インターネットのしくみ

―インターネットを支える基本技術―

森下 泰宏

(社)日本ネットワークインフォメーションセンター

yasuhiro@nic.ad.jp

本講義の主題

- インターネットの基本部分を支えるさまざまな技術
- インターネットを動かすためのさまざまな「しくみ」のうち、最も基本的なもの
- 今のところ「マウスでクリック」だけでは解決できにくいこと

本講義の対象者

- インターネットのしくみを知りたい人
- ネットワーク管理担当者
  - 新米の管理担当者(にさせられた人)
  - なんとなくマニュアル通りに管理しているが、わけがわかっているわけではない人
- 「マウスでクリック」の向こう側にあるものを知りたい人

本講義では話さないこと

- どこのプロバイダにつないだらいいの？
- どこのホスティングサービスを使ったらいいの？
- “自分の会社.co.jp”を使いたいけど、どうしたらいいの？

本講義における3つのキーワード

- ドメイン名(Domain Name)
  - インターネット上における「住所」の管理方法
- IPアドレス(IP address)
  - インターネット上における意思の疎通(データのやりとり)を行う際に必要な識別番号
- DNS(Domain Name System)
  - 「ドメイン名」を管理するための手段
  - 「ドメイン名」と「IPアドレス」を結びつけるための手段

ドメイン名、IPアドレス、DNS

- インターネットを支える3つの「しくみ」
- これらのいずれが欠けても、インターネットは満足に使えない
- いずれも、インターネットが爆発的に普及する以前に開発された
- 規模が数万倍以上に拡張しても、これら3つの基本的なしくみは変化していない

共通資源とJPNIC

- インターネット全体で共通に利用されるもの
  – ドメイン名、IPアドレス、プロトコル番号など
- インターネットの「共通資源」(common resources)と呼ばれている
- 日本における、これら共通資源の効率的な割り当て業務、円滑な管理運用

à JPNICの重要な業務の一つ

ドメイン名(1)ドメイン名の概要

- ドメイン名とは
  - ドメイン名の例
- ドメイン名の構成要素
- ドメイン名における階層構造
- トップレベルドメイン(TLD)
  - 2文字のTLD(ccTLD)
  - 3文字のTLD

ドメイン名とは

- ある組織やホストなどが属するドメイン(領域)を表す文字列
- URLや電子メールアドレスとして利用される(例)
- 一般社会における「住所」「屋号」に相当

ドメイン名の例

- URLにおける使用例
  - http://www.nic.ad.jp/index-j.html
- 電子メールアドレスにおける使用例
  - yasuhiro@nic.ad.jp
  - query@domain.nic.ad.jp
    (サブドメイン(後述)を伴った例)

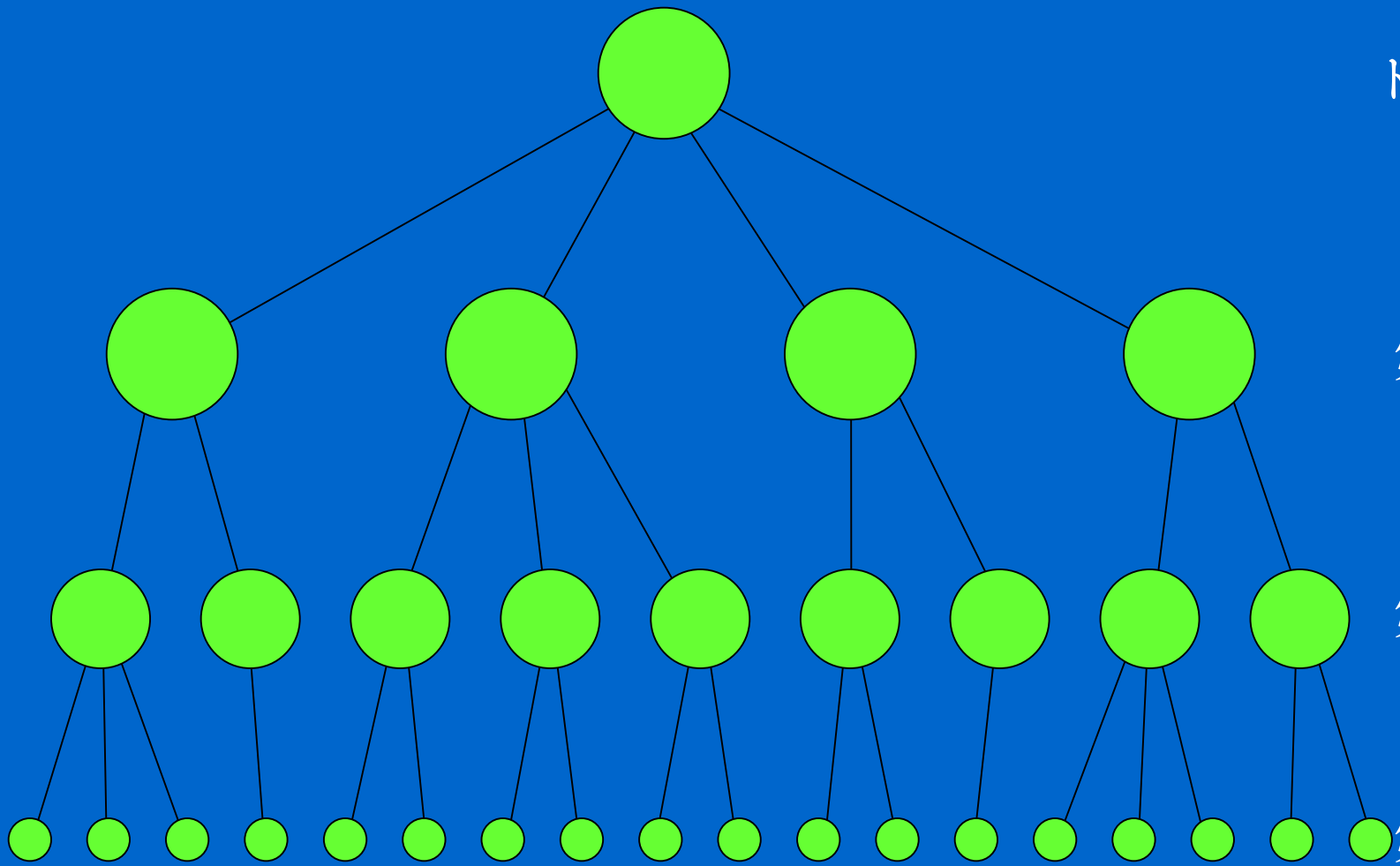
ドメイン名の構成要素

- アルファベット、数字、一部の記号(－など)、ピリオド(.)で構成
- ピリオドは、各要素の区切り文字として用いられる
- 大文字と小文字は区別されない
- 今のところ、漢字などは使えない
- 階層構造を持つ

ドメイン名における階層構造

- 右側の要素が「より広い」領域を表している
- 逆向き木構造(Inverse Tree Structure)
- トップレベルドメイン
  (Top Level Domain: TLD)
- 第2レベルドメイン、第3レベルドメイン…

逆向き木構造



トップレベルドメイン(TLD)

- 最上位レベルのドメイン
- ドメイン名表記において、いちばん右(トップレベル)に来る要素
- 2文字のTLD
- 3文字のTLD

2文字のTLD

- 国別コード(ISO3166 country code)に基づく2文字ドメイン
- ccTLDと呼ばれる
- 基本的に国単位で利用される
- 日本には“JP”が割り当てられている

ccTLDの例

- JP(日本)
- KR(韓国)
- DE(ドイツ)
- CA(カナダ)など
- 管理ポリシーは、各国に委ねられている

3文字のTLD

- ドメイン名が利用されるようになった当初から使われていたドメイン
- 米国を中心に使用されてきた
- 大まかに2種類に分類される
- gTLD(COM,ORG,NET)
- それ以外(EDU,GOV,MIL等)
- 今後どのように管理されるかは流動的

ドメイン名(2)(JPドメイン)

- JPドメインの現状
- JPドメインの構造
- 属性型ドメイン
- 地域型ドメイン

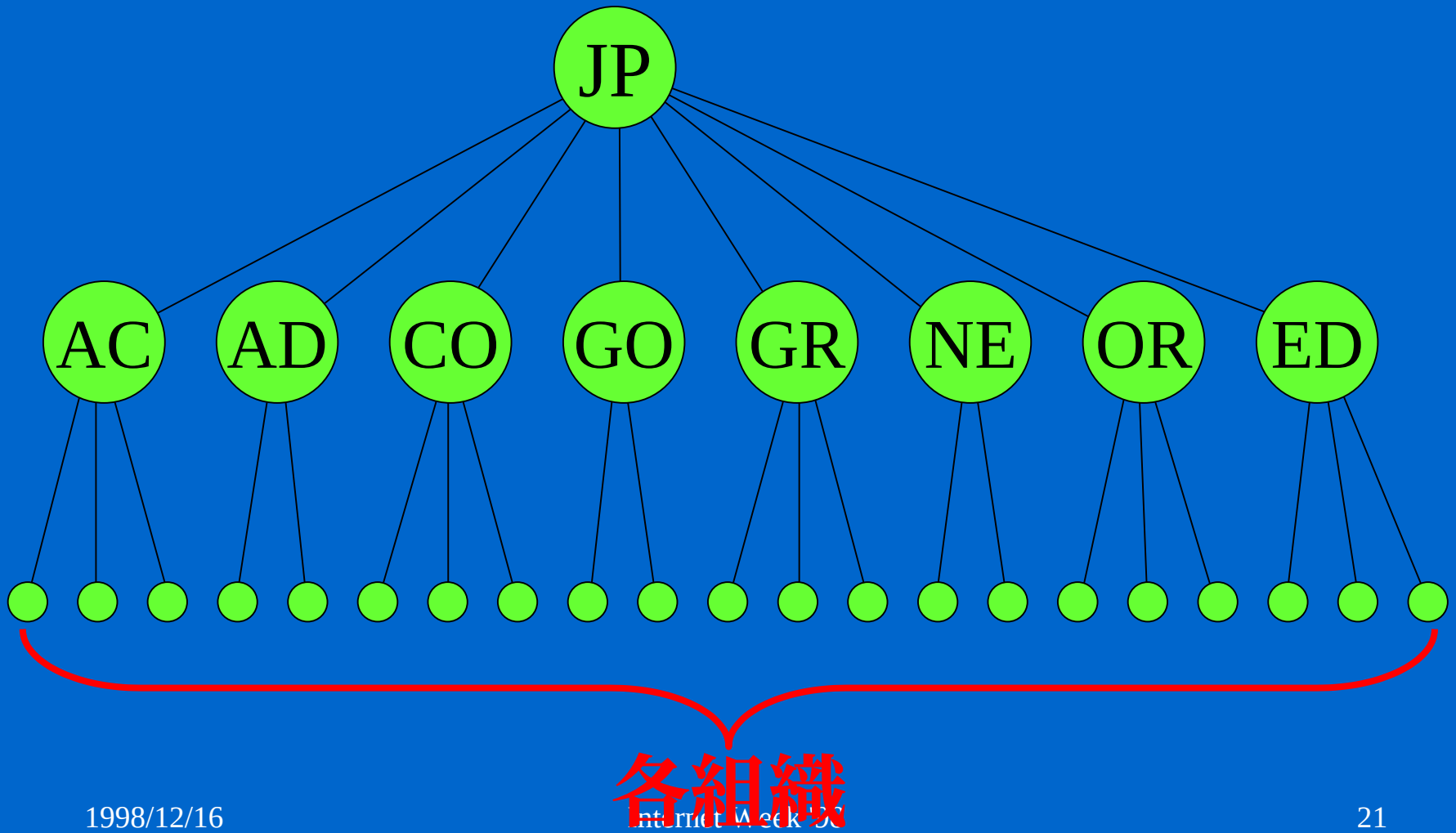
JPドメインの現状

- 日本を表すTLD: JP
- ISO3166により定義
- JPNICが管理･運用

JPドメインの構造

- 第2レベルまでJPNICが管理
- 2種の第2レベルドメイン
- 属性型ドメイン
- 地域型ドメイン

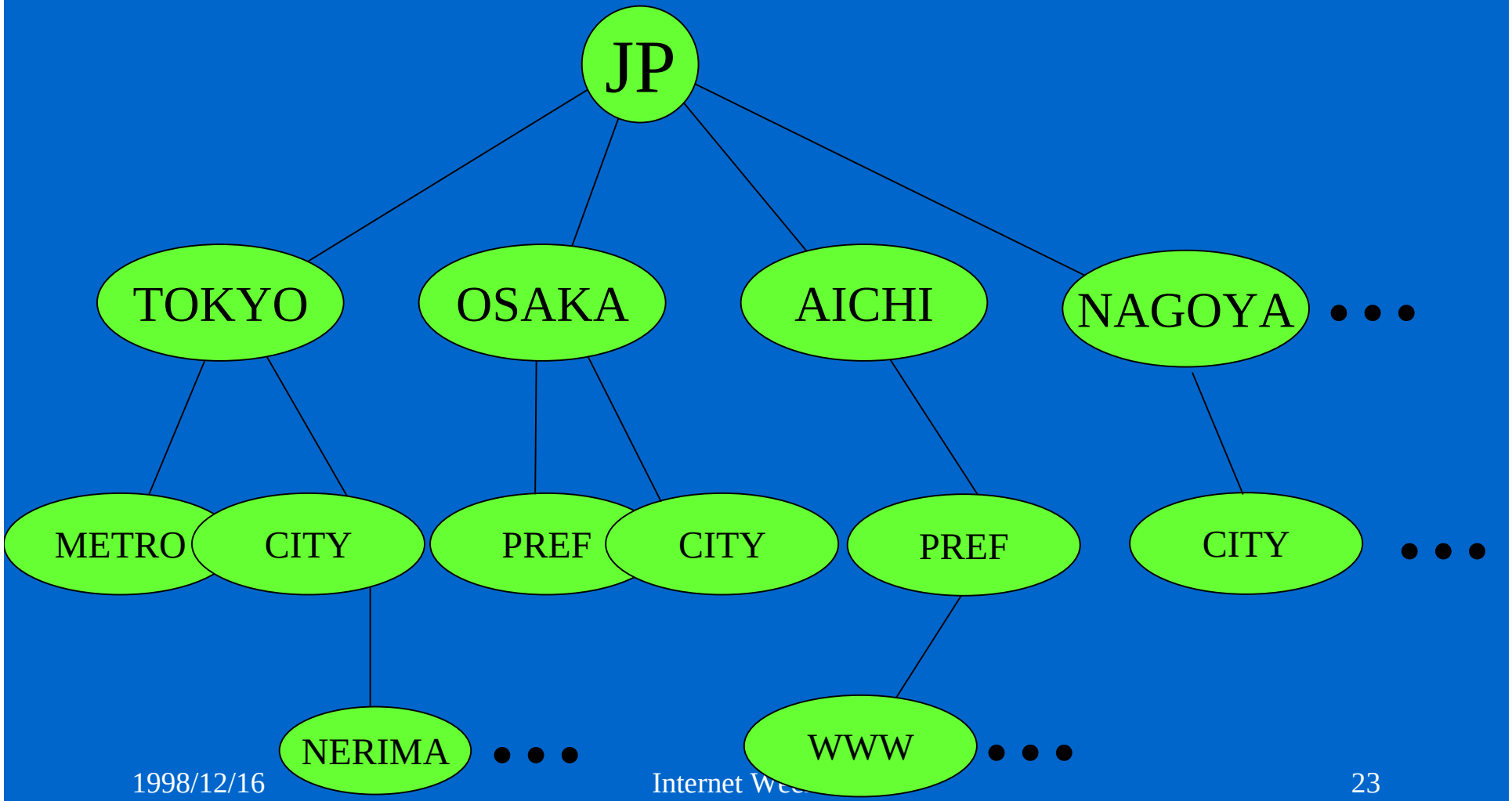
属性型ドメイン



属性型ドメイン

- 組織の属性により決定
- アルファベット2文字
- 7つの属性型ドメイン(1998年12月現在)
- ac, ad, co, go, gr, ne, or
- 1999年より、ed属性を追加予定

地域型ドメイン


JP
TOKYO
OSAKA
AICHI
NAGOYA
METRO
CITY
PREF
CITY
PREF
CITY
NERIMA
WWW

地域型ドメイン

- **都道府県名、政令指定都市名を利用**
- tokyo, osaka, aichi, sapporo, yokohamaなど
- **地域に根ざしたドメイン**
- **都道府県庁、地方公共団体、個人等が利用**

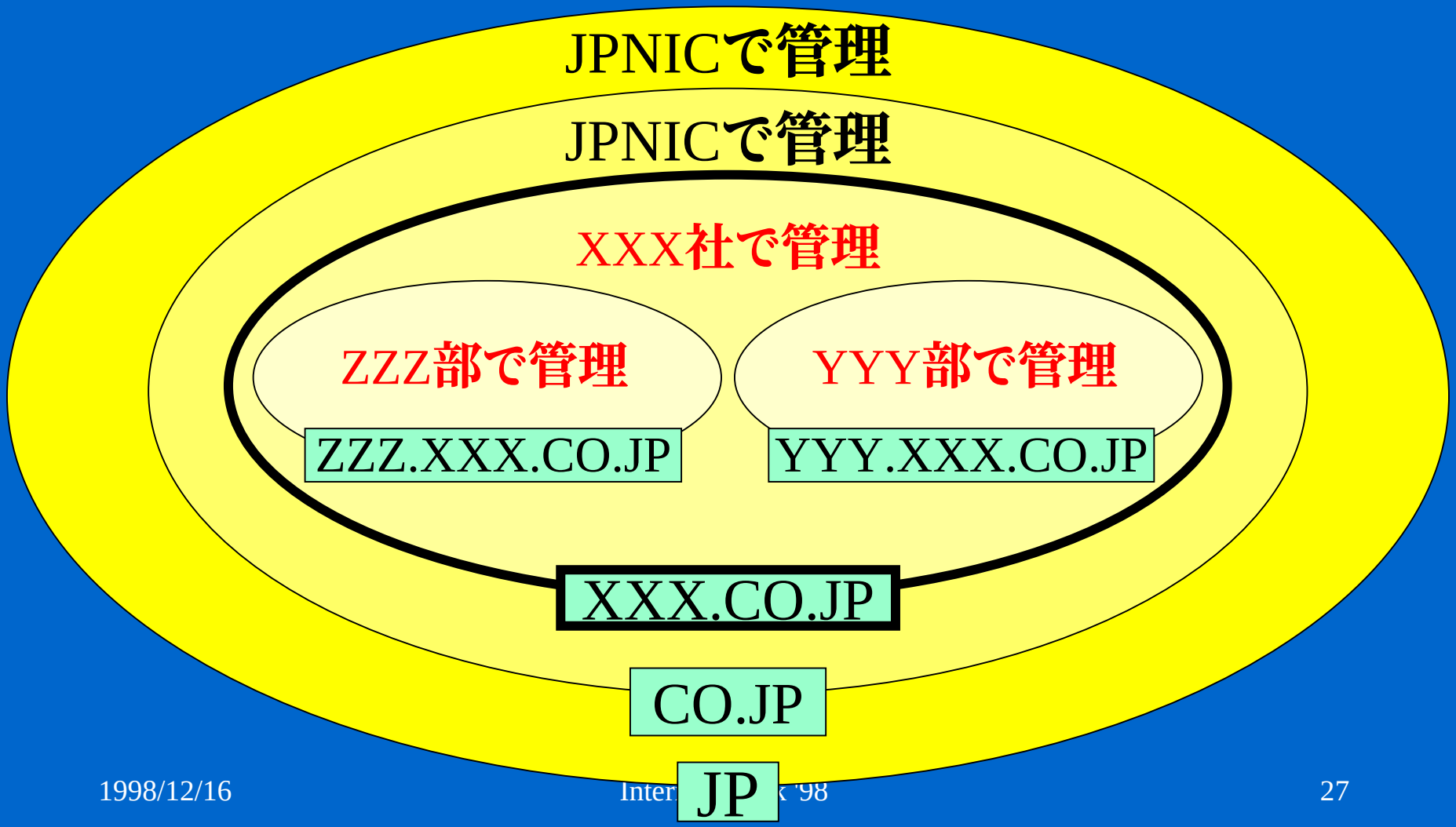
ドメイン名(3)サブドメイン

- サブドメインとは
- サブドメインと管理の委譲

サブドメインとは

- あるドメイン階層から見た、すぐ下のドメイン階層
- 属性型ドメインや地域型ドメインは、JPドメインのサブドメインに相当

サブドメインと管理の委譲



サブドメインと管理の委譲

- 組織ドメインの下流に、各組織で任意にサブドメインを設定することが可能
- これにより、一つの組織内でドメイン名をより細かく分割できる
- 管理部署毎に分割管理する等の手法が可能
- サブドメインを効率的に運用することにより、管理を委譲することができる

ドメイン名(4)よく聞かれる質問

- ドメイン名に「実体」は必要か

ドメイン名に「実体」は必要か

- ドメイン名に「実体」は必ずしも必要ない
- 1台のマシンに、仮想的に複数のドメイン名を割り当てることも可能
- 自組織のマシンに、別組織のドメイン名を付与することも可能
  - ホスティングサービス
  - バーチャルドメインサービス

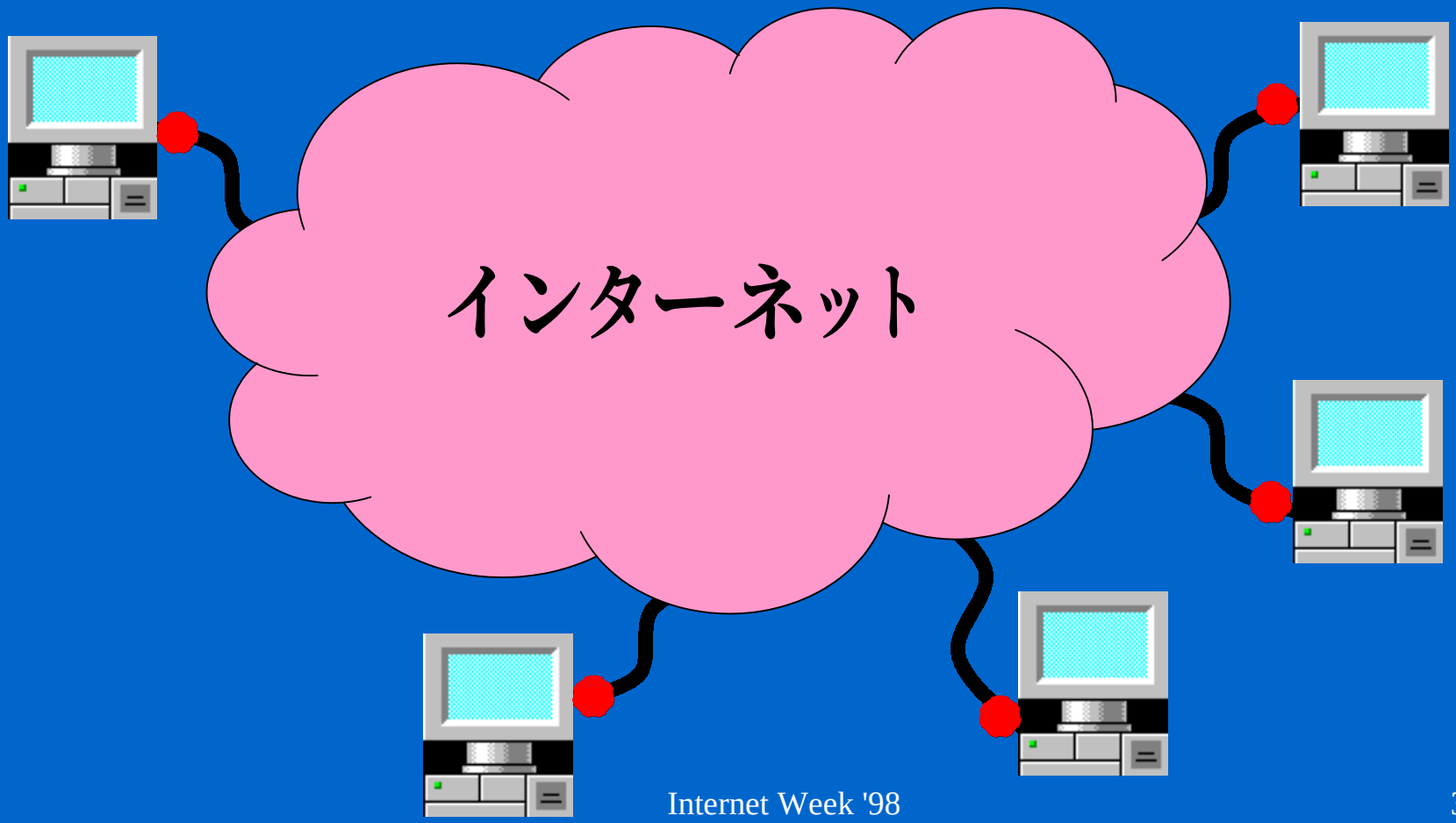
IPアドレス(1)概要

- IPアドレスとは
- プロトコル(Protocol)
- RFC
- TCP/IP
- TCP/IPの特徴

IPアドレスとは

- インターネット上の機器を識別するための番号
- インターネットに接続中のすべての機器に割り当てられている
- 電話における「電話番号」に相当
- インターネットを利用する際に必要不可欠のもの

IPアドレス



プロトコル(Protocol)

- 本来の意味: 条約案、議定書
- コンピュータ同士を接続して、データやメッセージをやりとりする(通信する)ために必要な手順や約束事、決まり
- 物理的な接続方法
- ネットワーク接続方法
- データの転送方法、など

RFC

- Request For Commentsの略
- インターネットで利用されている各種プロトコルについて記述された文書
- IETF(The Internet Engineering Task Force)により策定(URL: http://www.ietf.org/)

TCP/IP

- Transmission Control Protocol / Internet Protocolの略
- インターネット上でデータを送受信するためのプロトコル
- RFC791により定められている
(編者:故Jon Postel)

TCP/IPの特徴(IPアドレス)

- 通信元、通信先を判断するのに「IPアドレス」を用いる
  - à 通信元、通信先双方の機器にIPアドレスが割り当てられている必要がある
- TCP/IPプロトコルに準拠していれば、どのような機器とも通信できる
  - ® 機器の種類やソフトウェアを選ばない

TCP/IPの特徴(効率的な利用)

- 常時接続している必要がない
  - à 使いたいときだけIPアドレスが割り当てられれば十分
  - à ダイアルアップIP、DHCP等の手法による効率的な利用が可能

TCP/IPの特徴(媒体に非依存)

- データの到達性があれば、接続媒体にかかわらず利用可能
  - à 接続するためのメディアを選ばない
  - à 電話線、無線、UTPケーブル、光ファイバ等…

IPアドレス(2)より詳細な説明

- IPアドレスの仕様
- IPアドレスの体系
- IPアドレスにおけるクラス

à クラスA, クラスB, クラスC

à クラスD, クラスE

IPアドレスの仕様

11001010	00001100	00011110	10000110
202	12	30	134

- TCP/IPによって定められている
- 32ビット(4オクテット)の符号無し整数
- インターネットにおいて一意
- 8ビットずつ、ピリオド4つに区切る

IPアドレスの体系

- 従来からの体系
  à クラスによる体系
  à クラスA、クラスB、クラスC
- クラスレス(classless)なIPアドレス体系
  à CIDR(サイダー:後述)

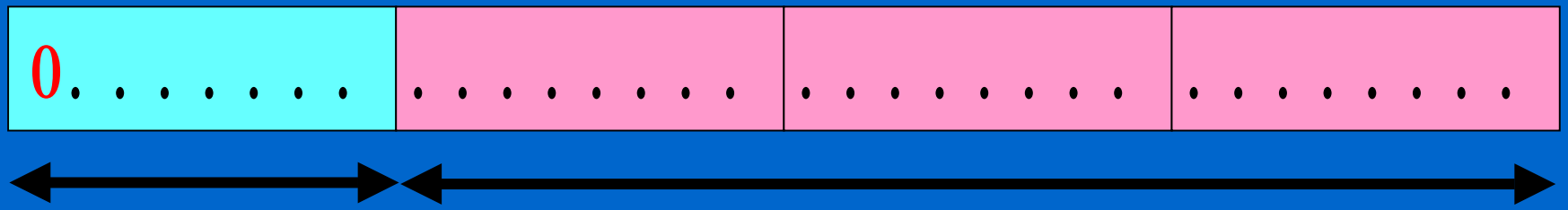
IPアドレスにおけるクラス

- 以前から利用されてきたアドレス体系
- IPアドレスを「ネットワーク部」と「ホスト部」に分割
- ネットワーク部が同じアドレスを、一つのネットワーク単位として取り扱う

IPアドレスにおけるクラス(続き)

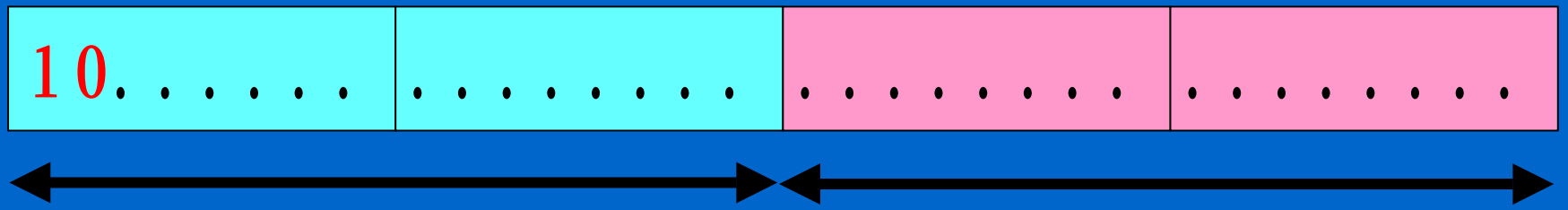
- IPアドレスをクラスA, B, Cの3つに区別
- 利用する組織のネットワークの規模に応じ、適切なクラスを利用
  - à 大規模(クラスA)
  - à 中規模(クラスB)
  - à 小規模(クラスC)

クラスA



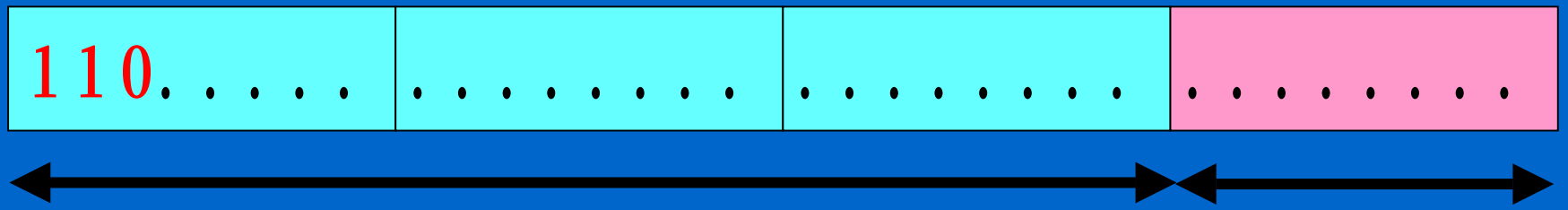
- IPアドレスの最上位ビットが 0
  - ―0.0.0.0～127.255.255.255
- ネットワーク部：上位1オクテット
  ホスト部　　：下位3オクテット
- 合計約1,670万ホストを接続可能
- 現在、新規割り当ては行われていない

クラスB



- IPアドレスの最上位ビットが 10
  - ―128.0.0.0～191.255.255.255
- ネットワーク部：上位2オクテット
  ホスト部　　：下位2オクテット
- 合計約65,000ホストを接続可能
- 現在、新規割り当ては行われていない

クラスC



- IPアドレスの最上位ビットが 110
  - ―192.0.0.0～223.255.255.255
- ネットワーク部：上位3オクテット
  ホスト部　　：下位1オクテット
- 合計約250ホストを接続可能
- 現在、この領域から割り当てられている

クラスD、クラスE

- クラスD
  - IPアドレスの上位4ビットが“1110”
  - IPマルチキャストで利用
- クラスE
  - IANAにより予約(現在利用されていない)
- 特殊な用途に用いられるIPアドレス
  - 組織には割り当てない

クラスによるIPアドレス割り当ての問題点

- それぞれのクラスにおける最大接続可能ホスト数にあまりにも差がある
- クラスA
  - 16,777,216(2の24乗)
- クラスB
  - 65,536(2の16乗)
- クラスC
  - 256(2の8乗)

問題点(アドレスの効率)

- クラスAを十分に使い切れるような組織は世界にほとんどない
  - à にもかかわらず、IPアドレスの半分はクラスA
- 最低単位がクラスC
  - à 1台～数台しか接続しない小さな組織でも一つのクラスCを割り当てるしかない

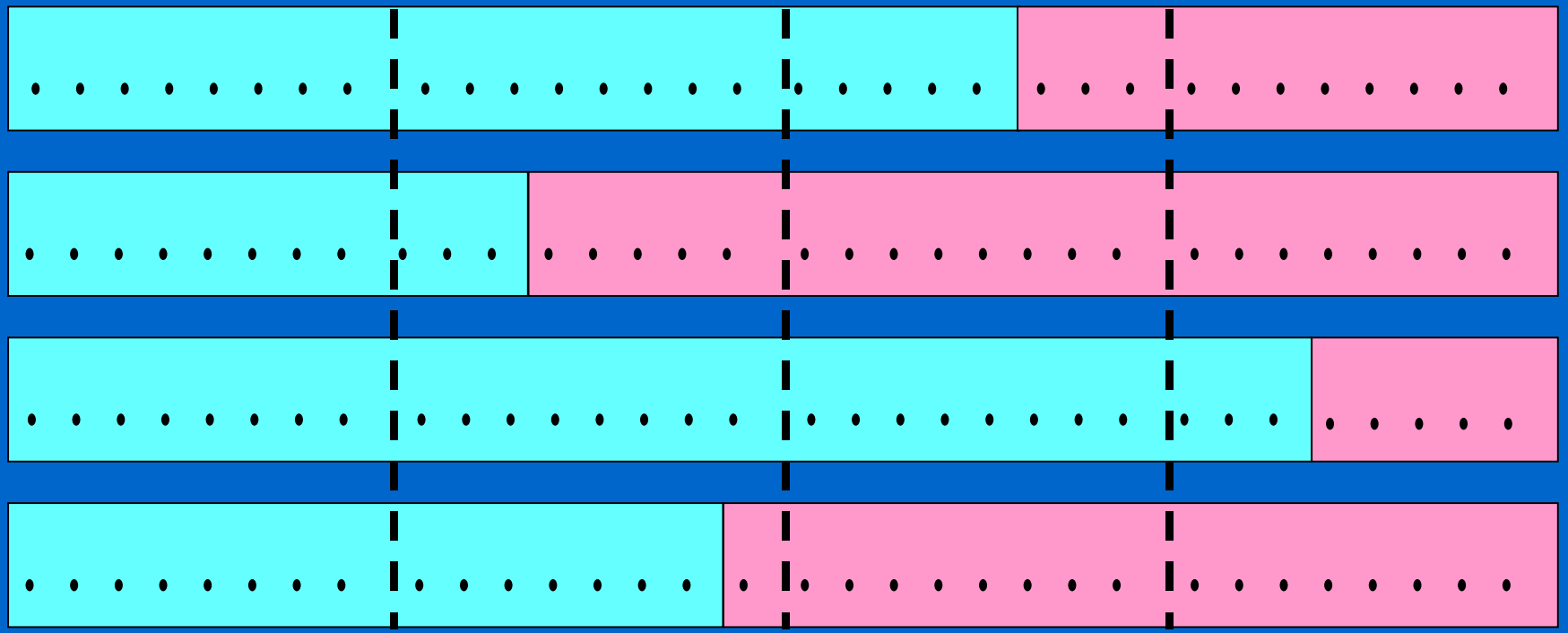
IPアドレス(3)CIDR

- クラスレスなIPアドレス体系
- CIDRの思想
- CIDRによる表記
- CIDRによる利点
- CIDRによる階層的な管理手法

クラスレスなIPアドレス体系

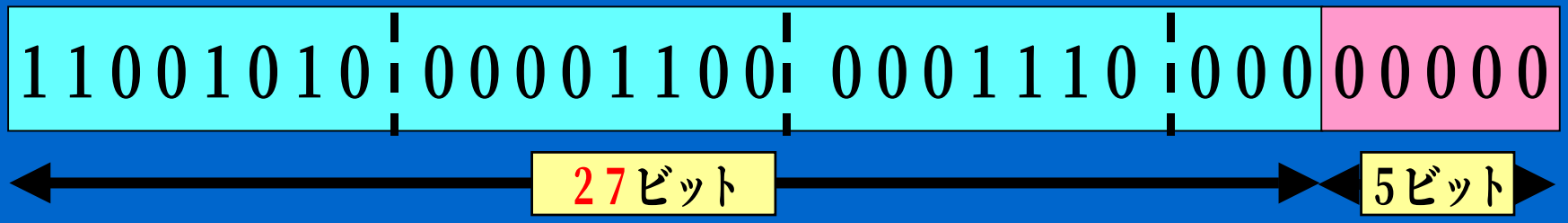
- クラス単位でのIPアドレス割り当てをやめ、任意のブロック単位でIPアドレスを割り当てられるようにしたもの
- CIDR(Classless Inter-Domain Routing)に基づいたIPアドレス割り当て体系

CIDRの思想



どこの位置でも
切れるようにしよう！

CIDRによる表記

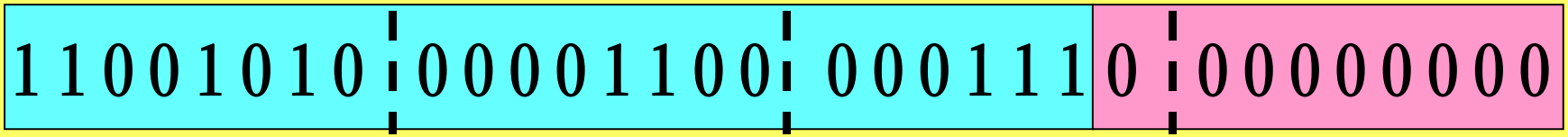


202.12.30.0 / 27

- 「プレフィックス長」の導入
- “ネットワーク番号 / プレフィックス長”で表記

CIDRによる利点

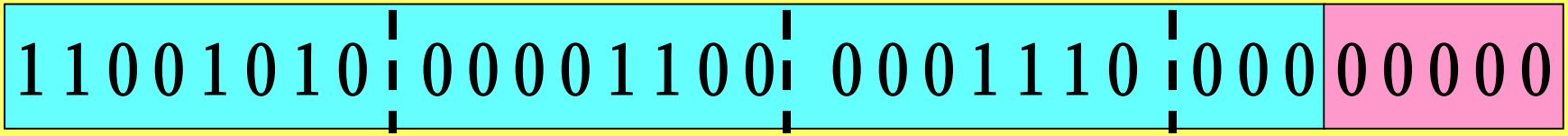
連続したクラスCを1つのCIDRブロックとして
取り扱うことが可能



CIDR表記：202．12．30．0／23

→ 202．12．30．0－202．12．31．255

クラスCよりも小さなアドレスブロックも、
他のブロックと同様に取り扱うことが可能



CIDR表記：202．12．30．0／27

→ 202．12．30．0－202．12．30．31

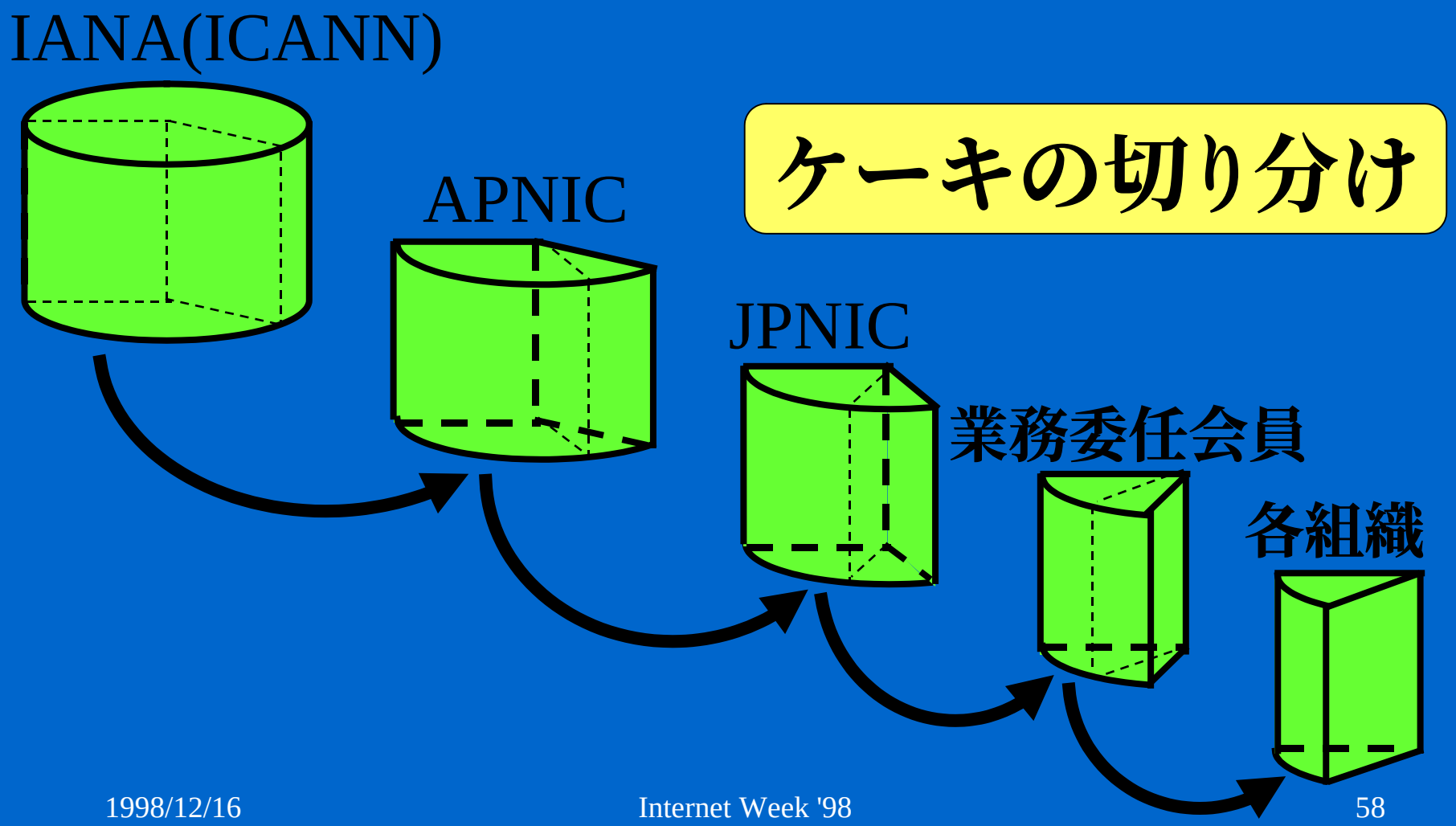
CIDRによる利点(続き)

- IPアドレスの割り当て効率の向上
  - à 限りあるIPアドレスの有効活用
- IPアドレスの管理体系の構造化(後述)が可能
  - à 階層的なアドレスブロックの管理
  - à 現在の管理体系に合致

IPアドレスの管理構造

- **階層的な管理構造**(CIDRの導入)
- APNICがJPNICにアドレスブロックを割り当て
- JPNICはそのブロックから各プロバイダにアドレスブロックを割り当て
- プロバイダは各ユーザの規模に応じてアドレスブロックを割り当て

IPアドレスの管理構造



CIDRによる階層的な管理手法

- アドレスをブロック(CIDRブロック)毎にまとめて管理できる
- 経路制御(基本技術の一つ)を行う際にも有効
- 経路情報テーブルを小さくできる(経路表を2のべき乗単位でまとめることができる)

IPアドレス(4)IPアドレスの有効活用

- IPアドレスで表せる大きさ
- 新しいIPプロトコル(IPv6)
- プライベートアドレス
- アドレス変換
- NATとIPマスカレード

IPアドレスで表せる大きさ

- 全アドレス数: 4,294,967,296(2^{32})
  - 43億弱
- 世界人口(約60億)や携帯電話の桁数で表せる電話番号(10^{10}=100億) よりも少ない
- 21世紀前半には枯渇すると言われている

新しいIPプロトコル(IPv6)

- 電話のように「端末の仕様変更をせずに桁を増やす」ことは非常に難しい
- 現在、全く新しいIPプロトコル(IPv6)が開発されている
- アドレス空間を128ビットに拡張

IPv6はすぐに使えるのか?

- RFC2460(1998年12月発行!)で定義
- 現在、Standards Track(標準化の草稿)の段階
- IPv6が完成し普及するまで、現在のIP(IPv4)を「もたせる(アドレスの枯渇を防止する)」必要がある
- そのためのさまざまな技術

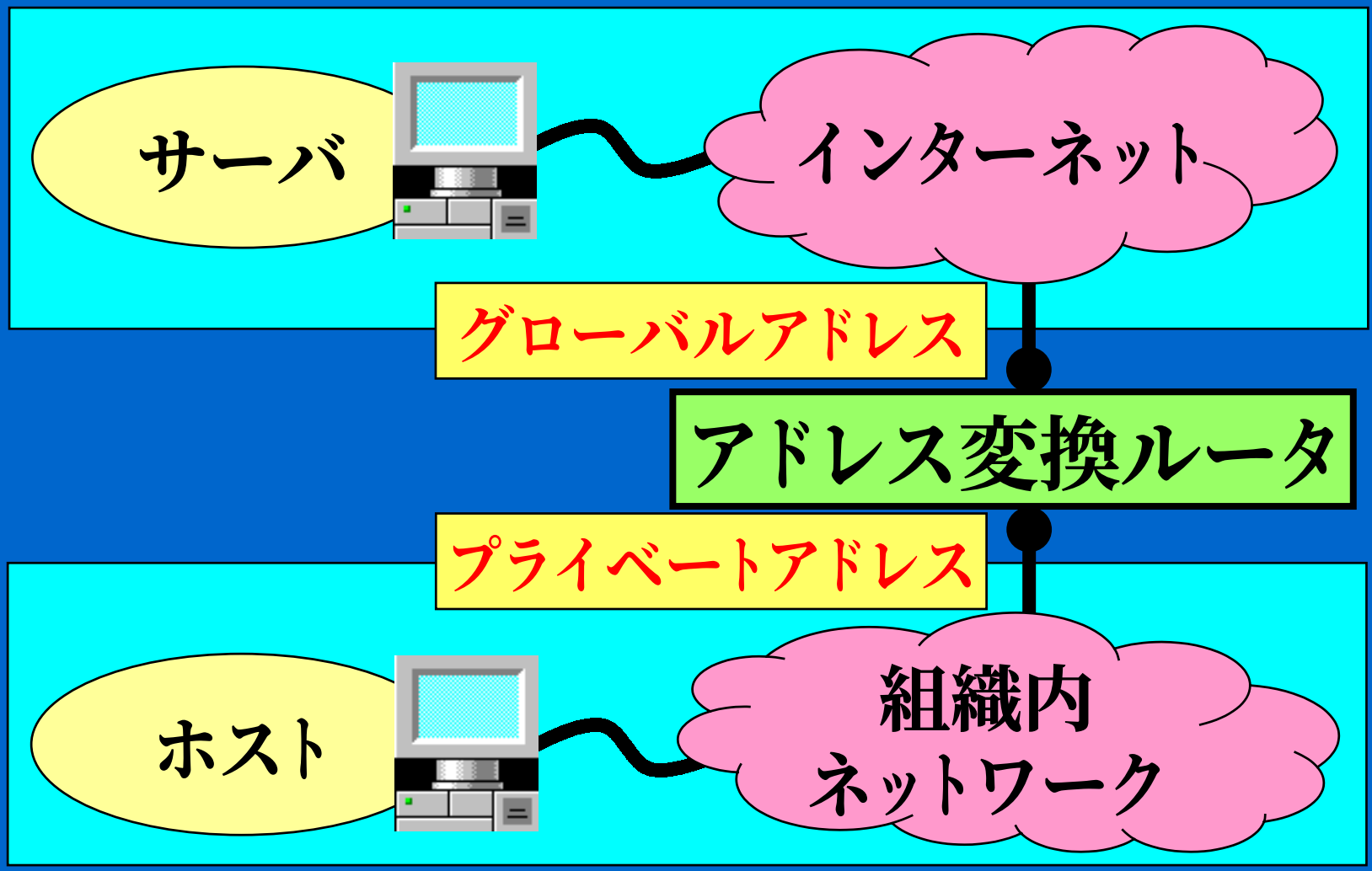
プライベートアドレス

- アドレスの枯渇を防止する手段の一つ
- 組織内で自由に使ってよいIPアドレス

à インターネット上で「使われていない」ことが保証されている

- RFC1918で定義
  - 10.0.0.0〜10.255.255.255(10.0.0.0/8)
  - 172.16.0.0〜172.31.255.255(172.16.0.0/12)
  - 192.168.0.0〜192.168.255.255(192.168.0.0/16)

アドレス変換


サーバ
インターネット
グローバルアドレス
アドレス変換ルータ
プライベートアドレス
ホスト
組織内
ネットワーク

アドレス変換

- IPアドレスを相互に変換する機能
  - NAT、IPマスカレード
- プライベートアドレスとグローバルアドレス間の相互変換
- プライベートアドレスがつけられた組織内のマシンからもインターネットを利用可能
- 最近のルータには標準で装備
- IPv4とIPv6との変換にも応用されている

NATとIPマスカレード

- NATはIPアドレスだけを変換
- IPマスカレードはIPアドレスだけではなく、ポート番号も変換
- IPマスカレードを使うことで、複数のプライベートアドレスを持つマシンが1つのグローバルアドレスで同時にインターネットを利用可能

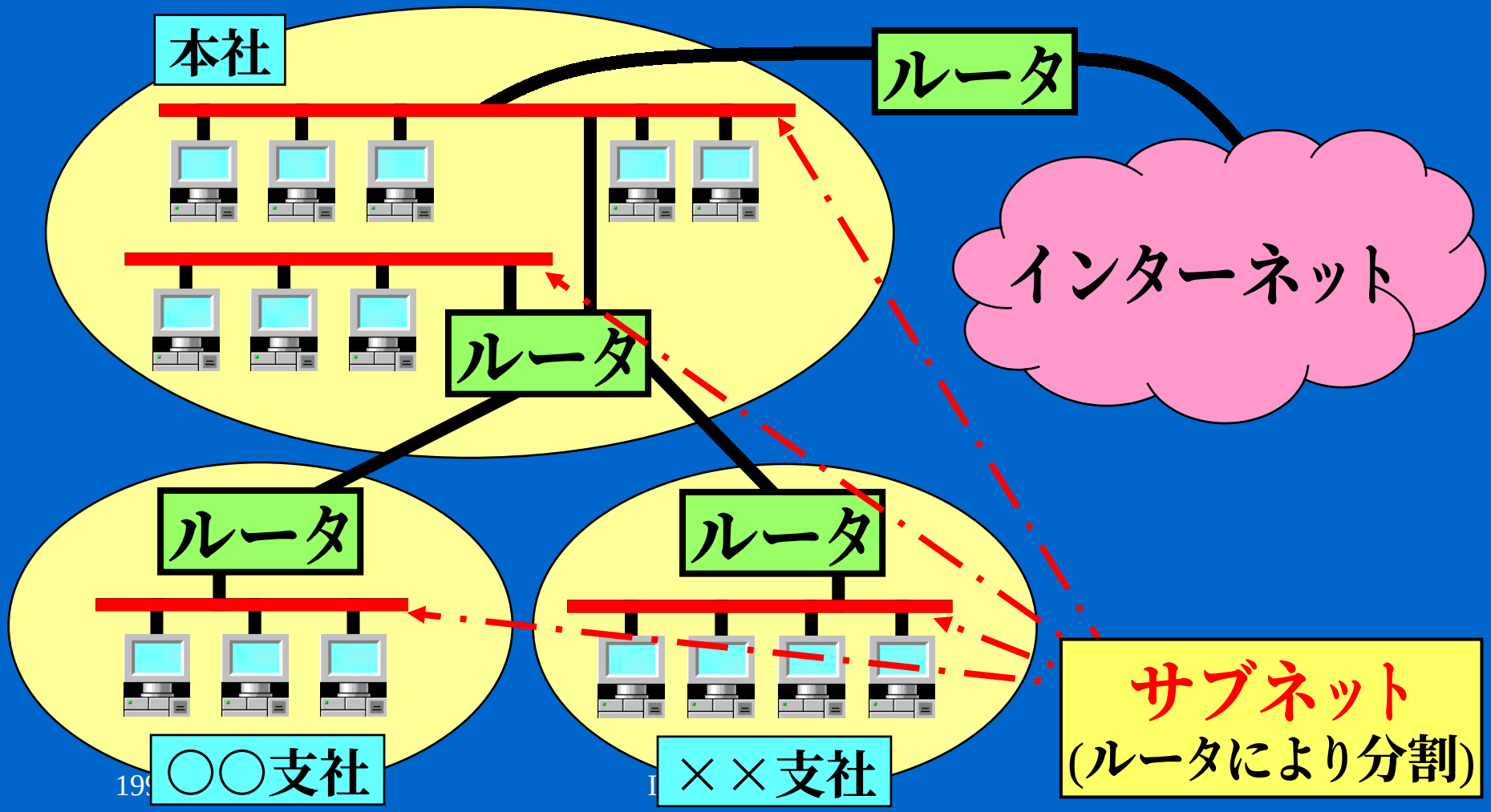
IPアドレス(5)

- サブネット
- 特別なIPアドレス

サブネット

- 一つのネットワークを、複数のネットワークに再分割して使用する技術
- これにより、一つの組織内においてネットワークをより細かく分割できる
- 管理部署毎に分割する等の手法が可能
- 組織内においても、CIDRによる効率のよい管理を行うことが望ましい

サブネットの例



特別なIPアドレス

- 自分自身を表すアドレス
- ネットワークを表すアドレス
- ブロードキャストアドレス

自分自身を表すアドレス

- 127.0.0.1(127.0.0.1/32)
- **ループバックアドレス**
- **ソフトウェアのテスト等の際に有効**

ネットワークを表すアドレス

- IPアドレスのホスト部のビットがすべて0
- マシンには割り当てない
- ネットワークそのものを表し、経路制御の際などに利用される
- ネットワークを複数のサブネットに分割した場合には、それぞれのサブネットについてそれぞれ一つずつ割り当てられる

ブロードキャストアドレス

- IPアドレスのホスト部のビットがすべて1
- その(サブ)ネットワークに接続されているすべてのマシンを表す
- ネットワークを表すアドレスと同様、それぞれのサブネットについてそれぞれ一つずつ割り当てられる
- 同報通信に使用

アドレス割り当ての実際

- 動的な割り当て(自動)
  - ダイヤルアップ接続した際にプロバイダから割り当て
  - LANに接続した際にサーバから割り当て
- 静的な割り当て(手動)
  - 常時接続する際にプロバイダから割り当て
  - LANにサーバを接続する際に割り当て
- 自動で割り当てる際に、接続形態に応じてDHCP、PPP等のプロトコルが用いられる

DNS(1)概要

- DNSとは
- なぜDNSが必要か
- HOSTS.TXTからDNSへ
- DNSの特徴

DNSとは

- Domain Name Systemの略称
- ドメイン名を階層的に管理するためのしくみ
- ドメイン名とIPアドレスを結びつけるためのしくみ

なぜDNSが必要か

- 以前(1980年代まで)、インターネット接続ホストはHOSTS.TXTというファイルで管理
- HOSTS.TXTにはすべての接続ホストの名前とIPアドレスを記述
- 接続した組織は、HOSTS.TXTを定期的にFTP等で入手

HOSTS.TXTからDNSへ

- 接続ホストの増加
- データベースの巨大化
- 変更履歴の即時反映が困難
- 自動更新、分散型データベースへの移行の必要性

à DNS(RFC882, RFC883)の誕生

- 現在ではRFC1034とRFC1035に更新

DNSの特徴

- 複数のホストにより管理
- 自動的に更新される分散型データベース
- 階層構造(木構造)を持つ
- 「名前空間」と呼ばれている

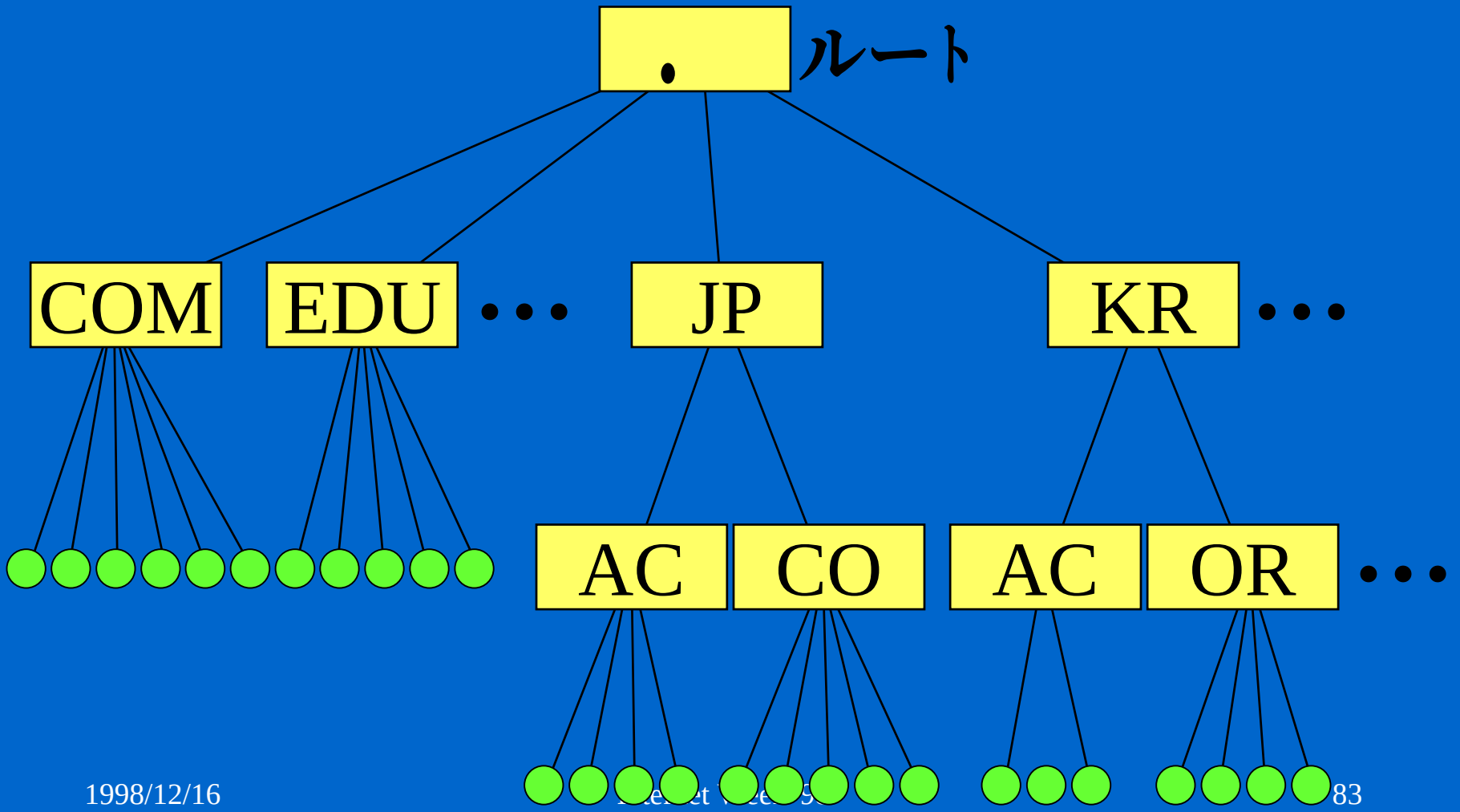
DNS(2)DNSのしくみ

- ネームサーバとリゾルバ
- DNSにおける木構造
- ルートサーバ
- 名前解決の流れ
- ルートサーバの重要性

ネームサーバとリゾルバ

- ネームサーバ: DNSのサーバ機能
  - リゾルバからの要求により名前空間の検索を行い、結果をリゾルバに渡す
- リゾルバ: DNSのクライアント機能
  - WWWブラウザ等のアプリケーションから呼び出され、ネームサーバに名前解決を要求するためのプログラム

DNSにおける木構造



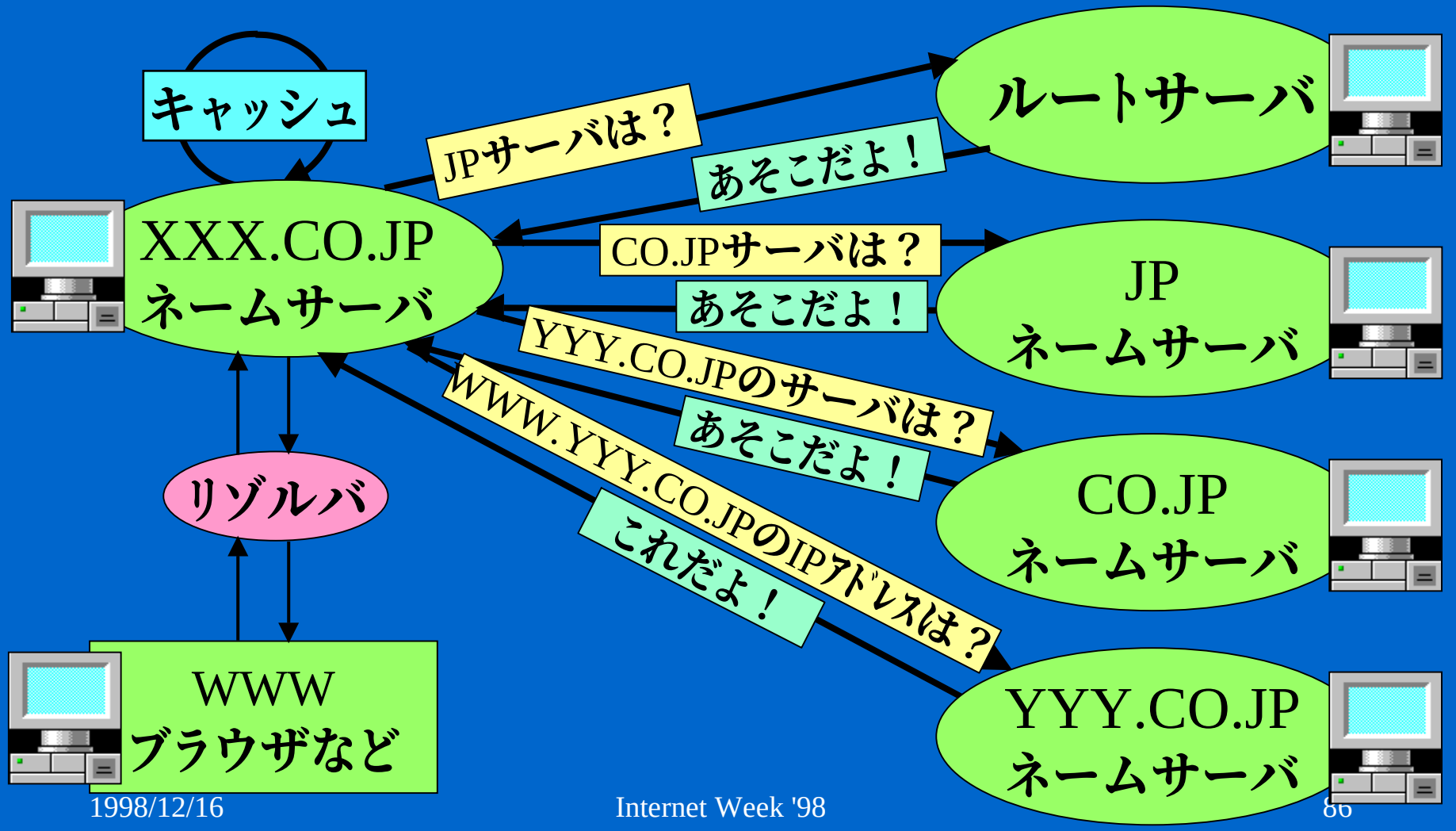
DNSにおける木構造

- 最上位にルート(.)ゾーンを持つ
- ルートゾーンはルートサーバにより管理される
- 各ゾーンのネームサーバは、一つ上位のサーバから指し示される
- ドメイン名の木構造に相当

ルートサーバ

- ルートゾーンを管理しているネームサーバ
- 全世界に13個
  - a.root-servers.net〜m.root-servers.net
- 日本にも1つある
  - m.root-servers.net
  - NSPIXP2に接続
  - WIDE Projectで管理・運用

名前解決の流れ


キャッシュ
JPサーバは？
あそこだよ！
ルートサーバ
XXX.CO.JP
ネームサーバ
CO.JPサーバは？
あそこだよ！
JP
ネームサーバ
YYY.CO.JPのサーバは？
あそこだよ！
WWW.YYY.CO.JPのIPｱﾄﾞﾚｽは？
これだよ！
CO.JP
ネームサーバ
リゾルバ
WWW
ブラウザなど
YYY.CO.JP
ネームサーバ

名前解決の流れ

- まず自分が「知っている」名前かどうか調べる
- 知らなければ、ルートサーバに問い合わせる
- ルートサーバは、一つ下位のサーバの場所(IPアドレス)を返す
- ネームサーバは、そのサーバに問い合わせる
- 以下順に各サーバに問い合わせることで、最終的に目的のIPアドレスを得る

ルートサーバの重要性

- DNSでは自分が解決できない名前の場合、必ずルートサーバに問い合わせる
- すなわち、最低1台のルートサーバへの到達性は保証されていなければならない
- m.root-servers.netが日本にない頃は、海外リンクがダウンするとルートサーバへの到達性が失われていた

DNS(3)
ドメイン名/IPアドレスとDNS

- ゾーンとドメイン名
- ネームサーバの重要性
- プライマリサーバとセカンダリサーバ
- 正引きと逆引き
- 逆引きのしくみ

ゾーンとドメイン名

- それぞれのドメインの階層毎にゾーンを設定
- nic.ad.jpゾーンの管理は、nic.ad.jpドメインのネームサーバにより行われる
- 逆に、nic.ad.jpドメインのネームサーバで管理される領域を、nic.ad.jpゾーンと呼ぶという定義も可能

ネームサーバの重要性

- 該当する組織(ゾーン)のネームサーバにアクセスできなかった場合、たとえその組織のWWWサーバ等が動作していても、WWWブラウザ等から利用できない

à つながらない

- このような状況を防ぐため、通常一つのゾーンについて複数のネームサーバを設定することが多い

プライマリサーバとセカンダリサーバ

- 複数のサーバを設置する場合、データの一意性を保つ必要がある
- 元データは1台のサーバで管理
  - プライマリサーバ
- 他のサーバはプライマリサーバのデータを定期的に複製
  - セカンダリサーバ
- セカンダリサーバは複数設定可能

正引きと逆引き

- 正引き:ドメイン名からIPアドレスを得ること
  - 主にサービスを利用する場合に使用される

à　www.nic.ad.jp⇒202.12.30.134

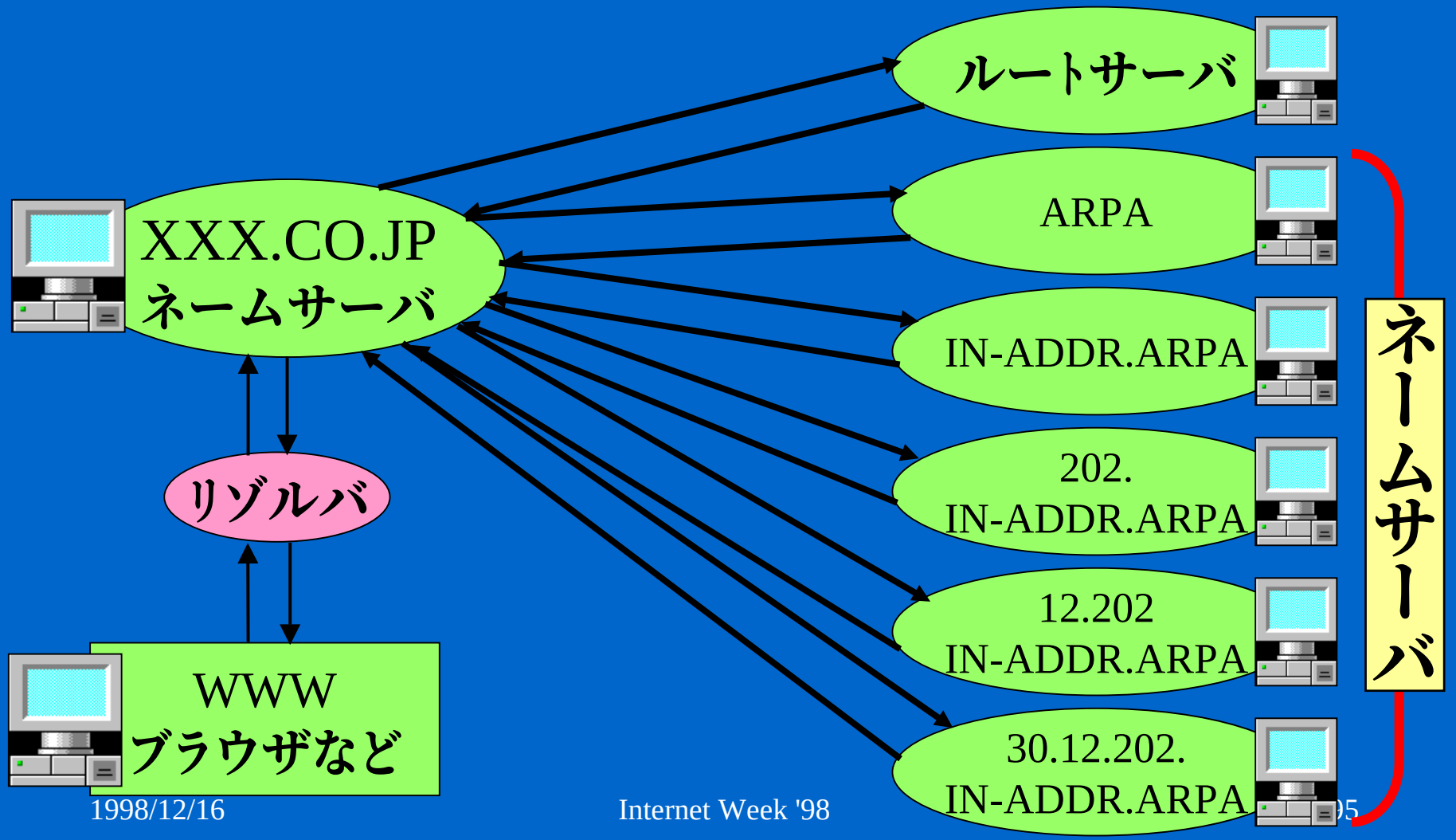
- 逆引き:IPアドレスからドメイン名を得ること
  - 主にサービスを提供する側で、統計情報等を作成する際に使用される

à　202.12.30.33⇒ns1.nic.ad.jp

逆引きのしくみ

- “in-addr.arpa”という特殊なドメイン名を使用
- 例えば202.12.30.134というIPアドレスを逆引きする場合、“134.30.12.202.in-addr.arpa”というドメイン名に対して問い合わせが行われる
- つまり、必ずルートサーバが参照されることに注意

逆引きのしくみ


ルートサーバ
ARPA
IN-ADDR.ARPA
202.
IN-ADDR.ARPA
12.202
IN-ADDR.ARPA
30.12.202.
IN-ADDR.ARPA
ネームサーバ
XXX.CO.JP
ネームサーバ
リゾルバ
WWW
ブラウザなど

DNS(4)
より効果的なDNSの利用

- 別名(CNAME)の指定
- メールホスト(MX)の指定
- BIND

別名(CNAME)の指定

- DNSでは特定のホスト名に対する別名(Canonical Name)を指定することも可能
- 別名を適切に利用することにより、サーバホストの切り替えや更新の際のスムーズな移行が可能
- 別名は“CNAME”レコードにより指定される
- “名前⇒正式名⇒そのホストのIPアドレス”の順で変換される

à ftp.nic.ad.jp⇒mw134.nic.ad.jp⇒202.12.30.134

メールホスト(MX)の指定

- 特定のドメイン名のメールを取り扱うためのホスト(メールホスト)を指定
- あるドメインのメールを特定のホストに集めることが可能
- メールホストは“MX”レコードにより指定
  - MX:Mail Exchanger
- メールホストを複数指定することにより、より安定したサービスを実現することが可能

BIND

- Berkeley Internet Name Domainの略称
- 最も広く利用されているDNSの実装の一つ
- 各種UNIXおよびWindows NTで動作
- 無償で利用可能
- ソースコードを公開
- 現在の最新版: 8.1.2
- URL: ftp://ftp.isc.org/isc/bind/ (オリジナル)

質疑応答