問2　DMZ 上の機器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。

U 社は，従業員数 1,500 名の機械部品製造会社である。横浜に本社及び工場があり，国内 10 か所に営業所がある。U 社では，本社に DMZ を設置し，電子メール（以下，メールという）の送受信，Web の閲覧及び Web サーバによる情報公開に利用している。ドメイン名は，u-sha.co.jp（以下，U 社ドメインという）である。U 社ドメインの管理には，B 社 DNS サービスを利用している。

U 社では，コピー機能，プリント機能，イメージスキャン機能及びイメージ送信機能が一体になった複合機を導入している。

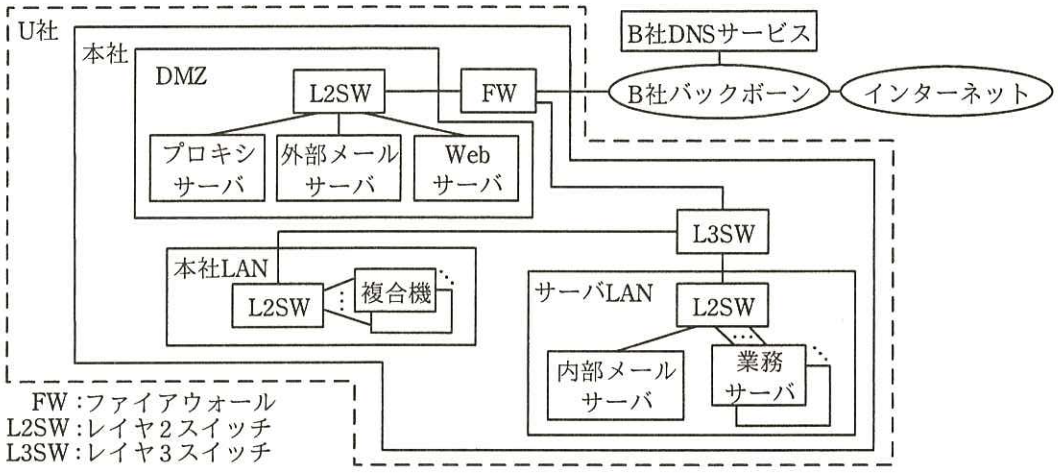
U 社で使用しているメールアドレスを表 1 に示す。

表 1　U 社で使用しているメールアドレス

種別		メールアドレス	概要
従業員用メールアドレス		*user*@u-sha.co.jp	従業員が使用するメールアドレスである。*user* は，従業員ごとに異なる。
特定目的用メールアドレス	メール管理者用メールアドレス	postmaster@u-sha.co.jp	メールシステム管理者用メールアドレスである。
	複合機用メールアドレス	scanner@u-sha.co.jp	全ての複合機に共通のメールアドレスである。送信専用である。

〔U 社情報システムの構成〕

U 社情報システムのネットワーク構成を図 1 に，機器の機能概要を表 2 に示す。



注記1　工場及び営業所については，記載を省略している。
注記2　本社 LAN に PC が接続されているが，記載を省略している。

図1　U社情報システムのネットワーク構成

表2　機器の機能概要（抜粋）

機器名	機能概要
プロキシサーバ	・DNS キャッシュ機能及びオープンリゾルバ防止機能 ・プロキシ機能及びオープンプロキシ防止機能 ・URL フィルタリング機能 ベンダが提供するベンダブラックリスト，及びサーバ管理者が登録できる管理者ブラックリストがある。
外部メールサーバ	・インターネットと内部メールサーバとの間のメール転送機能 ・インターネットから転送されるメールに対するフィルタリング機能 フィルタリングは次の(1)～(6)の順に行われる。 (1) 迷惑メールの送信に悪用される［ a ］を防止するために，エンベロープの宛先メールアドレスのドメイン名が U 社ドメイン以外のメールを拒否 (2) 迷惑メール対策として，［ b ］認証技術の一つである SPF（Sender Policy Framework）によって Fail と判定されたメールを拒否 (3) エンベロープの送信者メールアドレスとブラックリスト 1 の照合結果によって，メールを拒否 (4) エンベロープの宛先メールアドレスとブラックリスト 2 の照合結果によって，メールを拒否 (5) メールヘッダの送信者メールアドレスとブラックリスト 3 の照合結果によって，メールを拒否 (6) メールヘッダの宛先及び同報先メールアドレスとブラックリスト 4 の照合結果によって，メールを拒否 なお，ブラックリスト 1～ブラックリスト 4 には，拒否したいメールアドレス，又は拒否したいメールアドレスのドメイン名を登録する。照合は，完全一致によって行われる。

表2　機器の機能概要（抜粋）（続き）

機器名	機能概要
複合機	・コピー機能，プリント機能及びイメージスキャン機能 ・イメージ送信機能 送信者メールアドレスとして複合機用メールアドレスを用い，スキャンしたイメージを添付したメールを，イメージを作成した本人又は同じ部署の従業員のメールアドレスに送信する。

B社のDNSサービスに登録されているU社ドメインの設定を図2に示す。

```
u-sha.co.jp.      IN TXT "v=spf1 +ip4:x1.y1.z1.235 -all"
```

注記　x1.y1.z1.235は，外部メールサーバのIPアドレスである。

図2　U社ドメインの設定（抜粋）

〔情報セキュリティ対策の強化〕

最近，U社と同業のC社において，DMZ上の機器への不正侵入による情報漏えい事件が発生したとの報道があった。事件を知ったU社の経営幹部は，U社でも同様の問題が起こるおそれがあるかどうかについて，早急に調査するように，情報システム部長に指示した。調査は，情報システム部のKさんが担当し，セキュリティ専門業者Y社のW氏から支援を受けることになった。

〔DMZ上の機器の設定の点検〕

Kさんは，DMZ上の機器の設定を点検することにした。まず，外部メールサーバ，Webサーバ及びDMZ上のL2SWを点検することとし，W氏に相談した。W氏は，図3のようにインターネットで行われている攻撃の例を説明し，まず，プロキシサーバについて設定を点検すべきであると指摘した。

・DNSキャッシュポイズニング攻撃
・オープンリゾルバ防止機能が適切に設定されていない場合に起きるDNS［　c　］攻撃

図3　インターネットで行われている攻撃の例

W氏はKさんに，プロキシサーバの設定の点検方法を説明した。

〔プロキシサーバの設定の点検〕

K さんは，プロキシサーバの DNS キャッシュ機能について，名前解決問合せパケットの［ d ］のランダム化設定の有無を調べ，適切に設定されていることを確認した。K さんは，その設定が行われていない場合，どのようなことが起きるのかを W 氏に質問した。W 氏は，DNS 名前解決通信では UDP が使われており，UDP ヘッダの［ d ］のランダム化が設定されていないと，図 4 に示すような DNS キャッシュ機能への攻撃が成功する可能性が高まると答えた。

(1) 攻撃者が，メールサーバを用意する。
(2) 攻撃者が，取引先ドメイン名の MX レコードを用意する。
(3) 攻撃者が，プロキシサーバに対して DNS キャッシュポイズニング攻撃を行い，用意した MX レコードを DNS キャッシュに保存させる。

図 4　DNS キャッシュ機能への攻撃

W 氏は，図 4 の攻撃の結果，［ e ］が，DNS キャッシュに保存させられた MX レコードを参照するので，①メール配送に影響が生じることを説明した。K さんは，W 氏の説明を理解した。

次に，K さんは，URL として，https://www.example.ne.jp/user035/index.html をフィルタリングしようと設定してみたが，パス名を含めた URL 全体を設定できず，ホスト単位のフィルタリングだけが設定できる仕様となっていたことを説明し，その理由を W 氏に質問した。W 氏の回答は，次のとおりであった。

・この URL の場合，プロキシサーバ経由で HTTP over TLS 通信が行われる。
・PC の Web ブラウザは，CONNECT メソッドを用いてプロキシサーバに接続し，サーバ www.example.ne.jp との間のトンネルの確立を要求する。
・PC の Web ブラウザは，プロキシサーバからステータスコードが 200 である応答を受信した後，サーバ www.example.ne.jp との間の TLS セッションを開始する。

W 氏の説明を受け，K さんは，②HTTP over TLS 通信では URL フィルタリングがホスト単位となることを理解した。

K さんは，プロキシサーバが DNS［ c ］攻撃に悪用されないようにする対策を含めて，他の設定を点検し，他に問題がないことを確認した。

〔外部メールサーバの設定の点検〕

K さんは，外部メールサーバの設定を点検した。W 氏は，複合機用メールアドレスを詐称したメールがインターネットから送信されて，マルウェア感染が起きるおそれがあることを指摘した。指摘を踏まえ，K さんは，③外部メールサーバの設定を変更した。さらに，念のため，複合機用メールアドレスを詐称するメールについての注意喚起情報を社内に周知した。

K さんは，引き続き外部メールサーバの設定を点検し，他に問題がないことを確認した。

最後に，K さんは，Web サーバ及び DMZ の L2SW の設定を点検し，問題がないことを確認した。

設問 1　表 2 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。

設問 2　図 3 中及び本文中の［ c ］に入れる適切な字句を，10 字以内で答えよ。

設問 3　〔プロキシサーバの設定の点検〕について，(1)～(3)に答えよ。

(1)　本文中の［ d ］に入れる適切な字句を，10 字以内で答えよ。

(2)　本文中の［ e ］に入れる機器名を，図 1 中の字句を用いて，10 字以内で答えよ。また，本文中の下線①で生じるとしている影響を，40 字以内で具体的に述べよ。

(3)　本文中の下線②の理由は，CONNECT メソッドのどのような仕様によるものか。該当する仕様を，20 字以内で具体的に述べよ。

設問 4　本文中の下線③について，変更箇所を，表 2 中の字句を用いて 10 字以内で答えよ。また，変更内容を，30 字以内で具体的に述べよ。