インターネット数理科学第８回

～ネットワークそのものを支える数理科学その３～

2006年11月30日

株式会社インターネット総合研究所代表取締役所長
東京大学大学院数理科学研究科客員教授

藤原　洋

目　　次

1．ネットワークそのものを支える数理科学とは？

現在のインターネット数理科学の課題

③（ネットワークの）あちら側

⇒「グラフ理論」「金融工学理論」に基づくデータベース、検索
エンジン最適化、検索連動データベース、ネット金融サービス

①ネットワークそのもの

⇒「グラフ理論」による動的ルーティング、帯域制御、放送型ルーティング
「ディジタル信号処理理論」に基づく変復調技術

②（ネットワークの）こちら側

⇒「ディジタル信号処理理論」に基づくコンテンツ符号化技術

今後の「インターネット数理科学」の講義の進め方

IRI
Ubilabs Innovations

以下の3つの分野にわたって①②③⇒①②③⇒・・順に

③ネットワークのあちら側を支える数理科学

⇒「グラフ理論」「金融工学理論」に基づくデータベース、検索
エンジン最適化、検索連動データベース、ネット金融サービス

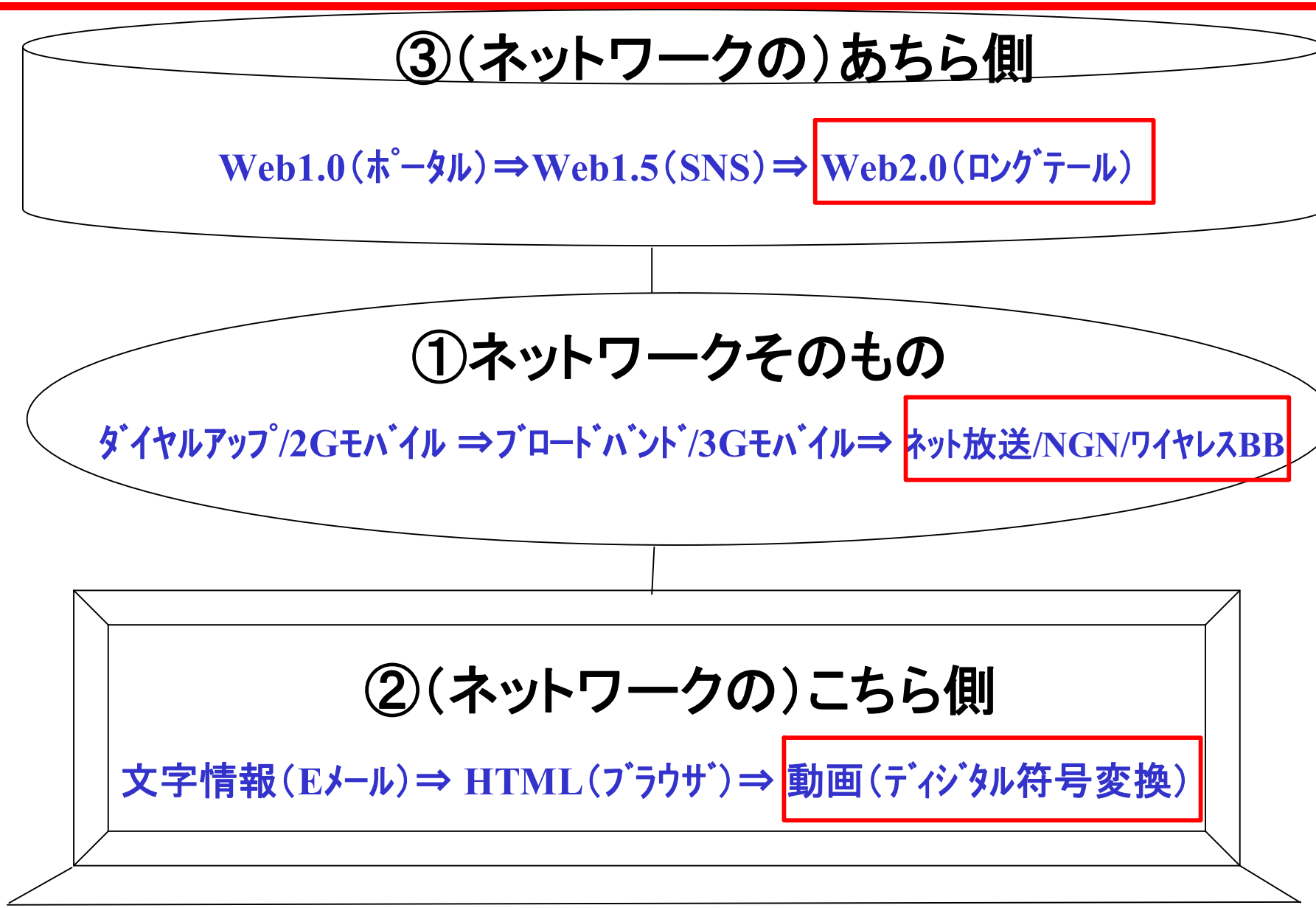
①ネットワークそのものを支える数理科学

⇒「グラフ理論」による動的ルーティング、帯域制御、放送型ルーティング
「ディジタル信号処理理論」に基づく変復調技術

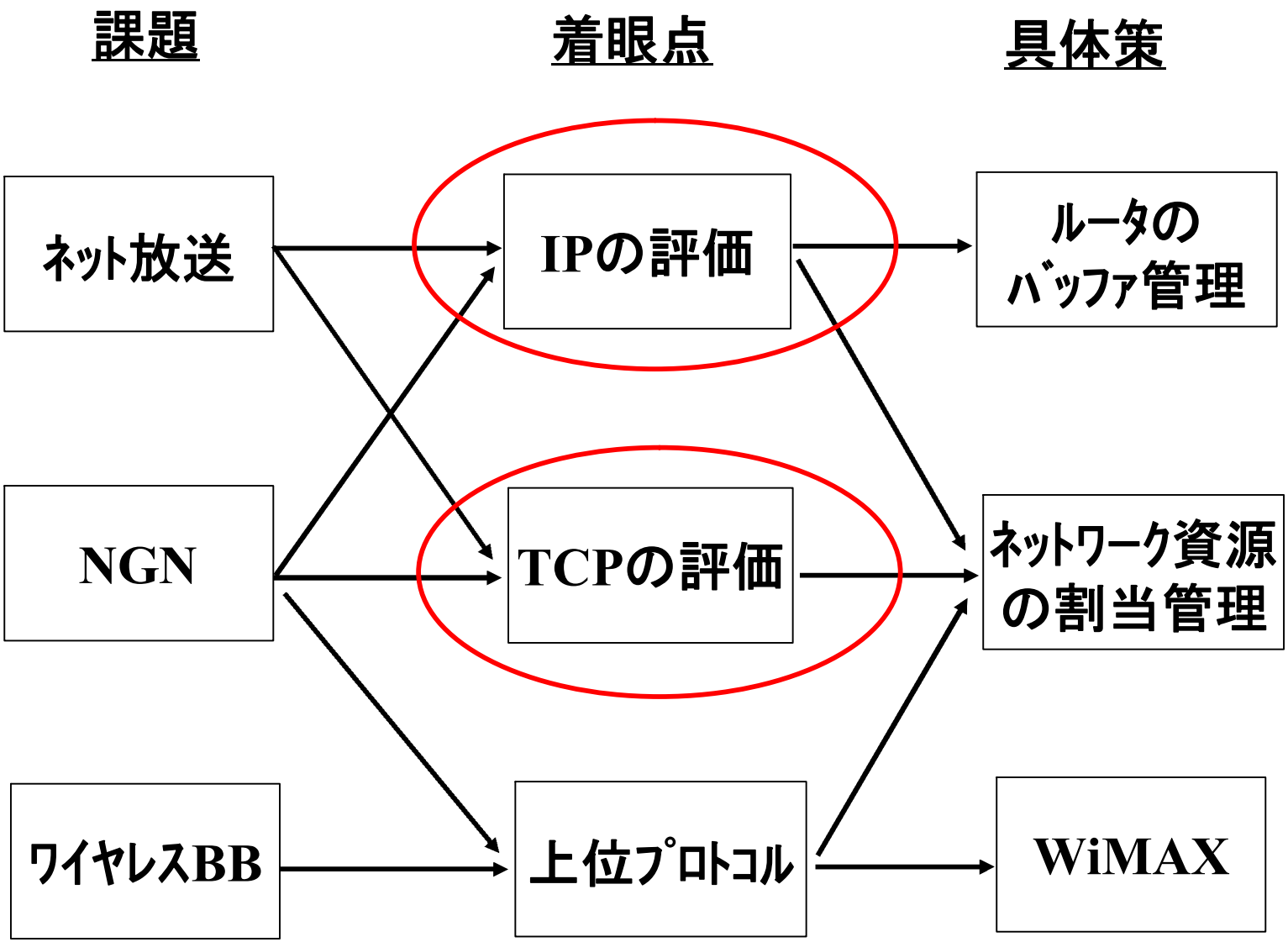
②ネットワークのこちら側を支える数理科学

⇒「ディジタル信号処理理論」に基づくコンテンツ符号化技術

インターネットにおける技術革新と最先端のテーマ



IP放送/NGN/ワイヤレスBB(ブロードバンド)などに潜在する数理科学とは？



2. ルーティング（経路制御）とは？

ルーティングの実際

IRI Ubilabs Innovations

1. ルータがルーティング・プロトコル・プログラムを実行し、ネットワーク内の他のルータとルート情報交換を実施
2. ルータが、同上情報を使用し、特定のルーティング・プロトコルに関連したルーティング・テーブルを作成
3. ルータが、複数のルーティング・プロトコルが動作している場合、各種ルーティング・テーブルを参照し、宛先への最適パスを選択
4. ルータが、該当する宛先に、ネクスト・ホップ・デバイスに付属するデータリンク・レイヤ・アドレスと、ローカル出力インタフェースとを関連づけ。通常は、ネクストホップデバイスは、他のルータ。
5. ルータのフォワーディング・テーブルにネクストホップ・デバイスの転送情報（データリンク・レイヤ・アドレスとローカル出力インタフェース）を書き込む。
6. ルータが、パケット受信し、ヘッダーから宛先アドレスを検出。
7. ルータが、フォワーディング・テーブルにネクストホップ・デバイスの転送情報（データリンク・レイヤ・アドレスとローカル出力インタフェース）を取得。
8. ルータが、付加機能*を実行し、パケットを適切なデバイスへ転送。
   *IP-TTL（パケットの有効期間を表す値）の減少、IP-TOS（Type of Service）操作等。
9. 以上の手順を宛先ホストに届くまで繰り返し実行。

動的ルーティング

IRI
Ubilabs Innovations

自動的にルーティングテーブルを構築する方法によって、経路制御を実行しようというものである。ルーティングテーブルの構築は、ルーティングプロトコルによって伝えられる情報に基づいておこなわれる。これによって、通信の断絶が起きないように、自律的なルーティング機能が実行されるが、現実には、意外と高度な技術が要求され、*現時点ではルーティングが完全に自動的に行われていない。*

インターネットのようなパケット交換方式ではデータはパケットに分解される。パケットには個々に宛先アドレスが付加され、独立にルーティングされる。
対照的な方法である公衆交換電話網のような回線交換方式でも、電話の発呼のように、回線への経路を探すためにルーティングが行われる。しかし一旦接続が成立すれば、完全な宛先をラベルとして貼らなくても連続的に大量のデータを送ることができる。

ルーティングを行う装置としては、スイッチングハブ、レイヤ3スイッチ、ルーターなどがあるが、一般的にルーティングと言う場合にはレイヤ3以上のアドレス（ここではIPアドレス）に関する経路制御を指す。

動的ルーティングの基本的考え方

IRI Ubilabs Innovations

　指示された経路が有効でなくなっている場合、現存するノードを使った別の経路を決めなければならない。
　これは通常ルーティングプロトコルと経路決定アルゴリズムによってなされる。経路決定アルゴリズムには二種類ある。

①距離ベクトルアルゴリズム (distance vector algorithm, DVA)

RIP (Routing information Protocol)

②リンク状態アルゴリズム (link state algorithm, LSA)

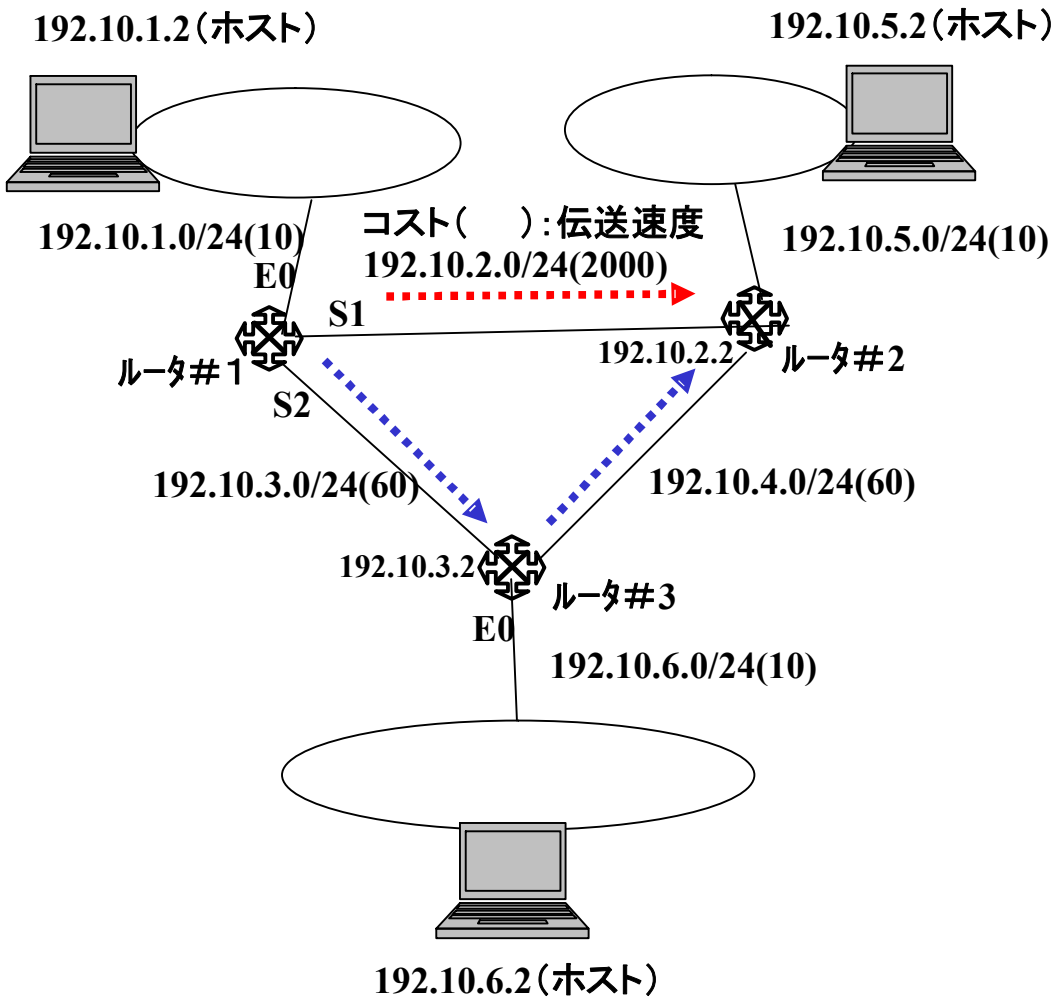
OSPF (Open Shortest Path Fast)

IS-IS (Intermediate System-to- Intermediate System)

この内どちらか一方が用いられる。
　インターネット上の経路決定問題は、これら2つに尽きる。
以下用いられる「コスト」ないし「距離」は経由するルータの数（「ホップ数」）や回線速度を数値化したもので、「メトリック metric」と呼ばれる。メトリックの決定法はプロトコルによって異なる。

ルーティングの基本動作

RIPまたはOSPFで



①距離ﾍﾞｸﾄﾙｱﾙｺﾞﾘｽﾞﾑ：DVA (distance vector algorithm)

DVAは Bellman-Ford アルゴリズムを用いている。この方法では、各ノード間に「コスト」と呼ばれる数値が割り振られる。二点間を結ぶ経路のコストは、その間に経由するノード間のコストの総和であり、その情報はノードから得られる。

アルゴリズムは極めて単純である。最初の段階では、各ノードは直近のノードがどれかという情報と、それらの間とのコストだけを知っている（このような、「行き先リスト」とそれぞれの総コスト、やりとりするべき「次の相手(next hop)」を集めたものがルーティングテーブルないし、ディスタンステーブルである）。

代表例としてRIP (Routing information Protocol)がある！

定期的にノード間でやりとりがなされ、互いにルーティングテーブルのデータを交換する。もし隣から渡されたデータに、自分のルーティングテーブルより優れたもの（同じ行き先に到達するのに、コストが少ない）があれば、それを用いてテーブルを更新する。自分のテーブルにない相手への情報が入っていた場合も同様である。時間をかけると、全てのノードがあらゆる宛先についての最良の「次の相手」と最良の「コスト」を見つけだす。

あるノードが脱落した場合は、そこを「次の相手」としていたノード全てにおいて、ルーティングテーブルの破棄と再構築が行われる。この情報は隣のノードに次々 伝えられて行き、最終的には到達可能な全てのノードについて最良の経路が発見されることになる。

②リンク状態アルゴリズム：LSA（ link state algorithm ）

LSAでは、各ノードが用いるのはネットワークのマップであり、それはグラフの形で格納されている。このマップをつくるために、全てのノードがネットワーク全体に「自分が接続しているノード」をブロードキャストする。各ノードはそのデータをもとに、個々独立してマップを計算し生成する。自分で生成したマップをもとに、各ノードは他のノードへの最短経路を決定する。
最短経路の計算にはダイクストラのアルゴリズムが用いられる

このアルゴリズムはネットワーク全体を木構造で表現する。木の根（最初の要素）は各ノードそれ自体である。次いで、ノードの集合から未登録のノードを一つずつ木に加えていく。

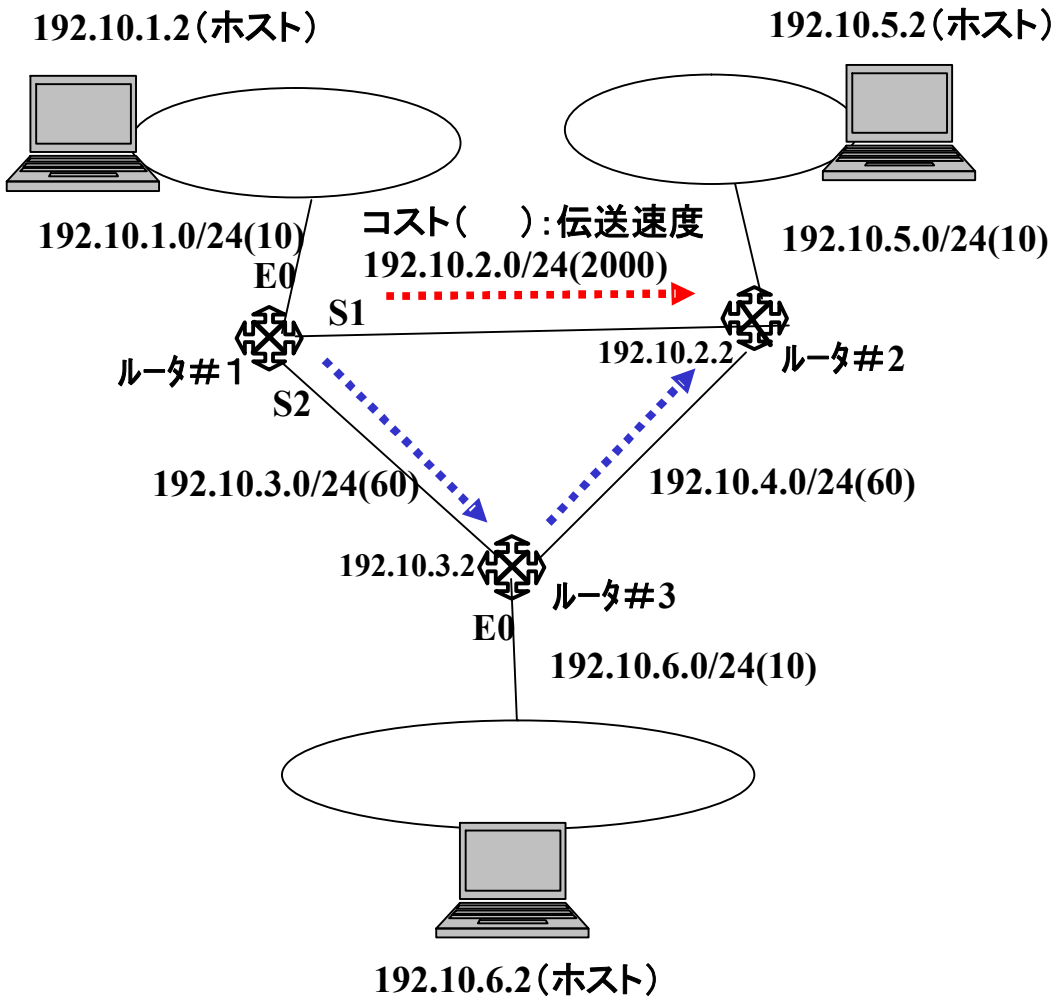
加えるノードは既に木に存在するノードのどれかから到達できるノードのうち、最も少ないコストで到達できるものである。ネットワーク上の全てのノードを登録するまでこれを繰り返す。

木構造ができあがったら、それを用いて、ルーティングテーブルをつくる。最良の「次の相手」等がそこに登録される。

代表例としてOSPF (Open Shortest Path Fast)がある！

DVAかLSAどちらが有利か？

RIPまたはOSPFで



ルータ＃1のルーティングテーブル（RIP）

宛先	ネクストホップ	ホップ数
192.10.1.0	接続（E0）	—
192.10.2.0	接続（S1）	—
192.10.3.0	接続（S2）	—
192.10.4.0	192.10.2.2 (S1) 192.10.3.2 (S2)	1 1
192.10.5.0	192.10.2.2 (S1)	1
192.10.6.0	192.10.3.2 (S2)	1

ルータ＃1のルーティングテーブル（OSPF）

宛先	ネクストホップ	コスト
192.10.1.0	接続（E0）	—
192.10.2.0	接続（S1）	—
192.10.3.0	接続（S2）	—
192.10.4.0	192.10.3.2 (S2)	120
192.10.5.0	192.10.3.2 (S2)	130
192.10.6.0	192.10.3.2 (S2)	70

DVAの課題と対策

IRI
Ubilabs Innovations

1．RIP-1では、ホップ数だけを指標とするため、ルータ#1からルータ#2経由でネットワーク192.105.0へは直接パスを選択するが、実際は、ルータ#3経由の方が有利。

2．ホップ数の上限値（通常は15）があり、超えると到達不能となる。

3．ルート情報交換に定期的ﾃﾞｨｽﾀﾝｽ･ﾍﾞｸﾀｰ･ﾌﾞﾛｰﾄﾞ　キャストを用いるため、ﾀｲﾏｰ起動間隔でしか更新さrないため、障害発生からの収束時間が遅くなる。

→RIP-2での対策：ﾄﾘｶﾞｰ･ｱｯﾌﾟﾃﾞｰﾄ（障害発生時）

4．クラスフルでVLSMやCIDRをサポートしていない。

→RIP-2とEIGRPは、VLSM、CIDRをｻﾎﾟｰﾄ！

→IGRP（Interior Gateway Routing Protocol）とEIGRP（Enhanced Interior Gateway Routing Protocol）は、ﾊﾟｽに沿ったﾘﾝｸ特性をﾒﾄﾘｯｸに組合せた計算機能あり！

VLSM（Variable Length Subnet Mask：可変長サブネットマスク）

クラスフルアドレッシングの「クラスネットワークでは同一のサブネットマスクを使用する」という制限をなくす技術。
１つのネットワークで異なるサブネットマスクを使用することができるようになり，サブネットをさらにサブネット化したり，複数のサブネットをまとめて1つの大きなサブネットにしたりすることが可能。

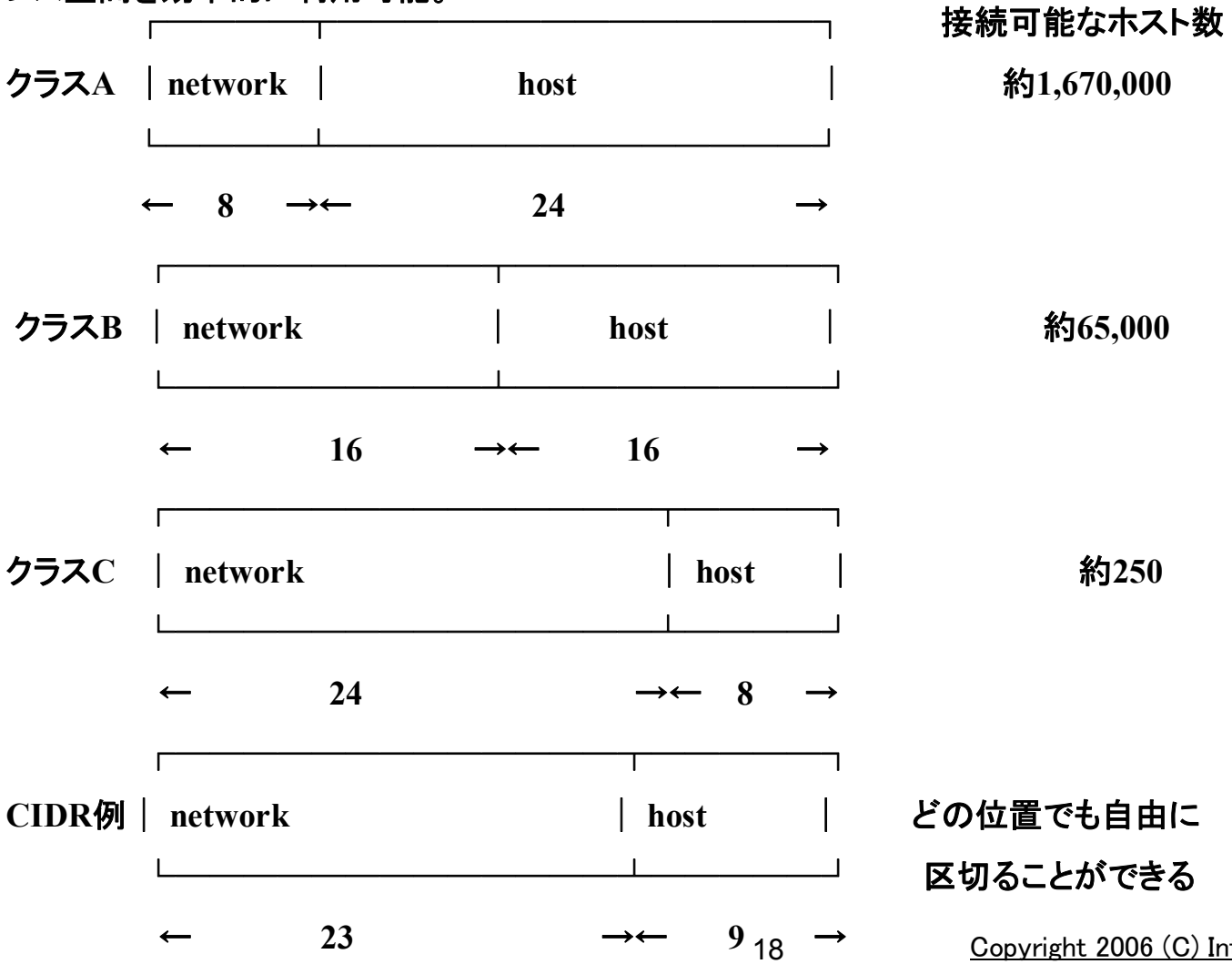
このVLSMの利用の効果

①IPアドレス割当に生じる無駄を省く。
②ネットワークで使用できるIPアドレス実数の増加
②ルート情報を集約

CIDR（Classless Inter-Domain Routing）

Ubilabs Innovations

サイダーと読む。CIDRは、クラスを使わないIPアドレスの割り当てと、経路情報の集成を行う技術。クラスとは、IPアドレスのネットワーク部とホスト部を決められたブロック単位 で区切る方法で、簡単だがアドレス空間の利用に無駄が生じる。これに対しクラスを使わないCIDRでは、任意のブロック単位で区切ることができ、IPアドレス空間を効率的に利用可能。



LSAの特徴とメリット

IRI Ubilabs Innovations

1. 反復分散ﾃﾞｰﾀﾍﾞｰｽﾓﾃﾞﾙ使用したより複雑なﾌﾟﾛﾄｺﾙ
2. ﾘﾝｸｽﾃｰﾄ（情報要素：ﾄﾞﾒｲﾝ内ﾘﾝｸやﾉｰﾄﾞの情報）をﾙｰﾀが交換
3. ﾙｰﾃｨﾝｸﾞ・ﾃｰﾌﾞﾙは、交換せず、隣接ﾙｰﾀ、接続に関するﾒﾄﾘｯｸ情報を保有。
4. ｼﾞｸﾞｿｰ・ﾊﾟｽﾞﾙ型ｱﾙｺﾞﾘｽﾞﾑで、ﾄﾞﾒｲﾝ内の全ﾉｰﾄﾞが、ﾊﾟｽﾞﾙﾋﾟｰｽ情報のｺﾋﾟｰを受信。
5. ﾈｯﾄﾜｰｸ内の各ﾙｰﾀは、個々にﾊﾟｽﾞﾙを組み立てる。

→ホップ数に制約されない
→リンクの帯域と遅延を計算可能
→収束の速さ
→VLSMとCIDRをサポート
→階層化に優れる

しかし、LSAは、ﾄﾞﾒｲﾝ間ﾙｰﾃｨﾝｸﾞへの適用不可！

そこで、DVA型の*BGP*をﾄﾞﾒｲﾝ間ﾙｰﾃｨﾝｸﾞへ適用！

DVAかLSAどちらが有利か？

①Routed protocol

ネットワークプロトコルのうち、パケットを転送すべきネットワーク層のアドレスについて十分な情報を与えるもの全てを呼ぶ。その情報を用いて、アドレッシングスキームに基づき、あるホストから他のホストへパケットの転送がなされる。Routed protocolはパケットに付加されたフィールドのフォーマットと利用法を定義するものである。パケットは端末から端末へ運ばれる。Internet Protocolが代表である。

②Routing protocol

ネットワーク間でルーティング情報を交換するための方法。これによって、ルータは動的にルーティングテーブルを生成可能。

伝統的なインターネットプロトコル(IP)によるルーティングは単純である。というのも、パケットを転送すべき「次の相手(next hop)」を用いているだけで、そこから先の経路については何も考えなくてよいからである。

この動的ルーティングは非常に複雑なものになりうるが、インターネットの柔軟性をもたらしているものでもあり、IPが用いられるようになって以来、8桁も大規模化しているが拡張性が実証。

ルーティングメトリック routing metric

1. 経路の優劣を比較できれば実はどんなものでもいい。

●帯域幅（≒データ転送速度） ●遅延 ●ホップ数 ●経路のコスト ●負荷
●MTU（Maximum Transmission Unit） ●信頼性 ●通信コスト 等

2. ルーティングテーブルは利用可能な最良の経路を記録するだけ

3. リンク状態、あるいはトポロジーのデータベースはそれ以上の情報を持

4. 管理上の距離 (Administrative distance) は複数のルーティングプロトコルで、同一の宛先に対し別の経路を最適とした場合、その中から最良のものを選択するのに用いられる値。この値は、ルーティングプロトコルの信頼性を定義するもので、その値によってプロトコルの優先順位が決まり（値が低い方が一般には優先される）、Preferenceと呼ばれる。

5. 他の自律システム (autonomous system, AS) に対するルータの相対的な位置によって、様々な種類のルーティングプロトコルが存在。

３．AS間のルーティング（経路制御）

～ドメイン間ルーティングの基本～

ドメイン間(ポリシーで決まる)ルーティングの小史

- 1987年完成したNSFNETでは初期のEGP (一般的なExterior Gateway Protocolではない) を使用
  - ⇒ ・ルーティンググループ上の制約
    ・トポロジー上の制約
- 現在：
  インターネット上の事実上の標準＝BGP-4

3つのルーティング手法

IRI
Ubilabs Innovations

1. スタティック・ルーティング
   - ルータに手作業で宛先を設定
   - ネットワークの状態は不問

2. デフォルト・ルーティング
   - ルータの知らない宛先のトラフィックを所定の出口へ送る
   - 唯一の出口で接続されるドメインで使用

3. ダイナミック・ルーティング
   - インテリア・ルーティングやエクステリア・ルーティングから学習したルート
   - ネットワークの状態に依存

AS(autonomous system)

インターネットにおける自律システム(autonomous system)（AS）とは、インターネットに接続する1つ（時に複数）のルーティングポリシー配下にあるIPネットワークやルータの集合。

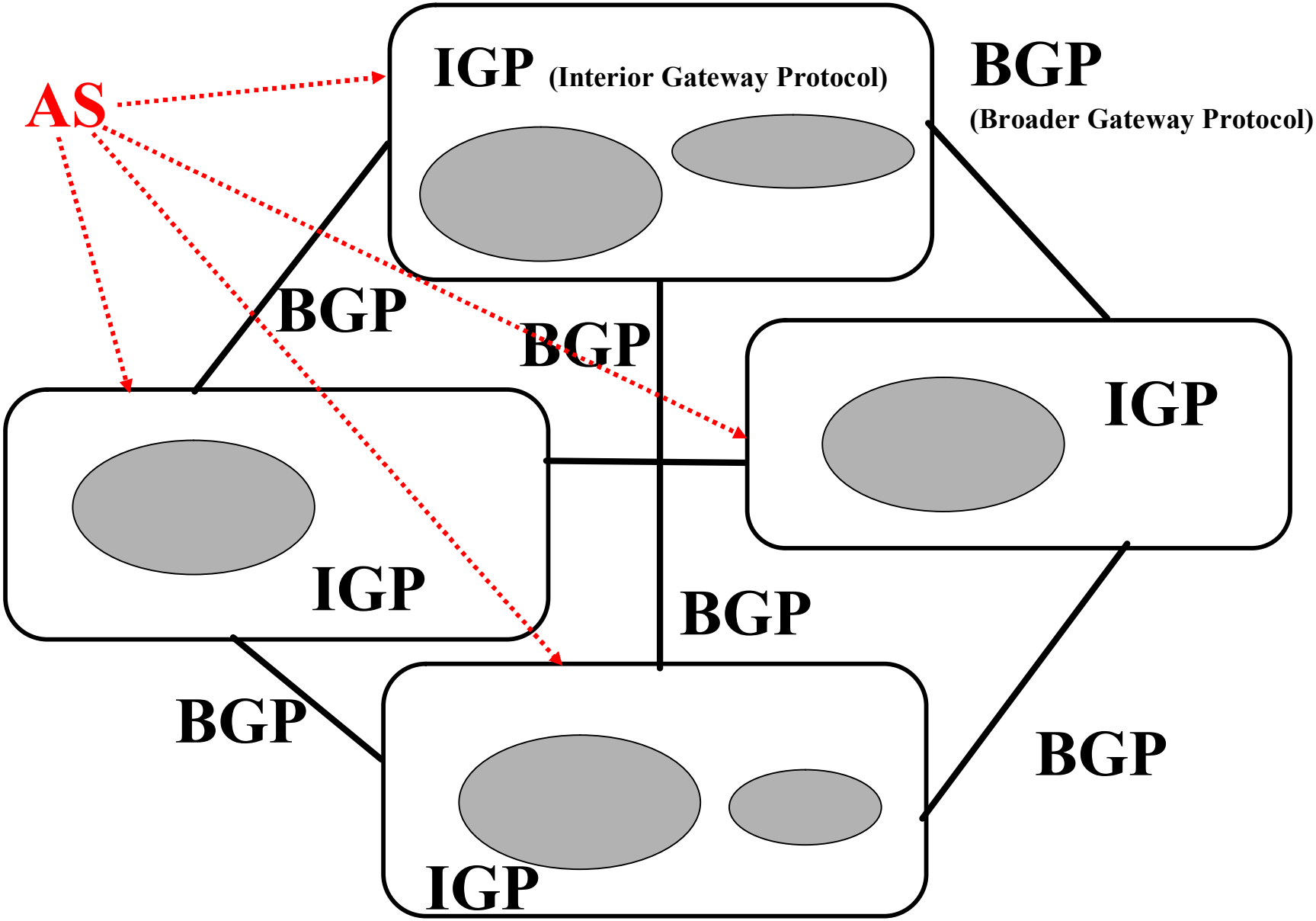
元来インターネットサービスプロバイダや複数のネットワーク接続されたに巨大な 組織など、1つのルーティングポリシーによって制御されているネットワークと定義。

RFC 1930で新しく定義されたのは、グローバルAS番号を持ったISPに接続される複数の組織においてプライベートAS番号を使用してBGPを走らせ、インターネット接続可能になった。

例えそのISPが複数のASを抱えていても、インターネットからはISPのルーティングポリシーが見えるだけ。ユニークなAS番号（AS number）はBGPのルーティングを行うのに必要なため、各ASごとに割り振られている。

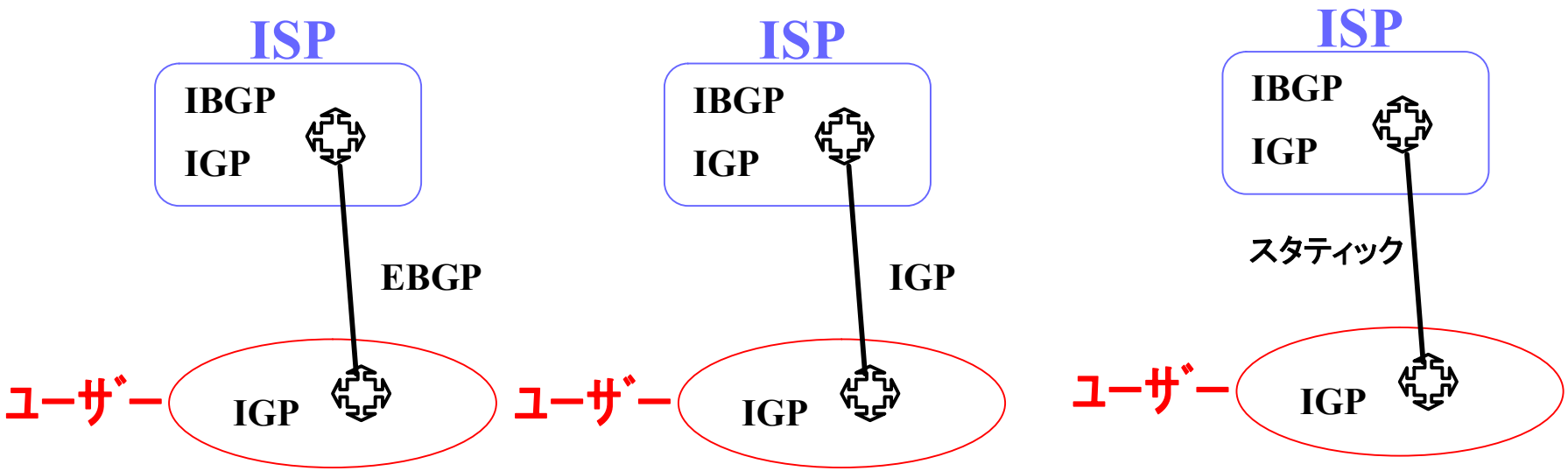
BGPにおいて、AS番号はそのユニークさをもってインターネット上の各々のネットワークを認識する。

AS，EGP，IGPの関係



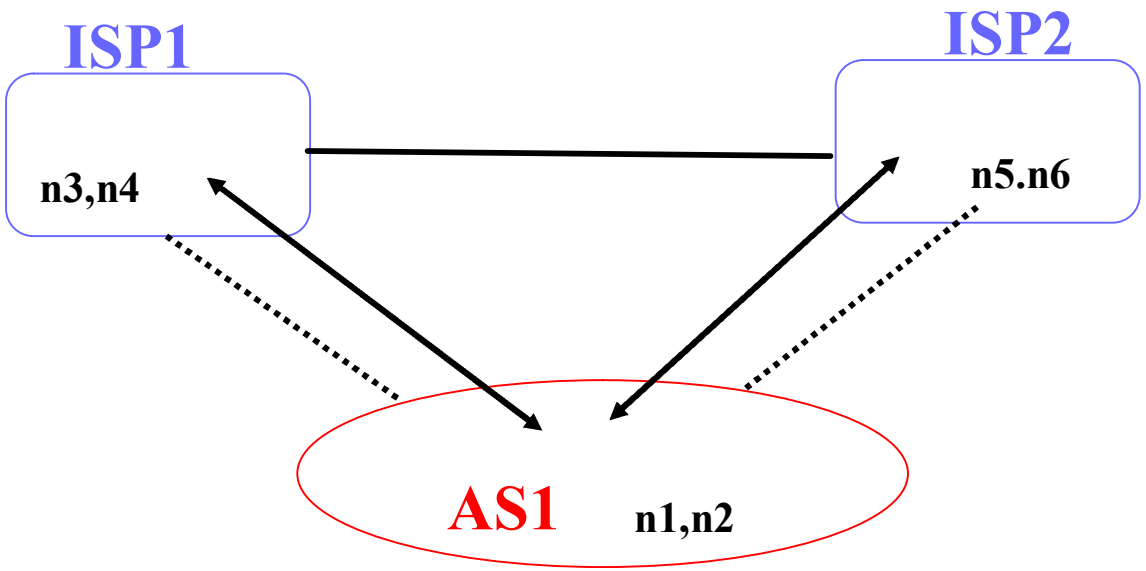
各種のASとトランジットの関係（その1）

- スタブAS
  - ・シングルホーム
  - ・唯一の出口を経由してドメイン外ネットワークに接続
  - ・デフォルト・ルーティングが可能
  - ・ISPはユーザー・ルートを他ネットワークへアドバタイズ可能
    - ⇒BGPでスタティックエントリーをアドバタイズ
    - ⇒IGPで自分のルートをアドバタイズ



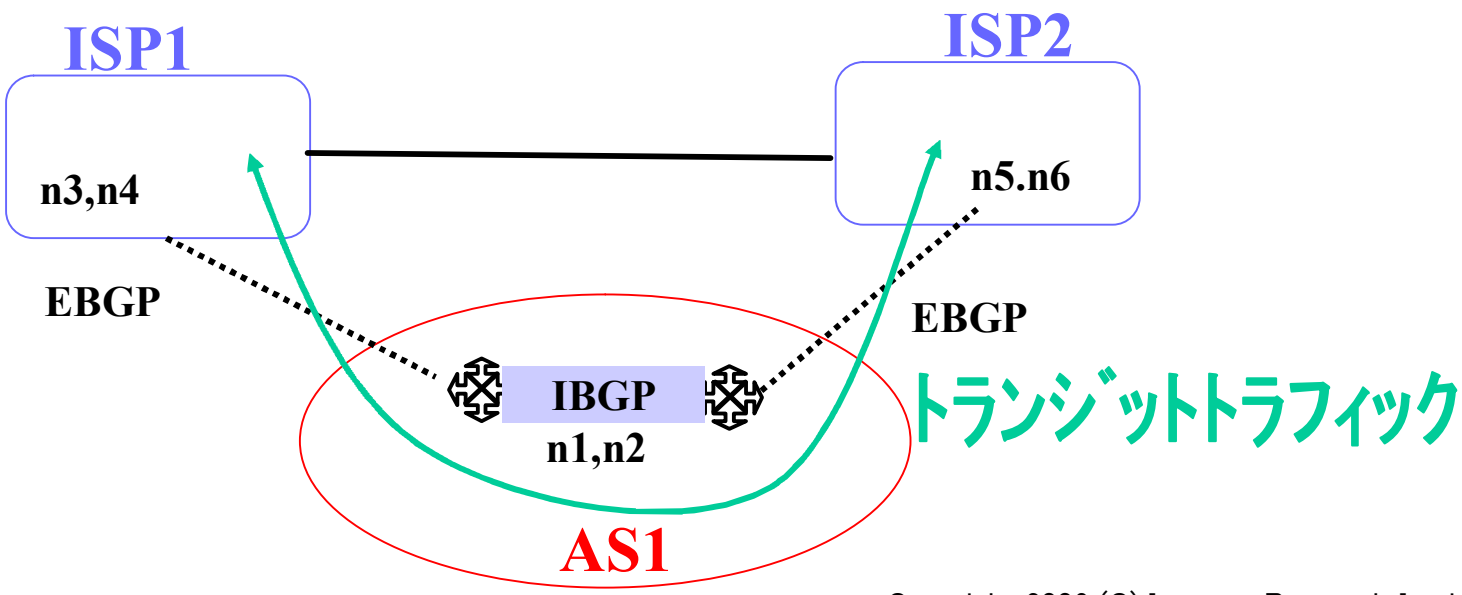
各種のASとトランジットの関係（その2）

- マルチホーム非トランジットAS（実際にはAS1とISP間にBGP-4は不要）
  - ・外部へ複数の出口がある＝マルチホーム
  - ・非トランジットAS＝トランジットトラフィックが当AS通過を否認
  - ・AS1はISP1を通じてn3とn4ルートを学習
  - ・AS1はISP2を通じてn5とn6ルートを学習
  - ・AS1はn1とn2ルートをISP1とISP2にアドバタイズする
  - ・AS1を経由してn5とn6に到達しようとするISP1の外部トラフィック、n3とn4に到達する外部トラフィックを防止可能



各種のASとトランジットの関係（その3）

- マルチホーム・トランジットAS
  - ・マルチホーム・トランジットAS＝外部に複数の通信路があり、他のASからのトランジットトラフィックに使用可能
  - ・トランジットトラフィック＝ローカルASに属さない起点/宛先を有するトラフィック
  - ・BGP-4は、エクステリアゲートウェイプロトコルだが、BGPの更新情報交換用パイプとしてAS内で利用可能
    ＝内部BGP（IBGP）
  - ・外部ADとのルータ間通信路＝外部BGP（EBGP）



ドメイン間ルーティングのまとめ

1. RIPを使用してISP接続する組織にBGPが必要になるのは、複数のISP接続する場合
2. 複数拠点でISP接続する場合は、IGPコネクションは通常１つなので、ISP次第で接続可能だがBGPを使用する方が効率的
3. ドメイン＝RIPドメイン、OSPFドメインのように同一ルーティングプロトコルで動作するルータの集合
4. AS（自律システム）＝統一した他ASとのルーティングポリシーをもつ集合体
5. BGPはAS間で有効であるだけでなく、ASがトランジットASの場合有効で、AS内でIBGPを使用するとトラフィック出口の選択が効率的
6. BGP-4以外のBGPには、EGP、BGP-1/2/3があるが古くて使われていない

3. ルーティング（経路制御）の上位プロトコル

OSIとTCP/IPの歴史

1970年代中頃、ネットワーク機器各社独自のネットワークアーキテクチャが次々に発表され始めた。機器を一つのメーカー製で揃えられるのであれば問題は無いが現実的には難しく、異なる機種同士を接続する為の標準化が急がれていた。

ISO(国際標準化機構)の情報処理システム技術委員会は1977年3月にSC16を設置、OSIの国際標準化を開始する。しかし、CCITT(国際電信電話諮問委員会)がOSI参照　モデル案を参考として独自の検討を開始。CCITTとSC16での意見のすり合わせを行い、基本的な意見を合意。1982年にトランスポート層の標準、1983年にセッション層の標準の草稿が完成。

1984年、情報処理システム技術委員会はSC16からSC21にOSIの標準化を引き継がせ、

1985年に応用層の新プロトコルを標準化項目に追加。その後現在まで、拡張や新たなプロトコルの制定が続けられている。

TCP/IPとOSI参照モデル

TCP/IPの基本仕様は1982年頃にはほぼ固まっており、OSI参照モデルは1984年に完成。当初の予定ではOSI参照モデルを基に、準拠した通信機器やソフトウェアが開発・製品化していくはずであったが、TCP/IPが1980年代後半から急速に普及した結果、OSI準拠製品は普及しなかった。

OSI参照モデルはネットワークの基本モデルとしてだけ残った。

OSI参照モデル

コンピュータの持つべき通信機能を階層構造に分割したモデル。OSI基本参照モデルとも呼ばれる。
1978年に、国際標準化機構(ISO)によって制定された、異機種間のデータ通信を実現するためのネットワーク構造の設計方針「OSI(Open Systems Interconnection)」に基づいて通信機能を以下の7階層に分割する。

第1層 - 物理層
　　電気信号の変換等。
第2層 - データリンク層
　　通信機器間の直接的な信号の受け渡し。
第3層 - ネットワーク層
　　ネットワークにおいて通信経路の選択。
第4層 - トランスポート層
　　ネットワークにおけるエンド・エンドの通信管理。
第5層 - セッション層
　　通信プログラム（プロセス）間の通信の開始から終了までの手順。
第6層 - プレゼンテーション層
　　データの表現方法。
第7層 - アプリケーション層
　　ユーザーが操作するインターフェース。

OSI参照モデル		
7	アプリケーション層	HTTP, SMTP, SNMP, FTP, Telnet, AppleTalk, X.500
6	プレゼンテーション層	SMTP, SNMP, FTP, Telnet
5	セッション層	NetBIOS, NWLink, PAP, 名前付きパイプ
4	トランスポート層	*TCP*, *UDP*, SPX, NetBEUI
3	ネットワーク層	*IP*, ARP, RARP, ICMP, DHCP, IPX, NetBEUI
2	データリンク層	イーサネット, トークンリング, アークネット, PPP, フレームリレー
1	物理層	RS-232, 電話線・UTP, ハブ, リピータ, 無線, 光ケーブル

OSIモデルは仕様ではなく指針であるため、全てのプロトコルやネットワークがOSIモデルに沿って実装されているとは限らない。従って、一部のプロトコルやサービスに関しては、OSIモデルのどの層に属するかについて、幾つかの異なる見解が存在する。複数層に跨っている物もある。図示の例はあくまでも例に過ぎない。

TCP(Transmission Control Protocol)

伝送制御プロトコルといわれ、TCP/IPの通信処理で使われるプロトコル。
OSI参照モデルのトランスポート層に相当。ネットワーク層のプロトコルであるIP上位プロトコルとして使用。
TCPは、セッションという形で1対1の通信を実現し、パケットシーケンスチェックによる欠損パケット再送などの伝送誤り制御機能を持ち、データ転送などの信頼性の必要な場面でよく使用される。
他のトランスポート層プロトコルに比べ、プロトコル上のオーバヘッドが大きいため、比較的低速となる、リアルタイム性の要求されるオーディオビジュアル情報の伝送には、速度が重要で信頼性をプロトコルに求めない場合のUDPがよく使用される。

IETFにより、RFC793による技術仕様が規定されている。
STD番号:7

上位プロトコルとして、HTTP、FTP、Telnet、SSHなどがある。

仕様概要
プロトコル番号:6
コネクション型通信であり、3ウェイハンドシェイク方式で接続を確立する。

TCPヘッダ

※ヘッダ長とフラグ

送信元ポート		送信先ポート	
シーケンス番号			
確認応答番号			
※		ウインドウサイズ	
チェックサム		緊急ポインタ	
(オプション)			
データ			

ビット	内容
15	ヘッダ長
14	
13	
12	
11	予約
10	
9	
8	
7	
6	
5	URG (緊急転送データ)
4	ACK (受信確認)
3	PSH (プッシュ)
2	RST (接続のリセット)
1	SYN (同期)
0	FIN (送信終了)

User Datagram Protocol(UDP)

主にインターネットで使用されるプロトコルの一つで、定義はRFC 768による。主にIP上に実装されておりOSI参照モデルのトランスポート層にあたる。送達確認などを行わない無手順方式でのデータ転送に用いる。通信中のパケット紛失や、データ誤り等の検出やその為の対応手段はアプリケーションで行う必要がある。しかし、その分TCPと比べデータ比率は高まるため、途中でデータが抜け落ちても問題が少ない音声や画像のストリーム形式での配信（VoIP、Realストリーミング、QuickTimeストリーミング）に用いられている。その他SNMPやTFTP、DNSやDHCPなどの各種上位プロトコルがある。

STD番号:6

仕様概要

プロトコル番号:17

TCP同様、ひとつのIPアドレスで16bit (65535個)の論理ポートを持つことができる。物理的・IPアドレス的に1つであっても、論理的に多重化された65535個までの通信を行うことができる。

UDPヘッダ

送信元ポート	送信先ポート
データ長*	チェックサム
データ	

File Transfer Protocol (ファイル トランスファー プロトコル、FTP)

●インターネットでファイルの転送を行うためのプロトコル。
　インターネット初期の頃から存在するプロトコルで、今でもインターネットでよく使用されるプロトコルの1つ。プロトコル上は任意のホスト間のファイル転送を行うことが可能であるが、通常は接続したクライアントとサーバ間の転送に利用される。
●用途
　Webページ用各種データファイル（HTML、画像など）のクライアント→ウェブサーバへのアップロード
ソフトやデータなどのFTPサーバ→クライアントへのダウンロード。
　ダウンロードについては、ブラウザソフトでも可能であるが、アップロードについてはFTPクライアントソフトやCUIコマンドが必要となる。
●任意のホスト間の転送を指示できる名残として、サーバへの接続時のコマンド用とは別にデータ転送用のコネクションを確立するが、この確立方法にアクティブモード、パッシブモードという2種類の方式がある。
●アクティブモード（ポートモード）では、クライアントがサーバへ待ち受けIPアドレスとポート番号を通知し、サーバがクライアントから通知されたIPアドレスのポート番号へコネクションを確立する。このとき利用するポート番号が毎回異なるので、ファイアーウォール、NAT（IPマスカレード）などを使った環境では場合によってはうまく接続できないこともある。この場合はパッシブモードを使用。
●パッシブモードではサーバがクライアントへ待ち受けポート番号を通知し、待ち受けポート番号の通知を受けたクライアントがサーバへコネクションを確立する。
●いずれのモードでもコマンド用とデータ用で別々のコネクションを張ることには変わりはない。
●サーバ側にファイヤーウォールがある場合、データコネクションのためにどのポート番号を使うかを設定してファイヤーウォールとの整合を確認する必要あり。
●パッシブモードを使っている限り、クライアント側のファイヤーウォールは気にする必要がない。
●通常、サーバに接続する際には、認証を必要とするが、専らファイル（主に無償のフリーソフトなど）を配布する目的で、匿名でアクセスできる Anonymous（匿名） FTP サーバを用いる場合もある。
●匿名アクセスでも認証は必要であり、この場合、ユーザとして"anonymous"または"ftp"、パスワードとして利用するユーザの電子メールアドレスを指定する。

Telnet（テルネット）

●汎用的な双方向8ビット通信を提供する端末間およびプロセス間の通信プロトコルである。RFC 854で規定。
●具体的には、IPネットワークにおいて、遠隔地（リモート）にあるサーバを端末から操作できるようにする仮想端末ソフトウェア（プログラム）、またはそれを可能にするプロトコルのことを指す。
●複数が同時に使用することを前提に開発されたUNIXでは、シリアル回線に複数の端末をつないで作業を行うことができた。この端末とホストの通信を、IPのネットワーク上で担うのがTelnetクライアントプログラムと、その通信手順を規定したTelnetプロトコルである。
●Telnetクライアントは、Telnetサーバとの間でソケットを開き、非常に単純なテキストベースの通信を行う。Telnet自身のコマンドを利用する際にはエスケープコードを利用する。リモートのシェルを利用するTelnetサービスは、基本的にポート番号23番を使用するが、ほとんどのクライアントはポート番号を指定でき、それ以外のテキストベースのソケット通信のクライアントとして利用することも可能である。
●現在、認証も含めすべての通信を暗号化せずに平文のまま送信するというTelnetプロトコルの仕様はセキュリティ上問題とされ、Telnetによるリモートログインを受け付けているサーバは少なく、リモート通信方法としての利用は奨励されない。
●リモートログインの代替プロトコルとしては、情報を暗号化して送信するSSHが知られている。

SSH

●Secure Shell（セキュアシェル）は、暗号や認証の技術を利用して、安全にリモートコンピュータと通信するためのプロトコル。パスワードなどの認証部分を含むすべてのネットワーク上の通信が暗号化される。スペルアウトするよりも、頭字語のSSHと呼称する。
●Telnetやrshやrloginなどといった、リモートホストのシェルを利用するための既存のプロトコルを代用する手段として考えられていた。
●TelnetやFTPは、ネットワーク上に平文でパスワードを送信してしまうため、パスワードをネットワーク経路上で盗聴されてしまう危険性が高く、商業的なインターネット空間では問題があった。Telnet同様に、リモートホスト間でのファイルコピー用のコマンドrcpを代用するSCPや、FTPを代用するためのSFTPも用意されている。
●SSHの暗号通信は、公開鍵暗号（RSA又はDSA）を用いて共通鍵暗号（トリプルDES、IDEAなど）の共通鍵を暗号化して鍵交換を行い、通信自体は高速な共通鍵暗号を用いる、いわゆるハイブリッド暗号である。
●なりすまし防止用の認証の仕組みも充実している。パスワード認証、公開鍵認証、ワンタイムパスワードなどが提供。
●バージョン1とバージョン2の2種類のプロトコルが共存しているが、バージョン1には脆弱性が発見されているため推奨されない。
●商用アプリケーションや　フリーソフトウェアなど幾つかの実装があり、一般に普及しているのは、オープンソースで開発されているOpenSSHで、Linuxなどでも標準的に利用されているため、現在では単純にSSHと言った場合、OpenSSHの実装を指すことが多い。

4. TCP/IPの次なる次世代ネットワークとは？

NGN登場の背景

【1】 IPの登場による固定電話/専用線事業の衰退

【2】 携帯電話事業の成長減速と数年後の衰退懸念

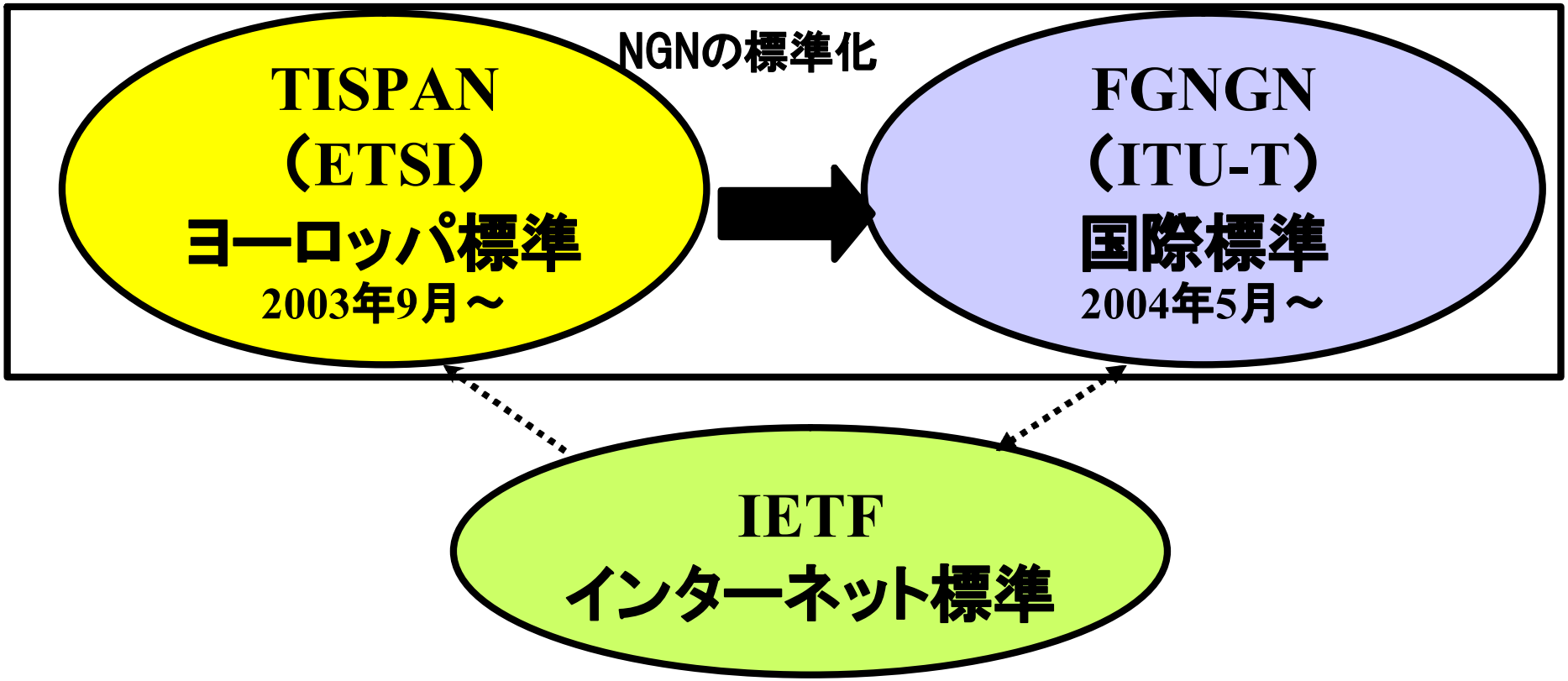
【3】 Skype型電話の爆発的普及

【4】 動画サービスの爆発的普及

【5】「技術革新」・「業界政治」・「国際政治」の複合的背景

⇒重要なのは「技術革新」への対応！

NGNの標準化団体の相関関係



ETSI（European Telecommunications Standards Institute

TISPAN（Telecommunications and Internet converged Services and Protocols For Advanced Networking）

FGNGN（Focus Group Next Generation Network）

ITU-T（International Telecommunication Union-Telecommunication Standardization Sector

IETF（Internet Engineering Task Force ）

NGNの概要と狙い

IRI
Ubilabs Innovations

1. NGNの概要(インターネットとは異なるIPネットワーク)

①SIP(session initiation protocol)を基本にIPネットワーク上での音声データ、映像マルチメディア・サービスを実現

②固定通信網と移動通信網を統合したシームレス・サービスとして FMC(fixed moile convergence)を実現

③基本ネットワーク・アーキテクチャとしてIMS(IP Multimedia Subsystem)を採用

【3G携帯電話標準化団体3GPP(3rd Generation Partnership Project)規定による】

④ネットワーク品質、端末の能力に応じたエンド・ツー・エンドQoS制御を実現

2. NGNの狙い

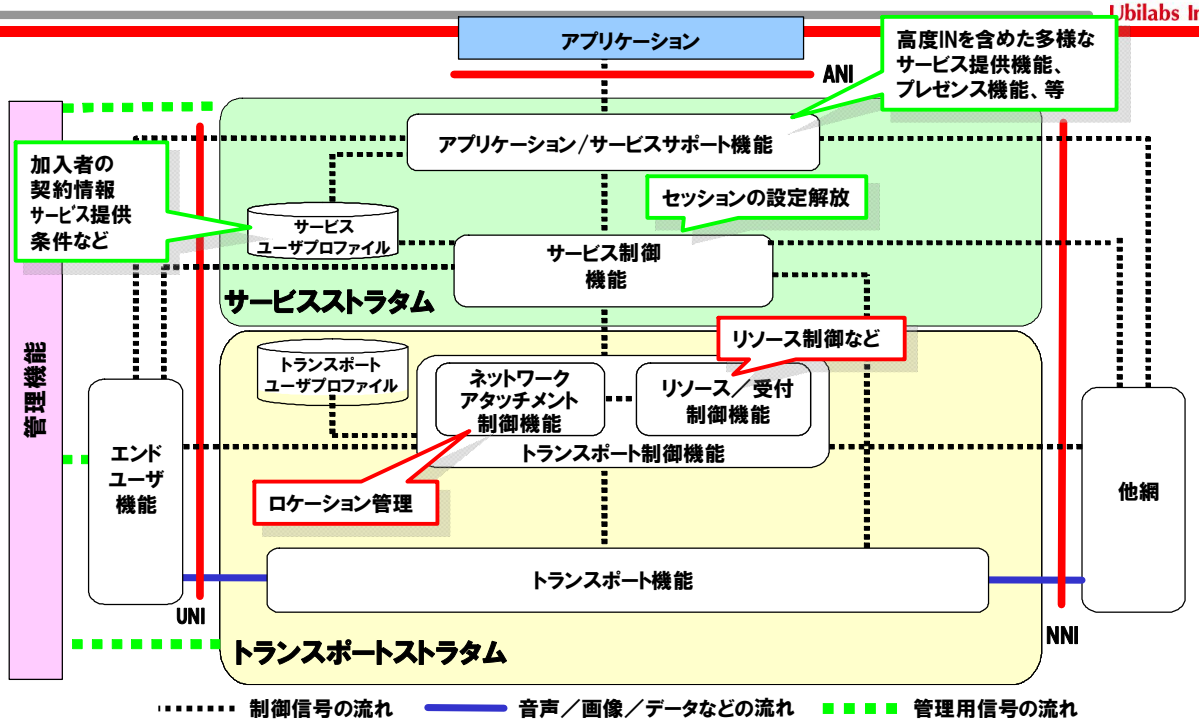
①電話中心のヨーロッパのキャリア、通信機ベンダーが、IPの出現によって電話主体の通信ビジネスに起こった構造変化を後追いではなく主導するための標準化

②ヨーロッパ標準に留まることなくITU-T＋IETFを巻き込んだ国際標準の確立

③IP出現以降の米国主導の通信ビジネスの構造変化に対する、ヨーロッパを主体するキャリア、通信機ベンダーによる巻き返し

通信キャリアによる次世代ネットワーク構築の取り組み（標準化（ITU-T）の動向）

NGNのアーキテクチャ



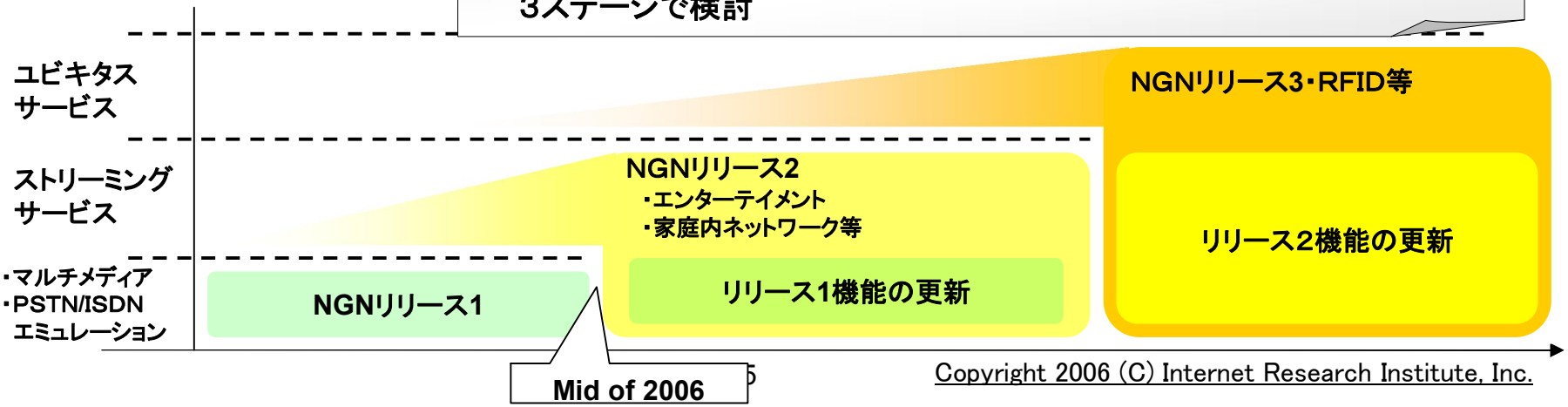
（注）

トランスポート層のトランスポート機能には、アクセス、コア、エッジ機能及びメディアハンドリング機能等が含まれている。

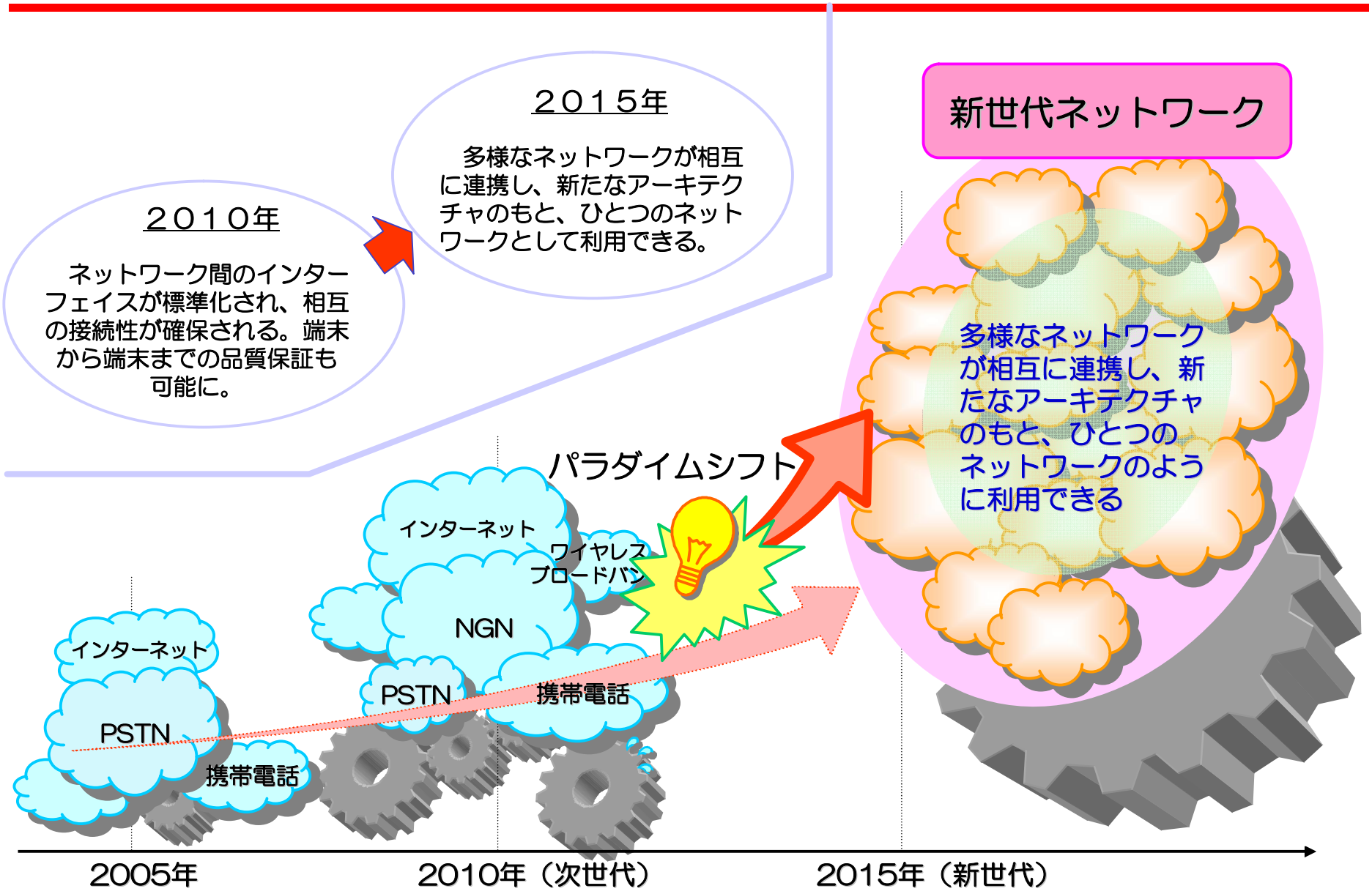
UNI、NNI及びANIはNGN特有の多様なインターフェースを許容する観点からノートが付されている。

NGN標準化のステップ

○ NGNでは特定のサービスと能力を段階的に実現
○ サービスの記述、アーキテクチャとプロトコル要求条件、プロトコルの3ステージで検討

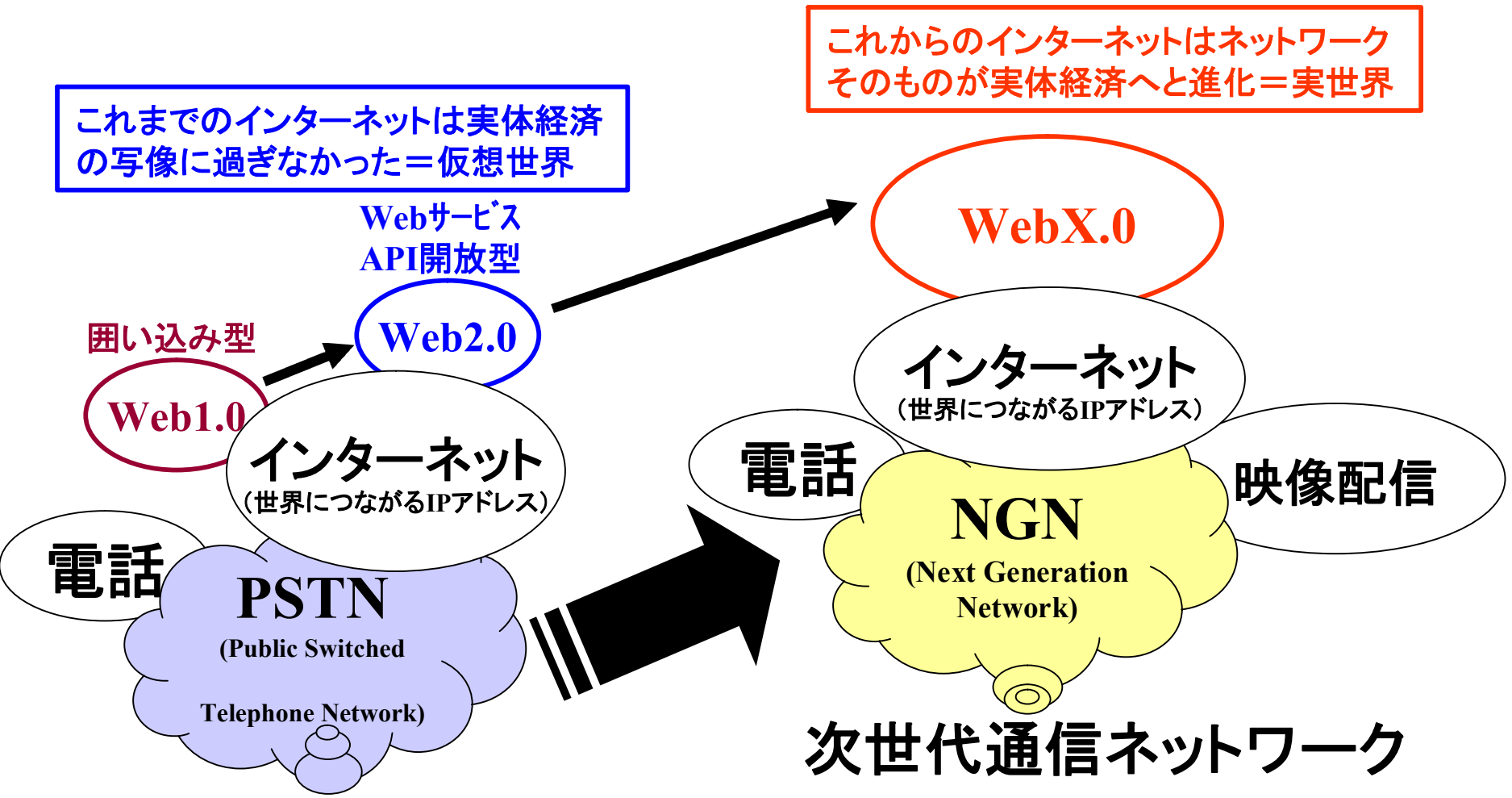


総務省研究会での議論（将来的なネットワークアーキテクチャの進展イメージ）



（出所：次世代ネットワークアークテクチャ検討会　資料）

次世代ネットワークとWebサービスの進化が同期



ご清聴ありがとうございました