

総合講座

インターネットと人々の生活

H18年12月9日

名城大学理工学部 渡邊 晃

内容:

- ・ IT革命とユビキタス社会
- ・ 電話とインターネットの違い
- ・ インターネットのしくみ

・農業革命 - > 定住

・産業革命 - > 生産性の向上

(機械の発明、交通・運輸機関の発達)

・IT(情報技術)革命 - > ?

インターネットにより、全ての人、物がインターネットに接続され、情報交換が可能になる。

- > 国境がなくなる

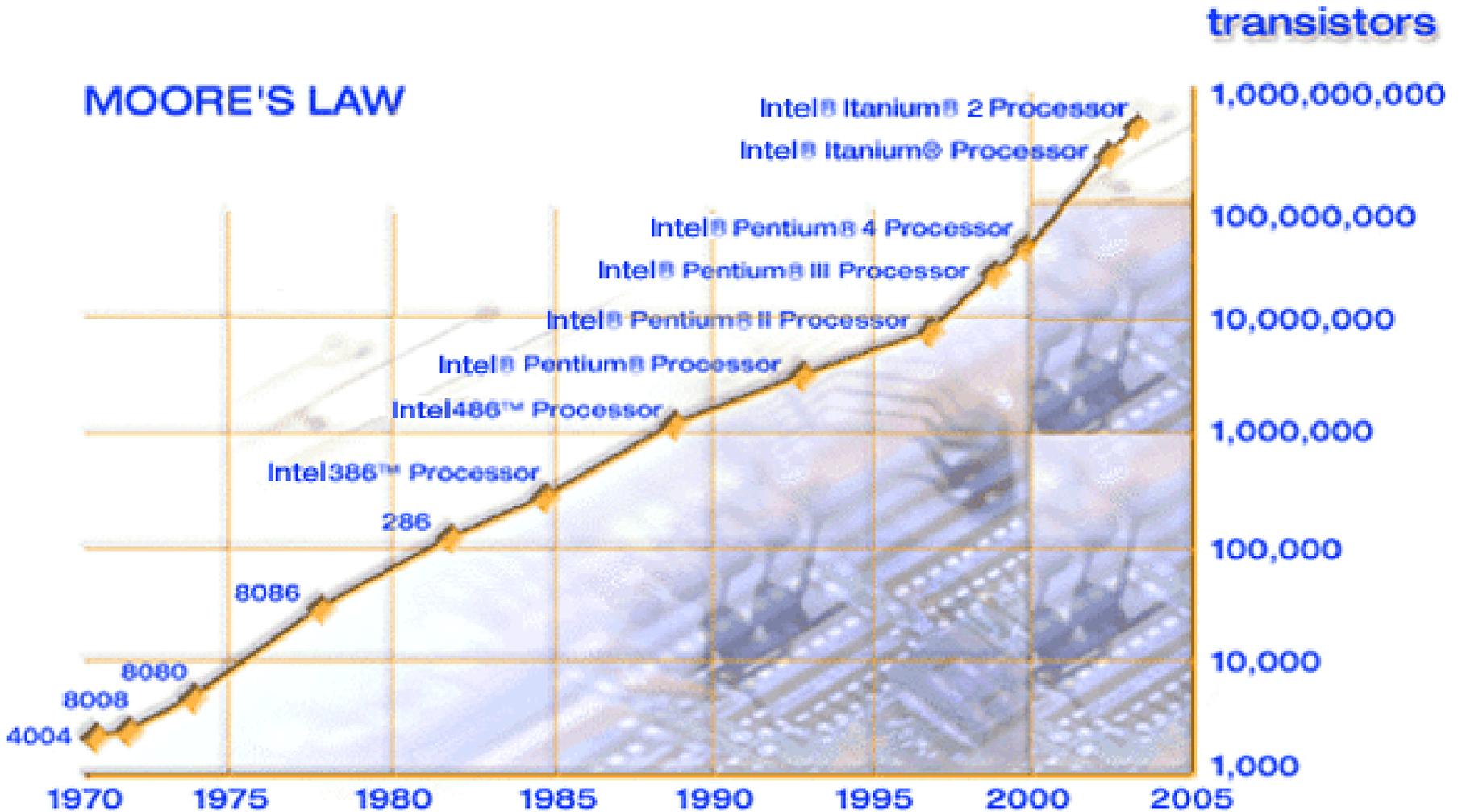
アイデアの時代

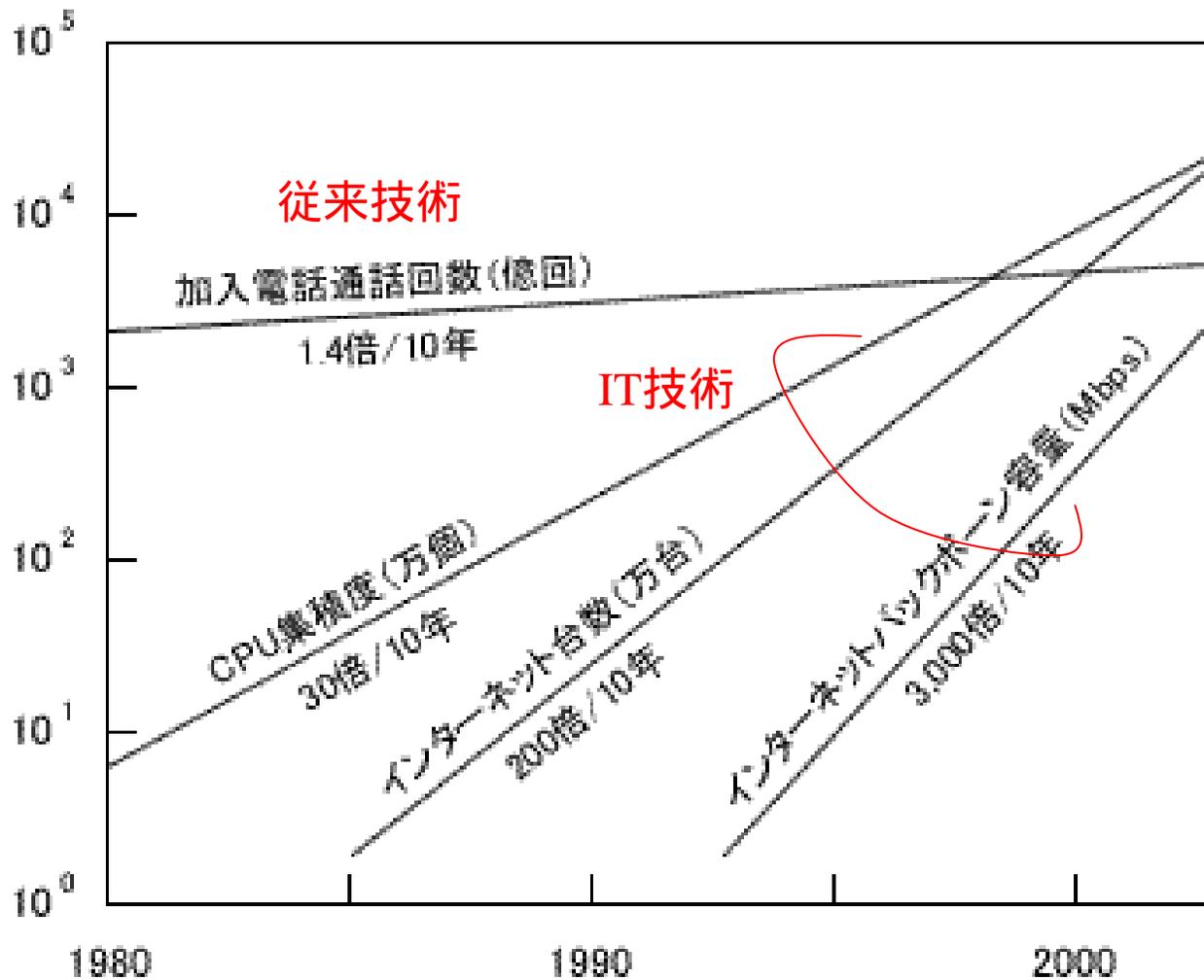
英語が公用語

ムーアの法則;IC の集積度は18ヶ月で2倍になる(1965年)

ゴードン・ムーア;インテルの創始者

出典;インテルHP





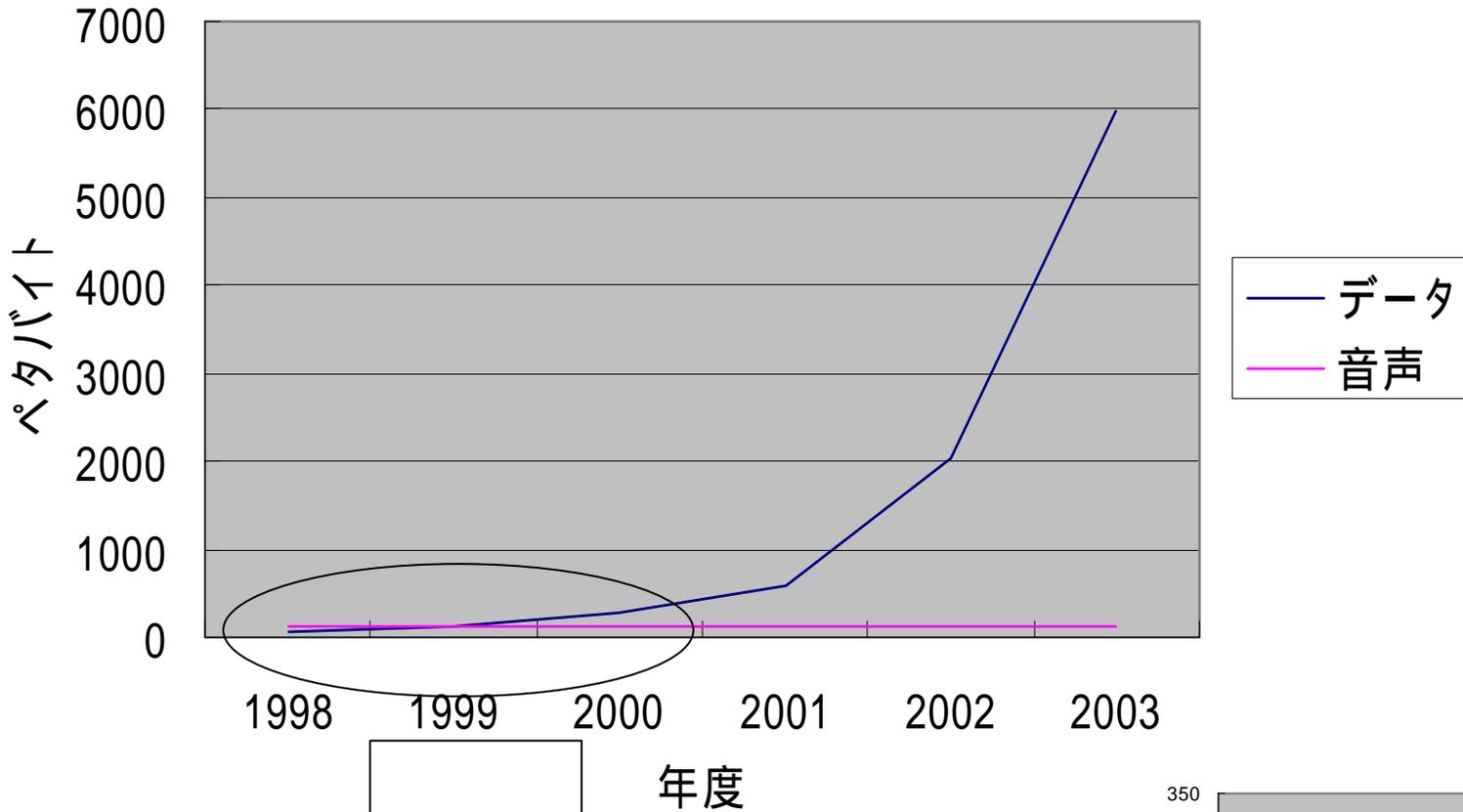
データソース:

<http://www.cs.columbia.edu/~hgs/internet/traffic.html>

<http://www.intel.com/research/silicon/mooreslaw.htm>

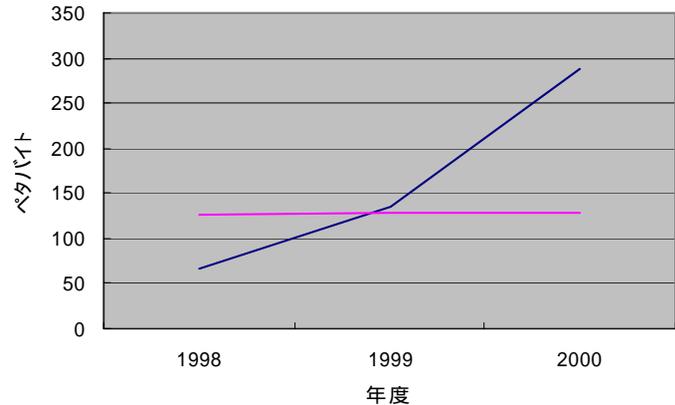
<http://www.isc.org/index.pl?/ops/ds/>

日本における情報流通量の変化(1998～2003)



電話網は消える

携帯電話網はしばらく残る(移動通信可能)



ユビキタス社会のイメージ



いつでも、誰でも、どこからでも、
ネットワークを利用して、情報入手、発信できる

ユビキタス社会では

- すべての人・物がネットワークに繋がる
- ネットワークは空気のような存在になる
- 情報の世界には国境がなくなる
- 物との対話ができる
 - 冷蔵庫, テレビ, ロボット
- 発信源の位置情報がわかる
 - 子供, ペット, 財布

技術的背景

- ネットワークへの接続機能が小型化され、どのようなものにも取り付けられる。
- 宇宙に浮かぶ太陽電池からマイクロ波で電源が供給される。
- ネットワークは、ブロードバンドでかつ常時接続であり使い放題。
- 無線技術によりネットワーク接続機器は自由に場所を移動できる。
- 情報発信源のある場所は、GPS (Global Positioning System)との連携により常に把握できる。

社会生活で何が変わるのか

圧倒的に多くの選択肢と大きな自由

リアルタイム/低コストで全世界へ知の配布

- ・資源を無駄にしない循環型社会(記憶媒体不要)
- ・販売手法/価格設定の方法(ネット直販)
- ・ビジネス手法(電子商取引, ネット銀行, ベンチャー)
- ・文明(印刷 ネットワーク)

インターネット

- 世界中に広がる通信基盤
- 格段に安い通信価格
- 核戦争に耐えられる耐障害性
- 共通の通信プロトコルTCP/IP
- セキュリティの確保が重要な課題

電話網とデータ通信網の目的の違い

電話網：

人間どうしの音声をやりとりする。

リアルタイム性が必要。

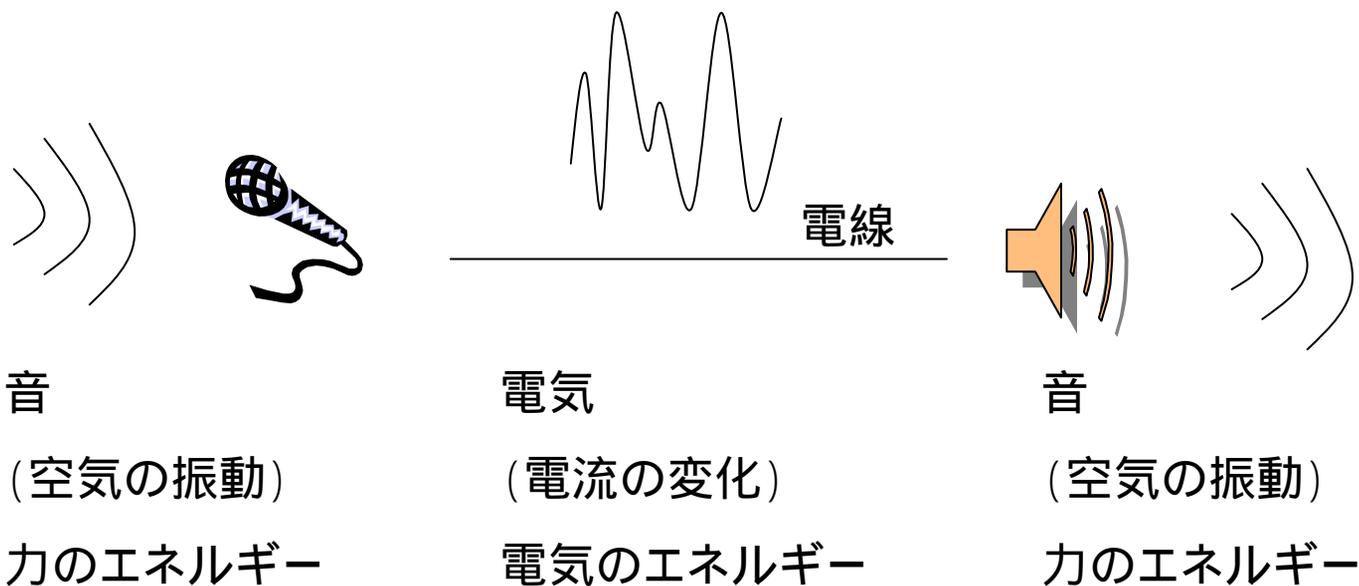
データ通信網(インターネット)：

コンピュータどうしの通信を行うのが目的。

確実な通信が必要。

電話

1876年 アメリカ ベル



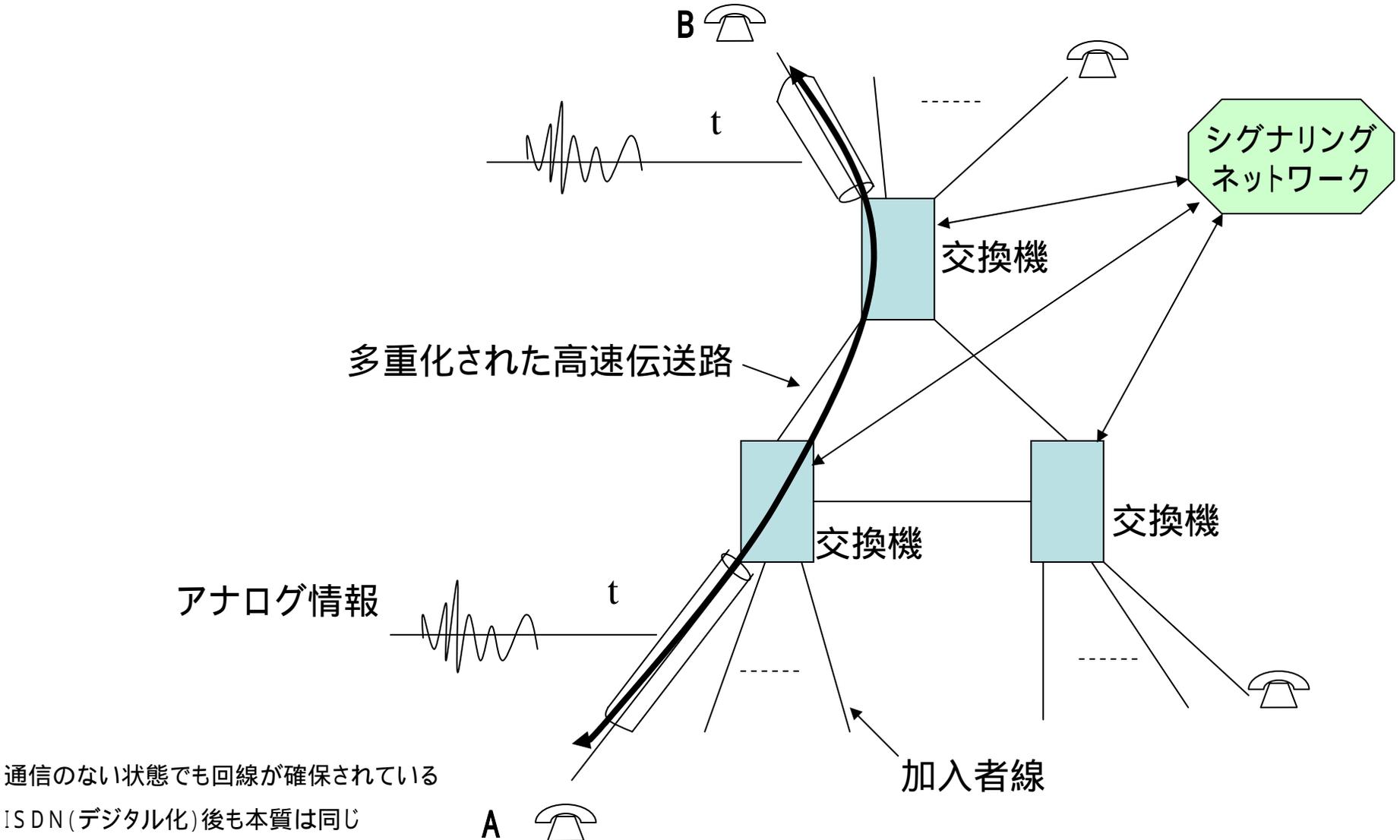
空気の振動

電流の変化

電話網の構成 --- 回線交換方式

ダイヤルにより相手を選択、選択後は接続固定

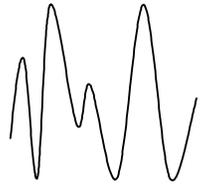
アナログ情報をそのまま伝達する



アナログからデジタルへ(但し基本的構造は同じ)

アナログ伝送

電流の変化



減衰と変形



増幅器

伝送路

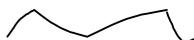
情報の劣化は原理的に抑えられない

デジタル伝送

100110



減衰と変形



100110



波形整形

伝送路

ノイズがなければ完全に復元される

コンピュータは

- ・「0」と「1」しか理解できない。
- ・全ての情報は「0」と「1」に変換される。
- ・全ての処理は「0」と「1」だけで実行される。

数字：2進数で表現

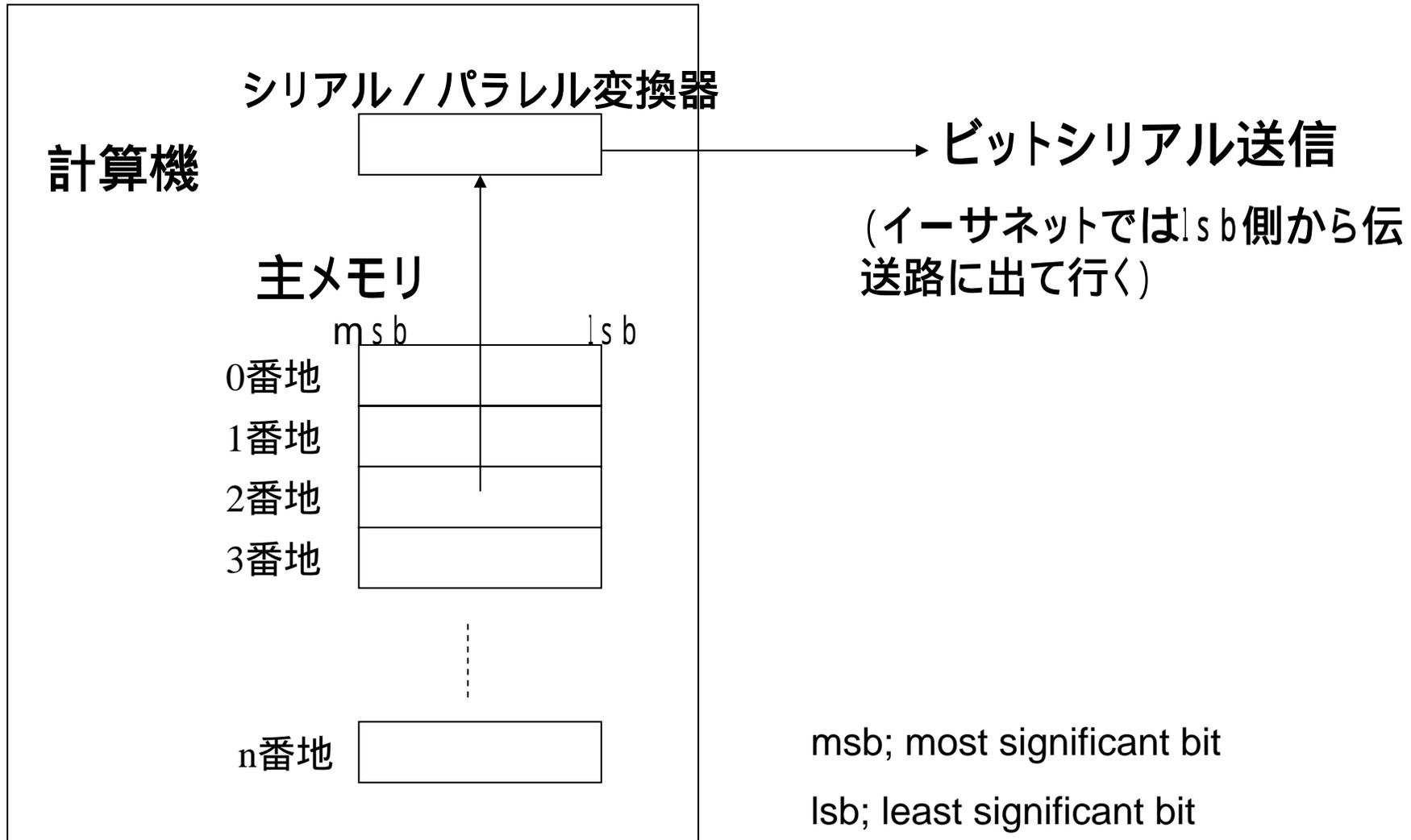
文字：1バイトまたは2バイトのコードで表現

画像：画素に分割、濃度を2進数で表現、カラーは3原色を用いる

アナログ情報：一定のサンプル間隔で、アナログ情報の値を読み取る

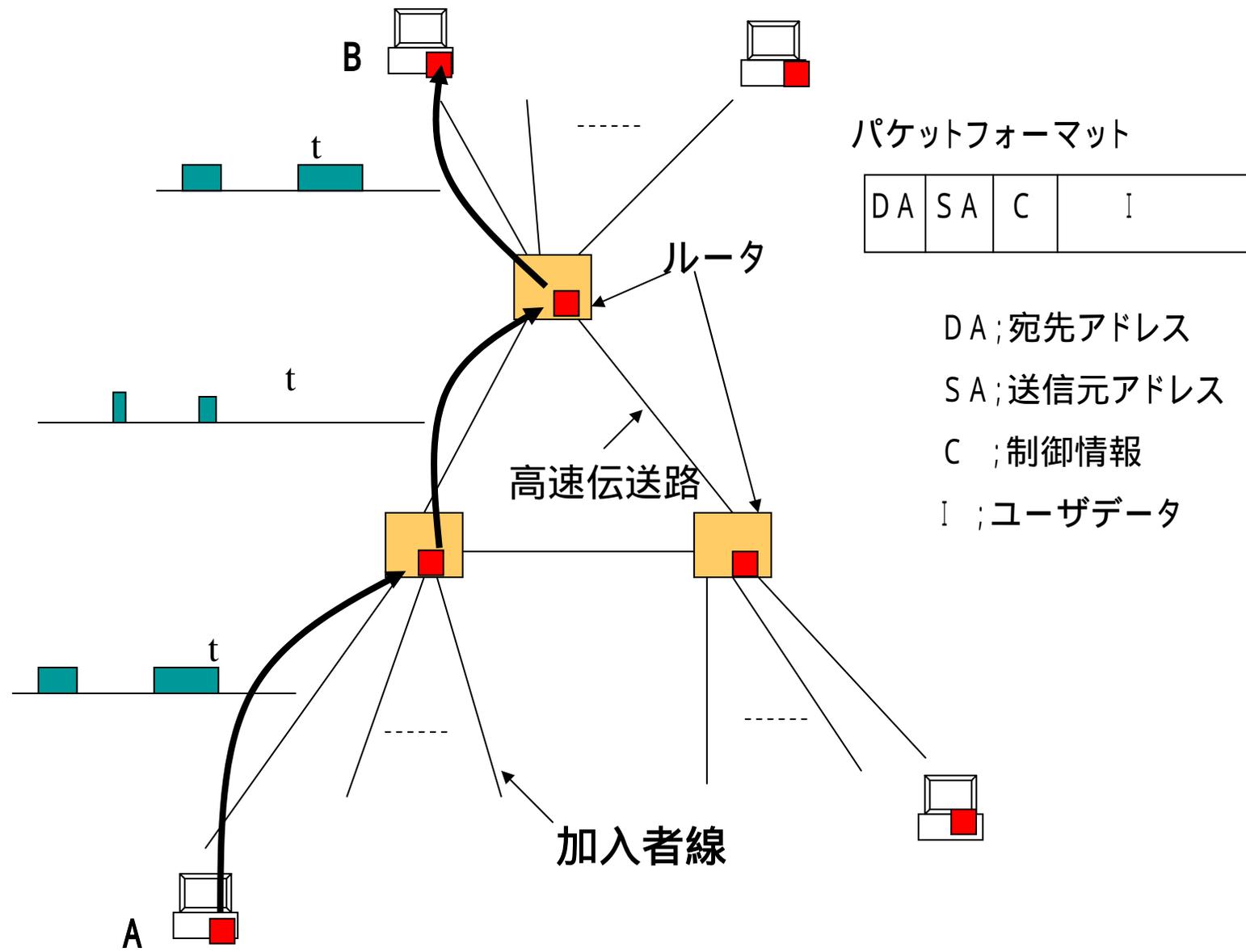
伝送路は1本 通信は必ずビットシリアル

コンピュータはパラレル処理



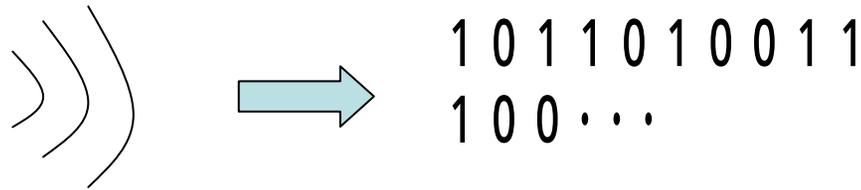
データ通信網の構成 --- パケット交換方式(蓄積交換方式)

情報をパケットの形にして中継装置をバケツリレーして行く



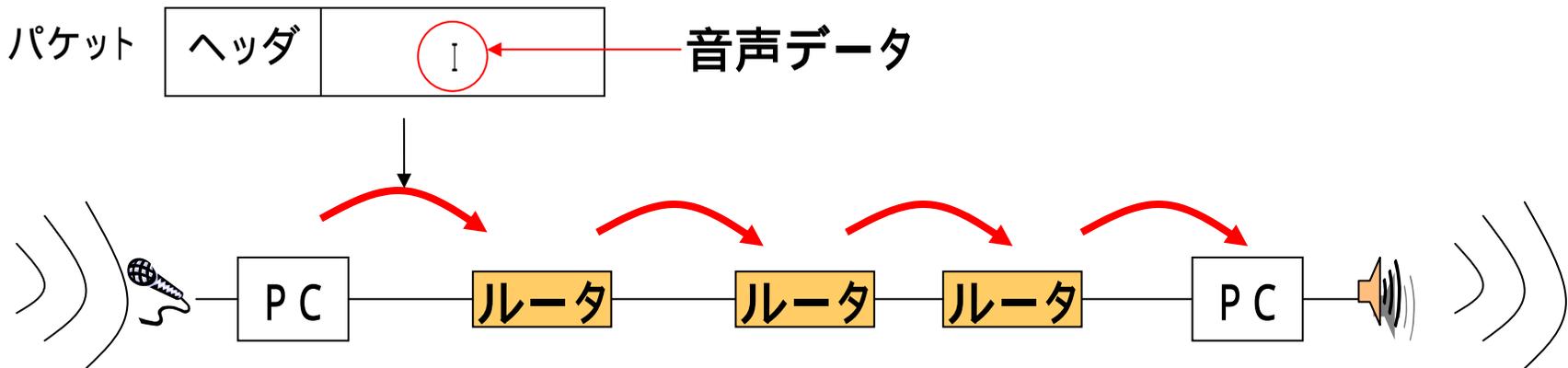
IP電話のしくみ

音声をデジタル情報に変換して、



パケット形式に組み立てなおし、パケットリレーで相手に伝える(50mSに1回、500バイト長)

(*)1バイト = 8ビット



200mS以内の遅延であれば会話可能。ネットワークの性能向上により実現性が高くなっている

電話網とデータ通信網の違い(まとめ)

電話網:

人間どうしの音声をやりとりする。

リアルタイム性が高い

- × 音声帯域以上の情報を通せない
- × 通話中は伝送路を占有する

データ通信網(インターネット):

コンピュータどうしの通信を行うのが目的。

確実な通信が可能

技術の進歩に合わせて高速化が可能

通信効率が高い(伝送路を占有しない)

- × リアルタイム性が低い 技術の進歩により改善

インターネットはなぜ安い？

パケット通信

伝送路を有効に使用できる。

ベストエフォート型

故障に対してできるだけのことをするが完全な保証はしないという考え(電話網はギャランティ型)。

オープン志向

技術を全てオープンにする。共通のインフラを皆で使用する。

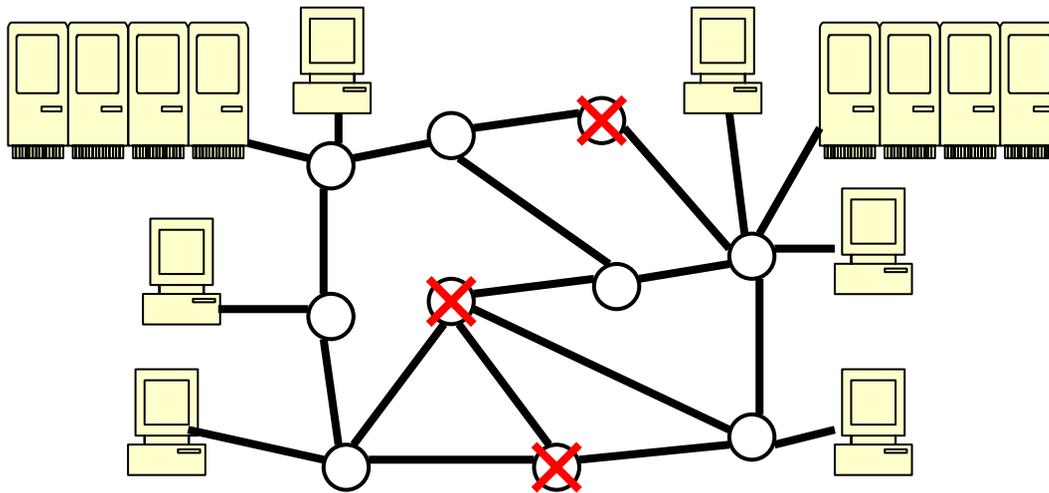
エンドエンドの原理

複雑な処理はすべて端末で行う。ネットワークは何もしない。

インターネットは信頼性が低いのか？

インターネットの起源は米国防総省のARPANET。

敵の攻撃にあってもシステム全体がダウンしないネットワークとして考案された。



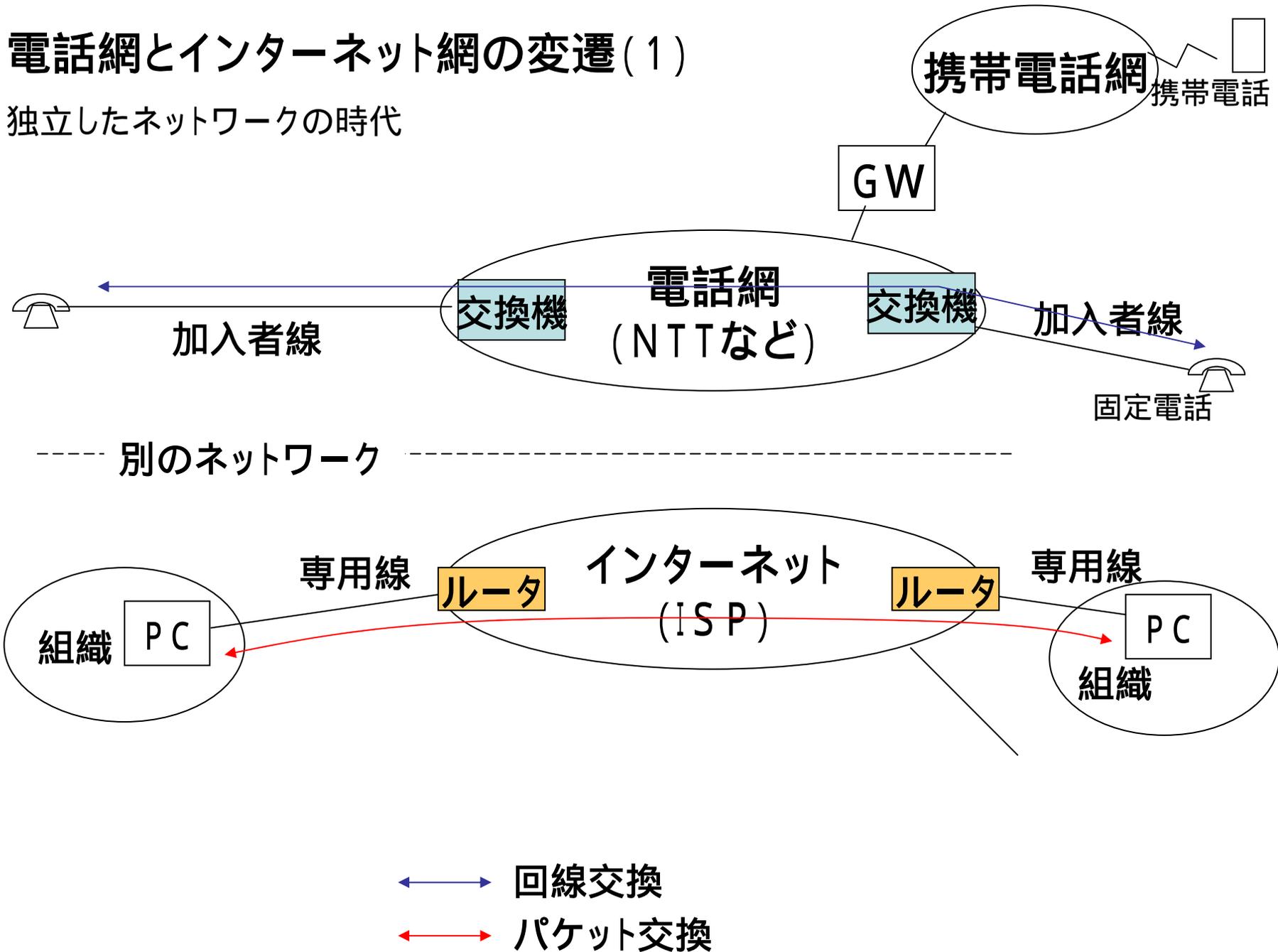
いくつかのサイトに障害が発生しても、迂回路を通してパケットを配送できる。

一部の障害が発生しても迂回路がある限り通信が可能

システム全体で見るとインターネットの信頼性は極めて高い

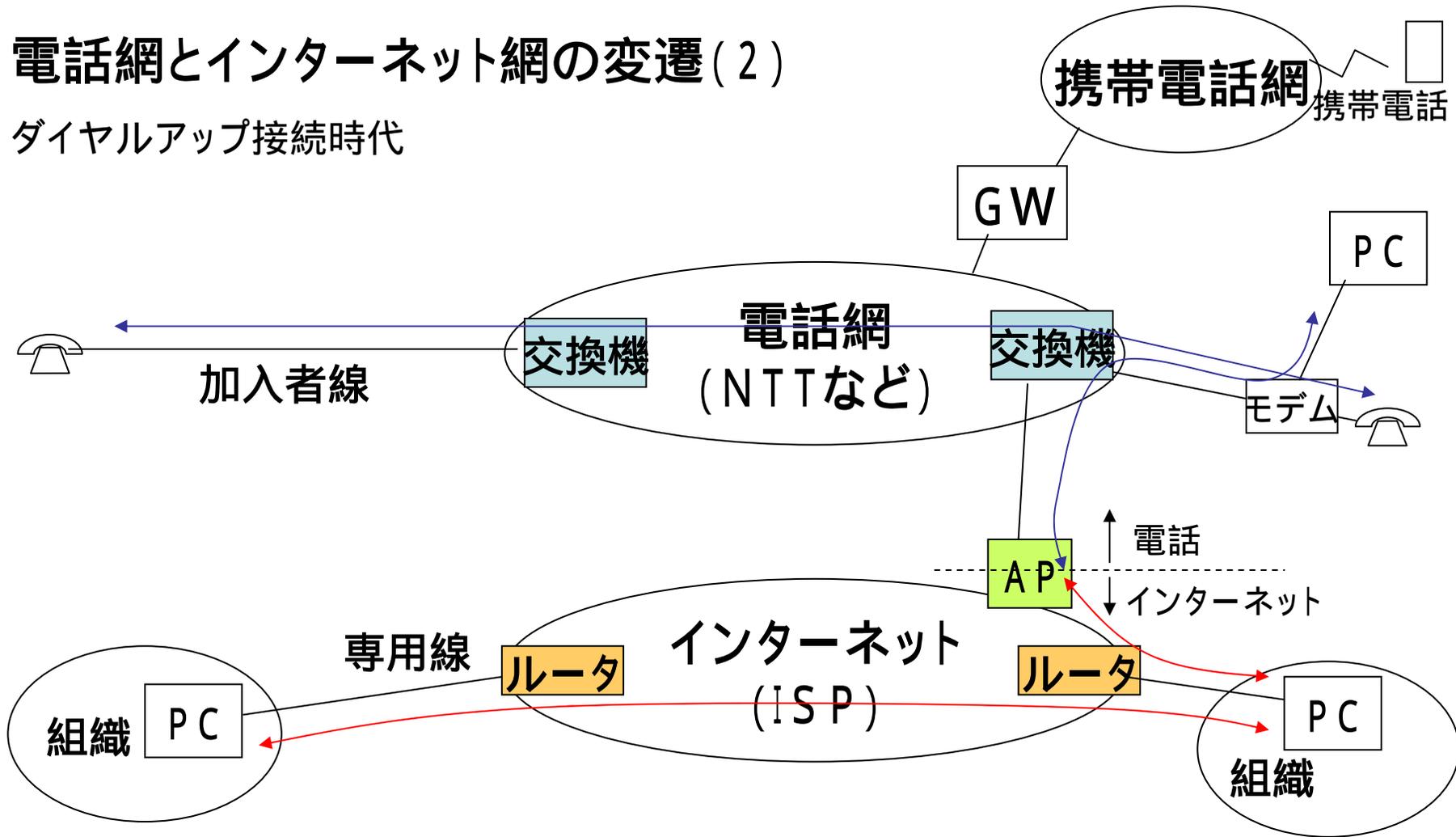
電話網とインターネット網の変遷(1)

独立したネットワークの時代



電話網とインターネット網の変遷(2)

ダイヤルアップ接続時代

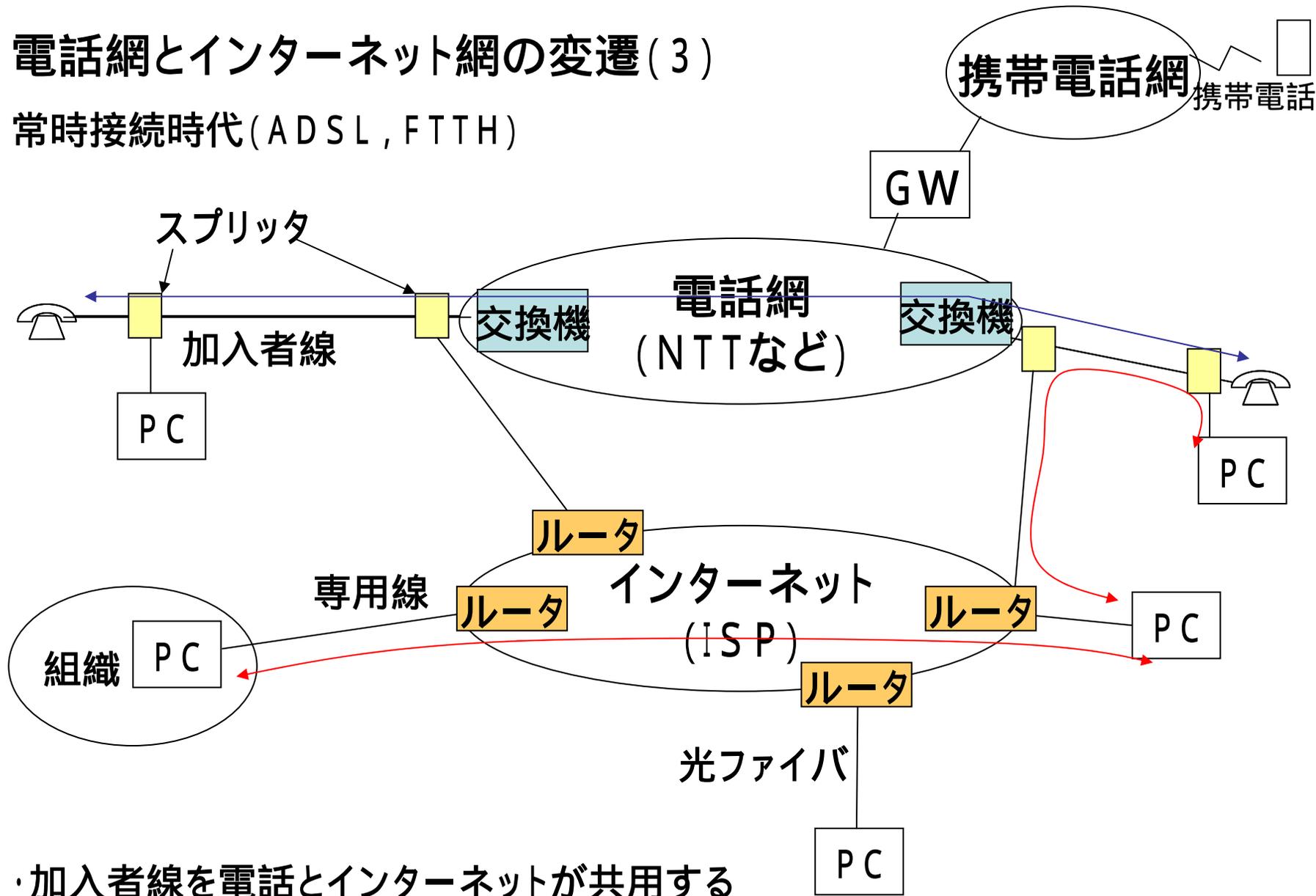


・PCからAPに電話をかける

AP (Access Point); ルータの1種

電話網とインターネット網の変遷(3)

常時接続時代(ADSL, FTTH)

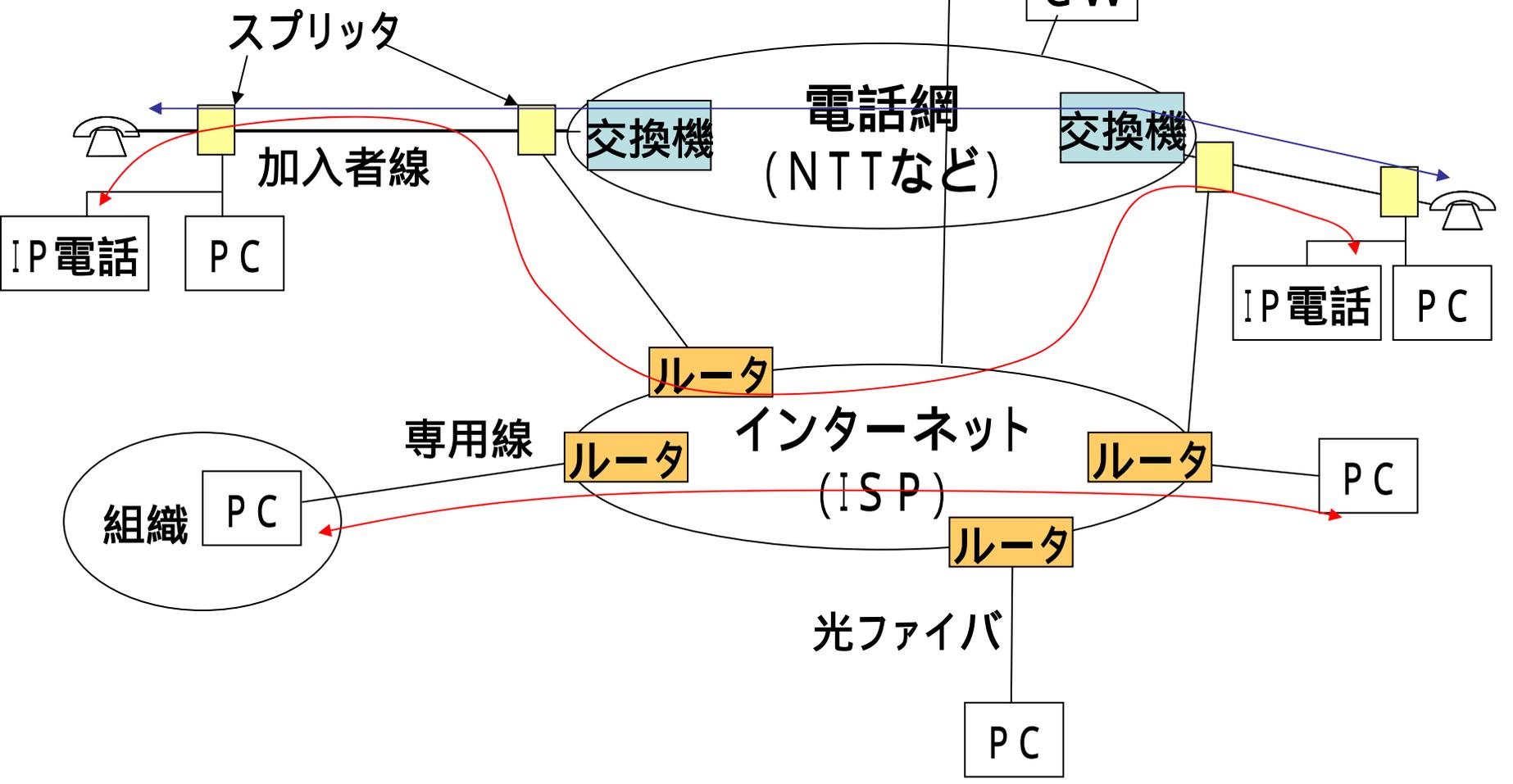


- ・加入者線を電話とインターネットが共用する
(スプリッタで周波数分割)

電話網とインターネット網の変遷(4)

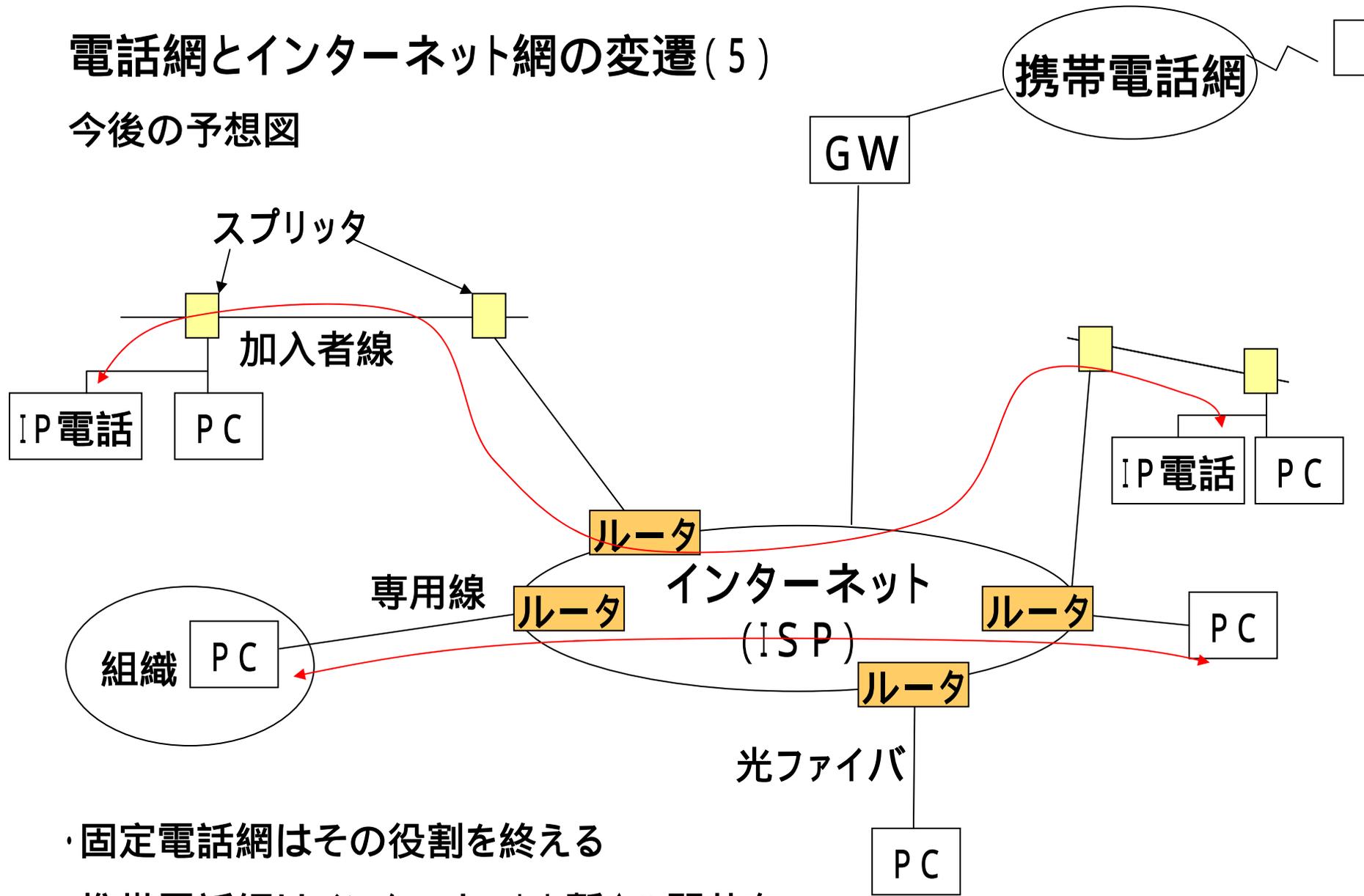
IP電話の登場

携帯電話網  携帯電話



電話網とインターネット網の変遷(5)

今後の予想図



- ・固定電話網はその役割を終える
- ・携帯電話網はインターネットと暫くの間共存する(通話中に移動が可能)

なぜIP電話では移動できないのか

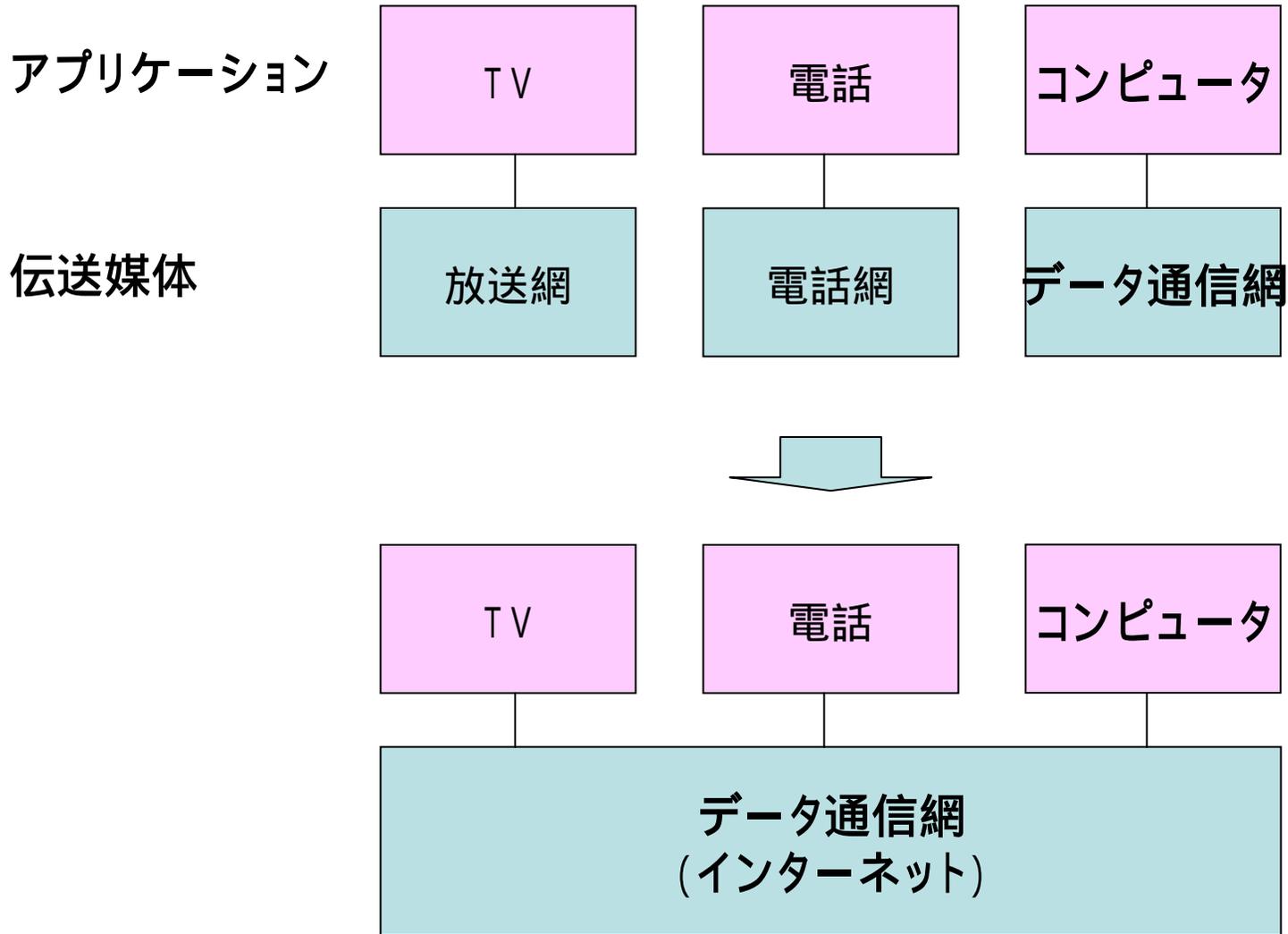
携帯電話とIP電話

- ・携帯電話は回線交換, IP電話はパケット交換
- ・携帯電話の電話番号は固定 移動しても電話番号は変わらない
どこに移動しても継続して通信ができる
- ・IPアドレスは場所に依存した情報 移動するとIPアドレスが変わる
移動すると通信の継続ができない

現在のIP電話は固定電話の代替にすぎない(携帯電話の代替にはならない)

移動可能な方式が提案されているがまだ研究段階(モバイルIP、MobilePPCなど)

通信媒体はインターネットに統合される



インターネットの課題はセキュリティ

インターネットはオープン

いつでも誰でもどこからでも(ユビキタス社会)

悪意を持つ第三者も自由に接続できる

盗聴、改ざん、なりすましの脅威

セキュリティ対策が必須

- ・暗号技術

 - 共通鍵暗号方式

 - 公開鍵暗号方式

- ・ファイアウォール

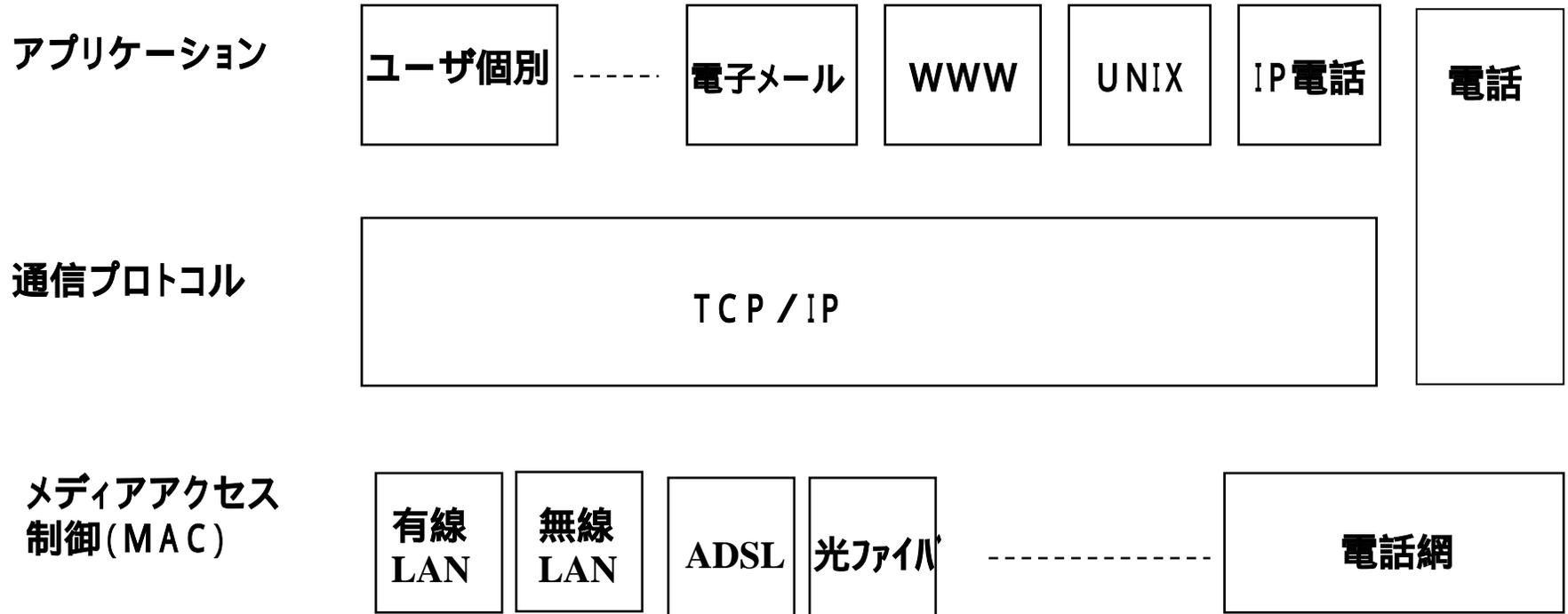
- ・ウィルス対策

 - ウィルス;自己伝染機能、潜伏機能、発病機能の1つ以上を有するもの

まとめ

- ・IT革命の本質はインターネット
- ・ユビキタス社会のイメージ
- ・電話網とインターネットの違い
- ・インターネットのしくみ

インターネットとTCP/IP



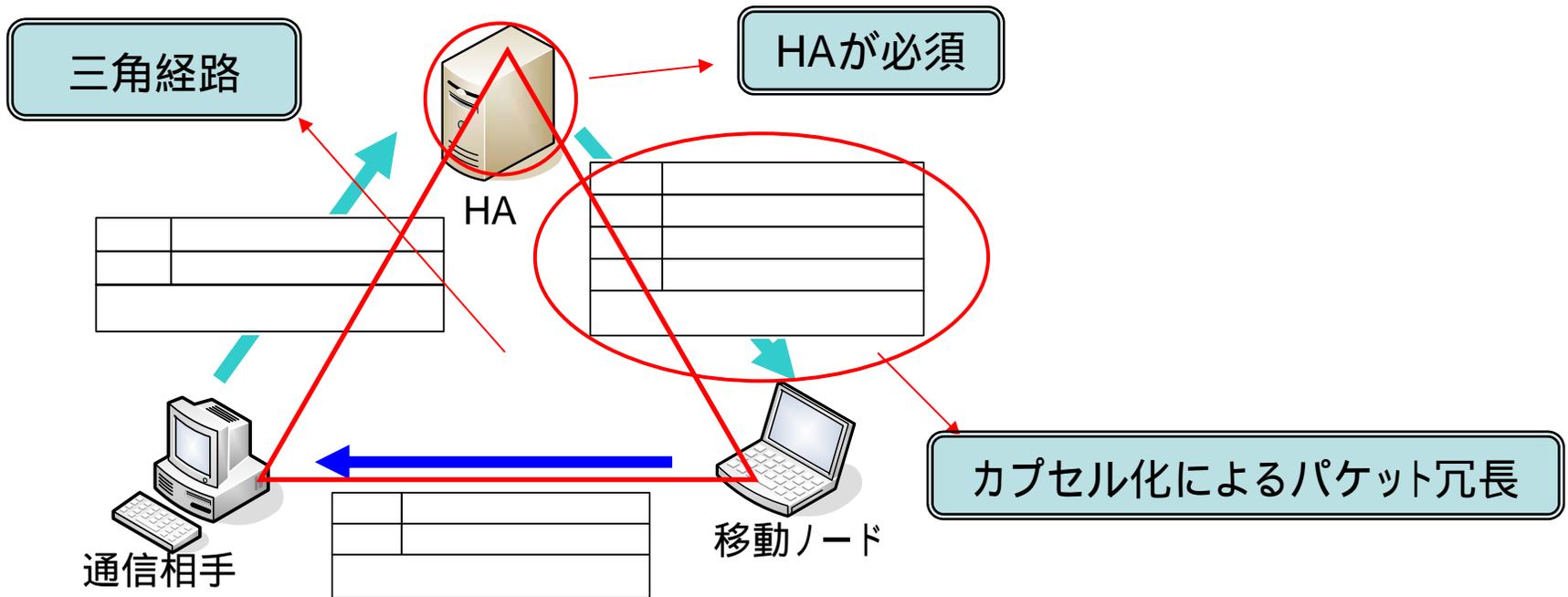
Everything over IP.

IP over everything.

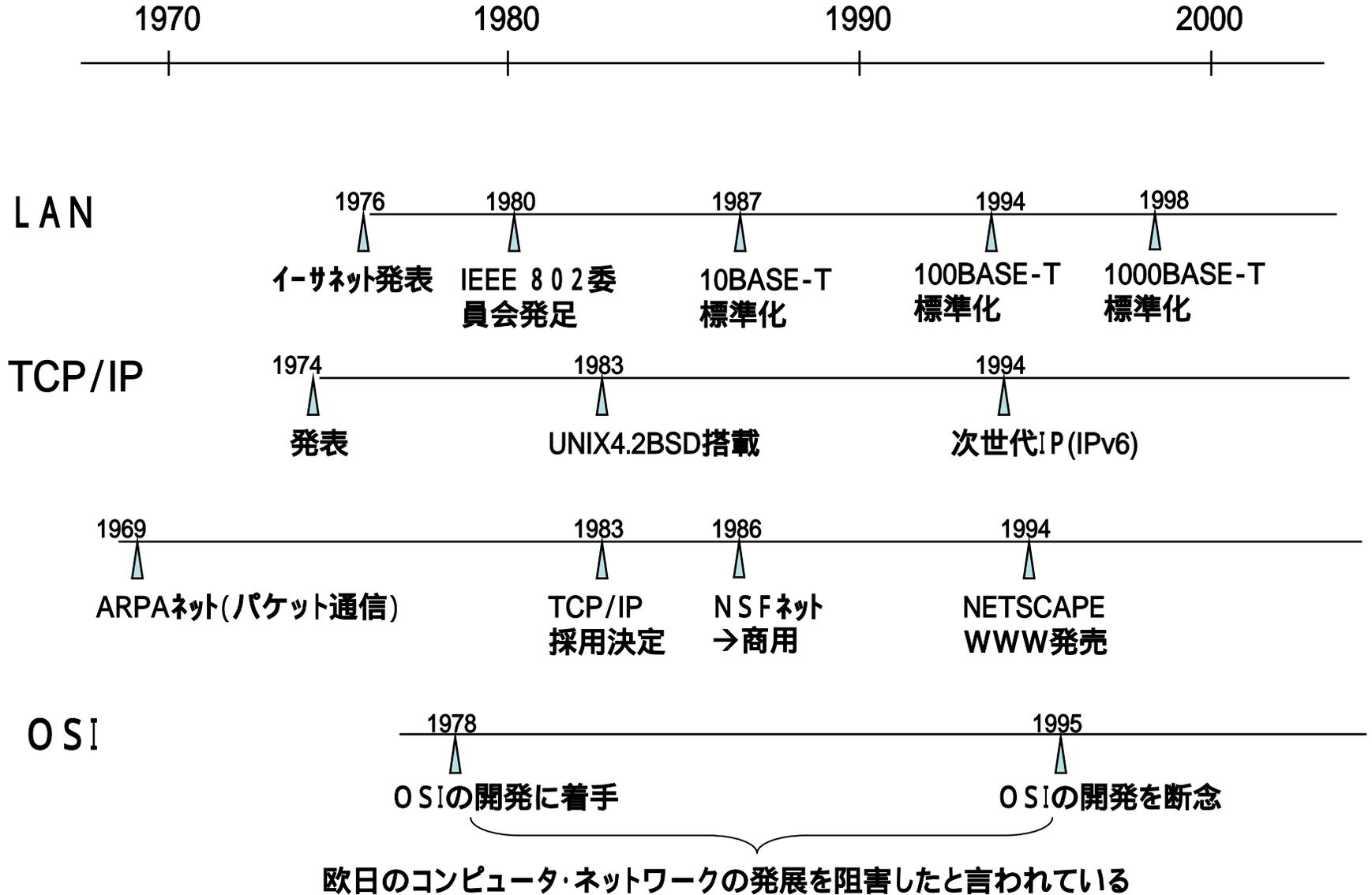
通信中に移動を可能とするための技術

- ・パケットを移動ノードに届ける手段
- ・上位ソフトウェアに対してアドレスの変化を隠蔽する手段

Mobile IP



インターネット関連技術の歴史

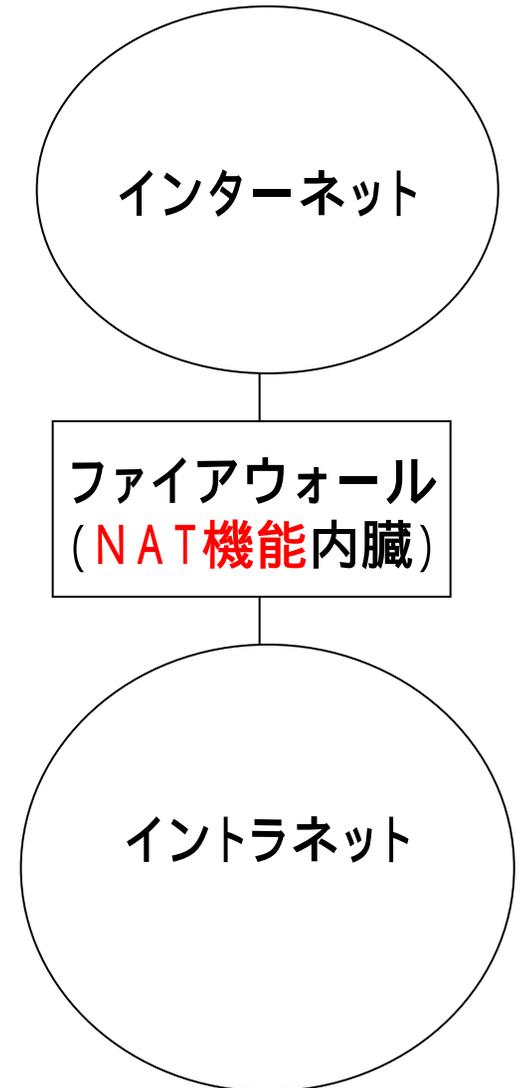


ファイアウォール

・組織内のネットワークを外部の脅威から守るための機器および技術の総称

・ファイアウォールを設置する理由

- ・情報流出入経路の限定
- ・内部ネットワークを統一的に保護
- ・内部ネットワークの隠蔽
- ・情報の取捨選択
- ・入出力ログの作成、アクセスの記録



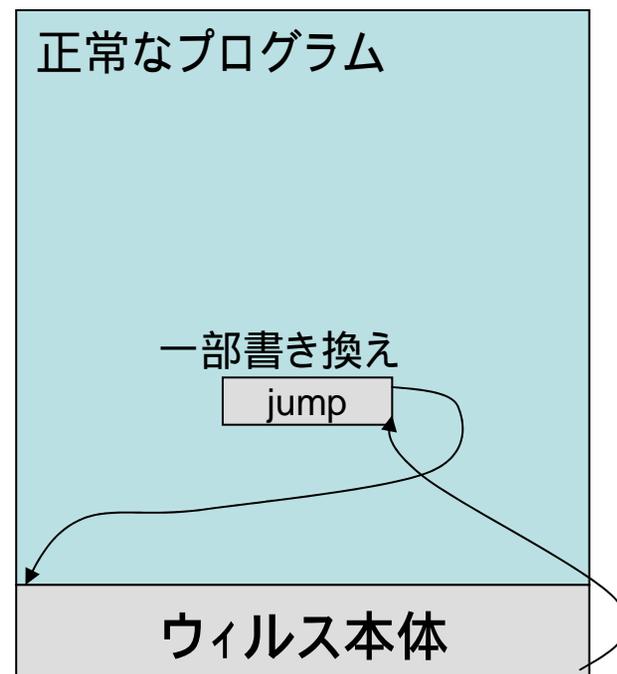
ウイルス対策ソフト

ウイルスに感染したファイルを修復し、コンピュータを感染前の状態に回復するアプリケーションソフトウェア。「ワクチンソフト」「アンチウイルスソフト」などとも呼ばれる。

コンピュータウイルスの定義

下記の行動パターンを1つ以上持つ不正プログラム

- ・感染； 他のファイルにウイルス自身を付着させる
- ・潜伏； 一定の条件が揃うのを待って悪質な行動をする
- ・発病； データの破壊、動作の不安定などユーザの意図しない行動をする



暗号化技術

暗号方式

共通鍵暗号 (慣用暗号, 対称暗号)

暗号化と復号に同じ暗号鍵を使う

DES (デス), 3DES (トリプルデス), AES など多数
太古の歴史あり

数字の列

公開鍵暗号 (非対称暗号)

暗号化と復号に異なる暗号鍵を使う

RSA

生まれて30年余り

20世紀最大の発明と言う人も

データ通信の基本

OSI参照モデル

レイヤ番号	レイヤ名	定義内容
7	応用層	業務に依存した処理方式
6	プレゼンテーション層	データの表現方法の取り決め
5	セッション層	業務の開始, 終了の取り決め
4	トランスポート層	エンド端末間の通信方式
3	ネットワーク層	異なるネットワーク間を中継するルーティング方式
2	データリンク層	同一ネットワーク内の通信方式
1	物理層	伝送路の物理特性

TCP

IP

OSI; Open Systems Interconnection

プロトコル乱立時代(1970年代、1980年代)

OSI参照モデル

メーカー独自

OSI準拠

パソコン系

UNIX系

アプリケーション層	SNA など	OSI	NetWare		FTP
プレゼンテーション層			WindowsNT		
セッション層			SPX	TCP/UDP	TCP/UDP
トランスポート層			IPX	IP	IP
ネットワーク層			LLC (ISO8802.2)		
データリンク層	MAC (ISO8802.3/8802.5/FDDI)				
フィジカル層					

- ・メーカー独自ネットワークは、オープンシステムの進展に伴い衰退した。
- ・OSI準拠ネットワークは、仕様が重く普及しなかった。
- ・パソコン系 / UNIX系はTCP / IPに統一され急速に普及した。

なぜOSIは失敗したのか

- ・あらゆる仕様を盛り込み複雑化、膨大な仕様。
- ・政治主義的な標準化活動に終始した。
 - 官僚主義、トップダウン方式で実践軽視
 - 各国の電信電話局の利権意識で規格が複雑化、長期化
 - 電話回線中心の発想
- > 開発期間の増大
 - 解釈の違いで相互接続困難
 - メモリ食う
 - 性能が出ない

なぜTCP/IPが生き残ったのか

- ・少数の優秀な技術者が開発。
- ・シンプル(データ通信に特化)。
- ・ソースを公開(UNIX)。安価に提供。
 - > 短期開発
相互接続容易
そこそこの性能

机上の論理が先行した技術(いずれも失敗)

- ・OSI < TCP/IP
- ・ATM < パケット通信
- ・FDDI < イーサネット

共通して言えることは？

- ・多数の優秀な技術者が検討に加わった
- ・仕様の膨大化、複雑化
- ・解釈の違いに起因する相互接続の困難さ
- ・開発期間の増大、コストの増大

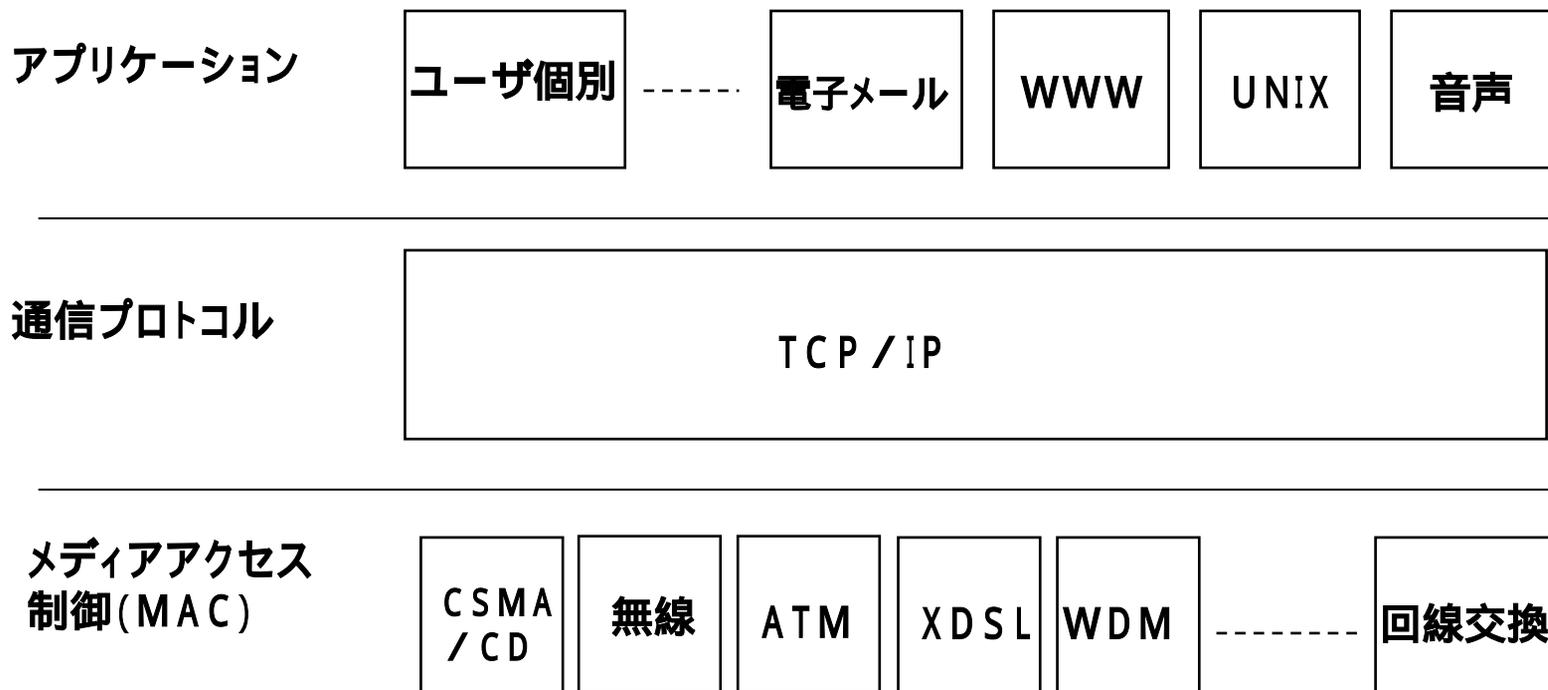
ATM; Asynchronous Transfer Mode

FDDI; Fiber Distributed Data Interface

TCP/IPによる抽象化(標準化されたことによる利点)

Everything over IP.

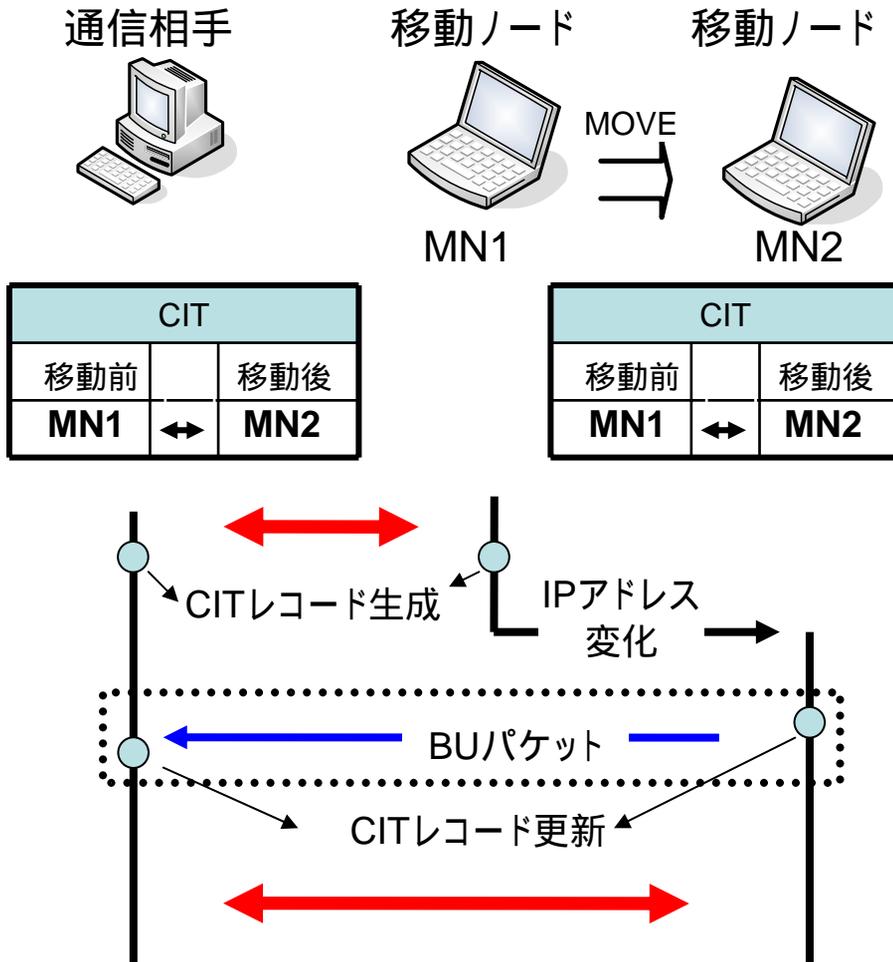
IP over everything.



・アプリケーションと伝送媒体が切り離された。

独立した発展が可能となった。

Mobile PPCの通信



通信開始時

- 両端末でCITレコード生成

移動時

移動ノードの処理

- 移動し, IPアドレスを取得
- CITレコードを更新
- BUパケットの生成・送信

通信相手ノードの処理

- BUパケットに含まれる情報を元に, CITレコードを更新

Mobile PPCの通信

- アドレス変換処理

- 更新されたCITレコードに従い、送受信パケットに対してIP層においてIPアドレスの書き換え処理



MOVE

移動ノード

MN1

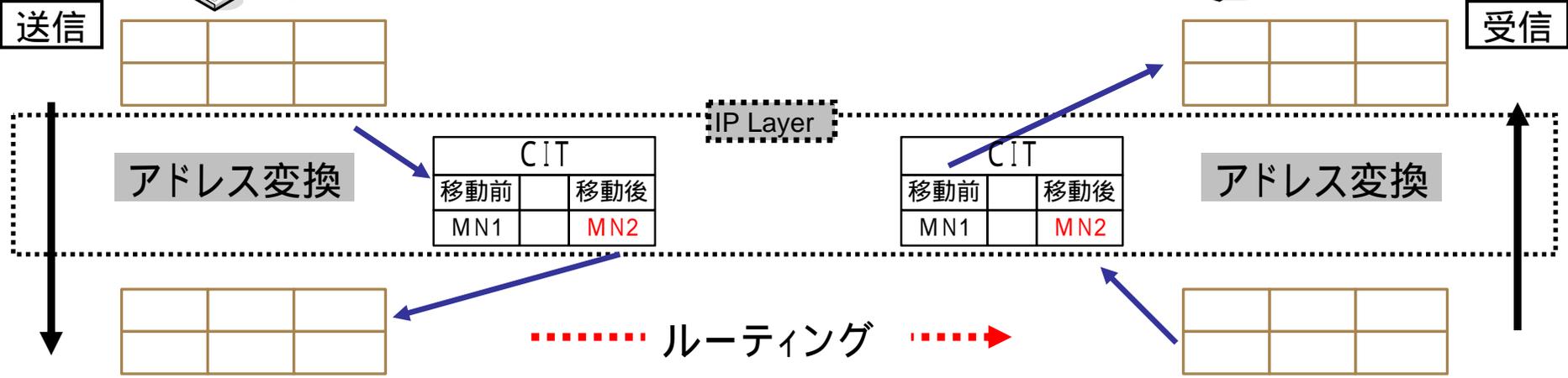
MN2



通信相手

CN1

←..... コネクション維持→



送信時

受信時

正しくルーティングされるようにアドレス変換

通信開始時のアドレスの組に一致するようにアドレス変換

IPアドレスの変化を上位層に隠蔽

宛先IP 送信元IP データ