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

ルチルMike
2025年7月6日 10:15

設問3 [ガイドラインを用いた点検の実施] 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3(1)

設問3 (1)　表２中の［ア］～［エ］にいれる適切な項番を答えよ

解き方

まず、問題を解いていくにあたって方針を確認します。

各空欄について、まず**表2で示されているガイドライン（表1の項番）の内容を理解**します。次に、そのガイドラインが**具体的にどのように実施されているか（または、いないか）を示す記述を図1の中から探し**、その項番を特定します。

〔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。

1. システムＳは，Ｌ社が３年前からＳ銀行向けに提供しているインターネットバンキングシステムである。運用と追加機能の開発をＬ社が請け負っている。
2. セキュリティ監視を情報セキュリティ会社のＮ社に委託している。開発は，Ｌ社従業員，Ｌ社に派遣された派遣エンジニア及び他の業務委託先の従業員が行っている。なお，運用ツールなど一部のソフトウェアはＮ社が開発することがある。
3. Ｌ社がシステムＳを運用するためにＳ銀行内にセキュアルームが用意されている。セキュアルームへの入室にＳ銀行が貸与するカードでの認証を必須とする入退室装置が導入され，Ｓ銀行の管理者及びＬ社の運用担当者しか入室できないようになっている。
4. 派遣元及び業務委託先との間では，Ｌ社のセキュリティポリシーの順守とプロジェクトでのセキュリティルールの順守について契約書で定めている。Ｎ社との業務委託契約には，Ｎ社内のセキュリティ管理についての実施事項及びＮ社が再委託を行わないことを明記している。Ｎ社での委託契約の順守状況を定期的な監査によって確認する。
5. 開発時に，要件定義段階での脅威モデリング及び設計段階での設計書の確認を行い，不要な機能やセキュリティ上の欠陥がないことを確認する。
6. プラットフォームＧに設計書を格納する。開発したソフトウェアのSBOMは作成しない。
7. 開発したソフトウェアのソースコードは，開発リーダーがレビューして承認する。開発したソフトウェアをリリースする際は，開発リーダーがリリースバージョンを更新する。

図１　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

8. 資産管理台帳にサーバ及びネットワーク機器の一覧を担当者が入力する。
9. システムSに組み込むOSSライブラリは，開発者が取得する。OSSライブラリは資産管理台帳に入力しない。
10. 開発は，L社内及びオフショア拠点で行い，次のLANに接続した端末で実施する。
・L社内に用意した従業員LAN
・L社内に用意したパートナーLAN
・オフショア拠点にある業務委託先のLAN
また，テストなどのためにシステムSの開発系サーバがあるLAN（以下，開発LANという）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。踏み台サーバには，L社，業務委託先など会社ごとに発行した共用アカウントでログインするが，ログインごとに，利用記録簿に記載する。開発LAN上のサーバには製品仕様上，アクセスログが取れないものもある。
11. インシデント発生時にL社のシステムSの担当者に連絡するための業務フローがインシデント対応手順書に定められており，システムSの担当者がインシデントのハンドリングを行う。
12. ツールFが開発者の端末とプラットフォームGにインストールされている。

図1　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（続き）

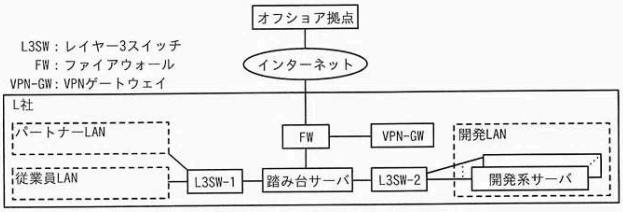


図2　システムSの開発環境の構成図（抜粋）

Bさんは，システムSの担当者へのヒアリング前に論点を整理しておこうと考え，表1の各項番について，図1に基づき，対策状況を確認した。結果は表2のとおりである。

表2　システムSの事前確認結果（抜粋）

工程	表1の項番	確認した図1の項番	確認結果又は問題点
共通	1	8，9	OSSライブラリを台帳管理していない。
	2	ア	a
調達	5	イ	問題なし。
開発	9	ウ	b
リリース・デプロイ	10	6	開発したソフトウェアについてSBOMを作成していない。
運用	15	エ	c

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

ステップ1：空欄「ア」の特定

該当ガイドラインの確認：

表2の「ア」が含まれる行は、表1の項番「2」に対応しています。表1の項番2は「**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**」というガイドラインです 。

図1での関連記述の探索 ：
　図1の記述の中で、アカウントの利用や利用者の特定に関連するものを探します。

該当箇所の特定：
　図1の**項番10**に「踏み台サーバには、L社、業務委託先など会社ごとに発行した**共用アカウント**でログインするが、ログインごとに、**利用記録簿に記載する**」という記述があります 。これは、**共用アカウントという問題点はありつつも、利用記録簿によって利用者の特定（責任追跡性の確保）を試みている状況を示しており、ガイドライン項番2に最も関連が深い記述です**。

結論：
　したがって、**ア** に入る項番は **10** です。

ステップ2：空欄「イ」の特定

該当ガイドラインの確認：
　表2の「イ」が含まれる行は、表1の項番「5」に対応しています。表1の項番5は「**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**」というガイドラインです 。

図1での関連記述の探索 ：
　図1の記述の中で、業務委託先との契約内容について言及している部分を探します。

該当箇所の特定 ：
　図1の**項番4**に「派遣元及び業務委託先との間では、L社のセキュリティポリシーの順守とプロジェクトでのセキュリティルールの順守について**契約書で定めている**。N社との業務委託契約には、N社内のセキュリティ管理についての**実施事項及びN社が再委託を行わないことを明記している**。」とあります 。これはガイドライン項番5の内容を具体的に実施している記述です。

結論：
　したがって、**イ** に入る項番は **4** です。

ステップ3：空欄「ウ」の特定

該当ガイドラインの確認：
　表2の「ウ」が含まれる行は、表1の項番「9」に対応しています。表1の項番9は「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」というガイドラインです 。

図1での関連記述の探索：
　図1の記述の中で、設計段階でのセキュリティ確認について言及している部分を探します。

該当箇所の特定：
　図1の**項番5**に「開発時に、要件定義段階での脅威モデリング及び**設計段階での設計書の確認**を行い、**不要な機能やセキュリティ上の欠陥がないことを確認する。**」とあります 。これはガイドライン項番9の内容をそのまま実施している記述です。

結論：
　したがって、**ウ** に入る項番は **5** です。

ステップ4：空欄「エ」の特定

該当ガイドラインの確認：
　表2の「エ」が含まれる行は、表1の項番「15」に対応しています。表1の項番15は「**インシデント対応手順書を作成すること**」というガイドラインです 。

図1での関連記述の探索：
　図1の記述の中で、インシデント対応や手順書について言及している部分を探します。

該当箇所の特定：
　図1の**項番11**に「インシデント発生時にL社のシステムSの担当者に連絡するための業務フローが**インシデント対応手順書に定められており**…」とあります 。これはガイドライン項番15の対応状況を示す記述です。

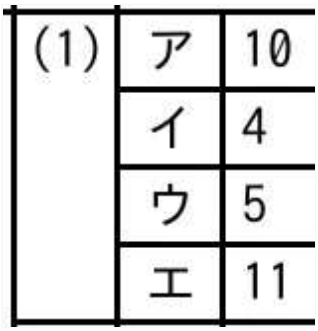
結論：
　したがって、**エ** に入る項番は **11** です。

まとめ

以上の手順により、各空欄に入る答えは以下の通りとなります。

- **ア：10**
- **イ：4**
- **ウ：5**
- **エ：11**

IPA解答例



つづいて、設問3(2)は設問3(1)で特定した関連箇所を基に、表2の空欄（a, b, c）に「確認結果」または「問題点」を記述する問題になります。

設問3(2)

設問3 (2)　表２中の［a］～［c］にいれる適切な字句を答えよ

解き方

ステップ1：空欄「a」の特定

関連情報の整理：
　ガイドライン（表1の項番2）：責任追跡性を確保するため、アカウントの利用者を特定できるようにする 。

システムSの状況（図1の項番10）：
　踏み台サーバへのログインに、会社ごとの**共用アカウント**を利用している

問題点の分析：
　ガイドラインでは、利用者を特定できる（＝責任追跡性がある）ことを求めています。しかし、システムSでは**共用アカウント**を使用しているため、「誰が」操作したのかをアカウント情報だけでは特定できません 。**利用記録簿への記載という対策は取られていますが、ガイドラインの本来の要求（アカウントと利用者が1対1で紐づくこと）は満たせていません**。これが問題点となります。

結論 ：
　したがって、**a** に入れるべき字句は「**踏み台サーバへのログインに共用アカウントを利用している**」など、共用アカウントの使用を指摘する内容です。

ステップ2：空欄「b」の特定

関連情報の整理：
　ガイドライン（表1の項番9）：設計書を確認し、不要な機能やセキュリティ上の欠陥がないことを確認する 。

システムSの状況（図1の項番5）：開発時に、脅威モデリングや**設計書の確認**を行い、**不要な機能やセキュリティ上の欠陥がないことを確認している** 。

-

状況の評価 図1の項番5の記述は、表1の項番9のガイドラインで要求されている内容を**そのまま実施している**ことを示しています 。事前確認の段階では、この点について特に問題は見当たりません。

結論：
　したがって、**b** に入れるべき字句は「**問題なし**」です。

ステップ3：空欄「c」の特定

関連情報の整理：
　ガイドライン（表1の項番15）：インシデント対応手順書を作成する 。

システムSの状況（図1の項番11）：インシデント対応手順書には、システムSの担当者への**連絡フロー**が定められており、担当者がインシデントの**ハンドリング**を行うことになっている 。

問題点の分析：
　インシデント対応手順書は存在しますが、その内容が「担当者への連絡」と「担当者が処理に着手すること（ハンドリング）」に限定されているように読めます 。本来、インシデント対応手順書には、インシデントの検知、分析、封じ込め、根絶、復旧、事後対応といった、より包括的なプロセスを定めるべきです。記述されている内容が限定的で、手順書として**不十分である可能性**が問題点となります。

結論：
　したがって、**c** に入れるべき字句は「**インシデント対応手順書の内容が、担当者への連絡フローなどに限定され不十分である**」など、手順書の内容が不十分であることを指摘する内容です。

IPA解答例

(2)	a	開発環境の踏み台サーバで共用アカウントを利用している。
	b	問題なし。
	c	問題なし。

さいごに

　(2)の cについて、IPA解答例は「問題なし」でしたので、私のインシデント対応手順書の内容が不十分であるというのは、考えすぎ（問題文を元に想像しすぎ）ということでした。ちゃんと問題文の世界で解答をしなければならないという学びを得ました。