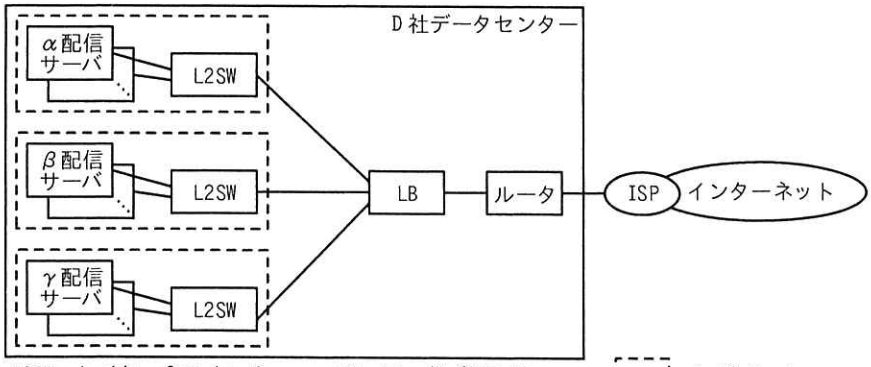
問1　コンテンツ配信ネットワークに関する次の記述を読んで，設問に答えよ。

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。

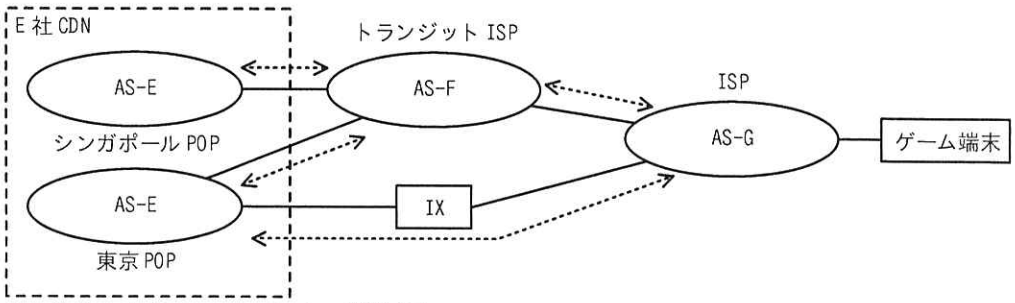
あるPOPが端末からアクセスを受けると，POP内でLBがキャッシュサーバにアクセスを振り分ける。E社CDNのキャッシュサーバにコンテンツが存在しない場合は，D社データセンターの配信サーバからE社CDNのキャッシュサーバにコンテンツが同期される。

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。

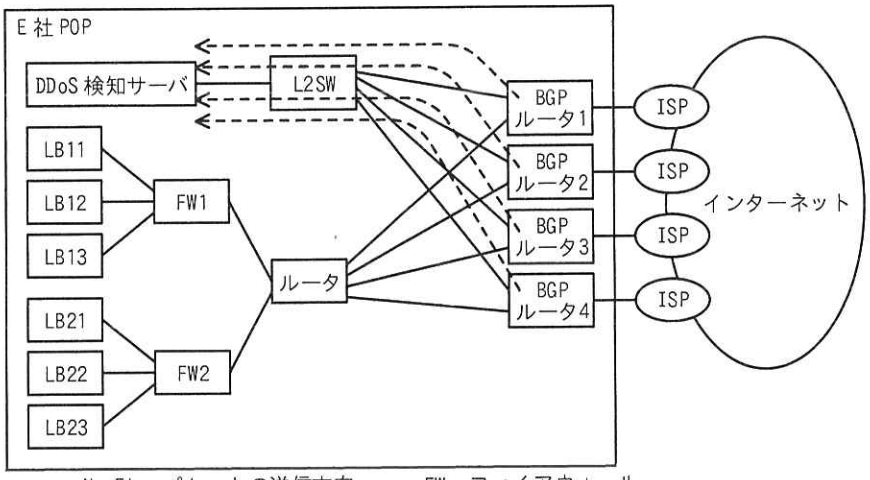
BGP での経路選択では，LP（LOCAL_PREF）属性については値が［　ウ　］経路を優先し，MED（MULTI_EXIT_DISC）属性については値が［　エ　］経路を優先する。E 社では，LP 属性と MED 属性が経路選択に影響を及ぼさないように設定している。これによって②E 社のある POP からゲーム端末へのトラフィックの経路は，その POP の BGP ルータが受け取る AS Path 長によって選択される。

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。