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。

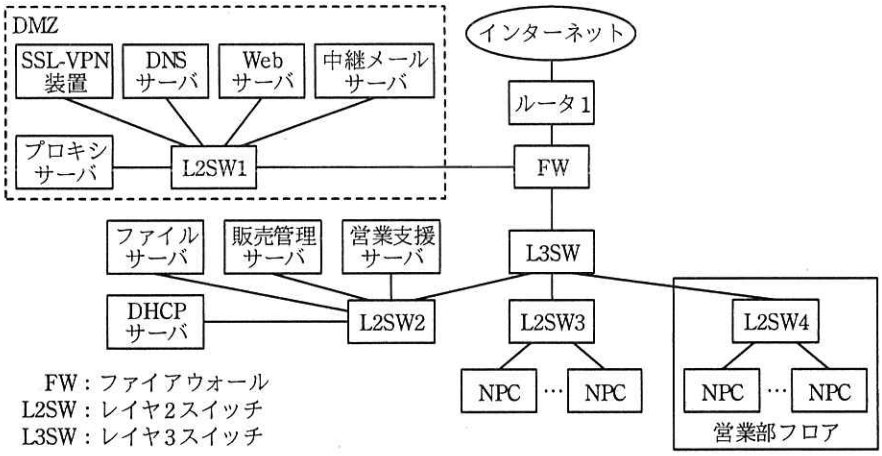


図 1　本社の現在の LAN 構成（抜粋）

〔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。

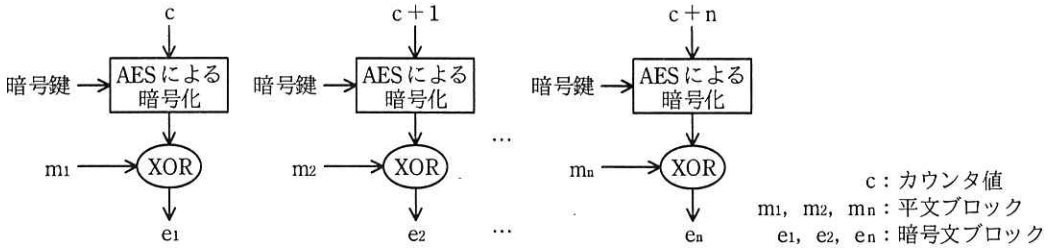
(2) WPAでは，TKIPによって暗号鍵を生成する。TKIPでは，暗号鍵の基になる一時鍵（Temporal Key）が動的に生成される。エンタープライズモードの場合，一時鍵は，IEEE 802.1Xの認証成功後に［　h　］で動的に生成されてクライアントに配布されるPMK（Pairwise Master Key）を基に，無線LAN端末及び

[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（160 MHz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（80 MHz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

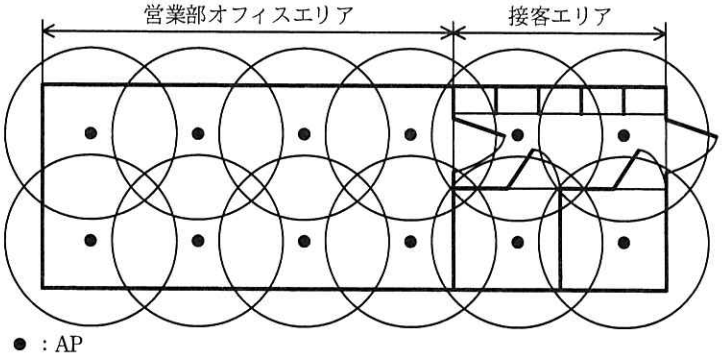
・AP の負荷分散制御，PMK の保持などによるハンドオーバ制御機能

・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。

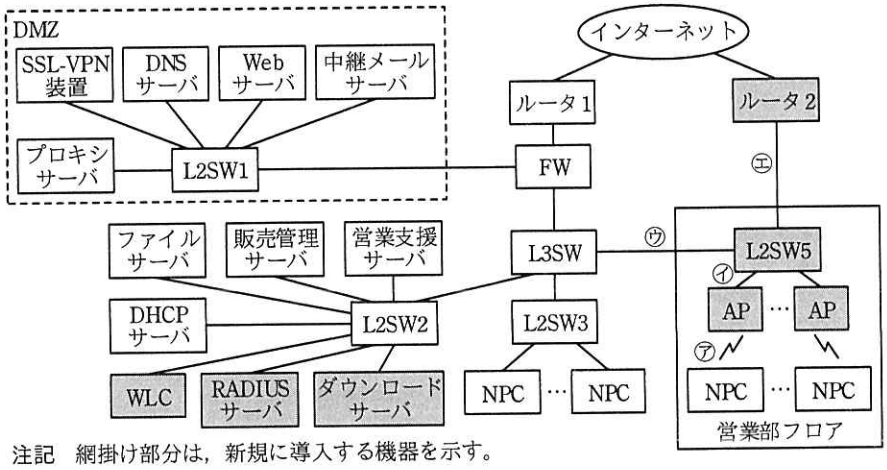
次に，J 君は，ダウンロードサーバの設置場所について検討した。

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