

DNS ルートサーバシステム

非技術者に向けたご説明

原文: Jeff Osborn, RSSAC Chair at ICANN 79, San Juan, Puerto Rico, March 2024

日本語訳: 大谷亘, JPNIC

ICANN79 によろこ

- ルートサーバシステム諮問委員会 (RSSAC)
 - ICANN コミュニティに対し, ルートサーバシステム関連のアドバイスを行う
 - 各ルートサーバ運用者 (RSO) が正副 1 名ずつメンバを指名 (+ リエゾン複数名)
- 今回は「自分はエンジニアではない」という前提でお聞きください
 - DNS がどう動くのか
 - ルートサーバシステムが DNS で果たす役割はなにか
 - ルートサーバシステムが (他と比較して) どれだけ重要か

DNS とは

• 人間用の名前からコンピュータ用のアドレスを探すしくみ

- 人間は `www.amazon.com` のような名前を解釈する
 - コンピュータは `18.64.129.218` のような IP アドレスを解釈する
 - DNS は “`www.amazon.com`” を “`18.64.129.218`” に翻訳する
 - 多くの場合, IP アドレスが変わることがあっても, 名前は変わらない
- ## • ほとんどのオンラインデバイスで DNS が使われる
- コンピュータ & サーバ
 - スマートフォン

• ドメイン名を質問し, IP アドレスを答える

DNS の利点

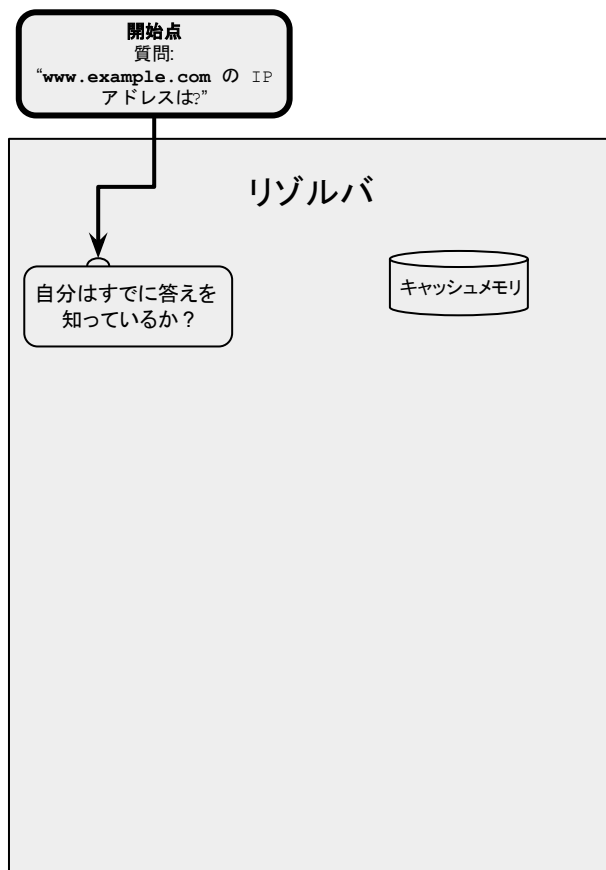
- **人間が扱いやすい** 識別子
 - `www.example.com` は `192.168.45.99` よりわかりやすい
- サービスの**可搬性**
 - 資源所有者が、ドメイン内のアドレスの紐付けを管理する
 - DNS が常に最新のオンライン上の場所へと案内してくれる
- 巨大だが利用しやすい分散ネットワーク
 - 数億のディレクトリ構造を柔軟に委任管理できる
 - **世界で一番大きな分散データベース**

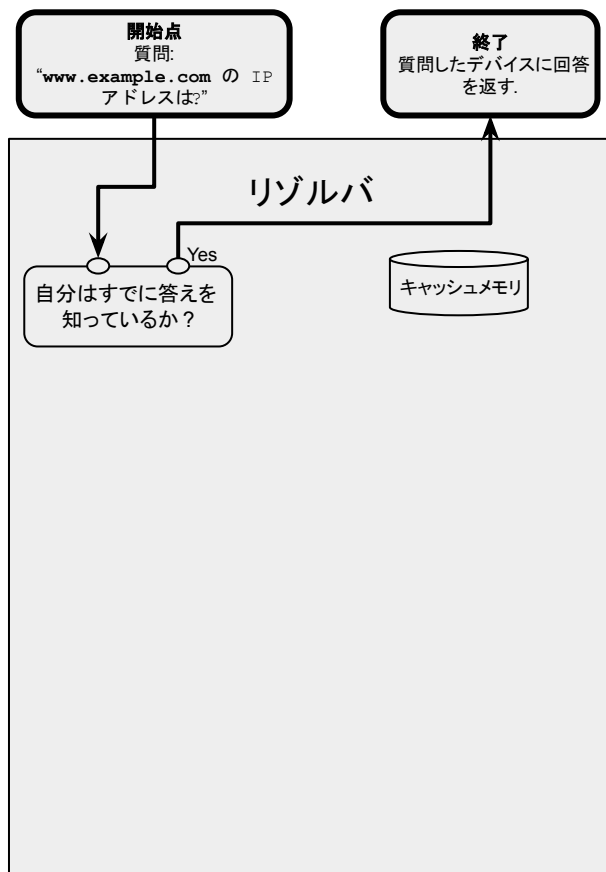
デバイスはリゾルバからアドレスを得る

- 数百万の**リゾルバ**が存在する
- リゾルバは世界中の電話帳を読めるような存在
 - 電話帳を**権威サーバ**と呼ぶ
 - 電話帳の中身を**ゾーンデータ**と呼ぶ
- www.amazon.com の「番号」は?
- www.amazon.com の番号は (今は) 18.64.129.218
 - **ミリ秒レベル**の速度で解決される
 - **毎日 500 兆回**ほど行われている

リゾルバは権威サーバからアドレスを得る

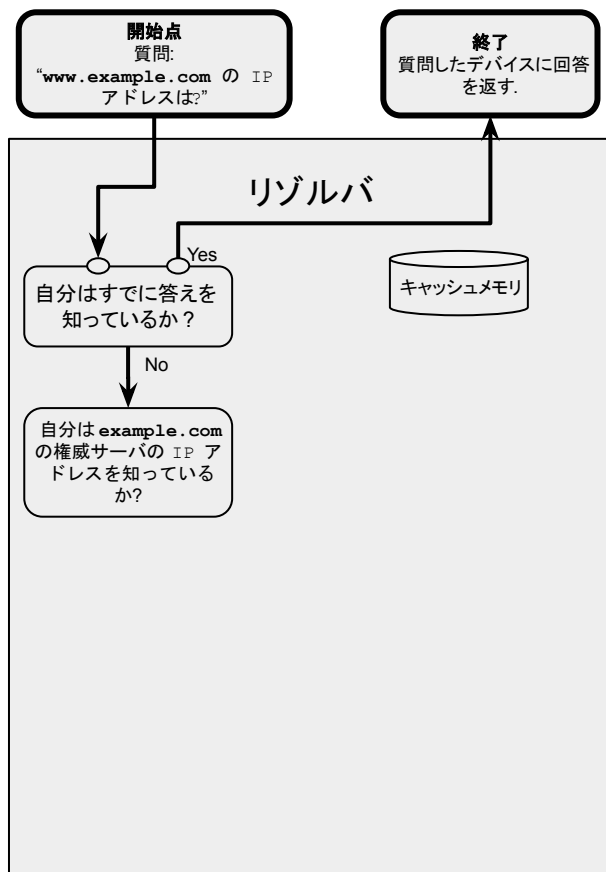
- リゾルバは一度得たアドレスを記憶する
 - キャッシュと呼ばれる動作
 - ほとんどの場合キャッシュから応答される
- たまに、新しく調べ直したりキャッシュのアドレスを確認する必要
- 場合によって以下のような情報が必要:
 1. ドメイン名の権威サーバ
 2. ドメイン名とTLDの権威サーバ
 3. ドメイン名とTLDとrootの権威サーバ





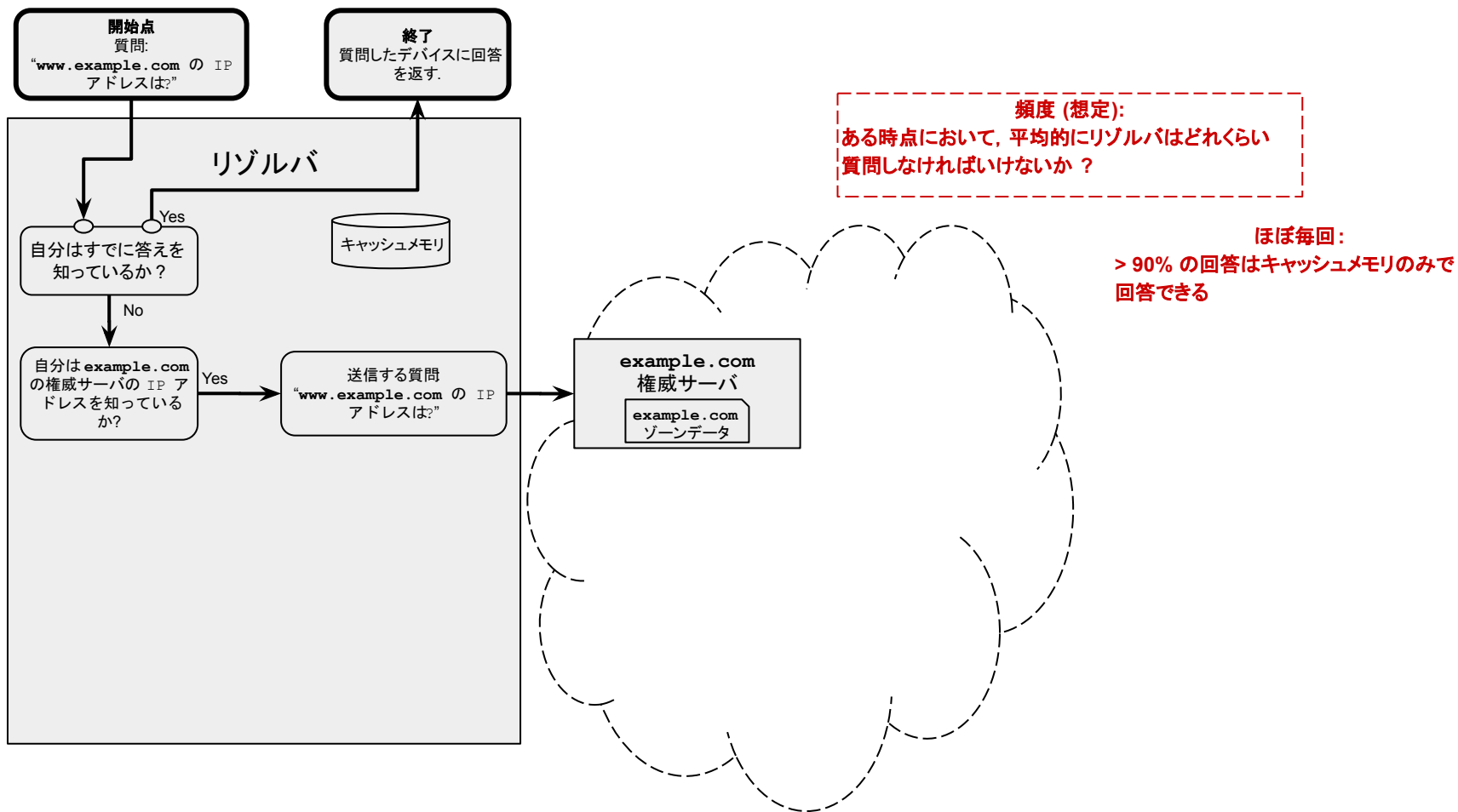
頻度 (想定):
ある時点において、平均的にリゾルバはどれくらい
質問しなければいけないか？

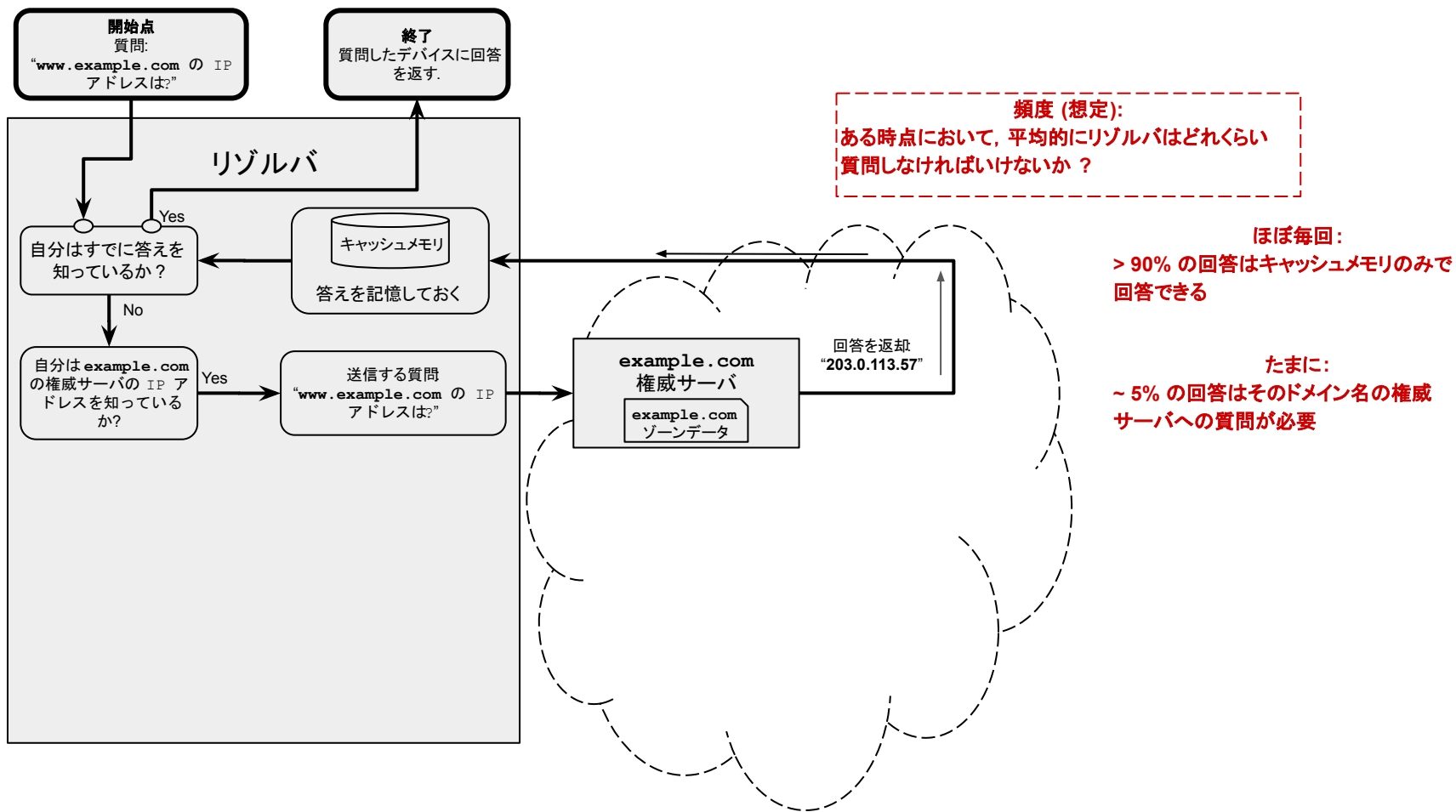
ほぼ毎回:
> 90% の回答はキャッシュメモリのみで
回答できる

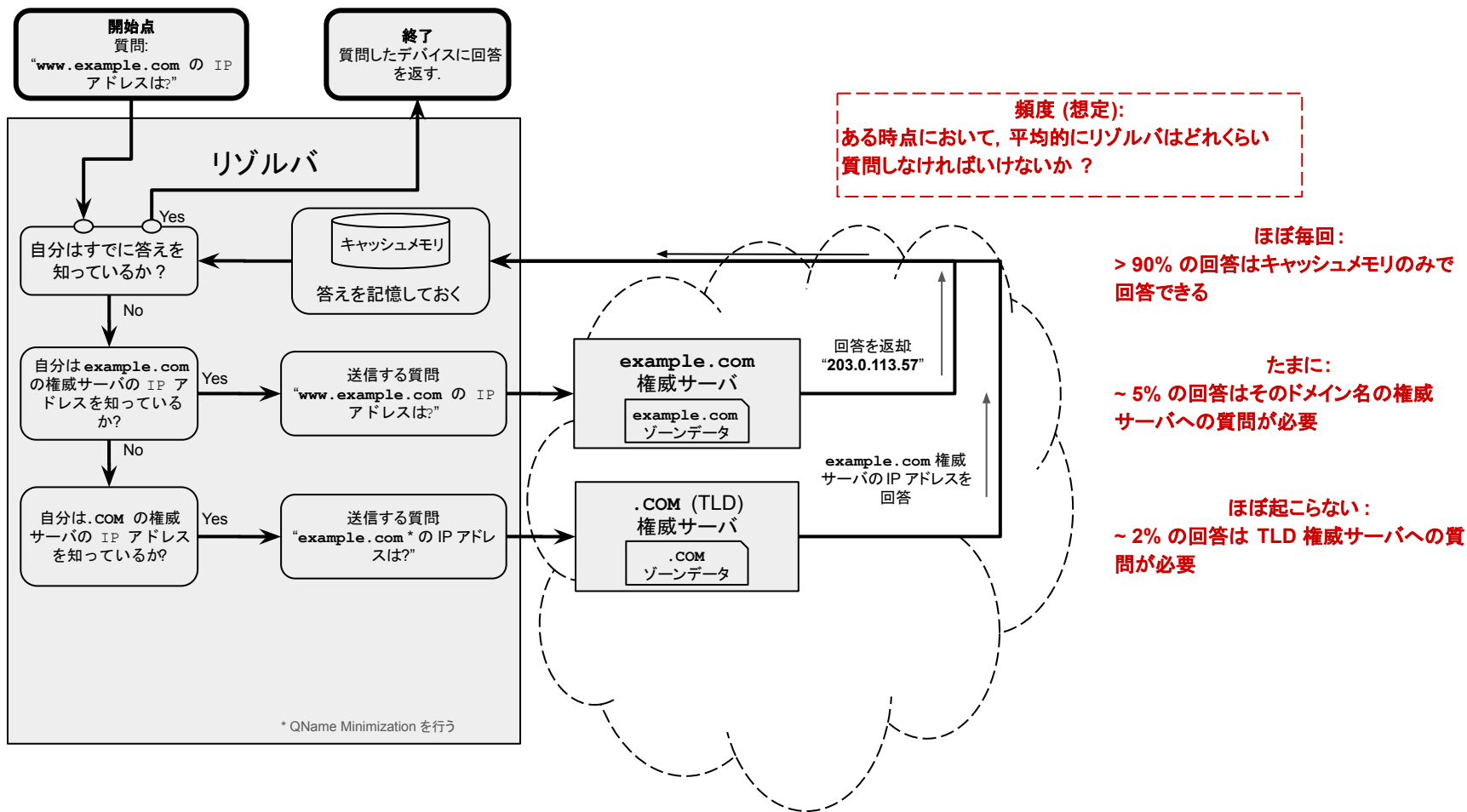


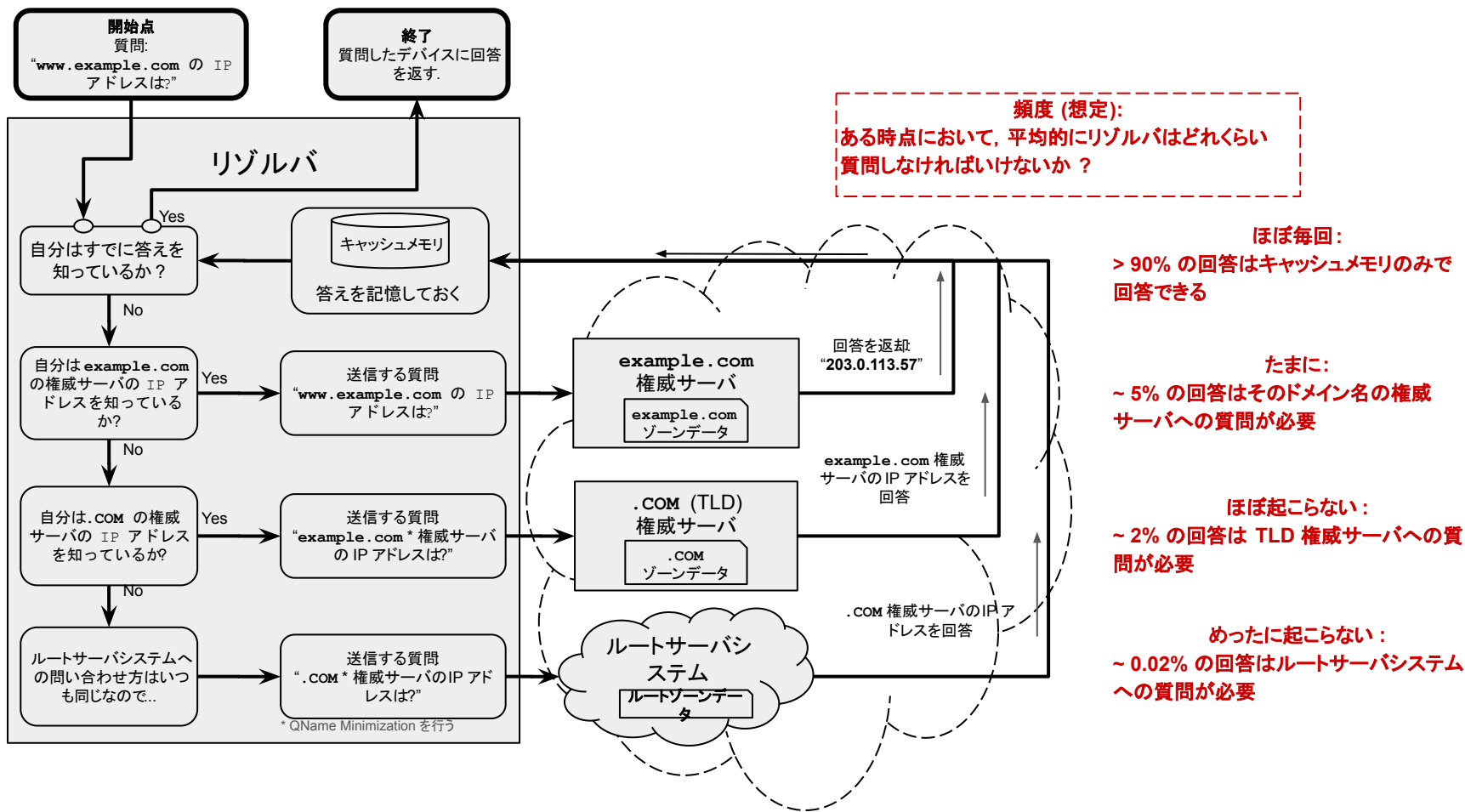
頻度 (想定):
ある時点において, 平均的にリゾルバはどれくらい
質問しなければいけないか?

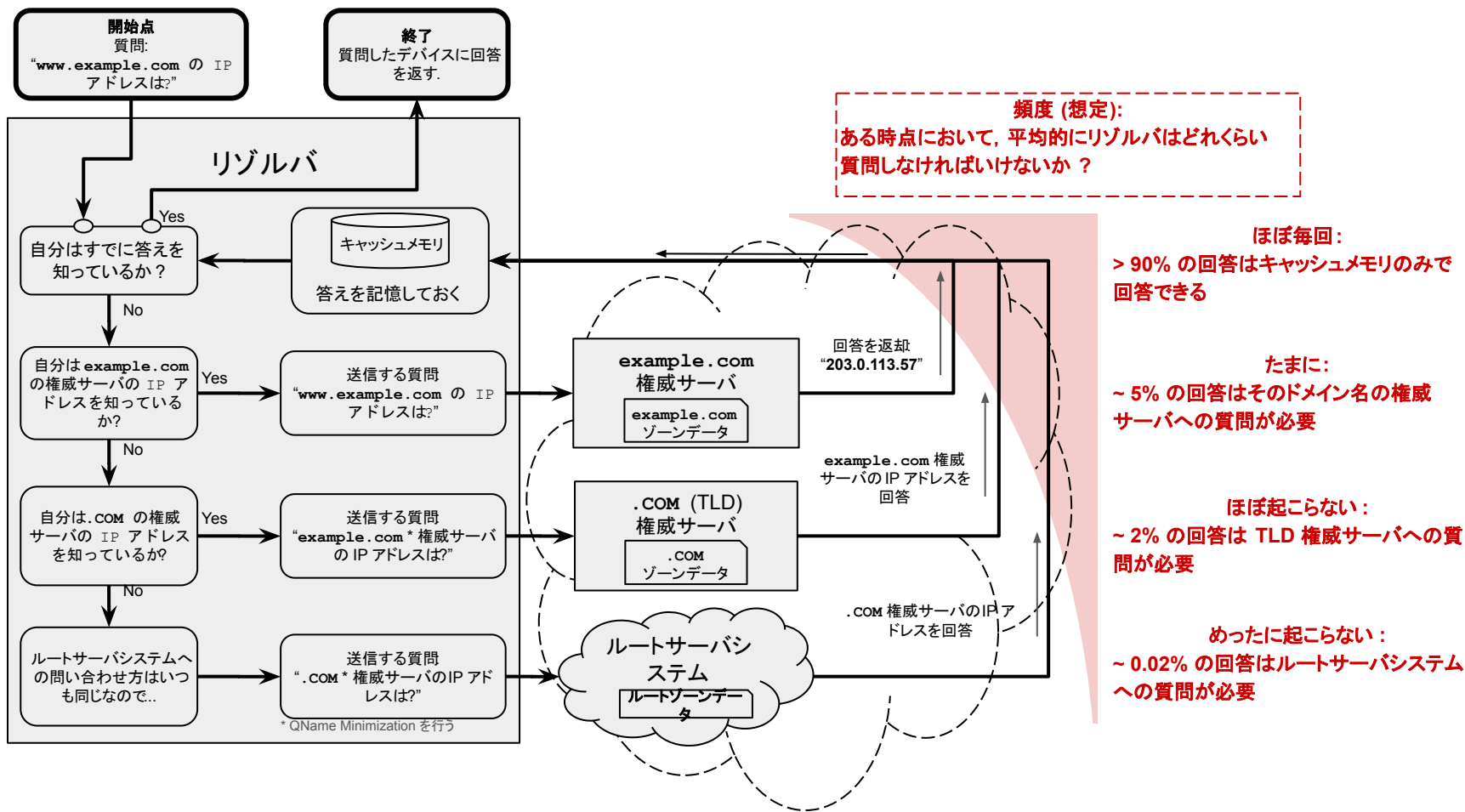
ほぼ毎回:
> 90% の回答はキャッシュメモリのみで
回答できる











まとめると

- **ルートサーバ**は**ルートゾーンデータ**のコピーを持つ
ルートゾーンは以下のような TLD のアドレスを知っている:
 - .com
 - .nl
 - .jobs (などなど)
- **TLD 権威サーバ**は次のステップへのアドレスを知っている
 - amazon.com や tiktok.com のような .com で終わるすべての名前
 - google.nl や amsterdam.nl のような .nl で終わるすべての名前
 - tech.jobs や highpay.jobs のような .jobs で終わるすべての名前
- **各ドメイン名の権威サーバ**は以下を知っている
 - www.amazon.com や mail.amazon.com や info.amazon.com に関する質問への答え
- **リゾルバ**がそれらを見つけて端末に返答する

リゾルバでのミリ秒単位の世界では、ルートサーバシステムへの質問はごくまれにしか発生しない。

ルートサーバシステムの運用

- **世界中に分散・大規模冗長化**された 1700 以上のサーバインスタンス
 - 各サーバはルートゾーンデータの「すべて」を持っている
 - 多様なハードウェアプラットフォーム
 - 多様な OS
 - 多様な DNS アプリケーション
 - 多様なデータルーティング
- 要するに: **技術的に単一点は存在しない**

ルートサーバシステムの運用

- 独立した 12 の運用者 (RSO) による協働運用

- 各 RSO は他の RSO から独立している
- RSO たちは継続的に他の RSO と協働している
- 単一 RSO に不可抗力 (Force majeure) が発生しても、運用上他の RSO には影響しない

- 要するに: 組織体制的に単一点は存在しない

RSO はルートゾーンデータの内容に干渉しない

- ゾーンデータはどうやって作られるか?
 - ドメイン名登録者が各ドメインのデータを管理する
 - ドメイン名登録者はレジストラを通して、権威サーバのアドレス情報をTLDレジストリに提供する
 - TLDレジストリはTLD権威サーバのアドレス情報をIANAに提供し、ルートゾーンに組み込まれる
 - IANAが認証後にルートゾーンデータの変更をルートゾーン管理者(RZM・IANA外部の立場)に送る
 - RZMがデジタル署名を付与し、RSOに送ることでルートゾーンとして使用される
- **RSOはIANAが送ってきたものをただ提供するだけ**

40 年の安定性・安全性・弾力性 (SSR)

- ルートサーバシステムは 1980 年代から今日まで運用
- 一度も大規模障害を発生していない
 - DDoS 攻撃は何度も試みられたが、すべて by design で失敗

まとめ

- ルートサーバシステムは名前解決において**重要ながら頻繁には使われない**
 - ほとんどの DNS クエリはキャッシュメモリから回答される
 - その他のクエリのほとんどは各ドメイン名の権威サーバから回答される
- ルートサーバ運用者 (RSO) はその**内容に干渉しない**
- ルートサーバシステムは
 - 何重にも冗長化されている
 - 技術的に多様である
 - 組織体制的に弾力性がある
- **The root server system works**