

IT専門学校で教える 【情報安全確保支援士】 【午後対策】 全122頁の資料から出題

R07春 午後 問2

ブラインドSQLインジェクション
CVSS基本値/現状値/環境値, EPSS値
きっと出る SVCC, NVD, CPE, SWID

【登録セキスペ】令和7年春午後問2の解説 (情報処理安全確保支援士試験)



せんない

2025年9月1日 12:10

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。

リスク値計算なのでSGを解いたことがある方は馴染み深いかも。この問題は、[IPA資料（全122頁）](#)に沿っているのが特徴です。

従来の解法は、まだまだ有効ですが割合は減りました。

- 問題文からヒントを探す基本解法：設問5(3)
[>長文問題を解く6つのテクニックNote（1）](#)
- 過去問経験が生きる：設問3(2)(3)
[>長文問題を解く6つのテクニックNote（6－4）](#)

一方「難易度ラインを引き上げるぞ」とメッセージ性の強い問題。従来はもう少しヒントを書いてくれてましたが、解答から少し遠めに控えられました。

- 深い理解/想像が必要
 - ：設問1, 設問2, 設問4
- 用語/仕様の知識が必要
 - ：設問3(1), 設問5(1)(2)



印象は、本試験でも実力が出せれば6割は切らない。設問6は救済策かなと。

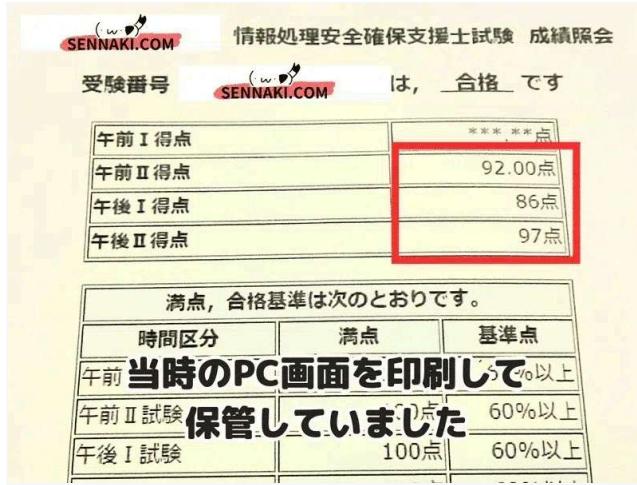
一方「今後は浅めのヒントに控えるぞ」「CVSS現状値やEPSSも出すからな」という布石ビンビン。このNoteでは、[IPA資料（全122頁）](#)に沿って解説しつつ、問題にでなかった内容も今後のためにピックアップしました。

今後はこれぐらいが当たり前、になります。過去問演習をしたら、9割以上まで高めるのは勿論、備えて広め深めに調べるのも「不意打ち」封じに重要になってきます。

この問題の復習は、かなり気合入れて取り組んで下さい。何回に分ける/何周かする必要があります。

このNoteで、学習品質の底上げを感じられて頂けたら嬉しいです。

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



undefined

▼ 目次

マーキングしていないなら力不足

講座 | SQLインジェクション

設問1 | 芋づる失点

深める | 「」の小細工の意味

講座 | ブラインドSQLインジェクション

設問2fg | 問題文にヒントないなら、少し想像する

設問3(1) | 事前察知するか呑むか

問2を選ぶ前に察知する

知らない用語に「へ理屈」で解答する

出題実績 | PFS (完全前方秘匿性)

すべて表示

マーキングしてないなら力不足

問題文1頁目（10頁）の以下にマーキングしたでしょうか？

わざわざ「任意である」「評判ある」なんて見逃せないです。

- ・ 「初回リリース後の両診断の実施については**任意である**」
→診断してなからたら不具合出るに決まってる
- ・ 「重要サイト以外に対する両診断の実施は**任意である**」
→診断してなからたら不具合出るに決まってる
→サイトXは重要サイトでないから問題発生（10頁）
- ・ 「P社のWebアプリ診断は、脆弱性が実際に悪用できることを確認した上で報告してくれるので、**評判がよい**」
→使う根拠。理由を聞かれる問題ができるかも（設問5(3)）

マーキングしてないなら長文基礎力が足りないかも。[>長文問題を読む6つのテクニックNote（6-3）](#)

講座 | SQLインジェクション

設問1のために、まずSQLインジェクションの復習をします。[> 7 3種類の攻撃手法Note \(SQLインジェクション\)](#)

通販サイトのように、Webで利用者が入力した値でデータベース検索をするシステムの話。入力した値をSQL文に組み込んで、データベースにアクセスします。

下図では「ペン」が入力され、SQL文に「ペン」が組み込まれて、データベースから商品名がペンである行の全列が表示されます。



SQLインジェクションは、入力値を小細工してデータベースから情報を抜き出します。

上図（赤）では、`1=1`が常に真、`name=ペン`と`or`で繋がっているので、商品名がペンでない（偽）であっても、`WHERE`句は常に真になります。データベースの全ての行で真なので、データベースの全行の全列が表示されてしまいます。

[> 7 3種類の攻撃手法Note \(SQLインジェクション\)](#)

設問1 | 芋づる失点

正答は

- a : ア (コンテンツがありません)
- b : ア (〃)
- c : ア (〃)
- d : ア (〃)
- e : イ (コンテンツが表示される)

難しい人には難しいです。ここで引き返すのはアリなので、半分も分からなかったら別問題へ。

図1に見逃せないルールが2つ。これ見逃すと大失点です。

- 「コンテンツ番号がDBサーバ上に存在しない場合、又はSQLが構文エラーになる場合は、"コンテンツがありません"というメッセージを返す」
- 「articleの値は～数値型」

表1の処理結果は以下の通り。

GETを受けてSQLを作る

SENNAKI.COM

https://site-x.m-sha.co.jp/info?article=20250401
SELECT url where article=20250401

https://site-x.m-sha.co.jp/info?article=20250401'
a SELECT url where article=20250401' SQL文法X

https://略/info?article=20250401'%20and%20'a='a
b SELECT url where article=20250401' and 'a'='a
'%20'はスペースになる SQL文法X

c SELECT url where article=20250401' and 'a'='b
SQL文法X

d SELECT url where article=20250401 and 1=0
SQL文法○ 1=0が偽→WHERE句が偽

e SELECT url where article=20250401 and 1=1
SQL文法○ 1=1が真→20250401次第

- a : 文法エラー。「」が1個しかなく、文字列の終端がないので。エクセルで関数の「（」があるけど「）」ないようなもの。構文エラーは"コンテンツがありません"でしたね。
- b : 文法エラー。数値の後に「」が続くため。連結するには「+」演算子が必要。なおURL「%20」は「」スペースになります。"コンテンツがありません"
- c : 文法エラー。bと同じ。"コンテンツがありません"
- d : 「1=0」が常に「偽」なので、「and」の所為でWHERE句も常に「偽」なので一切出力しない。例え「20250401」が存在しても出力しない。存在しない時も"コンテンツがありません"でしたね。
- e : 「1=1」が常に「真」、「20250401」が存在すれば出力する。なお「20250401」以外は出力されない。イ（当該コンテンツが返される）。

なおeにて「OR」にすれば、全データが出力されるはずです。「WHERE article = 20250401 or 1=1」の「1=1」が常に「真」、「OR」の所為でWHERE句は常に「真」。20250401だけでなく、全ての行が出力されます。

深める | 「」の小細工の意味

今回はarticleが数値型だったので「」の小細工をせずとも、そのまま「or 1=1」など入力すれば攻撃が通りました。結構珍しいです。

大抵の事例は文字列型に「」で小細工して攻撃を通します。せっかくなので、articleが文字列の場合を考えて見ました。

もし articleが文字列型だったら、
SENNAKI.COM

<https://site-x.m-sha.co.jp/info?article=20250401>

SELECT url where article='20250401'
両端に「」が付く SQL文法 ○

a SELECT url where article='20250401'" SQL文法 X

b SELECT url where article='20250401' and 'a'='a'
SQL文法 ○ a=aが真→20250401次第

c SELECT url where article='20250401' and 'a'='b'
SQL文法 ○ a=bが偽→WHERE句が偽

d SELECT url where article='20250401 and 1=0'
「20250401 and 1=0」って登録ある？→多分ない

e SELECT url where article='20250401 and 1=1'
「20250401 and 1=1」って登録ある？→多分ない

入力値の両端に自動的に「」が付けられてWHERE句に組み込まれるので、「」で強制的に一度切ります。

「20250401' or 'a'='a」とすれば「WHERE article='20250401' or 'a'='a」になり、全データが出力されてしまいます。

講座 | ブラインドSQLインジェクション

12頁頭に見逃せないセリフあり。「ブラインドSQLインジェクションの脆弱性に該当」。

今後穴埋め用語や説明作文に出していくと思いました。

「ブラインドSQLインジェクション」とは、SQLの実行結果が表示されなくても、応答時間/応答の可否からデータベースの構造/情報を特定する攻撃。[>参考Web \(Zenken社\)](#)

問題文12頁頭「ブラインドSQLインジェクションの脆弱性に該当する」は、表1で攻撃者がサーバの応答を観察している節から判断されました。

表1の応答では、データもエラーメッセージも出ず、応答も2種類ですが、それでも分析できる情報があるんです。

設問2fg | 問題文にヒントないなら、少し想像する

模範解答は

「新たな脆弱性が発見されたこと」
「リスクが変わったと評価し値を変えたこと」

せめて1つは得点したいですね。頑張って書きましょう。

自己採点が難しいので、模範解答の理解で留めます。

1つめ。「新たな脆弱性が発見されたこと」について。初回リリース当時に発見/認識してなかった新たな弱点が見つかること。

2つめ。「リスクが変わったと評価し値を変えたこと」について。「アップデートや設定変更をしていない」ので、ソフトウェア側の変化はありません。脆弱性の改善はなし。逆に新たな攻撃手法が現れ、リスクが高くなる（悪化）のはあり得ます。

基本解法で攻めても、問題文に、診断や変化原因のヒントはなし。想像で解答するしかありません。[>長文問題を解く6つのテクニックNote \(6\)](#)

設問3(1) | 事前察知するか呑むか

正答は「ウ（128, 曲線, 112, 鍵長）」。

知らないとどうしようもないです。私はビットは覚えないです。覚えても「128と中途半端」ぐらい。

一応論拠を紹介。

問題文表4と全く同じ記述が、IPA資料（48頁表18）下に「**鍵交換でECDHEを利用する場合には128ビットセキュリティ以上を満たす曲線～DHEを利用する場合には112ビットセキュリティ以上を満たす鍵長～**」と。

とはいって、私は覚える気ないです。

問2を選ぶ前に察知する

大事なのは【問2を選ぶ前に】この問題を察知しているか。

この問題は表1SQL（設問1）の面倒臭さ&芋づる失点、表4（設問3-1）の知らないと確実失点のリスクがあります。リスクを承知を選ばねばなりません。

解いてから「うわ難しい」「うわ知らない」で退いたら時間の無駄。退かなかつたらハンデを背負つて、もっと難しい後半戦に差し掛かります。

選択肢を半分以上知っているか、計算問題を計算できそうか、問題を選ぶ時に必ず見積もってください。>SCの時間配分/問題選び戦略Note

問題選びの際に、設問3(1)の選択肢を見て「数値覚えてるかな」「直線、曲線ってなんだ」と思い、表4の空欄h～kを見て「ECDHEとDHEの仕様覚えてない」なら、退くか呑むかを判断します。

私は設問1のSQLの面倒さと設問3(1)の仕様で、間違いなく退却します。解く前からハンデを背負い、防戦になると合格できません。ツバ迫り合いは勝ちの姿勢が大事です。

他にも、用語の選択肢問題。半分～7割は知らないと得点はキビシイです。消去法も効きません。>
SCの時間配分/問題選び戦略Note

知らない用語に「へ理屈」で解答する

知らないなりに理屈をこねます。

「ECDHE」をElliptic Curve（椭円）と推測してアとウに絞り（i=曲線）。>英単語で覚える2つの意味Note

「～ビットの鍵長は聞くけど、～ビットの署名って聞いたことあるか？」と邪推してウ（k=鍵長）。

でも模範解答を知ってから考える理屈ですね。本試では無理だろうなあ。

なお、一度出題されています（詳細は次節）。>平成29年秋午後1問3設問3(2)の解説Note

「Sならシステム、サーバー」など1文字から英単語が出るだけでも違いますよ。>英単語で覚える2つの意味Note

出題実績 | PFS（完全前方秘匿性）

「ECDHE」と「DHE」はPFS（完全前方秘匿性）として1度出題されました。>平成29年秋午後1問3設問3(2)の解説Note

PFS（完全前方秘匿性）とは、鍵交換に用いた秘密鍵が漏えいしても、過去の暗号が解読されない性質。お薦めのアルゴリズムが、DHEとECDHE。IPAの資料より

解説では更に調べて提案しました。しかし、今回は更にビットまで出ました。

- **DHE** : DH鍵。離散対数型。お互いに乱数だけを通信するだけで、共通鍵を生成できる。 [wikipedia より](#)
- **ECDHE** : DHEを楕円曲線暗号で実現
※利用方法に違いがあるため名前を変えた。 [IPA資料の20頁](#)

> [平成29年秋午後1問3設問3\(2\)の解説Note](#)

設問3(2) | 過去問頻出で、もはや基本

模範解答は「OpenSSHのログに認証タイムアウトのメッセージの出力が多数あつたらサイト担当者に電子メールでアラートを送る」。

問題文に「アラート」の記述がなくノーヒントですが、正解できるようになってください。新SCはそういうレベルになっています。

過去問に7回出ているので、必ず発想できるようになります（末尾にリスト掲載）。

13頁末～14頁頭。脆弱性は「OpenSSHのログに"Timeout before authentication"という認証タイムアウトのメッセージが多数出力」され表れ、攻撃が成立する可能性がでてくるとのこと。

ログに出力されるなら、ログをリアルタイムにチェックしてアラート（管理者にメッセージなりメール通知）すれば良いです。

模範解答は理解できますね。「OpenSSHのログに認証タイムアウトのメッセージの出力が多数あつたらサイト担当者に電子メールでアラートを送る」。

設問文に「具体的に」、しかも文字制限がないので詳しく書きます。前半は問題文そのまま流用で構いません。後半に担当者にアラートを伝える旨があればOK。

「アラート」機能が出てきた問題は以下。攻撃検知だけでなく、脆弱性テストでの一時的処置などでも出てきます。

- [> SC令和6年秋午後問1の解説Note](#)
 - [> SC令和6年春午後問1の解説Note](#)
 - [> SC令和5年春午後1問2の解説Note](#)
 - [> SC平成30年秋午後1問2の解説Note](#)
 - [> SC平成30年秋午後1問3の解説Note](#)
 - [> SC平成28年秋午後1問3の解説Note](#)
 - [> SC平成24年秋午後1問2の解説Note](#)
-

設問3(3) | 絶対に正解して！

模範解答は「クライアント認証を行う」。必ず正解してください。今までめちゃくちゃ出てきた王道手法ですから。

下線②「アクセス元のPCを認証する対策を採用した」。これだけで、すぐにクライアント認証に考え至ります。

具体的な技術手法を書いても大丈夫。問題文にクライアント認証の明記がないので、具体的にどう実装するかは採点基準ではないでしょう。

一番の代表格は「クライアント証明書」。私の過去問解説に9回も出ています（末尾にリスト掲載）。PCに証明書をどうインストールするかはさておきます。

次点は「送信元MACアドレス」。NICにハード的に刻印された世界唯一の番号なので、PCの特定ができます（USB-LANなどはさておき）。

「送信元IPアドレス」は、ギリ不正解かも。IPアドレスは変わる場面が高く、PCも特定できません。接続してくるPCが一般利用者なら尚更。また「認証」か？と言われると若干疑問。

他にも最近は「FIDO認証」もあります。ただ、生体認証の入力が必要なので、全てのPCで出来るかというと....。

でも今後「FIDO」は解答になってくるでしょうね。

クライアントを特定/制限した過去問は以下。

- クライアント証明書
 - >[令和5年午後問2の解説Note](#)
 - >[令和5年春午後1問3の解説Note](#)
 - >[平成31年春午後1問3の解説Note](#)
 - >[平成29年春午後1問1の解説Note](#)
 - >[平成26年春午後1問3の解説Note](#)
 - >[平成25年秋午後1問3の解説Note](#)
 - >[令和元年秋午後1問2の解説NoteTLS](#)
 - >[平成26年秋午後1問2の解説NoteSSL](#)
- MACアドレスフィルタリング/特定
 - >[令和5年午後問2の解説Note](#)
 - >[平成27年春午後1問2の解説Note](#)
- 送信元IPアドレス
 - >[令和6年秋午後問4の解説Note](#)
 - >[令和3年秋午後1問1の解説Note](#)
 - >[平成28年秋午後1問1の解説Note](#)
- サーバー証明書も絡む
 - >[平成31年春午後1問2の解説Note](#)
 - >[平成29年秋午後1問3の解説Note](#)
 - >[平成28年春午後1問3の解説Note](#)
 - >[令和6年春午後問2の解説Note](#)

設問4(1)WA-1 | こんなのは推測しろか

模範解答は「パラメータitemの値が容易に推測できること」

ハードル上がりましたね。ヒント量が一段減りました。

Lと評価された理由は、WA-1を調べるので、表5へ。表5脆弱性を見て、自分でもLと判断する理由を探していきます。

表5「itemの5桁の数字を変更して～本来閲覧できな商品を～閲覧」が脆弱性であり攻撃手法。

ヒントはここまで。

「itemの5桁の数字って当てるの簡単なんじゃ？」と推測して模範解答。「パラメータitemの値が容易に推測できること」

一段想像するようにハードル上がりましたね。

今までのSCだったら「推測できる」旨の匂わせがありました。例えば「itemは連番」「item=12345」など。連番なら必ず若い番号から当てていけますし、具体的な数値をみると推測できそうだとイメージできます。

なお、数字の桁が多くても「item=2025083000001」などでも、日付(YYYYMMDD)と連番5桁と分かることで推測が簡単ですね。

設問4(1)WB-1

模範解答は

- L 「発注確認機能のURLを入手する必要があること」
- H 「発注確認機能のURLが推測困難であること」

※解説のために解答順を変えました

表5WB-1より手順確認。

1. 管理者用アカウントでログイン、発注確認機能のURL入手

2. 一般利用者アカウントでログイン、発注確認機能のURLを入力
3. 管理者用画面が表示されるので、他人の発注情報が全て閲覧できた

管理者アカウントで見れる管理者用画面を、一般利用者アカウントでも見れるのが脆弱。

模範解答を理解していきます。

1つめの模範解答。「発注確認機能のURL」を入手するには「管理者用アカウントでログイン」が必要。管理者用ID, PWDが必要です。**ひょっとしたら、サーバへ管理者アカウントでログインする端末制限を社内限定にしてるかも。**なかなか困難ですね。

よって模範解答の意味は理解できます。「発注確認機能のURLを入手する必要があること」

2つめの模範解答。「一般利用者アカウントでログイン」は自分の捨て垢ですれば良いです。しかし「発注確認機能のURL」を管理者ログインなしでやるには、当てる（推測）しかなし。

URLは文字列なので文字種が多く、長いので文字数（桁）も多い。つまり推測は極めて困難。

よって模範解答の意味は理解できます。「発注確認機能のURLが**推測困難**であること」

講座 | ACの意味と別解

下線③ 「Attack Complexity (AC)」は、「攻撃」が成立する条件の「複雑さ」を意味します (IPA資料の74頁表A-2)。

- L : 特別な条件なくいつでも攻撃できる
- H : 攻撃者が条件を明らかにしないと攻撃できない

過去問に出たのでACは覚えます。

また表5の「CVSS : 3.1/AV:N~/A:N」の意味も調べます。今後出るかも。どこまで理解/覚えるかは後で判断。次節へ。

講座 | CVSS基本値の項目

表5の「CVSS : 3.1/AV:N~/A:N」などの項目を書き出しておきます。覚えるかはさておき。まずは調べて、自分で判断します。(IPA資料の74頁表A-2,A-3)

以下を自分なりに書き出して、キーワードや優先順位・覚えやすさにくさを考えてみてください。

- AV : 攻撃 「元」 区分
 - N : ネットワーク経由
 - A : 隣接ネットワーク (bluetoothなども)
 - L : ローカル環境 (攻撃者がログインする)
 - P : 物理環境 (USB経由)
- AC : 攻撃 「条件の複雑さ」
 - L : 条件なし。いつでも攻撃可能
 - H : 条件あり。条件を満たせば攻撃可能
- PR : 「必要な特権」 レベル
 - N : 特権不要。いつでも攻撃可能
 - L : 基本的権限があれば攻撃可能
 - H : 管理者権限があれば攻撃可能
- UI : 「ユーザ関与」 レベル
 - N : 不要。利用者が何もせずとも攻撃される
 - R : 要。利用者のクリック/閲覧などの操作が攻撃成立に必要
- S : 「スコープ」
 - U : 影響範囲に変更なし。
 - C : 影響範囲に変更あり（広がる）。他攻撃へ悪用されるなど。

- C : 機密性への影響
 - H : 高。機密漏えいリスクが全体に及ぶ
 - L : 低。影響は限定的
 - N : なし。影響なし
- I : 完全性への影響
 - H : 高。改ざん影響が全体に及ぶ
 - L : 低。情報改ざんは可能、しかし機密情報やシステムファイルの改ざんはできず、影響は限定的
 - N : なし。影響なし
- A : 可用性への影響
 - H : 高。リソースを完全に枯渇させ、システムを完全に停止できる
 - L : 低。リソースを一次的に枯渇、システムの遅延/一時中断ができる
 - N : なし。影響なし

最後のCIAは覚えなくて良さそうですね。完全/一時的に枯渇/妨害する程度。

AV（元）, AC（条件）, PR（権利）, UI（利用者）, S（範囲）も、2~3個は覚えられるかな。英語1文字だけでも知っていれば。UIはユーザ（利用者）、Cはコンプレックス（複雑さ）、Vはベクトル（方向→元）とか。[>IPA資料（74頁表A-1）](#)

詳しくは覚えません。CVSS v4.0ではじ色々変わるので（80頁表B-1, B-2）。せっかく覚えて出ない/変更されるなら水の泡かなと。

設問4(2) | 基本解法 似た言葉を探す

正答は「3」。

設問文「図2中の項番から選び、答えよ」なので、ヒントは図2。探す言葉は下線④より「管理者権限」。

図2に「管理者権限」の言葉なし。似た言葉で項番3に「一般利用者権限」ならあり。

Webアプリは一般利用者権限で実行されているので、管理者権限が必要な操作（コマンド、プログラム実行、ファイル操作、設定変更など）はできません。

「3」で良さそう。

講座 | CVSS値3種、EPSS値

問題にたくさんの値が出てくるので整理します。

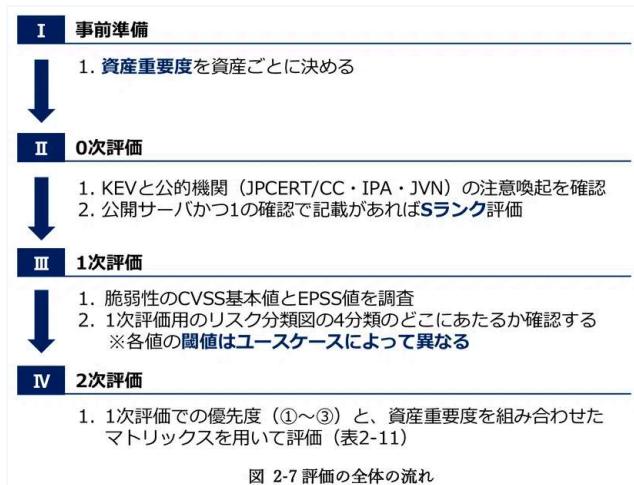
>参考Web (IPA)

>IPA資料

まずリスク評価の流れを把握します（29頁～）。

- 0次評価：脆弱性の洗い出し。「KEVカタログ」などで。
- 1次評価：「CVSS基本値」と「EPSS値」から優先度出し。
- 2次評価：1次評価の優先度と「CVSS環境値」orSSVCで。

「KEVカタログ」は、「悪用」が確認された脆弱性を掲載したカタログ。米国CISA（図1-5 21頁）。出題実績もあります。令和7年春午後問4設問4(2)(3)の解説Note



では本題。1次/2次評価に使われる値を整理します。

- CVSS

- CVSS**基本値**：脆弱性の特性の評価値。**変更されない。**
- CVSS**現状値**：脆弱性への**現在の対応状況**に応じた評価値。時間的に変化していく。外部機関が算出してれば**情報収集の手間が省ける**。算出されていない場合が多い。
- CVSS**環境値**：**利用環境**も含めて最終的な深刻度を評価する。ユーザごとに変化する値。算出に専門知識が必要。
- CVSS**補足評価基準**
※v4.0で追加。いずれ補足値と呼ばれるかも？

- EPSS**値**

脆弱性対応の優先度を判断する指標。今後30日に以内に「**悪用される蓋然性（＝確率）**」を算出。悪用された事実と可能性を考慮する。2021年から2回アプデされ現在v3。

表 2-1 評価指標の比較表（1次評価）

指標	運用リソース	内容
CVSS 基	低	外部ベンダーや公的機関が評価値を算出
CVSS 現	中	基本的に外部組織から算出されるが、実際には値が提供される場合が多くなく懸念が残る
CVSS 環	高	すべて自社での評価が必要。2次評価で活用
EPSS	低	FIRST が算出（ただし、スコアの変動あり）
SSVC	高	すべて自社での評価が必要。2次評価で活用
KEV	低	別枠で活用

今回の問題では以下の手順でした。

- 14頁：1次評価：

CVSS基本値とEPSS値から優先度を決める。図3のI～IVの優先度領域も決定

- 15頁：2次評価：

上記領域とCVSS環境値で対応

- 優先度を決定



設問5(1)CVSS現状値

現状値：「攻撃コードなどの情報を多くの公開サイトにある情報から判断する必要があるから」。知らないと無理。

問題文から「現状値」の性質（手間がらみ）を探します。遡りながら探しますがヒントなし。

残念ながら知らなければ無理です。

前節より作文するしかないです。

- CVSS**基本値**：脆弱性の特性の評価値。**変更されない**。
 - CVSS**現状値**：脆弱性への**現在の対応状況**に応じた評価値。時間的に変化していく。外部機関が算出してれば**情報収集の手間が省ける**。算出されていない場合が多い。
-

設問5(1)EPSS値

EPSS値：「FIRSTのサイトで公開されている値をそのまま使えば良いから」。知らないと無理。

問題文から「現状値」「EPSS値」の性質（手間がらみ）を探しますが、なし。

EPSSを学んでおきます。

前節より。

EPSS値

脆弱性対応の優先度を判断する指標。今後30日に以内に「**悪用される蓋然性（≒確率）**」を算出。悪用された事実と可能性を考慮する。2021年から2回アプデされ現在v3。

でも問題点も（このNoteの最後に掲載）。

EPSSは米国機関FIRSTが運営しているため、日本製品の情報が不足な面も。[\(IPA資料20頁\)](#)

設問5(2)I

模範解答は「EPSS値の監視」。

【空欄】周辺より、EPSS値の「しきい値」の見直し以外に、続けて行うことを考えます。境界（しきい値）が変わることもあれば、EPSS値自体が変わるのでと発想（するかなあ）。

なお、EPSS値は時間経過で上昇する傾向にあります。EPSS値の初期値と最大値のどちらを使うか、閾値を1%と10%どちらを使うかも議論事項。この辺りは運用面、対応する脆弱性の数・網羅できる比率などから考えます。[> IPA資料64頁](#)

設問5(3) | 問題文の「但し書き」

模範解答は「診断時に実際に悪用できることを確認しているから」。従来レベルなので拾ってください。

下線⑥にて「EPSS値は、しきい値Bよりも高い」と判断したってことは、危険度が高いってこと。「P社のWebアプリ診断であれば」なので、P社のWebアプリ診断の特性を探します。

問題文1頁目（10頁）中盤「P社のWebアプリ診断は、脆弱性が実際に悪用できることを確認した上で～評判が良い」。

よって模範解答に至ります。

終盤問題のヒントが問題文序盤、って隠し方は良くあります。難しい問題ほど、問題文序盤や図表の注記に目立たないように潜んでます。

>長文問題を解く6つのテクニックNote（5）

>長文問題を解く6つのテクニックNote（2）

正直飛んで火に入るなんとやら。私は読んだ時に◀印でマーキングしてました。「わざわざ書いてるなあ、解答に使うでしょこの特性」と。>長文問題を読む6つのテクニックNote（3－3）

設問6m～t | 丁寧に全問正解を！

正答は

m: 「A」

n: 「A」

o: 「C」

p: 「A」

q: 「B」

r: 「B」

s: 「A」

t: 「S」

必ず専門正解してください。

間違わないよう書き出しまとめる。

SENNAKI.COM

表3, 5 表7,(8) 下線⑥ 図3 表7, 8 表6

	基本値	EPSS	領域	環境値	優先度
m PB-1	8.1	39	I	8.1	A
n PC-1	5.9	96.54	I	7.7	A
o PD-1	7.2	0.0	II	5.7	C
p PD-2	9.8	8.0	I	8.0	A
q PE-1	6.5	6.5	III	6.5	B
r WA-1	4.3	B以上	III	5.0	B
s WB-1	5.3	B以上	III	7.1	A
t WC-1	9.8	B以上	I	9.8	S

※赤文字 ※>7 ※≥1 ※I, II
の意味

WA-1, WB-1, WC-1のEPSS値は、下線⑥より閾値B以上とする、のだけ見逃さないように。探すとは思いますが。

表を描いておくと見直しができます。書いてないと見直し=解き直しになり時間がかかります。解く時の時短が、後の苦労につながる点も考えて、やり方を選んでください。

なおCVSSの閾値7・EPSSの閾値1%も、[IPA資料（32頁図2-5）](#)に例示されていました。値を覚えなくては良いと思いますが、この資料がほぼそのまま出題されているのが重要です。

今回出なかった = 今後出るのかも

今回の問題のリスク分析は、[IPA資料](#)に即していました。

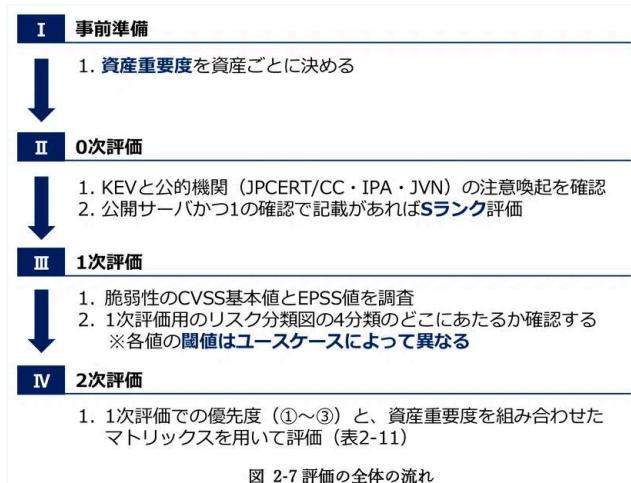
[IPA資料](#)は全122頁もあり、他にも記載事項はたくさんあります。

高度試験では全く同じ用語/パスはほぼ出ませんが、周囲は出ます。

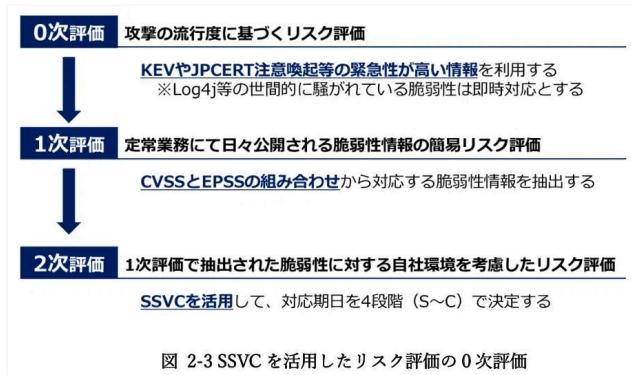
この節では、[IPA資料](#)を見て今回の問題で出てこなかつた点をピックアップしました。

SSVCによる2次評価

今回の問題では、2次評価ではCVSS環境値を使いました。



IPA資料にはもう1つの手法が掲載されています。「SSVC」を使って対応期日を出す手法（[IPA資料29頁図2-3](#)）。



SSVCは、3つの立場からのリスク評価指標。[>IPA資料（17頁）](#)。

- ・ デプロイナー：パッチを適用する組織
- ・ サプライヤー：パッチを提供する組織
- ・ コーディネータ：脆弱性情報を統制する組織

各々の立場で意志決定を決定木（ディシジョンツリー）が用意されています。[>IPA資料（図1-4）](#)

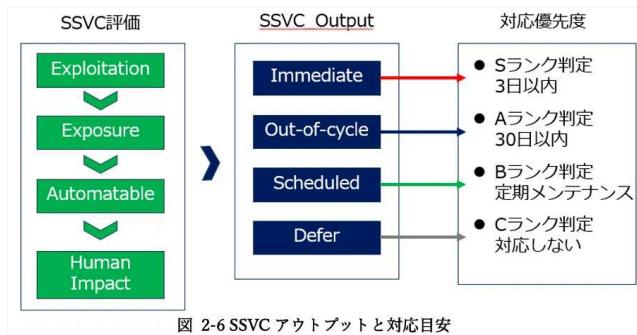
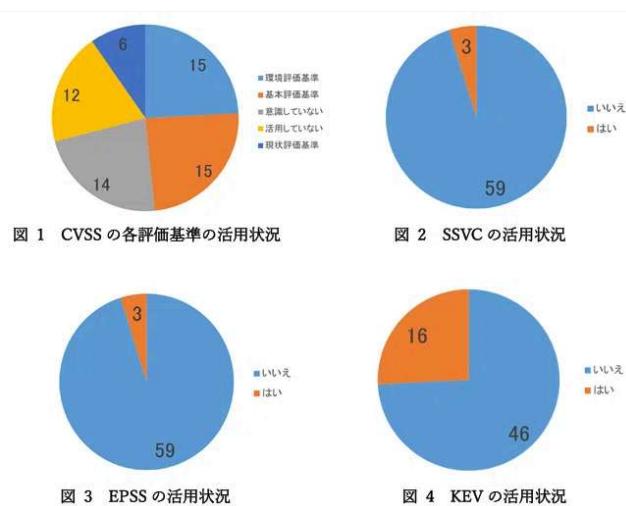


図 2-6 SSVC アウトプットと対応目安

今回のように試験で演習させるかは不明ですが、用語として「SSVC」を知っておくのは備えになるかと。

各指標の活用状況でも、SSVCの採用率は高いです。[>IPA資料（図2）](#)



各評価指標の課題/対応

今回、いくつか課題/対応が載っていました。

1次評価 (CVSS現状値, EPSS) →2次評価 (CVSS環境値) のパスでリスク分析をしてきました。

- CVSS現状値は調査の手間がかかる (16頁下線⑤, 設問5)
- EPSS値はFIRSTが公開している値を使えるので楽 (16頁下線⑤, 設問5)
- CVSS基本値の閾値=7, EPSS値の閾値=1% (閾値16頁図3下)

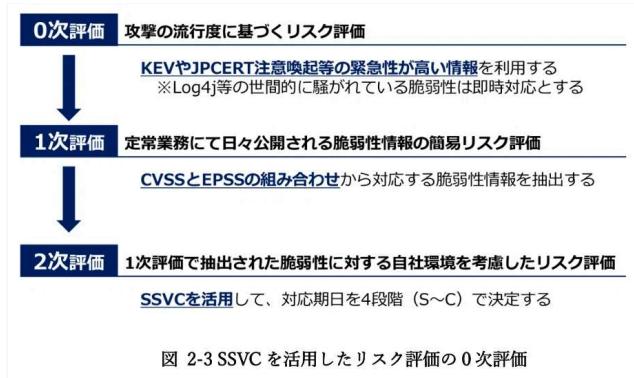
- EPSS値のモニタが必要 (16頁空欄, 設問5(2))
- EPSS値の報告がない場合、EPSSの閾値よりも高いとみなす (下線⑥)

とはいって、IPAの資料にはCVSS環境値、EPSS値の課題点も。

- CVSS現状値は、外部機関から提供される場合が少なく、自社で算出する手間になる(IPA資料12頁末)
- CVSS環境値は、実環境の正確な評価に専門的知識が必要。実質形骸化の一面も(IPA資料13頁頭)
- CVSSv4.0は2023年11月公開。運用実績が少ないが、v3.1同様普及していくだろう(IPA資料16頁)
- SVCCは「Exploitation」で用いる脅威情報の取得に専門知識が必要(IPA資料19頁)
- EPSSは米国機関FIRSTが運営しているため、日本製品の情報が不足(IPA資料20頁)
- EPSSは悪用情報+機械学習で、今後の悪用蓋然性(=確率)を算出しているが、機械学習部分がブラックボックスであり、説明不明瞭な面も(IPA資料20頁)
- KEVも米国CISAの運営なので、日本特有には情報不足な面も。網羅性や登録タイムラグにも注意が必要(IPA資料22頁)

以上の課題点は、用語の性質・最後「今後の課題点/改善点」の尻切れ問題に出るのかなと思いました。

特に注目は「SVCC」。この問題での2次評価では「CVSS環境値」を使いましたが、「SVCC」を用いる場合もあります(IPA資料29頁)。



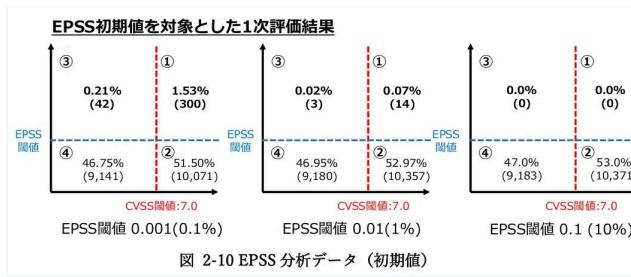
出ていない箇所 | 閾値・第三章運用面

今回の問題では、1次評価の閾値でCVSS現状値=7, EPSS値=1%を使っていました。[IPA資料](#)でも典型値として書かれています（[資料44頁表2-8](#), [資料47頁表2-10](#)）。

資料には閾値を選んだ議論がありますが、今回の問題では全てカット。統計が絡みますが、出題可能性はあるやも。

表 2-8 各 CVSS 基本値での効率性と網羅性（再掲）

CVSS 基本値	効率性 [%]	網羅性 [%]
10	23.1	7.0
9	23.2	14.5
8	23.1	14.9
7	31.5	53.2
6	29.2	65.9
5	26.1	80.8



さらに「第三章：運用編」は全く出ていません。今回の問題は「第一章中盤～第二章」です。今後「第三章」に特化した問題もあり得ます。

「第三章」で見慣れないものは、「NVD」・情報書式「CPE」「NVDのAPI出力結果」でした。

- **NVD** : NISTが運営する脆弱性DB（[資料54頁表3-1](#)）
- **CPE** : 製品（ハード/ソフト）を識別する。ゆくゆくは「**SWID**」が普及するかも（[資料55頁③, 56頁参考](#)）
- NVDのAPI出力結果 : JSON形式。PG系問題に出るかも（[資料59頁図3-6](#)）

```
[  
    "source": "nvd@nist.gov",  
    "type": "Primary",  
    "cvssData": {  
        "version": "3.1",  
        "vectorString":  
            "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H",  
        "attackVector": "NETWORK",  
        "attackComplexity": "LOW",  
        "privilegesRequired": "NONE",  
        "userInteraction": "NONE",  
        "scope": "CHANGED",  
        "confidentialityImpact": "HIGH",  
        "integrityImpact": "HIGH",  
        "availabilityImpact": "HIGH",  
        "baseScore": 10,  
        "baseSeverity": "CRITICAL"  
    },  
    "exploitabilityScore": 3.9,  
    "impactScore": 6  
,
```

図 3-6 NVD の API 出力結果（一部抜粋）

資料全体として、「属人性の排除」「網羅性」「対象とする脆弱性の数（月何件か）」が多く語られていました。

KEV・CVSS現状値と環境値・EPSSで客觀性が増したが、情報不足は「網羅性」に疑念、自社算出するなら「属人性」が増してしまうジレンマ。閾値を高くすると網羅性が減り、低くすると「対象とする脆弱性の数（月何件か）」が増えすぎて捌ききれない議論がありました。

まとめ | ライン変更に対応する

お疲れ様でした！

焦らずじっくり取り込まないと、ヒントに気づかない/延長の想像ができない/計算ミスをしてしまう油断ならない問題の印象でした。

一段深い理解/想像が必要な難易度へ	
設問	解答例・解説の要点
設問 1	<p>A B C D E</p> <p>SQI理解不足/ヒント見逃しで芋づる失点</p>
設問 2	<p>「新たな脆弱性が発見されたこと リスクが変わったと評したことを変化の可能性を想像</p>
設問 3	<p>「OpenSSH のログに認証タイムアウトのメッセージの出力が過去問頻出の「アラート」担当者は電子メールでアラートを送る。 クライアント認証を行なう。」</p> <p>無理だが推測もできる</p>
設問 4 (1)	<p>「A-1 バラメータ ite の値が容易に推測できること WB-1 発注確認機能の URL が推測困難であること C-1 発注確認機能の URL を入手する必要があること」</p> <p>芽から育てる想像</p>
設問 4 (2)	<p>「13 言葉に注目した基本解法</p>
設問 5 (1)	<p>「状値 攻撃コードなどの情報を多くの公開サイトから情報から判断する必要があるから」</p> <p>今後も出てくるでしょう！</p>
設問 5 (2)	<p>「FPSS 値 FIRST のサイトで公開されている値をそのまま」</p> <p>言葉に注目した基本解法</p>
設問 6	<p>「診断書に実際に適用できることを確認しているから」</p> <p>ミス/見直しのために時間かけても表にまとめる</p>

やはり印象的なのは「CVSS現状値」「EPSS値」の深めの理解。最新の教科書やIPA資料で傾向を抑える必要がありますが、正直手が回らない面が強いです。[>IPA資料](#)

何がどこまで出るか分かりません。「初見で狩られる」のは仕方ない面もあります。私たちにできることは「過去問の経験を生かす」「学習を広め深めに」の意識です。

「過去問の経験を生かす」では、どんな技術が出てきたか、どんな模範解答があったか。「おめーの過去の模範解答、×に出来るならやってみい」と流用仕返しましょう。>[長文問題を解く6つのテクニックNote \(6-4\)](#)

「学習を広め深めに」は、例えば問題文に「値」が出てきたら「変化するかな（CVSS, EPSS）」「推測できるかな（item）」「入手はどうするの」ぐらいまで考えて良いとこ。

問題文のヒントと解答との距離が広がりました。ライン（境界）が変わったので、こちらも対応して遅しくなりましょう。

以上になります！

少しでも意識調整のご参考になつたら嬉しいです。

＼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

