

# サンプル問題 午前 問題

ここでは、IPAが公開した「情報セキュリティマネジメント試験」のサンプル問題を取り上げます。出題レベルの指針となる問題ですので、ぜひチャレンジして、解けなかった問題はじっくり解説を読み理解を深めてください。



## 問 1

情報セキュリティにおいて、業務で利用しているシステムに影響を与える事象a～dのうち、脅威によって直接的に引き起こされたものだけを全て挙げたものはどれか。

- a CD-ROMの劣化によって、保存しておいた顧客リストが利用できなくなる。
- b 自然災害による停電や断水によって、システムが利用できなくなる。
- c 定期的なメンテナンスによって、メンテナンス期間中はシステムが利用できなくなる。
- d メールサーバの設定ミスによって、メールサーバと連携して動作する自動問合せ業務システムが利用できなくなる。

ア a, b

イ a, b, d

ウ b, c

エ c, d



## 問 2

デジタルフォレンジックスの活動に含まれるものはどれか。

- ア インシデントの原因究明に必要となるデータの収集と保全
- イ 自社システムを攻撃して不正侵入を試みるテストの実施
- ウ 定期的なウイルスチェック
- エ パスワード認証方式からバイオメトリクス認証方式への切替え



## 問 3

電子的な文書ファイルの機密性を維持するために使用するセキュリティ対策技術として、適切なものはどれか。

ア アクセス制御

イ タイムスタンプ

ウ デジタル署名

エ ホットスタンバイ

## 解説

### 問 1 脅威

情報セキュリティにおける**脅威**とは、情報システムや情報資産に損害を与える原因のことです。

脅威は、主に次の三つに分類できます。

- **人的脅威**：人間の意図的な攻撃、または偶発的なミスによって発生する脅威です。従業員が社内の機密情報を密かに持ち出したり、メールの誤送信によって個人情報を外部に流出させたりすることなどが該当します。
- **技術的脅威**：不正アクセス、マルウェア、DoS攻撃などの技術的な手法によって、情報システムや情報資産に損害が与えられることです。
- **物理的脅威**：地震などの災害や不審者の侵入などによって、情報システムを構成する機器などが物理的に破壊さ

れたり、それが原因で情報資産にアクセスできなくなったりすることです。

aのCD-ROMの劣化は物理的脅威に分類されます。bの自然災害による停電や断水は物理的脅威に分類されます。dのメールサーバの設定ミスは人的脅威に分類されます。cはシステムの運用を継続するための定期的なメンテナンス作業であり、情報システムや情報資産に損害を与えようとしていないので、脅威ではありません。

以上から、**イ**が正解です。

## 問 2 デジタルフォレンジックス

**デジタルフォレンジックス**とは、コンピュータ犯罪(不正アクセスなど)やインシデント(情報システムに影響を与える事象)に対する科学的調査のことです。不正アクセスを法的に立証するために必要な情報を収集します。よって、インシデントの発生原因を究明するためのデータの収集・分析(**ア**)が正解です。

○ **ア** 正解です。

× **イ** ペネトレーションテストの説明です。

× **ウ** ウイルス感染を検知するための措置です。

× **エ** デジタルフォレンジックスでは、認証方式を切り替えるのではなく、不正アクセスなどの情報を収集します。

## 問 3 機密性

情報セキュリティを確保するために必要な次の三つの要素を、**情報セキュリティの3要素**といいます。

① **機密性**：情報にアクセスする権限のない者に、情報を不正に読まれないようにすること

② **完全性**：情報の内容が正確であり(矛盾していないこと)、改ざんなどがされないようにすること

③ **可用性**：アクセス権限のある者が、いつでも情報にアクセスできるようにすること(障害などが発生しても情報にアクセスできるようにすること)

電子的な文書ファイルの機密性を維持するには、文書ファイルを暗号化して第三者に読まれないようにしたり、適切なアクセス権限をもつ者しか参照できないようにしたりすることが有効です。よって、**ア**のアクセス制御が正解です。

○ **ア** 正解です。

× **イ** タイムスタンプは、ある時刻においてファイルが存在しており、かつ内容が改ざんされていないことを保証するための技術で、完全性を維持するために使用されます。

× **ウ** デジタル署名は、ファイルの作成者の本人性の証明や改ざんを検知するための技術で、完全性を維持するために使用されます。

× **エ** ホットスタンバイは、本番系と待機系の二つのシステムを用意して、本番系に障害が発生しても、すぐに待機系に切り替えて業務を継続するための手法で、可用性を維持するために使用されます。

○ 解答 ○

問 1 **イ**

問 2 **ア**

問 3 **ア**

# サンプル問題 午後 問題

**問 1** 内部不正防止のためのログのレビューに関する次の記述を読んで、設問1～6に答えよ。

A社は、高級化粧品を個人に販売しており、従業員は100人である。A社は総務部、情報システム部、購買部、営業部から成り、営業部には60人の従業員が属している。営業部は企画課、営業1課～4課から構成される。営業部のIT環境は次のとおりである。

- ・営業部員は全員A社所有のノートPCを使用している。
- ・社内ネットワークに接続された、スキャナ用の共用PCが1台設置されている。
- ・営業部員は、社外から社内のシステムを使用する際には、ノートPCをインターネット経由でA社のVPNサーバに接続して使用している。

なお、A社では、インターネットの使用を広く認めており、Webメールやファイル共有サービスなどを含め、サービスの使用を制限していない。

A社では、顧客情報などの機密情報の漏えいを防ぐ目的で、退職後も一定期間有効な損害賠償条項を含む機密保持契約を全従業員と締結している。

A社では、営業部員が表計算ソフトを使用してノートPCで顧客情報を管理していたが、顧客管理パッケージ(以下、Bシステムという)を社内を導入し、そこで集約して管理することを決定した。Bシステムに関する方針は次のとおり定めた。

- ・Bシステムの主管部門は営業部である。
- ・Bシステムを使用するのは営業部だけである。
- ・見込み客の登録から販売後のフォローアップまでを一貫してBシステムによって管理する。
- ・Bシステムの導入及び運用はA社の情報システム部が行う。
- ・Bシステムは2か月後から使用開始する。
- ・表計算ソフトを使用して管理していた顧客情報はBシステムに移行後、ノートPCから削除する。

情報システム部は、Bシステムに関して、利用者IDの管理、データのバックアップ取得、ログの記録などに関する要件について営業部との間で合意した。Bシステムは顧客情報を取り扱うシステムなので、内部不正による顧客情報の漏えいを防止するため、採取するログの保存方法や、レビュー方法(誰がいつ、どのように)についてC君が検討を開始した。

## 〔ログのレビュー方法の検討〕

営業部の企画課に所属するC君は、営業部の情報セキュリティリーダーを兼ねている。C君はBシステムのログの仕様を確認しようと思い、情報システム部担当者のD君にログの仕様の調査を依頼した。そこでD君は、Bシステムのログのサンプルを提示した(表1)。ログイン及びログアウトのログはサーバXで、それ以外のログはサーバYで記録されるが、表1は、情報システム部でツールを用いてそれらのログを同じ形式に整え、表計算ソフトを使用して時系列順に並び替えたもの(以下、加工済みログという)とのことであった。

表1 Bシステムの加工済みログ(抜粋)

| 日時                  | 利用者の IP アドレス | 利用者ID | 操作     | 顧客ID  |
|---------------------|--------------|-------|--------|-------|
| 2015/03/10 15:30:10 | 10.0.0.5     | 1013  | LOGIN  | 0     |
| 2015/03/10 15:40:03 | 10.0.0.5     | 1013  | READ   | 10023 |
| 2015/03/10 15:40:10 | 10.0.0.5     | 1013  | READ   | 10025 |
| 2015/03/10 15:40:15 | 10.0.0.5     | 1013  | READ   | 10102 |
| 2015/03/10 15:45:20 | 10.0.0.5     | 1013  | UPDATE | 10102 |
| 2015/03/10 15:50:16 | 10.0.0.5     | 1013  | DELETE | 10023 |
| 2015/03/10 16:03:10 | 10.0.0.8     | 1002  | LOGIN  | 0     |
| 2015/03/10 16:15:03 | 10.0.0.8     | 1002  | READ   | 10105 |
| 2015/03/10 16:16:10 | 10.0.0.8     | 1002  | READ   | 10321 |
| 2015/03/10 16:16:15 | 10.0.0.8     | 1002  | READ   | 10222 |
| 2015/03/10 16:20:12 | 10.0.0.5     | 1013  | LOGOUT | 0     |
| 2015/03/10 16:25:19 | 10.0.0.8     | 1002  | LOGOUT | 0     |

注記 顧客IDの0は、顧客情報に関係しない操作であることを意味する。

D君は、Bシステムでは、次の対策を実施することをC君に説明した。

- ・加工済みログの順番が、実際に営業部員がBシステムに対して実施した操作の順番どおりになるよう、aを行う。
- ・ログが故意に消されてしまうことがないようにbを行う。

営業部では、顧客ごとに担当営業を決めているが、担当営業が休みの際のサポートなどが必要なので、Bシステムでは、全営業部員が全顧客情報にアクセスできるようにする。

最近、同業他社で、従業員が、共有ファイルサーバにある全ての顧客情報をUSBメモリにコピーして持ち出し、転職先で使ったという事件が発生した。そこで営業部長は、C君に図1の要件を伝え、対策の検討を指示した。

- ・顧客情報への業務目的外のアクセスをログのレビューによって検出したい。ログのレビュー手順は、まずログの内容を確認し、もし業務目的外と思われる顧客情報へのアクセスログがあった場合は、遅滞なく営業部長に報告の上、そのログが示す操作を行った営業部員がなぜその操作を行ったかを適切な方法で確認する。
- ・万が一問題が発生したときに備えて、後からでもどの営業部員がどの顧客情報にアクセスしたか特定できるようにしておきたい。

図1 営業部長が伝えた要件

営業部長は、①リスクを更に低減させるために、営業部員が退職する際に新たな手続を実施することとした。

②C君は、営業部長が伝えた要件を基に、どのような立場の人がどの程度の頻度でレビューをすべきかを検討した。③さらにC君は、ログの長期的な保存方法についても検討を行った。C君が、検討結果を営業部長に説明したところ、営業部長もこれに同意した。

情報システム部によるBシステムの導入完了後、各営業部員は、表計算ソフトを使用して管理していた顧客情報をBシステムに移行し、ノートPCから削除した。移行完了後、営業部ではBシステムの使用を開始した。

## 〔ログのレビュー開始〕

Bシステムの使用を開始して1か月が経過し、ログのレビューが開始された。Bシステムには約4,000人の顧客情報が保管されている。ログの生成件数を考えると、30日間で100人以上の顧客情報にアクセスした営業部員のログに限定してレビューを行うべきだということになった。そこで、④C君は、過去30日間に発生したREADのログからレビュー対象のログを抽出する条件を示してD君にログの抽出を依頼した。抽出されたログを見たC君は、ある営業部員が1,000人分の顧客情報にアクセスしたことを示すログを発見した。そこで、C君はすぐに営業部長に報告し、その営業部員の上長の課長に確認した。その結果、その課長の指示でダイレクトメールを送付していたことが分かり、問題はないことが確認できた。

営業部長とC君で相談した結果、レビューを行う人、及び頻度は検討結果のとおりとし、抽出条件に基づいて抽出したログだけをレビュー対象とすることとした。営業部長は、ログをレビューするに当たり、次のことを指示した。

- ・全ての営業部員に対し、ログをレビューすることを伝えること。ただし、ログのレビューを回避されないように、抽出条件を営業部員には伝えないこと。
- ・ログがレビューされていることを営業部員に印象付けるために、ログに記録されているアクセスについて定期的に必ず営業部員にアクセスの目的を確認すること。

## 〔課題の発見とリスクの更なる低減〕

C君は、職場内でBシステムが適切に使用されているかどうかを観察していたところ、いくつかの事象が目にとまり、このままでは、⑤ログのレビューを適切に実施したとしても、図1の要件が実現できないことに気付いた。そこでC君は、営業部長に相談の上、各課長に改善を依頼した。

Bシステムの使用開始から1年間が経過した。ログのレビューによって営業部全体の情報セキュリティ意識が高まり、営業部長のC君に対する評価は大きく高まった。

**設問 1** 本文中の a と b に入れる組合せとして正しい答えを、解答群の中から選べ。

a, bに関する解答群

|                                                                 | a               | b               |
|-----------------------------------------------------------------|-----------------|-----------------|
| <span style="background-color: #ff9966; padding: 2px;">ア</span> | サーバの時刻同期        | ログのWORMメディアへの記録 |
| <span style="background-color: #ff9966; padding: 2px;">イ</span> | サーバの時刻同期        | ログの暗号化          |
| <span style="background-color: #ff9966; padding: 2px;">ウ</span> | ログのWORMメディアへの記録 | サーバの時刻同期        |
| <span style="background-color: #ff9966; padding: 2px;">エ</span> | ログのWORMメディアへの記録 | ログの暗号化          |
| <span style="background-color: #ff9966; padding: 2px;">オ</span> | ログの暗号化          | サーバの時刻同期        |

注記 WORM: Write Once Read Many

**設問 2** 本文中の下線①で実施することになった手続はどれか。解答群のうち、最も適切なものを選べ。

解答群

- ア 退職する営業部員が担当していた顧客情報を、他の営業部員に引き継ぐ。
- イ 退職する営業部員が担当していた顧客情報を、Bシステムから完全に消去する。
- ウ 退職する営業部員に、その営業部員と締結した機密保持契約書を見せ、その営業部員がアクセスした顧客情報がログに記録されていることを説明する。
- エ 退職する営業部員のPCのハードディスクは再利用せず、完全に物理破壊する。

**設問 3** 本文中の下線②における、C君の検討結果はどれか。解答群のうち、最も適切なものを選び。

解答群

- ア** 営業部の各課長が、情報システム部担当者の依頼があった都度、ログをレビューする。
- イ** 営業部の各課長が、毎週、ログをレビューする。
- ウ** 情報システム部担当者が、営業部長が指定した頻度でログをレビューする。
- エ** 情報システム部担当者が、毎週、ログをレビューする。

**設問 4** 本文中の下線③においてC君が検討したログの保存方法はどれか。解答群のうち、最も適切なものを選び。

解答群

- ア** 情報システム部が全てのログを10年間保存する。
- イ** 情報システム部が営業部員ごとにログを仕分けして、各営業部員が自分の分を保存する。
- ウ** レビュー後のログは保存せず、情報システム部担当者が速やかに削除する。
- エ** レビューで不審であると判断したログだけを情報システム部が10年間保存する。

**設問 5** 本文中の下線④でC君がD君に示した抽出条件を、解答群の中から選べ。

解答群

- ア** アクセスしたユニークな顧客ID数が100以上の営業部員のログ
- イ** アクセスしたユニークな顧客ID数が100以上の日のログ
- ウ** ログ件数が100以上の営業部員のログ
- エ** ログ件数が100以上の日のログ

**設問 6** C君が観察した次の(i)～(iv)の事象のうち、本文中の下線⑤の原因となるものを全て挙げた組合せを、解答群の中から選べ。

- (i) Bシステムで表示した顧客情報をコピーし、表計算ソフトにペーストした上でA社の共有ファイルサーバに置いて共有している。
- (ii) Bシステムの使用申請をしてから、営業部長が承認するまでに2週間掛かっている。
- (iii) ある営業部員が共用PCからBシステムにログインし、ログインしたままそのPCで他の営業部員がBシステムを使っている。
- (iv) ある営業部員が頻繁にBシステムにログイン、ログアウトを繰り返している。

解答群

- |                      |                            |                     |                      |
|----------------------|----------------------------|---------------------|----------------------|
| <b>ア</b> (i), (ii)   | <b>イ</b> (i), (ii), (iv)   | <b>ウ</b> (i), (iii) | <b>エ</b> (i), (iv)   |
| <b>オ</b> (ii), (iii) | <b>カ</b> (ii), (iii), (iv) | <b>キ</b> (ii), (iv) | <b>ク</b> (iii), (iv) |



営業部門が保有する顧客情報へのアクセスログのレビューを主題として、ログのレビューの目的を理解し、ログのレビューを適切に運用する能力を確認する問題です。

## 設問 1 ログの対策

### 空欄 a

表 1 の内容から、利用者 ID が 1013 の利用者が 2015 年 3 月 10 日の 15 時 30 分 10 秒に LOGIN (ログイン) した後、同じ人が 15 時 40 分 03 秒に最初の READ 操作を行っています。また、利用者 ID が 1002 の利用者がログインしたときも、ログインから最初の READ 操作を行うまで 10 分以上経過しています。利用者が B システムにログインした後の最初の READ 操作の時刻が、ログイン時の時刻よりも大きい状況がログに記録されています。

【ログのレビュー方法の検討】で「ログイン及びログアウトのログはサーバ X で、それ以外のログはサーバ Y で記録される」と説明されています。サーバ X の時刻とサーバ Y の時刻がずれているので、ログインやログアウトの時刻と READ などの操作の時刻に差が生じたと考えられます。このようなずれがあるため、加工済みログにおいては利用者が行った一連の操作のうち、ログアウトの操作だけが他の操作と並んで記録されておらず、見にくくなっています。

図 A のように、加工済みログの順番が実際の利用者の操作の順番どおりにならず、ログを参照しても利用者の操作を適切に確認できないことがあります。よって、「サーバの時刻同期」を行い、サーバ X とサーバ Y の時刻を合わせる必要があります。

### 空欄 b

「ログが故意に消されてしまうことがないように [b] を行う」とあることから、空欄 b の対策はログが消されないようにするためのものです。ハードディスクや USB メモリなど、データの更新や消去が何回でも可能な電子媒体にログを保存すると、ログの内容が故意に消され、不正アクセスの証拠が残らなくなる危険性があります。CD-R や DVD-R など、読みみは何回でも可能だが書き込みは 1 回しかできず、消去もできないメディアにログを保存すると、ログが故意に消されることはなくなります。このようなメディアのことを、WORM (Write Once Read Many) と呼びます。空欄 b には「ログの WORM メディアへの記録」が入ります。

以上から、アが正解です。

## 設問 2 退職者の扱い

【ログのレビュー方法の検討】にて「最近、同業他社で、従業員が、共有ファイルサーバにある全ての顧客情報を USB メモリにコピーして持ち出し、転職先で使った

表 1 B システムの加工済みログ (抜粋)

| 日時                  | 利用者の IP アドレス | 利用者 ID | 操作     | 顧客 ID |
|---------------------|--------------|--------|--------|-------|
| 2015/03/10 15:30:10 | 10.0.0.5     | 1013   | LOGIN  | 0     |
| 2015/03/10 15:40:03 | 10.0.0.5     | 1013   | READ   | 10023 |
| 2015/03/10 15:40:10 | 10.0.0.5     | 1013   | READ   | 10025 |
| 2015/03/10 15:40:15 | 10.0.0.5     | 1013   | READ   | 10102 |
| 2015/03/10 15:45:20 | 10.0.0.5     | 1013   | UPDATE | 10102 |
| 2015/03/10 15:50:16 | 10.0.0.5     | 1013   | DELETE | 10023 |
| 2015/03/10 16:03:10 | 10.0.0.8     | 1002   | LOGIN  | 0     |
| 2015/03/10 16:15:03 | 10.0.0.8     | 1002   | READ   | 10105 |
| 2015/03/10 16:16:10 | 10.0.0.8     | 1002   | READ   | 10321 |
| 2015/03/10 16:16:15 | 10.0.0.8     | 1002   | READ   | 10222 |
| 2015/03/10 16:20:12 | 10.0.0.5     | 1013   | LOGOUT | 0     |
| 2015/03/10 16:25:19 | 10.0.0.8     | 1002   | LOGOUT | 0     |

注記 顧客 ID の 0 は、顧客情報に関係しない操作であることを意味する。

利用者 ID が 1013 の利用者の一連の操作のうち、ログアウトが他の利用者の操作の後に記録されており、ログの参照時に見にくい。

図 A

という事件が発生」しており、そのリスクを更に低減させるために、下線①では営業部員が「退職する際」に新たな手続を実施しています。営業部員が在職中に密かに保存していた顧客情報を、退職してから外部に流出させようとするリスクが考えられます。

A社では「顧客情報などの機密情報の漏えいを防ぐ」目的で、退職後も一定期間有効な損害賠償条項を含む機密保持契約を全従業員と締結しているため、退職した営業部員が一定期間内に顧客情報を流出させた場合、この機密保持契約に従って損害賠償を求めることができます。営業部員の退職時に機密保持契約を見せたり、その営業部員がアクセスした顧客情報がログに記録されていることを説明したりすることで、顧客情報の流出を抑止する効果があります。

このようにすることで下線①のリスクを低減させることが可能です。**ウ**が正解です。

- × **ア** 退職する営業部員が担当していた顧客情報を他の営業部員に引き継ぐだけでは、退職した営業部員の犯行を防ぐことはできません。
- × **イ** 退職する営業部員が担当していた顧客情報をBシステムから消去すると、その顧客に対して今後営業活動ができなくなります。
- **ウ** 正解です。
- × **エ** 退職する営業部員のPCのハードディスクを物理破壊しても、その営業部員が在職中に顧客情報をUSBメモリなどにコピーして自宅などに保管している場合、顧客情報の流出を防げません。

### 設問3 レビューの担当

- ア** Bシステムのログのレビューは、営業部の営業活動に関して顧客情報へのアクセスが適切に行われているかを検証するために実施します。その実施権限は営業部にあるので、情報システム部担当者の依頼などを受けて行うのではなく、営業部の部長または課長といった管理者が、自らの責任で行うべきことです。不適切な記述です。
- イ** 営業部の各課長が毎週ログをレビューすることで、顧客情報への業務目的外のアクセスを定期的に検出することができます。適切な検討結果です。
- ウ、エ、ア** で説明したとおり、Bシステムのログのレビューは営業部に実施権限があり、情報システム部担当者にはありません。

以上から、**イ**が正解です。

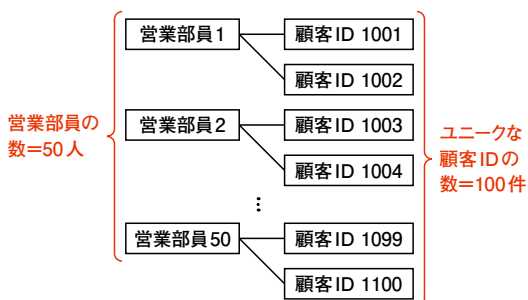
### 設問4 ログの保存方法

- ア** 情報システム部が全てのログを10年間保存することで、**図1**の「万が一問題が発生したときに備えて、後からでもどの営業部員がどの顧客情報にアクセスしたか特定できるようにしておきたい」という要件を満たすことができます。適切なログの保存方法です。
- イ** 各営業部員が自分の分のログを保存すると、不正アクセスしたときのログを自ら改ざんして、不正を隠ぺいすることが可能になります。
- ウ** このようにすると、**図1**の上記要件を満たすことができません。
- エ** レビューで不審であると判断したログだけを保存すると、不正アクセスの証拠が記録されていたログを、情報システム部が不審でないと誤って判断して削除してしまった場合に、**図1**の上記要件を満たすことができなくなります。

以上から、**ア**が正解です。

### 設問5 レビュー対象

- ア** 【ログのレビュー開始】において「30日間で100人以上の顧客情報にアクセスした営業部員のログに限定してレビューを行うべき」としています。このようなログを抽出するのが適切です。アクセスしたユニークな顧客ID数が100以上の営業部員のログには、その営業部員が100人以上の顧客に30日間でアクセスしたことが記録されています。
- イ** 例えば、各営業部員がある日にそれぞれ異なる顧客の情報に2件ずつアクセスした場合、その日に記録されるユニークな顧客ID数の合計は100以上になります。





ユニークな顧客ID数が100以上の日のログを抽出しても、30日間で100人分以上の顧客情報にアクセスした営業部員を特定することはできません。

ウ 例えば、毎日同じ4人分の顧客情報だけにアクセスする営業部員でも、30日間で記録されるログの件数は100件以上になります。ログ件数が100以上の営業部員のログを抽出しても、30日間で100人分以上の顧客情報にアクセスした営業部員を特定することはできません。ログ件数だけを確認するのではなく、ユニークな顧客ID数が100以上の営業部員のログを対象にするのが適切です。

エ イと同様の理由で、ログ件数が100以上の日のログにアクセスしても、30日間で100人分以上の顧客情報にアクセスした営業部員を特定することはできません。

以上から、アが正解です。

## 設問6 レビューの課題

### ● (i) の事象

このようにすることで、営業部員はBシステムにログインしなくても、A社の共有ファイルサーバ上にある顧客情報を参照できるので、Bシステムのログをレビューしても顧客情報への業務目的外のアクセスを検出できなくなります。下線⑤の原因になります。

### ● (ii) の事象

Bシステムの使用申請をしてから、営業部長が承認す

るまでに2週間掛かっているため、その間は利用者がBシステムを利用できず、顧客情報にアクセスできません。その間は顧客情報の流出なども発生しなくなります。下線⑤の原因にはなりません。

### ● (iii) の事象

ある営業部員(利用者IDを1100とする)が共用PCからBシステムにログインし、ログインしたままのPCで他の営業部員(利用者IDを1200とする)がBシステムを使った場合、Bシステムのログには利用者IDとして1100が記録され、Bシステムを実際に使った営業部員の情報がログに残らなくなります。このような状況では、どの営業部員がどの顧客情報にアクセスしたか特定できず、図1の要件を満たせません。下線⑤の原因になります。

### ● (iv) の事象

頻繁にBシステムにログイン、ログアウトを繰り返しているだけで、顧客情報へのアクセスがなければ、顧客情報への業務目的外のアクセスをしていないので、下線⑤の原因にはなりません。

以上から、ウが正解です。

## 解答

|      |   |      |   |      |   |
|------|---|------|---|------|---|
| 設問 1 | ア | 設問 2 | ウ | 設問 3 | イ |
| 設問 4 | ア | 設問 5 | ア | 設問 6 | ウ |