NW

平成21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. この注意事項は，問題冊子の**裏表紙**に続きます。必ず読んでください。
4. **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。**
5. 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

6. 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，採点されません。
   (3) **生年月日欄**に，受験票に印字されているとおりの**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。
   (4) **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。
   なお，○印がない場合は，採点の対象になりません。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。
   (5) 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。
   (6) 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。

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。

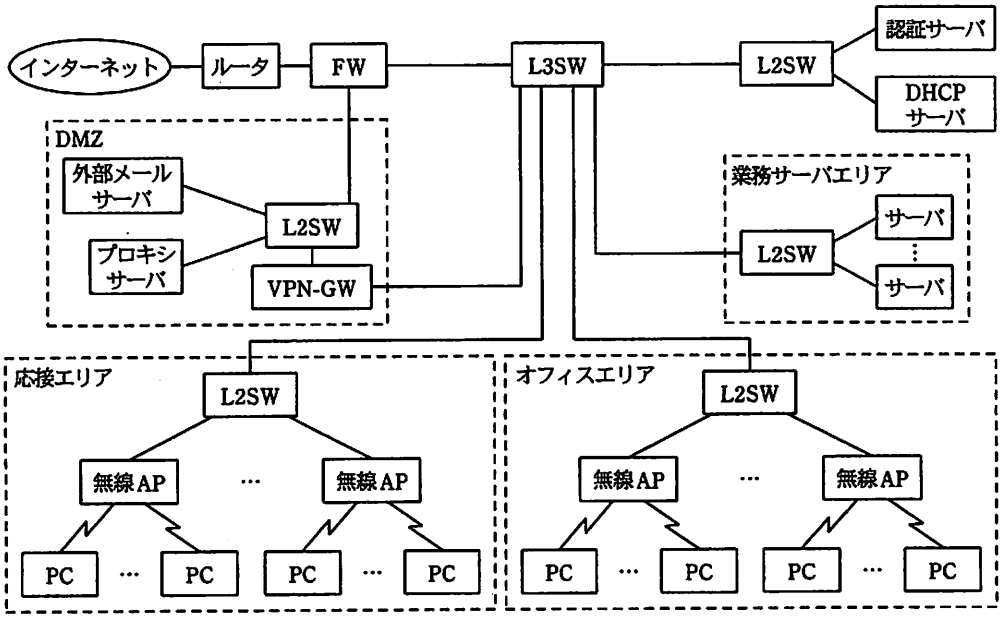
(3) 無線 LAN を利用して，社員がどのエリアから社内ネットワークに接続する場合でも，所属する部門 LAN に接続して，これまでと同様の使い方ができるポータビリティを実現する。

(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。

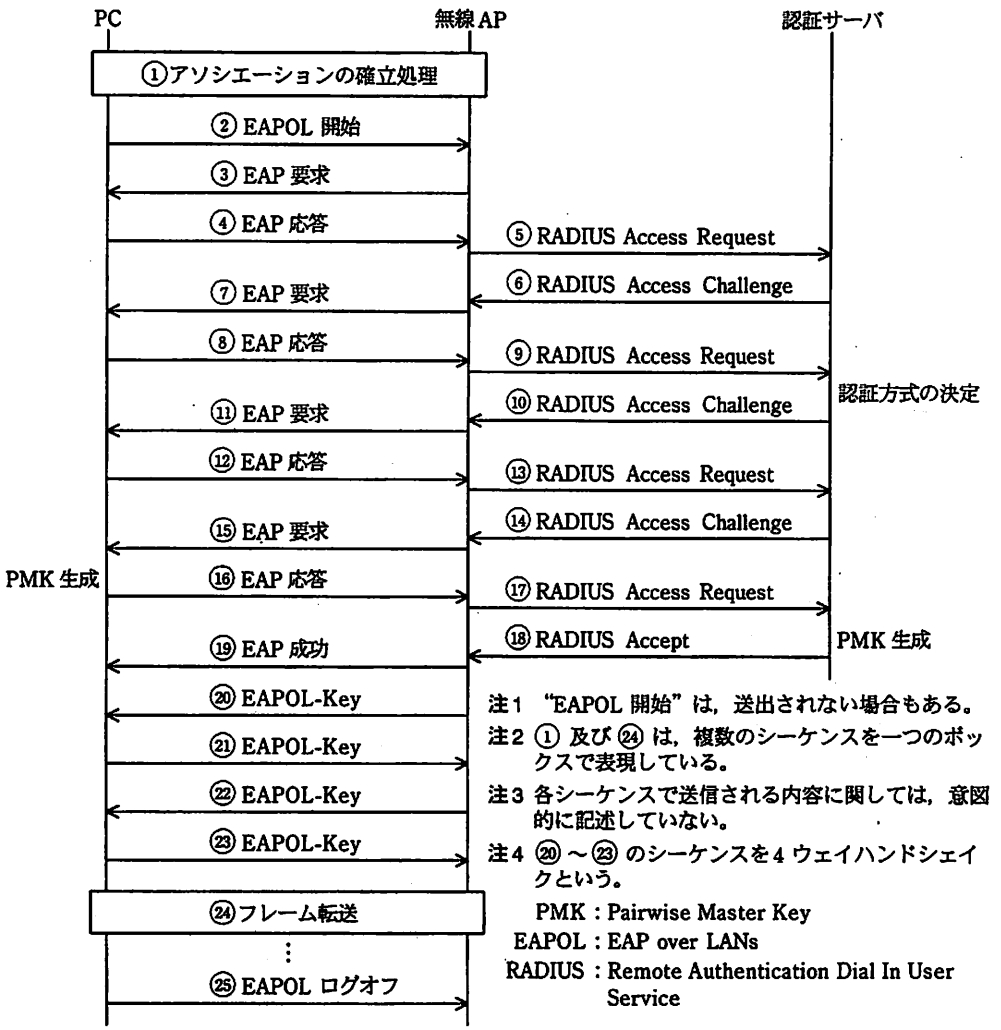


図 2　IEEE 802.11i に基づく EAP-TLS 方式の認証と鍵配送の概略シーケンス

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。

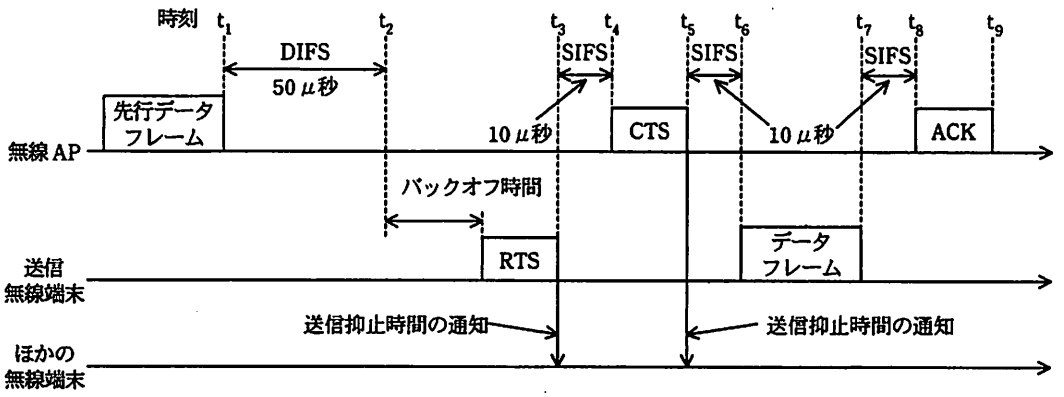
電子証明書の有効期限内であっても，異動などに伴い，社内ネットワークに接続できないようにする必要が生じた場合は，［　エ　］を作成して電子証明書を無効にする。

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。

問2　サーバの移設に関する次の記述を読んで，設問1～5に答えよ。

D社は，東京に本社がある精密機械製造会社であり，全国10か所に支店と工場（以下，拠点という）がある。D社では，本社にあるサーバ室に設置されている約200台のサーバに，本社及び拠点のクライアントからTCP/IPで接続し，一部ではサーバ同士も接続する形態をとっている。サーバ室には，レイヤ3スイッチ（以下，L3SWという）と，サーバを接続するレイヤ2スイッチ（以下，L2SWという）が設置されている。D社ネットワークシステムの概要を図1に示す。

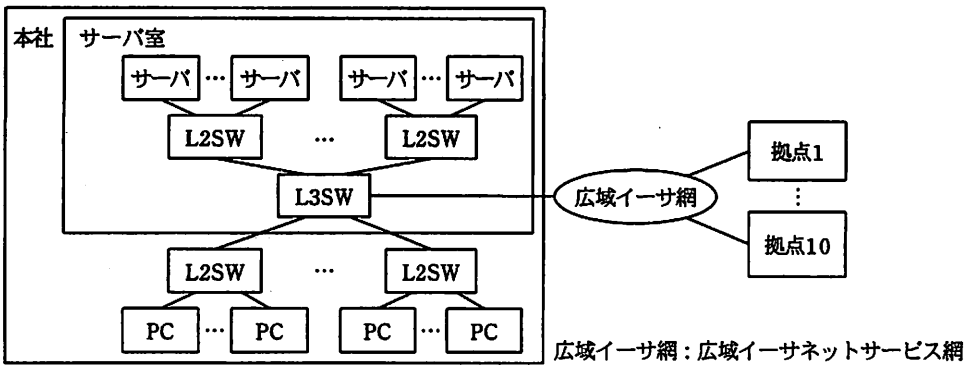


図1　D社ネットワークシステムの概要

このたびD社では，BCM（Business Continuity Management）の一環として，データセンタ事業者であるE社のデータセンタ（以下，DCという）に，サーバを移設することになった。予算の都合と早急な対策が必要であることから，情報システム部のF部長に対し，“年度内に移設作業を終了させるように”という指示があった。そこでF部長は，部内からメンバを集め，プロジェクトチームを発足させた。

〔システムの管理状況と移設方針〕

社内のシステムは，全体で50ほどあり，情報システム部以外の部署が管理するものが多く，構築したSI業者もまちまちだった。そこで，プロジェクトのメンバは，各システムの担当者（以下，S担という）から現状をヒアリングした。その結果，構成情報などの文書が導入時のままで，その後の変更が反映されていないことが分かった。現状を把握するのに時間がかかったが，概要がほぼ分かったところで，F部長は，

1 日ですべてのシステムを移設することは困難であると判断し，24 ビットでマスクされたサブネットを基にグルーピングし，数回に分けて実施することにした。F 部長は，次に示すネットワークの移行方針を立てた。

・サーバの IP アドレスの変更は，原則として行わない。
・DC に L3SW を 2 台導入し，冗長化構成とする。
・第 1 回の移設作業日より前に，DC を広域イーサ網の 1 拠点として追加し，ネットワークの疎通確認と L3SW の動作確認を行う。
・サーバを接続する L2SW は，原則として，使用中の機器を移設して使用する。
・ネットワークの変更は，サーバを取り外した後，該当するサブネットを本社側 L3SW から削除し，DC 側 L3SW に追加する手順とする。

〔システムの運用状況〕

サーバ室では，情報システム部に所属するオペレータ（以下，OP という）が，システム操作のほか，バックアップの取得や，監視サーバを用いた監視などの業務を行っている。監視サーバでは，サーバの稼働監視やジョブ監視などを行っており，障害を検知したときは，画面に障害状況を表示するとともに，該当する S 担に電子メールを送信する。OP の勤務体制は，平日 8 時から 22 時までの 2 交代なので，勤務時間外となる深夜，早朝及び休日は無人運転となる。無人運転中でも，監視サーバが障害を検知したときは S 担に電子メールが送信されるが，障害への対応は，OP や S 担の出社後になってしまう。その影響で業務の開始が遅れてしまうことがあり，利用部門から運用体制の改善を求められている。

WAN の障害検知については，通信事業者の監視サービスを利用している。通信事業者の監視センタからの連絡は，情報システム部のネットワーク担当者（以下，NW 担という）が受けており，NW 担と OP，S 担との連携がうまくいかないこともあった。

OP が検知した障害は，OP 自身がマニュアルに則して復旧作業を行っているが，マニュアルと実際の構成が異なっていることもあり，結果として S 担や NW 担が対応することが多い。

なお，それぞれの担当者では解決できない場合は，ネットワーク部分については NW 担が通信事業者又は保守業者に，それ以外は S 担が SI 業者に連絡して，対応してもらっている。

〔システムの運用委託方針〕

構成管理の不備と障害時の連携の不備については，D 社内でも以前から問題とされていた。そこで，DC を利用する目的の一つには，単なるサーバ設置だけでなく，これらの問題を解決するための運用委託も見据えていた。しかし，期間が限られていたので，移設作業を優先し，当面は，サーバ設置に伴う最低限必要な運用だけを E 社に委託することになった。その委託内容は次のとおりである。

・バックアップの取得とバックアップ媒体の管理
・サーバなどの LED の目視確認
・本社の監視サーバからの電子メール受信
・異常状態を検知したときの S 担への電話連絡

E 社は，今後の運用範囲の拡大にも対応できるように，監視オペレータのほかに D 社担当の運用 SE を選任し，E 社内部の情報を一元的にとりまとめる役割をもたせることにした。そして，移設作業完了後は，ITIL をベースに開発された［　ア　］マネジメントシステムの国際規格である ISO/IEC 20000 を適用して，課題を改善しながら，E 社へ委託する運用範囲を順次拡大していくことも合意された。

また，S 担が引き続き本社でサーバを操作できるように，リモート KVM スイッチを導入することも決定した。リモート KVM スイッチとは，IP ネットワークなどを介して遠隔地にある複数台のサーバを，一組のキーボード，［　イ　］及びマウスで操作するものである。

D 社が導入することにしたリモート KVM スイッチは，Web ブラウザの URL 入力域に，http://［　a　］/ を指定してログインし，対象のサーバを画面上で選択し，操作するものである。

〔サーバの移設計画〕

ネットワークの移行方針とシステムの運用委託方針が決まったので，移設作業手順書の作成に取り掛かることになった。作成に当たっては，移設前と移設後の構成を把握することが重要である。移設後の構成については，現状の構成を整理しながら，物理的にどのように配置するかを決めていく。機器の配置が決まれば，ラックや電源，リモート KVM スイッチなどの数と構成，及び当日の作業手順も決定する。移設後の構成が出来上がった段階で，運用マニュアルにも反映させることにした。

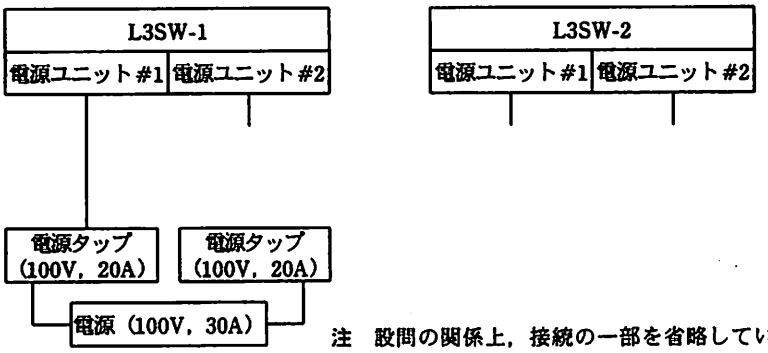
機器の配置設計では，複数のラックに散らばっているサーバを，システム単位にまとめることを優先したが，必要となる電源容量も考慮しなければならない。ラックに供給される電源は，定められた範囲内で正しく利用しないと，電源容量の超過で［ ウ ］が落ちて，システムが停止してしまうことになる。

最初に，事前に導入する L3SW の配置を検討した。L3SW を 2 台導入して冗長化構成とし，さらに L3SW の電源ユニットも冗長化することにした。この L3SW の電源ユニットは，負荷分散が可能であり，保守性を高める［ エ ］対応のものを 2 台組み込むと，片方が故障した場合には，システムの電源を落とさずに交換することができる。表 1 に L3SW の電源仕様を示す。

表 1　L3SW の電源仕様（抜粋）

項目	仕様
入力電圧	AC100～120V　/　AC200～240V
最大入力電流	12A（100V のとき）/［ b ］A（200V のとき）
最大消費電力	1,080W（100V，200V とも）

E 社が提供するラックには，標準として，交流 100 V で 30 A の電源が用意されている。その電源には，20 A まで使用可能な電源タップが二つ接続される。したがって，L3SW の電源ユニットの冗長化を生かすには，電源ケーブルの接続の仕方を考慮しなければならないので，図 2 に示す接続構成をとることにした。このようにして，L3SW の配置設計を終えた後，そのほかのサーバや L2SW などの配置設計を行った。



注　設問の関係上，接続の一部を省略している。

図 2　冗長化構成時の電源ケーブル接続構成

第 1 回の移設作業では，8 システムが対象となった。その中には，この移設プロジェクトの発足前に更改することが決定していたシステムがあったので，更改作業を移設作業と同時に行うことになった。そこで，新規サーバ（以下，サーバαという）を，移設日より前に DC に設置し，システムの構築を行うことにした。テスト実施時には，現行サーバとは別の IP アドレスを使用して，新規導入する L3SW に接続する。テスト終了後，ほかのシステムを移設する時点で，サーバαの IP アドレスを現行サーバの IP アドレスに変更するようにした。

以上を基に，F 部長は，作業内容をまとめて，移設作業当日のタイムチャート（図3）と移設作業手順書を作成した。移設作業は，複数のシステムを並行して実施するので，タイムチャート上にチェックポイント（設問の関係上，省略している）を設定した。これは，主要関係者が集まり，そこまでの状況確認をした上で，次工程に進むか否かを判断するポイントである。

項番・作業項目	場所	担当	金曜日	土曜日	日曜日
① 業務停止	本社	S担			
② c	本社	S担			
③ 電源オフ，取外し	本社	S担			
④ 梱包，搬出	本社	E社			
⑤ 移送	－	E社			
⑥ 搬入，開梱	DC	E社			
⑦ 取付け，電源オン	DC	S担			
⑧ ネットワークの移行	DC/本社	NW担			
⑨ d	DC	SI業者			
⑩ サーバ動作確認	DC	S担			
⑪ 業務確認	DC/本社	S担ほか			

注 ■■■ は，ほかの作業項目と異なり，この時間内に作業を完了させればよいことを示す。

図3　移設作業当日のタイムチャート

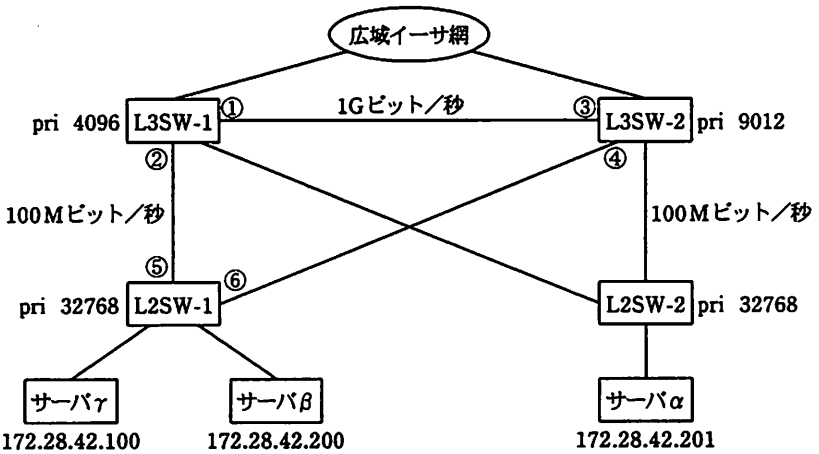
移設作業手順書には，作業中に発生し得るリスクを想定し，その回避策や軽減策，リスクが顕在化した場合にとるべき行動をまとめた［　オ　］プランも含まれる。

移設作業手順書の完成後，机上で検証し，できる範囲内で［　カ　］を行った。その目的は，作業手順だけでなく，［　キ　］や移設体制の確認，発生したトラブル

などの回避策を整理することなどがある。この結果を受けて，手順書やタイムチャートの修正，移設体制の見直しなどを行い，移設作業開始の当日を迎えることになった。

〔障害事例 1〕

第 1 回の移設作業は，図 3 中の項番⑩まで問題なく終了し，監視サーバがすべてのサーバを監視できることも確認した。しかし，日曜日に項番⑪を行ったところ，図 4 に示すサーバ接続構成において，特定のサーバからサーバαへの接続が失敗するという障害が発生した。この構成は，VRRP と STP による冗長化をとっており，図 4 中の LAN 構成は，障害に関係する一つの VLAN だけを図示している。



pri：ブリッジプライオリティ
注1 ①～⑥は，ポートの識別用の番号を示す。
注2 サーバの下の数字は，IPアドレスを示す。

図 4　サーバ接続構成（抜粋）

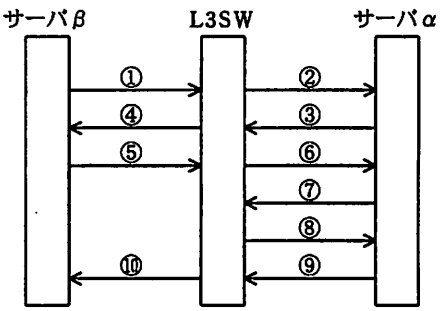
F 部長は，該当の S 担と，当日の立会いを行っていた，サーバαのシステムを構築した SI 業者を交えて，その障害状況を次のように整理した。

・本社サーバ室にあるサーバからサーバαへの ping は，成功する。
・DC 内のサーバβからサーバαへの ping は，成功する。
・DC 内のサーバγからサーバαへの ping は，失敗する。

SI 業者は，サーバαに原因があると推定し，更に情報を収集するためにトラフィックモニタを利用して調査しようと考えた。しかし，サーバαを接続する L2SW-2 には，

［　ク　］機能がなかったので，サーバのソフトを利用して調査した。サーバβ及びサーバγで，サーバαに対する ping コマンドを投入し，三つのサーバで情報を採取した。サーバβでコマンド投入したときの情報を基に作成したメッセージフローを，図5に示す。

なお，この図はL2SWが省略されており，サーバαにARPキャッシュが存在しない状態のものである。



項番	フレームの種類	あて先MACアドレス	送信元MACアドレス
①	ARP要求	ブロードキャスト	サーバβ
②	ARP要求	ブロードキャスト	サーバβ
③	ARP応答	サーバβ	サーバα
④	（設問の関係上，省略している。）		
⑤	ICMP echo要求	サーバα	サーバβ
⑥	（設問の関係上，省略している。）		
⑦	（設問の関係上，省略している。）		
⑧	（設問の関係上，省略している。）		
⑨	（設問の関係上，省略している。）		
⑩	ICMP echo応答	サーバβ	L3SW

図5　メッセージフロー

解析の結果，サーバαが保持する経路情報に誤りがあることが分かった。障害発生時の経路情報を，表2に示す。

表2　経路情報

あて先ネットワーク	ネットマスク	ゲートウェイ	インタフェース
0.0.0.0	0.0.0.0	172.28.42.254	172.28.42.201
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1
172.28.42.0	255.255.255.128	172.28.42.126	172.28.42.201
172.28.42.0	255.255.255.0	172.28.42.201	172.28.42.201
172.28.42.128	255.255.255.128	172.28.42.254	172.28.42.201
172.28.42.201	255.255.255.255	127.0.0.1	127.0.0.1
172.28.42.255	255.255.255.255	172.28.42.201	172.28.42.201
224.0.0.0	240.0.0.0	172.28.42.201	172.28.42.201
255.255.255.255	255.255.255.255	172.28.42.201	172.28.42.201

原因を追究した結果，何らかの理由で現行サーバに追加されていた不要ファイルが，サーバαにコピーされていたことが判明した。システムを更改したことで，この不要ファイルが使用されてしまうという事象が発生してしまったらしい。更に詳しく調査してみると，変更作業中に，SI 業者の担当者が新旧のサーバを比較したところ，このファイルがサーバαになかったので，独断でコピーしていたことが分かった。その後，SI 業者が該当ファイルを削除し，サーバαを再起動して，問題がないことが確認できたので，移設作業は完了となった。F 部長は，今回発生した障害の原因を分析し，その対策を次回以降の作業に反映させることにした。

〔障害事例2〕

E 社による暫定運用が始まってからしばらくすると，本社及び拠点から，DC の一部のサーバに接続できなくなり，最終的にはすべてのサーバに接続できなくなるという障害が発生した。この障害対応では，検知から復旧までに時間がかかってしまった。その経緯を，表3に示す。

表3　障害対応の経緯

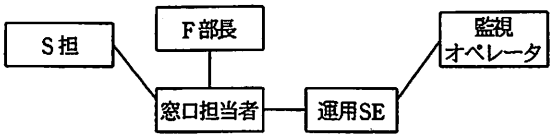
時刻	対応
1:26	監視サーバからの電子メールを，E 社監視オペレータが受信
1:30	E 社監視オペレータが，該当の S 担への連絡を開始
1:34	S 担から E 社監視オペレータに，該当サーバの状況確認を指示
1:40	E 社監視オペレータから S 担へ，確認した状況を報告 S 担は，サーバに問題がないと判断し，出社後対応するので対応不要の旨を E 社監視オペレータに伝達
7:48	OP が，監視システムで検知している状況（DC の全サーバダウン）を NW 担へ連絡
8:25	NW 担が出社し，L3SW の保守業者及び通信事業者に状況確認したところ，問題なしとの報告あり
9:24	NW 担から E 社運用 SE に，E 社側設置機器の状況確認を依頼
9:35	E 社運用 SE が関係者を招集し，D 社と E 社間で対応策の協議を開始
10:02	E 社運用 SE の提案で，L2SW，L3SW のログ取得を決定
11:45	事象を特定し，E 社運用 SE から E 社監視オペレータへ障害復旧処置を指示
12:07	復旧を確認し，対策会議を終了したが，NW 担による調査は継続

E 社の監視オペレータは，用意された手順書どおりに対応しており，問題はなかった。しかし，サーバに問題がないと判断してからの D 社の動きが従来と変わっていなかった。D 社の社員が出社し，調査が始まったものの，関係者間での情報共有が遅れ，原因特定までに時間がかかってしまった。

最終的には，NW 担からの連絡で，保守業者が調査した結果，図 4 のサーバ接続構成において，最初に接続できなくなったサーバが接続されている L2SW-1 にポート障害が発生したことが原因であることが判明した。ポート障害によって，L2SW-1 の CPU 負荷が高くなり，BPDU（Bridge Protocol Data Unit）を処理できなくなったのである。L2SW-1 に接続されているサーバの業務調整を行い，保守業者が L2SW を交換して，この障害は解決した。

〔連絡体制の整備〕

今回の障害対応によって，連絡体制の不備が明らかになった。そこで，E 社は，関係する事業者を含めた連絡体制の整備を，F 部長に提案した。E 社が提案した障害時連絡体制を，図 6 に示す。ポイントは，それぞれの会社内での一元管理である。



注1　設問の関係上，一部を省略している。
注2　S担は，システムごとに存在する。

図6　E社が提案した障害時連絡体制

F部長は，運用SEの役割に，E社設置機器の保守業者と通信事業者への対応も含めるよう要望した。その結果，F部長の要望を反映させた連絡体制が完成した。F部長は，今回新設される窓口担当者に，情報システム部のメンバを選任した。窓口担当者の役割は，D社内部の情報を一元管理することである。

D社側連絡体制の整備を待って，新体制での運用が始まった。その後，移設作業は大きな問題もなく完了し，両社は運用改善に向け，新たなプロジェクトチームを作り，検討を開始した。

設問1　本文中の［　ア　］～［　ク　］に入れる適切な字句を答えよ。

設問2　〔システムの運用委託方針〕及び〔サーバの移設計画〕について，(1)～(6)に答えよ。

(1) リモートKVMスイッチを利用して図4中のサーバβの操作を行うときに，本文中の［　a　］に何を指定すればよいか。25字以内で答えよ。

(2) 表1において，100Vと200Vの電源効率が同じであると仮定したとき，［　b　］に入れる数値を答えよ。

(3) 図2の電源ケーブル接続構成について，別系統の電源と電源タップを追加し，解答欄の図を完成させよ。

(4) 図3中の［　c　］，［　d　］に入れる作業項目を，それぞれ15字以内で答えよ。

(5) 図3中の項番⑧の“ネットワークの移行”とは，具体的にどのような作業をいうか。40字以内で述べよ。

(6) 図3に設定するチェックポイントのうち，項番⑧及び項番⑩の後にチェックポイントが必要な理由を，それぞれ40字以内で述べよ。

設問3　〔障害事例1〕について，(1)～(3)に答えよ。

(1) 図5中の項番④，⑥～⑨の空欄に入れる適切な字句を答えよ。

(2) サーバγからサーバαへのpingが失敗した原因は何か。IPアドレスを具体的に示し，50字以内で述べよ。

(3) この障害が発生した原因への対策を，第2回以降の作業に反映させることにした。改善すべき点を，35字以内で述べよ。

設問4　〔障害事例2〕について，(1)～(3)に答えよ。

(1) 図4中におけるポート①～⑥の正常時の状態を解答群の中から選び，記号で答えよ。

解答群

ア　代表ポート　　イ　バックアップポート

ウ　ブロッキングポート　　エ　ルートポート

(2) L2SW-1がBPDUを処理できなくなったことが，ほかのL2SWに接続されているサーバの通信にまで影響したのはなぜか。図4中の機器名，ポートの識別用の番号を用いて，60字以内で述べよ。

(3) 表3中で，時刻11:45に運用SEが監視オペレータに指示した障害復旧処置を，30字以内で述べよ。

設問5　〔連絡体制の整備〕について，(1)，(2)に答えよ。

(1) 図6の障害時連絡体制にF部長の要望を反映させた体制について，本文中の役割名を用いて解答欄の図を完成させよ。

(2) 新たなプロジェクトチームでは，以前から問題とされていた“構成管理の不備”への対応から始めることになった。問題点を具体的に指摘し，その対応内容を，50字以内で述べよ。

〔 メ モ 用 紙 〕

7. 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

8. **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。
9. 問題冊子の余白などは，適宜利用して構いません。
10. 試験時間中，机上に置けるもの及び使用できるものは，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，黒鉛筆又はシャープペンシル，鉛筆削り，消しゴム，定規，時計（アラームなど時計以外の機能は使用不可），ハンカチ，ティッシュ
これら以外は机上に置けません。使用もできません。
11. 試験終了後，この問題冊子は持ち帰ることができます。
12. 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。
13. 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。