

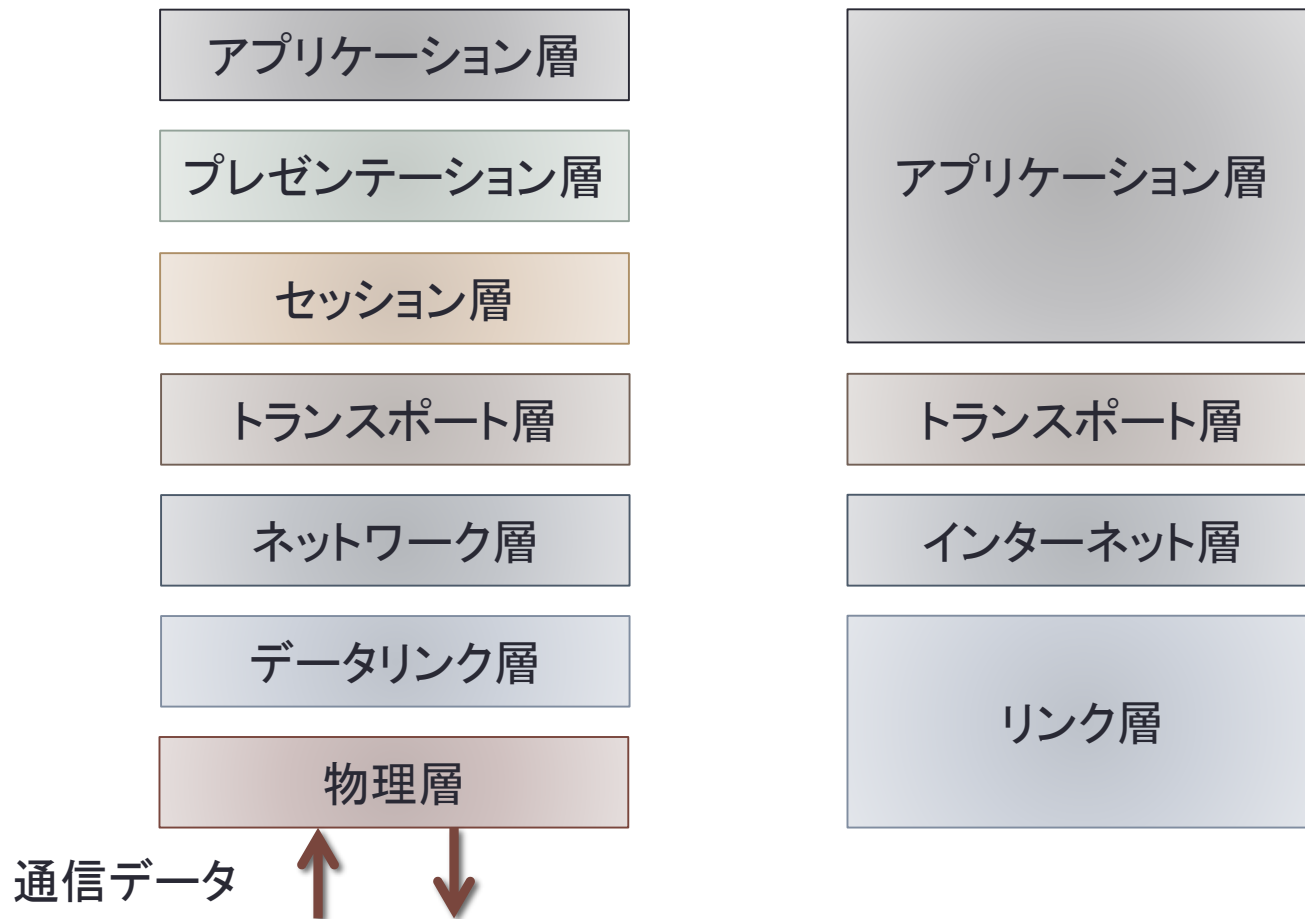
# 情報通信ネットワーク 第8回

---

理工学部情報科学科

松澤 智史

# 本日は……アプリケーション層



# DNS(Domain Name System)

- 名前解決のためのプロトコル
- ドメインネームをIPアドレスに,  
IPアドレスをドメインネームに変換するサービス
- サーバクライアントモデルを使用
- UDP上のプロトコル

# ドメインネーム(FQDN)

- 正確にはFQDN(Fully Qualified Domain Name)という
- FQDNの形式

**www.tus.ac.jp.**

ドット区切りの階層構造になっている

ルートドメイン→jpドメイン→acドメイン→tusドメイン→www(ホスト名)

このFQDNをIPアドレスに、IPアドレスをFQDNに変換するシステムがDNSである

**www.tus.ac.jp. ⇔ 133.31.180.213**

# DNS使用の例

理科大のWebサーバ  
IP:133.31.180.213



④133.31.180.213の  
TCP80番ポートに接続



①Webブラウザで  
www.tus.ac.jpを開く

②DNSのプロトコルに従って  
DNSサーバにwww.tus.ac.jpの  
IPアドレスを問い合わせる

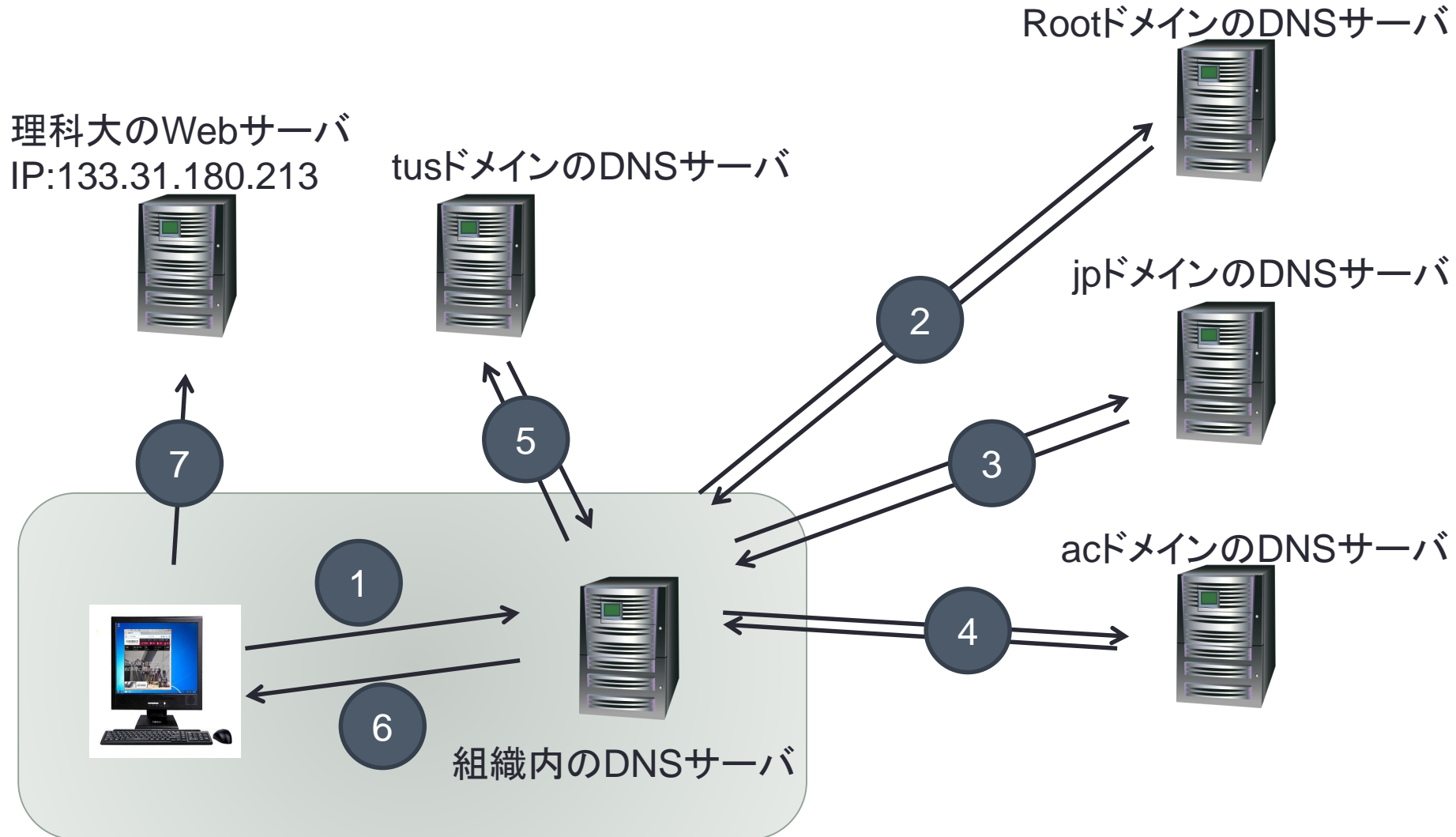
③www.tus.ac.jpの  
IPアドレス133.31.180.213を  
返答する



組織内のDNSサーバ

組織内のDNSサーバは  
すべての問い合わせに  
答えられるのだろうか？

# DNSは実は分散データベース



# DNSは実は分散データベース

## RootメインのDNS

.jp .com .uk .net .edu などの  
DNSサーバのIPアドレスを保持

## jpドメインのDNS

.ac .co .ne などの  
DNSサーバのIPアドレスを保持

## acドメインのDNS

.tus .u-tokyo .keio などの  
DNSサーバのIPアドレスを保持

## tusドメインのDNS

.ed .isなどのDNSサーバのIPアドレス  
wwwやmailなどのホスト名に対応するIPアドレスを保持

# DNSサーバの挙動の種類

- 再帰問い合わせ型

- 自身のデータベースに答えが無い場合は、ルートサーバに問い合わせ、目的の答えが得られるまで階層をたどる探索を行うDNSサーバ
- 階層が深いと問い合わせ処理が増大
- ※先ほどの図の組織内のDNSが該当

- 非再帰問い合わせ型

- 自身のデータベースに答えがない場合知っている情報のみ(下の階層のDNSサーバのIP)答えるサーバ
- どのような問い合わせにも処理は1回
- ※先ほどの図の組織内のDNS以外すべてのDNSが該当



# nslookupを使用して名前解決

```
t-matsu@mail:~$ nslookup www.tus.ac.jp
Server:      133.31.85.17
Address:     133.31.85.17#53  ← 問い合わせたDNSサーバ

Non-authoritative answer:
www.tus.ac.jp  canonical name = tuswap1.tus.ac.jp.
Name:   tuswap1.tus.ac.jp
Address: 133.31.180.213  ← 返答

t-matsu@mail:~$ nslookup 133.31.180.213
Server:      133.31.85.17
Address:     133.31.85.17#53

Non-authoritative answer:
213.180.31.133.in-addr.arpa  name = tuswap1.tus.ac.jp.  ← 返答

Authoritative answers can be found from:
180.31.133.in-addr.arpa nameserver = tusns1.tus.ac.jp.
180.31.133.in-addr.arpa nameserver = tusns.tus.ac.jp.
tusns.tus.ac.jp internet address = 133.31.8.3
tusns1.tus.ac.jp  internet address = 133.31.8.4

t-matsu@mail:~$
```

# nslookupの対話モード

```
t-matsu@mail:~$ nslookup
> www.tus.ac.jp
Server:      133.31.85.17
Address:     133.31.85.17#53

Non-authoritative answer:
www.tus.ac.jp canonical name = tuswap1.tus.ac.jp.
Name:   tuswap1.tus.ac.jp
Address: 133.31.180.213 ← 返答
> 133.31.180.213
Server:      133.31.85.17
Address:     133.31.85.17#53

Non-authoritative answer:
213.180.31.133.in-addr.arpa name = tuswap1.tus.ac.jp. ← 返答

Authoritative answers can be found from:
180.31.133.in-addr.arpa nameserver = tusns.tus.ac.jp.
180.31.133.in-addr.arpa nameserver = tusns1.tus.ac.jp.
tusns.tus.ac.jp internet address = 133.31.8.3
tusns1.tus.ac.jp internet address = 133.31.8.4
>
```

# DNSのレコードの種類

- Aレコード
  - 名前(FQDN)→IPアドレスのデータベース
- MXレコード
  - メールアドレスのドメイン名→IPアドレスのデータベース
- CNAMEレコード
  - 別名→名前(FQDN)
- AAAAレコード
  - IPv6用のAレコード
- PTRレコード
  - IPアドレス→名前(FQDN)のデータベース
- NSレコード
  - ドメイン名→そのドメインのDNSサーバのIPアドレスのデータベース

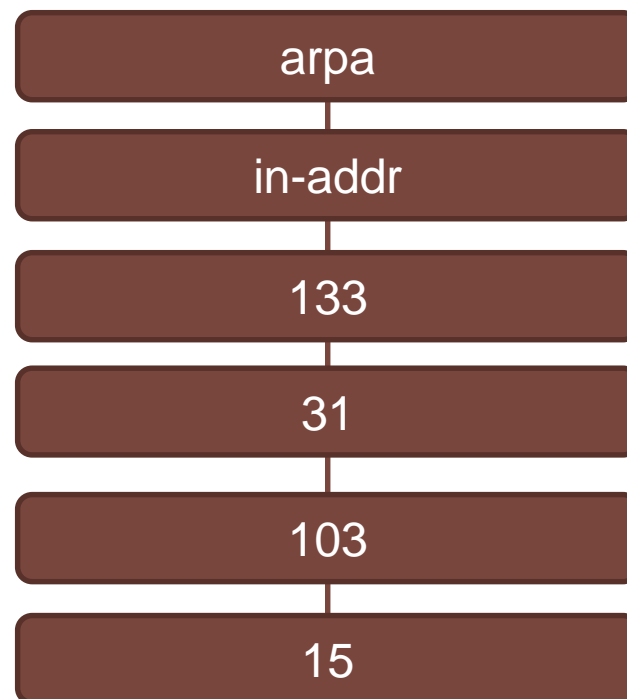
# PTRレコードについて

- 名前→IPアドレスを正引きと呼ぶが、IPアドレス→名前を逆引きと呼ぶ
- PTRレコードは逆引きに利用される
- PTRレコードも階層構造になっている

133.31.103.15のDNSドメインは

15.103.31.133.in-addr.arpa

となる



# nslookupでレコード変更して問い合わせ

```
t-matsu@mail:~$ nslookup
> set type=MX
> ed.tus.ac.jp
Server:      133.31.85.17
Address:     133.31.85.17#53

Non-authoritative answer:
ed.tus.ac.jp  mail exchanger = 10 ed-tus-ac-jp.mail.protection.outlook.com
.

Authoritative answers can be found from:
ed.tus.ac.jp  nameserver = tusns.tus.ac.jp.
ed.tus.ac.jp  nameserver = tusns1.tus.ac.jp.
tusns.tus.ac.jp internet address = 133.31.8.3
tusns1.tus.ac.jp internet address = 133.31.8.4
> set type=NS
> is.noda.tus.ac.jp
Server:      133.31.85.17
Address:     133.31.85.17#53

Non-authoritative answer:
is.noda.tus.ac.jp nameserver = isws01.is.noda.tus.ac.jp.

Authoritative answers can be found from:
> 
```

返答

返答

# DNSプロトコルのフォーマット

ヘッダ部 (Header Section)
問い合わせ部 (Query Section)
回答部 (Answer Section)
権威部 (Authority Section)
付加情報部 (Additional information Section)

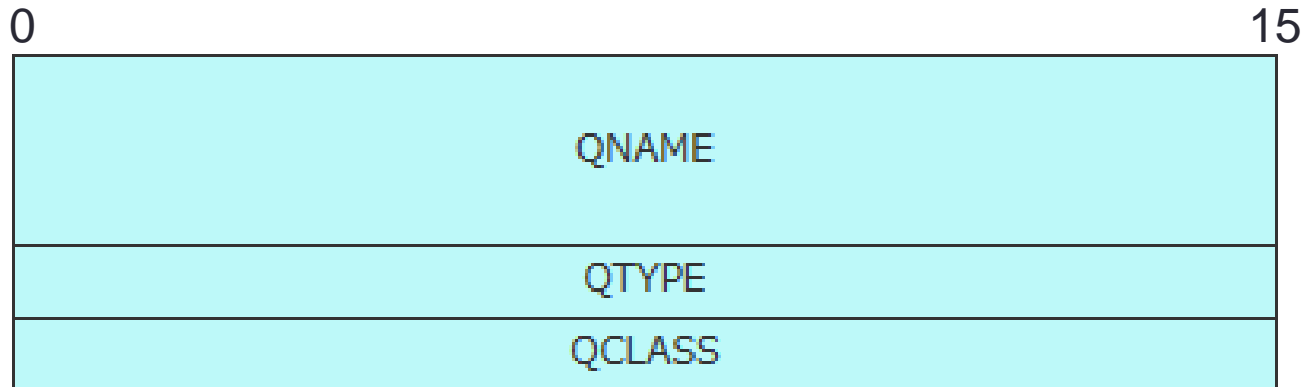
DNSのパケットは, 5つのパートからなる

# DNSヘッダ部(Header Section)

0 <span style="float: right;">15</span>							
ID							
QR	OPCode	AA	TC	RD	RA	Z	RCode
QDCount							
ANCount							
NSCount							
ARCount							

- ID(16bit) メッセージ識別用のID 問い合わせと返答で同じIDにする
- QR(1bit) 0が問い合わせ 1が返答
- OPCode(4bit) (0標準問い合わせ 1逆問い合わせ 2サーバステータス) ※あまり使われない
- AA(1bit) 返答が権威を持っているサーバか否か (0持っていない 1持っている)
- TC(1bit) 応答メッセージが規定値(512オクテット)を超えるか否か (0超えない 1超える)
- RD(1bit) 再帰問い合わせ(0反復処理を要求 1再帰処理を要求)
- RA(1bit) 再帰可能かどうかのフラグ 返答でのみ使われる
- Z(3bit) 拡張用 現在未使用
- RCode(4bit) 応答コード (0エラー無し 1フォーマットエラー 2サーバ障害 3ドメイン名エラー etc)
- \*\*Count (各16bit) それぞれのSectionのレコード数

# 問い合わせ部(Query Section)



- QNAME(可変長bit)  
問い合わせのFQDNを変換して格納する  
例: www.tus.ac.jp → 03 77 77 77 03 74 75 73 02 61 63 02 6A 70 00
- QTYPE(16bit)  
レコードのタイプ  
A(1) NS(2) CNAME(5) PTR(12) MX(15) など
- QCLASS(16bit)  
資源レコード 現在は 1(INternet)のみ使用



# 回答部(Answer Section)

0

15

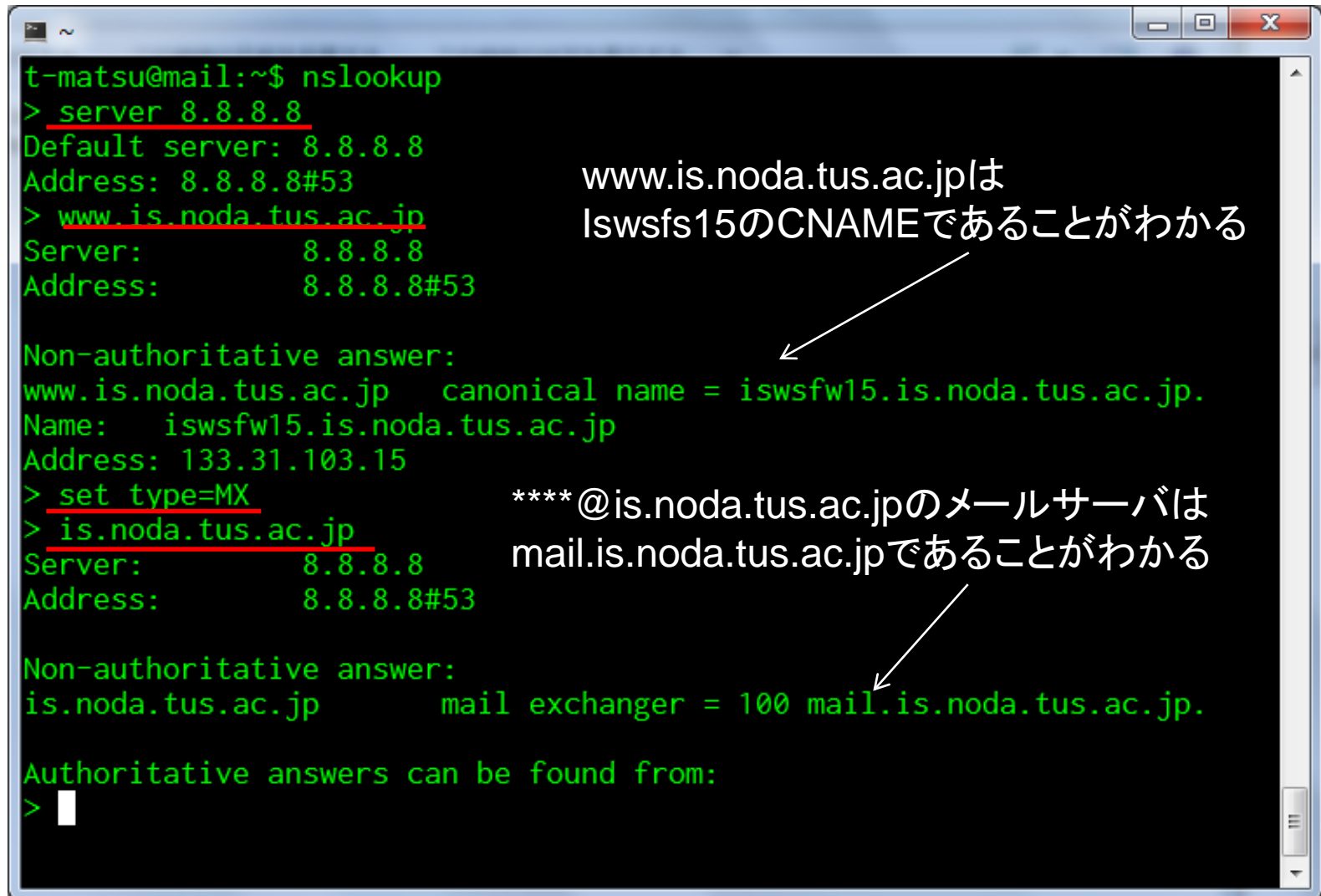
NAME
TYPE
CLASS
TTL
RDLENGTH
RDATA

- NAME(可変長bit) 資源レコードを定義しているドメイン(FQDN)名
- TYPE(16bit) レコードのタイプ (問い合わせ部と同じルールで記載される)
- CLASS(16bit) 資源レコード 現在は 1(Internet)のみ使用
- TTL(32bit) 資源レコードの有効期間(キャッシュ用)
- RLENGTH(16bit) RDATAの長さを8オクテット単位で記載する
- RDATA(可変長bit)資源レコードの資源の部分が記載される

# 権威部(Authority Section) と 付加情報部(Additional Information Section)

- どちらも回答部と同じフォーマット
- 権威部は権威を持っているNSレコードのデータが入る
- 付加情報部は署名等が書き込まれることがある
- どちらも省略されることも多い

# 再びnslookupで実験



```
t-matsu@mail:~$ nslookup
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> www.is.noda.tus.ac.jp
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
www.is.noda.tus.ac.jp  canonical name = iswsfw15.is.noda.tus.ac.jp.
Name:   iswsfw15.is.noda.tus.ac.jp
Address: 133.31.103.15
> set type=MX
> is.noda.tus.ac.jp
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
is.noda.tus.ac.jp      mail exchanger = 100 mail.is.noda.tus.ac.jp.

Authoritative answers can be found from:
> 
```

www.is.noda.tus.ac.jpは  
Iswsfs15のCNAMEであることがわかる

\*\*\*\*@is.noda.tus.ac.jpのメールサーバは  
mail.is.noda.tus.ac.jpであることがわかる

```
set d2
set type=A
www.tus.ac.jp
```

← DebugモードにしてAレコード  
www.tus.ac.jpを検索

```
>>> 権限のない回答:
サーバー: UnKnown
Address: 8.8.8.8
```

```
-----
SendRequest(), len 31
```

以下はwindows限定(Macの表示は異なるかも)

```
HEADER:
```

```
opcode = QUERY, id = 2, rcode = NOERROR
header flags: query, want recursion
questions = 1, answers = 0, authority records = 0, additional = 0
```

```
QUESTIONS:
```

```
www.tus.ac.jp, type = A, class = IN
```

```
-----
Got answer (69 bytes):
```

```
HEADER:
```

```
opcode = QUERY, id = 2, rcode = NOERROR
header flags: response, want recursion, recursion avail.
questions = 1, answers = 2, authority records = 0, additional = 0
```

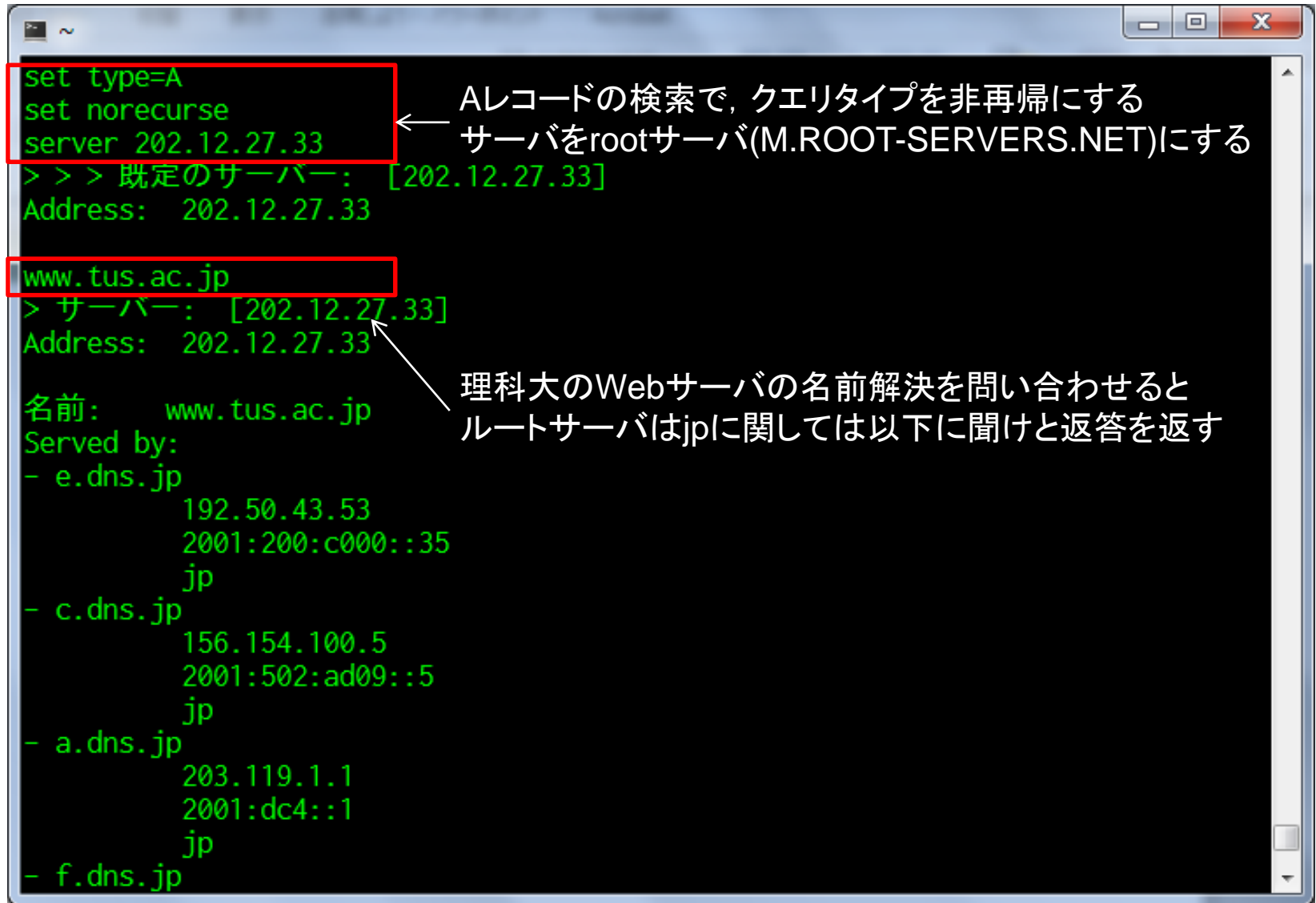
```
QUESTIONS:
```

```
www.tus.ac.jp, type = A, class = IN
```

```
ANSWERS:
```

```
-> www.tus.ac.jp
type = CNAME, class = IN, dlen = 10
canonical name = tuswap1.tus.ac.jp
ttl = 1297 (21 mins 37 secs)
-> tuswap1.tus.ac.jp
type = A, class = IN, dlen = 4
internet address = 133.31.180.213
ttl = 1297 (21 mins 37 secs)
-----
```

# 再帰問い合わせを手動でやってみる



```
> ~
set type=A
set norecurse
server 202.12.27.33
> > > 既定のサーバー: [202.12.27.33]
Address: 202.12.27.33

www.tus.ac.jp
> サーバー: [202.12.27.33]
Address: 202.12.27.33

名前:      www.tus.ac.jp
Served by:
- e.dns.jp
    192.50.43.53
    2001:200:c000::35
    jp
- c.dns.jp
    156.154.100.5
    2001:502:ad09::5
    jp
- a.dns.jp
    203.119.1.1
    2001:dc4::1
    jp
- f.dns.jp
```

← Aレコードの検索で、クエリタイプを非再帰にする  
サーバーをrootサーバー(M.ROOT-SERVERS.NET)にする

← 理科大のWebサーバの名前解決を問い合わせると  
ルートサーバーはjpに関しては以下に聞けと返答を返す

```
server 192.50.43.53
> > in-addr.arpa      nameserver = d.in-addr-servers.arpa
in-addr.arpa      nameserver = a.in-addr-servers.arpa
in-addr.arpa      nameserver = f.in-addr-servers.arpa
in-addr.arpa      nameserver = c.in-addr-servers.arpa
in-addr.arpa      nameserver = b.in-addr-servers.arpa
in-addr.arpa      nameserver = e.in-addr-servers.arpa
a.in-addr-servers.arpa  internet address = 199.212.0.73
b.in-addr-servers.arpa  internet address = 199.253.183.183
c.in-addr-servers.arpa  internet address = 196.216.169.10
d.in-addr-servers.arpa  internet address = 200.10.60.53
e.in-addr-servers.arpa  internet address = 203.119.86.101
f.in-addr-servers.arpa  internet address = 193.0.9.1
a.in-addr-servers.arpa  AAAA IPv6 address = 2001:500:13::73
b.in-addr-servers.arpa  AAAA IPv6 address = 2001:500:87::87
c.in-addr-servers.arpa  AAAA IPv6 address = 2001:43f8:110::10
d.in-addr-servers.arpa  AAAA IPv6 address = 2001:13c7:7010::53
e.in-addr-servers.arpa  AAAA IPv6 address = 2001:dd8:6::101
f.in-addr-servers.arpa  AAAA IPv6 address = 2001:67c:e0::1
既定のサーバー: [192.50.43.53]
Address: 192.50.43.53
```

提示されたjpドメインのDNSの1つを選択する

```
www.tus.ac.jp
> サーバー: [192.50.43.53]
Address: 192.50.43.53
名前: www.tus.ac.jp
Served by:
- tusns1.tus.ac.jp
  133.31.8.4
  tus.ac.jp
- tusns.tus.ac.jp
```

同じ問い合わせをするとtus.ac.jpに関しては  
以下に聞けと返答が来る

```
server 133.31.8.4
```

```
> > 31.133.in-addr.arpa nameserver = tusns.tus.ac.jp  
31.133.in-addr.arpa      nameserver = tusns1.tus.ac.jp  
既定のサーバー: [133.31.8.4]  
Address: 133.31.8.4
```

```
www.tus.ac.jp
```

```
> サーバー: [133.31.8.4]  
Address: 133.31.8.4
```

```
名前: tuswap1.tus.ac.jp  
Address: 133.31.180.213  
Aliases: www.tus.ac.jp
```

同様の処理を繰り返すと  
目的の133.31.180.213が得られる

# ルートサーバについて

- 世界中に13個あり, {a~m}.root-servers.netという名前がつけられている
- 13個目のm.root-servers.netは日本の大手町にある
- 当初UDPは512バイト制限があったため, 512バイト以内に収まるホスト名とIPアドレスの組が最大で13個入ることからルートサーバは13個となった



参考URL

<http://www.root-servers.org/>



# DNSのキャッシュ機能

- DNSサーバは一度検索した結果をキャッシュに保存する機能がある
- DNSのトラフィック(特にルートサーバへ)を激減させている
- キャッシュする時間は権威を持つサーバが自身の保持するレコード単位で設定されている

# 今回のまとめ

- DNS

- インターネット上に展開する分散型の階層データベースである
- 再帰問い合わせと非再帰問い合わせの2種類の挙動がある
- 名前→IPを正引き, IP→名前を逆引きと呼ぶ
- メールアドレスのドメインなどのレコードも存在する
- DNSサーバにはキャッシュ機能がある

質問あればどうぞ

次回はアプリケーション層(つづき)！