AP

令和７年度　春期
応用情報技術者試験
午後　問題

試験時間	13:00 ～ 15:30（２時間 30 分）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. 答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。
4. 問題は，次の表に従って解答してください。

問題番号	問１	問２～問 11
選択方法	必須	４問選択

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B 又は HB の黒鉛筆又はシャープペンシルを使用してください。
   (2) 受験番号欄に受験番号を，生年月日欄に受験票の生年月日を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) 選択した問題については，右の例に従って，選択欄の問題番号を○印で囲んでください。○印がない場合は，採点されません。問 2～問 11 について，5 問以上○印で囲んだ場合は，はじめの 4 問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問３，問４，問６，問８を選択した場合の例〕

選択欄	
必須	(問１)
４問選択	問２
	(問３)
	(問４)
	問５
	(問６)
	問７
	(問８)
	問９
	問10
	問11

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

次の問1は必須問題です。必ず解答してください。

問1　サイバー攻撃への対策に関する次の記述を読んで，設問に答えよ。

C社は首都圏に複数の販売店をもつ，中堅の中古車販売会社である。

C社はS県に複数の中古車販売店舗を展開するP社と業務提携しており，P社の中古車情報もC社の販売管理システムに登録した上で販売を行っている。

〔C社販売管理システムの概要〕

販売管理システムは，Webサーバ，アプリケーション（以下，APという）サーバ及びデータベース（以下，DBという）サーバから成り，C社及びP社の販売店は，Webサーバを経由して中古車情報や販売実績の登録を行う。C社の販売店の情報は，C社内のPC（以下，PC-Cという）から，APサーバの販売店情報登録ツール（以下，販売店ツールという）を利用して登録を行う。また，販売管理システムのWebサーバ，APサーバ及びDBサーバ（以下，C社各サーバという）のメンテナンスは，C社の社内システム担当が，社内システム用のPC（以下，PC-Sという）から管理者権限のあるID（以下，特権IDという）でC社各サーバにログインして実施している。

P社の販売店の情報は，P社従業員が，社内に設置したP社販売店情報登録用のPC（以下，PC-Pという）から，C社内に設置したP社販売店情報登録用のPC（以下，PC-Rという）にリモートデスクトップでログインし，販売店ツールを利用して登録を行う。P社は，P社従業員の自宅PC（以下，自宅PCという）からSSL-VPNを利用して，PC-Pにリモートデスクトップでログインできる環境を構築している。

C社及びP社のネットワーク構成（抜粋）を図1に示す。

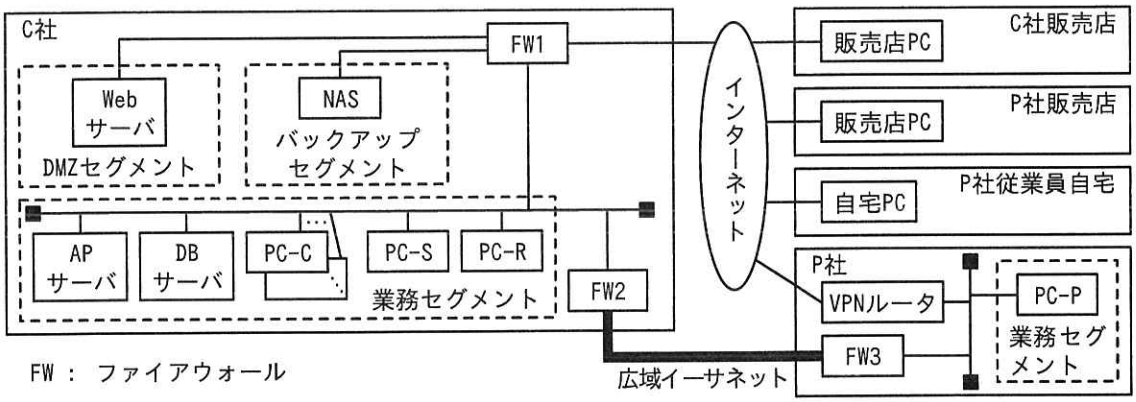

図1　C社及びP社のネットワーク構成（抜粋）

C 社 FW1，FW2 及び P 社 FW3 の許可ルール（抜粋）を表 1 に示す。

表 1　C 社 FW1，FW2 及び P 社 FW3 の許可ルール（抜粋）

機器	送信元	送信先	プロトコル/ポート番号
FW1	インターネット	DMZ セグメント	TCP/443（HTTPS）
FW1	Web サーバ	AP サーバ	TCP/80（HTTP）
FW1	Web サーバ	バックアップセグメント	TCP/22（SSH）
FW1	AP サーバ，DB サーバ	バックアップセグメント	TCP/22（SSH）
FW2	P 社の業務セグメント	C 社の業務セグメント	TCP/3389（RDP）
FW3	P 社の業務セグメント	C 社の業務セグメント	TCP/3389（RDP）

注記　FW1，FW2 及び FW3 は，応答パケットを自動的に通過させる，ステートフルパケットインスペクション機能をもつ。

C 社各サーバにはマルウェア対策ソフトウェアがインストールされている。C 社各サーバのデータは，毎日午前 0 時 30 分～午前 1 時 30 分の間にバックアップを行う。月曜日にデータのフルバックアップを行い，火曜日から日曜日まではデータの差分バックアップを行っている。NAS には月曜日を起点として最大 7 日分のバックアップを 1 世代分保存しており，次の世代のデータは前の世代のデータに上書き保存される。また，C 社各サーバのシステムバックアップも NAS に保存している。

C 社及び P 社の各 PC，各サーバ及びネットワーク機器のログは各機器内部に保存しており，ログのサイズが最大値に達した場合は，最も古い記録から上書きする設定になっている。

C 社の各 PC 及び各サーバはログインのロックアウトのしきい値を 5 回に設定している。

〔セキュリティインシデントの発生〕

ある月曜日の午前 9 時頃，C 社のシステム部門に，C 社販売店から販売管理システムが利用できないとの報告があった。システム部門の R 主任が販売管理システムを調査したところ，C 社各サーバのデータが暗号化されていることが判明した。

R 主任は外部のセキュリティ会社である U 社に連絡してインシデントの調査を依頼した。U 社の X 氏から“①電磁的記録の証拠保全，調査及び分析を行うので，C 社内のインターネットと広域イーサネットに接続しているネットワークを遮断した後，全ての PC の使用を停止してください”との要請があり，R 主任は要請に従った。

〔セキュリティインシデントの調査〕

X 氏から“PC，サーバ及びネットワーク機器のログを分析した結果，侵入者は次の(1)～(4)の順序で攻撃したことが判明した”と報告があった。

(1) インシデントの報告日の午前 3 時 15 分に，PC-P から PC-R にログインした。

(2) PC-R と同じパスワードのログイン ID が PC-S に存在していた。PC-R のログインに利用したパスワードで，PC-S にリバースブルートフォース攻撃を行い，PC-S にログインした。

(3) “社内システム担当がサーバにログインする際に利用した ID とパスワードを，PC-S のメモリ上に保存してしまう”という PC-S の AP ソフトウェアの脆弱(ぜい)性を利用して，C 社各サーバにログインした。

(4) C 社各サーバのマルウェア対策ソフトウェアのプロセスを強制終了して，ランサムウェアを実行した。

X 氏は“侵入経路である P 社の機器も C 社と同様に電磁的記録の証拠保全，調査及び分析を行う必要があるので，P 社へ連絡するように”と R 主任に要請した。

X 氏が PC-P 及び P 社のネットワーク機器を調査したところ，次の状況が判明した。

・VPN ルータには認証に関する脆弱性があった。

・攻撃に利用された PC-P の ID とパスワードは PC-R と同一であった。

・PC-P の ID は“admin”，パスワードは“password123456”であった。

・PC-P へは“administrator”の ID に対して異なるパスワードで約 1 万回ログインに失敗した後，“admin”の ID に対して異なるパスワードで 150 回ログインに失敗し，151 回目でログインに成功していた。

X 氏は“侵入者は VPN ルータの脆弱性を利用して，認証情報を取得した上で VPN 接続を行い，PC-P へ［ a ］攻撃を行い侵入した後，［ b ］で PC-R へログインした可能性が高い。PC-P のログインに関する設定が PC-R と異なっていたので，［ a ］攻撃を防げずに侵入されたと推測される。”と R 主任へ報告した。

〔暫定対応及びシステムの復旧〕

侵入経路と原因が判明したので，R 主任及び P 社は次の暫定対応を実施し，C 社各サーバのシステム及びデータをバックアップデータから復旧の上，販売管理システムの利用を再開した。

・VPN ルータと PC-S の AP ソフトウェアに，脆弱性に対応した修正プログラムを適用した。

・PC 及びサーバの ID とパスワードを推測が困難で複雑なものへ変更した。

・②今回と同様の攻撃を防御するために，PC-P の設定を変更した。ただし，パスワードが漏えいし，リバースブルートフォース攻撃を受けた場合は，この PC-P の設定変更では防御できないおそれがあるので，PC-R へのリモートデスクトップでのログインは，P 社からの利用申請を受けて C 社が許可したときだけ可能とするルールを設けることにした。

〔U 社から C 社への報告〕

U 社は C 社へ，C 社の課題をまとめて報告した。C 社の課題（抜粋）を表 2 に示す。

表 2　C 社の課題（抜粋）

項番	課題
1	C 社に接続する P 社の PC 及びネットワーク機器について，機器管理や脆弱性管理ができていない。
2	侵入者が特権 ID でログインし，今回のように C 社各サーバで操作を行った場合，マルウェアの検知ができなくなる。
3	インシデントの報告日の前日にランサムウェアに感染して暗号化されていた場合，③バックアップデータからの復旧に問題が生じたおそれがある。また，NAS に侵入されてバックアップデータが暗号化されるリスクもある。
4	一定期間に大量の攻撃を受けた場合，④過去に発生した事象が調査できなくなるおそれがある。

〔課題に対する対策〕

R 主任は，課題に対して次の対策案を検討した。

・項番 1 の対策として，C 社に接続する P 社の PC 及びネットワーク機器の情報を P 社から提供してもらい，機器の一覧を作成する。また，P 社に運用ルールの作成を依頼し，作成してもらった運用ルールが適切であることを確認する。

・項番 2 の対策として，R 主任を特権 ID 管理者とし，R 主任が許可した場合だけ，特権 ID を利用可能にする運用ルールを作成する。また，R 主任が許可した場合には，特権 ID にワンタイムパスワードを設定し，利用者に払い出す仕組みを導入する。

・項番 3 の対策として，バックアップデータが暗号化されないように，NAS に加えて，［ c ］バックアップに対応したストレージにバックアップデータを保存する。また，バックアップデータは 3 世代分保存する。

・項番 4 の対策として，ログサーバを設置し，PC，サーバ及びネットワーク機器のログを保存する。

R 主任は，C 社内の再発防止会議で対策案の報告を行い，対策案は承認された。

設問 1　本文中の下線①の調査方法の名称を，片仮名 12 字以内で答えよ。

設問 2　本文中の［ a ］に入れる適切な字句，本文中の［ b ］に入れる適切なプロトコル名をそれぞれ解答群の中から選び，記号で答えよ。

解答群

ア　HTTP	イ　HTTPS	ウ　RDP
エ　SSH	オ　辞書	カ　中間者
キ　パスワードスプレー	ク　リプレイ	

設問 3　本文中の下線②について，変更した設定項目を，本文中の字句を用いて 15 字以内で答えよ。また，防御できないおそれがある理由を，“同一”という字句を用いて 25 字以内で答えよ。

設問 4　〔U 社から C 社への報告〕について答えよ。

(1)　表 2 中の下線③について，バックアップデータに発生していたおそれがある事象を 30 字以内で答えよ。

(2)　表 2 中の下線④について，調査ができなくなる理由を 20 字以内で答えよ。

設問 5　本文中の［ c ］に入れる適切な字句を解答群の中から選び，記号で答えよ。

解答群

ア　イミュータブル	イ　インクリメンタル
ウ　ディファレンシャル	エ　マルチプル