問2　ドメイン名変更に関する次の記述を読んで，設問に答えよ。

A 社は，従業員 1,000 名の工作機械製造会社である。A 社の技術力は高く評価されている。A 社には，総務部，営業部，情報システム部，技術部及び製造部がある。

A 社の Web サイトでは，一般向けに IR 情報と関連会社へのリンクを，顧客向けに自社製の工作機械管理用アプリケーションプログラムとそのソフトウェア修正プログラムを提供している。また，A 社では，電子メール（以下，メールという）を用いて，顧客との間で見積書や注文書の送受信をしたり，ニュースサイトのメールマガジンに登録して最新の情報を収集したりしている。

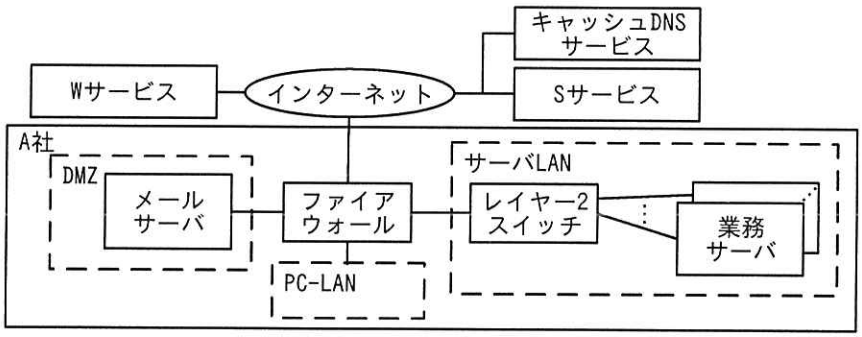
A 社のドメイン名を詐称したメールが毎週 2 通程度，送られていることが，多くの顧客から報告されている。情報システム部長は，顧客に詐欺などの被害が生じるおそれがあることを認識し，メールの詐称対策が必要であると考えている。

〔情報システムの現状〕

A 社は，10 年前にドメイン名 a-sha.co.jp（以下，A 社ドメイン名という）を取得して以降，A 社の Web サイト（以下，A-Web サイトという）及びメールアドレスのドメイン名として利用している。A 社ドメイン名は，DNS サービス事業者である S 社の権威 DNS サービス（以下，S サービスという）を用いて管理している。

A-Web サイトは，Web サービス事業者である W 社の Web サービス（以下，W サービスという）を用いて提供している。

A 社のネットワークを図 1 に，構成要素の機能を表 1 に示す。A 社の従業員は，PC-LAN 内の PC で業務を行っている。



注記　PC-LAN 内の PC の記載は省略している。

図 1　A 社のネットワーク（抜粋）

表1　構成要素の機能（抜粋）

構成要素	機能
メールサーバ	・S社が提供するキャッシュDNSサービスを用いて，DNS問合せを行う。 ・インターネットとの間で，SMTPを用いてメールを転送する。 ・PC-LAN及び業務サーバからSMTPを用いて送信されるメールを受信する。 ・宛先メールアドレスのドメイン名が［　a　］であるメールをメールボックスに格納する。 ・第三者中継防止のためのルールを用いて，第三者中継を防止する。第三者中継防止のためのルールを表2に示す。 ・メールボックス内のメールを，PC-LAN内のPCがPOP3を用いて受信できるようにする。

表2　第三者中継防止のためのルール

項番	転送元	宛先メールアドレスのドメイン名	転送処理
1	インターネット	［　a　］	許可
2	PC-LAN	［　b　］	許可
3	業務サーバ	A社ドメイン名	許可
4	全て	全て	拒否

注記　項番が小さいルールから順に，最初に一致したルールが適用される。

〔ドメイン名の変更についての検討〕

A社は，3か月後にZ社への社名変更を予定している。情報システム部長は，メールの詐称対策の導入及び社名変更に合わせたドメイン名変更を検討するように情報システム部のN主任に指示した。N主任は情報システム部のEさんと，次のとおり検討した。

・z-sha.co.jp（以下，Z社ドメイン名という）が過去に取得されたことがないドメイン名であることを確認してから取得する。
・Z社ドメイン名の管理もSサービスで行う。
・Wサービスで Z社ドメイン名のWebサイト（以下，Z-Webサイトという）も立ち上げる。
・図1のメールサーバでは，複数のドメイン名のメールを受信できないことから，商用のメールサービスに移行する。
・メールの詐称対策は，SPF，DKIM及びDMARCで対応する。

N 主任と E さんは，Z 社が送信するメールの詐称対策（以下，送信対応という）と，Z 社が受信するメールの詐称対策（以下，受信対応という）について方針をそれぞれ表 3 と表 4 のとおり作成した。

表 3　送信対応方針

項番	対応方針概要
1	送信するメールのエンベロープ From 及びヘッダーFrom のドメイン名を Z 社ドメイン名とする。
2	Z 社ドメイン名のメールを受信した側で SPF による認証及び DKIM による認証に失敗した場合のアクションを DMARC ポリシーとして定義する。
3	DMARC ポリシーレコード（以下，DMARC レコードという），SPF レコード及び DKIM キーレコード（以下，DKIM レコードという）を S サービスに登録する。
4	送信するメールには，DKIM 署名を付与する。
5	DMARC レポートを分析する。
6	顧客に，Z 社は送信するメールについて，SPF，DKIM 及び DMARC に対応済みであることを周知する。

表 4　受信対応方針

項番	対応方針概要
1	受信するメールの宛先メールアドレスのドメイン名は，Z 社ドメイン名とする。
2	顧客に，送信するメールについて SPF，DKIM 及び DMARC に対応するように依頼する。
3	SPF による認証及び DKIM による認証を行いそのいずれかが成功した場合，DMARC の認証が成功したものと判断し，受信する。
4	送信元の DMARC ポリシーに基づき，メールの受信，隔離又は拒否を行う。

N 主任と E さんは，これまでの結果を，情報システム部長に報告し，了承を得た。

〔メールサービスの機能の検討〕

N 主任と E さんは，メールサービスの機能について検討し，メールサービス事業者である U 社のメールサービス（以下，U サービスという）に移行することにした。U サービスの機能の概要を表 5 に示す。

表5　Uサービスの機能の概要（抜粋）

機能	概要
メール転送	・インターネットとの間は，SMTP を TLS で暗号化する［　c　］を使用してメールを転送することができる。
Web メール	・Web ブラウザを用いてメールを送受信する。
Uサービス管理 Web	・利用者アカウントの登録や削除を行う。 ・送信したメールについて DMARC レポートの分析結果を参照することができる。

〔Z-Web サイト及びUサービスへの移行手順の検討〕

E さんは，Z-Web サイト及び U サービスへの移行手順を検討した。検討結果を，図2及び図3にそれぞれ示す。

Web-Step1：A-Web サイトのコンテンツを全て，Z-Web サイトに同一構成で配置する。Z-Web サイトに配置したコンテンツ中の A 社ドメイン名を Z 社ドメイン名に書き換える。
Web-Step2：次を1年間，実施する。
・A-Web サイトへのアクセスを，Z-Web サイトのトップページにリダイレクトする。
Web-Step3：A-Web サイトを停止する。A-Web サイト用の DNS レコードは削除する。

図2　Z-Web サイトへの移行手順

Mail-Step1：試行期間として次を1か月間，実施する。
・総務部及び情報システム部のメンバーだけが，Z 社ドメイン名のメールアドレスを使用する。
・送信対応では，DMARC ポリシーを，特定のアクションを要求しないこととし，メールを受信してもらう。
・受信対応では，DMARC の認証結果にかかわらず受信する。
Mail-Step2：図1のメールサーバの利用をやめ，次を3か月間，実施する。
・Z 社全体が，U サービスを用いて Z 社ドメイン名のメールアドレスを使用する。
・Z 社ドメイン名でのメールの利用を顧客に文書で周知するとともに，Z-Web サイトで周知する。
・A 社ドメイン名宛てのメールを U サービスで受信する。
Mail-Step3：送信対応の DMARC ポリシーを隔離に変更し，その6か月後，拒否に変更する。
Mail-Step4：A 社ドメイン名でのメールの受信を停止する。メールサーバ用の DNS レコードは削除する。
Mail-Step5：問題がないと確認できたら，受信対応で DMARC の処理を行う。

図3　Uサービスへの移行手順

E さんは，図2及び図3を N 主任に説明し，了承を得た。

〔送信対応の設定内容についての検討〕

E さんは，送信対応に用いる SPF レコードを，U サービスから提供された情報に基づいて作成した。

次に，E さんは，送信対応に用いる DKIM レコードについて検討した。Z 社が U サービスを利用した場合，送信されるメールに付与される DKIM-Signature ヘッダーのタグの内容を表 6 に示す。

表 6　タグの内容（抜粋）

タグ	内容
v	1
a	rsa-sha256
d	z-sha.co.jp
h	From:To:Subject:Date:Message-ID:MIME-Version
s	z2024

表 6 から，①DKIM レコードの名称として使用する FQDN が決まる。E さんは，U サービスから提供された情報に基づき DKIM レコードを作成した。

最後に，E さんは，Mail-Step1 の送信対応では DMARC レコードを図 4 のとおりとすることにした。

v=DMARC1; p=［　d　］; rua=mailto:rua-report@z-sha.co.jp

図 4　DMARC レコード

E さんは，設定内容をまとめて N 主任に報告し，了承を得た。

〔A 社ドメイン名の契約についての検討〕

N 主任と E さんは，A 社ドメイン名使用の契約を継続するか解約するかについて検討した。解約した場合，第三者が A 社ドメイン名を取得することができる。N 主任と E さんは，第三者が A 社ドメイン名を取得した場合の A 社ドメイン名の悪用例を検討し，表 7 のとおりまとめた。

表7　A社ドメイン名の悪用例

項目	悪用の例
Webの悪用	第三者が，A社ドメイン名を用いて，現在のA-Webサイトと見た目が同じWebサイトを立ち上げるという悪用が考えられる。さらに，第三者が，コンテンツを細工してWebサイトの見た目を変えずに②顧客に影響を及ぼす攻撃をすることが考えられる。
メールの送信	第三者が，メールサーバを立ち上げ，A社ドメイン名のメールアドレスを送信元メールアドレスとしてメールを送信するという悪用が考えられる。
メールの受信	従業員が業務で用いる社外サービスがあり，メールでの連絡先として，A社ドメイン名のメールアドレスを登録していたとする。もし連絡先の変更を忘れてしまうと，③第三者が，社外サービスからA社ドメイン名のメールアドレスへのメールを受信し，そのメールを使って続きの攻撃を行うという悪用が考えられる。

N主任とEさんは，A社ドメイン名使用の契約を継続することを情報システム部長に報告し，承認を得た。

また，A社ドメイン名については，Mail-Step4の後で次のとおり，設定することにした。

・DMARCレコードを設定する。

・DMARCの受信対応を行った組織がA社ドメイン名からのメールを拒否できるようにする。

そのために，A社ドメイン名について，SPFレコードを図5のように設定する。DKIMレコードは設定しない。

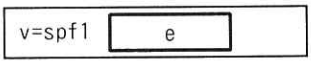


図5　SPFレコード

〔Uサービスへの移行の見直し〕

Mail-Step1において，DMARCレポートの分析結果を参照した結果，送信対応には問題がないことが確認できた。

Mail-Step2の開始1週間後，情報システム部のEさんに営業部のHさんから，図6に示すメールの一斉配信をしても問題ないか相談があった。

1. 定期的に，Z 社の公式情報の周知のためのメールを一斉配信する。
2. 宛先には，社内と社外のメールアドレスが含まれている。
3. 一斉配信には，T 社のサービス（以下，T サービスという）を利用する計画であり，T サービスの仕様は次のとおりである。
   ・配信方法
     - 宛先メールアドレスは，サービス契約者が登録できる。
     - 宛先メールアドレスごとに個別に送信する。
   ・メールのヘッダーの設定
     - From は，サービス契約者が所属する組織が保有するドメイン名を用いたメールアドレスだけを設定できる。
     - To は，宛先のメールアドレスから一つずつ，T サービスが設定する。
     - Subject は，一斉配信の都度，サービス契約者が設定する。
     - 他のヘッダーは，T サービスが設定する。

図 6　メールの一斉配信の説明

E さんから相談を受けた N 主任は，図 6 の一斉配信メールについて，次のとおり E さんに説明した。

・Mail-Step3 以降で，一斉配信されたメールが届かない場合がある。メールが届くように，Mail-Step2 の期間で，④表 3 の項番 3 での登録内容を見直す必要がある。

E さんは，見直し案を作成し，N 主任の了承を得てから，H さんに問題ないことを説明した。

Mail-Step2 の開始 2 週間後，情報システム部に技術部の J さんから，図 7 に示すメーリングリストを新たに利用することが可能か相談があった。

1. 使用するメーリングリストは一つである。
2. メーリングリストの管理者は，Z 社従業員である。
3. 製品に関する情報交換のために，メーリングリストを使用する。
4. メーリングリストの配信先となる宛先には，社内及び社外のメールアドレスを登録する（以下，登録されたメールアドレスを登録メンバーという）。
5. 登録メンバーから，メーリングリスト宛てにメールを送信できる。
6. メールサービス事業者である Y 社のサービス（以下，Y サービスという）を利用する計画であり，Y サービスの仕様は次のとおりである。
   (1) メーリングリストのメールアドレスは，サービス契約者ごとに割り当てられた Y サービスのメールアドレスである。ドメイン名は Y 社のドメイン名である。
   (2) Y サービスの管理画面で設定できる項目は(3)～(6)であり，配信されるメールに反映される。
   (3) エンベロープ From の設定
      ・メーリングリストの管理者のメールアドレスを設定する。
   (4) ヘッダーFrom の設定
      ・次のいずれかを選択する。
        ヘッダーFrom 設定 1：メーリングリスト宛てに送信されたメールのヘッダーFrom を使用する。
        ヘッダーFrom 設定 2：メーリングリストのメールアドレスを使用する。
   (5) Subject の設定
      ・次のいずれかを選択する。
        Subject 設定 1：メーリングリスト宛てに送信されたメールの Subject を使用する。
        Subject 設定 2：メーリングリスト宛てに送信されたメールの Subject にメールの通番情報を付加する。
   (6) Reply-To の設定
      ・メーリングリストのメールアドレスを設定する。
   (7) ヘッダーFrom，Subject 及び Reply-To 以外のヘッダー
      ・メーリングリスト宛てに送信したメールのヘッダーを引き継ぐ。
   (8) Authenticated Received Chain [1] (ARC) について
      ・ARC には，対応していない。

注 [1] メールが転送される場合でも，メールの認証結果を確認できるようにする仕組みとして，RFC 8617 に定義されている。

図 7　メーリングリストの説明

N 主任は，E さんに図 8 に示すとおり説明した。

・Mail-Step3 以降に Z 社の従業員が送信したメールについて
  - ヘッダーFrom 設定 1 と Subject 設定 1 の組合せでは，不達の問題は起きない。
  - ヘッダーFrom 設定 1 と Subject 設定 2 の組合せでは，⑤SPF による認証及び DKIM による認証の両方に失敗することによって不達の問題が発生することがある。
  - ヘッダーFrom 設定 2 については，Z 社の従業員が送信したメールであるかどうかの判定ができないので，用いるべきではない。
・Mail-Step3 以降に Z 社の従業員以外が送信したメールについて
  （省略）

図 8　N 主任の説明

N主任とEさんは，Jさんには，ヘッダーFrom設定1とSubject設定1の組合せを用いるよう説明した。

その後，Z-Webサイト及びUサービスへの移行は，順調に進み，完了した。

設問1　〔情報システムの現状〕について答えよ。

(1)　表1中及び表2中の［　a　］に入れる適切な字句を答えよ。

(2)　表2中の［　b　］に入れる適切な字句を答えよ。

設問2　表5中の［　c　］に入れる適切な字句を英字10字以内で答えよ。

設問3　〔送信対応の設定内容についての検討〕について答えよ。

(1)　本文中の下線①のFQDNを解答群の中から選び，記号で答えよ。

解答群

ア　rsa-sha256._dkim.z-sha.co.jp

イ　rsa-sha256._domainkey.z-sha.co.jp

ウ　z2024._dkim.z-sha.co.jp

エ　z2024._domainkey.z-sha.co.jp

オ　z2024.z-sha.co.jp

(2)　図4中の［　d　］に入れる適切な字句を解答群の中から選び，記号で答えよ。

解答群

ア　accept　　イ　none　　ウ　quarantine　　エ　receive

オ　reject

設問4　〔A社ドメイン名の契約についての検討〕について答えよ。

(1)　表7中の下線②について，攻撃の方法を具体的に答えよ。

(2)　表7中の下線③について，受信するメールの内容及び続きの攻撃の例を具体的に答えよ。

(3)　図5中の［　e　］に入れる適切な字句を解答群の中から選び，記号で答えよ。

解答群

ア　-all　　イ　?all　　ウ　block　　エ　deny　　オ　refuse

設問5　〔U サービスへの移行の見直し〕について答えよ。

(1)　本文中の下線④について，見直しの内容を具体的に答えよ。

(2)　図 8 中の下線⑤について，SPF による認証に失敗する理由及び DKIM による認証に失敗する理由をそれぞれ，S サービスへの登録内容と Y サービスの仕様を含めて，具体的に答えよ。