JPNIC総会講演会「IPにおけるアイデンティティとロケーション」のご紹介

- 社団法人日本ネットワークインフォメーションセンター
- IP事業部　奥谷泉

講演概要

- 日時
  - 2007年6月15日(金)16:00-17:30
- 会場
  - ホテルエドモント(飯田橋)
- 講演者
  - APNICチーフサイエンティスト　Geoff Huston
- テーマ
  - IPアーキテクチャにおける通信先のアイデンティティおよびロケーションの特定の仕組みに関する考察

現在のIPアーキテクチャにおける課題

- 通信先をインターフェース/セッション/ネットワーク単位で特定
  - 同一人物による通信であってもインターフェース/セッション/ネットワークが異なれば異なった通信先として識別

- しかし、インターネット上でのコミュニケーションにおいて実現したいことは通信したい相手を特定し、その相手と通信すること
  - 通信相手の特定はインターフェース/セッション/ネットワークを越えて普遍であることが望ましい

- 通信元/相手に安定したアイデンティティを付与することは可能か？

アイデンティティに求められるものは?

- 様々な程度での以下の特性:
  - 一意性
  - 持続性
  - 構造
  - 明確な適用範囲
  - 有効性と正当性
  - 権限の明確化

  - アイデンティティとは一方的に定められるものではない
    ー むしろ、一般に理解されている文脈において生み出された一意性の認知と捉えた方がよいだろう

※総会講演会資料より抜粋

現在提供されている技術:

- モバイルIPv4
- モバイルIPv6
- アドホックネットワーキング
- NEMO
- HIP
- SCTP
- SHIM6
- Teredo
- ダイナミックDNS
- NAPTR および　SNAPTR DNS RRs

※総会講演会資料より抜粋

実現方法の検討

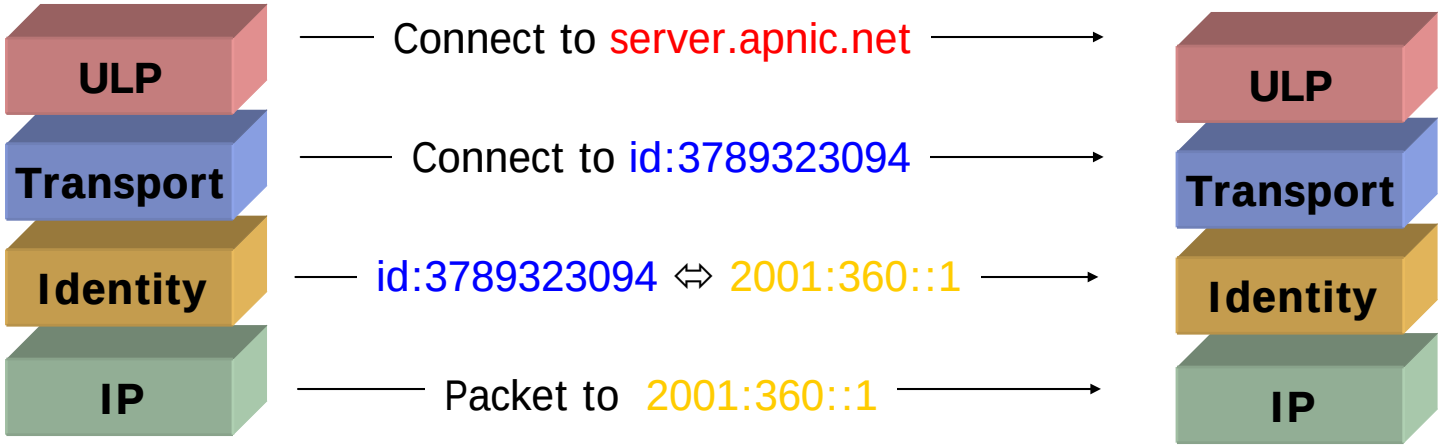
- プロトコルスタックモデルのどのレベルにおいてもアイデンティティオブジェクト(アイデンティティ情報)を注入することは可能
  - トランスポートセッションをまたがる「アプリケーションアイデンティティ」
  - スタックロケーションの変更を吸収できる「トランスポートアイデンティティ」
  - 保持しているすべてのセッションにおけるロケーションの違いを吸収した「ホストアイデンティティ」

- ここでいう「アイデンティティ」とは、通信の両(もしくは複数)サイドにおいて、複数のロケーターが、単一の通信状態にあることを認識するためのトークンである

※総会講演会資料より抜粋

アイデンティティの実現

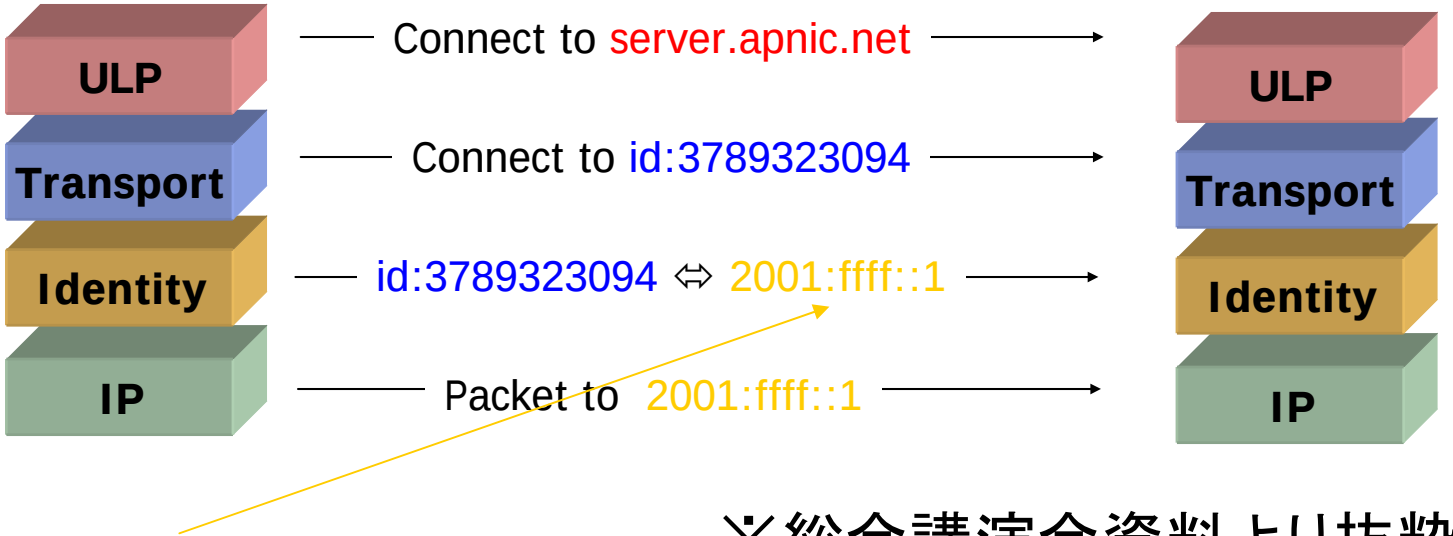
- アイデンティティのマッピングはどのように機能するのか?



※総会講演会資料より抜粋

アイデンティティの実現

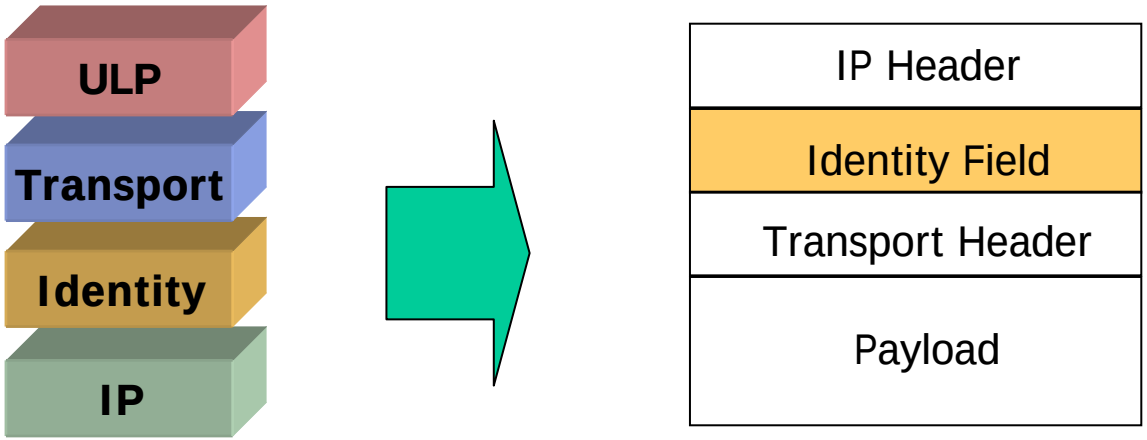
- アイデンティティのマッピングはどのように機能するのか?



※総会講演会資料より抜粋

アイデンティティの実装

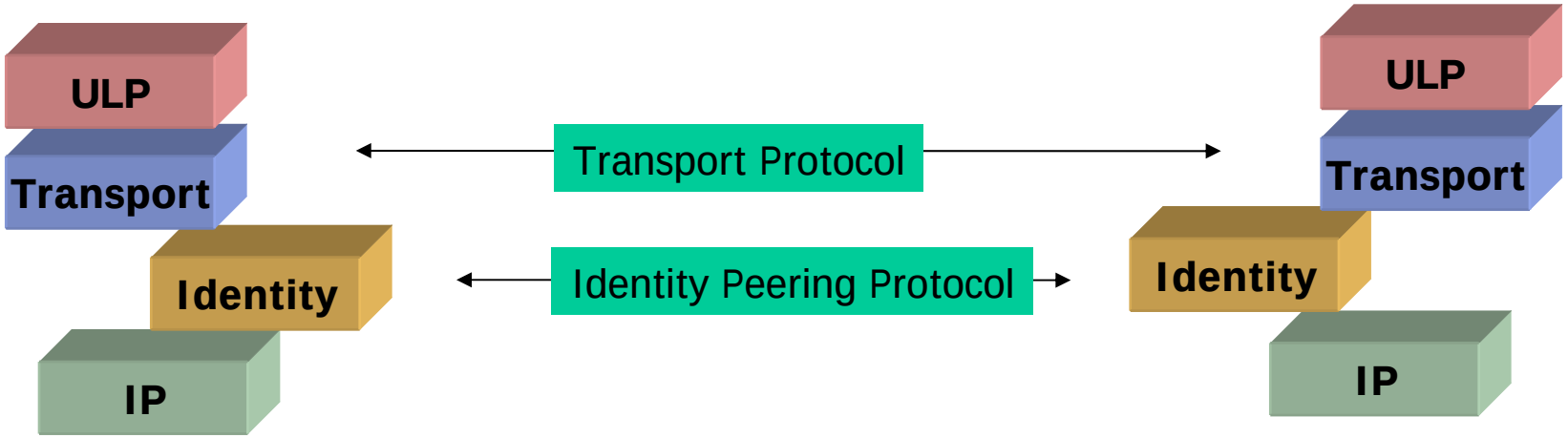
- 従来型
  - 上位層のプロトコルデータユニット(PDU)に対して wrapper(包むもの)を加え、インバンド空間を利用して 同じレイヤーでの通信相手(ピアエレメント)と通信を行う



※総会講演会資料より抜粋

アイデンティティの実装

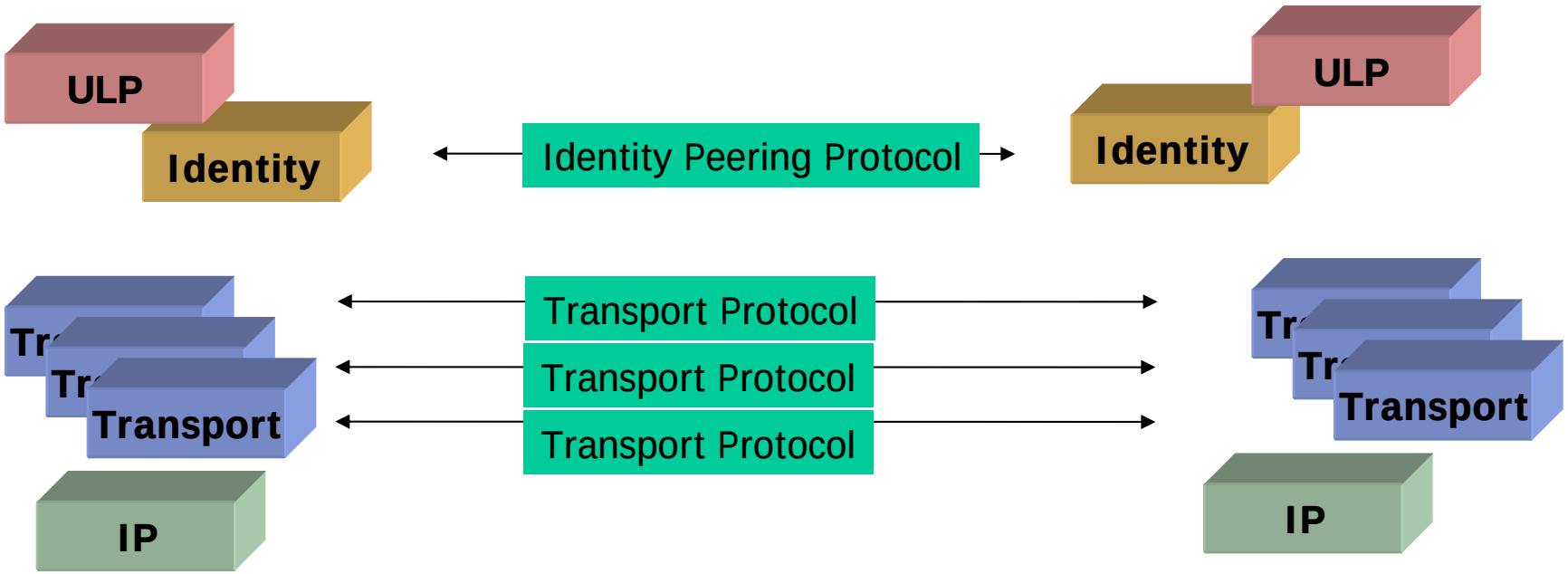
- アウトオブバンド型
  - プロトコルエレメント(プロトコル階層における各要素)がピア(通信相手)と情報交換できるよう、それぞれ別個のプロトコルを利用する



※総会講演会資料より抜粋

アイデンティティの実装

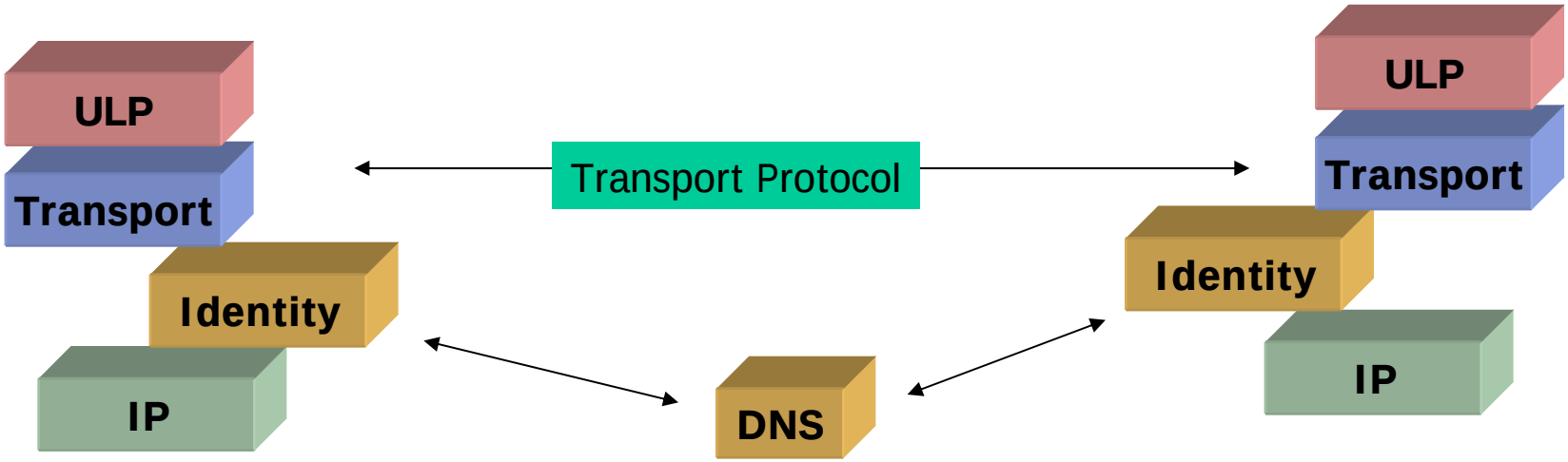
- アプリケーションのアイデンティティ: セッション層の上で実現



※総会講演会資料より抜粋

アイデンティティの実装

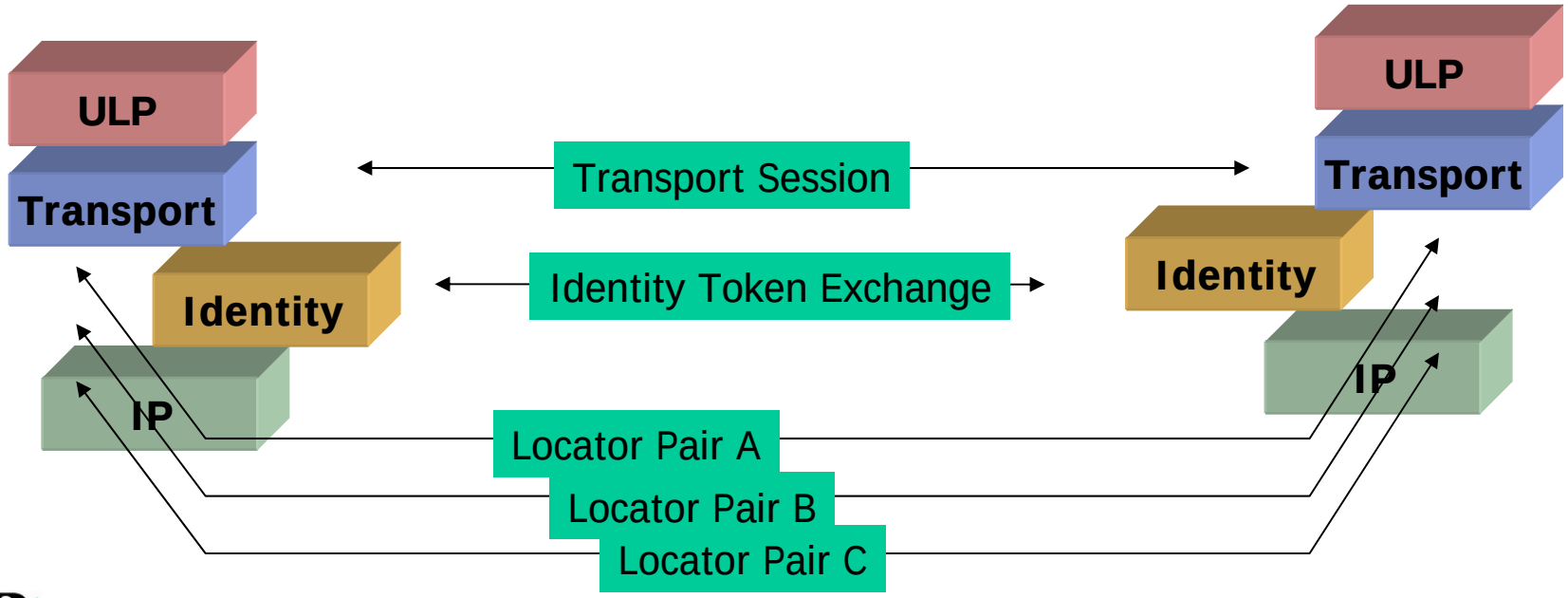
- 参照型
  - ピアリングの手段として、第三の参照ポイントを利用(例. DNSの識別子)



※総会講演会資料より抜粋

アイデンティティの実装

- 自己参照型
  - ロケーター群に該当するトークンとしてその時々に応じた便宜上のアイデンティティを利用する



※総会講演会資料より抜粋

IPレベルでのアイデンティティ

- アイデンティティとロケーターの紐付けを複数のセッションで共有することはできるか?
  - 共通のエンドポイントに向かうすべてのセッションがマッピングされている状態を実現するための、アイデンティティとロケーターのマッピング(紐付け)によるオーバーヘッドの削減
  - セッション指向(session oriented)のトランスポートプロトコルと(可能性としては)データグラムトランザクションの両方に対応した、より包括的なアイデンティティを提供できるようにしたい
  - アプリケーションおよびトランズポート層におけるセッションの複雑さを軽減し、IPレベルでエンドポイント単位でのマッピングができる機能を備える

※総会講演会資料より抜粋

アイデンティティの種別

- プロトコルの“アドレス空間”より抽出されたアイデンティティトークンを利用する
  - DNS, Appns, “特定のアドレス”をトランスポートが操作
  - IPの機能でロケーターに対応
  - プロトコルスタックエレメント(プロトコルスタックの各要素)でマッピングを実施
- FQDN をアイデンティティトークンとする
  - これは循環依存を生み出すか?
  - これはDNSの機能に対して無理な要求を強いることになるか？
- 体系化されたトークン
  - 新たなトークン空間の、上記の方法と区別される固有の特性はどんなものになるか？

- 体系化されていないトークン
  - 世界的な一意性は必ずしも保証されないアイデンティティ・トークンの自己生成 (便宜的なトークン)
  - 検索機能を利用してアイデンティティトークンとロケーターのマッピングをどのように行うか？またはそのようなマッピング機能の実装を回避する術はあるか？

※総会講演会資料より抜粋

アィデンティティとして利用できそうなもの

- IPv4アドレス
- Centrally Assigned IPv6 Unique Local Addresses(IPv6 ULA)
- 暗号技術を使った公開鍵のハッシュ値
- 暗号技術を使ったロケータのハッシュ値
- 通信の開始にあたり、IPv6アドレスを利用する
- IPv6アドレス
- DNS名
- URI
- 電話番号

※総会講演会資料より抜粋

アイデンティティ分野における課題

- エンドポイントの識別子として新たにグローバルに一意であるトークンの分配体系を維持するには多大な労力とコストがかかる
  - 一意性は安くない!
- 既存のトークンセットをアイデンティティセットとして利用した場合の影響
  - リサイクルは危険!
- ロケーターとアイデンティティのダイナミックな紐付けへの対応
  - スピード vs 正確性
- データグラム通信におけるアイデンティティ・ハンドシェイクのためのプロトコルのオーバーヘッド
- アイデンティティの完全性を保つためのセキュリティ

※総会講演会資料より抜粋

一花独放，一家主鳴 *

- アイデンティティモデルは単一であるべきか?
  - すべての要求を強制的に単一のアイデンティティ体系にまとめることはできるのか？
  - もしくはアイデンティティとして望ましい性質が多用であるがため、それらが衝突することもあり、ひとつの解決策はないのか？
  - これまで考察してきた方法の多くは特定のひとつのアイデンティティ体系のみに重点を置き、他のアイデンティティ体系が並行して実装されていた場合の影響は考慮していない
  - 一方、今日のIPアーキテクチャにアイデンティティ機能に改造を加えようとした場合、例えそれが他のアイデンティティ機能に枝分かれしないとしても、古くからの要求にも対応することがすでに充分に厄介である

※総会講演会資料より抜粋

では今後どうすればよいか？

- もっと学ばなければいけないことは多いようだ
  - ルーティングにおけるスケーリング、リナンバやマルチホームの回避に留まらない
  - IPv4、IPv6に留まらない
  - 多様なコミュニケーションの環境やサービスへの対応にあたり、敏捷で柔軟なパケットネットワークモデルをもし望むのであれば、発信者の意図が、可能な通信方法とどれほど乖離しているか理解する必要がある

※総会講演会資料より抜粋

講演内容について

- 当日はIPv4とIPv6の問題とからめて発表が行なわれたが、応用範囲は広いと思われる

Q&A