

IPアドレスとドメイン (初級)

相原 玲二

広島大学 総合情報処理センター

Internet Week '97

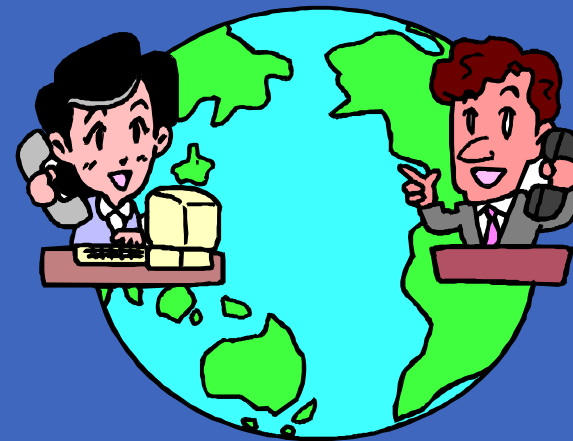
目的

- IPアドレス、ドメイン名、DNS がどういう仕組みになっているかについてやさしく解説
- インターネットの仕組みを知って、これから管理者をめざそうとする方が対象



概要

- IPアドレス
- ドメイン名
- DNSの概要と設定
- 各種申請手続き
- 質疑応答

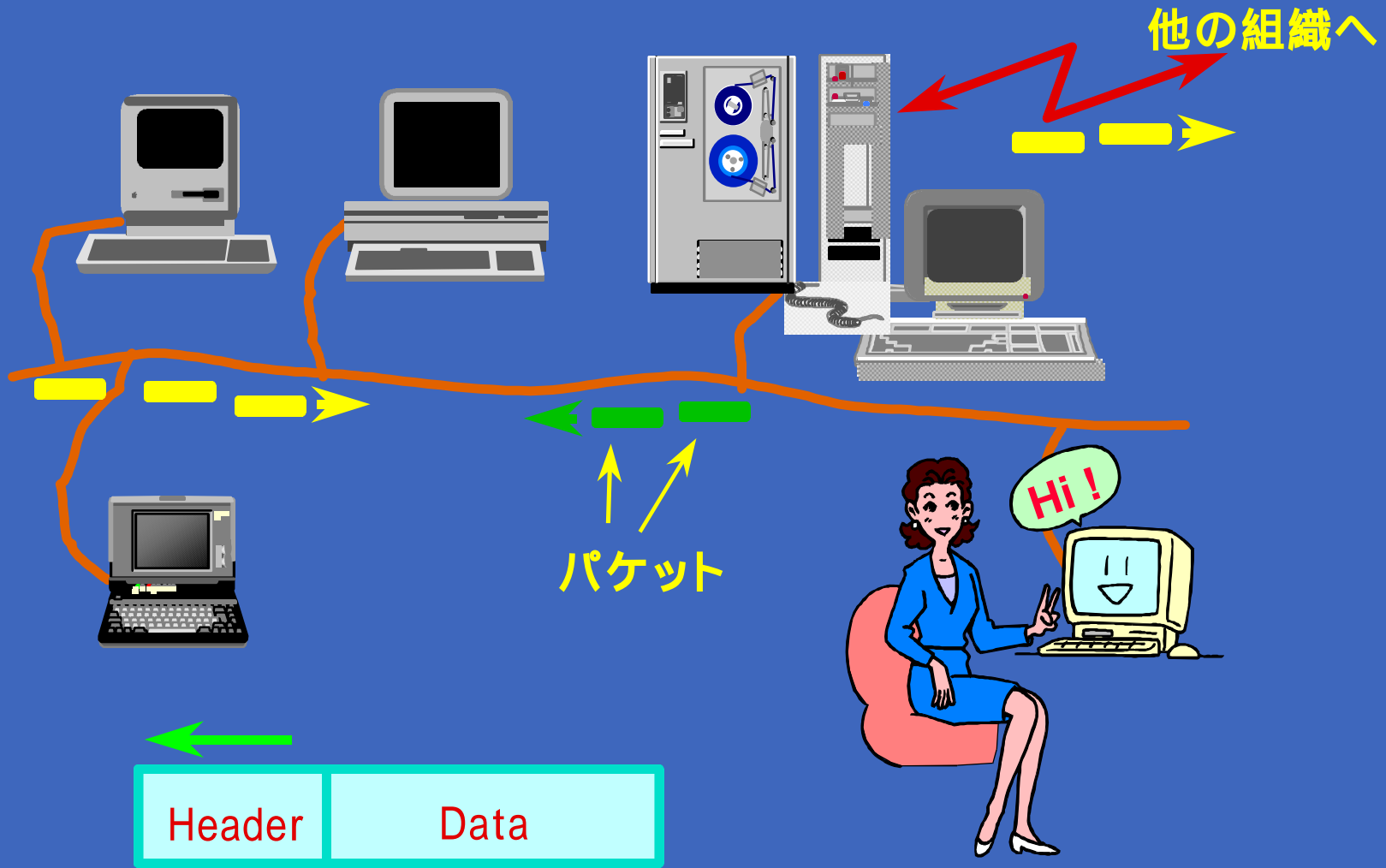


IPアドレス

- IPアドレスはなぜ必要
 - インターネットはパケットによる通信
 - 宛先 送主の表示 識別
- IPアドレスの種類と形式 (IPv4)
- IPアドレスとレーティング
- CIDR
- IPアドレスの今後 (IPv6)

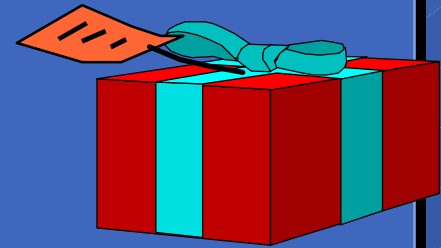
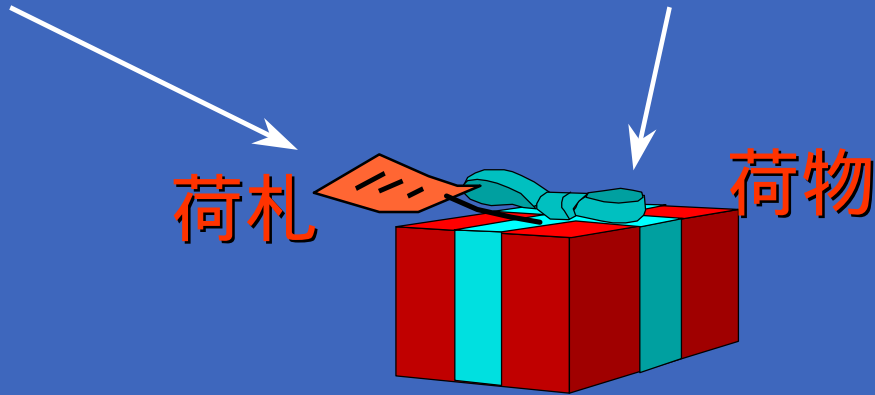
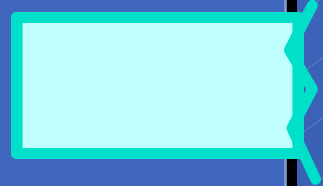


パケットによるデータ通信



パケットとIPアドレス

← ~ 1500 バイト →



宛先 送主の表示 → IPアドレス

(例) 133.41.4.2
165.242.40.33

IPアドレスによる指定

■ コンピュータを指定

リモートログイン

```
% telnet 133.41.4.2
```

ファイル転送

```
% ftp 165.242.40.33
```

0 ~ 255 の数値が
ドットで区切られ
4つ並ぶ

IPアドレス形式 (IPv4)

2進数表現

- Class A アドレス (1.0.0.0 - 127.255.255.255)



- Class B アドレス (128.0.0.0 - 191.255.255.255)



- Class C アドレス (192.0.0.0 - 223.255.255.255)



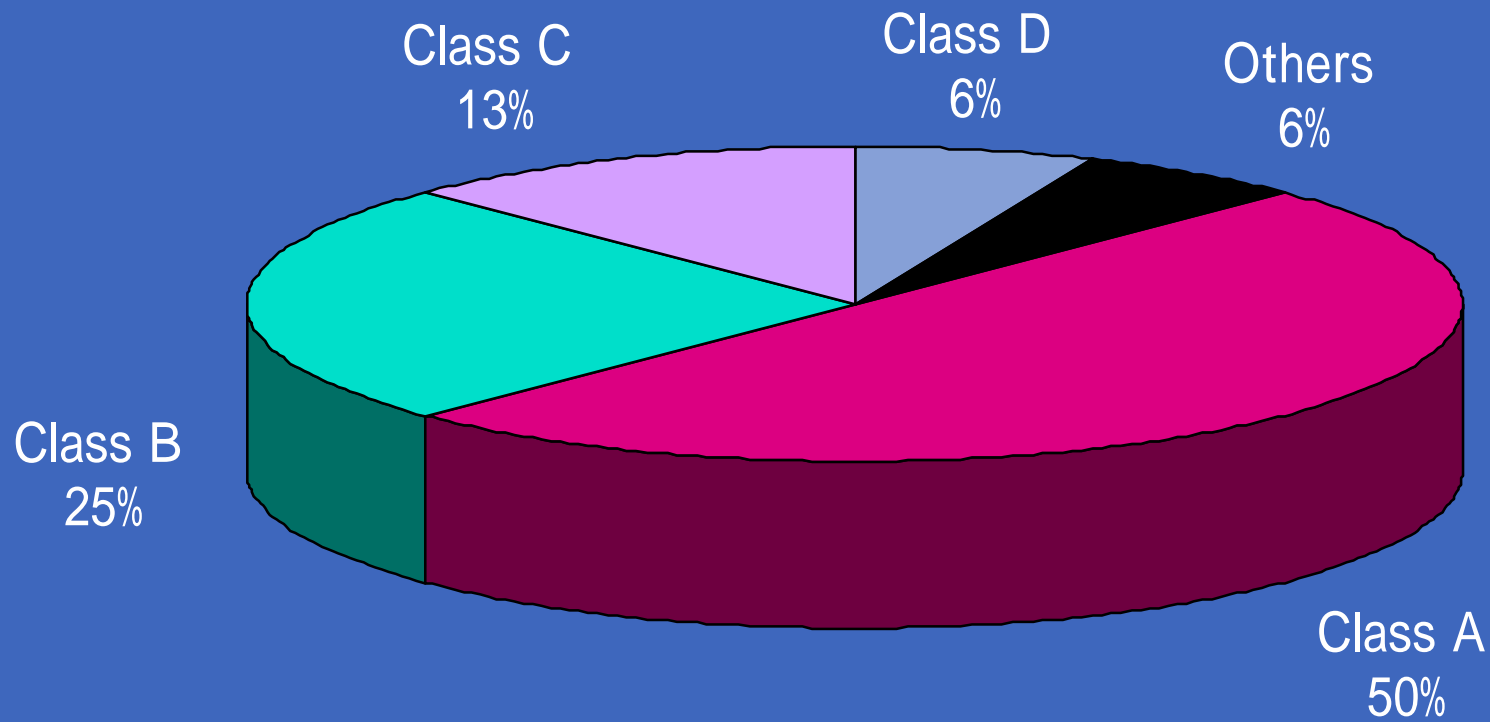
- Class D アドレス (224.0.0.0 - 239.255.255.255)



IPアドレスで表現できる数

- Class A (大規模ネットワーク)
 - host: 16,777,216 network: 128
- Class B (中規模ネットワーク)
 - host: 65,536 network: 16,384
- Class C (小規模ネットワーク)
 - host: 256 network: 2,097,152

IPアドレス空間

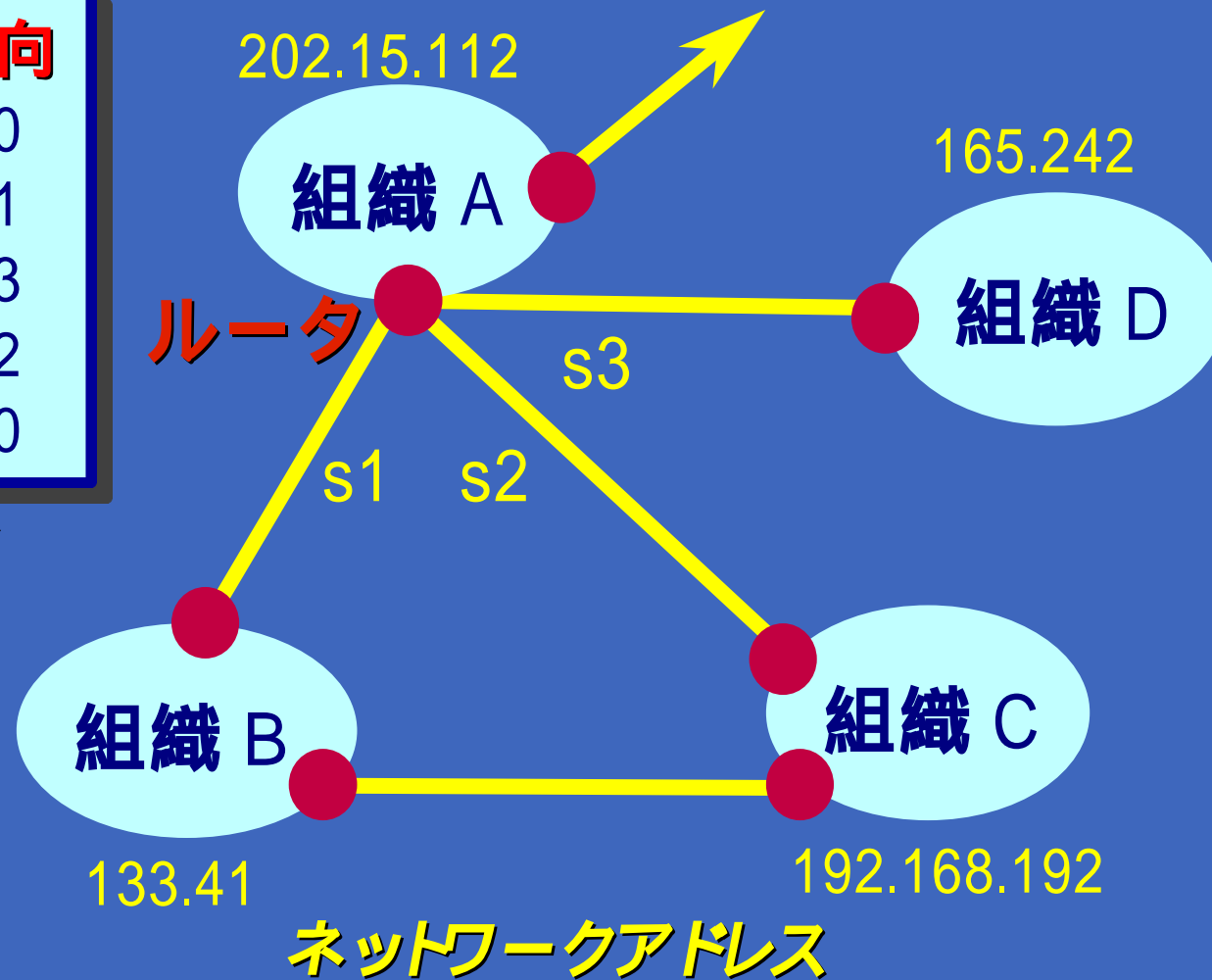


全アドレス数: $2^{32} = 4,294,967,296$

ルーティング

| 宛先 | 方向 |
|-------------|----|
| 202.15.112 | e0 |
| 133.41 | s1 |
| 165.242 | s3 |
| 192.168.192 | s2 |
| default | e0 |

ルーティング
テーブル



IPアドレスの付与

- ネットワークアドレス
 - IPアドレスのネットワーク部分のみ
 - 経路を決めるために使用される
- ホストアドレス
 - ネットワーク部 + ホスト部 (全部)
 - すべてのネットワーク接続機器に付与
 - » コンピュータ、PC、ルータ、ネットワークプリンタ等
 - 複数のインターフェースにもそれぞれ付与

組織内ルーティング

■ サブネット

- 組織内で幾つかのネットワークを構成
- 組織外からは 1つのネットワークとして見える

組織アドレス
133.41.0.0

サブネット

133.41.4.0

133.41.5.0

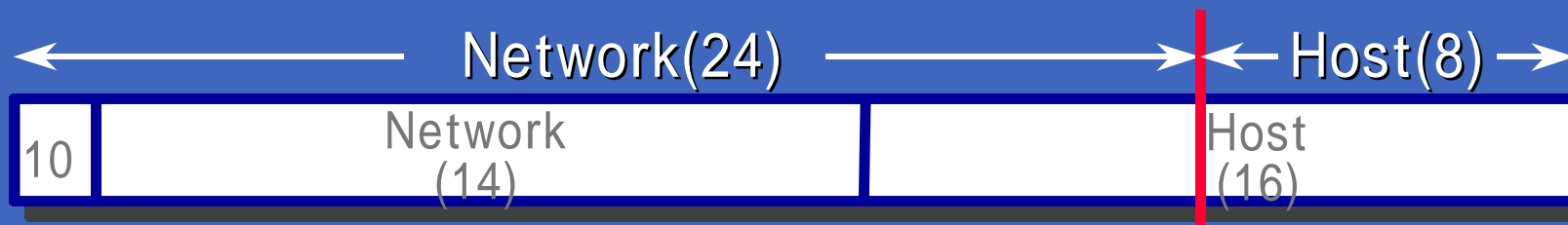
133.41.6.0

133.41.7.0

サブネットマスク

■ 組織内ネットワーク部を指定

- 202.15.112.0 mask 255.255.255.240
- 133.41.0.0 mask 255.255.255.0



■ 可変長サブネットマスク (VLSM)

- サブネットごとにサブネットマスク長を設定
- 経路情報交換プロトコルが対応する必要あり

IPアドレスの問題点

- 32bit アドレスの限界
 - 40億個では1人1ホストに対応できない
 - IPv4 設計時点では妥当な選択だった
- Class の制約による非効率な割当て

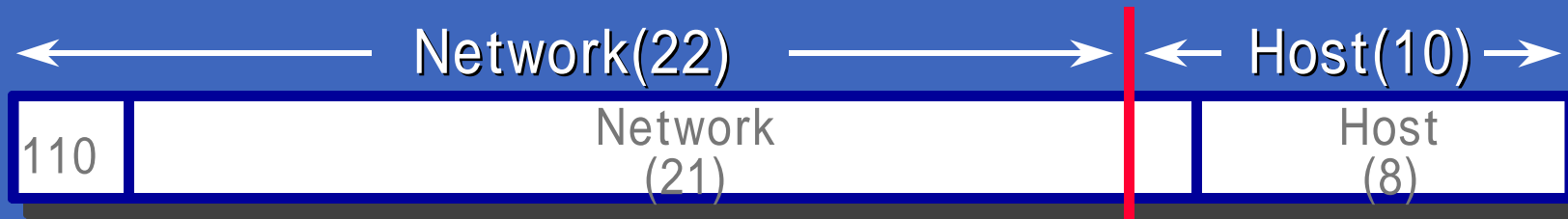


短期的対策 :CIDR

中長期的対策 :IPv6

CIDR: Classless Inter-Domain Routing

- ネットワーク部とホスト部の境界を指定
 - 133.41.0.0 / 16 Class B
 - 202.15.112.0 / 24 Class C
 - 202.15.112.0 / 22

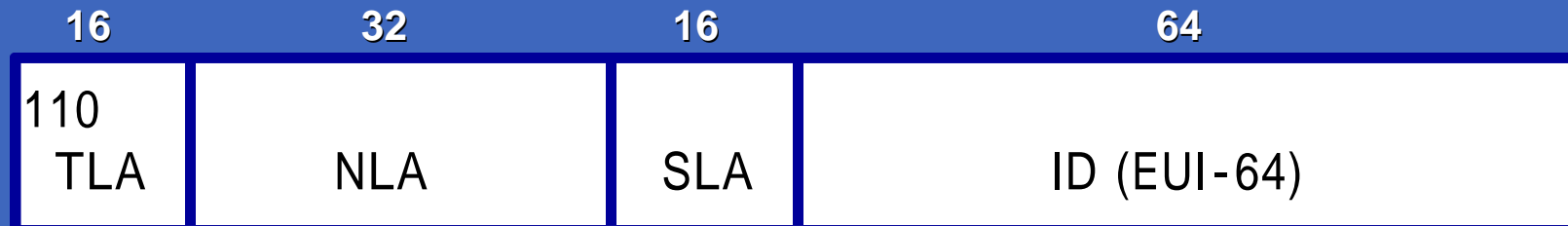


- CIDR 組織間ルーティングで使用可能
 - サブネット 組織内ルーティング、Class あり

CIDR: Classless Inter-Domain Routing

- IPアドレスの効率的利用
 - Class を使用しない
 - 例 : 202.15.112.0 / 22 (112 ~ 115)
- 経路情報削減
 - 経路情報を集約してアナウンス可能
 - 例 : 202.15.64.0 / 18 (64 ~ 127)
- CIDRブロック
 - IPアドレスのうち**2のべき乗**ごとの固まり

IPアドレス形式 (IPv6)



■ 128bit アドレス

- 上位 64bit : 経路制御に使用
 - » TLA(16) + NLA(32) + SLA(16)
- 下位 64bit : ホスト識別に使用
 - » EUI-64 (MAC 48bit)

■ 各種アドレス

- リンクローカル、サイトローカル、グローバル

ドメイン名

- ドメイン名はなぜ必要
 - 相手コンピュータの指定
 - 電子メールのアドレス
 - WWWのURL
- ドメイン名空間の構造
- トップレベルドメイン (TLD)



ドメイン名による指定

■ コンピュータを指定

リモートログイン

```
% telnet ns.hiroshima-u.ac.jp
```

ファイル転送

```
% ftp mail.ipc.hiroshima-cu.ac.jp
```

英数字、ハイフンが
ドットで区切られ
任意の数並ぶ

電子メールのアドレス

- あるコンピュータ上のあるユーザを指定

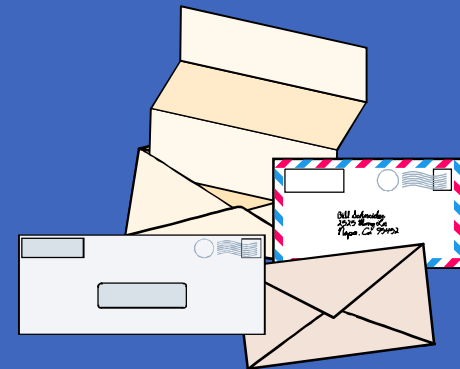
ray@ipc.hiroshima-u.ac.jp



ユーザ名



ドメイン名



WWWのURL

- あるコンピュータ上のある資源（ファイル等）を、通信手順と共に指定
 - URL: Uniform Resource Locator

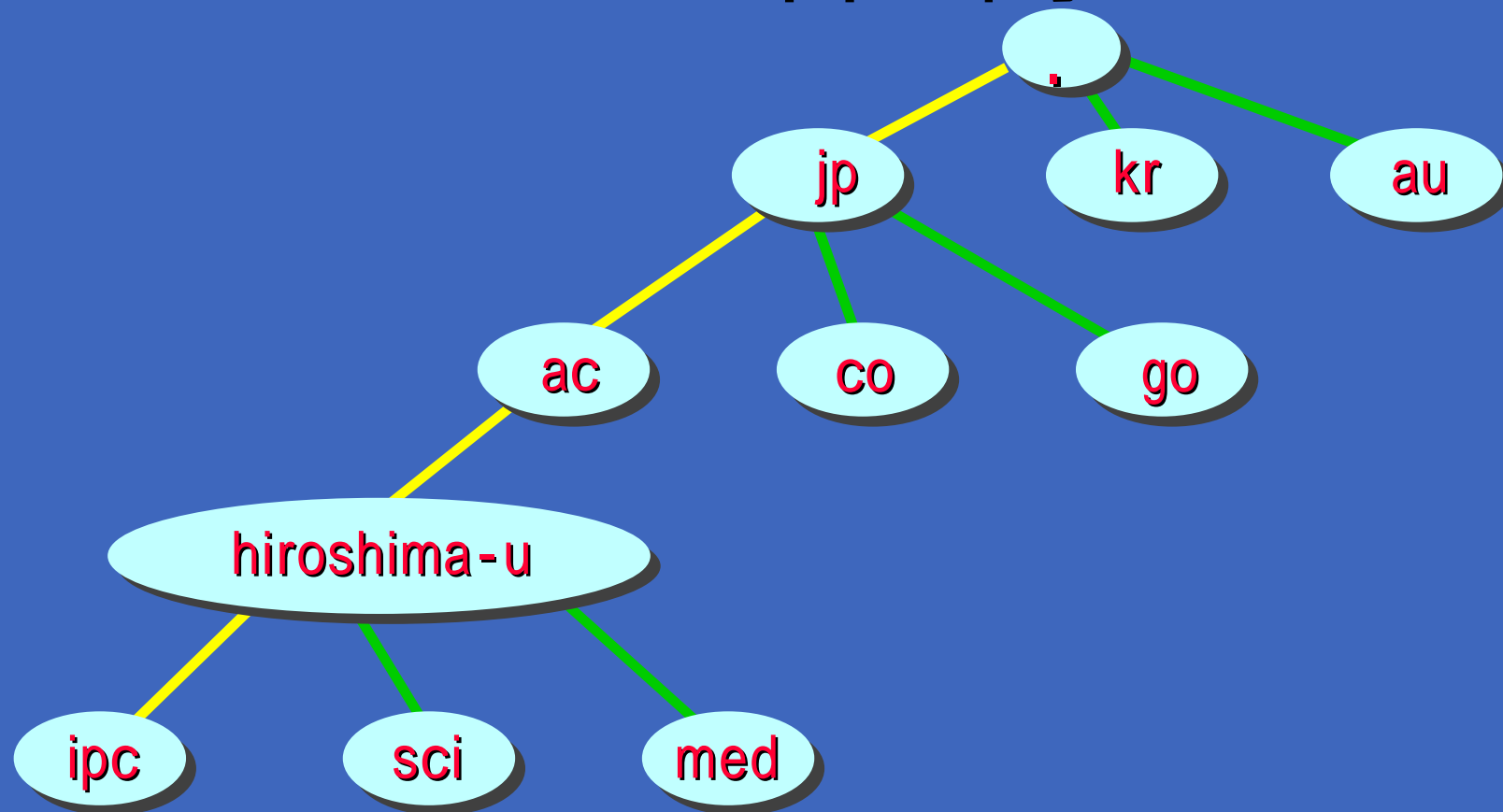
http://www.ipc.hiroshima-u.ac.jp/ipc/

↑
プロトコル名

↑
ドメイン名

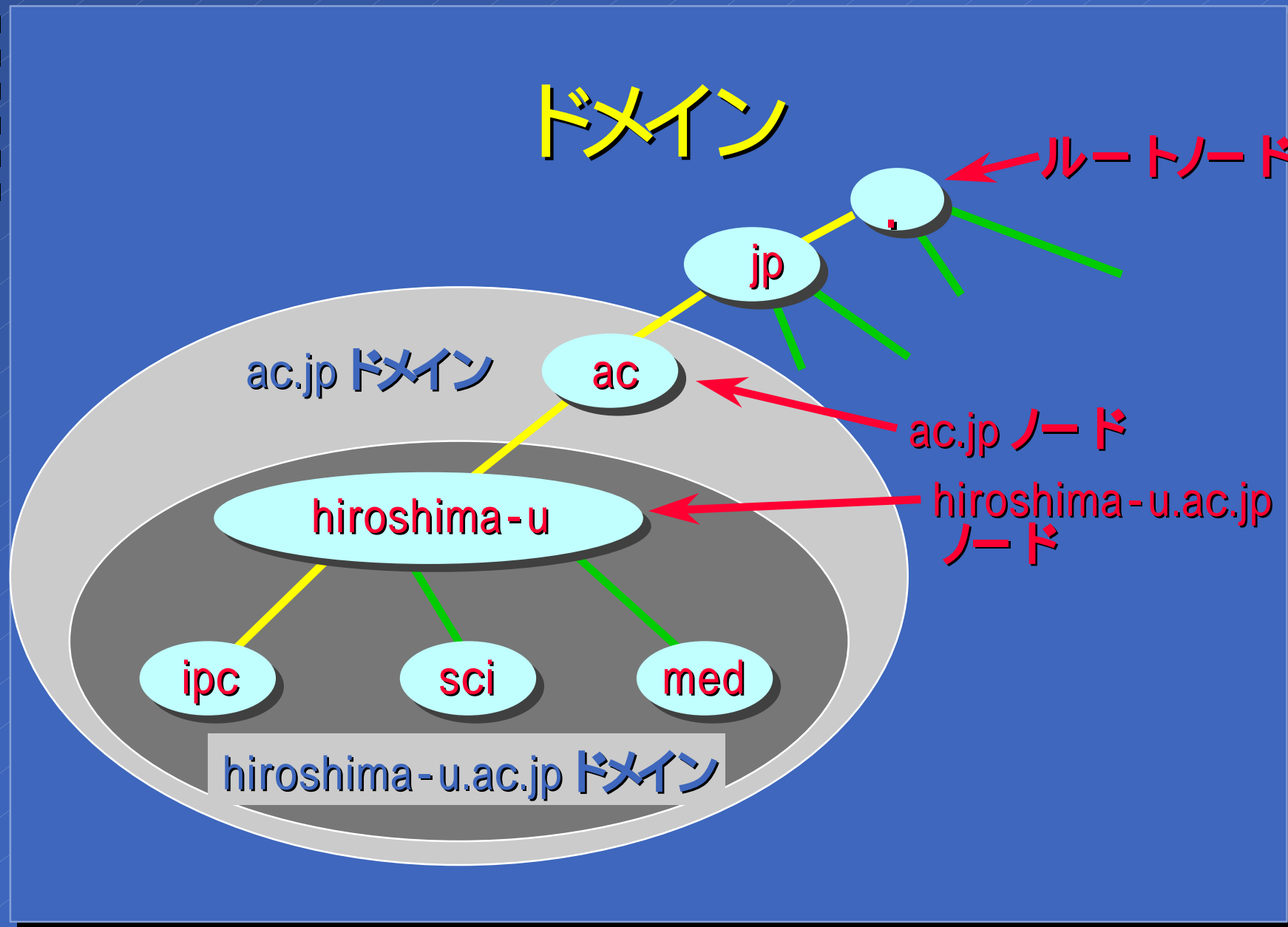
↑
パス名

ドメイン名空間



ipc.hiroshima-u.ac.jp : FQDN (fully-qualified domain name)

ドメイン



ドメインとホストの関係

- ドメインはドメイン名空間のサブツリー
- ホストもドメインの一種
 - ホストはIPアドレスを持つドメイン
 - ツリーのリーフの場合が多い (例外あり)

| ホスト | IPアドレス |
|--------------------------|--------------|
| ipc.hiroshima-u.ac.jp | 133.41.16.10 |
| ws.ipc.hiroshima-u.ac.jp | 133.41.17.20 |
| pc.ipc.hiroshima-u.ac.jp | 133.41.17.21 |

トップレベルドメイン (TLD)

- ルートノードへ直接接するドメイン
 - 第1レベルドメイン
- 国別コード (ISO 3166)
 - JP, KR, AU, US, ... (UKは例外)
- gTLD (<http://www.iahc.org/draft-iahc-recommend-00.html>)
 - COM, ORG, NET, FIRM, STORE, WEB, ...
- その他
 - INT, EDU, GOV, MIL, ...

DNSの概要と設定

- DNS (Domain Name System) とは
- ドメインとゾーン、権限と権限の委任
- プライマリサーバ、セカンダリサーバ
- IPアドレスからドメイン名を検索 (逆引き)
- ネームサーバの設定
- クライアントの設定



DNS: Domain Name System

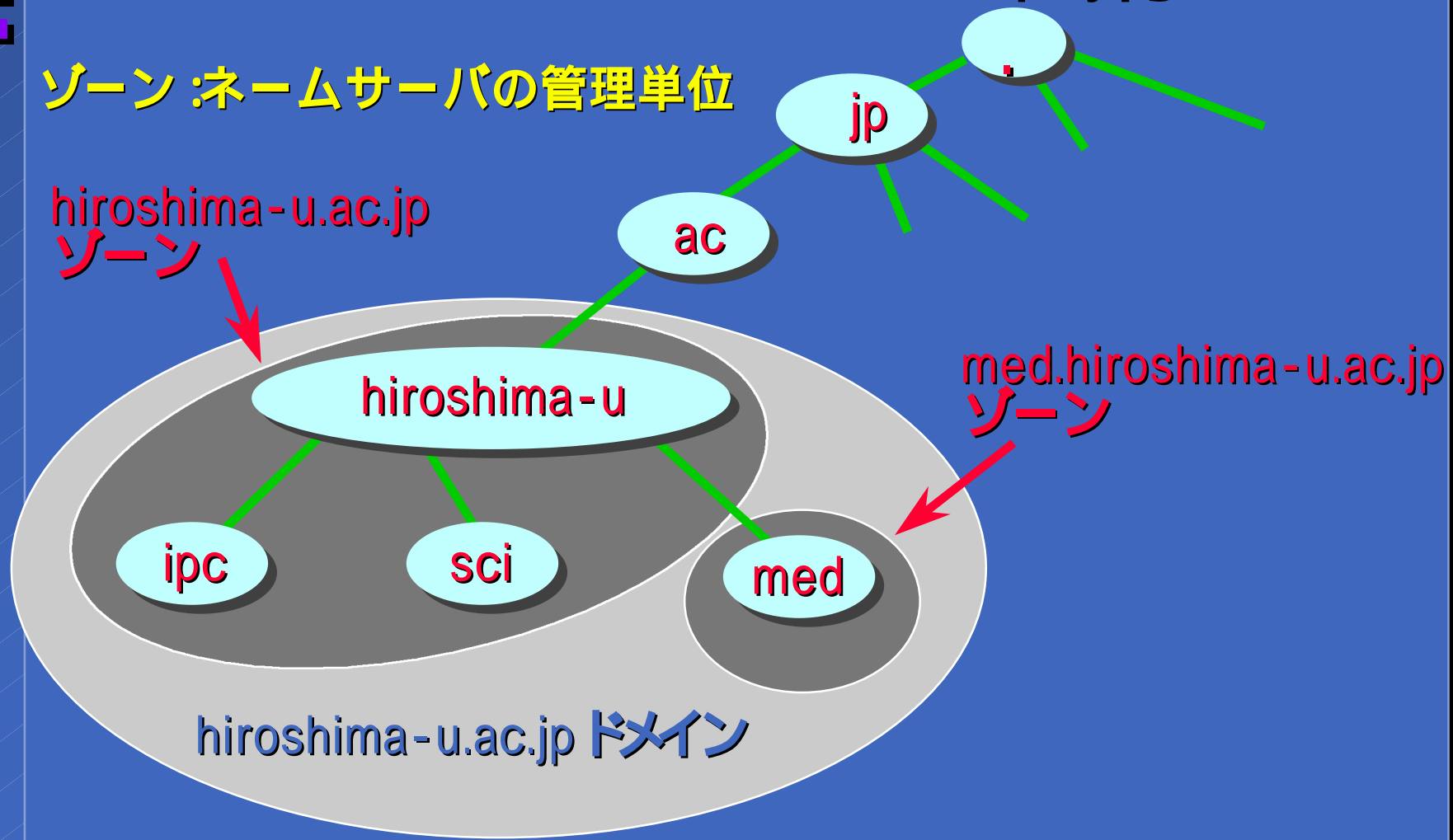
- ドメイン名から各種情報を検索
- 分散データベース
 - データ各部は、それぞれローカルで管理
 - ネットワーク上のどこからでも参照可能
- 歴史
 - ARPANET時代のHOSTS.TXT (SRI-NIC)
 - 問題点 : 負荷集中、名前の衝突、一貫性等
 - 仕様 : RFC882, 883 RFC1034, 1035

BINDとネームサーバ

- **BIND** :Berkeley Internet Name Domain
 - DNSを実現するプログラムの一つ
 - 最新バージョン :8.1.1 (または 4.9.6)
- **ネームサーバ** :DNSのサーバ機能
 - ドメイン名空間の情報を持つプログラム
 - **ゾーン** :ネームサーバの管理単位
- **リゾルバ** :DNSのクライアント機能

ドメインとゾーンの関係

ゾーン : ネームサーバの管理単位



権限と権限の委任

- **権限** :あるゾーン情報の提供を公式に認められること
 - 上位ゾーンの権限を持つサーバから権限の委任を受ける
- **権限の委任** :ドメインの一部の権限を別のサーバへ移すこと
 - 委任するサーバは該当ドメインに対応するゾーンの権限を持っている必要がある

ネームサーバの種類

■ プライマリサーバ

- 権限を持つゾーンの情報をローカルファイルから読み込み、情報提供するネームサーバ

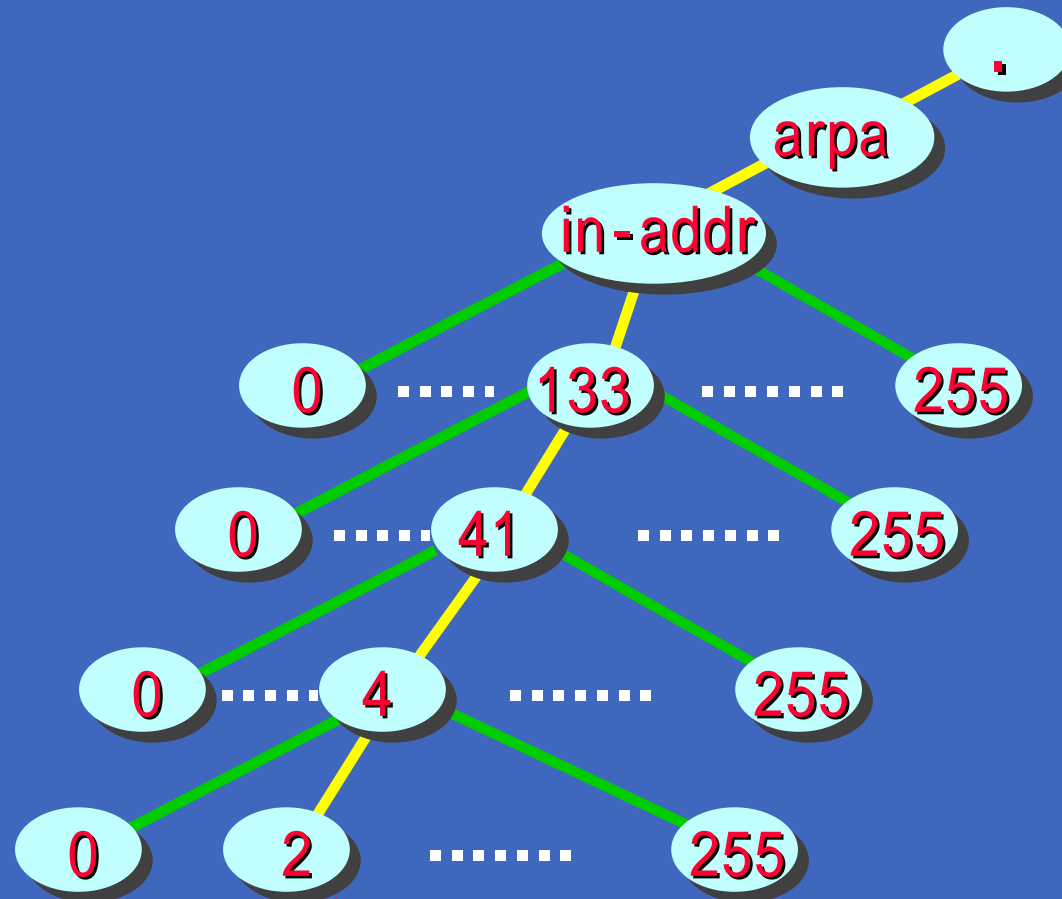
■ セカンダリサーバ

- 権限を持つゾーンの情報をプライマリサーバからコピーし、情報提供するネームサーバ
- 起動時および定期的にコピー
- サーバマシンの故障に対応できる

IPアドレスからドメイン名を検索

- DNSの仕組みをそのまま利用
- IPアドレスの名前空間を作る
 - IPアドレス A.B.C.D
名前空間 D.C.B.A.in-addr.arpa
 - 例 133.41.4.2 2.4.41.133.in-addr.arpa
- **逆引き** :IPアドレスからドメイン名を検索

in-addr.arpa 空間

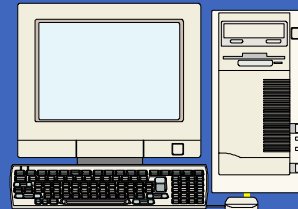
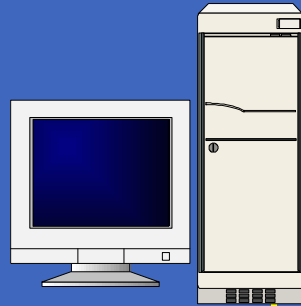


ホスト名 `ns.hiroshima-u.ac.jp`

ネットワーク構成例

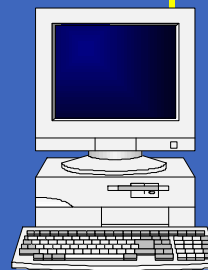
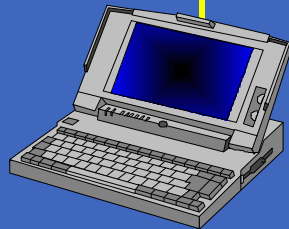
プライマリネームサーバ
ns.iw97.co.jp
202.15.115.2

セカンダリネームサーバ
ws.iw97.co.jp
202.15.115.3



ドメイン : iw97.co.jp
IP : 202.15.115.0 / 24

クライアント

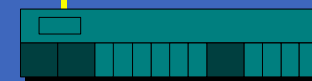


pc1.iw97.co.jp
202.15.115.11

pc2.iw97.co.jp
202.15.115.12

ルータ

gw.iw97.co.jp
202.15.115.1



プロバイダへ

ネームサーバを動作させるには

■ 必須条件

- 24時間運転
- セカンダリサーバ

■ 推奨条件

- 最新のBINDまたは同等の機能が動作
 - » セキュリティー上の問題等にすばやく対応
- よく管理されていること
 - » ネームサーバは攻撃を受けやすい

BINDの入手とインストール

- ソースコード公開 (無償で利用可能)
 - <ftp://ftp.isc.org/isc/bind/src/> (original)
 - 多くのftpサーバでミラーされているので、**最寄りのサーバから取得**すること
 - RingServer FTPサイトの場合のpath:
`/pub/net/iij/isc/bind/src/`
- インストール
 - 機種・OSに依存 (付属のドキュメント参照)

BIND設定の概要 (4.9.6)

- 起動ファイルの作成
- 資源レコードファイルの作成
 - 正引き用ファイル (ドメイン名 IPアドレス等)
 - 逆引き用ファイル (IPアドレス ドメイン名)
 - ローカルホスト用ファイル
 - ルートキャッシュファイル
- クライアントの設定
- ネームサーバの起動、動作確認

起動ファイルの例

■ /etc/named.boot

| | | |
|------------------|--------------------------------|-----------------------|
| directory | /etc/ns | |
| primary | iw97.co.jp | iw97.zone |
| primary | 115.15.202.in-addr.arpa | 202.15.115.rev |
| primary | localhost | localhost.zone |
| primary | 0.0.127.in-addr.arpa | localhost.rev |
| cache | . | named.root |

正引き用ファイルの例

```
; iw97.zone: zone file for iw97.co.jp
iw97.co.jp.      IN  SOA  ns.iw97.co.jp. root.iw97.co.jp. (
                    199711020 ; Serial (yyyymmddv)
                    3600      ; Refresh
                    900       ; Retry
                    3600000   ; Expire
                    86400    ) ; Minimum TTL

;
iw97.co.jp.      IN  NS  ns.iw97.co.jp.
iw97.co.jp.      IN  NS  ws.iw97.co.jp.
;
ns.iw97.co.jp.   IN  A  202.15.115.2
ws.iw97.co.jp.   IN  A  202.15.115.3
pc1.iw97.co.jp. IN  A  202.15.115.11
pc2.iw97.co.jp. IN  A  202.15.115.12
```


省略記法

- デフォルトドメイン
 - 起動ファイルで指定されるドメイン名
 - @ により指定可能
- デフォルトドメイン名の付加
 - ドット"." で終わらないドメイン名にはデフォルトドメイン名が付加される
- 直前の名前の繰り返し
 - 名前の指定が省略された場合

省略記法の活用

```
; iw97.zone: zone file for iw97.co.jp  
@          IN SOA ns.iw97.co.jp. root.iw97.co.jp. (  
          199711020 ; Serial (yyyymmddv)  
          3600      ; Refresh  
          900       ; Retry  
          3600000   ; Expire  
          86400    ) ; Minimum TTL  
  
;  
          IN NS ns  
          IN NS ws  
  
;  
ns        IN A 202.15.115.2  
ws        IN A 202.15.115.3  
pc1       IN A 202.15.115.11  
pc2       IN A 202.15.115.12
```

資源レコード (RR)

- SOA (Start of Authority)
 - 資源レコードファイルの先頭に置かれる
 - 資源に関する権限 (Authority) 等の宣言
 - root@iw97.co.jp root.iw97.co.jp.
- NS (Name Server)
 - プライマリおよびセカンダリネームサーバ
- A (Address)
 - ドメイン名 IPアドレス

資源レコード (続き)

- PTR (Pointer)
 - IPアドレス ドメイン名
- MX (Mail eXchanger)
 - Aレコード以外のホストへメールを配送
- CNAME (Canonical NAME)
 - 別名に対する規準名を指定
- HINFO (Host INFOrmation)
 - ハードウェアタイプおよび OS

逆引き用ファイルの例

```
; 202.15.115.rev: rev file for 202.15.115
@           IN SOA ns.iw97.co.jp. root.iw97.co.jp. (
            199711020 ; Serial (yyyymmddv)
            3600      ; Refresh
            900       ; Retry
            3600000   ; Expire
            86400    ) ; Minimum TTL

;
                IN NS ns
                IN NS ws
0              IN PTR iw97net.iw97.co.jp.
2              IN PTR ns.iw97.co.jp.
3              IN PTR ws.iw97.co.jp.
11             IN PTR pc1.iw97.co.jp.
12             IN PTR pc2.iw97.co.jp.
```

ローカルホストファイル (1)

```
; localhost.zone  
@          IN SOA localhost. root.localhost. (  
          1          ; Serial  
          3600       ; Refresh  
          900        ; Retry  
          3600000    ; Expire  
          86400 )    ; Minimum TTL  
  
;  
          IN NS 127.0.0.1  
          IN A 127.0.0.1
```

ローカルホストファイル (2)

```
; localhost.rev  
@          IN SOA localhost. root.localhost. (  
          1          ; Serial  
          3600       ; Refresh  
          900        ; Retry  
          3600000   ; Expire  
          86400 )   ; Minimum TTL  
  
;  
          IN NS localhost.  
0        IN PTR localnet.  
1        IN PTR localhost.
```

ルートキヤツシュ

- ルートドメイン "." の権限を持つサーバの情報を保持
- 最新のファイルを取得
 - ftp://ftp.nic.ad.jp/pub/internet/rs.internic.net/domain/named.root
 - /etc/ns/named.root としてセーブ
- 時々更新されるので注意が必要

クライアントの設定 (BIND)

■ /etc/resolv.conf

```
domain          iw97.co.jp
nameserver      202.15.115.2
nameserver      202.15.115.3
```

クライアントの設定 (Windows)

マイコンピュータ

コントロールパネル

ネットワーク

TCP/IPのプロパティ

DNS設定

TCP/IPのプロパティ

バインド | 詳細設定 | **DNS 設定** | ゲートウェイ | WINS 設定 | IP アドレス

DNS を使わない(L)

DNS を使う(E)

ホスト(H): ドメイン(D):

DNS サーバーの検索順

| | |
|--|-------|
| <input type="text" value=" . . ."/> | 追加(A) |
| <input type="text" value="202.15.115.2 202.15.115.3"/> | 削除(D) |

ドメイン サフィックスの検索順

| | |
|----------------------|-------|
| <input type="text"/> | 追加(A) |
| <input type="text"/> | 削除(D) |

OK キャンセル

DNSとBIND書籍情報

- 「DNS & BIND」 (アスキー出版局)
- 「UNIX Magazine」 (アスキー出版局)
 - UNIX知恵袋 (ネームサーバ) 1997年3～7月号

各種申請手続き

■ IPアドレス申請

- <ftp://ftp.nic.ad.jp/jpnic/ipaddress/ip-addr-guide.txt>

■ JPドメイン名申請

- <ftp://ftp.nic.ad.jp/jpnic/domain/domain-name-all.txt>

■ JPNICが管理するDNS申請

- <ftp://ftp.nic.ad.jp/jpnic/dns/dns-info.txt>

■ JPNICの情報

- <http://www.nic.ad.jp/>