平成30年度 秋期 午前Ⅱ問題の解答・解説

□問 1	ウ	□問 11	イ	□問 21	イ
□問 2	ア	□問 12	イ	□問 22	エ
□問 3	ア	□問 13	イ	□問 23	イ
□問 4	ア	□問 14	エ	□問 24	ウ
□問 5	ア	□問 15	エ	□問 25	ア
□問 6	イ	□問 16	イ		
□問 7	イ	□問 17	ウ		
□問 8	イ	□問 18	イ		
□問 9	ウ	□問 19	ア		
□問 10	ア	□問 20	ウ		

問 1：正解ウ

OFDM（Orthogonal Frequency Division Multiplexing，直交周波数分割多重方式）とは，高速無線通信で使用されている多重化方式の一つである。キャリア（搬送波）を複数のサブキャリアに分割した上で，サブキャリアごとにデータ信号を変調させて伝送する。各サブキャリアは相互に干渉しないように配置されているため，狭い周波数帯域を効率的に利用した高速伝送を実現している。よって，正解は選択肢**ウ**である。

問 2：正解ア

複数のノードが伝送媒体を共有しているネットワークでは，複数のノードが同時にデータを送信すると信号が衝突して壊れてしまう。そこで CSMA 方式では，送信する前にキャリア信号の有無を検出する仕組みを採用している。キャリア信号を検出したら送信を控えることによって，衝突を未然に防ぐことができる。

なお，キャリア信号とは，媒体上を実際に伝播する信号である。物理層レベルでは，ノード間の通信はキャリア信号にデータを搬送することによって行われている。

ア：**正解**。CSMA 方式について適切に記述している。
イ：トークンパッシング方式について記述したものである。
ウ：「直ちに」ではなく，ランダム時間が経過してから再送を行う。
エ：複数のノードが同時にデータを送信すると，信号が衝突して壊れてしまう。したがって，伝送路が使用中のときに送信はできない。ただし，（選択肢エでは明記されていないが）この「伝送路」は複数のノード間で共有されているものとする。

問 3：正解ア

ア：**正解**。アドミッション制御について適切に記述している。
イ：シェーピングではなく，ポリシングについて記述したものである。TCP で通信しているとき，途中経路でパケットが破棄されると TCP の輻輳制御が働くため，輻輳が生じない程度までトラフィックの出力レートが調整される。
ウ：ポリシングではなく，シェーピングについて記述したものである。最大速度を超過したパケットはバッファにいったん蓄えられ，後から送信される。そのため，大幅な遅延が許されない音声通信には不向きである。なお，バッファの容量を超えてしまうとパケットは破棄される。

エ：ベストエフォートではなく，優先制御について記述したものである。フレームの種類や宛先に応じてクラス分けを行い，クラスごとに設けられたキュー（待ち行列）に配置する。それぞれのキューには異なる優先度が割り当てられており，これは優先キューと呼ばれる。優先キューからフレームを取り出す処理のことをスケジューリングといい，様々な方式がある。

問 4：正解ア

MTU（Max Transmission Unit，最大転送単位）は，パケットのペイロード部分の最大長である。

本問はイーサネットパケットの MTU が問われているので，ペイロード部分は IP ヘッダからデータまでとなる。

よって，正解は選択肢**ア**となる。

問 5：正解ア

BGP は，AS（Autonomous System，自律システム）間を接続するルーティングプロトコルである。よって，正解は選択肢**ア**である。

他の選択肢は，いずれも AS 内で使用されるルーティングプロトコルである。

問 6：正解イ

問題文には，「送付されるパケットの宛先 IP アドレスである端末 C の IP アドレスと，端末 C の MAC アドレスとを対応付けるのはどの機器か」と記述されている。

IP アドレスと MAC アドレスを対応付ける機器は，ARP 要求を送信する IP ノードである。その目標アドレスについて，問題文は「送付されるパケットの宛先 IP アドレスである端末 C の IP アドレス」と述べている。したがって，目標アドレスは IP パケットの宛先であることが分かる。

要するに，本問が問うているのは，

- 送付 IP パケットの宛先 IP アドレスを目標とする ARP 要求を送信する IP ノードはどれか？

ということである。

この ARP 要求で解決される MAC アドレスは，宛先 IP ノード自身のものとなる。つまり，当該 IP パケットを格納したイーサネットフレームを受信する IP ノードは，宛先自身となる。

一般的に言って，送付 IP パケットを格納したイーサネットフレームに関し，送付 IP パケットの宛先 IP アドレスが指す IP ノードと，送付イーサネットフレームの宛先 MAC アドレスが指す IP ノードとを照らし合わせたとき，両者が一致する条件は，次のとおりである。

［送付イーサネットフレームの宛先 IP ノード］
　送付 IP パケットの宛先自身であること
［送付イーサネットフレームの送信元 IP ノード］
　宛先 IP ノードと同一サブネットに存在すること

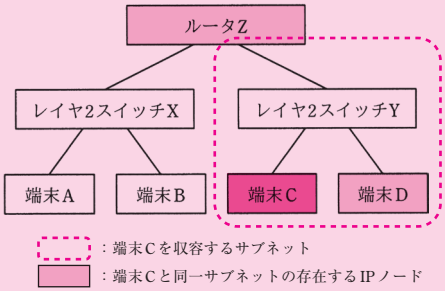
このイーサネットの宛先 MAC アドレスは，宛先の IP アドレスを目標とする ARP パケットにより得られたものである。ARP パケットをやり取りする IP ノードは次のとおりである。

［送付 IP パケットの宛先 IP アドレスを目標とする ARP 要求を送信する IP ノード］
　送付イーサネットフレームの送信元 IP ノード

ARP 応答を返信する IP ノードは，言うまでもないが，ARP 要求の目標アドレスで指定された IP ノード，すなわち，送付イーサネットフレームの宛先 IP ノード自身である。

したがって，「送付されるパケットの宛先 IP アドレスである端末 C の IP アドレスと，端末 C の MAC アドレスとを対応付ける機器」（送付 IP パケットの宛先 IP アドレスを目標とする ARP 要求を送信する IP ノード）は，送付イーサネットフレームの送信元 IP ノードであり，宛先である端末 C と同一サブネットに存在している。

問題文の図を見ると，これに該当する IP ノードは，ルータ Z，端末 D のいずれかである。



図：端末 C と同一サブネットに存在する IP ノード

二つの IP ノードのうち，本問の選択肢に列挙されているのは，ルータ Z である。

よって，正解は選択肢**イ**である。

ARP（プロキシ ARP を含む）について，詳しくは本書の第 3 章「3.4　ARP」を参照していただきたい。

●ルータ Z にプロキシ ARP が設定されている場合，どうなるか？

問題文には，「ルータ Z においてプロキシ ARP は設定されていないものとする」とある。もしもこの条件に反し，次に示すプロキシ ARP がルータ Z に設定されていたら，どうなるだろうか？

［プロキシ ARP を設定するインタフェース］
　端末 A を収容しているサブネットのインタフェース
［プロキシ ARP の設定］
　目標アドレスが端末 C である ARP 要求に対し，前記インタフェースの MAC アドレスを応答する。

さらに，端末 A から見て端末 C が同一サブネットに存在するように見せかけるため，端末 A のサブネットマスクの設定を調整したとしよう。

つまり，この調整によって，端末 A を収容している（と見せかけている）サブネットは，端末 A を実際に収容するサブネットと端末 C を実際に収容するサブネットを集約したものとなる。

このとき，端末 A は端末 C に直接 IP パケットを転送するので，端末 C の IP アドレスを目標とする ARP 要求を送信する。

前述のプロキシ ARP がルータ Z に設定されていれば，この ARP 要求にルータ Z が応答するので，送付 IP パケットを格納するイーサネットフレームが送信される。これを受け取ったルータ Z は，通常どおり，本問で解説したように ARP のやり取りを行った後，端末 C に送付 IP パケットを転送する。

つまり，ルータ Z にプロキシ ARP が設定されている場合，（かつ，端末 A から見て端末 C が同一サブネットに存在するようにサブネットマスクが調整されている場合，）選択肢ア「端末 A」と選択肢イ「ルータ Z」の二つが正解になってしまうのだ。

プロキシ ARP に関する問題文の記述は，このような別解が生じないように設定されたのである。

問 7：正解イ

DNS でのホスト名と IP アドレスの対応付けは，選択肢イに記述されているとおり，多対多である。よって，正解は選択肢**イ**である。

ホスト名と IP アドレスの対応付けは A レコードに登録する。一つのホスト名に複数の IP アドレスを対応させたい場合，及び，複数のホスト名に一つの IP アドレスを対応させたい場合は，それぞれ次の図に示すように指定する。なお，一つのホスト名に複数の IP アドレスを対応させた場合，名前解決時にラウンドロビンされる。

〔一つのホスト名に複数の IP アドレスを対応させる例〕

hostA	IN	A	192.0.2.1
hostA	IN	A	192.0.2.2
hostA	IN	A	192.0.2.3

名前解決時にラウンドロビンされる

〔複数のホスト名に一つの IP アドレスを対応させる例〕

hostB	IN	A	192.0.2.4
hostC	IN	A	192.0.2.4
hostD	IN	A	192.0.2.4

図：A レコードの登録例

問 8：正解イ

IGMP（Internet Group Management Protocol）は，IP ネットワークでマルチキャスト通信を行うために，ルータとホストが使用するプロトコルである。ホストは，マルチキャストグループへの参加や離脱を通知するために，IGMP メッセージを送信する。ルータは，マルチキャストグループに参加しているホストの存否を定期的に（デフォルトで 60 秒間隔）チェックするために使用する。よって，正解は選択肢**イ**となる。

ア：ICMP（Internet Control Message Protocol）は，IP の上位階層のプロトコルである。ICMP は，アプリケーションのデータをペイロードにもつプロトコルではなく，IP ネットワークの制御のために使用されるプロトコルである。例えば，IP パケットの転送エラーを送信元ノードに通知する機能や，接続性を確認するエコー要求／応答メッセージを転送する機能をもつ。

ウ：RTP（Real-time Transport Protocol）は，音声や映像などリアルタイム性のあるデータをストリーミング配信する仕組みを備えたプロトコルである。

エ：SDP（Session Description Protocol）は，リアルタイム通信のメディア（音声，動画，

等）の種類とその符号化方式，リアルタイム通信に用いるプロトコルとそのポート番号，端末の IP アドレス，等の情報を記述する方法を規定したものである。リアルタイム通信を行うアプリケーションは，リアルタイム通信に先立ち，SIP（Session Initiation Protocol）のやり取りを通じてセッションを確立する。その確立時に，SDP で記述された情報交換を行う。

問 9：正解ウ

LDAP（Lightweight Directory Access Protocol）は，ITU-T 勧告である X.500 を簡略化して RFC2251 で規定された，ディレクトリサービスを実現するプロトコルである。

ディレクトリサービスとは，資源とその属性を登録し検索できるようにしたシステムである。各資源は，DNS のドメインに似たツリー構造で管理されている。

したがって，選択肢**ウ**にあるとおり，LDAP は「ディレクトリツリーへのアクセス手順や，データ交換フォーマットが規定されている」と言える。よってこれが正解である。

ア：LDAP は X.500 を簡略化したものである。したがって，「X.500 シリーズに機能を追加して作成され，X.500 シリーズのプロトコルを包含している」という記述は誤りである。

イ：LDAP は，個々の組織が自分たちのリソースを一元的に管理するために使用されている。世界中のあらゆる組織のリソースを一元的に管理したディレクトリツリーは存在していない。したがって，「インターネット上の LDAP サーバの最上位サーバ」が存在しているわけではないため，誤りである。

なお，問題文にある「ルート DSE」（ルート DSA Specific Entry）とは，ディレクトリツリーのルートにあるエントリであり，LDAP サーバ固有の情報が登録されている。

エ：LDAP は，トランスポート層として TCP を使用する。したがって，「TCP は使わず UDP によって通信」という記述は誤りである。

問 10：正解ア

サブネットマスクが FFFFFF80 であるとき，サブネット長は 25 ビットである。したがって，ホストアドレス部のビット長は，7 ビットとなる。

ホストアドレス部のビットパターン数は 2 の 7 乗，すなわち 128 個ある。このうち，全ビットが 0 のものはネットワークアドレスとして，全ビットが 1 のものはブロードキャストアド

レスとして予約されているため，これら 2 個はホストに割り当てることができない。

したがって，利用可能なホスト数の最大値は，

128 − 2 = 126

となる。よって，正解は選択肢**ア**である。

問 11：正解イ

マルチキャストアドレスブロックは，アドレスの上位 4 ビットが「1110」，すなわち，通常表記で 224.0.0.0 ～ 239.255.255.255 の範囲内のものである。これは，クラス D のアドレスに相当する。よって，正解は選択肢**イ**となる。

ア：マルチキャストアドレスブロックには，アドホックブロックが割り当てられている。これは，あらかじめ用途を固定するのが適さないアプリケーション用のマルチキャスト通信に使用される。

ウ：マルチキャストパケットも，ユニキャストパケットと同様に，TTL の値が 0 になったら破棄される。

エ：マルチキャスト通信は，送信元と宛先が 1 対多となる形態の通信である。その宛先は，ネットワーク上の全てのホストが対象となることもあれば，そうではないこともある。

マルチキャストパケットを受信したホストは，宛先 IP アドレスに指定されたマルチキャストアドレスに基づき，自ホストがこのパケットを受け取る対象に含まれているか否かを判断する。この判断はインターネット層（IP）で行われる。

受け取る対象であれば，IP パケットのペイロードを上位層に渡す。そうでなければ，IP パケットを廃棄する。

問 12：正解イ

ア：Bluetooth は，半径 10 ～ 20m 以内のパーソナルエリアをターゲットにした無線 PAN（Personal Area Network）の通信規格の一つであり，IEEE802.15.1 で標準化されている。無線通信に使用する周波数帯域は，2.4GHz 帯である。

イ：**正解**。IEEE802.11ac は，無線 LAN の通信規格の一つである。無線通信に使用する周波数帯域は，5GHz 帯である。

ウ，エ：IEEE802.11b 及び 11g は，無線 LAN の通信規格の一つである。無線通信に使用する周波数帯域は，どちらも 2.4GHz 帯である。

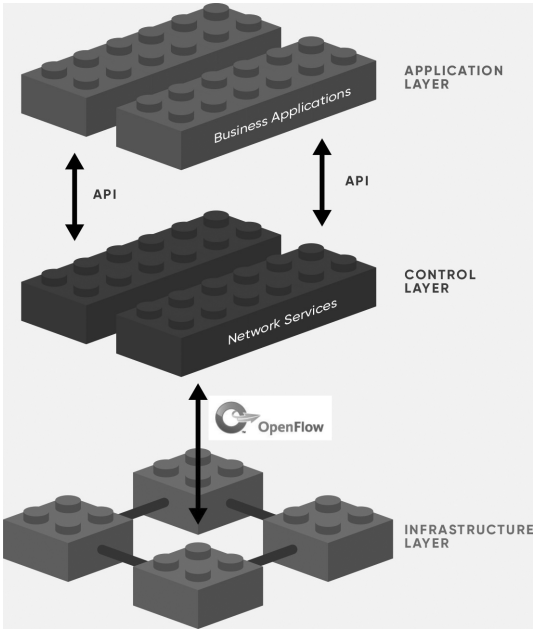
無線 LAN の通信規格について，詳しくは本書の第 1 章「1.3.1　無線 LAN の種類と仕様」を参照していただきたい。

問 13：正解イ

SDN（Software-Defined Networking）は，ネットワーク機器の機能をソフトウェアで定義できるようにした技術や規格である。

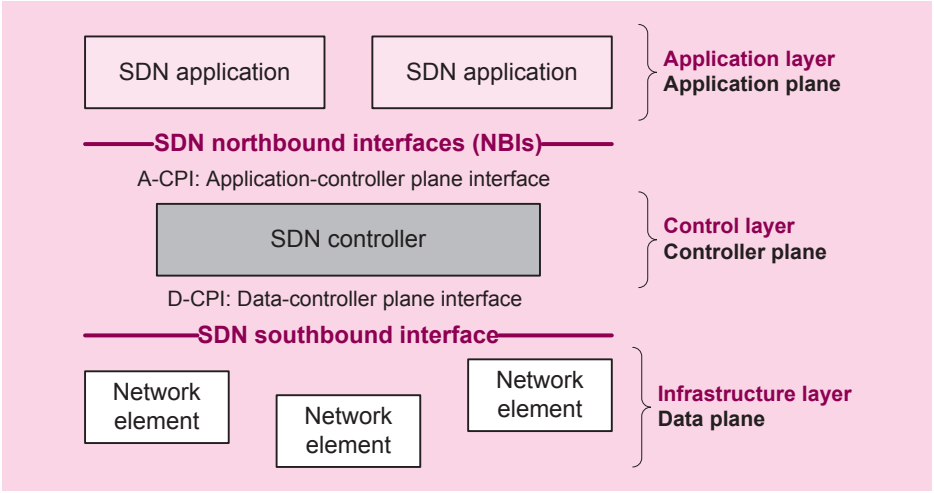
従来のネットワーク機器を，経路制御などの管理機能を実行するコントローラと，データ転送を行うネットワーク機器に分け，パケットの経路制御をコントローラが集中制御する方式を採用している。コントローラとネットワーク機器は，制御用のネットワークで接続されている。

SDN 技術の中で標準化が進んでいるものが，OpenFlow である。OpenFlow の標準化団体である ONF（Open Networking Foundation）が定めた，SDN の定義及び構成要素を示す。



図は下記より引用：
「Software-Defined Networking（SDN）Definition」
https://www.opennetworking.org/sdn-definition/

図：SDN の定義



図は右記より引用：「SDN architecture Issue1 June, 2014 ONF TR-502」
https://www.opennetworking.org/wp-content/uploads/2013/02/TR_SDN_ARCH_1.0_06062014.pdf

注）SDN architecture の最新版は Issue1.1 である。ここに引用した図は旧版の Issue1 の方だが，本問で問われている知識の範囲においては，Issue1 を用いても差し支えがない。ここでは大要をつかめば十分であるため，解説の都合上，より明瞭な図を掲載している Issue1 を引用した次第である。

図：SDN の構成要素

図「SDN の定義」を見ると，OpenFlow は，コントロール層とインフラストラクチャ層間の通信規約であることが分かる。図「SDN の構成要素」を見ると，コントロール層の構成要素が「コントローラ」（SDN controller）であり，インフラストラクチャ層の構成要素が「ネットワーク機器」（Network element）である。つまり端的に言うと，OpenFlow とは，コントローラとネットワーク機器間の通信を標準化したプロトコルである。

OpenFlow は，コントローラがスイッチの経路制御動作を集中制御する方法として，次の 2 種類を定めている。

1. ネットワーク機器は，パケット受信を契機に，コントローラからの指示を仰ぐために当該パケットをコントローラに転送する。その後，コントローラは当該パケットに応じたコマンドを送り，経路制御の動作をネットワーク機器に指示する。
2. 通信に先立ち，コントローラは，ネットワーク機器が行う経路制御の動作を登録しておく。

したがって，選択肢**イ**にあるとおり，OpenFlow を用いたネットワークでは，「ネットワーク機器がデータ転送を行うための情報はコントローラから提供される」と言える。よってこれが正解である。

ア：OpenFlow は，コントローラとネットワーク機器のやり取りを標準化したプロトコルである。
ウ：図「SDN の構成要素」に示したとおり，アプリケーションは，A-CPI（Application-Controller Plane Interface）を通じて，コントローラに指示を出す。
エ：図「SDN の構成要素」に示したとおり，アプリケーションはコントローラとやり取りし，コントローラはネットワーク機器とやり取りする。したがって，アプリケーションはネットワーク機器に直接指示を出さない。

問 14：正解エ

URL 表記でポート番号を決定する要素は，優先順位の高い順に次の二つである。

1. 明示的に指定されたポート番号（省略可）
2. スキーム

明示的にポート番号を指定するには，コンピュータ名（ホスト名又は IP アドレス）の直後にコロン「:」を置き，それに続けてポート番号を記述する。スキームとは，ページを取得する手段のことであり，URL の先頭に置かれる（「://」より前の部分）。ポート番号を明示的に指定しないとき，スキームごとに規定されたポート番号が採用される。

なお，ホスト名やクエリストリングは，ポート番号を決定する要素ではない。

さて，出題された URL は，次のように記述されている。

https://ftp.example.jp/index.cgi?port=123

URL が「https://」から始まっているので，スキームは「https」であり，ブラウザは SSL 通信を行う。ポート番号が直接指定されていないため，ポート番号はスキームのデフォルト値となる。したがって，SSL 通信のポート番号である 443 ポートで通信する。よって，正解は選択肢**エ**となる。

参考までに，出題された URL で 8080 ポートを明示的に指定したいときは，次のように記述すればよい。

https://ftp.example.jp:8080/index.cgi?port=123

前述のとおり，明示的に指定されたポート番号は，スキーム「https」のデフォルト値よりも優先順位が高い。したがって，コンピュータ「ftp.example.jp」に 8080 ポートで通信する。

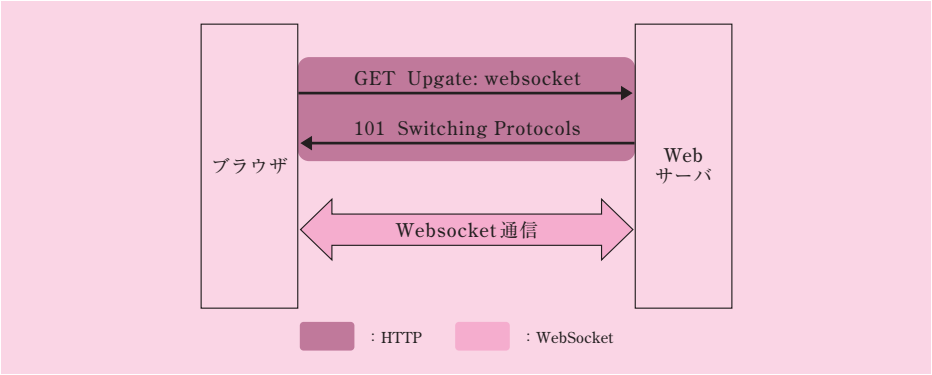
問 15：正解エ

WebSocket は，Web コンピューティングにおける双方向のプッシュ配信を実現する技術である。プロトコルの規格は IETF が策定し，RFC6455 で標準化されている。API の規格は W3C が策定しており，これを受けてクライアント側（主要ブラウザの JavaScript），サーバ側（Java EE，PHP，Node.js など）の双方で，WebSocket の実装が普及している。

WebSocket は，プッシュ配信に先立ち，既存の HTTP 通信（GET メソッド）を用いて，クライアントがサーバに WebSocket 通信の開始を要求する。より正確に言うと，この HTTP 通信を WebSocket 通信に切り替えることを要求する。

次いで，サーバがこの要求を受理した旨（ステータスコード：101）を応答する。その後，WebSocket による双方向通信が行われる仕組みになっている。

よって，正解は選択肢**エ**となる。



図：HTTP 通信から WebSocket 通信への切替

なお，HTTP 通信から WebSocket 通信への切替えはアプリケーション層で行われているものなので，トランスポート層以下の通信が切り替わることはない。つまり，ポート番号と IP アドレスは，HTTP 通信のものをそのまま引き継いでいる。

問 16：正解イ

ICMP 通信はデータグラム型通信（コネクションレス型通信）なので，送信元 IP アドレスを詐称した通信が可能である。これを悪用した攻撃に，ICMP Flood 攻撃がある。

攻撃者は，送信元 IP アドレスを偽装した上で，標的ノードに ICMP echo 要求パケットを送信する。この偽装された ICMP echo 要求は，例えば，自ホストの IP アドレスを偽装した上で ping コマンドを投入すれば，発行することができる。

標的ノードは，これを受信すると，ICMP echo 応答パケットを送信元に返信する。標的ノードのネットワーク回線は，要求パケット及び応答パケットの通信のためにネットワーク帯域を無駄に消費させられる。

ICMP Flood 攻撃とは，このような ICMP パケットを大量に送り付けることによって，サービス妨害をもたらす攻撃である。

なお，攻撃者のネットワーク帯域も ICMP echo 要求パケットを送信する分だけ消費することになるが，ボットネット上の複数の攻撃元から分散型 DoS 攻撃を仕掛けることにより，個々の攻撃元の帯域消費を抑えることが可能である。

よって，正解は選択肢**イ**である。

ア：HTTP GET フラッド攻撃に関する説明である。これは，大量の HTTP GET パケットを利用した DoS 攻撃である。

ウ：SYN フラッド攻撃に関する説明である。これは，大量の TCP コネクションをハーフオープン状態にしたままにすることにより，正当な TCP コネクションの確立を阻害したり，リソースが枯渇したりすることをねらった DoS 攻撃である。

エ：Connection Exhaustion 攻撃に関する説明である。これは，大量の TCP コネクションを確立・維持させることにより，正当な TCP コネクションの確立を阻害したり，リソースが枯渇したりすることをねらった DoS 攻撃である。

問 17：正解ウ

ア：EAP-FAST（Flexible Authentication via Secure Tunneling）は，Cisco Systems 社が仕様を定め，RFC4851 で標準化された EAP 認証の方式である。EAP-FAST は，ディジタル証明書を用いない TLS 通信を使用することができる。ディジタル署名の代わりに，同社の独自仕様である PAC（Protected Access Credential）と呼ばれる情報に基づく認証を行う。

イ：EAP-MD5 は，チャレンジレスポンス方式を用いたワンタイムパスワードに基づく

クライアント認証を行う。なお，EAP の当初の標準である RFC3748 に規定されていたが，今日では MD5 が安全ではないため，使用すべきではない。

ウ：**正解**。EAP-TLS は，RFC5261 で標準化された EAP 認証の方式である。EAP-TLS は，TLS 通信を用いて，ディジタル証明書に基づくサーバ認証及びクライアント認証を行う。

エ：EAP-TTLS（Tunneled TLS）は，Funk Software 社，Certicom 社が共同で仕様を定めた EAP 認証の方式である。EAP-TTLS は，TLS 通信を用いて，ディジタル証明書に基づくサーバ認証を行う。TLS で暗号化された安全な通信を確立した後，パスワードに基づくクライアント認証を行う。

問 18：正解イ

ア：Content-Security-Policy レスポンスヘッダは，意図しないコンテンツの読込みを防止する目的で使用される。具体的に言うと，同ヘッダには，ブラウザにコンテンツを提供する URI，ブラウザに提供するコンテンツの種類などを指定する。

クロスサイトスクリプティング攻撃（XSS 攻撃）は，攻撃者が用意したスクリプト（すなわち，Web サイトが意図したものではないスクリプト）をブラウザ上で実行させることをねらっている。それゆえ，同ヘッダでコンテンツをきめ細かく指定することで，この攻撃を防ぐ効果が得られる。

イ：**正解**。Strict-Transport-Security レスポンスヘッダは，Web ブラウザに対して，当該 Web サイトへのアクセスを HTTPS で行うように指示するために使用される。

ウ：X-Content-Type-Options レスポンスヘッダは，ブラウザのコンテンツ処理を制御するために使用される。X-Content-Type-Options レスポンスヘッダの値を「nosniff」に指定すれば，Content-Type レスポンスヘッダに指定されたメディアタイプどおり忠実に処理するよう，ブラウザに指示することができる。

X-Content-Type-Options レスポンスヘッダが必要になった理由は，Windows 8.1 まで標準装備されていたブラウザ Internet Explorer（IE）がコンテンツの内容を適宜解釈して表示しており（すなわち，Content-Type ヘッダを軽視しており），これを悪用する攻撃が行われるようになったためである。その対策として，X-Content-Type-Options レスポンスヘッダで「nosniff」に指定するようになった。

さらに，IE 以外のブラウザ（Chrome，Firefox 等）でも，JSON や JSONP が普及し始めた頃，Content-Type レスポンスヘッダを不適切に設定することでコンテンツの処理に問題が生じることがあり，これを悪用する攻撃が問題視されたことがあった。その対策として，Content-Type レスポンスヘッダを厳格に指定するとと

もに，ブラウザがこれに忠実に従うよう，X-Content-Type-Options レスポンスヘッダで「nosniff」に指定するようになった。

エ：X-XSS-Protection レスポンスヘッダは，ブラウザが装備する XSS 攻撃フィルタ機能の有効化／無効化を制御するために使用する。XSS 攻撃フィルタとは，ブラウザが XSS 攻撃を検知した際，コンテンツの表示を停止する機能である。通常，この機能を有効化するため，X-XSS-Protection レスポンスヘッダの値を「1; mode=block」に指定する。

問 19：正解ア

ア：**正解**。IPsec の通信モードをトンネルモードに指定すると，元の IP パケット全体をカプセル化することができる。さらに，IPsec プロトコルを ESP に指定すると，IPsec でカプセル化する際，暗号化することができる。

イ：IKE はポート番号 500 を用いる。なお，「IKE は IPsec の鍵交換のためのプロトコルであ（る）」という記述は正しい。

ウ：HMAC-SHA1 は，暗号化のアルゴリズムではなく，メッセージ認証のアルゴリズムである。

エ：IPsec の通信に先立ち，メッセージ認証や暗号化のアルゴリズムを決定するのに用いられるプロトコルは，IKE である。

問 20：正解ウ

ア：Web サーバのディジタル証明書には，通常，Web サーバのホスト名（FQDN）が記載されている。IP アドレスの記載は必須ではないため，Web サーバの IP アドレスを変更しても，ディジタル証明書を再度取得する必要はない。

イ：TLS で使用する共通鍵の長さは，128 ビット以上の値を指定できる。

ウ：**正解**。ディジタル証明書は IC カードに格納でき，利用する PC を特定の PC に限定する必要はない。

エ：TLS は，サーバから要求したときだけ，クライアント認証を行う仕様になっている。このクライアント認証にはディジタル証明書を用いるが，ごく一般的なインターネットの利用者は，自らを認証する用途でディジタル証明書を認証局から取得してはいない。それゆえ，インターネット上で不特定多数のクライアントからアクセスを受け付ける Web サーバは，TLS のクライアント認証を行わない。

したがって，選択肢にある「TLS は Web サーバと特定の利用者が通信するための

プロトコル」「Web サーバへの事前の利用者登録が不可欠」という記述は誤りである。

問 21：正解イ

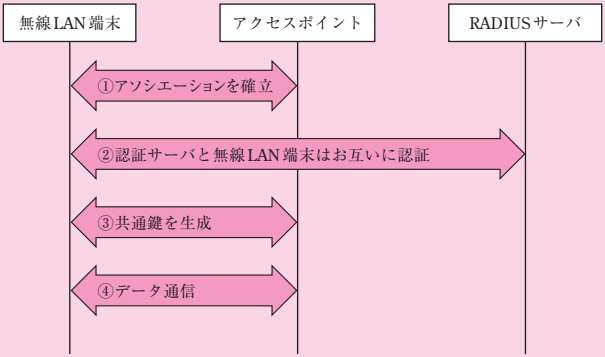
本問は，利用者認証とアクセス制御に IEEE802.1X と RADIUS を使用する場合の実装方法を問うている。まず，IEEE802.1X と RADIUS を使用したときの，認証とアクセス制御のシーケンスについて解説する。次いで，解を導こう。

●認証とアクセス制御のシーケンス

無線 LAN 環境で IEEE802.1X 認証を導入すると，認証に成功した端末だけが，アクセスポイントを経由したデータ通信を行えるようになる。

IEEE802.1X と RADIUS を使用したときの，認証とアクセス制御の一般的なシーケンスは，おおよそ次のとおりである。

① 無線 LAN 端末とアクセスポイントの間でアソシエーションが確立される。
② RADIUS サーバと無線 LAN 端末はお互いに認証する。アクセスポイントは，両者のやり取りを中継する。
③ 認証に成功すると，アクセスポイントは，無線 LAN 端末との間で共通鍵を生成する。
④ 無線 LAN 端末は，アクセスポイントを経由したデータ通信を行う。その際，③で生成した共通鍵で通信を暗号化する。



図：IEEE802.1X 認証の動作シーケンス

ここで，IEEE802.1X 認証の処理が行われているのは，項番②である。

なお，共通鍵を生成する処理である項番③は，本問で問われているわけではないが，参考までに掲載した。無線 LAN のセキュリティの規格である IEEE802.11i は，認証（項番②）と暗号化（項番③）を規定している。IEEE802.1X 認証を導入するときは暗号化も含めて IEEE802.11i に対応するのが一般的である。

IEEE802.1X 認証を利用しない場合（より正確に言うと，IEEE802.11i に対応しない場合），項番①でアソシエーションを確立したら，すぐに項番④で通信を行える状態になる。

●解の導出

項番②の処理を行うには，アクセスポイントが，IEEE802.1X 認証に対応した機能をもっていなければならない。この機能を実装した機器のことを，IEEE802.1X 規格の用語で「オーセンティケータ」と呼ぶ。オーセンティケータがもつべき機能には，項番②のやり取りを中継すること，認証が成功するまでは項番④の通信を許可しないこと，などがある。

さらに，項番②の処理を行うには，オーセンティケータが，RADIUS クライアントの機能をもっていなければならない。

よって，正解は選択肢**イ**となる。

IEEE802.1X について，詳しくは本書の第 8 章「8.4.3　IEEE802.1X」を参照していただきたい。

問 22：正解エ

ア：イーサネットのフロー制御に関する説明である。全二重通信では IEEE802.3x の PAUSE フレームが，半二重通信ではバックプレッシャが，それぞれ用いられる。

イ：イーサネットのオートネゴシエーションに関する説明である。

ウ：NIC チーミングは，選択肢ウに述べられているような，1 枚の物理 NIC を複数の論理 NIC としてエミュレートする技術ではない。これは，複数の物理 NIC を論理的に 1 枚の論理 NIC として動作させる技術である。

エ：**正解**。NIC チーミングは，複数の物理 NIC を論理的に 1 枚の NIC として動作させる技術である。この論理的な NIC に一つの IP アドレスを割り当てる。物理的には複数の物理 NIC から構成されているので，物理 NIC にパケットを振り分けて負荷を分散したり，複数ある物理 NIC のどれかに障害が発生しても残りの物理 NIC がある限り論理 NIC としての動作を継続させたりすることができる。

問 23：正解イ

問題文に記述されているとおり，性能 P は，次の式で表される。

$$P = \frac{n}{1+(n-1)a}$$

右辺の分母と分子を n で通分すると，次の式のようになる。

$$P = \frac{1}{\frac{1}{n}+\left(\frac{n-1}{n}\right)a}$$

ここで，n を大きくすると，「$1 \diagup n$」の値が 0 に近づき，「$(n-1) \diagup n$」の値が 1 に近づく。つまり，次の式で近似できる。

$$P = \frac{1}{a}$$

問題文には，「$a = 0.1$」とあるので，これを代入すると P の値は 10 となる。よって，正解は選択肢**イ**となる。

問 24：正解ウ

「全国に分散しているシステム」という観点から解を導く。保守センタを 1 か所集中にすると遠隔保守を行う必要があり，発生した故障の種類によっては保守要員が現地に移動しなければならない。保守センタを分散配置した場合に比べると，その移動にかかる時間が MTTR を長くする。よって，正解は選択肢**ウ**である。

ア，イ：事後保守（故障発生時の保守）の成否は MTTR の長短に直結している。しかし，MTBF とは直接関係がない。

エ：予防保守を実施することによって MTBF を短くすることができる。しかし，MTTR とは直接関係がない。

問 25：正解ア

リファクタリングとは，プログラムの外部から見た振る舞いを変更することなく，内部の

変数名や構造を変更する技術である。リファクタリングによって，プログラムの機能を保ったまま，保守性や性能など他の品質を高めることができる。よって，正解は選択肢**ア**である。