情報処理安全確保支援士への道(2)：令和７年 春 午後問題 続・問1を解いてみる(設問2(1)～(3)編)

ルチルMike
2025年7月5日 21:05

設問2 [過去のインシデントの確認] について

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

すべて表示

設問2(1)

設問2 (1)「本文中の下線③について、影響を受けない配置方法を答えよ」

解き方

ステップ1：設問の要求を正確に把握する

まず、設問が何を求めているのかを明確にします。

- **要求**: 過去のインシデントにおいて、影響を受けなかった**「配置方法」**は何かを答えること。
- **対象**: 本文中の下線③。この下線は、D氏が「**スクリプトPの配置方法が違えば、影響を受けなかったようですね**」と述べている箇所です 。

B さん ：システム Q の利用者からの問合せで気付き，対策を実施しました。当時の情報セキュリティ担当は，サーバ T が侵害されたというニュースは知っていましたが，システム Q へのアクセスが影響を受けることを把握していませんでした。
D 氏 ：他社の発表によると，③スクリプト P を利用していたシステムでもスクリプト P の配置方法が違えば，影響を受けなかったようですね。
B さん ：はい。違う配置方法にするという対策もありました。しかし，Web ブラウザ開発元での古い Web ブラウザの公式サポートが終了していたことから，当社の対策としては，④システム Q のソースコードに変更を加えて，古い Web ブラウザのサポートを終了しました。

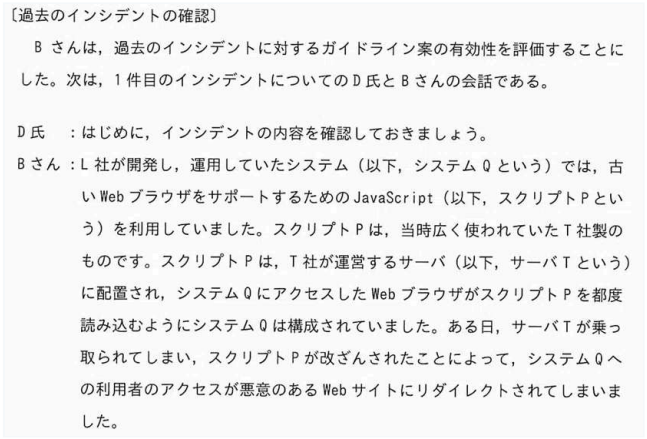
ページ4 下線③、④

ステップ2：インシデントの原因を分析する

影響を受けない方法を考えるために、まず影響を受けた原因を問題文から正確に読み取ります。

- **インシデントの内容**: L社のシステムにアクセスした利用者が、悪意のあるWebサイトにリダイレクトされた 。

- **脆弱だった配置方法**: L社のシステムは、当時広く使われていたT社製のJavaScript（スクリプトP）を、T社が運営するサーバ（サーバT）から**利用者が都度直接読み込む**ように構成されていた 。



〔過去のインシデントの確認〕

B さんは，過去のインシデントに対するガイドライン案の有効性を評価することにした。次は，1 件目のインシデントについての D 氏と B さんの会話である。

D 氏　：はじめに，インシデントの内容を確認しておきましょう。

B さん：L 社が開発し，運用していたシステム（以下，システム Q という）では，古い Web ブラウザをサポートするための JavaScript（以下，スクリプト P という）を利用していました。スクリプト P は，当時広く使われていた T 社製のものです。スクリプト P は，T 社が運営するサーバ（以下，サーバ T という）に配置され，システム Q にアクセスした Web ブラウザがスクリプト P を都度読み込むようにシステム Q は構成されていました。ある日，サーバ T が乗っ取られてしまい，スクリプト P が改ざんされたことによって，システム Q への利用者のアクセスが悪意のある Web サイトにリダイレクトされてしまいました。

ページ4 [過去のインシデントの確認]の導入部

- **根本原因**: 外部のサーバである**サーバTが乗っ取られ、スクリプトPが改ざんされた**こと 。

つまり、リスクの根源は「**自社で管理できない外部サーバ上のリソースを、直接利用者のブラウザに読み込ませていた**」点にあります。

ステップ3：影響を受けないための対策を考える

原因がわかったので、それを解消する方法を考えます。

- **原因**: 外部サーバ（サーバT）にある改ざんされたスクリプトを読み込んだこと。
- **対策**: 外部サーバから直接読み込まなければ良い。
- **具体策**: では、どこから読み込むべきか？ → **自社で管理している安全なサーバ**だと安全ではないか。

つまり、**L社はあらかじめ安全な状態の「スクリプトP」をT社のサーバからダウンロードしておき、自社のWebサーバ（システムQが稼働しているサーバ）に配置すべき**でした。

ステップ4：解答として具体的な配置方法を記述する

ステップ3で考えた内容を、設問の要求である「配置方法」として簡潔にまとめます。

- **NGな方法**: 外部サーバから直接読み込む。
- **OKな方法**: 自社のサーバに配置して、そこから読み込む。

この内容を解答として記述します。

ステップ5：解答を最終化する

以上のプロセスを経て、解答を完成させます。

解答例: スクリプトPを外部のT社のサーバから直接読み込むのではなく、L社が管理する自社のサーバ上に配置し、そこから読み込む方法。

IPA解答例

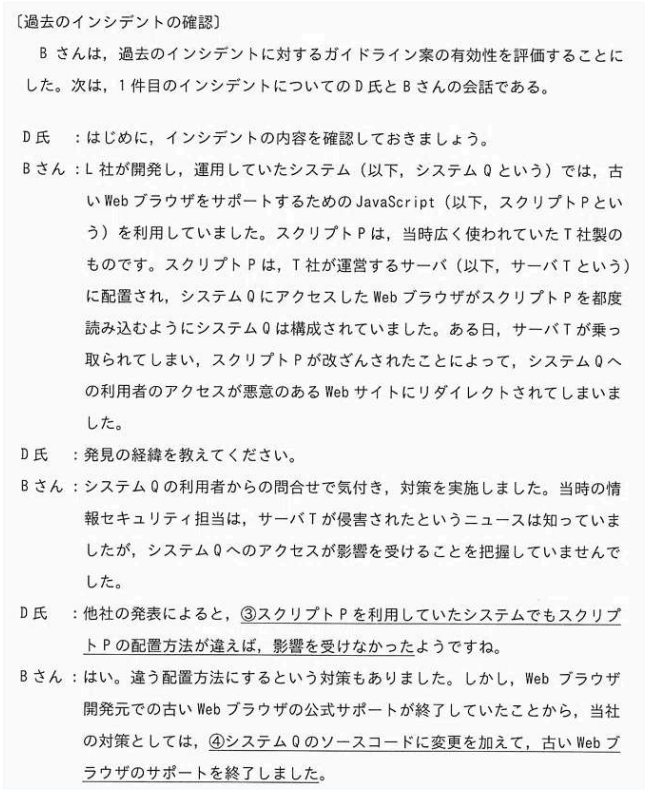
設問2 (2)

設問2 (2)「本文中の下線④について、加えた変更を、具体的に答えよ」

解き方

ステップ1：設問の要求を把握する

まず、設問が何を求めているのかを正確に理解します。



〔過去のインシデントの確認〕

B さんは，過去のインシデントに対するガイドライン案の有効性を評価することにした。次は，1 件目のインシデントについての D 氏と B さんの会話である。

D 氏　：はじめに，インシデントの内容を確認しておきましょう。

B さん：L 社が開発し，運用していたシステム（以下，システム Q という）では，古い Web ブラウザをサポートするための JavaScript（以下，スクリプト P という）を利用していました。スクリプト P は，当時広く使われていた T 社製のものです。スクリプト P は，T 社が運営するサーバ（以下，サーバ T という）に配置され，システム Q にアクセスした Web ブラウザがスクリプト P を都度読み込むようにシステム Q は構成されていました。ある日，サーバ T が乗っ取られてしまい，スクリプト P が改ざんされたことによって，システム Q への利用者のアクセスが悪意のある Web サイトにリダイレクトされてしまいました。

D 氏　：発見の経緯を教えてください。

B さん：システム Q の利用者からの問合せで気付き，対策を実施しました。当時の情報セキュリティ担当は，サーバ T が侵害されたというニュースは知っていましたが，システム Q へのアクセスが影響を受けることを把握していませんでした。

D 氏　：他社の発表によると，③スクリプト P を利用していたシステムでもスクリプト P の配置方法が違えば，影響を受けなかったようですね。

B さん：はい。違う配置方法にするという対策もありました。しかし，Web ブラウザ開発元での古い Web ブラウザの公式サポートが終了していたことから，当社の対策としては，④システム Q のソースコードに変更を加えて，古い Web ブラウザのサポートを終了しました。

（再掲）ページ 4

- **要求**: 本文中の下線④について、**L社がシステムQのソースコードに「加えた変更」を具体的に**答えること。

ステップ2：本文中の下線部と関連情報を確認する

次に、下線④が登場する前後の文脈を追い、変更の目的と内容に関する手がかりを探します。

- **下線部の記述**: 「当社の対策としては、④システムのソースコードに変更を加えて、古い Web ブラウザのサポートを終了しました。」
- **変更の目的**: 「古い Web ブラウザのサポートを終了」すること 。
- **インシデントの原因**: 「古い Web ブラウザをサポートするための JavaScript (以下、スクリプトPという)」を外部サーバから読み込んでいたこと。

ステップ3：変更内容を論理的に推測する

ステップ2で集めた情報を基に、どのようなソースコード変更が行われたかを論理的に考えます。

目的と手段の関連付け: L社の目的は「古いWebブラウザのサポート終了」です。
原因との関連付け: そもそもインシデントの原因となった「スクリプトP」は、「古いWebブラウザをサポートするため」のものでした

結論: ということは、**「古いWebブラウザのサポート」をやめるのであれば、そのために使っていた「スクリプトP」は不要になります。**

したがって、L社がソースコードに加えた具体的な変更とは、**不要になったスクリプトPを読み込む処理を削除すること**だと結論付けられます。

ステップ4：解答として具体的な変更点を記述する

ステップ3の結論を、設問の要求通り「具体的に」記述します。**Webページが外部のJavaScriptを読み込む際は、通常HTMLの<script>タグなどを使用します**。その記述を削除した、という内容を盛り込みます。

※具体的な手法について

　Webページが外部のJavaScriptファイルを読み込む際に、HTMLの<script>タグを使用するのが最も一般的で標準的な手法です

<script>タグを使用する方法

　HTMLファイルの中で、src（ソース）属性を使って外部JavaScriptファイルのパスを指定します。ブラウザがこのタグを読み込むと、指定されたファイルをダウンロードして実行します。

記述例:　HTML

```
<!DOCTYPE html>
<html>
<head>
    <title>My Web Page</title>
</head>
<body>
    <h1>こんにちは！</h1>
    <p>このページは外部のJavaScriptを読み込みます。</p>

    <script src="js/myscript.js"></script>
```

```
</body>
</html>
```

この例では、jsフォルダの中にあるmyscript.jsというファイルを読み込んでいます。

その他の方法

近年では、より高度な方法も使われています。

- **動的インポート**: JavaScriptのコード内で、必要になったタイミングで動的にスクリプトを読み込む方法です。import()関数などが使われます。
- **ESモジュール**: import / export 構文を使い、JavaScriptファイル同士で機能をモジュールとして読み込み合う方法です。現代的なWebアプリケーション開発で広く利用されています。

これらの高度な方法も、最終的にはブラウザの<script type="module">の仕組みなどを利用しており、<script>タグが基本であることに変わりはありません。

ステップ5：解答を最終化する

以上のプロセスを経て、解答を完成させます。

解答例:

Webページのソースコードから、古いWebブラウザをサポートするための外部スクリプト（スクリプトP）を読み込むための記述を削除した変更。

IPA解答例

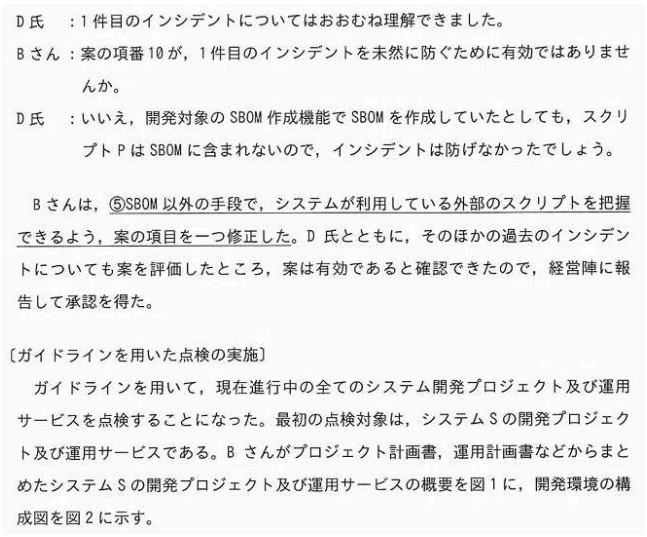
(2)	スクリプト P を読み込む箇所をソースコードから削除する。

設問2(3)

設問2 (3)「本文中の下線⑤について、修正した項番と修正内容を答えよ」

解き方

ステップ1：設問の要求を把握する



D氏　：1件目のインシデントについてはおおむね理解できました。
Bさん：案の項番10が，1件目のインシデントを未然に防ぐために有効ではありませんか。
D氏　：いいえ，開発対象のSBOM作成機能でSBOMを作成していたとしても，スクリプトPはSBOMに含まれないので，インシデントは防げなかったでしょう。

Bさんは，⑤SBOM以外の手段で，システムが利用している外部のスクリプトを把握できるよう，案の項目を一つ修正した。D氏とともに，そのほかの過去のインシデントについても案を評価したところ，案は有効であると確認できたので，経営陣に報告して承認を得た。

〔ガイドラインを用いた点検の実施〕

ガイドラインを用いて，現在進行中の全てのシステム開発プロジェクト及び運用サービスを点検することになった。最初の点検対象は，システムSの開発プロジェクト及び運用サービスである。Bさんがプロジェクト計画書，運用計画書などからまとめたシステムSの開発プロジェクト及び運用サービスの概要を図1に，開発環境の構成図を図2に示す。

ページ5より、下線部⑤の周辺を抜粋

まず、設問が何を求めているのかを正確に理解します。この設問は、以下の2つの点を答えるよう求めています。

- Bさんが修正したガイドラインの**「項番」**
- その**「修正内容」**

ステップ2：本文中の下線部から修正の目的を読み取る

次に、下線⑤の前後の文脈から、なぜ、何を修正しようとしているのかを把握します。

- **きっかけ**: D氏が「開発対象のSBOM作成機能でSBOMを作成していたとしても、スクリプトPはSBOMに含まれないので、インシデントは防げなかったでしょう」と指摘したこと 。
- **修正の目的**: 「SBOM以外の手段で、システムが利用している**外部のスクリプトを把握できる**ように」すること 。

ここから、**「資産として管理すべき対象のリストに漏れがあったので、それを追加する」**という修正の方向性が見えてきます。

ステップ3：修正対象となるガイドライン項目を特定する

ステップ2で把握した「資産のリストに項目を追加する」という目的に最も合致するガイドライン項目を表1（ガイドライン案）から探します。

表1　ガイドライン案（抜粋）

工程	項番	対策
共通	1	システムに関連する情報資産を，業務委託先と共同で利用するものも含めて一覧化し，管理すること。一覧化すべき情報資産は，次のとおりである。 ・サーバ ・ネットワーク機器 ・ソースコード ・リポジトリ内のライブラリ
	2	各工程で利用するシステムのアカウントは，業務委託先を含めて必要な利用者にだけ発行すること。その際，責任追跡性を確保するためにアカウントの利用者を特定できるようにすること
	3	一覧化した情報資産ごとに，パッチ適用状況など最新の構成情報を把握すること
調達	4	業務委託先の企業を，再委託先まで含めて一覧として管理すること
	5	業務委託先でのセキュリティ管理に関する要件を，業務委託先との契約に含めること
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
リリース・デプロイ	10	開発したソフトウェアのSBOMを作成すること
	11	リリースしたソフトウェアは，リリースバージョンを管理すること
運用	12	システムの稼働環境において，稼働状況を監視すること
	13	システムの稼働環境において，要件に応じたアクセス制御を実施すること
	14	システムの運用端末がある部屋は，要件に応じた入退室管理を実施すること
	15	インシデント対応手順書を作成すること

- **項番1**:「システムに関連する**情報資産を**、...**一覧化し、管理する**こと。」この項目は、管理すべき情報資産のリストそのものを定義しています。外部スクリプトも情報資産の一種なので、このリストに追加するのが最も自然で論理的です。
- **その他の候補**:
  項番10（SBOMの作成）は、今回の問題点をカバーできないと名指しされているため、修正対象としては不適切です。
  他の項目は、資産の一覧化とは直接関係が薄いです。

したがって、修正対象は**項番1**であると特定できます。

ステップ4：具体的な修正内容を考える

項番1をどのように修正すれば、「外部のスクリプトを把握できる」ようになるかを考えます。

- **修正前の”項番1”**: 管理すべき情報資産として「サーバ」「ネットワーク機器」「ソースコード」「リポジトリ内のライブラリ」が挙げられている
- **問題点**: このリストには、**インシデントの原因となった「外部サーバから読み込むスクリプトP」のような資産が含まれていません。**
- **修正内容**: よって、この情報資産のリストに、**「外部サーバから読み込むスクリプトやライブラリ」**といった趣旨の項目を新たに追加する必要があります。

ステップ5：解答を最終化する

以上のプロセスで特定した「項番」と「修正内容」を、設問の形式に合わせてまとめます。

- **修正した項番**: 1
- **修正内容**: 項番1で一覧化すべき情報資産のリストに、「外部サーバから読み込むスクリプトやライブラリ」などの項目を追加する修正。

IPA解答例

(3)	項番	1
	修正内容	連携している外部サービスを管理対象に含める。

さいごに

問題テキストに記載されている言葉を活用しても、回答が自由記載なので、IPAが開示している解答例と一字一句は同じにならないが、×（バツ）にはならないのかなと思います。部分点？なのかな。