〔No. 1〕　コンピュータの構成要素として、ハードディスクが該当するものはどれか。

1. 演算装置
2. 制御装置
3. 主記憶装置
4. 補助記憶装置
5. 出力装置

〔No. 2〕　USB3.0 の説明として、**誤っているもの**はどれか。

1. USB2.0 と比べて、最大電流及び最大電圧が引き上げられたことから、より早く充電することが可能になった。
2. 最大伝送距離は、USB1.0 よりも短い。
3. 下位互換性があるため、コネクタの種類が合えば、古い USB 機器でも使用することができる。
4. USB2.0 と区別するため、一部が青色のコネクタを使用することが多い。
5. 最大転送速度の理論値は、USB2.0 の 10 倍以上である。

〔No. 3〕　ハードディスクで使用されるインターフェース（接続規格）として、**誤っているもの**はどれか。

1. IDE
2. SATA
3. USB3.0
4. USB2.0
5. HDMI

〔No. 4〕　複数のハードディスクを利用して、書き込み速度や可用性の向上を図るRAIDの種類として、最も高速にデータを書き込むことが期待できるものは、次のうちどれか。

1. RAID1
2. RAID10
3. RAID6
4. RAID5
5. RAID0

〔No. 5〕　スマートフォンのカメラなどで読み取って利用される二次元コードの説明として、適切なものはどれか。

1. 縦、横、斜めの三方向に情報を持つことができる。
2. 最も普及している二次元コードの一つとして、バーコードが挙げられる。
3. 最低でも１cm以上の大きさが必要である。
4. 二次元コードを利用すれば、URL等を入力する手間が省ける。
5. 偽の二次元コードを張り付けた場合、不正を検知する機能が働くので、正常に動作することはない。

〔No. 6〕　一般的なOSが取り扱うファイルシステムの種類として、**誤っているもの**はどれか。

1. FAT
2. NTFS
3. HFS
4. XFS
5. SSD

〔No. 7〕　メモリリークの説明として、適切なものはどれか。

1. サイバー攻撃を受けて、メモリの内容が漏れてしまうこと。
2. 通信帯域を圧迫するDoS攻撃を受けたことにより、サービスの提供が滞ること。
3. プログラムがメモリを確保した後、その使用が終わっても解放することなく確保し続けてしまうこと。
4. ウイルスに感染したことを端緒として、メモリの内容の一部が流出すること。
5. ファイル共有ソフトに含まれるバグが原因で、情報流出が発生すること。

〔No. 8〕　NAPT（IPマスカレード）の説明として、適切なものはどれか。

1. インターネット接続に利用されており、転送速度は速いが信頼性は低いという特徴がある。
2. 一つのグローバルIPアドレスを複数の機器で共有する。
3. 機器を管理するプロトコルで、MIBという通信機能を使って、エージェントに特定のイベントが発生したことを通知する。
4. IPアドレスやデフォルトゲートウェイといったインターネット接続に必要な設定を自動化するプロトコルである。
5. ネットワークを経由して他のコンピュータに接続することで、遠隔操作ができるプロトコルである。

〔No. 9〕　TCP や UDP において、ウェルノウンポートと呼ばれるポート番号に含まれるものはどれか。

1. 22
2. 8080
3. 1024
4. 3306
5. 3389

〔No.10〕　電子メールを送信するときのほか、サーバ間でメールを転送するときにも使われているプロトコルはどれか。

1. APOP
2. PPPoE
3. IMAP
4. SMTP
5. POP3

〔No.11〕　TCP/IP ネットワークにおいて、IP アドレスとドメイン名やホスト名を対応付ける役割をもつサーバはどれか。

1. DNS サーバ
2. DHCP サーバ
3. プロキシサーバ
4. SMTP サーバ
5. FTP サーバ

〔No.12〕　IP アドレス 32.24.16.6/29（サブネットマスク　255.255.255.248）が属する IPv4 ネットワークのブロードキャストアドレスとして適切なものはどれか。

1. 32.24.16.8
2. 32.24.16.248
3. 32.24.16.0
4. 32.24.16.29
5. 32.24.16.7

〔No.13〕　クライアントのパソコンと WEB サーバが HTTPS で通信している。クライアントから WEB サーバに送られる通信パケットを確認すると送信元のポート番号は 55555、送信先のポート番号は 443 であった。この場合、WEB サーバから戻ってくる通信パケットの送信元のポート番号及び送信先のポート番号として適切な組み合わせはどれか。

1. 送信元のポート番号　443　　送信先のポート番号　55556
2. 送信元のポート番号　55555　送信先のポート番号　55556
3. 送信元のポート番号　55556　送信先のポート番号　443
4. 送信元のポート番号　443　　送信先のポート番号　55555
5. 送信元のポート番号　444　　送信先のポート番号　443

〔No.14〕　ファイアウォールのパケットフィルタリング機能を利用することで実現できるものはどれか。

1. パケットの送信先や送信元の IP アドレスなどを確認し、あらかじめ定めたルールに基づいてパケットを遮断したり、通過させたりして通信を制御する。
2. パケットの内容を監視し、アクセスすることが望ましくないサイトやコンテンツなどへの通信が発生した場合は、通信を遮断するなどして、あらかじめ定めたルールに基づいてアクセスを制御する。
3. パケットの内容を監視し、不正なアクセスがないかを確認し、不正なアクセスやその兆候を検出した場合は管理者に知らせるが、不正なアクセスを遮断することはできない。
4. メールサーバ間でやりとりされるメールの内容について確認し、メールにウイルスが添付されている可能性が高い場合はメール転送の中止やメールの削除などを行い、ウイルスの拡散を防ぐ。
5. パケットの内容を監視し、不正なアクセスがないかを確認し、不正なアクセスやその兆候を検出した場合は管理者に知らせ、不正なアクセスを遮断する。

〔No.15〕　IP アドレス 192.168.6.60/22（サブネットマスク 255.255.252.0）が割り振られたホストが所属するネットワークアドレスはどれか。

1. 192.168.3.0
2. 192.168.4.0
3. 192.168.5.0
4. 192.168.6.0
5. 192.168.7.0

〔No.16〕　OSI 参照モデルの第３層に分類されるプロトコルを列挙したものは、次のうちどれか。

1. HTTP、HTTPS
2. ICMP、SSH
3. PPP、ICMP
4. TCP、UDP
5. ARP、ICMP

〔No.17〕　PPPoE 接続した IPv4 ネットワークで TCP を使用するとき、フラグメント化されることなく送信できるデータの最大長は何オクテットか。ここで TCP パケットのフレーム構成は図のとおりであり、ネットワークの MTU は 1,500 オクテットとする。また、( ) 内はフィールド長をオクテットで表したものである。

Ethernet ヘッダ (14)	PPPoE ヘッダ (6)	PPP ヘッダ (2)	IP ヘッダ (20)	TCP ヘッダ (20)	データ	FCS (4)

1. 1,434
2. 1,452
3. 1,482
4. 1,488
5. 1,492

〔No.18〕　ファイアウォールに関する内容として、**誤っているもの**はどれか。

1. ブラックリストとは「拒否リスト」のことであり、ブラックリストに記載されているネットワーク通信は全て遮断される。
2. パケットフィルタリング型はパケットのヘッダ部分を見て通信の許可と拒否を判断する。
3. ダイナミックパケットフィルタリングは、パケットのデータ部を確認して不正なアクセスを防止できる。
4. サーキットレベルゲートウェイ型やアプリケーションゲートウェイ型などの種類がある。
5. ステートフルインスペクションは、過去に通過したパケットから通信セッションを認識し、受け付けたパケットを通信セッションの状態に照らし合わせて通過させるかどうか判断する。

〔No.19〕　MAC アドレスから対応する IP アドレスを取得するプロトコルはどれか。

1. ARP
2. SMTP
3. SSH
4. Telnet
5. RARP

〔No.20〕　デジタル署名などに用いるハッシュ関数の特徴について、**誤っているもの**はどれか。

1. ハッシュ関数は、改ざん検出などに使われる。
2. 同じメッセージダイジェストになる二つの異なるメッセージは容易に求められる。
3. メッセージダイジェストはメッセージの長さに関係なく、固定長である。
4. 元データが同じであれば、出力されるハッシュ値は必ず同じになる。
5. ハッシュ関数の種類としては、MD5 や SHA-1 などがよく知られている。

〔No.21〕　情報セキュリティにおけるバックドアの説明として、適切なものはどれか。

1. バックアップを作成するときに利用するインターフェースのことを、バックドアという。
2. バックドアを使う場合であっても、ID とパスワードは必ず入力しなければならない。
3. 大規模な情報システムを構築するときには、バックドアの設置が推奨される。
4. バックドアの確認方法としては、CRL を確認する方法と、OCSP を確認する方法がある。
5. バックドアを悪用することにより、攻撃者はいつでも情報を盗み取ることができる。

〔No.22〕　ウイルス対策に関する仕組みの一つであるサンドボックスの説明として、適切なものはどれか。

1. インターネットから届くパケットのうち、攻撃と思しきものを緩衝する。
2. バックアップしたデータを、長期保存に適したデータ形式へ変換する。
3. ファイアウォール等の設定を確認するため、様々な仮想攻撃を外部から行う装置のこと。
4. 隔離された領域でファイルを実行することにより、ウイルスだった場合の被害を回避する。
5. 内部のネットワークを保護するため、ウェブサーバ等の外部に公開するサーバを別のネットワークに隔離する技術のこと。

〔No.23〕　２要素認証の説明として、**誤っているもの**はどれか。

1. ATM にキャッシュカードを挿入し、パスワードで認証する方法は２要素認証である。
2. 登録 ID とパスワードを入力後、あらかじめ設定していた秘密の質問の答えを入力して認証することは２要素認証である。
3. 顔認証と指認証を組み合わせることは２要素認証ではない。
4. 登録 ID とパスワードを入力後、あらかじめ登録しておいた携帯電話番号に送られてきた認証コードを入力して認証することは２要素認証である。
5. ハードウェアトークンを利用し発行されるワンタイムパスワードのみで認証することは２要素認証ではない。

〔No.24〕　リフレクタ攻撃に悪用されることの多いサービスを列挙したものとして、適切なものはどれか。

1. DNS、HTTP、HTTPS
2. SSL、SSH
3. NTP、SSL
4. Telnet
5. DNS、NTP、LDAP

〔No.25〕　cookie に Secure 属性が設定されていた場合のブラウザの処理はどれか。

1. ブラウザは、cookie の“Secure=”に続いて指定されたホスト名を参照し、指定されたホストにその cookie を送信する。
2. ブラウザは、cookie の“Secure=”に続いて指定されたサーバのパスを参照し、指定されたパスが一致する場合にその cookie を送信する。
3. ブラウザは、cookie の“Secure=”に続いて指定された時間を参照し、指定された時間を過ぎている場合にその cookie を削除する。
4. ブラウザは、cookie の“Secure”を参照し、HTTPS 通信時だけその cookie を送信する。
5. ブラウザは、cookie の“Secure”を参照し、ブラウザの終了時にその cookie を削除する。

〔No.26〕　パケットフィルタリング型ファイアウォールがルール一覧に基づいてパケットを制御する場合、パケット A に適用されるルールとその時の動作はどれか。ここで、ファイアウォールでは、ルール一覧に示す番号の１から順にルールを適用し、一つのルールが適合したときには残りのルールは適用しない。

番号	送信元 アドレス	宛先 アドレス	プロトコル	送信元 ポート番号	宛先 ポート番号	動作
1	172.16.2.3	＊	＊	＊	＊	通過禁止
2	＊	172.17.3. ＊	TCP	＊	25	通過許可
3	＊	172.1. ＊	TCP	＊	25	通過許可
4	172.17.3.4	＊	TCP	25	＊	通過許可
5	＊	＊	＊	＊	＊	通過禁止

注）＊は任意のパターンを表す。

パケット A

送信元 アドレス	宛先 アドレス	プロトコル	送信元 ポート番号	宛先 ポート番号
172.17.3.4	172.16.2.3	TCP	1700	25

1. 番号１によって、通過を禁止する。
2. 番号２によって、通過を許可する。
3. 番号３によって、通過を許可する。
4. 番号４によって、通過を許可する。
5. 番号５によって、通過を禁止する。

〔No.27〕　デジタルフォレンジックスの説明として適切なものはどれか。

1. ネットワーク管理者や利用者等から、巧みな話術や盗み聞き、盗み見などの手段によって、パスワード等のセキュリティ上重要な情報を入手する。
2. コンピュータやネットワークのセキュリティ上の脆弱性を発見するため、システムを実際に攻撃して侵入を試みる。
3. 犯罪に関する証拠となり得るデータを保全し、その後の訴訟に備える。
4. 画像や音楽等のデジタルコンテンツに別の情報を埋め込んで隠す。
5. 磁気ディスク等の書き換え可能な記録媒体を単に初期化するだけでは、データを復元される可能性があるので、覆い隠すように上書きする。

〔No.28〕　プロキシ経由でインターネットアクセスする環境において、ブラウザの URL 入力欄に次の URL を入力したときに、ブラウザがプロキシに最初に送信する HTTP メッセージのリクエストラインはどれか。

入力した URL：https://○○.com/index.html

1. CONNECT ○○.com:443 HTTP/1.1
2. POST ○○.com:443/index.html HTTP/1.1
3. GET ○○.com:443/index.html HTTP/1.1
4. SSL ○○.com:443 HTTP/1.1
5. TLS ○○.com:443 HTTP/1.1

〔No.29〕　SPF によるドメイン認証を実装する場合、SPF の導入時に、電子メール送信元アドレスのドメイン所有者側で行う必要がある設定はどれか。

1. DNS サーバの MX レコードに正当なメールサーバの IP アドレスやホスト名を登録する。
2. DNS サーバの MX レコードに公開鍵を登録する。
3. DNS サーバの TXT レコードに正当なメールサーバの IP アドレスやホスト名を登録する。
4. DNS サーバの TXT レコードに公開鍵を登録する。
5. DNS サーバの問い合わせで使用するポート番号を変更する。

〔No.30〕　不審メールのメールヘッダから送信元又は中継元の ISP 又は組織を特定する手がかりの内、最も信頼できるものはどれか。

```
Return-Path: <ユーザ名@ホスト名.ドメイン名 ① >
Received: from ホスト名.ドメイン名 ② (ホスト名.ドメイン名 ③ [IP アドレス])
        By 受信メールサーバ名 with ESMTP id ●●
        For  <ユーザ名@ホスト名.ドメイン名>; 日  時
Received: from ホスト名.ドメイン名 ④ (ホスト名.ドメイン名 [IP アドレス])
        By メールサーバ名 with SMTP id ●●
        For  <ユーザ名@ホスト名.ドメイン名>; 日  時
From: <ユーザ名@ホスト名.ドメイン名 ⑤ >
To: <ユーザ名@ホスト名.ドメイン名>
```

1. エンベロープ FROM であるホスト・ドメイン名①
2. 中継元が SMTP の HELO コマンドで通知したホスト・ドメイン名②
3. 中継元の IP アドレスから逆引きされたホスト・ドメイン名③
4. 送信元が SMTP の HELO コマンドで通知したホスト・ドメイン名④
5. From ヘッダに設定されたホスト・ドメイン名⑤

〔No.31〕　ランサムウェアに関する説明として、**誤っているもの**はどれか。

1. ランサムウェアとは感染したパソコンのデータを暗号化して、その復号と引換えに金銭を要求するマルウェアのことをいう。
2. 身代金要求型ウイルスとも呼ばれる。
3. 最近では、情報漏えいによる脅迫を組みわせたものもある。
4. 令和３年中の国内のランサムウェアによる被害企業・団体へのアンケート調査回答で、感染経路として最も多かったものは「不審メールやその添付ファイル」によるものであった。
5. 令和３年中に警察庁に報告された国内のランサムウェアによる被害件数は 146 件であり、前年以降右肩上がりで増加を続けている。

〔No.32〕　リバースブルートフォース攻撃の対策として、**適切でないもの**はどれか。

1. 推察されやすいパスワードを使用しない。
2. パスワードを長く、英字や数字を組み合わせたものにする。
3. １つのユーザ ID で一定回数以上パスワードを間違えると、ユーザ ID をロックさせる。
4. 同一 IP アドレスからのログイン試行回数を制限する。
5. ログイン可能な端末を制限する。

〔No.33〕　SSL の説明として、**誤っているもの**はどれか。

1. SSL とは、ウェブブラウザとウェブサーバの間のデータ通信を暗号化し、送受信させる仕組みのことである。
2. 第三者からの盗聴や改ざんを防ぐ役割を持っている。
3. SSL 証明書には、DV 証明書、OV 証明書、EV 証明書があり、認証レベルが一番高いのは、EV 証明書である。
4. SSL 証明書は、どの種類のものも、ドメインの所有権は証明事項として必要である。
5. SSL 証明書は、どの種類のものも、企業の実在性は証明事項として必要である。

〔No.34〕　警察署表と拾得件数表に対して、次の SQL 文を実行した結果として正しいものはどれか。

```
SELECT　警察署表.警察署名, 拾得件数表.拾得件数
FROM　警察署表, 拾得件数表
WHERE　警察署表.警察署 ID = 拾得件数表.警察署 ID
　　AND 拾得件数表.拾得件数 > 100
ORDER BY 拾得件数表.拾得件数 DESC;
```

警察署表

警察署 ID	警察署名
1	A 警察署
2	B 警察署
3	C 警察署
4	D 警察署
5	E 警察署

拾得件数表

警察署 ID	拾得件数
2	250
3	125
1	85
5	300

1.

警察署名	拾得件数
E 警察署	300
B 警察署	250
A 警察署	125

2.

警察署名	拾得件数
B 警察署	250
C 警察署	125
E 警察署	300

3.

警察署名	拾得件数
E 警察署	300
B 警察署	250
C 警察署	125

4.

警察署名	拾得件数
E 警察署	300
D 警察署	
C 警察署	125
B 警察署	250
A 警察署	85

5.

警察署名	拾得件数
E 警察署	300
B 警察署	250
C 警察署	125
A 警察署	85
D 警察署	

〔No.35〕　次の再帰的に処理を行う関数の f(10)の値として正しいものはどれか。

```
f(x) = if x < 3 then 5
               else f(x - 3) + 1
```

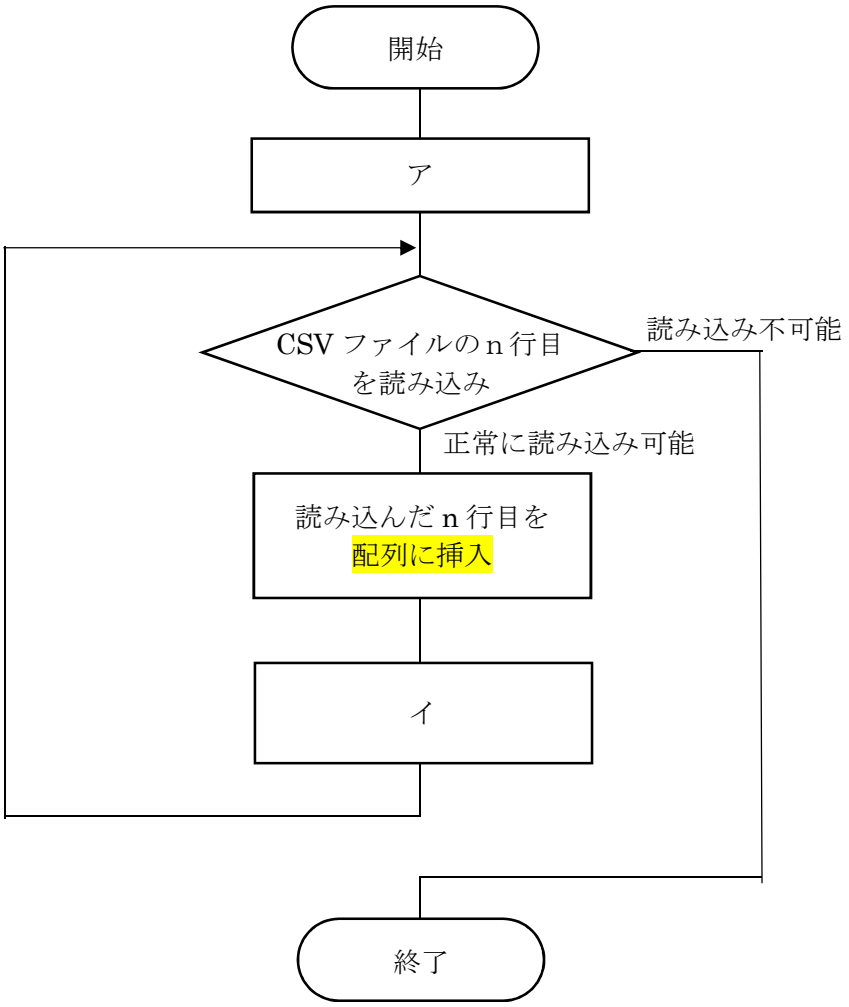
[if 文の説明]

```
if　条件式　then　処理A
            else　処理B
```

条件式が真の場合は処理 A を、偽の場合は処理 B を実行する。

1. 10
2. 15
3. 7
4. 8
5. 5

〔No.36〕　次のフローチャートは、CSV ファイルで記録された 100 名の職員の名簿を取り込み、1 行毎に配列に取り込む処理を行うプログラムのものである。空欄の中に入る適切な処理の組み合わせについて、適切なものはどれか。



1. ア　n = 1　イ　n = n + 1
2. ア　n = 100　イ　n = 1
3. ア　n = 0　イ　n = 100
4. ア　n = 0　イ　n = 100 − n
5. ア　n = 1　イ　n = 100 + n

〔No.37〕　不正アクセス禁止法によって処罰の**対象とならない行為**はどれか。

1. セキュリティホールを攻撃して、サーバに侵入した。
2. フィッシングにより、他人の ID、パスワードを不正に取得した。
3. 本人の許可を得ずに、インターネット上のサービスへログインする際に使うパスワードを第三者に教えた。
4. ネットワークに接続されていないスタンドアロンのパソコンを使って、本人の許可を得ずにログインした。
5. 不正アクセスを行う目的で、他人の ID 及びパスワードを入手したが、これまでに不正アクセスは行っていない。

〔No.38〕　不正指令電磁的記録に関する罪に抵触する可能性があるものはどれか。

1. 自分に送られてきたコンピュータウイルスを、それとは知らずに他者に転送した。
2. サーバに対し DDoS 攻撃を行った。
3. 会社でライセンスを購入したソフトウェアパッケージをコピーし、無断で個人所有のパソコンにインストールした。
4. ウイルス対策ソフトの開発のため、新しいウイルスを作成した。
5. 正当な理由なく、他人のコンピュータを誤作動させるウイルスを収集し、自分のパソコンに保管した。

〔No.39〕　不正競争防止法で禁止されている行為として、**誤っているもの**はどれか。

1. 競争相手に対抗するため、商品の小売価格を安く設定した。
2. 他社の製品の形態を模倣した商品を提供した。
3. 営業秘密を不正に取得、使用した。
4. 他社の著名なサイトと同一・類似のドメイン名を不正に取得、使用した。
5. 技術的制限手段によりコピー等が制限されているデータを、利用可能にするソフトを提供した。

〔No.40〕　著作権法上、違法となる行為として、**誤っているもの**はどれか。

1. 職務著作のプログラムを、作成した当事者が会社の許可を得ることなく複製し、他社に提供した。
2. 購入したプログラムを、特定のコンピュータで使用できるようにするため改変した。
3. 海賊版の動画と知っていたが、個人的に楽しむためにダウンロードした。
4. 人気アニメを撮影して、動画共有サイトに投稿した。
5. 業務処理用で購入したプログラムを複製し、社内教育用として各部門に配布した。