問4　災害復旧対策（ディザスタリカバリ）に関する次の記述を読んで，設問 1～4 に答えよ。

G 社は，全国に営業店をもつ，中堅の専門商社である。現在，東京の本社ビルの一室をサーバルームとして，社内業務システムを運用している。今年度の事業計画に事業継続計画の策定が挙げられていて，その一環として，本社ビルのサーバルームが災害などで使用不能となった際の対策を検討することになった。

〔G 社の社内業務システム〕

現在，G 社の社内業務システムには，会計，販売管理，人事の三つのシステムがあり，それぞれ Web システムとして実現している。社内業務システムのネットワーク構成を図 1 に示す。各 Web サーバはアプリケーションサーバの機能も有しており，仮想サーバで実現している。データベースサーバ（以下，DB サーバという）は 2 台のクラスタ構成で，全システムで共用している。営業店から社内業務システムへは IP-VPN 経由でアクセスしている。

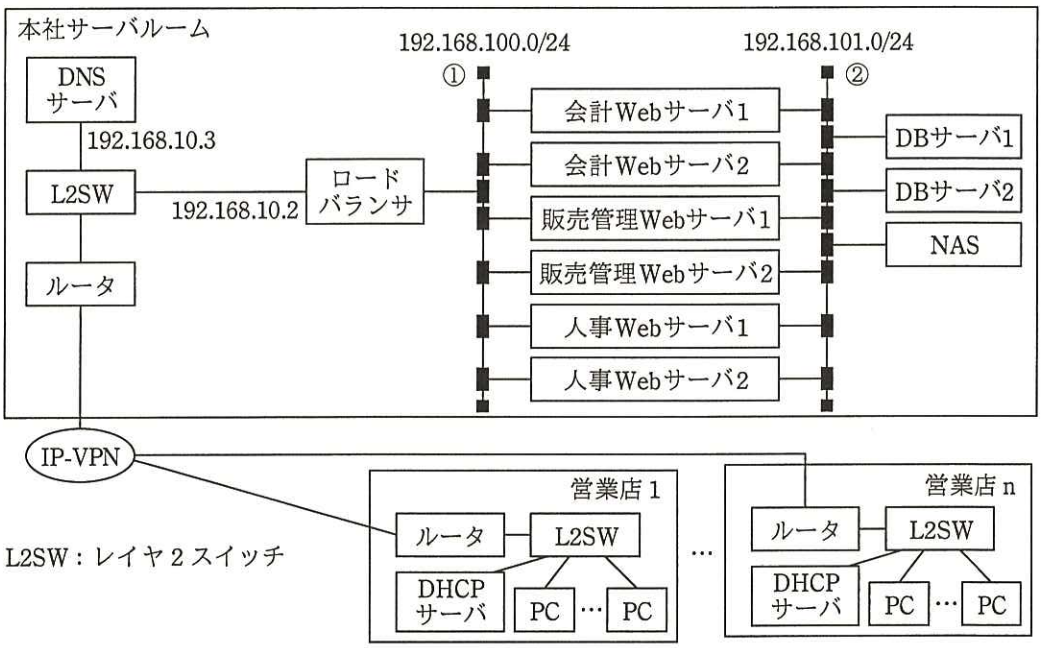

図 1　G 社の社内業務システムのネットワーク構成（抜粋）

各システムにアクセスする際の URL を表 1 に示す。ロードバランサでは，URL のパスから対応するシステムの Web サーバに PC からのリクエストを振り分けている。また，複数台ある Web サーバの負荷分散も行っている。

営業店の PC が社内業務システムにアクセスする際は，DNS を利用して webap.example.co.jp の IP アドレスを取得してアクセスする。DNS サーバの IP アドレスは，PC の起動時に各営業店の DHCP サーバから配布される。現在，プライマリ DNS サーバとして，192.168.10.3 が登録されており，セカンダリ DNS サーバは未登録である。DNS に登録されているリソースレコードの情報を表 2 に示す。

表 1　各システムの URL

システム名	URL
会計	http://webap.example.co.jp/account/
販売管理	http://webap.example.co.jp/sales/
人事	http://webap.example.co.jp/hr/

表 2　DNS のリソースレコード

項目	値
NAME	webap.example.co.jp
TYPE	A
CLASS	IN
TTL（Time to Live）	86400
RDATA	192.168.10.2

DB サーバ上のデータベースのバックアップは，フルバックアップと更新ログから成る。毎日深夜 1 時にフルバックアップを取得し，過去 1 週間分を NAS に保管している。また，1 時間ごとに，その 1 時間の間に発生したトランザクションの更新ログを採取し，1 ファイルとして NAS に保管している。フルバックアップの取得は 30 分以内，更新ログの採取は 5 分以内に完了する。データベースが壊れた場合は，フルバックアップと，フルバックアップ取得後からデータベースが壊れるまでに採取した更新ログから，データベースを復旧する。

〔災害復旧対策〕

災害復旧対策において目標とする復旧のレベルの指標として，目標復旧時間（RTO : Recovery Time Objective）及び目標復旧時点（RPO : Recovery Point Objective）を用いる。RTO は，システムが使用不能になった時（以下，災害時刻という）から，業務が再開されるまでに掛かる時間の目標を表す。RPO は，災害時刻にどれだけ近い時刻の状態にデータを復旧できるかの目標を，災害時刻との時間差で表す。RTO と RPO を検討した結果，RTO は 24 時間，RPO は 1 時間とした。

別の拠点に，本社ビルと同等のサーバルームを用意するのはコストが掛かり過ぎ，実現が難しい。そこで，低コストで災害復旧対策を実現する方法を調査したところ，クラウドサービスを利用する方法があることが分かった。調査したクラウドサービスでは，コストは，サーバが稼働している時間，使用しているストレージの容量，及び下りデータの通信量に応じて掛かるので，サーバを停止していれば安価になると考えた。

各システムの Web サーバのイメージファイルから，クラウド上に Web サーバを作成し，DB サーバには本社と同じデータベースを作成しておく。DNS サーバは本社と同じ設定でセカンダリ DNS サーバとして使えるように稼働しておく。通常時は，ロードバランサ，Web サーバ，DB サーバは停止しておく。本社でデータベースのバックアップを作成次第，クラウドの NAS にアップロードする。被災運用が発動された際は，ロードバランサ，DB サーバを起動して，データベースを復旧し，Web サーバを起動して動作確認をした後，DNS の登録内容を変更して被災運用を開始する。被災運用時用システムのクラウド上のネットワーク構成を図 2 に示す。

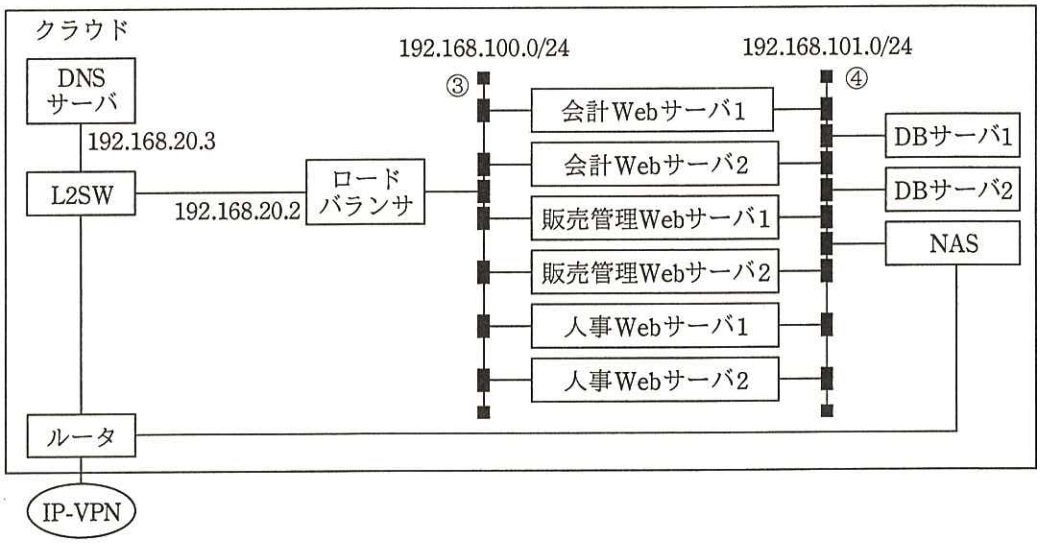

図 2　被災運用時用システムのクラウド上のネットワーク構成

〔被災運用の発動手順〕

実際に被災運用が発動された際の手順を表 3 のとおり定めた。また，各作業に必要な時間を表 4 に示す。全システムの動作確認が完了する前に，営業店から被災運用時用システムにアクセスすることがないよう，DNS の変更は手順の最後にした。

動作確認の際は，DNS を利用せず被災運用時用のロードバランサの IP アドレスを用いる。

表3　被災運用発動時の手順

作業順	作業内容
1	ロードバランサ及びDBサーバを起動する。
2	フルバックアップからデータベースをリストアする。
3	必要な更新ログをデータベースに反映する。
4	販売管理システムのWebサーバを起動する。
5	販売管理システムの動作確認をする。
6	会計システムのWebサーバを起動する。
7	会計システムの動作確認をする。
8	人事システムのWebサーバを起動する。
9	人事システムの動作確認をする。
10	⑤DNSの登録内容を変更する。

表4　被災運用発動時の各作業の時間

作業	作業時間
ロードバランサ及びDBサーバの起動	20分
フルバックアップからのデータベースのリストア	30分
更新ログの反映（更新ログ1ファイルごとに）	10分
Webサーバの起動（各システムごとに）	10分
動作確認（各システムごとに）	60分
DNSの登録内容の変更	10分

設問1　G 社では，10 月 10 日の 10 時 30 分に本社ビルのサーバルームが被災して使用できなくなってしまった場合，社内業務システムは，いつまでに，いつ時点のデータで被災運用が開始されることを目標としているかを答えよ。

設問2　図 1 中の①と図 2 中の③のネットワークアドレス，及び図 1 中の②と図 2 中の④のネットワークアドレスが同じである理由を 35 字以内で述べよ。

設問3　DHCP サーバと DNS サーバは，あらかじめ現在の設定を変更しておかないと，災害が発生した場合に〔被災運用の発動手順〕に従って作業を進めても，営業店の PC から被災運用時用システムにアクセスすることができない。被災運用に対する準備について，(1)，(2)に答えよ。

(1)　DHCP サーバの設定で，あらかじめ変更しておくべき内容を 40 字以内で述べよ。

(2)　表 2 の DNS サーバの設定で，あらかじめ変更しておくべき内容を解答群の中から選び，記号で答えよ。

解答群

ア　RDATA を 192.168.20.2 に変更　　イ　TTL を 600 に変更

ウ　TTL を 172800 に変更　　エ　TYPE を AAAA に変更

設問4　〔被災運用の発動手順〕について，(1)，(2)に答えよ。

(1)　10月10日の10時30分に本社ビルのサーバルームが被災して使用できなくなってしまい，11 時に被災運用を発動した場合，社内業務システムは，いつから被災運用が開始できるかを答えよ。

(2)　表 3 中の下線⑤で変更する登録内容について，表 2 の項目と変更後の値を答えよ。