資料1

インターネットの中核機能のリスク管理

山口　英
奈良先端科学技術大学院大学

概要

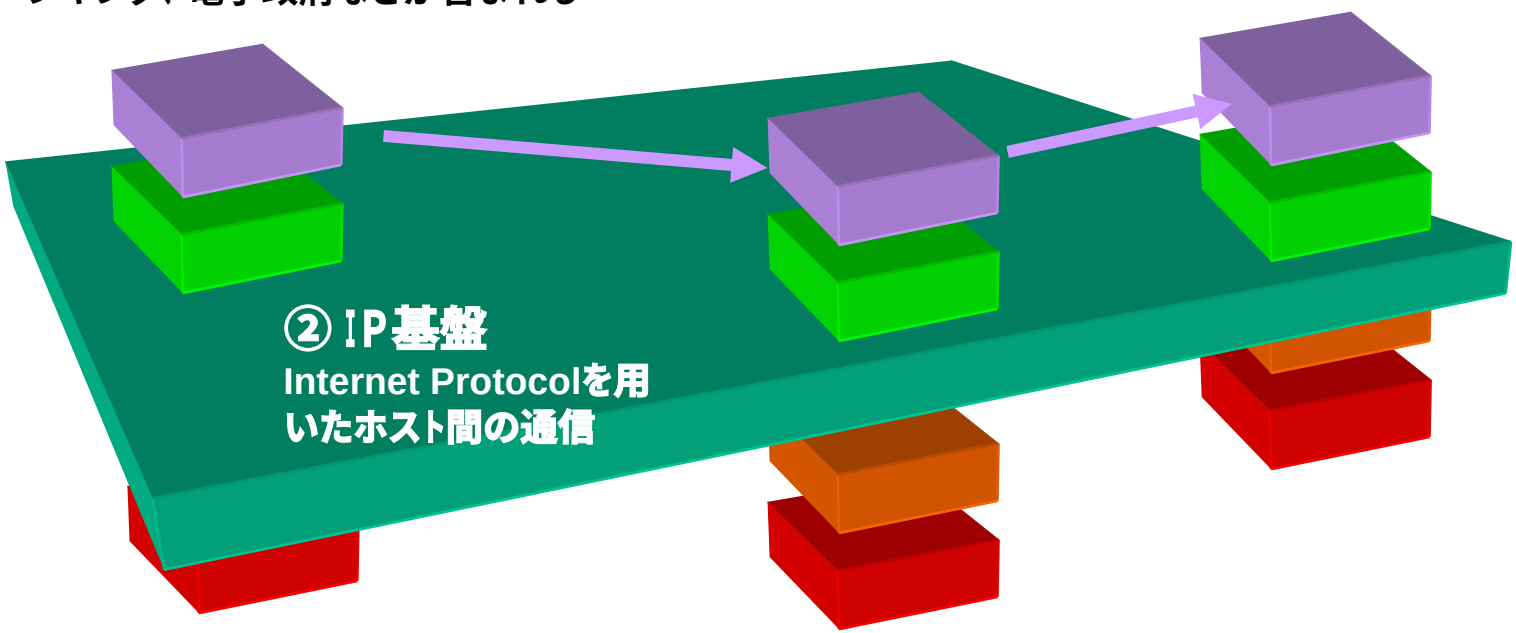
- インターネットの中核機能
  - 基盤を支える機能：IX, DNS
  - 社会にとって重要な機能
- 現時点での取り組みの概要
- 課題

- (参考) システム工学面から見た耐故障性確保手法

インターネットを構成するもの

① ネットワーク・サービス

様々な企業団体によって提供される多彩なサービスが存在。オンラインバンキング、電子政府などが含まれる



③ 伝送路

通信事業者によって提供される光ファイバなどによる広帯域接続が一般的

目標と戦略

- **サービス提供の連続性確保**
  - **インターネット基盤を支える重要機能（②に組み込み）**
    - Internet Exchange (IX)
    - DNS service, **特に** root DNS service, .jp ccTLD DNS service
    - **将来的には** RR **など**
  - **社会にとって重要なサービスを提供するネットワークサービス（①のレベルのサービス）**
    - **重要インフラに関わるサービス**
      - Online banking, reservation system, …
- **サービスを分散させ、単一障害点を除去する**
  - **システム工学での定番手法を利用**
  - **しかしながら、インターネットでの運用との整合性が高い手法を採用することがポイント**

- **自律･分散･非統一性**
  - **非対称性による強さの追求**
  - **組織の特性、システム、運用方法、資源….**

何を分散させるのか (1)

- **インターネット基盤を支える最重要機能**
  - ISP**の相互接続点** (IX: Internet eXchange)
  - **名前解決のためのサービス**
    - **名前** (FQDN)**から、IPアドレスなどへのマッピング**
      - Ex. ns.aist-nara.ac.jp ⇒ 163.221.80.13
    - **世界レベルでのサービスのコア**：root name server
    - **日本国内でのサービスのコア**: .jp ccTLD root name server
  - **将来的には** RR (Routing Registry) **などの経路制御に関わる情報も分散させる必要がある**
  - **これは、インターネットコミュニティとしての責任**

何を分散させるのか（2）

- 社会に密接に関連したネットワークサービス
  - 例えば、航空会社の予約システム、証券取引システム、オンラインバンキング、….
  - 各企業の努力の範囲でシステムの耐久性を確保する
    - 何らかの障害が発生しても、サービスが停止しないような形でのシステム設計と運用が求められる
    - しかしながら、最終的には企業体力の問題
      - お金がない企業にシステム運用の強化を要求することは残酷
      - 特に、この不況下では、企業におけるコスト削減は限界に達している
  - サービス提供者の社会的責任において実施
  - 将来的には電子政府サービスも含まれる
    - 本格的な投資が必要になるが….

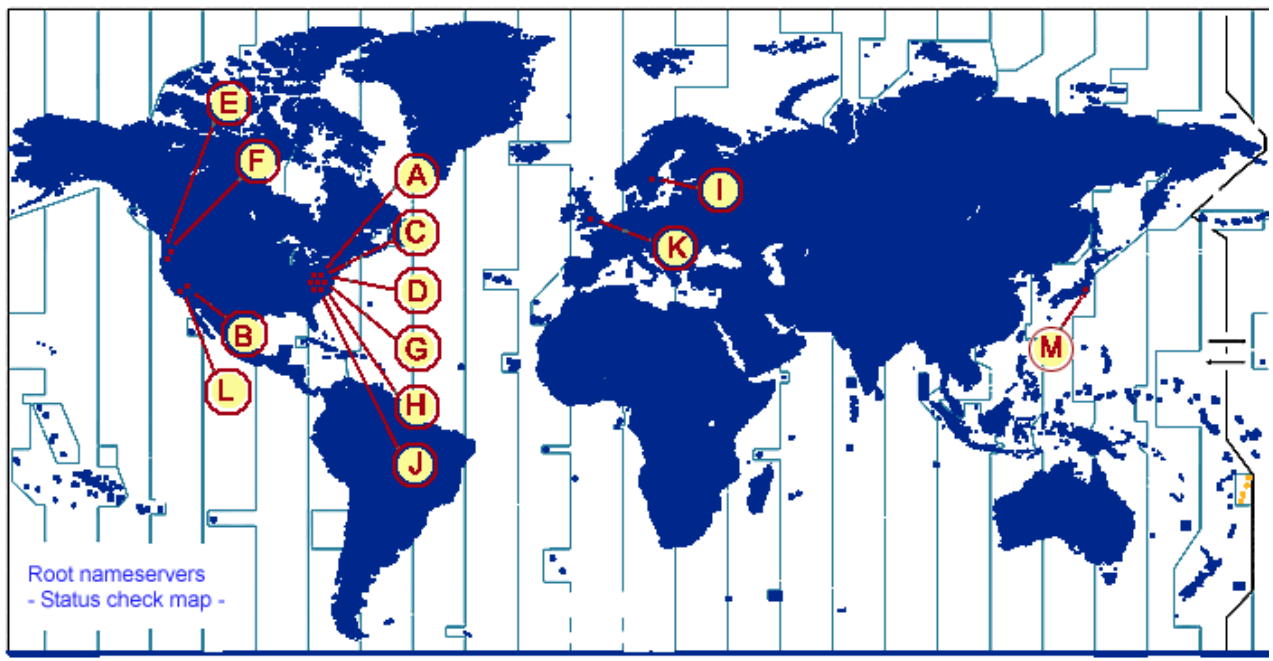
1. Root DNS server

- **世界中で**13**台の** root DNS **が存在**
  - A**から**M**まで**
  - M root DNS **は日本の**WIDE Project**が運用責任を持っている**
  - **各**root DNS **が社会的な責任をもって運用している**
  - www.root-servers.org
    - Root DNS**に関する情報のポータルサイト**
    - **大学や軍、企業、任意団体など、運用している組織としての多様さも重要**

List of the Root Servers

name	org	city	type	url
a	InterNIC	Herndon,VA, US	com	http://www.internic.org
b	ISI	Marina del Rey,CA, U	edu	http://www.isi.edu/
c	PSInet	Herndon,VA, US	com	http://www.psi.net/
d	UMD	College Park,MD, US	edu	http://www.umd.edu/
e	NASA	Mt View, CA, US	usg	http://www.nasa.gov/
f	ISC	Palo Alto, CA, US	com	http://www.isc.org/
g	DISA	Vienna, VA, US	usg	http://nic.mil/
h	ARL	Aberdeen, MD, US	usg	http://www.arl.mil/
i	NORDUnet	Stockholm, SE	int	http://www.nordu.net/
j	(TBD)	(colo w/ A)	()	http://www.iana.org/
k	RIPE	London, UK	int	http://www.ripe.net/
l	ICANN	Marina del Rey,CA, U	org	http://www.icann.org/
m	WIDE	Tokyo, JP	int	http://www.wide.ad.jp/

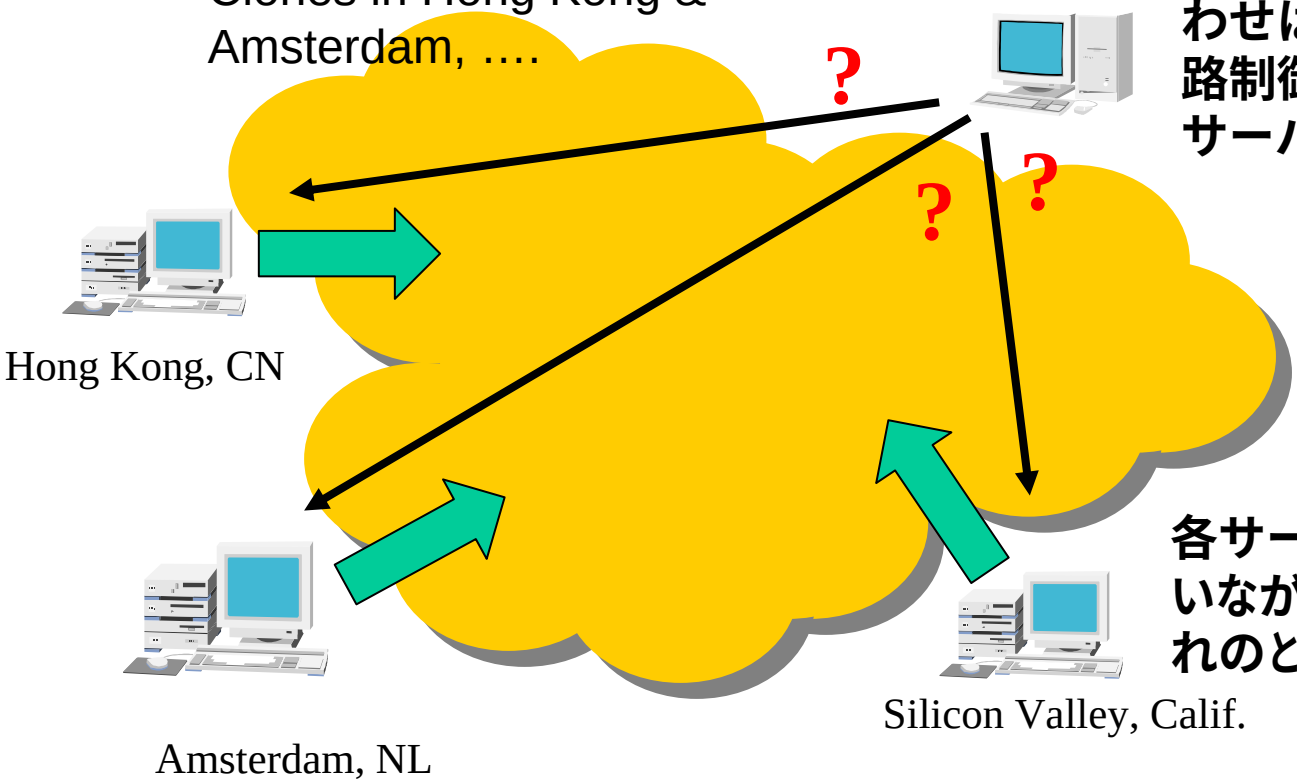
Geographical locations of root DNS servers



Server	Operator	Status
A	Network Solutions, Inc	working
B	USC/ISI	working
C	PSInet	working
D	UMD	working
E	NASA	working
F	ISC	working
G	DISA	working
H	ARL	working
I	NORDUnet	working
J	(TBD)	working
K	RIPE	working
L	ICANN/IANA	working
M	WIDE	working

Geographical distribution using “Anycast”

- F root DNS
  - Originally at ISC in Silicon Valley, Calif.
  - Clones in Hong Kong & Amsterdam, ….



クライアントからの問い合わせは、ネットワークの経路制御に依存して最短のサーバにたどり着く

各サーバは同じアドレスを使いながら、経路情報をそれぞれのところから流し込む

現在の運用状況

- Root DNS全部で100以上のクローンが作られ、6大陸すべてで運用されている
  - M root serverではANYCASTを利用した複数クローンの並行運用を積極的に実施
    - 東京、大阪、パリ、カリフォルニア、ソウル
- .JP ccTLD DNSも同じ仕掛けを利用
  - 少なくとも東京、大阪、海外の拠点に分散

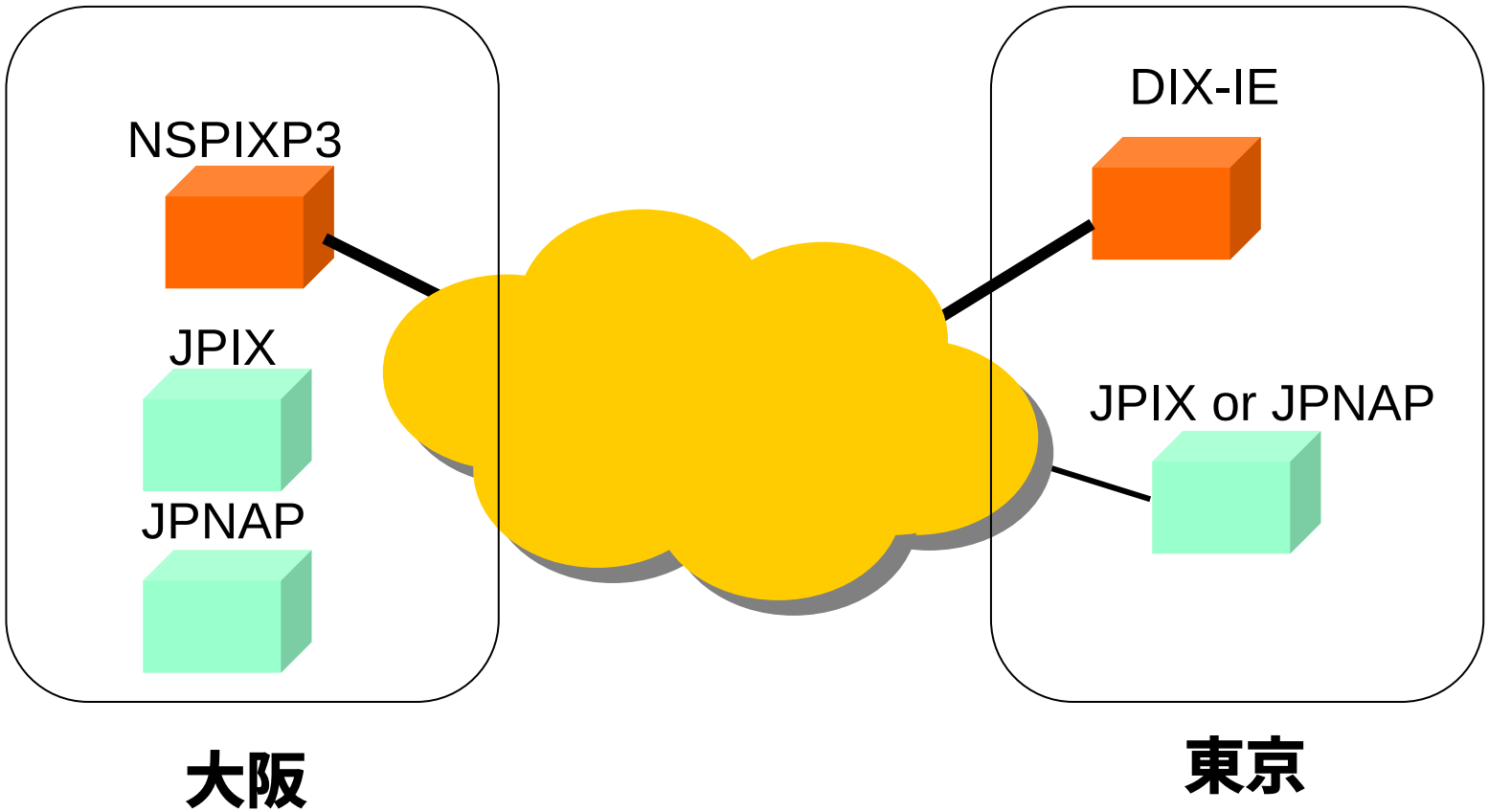
- “Escrow service”の利用
  - DNS運用を継続できるデータの外部蓄積
  - Data escrow
  - DNSの運用継続を脅かすリスクを軽減

2. 国内のIX

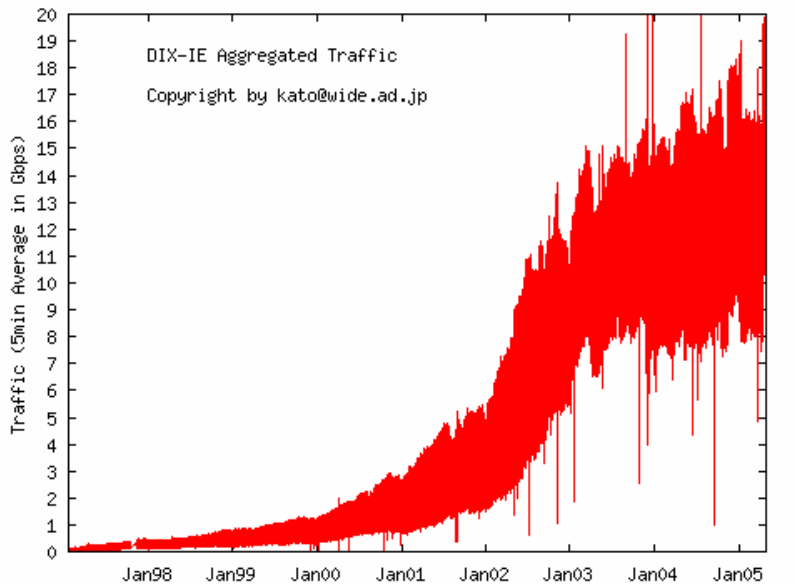
- **現在の国内で稼動する** global IX **は3系統**
  - DIX-IE (**東京**) , NSPIXP3 (**大阪**)
  - JPIX (**東京、名古屋、大阪**)
  - JPNAP (**東京、大阪**)

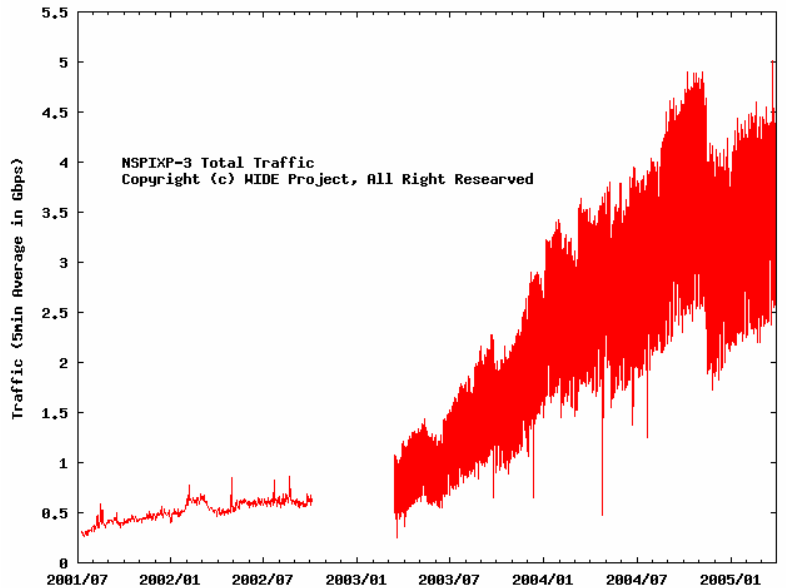
- **多くの大手ISPが2箇所以上のIXに接続**
  - **主にトラヒック交換が標準では東京で行われている**
  - **異常時には、大阪でトラヒック交換が発生する**
    - **最近は大阪でのトラヒック交換も多い**
  - **地理的分散によるリスク分散**
    - **大阪ならば大手ISPは全てPOPを持っている**
    - **大阪ならば相互接続点を持っても問題はない**

単一ISPにとっての複数IX接続例



現在のトラヒック (DIX-IE & NSPIXP)



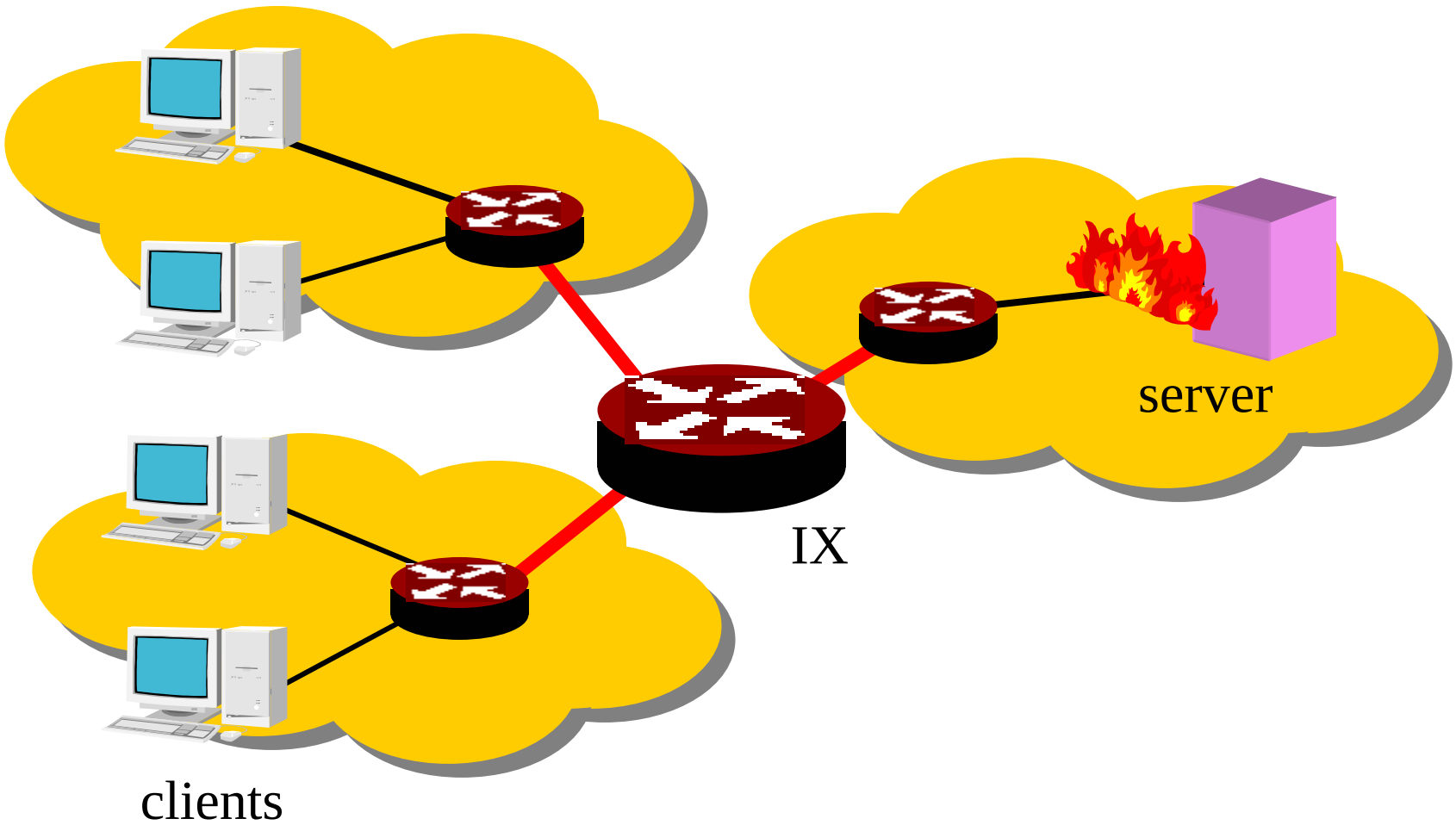


- 当面のトラヒック増加に耐えうるシステム構成可能
- 他のIXへのトラヒック分散が急速に進みつつある
- private peerの増加についての把握必要
  - トラブル発生時の影響評価が必須
- DoS攻撃についての対応は複数のISPで協調対応が必要

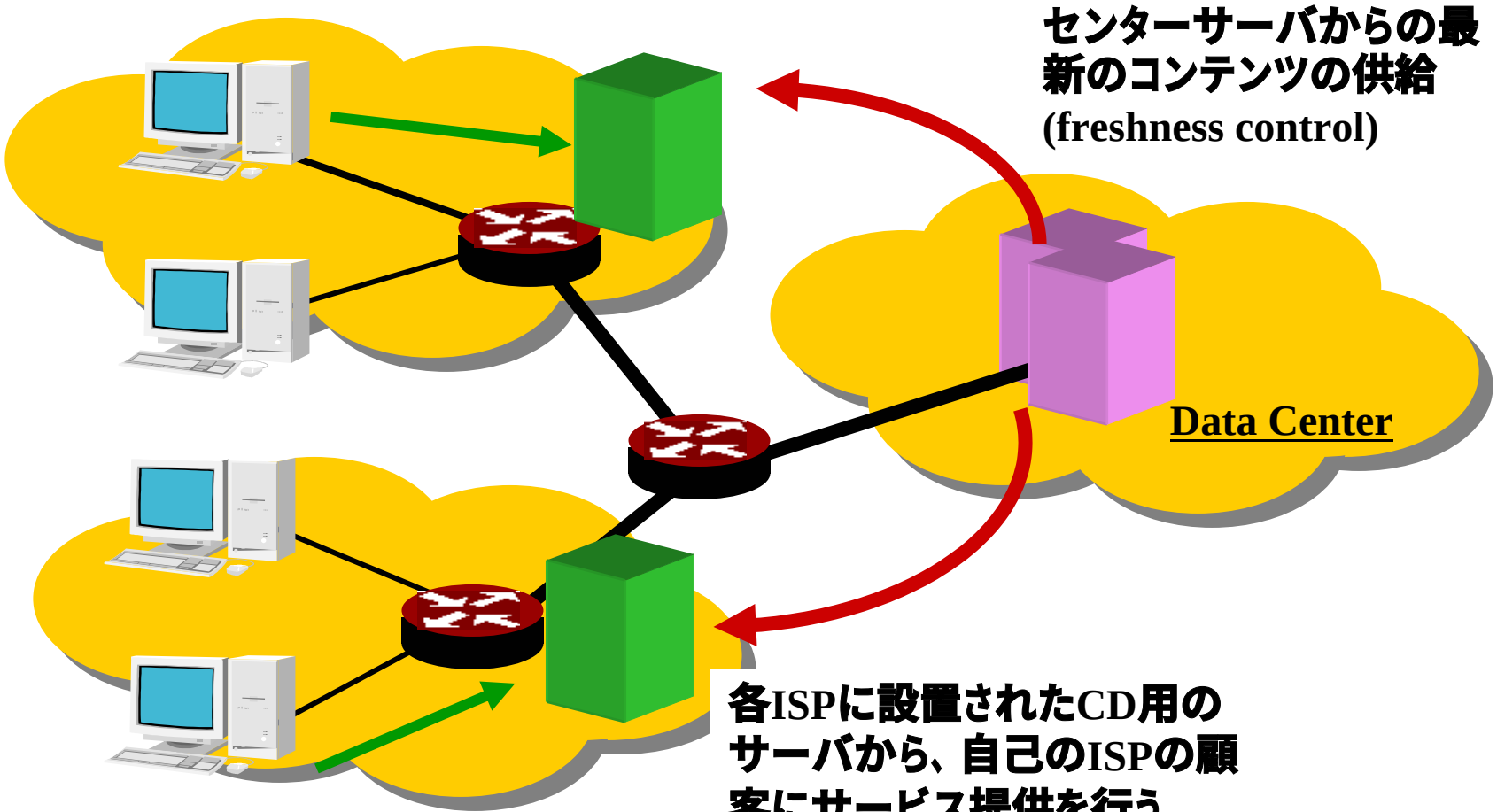
3．サービスの分散

- 多くのネットワークサービスは、東京と大阪で二重化されたシステムを運用している例が多い
- Global load balancer の利用
  - 地理的分散に対応した負荷分散装置
  - 2000年ごろから一般的
- 負荷分散サービスを一般化したものがコンテンツ･デリバリサービス、あるいは、CDN (Contents Delivery Network)
  - システムを統合することでコストメリットを出す
  - 負荷分散請負業

Providing Service at your site….



Contents Delivery Network



組織としての対応

- ISP
  - **電気通信事業者としての責任が明確に定義**
    - **したがって、電気通信事業者法による義務付け行為をまっとうに行うことが、危機管理、あるいは、緊急対応**
    - **電気通信事業者の監督官庁である総務省とのインタフェース**

- **ネットワークサービス提供業者**
  - **責任は明確に定義されていない**
  - **サービス約款で実は免責事項が山のように設定されている**
  - **社会的道義的責任以上の責任の取り方は難しい**
  - **無理強いは出来ないというのも本音**

課題 (1)

- インターネット基盤としてのリスク管理
  - 地震などの災害やシステム障害などのリスクに対応するため、多種多様な技術を用いた基盤整備が進む
  - 特に、root DNS, .jp ccTLD DNS, IXなどで対応が加速

- 重要なネットワークサービスでの対応は難しい
  - 各サービス提供者が対応
  - 重要インフラに関わるサービスでは事業者法などで対応
  - その他のサービスが問題になる可能性大
    - 世の中で広範に使われるサービス
    - 電子政府サービス
  - コスト負担の重み

課題 (2)

- 既に東京に構築されてしまったサービスを地方分散させるのはかなり難しい
  - 情報通信サービス構築を考えると、東京はコスト的に優位性が高い
  - 人材、運用コスト、必要な資源確保
  - 特に、人的資源確保は東京が一番

- リスク管理のための新たな挑戦が必要
  - 「なぜ root DNS, .jp ccTLD DNSが分散できたか」のミソは何か?
    - ポイントは、産学協同での取り組み
    - 「学」をひとつの中核機関と捉えると、地方分散が可能
    - コスト面、および、人材面での解決策になりうる
  - 「産」だけの取り組みでは、東京から引き剥がせない (まず無理)
  - 「官」と「政」の関与は、問題を複雑にさせるので運用側としては頭痛の種になりうる….

(参考) 一般的な障害対策技術

情報システムにおける障害対策 (1)

- Adding “Fault Tolerant” capability
  - **耐故障性能と日本語では言う**
  - **単一故障点** “Single Point of Failure” **の除去**
    - **電源ユニット、CPUなどのハードウェア要素の二重化**
    - **処理単位 (プロセスやスレッド) に対しては多数決システム**
  - **壊れても耐え切るシステムを作る**

- Operational Flexibility
  - **活線挿脱** (hot swap)
  - Check pointing, Epoch dump, atomic transaction, ….
  - **システムを止めても、そのまま状況を復旧できるような技術**

情報システムにおける障害対策（2）

- 代替システムの確保
  - バックアップシステム
  - 情報と処理の完全な同期
    - Hot stand-by, Cold stand-by
  - 二重システムは当然、最近は三重システムの導入が大規模情報システムでは進む
    - 1系、2系、試験系
    - 巨大なソフトウェアシステムの試験は難しいので、いきなり稼動系に入れて動かすような「博打」はできない
      - 例えば、2003.3の東京ＡＴＣでのシステムトラブルについては、関係者は猛省すべき

情報システムにおける障害対策 (3)

- **分散処理システムへの発展**
  - **二重化 (多重化) されたシステム**
    - Mirroring / backup system operation
    - **単一システムでパッケージできる場合にはＯＫ**
  - **機能分散されたシステム**
    - Functional distributed system
    - **複数のシステムから構成される場合には、機能分散とバックアップの併用が普通**
    - **現在のインターネットのサービスの作り方**

通信システムにおける障害対策 (4)

- **代替経路の確保**
  - **一つの通信経路が途絶したとしても、別の代替経路を確保する**
  - **代替経路への切り替えを自動的に行う機構を、各レベルで確保**
    - **伝送回線レベル**: SONET path exchange
    - **ネットワーク管理レベル**: IP Layer dynamic routing
    - **障害発生時に短時間に切り替えられると同時に、振動** (flapping) **しないような安定性を確保する機構を開発**

- Avoiding “Single Point of Failure”
  - **ルータなどの機器が障害を起した場合を想定**
  - VRRP**などのルータグループ形成のための仕掛けが出来始めている**