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。

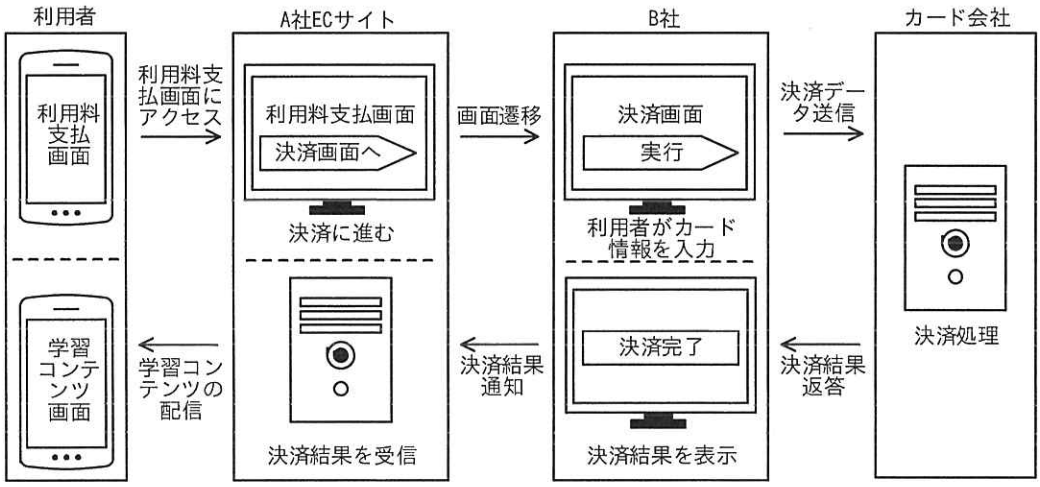

図１　リダイレクト型の非通過方式によるカード決済の流れ

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。