問1　インターネットに公開されているサーバの情報セキュリティ対策に関する次の記述を読んで，設問1～4に答えよ。

Y社は，従業員数1,000名の通信販売会社である。Y社では，会員として登録した顧客あてに，3か月ごとに商品カタログを送付し，会員からの注文を，電話，ファックス及び郵便によって受け付けている。さらに，商品カタログを掲載するWebサーバ（以下，カタログWebサーバという）と，会員からの注文を受け付けるWebサーバ（以下，受注Webサーバという）などからなる受注システムを用いたネット通販も行っている。

Y社のネットワーク構成を図1に示す。従業員による社内業務サーバの利用，電子メール（以下，メールという）の送受信及びプロキシサーバ経由のインターネットWebサイトの閲覧のためにPCを設置している。

図1中の，現在の受注システムのサーバ群が老朽化したので，更新することになった（以下，更新後のシステムを新受注システムという）。新受注システムのサーバ構成は，現在の受注システムと同じである。

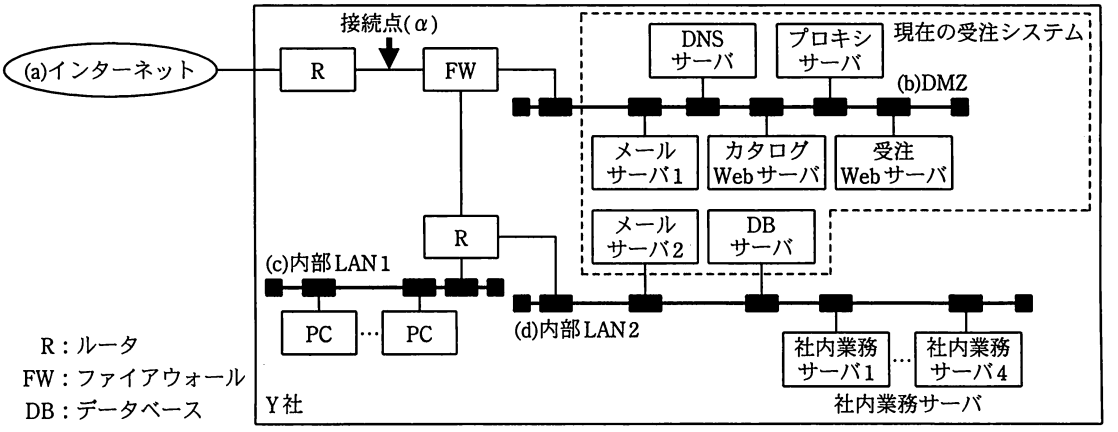

図1　Y社のネットワーク構成

FWのフィルタリングルール（以下，FWルールという）では，通信パケットの送信元，あて先及びサービスの組合せによって，許可又は拒否の動作を指定することができる。FWルールを表1に示す。

表1　FWルール

項番	送信元	あて先	サービス	動作
1	すべて	カタログWebサーバ	HTTP	許可
2	すべて	受注Webサーバ	HTTPS	許可
3	内部LAN1	プロキシサーバ	代替HTTP	許可
4	内部LAN1	すべて	すべて	拒否
5	プロキシサーバ	インターネット	HTTP，HTTPS	許可
6	インターネット	DNSサーバ	DNS	許可
7	DNSサーバ	インターネット	DNS	許可
8	インターネット	メールサーバ1	SMTP	許可
9	メールサーバ1	インターネット	SMTP	許可
10	メールサーバ2	メールサーバ1	SMTP	許可
11	メールサーバ1	メールサーバ2	SMTP	許可
12	すべて	DMZ	SSH	許可
⋮	⋮	⋮	⋮	⋮
18	すべて	すべて	すべて	拒否

注1　上から順に，最初に一致したルールが適用される。

注2　Y社で利用する主要なサービスのポート番号を，次に示す。

HTTP：80，HTTPS：443，代替HTTP：8080，DNS：53，SMTP：25，SSH：22

注3　項番13～17のFWルールは，カタログWebサーバとDBサーバ間の通信，受注Webサーバと DBサーバ間の通信，時刻同期の通信，サーバ監視の通信及びネットワーク監視の通信に関するものである。

DMZに設置されているサーバのIPアドレスは表2のとおりである。

表2　DMZに設置されているサーバのIPアドレス

サーバ	IPアドレス
DNSサーバ	x1.y1.z1.2
プロキシサーバ	x1.y1.z1.3
メールサーバ1	x1.y1.z1.4
カタログWebサーバ	x1.y1.z1.5
受注Webサーバ	x1.y1.z1.6

新受注システムへの更新は情報システム部で行うことになった。

情報システム部は，技術グループ（以下，技術Gという），開発グループ（以下，開発Gという）及び運用グループ（以下，運用Gという）から構成されている。各グループの主な業務は次のとおりである。

・技術Gは，情報システム関連技術の調査及びY社の情報システムの品質管理を行う。

・開発 G は，Y 社の情報システムのインフラ構築及びアプリケーション開発を行う。

・運用 G は，Y 社の情報システムの運用，監視及び保守を行う。

情報システム部では，新受注システムへの更新を機会に，情報セキュリティ対策として，次の二つを行った。

(1) 最新の情報セキュリティ対策を盛り込み，DMZ に設置されるサーバの情報セキュリティ対策基準（以下，DMZ 対策基準という）を作成

(2) 情報セキュリティ品質向上のために，DMZ に設置されるサーバの導入手順（以下，サーバ導入手順という）を作成

作成した DMZ 対策基準を図 2 に示す。この DMZ 対策基準は新受注システムに適用される。

(1) 共通対策基準
  (1-a) 不要な機能は停止する。
  (1-b) 脆弱性への対応を行う。
  (1-c) 導入するソフトウェアは最新版とし，最新の修正プログラムを適用する。
  (1-d) 開発 G 及び運用 G の担当者の利用者 ID だけを登録する。
  (1-e) ネットワーク経由の OS へのログインには暗号化した通信とセキュアな認証を使用する。
  （省略）
(2) DNS サーバ対策基準
  (2-a) オープンリゾルバを禁止する。
  (2-b) DNS キャッシュポイズニング対策を行う。
  （省略）
(3) メールサーバ対策基準
  (3-a) メールアカウントを設定しない。
  (3-b) オープンリレー対策を行う。
  (3-c) 迷惑メール対策を行う。
  （省略）
(4) Web サーバ対策基準
  (4-a) 個人情報を入力する画面では HTTPS を使用する。
  (4-b) 次の Web アプリケーション攻撃への対策を行う。
    ・SQL インジェクション
    ・クロスサイトスクリプティング
  （省略）
(5) プロキシサーバ対策基準
  （省略）
(6) FW 対策基準
  (6-a) 不要な通信は拒否する。
  (6-b) 拒否した通信のログを残す。
  （省略）

図 2　DMZ 対策基準

作成したサーバ導入手順の概要を図 3 に示す。このサーバ導入手順は新受注システムに適用される。

(1) 設計書作成及び設計書審査
(1-a) 開発 G において，DMZ に設置するサーバの設計書を作成する。
(1-b) 技術 G において，設計書を書面査読形式で審査する。審査の結果，DMZ 対策基準に準拠していない事項（以下，審査指摘事項という）がなければ (2) に移る。審査指摘事項があれば開発 G に通知する。
(1-c) 開発 G において，審査指摘事項への対処を実施する。
(1-d) 技術 G において，再度，審査を実施し，審査指摘事項への対処結果を確認する。審査指摘事項が解決されていれば (2) に移る。審査指摘事項が解決されていなければ，開発 G に通知し，(1-c) に戻る。
(2) サーバ設定及びサーバ設定検査
(2-a) 開発 G において，設計書に基づいて，サーバ設定を行う。
(2-b) 技術 G において，DMZ 上と同じ機器構成のテスト用ネットワークにサーバと検査機器を接続して，ペネトレーションテスト（以下，接続前 P テストという）を実施する。接続前 P テストによって脆弱性（以下，設定検査指摘事項という）がなければ (3) に移る。設定検査指摘事項があれば開発 G に通知する。
(2-c) 開発 G において，設定検査指摘事項への対処を実施する。
(2-d) 技術 G において，再度，接続前 P テストを実施し，設定検査指摘事項への対処結果を確認する。設定検査指摘事項が解決されていれば (3) に移る。設定検査指摘事項が解決されていなければ，開発 G に通知し，(2-c) に戻る。
(3) Web アプリケーション検査
（省略）
(4) DMZ 接続及び DMZ 接続検査
(4-a) 開発 G において，サーバを DMZ に接続する。
(4-b) 技術 G において，図 1 中の接続点 (α) に検査機器を接続して，ペネトレーションテスト（以下，接続後 P テストという）を実施する。接続後 P テストによって脆弱性（以下，接続検査指摘事項という）がなければ，運用を運用 G において開始する。接続検査指摘事項があれば開発 G に通知する。
(4-c) 開発 G において，接続検査指摘事項への対処を実施する。
(4-d) 技術 G において，再度，接続後 P テストを実施し，接続検査指摘事項への対処結果を確認する。接続検査指摘事項が解決されていれば，運用を運用 G において開始する。接続検査指摘事項が解決されていなければ，開発 G に通知し，(4-c) に戻る。

図 3　サーバ導入手順の概要

〔設計書作成及び設計書審査の実施〕

新受注システムへの更新は，開発 G の M 主任と N さんが担当することになった。M 主任と N さんは，設計書の作成を行った。技術 G によって設計書審査が行われ，審査指摘事項が図 4 のとおり通知された。

(1) DMZ に設置されるサーバへの SSH 接続について
・パスワード認証方式の利用を中止し，公開鍵認証方式に変更すること。
・FW ルールの設定内容を見直し，より厳しく制限すること。
(2) DNS 機能について
・DNS キャッシュポイズニング対策を行うこと。

図 4　審査指摘事項

M 主任と N さんは審査指摘事項について検討を始めた。

〔DMZ に設置されるサーバへの SSH 接続に関する検討〕

運用 G では，DMZ に設置されているサーバにログインが必要な場合は，各サーバのコンソールからログインを行っている。しかし，休日や夜間は，運用 G のメンバが不在なので，トラブルに対して社外からの緊急対応が必要な場合に備え，各サーバ上に SSH サーバソフト（以下，SSH サーバという）を導入し，運用 G のメンバにノート PC と通信カードを貸与した上で，SSH 接続によるログインを可能としている。契約している通信カードのインターネット接続サービス（以下，契約通信サービスという）では，通信サービス会社が管理している IP アドレスを動的に割り当てる。

M 主任と N さんは，DMZ に設置されるサーバへの接続についての審査指摘事項を確認した。指摘を受ける前，N さんは，サーバへの接続は，SSH によって通信が暗号化されること及び推測しにくいパスワードを使用していることから，パスワード認証方式でもセキュアであると考えていた。しかし，コンピュータセキュリティインシデント対応機関から発表された SSH サーバへのパスワード総当たり攻撃についての注意喚起においては，パスワードが推測される可能性が高いと説明されていた。そのため，開発 G は，図 4 の審査指摘事項に従って，SSH の認証方式を公開鍵認証方式に設計変更した。

次に，FW ルールの設定内容についての見直しを行った。見直しの結果，契約通信サービスを，Y 社専用の IP アドレスが割り当てられるものに変更し，更に①FW ルールの設定内容も変更することにした。

〔DNS 機能に関する検討〕

Y 社の DMZ に設置されているサーバのドメイン名の情報は，DNS サーバを使用して管理している。Y 社の PC 及びサーバは，内部 LAN1 に接続されている PC 及び内部 LAN2 に接続されているサーバの名前解決には，hosts ファイルを用いている。

M 主任と N さんは，DNS キャッシュポイズニング対策について検討した。根本的な対策として，［ a ］という DNS のセキュリティ拡張方式の導入が考えられた。［ a ］は，DNS のレコードに公開鍵暗号方式による［ b ］を付加し，応答を受け取った側ではその［ b ］を検証する方式である。しかし，［ a ］に

は，鍵の管理をどのように行うかなど，今までのDNSサーバにはない運用手順が必要であること，Y社だけでなく大多数の組織が対応していなければならないことから，すぐには採用できない。M主任は，開発Gだけでは解決が難しいと判断し，DNSサーバに導入しているDNSソフトの製品サポート窓口に対応方法を照会した。DNSソフトの製品サポート窓口からは，現時点でとり得る対策として，DNSサーバで，②名前解決の問合せにおいてDNSキャッシュポイズニング攻撃を受けやすい不適切な設定を行わないという解決策が提示され，それに従い設計書を修正した。念のため，現在のDNSサーバの設定を確認したところ，設定は適切であった。

開発Gでの設計書の修正に対して，技術Gは，設計書の審査指摘事項がすべて解決されていることを確認した。

〔サーバ設定及びサーバ設定検査の実施〕

開発Gでは設計書に基づいて，サーバ設定を行った。構築後，技術Gは，接続前Pテストを実施し，図5の設定検査指摘事項を通知した。

(1) 迷惑メール対策について
・カタログWebサーバ及び受注Webサーバのドメイン名を使用したメール送信
DNSサーバの設定によって［ c ］を行うこと。
・メールサーバ1における配送不能通知メール（以下，NDRメールという）
メールサーバ1から送信されるNDRメールが迷惑メールとならない対策を実施すること。

図5　設定検査指摘事項

〔迷惑メール対策に関する検討〕

M主任とNさんは設定検査指摘事項について検討を行った。次は，迷惑メール対策について検討した際の会話である。

M主任：まず，カタログWebサーバ及び受注Webサーバのドメイン名を使用したメール送信について検討しよう。

Nさん：当社では表3のとおり，三つのドメイン名（以下，Y社管理ドメイン名という）を使用しています。カタログWebサーバ及び受注Webサーバに使用するドメイン名を使ったメールの送信は一切ありません。［ c ］を行うことという設定検査指摘事項の必要性がよく理解できません。

表３　Ｙ社が使用しているドメイン名と使用方法

用途	ドメイン名	使用方法
メールアドレス	y-sha.co.jp	*user*@y-sha.co.jp(1)
カタログ Web サーバ	catalog.y-sha.co.jp	http://www.catalog.y-sha.co.jp/
受注 Web サーバ	order.y-sha.co.jp	https://www.order.y-sha.co.jp/

注(1)　*user* は利用者によって異なる。

M 主任：例えば，送信者メールアドレスとしてカタログ Web サーバのドメイン名を使用したメールがお客様あてに届いているとしよう。当社から，メール送信をしていないのに，だれが送信したのかな。

N さん：迷惑メールの送信者でしょうか。

M 主任：そのとおりだ。送信者メールアドレスとしてカタログ Web サーバのドメイン名を使用し，当社以外のサーバから送信されたメール（以下，詐称メールという）だから，当社では止めることができない。どのような対処が必要かな。

N さん：受信側のメールサーバで詐称メールを拒否するか破棄するしかありません。受信側のメールサーバでは，どのように判定できるのでしょうか。

M 主任：メールを送信するサーバはどれかということを判定してもらうために，送信側の DNS サーバに Sender Policy Framework（SPF）の設定を追加すれば対応できるよ。メールを送信するサーバがない場合は，それに対応した設定をすることもできる。詐称メールの送信を止めることはできないが，受信側のメールサーバにおいて，当社からのメールであるかどうかを判別してもらうことができる。

N さん：［　c　］の方法の一つですね。

M 主任：そのとおりだ。送信者メールアドレスとしてカタログ Web サーバ及び受注 Web サーバのドメイン名を使用したメールは送信しない。③その事実を踏まえて DNS サーバに SPF の設定を追加してくれ。

N さん：はい，分かりました。

M 主任：次に，NDR メールの対策について検討しよう。例えば，受信者メールアドレスとして，カタログ Web サーバのドメイン名を使用したメールがメールサーバ１に届いたとしよう。どうなるかな。

N さん：メールの送受信方法は図 6 のとおりで，④メールサーバ１ではオープンリレー防止設定がされているので，そのメールは転送拒否されます。

・社内 PC でのメール送信
　SMTP を使用し，メールサーバ 2 へ送信する。
・社内 PC でのメール受信
　POP3 を使用し，メールサーバ 2 から受信する。
・インターネット側から Y 社あてのメール受信
　SMTP を使用し，メールサーバ 1 で受信し，［　d　］である場合はメールサーバ 2 へ転送し，ほかの場合は拒否する。
・Y 社からインターネット側へのメール送信
　SMTP を使用し，メールサーバ 2 からメールサーバ 1 へ転送し，メールサーバ 1 では，受信者メールアドレスに対応するメールサーバへ転送する。

図 6　Y 社のメール送受信方法

M 主任：そのとおりだ。では，ドメイン名が y-sha.co.jp の実在しない受信者メールアドレスあてにメールが届いた場合はどうなるかな。

N さん：メールサーバ 1 からメールサーバ 2 に転送しようとするが，受信者メールアドレスが実在しないので転送せずに，転送できなかったメールを添付ファイルとした NDR メールを送信者メールアドレスに向けて送信します。

M 主任：では，送信者メールアドレスを偽って，ドメイン名が y-sha.co.jp の実在しない受信者メールアドレスあてに送信されたらどうなるかな。

N さん：偽られた送信者メールアドレスあてに，NDR メールを送信します。送信者メールアドレスが正しいのか偽りなのかはメールサーバ 1 とメールサーバ 2 では判断できません。

M 主任：仮に，偽られた送信者メールアドレスが実在したらどうなるかな。

N さん：偽られた送信者メールアドレスあてに NDR メールが届きます。

M 主任：⑤そうした NDR メールが多いと，メールサーバ 1 がスパム発信源としてブラックリストに登録される可能性があり，対策が必要だね。

N さん：はい，分かりました。

以上を踏まえて，迷惑メールに関する対策を行った。技術 G において，再度，接続前 P テストを実施し，設定検査指摘事項がすべて解決されていることを確認した。

続いて，Web アプリケーション検査を実施した。

〔DMZ 接続及び DMZ 接続検査の実施〕

開発 G で現在の受注システムのサーバ群を一時的に新受注システムのサーバ群に切り替えた後，技術 G で接続後 P テストを実施した。検査の結果，問題が発見され，技術 G は接続検査指摘事項を図 7 のとおり通知した。

(1) DNS サーバについて
・オープンリゾルバについて
⑥図 1 中の接続点(α)から DNS サーバに対して，Y 社管理ドメイン名以外の名前解決を試みると，成功する場合があり，オープンリゾルバである可能性がある。DNS キャッシュポイズニング攻撃を防止するため，次の A 案，B 案のいずれかを実施すること。
A 案：サーバを追加し，コンテンツ機能とキャッシュ機能を異なるサーバに配置する。
B 案：DNS サーバは 1 台のままとし，名前解決問合せ通信のアクセス制御ルールを適切に修正する。

図 7　接続検査指摘事項

〔オープンリゾルバ対策に関する検討〕

開発 G は，まず，A 案を検討した。検討の結果，次の三つを行うことで，オープンリゾルバ対策を技術的に実現できることが分かった。

・DNS サーバにコンテンツ機能だけを割り当てる。

・DMZ にキャッシュ DNS サーバを導入し，キャッシュ機能だけを割り当てる。

・表 4 のとおり，表 1 中の項番 7 を修正する。

表 4　FW ルールの修正案

項番	送信元	あて先	サービス	動作
⋮	⋮	⋮	⋮	⋮
6	インターネット	DNS サーバ	DNS	許可
7	キャッシュ DNS サーバ	e	DNS	許可
8	インターネット	メールサーバ 1	SMTP	許可
⋮	⋮	⋮	⋮	⋮

しかし，キャッシュ DNS サーバの導入は，インフラ構築のための時間を必要とし，運用開始に間に合わない。

次に，B 案を検討した。今回，指摘があった現状の名前解決問合せ通信のアクセス制御ルールを表 5 に示す。

表5　現状の名前解決問合せ通信のアクセス制御ルール

項番	問合せ元	問合せ方法	問合せ対象ドメイン名	動作
1	すべて	非再帰的な問合せ	すべてのドメイン名	許可
2	DMZ	再帰的な問合せ	すべてのドメイン名	許可
3	すべて	再帰的な問合せ， 又は非再帰的な問合せ	すべてのドメイン名	拒否

注　上から順に，最初に一致したルールが適用される。

表5で動作が許可の場合は，表6に示すY社のDNSサーバの名前解決アルゴリズムを実行する。表5で動作が拒否の場合は，拒否を返答する。

表6　Y社のDNSサーバの名前解決アルゴリズム

問合せ方法 / 問合せ対象ドメイン名	再帰的な問合せ	非再帰的な問合せ
Y社管理ドメイン名	Y社管理ドメイン名に関する情報を問合せ元に返答する。解決できなかった場合は，ネームエラーを問合せ元に返答する。	左に同じ
キャッシュ領域に保持されているY社管理ドメイン名以外のドメイン名	キャッシュ領域に保持されているY社管理ドメイン名以外のドメイン名に関する情報を問合せ元に返答する。	左に同じ
キャッシュ領域に保持されていないY社管理ドメイン名以外のドメイン名	Y社以外のDNSサーバに問合せを行い，その結果を問合せ元に返答する。解決できなかった場合は，ネームエラーを問合せ元に返答する。結果は，キャッシュ領域に一定時間保持される。	解決できずに，問合せ元にネームエラーを返答する。

M主任とNさんが一緒に表5を見直したところ，表5には問題があり，実際に図1中の接続点(α)からDNSサーバに対してY社管理ドメイン名以外の名前解決を試みると，場合によっては成功することが判明した。更に検討を行い，表5のアクセス制御ルールを修正すればこの問題は解決できるというめどがついた。

開発Gにおいて，A案とB案との比較検討を行った結果，運用開始を延期しなくてもよいB案を採用することに決定した。Nさんは，表5の名前解決問合せ通信のアクセス制御ルールを表7のように修正し，技術Gは図1中の接続点(α)から，Y社管理ドメイン名以外の名前解決ができないことを確認した。

表7　修正した名前解決問合せ通信のアクセス制御ルール

項番	問合せ元	問合せ方法	問合せ対象ドメイン名	動作
1	すべて	非再帰的な問合せ	f	許可
2	g	非再帰的な問合せ	すべてのドメイン名	許可
3	DMZ	再帰的な問合せ	すべてのドメイン名	許可
4	すべて	再帰的な問合せ， 又は非再帰的な問合せ	すべてのドメイン名	拒否

注　上から順に，最初に一致したルールが適用される。

技術Gは接続検査指摘事項への対処結果に問題がないことを確認して，運用Gでの新受注システムの運用が開始された。

設問1　〔DMZに設置されるサーバへのSSH接続に関する検討〕について，(1)，(2)に答えよ。

(1) 初めてSSHサーバにSSH接続を行う際には，利用者はSSHサーバのフィンガプリントと呼ばれる情報を確認する必要がある。フィンガプリントから確認できることを30字以内で述べよ。

(2) 本文中の下線①について，表1中の項番12の定義内容のうち，送信元又はあて先を変更することになった。変更箇所は送信元又はあて先のいずれか。答案用紙の“送信元・あて先”のいずれかの文字を○印で囲んで示せ。また，その変更後の内容を40字以内で述べよ。

設問2　〔DNS機能に関する検討〕について，(1)～(3)に答えよ。

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

(2) Y社のDNSサーバがDNSキャッシュポイズニング攻撃を受けた場合，Y社のPCでのインターネットへのWebアクセスにおいて，どのような問題が発生するか。40字以内で述べよ。

(3) 本文中の下線②について，DNSキャッシュポイズニング攻撃を受けやすいDNSサーバの不適切な設定とはどのような設定であるか。25字以内で述べよ。

設問3　迷惑メール対策について，(1)～(4)に答えよ。

(1) 図5及び本文中の［c］に入れる適切な迷惑メール対策技術の名称を10字以内で答えよ。

(2) 本文中の下線③について，カタログ Web サーバのドメイン名に対して，SPF を設定した TXT レコードを解答群から一つ選び，記号で答えよ。

解答群

ア `catalog.y-sha.co.jp. IN TXT "v=spf1 +ip4:x1.y1.z1.2 -all"`

イ `catalog.y-sha.co.jp. IN TXT "v=spf1 +ip4:x1.y1.z1.4 -all"`

ウ `catalog.y-sha.co.jp. IN TXT "v=spf1 +ip4:x1.y1.z1.5 -all"`

エ `catalog.y-sha.co.jp. IN TXT "v=spf1 +ip4:x1.y1.z1.6 -all"`

オ `catalog.y-sha.co.jp. IN TXT "v=spf1 -all"`

(3) 本文中の下線④について，メールサーバ 1 ではインターネット側から届いたメールに対して，どのようなオープンリレー防止設定を実装しているか。図 6 中の［ d ］に入れる条件を表 3 中の字句を含めて 40 字以内で述べよ。

(4) 本文中の下線⑤について，対策を行わない状態で悪用されたとき，Y 社のメール送信において，受ける被害を 60 字以内で述べよ。

設問 4 オープンリゾルバ対策について，(1)～(3)に答えよ。

(1) 図 7 中の下線⑥について，どのような場合に成功するかを 50 字以内で述べよ。

(2) 表 4 中の［ e ］に入れる適切なあて先を，図 1 中の (a)～(d) の記号で答えよ。

(3) 表 7 中の［ f ］，［ g ］に入れる適切な字句を答えよ。