応用情報技術者

午後対策問題集

無料体験入学者用

TAC

はじめに

この問題集は,弊社刊「応用情報技術者試験対策テキストⅠ・Ⅱ・Ⅲ」の各学習項目に対応させて作成された問題集です。応用情報技術者試験の午後試験出題範囲である各分野(テクノロジ系，マネジメント系,ストラテジ系)の問題を，広く多数掲載しています。

本書は，過去の情報処理技術者試験において出題された午後問題で構成されています。実際の応用情報技術者試験の出題形式に合わせ,テーマごとに問題を集めて掲載しています(出典は目次の後)。

試験に合格するためには，テキストによる知識のインプットだけではなく,問題演習によるアウトプット(力試し)が非常に重要になります。問題を解き，間違えた問題のジャンルについては学習しなおして再度挑戦するという学習サイクルを身に付けましょう。

本書が，応用情報技術者試験の合格のお役に立てることを願ってやみません。

TAC情報処理講座

目　次

出典一覧

第1章　プログラミング

問1	令和3年度秋期本試験	問3
問2	令和元年度秋期本試験	問3
問3	令和2年度本試験	問3
問4	令和4年度秋期本試験	問3

第2章　システムアーキテクチャ

問1	令和3年度秋期本試験	問4
問2	平成31年度春期本試験	問4
問3	令和元年度秋期本試験	問4
問4	令和4年度秋期本試験	問4

第3章　データベース

問1	平成30年度春期本試験	問6
問2	平成元年度秋期本試験	問6
問3	令和2年度本試験	問6
問4	令和4年度秋期本試験	問6

第4章　ネットワーク

問1	令和2年度本試験	問5
問2	令和3年度秋期本試験	問5
問3	平成30年度春期本試験	問5
問4	平成29年度秋期本試験	問5

第5章　情報セキュリティ

問1	平成29年度秋期本試験	問1
問2	平成31年度春期本試験	問1
問3	令和元年度秋期本試験	問1
問4	令和4年度秋期本試験	問1
問5	令和3年度春期本試験	問1
問6	令和2年度本試験	問1
問7	令和4年度春期本試験	問1
問8	令和3年度秋期本試験	問1

第6章　情報システム開発

問1	平成30年度春期本試験	問8
問2	令和3年度秋期本試験	問8
問3	平成29年度春期本試験	問8
問4	令和4年度春期本試験	問8

第7章　組込みシステム開発

問1	平成31年度春期本試験	問7
問2	令和3年度春期本試験	問7
問3	令和元年度秋期本試験	問7
問4	令和4年度春期本試験	問7

第8章　プロジェクトマネジメント

問1	令和4年度秋期本試験	問9
問2	令和元年度秋期本試験	問9
問3	平成31年度春期本試験	問9
問4	令和3年度秋期本試験	問9

第9章　サービスマネジメント

問1	令和4年度春期本試験	問10
問2	令和3年度秋期本試験	問10
問3	平成30年度秋期本試験	問10
問4	令和3年度春期本試験	問10

第10章　システム監査

問1	令和2年度本試験	問11
問2	平成31年度春期本試験	問11
問3	令和4年度秋期本試験	問11
問4	平成29年度春期本試験	問11

第11章　経営戦略

問1	令和3年度春期本試験	問2
問2	平成30年度春期本試験	問2
問3	令和4年度秋期本試験	問2
問4	令和元年度秋期本試験	問2

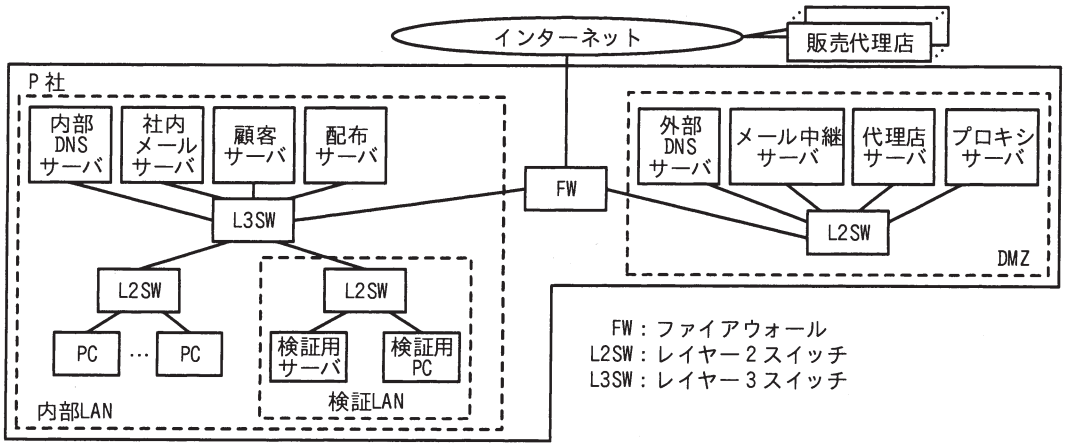
第５章　情報セキュリティ

問4　マルウェアへの対応策に関する次の記述を読んで，設問に答えよ。

P社は，従業員数400名のIT関連製品の卸売会社であり，300社の販売代理店をもっている。P社では，販売代理店向けに，インターネット経由で商品情報の提供，見積書の作成を行う代理店サーバを運用している。また，従業員向けに，代理店ごとの卸価格や担当者の情報を管理する顧客サーバを運用している。代理店サーバ及び顧客サーバには，HTTP Over TLSでアクセスする。

P社のネットワークの運用及び情報セキュリティインシデント対応は，情報システム部（以下，システム部という）の運用グループが行っている。

P社のネットワーク構成を図1に示す。



注記1　配布サーバは，PCにセキュリティパッチなどを配布するサーバである。
注記2　検証LANは，サーバ及びPCの動作検証などを行うためのLANである。

図1　P社のネットワーク構成

〔セキュリティ対策の現状〕

P社では，複数のサーバ，PC及びネットワーク機器を運用しており，それらには次のセキュリティ対策を実施している。

・［　a　］では，インターネットとDMZ間及び内部LANとDMZ間で業務に必要な通信だけを許可し，通信ログ及び遮断ログを取得する。

・［　b　］では，SPF（Sender Policy Framework）機能によって送信元ドメイン認証を行い，送信元メールアドレスがなりすまされた電子メール（以下，電子メールをメールという）を隔離する。

・外部 DNS サーバでは，DMZ のゾーン情報の管理のほかに，キャッシュサーバの機能を稼働させており，外部DNSサーバを①DDoSの踏み台とする攻撃への対策を行う。
・P 社からインターネット上の Web サーバへのアクセスは，DMZ のプロキシサーバを経由し，プロキシサーバでは，通信ログを取得する。
・PC 及びサーバで稼働するマルウェア対策ソフトは，毎日，決められた時刻にベンダーの Web サイトをチェックし，マルウェア定義ファイルが新たに登録されている場合は，ダウンロードして更新する。
・システム部の担当者は，毎日，ベンダーの Web サイトをチェックし，OS のセキュリティパッチやアップデート版の有無を確認する。最新版が更新されている場合は，ダウンロードして検証 LAN で動作確認を 1 週間程度行う。動作に問題がなければ，PC 向けのものは［ c ］に登録し，サーバ向けのものは，休日に担当者が各サーバに対して更新作業を行う。
・PC は，電源投入時に［ c ］にアクセスし，更新が必要な新しい版が登録されている場合は，ダウンロードして更新処理を行う。
・FW 及びプロキシサーバのログの検査は，担当者が週に 1 回実施する。

〔マルウェア X の調査〕

ある日，システム部の Q 課長は，マルウェア X の被害が社外で多発していることを知り，R 主任にマルウェア X の調査を指示した。R 主任による調査結果を次に示す。

(1) 攻撃者は，不正なマクロを含む文書ファイル（以下，マクロ付き文書ファイル A という）をメールに添付して送信する。
(2) 受信者が，添付されたマクロ付き文書ファイル A を開きマクロを実行させると，マルウェアへの指令や不正アクセスの制御を行うインターネット上の C&C サーバと通信が行われ，マルウェア X の本体がダウンロードされる。
(3) PC に侵入したマルウェア X は，内部ネットワークの探索，情報の窃取，窃取した情報の C&C サーバへの送信及び感染拡大を，次の(a)～(d)の手順で試みる。
(a) ②PC が接続するセグメント及び社内の他のセグメントの全てのホストアドレス宛てに，宛先アドレスを変えながら ICMP エコー要求パケットを送信し，連続してホストの情報を取得する。
(b) ③(a)によって情報を取得できたホストに対して，攻撃対象のポート番号を

セットしたTCPのSYNパケットを送信し，応答内容を確認する。

(c)　(b)でSYN/ACKの応答があった場合，指定したポート番号のサービスの脆弱性を悪用して個人情報や秘密情報などを窃取し，C&Cサーバに送信する。

(d)　侵入したPCに保存されている過去にやり取りされたメールを悪用し，当該PC上でマクロ付き文書ファイルAを添付した返信メールを作成し，このメールを取引先などに送信して感染拡大を試みる。

R主任が調査結果をQ課長に報告したときの，2人の会話を次に示す。

Q課長：マルウェアXに対して，現在の対策で十分だろうか。

R主任：十分ではないと考えます。文書ファイルに組み込まれたマクロは，容易に処理内容が分析できない構造になっており，マルウェア対策ソフトでは発見できない場合があります。また，④マルウェアXに感染した社外のPCから送られてきたメールは，SPF機能ではなりすましが発見できません。

Q課長：それでは，マルウェアXに対する有効な対策を考えてくれないか。

R主任：分かりました。セキュリティサービス会社のS社に相談してみます。

〔マルウェアXへの対応策〕

R主任は，現在のセキュリティ対策の内容をS社に説明し，マルウェアXに対する対応策の提案を求めた。S社から，セキュリティパッチの適用やログの検査が迅速に行われていないという問題が指摘され，マルウェアX侵入の早期発見，侵入後の活動の抑止及び被害内容の把握を目的として，EDR（Endpoint Detection and Response）システム（以下，EDRという）の導入を提案された。

S社が提案したEDRの構成と機能概要を次に示す。

・EDRは，管理サーバ，及びPCに導入するエージェントから構成される。

・管理サーバは，エージェントの設定，エージェントから受信したログの保存，分析及び分析結果の可視化などの機能をもつ。

・エージェントは，次の(i)，(ii)の処理を行うことができる。

(i)　PCで実行されたコマンド，通信内容，ファイル操作などのイベントのログを管理サーバに送信する。

(ii)　PCのプロセスを監視し，あらかじめ設定した条件に合致した動作が行われたことを検知した場合に，設定した対応策を実施する。例えば，EDRは，(a)～

(c)に示した⑤マルウェア X の活動を検知した場合に，⑥内部ネットワークの探索を防ぐなどの緊急措置を PC に対して実施することができる。

R 主任は，S 社の提案を基に，マルウェア X の侵入時の対応策をまとめ，Q 課長に EDR の導入を提案した。提案内容は承認され，EDR の導入が決定した。

設問 1　〔セキュリティ対策の現状〕について答えよ。

(1)　本文中の［ a ］～［ c ］に入れる適切な機器を，解答群の中から選び記号で答えよ。

解答群

ア　FW　　イ　L2SW　　ウ　L3SW

エ　外部 DNS サーバ　　オ　検証用サーバ　　カ　社内メールサーバ

キ　内部 DNS サーバ　　ク　配布サーバ　　ケ　メール中継サーバ

(2)　本文中の下線①の攻撃名を，解答群の中から選び記号で答えよ。

解答群

ア　DNS リフレクション攻撃　　イ　セッションハイジャック攻撃

ウ　メール不正中継攻撃

設問 2　〔マルウェア X の調査〕について答えよ。

(1)　本文中の下線②の処理によって取得できる情報を，20 字以内で答えよ。

(2)　本文中の下線③の処理を行う目的を，解答群の中から選び記号で答えよ。

解答群

ア　DoS 攻撃を行うため

イ　稼働中の OS のバージョンを知るため

ウ　攻撃対象のサービスの稼働状態を知るため

エ　ホストの稼働状態を知るため

(3)　本文中の下線④について，発見できない理由として最も適切なものを解答群の中から選び，記号で答えよ。

解答群

ア　送信者のドメインが詐称されたものでないから

イ　添付ファイルが暗号化されているので，チェックできないから

ウ　メールに付与された署名が正規のドメインで生成されたものだから

エ　メール本文に不審な箇所がないから

設問３　〔マルウェアＸへの対応策〕について答えよ。

(1)　本文中の下線⑤について，どのような事象を検知した場合に，マルウェアＸの侵入を疑うことができるのかを，25字以内で答えよ。

(2)　本文中の下線⑥について，緊急措置の内容を25字以内で答えよ。

(3)　EDR 導入後にマルウェア X の被害が発生したとき，被害内容を早期に明らかにするために実施すべきことは何か。本文中の字句を用いて 20 字以内で答えよ。

問5　DNSのセキュリティ対策に関する次の記述を読んで，設問1～3に答えよ。

R社は，Webサイト向けソフトウェアの開発を主業務とする，従業員約50名の企業である。R社の会社概要や事業内容などをR社のWebサイト（以下，R社サイトという）に掲示している。

R社内からインターネットへのアクセスは，R社が使用するデータセンタを経由して行われている。データセンタのDMZには，R社のWebサーバ，権威DNSサーバ，キャッシュDNSサーバなどが設置されている。DMZは，ファイアウォール（以下，FWという）を介して，インターネットとR社社内LANの両方に接続している。データセンタ内のR社のネットワーク構成の一部を図1に示す。

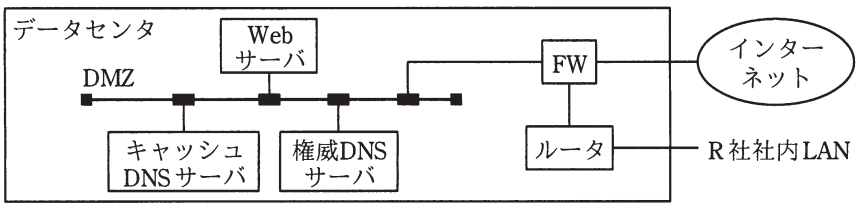


図1　データセンタ内のR社のネットワーク構成（一部）

R社サイトは，データセンタ内のWebサーバで運用され，インターネットからR社サイトへは，HTTP Over TLS（以下，HTTPSという）によるアクセスだけが許されている。

〔インシデントの発生〕

ある日，R社の顧客であるY社の担当者から，“社員のPCが，R社サイトに埋め込まれていたリンクからマルウェアに感染したと思われる”との連絡を受けた。Y社は，Y社が契約しているISPであるZ社のDNSサーバを利用していた。

R社情報システム部のS部長は，部員のTさんに，R社のネットワークのインターネット接続を一時的に切断し，マルウェア感染の状況について調査するように指示した。Tさんが調査した結果，R社の権威DNSサーバ上の，R社のWebサーバのAレコードが別のサイトのIPアドレスに改ざんされていることが分かった。R社のキャッシュDNSサーバとWebサーバには，侵入や改ざんされた形跡はなかった。

Tさんから報告を受けたS部長は，①Y社のPCがR社の偽サイトに誘導され，マルウェアに感染した可能性が高いと判断した。

〔当該インシデントの原因調査〕

S部長は，当該インシデントの原因調査のために，R社の権威DNSサーバ，キャッシュDNSサーバ及びWebサーバの脆弱性診断及びログ解析を実施するよう，Tさんに指示した。Tさんは外部のセキュリティ会社の協力を受けて，脆弱性診断とログ解析を実施した。診断結果の一部を表1に示す。

表1　R社サーバの脆弱性診断及びログ解析の結果（一部）

診断対象	脆弱性診断結果	ログ解析結果
権威DNSサーバ	・OSは最新であったが，DNSソフトウェアのバージョンが古く，［a］を奪取されるおそれがあった。 ・インターネットから権威DNSサーバへのアクセスはDNSプロトコルだけに制限されていた。	業務時間外にログインされた形跡が残っていた。
キャッシュDNSサーバ	・OS及びDNSソフトウェアは最新であった。 ・インターネットからキャッシュDNSサーバへのアクセスはDNSプロトコルだけに制限されていた。	不審なアクセスの形跡は確認されなかった。
Webサーバ	・OS及びWebサーバのソフトウェアは最新であった。 ・インターネットからWebサーバへのアクセスはHTTPSだけに制限されていた。	Y社のPCがマルウェア感染した時期に②R社サイトへのアクセスがほとんどなかった。

診断結果を確認したS部長は，R社の権威DNSサーバのDNSソフトウェアの脆弱性を悪用した攻撃によって［a］が奪取された可能性が高いと考え，早急にその脆弱性への対応を行うようにTさんに指示した。

Tさんは，R社の権威DNSサーバのDNSソフトウェアの脆弱性は，ソフトウェアベンダが提供する最新版のソフトウェアで対応可能であることを確認し，当該ソフトウェアをアップデートしたことをS部長に報告した。S部長はTさんに，R社の権威DNSサーバ上のR社のWebサーバのAレコードを正しいIPアドレスに戻し，R社のネットワークのインターネット接続を再開させたが，Y社のPCからR社サイトに正しくアクセスできるようになるまで，③しばらく時間が掛かった。R社は，Y社に謝罪するとともに，当該インシデントについて経緯などをとりまとめて，R社サイトなどを通じて，顧客を含む関係者に周知した。

〔セキュリティ対策の検討〕

S 部長は，R 社の権威 DNS サーバに対する④同様なインシデントの再発防止に有効な対策と，R 社のキャッシュ DNS サーバ及び Web サーバに対するセキュリティ対策の強化を検討するように，T さんに指示した。

T さんは，R 社の Web サーバが使用しているディジタル証明書が，ドメイン名の所有者であることが確認できる DV（Domain Validation）証明書であることが問題と考えた。そこで T さんは，EV（Extended Validation）証明書を導入することを提案した。R 社の Web サーバに EV 証明書を導入し，Web ブラウザで R 社サイトに HTTPS でアクセスすると，R 社の［ b ］を確認できる。

また T さんは，⑤R 社のキャッシュ DNS サーバがインターネットから問合せ可能であることも問題だと考えた。その対策として，FW の設定を修正して R 社社内 LAN からだけ問合せ可能とすることを提案した。また，R 社のキャッシュ DNS サーバに，偽の DNS 応答がキャッシュされ，R 社の社内 LAN 上の PC がインターネット上の偽サイトに誘導されてしまう，［ c ］の脅威があると考えた。DNS ソフトウェアの最新版を確認したところ，ソースポートのランダム化などに対応していることから，この脅威については対応済みとして報告した。

設問 1　本文中の下線①で，Y 社の PC が R 社の偽サイトに誘導された際に，Y 社の PC に偽の IP アドレスを返した可能性のある DNS サーバを，解答群の中から全て選び，記号で答えよ。

解答群

ア　DNS ルートサーバ　　イ　R 社のキャッシュ DNS サーバ

ウ　R 社の権威 DNS サーバ　　エ　Z 社の DNS サーバ

設問 2　〔当該インシデントの原因調査〕について，(1)～(3)に答えよ。

(1)　表 1 及び本文中の［ a ］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　管理者権限　　イ　シリアル番号

ウ　ディジタル証明書　　エ　利用者パスワード

(2)　表1中の下線②で，R社サイトへのアクセスがほとんどなかった理由を20字以内で述べよ。

(3)　本文中の下線③で，Y社のPCが正しいR社サイトにアクセスできるようになるまで，しばらく時間が掛かった理由は，どのDNSサーバにキャッシュが残っていたからか，解答群の中から選び，記号で答えよ。

解答群

ア　DNSルートサーバ　　イ　R社のキャッシュDNSサーバ

ウ　R社の権威DNSサーバ　　エ　Z社のDNSサーバ

設問3　〔セキュリティ対策の検討〕について，(1)～(4)に答えよ。

(1)　本文中の下線④で，同様なインシデントの再発防止に有効な対策として，R社の権威DNSサーバに実施すべきものを，解答群の中から選び，記号で答えよ。

解答群

ア　逆引きDNSレコードを設定する。

イ　シリアル番号の桁数を増やす。

ウ　ゾーン転送を禁止する。

エ　定期的に脆弱性検査と対策を実施する。

(2)　本文中の［　b　］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　会社名　　イ　担当者の電子メールアドレス

ウ　担当者の電話番号　　エ　ディジタル証明書の所有者

(3)　本文中の下線⑤で，R社のキャッシュDNSサーバがインターネットから問合せ可能な状態であることによって発生する可能性のあるサイバー攻撃を，解答群の中から選び，記号で答えよ。

解答群

ア　DDoS攻撃　　イ　SQLインジェクション攻撃

ウ　パスワードリスト攻撃　　エ　水飲み場攻撃

(4)　本文中の［　c　］に入れるサイバー攻撃手法の名称を，15字以内で答えよ。

第５章　情報セキュリティ　解答・解説

問4

解答

設問		解答例	備考
設問1	(1)	a　ア　b　ケ　c　ク	
	(2)	ア	
設問2	(1)	稼働中のホストのIPアドレス	
	(2)	ウ	
	(3)	ア	
設問3	(1)	ICMPエコー要求パケットの連続した送信	
	(2)	マルウェアに感染したPCを隔離する。	
	(3)	EDRが保存するログの分析	

解説

設問1

(1)

aについて

空欄aの後では，「インターネットとDMZ間及び内部LANとDMZ間で業務に必要な通信だけを許可し，通信ログ及び遮断ログを取得する」と述べられている。図1を見ると，インターネットとDMZ間，内部LANとDMZ間で通信を行うためには，必ずFW（ファイアウォール）を通ることが分かる。したがって，インターネットとDMZ間及び内部LANとDMZ間の通信の許可や遮断が行える装置は，

FW　（ア）

である。

bについて

SPF（Sender Policy Framework）は，送信元ドメイン認証の一つである。送信元ドメイン認証では外部からメールが送られてきた際に，送信元のメールサーバと送信元のドメインが一致することを確認することにより，不正なメールの受信を防止する。

空欄aでも述べたように，FWはインターネットとDMZ間及び内部LANとDMZ間の通信のみを許可しているので，インターネットからのメールを社内メールサーバが直接受信することはない。つまり，外部からP社に送られてきたメールは，メール中継サーバで受信することになる。よって，SPF機能によって送信元ドメイン認証を行っているのは，

メール中継サーバ　（ケ）

である。

cについて

空欄cの前にある文章から，ここではOSのセキュリティパッチやアップデート版をPC向けに配布する場合の作業について考えればよい。二つ目の空欄cの前後に注目すると，PCは空欄cの機器から新しい版をダウンロードし，更新することがわかる。図1の注記1では，「配布サーバは，PCにセキュリティパッチなどを配布するサーバである」と説明されているので，空欄cには，

配布サーバ （ク）

を入れればよい。

(2)

下線①の前で「キャッシュサーバの機能を稼働させており」と述べられていることから，インターネット上のキャッシュサーバを利用してDDoS攻撃を行う攻撃を考えればよい。解答群のうち，これに該当する手法は，

DNSリフレクション攻撃 （ア）

のみである。

DNSリフレクション攻撃は，送信元IPアドレスを攻撃対象に偽装したDNS問合せパケットをインターネット上のキャッシュサーバに対して送信し，DNS応答パケットを攻撃対象に返送させる攻撃である。マルウェア(ボット)などを利用して一斉に問合せを行うことにより，大量のDNS応答パケットを攻撃対象に送り付けることが可能となる。この結果，攻撃対象となるサーバは過負荷状態となり，通常のサービスを提供できなくなる。

この攻撃はキャッシュサーバが攻撃パケットを反射しているように見えることから，DNSリフレクション攻撃，あるいはDNSリフレクタ攻撃という。また，DNS応答パケットはDNS問合せパケットよりもサイズが大きく，パケットサイズを増幅できることからDNSアンプ攻撃ともいう。

セッションハイジャック攻撃：主にWebアプリケーションにおいて，窃取・推測したセッション識別子を利用して他人になりすましてアクセスし，サービスを不正利用する攻撃

メール不正中継攻撃：オープンリレー状態（社外からの社外に宛てたメールを中継するように設定された状態）のメールサーバを踏み台として利用し，スパムメールやウイルスメールなどを中継させる攻撃

設問2

(1)

ICMP(Internet Control Message Protocol)は，IPネットワークで制御メッセージを伝送するためのプロトコルである。ICMPでは用途に応じたメッセージが用いられ，その一つであるICMPエコーはネットワークにおける到達性を確認するために用いられる。具体的には，ICMPエコー要求を受け取った機器は原則として送信元にICMPエコー応答を返すため，宛先からICMPエコー応答が返ってくれば宛先までパケットは届き，機器も稼働していることが確認できる。逆にICMPエコー応答が返ってこない場合は，通信経路やネットワーク設定に問題があるか，又は機器が稼働していないことが確認できる。

下線②のように，宛先アドレスを変えながらICMPエコー要求パケットを送信すると，どのホストからICMPエコー応答が返ってくるかを調べることで，どのIPアドレスが稼働中であるか（通信可能であるか）を把握することができる。ここでは「取得できる情報」が問われているので，

稼働中のホストのIPアドレス

のように解答すればよい。

(2)

TCPのSYNパケットとは接続要求を意味し，TCPコネクションを確立する際に用いられる。TCPでは，次のような手順で通信に先立って論理的な通信路であるコネクションを確立する。これを，3ウェイハンドシェイクという。なお，TCP/IPにおけるプロトコルの多くはクライアントサーバ型であり，通常はクライアントがサーバに対して接続を要求する。

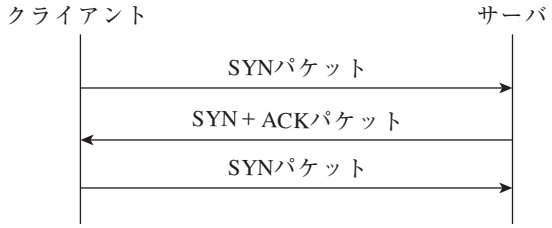


図2　3ウェイハンドシェイク

この図を見てもわかるように，サーバはクライアントのSYNパケットに対して応答し，SYN＋ACKパケットを返す。よって，SYN＋ACKパケットが返ってくれば接続を要求したサービスが稼働していることがわかり，SYN＋ACKパケットが返ってこなければ接続を要求したサービスは稼働していないことがわかる。

下線③のように，「攻撃対象のポート番号をセットしたTCPのSYNパケットを送信し，応答内容を確認する」のは，当該ポート番号での

攻撃対象のサービスの稼働状態を知るため　（ウ）

である。

(3)

SPFでは，インターネット上のメールサーバからメールを受信したメールサーバが，送信元メールサーバのドメインを管理するDNSサーバに問合せを行い，SPFの情報が記載されたtxtレコードを取得する。このtxtレコードには，そのドメインからメールを送信する可能性のあるメールサーバ（IPアドレスなど）の一覧が記載されているので，送信元メールサーバが一覧に記載されていれば正当なメールサーバと判断でき，記載されていなければメールサーバがなりすまされていると判断できる。

下線④では「マルウェアXに感染した社外のPCから送られてきたメール」と述べられているので，マルウェアXの挙動について確認すると，〔マルウェアXの調査〕(3)(d)でマルウェアXは過去にやり取りしたメールに返信する形で感染拡大を試みる旨が述べられている。過去のメールに返信するということは，メールソフトなどに設定された正規のメールサーバを

利用しているはずである。この場合，送信元をなりすましたことにはならないので，SPFでなりすましを発見することができない。よって，

送信者のドメインが詐称されたものでないから　　（ア）

を解答すればよい。

設問3

(1)

下線⑤の直前で「(a)～(c)に示した」マルウェアXの活動を検知と述べられていることから，まずは〔マルウェアXの調査〕(3)(a)～(c)に注目する。すると，PCがマルウェアXに感染すると，最初に「PCが接続するセグメント及び社内の他のセグメントの全てのホストアドレス宛てに，宛先アドレスを変えながらICMPエコー要求パケットを送信」することがわかる。通常の通信では，全てのホストアドレス宛てにICMPエコー要求を送信する必要はないので，このような活動が検知されればマルウェアXに感染していると判断できる。これを制限字数内にまとめ，

ICMPエコー要求パケットの連続した送信

のように解答すればよい。

(2)

下線⑥では「内部ネットワークの探索を防ぐ」と述べられている点に注目する。マルウェアXは，内部ネットワークの探索を，〔マルウェアXの調査〕(3)(a)，(b)によって行う。よって，マルウェアXが内部ネットワークを探索することを防ぐためには，PCが通信を行えないようにネットワークから隔離すればよい。以上より，

マルウェアに感染したPCを隔離する。

のように解答すればよい。

(3)

設問文では，「EDR導入後に」「被害内容を早期に明らかにするために実施すべきこと」が問われている。被害内容を明らかにするためには，何が行われたかを事後に確認できる情報が必要である。これを踏まえてEDRの機能を確認すると，〔マルウェアXへの対応策〕において，EDRは管理サーバとPCに導入するエージェントから構成されており，管理サーバは，エージェントの設定，エージェントから受信したログの保存，分析及び分析結果の可視化などの機能をもつことが述べられている。何が行われていたかを確認するためには，このログを活用すればよい。管理サーバはログの分析や分析結果の可視化といった機能をもっているので，

EDRが保存するログの分析

を行えばよい。

問5

解答

設問		解答例	備考
設問1		ウ，エ	
設問2	(1)	a　ア	
	(2)	顧客がR社の偽サイトに誘導されたから	
	(3)	エ	
設問3	(1)	エ	
	(2)	b　ア	
	(3)	ア	
	(4)	c　DNSキャッシュポイズニング	

解説

設問1

Y社のPCに偽のIPアドレスを返した可能性のあるDNSサーバが問われているので，まずはY社のPCが利用しているDNSサーバが何かを把握する。本文中に「Y社は，Y社が契約しているISPであるZ社のDNSサーバを利用していた」と述べられていることから，Y社はISPであるZ社のDNSサーバをDNSキャシュサーバとして利用していると推測できる。この場合，DNSの問合せは次のように行われる。

①Y社のPCは，Z社のDNSサーバへ，R社WebサーバのIPアドレスを問い合わせる。
②Z社のDNSサーバは，ルートDNSサーバから順に下位のDNSサーバに名前解決を繰り返す反復問合せを行い，最終的にR社の権威DNSサーバから，R社WebサーバのIPアドレスを得る。
③Z社のDNSサーバは，R社WebサーバのIPアドレスをY社のPCへ返答する。

ここで，〔インシデントの発生〕において，「R社の権威DNSサーバ上の，R社のWebサーバのAレコードが別のサイトのIPアドレスに改ざんされていることがわかった」と述べられている点に注目する。Aレコードは，ドメイン名に対応するIPアドレスを管理するためのレコードである。このAレコードが改ざんされると，R社のWebサーバのドメイン名を正しく指定しても，そのIPアドレスとして改ざんされた「別のサイトのIPアドレス」が返されてしまうことになる。よって，次のように，名前解決が行われたと推測できる。

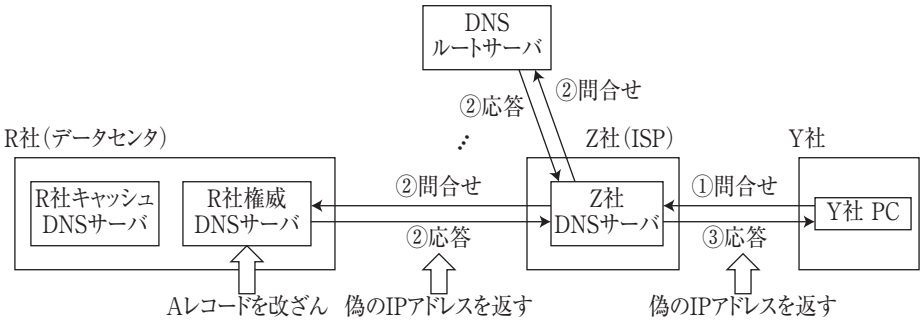


図2　名前解決の順序

以上の動作を考慮すると，Y社のPCに偽のIPアドレスを返した可能性のあるDNSサーバとして，

R社の権威DNSサーバ（ウ）とZ社のDNSサーバ（エ）

が考えられる。

設問2

(1)

表1を見ると，空欄aの前で「OSは最新であったが，DNSソフトウェアのバージョンが古く」と述べられており，本文中の空欄aの前では「R社の権威DNSサーバの脆弱性を悪用した攻撃によって」と述べられている点に注目する。

このようにソフトウェアのバージョンが古い場合，バッファオーバフロー攻撃などに代表される既知のセキュリティホール（脆弱性）を悪用した攻撃によって，攻撃者が送り込んだ任意のプログラム（一般的には攻撃用の不正プログラム）を実行させられる可能性が高くなる。攻撃対象のソフトウェアが管理者権限で動作していた場合には，管理者権限で動作するシェルを起動されるなどして，管理者権限を奪取されることにつながる。よって，DNSソフトウェアのバーションが古いことで奪取される可能性があるのは，

管理者権限（ア）

である。

(2)

下線②の前では「Y社のPCがマルウェアに感染した時期に」と述べられていることから，Y社のPCがマルウェアに感染した経緯を確認する。すると，本文中の下線①では「Y社のPCがR社の偽サイトに誘導され，マルウェアに感染した」と述べられており，その前では，R社の権威DNSサーバ上の，R社のWebサーバのAレコードが別のサイトのIPアドレスに改ざんされている旨が述べられている。DNSのレコードが改ざんされたということは，この時期にはR社サイトへのアクセスのほとんどがR社の偽サイトに誘導されているはずである。よって，下線②の理由としては，

顧客がR社の偽サイトに誘導されたから

顧客がR社の偽サイトにアクセスしたから

などを答えればよい。

(3)

DNSのキャッシュとは，キャッシュサーバが名前解決で行った問合せの結果を保存する仕組み，または保存された問合せ結果のことである。設問1の解説で述べたように，キャッシュサーバはクライアントからの依頼を受けると，権威DNSサーバに名前解決の問合せを行う。この問合せ結果は，クライアントに返送されるとともに，キャッシュとしてキャッシュサーバに保存される。キャッシュサーバはキャッシュに残る名前解決の依頼を受けると，権威DNSサーバに問合せを行なうことなくキャッシュに保存された問合せ結果を返送する。これにより，DNSサーバの負荷軽減や問合せの高速化を実現できる。キャッシュには，破棄されずにキャッシュに残る期間（TTL：Time To Live）が設定されており，この期間を超えるまで，キャッシュの内容は破棄されずに同じIPアドレスが返されることになる。

本問の場合は，Y社のPCがキャッシュサーバとして利用するのは，

Z社のDNSサーバ（エ）

である。Z社のDNSサーバがR社の権威DNSサーバに問合せを行った際，改ざんされたAレコードが返されると，Z社のDNSサーバはそれをキャッシュとして保存してしまう。そして，R社の権威DNSサーバ上のAレコードを元に戻したとしても，Z社のDNSサーバがキャッシュを破棄するまでのしばらくの間は，Y社のPCには改ざんされたIPアドレスが返送されてしまい，Y社のPCから正しいR社サイトにアクセスすることができなくなる。

設問3

(1)

今回のインシデントは，DNSソフトウェアのバージョンが古いことで，既知の脆弱性を突いた攻撃を受け，管理者権限を奪取されたことが原因となっている。ここから，DNSソフトウェアの脆弱性情報を収集する，OSやアプリケーションを最新のバージョンに更新する，といったセキュリティ関連の管理が日常的に行われていなかったと推測できる。

サーバソフトウェアに限らず，あらゆるソフトウェア（OS，ライブラリなども含む）は，既知の脆弱性を付く攻撃を受けないよう，日頃から脆弱性情報を収集して最新のバージョンに更新することが重要である。よって，再発防止策としては，

定期的に脆弱性検査と対策を実施する（エ）

ことが求められる。

ア　IPアドレスに対応するドメイン名を得ることを，逆引きという。逆引きのレコードを設定することと，脆弱性を悪用した攻撃とは関連がない。

イ　DNSにおけるシリアル番号とは，DNSサーバに設定するDNS情報（ゾーン情報）のバージョンを識別するために設定される番号である。通常，ゾーン情報を更新するとシリアル番号は以前よりも大きくなるよう更新され，最も大きなシリアル番号をもつゾーン情報を最新とみなす。シリアル番号と，脆弱性を悪用した攻撃とは関連がない。

ウ　ゾーン転送とは，複数のDNSサーバ間でゾーン情報を同期させる仕組みであり，ゾーン情報の配布元をマスタサーバ，ゾーン情報の配布先をスレーブサーバという。ゾーン転送と，脆弱性を悪用した攻撃とは関連がない。

(2)

ここでは，「EV証明書」を導入した際に確認できる事項が問われているが，その前に「DV証明書」と述べられているように，ディジタル証明書にはいくつかの種類がある。ディジタル証明書の種類を，次に示す。

表2　ディジタル証明書の種類

種類	説明
ドメイン認証（DV）証明書	ドメインの所有を証明する証明書である。証明書には，サーバのFQDNだけが記載されている。
組織認証（OV）証明書	ドメインの所有のほかに，組織の実在性も証明する証明書である。証明書には，サーバのFQDNのほかに，組織名（個人，法人），組織の所在地（国名，都道府県名）などが記載されている。
EV証明書	組織（法人）の活動実態まで含めて，OV型よりもさらに厳しく審査した証明書である。ブラウザによっては，アドレスバーに組織名が表示されたり，アドレスバーが緑色になったりする。

EV証明書を導入し，WebブラウザでR社サイトにHTTPSでアクセスすると，Webブラウザのアドレスバーに，R社の

会社名（ア）

が表示され，ユーザは正しいサイトにアクセスしたことを手間をかけずに確認できる。

(3)

下線⑤で「R社のキャッシュDNSサーバがインターネットから問合せ可能である」と述べられていることを考慮すると，下線⑤によって発生し得るサイバー攻撃は，キャッシュDNSサーバそのものに対する攻撃ではなく，インターネットからDNSの問合せの仕組みを悪用する攻撃のはずである。このような攻撃手法として，

① 他のサーバに過負荷を与えてサービスの提供を妨害するDoS攻撃(DDoS攻撃)

② 偽のDNS応答をキャッシュさせ，偽サイトに誘導するDNSキャッシュポイズニング攻撃

の2種類が考えられる。このうち，選択肢にあるのは，

DDoS攻撃（ア）

のみである。

DoS攻撃とは，大量のパケットや処理要求を送りつけてサーバやネットワーク回線を過負荷状態に陥れるなどの方法で，サービス提供を妨害する攻撃である。マルウェアなどを利用して多数の踏み台から同時にDoS攻撃を仕掛ける攻撃は，DDoS(Distributed DoS)攻撃ともいう。DNSの仕組みを利用したDoS攻撃(DDoS攻撃)には，DNS水責め攻撃(ランダムサブドメイン攻撃)やDNS amp攻撃(DNSリフレクタ攻撃)などがある。

・DNS水責め攻撃(ランダムサブドメイン攻撃)：オープンリゾルバ（組織外部から利用できるキャッシュDNSサーバ）に対して集中的にDNSの問合せを行うことにより，権威DNSサーバやキャッシュDNSサーバのサービス提供を妨害する攻撃。攻撃対象のドメイン名に対して，ランダムなサブドメイン名を付加することにより，DNSのキャッシュを無効化することができる。

・DNSamp攻撃（DNSリフレクタ攻撃）：送信元IPアドレスを標的ホストのIPアドレスに偽装したDNS問合せをキャッシュDNSサーバ又は権威DNSサーバに対して送信し，DNS応答を標的ホストに集中させることで，標的ホストのサービス提供を妨害する攻撃。DNS問合せに比べてDNS応答はサイズが大きいため，攻撃の効率を高くすることができる。

・SQLインジェクション攻撃：不正なSQL文の一部を混入させた入力データをWebアプリケーションに送りつけ，Webアプリケーションに不正なSQL文を実行させる攻撃。データベースサーバと連携して動作するWebアプリケーションを狙う攻撃の一種であり，データベースサーバの不正な操作などを行う。

・パスワードリスト攻撃：他のサイトから流出したユーザID，パスワードをそのまま利用してログインを試みる攻撃。

・水飲み場攻撃：標的企業の社員がよく利用するサイトを改ざんしたり，標的企業の社員が興味を持つ話題を扱う不正サイトを用意したりして，マルウェアを仕掛けたサイトに標的をおびき寄せ，マルウェアに感染させる攻撃。

(4)

設問3(3)の解説でも述べたように，キャッシュDNSサーバに偽のDNS応答をキャッシュさせ，クライアントを偽サイトに誘導する攻撃を，

DNSキャッシュポイズニング

という。

なお，DNSキャッシュポイズニング攻撃はキャッシュDNSサーバを対象とした攻撃であり，DNS権威サーバが管理するゾーン情報（Aレコード）を改ざんする必要はない。本問の〔インシデントの発生〕では，DNSキャッシュポイズニング攻撃ではなく，DNSサーバに対する侵入とゾーン情報の改ざんが行われている。