# だれでも使えるセキュアな端末
# - Plug and Play Security の実現に向けて -

Secured Terminal for Dummies

- On the Realization of Plug and Play Security -

宮川　晋

NTTコミュニケーションズ株式会社

慶應義塾大学SFC研究所

WIDEプロジェクト

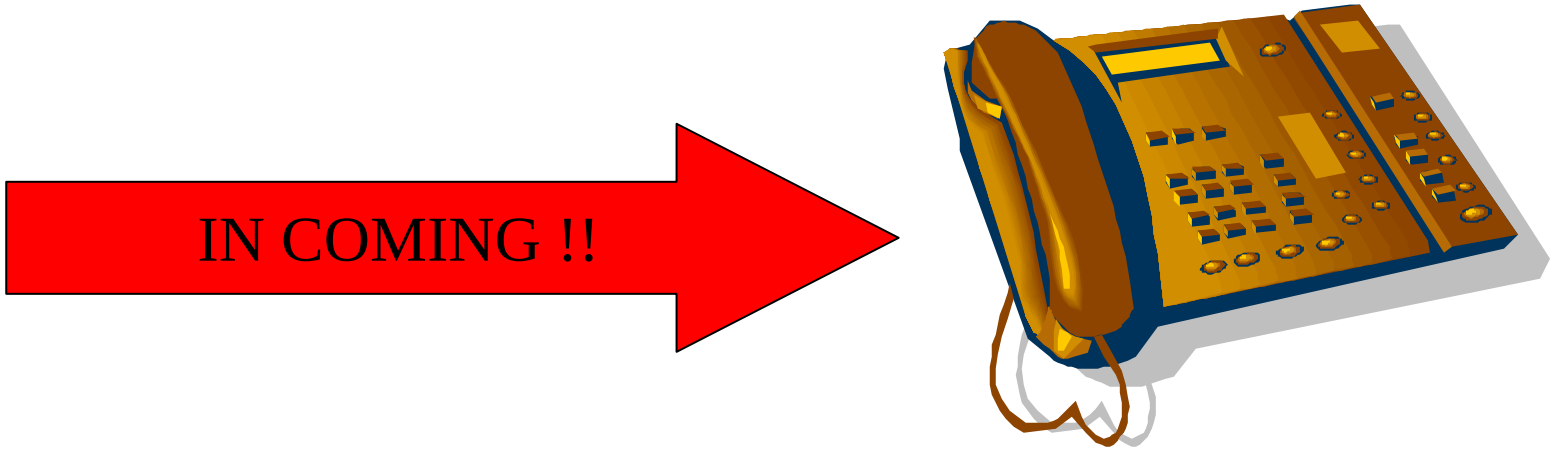
miyakawa@{nttv6, wide.ad}.jp

# IPv6の目的

- もともとはIPv4のアドレスが足りなくなることへの対処
  - 実際にこれは今でも重要な課題である。
  - 残っているIPv4アドレス空間に関する推定値:
    - 2020年頃にはIANAから消滅
    - 2025年頃にはRIRから消滅
    - 2030年頃には完全に消滅
    - 2015年頃には割り当てが困難になるものと推定
- しかし、より重要なのは
  - Peer2Peerアプリケーションへの応用
    - クライアント･サーバ型ではないアプリケーション
    - IN-COMING CALLの実現
  - 自動設定（Plug and PlayあるいはAuto-configuration)によるユーザ数の拡大
  - IPSECの多用によるセキュリティ増進

# P2Pアプリケーション

- 代表例
  - 「かかってくることのあるVoIP」
    - 動きまわるものだとさらに完璧



# プラグアンドプレイ

- 店で端末を買ってきたらすぐに挿して使えること
- ユーザからみて実質的に自動設定できることが重要
  - ユーザの集合を広げるための絶対条件
- 1億2千万人の人口の日本で
  - インターネットユーザは2000万から3000万　(独自推計)
  - 携帯でのネットワークのユーザは7000万　　(同上)
  - すなわち5000万人は携帯は使うがインターネットは使わない
  - なんで？　だって、使うのが大変なんだもの
    - 私の義姉はWindows Updateでさえ面倒くさがる
    - ADSLルータの設定なんてできるわけない
- 私のおばあちゃんも使えますか？
  - Non Technical Peopleこそ（適切な範囲で）お金を払ってくれる･･･はずだ

# セキュリティの確保

- 「セキュリティ」とは便利な言葉だが・・・
- とにかくセキュリティは重要だとされている
  - そもそもセキュリティとは？一般に以下のようなことをいうようだ
    - 認証
      - コミュニケーションしている相手がだれなのか特定したい
    - 秘匿
      - コミュニケーションの内容を第三者から隠蔽したい
    - 改竄防止
      - コミュニケーションの内容を第三者に書き換えられたくない
    - 他にもあるかも
- ネットワーク管理者は別の「セキュリティ」を気にする
    - 勝手に秘話通信されると困る
      - 社員が情報の持ち出しをしていないかチェックしたい
      - ネットワークを目的外に使用していないか調べたい

# P2Pとセキュリティとプラグアンドプレイの矛盾

- 挿すだけで使える、けれど、その場合
  - 自分をIDENTIFYするにはどうしたらいいのか？
  - 何もしないのに「自分」であることは示せない
- ファイアウォールは？
  - IN-COMING CALLはどうしたらいいの？
  - ファイアウォールに穴を開けるしかないが…
- 名前解決
  - 挿すだけで使えるとして、どうやって相手を探す？
  - 相手が本当にコンタクトしたい相手だとどうやって確認する？
- 管理したい人、どう納得させるか？
  - 組織のセキュリティ VS 個人のセキュリティ

# 自動設定

- 端末に対する何らかの入力の必要性
  - キー／ユーザIDとパスワード･パスフレーズ
  - あるいは証明書
  - 以上の混合あるいはバリエーション
    - 生体認証、IC-CARDなどはネットワーク側から見たときには、証明書やパスワードなどと本質的な差はない
    - 通信路での偽造やリプレイアタックなどに関しての安全性も考えないといけない
- すなわちプラグアンドプレイの認証には「入力」を自動設定することが必然的
  - であるが、インターネットの端末をNon Technical Peopleが設定することには無理がある。

# 頭を切り替えて・・・

- 電話を使うときに、電話番号以外の、なんらかの入力をしていますか？
- 課金を行われることに異存はありませんか？

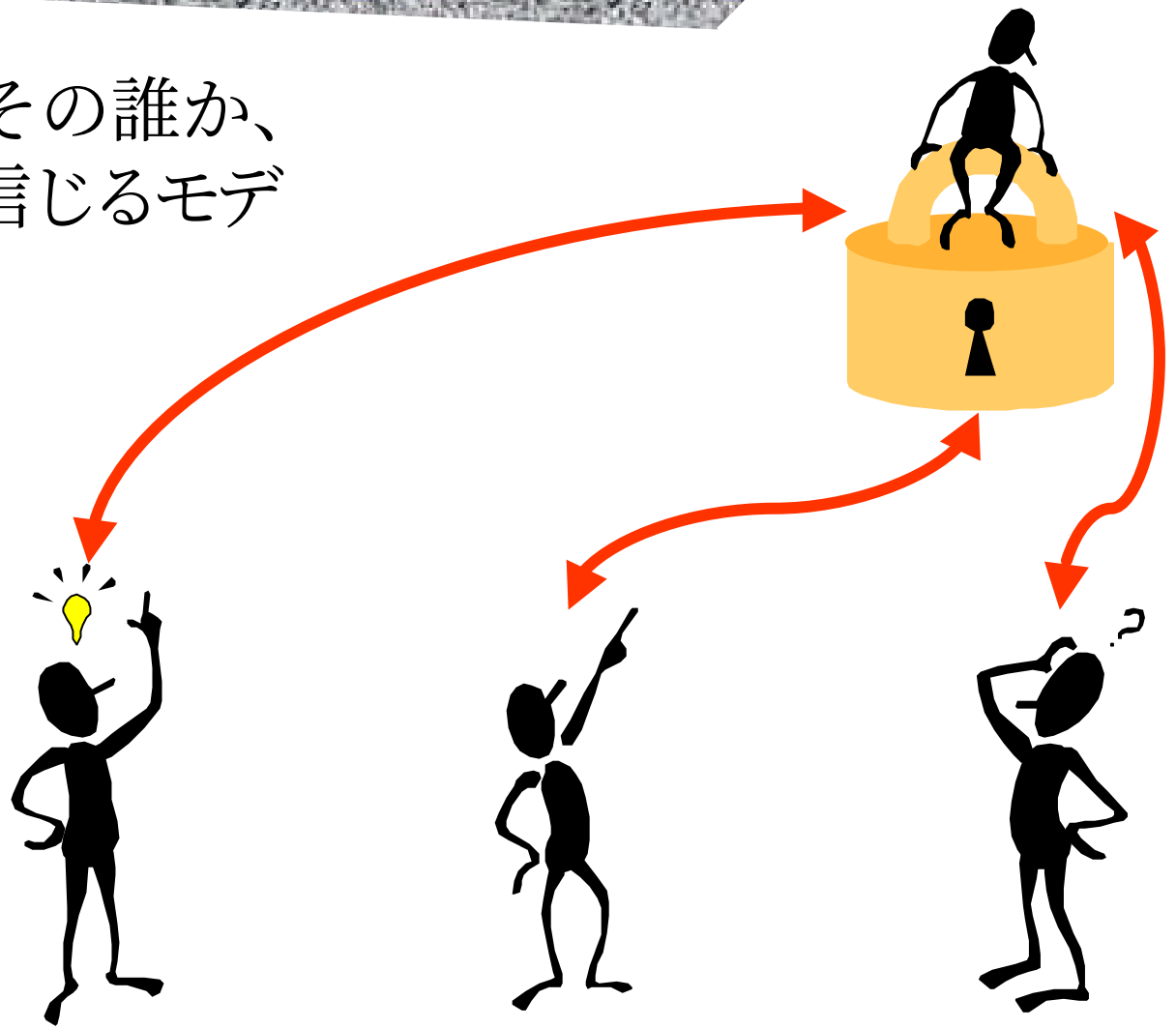
真のプラグアンドプレイ端末

# 純粋インターネットと電話の違い

- インターネットのもともとの特性
  - エンドツーエンド
  - すべての機能は端末に
  - ネットワークはパケットの転送だけをおこなう
  - 　難しいことはDNSに押し付けてある)
- 電話
  - ネットワークが機能を持つ
  - 端末は従属的に動く

# 3rd Trusted Party Model

- 誰かを信じ、その誰か、が言うことを信じるモデル



# セキュリティvs使いやすさ

- 一般にセキュリティと使いやすさはトレードオフの関係にあるとされる
- 3rd trusted partyを受容することができるならば、解消できる
  - その特定第三者に関しての信用の範囲内においてセキュリティ（特にプライバシ）は保護される

# ファイアウォール制御

- 外からファイアウォールを開けてもらうという仕掛けはどうやったら作れるか？
  - エンドツーエンドモデルでは固定的な相手からの通信ならばなんとかなるが、
  - 相手がモーバイルだとお手上げにちかい
- 3rd trusted partyを仮定できれば問題は解決

# 管理者 vsプライバシ

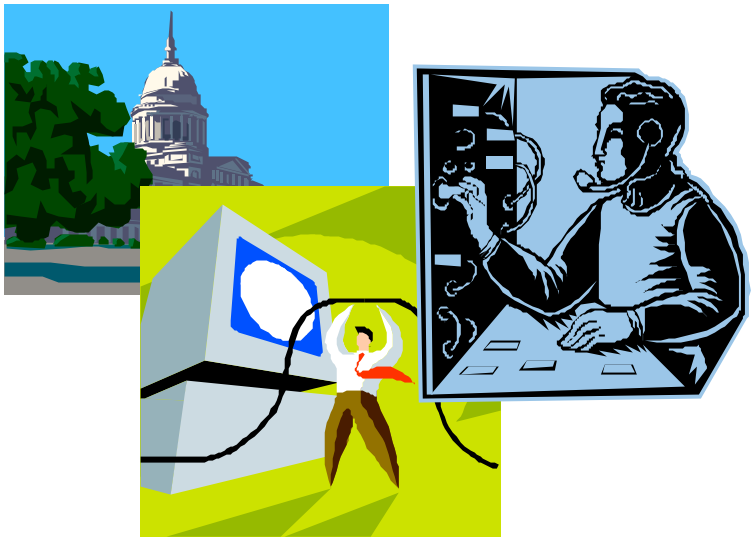
- 管理者は過度のプライバシ侵害をしてはいけない
  - 判例があるので注意しなければならない
- とはいえ、企業ネットワークの管理者が企業からの情報流出を防ぐための適切なチェックはしてもよいことは厳然たる事実
  - 企業の内部に関しては管理者が3rd trusted partyになればよい

# 既にインターネットにある3rd trusted party

- PKI認証業者
  - 信用したくなければしなくてもよい
  - PGP至上主義者はPKIなんか信じない
- DNSのROOT SERVERのオペレータ
  - 不可避
  - これが信じられないとするとかなり問題になる
  - インターネット原理主義者であってもこれだけは例外
  - Alternate Root Serverの恐怖

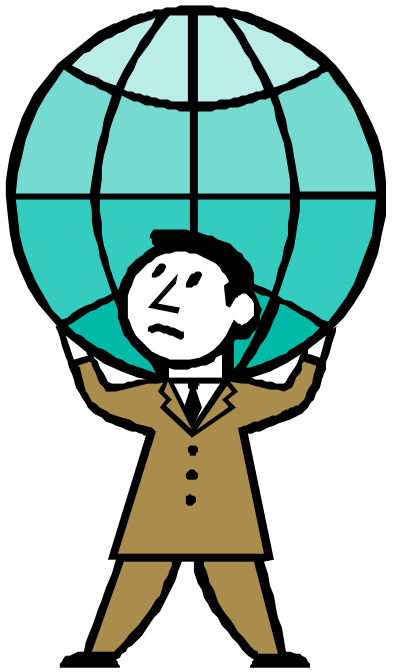
# 世の中で3rd trusted serverになれる人なれない人

- なれそうだ、というか、既にそうなっている例
  - 政府
  - 銀行
  - 通信業者（の一部）
- なれなそう、あるいは、かなり努力が必要な例
  - 個人
  - ベンチャー企業

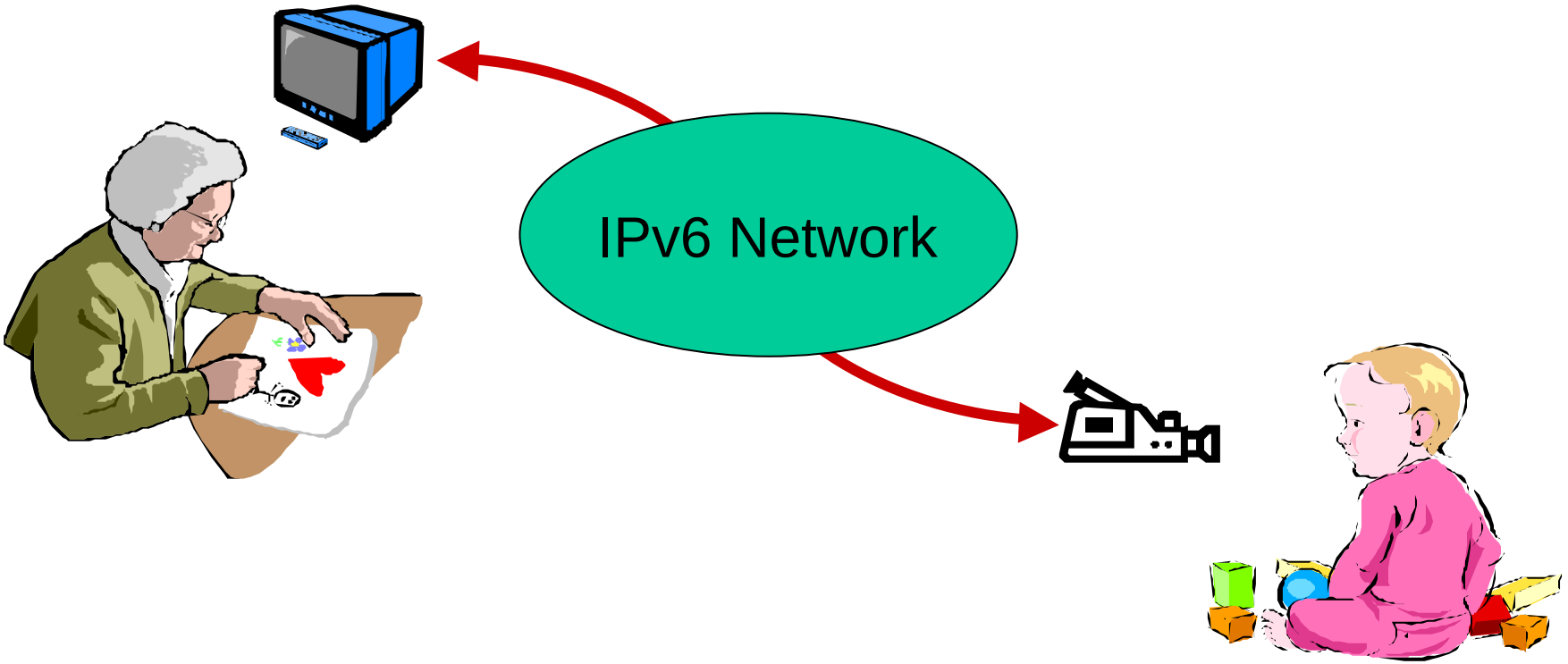


# 3rd trusted party

- 情報管理の体制、従業員のモラル、内部監査のシステムといったノウハウ無しではできない
  - さらに問題が起こったときの対処はどうするか
- 社会的責任を考えるとおいそれとはできない

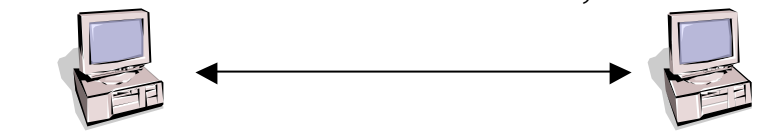


# “Grand-ma in the country”



# An approach

***1.*** Plain IP communications, at first

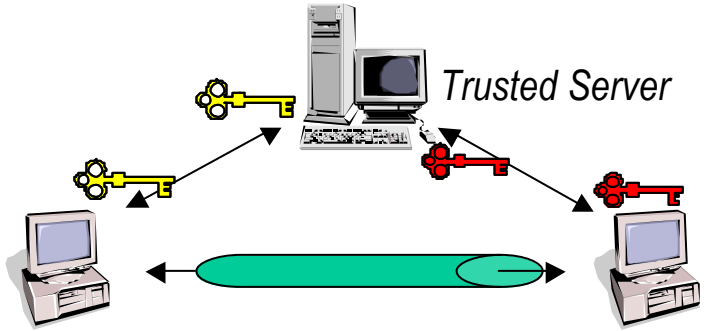



***2.***

Protected by IPsec after a while

(Authentication-less, and vulnerable to man-in-the-middle at this phase)

***3 (option).***
Each device has unique ID and shares symmetry key with the trusted server




-Proved to be man-in-the-middle free
-Authenticated
-Authorized
-Logged

# Plug and play IPsec Architecture (PIA)

- IPv6拡張ヘッダを利用したプロトコル定義案
- FreeBSDによる試作実装
  - Network + Interop　およびITU Telecom World 2003にてデモンストレーション済
- 課題
  - ビジネスモデルの策定
  - 名前解決の方法
  - 標準化作業、他のプレイヤーとの協調による実用化

# おわりに

- インターネットと電話のよいとこどりをすることでユーザの利便性を考えたシステムがつくれるはず