NW

令和６年度　春期
ネットワークスペシャリスト試験
午後Ⅰ　問題

試験時間	12:30 ～ 14:00（1 時間 30 分）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. 答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。
4. 問題は，次の表に従って解答してください。

問題番号	問１～問３
選択方法	２問選択

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B 又は HB の黒鉛筆又はシャープペンシルを使用してください。
   (2) 受験番号欄に受験番号を，生年月日欄に受験票の生年月日を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) 選択した問題については，次の例に従って，選択欄の問題番号を○印で囲んでください。○印がない場合は，採点されません。3 問とも○印で囲んだ場合は，はじめの 2 問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問１，問３を選択した場合の例〕

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

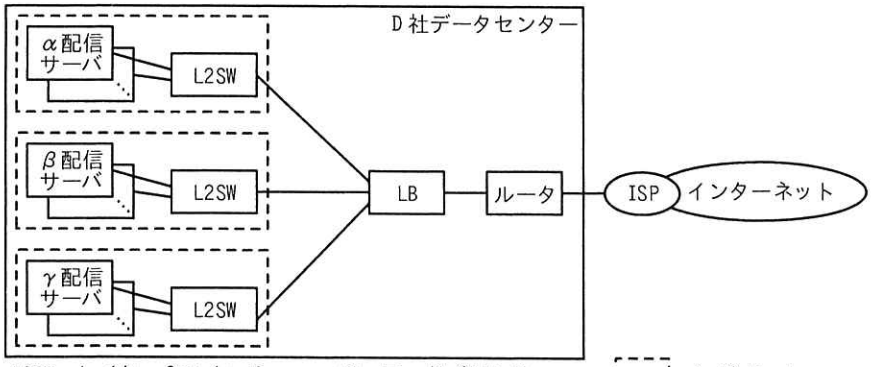
問1　コンテンツ配信ネットワークに関する次の記述を読んで，設問に答えよ。

D 社は，ゲームソフトウェア開発会社で三つのゲーム（ゲームα，ゲームβ，ゲームγ）をダウンロード販売している。D 社のゲームはいずれも利用者の操作するゲーム端末上で動作し，ゲームの進捗データやスコアはゲーム端末内に暗号化して保存される。D 社のゲームは世界中に利用者がおり，ゲーム本体及びゲームのシナリオデータ（以下，両方をゲームファイルという）はインターネット経由で配信されている。

〔現状の配信方式〕

D 社は，ゲームファイルの配信のためのデータセンターを所有している。

D 社データセンターの構成を図 1 に示す。



注記　α配信サーバは，ゲームαのゲームファイルを配信するサーバである（β，γも同様）。

図 1　D 社データセンターの構成（抜粋）

ゲーム端末は，インターネット経由でゲームごとにそれぞれ異なる URL に HTTPS でアクセスする。LB は，プライベート IP アドレスが設定された HTTP の配信サーバにアクセスを振り分ける。また，①LB は配信サーバに HTTP アクセスによって死活確認を行い，動作が停止している配信サーバに対してはゲーム端末からのアクセスを振り分けない。

ゲームファイルの配信に利用する IP アドレスとポート番号を，表 1 に示す。

表1　ゲームファイルの配信に利用するIPアドレスとポート番号

内容	URL	LB		配信サーバ	
		IPアドレス	ポート	所属セグメント	ポート
ゲームα	https://alpha.example.net/	203.x.11.21	443	172.21.1.0/24	80
ゲームβ	https://beta.example.net/	203.x.11.21	443	172.22.1.0/24	80
ゲームγ	https://gamma.example.net/	203.x.11.21	443	172.23.1.0/24	80

注記　203.x.11.21はグローバルIPアドレス

D社が導入しているLBのサーバ振分けアルゴリズムには，ラウンドロビン方式及び最少接続数方式がある。ラウンドロビン方式は，ゲーム端末からの接続を接続ごとに配信サーバに順次振り分ける方式である。最少接続数方式は，ゲーム端末からの接続をその時点での接続数が最も少ない配信サーバに振り分ける方式である。

D社のゲームファイル配信では，振り分ける先の配信サーバの性能は同じだが，接続ごとに配信するゲームファイルのサイズに大きなばらつきがあり，配信に掛かる時間が変動する。各配信サーバへの同時接続数をなるべく均等にするために，LBの振分けアルゴリズムとして［　ア　］方式を採用している。

ゲームβの配信性能向上が必要になる場合には，表1中の所属セグメント［　イ　］にサーバを増設する。

〔配信方式の見直し〕

D社は，ゲームファイルの大容量化と利用者のグローバル化に伴い，ゲームファイルの配信をコンテンツ配信ネットワーク（以下，CDNという）事業者のE社のサービスで行うことにした。

E社CDNは，多数のキャッシュサーバを設置する配信拠点（以下，POPという）を複数もち，その中から，ゲーム端末のインターネット上の所在地に対して最適なPOPを配信元としてコンテンツを配信する。

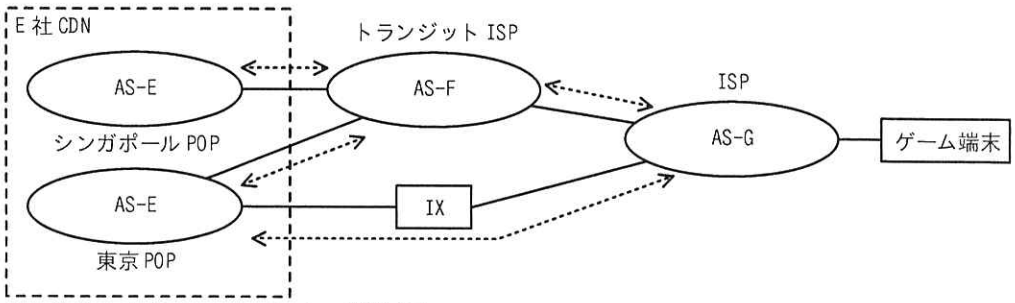
あるPOPが端末からアクセスを受けると，POP内でLBがキャッシュサーバにアクセスを振り分ける。E社CDNのキャッシュサーバにコンテンツが存在しない場合は，D社データセンターの配信サーバからE社CDNのキャッシュサーバにコンテンツが同期される。

配信方式の見直しプロジェクトはXさんが担当することになった。Xさんは，E社

が提供している BGP anycast 方式の POP 選択方法を調査した。X さんが E 社からヒアリングした内容は次のとおりである。

E 社 BGP anycast 方式では，同じアドレスブロックを同じ AS 番号を用いてシンガポール POP 及び東京 POP の両方から BGP で経路広告する。シンガポール POP と東京 POP の間は直接接続されていない。ゲーム端末が接続する ISP では，E 社 AS の経路情報を複数の隣接した AS から受信する。どの経路情報を採用するかは BGP の経路選択アルゴリズムで決定される。ゲーム端末からの HTTPS リクエストのパケットは，決定された経路で隣接の AS に転送される。

BGP anycast 方式による E 社の経路広告イメージを図 2 に示す。



IX：Internet Exchange　<----> : BGP ピア

注記　AS-E は E 社の AS，AS-G はゲーム端末が接続する ISP の AS を示す。

図 2　BGP anycast 方式による E 社の経路広告イメージ

図 2 で IX は，レイヤー2 ネットワーク相互接続点であり，接続された隣接の AS 同士が BGP で直接接続することができる。

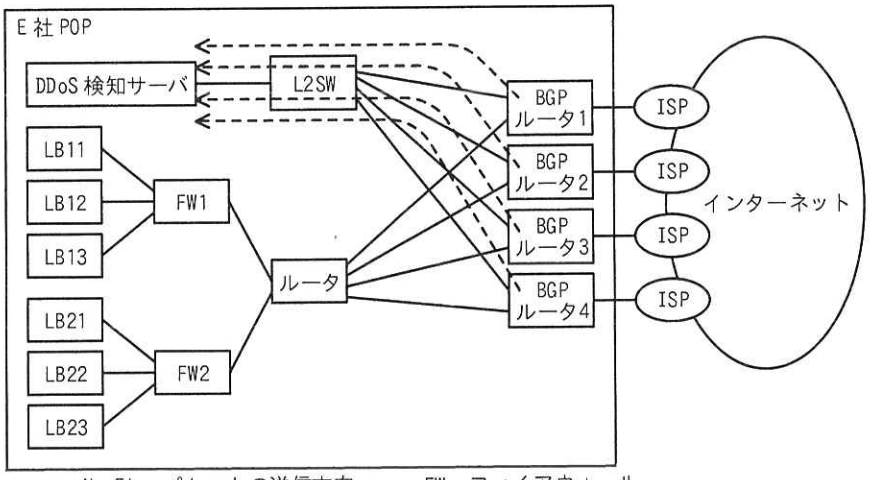
BGP での経路選択では，LP（LOCAL_PREF）属性については値が［　ウ　］経路を優先し，MED（MULTI_EXIT_DISC）属性については値が［　エ　］経路を優先する。E 社では，LP 属性と MED 属性が経路選択に影響を及ぼさないように設定している。これによって②E 社のある POP からゲーム端末へのトラフィックの経路は，その POP の BGP ルータが受け取る AS Path 長によって選択される。

X さんは，BGP のセキュリティ対策として何を行っているか，E 社の担当者に確認した。E 社 BGP ルータは，③隣接 AS の BGP ルータと MD5 認証のための共通のパスワードを設定していると説明を受けた。また，④アドレスブロックや AS 番号を偽った不正な経路情報を受け取らないための経路フィルタリングを行っていると説明があっ

た。

〔配信拠点の保護〕

D社ではDDoS攻撃を受けることが何度かあった。そこでXさんは，コンテンツ配信サーバへのDDoS攻撃対策について，どのような対策を行っているかE社の担当者に確認したところ，E社ではRFC 5635の中で定義されたDestination Address RTBH (Remote Triggered Black Hole) Filtering（以下，RTBH方式という）のDDoS遮断システムを導入しているとの回答があった。E社POPの概要を図3に示す。



<---：NetFlowパケットの送信方向　　FW：ファイアウォール

注記　装置間の接続とISPの接続は，全て10Gビットイーサネットである。

図3　E社POPの概要（抜粋）

E社のDDoS遮断システムは，RFC 3954で定義されるNetFlowで得た情報を基にDDoS攻撃の宛先IPアドレスを割り出し，該当IPアドレスへの攻撃パケットを廃棄することで，ほかのIPアドレスへの通信に影響を与えないようにする。DDoS検知サーバは，E社POP内の各BGPルータとiBGPピアリングを行っている。

E社のBGPルータは，インターネット側インタフェースから流入するパケットの送信元と宛先のIPアドレス，ポート番号などを含むNetFlowパケットを生成する。生成されたNetFlowパケットはDDoS検知サーバに送信される。DDoS検知サーバは，送られてきたNetFlowパケットを基に独自アルゴリズムでDDoS攻撃の有無を判断し，攻撃を検知した場合はDDoS攻撃の宛先IPアドレスを取得する。

DDoS検知サーバは，検知したDDoS攻撃の宛先IPアドレスへのホスト経路を生成しRTBH方式の対象であることを示すBGPコミュニティ属性を付与して各BGPルータに経路広告する。RTBH方式の対象であることを示すBGPコミュニティ属性が付いたホスト経路を受け取った各BGPルータは，そのホスト経路のネクストホップを廃棄用インタフェース宛てに設定することで，DDoS攻撃の宛先IPアドレス宛ての通信を廃棄する。

DDoS遮断システムの今後の開発予定をE社技術担当者に確認したところ，RFC 8955で定義されるBGP Flowspecを用いる対策（以下，BGP Flowspec方式）をE社が提供する予定であることが分かった。

BGP Flowspec方式では，DDoS検知サーバからのiBGPピアリングで，DDoS攻撃の宛先IPアドレスだけではなく，DDoS攻撃の送信元IPアドレス，宛先ポート番号などを組み合わせてBGPルータに広告して該当の通信をフィルタリングすることができる。

Xさんは，⑤BGP Flowspec方式の方が有用であると考え，E社技術担当者に早期提供をするよう依頼した。

Xさんは，E社CDNとDDoS遮断システムを導入する計画を立て，計画はD社内で承認された。

設問1　〔現状の配信方式〕について答えよ。

(1)　本文中の下線①について，HTTPではなくICMP Echoで死活確認を行った場合どのような問題があるか。50字以内で答えよ。

(2)　本文中の［　ア　］に入れる適切な字句を，本文中から選んで答えよ。また，本文中の［　イ　］に入れる適切なセグメントを，表1中から選んで答えよ。

(3)　HTTPSに必要なサーバ証明書はどの装置にインストールされているか。必ず入っていなければならない装置を一つだけ選び，図1中の字句で答えよ。

設問2　〔配信方式の見直し〕について答えよ。

(1)　本文中の［　ウ　］，［　エ　］に入れる適切な字句を，“大きい”，“小さい”のいずれかから選んで答えよ。

(2)　本文中の下線②について，図2でAS-E東京POPにAS-GからのHTTPSリク

エストのパケットが届く場合，E 社トラフィックはどちらの経路から配信されるか。途中通過する場所を，図2中の字句で答えよ。ここで，AS Path 長以外は経路選択に影響せず，途中に無効な経路や経路フィルタリングはないものとする。

(3) 本文中の下線③の設定をすることで何を防いでいるか。“BGP”という字句を用いて 10 字以内で答えよ。

(4) 本文中の下線④について，フィルタリングせずに不正な経路を受け取った場合に，コンテンツ配信に与える悪影響を“不正な経路”という字句を用いて 40 字以内で答えよ。

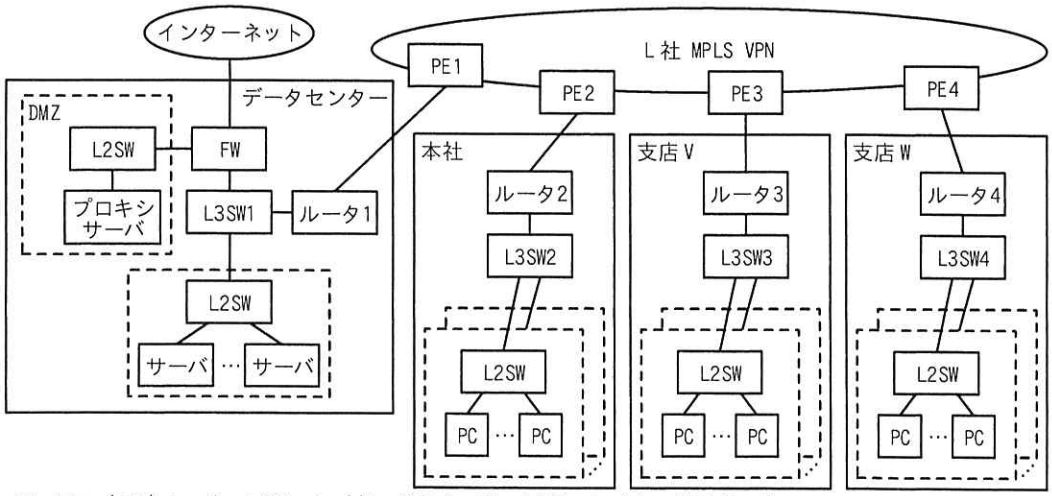
設問3 〔配信拠点の保護〕について答えよ。

(1) 図3において，インターネットから BGP ルータ 1 を経由して LB11 に HTTPS Flood 攻撃があったとき，FW1 でフィルタリングする方式と比較した RTBH 方式の長所は何か。30 字以内で答えよ。

(2) 本文中の下線⑤について，RTBH 方式と比較した BGP Flowspec 方式の長所は何か。30 字以内で答えよ。

問２　SD-WAN による拠点接続に関する次の記述を読んで，設問に答えよ。

G 社は，本社とデータセンター及び二つの支店をもつ企業である。G 社では，業務拡大による支店の追加が計画されている。支店の追加によるネットワーク構成の変更について，SD-WAN を活用することで，設定作業を行いやすくするとともに WAN の冗長化も行うという改善方針が示された。そこで，情報システム部の J さんが設計担当としてアサインされ，対応することになった。G 社の現行ネットワーク構成を図 1 に示す。



FW：ファイアウォール　L2SW：レイヤー２スイッチ　L3SW：レイヤー３スイッチ
PE：プロバイダエッジルータ　MPLS VPN：MPLS VPN サービス網
注記　[ ]はサブネットを示す。

図 1　G 社の現行ネットワーク構成（抜粋）

〔現行ネットワーク概要〕

G 社の現行ネットワーク概要を次に示す。

・G 社には，データセンター，本社，支店 V 及び支店 W の四つの拠点がある。これらの拠点は，L 社が提供する MPLS VPN（以下，L 社 VPN という）を介して相互に接続している。

・各拠点の PC とサーバは，データセンターのプロキシサーバを経由してインターネットへアクセスする。

・データセンターの FW は，パケットフィルタリングによるアクセス制御を行ってい

る。

・PE1～4は，L社VPNの顧客のネットワークを収容するために設置した，プロバイダエッジルータ（以下，PEルータという）である。

・ルータ 1～4 は，拠点間を接続する機器であり，L 社の PE ルータと対向する［ア］エッジルータである。

・L社のPEルータは，G社との間のBGPピアにas-overrideを設定している。この設定によって，G社の複数の拠点で同一のAS番号を用いる構成が可能になっている。一般に，PE ルータにおける as-override 設定の有無によって，経路情報交換の処理をする際にやり取りされる経路情報が異なったものとなる。例えば，本社のルータ2に届く支店Vの経路情報は，① as-override設定の有無で表1となる。② G社現行ネットワークで利用している各拠点のIPアドレスとAS番号を表2に示す。

表1　本社のルータ2に届く支店Vの経路情報

	Prefix	AS PATH
as-override設定無し	a	64500　65500
as-override設定有り	a	b

注記　64500は，L社VPNのAS番号である。

表2　各拠点のIPアドレスとAS番号一覧

ネットワーク	IPアドレス	AS番号
データセンター	10.1.0.0/16	c
DMZ	x.y.z.0/28	
本社	10.2.0.0/16	d
支店V	10.3.0.0/16	e
支店W	10.4.0.0/16	f

注記　x.y.z.0は，グローバルアドレスを示す。

〔現行の経路制御概要〕

G社の現行の経路制御の概要を次に示す。

・拠点内は，OSPFによって経路制御を行っている。

・拠点間は，BGP4によって経路制御を行っている。

・OSPF エリアは全てエリア 0 である。

・ルータ 1～4 で二つのルーティングプロトコル間におけるルーティングを可能にするために，経路情報の［　イ　］をしている。このとき，一方のルーティングプロトコルで学習された経路がもう一方のルーティングプロトコルを介して③再び同じルーティングプロトコルに渡されることのないように経路フィルターが設定されている。

・全拠点からインターネットへの http/https 通信ができるように，［　ウ　］のサブネットを宛先とする経路を OSPF で配布している。この経路情報は，途中 BGP4 を経由して，④3 拠点（本社，支店 V，支店 W）のルータ及び L3SW に届く。

・BGP4 において，AS 内部の経路交換は iBGP が用いられるのに対し，各拠点のルータと PE ルータとの経路交換では［　エ　］が用いられる。

・L 社 VPN と接続するために，AS 番号 65500 が割り当てられている。この AS 番号はインターネットに接続されることのない AS のために予約されている番号の範囲に含まれる。このような AS 番号を［　オ　］AS 番号という。

・L 社 VPN の AS 番号は 64500 である。

〔SD-WAN 導入検討〕

J さんは，SD-WAN を取り扱っているネットワーク機器ベンダーK 社の技術者に相談しながら検討することにした。また，K 社がインターネット経由でクラウドサービスとして提供している SD-WAN コントローラーの活用を検討することにした。

K 社の SD-WAN 装置と SD-WAN コントローラーの主な機能を次に示す。

・SD-WAN コントローラーは，SD-WAN 装置に対して独自プロトコルを利用して，オーバーレイ構築に必要な情報の収集と配布を行うことで，複数の SD-WAN 装置を集中管理する。

・アンダーレイネットワークとして，MPLS VPN とインターネット回線が利用可能である。

・オーバーレイネットワークは，SD-WAN 装置間の IPsec トンネルで構築される。IPsec トンネルの確立では SD-WAN 装置の IP アドレスが用いられる。IPsec トンネルの端点を TE（Tunnel Endpoint）と呼ぶ。

・オーバーレイネットワークは，アプリケーショントラフィックを識別したルーテ

ィングを行う。このように，アプリケーショントラフィックを識別したルーティングを［　カ　］ルーティングという。

・SD-WAN コントローラーが SD-WAN 装置に配布する主な情報は，SD-WAN 装置ごとのオーバーレイの経路情報と，⑤ IPsec トンネルを構築するために必要な情報の 2 種類がある。

・SD-WAN コントローラーと SD-WAN 装置間の通信は TLS で保護される。

・SD-WAN 装置は，VRF（Virtual Routing and Forwarding）による独立したルーティングインスタンス（以下，RI という）を複数もつ。そのうちの一つの RI はコントロールプレーンで用いられ，他の RI はデータプレーンで用いられる。

・SD-WAN 装置は，RFC 5880 で規定された BFD（Bidirectional Forwarding Detection）機能を有する。

J さんは，K 社の SD-WAN を G 社ネットワークへ導入する方法を検討し，実施する項目として次のとおりポイントをまとめた。

・各拠点のルータを K 社の提供する SD-WAN 装置に置き換える。各拠点の SD-WAN 装置を 2 台構成とする冗長化は次フェーズで検討する。

・SD-WAN 装置の設定については，K 社がクラウドサービスとして利用者に提供する SD-WAN コントローラーで集中管理する。

・拠点ごとに新規にインターネット接続回線を契約し，SD-WAN 装置に接続する。

・拠点の SD-WAN 装置間に，インターネット経由と L 社 VPN 経由で IPsec トンネルを設定する。

・⑥拠点の SD-WAN 装置のトンネルインタフェースで，BFD を有効化する。

・全体的な経路制御は SD-WAN コントローラーと SD-WAN 装置で行う。

・PC からインターネットへのアクセスは現行のままデータセンターのプロキシサーバ経由とし，各拠点から直接インターネットアクセスできるようにすることは次フェーズで検討する。

J さんが検討した，G 社の SD-WAN 装置導入後のネットワーク構成を図 2 に示す。

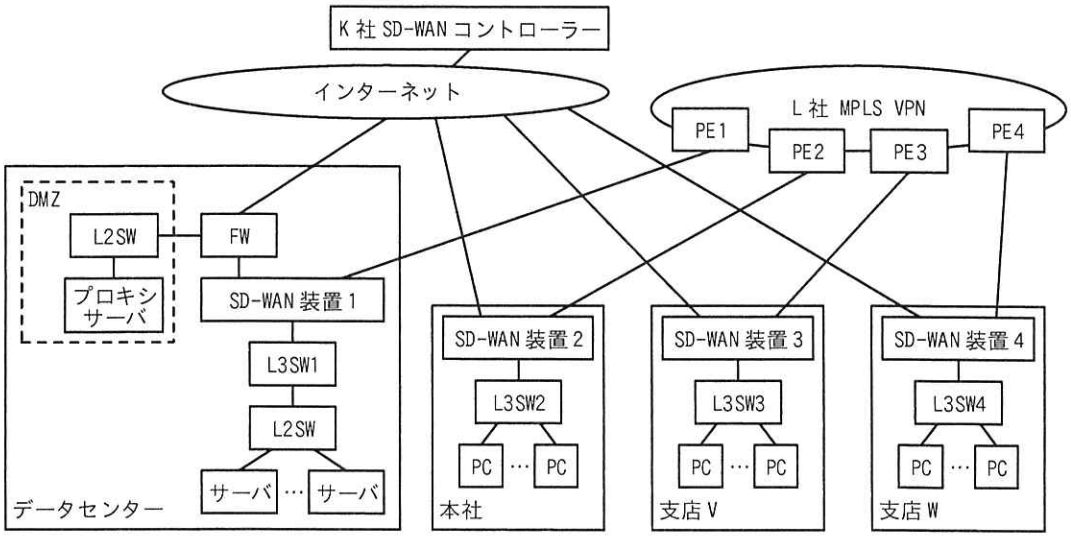


図 2　G 社の SD-WAN 装置導入後のネットワーク構成（抜粋）

〔SD-WAN トンネル検討〕

J さんは，図 2 のネットワーク構成における SD-WAN 装置間の IPsec トンネルの構成について検討した。J さんが考えた SD-WAN 装置間の IPsec トンネルの構成を図 3 に示す。

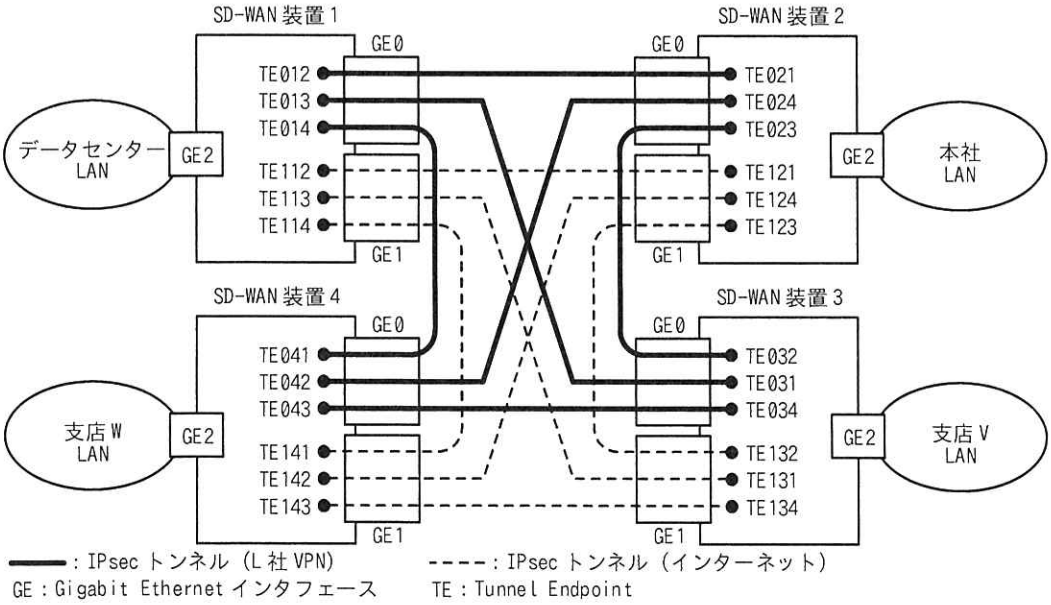


図 3　J さんが考えた SD-WAN 装置間の IPsec トンネルの構成

Jさんは，このIPsecトンネルの構成を前提として，今後設計するSD-WANの動作を次のようにまとめた。

・SD-WANコントローラーは，各拠点のSD-WAN装置から経路情報を受信し，それらにポリシーを適用して，全拠点のSD-WAN装置に経路情報をアドバタイズする。
・このときアドバタイズされる経路情報は，SD-WAN装置にローカルに接続されたネットワーク情報とそれぞれのSD-WAN装置がもつTE情報である。
・拠点間の通信は，⑦L社VPNを優先的に利用し，L社VPNが使えないときはインターネットを経由する。

Jさんは，これらの検討結果を基に報告を行い，SD-WAN導入の方針が承認された。

設問1　本文中の［　ア　］～［　カ　］に入れる適切な字句を答えよ。

設問2　〔現行ネットワーク概要〕について答えよ。

(1)　本文中の下線①について，as-override設定の前後における経路情報の違いについて，表1中の［　a　］，［　b　］を埋めて表を完成させよ。

(2)　本文中の下線②について，G社現行ネットワークで用いられているAS番号は何か。表2中の［　c　］～［　f　］を埋めて表を完成させよ。

設問3　〔現行の経路制御概要〕について答えよ。

(1)　本文中の下線③について，経路フィルターによって防止することが可能な障害を20字以内で答えよ。

(2)　本文中の下線④について，3拠点のL3SWにこの経路情報が届いたときのOSPFのLSAのタイプを答えよ。また，支店VのL3SW3にこのLSAが到達したとき，そのLSAを生成した機器は何か。図1中の機器名で答えよ。

設問4　〔SD-WAN導入検討〕について答えよ。

(1)　本文中の下線⑤について，SD-WANコントローラーから送られる情報を二つ挙げ，それぞれ25字以内で答えよ。

(2)　本文中の下線⑥について，トンネルインタフェースにBFDを設定する目的を，“IPsecトンネル”という用語を用いて35字以内で答えよ。

設問5　〔SD-WANトンネル検討〕について答えよ。

(1)　本文中の下線⑦について，通常時に本社のPCから支店VのPCへの通信が

通過するTEはどれか。図3中の字句で全て答えよ。

(2) (1)において支店Vの L 社 VPN 接続回線に障害があった場合，本社の PC から支店Vの PC への通信が通過する TE はどれか。図3中の字句で全て答えよ。

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。

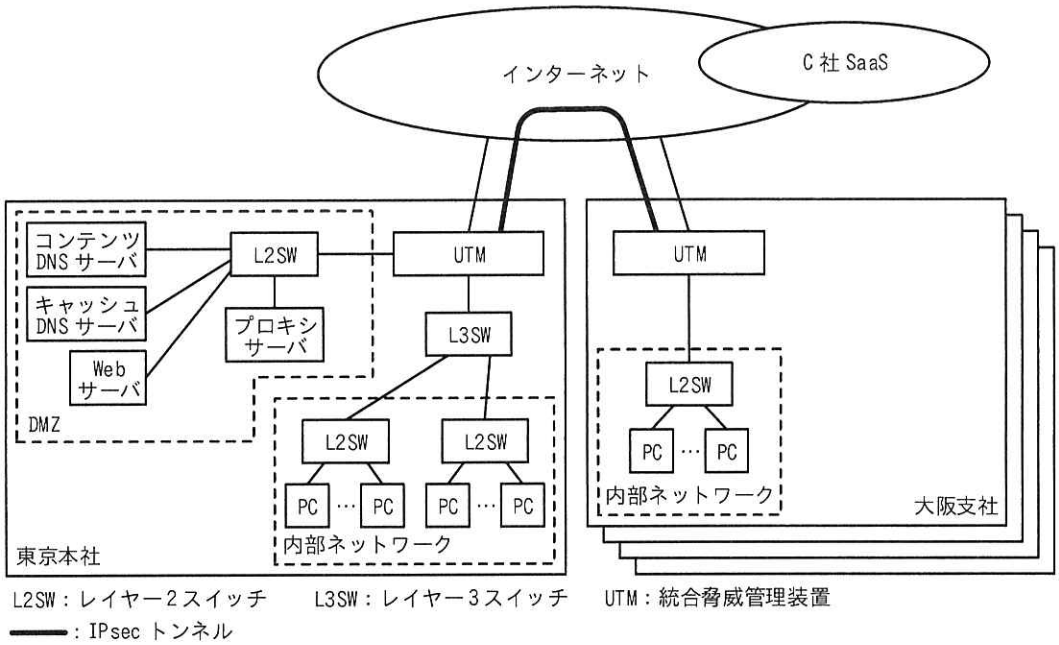


図 1　現在の A 社のネットワーク構成（抜粋）

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。

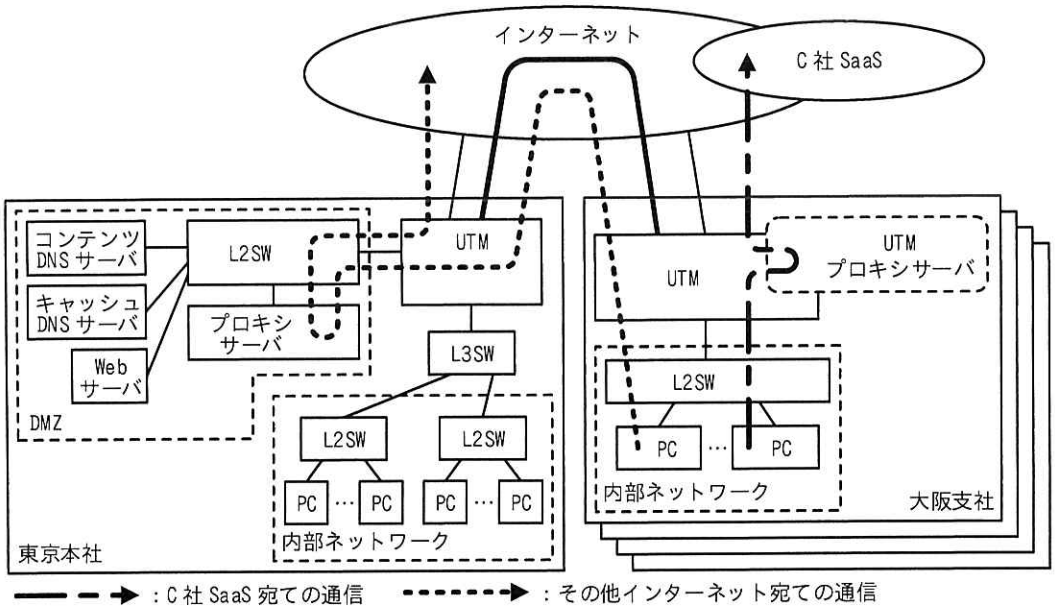


図 3　各支社の PC から，C 社 SaaS 宛てとその他インターネット宛ての通信の流れ

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。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 退室可能時間中に退室する場合は，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	13:10 ～ 13:50

7. 問題に関する質問にはお答えできません。文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，次のものに限ります。

   なお，会場での貸出しは行っていません。

   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。
13. 午後 II の試験開始は 14:30 ですので，14:10 までに着席してください。