JP-RISSA
情報処理安全確保支援士会

情報処理安全確保支援士試験 対策セミナー #6 「こう出たR4春セキスペ解答解説」

2022年7月16日 19:30-21:00　於 YouTube Live

一般社団法人 情報処理安全確保支援士会

理事　村山直紀（むらやま･なおき）　@MurayamaNaoki

（情報処理安全確保支援士 登録番号第000029号）

資料の配布元など

JP-RISSA
情報処理安全確保支援士会

- 配布資料のURLは，本日19時過ぎに応募者（参加者＋補欠者）全員にconnpass経由でお送りしたメールに記しています。

- YouTube Live配信URLも，connpass経由のメールに記しています。
  - 後日，当会のYouTubeチャンネル（下記URL）で公開予定。
    - https://www.youtube.com/channel/UCSVHGI28t7h5sVCRO_P88DA

- 参考：本セミナーのconnpass募集ページ
  - https://connpass.com/event/245826/

TLP：WHITE

一般社団法人 情報処理安全確保支援士会

JP-RISSA
情報処理安全確保支援士会

- 設立目的
  「情報処理安全確保支援士」の活躍の場をひろげ、情報社会におけるサイバーセキュリティを含む情報セキュリティを取り巻く環境が向上することを目的とした団体。2019年8月に設立された任意団体を母体として、2020年4月に一般社団法人に改組。

開催の目的【会員の獲得】
入会金 コロナ割で0円（2023/3/11迄）
年会費4800円 詳しくはWebで。

- 主な運営体制
  - 代表理事・会長　山口　敏行
  - 副会長　清土　桂一郎、大島　真言、青羽　真利
  （理事：21名、監事：2名）

【会員の獲得】←ここ大事
① まずは受かってもらう
② 登録・有資格者になる
③ 当会に入会してもらう

- 会員　471名（2022年7月時点）

- WEB　https://www.jp-rissa.or.jp/
  https://twitter.com/jp_rissa

TLP：WHITE

過去のアーカイブ

- 対策セミナー #5「こう出た**R3秋セキスペ**解答解説」2022/1/15開催
  - 動画
    - https://youtu.be/WootX6IFd0g
  - スライド
    - https://www.jp-rissa.or.jp/wp-content/uploads/2022/01/JP-RISSA_R03-Autumn-Test_Ans.pdf
- 対策セミナー #4「こう出た**R3春セキスペ**解答解説」2021/7/17開催
  - 動画
    - https://youtu.be/GeyT_4zx1cE
  - スライド
    - https://www.jp-rissa.or.jp/wp-content/uploads/2021/08/20210717murayama_v2.pdf
- 対策セミナー #3「こう出た**R2セキスペ**解答解説」2021/1/16開催
  - スライド
    - https://www.jp-rissa.or.jp/wp-content/uploads/2021/04/JP-RISSA_R02-Autumn-Test_Ans.pdf

TLP：WHITE

本日の担当（村山直紀）

JP-RISSA
情報処理安全確保支援士会

- 電子デバイス・FPGA用論理合成ツールの輸入販売（H7～H11）
- IT人材育成に転じ，主に企業SE向け研修を担当（H11～）
- コンサルティング，資格試験対策書の執筆・監修（H18～）

本資料は【同書の追補】も兼ねる

- 修士（学術）電気通信大学（注：専門は社会情報学）
- RISS，電通主任（伝交･線路），ネットワークスペシャリスト ほか
- IEEE，情報処理学会，社会情報学会　各会員。当会理事。

TLP：WHITE

免責事項

JP-RISSA
情報処理安全確保支援士会

- 本資料は，村山直紀（以下「村山」）が独自に調査した結果や考察を公表したものであり，情報処理安全確保支援士試験の実施団体（以下「IPA」）の活動とは一切関係がありません。

盗用は340万円を村山に支払う事に同意したものとみなします。

- 本セミナーならびに本資料には，村山が後日，商用として書籍化するネタを多数投入しています。このため本セミナーの私的な録画・録音・写真撮影・スクリーンショットは禁止です。また本資料の再配布時の改変も禁止です。
- 本資料の内容について万全を期して作成しましたが，IPA公表の情報と本資料との間で内容に相違がある場合は，村山が特段の理由を示す場合を除き，IPAが公表する情報の内容が優先します。
- 本セミナーならびに本資料によって受講者が得た情報は，受講者の自己責任での御利用をお願いします。受講者が本セミナーならびに本資料によって受けた金銭その他の損害の責任を，村山ならびに（一社）情報処理安全確保支援士会（JP-RISSA）は一切負いません。
- 本セミナーは子育てママさんを勝手に応援します。

TLP：WHITE

なさっても構わないこと

- **セミナー中は主に，YouTube Live のチャットを拾います。**
- **ツイートはご自由に。**
  - **推奨ハッシュタグ #jprissa**（大文字の **#JPRISSA** も可）
  - ただし，セミナー中に村山がツイートを拾うのはキツいです。
- **後日，感想や概要をブログ等に書くのは大歓迎。**
  - 一点だけ。私（村山直紀）は名前を間違われるのを嫌がります。
- **他人に迷惑をかけない範囲での，飲酒 飲食 ノーマスクもOK。**
  - お好きなスタイルで。

TLP：WHITE

本日の進行予定

対策セミナー#6　7月16日（土）19時半 ～ 21時

- 当日の概要，JP-RISSAの紹介　5分（済み）
- こう出た【概観・午前Ⅱ】　10分
- こう出た【午後Ⅰ】　30分
- 休憩　5分
- こう出た【午後Ⅱ】　35分
- 質問，クロージング　5分

TLP：WHITE

こう出た【概観・午前Ⅱ】①

JP-RISSA
情報処理安全確保支援士会

問1　Web サーバのログを分析したところ，Web サーバへの攻撃と思われる HTTP リクエストヘッダが記録されていた。次の HTTP リクエストヘッダから推測できる，攻撃者が悪用しようとしていた可能性が高い脆弱性はどれか。ここで，HTTP リクエストヘッダ中の“%20”は空白を意味する。

〔HTTP リクエストヘッダの一部〕

```
GET /cgi-bin/submit.cgi?user=;cat%20/etc/passwd HTTP/1.1
Accept: */*
Accept-Language: ja
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent:  （省略）
Host: test.example.com
Connection: Keep-Alive
```

ア　HTTP ヘッダインジェクション（HTTP Response Splitting）
イ　OS コマンドインジェクション
ウ　SQL インジェクション
エ　クロスサイトスクリプティング

問2　SAML（Security Assertion Markup Language）の説明として，最も適切なものはどれか。

ア　Web サービスに関する情報を公開し，Web サービスが提供する機能などを検索可能にするための仕様
イ　権限がない利用者による読取り，改ざんから電子メールを保護して送信するための仕様
ウ　デジタル署名に使われる鍵情報を効率よく管理するための Web サービスの仕様
エ　認証情報に加え，属性情報と認可情報を異なるドメインに伝達するための Web サービスの仕様

午後Ⅱ問2設問3（1）～（4）に
SAMLのシーケンスの出題が。
→ 午前Ⅱ問2は，その前触れ？

午後Ⅰ問2設問2（2）では，こう書かせた。

TLP：WHITE

こう出た【概観・午前Ⅱ】②

JP-RISSA 情報処理安全確保支援士会

- 【「午前Ⅱ」新出題】①

R03秋SC午前Ⅱが「サイバーキルチェーン」初登場
昨秋に問われたのは，この用語の意味どまり

  - **問5**　標的型攻撃における攻撃者の行動をモデル化したものの一つに**サイバーキルチェーン**があり，攻撃者の行動を7段階に分類している。標的とした会社に対する攻撃者の行動のうち，**偵察の段階に分類されるもの**はどれか。
    - イ　攻撃者が，会社の役員が登録しているSNSサイトから，攻撃対象の人間関係，趣味などを推定する。
  - **問6**　**量子暗号の特徴**として，適切なものはどれか。
    - エ　量子通信路を用いて安全に共有した乱数列を使い捨ての暗号鍵として用いることによって，原理的に第三者に解読されない秘匿通信が実現できる。

R03秋SC午前Ⅱに出たのは
「PQC（耐量子計算機暗号）」

  - **問7**　安全・安心なIT社会を実現するために創設された制度であり，**IPA“中小企業の情報セキュリティ対策ガイドライン”に沿った情報セキュリティ対策に取り組むことを中小企業などが自己宣言するもの**はどれか。
    - エ　SECURITY ACTION

支援士がその業務で使う文書ゆえ，の出題？

TLP：WHITE

こう出た【概観・午前Ⅱ】③

JP-RISSA 情報処理安全確保支援士会

- 【「午前Ⅱ」新出題】②
  - **問9**　経済産業省とIPAが策定した**“サイバーセキュリティ経営ガイドライン（Ver2.0）”に関する記述のうち，適切なもの**はどれか。
    - イ　経営者が認識すべきサイバーセキュリティに関する原則と，経営者がリーダシップを発揮して取り組むべき項目を取りまとめたものである。

文書名「サ（略）」は既出でも，この選択肢は初

  - **問15**　**TLSに関する記述のうち，適切なもの**はどれか。
    - ウ　TLSで使用する個人認証用のデジタル証明書は，ICカードにも格納することができ，利用するPCを特定のPCに限定する必要はない。

既出だが，なんと「ディジタル」が「デジタル」に！

  - **問16**　**電子メールを**スマートフォンで**受信する際の**メールサーバとスマートフォンとの間の通信を，**メール本文を含めて暗号化するプロトコル**はどれか。
    - イ　IMAPS
  - **問19**　インターネットに接続されたPCの**時刻合わせに使用されるプロトコル**はどれか。
    - ウ　SNTP

「NTP」は基礎用語でも，その簡易版（Simple）である「SNTP」の出題はSC試験で初

TLP：WHITE

こう出た【概観・午前Ⅱ】④

JP-RISSA
情報処理安全確保支援士会

- 【「午前Ⅱ」新出題】③
  - **問21　データウェアハウスのメタデータ**に関する記述のうち，**データリネージ**はどれか。
    - ウ　データがどこから発生し，どのような変換及び加工を経て，現在の形になったかを示す情報であり，データの生成源の特定又は障害時の影響調査に利用できる。

lineage：原義は“血統，家系”

  - **問22　システムに規定外の無効なデータが入力されたとき，誤入力であることを伝えるメッセージを表示して正しい入力を促すことによって，システムを異常終了させない設計**は何というか。
    - ア　フールプルーフ

用語「フールプルーフ」は基礎用語だが，この問い方は，知る限りSC試験で初

  - **問23　JIS X 0160:2021（ソフトウェアライフサイクルプロセス）**によれば，ライフサイクルモデルの目的及び成果を達成するために，**ライフサイクルプロセスを修正するか，又は新しいライフサイクルプロセスを定義すること**を何というか。
    - イ　修整（Tailoring）

同規格は2021年版だが，書籍『共通フレーム2013』の改訂を伴わない。

こう出た【概観・午前Ⅱ】⑤

JP-RISSA 情報処理安全確保支援士会

- 【「午前Ⅱ」新出題】④
  - **問25**　金融庁“財務報告に係る内部統制の評価及び監査に関する実施基準（令和元年）”におけるアクセス管理に関して，**内部統制のうちのITに係る業務処理統制に該当するもの**はどれか。
    - ウ　組織内のアプリケーションシステムに，業務内容に応じた権限を付与した利用者IDとパスワードによって認証する機能を設ける。

- ア　組織としてアクセス管理規程を定め，統一的なアクセス管理を行う。
- イ　組織としてアクセス権限の設定方針を定め，周知徹底を図る。
- **ウ　組織内のアプリケーションシステムに，業務内容に応じた権限を付与した利用者IDとパスワードによって認証する機能を設ける。**
- エ　組織内の全ての利用者に対して，アクセス管理の重要性についての教育を行う。

ア イ エ の三つは「ITに係る全般統制」。ウの「ITに係る業務処理統制」よりも一歩引いた視点から，いわば“管理するための管理”を行っている。

TLP：WHITE

こう出た【概観・午前Ⅱ】⑥

JP-RISSA
情報処理安全確保支援士会

- 【「午後Ⅰ・Ⅱ」概観】その①
  - IPA『採点講評』より
    - **【午後Ⅰ】**
      - **問1**では，情報共有用のWebシステムの開発を題材に，**システム開発における脆弱性の分析と対策方法について**出題した。全体として**正答率は平均的**であった。
      - **問2**では，IoT機器の製品を題材に，**セキュリティインシデント対応と脆弱性対策について**出題した。全体として**正答率は平均的**であった。
      - **問3**では，スマートフォン向けQRコード決済サービスを題材に，**決済サービスで不正利用が発生するリスクとその対策について**出題した。全体として**正答率は平均的**であった。
    - **【午後Ⅱ】**
      - **問1**では，Webサイトのセキュリティを題材に，**脆弱性に関する知識，開発プロセスについて**出題した。全体として**正答率は平均的**であった。
      - **問2**では，クラウドサービスへの移行を題材に，**各種認証の仕組み，認証に関するセキュリティ対策について**出題した。全体として**正答率は平均的**であった。

各問「正答率は平均的」とあるが…
（今期もR03春秋も 全問この表現）

TLP：WHITE

検証

これを採点してみた。

JP-RISSA 情報処理安全確保支援士会

- 午後Ⅰ　A社 解答速報（1問50点，2問選択）
  - 問1　37点，　問2　44点，　問3　38点
  - （37＋44＋38）÷ 3 × 2 ＝ **79.33... 点**
- 午後Ⅰ　B社 解答速報（1問50点，2問選択）
  - 問1　50点，　問2　32点，　問3　38点
  - （50＋32＋38）÷ 3 × 2 ＝ **80 点**
- 午後Ⅱ　A社 解答速報（1問100点，1問選択）
  - 問1　89点，　問2　93点
  - （89＋93）÷ 2 ＝ **91 点**
- 午後Ⅱ　B社 解答速報（1問100点，1問選択）
  - 問1　81点，　問2　96点
  - （81＋96）÷ 2 ＝ **88.5 点**

【考察】低い。今期の出題は，誤答を生みやすそうだ。

【参考① R3 秋期試験】
午後Ⅰ
A社 92.66... 点
B社 92.66... 点
午後Ⅱ
A社 96.5点
B社 91.5点

【参考② R3 春期試験】
午後Ⅰ
A社 90点
B社 81.33... 点
午後Ⅱ
A社 87点
B社 96点

【参考③ R2 10月試験】
午後Ⅰ
A社 82.66... 点
B社 84.66... 点
午後Ⅱ
A社 87点
B社 81.5点

TLP：WHITE

こう出た【概観・午前Ⅱ】⑦

JP-RISSA 情報処理安全確保支援士会

- 【「午後Ⅰ・Ⅱ」概観】その②
  - 【午後Ⅰ】
    - **問1　Webアプリケーションプログラム開発のセキュリティ対策**に関する次の記述を読んで，設問1～3に答えよ。
    - **問2　セキュリティインシデント対応**に関する次の記述を読んで，設問1～4に答えよ。
    - **問3　スマートフォン向けQRコード決済サービスの開発**に関する次の記述を読んで，設問1～3に答えよ。
  - 【午後Ⅱ】
    - **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。
    - **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。

通例，二度あることは三度は無い。

「徳丸試験」テイスト出題が今期も！ 言語はJavaと一部SQL

ネットワーク技術（特にHTTP）と，Linuxの知識が得点を左右

本人確認（eKYC）と，公表された各種文書を題材とした出題

「徳丸試験」テイスト出題は午後Ⅱにも！ Webセキュリティと一部アジャイル開発

ネットワーク技術と，Kerberos，SAML，OAuth2.0，OpenID Connectのシーケンスを問う（作問者にとって楽な）出題

・誤解や別解を生じやすい出題が目立った，という印象。
・HTTPリクエストの知識が午後Ⅰ問1･2，午後Ⅱ問1･2で必要。
・特定の文献･プロトコルのシーケンスからの知識問題が目立つ。

※ 村山個人の感想です。

TLP：WHITE

本日の進行予定

対策セミナー#6　7月16日（土）19時半 ～ 21時

- 当日の概要，JP-RISSAの紹介　5分（済み）
- こう出た【概観・午前Ⅱ】　10分（済み）
- こう出た【午後Ⅰ】　30分
- 休憩　5分
- こう出た【午後Ⅱ】　35分
- 質問，クロージング　5分

TLP：WHITE

午後Ⅰ 問1

Webアプリケーションプログラム開発のセキュリティ対策に関する次の記述を読んで，設問1～3に答えよ。

「**問1**では，情報共有用のWebシステムの開発を題材に，**システム開発における脆弱性の分析と対策方法について**出題した。全体として**正答率は平均的**であった。」
（『採点講評』より）

通例，二度あることは三度は無い。

「徳丸試験」テイスト出題が今期も！ 言語はJavaと一部SQL

- 出題趣旨（『解答例』より）
  - システム開発においては，要件定義からテストまでの全てのプロセスでセキュリティ対策が必要であることは広く認識されている。一方で，アクセス制御における設計上の考慮不足や実装の不備による情報流出の被害事例が後を絶たない。たとえアクセス制御が単純なものであっても，問題が発生しているのが現実である。
  - 本問では，情報共有用Webアプリケーションプログラム開発のセキュリティ対策を題材として，システム開発の設計，実装，テストの各プロセスにおける脆弱性の分析及び修正に関わる能力を問う。

TLP：WHITE

R04春 SC午後Ⅰ問1 その①

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅰ問1設問1（1）

「Webアプリケーションプログラム（略）を開発する」H社は，「表1に示す方法に従って，脆弱性検査を実施する。

表1　脆弱性検査の方法（抜粋）

項番	脆弱性	検査の方法	脆弱性が検出された場合の対策方法
1	HTTP ヘッダインジェクション	利用者の入力を基に HTTP レスポンスヘッダを生成する処理において，①改行コードを意味する文字列を入力したときに，HTTP ヘッダフィールドが追加されないことを確認する。 （省略）	（省略）
2	SQL インジ	（省略）	SQL 文の組立てにおいて SQL 文のひ

「設問1（1）は，正答率がやや低かった。ウのHTML改行タグの解答が多かった。HTTPとHTMLの理解が不十分である結果と想定される。」（『採点講評』より）

【Q】表1中の下線①について，適切な文字列の例を，解答群の中から選び，記号で答えよ。

ア　%0D%0A　　イ　%20　　ウ　
　　エ　<p>

【A】「ア」

%0Dは“CR”，%0Aは“LF”

HTTPリクエストの構造	GETに存在しうる	POSTに存在しうる
・リクエストライン	○	○
・リクエストヘッダ	○	○
・（CR+LF）		○
・リクエストボディ		○

今期のSC［午後］では，**HTTPリクエストの構造の知識を踏まえさせた出題**が，下記に見られた。

午後Ⅰ 問1・問2　　午後Ⅱ 問1・問2

TLP：WHITE

R04春 SC午後Ⅰ問1 その②

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅰ問1設問1（2），設問1（3）

「Webアプリケーションプログラム（略）を開発する」H社は，「表1に示す方法に従って，脆弱性検査を実施する。

表1　脆弱性検査の方法（抜粋）

項番	脆弱性	検査の方法	脆弱性が検出された場合の対策方法
2	SQL インジェクション	（省略）	SQL 文の組立てにおいて，SQL 文のひな形の中に②変数の場所を示す？記号を置く技法を利用する。
3	メールヘッダインジェクション	（省略）	次のいずれかの対策を実施する。 (1)　メールヘッダを固定値にする。 (2)　外部からの入力を適切に処理するメール送信用 API を使用する。 (3)　外部からの入力の全てについて，［　a　］を削除する。

【Q1】表1中の下線②について，名称を，10字以内で答えよ。

【A1】「プレースホルダ（7字）」

【Q2】表1中の［　a　］に入れる適切な字句を，5字以内で答えよ。

【A2】「改行コード（5字）」

URLの後ろに付く“クエリ文字列”とは要区別。
今回のSC試験［午後］の特徴として，URLの“https://example.com/toiawase?id=12321”でいう“id=12321”部分，“クエリ文字列”についての出題が何問か出てくる。

ここでの『徳丸本2版』とは下記の本。

徳丸浩『体系的に学ぶ 安全なWebアプリケーションの作り方 第2版』（SBクリエイティブ[2018]）

徳丸本2版（p.270）「メールヘッダ・インジェクション脆弱性のまとめ」より引用。
【対策の概要】
「メール送信には専用のライブラリを使用した上で、以下のいずれかを行う。」
・「外部からのパラメータをメールヘッダに含ませないようにする」
・「外部からのパラメータをメールヘッダに含ませる場合は改行を含まないようにチェックする」

TLP：WHITE

R04春 SC午後Ⅰ問1 その③

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅰ問1設問2（1）

H社の「開発部では，**自部で開発したSシステムというWebシステムを利用して**，コーディングルールなどの**社内ルールを含む各種の情報を共有している**」。
1.5ページ略，Sシステム改修の担当者に任命された**Dさんが設計した「利用者のアクセス制御」は下記等。**
・「プロジェクトを識別する**プロジェクトIDを連番で採番**する。」
連番なので，有効なプロジェクトIDの値の推測は容易
・「利用者IDそれぞれに対して，その利用者が参加するプロジェクトのプロジェクトIDを登録しておく。」
・「**プロジェクトIDを次に示す方法で取得**し，そのプロジェクトIDを用いてアクセス制御する。」
「**方法1：**ログイン時にその利用者IDに対して（注：その人に一つだけ）登録されているプロジェクトIDを取得し，**GETリクエストのクエリ文字列に，“id=プロジェクトID”の形式で指定する。**（注：**Sシステムがもつ**）**情報選択機能は，クエリ文字列からプロジェクトIDを取得する。**」

この「方法1」の改善案は，次のスライド

H社の情報セキュリティ部は，**プロジェクトの各種情報を，「そのプロジェクトには参加していない利用者が，**③そのプロジェクトに参加しているかのように偽って**リスト可能であるという脆弱性**を指摘した。**これは，情報選択機能においてクエリ文字列で受け取ったプロジェクトIDをチェックせずに利用していることに起因**していた」。

【Q】本文中の下線③について，未参加のプロジェクトに参加しているかのように偽るための操作を，40字以内で具体的に述べよ。

ウソのGETリクエスト文字列を作って送りつける，の意。

【A】「クエリ文字列のidに，未参加のプロジェクトのプロジェクトIDを指定する。（36字）」

R04春 SC午後Ⅰ問1 その④

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅰ問1設問2（2）

H社の「開発部では，**自部で開発したSシステムというWebシステムを利用して**，コーディングルールなどの**社内ルールを含む各種の情報を共有している**」。
次ページの表2注記より，**Sシステムでは「利用者のログイン後，セッションIDでセッション管理を行っている。セッションIDは，ログイン時に発行される推測困難な値であり，secure属性が付与されたcookieに格納される**」。
次ページ，Sシステム改修の担当者に任命された**Dさんが設計した「利用者のアクセス制御」について**，H社の情報セキュリティ部は，**プロジェクトの各種情報を**，「そのプロジェクトには参加していない利用者が，（注：設問2（1）解答例，**URL中の「クエリ文字列のidに，未参加のプロジェクトのプロジェクトIDを指定する。」という操作によって**）③そのプロジェクトに参加しているかのように偽って**リスト可能であるという脆弱性**を指摘した」。「Dさんは，**プロジェクトIDの取得方法として，次に示す別の方法**を提示した」。
「**方法2：**情報選択機能の利用時に，**セッション情報から利用者情報を取得する**。情報選択機能は，当該利用者情報からプロジェクトIDを取得する。」

こう比較して尋ねているので，「方法1」には登場しない「セッションID」の強みを誉めただけ，例えば“セッションIDの推測は，他人には困難だから”はバツ。

「情報セキュリティ部は，④方法1の脆弱性が方法2で解決されることを確認した」。

【Q】本文中の下線④について，方法1の脆弱性が方法2で解決されるのはなぜか。30字以内で述べよ。

【A】【内一つ】「プロジェクトを示すパラメタを外部から指定できないから（26字）」「セッション情報からプロジェクトIDを取得するから（24字）」

文頭に“推測困難な値である「セッションID」に基づく”を補うと分かりやすい。

TLP：WHITE

R04春 SC午後Ⅰ 問1 その⑤

JP-RISSA 情報処理安全確保支援士会

DBへの接続を確立する「jdbc:mysql://（略）」とかが入る。

R04春SC午後Ⅰ 問1設問2（3），設問2（4）

```
5:        con = java.sql.DriverManager.getConnection(（省略）);      // データベースに接続する処理
6:        int projectId =（省略）;   // 利用者の参加プロジェクトのプロジェクトIDを利用者テーブル
                                          から取得し，代入する処理
7:        String sql = "SELECT 情報番号, 情報名 FROM 情報管理テーブル WHERE プロジェクトID = ?";
8:        java.sql.［    b    ］ stmt = con.prepareStatement(sql);
9:        ［    c    ］.setInt(1, projectId);
10:       java.sql.ResultSet rs = stmt.executeQuery();
```

プレースホルダの各「?」記号の，先頭から数えて「1」個目に代入する，の意。

図2　修正後の情報選択機能のソースコード（村山注：抜粋）

「stmt」は，プリコンパイルされたSQL文を示すオブジェクト

```
9:        java.sql.［    b    ］ stmt = con.prepareStatement(sql);
```

図3　修正後の情報表示機能のソースコード（村山注：抜粋）

【Q1】図2中及び図3中の［　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。
ア　Connection　　イ　DriverManager　　ウ　PreparedStatement　　エ　Statement

【A1】「ウ」

【Q2】図2中の［　c　］に入れる適切な字句を答えよ。

【A2】「stmt」

「設問2（3）は，正答率がやや低かった。StatementでもSQLの実装は可能であるが，本文に示されているプレースホルダの実装にはStatementを継承したPreparedStatementが必要である。」（『採点講評』より）

TLP：WHITE

R04春 SC午後Ⅰ 問1 その⑥

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅰ 問1設問3

「設問3は，正答率がやや低かった。SQLの構文が誤っている解答が見受けられた。データベースのアクセス制御の設計，実装及びレビューを行うために，SQLの構文やE-R図の表記法を知っておいてほしい。」（『採点講評』より）

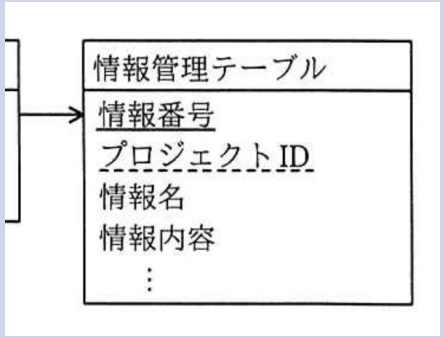


図1　参照するデータベースのE-R図（村山注：抜粋）

表示させたい情報の番号（属性「情報番号」）と，利用者が参加しているプロジェクトのID（属性「プロジェクトID」）は，プレースホルダ経由で受け取る。

「修正後の情報表示機能のソースコードを図3に示す。」

```
8:      String sql = "SELECT 情報番号, 情報名, 情報内容 FROM 情報管理テーブル WHERE ［　 d 　］";
9:      java.sql.（注：「PreparedStatement」（空欄b））　stmt = con.prepareStatement(sql);
        （省略） // SQL文のひな型に変数を代入する処理
```

図3　修正後の情報表示機能のソースコード（村山注：抜粋）

【Q】図3中の［　d　］に入れる適切な字句を，図1中の属性名を含めて答えよ。

【A】「情報番号 = ? AND プロジェクトID = ?」

9行目より後の「（省略） // SQL文のひな型に変数を代入する処理」に書かれる，stmt.setInt(何番目の?印か, その?印を置換する変数名)の，?印が何番目かという値さえ適切であれば，“ プロジェクトID = ? AND 情報番号 = ? ”も可能。
多分ヨーダ記法も可能。例えば，“ ? = 情報番号 AND ? = プロジェクトID ”，“ ? = プロジェクトID AND ? = 情報番号 ”

あんまりひねくれて書くと，採点者がうっかりバツにするリスクは高まる。

TLP：WHITE

午後Ⅰ 問2

セキュリティインシデント対応に関する次の記述を読んで，設問1～4に答えよ。

「**問2**では，IoT機器の製品を題材に，**セキュリティインシデント対応と脆弱性対策について**出題した。全体として**正答率は平均的**であった。」（『採点講評』より）

ネットワーク技術（特にHTTP）と，Linuxの知識が得点を左右

- 出題趣旨（『解答例』より）
  - IoT機器の普及に伴い，利用者が専門知識なしに容易に機器を設置できるようになる中，開発者がセキュリティを考慮していなかったり，利用者が脆弱性修正プログラムを適用していなかったりするケースが増えている。
  - 本問では，ルータやNASを題材として，IoT機器のインターネット接続に使われる技術，仕組みを理解するとともに，脆弱性を作り込んでしまうことの多いWeb機能についてセキュリティの観点から正しく実装する能力を問う。

TLP：WHITE

R04春 SC午後Ⅰ 問2 その①

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅰ 問2設問1（1）

ダイナミックDNSサービスを提供する「Z社のDNSサーバの設定で**ホスト名nas-aに割り当てているIPアドレスを変更するために，［　a　］レコードを更新**する。**そのレコードの［　b　］は，300秒に設定**されていた」。

出題のIPv6本格対応は，いつの日だろう…

【Q】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。

ア　A　　イ　MX　　ウ　TLS　　エ　TTL　　オ　TTY　　カ　TXT

【A】【a】「ア」，【b】「エ」

載録の順番を入れ替えています。

R04春SC午後Ⅰ 問2設問4

ダイナミックDNSサービスである「DDNS-Zを使用して製品Xにアクセスするための**URLは，インターネットの検索エンジンで特定のキーワードを検索すると容易に見つけることができてしまい，攻撃対象になりやすい**ことが分かった。**インターネットの検索エンジンで検索されないようにするために，各Webページの<head>セクションに<meta name="robots" content="［　h　］">を記載する**ことを検討した」。

【Q】本文中の［　h　］に入れる適切な字句を，英字10字以内で答えよ。

【A】【内一つ】「noindex（7字）」「none（4字）」

「設問4は，正答率が低かった。インターネット上でIoT機器を検出する方法と，それを抑止する方法を知っておいてほしい。」（『採点講評』より）

一般には「noindex」を記載するとして。他方の「none」とは？
→「none」は，「noindex」で実現できる事を含む。具体的には，「noindex」と「nofollow」の両方の効果が得られる。
∴ 本問が問う「インターネットの検索エンジンで検索されないようにするために」という目的は，「none」でも達成できる。

TLP：WHITE

R04春 SC午後Ⅰ問2 その②

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅰ問2設問1（2）

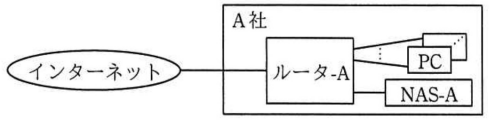


図1　A社のネットワーク構成（抜粋）

「NAS製品である製品X」の，A社内での呼称

表1　NAS-Aの設定内容（抜粋）

設定項目	設定値	説明
ファイル共有機能	・SMB：有効 ・NFS：無効	有効に設定したプロトコルで，ファイルを共有する。
UPnP[1]設定要求機能	・有効 ・製品YのWAN側TCPポート：443 ・NAS-AのTCPポート：443	左記の設定にすると，製品YのWAN側ポート宛てのパケットをNAS-Aのポートにフォワードする設定を製品Yに要求する。
Web操作機能	・有効	Webブラウザから HTTPSで，一般利用者権限のアカウントで本機能にログイン後，ファイルの操作ができる。
Web管理機能	・有効	Webブラウザから HTTPで，管理者権限のアカウントで本機能にログイン後，NAS-Aの設定変更などができる。

注[1]　Universal Plug and Playの略称。認証なしでリクエストを受け付ける仕様のプロトコルである。

「ルータ製品である製品Y」の，A社内での呼称

「全て拒否」ですけど…

表2　ルータ-Aの設定内容（抜粋）

設定項目	設定値	説明
ファイアウォール機能	・インバウンド通信：全て拒否[1] ・アウトバウンド通信：全て許可	ステートフルパケットインスペクション型である。
UPnP機能	・LAN側：有効	LAN側の機器から受け付けたリクエストの内容で，ポートフォワーディングの設定とファイアウォール機能の設定を行う。①WAN側は，本機能を有効にできない仕様になっている。

注記　ルータ-Aがインターネットに接続するためのISP回線では，グローバルIPアドレスが動的に割り当てられる。

注[1]　UPnP機能による設定が優先される。

あっ！こんなこと書いてある

【Q】表2中の下線①について，WAN側でUPnP機能を有効にできる仕様とした場合，ルータ-Aが操作されることによって，どのようなセキュリティ上の問題が発生するか。発生する問題を，30字以内で述べよ。

【A】「外部からLAN側への通信の許可設定が変更される。（24字）」

意味は，“ルータ-Aがもつ，せっかくのファイアウォール機能をオーバーライドしてしまう。”

どゆこと？ 表1には「UPnP設定要求機能」として，「製品YのWAN側TCPポート：443」と書いてある。だけど表2には，「UPnP機能」は「①WAN側は，本機能を有効にできない仕様になっている。」とあり，“製品Y（ルータ-A）のWAN側はUPnPを有効にできない，という仕様”だと読めるんだけど。
→ 表1の「UPnP設定要求機能」と，表2の「UPnP機能」は，言葉の意味が違う。また，下線①の文意は，“製品Y（ルータ-A）のWAN側インタフェースに設定用のイーサネットケーブルとかをつないでも，そこ経由では，製品Y（ルータ-A）の設定をいじれない”ということ。

TLP：WHITE

R04春 SC午後Ⅰ問2 その③

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅰ問2設問1（3）

Z社の**NAS製品である「製品X」は「Linuxをベースとした OSを搭載している」**。
1.8ページ略，Z社のK氏が，**A社内に設置した製品X（NAS-A）を調査して分かったことは**，共にNAS-Aの機能である**「ファイル共有機能でもWeb操作機能でもアクセスできない/rootディレクトリ配下のファイルも暗号化されていた。」**等。
「K氏は，今回の障害がランサムウェアに起因するものであり，さらに，（注：NAS-Aを利用する）②A社のPCがランサムウェアに感染したのではなく，NAS-A自体がランサムウェアに感染したことによってNAS-Aのファイルが暗号化された可能性が高いと判断した」。

【Q】本文中の下線②のように判断した理由を，40字以内で述べよ。

【A】「PCからのファイル操作ではアクセスできない領域のファイルが暗号化されたから（37字）」

意味は，“NAS-A自身からしかアクセスできない領域のファイルが暗号化されているから（37字）”

R04春SC午後Ⅰ問2設問2（1）

製品Xは**「http://192.168.0.1/images/..%2fstatus.cgiのURLにアクセスすると，http://192.168.0.1/status.cgiに認証なしでアクセスできてしまう。これは，URLに“..%2f”を使用した［　c　］と呼ばれる攻撃手法**である」。

【Q】（略）［　c　］に入れる適切な字句を，15字以内で答えよ。

【A】「パストラバーサル（8字）」

“..%2f” は，URLデコードで “../” に置換される。

“ディレクトリトラバーサル” はバツ？
徳丸本2版にも，IPA『安全なウェブサイトの作り方』にも，“デ（略）” と書いてあるし。はて…🤔

“URL上のパスと，Webサーバでのファイル格納上のパス（ディレクトリ構成）とは，厳密に言うと1対1には対応しない”，とかそういうこと？

TLP：WHITE

R04春 SC午後Ⅰ問2 その④

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅰ問1設問2（2）

NAS製品である「**製品Xには，Web管理機能の一つとして，IPアドレスを指定してpingを実行する機能がある。このIPアドレスの処理に脆弱性があり，任意のOSコマンドを実行できてしまう。**次は，その脆弱性を悪用した例であり，**“ping 127.0.0.1;whoami”というコマンドが実行される。**

```
POST /ping.cgi HTTP/1.0
Content-Length: 21

addr=127.0.0.1;whoami
```

伏線回収その①
午後Ⅰ問1設問1（1）「ア %0D%0A」
（%0Dは“CR”，%0Aは“LF”）

これは，［　d　］と呼ばれる攻撃手法である」。

【Q】（略）［　d　］に入れる適切な字句を，15字以内で答えよ。

【A】「OSコマンドインジェクション（14字）」

伏線回収その②
午前Ⅱ問1「イ　OSコマンドインジェクション」

問1　Web サーバのログを分析したところ，Web サーバへの攻撃と思われる HTTP リクエストヘッダが記録されていた。次の HTTP リクエストヘッダから推測できる，攻撃者が悪用しようとしていた可能性が高い脆弱性はどれか。ここで，HTTP リクエストヘッダ中の“%20”は空白を意味する。

〔HTTP リクエストヘッダの一部〕

```
GET /cgi-bin/submit.cgi?user=;cat%20/etc/passwd HTTP/1.1
Accept: */*
Accept-Language: ja
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: （省略）
Host: test.example.com
Connection: Keep-Alive
```

ア　HTTP ヘッダインジェクション（HTTP Response Splitting）
イ　OS コマンドインジェクション
ウ　SQL インジェクション
エ　クロスサイトスクリプティング

TLP：WHITE

R04春 SC午後Ⅰ問2 その⑤

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅰ問2設問2（3）

「NAS製品である製品X」

脆弱性1
製品Xでは，除外リスト[1]に次のディレクトリが指定されている。

```
/css
/images
/js
```

認証なしアクセスの処理に脆弱性があり，除外リストに指定されていないディレクトリ配下のファイルにも認証なしでアクセスできてしまう。例えば，http://192.168.0.1/images/..%2fstatus.cgi のURLにアクセスすると，http://192.168.0.1/status.cgi に認証なしでアクセスできてしまう。これは，URLに“..%2f”を使用した［ c ］と呼ばれる攻撃手法である。

空欄c「パストラバーサル」

注[1] 除外リストに指定されたディレクトリ配下のファイルには，認証なしでアクセスできる。除外リストは，利用者が変更できない。

パッチMでは，脆弱性1の対策として，認証なしアクセスの処理の流れにパス名の正規化の処理を加え，さらに，図3に示す順序にした。パス名の正規化とは，相対パスで記述されたパス名を，相対パス記法を含まない形式に変換することである。

［ e ］ → ［ f ］ → ［ g ］

図3 パッチM適用後の認証なしアクセスの処理の流れ

【Q】図3中の［ e ］～［ g ］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。
ア URLデコード　　イ 除外リストとの比較　　ウ パス名の正規化

【A】【e】「ア」，【f】「ウ」，【g】「イ」

「設問2（3）は，正答率が平均的であった。本文に示した認証なしでアクセスできるURLでは除外リストとの比較に漏れがないように，URLデコードを行った上で，“../”などを含んだパス名を正規化してから，除外リストとの比較を行う必要があることを理解してほしい。」（『採点講評』より）

①まず，「ア（URLデコード）」で，パーセントエンコードを普通の文字（列）に変換する。（例：「%2f」→「/」）
②次に「ウ（パス名の正規化）」で，「../」とかを正しく解釈しなおす。すると，“http://192.168.0.1/status.cgi”という文字列が得られる。
③その後「イ（除外リストとの比較）」をすれば，“「除外リスト」に合致しないから，認証無しではアクセスさせない。”と適切に判断できる。

TLP：WHITE

R04春 SC午後Ⅰ 問2 その⑥

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅰ 問2設問3（1）

〔アクセスログの調査〕

NAS-A のアクセスログを調査したところ，外部から HTTPS リクエストを使用して OS コマンドを実行する攻撃ツール（以下，WebShell という）が NAS-A に配置されており，OS コマンドが実行されたことが分かった。NAS-A のアクセスログから WebShell に関連するものを抽出した結果を表 3 に示す。

表 3　WebShell に関連する NAS-A のアクセスログ

No.	時刻	リクエスト	ステータスコード	応答バイト数
1	13:01	GET /images/..%2fstatus.cgi HTTP/1.1	200	634
2	13:02	POST /images/..%2fping.cgi HTTP/1.1	200	418
⋮	⋮	⋮	⋮	⋮
18	13:05	GET /images/shell.cgi?cmd=whoami HTTP/1.1	200	1418
⋮	⋮	⋮	⋮	⋮
89	13:18	POST /images/shell.cgi HTTP/1.1	200	2490

注記　一部の項目は省略している。

意味は “表3から読み取れる範囲では”

「POST」の行には，この部分が書かれていない。

「**表3からは**，GETメソッドを使用して実行されたOSコマンドの内容は分かったが，③POSTメソッドを使用して実行されたOSコマンドの内容は分からなかった」。

【Q】本文中の下線③について，実行されたOSコマンドの内容が分からなかった理由を，35字以内で述べよ。

【A】「POSTメソッドで送信したボディがアクセスログに残っていなかったから（34字）」

【この解答例の解釈について】
決して，“GETとは異なり，そもそもPOSTのリクエストは「HTTPリクエストボディ」をもたないから”ではない。逆！

正しい解釈は，“POSTメソッドで送信された「HTTPリクエストボディ」を，アクセスログ（表3）では記録していなかったから（53字，字数オーバ）”。

TLP：WHITE

覚え方を考えてみた。

- あれ。**“GET”と“POST”，HTTPリクエストボディが付くのは，どっちだっけ…？**
  - 用意するもの。八尺様（みんな大好き高身長女子）
- **「ぽぽぽ…」の八尺様は高身長 → ぽ（PO）の方が長い**
  - ここでいう「長い」は，CR+LF や HTTPリクエストボディが続く，の意。

こちらは尺八様（イメージ図）　©山野楽器
https://www.yamano-music.co.jp/lesson/adult/shakuhachi

HTTPリクエストの構造	GETに存在しうる	POSTに存在しうる
・リクエストライン	○	○
・リクエストヘッダ	○	○
・（CR+LF）		○
・リクエストボディ		○

ここらへんが八尺様の本気

TLP：WHITE

R04春 SC午後Ⅰ 問2 その⑦

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅰ 問2設問3（2）

「WebShellが配置されたディレクトリは，書込み不可であるが，rootアカウントを用いれば書込み可能に変更できる。**製品Xでは，sudoコマンドの設定ファイルが図4のようになっている。**」

```
www ALL=NOPASSWD: /bin/tar
```

図4　sudoコマンドの設定ファイル（抜粋）

/etc/sudoers ファイル

「tarコマンドは，標準のOSコマンドであり，複数のファイルを一つのアーカイブファイルにまとめたり，アーカイブファイルを展開したりできる。**製品Xでは，ファームウェアのアップデート時，wwwアカウントの権限でsudoコマンドを使用してtarコマンドを実行することで，rootアカウントの権限でアーカイブファイルを展開**している。この**tarコマンドには，任意のOSコマンドを実行できるオプションがある。ただし，ファームウェアのアップデート時にこのオプションは使用していない。**当該オプションを悪用する例を図5に示す。」

```
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=whoami
```

図5　tarコマンドのオプションを悪用する例

「設問3（2）は，正答率が平均的であった。ファームウェアのアップデート時にアーカイブファイルを展開するために使っているtarコマンドが，製品Xでは不要なオプションも使える設定であり，本設問は，そのようなオプションの悪用を防ぐ対策を問うているので，sudoの設定でオプションの使用を制限するなど，具体的に解答してほしい。」（『採点講評』より）

「K氏は，“攻撃者が，Web管理機能の脆弱性とtarコマンドのオプションを悪用し，書込み不可のディレクトリを書込み可能に変更してWebShellを配置した後，WebShellを使用してランサムウェアを実行した”と推測した。そこで，④製品Xでtarコマンドのオプションが悪用されるのを防ぐ対策を検討することにした。」

【Q】本文中の下線④について，対策を，50字以内で具体的に述べよ。

/bin/tar の後に，正規表現に似たワイルドカードを書き足す設定で，マッチング処理ができる（らしい）

【A】「sudoコマンドの設定ファイルで，tarコマンドのオプションを受け付けないように設定する。（45字）」

【設問4はスライドp.26下】

TLP：WHITE

午後Ⅰ 問3

スマートフォン向けQRコード決済サービスの開発に関する次の記述を読んで，設問1～3に答えよ。

「**問3**では，スマートフォン向けQRコード決済サービスを題材に，**決済サービスで不正利用が発生するリスクとその対策について**出題した。全体として**正答率は平均的**であった。」（『採点講評』より）

本人確認（eKYC）と，公表された各種文書を題材とした出題

- 出題趣旨（『解答例』より）
  - 近年，スマートフォンを用いた決済において不正利用事件が多発している。IPAが公開している“情報セキュリティ10大脅威”の個人部門では“スマホ決済の不正利用”が2020年度，2021年度で1位となっており，サービス提供者による対策が望まれている。
  - 本問では，スマートフォン向けQRコード決済サービス用プログラムの開発を題材として，不正利用が発生するリスクとサービス提供者での対策について，セキュリティの観点での対応力を問う。

TLP：WHITE

R04春 SC午後Ⅰ 問3 その①

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅰ 問3設問1

「L社は，**QRコードを利用した実店舗向けの決済サービス（以下，Qサービスという）**を提供することを決め，Qサービス用のサーバプログラムと，**Qサービスを利用するためのスマートフォン向けアプリケーションプログラム（以下，Qアプリという）**を開発することになった」。

表1　Qサービス用のサーバプログラム及びQアプリの機能ごとの概要

機能	概要
アカウント作成	・Qサービスのアカウント情報として，利用者IDとパスワード，氏名，生年月日，携帯電話番号を登録する。
Qサービスへのログイン	・利用者IDとパスワードでQサービスにログインする。ログインに連続して5回失敗すると，アカウントが一時的にロックされる。
銀行口座との［　a　］	・利用者の銀行口座との［　a　］は，手順を次に示す。

【認証の3要素】
・知識によるもの：Something You Know
・所持によるもの：Something You Have
・身体的な特徴（生体）によるもの：Something You Are

「経済産業省が2020年に公表した**“オンラインサービスにおける身元確認手法の整理に関する検討報告書”**」では，「**身元確認は，“登録する氏名・住所・生年月日等が正しいことを証明／確認すること”**と定義されている。また，**当人認証は，“認証の3要素のいずれかの照合で，その人が作業していることを示すこと”**と定義されている。したがって，Qサービスにおいては，**表1の［　a　］時に身元確認を，表1の［　b　］時に当人認証を実施する**ことになる」。

【Q】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。
ア　Qサービスへのログイン　　イ　アカウント作成

【A】【a】「イ」，【b】「ア」

【参考文献】経済産業省「オンラインサービスにおける身元確認手法の整理に関する検討報告書を取りまとめました」
https://www.meti.go.jp/press/2020/04/20200417002/20200417002.html
【別の箇所の空欄aで登場】「犯罪による収益の移転防止に関する法律施行規則」
https://elaws.e-gov.go.jp/document?lawid=420M60000f5a001

TLP：WHITE

R04春 SC午後Ⅰ 問3 その②

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅰ 問3設問2（1）

「L社は，**QRコードを利用した実店舗向けの決済サービス（以下，Qサービスという）**を提供することを決め，Qサービス用のサーバプログラムと，**Qサービスを利用するためのスマートフォン向けアプリケーションプログラム（以下，Qアプリという）**を開発することになった」。

【表1中の「銀行口座とのひも付け」】
「利用者の銀行口座とのひも付けを行う。手順を次に示す。」
「（1）Qアプリ上では，Qサービスの連携先としてあらかじめL社と契約した銀行がリストされている。利用者は，そのリストから銀行を一つ選択する。**選択された銀行には，利用者を認証するために，Qサービスを介してアカウント情報の氏名が提供される。**」
「（2）次に，当該銀行が運用する口座振替登録用のWeb画面が開かれるので，**利用者は，口座番号，キャッシュカードの数字4桁の暗証番号を入力する。**」
「（3）（1）で提供された情報と（2）で入力された情報が共に正しければ認証に成功し，アカウントと利用者の銀行口座とのひも付けが完了する。連続して認証に5回失敗すると，当該口座とのひも付けができなくなる。」

L社の「C課長は，**表1の銀行口座とのひも付けでは，キャッシュカードの所持が確認されず，暗証番号で照合されるだけ**なので，**攻撃者が他人の氏名で**（注：**Qサービスの**）**アカウント作成を行い，**①他人の銀行口座とのひも付けを行う**リスク**を低減するためには（略）身元確認を実施する必要があると指摘した」。

【Q】本文中の下線①について，攻撃者はどのようにして他人の銀行口座とのひも付けを成功させるか。その方法を二つ挙げ，それぞれ30字以内で述べよ。

解答例が公表されて，初めて分かった。設問にある「その方法」の「その」が指すのは，
× ひも付けを成功させる　○（ひも付けを成功させるために）他人の銀行口座を把握する

【A】【順不同】「漏えいしている口座番号と暗証番号を悪用する方法（23字）」「口座番号と暗証番号をだまして聞き出し，悪用する方法（25字）」

下線①の直前，「攻撃者が他人の氏名でアカウント作成を行い，」の正しい解釈は，“先に攻撃者は（不正に）他人さんの口座番号と暗証番号を把握済み”。その把握を済ませた上で，下線①を行う，という話。

TLP：WHITE

R04春 SC午後Ⅰ問3 その③

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅰ問3設問2（2），設問2（3），設問2（4）

表2　個人顧客向けの本人確認方法

項番	分類	方法
1	本人確認書類を用いた方法	次の2点を用いた方法 ・［　c　］付き本人確認書類の画像 ・容貌の画像
2		次の2点を用いた方法 ・［　c　］付き本人確認書類のICチップ情報 ・容貌の画像
5	電子証明書を用いた方法	公的個人認証サービスの署名用電子証明書[1]を用いた方法
6		民間事業者発行の電子証明書を用いた方法

注[1]　マイナンバーカードに記録された署名用電子証明書

下記が本問の元ネタ。IPA解答例の「写真」という表現も，文書内そのまま。
『犯罪収益移転防止法における オンラインで完結可能な本人確認方法の概要』
https://www.fsa.go.jp/common/law/guide/kakunin-qa/2.pdf

「**マイナンバーカードには，地方公共団体情報システム機構が発行した署名用電子証明書などが格納されている。**（注：本問で提供する）Qサービスの利用者は，NFC機能のあるスマートフォンを利用して，マイナンバーカードを読み取り，署名用電子証明書のパスワードを（注：今回開発する）Qアプリに入力する。**入力されたパスワードが正しい場合，マイナンバーカード内の［　d　］でQサービスの申込用のデータにデジタル署名**し，当該デジタル署名，当該データ本体，署名用電子証明書をQサービスに送付する。Qサービス側で，**デジタル署名が利用者本人のものであり，改ざんされていないことをQサービスの利用者の［　e　］を用いて確認**した後，**地方公共団体情報システム機構に［　f　］を確認**する」。

【Q1】表2中の［　c　］に入れる適切な字句を，5字以内で答えよ。

【A1】「写真（2字）」

“本人の顔写真”という意味が読み取れる表現なら，マルが付いたと考えられる。

【Q2】本文中の［　d　］，［　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。
ア　共通鍵　　イ　公開鍵　　ウ　秘密鍵

【A2】【d】「ウ」，【e】「イ」

【Q3】本文中の［　f　］に入れる適切な字句を，15字以内で述べよ。

【A3】【内一つ】「署名用電子証明書の有効性（12字）」「署名用電子証明書の失効の有無（14字）」

「設問2（4）は，正答率が低かった。公開鍵暗号の仕組みにおいて，電子証明書の有効性を確認する方法が必要となるが，このことを理解していないと思われる解答が多かった。公的個人認証サービスでは，地方公共団体情報システム機構（J-LIS）がOCSPによる方法とCRLによる方法を提供している。これらの方法について知っておいてほしい。」（『採点講評』より）

R04春 SC午後Ⅰ問3 その④

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅰ問3設問2（5）

【表2中の項番1：「本人確認書類を用いた方法」】
「**次の2点を用いた方法**」
・「（注：「**写真**」（空欄c））**付き本人確認書類の画像**」
・「**容貌の画像**」

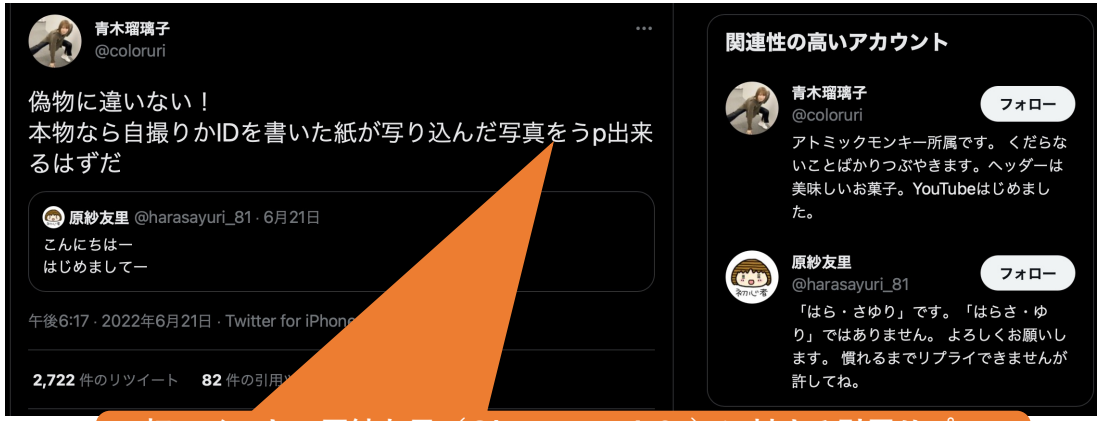
C課長「項番1では**事前に準備した他人の画像を用いられないようにする**必要がある。」
Bさん「どうすればよいでしょうか。」
C課長「完全な対策はないが，**政府が犯収法規則の改正において意見公募を実施した際の“警察庁及び共管各省庁の考え方”に記載されている方法**を採用すると，（注：**スマホ用の今回開発する**）**“Qアプリが毎回ランダムな数字を表示し，利用者が［　g　］して，直ちに送信することによって，L社では提出された画像が事前に準備されたものではないことを確認する”という方法**が考えられる。この方法で身元確認しよう。」

【Q】本文中の［　g　］に入れる適切な字句を，40字以内で述べよ。

【A】「そのランダムな数字を紙に書き，その紙と一緒に容貌や本人確認書類を撮影（34字）」

【まじめに解くなら，この文書】
『「犯罪による収益の移転防止に関する法律施行規則の一部を改正する命令案」に対する意見の募集結果について』
https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000212472

【参考】2022/6/21 青木瑠璃子（@coloruri）のツイート
https://twitter.com/coloruri/status/1539175678582886400



初ツイートの原紗友里（@harasayuri_81）に対する引用リプ。「古のねらーやめろw」「インターネット老人会で草」など大反響

「設問2（5）は，正答率がやや低かった。Qアプリが表示するランダムな数字について，“当該数字を撮影する”という解答が多かった。そういった方法では，撮影したのが本人なのかを確認できない。オンラインにおける本人確認手法は，今後も様々な手法が提案されると思われるが，現在使われている最新の手法を理解しておいてほしい。」（『採点講評』より）

TLP：WHITE

R04春 SC午後Ⅰ問3 その⑤

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅰ問3設問3（1），設問3（2）

「L社は，**QRコードを利用した実店舗向けの決済サービス（以下，Qサービスという）**を提供することを決め，Qサービス用のサーバプログラムと，**Qサービスを利用するためのスマートフォン向けアプリケーションプログラム（以下，Qアプリという）**を開発することになった」。

3.6ページ略，L社のBさんは，「利便性を向上させるために，**ログインが成功した場合は，1か月間，ログイン状態を保持する**ことを考えた。**しかし**，②Qサービスにログインした状態で，スマートフォンの画面ロックを設定していないと，Qサービスが不正利用されることがある。そこで，**Qサービスにログインした状態を保持することにした上で**，③Qアプリに不正利用を防ぐための機能を追加することにした」。

【Q1】本文中の下線②について，スマートフォンの画面ロックを設定していないと，どのような場合に不正利用が行われるか。20字以内で具体的に述べよ。

【A1】「スマートフォンを盗まれた場合（14字）」

「設問3（1）は，正答率が平均的であった。オンラインサービスの設計では，どのような不正が発生するのかを洗い出して，対策を検討することを心掛けてほしい。」（『採点講評』より）

【Q2】本文中の下線③について，どのような機能が考えられるか。30字以内で具体的に述べよ。

【A2】「Qアプリの起動時に，PINコードで利用者を認証する機能（27字）」

“強制的にログアウトさせる機能”はバツ。
村山は最初“生体認証をさせる”と思いましたが，IPAが「PINコード」を正解としたのは，右記の記述からではと。（問題冊子 p.17）
“低機能なスマホでも「Qサービス」を行いたい”という願いから。

B さん：項番 5 の方法では，利用者が NFC 機能のあるスマートフォンとマイナンバーカードを用意する必要があるのですね。それならば，項番 1 の方が，利用者にとっては利用しやすい方法と言えそうです。項番 1 では，注意点はありますか。

TLP：WHITE

本日の進行予定

対策セミナー#6　7月16日（土）19時半 ～ 21時

- 当日の概要，JP-RISSAの紹介　5分（済み）
- こう出た【概観・午前Ⅱ】　10分（済み）
- こう出た【午後Ⅰ】　30分（済み）
- 休憩　5分
- こう出た【午後Ⅱ】　35分
- 質問，クロージング　5分

TLP：WHITE

本日の進行予定

対策セミナー#6　7月16日（土）19時半 ～ 21時

- 当日の概要，JP-RISSAの紹介　5分（済み）
- こう出た【概観・午前Ⅱ】　10分（済み）
- こう出た【午後Ⅰ】　30分（済み）
- 休憩　5分（済み）
- こう出た【午後Ⅱ】　35分
- 質問，クロージング　5分

TLP：WHITE

午後Ⅱ 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。

「**問1**では，Webサイトのセキュリティを題材に，**脆弱性に関する知識，開発プロセスについて**出題した。全体として**正答率は平均的**であった。」（『採点講評』より）

「徳丸試験」テイスト出題は午後Ⅱにも！
Webセキュリティと一部アジャイル開発

- 出題趣旨（『解答例』より）
  - アジャイル開発を行っている企業が増えている中，短期間でリリースすることを優先した結果，システムの脆弱性対応が後回しになっているケースも見られる。
  - 本問では，Webサイトのセキュリティを題材として，Webサイトにおける脆弱性対策の理解力，開発プロセスの変化に応じたセキュリティへの対応方法を検討する能力を問う。

R04春 SC午後Ⅱ問1 その①

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅱ問1設問1（1）

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。

（村山注：XSSは「クロスサイトスクリプティング」の略）

```
（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

【Q】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。

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)><"

【A】「ア」

「ア」の「confirm?"><img src=1 onerror=alert(1)><"」が「scriptName」部分に，下記のように代入される。サーバ名は“example.com”。
「 <meta property="og:url" content="https://example.com/confirm?"><img src=1 onerror=alert(1)><"?"> 」

TLP：WHITE

R04春 SC午後Ⅱ問1 その②

JP-RISSA 情報処理安全確保支援士会

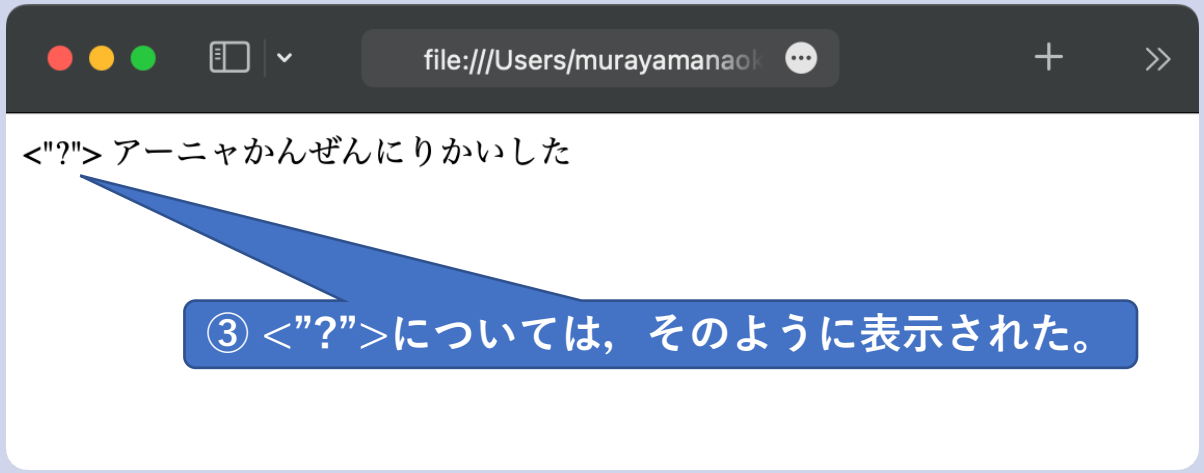
【つづき】R04春SC午後Ⅱ問1設問1（1）

【よく分からん（特に「<”?”>」の扱いが）から選択肢「ア」で作ってみた。】

```
<?xml version=”1.0” encoding=”utf-8”?>
<html>
<head>
  <meta property=”og:url” content=”https://example.com/confirm?”><img src=1 onerror=alert(1)><”?”>
  <title>（R04春SC午後Ⅱ問1設問1（1））確認用</title>
</head>
<body>
  アーニャかんぜんにりかいした<br>
</body>
</html>
```

「ア」がうまく刺さったもの

『SPYxFAMILY』©2022 遠藤達哉／集英社



TLP：WHITE

R04春 SC午後Ⅱ問1 その③

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅱ問1設問1（2）

ITサービス会社の「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**（注：クロスサイトスクリプティング）**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」。

【Q】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。

【A】【内一つ】「ダウンロードするライブラリに既知の脆弱性がないかを確認する。（30字）」「特定のWebサイトからの入手をルール化し，明文化する。（27字）」

【疑問その①-1】
B社が「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」らしい。

【疑問その①-2】
…と書いてあるのになんで，B社が使った「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」だったの？ 前言はウソ？

【疑問その②】
IPA公表の解答例の中には，“使用するライブラリには，常に最新版を用いる。”という線の答が無い。なんで？

【次スライド】
本問の解釈，これしかない！

TLP：WHITE

利用している。
（利用しているとは言ってない）

R04春 SC午後Ⅱ問1 その④

JP-RISSA 情報処理安全確保支援士会

【再掲】R04春SC午後Ⅱ問1設問1（2）

ITサービス会社の「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**（注：クロスサイトスクリプティング）**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」。

【Q】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。

【A】【内一つ】「ダウンロードするライブラリに既知の脆弱性がないかを確認する。（30字）」「特定のWebサイトからの入手をルール化し，明文化する。（27字）」

【この解釈で辻褄が合う】
ここの「利用している。」の意味は，

× 利用している。（事実）
○ 利用することにしている。（制度）

利用している。
（利用しているとは言ってない）

【疑問その① タネ明かし】
B社が使った「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」。これを，B社では社内ルールを破って使っていた。

【疑問その② タネ明かし】
IPA解答例の言いたいことは，“「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（略）ダウンロードし，利用」するよう，ルール化する。”

『採点講評』では本問，スルーされた。

TLP：WHITE

R04春 SC午後Ⅱ問1 その⑤

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅱ問1設問2

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。

（村山注：CSRFは「クロスサイトリクエストフォージェリ」の略）

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

csrftoken=3f4aee446f680df6e0842d7179fcefd00fe5b232
```

CR+LF（八尺様の本気）

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。

徳丸本2版 p.196に「SameSite-Lax」の言及あり。

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。

別の値の発行は，なされるが…（という話）

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。

【Q】本文中の［ a ］，［ b ］に入れる適切な字句を答えよ。

“セッションID”も，許される答かなと思います。

【A】【a，b順不同】【a】「利用者ID」，【b】「セッションオブジェクト」

TLP：WHITE

R04春 SC午後Ⅱ問1 その⑥

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。

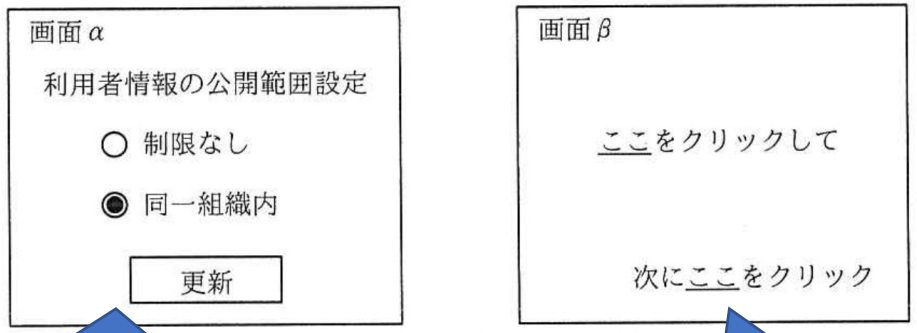


図3　攻撃者が用いる画面

操作できる手前（パワポでいう「最前面」）を透明に

奥（同「最背面」）を可視に

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。

半年前も「Content-Security-Policy」が出た。

R04春SC午後Ⅱ問1設問3（1），設問3（2）

【Q1】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

『安全なウェブサイトの作り方 改訂第7版』p.41～43「1.9 クリックジャッキング」https://www.ipa.go.jp/files/000017316.pdf

【A1】【c】「イ」，【d】「ア」，【e】「ア」，【f】「ア」，【g】「イ」，【h】「イ」

【Q2】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。

ア　Content-Disposition
イ　Content-Security-Policy
ウ　X-Content-Type-Options
エ　X-Frame-Options

空欄iは徳丸本2版p.197と『安全なウェブサイトの作り方 改訂第7版』p.42に言及あり。空欄jは徳丸本2版p.428。確かにこの策を使えば，他所から付け入る隙を与えないことでクリックジャッキングを防ぐ，という目的は達成できる。

【A2】【i】「エ」，【j】「イ」

「設問3（2）は，正答率が低かった。クリックジャッキングの対策に使うレスポンスヘッダについては，標準化の動向を含めて正しく理解しておいてほしい。」（『採点講評』より）

TLP：WHITE

R04春 SC午後Ⅱ問1 その⑦

JP-RISSA 情報処理安全確保支援士会

R04春SC午後Ⅱ問1設問4

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/

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。

HTTPリクエスト中の「topicの値」

```
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。（村山注：SSRFは「サーバサイドリクエストフォージェリ」の略）

「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」のURL

【Q】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。

【A】「topicの値をhttps://db-y.b-sha.co.jp/に変更した。（39字）」

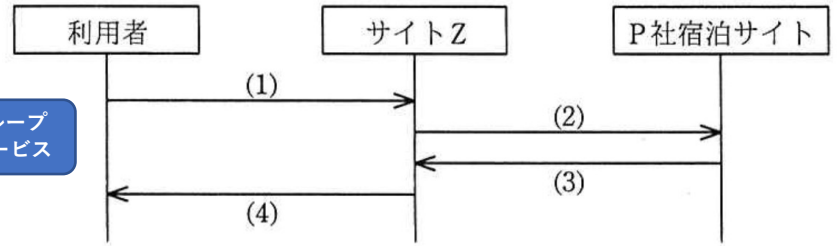
TLP：WHITE

R04春 SC午後Ⅱ問1 その⑧

JP-RISSA 情報処理安全確保支援士会

サイトZ（z.b-sha.co.jp）の，「旅行会社P社の宿泊サイト」との連携機能

B社がやってるグループウェア的なWebサービス



④ウソの駅名でエラーを促してみる

「V氏」は診断する人

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。

リダイレクト先を示すHTTPのヘッダ

⑤注意！ 空欄kには，SSRFを招く不適切な言葉を入れて下さい。

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

この6バイトで“東京”の2字

①ここの文字列（サイトZのホスト）を…

②ここに代入…というか流用，てゆうかバカコピペ

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

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。

R04春SC午後 II 問1設問5（1），設問5（2）

【Q1】表4中の［　k　］に入れる適切な字句を，15字以内で答えよ。

【A1】「V氏が用意したサイト（10字）」

【Q2】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。

【A2】「returnURLの値を固定値にする。（19字）」

③言葉は丁寧でも意味はバカコピペ

「設問5（2）は，正答率が低かった。脆弱性対策のために必要な実装は，システムによって異なる場合がある。システムごとに最適な方法を検討できるようにしておいてほしい。」（『採点講評』より）

TLP：WHITE

R04春 SC午後Ⅱ問1 その⑨

JP-RISSA 情報処理安全確保支援士会

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で，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。

【発見できない】ソートコードレビュー①

【発見できない】ソートコードレビュー②

【発見できない】ツールによる脆弱性診断

【発見できる】専門技術者による脆弱性診断

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

「・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。」

「・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。」

R04春SC午後Ⅱ問1設問6（1）

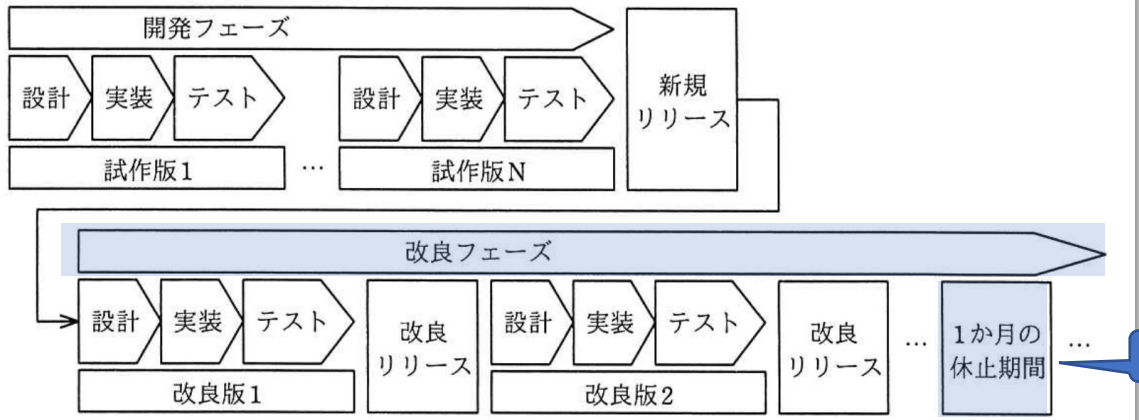
【Q】本文中の下線⑤について，該当する脆弱性を二つ挙げ，それぞれ15字以内で答えよ。

【A】【順不同】「一部のセッション管理の脆弱性（14字）」「認可・アクセス制御の脆弱性（13字）」

「設問6（1）は，正答率が低かった。脆弱性の種類によって，検出に有効な手段が異なる。それぞれの脆弱性について，どのような検出手段が有効かを理解しておいてほしい。」（『採点講評』より）

TLP：WHITE

R04春 SC午後Ⅱ問1 その⑩



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

半年に1回

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が，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。

表1より，「専門技術者による脆弱性診断」は，約10日間。

（2週間周期×およそ20回）→ 年に1～2回，大規模な改修あり

R04春SC午後Ⅱ問1設問6（2），設問6（3）

【Q1】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。

【A1】「改良フェーズにおける1か月の休止期間（18字）」

【Q2】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。

【A2】【内一つ】「専門技術者による脆弱性診断が必要なときは，改良リリースを次回に持ち越す。（36字）」「半年に一度，改良リリースの期間を長くする。（21字）」「定期的に，期間の長い改良リリースを設ける。（21字）」

TLP：WHITE

R04春 SC午後Ⅱ問1 その⑪

JP-RISSA 情報処理安全確保支援士会

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。

R04春SC午後Ⅱ問1設問6（4）

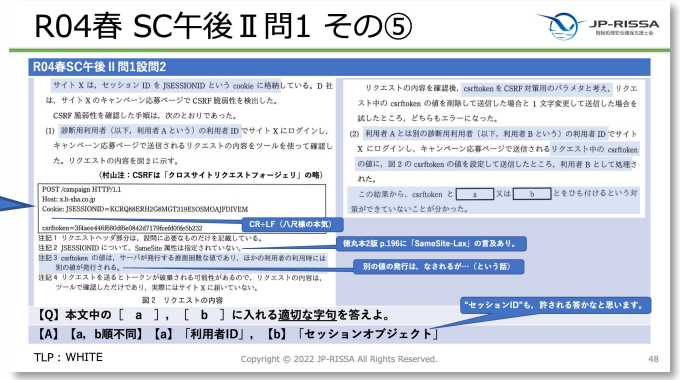
【Q】本文中の下線⑧について，CSRF（注：クロスサイトリクエストフォージェリ）脆弱性の場合では，どのような処理を行う機能が考えられるか。その処理を，55字以内で具体的に述べよ。

【A】「CSRF対策用トークンの発行，HTMLへの埋め込み，必要なひも付け，及びこれを検証する処理（45字）」

こんな表現どっから出てくるん？
どうやったら解けるのん？

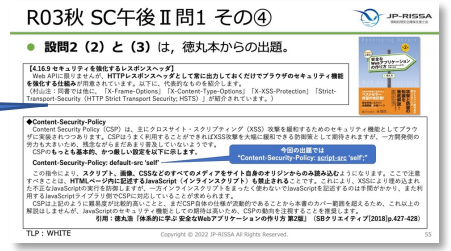
「設問6（4）は，正答率が低かった。ソフトウェア開発に使われているフレームワークにどのような脆弱性対策が組み込まれているかを知っておいてほしい。」（『採点講評』より）

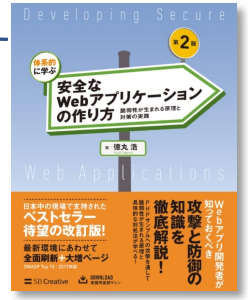
【解法 その①】
「設問2」関連の記述を要約



【解法 その②】
徳丸本を覚える

半年前も徳丸本でた





◆ 秘密情報（トークン）の埋め込み

「CSRF攻撃への対策が必要なページ（登録画面、注文確定画面など）に対して、第三者が知り得ない秘密情報を要求するようにすれば、不正なリクエストを送信させられても、アプリケーション側で判別することができます。このような目的で使用される秘密情報のことを、トークン（*token*）と呼びます。

最近はアプリケーションフレームワーク側でトークンの生成とチェックの機能を持つものが増えてきました。CSRF防御に対応したフレームワークを使用する場合は、その機能を有効化することで対策が可能です。」

引用：徳丸浩『体系的に学ぶ 安全なWebアプリケーションの作り方 第2版』（SBクリエイティブ[2018]p.192）

午後Ⅱ 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。

「**問2**では，クラウドサービスへの移行を題材に，**各種認証の仕組み，認証に関するセキュリティ対策について**出題した。全体として**正答率は平均的**であった。」
（『採点講評』より）

ネットワーク技術と，Kerberos，SAML，OAuth2.0，OpenID Connectのシーケンスを問う（作問者にとって楽な）出題

- 出題趣旨（『解答例』より）
  - 昨今，クラウドサービスが積極的に活用されるようになってきており，クラウドサービスへの移行が増加している。クラウドサービスへの移行では，情報セキュリティについて，オンプレミスのシステムとは異なる知識と技術，運用の知見が求められる。
  - 本問では，クラウドサービスへの移行を題材として，各種認証の仕組み，認証に関するセキュリティ対策などの知識及び技術力を問う。

“書かせる” 出題が明らかに少ない

JP-RISSA 情報処理安全確保支援士会

設問			解答例・解答の要点	備考
設問 1	(1)	a	<	
		b	>	
	(2)	c	エ	
設問 2	(1)	http://又は https://で始まる URL だけを出力するようにする。		
	(2)	URL と同じオリジンであるスクリプトファイル		
	(3)	スクリプト	HTML ファイル中に記載されたスクリプト	
		呼出し方法	スクリプトを別ファイルとして同一オリジンに保存して，HTML ファイルから呼び出す。	
設問 3	(1)	d	ウ	
		e	ア	
	(2)	ファイルを U 社が管理する鍵で暗号化してからアップロードする。		
設問 4	(1)	f	同一利用者 ID でのログイン失敗	
	(2)	アクセス元 IP アドレスを変えながら，不正アクセスを続けた場合		
設問 5	(1)	g	メッセージを K サービスとの間で中継	
	(2)	h	生体認証	
		i	K サービス	
		j	アカウントを削除	
		k	アカウントを無効に	
	(3)	G サービスへのアクセスを，ファイル受渡し用 PC からのアクセスだけに限定できるから		

設問			解答例・解答の要点	備考
設問 1	(1)	a	ア	
		b	イ	
		c	イ	
		d	ウ	
	(2)	e	CRYPTREC	
設問 2	(1)	エ		
	(2)	B サービスのアクセス制限機能によって通信が拒否されたから		
設問 3	(1)	マルウェア内に FQDN で指定した C&C サーバの IP アドレスの変更		
	(2)	C&C サーバとの通信時に DNS への問合せを実行しない場合があるから		
	(3)	f	イベントログの消去を示すログ	
	(4)	横展開機能と待機機能だけを実行していた場合		
	(5)	UTM の IDS 機能によって攻撃が検知でき，システム管理者に連絡がされるから		
設問 4	(1)	g	7 月 14 日	
	(2)	h	IP リストに登録された IP アドレス	
	(3)	連携端末以外の IP アドレスを送信元とする通信記録		
	(4)	連携端末を一時的にネットワークから切り離した対応		

【参考】R03秋SC午後 II 問1，問2

設問			解答例・解答の要点	備考
設問 1	(1)	ア		
	(2)	・ダウンロードするライブラリに既知の脆弱性がないかを確認する。 ・特定の Web サイトからの入手をルール化し，明文化する。		
設問 2		a	利用者 ID	順不同
		b	セッションオブジェクト	
設問 3	(1)	c	イ	
		d	ア	
		e	ア	
		f	ア	
		g	イ	
		h	イ	
	(2)	i	エ	
		j	イ	
設問 4		topic の値を https://db-y.b-sha.co.jp/に変更した。		
設問 5	(1)	k	V 氏が用意したサイト	
	(2)	returnURL の値を固定値にする。		
設問 6	(1)	①	・一部のセッション管理の脆弱性	
		②	・認可・アクセス制御の脆弱性	
	(2)	改良フェーズにおける 1 か月の休止期間		
	(3)	・専門技術者による脆弱性診断が必要なときは，改良リリースを次回に持ち越す。 ・半年に一度，改良リリースの期間を長くする。 ・定期的に，期間の長い改良リリースを設ける。		
	(4)	CSRF 対策用トークンの発行，HTML への埋め込み，必要なひも付け，及びこれを検証する処理		

R04春SC午後 II 問1
（設問6（3）は実質，1行）

R04春SC午後 II 問2
（「述べよ」の量は午後 I 並み）

このあたりは記号ばっかり
（プロトコルのシーケンスの知識問題など）

設問			解答例・解答の要点	備考
設問 1	(1)	a	キャッシュ	
	(2)	b	DDoS	
	(3)	c	Host	
	(4)	Y-CDN-U-FQDN を名前解決した IP アドレスと同じ IP アドレスをもつ Web サイト		
	(5)	d	TLS の接続先サーバ名	
設問 2	(1)	ST は認証サーバに送られないから		
	(2)	総当たり攻撃はオフラインで行われ，ログインに失敗しないから		
設問 3	(1)	e	ウ	
	(2)	f	ア	
	(3)	g	偽造	
	(4)	h	1	
		i	3	順不同
		j	4	
設問 4	(1)	k	ウ	
		l	イ	
		m	ア	
	(2)	n	エ	
	(3)	o	(2)	
		p	(6)	
	(4)	q	ウ	
設問 5	(1)	r	オ	
		s	エ	
		t	ウ	
	(2)	u	(8)	
	(3)	v	イ	
	(4)	w	認証要求	
		x	ID トークン	

TLP：WHITE

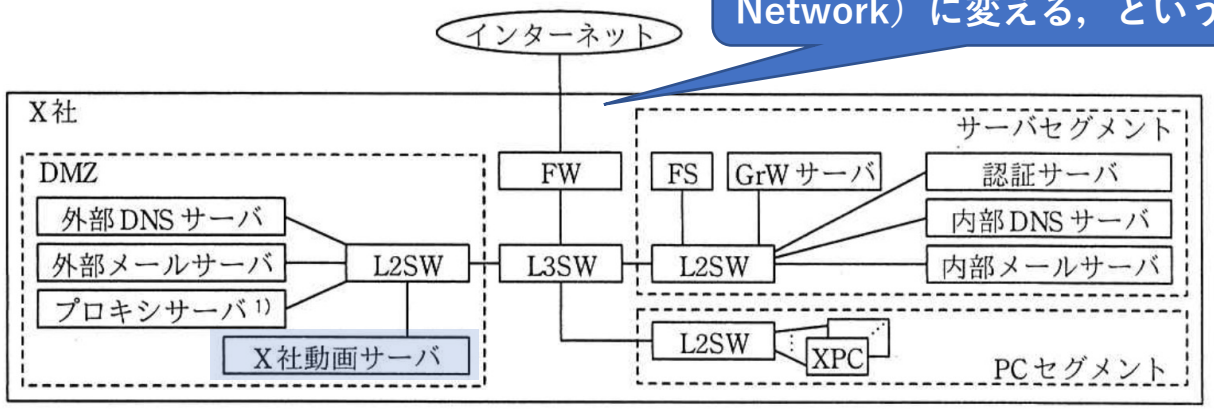
R04春 SC午後Ⅱ問2 その①

JP-RISSA 情報処理安全確保支援士会

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

X社…🤔どんな動画だ

これをCDN（Content Delivery Network）に変える，という話。



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

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さん：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

“代理応答”はバツ。だが，AWSのCDN “Amazon CloudFront” では “Edge” と呼び，Akamaiの資料にも “エッジ” とある…🤔🤔

単に “DoS” と書くと，直前にF氏が言った「多くの動画配信が代理応答されるので，」という仕組みとの整合がとれない。

R04春SC午後Ⅱ問2設問1（1），設問1（2）

【Q1】本文中の［　a　］に入れる適切な字句を，5字以内で答えよ。

【A1】「キャッシュ（5字）」

【Q2】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。

【A2】「DDoS（4字）」

TLP：WHITE

R04春 SC午後Ⅱ問2 その②

F氏：支援士

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。

X社が

…から，X社…

(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。

あだ名を付けられるやつ

(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）

午後Ⅱ問1（図2，図5，図6）に「Host:」と書いてある…！

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

Cさん：システム部の担当者

理解はや

設問1（5）の答

レイヤ間で食い違わせることによる攻撃，が設問1（5）

レイヤが違うTLSとHTTP，それぞれが「X-FQDN」を扱う。
（TLSはSNI（Server Name Indication），HTTPはHost）

…は，X社からH…

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

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。

すごいよCさん

R04春SC午後Ⅱ問2設問1（3），設問1（5）

【Q1】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。

【A1】「Host（4字）」

【Q2】本文中の［　d　］に入れる適切な字句を，20字以内で答えよ。

【A2】「TLSの接続先サーバ名（11字）」

「設問1（3）及び（5）は，正答率が低かった。HTTPとTLSに関する問題であったが，DNSと混同していると思われる解答が多かった。CDNを悪用したドメインフロンティング攻撃は，標的型攻撃などでもよく登場する攻撃手法なので，是非知っておいてほしい。」（『採点講評』より）

TLP：WHITE

R04春 SC午後Ⅱ問2 その③

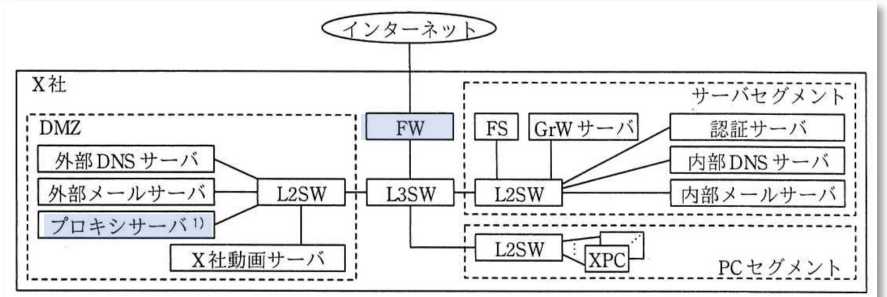


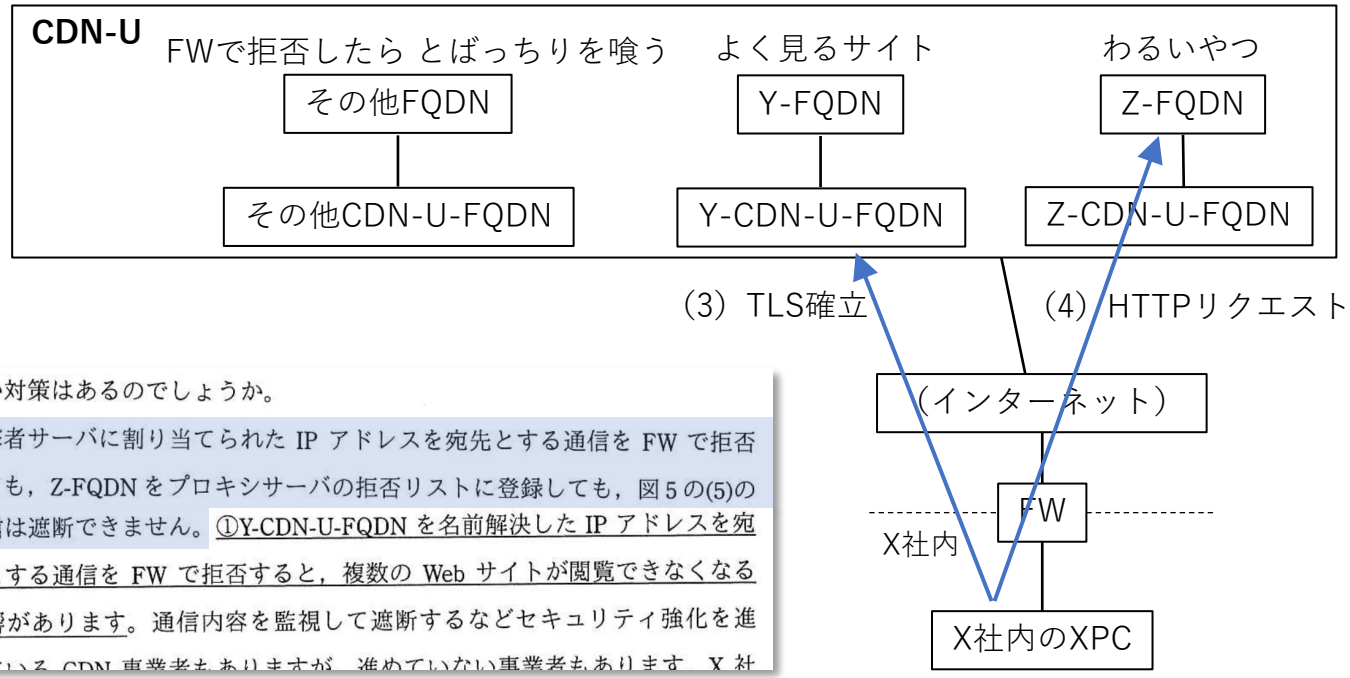
図1 X社のシステム構成

ここを見落とすと地獄

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。
…は，X社内からH…
空欄c「Host」
(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

R04春SC午後Ⅱ 問2設問1（4）

【Q】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。

【A】「Y-CDN-U-FQDNを名前解決したIPアドレスと同じIPアドレスをもつWebサイト（43字）」

TLP：WHITE

Kerberos認証ネタはNW試験と共用

JP-RISSA 情報処理安全確保支援士会

〔ケルベロス認証の概要と通信手順〕

X主任が調査して理解した，ケルベロス認証の概要と通信手順を次に示す。

・ケルベロス認証では，共通鍵暗号による認証及びデータの暗号化を行っている。

・PCとサーバの鍵の管理及びチケットの発行を行う鍵配布センタ（以下，KDCという）が，DSから取得したアカウント情報を基にPC又はサーバの認証を行う。

・KDCが管理するドメインに所属するPCとサーバの鍵は，事前に生成してPC又はサーバに登録するとともに，全てのPCとサーバの鍵をKDCにも登録しておく。

・チケットには，PCの利用者の身分証明書に相当するチケット（以下，TGTという）と，PCの利用者がサーバでの認証を受けるためのチケット（以下，STという）の2種類があり，これらのチケットを利用してSSOが実現できる。

・PCの電源投入後に，利用者がID，パスワード（以下，PWという）を入力してKDCでケルベロス認証を受けると，HTTP over TLSでアクセスする業務サーバや営業支援サーバにも，ケルベロス認証向けのAPIを利用すればSSOが実現できる。

・KDCは，導入予定のDSで稼働する。

【TGT（ticket-granting ticket）】
・「PCの利用者の身分証明書に相当するチケット」
【ST（service ticket）】
・「PCの利用者がサーバでの認証を受けるためのチケット」

X主任は，内部LANにDSを導入したときの，SSOの動作をまとめた。PCの起動から営業支援サーバアクセスまでの通信手順を図2に示す。

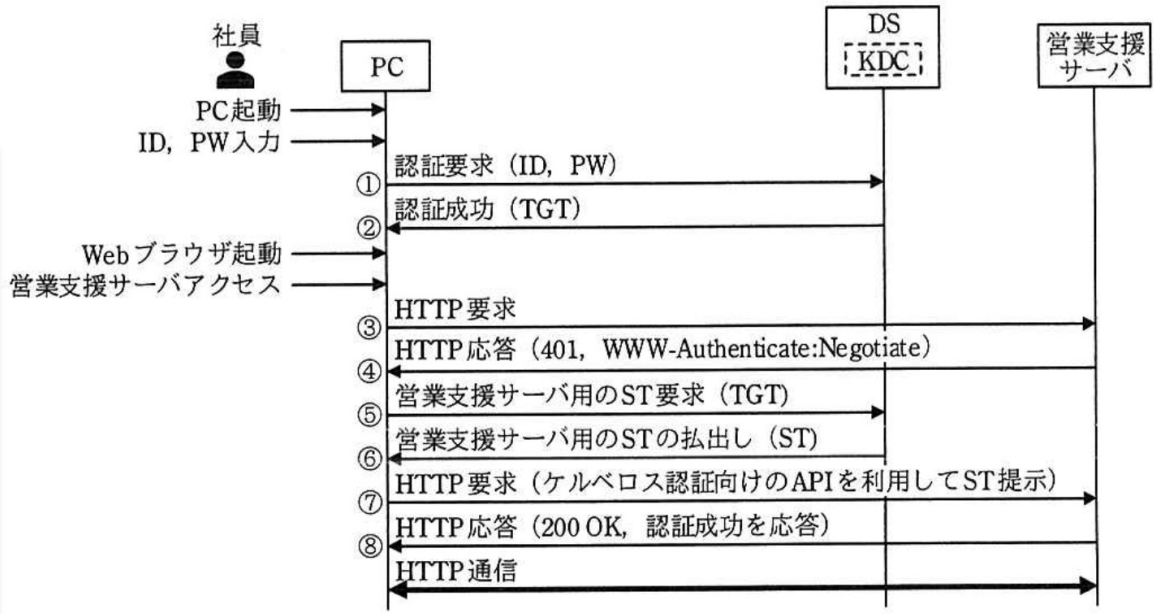


図2　PCの起動から営業支援サーバアクセスまでの通信手順（抜粋）

① PCは，DSで稼働するKDCにID，PWを提示して，認証を要求する。

② KDCは，ID，PWが正しい場合にTGTを発行し，PCの鍵で暗号化したTGTをPCに払い出す。PCは，TGTを保管する。

③ 省略

④ 省略

⑤ PCは，KDCにTGTを提示して，営業支援サーバのアクセスに必要なSTの発行を要求する。

⑥ KDCは，TGTを基に，PCの身元情報，セッション鍵などが含まれたSTを発行し，営業支援サーバの鍵でSTを暗号化する。さらに，KDCは，暗号化したSTにセッション鍵などを付加し，全体をPCの鍵で暗号化した情報をPCに払い出す。セッション鍵は，通信相手の正当性の検証などに利用される。

⑦ PCは，全体が暗号化された情報の中からSTを取り出し，ケルベロス認証向けのAPIを利用して，STを営業支援サーバに提示する。

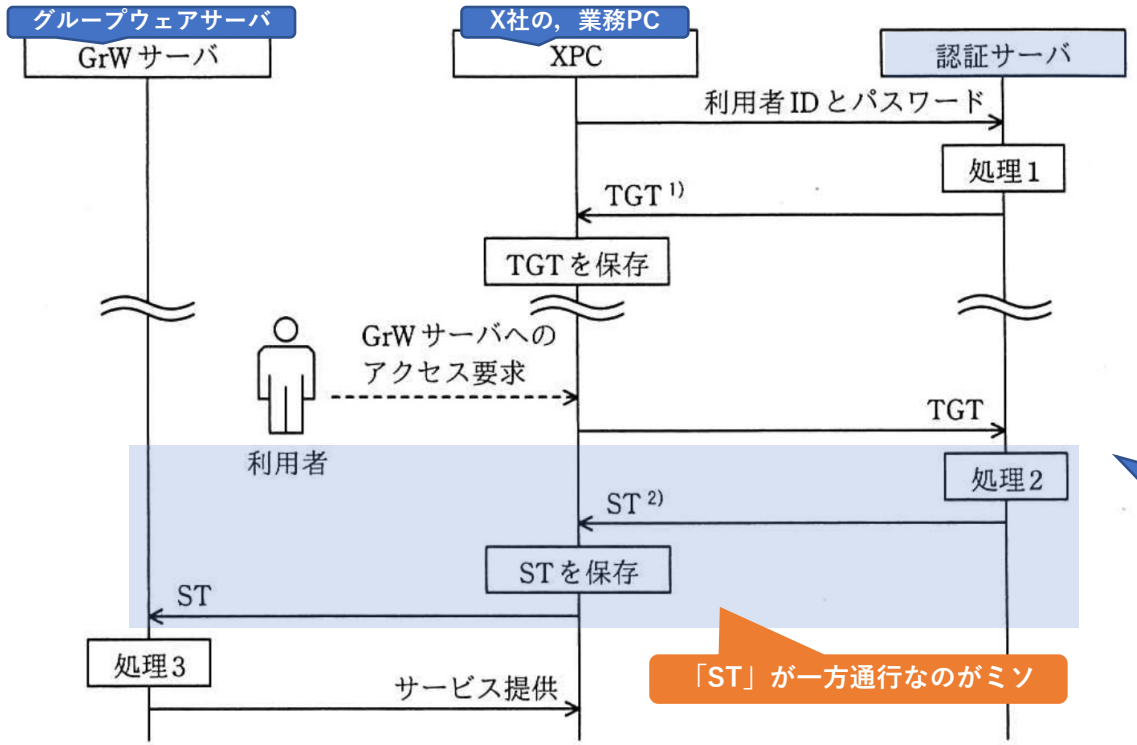
⑧ 営業支援サーバは，STの内容を基にPCを認証するとともに，アクセス権限をPCに付与して，HTTP応答を行う。

※こっちの方が読みやすい
R04春NW
午後Ⅰ問3より

TLP：WHITE

R04春 SC午後Ⅱ問2 その④

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。

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。

…と，アクセス対象のサ…

【TGT（ticket-granting ticket）】
・「PCの利用者の身分証明書に相当するチケット」
【ST（service ticket）】
・「PCの利用者がサーバでの認証を受けるためのチケット」

R04春SC午後Ⅱ 問2設問2（1）

【Q】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。

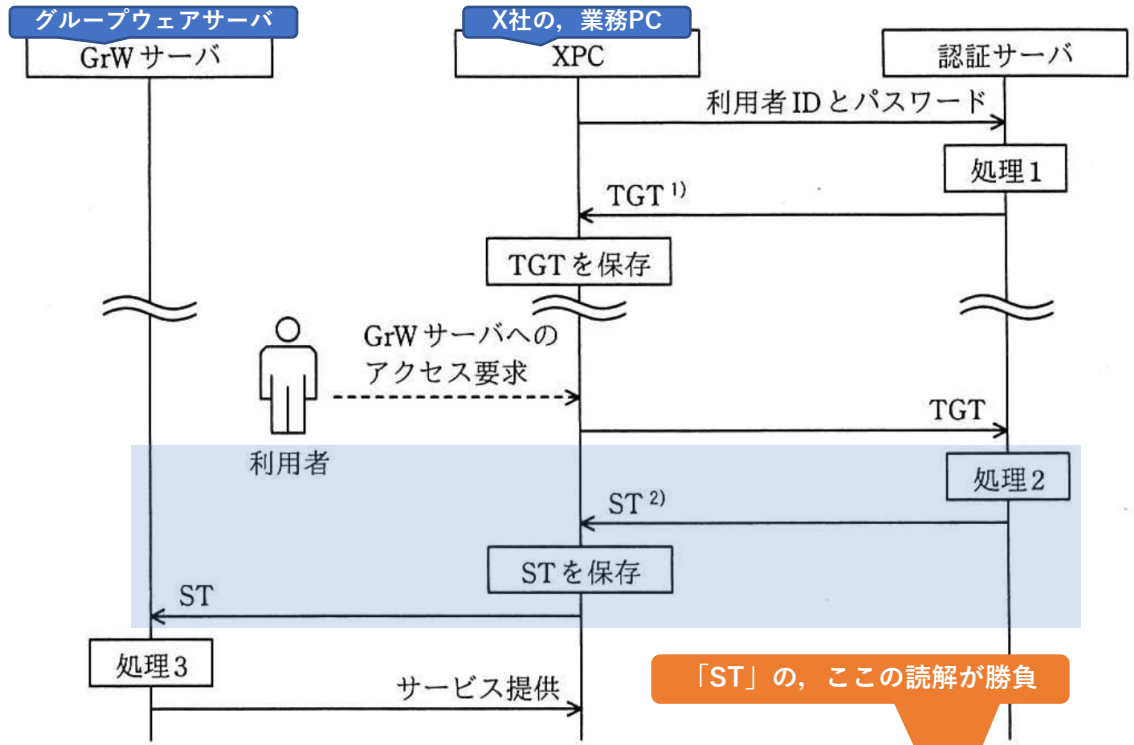
【A】「STは認証サーバに送られないから（16字）」

“認証サーバではSTの偽造を検知しないから”と答えると，これは，下線②の単なる書き直しだと判断されでバツ。

TLP：WHITE

R04春 SC午後Ⅱ問2 その⑤

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

「ST」の，ここの読解が勝負

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。

すごいよCさん

下線③は，よくある“ブルートフォース攻撃”対策。
サーバ側でこの攻撃を検知できるには，下記などの前提も必要。
・サーバ側が「ログイン」の試行を把握できている。
・サーバ側が「連続失敗」の回数を数えている。

R04春SC午後Ⅱ 問2設問2（2）

【Q】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。

【A】「総当たり攻撃はオフラインで行われ，ログインに失敗しないから（29字）」

“攻撃者がローカルで解析する行為は，サーバ側では把握できない。”を含意

「設問2（2）は，正答率が平均的であった。オフラインにおける総当たり攻撃の問題であったが，パスワードスプレー攻撃などパスワードに対するオンラインの攻撃手法に言及した解答も散見された。パスワードに対する攻撃手法の種類や違いについて，理解を深めてほしい。」（『採点講評』より）

TLP：WHITE

設問3ではSAMLが登場（5年ぶり）

JP-RISSA 情報処理安全確保支援士会

〔SAML を用いた認証連携と接続元制限方式の概要〕

SAML は，認証，認可などの情報を安全に交換するためのフレームワークである。SAML を用いることによって，利用者にサービスを提供するサービスプロバイダ（以下，SP という）と，ID プロバイダ（以下，IdP という）との間で利用者の認証結果などの情報を安全に連携することができる。SAML には複数の処理方式が存在する。今回 F 社で導入を検討している方式のシーケンスを図 1 に示す。図 1 中の各通信のプロトコルは，IdP と LDAP サーバ間は LDAP であり，それ以外は HTTP over TLS である。

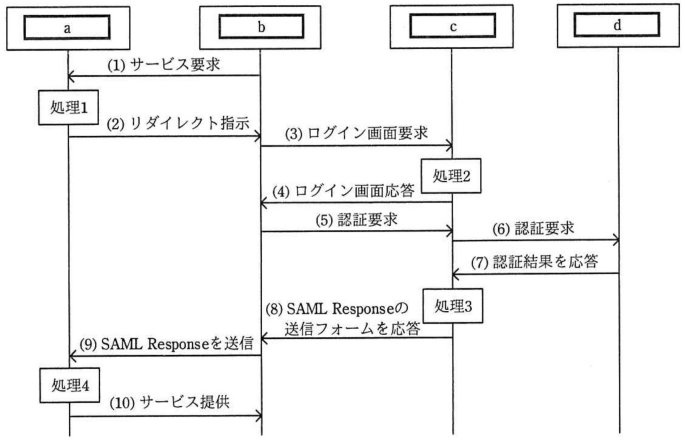


図 1　導入を検討している方式のシーケンス

SAML を用いた認証連携を行うためには，事前に IdP と SP との間で様々な情報を共有することによって，信頼関係を構築しておく必要がある。事前に共有する情報としては，通信の方式や連携する属性情報などが記述されたメタデータ，［ e ］で生成して送出する URL，［ f ］において必要な IdP のディジタル証明書などがある。

図 1 中の処理 1～4 の処理内容を表 1 に示す。

表 1　処理内容

処理番号	処理内容
処理 1	・IdP に認証を要求する SAML Request を生成する。 ・SAML Request をエンコードする。 ・エンコード結果を IdP のログイン画面の URL と組み合わせて，リダイレクト先 URL を生成する。
処理 2	・URL 内の［ g ］から SAML Request を取得する。 ・信頼関係が構築された SP からの認証要求であることを検証する。
処理 3	・利用者の認証が成功した場合，認証結果や SP との間で連携する属性情報，有効期間，それらの情報に対するディジタル署名を含めた SAML Response を生成する。
処理 4	・SAML Response に含まれるディジタル署名を検証することによって，ディジタル署名が［ h ］によって署名されたものであること，及びデータの［ i ］がないことを確認する。 ・SAML Response 内の属性情報も検証することによって，サービスを提供すべきか決定する。

C 主任は図 1 のシーケンスから，②IdP を社内ネットワークに設置しても認証情報の連携が成立することを確認した。そこで，IdP は社内ネットワークに設置し，IdP のログイン画面の URL の FQDN には，社内の FQDN を割り当てることにした。

H29春SC午後Ⅰ問3でのレベル感は，こんな感じ。

設問 2　〔SAML を用いた認証連携と接続元制限方式の概要〕について，(1)～(5)に答えよ。

(1)　図 1 中の［ a ］～［ 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　IdP　　イ　LDAP サーバ

ウ　SP　　エ　利用者端末の Web ブラウザ

(2)　本文中の［ e ］，［ f ］に入れる適切な処理番号を，表 1 中の処理 1～4 の中から選び，答えよ。

(3)　表 1 中の［ g ］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　スキーム　　オ　リファラ

(4)　表 1 中の［ h ］，［ i ］に入れる適切な字句を，それぞれ 5 字以内で答えよ。

(5)　本文中の下線②について，SP と IdP が直接通信できないにもかかわらず，認証情報の連携が成立するのはなぜか。その理由を，35 字以内で述べよ。

設問 2	(1)	a	ウ	
		b	エ	
		c	ア	
		d	イ	
	(2)	e	処理 1	
		f	処理 4	
	(3)	g	ウ	
	(4)	h	IdP	
		i	改ざん	
	(5)	認証に関する情報を利用者端末の Web ブラウザが中継するから		

TLP：WHITE

R04春 SC午後Ⅱ問2 その⑥

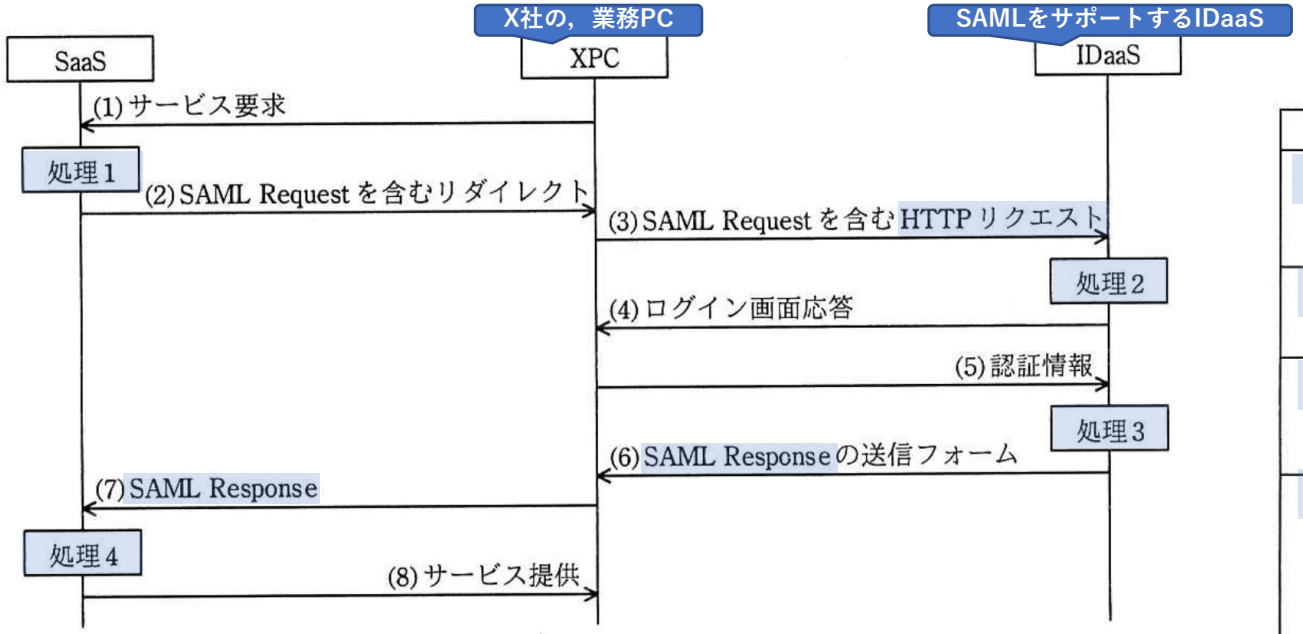


図 8　SAML 認証の流れ

「URLを生成」なので，POSTではなく，GETで（URLに含めて）伝える。
（POSTメソッドで行う方式もある，らしい。）

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。

…，SaaSが検…
…を，IDaaSが生…

R04春SC午後 II 問2設問3（1），設問3（2），設問3（3）

【Q1】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。　ア cookie　イ HTML　ウ クエリ文字列　エ ボディ　オ リファラ

【A1】「ウ」

【Q2】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。　ア IDaaS　イ SaaS　ウ XPC

【A2】「ア」

【Q3】表2中の［ g ］に入れる適切な字句を，5字以内で答えよ。

【A3】「偽造（2字）」

空欄g，IPA解答例に“改ざん”は含まれず。
∵「SAMLアサーション」は「処理3」で（初めて）生成されるものなので，たとえそれがウソの値で生成されたとしても，“改ざん”されてはいない値だから。（多分そんな理屈。）

TLP：WHITE

R04春 SC午後Ⅱ問2 その⑦

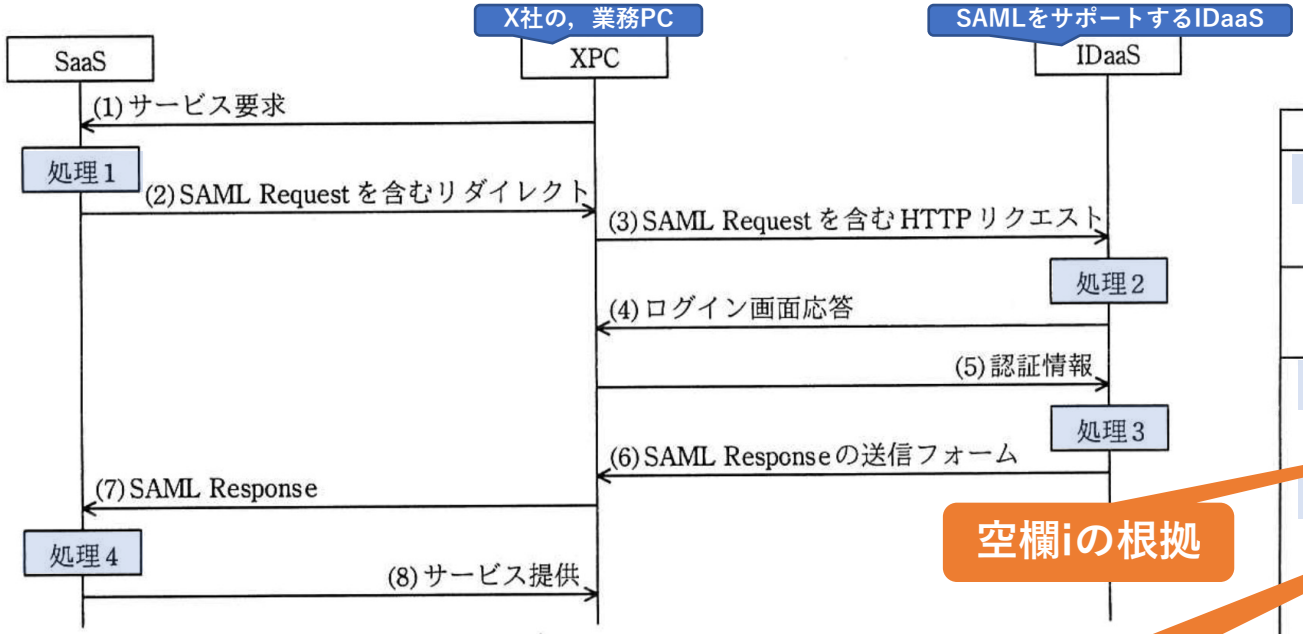


図 8　SAML 認証の流れ

空欄hの根拠

空欄iの根拠

空欄jの根拠

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。

…，SaaSが検…

…を，IDaaSが生…

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。

あっ！“ディジタル”ではなく
今期からは“デジタル”だ！

R04春SC午後 II 問2設問3（4）

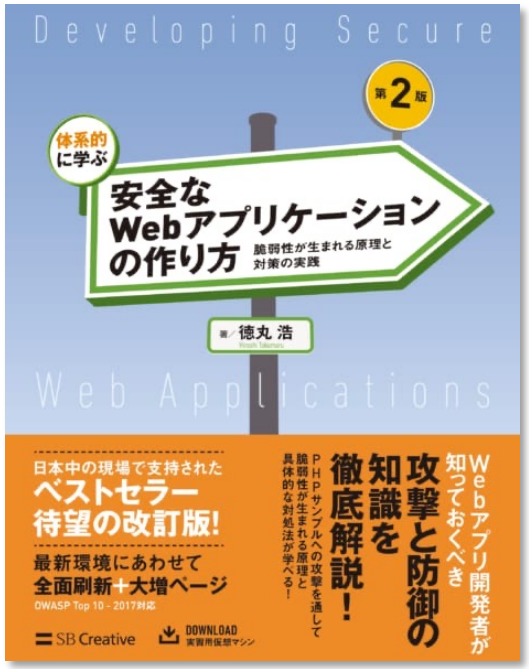
【Q】本文中の［ h ］～［ j ］に入れる適切な数字を，それぞれ答えよ。

【A】【h】「1」，【i，j順不同】【i】「3」，【j】「4」

TLP：WHITE

設問4以降　選手交代のお知らせ

JP-RISSA
情報処理安全確保支援士会



徳丸浩『体系的に学ぶ 安全なWebアプリケーションの作り方 第2版』
（SBクリエイティブ[2018]）ISBN978-4-7973-9316-3 C0055 ¥3200E

税抜，自腹

中村雄一 ほか『認証と認可 Keycloak入門　OAuth/OpenID Connectに準拠したAPI認可とシングルサインオンの実現』
（リックテレコム[2022]）ISBN978-4-86594-322-1 C3055 ¥4000E

本年の1月31日 発行
今春の作問にギリ間に合った？

税抜，自腹

TLP：WHITE

R04春 SC午後Ⅱ問2 その⑧

JP-RISSA 情報処理安全確保支援士会

れた 3 か月後に，システム部は，G社が提供するグループウェアサービス について，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。

設問4（2）のヒント

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。

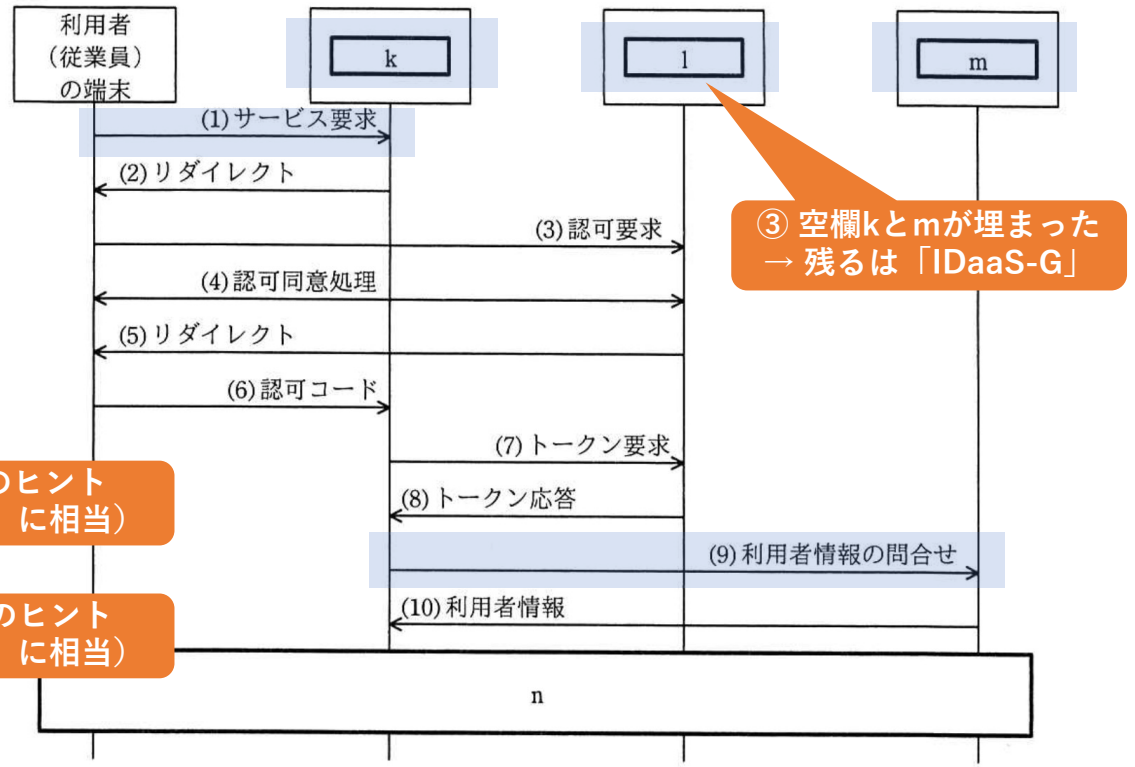
「利用者」は主催者にもなる

① 空欄kのヒント（図9の（1）に相当）

② 空欄mのヒント（図9の（9）に相当）

G社が提供するIDaaS

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。



③ 空欄kとmが埋まった → 残るは「IDaaS-G」

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

R04春SC午後Ⅱ問2設問4（1）

【Q】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。
　ア GrW-G　　イ IDaaS-G　　ウ Sサービス

【A】【k】「ウ」，【l】「イ」，【m】「ア」

TLP：WHITE

R04春 SC午後Ⅱ問2 その⑨

JP-RISSA 情報処理安全確保支援士会

か，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

G社が提供するグループウェアサービス

ヒント ①

ヒント ②

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。

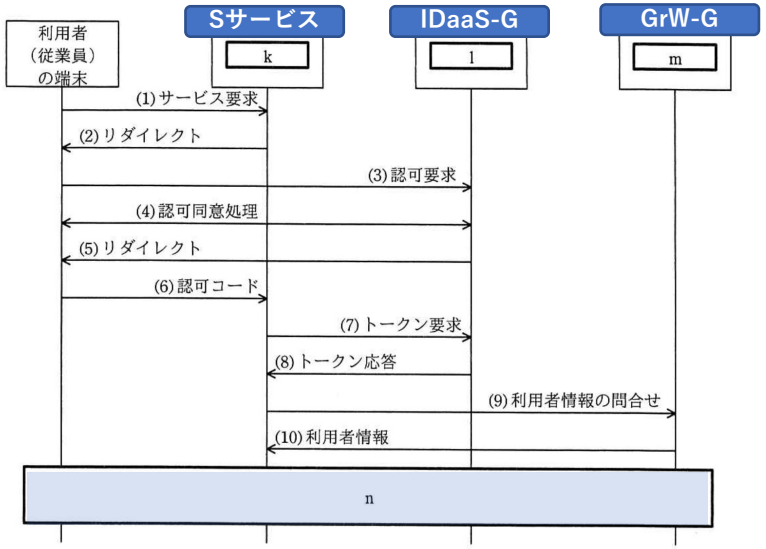
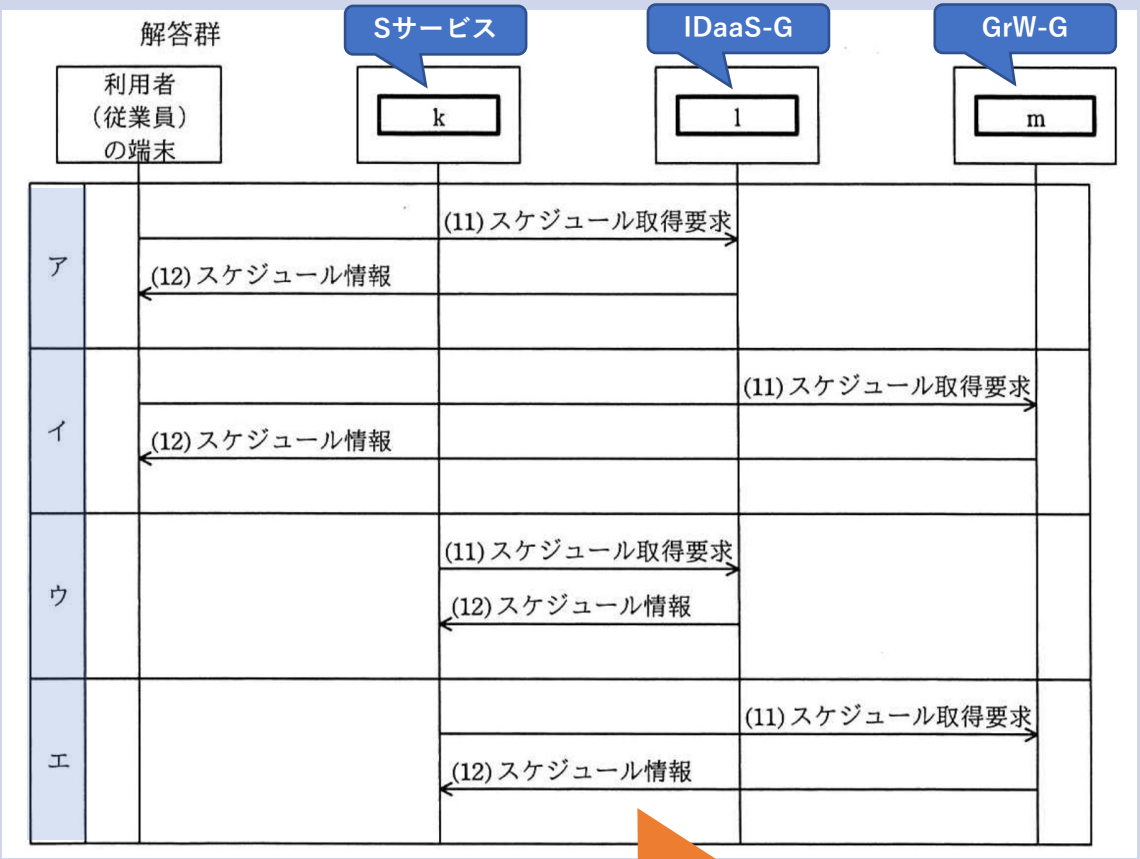


図 9　OAuth 2.0 を利用したサービス要求からスケジュール情報の取得までの流れ

R04春SC午後Ⅱ問2設問4（2）

【Q】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。



【A】「エ」

「Sサービス」と「GrW-G」両者のやり取りがあるのは…

TLP：WHITE

R04春 SC午後Ⅱ問2 その⑩

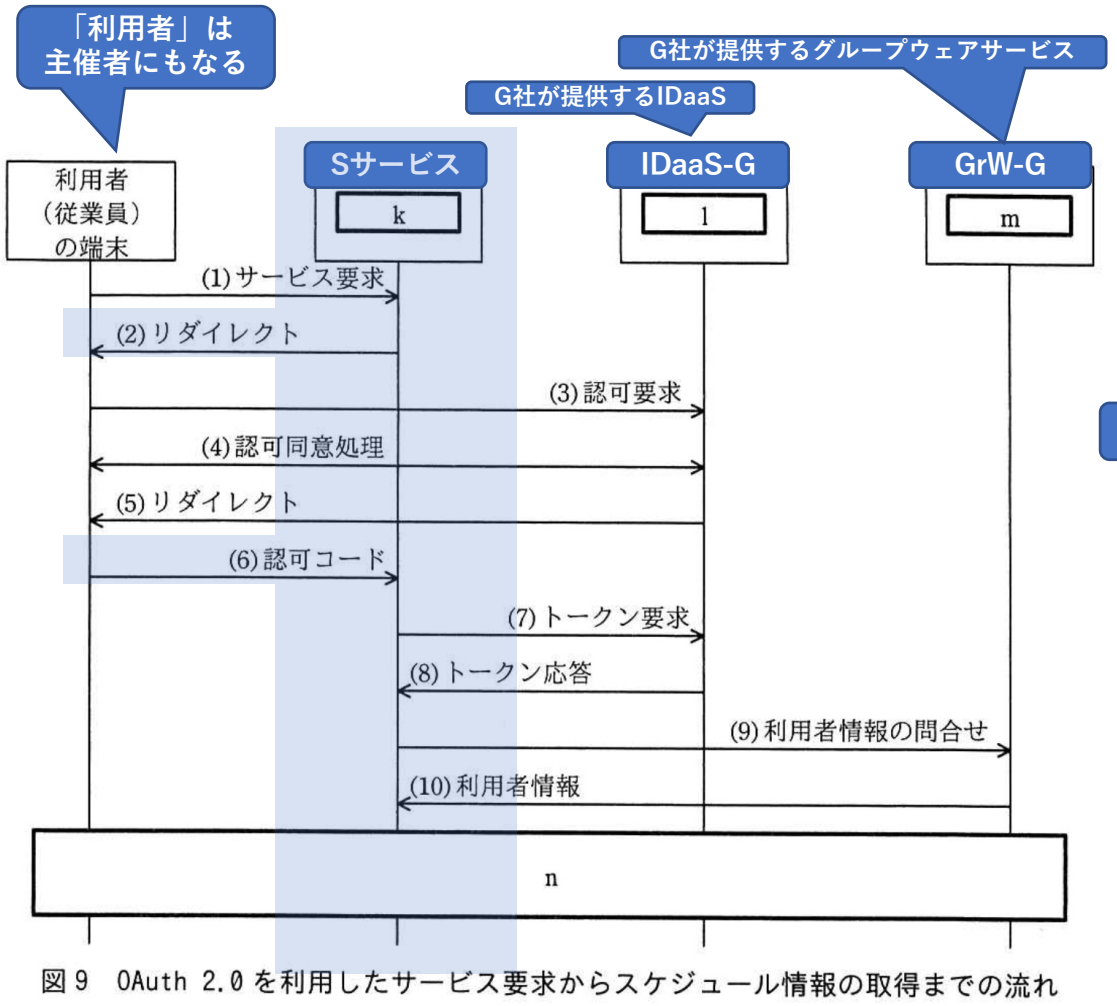


図9　OAuth 2.0を利用したサービス要求からスケジュール情報の取得までの流れ

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。

ここの意味は，“攻撃者が，「重要な秘密を扱う会議の主催者として日程を決定する」「利用者」を「標的」にする「場合」”

『認証と認可』p.185

ここの記述は『認証と認可』p.186に沿う。

認可コードに付与する

「『state』パラメータを用いた認可リクエストを実施するために、Keycloak側では特別な設定は必要なく、クライアント側で、認可リクエストにstateを付与したりチェックする実装が求められます。」
（『認証と認可』p.186より引用）

ここで言う「クライアント」は，認可サーバから見たクライアント。図9でいう，空欄k（Sサービス）のこと。

R04春SC午後Ⅱ問2設問4（3）

【Q】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。

【A】【o】「（2）」，【p】「（6）」

「設問4（3）は，正答率が低かった。OAuth 2.0のメカニズムと攻撃手法は，安全なAPIアクセスの実現のために必要な知識なのでよく理解してほしい。」（『採点講評』より）

TLP：WHITE

R04春 SC午後Ⅱ問2 その⑪

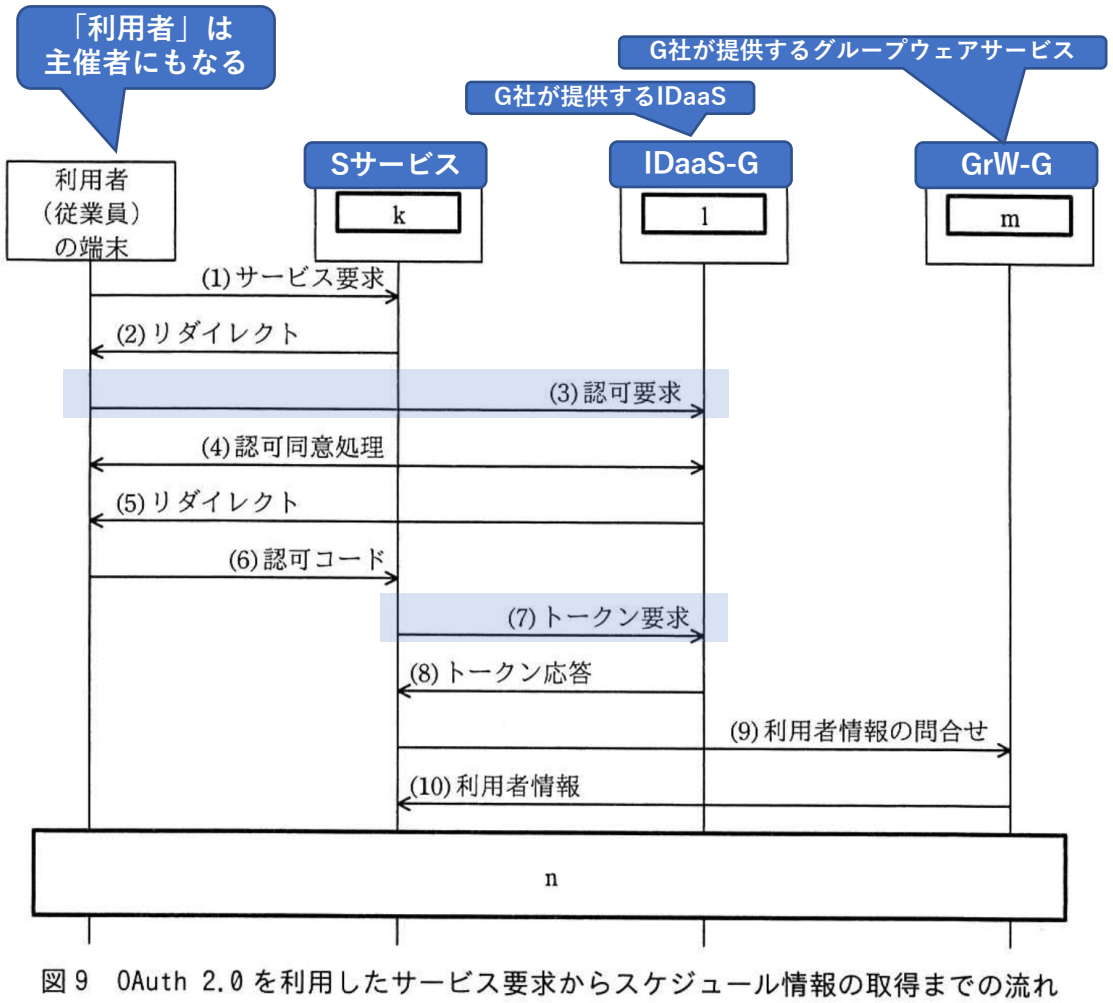


図9　OAuth 2.0を利用したサービス要求からスケジュール情報の取得までの流れ

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。

『認証と認可』p.185

『認証と認可』p.188

RFC 7636

もう勘弁して…

R04春SC午後Ⅱ問2設問4（4）

【Q】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。

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）

【A】「ウ」

設問5　OIDC（右図）について

「利用者」は
主催者にもなる

G社が提供するグループウェアサービス

G社が提供するIDaaS

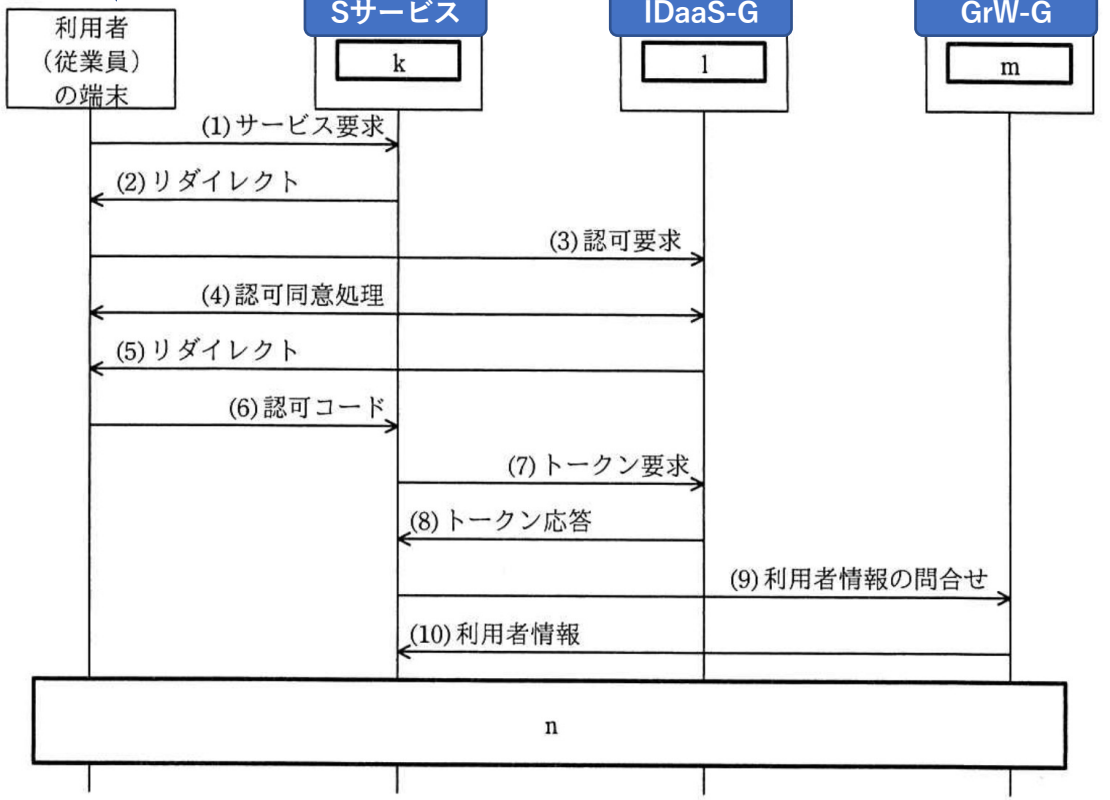


図 9　OAuth 2.0 を利用したサービス要求からスケジュール情報の取得までの流れ

「認可」とか「認証」とか。そろそろ
“ゼロトラスト”を出すための布石？

OIDC（OpenID Connect）は，OAuth 2.0を拡張したもの
∴ そのシーケンスは自ずと，左図と似たものとなる。

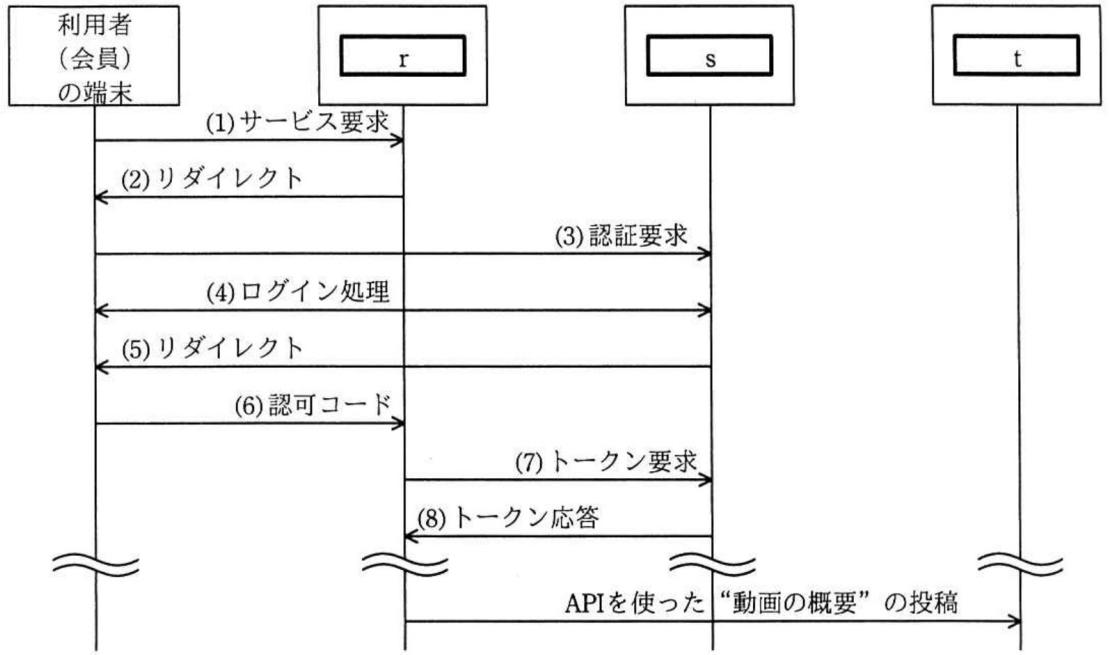


図 10　OIDC を用いた T 社投稿サイトと X 社動画サーバの連携の流れ

認可に特化したOAuth 2.0との違いとして，**OpenID Connect 1.0では，「誰（OpenIDプロバイダ）が、誰（ユーザー）を、誰（スマホアプリなど）のために認証したのか**、また、**そのユーザーの属性情報や認証した日時などの情報をAPI側が確認できる**ようになります。」
（技術評論社 Software Design誌 2020年11月号 p.34より引用）

TLP：WHITE

R04春 SC午後Ⅱ問2 その⑫

JP-RISSA 情報処理安全確保支援士会

〔企画チームからの要望〕

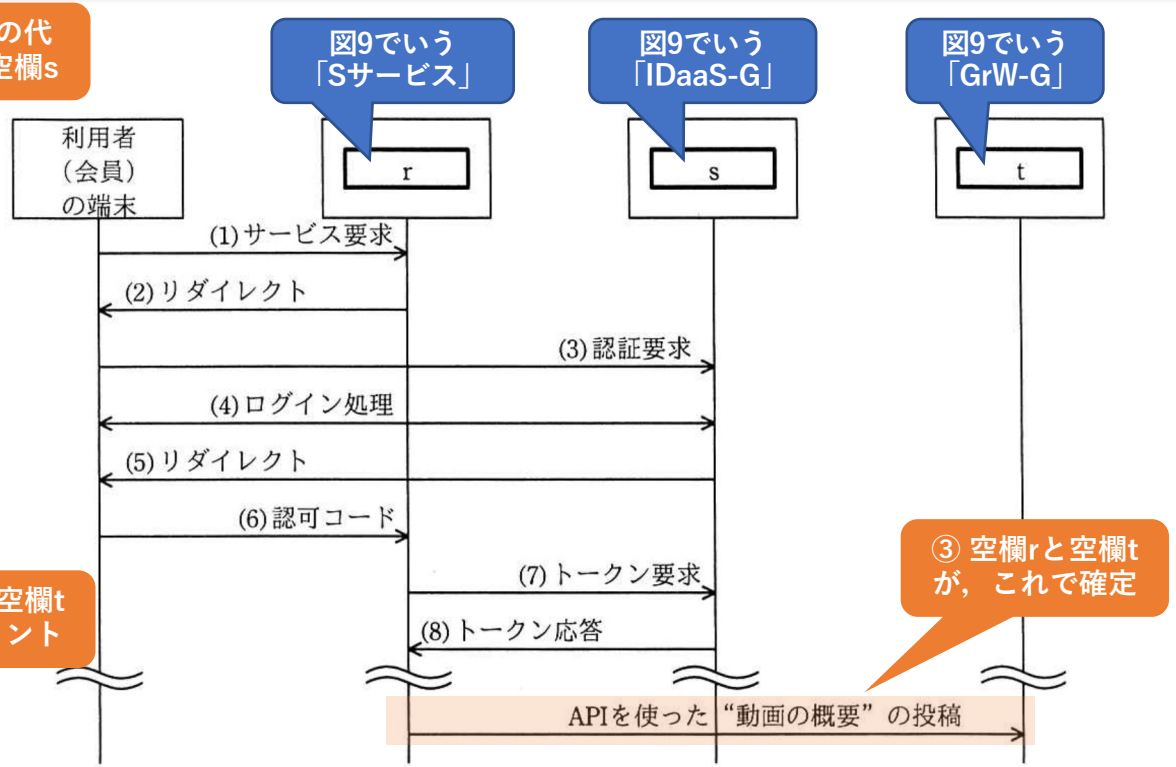
ツイッター的な？

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。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。

①「IDaaS-G」の代わりとなるる，空欄s

② 空欄rと空欄tが埋まるヒント



③ 空欄rと空欄tが，これで確定

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

参考：『認証と認可』 p.60～68

R04春SC午後 II 問2設問5（1）

【Q】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。

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

【A】【r】「オ」，【s】「エ」，【t】「ウ」

TLP：WHITE

R04春 SC午後Ⅱ問2 その⑬

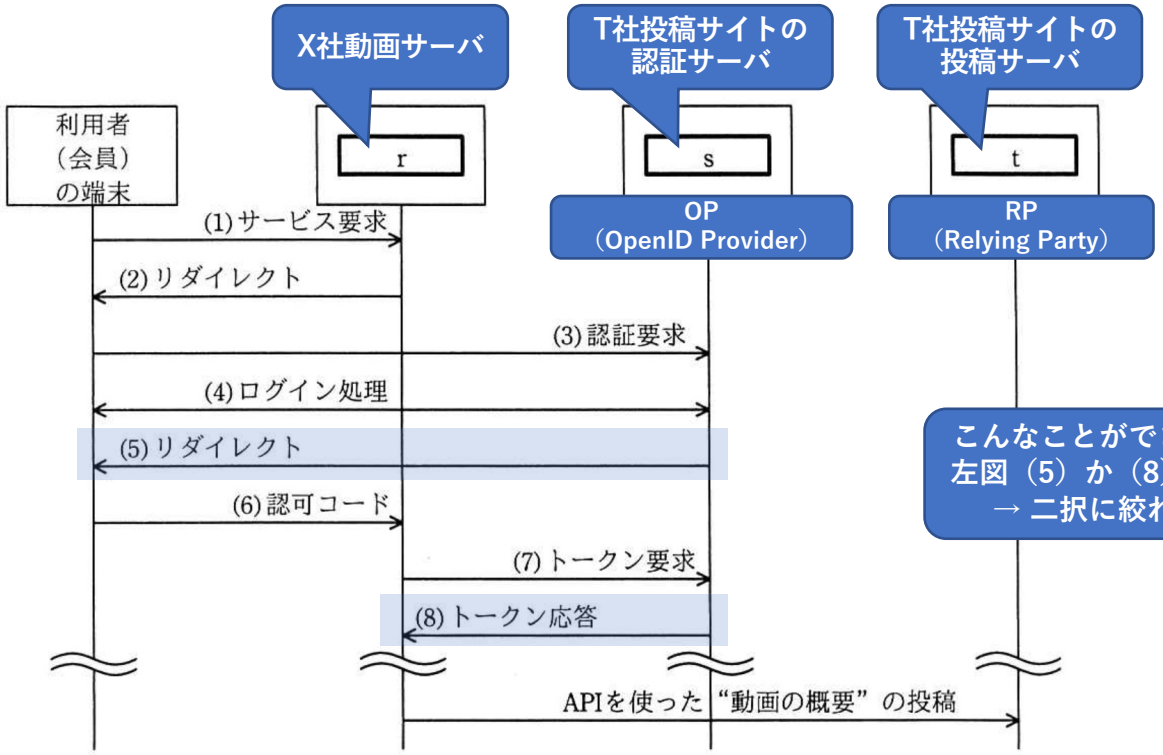


図 10　OIDC を用いた T 社投稿サイトと X 社動画サーバの連携の流れ

参考：『認証と認可』p.60～62

いきなり出てきた「認可コードフロー」。これは，OAuthの「認可コードフロー」（本問の図9）を拡張したもの，すなわち図10。OpenID Connect 1.0が定義するフローの内，下記①を指す。

① Authorization Code Flow：「認可コードと交換する形でIDトークン（とアクセストークン）を受け渡す」
② Implicit Flow：「IDトークンを受け渡す際、署名の検証が必須」
③ Hybrid Flow：「Authorization Code Flow と Implicit Flowを融合」

（技術評論社 Software Design誌 2020年11月号 p.34より引用）

こんなことができるのは左図（5）か（8）だけ。
→ 二択に絞れる。

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。

R04春SC午後 II 問2設問5（2），設問5（3）

【Q1】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。

【A1】「（8）」

【Q2】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。
ア base32　イ base64url　ウ ROT13　エ UTF-8

【A2】「イ」

参考：『認証と認可』p.46

TLP：WHITE

R04春 SC午後Ⅱ問2 その⑭

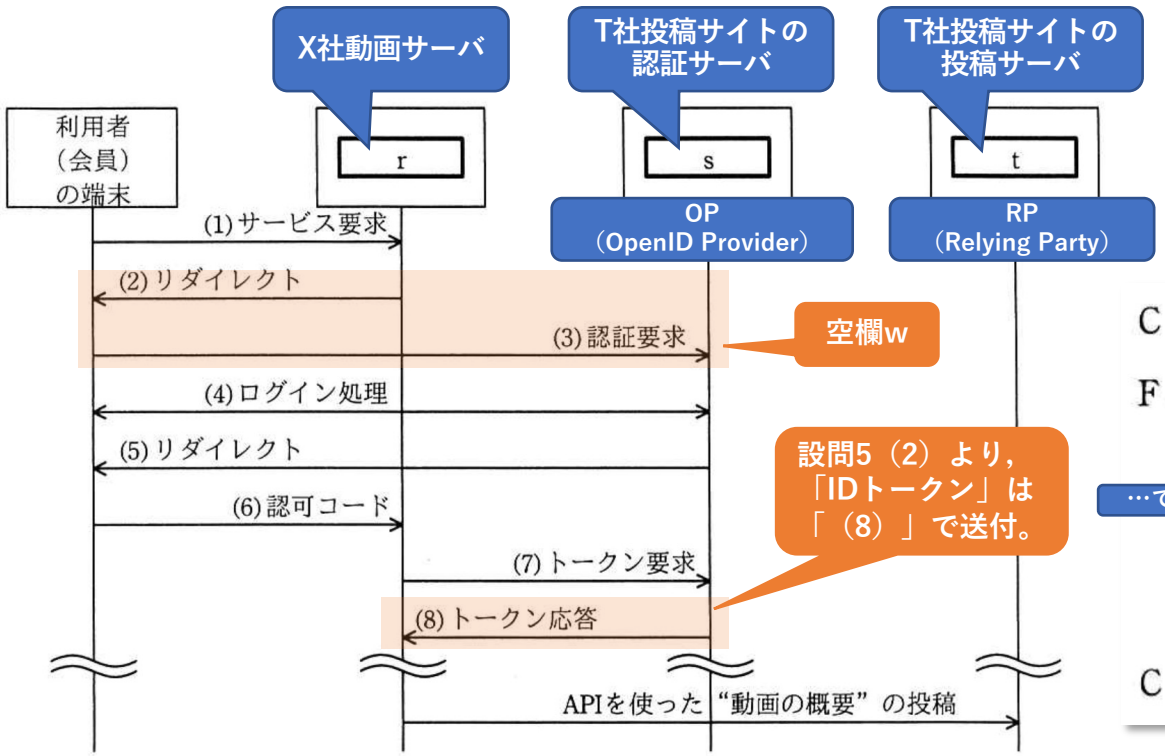


図 10　OIDC を用いた T 社投稿サイトと X 社動画サーバの連携の流れ

空欄w

設問5（2）より，「IDトークン」は「（8）」で送付。

いきなり出てきた「ハイブリッドフロー」。これは，OpenID Connect 1.0が定義するフローの内，下記③を指す。

① Authorization Code Flow：「認可コードと交換する形でIDトークン（とアクセストークン）を受け渡す」
② Implicit Flow：「IDトークンを受け渡す際、署名の検証が必須」
③ Hybrid Flow：「Authorization Code Flow と Implicit Flowを融合」

（技術評論社 Software Design誌 2020年11月号 p.34より引用）

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。

…を生成･保持する機能を「X社動画サーバが」実…

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

…を「X社動画サーバ」が生…

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

…て「T社投稿サイトの認証サーバ」に送…

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

…に，図10の「（8）」で送…　…を「X社動画サーバ」が検…

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。

もう弟子にしてください

参考：『認証と認可』p.192～193

R04春SC午後 II 問2設問5（4）

【Q】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。

【A】【w】「認証要求（4字）」，【x】「IDトークン（6字）」

「設問5（4）は，正答率が低かった。OpenID Connectのメカニズムと攻撃手法は，安全な認証基盤の実現のために必要な知識なのでよく理解してほしい。」（『採点講評』より）

“リダイレクト”ではアカンのかね…🤔

TLP：WHITE

おつかれさまでした。

対策セミナー#6　7月16日（土）19時半 ～ 21時

- 当日の概要，JP-RISSAの紹介　5分（済み）
- こう出た【概観・午前Ⅱ】　10分（済み）
- こう出た【午後Ⅰ】　30分（済み）
- 休憩　5分（済み）
- こう出た【午後Ⅱ】　35分（済み）
- 質問，クロージング　5分

TLP：WHITE

HomePage：https://www.jp-rissa.or.jp/

お問い合わせ：contact@jp-rissa.or.jp

Twitter：@jp_rissa

JP-RISSA

情報処理安全確保支援士会