DNSとプライバシー

V0.1.1

株式会社インターネットイニシアティブ
其田　学

Ongoing Innovation

Internet Initiative Japan

なぜDNSのプライバシーが重要になってきたのか

DNSメッセージ＝通信の一部

どこに通信しようとしているのか（A,AAAA）
何をしようとしているのか（MXとか）

▼

DNSメッセージの収集≒個人の通信記録の収集

きっかけはスノーデン事件

米国政府による広範囲な通信の監視がなされていることが明らかに

米国だけでは無く、様々な国、組織がネットワークの監視をしている

▼

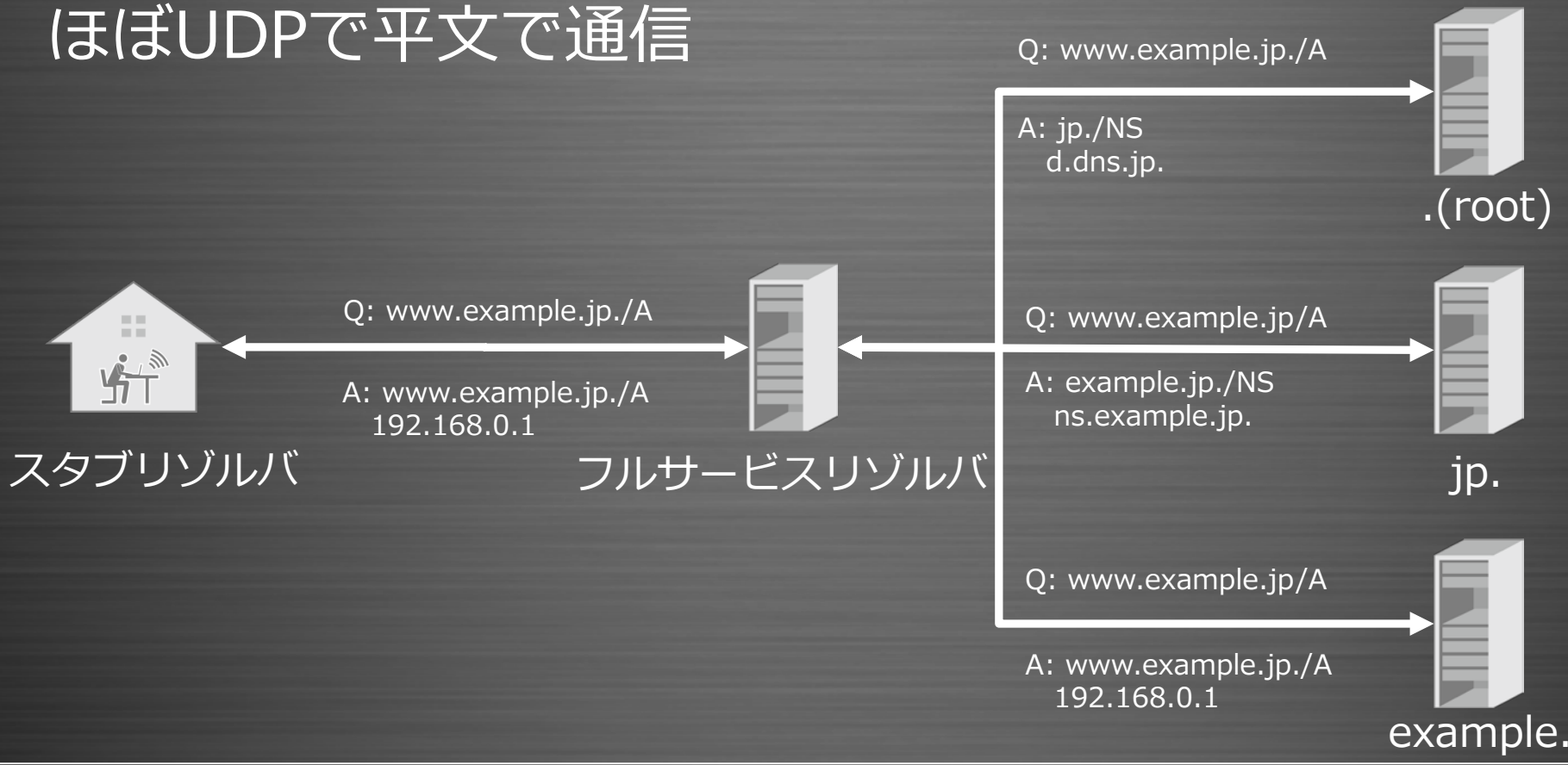
RFC7258 Pervasive Monitoring Is an Attack

大規模な盗聴行為は攻撃である

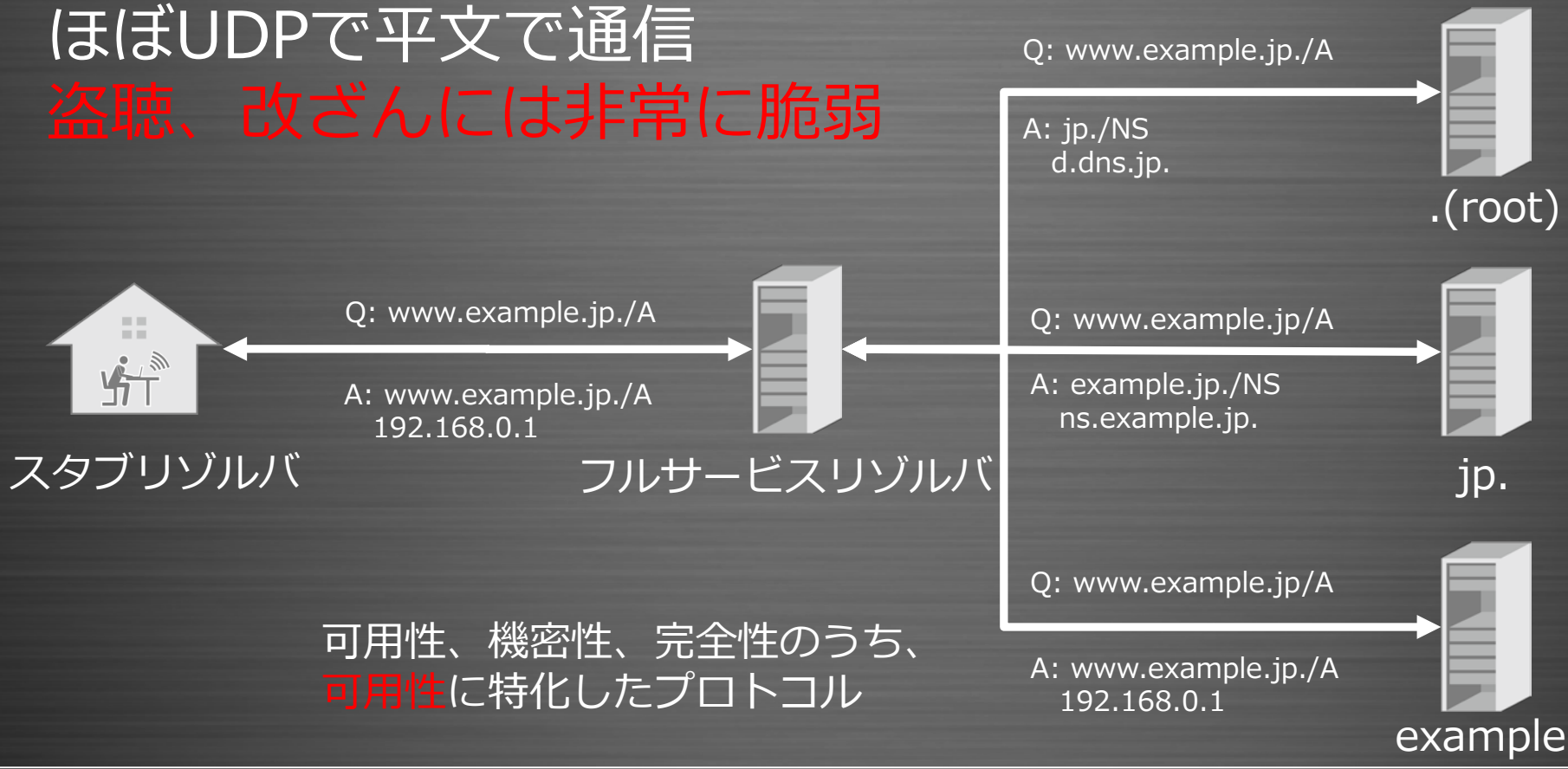
IETFで設計されるプロトコルは、これらの脅威を軽減するような
考慮がされていなければならない。

で、DNSプロトコルは？

ほぼUDPで平文で通信



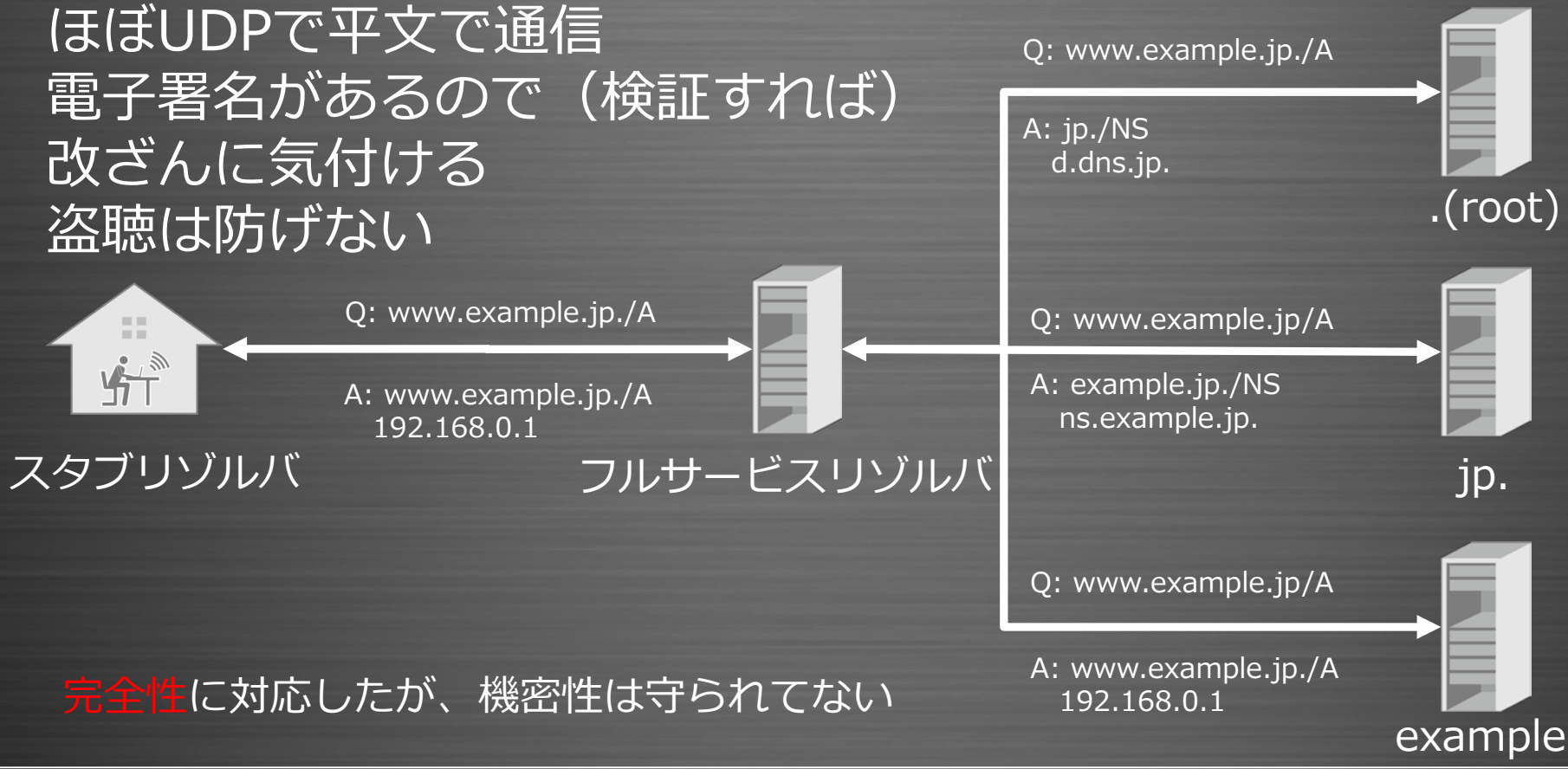
ほぼUDPで平文で通信
盗聴、改ざんには非常に脆弱



可用性、機密性、完全性のうち、
可用性に特化したプロトコル

DNSSEC

ほぼUDPで平文で通信
電子署名があるので（検証すれば）
改ざんに気付ける
盗聴は防げない



完全性に対応したが、機密性は守られてない

盗聴行為を防ぐ新しいDNSプロトコル達

権威DNSーフルリゾルバ間

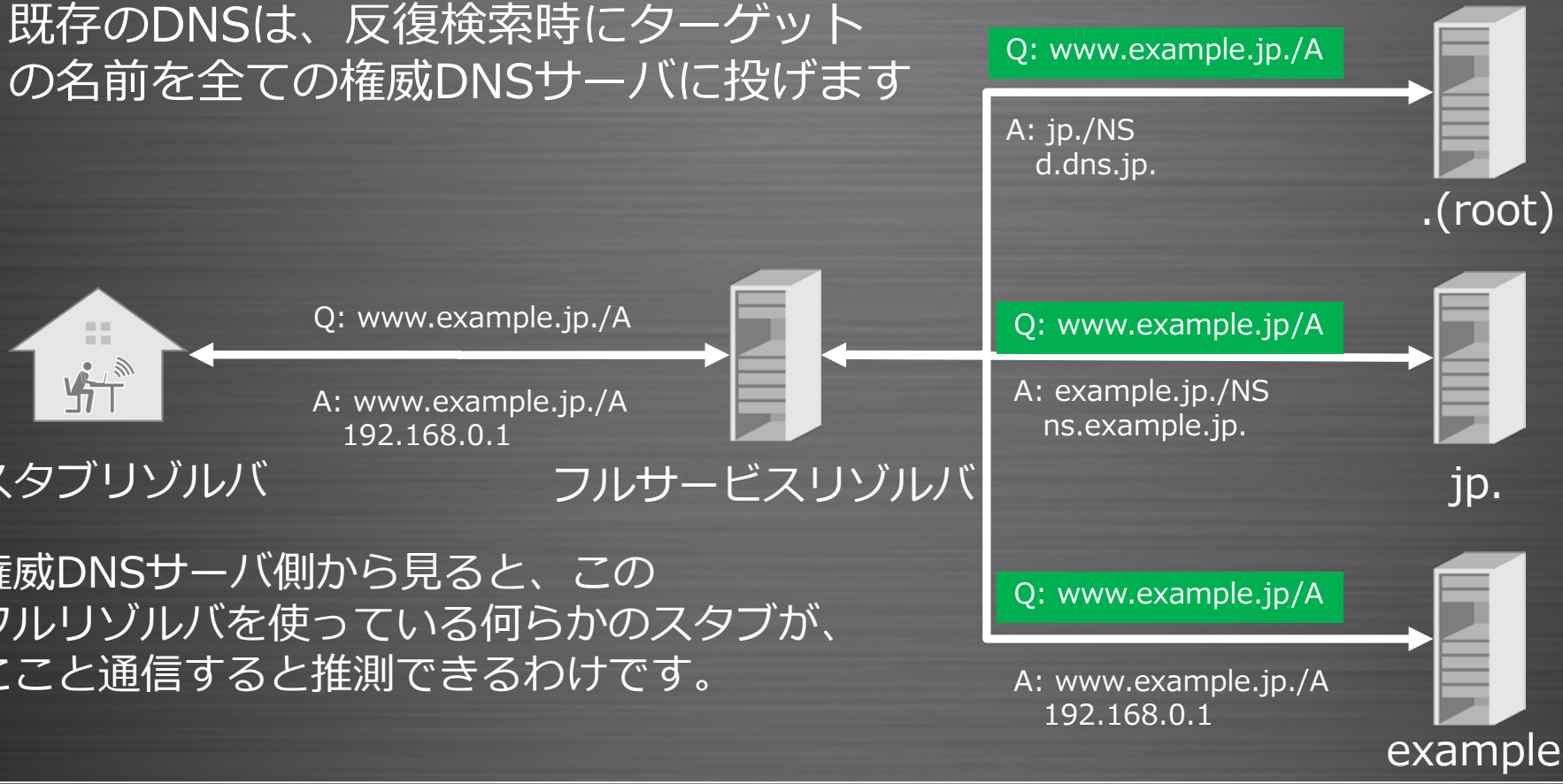
- QNAME minimization
- DNS over TLS

フルリゾルバースタブリゾルバ間

- DNS over TLS
- DNS over HTTPS
- DNS over DTLS

QNAME minimization(舌かみそう)

既存のDNSは、反復検索時にターゲット
の名前を全ての権威DNSサーバに投げます

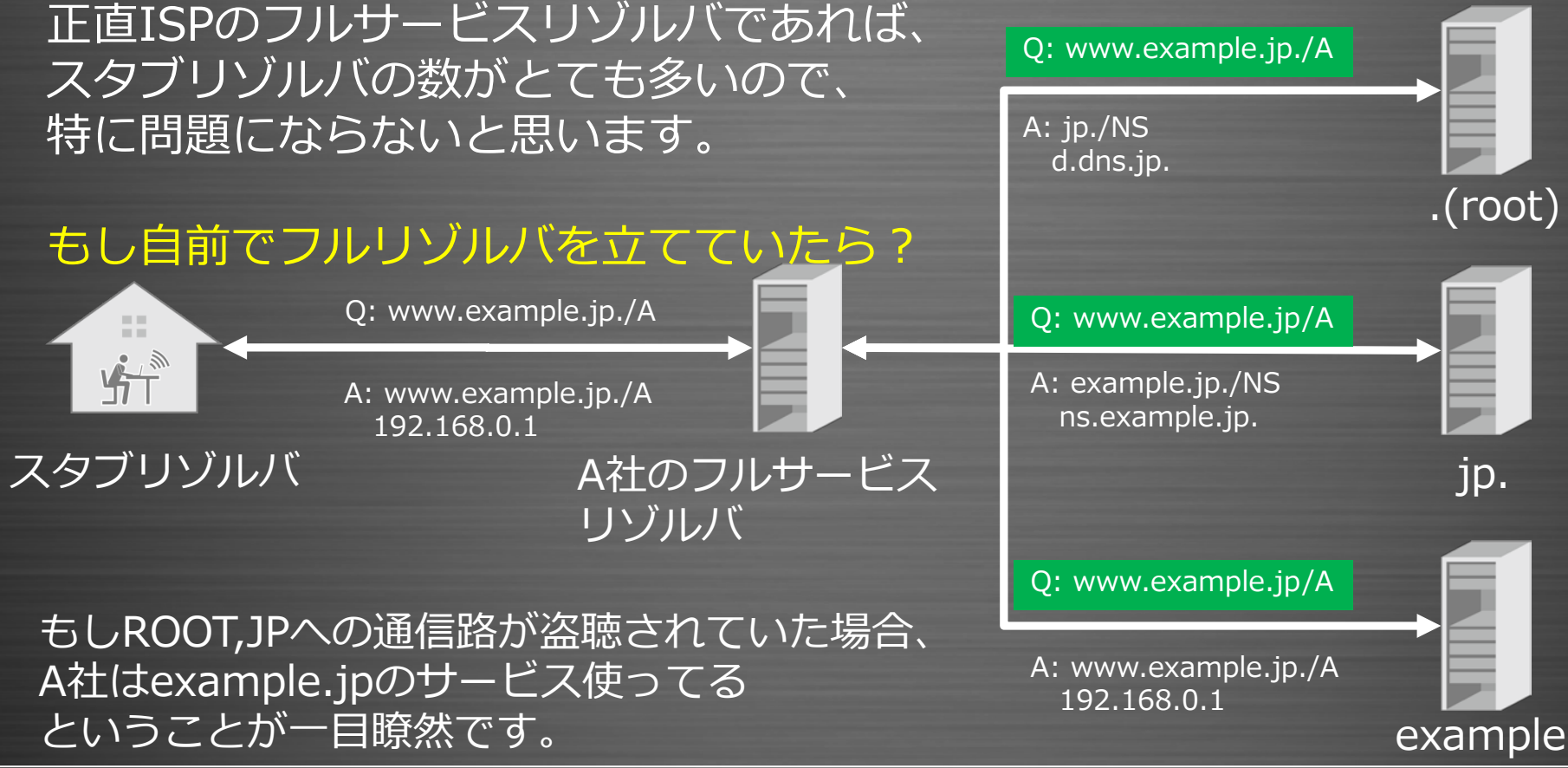


権威DNSサーバ側から見ると、この
フルリゾルバを使っている何らかのスタブが、
ここと通信すると推測できるわけです。

QNAME minimization(舌かみそう)

正直ISPのフルサービスリゾルバであれば、
スタブリゾルバの数がとても多いので、
特に問題にならないと思います。

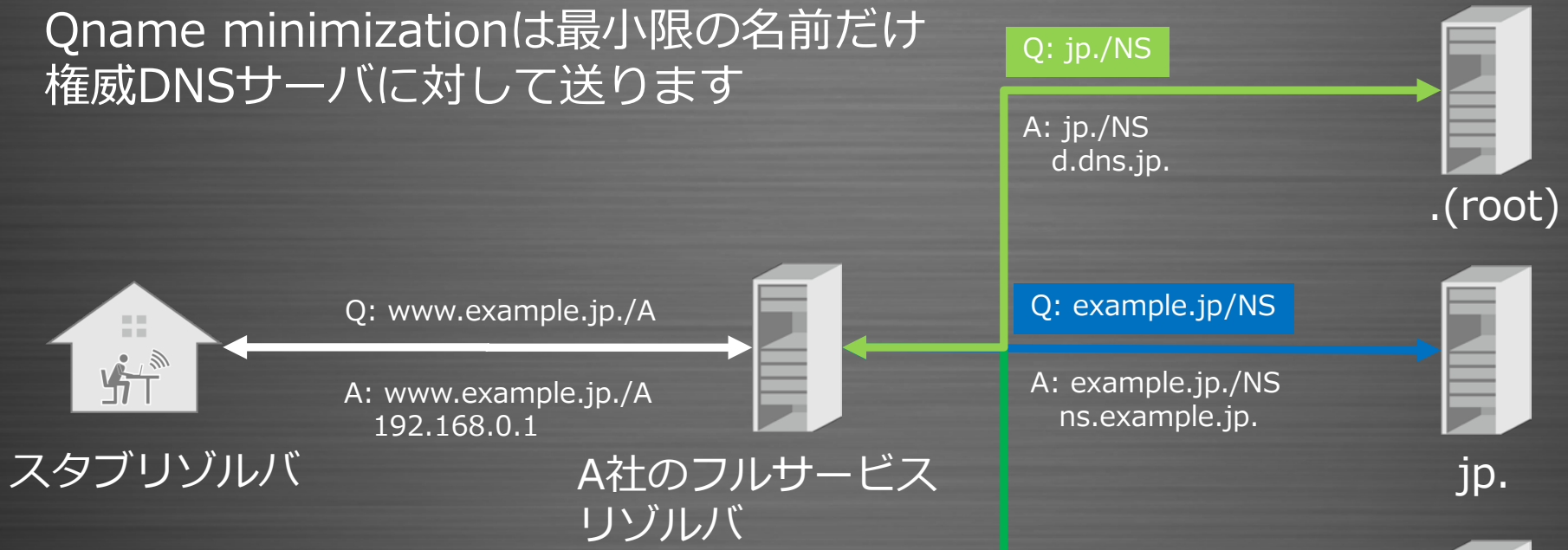
もし自前でフルリゾルバを立てていたら？



もしROOT,JPへの通信路が盗聴されていた場合、
A社はexample.jpのサービス使ってる
ということが一目瞭然です。

QNAME minimization(舌かみそう)

Qname minimizationは最小限の名前だけ
権威DNSサーバに対して送ります



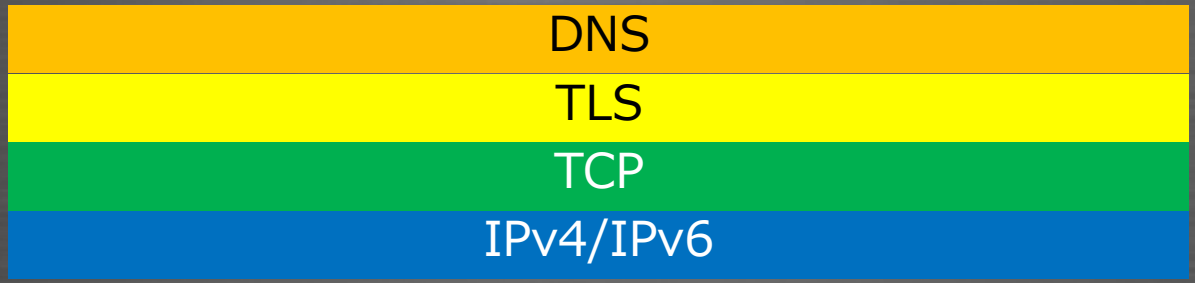
これにより、rootやTLDの権威DNSサーバの
ネットワークを盗聴されたとしても、
得られる情報は最小限になります。

DNS over TLS(DoT)

TLS上にTCPのDNSメッセージを載せたプロトコルです。
HTTPに対するHTTPSとまったく同じ発想のものです。
TLSに包むだけなので最も実装が容易です

現在は主にフルサービスリゾルバ＝スタブリゾルバ間で使われていますが
将来的にはフルサービスリゾルバ＝権威DNS間でも使われるようになるはず。

スタブリゾルバ

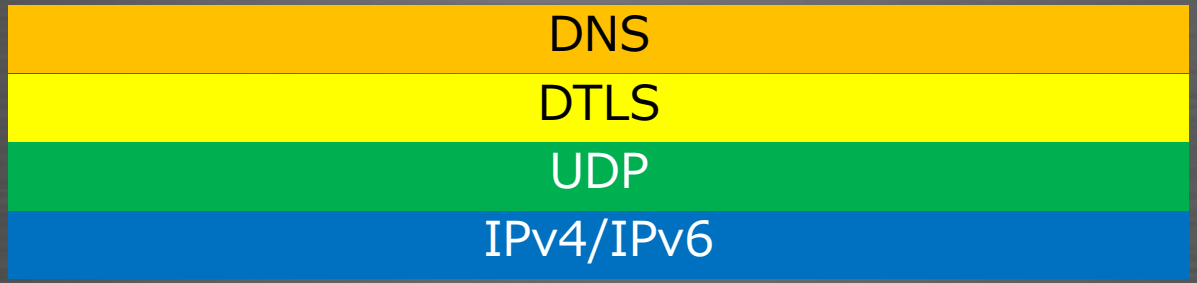


フルサービス
リゾルバ

DNS over DTLS(DoD)

DTLS上にDNSメッセージを載せたプロトコルです。
DTLS実装が難しいためか、使える実装はなく、
実装しようとする人もいないので、今後普及することはないです

スタブリゾルバ

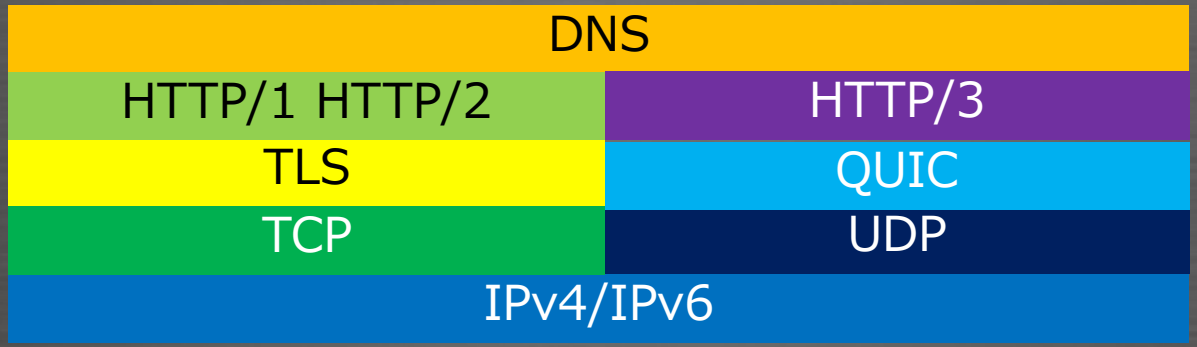


フルサービス
リゾルバ

DNS over HTTPS(DoH)

HTTPS上にDNSメッセージを載せたプロトコルです。
リクエストは、GET/POSTに対応していますが、一般的にはPOSTを使います。
（GETだとアクセスログ等にリクエストしたパケットが残ってしまう為）

スタブリゾルバ

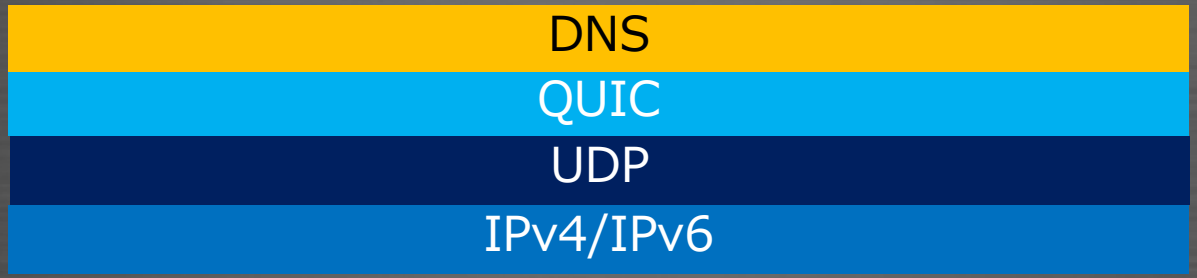


フルサービス
リゾルバ

DNS over Quic(DoQ)

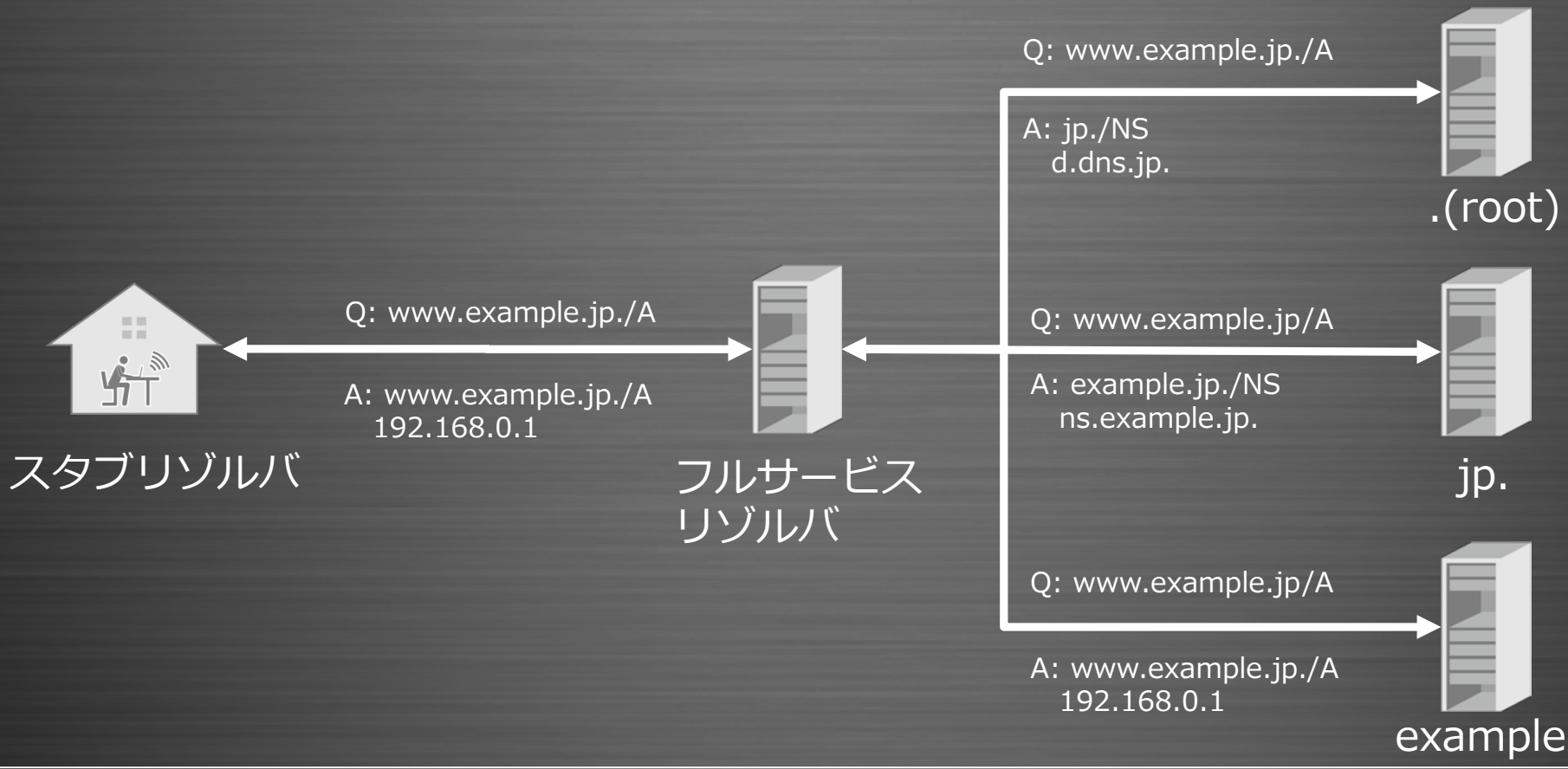
QUIC上にDNSメッセージを載せたプロトコルです。

スタブリゾルバ

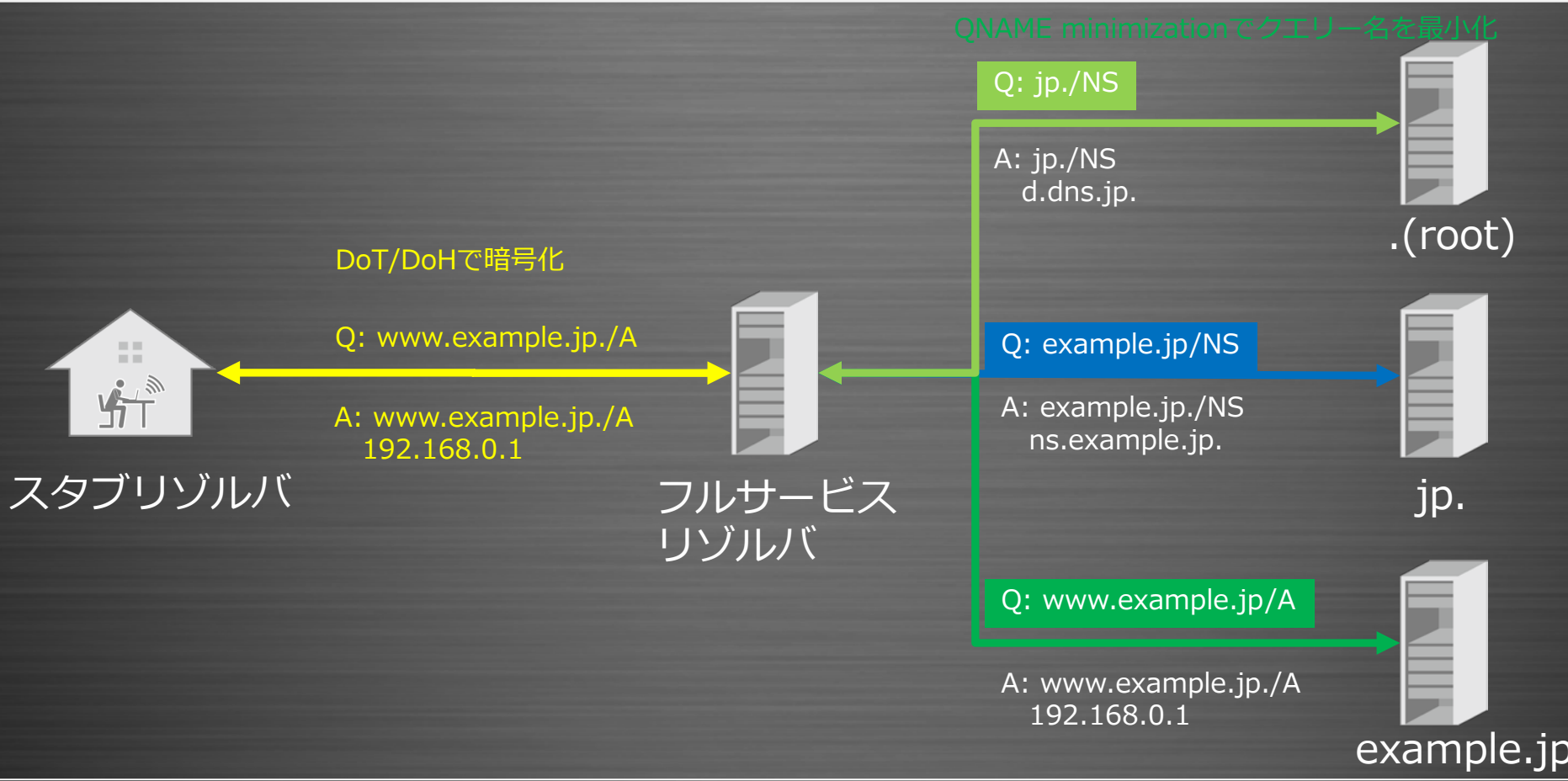


フルサービス
リゾルバ

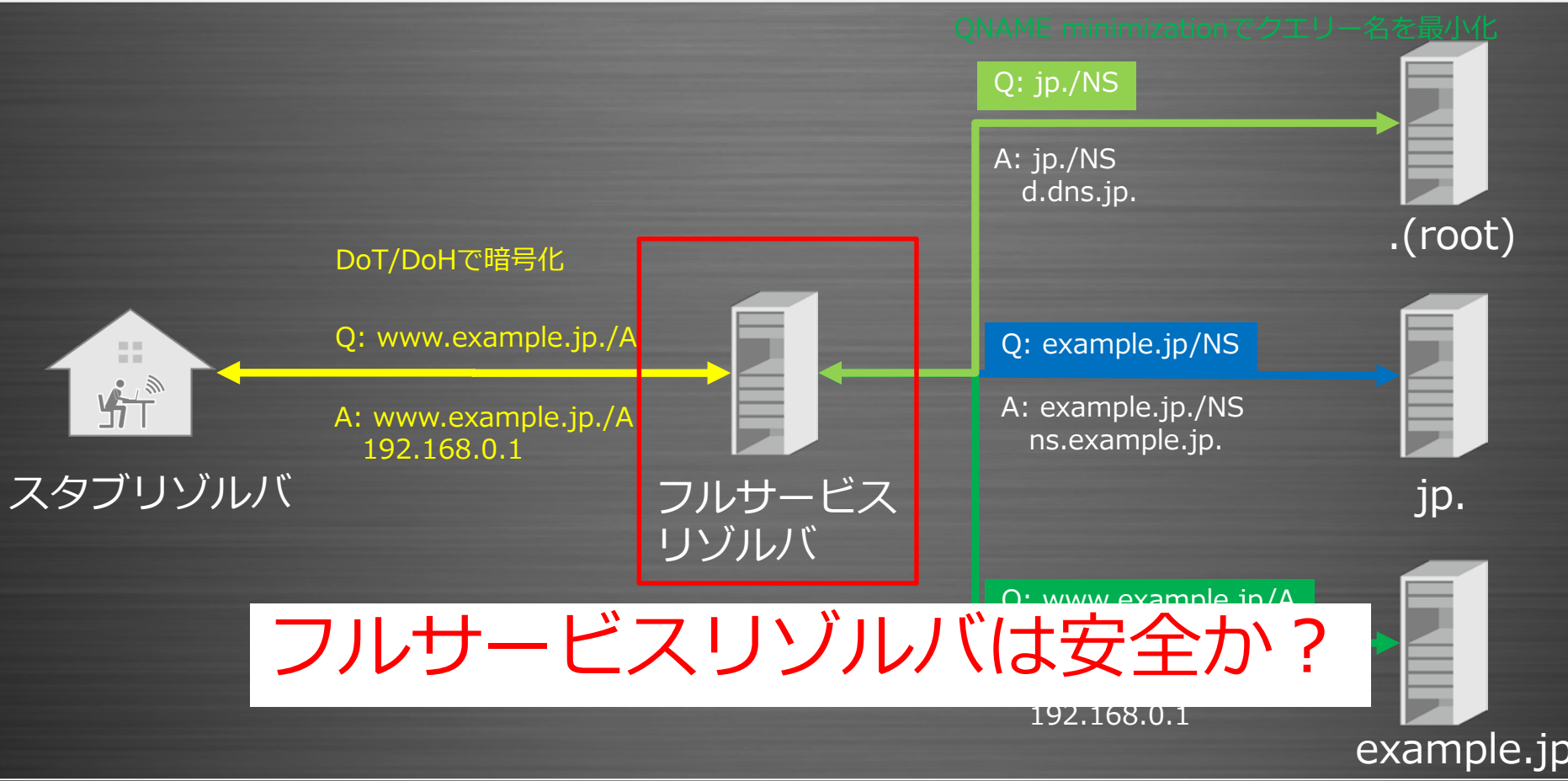
従来のDNS



現状頑張るとこんな感じ



現状頑張るとこんな感じ



フルサービスリゾルバとDNSプライバシー

- 自前リゾルバなら自前リゾルバ上で盗聴されるリスクは低いです。
  - まだ、反復検索を盗聴されるリスクは残ります。
- ISPのリゾルバは安全？
  - 運用管理上必要であれば正当業務行為としてクエリログは取れます。
    - そのクエリログを同意なく転用しようとしたらアウト
    - 万が一そのクエリログが外部に漏れたら。。。。。。

フルサービスとDNSプライバシー

- Public DNSは安全？
  - 海外の会社で、実態が日本にない場合は日本法は適用されません。
    - 通信の秘密なに、それ美味しいの？
    - 適用しようとしている議論はあります！
  - Public DNS のポリシーを読みましょう。
    - Google
      - https://developers.google.com/speed/public-dns/privacy
    - Quad9
      - https://www.quad9.net/policy/
    - 1.1.1.1
      - https://developers.cloudflare.com/1.1.1.1/
  - IPアドレスを削ったりして、匿名化、追跡不能化されたデータはDNS以外の用途で利用される場合があることがある。
    - セキュリティベンダに提供、広告配信、CDNのために転用など

draft-ietf-dprive-bcp-op

DNSプロバイダとしてのベストプラクティス

6.1.1 推奨されるポリシー

- IPアドレスは個人識別情報として扱うことを定めること。
- IPアドレスが記録されているか公開する
- どのようなデータが記録されているか、（集計したデータも含めて）公開する
  - また、保存期間、パートナーとの共有、第３者への共有、移転、販売があるか明記する
- 上記の例外を事項を定めること。
  - 攻撃を受けている場合など
- パートナー第三者の出所を公開する
- ユーザのDNSデータが事業者の他のデータと関連づけするかどうか公開する

draft-ietf-dprive-bcp-op

レスポンスフィルタリング
下記のカテゴリについて、フィルタリングリストの作成、管理方法、第３者のソースを使うかを明記する必要があります。

- ネットワーク、コンピュータセキュリティ上の理由
  - ボットネットとか
- 裁判所、または公的機関による拘束力のある命令
  - 日本だと無いのかも
- 自主的な法的理由
- 商業的な理由を含むその他の理由

Mozilla’s Trusted Recursive Resolver(TRR) Requirements

Mozilla(Firefox)のTRR Programのパートナーとして満たさなければならない
最低限度の要求事項

プライバシー、透明性、ブロッキングの３つからなる

今の所、唯一公に出ている、
フルサービスリゾルバに対してのプライバシー要求仕様

https://wiki.mozilla.org/Security/DOH-resolver-policy

プライバシー

リゾルバでのユーザデータ（クエリ）の収集と共有を制限する

内容

1. 利用者に紐づくデータをサービスを運営する目的のみで収集できる。
   ただし24時間以上は保持してはならない。
2. 法律で要求される場合を除き、DNSクエリ情報やIPアドレス、
   その他ユーザ情報を、保持、第３者へ譲渡、移転、販売してはならない
3. エンドユーザを識別してクエリーから収集したデータと、
   その他のデータを組み合わせてはならない。
4. ユーザーデータに対する権利を他の個人、組織に販売、使用許諾してはならない。
5. QNAME minimizationに対応しなければならない
6. 権威DNSサーバに対して不必要な情報を伝えてはならない。
   特にEDNS Client SUBNET拡張は権威DNSサーバとの接続が暗号化が必須…(略

透明性

データの収集に透明性がなければならない

以下の内容を文書化し公開しなければない。

- 24時間保存されるデータの項目
- 24時間を超えて保存される集計データの項目
- プライバシーの2–4項に対するポリシー
- ユーザデータに対する法執行機関からの開示要求をどのように処理するかの文書化
- 開示が禁止されている場合を除き、開示要求、回答の種類と数を文書化

ブロッキング、改ざんの禁止

- リゾルバを運営する地域の法律で要求されている場合を除き、デフォルトでドメインをブロッキング、フィルタリングしてはならない。
- ブロッキング、フィルタリングを行う場合、ユーザの明示的な同意を得なければならない。
  また、ブロッキングされているドメインの公開と、特定のドメインがいつ、ブロックリストに追加、削除されたかログを保持しなければならない。
- NXDOMAIN応答を修正して、代替コンテンツの応答をしてならない。

Mozilla’s Trusted Recursive Resolver(TRR) Requirements

- 何もブロッキングしない、ログも取らないなら楽々通るポリシー
- 何かやろうとすると、透明性が求められるようになる。
- 今後同様のものがChromeなりAndroidなりにもできることが予想される

フルリゾルバのプライバシーの基準として、 TRR Requirementsが
求められる時代がくるかも

public.dns.iij.jpの例

https://public.dns.iij.jp/

本サービスの提供における利用者に係るデータの取扱いは、以下のとおりとします。
（1）DNSのリクエストデータ及びレスポンスデータを取得します。
　　データの取得範囲（実際はもっと詳しい内容が書かれている）
（2）個人が特定できるデータを取得することはありません。
　　個人が特定できるデータ持つの大変なので、持ちません宣言！
（3）取得したデータは、本サービスの運用及びDNSの研究調査のためにのみ用いられます。
　　データの利用内容

public.dns.iij.jpの例

（4）取得したデータは、有償、無償を問わず、第三者に提供されません。
　　データの第三者への移転の有無
（5）取得したデータは、取得後、24時間以内に当社設備から削除されます。
　　データの保存期間
（6）統計処理したデータを保存し、DNSの研究発表のために使用することがあります。
　　統計化したデータの取り扱い

まとめ

- DNSでもプライバシーが重要視され始めています
- それに対応したプロトコルも既に使えます
  - DoT, DoH, QNAME minimization

- また、フルサービスリゾルバにもプライバシーが求められています
  - TRR Requirementsはその基準になっていくかもしれません

Ongoing Innovation

IIJ Internet Initiative Japan

ご清聴ありがとうございました