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

ルチルMike
2025年7月5日 19:16

要約

　情報処理安全確保支援士の資格試験を目指すことになりましたので、モチベーションを高めるためにも勉強の記録を残してい行きたいと思います。
まずは直近の２０２５年春　午後問題の解き方をステップｂｙステップで解き方をまとめていきたいと思います。もし、同じ境遇の方がいらっしゃいましたら、ぜひ一緒に頑張りましょう。
今回は問１「サプライチェーンのリスク対策」を題材に扱います。

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

問1の概要

問題文の要約

　この問題は、金融業向けにシステム開発を行うL社を舞台としています。近年、業務委託先が原因となるセキュリティインシデントが増加していることを受け、L社の経営陣はサプライチェーン全体でのリスク対策強化を決定しました。

　物語は、情報セキュリティ担当のBさんが、コンサルタントD氏の助言を受けながら、以下の活動を進めていく形で展開されます。

1. **セキュリティガイドラインの作成:**
   システムのライフサイクル（調達、開発、リリース、運用など）に沿った、サプライチェーンリスク対策を強化するための新しいセキュリティガイドラインを作成します。
2. **過去のインシデントによる有効性評価:**
   作成したガイドライン案が、過去にL社で発生したインシデント（外部のJavaScriptライブラリが改ざんされた事案）を防ぐのに有効であったかを検証します。
3. **既存プロジェクトの点検:**
   完成したガイドラインを用いて、現在進行中のインターネットバンキングシステム「システムS」の開発プロジェクトを点検します。この点検を通じて、資産管理（OSSライブラリの未管理）、アクセス管理（共用アカウントの使用）、開発プロセス（SBOMの不作成、SASTツールの未活用）などの問題点が明らかになります 6。

4. **改善策の検討:**
   プロジェクト担当者のCさんへのヒアリングを行い、明らかになった問題点について、具体的な改善策（アクセスログの取得場所や、開発フローにおけるSASTツールの最適な実行タイミングなど）を検討します。

背景の概要

　この問題の背景には、現代のソフトウェア開発が自社だけで完結せず、多くの外部委託先、オープンソースソフトウェア（OSS）、外部サービスなどを組み合わせて行われるという**「サプライチェーンの複雑化」**があります。

　製品やサービスを構成する一部（ソフトウェア部品や委託先の管理体制など）に脆弱性があると、それが全体のセキュリティリスクに直結します。そのため、自社のセキュリティ対策だけでなく、自社に関わる全ての組織やソフトウェアを含めたサプライチェーン全体のリスクを管理・統制することの重要性が高まっています。

この問題は、そうした背景を踏まえ、企業がサプライチェーンリスクにどう向き合い、具体的な管理体制（ガイドライン）を構築し、それを実務に適用していくかという一連のプロセスを通して、情報セキュリティ専門家としての実践的な知識と判断力を問うものとなっています。

設問1 (1)

設問1 (1)「セキュリティ・バイ・デザインがどのような考え方か答えよ」

解き方

ステップ1：設問の要求を正確に理解する

まず、何が問われているのかを明確にします。

この設問は、専門用語である「**セキュリティ・バイ・デザイン**」の「**考え方（定義）**」を記述することを求めています（文字数制限はありません）

ステップ2：本文から手がかりを探す

では、問題文の中から「**セキュリティ・バイ・デザイン**」に関連する箇所を探し、文脈を掴みます。

1. **下線①の該当箇所の特定:**
   本文の3ページ目、Bさんの「①セキュリティ・バイ・デザインの考え方を一部取り入れました」という発言が直接の該当箇所です。
2. **文脈の確認:**
   この発言は、Bさんが表1の「ガイドライン案」を作成した直後になされています。したがって、**表1の内容に「セキュリティ・バイ・デザイン」の考え方が反映されている**と推測できます。
3. **具体例の探索:**
   表1の対策項目の中で、特にこの考え方を体現しているものを探します。**開発工程の項番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」が関連していることに気が付きます。
   この項目は、開発が完了した後ではなく、**システムの「設計」の段階でセキュリティ上の欠陥がないかを確認する活動です。これがまさに「設計（デザイン）」によってセキュリティを確保しようとするアプローチの具体例**と言えます。

ステップ3：専門用語の一般的な知識と結びつける

本文の手がかりと、自身が持つ（あるいは学習した）一般的な知識を結びつけます。

- 「バイ・デザイン（by Design）」とは、「設計によって」「設計上」という意味です。
- したがって、「セキュリティ・バイ・デザイン」とは、セキュリティ対策を後から付け足す（アドオン）のではなく、**システムの企画・設計といった開発の上流工程から、あらかじめ機能として組み込んでおく（ビルトイン）という考え方**です。

ステップ4：解答の骨子を組み立てる

ステップ2と3で得られた情報から、解答に含めるべきキーワードを抜き出して骨子を作ります。

- **いつ？** →「企画・設計段階」「開発の上流工程」「最初から」
- **何を？** →「セキュリティ」
- **どうする？** →「確保するための方策（機能）を組み込む」「あらかじめ考慮に入れる」

これらの要素を組み合わせ、例えば以下のような文章の骨格を作ります。

「（いつ）システムの企画・設計段階から、（何を）セキュリティを確保するための機能を、（どうする）あらかじめ組み込んでおく考え方。」

ステップ5：解答として文章を完成させる

最後に、ステップ4で作成した骨子を、簡潔で分かりやすい日本語の文章にまとめます。

- （例）システムの企画・設計段階から、セキュリティを確保するための方策を検討し、機能として組み込む考え方。

IPA解答例

設問1 (2)

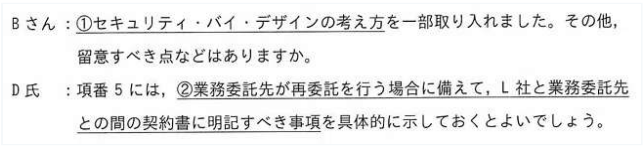
設問1 (2)「本文中下線②について、明記すべき事項を、５０字以内で答えよ」

解き方

ステップ1：設問の要求と制約を確認する

まず、設問が何を求めているのか、どのような制約があるのかを正確に把握します。

- **要求**: 業務委託先が**再委託**を行う場合に備え、契約書に**明記すべき事項** 。



3ページの下段に下線部②が書かれている

- **制約**: **50字以内**で記述する 。この字数制限は非常に重要で、解答の簡潔さが求められます。

ステップ2：本文から背景と文脈を読み取る

次に、下線②がどのような文脈で登場したかを確認します。

- **発言者**: コンサルタントのD氏 。
- **対象**: ガイドライン案の項番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」に対する助言です 。

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

表１中の項番5の記載内容

- **核心**: **L社が直接契約していない「再委託先」のセキュリティを、どうやってコントロールするかが論点であると読み取れます。**L社から見ると、「再委託先」は自社の管理が直接及ばない存在です。しかし、情報漏えいなどのインシデントが再委託先で発生した場合でも、契約上の責任はL社と直接契約している業務委託先が負うことが一般的であり、L社の事業にも大きな影響が及びます。そのため、問題文では「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」ことや、「業務委託先が再委託を行う場合に備えて、L社と業務委託先との間の契約書に明記すべき事項」を検討するなど、直接契約関係にない再委託先をいかにコントロールするかが、サプライチェーンリスク管理の重要な課題として扱われています

ステップ3：サプライチェーンリスクの観点から考える

設問の背景にある「**サプライチェーンリスク**」という視点から、具体的に何を契約で定めるべきかを考えます。もし委託先がL社に無断で再委託した場合、以下のようなリスクが発生します。

- L社が把握できないところで、自社の情報資産が扱われる。
- 再委託先のセキュリティレベルがL社の基準を満たしているか不明になる。

これらのリスクを防ぐために、契約書で縛るべき最も重要な項目は何かを考えます。

1. **承認のプロセス**: 勝手に再委託させないためのルール。
   「再委託する場合は、L社の**事前承諾**を必ず得ること」
   は、必須の項目です。
2. **義務の継承**: もし再委託を認める場合でも、セキュリティレベルを維持するためのルール。
   「再委託先にも、元の委託先と**同等のセキュリティ義務**を課すこと」
   が、必要です。

ステップ4：解答の要素を組み立て、字数内で表現する

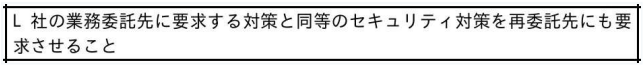
ステップ3で考えた2つの重要項目を、50字以内に収まるように簡潔な文章にまとめます。

- 要素A：再委託には**L社の事前承諾**が必要。
- 要素B：再委託先にも**同等の義務**を遵守させる。

これらの要素を組み合わせ、日本語として自然で、かつ要求内容を過不足なく満たす表現を探します。

（例）「**再委託を行う場合はL社の事前承諾を得ること、再委託先に委託元と同等のセキュリティ義務を遵守させること**」 → これで50文字です。要求されている要素が両方含まれており、字数制限もクリアしています。

IPA解答例



IPA解答と私の作成した解答とを比較してみたところ、IPA解答に事前承認を得ることは書かれていません。一方、再委託先に委託先と同等のセキュリティ義務を遵守させることは書くことができているので、今回の私の回答は × にはならないと思います。（知らんけど）

さいごに

設問２に向けても解答例の作り方をまとめていきたいと思います。気長にお待ちください