.jprs DDoS 攻撃対策実証実験
（ローカルノードの設置・運用）
実証実験報告書

第 1.0 版

2021 年 11 月

株式会社日本レジストリサービス

北海道総合通信網株式会社

株式会社オプテージ

株式会社 QTnet

目次

概要

実証実験の背景・目的

2016 年から 2017 年にかけて JPRS と電力系通信事業者 9 社が共同で実施した「大規模災害時のインターネット継続利用実証研究」(以下、前回研究)では、わが国において大規模な災害が発生し、通信回線の切断をはじめとする物理的な障害により国内のインターネットが物理的に分断されたことを想定し、TLD の権威 DNS サーバーのローカルノードを国内の複数拠点に分散配置することで名前解決サービスを継続させ、当該 TLD を使用したインターネットサービスの安定性・継続性を高めることについて検証した。

その成果として、大規模災害により TLD の権威 DNS サーバーのグローバルノードへの到達性が失われている状況においても、当該地域内に設置したローカルノードにより当該 TLD の名前解決サービスを継続でき、インターネットサービスの安定性・継続性向上に有効であることを確認できた。

一方、日々の DNS の運用において名前解決の安定性を脅かす重大な脅威として、サイバー攻撃が挙げられる。中でも、情報を提供する権威 DNS サーバーや情報を検索するフルリゾルバーを標的とした DDoS 攻撃が継続して観測されており、被害事例も報告されている。サイバー攻撃は注目度が高いイベントを狙って実行される傾向があり、2020 年に予定され、2021 年に延期された東京オリンピック・パラリンピック競技大会(以下、東京大会)においても、DDoS 攻撃をはじめとする大規模なサイバー攻撃の発生が懸念されている。

権威 DNS サーバーやフルリゾルバーが DDoS 攻撃を受けることで名前解決を継続できなくなった場合、前述した災害発生時におけるインターネットの物理的な分断と同様の状況が発生することになる。そのため、名前解決の安定性・継続性を向上させるためには災害等によるインターネットの物理的な分断に加え、サイバー攻撃による「論理的な分断」を回避するための対策も考慮・実施する必要がある。

以上の状況を踏まえ、国内の ISP3 社と JPRS による「.jprs DDoS 攻撃対策実証実験（ローカルノードの設置・運用）（以下、本研究）」を実施した。本テーマにおける実証実験（以下、本実証実験）では、TLD の権威 DNS サーバーを標的とした DDoS 攻撃によって当該サーバーへの到達性が失われた状況を想定し、物理的な分断において有効であったローカルノードの配置が論理的な分断においても名前解決サービスの継続に有効であるかの検証を実施した。本実証実験に用いるローカルノードは株式会社 QTnet(以下、QTnet)、株式会社オプテージ(以下、OPTAGE)、北海道総合通信網株式会社(以下、HOTnet)の 3 社に設置した。

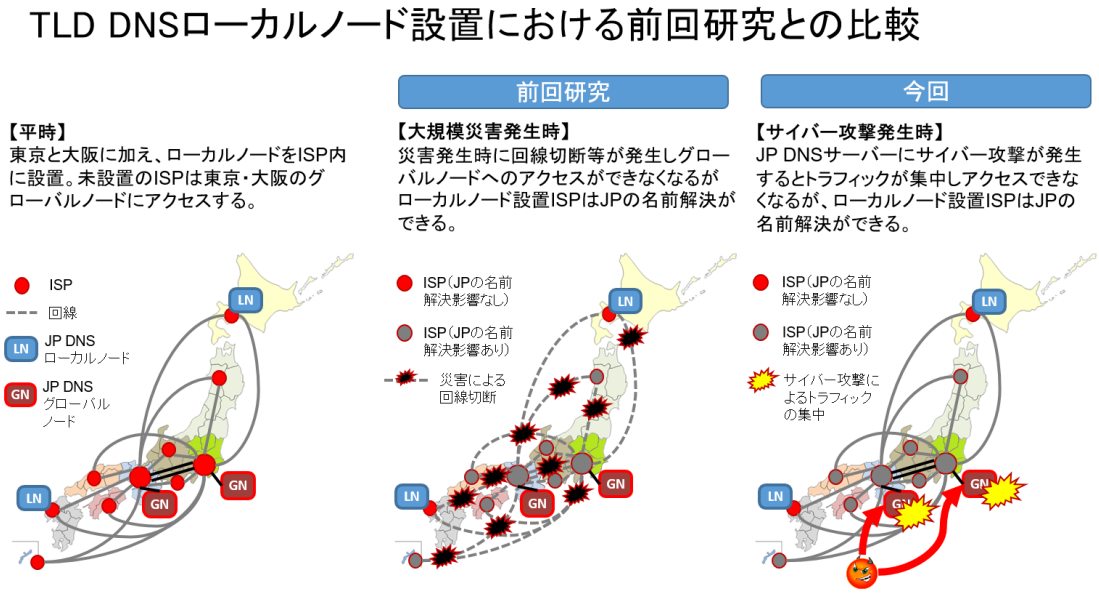


図: TLD DNS ローカルノード設置における前回研究との比較

実証実験の対象

想定したサイバー攻撃

本実証実験では、DDoS 攻撃の対象として TLD の権威 DNS サーバーを想定し、攻撃方法としてランダムサブドメイン攻撃を選択した。

ランダムサブドメイン攻撃は攻撃対象の権威 DNS サーバーにクエリを集中させることで、攻撃対象の権威 DNS サーバーやフルリゾルバーをサービス不能の状態に陥らせることを狙った攻撃手法である。2014 年頃から攻撃の発生が世界的に報告されており、複数の被害事例も確認されている。

ランダムサブドメイン攻撃では、攻撃対象の権威 DNS サーバーがホストするドメイン名（例：example.jp や example.co.jp)にランダムなサブドメインを付加した攻撃トラフィックを送信する。具体的には、ランダムな文字列を該当ドメイン名の 3LD や 4LD に付加したものになる（例：{ランダムな文字列}.example.jp）。攻撃者はあらかじめ用意した世界中にあるセキュリティの設定に問題がある端末を乗っ取り(ボット化)、それらの端末から攻撃トラフィックを送信する。乗っ取った大量の端末から攻撃トラフィックを送信することで、権威 DNS サーバーがサービス提供不能の状態になるように仕向ける。

ランダムサブドメイン攻撃では、乗っ取った端末(ボット)は ISP のフルリゾルバーへ攻撃トラフィックを送信する。通常、同一の QNAME（例：www.example.jp 等）についてはフルリゾルバーのキャッシュ機能により、キャッシュが有効であ

る間は権威 DNS サーバーへの問い合わせは発生しない。しかし、ランダムサブドメイン攻撃は、ランダムな文字列を含む QNAME のクエリを攻撃トラフィックとして送信しているためフルリゾルバーのキャッシュ機能が働かず、権威 DNS サーバーへの問い合わせが毎回発生する。

このように、ランダムサブドメイン攻撃ではフルリゾルバーのキャッシュ機能を迂回させ、かつボットではなく正当なフルリゾルバーからターゲットとなる権威 DNS サーバーへ攻撃トラフィックが送信されるため、権威 DNS サーバー側では対処が難しい攻撃手法の一つである。

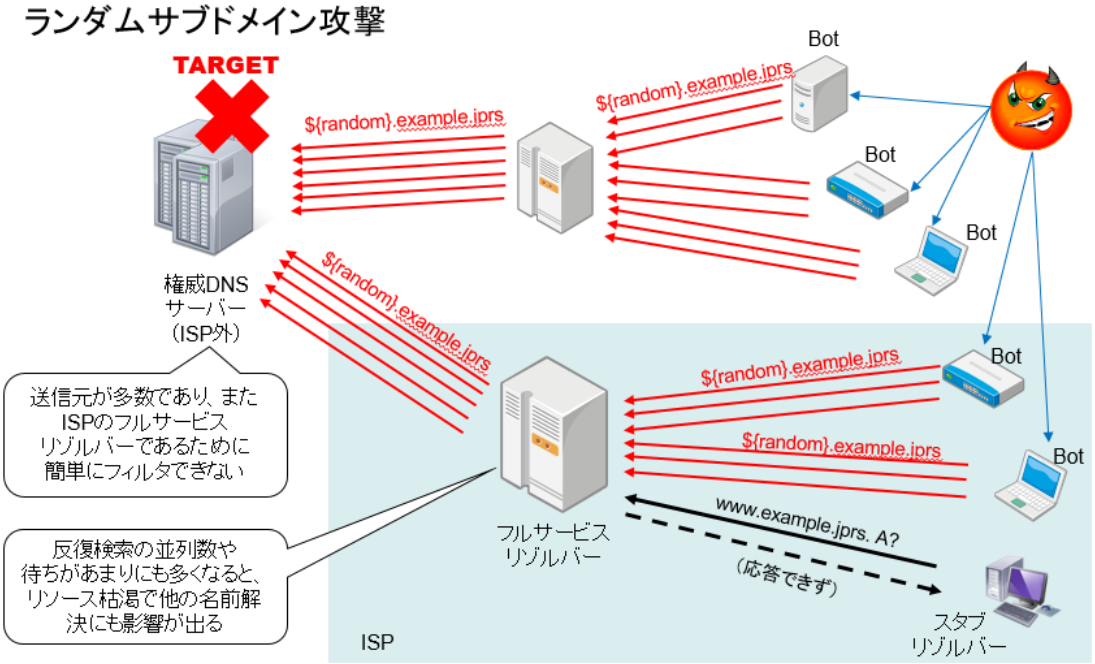


図:ランダムサブドメイン攻撃

本実証実験では、TLD の権威 DNS サーバーそのものがランダムサブドメイン攻撃の攻撃対象となることを想定し、攻撃トラフィックとして QNAME の 2LD にランダムな文字列を設定したうえで、ボットから大量に送信する形を想定して設定した。

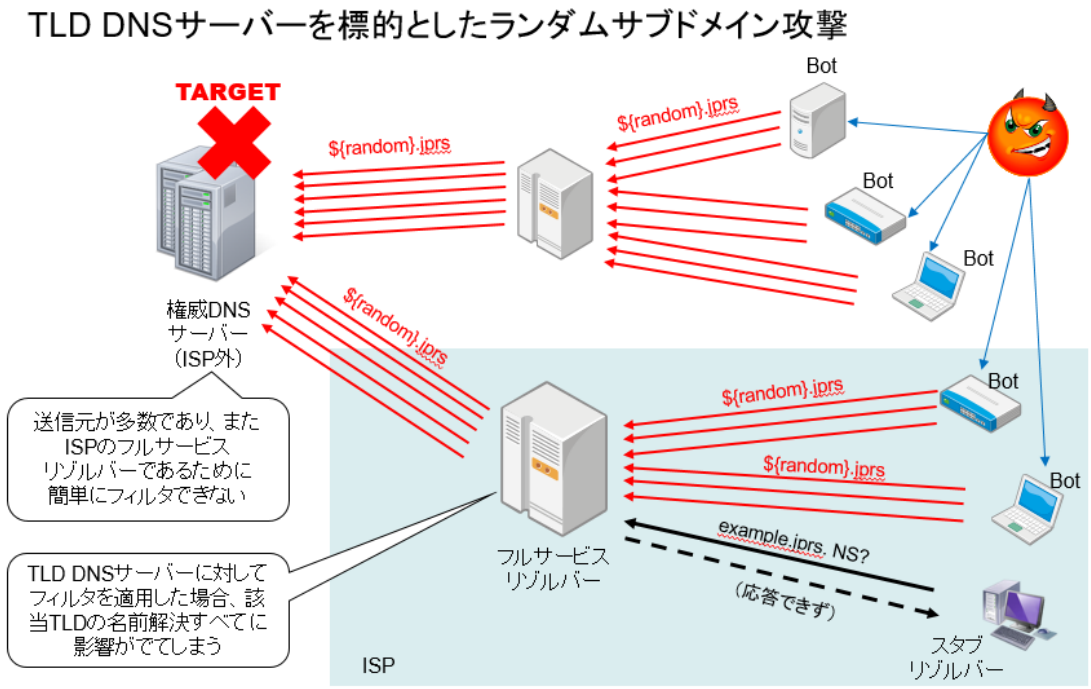


図: TLD DNS サーバーを標的としたランダムサブドメイン攻撃

ローカルノードの設置

本実証実験では、前回研究と同様に実証実験に参加した ISP のネットワークの内部に TLD の権威 DNS サーバーのローカルノードを設置し、JPRS が 当該権威 DNS サーバーのグローバルノードを運用する構成とした。

ローカルノードは、設置されたネットワーク内に対してのみ名前解決サービスを提供する権威 DNS サーバーを指す。ローカルノードを設置していないネットワークには、インターネット上に設置されたグローバルノードが名前解決サービスを提供する。ローカルノードを設置することで、当該 TLD の権威 DNS サーバーが提供する委任情報がそのネットワーク内で得られるようになり、かつ、ローカルノードには外部ネットワークからの名前解決トラフィックの流入がないため、TLD の権威 DNS サーバーを標的とした DDoS 攻撃の影響の低減が可能になる。これにより、ローカルノードを設置したネットワークの利用者に対する、当該 TLD の安定した名前解決サービスの提供が期待できる。

本実証実験のシステム構成を以下に示す。

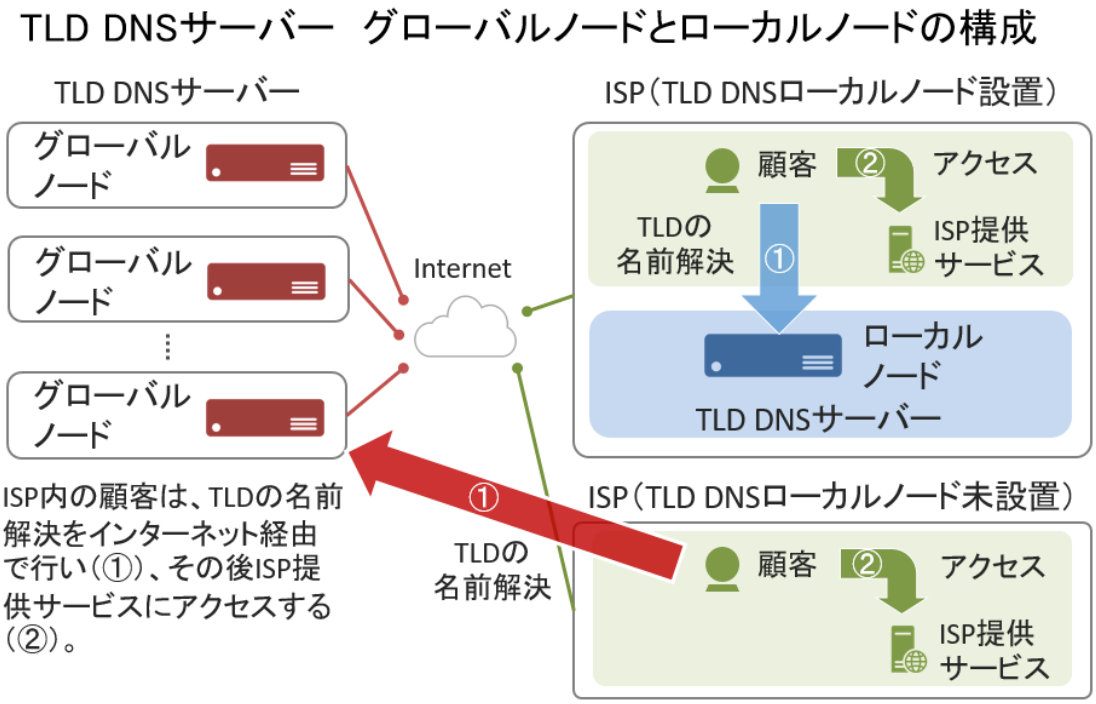


図: TLD DNS サーバー グローバルノードとローカルノードの構成

IP Anycast を用いたローカルノードの設置方式には、TLD の権威 DNS サーバーの AS 番号と IP アドレスの双方を ISP 内部に持ち込み、BGP で接続する BGP 接続方式と、TLD の権威 DNS サーバーの IP アドレスのみを ISP 内部に持ち込み、ISP 側で Static route を設定する Static 接続方式の 2 種類がある。

今回は JPRS における IP Anycast の運用実績から、BGP 接続方式を選択することとした。なお、ISP 内におけるネットワーク運用上の理由により OPTAGE のみ、BGP 接続においてローカルノード側でプライベート AS 番号を使用し、サービス用の IP アドレスと共に持ち込む方式を採用した。

TLD の権威 DNS サーバーの構成を以下に示す。実証実験にあたり、5 から 7 までのローカルノードを、それぞれの ISP に設置している。

No.	ホスト名	AS 番号	経路広告	ノード種別
1	tld1.nic.jprs	AS18149	グローバルノード	商用環境(JPRS)
2	tld2.nic.jprs	AS2914	グローバルノード	商用環境(JPRS)
3	tld3.nic.jprs	AS12041	グローバルノード	商用環境(JPRS)
4	tld4.nic.jprs	AS131905	グローバルノード	商用環境・実証実験環境(JPRS)
5	tld4.nic.jprs	AS131905	ローカルノード	実証実験環境(HOTnet)
6	tld4.nic.jprs	AS64564	ローカルノード	実証実験環境(OPTAGE)
7	tld4.nic.jprs	AS131905	ローカルノード	実証実験環境(QTnet)
8	tld5.nic.jprs	AS12041	グローバルノード	商用環境(JPRS)

ローカルノード以外の実験用設備

ローカルノード以外の用途に使用した実験用設備として、以下を準備した。

ISP 側

No.	設備	用途
1.	実証実験用 疑似攻撃送信端末	ランダムサブドメイン攻撃のトラフィックを生成する端末
2.	実証実験用 スタブリゾルバー	ISP 内の顧客に相当する通常の端末
3.	実証実験用 フルリゾルバー	No.1,No.2 が利用するフルリゾルバー
4.	実証実験機材 収容ネットワーク機器	No.1, No.2, No.3 を収容するネットワーク機器
5.	管理ネットワーク用 ルーター	実証実験用ローカルノードの運用管理ネットワーク接続機器
6.	BGP ルーター	ローカルノードへのサービストラフィックを処理するルーター

JPRS 側

No.	設備	用途
a.	監視サーバー	グローバルノード DNS サーバー、ローカルノード DNS サーバーの死活監視
b.	グローバルノード	TLD(.jprs) DNS サーバーのグローバルノード(tld1, tld2, tld3, tld5))

c.	ゾーン転送 サーバー	TLD(.jprs) DNS サーバーに.jprs ゾーンを転送するためのサーバー
d.	実証実験用 DNS 攻撃監視 サーバー	TLD DNS サーバー(tld4.nic.jprs)への攻撃トラフィックを検知・通報するためのサーバー
e.	実証実験用 グローバルノード	TLD DNS サーバーのグローバルノード(tld4)。ローカルノード DNS サーバーと同一系統のシステム
f.	実証実験用 L2 スイッチ	No.e を収容するネットワーク機器
g.	実証実験用 BGP ルーター	実証実験用グローバルノードへのサービストラフィックを流すためのルーター

No.d の実証実験用 DNS 攻撃監視サーバーは、攻撃を受けたことを検知し、TLD DNS サーバーオペレーターである JPRS のシステム運用者に通知を送信するためのシステムである。本来、設置したすべての TLD の権威 DNS サーバーのトラフィックを監視して攻撃を検知することが望ましいが、今回の実証実験では、実証実験用に位置付けている tld4.nic.jprs のみに導入した。

システム構成

システム構成の全体像は以下の通り。

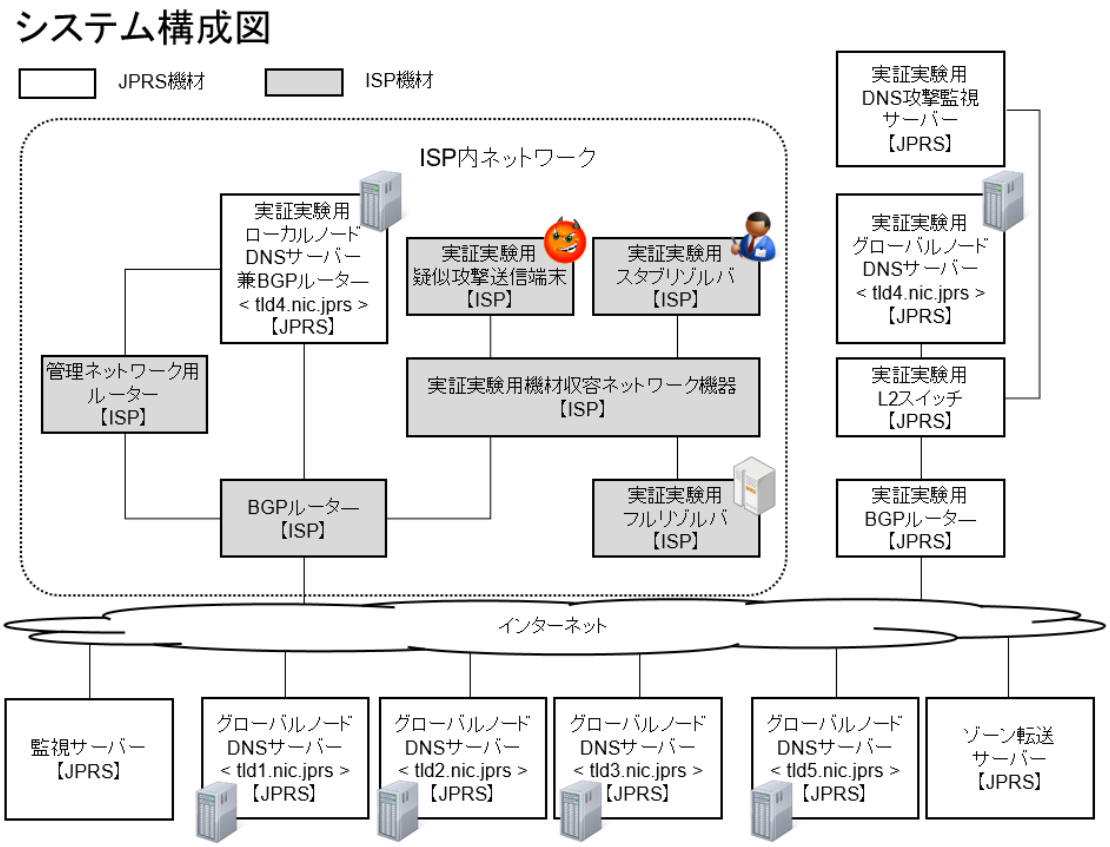


図: システム構成図

実験シナリオ

想定した攻撃シナリオにおいてローカルノードによる効果を確認する実験シナリオとして、以下の 2 種類を用意した。

- 実験シナリオ a ローカルノード設置の効果を確認するシナリオ
- 実験シナリオ b ローカルノード設置後、攻撃の発生から検知・対処までの運用を訓練するシナリオ

実験シナリオ a は、ローカルノード設置前と設置後のそれぞれの状態において TLD の権威 DNS サーバーへの DDoS 攻撃が発生した際に、どのような違いがあるかを検証するためのシナリオである。本シナリオでは、グローバルノードのみが設置された状態とローカルノードを実験参加 ISP 内に設置した状態のそれぞれにおいて、ランダムサブドメイン攻撃が発生した際の影響を確認・比較することで、その効果を検証することとした。なお、ローカルノード設置後のシナリオには、攻撃者がローカルノードを設置した ISP 以外のネットワークに存在する場合と、ローカルノードを設置した ISP 内のネットワークに存在する場合の 2 種類の

攻撃パターンが含まれている。これにより、ローカルノードを設置した際の限界点に関する検証も実施している。

実験シナリオ b は、ランダムサブドメイン攻撃を検知するシステムを TLD の権威 DNS サーバーに準備し、攻撃発生時の検知から対処までの運用の訓練を主眼にしたシナリオである。本シナリオでは、ローカルノードが ISP 内に設置された状態でランダムサブドメイン攻撃を発生させ、攻撃を検知するシステムが TLD の権威 DNS サーバーのオペレーターに攻撃情報を通知し、情報を受け取った TLD の権威 DNS サーバーのオペレーターが当該 ISP のオペレーターにその内容を共有することで、攻撃情報の共有と状況の確認を進める。また、攻撃情報を共有された ISP が自身のネットワークやフルリゾルバーの動作状況を確認し、TLD の DNS サーバーオペレーターと連携して攻撃への対処を進めることも含まれている。

実験シナリオ a と実験シナリオ b の概略を以下に示す。

シナリオ a の概要

シナリオ a：ローカルノード設置による効果確認のための実験シナリオ

- グローバルノードのみの状態での実験
  - 項番#1：通常時（ローカルノード未設置）
  - 項番#2：グローバルノードに対する攻撃開始
  - 項番#3：グローバルノードに対する攻撃終了
- グローバルノードとローカルノードを組み合わせた実験
  - 項番#4：実験参加 ISP 内にローカルノードを設置
  - 項番#5：グローバルノードに対する攻撃開始
  - 項番#6：ローカルノード設置 ISP 内（1 社）からも攻撃開始
  - 項番#7：ローカルノード設置 ISP 内（2 社）からも攻撃開始
  - 項番#8：ローカルノード設置 ISP 内（3 社）からも攻撃開始
  - 項番#9：ローカルノード設置 ISP 内（1 社）からの攻撃終了
  - 項番#10：ローカルノード設置 ISP 内（2 社）からの攻撃終了
  - 項番#11：ローカルノード設置 ISP 内（3 社）からの攻撃終了
  - 項番#12：すべての攻撃終了

シナリオ b の概要

- グローバルノードとローカルノードを設置
  - 項番#1: 通常時
- 攻撃発生の検知・連携・対処の訓練
  - 項番#2: 攻撃発生
  - 項番#3: 攻撃検知と連携
  - 項番#4: グローバルノードダウンの検知
  - 項番#5: グローバルノードダウンの連携
  - 項番#6: フルリゾルバー/ローカルノードの状況確認
  - 項番#7: グローバルノードの復旧

シナリオ a の構成図

項番#1：通常時（ローカルノード未設置）

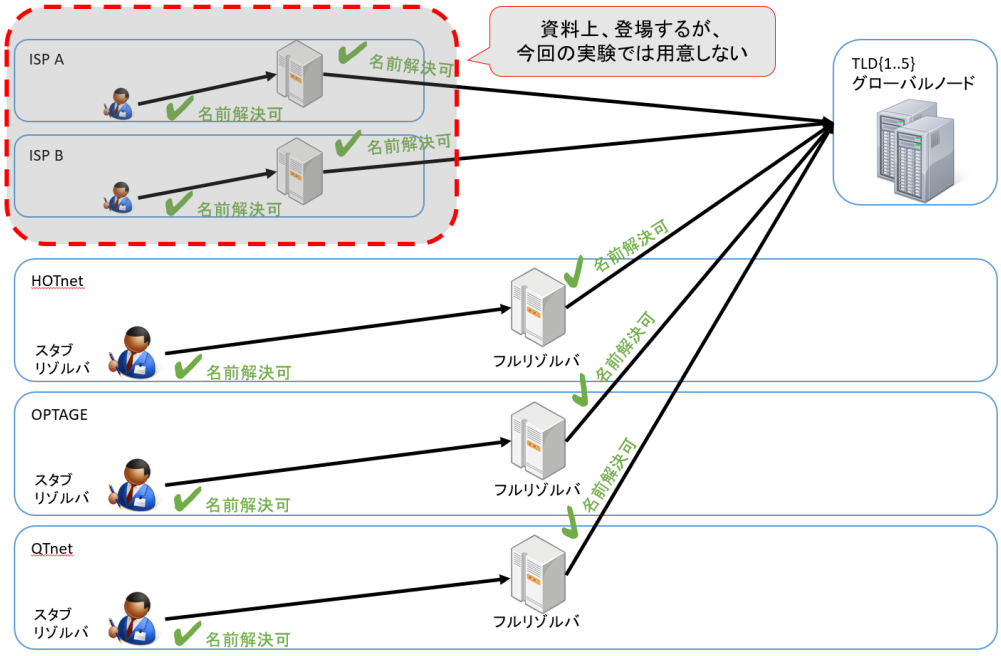


図: 項番#1:通常時

項番#2：グローバルノードに対し攻撃が発生

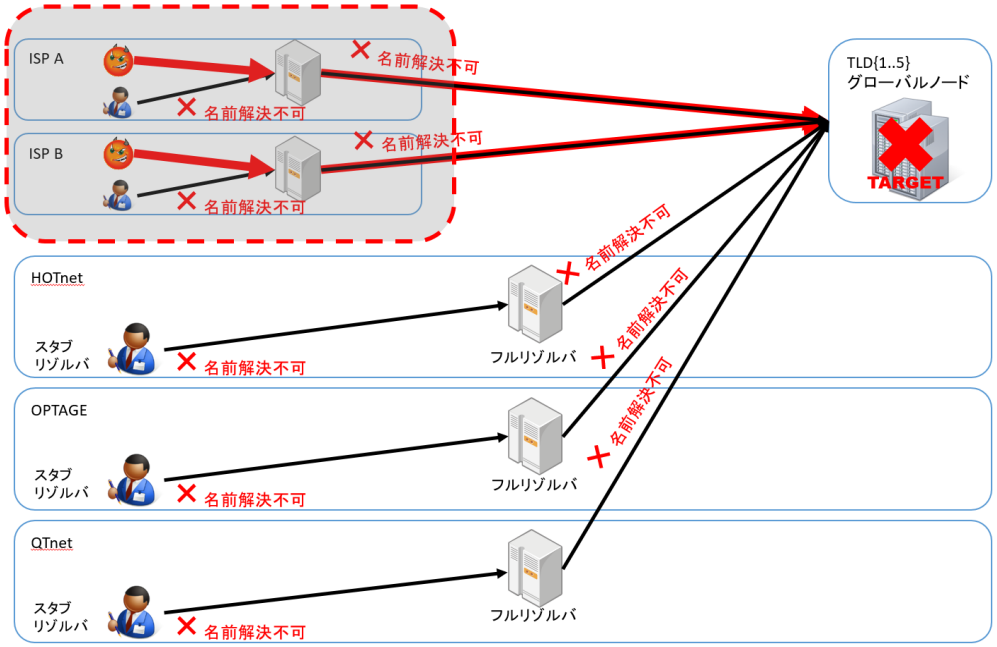


図: 項番#2: グローバルノードに対し攻撃が発生

項番#3：グローバルノードに対する攻撃が終了

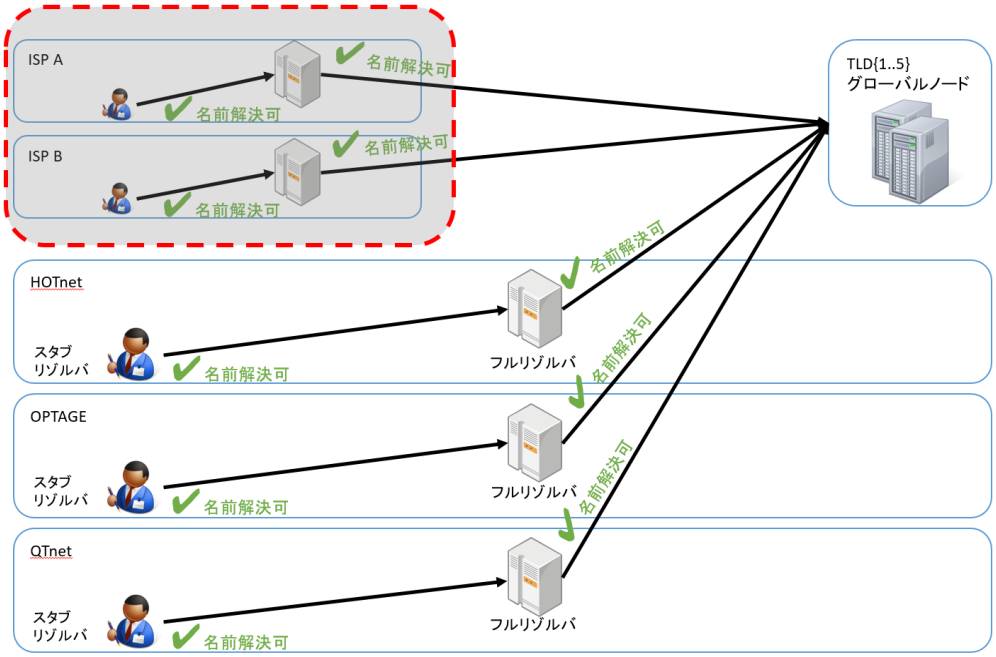


図: 項番#3: グローバルノードに対する攻撃が終了

項番#4：実験参加ISP内にローカルノードを設置

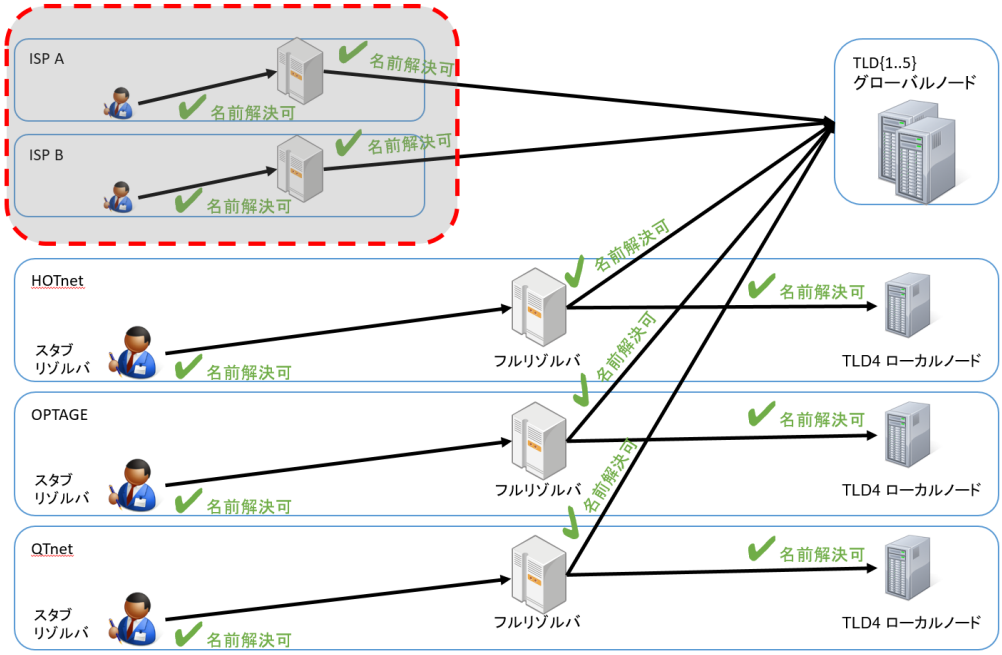


図: 項番#4: 実験参加 ISP 内にローカルノードを設置

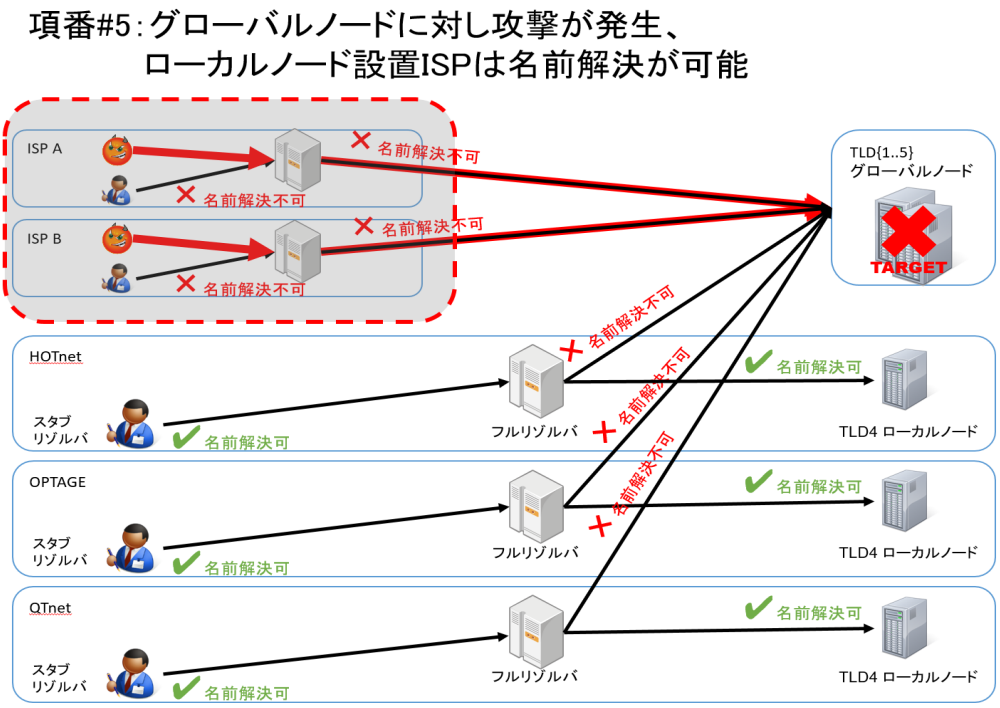


図: 項番#5: グローバルノードに対し攻撃が発生、ローカルノード設置 ISP は名前解決が可能

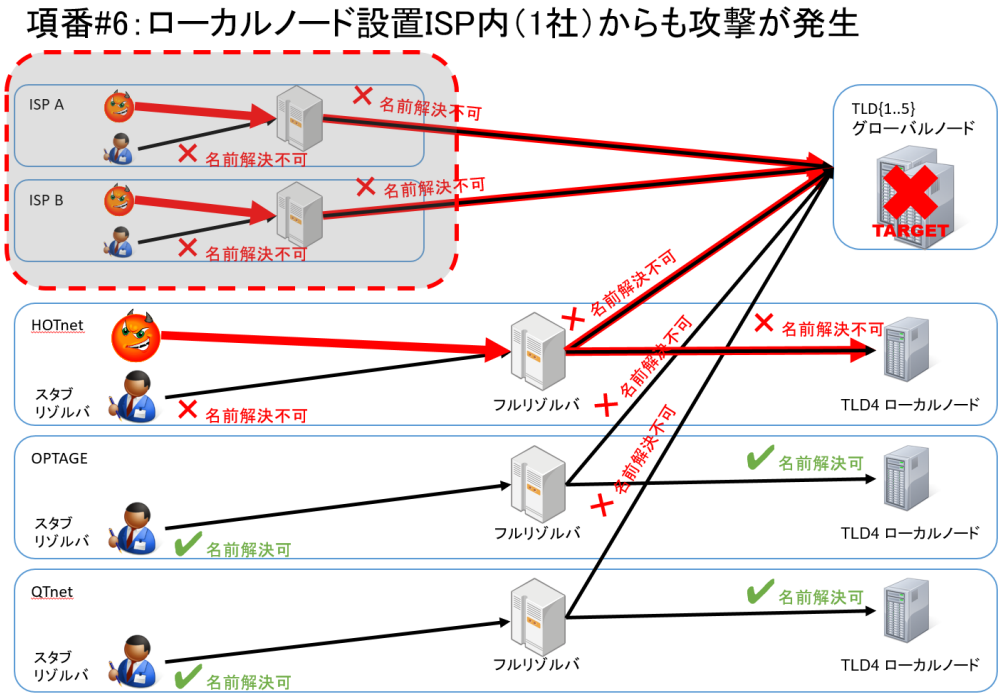


図: 項番#6: ローカルノード設置 ISP 内（1 社）からも攻撃が発生

項番#7：ローカルノード設置ISP内（2社）からも攻撃が発生

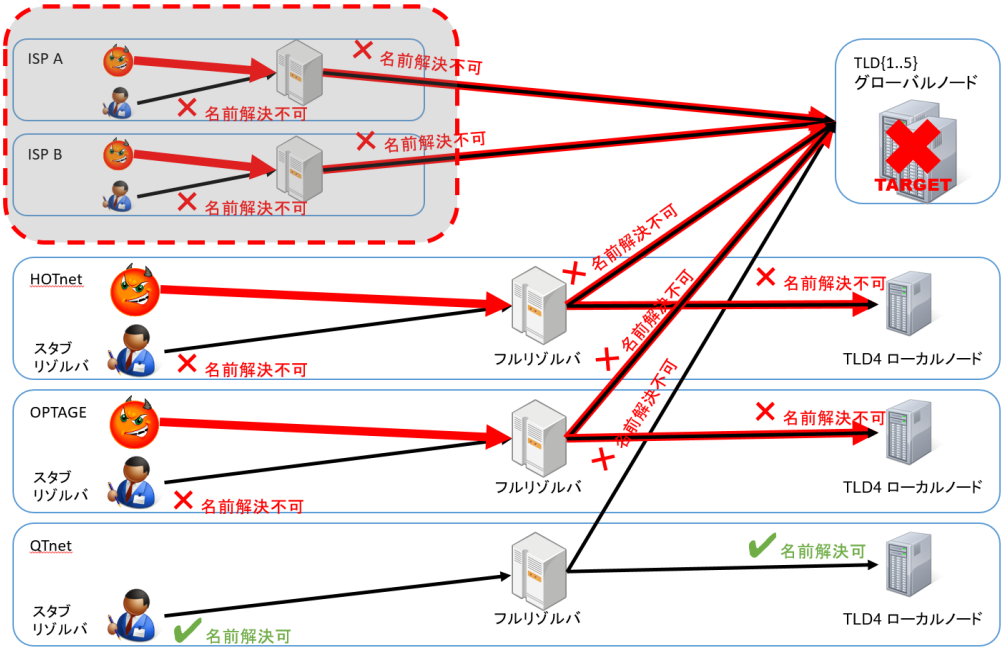


図: 項番#7: ローカルノード設置 ISP 内（2 社）からも攻撃が発生

項番#8：ローカルノード設置ISP内（3社）からも攻撃が発生

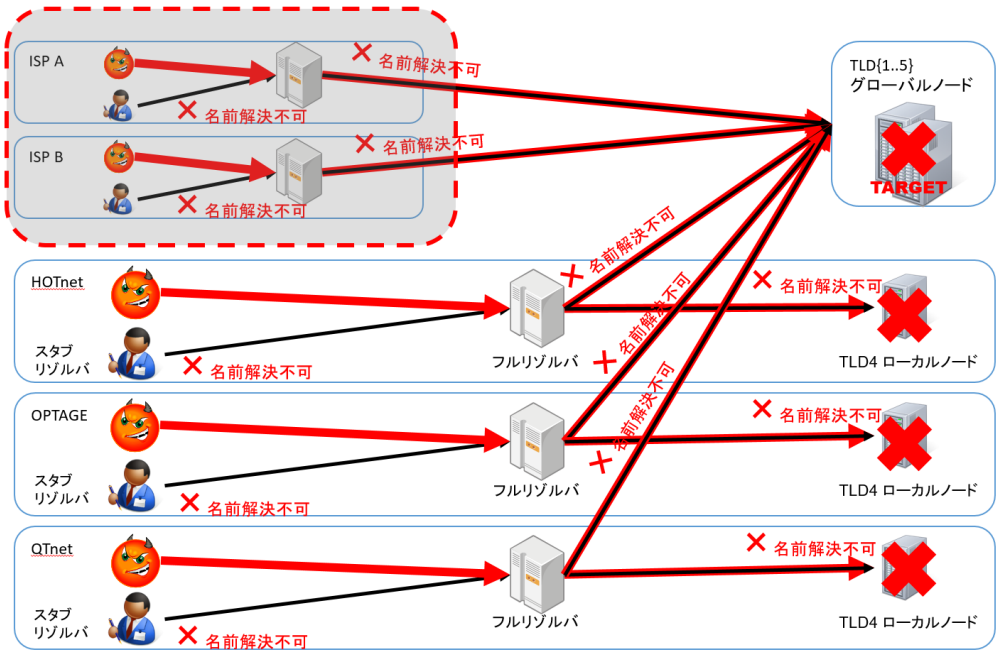


図: 項番#8: ローカルノード設置 ISP 内（3 社）からも攻撃が発生

項番#9：ローカルノード設置ISP内（1社）から攻撃が終了

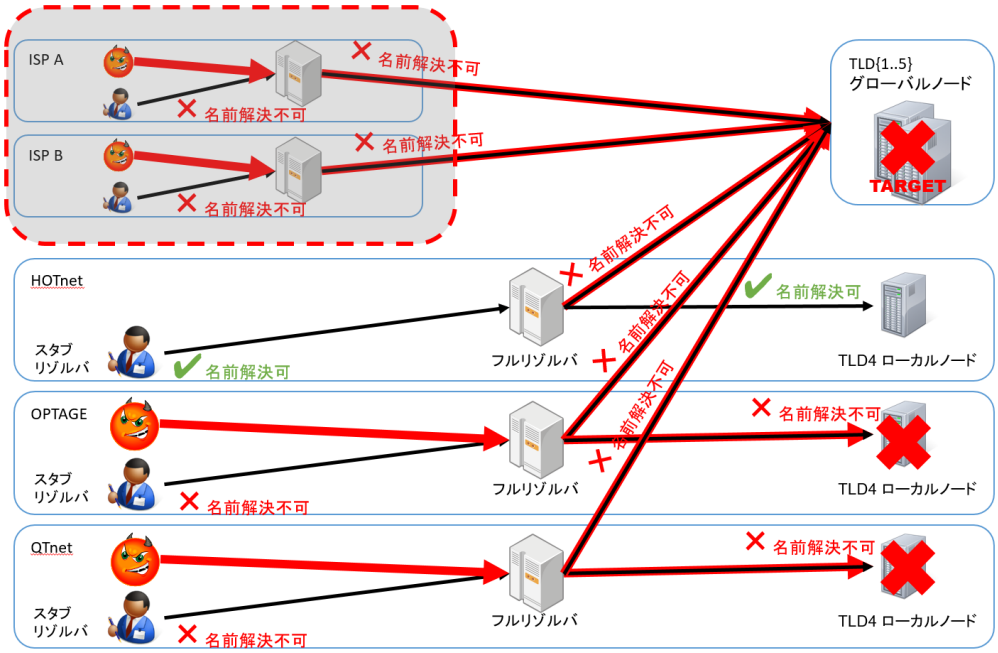


図: 項番#9: ローカルノード設置 ISP 内（1 社）から攻撃が終了

項番#10：ローカルノード設置ISP内（2社）から攻撃が終了

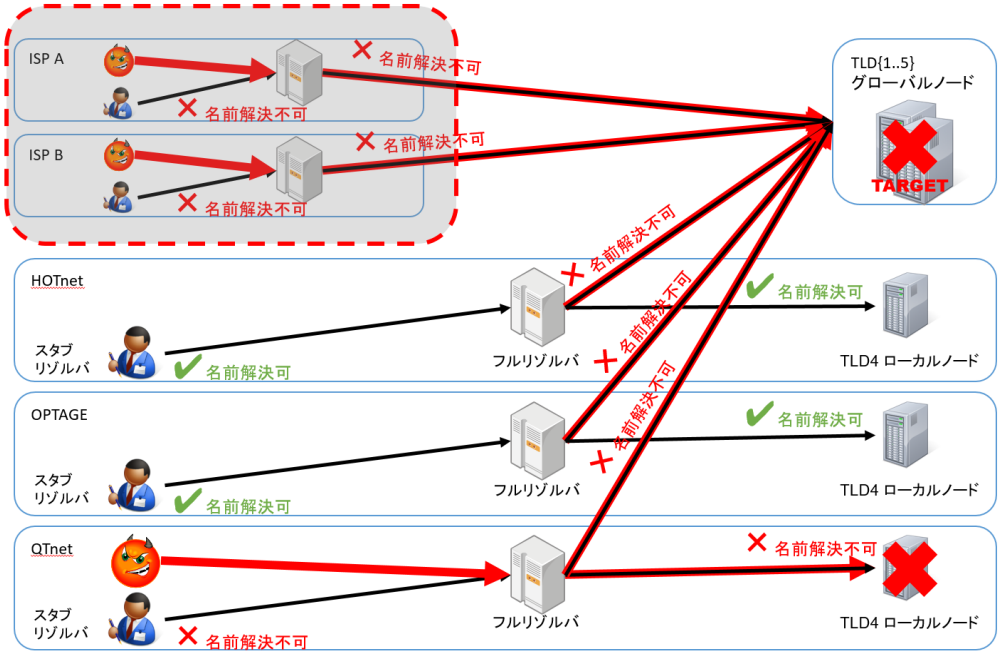


図: 項番#10: ローカルノード設置 ISP 内（2 社）から攻撃が終了

項番#11：ローカルノード設置ISP内（3社）から攻撃が終了

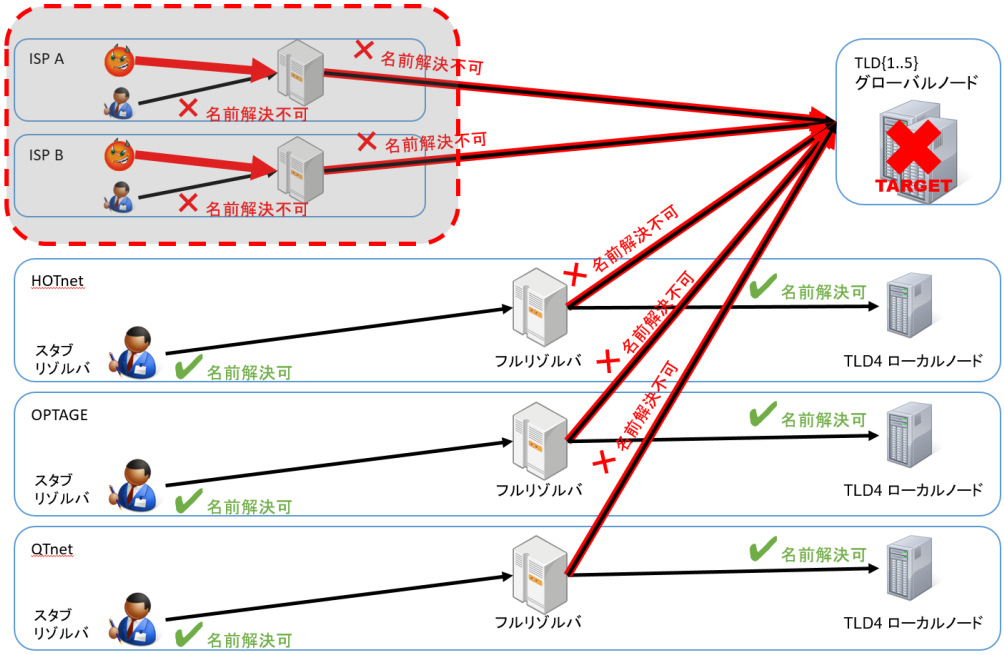


図: 項番#11: ローカルノード設置 ISP 内（3 社）から攻撃が終了

項番#12：すべての攻撃が終了

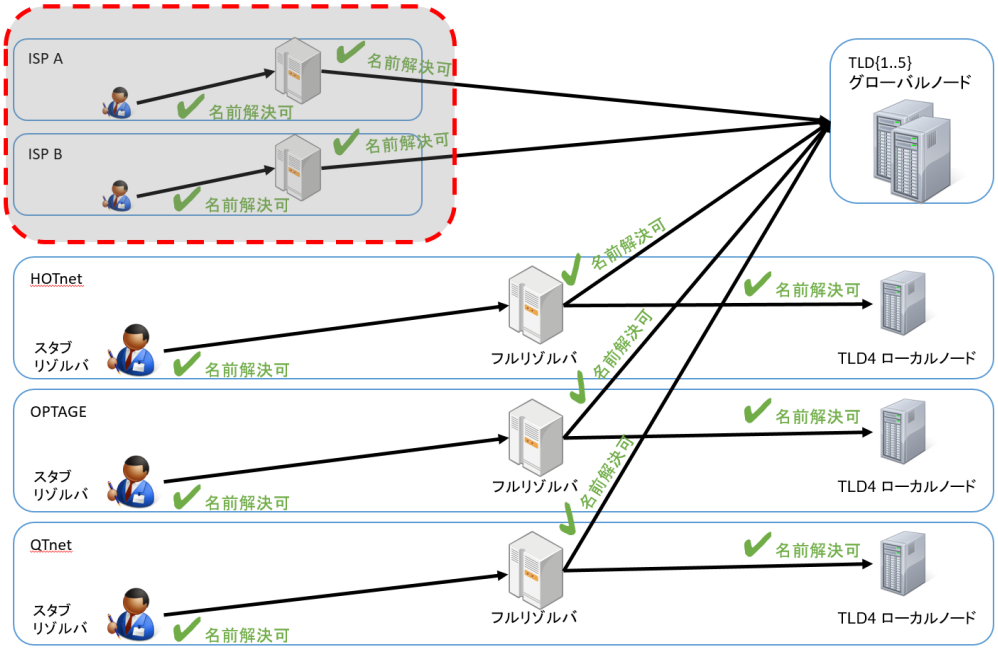


図: 項番#12: すべての攻撃が終了

シナリオ b の構成図

項番#1: 通常時

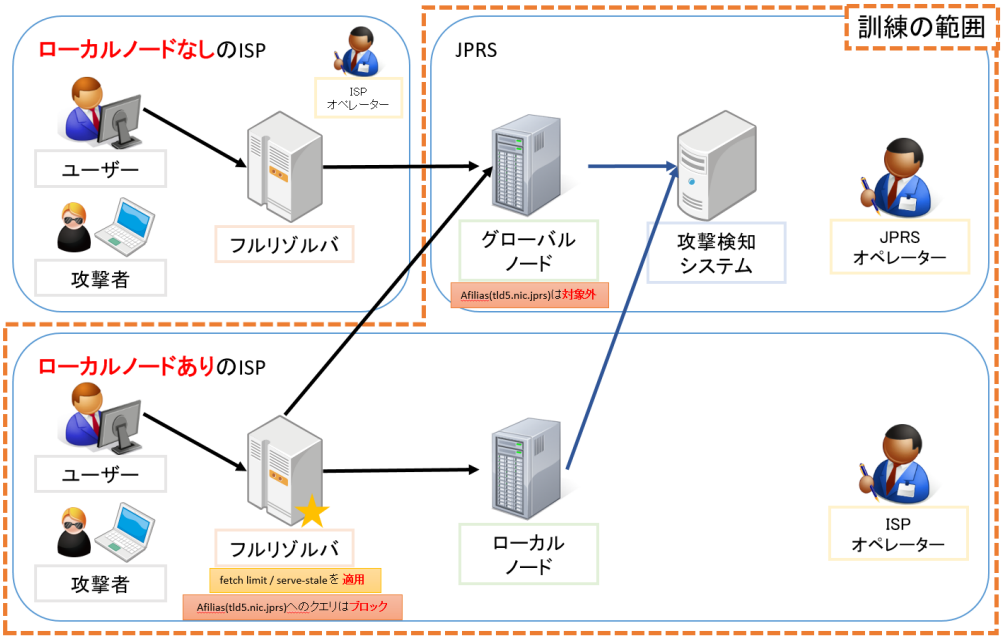


図: 項番#1: 通常時

項番#2: 攻撃発生

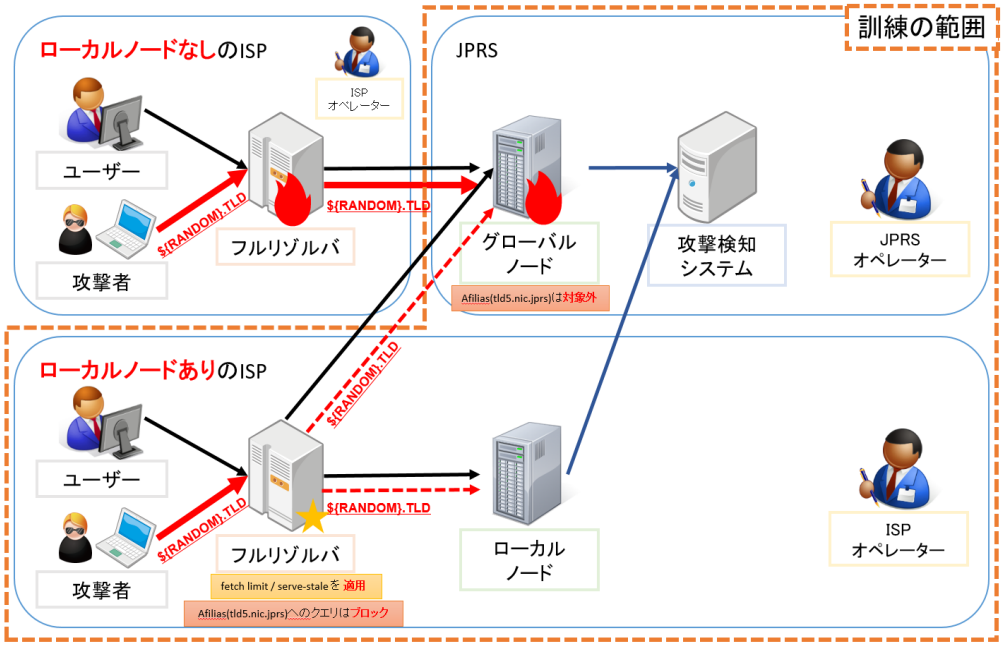


図: 項番#1: 攻撃発生

項番#3: 攻撃検知と連携

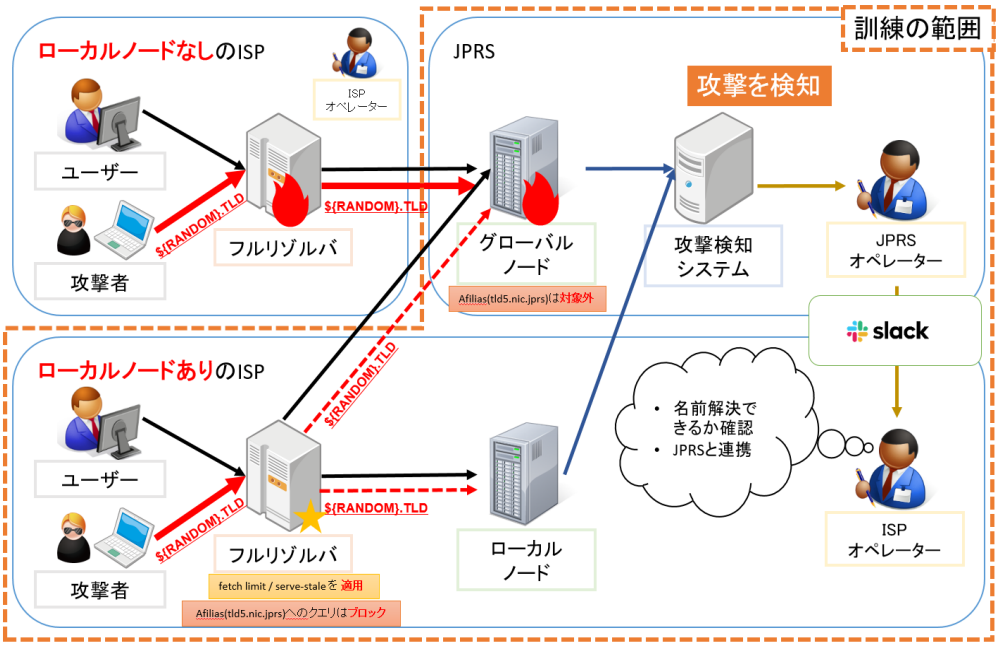


図: 項番#3: 攻撃検知と連携

項番#4: グローバルノードダウンの検知

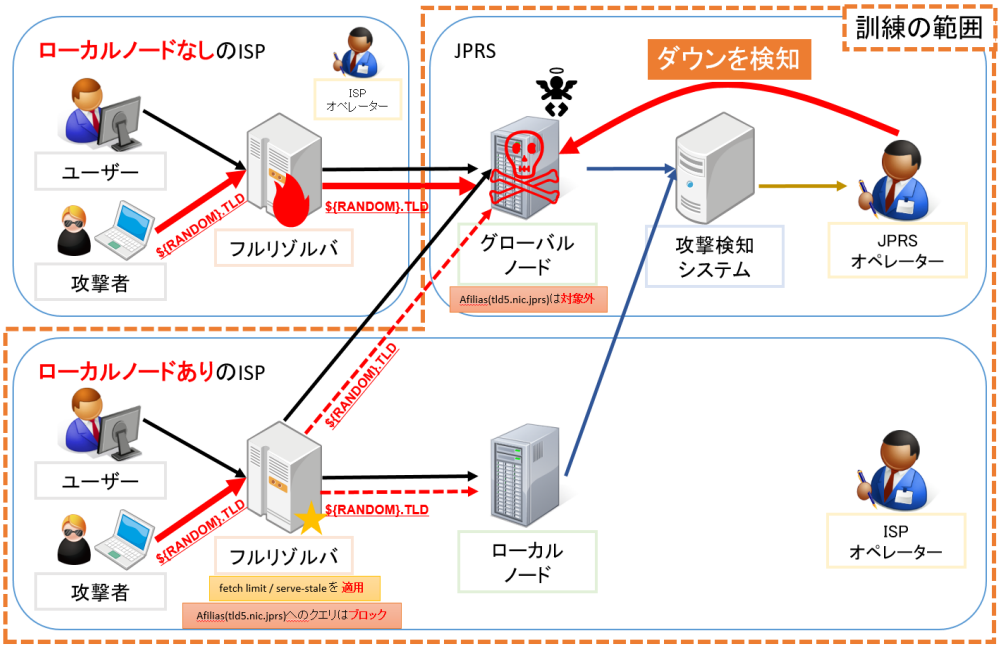


図: 項番#4: グローバルノードダウンの検知

項番#5: グローバルノードダウンの連携

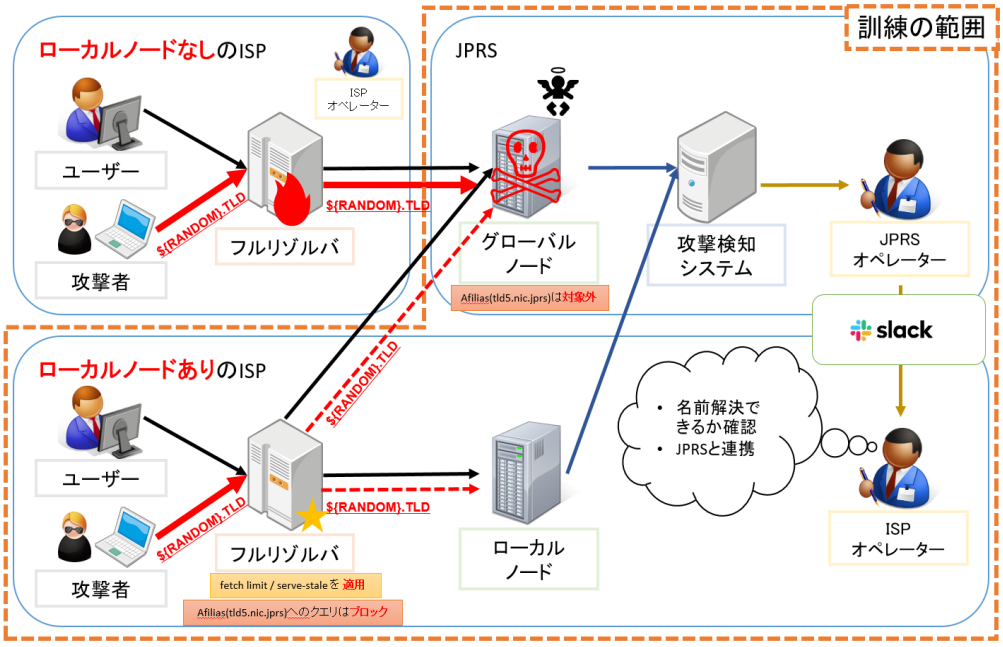


図: 項番#5: グローバルノードダウンの連携

項番#6: フルリゾルバ/ローカルノードの状況確認

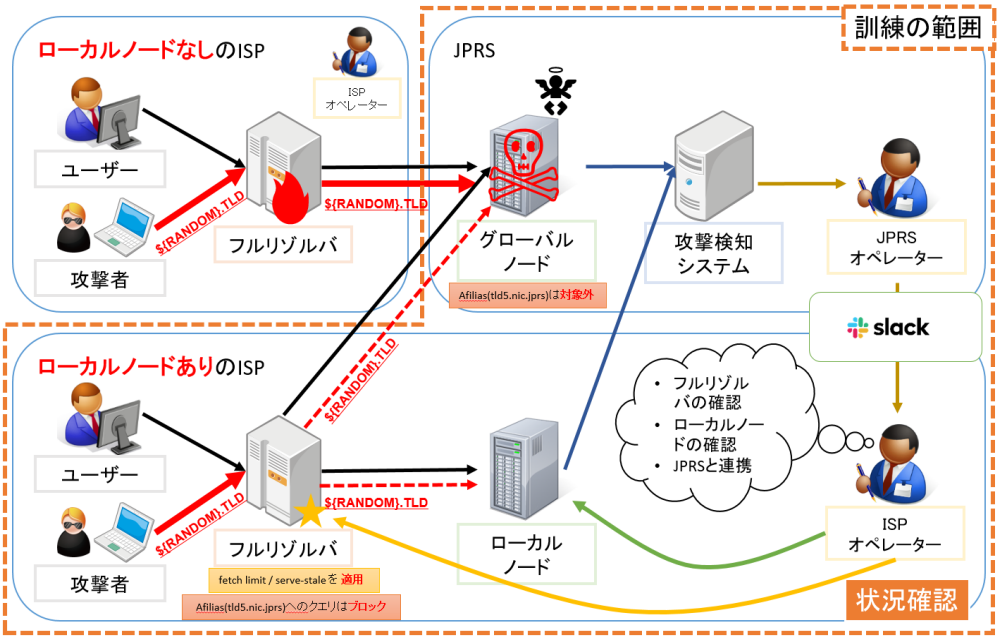


図: 項番#6: フルリゾルバ/ローカルノードの状況確認

項番#7: グローバルノードの復旧

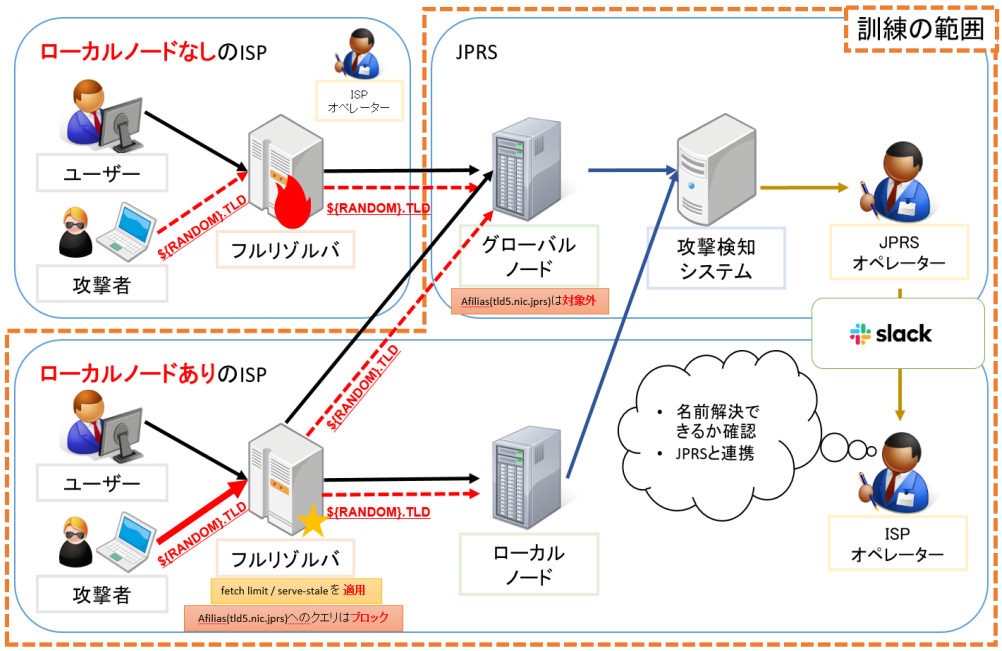


図: 項番#7: グローバルノードの復旧

検証内容に関する特記事項

1. 本実証実験では TLD の権威 DNS サーバーの名前解決の安定性の測定・評価を目的としており、ルートサーバーに対する到達性は常に確保されていることを前提としている。そのため、ルートサーバーも含めた総合的なドメイン名の名前解決の安定性・継続性の測定・評価については、別途、検証や実験が必要になる。
2. 運用中の権威 DNS サーバーやフルリゾルバーが接続されているネットワークをインターネットから実際に切断することは運用中のインターネットサービスに影響を及ぼすため、本実証実験では機器の設定変更による擬似的な切断を発生させることで、検証を実施することとした。なお、その方法は当該組織の上位ネットワークへの接続形態に依存することから各 ISP と協議の上、適切な方法で検証することとした。
3. ローカルノードを設置した ISP 内の利用者の端末が大規模な攻撃に使われた場合、当該 ISP における名前解決が継続不能にある可能性がある。本実証実験では前述の通り、こうした状況が発生した場合の影響についても検証している。

本実証実験における制約事項

1. 本実証実験におけるプラットフォームとして使用した.jprs は、ICANN と JPRS の間で締結されたレジストリ契約により、レジストリオペレーターである JPRS が委任を受けている TLD である。レジストリ契約には.jprs TLD の権威 DNS サーバーのサービスレベルに関する遵守事項(SLA)が含まれるため、それに抵触する状況を故意に発生させる、例えば、.jprs TLD そのものを長時間にわたってインターネットから切断するといった実験は実施不可能である。
2. 各 ISP に設置したローカルノード、及び JPRS が運用するグローバルノードは共に、インターネットに接続されている。本実証実験ではこれらのノードに対し、インターネット経由で DDoS 攻撃をシミュレーションした実トラフィックを生成・送出するため、ISP や JPRS が運用中の既存のサービスに影響しないように、生成・送出する攻撃トラフィックのボリュームを制限するなどの配慮が必要になる。

参考：ICANN による新 gTLD DNS サーバーの SLA

機能	項目	月間のサービスレベル
DNS 名前解決機能	TCP DNS 応答の RTT	の 95%以上が＜1500 未秒
	UDP DNS 応答の RTT	の 95%以上が＜500 ミリ秒
	TCP,UDP DNS 応答の有無	月間停止時間の合計＜432 分(可用性 99%)
ゾーン転送機能	差分更新反映時間	観測値の 95%以上が＜15 分で転送完了
	全量更新反映時間	観測値の 95%以上が＜120 分で転送完了

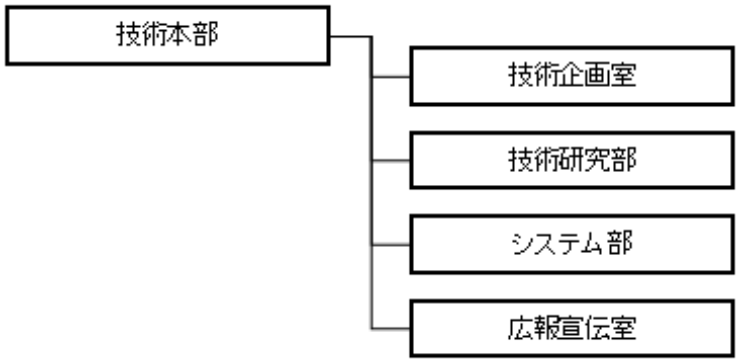
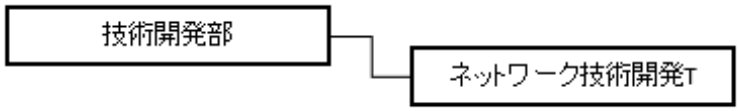
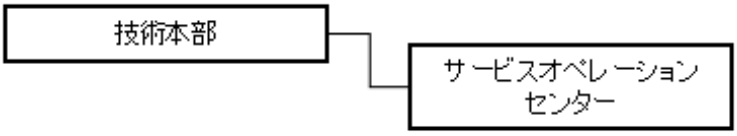
実証実験の体制

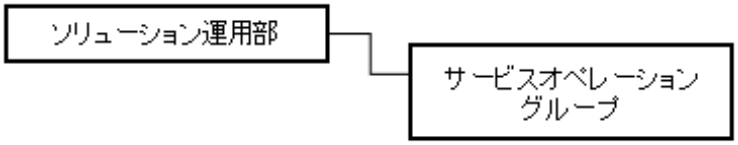
(1) 実証実験実施組織

本研究には、JPRS 及び国内の ISP3 社（五十音順）が参加した。

- TLD DNS サーバー グローバルノードの実証実験組織
  - 株式会社日本レジストリサービス(JPRS)
- TLD DNS サーバー ローカルノード・フルリゾルバーの実証実験組織（五十音順）
  - 株式会社オプテージ(OPTAGE)
  - 株式会社 QTnet(QTnet)
  - 北海道総合通信網株式会社(HOTnet)

(2) 実証実験管理体制

組織名	体制図
株式会社日本レジストリサービス(JPRS)	
株式会社オプテージ(OPTAGE)	
株式会社 QTnet(QTnet)	

北海道総合通信網株式会社(HOTnet)	

実証実験報告（株式会社日本レジストリサービス）

実験シナリオ a

実証実験環境の構成

全体構成

実験シナリオ a における、実験環境の構成を以下に示す。

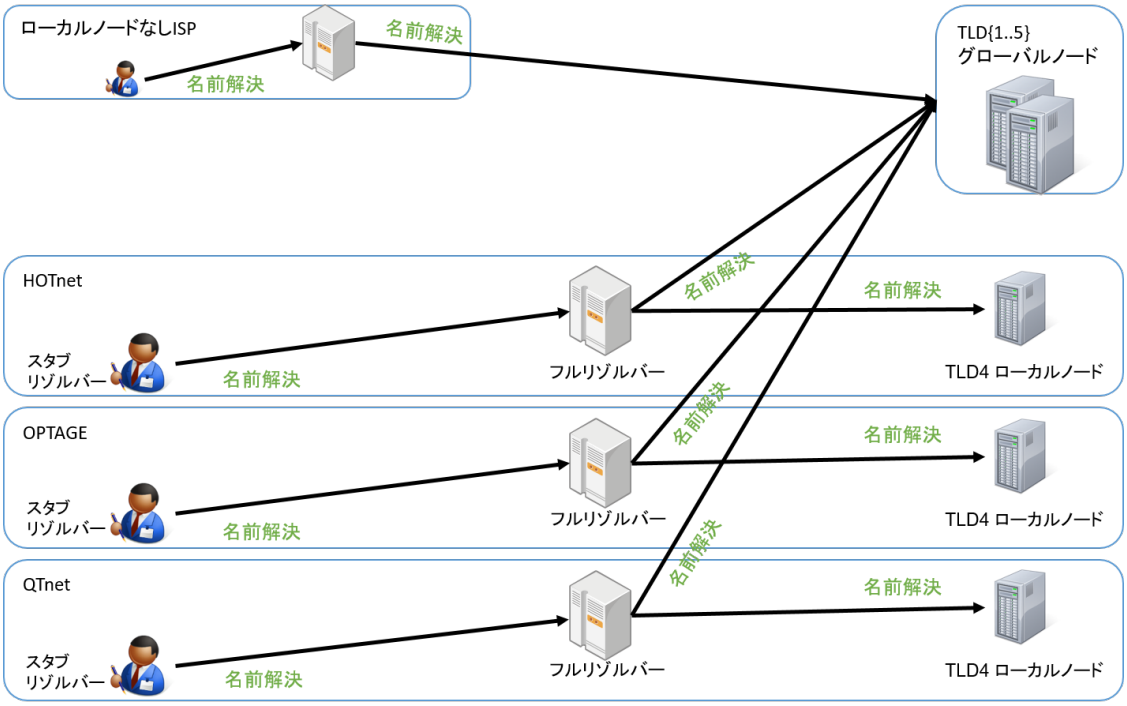


図: 実験シナリオ a 構成図

TLD に属するドメイン名の名前解決要求を受け取ったフルリゾルバーはその TLD の権威 DNS サーバーにアクセスして、名前解決を実行する。その際、その TLD のローカルノードが設置されていない ISP のフルリゾルバーのアクセスは、外部に設置されたグローバルノードに到達する。

一方、ローカルノードが設置された各 ISP では、ISP のフルリゾルバーのアクセスは内部に設置されたローカルノードと、外部に設置されたグローバルノードの双方に到達する。

ローカルノードの内部構成

ローカルノードの内部構成を以下に示す。

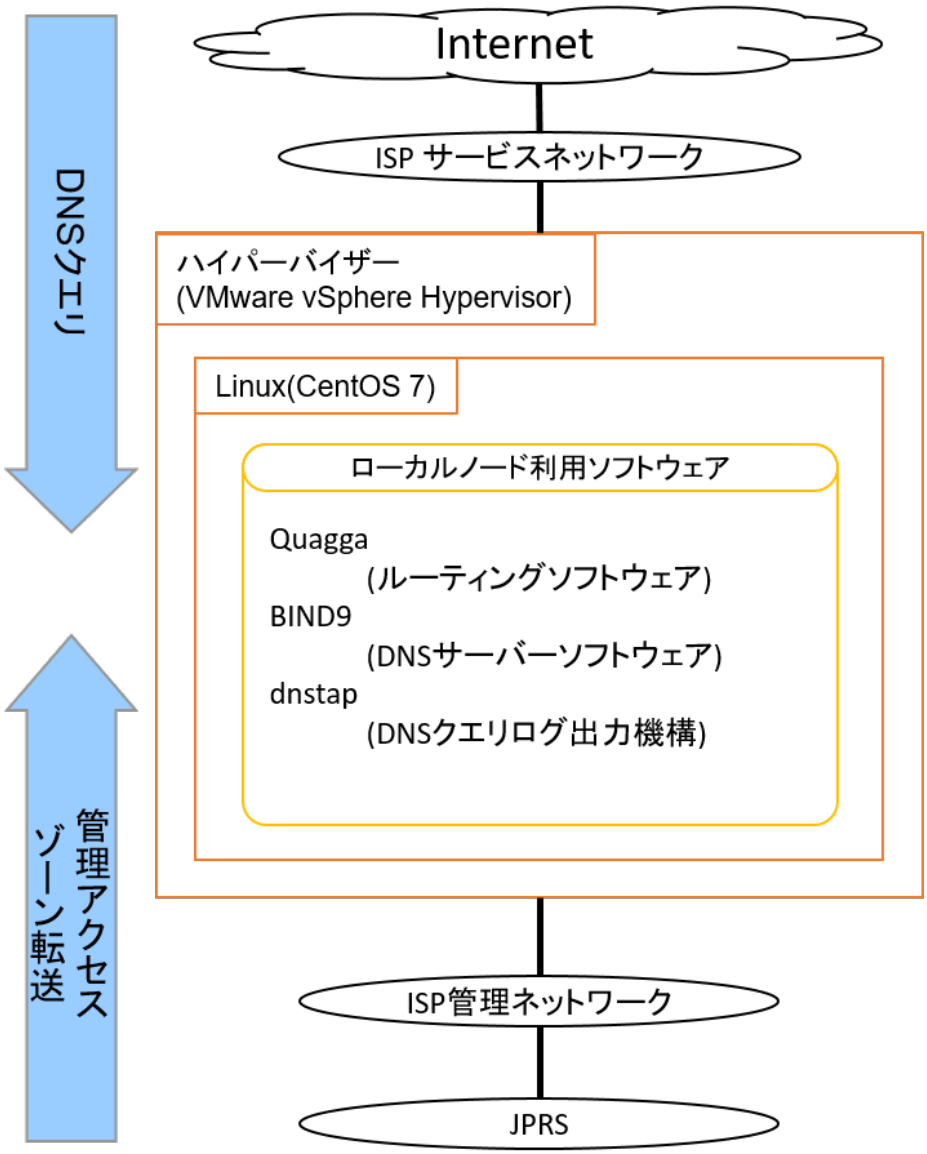


図: ローカルノード構成図

権威 DNS サーバーに IP Anycast を適用する手法を記述した RFC 3258 に従い、ローカルノードは DNS クエリを受け付けるサービス用のネットワークと、サーバーのメンテナンスやゾーン転送に用いるマネージメント用のネットワークの双方に接続する構成とした。これにより、DDoS 攻撃によってサービス用のネットワークにアクセスできない状態になった際にも、障害対応やゾーン転送への影響を回避することが可能になる。

ローカルノードではハイパーバイザーとして VMware vSphere Hypervisor を動作させ、ハイパーバイザー上にインストールされた CentOS 7 にルーティングソフト

ウェアとして Quagga、DNS サーバーソフトウェアとして BIND 9 をそれぞれ動作させることで、権威 DNS サーバーとして構成した。また、BIND 9 には DNS の統計情報を取得するソフトウェアである、dnstap が組み込まれている。

実験シナリオ a の実施内容

実験シナリオ a は、グローバルノードのみの状態で実施する項番 1 から項番 3 と、ローカルノードとグローバルノードを組み合わせた状態で実施する項番 4 から項番 12 により構成される。

以下、それぞれの項番における実施内容について記述する。

グローバルノードのみの状態での実験

1. 通常時（ローカルノード未設置）
    - スタブリゾルバーからクエリを発生させ、名前解決が問題なく行えることを確認する
    - フルリゾルバー#1～#3 からのクエリがグローバルノード#1～#5 に分散されることを確認する
2. グローバルノードに対し攻撃が発生
    - フルリゾルバー#1～#3 で、グローバルノード#1～#5 の IP アドレスへのパケットが当該サーバーに到達しないように設定する。
    - それにより、フルリゾルバー#1～#3 からの.jprs ドメイン名への名前解決が継続可能な状態となるか、クエリの傾向がどのように変化するかを確認する。
3. グローバルノードに対する攻撃が終了
    - フルリゾルバー#1～#3 で項番 2 の設定を解除し、グローバルノード#1～#5 の IP アドレスへの到達性を回復させる。
    - グローバルノード#1～#5 の分断が解除されたことに伴い、復帰することを確認する。

グローバルノードとローカルノードを組み合わせた実験

4. 実験参加 ISP 内にローカルノードを設置
    - ローカルノード#1～#3 を稼働させる。
    - グローバルノード#4 から各ローカルノードへ DNS クエリが移動することを確認する。
    - グローバルノード#1～#3, #5 における DNS クエリの割合の変化を確認する。
5. グローバルノードに対し攻撃が発生

- フルリゾルバー#1～#3 で、グローバルノード#1～#3, #5 の IP アドレスへのパケットが当該サーバーに到達しないように設定する。
- それにより、フルリゾルバー#1～#3 からの.jprs ドメイン名への名前解決が継続可能な状態となるか、クエリの傾向がどのようになるかを確認する。

6. ローカルノード設置 ISP 内（1 社）からも攻撃が発生
   - 項番 5 の状態に加え、フルリゾルバー#1 でローカルノード#1 の IP アドレスへのパケットが当該サーバーに到達しないように設定する。
   - それにより、フルリゾルバー#1 からの.jprs ドメイン名へのクエリがどう変化するか、名前解決が可能かを確認する。
7. ローカルノード設置 ISP 内（2 社）からも攻撃が発生
   - 項番 6 の状態に加え、フルリゾルバー#2 でローカルノード#2 の IP アドレスへのパケットが当該サーバーに到達しないように設定する。
   - それにより、フルリゾルバー#2 からの.jprs ドメイン名へのクエリがどう変化するか、名前解決が可能かを確認する。
8. ローカルノード設置 ISP 内（3 社）からも攻撃が発生
   - 項番 7 の状態に加え、フルリゾルバー#3 でローカルノード#3 の IP アドレスへのパケットが当該サーバーに到達しないように設定する。
   - それにより、フルリゾルバー#3 からの.jprs ドメイン名へのクエリがどう変化するか、名前解決が可能かを確認する。
9. ローカルノード設置 ISP 内（1 社）から攻撃が終了
   - フルリゾルバー#1 で項番 6 の設定を解除し、ローカルノード#1 の IP アドレスへの到達性を回復させる。
   - それにより、フルリゾルバー#1 からの.jprs ドメイン名へのクエリがどう変化するか、名前解決が可能かを確認する。
10. ローカルノード設置 ISP 内（2 社）から攻撃が終了
    - フルリゾルバー#2 で項番 7 の設定を解除し、ローカルノード#2 の IP アドレスへの到達性を回復させる。
    - それにより、フルリゾルバー#2 からの.jprs ドメイン名へのクエリがどう変化するか、名前解決が可能かを確認する。
11. ローカルノード設置 ISP 内（3 社）から攻撃が終了
    - フルリゾルバー#3 で項番 8 の設定を解除し、ローカルノード#3 の IP アドレスへの到達性を回復させる。
    - それにより、フルリゾルバー#3 からの.jprs ドメイン名へのクエリがどう変化するか、名前解決が可能かを確認する。
12. すべての攻撃が終了

- フルリゾルバー#1～#3 で、グローバルノード#1～#3, #5 の IP アドレスへの到達性を回復させる。
- グローバルノード#1～#3, #5 への分断が解除されたことに伴い、復帰することを確認する。

実験における特記事項

- 今回の実験では運用中のネットワークへの影響を回避するため、実際の DDoS 攻撃に替え、ISP のフルリゾルバーにおけるフィルタリングを実施することで、攻撃を模擬した。
- 参加 ISP とチャットツールを用い、連携する形で実験を実施した。

JPRS における比較実験とその結果

JPRS では各 ISP における実験結果との比較を目的とし、ローカルノード未設置の環境について、外部の VPS サービスを利用した比較実験を実施した。

以下、比較実験で用いた環境と、その結果について記述する。

VPS サービス	Amazon Web Service EC2
リージョン	ap-northeast-1
インスタンス	t3a.nano
OS	Amazon Linux
DNS サーバー	BIND 9.11.10

今回の比較実験ではキャッシュの影響を排除するため、ローカルノード・スタブリゾルバーにおける各項番の操作ごとに、フルリゾルバーにおいてキャッシュのクリアを実施した。

比較実験の結果を以下に示す。この結果は VPS 環境から.jprs の各 NS に対し、1 分ごとに 5 回の ping を試行し、その平均値をプロットしたものである。

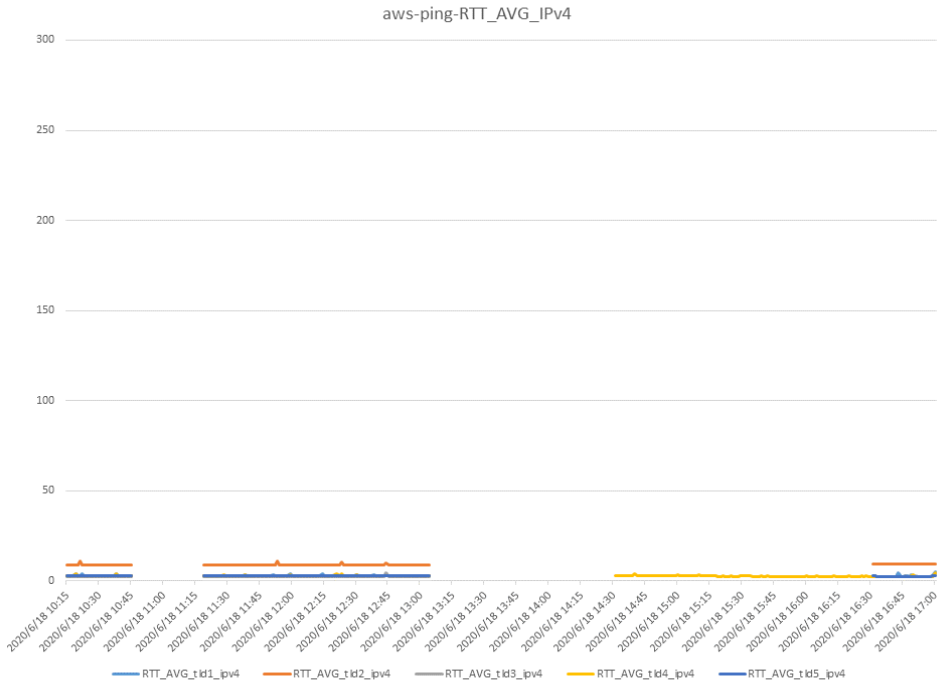


図: VPS からの IPv4 PING 結果

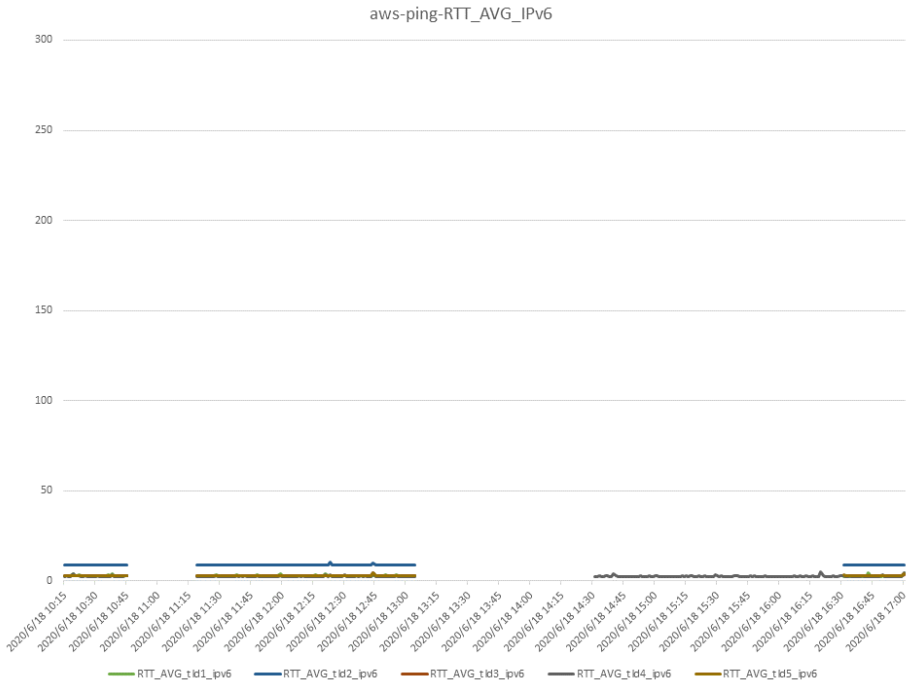


図: VPS からの IPv6 PING 結果

当該実験環境にはローカルノードが存在しないため、名前解決の際にはグローバルノードにアクセスことになる。そのため、すべてのグローバルノードに到達できなくなった場合、名前解決の継続性が失われる。

今回の比較実験の結果から、10:45～11:15 のすべてのグローバルノードがサービスダウンしたタイミングで、すべての TLD への ping 到達性が失われていることが読み取れる。また、シナリオによって 14:30 に TLD4 のグローバルノードへの到達性が回復し、グラフ上においても、TLD4 のみ応答が返って来るようになっていることが読み取れる。

その後、16:30 に TLD1,2,3,5 のグローバルノードへの到達性も回復し、ping の応答が返って来ていることが読み取れる。

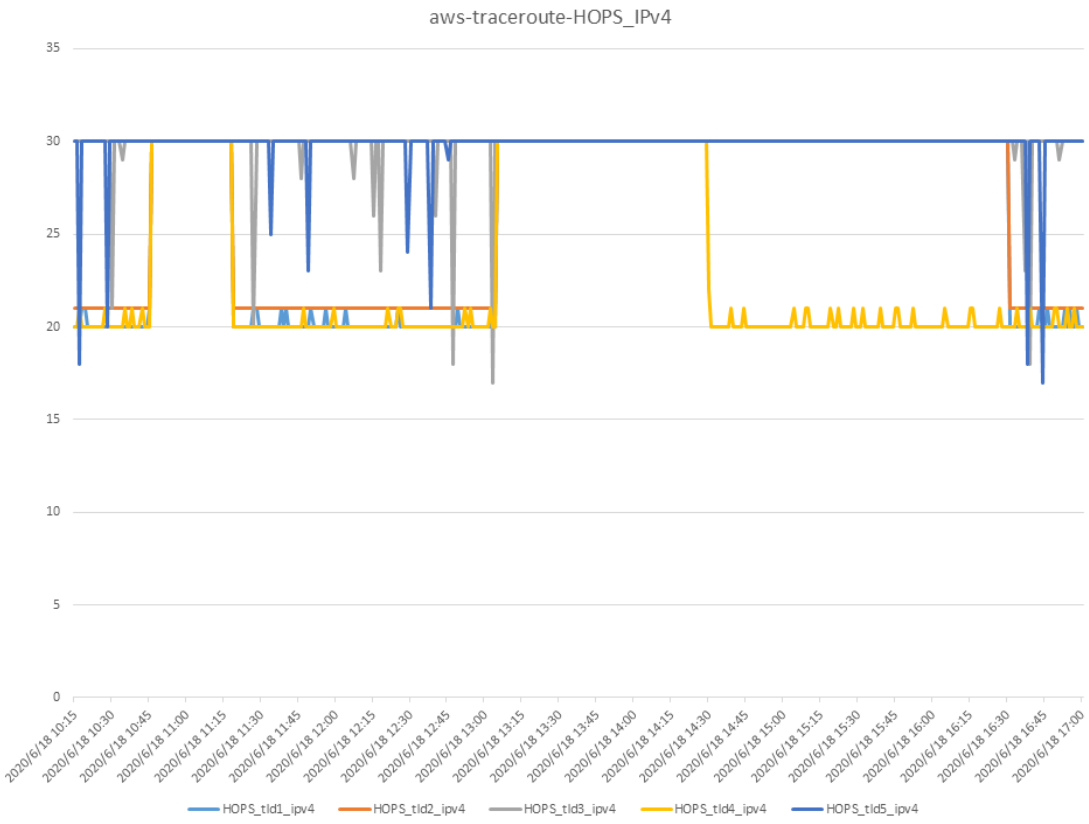


図: VPS からの IPv4 traceroute hop 数

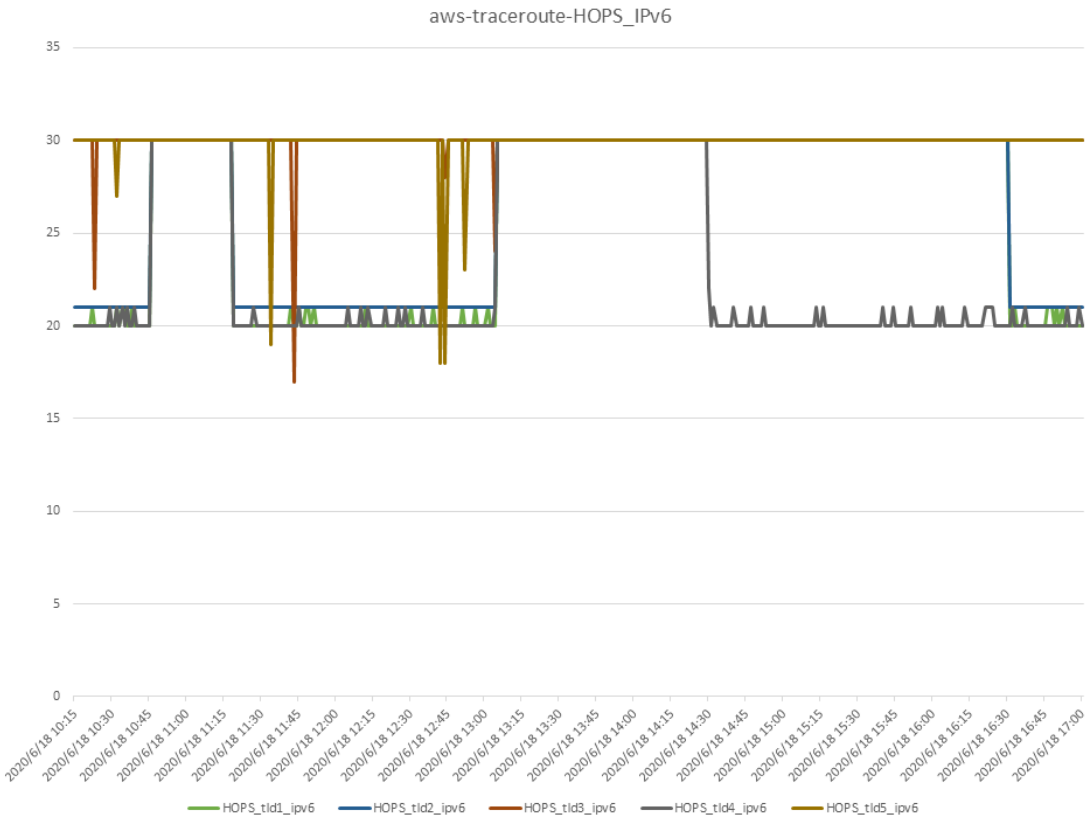


図: VPS からの IPv6 traceroute hop 数

なお、今回の実験では、Amazon Web Service EC2 からグローバルノードへの経路の HOP 数について、途中のルーターで値の出力が止まってしまうケース、途中の経路までは IP アドレスが表示されるものの、以降の出力においてルーターからの応答がない旨の*表示が traceroute コマンドの最大値である 30HOP まで出力され続けるケースが観測された。

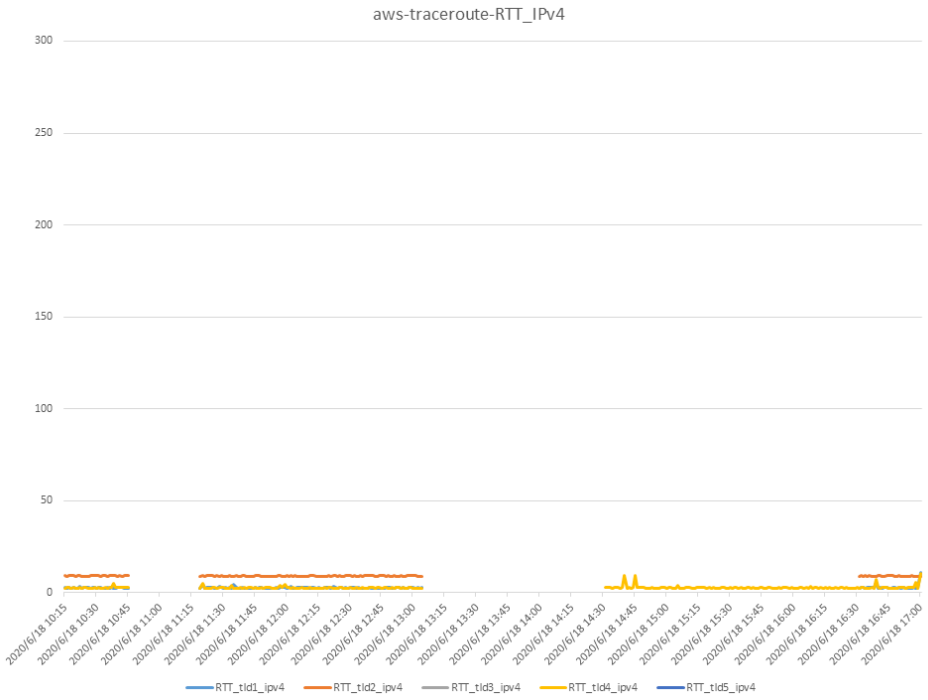


図: VPS からの IPv4 traceroute RTT

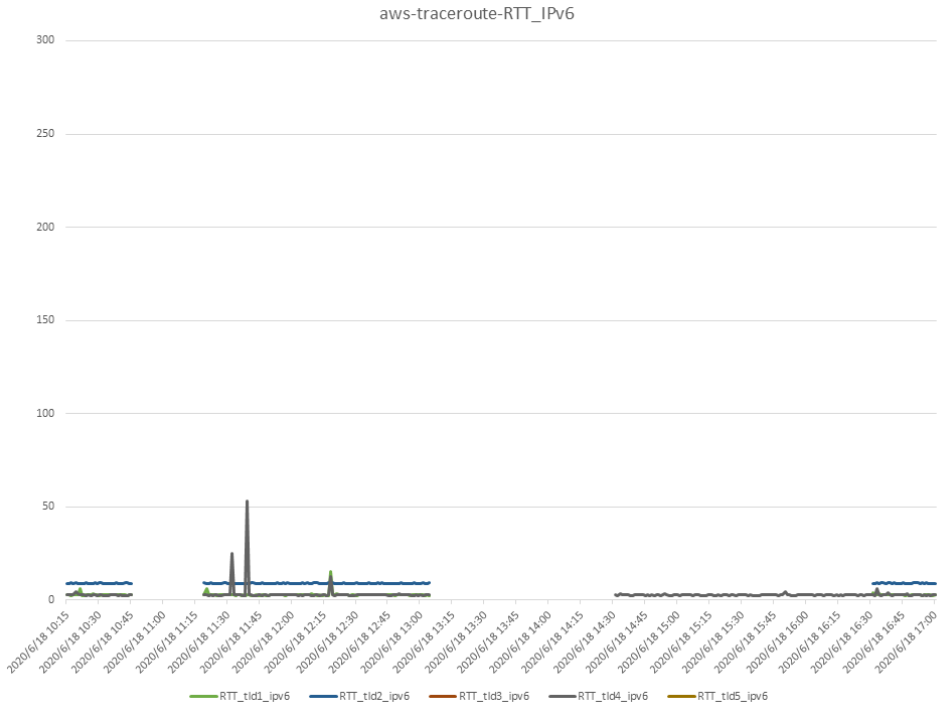


図: VPS からの IPv6 traceroute RTT

traceroute コマンドで出力される RTT についても IPv4, IPv6 共に、ping の RTT と同様の傾向が観測された。10:45～11:15 のすべてのグローバルノードがダウンしたタイミングで、すべての TLD への到達性が失われていることが読み取れる。前述した結果と同様、シナリオによって 14:30 に TLD4 のグローバルノードが回復し、グラフ上も、TLD4 のみ応答が返ってくるようになっていることが読み取れる。

その後、16:30 に TLD1,2,3,5 のグローバルノードも回復し、応答が返ってきていることが読み取れる。

比較実験により得られた知見

JPRS で実施した比較実験により、以下の知見が得られた。

- ローカルノードがなく、グローバルノードにのみが存在する構成では、グローバルノードへの到達性が失われた場合、名前解決の継続性に問題が生じる。
- ローカルノードがない環境であっても、グローバルノードとの接続性が回復した場合、名前解決が再開される。

実運用に向けた課題

実証実験・比較実験により得られた、ローカルノードの実運用に向けた課題について解説する。

- 実運用において、ISP ネットワーク内のフルリゾルバーから権威 DNS サーバーへの経路がグローバルノードからローカルノードに切り替わっていることを確認する必要がある。解決方法として、経路の変更を確認するためのプローブを ISP 網内に設置することが考えられる。
- 今回の実験では ISP に設置するノードをローカルノードとし、動的な経路広告を実施しない形で実験した。実運用においては、ローカルノードをグローバルノードに変更する、あるいはその逆のケースのように、経路広告を動的に変更する運用が可能かどうかについても、検討・実験を進めることが考えられる。
- 攻撃者が ISP 網内に存在するケースでは、グローバルノードがダウンしてしまった場合、ローカルノードの容量の範囲内でサービスを提供する必要がある。それを実現するためには早期警戒・フルリゾルバーにおける対策との併用・当該 ISP 内で発生しうるトラフィック量などに応じた性能設計が必要になる。
- ローカルノードを地理的・ネットワーク的にどう配置するかにより、効果が大きく変化する。そのため、ローカルノードの設置にあたっては、トラフィ

ック量、ネットワーク構造、災害発生頻度などを考慮したうえで、その設置箇所を決める必要がある。

- ローカルノードに対する大量攻撃によって当該ローカルノードの BGP の経路情報が失われた場合、攻撃トラフィックが ISP から漏出し、グローバルノードに到達する可能性がある。攻撃の影響を局所化するためには、当該 ISP との BGP ピアリングを優先的に保護ことが必要になる。
- その一方、DDoS 攻撃によってローカルノードが停止し、当該 ISP から他のグローバルノードへの疎通性も失われた場合、ISP 網内の利用者は名前解決ができない状態になる。そのため、DDoS 攻撃の局所化とグローバルノードの保護については、権威 DNS サーバーのトータルなサービスレベルを念頭に置いた、総合的な検討を実施する必要がある。

実験シナリオ b

実証実験環境の構成

実験シナリオ b における、実験環境の構成を以下に示す。

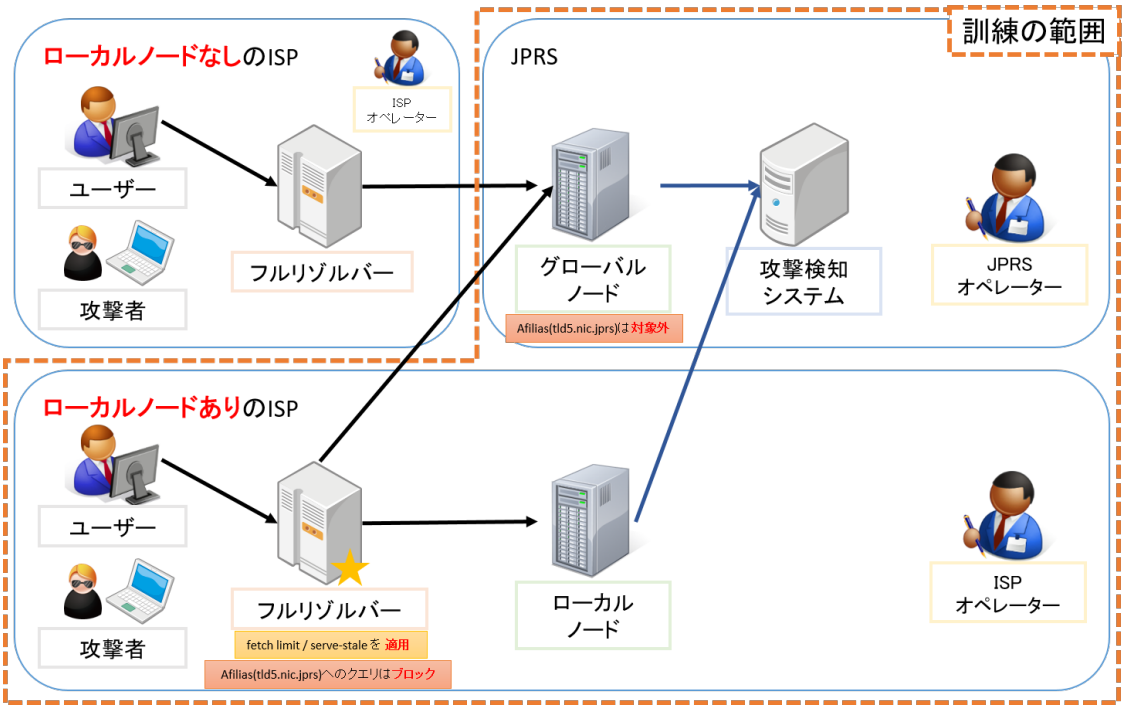


図: 実験シナリオ b 構成図

実験シナリオ a と同様、ISP 内にはフルリゾルバーとローカルノードを設置している。ISP のフルリゾルバーのアクセスは ISP の内部に設置されたローカルノードと、外部に設置されたグローバルノードの双方に到達する。

また、本シナリオでは JPRS 側に、各ローカルノード・グローバルノードに対するランダムサブドメイン攻撃を検知する、攻撃検知システムを設置している。攻撃検知システムでは、各ローカルノード・グローバルノードから収集したクエリデータを処理し、どのノードにどのようなクエリが到達したかを分析、可視化するためのツールを動作させている。

この状況において、各ノードを標的としたランダムサブドメイン攻撃を発生させ、JPRS のオペレーターが攻撃検知システムからアラートを受信し、当該 ISP のオペレーターにその状況を共有する。ISP のオペレーターは JPRS から共有された情報を元に、状況の判断、対応を進める。

なお、本実験環境では ISP のフルリゾルバー側における DDoS 攻撃対策として fetch-limit 機能を導入している。本機能はランダムサブドメイン攻撃を受けた際の権威 DNS サーバーの各ノード（ローカルノード・グローバルノード）への過剰なクエリを抑制し、攻撃の効果を軽減するものである。

JPRS と各組織間の連絡・情報共有には、汎用のチャットツールである Slack を使用している。

実験の内容

項番	実施日	時間	シナリオ	実施概要	実施作業		
					JPRS		ISP
					事務局	プレイヤー	
0	2020/4/8（水）	14:00	事前準備	訓練を行うための事前準備	・[LN] ローカルノード立ち上げ作業(上がっていない場合） ・ISP へ作業依頼 ・[LN][GN] パケットキャプチャ開始	・待機	開始条件:事務局からの連絡 ・[LR] ローカルリゾルバ立ち上げ作業（上がっていない場合） ・手順 A [LR] tld5.nic.jprs のフィルタ ・手順 B [LR] パケットキャプチャ ・手順 C [SR] パケットキャプチャ ・手順 D [SR] 継続 dig ・手順 E [LR] 継続 ping
1	2020/4/8（水）	14:20	通常時	訓練開始までの待ち合わせと、平常時の状態のログを記録。	・項番 0 完了後 10 分放置	・待機	開始条件:#0 終了後自動的に移行 ・項番 0 完了後 10 分放置

2	2020/4/8（水）	14:30	攻撃発生	ISP 網内から攻撃が発生。攻撃検知システムで JPRS が攻撃を検知。	・ISP へ作業依頼	開始条件:攻撃検知システムからアラートが飛んだら ・攻撃を検知	開始条件:事務局からの連絡 ・手順 F [SR] 攻撃スクリプトを実行
3	2020/4/8（水）	14:40	攻撃検知と連携	攻撃を検知。JPRS から各 ISP に攻撃が発生している旨を連絡する。各 ISP は JPRS からの連絡を受け、名前解決に影響が出ていないことを確認し、JPRS に連携する。		開始条件:#2 で攻撃を検知したら ・Slack で各組織に攻撃の検知を連絡（伝え方はアドリブ）	開始条件:JPRS プレイヤーからの連絡 ・JPRS から Slack で連絡を受け、対応、問い合わせなど（下記手順の結果の共有+アドリブ） ・名前解決に影響が出ていないことを確認、JPRS に共有 ・手順 G [SR] dig をしてみて失敗しないことを確認 ・手順 H [LR] dig をしてみて失敗しないことを確認

4	2020/4/8（水）	15:00	グローバルノードダウンの検知	JPRS 社内で全グローバルノードがダウンしていることを検知。 各 ISP でもグローバルノードに対して名前解決が不可能になる。	・ISP へ作業依頼 ・JPRS プレイヤーへ連絡	開始条件:事務局からの連絡 ・グローバルノードのダウンを検知(訓練事務局から通知、みなしで実施する)	開始条件:事務局からの連絡 ・手順 I [LR] tld{1..3}.nic.jprs へのトラフィックをフィルタ ・手順 I 実施後に tld{1..3}.nic.jprs からの応答が無くなったことを JPRS に連携
5	2020/4/8（水）	15:10	グローバルノードダウンの連携	JPRS から各 ISP にグローバルノードがダウンしたことを通知。 各 ISP は JPRS からの連絡を受け、名前解決に影響が出ていないことを確認し、JPRS に連携する。		開始条件:#4 でグローバルノードのダウンを検知したら ・各組織にグローバルノードのダウンを連携（伝え方はアドリブ）	開始条件:JPRS プレイヤーからの連絡 ・JPRS から Slack で連絡を受け、対応、問い合わせなど（下記手順の結果の共有+アドリブ） ・名前解決に影響が出ていないことを確認し、JPRS に共有 ・手順 J [SR] dig をしてみて失敗しないことを確認 ・手順 K [LR] dig をしてみて失敗しないことを確認

6	2020/4/8（水）	15:30	状況確認	JPRS から各 ISP にグローバルノードの状況を連携。 JPRS と外部のネットワークが飽和しており、JPRS からローカルノードへのログイン不可。 各 ISP にローカルノードの状態を確認してもらい、結果の共有を受ける。	・JPRS プレイヤーへ連絡	開始条件:事務局からの連絡 ・グローバルノードの復旧状況を伝える（16:00 頃に復旧予定、アドリブで伝える） ・JPRS から（帯域飽和のため）ローカルノードにログインできないため、状態を確認してもらうよう依頼（伝え方はアドリブ）	開始条件:JPRS プレイヤーからの連絡 ・フルリゾルバの状況確認 ・手順 L [LR] ログを見て、jprs が ratelimit 対象になっているか確認 ・ローカルノードの状態確認 ・手順 M [LN] named のプロセス、ログを確認

7	2020/4/8（水）	16:00	グローバルノード復旧	グローバルノードが復旧。JPRS から、各 ISP へ連絡。 各 ISP からグローバルノードへ名前解決ができることを確認し、JPRS に結果を共有。	・ISP へ作業依頼 ・JPRS プレイヤーへ連絡	開始条件:事務局からの連絡 ・グローバルノードが復旧したことを伝える（伝え方はアドリブ）	開始条件:事務局からの連絡 ・手順 N [LR] フィルタの解除 ・手順 N 実施後に tld{1..3}.nic.jprs からの応答が復旧したことを JPRS に連携
8	2020/4/8（水）	16:15	訓練終了準備	訓練終了のため、データ記録の停止を行う。	・ISP へ作業依頼 ・[LN][GN] パケットキャプチャ開始	・終了準備	開始条件:事務局からの連絡 ・手順 O [LR] パケットキャプチャの停止 ・手順 P [SR] パケットキャプチャの停止 ・手順 Q [SR] 継続 dig の停止 ・手順 R [LR] 継続 dig の停止
9	2020/4/8（水）	16:30	訓練終了	訓練終了	・ISP/JPRS へ終了連絡	・訓練終了	・訓練終了

実験結果

以下に、実験実施中の Slack による連絡・情報共有の状況を抜粋したものを掲載する。Slack を用いた情報共有により、JPRS と実験に参加した ISP の間における迅速な情報共有と、円滑な連携を実現している。

Slack では、攻撃検知システムのアラートを契機としたランダムサブドメイン攻撃の発生・各 ISP における名前解決の状況などを随時共有した。これにより、攻撃によってグローバルノードへの到達性が失われた際にローカルノードを用いた名前解決が継続されること、権威 DNS サーバー側における攻撃の検知と円滑な情報共有、フルリゾルバー側における DDoS 攻撃対策の実施が DNS の安定運用において有用であることを確認できた。

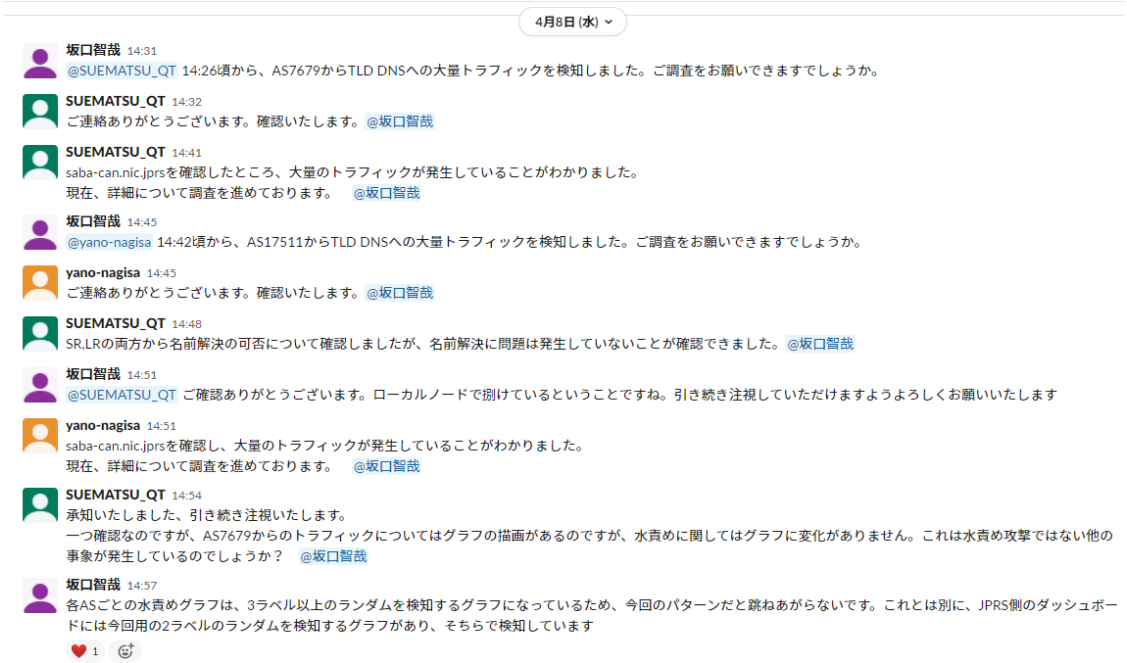


図: Slack でのやり取り

本実験により得られた知見

本実験により、DNS オペレーター間の連携強化に関する以下の知見が得られた。

- ローカルノードの設置に加え、ランダムサブドメイン攻撃の検知と情報共有により、グローバルノードに対する攻撃が開始された段階で、警戒態勢を構築できる。
- ローカルノードの設置に加え、フルリゾルバー側に DDoS 攻撃対策として fetch-limit 機能を導入しておくことで、ローカルノードが ISP の内部からランダムサブドメイン攻撃を受けた場合の影響を緩和できる。

- 攻撃検知システムの構築・運用により攻撃元の判定と攻撃先の検知を迅速に実施することは、DNS オペレーター間の連携強化に有効である。

実運用に向けた課題

本実験により得られた、実運用における DNS オペレーター間の連携強化に向けた課題について記述する。

- 今後、シナリオや攻撃パターンなどを変更した上で同様の実験を継続し、さまざまな攻撃パターンへの対応や各組織間における最適な連絡手段の決定に資するための取り組みを進めていく必要がある。
- 実運用において、JPRS に設置した攻撃検知システムから各 ISP のフルリゾルバーのオペレーターに、アラートを直接送信・対応する運用形態を採用することも検討されうる。ただし、その実現には ISP 側における緊急対応体制の構築・False positive や False negative に対する対応など、解決すべき課題が存在する。
- 攻撃者が ISP 網内に存在する場合、ローカルノードを設置し、フルリゾルバー側に fetch-limit を導入した場合であっても、グローバルノード・ローカルノードに対する通常の DNS クエリへの制限が発動する場合がある。このため、そうした攻撃が発生した場合、当該 ISP における名前解決に一定の影響が及ぶ。
- 各ノードに対するゾーン転送は今回の実験における検証の対象外とした。そのため、実運用にあたり攻撃のゾーン転送への影響について、別途検証する必要がある。
- 本研究における手法、すなわちローカルノードの設置により攻撃耐性を向上させる方法では、ローカルノード設置のメリットを受けられるのは当該ノードを設置した ISP に限定される。今後、ローカルノードからグローバルノード・グローバルノードからローカルノードへの動的な変更、広告範囲を限定した上での経路広告によるサービス範囲の柔軟な制御など、当該ノードを設置した ISP 以外の ISP にもノード設置のメリットが及ぶようにする手法について、検討を継続していきたい。
- 今回は情報共有の手段として Slack を用いることで、迅速な情報共有と円滑な連携を実現できた。しかし、Slack は第三者が運営する外部サービスであり、各組織の運用ポリシーや契約上の問題などから、実運用において即座に導入することができないケースがあり得る。今後、そうした状況に対応するための、最適な情報共有の手段についても検討を進めていく必要がある。

実証実験報告（北海道総合通信網株式会社）

実験シナリオ a

目的

北海道は東京・大阪から地理的に離れており、大規模障害の発生時に TLD DNS サーバーへの到達性が失われるリスクが、他地域に比べて高い。また、障害が実際に発生した場合、復旧までにある程度の時間を要することが想定される。

そうした状況から、前回研究では HOTnet の ISP ネットワーク内にローカルノードを設置することで、震災などによる大規模障害によりネットワークが分断された場合にも、当該 TLD を使ったインターネット上のサービスが継続的に利用可能になることを検証した。

一方、近年 DNS サービスを標的としたサイバー攻撃が増加しており、大規模なイベントを標的とした DDoS 攻撃によって DNS サービスが停止した場合、インターネットの利用やサービス提供において、致命的な影響が発生することが想定される。

こうした状況から、本実験では TLD DNS サーバーがサイバー攻撃によって応答不能となる状況を想定し、HOTnet の ISP ネットワーク内にローカルノードを設置することで名前解決の継続を図るための技術検証、及び評価を目的とした。

構成

本実験の実施に際し、HOTnet において以下の環境を構築した。

【構成概要図】

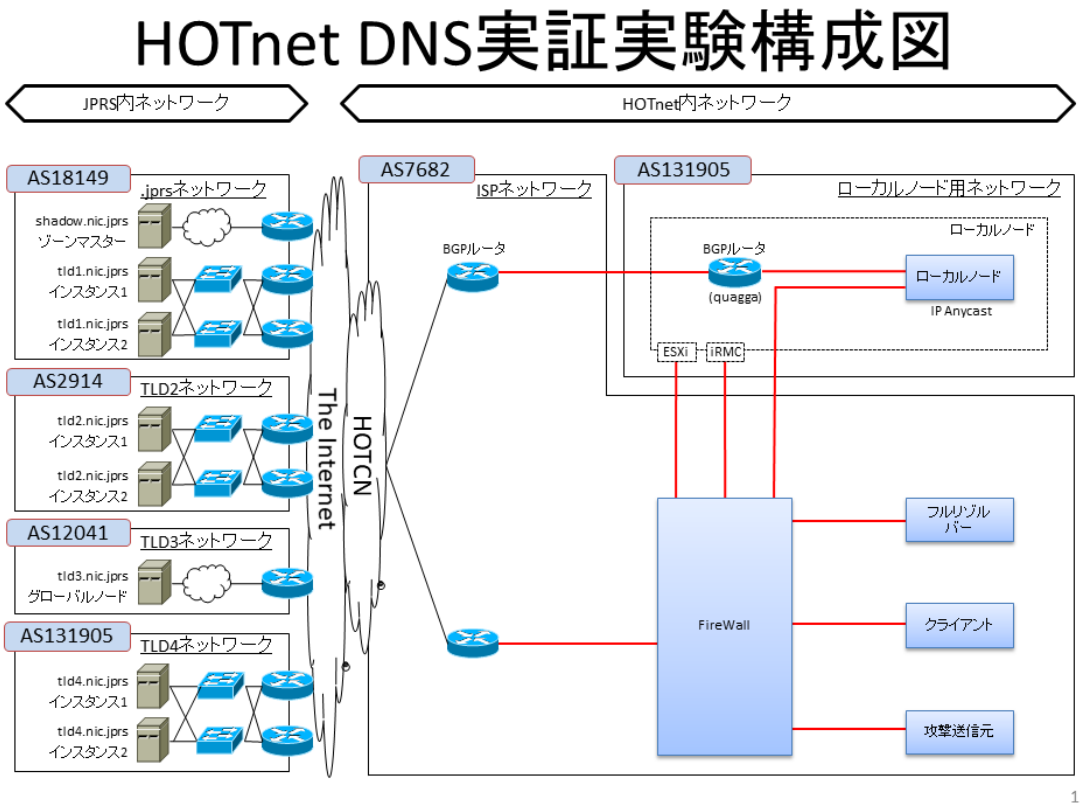


図 1: HOTnet DNS 実証実験構成図

構成機器概要

- 実証実験用スタブリゾルバー
- dig:9.11.4
- 実証実験用フルリゾルバー
- DNS：BIND 9.11.10

実験内容

JPRS 準備の「2.1.3 のシナリオ」に従い、実証実験を遂行した。

実験結果

本実験ではスタブリゾルバーおよびフルリゾルバーにおいて ping, traceroute コマンドを実行し、各種データを取得した。シナリオの概要、および取得したデータをグラフ化した図を以下に示す。

- シナリオの概要

1. 平常時の状態
2. グローバルノードへの攻撃が発生し、グローバルノードがダウン
3. グローバルノードへの攻撃が収束し、グローバルノードが回復
4. ローカルノードの稼働開始
5. グローバルノードへの攻撃が発生し、グローバルノードがダウン
6. HOTnet ローカルノードへの攻撃が発生し、HOTnet ローカルノードがダウン
7. OPTAGE ローカルノードへの攻撃が発生し、OPTAGE ローカルノードがダウン
8. QTnet ローカルノードへの攻撃が発生し、QTnet ローカルノードがダウン
9. HOTnet ローカルノードへの攻撃が収束し、HOTnet ローカルノードが復旧
10. OPTAGE ローカルノードへの攻撃が収束し、OPTAGE ローカルノードが復旧
11. QTnet ローカルノードへの攻撃が収束し、QTnet ローカルノードが復旧
12. グローバルノードへ攻撃が収束し、グローバルノードが回復

各シナリオ状況における、HOP 数および RTT 計測結果

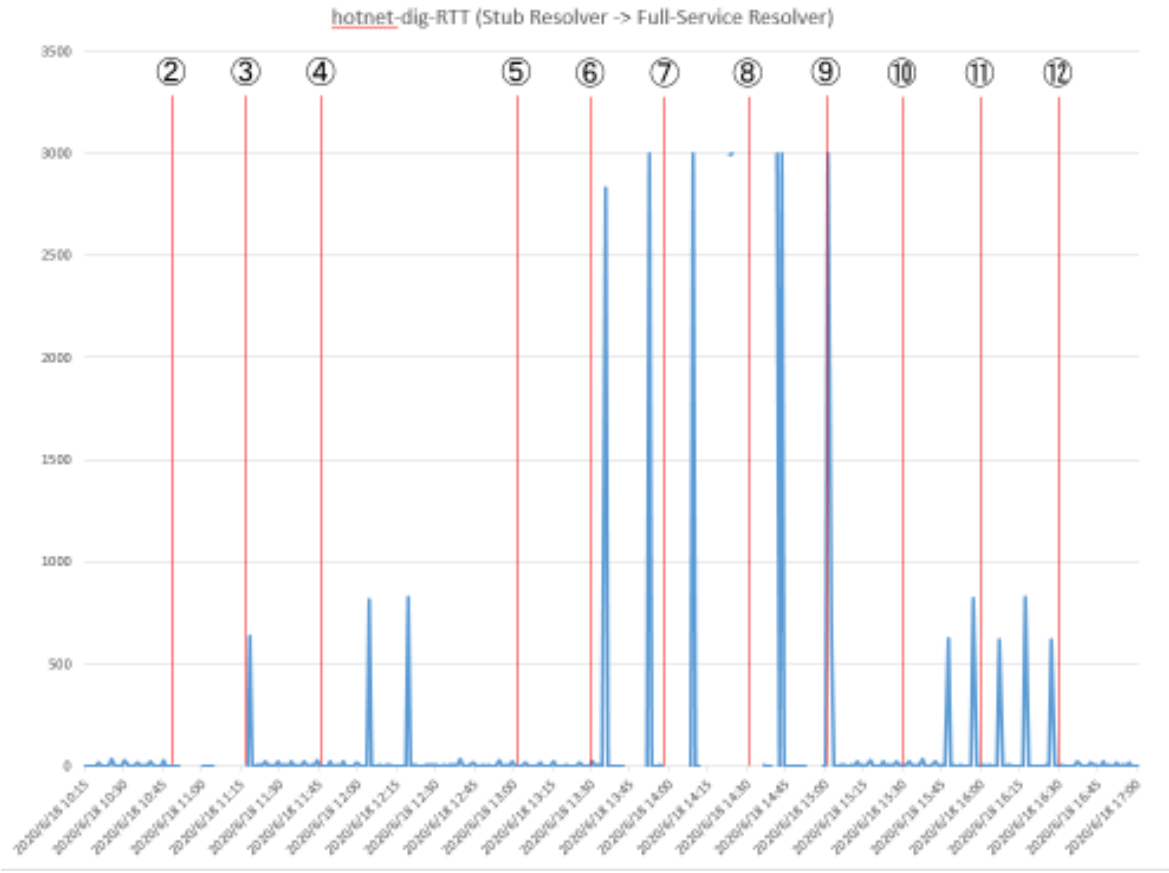


図 2. dig-rtt(スタブリゾルバーからフルリゾルバーへの dig による、RTT 値計測)

- グローバルノードがダウンした②で名前解決の応答が得られなくなっており、③でグローバルノードが復旧したタイミングで応答が復旧している。
- ⑥から⑨までは HOTnet ローカルノードがダウンしたことにより、名前解決の応答が得られなくなっている。
- ⑨以降は HOTnet ローカルノードが復旧したことにより、名前解決の応答が復旧している。

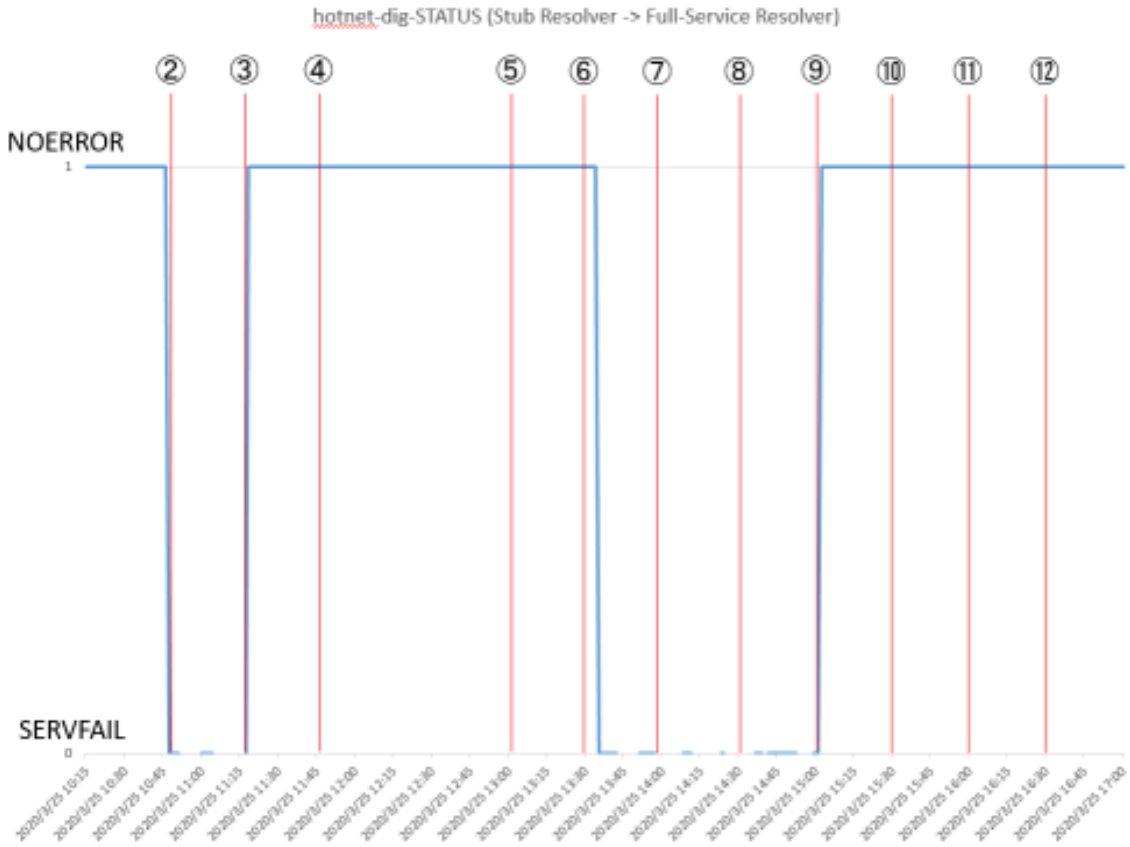


図 3. dig-status(スタブリゾルバーからフルリゾルバーへの dig による、応答 STATUS の計測)

- グローバルノードがダウンした②で名前解決の応答が得られなくなっており、③でグローバルノードが復旧したタイミングで応答が復旧している。
- ⑥から⑨までは HOTnet ローカルノードがダウンしたことにより、名前解決の応答が得られなくなっている。
- ⑨以降は HOTnet ローカルノードが復旧したことにより、名前解決の応答が復旧している。

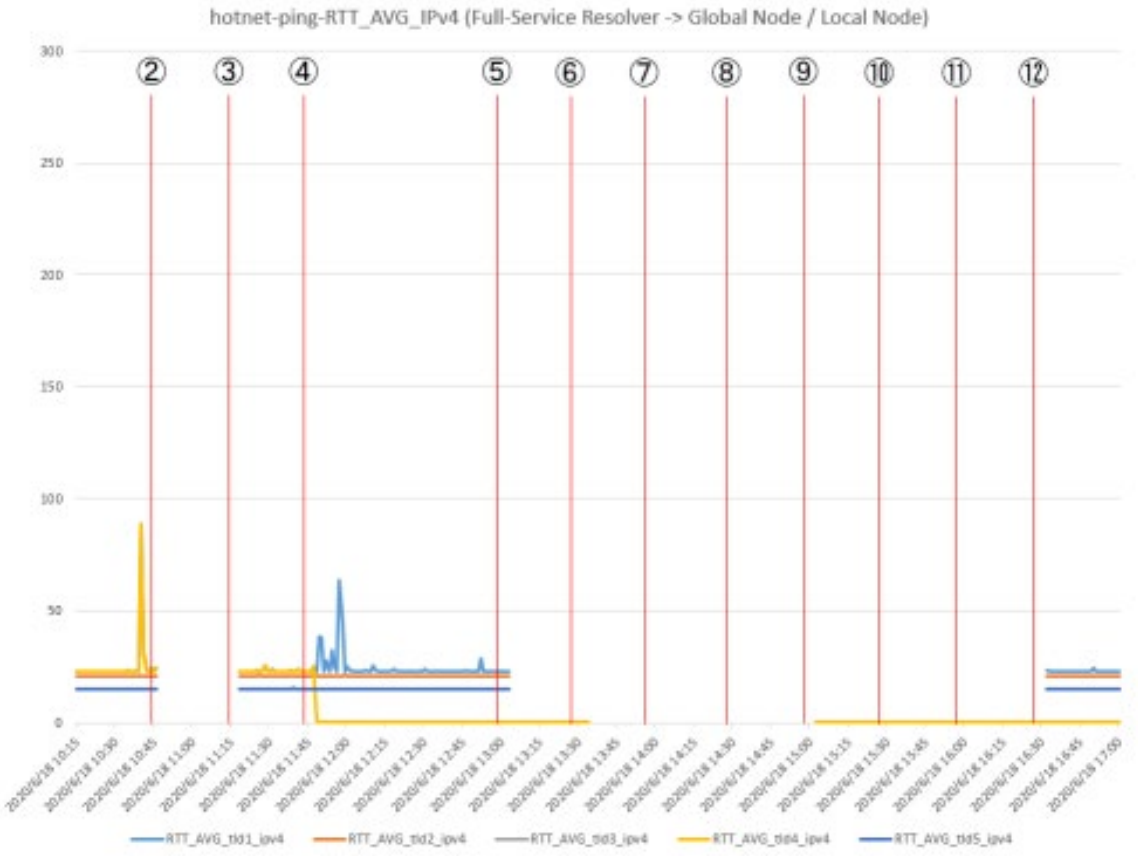


図 4. ping-rtt-v4(フルリゾルバーからグローバルノードへの ping による、IPv4 応答の RTT 値計測)

- グローバルノードがダウンした②で ping の応答が得られなくなっており、③でグローバルノードが復旧したタイミングで復旧している。
- ④でローカルノードを追加したタイミングで、tld4 への RTT 値が想定通り下がっていることを確認できた。
- ⑥から⑨までは HOTnet ローカルノードがダウンしたことにより、ping の応答がなくなっている。
- ⑨以降は HOTnet ローカルノードが復旧したことにより、ping の応答が復旧している。

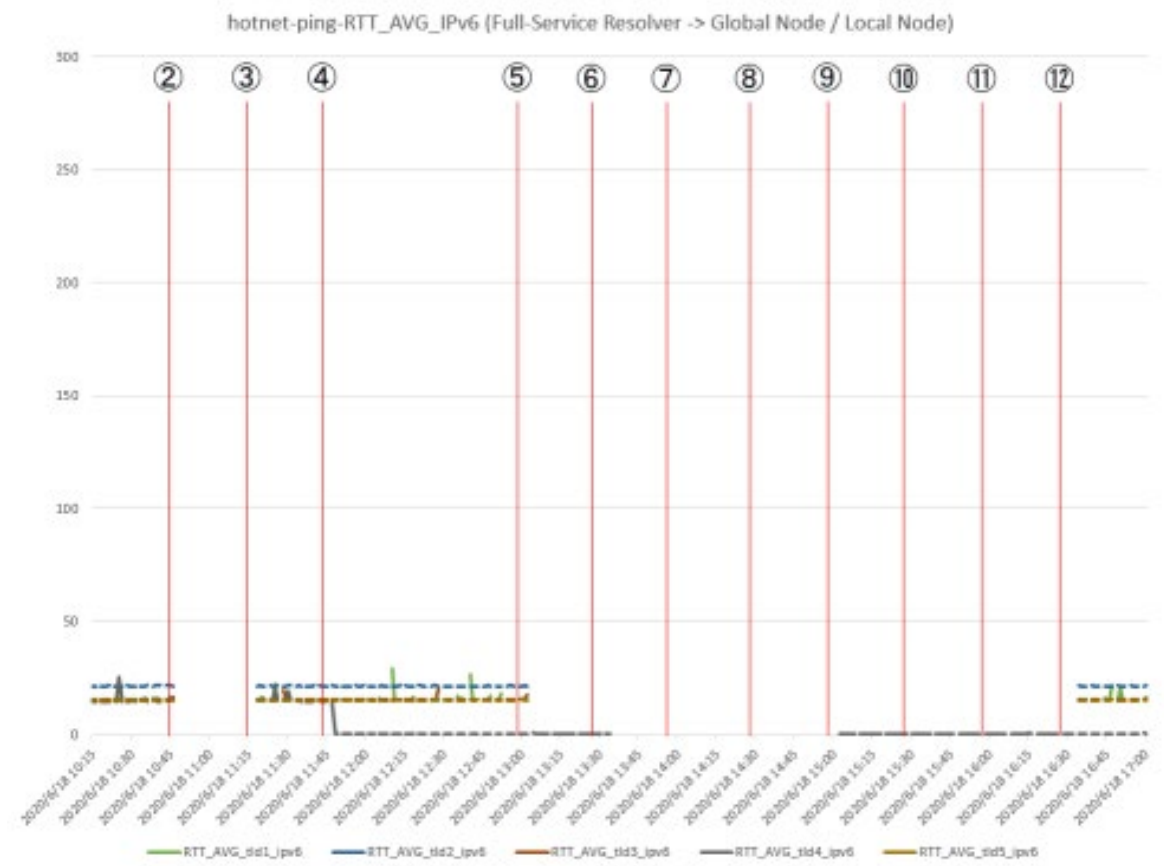


図 5. ping-rtt-v6(フルリゾルバーからグローバルノードへの ping による、IPv6 応答の RTT 値計測)

- グローバルノードがダウンした②で ping の応答が得られなくなっており、③でグローバルノードが復旧したタイミングで復旧している。
- ④でローカルノードを追加したタイミングで、tld4 への RTT 値が想定通り下がっていることを確認できた。
- ⑥から⑨までは HOTnet ローカルノードがダウンしたことにより、ping の応答がなくなっている。
- ⑨以降は HOTnet ローカルノードが復旧したことにより、ping の応答が復旧している。

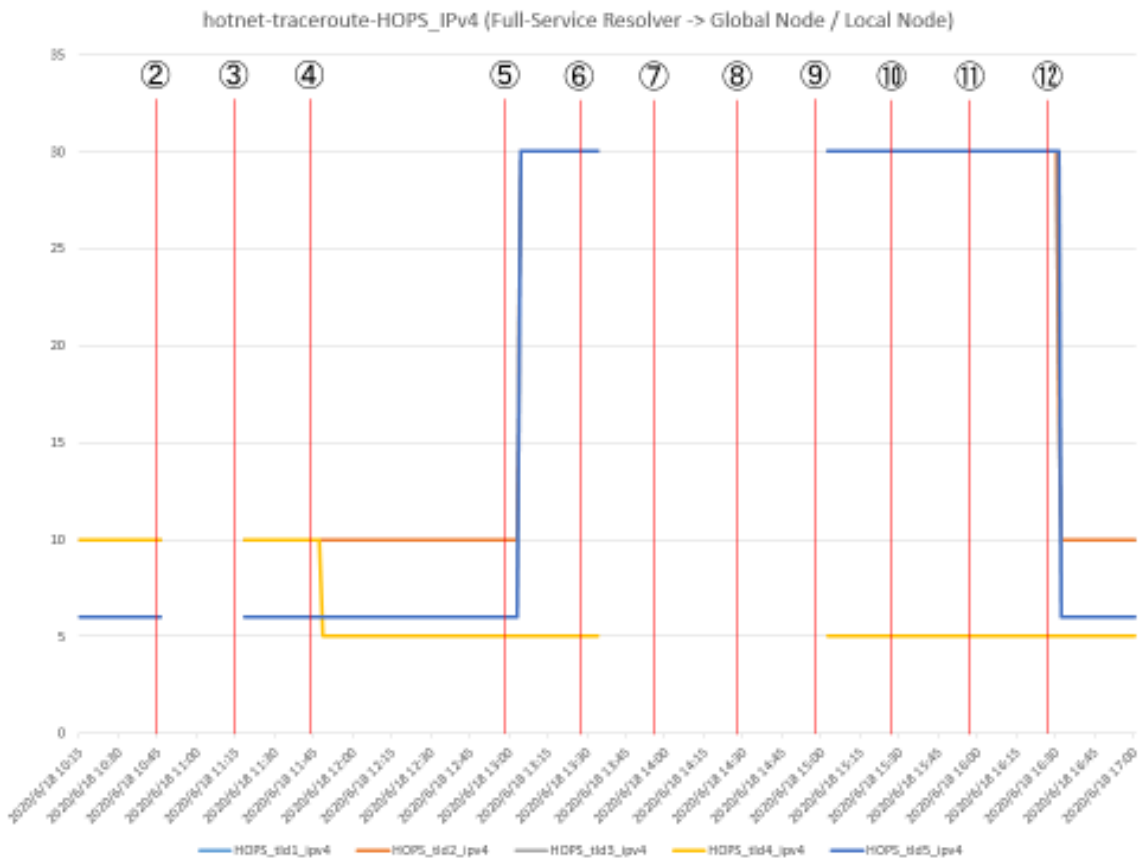


図 6. dig-rtt-v4(フルリゾルバーからグローバルノードへの traceroute による、IPv4 応答の HOPS 値計測)

- グローバルノードがダウンした②で dig の応答が得られなくなっており、③でグローバルノードが復旧したタイミングで復旧している。
- ローカルノードを追加した④で tld4 への HOPS が想定通りに下がっていることが確認できた。
- グローバルノードがダウンした⑤のタイミングでグローバルノードに到達できず、HOPS が跳ね上がることを確認した。
- ⑥から⑨までは HOTnet ローカルノードがダウンしたことにより、dig の応答が得られなくなっている。
- ⑨以降は HOTnet ローカルノードが復旧したことにより、dig の応答が復旧している。

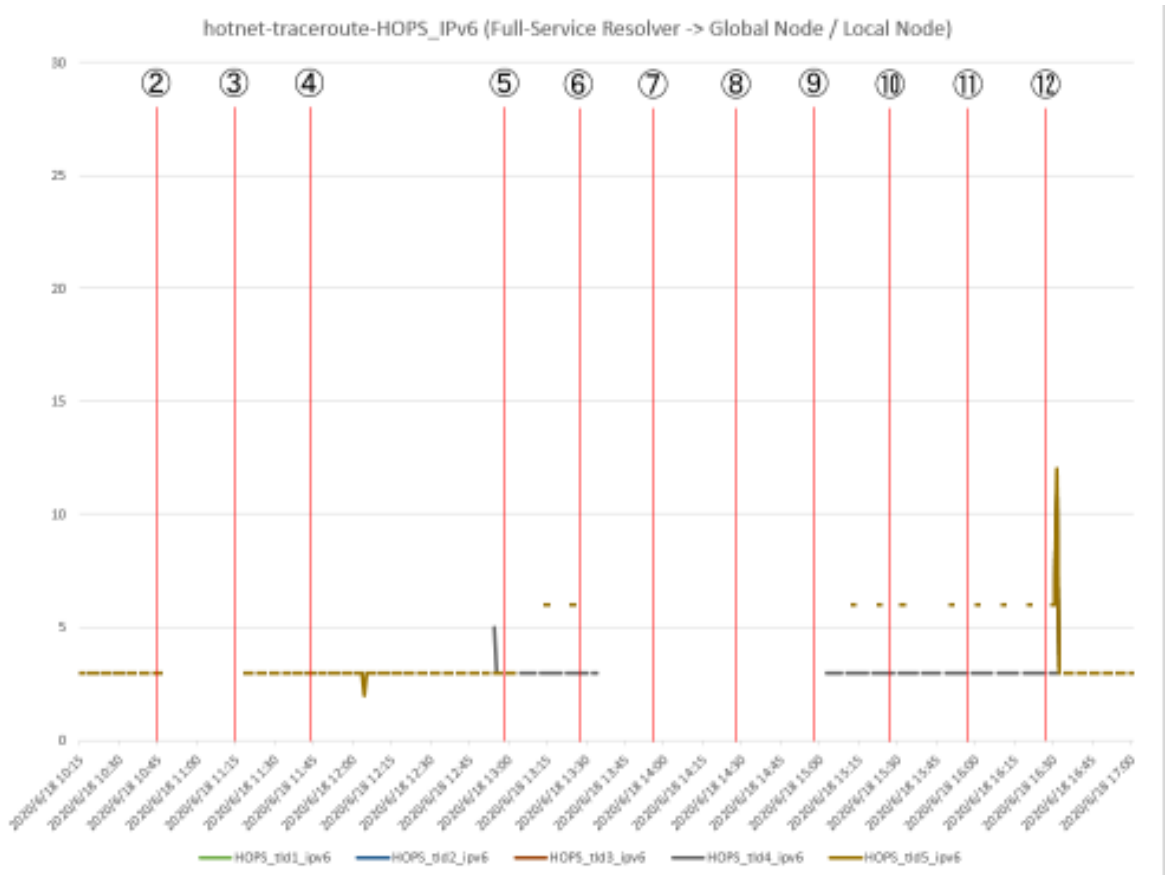


図 7. dig-rtt-v6(フルリゾルバーからグローバルノードへの traceroute による、IPv6 応答の HOPS 値計測)

- グローバルノードがダウンした②で dig の応答が得られなくなっており、③でグローバルノードが復旧したタイミングで復旧している。
- ローカルノードを追加した④で tld4 への HOPS が下がることを想定したが、当社の実験環境要因により IPv6 の traceroute 結果が経路途中で破棄されてしまい、有効なデータの取得ができていなかった為、評価対象としなかった。

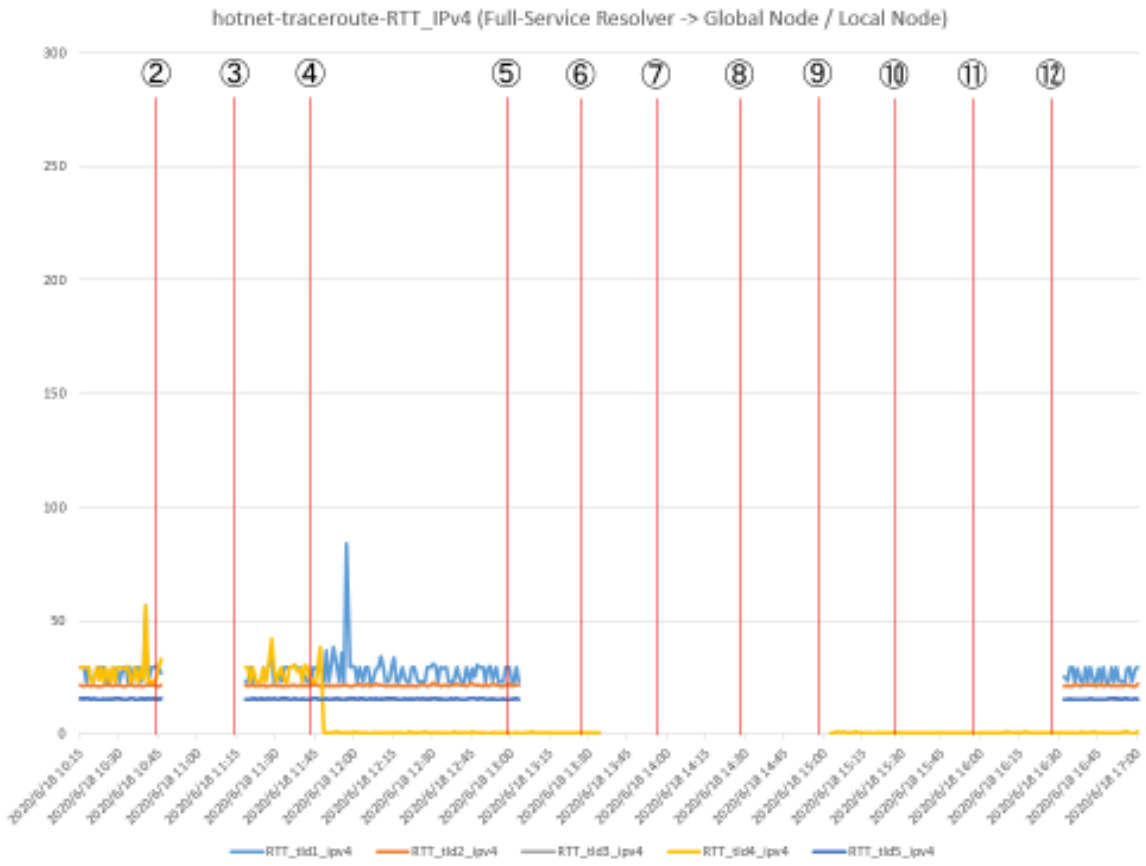


図 8. dig-rtt-v4(フルリゾルバーからグローバルノードへの traceroute による、IPv4 応答の RTT 値計測)

- ④でローカルノードを追加したタイミングで、tld4 への RTT 値が想定通り下がっていることを確認できた。

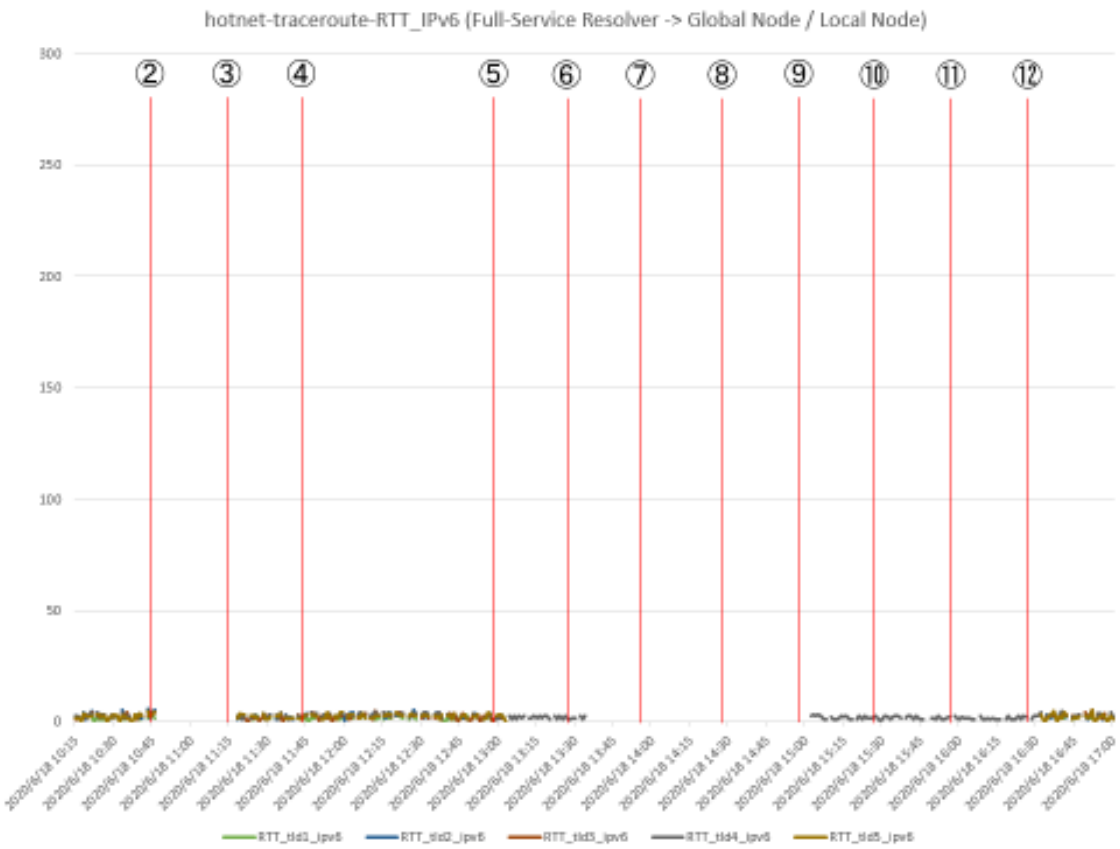


図 9. dig-rtt-6(フルリゾルバーからグローバルノードへの traceroute による、IPv6 応答の RTT 値計測)

- ローカルノードを追加した④で tld4 への RTT 値が下がることを想定したが、当社の実験環境要因により IPv6 の traceroute 結果が経路途中で破棄されてしまい、有効なデータの取得ができていなかった為、評価対象としなかった。

結果および得られた知見

- ローカルノードを設置することでグローバルノードから応答が得られなくなった場合にも、自社 ISP ネットワーク内における名前解決が可能であることを確認した。
- グローバルノードから応答が得られない場合、ローカルノードがダウンすると自社 ISP ネットワーク内は名前解決不可となるが、ローカルノード設置している他社 ISP には期待通り影響が及ばなくなることを確認した。
- 他社ローカルノードがダウンしても自社 ISP ネットワーク内の名前解決は想定通り継続して可能であり、影響が及ばないことを確認した。

- グローバルノードおよびローカルノードのサービスが全停止した状態からローカルノードのみが復旧した場合、グローバルノードが復旧しない状態でも自社 ISP ネットワーク内の名前解決が可能になることを確認した。
- ローカルノードのみが復旧している状態でグローバルノードが復旧した場合、想定通り名前解決のサービスに影響がないことを確認した。
- ローカルノードを参照するユーザーにとっては DNS 応答の RTT 値が小さくなり、応答速度が向上することを確認できた。ローカルノードの設置が、自社 ISP 内顧客の名前解決において、サービス品質向上に寄与することが期待できる。

課題

- ローカルノードの有効性について
  - グローバルノードにおいて障害が発生した際、ローカルノードを参照して名前解決を行う自社 ISP ネットワーク内の顧客に対するサービスが継続されるため、ローカルノードの設置はサービス継続性にとって有効である。ただし、当該ローカルノードは自社 ISP ネットワーク内の顧客からの DNS クエリのみを受け付けることを想定している為、近隣のエリア内のインターネットユーザーはローカルノードによる名前解決を継続できない。
- ローカルノードの実運用を想定した場合の課題事項
  - ローカルノードが停止した際に、経路広報を停止する方法を考慮する必要がある。
  - ゾーン転送が適切にされているかなど、ローカルノードが正常に稼働するために必要な前提条件については本実験のスコープ外となっているため、ローカルノードにおける障害対応を進めるにあたり、別途検討が必要になる。

実験シナリオ b

目的

本実験は、実験シナリオ a で設置したローカルノードを運用している状況を想定し、実際にサイバー攻撃が発生した際に、TLD DNS サーバーオペレーターと ISP オペレーターが攻撃に対し想定シナリオ通りに対処が可能かについて確認することを目的とした訓練である。

本実験では以下の項目を評価対象とし、実際の DDoS 攻撃を模した状況下における有効性について検証した。

- DDoS 攻撃検知システムによる検知および ISP 間の情報連携
- DNS ソフトウェアによる DDoS 攻撃を緩和する機能の有効性検証
- ISP 網内へのローカルノード設置による名前解決の継続性

構成

実験シナリオ a と同物理構成で実施

実験内容

JPRS 準備のシナリオに基づいて実施した。

実験結果

DDoS 攻撃検知システムによる検知および ISP 間の情報連携

- JPRS 構築の攻撃検知システムを参照することで、想定通り攻撃元 IP アドレスの識別および、攻撃を受けている時間帯が可視化されることを確認できた。
  - クエリログより送信元 IP アドレスが確認でき、それを可視化することで状況の理解が短時間のうちに可能であった。
- TLD DNS サーバーの応答確認と合わせトラフィック量をグラフで確認でき、状況把握が容易になった。
- DNS オペレーターの習熟度に関わらず、状況の把握が容易になった。
- メールと Slack は速やかな情報共有をする上で十分に機能することを確認できた。
  - メールは既存のフローで利用可能であるため、業務実装の実現性が高い。

- Slack を使用すると双方向の情報共有が容易である点に、利便性の高さを感じられた。

- JPRS シナリオにおける DNS の障害発生時に、コミュニケーションツールとして Slack を用いることで、事業者間の円滑な情報共有を行えることを確認できた。

DNS ソフトウェアによる DDoS 攻撃を緩和する機能の有効性検証

- 自社網内から TLD DNS サーバーに対するランダムサブドメイン攻撃に際し、”攻撃クエリを絞り込む”という期待した効果が得られることを確認できた。

ISP 網内へのローカルノード設置による名前解決の継続性

- DNS の名前解決の継続性について、想定通りグローバルノードがダウンした場合も設置したローカルノードによって名前解決が可能であることを確認し、JPRS と双方向のコミュニケーションをとりながらサービス復旧までの一連の流れについて、訓練することができた。

得られた知見

- 攻撃検知システムでの検知および JPRS からの情報共有により、DNS に対する攻撃が開始された時点で攻撃を受けている可能性がある状況を、いち早く知ることができる。
  - 本実験で用いたコミュニケーションツールである Slack を併用することで、双方向の迅速な情報共有を実現できる。
- ローカルノードの設置によって DNS 名前解決のサービス冗長性が向上しただけでなく、DDoS 対策をフルリゾルバーに設定することで、自社 ISP ネットワーク内に攻撃者が存在する場合も、攻撃の影響を緩和することが可能になると考えられる。

課題

- 実運用を想定した場合、ローカルノードの状態確認手順、操作手順について運用部門のメンバーが対処可能な資料およびフローを作成する必要がある。
  - 迅速な対応を実現するためには資料および手順書を作成した後も、定期的な模擬訓練が必要である。
- 連絡手段について、あらかじめ体制の構築と訓練を実施しておく必要がある。
  - 休日、夜間帯などどのような方法で連絡するか、自社の既存の連絡手段である電話連絡やメール連絡の場合についても、連絡フローを改めて定める必要がある。

  - 本実験で活用した Slack は双方向の情報共有において有用であったが、自社の実運用へ適用するためには、社内ルールの検討などの手順・時間を要する。
- 今回採用した DDoS 攻撃対策は攻撃クエリ以外に、通常クエリに対しても制限が加わる。その為、自社顧客の名前解決において一定の影響を及ぼすと考えられることから、実運用への適用は慎重に検討する必要がある。

全体を通した所感

- 本実験では JPRS が準備したシナリオに基づいて実験を実施した。実験に対して課題が出た際には実験の参加者同士で意見を出し合いながら、あるいは状況を共有しながら、問題を解決するという場面がいくつかあった。
  - インターネットという様々な組織が関わる環境でサービスを維持するという観点では、自社のサービス向上にとどまらず、他社との双方向のコミュニケーションを実施可能な、今回のような機会も貴重であると思われた。
- こうした実験に参加することで DNS の技術に対する理解度が深まる、オペレーターの訓練につながるといった、副次的な効果も期待できる。

実証実験報告（株式会社オプテージ）

実験シナリオ a

目的

近年、大規模なイベントの開催時期を狙ったサイバー攻撃が増加している。TLD DNS サーバーなどの重要な DNS サーバーを標的とした DDoS 攻撃が発生することで DNS サービスが停止すると、インターネット上のさまざまなサービスに対して甚大な被害をもたらすことが想定される。

本実験では、TLD DNS サーバーが攻撃により応答不可となる状況を再現し、ISP 網内にローカルノードを設置することで名前解決が継続して可能であることを確認する。

構成

本実験を実施するにあたり、OPTAGE は以下の環境を構築した。

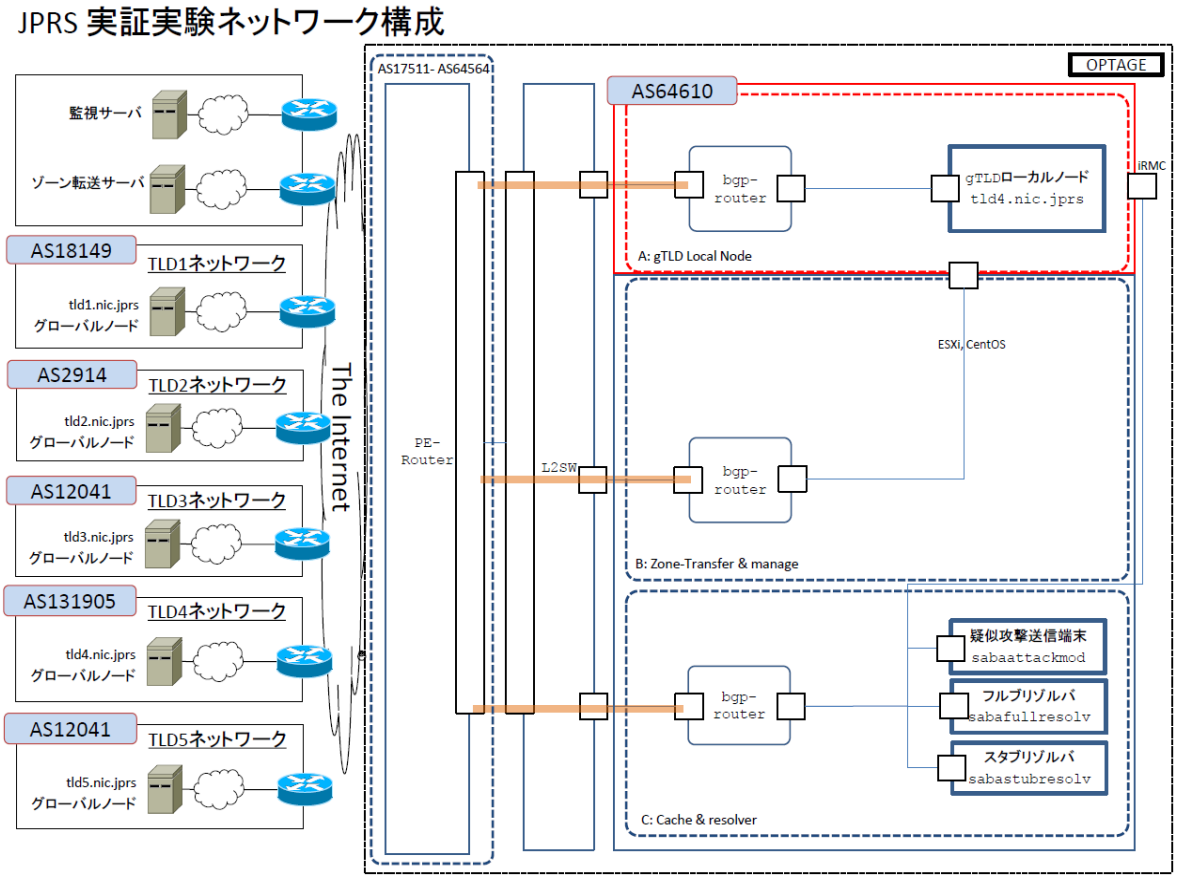


図: JPRS 実証実験ネットワーク構成

実験内容

2.1.3 のシナリオに基づいて実施した。 ※BGP operationは実験環境の都合上、JPRS 側で実施した。

実験結果

dig/ping/traceroute コマンドによる RTT/STATUS/HOP 数計測結果
(ping/traceroute は IPv4/IPv6 でそれぞれ実施)

グラフ中の各フェーズ番号の説明

①初期状態(ローカルノード稼働前)

②グローバルノードへの攻撃開始

③グローバルノードへの攻撃収束

④ローカルノード(#1,#2,#3)稼働開始

⑤グローバルノードへの攻撃開始

⑥ローカルノード#1(HOTnet)への攻撃開始

⑦ローカルノード#2(OPTAGE)への攻撃開始

⑧ローカルノード#3(QTnet)への攻撃開始

⑨ローカルノード#1(HOTnet)への攻撃収束

⑩ローカルノード#2(OPTAGE)への攻撃収束

⑪ローカルノード#3(QTnet)への攻撃収束

⑫グローバルノードへの攻撃収束

※OPTAGE のみ他社 ISP とは別日に再実験を実施した際の結果であるため、フェーズ②～④の時刻が他社の結果と比べ、15 分程度前にずれている

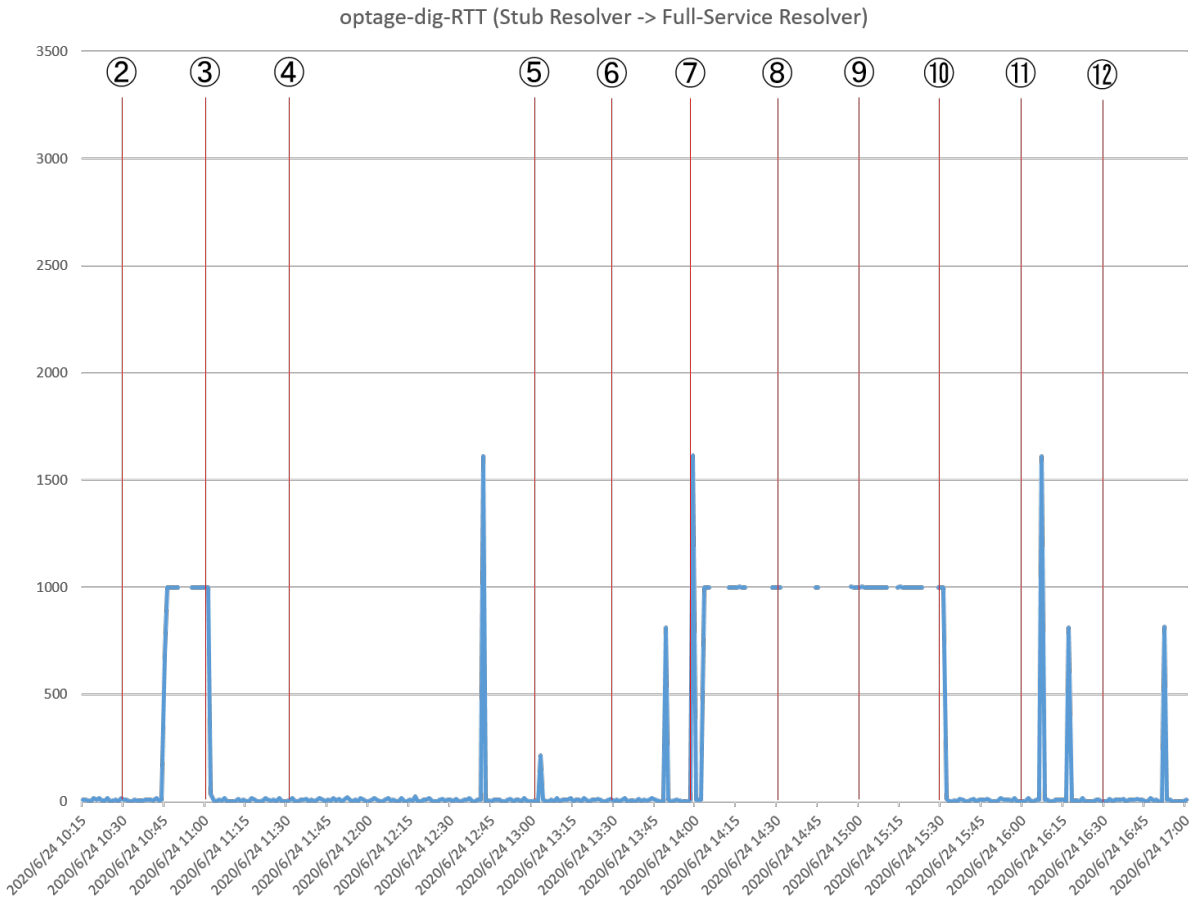


図: dig-RTT(スタブリゾルバー->フルリゾルバーへの dig RTT 値)

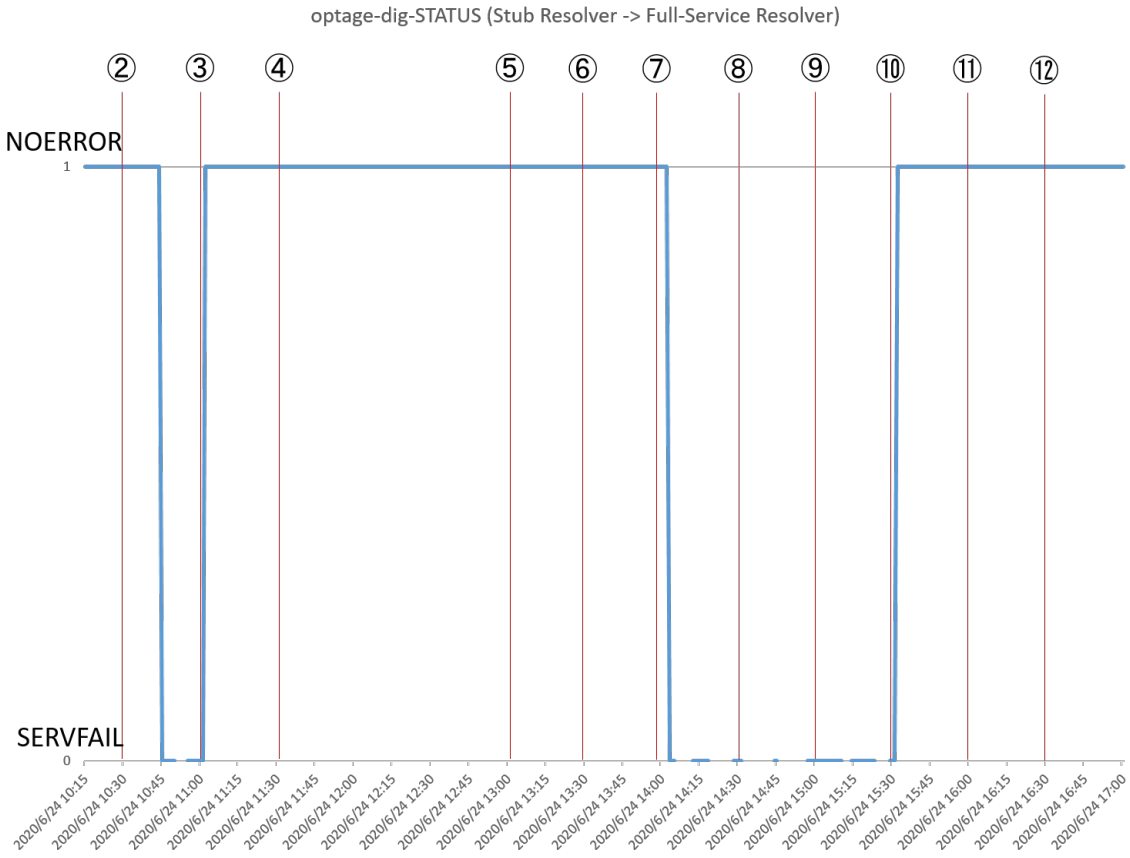


図: dig-STATUS(スタブリゾルバー->フルリゾルバーへの dig STATUS)

- フェーズ②のパケットロス設定投入後も NOERROR で dig 応答有となっていたが、フルリゾルバーのキャッシュクリアを実施したタイミングで想定通り SERVFAIL となり、フェーズ③でグローバルノードが復旧したタイミングで NOERROR となった。
- フェーズ⑦から⑩の間は継続的に名前解決ができていないことが読み取れる。2 種類の状態の詳細…応答なし:(タイムアウト) / RTT 1000ms:SERVFAIL
- フェーズ⑩以降はローカルノード#2 が復旧したことによって NOERROR となり、以降は名前解決ができる状態となった。

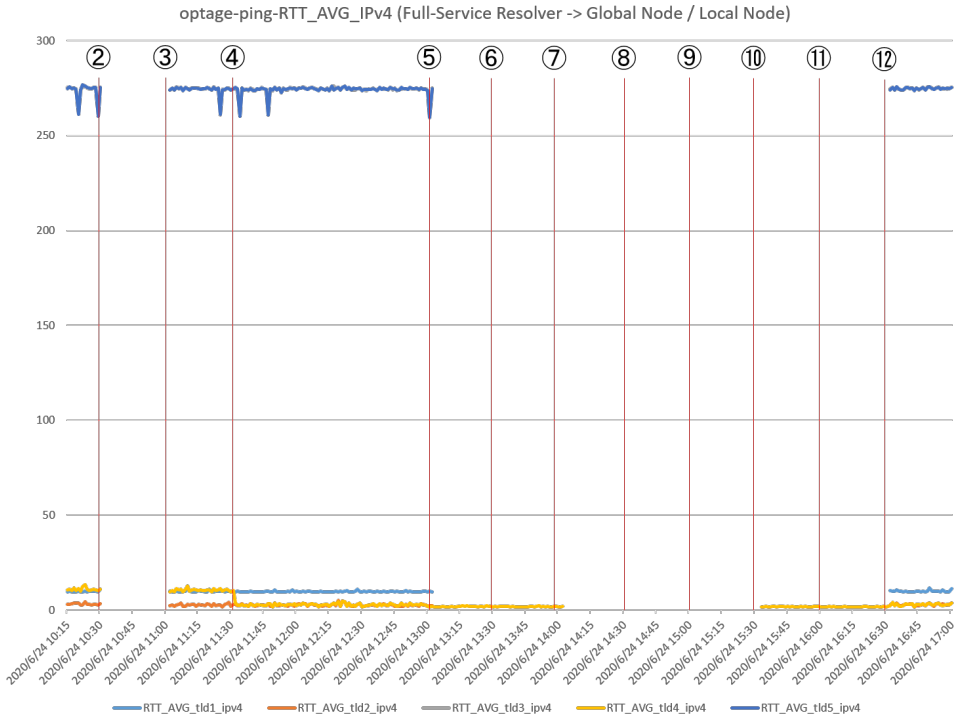


図: ping-RTT-IPv4(フルリゾルバー->グローバルノードへの ping(IPv4)RTT 平均値)

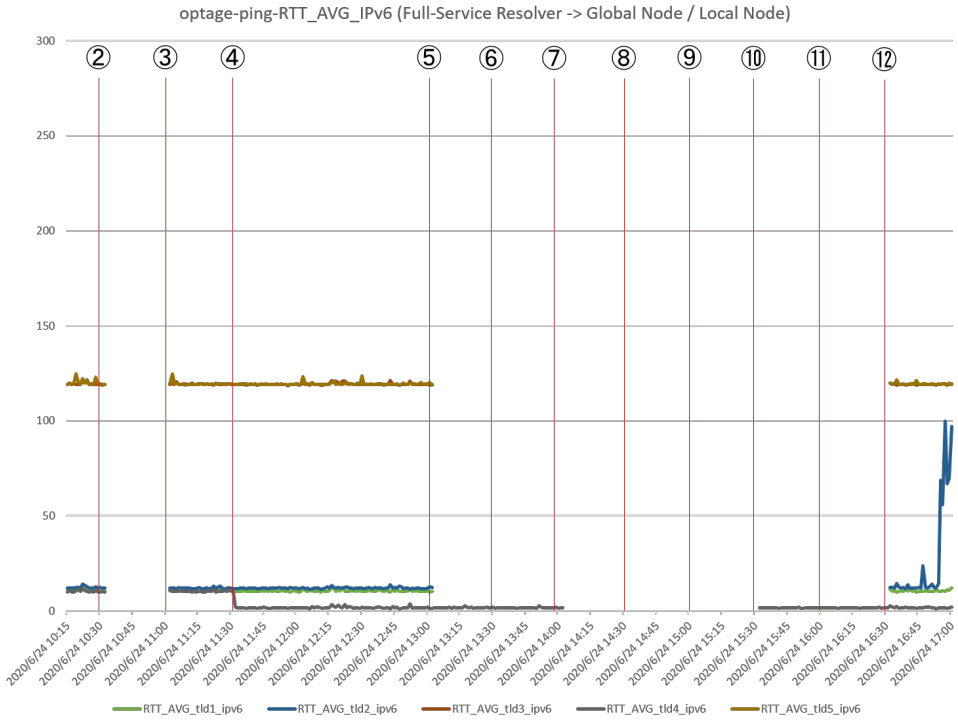


図: ping-RTT-IPv6(フルリゾルバー->グローバルノードへの ping(IPv6)RTT 平均値)

- フェーズ④(ローカルノード稼働開始)のタイミングで IPv4/IPv6 共に tld4 への RTT 値が、想定通り下がっていることを確認できた。

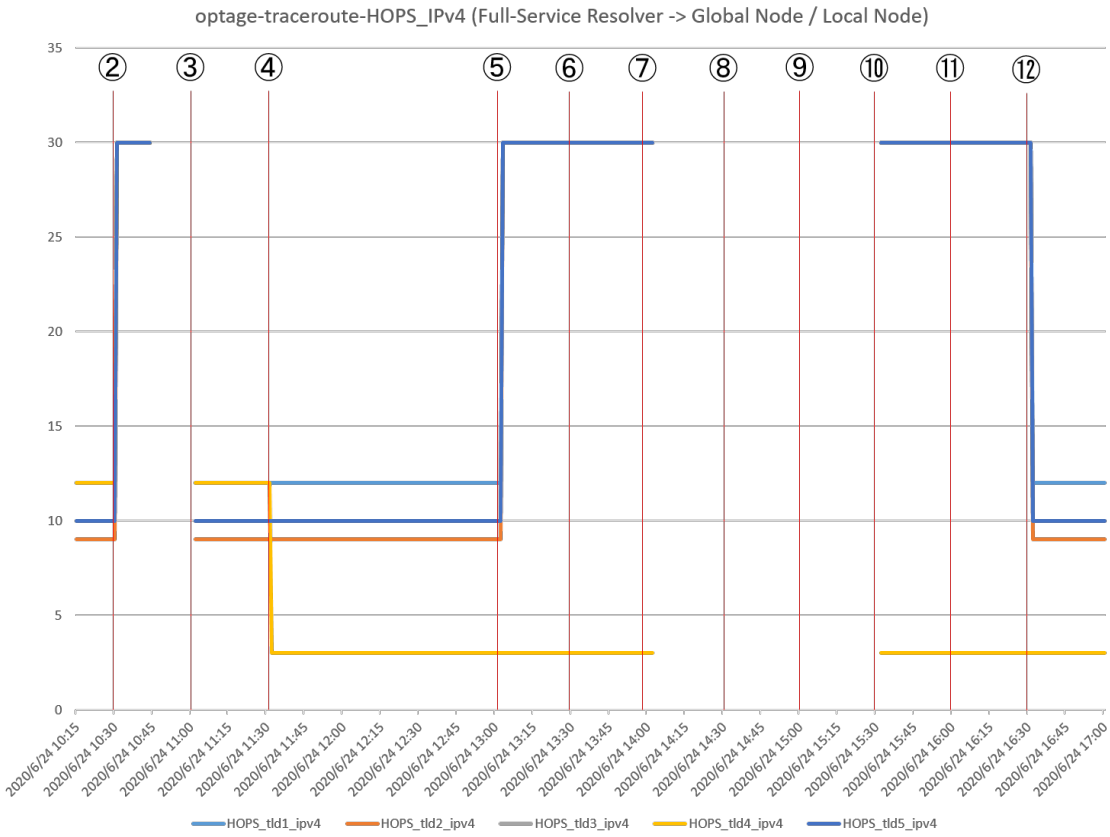


図: traceroute-HOPS-IPv4(フルリゾルバー->グローバルノードへの traceroute(IPv4)HOP 数)

- グローバルノードがダウンしたフェーズ②および⑤のタイミングでグローバルノードへの到達性がなくなり、HOP 数が増加していることが確認できた。
- フェーズ④(ローカルノード稼働開始)のタイミングで tld4 への HOP 数が、想定通りに下がっていることが確認できた。

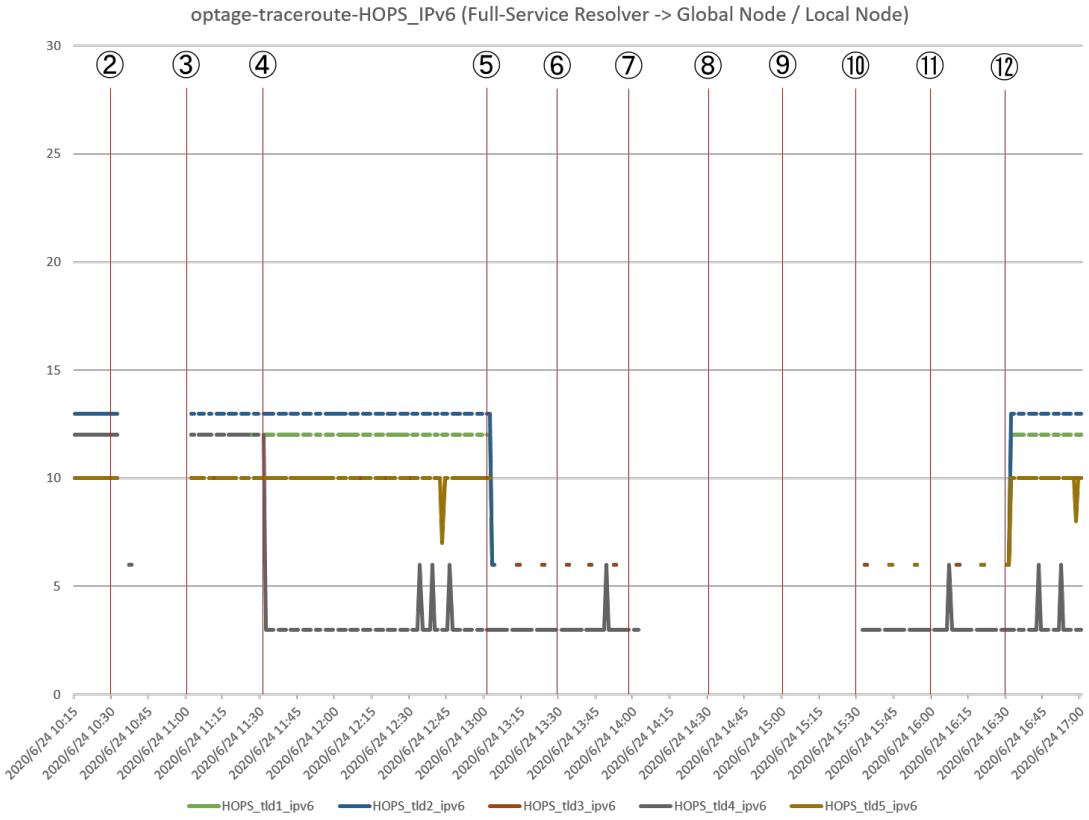


図: traceroute-HOPS-IPv6(フルリゾルバー->グローバルノードへの traceroute(IPv6)HOP 数)

- フェーズ④(ローカルノード稼働開始)のタイミングで tld4 への HOP 数が下がることを想定したが、実験環境設定不備のため、IPv6 の traceroute が経路途中でタイムアウトとなった。
- グラフの傾向の読み取りやすさを優先し、原データからタイムアウト値を除いたもので結果を分析したところ、HOP 数が想定通りに下がっていることが確認できた。

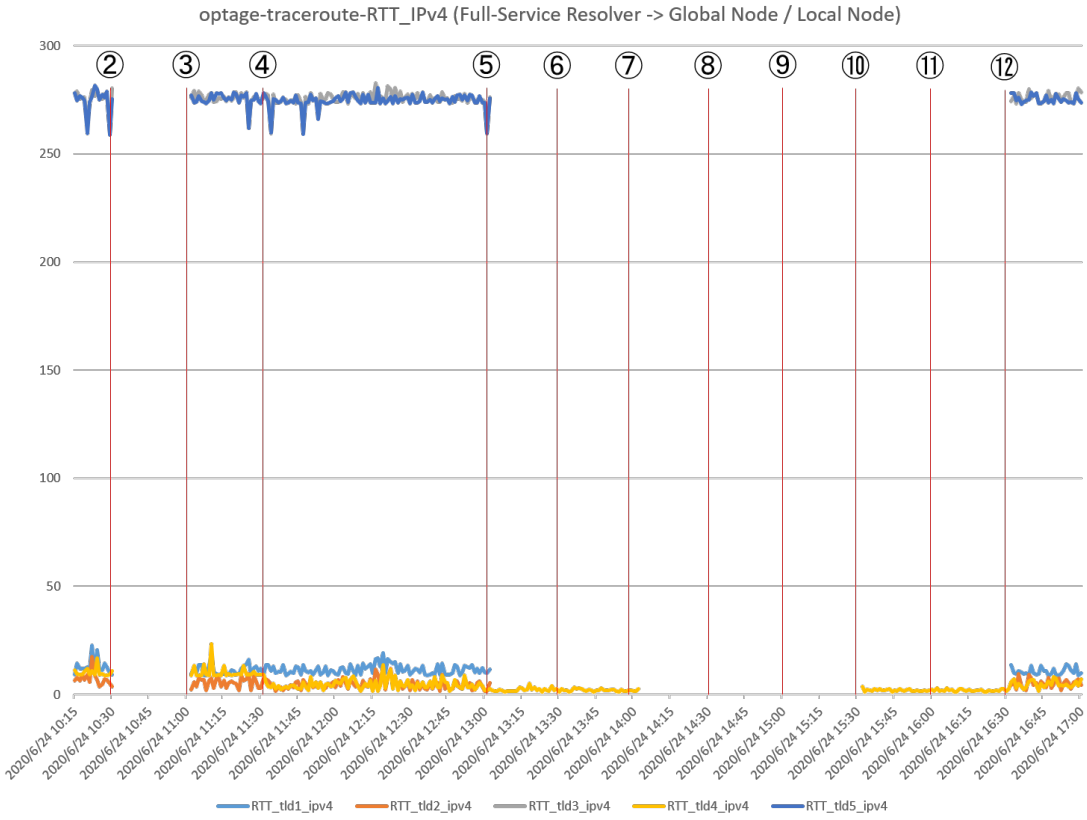


図: traceroute-RTT-IPv4(フルリゾルバー->グローバルノードへの traceroute(IPv4)RTT 値)

- グローバルノードがダウンしたフェーズ②および⑤のタイミングで、グローバルノードに到達できなくなっていることが確認できた。
- フェーズ④(ローカルノード稼働開始)のタイミングで、tld4 への RTT 値が想定通りに下がっていることが確認できた。

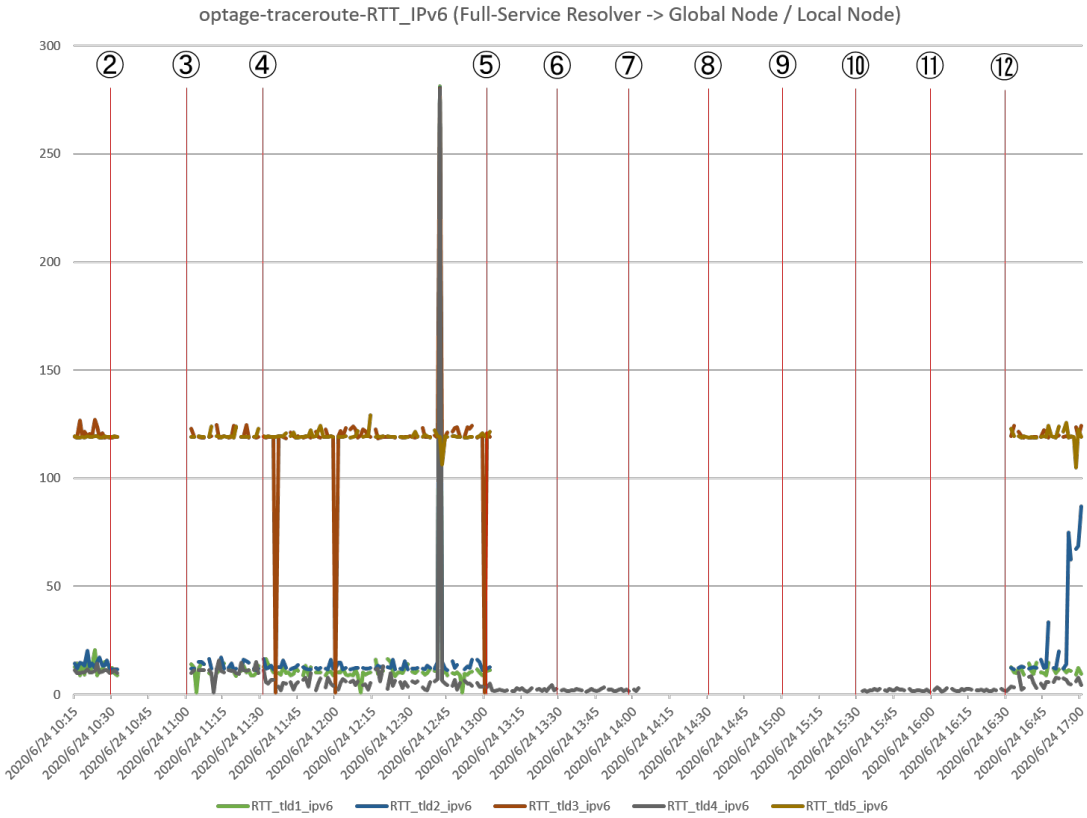


図: traceroute-RTT-IPv6(フルリゾルバー->グローバルノードへの traceroute(IPv6)RTT 値)

- フェーズ④(ローカルノード稼働開始)のタイミングで tld4 への RTT 値が下がることを想定したが、実験環境設定不備のため、IPv6 の traceroute が経路途中でタイムアウトとなった。
- グラフの傾向の読み取りやすさを優先し、原データからタイムアウト値を除いたもので結果を分析したところ、RTT 値が僅かではあるが想定通りに下がっていることが確認できた。
- .jprs TLD の名前解決の継続性が確保されたか グローバルノードが名前解決不可となった後も、ローカルノードで名前解決の継続性が確保された。

得られた知見

- ローカルノードが未設置の場合にグローバルノードがダウンすると、名前解決が不可能になること
- ローカルノードを設置した場合にグローバルノードがダウンしても、継続して名前解決が可能であること
- グローバルノードが復旧した際にローカルノードの情報を保持し続けることを避けるため、フルリゾルバーのキャッシュクリアをする必要があること
- グローバルノードおよびローカルノードがダウンすると、名前解決が不可能になること
- ローカルノードが有効なケース、有効でないケースについて
    - 有効なケース:今回のシナリオのように、グローバルノードでの名前解決不可となった場合
    - 有効でないケース:ISP において、外部接続用機器に障害が発生した場合

課題

- ローカルノードの実運用を想定した場合の課題
    - 障害を検知した際、JPRS->OPTAGE 監視部門へ通知するフローの整備が必要である
    - 定期メンテナンスや物理的な障害など、ローカルノードの物理作業が必要になった場合の対応フローの整備が必要である
    - ゾーン転送ができなくなった場合の対処方法について、整備が必要である
    - ローカルノードの機能が停止した場合、BGP の経路広告を停止する仕組み(できれば自動化したい)を検討する必要がある

実験シナリオ b

目的

実験シナリオ a のシナリオを想定し、攻撃が発生した際に TLD DNS オペレーターと ISP オペレーターがシナリオ通りに対処することが可能かどうかを確認するための訓練を実施する。

訓練にあたり、攻撃検知システム・Slack による情報共有の行いやすさを評価し、ローカルノードを設置した実運用を想定した場合に考えられる課題を確認する。

構成

実験シナリオ a と同様の構成で実施した。

実験内容

実験シナリオ b 実験シナリオに基づき実施した。

実験結果

全シナリオにおいて、想定通り名前解決を継続して行うことができた。また、今回は ISP 側から DDoS 攻撃を模擬したトラフィックを発生させたが、攻撃開始から検知まで素早く、速やかに対処できた。

得られた知見

- チャットツール(今回は Slack を利用)による各社との情報共有が迅速かつ容易であることが確認できた。
- 攻撃が発生して TLD DNS サーバーがダウンした場合でも、ローカルノードを設置することにより継続して名前解決が可能となり、サービスの冗長性が高まることが確認できた。

課題

- 実運用を想定した場合、チャットツールでの攻撃検知の通知に即時に反応できないケースがあり得るため、当社内部の監視システムと連動するような仕組みを構築する必要がある。
- 運用部門に対するローカルノードにおける操作手順の説明や模擬訓練の実施など、運用開始に先立ち、ある程度の期間を確保して運用体制を整備する必要がある。

- 本実験で検証した攻撃対策は通常の顧客の DNS クエリにも影響するため、有事の際に関係するカスタマーサポートの担当部署等と、対応可否の判断基準について綿密に調整を行う必要がある。

所感

日頃の業務では他者から意見をもらったとしても社内の観点に限ったものであったが、本実験では他社 ISP の方の観点での意見を聞くことができ、非常に有意義であった。また、DNS 担当となってまだ日が浅い頃から実験に参加させていただいたため、ネットワークや DNS サーバーを一から構築し、攻撃へ対処するための DNS の機能を検証することで大変貴重な経験となった。

本実験で得られた知識により、DNS オペレーターとしてさらなる技術力の向上が期待できると感じた。

実証実験報告（株式会社 QTnet）

実験シナリオ a

目的

東京 2020 オリンピック・パラリンピックでは過去の大会と同様、関連サイトやネットワークなどを標的とした、様々なサイバー攻撃の発生が予測されている。開催を控え、インターネットサービスの利用・提供に必要不可欠な DNS に関しても各種攻撃に対し、備える必要がある。

そのため、本実験ではグローバルノードが攻撃により応答不能となった際においても、ISP 内にローカルノードを設置することで名前解決が継続可能であるかの評価を実施する。また、ローカルノードを設置した際のネットワークの遅延についての評価も実施する。

グローバルノード：インターネット全体に対しサービスを提供するノード ローカルノード：設置した ISP のみにサービスを提供するノード

構成

本実験に際し構築した環境の全体構成を、図 1 に示す。

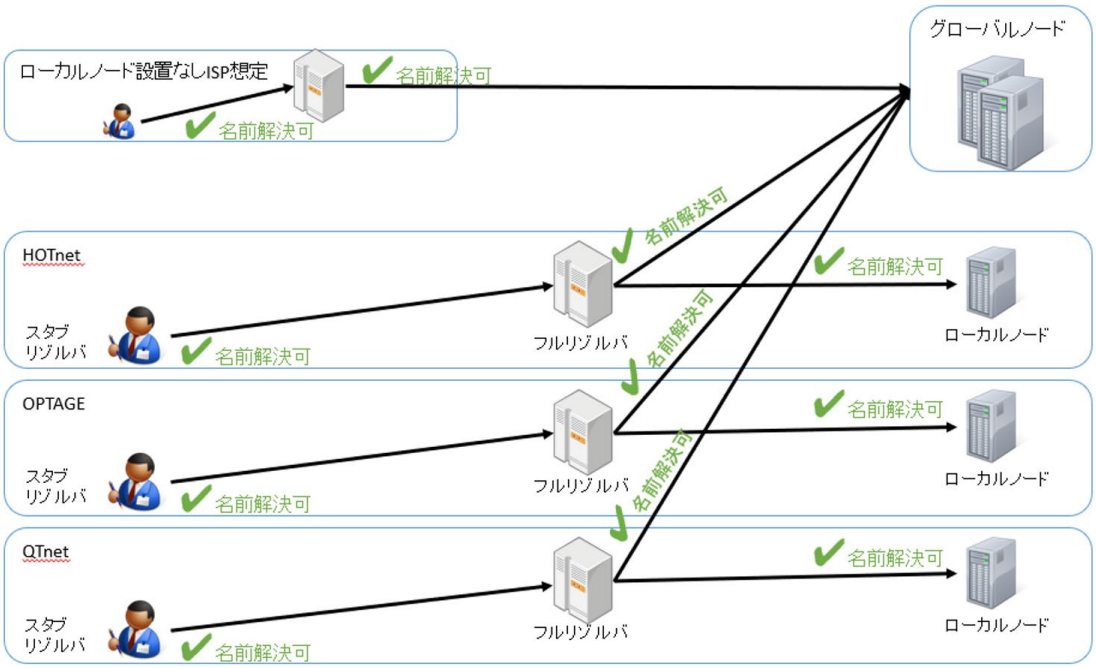


図 1. 実験環境の全体構成図

実験内容

「2.1.3 のシナリオ」に基づき、評価実験を実施した。

本実験では、ISP 内にローカルノードを設置した環境下において以下の条件を模擬し、名前解決の可否、及びネットワーク遅延の観点から評価を実施した。

・DDoS 攻撃により、グローバルノードが応答不能な状態

・ISP 内部からの攻撃により、ローカルノードが応答不能な状態

評価 I ISP の顧客を想定した、スタブリゾルバーからの名前解決の可否

評価 II フルリゾルバーとグローバルノード/ローカルノードの間のネットワーク遅延

実験シナリオ

①初期状態 (平常時)

②グローバルノードへの攻撃が発生し、全てのグローバルノードがダウン

③グローバルノードへの攻撃が収束し、全てのグローバルノードが復旧

④全ローカルノード稼働開始（HOTnet, OPTAGE, QTnet）

⑤グローバルノードへの攻撃が発生し、全てのグローバルノードがダウン

⑥ローカルノード#1 への攻撃が発生し、HOTnet ローカルノードがダウン

⑦ローカルノード#2 への攻撃が発生し、OPTAGE ローカルノードがダウン

⑧ローカルノード#3 への攻撃が発生し、QTnet ローカルノードがダウン

⑨ローカルノード#1 への攻撃が収束し、HOTnet ローカルノードが復旧

⑩ローカルノード#2 への攻撃が収束し、OPTAGE ローカルノードが復旧

⑪ローカルノード#3 への攻撃が収束し、QTnet ローカルノードが復旧

⑫グローバルノードへの攻撃が収束し、全てのグローバルノードが復旧

各項番のグローバルノード及びローカルノードの稼働状況を示す(表 1)。

表 1. グローバルノード/ローカルノード稼働状況

	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫
グローバルノード稼働状態	○	×	○	○	×	×	×	×	×	×	×	○
HOTnet ローカルノード稼働状態	×	×	×	○	○	×	×	×	○	○	○	○
OPTAGE ローカルノード稼働状態	×	×	×	○	○	○	×	×	×	○	○	○
QTnet ローカルノード稼働状態	×	×	×	○	○	○	○	×	×	×	○	○

実験結果

本実験では、スタブリゾルバーからの名前解決の可否と、ネットワーク遅延の測定を実施した。

評価 I 結果 ISP の顧客を想定した、スタブリゾルバーからの名前解決の可否

表 2. 名前解決の可否

	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪	⑫
想定結果	○	×	○	○	○	○	○	×	○	○	○	○
実験結果	○	×	○	○	○	○	○	×	○	○	○	○

評価 II 結果 フルリゾルバーからグローバルノード/ローカルノードへのネットワーク遅延(ms)

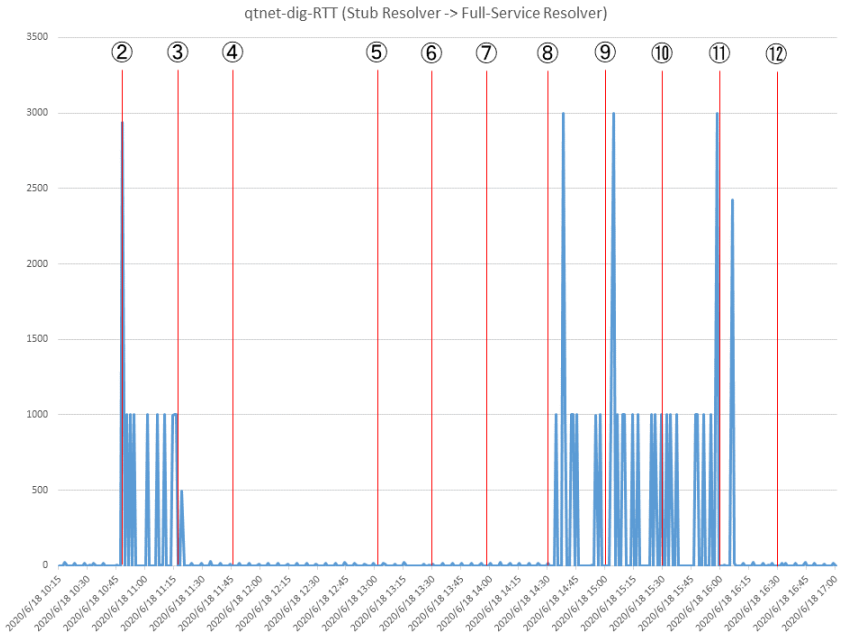


図 2. dig-rtt(スタブリゾルバーからフルリゾルバーへの dig による RTT 値の計測)

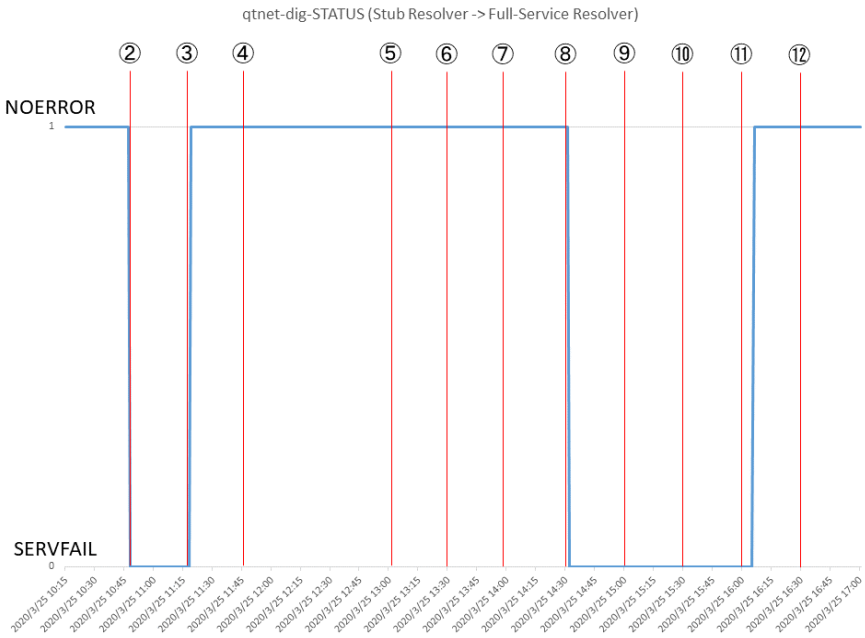


図 3. dig-status(スタブリゾルバーからフルリゾルバーへの dig による応答 STATUS の計測)

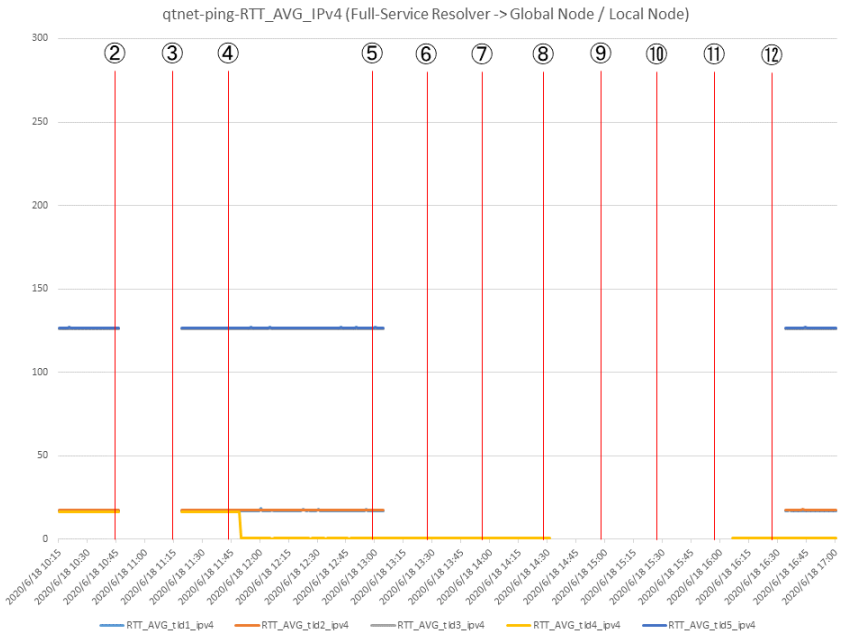


図 4. ping-rtt-v4(フルリゾルバーからグローバルノードへの IPv4 による ping 応答の RTT 値の計測)

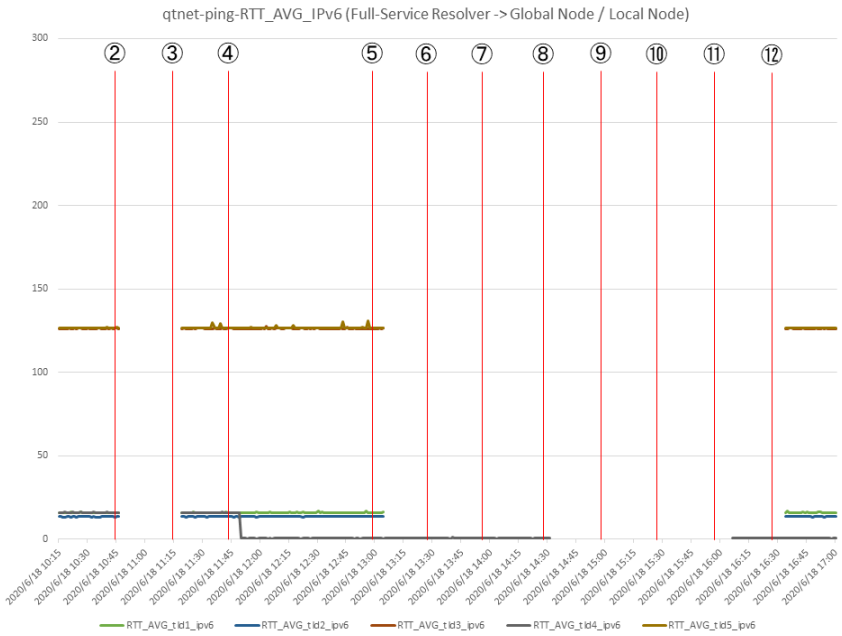


図 5. ping-rtt-v6(フルリゾルバーからグローバルノードへの IPv6 による ping 応答の RTT 値の計測)

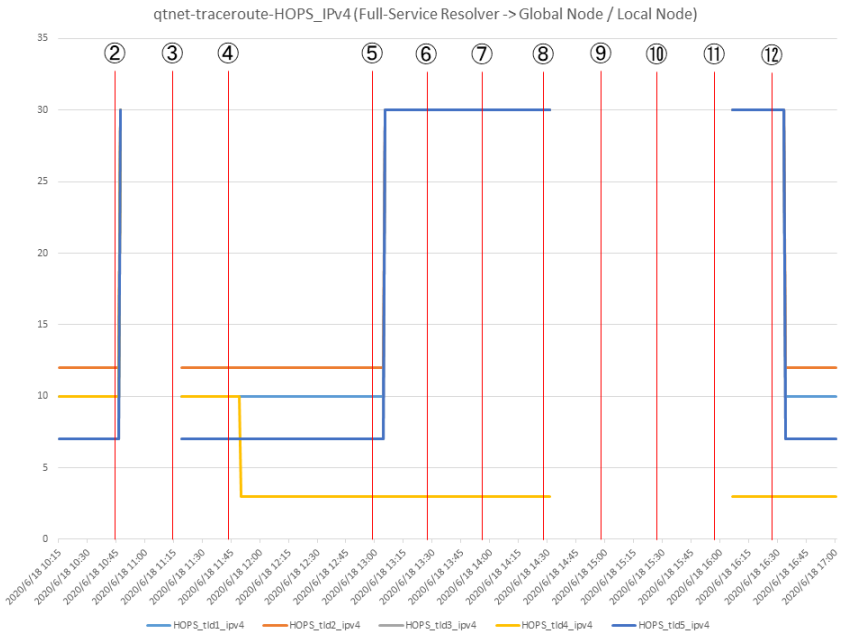


図 6. dig-rtt-v4(フルリゾルバーからグローバルノードへの IPv4 による traceroute 応答の HOPS 値の計測)

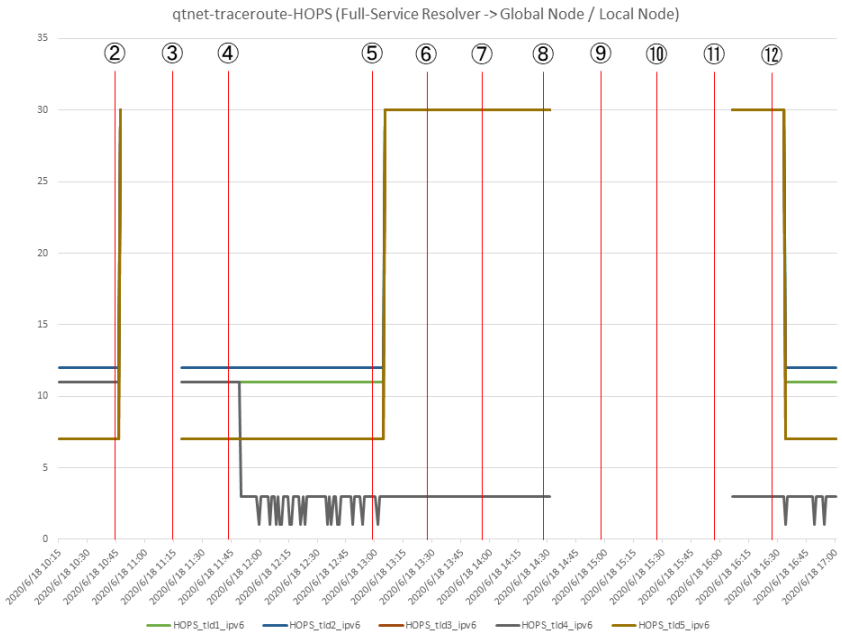


図 7. dig-rtt-v6(フルリゾルバーからグローバルノードへの IPv4 による traceroute 応答の HOPS 値の計測)

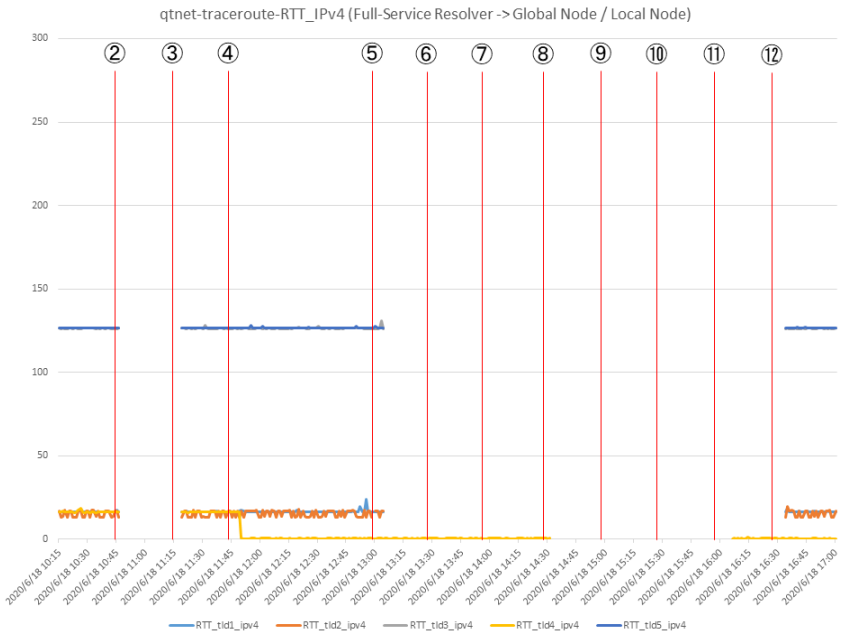


図 8. dig-rtt-v4(フルリゾルバーからグローバルノードへの IPv4 による traceroute 応答の RTT 値の計測)

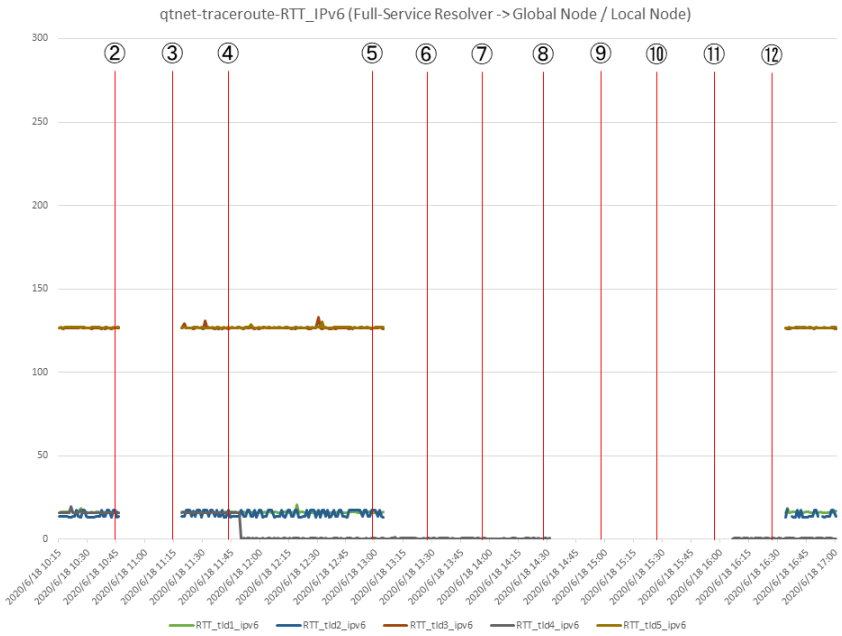


図 9. dig-rtt-6(フルリゾルバーからグローバルノードへの IPv6 による traceroute 応答の RTT 値の計測)

結果の評価

評価 I ISP の顧客を想定したスタブリゾルバーからの名前解決の可否

ISP 内にローカルノードを設置することで、DDoS 攻撃により全グローバルノードが応答を返せない状況下においても、名前解決が継続可能であることを確認できた(表 2)。

評価 II フルリゾルバーからグローバルノード/ローカルノードへのネットワーク遅延

フルリゾルバーからグローバルノードへの通信における遅延は約 20ms であり、ローカルノードへの通信における遅延は 0.5ms であった(図 4)。この結果から、ISP 内にローカルノードを設置することで、平常時においても名前解決が低遅延で行える結果が得られた。

実験シナリオ b

目的

本テーマでは、ローカルノードを設置した環境下において実際に DDoS 攻撃が発生した際の状況を模擬し、組織間の連携を図る訓練を実施した。

構成

実験シナリオ a と同様の構成で実施した。また、DDoS 攻撃を模擬したトラフィックは ISP 内の利用者を想定した端末から送出した。

連携訓練内容

「ランダムサブドメイン攻撃の検知と ISP との連携・対処の訓練シナリオ」に基づいて実施した。

本実験では、ローカルノードを設置した環境下において実際に DDoS 攻撃が発生した際の状況を模擬し、組織間の連携を図る訓練を実施した。 *評価* チャットツールを用いた情報連携

シナリオ概要

① 訓練開始

② 攻撃発生

③ 攻撃検知と連携(ISP への通知)

④ グローバルノードダウンの検知

⑤ グローバルノードダウンに伴う連携(ISP への通知)

⑥ 状況確認

⑦ グローバルノード復旧

⑧ 訓練終了準備

⑨ 訓練終了

結果

評価 チャットツールを用いた情報連携

ランダムサブドメイン攻撃を攻撃検知システムにおいて検知でき、チャットツール(Slack)を用いることで、攻撃の発生状況を迅速に情報共有できた(図 10)。

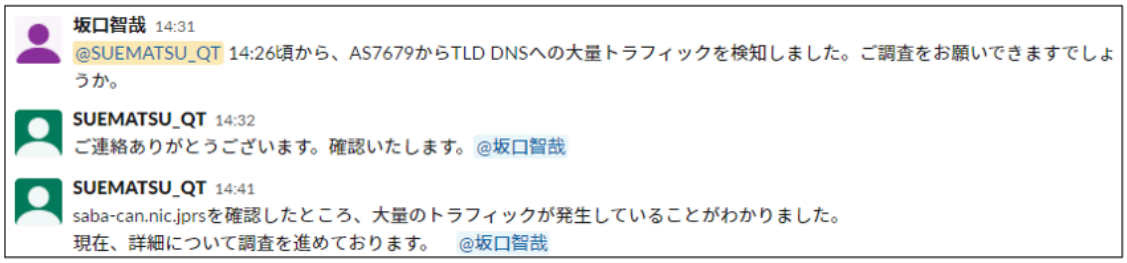


図 10. チャットツールによる情報連携の様子

その他

チャットツールを用いることで、組織間において情報を正確かつ円滑に連携でき、シナリオ実行時における軽微な問題を解決できた。

総括

本研究に関するまとめ

本研究における実証実験は、前回研究により大規模災害によるインターネットの物理的な分断に対し有効であると判明したローカルノードの配置が、サイバー攻撃による論理的な分断においても名前解決サービスの継続に有効であるかの検証を目的とし、ISP3 社と JPRS が共同で実施した。実験では、以下の 2 つの攻撃シナリオ（実験シナリオ a・実験シナリオ b）を作成し、ローカルノード設置の効果を確認するとともに、攻撃発生時の検知・対処までの運用手順の妥当性を検証した。

- 実験シナリオ a ローカルノード設置の効果を確認するシナリオ
- 実験シナリオ b ローカルノード設置後に攻撃の発生から検知・対処までの運用を訓練するシナリオ

実験シナリオ a では、ローカルノードを設置した ISP の外部で TLD の権威 DNS サーバーを標的とした DDoS 攻撃が実行された場合、当該 ISP は攻撃の影響を受けず、名前解決サービスが継続できていることを検証した。また、ローカルノードを設置した ISP の内部で TLD の権威 DNS サーバーを標的とした DDoS 攻撃が実行された場合、ローカルノードにより攻撃トラフィックが隔離され、当該 ISP の外部に送られなくなることでグローバルノードが保護され、TLD の権威 DNS サーバー全体における名前解決サービスの継続性を高められることも確認した。

実験シナリオ b では、TLD の権威 DNS サーバーを標的とした DDoS 攻撃が発生したことを想定し、当該 TLD の権威 DNS サーバーのオペレーターによる攻撃の検知、ローカルノードを設置した ISP への連絡、オペレーター間の相互連携による攻撃への対処という一連の対応訓練を実施した。本実験により、全体を把握できる当該 TLD の権威 DNS サーバーのオペレーターが DDoS 攻撃の状況を把握し、対処に必要な情報を ISP に連絡・相互連携することが、攻撃対処の初動における調査活動に対して有用であることを確認した。

以上の実証実験の結果、大規模災害によるインターネットの物理的な分断に対し有効であった TLD の権威 DNS サーバーのローカルノードの配置が、サイバー攻撃による論理的な分断においても名前解決サービスの継続に有効であることが確認できた。今後、本実証実験により得られた結果・知見を JP DNS サーバーに適用することで、JP ドメイン名の名前解決の安定性を向上させるための具体的な実装・運用の方法について検討を進める予定である。

ローカルノードの設置地域・設置数に関する考察

ここでは、前回研究並びに本研究における実証実験の成果を踏まえた、大規模災害とサイバー攻撃の双方を想定したわが国におけるローカルノードの効果的な設置箇所に関する考察をまとめる。

わが国の ISP 間における相互接続の構成を図 XX に示す。このように、わが国では関東圏・関西圏が相互接続の中心となり、それ以外の地域の拠点を接続する形態が主流となっている。また、国外との接続に使われる海底ケーブルもその多くが関東圏・関西圏で陸揚げされ、ISP に接続されていることから、わが国と海外の間のネットワークトラフィックの多くも、関東圏・関西圏を経由していると考えられる。

本研究の実証実験で用いた TLD (.jprs)の権威 DNS サーバーは、関東圏、関西圏、及び海外に設置されている。そのため、当該サーバーを標的とした大規模なサイバー攻撃が発生した場合、前述したわが国の ISP 間における相互接続の特性により、当該サーバーが接続している関東圏と関西圏の ISP のネットワークにおいて攻撃トラフィックによる輻輳が発生し、当該サーバーへの接続性が失われる可能性がある。

また、わが国において地震をはじめとする大規模な災害が発生した場合、建物・設備における物理的な故障により、ISP が外部との接続に使用しているケーブル、特に海底ケーブルが切断される恐れがある。そのため、こうした災害の発生時に北海道や九州など、本州以外の地域を中心にサービスを提供・展開する ISP はそれ以外の ISP と比べ、当該サーバーへの接続性が失われる可能性が高くなる。

以上の状況から、わが国における名前解決サービスの安定性を向上させるためには、関東圏・関西圏以外の地域のうち、本州と陸続きではない北海道・四国・九州・沖縄の各地域にローカルノードを優先的に設置することが適切であると考えられる。なお、サイバー攻撃は場所によらず発生する可能性があることから、これら以外の地域の ISP においても、ローカルノードの設置が名前解決サービスの安定性向上に一定の効果を発揮すると考えられる。

また、ローカルノードとグローバルノードは設定変更により、動的に変更可能である。そのため、大規模災害によって名前解決サービスに影響が生じた際に設置済みのローカルノードをグローバルノードに一時的に変更し、サービス対象外の ISP に対して名前解決サービスを提供するといった、柔軟な運用も論理的には可能である。しかし、ローカルノードをグローバルノードに変更した場合、ISP 外でサイバー攻撃が発生した際の攻撃トラフィックを受信することになるため、名前解決サービスに加え、当該 ISP のその他のサービスにも影響が及ぶ可能性がある。

こうした状況から、大規模災害とサイバー攻撃の双方について最大限の対応が可能になるように、北海道・四国・九州・沖縄の各地域へのローカルノードの設置を優先的に進めた上で、安定運用が可能な範囲でなるべく多くの地域やネットワークにローカルノードを設置することが、名前解決サービスの安定性向上に有効であると考えられる。

サイバー攻撃発生時におけるローカルノードの効果

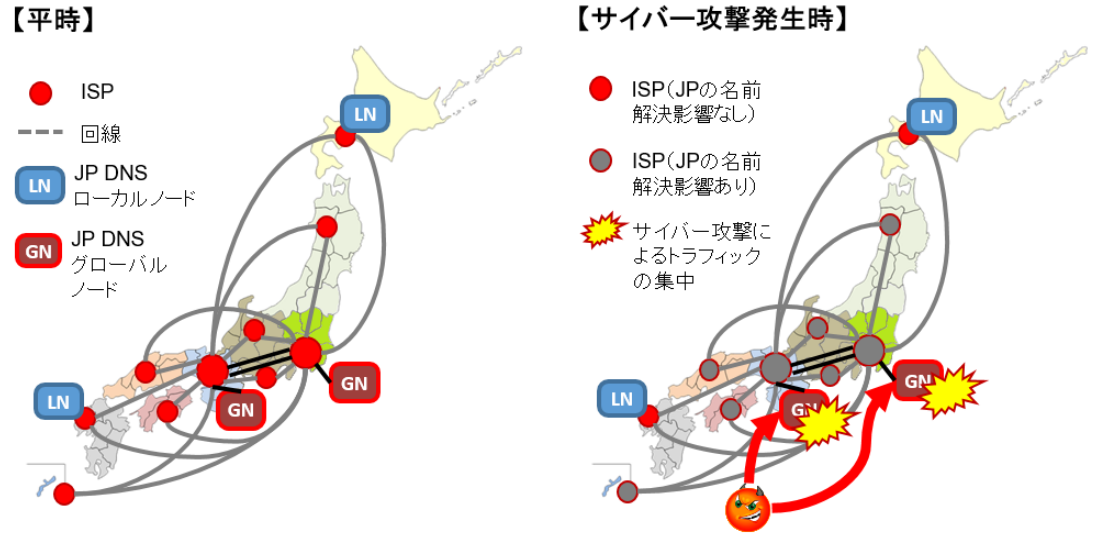


図: サイバー攻撃発生時におけるローカルノードの効果

（前回研究）大規模災害発生時におけるローカルノードの効果

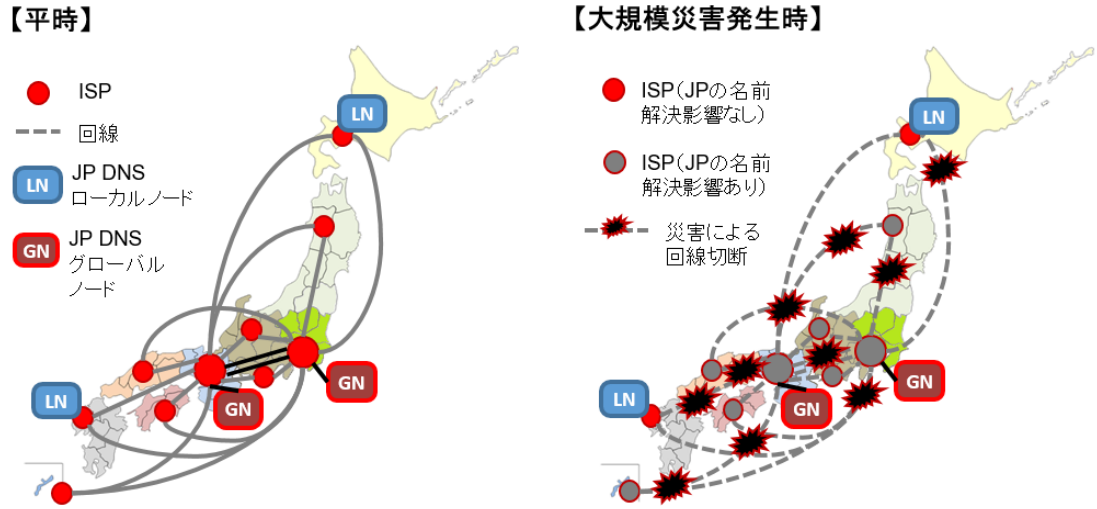


図: （前回研究）大規模災害発生時におけるローカルノードの効果

ローカルノードの設置方式とメンテナンス作業における知見

ここでは、本研究の実証実験によって得られた、ローカルノードの設置方式とそれに伴うローカルノードのメンテナンス作業における知見について記載する。

前回研究ではローカルノードを ISP に設置・接続するための方式として、接続に BGP を使用した BGP 方式と、フルリゾルバー側で DNS クエリをローカルノードに対し静的にフォワードする static 方式の 2 種類を採用し、比較を実施した。本研究の実証実験では JPRS における稼働実績、及び後述する運用のしやすさから、BGP 方式のみを採用した。

BGP 方式を採用することで、BGP による経路送出を停止することで当該ローカルノードへの DNS クエリがグローバルノードに自動的に迂回され、サービスを中断することなくローカルノードのメンテナンスを実施することが可能になった。これにより、本実験の実施期間中に必要になった BIND 9 のバージョンアップ作業実施にあたっての関係各所との事前調整が不要になり、運用における柔軟性が向上した。

今後の課題

実験シナリオ a における課題

実験シナリオ a における課題として、ローカルノードを設置した ISP 内からの攻撃により、ISP のフルリゾルバーから参照されるローカルノード及びグローバルノードの双方が応答できない状況となり、名前解決ができなくなるケースが挙げられる。このようなケースでは、ローカルノードの設置により得られる効果は限定的なものとなる。

本課題の対策として、ISP 内のフルリゾルバーにおいて DNS トラフィックを削減する機能を導入することが挙げられる。その一つとして、DNSSEC の不存在証明を積極的に活用してランダムサブドメイン攻撃による DNS クエリをフルリゾルバーから権威 DNS サーバーに送信しないようにする「Aggressive Use of DNSSEC-Validated Cache (RFC 8198)」の導入が有効である。

DNSSEC の不存在証明として NSEC を採用している場合、本機能は比較的容易に実装可能であることから、BIND 9 や Unbound などの主要なフルリゾルバーに実装されており、利用可能である。一方、不存在証明として NSEC3 を採用している場合、本機能を用いた不存在の判定が複雑になることから、フルリゾルバーにおける実装は Knot resolver などにおける、実験的なものに留まっている。

また、一部の TLD ではドメイン名の一覧を外部から入手困難にするため、不存在証明の方式として NSEC3 を採用した上で、DNSSEC に対応していない委任情報を署名対象外とする Opt-Out 機能を有効にしており、JP ドメイン名をはじめとするそうした TLD では、Aggressive Use of DNSSEC-Validated Cache の導入は効果を発揮しないことになる。

本シナリオにおけるもう一つの課題として、当該ローカルノードは設置した ISP のみをサービス対象としているため、同一地域内であっても ISP が異なる場合、設置の恩恵を受けられないという点がある。

本課題の対策として、近隣の ISP から送信される DNS クエリを何らかの方法でローカルノードを設置した ISP に中継し、サービス対象とする方法が挙げられる。これにより、特定地域の複数の ISP において、名前解決の安定性向上を図ることが期待できる。

ただし、本手法を適用することでローカルノード及びネットワーク回線の負荷が上昇する。そのため、ISP のサービス運用に影響を及ぼさないようにすることを目的とした DNS クエリの流量の把握、BGP の活用による柔軟なトラフィック制御の検討・適用といった運用技術が必要になる。

以上、各 ISP におけるローカルノードの設置・運用は名前解決サービスの継続性向上に大きく寄与する一方、わが国の全ての ISP にローカルノードを設置することは現実的でないため、各ノードの具体的な設置計画、及び運用技術の適用方法については、今後も継続的な検討が必要である。

実験シナリオ b における課題

実験シナリオ b における課題として、権威 DNS サーバーを対象としたサイバー攻撃が発生した際の攻撃元の特定、攻撃トラフィックのフィルタリングをはじめとする具体的な対策をどのように実施・運用するかという点が挙げられる。

TLD の権威 DNS サーバーを標的としたサイバー攻撃、特に ISP のフルリゾルバーを経由したランダムサブドメイン攻撃の発生源が ISP の顧客側の機器であった場合、顧客との契約上の制限・電気通信事業法における通信の秘密の遵守などの理由により ISP 側で実施可能な対策は限られており、当該顧客との調整や顧客側における機器の設定変更・交換などが必要になるケースも存在することから、迅速かつ有効な対策を実施できない場合がある。また、ランダムサブドメイン攻撃では攻撃の DNS クエリにランダムな文字列が含まれるため、一般的なネットワーク機器におけるフィルタリングでは条件の指定が複雑になり、フィルタの適用による負荷上昇・パフォーマンス低下といった状況が発生する懸念もある。

対策としては実験シナリオ a と同様、Aggressive Use of DNSSEC-Validation Cache を ISP のフルリゾルバーに導入・適用する方法が有効である。ただし、前述した理由により現時点において、その効果は限定的である。

また、本実証実験では TLD の権威 DNS サーバーオペレーターと ISP の間の連絡手段として、チャットシステムとして広く普及している Slack を採用した。しかし、実運用に携わるオペレーター間においてより効果的、かつ緊密な連携を構築するためにはより細やかな調整が必要になり、チャットに加え、メールや電話といった追加の手段も適宜使用する必要があった。

かつ、連絡・情報共有の手段・手順に加え、ローカルノードの一時停止や設定変更などの攻撃のモデルケースを想定した、オペレーター間における役割分担を事前に決めておくなど、有事における効果的な運用体制を事前に検討・策定しておく必要がある。

本研究の成果公開

本実証実験の成果公開の状況を以下に示す(()内は公開件数)。

種別	2020 年 4 月～6 月	2021 年 1 月～3 月	2021 年 4 月～7 月
特許出願	(0)	(0)	(0)
研究論文	(0)	(0)	(0)
外国発表予稿等	(0)	(0)	(0)
収録論文	(0)	(0)	(0)
学術解説等	(0)	(0)	(0)
外部機関誌論文	(0)	(0)	(0)
著書等	(0)	(0)	(0)
一般口頭発表	(0)	(1) APPRICOT (2021/02)	(2) JANOG (2021/07)
報道発表	(0)	(0)	(0)
その他資料	(0)	(0)	(0)
展示会(社外開催)	(0)	(0)	(0)
展示会(社内開催)	(0)	(0)	(0)
標準化提案	(0)	(0)	(0)

注記事項