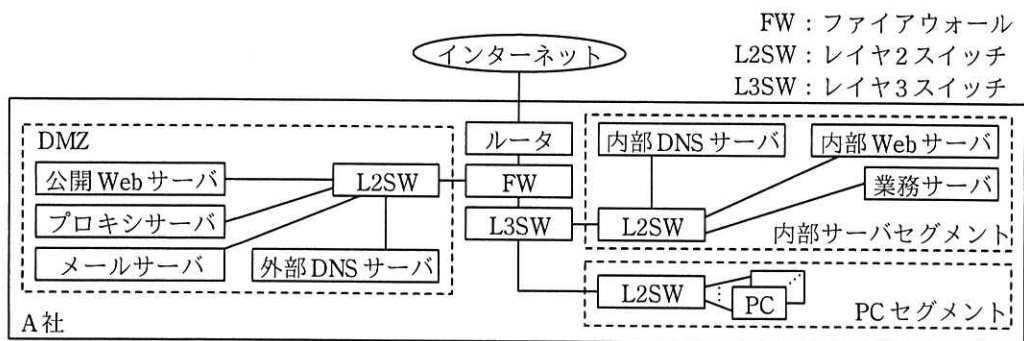


問2 ネットワークのセキュリティ対策に関する次の記述を読んで、設問 1, 2 に答えよ。

A 社は、従業員 500 名の中規模の小売業であり、インターネットを介して消費者向けに商品を宣伝している。A 社のネットワークは、同社の情報システム部（以下、情シ部という）の L 部長と M 主任を含む 7 名で運用している。A 社のネットワーク構成を図 1 に、図 1 中の主な機器とその概要を表 1 に示す。



注記 DMZ の機器にはグローバル IP アドレスを割り当てている。

図 1 A 社のネットワーク構成

表 1 図 1 中の主な機器とその概要

機器	概要
公開 Web サーバ	消費者向けの商品の宣伝に使用されている。
プロキシサーバ	PC から公開 Web サーバ及びインターネット上の Web サーバへの HTTP 及び HTTPS 通信を中継している。
メールサーバ	社内外との電子メールの送受信に使用されている。
外部 DNS サーバ ¹⁾	A 社ドメインの権威 DNS サーバ及び再帰的な名前解決を行うフルサービスリゾルバ ²⁾ として使用されている。
内部 DNS サーバ ¹⁾	内部サーバセグメントのゾーン情報の管理に使用されている。
PC	A 社の従業員が使用している。Web ブラウザには、公開 Web サーバ及びインターネット上の Web サーバにアクセスできるように、プロキシの設定が適切にされている。

注記 1 A 社では、インターネットドメイン名 a-sha.co.jp を取得しており、レジストラとして X 社を利用している。

注記 2 公開 Web サーバ及びインターネット上の Web サーバの名前解決は、プロキシサーバが外部 DNS サーバに問い合わせる設定になっている。

注¹⁾ DNS サーバ用の OSS である D ソフトを使用している。

²⁾ フルサービスリゾルバとしては、プロキシサーバとメールサーバが使用している。

FW のフィルタリングルールを表 2 に示す。

表 2 FW のフィルタリングルール

項番	送信元	宛先	サービス	動作
1	プロキシサーバ	インターネット	HTTP, HTTPS	許可
2	インターネット	公開 Web サーバ	HTTP, HTTPS	許可
3	メールサーバ	インターネット	SMTP	許可
4	インターネット	メールサーバ	SMTP	許可
5	外部 DNS サーバ	インターネット	DNS	許可
6	インターネット	外部 DNS サーバ	DNS	許可
7	PC セグメント	プロキシサーバ	HTTP, HTTPS	許可
8	PC セグメント	メールサーバ	SMTP, POP3	許可
⋮	⋮	⋮	⋮	⋮
14	全て	全て	全て	拒否

注記 1 FW は、ステートフルパケットインスペクション型である。

注記 2 項番が小さいルールから順に、最初に一致したルールが適用される。

注記 3 項番 9～13 には、DNS に関するルールは記述されていない。

ある日、D ソフトの脆弱性^{ぜい}を悪用した DoS 攻撃で同業他社が踏み台になったというニュースが配信された。情シ部では、脆弱性情報が公開されると、CVSS の値を参考にして自社への影響を評価し、影響が大きいケースでは、早期に脆弱性修正プログラムを適用している。今回の攻撃に使われた D ソフトの脆弱性に対する修正プログラムは既に適用されていた。A 社では、今回のニュースを契機に、DNS におけるリスクと対策の検討を、M 主任を中心に行うことにした。

〔リスクと対策の検討〕

M 主任は、まず、①A 社の外部 DNS サーバがサービス停止になった場合の影響を確認した。次に、外部 DNS サーバが攻撃を受けるリスク及び外部 DNS サーバにおけるその他のリスクを調査し、外部 DNS サーバが攻撃を受けるリスクについて、主なものを三つ挙げた。

一つ目のリスクは、踏み台になるリスクである。表 1 及び表 2 の構成では、攻撃者は、②送信元の IP アドレスを偽装した名前解決要求を外部 DNS サーバに送ることによって、外部 DNS サーバを踏み台とし、攻撃対象となる第三者のサーバに対し大量の DNS パケットを送り付けるという DoS 攻撃を行える。そこで、外部 DNS サーバを廃止した上で、DNS-K と DNS-F という DNS サーバを DMZ 上に新設し、権威 DNS サーバの機能を DNS-K に、フルサービスリゾルバの機能を DNS-F に移行することを

考えた。これと併せて、FW のフィルタリングルールを表 3 のように変更することで一つ目のリスクへの対策となる。

表 3 変更後の FW のフィルタリングルール

項番	送信元	宛先	サービス	動作
5	a	インターネット	DNS	許可
6	インターネット	b	DNS	許可

注記 項番 5, 6 以外は、表 2 と同一である。

二つ目のリスクは、DNS キャッシュポイズニング攻撃によるリソースレコードの改ざんのリスクである。DNS キャッシュポイズニング攻撃が成功すると、攻撃対象のフルサービスリゾルバが管理するリソースレコードのうち、メールサーバの c レコードの IP アドレスが、例えば攻撃者のメールサーバのものに書き換えられてしまい、電子メールが攻撃者のサーバに送信されてしまう。この攻撃への対策として、M 主任は、三つの対策を考えた。一つ目の対策は、一つ目のリスクへの対策を流用することである。二つ目の対策は、送信元ポート番号を d する対策である。D ソフトでも可能である。三つ目の対策は、e という技術の利用である。この技術は、DNS サーバから受け取るリソースレコードに付与されたデジタル署名を利用して、リソースレコードの送信者の正当性とデータの完全性を検証するものである。ただし、この技術は、運用として、鍵の管理など新たな作業が必要になる。

三つ目のリスクは、中間者攻撃による DNS 通信内容の盗聴、改ざんのリスクである。この対策の一つとして、DNS 通信を暗号化する DNS over TLS（以下、DoT という）という技術が標準化されている。DoT は、f と g 間の通信を暗号化するために開発されたものである。

これらの調査と検討を踏まえ、M 主任は、外部 DNS サーバが攻撃を受けるリスク、外部 DNS サーバの機能を 2 台の DNS サーバに移行する対策案、及び送信元ポート番号を d する対策案を L 部長に報告した。

[ホスティングサービス上に新設する DNS サーバの利用]

M 主任は、外部 DNS サーバにおけるその他のリスクへの対策として、外部のホスティングサービス上に DNS サーバを新設して利用することを検討した。

M 主任は、DNS サーバの構成について、二つの案を考えた。

一つ目の案は、外部 DNS サーバを廃止した上で、DNS-K と DNS-F という DNS サーバを DMZ 上に、DNS-S という DNS サーバを X 社のホスティングサービス上に新設し、③プライマリの権威 DNS サーバの機能を DNS-K に、セカンダリの権威 DNS サーバの機能を DNS-S に移行し、フルサービスリゾルバの機能を DNS-F に移行するものである。M 主任は、DNS-K と DNS-S のゾーン情報を同期するために、DNS-K でのゾーン転送の内容を示す設定ファイル、正引きゾーンファイル、逆引きゾーンファイルを設定することにした。M 主任が設定することにした DNS-K の正引きゾーンファイルを図 2 に示す。

なお、X 社のホスティングサービスに用いるドメイン名は x-sha.co.jp、DNS-S のホスト名は dns-s である。

@	IN	SOA	dns-k.a-sha.co.jp.	admin.dns-k.a-sha.co.jp.	(
(省略))
	IN	NS	dns-k.a-sha.co.jp.		
	IN	NS	h		
	IN	MX	10	i	
dns-k	IN	A	x1.y1.z1.t1		
www	IN	A	x1.y1.z1.t2		
mail	IN	A	x1.y1.z1.t3		

図 2 DNS-K の正引きゾーンファイル（抜粋）

DNS-K のホスト名は dns-k、公開 Web サーバのホスト名は www、メールサーバのホスト名は mail であり、各サーバの IP アドレスは x1.y1.z1.t1～x1.y1.z1.t3 である。

ゾーン転送では、ゾーン情報が流出するリスクがある。M 主任は、この対策として、DNS-K と DNS-S について、ゾーン転送要求に対する許可を必要最小限にするために、表 4 の設定にすることにした。

表 4 ゾーン転送要求に対する許可を必要最小限にするための設定

ゾーン転送要求元	ゾーン転送要求先	
	DNS-K	DNS-S
DNS-K		j
DNS-S	k	
上記以外の IP アドレス	l	m

二つ目の案は、外部 DNS サーバを廃止した上で、DNS-HK、DNS-S、DNS-HF という DNS サーバを X 社のホスティングサービス上に新設し、プライマリの権威 DNS サーバの機能を DNS-HK に、セカンダリの権威 DNS サーバの機能を DNS-S に、フルサービスリゾルバの機能を DNS-HF に移行するものである。DNS-K と DNS-F の DMZ への設置は実施しない。この案の場合、FW のフィルタリングルールを表 5 のように変更する必要がある。

表 5 二つ目の案の場合の FW のフィルタリングルール

項番	送信元	宛先	サービス	動作
5	n	o	DNS	許可
6	p	o	DNS	許可

注記 項番 5, 6 以外は、表 2 と同一である。

その後、A 社では、更に検討を進め、外部 DNS サーバを X 社のホスティングサービスに移行することにした。

設問 1 【リスクと対策の検討】について、(1)～(7)に答えよ。

- (1) 本文中の下線①について、A 社の公開 Web サーバへの影響を、30 字以内で述べよ。
- (2) 本文中の下線②の攻撃の名称を 20 字以内で答えよ。
- (3) 表 3 中の a , 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 DNS-F | イ DNS-K | ウ PC |
| エ 内部 DNS サーバ | オ プロキシサーバ | カ メールサーバ |

- (4) 本文中の に入れる DNS のリソースレコードのタイプ名を 6 字以内で答えよ。
- (5) 本文中の に入れる適切な字句を 15 字以内で答えよ。
- (6) 本文中の に入れる技術の名称を英字 10 字以内で答えよ。
- (7) 本文中の , 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 DNS Changer | イ RADIUS クライアント |
| ウ RADIUS サーバ | エ 権威 DNS サーバ |
| オ スタブリゾルバ | カ フルサービスリゾルバ |

設問 2 「ホスティングサービス上に新設する DNS サーバの利用」について、(1)～(4)に答えよ。

- (1) 本文中の下線③を実施することによって低減できるリスクを 30 字以内で具体的に述べよ。
- (2) 図 2 中の , 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 dns-k. | イ dns-k.a-sha.co.jp. | ウ dns-k.x-sha.co.jp. |
| エ dns-s. | オ dns-s.a-sha.co.jp. | カ dns-s.x-sha.co.jp. |
| キ mail. | ク mail.a-sha.co.jp. | ケ mail.x-sha.co.jp. |

- (3) 表 4 中の ～ に入れる適切な内容を、“許可”又は“拒否”のいずれかで答えよ。
- (4) 表 5 中の ～ 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 DNS-HF | イ DNS-S | ウ PC |
| エ 公開 Web サーバ | オ プロキシサーバ | カ メールサーバ |