2014.04.18
JANOG33.5

APRICOT2014レポート

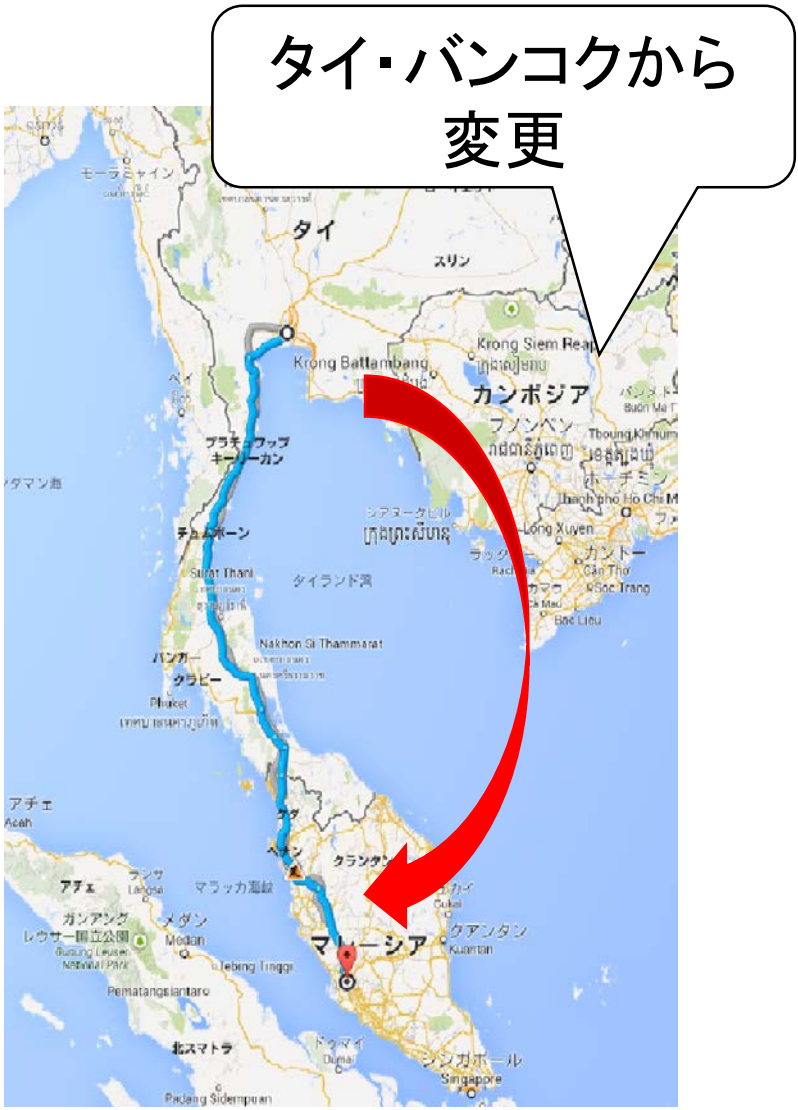
JPNIC　IP事業部・インターネット推進部
奥谷泉

一般社団法人 日本ネットワークインフォメーションセンター

カンファレンスの概要

- **開催期間:**
  - 2014年2月18日-28日
- **開催地:**
  - マレーシア・ペタリン ジャヤ
- **ローカルホスト:**
  - 今回なし
- **参加者:**
  - 466名(リモート参加262名)
  - 53カ国

https://conference.apnic.net/37/about



APRICOTとは

- **アジア太平地域のネットワークカンファレンス**
  - 技術的な教育、技術動向に関する議論等を実施
  - 地域全体の技術者が集まる機会であり、地域外からの参加も多い

- **APNICカンファレンスと併催、他APAC地域をベースに活動する各種フォーラムがセッション開催**

- **主催はAPIA：http://www.apia.org/**
  - 理事会のChair：Philip Smith、Vice-Chair：松崎吉伸

APRICOT
Asia Pacific Regional Internet Conference on Operational Technologies

https://www.apricot.net/

JPNIC

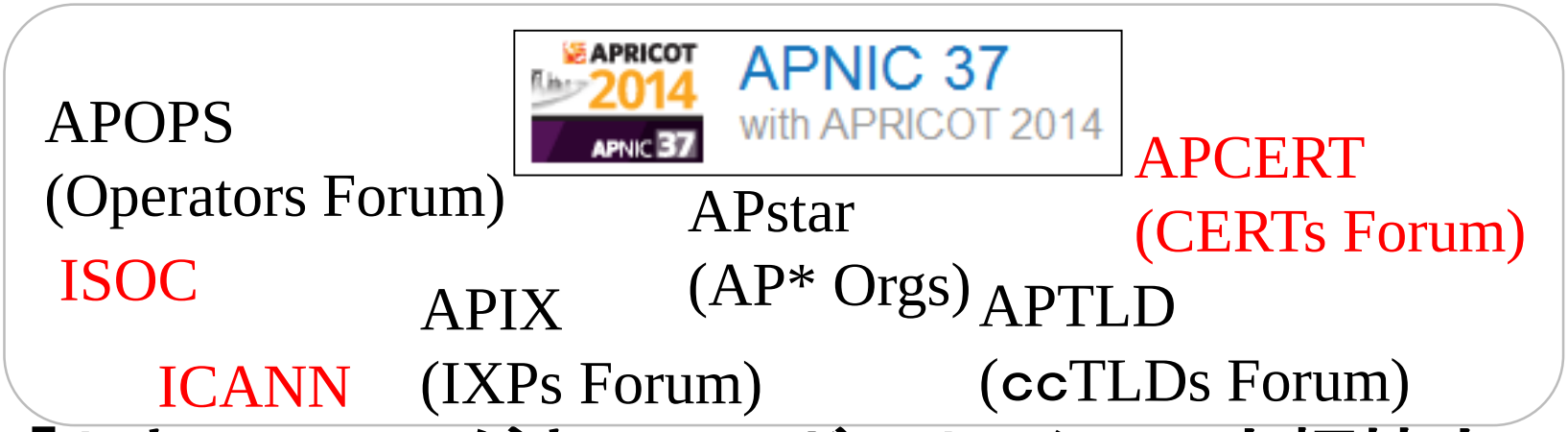
プログラム構成

- **18–23日：**
  - ハンズオン中心のワークショップ
  - APTLD、APIXなどメンバー限定セッション
- **24–28日：**
  - より幅広い参加者が集まる会議
    - 各種チュートリアル・ワークショップ
    - Asia Pacific Network Operators Forum （APOPS)
    - Peering フォーラム
    - 特定のテーマに関するセッション、Lightning Talks
    - 各種Special Interest Groups(SIG): Policy SIG、NIR SIG
    - 各種Birds of Feather(BoF)
    - レジストリアップデート(RIR、NIRなど)、NOGレポート
    - 開会・閉会セッション、APNIC総会

最近はチュートリアル・ワークショップに注力、メニューも充実

今回の特徴

- 新たな試みとしてAPCERT、ISOC、ICANN主催のセッション開催



- 「セキュリティ」がキーワードのセッション大幅拡大
- 「IPv6」に関するセッションはBoF以外なし
- BoFが充実：数多数、テーマも多様
- NOG方面では新設BDNOGから発表あり

今回議論された主なトピックス

- セキュリティ
- IX・Peering
- IPv6
- CGN
- IPv4
- ドメイン名・IPアドレスポリシー
- インターネットガバナンス

セキュリティ

- **APCERTとの連携**
  - ccTLDへの攻撃、WHOIS運用などにおいてAPTLDとしても連携していきたい
- **Open Resolver → NTP**
  - NTPについて対応の呼びかける発表 “NTP and Evil”
  - NTPをバージョンを4.2.7p26以降にアップグレード、ソースアドレスフィルタリング、BCP38の導入
  - ルータベンダー、OSごとの設定テンプレート紹介
- **JPの取組み紹介**
  - 日本におけるOpen Resolverへの対応
  - JANOGのNTP WG

“NTP and Evil” 発表資料 抜粋

Being Nice on a (cisco ios) Router

ios (recent 12.* releases)

```
access-list 46 remark utility ACL to bl
access-list 46 deny any
!
access-list 47 remark NTP peers/serv
access-list 47 permit 10.0.0.1
access-list 47 permit 10.0.0.2
access-list 47 deny any
!
! NTP access control
ntp access-group query-only 46   ! de
ntp access-group serve 46        ! de
ntp access-group peer 47         ! pe
ntp access-group serve-only 46   ! de
```

Being Nice on a (cisco xr) Router

ios

```
Ntp
serv
Serv
sour
upda
!
! loc
Ipts
flow
flow
!
! The
cont
man
 inba
 inte
 !!!
```

Being Nice on a (juniper) Router

juniper

This is a firewall filter fragment for a loopback filter which assumes a default permit

```
term ntp {
   from {
     source-address {
        0.0.0.0/0;
        /* NTP servers to get time from */
        10.0.0.1 except;
        10.0.0.2 except;
        }
     protocol udp;
     port ntp;
     }
   then {
      discard;
      }
   }
```

The alternative is to use a loopback default deny filter, in which case you would need the inverse form of the filter to accept NTP packets from the configured servers:

```
term ntp {
    from {
      source-address {
         10.0.0.1/23;
         10.0.0.2/32;
         }
      protocol udp;
      port ntp;
      }
    then {
       count ntp-requests;
       accept;
       }
    }
```

https://conference.apnic.net/data/37/2014-02-25-ntpddos_1392941955.pdf

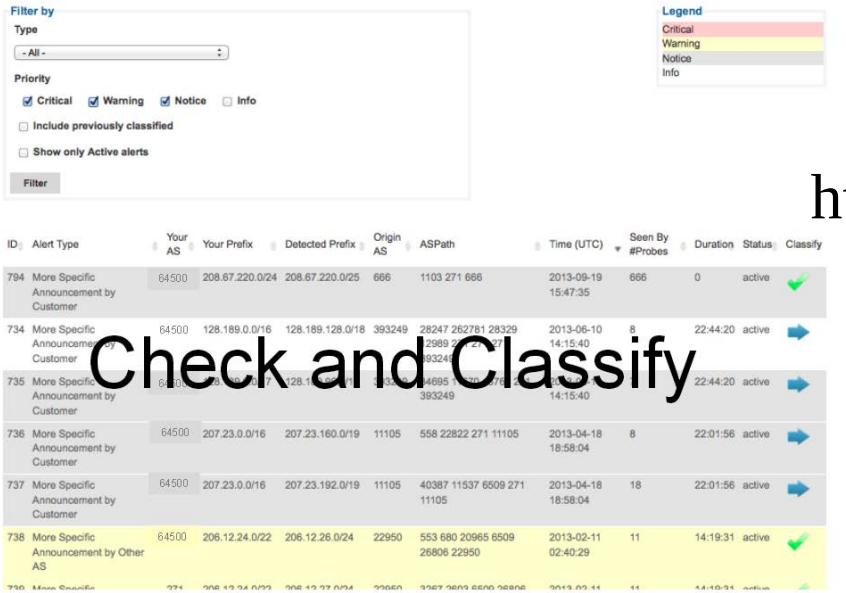
Peering・ルーティング

- APIX、Peering Forumなど情報交換・ネットワーキングの場は定着しつつある
- Geoff Hustonの発表：BGP in 2013
  - https://conference.apnic.net/data/37/2014-02-27-bgp2013_1392943641.pdf
- RPKI：日本の取組みを紹介、NZからRPKIの紹介
- ISOCでRouting Resiliency Surveyを実施
  - https://conference.apnic.net/data/37/201402-NetOps-Routing-Resilience-Survey.pdf

Routing Resiliency Survey

- BGPMONと協力し、サーベイ参加者ネットワーク特有のデータを提示
- AS番号と電子メールアドレスをrrs-admin@isoc.orgまで送れば協力可能

Evidence based risk analysis



Check and Classify

https://www.internetsociety.org/rrs/

IPv6

- **国単位での状況アップデートや計測情報の共有は定常化**
  - IPv6 Readiness Measurement WGは今後計測方法の共有、基準の統一を目指したい
- **NSDs (Network Security Devices) IPv6 Verification BoFは今回新しい**
  - セキュリティ機能が対応していないと導入の障壁
  - 対応機器の情報共有、仕様をまとめてベンダーに提示

NSDs (Network Security Devices) IPv6 Verification BoF

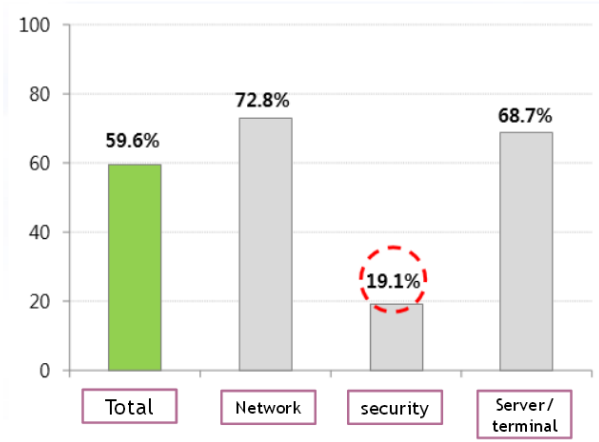
- FW : security effectiveness(4), network processing performance(6)

No.	Test factor	reference	Index(unit)
1	"allow all" policy configuration possible. And act normally.	NSS Labs	PASS/FAIL/NA
2	Simple outbound and inbound policies allowing basic browsing and email access for internal clients and no external access	NSS Labs	PASS/FAIL/NA
3	IPv4/IPv6 network interoperability	USGv6	PASS/FAIL/NA
4	Syn flood protection	NSS Labs	PASS/FAIL/NA

No.	Test factor	reference	Index(unit)
1	Throughput and latency with UDP varying packet size ※ both CPU, memory usage rate ※ every IPv4 / IPv6 mode	RFC 1242, RFC 2544, TTAS.KO-12.0044	Throughput(Mbps), Latency(㎲) CPU usage rate(%), usage rate(%)
2	Throughput and latency with UDP pac IPv4/IPv6 mixed mode		
3	Maximum concurrent session(CC) for specific response size ※ both IPv4 &		
4	Maximum Connections Per Secon varying response size ※ both IPv4 &		
5	Maximum Transactions Per Second(TPS response size and specific Get request pe ※ both IPv4 & IPv6 mode		
6	Application Average Response Time : I		

定義要件例

Telecommunication Device IPv6 Readiness Survey



Korean government telecommunication device ipv6 readiness : 60%,
Network, server, terminal are ipv6 supportable by OS upgrade.
But, about 80% of Security Device are need to replace ipv4 only devices with IPv6 enabled one.
(Nov/2010)

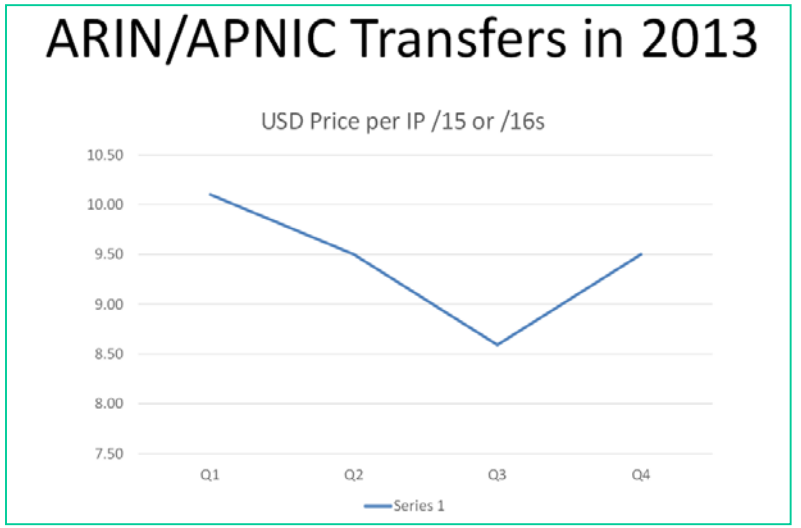
担当者： KISA のYoung Sun La (rays@kisa.or.kr)

CGN：Carrier Grade NAT

- CGNパネル
  - 利用可能/利用できない場合、導入事例、課題の紹介
  - CGNを導入してもIPv4枯渇問題は継続、IPv6の本格導入までの対応との見方、課題も認識したうえで導入
  - http://2014.apricot.net/program#session/66283

IPv4

- **他地域のIPv4在庫枯渇時期**
  - ARIN、LACNICが2014年中に枯渇する予測
- **IPv4アドレスの相場**
  - LTでブローカーから値段の紹介　/16～/15 約US$10
  - “Global IPv4 Transfer Market2013 Pricing Trends & 2014 Outlook”
- **IPv4アドレスのリース**
  - どう対応すべきかBoFで議論



https://conference.apnic.net/data/37/4-ipv4marketgrouppresentationapnic37v2_1393292152_1393488933.pdf

ドメイン名・IPアドレスポリシー

- **ICANNからgTLD関連のポリシー紹介・議論が新たな試み**
  - 新gTLD、IDNに伴う影響、gTLD WHOISの見直し・多言語化に向けた検討
  - https://community.icann.org/display/gseasiawkspc/Asia+Pacific+Regional+Discussions+–+APRICOT%2C+Feb+2014
- **アドレスポリシーは3点中2点は1.0.0.0/8関連**
  - コンセンサスが得られた提案は1点：APNICへの研究目的でのアドレス割り当て「1.0.0.0/24」、「1.1.1.0/24」
  - DNS anycast用のアドレス「1.2.3.0/24」の提案は会議後も議論が継続、最終的には提案者が取り下げ
  - IPv6のデフォルト初回割り振りサイズを、/32→/32～/29まで拡張する提案は継続議論

IPA

http://jpopf.net/Opinion%20collection%20meeting%20about%20proposal%20in%20APNIC%2037%20hosted%20by%20Policy-WG

インターネットガバナンス

- IANA機能に関するパネル実施
  - APNICが余計なことに労力をかけているとの議論にAPNIC総会およびAPNICのMLで発展
  - より効果的にコミュニケーションを行うべき、優先順位に基づいたコスト明確化を求める方向に議論が移り、現在新たな議論はない

- その後実際米国政府からIANA機能移管の発表あり
  - https://www.nic.ad.jp/ja/topics/2014/20140317-02.html
  - IAB、ISOCなどのコミュニティで議論が進んでいる
  - APNICでも専用ウェブサイトとMLが作成された

IANA oversight transition
http://www.apnic.net/community/iana-transition

IANAxfer （APNICのML)
http://mailman.apnic.net/mailman/listinfo/IANAxfer

詳しく知りたいと思ったら

- 後からセッションの様子を知ることもできる
  - 資料、セッション動画、トランスクリプト(発言録)をいつでも参照可能
  - プログラムページから、VideoやTranscriptへのリンクをクリック！
  - http://2014.apricot.net/program

オープニングセレモニー

APIA Chair
のスピーチ

タイの当初ローカル
ホストもスピーチ

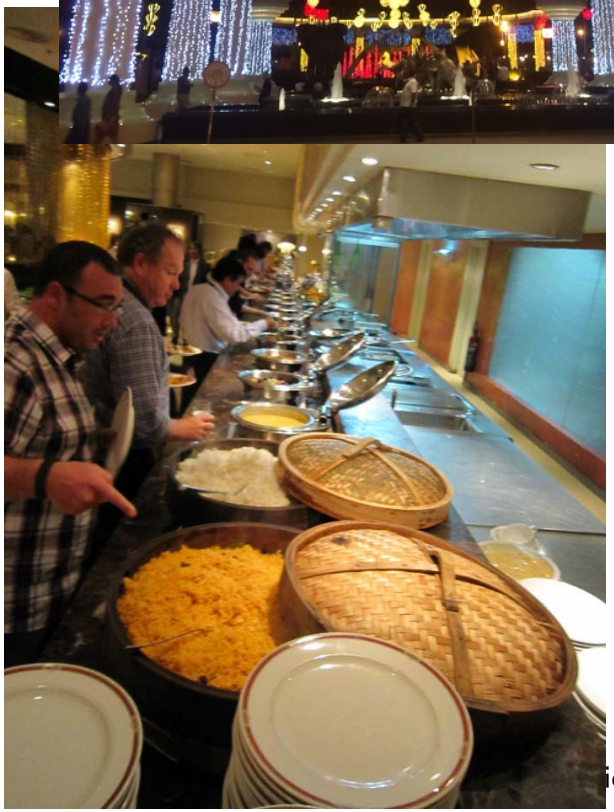
ダンスショー

会場の雰囲気

登録デスク

外観

休憩タイム



懇親会

ワークショップの様子： ISOC NetOPS

満席のため、床に座る参加者も

ポリシー関連のセッション

ICANNアップデート
セッション

ポリシーSIGでの
マイク順番待ち

APNICのCOO Sanjaya
APNICの運用について
共有@ポリシーSIG

2014.04.18
JANOG33.5

終わりに

最後に

- JPからの参加者にとっては地域内の他国の状況を理解してJPの立ち位置を知る/ネットワーキングの機会
- 発表しやすいので初の海外カンファレンスでの発表としては利用しやすい
- APRICOT2014の状況を＃でつぶやく試みを実施：今回広く告知しなかったがあるとうれしい？

謝辞
APRICOTに日本から参加したみなさんから
多くの情報を寄せていただきました。
ありがとうございました！

次回のAPRICOTは福岡開催

- APRICOT・APAN 2015 福岡 (2015/2/24～3/6)
  - APAN39とも併催
  - 英語サイト：https://2015.apricot.net/
  - 日本語サイト：http://apricot-apan.e-side.co.jp/

- スポンサーも募集中！
  - http://jp.apricot-apan.asia/files/sponsorship.pdf

APRICOT・APAN 2015

24 February - 6 March, 2015 Fukuoka, Japan

2014.04.18
JANOG33.5

参考情報

一般社団法人 日本ネットワークインフォメーションセンター

テーマ別テクニカルセッション・BoF

- テーマセッション
  - セキュリティ、CGN、DNS、基盤インフラ、インターネットガバナンス
- BoF
  - 災害時の緊急通信 (Disaster Emergency Communication)
  - ネットワークセキュリティ機器におけるIPv6対応 (NSDs (Network Security Devices) IPv6 Verification)
  - IPv4アドレスのリース (IPv4 Address Leasing)
  - 国別IPv6の状況およびIPv6対応状況の計測 (APIPv6TF and IPv6 Readiness Measurement)
  - ネットワークの不正利用 (Network Abuse)
  - Network Function Virtualization (NfV)
  - 情報通信業界での女性 (Women in ICT)

Women in ICT

チュートリアル・ワークショップトピックス

- ワークショップ
  - Intro to Routing、Advanced BGP、MPLS
  - Security
  - Network Management/Monitoring
  - ISOC NetOps Workshop（IPv6 Deployment、Security and Resilience、Collaboration and coordination）
- チュートリアル
  - Internet Resource Management
  - IPv6 in Mobile Networks
  - 464XLAT: Breaking Free of IPv4
  - BGP Multihoming 、Traffic Engineering、IRR Tutorial
  - Response Rate Limiting with BIND

DNS anycast用のアドレス「1.2.3.0/24」提案

- **施行された場合の懸念**
  - このアドレスは経路広告しないことが前提だが漏らす人は必ず出て、想定しないトラフィックを引き寄せる
  - 漏れた情報を意図的に集めて悪用されるとセキュリティリスクにつながる

- **ポリシーSIGでコンセンサス、その後APNIC総会で棄却**
  - ポリシーSIGに参加したオペレータが限られていた
  - 懸念があれば、最終的にコンセンサスに至る前に、反対して結果を変えることは可能

DNS anycast用のアドレス「1.2.3.0/24」提案

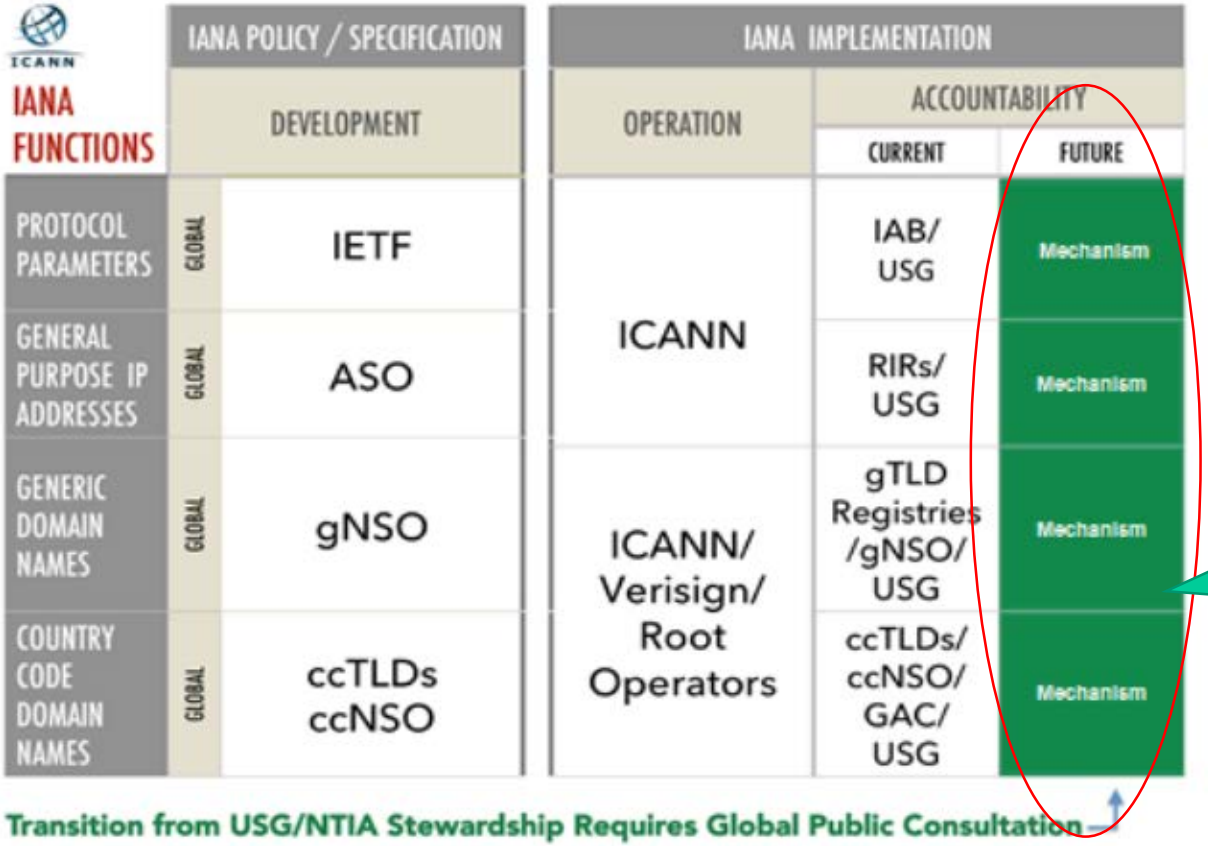
- ***To***: <sig-policy@lists.apnic.net>
- ***Subject***: Re: [sig-policy] New version of prop-110: Designate 1.2.3.0/24 as Anycast to support DNS Infrastructure
- ***From***: Job Snijders <job.snijders@hibernianetworks.com>
- ***Date***: Fri, 28 Feb 2014 14:33:56 +0800
- ***Delivered-to***: sig-policy@clove.apnic.net
- ***List-archive***: <http://mailman.apnic.net/mailing-lists/sig-policy/>
- ***List-help***: <mailto:sig-policy-request@lists.apnic.net?subject=help>
- ***List-id***: APNIC SIG on resource management policy <sig-policy.lists.apnic.net>
- ***List-post***: <mailto:sig-policy@lists.apnic.net>
- ***List-subscribe***: <http://mailman.apnic.net/mailman/listinfo/sig-policy>, <mailto:sig-policy-request@lists.apnic.net?subject=subscribe>
- ***List-unsubscribe***: <http://mailman.apnic.net/mailman/options/sig-policy>, <mailto:sig-policy-request@lists.apnic.net?subject=unsubscribe>
- ***Thread-topic***: New version of prop-110: Designate 1.2.3.0/24 as Anycast to support DNS Infrastructure
- ***User-agent***: Mutt/1.5.21 (2010-09-15)

```
Dear fellow networkers,

> A new version of the proposal "prop-110: Designate 1.2.3.0/24 as
> Anycast to support DNS Infrastructure" has been sent to the Policy SIG
> for review.
>
> Information about earlier versions is available from:
>
> http://www.apnic.net/policy/proposals/prop-110
>
> You are encouraged to express your views on the proposal:
>
> - Do you support or oppose this proposal?  - Is there anything in the
> proposal that is not clear?  - What changes could be made to this
> proposal to make it more effective?

I am a time traveller, just got back from 2016. In my time slice the
internet has become unusable due to ongoing gigantic amplification
attacks and security issues. Therefor I am here to warn you about
prop-110 and highlight some past events:

In July 2014, prop-110 is ratified and small group of operators start
anycasting the 1.2.3.0/24 prefix.

By September 2014, the 1.2.3.0/24 prefix gains traction, it has become
globally visible despite recommendations to only propagate in a
localized scope. Many operators pride themselves in providing this
service to the general public.

A milestone: In december 2014 a large merchant silicon CPE vendor
hardcoded 1.2.3.4 as the solo caching resolver in its firmware. Milions
```

ポリシーSIGで
コンセンサスが得られた後、
「未来のタイムトラベラー」
による投稿あり

参考図：IANA機能と関係機関の整理

- IANA機能は米国政府が、ICANNに業務委託をしているのが現在の仕組み

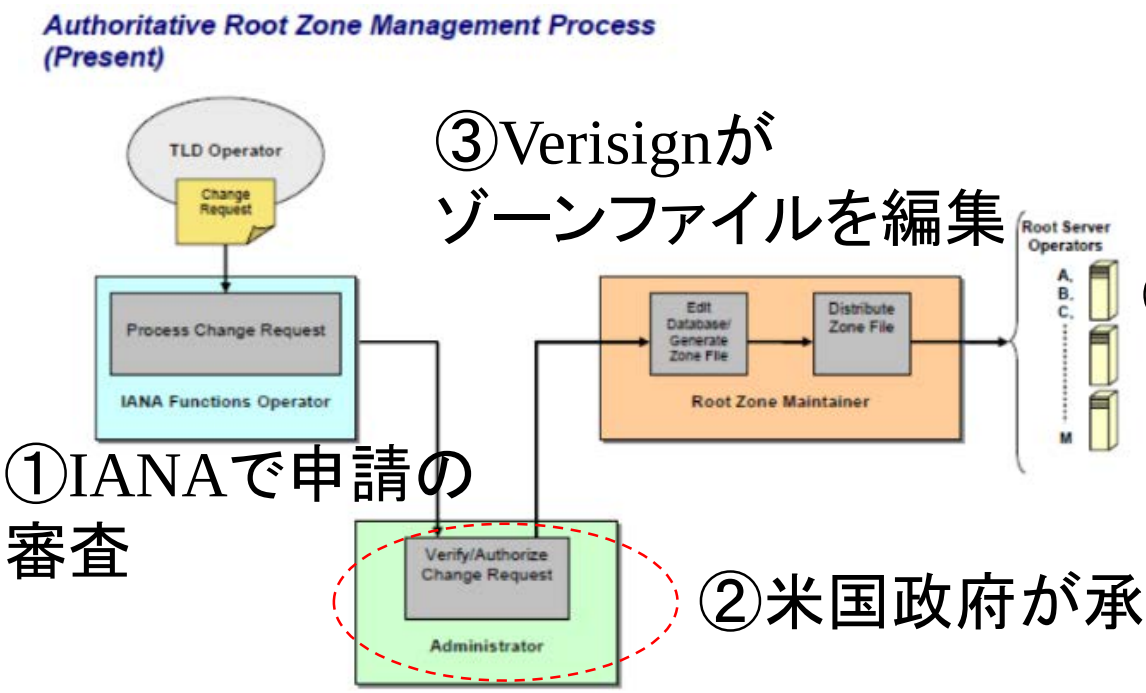


USG=米国政府

今後
どうするか？

http://www.icann.org/en/about/agreements/iana/iana-transition-scoping-08apr14-en.pdf

参考図：現在のルートゾーンの管理プロセス



③Verisignが
ゾーンファイルを編集

④ルートDNSに反映

①IANAで申請の
審査

②米国政府が承認

http://www.icann.org/en/about/agreements/iana/contract-01oct12-en.pdf

今回決議されたこと

- **アドレスポリシー提案3点**
  - 1点がコンセンサスに至る
- **APNIC Executive Council(理事会)選挙**
  - 席数と候補者数が同数のため選挙なし
  - JPNIC　前村含め、現職3名が継続して着任
- **APIA Board(理事会)選挙**
  - IIJ　松崎吉伸氏再選

