問３　ローカルブレイクアウトによる負荷軽減に関する次の記述を読んで，設問に答えよ。

A 社は，従業員 300 人の建築デザイン会社である。東京本社のほか，大阪，名古屋，仙台，福岡の 4 か所の支社を構えている。本社には 100 名，各支社には 50 名の従業員が勤務している。

A 社は，インターネット上の C 社の SaaS（以下，C 社 SaaS という）を積極的に利用する方針にしている。A 社情報システム部ネットワーク担当の B さんは，C 社 SaaS 宛ての通信が HTTPS であることから，ネットワークの負荷軽減を目的に，各支社の PC から C 社 SaaS 宛ての通信を，本社のプロキシサーバを利用せず直接インターネット経由で接続して利用できるようにする，ローカルブレイクアウトについて検討することにした。

〔現在の A 社のネットワーク構成〕

現在の A 社のネットワーク構成を図 1 に示す。

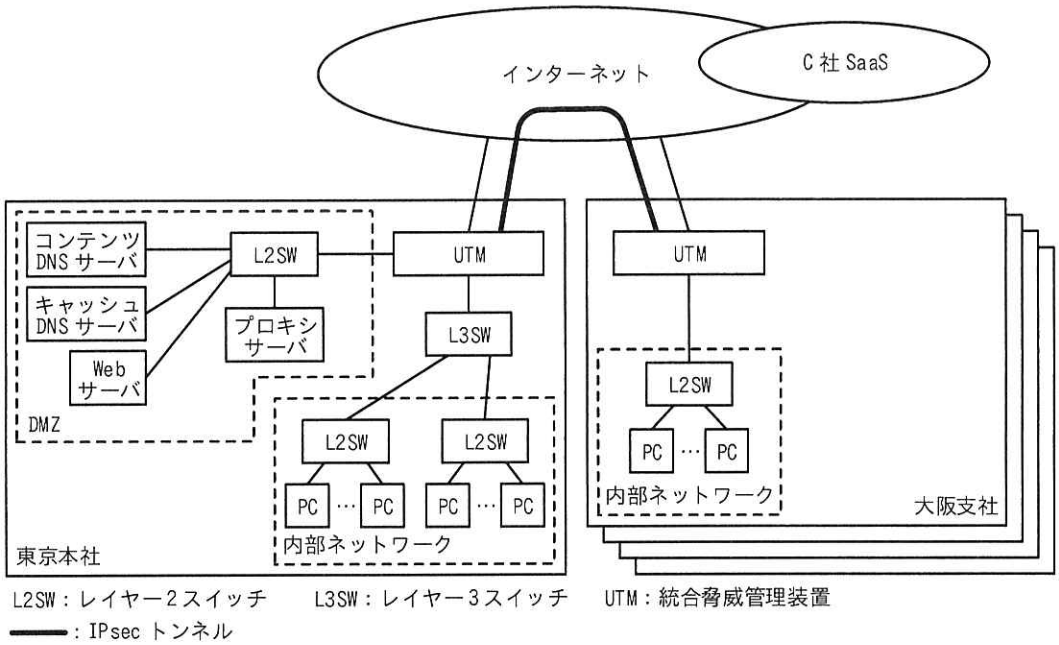

図 1　現在の A 社のネットワーク構成（抜粋）

現在のA社のネットワーク構成の概要を次に示す。

・本社及び各支社はIPsec VPN機能をもつUTMでインターネットに接続している。

・プロキシサーバは，従業員が利用するPCのHTTP通信，HTTPS通信をそれぞれ中継する。プロキシサーバではセキュリティ対策として各種ログを取得している。

・DMZや内部ネットワークではプライベートIPアドレスを利用している。

・PCには，DHCPを利用してIPアドレスの割当てを行っている。

・PCが利用するサーバは，全て本社のDMZに設置されている。

・A社からインターネット向けの通信については，本社のUTMでNAPTによるIPアドレスとポート番号の変換をしている。

〔現在のA社のVPN構成〕

A社は，UTMのIPsec VPN機能を利用して，本社をハブ，各支社をスポークとする［ア］型のVPNを構成している。本社と各支社との間のVPNは，IP in IP トンネリング（以下，IP-IPという）でカプセル化し，さらにIPsecを利用して暗号化することでIP-IP over IPsecインタフェースを構成し，2拠点間をトンネル接続している。①本社のUTMと支社のUTMのペアではIPsecで暗号化するために同じ鍵を共有している。②この鍵はペアごとに異なる値が設定されている。

③ IPsec の通信モードには，トランスポートモードとトンネルモードがあるが，A社のVPNではトランスポートモードを利用している。

A社のVPNを構成するIPパケット構造を図2に示す。

(1) 元のIPパケットをIP-IPでカプセル化したIPパケット

IPヘッダー	元のIPパケット	
	元のIPヘッダー	元のIPペイロード

(2) (1)のIPパケットを更にIPsecで暗号化したIPパケット

IPヘッダー	ESPヘッダー	元のIPパケット		ESPトレーラ	ESP認証データ
		元のIPヘッダー	元のIPペイロード		

注記　元のIPパケットは，DMZや内部ネットワークから送信されたIPパケットを示す。

図2　A社のVPNを構成するIPパケット構造

VPNを構成するために，本社と各支社のUTMには固定のグローバルIPアドレスを割り当てている。④IP-IP over IPsecインタフェースでは，IP Unnumbered 設定が行

われている。また，⑤ IP-IP over IPsec インタフェースでは，中継する TCP パケットの IP フラグメントを防止するための設定が行われている。

〔プロキシサーバを利用した制御〕

B さんが UTM について調べたところ，追加ライセンスを購入することでプロキシサーバ（以下，UTM プロキシサーバという）として利用できることが分かった。

B さんは，ネットワークの負荷軽減のために，各支社の PC から C 社 SaaS 宛ての通信は，各支社の UTM プロキシサーバをプロキシサーバとして指定することで直接インターネットに向けることを考えた。また，各支社の PC からその他インターネット宛ての通信は，通信相手を特定できないことから，各種ログを取得するために，これまでどおり本社のプロキシサーバをプロキシサーバとして指定することを考えた。各支社の PC から，C 社 SaaS 宛てとその他インターネット宛ての通信の流れを図 3 に示す。

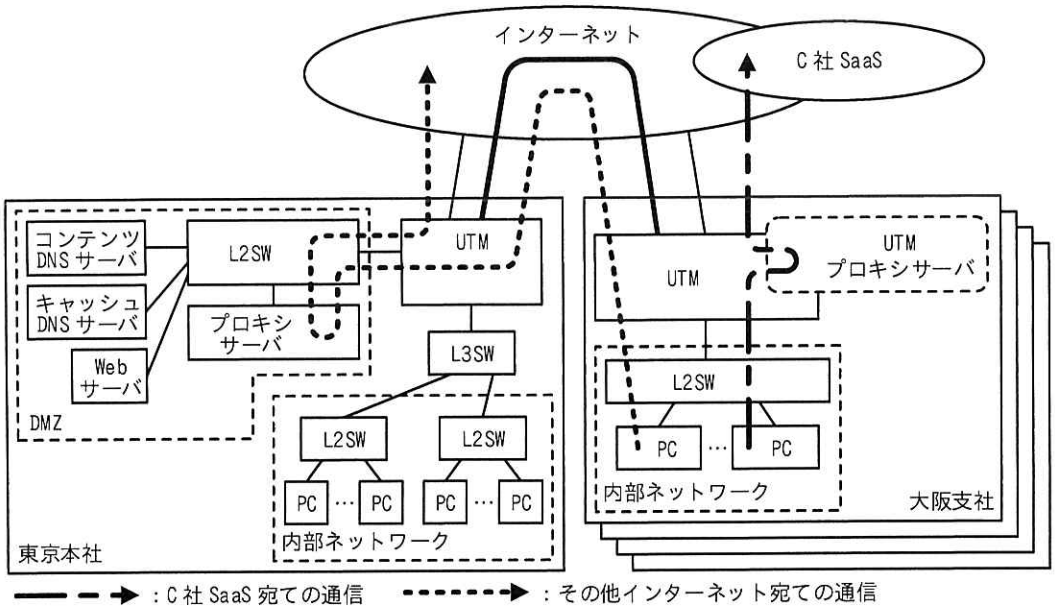

図 3　各支社の PC から，C 社 SaaS 宛てとその他インターネット宛ての通信の流れ

B さんは，各支社の PC が利用するプロキシサーバを制御するためにプロキシ自動設定（以下，PAC という）ファイルと Web プロキシ自動検出（以下，WPAD という）の

導入を検討することにした。

〔PAC ファイル導入検討〕

B さんは PAC ファイルの作成方法について調査した。PAC ファイルは JavaScript で記述する。PAC ファイルに記述する FindProxyForURL 関数の第 1 引数である url にはアクセス先の URL が，第 2 引数である host にはアクセス先の URL から取得したホスト名が渡される。これらの引数に渡された値を様々な関数を用いて条件分けし，利用するプロキシサーバを決定する。FindProxyForURL 関数の戻り値が“DIRECT”ならば，プロキシサーバを利用せず直接通信を行う。戻り値が“PROXY host:port”ならば，指定されたプロキシサーバ（host）のポート番号（port）を利用する。

テスト用に大阪支社の UTM を想定した PAC ファイルを作成した。B さんが作成した大阪支社の UTM の PAC ファイルを図 4 に示す。

```
function FindProxyForURL(url, host) {
  // (a)
  var ip = dnsResolve(host);

  // (b)
  if (localHostOrDomainIs(host, "localhost") ||
      isInNet(ip, "10.0.0.0", "255.0.0.0") ||
      isInNet(ip, "127.0.0.0", "255.0.0.0") ||
      isInNet(ip, "172.16.0.0", "255.240.0.0") ||
      isInNet(ip, "192.168.0.0", "255.255.0.0") ||
      dnsDomainIs(host, ".a-sha.jp")
      ) {
    return "DIRECT";
  }

  // (c)
  if (
      dnsDomainIs(host, "image.cdn.example") ||
      shExpMatch(host, "*.c-saas.example") ) {
      return "PROXY proxy.osaka.a-sha.jp:8080";
  }

  // (d)
  return "PROXY proxy.a-sha.jp:8080";
}
```

処理名	処理の説明文
(a)	host を IP アドレスに変換し，変数 ip に代入する。
(b)	host が localhost，又は(a)で宣言した ip がプライベート IP アドレスやループバックアドレス，又は host が A 社の社内利用ドメイン名に属する場合，FindProxyForURL 関数の戻り値として“DIRECT”を返す。
(c)	host が C 社 SaaS 利用ドメイン名に属する場合，又は host が C 社 SaaS 利用ドメイン名のシェルグロブ表現に一致する場合，FindProxyForURL 関数の戻り値として“PROXY proxy.osaka.a-sha.jp:8080”を返す。
(d)	(b)，(c)どちらにも該当しない場合，FindProxyForURL 関数の戻り値として“PROXY proxy.a-sha.jp:8080”を返す。

a-sha.jp：A 社の社内利用ドメイン名
proxy.a-sha.jp：本社のプロキシサーバの FQDN
proxy.osaka.a-sha.jp：大阪支社の UTM プロキシサーバの FQDN
image.cdn.example：C 社 SaaS 利用ドメイン名
c-saas.example：C 社 SaaS 利用ドメイン名

注記　説明文中の host は，引数 host に渡された値（ホスト名）を示す。

図 4　B さんが作成した大阪支社の UTM の PAC ファイル

Bさんは，テスト用のPCとテスト用のUTMプロキシサーバを用意し，作成したPACファイルを利用することで，テスト用のPC からC社SaaS宛ての通信が，期待どおりに本社のプロキシサーバを利用せずに，テスト用のUTMプロキシサーバを利用することを確認した。⑥Bさんは各支社のPACファイルを作成した。

〔WPAD導入検討〕

WPADは，［ イ ］や［ ウ ］の機能を利用して，PACファイルの場所を配布するプロトコルである。PCやWebブラウザのWebプロキシ自動検出が有効になっていると，［ イ ］サーバや［ ウ ］サーバと通信を行い，アプリケーションレイヤープロトコルの一つである［ エ ］を利用して［ エ ］サーバからPACファイルのダウンロードを試みる。

WPADの利用には，PCやWebブラウザのWebプロキシ自動検出を有効にするだけでよく，簡便である一方，悪意のある［ イ ］サーバや［ ウ ］サーバがあると⑦PCやWebブラウザが脅威にさらされる可能性も指摘されている。Bさんは，WPADは利用しないことにし，PCやWebブラウザのWebプロキシ自動検出を無効にすることにした。PCやWebブラウザには PACファイルの［ オ ］を直接設定する。

Bさんが検討した対応案が承認され，情報システム部はプロジェクトを開始した。

設問1　〔現在のA社のVPN構成〕について答えよ。

(1)　本文中の［ ア ］に入れる適切な字句を答えよ。

(2)　本文中の下線①について，本社のUTMと支社のUTMのペアで共有する鍵を何と呼ぶか答えよ。

(3)　本文中の下線②について，鍵は全て同じではなく，ペアごとに異なる値を設定することで得られる効果を，鍵の管理に着目して25字以内で答えよ。

(4)　本文中の下線③について，A社のVPNで利用しているトランスポートモードとした場合は元のIPパケット（元のIPヘッダーと元のIPペイロード）とESPトレーラの範囲を暗号化するのに対し，A社のVPNをトンネルモードとした場合はどの範囲を暗号化するか。図2中の字句で全て答えよ。

(5)　本文中の下線④について，IP Unnumbered設定とはどのような設定か。“IP

アドレスの割当て”の字句を用いて30字以内で答えよ。

(6) 本文中の下線⑤について，中継するTCPパケットのIPフラグメントを防止するための設定を行わず，UTMでIPフラグメント処理が発生する場合，UTMにどのような影響があるか。10字以内で答えよ。

設問2 〔PACファイル導入検討〕について答えよ。

(1) 図4について，DMZにあるWebサーバにアクセスする際，プロキシサーバを利用する場合はプロキシサーバ名を答えよ。プロキシサーバを利用しない場合は“利用しない”と答えよ。

(2) 図4について，インターネット上にあるhttps://www.example.com/foo/index.htmlにアクセスする際，プロキシサーバを利用する場合はプロキシサーバ名を答えよ。プロキシサーバを利用しない場合は“利用しない”と答えよ。

(3) 図4について，isInNet(ip, “172.16.0.0”, “255.240.0.0”)のアドレス空間は，どこからどこまでか。最初のIPアドレスと最後のIPアドレスを答えよ。

(4) 図4について，変数ipがプライベートIPアドレスの場合，戻り値を“DIRECT”にすることで得られる効果を，“負荷軽減”の字句を用いて20字以内で答えよ。

(5) 本文中の下線⑥について，PACファイルは支社ごとに用意する必要がある理由を25字以内で答えよ。

設問3 〔WPAD導入検討〕について答えよ。

(1) 本文中の［ イ ］～［ オ ］に入れる適切な字句を答えよ。

(2) 本文中の下線⑦について，どのような脅威があるか。25字以内で答えよ。