問3　プロキシ経由のWebアクセスに関する次の記述を読んで，設問1～3に答えよ。

T社は従業員数3,000名の食品卸売業を営む企業であり，全国10都市に支社を展開している。T社ではデータセンタ（以下，T社DCという）内に各種サーバを設置し，本社と各支社間を広域イーサネットで接続している。

T社の従業員には1台ずつPCが貸与されている。T社では広域イーサネットとは別にインターネットも利用しており，インターネットへのアクセス管理ルールでは，業務目的に限りインターネット上のWebサイト（以下，インターネットサイトという）へのアクセスを許可すること，並びに各従業員のインターネットサイトへのアクセス状況を記録するために，アクセスログを取得すること及びインターネットサイトに向けて送信された内容をログとして取得することを定めている。

T社本社及び各支社のLANに設置したPCからは直接インターネットにアクセスできないように，ルータ及びファイアウォールを設定している。ブラウザからインターネットサイトへのアクセスは，T社DCに設置したプロキシを経由して行う。T社のネットワーク構成の概要を図1に示す。

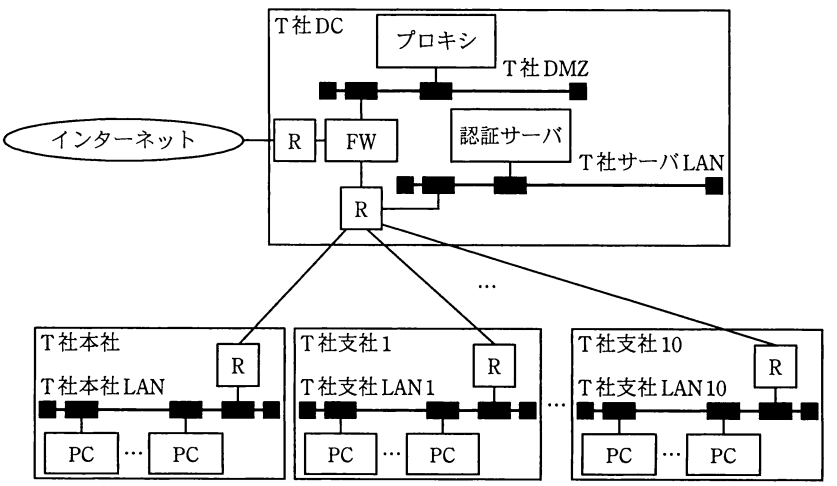

図1　T社のネットワーク構成（概要）

プロキシにはU社のプロキシ製品（以下，Uプロキシという）が使われている。

T社がUプロキシで利用している機能の利用目的を図2に示す。

(1) 利用者認証機能
利用目的：インターネットサイトにアクセスする従業員を識別し認証する。
ブラウザがHTTPリクエストのProxy-Authorizationヘッダに付与し，Uプロキシに送信した認証情報を，各従業員に一意に割り当てられた利用者IDとパスワードに照らして，アクセスした利用者を識別し認証する。
(2) アクセスログ取得機能
利用目的：従業員によるインターネットサイトへのアクセスについて，HTTPリクエストごとに，次の項目を取得する。
アクセス日時，アクセス元のIPアドレス，利用者ID，リクエストライン（HTTPメソッド，URL，HTTPプロトコルのバージョン），インターネットサイトのIPアドレス，受信データサイズ，インターネットサイトからのレスポンスコード
(3) 送信内容取得機能
利用目的：インターネットサイトにデータが送信された場合（POSTリクエスト，PUTリクエストの利用時など）に，その送信内容を取得する。
(4) フィルタリング機能
利用目的：インターネットサイトへのアクセスを業務目的だけに制限する。
HTTP通信ではブラックリスト方式，HTTPS通信ではホワイトリスト方式で，インターネットサイトのホストのFQDNに基づいたアクセス規制をする。
(5) ウイルスチェック機能
利用目的：インターネットサイトからのウイルス感染やインターネットサイトへのウイルス送信を防止する。
送受信データ内のウイルスをチェックする。

図2 T社がUプロキシで利用している機能の利用目的（抜粋）

〔HTTPS通信の制限〕

T社では，①インターネットへのアクセス管理ルールに基づき，インターネットサイトへのHTTPS通信によるアクセスを原則として禁止している。業務上，HTTPS通信が必要なインターネットサイトはホワイトリストに登録し，Uプロキシのフィルタリング機能を用いて，アクセスを許可している。

HTTPS通信を許可するホワイトリストは，定期見直しを情報システム部で四半期ごとに行っている。この見直しにおいて，インターネットで電子ファイルをやり取りできるファイル共有サービスのURLが登録されていたことが判明した。このURLのインターネットサイトにアクセスしていた従業員に確認したところ，顧客との間で電子ファイルをやり取りしていたことが分かった。業務上，同インターネットサイトを利用する必要があるので，アクセスは禁止できないが，同インターネットサイトを利用すれば社外に情報を持出し可能なこと，また，電子ファイルを不正に社外へ持ち出された場合に，当該電子ファイルを特定できないことが懸念として浮上した。そのため，情報システム部のS部長は，インターネットサイトへのアクセスに対するプロキシでのログ取得方式の改善を検討するよう，情報セキュリティ担当のK主任に指示した。

〔新たなプロキシ製品導入の検討〕

K 主任は，HTTPS 通信時にプロキシで詳細なログを取得するためには，U プロキシとは異なる仕組みをもつプロキシ製品を導入する必要があると考えた。そこで，U プロキシを，HTTPS 通信を一旦復号する機能をもつ L 社のプロキシ製品（以下，L プロキシという）で置き換えることが可能かどうかを確認することにした。

U プロキシを利用した HTTPS 通信では，暗号化された通信路をブラウザと Web サーバ間で確立する。U プロキシを利用した場合の HTTPS 通信を図 3 に示す。

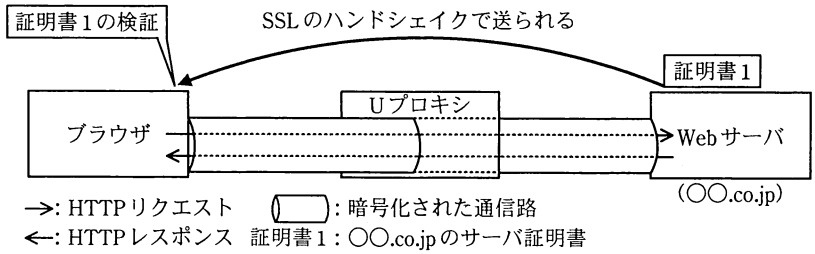

図 3　U プロキシを利用した場合の HTTPS 通信

一方，L プロキシを利用した HTTPS 通信では，ブラウザと L プロキシ間，及び L プロキシと Web サーバ間において，それぞれ独立の暗号化された通信路を確立する。L プロキシは証明書 1 を受け取ると，ブラウザには転送せずに，自身で証明書 1 の検証を行う。次に，L プロキシは認証局として証明書 1 と同じコモンネームのサーバ証明書（以下，証明書 2 という）を新たに作成し，ブラウザに送る。L プロキシを利用した場合の HTTPS 通信を図 4 に示す。

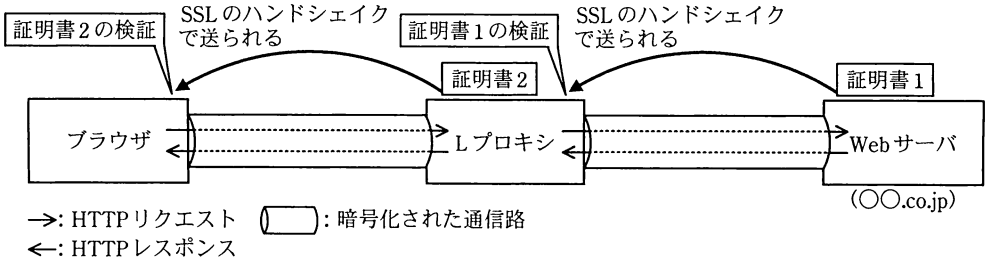

図 4　L プロキシを利用した場合の HTTPS 通信

ブラウザがLプロキシ経由でWebサーバとHTTPS通信を行うとき，ブラウザが暗号化してLプロキシに送信したデータはLプロキシで一旦復号される。Lプロキシでアクセスログの取得，送信内容の取得及びウイルスチェックが行われた後，送信データは再度暗号化されて，Webサーバに送信される。受信データについてもLプロキシで同様の処理が行われる。

〔HTTPS通信時の安全性の確認〕

K主任は，確認したLプロキシの仕様をS部長に説明した。次は，K主任とS部長の会話である。

S部長：HTTPS通信でWebサーバのサーバ証明書の正当性を確認しないまま，ブラウザがアクセスを継続すると，偽サイトに誘導された場合でなくても，［ a ］攻撃を受けて，通信を盗聴される可能性があるので，アクセスを許可してはいけない。そこで，まずLプロキシを利用したHTTPS通信時のサーバ証明書の検証について確認したい。Lプロキシでは二つのサーバ証明書を利用しているが，②ブラウザは証明書2の検証において，証明書2の正当性を確認できないのではないか。

K主任：ご指摘のとおり，事前に何の準備もしなかった場合は，証明書2の正当性を確認できません。証明書2の正当性を確認できるようにするためには，事前にブラウザで［ b ］必要があります。

S部長：証明書1の正当性はどこで確認するのかね。

K主任：証明書1の正当性はLプロキシで検証します。証明書1の正当性を確認できなかった場合のWebサーバへのアクセスの可否は，Lプロキシで設定できます。

S部長：なるほど。サーバ証明書の検証については問題なさそうだね。

情報システム部における検討結果を踏まえ，T社ではLプロキシを採用する方針とし，Lプロキシの導入に向けた動作検証を行うことにした。

設問1　T社におけるインターネットサイトへのアクセスについて，(1)～(3)に答えよ。

(1) 本文中の下線①について，T社がHTTPS通信によるアクセスを原則として禁止しているのは，どのような理由からか。20字以内で述べよ。

(2) 図2について，HTTPS通信を行うことで利用目的を達成できなくなるものはどれか。図2中の項番(1)～(5)から選び，全て答えよ。

(3) ブラウザのURL入力欄に次のURLを入力したときに，ブラウザがプロキシに最初に送信するHTTPメッセージのリクエストラインはどれか。解答群の中から選び，記号で答えよ。

入力したURL：https://○○.co.jp/index.html

解答群

ア　CONNECT ○○.co.jp:443 HTTP/1.1

イ　GET ○○.co.jp:443/index.html HTTP/1.1

ウ　POST ○○.co.jp:443/index.html HTTP/1.1

エ　SSL ○○.co.jp:443 HTTP/1.1

設問2　HTTPS通信時の安全性の確認について，(1)，(2)に答えよ。

(1) 本文中の［　a　］に入れる用語を答えよ。

(2) サーバ証明書の検証においてブラウザが確認すべき内容のうち，［　a　］攻撃のような攻撃への対策となるものを二つ挙げ，それぞれ35字以内で述べよ。

設問3　Lプロキシについて，(1)～(3)に答えよ。

(1) 本文中の［　b　］に入れる，事前にブラウザで実施することは何か。40字以内で述べよ。

(2) 本文中の下線②について，上記(1)を実施しないとブラウザが証明書2の正当性を確認できないのはなぜか。40字以内で述べよ。

(3) 図4中の証明書2について，Lプロキシ自身のサーバ証明書を利用するのではなく，Webサーバのサーバ証明書と同じコモンネームのサーバ証明書をLプロキシが新たに作成する必要があるのはなぜか。40字以内で述べよ。