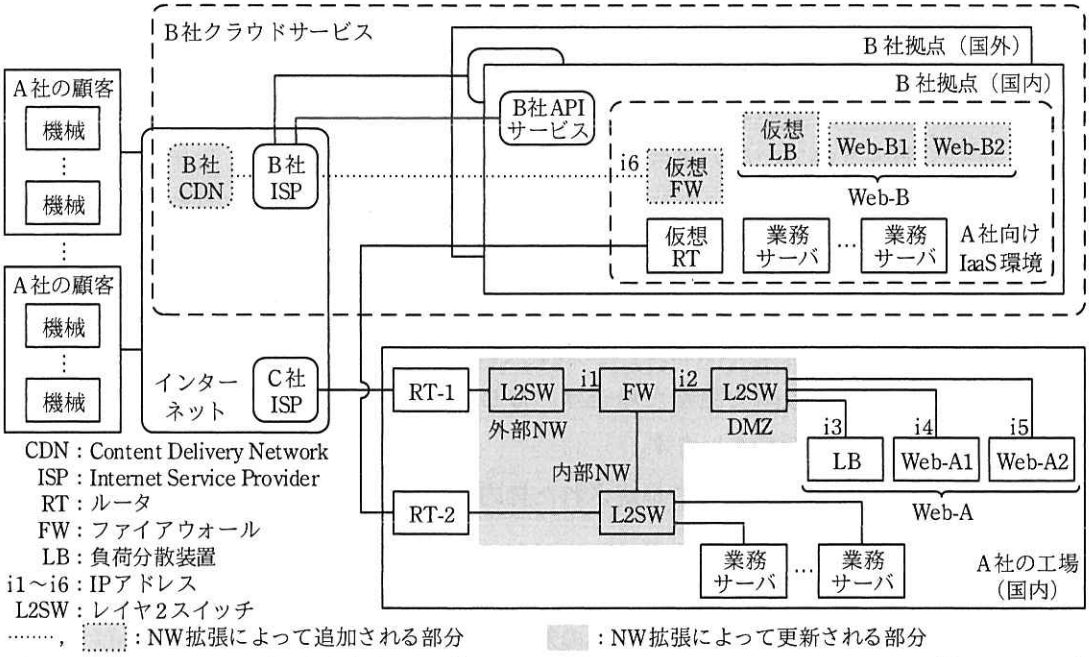
問１　SDN とクラウドの活用に関する次の記述を読んで，設問 1～4 に答えよ。

A 社は，国内外に顧客をもつ生産機械メーカである。A 社では，IoT 時代に適応するために，新たな情報システム基盤を整備中である。

現在の情報システム基盤は，国内工場の自社設備と，国内外にサービス用拠点をもつクラウドサービス事業者 B 社の IaaS 環境で構成されている。B 社の A 社向け IaaS 環境は国内にあり，工場とは専用線で接続されている。インターネットと工場とは，インターネットサービス事業者 C 社の国内拠点を介して接続されている。

A 社の情報システム部は，顧客の拠点で稼働中の生産機械（以下，機械という）と情報システム基盤の Web サーバで構成されたシステム（以下，新システムという）を開発中である。また，本年度は，ネットワーク（以下，NW という）の拡張を予定している。NW 拡張の概要を図 1 に示す。



注記１　A社は，インターネットを経由してB社APIサービスにアクセスし，HTTPリクエストを使って，利用するB社クラウドサービスの追加や変更を行う。

注記２　Web-Aは，LBと2台のWebサーバ（Web-A1，Web-A2）から構成された，新システムの試行環境である。Web-Aは，既に稼働している。

注記３　Web-Bは，仮想LBと2台のWebサーバ（Web-B1，Web-B2）から構成された，新システムの本運用環境である。Web-Bは，NW拡張の中で導入される。

図１　NW 拡張の概要（抜粋）

NW 拡張の目的を次に示す。

・工場 LAN の SDN（Software-Defined Networking）化：　SDN 技術を用いて，現在の工場 LAN を，ビジネス変化に対応できる柔軟性と拡張性を備えた新たな工場 LAN（以下，新工場 LAN という）に刷新する。新工場 LAN では，物理配線の変更なしに，自社要員だけで構成変更ができるようにする。

・クラウドサービスの利用拡大：　開発中の新システムは，国内外の多数の機械に対する，ファームウェアの一斉更新，稼働状況の定期収集に用いられる。新システムの本運用のために，Web-A よりも大規模な Web-B を構築し，B 社クラウドサービス（図 1 中の B 社 CDN，B 社 ISP）を活用して，Web-A へのアクセス経路よりも高速な Web-B へのアクセス経路を実現する。

機械から Web-A へのアクセスの概要を次に示す。

・Web-A を収容している DMZ は，プライベートアドレスが割り当てられている。

・機械から送信された IP パケットは，C 社 ISP を経由し，FW に転送される。その宛先 IP アドレスは，図 1 中の［　あ　］である。

・FW は，受信した IP パケットを LB に転送する。その際，FW の［　い　］機能によって，宛先 IP アドレスは図 1 中の［　う　］に書き換えられる。

・LB は，サーバの稼働状況をチェックしながら，受信した IP パケットを動的に Web-A1 又は Web-A2 に振り分ける。

NW 拡張後は，B 社クラウドサービスを使って，機械から Web-B へ同様のアクセスが行われるようになる。機械は，Web-A へのアクセスと Web-B へのアクセスを切り換えられるようになっており，試行環境と本運用環境を使い分けながら，新システムの機能拡充を進めていく予定である。

情報システム部の NW 拡張プロジェクトでは，新工場 LAN の提案と構築をベンダに委託し，それ以外の作業を自社要員が担当する。NW 拡張プロジェクト発足に先立ち，情報システム部の D 君が，次の準備作業を行っている。

・新工場 LAN に適用する SDN 技術の調査：　ベンダから提案があった，新工場 LAN に適用する SDN 技術について，その概要を整理する。

・新工場 LAN の運用の調査：　ベンダから提案があった，新工場 LAN の論理構成と通信方式の概要を整理する。

・クラウドサービス利用拡大の検討：　新システムの本運用に用いる，B 社 CDN と B 社 ISP を使った NW の導入案を作成する。

・A 社向け IaaS 環境のバックアップの検討：　B 社拠点（国内）が長時間使えない場合を想定し，新システムの稼働を再開させるための代替手段を検討する。

〔新工場 LAN に適用する SDN 技術の調査〕

ベンダから提案があった SDN 技術について，D 君は次のように整理した。

・従来のスイッチ機能を，経路制御などの管理機能を実行するフローコントローラ（以下，OFC という）と，データ転送を行うスイッチ（以下，OFS という）に分け，OFS に入るパケットの経路制御を OFC が集中制御する方式を採用する。

・OFS と OFC は，管理のための専用 NW（以下，管理 NW という）を介して，通信メッセージを交換する。OFC と OFS 間の通信メッセージを表 1 に示す。

表 1　OFC と OFS 間の通信メッセージ（抜粋）

通信メッセージ名	通信の方向	用途
Packet-In	OFS→OFC	入力パケットと入力ポート ID を，OFC に通知する。
Packet-Out	OFC→OFS	出力パケットと出力ポート ID を送り，OFS に出力させる。
Flow-Mod	OFC→OFS	変更情報を送り，OFS の管理テーブルを変更させる。

・OFS は，IP アドレス，MAC アドレスなどのパケット識別子（Match Field，以下，MF という）を使ったパケット識別条件と，識別されたパケットの処理（以下，Action という）の組合せ（以下，エントリという）を，OFS 内の管理テーブルで管理する。

・OFS は，入力パケットに対して，管理テーブル内のパケット識別条件が一致するエントリを探し，そのエントリの Action を実行する。一致するエントリがない場合は，事前の設定に従い，入力パケットを破棄するか，Packet-In メッセージを使って OFC に入力パケットを転送する。今回の提案では，OFC への通信集中を避けるために，入力パケットを破棄させる設定を全 OFS に対して行う。

・MF と Action の例を表 2 に示す。

表2　MF と Action の例

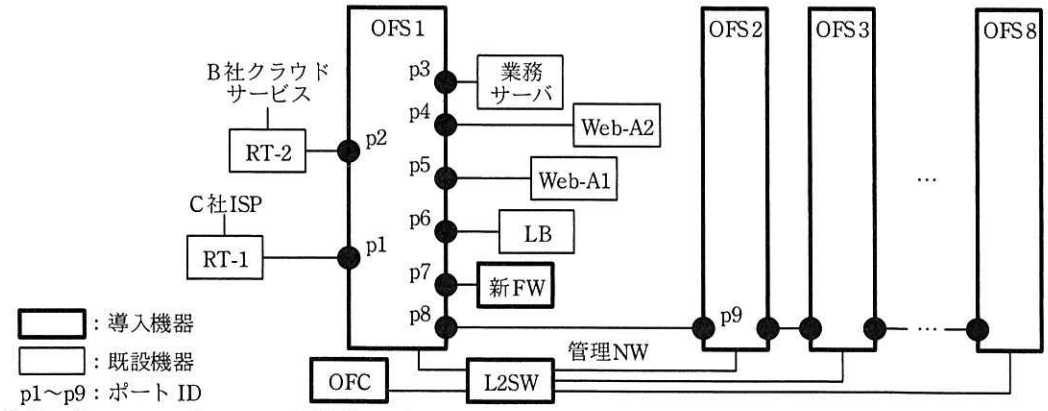
MF の例

レイヤ	MF 名	説明
L1	IN_PORT	入力ポート ID
L2	ETH_DST	宛先 MAC アドレス
	ETH_SRC	送信元 MAC アドレス
	ETH_TYPE	イーサネットタイプ
	VLAN_VID	VLAN ID
L3	IPV4_SRC	送信元 IP アドレス
	IPV4_DST	宛先 IP アドレス

Action の例

Action 名	説明
Output(　)	(　)内に指定された次に示すパラメータに従い，パケットを出力する。 ・ポート ID：指定ポートに出力する。 ・controller：Packet-In メッセージを使い OFC に転送する。
Drop	パケットを破棄する。
Set-Field	パケットのヘッダの一部を書き換える。 ・表記例：Set-Field ETH_DST=m1 （宛先 MAC アドレスを m1 に書き換える場合）
Push-VLAN	パケットに VLAN ヘッダを付加する。
Pop-VLAN	パケットの VLAN ヘッダを削除する。

ベンダの提案では，8 台の OFS を導入する。ベンダから提案があった新工場 LAN の物理構成案を，図 2 に示す。



注記　新FWは，現行のFWに置き換わる新しい機器である。

図 2　新工場 LAN の物理構成案（抜粋）

OFS 同士の接続情報を OFC が収集する通信シーケンスについて，D 君はベンダから説明を受けた。例えば，図 2 中の OFC が，OFS1 と OFS2 の接続情報を得る場合の OFS 接続情報収集の通信シーケンス例は，図 3 のようになる。

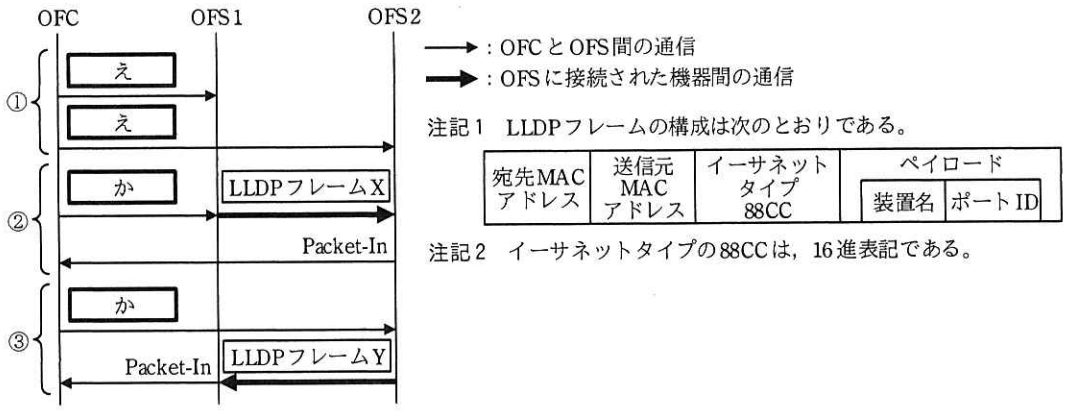


図 3　OFS 接続情報収集の通信シーケンス例

OFS 接続情報の収集では，IEEE 802.1AB で規定されている LLDP（Link Layer Discovery Protocol）の仕組みを流用する。図 3 中の OFC は，固有のイーサネットタイプ 88CC をもつ LLDP フレームを使って，次のように，LLDP フレーム X と LLDP フレーム Y の内容から OFS1 の p8 と OFS2 の p9 の接続情報を得ている。

① OFC は，表 1 中の［　え　］メッセージを使って，ETH_TYPE が 88CC に等しいときの Action として，Output(［　お　］)を，OFS 内の管理テーブルに登録させる。

② OFC は，表 1 中の［　か　］メッセージを使って，OFS1 の全ポートについて，OFS1 の装置名とそれぞれのポート ID を格納した LLDP フレームを出力させ，装置名 OFS1 とポート ID p8 が格納された LLDP フレーム X を OFS2 から受け取る。

③ OFC は，OFS2 に対して②と同様の操作を行い，装置名［　き　］とポート ID［　く　］が格納された LLDP フレーム Y を OFS1 から受け取る。

〔新工場 LAN の運用の調査〕

新工場 LAN の運用について，ベンダからは次のような提案があった。

・OFS を使って，図 1 中の工場の外部 NW，DMZ，内部 NW に対応した，仮想的なレイヤ 2 ネットワーク（以下，仮想 NW という）を構成する。

・仮想 NW 間の通信は，新 FW を経由させる。新 FW と OFS はトランク接続し，仮想 NW に対応した VLAN ID を定義する。

・現行 FW のフィルタリング機能と NAT 機能を，新 FW に移行する。

機械から送信された SYN パケットが，RT-1 から振り分け先の Web-A1 に転送される場合の，新工場 LAN の論理構成と通信シーケンス例を，図 4 に示す。

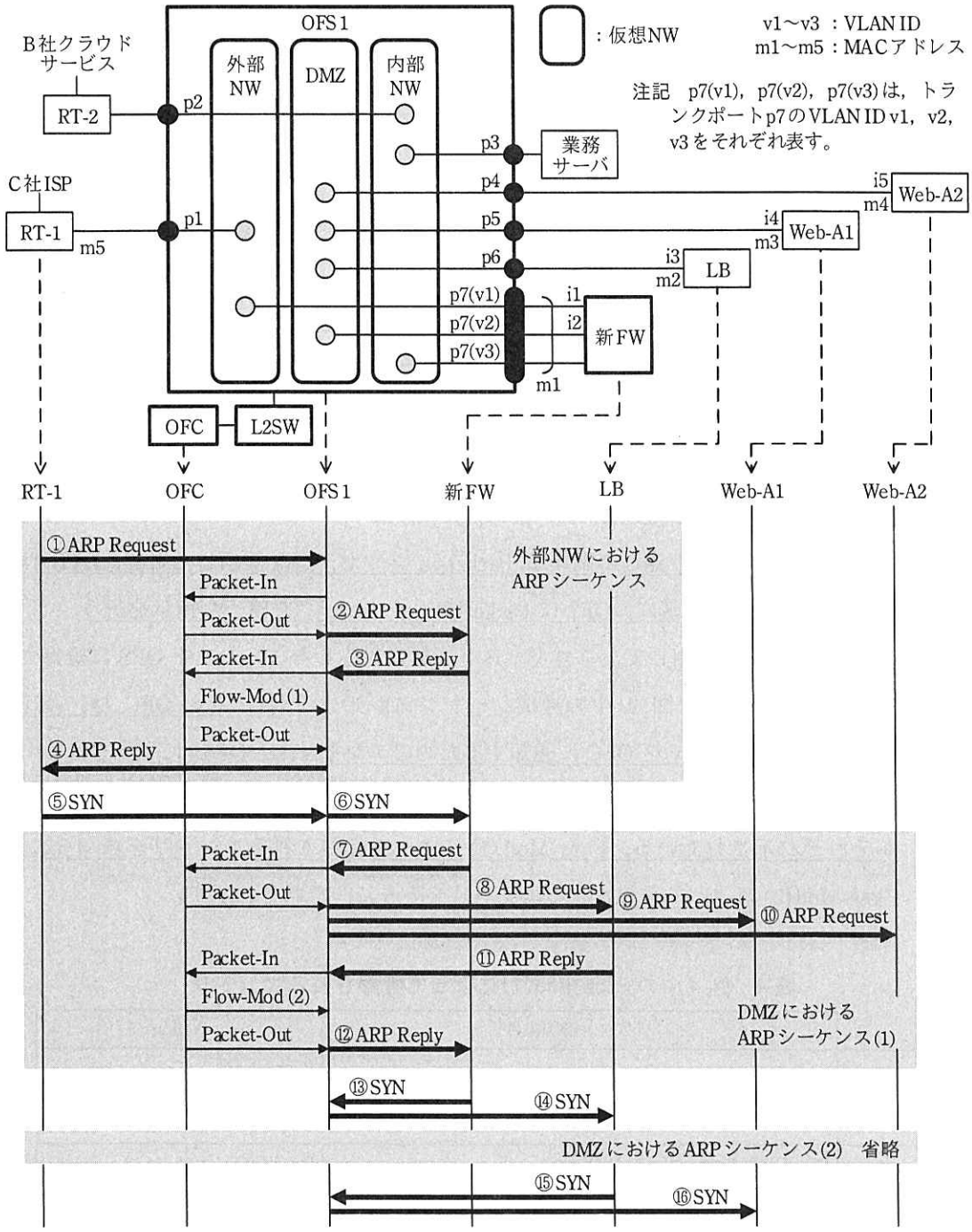


図 4 新工場 LAN の論理構成（抜粋）と通信シーケンス例

図 4 中の⑤のパケットヘッダは，転送する複数の装置によってそれぞれ書き換えられる。図 4 中のパケット⑥，⑬～⑯のヘッダ情報を，表 3 に示す。

表 3　図 4 中のパケット ⑥，⑬～⑯ のヘッダ情報

	VLAN ID	宛先 MAC アドレス	送信元 MAC アドレス	宛先 IP アドレス
⑥	v1	m1	m5	i1
⑬	け	さ	m1	i3
⑭	こ	さ	m1	i3
⑮	なし	し	m2	す
⑯	なし	し	m2	す

注記　“なし” は VLAN ヘッダがないことを表す。

図 4 中の通信シーケンスに関する，OFC と OFS の動作を，次に示す。

・OFC には，次のような仮想 NW の構成に関する構成情報が登録されている。

－OFS1 の外部 NW の構成要素：p1，p7(v1)

－OFS1 の DMZ の構成要素：p4，p5，p6，p7(v2)

(i) ブロードキャスト通信に関する Packet-In メッセージを受信したとき，OFC は，これらの構成情報を基に，OFS に Packet-Out メッセージを使った指示を行う。

・OFC は，ARP を利用して，ユニキャスト通信に対応したエントリを OFS に登録させる。そのために，図 4 中の通信シーケンスが始まる前に，(ii) OFC は，ARP Request と ARP Reply を OFC に通知するためのエントリを，OFS1 に登録させる。

・(iii) 図 4 では，二つのユニキャスト通信について，エントリ登録の通信シーケンスがそれぞれ示されている。Flow-Mod (1) によって登録されるエントリを表 4 に，Flow-Mod(2) によって登録されるエントリを表 5 に，それぞれ示す。

表 4　図 4 中の Flow-Mod(1)によって登録されるエントリ

	パケット識別条件	Action
エントリ 1	IN_PORT = p1,　VLAN_VID = なし, ETH_DST = m1,　ETH_SRC = m5	Push-VLAN, Set-Field VLAN_VID＝v1, Output(p7)
エントリ 2	IN_PORT = p7,　VLAN_VID = v1, ETH_DST = m5,　ETH_SRC = m1	Pop-VLAN, Output(p1)

注記　パケット識別条件は，エントリ内に記述された全ての条件が満たされることを表し，Action は，エントリ内に記述された全ての Action を実行することを表す。

表5　図4中のFlow-Mod(2)によって登録されるエントリ

	パケット識別条件	Action
エントリ1	IN_PORT = せ，VLAN_VID = そ， ETH_DST = た，ETH_SRC = ち	（設問のため省略）
エントリ2	IN_PORT = p7，VLAN_VID = v2， ETH_DST = m2，ETH_SRC = m1	Pop-VLAN， Output(p6)

〔クラウドサービス利用拡大の検討〕

D君が検討した，B社CDNとB社ISPを利用したNWの概要を次に示す。

・機械からA社向けIaaS環境へのアクセスは，B社ISPを経由する。

・B社APIサービスを使って，B社ISP利用時の通信速度を指定する。試行に使っているC社ISP利用時の通信速度に比べて，十分な通信速度を確保する。

・機械からWeb-Bへのアクセスは，FQDN“weblive.asha.example.com”を使って行う。FQDNをWeb-Bのグローバルアドレス（図1中のi6）に変換するために，B社のDNSサービスを利用する。

・高負荷が予想されるときには，B社APIサービスを使って，必要な期間だけB社CDNを適用する。B社CDNの適用は次のように行う。

－世界中に設置されているB社CDNのエッジサーバが，指定されたB社のIaaS環境内のWebサーバ（以下，オリジンサーバという）の処理を代行する。

－エッジサーバは，HTTPクライアントからのHTTPリクエストに応じて，キャッシュ又はプロキシの動作を行う。これらの動作はHTTPプロトコルを使って自動的に行われるので，特別な運用（データ配信など）は不要である。

－A社の場合には，Web-Bをオリジンサーバに指定する。B社CDNを適用する場合には，B社から割り当てられるFQDN“webasha.bshacdn.example.net”を使ってアクセスする。

B社CDNをA社に適用したときの概念図を，図5に示す。

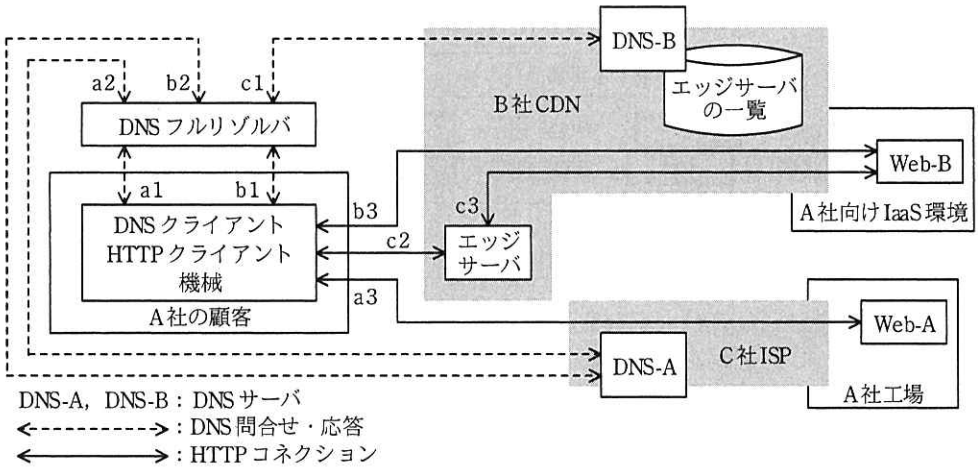


図5　B社CDNをA社に適用したときの概念図

B社CDNを適用する場合には，図5中のDNS-Aのゾーンファイルを書き換え，機械からのアクセスを，Web-Bからエッジサーバへ切り換える。D君が考えたエッジサーバへの切換え方法を，図6に示す。

図5中のDNS-Aのゾーンファイル（抜粋）

```
$TTL 3600
$ORIGIN asha.example.com.
@          IN SOA ns1.asha.example.com.（省略）
   （省略）
webtest IN A      i1
weblive IN A      i6
   （省略）
```

webtest：試行時のWebサーバのホスト名
weblive：本運用時のWebサーバのホスト名
webasha：B社から割り当てられたWebサーバのホスト名

図5中のDNS-Bのゾーンファイル（抜粋）

```
$TTL 3600
$ORIGIN bshacdn.example.net.
@          IN SOA ns1.bshacdn.example.net.（省略）
   （省略）
webasha IN A  【最寄りのエッジサーバのIPアドレス】
   （省略）
```

エッジサーバの一覧
最適なエッジサーバを動的に選択する。

B社CDNを適用する場合には，次のレコードに置き換える。

weblive IN [つ] webasha.bshacdn.example.net.

図6　D君が考えたエッジサーバへの切換え方法

図5と図6の概要を次に示す（a1～a3，b1～b3，c1～c3は，図5中のアクセス経路を示す）。

・機械の動作には，試行モードと本運用モードがある。

・試行モードでは，機械からWeb-Aにアクセスする（a1，a2，a3）。

・本運用モードでは，機械からWeb-Bにアクセスする（b1，b2，b3）。

・本運用モードにおいて高負荷が予想される期間は，B 社 CDN を適用する（b1，b2，c1，c2，c3）。

・c1 において，DNS-B は，DNS メッセージの送信元 IP アドレスを基に，最適なエッジサーバを選択し，その IP アドレスを返す。(iv) EDNS-Client-Subnet（RFC 7871）を使って DNS クライアントの情報が通知された場合には，その情報も利用し，より適したエッジサーバを選択する。

・機械から本運用環境への二つのアクセス（b3，c2）を比較したとき，(v) HTTP の GET リクエストを使うファームウェアの一斉更新の場合に，B 社 CDN 適用による TAT（Turn Around Time）の改善が期待できる。

〔A 社向け IaaS 環境のバックアップの検討〕

情報システム部では，A 社向け IaaS 環境へのサーバ移行を順次進めており，A 社向け IaaS 環境が存在する B 社拠点（国内）が長時間使えないリスクを想定し，そのバックアップ対策（以下，DR という）を運用マニュアルに盛り込むことにしている。

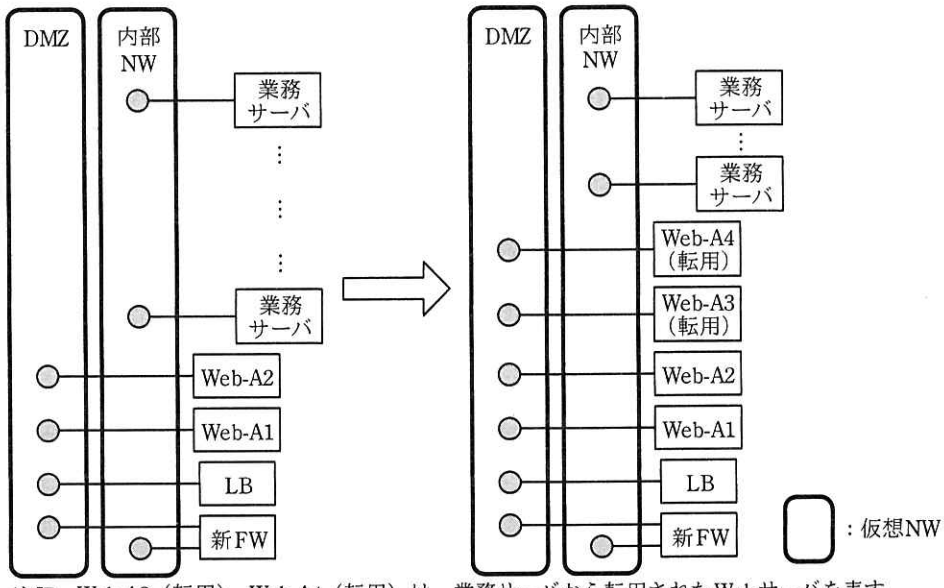
現在，A 社では，サーバ，LB，DNS-A の運用は自社の運用要員が行い，それ以外の NW 機器の運用は，ベンダに委託している。NW 拡張後は，自社の運用要員が，OFC の管理ソフトウェアを使って新工場 LAN の構成を変更し，API サービスを使ってクラウドサービス利用形態を変更するようになる。D 君は，自社の運用要員だけで対応できることを前提に，新システムの DR 案とその DR 案に必要な NW に関する準備を検討し，次の (1) と (2) を提案することにした。

(1) “自社設備利用 DR 案”と NW に関する準備

工場の Web-A を使い，A 社向け IaaS 環境の Web-B を代替する。Web-A の性能不足に備え，工場内の重要度が低い業務サーバを Web サーバに転用し，Web-A をスケールアウトする。そのために次の NW に関する準備を行う。

・(vi) 転用後の業務サーバの IP アドレスを決め，それを用いて準備作業を行う。

・転用後の業務サーバを DMZ に接続するために，OFC の管理ソフトウェアに，新工場 LAN の構成変更に関する定義を登録する。DR 時の新工場 LAN の構成変更の概要を図 7 に示す。



注記　Web-A3（転用），Web-A4（転用）は，業務サーバから転用されたWebサーバを表す。

図7　DR時の新工場LANの構成変更の概要

・(vii) 図6中のDNS-Aのゾーンファイルのリソースレコードを置き換えて，機械の本運用モードのアクセスをWeb-Aに切り換える。そのための手順を用意する。

(2)　“B社拠点（国外）利用DR案”とその準備

B社との現行契約では，B社APIサービスを使って，B社拠点（国外）のA社向けIaaS環境も利用できるので，そこにWeb-Bのバックアップを作成する（以下，NWに関する準備については省略）。

D君は，以上の検討結果を，情報システム部長に報告した。その後，NW拡張プロジェクトが開始され，D君はその技術担当リーダに着任した。

設問1　本文中の［　あ　］～［　く　］に入れる適切な字句を答えよ。

設問2　〔新工場LANの運用の調査〕について，(1)～(6)に答えよ。

(1)　表3中の［　け　］～［　す　］に入れる適切な字句を答えよ。

(2)　本文中の下線(i)のPacket-Outメッセージによって送出されたパケットを，図4中の①～⑯から選び，①～⑯の記号で全て答えよ。

(3)　本文中の下線(ii)について，エントリに含まれるパケット識別条件を，表2

中の MF を用いて，30 字以内で述べよ。

(4) 本文中の下線 (iii) について，表 4 のエントリに対応するユニキャスト通信を，20 字以内で答えよ。

(5) 表 5 中の［　せ　］～［　ち　］に入れる適切な字句を答えよ。

(6) 表 5 中のエントリ 1 の Action を答えよ。

設問 3　〔クラウドサービス利用拡大の検討〕について，(1)～(5) に答えよ。

(1) 図 6 中の［　つ　］に入れる適切な字句を答えよ。

(2) 図 6 中のゾーンファイルの定義内容を参考にして，図 5 中の a1 によって名前解決される FQDN を答えよ。

(3) 図 6 中のゾーンファイルの定義内容を参考にして，図 5 中の b1 によって名前解決される FQDN を答えよ。

(4) 本文中の下線 (iv) について，より適したエッジサーバが選択される場合を，50 字以内で述べよ。

(5) 本文中の下線 (v) の場合に，B 社 CDN の適用によって解消される TAT 悪化の要因を二つ挙げ，それぞれ 20 字以内で答えよ。

設問 4　〔A 社向け IaaS 環境のバックアップの検討〕について，(1)～(5) に答えよ。

(1) 本文中の下線 (vi) の準備作業を 40 字以内で述べよ。

(2) 本文中の下線 (vii) について，置換え前と置換え後のリソースレコードを，それぞれ答えよ。ここで，B 社 CDN は適用していないものとする。

(3) 新工場 LAN を使った自社設備利用 DR 案について，現行の工場内 LAN を使った自社設備利用 DR 案と比較して，障害復旧時間（RTO）が短縮できる要因を二つ挙げ，それぞれ 30 字以内で述べよ。

(4) B 社拠点（国外）利用 DR 案の NW に関する準備を，50 字以内で述べよ。

(5) B 社拠点（国外）利用 DR 案について，自社設備利用 DR 案と比べたときの利点を二つ挙げ，それぞれ 30 字以内で述べよ。