演習　セキュリティ管理における脆弱性検査

平成24年度 問4

問　セキュリティ管理における脆弱(ぜい)性検査に関する次の記述を読んで，設問1～3に答えよ。

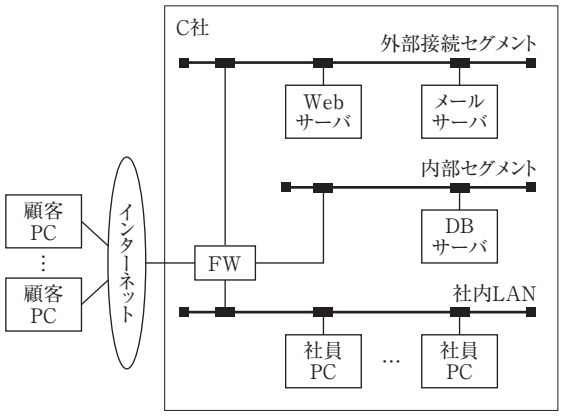
C社は，健康食品の製造・販売会社である。インターネットを利用した販売を行うためのシステムとして，Webサーバ，データベースサーバ（以下，DBサーバという），メールサーバなどで構成される販売管理システムを運用している。

最近，インターネットを利用した同業他社の販売管理システムが不正アクセスを受け，顧客情報が漏えいする事件があった。そこで，情報システム部のJ部長は，セキュリティ対策の有効性を確認するために脆弱性検査を行う必要があると考え，ITサービスマネージャのD氏に，脆弱性検査会社のR社と協力して検査を行うよう指示した。

〔C社販売管理システムの概要〕

販売管理システムの利用者には，顧客，営業部員などがいる。顧客は，顧客PCからインターネット経由でWebサーバにアクセスし，商品を検索して購入する。営業部員は，社員PCからWebサーバにアクセスし，受注，在庫確認などを行う。

販売管理システムの構成を図1に示す。



外部接続セグメント：インターネットに接続するサーバを設置するセグメント
内部セグメント：社内LAN及び外部接続セグメントだけからアクセス可能なセグメント
社内LAN：社員PCを設置するセグメント
FW：ファイアウォール

図1　販売管理システムの構成

・Webサーバは，アプリケーションサーバ機能も兼ねている。
・DBサーバは，受注情報，商品の在庫情報・価格情報，及び利用者情報（利用者ID，パスワード）を管理している。
・メールサーバは，電子メールを送受信する機能と，DNSの機能を備えている。
・Webサーバ，DBサーバ及びメールサーバでは，ログを取得している。情報システム部では，それらを販売管理システムのログとして管理している。
・販売管理システムは，月1回の定期保守日を除いて，稼働している。

〔販売管理システムのセキュリティ対策〕

販売管理システムのセキュリティ対策は次のとおりである。

(1) 利用者認証は，利用者IDとパスワードの組合せで行う。
・利用者IDは，利用者を一意に識別する。
・パスワードは，8文字以上の文字列で設定し，90日以内に更新することを義務付けている。また，直近の3世代のパスワードは再設定不可としている。
・システムの管理にはシステム管理特権を有する利用者ID（以下，特権IDという）が必要である。情報システム部のシステム管理者には特権IDが付与されている。システム管理者が特権IDを利用した作業を行う場合は，J部長に申請する。
・システム管理者以外の情報システム部員がシステムの管理を行う場合，作業内容を添えて特権IDの付与をシステム管理者に申請する。システム管理者は申請内容を確認し，作業期間だけ有効な特権IDを新規に作成し，申請者に付与する。

(2) 特権IDを使用した操作が実施されると，操作日時と操作内容が記載された電子メール（以下，特権ID行使メールという）がシステム管理者に通知される。

(3) システム管理者は，通知を受けた特権ID行使メールを基に販売管理システムのログを参照し，特権IDを使った操作に問題がないことを確認する。また，D氏は，ログとその統計情報から不正アクセスの有無を点検している。

(4) 情報システム部では，販売管理システムの脆弱性を改善するために，セキュリティパッチの適用を定期的に実施している。

〔FWのアクセス制御要件〕

FWのアクセス制御要件は次のとおりである。

・インターネットからメールサーバへは，DNSサービス，SMTPサービスへのアクセスだけを許可する。
・インターネットからWebサーバへは，HTTPサービス，HTTPSサービスへのアクセスだけを許可する。

・社内LANから内部セグメント及び外部接続セグメントへは，全サービスへのアクセスを許可する。
・WebサーバからDBサーバへのアクセスを許可する。
・メールサーバからインターネットへは，DNSサービス，SMTPサービスへのアクセスだけを許可する。
・上記以外のアクセスは全て遮断する。

〔サーバの監視〕

販売管理システムのサーバの監視は，監視サービス会社に委託している。レスポンスの低下及びハードウェア障害を検知した場合は，自動的に監視サービス会社に通知され，監視サービス会社が迅速に初動対応を行っている。

月1回の定期保守の際，システム管理者が各サーバの時刻を確認し，FWの時刻と異なる場合は，手動で時刻を補正しているが，時刻が大きくずれていることも多い。

〔脆弱性検査の計画〕

D氏は，R社と打合せを行い，脆弱性検査を，次のように計画した。

(1) 検査は，本番サービス中に行う。
(2) 検査は，Webサーバとメールサーバに対しては社外と社内の両方から実施し，DBサーバに対しては社内から実施する。社外からの検査は，R社の検査端末からインターネット経由で実施する。一方，社内からの検査は，社内LANにC社の検査端末として設置したPCから実施する。
(3) 検査によってシステムへの負荷が増えるが，潜在する脆弱性を極力洗い出すために，R社が検査可能な項目のほぼ全てを検査する。
(4) 検査日程と，考えられる検査の影響を社内関連部門に事前に通知する。

検査の準備作業として，D氏は，社内LANに設置するC社の検査端末のプライベートIPアドレスをR社に連絡するとともに，(ア)R社の検査端末のグローバルIPアドレスを確認した。

〔脆弱性検査の結果〕

R社からC社に対して，脆弱性検査の結果が報告された。報告の一部として，発見されたサーバとサービスを表1に，発見された脆弱性を表2に示す。

表1　発見されたサーバとサービス

検査元	経由	検査先セグメント	発見されたサーバ	サービス					
				HTTP	HTTPS	TELNET	DNS	SMTP	POP
R社検査端末	インターネット	外部接続セグメント	Webサーバ	○	○	○			
			メールサーバ				○	○	
C社検査端末	社内LAN	外部接続セグメント	Webサーバ	○	○	○			
			メールサーバ				○	○	○
		内部セグメント	DBサーバ						

注記　○は，発見されたサービスを示す。

表2　発見された脆弱性

No.	発見された脆弱性の緊急度・詳細内容		検査対象サーバ	
	緊急度	詳細内容	Webサーバ	メールサーバ
1	高	脆弱性①：パッチXが未適用であり，バッファオーバフローによって管理者権限を奪われる	○	○
2	高	脆弱性②：総当たり攻撃によってシステム管理者の利用者IDとパスワードが発見される	○	
3	高	脆弱性③：メールヘッダインジェクションによって意図しないメール送信が可能である	○	
以下省略				

注記　○は，脆弱性が発見されたサーバを示す。

〔脆弱性への対応〕

D氏は，R社からの報告を受け，(イ)過去のログを確認した。また，次の対策を検討し，J部長の承認を得た。

・脆弱性①：パッチXは，バッファオーバフローによって管理者権限を奪われる攻撃を防ぐものであるが，Webサーバ及びメールサーバで稼働しているアプリケーションの動作に影響するので適用を見送る。代替案として，Webサーバ及びメールサーバへのセキュリティ対策ソフトウェアの導入によって，脆弱性を回避する。

・脆弱性②：パスワードの設定規則をより強固なものに変更するとともに，総当たり攻撃への対策として(ウ)販売管理システムのログイン処理に機能を追加する。

・脆弱性③：---略---

・FWの脆弱性：〔FWのアクセス制御要件〕を満たしていないので，FWに対して，

［ a ］から［ b ］への，［ c ］サービスへのアクセスを許可しない設定を行う。

〔外部監査人の指摘〕

C社は，内部統制強化の一環として，システム運用に関して，外部監査人による監査を受けた。監査の結果，2点の指摘を受けた。

① (エ) システム管理者が特権IDを使う操作をした場合，内部統制の観点で問題がある。

② 販売管理システムのログを分析し，特権IDを使用した操作の正当性を確認する際に，ログの分析に支障を来すおそれがある。

D氏は，②の対策として，NTPサーバの導入をJ部長に提案し，了承を得た。

設問1　〔脆弱性検査の計画〕について，(1)，(2)に答えよ。

(1) 脆弱性検査を本番サービス実行中に行う予定である。これによる混乱を避けるために，事前に実施すべき対策が他にもある。対策を40字以内で述べよ。

(2) 本文中の下線(ア)について，D氏がグローバルIPアドレスを確認した目的を，40字以内で述べよ。

設問2　〔脆弱性への対応〕について，(1) ～ (3)に答えよ。

(1) 本文中の下線(イ)について，過去のログを確認する目的を，40字以内で述べよ。

(2) 本文中の下線(ウ)について，追加する機能を40字以内で述べよ

(3) 本文中の［ a ］～［ c ］に入れる適切な字句を，表1の中から選んで答えよ。

なお，［ a ］は“経由”例から，［ b ］は“発見されたサーバ”列から選べ。

設問3　〔外部監査人の指摘〕について，(1)，(2)に答えよ。

(1) 本文中の下線(エ)の指摘について，改善策を30字以内で述べよ。

(2) D氏が，NTPサーバの導入を提案した理由を40字以内で述べよ。

解答例

設問1　（1）40字以内　（2）40字以内

（1）

〔試験センターによる解答例〕
販売管理システムの監視サービス会社に対し，脆弱性検査の計画を通知する。

（2）

〔試験センターによる解答例〕
各サーバのログを，検査に伴うレコードと通常運用のレコードに区別するため

設問2　（1）40字以内　（2）40字以内

（1）

〔試験センターによる解答例〕
不正アクセスがあった場合，対策の内容と対策の緊急度を決めるため

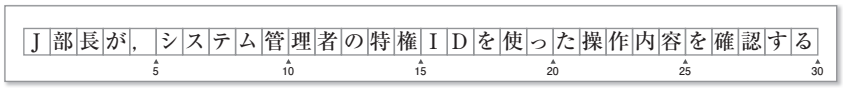
（2）

〔試験センターによる解答例〕
連続して利用者認証に失敗した場合に，該当する利用者IDをロックする機能

（3）　空欄a：インターネット
空欄b：Webサーバ
空欄c：TELNET

設問3　（1）30字以内　（2）40字以内

（1）



〔試験センターによる解答例〕

システム管理者以外の情報システム部員が作業内容を確認する。

（2）

〔試験センターによる解答例〕

全サーバの時刻が一致していないと，取得したログの分析に支障があるから

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

設問1

(1) 本問がいう脆弱性検査とは，“ペネトレーションテスト”とも呼ばれ，検査会社の担当者が検査対象システム及びネットワークを外部から実際に攻撃し，侵入を試みて，セキュリティ上の弱点を発見するテスト手法である。したがって，この疑似攻撃によって本番サーバがダウンする，もしくはウイルスが蔓延するなどのインシデントが発生した場合，検査を依頼した会社は大混乱する。そこで，通常は，本番環境をコピーして構築したテスト環境に対し，ペネトレーションテストを実施する。しかし，本問では，問題の設定上，本番サービス実行中に脆弱性検査を実施している。

本設問のヒントは，問題文〔脆弱性検査の計画〕(4)の“検査日程と，考えられる検査の影響を社内関連部門に事前に通知する”である。事前通知は，社内関連部門だけではなく，脆弱性検査によって何らかの不利益を受けそうな利害関係者全員になされるべきである。

問題文〔サーバの監視〕の1文目は“販売管理システムのサーバの監視は，監視サービス会社に委託している”となっているので，監視サービス会社に事前通知しなければならない。

また，C社の顧客にも事前通知しなければならないとも考えられるが，顧客の中にハッカーやクラッカーのような悪意者がいる可能性も否定できないので，顧客は事前通知の対象にならない。

(2) 本文中の下線(ア)に記述されている“R社の検査端末”は，C社の販売管理システムに攻撃を仕掛ける端末である。問題文〔脆弱性検査の計画〕(2)の1文目は“検査は，Webサーバとメールサーバに対しては社外と社内の両方から実施し，DBサーバに対

しては社内から実施する。社外からの検査は，R社の検査端末からインターネット経由で実施する”としているので，R社の検査端末は，Webサーバとメールサーバに対して疑似攻撃を仕掛ける。

問題文〔C社販売管理システムの概要〕の最後から3文目は“Webサーバ，DBサーバ及びメールサーバでは，ログを取得している”としているので，R社の検査端末のグローバルIPアドレスは，そのログに記録されるはずである。また，脆弱性検査は本番サービス中に実施されるので，そのログには，顧客PCのグローバルIPアドレスも記録される。

D氏が，R社の検査端末のグローバルIPアドレスを確認した目的は，Webサーバとメールサーバのログのうち，R社の検査端末が作成したものを特定するためである。

設問2

(1) 本文中の下線(イ)を含む文は“D氏は，R社からの報告を受け，(イ)過去のログを確認した”となっており，そのR社からの報告は，表1及び表2に示されている。表2のNo.1 ～ 3の緊急度はすべて“高”になっており，“管理者権限が奪われる”・“利用者IDとパスワードが発見される”・“意図しないメール送信が可能である”といった脆弱性が発見されている。

したがって，D氏は過去のログを確認して，その脆弱性を突く攻撃もしくは不正アクセスの試みの有無を調査したのである。

(2) 本文中の下線(ウ)を含む文は“パスワードの設定規則をより強固なものに変更するとともに，総当たり攻撃への対策として(ウ)販売管理システムのログイン処理に機能を追加する”となっている。上記の点線の下線部の総当たり攻撃とは，ブルートフォース攻撃とも呼ばれ，攻撃用のプログラムによって，考えられるすべてのパスワードの組合せを“しらみつぶし”に試してみる方法である。

総当たり攻撃への対策には，通常，“アカウントロックアウト機能”が採用される。アカウントロックアウト機能とは，一定回数(通常3回)以上，間違ったログインパスワード入力がなされると，その利用者IDをロックし，使用できなくすることである。

(3) 問題文〔FWのアクセス制御要件〕の3文目は“インターネットからWebサーバへは，HTTPサービス，HTTPSサービスへのアクセスだけを許可する”となっている。これに対し，次の表1の網掛けで示した○の部分は，違反している。

検査元	経由	検査先セグメント	発見されたサーバ	サービス					
				HTTP	HTTPS	TELNET	DNS	SMTP	POP
R社 検査端末	インターネット	外部接続セグメント	Webサーバ	○	○	○			
			メールサーバ				○	○	
C社 検査端末	社内LAN	外部接続セグメント	Webサーバ	○	○	○			
			メールサーバ				○	○	○
		内部セグメント	DBサーバ						

したがって，空欄aは“インターネット”，空欄bは“Webサーバ”，空欄cは“TELNET”になる。

設問3

(1) 本文中の下線(エ)は，“(エ)システム管理者が特権IDを使う操作をした場合，内部統制の観点で問題がある”となっている。この内部統制の観点の一つに“内部牽制”がある。これは，適切な職務分掌(一つの職務を2人で分担すること)により，企業などで不正・誤謬を事前に防ぐ制度のことである。例えば，Aさんがある職務を完了すると，Bさんがそれをチェックし，その正当性を確認することである。こうすれば，Aさんが背任行為を行っても，Bさんはそれに気づくはずである。

問題文〔販売管理システムのセキュリティ対策〕の7文目は“情報システム部のシステム管理者には特権IDが付与されている”であり，9，10文目は“システム管理者以外の情報システム部員がシステムの管理を行う場合，作業内容を添えて特権IDの付与をシステム管理者に申請する。システム管理者は申請内容を確認し，作業期間だけ有効な特権IDを新規に作成し，申請者に付与する”である。したがって，特権IDを使用できるのは，システム管理者と申請をしたシステム管理者以外の情報システム部員である。

問題文〔販売管理システムのセキュリティ対策〕の(2)(3)は，以下のようになっている。

> (2) 特権IDを使用した操作が実施されると，操作日時と操作内容が記載された電子メール(以下，特権ID行使メールという)がシステム管理者に通知される。
> (3) システム管理者は，通知を受けた特権ID行使メールを基に販売管理システムのログを参照し，特権IDを使った操作に問題がないことを確認する。

前の記述より，システム管理者が特権IDを使用した操作を実施した場合，自らがその操作に問題がないことを確認することになり，上記の内部牽制ができない。
したがって，システム管理者が特権IDを使う操作をした場合，システム管理者以外の情報システム部員もしくはJ部長が操作内容とその結果に問題がないことを確認しなければならない。
筆者の解答例は，問題文〔販売管理システムのセキュリティ対策〕の8文目である“システム管理者が特権IDを利用した作業を行う場合は，J部長に申請する”をヒントにして，J部長が確認することにした。

(2) 問題文〔外部監査人の指摘〕の最後から2文は，下記のようになっている。

> ② 販売管理システムのログを分析し，特権IDを使用した操作の正当性を確認する際に，ログの分析に支障を来すおそれがある。
> D氏は，②の対策として，NTPサーバの導入をJ部長に提案し，了承を得た。

NTP（Network Time Protocol）サーバは，インターネットで標準的に利用されているサーバやネットワーク機器などの時刻同期を取るためのプロトコルである。サーバなどの時刻は，内蔵タイマによって管理されており，各サーバなどの内蔵タイマの時刻が一致している保証はない。そこで，各サーバなどは，NTPサーバにアクセスして標準時刻を取得し，内蔵タイマの時刻をそれに合わせる。こうすれば，各サーバなどの内蔵タイマの時刻は実用上問題のない範囲で一致する。
もし，各サーバなどの内蔵タイマの時刻が異なっている場合，ログに出力されるタイムスタンプはまちまちになり，各ログの時間的な前後や間隔が分からなくなる。したがって，上記の下線部のようにログ分析に支障を来すおそれがある。