問1　無線 LAN システムの構築に関する次の記述を読んで，設問1～4に答えよ。

通信機器や通信サービスの販売会社である A 社は，分散していたオフィスを集約することになった。集約に当たっては，工事を極力少なくし，費用の削減や期間の短縮を図るために無線 LAN の活用を考えている。加えて，集約を契機に，座席はフリーアドレスとし，座席数は在席率を考慮して社員数より少なくし，代わりに不足気味のミーティングスポットを確保するなど，オフィススペースの有効活用と業務の効率向上を図りたいと考えている。

また，最近，来訪者から，“応接室，会議室及びロビー（以下，応接エリアという）で，無線 LAN を利用してインターネット経由で自社に接続したい”という要望が出ている。

現状，A 社内では VLAN を使用した部門ごとの LAN（以下，部門 LAN という）が用意されており，当該部門の業務サーバもそこに設置されている。社員は，各人に支給された PC を所属する部門 LAN に接続し，サーバを利用している。

〔要件の整理〕

システム部の B 主任と C 君は，集約後の無線 LAN システム構築の担当者に任命された。具体的な設計に当たり，B 主任は C 君に (1)～(5) の考慮すべき要件を示した。

(1) A 社内の PC は，無線 LAN を使用して社内のネットワーク（以下，社内ネットワークという）に接続する。

(2) 来訪者は，応接エリアから無線 LAN を経由してインターネット接続だけを利用できる。

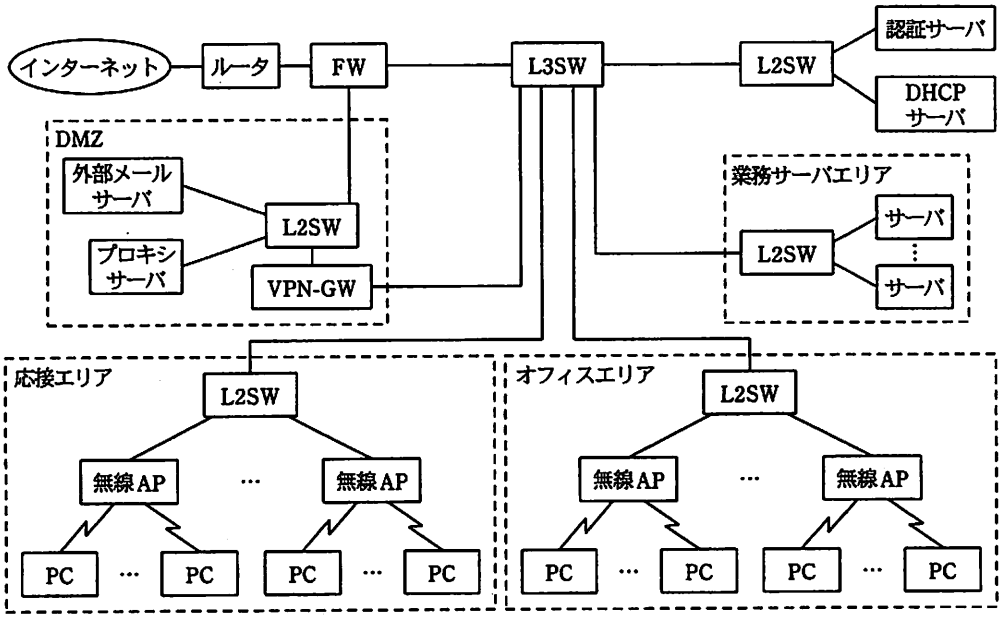
(3) 無線 LAN を利用して，社員がどのエリアから社内ネットワークに接続する場合でも，所属する部門 LAN に接続して，これまでと同様の使い方ができるポータビリティを実現する。

(4) 許可された利用者の PC だけが社内ネットワークに接続できる。

(5) 社員は，許可されたサーバだけを利用できる。

無線 LAN は有線 LAN と比べてセキュリティ面のリスクが高いので，要件 (1)～(4) の実現に当たっては，それに配慮した設計を行うことにする。

図1は，集約後の無線LANシステム構成図である。



FW：ファイアウォール　VPN-GW：VPNゲートウェイ　L2SW：レイヤ2スイッチ
L3SW：レイヤ3スイッチ　無線AP：無線LANアクセスポイント

注　業務サーバエリアには，メールや情報共有のための社内Webサーバなどの共用サーバや，各部門専用の業務サーバが設置されている。

図1　集約後の無線LANシステム構成図

C君は，システム検討に当たり，まず無線LANを使う上でのセキュリティ確保の方式について検討し，その後，必要となる認証基盤の構築，無線LAN規格の混在による影響とその対応，及び社員の利便性を高めるポータビリティの実現，の順に検討を進めることにした。

〔セキュリティ確保の方式〕

無線LANは，電波の届く範囲ならどこからでもアクセスできるので，暗号化や利用者の認証が重要になる。C君は，無線LANの使用に当たって，WEP（Wired Equivalent Privacy）方式では，認証方式，暗号方式及び鍵の秘匿性について脆弱性が問題になっていることから，セキュリティが強化されたIEEE 802.11i規格の採用を検討することにした。

IEEE 802.11iではセキュリティを高めるため，IEEE 802.1X認証方式を採用し，よ

り強固な暗号鍵の生成と配送方式を規定している。IEEE 802.1X 認証方式は，IETF（Internet Engineering Task Force）が規定した EAP（Extensible Authentication Protocol）という，認証や暗号鍵配送用のフレームワークを利用している。EAP-TLS（Transport Layer Security）方式では，電子証明書を使用した認証を行う。C 君は，セキュリティ重視の観点から EAP-TLS 方式を採用することにした。

図 2 は，C 君が調査した IEEE 802.11i に基づく EAP-TLS 方式の認証と鍵配送の概略シーケンスを示している。

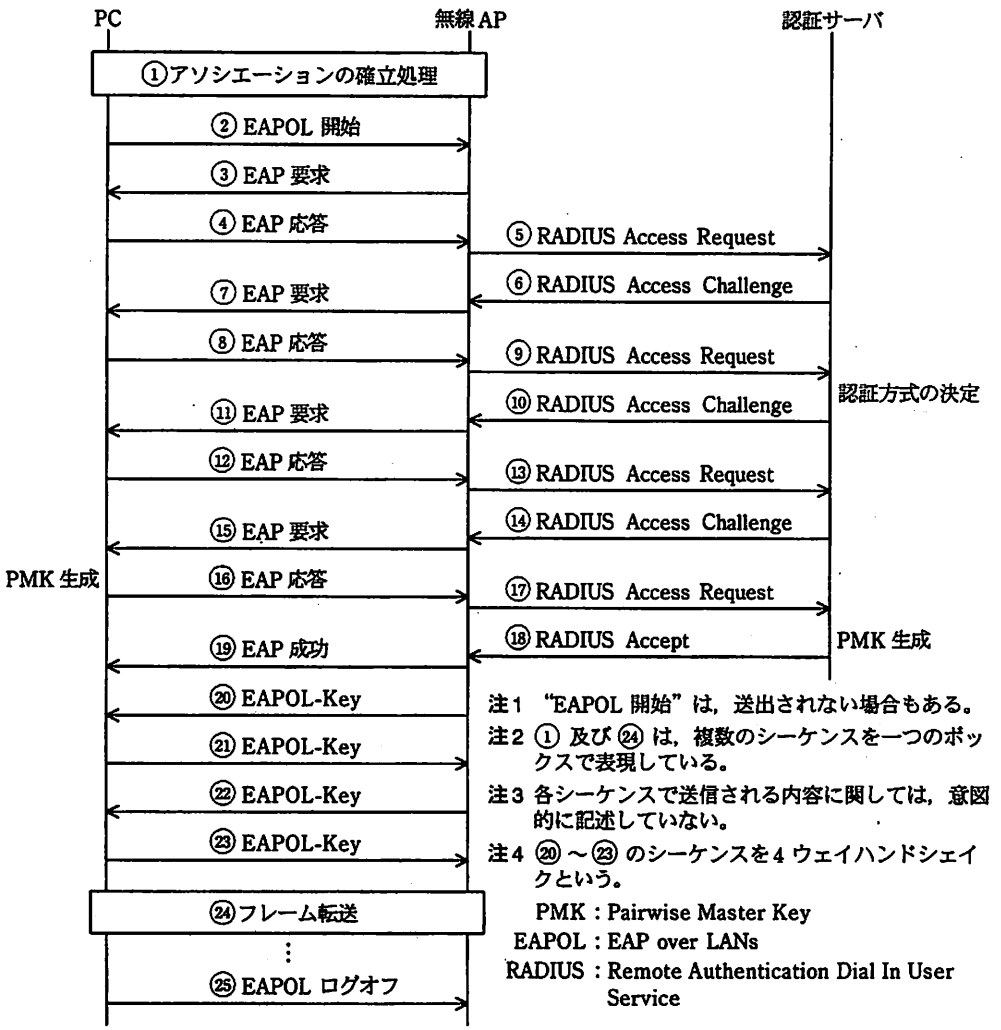


図 2　IEEE 802.11i に基づく EAP-TLS 方式の認証と鍵配送の概略シーケンス

EAP-TLS 方式において，PC と認証サーバ間でやり取りされる EAP パケットは，PC と無線 AP 間は EAPOL フレームのデータとして送られ，無線 AP と認証サーバ間は RADIUS パケットのデータとして送られる。

認証処理は，無線 AP から PC に EAP 要求を送信することから始まる。この応答として，PC は，利用者が入力した自分自身の識別情報を送信する。その後，PC と認証サーバとの間で認証方式の選択処理が行われる。認証方式（今回は EAP-TLS）が決定すると，PC と認証サーバ間で電子証明書が送受信され，相互の認証が行われる。単に，PC と認証サーバの電子証明書を相互に送受信しただけでは，相互認証はできないので，認証を可能にする追加の情報も送受信する。

EAP-TLS 方式では，暗号鍵作成のための機能強化も図られている。認証処理に加えて，暗号鍵を生成するための乱数などの情報が認証過程でやり取りされ，図 2 中の⑲のシーケンスが終了した時点で，256 ビットの PMK と呼ばれる暗号鍵が PC と認証サーバで共有される。PMK は，PC と無線 AP 間のデータを暗号化するために使われるので，認証サーバから無線 AP にも転送される。

実際のフレーム転送時に使われる 128 ビットの暗号鍵 TK（Temporal Key）は，4 ウェイハンドシェイクと呼ばれる手順で PC と無線 AP 間で送受信される情報と，PMK を基に生成される。これによって，TK は①WEP 方式の暗号鍵とは異なり，予測されにくい暗号鍵となっている。

IEEE 802.1X は，スイッチのポートベースのアクセス制御を実現する技術である。有線 LAN で使用する場合は，スイッチの物理ポート単位に通信を制御している。IEEE 802.1X を実装するスイッチの配下に HUB を接続するような場合には，認証されていない PC との通信が行われることを防止するため，有線 LAN では独自の実装が必要である。一方，無線 LAN では，PC と無線 AP との論理的接続である［　ア　］をポート接続と見なすようにポートの概念を拡張している。これによって，②有線 LAN で使用する場合と比べて，接続制御上の問題が少なくなる。

このように，EAP-TLS 方式を使うことで，要件の一つである，許可された利用者の PC だけが社内ネットワークに接続できることになった。

〔認証基盤の構築〕

EAP-TLS 方式の実現には［　イ　］と呼ばれる認証基盤の構築が必要であり，認証局の設置，電子証明書の発行と配布，及び社員の異動や有効期限切れに伴う電子証明書のメンテナンスが必要になる。C 君は，電子証明書の初期配布やその後のメンテナンスを容易に行えるように配慮して，認証基盤を構築することにした。

認証サーバとしては，認証局機能と RADIUS 機能の両方の機能を備えたアプライアンス型の認証サーバ製品を使い，プライベート認証局を設置することにした。

社員への電子証明書の配布については，個別対応の負担をできるだけ軽減する必要があるので，電子証明書のダウンロード用 Web サーバ（以下，配布サーバという）を用意し，そこからダウンロードさせることを検討した。配布サーバには，必要なファイルを認証サーバからコピーして格納しておく。配布サーバの設置に関しては，社員の社内ネットワーク接続方法に関係するので，C 君は，ポータビリティの実現と併せて検討することにした。

C 君が考えた電子証明書の運用手順の概略は，次のとおりである。

(1) 社員には利用申請書を提出してもらう。ただし，今回の集約に伴う移転に関しては，システム部が対象者の情報を人事部から入手し，一括処理するので，提出は不要とする。

(2) 社員には，配布サーバの URL と，ダウンロード専用の社員ごとのパスワードをメールや郵便で通知する。

(3) 社員は，移転先で初めて社内ネットワークに接続するとき，配布サーバに接続し，各自のクライアント証明書，クライアントの［　ウ　］及び認証局証明書（以下，証明書類という）をダウンロードして PC にセットする。

証明書類の継続更新処理は，電子証明書の有効期限内であれば，有効期限の 1 か月前から，申請手続なく社員各自が，配布サーバから更新済の証明書をダウンロードできるようにする。有効期限内に更新処理を行わなかった場合は，利用申請書を再度提出する(1) ～ (3)の運用手順が必要になる。

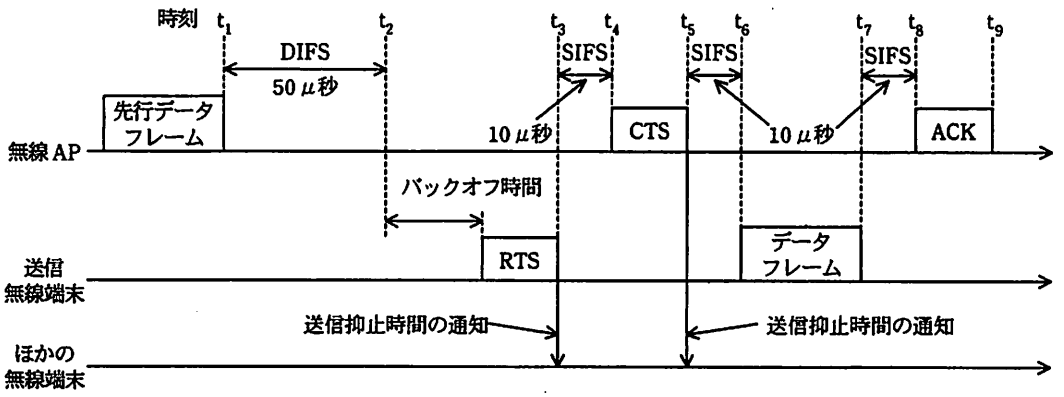
電子証明書の有効期限内であっても，異動などに伴い，社内ネットワークに接続できないようにする必要が生じた場合は，［　エ　］を作成して電子証明書を無効にする。

C 君が，(1)～(3)の運用手順及び証明書類の継続更新処理手順の案を B 主任に報告したところ，③“PC に証明書類をセットするだけでは，ユーザ認証という観点では問題がある”という指摘を受けた。そこで C 君は，対策として PC の運用方法を改善することにした。更に調べてみると，証明書類をより安全に管理するための USB 接続のデバイス（以下，トークンという）があることが分かった。トークンは，証明書類を格納するが，USB メモリとは異なり，パスワードによる不正利用防止機能及びトークン内での暗号処理機能を実現している。A 社では，社外に持ち出す PC をシンクライアント化し，トークンを利用することにした。

〔無線 LAN 規格の混在による影響とその対応〕

A 社で使用している PC は，ほとんどノート型である。デスクトップ型の PC については集約時に，最新型のノート PC に入れ替える予定である。ノート PC が対応する無線 LAN 規格には IEEE 802.11a，IEEE 802.11b 及び IEEE 802.11g と複数種あり，中には IEEE 802.11b にだけ対応する PC もあった。特に同一周波数帯域を使用する IEEE 802.11b と IEEE 802.11g の場合には，混在による影響が懸念された。そこで C 君は，その影響について調べてみた。

無線 LAN では，イーサネットと異なる［　オ　］方式と呼ばれるアクセス方式が使われている。通信を開始する無線端末が，ほかの端末が電波を出していないかを，事前に確認する方式である。しかし，電波の伝搬にかかわる無線端末の位置関係，障害物の影響などの空間的な原因や無線 LAN 規格の混在が原因で，事前の確認ができない場合もある。これを回避する方法として考えられたのが，RTS（Request To Send）及び CTS（Clear To Send）という制御フレームを利用する方式（以下，RTS/CTS 方式という）である。この RTS/CTS 方式を使用した衝突回避の通信シーケンス例を図 3 に示す。



DIFS : Distributed Inter Frame Space　　SIFS : Short Inter Frame Space　　ACK : ACKnowledgement

注1　制御フレームのMAC フレーム長は，RTS が20 バイト，CTS が14 バイト，ACK が14 バイトである。

注2　DIFS 及びSIFS の値は，IEEE 802.11b とIEEE 802.11g が混在している場合の例である。

図3　RTS/CTS 方式を使用した衝突回避の通信シーケンス例

図 3 は，送信無線端末が無線 AP に向けてデータを送る場合の例を示している。データ送信に先立ち，送信無線端末が RTS を送信し，RTS を受信した無線 AP が CTS を送信する。RTS 及び CTS には送信抑止時間が含まれており，これらの制御フレームを受信したほかの無線端末は，指定された時間の送信を抑止し，アクセスの衝突を回避する。

RTS/CTS 方式では，RTS 及び CTS の 2 個のフレームを送信するので利用効率が低下する。そこで，送信無線端末が RTS の代わりに，CTS を送信する方式（以下，自己 CTS 方式という）も考えられている。

C 君は，RTS や CTS のような衝突回避に使われる制御フレームの送信に必要な時間を試算してみた。これらは無線 AP に接続する無線端末が認識できるように，互換性のあるフレーム形式で送信される必要がある。そのために，MAC フレームの先頭に付加されるプリアンブル部 144 ビットと物理ヘッダ部 48 ビットは，固定の 1M ビット／秒で送られる。MAC フレーム部は，IEEE 802.11b と IEEE 802.11g が混在した場合，11 M ビット／秒で送られる。したがって，14 バイトの CTS フレームの送信には，合計 [a] μ秒の時間がかかる。一方，データフレームについては，1,500 バイトのフレームを 54 M ビット／秒で送る場合，約 230μ秒かかることから，制御フレームのオーバヘッドは非常に大きいことが分かる。

C 君は，混在による性能低下が大きいので，共存時に性能低下が大きい IEEE

802.11b の利用をやめ，IEEE 802.11b だけに対応する PC の利用者には，IEEE 802.11g 対応の無線 LAN カードを支給することにした。IEEE 802.11g より高速の伝送が可能な新規格である IEEE [カ] 規格の標準化が進んでいることから，支給する無線 LAN カードには，将来制御用ソフトウェアの更新によって，新規格にも対応可能な無線 LAN カードを選定した。

このように，A 社では，使用する無線 LAN 規格を IEEE 802.11a と IEEE 802.11g に統合し，さらに，将来の無線 LAN 高速化への対応を図った。

〔ポータビリティの実現〕

応接エリアでは，社員だけでなく来訪者も無線 LAN を使用することになるので，社員か来訪者かによって接続先を切り替える制御が必要になる。C 君は社員用の ESS-ID とは別に，来訪者用の ESS-ID を設定することにした。応接エリアの無線 AP に接続された来訪者の PC からのトラフィックは，インターネット接続用のルータに転送する。無線 LAN を利用したい来訪者には，接続のための設定情報が書かれたカードを受付で渡し，持ち込んだ PC にその情報を設定してもらうことにした。

部門 LAN を経由したサーバの利用では，ポータビリティを実現するためには，どの無線 AP に接続しても，社員の所属部門を認識し，所属部門の部門 LAN に接続できる仕組みが必要である。その際に，PC 側の操作が必要だと，使い勝手が悪いので，PC 側の操作を不要にしたい。

C 君は，PC を無線 LAN に接続したときに，社員の所属を区別する VLAN ID を付与できればよいと考えた。VLAN ID 付与の方式として，無線 AP への設定を工夫する方式と，IEEE 802.1X 認証の仕組みを活用する方式の二つを考え，B 主任に相談した。

B 主任からは，“無線 LAN のアクセス認証に EAP-TLS を使用しているのだから，それを生かした方式の方がよいのではないか”というアドバイスを受けた。

また，C 君は，④認証基盤の構築で用意した配布サーバへの最初のアクセス制御にも IEEE 802.1X 認証の仕組みを利用することを考えたが，これについても B 主任から“セキュリティに関して大丈夫か”との指摘を受けた。C 君は，当初考えていた配布サーバへのユーザ ID とパスワードによるアクセス保護に加え，不正にダウンロードされにくい対策をとることにして，B 主任の了承を得た。

IEEE 802.1X 認証の仕組みを活用する方式では，⑤社員の所属部門が変わった場合

の運用が容易なこともあり，C 君は，この方式で進めることにした。

このようにして，C 君は A 社の無線 LAN システムの設計を終え，集約先オフィスへのシステム導入の準備を開始した。

設問 1　〔セキュリティ確保の方式〕について，(1)～(4)に答えよ。

(1) PC がクライアント証明書を送出するシーケンスはどれか。図 2 中のシーケンス番号で答えよ。また，このときに，電子証明書とともに送る認証用データは何か。10 字以内で答えよ。

(2) 本文中の下線①に関して，どのような手段によって，WEP 方式に比べて暗号鍵の予測を困難にしているのか。40 字以内で述べよ。

(3) 本文中の［　ア　］に入れる適切な字句を答えよ。

(4) 本文中の下線②に関して，有線 LAN で使用する場合と比べて，接続制御上の問題が少ない理由を 30 字以内で述べよ。

設問 2　〔認証基盤の構築〕について，(1)～(4)に答えよ。

(1) 本文中の［　イ　］～［　エ　］に入れる適切な字句を答えよ。

(2) 本文中の下線③に関して，B 主任が指摘した問題点を 40 字以内で述べよ。

(3) B 主任が指摘した問題点への対策として，C 君が考えた PC の運用方法の具体的な改善案を 25 字以内で述べよ。

(4) トークン内で暗号処理を行うことで，セキュリティ管理上得られる利点を 30 字以内で述べよ。

設問 3　〔無線 LAN 規格の混在による影響とその対応〕について，(1)～(5)に答えよ。

(1) 本文中の［　オ　］，［　カ　］に入れる適切な字句を答えよ。

(2) 自己 CTS 方式の場合，RTS/CTS 方式と比べて衝突を回避できない場合は，どのような場合か。25 字以内で述べよ。

(3) 図 3 中の制御フレームのうち，同一の無線 AP に接続するすべての無線端末で受信される必要のあるフレームはどれか。図 3 中の字句で答えよ。

(4) 図 3 において，ACK を送信しなければならない理由を，無線 LAN の技術的特性に触れて，50 字以内で述べよ。

(5) 本文中の［　a　］に入れる数値を求めよ。答えは，小数点以下を切り上げて整数で求めよ。

設問4　〔ポータビリティの実現〕について，(1)～(5)に答えよ。

(1) IEEE 802.1X 認証を用いた場合，VLAN ID が有効になる契機は，図2中のどのシーケンスによるものか。図2中のシーケンス番号で答えよ。

(2) C 君が採用した IEEE 802.1X 認証の仕組みを活用する案は，どのようなやり方と考えられるか。55字以内で具体的に述べよ。

(3) 本文中の下線④に関して，配布サーバへのアクセスの制御をどのように実現しようとしたのか。40字以内で述べよ。

(4) 配布サーバ上に格納したクライアントの証明書類の管理について，C 君が採用した不正にダウンロードされにくい対策とはどのような方法と考えられるか。40字以内で述べよ。

(5) 本文中の下線⑤に関して，無線 AP への設定を工夫する方式と比べた場合の運用上の利点を45字以内で述べよ。