

ECS(RFC 7871)を实际使おうと思うと困ること

～商用利用を前提とした検証結果の共有～

免責事項

発表内容は個人の見解であり、所属する組織の見解やソフトウェア開発元の見解を示すものではありません。

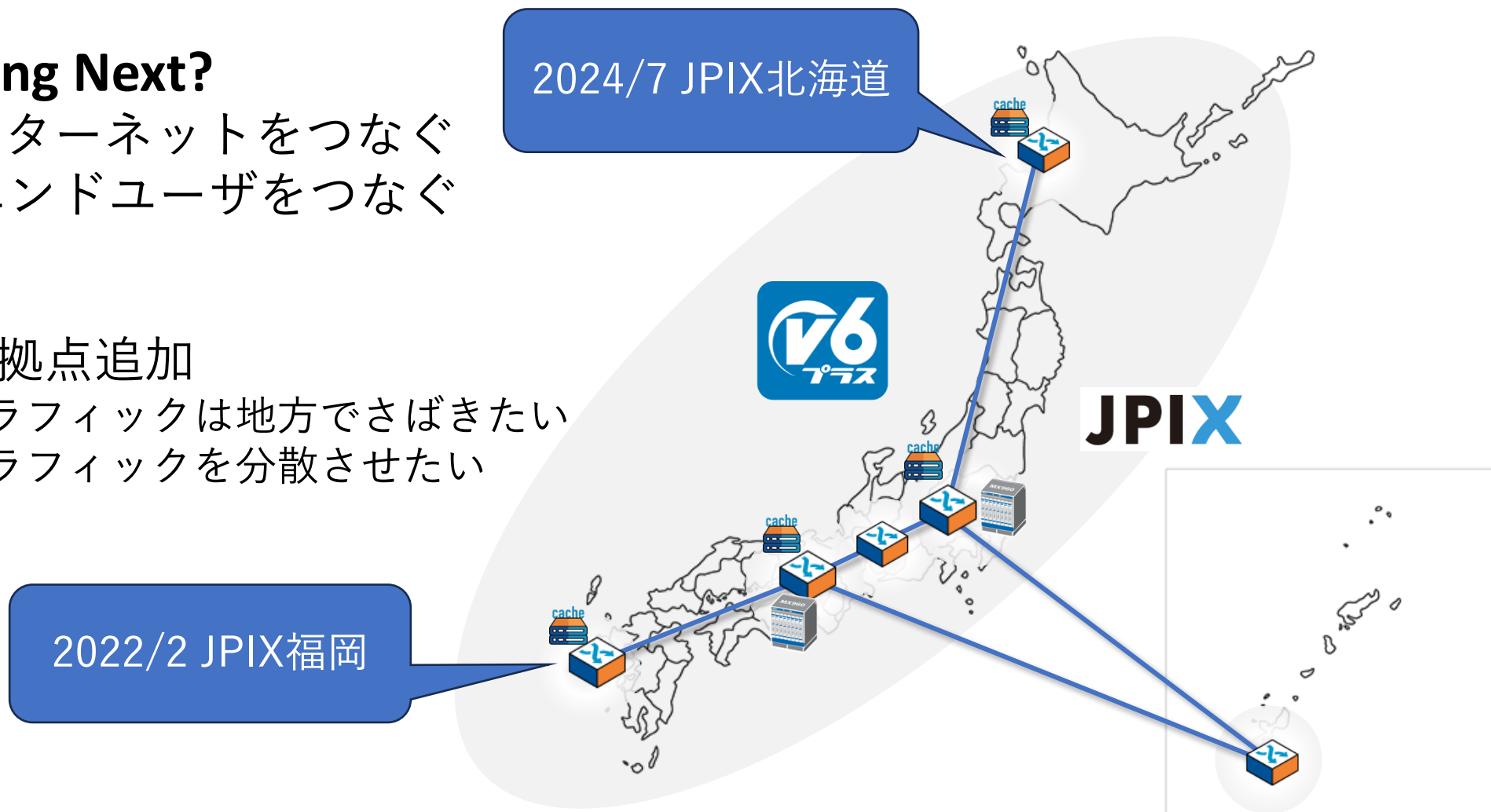
2025年7月30日
株式会社JPIX

What's Crossing Next?

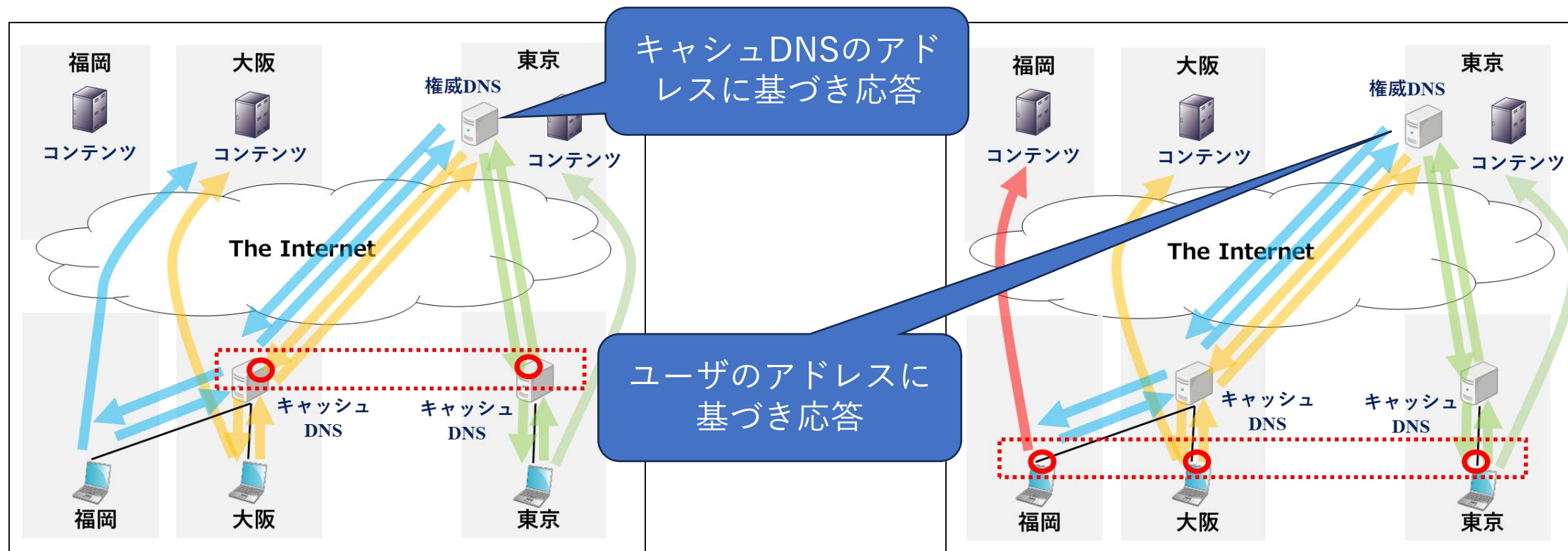
- ✓ IXでインターネットをつなぐ
- ✓ VNEでエンドユーザをつなぐ

北海道、福岡拠点追加

- 地方のトラフィックは地方でさばきたい
- 地方にトラフィックを分散させたい



DNSのECS（EDNS Client Subnet）とは、DNSの拡張プロトコルであるEDNS0を使用して、DNSクエリにユーザのアドレス情報を追加する技術です。（RFC7871）
ECSにより、ユーザの地理的な位置に基づいて最適なサーバーを選択し、より迅速な応答を提供することができます。



RFC7871 Client Subnet in DNS Queries

7.1.1. Recursive Resolvers

キャッシュDNSのクエリについて

7.2.1. Authoritative Nameserver

権威DNSの応答について

7.3.1. Caching the Response

キャッシュDNSのキャッシュについて

maximum cacheable prefix length

- キャッシュDNS側で設定する
- キャッシュする範囲（prefix長）の最大値

source prefix length

- キャッシュDNS側で設定する
- クエリに含むユーザアドレスの範囲（prefix長）

scope prefix length

- 権威側DNSで設定する
- アンサーが有効なユーザアドレスの範囲（prefix長）

7.1.1. Recursive Resolvers

In the usual case, where no ECS option was present in the client query, the Recursive Resolver initializes the option by setting FAMILY of the client's address. It then uses the value of its maximum cacheable prefix length to set SOURCE PREFIX-LENGTH.

If the triggering query included an ECS option itself, it MUST be examined for its SOURCE PREFIX-LENGTH. The Recursive Resolver's outgoing query MUST then set SOURCE PREFIX-LENGTH to the shorter of the incoming query's SOURCE PREFIX-LENGTH or the server's maximum cacheable prefix length.

Finally, in both cases, SCOPE PREFIX-LENGTH is set to 0 and ADDRESS is then added up to SOURCE PREFIX-LENGTH number of bits, with trailing 0 bits added, if needed, to fill the final octet.

通常の場合、クライアントクエリにECSオプションが存在しない場合、リカーシブリゾルバはクライアントのアドレスのFAMILYを設定してオプションを初期化します。その後、maximum cacheable prefix lengthの値を使用してsource prefix lengthを設定します。

トリガーとなったクエリ自体にECSオプションが含まれていた場合は、そのsource prefix lengthを確認しなければなりません。リカーシブリゾルバが送信するクエリでは、受信したクエリのsource prefix lengthとサーバーのmaximum cacheable prefix lengthのうち、短い方をsource prefix lengthとして設定しなければなりません。

最後に、どちらの場合でも、scope prefix lengthは0に設定され、ADDRESSにはsource prefix lengthのビット数までのアドレスが追加されます。必要に応じて、最後のオクテットを埋めるために末尾に0ビットが追加されます。

7.2.1. Authoritative Nameserver

The specific logic that an Authoritative Nameserver uses to choose a tailored response is not in the scope of this document. Implementers are encouraged, however, to carefully consider their selection of SCOPE PREFIX-LENGTH for the response in the event that the best tailored response cannot be determined, and what the implications would be over the life of the TTL.

Authoritative Nameservers might have situations where one Tailored Response is appropriate for a relatively broad address range, such as an IPv4 /20, except for some exceptions, such as a few /24 ranges within that /20. Because it can't be guaranteed that queries for all longer prefix lengths would arrive before one that would be answered by the shorter prefix length, an Authoritative Nameserver MUST NOT overlap prefixes.

権威DNSサーバーがカスタマイズされた応答を選択するための具体的なロジックは、この文書の範囲外です。しかし、実装者は、最適なカスタマイズ応答を決定できない場合に備えて、応答のscope prefix lengthの選択を慎重に検討し、そのTTLの期間中の影響を考慮することが推奨されます。

権威DNSサーバーは、IPv4 /20のような比較的広いアドレス範囲に対して適切な応答を提供する状況があるかもしれません。ただし、その/20内のいくつかの/24範囲のような例外もあります。すべてのより長いプレフィックス長（例：/24など）に対するクエリが、より短いプレフィックス長（例：/20）に対する応答よりも先に届くとは限らないため、権威DNSサーバーはプレフィックスを重複させてはなりません。

7.3.1. Caching the Response

If SCOPE PREFIX-LENGTH is not longer than SOURCE PREFIX-LENGTH, store SCOPE PREFIX-LENGTH bits of ADDRESS, and then mark the response as valid for all addresses that fall within that range.

Similarly, if SOURCE PREFIX-LENGTH is the maximum configured for the cache, store SOURCE PREFIX-LENGTH bits of ADDRESS, and then mark the response as valid for all addresses that fall within that range.

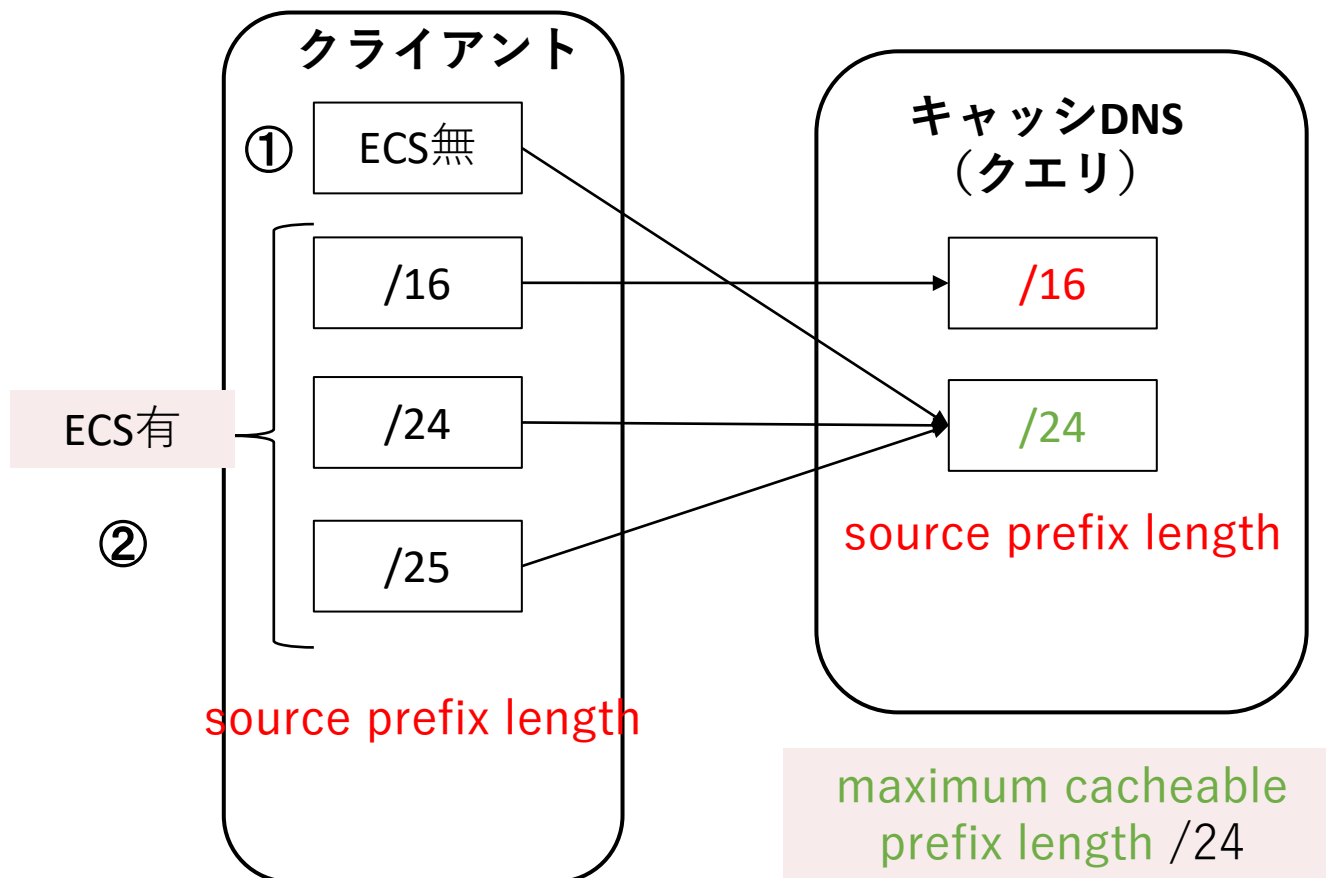
If SOURCE PREFIX-LENGTH is shorter than the configured maximum and SCOPE PREFIX-LENGTH is longer than SOURCE PREFIX-LENGTH, store SOURCE PREFIX-LENGTH bits of ADDRESS, and then mark the response as valid only to answer client queries that specify exactly the same SOURCE PREFIX-LENGTH in their own ECS option.

scope prefix lengthがsource prefix lengthより短い場合は、ADDRESSのうちscope prefix lengthビットを保存し、その範囲に含まれるすべてのアドレスに対してレスポンスが有効であるとマークします。

同様に、source prefix lengthがキャッシュに設定されたmaximum cacheable prefix lengthである場合は、ADDRESSのうちsource prefix lengthビットを保存し、その範囲に含まれるすべてのアドレスに対してレスポンスが有効であるとマークします。

source prefix lengthが設定されたmaximum cacheable prefix lengthより短く、かつscope prefix lengthがsource prefix lengthより長い場合は、ADDRESSのうちsource prefix lengthビットを保存し、同じsource prefix lengthをECSオプションに指定したクライアントクエリに対してのみレスポンスが有効であるとマークします。

7.1.1. Recursive Resolvers



① クライアントクエリにECSオプションが存在しない場合

maximum cacheable prefix lengthの値を
source prefix lengthに設定する。

② クライアントクエリにECSオプションが含まれていた場合

受信したクエリのsource prefix lengthと
maximum cacheable prefix lengthのうち、
短い方を設定する。

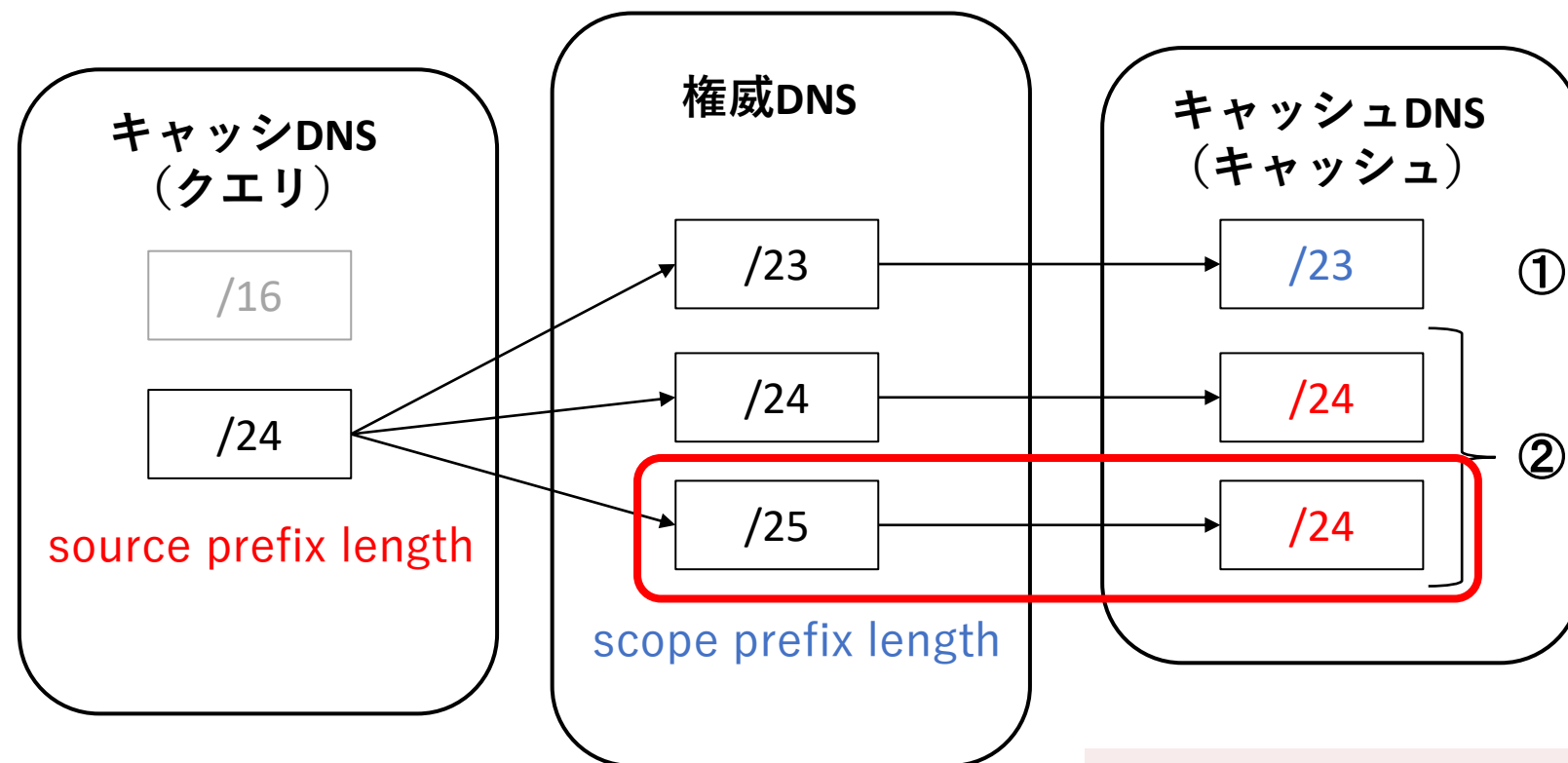
7.3.1. Caching the Response

- ① scope prefix lengthがsource prefix lengthより短い場合

scope prefix lengthビットでキャッシュする。

- ② source prefix lengthがmaximum cacheable prefix lengthである場合

source prefix lengthビットでキャッシュする。



maximum cacheable
prefix length /24

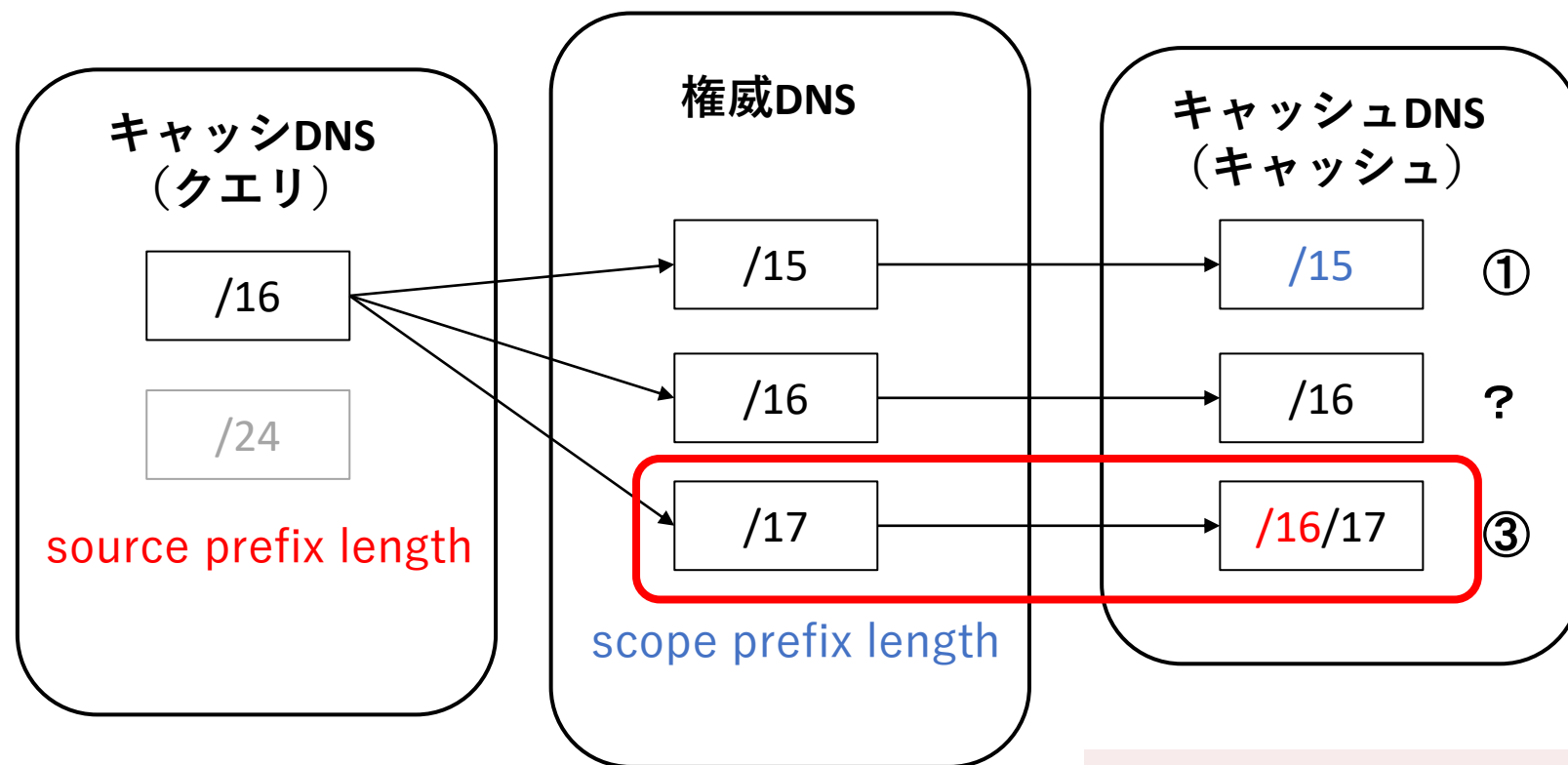
7.3.1. Caching the Response

- ① scope prefix lengthがsource prefix lengthより短い場合

scope prefix lengthビットでキャッシュする。

- ③ source prefix lengthが設定されたmaximum cacheable prefix lengthより短く、かつscope prefix lengthがsource prefix lengthより長い場合

source prefix lengthビットでキャッシュし、同じsource prefix lengthをECSオプションに指定したクライアントクエリに対してのみレスポンスが有効



7.2.1. Authoritative Nameserver

権威DNSサーバーはプレフィックスを重複してはいけない

1.2.0.0/20の範囲に対して応答Aを返すように設定されているが、例外として1.2.3.0/24に対しては応答Bを返す場合、1.2.3.0/24だけを例外として分離し、それ以外はできるだけ大きなブロックでまとめて応答Aを適用する。

応答A	応答B
1.2.0.0/23	
1.2.2.0/24	
1.2.4.0/22	1.2.3.0/24
1.2.8.0/21	

観点	メリット	デメリット
ユーザ	より近いコンテンツキャッシュを利用することにより高速なコンテンツ取得が可能となる	ユーザアドレスを晒すセキュリティリスクがある
事業者 (プロバイダ)	地方一都心間のトラフィック伝送コストが削減可能となる DNSをアウトソースしても適切にトラフィックをコントロールできる	DNS事業者やCP（CDN）との調整が必要となる
キャッシュDNS 権威DNS		キャッシュ(メモリ)が増える 新たな運用知識が必要となる 導入における機能検証が必要となる 構築にかかる設備コストが必要となる
CP（CDN）	トラフィック（リソース）分散が可能となる	

What's Crossing Next?

JPIX