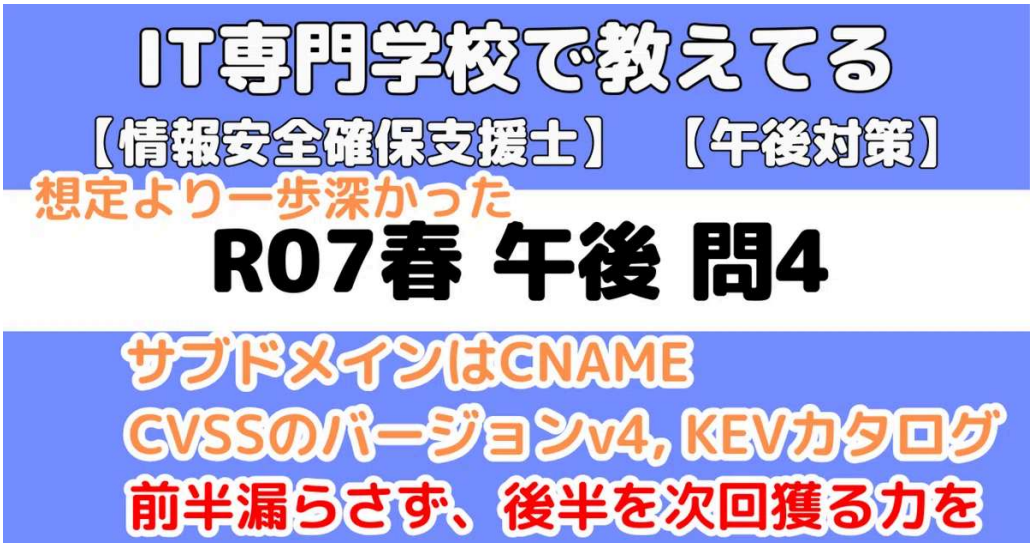
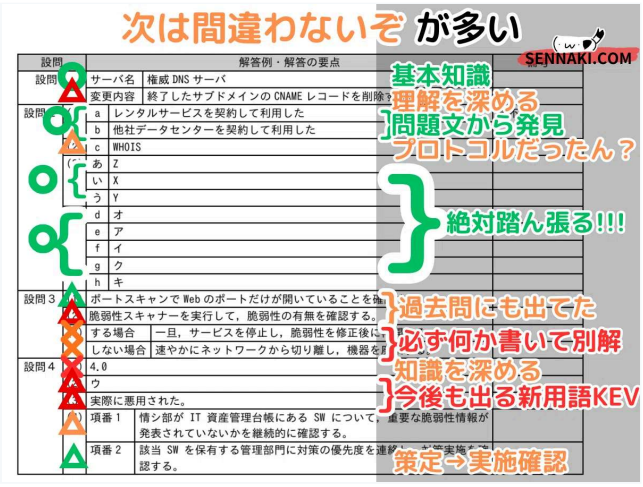


【登録セキスペ】令和7年春午後問4の解説（情報処理安全確保支援士試験）

せんない
2025年8月29日 06:45

このNoteでは「セキスペ令和7年春午後問4」の解説をします。

ネットワーク系なので、私の主軸です。とはいえ、今回は複雑でした。中盤設問2(2)(3)をミスると詰みます。



後半戦は△×判定が多くなりましたが、人に依ります。私は過去問に出た解答に強く、用語の詳細（CVSSのバージョン, KEV）に弱いです。

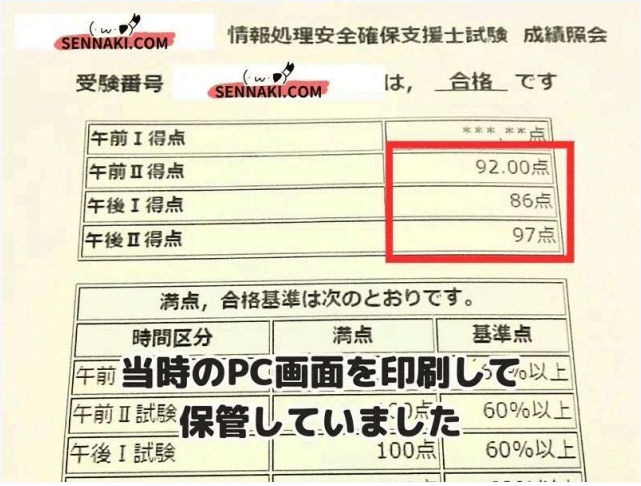
今回の学びでは、問題文に記載なくても「ポートスキャン」**「脆弱性スキャナー」**を発想して良いのも分かりました。

過去問演習としては、前半を落とさず、後半に粘れる/次出たら仕留める、方向がチェックポイントです。

PG系の問2, 3がメチャクチャキビシイです。1つでも安定&6割を切らない問題を作る必要があります。私の場合はネットワーク系問題。

このNoteが合格安定化の参考になったら嬉しです。

私はSCPMIIを97点で独学合格し、IT専門学校で授業しています。このNoteには、授業で教えていること以上の情報を詰め込みました。



それでは始めましょう！

※このNoteは2025秋本試まで全編無料公開します。本試以降は有料マガジンに組み込まれます。従来はXリポスト割引をしましたが、リポストを即消すなど、ココロを踏みにじる悪質な行為があるため取りやめました。どうぞご容赦ください。

＞午前2対策Noteのリスト

【SC：92, 86, 97点の学習ノート】ガチ勢の登録セキスペ合格勉強法（情報処理安全確保支援士試...

このNoteには、私が情報安全確保支援士（登録セキスペ）で午後II 97点を取るに至った経緯をまとめました。残念ながら「たった1ヶ月で」「最速で」合格する方法はありません。「絶対に合格したい！」なら、このNoteに書かれた勉...

♡ 45

せんない
2024/05/01 06:29

▼ 目次

すべて表示

設問1 | 外部向けは権威サーバ, 内部向けはキャッシュサーバ

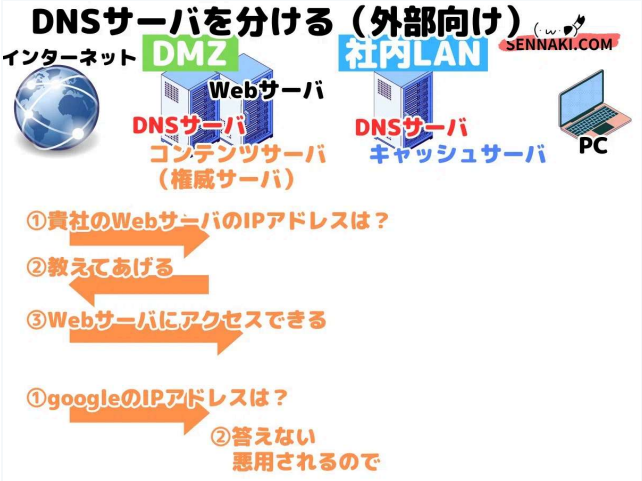
模範解答は、
「権威DNSサーバ」
「終了したサブドメインのCNAMEレコードを削除する」
サーバ名は必ず正解してください。

下線①までの話の流れは「CDN事業者のサービスを利用して～**解約**した経緯がある」。これは少し上（表1下）のニュース「(2)著名な会社が～CDNサービスを**解約**した」と状況が同じ。その後「～サービスサブドメインが海外の会社の広告サイトとして使われ」るリスクに。

サブドメインの取り扱いを改善したい、と考え至ります。

下線①「図1中のサーバ」は沢山ありますが、サブドメインと絡むのはDNSサーバ。

> **外部の人に「名前解決：ドメイン→IPアドレス」をするのは「権威サーバ」。**
> **「コンテンツサーバ」と云うことも。**



＞【AP】12種類のサーバ配置Note

変更内容のCNAMEは難しいでした。

私の解答は「AレコードのサブドメインのIPアドレスを、公開Webに変更」29文字。×だと思います。

CNAMEは「別名」のイメージが強い。
＞「SC, NW」DNSレコードのNote
＞【NW-AM2】DNSのNote

サブドメイン対応もするとは知りませんでした💦 てっきりAレコードで解決するものだと。サブドメインを書くか、後方一致とかあるのかなって。

今回で**「別名（エイリアス）・サブドメイン→CNAME」**と心に刻みました。＞参考web（株式会社ラクスライトクラウド）

設問2(1)ab | キーワードを探し、アレンジを真似る

模範解答は
「レンタルサービスを契約して利用した」
「他社データセンターを契約して利用した」
必ず正解してください。問題文に答えがあるので。

> **空欄「2つ」は問題文に答え/ヒントがあるはずです。**なぜならノーヒントで2つはハードルが高すぎるので。

> 空欄が1つなら、ノーヒントもあり得ます。流行の新技術・自分で想像・日常生活から考え出します。**＞長文問題を解く６つのテクニック（６）**

探すものを明確にします。図2では空欄aもbも「公開IT資産」。しかも「未登録の」。

「公開IT資産」とは、表1「IT資産管理」の3「インターネットからアクセス可能な全てのIT資産」。

図2に既に書かれていた「クラウドサービスを契約している公開IT資産」は表1-5(3)、同じく「他社データセンター」「レンタルサービス」もあり「IT資産管理台帳に登録していない」。

ちょうど2つあって空欄a,bの候補。

あとは図2の**クラウドサービスと同様にアレンジ**「を契約して利用した」を追加したら、模範解答の出来上がり。

設問2(2) | WHOISはプロトコル？

正答は「WHOIS」
今後は必ず正解しましょう。

試しに「google.co.jp」を入力してみてください。＞WHOISデータベース

私は、空欄c前に「プロトコル」と書かれていたので直結しませんでした。WHOISは「サービス」ってイメージが強かったです…。設問1の「サブドメイン→CNAME」といい、まだまだ甘かったです。

DNS周りのコマンド/プロトコル

WHOISのついでにDNS絡みの**コマンド「dig」**を補強。

DNSサーバに名前解決（ドメイン→IPアドレス）を依頼したり、A/MX/NSなどの情報を入手します。
＞wikipedia
＞参考Web（IIJ社）

ただし、digはプロトコルではないので、今回は不適切。digはコマンド（プログラム）で、使っているプロトコルはTCPとUDPです。

同じく、DNSプロトコルはUCPでもUDPでも通信できます。

FWのフィルタリングルールや、netstatコマンドでTCP/UDPのどちらを指定するかが問われることがあります。

> digコマンドやDNSプロトコルはTCP/UDPの両方が使えるので珍しい印象。普通はHTTPはTCP, NTPはUDPのように、片方だけ使う印象が強いです。

＞【NW-AM2】DNSのNote
＞【SC】DNSECのNote
＞【SC, NW】DNSレコードの全てNote

設問2(3)(4) | 図で可視化＋ほころびを見つける

正答は、
「Z」「X」「Y」
オ, ア, イ, ク, キ
全問正解できます。合格の踏ん張りどころ。

図3上のFリスト作成に必要な情報9個を得る、サービスとワードを描きだしました。検索ワード（緑帯）が特定できましたが、足りない繋がりがも表3〜5から追加（青矢印）

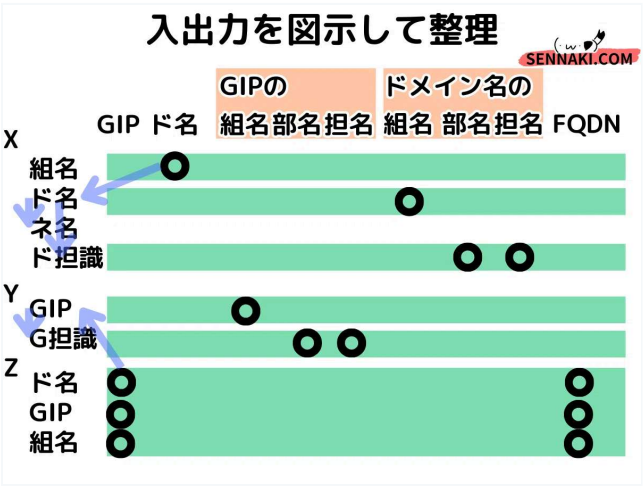
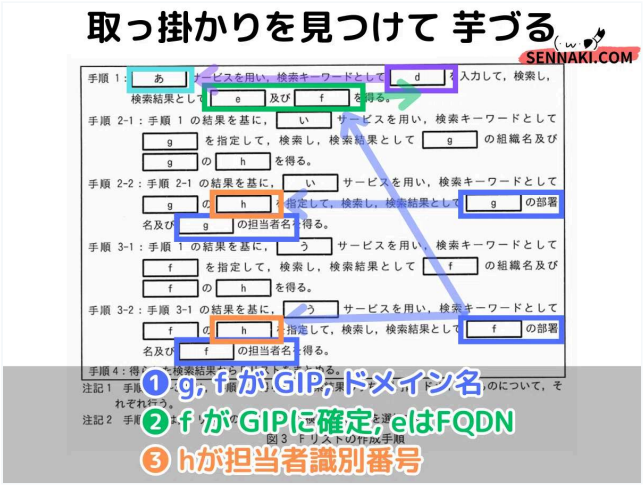


図3の空欄まみれに、取っ掛かりを探します。色んな考え方/道があるので、参考までに。

gとfから紐解きました（青）。
「gの部署名及びgの担当者名」
「fの部署名及びfの担当者名」
で共通しているので
gにGIP/ドメイン、fにGIP/ドメイン。特定はまだ。



緑：fだけが手順1に表れます。さらにeが手順1以外に表れません。よってeが「FQDN」と決まり、fが「GIP」に確定。「あ」が「Z」。

fが「GIP」だったので、gは「ドメイン名」。

fとgが確定したので、f「GIP」絡みの「う」が「Y」。g「ドメイン名」絡みの「い」が「X」。

青→橙。「gの部署名及びgの担当者名」「fの部署名及びfの担当者名」を求めるには「担当者識別番号」が必要なので、h確定。

紫。一番最初に何を検索するか。Zサービスでドメイン名/GIP/組織名のどれか。Zは図3上のB部長「当社が管理すべき公開IT資産をできるだけ多くリストアップ」より、組織名＝選択肢の「V社」と確定。

ドメイン名だと他のドメインを取っていたら漏れます。GIPも同じく漏れます。

他にも、図3注記1の手順2-1～3-1が「.jp」ドメインに限定しているので、表3注記2のXサービスの制限とも一致。少なくともXを手順1「あ」で使わないだろうと。

Zサービスは有償（表3上）、色々「全て」出力される（表5注記）ので、初手「あ」が良いかなと。目星もつけられます。

解説が文章だけでキビシかったですが、図示も難しいでした。ぜひご自分でも描いてみて考えてみてくださいね。お手数おかけします。

設問3(1) | 今まで問題文に書かれていたことを発想&言語化

模範解答は「**ポートスキャン**でWebポートだけ開いていることを確認する」。
発想できるようになって下さい。Iパスから馴染みあるので。

下線②「X, Y, Zサービス以外の調査」なので、「調査」をキーワードに**問題文を探しますが、見つかりません。ノーヒント問題と判断。**

私が注目したのは「**Webだけが**稼働している」と分かった点。他サービスも調査したからこそ、Webだけと判断したのかな→色んなサービスの稼働を調査する→ポート番号、と発想しました。

設問3(2) | 今まで問題文に書かれていたことを発想&言語化

模範解答は「**脆弱性スキャナー**を実行して、脆弱性の有無を確認する」。今後正解していきたいです。

脆弱性スキャナーは、Webアプリやサーバ/ネットワーク機器に脆弱性があるかを検索するツールです。
＞参考Web（IBM社）
＞wikipedia

他の過去問でも「診断ツール」などの言葉で出てきました。ポートスキャンや脆弱性スキャナーによるセキュリティテストも、今後はすんなり発想できるようになりたいですね。

設問3(3) | 何ならかの「伝わる解答」をする

模範解答は
継続「一旦、サービスを**停止**し、脆弱性を**修正後に再開**する」
廃止「**速やか**にネットワークから**切り離し**、**機器を廃棄**する」
何らかの解答はしてください。白紙はダメ。

模範解答は、読めば理解できます。しかし問題文をヒントに組み立てるよりは、セキュリティの一般的な作業でした。

本試験の動作で、解答を組み立ててみます。

問題文に方針や手順が書かれていないか探します。

結構探しました。表1の1頁目上段6「IT資産の廃棄は管理部門が実施し、その際に、管理部門がIT資産管理台帳を更新する」。

40文字なので35文字制限に対応して**「廃棄し、IT資産管理台帳を更新する」17文字。**模範解答に半分は似ました。本試験ではこれぐらいが限度でしょう。

どこかでノーヒントと考えるべきだった

私の解答はダメかも。
継続「運用について情シ部に相談して**必要な処置**をする」22文字。
廃止「**W社**にドメインv-sha.g.jpの廃止を依頼する」25文字
正解になるかは分からないです。

継続について。G事業の忘れ形見なので、K事業部は利用してない点に注目し、表2のK-4「利用が終了した公開IT資産について、**必要な措置**を漏れなく行う」を使いました。

しかし設問文の「具体的に」には不足かな。

廃止について。表6のFQDN「sub1.v-sha-g.jp」が、表1下段-1(1)「v-sha.co.jp」と違います。現在使ってないならドメインを廃止すべきと考えました。

更に表1下段-1(1)に「ドメイン名を～W社から取得」とあるため、ドメインの取得/廃止を依頼できると判断。

メタ読みすると、この部分は今までの設問でもヒントとして使われていないため。この問題で使うんじゃないかなと。**＞長文問題を解く６つのテクニック（３）**

以上のように、問題文を使った解答が前提です。

しかし模範解答に至るには、どこかで「これ、ノーヒント問題だな。まずは一般的な対処で書いてみるか」の判断が必要でした。**＞長文問題を解く６つのテクニック（６）**

難しい判断です。過去問演習を通して身に着くセンスですが、今回私は見切れませんでした。

設問4(1) | 今回で少し深く覚える

正答は「4.0」
仕方ないです。でも今回で**「v4.0」**や管理団体**「FIRST」**を覚えればOK。今まで**「脆弱性の深刻度」**程度でしたが、少し深く必要になったみたい。

私は恥ずかしながら知らなかったので、問2に「CVSSv3」とあったので採用しましたがダメでした。

CVSS v1.0 2005年
CVSS v2.0 2007年
CVSS v3.0 2015年
CVSS v3.1 2019年
★**「CVSS v4.0」** 2023年
★**「FIRST」**が管理も覚えておきますか。
＞wikipedia（英語）

直近は4年で更新なので、2027以降ですかね。v5の情報も確認できませんでした。しばらく安泰。

CVSSの兄弟たちも復習。IパスやFEにも出てましたね。

- **CVE**：脆弱性**識別子**。つまりID
- **CWE**：脆弱性の**種類**。つまりカテゴリ
- **CVSS**：脆弱性の**深刻度**
  ※4文字なので一番「深い」と覚えてます。

＞【SC】平成30年秋午後1問3設問2aの解説Note
＞【SC】平成30年秋午後1問2設問1deの解説Note

設問4(2)(3) | おそらく今後の流行語

正答は
「ウ」
「実際に悪用された」

> **「KEVカタログ」**は**「実際に悪用された脆弱性のリスト」**。**「CISA」**が管理。
> 2021年から掲載が始まったので今後も新用語/流行語として出題されるでしょうね。
> ＞参考Web（NES社）
> ＞参考Web（CISA）

勘でも良いですが、自分なりに理屈を付けて解答した方が後悔がないと思います。

私は英語から推測しました。

Exploitedは、**「エクスプロイトコード」「Exploit攻撃」**で見た言葉なので攻撃的だな連想。Exposureは、カメラを少し触ってると「露出（露光）」と知ってるかも。

Exploit攻撃（エクスプロイト攻撃）：OSやソフトウェアの脆弱性/バグ/不具合を利用したプログラムによる攻撃。**＞SC平成24年春午後1問2設問2(1)gの解説Note**

Key（キー, データベース的？）かKnown（既知）なら、Knowだろうと。既知だからカタログになっているんだろうなと。Keyを選ぶ可能性もありましたが。

困ったら時は流行語も

たぶん「KEVカタログ」は今後も出るので、流行語リストに追加しました。

セキスペの最後に「改善するにはどうすれば良いか」と問われた時、まったくヒントがない/分からない時に役立ちます。

- **ゼロトラスト**：従来の境界防御（FW）ではなく、情報への**全アクセスを信頼せずに疑う**
- **SIEM**：**各機器のログを収集**・分析し管理者に通知

- **CASB**：各社員の**クラウド利用の可視化**
- **EDR**：端末を監視し異常や不審な動きがあれば、**ネットワーク切断・プロセス終了**
- **DLP**：**機密情報を自動的**に特定し、送信や出力などを**検知しブロック**
- **KEV**カタログ：**実際に悪用された**脆弱性のリスト
  ※**今回のNoteで追加！！**

改善が実現できそうなら解答に使ってみて下さい。採点者が「それもあり得るね」と思えば正解にしてくれますよ。**＞SIEMやCASBなど流行語Note**

設問4(4)項番1

模範解答は「情シ部が**IT資産管理台帳にあるSW**について、重要な脆弱性情報が発表されていないかを継続的に確認する」

表2のK-3「脆弱性を事業部が修正したどうかを情シ部が確認できるように」、表1の脆弱性管理の項番1「**サーバに導入したSW**の脆弱性情報は、情シ部が脆弱性ニュースを毎日みて確認」。

「サーバに導入したSW」だったのを「IT資産管理台帳にあるSW」に拡張した話。

表1はIT資産管理台帳に抜けがあった時期の方針。それを改善したので（図2の3種の資産, 設問2(1)ab）、ニュースを探す対象範囲も広げています。

なかなか気づかないかなと。文章も表も長くてもう頭ゴチャゴチャですから。

設問4(4)項番2

「担当SWを保有する管理部門に対策の優先度を連絡し、対策**実施を確認する**」。これは正解しましょう。

表2のK-3「脆弱性を事業部が修正したどうかを情シ部が**確認**できるように」、しかし表1の脆弱性管理の項番2「脆弱性情報を全部門に連絡」まで。連絡して終わりではなく、**修正したか確認**したいと分かります。

私の解答は「各部門から連絡した脆弱性への対応状況の報告を得る」24文字。投げっぱなしではなく、監督/把握もと。

まとめ

お疲れ様でした！

図3の穴だらけが異彩放ってました。またCVSSのバージョン・KEVの英語・サブドメインとCNAMEなど、想定の一歩先の知識が要求されました。

本試験では、図3の穴だらけでも選ぶぐらいの自信、後半の知識/過去問/作文を拾っていく粘り強さが必要でした。今回がボロボロでも、次回は得点していけるよう、もう一度教科書・最新情報をチェックするのが必要かもしれません。

以上になります！

＼私の3ヶ月の学習履歴／

【SC：92, 86, 97点の学習ノート】ガチ勢の登録セキスペ合格勉強法（情報処理安全確保支援士試...

このNoteには、私が情報安全確保支援士（登録セキスペ）で午後II 97点を取るに至った経緯をまとめました。残念ながら「たった1ヶ月で」「最速で」合格する方法はありません。「絶対に合格したい！」なら、このNoteに書かれた勉...

♡ 45

せんない
2024/05/01 06:29