大阪大学

NiCT 情報通信研究機構 National Institute of Information and Communications Technology

2009年度 電気工学特別講義 第6回
これからのインターネットが抱える技術的・社会的課題

力武 健次
NICT インシデント対策グループ

2009年6月16日

大阪大学

NiCT 情報通信研究機構 National Institute of Information and Communications Technology

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

レポートの課題は別途配ります

講義の要約や案内はWebに出します

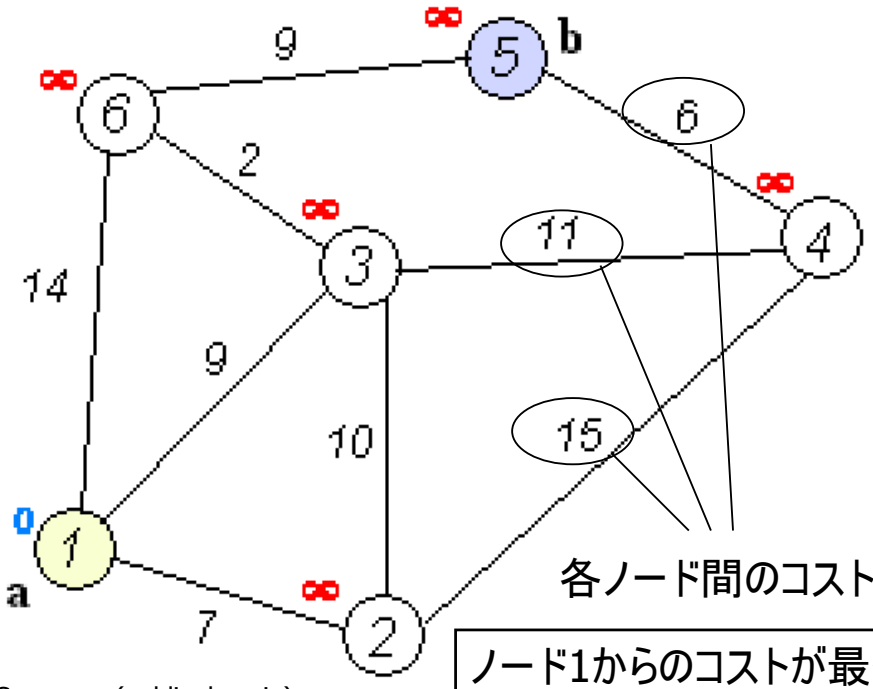
http://www.k2r.org/kenji/jp-oueees2009.html

今日の講義の内容

インターネットが抱える技術的・社会的課題

- ネットワークの経路数/経路情報の問題
  ダイクストラ(Dijkstra)の最短経路問題
- セキュリティとプライバシーに関する問題
- ネットワーク中立性と政治・経済・社会の問題
- クラウド・コンピューティングによる大規模分散システム環境の実現，そしてそれにまつわる問題

最短経路問題(1/5)

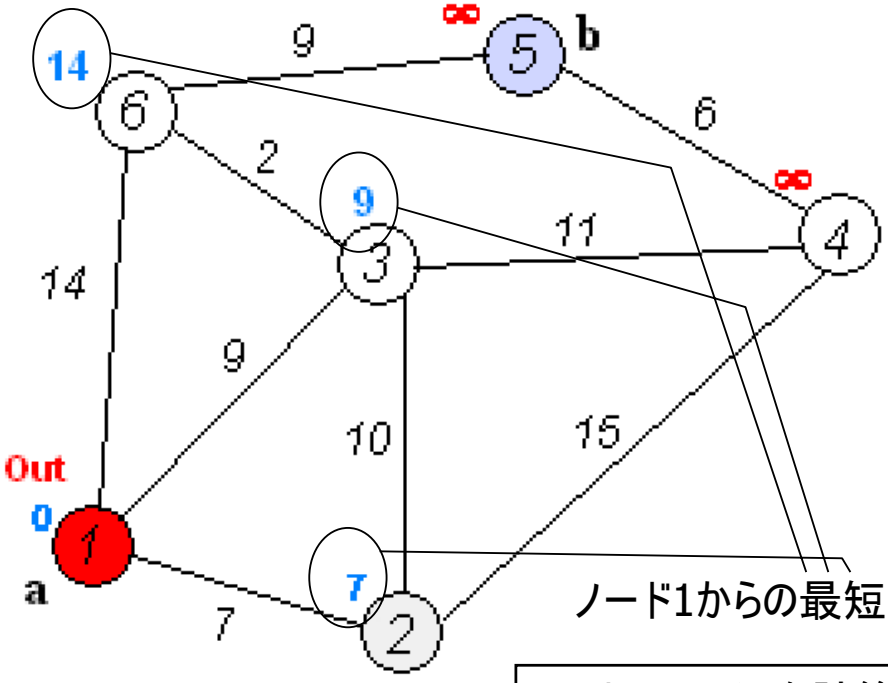


各ノード間のコスト

ノード1からのコストが最低になる
経路を確定しコストを求める

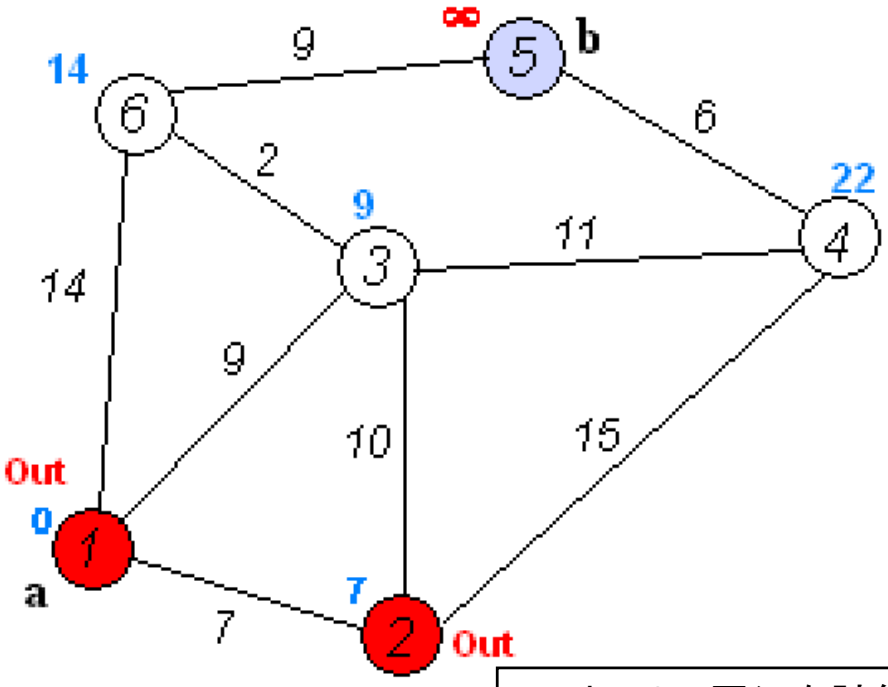
Source: Wikimedia Commons (public domain)
http://commons.wikimedia.org/wiki/File:Dijksta_Anim.gif

最短経路問題(2/5)



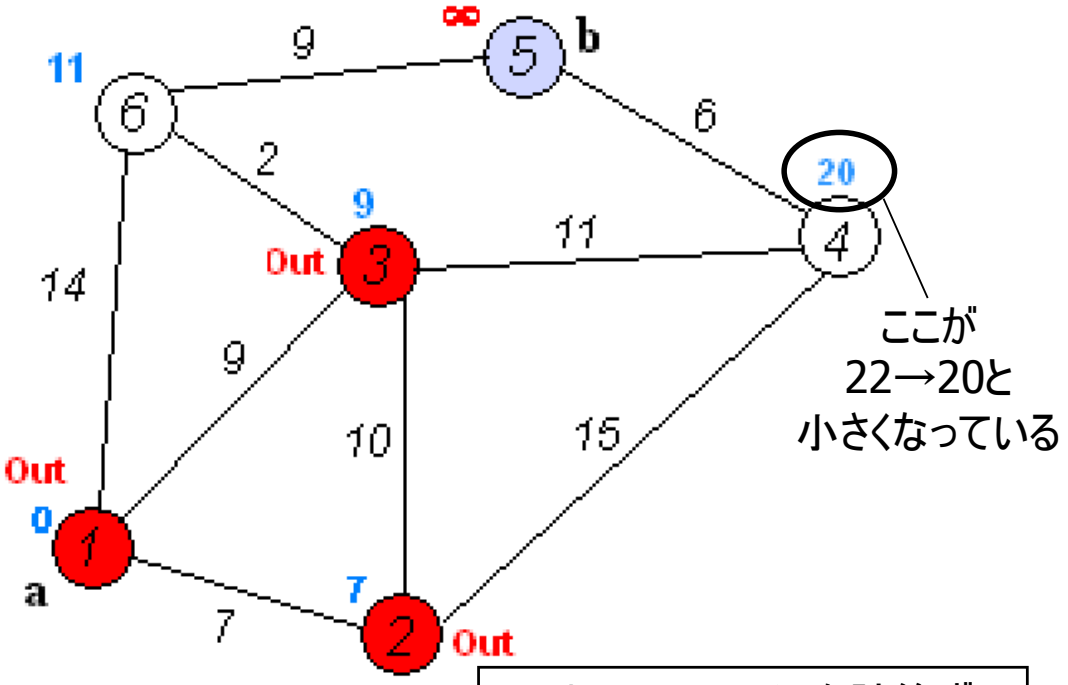
ノード1の周辺を計算ずみ

最短経路問題(3/5)



ノード1,2の周辺を計算ずみ

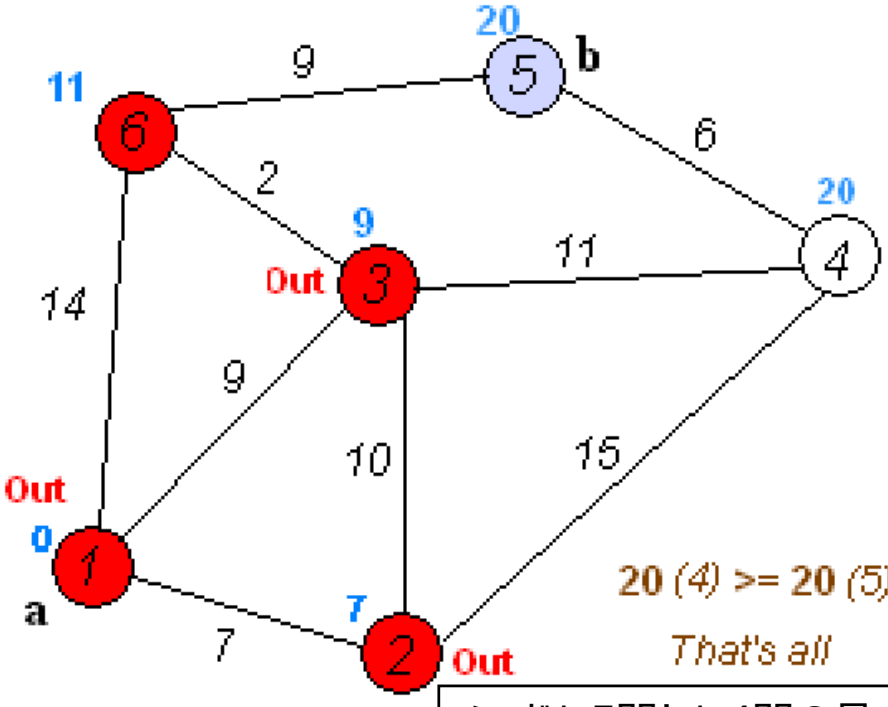
最短経路問題(4/5)



ここが
22→20と
小さくなっている

ノード1,2,3の周辺を計算ずみ

最短経路問題(5/5)



ノード1-5間と1-4間の最小コストは
同じ値なので，これで計算終了

経路数の爆発的増加が最大の技術課題

つなぐ相手が増えるほど経路数も増える

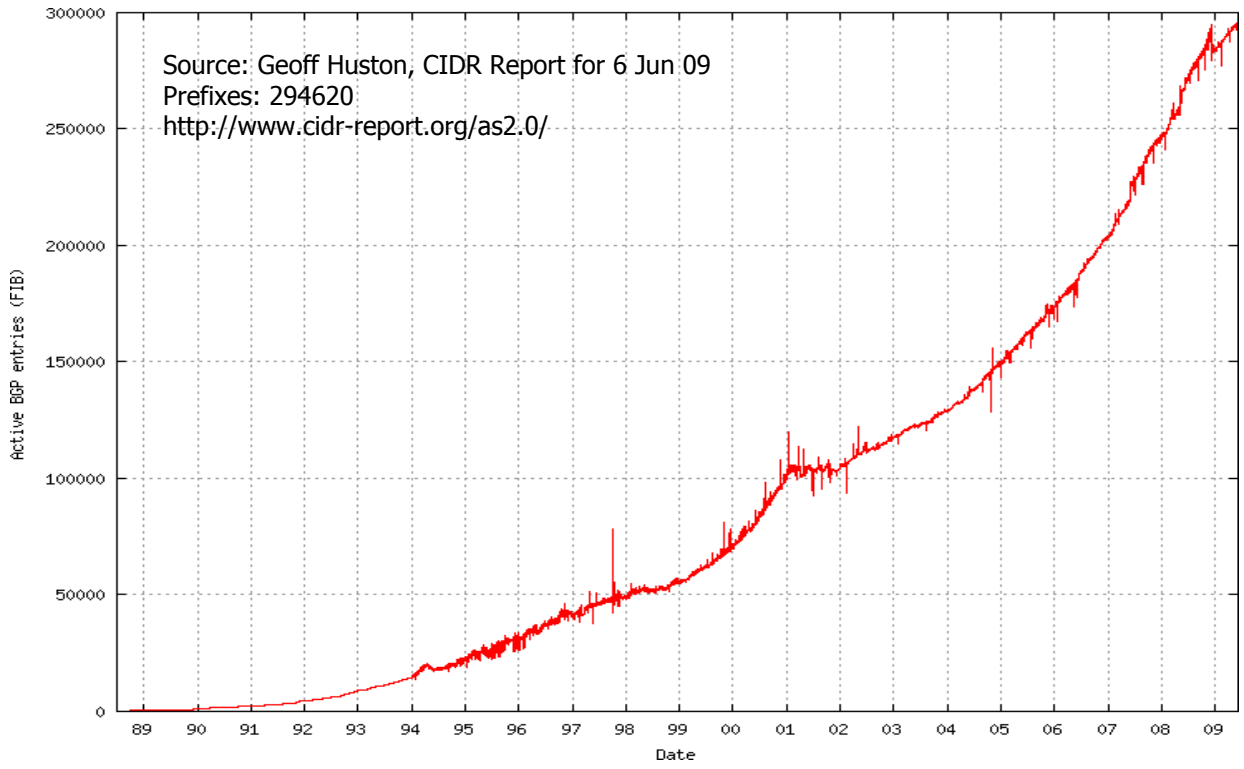
経路数の問題はIPv4でもIPv6でも同じ

- どこかで経路集約をしない限り減ることはない
  - 経路集約の障害要因は社会的/政治的なもの
    - 国境，組織間の壁，新規機器へのコストが払えない，etc.

各ルータの計算量はノード数の2乗に比例

- ノード数が100倍→計算量は10000倍
- 最適経路は変動するため常に再計算が必要

爆発するBGP経路数(IPv4)



「情報セキュリティ」の意味(1)

間違いや誤動作は永遠になくならない

- 人間は基本的に間違える

プログラミングエラーによる事故の例

- 1999年 Mars Climate Orbiter
  メートル法とヤード・ポンド法の換算間違いで墜落
- 2009年3月 Airbus A340-500
  燃料量の入力間違いで離陸時のしりもち事故
  （2004年10月には同じ理由で747貨物機が墜落）

「情報セキュリティ」の意味(2)

安全性と速度/コスト節約は両立できない

- 機器を高速にするために値のチェックを省く
  →外部から任意の命令を送り込まれてしまう
- 早く製品を世に出すために試験を省く
  →実用に耐えない情報システムが世に出てしまう
- コストを下げるために必要な部品の購入を省く
  →当該部品の故障や有効期限切れで大事故
  1986年1月28日: スペースシャトルの爆発事故
  2008年9月14日: ANAの発券システムが停止

「情報セキュリティ」の意味(3)

完全なID管理(による認証)は不可能

- インストールの時に証明書をチェックしてますか?

人間をだますのは安上がり

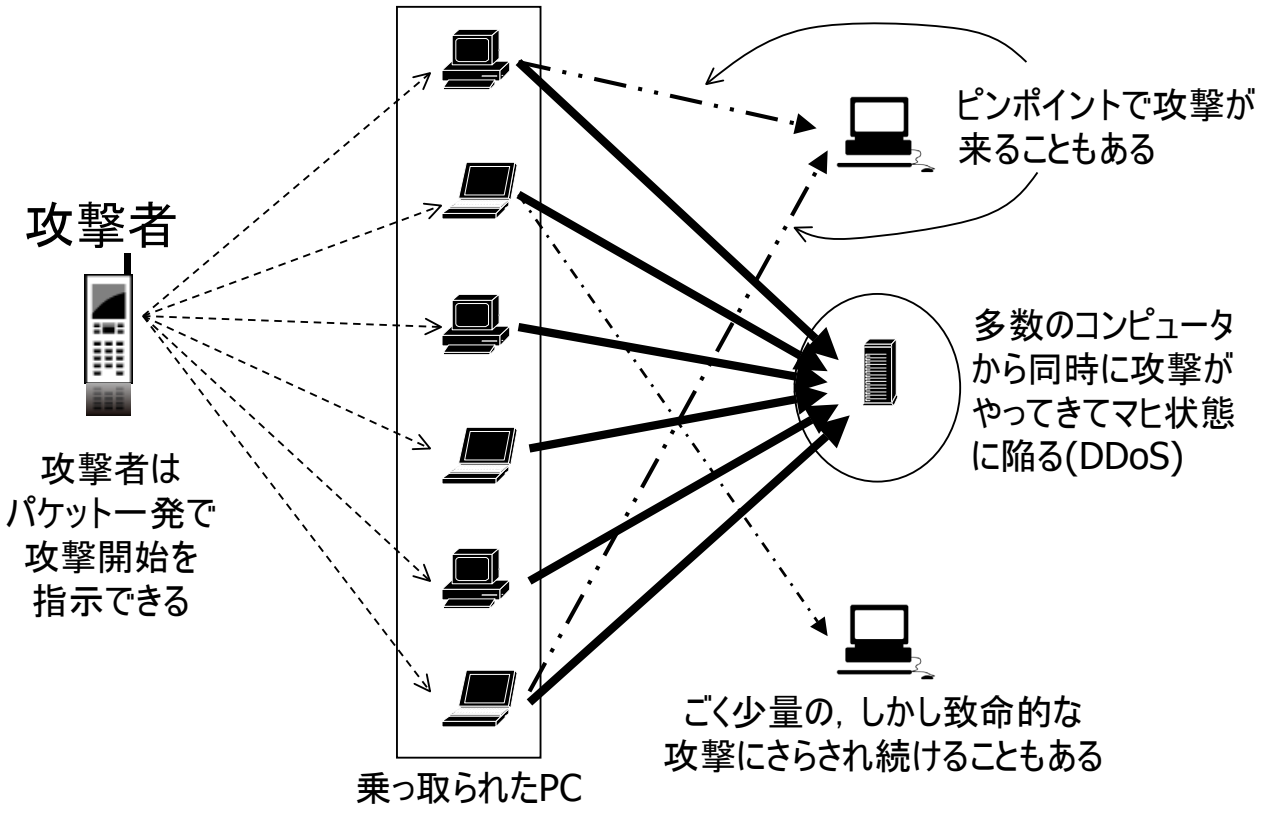
- 「振り込め詐欺」: 年間数百億円規模
  民事の詐欺ではまずお金は返ってきません!
- social engineering
  誘導尋問: mixiの「バトン」やアンケートなども注意
  phishing: 有効に防護する方法がない

「情報セキュリティ」の意味(4)

人間の犯罪の道具にインターネットを使う

- マルウェア(ウイルス)が仕込まれる理由
  無防備なコンピュータを乗っ取る
  攻撃者を直接探知できなくなってしまう
- 同時に多数のコンピュータを攻撃に使う
  大量のパケット処理を強要して相手をマヒさせる
  →Denial-of-Service (DoS)攻撃
  各所に分散(Distributed)したDDoS攻撃も一般的

間接的な攻撃の怖さ



「情報セキュリティ」の意味(5)

普通の犯罪をコンピュータを使って行う時代

- キーロガーを仕掛けて秘密情報を盗み取る
- 気に入らない相手のアカウントを消去する
- 他人になりすますことで損害を与える

攻撃相手をすぐに特定できない恐ろしさ

- (日本では特に)匿名の誹謗中傷が一般的
- しかし司法当局も黙って見てはいない

  ブログ「炎上」の加害者を特定し逮捕

「情報セキュリティ」の意味(6)

では，情報セキュリティの仕事とは何?

- 悪いことをしにくくする技術の研究開発と実証
  - 暗号技術に基づく盗聴されにくい通信方式の実現
  - プロトコル脆弱性の対策とより安全な設計法の確立
- セキュリティ事故の早期発見と予防
  - 個別事例の詳細分析で対策に役立つ情報を得る
  - ネットワーク全体の活動観測による事故傾向の予測
- 個人の基本的人権は制限できない

再び「ネットワーク中立性」について

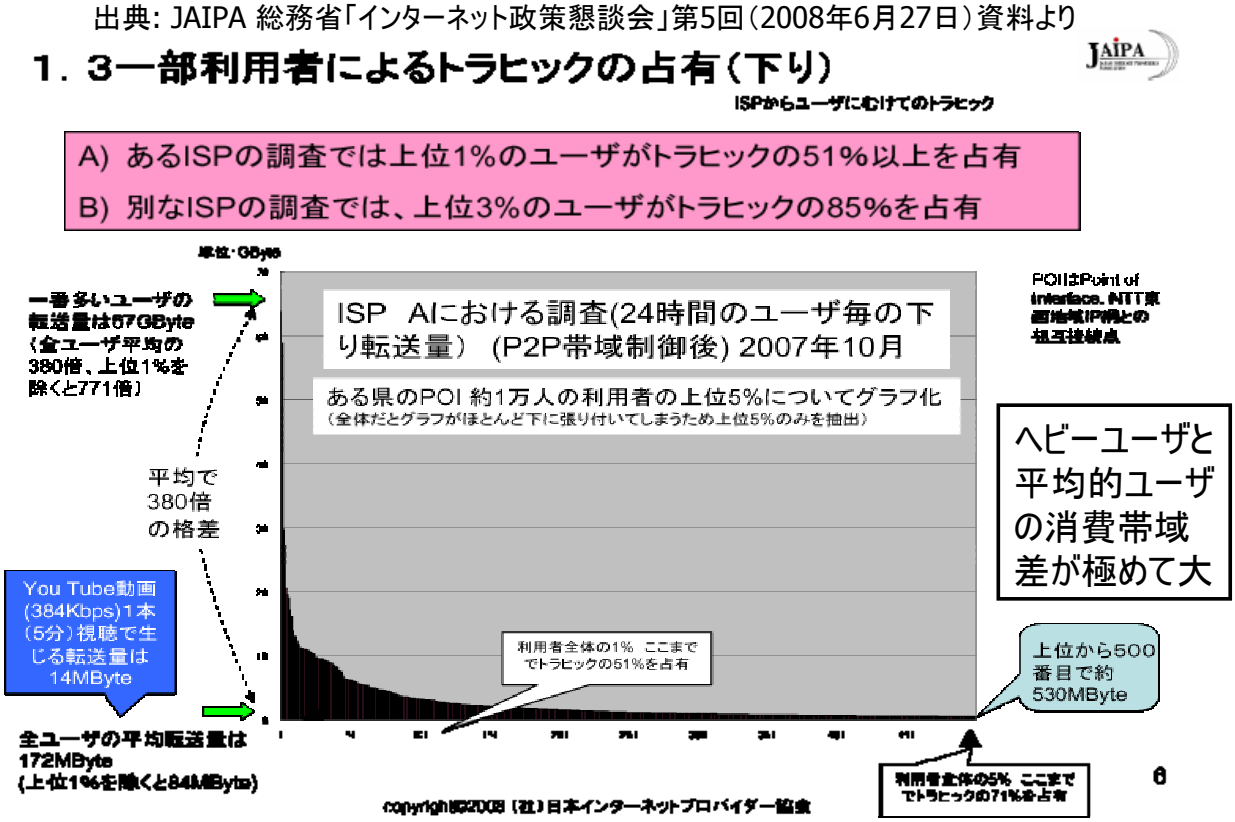
総務省の考える論点は2つ

- ネットワークのコスト負担の公平性
  - ブロードバンド普及でネットワークが混雑し始めている
  - アプリ別帯域制御だけでは制御しきれない
  - 上位1～3%の利用者が帯域の50～90%を占有
- ネットワークの利用の公平性
  - NGNか従来のインターネットかという選択の自由
  - サービスプラットホームの適正対価の利用の自由

出典: 谷脇康彦「ネットワークの中立性と競争政策」, 信学通誌, No. 9, 2009年6月, pp. 20～28.

一部利用者によるトラフィックの占有（下り）

出典: JAIPA 総務省「インターネット政策懇談会」第5回（2008年6月27日）資料より



http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/internet_policy/pdf/080627_2_si5-2.pdf

中立性を阻害する要因

言論の自由の制限

- 国家，地域政府，あるいはISPに対する批判

既存メディアとの利害対立

- テレビ，新聞，広告代理店，出版社の寡占

一部の利用者が大部分の帯域を使う現象

- 文字→動画へとより広い帯域への要求

誰が中立性を守るのか?

- 政府? ISP? 技術者? 創作者? 利用者?

クラウドコンピューティングとは

クラウド(cloud: 雲)の意味

- インターネットも雲に例えられる
- 通信機能だけでなく，コンピュータの機能までネットワークの雲の中に取り込まれるイメージ
- 決して crowd = 群集 や crowded =混雑，などではない (l と r は間違えないように)

もっとも，クラウドコンピューティングの提供システムが混雑で使い勝手が悪くなるのは時間の問題かも…

クラウドコンピューティングの技術的背景

コンピュータの単独性能の向上は難しい

- 電力消費，発熱，集中によるボトルネック

大量のコンピュータに分散して作業をさせる

- 複数CPU(コア)を持つコンピュータの普及
- 並行処理，並列処理による計算能力の向上

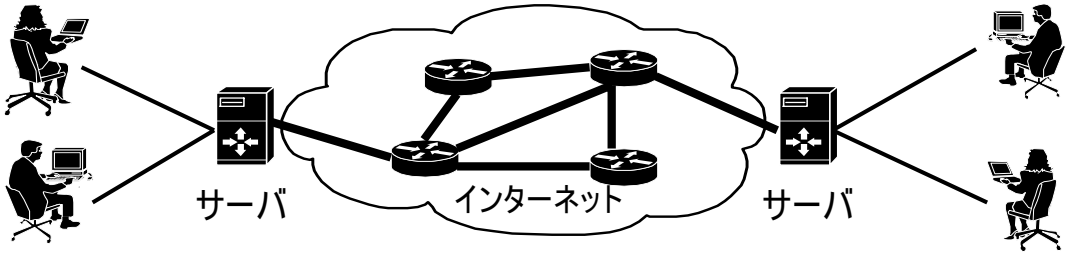
発想の転換とソフトウェアの全面変更を必要とする

- 一部が壊れても全体が壊れないシステム構成

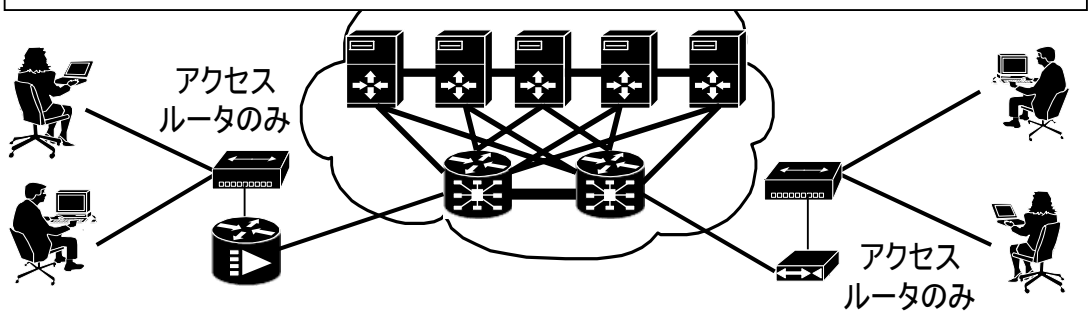
安いPCなら壊れても取り替えがすぐにできる

クラウドコンピューティングのイメージ

今はそれぞれの組織でサーバやルータを持ち，それらをインターネットに接続している



高機能ルータと冗長性を高めたコンピュータの大規模集合から成るクラウド



クラウドコンピューティングではコンピュータがネットワークに取り込まれ一体化する

クラウドのシステムに必要な能力

柔軟な機器構成

- CPU，ストレージ，サーバの能力は増減が自由
  需要の変動に応じて自由に割り当てを変えられる
- 故障しても予備機材に切り替わる
  ユーザには故障の状態はわからない程の高冗長性
- 自分で機器を所有するより安くできる
  使った記憶容量や通信量の分だけ課金される
- Webなどで統一して使うことができる

すでにクラウド的運用手法は普及している

冗長性を高めたWebサービスの大多数
- Google Apps, flickr, Twitter, Yahoo!, etc.

特定用途向け情報システムの普及
- Salesforce (SaaS), Akamai (CDN) など

クラウドコンピューティング開発基盤の普及
- Amazon Web Services (AWS)

  ストレージ(S3)，CPU(EC2)，その他データベースなど

  複数地域での冗長性確保や課金機能まで統合

クラウドの利点と問題点

利点: 機器なしの柔軟なシステム設計
- 自分でハードウェアの保守をする必要がない
- 処理能力の増大には契約変更で対応できる

欠点: データの所在や安全性が不透明
- データはクラウドの「向こう側」に行ってしまう

  フルバックアップを手元に置くと利点が減ってしまう
- データの消失に対する保証は誰がするのか?
- 国や地域の境を越えた場合の法的問題は?

レポート課題の要点

クラウドコンピューティングでこれからどうなる?

- 政治，経済，社会的な問題とのかかわり
- 並行処理化で変わるシステム構築技術
- データの所有権や利用権とプライバシーは?
- そしてインターネットにもたらす変化は?

これからのことですから誰も答は知りません

- 皆さんの頭で考えて文章で書いてみてください