

# 問題

問 1

正解

完璧



直前  
CHECK

ZigBeeの特徴はどれか。

- ア 2.4GHz帯を使用する無線通信方式であり、一つのマスタと最大七つのスレーブからなるスター型ネットワークを構成する。
- イ 5.8GHz帯を使用する近距離の無線技術であり、有料道路の料金所のETCなどで利用されている。
- ウ 下位層にIEEE 802.15.4を使用する低消費電力の無線通信方式であり、センサネットワークへの応用が進められている。
- エ 広い周波数帯にデータを拡散することで高速な伝送を行う無線通信方式であり、近距離での映像や音楽配信などへの応用が検討されている。

問 2

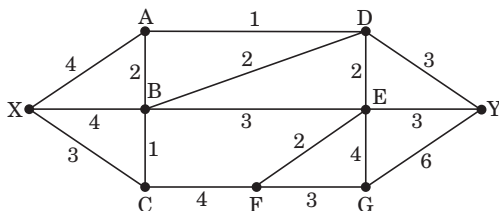
正解

完璧



直前  
CHECK

図のネットワークで、数字は二つの地点間で同時に使用できる論理回線の多重度を示している。X地点からY地点までには同時に最大幾つの論理回線を使用することができるか。



ア 8

イ 9

ウ 10

エ 11

問 3

正解

完璧



直前  
CHECK

高速無線通信で使われている多重化方式で、データ信号を複数のサブキャリアに分割し、各サブキャリアが互いに干渉しないように配置する方式はどれか。

ア CCK

イ CDM

ウ OFDM

エ TDM



## 問 1

ウ

**ZigBee**は、低コスト・低消費電力なワイヤレスセンサネットワーク構築に適した無線PAN (Personal Area Network) の規格である。無数のセンサを必要とするシステムではそのセンサへの配線コストが無視できなくなるので、無線接続しようとするものがZigBeeである。ZigBeeは、低伝送速度の無線PANの規格であるIEEE 802.15.4を用いている。

ア：**Bluetooth**に関する記述である。

イ：**DSRC** (Dedicated Short Range Communication：専用狭域通信)に関する記述である。

エ：直接スペクトラム拡散方式の近距離無線伝送技術には**UWB** (Ultra Wide Band)が考えられる。



## 問 2

ウ

経路を次の四つの部分に分けて考え、それぞれの部分の回線数の合計を示す。

- ・最初の区間： $X \rightarrow A=4$ ,  $X \rightarrow B=4$ ,  $X \rightarrow C=3$ ・・・合計11回線
- ・中間の左部分： $A \rightarrow D=1$ ,  $B \rightarrow D=2$ ,  $B \rightarrow E=3$ ,  $C \rightarrow F=4$ ・・・合計10回線
- ・中間の右部分： $A \rightarrow D=1$ ,  $B \rightarrow D=2$ ,  $B \rightarrow E=3$ ,  $F \rightarrow E=2$ ,  $F \rightarrow G=3$ ・・・合計11回線
- ・最後の区間： $D \rightarrow Y=3$ ,  $E \rightarrow Y=3$ ,  $G \rightarrow Y=6$ ・・・合計12回線

使用できる最大の論理回線数はボトルネック、すなわち全区間で最も回線数の少ない区間に制約される。

したがって、使用できる最大の論理回線数は10回線となることがわかる。各地点の回線の「入り」と「出」を確認すると、10回線確保できることが検証できる。もし、 $A \rightarrow B$ 間が1回線なら、全体では9回線となる。



## 問 3

ウ

**CCK** (Complementary Code Keying, 相補符号変調)：コンプリメンタリコード (相補符号)を用いて**DQPSK** (差動4相位相変調) 信号を拡散する方式である。

**CDM** (Code Division Multiplex, 符号分割多重化)：拡散符号を各情報に割り当てて、スペクトル拡散変調する方式である。

**OFDM** (Orthogonal Frequency Division Multiplexing, 直交波周波数分割多重)：データを直交したサブキャリアに乗せることで、密に並べても互いに干渉しない多重化方式である。

**TDM** (Time Division Multiplex, 時分割多重化)：時分割した固定スロットをそれぞれの情報に割り当てる方式である。

# 問題

問 4

正解

完璧



直前  
CHECK

LANに関する記述のうち、1000BASE-Tを説明したものはどれか。

- ア 2対のUTPケーブルを使用し、最大距離は100mである。
- イ 4対のUTPケーブルを使用し、最大距離は100mである。
- ウ シングルモード光ファイバケーブルを使用し、最大距離は5kmである。
- エ マルチモード光ファイバケーブルを使用し、最大距離は400mである。

問 5

正解

完璧



直前  
CHECK

無線LANで使用される搬送波感知多重アクセス／衝突回避方式はどれか。

- ア CDMA      イ CSMA/CA      ウ CSMA/CD      エ FDMA

問 6

正解

完璧



直前  
CHECK

FDDIにおける送信権制御に関する記述として、適切なものはどれか。

- ア 各ノードは、他ノードが伝送媒体に送信した信号の有無を調べ、信号がなければ送信を行う。これによって、送信競合の頻度を低減する。
- イ トークンと呼ばれる特殊な電文をノードからノードへ巡回させ、送信要求のあるノードは、トークンを受信したときに送信権を得る。
- ウ マスタコントローラは、各ノードから送信メッセージを受け取り、あて先に中継することによって、送信競合を防ぐ。
- エ マスタコントローラは、各ノードに送信要求の有無を問い合わせ、送信要求のあるノードに送信権を与える。

**問4****イ**

- ア：2対のUTPケーブルを使用するのは10BASE-Tである。  
イ：1000BASE-Tは4対のUTPケーブルを使用し、伝送最大距離は100mである。  
ウ：シングルモード光ファイバケーブルを使用し、伝送最大距離が5kmとなるものは、1000BASE-LXである。  
エ：1000BASE-Tでは、エンハンストカテゴリ5以上のUTPケーブルを使用する。

**問5****イ**

搬送波感知多重アクセス/衝突回避方式は、CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) である。無線LANでは、パケットの衝突(コリジョン)を検出することができない。そのため、各端末は通信路が一定時間以上継続して空いていることを確認(Collision Avoidance)してからデータを送信する。

**CDMA** (Code Division Multiple Access)：主に携帯電話で利用されている。複数の端末が同時に同じ周波数帯域に接続しても、一つ一つの端末を識別して電波を共有する仕組みである。

**CSMA/CD** (Carrier Sense Multiple Access with Collision Detection)：LAN上のパケットの衝突を検出し、それを避けてデータを送信する仕組みである。

**FDMA** (Frequency Division Multiple Access：周波数分割多元接続)：周波数帯域を分割した各帯域にチャンネルを割り当てることで、複数の発信者が同時に通信を行う方式である。

**問6****イ**

- ア：CSMA/CD方式の説明である。  
イ：FDDI (Fiber-Distributed Data Interface) はトークンリング方式であり、その説明である。  
ウ、エ：ポーリング/セレクティング方式の説明。



**問7****工**

**MIME** (Multipurpose Internet Mail Extension) : 電子メールで映像や音声, 各国語などを扱うための規格。

**MIMO** (Multiple Input Multiple Output) : 送受信の帯域を広げるために, 複数のアンテナを組み合わせる無線通信技術。

**マルチパート** : 一通の電子メールに映像や音声など, 異なる形式のデータを格納するためのMIME規格の拡張仕様である。

**リンクアグリゲーション** : 複数の物理的な回線を仮想的に束ね, 1本の回線のように扱う技術。IEEE P802.3adで規定されている。

**問8****ア**

**BGP-4**は, 組織間の経路情報をやり取りする経路制御プロトコルである。対象となる組織を自律システム (AS : Autonomous System) と呼ぶ。主にプロバイダ間の経路制御に用いられる。

イ : **OSPF** (Open Shortest Path First) に関する記述である。

ウ : **RIP** (Routing Information Protocol) に関する記述である。

エ : **ソースルーティング**に関する記述である。

**問9****イ**

**ARP** (Address Resolution Protocol) : IPアドレスからEthernetアドレス (MACアドレス) を得るプロトコルである。OSIのデータリンク層 (レイヤ2) で動く。

**CHAP** (Challenge Handshake Authentication Protocol) : PPPによりISP等と接続する際に使われる, メッセージダイジェストを利用した認証方式。ハッシュ関数による計算でパスワード認証を行うため, **PAP** (Password Authentication Protocol) よりもセキュリティ上好ましい。

**PAP** (Password Authentication Protocol) : ユーザ名とパスワードで認証する。

**PPTP** (Point to Point Tunneling Protocol) : Microsoft社によって提案されたVPN接続を行うための技術である。

# 問題

問 10

正解

完璧



直前  
CHECK

DNSでのホスト名とIPアドレスの対応付けに関する記述のうち、適切なものはどれか。

- ア 一つのホスト名に複数のIPアドレスを対応させることはできるが、複数のホスト名に同一のIPアドレスを対応させることはできない。
- イ 一つのホスト名に複数のIPアドレスを対応させることも、複数のホスト名に同一のIPアドレスを対応させることもできる。
- ウ 複数のホスト名に同一のIPアドレスを対応させることはできるが、一つのホスト名に複数のIPアドレスを対応させることはできない。
- エ ホスト名とIPアドレスの対応はすべて1対1である。

問 11

正解

完璧



直前  
CHECK

IPv6においてIPv4から仕様変更された内容の説明として、適切なものはどれか。

- ア IPヘッダのTOSフィールドを使用し、特定のクラスのパケットに対する資源予約ができるようになった。
- イ IPヘッダのアドレス空間が、32ビットから64ビットに拡張されている。
- ウ IPヘッダのチェックサムフィールドを追加し、誤り検出機能を強化している。
- エ IPレベルのセキュリティ機能（IPsec）である認証と改ざん検出機能がサポート必須となり、パケットを暗号化したり送信元を認証したりすることができる。

問 12

正解

完璧



直前  
CHECK

クラスDのIPアドレスを使用するのはどの場合か。

- ア 端末数が250台程度までの比較的小規模なホストアドレスを割り振る。
- イ 端末数が65,000台程度の中規模なホストアドレスを割り振る。
- ウ プライベートアドレスを割り振る。
- エ マルチキャストアドレスを割り振る。



## 問 10

イ

DNS (Domain Name System) のホスト名は、厳密には**FQDN** (Fully Qualified Domain Name) で記述される。これは、**TLD** (トップレベルドメイン) までのドメイン名が記述されたホスト名である。基本的に、**FQDN**とIPアドレスは1対1であるが、バーチャルホストを用いると、一つのホストを複数の**FQDN**に対応付けられる。**DNSラウンドロビン**を用いると、一つの**FQDN**を複数のIPアドレスに対応付けることができる。したがって、選択肢イが正解である。

なお、DNSラウンドロビンは負荷分散で用いる技術である。



## 問 11

エ

ア: IPv4の**TOS** (Type Of Service) フィールドは、転送優先順位を指定する。IPv6には**TOS**フィールドはないが、**Traffic Class**フィールドが同じ機能を果たしている。

イ: IPv6では、IPヘッダのアドレス空間が32ビットから128ビットに拡張された。

ウ: IPv4の**Header Checksum**フィールドはIPv6にはない。

エ: **IPsec**機能を標準装備することで、認証と改ざん検出、暗号化機能が利用可能となった。



## 問 12

エ

クラスDのIPアドレスは、マルチキャストアドレスを割り振るために使用する。**マルチキャスト**とは、単一のパケットで複数のノードに同一データを送信するパケット通信技術 (同報通信) による通信方法である。

ア: クラスAは254台 ( $2^8-2$ ) のホストアドレスを持つ。

イ: クラスBは65,534台 ( $2^{16}-2$ ) のホストアドレスを持つ。

ウ: プライベートアドレスは、クラスA, B, Cすべてで利用できる。



# 問題

問 13

正解

完璧



直前  
CHECK

RSVPの説明として、適切なものはどれか。

- ア IPネットワークにおいて、ホスト間通信の伝送帯域を管理するためのプロトコルである。
- イ LANシステムにおいて、物理的なケーブルやノードの接続形態に依存せず、ノードを任意に論理的なグループに分ける技術である。
- ウ PPPによるデータリンクを複数束ねることができるように拡張したプロトコルである。
- エ リモートアクセスを利用する利用者の認証を行うためのプロトコルである。

問 14

正解

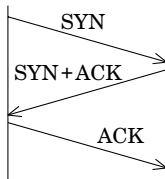
完璧



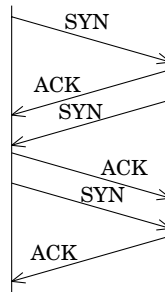
直前  
CHECK

TCPのコネクション確立方式である3ウェイハンドシェイクを表す図はどれか。

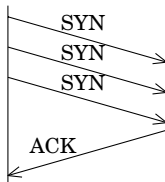
ア コネクション要求元      コネクション要求先



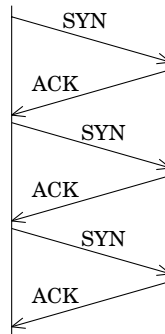
イ コネクション要求元      コネクション要求先



ウ コネクション要求元      コネクション要求先



エ コネクション要求元      コネクション要求先



平成22年度秋期試験 午前II

**問 13****ア**

**RSVP** (Resource reSerVation Protocol) は、ネットワークの帯域制御用プロトコルである。通信相手までのネットワーク帯域を予約して、通信品質を確保するために利用される。

イ：**VLAN**の説明である。

ウ：**MP** (Multilink Protocol) の説明である。

エ：**PPP**の説明である。

**問 14****ア**

TCPのコネクションを確立するためには、相互にシーケンス番号を交換することが必要となる。そのためには、コネクションの要求元から要求先へ**SYN**セグメントを送り、要求元のシーケンス番号の初期値を通知する。要求先はこのセグメントを受け取ると、**ACK**とともに要求先のシーケンス番号の初期値を**SYN**セグメントで通知する。このセグメントを受け取った要求元は、**ACK**を応答として返す。

# 問題

問 15

正解

完璧



直前  
CHECK

クラスCのIPアドレスを分割して、10個の同じ大きさのサブネットを使用したい。ホスト数が最も多くなるように分割した場合のサブネットマスクはどれか。

- ア 255.255.255.192                      イ 255.255.255.224  
ウ 255.255.255.240                      エ 255.255.255.248

問 16

正解

完璧



直前  
CHECK

SDP (Session Description Protocol) の説明として、適切なものはどれか。

- ア 音声、映像などのメディアの種類、データ通信のためのプロトコル、使用するポート番号などを記述する。  
イ 音声情報をリアルタイムストリームとしてIPネットワークに送り出す際のペイロード種別、シーケンス番号、タイムスタンプを記述する。  
ウ パケットの欠落数やパケット到着間隔のばらつきなどの統計値のやり取りに使用する。  
エ ユーザエージェント相互間で、音声や映像などのマルチメディア通信のセッションの確立、変更、切断を行う。

問 17

正解

完璧



直前  
CHECK

ネットワーク管理プロトコルであるSNMPバージョン1のメッセージタイプのうち、異常や事象の発生を自発的にエージェント自身がマネージャに知らせるために使用するものはどれか。

- ア get-request              イ get-response              ウ set-request              エ trap

**問 15****ウ**

クラスCのアドレス空間の大きさは $2^8=256$ である。これを同じ大きさの10個のサブネットに分割すると、現実にはアドレス空間の大きさが16となるサブネットを16作ることになる( $2^4 \times 2^4 = 16 \times 16 = 256$ )。つまり、ホスト用に4ビット、サブネット用に4ビット使うことになる。したがって、サブネットマスクは次のようになる。

255.255.255.11110000

なお、上位3オクテットは10進数表記、最後のオクテットは2進数表記をしている。この最後のオクテットを10進数表記すると、240である。

**問 16****ア**

SDPは、セッションの通知やセッションへの招待、その他のマルチメディアセッションの確立を目的とするマルチメディアセッションの記述用プロトコルである。

イ：RTP (Real-time Transport Protocol) に関する記述である。

ウ：RTCP (RTP Control Protocol) に関する記述である。

エ：SIP (Session Initiation Protocol) に関する記述である。

**問 17****工**

SNMP (Simple Network Management Protocol) は、LANの構成機器の動作をネットワーク管理者が把握できるように、機器の状態を監視するプロトコルである。スイッチやルータなど、ネットワーク上にある管理対象をSNMPエージェントと呼び、SNMPマネージャで一括管理する。管理対象の機器は、管理情報データベースMIB (Management Information Base) を持つ。

ネットワーク機器の状況の変化をSNMPマネージャに通知するためにTrapが用いられる。Trapは、マネージャからの問合せがなくても、機器の状態が変化したときにエージェントから通知される。

**get-request** : SNMPエージェントに情報取得を要求するメッセージタイプ。

**get-response** : SNMPマネージャからの要求に応答するメッセージタイプ。

**set-request** : SNMPエージェントに情報変更を要求するメッセージタイプ。

**trap** : 自発的に事象をSNMPマネージャに通知するメッセージタイプ。

# 問題

問 18

正解

完璧

直前  
CHECK

シングルサインオンの説明のうち、適切なものはどれか。

- ア クッキーを使ったシングルサインオンの場合、サーバごとの認証情報を含んだクッキーをクライアントで生成し、各サーバ上で保存、管理する。
- イ クッキーを使ったシングルサインオンの場合、認証対象の各サーバを異なるインターネットドメインに配置する必要がある。
- ウ リバースプロキシを使ったシングルサインオンの場合、認証対象の各Webサーバを異なるインターネットドメインに配置する必要がある。
- エ リバースプロキシを使ったシングルサインオンの場合、利用者認証においてパスワードの代わりにデジタル証明書を用いることができる

問 19

正解

完璧

直前  
CHECK

社内とインターネットの接続点にパケットフィルタリング型ファイアウォールを設置したネットワーク構成において、社内のPCからインターネット上のSMTPサーバに電子メールを送信するとき、ファイアウォールで通過許可とするTCPパケットのポート番号の組合せはどれか。

		送信元	あて先	送信元 ポート番号	あて先 ポート番号
ア	発信	PC	SMTPサーバ	25	1024以上
	応答	SMTPサーバ	PC	1024以上	25
イ	発信	PC	SMTPサーバ	1024以上	25
	応答	SMTPサーバ	PC	25	1024以上
ウ	発信	SMTPサーバ	PC	110	1024以上
	応答	PC	SMTPサーバ	1024以上	110
エ	発信	SMTPサーバ	PC	1024以上	110
	応答	PC	SMTPサーバ	110	1024以上

**問 18****工**

シングルサインオン（SSO：Single Sign-On）とは、ユーザが一度認証を受けるだけで、許可されているすべてのサーバを利用できるようになる機能のことである。認証対象（サーバ）ごとにIDとパスワードを入力する手間を省くことができるので、ユーザが記憶しておく必要のあるID・パスワードを減らすこともできる。

ア：クッキーはクライアント上に保存される。

イ、ウ：認証対象のサーバは同じインターネットドメインでもよい。

エ：デジタル証明書やその他の認証要素（認証トークン、ICカードなど）に対応したSSOシステムもある。

**問 19****イ**

社内のPCからSMTPサーバに送るパケットとその応答のパケットの通過を許可する。発信では送信元が社内のPCとなり、あて先はSMTPサーバとなる。このとき、送信元のポート番号はOSが付与する1024以上の任意の番号であり、あて先ポート番号はSMTPの25番となる。

応答では送信元がそのSMTPサーバとなり、あて先は社内のPCである。このとき、送信元のポート番号はSMTPの25番であり、あて先ポート番号は発信の時にOSが付与した1024以上の任意の番号である。

# 問題

問 20

正解

完璧

直前  
CHECK

ファイアウォールにおいて、自ネットワークのホストへの侵入を防止する対策のうち、IPスプーフィング (spoofing) 攻撃に有効なものはどれか。

- ア 外部から入るTCPコネクション確立要求パケットのうち、外部へのインターネットサービスの提供に必要なもの以外を阻止する。
- イ 外部から入るUDPパケットのうち、外部へのインターネットサービスの提供や利用したいインターネットサービスに必要なもの以外を阻止する。
- ウ 外部から入るパケットのあて先IPアドレスが、インターネットとの直接の通信をすべきでない自ネットワークのホストのものであれば、そのパケットを阻止する。
- エ 外部から入るパケットの送信元IPアドレスが自ネットワークのものであれば、そのパケットを阻止する。

問 21

正解

完璧

直前  
CHECK

送信元を詐称した電子メールを拒否するために、SPF (Sender Policy Framework) の仕組みにおいて受信側が行うことはどれか。

- ア Resent-sender:, Resent-From:, Sender:, From:などのメールヘッダ情報の送信者メールアドレスを基に送信メールアカウントを検証する。
- イ SMTPが利用するポート番号25の通信を拒否する。
- ウ SMTP通信中にやり取りされるMAIL FROMコマンドで与えられた送信ドメインと送信サーバのIPアドレスの適合性を検証する。
- エ 付加されたデジタル署名を受信側が検証する。

問 22

正解

完璧

直前  
CHECK

表示解度が1,000×800ドットで、色数が65,536色 ( $2^{16}$ 色) を表示するのに最低限必要なビデオメモリ容量は何Mバイトか。ここで、1Mバイト=1,000kバイト、1kバイト=1,000バイトとする。

- ア 1.6
- イ 3.2
- ウ 6.4
- エ 12.8



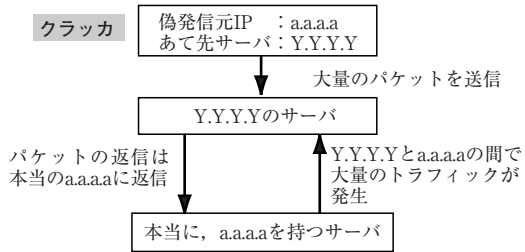
## 問20

## 工

IPスプーフィングとは、攻撃者が送信元を隠ぺいするために、送信元IPアドレスを偽装したパケットを相手に送りつけることである。外部からのパケットは、通常であれば発信元は「外部」、あて先は「自ネットワーク」となる。しかし選択肢エでは、発信元が自ネットワークであり、自ネットワークを発信元としたパケットが外部から送られてくることは不自然である。

選択肢ア、イ、ウは、IPスプーフィングではなく、不正アクセスに対する防止策である。

IPスプーフィングで発信元を偽装したDoS攻撃のときのパケットの流れは、右図のようになる。



## 問21

## ウ

SPFは、電子メールの差出人メールアドレスを認証する仕組みである。差出人アドレスに記載されたドメイン名からDNSで公開している認証情報を取得し、その情報と電子メールの送信サーバのIPアドレスとの整合性を検証する。デジタル署名などを用いないため、導入が容易である。

IPアドレスの詐称は「From:」などのメールヘッダ情報の詐称より難しいということを前提にしている。



## 問22

## ア

色数が $2^{16}$ 色なので、1ドットの画素には2バイト（16ビット）の容量が必要になる。したがって、ビデオメモリの容量は次の式で計算され、1.6Mバイトとなる。

$$1,000 \times 800 \times 2 = 1.6 \times 10^6$$



# 問題

問 23

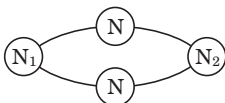
正解

完璧

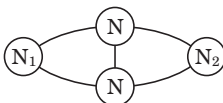
直前  
CHECK

ノード $N_1$ とノード $N_2$ の間をノード $N$ を介して通信路で結んだデータ伝送網がある。 $N_1$ と $N_2$ の間の構成についてA～Cの三つの案を考えた。ノードは故障しないものとし、各ノード間の通信路が故障する確率は、すべて等しく $F$  ( $0 < F < 1$ ) とする。三つの案を、稼働率が高い順に並べたものはどれか。

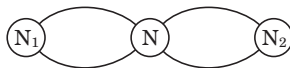
A案



B案



C案



ア B案>A案>C案

ウ B案>C案>A案

エ C案>A案>B案

エ C案>B案>A案

問 24

正解

完璧

直前  
CHECK

オブジェクト指向におけるオブジェクト間の代表的な関係には、is-aとpart-ofの二つがある。表に示すオブジェクト間の関係の組合せのうち、適切なものはどれか。

オブジェクト間の関係			
	タイヤと自動車	人間と動物	辞書と書物
ア	is-a	part-of	is-a
イ	is-a	part-of	part-of
ウ	part-of	is-a	is-a
エ	part-of	is-a	part-of

問 25

正解

完璧

直前  
CHECK

SOA (Service Oriented Architecture) でサービスを設計する際の注意点のうち、適切なものはどれか。

ア 可用性を高めるために、ステートフルなインターフェースとする。

イ 業務からの独立性を確保するために、サービスの命名は役割を表すものとする。

ウ 業務の変化に対応しやすくするために、サービス間の関係は疎結合にする。

エ セキュリティを高めるために、一度開発したサービスは再利用しない方がよい。

**問23****エ**

B案は、NとNを結ぶ通信路の稼働率が0となるとA案と同じ稼働率となり、同じ通信路の稼働率が1の場合はC案と同じ稼働率となる。NとNを結ぶ通信路の稼働率が高ければ、全体の稼働率は高くなり、低ければ、全体の稼働率も低くなるので、C案が最も稼働率が高く、A案が最も稼働率が低くなる。

▼  
**解答****問24****ウ**

**is-a関係**は、「Dog is a Animal」に代表されるように汎化（特化）の親子関係なので、「人間と動物」と「辞書と書物」が該当する。

**part-of関係**は部分と全体の関係なので、「タイヤと自動車」が該当する。

**問25****ウ**

SOA (Service-Oriented Architecture : サービス指向アーキテクチャ) は、システムの各機能をサービスという単位で独立・分散させるシステムアーキテクチャである。従来のシステムでは、コンポーネントとして各機能が分割されていた。サービスはコンポーネントよりも抽象度（機能の粒度）が高く、一つのサービスが一つの業務システムそのものである場合もある。

サービス間の関係は**疎結合**となり、メッセージを介して機能を利用する。

ア：SOAのインタフェースは、伝達したメッセージの応答が返ってこないこともある。つまり、セッションを維持しないステートレスなサービスである。

エ：SOAは、ソフトウェア部品の再利用をサービスの視点で行うものである。