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。

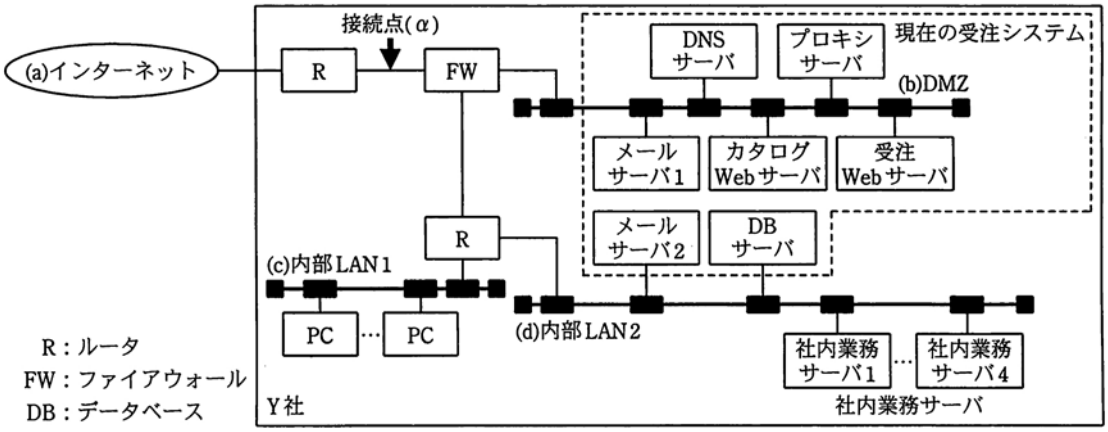

図1　Y社のネットワーク構成

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，DNSl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キャツ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.cojp 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

問合せ対象ドメイン名 ＼ 問合せ方法	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 5O 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。

問 2　情報セキュリテイインシデント対応に関する次の記述を読んで, 設問 l〜5 に答えよ。

X 社は，従業員数 300 名のソフトウェア開発会社である。X 社の主要な事業内容は，ソフトウェア製品の自社開発，Web アプリケーションの受託開発及びオープンソースソフトウェア（OSS）を利用したサーバとネットワークの構築サービスである。また，契約した顧客に対しては，ハードウェア及びソフトウェアの保守サポートも有償で提供しているが，顧客のシステムの運用は行っていない。

X 社の組織を図 1 に示す。

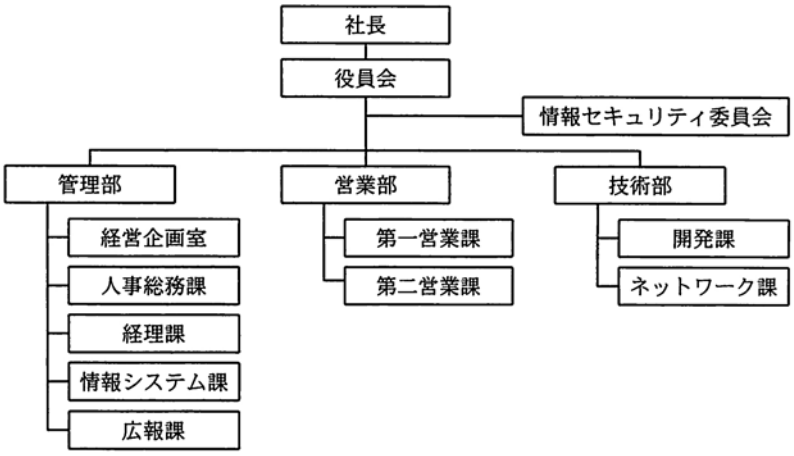

図 1　X 社の組織

X 社では，各部署の部長及び課長から構成される情報セキュリティ委員会と，その

委員会の事務局を担当している情報システム課が連携して，情報セキュリティポリシ（以下，ポリシという）の策定やセキュリティ対策の実施を行っている。

X 社では，社内の情報システム，ネットワークなどは自社で企画し，開発や構築を行っている。社内の情報システムは業務系システムと開発系システムの二つに分かれており，セキュリティ確保の観点からこの二つのシステムはネットワークを分け，それぞれ別の回線を通じてインターネットに接続されている。業務系システムの運用は情報システム課が行い，開発系システムの運用は開発課とネットワーク課が共同で行っている。

業務系ネットワークには各部署の LAN が接続され，全社共通のグループウェアサーバや営業管理サーバ，経理事務サーバなどの業務系サーバ群と接続できるようになっている。また，DMZ 上にメールサーバ，Web サーバ及び DNS サーバが設置され，インターネットに公開されている。

開発系システムは技術部のプロジェクト単位で開発環境が構築されており，その上でソフトウェアの開発や機器のテストなどを行っている。それぞれの開発環境からは OSS の技術情報収集やセキュリティパッチ取得のために，インターネットに対して HTTP や FTP でのアクセスが可能になっている。ただし，インターネットに対して公開しているサーバは開発系ネットワークにはない。

X 社のシステム構成を図 2 に示す。

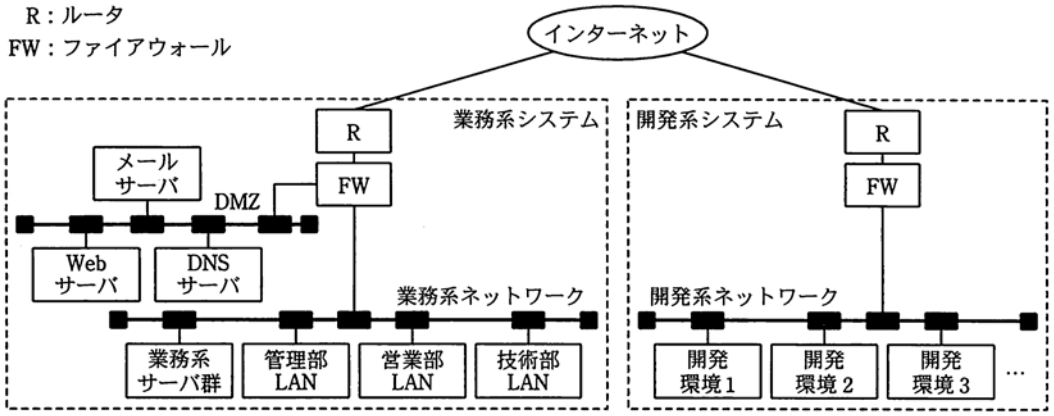

図２　X社のシステム構成

年度末を控えたある日，X 社の営業部員が外出した際に，顧客のシステムに関する重要な情報が保管されている業務用のノート PC を紛失するという情報セキュリティインシデント（以下，情報セキュリティインシデントをインシデントという）が発生した。

このインシデントへの X 社の対応は迅速とは言い難かった。ノート PC には指紋認証機能が備わっていたので，正当な利用者以外の者がハードディスクや OS にアクセスする可能性は低かったものの，連絡体制の不備から事実関係の把握に手間取り，顧客への連絡も遅れてしまった。数日後にノート PC は発見され，情報流出の可能性は極めて低いものと判断されたが，このインシデントによって X 社はインシデント対応の重要性を改めて認識した。このため，情報セキュリティ委員会は今回の反省を踏まえてインシデント対応についての取組みを強化することとし，事務局である情報システム課にインシデント対応計画を策定させることとした。

〔インシデント対応計画の策定〕

次は，情報システム課の S さんと T 課長の会話である。

S さん：当社ではこれまで，予防策を中心としたセキュリティ対策を進めてきましたが，今回のインシデントでそれだけでは不十分なことがよく分かりました。

T 課長：一つは，社内の連絡体制に問題があった。紛失者から直属の上司である第一営業課の課長にはすぐ連絡があったが，第一営業課ではその先の連絡先が分からなかったことに加えて，発生が金曜日の夕方だったこともあり，本来ならすぐに通知すべき情報システム課や情報セキュリティ委員会への連絡が遅れてしまった。連絡することはポリシに記載されているのだが，インシデント発生時の具体的な連絡先についての周知，教育が不足していたことは否めないね。

S さん：社内だけでなく，社外への連絡が遅れたことも反省しなければいけませんね。

T 課長：インシデントが発生したときの，関係者へ連絡を行う担当や手順が明確になっていなかったことも反省点だね。また，当社では個人情報を扱う業務はそれほど多くないので付与を受けていないが，JIPDEC などの機関から［ a ］の付与を受けた企業では，個人情報の漏えいが発生したときだけでなく，本人以外の個人情報を含むノート PC の紛失などの際にも，その機関に対して事故報告書を提出する必要があるようだ。

S さん：今回はノート PC の紛失でしたので警察にも遺失物届を出しましたが，Web サーバのコンテンツが改ざんされるなど，被害が発生した場合には，警察への連絡が必要になりますね。

T 課長：場合によっては発生したインシデントの内容を［ b ］/ClC（コーディネーションセンター）のような外部機関に報告する必要もありそうだ。そのような場合の手順も整備しないといけないね。

S さん：どれだけ予防策をとってもインシデントの発生をゼロにすることはできないので，<u>①インシデント対応の体制を事前に作っておくこと</u>が必|要ではないでしょうか。

T 課長：そうだね。これまでは情報システム課が業務系システムのインシデント発生に対応してきたが，情報システム課だけでは対応しきれないことも多い。全社横断的なインシデント対応チーム（以下，IRT という）を設置して，PC 紛失のような事例も含めて，インシデント対応に関する社内の体制と役割を明確にするのがよいだろうね。

S さん：システムに関するインシデントでは技術的なセキュリティ対策に関する知識やシステムの実装に関する情報が必要になります。技術的なセキュリティ対策については技術部の方が詳しいですし，こちらでは開発系システムについて詳しく把握できていないこともありますから，技術部と互いに協力して会社全体でのインシデント対応を進められるとよいですね。

このように情報システム課で議論した結果，社内に IRT を設置し，インシデントに対応していく計画を情報セキュリティ委員会へ提案することにした。情報システム課がまとめたインシデント対応計画の骨子を図 3 に示す。

(1) 本計画は，当社におけるインシデントへの対応を定めるものである。
(2) 当社は全社横断的に IRT を組織し，選任された従業員が IRT メンバを兼務する。
(3) IRT が対応を行うインシデントは，次のとおりとする。
  (a) 当社の所有する情報資産の紛失，改ざん，漏えいなどが疑われる場合
  (b) 当社の業務系システムに異常，不具合などが発生した場合
  (c) 当社の開発系システムに異常，不具合などが発生した場合
(4) IRT は，インシデント対応のために，社内の各部署及び社外の各機関との連携を図る。
(5) IRT は，インシデント対応マニュアルを整備する。
(6) IRT は，社内で発生したインシデントについての報告先となる。
(7) IRT は，インシデント検知のために，社内の情報システム及びネットワークのログなどにおける異常事象を分析する。
(8) IRT は，インシデント対応に必要な脆弱性情報やセキュリティパッチに関する情報（以下，セキュリティ情報という）を収集し，関連する社内の部署に情報提供を行う。
(9) IRT は，インシデントを検知した際の初期対応を実施する。
(10) IRT は，インシデント対応に必要な証拠の収集と保全，分析を行う。
(11) IRT は，従業員に対してインシデント対応に関する周知，教育を行う。

図３　X社におけるインシデント対応計画の骨子

この対応計画を情報セキュリティ委員会に提案したところ，②X 社の事業内容を踏まえると　図 3 で対象としたインシデント以外にも，IRT が対応すべきインシデントがあるのではないかとの意見があり，情報システム課は対応計画を修正した。その後，情報セキュリティ委員会での審議と役員会の承認を経て，社内のポリシが改定され，IRT が発足することとなった。これに伴って X 社は情報セキュリティに関して表 1 のように各組織で役割を分担することとした。

表１　情報セキュリティに関するＸ社の組織と役割分担

組織	役割
情報セキュリティ委員会	情報セキュリティ全体の継続的改善
IRT	発生したインシデントの報告の受付 業務系システムと開発系システムのログなどにおける異常事象の分析 インシデント発生時の初期対応と原因究明 セキュリティ情報の収集と提供
情報システム課	業務系システムの運用と監視，セキュリティ対策の実施
広報課	Web コンテンツの作成，更新 重大なインシデントが発生した際の対外広報
開発課	開発系システムの運用と監視，セキュリティ対策の実施 セキュリティを保ったソフトウェア開発 ソフトウェア製品の保守サポート ソフトウェア製品のセキュリティパッチ作成
ネットワーク課	開発系システムの運用と監視，セキュリティ対策の実施 セキュリティを保ったネットワーク構築 ハードウェア機器の保守サポート

〔IRT メンバ向けのインシデント対応マニュアルの整備〕

新たに発足した IRT には，情報システム課の T 課長と S さんのほか，社内の各部署からメンバが選出され，T 課長がチームリーダを務めることとなった。IRT では，イ

ンシデント対応を円滑に行うためにIRTメンバ向けのインシデント対応マニュアルを作成することとし，その具体的な内容として図4に示す各項目を検討した。

(1) インシデント対応に必要なリソース（機器や情報など）の整備
(2) ログ管理
(3) ログなどにおける異常事象の分析
(4) インシデント発生時の初期対応と作業の記録
(5) インシデントの証拠収集
(6) 収集した証拠の分析と原因の究明，システムの復旧方法
(7) 社内外の連絡方法と最新のセキュリティ情報の収集

図4　IRTメンバ向けのインシデント対応マニュアルに記載する内容

図4中の(1)に関し，必要な機器については，予算面の問題もあることから，優先度の高いものから順に整備を進めていくことになった。また，業務系システムと開発系システムの構成情報は情報システム課と開発課，ネットワーク課が個別に管理していたが，既存のグループウェアを利用してIRTメンバが双方のシステムの構成情報を閲覧できるようにした。

図4中の(2)については，まず，現状を把握するために，現在の業務系と開発系のシステムで取得しているログの情報を収集し，リストアップすることにした。その結果，取得しているログの管理が機器ごとにそれぞれ異なることが判明した。このままでは，インシデントの原因究明に必要な情報を安全に確保及び保全することが困難なことから，IRTでは今年度中に③ログ管理のポリシを策定することとした。来年度以降には各機器のログのバックアップと統合管理を行うシステムの導入を検討する予定である。

図4中の(3)については，情報システム課と共同でシグネチャベースのIPS(侵入防止システム)をDMZに導入し，攻撃を受ける可能性が高いDMZ上のサーバへの脅威を分析することとした。開発系システムにもIPSの導入を検討したが，予算が厳しいことと，インターネットに対して公開しているサーバがないことから今年度の導入は見送った。ただし，開発系システムのFWのログについては定期的な分析を行うことにした。

図4中の(4)については，インシデント発生の報告を受けた後の対応について検討した。 PCの紛失やサーバへの攻撃など，インシデントのタイプを何種類か想定し，そのタイプごとにインシデント原因の究明，被害の拡大防止及び仮復旧の方法をマニュアル化することにした。また，作業記録のフォーマットを整備し，個々のインシデント対応に当たってどのような作業を実施したかを記録することにした。

図4中の(5)は，いわゆるコンピュータフォレンジクスの技法についての検討である。インシデント発生時の被害の内容及び範囲の確認並びに発生原因の調査のために必要な情報を確実に保全し，発生した事象を様々な要素から解明することが目的である。 IRTでは，ネットワークのインシデントに関する情報はIPS及びFWでの監視並びにログの取得を行うことで保全することとした。また，コンピュータに接続された記憶媒体上の情報は専用の機器を導入して保全できるようにした。保全された情報は，IRTが分析を行うことにした。

図4中の(6)については，コンピュータフォレンジクスで利用する機器やソフトウェアのベンダや，セキュリティ団体が主催するセミナにIRTメンバが出席するなどして，具体的な技法の習得と(6)の手順化に努めることにした。

図 4 中の(7)については，インシデント発生時の社内の連絡網及び外部の連絡先を整理し，関連部署への周知を図った。また，外部からのセキュリティ情報の収集の際に IRT では，インシデント対応のコミュニティにおいて広く利用されている実績がある④PGP を利用した電子署名を採用することにした。

このような検討を経て，IRT メンバ向けのインシデント対応マニュアルが完成し，X 社のインシデント対応が本格的に始動することになった。

〔IPS の運用〕

情報システム課はネットワーク課の協力を得て DMZ に IPS を導入した。この IPS ではネットワークの脅威を検知して不正な通信を遮断することができる。また，脅威の検知時刻，通信パケットの送信元及びあて先それぞれの IP アドレス及びポート番号，検知した脅威の種類を示すシグネチャの識別番号(ID)，脅威の名称，詳細な通信の内容などの情報をログに記録できる。IPS の管理端末からはこのログを閲覧できるほか，脅威についての解説も閲覧できる。さらに，脅威の検知状況を日次，週次及び月次でレポート化することができる。

なお，IPS のシグネチャは，定期的に最新の状態に更新することとした。

シグネチャによって検知される個々の脅威の危険度はベンダによって 4 段階のレベルに分類されており，レベル 4 が最も危険度が高く，レベル 1 が最も危険度が低い。ただし，利用者側で個々のシグネチャの設定を変更して危険度のレベルを変えることが可能であり，利用者側で設定した脅威の危険度はシグネチャが更新されても維持される。

シグネチャの設定は既定値のままとし，レベル 4 又はレベル 3 の脅威が検知されたときには IRT メンバに対して警告メールが送信される設定を行った上で試験運用を開始したところ，最初の 1 時間のうちに大量の警告メールが IRT メンバに送信された。このため，T 課長はネットワーク課の IRT メンバである U 君に協力を求め，一緒に対応に当たることにした。T 課長が IPS の管理端末から 1 時間の脅威の検知件数を確認したところ，表 2 のような結果が得られた。

表 2　IPS で検知した脅威の集計

ID(注1)	危険度のレベル	脅威の名称	件数
1040	4	TCP SYN/FIN Packet	135
1042	4	TCP NULL Packet	123
5021	4	Password File Access Attempt	14
5829	3	HTTP Tunneling	2

注(1)　脅威の種類を示す IPS のシグネチャの識別番号

次は，T 課長と U 君の会話である。

T 課長：とりあえずこの集計を見てくれるかな。どう思うかね。‘
U 君　：警告が出た脅威は IPS で遮断しているので，特に問題はないと思いますが，警告メールが多すぎるのは困りますね。調べてみましょう。

U 君は IPS の管理端末でログを確認し，検知した脅威に関する解説を表示させた。

U 君　：ID が 1040 番と 1042 番の脅威は，Web サーバとメールサーバの IP アドレス

に対する特殊なポートスキャンのようですね。1040 番の脅威は，TCP のコネクションを開始する際に SYN/FIN プラグが付加されていたものです。 1042 番の方は，どのフラグも付加されていなかったものです。

T 課長：通常のポートスキャンとはどう違うのかな。

U 君　：この方法では TCP のコネクションが正常に確立しないので，対象となったホスト上で [c] されにくいという特徴があります。こうした特徴から，ステルススキャンなどと呼ばれることもあるようです。しかし，この脅威も IPS で遮断されていますし，DoS 攻撃が成立するほど大量に発生しているわけでもありませんので，システムへの影響はないと思います。

T 課長：次に進もうか。 5021 番の脅威では，図 5 のようなアクセスがたくさんあるようだが，これは当社の Web サーバには影響はないと考えていいね。

```
GET /cgi-bin/enquete.cgi
view=../../../../../../../../../../../../../../../../../../../../etc/passwd HTTP/1.1
```

図 5　5021 番の脅威と判定したパケットに含まれていた文字列

U 君　：はい。これは，広く使われている CGI プログラムに対する無差別攻撃のようですね。この CGI プログラムは当社では利用していないはずですが，念のため，後で Web サーバの設定とアクセスログを確認してみます。パケットに含まれる文字列からすると，CGI プログラムに含まれる [d] の脆弱性を利用して，パスワードファイルを取得することをねらったもののようです。

T 課長：5829 番の脅威では図 6 のようなアクセスが発生しているが，これはどうだろう。 Web サーバを悪用する攻撃のようだが。

```
[ e ] mail.example.com:25 HTTP/1.1
```

図 6　5829 番の脅威と判定したパケットに含まれていた文字列

U 君　：設定に問題のある Web サーバを悪用して，外部のメールサーバと SMTP で通信させようとしたようですね。

T 課長：Web サーバなのに SMTP で通信しようとしているというのはちょっと変じゃないかな。

U 君　：図 6 を見ると，HTTP/1.1 で定義されている [e] というメソッドが利用されています。これは Web サーバがいわゆるプロキシサーバとして動作しているときに，TCP の通信を透過的に中継させる目的で利用されるものです。主に SSL を中継させるのに使うことが多いのですが，SMTP のようなプロトコルも中継させることができます。

T 課長：なるほど。この脅威についてはどのように対処しているのかな。

U 君　：IPS で遮断していますが，当社では Web サーバをプロキシサーバとして利用しないので，⑤Web サーバではこのメソッドを受け付けない設定になっていますから，仮に IPS で遮断しなくても問題は発生しません。

T 課長：今日の警告メールについては，システムへの問題はないということだね。それにしても，警告メールが大量に来るのはちょっと困るな。⑥一定の条件を満

たす場合には警告メールを送らないよう，シグネチャの設定を調整して危険度のレベルを変えるのがよいだろうね。

U 君　：そうですね。シグネチャの設定を調整し，対応マニュアルも書き換えます。

U 君がシグネチャの設定を調整したところ，IRT メンバに大量の警告メールが来ることはなくなった。

〔インシデントの発生と対応〕

その後，大きな問題もなく数か月が経過したある日，U 君が開発系システムの FW のログを分析したところ，開発系システムの特定の IP アドレスからインターネット上の幾つかの IP アドレスに対して，通常見られない大量の通信が行われていることに気が付いた。

開発系システムの構成情報で送信元の IP アドレスを確認したところ，送信元の IP アドレスに該当する機器が記載されていなかったので，U 君は開発課に問い合わせた。担当者の話によると，この機器は，近々顧客に納入する Web コンテンツの動作検証を行うため，開発課が一時的に開発環境に接続したサーバ機であるとのことだった。

U 君が更にログを確認したところ，通信の内容に不審なところが見られたことから，U 君は T 課長に連絡し，インシデント対応マニュアルに従って初期対応に取り掛かった。

U 君が証拠収集に必要な機材を持参して開発課に駆けつけたところ，当該サーバ機は U 君が電話で問い合わせた直後に担当者がシャットダウンし，電源が切断された後だった。このため、⑦U 君はこのサーバ機の電源を再投入せず、サーバ機からハードディスクを取り出した。取り出したハードディスクの内容は，専用の複製装置を用いて別のハードディスクに全セクタを複製し，⑧この複製に対してフォレンジックツールを実行して解析を行った。

解析の結果，サーバ機が最近流行しているボットに感染し，インターネットと通信を行っていた形跡が認められた。開発課によると，サーバ機を開発系ネットワークに接続する前に行うべき OS のパッチ適用を怠っていたとのことであった。情報を最終的に総合すると，パッチ未適用で OS の脆弱性が放置されたまま，フリーのソフトウェアの配布先にアクセスし，その際に脆弱性を悪用するポットに感染したため，インターネットと通信を行っていたものと推測された。

IRT はこうした解析結果を開発課に伝え，ボットに感染したサーバ機を再感染しないように再構築するよう指示した。開発課は IRT の指示に従ってハードディスクを初期化した上で OS を再インストールし，最新のパッチをすべて適用した上でサーバ機を再構築した。納期が迫る中ではあったが，再構築したサーバの動作検証は順調に進み，開発課は無事に顧客への納品を済ませることができた。

〔インシデントからの反省〕

今回のボット感染のインシデント対応が一段落した後で，IRT はメンバ全員を集めて反省会を行った。その席で，IRT での対応に関する反省に加え，⑨従業員に対する周知，教育が不足していたために対応に問題が生じたのではないかとの意見があった。そこで，IRT は，全従業員向けのインシデント対応マニュアルを作成してインシデント対応に関する周知，教育を図るという改善計画を，情報セキュリティ委員会に提出した。

IRT は改善計画に従ってインシデント対応マニュアルを作成するとともに，全従業員

への周知，教育を行い，社内でのインシデント対応への取組みを強化することができた。

設問 1　〔インシデント対応計画の策定〕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，それぞれ 10 字以内で答えよ。

(2)本文中の下線①について，“事前に作っておくこどのメリットを，インシデントの原因究明の観点から，35 字以内で述べよ。

(3)本文中の下線②について，X 社では更にどのようなインシデントを対象として追加すべきか。35 字以内で述べよ。

設問 2　〔IRT メンバ向けのインシデント対応マニュアルの整備〕について，(1)，(2)に答えよ。

(1)本文中の下線③について，ログ管理のポリシに盛り込むべき具体的な内容を，25 字以内で述べよ。

(2)本文中の下線④について，IRT では PGP を利用した電子署名を主にどのようなことを確認する目的で採用したと考えられるか。IRT の業務に即して 35 字以内で述べよ。

設問 3　〔IPS の運用〕について，(1)～(3)に答えよ。

(1)本文中の［ c ］～［ e ］に入れる適切な字句を，それぞれ 15 字以内で答えよ。

(2)本文中の下線⑤について，IPS が設置されておらず，かつ Web サーバでこのメソッドが受け付けられる設定になっている状態で図 6 の脅威が発生した場合には，Web サーバでどのような問題が発生する可能性が高いと考えられるか。30 字以内で述べよ。

(3)本文中の下線⑥について，T 課長がシグネチャの設定を調整するように求めたセキュリティ上の理由を 40 字以内で述べよ。また，ある特定の脅威について危険度のレベルを既定値から下げることを許容する場合の条件を 35 字以内で述べよ。

設問 4　〔インシデントの発生と対応〕について，(1)，(2) に答えよ。

(1) 本文中の下線⑦について，U 君が電源を再投入しなかった理由を 40 字以内で述べよ。

(2) 本文中の下線⑧について，U 君が取り出したハードディスクを直接用いて解析を行わなかった理由を 35 字以内で述べよ。

設問 5　〔インシデントからの反省〕について，本文中の下線⑨の，周知，教育が不足していたために，ボット感染のインシデント対応において露呈したと考えられる問題を二つ挙げ，それぞれ 35 字以内で述べよ。また，それらの問題への対応として，全従業員向けインシデント対応マニュアルに記載すべき具体的な内容をそれぞれ 35 字以内で述べよ。

解答例

問 1

出題趣旨

インターネットに公開されているサーバは，セキュリティ侵害の脅威にさらされている。サーバの導入時や更新時に脅威への対応が行われていることを確認するため，セキュリティ検査の実施が望まれる。

本問では，システムの更新時に実施するセキュリティ検査を題材にして，ファイアウォール，SSH サーバ，DNS サーバ及びメールサーバに関する知識と設計能力について問う。

設問 1　(1) SSH サーバの公開鍵が正しく，なりすましがないこと

(2) 更新箇所　送信元，あて先

変更後の内容　契約通信サービスにおいて割り当てられる Y 社専用の IP アドレス

設問 2　(1) a　DNssEc

b　ディジタル署名

(2) アクセスしたい web サーバとは別のサーバにアクセスしてしまう。

(3) 送信元ポート番号を固定する設定

設問 3　(1) c　送信ドメイン認証

(2) オ

(3) d　受信者メールアドレスのドメイン名が y-sha.co.jp

(4) メールサーバ 1 から送信される正常なメールが，ブラックリストを利用しているメールサーバで受信拒否される。

設問 4　(1) 非再帰的な問合せで，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名前解決を行った場合

(2) e　(a)

(3) f　Y 社管理ドメイン名

g　DMz

問 2

出題趣旨

これまでの情報セキュリティ対策では，予防策を中心とする事前の対策が重視されてきた。　しかし，近年になってインシデント発生後の対応が適切か否かが組織の信頼や評判にも影響を及ぼすことが認識されるようになり，“事故前提社会”の観点からもインシデント対応に対する注目が高まりつつある。

本問では，ソフトウェア開発会社におけるインシデント対応体制の構築を題材として，インシデント対応についての理解や，インシデント対応に関連する種々の技術要素についての理解を問う。

設問 1　(1)　a　プライバシーマーク

b　JPCERT

(2) 原因究明に必要な情報の収集に迅速かつ組織的に着手できること

(3) 出荷後の自社開発のソフトウェア製品に関するインシデント

設問 2　(1) 取得するログの種類や保管方法，保管期間

(2) セキュリティに関する情報やソフトウェアの提供元の真正性

設問 3 (1) c アクセスがログに記録
d ディレクトリトラバーサル
e CONNECT
(2) Web サーバがメールの不正中継に利用されるという問題
(3) **理由** 対応が不要な警告メールが多いと対応が必要な警告メールを見落とすから
条件 DMZ では利用していないシステムや機能に関する警告メールであること

設問 4 (1) 再起動することでサーバ機上のファイルが改変される可能性があるから
(2) 解析の際に原本のデータを書き換えてしまう可能性があるから

設問 5 ① **問題** 開発系システムの構成情報が最新に保たれていなかったこと
記載内容 一時的な変更の際も，開発系システムの構成情報を常に最新に保つ。
② **問題** 開発課の担当者が勝手にサーバ機をシャットダウンしたこと
記載内容 インシデント発生時の機器の操作は IRT の指示に従って行う。

採点講評

問 1

問 1 では，インターネットに公開されているサーバの導入における SSH サーバ，DNS サーバ及びメールサーバの情報セキュリティ対策について出題した。全体として正答率は想定どおりだった。

設問 1(1)は，正答率が低かった。初めて SSH サーバに SSH 接続を行う際の，公開鍵の真正性を確認することの重要性について，よく理解しておいてほしい。

設問 2(2)は，正答率が高かったが，(1)及び(3)は，正答率が低かった。 DNS キヤッシュポイズニング攻撃についての理解は高いが，DNS サーバの設定に関する知識がまだ不十分であるための結果と思われる。 DNS サーバには，DNS プロトコルの性質から様々な脆弱性が指摘されており，設定には細心の注意が必要であることを理解してほしい。

設問 3(2)は，選択肢形式であるにもかかわらず正答率が低かった。問題中の記述と図表をよく読めば正答を導けるはずである。インターネットに公開されているメールサーバでの迷惑メール対策についてよく理解しておいてほしい。

問 2

問 2 では，ソフトウェア開発会社における情報セキュリティインシデント対応について出題した。全体として正答率は想定どおりだった。

設問 1 (1) b は，正答率が低かった。 JPCERT/CC はインシデント対応に関する様々な活動を行っており，有用な情報を Web サイト上で提供しているので，是非，目を通しておいてほしい。

設問 3(1) d 及び e は，正答率が低かった。d では“バッファオーバフロー”，e では“POST”や“PUT”といった解答が目立った。 Web に関する脆弱性は多岐にわたるが，代表的なものについては，用語を覚えるだけではなく，その内容を掘り下げて理解しておいてほしい。

設問 5 では，インシデントが発生した原因だけに着目した解答が見られた。パッチの適用や，フリーのソフトウェアのダウンロードの禁止などのセキュリティ対策は，インシデ

ント予防の面から極めて重要であることは言うまでもない。　しかし，今回のインシデントの原因をそれらの対策によって除去できたとしても，それだけでは不十分である。全く異なる原因によってインシデントが発生する場合や，いわゆるゼロデイ攻撃など，既知の予防策のないインシデントが発生することも想定しておく必要がある。そうしたインシデントに対しても適切に対応できるよう，原因究明のための情報確保が重要であることに気づいてほしかった。