JANOG 35 Shizuoka

地域ネットワーク事業者の課題と要望

株式会社倉敷ケーブルテレビ
小山 海平

はじめに

- 限られた選択肢の中でトラフィック増・冗長性・コストダウンを迫られてきたISPを始めとするネットワーク事業者。ここ最近の傾向や出来事から生まれてくる課題や取り組みを紹介し討論していきたい。
  - ここ最近の傾向・出来事って何？
  - フレッツ卸し ー 短期的・長期的インパクト。存在意義。
  - DDoS ー バーストトラフィック。今後も減らない。

プレゼンテーション紹介

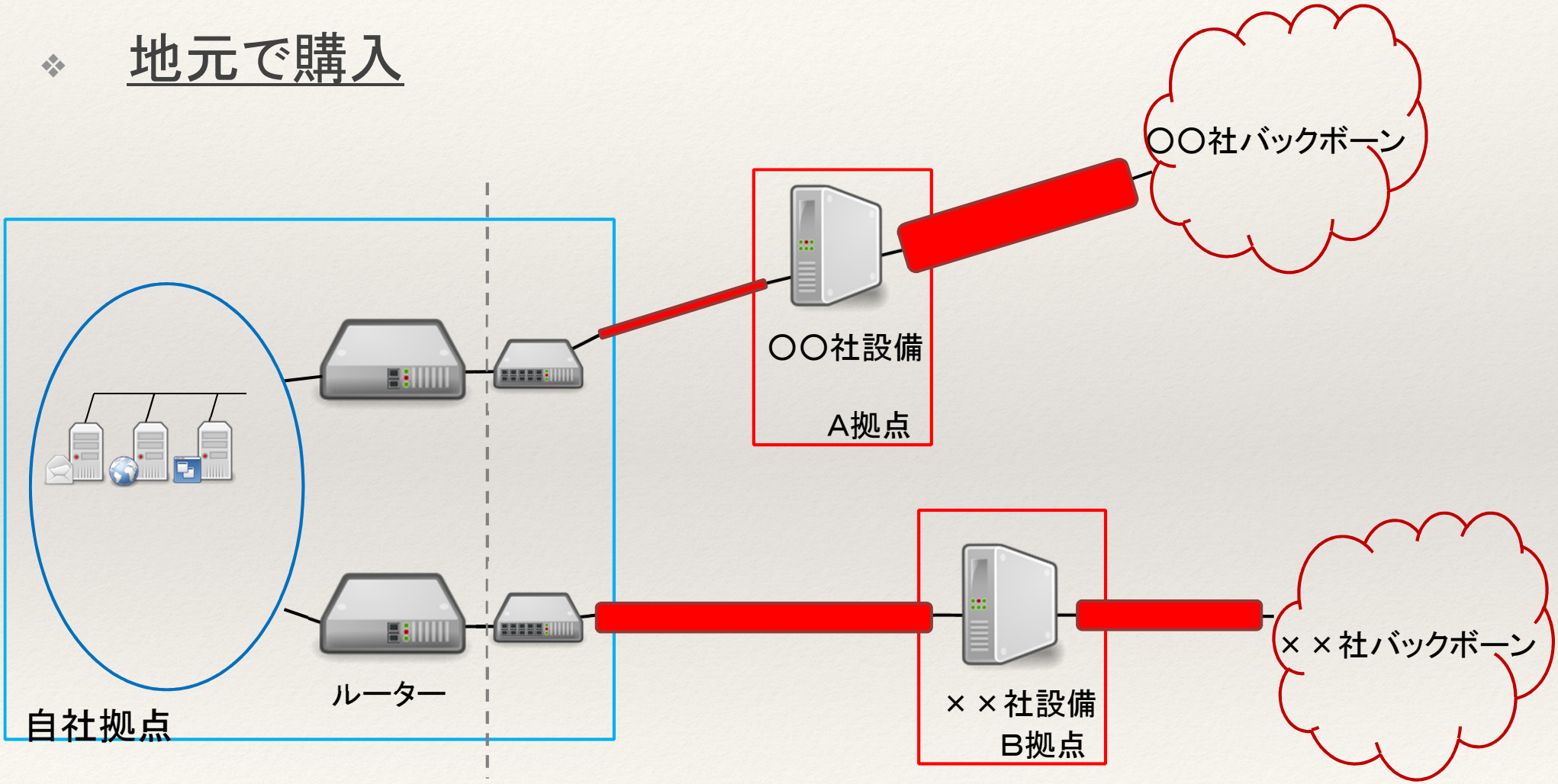
- 日里さん
  - 早期にFTTHを開始されている。
  - ロケーションはあまり今まで話に出てきてない。
  - 質問
- 熊本さん
  - 面白い取り組みをされている。（考えている）
  - 質問

DDoS痛かったです

- NTPリフレクションが2014年GWから数回。
  - 昨年末から ntpd への攻撃は増えていた。
  - ウイルス感染したユーザー向けに大量のNTPが。
    - 再発したユーザーのPC回収して確認すると、同様のウイルス感染があった。
  - 100台以上のNTP Serverから。ざっと見て中国と東欧が多い。
  - おそらくは総量で6G程度かそれ以上。通常ピーク対比で XX 倍。

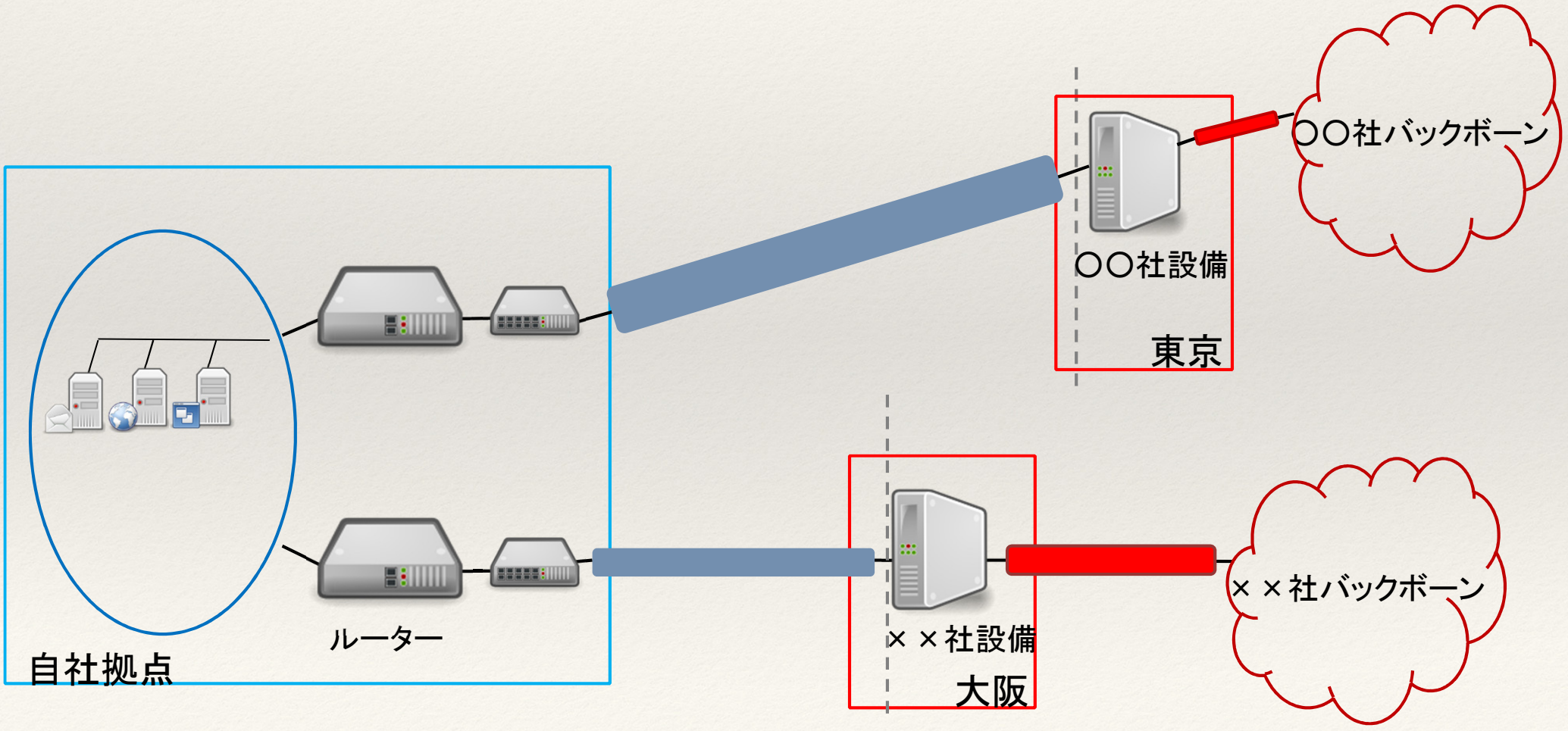
ネットワーク形態

- 地元で購入



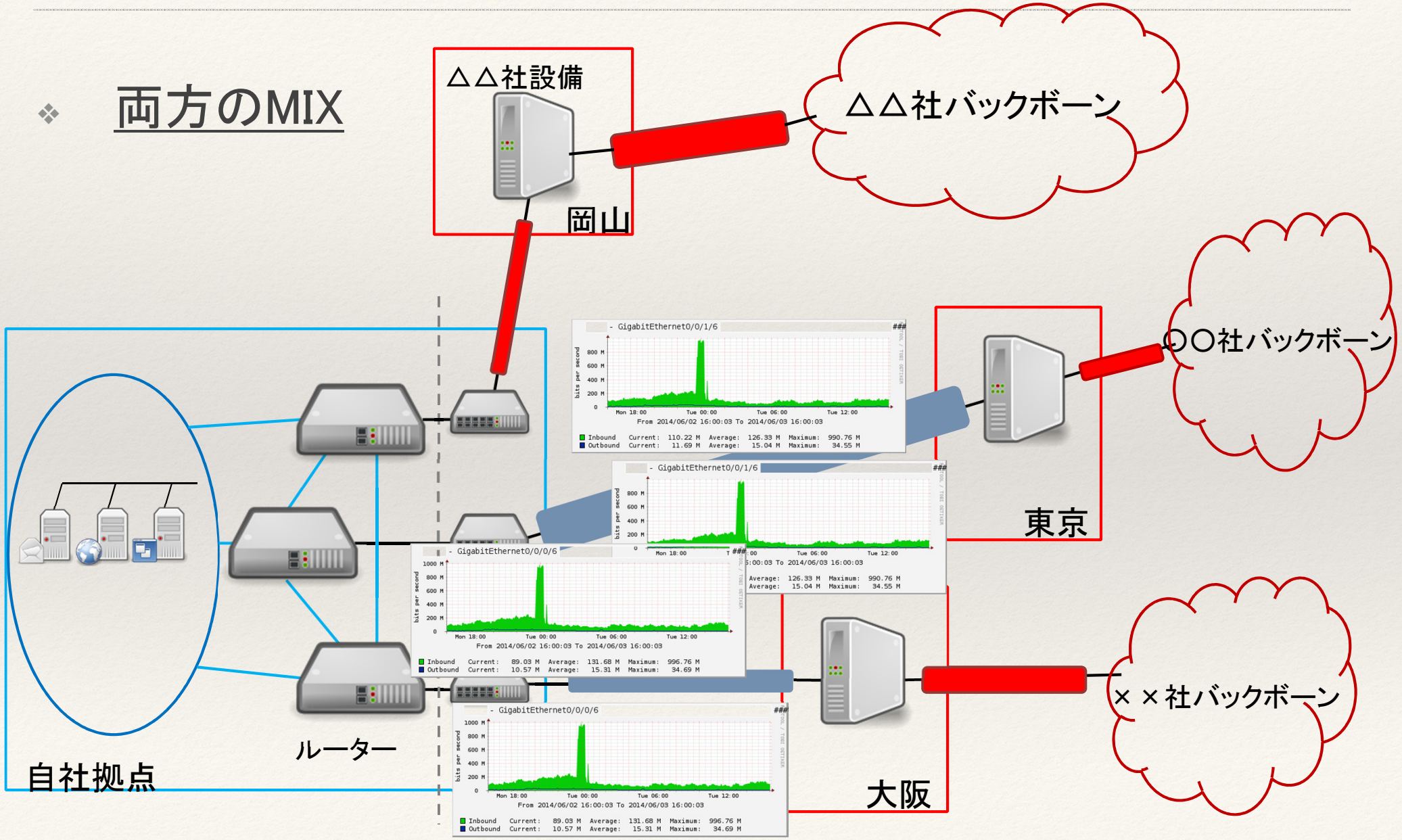
ネットワーク形態

- 東京・大阪で購入。



ネットワーク形態

- 両方のMIX



どう対応した？

- 弊社で行った対応
  - dest IPの特定。/32でのBlackHoleの依頼。
    - 該当IPをDHCPでomit。該当ユーザーの契約回線再開により、別IPアドレスにて再発。
  - 下り制御での影響範囲の軽減。
    - 元々、広報しているprefixで下り静的に決めれる環境にあった。
    - これを機に広報しているprefixの細分化
    - DDoS発生時に長距離回線自体をBlackHole化するようなもの。
    - なんとなく感じたこと。後述。

どう対応した？

- dest IP、source port でのFilter依頼。
  - 最終的にはこれで止まる。
  - NTPに関してはPCでの時刻同期も相手先により出来なくなるので、自社NTP Serverなどのユーザーアナウンス。
- ちなみに他の対応聞いてみました。（5社）
  - リアルに観測・検知したが、何らかの対応前に終わった。2社。
  - BlackHoleの依頼をしている最中に終わった。1社。
  - 後で気づいた。2社。
  - 想像している事。前述。

何が必要？

- ある程度、DDoSでのバーストが来る事を想定して、シミュレーションしておかないといけない。防災訓練。
- 下りをコントロール・制御したい。
  - AS PATHだけではちょっと。community みてlocal-pref変えてくれるとか、ある程度の細分化したprefixを受け取ってもらうとか(常時ではなくていいので)。
  - 上りはそこまでコントロール出来なくてもいいかな。どっちにしても対象にはならないし。
    - 尚更、隣接しているASが少ないならフルルートいらない。

何が必要？

- 対外接続回線・長距離線＜DDoS量となると、上位など対外接続先に依頼して止めてもらう。
  - ネットワークの可視化。DDoSを想定した監視。迅速化。
  - 回線を強化してもそれ以上のDDoS量になれば同じ。
  - 自分以外への影響もあり得る。トランジット提供側の監視体制もあると思うが、提供側へのエスカレーションも必要。
  - もちろん、対応してくれますよね？
  - 逆も考えましょう。自分も依頼があれば止めるスキームと訓練。
- どのような対応するかを踏まえた上での調達。

まとめ

- 質問・ディスカッション

ご清聴ありがとうございました