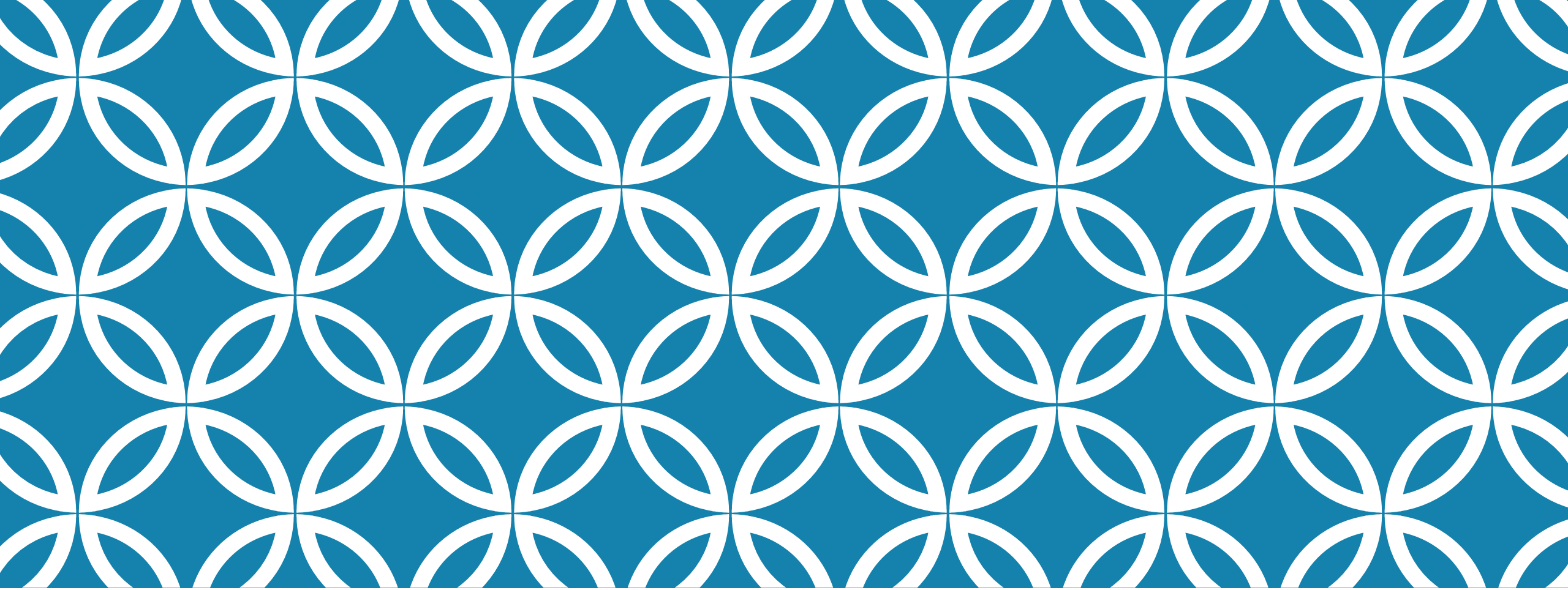


# インターネットレジストリをイチから考える

WIDE Project
白畑 真

*Disclaimer: 本発表は個人の意見でありWIDE Projectならびに所属組織の見解を代表するものではありません*

# インターネットレジストリとは何か
## サービスと周辺領域

**Whois/RDAP**
IPアドレス/ASNに関する
登録情報を開示

**RPKI**
IPアドレス/Origin ASNの
情報(ROA)を
PKIの証明書として発行

+ Origin AS/CIDR情報

**Routing Registry**
ASNと経路制御に関する
情報を登録・開示

+ Maintainer, Route, AS,
AS-SET Object情報

**逆引きDNS**
IPアドレスブロックに
紐付けられた逆引きDNS
権威サーバの登録・委任

+ 委任先DNSサーバ情報

**IPアドレス・AS番号の管理業務: ”登記簿”の管理 (IANA/RIR/NIR)**
- 番号資源の割り振り・割り当て
  - ニーズの審査
  - 在庫管理
- 移転手続きへの対応

**メンバーシップ・ポリシー策定プロセス (PDP)**
- 地域コミュニティでのボトムアッププロセスによるルール作り (例: JPOPF)

**アーキテクチャ (IETF/IANA)**
- インターネットそのもののアーキテクチャ、番号の意味などを定義
- 例: プライベートIPアドレスやISP Sharedアドレス(100.64.0.0/10), Link-Localアドレス、AS23456など

主として人間向けデータを提供　主として機械向けデータを提供

# ~~よくある話~~

「192.168.0.1は私のIPアドレスです。
勝手に使わないでください。JPNICにも通報しました！」


IPアドレスが一意な範囲が異なる

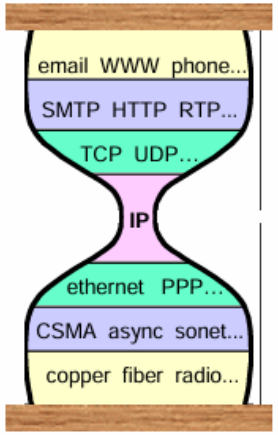
- プライベートIPアドレスは**<u>各ネットワーク内において一意</u>**、世界で唯一ではない
  世界中で同一のIPアドレスが利用されている
- 他方、グローバルIPアドレスは**<u>世界規模での一意性が重要</u>**

Source(イラスト): いらすとや https://www.irasutoya.com/2017/04/blog-post_797.html

# IPレイヤがインターネットアーキテクチャのキモ

## Why the Hourglass Architecture?

- Why an internet layer?
  - make a bigger network
  - global addressing
  - virtualize network to isolate end-to-end protocols from network details/changes
- Why a *single* internet protocol?
  - maximize interoperability
  - minimize number of service interfaces
- Why a *narrow* internet protocol?
  - assumes least common network functionality to maximize number of usable networks



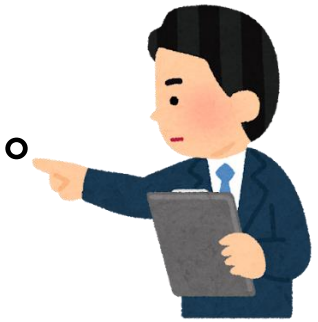

3

Source: Steve Deering, “Watching the Waist of the Protocol Hourglass (IETF 51 London Keynote)”, Aug 2001
https://www.ietf.org/proceedings/51/slides/plenary-1/index.html

# あったら怖い、こんな○○NIC

「御社には127.11.29.0/24を割り当てます」

「このIPアドレスを使うとなぜか通信できません。
不良品なので交換してください」



「仕方ないなあ、代わりに241.11.29.0/24を
特別に割り当てます。」

Source(イラスト): いらすとや

# 誰がIPアドレスのアーキテクチャを規定するのか

**Whois/RDAP**
IPアドレス/ASNに関する
登録情報を開示

**RPKI**
IPアドレス/Origin ASNの
情報(ROA)を
PKIの証明書として発行

+ Origin AS/CIDR情報

**Routing Registry**
ASNと経路制御に関する
情報を登録・開示

+ Maintainer, Route, AS,
AS-SET Object情報

**逆引きDNS**
IPアドレスブロックに
紐付けられた逆引きDNS
権威サーバの登録・委任

+ 委任先DNSサーバ情報

**IPアドレス・AS番号の管理業務 (IANA/RIR/NIR)**
- 番号資源の割り振り・割り当て
  - ニーズの審査
  - 在庫管理
- 移転手続きへの対応

**メンバーシップ・ポリシー策定プロセス (PDP)**
- 地域コミュニティでのボトムアッププロセスによるルール作り (例: JPOPF)

**アーキテクチャ (IETF/IANA)**
- インターネットそのもののアーキテクチャ、番号の意味などを定義
- 例: プライベートIPアドレスやISP Sharedアドレス(100.64.0.0/10), Link-Localアドレス、AS23456など

主として人間向けデータを提供　主として機械向けデータを提供

あったら怖い、こんな○○NIC
# RIR機能不全となった場合のシナリオ

## シナリオ1: WHOISデータベース消失

- システム障害や不正アクセスで登録情報が失われる
- IPアドレスの正当な登録者がわからず、ルーティングや法執行に混乱

## シナリオ2: RPKI Trust Anchorが停止

- RPKIシステムが長期間ダウンし、ROAが検証不能に
- ルーティングが無保護状態となり、経路ハイジャック頻発

# AFRINICにおける不正IPアドレス流用事件(2019)


AFRINICの職員(当時)が、ダミー会社や既に存在しない企業を利用してIPアドレスを不正に取得し、少なくとも5,000万米ドル以上の価値がある400万件のIPアドレスを不正に流用したとされている事件

*AFRINICは、約400万のIPv4アドレスが不正に流用されたと信じる理由があります。*

1. *AFRINIC IPv4プールの約[illegible]AFRINIC WHOISデータベースでレガシーアドレス空間として誤って再分[illegible]した。*
2. *レガシーアドレス空間とし[illegible]約170万のIPアドレスが不正に流用されました。*

AFRINICは当該職員を解[illegible]

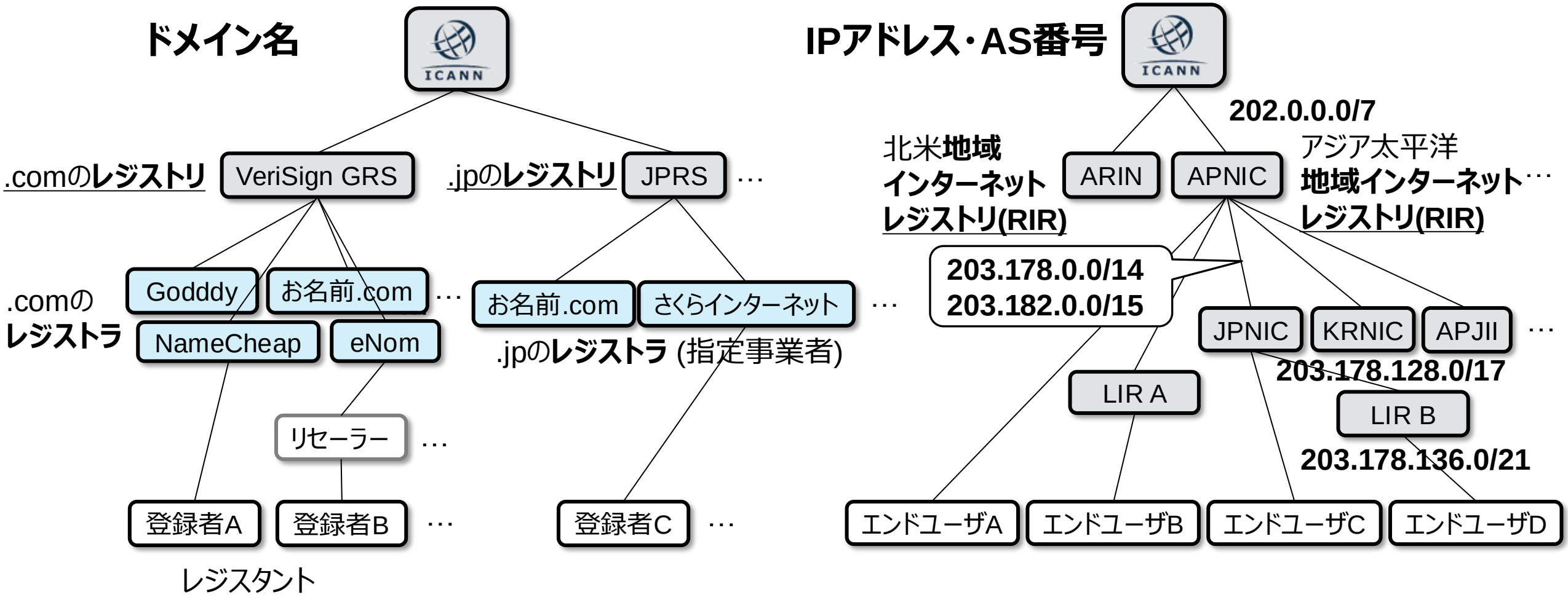
RIRの信頼性を著しく損う事件

*"私たちは、私たちに委ねられたインターネット番号リソースを保護し、AFRINIC WHOISデータベースの正確性とセキュリティを確保することをお約束します。"*

**IPv4アドレス在庫枯渇でIPv4アドレスに経済的価値が生まれた**

Source: Misappropriation of IP addresses in the AFRINIC region", AFRINIC, https://afrinic.net/20200826-ceo-statement-on-ip-address-misappropriation
"The Great $50M African IP Address Heist", Krebs on Security, https://krebsonsecurity.com/2019/12/the-great-50m-african-ip-address-heist/

# ドメイン名と名前資源管理の類似性




**ドメイン名のコミュニティから番号資源のコミュニティが学べる知見があるのでは**

# インターネットレジストリとDNSコミュニティの体制比較

| 項目 | インターネットレジストリ(RIR/NIR) | TLDオペレーター | DNSルートサーバー運用者(RSO) |
|---|---|---|---|
| 役割 | 地域ごとのIPアドレス/AS番号管理 | 特定TLDのレジストリ運営 | ルートDNS (A～M)のサーバー運用 |
| 組織形態 | 非営利・地域コミュニティ制 | 民間企業主体（ICANNと契約） | 大学・企業・研究所など、多様な非営利/営利形態 |
| 紛争解決メカニズム | (ARINやRIPEなど)RIRによっては紛争時の内部調停・仲裁を含む契約条項あり; ADR規定あり | UDRP, JP-DRPなどのドメイン名に関する紛争処理方針あり | 不適切な運用者の扱いはRSSAC056で定義 |
| 新規参入 | 過去にはNIRの追加などあったが、RIRレベルでの新設は極めてまれ | 新gTLDプログラムで多数のレジストリが参入可能 | M-ROOTが1997年に追加されたのが最後。RSSAC037で示唆あり。戦略・アーキテクチャ・ポリシー機能(SAPF)が判断、DRFが実施 |
| 退出・交代 | 基本的に想定外か? | 契約終了・違反・経営破綻でレジストリ交代も。EBERO等で継続性確保 | RSSAC037で示唆あり。戦略・アーキテクチャ・ポリシー機能(SAPF)が判断、DRFが実施 |
| データエスクロー | なし | RDE(Registrar Data Escrow)プログラムを原則義務づけ。DENIC他がエスクローを担う | なし(不要? See root.zone) |
| 事例 | AFRINICの訴訟 | .amazon問題、.org売却問題、新gTLDの閉鎖・EBERO発動など | 顕著な入れ替えはないが、CogentによるPSINet買収事例あり。一部RSOはCloudflareと協業 |

# EBROとは

- EBERO(Emergency Back-End Registry Operators)
  - TLD(トップレベルドメイン名)レジストリオペレータの障害が発生した場合に重要なレジストリ機能を提供するために、ICANNと契約を締結しているレジストリオペレーター
  - 現在はCIRA(カナダ), CNNIC(中国), Nominet(イギリス)の3社が選任されている
- TLDのレジストリオペレータが以下の5点の重要なレジストリ機能のいずれかを維持できなくなる恐れがある場合に、一時的に発動する
  1. 登録したドメイン名のDNS解決
  2. 共有登録システムの運用
  3. 登録データディレクトリサービスの運用
  4. レジストリデータエスクロー委託
  5. DNSSEC要件に従って適切に署名されたゾーンの保守
- 直近では” .nowruz”ドメインにEBROが発動(2024/7)
  - 5件のTLDを運営する事業者のAsia Green IT System Bilgisayar San. ve Tic. Ltd. Sti.がICANNと合意した基準を満たせず
  - NominetがEBROオペレーターとして”.nowruz” TLDの運用を暫定的に引き継ぎ
  - 過去にも”.desi”や”.wed” TLDがEBROの対象になっている

Source: ICANN
https://www.icann.org/resources/pages/ebero-2018-10-12-ja
https://www.icann.org/en/announcements/details/icann-to-move-four-gtlds-into-the-emergency-back-end-registry-operator-program-12-07-2024-en
https://www.nominet.uk/nominet-named-ebero-provider-for-nowruz-gtld/

# インターネット「参加」の手引き


✖ お客様

〇 メンバー

# おわりに: RIRの重要性とエンジニアの役割

1. **RIRの健全な運営を担保するために必要なこと**
   - **コミュニティ参加と建設的関与:** ポリシーフォーラム(JPOPMやAPNIC Policy Meeting)での議論や適切な組織運営(i.e.透明性やアカウンタビリティ)への関心を持つ
   - **技術協力:** RPKI導入やWHOIS正確性(データの最新化)向上、運用のベストプラクティス普及
   - **経済的支援:** RIRの会員としての会費負担
2. **JANOGerを含むインターネットコミュニティにとってのメリット**
   - **インターネットレジストリの安定的かつ健全な運用**
     - **IPアドレス・AS番号の管理:** 新規割り振り・割り当て・移転対応でインターネットの運用、拡張を支援
     - **WHOISの正確性:** abuse対応やインターネットの安定的な運用の基礎に
   - **インターネットの根幹インフラの継続的・安定的運用体制の確保**
     - RPKIのTrust Anchorの安定的な運用
     - 逆引きDNSの安定的な運用

**RIRを支えるのはインターネットコミュニティ**