情報処理安全確保支援士への道(4)：令和７年 春 午後問題 続・問1を解いてみる(設問4～設問5(1)(2)編)

ルチルMike
2025年7月6日 11:20

問題冊子・配点割合・解答例・採点講評（2025年度、令和7年度） | 試験情報 | IPA 独立行政法人 情...

情報処理推進機構（IPA）の「問題冊子・配点割合・解答例・採点講評（2025年度、令和7年度）」に関する情報です。

www.ipa.go.jp

目次

ステップ2: ネットワーク経路を確認する

ステップ3: ログ取得に最適な場所を特定する

IPA解答例

設問5(2) 本文中の 下線⑦について（あ）、（い）で実行する利点を、それぞれ40字以内で答えよ

すべて表示

設問4 下線⑥について、脆弱性管理がしやすくなる理由を、具体的に答えよ

この設問は、下線部⑥にある「SBOM（Software Bill of Materials）を利用すると、将来、脆弱性管理がしやすくなる」理由を具体的に説明する問題です。

〔SBOM についての確認〕

次は，表 1 の項番 10 についての C さんと B さんの会話である。

C さん ：システム S のソフトウェア構成は設計書で把握できると考えていますが，SBOM の作成も必要でしょうか。

B さん ：SBOM を利用すると，⑥将来，脆弱性管理がしやすくなります。プラットフォーム G で作成することができます。

C さん ：なるほど。それでは，SBOM の作成を検討します。

ページ7

解き方

ステップ1: SBOMの役割を理解する

まず、SBOMが何かを理解します。SBOMは「ソフトウェア部品表」とも呼ばれ、ソフトウェアを構成するコンポーネント（ライブラリやモジュールなど）の一覧です 。どのソフトウェアが、どのバージョンで、どこに含まれているかを正確に記録したリストです。

ステップ2: 脆弱性管理の課題を考える

次に、一般的な脆弱性管理の流れとその課題を考えます。

- 新たな脆弱性が公表されます。この脆弱性情報は、特定のソフトウェアコンポーネント（例：〇〇ライブラリのバージョン1.2.3）に関連付けられています。
- 企業は、自社が開発・運用するシステムに、その脆弱なコンポーネントが含まれていないかを確認する必要があります。

課題:
　正確な部品表（SBOM）がない場合、どのシステムにどのコンポーネントが使われているかを特定する作業は、非常に時間がかかり、調査漏れが発生するリスクがある。

ステップ3: SBOMが課題をどう解決するかを考える

SBOMは、ステップ2の課題を解決します。

迅速・正確な特定:
　SBOMがあれば、自社の全システムのソフトウェア部品がリスト化されています。そのため、新たな脆弱性が公表された際に、その脆弱性を持つコンポーネントが自社のシステムに含まれているかどうかを、**機械的に、素早く、そして正確に**照合して特定できます。

結論（解答の組み立て）

以上の内容をまとめて、解答を作成します。

解答のポイント:
　「**ソフトウェアを構成するコンポーネントの一覧**」と「**脆弱性情報との迅速・正確な照合**」の2点を含めることが重要です。

解答例:
　ソフトウェアを構成するコンポーネントの一覧が明確になるため、新たな脆弱性が発見された際に、その脆弱性の影響を受けるコンポーネントがシステムに含まれているかを迅速かつ正確に特定できるから。

IPA解答例

利用しているソフトウェアやそのバージョンが明確になり，脆弱性の影響有無を容易に把握できるから

設問5 [開発工程のセキュリティ対策についての確認] について

設問5(1) 本文中の [d] にいれる適切な字句を、図2中の名称で答えよ

解き方

ステップ1: 問題の状況を理解する

まず、本文の会話内容から、解決すべき課題を把握します。

開発	6	ソフトウェア開発プラットフォームなどの開発環境は，アクセス制御を行い，必要な利用者だけがアクセスできるようにすること
	7	開発環境にアクセスしたアカウントを特定できるようにアクセスログを記録すること
	8	開発したソフトウェアのソースコードは，人手によるレビュー及びSASTツールによるチェックを行うこと
	9	システムの仕様，機能を精査し，不要な機能やセキュリティ上の欠陥がないことを設計書から確認すること

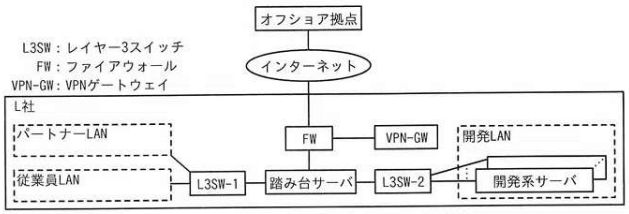


図2　システムSの開発環境の構成図（抜粋）

〔開発工程のセキュリティ対策についての確認〕

Bさんは，表1の項番7，8について確認した。次は，そのときのBさんとCさんの会話である。

Bさん：表1の項番7の対策は実施できていますか。

Cさん：オフショア拠点から開発LANへのアクセスについてはVPN-GWでアクセスログを取得できているものの，社内からのアクセスについては取得できていません。

Bさん：アクセスログは図2中の［　d　］で取得するのがよいでしょう。

Cさん：分かりました。

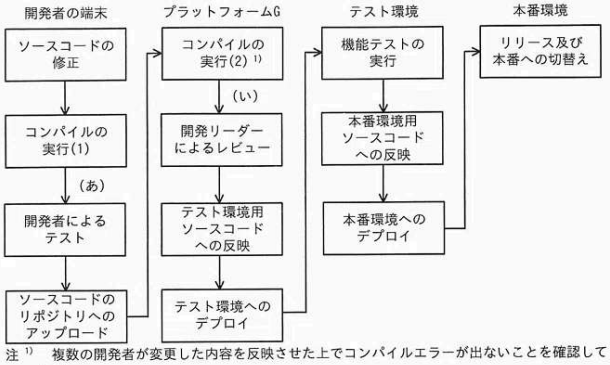
Bさん：表1の項番8の対策はどのようにしていますか。

Cさん：現在はソースコードの変更内容を開発リーダーがレビューしています。

Bさん：開発リーダーによるレビューに加えて，ツールFでチェックするのがよいでしょう。

Cさん：開発フローのどこでツールFを実行するのがよいでしょうか。

Bさん：ツールFの特性を踏まえると，図3のシステムSの開発フロー中の(あ)又は(い)で実行するのがよいと考えられます。⑦それぞれ利点が異なります。



注 1) 複数の開発者が変更した内容を反映させた上でコンパイルエラーが出ないことを確認している。

図3 システムSの開発フロー

ガイドラインを用いた点検の後，L 社のサプライチェーンリスク対策は強化された。

課題:
　オフショア拠点からのアクセスログはVPN-GWで取得できているが、**社内（従業員LAN、パートナーLAN）から開発LANへのアクセスログが取得できていない** 。

目的:
　Bさんは、この課題を解決するために、アクセスログを取得すべき最適な場所 [d] を提案しています。

ステップ2: ネットワーク経路を確認する

次に、図2の構成図を見て、ログが取得できていない「社内から開発LANへ」の通信が、どの機器を通過するのかを確認します。

通信は「従業員LAN」または「パートナーLAN」から始まります 。

これらのLANからの通信は「L3SW-1」に集約されます 。

その後、必ず「**踏み台サーバ**」を経由します 。

「踏み台サーバ」から「L3SW-2」を通り、「開発LAN」へ到達します 。

経路： **社内LAN → L3SW-1 → 踏み台サーバ → L3SW-2 → 開発LAN**

ステップ3: ログ取得に最適な場所を特定する

ステップ2で確認した経路上の機器の中から、社内からのアクセスを一元的に監視・記録できる最も効果的な場所を探します。

L3SW-1:
経路の途中にありますが、ここではIPアドレスレベルのログしか取得できない可能性が高いです。ガイドラインが求める「アカウントの特定」 には不十分です。

踏み台サーバ:
図1の項番10に「アクセスする際には**一旦、踏み台サーバにログインする**」と明記されており、**社内からのアクセスが必ず経由するポイント**です 。**サーバの機能として、誰が・いつログインしたかというアカウント単位での詳細なアクセスログを取得するのに最適**です。

L3SW-2:
踏み台サーバの後に位置するため、ここでログを取得しても、元の利用者アカウントを特定するのは困難です。

以上のことから、社内からのアクセスをアカウントレベルで特定するという目的を達成するためには、「踏み台サーバ」が最も適切なログ取得場所となります。

結論

したがって、**d** に入れるべき適切な字句は「**踏み台サーバ**」です。

IPA解答例

(1)	d	踏み台サーバ

設問5(2) 本文中の 下線⑦について（あ）、（い）で実行する利点を、それぞれ40字以内で答えよ

解き方

ステップ1: ツールFと(あ)、(い)の時点の特性を理解する

まず、問題文からツールFと各時点の情報を整理します。

ツールFの特性:
　コンパイルエラーが解消されたソースコードに対して正常な検査が可能 。

時点(あ)の状況:

場所: 開発者の端末上 。

タイミング:
　開発者が自身のコードをコンパイルした後で、リポジトリにアップロードする前 。

時点(い)の状況:

場所: プラットフォームG上 。

タイミング: 複数の開発者のコードが統合・コンパイルされた後で、開発リーダーがレビューする前 。

ステップ2: 時点(あ)で実行する利点を考える

時点(あ)は、開発者がコーディングを終えた直後の、個人の環境です。

誰が、いつ見つけるか:
　開発者自身が、コードをリポジトリに登録する「前」に脆弱性を発見できます。
発見後の対応:
　開発者自身がすぐに修正できます。他の開発者への影響や、後の工程での修正依頼といったコミュニケーションコストが発生しません。

利点の要約:
　この「早期発見・即時修正」による**手戻りの削減**が最大の利点です。

解答の組み立て（あ）:
　開発者が早期に脆弱性を検出し修正でき、手戻りを削減できる。 (33文字)

ステップ3: 時点(い)で実行する利点を考える

　時点(い)は、複数の開発者のコードが統合された、共有リポジトリの環境です。

何を検査対象とするか:
　個々の開発者のコードだけでなく、**統合された状態のコード全体**を検査対象とします。コード間の連携によって発生する脆弱性も検出できる可能性があります。
どのような役割を果たすか:
　開発リーダーのレビュー前に、機械的・網羅的なチェックを行うことで、リポジトリに登録されるコードの**品質を一定に保つ**「品質ゲート」としての役割を果たします。
利点の要約:
　全員のコードを**一元的に検査**し、プロジェクト全体の**品質を担保**できる点が利点です。

解答の組み立て（い）:
　複数開発者のコードを統合した状態で、一元的に検査できる点。 (30文字)

まとめ

以上の考察から、それぞれの利点を40字以内でまとめます。

- **(あ)の利点**: 開発者が早期に脆弱性を検出し修正でき、手戻りを削減できる。
- **(い)の利点**: 複数開発者のコードを統合した状態で、一元的に検査できる点

IPA解答例

(2)	(あ)	ツール F で検知できるエラーをより早く発見することができる。
	(い)	CI/CD パイプラインの管理機能を使って自動実行することができる。

さいごに

設問５(2)は、IPA解答例と論点のずれがありましたので、このあたりは部分点狙いになりますね。きっとIPAのホームページで発信している情報の中に解答例にきわめて近い書き方がされているのかもしれません。そのあたりも情報収集が必要だなと感じました。

補足(2025/7/13)

　情報安全確保支援士に関連する note記事を調べていると、非常に有用な記事がありました（以下にリンクを貼らせていただいています）。この方の分析によると過去問を解いても、午後問題対策として十分とは言えないとのこと。

　この記事を読んだあと、改めて問１で扱われたテーマである「サプライチェーンのリスク対策」が、IPAの資料の中で取り上げられたテーマなのかを調べてみました。なんと、情報セキュリティ10大脅威 2025(情報セキュリティ10大脅威 2025 解説書(組織編))では、「サプライチェーンや委託先を狙った攻撃」が2位にランクインしていることがわかりました。

　学ぶべき領域と実社会での脅威とをつなぎ合わせることの重要度が増したように思います。