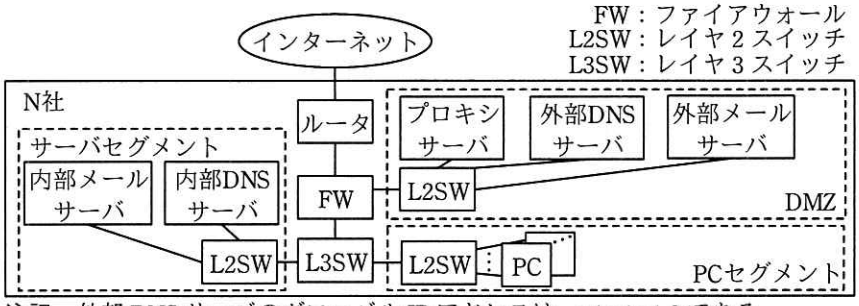
問1　電子メールのセキュリティ対策に関する次の記述を読んで，設問1～4に答えよ。

N社は，従業員数500名の情報サービス事業者である。N社の情報システムの構成を図1に示す。



注記　外部DNSサーバのグローバルIPアドレスは，x1.y1.z1.2である。

図1　N社の情報システムの構成

N社の情報システムは，情報システム部（以下，情シ部という）のQ部長とU主任を含む5名で運用している。

各PC及び各サーバは脆弱(ぜい)性修正プログラムが自動的に適用され，導入済のマルウェア対策ソフトのマルウェア定義ファイルが自動的にアップデートされる設定になっている。外部メールサーバでは，スパムメールフィルタの機能を利用している。

N社では，インターネットドメイン名n-sha.co.jp（以下，N社ドメイン名という）を取得しており，メールアドレスのドメイン名にも使用している。外部DNSサーバは，電子メール（以下，メールという）に関して図2のように設定してある。

```
n-sha.co.jp.        IN MX   10   mail.n-sha.co.jp. 1)
mail.n-sha.co.jp.   IN A    x1.y1.z1.1 2)
```

注記　逆引きの定義は省略しているが，適切に設定されている。
注1)　mail.n-sha.co.jpは，外部メールサーバのホスト名である。
2)　x1.y1.z1.1は，グローバルIPアドレスを示す。

図2　N社の外部DNSサーバのメールに関する設定

送信者メールアドレスには，SMTPの［　a　］コマンドで指定されるエンベロープの送信者メールアドレス（以下，Envelope-FROMという）と，メールデータ内のメールヘッダで指定される送信者メールアドレス（以下，Header-FROMという）

がある。送信したメールが不達になるなど配送エラーとなった場合，Envelope-FROM で指定したメールアドレス宛てに通知メールが届く。N 社では，従業員が PC からメールを送信する場合，Envelope-FROM 及び Header-FROM とも自身のメールアドレスが設定される。

昨今，メールを悪用して企業秘密や金銭をだまし取る攻撃が発生しており，N 社が属する業界団体の会員企業でも，なりすましメールによる攻撃によって被害が発生した。こうした被害を少しでも抑えるため，同団体から送信者メールアドレスが詐称されているかをドメイン単位で確認する技術（以下，送信ドメイン認証技術という）を普及させるよう働きかけがあったことから，N 社でも情シ部が中心になって送信ドメイン認証技術の利用を検討することになった。

〔送信ドメイン認証技術の検討〕

Q 部長と U 主任は，送信ドメイン認証技術の利用について検討を始めた。次は，その際の Q 部長と U 主任の会話である。

Q 部長：当社でも送信ドメイン認証技術を利用すべきだと経営陣に報告したい。まずは，どのような送信ドメイン認証技術を利用するかを検討しよう。

U 主任：送信ドメイン認証技術では，SPF，DKIM，DMARC が標準化されています。当社の外部メールサーバでは，いずれも利用が可能です。

Q 部長は，図 3 のなりすましメールによる攻撃の例を示し，送信ドメイン認証技術が各攻撃の対策となるかどうかをまとめるように U 主任に指示した。

攻撃 1　N 社の取引先のメールアドレスを送信者として設定したメールを，攻撃者のメールサーバから N 社に送信する。
攻撃 2　N 社のメールアドレスを送信者として設定したメールを，攻撃者のメールサーバから N 社の取引先に送信する。

図 3　なりすましメールによる攻撃の例

U 主任は，SPF への対応と各攻撃に対する効果の関係を表 1 にまとめ，SPF が対策となるかどうかを同表を用いて Q 部長に説明した。

表1　SPF への対応状況と各攻撃に対する効果

項番	SPF への対応状況				攻撃1に対する効果	攻撃2に対する効果
	外部 DNS サーバでの設定 1)	外部メールサーバでの対応 2)	取引先の DNS サーバでの設定 1)	取引先のメールサーバでの対応 2)		
1	設定済み	実施する	設定済み	実施する	○	○
⋮	⋮	⋮	⋮	⋮	⋮	⋮
4	設定済み	実施する	未設定	実施しない	b	c
⋮	⋮	⋮	⋮	⋮	⋮	⋮
6	設定済み	実施しない	設定済み	実施しない	d	e
7	設定済み	実施しない	未設定	実施する	f	g
⋮	⋮	⋮	⋮	⋮	⋮	⋮
13	未設定	実施しない	設定済み	実施する	h	i
⋮	⋮	⋮	⋮	⋮	⋮	⋮
16	未設定	実施しない	未設定	実施しない	×	×

注記　表中の“○”は送信者メールアドレスが詐称されているかを判断可，“×”は判断不可を示す。
注 1)　SPF に必要な設定を DNS サーバに設定済みかを示す。
2)　メール受信時に，SPF に必要な問合せを実施するかを示す。

次は，その後の Q 部長と U 主任の会話である。

Q 部長：SPF に対応するには，具体的にどのような設定が必要になるのか。

U 主任：DNS サーバでの設定は，当社の外部 DNS サーバに図 4 に示す TXT レコードを登録します。

```
n-sha.co.jp.  IN TXT  "v=spf1 +ip4:[ j ] -all"
```

図 4　TXT レコード

メールサーバでの対応は，当社の外部メールサーバの設定を変更します。SPF による検証（以下，SPF 認証という）が失敗したメールは，件名に[NonSPF]などの文字列を付加して，受信者に示すこともできます。

Q 部長：なるほど。SPF の利用に注意点はあるのかな。

U 主任：メール送信側の DNS サーバ，メール受信側のメールサーバの両方が SPF に対応している状態であっても，その間で SPF に対応している別のメールサーバが Envelope-FROM を変えずにメールをそのまま転送する場合は，①メール受信側のメールサーバにおいて，SPF 認証が失敗してしまうという制

約があります。

Q部長：なるほど。それでは，DKIMはどうかな。

U主任：DKIMに対応したメールを送信するためには，まず，準備として公開鍵と秘密鍵のペアを生成し，そのうち公開鍵を当社の外部DNSサーバに登録し，当社の外部メールサーバの設定を変更します。DKIM利用のシーケンスは，図5及び図6に示すとおりとなります。

図5　DKIM利用のシーケンス

1. DKIM-Signatureヘッダにディジタル署名を付与し，メールを送信する。
2. 受信側メールサーバは，DKIM-Signatureヘッダのdタグに指定されたドメイン名を基に，外部DNSサーバに公開鍵を要求する。
3. 要求を受けた外部DNSサーバは，登録されている公開鍵を送信する。
4. ②受信した公開鍵，並びに署名対象としたメール本文及びメールヘッダを基に生成したハッシュ値を用いて，DKIM-Signatureヘッダに付与されているディジタル署名を検証する。

図6　DKIM利用のシーケンスの説明

Q部長：DKIMの方が少し複雑なのだな。

U主任：はい。しかし，DKIMは，メール本文及びメールヘッダを基にディジタル署名を付与するので，転送メールサーバがディジタル署名，及びディジタル署名の基になったメールのデータを変更しなければ，たとえメールが転送された場合でも検証が可能です。SPFとDKIMは併用できます。

Q部長：分かった。両者を導入するのがよいな。それでは，DMARCはどうかな。

U主任：DMARCは，メール受信側での，SPFとDKIMを利用した検証，検証したメールの取扱い，及び集計レポートについてのポリシを送信側が表明する方法です。DMARCのポリシの表明は，DNSサーバにTXTレコードを追加することによって行います。TXTレコードに指定するDMARCの主なタグ

を表2に示します。

表2　DMARC の主なタグ（概要）

タグ	タグの説明	値と説明
p	送信側が指定する受信側でのメールの取扱いに関するポリシ（必須）	none：何もしない。 quarantine：検証に失敗したメールは隔離する。 reject：検証に失敗したメールは拒否する。
aspf	SPF 認証の調整パラメタ（任意）	r：Header-FROM と Envelope-FROM に用いられているドメイン名の組織ドメインが一致していれば認証に成功 s：Header-FROM と Envelope-FROM に用いられている完全修飾ドメイン名が一致していれば認証に成功
adkim	DKIM 認証の調整パラメタ（任意）	r：DKIM-Signature ヘッダの d タグと Header-FROM に用いられているドメイン名の組織ドメインが一致していれば認証に成功 s：DKIM-Signature ヘッダの d タグと Header-FROM に用いられている完全修飾ドメイン名が一致していれば認証に成功
rua	DMARC の集計レポートの送信先（任意）	URI 形式で指定する。

注記　完全修飾ドメイン名が“a-sub.n-sha.co.jp”の場合，組織ドメインは“n-sha.co.jp”となる。

これらの検討結果を経営陣に報告したところ，N 社は送信ドメイン認証技術として SPF，DKIM，DMARC を全て利用することになり，情シ部が導入作業に着手した。

〔ニュースレターの配信〕

送信ドメイン認証技術の導入作業着手から 1 週間後，N 社営業部で取引先宛てにニュースレターを配信する計画が持ち上がった。ニュースレターの配信には，X 社のクラウド型メール配信サービス（以下，X 配信サービスという）を利用する。ニュースレターは，X 社のメールサーバから配信され，配送エラーの通知メールは，X 社のメールサーバに届くようにする。Header-FROM には，N 社ドメイン名のメールアドレス（例：letter@n-sha.co.jp）を設定する。Envelope-FROM には，N 社のサブドメイン名 a-sub.n-sha.co.jp のメールアドレス（例：letter@a-sub.n-sha.co.jp）を設定する。X 社のメールサーバのホスト名は，mail.x-sha.co.jp であり，グローバル IP アドレスは，x2.y2.z2.1 である。X 社の DNS サーバのグローバル IP アドレスは，x2.y2.z2.2 である。X 配信サービスでは，SPF，DKIM，DMARC のいずれも利用が可能である。

N 社は，ニュースレターの配信についても，3 種類の送信ドメイン認証技術を利用することにした。具体的には，N 社の外部 DNS サーバに図 7 のレコードを追加する。

a-sub.n-sha.co.jp. IN MX 10 [k]
a-sub.n-sha.co.jp. IN TXT "v=spf1 +ip4:[l] -all"

注記 1　逆引きの定義は省略しているが，適切に設定されている。
注記 2　DKIM，DMARC のレコードは省略しているが，適切に設定されている。

図 7　追加するレコード

ここで，受信側で検証に失敗したメールは隔離するポリシとするため，DMARC の p タグと aspf タグの設定は表 3 のとおりとする。

表 3　DMARC のタグ設定

タグ	値
p	[m]
aspf	[n]

注記　ほかのタグは省略しているが，適切に設定されている。

その後，N 社と主要な取引先での送信ドメイン認証技術の導入が完了した。

設問 1　本文中の［ a ］に入れる適切な字句を答えよ。

設問 2　〔送信ドメイン認証技術の検討〕について，(1)～(4)に答えよ。

(1)　表 1 中の［ b ］～［ i ］に入れる適切な内容を，“○”又は“×”のいずれかで答えよ。

(2)　図 4 中の［ j ］に入れる適切な字句を答えよ。

(3)　本文中の下線①について，SPF 認証が失敗する理由を，SPF 認証の仕組みを踏まえて，50 字以内で具体的に述べよ。

(4)　図 6 中の下線②の検証によってメールの送信元の正当性以外に確認できる事項を，20 字以内で述べよ。

設問 3　図 7 中の［ k ］，［ l ］，表 3 中の［ m ］，［ n ］に入れる適切な字句を答えよ。

設問 4　攻撃者がどのように N 社の取引先になりすまして N 社にメールを送信すると，N 社が SPF，DKIM 及び DMARC では防ぐことができなくなるのか。その方法を 50 字以内で具体的に述べよ。