社会インフラとしてのインターネットとセキュリティ課題 ～ xSPの視点からの総括 ～

山口 英

奈良先端科学技術大学院大学

概要

- インターネット概況
  - セキュリティの視点から
  - 実はそんなにうまく守れているわけではない
- 社会インフラとしてのインターネット
  - xSPへの期待と現実
  - 私たちはいったい何をしなければならないのか

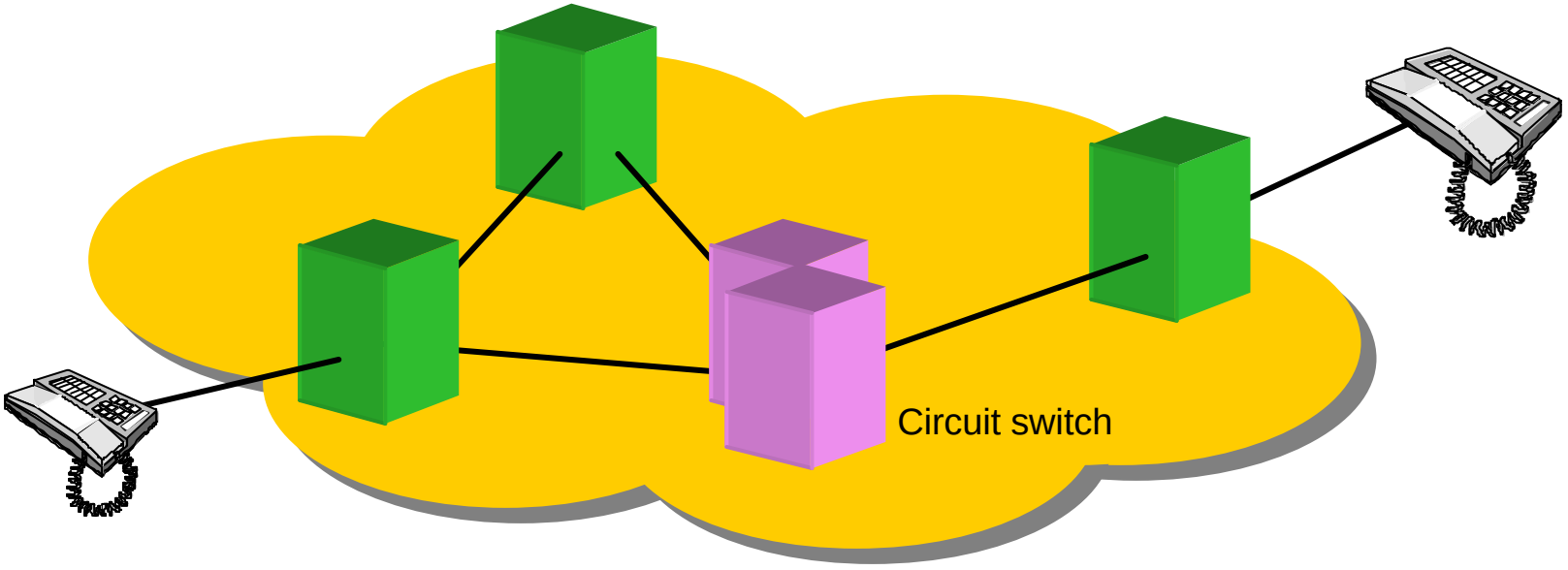
セキュリティから考えたインターネットの現状

特徴

1. Internet for everything, “invisible computers”の利用急増 (Donald A. Norman, MIT press, 1999)
2. どこでもブロードバンド
   - どこでも数Mbpsの帯域は購入可能
   - 光ファイバによる50Mbps以上の接続も着実に増加
3. 社会インフラとしてのインターネット
   - 社会システムの中で重要な役割を負う
4. “Border protection”の破綻

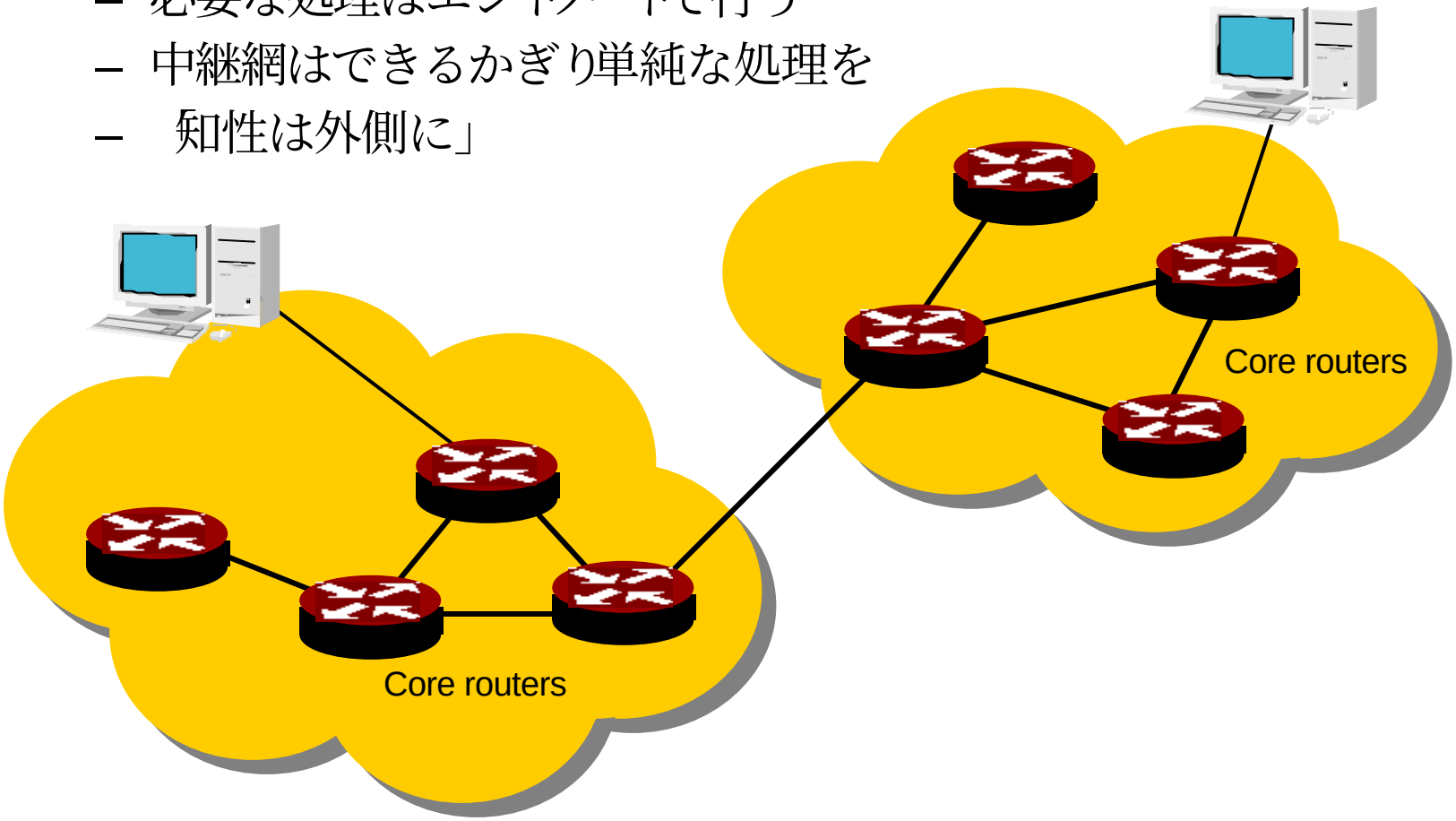
PSTN: 網における技術が支配的

- Network as service infrastructure
  - 端末はできる限りシンプルかつ安価
  - 網においてサービスを構築する
    - 網側に大きな投資を必要とする
    - サービス・メニューはキャリアによって決められてしまう



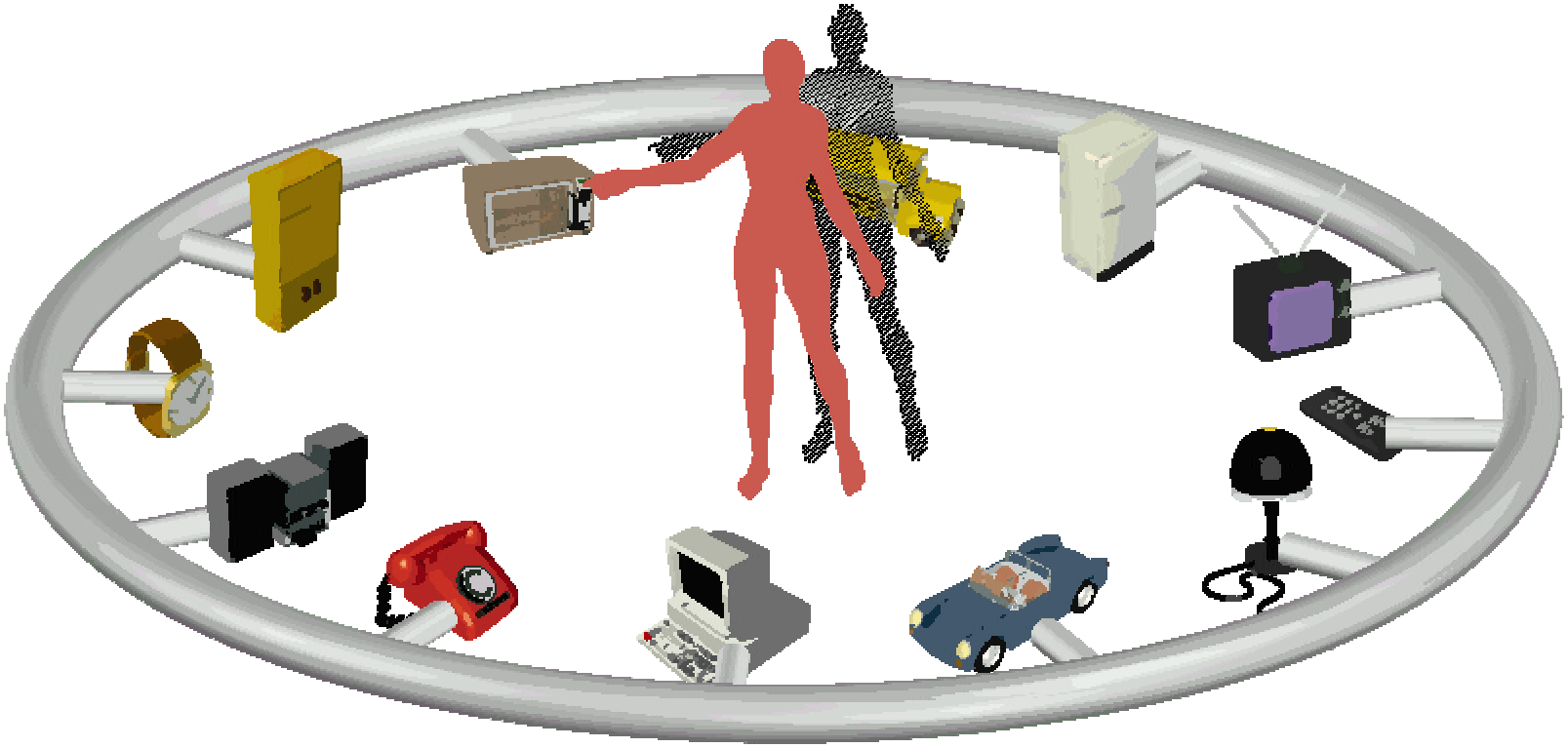
Internet: 端末における技術が支配的

- End-to-End model
  - 必要な処理はエンドノードで行う
  - 中継網はできるかぎり単純な処理を
  - 知性は外側に」

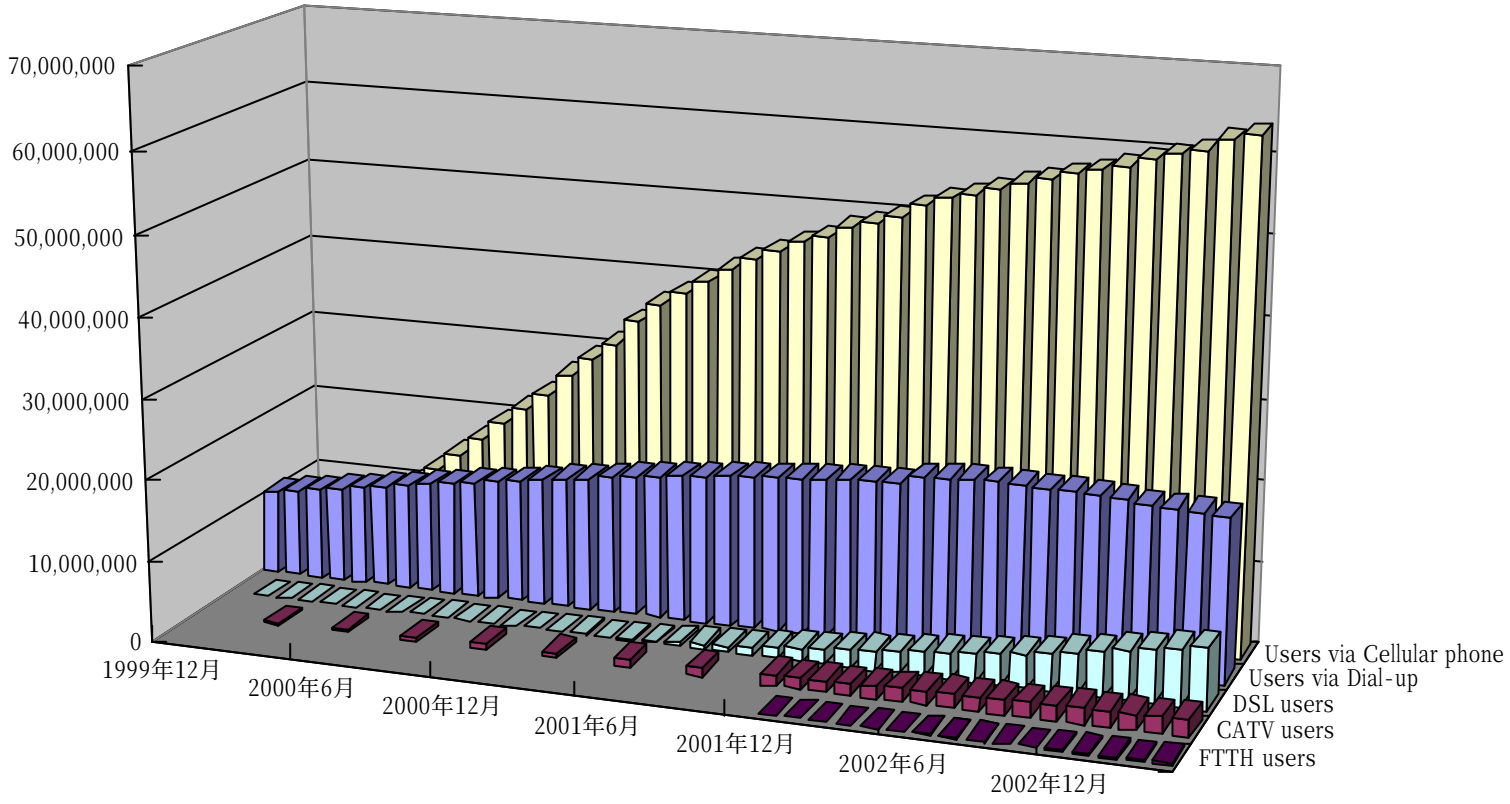


Internet for Everything

- Always connected with global address
- New services with various kind of devices

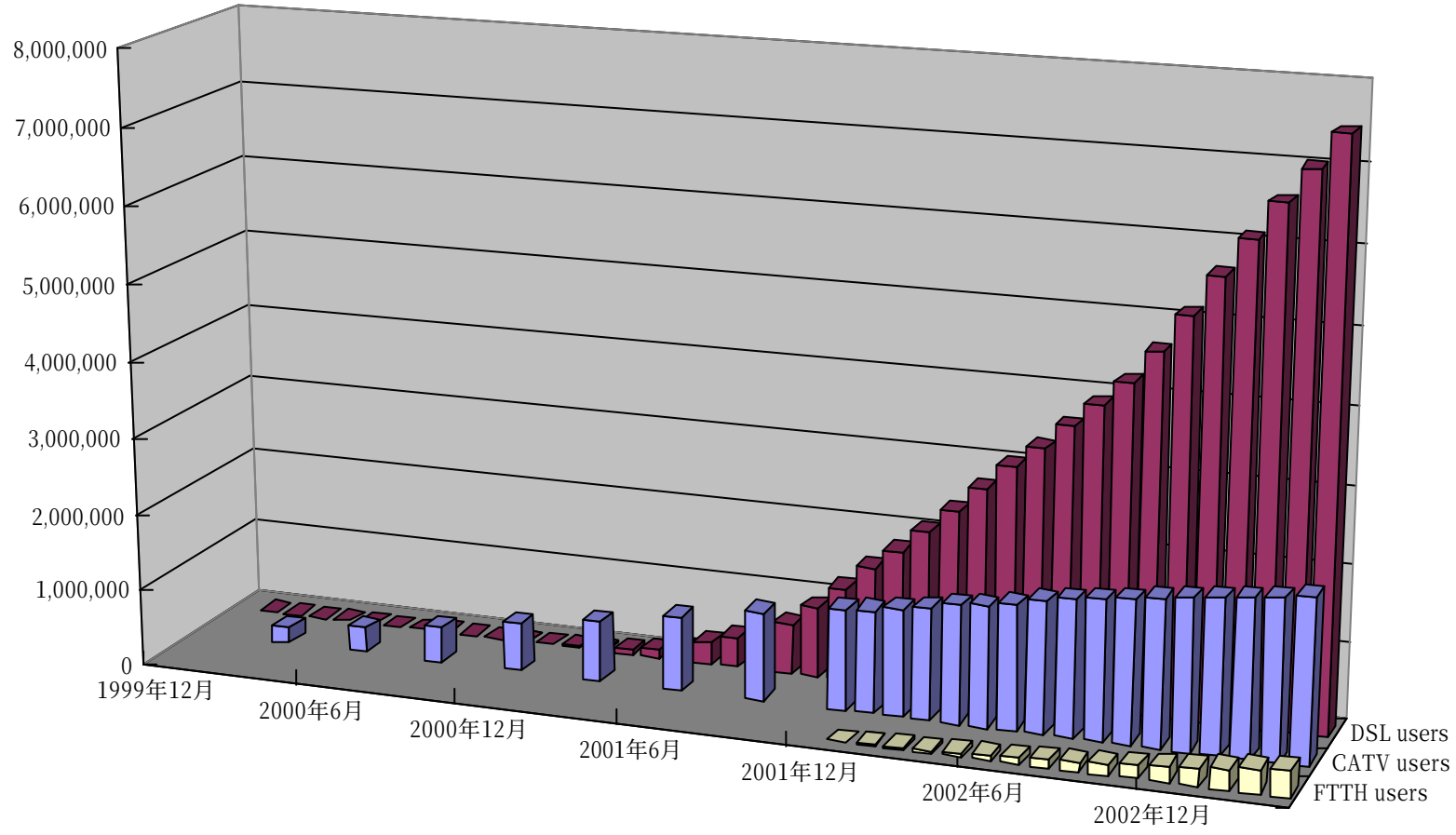


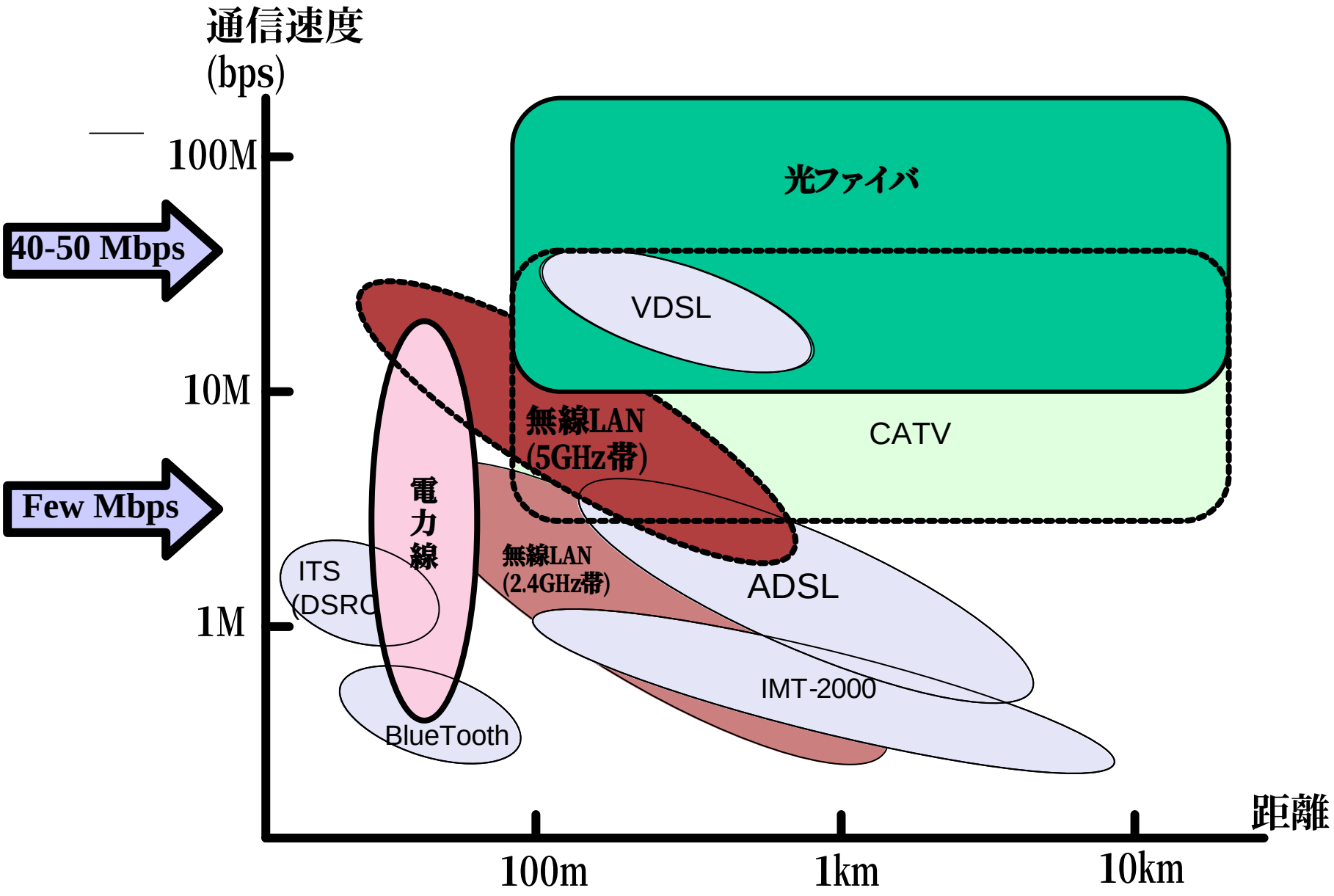
みんなブロードバンド (1)



FTTH users CATV users DSL users Users via Dial-up Users via Cellular phone

みんなブロードバンド (2)

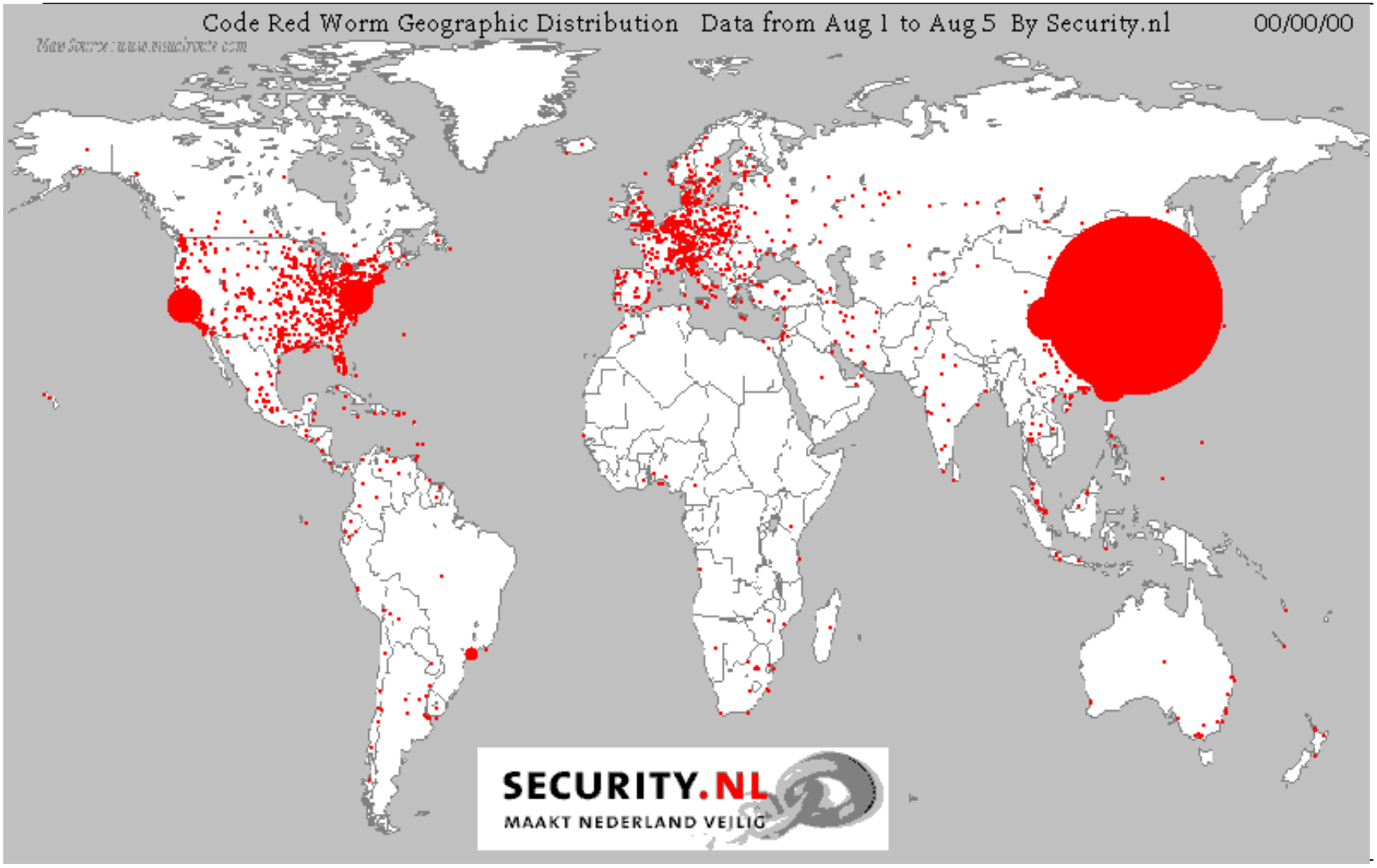



通信速度
(bps)
100M
10M
1M
40-50 Mbps
Few Mbps
光ファイバ
VDSL
CATV
無線LAN
(5GHz帯)
電力線
無線LAN
(2.4GHz帯)
ITS
(DSRC
ADSL
IMT-2000
BlueTooth
距離
100m
1km
10km

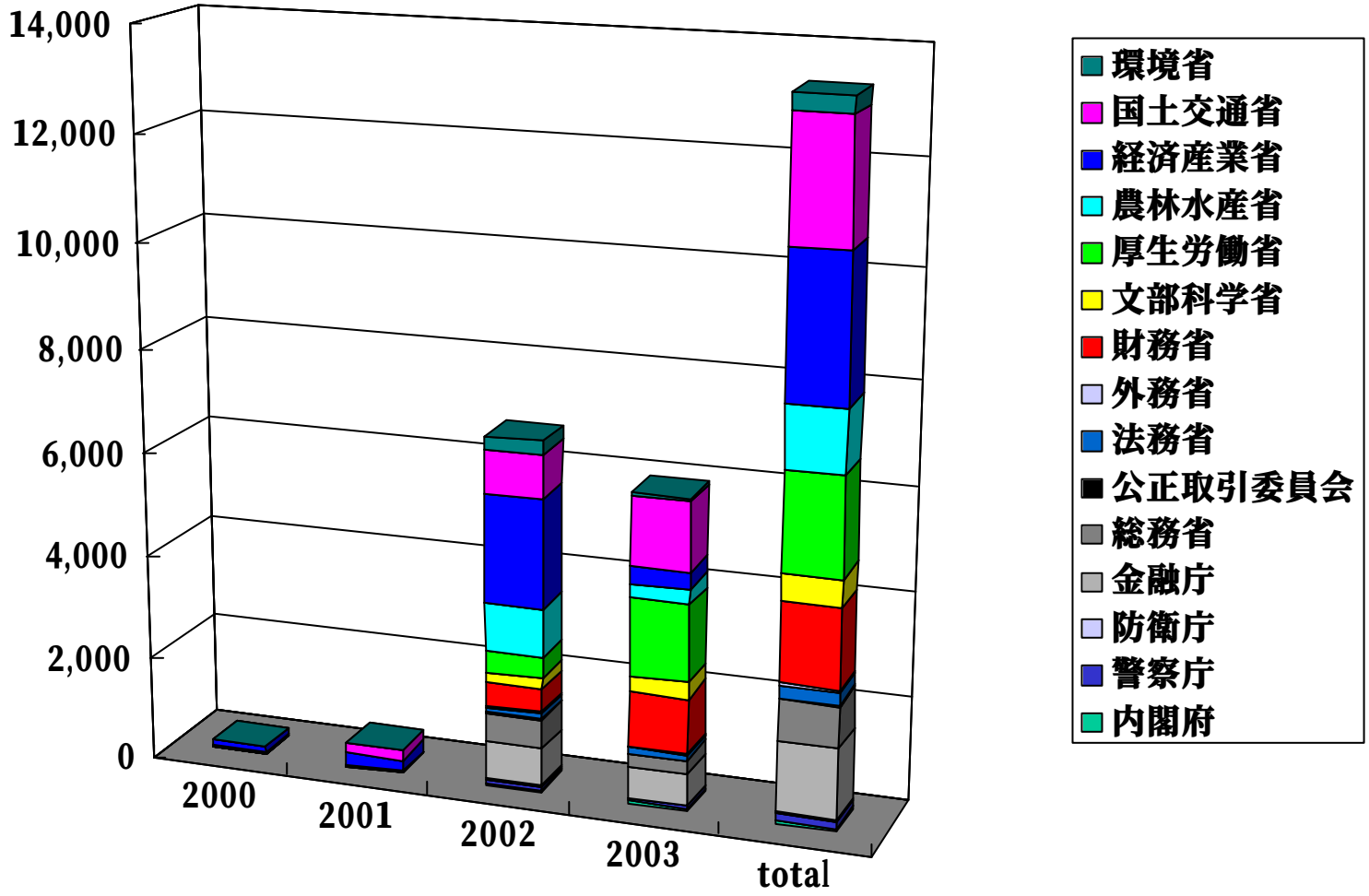
伝送速度と時間

- CD-ROM 1枚 600MB を転送するには…
  - V. 32　524288 (sec)　約146時間
  - ISDN Bチャネル　76800 (sec)　約21.3時間
  - T1　3200 (sec)　約53分
  - Ethernet　480 (sec)　8分
  - T3　106 (sec)　1.78分
  - OC-3　31 (sec)
  - OC-48　1.9 (sec)
  - OC-192　0.4 (sec)

CodeRedの発生状況



国の行政機関が扱う申請・届出等手続きの各府省別新アクション/プラン

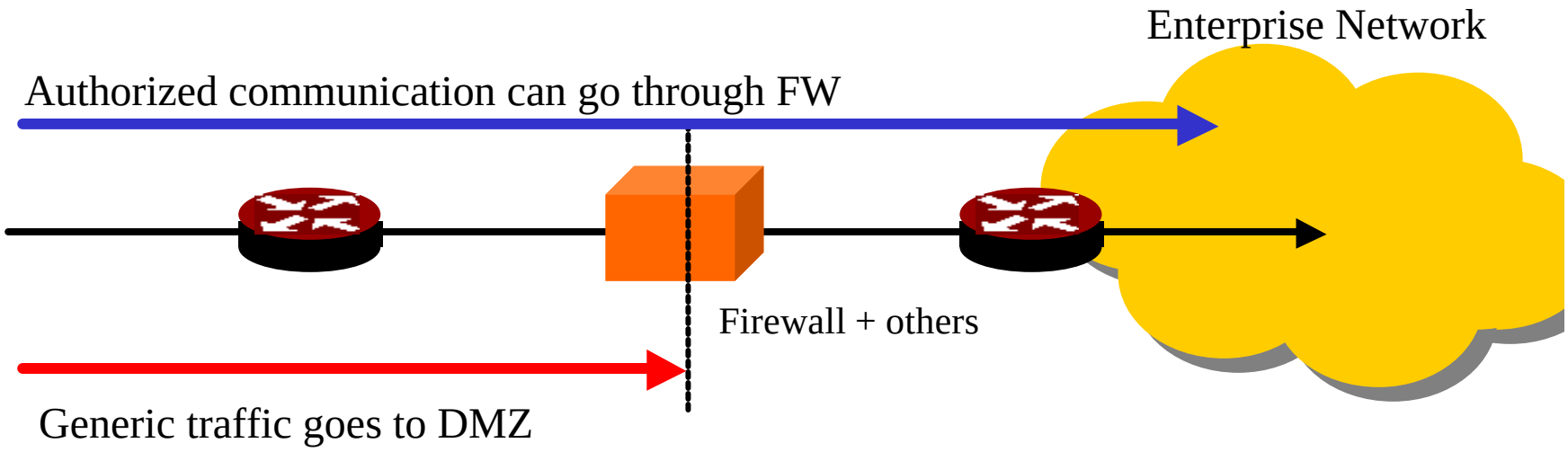


最近のセキュリティ機能

- 捨てる
  - パケットフィルタリング
  - firewall
- どける
  - 迂回経路へのトラヒック誘導 (DoS対策)
  - 検査
- 調べる
  - IDS, virus check, ….
  - Monitoring & analysis
- 騙す
  - Honeypot
- 耐える
  - Load splitting (DoS対策)
- やり直し
  - Out-band management
  - サービス提供アーキテクチャの考え直し

Border Protection

- Firewallにおいて「通す・通さない」を決める
  - 確かに内部犯行・内部トラブルを前提にしないのならばそれでもよい
  - ところが、最近は内部犯行・内部トラブルも頻発している
    - JNSAレポート(2002)によれば国内企業への聞き取り調査でも42%は内部犯行



Border Protection (2)

- Broadband 化による相対的性能劣化
  - 接続される回線は、いまや広帯域回線
  - Firewall のスループットが低いと、結局広帯域回線のメリットを享受することが出来ない
    - 投資効果が下がる
  - より広帯域スループットをもつ firewall は作れないのか
    - Clustered firewall

- Broadband化による機能不全
  - all packet dump & testing
  - 10Gbps回線ではかなり難しい
  - 投資効果を考えた場合、本当にバランスの良い投資なのか?

状況分析

- 多種多様なサービスが提供され、社会に浸透している。インターネットが壊れると多くの人が困る
- Internetにおける安全性確保は、エンドノードの機能によって支配的。網による安全性確保の手法は「通過させる・させない」以外の手段が殆ど無い
- Internetに接続される端末の種類増加。特に “Invisible Computers” が大きな問題。
  - Ex. ウィルスに感染するプリンタ
- ユーザが手にする通信帯域は年々急増。これにより、ネットワーク伝搬型インシデントは急速に拡散する
- ネットワーク上で交換されるデータの制限が年々少なくなる。すなわち、知見の交換は年々容易になり、「秘密にすることによるセキュリティ」は効果が減少

技術的な閉塞感

- “border protection” の呪縛から逃れられない製品群
  - これまでの FW, IDS は第一世代
  - 最低限度の機能を力技で実現
  - 組み合わせての利用も拡大しているが、結局機能的なブレークスルーを実現していない
    - トラヒックをとめる
    - 怪しいものを片っ端から見つける
    - 最後は人間が判断しなければどうしようもない
    - 手間ばかりかかるシステム

技術的な閉塞感 (2)

- より新しい技術開発が必要
  - Protection everywhere 的な話
  - Protection at end node 的な話
  - 真に broadband に対応したセキュリティ技術 (around 10Gbps)
  - False positive / false negative
  - Industrial espionage, Attacks conducted by insiders
  - 真に使える traceback
  - Computer Forensics & Crime-scene Investigations
  - サービスそのものを守って止めない運用技術
  - 大規模システムの試験環境技術 (1-2-3系)

xSPをとりまく状況

概要

- xSPを取り巻くセキュリティ課題を紹介
- 具体的な解決策についてはみんなで考えよう！
  - すなわち、100%決定打の解決法がまだまだ出てこない

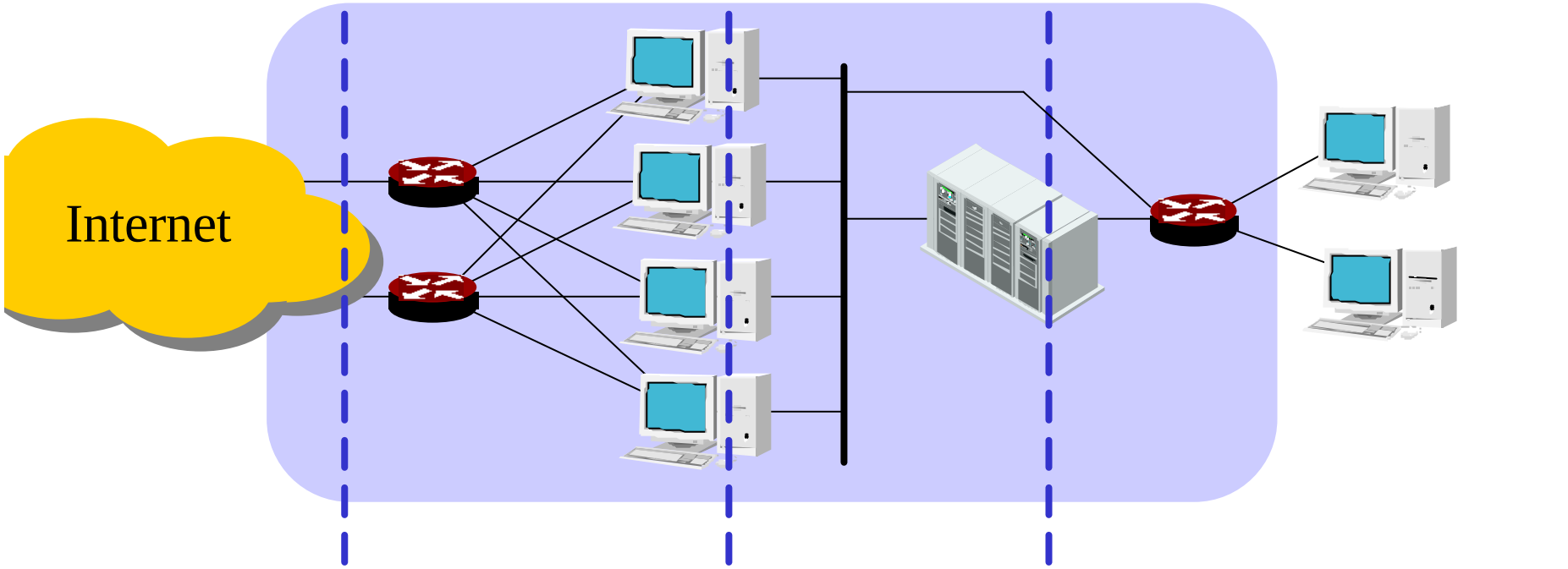
xSPとは何か

- サービス提供事業者 (Service Provider)
  - ISP: Internet SP
  - ASP: Application SP
  - SSP: Security SP
  - SSP: Storage SP
  - ……
- 何らかのサービスを提供する法人(組織)
  - 法律、省令、約款、契約などにより提供されるサービスの制限、限界が設定される
  - 基本的には（ISPを除き）アウトソーシングの意味が強い

アウトソーシング先としてのxSP

- 結局、アウトソーシング元に代わってサービスを提供しなければならない
  - セキュリティ技術はプロフェッショナルとして扱うことができる
  - 基本的なセキュリティ機能設計
    - Confidentiality (秘匿性）
    - Integrity (完全性 ・非改ざん性）
    - Authentication & Authorization （有適格者への提供の確保）
  - トラブル発生時の対応技術
    - Accountability （説明責任）
    - Traceability (tractability) （追跡性確保）
    - Contingency Planning & Incident Response （緊急対応）

例） データセンタでのサービス提供



サービス提供部分
(データセンター)

バックエンドサーバ
(両者共同管理？)

データステージング
(契約者側)

ポリシの設定と責任分担の切り分け困難

- Demarcation
  - 誰が、どの構成要素を、どのポリシにしたがって、どのように管理するのか
  - xSPが関与するとどこまでが管理される箱なのかが分かりにくい
    - データセンターの例を見ただけでも、どの箱を誰が管理するのかが、全然わからない。
    - さらに、「データステージング」部分が相手先企業にあったようなばあいには、さらに複雑な構造になる
  - 契約書に書き下しきれるか?
    - ほぼ不可能
    - 結局、現場での打ち合わせのなかで調整
    - トラブルが出るとおおもめ

なぜアウトソースするのか

- 多くの場合には、コスト削減を狙い、かつ、自分自身が持たないプロフェッショナル性を買う
  - すなわち、お客さんはお金を払いたくないアマチュア
    - セキュリティ管理はお金を産まないので、できる限り切り捨てたくなるカスタマ
    - 適正投資をどのように行わせるのか
  - セキュリティ管理がいい加減でも安ければよいところに、最近お客さんが流れがち
    - セキュリティ管理をエキストラサービスと思う気持ちがあまりに強い
  - いかにうまくお金を回収するかについての骨太のプランが必要
    - サービスオプションとしてのセキュリティから、必須サービスへの展開とコストの応分負担モデルの適用

Accountability & Traceability

- セキュリティ・インシデントが発生した
  - お客としては、何が起きたかを明らかにし、損害として何が発生してしまったのかを明確に知りたい
  - 何がシステムに起きているかを知るための機構を用意してなければならない
    - ログ管理
    - 大量のログからのシステム挙動の解析
    - IDSなどの、より目的に合致したシステムの導入と運用
    - 解析結果から説明資料へ

- ところが現時点でもあまり良い技術があるわけではない
  - 結局お手製・自家製のシステム運用
  - JANOGなどのオペレータ会議などでの情報交換

今後すぐに必要になる対応

- 個人情報保護法に基づく個人情報取り扱い
  - 個人情報を取り扱う場合の取り扱い規定の設定
  - 情報を提供する個人との間での提供確認行為
  - システム化した環境
- 警察や司法機関との関係
  - 特にセキュリティ・インシデントが発生した場合の対応の仕方
  - 警察からの捜査協力が言われた場合の対応手順の事前設定

対策を考えるときのコツ

- どこが責任分界点なのか
- 何を守るのか
- どのように情報を収集するのか
- 収集した情報の解析手法、特にコストのかからない解析方法は何か
- 法的に対応しなければならないところの手順化・マニュアル化
- 新しいセキュリティ技術の投入