NW

平成29年度　秋期
ネットワークスペシャリスト試験
午後Ⅱ　問題

試験時間	14:30 ～ 16:30（2時間）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
4. 問題は，次の表に従って解答してください。

問題番号	問1，問2
選択方法	1問選択

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B又はHBの黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に**受験番号**を，**生年月日欄**に**受験票の生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **選択した問題**については，次の例に従って，**選択欄**の**問題番号**を**○印**で囲んでください。○印がない場合は，採点されません。2問とも○印で囲んだ場合は，はじめの1問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問2を選択した場合の例〕

選択欄	
1問選択	問1
	(問2)

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

正　誤　表

平成29年10月15日実施

ネットワークスペシャリスト試験　午後Ⅱ　問題

ページ	問題番号	行	誤	正	訂正の内容
9	1	下から13行目	B社のDNSサービス	C社のDNSサービス	下線部分を訂正する。

正　誤　表

平成29年10月15日実施

ネットワークスペシャリスト試験　午後Ⅱ　問題

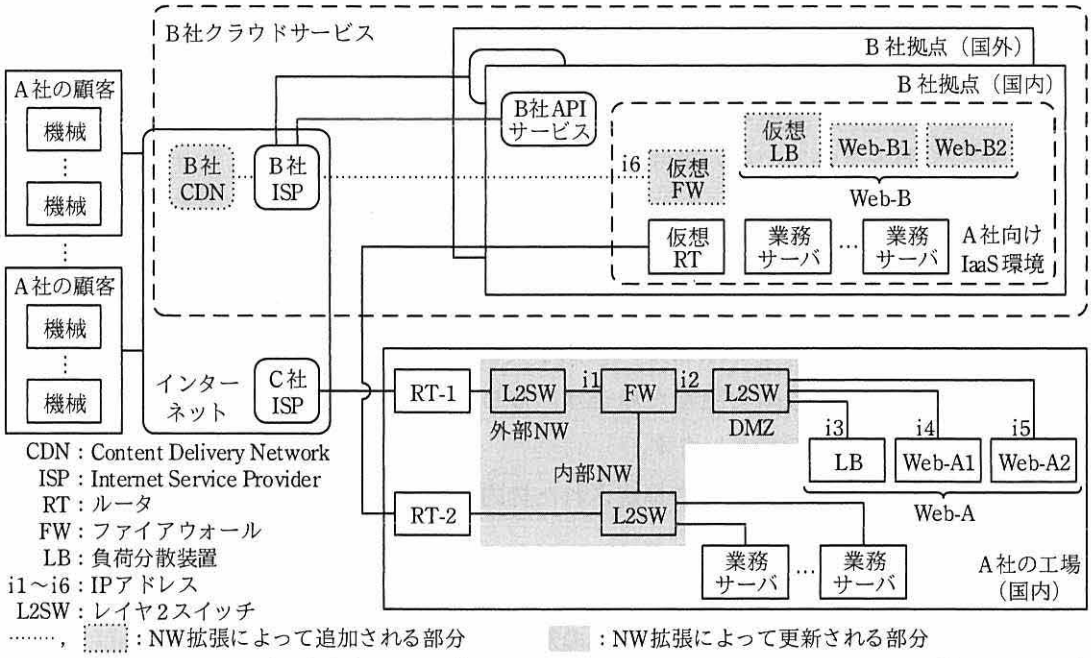
ページ	問題番号	箇所	誤	正	訂正の内容
17	2	図2 右上	c＋n	c＋(n－1)	下線部分を訂正する。

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

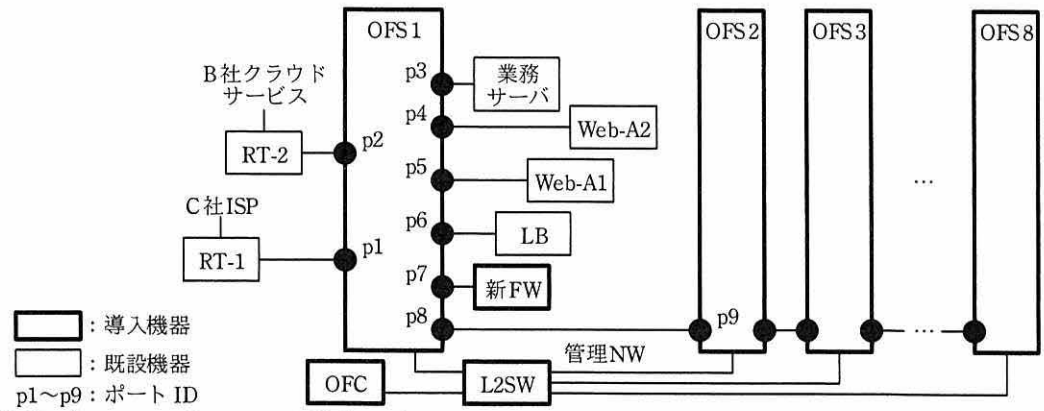
MF の例

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。

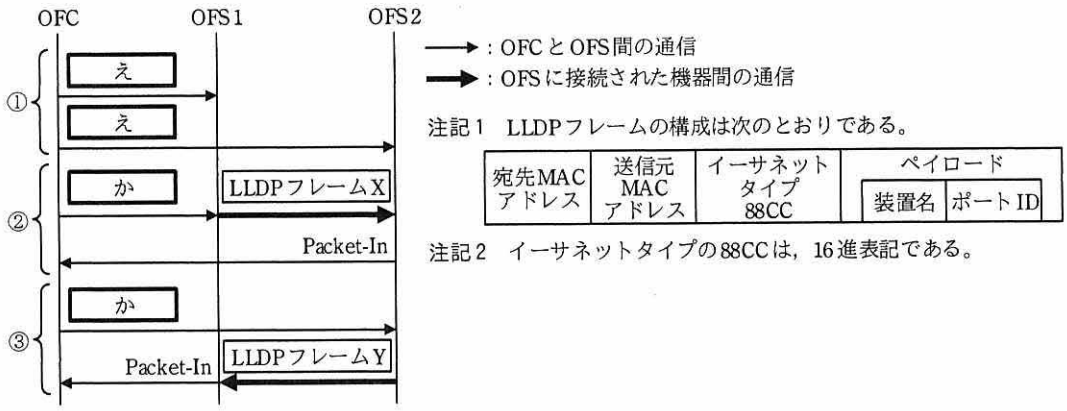


図3　OFS接続情報収集の通信シーケンス例

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。

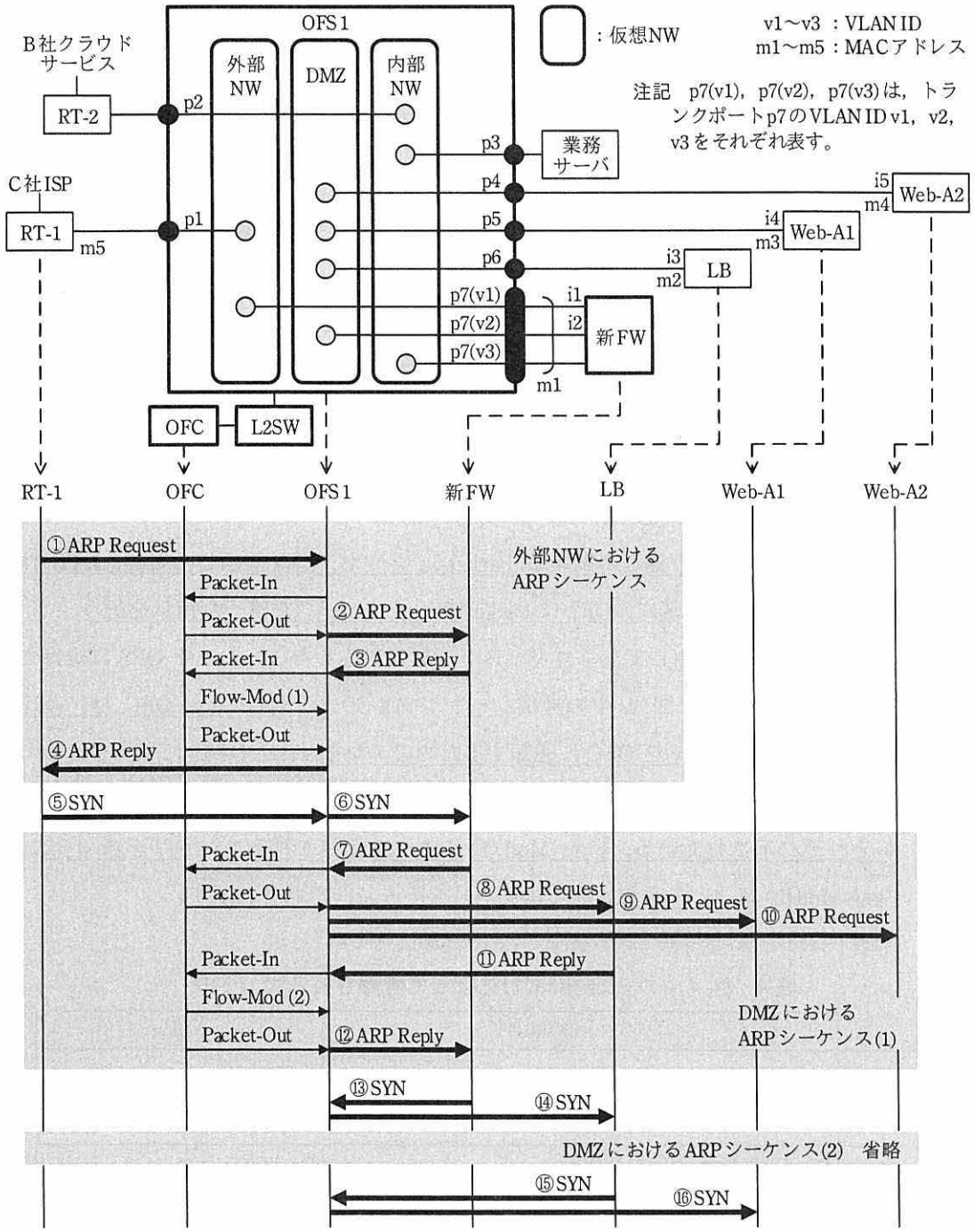


図 4　新工場 LAN の論理構成（抜粋）と通信シーケンス例

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。

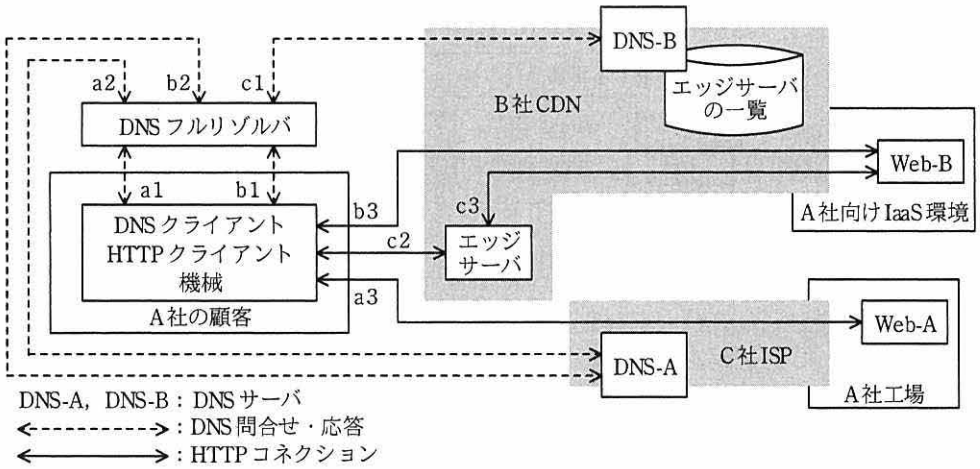


図5　B社CDNをA社に適用したときの概念図

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。

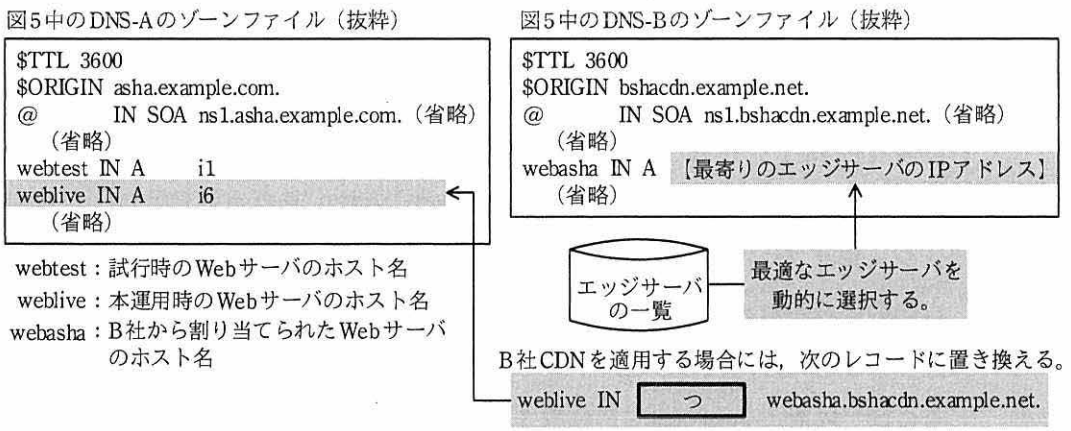


図6　D君が考えたエッジサーバへの切換え方法

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。

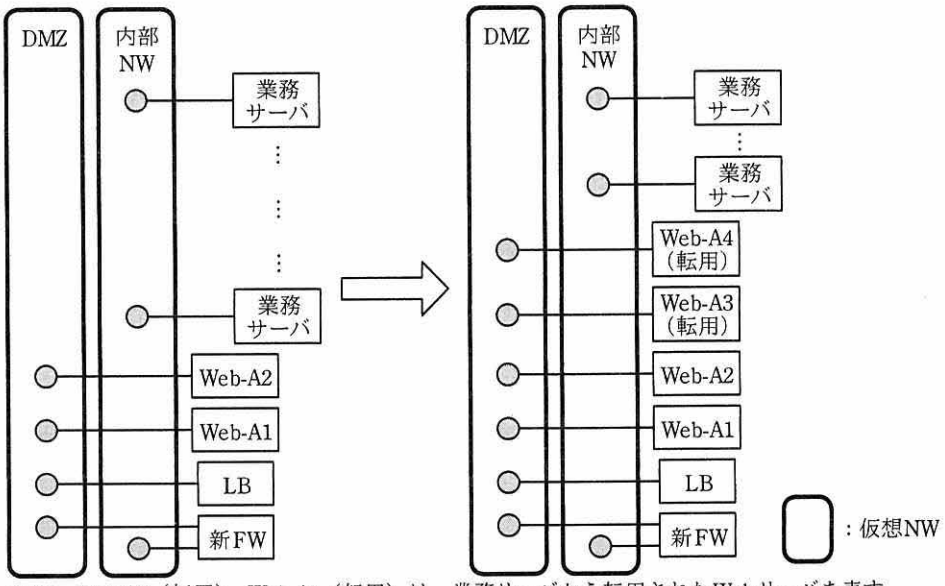
現在，A 社では，サーバ，LB，DNS-A の運用は自社の運用要員が行い，それ以外の NW 機器の運用は，ベンダに委託している。NW 拡張後は，自社の運用要員が，OFC の管理ソフトウェアを使って新工場 LAN の構成を変更し，API サービスを使ってクラウドサービス利用形態を変更するようになる。D 君は，自社の運用要員だけで対応できることを前提に，新システムの DR 案とその DR 案に必要な NW に関する準備を検討し，次の (1) と (2) を提案することにした。

(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。

問2　無線 LAN システムの導入に関する次の記述を読んで，設問 1～5 に答えよ。

Y 社は，中規模のネットワーク関連製品販売会社であり，オフィスビルの 2 フロアを使用している本社の他に複数の営業所がある。本社の営業部には 110 名の営業員が，営業所には合計 50 名の営業員が在籍している。本社と営業所の営業員には，ノート PC（以下，NPC という）の他にモバイル Wi-Fi ルータ（以下，Wi-Fi ルータという）が貸与され，社外での商品説明，在庫照会，電子メール（以下，メールという）の送受信などに使用されている。社内では，NPC を有線 LAN に接続して営業業務を行っている。インターネットアクセスは，本社 DMZ のプロキシサーバ経由で行われている。営業部の NPC は，同一 VLAN に属している。本社の現在の LAN 構成を図 1 に示す。

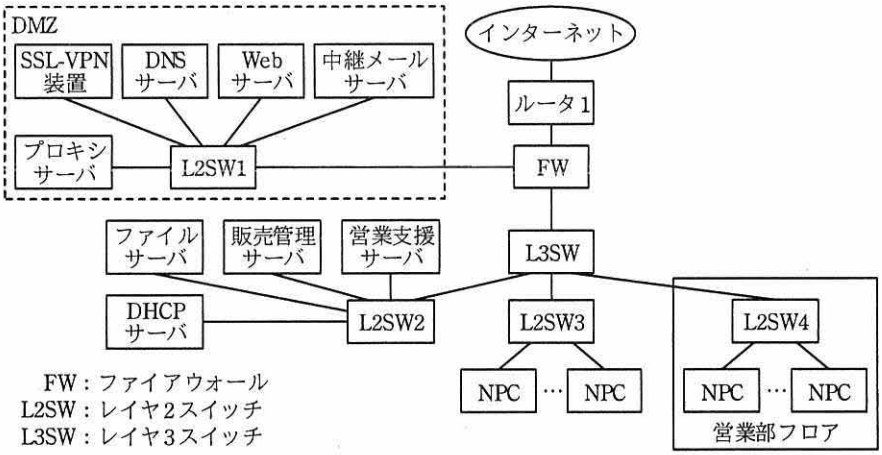


図 1　本社の現在の LAN 構成（抜粋）

〔営業部の課題と対策〕

営業部のフロアには，営業部のオフィスエリアの他に，応接室，会議室などの接客エリアがあるが，取引先の増加に伴って，接客エリアの不足に悩まされている。

Y 社を訪問する取引先の営業員（以下，来訪者という）の多くは，NPC を携帯しており，中には Wi-Fi ルータを持参して LTE 回線経由でインターネットを利用している者もいる。しかし，Wi-Fi ルータを持たない来訪者から，インターネット接続環境を提供してほしいとの要望が挙がっている。

Y社では，書類の電子化を推進した結果，書類棚やサイドキャビネットに保管している書類が半減し，机上の書類も一掃された。そこで，営業部の座席をフリーアドレスにしてオフィスエリアを縮小し，接客エリアを拡大することにした。

これらを実現する目的で，営業部フロアに無線 LAN システムを導入することを決め，無線 LAN 導入プロジェクトを発足させた。プロジェクト責任者には情報システム部（以下，情シスという）の M 課長が任命された。M 課長は，部下の N 主任と J 君をプロジェクトメンバに指名し，無線 LAN システムの設計を担当させることにした。

無線 LAN システムの設計に当たって，N 主任は，無線 LAN 技術の調査と選定を J 君に指示した。

〔無線 LAN 技術の調査と選定〕

N 主任の指示を受け，J 君は，無線 LAN 技術を調査し，その結果を表 1～3 にまとめた。IEEE 802.11 で使用される周波数帯を表 1 に，無線 LAN のアクセス制御方式を表 2 に，無線 LAN のデータ暗号化方式を表 3 に示す。

表 1　IEEE 802.11 で使用される周波数帯

規格	周波数帯	伝送速度
802.11n	[a] GHz，[b] GHz	最大 600 M ビット／秒
802.11ac	[b] GHz	最大 6.93 G ビット／秒

表 2　無線 LAN のアクセス制御方式

方式	機能
SSID（又は ESSID）	無線 LAN アクセスポイントの識別子によって制御する機能
[c] 接続拒否	SSID が空白又は [c] での接続要求を拒否する機能
SSID 隠蔽	ビーコン信号に SSID を含めない機能
MAC アドレスフィルタリング	送信元 MAC アドレスによって，無線 LAN アクセスポイントに対するクライアントのアクセスを制御する機能
IEEE 802.1X 認証	RADIUS サーバを利用するなどしたクライアント認証機能

表3　無線 LAN のデータ暗号化方式

方式	説明
WEP （Wired Equivalent Privacy）	RC4 と呼ばれる暗号化アルゴリズムを使用した［　d　］鍵暗号方式
WPA （Wi-Fi Protected Access）	暗号化アルゴリズムは WEP と同じ RC4 を使用するが，暗号化プロトコルに TKIP（Temporal Key Integrity Protocol）を使用して暗号強度を高めた方式
WPA2 （Wi-Fi Protected Access 2）	暗号化アルゴリズムは AES に対応し，暗号化プロトコルに CCMP（Counter-mode with CBC-MAC Protocol）を使用した，WPA よりも堅牢（ろう）な IEEE［　e　］準拠の方式

Y 社の NPC は，IEEE 802.11ac 対応の無線 LAN アダプタを内蔵しているので，IEEE 802.11ac 対応の無線 LAN アクセスポイント（以下，AP という）を導入する。来訪者の NPC の中には，IEEE 802.11n しか使用できないものもあると考えられたので，IEEE 802.11n にも対応した AP 製品を選定すれば，来訪者へのインターネットアクセス環境も提供できる。

無線 LAN では通信に電波が使用されるので，盗聴や不正アクセスを防ぐ対策が重要である。そこで，J 君は，暗号化方式と認証方式について検討した。

〔暗号化方式と認証方式の検討〕

無線 LAN のデータ暗号化方式について J 君が検討した結果を，次に示す。

(1) WEP では，1 バイト単位の［　f　］暗号である RC4 を使用して，パケットの暗号化が行われる。WEP は，一つの AP と複数の無線 LAN 端末間で WEP キーを共有し，WEP キーと IV（Initialization Vector）を基に，暗号鍵であるキーストリームを生成する。WEP は，［　g　］の WEP キーが使用され続けることに加え，暗号化アルゴリズムも複雑ではないことから，短時間での暗号解読が可能になっているので採用しない。

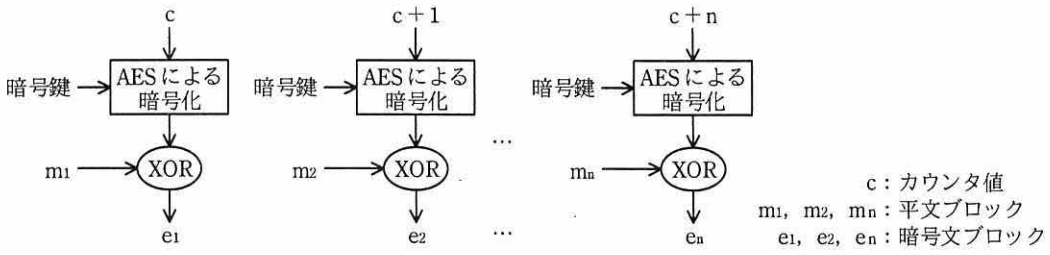
(2) WPA では，TKIP によって暗号鍵を生成する。TKIP では，暗号鍵の基になる一時鍵（Temporal Key）が動的に生成される。エンタープライズモードの場合，一時鍵は，IEEE 802.1X の認証成功後に［　h　］で動的に生成されてクライアントに配布される PMK（Pairwise Master Key）を基に，無線 LAN 端末及び

[h]の両者で生成される。TKIP では，フェーズ 1 で，一時鍵，IV 及び無線 LAN 端末の[i]の三つを混合してキーストリーム 1 を生成する。フェーズ 2 で，キーストリーム 1 に IV の拡張された部分を混合して，暗号鍵であるキーストリーム 2 を生成する。キーストリーム 1 とキーストリーム 2 は，通信途中に変更される。2 段階の鍵混合，キーストリームの変更によって，WEP よりも高い安全性を実現しているが，脆弱(ぜい)性が報告されているので採用しない。

(3) WPA2 では，AES をベースにした CCMP が採用されている。

WPA2 では，事前[j]の方法及び PMK の保持方法が規定されている。これらによって，無線 LAN 端末が AP 間を移動（以下，ハンドオーバという）するタイミングでの認証や認証済みの AP に戻ってきたときの PMK の再生成が不要になることから，ハンドオーバ時間が短縮される。

AES はブロック暗号なので，暗号化するメッセージを一定サイズのブロック単位に分割して処理する必要がある。メッセージをブロック単位に分割すると，最後のメッセージがブロックサイズに満たない場合もあるので，CCMP ではカウンタモードが採用されている。カウンタモードでは，暗号化するメッセージをダイレクトに暗号化するのではなく，ブロックサイズと同じバイト数のカウンタ値を暗号化して，暗号化したカウンタ値と暗号化するメッセージとを XOR（排他的論理和）して暗号文を生成する。カウンタモードによる暗号化手順を図 2 に示す。



注記　平文は，m_1，m_2，…，m_nで表され，暗号文は，e_1，e_2，…，e_nで表される。

図 2　カウンタモードによる暗号化手順

CCMP では，①暗号化と復号は同じ手順で行われ，復号時も AES が使用される。

以上の検討を基に，暗号化方式は安全性が高い WPA2 を採用することにした。

次に，J君は，利用者認証方式について検討した。

WPA2の利用者認証には，パーソナルモードと，IEEE 802.1Xを利用するエンタープライズモードがある。営業員の認証にはエンタープライズモードを利用する。IEEE 802.1Xには複数の認証方式がある。その中でセキュリティが強固であるとともに，Y社のNPCでは標準サポートのEAP-TLSを利用することを考え，EAP-TLSの運用に適したRADIUSサーバ製品を選定することにした。

J君は，無線LANはIEEE 802.11acを採用し，IEEE 802.11nにも対応したAP製品を選定することと，暗号化方式はWPA2，認証方式はEAP-TLSを利用することをN主任に報告した。無線LANの規格，暗号化及び認証方式がN主任に了承され，次に，APの設置方法とディジタル証明書の配布方法についての検討を指示された。

〔APの設置方法の検討〕

J君は，フロア図面を基に，APの導入台数と設置について検討した。

現在，Y社では，NPCを100Mビット／秒で有線LANに接続しているので，無線LANでも100Mビット／秒程度の速度で通信できるようにしたい。

IEEE 802.11ac規格では，八つのチャネルを束ねる8チャネルボンディング（160MHzの帯域幅）を行えば，アンテナ1本当たり最大約867Mビット／秒の通信が可能である。8チャネルボンディングと8本のアンテナによるMIMO（Multiple Input Multiple Output）で8ストリームの同時伝送を行えば，理論上最大約6.93Gビット／秒で通信できる。②検討しているAP製品は，4チャネルボンディング（80MHzの帯域幅）まで行え，3本のアンテナが搭載されているので，1Gビット／秒以上の通信速度が達成できる。したがって，APに同時接続させるNPCを10台に制限すれば，1台のNPCで100Mビット／秒以上の通信速度を確保できる。そこで，APに同時接続させるNPC台数を10台に制限して，APの導入台数と配置を決めることにした。

現在，営業部には110名の営業員が在籍しており，営業部のオフィスエリアには120名の収容スペースがある。本社の営業員の在席率は最大で60%程度なので，オフィスエリアを80%に縮小して，削減した20%を接客エリアにすれば接客エリア不足の解消になる。オフィスエリアには，最大で約66名の営業員が同時に在席することになるが，余裕をもたせて8台のAPを設置し，接客エリアには4台のAPを設置する。合計12台のAPの個別管理は困難なので，無線LANコントローラ（以下，

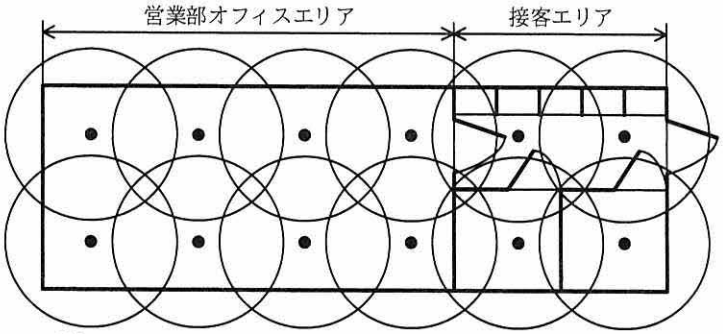
WLC という）も導入する。調査したところ，WLC には複数の方式があったが，次の三つの主要機能をもつ製品を選定することにした。

・有線 LAN 経由での複数の AP に対する設定変更，ファームウェアのアップデートなどの一括処理機能
・AP の負荷分散制御，PMK の保持などによるハンドオーバ制御機能
・利用者認証，認証 VLAN などのセキュリティ対策機能

選定する WLC 製品の概要を次に示す。

WLC は分散処理方式で，通信データの暗号化と復号を AP に任せるものである。WLC で EAP-TLS を利用するときは，AP と WLC 間でトンネルが設定され，無線 LAN 端末と WLC 間で認証情報の交換が行われる。WLC は，利用者認証を行った後，利用者 ID に対応した VLAN を AP に設定する認証 VLAN 機能をもっている。③認証後に行われる無線 LAN 端末による通信は，WLC を経由しない。

AP は，電波の到達性を考慮して天井に設置する。営業部のオフィスエリアに，営業員が自由に着席できる机が均等に配置されたときの，営業部フロアへの AP の設置イメージを図 3 に示す。



注記　図中の円弧は，APがカバーするエリア（以下，セルという）を示す。

図 3　営業部フロアへの AP の設置イメージ

AP の設置場所は，営業部フロアでの電波伝搬状態を測定してから決める。このとき，④外来電波による悪影響が発生する可能性があるかどうかを調査し，必要に応じて対策を講じる。電波伝搬状態の測定，外来電波の影響調査，AP の設置設計及び

設置工事は，業者に委託する。

AP は天井に設置することから，天井裏でのケーブル配線が必要になる。AP を接続する L2SW を営業部フロアに設置すれば，L2SW と全ての AP とを LAN ケーブルで直結できる。L2SW の PoE（Power over Ethernet）機能を利用することによって，LAN ケーブル経由で AP に電源が供給できるので，PoE 対応の AP を導入する。このとき，AP を収容することになる図 1 中の L2SW4 は，PoE 対応の製品に交換し，適切な場所に設置する必要がある。

以上の検討結果を基に，J 君は，導入する AP，WLC 及び RADIUS サーバ製品を選定した。選定した AP 製品の消費電力は最大 18 W なので，IEEE 802.3af 規格では供給電力が不足することが分かった。そこで，⑤ IEEE 802.3at 対応の L2SW を 1 台導入することにした。

次に，J 君は，ディジタル証明書の配布方法について検討した。

〔ディジタル証明書の配布方法の検討〕

ディジタル証明書の配布方法について J 君が検討した結果を，次に示す。

選定した RADIUS サーバ製品は，EAP-TLS で必要になるディジタル証明書（サーバ証明書又はクライアント証明書）を発行する CA（Certification Authority）機能をもっている。サーバ証明書とクライアント証明書は，RADIUS サーバの CA 機能を使って発行する。

クライアント証明書は，情シスの担当者が本社の営業員の NPC に直接インストールすれば安全であるが，情シスの負担が大きい。そこで，本社 LAN に，クライアント証明書を NPC にダウンロードさせるサーバ（以下，ダウンロードサーバという）を新規に構築して，LAN 経由でクライアント証明書を配布すれば情シスの負担が抑えられる。

ダウンロードサーバによるクライアント証明書の配布案内は，無線 LAN 導入後に，情シスから全営業員宛てに一斉メールで通知する。案内文には，ダウンロードサーバの導入目的，利用方法，ダウンロードサーバの URL などを記載する。その後，各営業員に，ダウンロードサーバ利用のための利用者 ID とパスワードを個別に連絡する。営業員は，情シスからの案内を基に，クライアント証明書のインストールを行

う。

J 君は，ダウンロードサーバの機能とクライアント証明書の運用について検討した。検討結果を次に示す。

(1) クライアント証明書の管理機能

ダウンロードサーバは，RADIUS サーバで生成されたクライアント証明書と⑥その他に NPC で必要となる情報を RADIUS サーバからコピーし，RFC 7292 で規定されている PKCS #12 形式のファイルに変換して管理する。

(2) NPC へのダウンロード機能

ダウンロードサーバは，アクセスした営業員を利用者 ID，パスワードで認証し，認証を受けた営業員の NPC に，PKCS #12 形式のファイルを一度だけダウンロードさせる。NPC は，ダウンロードしたファイルを直接インポートできる。

(3) クライアント証明書の運用

情シスの担当者は，クライアント証明書の有効期限の 1 か月前に，RADIUS サーバでクライアント証明書を発行し，ダウンロードサーバに保管して，クライアント証明書の更新案内を当該営業員にメールで通知する。

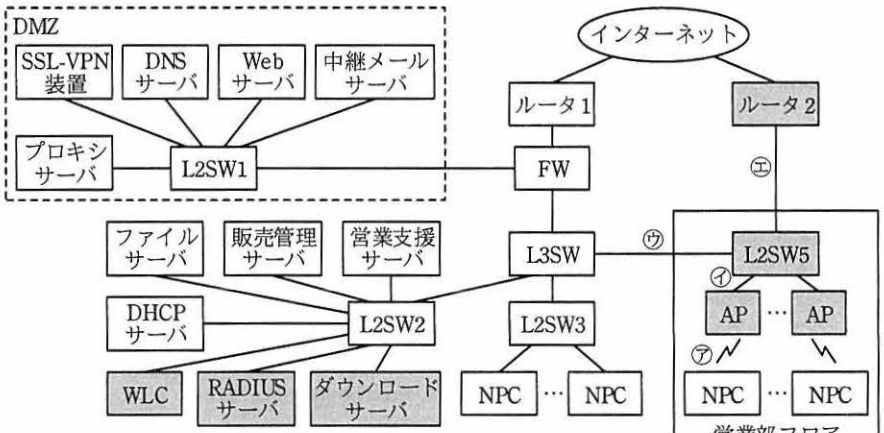
次に，J 君は，ダウンロードサーバの設置場所について検討した。

最初に，無線 LAN 経由でダウンロードサーバにアクセスさせる方法を検討した。この方法では，NPC にクライアント証明書がインストールされていないので，認証エラーになる。そこで，認証エラー時に WLC の認証 VLAN 機能によって，特別な VLAN を AP に設定し，この VLAN にダウンロードサーバを設置することを考えた。しかし，その場所にダウンロードサーバを設置すると，⑦クライアント証明書の配布に関してセキュリティ上問題がある。さらに，クライアント証明書の更新のためのダウンロードもできない。そこで，営業部オフィスエリアの有線 LAN 接続でアクセスできる場所にダウンロードサーバを設置することにした。無線 LAN に移行した後，営業部オフィスエリアをフリーアドレスにして NPC 接続用の有線 LAN は撤去するが，クライアント証明書の更新は無線 LAN 経由で可能である。しかし，⑧状況によっては，クライアント証明書をダウンロードできない本社の営業員も出てくる。その営業員には，情シスの担当者がクライアント証明書などの必要な情報を NPC にインストールして，当該営業員に渡す。

J 君は，AP の設置方法とディジタル証明書の配布方法について N 主任に説明し，了承されたので，最後に，既設 LAN への無線 LAN の接続構成の設計を行った。

〔既設 LAN への無線 LAN の接続構成の設計〕

J 君が設計した，既設 LAN に無線 LAN システムを導入したときの LAN 構成を図 4 に示す。



注記　網掛け部分は，新規に導入する機器を示す。

図 4　既設 LAN に無線 LAN システムを導入したときの LAN 構成（抜粋）

Y 社では，DHCP サーバで PC と NPC に IP アドレスなどのネットワーク情報を付与している。無線 LAN 導入後も，本社の営業員の NPC には DHCP サーバでネットワーク情報を付与する。

EAP-TLS で認証を受けた本社の営業員の NPC には，営業員向けの VLAN（VLAN100）を割り当て，既設の有線 LAN 使用時と同じ作業ができるようにする。オフィスエリアの AP には来訪者の NPC は接続させないが，接客エリアの AP には営業員と来訪者が無線 LAN を同時に利用できる設定を行う。

NPC を持参した来訪者には，Y 社の担当者が，⑨ WPA2 又は WPA のパーソナルモードで無線 LAN に接続するための情報を教える。来訪者は，教えられた情報を NPC に設定することで，無線 LAN の利用が可能になる。来訪者の NPC には，AP が ESSID に対応した来訪者向けの VLAN（VLAN200）を割り当てる。VLAN200 が割り当てられることによって，来訪者の NPC は，無線 LAN へのアソシエーション後に，

ルータ 2 がもつ DHCP 機能でネットワーク情報が付与され，インターネットアクセスだけができるようになる。

J 君は，以上の設計内容を N 主任に説明した。N 主任は，J 君の設計内容を基に無線 LAN 導入計画書を作成し，J 君と一緒に M 課長に説明したところ，導入計画書は M 課長に承認され，実施に移されることになった。

設問 1　表 1～3 中の［ a ］～［ e ］に入れる適切な字句又は数値を答えよ。

設問 2　〔暗号化方式と認証方式の検討〕について，(1)，(2) に答えよ。

(1) 本文中の［ f ］～［ j ］に入れる適切な字句を答えよ。

(2) 本文中の下線①について，図 2 中の暗号文ブロック e1 を平文ブロック m1 に復号する手順を，40 字以内で述べよ。

設問 3　〔AP の設置方法の検討〕について，(1)～(5) に答えよ。

(1) 本文中の下線②について，検討している AP 製品で最大約 867 M ビット／秒の通信速度を得るのに，最低限必要な周波数帯域幅とアンテナ本数を，それぞれ答えよ。

(2) 本文中の下線③の方式について，無線 LAN 端末による通信が WLC を経由する方式と比較したときの利点を二つ挙げ，それぞれ 40 字以内で述べよ。

(3) 本文中の下線④の悪影響の内容を，25 字以内で述べよ。

(4) 図 3 の構成で AP を設置して，チャネルボンディングした周波数帯が重ならないようにするためには，少なくとも幾つの周波数帯のグループが必要になるかを答えよ。また，各 AP のセルを重ねる目的を，25 字以内で述べよ。

(5) 本文中の下線⑤について，IEEE 802.3at 規格の PoE 機能の呼称，及び当該 L2SW で今回必要になる最小供給電力を，それぞれ答えよ。

設問 4　〔ディジタル証明書の配布方法の検討〕について，(1)～(3) に答えよ。

(1) 本文中の下線⑥について，NPC で必要になる情報を二つ挙げ，それぞれ 15 字以内で答えよ。

(2) 本文中の下線⑦の問題を，60 字以内で述べよ。

(3) 本文中の下線⑧について，ダウンロードできない本社の営業員を，25 字以内で答えよ。ただし，NPC の紛失，故障などで新たに貸与されるケースは除

く。

設問5　〔既設 LAN への無線 LAN の接続構成の設計〕について，(1)～(6) に答えよ。

(1) 図 4 中で，IEEE 802.1X のサプリカントとなる機器及びオーセンティケータとなる機器を，図 4 中の機器名でそれぞれ答えよ。

(2) 本文中の下線⑨について，来訪者に教える情報を二つ挙げ，それぞれ答えよ。

(3) 図 4 中で，今回新たにタグ VLAN が設定される箇所を，図 4 中の㋐～㋓から選び，記号で答えよ。

(4) 図 4 の構成で，来訪者の NPC にインターネットアクセスだけを可能にするための，L2SW5 への VLAN 設定内容を，40 字以内で述べよ。

(5) 図 4 中の NPC が認証された後に WLC に障害が発生した場合，当該 NPC で発生する問題を，20 字以内で答えよ。また，その理由を，40 字以内で述べよ。

(6) 図 4 中で，認証後の営業員の NPC によるインターネットアクセスにおいて，経由する機器名又はサーバ名を，【転送経路】の表記法に従い，経由する順に全て列挙せよ。

【転送経路】

NPC → | 経由する順に全て列挙 | → インターネット

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 退室可能時間に途中で退室する場合には，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	15:10 ～ 16:20

7. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，次のものに限ります。

   なお，会場での貸出しは行っていません。

   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。