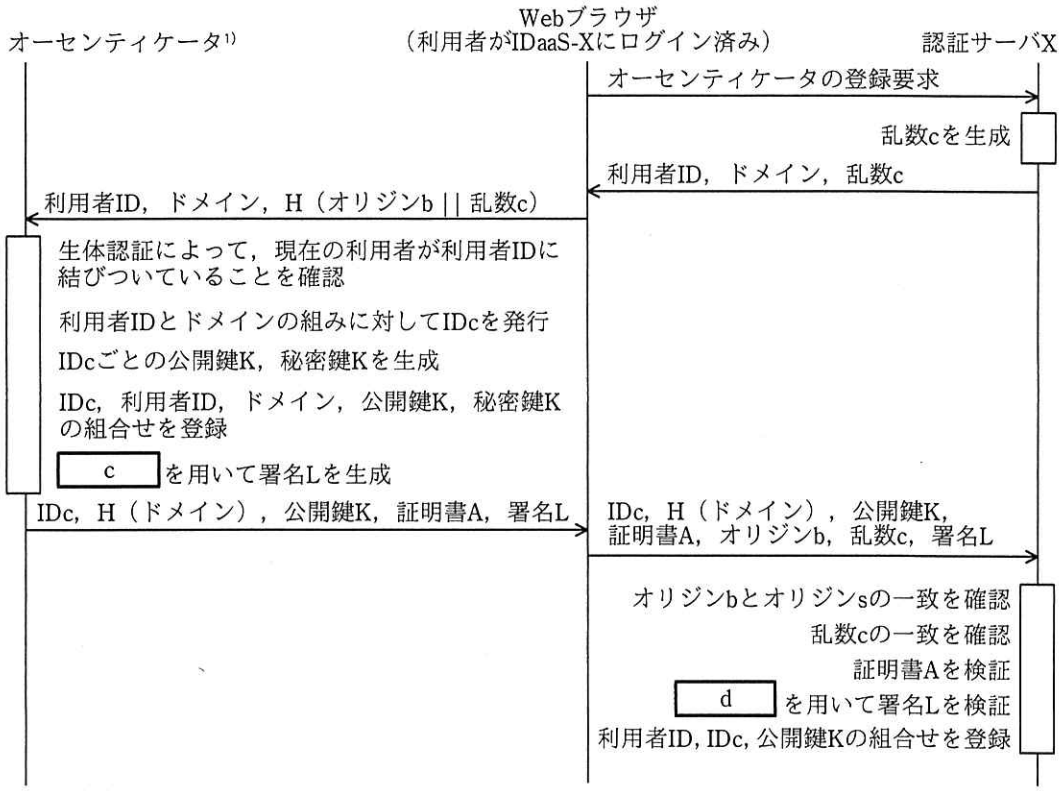


図 4　IDaaS-X における OTP 認証方式の認証処理

OTP 認証方式を利用した場合，ログインには時刻によって変化する OTP も必要になるので，パスワードが窃取された場合でも不正ログインを防ぐことが可能となる。しかし，③OTP 認証方式を利用し，かつ，登録処理を正しく行ったとしても，要求 2 を満たすことができないおそれがある。

次に T さんは，パスワードレス認証方式を検討した。IDaaS-X におけるオーセンティケータ登録処理を図 5 に，認証処理を図 6 に示す。



H（A）：Aのハッシュ値

A || B：AとBを連結

オリジンb：Webブラウザがアクセスしたwebサイトのオリジン

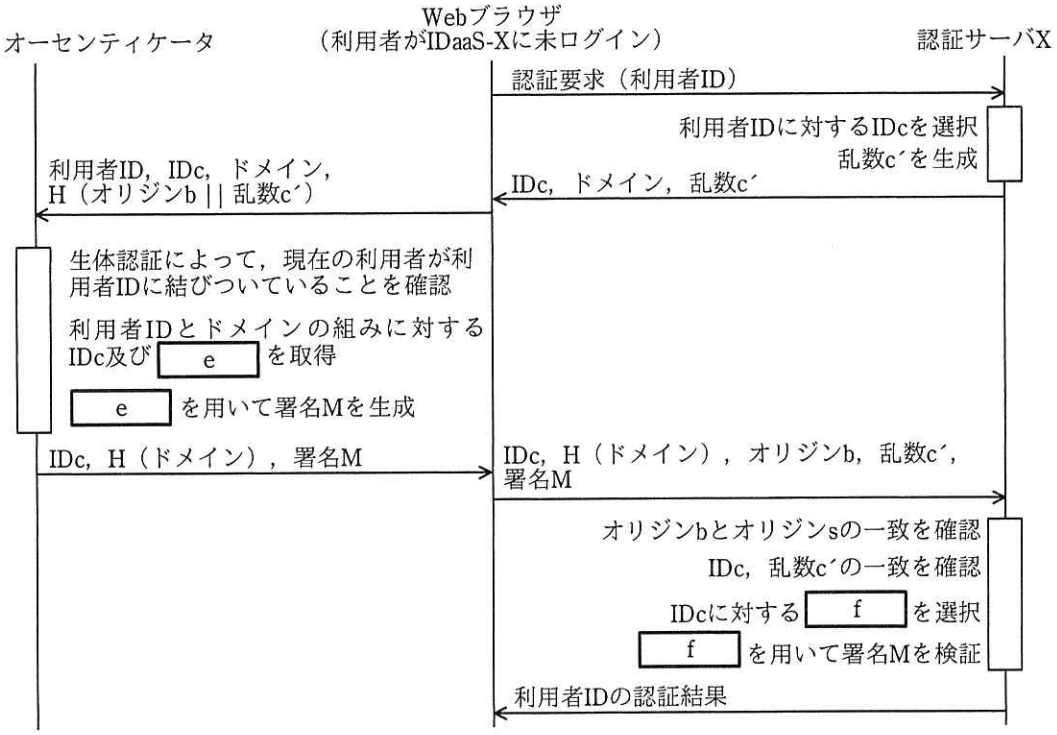
オリジンs：認証サーバXのWebサイトのオリジン

IDc：利用者IDとドメインの組みに対して，オーセンティケータごとに発行されるID

署名L：IDc，H（ドメイン），公開鍵K，H（オリジンb || 乱数c）に対するディジタル署名

注 1) オーセンティケータには，搭載されたデバイスごとにユニークな公開鍵 A，秘密鍵 A，及び証明書 A が組み込まれている。ここで，証明書 A は，信頼された認証局が発行した，公開鍵 A に対するディジタル証明書である。

図 5　IDaaS-X におけるオーセンティケータ登録処理



署名M：H（ドメイン），H（オリジンb || 乱数c´）に対するディジタル署名

図6　IDaaS-X におけるパスワードレス認証方式の認証処理

④パスワードレス認証方式を利用すれば，要求2を満たすことができると考えられた。

Tさんは，検討結果を情報システム部長に報告した。情報システム部長は，海外拠点Qにおけるメールサービスpへのパスワードレス認証方式の導入を，Tさん及びYさんに指示した。

海外拠点で従業員に貸与しているスマートフォンとノート PC にはオーセンティケータが搭載されていたので，パスワードレス認証方式を速やかに導入することができた。

U社では，他の海外拠点でのクラウドサービスについても，同様の方式を導入することにした。

設問1　〔経緯の調査〕について，(1)～(3)に答えよ。

(1) 図2中の下線①について，攻撃者が用意した無線LANアクセスポイントには何が設定されていたと考えられるか。設定を30字以内で述べよ。

(2) 図2中の［　a　］，［　b　］に入れる適切な字句を，本文，図1又は図2中の字句を用いて答えよ。

(3) 図2中の下線②について，この時，サーバ証明書が信頼できない旨のエラーが表示されなかったのはなぜか。メールサービスPにHSTSが実装されていないことを踏まえ，理由を20字以内で述べよ。

設問2　〔認証方式の強化〕について，(1)～(3)に答えよ。

(1) 本文中の下線③について，偽サイトにおいてどのような処理が行われればメールサービスPへの不正アクセスが成立するか。行われる処理を35字以内で述べよ。

(2) 図5及び図6中の［　c　］～［　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。

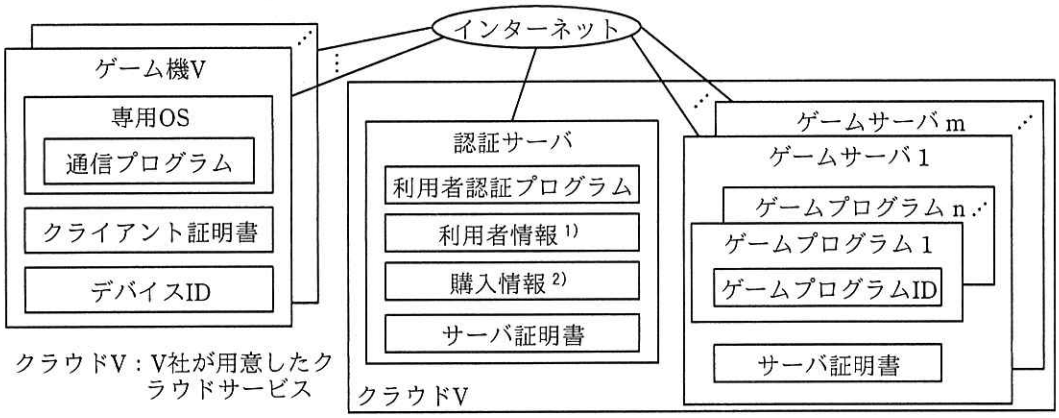
解答群

ア　公開鍵A　　イ　公開鍵K　　ウ　秘密鍵A　　エ　秘密鍵K

(3) 本文中の下線④について，理由を図5又は図6中の字句を用いて，40字以内で述べよ。

問３　IoT 機器の開発に関する次の記述を読んで，設問 1～3 に答えよ。

V 社は，IoT 機器を製造・販売している従業員数 3,000 名の会社である。家庭用ゲーム機（以下，ゲーム機 V という）の発売を予定しており，設計を開発部が担当している。設計リーダは，開発部の H さんである。利用者はゲーム機 V とゲームプログラムの利用権を購入し，ゲーム機 V からゲームサーバ上のゲームプログラムを利用する。複数のゲームプログラム開発会社が，それぞれ複数のゲームプログラムを開発し，販売する予定である。開発部が設計したゲーム機 V，認証サーバ及びゲームサーバ（以下，三つを併せてゲームシステム V という）の構成を図 1 に，構成要素とその概要を表 1 に示す。



注記 1　ファイアウォールなどのネットワーク機器は省略している。
注記 2　ゲーム機 V と各サーバとの間の通信には，HTTP over TLS を使用する。
注 1)　利用者 ID，パスワードのハッシュ値，ニックネーム，性別及び誕生日から成る。
2)　利用者 ID，利用者が購入したゲームプログラムのゲームプログラム ID から成る。

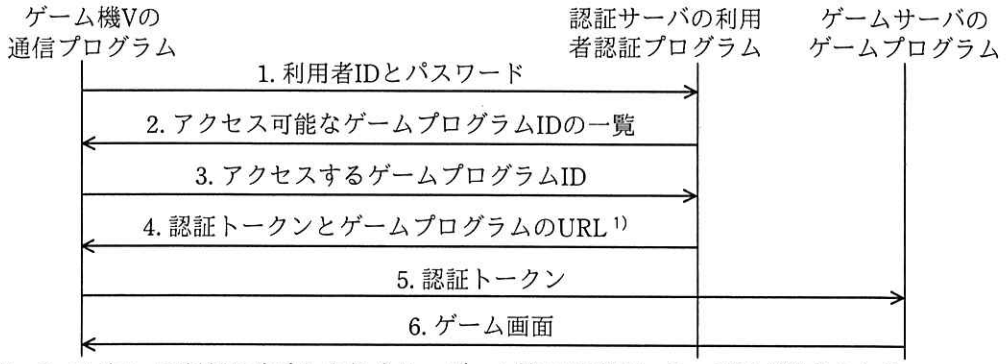
図 1　ゲームシステム V の構成（概要）

表1　ゲームシステムVの構成要素とその概要

構成要素	概要
ゲーム機V	・無線LAN機能，コントローラ[1]及びディスプレイを備えている。 ・専用OSがインストールされており，ブートローダから起動される。 ・専用OSに含まれる通信プログラムは，ゲームサーバ上のゲームプログラム及び認証サーバ上の利用者認証プログラムと通信する。 ・通信プログラムは，コントローラの操作情報をリアルタイムにゲームプログラムに送信し，ゲームプログラムからゲームの処理結果をゲーム画面として受信してディスプレイに表示する。 ・ゲーム機Vごとに一意のデバイスIDが付与される。 ・ゲーム機Vごとに発行されたクライアント証明書を格納している。各サーバとの通信時には，クライアント証明書を使用したクライアント認証が行われる。 ・各サーバとの通信時には，サーバ認証を行い，クラウドV中のサーバとだけ通信を行う。 ・初期セットアップ時に認証サーバに利用者情報を登録する。 ・PCに接続しても外部ストレージとして認識されず，内部のデータを直接読み出すことはできない。
ゲームサーバ	・クラウドVに複数のゲームプログラム開発会社がそれぞれゲームサーバを立ち上げ，各ゲームサーバで一つ又は複数のゲームプログラムを稼働させる。 ・ゲームプログラム開発会社のゲームサーバ管理者が運用する。 ・各ゲームプログラムには，固有のゲームプログラムIDが付与される。 ・ゲームサーバごとに発行されたサーバ証明書を格納している。
認証サーバ	・利用者情報と購入情報を管理する。 ・利用者認証プログラムは，ゲーム機Vがゲームプログラムを利用する際の利用者の認証を行う。認証の結果，利用者が購入したゲームプログラムだけの利用を許可する。 ・認証サーバに発行されたサーバ証明書を格納している。

注[1]　ゲームを行う際などに使用する入力装置

ゲームを行う際は図2の認証フローで利用者の認証が行われる。



注記　1. 又は5. で認証に失敗した場合は，ゲーム機Vに認証エラー画面が送信される。
注[1]　URLはゲームプログラムごとに固有である。

図2　利用者がゲームを行う際の認証フロー

認証トークンには，認証サーバの FQDN，利用者 ID 及び MAC（Message Authentication Code）が格納される。①MAC は，認証サーバの FQDN と利用者 ID に対して，ハッシュ関数を共通鍵と組み合わせて使用し，生成する。共通鍵は，ゲームシステム V 全体で一つの鍵が使用され，ゲームサーバ管理者がゲームプログラムに設定する。図 2 の 5. では，ゲームプログラムによる認証トークンの MAC の検証が成功し，かつ，FQDN が確かに認証サーバのものであることが確認された場合だけ，認証が成功し，図 2 の 6. でゲームプログラムからゲーム画面が送信される。

〔セキュリティレビューの実施〕

認証トークンが認証サーバ以外で不正に生成されると，購入していないゲームプログラムを利用されたり，クラウド V 上のリソースを不正に利用されたりするおそれがある。そこで仮に認証サーバ以外で認証トークンを生成されたとしてもゲームプログラムでは検証に失敗することが求められる。また，利用者がコントローラの不正な操作情報をゲーム機 V から送信することによって，ゲームを有利に進めるといったことも防ぐ必要がある。

V 社では，システム設計にセキュリティ上の問題がないか，製品の設計工程でセキュリティレビュー（以下，レビューという）を実施することになっており，ゲームシステム V はセキュリティ部の N さんがレビューを担当することになった。次は，N さんがゲームシステム V のレビューを行った時の，H さんとの会話である。

N さん：現状の認証トークンの設計には二つの問題があります。一つ目の問題は，現在の設計では認証トークンに格納される情報が不足しているということです。情報が不足していることによって，ゲームプログラム A 用の認証トークンがゲームプログラム B においても認証に成功してしまうので，攻撃者がゲームプログラムの URL を知ることができれば，購入していないゲームプログラムも利用できてしまいます。②この問題への対策を検討してください。

H さん：分かりました。

N さん：二つ目の問題は，③認証トークンをゲームサーバ管理者が不正に生成できてしまうことです。

H さん：その問題への対策としては，ゲームプログラムごとに別の共通鍵を利用するという設計はどうでしょうか。

N さん：それでは対策として不十分です。④その設計にしたとしても，不正にゲームプログラムが利用できる認証トークンをゲームサーバ管理者が生成できてしまいます。

H さん：MAC ではなく，ディジタル署名を利用すれば対策になりますか。

N さん：はい。そうすればゲームサーバ管理者が認証トークンを不正に生成したとしても，ゲームプログラムで検証が失敗します。

H さん：では，［ a ］で公開鍵と秘密鍵の鍵ペアを生成し，［ b ］をゲームサーバに配布しておきます。［ a ］が［ c ］を使って認証トークンに署名を付加し，ゲームプログラムでは［ b ］を使って署名の検証を行います。

N さん：それで問題ありません。次に，不正な機器から認証サーバとゲームサーバへのアクセスをどのようにして防ぐのか教えてください。

H さん：クライアント認証を使います。

N さん：ゲーム機 V 内のクライアント証明書とそれに対応する秘密鍵（以下，鍵 C という）が攻撃者の PC から不正に使用できると，その PC から各サーバに接続されてしまいます。さらに，コントローラの操作情報を改ざんして送信することによって，ゲームを有利に進めることも考えられます。クライアント証明書と鍵 C はゲーム機 V のどこに格納しますか。

H さん：鍵 C を含めた全てのデータは，搭載する SSD（Solid State Drive）に格納します。搭載する SSD は，広く流通しているものです。

N さん：それでは問題がありますね。現状の設計では，専用 OS に脆弱性が存在しなかったとしても，⑤攻撃者がゲーム機 V を購入すれば，専用 OS を改ざんせずに，ゲーム機 V 内のクライアント証明書と鍵 C を PC などから不正に使用できます。

H さん：どのように対策したらいいでしょうか。

N さん：TPM（Trusted Platform Module）をゲーム機 V に搭載し，TPM 内に鍵 C を保存するという方法があります。TPM は，⑥内部構造や内部データを解析されにくい性質を備えているので，TPM 内に鍵 C を保存すれば不正に読み

取ることは困難になります。

また，ブートローダ又は専用 OS の改ざんはゲーム機 V の不正利用につながります。例えば，コントローラの不正な操作情報を送信されるおそれがあります。そのため，ブートローダ及び専用 OS の改ざん対策についても検討してください。

H さん：分かりました。設計を見直します。

〔ブートローダ及び専用 OS の改ざん対策〕

2 回目のレビューでは，ブートローダ及び専用 OS の改ざん対策について確認した。次は，その時の H さんと N さんの会話である。

H さん：ブートローダ及び専用 OS の改ざんに備えた対策として，ブートローダ又は専用 OS が改ざんされていると判定されたときは，ゲーム機 V の起動処理を中止するようにしました。ブートローダ及び専用 OS の改ざん対策の処理の流れを図 3 に示します。

1. ブートローダ及び専用 OS 中の起動時に実行されるファイルのハッシュ値をあらかじめ計算し，ハッシュ値のリスト（以下，ハッシュ値リストという）を作成しておく。ゲーム機 V への専用 OS の導入時，ハッシュ値リストを併せて保存する。起動時に専用 OS 中のファイルが実行される順番は，あらかじめ決められている。
2. ゲーム機 V の起動時には，CRTM（Core Root of Trust for Measurement）と呼ばれる，改ざんが困難な起動コードから起動処理を開始する。
3. CRTM は，ブートローダのハッシュ値を計算し，そのハッシュ値がハッシュ値リスト中に存在することを確認できたら実行する。
4. ブートローダは，専用 OS の最初に実行されるファイルのハッシュ値を計算し，ハッシュ値リスト中に存在することを確認し，実行する。同様に，後続のファイルについて計算，確認，実行を繰り返し，専用 OS が起動する。
5. ハッシュ値がハッシュ値リスト中に存在しないファイルは改ざんされていると判定され，起動処理が中止される。

図 3　ブートローダ及び専用 OS の改ざん対策の処理の流れ

N さん：処理の流れは分かりました。ハッシュ値リストが保護されていないと，改ざんされたファイルが実行されるおそれがありますが，どのように対策していますか。

Hさんは，⑦ハッシュ値リストを保護するための方法を説明した。

Nさん：それであれば，改ざんされたファイルが実行される危険性は低いですね。

その後，クラウドVの準備が整い，ゲーム機Vが発売された。

設問1　本文中の下線①に該当する方式はどれか。該当する方式を解答群の中から選び，記号で答えよ。

解答群

ア　CBC-MAC	イ　CMAC	ウ　CSR
エ　HMAC	オ　MD5	カ　RC4

設問2　〔セキュリティレビューの実施〕について，(1)～(6)に答えよ。

(1)　本文中の下線②について，対策として認証トークンに追加する必要がある情報を，15字以内で答えよ。

(2)　本文中の下線③について，その原因となるゲームサーバの仕様を，30字以内で述べよ。

(3)　本文中の下線④について，その原因となる認証トークンの仕様を，20字以内で述べよ。また，不正に生成した認証トークンで利用できるゲームプログラムの範囲を，35字以内で述べよ。

(4)　本文中の［　a　］～［　c　］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　共通鍵	イ　ゲーム機V	ウ　ゲームサーバ
エ　公開鍵	オ　認証サーバ	カ　秘密鍵

(5)　本文中の下線⑤について，どのようにするとクライアント証明書と鍵Cを PC などから使用可能にしてしまうことができるか。攻撃者が使用前に行う必要があることを，25字以内で具体的に述べよ。

(6)　本文中の下線⑥について，この性質を何というか。10字以内で答えよ。

設問3　本文中の下線⑦について，保護するための適切な方法を本文中の用語を使って，25字以内で具体的に述べよ。

〔 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	13:10 ～ 13:50

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。
13. 午後Ⅱの試験開始は **14:30** ですので，**14:10** までに着席してください。