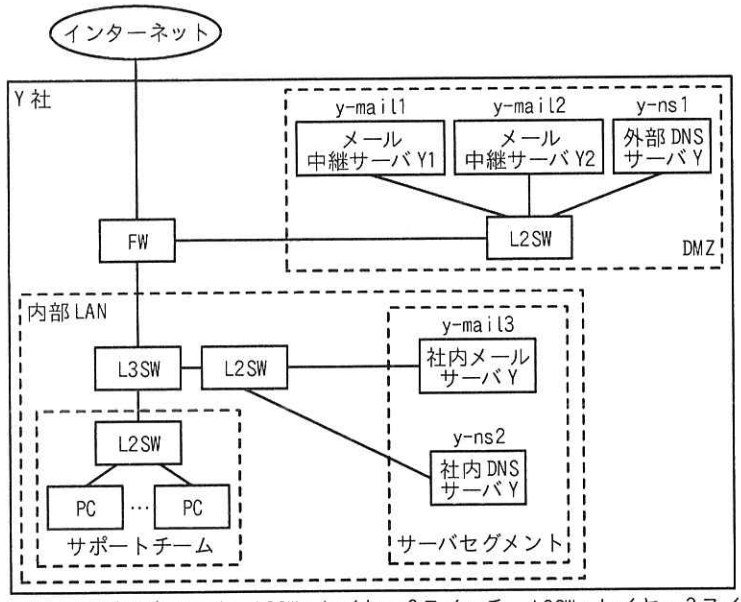
問2　電子メールを用いた製品サポートに関する次の記述を読んで，設問に答えよ。

Y 社は，企業向けに IT 製品を販売する会社であり，電子メール（以下，メールという）を使用して，販売した製品のサポートを行っている。Y 社では，取扱製品の増加に伴って，サポート体制の強化が必要になってきた。そこで，サポート業務の一部を，サポートサービス専門会社の Z 社に委託することを決定し，Y 社の情報システム部の X 主任が，委託時のメールの運用方法を検討することになった。

Y 社のネットワーク構成を図 1 に，外部 DNS サーバ Y が管理するゾーン情報を図 2 に，社内 DNS サーバ Y が管理するゾーン情報を図 3 に示す。



FW：ファイアウォール　L2SW：レイヤー2スイッチ　L3SW：レイヤー3スイッチ

注記　y-ns1，y-ns2，y-mail1，y-mail2，及び y-mail3 はホスト名である。

図 1　Y 社のネットワーク構成（抜粋）

$TTL　172800				
y-sha.com.	IN	MX	20	y-mail1.y-sha.com.
y-sha.com.	IN	MX	1	y-mail2.y-sha.com.
y-mail1.y-sha.com.	IN	A		200.a.b.1
y-mail2.y-sha.com.	IN	A		200.a.b.2

注記　200.a.b.1 及び 200.a.b.2 はグローバル IP アドレスである。

図 2　外部 DNS サーバ Y が管理するゾーン情報（抜粋）

```
$TTL    172800
y-mail3.y-sha.lan.              IN      A       192.168.1.1
mail.y-sha.lan.         60      IN      A       192.168.0.1
mail.y-sha.lan.         60      IN      A       192.168.0.2
y-mail1.y-sha.lan.              IN      A       192.168.0.1
y-mail2.y-sha.lan.              IN      A       192.168.0.2
```

図3　社内DNSサーバYが管理するゾーン情報（抜粋）

Y社では，サポート契約を締結した顧客企業の担当者（以下，顧客という）からの製品サポート依頼を，社内メールサーバYに設定された問合せ窓口のメールアドレスである，support@y-sha.com で受け付けている。このメールアドレスはグループアドレスであり，support@y-sha.com 宛てのメールは，Y社のサポート担当者のメールアドレスに配信される。サポート担当者は，送信元メールアドレスが support@y-sha.com にセットされた製品サポートのメール（以下，サポートメールという）を，社内メールサーバYを使用して顧客に返信している。

〔Y社のネットワーク構成とセキュリティ対策の背景〕

Y社のネットワーク構成とメールのなりすまし防止などの情報セキュリティ対策の背景について次に示す。

・サポート担当者が送信したサポートメールが①社内メールサーバYからメール中継サーバに転送されるとき，②DNSラウンドロビンによってメール中継サーバY1又はY2に振り分けられる。

・転送先のメール中継サーバが障害などで応答しないとき，社内メールサーバYは，他方のメール中継サーバ宛てに転送する機能をもつ。

・顧客が送信したサポートメールがメール中継サーバに転送されるときは，外部DNSサーバYに登録されたMXレコードの［　a　］値によって，平常時は，ホスト名が［　b　］のメール中継サーバが選択される。

・FWには，インターネットからDMZのサーバ宛ての通信に対して，静的NATが設定されている。

FW に設定されている静的 NAT を表 1 に示す。

表 1　FW に設定されている静的 NAT（抜粋）

宛先のホスト	宛先 IP アドレス	変換後の IP アドレス
y-mail1.y-sha.com	ア	イ
y-mail2.y-sha.com	省略	省略

送信元メールアドレスの詐称の有無に対しては，DNS の［　c　］と呼ばれる名前解決によって，送信元メールサーバの IP アドレスからメールサーバの FQDN を取得し，その FQDN と送信元メールアドレスのドメイン名が一致した場合，詐称されていないと判定する検査方法が考えられる。しかし，③攻撃者は，自身が管理する DNS サーバの PTR レコードに不正な情報を登録することができるので，ドメイン名が一致しても詐称されているおそれがあることから，検査方法としては不十分である。このような背景から，受信側のメールサーバが送信元メールアドレスの詐称の有無を正しく判定できるようにする手法として，送信ドメイン認証が生まれた。

送信ドメイン認証の技術には，送信元 IP アドレスを基に，正規のサーバから送られたかどうかを検証する SPF（Sender Policy Framework）や，送られたメールのヘッダーに挿入された電子署名の真正性を検証する DKIM（DomainKeys Identified Mail）などがある。Y 社では SPF 及び DKIM の両方を導入している。

〔Y 社が導入している SPF の概要〕

SPF では，送信者のなりすましの有無を受信者が検証できるようにするために，送信者のドメインのゾーン情報を管理する権威 DNS サーバに，SPF で利用する情報(以下，SPF レコードという)を登録する。Y 社では，外部 DNS サーバ Y に SPF レコードを TXT レコードとして登録している。

Y 社が登録している SPF レコードを図 4 に示す。

```
y-sha.com.    IN    TXT    "v=spf1 +ip4: [　ウ　] +ip4: [　エ　] -all "
```

図 4　Y 社が登録している SPF レコード

Y社が導入しているSPFによる送信ドメイン認証の流れを次に示す。

(i) サポート担当者は，送信元メールアドレスがsupport@y-sha.comにセットされたサポートメールを，顧客宛てに送信する。

(ii) サポートメールは，社内メールサーバYからメール中継サーバY1又はY2を経由して，顧客のメールサーバに転送される。

(iii) 顧客のメールサーバは，メール中継サーバY1又はY2から，メール転送プロトコルである［ d ］の［ e ］コマンドで指定されたメールアドレスのドメイン名の［ f ］を入手する。顧客のメールサーバは，DNSを利用して，［ f ］ドメインのゾーン情報を管理する外部DNSサーバYに登録されているSPFレコードを取得する。

(iv) 顧客のメールサーバは，④取得したSPFレコードに登録された情報を基に，送信元のメールサーバの正当性を検査する。

(v) 正当なメールサーバから送信されたメールなので，なりすましメールではないと判断してメールを受信する。なお，正当でないメールサーバから送信されたメールは，なりすましメールと判断して，受信したメールの隔離又は廃棄などを行う。

〔Y社が導入しているDKIMの概要〕

DKIMは，送信側のメールサーバでメールに電子署名を付与し，受信側のメールサーバで電子署名の真正性を検証することで，送信者のドメイン認証を行う。電子署名のデータは，メールの［ g ］及び本文を基に生成される。

DKIMでは，送信者のドメインのゾーン情報を管理する権威DNSサーバを利用して，電子署名の真正性の検証に使用する鍵を公開する。鍵長は，2,048ビットより大きな鍵を利用することも可能である。しかし，DNSをトランスポートプロトコルである［ h ］で利用する場合は，DNSメッセージの最大長が［ i ］バイトという制限があるので，［ i ］バイトに収まる鍵長として，一般に2,048ビットの鍵が利用される。

DKIMの電子署名には，第三者認証局（以下，CAという）が発行した電子証明書を利用せずに，各サイトの管理者が生成する鍵が利用できる。

Y社では，Y社のネットワーク運用管理者が生成した鍵などのDKIMで利用する情報

（以下，DKIM レコードという）を，外部 DNS サーバ Y に TXT レコードとして登録している。

Y 社が登録している DKIM レコードを図 5 に，DKIM レコード中のタグの説明を表 2 に示す。

```
sel.ysha._domainkey.y-sha.com.    IN    TXT    "v=DKIM1; k=rsa; t=s; p=（省略）"
```

注記　sel.ysha は，y-sha.com で運用するセレクター名を示し，y-sha.com.は，電子署名を行うドメイン名を示す。

図 5　Y 社が登録している DKIM レコード

表 2　DKIM レコード中のタグの説明（抜粋）

タグ	説明
v	バージョン番号を示す。指定する場合は“DKIM1”とする。
k	電子署名の作成の際に利用する鍵の形式を指定する。
t	DKIM の運用状態が本番運用モードの場合は“s”を指定する。
p	Base64 でエンコードした［　オ　］のデータを指定する。

DKIM における送信側は，電子署名データなどを登録した DKIM-Signature ヘッダーを作成して送信するメールに付加する処理（以下，DKIM 処理という）を行う。DKIM では，一つのドメイン中に複数のセレクターを設定することができ，セレクターごとに異なる鍵が使用できる。セレクターは，DNS サーバに登録された DKIM レコードを識別するためのキーとして利用される。

DKIM-Signature ヘッダー中のタグの説明を表 3 に示す。ここで，DKIM-Signature ヘッダーの構成図は省略する。

表 3　DKIM-Signature ヘッダー中のタグの説明（抜粋）

タグ	説明
b	Base64 でエンコードした電子署名データ
d	電子署名を行ったドメイン名
s	複数の DKIM レコードの中から鍵を取得する際に，検索キーとして利用するセレクター名

Y 社は，顧客宛てのサポートメールに対する DKIM 処理を，メール中継サーバ Y1 及

び Y2 で行っている。Y 社では，ドメイン名が y-sha.com でセレクター名が sel.ysha のセレクターを設定している。Y 社が送信するメールの DKIM-Signature ヘッダー中の s タグには，図 5 中に示したセレクター名の sel.ysha が登録されている。

Y 社が導入している DKIM による送信ドメイン認証の流れを次に示す。

（ｉ） サポート担当者は，送信元メールアドレスが support@y-sha.com にセットされたサポートメールを，顧客宛てに送信する。

（ii） サポートメールは，社内メールサーバ Y からメール中継サーバ Y1 又は Y2 を経由して，顧客のメールサーバに転送される。

（iii） メール中継サーバ Y1 又は Y2 は，サポートメールに付加する DKIM-Signature ヘッダー中に電子署名データなどを登録して，顧客のメールサーバに転送する。

（iv） 顧客のメールサーバは，DKIM-Signature ヘッダー中の d タグに登録されたドメイン名である y-sha.com と s タグに登録されたセレクター名を基に，DNS を利用して，当該ドメインのゾーン情報を管理する外部 DNS サーバ Y に登録されている DKIM レコードを取得する。

（v） 顧客のメールサーバは，⑤取得した DKIM レコードに登録された情報を基に，電子署名の真正性を検査する。

（vi） 正当なメールサーバから送信されたメールなので，なりすましメールではないと判断してメールを受信する。なお，正当でないメールサーバから送信されたメールは，なりすましメールと判断して，受信したメールの隔離又は廃棄などを行う。

〔Z 社に委託するメールの運用方法の検討〕

まず，X 主任は，自社のメールシステムのセキュリティ運用規程に，次の規定があることを確認した。

（あ） 社内メールサーバ Y には，Y 社に勤務する従業員以外のメールボックスは設定しないこと

（い） 社内の PC によるメール送受信は，社内メールサーバ Y を介して行うこと

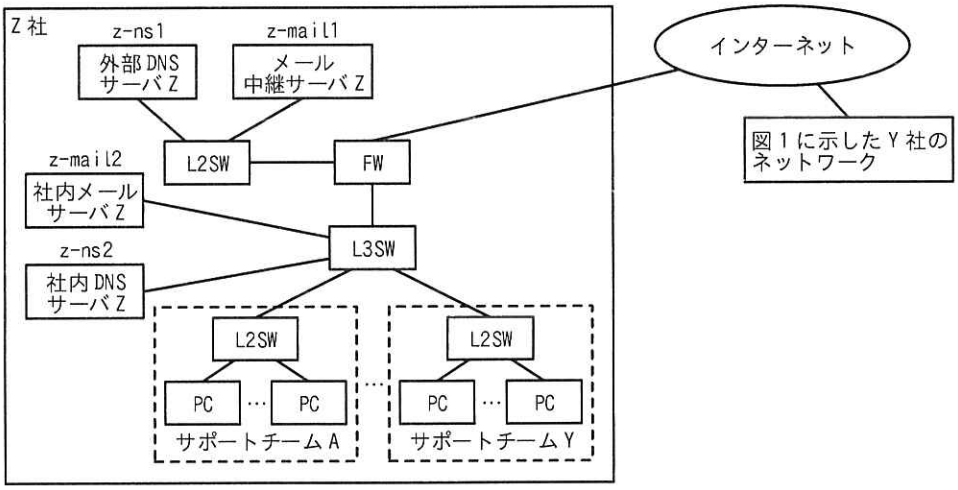
（う） メール中継サーバ Y1 及び Y2 にはメールボックスは設定せず，社内メールサーバ Y から社外宛て，及び社外から社内メールサーバ Y 宛てのメールだけを中継す

ること

（え） Y 社のドメインを利用するメールには，なりすまし防止などの情報セキュリティ対策を講じること

次に，メールの運用方法の検討に当たって，X 主任は，Z 社のネットワーク構成とサポート体制を調査した。

Z 社のネットワーク構成を図 6 に，外部 DNS サーバ Z が管理するゾーン情報を図 7 に示す。



注記 1　z-ns1，z-ns2，z-mail1 及び z-mail2 はホスト名である。
注記 2　サポートチーム A は，A 社向けのサポート業務を行い，サポートチーム Y は，Y 社向けのサポート業務を行うチームである。

図 6　Z 社のネットワーク構成（抜粋）

z-sha.co.jp.	IN	MX	10	z-mail1.z-sha.co.jp.
z-mail1.z-sha.co.jp.	IN	A		222.c.d.1

注記　222.c.d.1 はグローバル IP アドレスである。

図 7　外部 DNS サーバ Z が管理するゾーン情報（抜粋）

Z 社は，複数の企業から受託したメールを用いたサポート業務を，チームを編成して対応している。

X 主任は，Z 社のネットワーク構成，サポート体制及び Y 社のメールシステムのセキュリティ運用規程を基に，Z 社に委託するメールによるサポート方法を，次のようにまとめた。

・Z 社のサポートチーム Y のサポート担当者は，現在使用している問合せ窓口のメールアドレス support@y-sha.com でサポート業務を行う。
・support@y-sha.com 宛てのメール中から，Z 社に委託した製品のサポート依頼メール及びサポート途中のメールが抽出されて，Z 社のサポートチーム Y のグループアドレス宛てに転送されるようにする。
・サポートチーム Y のサポート担当者は，送信元メールアドレスが support@y-sha.com にセットされたサポートメールを，社内メールサーバ Z を使用して Y 社の顧客宛てに送信する。

次に，セキュリティ運用規程の(え)に対応するために，Z 社に委託するサポートメールへの SPF と DKIM の導入方法を検討した。

SPF には，⑥ DNS サーバに SPF で利用する情報を登録することで対応できると考えた。

DKIM には，図 6 中のメール中継サーバ Z で，送信元メールアドレスが support@y-sha.com のメールに対して DKIM 処理を行うことで対応できると考えた。このとき，顧客のメールサーバが，外部 DNS サーバ Y を使用して DKIM の検査を行うことができるように，DKIM-Signature ヘッダー中の d タグで指定するドメイン名には［ j ］を登録し，⑦ s タグで指定するセレクター名は sel.zsha として，Y 社と異なる鍵を電子署名に利用できるようにする。また，外部 DNS サーバ Y に，sel.zsha セレクター用の DKIM レコードを追加登録する。

委託時のメールの運用方法がまとまったので，検討結果を上司の W 課長に説明したところ，⑧ “Z 社のサポートチーム Y 以外の部署の従業員が，送信元メールアドレスに support@y-sha.com をセットしてサポート担当者になりすました場合，顧客のメールサーバでは，なりすましを検知できない”，との指摘を受けた。そこで，X 主任は，追加で実施する対策について調査した結果，S/MIME（Secure/MIME）の導入が有効であることが分かった。

〔S/MIME の調査と実施策〕

S/MIME では，受信者の MUA（Mail User Agent）によるメールに付与された電子署名の真正性の検証で，なりすましやメール内容の改ざんが検知できる。

MUA による電子署名の付与及び電子署名の検証の手順を表 4 に示す。

表4　MUAによる電子署名の付与及び電子署名の検証の手順

処理MUA	手順	処理内容
送信者のMUA	1	ハッシュ関数hによってメール内容のハッシュ値aを生成する。
	2	⑨ハッシュ値aを基に，電子署名データを作成する。
	3	送信者の電子証明書と電子署名付きのメールを送信する。
受信者のMUA	4	⑩受信したメール中の電子署名データからハッシュ値aを取り出す。
	5	ハッシュ関数hによってメール内容のハッシュ値bを生成する。
	6	⑪ハッシュ値を比較する。

X主任は，S/MIME導入に当たってY社とZ社が実施すべき事項について検討し，次の四つの実施事項をまとめた。

・Y社のホームページ上で，サポートメールへのS/MIMEの導入をアナウンスし，なりすまし防止対策を強化することを顧客に周知する。
・取得した電子証明書は，Z社にも秘密鍵と併せて提供する。
・Y社のサポート担当者及びZ社のサポートチームYのサポート担当者は，自身のPCに電子証明書と秘密鍵をインストールする。
・Y社及びZ社のサポート担当者は，送信するメールに電子署名を付与する。

X主任は，サポートメールにSPFとDKIMだけでなく新たにS/MIMEも導入したメールの運用方法と，サポート委託を開始するまでにY社及びZ社で実施すべき事項をW課長に報告した。報告内容が承認されたので，X主任は，委託時のメールの運用を開始するまでの手順書の作成，及びZ社の窓口担当者との調整に取り掛かった。

設問1　〔Y社のネットワーク構成とセキュリティ対策の背景〕について答えよ。

(1)　本文中の下線①について，転送先のメール中継サーバのFQDNを答えよ。

(2)　本文中の下線②について，社内メールサーバYからメール中継サーバY1又はY2へのメール転送時に，振分けの偏りを小さくするために実施している方策を，25字以内で答えよ。

(3)　本文中の［a］～［c］に入れる適切な字句を答えよ。

(4)　表1中の［ア］，［イ］に入れる適切なIPアドレスを答えよ。

(5)　本文中の下線③について，攻撃者がPTRレコードに対して行う不正な操作

の内容を，次に示す図8を参照して45字以内で答えよ。

ホストのIPアドレス	IN	PTR	ホストのFQDN

図8　PTRレコードの形式（抜粋）

設問2　〔Y社が導入しているSPFの概要〕について答えよ。

(1)　図4中の［ウ］，［エ］に入れる適切なIPアドレスを答えよ。

(2)　本文中の［d］～［f］に入れる適切な字句を答えよ。

(3)　本文中の下線④について，正当性の確認方法を，50字以内で答えよ。

設問3　〔Y社が導入しているDKIMの概要〕について答えよ。

(1)　本文中の［g］～［i］に入れる適切な字句又は数値を答えよ。

(2)　図5のDKIMレコードで指定されている暗号化方式のアルゴリズム名，及び表2中の［オ］に入れる適切な鍵名を答えよ。

(3)　本文中の下線⑤について，電子署名の真正性の検査によって送信者がなりすまされていないことが分かる理由を，50字以内で答えよ。

設問4　〔Z社に委託するメールの運用方法の検討〕について答えよ。

(1)　本文中の下線⑥について，登録するDNSサーバ名及びDNSサーバに登録する情報を，それぞれ，図1又は図6中の字句を用いて答えよ。

(2)　本文中の［j］に入れる適切な字句を答えよ。

(3)　本文中の下線⑦について，異なる鍵を利用することによる，Y社におけるセキュリティ面の利点を，50字以内で答えよ。

(4)　本文中の下線⑧について，顧客のメールサーバでは，なりすましを検知できない理由を，40字以内で答えよ。

設問5　〔S/MIMEの調査と実施策〕について答えよ。

(1)　表4中の下線⑨の電子署名データの作成方法を，25字以内で答えよ。

(2)　表4中の下線⑩のハッシュ値aを取り出す方法を，20字以内で答えよ。

(3)　表4中の下線⑪について，どのような状態になれば改ざんされていないと判断できるかを，25字以内で答えよ。