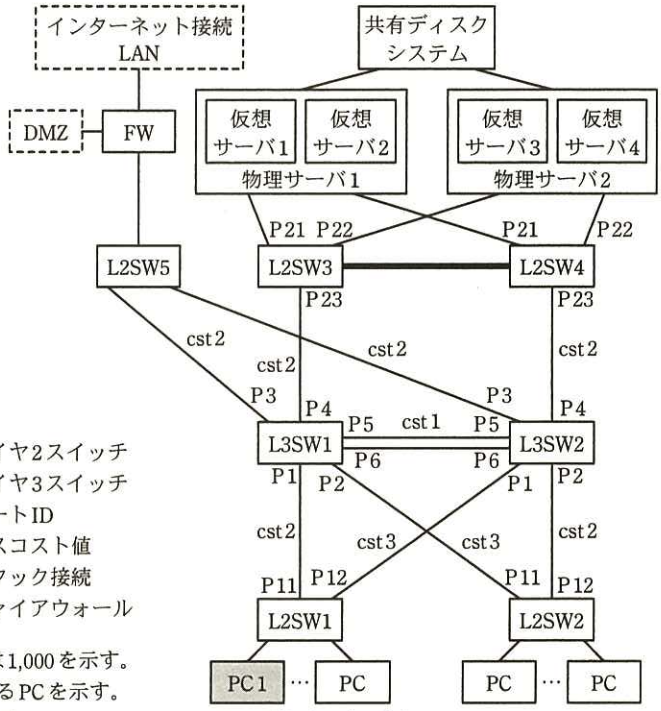
問1　無線 LAN の導入に関する次の記述を読んで，設問1～5に答えよ。

E 社は，コンピュータ関連製品の販売会社である。本社の他に複数の営業所があり，販売代理店経由で製品を販売している。本社では，販売，購買，会計などの基幹システムと，販売業務を支援する各種業務システムを運用している。これらのシステムは，複数台の物理サーバ上の仮想サーバで稼働させている。本社のネットワークシステム構成を，図1に示す。

VLANが設定されているポートと
VLAN設定内容

ポートID	VLAN ID
P1	10
P2	20
P3	120
P4，P23	100，110
P5，P6	10，20，100，110，120
P21，P22	100，110



L2SW1～L2SW5：レイヤ2スイッチ
L3SW1，L3SW2：レイヤ3スイッチ
P1～P6，P11，P12，P21～P23：ポートID
cst1～cst3：パスコスト値
━━━：スタック接続
FW：ファイアウォール

注記1　cst1は10，cst2は100，cst3は1,000を示す。
注記2　網掛け部分は，設問で使用されるPCを示す。

図1　本社のネットワークシステム構成（抜粋）

ここ数年，E 社の売上は低迷している。そこで，E 社では競争力を強化するために，急速に発展したスマートフォンやタブレット端末などのモバイル端末（以下，MN という）を活用して，顧客の要望に即応できるような体制づくりに着手することを決めた。第1段階として，本社に MN の活用環境を構築・整備することになり，情報システム部の R 課長は，部下の S 主任に無線 LAN 導入案の検討を指示した。

S 主任は，無線 LAN 導入案の検討に先立ち，ネットワーク構成の解析訓練を兼ねて，後輩の J 君に本社のネットワーク構成，ネットワークの運用状況などの調査を指示した。

〔現状調査〕

S 主任の指示を受けた J 君は，本社のネットワークシステムの現状調査を行った。調査結果は，次のとおりである。

・現在，本社の機器には固定 IP アドレスが設定されている。利用できる基幹システムと業務システムは，部署ごとに決められている。利用制限は，二つの方法によって行われている。一つは，アプリケーションプログラムに組み込まれた認証処理によるアクセス制御である。もう一つは，図 1 中の，PC からサーバへの経路上の機器である［　ア　］に設定された，パケットフィルタリング条件の適用である。パケットフィルタリング条件は，接続を許可する PC とサーバの IP アドレスの組合せで記述されている。

・物理サーバ又は仮想サーバに障害が発生したときには，他の物理サーバで新たに仮想サーバを起動して，基幹システム，業務システムを再稼働させる。

・図 1 中の，L3SW1 及び L3SW2 の P5，P6 には，リンクアグリゲーションが設定されている。

・物理サーバの，L2SW3 と L2SW4 への接続ポートには，アクティブ／アクティブ構成のチーミング機能が設定されている。

・L2SW と L3SW では，STP（Spanning Tree Protocol）が動作している。L3SW1 をルートブリッジとするために，L3SW1 のブリッジ ID は［　イ　］の値となっている。各リンクのパスコスト値と VLAN ID は，図 1 中に記載された内容である。

・L3SW1 と L3SW2 には，VRRP で仮想ルータが設定されている。L3SW1 と L3SW2 の仮想ルータの設定内容は，表 1 のとおりである。

表 1　L3SW1 と L3SW2 の仮想ルータの設定内容

項目＼スイッチ	L3SW1					L3SW2				
	VR1	VR2	VR3	VR4	VR5	VR1	VR2	VR3	VR4	VR5
VRRP グループ ID	1	2	10	11	12	1	2	10	11	12
仮想 IP アドレス	VIP1	VIP2	VIP3	VIP4	VIP5	VIP1	VIP2	VIP3	VIP4	VIP5
Priority 値	200	100	200	100	200	100	200	100	200	100
所属 VLAN ID	10	20	100	110	120	10	20	100	110	120

注記　VR1 ～ VR5 は，仮想ルータ名を示す。

・L2SW1 に接続された PC のデフォルトゲートウェイには VIP1 が，L2SW2 に接続された PC のデフォルトゲートウェイには VIP2 が設定されている。また，仮想サーバ

1と仮想サーバ2のデフォルトゲートウェイにはVIP3が，仮想サーバ3と仮想サーバ4のデフォルトゲートウェイにはVIP4が設定されている。これらの設定によって，仮想ルータの負荷分散が行われている。

J君は，調査結果を整理し，S主任に報告した。現状のネットワーク構成の解析ができたので，S主任は，MNでネットワークシステムを利用するための，無線LANの導入方法を検討することにした。さらに，無線LANの導入では，社内の電波状態を調査するサイトサーベイも必要と考え，サイトサーベイで実施すべき内容についても併せて検討するよう，J君に指示した。

〔無線LANの調査と導入検討〕

J君は，まず，無線LANの特徴とセキュリティ上の問題点を調査した。

無線LANの最初の標準規格IEEE [ウ] は，物理レイヤとMACレイヤの規格で構成され，その規格中には，次に示す認証と暗号化方式が標準化されている。

(1) 認証

① オープンシステム認証

本認証は，アクセスポイント（以下，APという）での端末認証が，実質的には行われない。

② 共有鍵認証

本認証は，MNが，APと共有するWEPキーを使用して，APから受信した乱数を [エ] して返送する，チャレンジレスポンス方式で行われる。ただし，WEPキーが，電波を不正に傍受している装置に見破られると，<u>（あ）不正アクセス以外にも重大なセキュリティリスクが発生する</u>ので，この認証方式は，一般に利用されない。

(2) 暗号化方式

方式としてWEPが規定されている。WEPは，[オ] と呼ばれる暗号アルゴリズムを基にした共通鍵暗号を採用している。暗号化には，WEPキーと呼ばれる共通鍵が使用される。MNとAPには，同じWEPキーを設定する必要があり，動的に鍵の変更が行われないことから，解読される危険性が高い。

以上の，IEEE [ウ] のセキュリティ上の問題点を解決するために，IEEE

802.11i が規格化された。IEEE 802.11i を基に策定された WPA2（Wi-Fi Protected Access 2）では，セキュリティ面の改善の他に，（い）事前認証及び認証キーの保持（Pairwise Master Key キャッシュ）を行う方法が規定されているので，接続先の AP を切り替える時間を短縮することが可能になった。

無線 LAN において，MN が異なる AP 間を渡り歩けるような機能のことを，ローミングという。ローミングのためには，ローミングの対象となる全ての AP について，ネットワークの識別子である [カ] が同じである必要がある。MN が接続先の AP を切り替えるときには，新たな接続先となる AP との間で，論理的接続であるアソシエーション，認証処理などが行われる。

IEEE 802.1X 認証を行った場合の，無線 LAN への接続手順を，図 2 に示す。

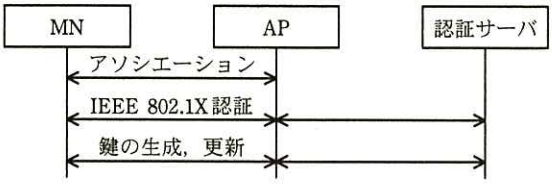
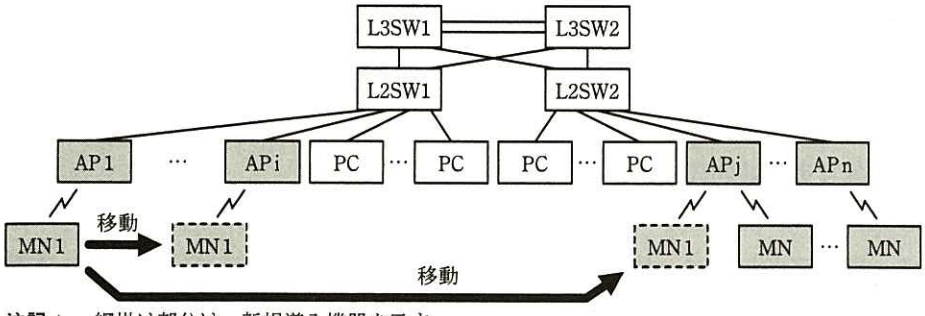


図 2　無線 LAN への接続手順

調査結果を基に，J 君は，導入する無線 LAN には WPA2 を利用し，認証には，IEEE 802.1X で利用可能な方式のうち，運用が容易な PEAP を採用することにした。

次に，J 君は，図 1 のネットワークシステムに，無線 LAN を導入する構成を検討した。J 君がまとめた，AP の導入構成案を，図 3 に示す。



注記 1　網掛け部分は，新規導入機器を示す。
注記 2　本図では，図 1 中の L3SW1 と L3SW2 から下側を示した。

図 3　AP の導入構成案（抜粋）

新規に導入する MN でも，現状と同等のセキュリティ対策が行われるように，MN には，部署ごとに割り当てられた固定 IP アドレスを設定したい。しかし，その場合，E 社の構成では次のような問題が発生する。図 3 において，AP1 と接続していた MN1 が移動して，図 2 の手順で AP i に接続したとき，MN1 は通信を継続できるが，AP j に接続すると，（う）サーバやインターネットとの通信ができなくなってしまう。

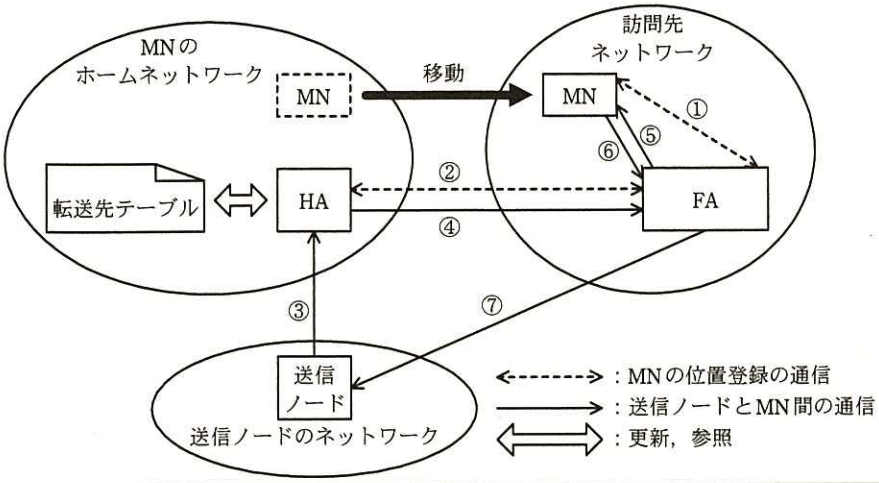
J 君は，この問題の対応策について S 主任に相談した。S 主任は，AP を集中管理・集中制御する無線 LAN コントローラ（以下，WLC という）を導入すれば，問題を解決できるのではないかと考え，WLC の調査を指示した。

〔サブネット間のローミングの調査と設計〕

指示を受けた J 君は，WLC について調査した。調査結果は，次のとおりである。

WLC は，AP と連携して認証，暗号化，電波出力調整，ローミングなどの機能を実現する。WLC の実装は，ベンダによって異なっている。ベンダ Y 社の WLC を導入すると，サブネット間のローミングが可能になることが分かった。Y 社の WLC は，RFC 2002 で基本動作の仕組みが定義されているモバイル IP 技術を基にして，これに Y 社独自の工夫を加えて，無線 LAN におけるローミングを可能にしている。そこで，J 君は，基になっている RFC 2002 のモバイル IP について調査した。調査結果は，次のとおりである。

・モバイル IP は，MN が異なるサブネットに移動しても，MN との通信を試みるホスト（以下，送信ノードという）が MN と通信できるようにする技術である。
・モバイル IPv4 では，MN と送信ノード間の通信を仲介する，home agent（以下，HA という）と foreign agent（以下，FA という）が存在する。
・MN が本来稼働すべきネットワークを，ホームネットワークという。MN には，ホームネットワークでホームアドレスと呼ばれる IP アドレスが付与されている。
・HA は，MN のホームネットワークに設置されている。それに対して FA は，MN の移動先である訪問先ネットワークに設置されている。
・移動先の MN にパケットを渡すための転送先 IP アドレスは，気付アドレスと呼ばれる。気付アドレスは，訪問先ネットワークに設置された FA の IP アドレスでもある。
・HA と FA を経由した MN の位置登録の通信手順及び送信ノードと MN 間の通信手順は，図 4 のとおりである。



【MN の位置登録の通信手順】

① MN は，FA から送出される Advertisement メッセージを受信し，ホームネットワークにいるのか，訪問先ネットワークにいるのかを判別する。訪問先ネットワークへの移動を検出すると，Advertisement メッセージの中から気付アドレスを取得し，MN 自体のホームアドレスと気付アドレスを対応付けて，位置登録の要求を行う。

② FA は，MN から受信した位置登録情報を，MN のホームネットワークの HA 宛てに送信する。HA は，MN の気付アドレスとホームアドレスを対にして，転送先テーブルに登録する。登録後，登録完了メッセージを FA 宛てに送信する。

【送信ノードと MN 間の通信手順】

③ 送信ノードから送信された MN 宛てのパケットが，MN のホームネットワークに到達すると，（え）HA によって代理受信される。

④ HA は，転送先テーブルを参照して移動中の MN の気付アドレスを取得し，受信したパケットをカプセル化して，気付アドレス宛てに転送する。

⑤ FA は，受信したパケットのカプセル化を解除して，MN に送信する。

⑥ MN のデフォルトゲートウェイに FA が設定されている場合は，MN が送信ノード宛ての返送パケットを，デフォルトゲートウェイである FA 宛てに送信する。

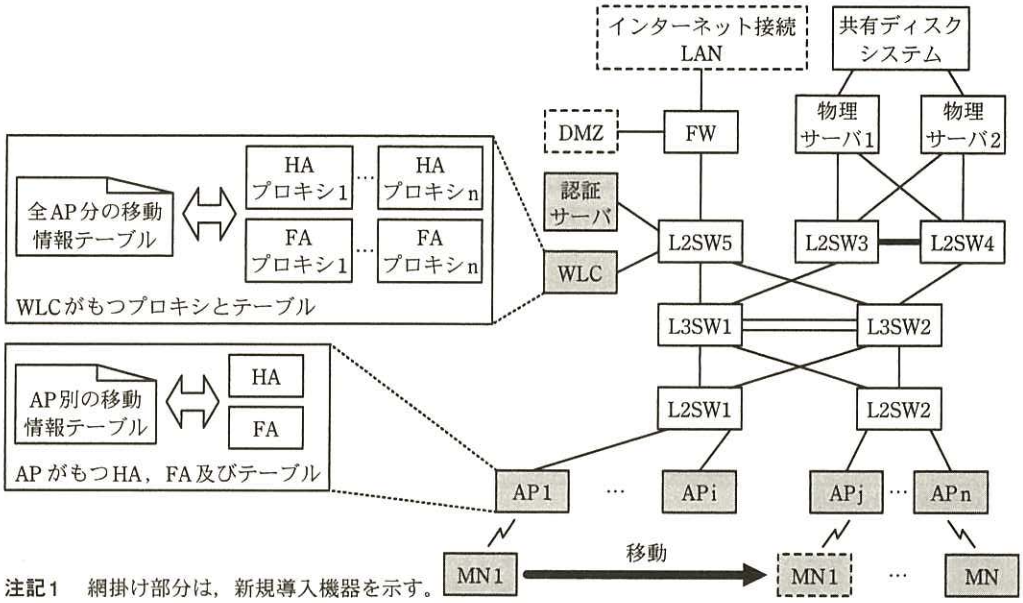
⑦ FA は，受信したパケットを送信ノードに中継する。

図 4　HA と FA を経由した MN の位置登録の通信手順及び送信ノードと MN 間の通信手順

図 4 に示されているように，RFC 2002 の MN にはモバイル IP 機能の実装が必要である。

E 社が想定する MN にはモバイル IP 機能がない。しかし，Y 社の WLC には，モバイル IP 機能が実装されていない MN でも，サブネット間のローミングができるような工夫が施されている。

Y 社の資料を参考に，J 君は，WLC と AP を導入するときの構成を，図 5 のように設計した。また，モバイル IP に関連して WLC と AP がもつ機能の名称と機能の概要を整理し，表 2 を作成した。



注記1　網掛け部分は，新規導入機器を示す。
注記2　HAプロキシは，HAの代理として，WLC内でHAの機能の一部を担う。
注記3　FAプロキシは，FAの代理として，WLC内でFAの機能の一部を担う。

図5　WLCとAPを導入するときの構成（抜粋）

表2　モバイルIPに関連してWLCとAPがもつ機能の名称と機能の概要

機器名	機能の名称	機能の概要
AP	HA	MNのホームネットワークに送信されたMN宛てのパケットを受信し，AP別の移動情報テーブルで調べ，そのMNが移動中のときは，受信したパケットをカプセル化してWLCのFAプロキシに送信する。
	FA	① 無線LAN側で受信したパケットの送信元IPアドレスが，当該FAが稼働するAPのサブネットと異なるサブネットのもののときは，保持する経路情報に基づいて，受信したパケットを中継処理する。 ② WLCから送信されたパケットを受信したときは，受信したパケットのカプセル化を解除して，MNに送信する。
WLC	（各APの）HAプロキシ	MNの認証時に，MNとMNのホームネットワークの情報，又はMNの訪問先ネットワークに関連する情報を，WLCが保持する全AP分の移動情報テーブルに登録するとともに，登録情報を該当するAPのHAに送信する。
	（各APの）FAプロキシ	HAから送信された移動中のMN宛てのパケットを受信し，カプセル化を解除して，移動情報テーブルから移動先のAPを判別した後，再度カプセル化してパケットを移動先のAPのFAに送信する。

図5に示したように，Y社のAPはHAとFAをもち，WLCはHAプロキシとFAプロキシをもつ。

MNがAPと接続するときに行われるIEEE 802.1Xの認証では，WLCがオーセンテ

ィケータとして働く。MN の認証時に，WLC で稼働する HA プロキシが MN の移動状態を把握して，移動情報テーブルに位置情報を登録する。この処理で，モバイル IP 機能をもたない MN でも，移動状態が管理され，サブネット間のローミングを可能にしている。

図 5 において，MN1 が AP1 と接続するときには，MN1 と WLC 間で認証処理が行われる。このとき，表 2 に示したように，HA プロキシが，認証時のパケットの情報を基に，全 AP 分の移動情報テーブル中に MN1 に関する位置情報を登録する。登録された情報は，MN1 のホームネットワークの AP1 の HA に送信される。

図 5 中の AP1 に接続していた MN1 が，インターネットを経由して社外と通信中に APj に移動したときの MN1 に関連する通信の内容は，図 6 のようになる。

(i) MN1 は，移動後に APj への接続処理を行う。そのとき，MN1 と WLC 間で認証処理が行われる。
(ii) WLC の [a] は，移動情報テーブルの MN1 に関する位置情報を更新し，更新内容を MN1 のホームネットワークの AP1 の HA に送信する。
(iii) MN1 は APj と接続した後，インターネット経由の社外宛てパケットを APj に送信する。
(iv) AP j の [b] は，受信したパケットの送信元 IP アドレスと宛先 IP アドレスが，AP j のサブネットとは異なるサブネットのものなので，受信したパケットを L3SW に送信する。
(v) 社外から，インターネット経由で MN1 宛てに送信された応答パケットが，MN1 のホームネットワークに到達し，AP1 が受信する。
(vi) AP1 の [c] は，宛先の MN1 が移動中であることを，移動情報テーブルを参照して知り，受信したパケットをカプセル化して WLC に送信する。
(vii) WLC の [d] は，受信したパケットのカプセル化を解除し，宛先 IP アドレスから MN1 宛てであることを知る。このとき，移動情報テーブルを参照すると，MN1 は AP j のサブネットに移動中なので，再度パケットをカプセル化して APj に送信する。
(viii) APj の [e] は，受信したパケットのカプセル化を解除して，MN1 にパケットを送信する。
(以下，省略)

図 6　MN1 が APj に移動したときの MN1 に関連する通信の内容

J 君は，無線 LAN の導入方法の検討が完了したので，次に，サイトサーベイの検討を行った。

〔サイトサーベイの検討〕

J 君は，無線 LAN 導入に当たって留意すべき事項を調査し，その結果，サイトサーベイの実施について，次のように進めた。

本社は，テナントビルに入居し，隣接した複数のフロアを使用している。各フロア

のオフィスは，壁やパーティションなどで分割されている。本社のオフィスに複数のAP を導入するとき，サイトサーベイを実施しないと，（お）(a) 導入後に通信できないエリアが発生する，(b) 他社の無線 LAN の影響を受ける，(c) 期待どおりの通信速度が得られない，などの問題が発生する可能性が高い。この問題を防ぐためには，専用機材を用いて，AP から送出される電波の伝搬状態及び電波干渉の発生源を十分に把握しておくことが重要である。

AP から送出される電波の伝搬状態を把握していないと，AP の最適な場所への設置，適切な電波強度の設定ができない。電波状態の調査には専門的なノウハウが必要であることから，J 君は，サイトサーベイは，専門業者に委託するのがよいと判断し，調査・検討の結果を，S 主任に報告した。

S 主任と J 君は，これまでの検討を基に設計した無線 LAN 導入構成及びサイトサーベイの実施方法を，R 課長に報告した。説明を受けた R 課長は，設計内容及びサイトサーベイの実施方法に問題がないことを確認できたので，無線 LAN の導入を進めることにした。

設問 1　本文中の［　ア　］～［　カ　］に入れる適切な字句を答えよ。

設問 2　〔現状調査〕について，(1) ～ (5) に答えよ。

(1) 図 1 において，L3SW1 の P5 と L3SW1 の P6 の組，及び L3SW2 の P5 と L3SW2 の P6 の組以外に，リンクアグリゲーションが 2 組設定されている。その組を，それぞれ図 1 中の機器名，ポート ID で答えよ。

(2) 表 1 中の仮想ルータ VR1 がマスタルータとなるスイッチ名を，図 1 中の機器名で答えよ。

(3) L2SW2 と L3SW1 間の経路において，L2SW2 の P11 がブロッキングポートになる。その理由を，STP の経路計算アルゴリズムを基に，図 1 を参照して，40 字以内で述べよ。

(4) L3SW1，L3SW2，L2SW3 及び L2SW4 の間を接続する経路のブロッキングポートを，図 1 中の機器名とポート ID で答えよ。

(5) 図 1 中の PC1 と仮想サーバ 3 間のフレーム転送経路を，次の【転送経路】に示す。(A)，(B) に入れる適切な機器名を，【転送経路】の表記方法に従い，経由する順に列挙せよ。

【転送経路】

PC1 → [(A)] → L2SW3 及び L2SW4 → 仮想サーバ 3

仮想サーバ 3 → L2SW3 及び L2SW4 → [(B)] → PC1

設問 3　〔無線 LAN の調査と導入検討〕について，(1) ～ (3) に答えよ。

(1) 本文中の下線（あ）のセキュリティリスクの内容を，25 字以内で述べよ。

(2) 本文中の下線（い）によって，ローミング時間が短縮される。その理由を，図 2 の手順を参考にして，25 字以内で述べよ。

(3) 本文中の下線（う）が発生する理由を，MN1 に設定されているネットワーク情報が変更されないことに着目して，35 字以内で述べよ。

設問 4　〔サブネット間のローミングの調査と設計〕について，(1) ～ (4) に答えよ。

(1) 図 4 中の ① で，FA から送信される Advertisement メッセージには，IP ヘッダが付加される。この IP ヘッダの宛先 IP アドレスの種類を答えよ。

(2) 図 4 中の ② で，転送先テーブルを更新した後，HA は，サブネット内のホスト宛てに，ある通信を行う。その通信プロトコルの名称を答え，その目的を，40 字以内で述べよ。

(3) 図 4 中の下線（え）のために，MN 宛ての ARP 要求に対して HA が行う処理の内容を，20 字以内で述べよ。

(4) 図 6 中の [a] ～ [e] に入れる適切な字句を，表 2 中の機能の名称で答えよ。

設問 5　〔サイトサーベイの検討〕について，(1) ～ (3) に答えよ。

(1) 本文中の下線（お）の問題が発生するのを避けるために，サイトサーベイで調査すべき電波の状態を二つ挙げ，それぞれ 25 字以内で答えよ。

(2) サイトサーベイの調査結果を基に，導入作業前に確定すべき設計項目を二つ挙げ，それぞれ 15 字以内で答えよ。

(3) 無線 LAN を設置した後，ping コマンドによる接続確認テストの他に，MN を使用して実施すべきテストを二つ挙げ，それぞれ 25 字以内で答えよ。