2010年度 電気工学特別講義 第4回
インターネットとTCP/IPの基礎技術
そしてセキュリティ

力武 健次
京都大学
学術情報メディアセンター
2010年5月25日

自己紹介

力武 健次（りきたけ けんじ）

- 1965年生まれ 45歳
- インターネットそのものが仕事です

  1985年からネットワークの楽しさにハマっています

  専門: ネットワーク運用とセキュリティの調査研究

この講義ではインターネットの技術と社会が今抱えている問題について共に考えて行きたい

特にセキュリティとプライバシーの問題は重要不可欠

講義に関する注意

出席を取るための名簿を回します
- 自分の名前を書いてください
- 講義後毎回回収します

できるだけ音を立てないでください
- ケータイはマナーモードにしてくださいね

講義の要約や案内はWebに出します

http://www.k2r.org/kenji/jp-oueees2010.html

今日の講義の内容

インターネットの基礎的な技術（TCP/IP）
- 情報伝送のパケット化で変わった世界
- 4階層に分けてネットワークの機能を考える
- IPアドレスの役割と利点・欠点
- トランスポート層の役割と利点・欠点

  パケットをただ投げるだけのUDP

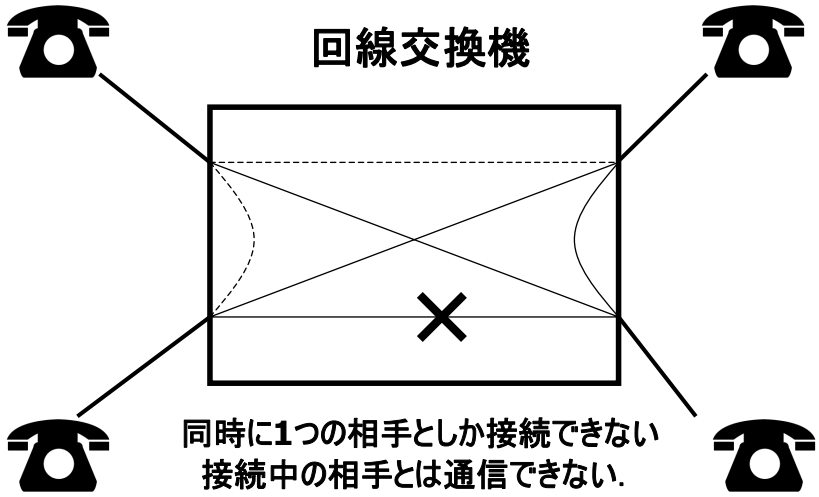
  連続情報の流れをパケットで実現するTCP
- パケット化によるセキュリティの問題

大阪大学

情報をパケットに分ける理由(1)

パケット以前は回線を継ぎ換えていた

- 回線交換＝古い電話の交換技術

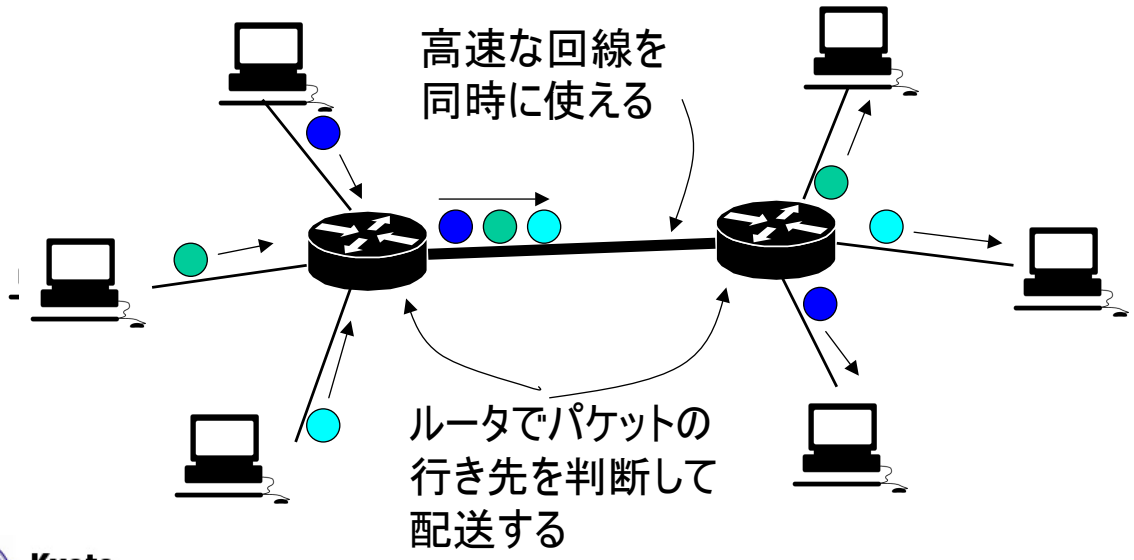


大阪大学

情報をパケットに分ける理由(2)

パケットに分けて送るとみんなで線が使える

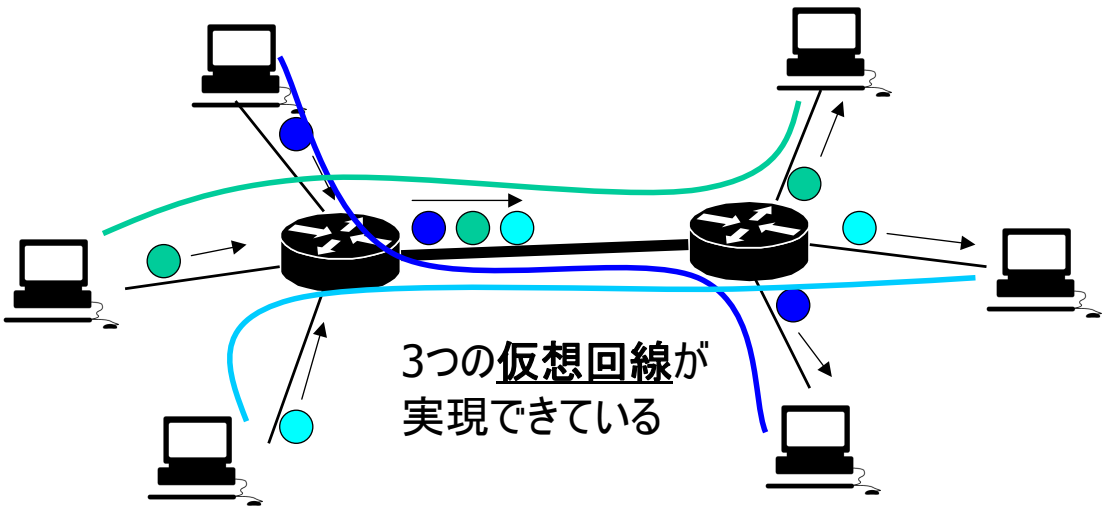
- インターネットでは情報はパケットになっている



情報をパケットに分ける理由(3)

あたかも同時に接続しているように使える

- パケットの流れと物理的配線を切り離せる

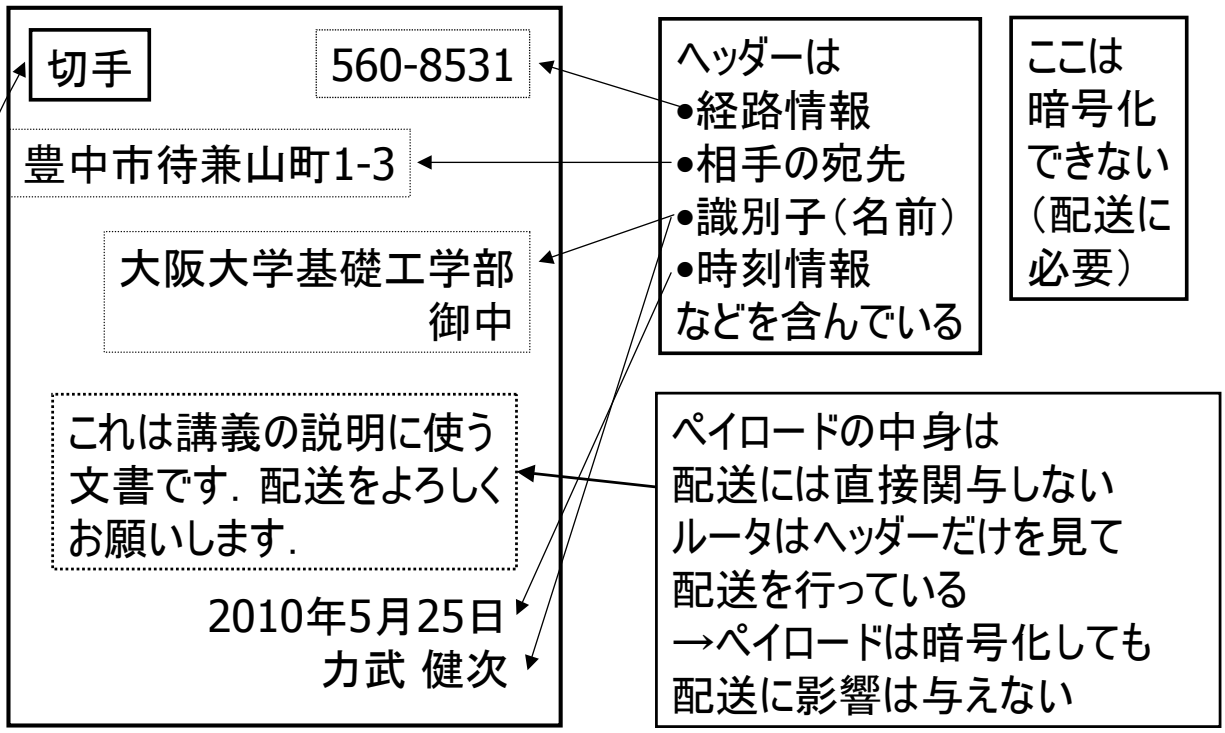


(ところで)パケットとは何か?

- パケット(packet) = ヘッダー + ペイロード
- ヘッダー(header): ペイロードに関する情報
  宛先, 発信元, 通し番号, などなど
- ペイロード(payload): 情報の部分
  1つのパケットで送れる情報量には制限がある
  →大量の情報は多数のパケットに分けて送る
- パケットはなくなることもある
  一定時間以内に届かなければ再送することで対応

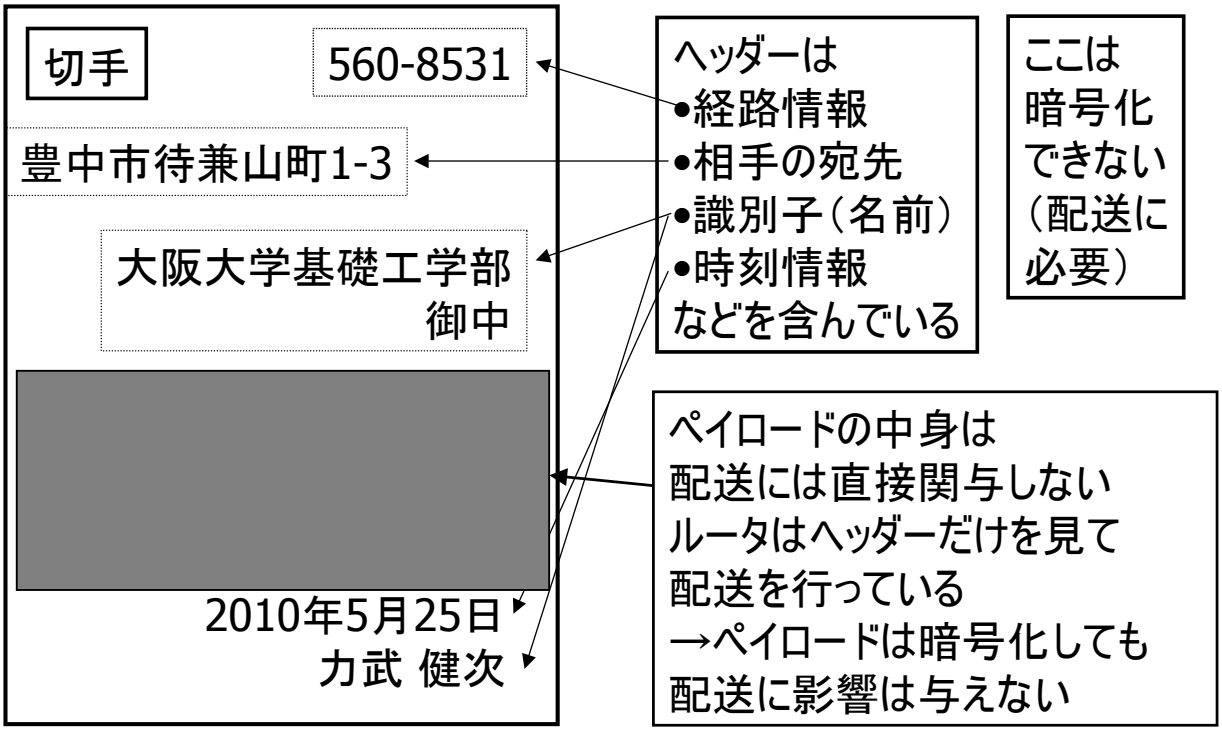
大阪大学

パケットを「はがき」に例えてみると…



大阪大学

暗号化された「はがき」



ペイロードを暗号化しても，はがきは届く（はず）

パケット化の利点と欠点

利点: 複数のやり取りを1つの回線で行える
- 厳密な同期を必要とせずコストが低い

欠点: いつ届くかは厳密にはわからない
- 送った通りの順番で届くとは限らない

構造上の問題: ルータに情報が集中
- パケットを集約し分配する手間がかかる
  ルータは宛先の経路を知っておく必要がある
- ルータで情報を一斉検査(改変)できてしまう

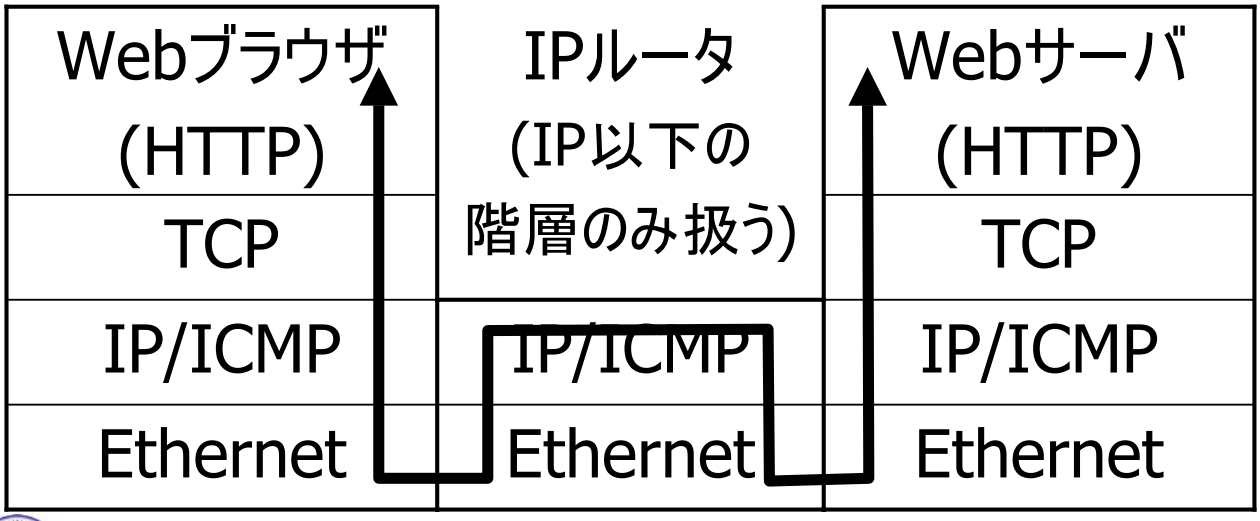
階層別にインターネットを考える(1)

階層ごとに通信の役割が分かれている
- アプリケーション(とプロトコル): Web / HTTP
  ネットワーク上での機能を実現する
- トランスポート: TCP/UDP
  アプリケーション間の情報とパケットを相互変換する
- パケット: IP/ICMP
  パケットを相手に届ける役割を担う
- 物理層: Ethernet, 光ファイバなど

大阪大学

階層別にインターネットを考える(2)

- 各機能階層は同じ階層の相手しか考える必要はない
- 下の階層で何が起こっていても上の階層には見えない
  →各々の階層で暗号化を行うこともできる



大阪大学

IP/ICMPとIP(v4)アドレス

IP: Internet Protocol

- ICMP: Internet Control Message Protocol

  ICMPはIPの一部: 相手と通信できなかったり，アドレスが不正な場合などの制御を担当する

IP(v4)アドレス: 32ビットの整数

- 8ビットごとに0~255までの10進数に分けて書く

  例: 192.168.0.1, 133.1.192.3

大阪大学

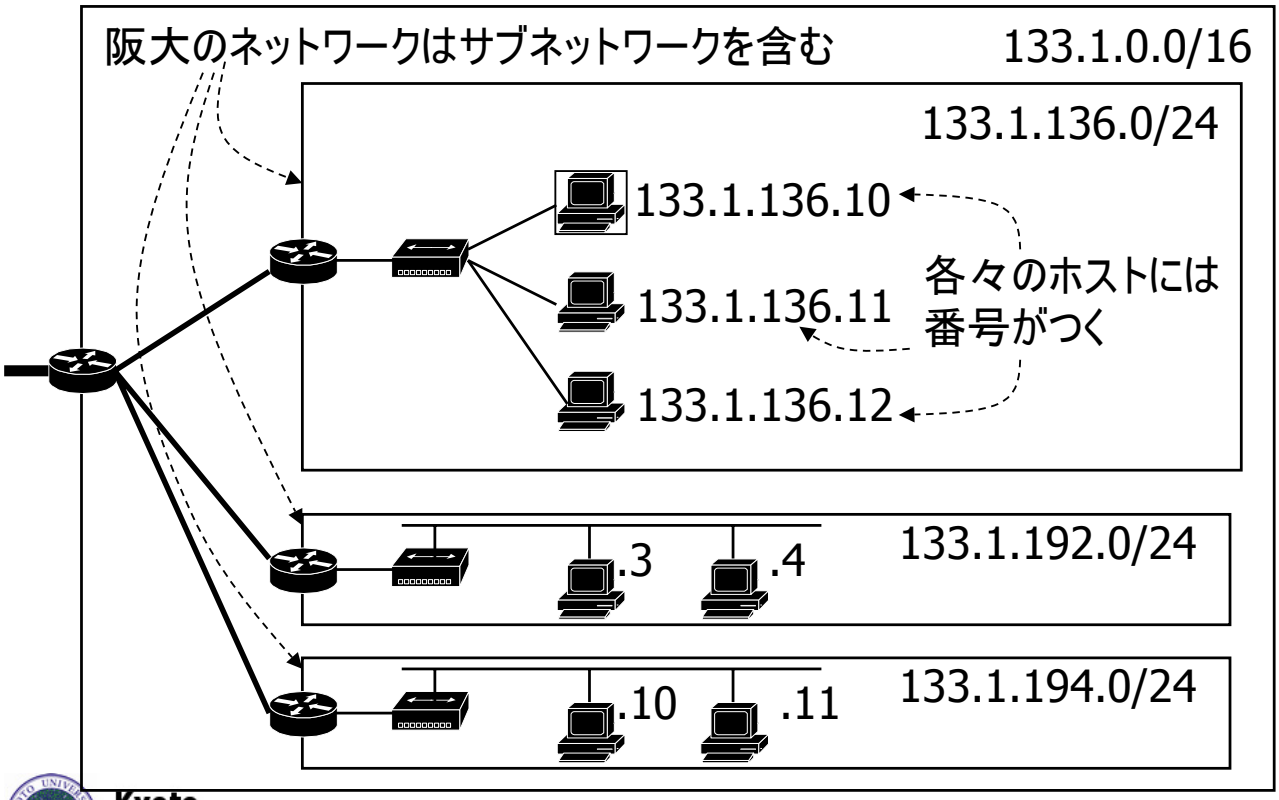
IPアドレスの構造とIPネットワーク

IPアドレス = ネットワーク部 + ホストID

- 例: 192.168.0.1 = 192.168.0.0/24 というネットワーク の ホストID 1番
- ネットワーク部の区切りはどこでつけてもよい
  上位桁のビット数:プレフィクス(prefix)（例: /24）
- ネットワークは別のネットワークを含んでもよい
  例: /16のネットワーク → /24のネットワーク 256個
  再分割されたネットワークを「サブネットワーク」という

大阪大学

IPネットワークとサブネットワークの例



IPアドレスの利点と欠点

利点：物理層に依存しない

- PCやケータイ等区別せずアドレスが付けられる
- 同じ機器が複数のIPアドレスを持っても良い
  役割ごとにIPアドレスを分けている運用も一般的

欠点：ネットワーク間の移動が大変

- 違うIPネットワークでは違うアドレスが必要
- ホスト（機器）と経路の情報を切り離せない
  →IPアドレスでネットワーク上の場所が推定できる

トランスポート層がなぜ必要か（1）

IPはパケットの転送はしても**到達は無保証**

- 送信したパケットが届くかどうかは確認しない
- 順番通りに届くかどうかも一切確認しない
- 送ったはずのパケットはときどきなくなる
  0.1～1%ぐらいのパケットロスは想定する必要がある
  伝送路の雑音や障害
  輻輳（ふくそう，あふれること）によるパケットロス
  転送できなくなるとパケットを捨ててしまう

大阪大学

トランスポート層がなぜ必要か(2)

同じホストでアプリケーションを区別したい

- IPアドレスだけでは区別することができない

ポート番号: 各ホストごとに16ビット

- 宛先ポート番号でアプリケーションを区別する
  HTTP: 80, HTTPS: 443 など
- ポート番号とアドレスの組で接続を表現
  例: 192.168.0.2で動くHTTPサーバへの接続
  {192.168.0.1, 11111}→{192.168.0.2, 80}

大阪大学

UDP: IPとポート番号と中身の検査

UDP (User Datagram Protocol)

- 基本的にはIPにポート番号をつけただけ
  順番は保証されず，重複も発生し得る
  アプリケーションで通信手順を組む必要がある
- チェックサムでパケットごとの誤り検出をする
  内容の誤っているパケットは単に捨てられるだけ
- その代わり伝送は高速で遅延も短い
  音声，動画，DNS(ドメイン名システム)などに使用

大阪大学

TCP: IPの上でのストリームの実現

ストリーム: 以下の条件を満たす通信

- いつ接続したか，切ったかがわかる
- ストリーム上のデータの順番は保証される
- ストリーム上のデータが重複することはない
- ストリーム上に誤ったデータは送信されない

TCP (Transmission Control Protocol)

- ストリームをIP上で実現するための手順
- WebやメールはTCPの上で成立している

大阪大学

TCPのしくみ

ストリームを実現するための機能

- データにはバイト単位の番号が付く
  パケットが届かないとどの部分が抜けたかわかる
  抜けた後の部分が先に届いた場合溜めて待つ
- 一定時間届かなかったら再送を要求

パケット1	~~パケット2~~	パケット3	パケット4
ここまでは→ 確実に届いている	↑↑↑ 届かなかった時は再送を要求	この場合，パケット1までしかアプリケーションには伝わらない （2が届くまで3，4は伝えない）	

TCPの利点と欠点

利点: 楽に使えてネットワーク全体に優しい

- アプリケーションからの利用が簡単
- 輻輳制御をするため多数同時利用に適する

欠点: 通信のタイミングが予想できない

- どうパケットに分割されるかは予想ができない
- データの各部分がいつまでに届くかもわからない

注意: データの改ざんには対応できない

- パケットは偽造される可能性があり得る

トランスポート層プロトコルの使い分け

大半のサービスはTCPの上に成り立っている

- ファイルやストリームにできるものはすべて可

  オンデマンド動画や即時性を持たない動画中継など

  再生速度より遥かに高速に送ることで問題を解決している

即時性の必要なものはUDPでやっている

- インターネット電話の呼び出しなど(SIP)

他のプロトコルも使われていくだろう

- 複数ストリームの状況に応じた選択(SCTP)

次回予告

- 電話やテレビ放送は本当にインターネットで実現できるのだろうか?
- インターネットのアドレスは有限だけど，足りなくなったら，どうしたらいいだろう?
- インターネットは本当に誰に対しても公平で中立な利用環境であり続けられるだろうか?