演習　情報セキュリティの運用と管理

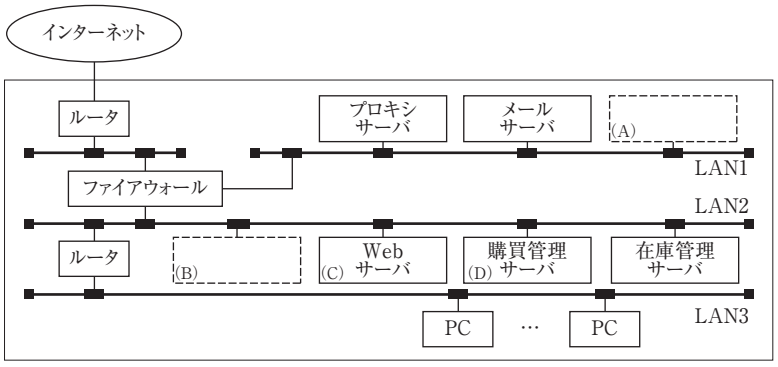
平成22年度 問4

問　情報セキュリティの運用と管理に関する次の記述を読んで，設問1～3に答えよ。

E社は，日用品雑貨の卸売業者であり，全国6か所の営業所で販売業務を行っている。本社には，総務部，情報システム部，購買部などがある。購買部では，購買管理システムを使用して，商品の発注業務，検収業務などを行っている。

〔購買管理システムの概要〕

購買管理システムでは，PCから，Webサーバ上の業務ポータル画面を介して，購買管理サーバと在庫管理サーバにアクセスする構成を採用している。また，購買部と取引先の連絡は，メールサーバを介したインターネット経由での電子メールを利用して行われている。購買管理システムの構成を，図に示す。



注(A)～(D)は設問1で参照する。(A),(B)は新規に設置するサーバに,(C)はWebサーバに,
(D)は購買管理サーバに,それぞれ保存されるファイルを示す。
LAN1：社外向けサーバを接続するネットワーク
LAN2：社内向けサーバを接続するネットワーク
LAN3：部門に設置されたネットワーク

図　購買管理システムの構成

〔購買管理システムの利用状況〕

購買管理システムは，購買部の正社員のほかに，購買部の支援作業を行う派遣社員が利用している。派遣契約は，総務部が派遣会社と締結している。利用者IDは個人単位に発行

されていて，正社員及び派遣社員が購買管理システムを利用する際は，利用者IDとパスワードで認証される。

情報システム部の正社員は，購買管理システムにログインして運用管理を行っている。システム構成の管理やアカウントの管理など，一般の利用者IDでは実施できない操作を行う場合は，特権IDを使用している。

なお，特権IDでは，サーバの起動・停止や格納されているデータの変更などあらゆる操作の実行が可能なので，情報システム部のサーバ管理者に利用を限定している。

〔アカウントの管理〕

E社の各サーバへのアクセスは，利用者IDとパスワードによって認証する方法が採られている。パスワードは有効期間が定められていて，購買管理システムの場合は60日間である。認証時に，サーバのシステム日付とパスワード設定日を比較し，有効期限を超過している場合には，パスワードの変更を強制する機能が組み込まれている。パスワードの変更は，随時可能である。

アカウントの管理については，次の(1) ～ (4)に示す運用規程を定めている。

(1) アカウントのサーバへの登録及び削除は，情報システム部のサーバ管理者が行う。

(2) アカウントの付与は，各部門の課長が作成して部長が承認したアカウント付与依頼書に基づいて行う。アカウント付与依頼書には，利用者名，担当する業務内容などが記載されている。派遣社員のアカウントの付与については，承認者を総務部長に一元化している。購買管理システムにおけるアカウントの付与は，正社員の場合にはアカウント付与依頼書に購買部長の承認が必要であり，派遣社員の場合には購買部長がアカウント付与依頼書を確認後，購買部長名で総務部長に依頼して承認を得る必要がある。

(3) 承認されたアカウント付与依頼書は，サーバ管理者に送付される。サーバ管理者は利用者IDと初期パスワードを設定し，アカウント付与依頼書に記載された業務内容に応じたサーバにアカウントを登録するとともに，設定内容をアカウント付与依頼書に記入して発行元の部門に返送する。各部門は返送されたアカウント付与依頼書を保管する。

(4) アカウントの削除は，各部門の課長が作成して部長が承認したアカウント削除依頼書に基づいて，アカウントの付与と同様の手順で行う。承認者はアカウントの付与と同様である。

派遣社員のアカウントの付与について，購買部長は比較的早期に確認しているのに対して，総務部長は承認に時間を要している。退職した正社員・派遣社員のアカウントの削除については，直ちに承認されているが，サーバからの削除は2週間ごとに実施する定期メンテナンス作業の中で行っている。

最近，派遣社員の増強に伴って，購買部が派遣契約を締結することになった。

〔セキュリティ要件〕

E社では，アカウントやログの管理に関する脅威を想定して，表に示すセキュリティ要件を規定している。

表　セキュリティ要件

	想定脅威	セキュリティ要件
アカウントの管理	不正利用した個人を特定できない	アカウントの付与は特定の個人を対象とし，規定された承認者の承認を得ること
	退職者のアカウントの不正利用	アカウントを利用する必要がなくなった場合は，速やかに削除すること
	管理者による不正利用	承認者と行為者の職務を分離すること
	a	パスワードは，定期的に変更することとし，類推が困難な文字列を採用すること
ログの管理	ログを収めたファイルの改ざん	ファイルは，外部から書き換えられないように，独立したサーバに集約すること
	サーバへの不正侵入や不正操作	ログは，一定期間保存し，定期的に分析すること

〔ログの管理〕

購買管理システムでは，サーバへの不正侵入や不正操作がなかったかどうかを検証するために，ログイン時のパスワードの誤り，特権IDを使用した操作，システムからの警告や障害の情報のログを取得している。ログには，ログインを試みた日時，ID，サーバ名，ログインの成否などの項目を記録している。ログはオーバラップ方式で記録し，セキュリティ要件で規定された期間中は保存できる設計となっている。

〔トラブルの発生〕

ある日，営業担当者が，一部の商品の在庫量が異常に多いことに気付き，購買部に問い合わせて確認したところ，営業所から発注を依頼された数量と，購買部が実際に発注入力した数量が違っていた。購買部では，原因を特定するために，購買管理システムの利用状況を確認するように情報システム部に依頼した。

依頼を受けた情報システム部が購買管理システムのログを確認したが，発注入力した日のログからは，原因を特定できなかった。その後の調査で，購買部のある派遣社員が，退職した前任者の利用者IDとパスワードを使ってアクセスしていたことが判明した。前任者はアカウントを付与されてから30日後に退職したので，保管してあるアカウント付与依頼書に記載されていた初期パスワードが有効な状態であった。その派遣社員は業務に不慣れであったので，数量のけたを間違えて入力していた。

E社のITサービスマネージャであるK氏は，今回のトラブルで発覚したアカウントの不正利用をセキュリティインシデントとしてとらえ，セキュリティインシデントの再発を防止するための対策を講じることにした。

〔セキュリティ監査〕

E社では，今回のセキュリティインシデントの発生を契機に，社内の監査部門がセキュリティ監査を実施した。セキュリティ監査では，新規のアカウント付与や退職者のアカウント削除が円滑に行われておらず，セキュリティ要件の規定順守に問題があることが指摘された。また，特権IDの運用についても，管理者による不正利用防止の規定順守に問題があることが指摘された。

K氏は，指摘に対する是正策として，アカウントの管理の運用改善策，特権IDの運用改善策について検討した。検討の結果，アカウントの管理の運用改善策として，サーバ管理者がサーバに登録されているアカウントを定期的に点検することにした。また，特権IDの運用改善策として，サーバ管理者とは別に特権ID管理者を設定し，職務を分離することにした。

設問1　〔セキュリティ要件〕について，(1)，(2)に答えよ。

(1)　表中の［　a　］に入れる適切な字句を20字以内で述べよ。

(2)　購買管理システムのログは，図中の(A)～(D)のうち，どの場所に保存するのが適切か。一つ選び記号で答えよ。また，その理由を40字以内で述べよ。

設問2　〔トラブルの発生〕について，(1)～(3)に答えよ。

(1)　初期パスワードが不正利用されないための対策を，30字以内で述べよ。

(2)　今回のセキュリティインシデントの再発を防ぐためには，アカウントの管理の運用をどのように変更すべきか。変更内容を，30字以内で述べよ。

(3)　今後のトラブル発生に備え，特権IDだけでなく，すべての利用者IDを使用した操作のログを取得することになった。これに伴って確認しておくべき事項は何か。30字以内で述べよ。

設問3　〔セキュリティ監査〕について，(1) ～ (3) に答えよ。

(1) アカウントの管理に関する運用規程を修正することで，アカウントの付与を円滑にしたい。どのような修正が考えられるか。修正内容を40字以内で述べよ。

(2) アカウントの管理の運用改善策として，定期的な点検で実施すべき事項を挙げ，40字以内で具体的に述べよ。

(3) 特権IDの運用改善策では，特権ID管理者に対する統制が必要になる。セキュリティ要件に適合した施策内容を，40字以内で述べよ。

解答例

設問1　(1) 20字以内　(2) 理由：40字以内

(1)

辞書攻撃等によるパスワードクラック

〔試験センターによる解答例〕
なりすましによる不正利用

(2)　場所：(B)

理由：

外部から書き換えられないように，独立したサーバに集約しなければならないから

〔試験センターによる解答例〕
理由：セキュリティが確保されたLAN上でE社のセキュリティ要件を満たす場所であるから

設問2　各30字以内

(1)

初回ログイン時に，本パスワードを入力させる仕組みを採用する

〔試験センターによる解答例〕
初回ログイン時に初期パスワードの変更を強制する。

(2)

退職した正社員・派遣社員のアカウントは，承認後すぐ削除する

〔試験センターによる解答例〕
退職者のアカウント削除を，削除依頼時点で即時実施する。

(3)

すべてのログが，ログファイルに格納可能か否かを確認する

〔試験センターによる解答例〕
現在準備されているログ保存用の記憶容量で十分か確認する。

設問3　各40字以内

(1)

〔試験センターによる解答例〕

派遣社員のアカウントを付与する承認者を，総務部長から購買部長に変更する。

(2)

〔試験センターによる解答例〕

登録されているアカウントの一覧をサーバごとに作成し，承認者に確認を依頼する。

(3)

〔試験センターによる解答例〕

- 特権ID管理者は，承認だけ行い，特権IDを使った操作はできないようにする。
- 特権ID管理者が特権IDを不正に使用していないことをログで確認する。

設問別解説

設問のパターンと難易度

設問1	(1)	B	ヒント＋記述型　易
	(2)	B	ヒント＋記述型　易
設問2	(1)	C	記憶＋記述型　中
	(2)	B	ヒント＋記述型　易
	(3)	B	ヒント＋記述型　中
設問3	(1)	B	ヒント＋記述型　易
	(2)	B	ヒント＋記述型　易
	(3)	C	記憶＋記述型　中

設問1

(1) 本設問のヒントは，空欄aの右側のセキュリティ要件“パスワードは，定期的に変更することとし，類推が困難な文字列を採用すること”である。これは，“辞書攻撃等によるパスワードクラック”を想定脅威としたセキュリティ要件である。

(2) 本設問のヒントは，空欄aの右下のセキュリティ要件“ファイルは，外部から書き換えられないように，独立したサーバに集約すること”である。このファイルは，空欄aの下の想定脅威“ログを収めたファイルの改ざん”からログを収めたファイルである。したがって，購買管理システムのログを収めたファイルは，①外部から書き換えられないように，②独立したサーバに集約しなければならない。
上記の①から，解答の候補は，ファイアウォールによって守られた内部LAN側にある(B)(C)(D)に絞られ，さらに②から新規に設置するサーバである(B)に特定される。

設問2

(1) 初期パスワードが不正利用されないための対策は，初回ログイン時に，初期パスワードの認証に成功したら，本パスワードを入力させる仕組みを採用することである。この方法は，“初期パスワードは，利用者の住所等に郵便物による郵送等のネットワーク以外の手段を使って安全に送付すること”と一緒に覚えておくとよい。

(2) 問題文〔トラブルの発生〕の5文目は“前任者はアカウントを付与されてから30日後に退職したので，保管してあるアカウント付与依頼書に記載されていた初期パスワードが有効な状態であった。”としている。これは，問題文〔アカウントの管理〕の最後から2文目のように，“退職した正社員・派遣社員のアカウントの削除については，直ちに承認されているが，サーバからの削除は2週間ごとに実施する定期メンテナンス作業の中で行っている。”からである。
したがって，今後は，退職した正社員・派遣社員のアカウントは，承認後，サーバから直ちに削除すればよい。

(3) 本設問の弱いヒントは，問題文〔ログの管理〕の最終文“(前略) セキュリティ要件で規定された期間中は保存できる設計となっている。”である。特権IDだけではなく，すべての利用者IDを使用した操作のログを取得すれば，保存するログの量は現状よりもはるかに多いものとなるだろう。
したがって，すべての利用者IDを使用した操作を含む全ログが，ログファイルに格納可能か否かを確認しなければならない。

設問3

(1) アカウント付与の現状は，問題文〔アカウントの管理〕(2) の3，4文目“派遣社員のアカウントの付与については，承認者を総務部長に一元化している。購買管理システムにおけるアカウントの付与は，正社員の場合にはアカウント付与依頼書に購買部長の承認が必要であり，派遣社員の場合には購買部長がアカウント付与依頼書を確認後，購買部長名で総務部長に依頼して承認を得る必要がある”のとおりである。
しかし，問題文〔アカウントの管理〕の最後から3文目は，“派遣社員のアカウントの付与について，購買部長は比較的早期に確認しているのに対して，総務部長は承認に時間を要している。”としており，アカウント付与が円滑にできない原因を示している。
問題文〔アカウントの管理〕の最終文“最近，派遣社員の増強に伴って，購買部が派遣契約を締結することになった。”ような状況だから，派遣社員の場合には購買部長がアカウント付与依頼書を確認して承認する運用規程に変更すればよい。

(2) 本設問のヒントは，問題文〔セキュリティ監査〕の最後から2文目の“検討の結果，アカウントの管理の運用改善策として，サーバ管理者がサーバに登録されているアカウントを定期的に点検することにした。”である。この運用改善策は，問題文〔セキュリティ監査〕の2文目の“セキュリティ監査では (中略) 退職者のアカウント削除が円滑に行われておらず，セキュリティ要件の規定順守に問題がある (後略)”を受けたものだから，サーバに登録されているアカウントを一覧表にし，退職者・部門異動者・

職務変更者等の権限喪失者がアカウントから削除されていることを定期的に確認すればよい。

(3) 本設問は，セキュリティ要件に適合した施策を問うているので，“表　セキュリティ要件”からヒントを探す。しかし，特権ID管理者に関するセキュリティ要件は特に記載されていないので，記憶に照らして考える。
特権ID管理者は，他の利用者よりも，強い権限を持っているので，不正操作をした場合，多大な被害を企業に与えてしまう。そこで，ログを定期的に分析し，特権ID管理者が実施した操作をチェックしなければならない。“表　セキュリティ要件”の最下行のセキュリティ要件である“ログは，一定期間保存し，定期的に分析すること”は，その一部を示している。
したがって，解答は“ログを定期的に分析し，特権ID管理者が不正な操作をしていないかをチェックする”のようにまとめればよい。