演習　セキュリティ管理

平成23年度 問3

問　セキュリティ管理に関する次の記述を読んで，設問1～4に答えよ。

A社では，カタログで紹介している健康食品の注文を，電話，メールで受け付けて，販売してきた。販売管理システムを利用して販売実績管理を行っており，運用及び保守はシステム部が担当している。

〔販売管理システムのアカウントの管理〕

販売管理システムへのアクセスは，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。

社員の利用者IDの付与プロセスは，次のとおりである。

(1) 利用者IDを必要とする社員が，自身の上長に利用者ID付与申請書を提出する。
(2) 上長は，社員への利用者ID付与が必要と判断した場合，社員からの利用者ID付与申請書を承認した上で，システム部の利用者ID管理者であるC氏に送付する。
(3) C氏は，利用者ID付与申請書に基づいて，システムに利用者IDを登録し，当該社員及び上長に利用者ID付与完了通知を送付する。

A社では社員の退職などによって利用者IDが不要になった場合には，上長が，利用者IDの削除を申請する。

利用者IDの削除プロセスは，次のとおりである。

(1) 上長がC氏に利用者ID削除申請書を送付する。
(2) C氏は，毎月月末のID一覧表更新作業に合わせて，削除申請のあった利用者IDをシステムから削除する。
(3) 利用者IDを削除した後，C氏は，上長に利用者ID削除完了通知を送付する。

システムの保守作業には，サーバの起動・停止，格納データの変更など，あらゆる操作が可能な特権IDが必要である。管理を簡素化するために，システム部全員で，一つの特権IDを共用している。特権IDを使用する場合は，個人の利用者IDでサーバにログインし，切替コマンドで個人の利用者IDから特権IDに切り替える仕組みにしている。

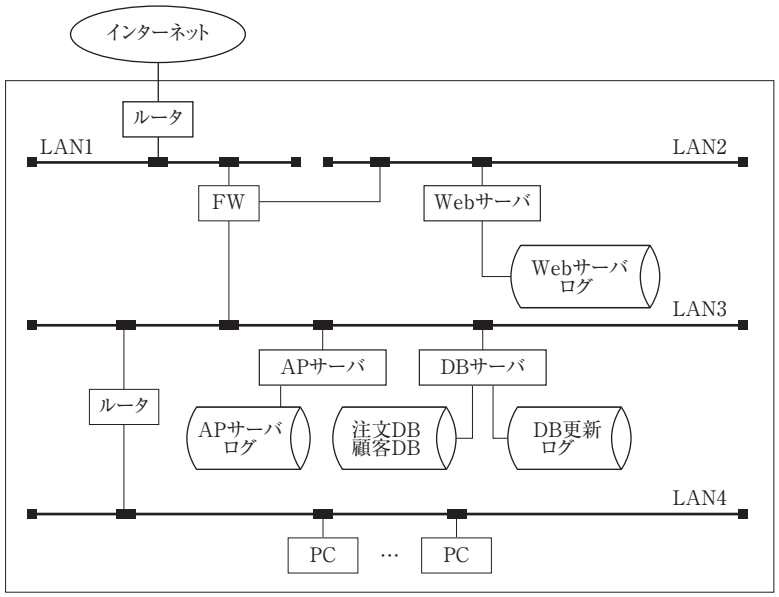
〔注文受付システムの検討〕

顧客の利便性を考慮して，今後はWebサイトで注文を受け付けることになった。そのための注文受付システムの構成を，システム部のK氏が検討した。

検討した注文受付システムの構成は，図1のとおりである。

注文受付システムのためのWebサーバ，アプリケーションサーバ，データベース（以下，DBという）サーバを新たに導入し，注文情報を注文DBに，顧客情報を顧客DBに保存する。

また，インターネットからの利用は，ファイアウォール（以下，FWという）を経由し，Webサーバにアクセスして注文ができるようにする。このとき，FWのパケットフィルタリング機能で，HTTPSのパケットだけを許可する。



LAN1：外部接続セグメント　LAN2：非武装セグメント　LAN3：内部セグメント
LAN4：社内LAN　APサーバ：アプリケーションサーバ

図1　注文受付システムの構成

〔セキュリティ要件〕

A社では，注文受付システムのセキュリティ要件を，次のように規定している。

(1) インターネットからの不正アクセスを防止する。

(2) 情報漏えいなどの問題が発生した場合に，アクセス元，アクセス者，アクセスされた情報などを調査するために，全てのサーバのアクセスログを1年間保存する。
(3) アクセスログとして保存する項目のうち，顧客情報などの個人情報は，必要最小限にする。
(4) 保存したアクセスログの改ざん・削除の防止対策を実施する。

〔注文受付システムの見直し〕

システム部のB氏は，K氏が検討した注文受付システムを，セキュリティ要件に基づいて，次のように見直した。

(1) 外部からの攻撃の監視
- FWのログを取得し，外部からの攻撃の有無を調査する。
- 次の手順に示すように，図2の形式で保存されているFWのログを毎日，分析し，ポートスキャンの有無を調査する。
  ① FWのログから，アクションがDrop又はRejectである外部からのパケットを抽出する。
  ② 同一の［ a ］から複数の［ b ］へのログが短時間に大量に発生している場合，ポートスキャンの有無を調査する。

日時	発信元IPアドレス	発信元ポート番号	宛先IPアドレス	宛先ポート番号	プロトコル	アクション

図2　FWのログ

(2) ログの管理
- 当初の検討ではリカバリ用に保管されているDB更新ログをDBサーバのアクセスログとして流用し，保存期間を1年間に延長することを考えていたが，DB更新ログを流用せず，新たにDBアクセスログを作成して，利用者ID，イベントタイプ，日時，成功／失敗，対象データのキー項目などを保存する。
- FWのログ，Webサーバログ，APサーバログ，DBアクセスログを一元管理するために，ログサーバをLAN2に導入する。
- ディスク容量の制約から1か月ごとに，アクセスログをログサーバのディスクに直近1か月分を残したまま，磁気テープに退避して保管する。

〔Webサーバのコンテンツ改ざん〕

Webサーバのコンテンツが改ざんされる事件が発生した。インターネットからWebサーバのセキュリティホールが攻撃可能な状態になっていたので，Webサーバに侵入され，コン

テンツが改ざんされてしまった。システム部で調査したところ，FWの設定は正しく行われていたが，HTTPSを利用して改ざんされていたことが判明した。

A社では，再発防止策として，脆弱性対策及び不正プログラム対策と併せて，新たに侵入検知システム（以下，IDSという）を導入することにした。IDSでは，接続しているネットワークセグメントのトラフィックを監視し，ネットワークを流れるパケットのプロトコルヘッダやデータをあらかじめ定義されたルールに基づいて解析する。不正なパケットを検知した場合は，管理者の端末に異常を通知する。

ただし，解析処理に多くのCPU資源を使用することから，ネットワークトラフィックが増加すると，侵入検知機能が停止してしまうおそれがあるので，IDSの設置場所と，その設置場所に応じた処理能力の検討が必要である。

設問1　〔販売管理システムのアカウントの管理〕について，(1)～(3)に答えよ。

(1) 現状の利用者IDの削除プロセスには問題がある。その問題の解決策を具体的に，30字以内で述べよ。

(2) アカウントの管理を補完する目的で，定期的に実施すべき作業がある。C氏が，各上長に依頼すべき作業内容を，40字以内で具体的に述べよ。

(3) 個人の利用者IDでサーバにログインし，切替コマンドで個人の利用者IDから特権IDに切り替える仕組みにしている理由を，25字以内で述べよ。

設問2　〔注文受付システムの見直し〕の外部からの攻撃の監視について，［ a ］，［ b ］に入れる適切な字句を，図2の項目から選択して答えよ。

設問3　〔注文受付システムの見直し〕のログの管理について，(1)～(3)に答えよ。

(1) DB更新ログを流用せず，新たにDBアクセスログを作成することにした理由は何か。セキュリティ要件から，30字以内で述べよ。

(2) 保存したログを磁気テープに退避する目的は何か。セキュリティ要件から，35字以内で述べよ。

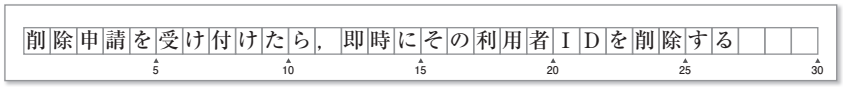
(3) ログサーバをLAN2に設置することには問題点がある。この問題点を40字以内で具体的に述べよ。

設問4　〔Webサーバのコンテンツ改ざん〕について，IDSを設置する最も適切な場所を，LAN1，LAN2及びLAN3の中から一つを選択して答えよ。また，その理由を40字以内で述べよ。

解答例

設問1　（1）30字以内　（2）40字以内　（3）25字以内

（1）



〔試験センターによる解答例〕
削除申請のあった利用者IDをすぐにシステムから削除する。

（2）

〔試験センターによる解答例〕
システムに登録されている全ての利用者IDを抽出し，登録内容を確認すること

（3）

〔試験センターによる解答例〕
特権IDの利用者を特定できるようにしたいので

設問2

空欄a：発信元IPアドレス
空欄b：宛先ポート番号

設問3　（1）30字以内　（2）35字以内　（3）40字以内

（1）

〔試験センターによる解答例〕
多くの個人情報を含んでいてセキュリティ要件に反するので

（2）

〔試験センターによる解答例〕
ディスク容量の制約がある中で，ログの1年間保存に対応するため

(3)

LAN2はDMZであり，ログサーバのログの削除や改ざんの可能
性が高くなる

〔試験センターによる解答例〕
外部から不正アクセスによって，ログを改ざん，削除されるおそれがある。

設問4　40字以内

場所：LAN2

理由：

FWがWebサーバへのパケットだけを通過許可し，IDSの処理
能力が最小で済むから

〔試験センターによる解答例〕
FWが許可するパケットだけを解析することで，IDSの負荷が軽減されるので

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　中
	(2)	C 記憶＋記述型　中
	(3)	B ヒント＋記述型　易
設問2		A 解答探索型　中
設問3	(1)	B ヒント＋記述型　中
	(2)	B ヒント＋記述型　易
	(3)	B ヒント＋記述型　中
設問4		B ヒント＋記述型　易

設問1

(1) 利用者IDの削除プロセスは，問題文〔販売管理システムのアカウントの管理〕の上から二つ目の(1)～(3)に記述してある。

> (1) 上長がC氏に利用者ID削除申請書を送付する。
> (2) C氏は，毎月月末のID一覧表更新作業に合わせて，削除申請のあった利用者IDをシステムから削除する。
> (3) 利用者IDを削除した後，C氏は，上長に利用者ID削除完了通知を送付する。

上記の下線部が本問のヒントになっている。下線部の“毎月月末に利用者IDを削除する”としている点が問題があり，削除申請を受け付けたら，即時にその利用者IDを削除しなければならない。退職者や休職者のIDを不正利用したコンピュータ犯罪事例が発生しており，警視庁はセキュリティ対策（管理者向け）Webページで“退職した社員等のID・パスワードはすぐに無効にする手続をしたり，社員への情報セキュリティ教育の徹底を図って下さい”と呼びかけている。

(2) 本設問は，ヒントのない問題である。各上長は，自分の部下を熟知しているはずである。したがって，各上長は定期的にアカウントの管理を補完する目的で，システムから出力した自分の管理している部下の名簿一覧表を査閲して，間違いがないかを確認すればよい。例えば，先月退職した部下が残っている，見知らぬ名前が名簿にある，勤務している部下が記載されていない，などを発見するために，名簿一覧をレビューするのである。

(3) 問題文〔販売管理システムのアカウントの管理〕の最終段落は，下記のようになっている。

> システムの保守作業には，サーバの起動・停止，格納データの変更など，あらゆる操作が可能な特権IDが必要である。管理を簡素化するために，システム部全員で，一つの特権IDを共用している。特権IDを使用する場合は，個人の利用者IDでサーバにログインし，切替コマンドで個人の利用者IDから特権IDに切り替える仕組みにしている。

上記の実線の下線部には，“システム部全員で，一つの特権IDを共用している”と記述されているのだから，そのままでは一つの特権IDしかログに記録されず，特権IDを使ったシステム部の操作者を特定できない。それでは困るので，上記の点線の下線部のとおり“特権IDを使用する場合は，個人の利用者IDでサーバにログインし，切替コマンドで個人の利用者IDから特権IDに切り替える仕組みにしている”のである。したがって，本設問が問うている“個人の利用者IDでサーバにログインし，切替コマンドで個人の利用者IDから特権IDに切り替える仕組みにしている”理由は，“特権IDを使ったシステム部の操作者を特定したいから”になる。
情報セキュリティ管理基準（平成20年改正版）には，下記のような規定がある。

> 7.2.2.9 特権は，通常の業務用途に利用される利用者IDとは別の利用者IDに割り当てる
> 7.5.2.5 利用者のグループ又は特定の業務に対して，共有利用者IDを用いる場合，責任の追跡性を維持するための追加の管理策を導入する

なお，情報セキュリティ管理基準（平成20年改訂版）は，情報セキュリティ管理基準（平成28年改正版）に改訂されているが，本問は，平成23年度の問題なので，情報セキュリティ管理基準（平成20年改訂版）に準拠して解説している。

設問2

空欄a，bを含む問題文は，“同一の［ a ］から複数の［ b ］へのログが短時間に大量に発生している場合，ポートスキャンの有無を調査する”である。本設問のヒントは，この下線部のポートスキャンであり，これは“攻撃目標のサーバに，0，1，2，…のように順番にTCP及びUDPの宛先ポート番号でアクセスを行い，アクセス可能なポート番号を探し出す不正行為”である。ポートスキャンによって空きポート番号が判明すれば，そのポート番号を使ってDoS攻撃などを仕掛けてくるので，ポートスキャンは，攻撃の準備作業であ

るともいえる。

問題文〔注文受付システムの見直し〕(1)の2文目は“次の手順に示すように，図2の形式で保存されているFWのログを毎日，分析し，ポートスキャンの有無を調査する”としている。したがって，次の“図2　FWのログ”の項目名のいずれかが，空欄a，bに入る。

日時	発信元 IPアドレス	発信元 ポート番号	宛先 IPアドレス	宛先 ポート番号	プロトコル	アクション

ポートスキャンは，特定のPCから実行されるので空欄aは“発信元IPアドレス”になり，0，1，2，…のように順番にTCP及びUDPの宛先ポート番号でアクセスを行うので空欄bは“宛先ポート番号”になる。

設問3

(1) 本設問は，“セキュリティ要件から”と第1のヒントがあるので，第2のヒントを問題文〔セキュリティ要件〕から探してみる。

第2のヒントは，問題文〔セキュリティ要件〕(3)の“アクセスログとして保存する項目のうち，顧客情報などの個人情報は，必要最小限にする”である。問題文〔注文受付システムの検討〕の4文目は“注文受付システムのためのWebサーバ，アプリケーションサーバ，データベース（以下，DBという）サーバを新たに導入し，注文情報を注文DBに，顧客情報を顧客DBに保存する”となっており，DB更新ログには，顧客情報などの個人情報を含んでいる。したがって，それらの個人情報を取り除いたDBアクセスログを別に作成する。

なお，DBアクセスログに格納される項目は，〔注文受付システムの見直し〕(2)の1文目の“利用者ID，イベントタイプ，日時，成功／失敗，対象データのキー項目など”である。

(2) 本設問は，“セキュリティ要件から”と第1のヒントがあるので，第2のヒントを問題文〔セキュリティ要件〕から探してみる。

第2のヒントは，問題文〔セキュリティ要件〕(2)の“情報漏えいなどの問題が発生した場合に，アクセス元，アクセス者，アクセスされた情報などを調査するために，全てのサーバのアクセスログを1年間保存する”である。問題文〔注文受付システムの見直し〕(2)の最終文は“ディスク容量の制約から1か月ごとに，アクセスログをログサーバのディスクに直近1か月分を残したまま，磁気テープに退避して保管する”となっている。

上記の2か所の下線部より，ディスクの容量の制約からログサーバには1か月分のログ情報しか保存できないのに，セキュリティ要件は1年間分のログ情報の保存を要求しているから，保存したログ情報を磁気テープに退避するのだと解答を導ける。

(3) LAN2には，外部に公開しているWebサーバがあり，図1の注書きにもあるとおり，LAN2は，DMZ（DeMilitarized Zone：非武装セグメント）である。FW（ファイアウォール）は，インターネットからLAN2内にあるWebサーバへのパケットの通過を許可せざるを得ない。したがって，LAN2はLAN3やLAN4のような内部セグメントや社内LANよりも，インターネットからの攻撃を受けやすい。
攻撃を受けやすいLAN2にログサーバを設置すると，ログサーバ内にあるログ情報の削除や改ざんの可能性が高くなるので，それを解答にまとめればよい。

設問4

〔Webサーバのコンテンツ改ざん〕の5文目は，“IDSでは，接続しているネットワークセグメントのトラフィックを監視し，ネットワークを流れるパケットのプロトコルヘッダやデータをあらかじめ定義されたルールに基づいて解析する”としており，導入されるIDSを説明している。このようなIDSを“ネットワーク型IDS”といい，ホスト（サーバなど）を監視対象にして不正侵入を監視する“ホスト型IDS”と対比される。

本設問のヒントは，〔Webサーバのコンテンツ改ざん〕の最終文“ただし，解析処理に多くのCPU資源を使用することから，ネットワークトラフィックが増加すると，侵入検知機能が停止してしまうおそれがあるので，IDSの設置場所と，その設置場所に応じた処理能力の検討が必要である”の下線部である。

WebサーバはLAN2内にあるので，Webサーバを攻撃対象にするパケットを効率よく発見するためには，FW（ファイアウォール）によってWebサーバへのパケットだけが通過許可されるLAN2内に本問のIDSを設置するのが適切である。こうすると，IDSのパケット解析処理能力は，最小で済む。