2010年度 電気工学特別講義 第6回
今後のインターネットサービスが抱える セキュリティ課題

力武 健次
京都大学
学術情報メディアセンター
2010年6月8日

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

アンケート課題の用紙は別途配ります

講義の要約や案内はWebに出します

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

- 「情報セキュリティ」の経験則
- ネットワークの経路数/経路情報
- ネットワーク中立性と政治・経済・社会
- クラウド環境と情報の安全性

この授業の最後にアンケートをお願いします

- 成績評価以外の目的では使用しません

「情報セキュリティ」の経験則(1)

間違いや誤動作は永遠になくならない

- 人間は数%の確率で必ず間違える

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

大阪大学

「情報セキュリティ」の経験則(2)

安全と時間短縮/コスト節約は両立しない

- 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
  データベースの不正操作: SQL injection
- 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

Kyoto University

大阪大学

「情報セキュリティ」の経験則(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?
- そもそも証明書の発行元を信用できるか?

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: アンケートや占いサイトなども注意

Kyoto University

大阪大学

「情報セキュリティ」の経験則(4)

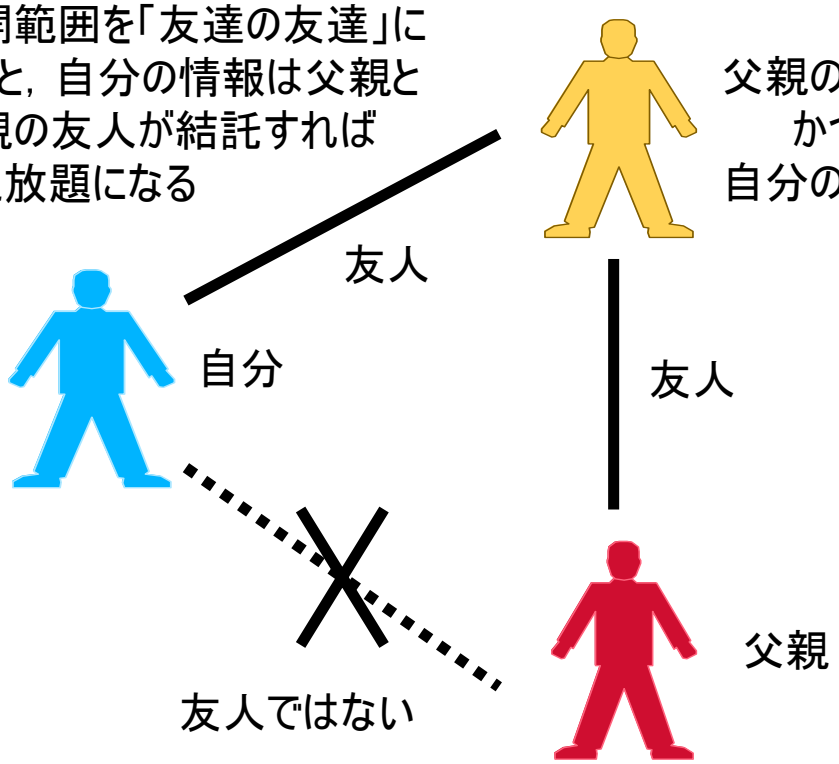
プライバシーを守らせない仕組み

- Facebook: 既定値が「公開」になっている
  会員でなくても書き込み内容が検索し放題
- opt-out原則＝何も言わなければ参加
  「opt-in＝何も言わなければ参加しない」であるべき
- 「信頼の連鎖」モデルの限界
  「友達の友達」は友達，では秘密は守れない
- 理由: 個人の行動履歴は営業に大変有効

大阪大学

「友達の友達」が友達でない例

公開範囲を「友達の友達」にすると，自分の情報は父親と父親の友人が結託すれば見え放題になる



大阪大学

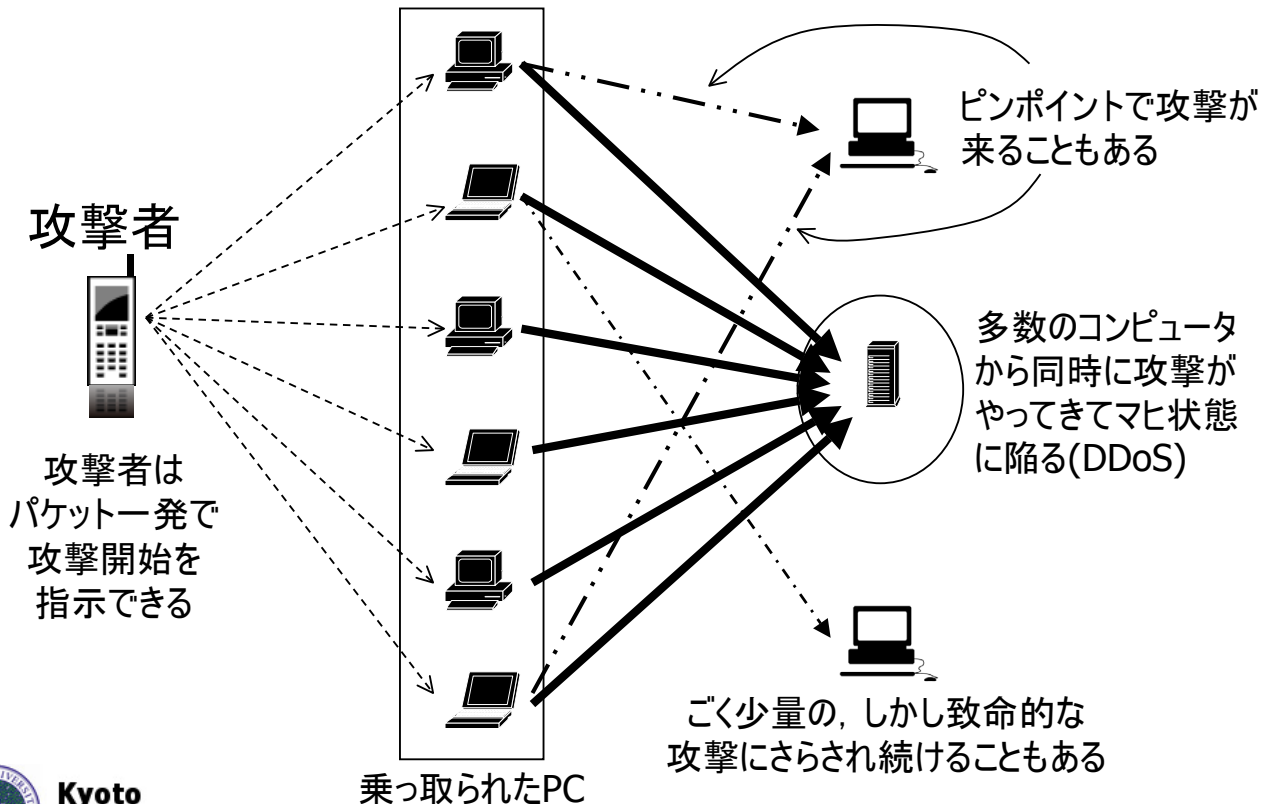
「情報セキュリティ」の経験則(5)

インターネットは犯罪攻撃の道具になった

- 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
    - 2008年: ロシア・グルジア間の戦争で大規模に使用

大阪大学

間接的な攻撃の怖さ



大阪大学

「情報セキュリティ」の経験則(6)

普通にコンピュータで悪事を働く時代

- 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

攻撃相手をすぐに特定できない恐ろしさ

- 匿名の誹謗中傷が世界的に増加中

しかし黙認される時代はもう終わった

大学でも学内ネットの利用規程を作り，不正行為は学内で見つけて対処するところが増えています

Kyoto University

大阪大学

「情報セキュリティ」の仕事

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

とはいえ「正当な権利」は制限できない

大学であれば「教育・研究活動」の自由は優先事項

Kyoto University

大阪大学

最大の技術課題: 経路数の爆発的増加

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.

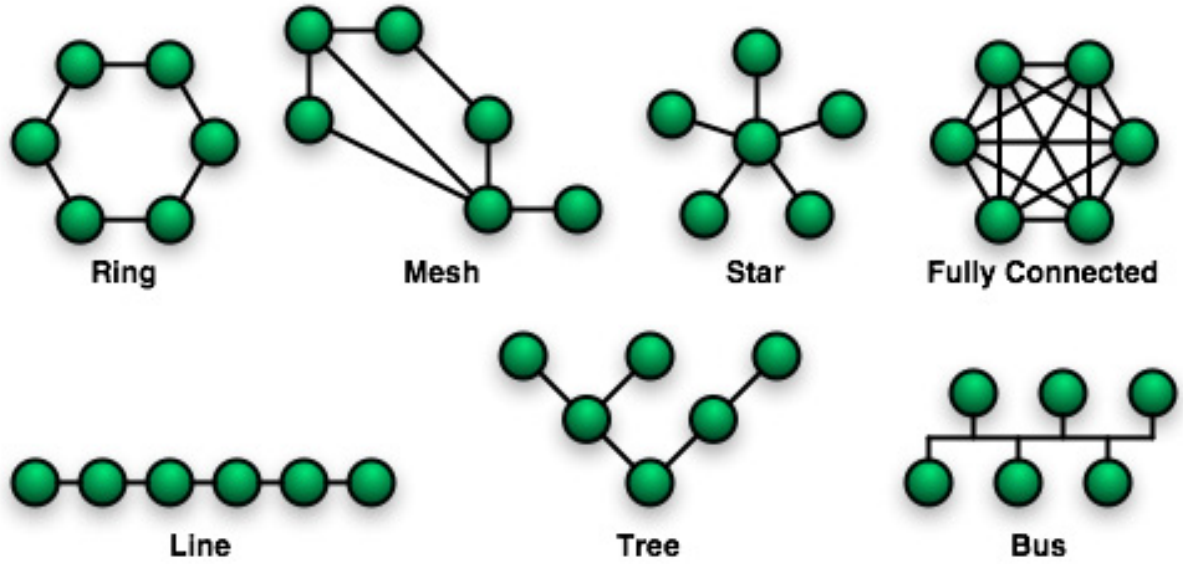
各ルータの計算量はノード数の2乗に比例

- ノード数が10倍→計算量は100倍
- 最適経路は変動するため常に再計算が必要

大阪大学

経路構成の例（トポロジー）

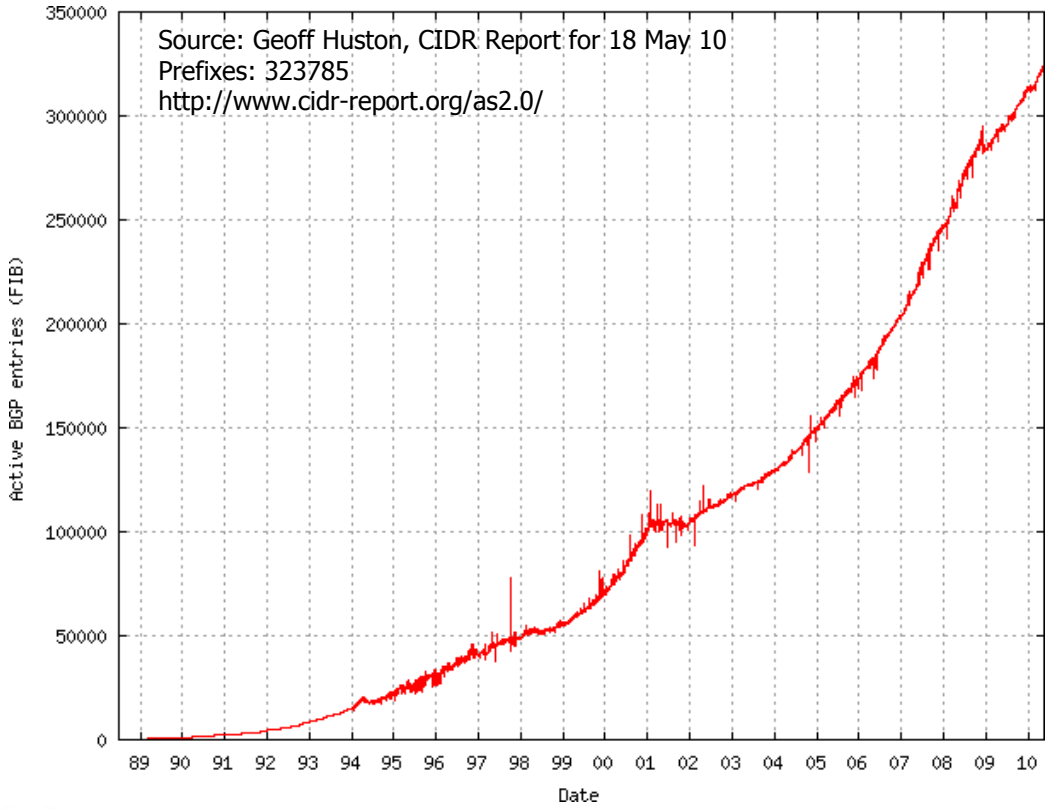
実際には2点接続間の速度，遅延，帯域などで決まるコストに配慮して
最適な経路を逐次計算し直していく必要がある



Source: http://en.wikipedia.org/wiki/File:NetworkTopologies.png

大阪大学

爆発するBGP経路数(IPv4)



Kyoto University

大阪大学

「ネットワーク中立性」について

総務省の論点(2009年夏)

- 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

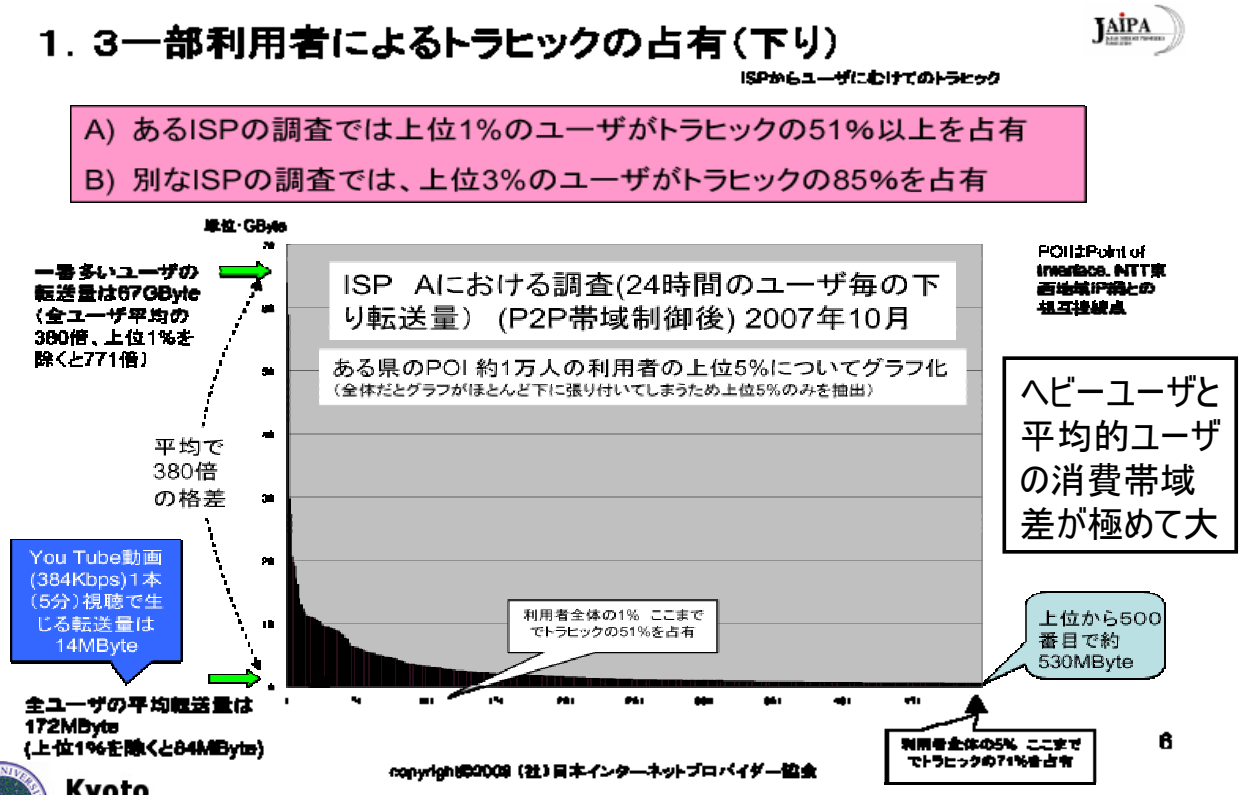
出典: 谷脇康彦「ネットワークの中立性と競争政策」, 信学通誌, No. 9, 2009年6月, pp. 20～28.

Kyoto University

大阪大学

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



Kyoto University

大阪大学

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

中立性は本当に守られていくのだろうか?

Kyoto University

大阪大学

インターネットを動かすためのお金の話(1)

1990年代前半は仕事には使えなかった

- 研究目的用ネットワーク: 営利利用の禁止
- 財源はほとんど（各国の）学術研究費

インターネットの回線そのものでは儲からない

- ひたすら増えつづける利用者の帯域要求
  文字→音声→静止画→動画 + ファイル共有
- 国際回線の敷設には莫大な金額がかかる
  太平洋の底に海底ケーブルを引かないといけない

大阪大学

インターネットを動かすためのお金の話(2)

2000年代: 突如として広告ビジネスに変身

- Googleの検索キーワードとの連動広告
- 物品販売に誘導する「アフィリエイト」広告
- Page viewの「視聴率」化による出来高払い

しかし経済崩壊で広告業界が総崩れ

- 誰も払えないからツケは利用者に回ってくる
- 「無料」サービスの消滅（すでに中小では顕著）
- 課金前提への徹底した差別化の開始

インターネットサービスのクラウド環境化

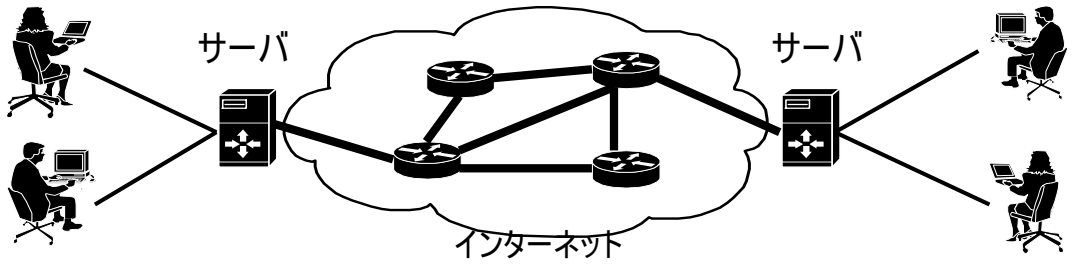
冗長性を高めたWebサービスの大多数
- Google, Twitter, Yahoo!, Facebook, etc.

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

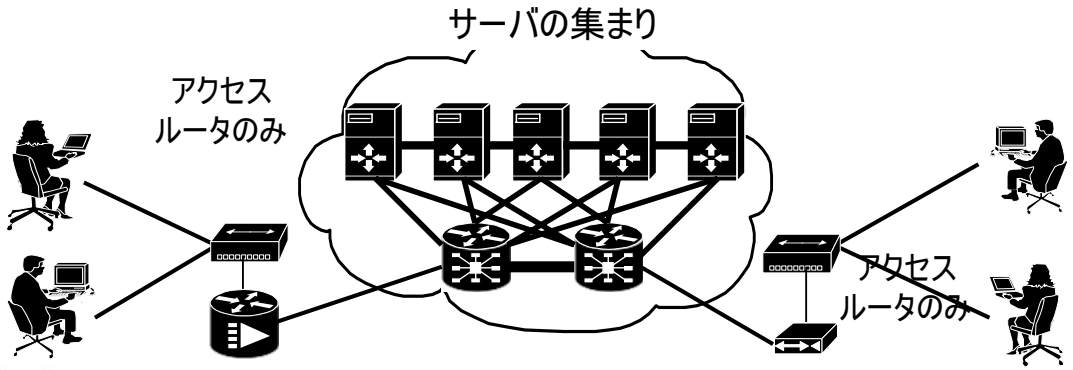
クラウド開発基盤の普及
- Amazon Web Services (AWS)
  複数地域での冗長性確保や課金機能まで統合
- Google Application Engine

クラウド環境のイメージ

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



クラウド環境では**コンピュータがネットワークに取り込まれ一体化**する



クラウド環境の技術的背景

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

クラウド環境の構成要件

柔軟な機器構成が可能であること

- 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可能性
  使った記憶容量や通信量の分だけ課金される
- Webなどで統一して扱うことができる

クラウドの利点と課題

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

課題: 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?

アンケート課題(20分)

1. ネット上のやり取りと, それ以外とでは, どちらが秘密の話がしやすいと思いますか? 理由も書いてください.
2. ネットが原因で生活上の被害を被ったことがありますか. それはどんなことでしたか.
3. その他, インターネットが現代の, そして未来の私達の生活に及ぼすであろう影響について, 思うところを自由に述べてください.