インターネット工学2006年解答

インターネット工学2011年解答

1. ベストエフォート型のネットワークであるため多数の人が同時に利用できる

状態管理がソフトステートのためリカバリーが容易

デジタル伝送でノイズをなくす

パケット転送によって回線に障害が生じても柔軟に経路を変更して有効利用や大量通信ができる

エンドツーエンドの原則によって情報管理量の爆発を抑える、出発点と目的地以外の責任を持たない。

２．オープンシステムを採用し各階層のインターフェースを公開し、それに基づき製品が開発されるための各階層のインスタンスを交換・分担可能にすることで、階層構造によって実現可能となった、ネットワーク構築のための汎用システムを作れるようになったから。

３．言葉は、伝えようとした言葉の意味を自分も相手も知っているため誤りのない複製と伝達を行うことができ、言葉が伝わらない場合でも様々な対応をして自律的に誤りを訂正する機能を持ち、声や文字などの伝達媒体に依存しない、という特徴を持つ。

４．クライアント（依頼者）とサーバ（提供者））が決まっている放送に対し、電話とインテ―ネットは全ての人がサーバにもクライアントにもなりうるP２Pである。また放送と電話はサービス品質を保証してくれるが、インターネットはそういった保証がないベストエフォート型である。状態管理ポリシーとしては、放送・電話はシグナリング手順を持ち通信経路が決まっているハードステートであるのに対し、インターネットはシグナリング手順を持たず自動的に転送サービスの実現可能な経路を探し出すソフトステートである。

５．インターネットにおける動的経路制御（ルーティング：RIPやBGPなど）の機能は、数学的にはどのようなことを行っているか、簡単に説明しなさい。

答）あるノード（目的地）をルート（根）とするツリーを形成する。このようなツリーは多数存在可能であるが、定まったコスト関数を用いて絶えずルーティングテーブルを作成し、唯一のツリーを選択する。これをすべてのノードに対して行うが、全世界規模の完全なツリーを管理することは難しいので、再帰的な構造を持ちこんでいる。

補足）・決定は通常ルーティングプロトコルと経路決定アルゴリズムによってなされる。

・RIPでは、メトリックがより少ない経路情報が最適経路として使用されます。最大メトリックは15となっており、これを超えた場合は到達不能と見なされます。RIPでは、これらのすべての経路情報を30秒周期で隣接ルータにアナウンスすることにより、情報の更新を行います。

・BGPルータは、隣接したルータとTCPを用いて1対1のセッションを確立し、セッション確立直後にすべての経路情報を交換します。その後、この情報に更新がない場合は、Keep Aliveパケットによる生存確認のみを行います。また、更新があった場合には、その差分情報だけを交換します。BGP経路情報には、パス属性と呼ばれるパスに関する情報が含まれており、これに基づき最適経路が決定されます。このため、BGPではこれらのパス属性の変更で柔軟にトラフィック・コントロールを行うことが可能であり、これはBGPの大きな特徴といえます。

※数学的に、というのがどの程度かははっきり言えないので、不安な人はRIPやBGPを例に、数学的な考えに触れておくのがベターかもしれません。

６．暗号化は、数学的にはどのようなことを行っているのかを説明しなさい。

答1）「平文」文字空間と「暗号」文字空間との間の写像（文字、パラメータ）の計算を行っている。「暗号」文を「たくさん」眺めると、文字とパラメータが見える。この「たくさん」が大きいほどよい（レジュメより）

答2）平文→（暗号化）→暗号文→（復号）→平文という作業を行列や素因数分解を用いて行っている。たとえば、一般的に使われるRSA暗号では、以下略（必要だと思った人は補足を参照してください）

補足）RSA暗号

を相異なる素数ｐ１，ｐ２，・・・，ｐｒ の積とします。 ｅ を gcd(e,φ(ｎ))=1 となる正整数とします。 ここで，φ(ｎ) は ｎのオイラー関数です。このとき，,φ(ｎ) を法とするeの逆元が存在します（整数の合同参照）。それを d （1≦d≦p-1）とします。このとき，

ed ≡ 1 (mod φ(ｎ))

が成立します。従って ｘ （0≦ｘ＜ｎ）に対して，オイラーの定理から，

xed≡x (mod ｎ)

となります。（gcd(x,n)>0のときはオイラーの定理は使えませんが，この場合でも上の式は成立することが分かります。）

　上の性質からxの範囲が0≦ｘ＜n であることを使うと，dを知っていれば，xeから x が求められることになります。従って

x　→（暗号化）→　xe　→（復号）→　xed≡ x (mod n)

によって，eを暗号化鍵，dを復号鍵とする暗号が得られます。ここまでは指数型暗号(exponentiation cipher)と よく似ています。しかし，１つだけ重要な違いがあります。それは，次のことです。

e から d を計算するとき，φ(ｎ)が必要となります。しかし他方，ｘから 　xe　を計算するときはｎが必要ですが，φ(ｎ)は必要 はありません。さらに，ｎからφ(ｎ)を求めるには ｎの素因数分解が必要になります。この素因数分解が大変難しいため、暗号として成立しています。

７．TCPを用いたデータ転送において、高スループットを実現するために適用されている手法であるウィンドー制御を簡潔に説明し、さらに最大スループットを実現するための必要条件を示しなさい。

説明：インターネットで標準的に用いられるトランスポート層のプロトコルであるTCPなどで採用されている、効率的なデータ転送の方式の一つ。「ウィンドー」(window)と呼ばれるバッファメモリ領域を確保して、大きな単位でデータを転送する方式。

条件：

８．アナログ回線を用いてデジタルデータを伝送するモデムの動作原理を説明しなさい。

デジタル信号をアナログ回線で伝送できるように、伝送路の特性に合わせたアナログ信号にデジタル変調して送信する。アナログ回線の伝送路からのアナログ信号をデジタル信号に復調して受信する。

※これ以上書くこと思いつかなかった

９．NAT の動作原理を説明し、その利点と欠点をそれぞれ２つ挙げなさい。（p.190～192）

※NAT：プライベートIPアドレスを持つ組織内のノードとグローバルIPアドレスを持つノード間の通信のためにルータでIPアドレスの変換を行う機能のこと

パケットの送信元に対して、NATルータがグローバルIPアドレスを割り当て、送信元の持つプライベートIPアドレスと関連付ける。以後、内外からくるパケットを、IPアドレスを変換することにより伝達する。

利点（※恐らく）

・多数のホストのIPアドレスを1つにできるため、IPアドレスの枯渇に耐えることができること

・パケットがNATを通るときにパケットフィルタリングを行うことでセキュリティを高めることが可能なこと

欠点

・同時に行うことのできるセッションに限りがあること

・そのために多数のユーザーが利用しているときは使えるセッション数が極端に少なくなること

１０．大規模 WEB システムにおける処理負荷の分散手法には、大きく２つの手法が存在する。これら２つの手法を、コンピュータのアーキテクチャを比較しながら、簡潔に説明しなさい。（p.390）

水平分散：複数のサーバに並列的に処理を実行させる。特定の機能ごとに専門化したサーバを用意し、適切に分担して使う。コンテンツを常に同期させる必要がある。

垂直分散：キャッシュやプロクシを利用し、わざわざ大元のサーバまで情報を取りに行かなくていいようにして、データ処理をクライアントに近い仮想ノードで分担する。キャッシュを取るため必ずしもオリジナルコンテンツとの同期はなされていない。（ダイナミックにコンテンツが変わるサービスには垂直分散は向いていない）

１１．「セキュリティー」は何を実現することを目的としているのか簡潔に述べよ。（p.424～435）

安心してのびのびと仕事ができる環境を実現することが目的である。この目的のために必要な事項である「守るべきものを破壊、または盗難されないこと」がセキュリティーによって実現される。（完全にリスクをなくすことではない。）

１２．レポジトリとレジストリの違いを説明し、それと関連して Google と Yahoo!のビジネスモデルの違いを説明しなさい。（p.284～285）

repository:貯蔵庫/データ自体の集積をするもの

registry:登録所/データに関する情報（メタデータ）を格納するもの

Googleは情報を集めることが目的（情報の流通と加工・レポジトリ）

Yahoo!は物を売ることが目的（物流の仲介・レジストリ）

中身まで含めて全部把握する（それ自体が目的）か名前だけ把握して中身は後で引き出す（何かの目的に利用する）かの違い？