

ネットワーク構成運用論

2004/05/24

芸術情報設計学科

藤村 直美

インターネットに共通の資源

- IPアドレス
 - 世界中の計算機を一意に識別
 - 133.5.112.1
 - 202.26.222.129
- ドメイン名
 - 組織を表わす
 - design.kyushu-u.ac.jp
 - kyushu-id.ac.jp
 - mit.edu

IPアドレスの管理組織

- グローバルIPアドレスはIANA (Internet Assigned Numbers Authority) が管理
- IANAはISOCの下部組織
- 1998年以降はICANNに移行した
- アジア・太平洋地区はAPNICが担当
- 日本国内はJPNICが担当

Internet Assigned Numbers Authority

- 南カリフォルニア大学情報科学研究所 (ISI) のJon Postel教授が中心となって始めたプロジェクトグループ
- ドメイン名、IPアドレス、プロトコル番号などのグローバルな管理
- その成果は、インターネット全体の共通資産という側面を多分に持ち、
- その運用は、インターネット的なボランティア精神を尊重している

Internet Assigned Numbers Authority(2)

- 運営費用の一部にアメリカ政府の研究予算が使われていたため「インターネットはアメリカ政府の投資によってできた」との主張の一つの根拠とされた
- 1998年10月に国際的な非営利法人ICANNが設立されてインターネットの管理体制が変化し、
- 2000年2月にはICANN、南カリフォルニア大学、及びアメリカ政府の三者の合意により、IANAが行っていた各種資源のグローバルな管理の役割はICANNに引き継ぎ
- 現在IANAは、ICANNにおける機能の名称として使用

ICANN

- ドメイン名や IP アドレスなどの世界的な調整 (トップレベルドメインの新設やドメイン名に関する世界的な方針の調整・策定など)
- 「the Internet Corporation for Assigned Names and Numbers」の略。(ドメインネームとIPアドレスの割り当てに関するインターネット法人)
- <http://www.icann.org/>

ICANN(2)

- ドメイン名、IPアドレス、プロトコル、ルートサーバなどのインターネットの基盤となる資源に関する技術的調整を行うために1998年にアメリカ合衆国で設立された民間の非営利法人
- 1998年9月までは、米国政府との契約に基づき、IANA(Internet Assigned Numbers Authority: 故ジョン・ポステル氏を中心とする南カリフォルニア大学の機能)がIPアドレスの割り当て、ドメイン名の調整を実施 (<http://www.nic.or.jp>)



<http://www.nic.ad.jp/ja/ip/basics.html>

IPアドレス

- 世界中の計算機を一意に識別
 - IPv4は32ビット
 - 43億個に割り当て可能
 - 8ビットずつ、4つに分けて表示
202.26.222.128
- 11001010 00011010 11011110 10000000
- クラスに分けて割り当て

IPアドレスのクラス

- A (0.x.x.x-127.x.x.x, 126, 16777214)
- B (128.0.x.x-191.255.x.x, 16383, 65534)
- C (192.0.0.x-223.255.255.x, 2097151, 254)
- D (224.0.0.x-239.255.255.x)
(マルチキャスト)
- E (240.0.0.x-255.255.255.x)
(実験用)

ネットワークアドレスとホストアドレス

- IPアドレスはネットワークアドレスとホストアドレスで構成
- 論理的にまとまりがある計算機の集合
- ネットワークアドレスはIPアドレスの上(左)の部分で、ネットワーク全体をあらわす
- ホストアドレスはIPアドレスの下(右)の部分でホストをあらわす



クラスによるIPアドレスの構成



サブネット

- 従来はクラスA、B、Cが単位
 - 133.22.0.0
 - 202.26.208.0
- ホスト部をさらに分割して使用 サブネット2ビットなら00、01、10、11の4つ
 - より細かなネットワークを構築可能
アドレスの無駄をなくす
- 現在は任意のビット長で実現 (CIDR)
 - クラスC × 16 を束ねると202.26.208.0/20

2ビットのサブネット

- 00 000000 - 111111
- 01 000000 - 111111
- 10 000000 - 111111
- 11 000000 - 111111

202.26.208.0	11001010 00011010 11010000 00000000
202.26.209.0	11001010 00011010 11010001 00000000
202.26.210.0	11001010 00011010 11010010 00000000
202.26.211.0	11001010 00011010 11010011 00000000
202.26.212.0	11001010 00011010 11010100 00000000
202.26.213.0	11001010 00011010 11010101 00000000
202.26.214.0	11001010 00011010 11010110 00000000
202.26.215.0	11001010 00011010 11010111 00000000

特別な意味を持つIPアドレス

- ホスト部が全部0
 - サブネットワークを表す
 - 202.26.208.0、133.5.0.0
- ホスト部が全部1
 - ブロードキャストアドレスと呼ぶ
 - 同じネットワーク内のすべての計算機と通信
 - 255.255.255.255をローカルブロードキャストアドレス
 - 202.26.222.255をダイレクトブロードキャストアドレス

ブロードキャスト

- 同じネットワーク上の全ての計算機に同報
- 全ビット1
- ルータを越えることができない
 - 自動設定を行うDHCPなどブロードキャストに依存するソフトウェアはサブネットを越えることはできない
 - Windows固有のブラウザでも不具合

IPアドレスと経路制御

- クラスBを配布でアドレス不足
133.22.0.0 202.26.208-223.0
- クラスCを配布で経路制御の情報爆発
- メモリの不足で通信不能組織が出る
- CIDR (Classless Inter-Domain Routing)
 - アドレスの階層的な割り当て
 - 経路情報の集成
- 政治的、経済的、性能的選択

CIDR (Classless InterDomain Routing)

- 従来の8ビット単位のネットワークアドレスから任意のビット長のネットワークアドレス
 - 202.26.213.0は202.26.213.0/24
 - サブネットにすると202.26.213.0/28など
 - クラスCを16個で202.26.208.0/20
- 適当な経路情報を束ねて集約可能
- クラスA相当のクラスレス割り当てを実施
<http://www.ripe.net/docs/ripe-155.html>

プライベートアドレス

- RFC1597で規定
- クラスA = 10.0.0.0(1個)
- クラスB = 172.16.0.0 ~ 172.31.0.0(16個)
- クラスC = 192.168.0.0 ~ 192.168.255.0(256個)

プライベートアドレス(2)

- プライベートアドレスは特定のLAN内では一意
- 他のLANには同じプライベートアドレスがあるかもしれない
- 外のインターネットと通信するにはグローバルアドレスを使用する
- プライベートアドレスとグローバルアドレスの変換(NAT、IPマスカレード)

NATとIPマスカレード

- NATでは
 - ヘッダー内のソースアドレスとデスティネーションアドレスをプライベートIPアドレスとグローバルIPアドレスで必要に応じて置き換える
 - これだけだとルータが持っているグローバルIPアドレス数しか通信できない
- IPマスカレードでは
 - 複数のプライベートIPアドレスに一つのグローバルIPアドレスを割り当て
 - 送信元と受信先のそれぞれのポート番号も併せて使用して識別

DHCP

- Dynamic Host Configuration Protocol
- ネットワークパラメータを自動設定する
- IPアドレス、ネットマスクなどを動的に確保
- 割り当て方式
 - 動的割り当て(一時的)
 - 自動割り当て(新規導入)
 - 手動割り当て(ディスクレスWSなど)
- 認証、DNSとの連動の欠如 動的DNS

DHCPによるパラメータ

- IPアドレス
- サブネットマスク
- ブロードキャストアドレス
- デフォルトゲートウェイのIPアドレス
- ローカルのDNSサーバのIPアドレス
- プリンタサーバのIPアドレス
- ホスト名

DHCPの接続の仕組み

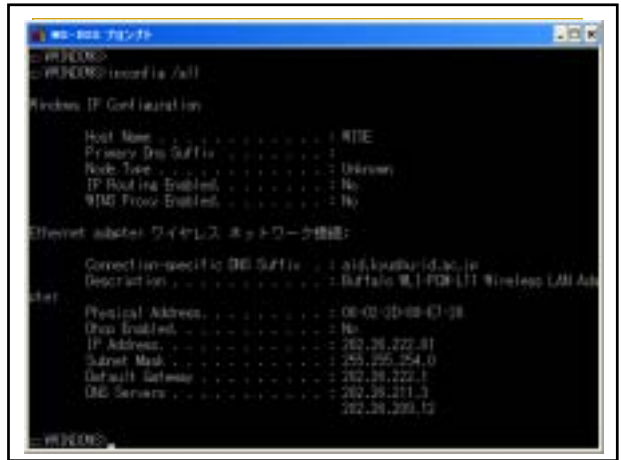
- クライアントがIPアドレスが欲しいというブロードキャスト
- DHCPサーバがIPアドレスを決めてクライアントに返事
- 受け取ったクライアントがサーバに使いたいと返事
- サーバがIPアドレスを確定してクライアントに返事

DHCPのアドレス割り当て方法

- 一定範囲のIPアドレスを請求に応じて割り当て
 - IPアドレスを有効利用することができる
 - 台数によっては割り当てできない可能性あり
- 特定のMACアドレスに決まったIPアドレス
 - IPアドレスを固定することができる
 - MACアドレスが登録されていない計算機にはIPアドレスを割り当てないこともできる
- 芸工大では2003年8月下旬からDHCPを導入

DHCPによるアドレスの特徴

- 割り当て有効期限がある
- 割り当て期限の半分以上を過ぎたら割り当て有効期限の更新を請求
- 割り当て期限内なら電源を切断して、再投入しても同じIPアドレス
- 割り当て期限を過ぎてから電源を再投入すると同じIPアドレスを請求しても、他に割り当てられている可能性あり



IPv4における問題

- ホスト数が激増してIPアドレス(IPv4)が枯渇
- 32ビットでは約43億個(地球人口約60億より少ない)
- 後、5分の1(約8億個)ぐらいしか残っていない
- クラスB、Cで小さいアドレスに移行
 - 経路制御表の増大
- 家電製品などをネットワークにつなぎたい
- セキュリティが考慮されていない
- ベストエフォート型である

IPv6

- 128ビット 沢山 (43億の4乗)
- 16進数で表示
2001:0000:0000:0000:0008:0800:200c:417a
2001::8:800:200c:417a
- 先頭ビットのパターンで用途を割り当て
- アドレスは階層化されていて、先頭32ビットでどのISPかわかる
 - 2001:240::/32はIJJ
 - 2001:260::/32はBIGLOBE
 - 2001:278::/32はODN

IPv6(2)

- 高いQoSの維持
 - 優先制御が明確に定義されている
- セキュリティ
 - 暗号化通信
 - 相手先の認証
- プラグアンドプレイ機能
- 現在、6Boneとして運用中
- 移行の問題
 - すべての計算機が対応するには時間がかかる

ドメイン名

- 世界中で組織を一意に識別
- 国別、組織の性格別
アメリカ, ntt.jp, ntt-data.jp, kek.jp
- 地域、個人、商標などによる取得
- 現在、改革中
 - ed, gr, 他

ドメイン名と管理組織

- gTLD (Generic Top Level Domain)
 - 国や地域の概念のない、世界中を対象としたドメイン名
- ccTLD (Country-Code Top-Level Domains)
 - 国別ドメイン名といわれ、2文字でそれぞれの国を表す
 - ccTLDの管理・運用はICANNから各国の管理団体(レジストリ)に委任

gTLD (Generic TLD)

- 世界中の誰もが登録できる「COM」、「ORG」、「NET」
- 一定の条件を満たすべき「EDU」、「GOV」、「MIL」、「INT」
- ICANNは2000年11月に「BIZ」、「INFO」、「NAME」、「PRO」、「MUSEUM」、「AERO」、「COOP」の7つの導入を決議(「INFO」を除けば一定の要件が必要)

ccTLD (Country Code TLD)

- ISO 3166のCountryコード(2文字)に基づき国や地域に割り当てられているトップレベルドメイン
- 例えば、日本は「JP」を使用
- 「KR(韓国)」、「NZ(ニュージーランド)」、「HK(香港)」、「UK(イギリス)」、「FR(フランス)」、「CA(カナダ)」、「US(アメリカ合衆国)」など

JPRS

- Japan Registry Service
- 2000年12月に設立、2002年4月からJPドメイン名管理の活動を開始
- JPドメイン名の登録管理
- DNSの運用
- whoisによる情報提供
- <http://jprs.co.jp/>

日本のドメイン名の種類

- 汎用JPドメイン名
 - 個人や組織で日本に住所があればよい
 - 漢字やひらがなもOK
- 属性型ドメイン名
 - 組織の種類ごとに区別されたもの
 - 1組織に一つ
- 地域型ドメイン名
 - 市町村名、都道府県名で構成

汎用ドメイン名

- 2001年2月から登録を開始したJPドメイン名
- 主な特徴
 - 「登録名.JP」の様に短いドメイン名
 - 1個人または1組織で複数のドメイン名を取得可能
 - ドメイン名に日本語を使用可能
 - 日本国内に在住する個人、または、拠点を置く組織であれば誰でも登録ができます。
- 制約緩和で、ドメイン名登録の自由度が高まった

属性型ドメイン名

- CO.JP: 一般企業
- OR.JP: 会社以外の団体
- NE.JP: ネットワークサービス
- AC.JP: 大学系教育機関
- AD.JP: JPNIC会員
- GO.JP: 政府機関
- ED.JP: 小・中・高校など主に18歳未満を対象とする各種学校
- GR.JP: 任意団体
- LG.JP: 地方公共団体

地域型ドメイン名

- 都道府県名、政令指定都市名、市区町村名を利用したドメイン名
 - 組織・個人が登録できる「一般地域型ドメイン名」
EXAMPLE.CHIYODA.TOKYO.JP
東京都千代田区に在住する個人が登録可能
 - 地方公共団体が登録できる「地方公共団体ドメイン名」
METRO.TOKYO.JP
東京都が登録できる地方公共団体型ドメイン名

ドメイン維持手数料

- ドメイン名の登録や維持に課金
- 汎用jpドメイン名では
 - 登録は14000円
 - 更新は7000円 / 年
- 属性ドメイン名では
 - 登録は5000円
 - 更新は3675円 / 年

DRP

- 「Dispute Resolution Policy」の略
- 特に説明がない場合は「ドメイン名紛争処理方針」の意味で用いられます。
- gTLD のドメイン名紛争解決方針としてはICANNが1999年に採択したUDRP
- 日本では2000年にJPNICによって制定されたJP-DRP

紛争処理手順(1)

- 被害を受けた人が紛争処理機関に申し立て
- 紛争処理機関は申し立てが条件を満たすか確認
 - 登録者のドメイン名が、申立人が権利または正当な利益を有する商標その他表示と同一または混同を引き起こすほど類似していること
 - 登録者が、当該ドメイン名の登録についての権利または正当な利益を有していないこと
 - 登録者の当該ドメイン名が、不正の目的で登録または使用されていること

紛争処理手順(2)

- 紛争処理機関は申し立てがあったことをドメイン名の登録者に通知、登録者は内容に相違があれば答弁書の形で回答
- 訴えた人からの申し立ての内容と、登録者の答弁書をもとに、紛争処理機関がそのドメイン名に対する裁定
- JPRS は、裁定に基づき、廃止や移転等の手続きを行う

ドメイン紛争の例 - J-Phone事件

- 1997年8月に大行通商(東京都港区)が「J-PHONE.CO.JP」を登録した
- 大行通商はアダルト・グッズや携帯電話関連用品を販売
- 2000年2月に訴訟
- 2001年4月、東京地裁で勝訴、12月に確定
- 2002年4月、日本知的財産仲裁センターに対してドメイン名移転を請求
- 6月11日、「移転裁定」の結果が通知され、7月2日に移転手続きが完了
- 現在はJ-PHONE.COM www.vodafone.jp

ドメイン紛争の例 - goo.co.jp

- 2000年11月にNTT-Xが工業所有権仲裁センターに対して、「goo.co.jp」の移転を求める申し立て(仕組みができてから初めての勝利)
 - goo(goo.ne.jp)の知名度と吸引力を利用して、アダルトサイトへの転送へ利用
- 有限会社ポップコーン
 - gooのサービスが始まる前(1996年8月)に登録と主張(検索gooは1997年2月)
 - 仲裁を不服として提訴
- 2002/11/29にNTT-Xが勝訴確定