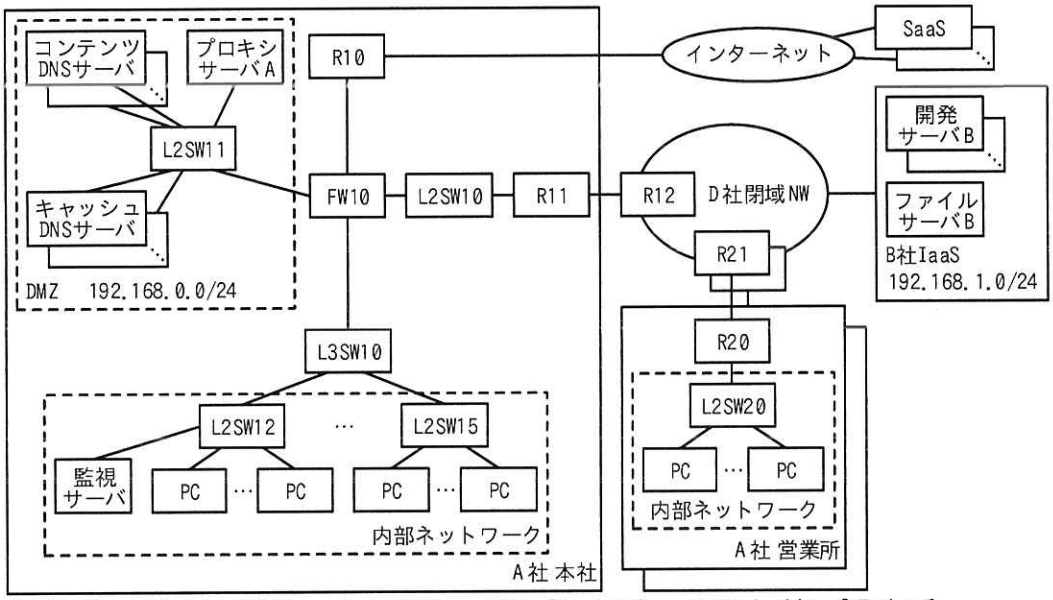
問１　マルチクラウド利用による可用性向上に関する次の記述を読んで，設問に答えよ。

A 社は，従業員 500 人のシステム開発会社である。A 社では，IaaS を積極的に活用して開発業務を行ってきたが，利用している IaaS 事業者である B 社で大規模な障害が発生し，開発業務に多大な影響を受けた。A 社のシステム部では，利用する IaaS 事業者をもう 1 社追加してマルチクラウド環境にし，本社を中心にネットワーク環境も含めた可用性向上に取り組むことになり，E さんを担当者として任命した。

現在の A 社のネットワーク構成を図 1 に示す。



R：ルータ　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
D 社閉域 NW：回線事業者である D 社が提供する閉域ネットワークサービス

図 1　現在の A 社のネットワーク構成（抜粋）

図 1 の概要を次に示す。

・A 社は本社と 2 か所の営業所で構成されている。

・D 社閉域 NW を利用して，本社と 2 か所の営業所を接続している。R11 及び R20 といった A 社と D 社閉域 NW とを接続するルータは，D 社からネットワークサービスとして提供されている。

・D 社閉域 NW と B 社 IaaS は相互接続しており，A 社は D 社閉域 NW 経由で B 社 IaaS

を利用している。

・A 社ネットワークでは静的経路制御を利用している。

・B 社からは，Web ブラウザを利用した画面操作によって，IaaS 上に仮想ネットワーク，仮想サーバを簡単に構築できる管理コンソールが提供されている。

・A 社のシステム部は，受託した開発業務ごとに開発サーバ B を構築し，A 社の担当部門に引き渡している。開発サーバ B の運用管理は担当部門で実施する。

・システム部は，共用のファイルサーバ B を構築し，A 社の全部門に提供している。

・A 社の全部門で利用する電子メールやチャット，スケジューラーなどのオフィスアプリケーションソフトウェアはインターネット上の SaaS を利用している。これらの SaaS は HTTPS 通信を用いている。

・A 社の一部の部門では，担当する業務に応じてインターネット上の SaaS を独自に契約し，利用している。これらの SaaS では送信元 IP アドレスによってアクセス制限をしているものもある。これらの SaaS も HTTPS 通信を用いている。

・プロキシサーバ A は，従業員が利用する PC やサーバからインターネット向けの HTTP 通信，HTTPS 通信をそれぞれ中継する。従業員はプロキシサーバとして proxy.a-sha.co.jp を PC の Web ブラウザやサーバに指定している。

・A 社は，本社設置の R10 を経由してインターネットに接続している。FW10 にはグローバル IP アドレスを付与しており，FW10 を経由するインターネット宛ての通信は NAPT 機能によって IP アドレスとポート番号の変換が行われる。

・キャッシュ DNS サーバは，PC やサーバからの問合せを受け，ほかの DNS サーバへ問い合わせた結果を応答する。キャッシュ DNS サーバは複数台設置されている。

・コンテンツ DNS サーバは，PC やサーバのホスト名などを管理し，PC やサーバなどに関する情報を応答する。コンテンツ DNS サーバは複数台設置されている。

・監視サーバは，ICMP を利用する死活監視（以下，ping 監視という）を用いて DMZ や IaaS にあるサーバの監視を行っている。監視サーバで検知された異常はシステム部の担当者に通知され，復旧作業などの必要な対応が行われる。

システム部では，ネットワーク環境の可用性向上の要件を次のとおりまとめた。

・新規に C 社の IaaS を契約し，B 社 IaaS と併せたマルチクラウド環境にし，D 社閉域 NW 経由で利用する。

・A 社本社と D 社閉域 NW との接続回線を追加し，マルチホーム接続とする。

・インターネット接続を本社経由から D 社閉域 NW 経由に切り替える。

可用性向上後の A 社のネットワーク構成を図 2 に示す。

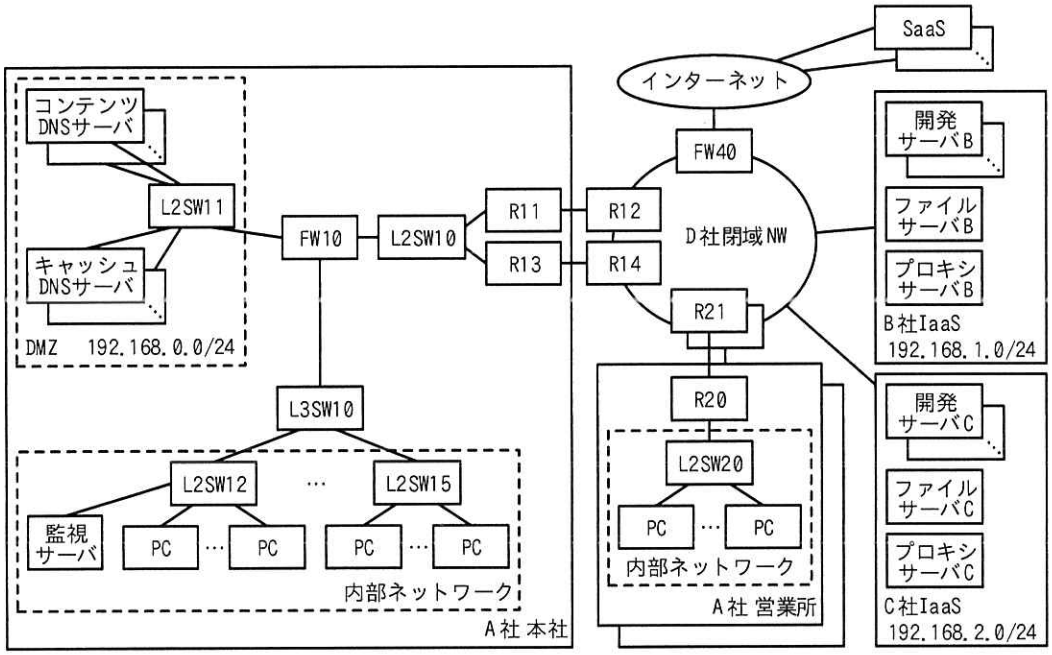


図 2　可用性向上後の A 社のネットワーク構成（抜粋）

〔B 社と C 社の IaaS 利用〕

C 社からも，B 社と同様に管理コンソールが提供されている。B 社 IaaS に構築された仮想ネットワーク，仮想サーバと C 社 IaaS に構築された仮想ネットワーク，仮想サーバは D 社閉域 NW を経由して相互に通信できる。

E さんは，B 社と C 社の IaaS 利用方針を次のとおり策定した。

・C 社 IaaS にファイルサーバ C を新たに構築し，ファイルサーバ B と常に同期をとるように設定する。A 社従業員はファイルサーバ B 又はファイルサーバ C を利用する。

・B 社 IaaS にプロキシサーバ B を，C 社 IaaS にプロキシサーバ C を新たに構築し，プロキシサーバ A から切り替える。

・B 社 IaaS を利用して開発サーバ B を，C 社 IaaS を利用して開発サーバ C を構築し，

A社の担当部門に引き渡す。

〔プロキシサーバの利用方法の検討〕

Eさんは，IaaSに構築するプロキシサーバBとプロキシサーバCの利用方法を検討した。プロキシサーバの利用方法の案を表1に示す。

表1　プロキシサーバの利用方法の案

案	概要
案1	平常時はプロキシサーバBを利用し，プロキシサーバBに障害が発生した際にはプロキシサーバCを利用するように切り替える。
案2	平常時からプロキシサーバB及びプロキシサーバCを利用し，片方に障害が発生した際には正常稼働しているもう片方を利用するように切り替える。

Eさんは，従業員が利用するプロキシサーバを，DNSの機能を利用して制御することを考えた。プロキシサーバに障害が発生した際には，DNSの機能を利用して切り替える。

プロキシサーバに関するDNSゾーンファイルの記述内容を表2に示す。

表2　プロキシサーバに関するDNSゾーンファイルの記述内容

	DNSゾーンファイルの記述内容
現在の設定	proxy.a-sha.co.jp.　IN A　192.168.0.145　；従業員が指定するホスト proxya.a-sha.co.jp.　IN A　192.168.0.145　；プロキシサーバAのホスト
案1の初期設定	proxy.a-sha.co.jp.　IN A　192.168.1.145　；従業員が指定するホスト proxya.a-sha.co.jp.　IN A　192.168.0.145　；プロキシサーバAのホスト proxyb.a-sha.co.jp.　IN A　192.168.1.145　；プロキシサーバBのホスト proxyc.a-sha.co.jp.　IN A　192.168.2.145　；プロキシサーバCのホスト
案2の初期設定	proxy.a-sha.co.jp.　IN A　192.168.1.145　；従業員が指定するホスト proxy.a-sha.co.jp.　IN A　192.168.2.145　；従業員が指定するホスト proxya.a-sha.co.jp.　IN A　192.168.0.145　；プロキシサーバAのホスト proxyb.a-sha.co.jp.　IN A　192.168.1.145　；プロキシサーバBのホスト proxyc.a-sha.co.jp.　IN A　192.168.2.145　；プロキシサーバCのホスト

注記 切替え期間中の設定を含む。

Eさんは，プロキシサーバの監視運用について検討した。監視サーバで利用できる①ping監視では不十分だと考え，新たにTCP監視機能を追加し，プロキシサーバのアプリケーションプロセスが動作するポート番号にTCP接続可能か監視することにし

た。また，監視対象として，従業員がプロキシサーバとして指定するホストに加えて，プロキシサーバ A，プロキシサーバ B，プロキシサーバ C のホストを設定することにした。

次に，監視サーバでプロキシサーバ B の異常を検知した際に，従業員がプロキシサーバの利用を再開できるようにするための復旧方法として，②DNS ゾーンファイルの変更内容を案 1，案 2 それぞれについて検討した。また，③平常時から proxy.a-sha.co.jp に関するリソースレコードの TTL の値を小さくすることにした。

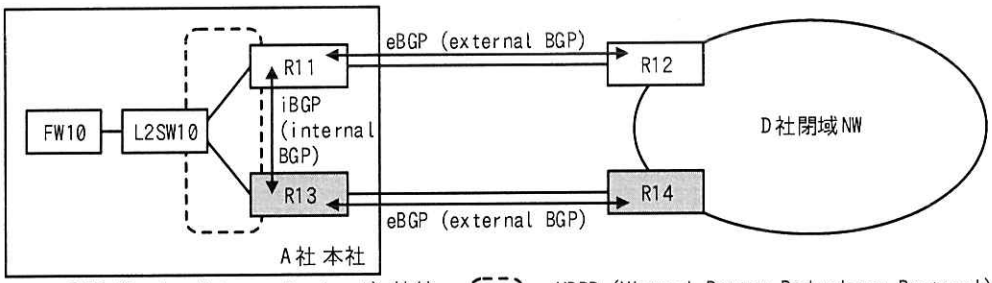
これらの検討の結果，プロキシサーバの負荷分散ができること，及びプロキシサーバの有効活用ができることから案 2 の方が優れていると考え，E さんは案 2 を採用することにした。

さらに，E さんは，自動でプロキシサーバを切り替えるために，④ DNS とは異なる方法で従業員が利用するプロキシサーバを切り替える方法も検討した。プロキシサーバを利用する側の環境に依存することから，DNS ゾーンファイルの書換えによる切替えと併用することにした。

〔マルチホーム接続〕

次に，E さんは D 社閉域 NW とのマルチホーム接続について検討した。A 社本社に増設するルータ及び回線は D 社からネットワークサービスとして提供される。マルチホーム接続の設計について D 社担当者から説明を受けた。

D 社担当者から説明を受けたマルチホーム接続構成を図 3 に示す。



注記　網掛け部分は，追加する機器を示す。

図 3　D 社担当者から説明を受けたマルチホーム接続構成（抜粋）

図3の概要は次のとおりである。

・本社とD社閉域NWとの間で，新たにR13と専用線がD社からネットワークサービスとして提供される。R11とR13とを併せてマルチホーム接続とする。

・増設する専用線の契約帯域幅は既設の専用線と同じにし，平常時は既設の専用線を利用し，障害発生時には増設する専用線を利用する。

・既存のR11とR12は，静的経路制御からBGPによる動的経路制御に変更する。

・R11とR12との間，R13とR14との間はeBGPで接続する。⑤ R11とR13との間はiBGPで接続し，あわせてnext-hop-self設定を行う。

・R11とR13との間ではVRRPを利用する。FW10はVRRPで定義する仮想IPアドレスをネクストホップとして静的経路設定を行う。

D社担当者からの説明を受けたEさんは，BGPについて調査した。

RFC 4271で規定されているBGPは，［ a ］間の経路交換のために作られたプロトコルで，TCPポート179番を利用して接続し，経路交換を行う。経路交換を行う隣接のルータを［ b ］と呼ぶ。BGPで交換されるメッセージは4タイプあり，表3に示す。

表3　BGPで交換されるメッセージ

タイプ	名称	説明
1	OPEN	BGP接続開始時に交換する。 自AS番号，BGPID，バージョンなどの情報を含む。
2	［ c ］	経路情報の交換に利用する。 経路の追加や削除が発生した場合に送信される。
3	NOTIFICATION	エラーを検出した場合に送信される。
4	［ d ］	BGP接続の確立やBGP接続の維持のために交換する。

経路制御は，［ c ］メッセージに含まれるBGPパスアトリビュートの一つであるLOCAL_PREFを利用して行うとの説明をD社担当者から受けた。LOCAL_PREFは，iBGPピアに対して通知する，外部のASに存在する宛先ネットワークアドレスの優先度を定義する。BGPでは，ピアリングで受信した経路情報をBGPテーブルとして構成し，最適経路選択アルゴリズムによって経路情報を一つだけ選択し，ルータの［ e ］に反映する。LOCAL_PREFの場合では，最も［ f ］値をもつ経路情

報が選択される。

また，E さんは，D 社担当者から静的経路制御から BGP による動的経路制御に構成変更する手順の説明を受けた。この時，⑥BGP の導入を行った後に VRRP の導入を行う必要があるとの説明だった。E さんが説明を受けた手順を表 4 に示す。

表 4　E さんが説明を受けた手順

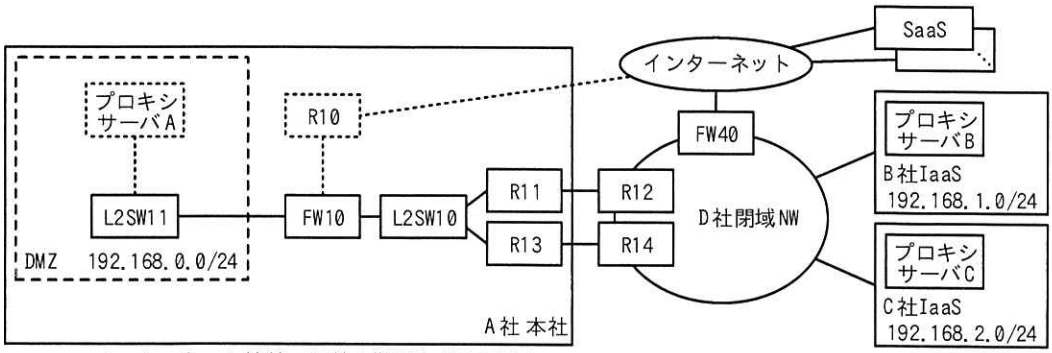
項番	作業内容
1	R13 及び R14 を増設する。
2	R13 と増設する専用線とを接続する。 R14 と増設する専用線とを接続する。 R13 と L2SW10 とを接続する。
3	R13 及び R14 のインタフェースに IP アドレスを設定する。
4	⑦増設した機器や回線に故障がないことを確認するために ping コマンドで試験を行う。
5	R11～R14 に BGP の設定を追加する。ただし，この時点では BGP 接続は確立しない。
6	全ての BGP 接続を確立させ，送受信する経路情報が正しいことを確認する。
7	⑧ R11 及び R12 の不要になる静的経路制御の経路情報を削除する。
8	R11 と R13 との間の VRRP で利用する新しい仮想 IP アドレスを割り当て，VRRP を構成する。
9	FW10 において VRRP で利用する仮想 IP アドレスをネクストホップとする静的経路制御の経路情報を設定する。
10	FW10 で不要になる静的経路制御の経路情報を削除する。

E さんは，設計どおりにマルチホームによる可用性向上が実現できたかどうかを確認するための障害試験を行うことにし，⑨想定する障害の発生箇所と内容を障害一覧としてまとめた。

〔インターネット接続の切替え〕

次に，E さんはインターネット接続を本社経由から D 社閉域 NW 経由へ切り替えることについて検討した。

インターネット接続の切替え期間中の構成を図 4 に示す。



------- ：インターネット接続の切替え期間中だけ利用する。

図4　インターネット接続の切替え期間中の構成（抜粋）

FW40 を使ってインターネット接続する。FW40 は D 社からネットワークサービスとして提供される。FW40 には新たにグローバル IP アドレスが割り当てられる。FW40 を経由するインターネット宛ての通信は NAPT 機能によって IP アドレスとポート番号の変換が行われる。A 社とインターネットとの通信を，R10 経由から FW40 経由になるようにインターネット接続を切り替える。

E さんは，設定変更の作業影響による通信断時間を極力短くするために，⑩ FW10 の設定変更は D 社閉域 NW の設定変更とタイミングを合わせて実施する必要があると考えた。

E さんは，⑪インターネット接続の切替えを行うと一部の部門で業務に影響があると考えた。対策として，全てのインターネット宛ての通信は FW40 経由へと切り替えるが，⑫一定期間，プロキシサーバ A からのインターネット宛ての通信だけは既存の R10 経由になるようにする。あわせて，E さんは，業務に影響がある一部の部門には切替え期間中はプロキシサーバ A が利用可能なことを案内するとともに，⑬恒久対応として設定変更の依頼を事前に行うことにした。

E さんは，プロキシサーバ A のログを定期的に調査し，利用がなくなったことを確認した後に，プロキシサーバ A を廃止することにした。

E さんが検討した可用性向上の検討案は承認され，システム部では可用性向上プロジェクトを開始した。

設問1　〔プロキシサーバの利用方法の検討〕について答えよ。

(1) 表2中の案2の初期設定について，負荷分散を目的として一つのドメイン名に対して複数のIPアドレスを割り当てる方式名を答えよ。

(2) 本文中の下線①について，ping監視では不十分な理由を40字以内で答えよ。

(3) 本文中の下線②について，表2の案1の初期設定を対象に，ドメイン名proxy.a-sha.co.jp.の書換え後のIPアドレスを答えよ。

(4) 本文中の下線③について，TTLの値を小さくする目的を40字以内で答えよ。

(5) 本文中の下線④について，DNSとは異なる方法を20字以内で答えよ。また，その方法の制限事項を，プロキシサーバを利用する側の環境に着目して25字以内で答えよ。

設問2　〔マルチホーム接続〕について答えよ。

(1) 本文中及び表3中の［ a ］～［ f ］に入れる適切な字句を答えよ。

(2) 本文中の下線⑤について，next-hop-self設定を行うと，iBGPで広告する経路情報のネクストホップのIPアドレスには何が設定されるか。15字以内で答えよ。

(3) 表3について，BGPピア間で定期的にやり取りされるメッセージを一つ選び，タイプで答えよ。また，そのメッセージが一定時間受信できなくなるとどのような動作をするか。30字以内で答えよ。

(4) 本文中の下線⑥について，BGPの導入を行った後にVRRPの導入を行うべき理由を，R13が何らかの理由でVRRPマスターになったときのR13の経路情報の状態を想定し，50字以内で答えよ。

(5) 表4中の下線⑦について，pingコマンドの試験で確認すべき内容を20字以内で答えよ。また，pingコマンドの試験で確認すべき送信元と宛先の組合せを二つ挙げ，図3中の機器名で答えよ。

(6) 表4中の下線⑧について，R11及びR12では静的経路制御の経路情報を削除することで同じ宛先ネットワークのBGPの経路情報が有効になる。その理由を40字以内で答えよ。

(7) 本文中の下線⑨について，想定する障害を六つ挙げ，それぞれの障害発生

箇所を答えよ。ただし，R12 と R14 については D 社で障害試験実施済みとする。

設問３　〔インターネット接続の切替え〕について答えよ。

(1)　本文中の下線⑩について，D 社閉域 NW の設定変更より前に FW10 のデフォルトルートの設定変更を行うとどのような状況になるか。25 字以内で答えよ。

(2)　本文中の下線⑪について，業務に影響が発生する理由を 20 字以内で答えよ。

(3)　本文中の下線⑫について，FW10 にどのようなポリシーベースルーティング設定が必要か。70 字以内で答えよ。

(4)　本文中の下線⑬について，どのような設定変更を依頼すればよいか。40 字以内で答えよ。