

令和7年度 秋期
システム監査技術者試験
午後Ⅰ 問題

試験時間

12:30 ~ 14:00 (1 時間 30 分)

注意事項

1. 試験開始及び終了は、監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで、問題冊子を開いて中を見てはいけません。
3. 答案用紙への受験番号などの記入は、試験開始の合図があってから始めてください。
4. 問題は、次の表に従って解答してください。

問題番号	問 1 ~ 問 3
選択方法	2 問選択

5. 答案用紙の記入に当たっては、次の指示に従ってください。
 - (1) B 又は HB の黒鉛筆又はシャープペンシルを使用してください。
 - (2) 受験番号欄に受験番号を、生年月日欄に受験票の生年月日を記入してください。
正しく記入されていない場合は、採点されないことがあります。生年月日欄については、受験票の生年月日を訂正した場合でも、訂正前の生年月日を記入してください。
 - (3) 選択した問題については、次の例に従って、選択欄の問題番号を○印で囲んでください。○印がない場合は、採点されません。3 問とも○印で囲んだ場合は、はじめの 2 問について採点します。
 - (4) 解答は、問題番号ごとに指定された枠内に記入してください。
 - (5) 解答は、丁寧な字ではっきりと書いてください。読みにくい場合は、減点の対象になります。

〔問 1、問 3 を選択した場合の例〕

選択欄	
2 問選択	問 1
	問 2
	問 3

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して、必ず読んでください。

問1 オープン API 態勢の監査に関する次の記述を読んで、設問に答えよ。

A 銀行は、以前から個人預金者（以下、顧客という）向けにインターネットバンキングによるサービス（以下、IB サービスという）として、口座残高、入出金明細などの照会サービス、及び振込、振込状況確認などの決済サービスを提供している。数年前からオープン API を利用して IB サービスの利便性向上を図っており、顧客はフィンテック事業者が提供するスマートフォンやタブレット向けのアプリケーションソフトウェア（以下、アプリという）から IB サービスを利用できるようになった。

〔オープン API を利用した IB サービスの概要〕

A 銀行が API を公開し、フィンテック事業者が提供する通帳、家計簿、決済などのアプリが、顧客の操作に応じて A 銀行の IB サービスにオープン API 経由でアクセスして結果を顧客に返す。当該アプリによる IB サービスへのアクセスは、A 銀行とオープン API 利用契約を締結したフィンテック事業者に対して、A 銀行がアクセストークンを発行することによって許可される。アクセストークンは、A 銀行の IB サービス利用に係る顧客との同意に基づく許可証であり、これによってフィンテック事業者のアプリがアクセスできる IB サービスの範囲が決定される。

〔金融オープン・イノベーションの推進〕

現在、インターネット経由で銀行口座の情報を取り扱うサービスを提供するフィンテック事業者には、電子決済などの代行業者（以下、電代業者という）としての登録が義務付けられている。また、銀行には努力義務として、オープン API を活用してセキュリティを確保しつつ電代業者との協業や連携を促進するオープン API 態勢の整備が求められている。

〔A 銀行のオープン API 態勢〕

A 銀行の IB サービスに係るオープン API 態勢は、次の各機能から構成される。

(1) IB サービスの企画・改善

リテール業務部は、オープン API 経由で顧客に提供する IB サービスを企画する。また、電代業者からの要望などを参考に、新規 IB サービスの企画や現行 IB サービス

スの改善を検討する。企画及び改善の内容は、IB サービス要件定義書にまとめられる。オープン API に係る新規公開、仕様変更及び廃止の通知は、実施の 1 か月前までに A 銀行のホームページに掲載されるとともに、オープン API 利用契約を締結している電代業者に送られる。

(2) オープン API の設計・開発・保守

情報システム部は、IB サービス要件定義書を基にオープン API 仕様書を作成し、オープン API の開発及び保守を行う。当該仕様書は、処理の詳細、処理を制御するパラメータと指定可能値、接続方法などを記載したものであり、オープン API の仕様変更やバグ修正に伴って改訂される。

(3) オープン API の運用

情報システム部は、オープン API 運用手順書に沿って、新規公開及び廃止を含めて運用を行う。運用ではオープン API が稼働するサーバ（以下、API サーバという）の負荷状況、接続遮断などの各種イベントの発生状況、オープン API 経由のアクセス状況が監視される。また、その結果は月次でオープン API 運用報告書にまとめられ、情報システム部内で回付される。

(4) オープン API の接続審査

情報システム部は、公益財団法人金融情報システムセンター発行の“API 接続チェックリスト”を基に、A 銀行独自の API 接続チェックリスト（以下、チェックリストという）を作成している。公開している API に対する電代業者からのオープン API 利用申請があった場合には、チェックリストを用いて、電代業者における情報セキュリティ対策の状況、認識している課題、課題への対応計画などについて審査を行う。そして、顧客情報の安全な提供が可能であることを確認した上でオープン API 利用契約を締結する。

〔システム監査の実施指示〕

内部監査部長は、オープン API 利用契約を締結する電代業者が増加してきたことから、オープン API 態勢の各機能が有効に働かない場合に電代業者及び顧客に及ぼす影響を懸念した。そして、オープン API 態勢の各機能の状況について監査を行うようシステム監査チームに指示した。

〔予備調査の結果〕

システム監査チームは、オープン API 態勢の各機能を担うリテール業務部及び情報システム部に対して予備調査を実施し、把握した状況を表 1 にまとめた。

表 1 オープン API 態勢の各機能の状況（抜粋）

項番	機能	状況
1	IB サービスの企画・改善	提供している各 IB サービスの利用状況を分析することによって、今後の顧客の利便性向上に役立つサービスを検討している。
2	オープン API の設計・開発・保守	自行のデータやシステムへの接続仕様を公開するので、アクセストークンで許可された範囲を超えるアクセスが、電代業者からできないようにするなど、セキュリティの確保に重点を置いている。
3	オープン API の運用	API サーバの過負荷を防ぐために、API サーバで単位時間当たりに受け付けるオープン API 接続リクエスト数の制限（以下、API レート制限という）を行っている。
4	オープン API の接続審査	電代業者からのオープン API 利用申請が増加しており、情報システム部によるチェックリストを用いた審査の負荷が高まっているので、審査の効率向上を図りたいと考えている。

〔本調査の結果〕

システム監査チームは、本調査を実施し、指摘事項及び改善提案を次のようにまとめた。

- (1) オープン API 運用報告書が情報システム部内での回付にとどまっており、オープン API 態勢において有効利用されていない。当該報告書にはオープン API 経由のアクセス状況が記載されているので、他に有効利用できる余地がある。
- (2) オープン API 態勢における電代業者との協業や連携の促進の観点からは、セキュリティの確保だけでなく、電代業者におけるアプリ管理への影響を抑えるために、次の事項を考慮する必要がある。
 - (a) オープン API の仕様変更が頻繁に発生しないような設計にすること
 - (b) オープン API の仕様変更が行われた場合、それによって電代業者が IB サービスを利用できなくなることを防ぐこと
- (3) API レート制限値を超えた場合には、エラーメッセージがアプリに返され、オープン API への接続が一時的に遮断されるが、API サーバの能力に余裕がある状態でも接続が遮断される事象が発生している。DDoS などのサイバー攻撃や不正アク

セスの検知、及びそれに伴う接続遮断の形跡がないので、API サーバで設定されている API レート制限値が適切でない可能性がある。不要な接続遮断による IB サービス提供の中断を避けるために、API レート制限値のチューニングが必要である。

- (4) チェックリストによる審査に時間を要しており、契約の可否判断が遅れる傾向にあるので、IB サービスの利用開始に関して、直接的には電代業者、間接的には顧客に影響を及ぼすおそれがある。チェックリストの各確認項目を同等に取り扱うのではなく、アクセストークンに基づくリスクベースアプローチによって、審査の効率向上を図る必要がある。

設問 1 [本調査の結果] (1)について、オープン API 運用報告書の有効利用に関してシステム監査チームが提案すべき改善内容を、30 字以内で答えよ。

設問 2 [本調査の結果] (2)について、(i), (ii)に答えよ。

(i) システム監査チームは、オープン API の仕様変更によって電代業者でどのような対応が必要になると考えて、(a)に示す改善提案を行ったか。30 字以内で答えよ。

(ii) システム監査チームによる改善提案(b)を行うために、仕様変更後の API 公開に当たって情報システム部が取り得る方策を二つ挙げ、それぞれ 30 字以内で答えよ。

設問 3 [本調査の結果] (3)について、API サーバで設定されている API レート制限値以外にシステム監査チームが入手した監査証拠を含め、当該状況を発見した監査手続を、45 字以内で答えよ。

設問 4 [本調査の結果] (4)について、システム監査チームが意図したリスクベースアプローチの内容を、50 字以内で答えよ。

問2 クラウドサービスを利用したシステムの監査に関する次の記述を読んで、設問に答えよ。

K 社は、事務機器を製造し、販売店経由で販売している企業である。K 社の情報システム部は、販売店を支援するために、専用 Web サイトで受発注、納期回答などの機能を提供する販売支援システム（以下、本システムという）を構築し、運用している。本システムは K 社が保有するシステム基盤上で稼働していたが、システム管理の負荷とコストの軽減を目的として、2 年前に L 社の IaaS に移行した。

移行後、大きな障害はなく順調に稼働していたが、2 か月前に、IaaS のシステム管理に使用するコンソール（以下、管理コンソールという）のアクセス制御において IP アドレス制限の設定漏れが見つかった。幸いにも情報の漏えい事故にはつながらなかったが、他社ではクラウドサービスの設定漏れを起因とした事故が多発している。そこで、K 社の内部監査室のシステム監査チームは、IaaS を利用する際のリスクに対して、本システムの管理が適切に行われているかどうかを監査することとした。

〔予備調査の結果〕

システム監査チームは、情報システム部から本システムに関する資料を入手するとともに、情報システム部長にインタビューを行い、本システムの概要と設定漏れの経緯を調査した。その結果の抜粋は次のとおりである。

(1) 本システムの概要

本システムの利用者は、当社の従業員及び販売店である。L 社の IaaS 上で稼働するアプリケーションシステム（以下、アプリケーションという）は外部委託先である M 社が開発している。製品情報、受発注情報、販売店情報などが IaaS 上のストレージに保管されている。

(2) 本システムの管理体制

情報システム部の S 氏がシステム管理者として任命されている。また、IaaS の管理業務とアプリケーションの保守業務は M 社に外部委託されている。インタビューの回答によると、現在、IaaS のシステム管理者権限を保有しているのは、S 氏及び M 社の担当者 2 名の計 3 名である。

(3) 設定漏れの経緯

2 か月前に、情報システム部がセキュリティベンダーに委託して、K 社のシステムに対する社外からのネットワーク診断を実施した。その結果、本システムの管理コンソールへのアクセスについて、IP アドレス制限が設定されていないとの指摘を受けた。

管理コンソールでは、仮想マシン、アクセス制御、ログ、監視、バックアップなどの IaaS の管理に係る重要な設定が行われる。そのために、IaaS の利用開始時から、K 社と M 社の接続元 IP アドレスだけにアクセスが制限されていた。

しかし、6 か月前の定期保守の際に、M 社の担当者が管理コンソールに接続できなくなる事象が発生したので、M 社から連絡を受けた S 氏が IP アドレスの制限を解除する設定を行い、対処した。その後、セキュリティベンダーから指摘を受けるまで、この設定を戻していなかった。

S 氏がログを確認したところ、3 か月前に、許可していない外部の接続元 IP アドレスから管理コンソールへのログインを試みたものの、失敗した履歴が残っていた。

(4) セキュリティ強化策

今回の設定漏れを踏まえて、情報システム部で次の二つの対策を行った。

- ① 管理コンソールで IaaS の設定をする際は、変更管理台帳にその記録を残すようにした。これに加えて、今回のような設定漏れを自動検知し、システム管理者に通知する自動化ツールの導入を検討中である。
- ② システム管理者権限のアカウントについて、IaaS の機能として利用できる多要素認証をアカウント単位で“必須”に設定し、セキュリティを強化した。

(5) その他のシステム管理状況

- ① K 社の“クラウドサービス利用に係る情報セキュリティ基準”（以下、クラウド利用基準という）では、IaaS を利用したシステムについて、ゲスト OS やミドルウェアなどのソフトウェアの脆弱性^{ぜい}診断を毎月実施することが定められている。また、発見された脆弱性の深刻度及び緊急度に応じた対処の判断基準が示されている。本システムも毎月脆弱性診断を実施しており、発見された脆弱性の対処に伴い不具合が発生しないと判断したセキュリティパッチは、四半期ごとの定期保守に合わせて適用する対処をしている。
- ② 緊急時に備え、IaaS の監査ログ機能を使用して、システム管理者権限の操作

ログを1年間取得している。なお、操作ログは暗号化され、システム管理者権限のアカウント以外では操作ログへアクセスできない。

③ L社の責任範囲であるデータセンターやハードウェア、ホストOSなどのセキュリティ管理状況については、L社の外部監査人による保証報告書がL社から提供されている。

④ M社とは、IaaSの管理業務とアプリケーションの保守業務に係る業務委託契約を締結している。S氏とM社とは毎週定例会を実施しており、業務の実施状況や課題などを議論し、議事録が残されている。

〔監査手続の検討〕

システム監査チームは、予備調査の結果を踏まえて、想定されるリスクの洗い出しと監査手続の検討に着手した。監査手続案を表1に示す。

表1 監査手続案（抜粋）

項番	想定されるリスク	監査手続案
1	システム管理者権限が不正に利用され、情報漏えいやシステム障害が発生する。	・ IaaS の設定を目視で確認し、管理コンソールへのアクセスが K 社及び M 社の接続元 IP アドレスに制限されていることを確かめる。 ・ S 氏のアカウントをサンプルとして管理コンソールへのログインテストを実施し、多要素認証が要求されることを確かめる。
2	脆弱性を突いたサイバー攻撃を受け、情報漏えいやシステム障害が発生する。	・ 脆弱性診断の記録を閲覧し、毎月脆弱性診断が実施されていることを確かめる。 ・ 脆弱性対処の記録を閲覧し、本システムへの影響評価に基づき対処されていることを確かめる。
3	システムの操作ログが残らず、内部不正やサイバー攻撃が追跡できない。	・ IaaS の設定を目視で確認し、システム管理者権限の操作ログの保管期間が1年間に設定されていることを確かめる。 ・ 操作ログの確認画面を目視で確認し、システム管理者権限の1年間分の操作ログが保管されていることを確かめる。
4	外部サービスのセキュリティ設定に不備があり、情報漏えいやシステム障害が発生する。	・ L 社の保証報告書を閲覧し、セキュリティ管理上の不備が発生していないことを確かめる。 ・ M 社との業務委託契約書を閲覧し、業務委託内容と責任範囲が合意されていることを確かめる。

〔内部監査室長の指示〕

内部監査室長は、予備調査の結果と表1をレビューして、次のとおり監査チーム

に指示した。

- (1) 表 1 項番 1 について、現在の監査手続案では不十分である。システム管理者権限が IaaS で適切に設定されていることを確かめる監査手続を盛り込むこと。
- (2) 表 1 項番 2 について、予備調査の結果を踏まえると、現在のコントロールには懸念がある。実施されているコントロールの詳細を確かめること。
- (3) 表 1 項番 3 について、現在の監査手続案では不十分である。システム管理者の権限に関して、保管されている操作ログの完全性が確保されていることを確かめること。
- (4) 表 1 項番 4 について、設定漏れを検知する自動化ツールが導入されるまでの間、実施可能な対策が講じられていることを確かめること。
- (5) 全体に係る内容として、予備調査の結果を踏まえると、K 社の本システムの管理体制は内部不正の観点で課題があるので、今後の対応方針や計画を確かめること。

設問 1 〔内部監査室長の指示〕(1)について、システム監査チームが追加で盛り込む監査手続において確認すべき内容を二つ挙げ、それぞれ 40 字以内で答えよ。

設問 2 〔内部監査室長の指示〕(2)について、内部監査室長が懸念している内容を、35 字以内で答えよ。

設問 3 〔内部監査室長の指示〕(3)について、システム監査チームが確認すべき具体的な内容を、30 字以内で答えよ。

設問 4 〔内部監査室長の指示〕(4)について、現時点で可能な対策と考えられる内容を、45 字以内で答えよ。

設問 5 〔内部監査室長の指示〕(5)について、内部監査室長が指摘した管理体制上の課題を、35 字以内で答えよ。

問3 IT投資計画の監査に関する次の記述を読んで、設問に答えよ。

R社は、中堅の食料品製造・販売業者である。R社では、近年のデジタル化の波に対応して企業変革を推進するべく、新規のIT投資計画を複数策定している。監査部は、IT投資計画が適切に作成され、経営陣に十分な判断材料が提供されているかどうかをテーマにシステム監査を行うことにした。今期計画されているIT投資案件の中から経営陣からも期待が高い案件である、基幹システムとデータ連携を行う消費者向けオンラインショッピングシステム（以下、ECシステムという）の構築案件を監査対象として選定した。

〔予備調査の結果〕

監査部は予備調査として、“IT投資計画書”の閲覧、DX推進室を中心とした関係者へのインタビューを実施し、ECシステムのIT投資計画（以下、本計画という）の概要を調査した。その結果は次のとおりである。

(1) 導入目的

ECシステムは、社外から人材を採用して新設されたDX推進室がシステムオーナーとなり、営業本部及び情報システム部と協力して導入する予定である。ECサイトを構築し、販売チャネルの拡大による売上増大、販売データなどを基にした新商品開発の意思決定の迅速化を行うことによって中期経営計画で定めた売上増大及び利益率向上を図るものである。

(2) システム概要

- ① ECシステムは大手ベンダーS社製のECパッケージをカスタマイズして導入する予定である。ECパッケージを採用することによって標準的な機能や定期的なバージョンアップが提供され、またR社として初めてIaaS上に構築されるシステムとなる。ECシステム及び基幹システムの概要は図1のとおりである。
- ② ECシステムの稼働直後は、一部商品から試験的に利用を開始し、その後対象商品を拡大していく計画である。ECシステムで使用するIaaSの処理能力、ストレージ容量などのリソースは、ECシステムの対象商品及び利用者の増加に応じて増強していく予定である。
- ③ 既存の基幹システムはオンプレミスで開発・導入したシステムである。本計画

では、IaaS 上の EC システムの導入・カスタマイズ、基幹システムのデータと IaaS 上の EC システムのデータを連携する機能（以下、データ連携機能という）の開発を、S 社に外部委託する。

- ④ EC システムと基幹システムとのデータ連携は、基幹システムの改修をできるだけ抑える方針であり、リアルタイムではなく日次のファイル連携処理で行う計画になっている。なお、基幹システム側の改修は情報システム部が行う計画であるが、情報システム部の業務が多忙であることから、改修範囲は要件定義段階で特定することになっている。
- ⑤ EC パッケージのカスタマイズは、R 社独自の商品カテゴリの構成変更や決済方法の追加、配送条件の個別設定などが予定されている。本番稼働後に、EC システムの利用状況や効果などを踏まえて、DX 推進室と営業本部が協力して追加のカスタマイズを予定している。

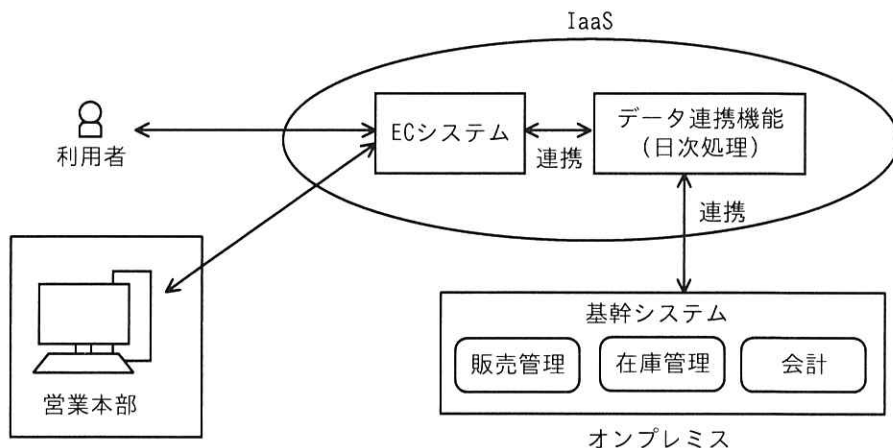


図1 ECシステム及び基幹システムの概要

(3) IT 投資の評価

- ① R 社では“投資管理規程”において IT 投資の評価基準として回収期間法を採用している。本計画の投資回収見込みは表1のとおりである。投資回収見込みによれば、データ連携機能の開発を含む EC システムの開発導入投資額と毎年のランニングコストは、計画どおりに売上増大及び利益率向上が実現すれば3年間で回収できる見込みである。R 社では投資判断基準としての回収期間について5年以内を目安としており、それよりも短い期間で回収可能と評価されている。

- ② 開発導入投資額は S 社が作成した見積り資料を基に DX 推進室が算定したものである。
- ③ ランニングコストの内訳は、IaaS の利用料、EC パッケージの保守契約費用である。IaaS の利用料は、使用する処理能力やストレージ容量などに応じた従量制による課金となっている。EC パッケージの保守契約の対象は、サポートデスクの問合せ対応及び問題発生時の調査・対応だけである。
- ④ 利益増加見込みは、経営会議で報告された R 社における過去の販売実績データ及び S 社が他社事例を基に作成した平均的な売上増加率に基づき、DX 推進室が独自に試算したものである。EC システムを活用した販路拡大によって見込まれる売上増大、販売データなどを基にした新商品開発による利益率向上を予測し、試算した。
- ⑤ EC システムが本番稼働した 1 年後に、DX 推進室と営業本部が本計画の投資評価を実施し、経営陣へ報告する予定である。

表 1 投資回収見込み

単位 千円

項目	本番稼働時点	稼働 1 年目	稼働 2 年目	稼働 3 年目
開発導入投資額	30,000	-	-	-
ランニングコスト	-	4,500	5,000	5,500
①支出額計	30,000	4,500	5,000	5,500
②利益増加見込み（収入額）	-	10,000	15,000	20,000
キャッシュフロー （②－①）	▲30,000	5,500	10,000	14,500
投資回収見込み	▲30,000	▲24,500	▲14,500	0

注記 本問では金利及び為替は考慮しないものとする。金額はキャッシュフローベースである。

〔本調査に向けた監査手続の検討〕

監査部は、予備調査の結果を踏まえて、本調査に向けて、次のように監査手続の検討を行っている。

- (1) EC システムは EC パッケージを導入する計画となっている。システム概要で把握した内容を基にすると、EC パッケージの保守契約費用に必要な項目が網羅的に含まれていないリスクがあるので、確認する必要がある。
- (2) EC システムと基幹システムのデータ連携について、表 1 の開発導入投資額だけ

では、支出額が低く計上されるリスクがあるので、追加の確認が必要である。

- (3) EC システムは当社として初めて IaaS 上に構築するシステムであり、不正アクセスによる情報漏えいなどのリスクがある。S 社の EC パッケージを導入するに当たり、EC システムの情報セキュリティ対策に漏れが生じないようにする必要がある。その観点から R 社の情報セキュリティ対策に係る支出額が適切に計上されていることを確認する必要がある。
- (4) 表 1 の利益増加見込みは、DX 推進室が独自に試算した売上増大及び新商品の開発による利益率向上の実現可能性が十分に検討されていることが重要と考えられる。それについて追加の確認が必要である。
- (5) EC システムの本番稼働後における本計画の投資評価が不十分となるおそれがある。十分な投資評価が行われるのかどうかを確認する必要がある。

設問 1 〔本調査に向けた監査手続の検討〕(1)について確認すべきことを、45 字以内で具体的に答えよ。

設問 2 〔本調査に向けた監査手続の検討〕(2)について、本調査で実施すべき監査手続を、50 字以内で答えよ。

設問 3 〔本調査に向けた監査手続の検討〕(3)について、R 社の情報セキュリティ対策に係る支出額が適切に計上されていることを確認する上で、S 社との関係でどのような点に留意すべきか。35 字以内で答えよ。

設問 4 〔本調査に向けた監査手続の検討〕(4)について、本調査で実施すべき監査手続を、40 字以内で答えよ。

設問 5 〔本調査に向けた監査手続の検討〕(5)について、十分な投資評価を行うために必要と考えられることを、35 字以内で答えよ。

[メモ用紙]

[メモ用紙]

6. 退室可能時間中に退室する場合は、手を挙げて監督員に合図し、答案用紙が回収されてから静かに退室してください。

退室可能時間	13:10 ～ 13:50
--------	---------------

7. 問題に関する質問にはお答えできません。文意どおり解釈してください。
8. 問題冊子の余白などは、適宜利用して構いません。ただし、問題冊子を切り離して利用することはできません。
9. 試験時間中、机の上に置けるものは、次のものに限ります。
- なお、会場での貸出しは行っていません。
- 受験票、黒鉛筆及びシャープペンシル（B 又は HB）、鉛筆削り、消しゴム、定規、時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可）、ハンカチ、ポケットティッシュ、目薬
- これら以外は机の上に置けません。使用もできません。
10. 試験終了後、この問題冊子は持ち帰ることができます。
11. 答案用紙は、いかなる場合でも提出してください。回収時に提出しない場合は、採点されません。
12. 試験時間中にトイレへ行きたくなったり、気分が悪くなったりした場合は、手を挙げて監督員に合図してください。
13. 午後Ⅱの試験開始は 14:30 ですので、14:10 までに着席してください。

試験問題に記載されている会社名又は製品名は、それぞれ各社又は各組織の商標又は登録商標です。

なお、試験問題では、TM 及び [®] を明記していません。