

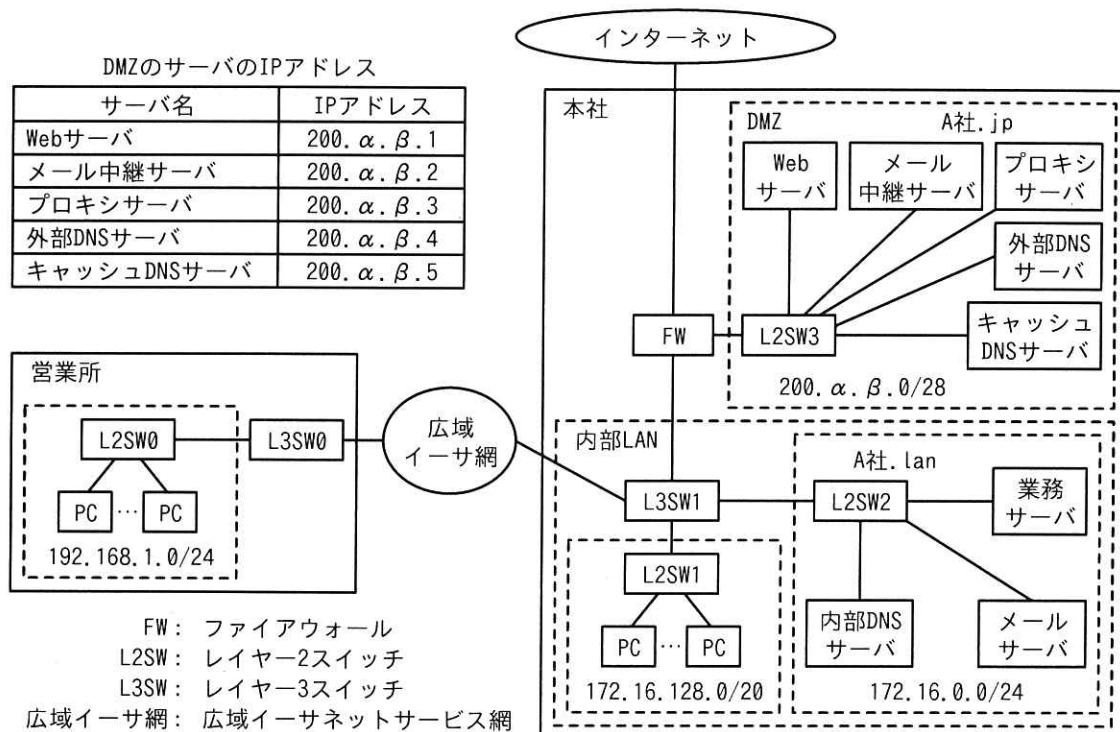
問5 クラウドサービスへの移行に関する次の記述を読んで、設問に答えよ。

A社は、本社と一つの営業所をもつオフィス機器の販売会社である。本社で、Webサーバ、電子メール（以下、メールという）サーバ、業務サーバなどを運用している。

このたび、A社では、サーバの運用管理及びセキュリティ対策の負荷軽減を図るために、社内で運用するサーバを、B社のクラウドサービスでA社が占有して利用できる環境（以下、BCL-Aという）に移行することを決定した。情報システム部のC主任が、サーバ移行に伴うネットワーク構成の設計を担当することになった。

〔現在のネットワーク構成と運用形態〕

現在のA社のネットワーク構成を図1に示す。



注記1 200.α.β.γはグローバルIPアドレスである。また、200.α.β.0/28はネットワークアドレスを示し、/28はサブネットマスク長を示す。

注記2 A社.jpはインターネット向けドメイン、A社.lanはA社内向けドメインである。

図1 現在のA社のネットワーク構成

現在の A 社のネットワークの構成及び運用形態を次に示す。

- ・ 本社及び営業所の PC（以下、社内 PC という）には、L3SW1 上で稼働する DHCP サーバから配付される IP アドレス、そのリース期間及びサブネットマスク、①デフォルトゲートウェイの IP アドレス並びに DNS サーバの IP アドレスを設定している。
- ・ メールサーバは、本社及び営業所の従業員によるメール送受信に利用される。
- ・ メール中継サーバは、メールサーバから送信された社外宛てのメールを社外のメールサーバに中継し、社外のメールサーバから A 社宛てに送信されたメールをメールサーバに中継する。
- ・ ②メール中継サーバでは、スパムメールの踏み台になることを避けるために、オープンリレー防止策を実施している。
- ・ 業務サーバは、社内 PC とだけ通信する。
- ・ 社内 PC は、内部 DNS サーバで名前解決を行う。
- ・ 内部 DNS サーバは、A 社.lan のゾーン情報を管理し、管理外のドメインのホストの名前解決要求を受信したときは、名前解決要求をキャッシュ DNS サーバに転送する。
- ・ 外部 DNS サーバは、A 社.jp のゾーン情報を管理する。
- ・ 業務サーバ及び DMZ の Web サーバは、HTTP Over TLS によるアクセスだけを受け付ける。
- ・ 社内 PC は、インターネット上の Web サイト及び DMZ の Web サーバに、DMZ のプロキシサーバ経由でアクセスする。

FW に設定されている、インターネットと DMZ との間の通信を許可するルールを表 1 に示す。

表 1 FW に設定されている、インターネットと DMZ との間の通信を許可するルール

アクセス経路	送信元	宛先	プロトコル／宛先ポート番号
インターネット→DMZ	any	a	TCP/443
	any	b	TCP/53, UDP/53
	any	メール中継サーバ	TCP/25
DMZ→インターネット	c	any	TCP/80, TCP/443
	キャッシュ DNS サーバ	any	TCP/53, UDP/53
	メール中継サーバ	any	TCP/25

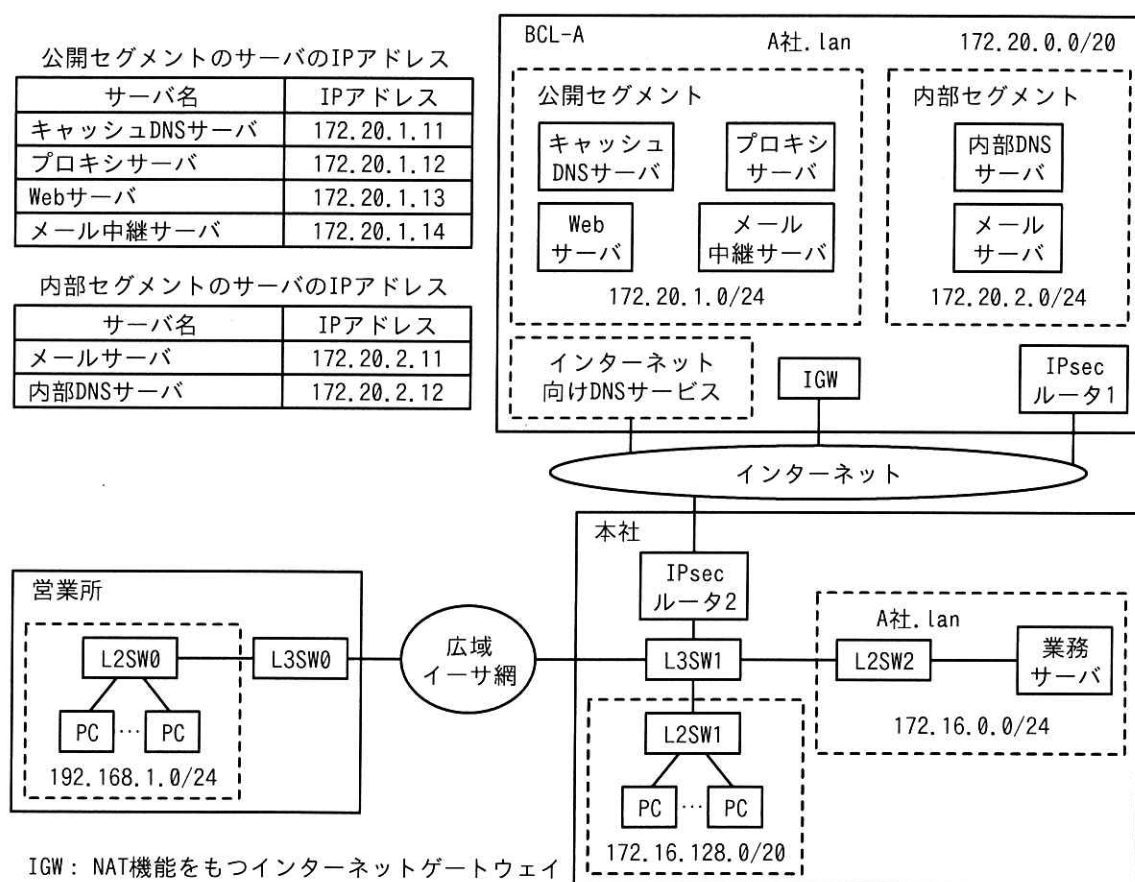
注記 FW は、応答パケットの通過を自動的に許可する機能をもつ。

〔BCL-A に移行後の構成の設計〕

C 主任は、サーバを BCL-A に移行した後の構成を、次の 3 点を前提として設計した。

- ・ 社内 PC を使用した業務の運用方法及び PC の操作は変更しない。
- ・ 移行作業時の障害によって業務が全面停止するのを避けるために、今回の移行では業務サーバを本社に残す。
- ・ BCL-A に移行後の各サーバのインターネット向けの IP アドレスには、移行前の DMZ の各サーバと同じグローバル IP アドレスを設定する。

サーバを BCL-A に移行した後のネットワーク構成を図 2 に示す。



IGW：NAT機能をもつインターネットゲートウェイ

注記 図 1 中の外部 DNS サーバの機能は、B 社が提供するインターネット向け DNS サービスを利用して実現する。

図 2 サーバを BCL-A に移行した後のネットワーク構成

サーバを BCL-A に移行した後の各種設定、動作及び構成を次に示す。

- ・ BCL-A には、公開セグメントと内部セグメントを設定する。
- ・ 公開セグメント及び内部セグメントには、それぞれ経路表を設定する。経路表には、サーバ同士の間及びサーバとインターネットとの間で移行前と同様な通信を行うことができる経路情報を登録する。
- ・ BCL-A のドメイン名は、A 社内向けドメインの A 社. lan とし、ネットワークアドレスは 172.20.0.0/20 を設定する。この 172.20.0.0/20 をサブネットに分割して、公開セグメントに 172.20.1.0/24 を、内部セグメントに 172.20.2.0/24 を設定する。
- ・ A 社. lan のゾーン情報は内部 DNS サーバで管理する。
- ・ 公開セグメントのサーバは、IGW 経由でインターネットと通信する。IGW は、NAT によって、公開セグメントの各サーバに設定された 172.20.1.11~172.20.1.14 をインターネットに公開する各サーバの対応する IP アドレスである 200.α.β.1~200.α.β.3, 200.α.β.5 に変換する。
- ・ 公開セグメントのインターネット向けドメイン名は、図 1 中の DMZ と同様の A 社. jp とし、A 社. jp の各サーバには、図 1 と同じ IP アドレスを設定する。
- ・ A 社. jp のゾーン情報はインターネット向け DNS サービスで管理する。
- ・ ③インターネットから公開セグメントのサーバ宛てに送信されたパケットは、IGW が公開セグメントのサーバに中継する。
- ・ 本社は、IPsec ルータ 2 及び IPsec ルータ 1 を経由して BCL-A と接続する。
- ・ ④IPsec ルータ 2 は、BCL-A 宛てのパケットを、IPsec ルータ 1 に転送する。
- ・ ⑤L3SW0 と L3SW1 の経路表及び DHCP サーバの配付情報を変更する。

C 主任は、設計内容を上司の D 課長に説明し、移行方法が承認された。

設問 1 〔現在のネットワーク構成と運用形態〕について答えよ。

- (1) 本文中の下線①について、営業所の PC に設定するデフォルトゲートウェイの IP アドレスをもつ機器を、図 1 中の名称で答えよ。
- (2) 本文中の下線②について、メール中継サーバで防止すべき処理を、40 字以内で答えよ。
- (3) 表 1 中の

a

 ～

c

 に入れる適切な機器名を、図 1 中の名

称で答えよ。

設問2 「BCL-Aに移行後の構成の設計」について答えよ。

- (1) 本文中の下線③について、A社宛てのSMTPパケットがIGWを通過するとき、IGW通過前と通過後の宛先IPアドレスを、それぞれ答えよ。
- (2) 本文中の下線④について、IPsecルータ1がBCL-Aのサーバに転送するパケットの送信元のネットワークアドレスを、図2中の表記で全て答えよ。
- (3) 本文中の下線⑤について、L3SW0及びL3SW1の経路表中の、社内PCを送信元とする経路の変更は、どのサーバがBCL-Aに移行することによって発生するか。図2中の名称で全て答えよ。