AU

令和５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〕

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　クレジットカード情報保護の監査に関する次の記述を読んで，設問に答えよ。

A社は，教育関連事業を営んでおり，ECサイトを通じて多くの学習コンテンツを月額定額制で配信している。利用料の支払方法については，口座振替のほかにクレジットカード（以下，カードという）などによるキャッシュレス決済を選択できる。

〔割賦販売法の一部を改正する法律の施行〕

カード会社，決済代行会社などは，カード業界の国際基準であるPCIデータセキュリティ基準（以下，PCI DSSという）への準拠を求められている。令和3年4月の割賦販売法の一部を改正する法律の施行に先立ち，カード情報の適切な管理及び不正利用防止対策の実務指針である“クレジットカード・セキュリティガイドライン”（以下，ガイドラインという）が定められ，カード加盟店は，カード情報の非保持化（以下，非保持化という）又はPCI DSS準拠のいずれかの実施を求められるようになった。A社は，カード加盟店のうち非対面でカード決済を行うEC加盟店に該当する。

〔非保持化の実施〕

非保持化とは，自社で保有する機器及びネットワークにおいてカード情報の保存，処理及び通過を行わないことをいう。非保持化は，PCI DSS準拠に比べて容易に実施できるカード情報保護対策であることから，A社は，ほとんどのEC加盟店と同様に非保持化を実施した。非保持化に際して採用したリダイレクト型の非通過方式によるカード決済の流れを図1に示す。これは，カード決済時にA社ECサイトから決済代行会社であるB社の決済画面に画面遷移させる方式である。

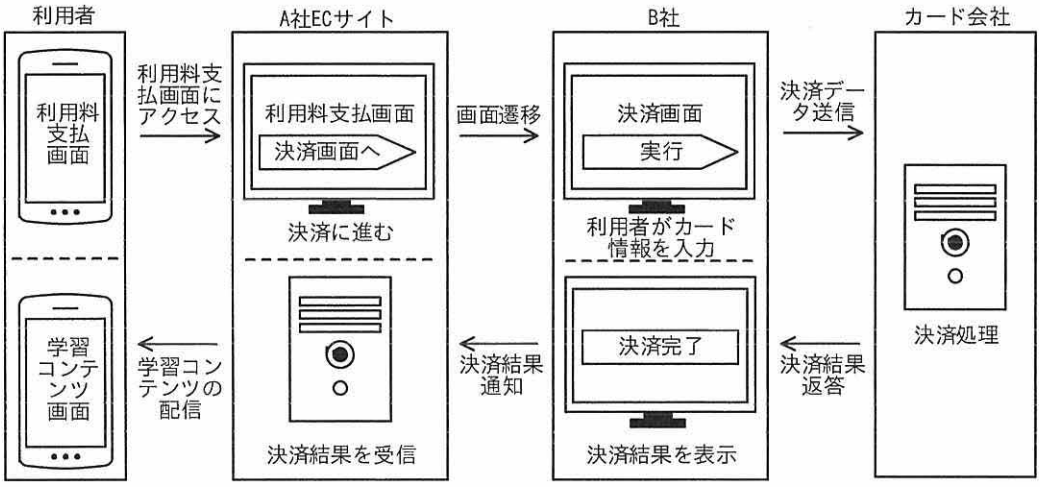

図1　リダイレクト型の非通過方式によるカード決済の流れ

A社は，以前からB社を決済代行会社として利用しており，A社ECサイトで入力されたカード情報をB社が受信してカード決済を行っていた。非保持化に際し，B社がPCI DSSに準拠していたことから，それまでカード情報を取り扱う業務を行っていたカスタマーサービス部は，B社の継続利用を決定した。

非保持化に伴い，カード情報を取り扱う業務がなくなったので，カスタマーサービス部の業務プロセスが変更された。ただし，非保持化前に取り扱ったカード情報を含む重要書類の画像データを，非保持化後も保持している。

なお，紙，画像データ及び音声データの形で記録されたカード情報については，ガイドラインで非保持化後も保持することが認められている。

〔他社でのカード情報漏えい事故の発生〕

非保持化を実施した他のEC加盟店で，カード情報漏えい事故が発生した。攻撃者によってECサイトが改ざんされ，ECサイト上に偽の決済画面へのリンクが作られたことによって，購入者が入力したカード情報が窃取されて不正利用された。さらにバックドアも設置され，攻撃者が継続的に侵入できる状態になっていた。

〔システム監査の実施〕

内部監査部長は，他社でのカード情報漏えい事故を受け，ECサイトを標的にした

攻撃に備えた情報セキュリティ対策及びカード情報保護対策の状況について，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，情報システム部のECサイト管理者にインタビューし，A社EC サイトにおける情報セキュリティ対策の項目，内容及び運用状況を表 1 のようにまとめた。カード決済方式をリダイレクト型の非通過方式にしたことによって，カード情報が A 社 EC サイトを通過しなくなったので，非保持化に伴った情報セキュリティ対策の強化は行われていなかった。また，カード情報を取り扱う業務を行っていたカスタマーサービス部が非保持化に伴って業務プロセスを変更していたことが分かった。

表 1　A 社 EC サイトにおける情報セキュリティ対策の項目，内容及び運用状況（抜粋）

項番	項目	内容	運用状況
1	ネットワーク型侵入防御システムの導入	DMZ にインライン接続して，ファイアウォールで遮断できなかった不正なパケットを検知し，遮断する。	誤検知が頻発し，事象解析などで管理者の作業負荷が高まり，運用に影響が出ている。現在，誤検知が頻発している状態を改善するために“チューニング計画書”を作成している。
2	内部リアルタイム監視型 Web 改ざん検知システムの導入	Web サーバ内の監視対象ファイルの改ざんをリアルタイムで検知し，改ざんされたファイルを自動的に復旧する。	次の各ファイルを監視している。 ・Web 画面の情報を格納しているコンテンツファイル ・Web アプリケーションソフトウェアの構成ファイル ・Web サーバの OS 構成ファイル

〔本調査の結果〕

予備調査の結果を踏まえ，システム監査チームは，情報システム部に加え，内部監査部長の承認を得てカスタマーサービス部も監査対象範囲に含め，本調査を実施した。その結果，次のような事実が判明した。

(1)　非保持化前に取り扱ったカード情報を含む重要書類の画像データが，社内ネットワーク上のカスタマーサービス部の共有フォルダに保存されており，異動によって業務上，当該データを必要としなくなった従業員も参照できる状態であった。こ

れによって，カード情報が窃取され，不正利用されるリスクがある。これらの画像データは訴訟などに備えたものであり，通常業務では使用されていないので，社内ネットワークに接続された環境で保存する必要性は低いと考えられる。

(2) 業務委託契約の締結又は変更時には，契約手続の過程で，A 社“情報セキュリティ規程”に基づく委託先の情報セキュリティ評価を行うことが，“業務委託規程”で定められている。しかし，カード決済方式の変更に伴う契約変更の際に，B 社が PCI DSS に準拠しているという理由で，情報セキュリティ評価が実施されないまま，B 社の継続利用が決定されていた。PCI DSS はカード情報を取り扱う環境を対象とした基準なので，B 社における［ a ］以外の情報セキュリティ対策が，A 社“情報セキュリティ規程”で定める要件を満たさないリスクがある。

(3) ネットワーク型侵入防御システムには，不正なパケットを検知するために，攻撃者によるアクセスに特徴的な受信データのパターンなどを定義した各種のシグネチャが設定されている。誤検知が頻発している状態を改善するための“チューニング計画書”を確認したところ，運用への影響を抑えるために，シグネチャの定義を詳細にして検知対象を絞っていた。しかし，“チューニング計画書”に記載されているシグネチャの定義では異なるリスクが増加する懸念があり，結果的に運用への影響を抑えられない可能性がある。

(4) 内部リアルタイム監視型 Web 改ざん検知システムでは，Web サーバ内の監視対象ファイルの新旧比較を行うので，あらかじめ監視対象ファイルの原本を別途保存しておく必要がある。情報システム部が“改ざん監視対象ファイルリスト”を作成しているが，最終更新日付は 6 か月前であり，最終更新日以降にコンテンツファイルの入換えによって使用されなくなった旧コンテンツファイルが監視対象として残っていた。一方で，使用中のコンテンツファイルの一部が監視対象に含まれていなかった。

設問 1 〔本調査の結果〕(1)について，想定されたリスクに対して，共有フォルダのアクセス権限管理強化のほかに，システム監査チームが備えるべきと考えたコントロールを，35 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)　本文中の［　a　］に入れる適切な字句を 10 字以内で答えよ。

(ii)　想定されたリスクを低減させるために，システム監査チームが行うべき改善提案の内容を，50 字以内で答えよ。

設問３　〔本調査の結果〕(3)について，システム監査チームが想定した，ネットワーク型侵入防御システムにおけるリスクを，理由を含めて 50 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は，当該事実をどのようにして発見したか。“改ざん監視対象ファイルリスト”のほかに入手した監査証拠も含めて，監査手続を 50 字以内で答えよ。

問２　ローコード／ノーコード開発ツールを利用したシステム開発の監査に関する次の記述を読んで，設問に答えよ。

C 社は，自動車部品を製造販売する企業である。販売，購買，生産などを管理する基幹系システムの開発・保守は，システム部が主体となって行っている。一方，業務効率の向上を目的とした簡易なシステム（以下，アプリという）については，利用部門が主体となって，プログラムのコードを書かなくても開発できるローコード／ノーコード開発ツール（以下，開発ツールという）を利用して開発を行ってきた。

C 社の CIO は，開発ツールを利用したアプリの開発（以下，アプリ開発という）には利点があることは認識していた。一方で，アプリ開発の管理ルールが定められていなければ，開発者の異動や退職などによって保守できなくなるアプリが発生するといったリスクがあることを懸念していた。そこで CIO は，システム部にアプリ開発の管理ルールを作成するよう指示し，システム部のシステム企画課に設置された事務局が管理ルール案を作成した。

〔アプリ開発の状況〕

営業部などの各利用部門でクラウドサービス事業者と契約して開発ツールを導入し，データの照会や集計など，簡易で高い可用性を求められないアプリを中心に開発している。

〔システム監査の目的と対象部門〕

監査部では，アプリ開発の状況を監査することにした。監査目的は，管理ルール案によってアプリ開発のリスクが低減できるかどうか，という点である。監査部は，アプリ開発を積極的に行っている営業部，及び管理ルール案を作成したシステム企画課を対象に予備調査を実施した。

〔予備調査の結果〕

監査部が予備調査を行った結果，次のことが分かった。

1．営業部長へのインタビュー結果

(1)　アプリ開発は，短期間・低コストで，利用部門のニーズに合致したアプリが開発できるという利点がある。

(2) 開発ツールの利用方法に習熟してもらうために，営業部の全部員に利用者用IDとは別に開発用IDを付与している。利用者用IDでは，権限に応じてデータの参照・更新の範囲が設定される。一方，開発用 ID では，開発を効率よく進めるために，本番環境のデータの参照が可能となる設定にしている。

2. システム企画課長へのインタビュー結果

(1) アプリ開発の利点を生かし，かつ，リスクを低減するために，必要最小限の管理ルールの作成を行う。

(2) 事務局が作成した管理ルール案の概要を表 1 に示す。システム部が開発するアプリについても，開発コストの削減や開発期間の短縮を目的として，開発ツールの利用を検討している。

表1 管理ルール案の概要（抜粋）

項番	項目	内容
1	適用対象	・利用部門によるアプリ開発の場合，アプリの利用者は部門内であることを原則とする。 ・個人情報を扱うアプリは，利用部門によるアプリ開発の対象外とする。
2	開発申請手続	・利用部門によるアプリ開発の場合，利用部門からの開発申請に基づき，開発可否を事務局が判断する。 ・次の項目を含む開発判断基準を設ける。 - 使用するデータの種別 - 想定されるデータ量（マスターファイル，トランザクションなど） - 処理の複雑度（高・中・低）
3	テスト	・データ量が多い，又は関連データが多いアプリの開発は，テストの実施基準を設ける。
4	ID管理	・開発用IDをシステム部で管理する。
5	リリース管理	・リリース手順及び利用者への周知手順を作成する。
6	開発後の管理	・開発したアプリは，管理台帳に登録して事務局で一元管理する。 ・必要最小限の設計ドキュメントを作成する。

(3) これまで開発されたアプリの中から，他のアプリでも利用可能なアプリの部品をシステム部が選定し，動作確認や分類を行ってテンプレートとして登録する。

今後開発するアプリは，それらのテンプレートを可能な限り利用する。開発ツールの利用方法や登録したテンプレートの利用ルールについて，利用部門に対して説明会を実施する予定である。

〔リスクの識別〕

監査部は，予備調査の結果を踏まえ，アプリ開発のリスクを識別し，それに対応する管理ルール案の内容を洗い出した。アプリ開発のリスクと管理ルール案の内容を表2に示す。

表2　アプリ開発のリスクと管理ルール案の内容（抜粋）

項番	分類	リスク	管理ルール案の内容
1	企画・開発段階	(1)　利用部門がそれぞれ独自にアプリを開発し，不要なアプリが乱立する。	・アプリの開発判断基準を作成し，周知する。
		(2)　必要な設計ドキュメントが作成されなかったり，テストが不足したりして，品質が低下する。	・必要最小限の設計ドキュメントを作成する。
		(3)　［　ア　］	・開発用 ID をシステム部で管理する。 ・開発ツールの開発用 ID の登録は申請に基づき行う。
2	運用・保守段階	(1)　開発担当者の異動や退職によって，アプリの仕様が分からず保守ができなくなる。	・必要最小限の設計ドキュメントを作成する。 ・テンプレートの利用ルールを定める。
		(2)　システム部が開発ツールを利用して開発するアプリに管理ルール案を適用した場合，必要なセキュリティ機能が実装されない。	・個人情報などの重要データにアクセスした際の操作内容を操作ログに記録する。

〔監査手続書の作成〕

監査部はリスクの高い項目について，本調査で確認すべきことを整理し，監査手続書を作成した。その概要は次のとおりである。

(1)　営業部長へのインタビュー結果(1)を踏まえ，表1の管理ルール案の適用によってアプリ開発の利点が損なわれる可能性がないか，管理ルール案の内容を確認する。

(2) 表 2 項番 1(1)について，開発判断基準がリスクを低減する内容になっているか，開発の可否を判断するのに必要な項目に漏れがないことを確認する。

(3) 表 2 項番 1(2)についてシステム部に確認したところ，システム部で利用している開発標準を流用して進捗管理や品質管理を行う予定であるとのことであった。しかし，そのまま流用するのは適切ではない場合もあることに留意する。

(4) 表 2 項番 1(3)について，開発用 ID を申請に基づいて必要最小限の部員に付与することでリスクの低減が期待できることに留意する。

(5) 表 2 項番 2(1)について，設計ドキュメントの作成基準として，記載が必要な項目の一覧と標準フォーマットが示されている。この作成基準の適用が実効性のあるものかどうかを事務局に確認する。

(6) 表 2 項番 2(2)について，開発ツールには，画面操作を行った利用者用 ID，操作内容などを記録した操作ログを取得する機能が備わっている。ただし，操作ログを取得するだけでは不十分なので，その他に必要なログの保全の要件についてもルールが定められていることを確認する。

設問 1 〔監査手続書の作成〕(1)について，監査部が考えた，アプリ開発の利点が損なわれる可能性を 35 字以内で答えよ。

設問 2 〔監査手続書の作成〕(2)について，検討されている開発判断基準に追加すべきと思われる項目を答えよ。

設問 3 〔監査手続書の作成〕(3)について，そのまま流用するのが適切ではない場合とはどのような場合か。25 字以内で答えよ。

設問 4 〔監査手続書の作成〕(4)について，監査部が考えたリスク［ ア ］を 35 字以内で答えよ。

設問 5 〔監査手続書の作成〕(5)について，監査部が事務局に確認しようとしている内容を 45 字以内で答えよ。

設問 6 〔監査手続書の作成〕(6)について，監査部が確認すべき具体的な要件を 30 字以内で答えよ。

問３　人材管理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。

サービス業のＤ社は，従業員が５千人を超え，グローバルな事業拡大とともに，職務に基づいた人材管理制度の導入を進めている。それに伴い，２年前に人材管理の業務効率と利便性の向上を目的として，人材管理システムを再構築した。監査部では，再構築の目的を実現できるように人材管理システムが活用されていることを確かめるために，システム監査を実施することにした。

〔人材管理システムの概要〕

人材管理システムは，グローバルで実績があるクラウドサービスを利用して再構築されており，人事情報管理，目標管理，スキル管理及びタレント管理の四つの機能がある。人材管理システムの概要を図１に示す。

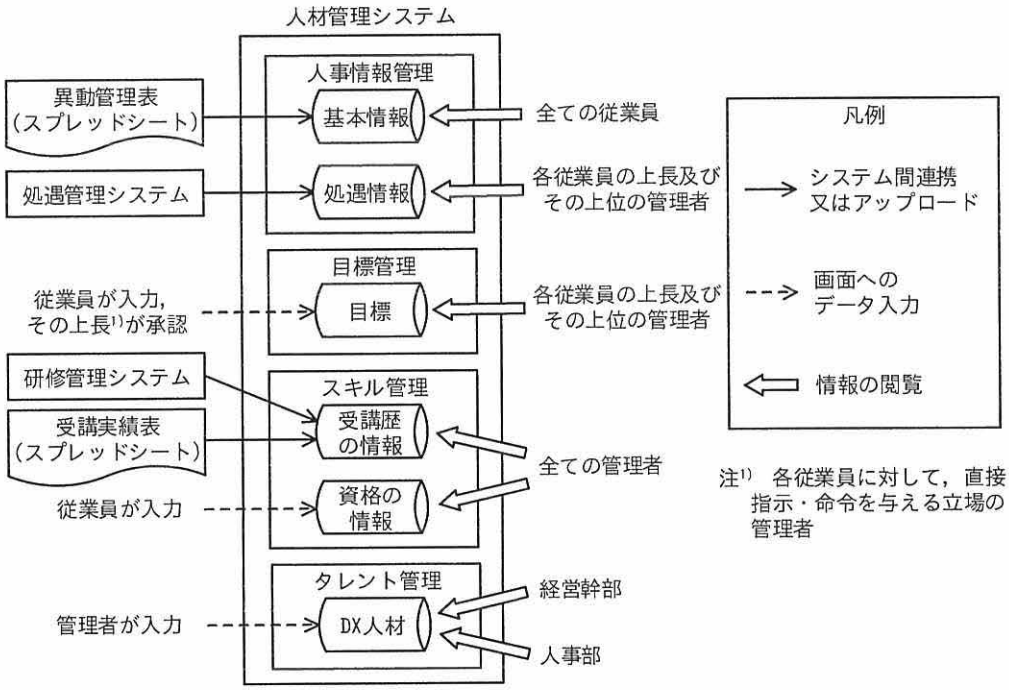

図１　人材管理システムの概要

〔人事部へのインタビュー〕

監査チームは，予備調査として，人材管理システムの説明資料を確認するとともに，人事部の企画課長にインタビューを行った。その結果は次のとおりである。

(1)　人事情報管理

再構築前から，各従業員の部署・役職・連絡先は全ての従業員が閲覧できたが，人材管理システム再構築によって，各従業員の上長の役職と氏名についても，“基本情報”として，全ての従業員が閲覧できるようになった。人事異動時には，人事部がスプレッドシートで作成した“異動管理表”のデータを人材管理システムへアップロードし，“基本情報”を更新する。現在はアップロードの前に“異動管理表”へ上長の役職と氏名を手作業で入力しており，その作業に数日を要している。

一方で，処遇制度上の等級などは“処遇情報”として，各従業員の上長及びその上位の管理者だけが閲覧できるように制限している。

(2)　目標管理

再構築前は，人事部がスプレッドシートで作成した目標管理のための帳票に各従業員が入力し，上長が承認して人事部へ提出していた。再構築後は，各従業員が画面に入力し，上長が承認することで目標管理が効率的に行えるようになった。

(3)　スキル管理

D 社では，人材管理システム再構築と並行して，社内の職務について職務記述書を作成し，その中で必要スキルを明示し，従業員のスキル向上を促している。そのため，人材管理システムにおいて，各従業員の社内研修の受講歴と取得した公的な資格の情報を管理しており，その情報は上長を含む全ての管理者が閲覧できる。

①　受講歴の情報

人事部が主催する研修の受講歴は研修管理システムで管理しており，人材管理システムへのデータ連携によって日次で自動更新される。そのほかに各事業部門が主催する研修があり，その受講歴は，各事業部門の研修担当者がスプレッドシートで作成した“受講実績表”のデータを“更新手順書”に基づいて人材管理システムへアップロードして，更新される。受講歴は，更新の都度，従業員へ通知が届き，本人が内容を確認している。結果として，従来は分散して把握しにくかった受講歴の情報が人材管理システムの中で一元的に参照できるようになった。

②　資格の情報

再構築前は人事部で管理していた資格取得の情報は，再構築後には，全ての管理者が閲覧できるようになった。従業員が資格を取得した場合は，設定されている資格マスターから選択して登録する。資格マスターにない資格を取得した場合

は，追加資格として従業員が資格名称を入力して登録する。資格名称の入力については決まりがなく，従業員が略称などで入力する場合もある。

(4)　タレント管理

昨年から，各部署の管理者がDX推進スキルをもつ人材（以下，DX人材という）を登録することになった。DX人材については選定基準が定められており，部署ごとの登録人数は，経営幹部の関心事項として管理者に対する評価項目になっている。

(5)　人材管理システムの利用状況の報告

人材管理システムの利用者数の推移や再構築の効果などについては，人事部が年1回，“利用状況報告書”を作成して経営幹部へ報告している。

〔情報システム部へのインタビュー〕

情報システム部で人材管理システムの運用を行っているグループでは，定期的に従業員の要望などを調査している。監査チームは予備調査として，そのグループの課長に調査結果についてインタビューした。その結果は次のとおりである。

(1)　多数の従業員が異動する際には，人材管理システムの“基本情報”へ異動の結果が反映されるまでに数日を要する場合があり，業務に支障が生じることがある。

(2)　特定の資格をもつ従業員が必要な場合には，従来は人事部に問い合わせていたが，人材管理システム再構築後は，管理者は自ら検索できるようになった。ただし，経営や技術の動向に対応して新設された資格について取得者を検索した場合には，実際には取得していても検索結果として表示されない場合がある。

(3)　従来は人事部を介して行っていた人材管理業務の多くが，人材管理システムの再構築後は，各職場の管理者や従業員が自ら行えるようになった。その結果，便利になったこともあるが，一方で人事に関わる情報の入力やその確認など，新たに各職場で行うことになった作業も多いと感じている。

〔本調査のための検討〕

予備調査の結果を基に，監査チームは本調査のための検討を行った。その内容は次のとおりである。

(1)　人事情報管理

①　多数の従業員が異動する際には情報の閲覧についてリスクがあるので，閲覧権

限が異動日に更新されることを関係者に確認する。

② “基本情報”が適時に更新されない問題への対処が検討されているかどうかを，人事部と情報システム部に確認する。

(2) スキル管理

① 受講歴の情報は，更新内容を本人が確認しているので正確性は確保できているが，それだけで網羅性が確保できているとはいえない。そのため，“更新手順書”を閲覧して作業内容を確かめる必要がある。

② 新設された資格の取得者を検索する際に支障が生じるリスクを低減する取組が検討されているかどうかを，人事部に確認する。

(3) タレント管理

入力された情報の用途から，DX 人材の選定基準に適合しない者を管理者が登録するリスクがあると考えられる。そのため，管理者の上長が，管理者の登録した対象者が選定基準に適合していることを確かめた上で承認していることを，人事部に確認する。

(4) 人材管理システム再構築の効果

業務効率向上の効果が過大に算定されている可能性があるので，“利用状況報告書”を閲覧して効果の算定内容を確認する。

設問1 〔本調査のための検討〕(1)の①について，監査チームが懸念したリスクを 35 字以内で答えよ。

設問2 〔本調査のための検討〕(1)の②について，監査チームが確認すべき内容を 35 字以内で答えよ。

設問3 〔本調査のための検討〕(2)の①について，監査チームが“更新手順書”を閲覧して確かめるべき具体的な内容を 35 字以内で答えよ。

設問4 〔本調査のための検討〕(2)の②について，監査チームが確認すべき取組の内容を 40 字以内で答えよ。

設問5 〔本調査のための検討〕(3)について，監査チームが想定したリスクを，40 字以内で答えよ。

設問6 〔本調査のための検討〕(4)について，監査チームが確認すべき内容を 30 字以内で答えよ。

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。