ドメインネームサービス

大東文化大学 経営学部 水谷正大

Masahiro Mizutani

インターネット通信の原則

- IPパケットを相手先コンピュータに送る
- 各コンピュータにIPアドレスを付与
  - 宛先指定にはIPアドレスだけを使う
    - IPアドレスはIPパケットのヘッダに書込まれる
    - IPv4：32桁の0-1列、IPv6：128桁の0-1列
      - 大東WebサーバのIPアドレス：192.47.204.101
- インターネットに流される情報には、IPアドレス以外に相手を指定する情報はない

通信相手のaddressing

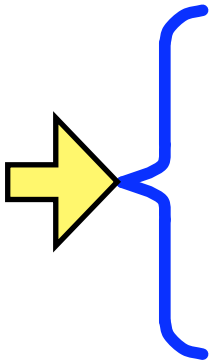
- コンピュータにとってはIPアドレスは便利
- 人間がIPアドレスを使うのは不便すぎる
  - 実際、メールアドレスにIPアドレスは現れない

DNS { コンピュータに名前をつける命名法
　　名前利用のための仕組みと動作

Domain Name System

ドメインの階層化とDNS名

- 各ネットワーク組織は、各自のドメインをもつ
- さらにサブドメインに分割して名前を付けてもよい
  - daito.ac.jp



st.daito.ac.jp
ic.daito.ac.jp
jm.daito.ac.jp

- 各ドメインにあるマシンに名前をつける
  - DNSホスト=host name.ドメイン名.親ドメイン名. … .TLD名
    - www.daito.ac.jp, www.google.com, www.yahoo.co.jp

URLに登場するDNS名

URL=スキーム + ホスト + ファイルへのパス

http://www.asahi.com/sports/baseball/index.html

スキーム

ホスト名

(//から最初の/まで)

IPアドレスで代用可能

ファイルへのパス

Webブラウザはホスト名をDNSに問合わせて

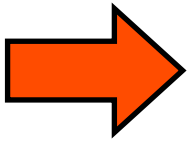
名前解決し、そのIPアドレスを知る

メールアドレスにも登場

メールアドレス = アカウント名 + ドメイン名

s11012345@st.daito.ac.jp

アカウント名　　**ドメイン名**



インターネットはIPアドレス通信が基本なのに

ドメイン名だけで何故メールが届くのか？

ドメイン名の階層構造

日本 jp のSLD名

SLDの種別	名称
高等学術機関	ac
政府機関	go
会社	co
ネットワーク組織	ne
法人	or
管理組織	ad

他にもある

トップレベルドメイン名

国・地域	名称	一般	名称
南極大陸	aq		org
日本	jp		edu
韓国	kr		net
中国	cn		biz
台湾	tw		com
バングラデッシュ	bb		gov
モンゴル	mn		info

他のタイプのTDL名もある

名前のつけ方

- 階層的にネットワークをドメインに分割
- TLD(**Top Level Domain**)
  - ccTLD: jp kr, cn, tw, bb, mn など
  - genericTLD: com, net, org, edu, biz など
  - TLDはICANNが管理している
- SLD(Second LD)
  - TLDを分割してTLDのサブドメインとしての名前
  - 日本ではICANNが社団法人JPNICにjpを管理業務委託
    - ac.jp, co.jp, ne.jp , go.jp, or.jp など
  - 3rdLD
    - SLDを分割し、SLDのサブドメインとしての名前
      - daito.ac.jp, docomo.ne.jp など

Top Level Domain（1）

2011年までは、255のcountry codeTLDを除くと以下の23件

generic TLD	sponsored TLD
.BIZ	.AERO
.COM	.ASIA
.INFO	.CAT
.NAME	.COOP
.NET	.EDU
.ORG	.GOV
.PRO	.INT
	.JOBS
infrastructure	.MIL
.ARPA	.MOBI
	.MUSEUM
	.POST
	.TEL
	.TRAVEL
	.XXX

最初から
2000年11月
2005年4月
2005年6月
2006年5月
2006年10月
2009年12月
2011年3月

Top Level Domain（2）

2012年から新gTLDを積極的に求めるように方針変更
要項と要件を明文化して有料で募集

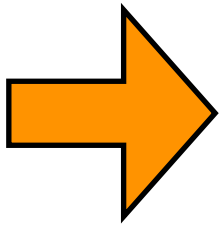
現在のgTLD一覧

http://www.iana.org/domains/root/db

DNSというインターネットの基本サービスの役割

名前の解決

- DNS(Domain Name System)
- ドメイン名からIPアドレスへの変換
- IPアドレスからドメイン名への逆引き
- メールサーバの通知



DNSサーバ（**ネームサーバ**）の集合体が
分散・協調してDNSサービスを実現

DNSドメイン名システム

- コンピュータ名とIPアドレスの対応を付ける仕組
- 名前の解決：　**名前 ⟺ IPアドレス**
- DNSサーバ：名前解決のために用意されたサーバ
- DNSサービス
  - ドメイン名とIPアドレスの対応問合わせサービス

名前解決の手順

1. アプリケーション（Webブラウザやメールソフトなど）がレゾルバ(resolver)に問合わせを委託
   - 名前解決のプロトコル
2. レゾルバは指定のDNSサーバに問い合わせ
3. 指定のDNSサーバが解決できない場合、指定のサーバは別のDNSサーバ群への問合わせ（再起検索）を繰り返して
4. 名前解決した応答を指定のDNSがアプリに返す
5. アプリケーションは目的のマシンにIPパケットにメッセージを載せて送信

ホストの resolv.conf ファイル

自ホストが常に参照するDNSサーバ（指定DNSサーバ）のIPアドレス情報が記載されている

Windowsの場合

C:\WINDOWS\system32\drivers\etc\resolv.conf

MacOSの場合

/etc/resolv.conf

名前解決コマンド nslookup

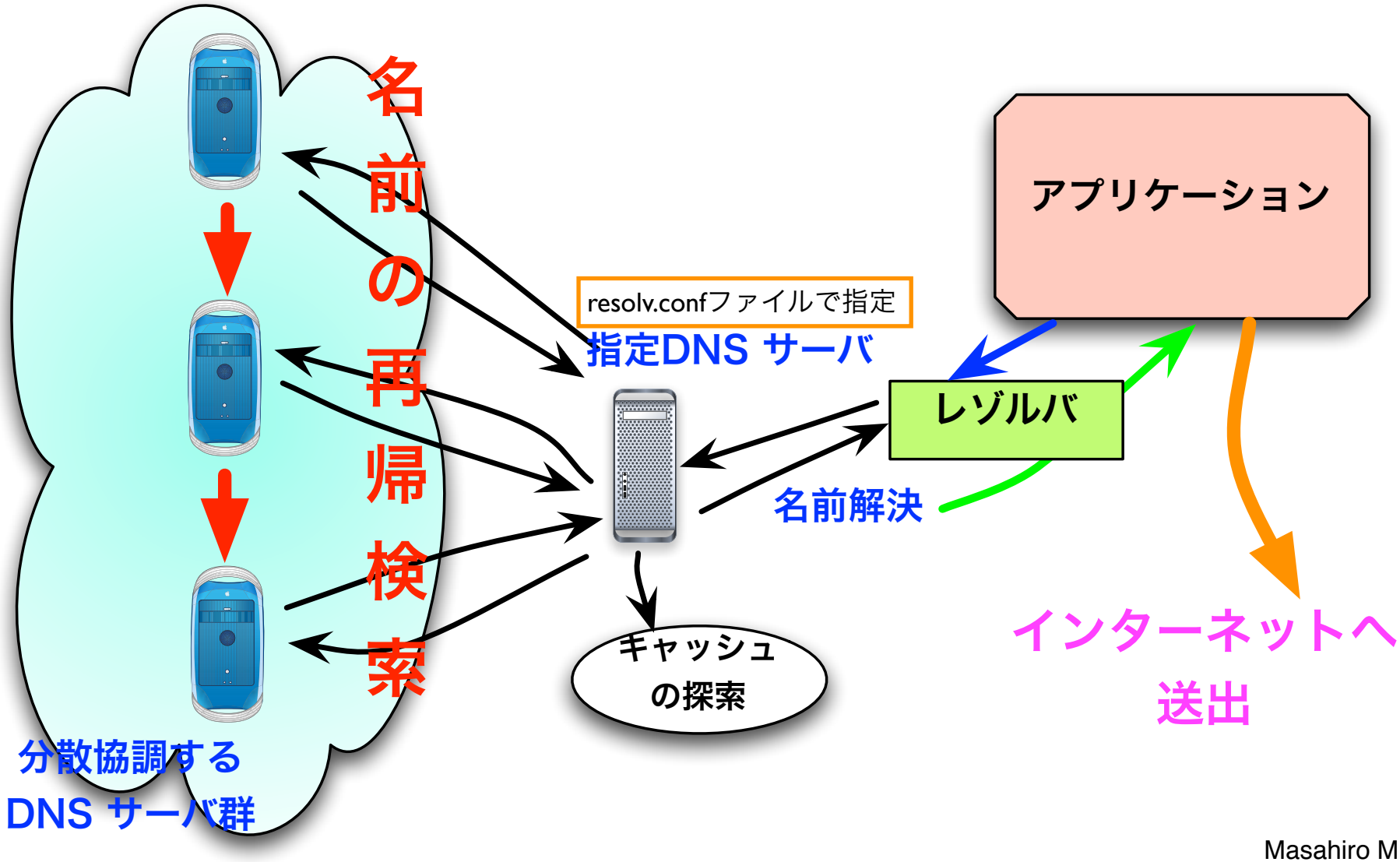
```
% nslookup www.kantei.go.jp
Server:     8.8.8.8
Address:    8.8.8.8#53

Non-authoritative answer:
Name:   www.kantei.go.jp
Address: 202.232.75.151
```

<= 名前解決を問い合わせたDNSサーバ

<= 問い合わせたDNSサーバから
直接得られた結果でないの意

DNSサーバの役割(I)

DNSサーバ群との協調による名前解決



指定ドメインで稼働している名前サーバを知る

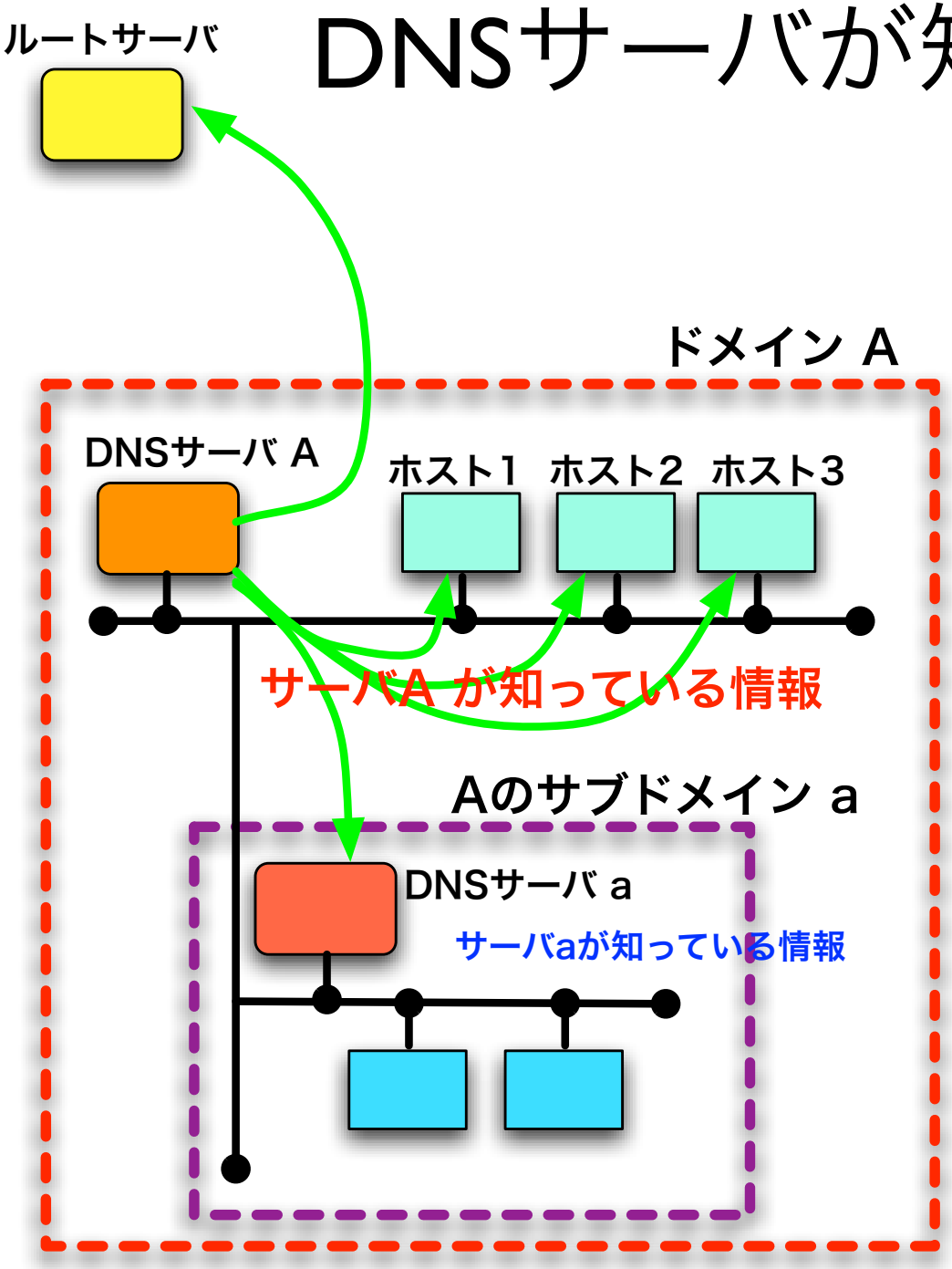
コマンド **nslookup** にドメイン名を指定、**-q=ns** をオプション指定して
Name Serverを問い合わせ

```
% nslookup -q=ns docomo.ne.jp
Server:     8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
docomo.ne.jp nameserver =
ns002.docomo.ne.jp.
docomo.ne.jp nameserver = ns001.docomo.ne.jp.
```

DNSサーバが知っている情報（1）

- 各ドメインごとに原則１つ以上のDNSサーバ
- どんなDNSサーバもルートサーバのIPアドレスを知っている
- DNSサーバは自ドメイン内の情報だけを保持
  - ドメイン内ホストのIPアドレスとDNS名の対応
  - 配下のサブドメインにあるDNSサーバ情報
  - ドメイン内のMXレコード

DNSサーバが知っている情報（2）



ドメインA内のDNSサーバの情報

- 自ドメインの直接配下にあるホスト
- 自ドメインが含むサブドメイン内のDNSサーバa
- ルートサーバの場所

サブドメインa内のDNSサーバ情報

- 自ドメインの直接配下にあるホスト
- ルートサーバの場所

DNSサーバの分散協調性

- レゾルバから最初に問合せされるDNSサーバ
  - ルートサーバのIPアドレスと自ドメイン内の情報だけを知っていればよい
- 各ドメインに位置するDNSサーバの知識
  - 自身が管理するドメイン内情報
  - サブドメインのDNSサーバ名、だけ
- 自分が知らない名前は、まずルートに聞く
  - ルートから順次下位ドメインのDNSサーバをたどる
    - 下位ドメインを信頼（権限の委譲）
  - 直接にホスト情報を保持しているDNSサーバに到達

ドメイン名(DNS名)による管理

- ホストをドメイン名で管理
  - IPアドレスとの対応の仕組みを提供
- ドメインツリー
  - ドメイン名は ” .”で区切られ、階層的に管理
- DNSサーバの分散サービス
    - 管理を委譲されているゾーン内のホストのドメイン名とIPアドレスとの対応を知っている
- 各階層は、それ以下に含まれる下位ドメインを管理
  - 下位ドメイン内のホスト情報の問合先を知っている

nslookupでSOAレコードを知る

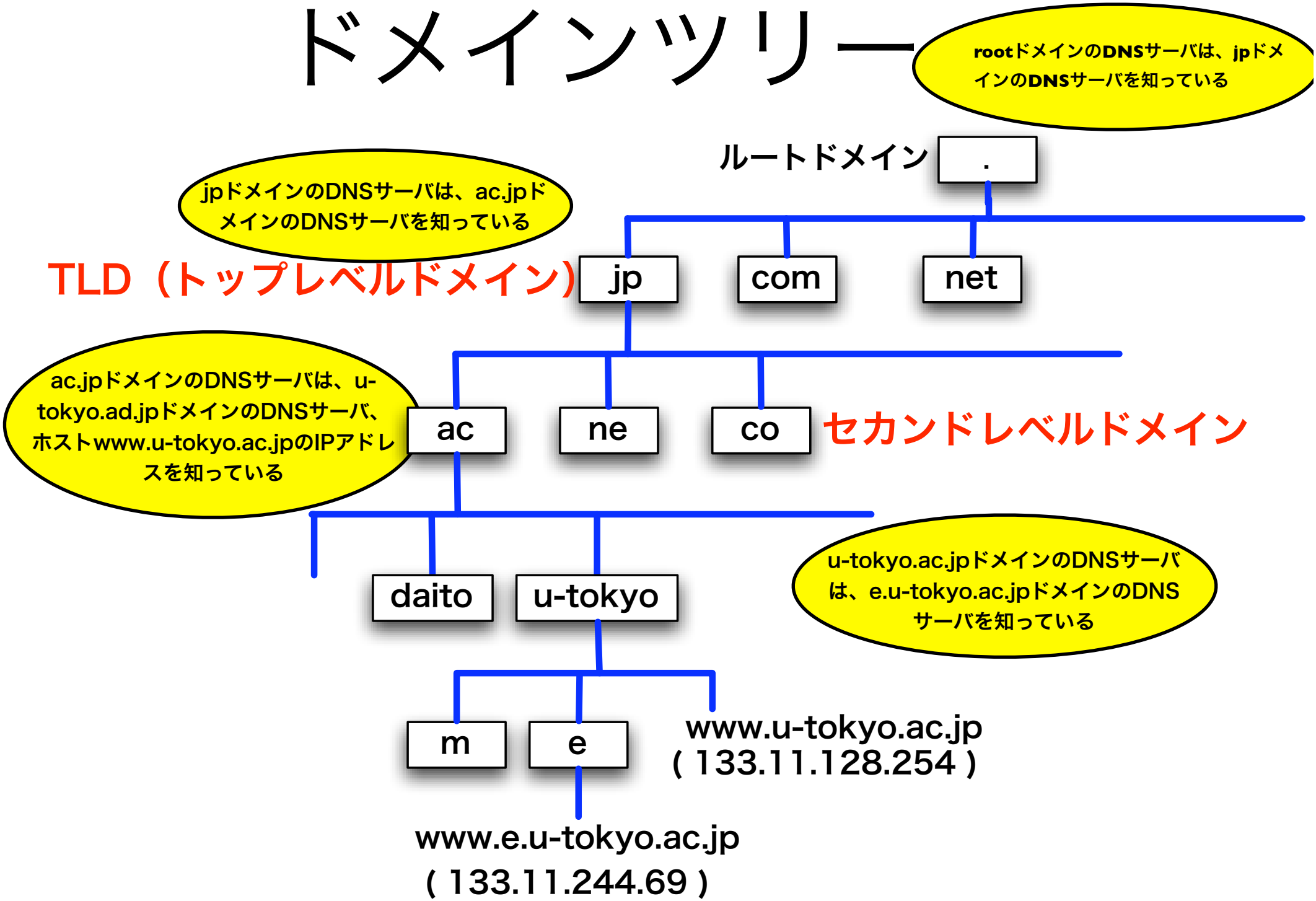
% **nslookup** -q=soa 指定ドメイン

DNSサーバの**SOA**(Start Of Authority)レコード

DNSゾーンの起点となる情報が記録されたレコード

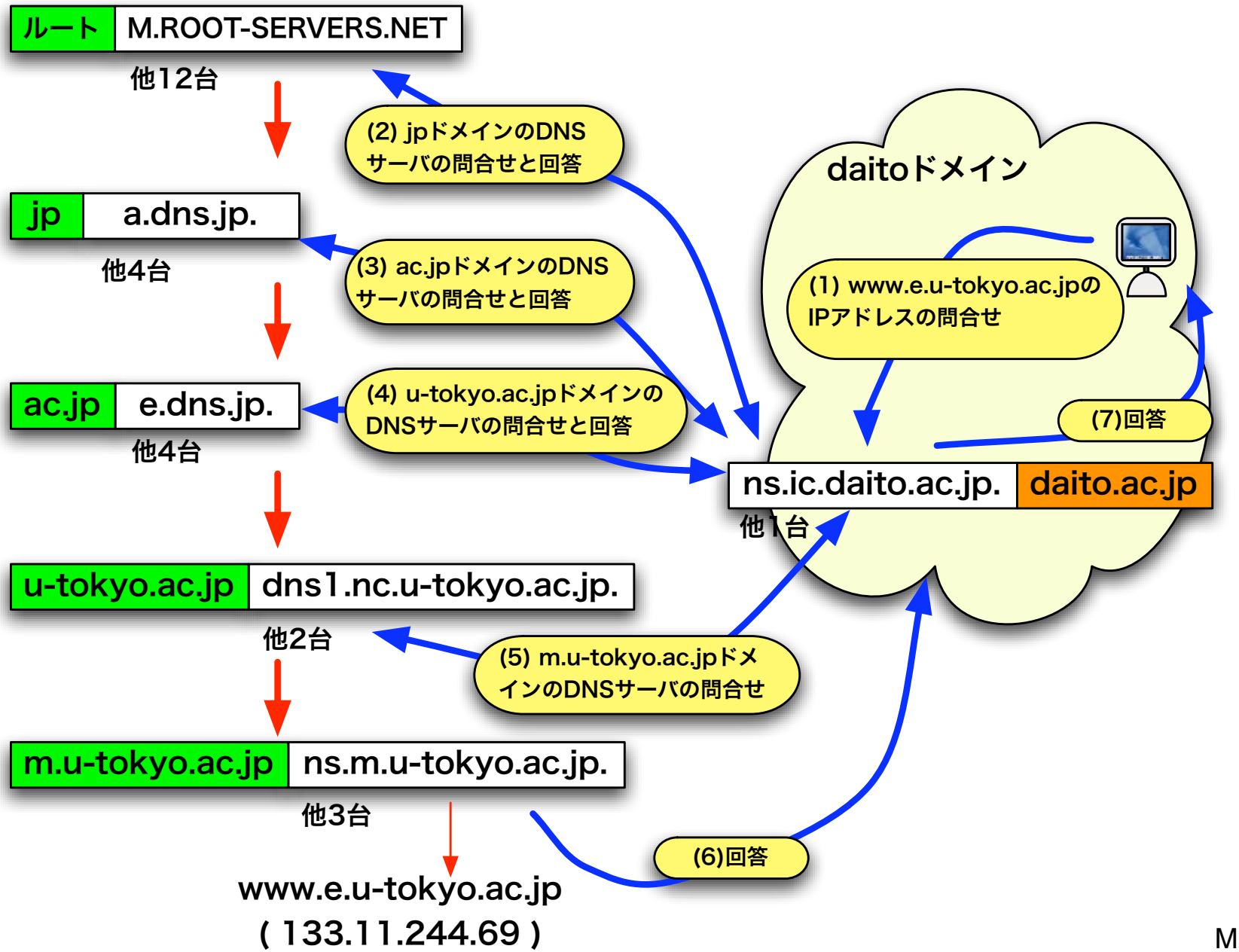
SOAにはDNS検索のためのネームサーバなど重要情報が格納されていて、クライアントはここに記録された情報から順番に辿ってドメイン内の各種レコード情報を取り出す

ドメインツリー



Masahiro Mizutani

DNSサーバの再帰探索



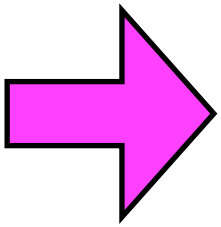
DNSサーバの役割(2)

メールサーバの通知

DNSサーバは、そのドメインで稼動しているメールサーバ(SMTPサーバ or Mail eXchangeサーバともいう)のホスト名およびそのIPアドレスの問い合わせに応じる

あるドメイン内のDNSサーバが保持する情報

ホスト名とIPアドレスの対応表だけでなく、MXレコードにそのドメインで稼動しているメールサーバ情報を記載



メールアドレス s987654321@st.daito.ac.jp だけで、何故メールが届くかの回答になっている

MXレコードの取得

nslookupにオプション -q=mx をつけて問い合わせる

```
$ nslookup -q=mx u-tokyo.ac.jp
Server:     8.8.8.8
Address:    8.8.8.8#53

Non-authoritative answer:
u-tokyo.ac.jp mail exchanger = 5 utmail2.nc.u-tokyo.ac.jp.
```

プレファンレンス値(preference)

小さなプレファンレンス値ほど優先度が高い

ルートネームサーバ

- 世界のDNSサービスの頂点にある
  - DNS名前解決探索の出発点
    - ローカル名前サーバが知らないと最初に尋ねる
  - 世界で13組織が管理（ミラーは多数ある）
    - アメリカ10台、ヨーロッパ2台、日本1台
      - WIDEプロジェクトがM.ROOT-SERVERS.NETを管理
- ルートサーバへの経路が無くなると解決不能
  - 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ルートサーバ管理組織

http://www.iana.org/domains/root/servers

ルートサーバ名	管理組織名	本拠地
A.root-servers.net	VeriSign Naming and Directory Services	US
B.root-servers.net	University of Southern California	US
C.root-servers.net	Cogent Communications	US
D.root-servers.net	University of Maryland	US
E.root-servers.net	NASA Ames Research Center	US
F.root-servers.net	Internet Systems Consortium	US
G.root-servers.net	U.S. 国防情報システム局	US
H.root-servers.net	U.S. 陸軍研究所	US
I.root-servers.net	Autonomica/Netnod	Sweden
J.root-servers.net	VeriSign Naming and Directory Services	US
K.root-servers.net	Reseaux IP Europeens -NCC	Netherlands
L.root-servers.net	ICANN	US
M.root-servers.net	WIDE Project	Japan

ルートネームサーバを増やせないか

結論：

現在のDNSプロトコルでは13台を越えて増やすことができない

理由：

DNS通信は応答速度を重視して（信頼性の落ちる）UDPパケットを使う。UDPで運ばれるメッセージは512バイトに制限されている(RFC1035 4.2節)ために、ネームサーバのリストを13個までしか通知できない。

ルートドメインのsoa照会

ルートネームサーとIPアドレスのリストが返る

```
% nslookup -q=soa .
Server:         133.99.161.3
Address:        133.99.161.3#53

Non-authoritative answer:
.
        origin = a.root-servers.net
        mail addr = nstld.verisign-grs.com
        serial = 2013052301
        refresh = 1800
        retry = 900
        expire = 604800
        minimum = 86400

Authoritative answers can be found from:
.       nameserver = j.root-servers.net.
.       nameserver = k.root-servers.net.
.       nameserver = l.root-servers.net.
.       nameserver = m.root-servers.net.
.       nameserver = a.root-servers.net.
.       nameserver = b.root-servers.net.
.       nameserver = c.root-servers.net.
.       nameserver = d.root-servers.net.
.       nameserver = e.root-servers.net.
.       nameserver = f.root-servers.net.
.       nameserver = g.root-servers.net.
.       nameserver = h.root-servers.net.
.       nameserver = i.root-servers.net.
a.root-servers.net      internet address = 198.41.0.4
a.root-servers.net      has AAAA address 2001:503:ba3e::2:30
b.root-servers.net      internet address = 192.228.79.201
c.root-servers.net      internet address = 192.33.4.12
d.root-servers.net      internet address = 199.7.91.13
d.root-servers.net      has AAAA address 2001:500:2d::d
e.root-servers.net      internet address = 192.203.230.10
f.root-servers.net      internet address = 192.5.5.241
f.root-servers.net      has AAAA address 2001:500:2f::f
g.root-servers.net      internet address = 192.112.36.4
h.root-servers.net      internet address = 128.63.2.53
```

```
% nslookup -q=soa .
```

DNSヘッダ

Question Section

Answer Section:
　SOAレコード

Authority Section:
　Name Serverリスト

Authority Record Section:
　Name ServerのIP address

このメッセージ全部がUDPメッセージ512バイト制限にギリギリ納まっている。14台を含めようとすると、UDPの制限を超えてしまう

DNSへの攻撃

サービス拒否(Deny of Service)攻撃

PCを乗っ取る/BOT感染させて大量のDNSパケットを送信して、処理能力をや回線を混雑、飽和、正常なサービスを妨害する

DNSキャッシュpoisoning攻撃

権威サーバからの連絡よりも先に偽の応答を返して、キャッシュとしてDNSサーバに偽の情報を保持させて、そのDNSサーバを利用するユーザに偽のWebサイトや偽の誘導を行う

DNSリフレクション攻撃

ゾーン転送要求による登録情報の収集

http://www.icann.org

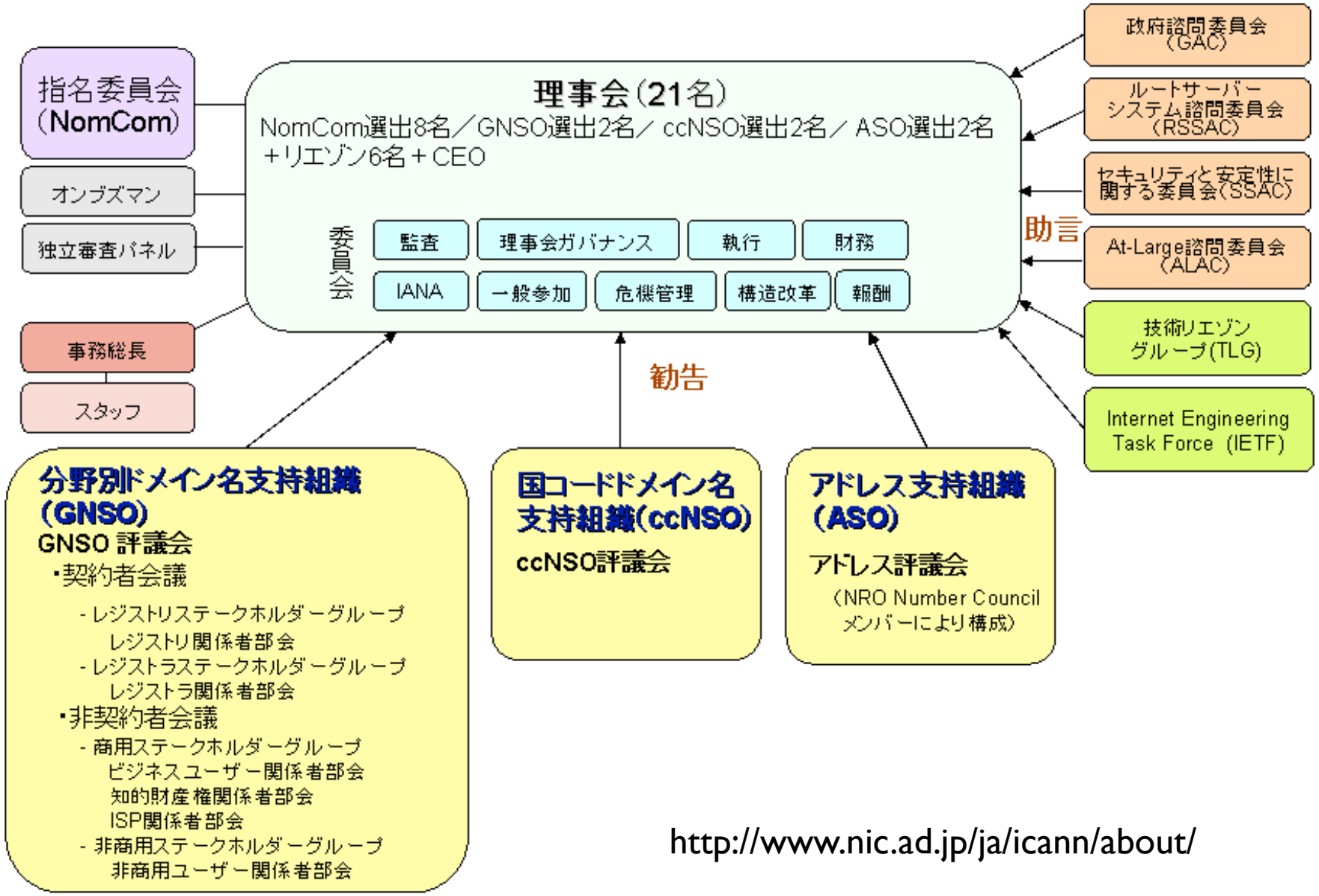
ICANN(Internet Corporation for Assigned Names and Numbers)

- 民間の非営利法人
  - 1998年10月に設立、クリントン政権時
  - 本拠地は米国カリフォルニア州
- インターネットの各種資源を全世界的に調整
  - TLDの決定・運営、IPアドレス・ポート番号ルートネームサーバのゾーン情報も管理
- gTLDはレジストラ・レジストリに管理委譲
- ccTLDは各国のネットワーク管理組織NICにICANNが管理を委譲

ICANNの具体的仕事

- 運用業務
- セキュリティ
  - DNSを構成するインフラストラクチャの各部分のセキュリティに関するポリシー調整
- ポリシー策定
  - gTLD登録に関するオープンなポリシー策定フォーラム
  - 米国政府のホワイトペーパーの指示
    - 安定性の維持、競争の促進
    - トムアップ的な参加の仕組み
    - 効率的な紛争処理手段の策定
    - 運用管理に対するアカウンタビリティ(説明責任)

ICANNの組織



http://www.nic.ad.jp/ja/icann/about/

レジストラとドメイン管理

- ICANNや各国NICがドメイン登録やDNSサーバの設定を行っている訳ではない
- ICANNなど管理機関の認定したレジストラが管理作業を代行
- ドメインレジストリ
  - レジストラがDNSサーバのゾーン情報登録時に使用するドメイン名登録用データベース
  - 複数のレジストラによって共有され、DNS登録情報の整合性を保つ
  - レジストリ：ドメインレジストリの管理者

ドメイン管理者を知るwhois

whoisとは ドメイン名、ネットワーク組織、AS番号の所有者を検索するためのデータベース問い合わせのプロトコル (RFC3912)

ドメイン名を管理するレジストリ組織がそのメンテナンス情報を提供している。日本ではwhoisサービスを分離して情報を提供している。

㈱**日本レジストリサービス**がドメイン名
http://whois.jprs.jp/

(社)**JPNIC**がIPアドレスおよびAS番号
http://www.nic.ad.jp/ja/whois/

技術的トラブルのための連絡情報だけでなく、**レジストリへの申請者**が必要とする情報提供、ドメイン名と商標などに関する**紛争解決**情報の提供、レジストリが適切に業務遂行しているか、など**ネットワークの円滑な運用**のためにwhoisを利用

課題

誰がドメインを持っているかプライバシー情報を本来の目的を逸脱した利用も広がっている。偽名での登録や代行業者名義などwhoisの役割を果たせない場合もある。

http://whois.jprs.jp/

JPRS whoisにドメイン nhk.or.jp を問い合わせる

jPRS jprs.jp に戻る

WHOIS

English ◀ BACK

このWHOISサービスはJPRSが 提供するドメイン名登録情報検索サービスです。

ご利用にあたっては、以下の規定をご覧ください。
→ JPドメイン名登録情報等の公開・開示に関する規則
→ gTLD等ドメイン名登録情報等の公開・開示に関する規則

詳しい使い方は「 JPRS WHOIS ご利用ガイド」をご覧ください。
WHOISについての一般的な説明は「 Whoisとは？」をご覧ください。

検索タイプ　　検索キーワード

ドメイン名情報　nhk.or.jp　検索

```
Domain Information: [ドメイン情報]
a. [ドメイン名]                NHK.OR.JP
e. [そしきめい]                にほんほうそうきょうかい
f. [組織名]                    日本放送協会
g. [Organization]              NHK (Japan Broadcasting Corporation)
k. [組織種別]                  特殊法人
l. [Organization Type]         Organization
m. [登録担当者]                SS8035JP
n. [技術連絡担当者]            SS8035JP
p. [ネームサーバ]              ns.nhk.or.jp
p. [ネームサーバ]              ns1.iij.ad.jp
s. [署名鍵]
[状態]                         Connected (2014/03/31)
[登録年月日]
[接続年月日]
[最終更新]                     2013/04/01 01:27:21 (JST)
```

株式会社日本レジストリサービス Copyright© Japan Registry Services Co., Ltd.

Masahiro Mizutani