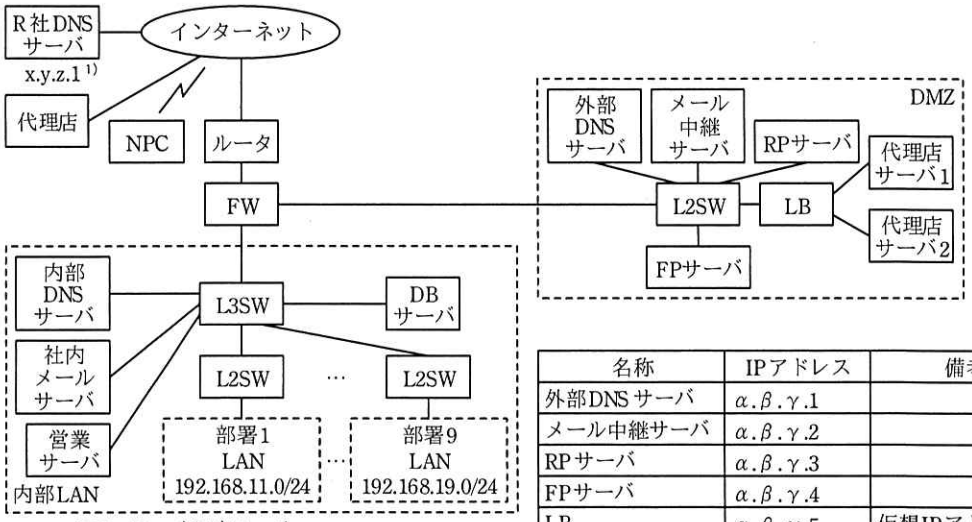
問2　ネットワークのセキュリティ対策に関する次の記述を読んで，設問 1～6 に答えよ。

W 社は，IT 製品の卸売会社であり，国内外のベンダ 50 社の製品を，500 社の販売代理店に卸している。W 社では，販売代理店向けに販売代理店支援システム（以下，代理店システムという）を，自社営業員向けに営業支援システム（以下，営業システムという）を稼働させている。W 社の本社 LAN の構成を図 1 に示す。



FW：ファイアウォール
RP サーバ：リバースプロキシサーバ
FP サーバ：フォワードプロキシサーバ
DB サーバ：データベースサーバ
L2SW：レイヤ 2 スイッチ
L3SW：レイヤ 3 スイッチ
LB：負荷分散装置
NPC：ノート PC

名称	IP アドレス	備考
外部 DNS サーバ	α.β.γ.1	
メール中継サーバ	α.β.γ.2	
RP サーバ	α.β.γ.3	
FP サーバ	α.β.γ.4	
LB	α.β.γ.5	仮想 IP アドレス
代理店サーバ 1	192.168.1.1	
代理店サーバ 2	192.168.1.2	
内部 DNS サーバ	192.168.10.1	
社内メールサーバ	192.168.10.2	
営業サーバ	192.168.10.10	
DB サーバ	192.168.10.20	

注記 1　DMZ の公開サーバ用のグローバル IP アドレスのネットワークアドレスは，α.β.γ.0/28 である。
注記 2　W 社の NPC は，部署 1～9 の LAN に接続されている。
注 1)　x.y.z.1 は，ISP 事業者である R 社の R 社 DNS サーバに付与されたグローバル IP アドレスを示す。R 社 DNS サーバは，スレーブ DNS サーバとして利用されている。

図 1　W 社の本社 LAN の構成

本社 LAN の各システム又は各機器の構成，機能及び動作は，次のとおりである。

・代理店システムは，DMZ の LB，代理店サーバ及び内部 LAN の DB サーバから構成されている。代理店サーバは 2 台あり，LB で負荷分散されている。

・営業システムは，DMZ の RP サーバと内部 LAN の営業サーバから構成されている。外出先からの営業システムの利用は，RP サーバ経由で行われる。

・内部 LAN の各部署の NPC から，インターネット上の Web サイトへのアクセス，及び DMZ と内部 LAN のサーバから，マルウェア対策ソフトの定義ファイル更新のためのベンダの Web サイトへのアクセスは，FP サーバ経由で行われる。
・外部 DNS サーバは，DMZ のゾーン情報を管理するだけでなく，再帰的な名前解決を行うフルリゾルバとしても機能している。外部 DNS サーバはマスタ DNS サーバであり，インターネット上の R 社 DNS サーバをスレーブ DNS サーバとして利用している。
・メール中継サーバは，社外のメールサーバ及び社内メールサーバとの間で，電子メール（以下，メールという）の転送を行う。
・内部 DNS サーバは，内部 LAN のゾーン情報を管理し，当該ゾーンに存在しないホストの名前解決要求は，外部 DNS サーバに転送する。
・社内メールサーバは，社員のメールボックスを保持し，内部 LAN の NPC との間でメールの送受信を行う。

昨今，サイバー攻撃が増加しており，情報システムは，情報漏えい，Web サービスの妨害，サーバの不正利用などの脅威にさらされている。そこで，W 社では，本社 LAN のセキュリティ対策を見直すことにした。情報システム部の M 課長は，ネットワーク運用担当の N 主任に，本社 LAN のセキュリティ対策の見直しを指示した。

N 主任は，部下の J さんへの指導を兼ねて，J さんと一緒に本社 LAN のセキュリティ対策を見直すことにした。

〔本社 LAN のセキュリティ対策の状況〕

まず，N 主任は J さんに，本社 LAN のセキュリティ対策の状況について確認した。その時の，2 人の会話を次に示す。

N 主任：本社 LAN のセキュリティ対策の状況を説明してくれないか。
J さん ：はい。本社 LAN は，FW でインターネットからの IP パケットをフィルタリングしています。また，FP サーバでは，フィルタリングソフトウェアを稼働させて，URL フィルタリングを行っています。DMZ と内部 LAN のサーバではマルウェア対策ソフトが稼働しており，インターネット上のベンダ

の Web サイトにアクセスし，マルウェア定義ファイルが更新されているときは，自動でダウンロードするように設定されています。サーバ OS やミドルウェアへのセキュリティパッチの適用は，サーバ運用担当が実施しているとのことです。

N 主任：分かった。それでは，FW のフィルタリングの詳細を調べてくれないか。

J さんは，FW の設定内容を調査し，通信を許可する FW のルールを表 1 にまとめた。

表 1　通信を許可する FW のルール

項番	アクセス経路	送信元 IP アドレス	宛先 IP アドレス	プロトコル／ポート番号
1	インターネット→DMZ	any	α.β.γ.1	UDP/53 [1]
2		ア	α.β.γ.1	TCP/53
3		any	α.β.γ.2	TCP/25
4		any	α.β.γ.3	TCP/80，TCP/443
5		any	α.β.γ.5	TCP/80，TCP/443
6	DMZ→インターネット	α.β.γ.1	any	TCP/53 [2]，UDP/53
7		α.β.γ.2	any	TCP/25
8		α.β.γ.4	any	TCP/80，TCP/443
9	DMZ→内部 LAN [3]	α.β.γ.2	192.168.10.2	TCP/25
10		α.β.γ.3	192.168.10.10	TCP/80，TCP/443
11		192.168.1.1	192.168.10.20	TCP，UDP/アクセス用ポート番号
12		192.168.1.2	192.168.10.20	TCP，UDP/アクセス用ポート番号
13	内部 LAN→DMZ	192.168.10.1	α.β.γ.1	UDP/53 [1]
14		192.168.10.2	α.β.γ.2	TCP/25
15		192.168.10.1	α.β.γ.4	TCP/8080 [4]
16		192.168.10.2	α.β.γ.4	TCP/8080 [4]
17		192.168.10.10	α.β.γ.4	TCP/8080 [4]
18		192.168.10.20	α.β.γ.4	TCP/8080 [4]
19		部署 1～9 の LAN	α.β.γ.4	TCP/8080 [4]
20		部署 1～9 の LAN	α.β.γ.5	TCP/80，TCP/443

注記 1　内部 LAN から行われる，DMZ のサーバの運用管理用通信の許可ルールは省略している。
注記 2　FW は，ステートフルパケットインスペクション機能をもつ。
注 [1]　DNS の応答は，TCP フォールバックが発生しないので，UDP/53 だけを許可している。
[2]　古い DNS サーバの存在を考慮して，TCP/53 の通信を許可している。
[3]　DMZ から内部 LAN のサーバへの通信は，直接 IP アドレスを指定して行われる。
[4]　TCP/8080 は，代替 HTTP のポートである。

〔FW のフィルタリング内容の調査結果〕

J さんは，表 1 を N 主任に説明した。その時の 2 人の会話を次に示す。

J さん　：調べたところ，FW で許可している通信は，表 1 のとおりになっていました。

N 主任：現在の設定で，［　a　］スキャンとポートスキャンには対応できているようだ。DoS 攻撃は，送信元 IP アドレスを偽装して行われることがある。我が社が利用している ISP では，①利用者のネットワークとの接続ルータで，uRPF（Unicast Reverse Path Forwarding）と呼ばれるフィルタリングを行っているので，偽装されたパケットが当社に到達することは少なくなっていると考えられる。しかし，DoS 攻撃がなくなっているわけではない。DoS 攻撃への対策状況について，J さんの考えを聞かせてくれないか。

J さん：②DMZ の全ての公開サーバを対象とするブロードキャストアドレス宛てのスマーフ（smurf）攻撃のパケットは，FW でブロックされます。クローズのポート宛てに UDP パケットを送ると，RFC 792 で規定された［　b　］パケットが送信元 IP アドレス宛てに返送されるのを悪用し，サーバのリソースを消費させる UDP フラッド（UDP flood）攻撃も，FW の設定で防げていると思います。

N 主任：そのとおりだ。しかし，SYN フラッド（SYN flood）攻撃については対策が必要だ。どのような対応が必要なのかを検討してくれないか。

J さん　：分かりました。SYN フラッド攻撃について調べてみます。

〔SYN フラッド攻撃手法と対策技術〕

J さんが，SYN フラッド攻撃手法と対策技術について調査した内容を次に示す。

SYN フラッド攻撃は，SYN パケットを受信したサーバが，TCP コネクション確立のために数十バイトのメモリを確保しなければならない仕様を悪用し，攻撃者が大量の SYN パケットを標的のサーバに送りつけてサーバをダウンさせる攻撃である。

例えば，インターネットから図 1 中のメール中継サーバ宛てに送信される，TCP/25 の SYN パケットは，表 1 中の項番［　c　］のルールによってメール中継サーバに転送される。SYN パケットを受信したメール中継サーバは，コネクション確立のためにメモリを確保し，ACK パケットの返送がなくても，確保したメモリを

一定時間解放しない。また，ACK パケットが返送されて不正なコネクションが確立された場合は，更に長い時間メモリが解放されない。そのため，メール中継サーバが大量の SYN パケットを受信すると，大量のメモリを消費して正常に稼働できなくなるおそれがある。

SYN フラッド攻撃の防御技術には，ディレイドバインディングと SYN クッキーがある。ディレイドバインディング技術を図 2 に示す。

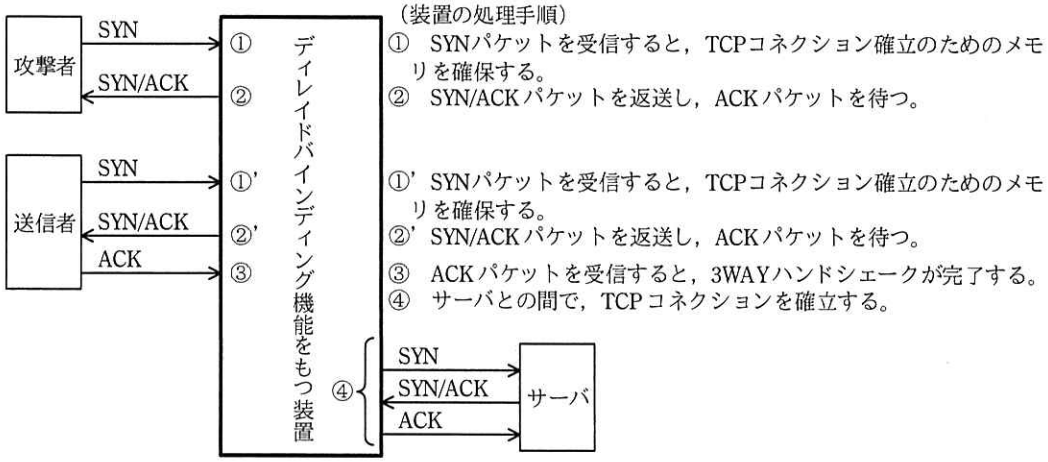


図 2　ディレイドバインディング技術

図 2 の方式によって，サーバでの不要なメモリ確保を抑止できる。しかし，図 2 の方式には，装置のメモリ容量によって同時接続数が制限される弱点がある。一方，SYN クッキーでは，この弱点が改善されている。SYN クッキー技術を図 3 に示す。

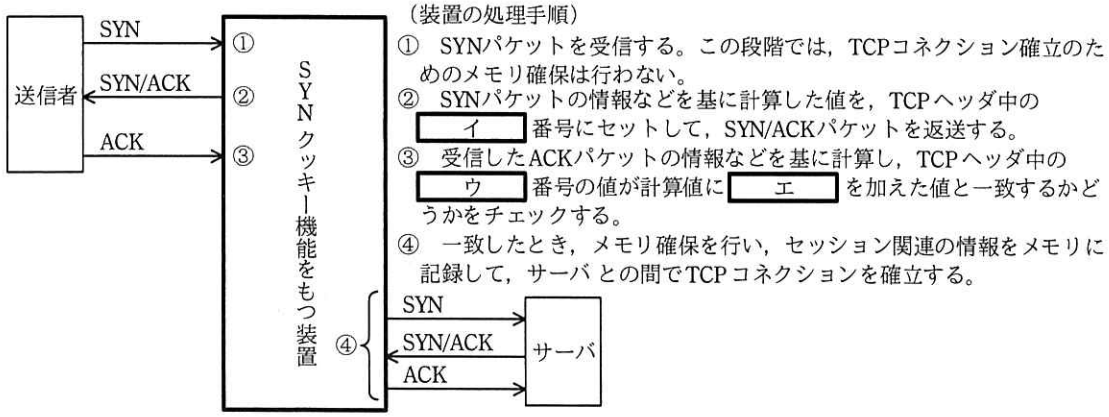


図 3　SYN クッキー技術

図 3 の方式は，パケット中の該当するコネクションに関連する情報などに，特別な演算によって計算した変換値をクッキーとして，TCP ヘッダ中のシーケンス番号に埋め込んで，通信の状態を監視するものである。

J さんは，二つの防御技術を比較した結果，③ SYN クッキーの方式では同時接続数の制限が緩和されることが分かったので，SYN クッキー技術をもつ IPS（Intrusion Prevention System）の導入を N 主任に提案した。その時の 2 人の会話を次に示す。

J さん ：SYN フラッド攻撃への対策が必要です。SYN クッキー技術をもつ IPS の導入を提案します。

N 主任：分かった。IPS を導入すれば，SYN フラッド攻撃だけでなく様々な不正な通信も遮断できるので，導入を検討しよう。そのほかに，DMZ のサーバが送信元偽装の目的で踏み台にされる可能性について，考えを聞かせてくれないか。

J さん ：④ FP サーバについては，FW の設定で防止できています。⑤メール中継サーバについては，サーバ自体の転送設定で防止しています。外部 DNS サーバについても大丈夫だと思います。

N 主任：外部 DNS サーバは，DNS リフレクタ攻撃の踏み台にされる可能性がありそうだ。安全面を考慮すれば，構成変更が必要になるかもしれない。対応策を考えてくれないか。

J さんは，外部 DNS サーバの構成上の問題点について考えた。外部 DNS サーバは，ゾーン情報管理サーバ（以下，コンテンツサーバという）の機能と，フルリゾルバの機能をもつので，表 1 中の項番 1 と項番 6 の通信が許可されている。フルリゾルバによるインターネット上のホストの名前解決は，［ d ］と［ e ］からの要求に対応できればよいが，コンテンツサーバは，インターネット上の不特定のホストからの名前解決要求に応答する必要がある。そこで，外部 DNS サーバを，コンテンツサーバとして機能する DNS サーバ 1 と，フルリゾルバサーバとして機能する DNS サーバ 2 に分離すれば，踏み台にされる可能性は低くなると考えた。その場合，表 1 中の項番 6 のルールの変更が必要になる。DNS サーバ 1 に $\alpha.\beta.\gamma.1$，DNS サーバ 2 に $\alpha.\beta.\gamma.6$ を割り当てたときの，表 1 の変更内容を表 2 に示す。

表2　表1の変更内容

項番	アクセス経路	送信元IPアドレス	宛先IPアドレス	プロトコル／ポート番号
6	（省略）	オ	カ	（省略）

J さんは，検討結果を N 主任に説明した。J さんの説明を受けた N 主任は，外部 DNS サーバの構成変更後の，DNS サーバへの攻撃についての調査を指示した。

〔DNS サーバへの攻撃と対策〕

J さんは，DNS サーバへの攻撃の中でリスクの大きい，DNS キャッシュポイズニング攻撃の手法について調査した。J さんが理解した内容を次に示す。

DNS キャッシュポイズニング攻撃は，次の手順で行われる。

(i) 攻撃者は，偽の情報を送り込みたいドメイン名について，標的のフルリゾルバサーバに問い合わせる。

(ii) フルリゾルバサーバは，指定されたドメインのゾーン情報を管理するコンテンツサーバに問い合わせる。

(iii) ⑥攻撃者は，コンテンツサーバから正しい応答が返ってくる前に，大量の偽の応答パケットを標的のフルリゾルバサーバ宛てに送信する。

(iv) フルリゾルバサーバは，受信した偽の応答パケットをチェックし，偽の応答パケットが正当なものであると判断してしまった場合，キャッシュの内容を偽の応答パケットを基に書き換える。

(ii) の問合せパケットと，(iii) の応答パケットの情報を表3に示す。

表3に示すように，(ii) の問合せパケットの送信元ポート番号には特定の範囲の値が使用されるケースが多いので，攻撃者は，(iii) の偽の応答パケットを正当なパケットに偽装しやすくなるという問題がある。調査の結果，この問題の対応策には，送信元ポート番号のランダム化があることが分かった。

表3 （ii）の問合せパケットと，（iii）の応答パケットの情報（抜粋）

項番	ヘッダ名	項目名	問合せパケットの情報	応答パケットの情報
1	IP ヘッダ	送信元 IP アドレス	フルリゾルバサーバの IP アドレス	キ
2		宛先 IP アドレス	コンテンツサーバの IP アドレス	ク
3		プロトコル	UDP	UDP
4	UDP ヘッダ	送信元ポート番号	n [1]	ケ
5		宛先ポート番号	53	コ
6	DNS ヘッダ	識別子	m [2]	サ
7		フラグ中の QR ビット	0（問合せ）	1（応答）

注 [1] n には特定の範囲の値が設定されるケースが多い。
注 [2] m には任意の値が設定される。

J さんは，⑦外部 DNS サーバの構成変更によって，インターネットからの DNS サーバ 2 へのキャッシュポイズニング攻撃は防げると判断した。さらに，万が一の場合に備え，DNS サーバ 2 には，送信元ポート番号のランダム化に対応した製品の導入を提案することにした。

J さんは，調査結果と対応策を N 主任に説明し，DNS サーバ 2 には送信元ポート番号のランダム化対応の製品の導入が了承された。

〔マルウェアの内部 LAN への侵入時の対策〕

次に，2 人は，マルウェアの内部 LAN への侵入時の対策について検討した。

ネットワークのセキュリティ対策を行っても，ソーシャルエンジニアリングなどによって W 社内の情報が漏えいすると，内部 LAN の NPC は，マルウェアに侵入されるおそれがある。NPC に侵入したマルウェアは，攻撃者が管理・運営する C&C（Command & Control）サーバとの間の通信路を設定した後，C&C サーバ経由で攻撃者から伝達された命令を実行して，自身の拡散や C&C サーバへの秘密情報の送信などを行うことがある。このとき，C&C サーバの IP アドレスが特定できれば，FP サーバで C&C サーバとの通信は遮断できる。しかし，Fast Flux と呼ばれる手法を用いて，IP アドレスの特定を困難にすることによって，C&C サーバなどを隠蔽する事例が報告されている。

Fast Flux は，特定のドメインに対する DNS レコードを短時間に変化させることによって，サーバの追跡を困難にさせる手法である。Fast Flux 手法が用いられたときのマルウェアによる C&C サーバとの通信例を，図 4 に示す。

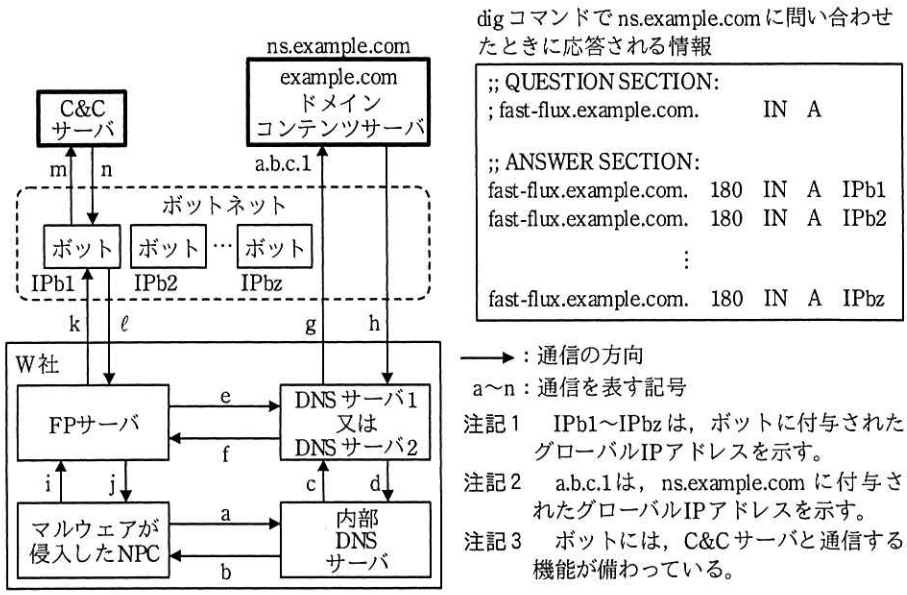


図 4 Fast Flux 手法が用いられたときのマルウェアによる C&C サーバとの通信例（抜粋）

攻撃者は，example.com ドメインを取得してコンテンツサーバ（ns.example.com）を設置する。図 4 中の ns.example.com には，fast-flux の FQDN に対する A レコードとして大量のボットの IP アドレス，及び DNS ラウンドロビンが設定される。

図 4 には，W 社の内部 LAN の NPC に侵入したマルウェアが，fast-flux.example.com にアクセスした後，ボットに備わる機能を利用して，C&C サーバとの間で行われる通信を示している。⑧図 4 中の example.com ドメインのコンテンツサーバの設定の場合，マルウェアが，一定間隔で fast-flux.example.com へアクセスを行えば，毎回，異なる IP アドレスで，ボットを経由して C&C サーバと通信することになる。

このような方法を用いることによって，C&C サーバの IP アドレスを隠蔽できる。しかし，マルウェアが同一の FQDN のホストにアクセスすることになるので，fast-flux.example.com へのアクセスによって C&C サーバとの通信が行われることが判明すれば，FP サーバの URL フィルタリングで C&C サーバとの通信は遮断できる。攻撃者は，これを避けるために Domain Flux と呼ばれる手法を用いることがある。

Domain Flux は，ドメインワイルドカードを用いて，あらゆるホスト名に対して，同一の IP アドレスを応答する手法である。Fast Flux と Domain Flux を組み合わせることによって，C&C サーバの FQDN と IP アドレスの両方を隠蔽できる。図 4 に示した構成の Fast Flux と Domain Flux を組み合わせたときの，ns.example.com に設定

されるゾーンレコードの例を図5に示す。

```
$ ORIGIN    example.com.
                        IN      NS      ns.example.com.
ns          86400       IN      A       a.b.c.1
*           180         IN      A       IPb1
*           180         IN      A       IPb2
                        :
*           180         IN      A       IPbz
```

図5　ns.example.com に設定されるゾーンレコードの例（抜粋）

このような攻撃が行われた場合を想定し，2人は，現行の FP サーバを HTTPS 通信の復号機能をもつ機種に交換し，プロキシ認証を併せて行うことにした。交換する FP サーバでのプロキシ認証のセキュリティを高めるために，社内の NPC の Web ブラウザで，オートコンプリート機能を無効にし，ID，パスワードのキャッシュを残さないようにすることにした。また，内部 LAN に侵入したマルウェアの活動を早期に検知するために，⑨ FP サーバと FW のログを定期的に検査することにした。

以上の検討を基に，N 主任と J さんは，(1) IPS の導入，(2) 外部 DNS サーバの構成変更と新機種の導入，(3) FP サーバの交換，(4) NPC の設定変更，及び (5) ログの定期的な検査から成る5項目の実施案をまとめ，M 課長に提出した。

2人がまとめた実施案は，経営会議で承認され，実施に移されることになった。

設問1　本文中の［　a　］～［　e　］に入れる適切な字句又は数値を答えよ。

設問2　表1中の［　ア　］に入れる適切な IP アドレスを答えよ。また，項番2のルールによって行われる通信の名称を答えよ。

設問3　〔FW のフィルタリング内容の調査結果〕について，(1)，(2) に答えよ。

(1)　本文中の下線①について，フィルタリングの内容を，70字以内で述べよ。

(2)　本文中の下線②の IP アドレスを答えよ。

設問4　〔SYN フラッド攻撃手法と対策技術〕について，(1)～(5) に答えよ。

(1)　図3中の［　イ　］～［　エ　］に入れる適切な字句又は数値を答えよ。

(2)　本文中の下線③の，制限が緩和されるのは，ディレイドバインディング方

式よりメモリ消費量が少なくて済むからである。その理由を，35 字以内で述べよ。

(3) 本文中の下線④について，防止できていると判断した理由を，40 字以内で述べよ。

(4) 本文中の下線⑤について，防止するためにメール中継サーバに設定されている処理方法を，50 字以内で述べよ。

(5) 表 2 中の［ オ ］，［ カ ］に入れる適切な字句を答えよ。

設問 5 〔DNS サーバへの攻撃と対策〕について，(1)～(3) に答えよ。

(1) 表 3 中の問合せパケットに対して，フルリゾルバサーバが正当な応答パケットと判断するパケットの内容について，表 3 中の［ キ ］～［ サ ］に入れる適切な字句又は数値を答えよ。

(2) 本文中の下線⑥では，大量の偽の応答パケットが送信される。当該パケット中で，パケットごとに異なる内容が設定される表 3 中の項目名を，全て答えよ。

(3) 本文中の下線⑦について，防げると判断した根拠を，60 字以内で述べよ。

設問 6 〔マルウェアの内部 LAN への侵入時の対策〕について，(1)～(5) に答えよ。

(1) 図 4 中で，fast-flux.example.com の名前解決要求と応答の通信を a～n の中から全て選び，通信が行われる順番に並べよ。

(2) 本文中の下線⑧について，DNS サーバ 2 がキャッシュした DNS レコードが消去されるまでの時間（分）を答えよ。

(3) 図 5 のようにゾーンレコードが設定された場合，C&C サーバを効果的に隠蔽するための，マルウェアによる C&C サーバへのアクセス方法について，25 字以内で述べよ。

(4) 本文中の下線⑨について，FP サーバのログに，マルウェアの活動が疑われる異常な通信が記録される場合がある。その通信の内容を，35 字以内で述べよ。

(5) 内部 LAN の NPC に侵入したマルウェアが，FP サーバを経由せずに C&C サーバの FQDN 宛てにアクセスを試みた場合は，マルウェアによる C&C サーバとの通信は失敗する。通信が失敗する理由を，40 字以内で述べよ。