問1　パケットログ解析に関する次の記述を読んで，設問1～3に答えよ。

A社は，従業員数500名の小売業者である。A社では，ネットワークの構築，運用を自社で行っている。ある朝，社内LANからインターネット上のWebページを閲覧しているときの応答が遅いといった苦情が寄せられ，システム管理部門のJ主任と運用担当のK君が調査を行うことになった。

〔原因調査と対処〕

J主任とK君は，Webページの閲覧状況の確認から始めることにした。

K君　：ブラウザでインターネット上のWebページを閲覧しようとすると，図1に示す状態が長く続き，表示までに時間が掛かります。

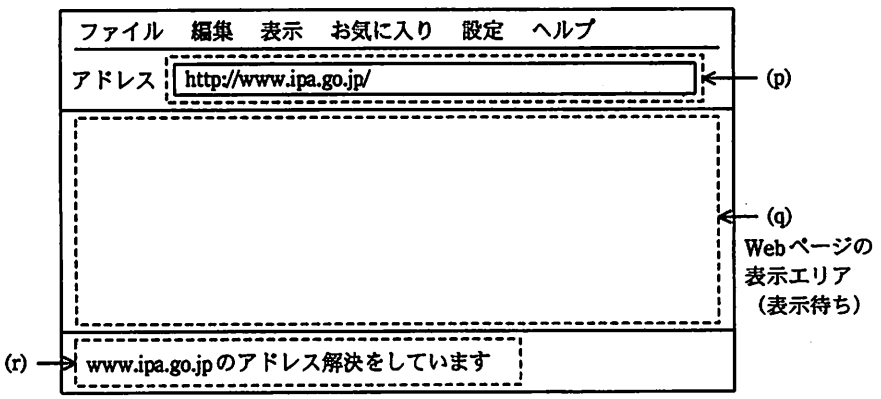

図1　Webページを閲覧しようとしたときのブラウザの状態

J主任　：なるほど，図1中の［　a　］を見ると，DMZ上のDNSサーバに問題があるようです。当社の社内ネットワークの構成は図2のとおりです。設置してあるパケットモニタの，該当する時間帯のログを解析してみましょう。

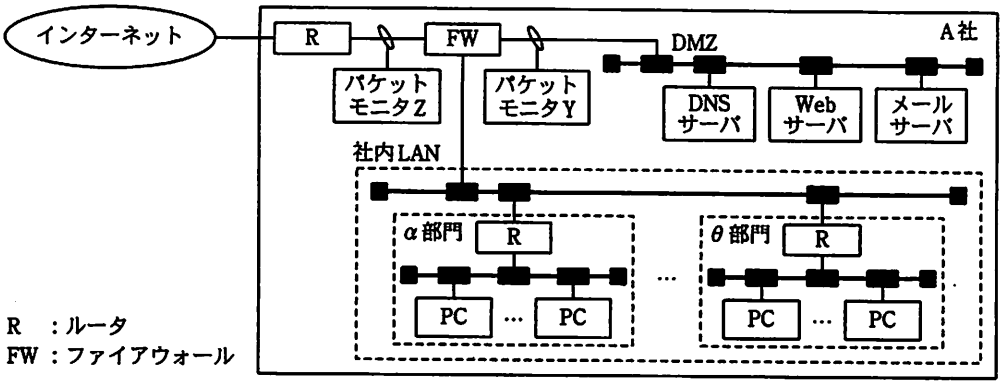

図2　A社の社内ネットワークの構成

K君　：パケットモニタYには，DNSクエリとそれに対応するDNSクエリレスポンスが多量に記録されていました。しかし，パケットモニタZには，DNSクエリを伴わないDNSクエリレスポンスが多量に記録されていました。パケットモニタZのログを図3に示します。

番号	経過時間(秒)	送信元	あて先	プロトコル	詳細	
1	0.000	p1.p2.p3.p4	r1.r2.r3.r4	DNS	Query response, No such name	(Ⅲ)
2	0.001	p1.p2.p3.p4	r1.r2.r3.r4	DNS	Query response, No such name	
3	0.003	p1.p2.p3.p4	r1.r2.r3.r4	DNS	Query response, A q1.q2.q3.q4	(Ⅳ)
4	0.004	p1.p2.p3.p4	r1.r2.r3.r4	DNS	Query response, A q1.q2.q3.q4	
5	0.007	p1.p2.p3.p4	r1.r2.r3.r4	DNS	Query response, A s1.s2.s3.s4	(Ⅴ)
6	0.008	p1.p2.p3.p4	r1.r2.r3.r4	DNS	Query response, A s1.s2.s3.s4	
		(Ⅰ)	(Ⅱ)			

p1.p2.p3.p4：DMZ上のDNSサーバのIPアドレス
q1.q2.q3.q4：DMZ上のWebサーバのIPアドレス
r1.r2.r3.r4，s1.s2.s3.s4：インターネット上のIPアドレス

図3　パケットモニタZのログ（抜粋）

J主任　：このようなログは，社内LAN上のPCがDNSクエリを送信するときに自身のIPアドレスを［　b　］のIPアドレスに［　c　］した場合に記録されます。

K君　：不正なDNSクエリが多量にDMZ上のDNSサーバに送りつけられたことで，Webページを閲覧するときの応答が遅くなったのですね。確かに，すべての社内PCからの名前解決を，DMZ上のDNSサーバが担っていますか

ら。

J主任 ：こういった通信は［ d ］攻撃と呼ばれています。至急，不正なパケットを棄却する設定をすべての部門のルータに適用してください。

K君 ：はい，分かりました。

J主任 ：こうした事象は，ウイルス感染によってよく引き起こされます。今回の事象以外にも，異常な通信が観測される可能性があります。社内LANに接続されているすべての部門のルータにパケットモニタを設置して，原因となっている社内PCを特定してください。

K君 ：ルータへの設定が終わり次第，パケットモニタによる調査を開始します。

J主任 ：ところで，図3中の［ e ］と［ f ］の記録から，DMZ上のDNSサーバが攻撃の踏み台に利用される危険性があることが分かります。①DNSサーバの不適切な設定も修正しておくべきですね。

K君 ：はい，分かりました。

〔異常PCの特定〕

K君は社内LANに接続されたすべての部門のルータの配下にパケットモニタを設置して，異常な通信の監視を開始した。

番号	経過時間(秒)	送信元	あて先	プロトコル	詳細	
1	0.000	a1.a2.a3.a4	b1.b2.b3.b4	DNS	Query, MX ipa.go.jp	
2	0.328	b1.b2.b3.b4	a1.a2.a3.a4	DNS	Query response, MX 10 ipa.go.jp	
3	1.503	a1.a2.a3.a4	c1.c2.c3.c4	DNS	Query, MX jitec.ipa.go.jp	
4	1.632	c1.c2.c3.c4	a1.a2.a3.a4	DNS	Query response MX 20 jitec.ipa.go.jp	(VI)
5	1.982	a1.a2.a3.a4	d1.d2.d3.d4	DNS	Query, MX sec.ipa.go.jp	
6	2.036	d1.d2.d3.d4	a1.a2.a3.a4	DNS	Query response MX 10 sec.ipa.go.jp	
⋮	⋮	⋮	⋮	⋮	⋮	
16	2.421	a1.a2.a3.a4	e1.e2.e3.101	Netbios	TCP-SYN	
17	2.532	a1.a2.a3.a4	e1.e2.e3.102	Netbios	TCP-SYN	(VII)
18	2.592	a1.a2.a3.a4	e1.e2.e3.103	Netbios	TCP-SYN	
19	2.604	a1.a2.a3.a4	e1.e2.e3.104	Netbios	TCP-SYN	
⋮	⋮	⋮	⋮	⋮	⋮	

a1.a2.a3.a4：α部門内のIPアドレス
b1.b2.b3.b4, c1.c2.c3.c4, d1.d2.d3.d4, e1.e2.e3.101～104：インターネット上のIPアドレス

図4 社内LANからインターネットに向けたパケットログ（抜粋）

K君　：図4がα部門に設置したパケットモニタのログです。

J主任　：②図4中の(Ⅵ)に示した箇所に，通常の社内PCには見られない不審な通信挙動が記録されていますね。これは［　g　］におけるアドレス探索に見られる特徴です。また，図4中の(Ⅶ)に示した箇所にも，不審な通信挙動が記録されていますね。(Ⅶ)に示す通信によって，③通信の異常な偏りが発生します。

K君　：なるほど，a1.a2.a3.a4に該当する社内PCが，原因となっているPCですね。

J主任　：こうした視点で，ほかの部門に設置したパケットモニタのログも確認してみましょう。

〔異常PCの対処と今後の対策〕

J主任とK君は，全部門のパケットモニタのログを調べた結果，IPアドレスがa1.a2.a3.a4のログだけに異常が見られたことから，このIPアドレスのPCへの対処を開始した。この対処として，通信プロセス名，実行ファイル名，通信のあて先のIPアドレスとポート番号を記録する通信プロセスモニタを，該当するPCに設定して監視を行った。

K君　：該当するPCに設定した通信プロセスモニタのログから，起動していた④不審な通信プロセスを特定でき，それがウイルスであることが分かったので，その実行ファイルを削除しておきました。このPCではウイルス対策ソフトが起動しており，そのパターンファイルの自動更新も設定されていました。検知できないウイルスもあるのですね。

J主任　：そのとおりです。昨今，次々と新たなウイルスが作られているので，完全な検知が難しくなっています。

K君　：該当するPCにログインしたまま1日間操作しないで通信状況を監視したところ，DNSパケットだけでなくすべてのTCP/UDPパケットの発信が止まったことを確認しました。

J主任　：それは変ですね。当社の設定では，操作しないPCでもPCにログインしていれば，⑤TCP/UDPパケットは自動的に発信されます。hostsファイルが改ざんされているのではないでしょうか。

K君　：図5がhostsファイルです。確かに，ウイルス対策ソフトのパターンファイルの配布サイト情報が追加されているようです。

J主任：hostsファイルの改ざん以外にも，ほかの設定ファイルの改ざんや未知のウイルスへの感染の可能性があります。OSの再インストールで対処してください。

K君　：はい，分かりました。

```
127.0.0.1    localhost
127.0.0.1    www.○○○.com
127.0.0.1    download.△△△.co.jp
127.0.0.1    get.□□□.com
127.0.0.1    update.◇◇◇.com
127.0.0.1    get.☆☆☆.com
```

ウイルス対策ソフトの
パターンファイルの配布サイト

注　図中の“○○○”，“△△△”，“□□□”，“◇◇◇”，“☆☆☆”は，特定の文字列を表す。

図5　異常PCのhostsファイル

その後，J主任とK君は，ウイルスの感染経路を特定し，再発防止策を講じた。

設問1　〔原因調査と対処〕について，(1)～(4)に答えよ。

(1) 本文中の［　a　］に該当する最も適切な箇所を図1中の(p)～(r)から選び，記号で答えよ。

(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。また，本文中の［　c　］に入れる適切な字句を，5字以内で答えよ。

bに関する解答群

ア　DMZ上のDNSサーバ　　イ　DMZ上のWebサーバ

ウ　インターネット上

(3) 本文中の［　d　］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 cache poisoning　　イ　DNS reflection

ウ　総当たり　　エ　ファーミング

(4) 本文中の［　e　］に該当する適切な箇所を図3中の(Ⅰ)，(Ⅱ)から，

[f] に該当する適切な箇所を (Ⅲ) ～ (Ⅴ) からそれぞれ選び，記号で答えよ。また，本文中の下線①について，どのような修正を行うべきか。50 字以内で述べよ。

設問 2 〔異常 PC の特定〕について，(1)，(2) に答えよ。

(1) 本文中の下線②の不審な通信挙動について，30 字以内で具体的に述べよ。また，本文中の [g] 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 amplification 攻撃　　イ UDP ポートスキャン

ウ ゾーン転送　　エ 迷惑メール送信

(2) 本文中の下線③の通信の異常な偏りについて，該当するものを解答群の中から二つ選び，記号で答えよ。

解答群

ア DNS クエリなしに通信を試みたあて先アドレス数の増加

イ TCP-RST パケット受信数の低下

ウ コネクション接続成功率の低下

エ 平均パケットサイズの増加

設問 3 〔異常 PC の対処と今後の対策〕について，(1)，(2) に答えよ。

(1) 本文中の下線④について，K 君はどのような通信挙動のプロセスに注目したか。40 字以内で述べよ。

(2) 本文中の下線⑤について，正常な PC を放置した場合，どのような TCP/UDP パケットが観測されるべきなのか。図 5 を考慮して 40 字以内で述べよ。