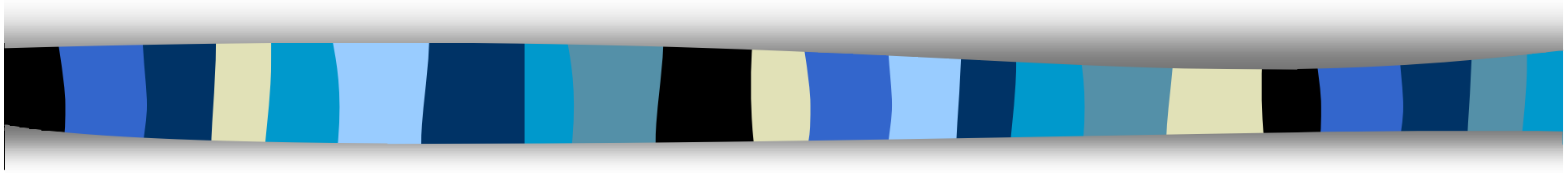
Inter-networkingのY2K問題



Yano Koiti

この文書について

- 本文書ではInternet上でのY2K問題の中でも特にInter-networkingの部分に限って取り扱う
- またこの文書で得られる知識に関しては無保証である

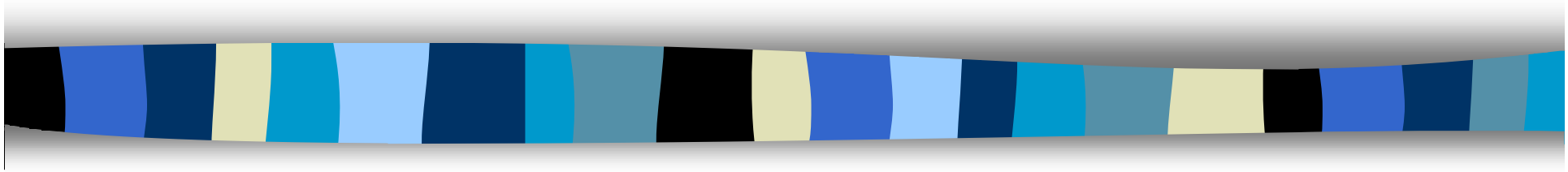
文書の構成

- 本文書は次のように構成されている

0. はじめに--Inter-networkingに関する検討の必要性--
1. トラブルパターン分類
2. プロトコルに関する検討（一部）
3. 経路制御プロトコルに関する検討（一部）
4. 各種機器に関する検討（未検討）
5. 各種リンク（回線）に関する検討（未検討）
6. Internetの構造的問題(Upstreamと日本、そしてIX)（一部）
7. Internet以外の問題（一部）
8. トラブルシナリオとその分析（未検討）

[付録] 非常時の連絡手段（一部）

はじめに



未検討課題Inter-networking Y2K

- 現在、各AS並びにISPでは2000年問題(以下、Y2K問題もしくはY2Kと表記)に対する対策が進んでいる。今後も各AS内、各ISP内のY2K対応ならびに危機対処はサービスを提供している事業者/団体の責任において行われるべきである。
- しかし、The Internetは各ネットワークの相互接続によって成り立っており、そのInter-networkingの部分でY2K問題がどのように現れるか、また問題にどのように対処すべきかに関しては今まであまり検討されてこなかった。

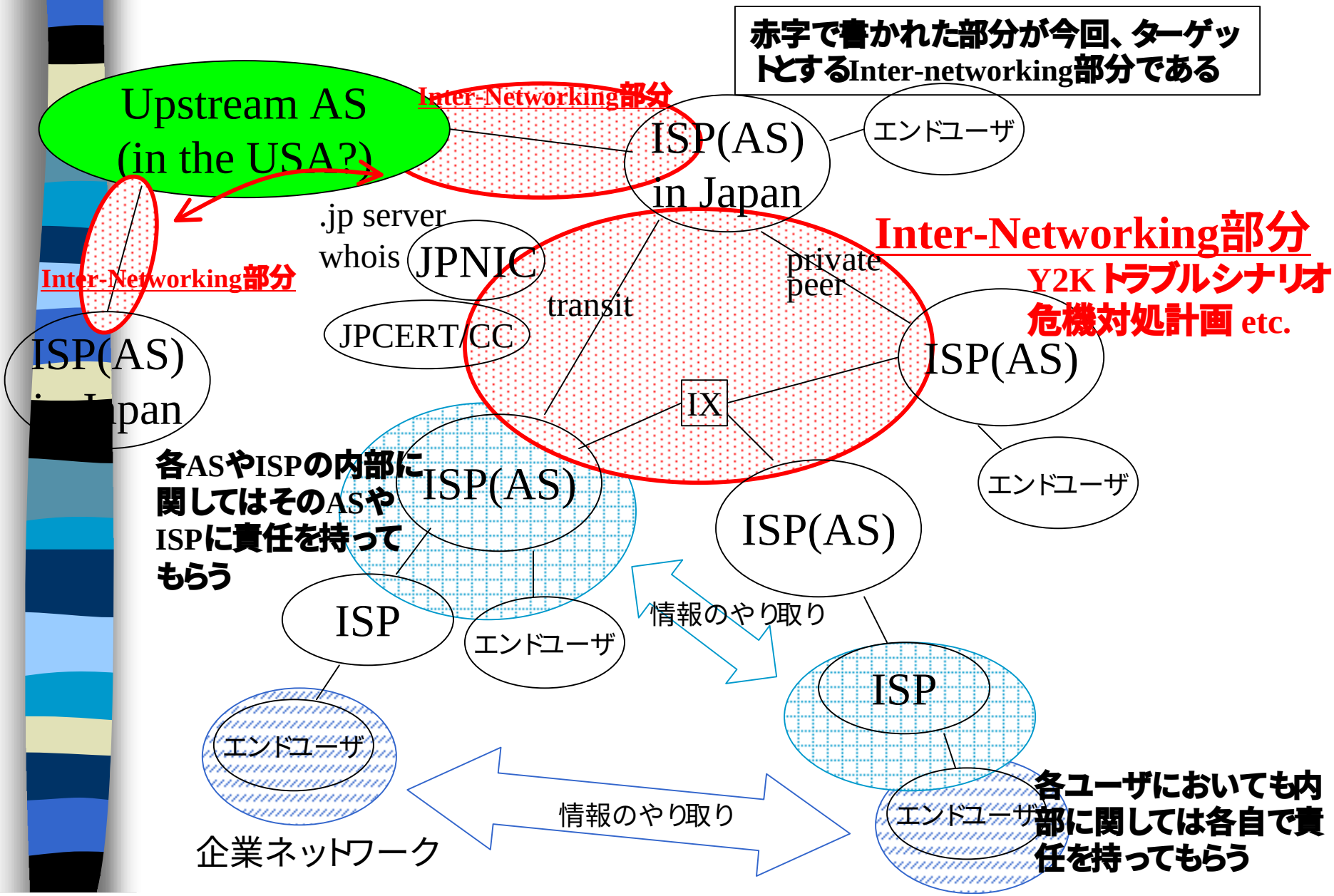
技術検討とシナリオの必要性

- Internet上で使用されている各種機器、ソフトの中にY2K問題を含んだものがあること、また「Y2K対応ではないために何が起こるか分からない」と言われている機器やソフトもある。
- それらに対する個別の対処は各団体/事業者で行なうべきであるが、2000年までのそのすべてに対処を行なうことは困難であり、2000年1月1日時点で相当数の未対処機器やソフトが残っているものと思われる。

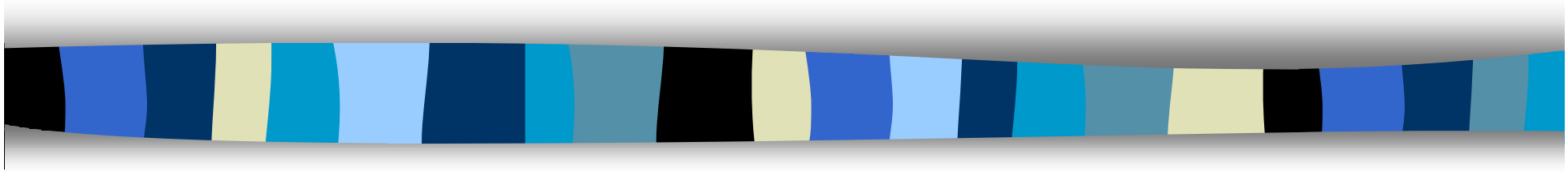
技術検討とシナリオの必要性(続)

- そのため、何らかのトラブルが発生する可能性がある。
- そのため、前記のような状況想定し、「どのようなトラブルが起こりうるのか」という問題に関する技術検討と、トラブルのシナリオを作成する。

Inter-networkingの領域



トラブルパターン分類

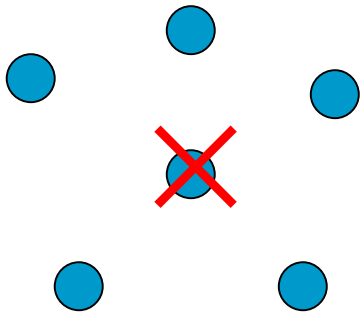


パターン分類

- ここでは起こりうるトラブルのパターンに関して整理する

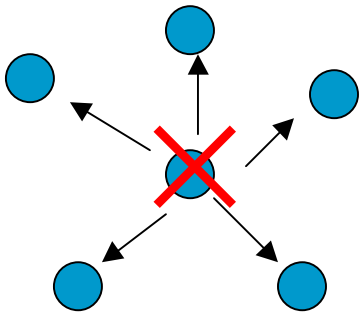
トラブルの波及形式による分類

孤立型



他へは影響なし

周囲波及型

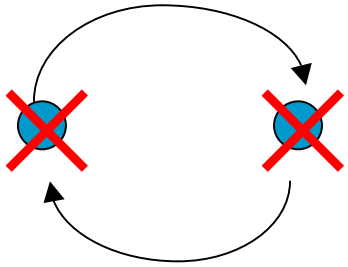


一拠点から他拠点へ影響

連鎖型

一拠点からトラブルが伝播

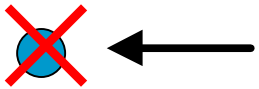
ループ型



トラブルがループ

その他

Bad Guy侵入型



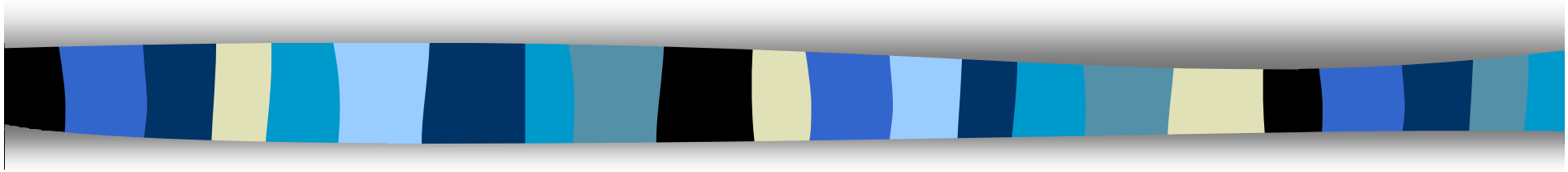
悪い奴(Cracker、愉快犯、産業スパイ)

Y2K問題もしくはその混乱に乗じてAttack

様々なパターンの複合ケース

- 実際のケースでは前述のパターンが複合し、同時多発でトラブルが発生する可能性がある。
- 未検討

プロトコルスタック上の検討



プロトコルに関する検討

- 問題が発生するレイヤとその属するプロトコルによって 問題がどのような形で、どこへ影響しするか」が変わってくる。
- そのため、ここではプロトコルに関して検討を行なう

Application層	L5,L6,L7
TCP/UDP層	L4
Internet Protocol層	L3
Network-Interface層	L2
物理層	L1

ここではTCP/IPプロトコルスタックで表記を行なっている。右にOSI参照モデルを併記

アプリケーション

- DNS,WHOIS,SMTP,POP,HTTP,NNTP, NTP etc.がある。

アプリケーション--DNS--

DNSの動作は基本的に次の二つに分けられる

1. Domain Nameがキャッシュされていない
   →必ずルートサーバから検索

[考えられるトラブル]

ルートDNSが引けない（この場合『ルートDNSダウン』と『ルートDNSまでの経路ダウン』の2種類が想定できる）

2. Domain Nameがキャッシュされている
   → 自分のキャッシュから検索

[考えられるトラブル]

自分のキャッシュが古くなったにも関わらず保持

（未熟な管理者がDNSのSerialを990804のような形で設定し、2000年に000101などとした場合、可能性がある）

DNS（続）

- Root DNSに関してはJPNICの協力が不可欠
- また、Root DNSのバックアップがいくつかあるが、それが同一のビル内にあったりしないことを確認する必要がある
- また、各ASやISPのDNSに関しては個別に対応が必要

アプリケーション--WHOIS

- JPNICの協力が不可欠
- WHOISサーバのバックアップは可能か？
- バックアップがあるとしてもそれが同一のビル内にあるようなことはないか？

アプリケーション--SMTP

- Sendmailの古いバージョン(1992年以前)のものは年を下2桁で扱っている
- qmailの古いバージョンは年を下2桁で扱っている(最新バージョンへのアップグレードの必要あり)
- その他のトラブル（スプール不足やメールのループ）に関しては今後の検討が必要
- 基本的にはMTA間のピアの問題

アプリケーション--SMTP

大量の年賀メール
間違った日付のメール

大量のトラヒックが途中のルータや
回線を圧迫する

アプリケーション--NNTP

- 未検討（NNTPの仕様ならびに実装を含めての検討が必要）
- 古いNewsなどが間違って大量に配信された場合かなりのトラヒックを消費することが考えられる。そのためにサーバやルータのダウンが考えられる

NTP

- Timesync-wgの協力が必要

TCP/UDP

- 未検討　基本的に年月に関わる部分はないはずであるが、仕様ならびに実装を含めての検討が必要 ）
- 例えば、TCPのsequence番号はランダムに生成されるはずだが、年号を種にして生成したりはしていないよね？

IP層の場合

- 未検討　基本的に年月に関わる部分はないはずであるが、仕様ならびに実装を含めての検討が必要）
- 例えば、HeaderのIdentificationの部分を作る時に年号をもとにランダムに数値を入れたりしていないか？　4.4BSDは利用している。現在は問題なし。でも古い奴は？Linux2.0.35などは問題なし）
- ルータのトラブルに関しては『ルータ」の項目で扱う

インターフェイス層の場合

- SONET/SDHなど一部のインターフェイス層では同期を取って通信している。チップの影響（Beach BUGなど）で同期が取れなくなり、リンク断の可能性がある（Etherのようなcsma/cdの場合はこういう心配はない）
- 基本的にはAS内部、ISP内部での影響にとどまる。ただし、IX（NSPXIPなど）で使われているために、検討が必要。

ノード

- ルータ、ハブ、スイッチ、DSU、加入者光アクセス、CSU、TDM、NT、TDM
- それぞれの機器には組み込みチップシステムが入っているため、トラブルの可能性がある。

リンク技術

- 10 Base Ethernet、100 Base Ether、Gigabit Ether、FR、ATM、専用線、SONET/SDH、ADSL、WDM
- 未検討

経路制御プロトコル

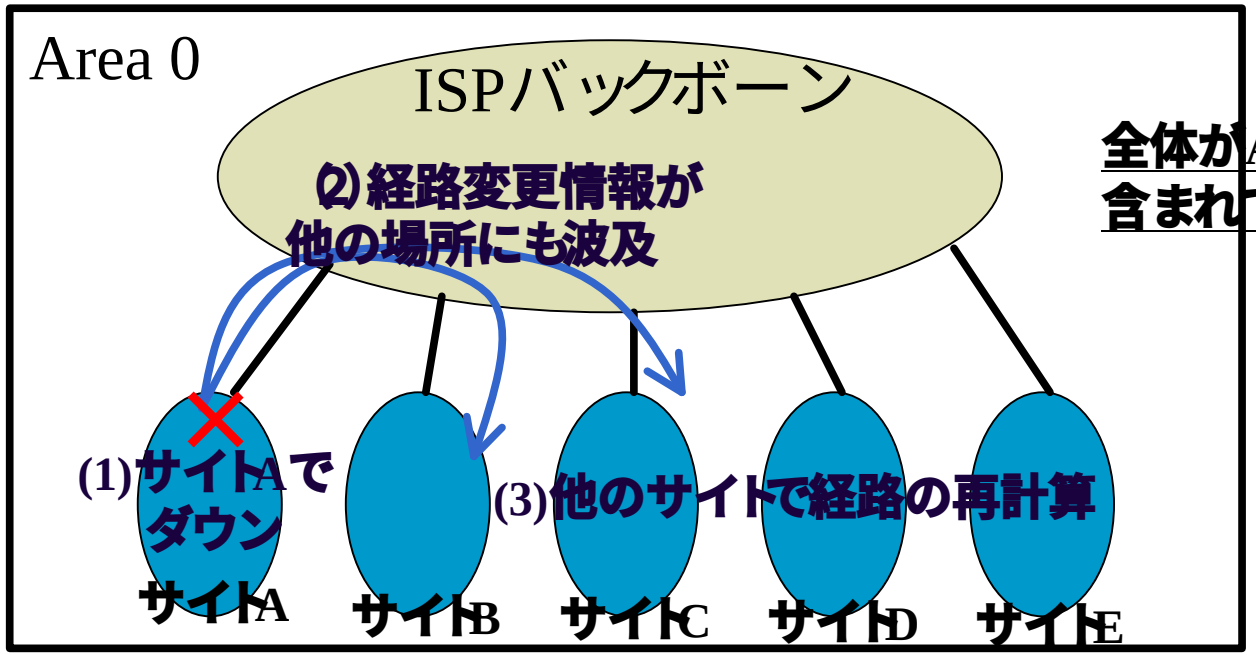
- RIP,OSPF,BGP,ISIS
- 経路制御の運営(AS間相互接続点)

経路制御プロトコル-- ＲＩＰ

- 未検討（仕様ならびに実装を含めての検討が必要）
- ＲＩＰの実装は古くからあるため、特に念を入れて調べる必要があるのではないか
- 特にＲＩＰv1を今でも使っているような古いネットワークではどうか？

経路制御プロトコル--OSPF

ISP内部でOSPFを使用しているが、Area 0（OSPFのバックボーン）やStubエリアなどのエリア分けがなされていない場合、ASが大規模化すると経路変更の際に経路再計算にかかる負荷が大きくなり、低スペックのルータでは対処できなくなる可能性がある



全体がArea0 に含まれている場合

他のサイトでもバックボーンと同じ数のIPエントリで経路の再計算が必要

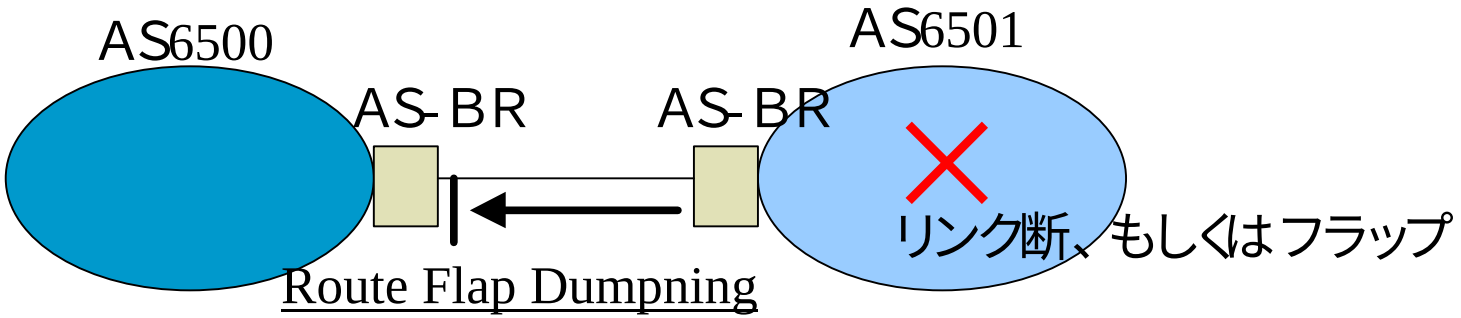
経路制御プロトコル--OSPF続

低スペックのルータの場合、経路計算が間に合わず、結果としてあるべきはずの経路が消えてしまうなどの現象が見られる場合もある。(某ISP ”B ”社で実際に見られた現象)

また、低スペックのルータではなくても、旧来型ルータで転送用CPUと経路計算用CPUが共用である場合、経路再計算が終わるまでスループットの低下が見られる

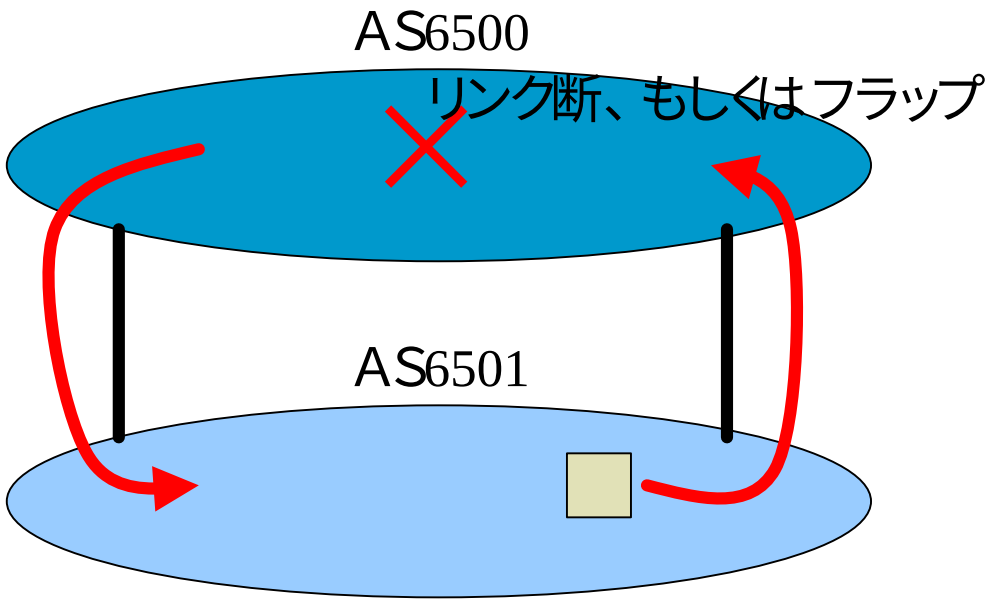
経路制御プロトコル--BGP

- 不適切な経路が広告されてきたり、ルートフラップが起こってBorderRouterに負荷がかかるなどの可能性
- 基本的にはRoute Flap Dumpningが聞くはずではある。



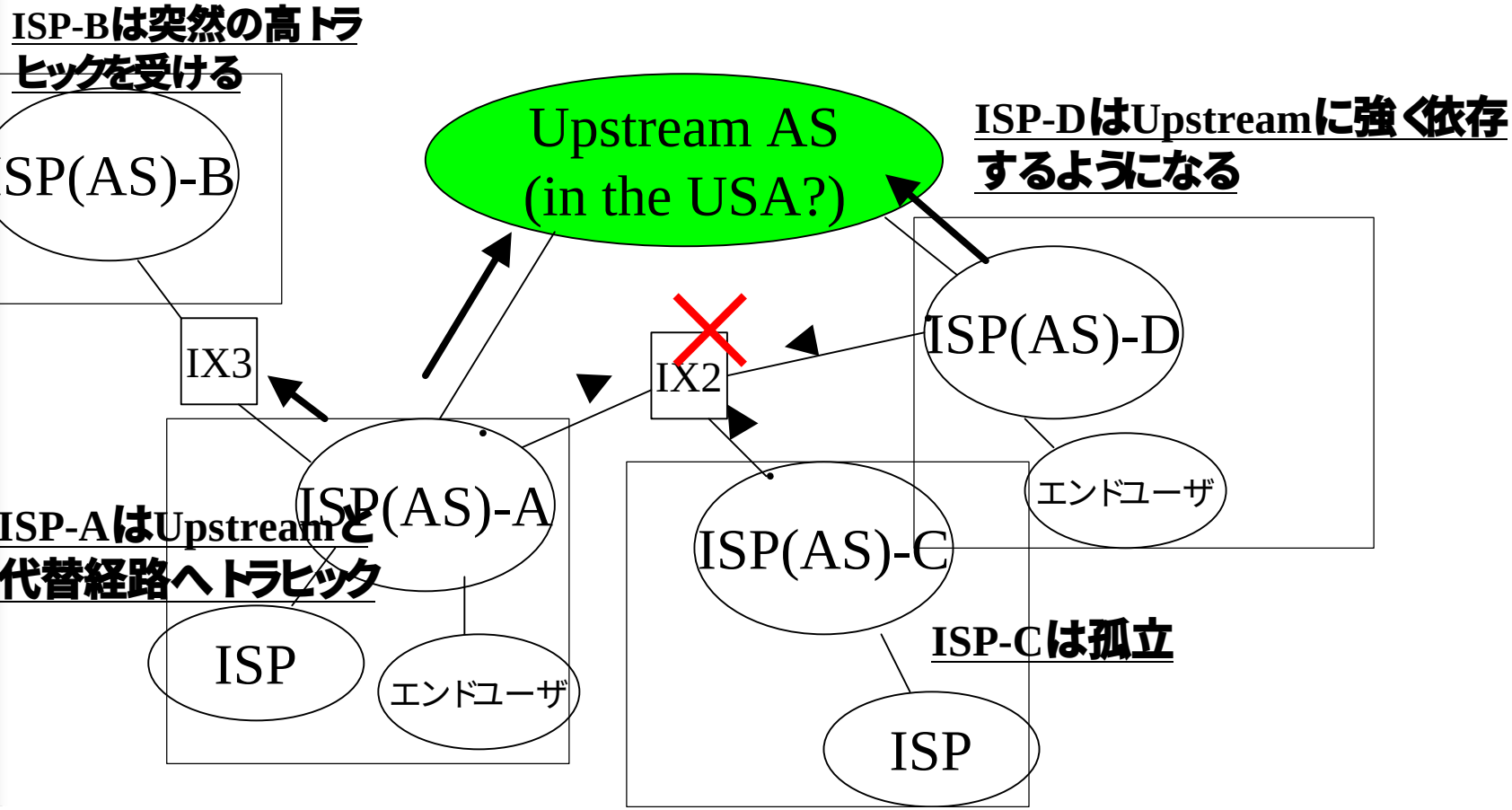
経路制御プロトコル--BGP

- Hot Potatoしていた時に経路がUpDownしたら？



IX

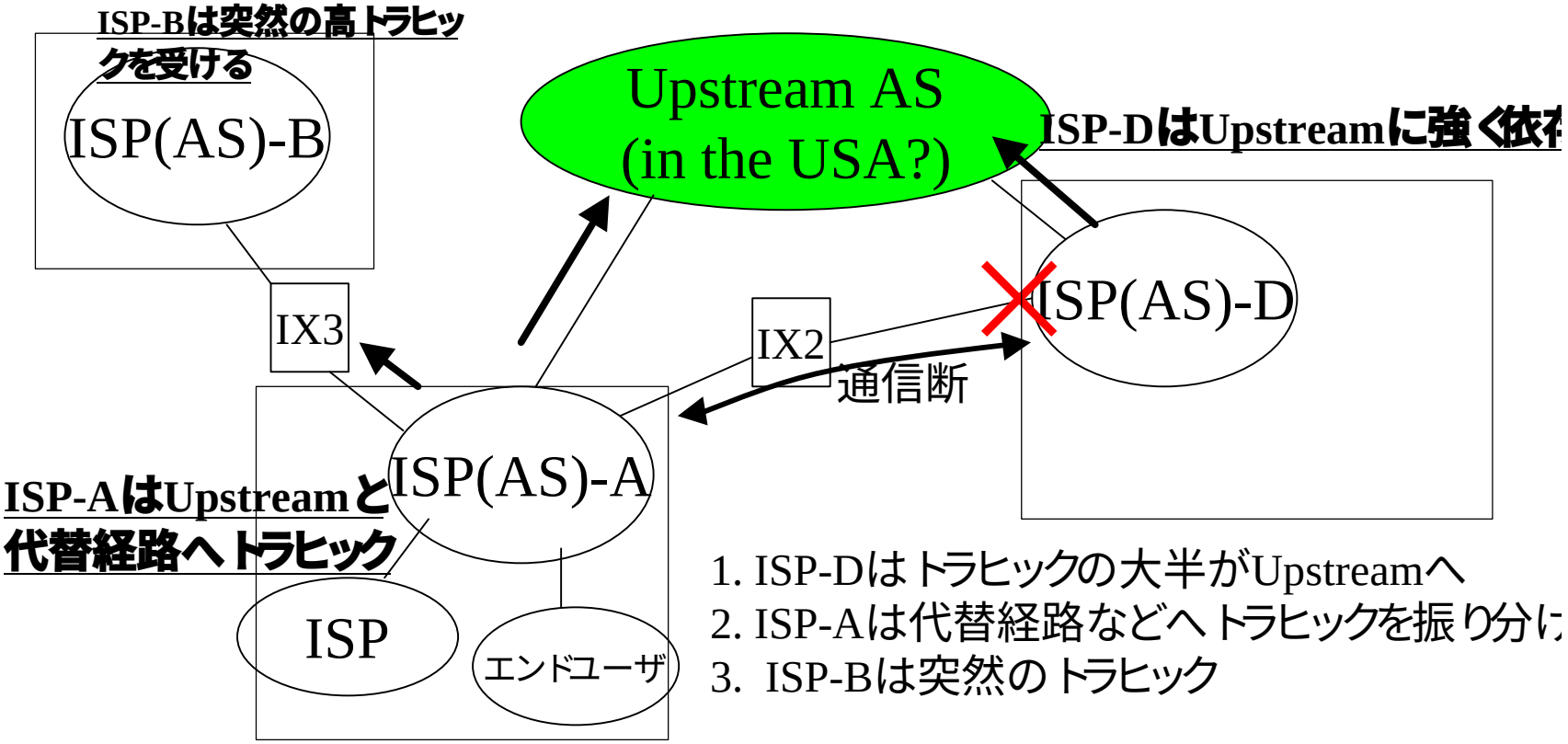
- IXがダウンした場合はどのような影響があるか？



IX(続き)

- IXでBorder Routerがダウン

例えば、ISP-DのIX用BRがダウンした場合



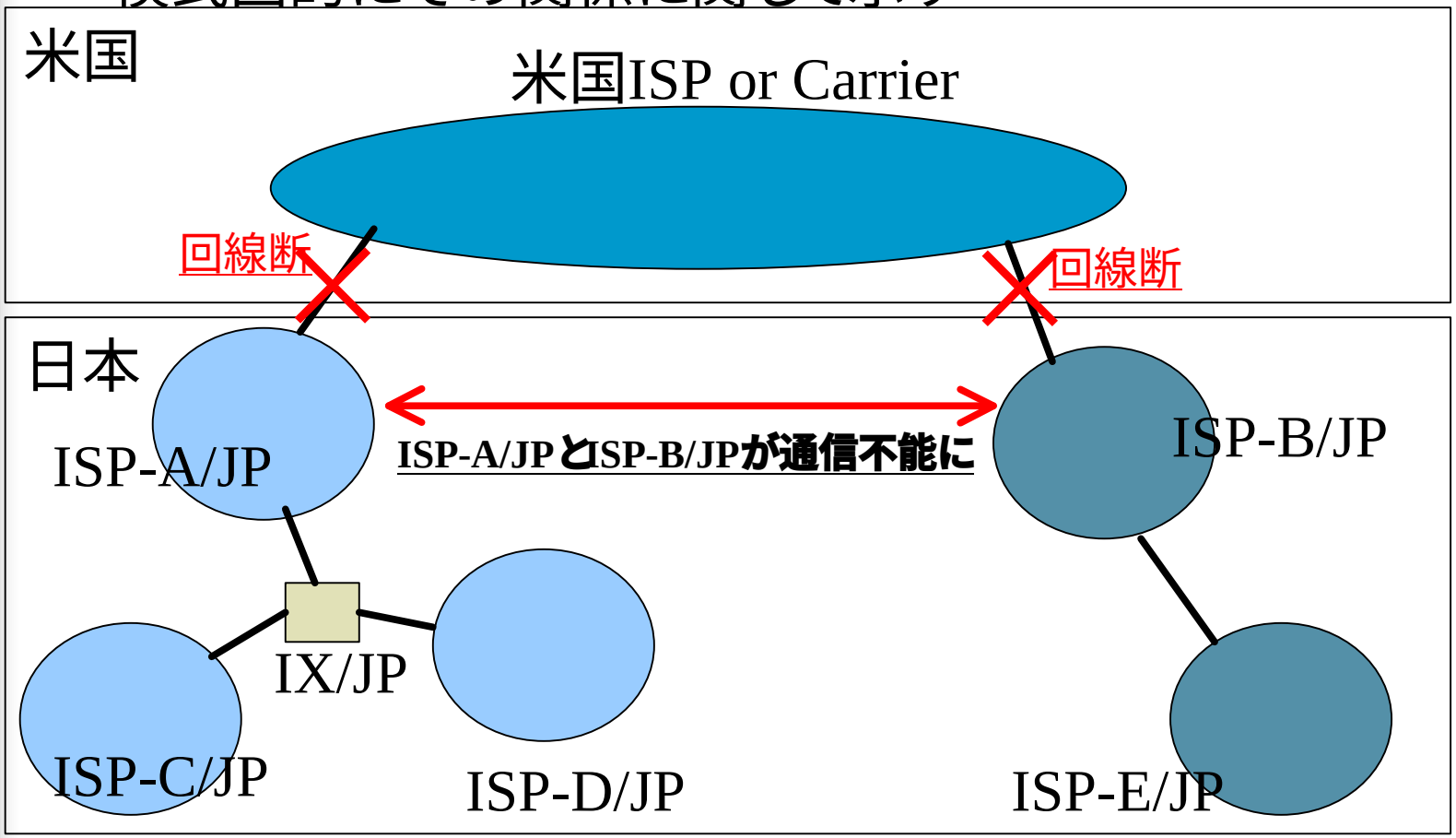
1. ISP-Dはトラヒックの大半がUpstreamへ
2. ISP-Aは代替経路などへトラヒックを振り分け
3. ISP-Bは突然のトラヒック

Upstreamと日本

- 日本国内のASは米国のUpstreamに強く依存しており、Upstreamから回線を切られたり、Upstreamでトラブルが発生した場合、日本国内の通信さえ不可能になる可能性がある。

Upstreamと日本（続）

模式図的にその関係に関して示す



例えば、トラブル回避などのために米国ISP or Carrierから回線を切られるとISP-A/JPとISP-B/JP間での通信が不可能になる

サーバ運用

- ISPの各種サーバ
- ハウジングされている各種サーバ

エンタープライズ固有

- 年末年始の運用停止（年末年始に運用を停止し、2000年1月4日火曜日にいっせいに各企業が運用を開始した場合、各機器や回線（リンク）に過度の負担がかかる可能性がある。また、その時点ではじめてY2Kトラブルが顕在化し、波及する可能性もある。）

セキュリティ

- 年末年始のアタック
- 時限ウィルス（トロイの木馬etc.）

年末年始特有の問題

- 年賀状メール　雑誌等でGreetingメールの宣伝が激しい。また、年末年始のために特別なサービスを始める企業や団体も多いと思われる。）
- これ自体はY2K問題ではないが、引き金となって被害が拡大する可能性はないか

問題の検出

- 各種UNIXコマンド (Ping,Traceroute,PathChar,nslookup,whois)
- 各種ルータコマンド(sh ip **)

インターネット以外の要素

- 電源断 → 予備電源は確保したか
- 専用線などのアクセス回線断 → キャリアへの連絡先と危機対処計画
- ダイアルアップ用の電話＆ISDN断→ キャリアへの連絡先と危機対処計画

非常時の連絡手段

- インターネット経由
- 電話＆ISDN
- 携帯
- 無線
- 衛星回線
- 自動車＆バイク＆自転車＆徒歩