ネットワークスペシャリスト試験　午後問題

一問一答　分野別問題集

平成28年度～令和7年度　統合版

全 234 問（問題編＋解答編）

ルーティング	25 問
IPアドレスとアドレス解決	19 問
DNSと名前解決	13 問
電子メール	11 問
WebとHTTP	21 問
暗号とTLS	15 問
認証とアクセス制御	9 問
VPNとWAN	26 問
無線LAN	13 問
スイッチングとLAN	19 問
マルチキャストと配信	5 問
クラウドと仮想化とSDN	9 問
冗長化と負荷分散	12 問
監視と運用	16 問
セキュリティ対策	6 問
IoT	15 問

使い方

PDFのダウンロードありがとうございます。

〈問題に関して〉

これは過去10年分の過去問のうち、**「知識で回答する単発問題」**だけに特化した問題集です。令和7年（2025年）から平成28年（2016年）の過去問から抜粋しています。抜粋はAIに手伝ってもらいましたが全ての問題に目を通し作者本人が実際に解いて不備がないこと及びクオリティが担保されていることを確認したつもりです。それでも不備などが紛れている可能性がありますので、何かあればTwitter（現𝕏）のアカウントにて報告してもらえると助かります。

たまに出てくる☆マークが付いている空欄は実際に試験で問われた箇所です。表の問題などには他の単語も覚えたいなと思って個人的に勝手に穴埋めにしたものも混ざっています。

さて、B問題、鬼門ですね。長文は腰を据えて勉強できる時間がないとなかなか集中できないこともあり、電車での移動中や何かの待ち時間など短い隙間時間に勉強できないのも難しさの理由の一つだと思います。日々の隙間時間にできることといえば単語の確認や調べ物だと個人的に思っています。このPDFを印刷して冊子のように使うことで小さな単語帳のように隙間時間を有効に活用できることを願っています。

配布開始時現在の11/5時点ではまだ大々的に発表していませんが、ネットワークスペシャリストに出てくる単語を学習する用のサイトとしてtokotokologos.comという辞書サイトを運営しています。開発中でまだ至らないところも多々ありますが、どんどん使いやすくしていこうと思っているので、もしよろしければそちらもお使いください

最後のネットワークスペシャリスト試験、後悔のないよう共に頑張りましょう！！！！！！！！！！！！

イマシルピー
連絡先　@ImashiruP

問題編

ルーティング　25問

Q1 〔令和7年 午後I 問1 a〕

A社NWのOSPFのエリアは、エリアIDが0.0.0.0と表記される**（ａ）**エリアだけで構成されている。

Q2 〔令和7年 午後I 問1 b〕

OSPFルータにはループバックインタフェースが作成され、ループバックIPアドレスが設定されている。ループバックIPアドレスは、OSPFルータを識別する**（ｂ）**IDとして利用されている。

Q3 〔令和6年 午後I 問1 ウ・エ〕

BGPでの経路選択では、LP（LOCAL_PREF）属性については値が**（ウ）**経路を優先し、MED（MULTI_EXIT_DISC）属性については値が**（エ）**経路を優先する。

Q4 〔令和6年 午後I 問2 イ〕

ルータ1～4で二つのルーティングプロトコル間におけるルーティングを可能にするために、経路情報の**（イ）**をしている。このとき、一方のルーティングプロトコルで学習された経路がもう一方のルーティングプロトコルを介して再び同じルーティングプロトコルに渡されることのないように経路フィルターが設定されている。

Q5 〔令和6年 午後I 問2 エ〕

BGP4において、AS内部の経路交換はiBGPが用いられるのに対し、各拠点のルータとPEルータとの経路交換では**（エ）**が用いられる。

Q6 〔令和6年 午後I 問2 オ〕

L社VPNと接続するために、AS番号65500が割り当てられている。このAS番号はインターネットに接続されることのないASのために予約されている番号の範囲に含まれる。このようなAS番号を**（オ）**AS番号という。

Q7 〔令和6年 午後I 問2 カ〕

オーバーレイネットワークは、アプリケーショントラフィックを識別したルーティングを行う。このように、アプリケーショントラフィックを識別したルーティングを（カ）ルーティングという。

Q8 〔令和6年 午後II 問1 d〕

L3SWは、OSPFで交換するLSA（Link State Advertisement）の情報から（d）というデータベースを作成する。

Q9 〔令和6年 午後II 問1 e〕

L3SWは、OSPFで交換するLSAの情報から作成したデータベースを基に、それぞれのL3SWを根とする（e）ツリーを作成して、ルーティングテーブルに経路情報を登録する。

Q10 〔令和5年 午後II 問1 a〕

RFC 4271で規定されているBGPは、（a）間の経路交換のために作られたプロトコルで、TCPポート179番を利用して接続し、経路交換を行う。

Q11 〔令和5年 午後II 問1 b〕

BGPは、TCPポート179番を利用して接続し、経路交換を行う。経路交換を行う隣接のルータを（b）と呼ぶ。

Q12 〔令和5年 午後II 問1 c〕

経路制御は、（c）メッセージに含まれるBGPパスアトリビュートの一つであるLOCAL_PREFを利用して行う。このメッセージは、表3（BGPで交換されるメッセージ）ではタイプ2に当たり、経路情報の交換に利用され、経路の追加や削除が発生した場合に送信される。

Q13 〔令和5年 午後II 問1 表3〕

BGPで交換されるメッセージは4タイプあり、表3に示す。各タイプの名称を答えよ。

表3 BGPで交換されるメッセージ

タイプ	名称	説明
1	（1）	BGP接続開始時に交換する。自AS番号、BGPID、バージョンなどの情報を含む。
2	（2）☆	経路情報の交換に利用する。経路の追加や削除が発生した場合に送信される。
3	（3）	エラーを検出した場合に送信される。
4	（4）☆	BGP接続の確立やBGP接続の維持のために交換する。

Q14 〔令和5年 午後II 問1 e〕

BGPでは、ピアリングで受信した経路情報をBGPテーブルとして構成し、最適経路選択アルゴリズムによって経路情報を一つだけ選択し、ルータの（ e ）に反映する。

Q15 〔令和5年 午後II 問1 f〕

LOCAL_PREFは、iBGPピアに対して通知する、外部のASに存在する宛先ネットワークアドレスの優先度を定義する。LOCAL_PREFの場合では、最も（ f ）値をもつ経路情報が選択される。

Q16 〔令和4年 午後I 問2 a〕

本社及び営業所のIPsecルータは、LAN及びインターネットのそれぞれでデフォルトルートを使用するために、VRF（Virtual Routing and Forwarding）を利用して二つの（ a ）テーブルを保持し、経路情報をVRFの識別子（以下、VRF識別子という）によって識別する。

Q17 〔令和3年 午後I 問2 b・c〕

LSAには幾つかの種別があり、それぞれのTypeが定められている。例えば、（ b ）LSAと呼ばれるType1のLSAは、OSPFエリア内のルータに関する情報であり、その情報には、（ c ）と呼ばれるメトリック値などが含まれている。

Q18 〔令和3年 午後I 問2 d〕

OSPFエリア内の各ルータは、集められたLSAの情報を基にして、（ d ）アルゴリズムを用いた最短経路計算を行って、ルーティングテーブルを動的に作成する。

Q19 〔令和3年 午後I 問2 e〕

D社のセグメントa～fのIPアドレスは172.16.0.0/23、172.16.2.0/23、172.16.4.0/23、172.16.6.0/23、172.16.8.0/23、172.16.10.0/23であり、広域イーサ網のセグメントgは172.16.12.64/26である。支社ネットワーク集約がされた状態で、本社のL3SWの経路テーブルを見ると、a～gのそれぞれを宛先とする経路（支社個別経路）が一つに集約された、（ e ）/16を宛先とする経路が確認できる。

Q20 〔令和3年 午後II 問2 表3〕

> **表3**は、BGPの最適経路選択アルゴリズムの仕様であり、評価は表中の評価順に行われる。LOCAL_PREFは、iBGPピアに対して通知する、外部のASに存在する宛先ネットワークアドレスの優先度であり、MED（MULTI_EXIT_DISC）は、eBGPピアに対して通知する、自身のAS内に存在する宛先ネットワークアドレスの優先度で、メトリックとも呼ばれる。各評価順の決め手となる語を答えよ。

表3 最適経路選択アルゴリズムの仕様

評価順	説明
1	LOCAL_PREFの値が最も（1）経路情報を選択する。
2	AS_PATHの長さが最も（2）☆経路情報を選択する。
3	ORIGINの値で（3），EGP，Incompleteの順で選択する。
4	MEDの値が最も（4）☆経路情報を選択する。
5	（5）ピアで受信した経路情報，iBGPピアで受信した経路情報の順で選択する。
6	NEXT_HOPが最も（6）経路情報を選択する。
7	ルータIDが最も（7）経路情報を選択する。
8	ピアリングに使用するIPアドレスが最も（8）経路情報を選択する。

Q21 〔令和3年 午後II 問2 キ〕

担当者：BGPでは、（キ）メッセージを定期的に送信します。専用線の障害時には、ルータがこのメッセージを受信しなくなることによって、ピアリングが切断され、AS内の各機器の経路情報が更新されます。

Q22 〔令和元年 午後I 問1 a〕

接続先ISPとデータセンタは異なるAS番号で接続している。コアルータとISPとの間の冗長経路接続のためのルーティングプロトコルは、パスベクトル型ルーティングプロトコルである（a）が用いられている。

Q23 〔令和元年 午後I 問1 b〕

コアルータとL3SWとの間、L3SWとL3SWとの間のルーティングプロトコルは、リンクステート型ルーティングプロトコルであるOSPFが用いられている。OSPFエリアは一つであり、（b）エリアだけで構成されている。

Q24 〔平成29年 午後I 問3 ウ〕

BGPはルーティングプロトコルの一つであり、特定のルーティングポリシで管理されたルータの集まりを示す**（ウ）**の間で、経路情報の交換を行うために開発されたプロトコルである。

Q25 〔平成29年 午後I 問3 エ〕

BGP接続を行う2台のルータ間では、トランスポートプロトコルの一つである**（エ）**のポート179番を使用し、経路情報の交換を行う。このコネクションのことをBGPピアと呼ぶ。

IPアドレスとアドレス解決 19問

Q26 〔令和7年 午後I 問2 a・b〕

ルータはISPと接続しており、校内からインターネットへのアクセスに対し、NAPTを使って内側の**（a）**IPアドレスをISPから割り当てられた**（b）**IPアドレスに変換している。

Q27 〔令和7年 午後II 問1 a・b〕

IPv4のARPによるアドレス解決では、要求元のノードは、求めるMACアドレスに対応するIPv4アドレスをARPリクエストの**（a）**フィールドに入れて、**（b）**キャストで送信する。

Q28 〔令和7年 午後II 問1 c〕

ARPリクエストを受信した、要求されたIPv4アドレスをもつノードは、自身のMACアドレスをARP**（c）**の送信元MACアドレスフィールドに入れて、要求元のノード宛てに送信する。

Q29 〔令和7年 午後II 問1 d〕

IPv6アドレスは128ビットで構成され、**（d）**ビットずつを":"で区切って表される。

Q30 〔令和7年 午後II 問1 e・f〕

インタフェース識別子の生成方法の一つは、**（e）**ビットのMACアドレスから**（f）**ビットのModified EUI-64形式のインタフェース識別子を生成する方法である。

Q31 〔令和7年 午後II 問1 i〕

IPv4のネットワークではFWによるアクセス制御に加えて、ルータBに**（i）**を設定しているので、インターネットから社内ネットワークには簡単に通信できない設計になっています。IPv6のネットワークではこれを利用しないので、FWのアクセス制御の設計については慎重に検討する必要があります。

Q32 〔令和5年 午後I 問3 h〕

WLAN端末へのIPアドレス配布はDHCPサーバを使用しますので、基幹L3SWには**（h）**を設定します。また、基幹L3SWのデフォルトルートは上位のFWに指定します。

Q33 〔令和3年 午後I 問1 設問1(1)〕

在庫管理端末はDHCPクライアントであり、DHCPによってIPアドレスの割当てを受ける。DHCPでは、端末のIPアドレスとともに、名前解決に用いるDNSサーバのIPアドレスも端末に通知することができる。在庫管理端末に、名前解決に用いるサーバのIPアドレスを通知するサーバは**（設問1(1)）**である。

Q34 〔令和3年 午後II 問2 a・b〕

各機器に付与されているアドレス（抜粋）：ルータ10Zのインタフェースh＝α.β.γ.1/30、ルータ10のインタフェースf＝α.β.γ.2/30、ルータ11Zのインタフェースi＝α.β.γ.5/30、ルータ11のインタフェースg＝α.β.γ.6/30。iBGPのピアリングでNEXT_HOPを書き換える設定を行わない場合に、FW10のルーティングテーブルに追加で必要になる宛先ネットワークアドレスは、インタフェースhとfが属するネットワークと、インタフェースiとgが属するネットワークであり、それぞれ**（a）**と**（b）**である（順不同）。

Q35 〔令和元年 午後I 問1 c〕

CRに顧客が設定したデフォルトルートのネクストホップは、L3SWで構成されるVRRPの仮想ルータのIPアドレスになる。マスタルータが故障した際には、新しくマスタになったルータが**（c）**パケットをブロードキャストすることによってL2SWのMACアドレステーブルを更新する。

Q36 〔令和元年 午後I 問3 設問1〕

PCのIPアドレスは、DHCPサーバによって割り当てられる。DHCPサーバとPCのセグメントが異なっている場合に、PCが送信するDHCPのブロードキャストをDHCPサーバへ中継するために、スイッチに必要となる機能は**（設問1）**である。

Q37 〔令和元年 午後I 問3 a・b〕

通信制限装置は、セグメント内のARPパケットを監視し、排除対象PCが送信したARP要求を検出すると、排除対象PCのパケット送信先が通信制限装置となるように偽装したARP応答を送信する。このARP応答の送信元ハードウェアアドレスは**（a）**、送信元プロトコルアドレスは**（b）**である。

Q38 〔令和元年 午後I 問3 c・d〕

通信制限装置は、同時に、アドレス解決対象が排除対象PC宛てに送信するパケットの送信先が通信制限装置となるように偽装したARP要求を、アドレス解決対象に送信する。このARP要求の送信元ハードウェアアドレスは**（c）**、送信元プロトコルアドレスは**（d）**である。

Q39 〔令和元年 午後II 問2 設問3〕

DMZの公開サーバ用のグローバルIPアドレスのネットワークアドレスは、α.β.γ.0/28である。DMZの全ての公開サーバを対象とするブロードキャストアドレス宛てのスマーフ攻撃のパケットは、FWでブロックされる。このときのブロードキャストアドレスは**（設問3）**である。

Q40 〔平成30年 午後I 問2 イ〕

echo requestパケットの宛先として、監視対象機器には**（イ）**を割り当てる必要がある。

Q41 〔平成29年 午後I 問3 ア〕

K社NWのPCとサーバには、プライベートIPアドレスを割り当てる。PC及びサーバからインターネットへのWeb閲覧などの通信は、FWでIPアドレスとポート番号の変換処理である**（ア）**を行う。

Q42 〔平成29年 午後II 問1 い〕

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。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アドレスは書き換えられる。

Q43 〔平成28年 午後I 問2 オ〕

タブレット端末がインターネット上のサーバと通信を行う際に、モバイルWi-Fiルータでは**（オ）**によるIPアドレスとポート番号の変換処理が行われる。

Q44 〔平成28年 午後II 問1 ウ・設問1(2)〕

ブラウザ2がインターネットへアクセスする際に、FWのNAT機能が送信元IPアドレスと**（ウ）**の両方をそれぞれ動的に変換する（以下、送信元NAPTという）。

条件：変換後のIPアドレス用に二つのグローバルIPアドレスが割り当てられている。ポート番号は16ビットであり、2の16乗＝65,536である。この送信元NAPTが同時に処理できるTCPコネクション数の上限は**（設問1(2)）**である。

DNSと名前解決 13問

Q45 〔令和7年 午後II 問1 h〕

DNSメッセージが最大のメッセージサイズを超えるときや、EDNSに対応していない権威DNSサーバと512バイトを超えるDNSメッセージを送受信するときには、**（h）**で送受信することになります。

Q46 〔令和6年 午後II 問2 c〕

送信元メールアドレスの詐称の有無に対しては、DNSの**（c）**と呼ばれる名前解決によって、送信元メールサーバのIPアドレスからメールサーバのFQDNを取得し、そのFQDNと送信元メールアドレスのドメイン名が一致した場合、詐称されていないと判定する検査方法が考えられる。

Q47 〔令和6年 午後II 問2 h・i〕

しかし、DNSをトランスポートプロトコルである**（h）**で利用する場合は、DNSメッセージの最大長が**（i）**バイトという制限がある。

Q48 〔令和5年 午後I 問1 b・c〕

DMZのDNSサーバは、G社のサービス公開用ドメインに対する**（b）**DNSサーバであると同時に、サーバセグメントのサーバがインターネットにアクセスするときの名前解決要求に応答する**（c）**DNSサーバである。

Q49 〔令和5年 午後II 問1 設問1(1)〕

> **表2** プロキシサーバに関するDNSゾーンファイルの記述内容のうち、案2の初期設定では、従業員が指定するホストproxy.a-sha.co.jpに対して、192.168.1.145と192.168.2.145の二つのAレコードが登録されている。このように、負荷分散を目的として一つのドメイン名に対して複数のIPアドレスを割り当てる方式を**（設問1(1)）**という。

Q50 〔令和5年 午後II 問2 a〕

図2 DNSサーバに設定されているゾーン情報の項番2：『IN （ａ） ns.example.jp.』このレコードは、ゾーンのDNSサーバ（ネームサーバ）を指定するリソースレコードである。

Q51 〔令和5年 午後II 問2 b〕

図2 DNSサーバに設定されているゾーン情報の項番3：『IN （ｂ） 10 mail.example.jp.』このレコードは、優先度（10）とメールサーバのホスト名を指定する、メールの配送先を示すリソースレコードである。

Q52 〔令和4年 午後I 問3 イ〕

> **表1** FWの許可ルール項番1、3、5では、DNSの通信のプロトコル/ポート番号として、TCP/53と（イ）が併記されている。

Q53 〔令和4年 午後II 問2 エ・エ〕

APごとに、コンテンツDNSサーバにリソースレコードの一つである（エ）レコードとして、VRRPで利用する仮想IPアドレスを登録し、FQDNとIPアドレスの対応付けを定義する。PCにインストールされているWebブラウザ及び専用クライアントソフトウェアは、DNSの（エ）レコードを参照して接続するAPのIPアドレスを決定する。

Q54 〔令和3年 午後II 問1 a〕

内部DNSサーバは、DNS（ａ）であり、PC及びサーバから送信された社外のドメインに関する名前解決要求を、ISPが提供するフルサービスリゾルバに転送する。

Q55 〔令和元年 午後II 問2 設問2〕

外部DNSサーバはマスタDNSサーバであり、インターネット上のR社DNSサーバをスレーブDNSサーバとして利用している。FWのルールは次のとおりである。

表1 FWのルール

項番	送信元	宛先	プロトコル/ポート番号
2	R社DNSサーバ	外部DNSサーバ（α.β.γ.1）	TCP/53

このルールによって行われる通信の名称は（設問2）である。

Q56 〔平成29年 午後II 問1 つ〕

B社CDNを適用する場合には、DNS-Aのゾーンファイルのレコード"weblive IN A i6"を、"weblive IN （つ） webasha.bshacdn.example.net."に置き換えて、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。

Q57 〔平成28年 午後I 問3 a〕

D社のプライマリDNSはDNS1である。DNS2は非公開のD社内ゾーン情報だけを保有するセカンダリDNSである。DNS3は公開ゾーン情報だけを保有するセカンダリDNSである。プライマリDNSは、セカンダリDNSとだけ通信を行う。ゾーン情報の更新時には、プライマリDNSがセカンダリDNSへ更新通知（NOTIFYメッセージ）を送信する。これを契機として、（a）が行われる。

電子メール 11問

Q58 〔令和6年 午後II 問2 a・b〕

図2 外部DNSサーバYが管理するゾーン情報（抜粋）には、y-sha.com. IN MX 20 y-mail1.y-sha.com. と、y-sha.com. IN MX 1 y-mail2.y-sha.com. が登録されている。顧客が送信したメールがメール中継サーバに転送されるときは、外部DNSサーバYに登録されたMXレコードの（a）値によって、平常時は、ホスト名が（b）のメール中継サーバが選択される。

Q59 〔令和6年 午後II 問2 d・e・f〕

サポート担当者は、送信元メールアドレスがsupport@y-sha.comにセットされたサポートメールを、顧客宛てに送信する。顧客のメールサーバは、メール中継サーバから、メール転送プロトコルである（d）の（e）コマンドで指定されたメールアドレスのドメイン名の（f）を入手し、DNSを利用して、そのドメインのゾーン情報を管理する外部DNSサーバYに登録されているSPFレコードを取得する。

Q60 〔令和6年 午後II 問2 g〕

DKIMは、送信側のメールサーバでメールに電子署名を付与し、受信側のメールサーバで電子署名の真正性を検証することで、送信者のドメイン認証を行う。電子署名のデータは、メールの（g）及び本文を基に生成される。

Q61 〔令和6年 午後II 問2 表2〕

> **表2**は、DNSサーバにTXTレコードとして登録するDKIMレコード中のタグの説明である。各タグを答えよ。なお、最後の空欄はpの説明文中の鍵名である。

表2 DKIMレコード中のタグの説明（抜粋）

タグ	説明
（1）	バージョン番号を示す。指定する場合は“DKIM1”とする。
（2）	電子署名の作成の際に利用する鍵の形式を指定する。
（3）	DKIMの運用状態が本番運用モードの場合は“s”を指定する。
（4）	Base64でエンコードした（5）☆のデータを指定する。

Q62 〔令和6年 午後II 問2 表3〕

> **表3**は、送信するメールに付加するDKIM-Signatureヘッダー中のタグの説明である。各タグを答えよ。

表3 DKIM-Signatureヘッダー中のタグの説明（抜粋）

タグ	説明
（1）	Base64でエンコードした電子署名データ
（2）	電子署名を行ったドメイン名
（3）	複数のDKIMレコードの中から鍵を取得する際に、検索キーとして利用するセレクター名

Q63 〔平成28年 午後I 問1 ア〕

外部のメールサーバは、DNS3に設定された資源レコードのうち、**（ア）**レコードの情報に従って、A社ドメイン宛てのメールをMSV3に転送する。A社内PCは、MSV3に届いたメールを、POP3を用いて取得する。

Q64 〔平成28年 午後I 問1 エ・設問2(5)②〕

本文：『MSV3は、SMTPプロトコル上でユーザ認証を行う方式である**（エ）**を導入し、TCPの**（設問2(5)②）**番ポートで接続を受け付ける。また、その通信に対してTLSによる暗号化を行う。』外部からDMZへの2種類の通信を許可するためにFWを設定変更する際、メール送信の宛先ポート番号はこの値である。

Q65 〔平成28年 午後I 問1 オ・キ〕

P社及びQ社は、迷惑メールの送信を防止する対策として、OP25B（Outbound Port 25 Blocking）のポリシでメールシステムを運用している。OP25Bのためのアクセスリストは次のとおりである。

アクセスリスト

項番	動作	プロトコル	宛先IPアドレス	宛先ポート番号
1	禁止	**（オ）**	any	**（キ）**

Q66 〔平成28年 午後I 問1 設問2(4)〕

MSV3は、SMTP-AUTHを導入し、TCPの587番ポートで、メールクライアントからのメール送信の接続を受け付ける。この587番ポートは**（設問2(4)）**と呼ばれる。

Q67 〔平成28年 午後I 問1 設問2(5)①〕

検討の結果、B社のPCからのメール送受信にはMSV3を用い、受信についてはPOP3をTLSで暗号化して用いることになった。メール送受信の通信の暗号化は、接続時に平文で通信を開始して途中で暗号化通信に切り替えるSTARTTLS方式を採用し、メールクライアントからのSTARTTLSコマンドに応じてTLS暗号化を開始する。外部からDMZへの2種類の通信を許可するためにFWを設定変更する際、POP3によるメール受信の宛先ポート番号は**（設問2(5)①）**である。

Q68 〔平成28年 午後I 問1 設問3(1)〕

SPFは、送信メールサーバの正当性（当該ドメインの真正のメールサーバであること）を、受信メールサーバ側で確認する方式である。受信側のメールサーバは、メール受信時に、"SMTP通信中にやり取りされる送信元ドメイン名"を得て、その送信元ドメイン名に対するSPFレコードをDNSに問い合わせ、得られたSPFレコードを用いて送信元ドメインの認証を行う。送信元ドメイン名が得られるSMTPプロトコルのコマンドは**（設問3(1)）**である。

WebとHTTP　21問

Q69 〔令和7年 午後I 問2 e・f〕

HTTPレイヤーでは、例えばWebページの表示のために10枚の画像データをダウンロードする場合、PCからのHTTP**（e）**と、それに対するサーバからのHTTP**（f）**を一つずつ10回実行することになり時間が掛かる。

Q70 〔令和7年 午後I 問2 g・h〕

それを抑えるために、HTTP/2では仮想的な通信単位であるストリームの概念が導入されました。ストリームにはそれぞれ**（g）**が付与され、一つのTCPコネクションの中で複数のストリームを利用できるようになり、HTTPセッションの多重化と**（h）**処理ができるようになっています。

Q71 〔令和7年 午後I 問3 d〕

本文：『J社ではPCのWebブラウザを利用して、社内の業務用サーバ、K社が提供する電子メール・ストレージサービス（K社SaaS）にHTTPSでアクセスして業務を行っている。』

表1 FWの許可ルール

項番	送信元	宛先	プロトコル/宛先ポート番号
8	内部セグメント	K社SaaS	TCP/**（d）**

Q72 〔令和6年 午後I 問3 イ・ウ〕

WPADは、**（イ）**や**（ウ）**の機能を利用して、PACファイルの場所を配布するプロトコルである。

Q73 〔令和6年 午後I 問3 エ〕

WPADは、PACファイルの場所を配布するプロトコルである。PCやWebブラウザのWebプロキシ自動検出が有効になっていると、DHCPサーバやDNSサーバと通信を行い、アプリケーションレイヤープロトコルの一つである**（エ）**を利用してPACファイルのダウンロードを試みる。

Q74 〔令和6年 午後I 問3 オ〕

WPADは、PACファイルの場所を配布するプロトコルである。Bさんは、WPADは利用しないことにし、PCやWebブラウザのWebプロキシ自動検出を無効にした。PCやWebブラウザにはPACファイルの**（オ）**を直接設定する。

Q75 〔令和5年 午後I 問1 a〕

WebサーバではHTTPサーバが稼働しており、静的コンテンツはWebサーバから直接配信される。一方、APサーバの動的コンテンツは、Webサーバで中継して配信される。この中継処理の仕組みを**（a）**プロキシと呼ぶ。

Q76 〔令和5年 午後I 問1 d〕

HTTP/2では、TCPコネクション内で複数のリクエストとレスポンスのやり取りを**（d）**と呼ばれる仮想的な通信路で多重化している。

Q77 〔令和5年 午後I 問1 e〕

ヘッダー圧縮では、HPACKと呼ばれるアルゴリズムによって、HTTPヘッダー情報がバイナリフォーマットに圧縮されている。ヘッダーフィールドには、**（e）**, :scheme, :pathといった必須フィールドがある。

Q78 〔令和5年 午後I 問2 II〕

IPカメラの死活監視、遠隔制御を行い、Webサーバ機能をもつサーバは、PCとはHTTPSで通信を行う。

表1 ユニキャスト通信の許可ルール

項番	通信経路	送信元	宛先	プロトコル/宛先ポート番号
2	執務エリア1、2→サーバ室	PC	このサーバ	TCP/**（II）**

Q79 〔令和4年 午後I 問1 c〕

また、プロキシサーバは、HTTPの**（c）**メソッドでトンネリング通信を提供し、トンネリング通信に利用する通信ポートを443に限定する。

Q80 〔令和4年 午後II 問2 設問2(2)〕

WebAPコンテナには、APごとに一つのFQDNを割り当て、コンテンツDNSサーバに登録する。

本文：『共用リバースプロキシは、クライアントからのHTTPリクエストを受け、**（設問2(2)）**情報からWebAPを識別し、WebAPが動作するWebAPコンテナへHTTPリクエストを振り分ける。』

Q81 〔令和3年 午後I 問1 設問2(2)〕

RTは、RT管理コントローラに、REST APIを利用してRTのシリアル番号とEPのIPアドレスを送信し、登録する。この登録に用いられる、OSI基本参照モデルでアプリケーション層に属するプロトコルは**（設問2(2)）**である。

Q82 〔令和元年 午後I 問2 イ〕

LBの死活監視機能について、Uさんは、WebAPの稼働状況を監視するために、レイヤ7方式を利用することにした。死活監視に用いるHTTPリクエストの設定は、宛先IPアドレス＝WebサーバのIPアドレス、ポート番号＝**（イ）**、メソッド＝GET、パス名＝/index.phpである。なお、LBとWebサーバ間の通信にはHTTPを用い、ポート番号にはHTTPのウェルノウンポート番号を用いる。

Q83 〔令和元年 午後I 問2 ウ〕

LBの死活監視（レイヤ7方式）では、Webサーバが正常に応答したことを確認するために、成功時のHTTPレスポンスのステータスコードが**（ウ）**であることをチェックする。

Q84 〔令和元年 午後I 問2 エ・オ〕

セッション維持機能のうち、セッションIDに基づいて行う方式では、WebサーバとWebブラウザ間で状態を管理するために用いられるCookieを利用する。LBは、HTTPレスポンスの**（エ）**ヘッダフィールドにセッションIDを追加する。HTTPレスポンスを受け取った利用者のWebブラウザは、そのセッションIDを、次に送信するHTTPリクエストの**（オ）**ヘッダフィールドに追加する。

Q85 〔平成30年 午後I 問1 ア・イ〕

一般に、プロキシには、**（ア）**プロキシと**（イ）**プロキシがある。F社のプロキシのように前者は、社内に対して、アクセス先URLのログ取得や、外部サーバのコンテンツをキャッシュして使用帯域を削減する目的で用いられる。一方、後者は、外部から公開サーバのオリジナルコンテンツに直接アクセスさせないことによる改ざん防止、キャッシュによる応答速度の向上、及び複数のサーバでの負荷分散を行う目的で用いられる。

Q86 〔平成30年 午後I 問1 設問2(1)〕

プロキシサーバを経由してHTTPSでアクセスする際に用いられる、HTTPプロトコルのメソッド名は**（設問2(1)）**メソッドである。

Q87 〔平成29年 午後I 問1 オ〕

SSL-VPNの基本的な動作には、**（オ）**、ポートフォワーディング、L2フォワーディングの3方式がある。

Q88 〔平成28年 午後I 問2 カ〕

プロキシサーバは、HTTPプロキシとHTTPSプロキシの各機能をもつ。HTTPプロキシの場合、プロキシサーバは、タブレット端末からのリクエストを受け付け、その内容を基に新たにHTTPサーバへリクエストを開始する。一方、HTTPSプロキシの場合、プロキシサーバは、タブレット端末からの**（カ）**要求によってHTTPSサーバへのTLSトンネルを中継し、その後のリクエストは、TLSトンネルの中をそのまま転送する。

Q89 〔平成28年 午後II 問1 カ・キ〕

前提：この通信は、IP-PBXのWebRTC機能を利用するものである。社外のブラウザ上で動作するAPがIP-PBXを介して社内のIP電話機と通信する。この通信では、最初にHTTP GETによるUpgrade要求と101 Switching Protocols応答があり、その後、REGISTERによる位置登録やINVITEによる発信へ進む。APは、通信プロトコル**（カ）**を使ってIP-PBXへアクセスし、その後のやり取り（HTTP GETのUpgradeヘッダによる要求と101 Switching Protocols応答）によって、通信プロトコルを**（キ）**に切り替え、切り替えた通信プロトコルの上でSIPプロトコルに基づくシグナリングを行う。

暗号とTLS 15問

Q90 〔令和5年 午後I 問1 f〕

一般的にHTTP/2は、HTTP/1.1と同じく“https://”のURIスキームが用いられる。そのため、通信開始処理において**（f）**プロトコルの拡張の一つであるALPN（Application-Layer Protocol Negotiation）を利用する。

Q91 〔令和4年 午後I 問2 h・h〕

R主任は、IPsec VPNの構成に用いるパラメータについて、現行の設計と比較検討した。検討したパラメータのうち、鍵の生成に用いるアルゴリズムと**（h）**を定めているDiffie-Hellmanグループ番号には、現行では1を用いているが、POPとの接続では1よりも**（h）**の長い14を用いた方が良いと考えた。

Q92 〔令和4年 午後II 問1 ア〕

TLSプロトコルのセキュリティ機能は、暗号化、通信相手の認証、及び**（ア）**である。

Q93 〔令和4年 午後II 問1 エ〕

認証局（以下、CAという）によって発行された電子証明書には、証明対象を識別する情報、有効期限、**（エ）**鍵、シリアル番号、CAのデジタル署名といった情報が含まれる。

Q94 〔令和4年 午後II 問1 カ〕

TLS1.3で規定されている鍵交換方式は、**（カ）**、ECDHE、PSKの3方式である。

Q95 〔令和4年 午後II 問1 設問2(1)〕

TLS1.3ではAEAD（Authenticated Encryption with Associated Data）暗号利用モードの利用が必須となっており、セキュリティに関する二つの処理が同時に行われる。その二つの処理とは、**（①）**と**（②）**である。

Q96 〔令和4年 午後II 問1 設問2(2)〕

TLSプロトコルで用いられる電子証明書の形式は、X.509によって定められている。X.509の電子証明書において、証明対象を識別する情報を示すフィールドは**（設問2(2)）**である。

Q97 〔令和4年 午後II 問1 設問3(6)〕

本文：『証明書失効リストは、失効した日時とクライアント証明書を一意に示す情報のリストになっている。』CAによって発行された電子証明書に含まれる情報のうち、クライアント証明書を一意に示す情報は、証明対象を識別する情報、有効期限、公開鍵に並んで記載される**（設問3(6)）**である。

Q98 〔平成30年 午後I 問1 ウ〕

アクセス先のURLを把握するために、プロキシサーバで暗号化通信を一旦復号し、必要な処理を行った上で再度暗号化した。しかし、社内PCでエラーメッセージ“証明書が信頼できない”が表示されたので、社内PCに**（ウ）**をインストールして解決した。

Q99 〔平成30年 午後II 問1 ア・イ・ウ〕

情報の漏えい及び改ざん対策のためにTLSを利用する。TLSには、情報を**（ア）**する機能、情報の改ざんを**（イ）**する機能、及び通信相手を**（ウ）**する機能がある。

Q100 〔平成29年 午後I 問1 ア・イ〕

十分な安全性を確保できないとされるハッシュアルゴリズムであるMD5又は**（ア）**を使用しないで済むように、TLSプロトコルのバージョン**（イ）**以上を利用する。

Q101 〔平成29年 午後I 問1 ウ・エ〕

SSL/TLSのコネクション開設時に、クライアント側から送られる**（ウ）**メッセージと、サーバ側から返される**（エ）**メッセージの交換が行われる。このとき、それ以降で用いられる暗号スイート（アルゴリズムの組合せを示した情報）が決定される。

Q102 〔平成29年 午後II 問2 d〕

> **表3** 無線LANのデータ暗号化方式（抜粋）：WEP（Wired Equivalent Privacy）は、RC4と呼ばれる暗号化アルゴリズムを使用した**（ d ）**鍵暗号方式である。

Q103 〔平成29年 午後II 問2 f〕

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。

Q104 〔平成28年 午後I 問2 ア〕

導入が検討されているタブレット端末及びモバイルWi-Fiルータは、WEP、WPA及びWPA2に対応しており、このうちのWPA2を採用する。WPA2は、無線LANの暗号化アルゴリズムとして**（ ア ）**が初めて採用された方式である。

認証とアクセス制御 9問

Q105 〔令和7年 午後I 問3 b〕

本文：『**（ b ）**は、プロキシサーバ及び業務用サーバの接続時にRADIUSプロトコルを用いて利用者認証を行っている。』

表1 FWの許可ルール

項番	送信元	宛先	プロトコル/宛先ポート番号
3	プロキシサーバ	このサーバ	UDP/1812

項番3の宛先もこのサーバである。

Q106 〔令和4年 午後I 問1 b〕

プロキシサーバのユーザ認証には、Base64でエンコードするBasic認証方式と、MD5やSHA-256でハッシュ化する**（ b ）**認証方式があるが、A社では後者の方式を採用している。

Q107 〔令和元年 午後II 問1 ウ〕

SIP UAがIP-PBXに位置情報登録を依頼する際、SIP UAはSIPメソッド**（ ウ ）**を使ってリクエストを行う。

Q108 〔令和元年 午後II 問1 エ〕

SIP UAがIP-PBXに位置情報登録を行う際、その登録リクエストでは、**（ エ ）**を認証するために“HTTPダイジェスト認証方式”が用いられる。

Q109 〔令和元年 午後II 問1 オ〕

認証情報がないリクエストを受け取ったIP-PBXはチャレンジ値を含むレスポンス“401 Unauthorized”を返す。SIP UAはチャレンジ値から生成した正しいレスポンス値を送り、IP-PBXはレスポンス“**（オ）**”を返す。

Q110 〔平成30年 午後I 問1 設問1(2)〕

社内PCからインターネットへのWebアクセスでは、プロキシサーバにおいて認証を行う。プロキシサーバで認証を行うことによって、アクセスログに付加できる情報は**（設問1(2)）**である。

Q111 〔平成30年 午後II 問1 ス〕

前提：Xシステムでは、Wさんは、認可コード、アクセストークン、及びリフレッシュトークンを使った認可の仕組みを採用することにした。業務サーバへの情報要求には、アクセストークンが用いられる。アクセストークンが有効でない場合、WebAPはリフレッシュトークンを使ったトークン要求を行い、トークン応答によって新しいアクセストークンを獲得する。

本文：『アクセストークンの有効期間を過ぎた場合でも、**（ス）**の有効期間内であれば、利用者の確認を行わずに、新しいアクセストークンが発行される。』

Q112 〔平成29年 午後II 問2 h〕

WPAでは、TKIPによって暗号鍵を生成する。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APの両者で生成される。

Q113 〔平成28年 午後I 問2 ウ〕

モバイルWi-Fiルータには、通信事業者が契約者を識別する情報が記録されている**（ウ）**が挿入されている。

VPNとWAN　26問

Q114 〔令和7年 午後I 問2 d〕

Vさんは実効速度を改善するために、インターネット接続サービスのベストエフォート型から**（d）**型への契約変更をU校に紹介することにした。

Q115 〔令和7年 午後II 問2 g〕

IPsecルータ1で動作するIKEv2は、IPsecルータ2との間で、四つのメッセージの交換を（ g ）往復で行い、SAD（Security Association Database）を作成する。

Q116 〔令和6年 午後I 問2 ア〕

PEルータは、L社VPNの顧客のネットワークを収容するために設置した、プロバイダエッジルータである。ルータ1～4は、拠点間を接続する機器であり、L社のPEルータと対向する（ ア ）エッジルータである。

Q117 〔令和6年 午後I 問3 ア〕

A社は、UTMのIPsec VPN機能を利用して、本社をハブ、各支社をスポークとする（ ア ）型のVPNを構成している。

Q118 〔令和4年 午後I 問2 e・f・g〕

前提：Q社SGWサービスを利用するために、本社及び営業所に導入する新IPsecルータ、並びにTPCは、Q社SGWサービスのPOPという接続点にトンネルモードのIPsec VPNを用いて接続する。IPsec VPNには、IKEバージョン2と、ESPのプロトコルを用いる。新IPsecルータ及びTPCとPOPは、IKE SAを確立するために必要な、暗号化アルゴリズム、疑似ランダム関数、完全性アルゴリズム及びDiffie-Hellmanグループ番号を、ネゴシエーションして決定し、IKE SAを確立する。次に、新IPsecルータ及びTPCとPOPは、認証及びChild SAを確立するために必要な情報を、IKE SAを介してネゴシエーションして決定し、Child SAを確立する。

本文：『新IPsecルータ及びTPCは、IPsec VPNを介して転送する必要があるパケットを、長さを調整するESPトレーラを付加して（ e ）化する。次に、新しい（ f ）ヘッダと、（ g ）SAを識別するためのESPヘッダ及びESP認証データを付加して、POP宛てに送信する。』

Q119 〔令和4年 午後II 問1 イ〕

SSL-VPNは、リバースプロキシ方式、ポートフォワーディング方式、（ イ ）方式の3方式がある。3番目の方式は、動的にポート番号が変わるアプリケーションプログラムでも社内のノードへのアクセスを可能にする方式である。

Q120 〔令和4年 午後II 問1 ウ〕

ポートフォワーディング方式のSSL-VPNは、社内のノードに対してTCP又はUDPの任意の（ ウ ）へのアクセスを可能にする。

Q121 〔令和4年 午後II 問1 オ〕

SSL-VPNには3方式がある。第1の方式は社内のWebアプリケーションへのアクセスを可能にし、第2の方式は社内のノードに対してTCP又はUDPの任意のポートへのアクセスを可能にし、第3の方式は動的にポート番号が変わるアプリケーションプログラムでも社内のノードへのアクセスを可能にする。

本文：『仮想PCへのアクセスのプロトコルはRDPとし、TCPの3389番ポートを利用する。SSL-VPN装置がRDPだけで利用されることを踏まえ、SSL-VPNの接続方式は**（オ）**方式とする。』

Q122 〔令和3年 午後I 問2 a〕

D社では、VPC GWとFWに、VPC内仮想セグメントのアドレス（192.168.1.0/24）、IPsec VPN認証用の事前**（a）**、相手の外部アドレス、D社内ネットワークアドレス（172.16.0.0/16、172.17.0.0/16）を設定している。

Q123 〔令和元年 午後II 問1 キ〕

Y-VPNは、Y社のクラウドPBXサービスを利用する顧客が共用するIP-VPNである。RFC 3031で標準化されている**（キ）**の技術が用いられている。

Q124 〔令和元年 午後II 問1 ク〕

D社の異なる拠点間の通話が他の拠点を経由しないように、Y-VPNの網内は**（ク）**構成となっている。

Q125 〔平成30年 午後I 問1 オ〕

本文：『SD-WANルータの設定は、**（オ）**によって集中制御される。』F社は、RSS配信されたIPアドレスブロックを検知するツールを作成して、自動的にツールからこのコントローラに指示を行い、全社のSD-WANルータの設定を変更することにした。

Q126 〔平成30年 午後I 問3 ア・イ〕

利用者のネットワークと事業者閉域IP網との接続点において、利用者が設置するCE（Customer Edge）ルータから送られたパケットは、通信事業者のPE（Provider Edge）ルータで**（ア）**と呼ばれる短い固定長のタグ情報が付与される。事業者閉域IP網内では、タグ情報を参照して中継され、ラベルは対向側の**（イ）**で取り除かれる。

Q127 〔平成30年 午後I 問3 ウ〕

IPsecは、暗号技術を利用してノード間通信を行うためのプロトコルであり、IPパケット通信の完全性・機密性を確保する。IPsecは、OSI基本参照モデルの**（ウ）**レイヤで動作する。

Q128 〔平成30年 午後I 問3 設問2(1)〕

本文：『IP-VPNは、事業者閉域IP網内で複数の利用者のトラフィックを中継するのに、RFC 3031で規定された方式が用いられる。』このパケット転送技術の名称は**（設問2(1)）**である。

Q129 〔平成29年 午後I 問3 イ〕

IPsecのフェーズ1では、接続する相手を認証する方式として、両方の機器であらかじめ、**（イ）**と呼ばれる同じ鍵を共有する方式を利用する。

Q130 〔平成28年 午後I 問2 エ〕

モバイルWi-Fiルータには、利用者IDやパスワードといった認証情報に加えて、LTE回線からインターネットのようなネットワークへのゲートウェイの指定を意味する、**（エ）**の情報を設定する。

Q131 〔平成28年 午後II 問2 ア〕

SAの内容が確定すると、SAに関連付けされたSPI（Security Parameters Index）が、**（ア）**ビットの整数値で割り当てられる。SPIは、IPsec通信の各パケット中に挿入され、そのパケットに適用されたSAの識別キーとなる。

Q132 〔平成28年 午後II 問2 イ〕

IPsecルータは、通信相手のIPsecルータにパケットを送信するとき、IPsec通信を行うか否か、IPsec通信を行うときはどのSAを使うかなど、当該パケットに施す処理を示したセキュリティポリシ（以下、SPという）を選択する。SPを選択するキーを**（イ）**と呼び、IPアドレス、プロトコル、ポート番号などが利用される。SPは、SPデータベースで管理される。

Q133 〔平成28年 午後II 問2 ウ〕

IKEフェーズ1には、メインモードと**（ウ）**モードがある。メインモードでは3往復の通信が行われるが、このモードは1往復半の通信で完了する。

Q134 〔平成28年 午後II 問2 表1〕

IPsecでは、IKEフェーズ1でISAKMP SAに必要なパラメータが決定される。

> **表1**は、IKEフェーズ1で決定されるパラメータ（抜粋）である。各パラメータを答えよ。

表1 IKEフェーズ1で決定されるパラメータ（抜粋）

パラメータ	説明
暗号化方式	ISAKMPメッセージの暗号化アルゴリズム
（1）	ISAKMPメッセージの完全性の検証と鍵計算に使用するハッシュアルゴリズム
（2）	ISAKMP SAの生存期間
認証方式	IPsec通信相手機器の認証方式
鍵交換方式	鍵交換のためのアルゴリズム

Q135 〔平成28年 午後II 問2 表2〕

IKEフェーズ2では、IPsec SAに必要なパラメータが決定される。

> **表2**は、IKEフェーズ2で決定されるパラメータ（抜粋）である。各パラメータを答えよ。

表2 IKEフェーズ2で決定されるパラメータ（抜粋）

パラメータ	説明
（1）	IPsec通信で使用する（2）
暗号化方式	IPsec通信で使用する暗号化アルゴリズム
認証方式	IPsec通信で使用する認証アルゴリズム
（3）	IPsec SAの生存期間
通信モード	（4）モード又は（5）モード

Q136 〔平成28年 午後II 問2 エ〕

IPパケットをGREでカプセル化すると、カプセル化された元のパケットの宛先への（エ）情報をインターネットがもたなくても、元のパケットによるエンドツーエンドの通信が可能になる。

Q137 〔平成28年 午後II 問2 オ〕

IPパケットをGREでカプセル化すると、GREトンネルインタフェースのMTUは、イーサネットインタフェースのMTUよりも24バイト小さくなる。このとき、PC及びサーバのイーサネットインタフェースのMTUサイズを適切な値に変更することによって、パケットの（オ）を防げる。

Q138 〔平成28年 午後II 問2 あ〕

条件：ジャンボフレームは使用されないものとし、イーサネットのMTUは1,500バイトとする。IPパケットをGREでカプセル化したときのパケット形式は、IPヘッダ1（20バイト）、GREヘッダ（4バイト）、IPヘッダ2（20バイト）、TCP/UDPヘッダ（20バイト）、データの順である。このとき、データの最大バイト数は**（あ）**である。

Q139 〔平成28年 午後II 問2 い〕

条件：ジャンボフレームは使用されないものとし、イーサネットのMTUは1,500バイトとする。PPPフレームをL2TPでカプセル化したときのパケット形式は、IPヘッダ1（20バイト）、UDPヘッダ（8バイト）、L2TPヘッダ（16バイト）、PPPヘッダ（2バイト）、IPヘッダ2（20バイト）、TCP/UDPヘッダ（20バイト）、データの順である。このとき、データの最大バイト数は**（い）**である。

無線LAN 13問

Q140 〔令和5年 午後I 問3 a〕

Wi-Fi 6では、2.4GHz帯と5GHz帯の二つの周波数帯によるデュアルバンドに加え、5GHz帯を二つに区別し、2.4GHz帯と合わせて計三つの周波数帯を同時に利用できる**（a）**に対応したAPが多く登場している。

Q141 〔令和5年 午後I 問3 b〕

Wi-Fi 6では、送受信側それぞれ複数の**（b）**を用いて複数のストリームを生成し、複数のWLAN端末で同時に通信するMU-MIMOが拡張されている。

Q142 〔令和5年 午後I 問3 c〕

個人向けのWPA3-Personalでは、PSKに代わってSAE（Simultaneous Authentication of Equals）を採用することでWPA2の脆弱性を改善し、更に利用者が指定した**（c）**の解読を試みる辞書攻撃に対する耐性を強化している。

Q143 〔令和5年 午後I 問3 d〕

B主任：はい、20MHz帯域幅チャネルを**（d）**によって二つ束ねた40MHz帯域幅チャネルによって、要件を満たす目途がついています。

Q144 〔平成29年 午後II 問2 a・b〕

表1 IEEE 802.11で使用される周波数帯（抜粋）

規格	使用する周波数帯	最大伝送速度
802.11n	（a）GHzと（b）GHz	600Mビット/秒

Q145 〔平成29年 午後II 問2 表2〕

> **表2**は、無線LANのアクセス制御方式とその機能をまとめたものである。各方式の名称を答えよ。

表2 無線LANのアクセス制御方式

方式	機能
（1）	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
（2）☆接続拒否	SSIDが空白又は（3）☆での接続要求を拒否する機能
（4）	ビーコン信号にSSIDを含めない機能
（5）	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
（6）	RADIUSサーバを利用するなどしたクライアント認証機能

Q146 〔平成29年 午後II 問2 e〕

> **表3** 無線LANのデータ暗号化方式（抜粋）：WPA2は、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よりも堅牢なIEEE（e）準拠の方式である。

Q147 〔平成29年 午後II 問2 表3〕

> **表3**は、無線LANのデータ暗号化方式とその説明をまとめたものである。各方式の名称を答えよ。

表3 無線LANのデータ暗号化方式

方式	説明
（1）	RC4と呼ばれる暗号化アルゴリズムを使用した（2）☆鍵暗号方式
（3）	暗号化アルゴリズムは（4）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
（5）	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，（6）よりも堅牢なIEEE（7）☆準拠の方式

Q148 〔平成29年 午後II 問2 g〕

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。

Q149 〔平成29年 午後II 問2 i〕

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。

Q150 〔平成29年 午後II 問2 j〕

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（ハンドオーバ）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。

Q151 〔平成29年 午後II 問2 設問3(1)〕

IEEE 802.11acでは、160MHzの帯域幅でアンテナ1本当たり最大約867Mビット/秒の通信が可能であり、通信速度は帯域幅とアンテナ本数に比例する。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）まで行える。このAP製品には、3本のアンテナが搭載されている。このAP製品で最大約867M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は（1）MHz、アンテナ本数は（2）本である。

Q152 〔平成28年 午後I 問2 イ〕

認証方式には、あらかじめタブレット端末とモバイルWi-Fiルータに同じパスフレーズを設定する（イ）認証を用いる。このパスフレーズは一定以上の長さで十分に複雑な文字列とし、SSIDと同様に、モバイルWi-Fiルータごとに異なる値を設定する。

スイッチングとLAN　19問

Q153 〔令和7年 午後I 問2 c〕

L2SWは、最大30Wを給電する（c）機能をもち、イーサネットケーブル経由でAPに電力を供給している。

Q154 〔令和5年 午後I 問3 e〕

PoEの方式はPoE+と呼ばれるIEEE802.3atの最大30Wでは電力不足のリスクがありますので、（ e ）と呼ばれるIEEE802.3btを採用します。

Q155 〔令和5年 午後I 問3 f〕

それではフロアL2SWとAPとの間には（ f ）と呼ばれる2.5GBASE-Tか5GBASE-Tを検討してみます。

Q156 〔令和5年 午後I 問3 g〕

基幹L3SWとサーバL2SWはそれぞれ2台を（ g ）接続して論理的に1台とし、サーバ、FW、WLC及びフロアL2SWを含む全てのリンクを、スイッチをまたいだリンクアグリゲーションで接続する構成です。

Q157 〔令和4年 午後I 問1 d〕

ベンダ：フレームを転送するときは、宛先MACアドレスがMACアドレステーブルに学習済みかどうかを確認した上で、学習済みの場合には学習されているポートに転送します。宛先MACアドレスが学習されていない場合は（ d ）します。

Q158 〔令和3年 午後I 問1 a〕

RT、L2SW及び在庫管理端末は、必要なIFからOSI基本参照モデルの第（ a ）層プロトコルであるLLDP（Link Layer Discovery Protocol）によって、隣接機器に自分の機器名やIFの情報を送信する。隣接機器は受信したLLDPの情報を、LLDP-MIBに保持する。

Q159 〔令和3年 午後I 問3 a〕

Y社が利用するVoIP（Voice over Internet Protocol）では、音声の符号化にG.729として標準化されたCS-ACELPが使用される。CS-ACELPのビットレートは、（ a ）kビット／秒である。

Q160 〔令和3年 午後I 問3 b〕

電話サービス導入後は、音声を全てIPパケット化し、データパケットと一緒にLAN上に流す。音声をIPパケット化してLAN上に流すと、イーサネットフレームヘッダのほかに、IP、（ b ）及びRTPヘッダが付加されるので、1回線当たり34.4kビット／秒の帯域が必要となる。

Q161 〔令和3年 午後I 問3 c〕

大量の動画パケットがL3SW0に入力されたことによって、L3SW0で音声パケットの遅延又は**（c）**が発生したことが原因であると推定できた。

Q162 〔令和3年 午後I 問3 d〕

L3SWに、Diffserv（Differentiated Services）による優先制御を設定する。CoS値に対応したDSCP（Diffserv Code Point）値を、IPヘッダの**（d）**フィールドをDSCPとして再定義した6ビットにマーキングする。

Q163 〔令和3年 午後I 問3 設問3(1)〕

条件：電話サービス導入後は、外線通話の音声パケットは全て本社のIPsecルータ経由で送受信され、L3SW0のポートaから出力される。現在の回線数は、本社のPBXに収容された外線が80回線、5か所の営業所のPBXに収容された外線がそれぞれ10回線である。音声をIPパケット化すると、1回線当たり34.4kビット／秒の帯域が必要となる。現在の回線数を維持する場合、L3SW0のポートaから出力される音声パケットの通信量の最大値は**（設問3(1)）**kビット／秒である。

Q164 〔令和3年 午後II 問1 e〕

STPのネットワークでトポロジの変更が必要になると、スイッチはポートの状態遷移を開始し、**（e）**テーブルをクリアする。

Q165 〔令和3年 午後II 問1 f〕

RSTPのネットワークでは、スイッチRがルートブリッジであり、スイッチAはスイッチRとスイッチBに、スイッチBはスイッチRに接続している。スイッチAにおいて、スイッチRに接続するポートのダウンを検知したとき、スイッチBはスイッチAにプロポーザルを送信する。スイッチAは、受信したプロポーザル内のブリッジプライオリティ値やパスコストと、自身がもつブリッジプライオリティ値やパスコストを比較する。比較結果から、スイッチAは、スイッチBがRSTPによって構成されるトポロジにおいて**（f）**であると判定し、スイッチBにアグリーメントを送信し、指定ポートをルートポートにする。

Q166 〔令和3年 午後II 問1 表3〕

> **表3**は、RSTPで追加されたポートの役割である。各役割の名称を答えよ。

表3 RSTPで追加されたポートの役割

役割	説明
（1）	通常，ディスカーディングの状態であり，ルートポートのダウンを検知したら，すぐにルートポートになり，フォワーディングの状態になるポート
（2）	通常，ディスカーディングの状態であり，指定ポートのダウンを検知したら，すぐに指定ポートになり，フォワーディングの状態になるポート

注記：ディスカーディングの状態は，MACアドレスを学習せず，フレームを破棄する。

Q167 〔令和3年 午後II 問1 設問2(1)〕

STPでは、ブリッジプライオリティ値とMACアドレスで構成されるブリッジIDを比較してルートブリッジを決定する。内部NWのL2SW及びL3SWに同じブリッジプライオリティ値を設定した場合、L2SW及びL3SWはブリッジIDの**（設問2(1)）**を比較してルートブリッジを決定する。

Q168 〔平成30年 午後II 問2 ア〕

L2SWaとL2SWbの間及びL2SWcとL2SWdの間は、**（ア）**接続して、それぞれ一つのL2SWとして動作できるようにする。

Q169 〔平成30年 午後II 問2 エ〕

物理サーバには2枚のNICを実装し、**（エ）**機能を利用してアクティブ／アクティブの状態にする。

Q170 〔平成29年 午後I 問2 設問1〕

プリント通信では、PCからプリントサーバに印刷データを送信したとき、一時的に大量の帯域を使用する。このような現象を引き起こす、短時間に集中するトラフィックを**（設問1）**という。

Q171 〔平成29年 午後II 問2 設問3(5)〕

選定したAP製品の消費電力は最大18W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、IEEE 802.3at対応のL2SWを導入することにした。IEEE 802.3at規格のPoE機能の呼称は**（1）**である。また、APを合計12台設置するとき、このL2SWに必要になる最小供給電力は**（2）**Wである。

マルチキャストと配信　5問

Q172　〔令和5年 午後I 問2 ア・イ〕

L2SWでは、マルチキャストフレームを受信した際、同一セグメント上の受信インタフェース以外の全てのインタフェースへ**（ア）**するので、通信帯域を無駄に使用し、接続先のインタフェースへ不必要な負荷を掛けてしまう。この対策機能として、**（イ）**スヌーピングがある。L2SWのこの機能は、レシーバから送信されるJoinやLeaveのパケットを監視し、マルチキャストフレームの配信先の決定に必要な情報を収集する。

Q173　〔令和5年 午後I 問2 ウ〕

本文：『IPマルチキャストの配信要求プロトコルとして、IGMPv3を用いる。』IGMPv3のパケットはマルチキャストパケットである。レシーバ11は、IGMPv3メンバーシップレポートの(S,G) Joinを作成し、IGMP用に割り当てられたIP**（ウ）**アドレス宛てに送信する。

Q174　〔令和5年 午後I 問2 エ〕

L3SW11は、(S,G) Joinを基に(S,G)エントリを作成し、ユニキャストルーティングテーブルに基づき、ソースの方向であるFW01へPIMの(S,G) Joinを送信する。これによってディストリビューション**（エ）**が作成される。

Q175　〔令和5年 午後I 問2 オ・カ〕

IPマルチキャストでは、マルチキャストルーティング用のプロトコルとしてPIM-SMと、PIM-SMの派生型であるSSM（Source-Specific Multicast）を用いる。SSMでは、レシーバがIGMPv3を用いてソースのIPアドレス及びグループアドレスを指定して配信要求を行う。FW01、L3SW11及びL3SW21では、マルチキャストルーティングを有効化し、全てのインタフェースにおいて**（オ）**を有効化する。また、L3SW11及びL3SW21では、マルチキャストルーティング用のプロトコルとして**（カ）**を有効化し、レシーバが接続されたL2SWと接続するインタフェースにおいて、IGMPv3を有効化する。

Q176　〔令和5年 午後I 問2 キ〕

本文：『配信先であるレシーバは、マルチキャストパケットの映像データを映像へ**（キ）**し、大型モニターへ表示する。』PCに新たに導入する、IGMPv3に対応したソフトウェア製品にも、映像データから映像へ同じ処理を行う機能をもたせる。

クラウドと仮想化とSDN　9問

Q177　〔令和6年 午後II 問1 a・b〕

RFC 7348で規定されたVXLANでは、VXLANヘッダー内の（ａ）ビットのVNI（VXLAN Network Identifier）を用いて、約1,677万個のレイヤー2のオーバーレイネットワークをレイヤー（ｂ）のネットワーク上に構成できる。

Q178　〔令和6年 午後II 問1 c〕

L3SWのVTEPは、サーバから受信したイーサネットフレームに、VXLANヘッダー、（ｃ）ヘッダー及びIPv4ヘッダーを付加したIPパケットを、宛先のVTEPに転送する。

Q179　〔令和6年 午後II 問1 f〕

本文：『イーサネットフレームが、BUM（Broadcast、（ｆ）、Multicast）フレームの場合には、図2中のIPv4ヘッダーの宛先IPアドレスに、IPマルチキャストのグループアドレスをセットして転送する。』EVPNの機能2では、VTEPはMP-BGPを利用して、リモートVTEPに接続されたVMのMACアドレス、VNI及びリモートVTEPのIPアドレスをあらかじめ学習するので、このユニキャストフレームによるフラッディングの発生を低減できる。

Q180　〔令和6年 午後II 問1 g〕

本文（機能3）：『EVPNを適用した場合、VTEPはMP-BGPを用いて、自身に接続されたサーバを識別する（ｇ）（Ethernet Segment Identifier）という識別子を交換できるようになる。同じ識別子を設定した論理インタフェースをもつ複数のVTEPは、サーバとの接続にリンクアグリゲーションを利用できる。』同一の物理サーバに接続する2台のL3SWに作成するリンクアグリゲーションの論理インタフェースには、同一の物理サーバに接続されていることを識別させるために、同じこの識別子を設定する。

Q181　〔令和4年 午後II 問2 ア〕

ホストサーバでは、サーバ仮想化を実現するためのソフトウェアである（ア）が動作する。ホストサーバは仮想SWをもち、NICを経由してL2SWと接続する。

Q182　〔平成30年 午後I 問1 エ〕

SDNは、利用者の通信トラフィックを転送するデータプレーンと、通信装置を集中制御する（エ）プレーンから構成されている。

Q183 〔平成29年 午後I 問1 設問2(3)〕

SSL-VPNのL2フォワーディング方式では、PCにインストールするクライアントモジュールからSSL/TLS接続を行い、接続時の認証に応じて、PCに適切なIPアドレスを割り当てる。割り当てられたIPアドレスは、PCの仮想ネットワークインタフェースカードである**（設問2(3)）**に設定される。

Q184 〔平成29年 午後II 問1 表1〕

> **表1**は、SDNにおけるOFC（フローコントローラ）とOFS（スイッチ）間の通信メッセージ（抜粋）である。各メッセージの名称を答えよ。

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
（1）	OFS→OFC	入力パケットと入力ポートIDを，OFCに通知する。
（2）☆	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。
（3）☆	OFC→OFS	変更情報を送り，OFSの管理テーブルを変更させる。

Q185 〔平成29年 午後II 問1 お〕

OFCは、Flow-Mod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。ここでOutputの引数には、指定ポートに出力させるポートIDの他に、Packet-Inメッセージを使ってパケットをOFCに転送させることを指示する値が入る。

冗長化と負荷分散 12問

Q186 〔令和7年 午後I 問1 c〕

R20、R21の内部ネットワークと接続するインタフェースでは、PCに設定するデフォルトルートのネクストホップに相当する**（c）**の可用性を向上するために、VRRPが動作している。

Q187 〔令和6年 午後I 問1 ア〕

D社が導入しているLBのサーバ振分けアルゴリズムには、ラウンドロビン方式及び最少接続数方式がある。ラウンドロビン方式は、ゲーム端末からの接続を接続ごとに配信サーバに順次振り分ける方式である。最少接続数方式は、ゲーム端末からの接続をその時点での接続数が最も少ない配信サーバに振り分ける方式である。D社のゲームファイル配信では、振り分ける先の配信サーバの性能は同じだが、接続ごとに配信するゲームファイルのサイズに大きなばらつきがあり、配信に掛かる時間が変動する。各配信サーバへの同時接続数をなるべく均等にするために、LBの振分けアルゴリズムとして**（ア）**方式を採用している。

Q188 〔令和5年 午後II 問2 g・h〕

ECサーバの増強策としてスケール**（g）**方式とスケール**（h）**方式を比較検討し、ECサイトを停止せずにECサーバの増強を行える後者の方式を採用した。採用した方式では、ECサーバを2台増設して3台にし、負荷分散装置（LB）によって処理を振り分ける。

Q189 〔令和5年 午後II 問2 設問4(1)〕

本文：『導入するLBには、負荷分散用のIPアドレスである**（設問4(1)）**で受信したパケットをECサーバに振り分けるとき、送信元IPアドレスを変換する方式（以下、ソースNATという）と変換しない方式の二つがある。』

Q190 〔令和4年 午後II 問2 イ〕

一つのAPは2台のAP仮想サーバで構成する。2台のAP仮想サーバでは、冗長構成をとるためにVRRPバージョン3を動作させる。サーバセグメントでは複数のAPが動作するので、VRRPの識別子としてAPごとに異なる**（イ）**を割り当てる。

Q191 〔令和4年 午後II 問2 ウ〕

VRRPの規格では、最大**（ウ）**組の仮想ルータを構成することができる。

Q192 〔令和3年 午後II 問1 b〕

L3SW1及びL3SW2でVRRPを構成し、L3SW1の**（b）**を大きく設定して、マスタルータにしている。

Q193 〔令和元年 午後I 問2 ア〕

HTTPリクエストの振分け機能について、Uさんは、HTTPリクエストをWebサーバに**（ア）**に振り分けるラウンドロビン方式を採用することにした。

Q194 〔平成30年 午後I 問2 設問2(1)〕

本文：『コアSWにはVRRPが設定してあり、正常時は、コアSW1がマスタルータで、コアSW2がバックアップルータとなるように設定している。』PC及びサーバに設定する情報のうち、VRRPによる冗長化の対象となるのは**（設問2(1)）**である。

Q195 〔平成30年 午後I 問2 設問2(2)〕

VRRPでは、バックアップルータは、あるメッセージを受信しなくなったときにマスタルータに切り替わる。そのメッセージ名は**（設問2(2)）**である。

Q196 〔平成30年 午後II 問2 イ〕

冗長構成では、アクティブの仮想FWが保持しているセッション情報が、装置間を直結するケーブルを使って、スタンバイの仮想FWに転送される。セッション情報を継承することで、仮想FWの**（イ）**フェールオーバを実現している。

Q197 〔平成30年 午後II 問2 ウ〕

LBは、負荷分散対象のサーバ群を一つのグループ（クラスタグループ）としてまとめ、クラスタグループを複数設定できる製品を選定する。クラスタグループごとに仮想IPアドレスと**（ウ）**アルゴリズムが設定できるので、複数の顧客の処理を1台で行える。

監視と運用 16問

Q198 〔令和7年 午後I 問3 a〕

本文：『**（a）**は、プロキシサーバ及び業務用サーバのアクセスログ、認証サーバの認証ログ、FWの通信ログ、L3SWのDHCPリースログ、J社内のサーバやスイッチのシステムログを保存している。』

表1 FWの許可ルール

項番	送信元	宛先	プロトコル/宛先ポート番号
1	DMZ	このサーバ	UDP/514

項番1の宛先もこのサーバである。

Q199 〔令和4年 午後I 問1 a〕

ログデータの転送は、イベント通知を転送する標準規格（RFC 5424）の**（a）**プロトコルを利用している。

Q200 〔令和4年 午後I 問1 設問3(4)〕

L2SWからミラーパケットを受信するサーバは、宛先MACアドレスが自分のMACアドレス以外のフレームも受信できるように、インタフェースを**（設問3(4)）**モードに設定する必要がある。

Q201 〔令和4年 午後I 問1 設問3(5)〕

条件：キャプチャサーバに流れるミラーパケットが平均100kビット／秒であるとき、1,000日間のミラーパケットを保存するのに必要なディスク容量は**（設問3(5)）**Gバイトである。ここで、1kビット／秒は10^3ビット／秒、1Gバイトは10^9バイトとする。ミラーパケットは無圧縮で保存するものとし、ミラーパケット以外のメタデータの大きさは無視する。

Q202 〔令和4年 午後II 問2 キ〕

ping監視は、監視サーバが監視対象の機器に対してICMPのエコー要求を送信し、一定時間以内に**（キ）**を受信するかどうかで、IPパケットの到達性があるかどうかを確認する。

Q203 〔令和4年 午後II 問2 ク〕

TCP接続監視では、監視サーバが監視対象の機器に対してSYNパケットを送信し、一定時間以内に**（ク）**パケットを受信するかどうかで、TCPで通信ができるかどうかを確認する。

Q204 〔令和4年 午後II 問2 ケ〕

URL接続監視では、監視サーバが監視対象の機器に対してHTTP**（ケ）**メソッドでリソースを要求し、一定時間以内にリソースを取得できるかどうかで、HTTPサーバが正常稼働しているかどうかを確認する。

Q205 〔令和3年 午後I 問1 b〕

運用管理サーバは、L2SWと在庫管理端末から**（b）**によってLLDP-MIBを取得して、L2SWと在庫管理端末のポート接続リストを作成する。

Q206 〔令和元年 午後I 問1 d〕

現行の監視方法の一つは、**（d）**プロトコルを利用したpingによって、各監視対象装置の管理IFのIPアドレスに対して死活監視を行う方法である。

Q207 〔令和元年 午後I 問1 e〕

現行の監視方法の一つは、SNMPによって、各監視対象装置からの状態変更通知である**（e）**を受信する方法である。

Q208 〔令和元年 午後I 問1 f〕

現行の監視方法の一つは、SNMPによって、各監視対象装置から5分ごとに管理情報ベースである**（f）**を取得する方法である。

Q209 〔平成30年 午後I 問2 ア〕

ping監視には、RFC 792で規定されているプロトコルである**（ア）**を利用する。

Q210 〔平成30年 午後I 問2 ウ〕

SYSLOGは、トランスポートプロトコルとしてRFC 768で規定されている**（ウ）**を用いている。

Q211 〔平成30年 午後I 問2 エ〕

SNMPエージェントとSNMPマネージャは、同じグループであることを示す**（エ）**を用いて、機器の管理情報（以下、MIBという）を共有する。

Q212 〔平成29年 午後I 問3 オ・カ〕

ネットワーク監視にはpingを用いる。pingは、**（オ）**のecho requestパケットを監視対象に送り、**（カ）**パケットが監視対象から返ってくることで到達性を確認する。

Q213 〔平成28年 午後II 問1 サ〕

サービス停止時間とは、切替作業、切替作業後の動作確認及び問題発生時の**（サ）**に要する時間の合計である。

セキュリティ対策　6問

Q214　〔令和7年 午後I 問3 表2〕

> **表2**は、クラウド型のSWGサービスのセキュリティ機能（抜粋）である。各機能名を答えよ。

表2 SWG サービスのセキュリティ機能（抜粋）

機能名	機能概要
（1）	直接接続リストに登録したFQDN，IPアドレスを宛先とする通信は，SWG サービスを経由させずに直接通信させる機能
サイトブロック機能	拒否リストに登録したFQDN，IPアドレス又はURL を宛先とする通信をブロックする機能
（2）	接続先のドメインや IP アドレスの安全性を数値化し，指定したしきい値以上の安全性をもつ Web サイトだけに接続を許可する機能
マルウェア駆除機能	ダウンロード・アップロードファイルに対して，パターン検査及び隔離環境上で動作を観察・分析してマルウェアを駆除する機能

（機能名は、意味が一致していれば語形の違いは問わない）

Q215　〔令和4年 午後I 問3 オ〕

表1 FWの許可ルール

項番	アクセス経路	送信元	プロトコル/ポート番号
4	DMZ→インターネット	プロキシサーバ	TCP/80及びTCP/443

プロキシサーバがインターネット上の不特定のWebサーバにアクセスするので、宛先には（オ）を設定する。

Q216　〔令和元年 午後II 問2 a〕

FWのフィルタリング内容の調査結果について、N主任は「現在の設定で、（a）スキャンとポートスキャンには対応できているようだ」と述べた。

Q217　〔令和元年 午後II 問2 b〕

クローズのポート宛てにUDPパケットを送ると、RFC 792で規定された（b）パケットが送信元IPアドレス宛てに返送されるのを悪用し、サーバのリソースを消費させるUDPフラッド攻撃も、FWの設定で防げている。

Q218 〔令和元年 午後II 問2 イ・ウ・エ〕

SYNクッキー技術では、SYNパケットを受信する段階では、TCPコネクション確立のためのメモリ確保は行わない。パケット中の該当するコネクションに関連する情報などに、特別な演算によって計算した変換値をクッキーとして、TCPヘッダ中の**（イ）**番号に埋め込んで、通信の状態を監視する。SYNパケットの情報などを基に計算した値を、TCPヘッダ中のシーケンス番号にセットして、SYN/ACKパケットを返送する。受信したACKパケットの情報などを基に計算し、TCPヘッダ中の**（ウ）**番号の値が計算値に**（エ）**を加えた値と一致するかどうかをチェックする。一致したとき、メモリ確保を行い、サーバとの間でTCPコネクションを確立する。

Q219 〔平成30年 午後II 問1 エ〕

工場内の機器とX社内の機器との通信は、いずれもクライアントサーバ型の通信であり、機器間の**（エ）**コネクションの確立要求は、工場からX社の方向に行われる。

IoT

15問

Q220 〔令和7年 午後II 問2 a〕

IoT向けには、LPWA（Low Power Wide Area）と呼ばれる、低**（a）**電力の無線通信技術が利用される。

Q221 〔令和7年 午後II 問2 b・c〕

LPWAは、セルラー系と非セルラー系の二つに大別される。**（b）**系にはLoRaWAN、Sigfoxなどがあり、**（c）**系にはLTE-M、NB-IoTなどがある。

Q222 〔令和7年 午後II 問2 d・e〕

920MHz帯はWi-Fiが利用する周波数帯と同様に、**（d）**バンドと呼ばれる周波数帯であるが、2.4GHz帯と比べて電波**（e）**の影響が少ない。

Q223 〔令和7年 午後II 問2 f〕

LTE-M、NB-IoTは、**（f）**と呼ばれる標準化プロジェクトが作成した技術仕様を基に、通信事業者が全国規模で構築したLTE網でサービスが提供されている。

Q224 〔令和7年 午後II 問2 i〕

Gメーターには、通信事業者が契約者を識別する情報を記録している**（i）**カードを装着する。

Q225 〔令和7年 午後II 問2 j〕

条件：Gメーター1台当たり1回の検針時の通信量を100バイトとし、1時間ごとに検針を実施する。通信費は1か月の通信量1,000バイト当たり1円とし、Gメーターごとに割り当てる1回線当たりの基本料金は月額300円とする。1か月が30日の場合、Gメーター1台当たりの検針に必要な1か月の利用料は**（j）**円である。

Q226 〔令和7年 午後II 問2 k〕

CoAPは、Webシステムにおける API の形式である**（k）**アーキテクチャを採用しているので、Web技術でIoTシステムを構築する場合に適している。

Q227 〔令和7年 午後II 問2 l〕

CoAPは、**（l）**層のプロトコルであるUDP上での動作を前提としている。

Q228 〔令和7年 午後II 問2 m・n〕

通信品質の劣るネットワークなどでは、パケットが**（m）**で到着したり、**（n）**して出現したり、通知なしに消失したりすることがあるので、CoAPは、メッセージIDを利用することによって、送受信が正しく行われるための仕組みを実装している。

Q229 〔令和7年 午後II 問2 o〕

CoAPでは、ACKの受信を待たずに連続してCONを送信することができる、非**（o）**通信が行われる。

Q230 〔令和7年 午後II 問2 p〕

CoAPクライアントはCONを送信後、デフォルトのタイムアウト時間ACKの受信を待ち、ACKが受信できなかった場合は、指数**（p）**と呼ばれる方式で算出した時間経過後にCONを再送する。

Q231 〔令和7年 午後II 問2 表1〕

CoAPの通信では、要求の場合にメソッドコードを、応答の場合にレスポンスコードを用いる。

> **表1**はCoAPのメソッドコード（抜粋）である。各コードのメソッド名を答えよ。

表1 メソッドコード（抜粋）

コード	メソッド名	説明
0.01	**（1）**	指定したリソースを取得する。
0.02	**（2）**	指定したリソースを作成する。
0.04	**（3）**	指定したリソースを削除する。

Q232 〔令和7年 午後II 問2 表2〕

> **表2**はCoAPのレスポンスコード（抜粋）である。各コードの状態を答えよ。

表2 レスポンスコード（抜粋）

コード	状態	説明
2.01	（1）	リクエストが正常に処理され，指定したリソースが作成された。
2.02	（2）	リクエストが正常に処理され，指定したリソースが消去された。
2.05	（3）	リクエストが正常に処理され，指定したリソースが取得された。

Q233 〔平成30年 午後II 問1 表1〕

MQTTを使ったメッセージ交換方式では、固定ヘッダ、可変ヘッダ及びペイロードから構成されたMQTTコントロールパケットを使う。

> **表1**にMQTTコントロールパケットの種別（抜粋）を示す。各パケットの種別を答えよ。

表1 MQTTコントロールパケットの種別（抜粋）

種別	用途	固定ヘッダ，可変ヘッダ又はペイロードに含まれる情報
（1）	クライアントからサーバへの接続要求	（省略）
（2）	（3）に対する確認応答	（省略）
（4）	メッセージの送信	QoSレベル，トピック名，パケットID，メッセージ
（5）	メッセージ受信の通知	パケットID
（6）	メッセージリリースの通知	パケットID
（7）	メッセージ送信終了の通知	パケットID
（8）	クライアントからサーバへの購読要求	QoSレベル，トピック名，パケットID
（9）	（10）に対する確認応答	パケットID

Q234 〔平成30年 午後II 問1 オ〕

本文：『配信先となるクライアントは、サーバに（オ）を送信し、購読対象のメッセージを、トピック名を使って通知する。』デバイスDiも、あらかじめ同じメッセージを交換サーバに送信し、トピック名がconfig/DiのPUBLISHが送信されるようにする。