

ENUMシステムにおけるネットワーク解析

第6回 ETJP全体ミーティング

2004年9月14日

株式会社アステック

発表の内容

- ネットワークアナライザとは
- ASTEC Eyes on the net
- ASTEC Eyes のENUM関連のデータへの対応状況
- ENUMシステムにおけるネットワーク解析
- デモンストレーション

ネットワークアナライザ

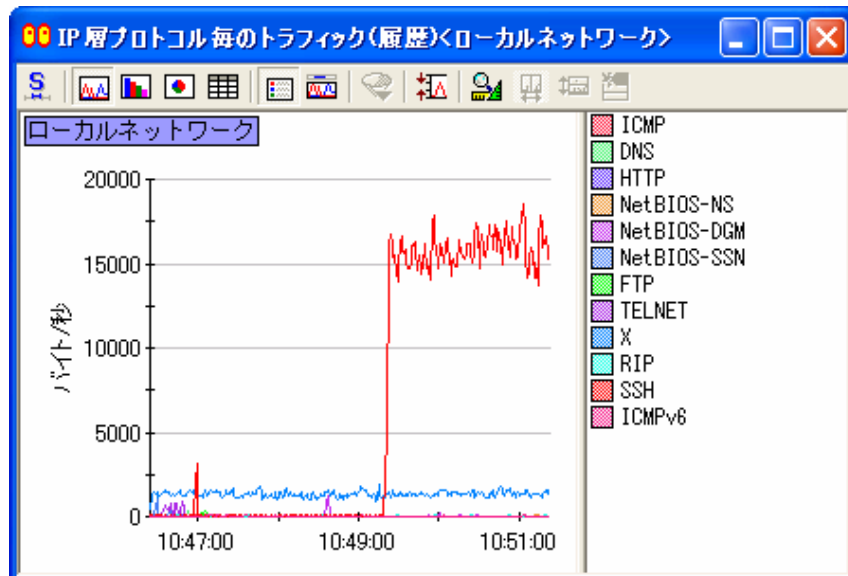
ネットワークの中を直接見るためのツール

- **モニタ機能**
 - ネットワークトラフィックの統計情報をグラフなどで表示
 - プロトコルやアドレスなど様々な視点から統計処理を行う
- **キャプチャ機能/デコード機能**
 - パケットそのものをバッファに取り込む(キャプチャ)
 - データをプロトコルに基づいて解析し、内容を表示(デコード)

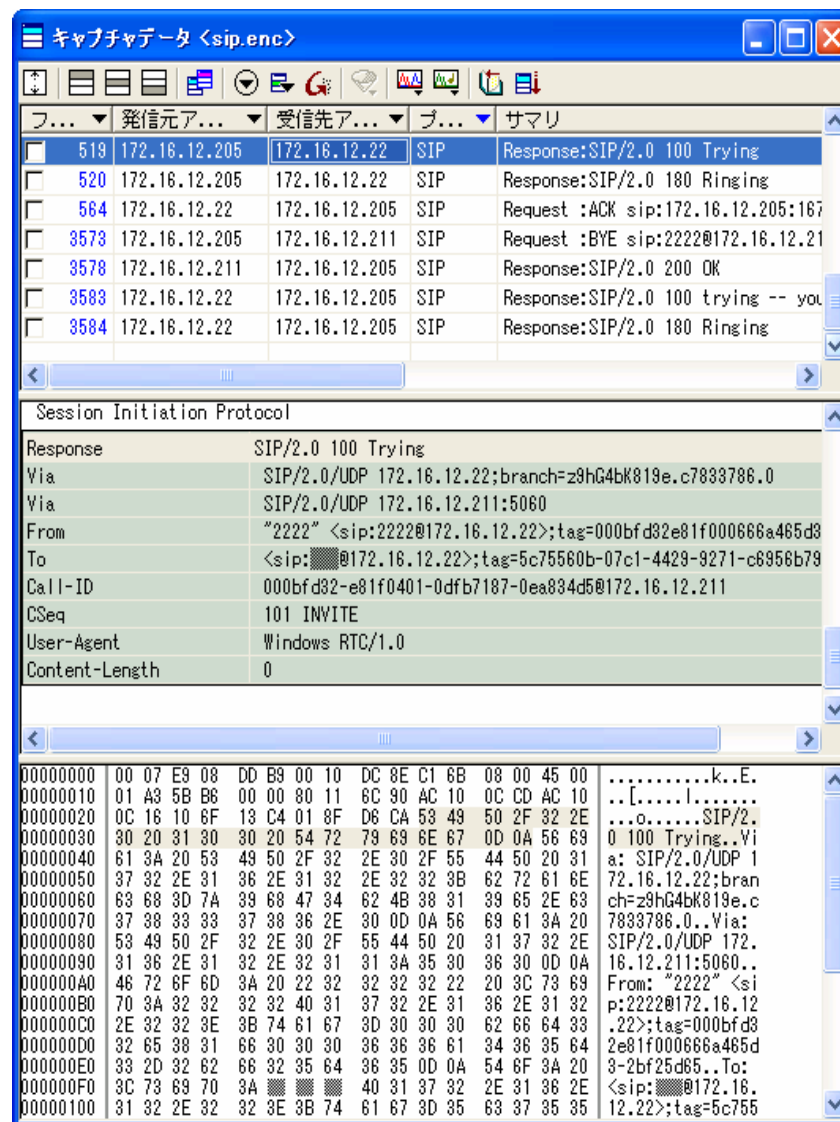
ASTEC Eyes on the net

- 株式会社アステックが開発しているソフトウェアのネットワークアナライザ
- 2000年発売開始、現在のバージョンは3.103
- リモートモジュールを利用してリモート監視が可能
- 2003年12月 ASTEC Eyes for VoIP発売

ASTEC Eyes の画面



モニタ機能
(IP層プロトコル毎のトラフィック)



...	発信元ア...	受信先ア...	ブ...	サマリ
519	172.16.12.205	172.16.12.22	SIP	Response:SIP/2.0 100 Trying
520	172.16.12.205	172.16.12.22	SIP	Response:SIP/2.0 180 Ringing
564	172.16.12.22	172.16.12.205	SIP	Request :ACK sip:172.16.12.205:167
3573	172.16.12.205	172.16.12.211	SIP	Request :BYE sip:2222@172.16.12.21
3578	172.16.12.211	172.16.12.205	SIP	Response:SIP/2.0 200 OK
3583	172.16.12.22	172.16.12.205	SIP	Response:SIP/2.0 100 trying -- you
3584	172.16.12.22	172.16.12.205	SIP	Response:SIP/2.0 180 Ringing

```

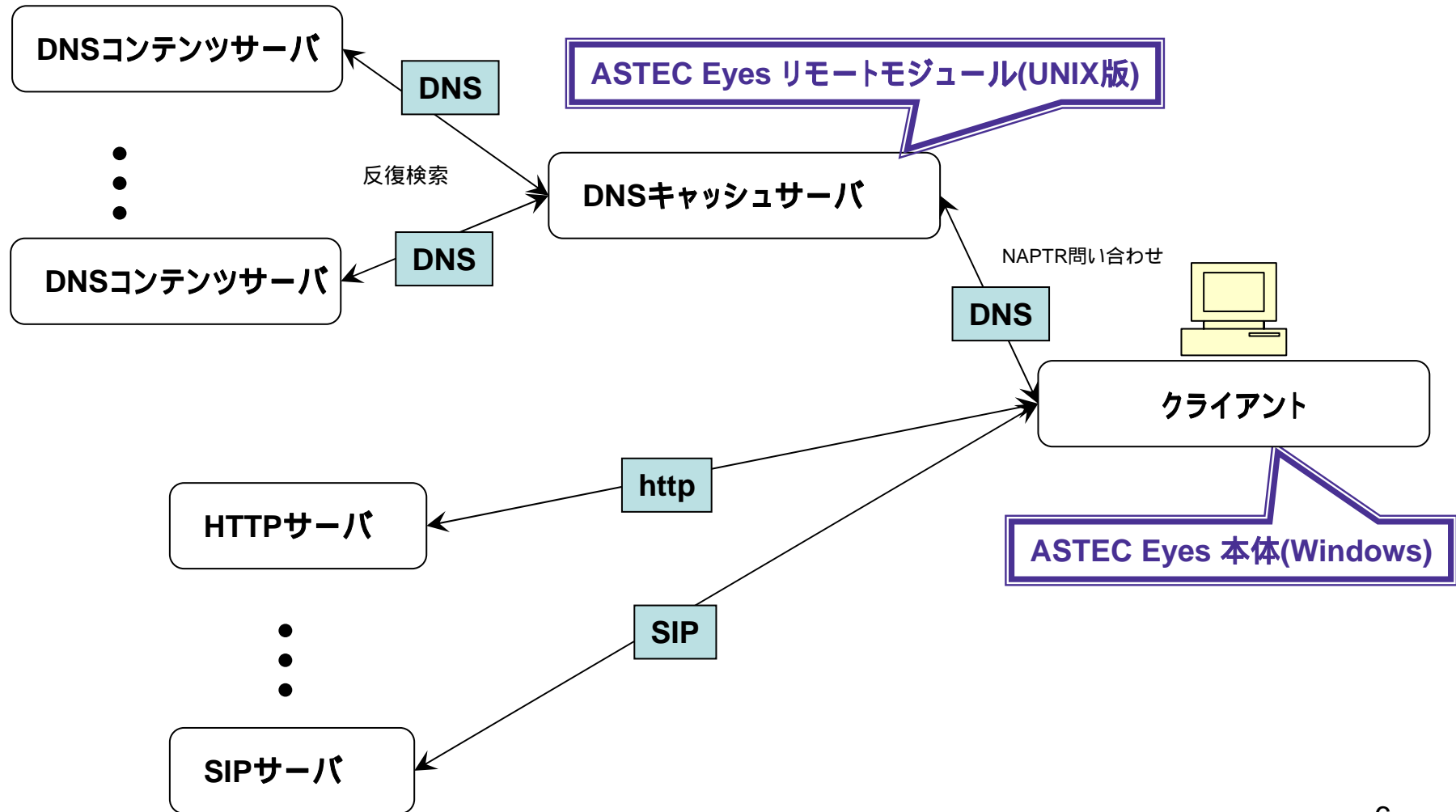
Session Initiation Protocol
Response          SIP/2.0 100 Trying
Via               SIP/2.0/UDP 172.16.12.22;branch=z9hG4bK819e.c7833786.0
Via               SIP/2.0/UDP 172.16.12.211:5060
From              "2222" <sip:2222@172.16.12.22>;tag=000bfd32e81f000666a465d3
To                <sip:#####@172.16.12.22>;tag=5c75560b-07c1-4429-9271-c6956b79
Call-ID           000bfd32-e81f0401-0dfb7187-0ea834d5@172.16.12.211
CSeq              101 INVITE
User-Agent        Windows RTC/1.0
Content-Length    0
    
```

```

00000000 00 07 E9 08 DD B9 00 10 DC 8E C1 6B 08 00 45 00 .....k..E.
00000010 01 A3 5B B6 00 00 80 11 6C 90 AC 10 0C CD AC 10 ..[.....].....
00000020 0C 16 10 6F 13 C4 01 8F D6 CA 53 49 50 2F 32 2E ...o.....SIP/2.
00000030 30 20 31 30 30 20 54 72 79 69 6E 67 0D 0A 56 69 0 100 Trying..Vi
00000040 61 3A 20 53 49 50 2F 32 2E 30 2F 55 44 50 20 31 a: SIP/2.0/UDP 1
00000050 37 32 2E 31 36 2E 31 32 2E 32 32 3B 62 72 61 6E 72.16.12.22;bran
00000060 63 68 3D 7A 39 68 47 34 62 4B 38 31 39 65 2E 63 ch=z9hG4bK819e.c
00000070 37 38 33 33 37 38 36 2E 30 0D 0A 56 69 61 3A 20 7833786.0..Via:
00000080 53 49 50 2F 32 2E 30 2F 55 44 50 20 31 37 32 2E SIP/2.0/UDP 172.
00000090 31 36 2E 31 32 2E 32 31 31 3A 35 30 36 30 0D 0A 16.12.211:5060..
000000A0 46 72 6F 6D 3A 20 22 32 32 32 32 20 3C 73 69 From: "2222" <si
000000B0 70 3A 32 32 32 32 40 31 37 32 2E 31 36 2E 31 32 p:2222@172.16.12
000000C0 2E 32 32 3E 3B 74 61 67 3D 30 30 30 62 66 64 33 .22>;tag=000bfd3
000000D0 32 65 38 31 66 30 30 30 36 36 36 61 34 36 35 64 2e81f000666a465d
000000E0 33 2D 32 62 68 32 35 64 36 35 0D 0A 54 6F 3A 20 3-2bf25d85..To:
000000F0 3C 73 69 70 3A ##### 40 31 37 32 2E 31 36 2E <sip:#####@172.16.
00000100 31 32 2E 32 32 3E 3B 74 61 67 3D 35 63 37 35 35 12.22>;tag=5c755
    
```

デコード機能
(SIPプロトコルのデコード結果)

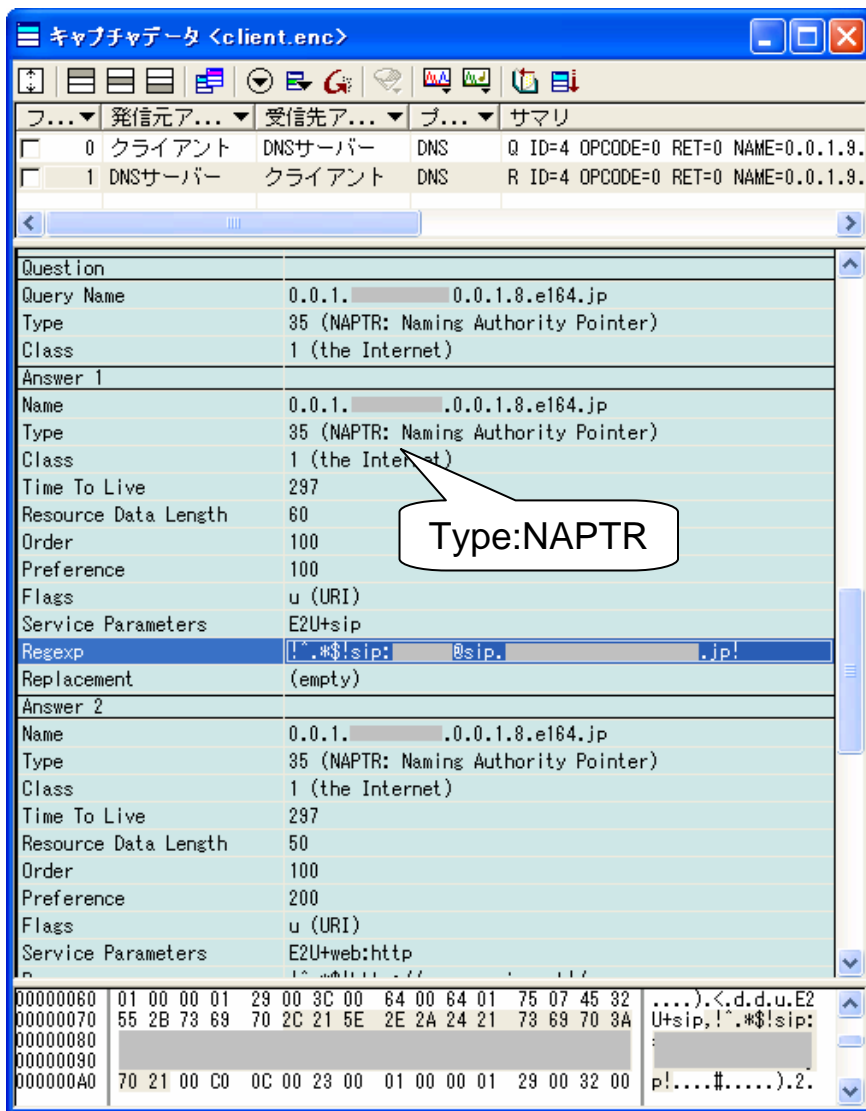
ENUMシステムにおけるデータの流れ



ASTEC Eyes の ENUM関連のデータへの対応

- DNS
 - NAPTR
 - DNSSEC
(DS,DNSKEY,RRSIG,NSEC,OPT)
- ENUM サービスプロトコルへの対応
 - SIP, H323, HTTP, SMTP など

デコード結果



キャプチャデータ <client.enc>

No.	Time	Source	Destination	Protocol	Length	Info
0	0.000000	クライアント	DNSサーバー	DNS	Q	ID=4 OPCODE=0 RET=0 NAME=0.0.1.8.e164.jp
1	0.000000	DNSサーバー	クライアント	DNS	R	ID=4 OPCODE=0 RET=0 NAME=0.0.1.8.e164.jp

Question

Query Name 0.0.1.8.e164.jp
 Type 35 (NAPTR: Naming Authority Pointer)
 Class 1 (the Internet)

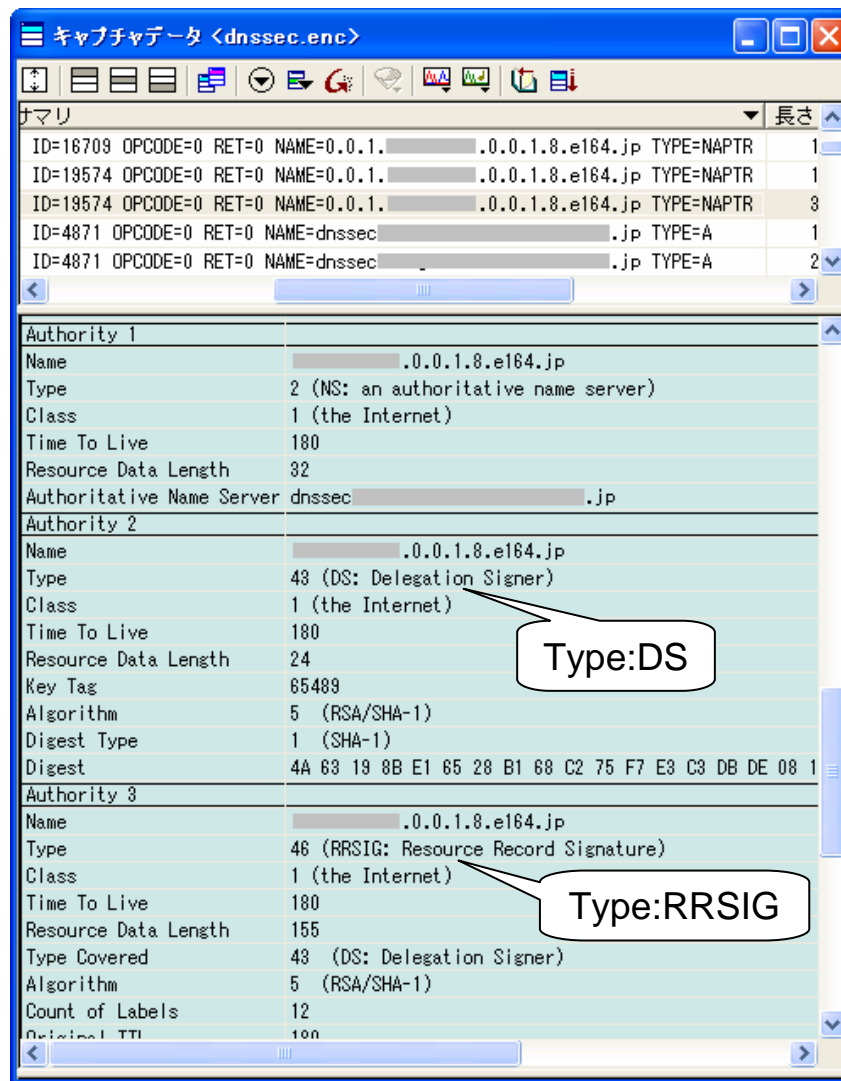
Answer 1

Name 0.0.1.8.e164.jp
 Type 35 (NAPTR: Naming Authority Pointer)
 Class 1 (the Internet)
 Time To Live 297
 Resource Data Length 60
 Order 100
 Preference 100
 Flags u (URI)
 Service Parameters E2U+sip
 Regexp !.*\$!sip: @sip. .jp!
 Replacement (empty)

Answer 2

Name 0.0.1.8.e164.jp
 Type 35 (NAPTR: Naming Authority Pointer)
 Class 1 (the Internet)
 Time To Live 297
 Resource Data Length 50
 Order 100
 Preference 200
 Flags u (URI)
 Service Parameters E2U+web:http

NAPTR レコード



キャプチャデータ <dnssec.enc>

ID	Opcode	Ret	Name	Type	Length
16709	0	0	0.0.1.8.e164.jp	NAPTR	1
19574	0	0	0.0.1.8.e164.jp	NAPTR	1
19574	0	0	0.0.1.8.e164.jp	NAPTR	3
4871	0	0	dnssec.jp	A	1
4871	0	0	dnssec.jp	A	2

Authority 1

Name 0.0.1.8.e164.jp
 Type 2 (NS: an authoritative name server)
 Class 1 (the Internet)
 Time To Live 180
 Resource Data Length 32
 Authoritative Name Server dnssec.jp

Authority 2

Name 0.0.1.8.e164.jp
 Type 43 (DS: Delegation Signer)
 Class 1 (the Internet)
 Time To Live 180
 Resource Data Length 24
 Key Tag 65489
 Algorithm 5 (RSA/SHA-1)
 Digest Type 1 (SHA-1)
 Digest 4A 63 19 8B E1 65 28 B1 68 C2 75 F7 E3 C3 DB DE 08 1

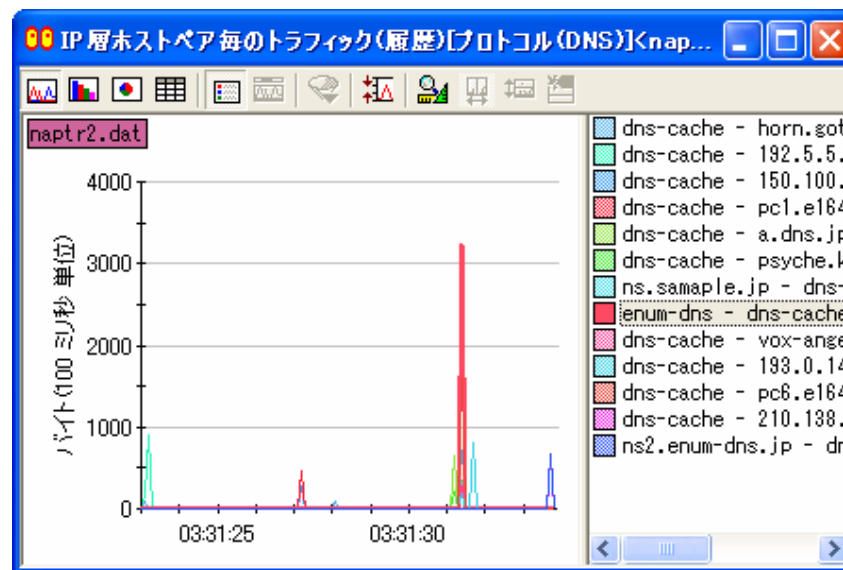
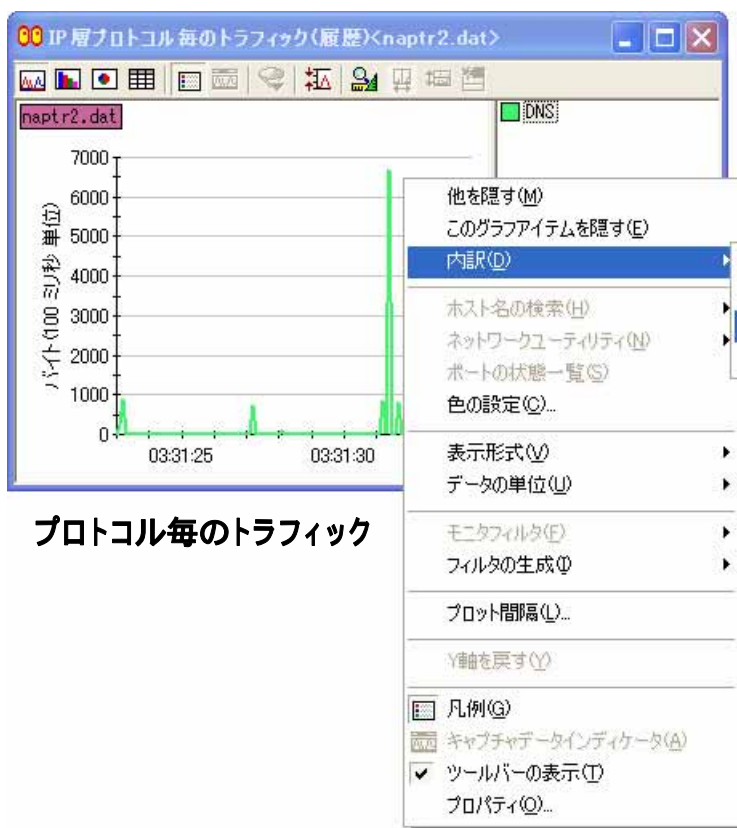
Authority 3

Name 0.0.1.8.e164.jp
 Type 46 (RRSIG: Resource Record Signature)
 Class 1 (the Internet)
 Time To Live 180
 Resource Data Length 155
 Type Covered 43 (DS: Delegation Signer)
 Algorithm 5 (RSA/SHA-1)
 Count of Labels 12
 Original TTL 100

DSレコードとRRSIGレコード

統計情報の表示

- 一旦キャプチャしたデータについて統計処理を行いグラフ表示を行う

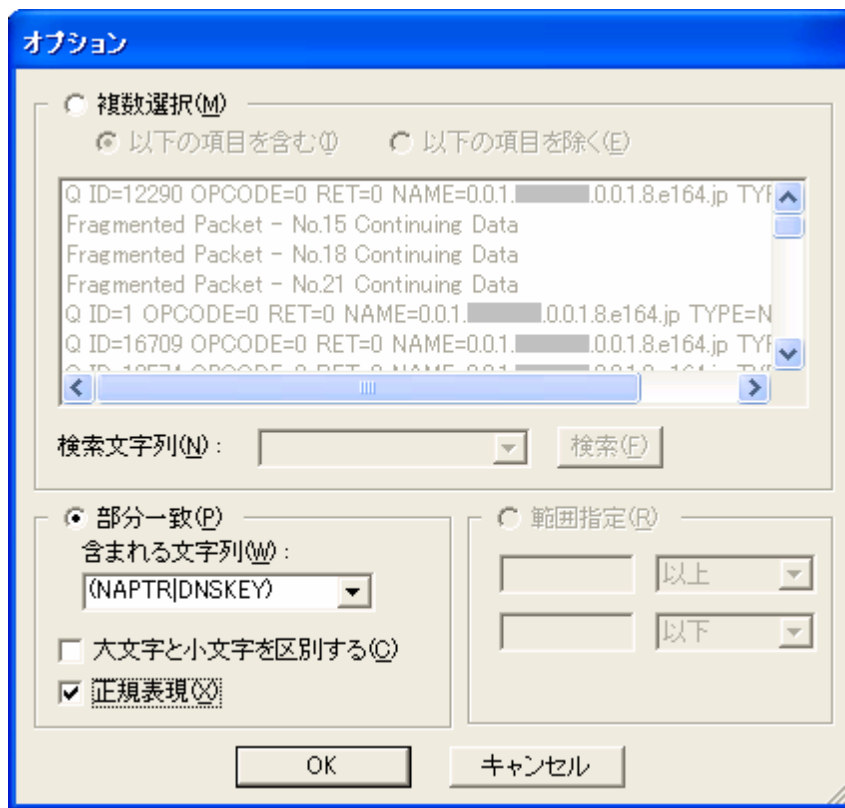


DNSについてドリルダウン
(ホストペアの内訳を表示)

フ.	発信元...	受信先...	ブ..	サマリ	長さ
0	enum-client	dns-cache	DNS	Q ID=1 OPCODE=0 RET=0 NAME=0.0.1. .0.0.1.8.e164.jp TYPE=NAPTR	91
1	dns-cache	ns0.nic.ad.jp	DNS	Q ID=16709 OPCODE=0 RET=0 NAME=0.0.1. .0.0.1.8.e164.jp TYPE=NAPTR	102
2	ns0.nic.ad.jp	dns-cache	DNS	R ID=16709 OPCODE=0 RET=0 NAME=0.0.1. .0.0.1.8.e164.jp TYPE=NAPTR	170
3	dns-cache	ns.164.jp	DNS	Q ID=19574 OPCODE=0 RET=0 NAME=0.0.1. .0.0.1.8.e164.jp TYPE=NAPTR	102
4	ns.164.jp	dns-cache	DNS	R ID=19574 OPCODE=0 RET=0 NAME=0.0.1. .0.0.1.8.e164.jp TYPE=NAPTR	349
5	dns-cache	e.dns.jp	DNS	Q ID=4871 OPCODE=0 RET=0 NAME=dnssec .jp TYPE=A	103
6	e.dns.jp	dns-cache	DNS	R ID=4871 OPCODE=0 RET=0 NAME=dnssec .jp TYPE=A	203
7	dns-cache	ns2.child.e...	DNS	Q ID=552 OPCODE=0 RET=0 NAME=dnssec .jp TYPE=A	103
8	dns-cache	dns0.spin.a...	DNS	Q ID=276 OPCODE=0 RET=0 NAME=psy .or.jp TYPE=A	88
9	ns2.child....	dns-cache	DNS	R ID=552 OPCODE=0 RET=0 NAME=dnssec .jp TYPE=A	201
10	dns-cache	vox-angelic...	DNS	Q ID=49160 OPCODE=0 RET=0 NAME=dnssec .jp TYPE=A	103
11	dns-cache	E.ROOT-SERV...	DNS	Q ID=24580 OPCODE=0 RET=0 NAME=ns2. .jp TYPE=A	97
12	dns0.spin....	dns-cache	DNS	R ID=276 OPCODE=0 RET=0 NAME=psy .or.jp TYPE=A	256
13	vox-angeli...	dns-cache	DNS	R ID=49160 OPCODE=0 RET=0 NAME=dnssec .jp TYPE=A	201
14	dns-cache	enum-dns	DNS	Q ID=12290 OPCODE=0 RET=0 NAME=0.0.1. .0.0.1.8.e164.jp TYPE=NAPTR	102
15	enum-dns	dns-cache	DNS	R ID=12290 OPCODE=0 RET=0 NAME=0.0.1. .0.0.1.8.e164.jp TYPE=NAPTR	1514
16	enum-dns	dns-cache	IPv4	Fragmented Packet - No.15 Continuing Data	679
17	dns-cache	enum-dns	DNS	Q ID=38913 OPCODE=0 RET=0 NAME=1. .0.0.1.8.e164.jp TYPE=DNSKEY	98
18	enum-dns	dns-cache	DNS	R ID=38913 OPCODE=0 RET=0 NAME=1. .0.0.1.8.e164.jp TYPE=DNSKEY	1514
19	enum-dns	dns-cache	IPv4	Fragmented Packet - No.18 Continuing Data	283
20	dns-cache	ns.e164.jp	DNS	Q ID=34874 OPCODE=0 RET=0 NAME=e164.jp TYPE=DNSKEY	78
21	ns.e164.jp	dns-cache	DNS	R ID=34874 OPCODE=0 RET=0 NAME=e164.jp TYPE=DNSKEY	1514
22	ns.e164.jp	dns-cache	IPv4	Fragmented Packet - No.21 Continuing Data	561
23	dns-cache	enum-client	DNS	R ID=1 OPCODE=0 RET=0 NAME=0.0.1. .0.0.1.8.e164.jp TYPE=NAPTR	356
24	E.ROOT-SER...	dns-cache	DNS	R ID=24580 OPCODE=0 RET=0 NAME=ns2. .jp TYPE=A	405
25	dns-cache	ns-jp.sinet...	DNS	Q ID=50205 OPCODE=0 RET=0 NAME=ns2. .jp TYPE=A	97
26	ns-jp.sine...	dns-cache	DNS	R ID=50205 OPCODE=0 RET=0 NAME=ns2. .jp TYPE=A	213
27	dns-cache	psyche.kaba...	DNS	Q ID=23244 OPCODE=0 RET=0 NAME=ns2. .jp TYPE=A	97
28	dns-cache	ns.child.e1...	DNS	Q ID=22219 OPCODE=0 RET=0 NAME=ns2. .jp TYPE=A	97
29	ns.child.e...	dns-cache	DNS	R ID=22219 OPCODE=0 RET=0 NAME=ns2. .jp TYPE=A	227

- DNSキャッシュサーバでキャプチャしたデータ
 - ENUM クライアント DNS キャッシュサーバ
 - DNSキャッシュサーバ DNSコンテンツサーバ

ENUM関連のパケットを抜き出す



- 通常の名前解決のDNSレコードが含まれる
- DNSSEC関連のデータの流を見やすくするために、サマリーにNAPTR,DNSKEYと表示されているパケットだけを取り出す

サマリーに含まれる文字列に対してフィルタをかける

フィルタした結果

キャプチャデータ <dnssec.enc>

フ.	発信元...	受信先ア...	プ..	サマリ	長さ	
<input type="checkbox"/>	0	enum-client	dns-cache	DNS	Q ID=1 OPCODE=0 RET=0 NAME=0.0.1. .0.0.1.8.e164.jp TYPE=NAPTR	91
<input type="checkbox"/>	1	dns-cache	ns0.nic.ad.jp	DNS	Q ID=16709 OPCODE=0 RET=0 NAME=0.0.1. .0.0.1.8.e164.jp TYPE=NAPTR	102
<input type="checkbox"/>	2	ns0.nic.ad.jp	dns-cache	DNS	R ID=16709 OPCODE=0 RET=0 NAME=0.0.1. .0.0.1.8.e164.jp TYPE=NAPTR	170
<input type="checkbox"/>	3	dns-cache	ns.164.jp	DNS	Q ID=19574 OPCODE=0 RET=0 NAME=0.0.1. .0.0.1.8.e164.jp TYPE=NAPTR	102
<input type="checkbox"/>	4	ns.164.jp	dns-cache	DNS	R ID=19574 OPCODE=0 RET=0 NAME=0.0.1. .0.0.1.8.e164.jp TYPE=NAPTR	349
<input type="checkbox"/>	14	dns-cache	enum-dns	DNS	Q ID=12290 OPCODE=0 RET=0 NAME=0.0.1. .0.0.1.8.e164.jp TYPE=NAPTR	102
<input type="checkbox"/>	15	enum-dns	dns-cache	DNS	R ID=12290 OPCODE=0 RET=0 NAME=0.0.1. .0.0.1.8.e164.jp TYPE=NAPTR	1514
<input type="checkbox"/>	17	dns-cache	enum-dns	DNS	Q ID=38913 OPCODE=0 RET=0 NAME=1. .0.0.1.8.e164.jp TYPE=DNSKEY	98
<input type="checkbox"/>	18	enum-dns	dns-cache	DNS	R ID=38913 OPCODE=0 RET=0 NAME=1. .0.0.1.8.e164.jp TYPE=DNSKEY	1514
<input type="checkbox"/>	20	dns-cache	ns.e164.jp	DNS	Q ID=34874 OPCODE=0 RET=0 NAME=e164.jp TYPE=DNSKEY	78
<input type="checkbox"/>	21	ns.e164.jp	dns-cache	DNS	R ID=34874 OPCODE=0 RET=0 NAME=e164.jp TYPE=DNSKEY	1514
<input type="checkbox"/>	23	dns-cache	enum-client	DNS	R ID=1 OPCODE=0 RET=0 NAME=0.0.1. .0.0.1.8.e164.jp TYPE=NAPTR	356

Number of Authority RRs 0 resource record(s)
 Number of Additional RRs 1 resource record(s)

Question

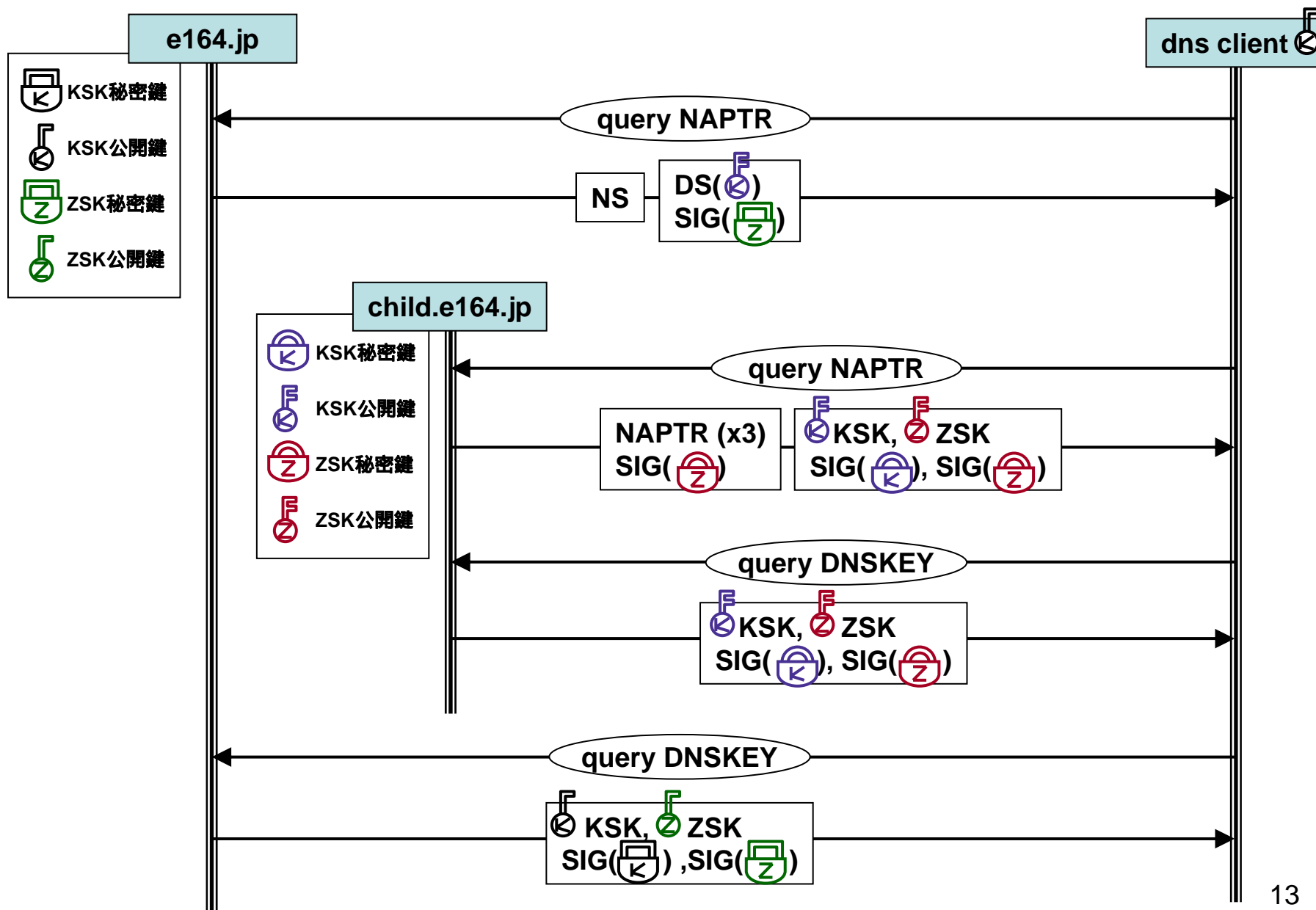
Query Name e164.jp
 Type 48 (DNSKEY: Domain Name System KEY)
 Class 1 (the Internet)

Additional

Name
 Type 41 (OPT)
 UDP payload size 4096
 Extended Response Code 0
 Version 0
 Z Field 0x8000
 DNSSEC 1... .. accept DNSSEC
 Zero .000 0000 0000 0000

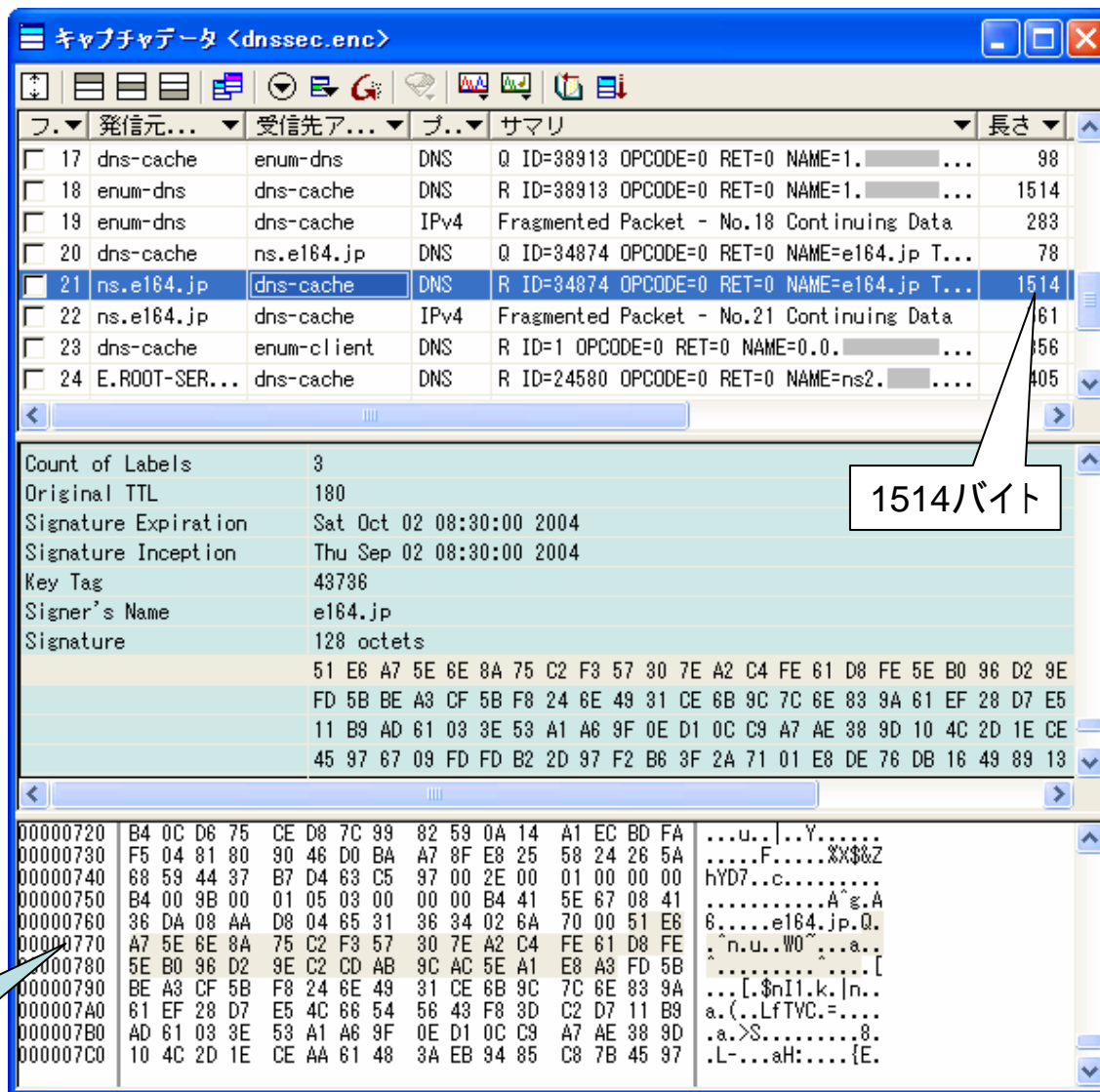
Resource Data Length 0
 Resource Data 0 octet(s)

DNSSEC関連のデータの流れ



IPパケットのフラグメント

- DNSのデータ量が大きく、Ethernetの規格を超えたため、IPレイヤで分割が起こる
- ASTEC Eyesは続きの packets を見つけて結合して解析
- キャプチャフィルタなどに注意も必要



The screenshot shows a packet capture window titled 'キャプチャデータ <dnssec.enc>'. The main table lists several packets. Packet 21 is highlighted in blue, showing a DNS response for 'ns.e164.jp' with a length of 1514 bytes. The details pane below shows the packet structure, including 'Count of Labels: 3', 'Original TTL: 180', and a signature block. A callout box points to the '長さ' column for packet 21, stating '1514バイト'. The hex dump at the bottom shows the raw data of the packet, with a callout box pointing to the offset 0x0770, stating '0x0770 = 1904 実際には含まれていない (別のパケットの)データ'.

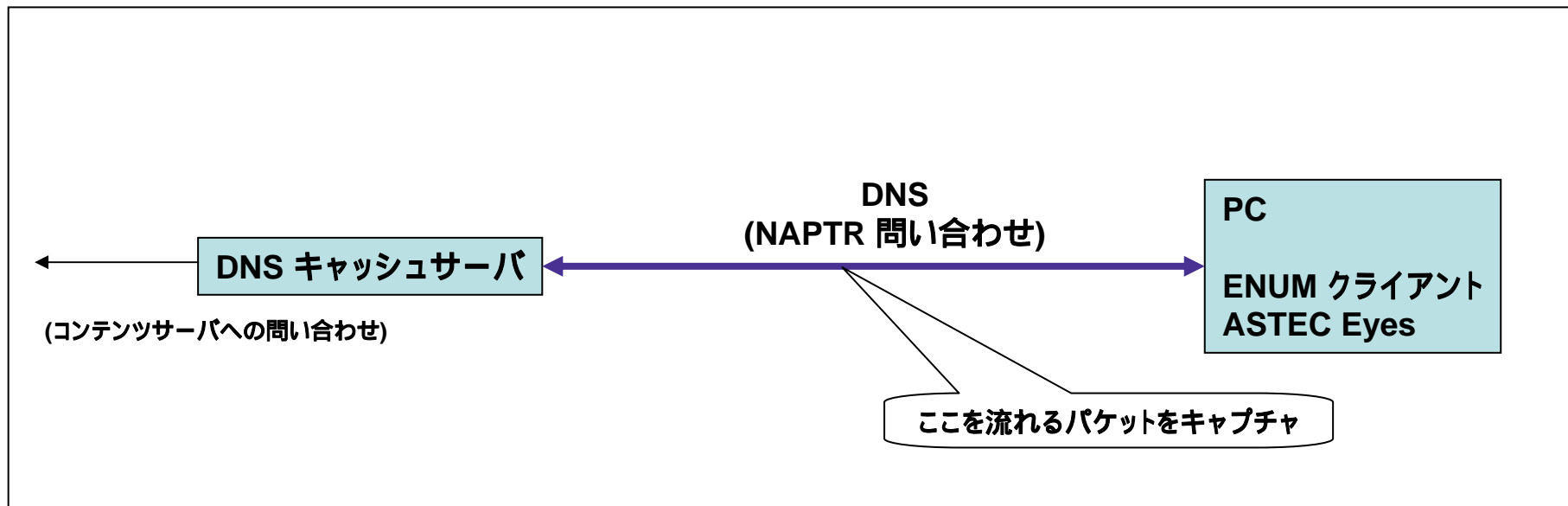
フ.	発信元...	受信先ア...	プ..	サマリ	長さ
17	dns-cache	enum-dns	DNS	Q ID=38913 OPCODE=0 RET=0 NAME=1.	98
18	enum-dns	dns-cache	DNS	R ID=38913 OPCODE=0 RET=0 NAME=1.	1514
19	enum-dns	dns-cache	IPv4	Fragmented Packet - No.18 Continuing Data	283
20	dns-cache	ns.e164.jp	DNS	Q ID=34874 OPCODE=0 RET=0 NAME=e164.jp T...	78
21	ns.e164.jp	dns-cache	DNS	R ID=34874 OPCODE=0 RET=0 NAME=e164.jp T...	1514
22	ns.e164.jp	dns-cache	IPv4	Fragmented Packet - No.21 Continuing Data	61
23	dns-cache	enum-client	DNS	R ID=1 OPCODE=0 RET=0 NAME=0.0.	156
24	E.ROOT-SER...	dns-cache	DNS	R ID=24580 OPCODE=0 RET=0 NAME=ns2.	405

Count of Labels: 3
 Original TTL: 180
 Signature Expiration: Sat Oct 02 08:30:00 2004
 Signature Inception: Thu Sep 02 08:30:00 2004
 Key Tag: 43736
 Signer's Name: e164.jp
 Signature: 128 octets
 51 E6 A7 5E 6E 8A 75 C2 F3 57 30 7E A2 C4 FE 61 D8 FE 5E B0 96 D2 9E
 FD 5B BE A3 CF 5B F8 24 6E 49 31 CE 6B 9C 7C 6E 83 9A 61 EF 28 D7 E5
 11 B9 AD 61 03 3E 53 A1 A6 9F 0E D1 0C C9 A7 AE 38 9D 10 4C 2D 1E CE
 45 97 67 09 FD FD B2 2D 97 F2 B6 3F 2A 71 01 E8 DE 76 DB 16 49 89 13

0x0770 = 1904
 実際には含まれていない
 (別のパケットの)データ

デモンストレーション

- JPRSのENUMクライアントでNAPTRレコードを検索する。
- 同時にASTEC Eyes でキャプチャし、DNSのパケットをデコードする。



おわりに

- ASTEC Eyes の評価版
 - <http://www.asteceyes.com/EVALUATION/>
現在のリリースにはENUM関連の実装は含まれません。
(ご希望の方は info@asteceyes.com にご連絡ください)
- ご意見やご希望など、お待ちしております
 - すぐに実装に反映できます。
- 謝辞

この報告を行うためにご協力いただいた方々に感謝いたします。
早稲田大学工学部の後藤先生と研究室の杉田様。
ETJP事務局の前畑様
ありがとうございました。