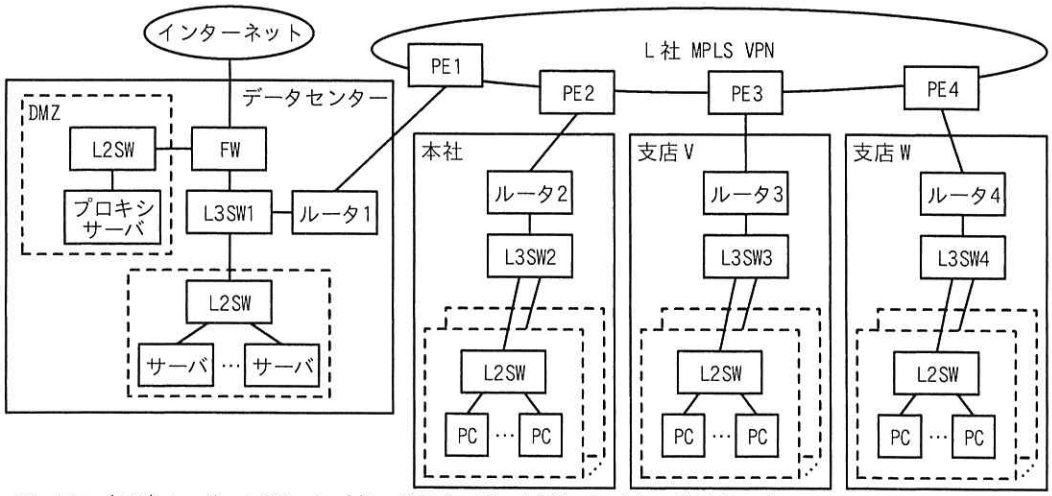
問２　SD-WAN による拠点接続に関する次の記述を読んで，設問に答えよ。

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。

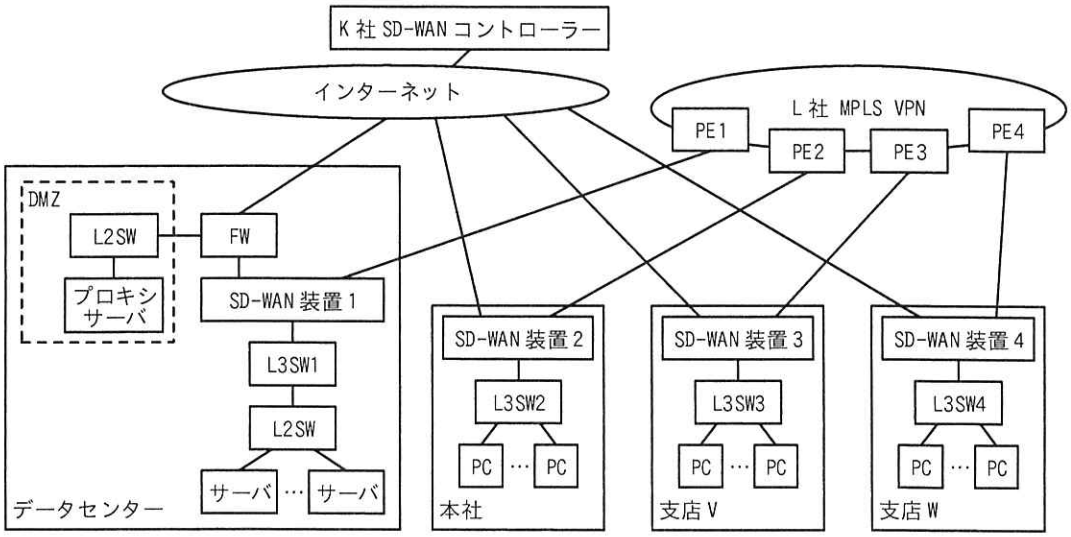


図 2　G 社の SD-WAN 装置導入後のネットワーク構成（抜粋）

〔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。

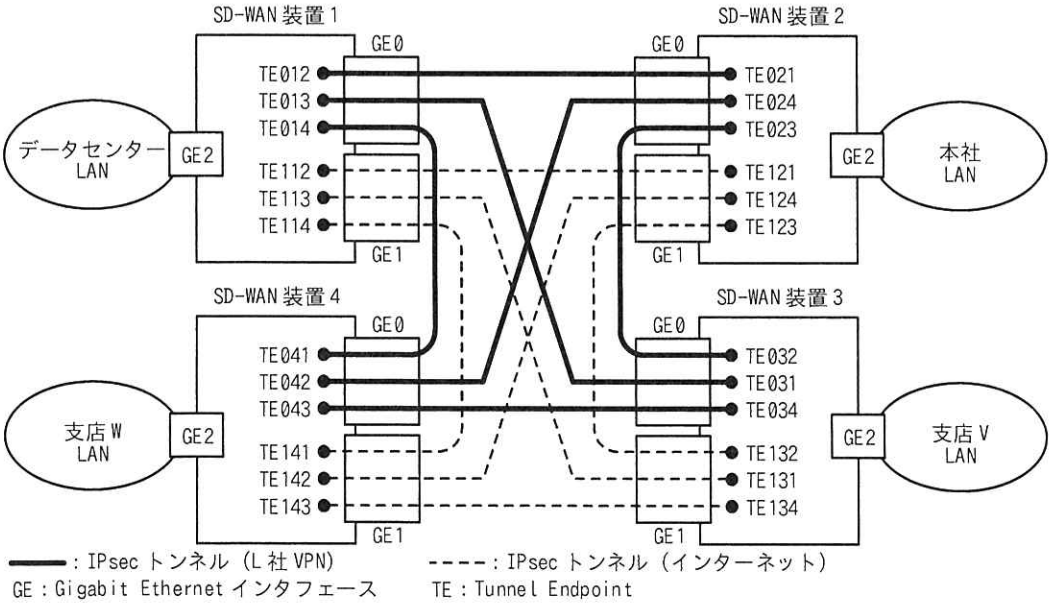


図 3　J さんが考えた SD-WAN 装置間の IPsec トンネルの構成

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。