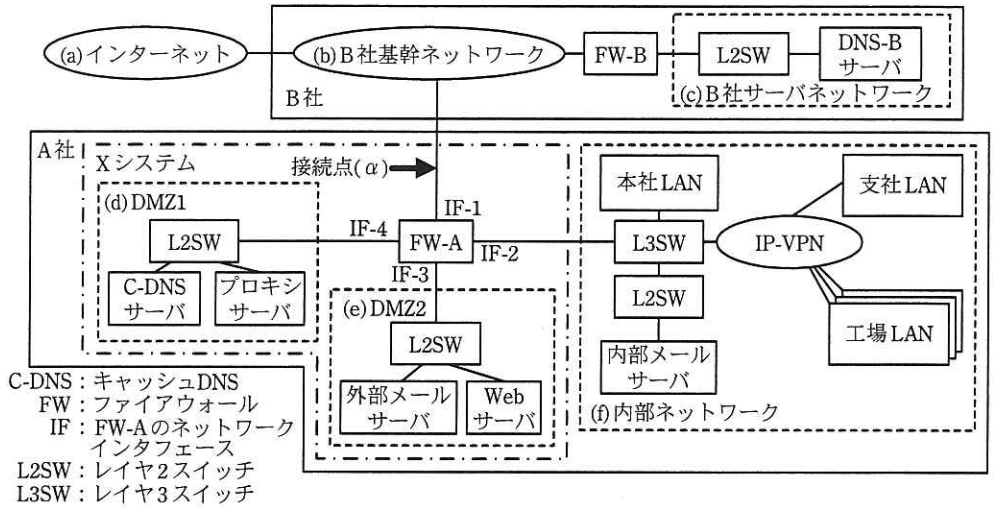
問2　IP アドレス詐称対策に関する次の記述を読んで，設問 1，2 に答えよ。

A 社は，従業員数 4,000 名の化学メーカである。東京に本社，大阪に支社，国内の 3 か所に工場がある。A 社では，電子メール（以下，メールという）の利用などのために，インターネット接続システム（以下，X システムという）を導入している。X システムは本社に設置され，B 社のインターネット接続サービス（以下，B 社サービスという）を利用している。また，本社，支社及び工場の LAN は IP-VPN で接続されている。

X システムの運用は，責任者である情報システム部の D 部長の下で，E 主任と F さんが担当している。X システムの各サーバでは，サーバへのアクセス及びプログラムの動作状況のログを記録している。

A 社のドメイン名は，B 社の DNS-B サーバで管理している。DNS-B サーバは DNS コンテンツサーバであり，リゾルバ機能（インターネット上のサーバ名の名前解決を行う機能）及び DNS キャッシュ機能（名前解決結果を一時的に保持する機能）をもたない。

現在の A 社及び B 社サービスのネットワーク構成を図 1 に，X システムの主な機器と機能を表 1 に示す。



注記 1　A 社の PC は全て本社 LAN，支社 LAN 又は工場 LAN に接続されている。
注記 2　PC の記載は省略している。

図 1　A 社及び B 社サービスのネットワーク構成

表1　Xシステムの主な機器と機能

機器名称	機能
FW-A	ステートフルパケットフィルタリング型FWであり，IPアドレス詐称対策機能及びパケットフィルタリング機能がある。IPアドレス詐称対策機能，パケットフィルタリング機能の順に処理する。また，通信の許可及び拒否のログを記録する機能がある。
C-DNSサーバ	リゾルバ機能及びDNSキャッシュ機能がある。
プロキシサーバ	プロキシ機能，Webコンテンツキャッシュ機能及びウイルススキャン機能がある。
外部メールサーバ	インターネットとの間及び内部メールサーバとの間のメール転送機能，SPF（Sender Policy Framework）検証機能並びにウイルススキャン機能がある。
Webサーバ	コンテンツ公開機能及びコンテンツ更新機能がある。

〔攻撃の検出〕

ある週の月曜日，Fさんが前週のFW-Aのログを分析したところ，C-DNSサーバを宛先とするDNSパケットが約10万件も通過を拒否されており，その全てが名前解決応答パケット（以下，応答PTという）であった。しかし，これらの拒否された応答PTに対応する名前解決問合せパケット（以下，問合せPTという）をC-DNSサーバから送信した記録は，FW-Aのログになかった。報告を受けたE主任は，次のことをFさんに説明した。

・DNSの名前解決通信は，主に［　a　］を用いる。［　a　］は，［　b　］ハンドシェイクを用いてコネクションを確立するTCPと比べて，送信元IPアドレスの詐称の検知が困難である。

・大量のDNSパケットは，応答PTの送信元IPアドレスや宛先ポート番号を細工した，キャッシュポイズニング攻撃（以下，CP攻撃という）のためのものだったと考えられる。

・CP攻撃への根本的な対策は，公開鍵暗号によるディジタル署名の仕組みを応用した［　c　］というDNSセキュリティ拡張方式を導入することだが，鍵の管理など，今までにない運用手順が必要になる。根本的な対策をするかどうか決める前に，なぜCP攻撃が発生したかを調査する必要がある。

そこで，E主任とFさんが，C-DNSサーバの設定を調べたところ，CP攻撃を成功しにくくする設定がなされていることを確認した。さらに，再帰的な名前解決の問合せPTの送信元を限定する設定が行われていることも確認した。

しかし，なおも拒否される応答 PT が多い状況が続いていることから，E 主任は，F さんに対し，図 1 中の接続点(α)にパケットモニタを接続した上で，FW-A 及び C-DNS サーバを調査するよう指示した。F さんが行った調査の結果を図 2 に示す。

(1) 送信元を詐称した問合せ PT
・C-DNS サーバは次のような問合せ PT を 10 分ごとに 1 個受信していた。
送信元が外部メールサーバであり，かつ，宛先が C-DNS サーバであり，かつ，FW-A が通過を許可した問合せ PT。内容は，国内の取引先の G 社が取得したドメイン名の TXT レコードの問合せであった。
(2) C-DNS サーバに向けた応答 PT
・(1)の問合せ PT が届いた直後の 1 秒間に，送信元が G 社の DNS サーバであり，かつ，宛先が C-DNS サーバである応答 PT が 100 個届き，FW-A が通過を拒否した。
・100 個の応答 PT の宛先ポート番号は，到着順に連番であった。
・応答内容は G 社のドメイン名の TXT レコードであった。
・TXT レコードには，SPF レコードが設定されていた。SPF レコードに設定されていた IP アドレスは，G 社に割り当てられたものではなかった。
・C-DNS サーバが(1)の問合せ PT の名前解決を行うための問合せ PT は，インターネット上の DNS サーバに送信されてはいなかった。
(3) C-DNS サーバのキャッシュ
・C-DNS サーバのキャッシュには，G 社のドメイン名の TXT レコードが保存されていた。
・TXT レコードには，SPF レコードが設定されており，G 社に割り当てられた IP アドレスのうち，G 社がメールを送信するサーバの IP アドレスが設定されていた。

図 2　F さんが行った調査の結果

この結果から，E 主任は，図 2 の(2)は G 社のドメイン名の TXT レコードに対する CP 攻撃であると判断した。

そこで，E 主任と F さんは，FW-A の設定を更に調べることにした。まず，送信元，宛先及びサービスの組合せによってパケットの許可又は拒否の動作を指定するフィルタリングルールを確認し，誤りがないことを確認した。

続いて，表 2 に示す IP アドレス詐称対策ルールを確認したところ，①表 2 の項番 1 の送信元に誤りがあることに気が付き，直ちに設定を修正した。

表2　IPアドレス詐称対策ルール

項番	FW-A の IF	送信元	動作
1	IF-1	DMZ1，内部ネットワーク	拒否
2	IF-1	全て	許可
3	IF-2	内部ネットワーク	許可
4	IF-2	全て	拒否
5	IF-3	DMZ2	許可
6	IF-3	全て	拒否
7	IF-4	DMZ1	許可
8	IF-4	全て	拒否

注記1　パケットが受信された“FW-A の IF”，及びパケットの“送信元”の組合せで，パケットの通過を許可するか又は拒否するかの“動作”を指定する。
注記2　項番が小さいものから順に，最初に一致したルールが適用される。

E 主任は，図 2 の(2)の攻撃は偶然に成功する可能性があることを F さんに説明した。E 主任は，②図 2 の(2)の攻撃に続いて行われる可能性が高い，TXT レコードを利用する機能への攻撃が発生していると考えた。そこで，X システムの各サーバのログを，過去 1 か月分にわたって調査するよう F さんに指示した。調査の結果，攻撃はあったものの，各サーバの設定が正しく行われていたので失敗に終わっていたことが確認された。

〔支社システムの検討と導入〕

A 社では，インターネット及び IP-VPN のトラフィックの増加に対処するために，支社に新たなインターネット接続システム（以下，支社システムという）の導入を計画していた。E 主任と F さんは，支社システムとして，支社に新たな FW を導入し，インターネット，新たな DMZ 及び支社 LAN を接続することにした。新たな DMZ には X システムのプロキシサーバと同じ機能の支社プロキシサーバを導入し，インターネットとの接続には，B 社サービスを利用することにした。

続いて，支社プロキシサーバでの名前解決に C-DNS サーバを利用し，支社プロキシサーバと C-DNS サーバとの間の通信を B 社サービス経由にする前提で，FW-A と C-DNS サーバの設定の見直しを検討した。検討の結果，送信元が支社プロキシサーバに詐称された問合せ PT を拒否する設定は不可能であり，FW-A の IP アドレス詐称対策機能が有効に機能しないことが分かった。そこで再検討した結果，③支社システムに

機能を追加することで対応することにした。この対応策によって，支社プロキシサーバと C-DNS サーバ間の通信が不要になることも確認した。支社システムへの［ c ］の導入は，X システムも併せて支社システムの完成後に検討することとし，今回は見送ることとした。

E 主任と F さんは，検討結果を支社システム導入計画としてまとめ，D 部長に報告した。D 部長は，支社システム導入計画を経営陣に説明し，了承を得た。E 主任と F さんは，支社システム導入計画の遂行に着手した。

設問 1　〔攻撃の検出〕について，(1)～(5)に答えよ。

(1) 本文中の［ a ］～［ c ］に入れる適切な字句を，［ a ］については英字 5 字以内，［ b ］については 6 字以内，［ c ］については英字 8 字以内で答えよ。

(2) E 主任と F さんが確認した，C-DNS サーバにおいて CP 攻撃を成功しにくくする対策とは何か。“ポート番号”という字句を用いて，対策の内容を 30 字以内で述べよ。

(3) C-DNS サーバにおいて，図 2 中の(1)の問合せ PT を拒否しない設定にしている理由を，40 字以内で述べよ。

(4) 本文中の下線①について，表 2 の項番 1 の送信元として設定すべき全てのネットワークを，図 1 中の(a)～(f)から選び，記号で答えよ。

(5) 本文中の下線②の攻撃の内容を，40 字以内で述べよ。

設問 2　〔支社システムの検討と導入〕について，(1)，(2)に答えよ。

(1) 送信元を支社プロキシサーバに詐称した問合せ PT に対し，FW-A の IP アドレス詐称対策機能が有効に機能しない理由を，60 字以内で述べよ。

(2) 本文中の下線③について，支社システムに追加する機能を，20 字以内で述べよ。