平成 26 年度 春期 情報セキュリティスペシャリスト

＜午後Ⅱ 解答･解説＞

＜問1＞ 百貨店事業におけるクレジットカード情報の安全な管理

■設問 1

〔試験センターによる解答例〕
VIP 会員担当が VIP ファイルに PAN を記録している点（27 字）

図 3 の方針 1.では，PAN の業務上不要な利用や保存，業務上の利便性だけの理由による利用や保存を禁止している。これを踏まえて〔会員サポート課の業務内容〕を見ると，「……VIP 会員の PAN，会員名，過去の問合せ履歴などを PC 内の VIP ファイルというファイルに記録している。会員管理システムでも同様の記録や管理は可能であるが，VIP 会員担当は，VIP ファイルの方が使いやすいと感じており，……」という記述がある。これは，方針 1.が禁じている「PAN の業務上不要な利用や保存」「業務上の利便性だけの理由による利用や保存」に該当する。

■設問 2

〔試験センターによる解答例〕
(1) イ
(2)
作業：ステータスコード確認作業（12 字）　又は　特別作業-2（6 字）
状態：PAN を表示しない状態（11 字）
(3)
方式名：方式 1
項目番号：3.4.1
動作：OS へのログインの成功後のデータアクセス時の自動的なデータの復号（32 字）
内容：復号キーがユーザアカウントと関連付けられていない。（25 字）
(4) 主キーである PAN に索引が設定されており暗号化できないから（29 字）
(5)
a：方式 3
b：方式 2
c：方式 3
d：方式 2

(1) 表 2 の保守課の業務概要にあるように，特別作業-1 では，運用課から作業指示書で指示された PAN をキーとして入力し，暗証番号の変更作業を行う必要がある。そのため，

特別作業-1 の DB の利用者 ID に対し，オーソリテーブルの PAN 列の復号権限を**与える**必要がある。
一方，特別作業-2 では，運用課から作業指示書で指示された決済処理番号をキーとして入力し，ステータスコード確認作業を行うが，この作業において PAN は必要ない。そのため，特別作業-2 の DB の利用者 ID に対し，決済集計テーブルの PAN 列の復号権限を**与える**必要はない。

(2) 保守課が方式 3 を採用することにより，特別作業-2 のステータスコード確認作業では，PAN を表示することなく作業を行うことが可能となる。これにより，図 3 の方針 2.にある「業務上 PAN の表示が必要な場合を除き，PAN の表示はしない」に従った対応をとることができる。

(3) 図 4 の「PCI DSS 要件」の 3.4 は，「すべての保存場所で PAN を少なくとも読み取り不能にする」ことである。これに対し，表 3 の方式 1～3 はいずれも暗号化を前提とした方式であり，PAN に索引を設定している場合などテーブルの仕様によっては採用できないケースはあるものの，3.4 の要件に違反する内容ではない。
続く「PCI DSS 要件」の 3.4.1 では，「ディスク暗号化が使用される場合，論理アクセスはネイティブなオペレーティングシステムの認証およびアクセス制御メカニズムとは別に管理する必要がある」「復号キーがユーザアカウントと関連付けられていない」といった内容となっているが，表現が異なるだけでこの 2 つはほぼ同じことを言っている。これに対し，表 3 の方式 1 では，「OS の利用者 ID のログインに成功すると，ハードディスクの全てのデータがアクセス時に自動的に復号されるようになる」とあり，3.4.1 の要件に違反している。方式 2，方式 3 では，「DB へのログインは OS の利用者 ID とは別の DB の利用者 ID で認証される」とあることから，3.4.1 の要件に違反することはない。
また，図 4 の「PCI DSS 要件」の 11.1 は無線 LAN のアクセスポイントに関する内容であり，表 3 の方式 1～3 とは無関係である。

(4) 表 3 の方式 3 の説明に「索引を設定した列は暗号化できない」とあるが，図 2 の会員管理テーブルの構造を見ると，**主キーである PAN に索引が設定されており，暗号化できない**ことがわかる。そのため，会員管理テーブルに方式 3 を採用した場合には図 4 の「PCI DSS 要件」の 3.4 にある「すべての保存場所で PAN を少なくとも読み取り不能にする」を満たすことができない。

(5) 問題文の下線③にあるように，方式 3 を採用して PAN を暗号化することで，L 社の PAN の取扱方針に，より一層従った状態で作業できるようになる。そのため，可能な限り方式 3 を採用し，方針 3 が困難な場合には方式 2 を採用する（PCI DSS の要件を満たさない方式 1 は極力避ける）ようにするべきである。しかし，前述のように方式 3 には「索引を設定した列は暗号化できない」という制限があるため，それらを踏まえて

採用する方式を決定する必要がある。
まず,決済集計テーブルについては図２にあるようにPANに索引は設定されておらず,表１の決済集計システムの概要からも PAN を暗号化して保存可能と判断できるため,方式３を採用する。
ポイントテーブルについてはPANに索引が設定されており，方式３が採用できないため，方式２を採用する。
オーソリテーブルについてはPANに索引は設定されておらず，表１のオーソリシステムの概要からもPANを暗号化して保存可能と判断できるため，方式３を採用する。
会員管理テーブルについては前述のように方式 3 を採用することができないため，方針２を採用する。

■設問３

〔試験センターによる解答例〕
(1) セキュリティポリシに反してワイヤレスアクセスポイントが設置されること
(2) e：5GHz 帯　又は　IEEE802.11a

(1) 図４の「PCI DSS 要件」の 11.1 では,ワイヤレスアクセスポイントの存在をテストし,承認されているものと承認されていないものを検出し,識別することが求められている。また，問題文の冒頭〔ハウスカードサービスのシステム概要〕にあるように，L 社ではセキュリティポリシによって全システムで無線 LAN の利用が禁止されている。
これらを踏まえると，「セキュリティ上の問題につながる事象」に該当するのは，L 社の**セキュリティポリシに反してワイヤレスアクセスポイントが設置されること**である。
ここで問われているのは「セキュリティ上の問題そのもの」ではなく，あくまでも「セキュリティ上の問題につながる事象」であることに留意する必要がある。

(2) 無線 LAN の規格として広く普及しているものとして，2.4GHz 帯の IEEE802.11b（伝送速度 11Mbps），IEEE802.11g（同 54Mbps）のほか，**5GHz 帯**の **IEEE802.11a**（同 54Mbps）などがある。図５の「W-AP スキャンの結果」を見ると，IEEE802.11a については検査ができていない。

■設問４

〔試験センターによる解答例〕
(1) 電話受付時の会員の特定を PAN ではなくお客様コードで行うように改善できる。
(2)
f：お客様コード，ポイント値，最終更新日
g：お客様コード，会員名，住所，電話番号，性別

(1) 表２にあるように，従前の会員サポート課の業務では，会員からの電話受付時に，会員を特定するために PAN，会員名，住所を聞き，会員管理システムで PAN をキーとして検索し，本人であることを確認の上，会員情報の参照や変更を行う，とある。新たな会員管理システムでは，クレジットカードごとに一意に採番したお客様コードをキーに会員情報を検索できるため，PAN コードを使用する必要がなくなる。これにより，図３の方針 1.「PAN の業務上不要な利用や保存はしない」に従い，会員からの**電話受付時の会員の特定に PAN ではなくお客様コードで行うように改善することが可能となる**。

(2) 前述のように，従前のポイントテーブル，会員管理テーブルでは PAN に索引が設定されているため，表３の方式 3 を採用することができなかった。新システムでは，PAN とお客様コードを相互に関係付けるテーブルをもつ変換 DB により，従前のポイントテーブル，会員管理テーブルで主キーとなっていた PAN をお客様コードに置き換え，PAN を削除することが可能となる。これにより，図３の方針 1.「PAN の業務上不要な利用や保存はしない」に従ったセキュアなテーブルの構造を実現できる。

＜問2＞ 金属加工業者におけるデータ管理

■設問１

〔試験センターによる解答例〕
(1) ファイルが書き換えられる可能性があるから（20 字）
(2) バックアップメディアに改ざんされたファイルが含まれている可能性があるから（36 字）
(3) D 社で定めたソフトウェア（12 字）

(1) ウイルス感染や攻撃者による侵入・改ざんなどの被害を受けた状態のサーバには，シャットダウン時や再起動時にファイルを書き換え，侵入や攻撃の痕跡を消したり，偽装したりする仕掛けなどが施されている可能性が高い。そのため，当該サーバをそのままシャットダウンすると，メモリやディスクにあるファイルが書き換えられてしまい，侵入経路，攻撃手法，原因などの調査が困難になる可能性がある。

(2) 問題文の〔情報システム課が運用している機器の概要〕を見ると，D 社では，DMZ に設置されたサーバの OS とプログラムについては年３回の脆弱性修正プログラムの適用前及び適用後にバックアップを行っており，同サーバのデータについては日次でバックアップを行っていることがわかる。
続いて図２の調査結果の概要を見ると，1.2 に「調査開始日の４週間以上前に改ざんが行われた可能性が高い」とあることから，上記の**バックアップメディアには改ざんされたファイルが含まれている可能性が高い**。こうしたことから，G 社はバックアップ

メディアからの復元ではなく，OS，Web サーバプログラム及びコンテンツ全文検索機能のプログラムの最新版をインストールし，コンテンツは E 社が納入したものを用いて復元することを推奨したと考えられる。

(3) 問題文の〔情報システム課が運用している機器の概要〕にあるように，D 社では，OS が Windows の場合は Q 社のウイルス対策ソフトと R 社の画像閲覧ソフトの導入を必須としている。
一方，脆弱性修正プログラムの適用状況を見ると，事務サーバ，設計管理サーバ及び CAD/CAM システムでは,OS の脆弱性修正プログラムがリリースされるとその週末に適用している，とあり，PC については，OS の脆弱性修正プログラムがリリースされると自動的に適用される，とある。つまり，脆弱性修正プログラムの適用対象は OS のみであり，ウイルス対策ソフトや画像閲覧ソフトについては適用対象外となっている。図２の 2 に「画像閲覧ソフトの脆弱性修正プログラムは，調査開始日の３週間前に，R 社の Web サーバからダウンロードできるようになっていた」とあるように，これら **D 社で定めたソフトウェア**についても脆弱性修正プログラムの適用対象とする必要がある。

■設問２

〔試験センターによる解答例〕
(1) SSH（3 字）
(2)
項目名：送信元
変更後の内容：E 社

(1) 「暗号や認証の技術を利用して，リモートコンピュータとの間でファイル転送や OS へのログインを安全に行うことができるプロトコル」に該当するのは **SSH**（Secure SHell）である。
SSH は，SSL/TLS と同様にトランスポート層とアプリケーション層で暗号化を行う方式である。当初は rlogin，rsh など BSD 系 UNIX を起源とする r 系のコマンドや，X11，Telnet などを安全に行うための手段として使用されていたが，現在では FTP，POP3 など，暗号化機能を備えていないプロトコルを安全に使用する技術として広く使用されている。

(2) 問題文の冒頭に「E 社の担当者は，E 社からインターネット経由で，FTP を使用してコンテンツを更新する」とあり，表２の項番 4 はこれを許可するためのフィルタリングルールであるが，送信元の設定を見ると「全て」となっていることがわかる。このままでは，E 社に限らず全ての送信元からのアクセスを許可してしまうことになるため，非常に危険である。対応としては，項番 4 の「**送信元**」を，「全て」から「**E 社**」に変更するべきである。

■設問３

〔試験センターによる解答例〕
課：経理課
不都合の内容：ブラウザのアドレスバーに表示される Web サイトの運営者名を確認できなくなる。（38 字）
(2)
b：OS ベンダの Web サーバ
c：Q 社の Web サーバ
d：R 社の Web サーバ
※b～d は順不同。

(1) 問題文の〔取引時の情報管理〕に D 社の設計課，製造課，経理課の業務に関する記述があるが，これらの中でプロキシサーバの HTTPS 通信対応機能に関係があるのはインターネットバンキングサービスを利用している経理課である。U 銀行のインターネットバンキングサービスでは EV SSL 証明書が使用されており，経理課では同サービスにログインする前に，ブラウザのアドレスバーに表示される Web サイト運営者名が U 銀行であることを確認している。
ところが，表 4 にあるように，プロキシサーバの HTTPS 通信対応機能を使用すると，接続元とプロキシサーバの間，及びプロキシサーバと接続先との間でそれぞれ独立の HTTPS 通信が確立される。したがって，同機能を使用して経理課の担当者が U 銀行のインターネットバンキングサービスを利用しようとすると，担当者のブラウザには，U 銀行の EV SSL 証明書ではなく，プロキシサーバが作成した証明書が送られてくる。そのため，**経理課の担当者がブラウザのアドレスバーに表示される Web サイトの運営者名を確認できなくなる**という不都合が生じる。

(2) 表 6 及び表 7 の URL 制御ルールの修正の意図は，事務サーバ，設計管理サーバ，CAD/CAM システムに対しては P 社提供リストによる URL 制御ではなく，ユーザ定義リストによる URL 制御を行うことで，必要最小限の Web アクセスに制限することである。表 7 のユーザ定義リスト 1 には，その必要最小限の接続先の URL を登録するが，これに該当するのは，OS，ウイルス対策ソフト，画像閲覧ソフトの更新や脆弱性修正プログラムのダウンロードのための通信である。具体的には，OS の脆弱性修正プログラムは「**OS ベンダの Web サーバ**」より，ウイルス対策ソフトのウイルス定義ファイルは「**Q 社の Web サーバ**」より，画像閲覧ソフトの脆弱性修正プログラムは「**R 社の Web サーバ**」よりダウンロードする必要があるため，これらを表 7 のユーザ定義リスト 1 に登録する。

■設問４

〔試験センターによる解答例〕
e：公開 Web サーバ
f：インターネット
g：全て

公開 Web サーバに感染したウイルスから，攻撃者が用意したサーバへの通信を検出することが目的であるから，［e］の送信元には「**公開 Web サーバ**」が入る。攻撃者が用意したサーバはインターネット上に存在するが，具体的なアドレス等は不明であるため，［f］の宛先は「**インターネット**」としておく。ウイルスからの通信はプロトコルを限定せずに検出する必要があるため，［g］のサービスは「**全て**」とする。

■設問５

〔試験センターによる解答例〕
(1) h：クライアント（6 字）
(2) CAD データ送信時の通信の暗号化が自動的に行われること（27 字）
(3)
・メールサーバを経由した F 社のメールサービスのサーバへの SMTP 通信（33 字）
・プロキシサーバを経由した P 社提供リストにないサーバへの FTP, HTTP 及び HTTPS 通信（44 字）
(4) プロキシサーバを経由しないインターネット上のサーバへの通信（29 字）

(1) 専用装置との間で HTTPS 通信を行う場合に使用できる認証方式であり，パスワード認証に加えて行うものであるから，該当するのはディジタル証明書を用いた**クライアント認証**である。なお，ディジタル証明書はその用途や場面によって「サーバ証明書」「クライアント証明書」「SSL 証明書」「S/MIME 証明書」「X.509 証明書」「公開鍵証明書」「電子証明書」など，様々な呼称があるため注意が必要である。クライアント認証に用いるディジタル証明書は通常「クライアント証明書」と呼ばれる。

(2) 問題文の〔取引時の情報管理〕にあるように，従来 CAD データを送付する際には，ウイルススキャンを行った後に暗号化した上で，メールに添付して送付，もしくは DVD-R などに記録して宅配便で送付のいずれかの方法で行い，復号用のパスワードを CAD データとは別にメールで送付していた。
これに対し，専用装置を用いた CAD データの送信では，メールへの添付による送信の場合とは異なり，誤送信が防止でき，復号用パスワードを別メールで送付する必要

がなくなるほか，HTTPS によって **CAD データ送信時の通信の暗号化が自動的に行われること**が大きな利点として挙げられる。これは，問題文の〔専門加工業者への CAD データ送信方法の検討〕にある「安全でかつ注文から納品までの時間を短縮できる電子的な方式」にそのまま合致する。

(3) 「ウイルスの活動による PC からインターネットへの通信のうち，止めることはできないがログの分析によって検出できる通信」とは，表２の FW-A のフィルタリングルールによって許可されている PC からインターネットへの通信であり，かつログを取得しているものということになる。表２からこれに該当するものを探すと，まず項番 6 及び項番 7 の，PC からプロキシサーバを経由したインターネットへの FTP，HTTP 及び HTTPS 通信が該当することがわかる。ただし，プロキシサーバには P 社提供リストによる URL フィルタリング機能があり，同リストにあるサーバへの通信は止めることができるため，正しくは「**プロキシサーバを経由した P 社提供リストにないサーバへの FTP，HTTP 及び HTTPS 通信**」である。

その他に該当するものとして，表２の項番 9 及び項番 3 の「**PC からメールサーバを経由した F 社のメールサービスのサーバへの SMTP 通信**」がある。これらはいずれも PC からインターネットへの通信であり，止めることはできないが，ログの分析によってウイルスの活動を検出することができる。

(4) 「ウイルスの活動による PC からインターネットへの通信のうち，止めることはできるがログを分析しても検出できない通信」とは，表２の FW-A のフィルタリングルールによって拒否されている PC からインターネットへの通信であり，かつログを取得していないものということになる。上記(3)で述べたように，PC からプロキシサーバやメールサーバを経由したインターネット上のサーバへの通信は，FTP, HTTP, HTTPS, SMTP について，P 社提供リストにないことを前提として許可しており，ログも取得している。一方，これに該当しない，PC から**プロキシサーバやメールサーバを経由しないインターネット上のサーバへの通信**については，表２の項番 10 によって拒否され，ログも残らない。したがって，「止めることはできるがログを分析しても検出できない」ということになる。