情報工学概論過去問

1,物流コンテナが、車など運ぶ媒体に影響されるのに対して、インターネットは、デジタル化することで、こうした運ぶ媒体に依存せずに運ぶことができるようになった。こうして、インターネットは、品質を劣化させずに、運ぶコストも大幅に少なくした。

2,「メッセージ」をアナログで伝達する場合は、音声という物理的な伝達が用いられる。具体的には、楽譜などのデジタル情報が音声によって、アナログ変換され、それを直接他人に伝達していたので、情報の品質は劣化していた。
　しかし、デジタルで伝達する場合は、デジタルの情報がデジタルのまま直接受け手に伝わるので、情報の品質が劣化せずに、また、情報のコストを大幅に削減して伝達することができる。

3,インターネットは、情報を提供することも、享受することも容易にでき、皆で情報を簡単に共有することができる。したがって、こうした相互に支援し合うことによって、自分の利益を社会に寄与することもできる。また、全体を統合するシステムでなく、自立分散的なシステムが形成され、環境の変化にも対応しやすいネットワークになった。したがって、インターネットが普及していったと考えられる。

4,セキュリティーとは、行動をできるだけ制限しないように、取り締まる基準を厳格にし過ぎないようにして、最大限のリスクに対処できるようにすることで、安心感を与えるようにすることを目的にする。例えば、暗号技術によって、ICカードや会員のアカウントなどの制度で人々の生活に利便性を与え、かつプライバシーの保護にも大いに貢献している。

5,プロトコルを階層に分けることによって、下の階層の差異は、直近の上の階層のシステムにのみ影響を与えるようなシステムを作り、下の階層におけるサービスや情報をインターフェイスによって、よりサービスや情報の付加価値を高くして上の階層に伝達していくシステムである。
　このシステムの利点としては、階層によって作業を独立させて分担できるの

で、他の階層の役割を熟知せずとも、仕事を行うことができる。また、他の階層に依存せずに容易に新機能を追加することや、作業を単純化することもできる。このことによって、機能の選択肢を容易に増加させることができる。
さらに、エラーの原因もより簡単に探し当てることもできる。

6,Web サーバーから、直接インターネットに送信すると、この送信時の IP アドレスは、プライベートのために、インターネットで破棄されてしまう。このために、ブロードバンドルータを中間に介して、NAT テーブルを設けることで、IP アドレスをプライベートからグローバルに変換して正しく送信することができるようにする。

具体的には、インターネットの Web サーバーの要求をブロードバンドルータが受け取り送信元をブロードバンドルータが受け持って、Web サーバーに送る。要求を受け取ると、Web サーバーが情報をブロードバンドルータに送って、NAT テーブルのとおり、IP アドレスを変換してインターネットに送ることで、正しく通信することができる。

7,

From E to	Link	Cost
A	(4)	2
B	(4)	1
C	(5)	1
D	(6)	1
E	local	0

8,「Three-Way Handshake」とは、TCP セッションの確立の際に、3 つのパケットを用いることであり、具体的には、最初に SYN(コネクションの確立の要求の制御メッセージ)を送り、そのコネクションが作れることを確認するために、ACK（制御メッセージ）を返信する。最後に、ACK に対する返信を行うと、TCP セッションを確立できる。また、IP パケットの破棄をしても良い理由は、途中で ACK が失われたときは、一定の時間が経過するとタイムアウトし、タイムアウト後に失われたパケットが再送されることが挙げられる。

9,シグナリングとは、エンドノード間において、仮想の回線を確立するための手続きである。ここで、TCP コネクションにおいては、DNS を用いて、DNS の階層的なドメインを各々の階層のサーバーから取得するなどして、宛先のノードで IP パケットを転送する情報を取得することで､TCP のコネクション確立手法(8 で述べた通り)を実行することができる。したがって、このことによって、エンドノード間に交換機/ルータ間に仮想の回線を確立することができる。

10,ssh は、送られてきた情報を公開鍵で暗号化し、それを秘密鍵で平文化する公開鍵暗号方式の１つである。具体的なシステムを述べると、サーバーとクライアント間において、まず公開鍵を交換しチェックする。また、クライアントはサーバーが提示した公開鍵を乱数によって生成した共通鍵（セッション鍵）を暗号化する。つぎに、暗号化された共通鍵をサーバーに送り、その鍵を自らの公開鍵で復号化する。そうして、サーバー/クライアント間で共通鍵の照合をし、クライアントの接続先のアカウントを共通鍵で暗号化したものをサーバーに送り、認証することによって、今後共通鍵で安全に通信することができる。

11,「尖閣諸島ビデオ流出事件」における問題点は、次の３つの通りとなる。

１つ目は、ISP の警察に対する対応において捜査令状がないので、この情報の提供が通信の内容を漏洩することや利用することができないという通信の秘匿性に反していることである。また、そうした違反に対する海上保安庁の処罰が直ちに施されていなかったことも問題となる。

２つ目においては、情報保全の問題が挙げられる。今回は YouTube などでアップロードされて、情報流出が顕在化したが、もし、公開されずに機密情報をこっそり使われていたときなどを想定したりするなど、情報保全のシステムの見直しも検討する必要がある。

３つ目は、政府のビデオを公開しないということを、外交の戦略なしで行ったということである。本来の知的財産権は、不当あるいは過度な制限をかけるものでなく、適度な制限によって交流を進めるものである。したがって、上記のように理由なしに、国民に公開を制限することは、知的財産権の本質から外れていると考えられる。