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 ＃3 「こう出たR2セキスペ解答解説」

一般公開用スライド

村山直紀（むらやま･なおき）@MurayamaNaoki
JP-RISSA 理事
情報処理安全確保支援士 登録番号第000029号

2021年1月16日 19:30-21:00 於 Zoom + YouTube Live

※ 本スライドの一般公開に際して

JP-RISSA
情報処理安全確保支援士会

- 本スライドは，表題のセミナー（2021年1月16日開催）で用いたスライドを，同年4月の一般公開にあたり，再編集したものです。
- 本スライドの記載内容は開催当時のものです。最新の情報ではない点，ご留意・ご了承ください。
- 本スライドには，表題のセミナーの開催時には刊行前であった，セミナー担当者（村山直紀）が著作権を有する書籍の記載内容を含みます。本スライドの記載内容を引用・参考とする場合には，その点にご留意ください。
  - 具体的には，本スライドは次に示す書籍の記載内容を含みます。
    - 『うかる！ 情報処理安全確保支援士 午後問題集』
    - 日本経済新聞出版 刊，ISBN978-4-532-41546-4

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、情報化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　山口 敏行
  - 副会長　清土 桂一郎
  - 副会長・事務局長　大島 真言

  （理事：17名、監事：2名）

- 会員　336名（2021年1月時点）

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

登録したら入ってほしいの♡

入会金 2000　年会費 4800
10月～翌3月入会なら翌春迄の会費 2400
詳しくはWebで。

※ 最重要事項
本日の目的
【会員の獲得】

その遠回りさは
シャケの人工孵化なみ！

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（以下「SC試験」）の実施団体（以下「IPA」）の活動とは関係がありません。
- 本セミナーならびに本資料には，村山が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および二次利用も禁止です。
- 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。

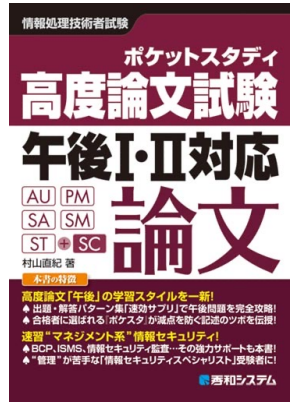
盗用は340万円を村山に支払う事に同意したものとみなします。

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～）



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

TLP：WHITE

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#3　1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

- 【「午前Ⅱ」目新しい出題】
  - **問6**　総務省及び国立研究開発法人情報通信研究機構（NICT）が2019年2月から実施している取組**“NOTICE”に関する記述**のうち，適切なものはどれか。
    - イ　国内のグローバルIPアドレスを有するIoT機器に，容易に推測されるパスワードを入力することなどによって，サイバー攻撃に悪用されるおそれのある機器を調査し，インターネットサービスプロバイダを通じて当該機器の利用者に注意喚起を行う。
  - **問7**　経済産業省が**“サイバー・フィジカル・セキュリティ対策フレームワーク（Version 1.0）”を策定した主な目的**の一つはどれか。
    - イ　新たな産業社会において付加価値を創造する活動が直面するリスクを適切に捉えるためのモデルを構築し，求められるセキュリティ対策の全体像を整理すること
  - **問9**　3Dセキュアは，ネットショッピングでのオンライン決済におけるクレジットカードの不正使用を防止する対策の一つである。**3Dセキュアに関する記述**のうち，適切なものはどれか。
    - エ　クレジットカード発行会社にあらかじめ登録したパスワードなど，本人しか分からない情報を入力させ，検証することによって，なりすましによるクレジットカードの不正使用を防止する。

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

- 【「午後Ⅰ」「午後Ⅱ」概観】その①
  - “書かせる” 出題，単なる知識問題は減った印象。下記の四つ程度。
    - **午後Ⅰ問1 設問2（2）空欄c 「FQDN」**
      - サーバ証明書の検証条件は，「サーバ証明書に（注：空欄b「オ subjectAltName」）のdNSNameがあれば，アクセス先のWebサーバNの［ **c** ］と合致し，（略）dNSNameがなければ，アクセス先のWebサーバNの［ **c** ］がsubjectの（注：空欄d「イ commonName」）と合致すること」。
    - **午後Ⅰ問2 設問1（1）空欄a 「LDAP」**
      - ディレクトリサーバの機能概要，「ディレクトリへのアクセスは，標準でTCPポートの389番を使用する［ **a** ］を用いる。」
    - **午後Ⅰ問2 設問1（2）空欄b 「OCSP」**
      - R社のPCのWebブラウザでは，「Webサーバのサーバ証明書が失効していないことを，RFC 6960で規定されている［ **b** ］を利用して確認できるようにしている。」
    - **午後Ⅱ問1 設問2 「本人の同意を得ないで，承継前における当該個人情報の利用目的の達成に必要な範囲を超えて，当該個人情報を取り扱ってはならない。」**
      - 会員向けWebサイトをもつ各社。「旧A社と旧B社の合併によるC社への事業承継に伴って取得した個人情報の取扱いに関し，個人情報保護法に定められている禁止事項は何か。」

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

- 【「午後Ⅰ」「午後Ⅱ」概観】その②
  - お騒がせインシデントを想わせる出題も

飲食業者がQRコード決済を自作するという野心作。悪いこと言いませんから，総務省の統一QR「JPQR」普及事業に乗っかりませんか？

俗称PPAPとかS/MIMEとか今春は出ない？

【午後Ⅰ】

- **問1　スマートフォンを用いた決済**に関する次の記述を読んで，設問1～3に答えよ。
- **問2　電子メール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3　Webシステムのセキュリティ診断**に関する次の記述を読んで，設問1，2に答えよ。

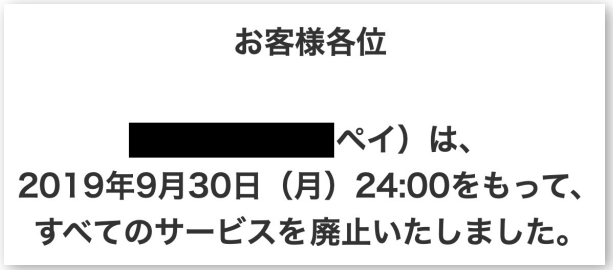
特に時事ネタでは無いけどT主任とUさんの熱血コンビ

【午後Ⅱ】

- **問1　百貨店におけるWebサイトの統合**に関する次の記述を読んで，設問1～5に答えよ。
- **問2　クラウドサービスを活用したテレワーク環境**に関する次の記述を読んで，設問1～6に答えよ。

設問4が，某ペイを想わせる出題

テレワークの出題は，近年（コロナ前から）の出題のトレンド，“働き方改革”ネタの一環でもあった。菅政権でどうなる？



©SEVEN PAY CO., LTD.

©2016 avex

©Keiichi ARAWI 2007

※ 画像はイメージです。

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

- 【「午後Ⅰ」「午後Ⅱ」概観】その③
  - 昨日公表，IPA『採点講評』によると
    - **【午後Ⅰ】**
      - **問1**では，スマートフォン用決済アプリケーションプログラムの開発を題材に，メッセージ認証を用いたなりすまし対策及びスクリーニング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，電子メールの暗号化を題材に，S/MIMEを使った電子メールシステムの設計について出題した。**全体として，正答率は平均的**であった。
      - **問3**では，ECサイトの脆弱性診断を題材に，診断を受ける企業での診断計画の策定について出題した。**全体として，正答率は平均的**であった。
    - **【午後Ⅱ】**
      - **問1**では，企業の合併に伴う複数のWebサイトの統合を題材に，リスク分析と，Webアプリケーションプログラムにおける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，働き方改革のためのマルチクラウドを活用したテレワーク環境の構築を題材に，クラウドサービス利用時のリスク評価について出題した。

なんでここだけ正答率が無い？

TLP：WHITE

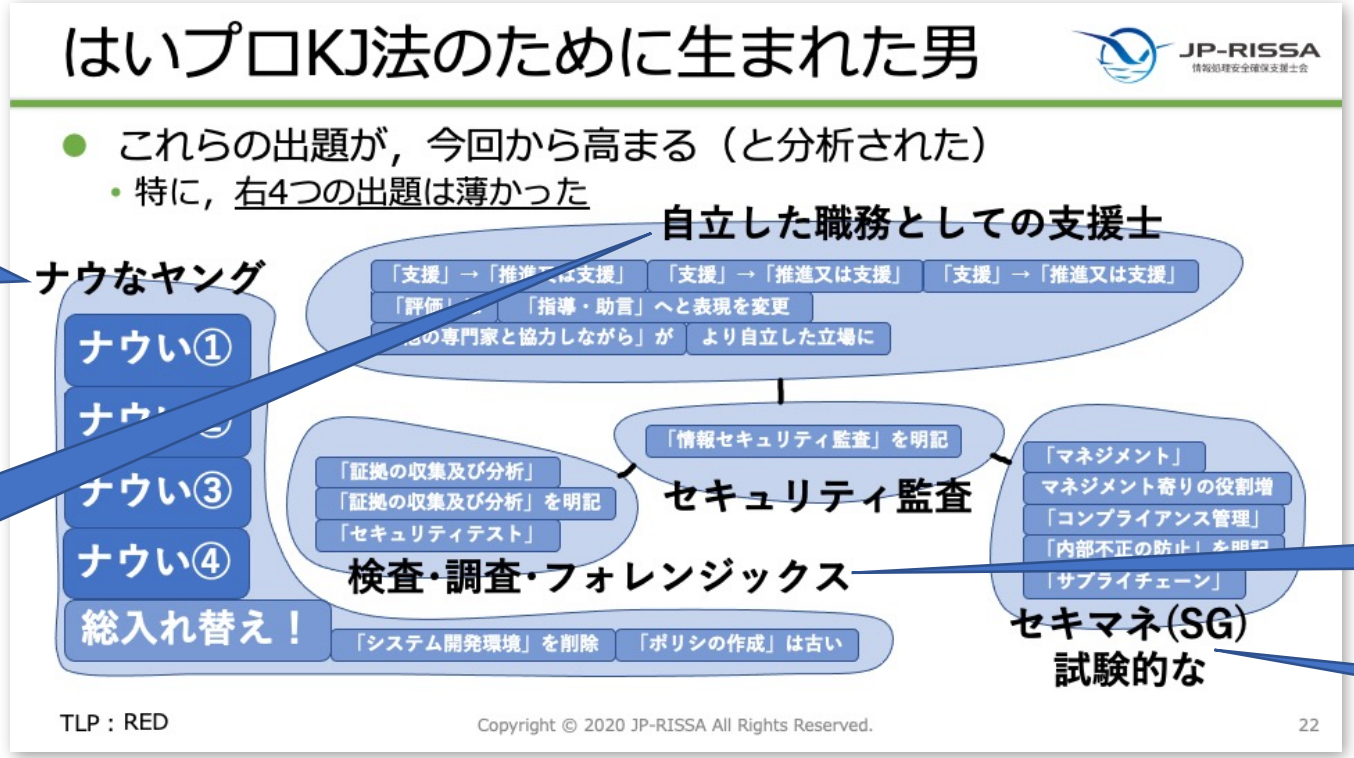
こう出た【概観・午前Ⅱ】⑤

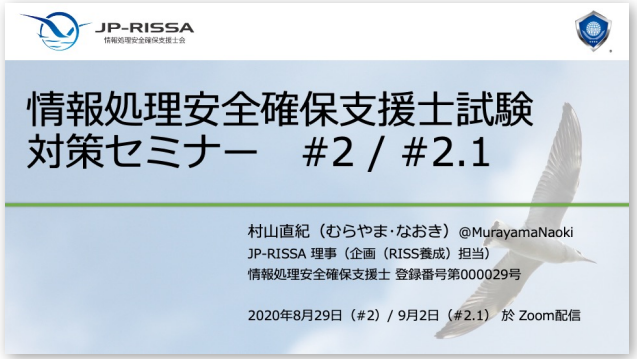
JP-RISSA 情報処理安全確保支援士会

- 【「午後Ⅰ」「午後Ⅱ」概観】その④
  - 昨夏に“マネジメント寄りの出題が増える”と予言したが，結果は？
    - その傾向は「午前Ⅱ」の目新しい3問に見られた。
  - “書かせる”出題の中心は，“知識を元に，状況を踏まえて推理せよ”。

時事ネタ的な出題
・午後Ⅰ問1，問2
・午後Ⅱ問1

推理させる出題
・午後Ⅰ問1，問2
・午後Ⅱ問2





※ 2020年8月29日／9月2日実施

脆弱性診断
・午後Ⅰ問3

「午前Ⅱ」の初出題

TLP：WHITE

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#3　1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

と，その前に

本セミナーを12月2日から募集したくせに，
村山理事には一抹の不安があった。

村山理事の戦績 その①

JP-RISSA 情報処理安全確保支援士会

令和２年度 １０月　情報処理安全確保支援士試験　成績照会

受験番号 SC204-0915 の方は，　合格　です

午前I得点	***.**点
午前II得点	92.00点
午後I得点	75点
午後II得点	62点

満点，合格基準は次のとおりです。		
時間区分	満点	基準点
午前I試験	100点	60%以上
午前II試験	100点	60%以上
午後I試験	100点	60%以上
午後II試験	100点	60%以上

「SC204」で始まる番号は，コロナ3密回避のため当初の会場のモード学園（新宿）がアフレてしまい，慶応義塾（三田）に飛ばされた人たちのもの

この免除のためだけに'19秋にAPに出願したら会場（東京都市大学）が台風で水没してしまい試験の数日前に会場がベルサール東京日本橋に代わる旨が村山にも届いたのだが，知らなかった多数の人が受験票通りに東京都市大に行ってしまったために大問題となった伝説の試験。てか会場水没ってなに。

午前 II の自己採点96点なのに…なんで？？

午後 I はこんなもんっす

午後 II 62点！どうゆうことやねんワレ💢

TLP：WHITE

村山理事の戦績 その②

JP-RISSA 情報処理安全確保支援士会

- こう書いた その①

午後Ⅰ 75点

※ 太字は誤答か微妙な表現

【午後Ⅰ】問2　電子メールのセキュリティ対策に関する次の記述
設問1（1）「LDAP」○
設問1（2）「OCSP」○
設問2（1）**「ZIPファイル復号用のパスワードがMLで皆に向けて送信されているから」**×
設問2（2）「メールサーバ」○
設問2（3）「S/MIME証明書を廃止したり破棄した場合」○
設問3　d**「S/MIME証明書」**×，e「検証」○，f「MLの登録メンバ」○，g「ML」○

【午後Ⅰ】問3　Webシステムのセキュリティ診断に関する次の記述を読んで（略）答えよ。
設問1（1）「N-IPSによって表面化が抑え込まれていた脅威が表面化するから」○
設問1（2）**「遮断モードに設定されていたものを検知モードに変える。」**×
設問1（3）**「（e）」**×
設問2（1）**「診断用の，利用者IDとポイント」**△
設問2（2）変更する項目「日時」○，変更する内容「PF診断の実施を0時～8時に変える。」○
設問2（3）機器「本番DBサーバ」○，変更後の設定**「ホスト型IPSの侵入検知設定を無効にする。」**△
設問2（4）c「本番DBサーバ」○，d「DB管理PC」○，e「許可」○

TLP：WHITE

村山理事の戦績 その③

JP-RISSA 情報処理安全確保支援士会

- こう書いた その②

午後Ⅱ 62点

※ 太字は誤答か微妙な表現

【午後Ⅱ】問2　クラウドサービスを活用したテレワーク環境に関する次の[illegible]答えよ。

設問1（1）「**エ**」×
設問1（2）「**初期設定用のQRコードを他人のスマホで先に読まれてしまう問題**」△
設問1（3）a「ウ」○，b「エ」○，c「イ」○，d「ア」○，e「カ」○，f「オ」○
設問2　「ノートPCの画面からの窃取や，スピーカからの音声の録音」○
設問3（1）「キャプチャ画面やキーロガーの情報を取得しインターネット経由で送出する。」○
設問3（2）「**ア，オ，カ**」×
設問4　「**ISMS等の認証の取得状況や，定期的に監査を受けているかを確認する。**」△
設問5　「**TOTPに従ってOTPを表示するスマホアプリ方式を採用したという対策**」×
設問6（1）「ノートPCへのログインに成功」○
設問6（2）「**利用者の死去等により二度とログインできなくなる**」×
設問6（3）「クライアント証明書等，クライアントのデバイスを認証する仕組み」○

TLP：WHITE

新春初嗤い

もう許して💧

© 見里朝希JGH・シンエイ動画／モルカーズ

午後Ⅰ・午後Ⅱ“書かせる”出題2～3問なら
落としても受かるんスね！

TLP：WHITE

試験対策のプロ？

“プロ() は，どう誤ったのか？”
時間に余裕があれば，その考察もしたく。

（再掲）本日の進行予定

対策セミナー#3　1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

昨夏のスライド

JP-RISSA
情報処理安全確保支援士会

除：用語穴埋め等，単なる知識問題

- 多数の別解候補を“枝払い”するヒントは，問題文のどこかにあり。
  - 本セミナーは「解答例至上主義」。“なぜ，その表現だけが正解なのか？”を考える（正解の根拠を問題文から掘り出す）ことが，良い勉強となります。
- IPA公表の解答例を見て「そんな答，実務じゃやらねーよ！」とか，その勢いで「この試験つかえねー」とかイキる人。
  - このイキりの原因は大抵，長い問題文（＋設問）の，端折り読み にあります。なので該当者は，問題文を丹念に読んでみましょう。
  - SC（ほか高度）試験は，「（長い問題文の）この条件下では，どんな答が導かれるか？」を問う試験。そこに，問題文の設定場面とは異なる育ち方をしてきた 己の経験だけに基づく答を書くと，エスパーでもない限り，バツ。
  - もし，端折り読みの癖があるなら，その原因は「これまでの人生で，国語力（特に読解力）を真剣に鍛えるチャンスが無かったから」かもしれません。
    - もし該当者なら，今日からは問題文を，一字一句だまさずに読み込んでみて下さい。

とは言っても，一朝一夕にできるものでもない → 代わりに要約しておきました。

TLP：WHITE

午後Ⅰ 問1

スマートフォンを用いた決済に関する次の記述を読んで，設問1～3に答えよ。

「問1では，**スマートフォン用決済アプリケーションプログラムの開発を題材に，メッセージ認証を用いたなりすまし対策及びスクリーニング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）

※ IPA公式解答例が出揃った後やもん，
解説は余裕の後出しジャンケンですわ。

TLP：WHITE

R02 SC午後Ⅰ問1 その①

JP-RISSA 情報処理安全確保支援士会

午後Ⅰ問1 設問1（1）

飲食業N社の，**飲食客のスマートフォンにもたせる**表1（**決済アプリ**の機能の概要（抜粋））**の内容は**，旧来からある「ポイントアプリの仕組みを利用し，16桁の**会員番号をバーコードとして表示する。**」等。また，表4（決済処理（抜粋））の内容は，飲食客である「利用者は，**決済アプリにバーコードを表示する。**」，「店員は，店舗アプリで，決済アプリに**表示されたバーコードを読み取る。**」，「バーコードが示す**会員番号に対して決済する。**」等。
次ページ，レビューでの指摘（表6）は，**「他者になりすまして決済できる。」**等。

【Q】どのような手段でなりすまして決済ができるのか。想定される手段を30字以内で具体的に述べよ。また，その攻撃が成功してしまう決済アプリにおける問題を25字以内で，具体的に述べよ。

【手段】【内一つ】「他者の会員番号を窃取してバーコードを生成し，決済する。（27字）」「他者のバーコードを会員番号から推測して表示する。（24字）」
【問題】【内一つ】「バーコードの内容が会員番号であること（18字）」「バーコードが永続的に利用できること（17字）」

「設問1（1）“問題”は，正答率がやや低かった。本問で扱うバーコードは，仕様上，決済のなりすましにつながるおそれがある。決済のなりすましが成功してしまう原因と防ぐ手段をよく理解してほしい。」（『採点講評』より）

※ バーコードやQRコードの生成方法（アルゴリズム）は，公知です。

TLP：WHITE

R02 SC午後Ⅰ問1 その②

JP-RISSA 情報処理安全確保支援士会

午後Ⅰ問1 設問1（2）

飲食業N社の，飲食客のスマートフォンで決済を行うシステムでは，**飲食客のなりすまし対策として「メッセージ認証を用いる**ことにした。具体的には，**決済機能利用時に**（注：飲食客側の）**決済アプリに表示する情報として，会員番号，**（注：**N社側の**）**WebサーバNで生成した乱数，時刻，**及び**それら三つの情報を基に生成されるHMAC**（Hash-based Message Authentication Code）**値を含める**ことにした」。
0.4ページ略，図3（QRコード生成及びQRコード検証の手順）が示す，**WebサーバNで行う「QRコード生成」の手順**は下記。
・「1. **WebサーバNがもつ秘密鍵Kを用いて，会員番号，乱数，時刻を基にしたHMAC値αを計算**する。」
・「2. **会員番号，乱数，時刻及びHMAC値αから成るQRコードを生成**する。」
また，**WebサーバNで行う「QRコード検証」の手順**は下記等。
・「1. **秘密鍵Kを用いて，**（注：飲食客側の決済アプリが表示する）**QRコード中の会員番号，乱数及び時刻を基にしたHMAC値βを計算**する。」
・「2. ［ a ］」

【Q】空欄に入れる適切な字句を，30字以内で述べよ。

「HMAC値αとHMAC値βの一致を検証する。（22字）」

※ 秘密鍵Kの値はWebサーバNしか知り得ないため，「HMAC値α」と「HMAC値β」は共に，WebサーバNにしか作ることができない値です。

TLP：WHITE

R02 SC午後Ⅰ問1 その③

JP-RISSA 情報処理安全確保支援士会

午後Ⅰ問1 設問2（1）

飲食業N社では，飲食客のスマートフォンによる「決済時に利用者（注：飲食客）のスマートフォンが確実に通信できるよう」，無線LANサービスを提供する。各店舗の「無線LANルータは全て同一の機種である」。また，**表5（無線LANルータの管理者機能の設定項目**（抜粋））**中，記号「い」**（設定項目名「**DNSプロキシ**」）**の設定内容は，「無線LANルータが参照するDNSサーバのIPアドレス」**。
レビューでの**表6**（Yさんの指摘）**の内容は，項番2が**「店舗の無線LANルータには**既知の脆弱性が存在する。その結果，インターネット側のインタフェースから**はアクセスできない仕様のはずが，**管理者機能のログイン画面にアクセスできてしまう。」，項番3が**「管理者機能のパスワードが**工場出荷時のパスワードから変更されていない**可能性がある。変更されていないと，店舗の無線LANルータに接続している利用者の端末から管理者機能にアクセスできる。」，**項番4が**「決済アプリ及び店舗アプリでの**サーバ証明書の検証に不備がある。**」等。
1.2ページ略，「**表6中の項番2～4の指摘を解決せずに**（注：利用者（飲食客）に）**無線LANサービスを提供し，**①攻撃者が無線LANルータの設定を変更する**と，攻撃者が用意したサーバに利用者が接続しても気付かない**おそれがある」。

【Q】下線①について，攻撃者はどの設定項目の内容をどのように変更するか。変更する設定項目を表5の中から選び，記号で答えよ。また，変更後の設定内容を25字以内で述べよ。

【変更する設定項目】「い」
【変更後の設定内容】「攻撃者のDNSサーバのIPアドレス（17字）」

TLP：WHITE

R02 SC午後Ⅰ問1 その④

JP-RISSA 情報処理安全確保支援士会

午後Ⅰ問1 設問2（2）

サーバ証明書が図4に示す条件を満たしているかどうかを検証するように決済アプリ及び店舗アプリを改修した。

・サーバ証明書に［ b ］のdNSNameがあれば，アクセス先のWebサーバNの［ c ］と合致し，サーバ証明書に［ b ］のdNSNameがなければ，アクセス先のWebサーバNの［ c ］がsubjectの［ d ］と合致すること
・有効期間内のサーバ証明書であること

図4　サーバ証明書の検証条件（抜粋）

【Q】（略）適切な字句を（略）［　c　］については5字以内で，それぞれ答えよ。

【b】「オ（subjectAltName）」【c】「FQDN（4字）」【d】「イ（commonName）」

「設問2（2）は，正答率が低かった。サーバ証明書のフィールドと，その検証方法をよく理解してほしい。」（『採点講評』より）

※ 本問の“dNSName”といった表記は，X.509証明書を規定したRFC 5280に倣ったもの。そして“subject”はその証明書の所有者を意味します。

TLP：WHITE

R02 SC午後Ⅰ問1 その⑤

JP-RISSA 情報処理安全確保支援士会

午後Ⅰ問1 設問3（1）

飲食業N社が開発する「**Nシステム**」では，「**アラート通知などの機能をもつWebサーバN**を用いて決済を実現する」。
次ページ，**Nシステムを構成する，飲食客のスマートフォンにもたせる「決済アプリ」での**，表3（**会員登録処理**（抜粋））は下記等。
・【入力されたメールアドレスが**会員登録されていない場合**】
「WebサーバNは，入力されたメールアドレスに（略）URLを電子メールで送信する。また，**決済アプリは，“電子メールを送信しました。”と表示**する。」
・【入力されたメールアドレスが**会員登録されている場合**】
「**決済アプリは，“既に使用されているメールアドレスです。”とエラー表示**する。」
2.9ページ略，「**攻撃者が，**（注：「**攻撃者の手元にあるパスワードリストから無効なものを取り除く**こと」を指す）②事前にスクリーニングを実行した**パスワードリストを用いて，パスワードリスト攻撃を行うと，Webサーバの**アラート通知機能では検知されない**おそれがある」。

【Q】下線②について，Nシステムのどのような挙動を利用してスクリーニングを実行したと考えられるか。利用したと考えられる挙動を40字以内で具体的に述べよ。

「メールアドレスが会員登録されているかどうかで表示が異なるという挙動（33字）」

※ やぶ蛇っスよね。このやぶ蛇を何とかする出題は，次のスライド。

TLP：WHITE

R02 SC午後Ⅰ問1 その⑥

JP-RISSA 情報処理安全確保支援士会

午後Ⅰ問1 設問3（2）

飲食業N社が開発する「**Nシステム**」では，「**アラート通知などの機能をもつWebサーバN**を用いて決済を実現する」。
次ページ，**飲食客のスマートフォンにもたせる「決済アプリ」での，表3（会員登録処理**（抜粋））は下記等。
・記号「2-a」【入力されたメールアドレスが**会員登録されていない場合】**
「WebサーバNは，**入力されたメールアドレスに詳細登録ページのURLを電子メールで送信**する。また，**決済アプリは，“電子メールを送信しました。”と表示**する。」
・記号「2-b」【入力されたメールアドレスが**会員登録されている場合】**
「**決済アプリは，“既に使用されているメールアドレスです。”とエラー表示**する。」
2.9ページ略，「**攻撃者が，**（注：**上記「2-a」「2-b」の表示差をヒントに「攻撃者の手元にあるパスワードリストから無効なものを取り除く**こと」を指す）②事前にスクリーニングを実行した**パスワードリストを用いて，パスワードリスト攻撃を行うと，WebサーバNのアラート通知機能では検知されない**おそれがある。そこで，Xさんは，③表3の会員登録処理を修正することにし（略）」。

【Q】下線③について，表3中の修正すべき処理を記号で答えよ。また，どのように修正すべきか。修正後の処理を，25字以内で述べよ。

【修正すべき処理】「2-b」
【修正後の処理】「2-aと同じメッセージを表示する。（17字）」

「設問3（1）は，正答率がやや高かった一方で，（2）“修正後の処理”の正答率は平均的だった。“修正後の処理”では，登録されているメールアドレスにエラーを通知するといった誤った解答が多かった。スクリーニングを防止するには，会員登録されている場合とされていない場合で表示内容を同じにする必要があることをよく理解してほしい。」（『採点講評』より）

午後Ⅰ 問2

電子メール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では，**電子メールの暗号化を題材に，S/MIMEを使った電子メールシステムの設計について出題した。**全体として，正答率は平均的であった。」（『採点講評』より）

R02 SC午後Ⅰ問2 その①

JP-RISSA 情報処理安全確保支援士会

午後Ⅰ問2 設問1（1）

表1中の「**ディレクトリサーバ**」**の機能概要**は，「・X.500モデルをサポートするディレクトリを管理し，当該ディレクトリへのアクセスを提供する。」，「・ディレクトリへのアクセスは，標準で**TCPポートの389番を使用する［　a　］を用いる。**」等。

【Q】空欄に入れる適切なプロトコル名を，英字5字以内で答えよ。

「LDAP（4字）」

※ 通常，LDAPサーバの運用では複数のポート番号を許可する必要があるため，「TCPポートの389番」と限定されたことで，かえって難しく捉えてしまった方もいた模様。

午後Ⅰ問2 設問1（2）

R社のPCのWebブラウザでは，「Webサーバの**サーバ証明書が失効していないことを，RFC 6960で規定されている［　　b　　］を利用して確認**できるようにしている」。

【Q】空欄に入れる適切なプロトコル名を，英字5字以内で答えよ。

「OCSP（4字）」

「設問1（2）は，正答率がやや低かった。SSHやFTPといった解答が散見された。OCSPは，X.509公開鍵証明書の失効状態をタイムリーに確認できるプロトコルである。OCSPの仕組みをよく理解してほしい。」（『採点講評』より）

※ “OSCP”だと資格名です。

TLP：WHITE

R02 SC午後Ⅰ問2 その②

JP-RISSA 情報処理安全確保支援士会

午後Ⅰ問2 設問2（1）

R社では，「委託先が社内ルールで外部のファイル交換サービスの利用を禁止している場合は，**設計ドキュメントファイルをパスワード付きZIPファイルにし，メールに添付**して，メーリングリスト（以下，MLという）のメールアドレス宛てに送信している。ZIPファイルのパスワードは，平文のメールでMLのメールアドレス宛てに送信している」。
2.2ページ略，**表3**（委託先との**メール利用についての要件**）**中の項番1，「送信者から受信者まで暗号化された状態で，メールを送受信**する。」に対するE主任の指摘は，「・①メールの通信を暗号化しただけでは，表3の項番1を満たせない。」等。
次ページ，「**S/MIMEを利用すれば表3の要件を実現できる**ことが分かった」。

【Q】下線①の理由を，35字以内で述べよ。

「メールサーバ上では，メールが暗号化されていないから（25字）」

※ 村山理事が答えた，“これってPPAPの話でしょ？ ならば「**ZIPファイル復号用のパスワードがMLで皆に向けて送信されているから**」よ！”**は，なぜバツ？**
→ 本問，変ちくりんな運用ではありますが，**ZIPファイルについてだけはエンドツーエンドの暗号化を達成済み**です。**対して，メールの本文（例：挨拶文）については平文のまま。これが途中のメールサーバ上では読めてしまう**，という点を汲むべき出題でした。

「設問2（1）は，正答率が平均的であった。SMTP over TLS及びPOP3 over TLSによって，通信は暗号されるが，メールサーバ上の電子メールは暗号化されていないということをよく理解してほしい。」（『採点講評』より）

TLP：WHITE

R02 SC午後Ⅰ問2 その③

JP-RISSA 情報処理安全確保支援士会

午後Ⅰ問2 設問2（2）

R社での，**表3（委託先とのメール利用についての要件）中の項番2**，「委託先とのやり取りの**メールがなりすまされたものでないかどうかを確認できるように，送信者を検証**する。」について，Hさんは，「**メールの通信を暗号化することによって**（略）**要件に対応できる**のではないか」と話した。
これに対するE主任の指摘は，「**・攻撃者が委託先を装った［　c　］を用意するようななりすましは，送信元の［　c　］の真正性を確認して検出できる。**一方，送信者メールアドレスとして委託先のメールアドレスを使うようなりすましは検出できないので，表3の項番2を満たせない。」等。

【Q】空欄に入れる適切な字句を，10字以内で答えよ。

「メールサーバ（6字）」

※ よくある誤答例，“**委託先の某社と紛らわしい「ドメイン名」**を用意する”**は，なぜバツ？**
→ **攻撃者が用意した（＝正当な手続きで取得した）ドメイン名からのメールであるなら，たとえ委託先の某社と紛らわしいドメイン名であっても，それは真正なメール**です。

TLP：WHITE

R02 SC午後Ⅰ問2 その④

JP-RISSA 情報処理安全確保支援士会

午後Ⅰ問2 設問2（3）

R社の「E主任とHさんは，**S/MIMEの利用を想定した次の方式**を考えた」。
・「（あ）R社CAで，S/MIMEで利用する鍵ペアを生成し，**S/MIMEに利用可能なクライアント証明書**（以下，**S/MIME証明書**という）**を発行**する。」
・「（い）（注：省略）。」
・「（う）S/MIME証明書が**失効していないことをメールクライアントから確認**する。」
・「（え）後でも参照する必要があるメールは，**②復号できなくなる場合**に備えて，復号してファイルサーバに保存する。」

【Q】下線②について，復号できなくなるのはどのような場合か。25字以内で述べよ。

「復号に必要な秘密鍵を意図せず削除した場合（20字）」

※ 本問のポイントは，**“S/MIMEで暗号化されたメールを後で復号したければ，復号に必要な秘密鍵をもつS/MIME証明書を，ずっと（永続的に）残しておくべき”**という点でした。

「設問2（3）は，正答率が高かった。S/MIMEでの電子メールの復号の仕様について，よく理解されていた。」（『採点講評』より）

TLP：WHITE

R02 SC午後Ⅰ問2 その⑤

JP-RISSA 情報処理安全確保支援士会

午後Ⅰ問2 設問3

システム開発会社R社の「各PCには，R社CAのルート証明書を信頼できる発行元として登録している」。R社での**表3（委託先とのメール利用についての要件）中の項番1は「メールの暗号化」，項番2は「送信者の検証」**。
次ページ，R社の「E主任とHさんは，S/MIMEの利用を想定した次の方式（注：「（あ）R社CAで，**S/MIMEで利用する鍵ペアを生成し，S/MIMEに利用可能なクライアント証明書**（以下，**S/MIME証明書**という）**を発行**する。」等）を考えた」。リストアップした「**解決すべき課題**」は下記等。
・「（ア）**R社CAのようなプライベート認証局のルート証明書をPCに登録することが，委託先によっては禁止**されており，その場合，**R社の従業員が送信したメールの［　d　］を［　e　］することができない。**」
・「**（ウ）ML**（注：**登録メンバに取引先も含むメーリングリスト**）**宛てのメールを暗号化できない。**」
次ページ，「**S/MIMEを用いて［　d　］を付与したメールを送信**すれば，受信者はS/MIME証明書も受け取れるし，送信者が他者になりすましていないことも確認できる（略）」。**上記（ウ）については「次の案を考えた」**。
・「（1）R社のプロジェクト管理者は，あらかじめ，（注：MLも提供する**G社のメールサービスである**）**Gサービスに［　f　］のメールアドレスのS/MIME証明書を登録**する。」
・「（2）R社のプロジェクト管理者は，**あらかじめ，［　g　］のメールアドレスのS/MIME証明書の発行手続をG社に依頼**する。」
・「（3）**メール送信者は，［　g　］のメールアドレスのS/MIME証明書を使って暗号化したメールを送信**する。」
・「（4）Gサービスは，メールを復号する。」
・「（5）**Gサービスは，［　f　］のメールアドレスのそれぞれのS/MIME証明書を使い**，受信後にそれぞれが復号できるようにして**メールを暗号化**する。」
・「（6）Gサービスは，暗号化したメールを送信する。」

【Q】（略）適切な字句を（略）答えよ。

【d】「ディジタル署名（7字）」，【e】「検証（2字）」，【f】「MLの登録メンバ（8字）」，【g】「ML（2字）」

TLP：WHITE

午後Ⅰ 問3

Webシステムのセキュリティ診断に関する次の記述を読んで，設問1，2に答えよ。

「問3では，**ECサイトの脆弱性診断を題材に，診断を受ける企業での診断計画の策定について出題した。**全体として，正答率は平均的であった。」（『採点講評』より）

TLP：WHITE

R02 SC午後Ⅰ問3 その①

JP-RISSA 情報処理安全確保支援士会

午後Ⅰ問3 設問1（1）

本問の「**PF診断**」は「プラットフォーム診断」の略であり，サーバやネットワーク機器への**全ポートのスキャンと，開いていたポートに対する脆弱性の検出**を指す。
ECサイトを運営するL社の，図1（Pシステムの**ネットワーク構成**（概要））**が示す接続は，「インターネット」**-「FW1」-「SSLアクセラレータ」-「**N-IPS**（注：ネットワーク型IPS）」-「L2SW」-「**本番Webサーバ**」等。
2.2ページ略，**本番Webサーバの脆弱性をインターネット側からPF診断する際，N-IPSによる脅威通信判定を**「有効なまま診断するケースと比べ，**無効にすると，**①より多くの脆弱性を検出する可能性があります」。

【Q】下線①について，その理由を35字以内で述べよ。

「N-IPSで遮断されていたPF診断の通信が通過するから（27字）」

※「機器を，そこに設置することにした理由は？」と問い，**答の軸に「そこはFWよりもLAN側なので，守ってくれるから。」を据えさせる出題は定番。**このように“ナニカに守られている”旨が図表から読み取れた場合，その箇所よりも内側ではヌクヌクとしていられます。
本問は，この理屈の反対を答えればOKです。

「設問1は，（1）の正答率が高かった。プラットフォーム診断を実施する際のネットワーク型IPSの基本的な挙動は，よく理解されていた。一方，（3）は正答率が低かった。診断PCの接続箇所を，管理LANにある接続箇所から選択した誤った解答が多かった。表2の“診断1”は，インターネットから本番Webサーバへの攻撃を想定した診断を内部のネットワークから実施するものであり，管理LANからでは適切な診断ができない。脆弱性診断の計画策定においては，どのような脅威を想定したものなのかを念頭に置くことが重要である。」（『採点講評』より）

R02 SC午後Ⅰ問3 その②

JP-RISSA 情報処理安全確保支援士会

午後Ⅰ問3 設問1（2）

表1より，ECサイトを運営するL社では「**N-IPS**（注：ネットワーク型IPS）」**で「インターネットから本番Webサーバへの通信**（略）**を監視している**。遮断モードと検知モードの2種類のモードがあり，（略）通信ごとに，**次の番号の小さい順に，最初に合致したルールが適用される**」。

・「**1．ホワイトリスト判定**：ホワイトリストに**登録したIPアドレスからの通信は，脅威ではないと判定**する。」

・「2．脅威通信判定：通信の内容を解析し，脅威レベルが高いと定義しているものは，脅威と判定する。」

「現在は，遮断モードに設定されており，ホワイトリスト判定と脅威通信判定が有効になっている。**ホワイトリストには，現在，IPアドレスは一つも登録されていない**」。

1.8ページ略，**本番Webサーバの脆弱性をインターネット側から診断する際，脅威通信判定を無効にすると「本物の攻撃を防げないというリスクも生ずる**。無効にするのではなく，<u>②N-IPSの設定を変更すれば</u>，そのようなリスクは生じない」。

【Q】下線②について，<u>どのような設定変更</u>をすべきか。設定変更の内容を30字以内で述べよ。

「ホワイトリストに診断PCのIPアドレスを登録する。（25字）」

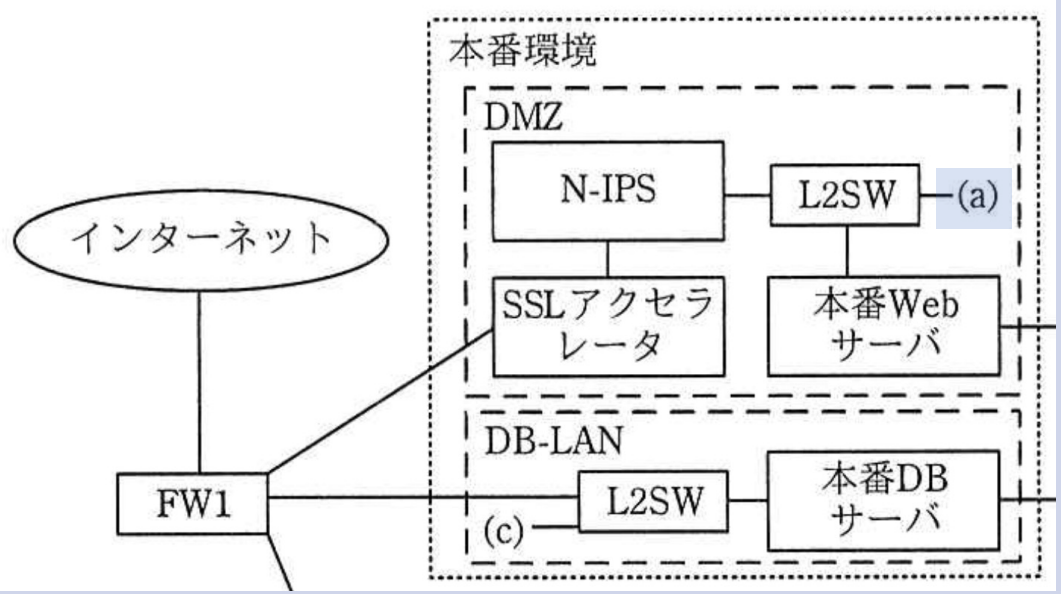
※ 答の軸には，**「ホワイトリストには，現在，IPアドレスは一つも登録されていない」＋“…を改善する。”** を据えましょう。そこに言葉を肉付けすればOK。

TLP：WHITE

R02 SC午後Ⅰ問3 その③

午後Ⅰ問3 設問1（3）

本問の「**PF診断**」は「**プラットフォーム診断**」の略。



PF 診断については，T 主任から助言を得ることにした。次は，本番 Web サーバがインターネットから攻撃される脅威を想定した時の，PF 診断に関する，U さんと T 主任の会話である。

T 主任：それと，インターネットからの PF 診断の通信経路を考慮すると，インターネットからの PF 診断だけでなく，内部のネットワークからの PF 診断も実施すべきだ。

U さん：分かりました。その場合は，想定する脅威を踏まえると，診断 PC を図 1 中の接続点 [a] に接続して診断すれば良いでしょうか。

【Q】（略）［ a ］に入れる診断PCの接続箇所を，図1中の接続点（a）～（f）の記号で答えよ。

【a】「（a）」

※“Uさんの言う「想定する脅威」が何を指すか”を読解させる，国語的な問題。（村山理事は×）

TLP：WHITE

R02 SC午後Ⅰ問3 その④

JP-RISSA 情報処理安全確保支援士会

午後Ⅰ問3 設問2（1）

ECサイトを運営する「L社のポイントサービス部が管理する**ポイントシステム**（以下，**Pシステム**という）」のネットワーク構成（図1）には，「本番環境」と検証用の「ステージング環境」が併存。
1.4ページ略，**脆弱性診断の要件**（図3）**は**，「2．**診断に当たって**（略）**設定及びデータを変更した場合は，診断終了後，診断前の状態に戻し**，システムの正常な動作を確認すること」等。「**Webアプリケーション診断**（以下，**Web診断**という）」**については**，「**・診断用の利用者IDを作成**する。その利用者に診断用のポイントを付与し，Pシステムにログインして診断する。」等のように実施することにした。
1.4ページ略，レビューでの指摘は，Web診断を「ステージング環境で実施する際，全ての診断の終了後に，担当者が，FW1の設定を元に戻すこと，及び**ステージング環境の［　b　］を削除することを，明確に手順書に記載する**こと」等。

【Q】空欄に入れる適切な字句を，15字以内で具体的に答えよ。

「診断用の利用者ID（9字）」

※ 本問の用語「ポイント」は，Pシステムで使えるポイント（例：何かのアイテムと交換できる値）を指します。**多くの受験者が“「診断用のポイント」も削除に加えるべきか？”に迷いました。**ですが，**「診断用の利用者ID」を削除すれば，通常は芋づる式で「診断用のポイント」も自動削除されます。**そのため，**IPA公表の解答例には，文字列「診断用のポイント」が含まれていません。**

「設問2（1）～（3）は，診断対象システムの業務影響や，既存のセキュリティ機器の運用への影響に関するマネジメントの問題であった。診断において重要であるので，よく理解してほしい。」（『採点講評』より）

TLP：WHITE

R02 SC午後Ⅰ問3 その⑤

JP-RISSA 情報処理安全確保支援士会

午後Ⅰ問3 設問2（2）

ECサイトを運営するL社の「**Pシステムが受信する1日の時間帯別の通信量の比率は，0時～8時が2%**，8時～16時が55%，16時～24時が43%である」。
1.2ページ略，今回行う**Pシステムへの脆弱性診断の要件**（図3）**は**，「1．**本番環境への影響を最小化すること**」等。
1.4ページ略，**診断計画（表2）中の項目「日時」**の内容は，「○月×日から○月△日（10営業日）**9時～17時**（うち，診断時間は1日当たり連続した5時間程度）」。
次ページ，レビューでの指摘は，**プラットフォームの診断は「サーバが異常停止した場合の影響を最小化するために**③計画の一部を変更すること」等。

【Q】下線③について，何をどのように変更すべきか。Pシステムの通信量に着目し，変更する項目を表2から選び答えよ。また，変更する内容を20字以内で述べよ。

【変更する項目】「日時」，【変更する内容】「診断時間を0時～8時の間にする。（16字）」

※ これはネットワークスペシャリスト試験か，ITサービスマネージャ試験で出しそうな出題。
通信量の比率が極端に低い「2%」という値を示す，Pシステムの「0時～8時」。この時間帯であれば，仮に脆弱性診断でヘマをやってサーバが停まったとしても，日中などよりは迷惑を掛けにくいと言えます。

TLP：WHITE

R02 SC午後Ⅰ問3 その⑥

JP-RISSA 情報処理安全確保支援士会

午後Ⅰ問3 設問2（3）

L社の，**図1**（Pシステムの**ネットワーク構成**（概要））**中の「本番DBサーバ」には**，表1より「**ホスト型IPSが導入されている**」。図2より，**下記の「判定で通信が拒否されると**（略，注：**ホスト型IPSは**）執務室内にある**警告灯を点灯させる**」。

・「**1．ホワイトリスト設定：**登録されたIPアドレスからの通信だけを許可し，それ以外を拒否する。**ホワイトリストには，現在，本番WebサーバとDB管理PCのIPアドレスだけが登録**されている。」

・「**2．侵入検知設定：**ホストの通信を監視して，脅威と判定した通信を拒否し，それ以外を許可する。**侵入検知設定は無効にもでき，無効にすると，ホストの通信を全て許可**する。」

次ページの図4より，脆弱性診断の診断サービスが用いる「**診断PCは**，既存の機器とは**別のIPアドレスを設定し，インターネット又は内部のネットワークに接続する**」。

1.8ページ略，レビューでの指摘は，**本番DBサーバへの脆弱性診断である「診断2の実施に当たっては**，警告灯が点灯することで社内に混乱が起きないよう，運用グループに④機器の設定の変更**を依頼する**こと」等。

【Q】下線④について，どの機器に対して，どのように設定を変更すべきか。機器は図1中から選び，変更後の設定は55字以内で具体的に述べよ。

【機器】「本番DBサーバ」，【変更後の設定】「ホスト型IPSのホワイトリスト設定に，診断PCのIPアドレスを登録し，侵入検知設定を無効にする。（48字）」

※ 図1，図2，図4の記載を統合して，初めて全容が見える出題です。

TLP：WHITE

R02 SC午後Ⅰ問3 その⑦

JP-RISSA 情報処理安全確保支援士会

午後Ⅰ問3 設問2（4）

ECサイトを運営するL社の，**図1**（Pシステムの**ネットワーク構成**（概要））**が示す接続は，本番環境**（「**本番Webサーバ**」「**本番DBサーバ**」）- 管理LANの「**FW2**」- **管理PCセグメント**（「**DB管理PC**」「**Web管理PC**」）等。
次ページ，表1（Pシステムの機器の概要（抜粋））より，**本番DBサーバには後述する「ホスト型IPSが導入されている」**。また，**FW2は**「ステートフルパケットインスペクション型のFWである。**管理PCセグメントから，本番Webサーバ，本番DBサーバ**，（注：ステージング環境に設置される）ステージングWebサーバ及びステージングDBサーバ**への通信を許可し，それ以外の通信は全て拒否している**」。
図2（**ホスト型IPS**の概要）の内容は，「（注：「**現在，本番WebサーバとDB管理PCのIPアドレスだけが登録されている**」）**ホワイトリスト設定**や侵入検知設定**による判定で通信が拒否されると**（略）執務室内にある**警告灯を点灯させる**。」等。
2.8ページ略，「**Web管理PCから本番DBサーバにログインを試みた。その結果，警告灯が点灯**（略）その再発防止策の一つとして，**FW2のルールを修正し，［　c　］宛ての通信については，［　d　］からの通信だけを［　e　］する**ことにした」。

【Q】［　c　］，［　d　］に入れる適切な字句を，図1中から選び答えよ。また，本文中の［　e　］に入れる適切な字句は，許可又は拒否のいずれか。（以下略）

【c】「本番DBサーバ」，【d】「DB管理PC」，【e】「許可」

TLP：WHITE

本日の進行予定

対策セミナー#3　1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

午後Ⅱ 問1

百貨店におけるWebサイトの統合に関する次の記述を読んで，設問1～5に答えよ。

「問1では，**企業の合併に伴う複数のWebサイトの統合を題材に，リスク分析と，Webアプリケーションプログラムにおける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）

本日の進行予定

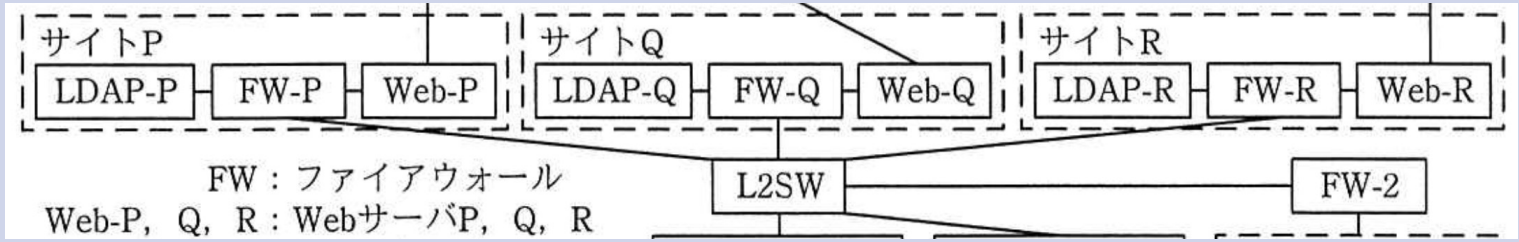
対策セミナー#3　1月16日（土）19時半 ～ 21時

- 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

R02 SC午後Ⅱ問1 その①

午後Ⅱ問1 設問1

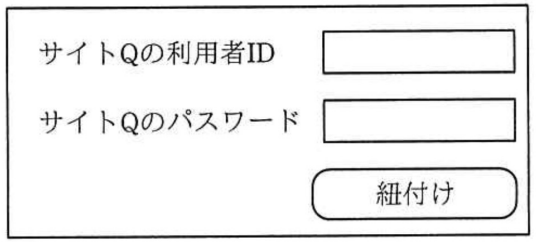


(1) サイトPのアカウントを親アカウントとし，サイトQ，Rのアカウントを子アカウントとして，子アカウントを親アカウントに紐付ける。主に旧A社の顧客向けである。

表2　変更後のFW-Pのルール

項番	送信元	宛先	プロトコル	動作
1	監視サーバ，管理コンソール，Web管理課LAN	Web-P，LDAP-P	管理用プロトコル	許可
2	Web-Q，Web-R	LDAP-P	LDAP	許可
3	Web-P	a	b	許可

サイトPのアカウントを親アカウントとし，サイトQのアカウントを子アカウントとして紐付けるときのサイトPの画面と処理内容は図2のとおりである。



［紐付け］ボタンが押された場合の処理
(i) Web-PのWebアプリが，LDAP-Qに問合せて，入力されたサイトQの利用者IDとパスワードを用いて認証を行う。
(ii) 認証に失敗したら，エラー画面を表示する。
(iii) Web-PのWebアプリが，LDAP-Pの該当するユーザエントリのsiteQid属性に，サイトQの利用者IDを書き込んで完了画面を表示する。

注記　サイトPにログイン済みである。

図2　サイトPにおけるサイトQのアカウントの紐付けの画面と処理内容

【Q】表2中の［　a　］，［　b　］に入れる適切な字句を答えよ。

【a】「LDAP-P，LDAP-Q，LDAP-R」，【b】「LDAP」

「設問1aは，正答率が低かった。サイトPを運用するために，Web-PからLDAP-Pへの通信が必要だという点を考慮できていない解答が多かった。ファイアウォールの設定は，セキュリティ確保の基本なので，細心の注意を払う必要があることに留意してほしい。」（『採点講評』より）

TLP：WHITE

R02 SC午後Ⅱ問1 その②

JP-RISSA 情報処理安全確保支援士会

午後Ⅱ問1 設問2

C社は「旧A社と旧B社が合併してできた会社」。
3.2ページ略，**C社Web管理課のJ主任は**，法務担当のMさんに，**旧A社・旧B社それぞれが運営していた会員向けWebサイトの「アカウントの共通利用について説明**し，個人情報の取扱いの観点から問題がないかどうか相談した。**Mさんは，合併前後の個人情報の利用目的の内容について確認**した」。

【Q】旧A社と旧B社の合併によるC社への事業承継に伴って取得した個人情報の取扱いに関し，個人情報保護法に定められている禁止事項は何か。70字以内で述べよ。

「本人の同意を得ないで，承継前における当該個人情報の利用目的の達成に必要な範囲を超えて，当該個人情報を取り扱ってはならない。（61字）」

※ 本問の元ネタは，個人情報保護法（個人情報の保護に関する法律）第十五条，「**個人情報取扱事業者は**，個人情報を取り扱うに当たっては、**その利用の目的**（以下「**利用目的**」という。）**をできる限り特定しなければならない**。」と，同法 第十六条，「個人情報取扱事業者は，**あらかじめ本人の同意を得ないで**，前条の規定により特定された**利用目的の達成に必要な範囲を超えて，個人情報を取り扱ってはならない**。」です 。

「設問2と設問4では，リスク分析について出題した。設問2は正答率がやや低く，設問4は正答率が平均的であった。消費者向けのWebサイトでは，個人情報を取り扱うことが多いので，個人情報保護に関する法規制について，よく理解してほしい。」（『採点講評』より）

TLP：WHITE

R02 SC午後Ⅱ問1 その③

JP-RISSA
情報処理安全確保支援士会

- すみません。下記の設問は正直，解説とスライド化がしんどいです。下記はいずれも記号穴埋め（または二者択一問題）なので，お手許にIPAの公式解答例と過去問題（PDFとか）をご用意の上，JavaやSAMLがお好きな方は御自身で解いて下さい。
  - 設問3（1）
  - 設問3（2）
  - 設問5（1）
  - 設問5（2）
  - 設問5（3）

ごめんね♡

© 見里朝希JGH・シンエイ動画／モルカーズ

「設問3と設問5では，Javaを題材として，Webアプリケーションプログラムにおけるセキュアプログラミングについて出題した。いずれも正答率が高かった。情報処理安全確保支援士の重要な業務の一つに，セキュリティの観点でのソースコードレビューが挙げられる。ソースコードレビューは，開発チーム全体の技術レベルを向上させる効果的な方法なので，ぜひとも今後の業務に生かしてほしい。」（『採点講評』より）

- 次に示すスライドが，今回のスライド化の限界です。

TLP：WHITE

R02 SC午後Ⅱ問1 その④

JP-RISSA 情報処理安全確保支援士会

午後Ⅱ問1 設問3（3）

本問のJavaソースコードの「インポート宣言には，javax.naming.NamingExceptionを含む」。また，**「図3及び図4は，サイトPのアカウントにサイトQのアカウントを紐付ける場合のサイトP上での紐付け処理のJavaソースコード」。図3**（Web-PのWebアプリにおける**AccountLinkのクラス定義）中のコンストラクタ内の処理は「childChecked = false;」等だが**，同クラスで定義されるメソッド「public int checkChild() throws NamingException」内の**判定処理「childChecked = childSite.equals("siteQ") || childSite.equals("siteR");」によって，childCheckedには通常はtrueが代入される。**
また，同クラスで定義され，**checkChild()が呼ぶメソッド**である「private int siteQAuth(String qID, String qPW) throws NamingException」**は，「必要な通信ができないなど，認証そのものが実行できない場合，例外NamingExceptionを投げる」**。この例外eを**catchしたcheckChild()は，行番号32で「throw e;」を行う。**
また，**図4**（Web-PのWebアプリにおける**AccountLinkのメソッドを呼んでいる部分**）中の処理は，「AccountLink idPair = new AccountLink(siteID, userID, userPassword, loginId);」を経て，**「catch (NamingException e)」した場合は**3回「再試行のために，一定時間待つ。」を繰り返し，**「if (!idPair.childChecked)」の条件に合致しなければ，「idPair.makeLink(); //アカウントの紐付けを実施する。」が（意図せず）実行されてしまう。**
「K主任は，**図3の32行目前後に着目し，［　i　］という修正案**を提示した」。

【Q】空欄に入れる適切な処理内容を50字以内で具体的に述べよ。

「NamingExceptionを投げる前に，childCheckedをfalseにする（43字）」

※ しんどいので本問の解説は今春発売予定の拙著をお読み頂ければ幸いです。

TLP：WHITE

R02 SC午後Ⅱ問1 その⑤

JP-RISSA 情報処理安全確保支援士会

午後Ⅱ問1 設問4（1）

本問の「**サイトR**」は，会員向けWebサイト。図5（サイトRの**パスワード失念時の操作画面**）**が示す入力項目は**，テキストボックス（「会員番号」「誕生日（月日）」）と**ボタン**（「**登録済みのメールアドレスでメールが受信できない場合**」等）**であり，このボタンをクリックすると，新たな**テキストボックス（「新たなメールアドレス」）と**ボタン**（「**新たなメールアドレスに現在のパスワードをメールで送信**」）**を表示する。**
「J主任は，**攻撃者がパスワード失念時の処理を悪用して，会員番号及び誕生日を総当たりで入力し，たまたま合致した当該顧客のアカウントを乗っ取った**ものと判断した」。L課長の発言は，「サイトRの**パスワード失念時の処理**」**がもつ問題の**「二つ目は，パスワードそのものをメールで送るという問題だ。**三つ目は，［ j ］という問題**だ。二つ目と三つ目の**問題の解決には，**（注：空欄k「**パスワードリセットのURLを，登録済みメールアドレスだけに送る**」）**ように改修すべき**だ。この方法では，一部の利用者はパスワード失念時にログインできなくなるが，その場合はコールセンタで対応することにしよう。」等。

【Q】空欄に入れる<u>適切な内容</u>を40字以内で述べよ。

「パスワードを，本人以外のメールアドレスに送ることができる（28字）」

※ 村山が採点者なら，“任意のメールアドレス宛てにパスワードを送ることができる”旨が述べてあればマルです。

TLP：WHITE

R02 SC午後Ⅱ問1 その⑥

JP-RISSA 情報処理安全確保支援士会

午後Ⅱ問1 設問4（2）

L課長の発言は，**会員向けWebサイトである「サイトRのパスワード失念時の処理」**がもつ**問題の「二つ目**は，**パスワードそのものを**（注：会員に新たに入力させるメールアドレスに）**メールで送る**という問題だ。**三つ目**は，（注：空欄j**「パスワードを，本人以外のメールアドレスに送ることができる」**）という問題だ。**二つ目と三つ目の問題の解決には，［　k　］ように改修すべき**だ。この方法では，一部の利用者はパスワード失念時にログインできなくなるが（略）」等。

【Q】空欄に入れる適切な内容を40字以内で述べよ。

「パスワードリセットのURLを，登録済みメールアドレスだけに送る（31字）」

※ **答の組み立て方は下記**。やってることは，文字列コンカチとコピペ改変です。

① **「パスワードそのものをメールで送るという問題」＋“を解決。”**
② **＋“加えて，”＋**
③ **「（略）本人以外のメールアドレスに送ることができる」問題 ＋“を解決。”**

①②③を更にコンカチし，表現を整えて，解答例と同義が作れたら勝ちです。

TLP：WHITE

R02 SC午後Ⅱ問1 その⑦

JP-RISSA 情報処理安全確保支援士会

午後Ⅱ問1 設問4（3）

A社とB社が合併した「C社は，**旧A社が発行していたクレジットカードの会員向けWebサイト**（以下，**サイトP**という），（注：**旧A社の**）**A百貨店の取扱商品を販売するオンラインストアWebサイト**（以下，**サイトQ**という），及び**旧B社のポイントカードを保有する会員向けWebサイト**（以下，**サイトR**という）を運営している」。
また，**各サイトの機能**（表1）**は，「サイトP」が**「クレジットカード**利用ポイントの**残高確認，**商品又は他社のポイントとの交換申請**」等，**「サイトQ」が「A百貨店の商品の購入」**等。
次ページ，**〔サイト間でのアカウントの共通利用〕の記述**は，**「サイトRのアカウントを親アカウントとし，サイトP，Qのアカウントを子アカウントとして**，子アカウントを親アカウントに**紐付ける。**」等。次ページ，「顧客が**アカウントの紐付けを設定すれば，子アカウントの代わりに親アカウントを用いて各サイトにログインできる**」。
5.9ページ略，**サイトRで生じたアカウント乗っ取り**について，「もしもこれらの問題に気付かずに**アカウントの共通利用を**（注：**サイトRが**）**提供していたら，**①利用者に更に大きな被害が発生するところだった」。

【Q】下線①について，更に大きな被害とは何か。具体的な被害を二つ挙げ，それぞれ30字以内で述べよ。

【順不同】「サイトPでポイントが不正に利用される。（19字）」「サイトQでA百貨店の商品が不正に購入される。（22字）」

※ シングルサインオンには “一点突破，全面展開” されるリスクあり。それと同じ発想で解きます。

TLP：WHITE

午後Ⅱ 問2

クラウドサービスを活用したテレワーク環境に関する次の記述を読んで，設問1～6に答えよ。

「問2では，**働き方改革のためのマルチクラウドを活用したテレワーク環境の構築を題材に，クラウドサービス利用時のリスク評価について出題した。**」（『採点講評』より）

R02 SC午後Ⅱ問2 その①

JP-RISSA 情報処理安全確保支援士会

午後Ⅱ問2 設問1（1）

まず，IDaaS-Y が対応している 2 要素認証について調査した。パスワード方式による認証に追加可能なものは次の 4 方式であった。

SMS 方式　：事前登録した電話番号に SMS でワンタイムパスワード（以下，OTP という）を送付する。

自動音声方式　：事前登録した電話番号に自動音声で OTP を通知する。

スマホアプリ方式：OTP 表示用のスマホアプリケーションソフトウェア（以下，OTP アプリという）を利用する。OTP アプリは TOTP（Time-Based One-Time Password Algorithm）に従って OTP を表示する。

FIDO 方式　：事前登録したデバイスで FIDO 認証を行う。

費用を抑えたいが，SMS 方式及び自動音声方式は認証の都度料金が発生する。また，FIDO 方式は，FIDO 認証に対応したスマホが必要となるが，貸与予定のスマホは FIDO 認証に対応していない。そこで，スマホアプリ方式を採用することにした。

OTP アプリは事前に次のようにして設定する。

1. PC から Web ブラウザで IDaaS-Y にログインする。
2. IDaaS-Y の OTP アプリ初期設定用の QR コードを表示する機能にアクセスし，OTP アプリ初期設定用の QR コードを表示させる。
3. ①当該 QR コードを OTP アプリで読み込む。

【Q】

(1) 本文中の下線①について，QR コードに含まれ，OTP アプリが OTP の生成に使用する情報を，解答群の中から選び，記号で答えよ。

解答群

ア　cookie	イ　シェアードシークレット
ウ　シリアル番号	エ　タイムスタンプ
オ　ディジタル署名	カ　フィンガプリント

「イ（シェアードシークレット）」

「設問1（1）は，正答率が低かった。知識として知らなくとも，ワンタイムパスワード生成に求められる要件から，QRコードには第三者に推測されない秘密情報が含まれている必要があると考えられれば解答できる問題であった。」（『採点講評』より）

※ RFC 6238（TOTP：Time-Based One-Time Password Algorithm）の用語。正直，知らんかった。

TLP：WHITE

R02 SC午後Ⅱ問2 その②

JP-RISSA 情報処理安全確保支援士会

午後Ⅱ問2 設問1（2）

テレワーク環境を検討中のE社が採用した**認証の方式「スマホアプリ方式」では**，「OTP（注：ワンタイムパスワード）表示用のスマホアプリケーションソフトウェア（以下，**OTPアプリ**という）**を利用する**。OTPアプリはTOTP（Time-Based One-Time Password Algorithm）に従ってOTPを表示する」。
次ページ，「**OTPアプリ初期設定用のQRコードを表示する機能へのアクセスは**，E社の利用者IDでログインするときには，②E社のネットワークからのアクセスだけに制限することにした」。

【Q】下線②について，E社のネットワークからのアクセスだけに制限しなかった場合，OTPについてどのような問題が起きると考えられるか。起きると考えられる問題を30字以内で述べよ。

「第三者のOTPアプリで不正にOTPを生成される。（24字）」

※ 下線②の「**E社のネットワークから**のアクセス」は，「**E社の“社外の人が立ち入れない場所にある”ネットワークから**のアクセス」だと読み替えましょう。
本問のQRコードを，社外のテレワーク環境（例：どこかの喫茶店）で表示させつつモタモタしていると，**傍で見ていた攻撃者がスマホにいち早く取り込む**事によって，認証の初期設定をヤラレてしまいます。

TLP：WHITE

R02 SC午後Ⅱ問2 その③

JP-RISSA 情報処理安全確保支援士会

午後Ⅱ問2 設問1（3）

図2（SaaS-XとIDaaS-Yとの認証連携）「OpenID Connectの認可コードフロー」

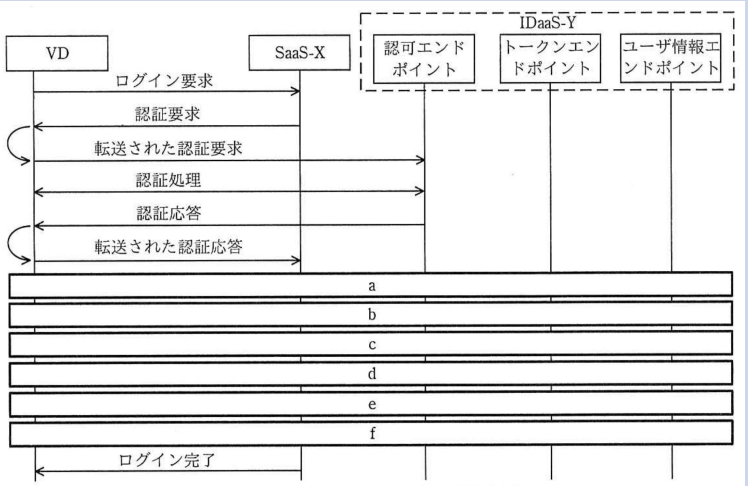


図2　SaaS-X と IDaaS-Y との認証連携

図3（会議ツールZとIDaaS-Yとの認証連携）「Implicitフロー」

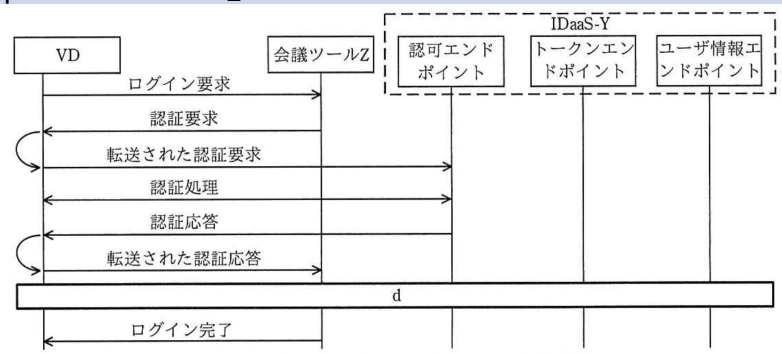
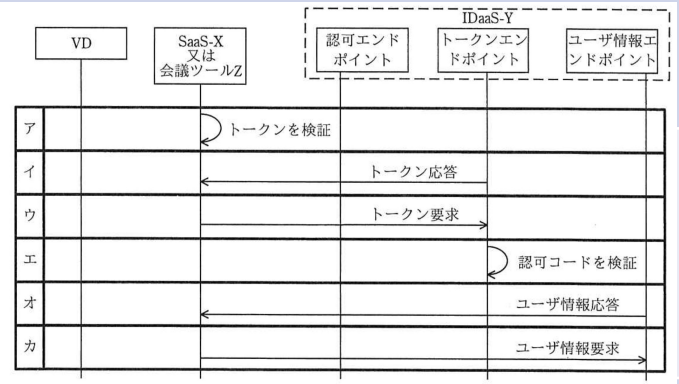


図3　会議ツールZとIDaaS-Yとの認証連携



【Q】図2及び図3中の［　a　］～［　f　］に入れる適切な通信メッセージ又は処理を，解答群の中から選び，ア～カの記号で答えよ。

【a】「ウ」，【b】「エ」，【c】「イ」，【d】「ア」，【e】「カ」，【f】「オ」

「設問1（3）は，正答率が高かった。発行された秘密情報（トークンや認可コード）をどのタイミングで検証すれば認証の安全性が担保されるかがよく理解されていた。」（『採点講評』より）

※ UMLの「シーケンス図」の読み方の基礎知識があれば，あてはめて解けます。

TLP：WHITE

R02 SC午後Ⅱ問2 その④

JP-RISSA 情報処理安全確保支援士会

午後Ⅱ問2 設問2

E社のテレワーク実証実験環境では，**仮想デスクトップ（VD）と「ノートPCとの間でクリップボード及びディスクの共有を禁止する**ように（注：VD基盤である）DaaS-Vを設定することにした。Gさんが設定してみたところ，**ノートPCからは，VDの閲覧，キーボード及びマウスによる操作，並びにマイク及びスピーカによる会話しかできなくなる**ことが確認できた。**しかし，この設定であっても**③利用者が故意に社内情報を持ち出すおそれがある。**これについては，簡単には技術的対策ができない**ので，利用規程で禁止することにした」。

【Q】下線③について，ノートPCを介して持ち出す方法を30字以内で具体的に述べよ。

「社内情報を表示した画面をカメラで撮影するという方法（25字）」

午後Ⅱ問2 設問3（1）

E社のテレワーク実証実験で貸与する「**ノートPCについては，自由なWebアクセスを許可した場合**，マルウェアに感染するリスク，及び**利用者が**（注：**ノートPCを端末とする「仮想デスクトップ」の略**である）**VDを利用中に**④マルウェアが社内情報を取得して持ち出すリスク**が高くなる**」。

【Q】下線④について，マルウェアが社内情報を取得する方法を35字以内で具体的に述べよ。

「社内情報を表示した画面のスクリーンショットを取るという方法（29字）」

※ 答の軸に “絵的にパクる” を据えさせる出題が，たまたま2問続くのは珍しい事です。

TLP：WHITE

R02 SC午後Ⅱ問2 その⑤

- すみません。設問3（2）については，村山がどうにも納得できていないため，飛ばさせて下さい。　（そんな奴のセミナーなんて）うそやで～

© あfろ・芳文社／野外活動委員会

午後Ⅱ問2 設問3（2）

すリスクが高くなる。そこで，それらのリスクを低減するために，MDM-W では，ノート PC から T 環境へのアクセスだけを許可し，⑤T 環境内のアクセスも必要最小限にする設定を行うことにした。

【Q】

(2)　本文中の下線⑤について，T 環境内のアクセスも必要最小限にする場合，許可するアクセス先を解答群の中から全て選び，記号で答えよ。

ア　DaaS-V	イ　EDR-U	ウ　IDaaS-Y
エ　MDM-W	オ　SaaS-X	カ　会議ツール Z

「ア，ウ，エ」

「設問3（2）は，正答率がやや低かった。ノートPCからアクセスするクラウドサービスと，仮想デスクトップからアクセスするクラウドサービスを混同した解答が散見された。」（『採点講評』より）

TLP：WHITE

R02 SC午後Ⅱ問2 その⑥

JP-RISSA 情報処理安全確保支援士会

午後Ⅱ問2 設問4
E社は，各**クラウドサービスプロバイダに「サービスの基盤についての脆弱性検査を実施させてもらえないか確認した。**そうしたところ，（略）利用者による脆弱性検査は，**サービス提供に影響を及ぼすおそれがあるので許可していない**との回答だった。そこでF次長は，**脆弱性検査を**⑥別の方法**とヒアリングで代替する**ことにした」。
【Q】下線⑥について，どのような方法か。35字以内で述べよ。
「セキュリティ対策についての第三者による監査報告書で確認するという方法（34字）」

※ この設問，村山は「ISMS等の認証の取得状況や，定期的に監査を受けているかを確認する。」と書きました。これは，**認証を受けるには第三者的な視点からの監査も必要なため**です。

TLP：WHITE

R02 SC午後Ⅱ問2 その⑦

JP-RISSA 情報処理安全確保支援士会

午後Ⅱ問2 設問5

E社が利用する「**IDaaS-Yが対応している2要素認証**について調査した。（注：**現在利用中の**）**パスワード方式による認証に追加可能なもの**は次の4方式であった」。内一つ，本問で採用する「スマホアプリ方式」は，「OTP表示用のスマホアプリケーションソフトウェア（以下，OTPアプリという）を利用する」。
2.0ページ略，仮想デスクトップ（VD）の基盤である「DaaS-Vの利用時は，**IDaaS-Yによる2要素認証に加えて，クライアント証明書によるデバイス認証をDaaS-Vで行う**ことにした」。
2.7ページ略，「仮に**DaaS-Vのフィッシングサイトで，利用者の入力が詐取されたとしても，その情報を悪用した不正アクセスは**⑦検討済みの他の対策**で防止できる**ので，（注：VDの端末として使う）ノートPCのアクセス先制限を緩和することにした」。

【Q】下線⑦について，該当する対策を本文中の用語を用いて35字以内で述べよ。

「DaaS-Vでのクライアント証明書によるデバイス認証（26字）」

※ 設問に「**本文中の用語を用いて**」と指定されていたなら，「**本文中の言葉を，できるだけ丸パクリせよ。」へと読み替えてOK**。
なお，検討済みの対策のうち「**OTPアプリ」は不正解**。OTPアプリの表示値も，利用者が入力するものの一つ。本問は，「これらの入力を詐取されても残る，最後の砦，とは？」を問うています。

TLP：WHITE

R02 SC午後Ⅱ問2 その⑧

JP-RISSA 情報処理安全確保支援士会

午後Ⅱ問2 設問6（1）

「ノートPCの盗難・紛失時の情報漏えい対策としては，**OSに搭載されたディスク暗号化機能**を使えばよいのではないでしょうか。」に対するF次長の回答は，「紛失した**ノートPCを第三者に取得されたときに，［ g ］されてディスクが復号されてしまう**おそれがある。（略）PINコードを利用したログイン方式を強制した場合を考えてみよう。（略）正しいPINコードが入力された場合，ディスクが復号される。」等。

【Q】空欄に入れる適切な字句を，20字以内で述べよ。

「パスワードの推測によってログイン（16字）」

※ 本問の場合，**「ディスクを抜き取って解析」は，バツ**。これを答えてしまうと，空欄gに続く**「PINコードを利用したログイン方式」の話と，辻褄が合いません。**

TLP：WHITE

R02 SC午後Ⅱ問2 その⑨

JP-RISSA 情報処理安全確保支援士会

午後Ⅱ問2 設問6（2）

「ノートPCの盗難・紛失時の情報漏えい対策として」，「**PINコードを利用したログイン方式を強制した場合**を考えてみよう。（略）正しいPINコードが入力された場合，ディスクが復号される。今回，⑧PINコードは，6桁の数字とし，システム管理者が事前にランダムなものを設定することにしよう。（略）誤った入力が5回連続で行われると管理者が回復用のパスワードを入力しない限りログインできなくなるように設定し，**回復用のパスワードには推測困難な十分に長いランダムな文字列を設定する**方法もある」。

【Q】下線⑧について，利用者に設定させるとどのような問題が起きると考えられるか。起きると考えられる問題を25字以内で具体的に述べよ。

「容易に推測可能なPINコードを設定する。（20字）」

「設問6（2）は，正答率がやや高かった。利用者に秘密情報を設定させるリスクがよく理解されていた。しかし，本問中ではPINコードとパスワードが明確に区別されていたのにもかかわらず，PINコードとパスワードを取り違えた誤った解答も散見された。」（『採点講評』より）

※ 一方，**村山は「利用者の死去等により二度とログインできなくなる」と答えました（バツ）。なぜ，そう答えた？**→ 本問のように「ユーザはヘンなことをやらかすものだから，管理者側がキッチリ管理してあげないといけない。」という，**上から目線で答えさせる出題は，10年ほど前に多かった出題パターン**。昨秋それが復活したわけですが，**村山は「21世紀も令和トゥーに，ここまでユーザをバカにする出題もなかろう。」と考えたのでした。この賭けは，失敗でした。**
では，**村山解答がバツである，その根拠は？**→ 下線⑧の後に「**管理者が回復用の（注：十分に長い）パスワード」を使えば復旧できる**旨が示されているため。**村山は，ここを見落としていました。**

TLP：WHITE

R02 SC午後Ⅱ問2 その⑩

JP-RISSA 情報処理安全確保支援士会

午後Ⅱ問2 設問6（3）

E社のテレワーク実証実験環境での，仮想デスクトップ（VD）へは「貸与するノートPCからだけログインできるようにする。」という「要件3への対応として，（注：**VD基盤である**）**DaaS-Vの利用時は**，IDaaS-Yによる**2要素認証に加えて，クライアント証明書によるデバイス認証をDaaS-Vで行う**ことにした」。
2.9ページ略，「二つ目の要望（以下，要望Xという）」は，「持込端末のインターネット接続が禁止されている顧客を訪問した際は，VDにアクセスできない。そこで，会社を出た後，訪問前にファイルサーバ上の営業資料をノートPCにダウンロードしておき（略）」。この「要望Xを実現すると，ノートPCに対する盗難・紛失時の情報漏えい対策が必要になる」。
0.7ページ略，「検討の結果，要望Xには原則として対応しないが，希望者には個別に申請してもらい，⑨申請が許可された利用者のノートPCについては，E社のネットワークとのインターネットVPNでの接続を可能とする方針にした」。

【Q】下線⑨について，DaaS-Vへのアクセスと同等のセキュリティを実現するためには，FWのVPN機能にどのような仕組みが必要か。必要な仕組みを30字以内で具体的に述べよ。

「クライアント証明書によるデバイス認証を行う仕組み（24字）」

※ 本問は「午後Ⅱ」のラスボスのくせに，割とアッサリと答が書けるものでした。

TLP：WHITE

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#3　1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

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