Japan Registry Service

IP Meeting 2004
トピックスレポート
～DNS & レジストリ(IANA/RIR)～

2004年12月2日
株式会社日本レジストリサービス（JPRS）
森下泰宏
<yasuhiro@jprs.co.jp>

Copyright © 2004 株式会社日本レジストリサービス

Japan Registry Service

DNSこの1年

Copyright © 2004 株式会社日本レジストリサービス

Copyright © 2003 株式会社日本レジストリサービス

DNSにおける3大トピックス

- IP Anycast化がさらに進行
- ルートゾーンへのIPv6 AAAA glueの登録が可能に
- BIND以外のDNSサーバの実装が充実

Copyright © 2004 株式会社日本レジストリサービス

IP Anycast化

- ルートサーバへのDDoS攻撃対策が契機
  - 2002年10月の大規模なDDoS攻撃
  - 13台のルートサーバのうち7台が一時的にサービス不能な状態に陥り、2台が断続的に影響
  - DNSサービスへの影響はなかったが、危機感が高まる
- DNSではプロトコル上の制限により、指定可能なサーバが最大13(=13個のIPv4アドレス)までに制限
  - 従来の方法では、それを超える数のサーバを配置できない

Copyright © 2004 株式会社日本レジストリサービス

Copyright © 2003 株式会社日本レジストリサービス

IP Anycastとは

- インターネット上の特定のノード（インターネットに接続されているホスト）に対して割り当てられるIPアドレスを、特定のサービスに対して共通に割り当てるための技術
- RFC 1546により定義
- DNSへのIP Anycastの導入方法については、RFC 3258で記述
- DNSサーバにIP Anycastを導入することにより、1つのIPアドレスを複数のDNSサーバに対して割り当てることが可能になる
  - 指定するIPアドレスを増やすことなく、実際のDNSサーバの数を増やすことが可能になる
  - DoS攻撃のインパクトを分散することが可能になる
  - 特定ノードへの「封じ込め」「局所化」

Copyright © 2004 株式会社日本レジストリサービス

IP Anycastの導入状況(2004年11月24日現在)

- ルートサーバ (root-servers.net)
  - 13サーバ中6サーバで導入済
  - BGP Anycast: F(28)、I(17)、J(15)、K(10)、M(3)
  - IGP Anycast: C(4)
- JP DNSサーバ (dns.jp)
  - 6サーバ中2サーバで導入済
  - BGP Anycast: A(2: 東京、大阪)
  - IGP Anycast: D(4: 東京、大阪、米西部、米東部)

(カッコ内はそれぞれの分散ノード数)

Copyright © 2004 株式会社日本レジストリサービス

Copyright © 2003 株式会社日本レジストリサービス

IP Anycastの例1
(筆者自宅→I.root-servers.net)

東京に設置され、きわめて近くなった(Mとほぼ同様)

```
sgtpepper% traceroute i.root-servers.net
traceroute to i.root-servers.net (192.36.148.17), 64 hops max, 40 byte packets
 1  router (192.168.123.254)  0.241 ms  0.188 ms  0.200 ms
 2  tokyo03-f05.flets.2iij.net (210.138.170.151)  1.677 ms  1.412 ms  1.497 ms
 3  210.138.170.161 (210.138.170.161)  2.227 ms  2.461 ms  2.220 ms
 4  210.138.170.129 (210.138.170.129)  3.10 ms  2.486 ms  2.826 ms
 5  tky001bb01.IIJ.Net (210.130.143.197)  3.951 ms  2.759 ms  2.787 ms
 6  tky001ix03.IIJ.Net (210.130.143.51)  3.132 ms  2.550 ms  2.866 ms
 7  202.249.2.180 (202.249.2.180)  3.112 ms  3.419 ms  3.550 ms
 8  i.root-servers.net (192.36.148.17)  3.589 ms  3.348 ms  3.193 ms
```

Copyright © 2004 株式会社日本レジストリサービス

IP Anycastの例2
(筆者自宅→J.root-servers.net)

東京に設置されているはず

しかし、実際には太平洋を横断し、米国に、、、

```
sgtpepper% traceroute j.root-servers.net
traceroute to j.root-servers.net (192.58.128.30), 64 hops max, 40 byte packets
 1  router (192.168.123.254)  0.282 ms  0.193 ms  0.156 ms
 2  tokyo03-f05.flets.2iij.net (210.138.170.151)  1.671 ms  1.418 ms  1.526 ms
 3  210.138.170.177 (210.138.170.177)  2.466 ms  2.30 ms  2.105 ms
 4  210.138.170.133 (210.138.170.133)  2.249 ms  3.105 ms  2.151 ms
 5  tky001bb00.IIJ.Net (210.130.143.209)  5.294 ms  2.882 ms  2.379 ms
 6  paloalto-bb2.IIJ.Net (216.98.96.195)  98.315 ms  98.496 ms  98.14 ms
 7  PaloAlto-bb3.IIJ.Net (216.98.97.54)  98.332 ms  98.240 ms  98.747 ms
 8  sjc002bb00.IIJ.Net (216.98.96.153)  99.815 ms  99.974 ms  99.36 ms
 9  sjc002ix00.IIJ.Net (216.98.96.166)  99.875 ms  99.830 ms  99.946 ms
10  ge-1-3-0-103.edge1.SanJose1.Level3.net (209.245.146.193)  99.669 ms  100.112 ms  99.929 ms
11  so-1-2-0.bbr1.SanJose1.Level3.net (209.244.3.137)  100.385 ms  99.862 ms  100.468 ms
12  so-14-0.hsa3.SanJose1.Level3.net (4.68.114.154)  101.749 ms  102.271 ms  102.231 ms
```

(次ページに続く)

Copyright © 2004 株式会社日本レジストリサービス

Copyright © 2003 株式会社日本レジストリサービス

IP Anycastの例2 (筆者自宅→J.root-servers.net)

…さらに、再度太平洋を横断し、最終的に韓国のサーバに案内

```
13  KT-CORPORATI.hsa3.Level3.net (4.79.58.18)  102.318 ms  101.862 ms  102.307 ms
14  211.48.63.233 (211.48.63.233)  238.908 ms  239.15 ms  238.959 ms
15  218.145.63.225 (218.145.63.225)  238.883 ms  239.417 ms  239.182 ms
16  220.73.167.158 (220.73.167.158)  239.324 ms  239.108 ms  239.284 ms
17  218.147.227.5 (218.147.227.5)  249.22 ms  249.2 ms  248.603 ms
18   199.7.63.69 (199.7.63.69)  324.282 ms  297.429 ms  249.216 ms
```

- このように、
  - IP Anycastはルーティング状況/peering状況に強く依存
  - IP Anycastの導入により、このようなケースもありうる
  - 運用における今後の課題の一つ

Copyright © 2004 株式会社日本レジストリサービス

IP Anycastの例3 (IW2004会場→J.root-servers.net)

確認: IW2004会場→Jはちゃんと近い

```
$ tracert j.root-servers.net

Tracing route to j.root-servers.net [192.58.128.30]
over a maximum of 30 hops:

  1    3 ms    2 ms    2 ms  gr2k.iw2004.internetweek.jp [202.178.110.1]
  2    4 ms    3 ms    2 ms  202.178.109.129
  3    8 ms   10 ms   12 ms  202.178.96.249
  4   10 ms    7 ms   15 ms  notc-m10-01-ge-0-1-0.ipboot.net [202.178.96.18]
  5    8 ms    8 ms    6 ms  61.120.145.209
  6   15 ms    7 ms   13 ms  ge-7-1-2.a20.tokyjp01.jp.ra.verio.net [61.200.92.22]
  7    7 ms    7 ms    6 ms  61.120.146.14
  8    7 ms    7 ms    7 ms  203.173.67.3
  9    8 ms    7 ms    7 ms  j.root-servers.net [192.58.128.30]

Trace complete.
```

Copyright © 2004 株式会社日本レジストリサービス

Copyright © 2003 株式会社日本レジストリサービス

Japan Registry Service

ルートゾーンへのIPv6 AAAA glueの登録

- 2004年7月にIANAから“IANA Administrative Procedure for Root Zone Name Server Delegation and Glue Data”文書がリリース
  - IPv6 AAAA glueの登録を含む、ルートゾーンへの更新リクエストに対するIANAにおける処理手順・ガイドラインについて、初めて公式に言及
  - 「Doug Barton効果(後述)」の一つ
- これに従い、2004年7月21日のJP、KRゾーンを皮切りに、多くのTLDへのIPv6でのアクセスが実現

Copyright © 2004 株式会社日本レジストリサービス

Japan Registry Service

IPv6 glueの登録状況(2004年11月24日現在)

- 29のAAAA glueがルートゾーンに登録済
  - SEC3.APNIC.NET. (AE, AM, AU, CH, CL, HK, ID, KH, LI, PH)
  - NS0.JA.NET. (AN, GB, GG, INT, JE)
  - MERAPI.SWITCH.CH. (AR, CH, GP, LI, LU, PY, AERO)
  - NS2.UNIVIE.AC.AT. NS-US1.NIC.AT. (AT)
  - BRUSSELS.NS.DNS.BE. (BE)
  - NS-EXT.ISC.ORG. (CA, IL, NL, PH, PT, AQ)
  - DOMREG.NIC.CH. (CH, LI)
  - A.GTLD-SERVERS.NET. B.GTLD-SERVERS.NET. (COM, NET)
  - A.NIC.DE. (DE)
  - C.NIC.FR. B.NIC.FR. D.EXT.NIC.FR. (FR, NL, TF)
  - NS3.NS.ESAT.NET. (IE, TP)
  - NS6.IEDR.IE. (IE)
  - NS-SEC.RIPE.NET. (INT)
  - A.DNS.JP. D.DNS.JP. E.DNS.JP. F.DNS.JP. (JP)
  - G.DNS.KR. (KR)
  - NS2.DNS.PT. (PT)
  - NS.ATI.TN. (TN)
  - A.DNS.TW. C.DNS.TW. D.DNS.TW. (TW)
  - NS4.NIC.UK. (UK)

(カッコ内は対応するTLD)

Copyright © 2004 株式会社日本レジストリサービス

Copyright © 2003 株式会社日本レジストリサービス

BIND以外のDNSサーバ

- BIND以外のDNSサーバの実装が充実
  - NSD
  - ANS/CNS

Copyright © 2004 株式会社日本レジストリサービス

BIND以外のDNSサーバ - NSD

- NSD (Name Server Daemon)
  - オランダNLNet Labsで開発
  - “an authoritative only, high performance, simple and open source name server” (NSD公式Webページより)
  - DNSコンテンツサーバ機能に特化
    - キャッシュサーバ機能なし
    - ロギング・統計情報機能なし
  - DNSSECに対応 (Version 2.0.0以降)
  - ルートサーバK(RIPE NCC)、H(U.S. Army Research Laboratory)で使用
    - Kで2003年2月より運用開始
      - DNSサーバの多様性確保が主眼
    - その後Hでも運用開始

Copyright © 2004 株式会社日本レジストリサービス

Copyright © 2003 株式会社日本レジストリサービス

BIND以外のDNSサーバ - ANS/CNS

- 米Nominum Inc.の商用DNSサーバ
- ANS (Authoritative Name Server)
  - DNSコンテンツサーバ
- CNS (Caching Name Server)
  - DNSキャッシュサーバ
- 高性能・セキュリティ・DoS耐性強化が「売り」

Copyright © 2004 株式会社日本レジストリサービス

レジストリ(IANA/RIR)この1年

Copyright © 2004 株式会社日本レジストリサービス

Copyright © 2003 株式会社日本レジストリサービス

IANAをめぐる動き

- 「Doug Barton効果」
  - 2003年11月にDoug Barton氏がGeneral Managerに就任
    - 技術者出身
    - FreeBSDのcontributor/developer/committer
    - ICANN SECSACメンバー
    - 「IANAの顔」として、各コミュニティとの間の連携
    - フルタイムでIANA業務を統括
  - 一言でいうと「タフガイ」

Doug Barton氏
(58th IETF Meetingにて)

Copyright © 2004 株式会社日本レジストリサービス

Doug Barton効果

- この1年で、、、
  - IANAの「技術部分」の充実
    - ルートサーバへのIPv6 glueの登録開始
    - ルートゾーンのDNSSEC化の具体的な検討開始
  - ICANN meetingにおける技術部分の充実
    - DNS/DNSSEC 関連ミーティング・ワークショップ等
  - IANA業務の円滑化
    - 業務状況の透明化
    - 各種「業務キュー」の目に見える減少
- 技術者からみて、より「顔の見える組織」になりつつあるという印象

Copyright © 2004 株式会社日本レジストリサービス

Copyright © 2003 株式会社日本レジストリサービス

RIRをめぐる動き – AfriNIC正式発足

- 2004年10月11日にAfriNIC (African Network Information Center)が正式にICANNから認定、5大RIR体制に
  - APNIC (アジア太平洋地域)
  - ARIN (北米およびアフリカ南部(AfriNICに移行予定))
  - LACNIC (中南米およびカリブ海地域)
  - RIPE NCC (ヨーロッパ・中東・中央アジア・アフリカ北部(AfriNICに移行予定))
  - **AfriNIC** (アフリカ地域)

Copyright © 2004 株式会社日本レジストリサービス

RIRをめぐる動き - NRO

- NRO (Number Resource Organization)
- RIRの連合体として発足
- 技術・ポリシー上のコーディネーションを目的
- ICANNやASOの「置き換え」ではなく、いわば「対等の立場」「是々非々」でやっていこうという意思の現われ

Copyright © 2004 株式会社日本レジストリサービス

Copyright © 2003 株式会社日本レジストリサービス

参考リンク

- DNS技術情報
  - http://jprs.jp/tech/
- 【レポート】急速に進むDNSルートサーバーのAnycast化
  ルートサーバー間の国際協調が今後の課題に～RIPE Meetingから
  - http://internet.watch.impress.co.jp/cda/special/2003/10/03/633.html
- Root Server Technical Operations Association
  - http://www.root-servers.org/
- IANA | IANA Administrative Procedure for Root Zone Name Server Delegation and Glue Data
  - http://www.iana.org/procedures/delegation-data.html
- nlnetlabs.nl - Name Server Daemon (NSD)
  - http://www.nlnetlabs.nl/nsd/
- Nominum, Inc. :: Products Technology
  - http://www.nominum.com/products_technology.php?id=85
- Afrinic - African Region Internet Registry
  - http://www.afrinic.net/
- The Number Resource Organization
  - http://www.nro.net/

Copyright © 2004 株式会社日本レジストリサービス

Copyright © 2003 株式会社日本レジストリサービス