DNS64
Akamai DNSi CacheServe のポリシー機能による課題解決

アカマイ・テクノロジーズ合同会社
シニア・ソリューション・エンジニア
松本 陽一

内容

- CacheServe のポリシー機能
- DNS64 と最近の話題
- DNS64 のオプション設定
- ポリシーの適用
  - Case 1 : IPv4 の接続もあるユーザ
  - Case 2 : NAT64/DNS64 と 464XLAT の振り分け
- まとめ

© Akamai Technologies, 2020
Akamai Experience the Edge

CacheServe のポリシー機能 (Precision Policy)

条件 (セレクタ) にマッチするクエリに特定の処理 (アクション) を行うルールの集合

- セレクタ: クエリの要素(送信元/先アドレス、QNAME、QTYPE、フラグ、曜日時刻 …) だけでなく、解決結果 (RCODE や値、サイズ) も条件にできる。AND/OR/NOT…
- アクション: アンサー内容、ドロップ、TC 応答、レートリミット、ロギング等… DNS64、DNS64逆引きもアクションとして実装

典型的な活用例

- ブロッキング、フィルタリング、アンプ攻撃対策等
- セキュリティやパーソナライゼーションのアプリケーション (SPS シリーズ)

AAAA フィルタリングのようなネットワーク、サービス運用上の課題解決にも
DNS64周りの各種課題への対応に役立つのでは？

注: ポリシー機能の利用にはオプション・ランセンスが必要

© Akamai Technologies, 2020
Akamai Experience the Edge

DNS64 とは

IPv6 のみのクライアントが IPv4 のみのサーバにアクセスさせるための技術として NAT64 と組み合わせて用いられる

- NAT64/DNS64 は、IPv6 のみのアクセスサービス上で IPv4 でアクセスさせる技術 (DS-Lite、MAP-E、MAP-T、464XLAT 等) と類似
  → 「10年前に IPv4アドレス枯渇対策で議論したよね。」

- NAT64/DNS64 ではクライアントは IPv6 オンリー
  →「IPv6 オンリー化へのステップとしてやっぱり必要？」

© Akamai Technologies, 2020
Akamai Experience the Edge

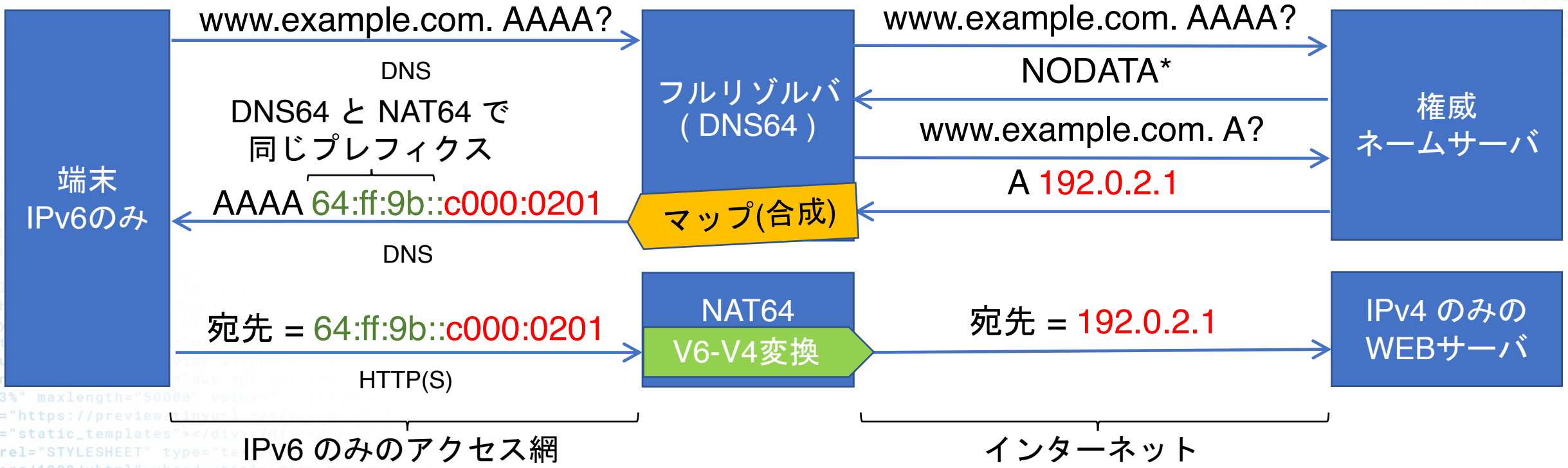
最近の DNS64 関連の話題

- BIGLOBE
  NAT64/DNS64 をモニターから正式サービスへ
  https://support.biglobe.ne.jp/ipv6/nat64.html
- NTT コミュニケーションズ 西塚 要 さん
  サーバーサイド Open NAT64
  https://qiita.com/__kaname__/items/0c77fb3b5fb01a796a4b
- Telstra
  NAT64/DNS64 + 464XLAT でモバイルサービスを IPv6 オンリー化
  http://lists.ausnog.net/pipermail/ausnog/2020-February/043869.html

© Akamai Technologies, 2020
Akamai Experience the Edge

DNS64 の動作

- クライアントからの AAAA クエリに対し、その名前に AAAA レコードが存在せず A レコードがある場合に A の IPv4 アドレスを IPv6 アドレスにマップした AAAA を返す



*NODATA: Answer セクションが空の NOERROR

© Akamai Technologies, 2020
Akamai Experience the Edge

DNS64 のオプション設定

各種課題に対応するため条件的に動作を変える各種オプションが存在

- **break-dnssec** (BIND) : no であれば DO=1 のクエリに対して RRSIG のあるレコードは DNS64 変換しない (デフォルト)
- **exclude** (BIND / CacheServe) : 指定された IPv6 アドレスの範囲であれば AAAA が存在しても DNS64 のものを返す
- **mapped** (BIND / CacheServe) : 指定された IPv4 アドレスの範囲は DNS64 変換しない
- **dns64-ignore-aaaa** (Unbound) : 指定したドメイン名は ~~DNS64 変換しない~~ AAAA が存在しても DNS64 のものを返す
- **dns64-synthall** (Unbound) : AAAA が存在しても常に DNS64 したものを返す

→ CacheServe ならいずれもポリシー機能で可能！
こういう課題はまだ他にもあるはず！

© Akamai Technologies, 2020

修正部分 : 発表後にご指摘いただき、訂正しました。

Akamai Experience the Edge

Case 1 : IPv4 の接続もあるユーザ

IPoE で IPv6 + NAT64/DNS64 を用いているユーザが、PPPoE で IPv4 も接続

1. AAAA では DNS64 の IPv6 アドレス、A では IPv4 アドレスを受け取るが、NAT64 経由と直接接続してくる場合でソース IP アドレスが変わり、同じユーザと判別されない問題

→ A クエリに対し NOERROR でかつ AAAA が存在しない場合、 NODATA を返すポリシー

2. トラフィックをできるだけ NAT64 (IPoE) に回したい

→ A クエリに対し NOERROR の場合、NODATA 応答するポリシー

(~~IPv4 のみのアプリケーションや~~ IPv4 アドレス直接指定するアプリケーションは PPPoE にまわる)

© Akamai Technologies, 2020

修正部分：発表時に事前資料に訂正を加えました。

Akamai Experience the Edge

広がるバリエーション

権威サーバの応答	QTYPE	通常	DNS64	exclude	1-1	1-2	AAAAフィルタ
IPv6 IPv4	AAAA	IPv6	IPv6	合成v6	IPv6	IPv6	NODATA
	A	IPv4	IPv4	IPv4	IPv4	NODATA	IPv4
IPv4 のみ	AAAA	NODATA	合成v6	合成v6	合成v6	合成v6	NODATA
	A	IPv4	IPv4	IPv4	NODATA	NODATA	IPv4
IPv6 のみ	AAAA	IPv6	IPv6	NODATA	IPv6	IPv6	IPv6
	A	NODATA	NODATA	NODATA	NODATA	NODATA	NODATA

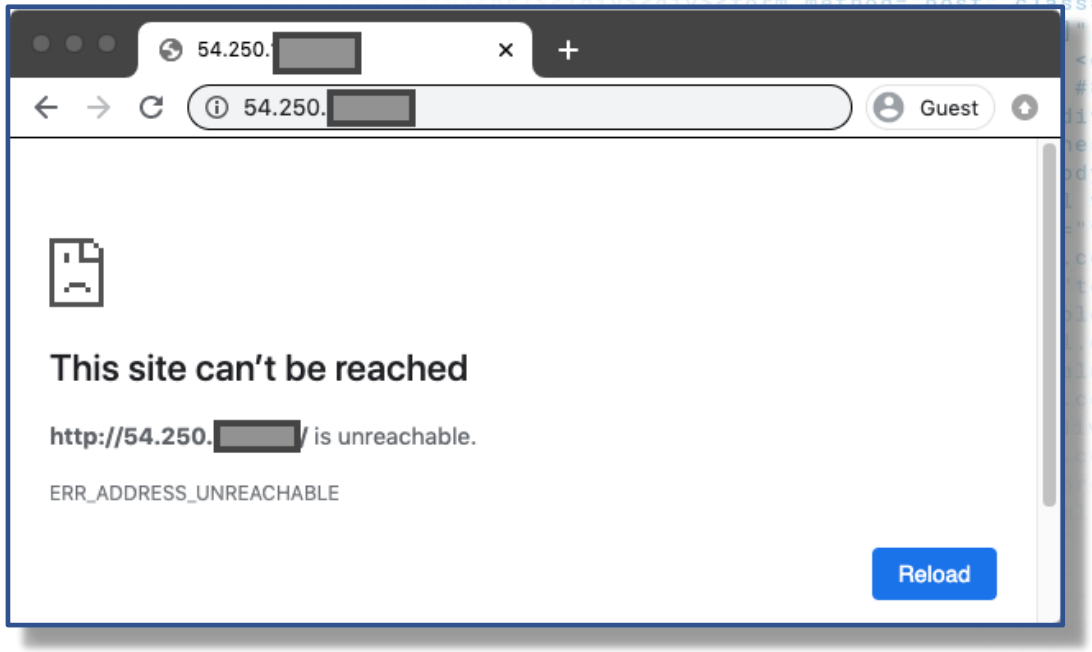
これらを送信元アドレス、宛先アドレス、ドメイン等によって使い分けられる

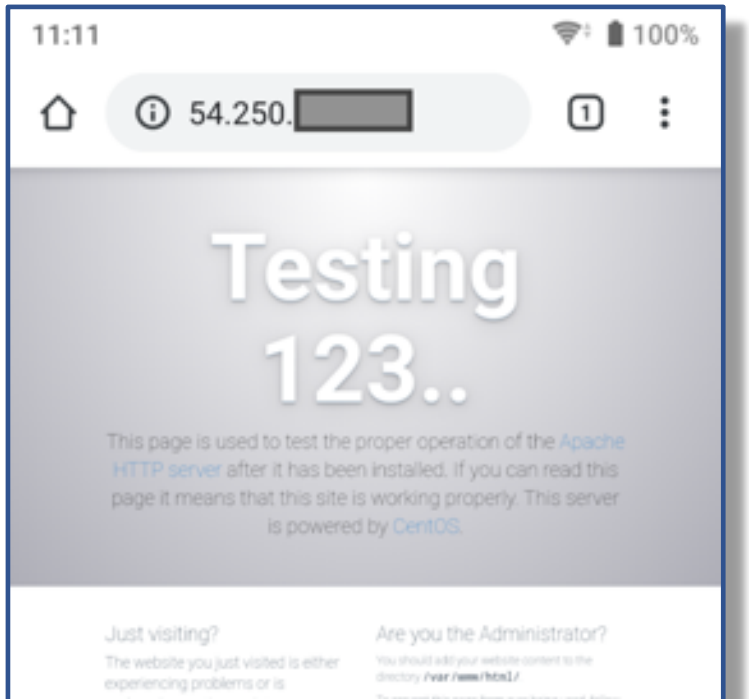
© Akamai Technologies, 2020
Akamai Experience the Edge

モバイル端末の場合

IPv6 オンリー NAT64/DNS64 環境の
「IPv4 のみのアプリや DNS を介さず直接 IPv4 アドレスでアクセスするアプリが通信できない」問題

Android や iOS では IPv4 アドレスでアクセスできる！
464XLAT のおかげ？





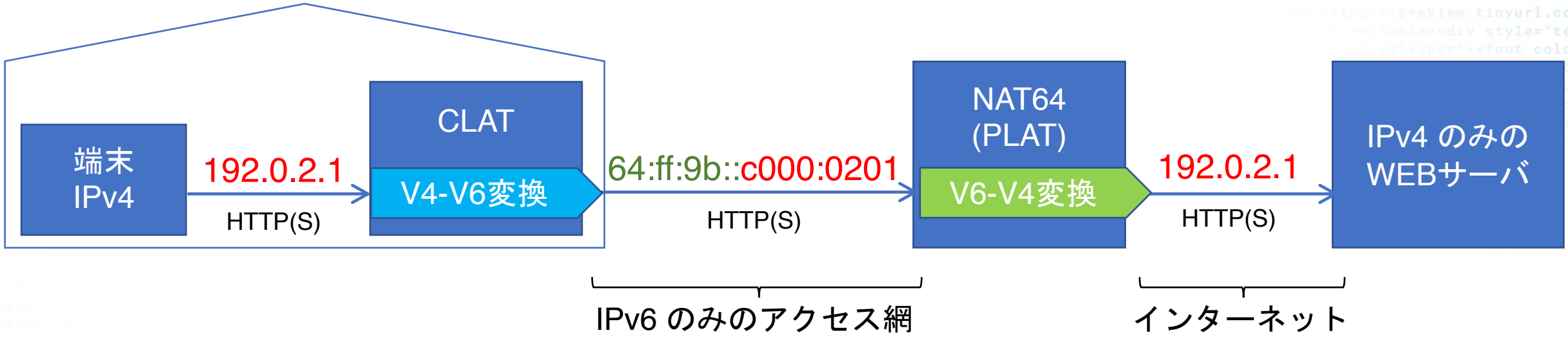
↑ Windows

← Android

© Akamai Technologies, 2020

Akamai Experience the Edge

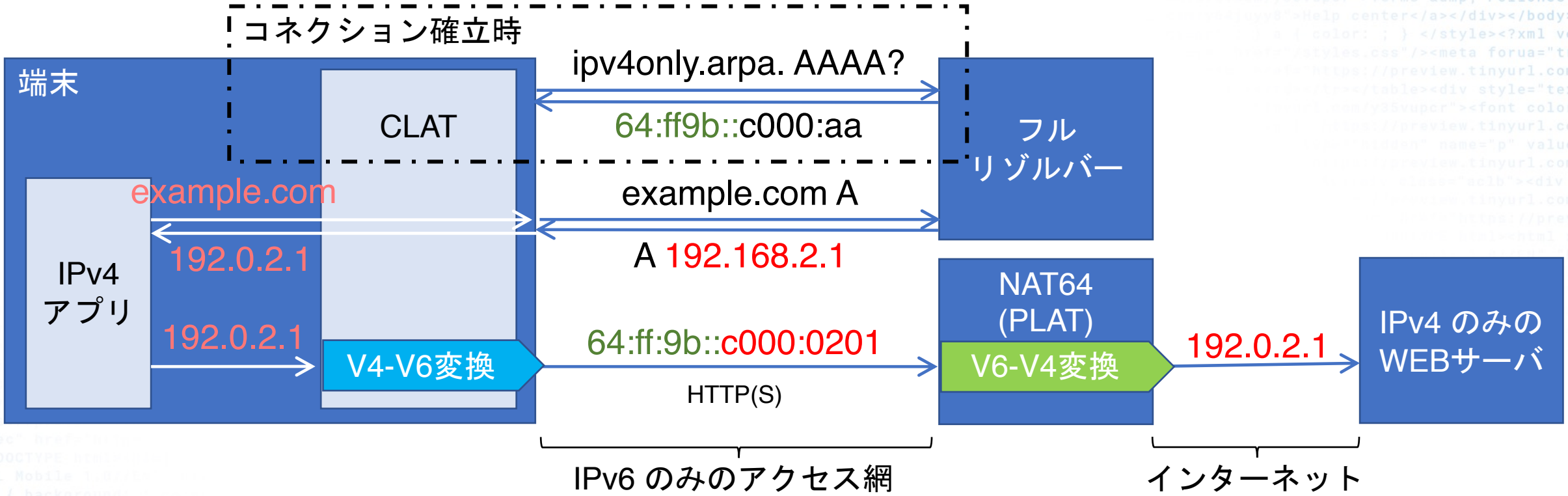
464XLAT



- IPv4 での通信は顧客側のゲートウェイ (CLAT)で IPv4 から IPv6 への変換を行い、サービスプロバイダ側の NAT64 (PLAT) で IPv4 に戻す

© Akamai Technologies, 2020
Akamai Experience the Edge

端末の 464XLAT (CLAT)



- CLAT は ipv4only.arpa. AAAA をクエリすることによりNAT64 (PLAT) の持つPrefix を見つける (Pref64::/n Discovery - RFC7050)
- 応答の形は DNS64と同じなので、DNS64 があれば自動的に 464XLAT が使われる (ipv4only.arpa はその名の通り IPv4 アドレスだけを持つ)

© Akamai Technologies, 2020
Akamai Experience the Edge

端末の 464XLAT (CLAT)

- Android 4.3 ～
- iOS 12 (2018)～
- Windows 10 デスクトップ版でも Creators Update (2017) 以降モバイルアクセス環境では対応*

接続サービスにおける IPv6 オンリー化と端末側の対応が並行して進んでいる

- https://techcommunity.microsoft.com/t5/networking-blog/core-network-stack-features-in-the-creators-update-for-windows/ba-p/339676

© Akamai Technologies, 2020

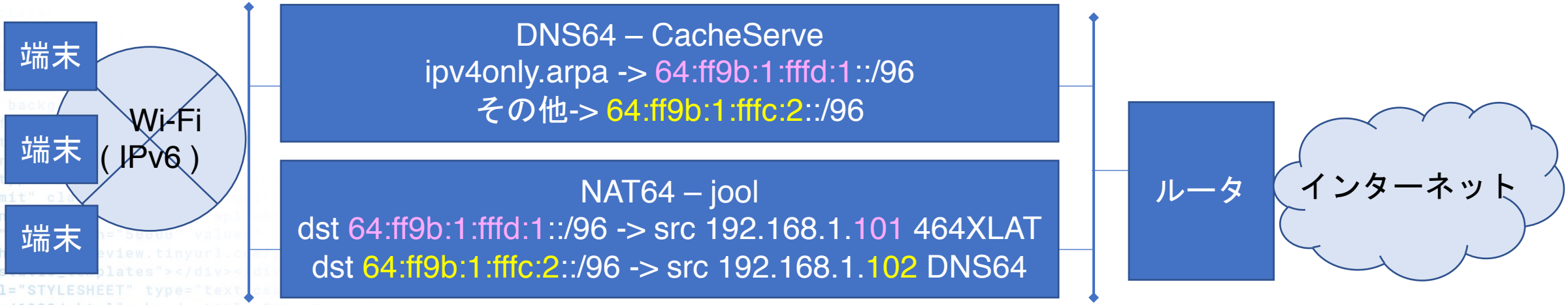
Case 2: NAT64/DNS64 と 464XLAT の振り分け

通常 DNS64 も 464XLAT も結果として同じアドレスにマップされる

- DNS64 なのか端末側でマップしているのか知りたい
- DNS64 と 464XLAT で NAT を分けたい

→ ipv4only.arpa とその他で別のプレフィクスにマップするポリシー

やってみた（プレフィクスにより異なる IPv4 プール）



© Akamai Technologies, 2020
Akamai Experience the Edge

まとめ

- 新機能追加を待つことなく、フルリゾルバとしての動作を柔軟に変更し課題の解決に役に立つ
- サービスの IPv6 オンリー化が着々と進む一方、464XLAT対応や DoH 等、端末側の動作も変化中
- 変化し続ける DNS の使われ方の中で、課題を解決したり解析するー手段として新機能を待つことなくロジックを変更できるポリシーが役に立つ場面がいろいろ出てきそう

© Akamai Technologies, 2020
Akamai Experience the Edge


Akamai
Experience the Edge