「権威 DNS サービス調査」
「インターネットの維持 近況」

ENOG74 Meeting

2022/6/10

TACHIBANA toshio

GREE, Inc.

「権威 DNS サービス調査」

ENOG74 Meeting

2022/6/10

TACHIBANA toshio

DNSOPS.JP/GREE, Inc.

権威 DNS サービス調査

- DNSOPS.JP(日本DNSオペレーターズグループ)が2020年4月から実施中の国内外で提供されている代表的な権威DNSサービスの機能調査
- 「市井の一ユーザとして」忖度なくガチ調査を実施
- 2年間の準備～調査実施、報告会を通じて運用者コミュニティ(DNSOPS.JP、JANOG)からフィードバックを受け、サービス調査そのものの知見が溜まってきた
- 利用者視点だけでなく権威DNSサービス提供者視点からも調査すべき項目があることに改めて気付くことができた

メンバー紹介

- 岡田 雅之
  - 長崎県立大学 情報システム学部教授
- 田中温子
  - 株式会社ミライコミュニケーションネットワーク
- 石田 慶樹
  - DNSOPS.JP代表幹事
  - 日本ネットワークイネイブラー株式会社フェロー
- 米谷 嘉朗
  - DNSOPS.JP幹事
  - 日本レジストリサービス株式会社
- 柴尾直輝
  - 長崎県立大学 情報システム学部
- 橘 俊男
  - DNSOPS.JP幹事
  - グリー株式会社

調査の背景

- 前提
  - インターネットサービスの多様化により、サービス情報を提供する汎用データベースとしてDNSの役割が増加している
  - それにともない新しいリソースレコードの定義や、既存リソースレコード(特にTXTレコード)のユースケース追加などが行われている
- 認識
  - 一般的な組織の権威DNSサーバ運用者(ゾーン管理者)はDNSプロトコルや新しいインターネットサービスの専門家ではないため、すべてのリソースレコードを理解し正しく設定できることは期待できない
  - 現代においては、権威DNSサーバの自前運用は設定ミスや大量クエリによるサービス障害の原因となり得るため、一般的な組織においても推奨されない

調査の目的

- 組織のシステム管理部門やサービス提供部門が、それぞれの目的に沿って適切な権威DNS(自ゾーン)を運用可能とするため、国内外で提供されている代表的な権威DNSサービスの機能一覧作成が望まれる
- 本調査の目的は、そのような機能一覧となることである

機能の優劣をつけることや、
特定のサービスを推奨することは目的ではありません。

調査項目

- 組織におけるDNSの利用目的に沿って適切な権威DNSサービスを容易に選択できるようになることを念頭に、以下の観点で権威DNSサービスの機能を調査する

項目	概要
機密性	サービスコンソールログインが多要素認証、ロールベース認証、ゾーン転送にTSIGが利用可能、サブドメイン名ハイジャック対策
可用性	権威DNSサーバの地域冗長性、レスポンスレートリミット、他権威DNSサービスとのセカンダリ連携、地域指定可能、SLA規定、更新処理のDR化
完全性	バックアップ有無・頻度、DNSSEC対応
利便性	専門知識を有しないユーザが目的の設定を容易に行えること、大量のリソースレコードを一括登録できることなど
リソースレコード	最低でもA/AAAA/CNAME/MX/NS/TXT/SRVに対応していること、CAAやDNSSECに対応していることなど
サポート	運用レポートが作成されること、問い合わせが可能で時間帯が明確であることなど
コスト・契約	課金体系が明確であること、契約期間や解除方法が明確であることなど

調査しながら整理中

調査項目

- 組織におけるDNSの利用目的に沿って適切な権威DNSサービスを容易に選択できるようになることを念頭に、以下の観点で権威DNSサービスの機能を調査する

項目	概要
機密性	サービスコンソールログインが多要素認証、ロールベース認証、ゾーン転送にTSIGが利用可能、サブドメイン名ハイジャック対策
可用性	権威DNSサーバの地域冗長性、レスポンスレートリミット、他権威DNSサービスとのセカンダリ連携、地域指定可能、SLA規定、更新処理のDR化
完全性	バックアップ有無・頻度、DNSSEC対応
サポート	[illegible]、問い合わせが可能で時間帯が明確であることなど
コスト・契約	課金体系が明確であること、契約期間や解除方法が明確であることなど

権威DNSサービスを提供する深い(本質的)理由は事業者それぞれ！

調査しながら整理中

最近1年間(2021年度)活動の状況

- 継続したサービスリストのアップデート
  - 人力調査によるリストの更新
  - https://docs.google.com/spreadsheets/d/1sM6r6pscUS4Ujngp2qQsreQNrUKFe3A32GDavDMvbM4/edit#gid=0
- 注目事業者のサービス試用
  - 1社に注目し、サービス・APIを実際に利用し使用感を確認
- 事業者インタビューに必要な予備調査
  - サービス提供事業者の状況を把握するため、複数事業者をリストアップし、インタビューを開始

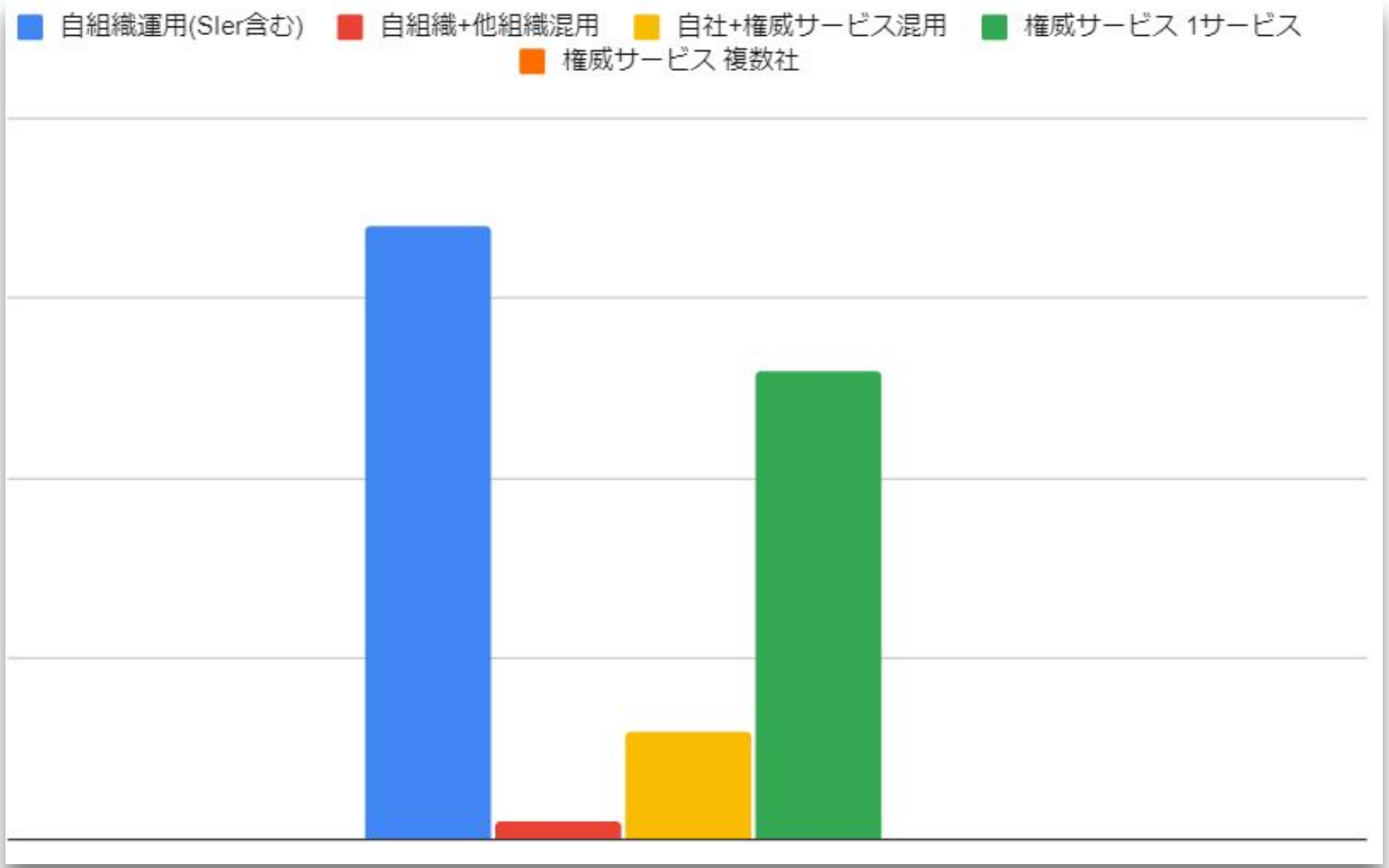
最近1年間の権威DNSサービスの動向

- リソースレコードの追加対応
  - HTTPS RRの対応が増加
- 一方DNSSECへの対応は現状維持
  - マルチサービス化を考慮、秘密鍵のエクスポート機能について照会
    - どの事業者も セキュリティ に関することでそのような機能は無い・予定していないと把握
  - 暗号スイートの違いなどもう少し突っ込んだ調査が必要(かも)
- DNSSEC対応の真の意味を探るためにも継続調査が必要
  - 対応した、というのはいったいどういうことなのか？

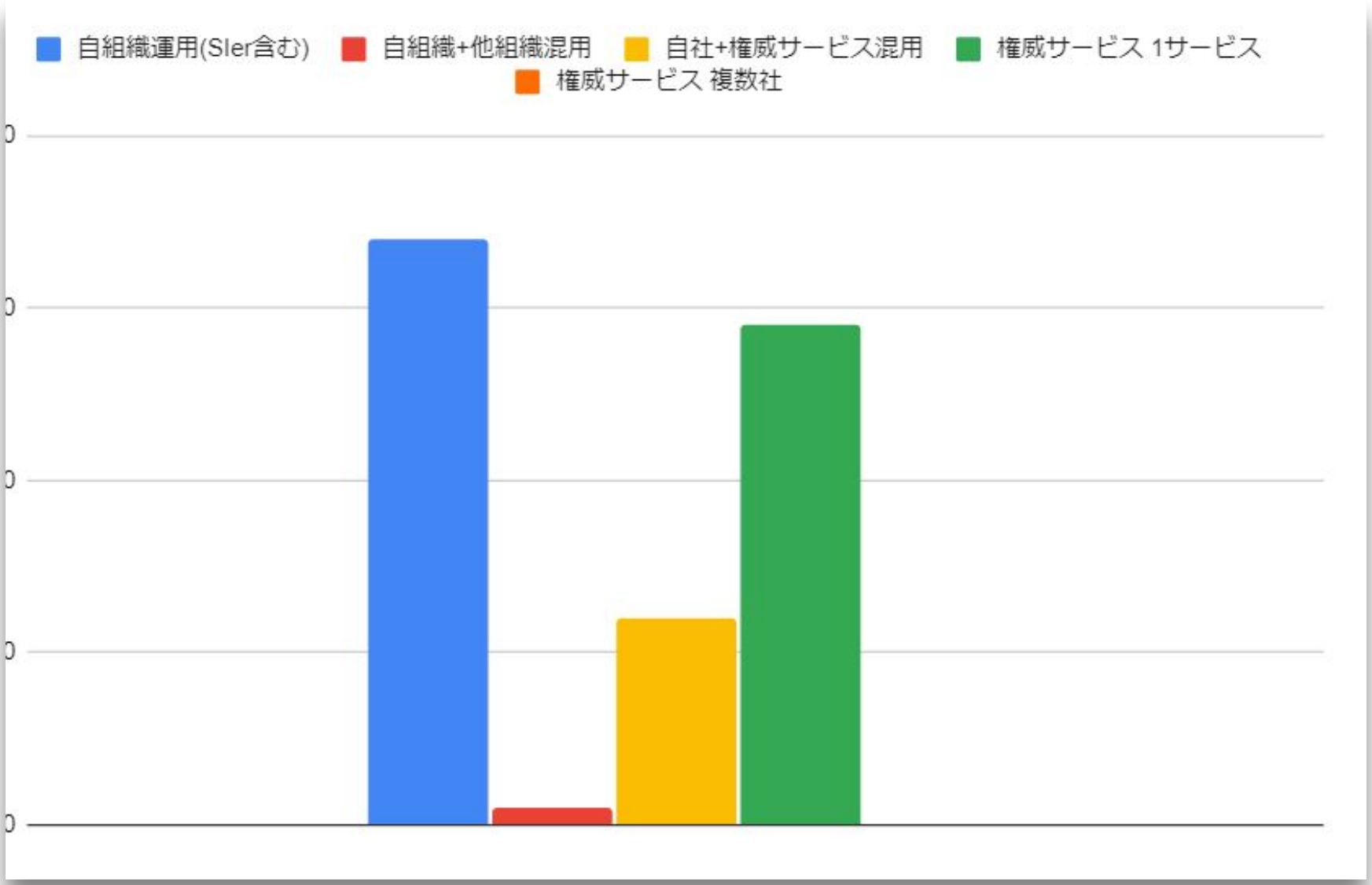
権威DNSサービス普及状況

- 権威DNSサービス自体のユーザ利用状況はどうか？
  - 普及の状況を共有することで現状を把握
- ドメイン名のリストからNSレコードを収集
  - NSレコードのドメイン名からNSの性質を分析
    - 明らかに権威DNSサービス
      - 超有名どころ
      - 巨大CDN
    - Webやクラウド運用の付加サービスとしての権威DNSサービス
    - SIer等のサービス？
    - 自社・自組織内の運用
  - 今回は赤枠の部分を権威DNSサービスとしてカウント

権威DNSサービス普及状況 TOPIX関連企業

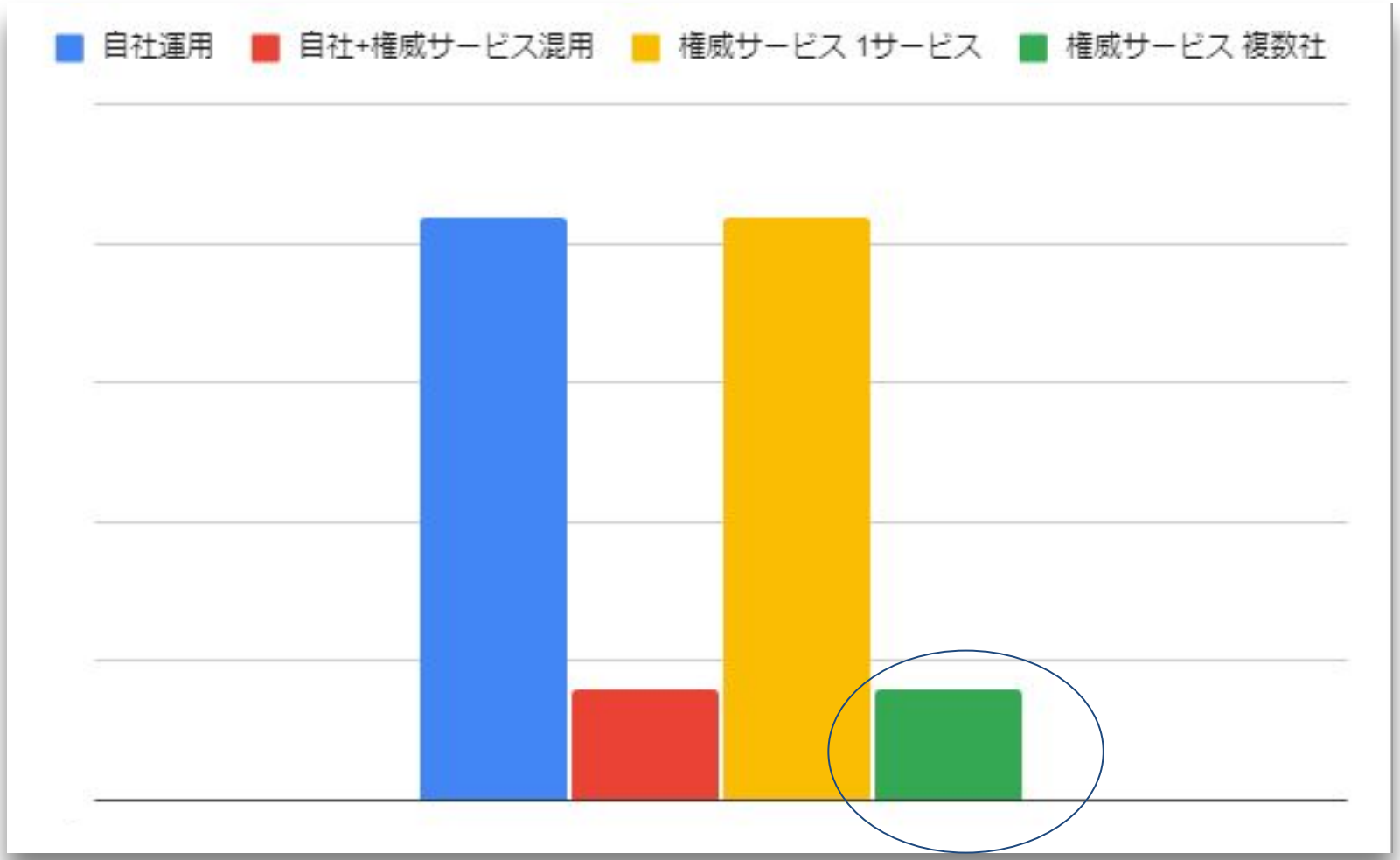


権威DNS普及状況 官公庁等

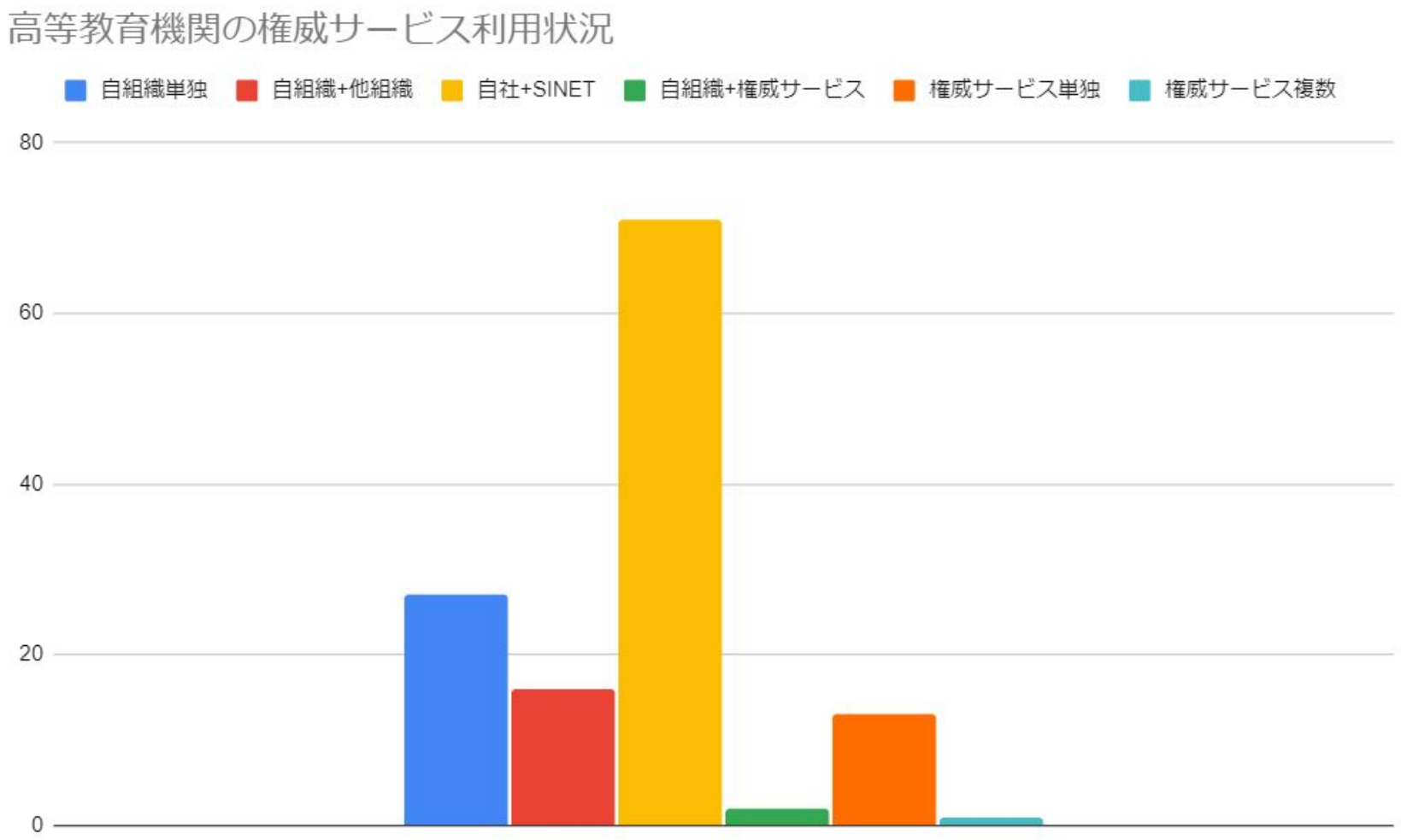


権威サービスの普及度合い

- Similar web Japan top 50から調査



高等教育機関


高等教育機関の権威サービス利用状況
自組織単独
自組織+他組織
自社+SINET
自組織+権威サービス
権威サービス単独
権威サービス複数
80
60
40
20
0

DNSOPS.jp
DNS Operators Group, Japan

- サービス提供事業者側の状況を知りたい
  - どの程度の技術レベルの顧客を想定しているのか？
  - サービス提供に関する事業としての継続性
  - どの程度利用者は頼ってよいのか？実態を知るためにインタービューを実施

ヒアリング対象事業者様

2022年3月7日
日本DNS・オペレーターズ・グループ 権威DNSサーバ調査チーム

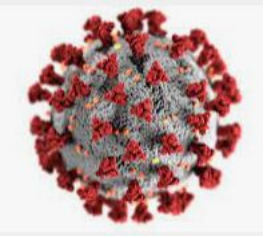
権威DNSサーバサービス調査 提供事業者ヒアリングについて(案)

利用目的に沿って適切な権威 DNS サービスを容易に選択できるようになることを念頭に、以下の観点で権威 DNS サービスの機能を調査しております。回答可能な項目についてご教示いただけますと幸いです。(これにサービス調査結果も渡して項目に対応していることを補記する)

1) 機密性
   - ISO27017 対応の状況
   - 以下の機能の実装状況
     - サービスコンソールへのログインへの多要素認証
     - ロールベース認証(RBAC)機能
     - ゾーン転送に対応している場合のTSIG
     - サブドメイン名ハイジャック対策
2) 可用性
   - 権威 DNS サーバが地域的・ネットワーク的に異なる複数拠点に展開されていること
   - 適切な閾値でレスポンス・レートリミットが可能であること
   - 他の権威 DNS サービスとセカンダリ構成をとることが可能
   - 指定した地域でサービスが利用可能であること
   - SLA の規定があること
   - 更新処理が ディザスタリカバリ 構成になっていること
3) 完全性
   - バックアップの有無、頻度、保存期間
     ゾーン情報のバックアップどうやってるか
   - ゾーンの棚卸してますか
   - DNSSEC に対応していること(鍵管理が可能であること)
4) 利便性

インタビューの結果

- 1社のインタービューを終えての所感
  - サービスについてのきわめてセンシティブな回答が多い
  - 複数社のインタビューを行い、匿名化したうえで情報を共有する必要性を把握
  - 今年度は、コロナ禍においても対面インタビューを意識していたため、対応は1社となった
  - 次年度は複数社をインタビュー予定



最近1年間の権威DNSサービスの動向

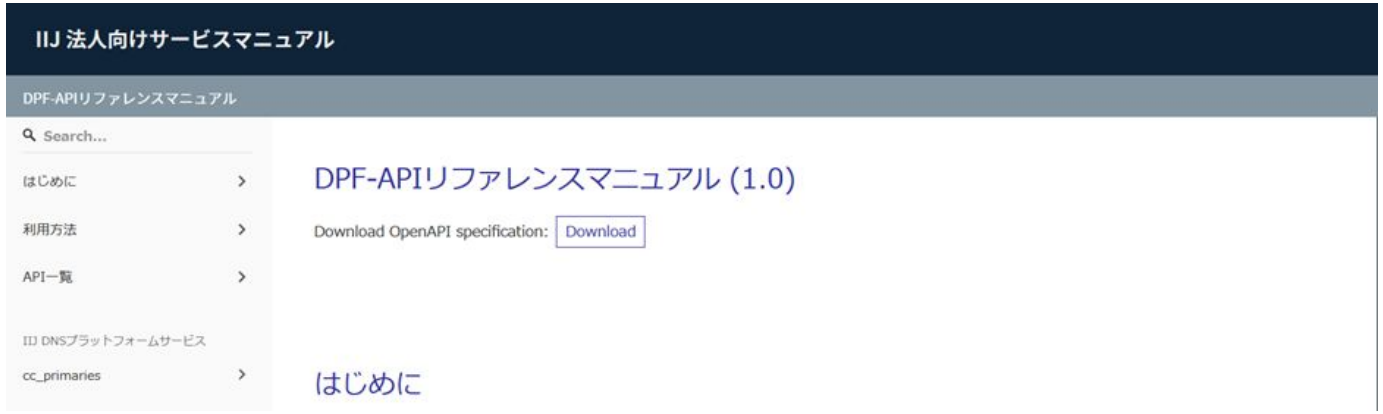
- 継続したサービスリストのアップデート
  - 人力調査によるリストの更新
  - https://docs.google.com/spreadsheets/d/1sM6r6pscUS4Ujngp2qQsreQNrUKFe3A32GDavDMvbM4/edit#gid=0
- 注目事業者のサービス試用
  - 1社に注目し、サービス・APIを実際に利用し使用感を確認
- 事業者インタビューに必要な予備調査
  - サービス提供事業者の状況を把握するため、複数事業者をリストアップし、インタビューを開始

DPF-API調査

- DPF-APIとは
- 調査のきっかけ
- DPF-APIを使った更新処理の流れ
- 使ってみた感想

DPF-APIとは？

- IIJ DNSプラットフォームサービス（略してDPF）のDNSレコードやゾーン情報等をプログラムから操作するためのAPI
- IIJ IDサービスの契約が必要（月額0円～）



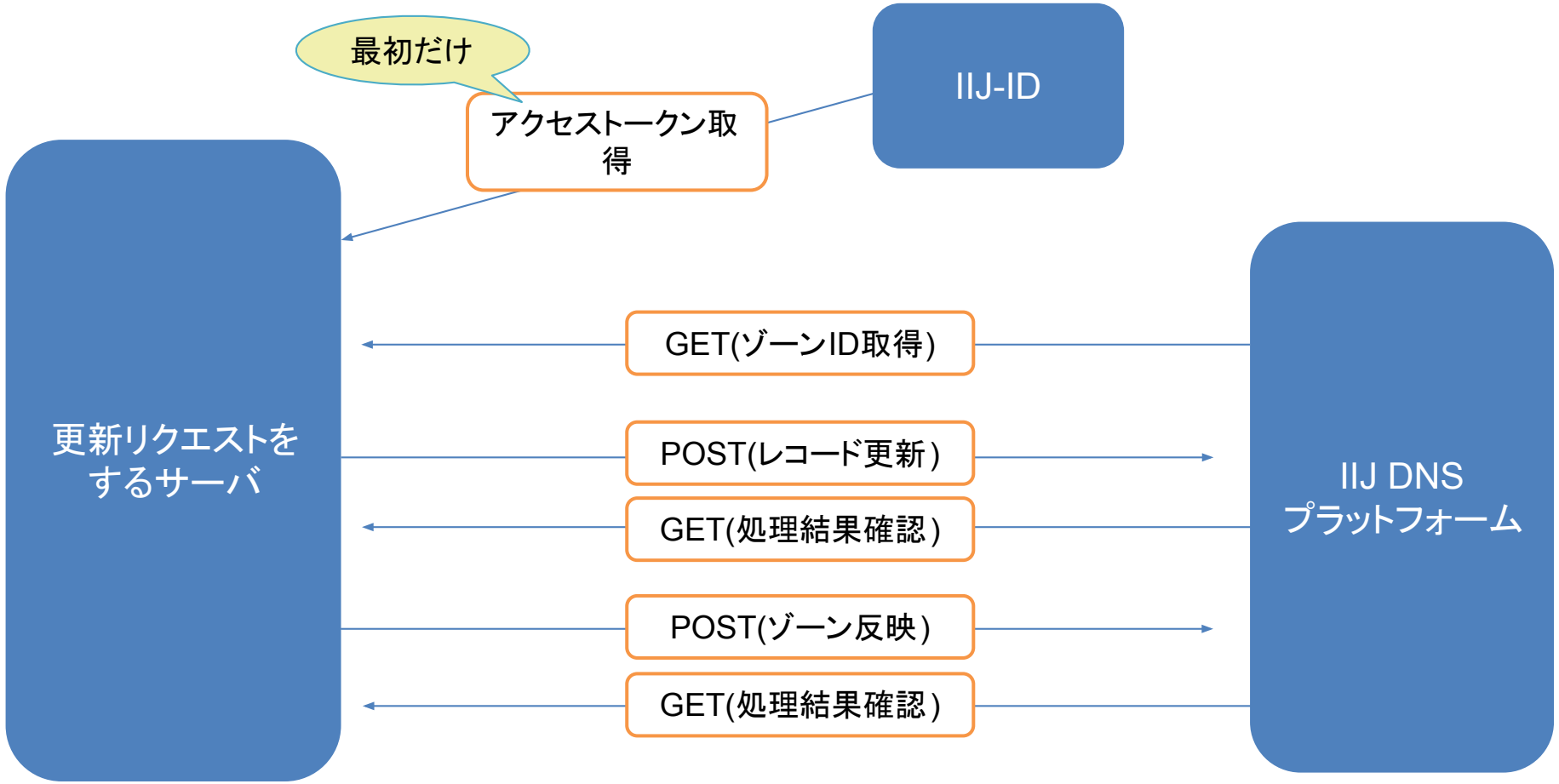
調査のきっかけ

- 権威DNSサービスのGUIでできないことがある
  - 時間指定で自動的にレコード反映

    （20時に新しいメールサーバに切り替えて、サイトを11時にリニューアルしたい、とか）
  - BINDのGENERATEの代わりに多数のレコードを追加

APIを使えばできるのか調査

DPF-APIを使った更新処理の流れ



所感

- わかりやすいマニュアルがあり使用するハードルは高くない
- 沢山のレコードをプログラムで追加するのには便利
- アクセストークンは定期的に更新するのがよい
  - 例えば有効期限を5年間にすると5年後に動かなくなる時限爆弾ができあがる
- 情報取得以外は（一応）非同期なので、理解した上で使う必要はある
  - 私が色々やってみた感触では即時反映
  - 反映を自動化するにしても、正しく切り替わったかの確認はやっぱり必要
  - DNSSECなど時間がかかる処理もあるそう

最近1年間(2021年度) 調査を通じて得た感想

- サービスを説明する言葉の抽象性の問題
  - 「DNSのセキュリティをあらゆる場面から実現」→？？？？？
  - 「マネージドでトータルなプラクティカルソリューション」→？？？？
  - 国内事業者や一部クラウド事業者の説明が変化
    - もしかしたら表現を直してくれた？
- 事業者の提供サービス一覧の標準化
  - 標準メニュー的なもの
  - 本調査の項目に〇/×してゆく形が実は最適化
- 可用性、運用関連はWebからの調査は限界
  - 実際にユーザ登録、ドメイン名の登録を行い調査を継続予定

最近1年間(2021年度) 調査を通じて得た感想

- 権威DNSサービス(マネジドDNSサービス)というものがあることを広く世に知らしめる
- 自組織運用(自前運用)を継続している理由を良し悪し区別なく教えてもらう
- 事業者インタビュー時の「答えやすい」質問を教えてもらう
- 権威DNSサービス調査の自動化(Webページの判定など)の手法を教えてもらう

みなさまへのお願い

- 調査に対するフィードバックにご協力ください
- 以下の2種類(ユーザー用・事業者用)がありますので、ご自身にとって適切と思われる方を選んでご回答ください

権威DNSサービスユーザー用

権威DNSサービス事業者用

調査費用(実費)はDNS Summer Day 2021に
協賛いただいた費用の一部を使用しております

みなさまの中で。。

- インタビューを受けたいという権威DNSサービス事業者の方はおられませんか？
  - 調査を充実させたいので対象を増やしたいと考えています
  - 協力してもいいよ。。という事業者の方はぜひ私まで！
- webをアクセスして内容を自動判定する技術をお持ちの方はおられませんか？
  - 労力を下げつつ、調査量を増やしたいと考えています
  - 「こんなやり方あるよー」等のアイデアをお持ちの方はぜひお話させてください！

【付録】権威DNSサービス調査の資料

https://dnsops.jp/documents.html から引用・加筆

調査報告書				
	2021年4月9日版			
	2022年4月14日版	***NEW!***		
フィードバックフォーム				
	一般ユーザー用フォーム	←権威DNSサービスを利用する視点で回答する場合		
	事業者用フォーム	←権威DNSサービスを運用・提供している視点で回答する場合		
過去の発表（各種イベントで発表した資料）				
	2020/06/26	DNS Summer Day 2020	資料1	資料2
	2020/11/26	DNSOPS.JP BoF 2020	資料	
	2021/04/09	権威DNSサービス調査報告会	資料1	資料2
	2021/06/25	DNS Summer Day 2021	資料1	資料2
	2021/07/16	JANOG48	資料1	資料2 資料3
	2021/11/19	DNSOPS.JP BoF 2021	資料1	資料2

「インターネットの維持 近況」

ENOG74 Meeting

2022/6/10

TACHIBANA toshio

GREE, Inc.

注意

固有の{組織|団体|コミュニティ}名

の好き嫌いについて言及しない様に努力します☺️

このシリーズの背景

- インターネットが好きで色々やってきたけど、ここらで「根っこ」を伝えることをやりたくなった
- 話者について
  - 過去の経験（順不同）
    - インターネットの普及と発展に寄与するための国際NPO組織の日本支部の運営
    - 国内のインターネットガバナンスについて語り合う場の運営
    - 番号資源管理ポリシーを決める国内フォーラムの運営
    - NOGの運営
  - 現在
    - DNSOPS.JP幹事(2013-)
    - ISOC-JP == インターネットの普及と発展に寄与するための国際NPO組織の日本支部
      - Officer(2022/5/1-2023/12/31)
      - Chair(2022)

- 本発表で目指すもの
  - The Internetの技術の奥底にある理念
  - あるがままのThe Internetを利用できる状態の大切さを知る事を通じて「The Internet」を維持することへの関心を増やしたい
- 伝えたい相手
  - みんな

特に「インターネット成立後の世代」

- Scope
  - Internet Protocol
  - Connectivity
  - Resource Management
- Out of scope
  - Business
  - Law

近況

- Internet Protocol
- Connectivity
- Resource Management

近況

- 概況
  - 前回(ENOG61)での発表(2019/2)以降、COVID-19の影響で諸々のアクティビティの開催形態が変わる

近況

- Internet Protocol
  - IETFは2020/3以降、フルオンラインでミーティングを実施
  - 2022/3のIETF113@ViennaをハイブリッドF2Fを再開
  - Towards a net zero IETF
    - https://www.ietf.org/blog/towards-a-net-zero-ietf/

近況

- Connectivity
- Resource Management
  - ICANN Meetingは2020/3以降、フルオンラインでミーティングを実施
  - 次回ICANN74はハーグ（オランダ）での開催を予定

つづく

GREE

Additional Slide

- Internet Protocol
- Connectivity
- Resource Management

- 二つのバージョン
  - RFC8200(Version 6)
  - RFC791(Version 4)

最低二つのノードによる手順の合意があれば通信可能

RFCとは？

- インターネットで利用する技術について書かれたメモ（意訳）
  (https://www.ietf.org/standards/rfcs/)

- RFCはどこで作る？
  - IETF(Internet Engineering Task Force)の活動の中で作成する

Internet Engineering Task Force

- Mission
  - The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.
    (https://www.ietf.org/about/mission/)

GREE

IETFとは(2)

- インターネットで使う技術標準を定める主たる団体（意訳）

- The IETF is the premier Internet standards organization. It follows open and well-documented processes for setting these standards. (https://www.ietf.org/standards/)

- ゴール
  - RFC(Request for Comments)をStandard Trackによって発行する
- 手順
  - RFC2026に定義
    https://datatracker.ietf.org/doc/rfc2026/
  - プロセス概要
    https://www.ietf.org/standards/process/

GREE

Standard Trackとは？

- RFC発行プロセスにおける分類の一つ

- RFCのタイプ
  - Standard(Internet/Draft/Proposedの三種)
  - Experimental
  - Informational
  - Historic

GREE

RFC発行の手順（超簡略版）

1. Internet-Draft(I-D)を書く
2. 目的に沿ったIETFのWorking GroupでI-Dを議論してコンセンサスを得る
3. IESGによるレビューと承認を得る
4. RFC Editorによる発番と発行

GREE

「インターネットの維持」視点での重要なポイント

- 誰でも参加できる
- RFC作成のプロセスはすべて公開
- RFCは誰でも無償で利用可能

GREE

Connectivity

- Internet Protocolを使った通信を行うための手段
- プレイヤーの視点によって分類は様々
  - 提供対象地域
    - Global/National/Regional
  - 使用する場所
    - Residential/Mobile
  - 提供形態
    - 有線/無線

GREE

「通信」にまつわる環境の変化

- 従来
  - 使う場所や相手を意識する
    - 市内/市外
    - 国内/国際
    - 公衆回線(PSTN)/専用線
- 最近
  - 使う場所や相手を意識しない
    - The Internet

「通信」とは

- 国家が持つ「主権」の一つ
  - 国際電気通信連合(ITU)憲章
  - 国際電気通信規則(ITR)
    - ITUは国際連合の専門機関の一つ

- 「主権」とはざっくりいうと国家が他国からの干渉を排して独自の意思決定を行う権利のこと

国家主権視点での「通信」とThe Internet

- The Internetは、既存の網の上で行われる過去に定義されていなかった「通信」
- The Internetの扱いは全ての国家で同じではない
  - 自由だったり、監視したかったり、制限したかったり

- 事業者がグローバルに展開していても、国や地域毎にサービスのルールが異なる

GREE

The Internet

- Internet Protocolを使うネットワークが相互に接続することを通じて成立
  - ネットワークにユーザーを接続することも広義には相互接続といえるが、ここでは割愛
- 自律分散協調(autonomous distributed cooperative)的な考え方

- The Internetという組織があるわけではない（念のため書く）

GREE

相互接続

- AS同士が接続する
  - AS=Autonomous System
    - ISP/DC単位
- 接続方法
  - BGPによって経路を制御する
  - BGPを使う為にAS単位でユニークな番号を割り当てる(AS番号)

GREE

「インターネットの維持」視点で重要なポイント

- 事業者の相互接続によって成立
- 完成した状態は無い
- The Internet全体を統治する主体は存在しない
  - →裏を返せば統治主体を置くと成立しない（はず）
- 国や地域によってThe Internetへの姿勢は異なっている
  - 本音と建前はあるけど、、、

GREE

Resource Management

- 目的
- 対象
- 管理方法

GREE

目的

- 通信に使う識別子が複数の利用者で重複して使用することを防ぐ
- 通信の互換性を保つ

GREE

対象

- 番号資源
  - IPv4アドレス/IPv6アドレス
  - AS番号
- ドメイン名
  - Root Zoneの管理
  - 特定のゾーンの管理(.arpa/.int)
- プロトコルの名前とパラメータ
  - Internet Control Message Protocol (ICMP) Parameters

GREE

管理方法

- Public Technical Identifiers (PTI) という組織が管理業務を実施
  - 昔はIANAという組織が管理
  - 現在はIANA function(機能)を提供するために設立された組織であるPTIが運営
  - PTIはICANNから委託された契約者としてIANA functionを提供(2016年10月より)

Public Technical Identifiers (PTI)

- 管理台帳の大元を管理
- 実際の利用者の情報登録業務は地域ごとのRegistry(Regional Internet Registry)に委託
  - さらにRIRから再委託しているケースもある(後述)

GREE

Regional Internet Registry(RIR)

- グローバルを5つに分割して登録業務を実施
  - AFRINIC
  - APNIC
  - ARIN
  - LACNIC
  - RIPE/NCC

- 地域によってはさらに配下に国別のRegistryが存在する
  - JPNICもその一つ

PTI誕生前夜

- 過去はIANAという組織が管理していた
  - Internet Assigned Numbers Authority
    - IANAは米国政府の官庁である商務省の部局からのStewardshipを受けていた
- 2014年商務省から「Stewardshipをマルチステークホルダーコミュニティに移管する」と告知
  - 当時、所謂「The Internetの米国による支配」に対する反発のムーブメントが表面化しつつあった
- いろいろあってPublic Technical Identifiers (PTI)が設立されIANA funtion(機能)を運営することとなった

GREE

「インターネットの維持」視点で重要なポイント

- 各種資源の重複利用を防ぐ為にIANA Functionは必須
- IANA Functionの維持にはマルチステークホルダーによる関与が必要
  - 日本視点ではAPNICコミュニティおよびJPNICコミュニティへの番号資源利用者の関与が不可欠

私の願い

The Internetの技術の奥底にある理念
あるがままのThe Internetを利用できる状態の大切さ
を
技術者が知る事を通じて
「The Internet」を維持すること
への関心を増やしたい

と！く！に！
「インターネット成立後の世代」へ伝えたい！

インターネットを通じて、
世界をより良くする。