総務省 次世代IPインフラ研究会
第2回セキュリティWG 資料
平成17年1月20日

WG2-2

ISP協調運用の悩み

ソフトバンクBB株式会社
笹木 一義

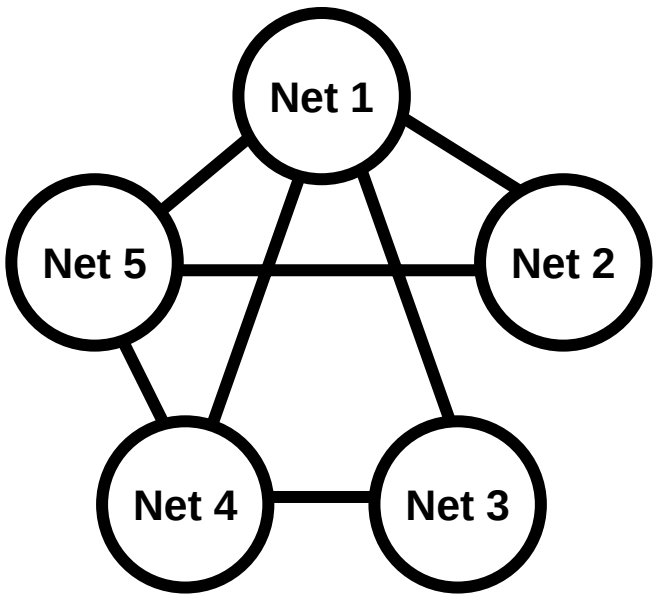
SOFTBANK BB

はじめに

- 本発表の内容
  - 弊社運用部隊からのヒアリングで得られた運用上の問題･困難･悩みを事業者間連携･国内Internetの共通問題という観点からまとめた
- 以下、あらかじめ御理解･御容赦頂きたく
  - 弊社の行き届かない所は棚にあげております
  - 一部第三者(通信事業者外)からの解決策を望むような提言がありますが、事業者個別の努力による解決策を否定するものではありません。
  - 以下内容は、すべて発表者(笹木)の個人的見解と御理解願います(不見識バイアスに御注意を!)

“ハブ”があるとうまい話もある

Internetの運用協調関係

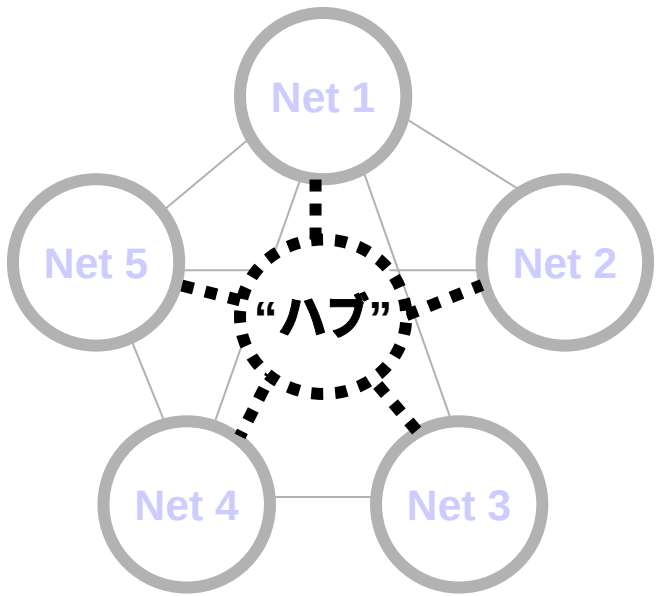


(部分)メッシュ構造

- 中心不在･仕切り人不在
- コミュニケーションの困難な2者関係が容易に発生

＋ 加えて ＋

追加で欲しい部分



“ハブ”を中心としたスター構造

- ハブ→中心→情報集約点･仕切り人
- ハブを経由したN対Nコミュニケーション

“ハブ”が無い事に関連したissue

- 2ホップ先問題
- NOC-NOCインターフェースばらばら問題
- 孤独なDNSオペレータ問題
- 全体的脅威への対応力問題

2ホップ先との協調運用の難しさ

- 「2ホップ(以上)先」のネットワーク(AS)とは？
  - 何のAgreementも無い(物理接続も無い)ネットワーク
  - そもそも「お前とPeeringしない」という事情だったりもする
- 障害対応・協調運用をする時に困難に直面する
  - whois(1)等の情報で（それらしい）コンタクト先をみつけて連絡
  - 普通の顧客は「2ホップ先」なんてことは理解してくれない
- 海外(文化が異なる)場合がとりわけ困難
  - 暗黙に期待するお願いに対するコミットメントの違い
  - 対処にかける時間感覚の違い
  - 「ほったらかし」＝「あたりまえ」のお国（お国柄）も
  - 国内だと「(感覚的に) 9割がた対応してくれる」
- 現場の声(wish)
  - 「特にやばい＊国」とは国対国レベルで事業者連携して障害対応できないか (深刻なセキュリティインシデントに限定せず)

NOC-NOCインターフェースがまちまち

- Transit/Peering Agreementに付随して連絡先情報は交換するものの、サービスレベルはまちまち。
  - 対応者のレベル・機能・権限;エスカレーション基準;インシデント対応力;Abuseポリシー＆対応力;提供される情報;言語;コミットメント etc…

→ 結果として自社顧客への説明に苦労することもある

- 相互接続先がN社あればN通りのインターフェースがあり得る

洋風のPeering Agreementの実例(抜粋)

(d) The parties will work together during the term of this Agreement to establish mutually agreed performance objectives and operational procedures to enable each party to provide the highest practical quality of service over its Internet Network and the interconnection provided hereunder, in a cost effective fashion. In connection therewith the parties shall use their reasonable efforts to achieve a minimum end-to-end one-way packet delay.

(i) Each of the parties will use its reasonable efforts to achieve a mean time to repair of four (4) hours or less for all outages at all Interconnection Points.

(ii) Both parties shall monitor the usage of each interconnection point. In the event either party detects an interconnection point exceeding 90% utilization for one hour for three consecutive days the detecting party shall initiate a discussion on how to increase capacity or reroute traffic to reduce utilization.

(e) Each party will, at its own expense and on a reasonable effort basis, provide NOC support in cooperation with the other. The parties shall develop operational procedures for resolving problems affecting the Interconnection Points, including inter-NOC problem management information exchanges (e.g., trouble ticket tracking) and NOC escalation procedures for addressing unscheduled outages or emergency maintenance.

(f) Each of the parties shall use reasonable efforts to secure their respective Internet Networks and traffic through the Interconnection Points from unauthorized access, transmission or use; furthermore, the parties shall cooperate to address security issues and develop security procedures.

和風の相互接続メモの実例(全文)

IXでのトラフィック交換における協調運用に関するメモ

2004年??月??日
????株式会社 技術本部

????????株式会社と????株式会社は、IXにおいて下記条件に従い相互にトラフィックを交換する。

○運用条件
トラフィックの交換は以下の運用条件のもとで行うものとする。

1. トラフィックの疎通に対する保障は行わないこととするが、BGP4のpeerを介した通信の維持について双方の通常業務に影響を与えない範囲で最善を尽くす。

2. この接続を経由したトラフィックが、双方のバックボーンネットワークに対して、通常のサービスを維持するのに支障をきたすと認められた場合には、事前連絡なしに、いつでもBGP peerを解除する事ができる。但し、BGP peerを作為的に解除した場合には必ず事後報告を行う。

3. 双方で交換する経路は基本的に双方の直後の顧客経路のみとし、具体的に交換する経路情報に関しては双方事前に連絡しあうものとする。それ以外の経路については協議の上決定する。

4. 双方とも互いのルータに対してデフォルト経路を向けないものとする。

○運用情報

【連絡窓口】

????????側窓口

住所: 〒???-????

所属: 技術本部
担当者: ????????<????@??.?????.net>
電話番号: 03-????-????
Fax番号: 03-????-????
e-mail: peering@??.?????.???

????株式会社側窓口

住所: 〒???-????
????????? ?-?-? ???? ??F
所属: 技術本部 ネットワーク技術部
担当者: ??? ???? <?????@????.ad.jp>
電話番号: 03-????-????
Fax番号: 03-????-????
e-mail: peering@????.ad.jp

【BGP設定に関する情報】

???????????株式会社側

AS名: ******-**
AS番号: ????
IPアドレス: ???.???.???.???(D**-*E)
???.???.???.???(**IX)
???.???.???.???(**NAP) # MED = IGP metric
広報するAS-PATH:

^(????_)+$
^(????_)+(????_)+$
^(????_)+(????_)+$
:

????株式会社側

AS名: ****
AS番号: ????
IPアドレス: ???.???.???.???(**IX) MED/60
???.???.???.???(JPIX) MED/50
???.???.???.???(D**-*E) MED/70
???.???.???.???(**NAP/TOKYO) MED/80
???.???.???.???(**NAP/OSAKA) MED/80

広報するAS-PATH

^(????_)+$
^(????_)+(????_)+$
^(????_)+(????_)+$
:
以上。

ネットワーク協調運用の現実

- 書面上のNOC-NOCインターフェースをショートカットする協調運用チャネルの存在・貢献が極めて大!
  - 某オペレーターコミュニティ
  - 某メーリングリスト(セキュリティ系・IX運用者系)
  - 某会員制組織
  - BGPオペレータ個々人の私的繋がり
    - IX事業者主催の懇親会、飲み会、焼肉会
- スッキリしたい「通信の秘密」&「個人情報保護」
  - 建前:「君子危きに近よらず」「李下に冠を正さず」
  - 現実:個人的信頼ベースでの真摯な・密やかな情報共有
    - 圧倒的にこちらのほうが有用・効果的・即時的
    - しかしその行為がどこまで公に許されている事なのかよくわからない

    → 十分注意もしており、たぶんOKだろうと思ってはいるものの…

→ガイドライン化とともに公的是認もアリでは？

DNS(等)サーバ運用の情報共有

- 言うまでも無く、DNSはインターネットの最重要インフラ
- ISP DNS屋が孤独感を感じた時
  - 存在しないドメインの問い合わせ急増でDNSサーバ負荷上昇!
    - 原因：ヘッポコPnP実装(?)、DDoSゾンビ(?)、Spamゾンビ(?)
  - 顧客がMS＆Y!全不通(DNS引けず) → すわ自社DNS大障害か!?
    - 原因：某DNSロードバランス屋(米国)がこけてた

  → いずれも蓋を開けてみれば各社共通の悩み(のはず)
- お悩み情報共有したいけど、どこに相談したら良い？
  - c.f. BGP屋コミュニティは活発

全体的脅威への対応力は十分か?

- インターネット全体(少なくとも日本全体)を見て即応的に仕切るものは存在しない
- 果たして組織的な攻撃(テロ)が発生した場合に対処できるのか？
  - 幸いこれまではそうしたものが無かったが…

とはいえ…

- 仕切り人がいると面倒なこと(面倒におもう人)もある
- そもそも、だれも仕切らないからこそ”Inter-net”

おまけ

愚痴等

- ＊国の近隣IPアドレスブロック使っていると、まとめて遮断されて泣く
- 戻りルーティングの確認は困難なので、各社で他事業者向け traceroute サイトを用意すると良いかもしれない
  - or 各社経路情報を何らかの”ハブ”に集約参照
- 最先端のセキュリティ情報は英語に集中
  - 日本語読み書きだけではやっていけない
- ネットワークセキュリティベンダーの料金根拠が謎(「ボッタクリ感」あり)

人材問題

- 懸念:「エンジニアが小粒になりつつある」
  - 個々のエンジニアが小領域の技術の専門職化
  - Internetの社会における規模･位置づけの変化が原因と見る
- その昔
  - のんびり
  - 「インターネット」＝マニアの世界
  - 副業的担当、ベストエフォート、仕事＝趣味の延長(?)、
  - 一人でサーバ･ルータ･ネットワーク･ヘルプデスクまで全部看る
  - 「現用設備で覚えました。止めちゃったこともあるよ。」
- 今
  - キチキチ
  - 「インターネット」＝社会インフラ「絶対落とすな！」
  - 変な操作するな、ミッションクリティカル
  - ネットワーク技術の高度化･複雑化 → 業務の細分化･専門化
  - 「ベンダーのラボ設備で覚えました。現用止めたらボーナス無いです。」
- セキュリティ技術者育成
  - 各々の技術者の守備範囲を意識的に広げる事も考慮したい
  - セキュリティ技術は技術の総合格闘技的な側面あり