# DNSの例
# (実際のパケットダンプを使った説明)

2001年11月1日

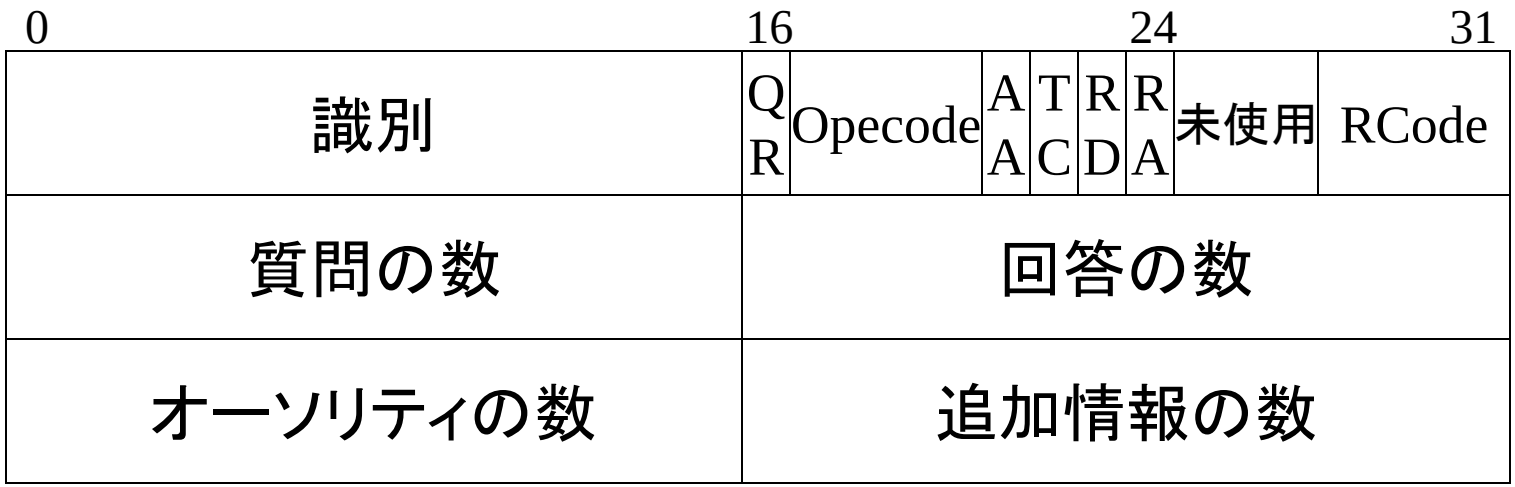
上牧瀬　誠

# DNSプロトコルフォーマット

- DNSメッセージはUDPプロトコルで運ばれる
- 53番のポートが使われる
- メッセージタイプにより空になるセクションもある

| |
|---|
| ヘッダ<br>(必須) |
| 質問<br>(ネームサーバ宛ての質問) |
| 回答<br>(質問への回答としてのリソースレコード) |
| オーソリティ<br>(オーソリティをポイントするリソースレコード) |
| 追加情報<br>(追加情報をもつリソースレコード) |

# ヘッダ




識別　：　問い合わせを生成するシステムが割り当てる固有の番号
QR　：　問い合わせ(0)，応答(1)
Opecode　：　問い合わせのタイプ
AA　：　応答が正式なものである
TC　：　メッセージが短縮されている
RD　：　問い合わせホストが再帰問い合わせを希望
RA　：　再帰サービスをネームサーバが希望できる
Rcode　：　エラーの種類

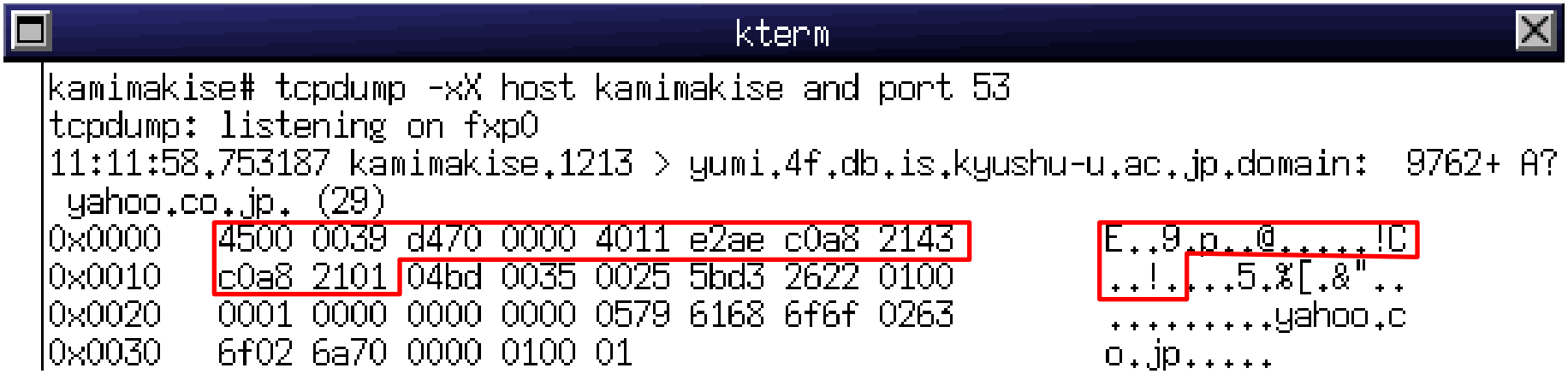
# 質問


QName　:　問い合わせの対象ドメイン名
QType　:　問い合わせのタイプ
QClass　:　問い合わせのクラス

# 実際の例

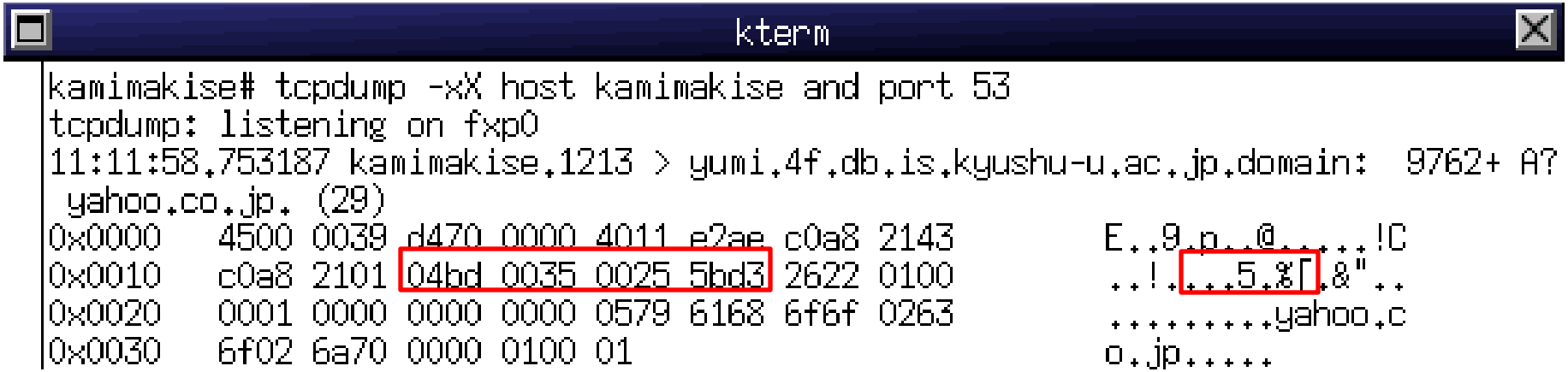
- rootでtcpdumpを実行
  - tcpdump –xX –s 1000 host kamimakise and port 53
- 次のpingコマンドを実行
  - ping yahoo.co.jp
- IPアドレスがわからないのでDNS(yumi)にyahoo.co.jpのIPアドレスを問い合わせる

# 実際の例(IPヘッダ)



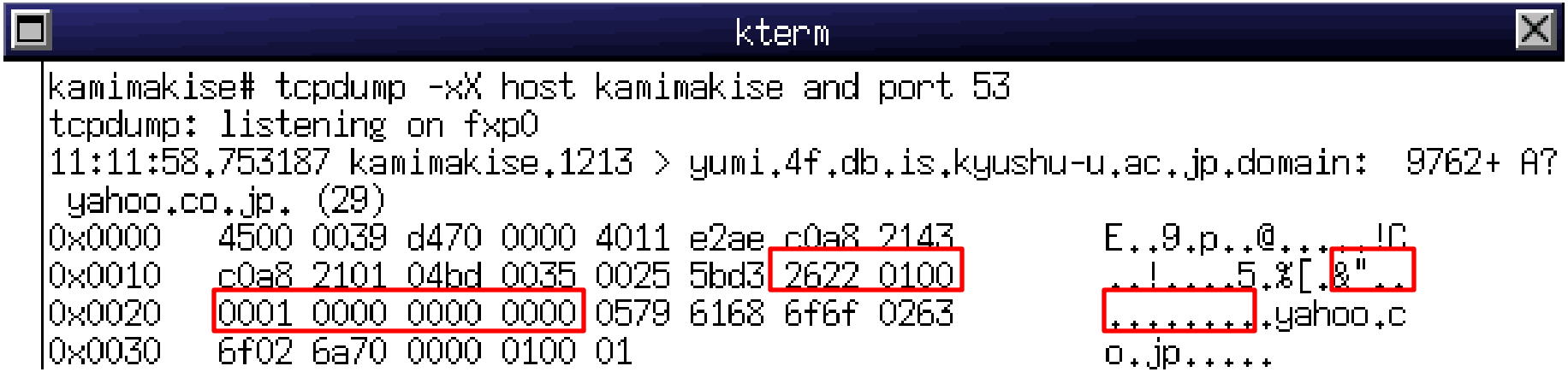

4 ： バージョン
5 ： ヘッダ長
00 ： サービスタイプ
0039 ： パケット長(57オクテット)
d470 ： 識別子
0000 ： フラグ，フラグメントオフセット
40 ： 生存時間
11 ： プロトコル(UDP)
e2ae ： チェックサム
c0a82143 ： 送信元IPアドレス(192.168.33.67(kamimakise))
c0a82101 ： 宛先IPアドレス(192.168.33.1(yumi))

# 実際の例(UDPヘッダ)



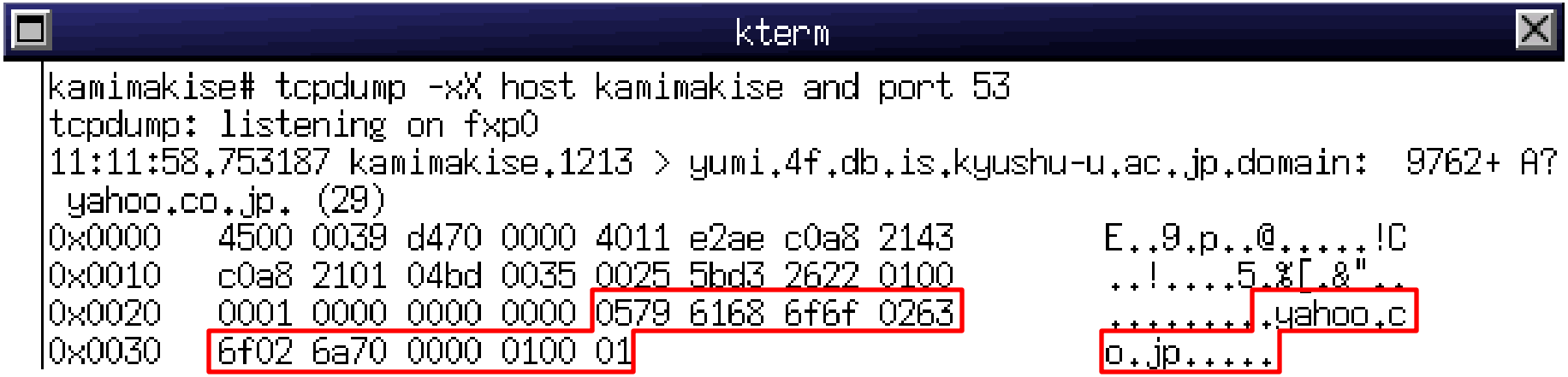

04bd ： 送信元ポート(1243番)
0035 ： 宛先ポート(53番)
0025 ： 長さ(37オクテット)
5bd3 ： チェックサム

# 実際の例(DNSヘッダ)




2622 : 識別子
0100 : 標準問い合わせ，再帰希望，エラーなし
0001 : 質問の数(1個)
0000 : 回答の数(なし)
0000 : オーソリティの数(なし)
0000 : 追加情報の数(なし)

# 実際の例(DNSデータ)




057961686f6f ： 5オクテット(yahoo)

02636f ： 2オクテット(co)

026a70 ： 2オクテット(jp)

00 ： ヌルラベル(終了)

0001 ： ホストアドレスの問い合わせ

0001 ： インターネットシステム

# 実際の例(応答パケット)

```
10:29:14.562632 yumi.4f.db.is.kyushu-u.ac.jp.domain > kamimakise.dwf:  13488* 8/
3/3 A w10.yahoo.co.jp, A www123.yahoo.co.jp, A www115.yahoo.co.jp, A w01.yahoo.c
o.jp, A w02.yahoo.co.jp, A w03.yahoo.co.jp, A w08.yahoo.co.jp, A w09.yahoo.co.jp
  (275)
0x0000   4500 012f 1891 0000 4011 9d98 c0a8 2101        E../....@.....!.
0x0010   c0a8 2143 0035 05aa 011b 2ec9 34b0 8580        ..!C.5.....4...
0x0020   0001 0008 0003 0003 0579 6168 6f6f 0263        .........yahoo.c
0x0030   6f02 6a70 0000 0100 01c0 0c00 0100 0100        o.jp............
0x0040   0001 2c00 04d2 5199 46c0 0c00 0100 0100        ..,...Q.F.......
0x0050   0001 2c00 04d2 98ec 32c0 0c00 0100 0100        ..,.....2.......
0x0060   0001 2c00 04d2 8cc8 10c0 0c00 0100 0100        ..,.............
0x0070   0001 2c00 04d2 98ec 6fc0 0c00 0100 0100        ..,.....o.......
0x0080   0001 2c00 04d2 98ec 70c0 0c00 0100 0100        ..,.....p.......
0x0090   0001 2c00 04d2 98ec 71c0 0c00 0100 0100        ..,.....q.......
0x00a0   0001 2c00 04d2 5199 44c0 0c00 0100 0100        ..,...Q.D.......
0x00b0   0001 2c00 04d2 5199 45c0 0c00 0200 0100        ..,...Q.E.......
0x00c0   0003 8400 0704 646e 7331 c00c c00c 0002        ......dns1......
0x00d0   0001 0000 0384 000a 0764 6e73 6e32 3031        .........dnsn201
0x00e0   c00c c00c 0002 0001 0000 0384 0011 026e        ...............n
0x00f0   7308 746f 6b79 6f6e 6574 0261 64c0 15c0        s.tokyonet.ad...
0x0100   a900 0100 0100 0003 8400 04d2 8cc8 32c0        ..............2.
0x0110   bc00 0100 0100 0003 8400 04ca e5c6 78c0        ..............x.
0x0120   d200 0100 0100 0151 8000 04ca ef3d 3d          .......Q.....==
```

# 実際の例(応答パケットの内容)

- 質問　：　1個
  - yahoo.co.jp
- 回答　：　8個
  - d2519946　：　210.81.153.70
  - d298ec32　：　210.152.236.50
  - d28cc810　：　210.140.200.16
  - d298ec6f　：　210.152.236.111
  - d298ec70　：　210.152.236.112
  - d298ec71　：　210.152.236.113
  - d2519944　：　210.81.153.68
  - d2519945　：　210.81.153.69

# 実際の例(応答パケットの内容)

- オーソリティ　：　3個
  - dns1.yahoo.co.jp
  - dnsn201.yahoo.co.jp
  - ns.tokyonet.ad.jp
- 追加情報　：　3個
  - d28cc832　：　210.140.200.50
  - cae5c678　：　202.229.198.120
  - caef3d3d　：　202.239.61.61