情報セキュリティマネジメント試験　サンプル問題（午後試験）

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）を社内に導入し，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 人分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留まり，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
ア	サーバの時刻同期	ログの WORM メディアへの記録
イ	サーバの時刻同期	ログの暗号化
ウ	ログの WORM メディアへの記録	サーバの時刻同期
エ	ログの WORM メディアへの記録	ログの暗号化
オ	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べ。

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べ。

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

ア　(i)，(ii)	イ　(i)，(ii)，(iv)	ウ　(i)，(iii)
エ　(i)，(iv)	オ　(ii)，(iii)	カ　(ii)，(iii)，(iv)
キ　(ii)，(iv)	ク　(iii)，(iv)	

情報セキュリティマネジメント試験　サンプル問題（午後試験）　解答例

問番号		正解	備考
問 1	設問 1	ア	
	設問 2	ウ	
	設問 3	イ	
	設問 4	ア	
	設問 5	ア	
	設問 6	ウ	

出題趣旨
情報セキュリティにおいて，権限をもった者による内部不正を防止することは一般に困難である。内部不正が行われていたことを発見する手段として，記録したログのレビューを適切に実施することが有効な選択肢となり得る。しかし，レビューのプロセスが適切に設計されていないと機能しない。具体的には，レビュー実施者，レビュー頻度，レビュー対象となるログの抽出条件などを適切に設計する必要がある。そして，レビューに当たっては，業務をよく理解したユーザ部門が主体的に関与することが重要である。 本問では，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題材として，ログのレビューがどのような目的で行われるかを理解した上で，プロセスが適切であるか判断する能力と，ログのレビューを適切に運用する能力を問う。