DNS セキュリティ -水責め攻撃について考える-
被害サーバから見た DNS水責め攻撃の傾向

令和五年度 電気・電子・情報関係学会 東海支部連合大会
2023/08/29

GMOインターネットグループ株式会社
永井祐弥

自己紹介

■名前

永井　祐弥（ながい　ゆうや）

■所属

GMOインターネットグループ株式会社
システム統括本 インフラ・運用本部
ソフトウェア・仮想化技術部 仮想化技術チーム

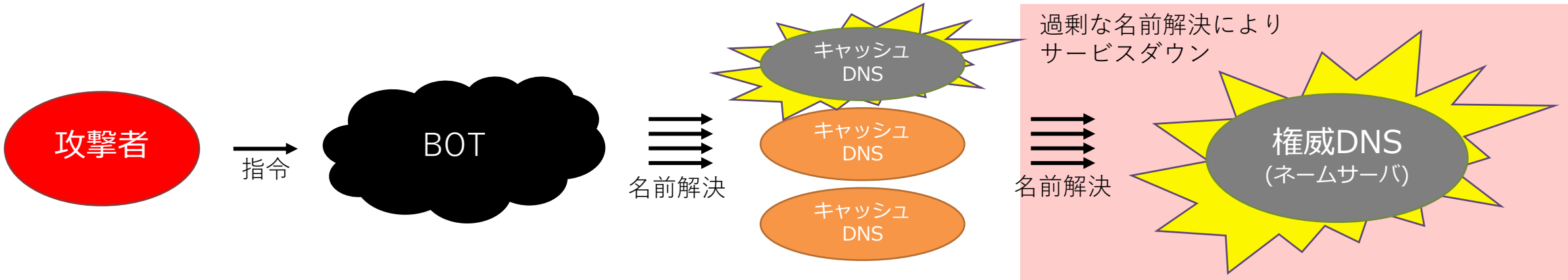
■略歴

2012年入社。自社のDNSサービス、DNSサーバ全般や、
GMOインターネットグループ会社でレジストリシステムのDNSなど、
DNSとDNSに関連するサービスの開発、運用を担当

ランダムサブドメイン攻撃(DNS水責め攻撃)とは

2014年初頭（1～2月頃）から世界的に観測され始めた
ネームサーバを標的としたDDoS攻撃の手法

特徴	ランダムなサブドメインの名前解決（DNSクエリ）を攻撃対象となる ネームサーバへ過剰に送りつけることでサービス停止に追い込む
	キャッシュDNSサーバが未対策の場合、攻撃の影響を受ける可能性もある
	このランダムなサブドメインを用いた攻撃手法は別名「DNS水責め攻撃」 「ランダムプレフィックス攻撃」とも呼ばれる



ランダムサブドメイン攻撃のイメージ

ランダムサブドメイン攻撃のパケットログ

- 実際に6月上旬に発生したネームサーバへのDNSクエリ（一部加工）
- 当時1秒間に16万クエリ(160,000/qps)の攻撃規模を観測
- 攻撃に使用されたIPアドレスは推定12,000個以上

```
16:33:17.230226 IP [redacted].24.37007 > 157.7.32.53.53: 53245% [1au] CNAME? azure.example.tokyo. (48)
16:33:17.230291 IP [redacted]28.32610 > 157.7.32.53.53: 29569% [1au] CNAME? akamai.example.tokyo. (49)
16:33:17.230323 IP [redacted]14.38074 > 157.7.32.53.53: 26122% [1au] CNAME? VEGa.eXAmPle.TokYo. (47)
16:33:17.230350 IP [redacted].8.59641 > 157.7.32.53.53: 60286% [1au] CNAME? VectOR.EXampLe.TOkyO. (49)
16:33:17.230393 IP [redacted]3.21989 > 157.7.32.53.53: 15384% [1au] CNAME? lulu.example.tokyo. (47)
16:33:17.230475 IP [redacted]86.47507 > 157.7.32.53.53: 36114% [1au] CNAME? casa.example.tokyo. (47)
16:33:17.230532 IP [redacted]3.8642 > 157.7.32.53.53: 21148% [1au] CNAME? video4.example.tokyo. (49)
16:33:17.230563 IP [redacted].99.64712 > 157.7.32.53.53: 64246% [1au] CNAME? pUsHmAiL.ExAmpLE.tOKyO. (51)
16:33:17.230599 IP [redacted]49.17213 > 157.7.32.53.53: 4777% [1au] CNAME? gj.example.tokyo. (45)
16:33:17.230673 IP [redacted]229.32311 > 157.7.32.53.53: 6944% [1au] CNAME? cookie.example.tokyo. (49)
16:33:17.230724 IP [redacted]54.61533 > 157.7.32.53.53: 17538 [1au] CNAME? accounting.example.tokyo. (53)
16:33:17.230751 IP [redacted]107.39892 > 157.7.32.53.53: 51848 [1au] CNAME? lobby.example.tokyo. (48)
16:33:17.230805 IP [redacted]32.52280 > 157.7.32.53.53: 46459% [1au] CNAME? web6.example.tokyo. (47)
16:33:17.230885 IP [redacted]2.35641 > 157.7.32.53.53: 14367% [1au] CNAME? sv02.example.tokyo. (47)
```

ランダムサブドメイン攻撃の防御手段

ランダムサブドメイン攻撃は通常の名前解決を利用した
DDoS攻撃のため簡易的な対策では効果が弱い

- DNSサーバのパフォーマンスの強化
  - 1つのIPアドレスに対する負荷分散強化（Load Balancer、IP Anycast）
  - 1つのドメイン名に対するネームサーバの追加（DNSサービス、設備追加）
  - 高性能なソフトウェアへの切り替え
  - 一定以上の性能（例えば1,000,000/qps）の確保
- 過剰な名前解決の防止
  - レートレミットなど、過剰な名前解決を制限する設定
  - キャッシュDNSのACL設定見直しや、ボットネットなどの不正利用対策
- ランダムサブドメイン攻撃のブロック
  - DNSに対応したDDoS Mitigation、Protection機能を謳っている製品の導入
  - FWやDNS Load Balancerなどによるパケットベースのフィルタリング

攻撃影響を受ける実際のソフトウェアや環境

低パフォーマンスなDNSソフトウェア

- DNSクエリを都度バックエンドやHDDなどに処理を流している場合
- BINDやPowerDNSはバックエンドにMySQLなどのRDBMSを利用出来る
- SQLによるゾーンファイル操作は非常に便利な一方で性能は低い

低キャパシティなネームサーバ構成

- 1つのNSレコードに対して1台の権威DNSサーバしか存在しないなど
  スケールアウトを考慮していない環境はDDoS攻撃に対して非常に脆い
- 低スペックなハードウェアではソフトウェアも十分な性能を発揮できない

- DNSに対するリスクの過小評価
  - 性能上限や稼働状況を把握していない
  - 辛うじて動作している状態を看過している

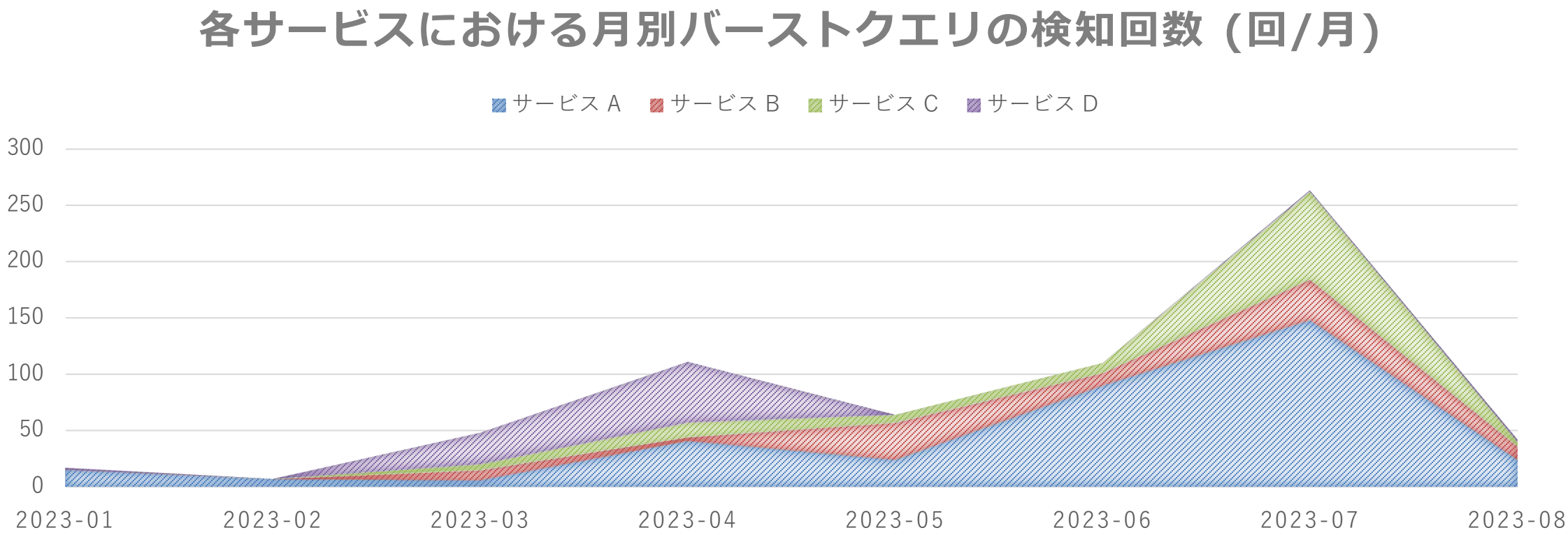
観測対象(被害サーバ)について

本発表における観測対象の情報は次の通り

	登録ゾーン件数	平常時の秒間クエリ数(QPS)	サービスの特徴
DNSサービス A	680,000	20,000/qps	ドメイン名レジストラ
DNSサービス B	250,000	4,000/qps	ホスティングサービス 1
DNSサービス C	320,000	3,000/qps	ホスティングサービス 2
DNSサービス D	570,000	2,000/qps	ホスティングサービス 3

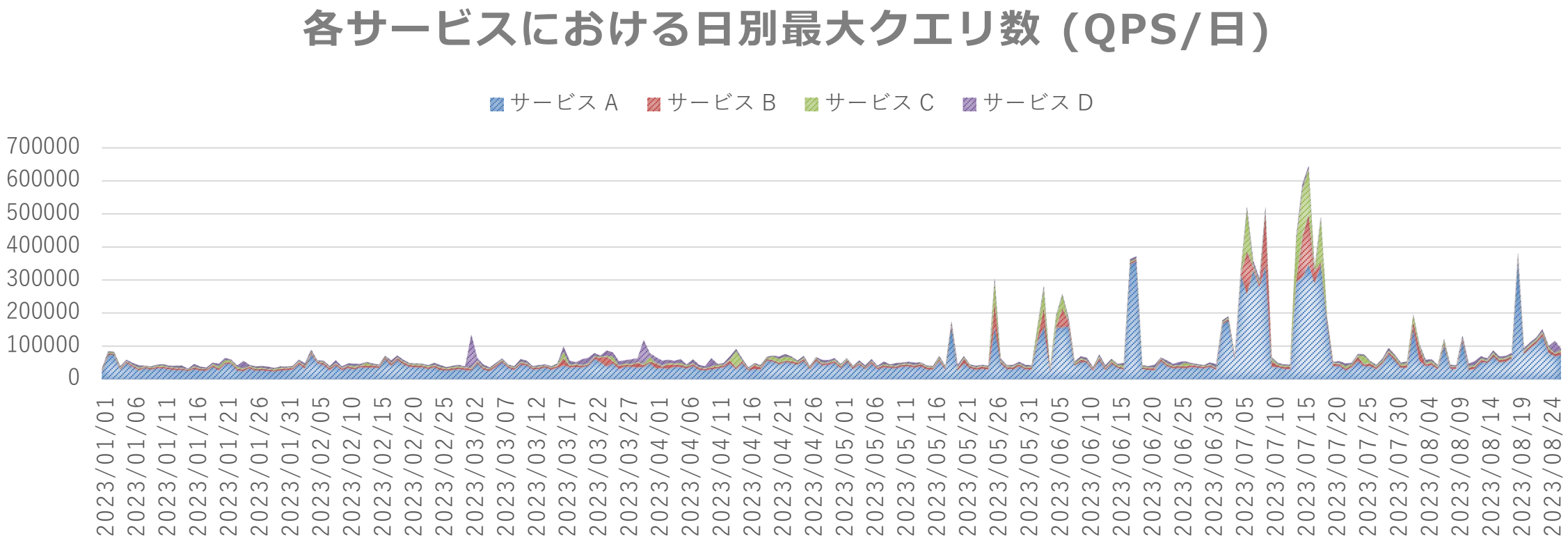
- QPS: query per second
- 観測ツールとしてDSC(pcap)を使用し、権威DNSサーバに到達したクエリの統計情報を収集
  - 毎分のクエリ数、
- 一部、tcpdumpによるデータ分析

2023年の傾向 - バーストクエリの検知



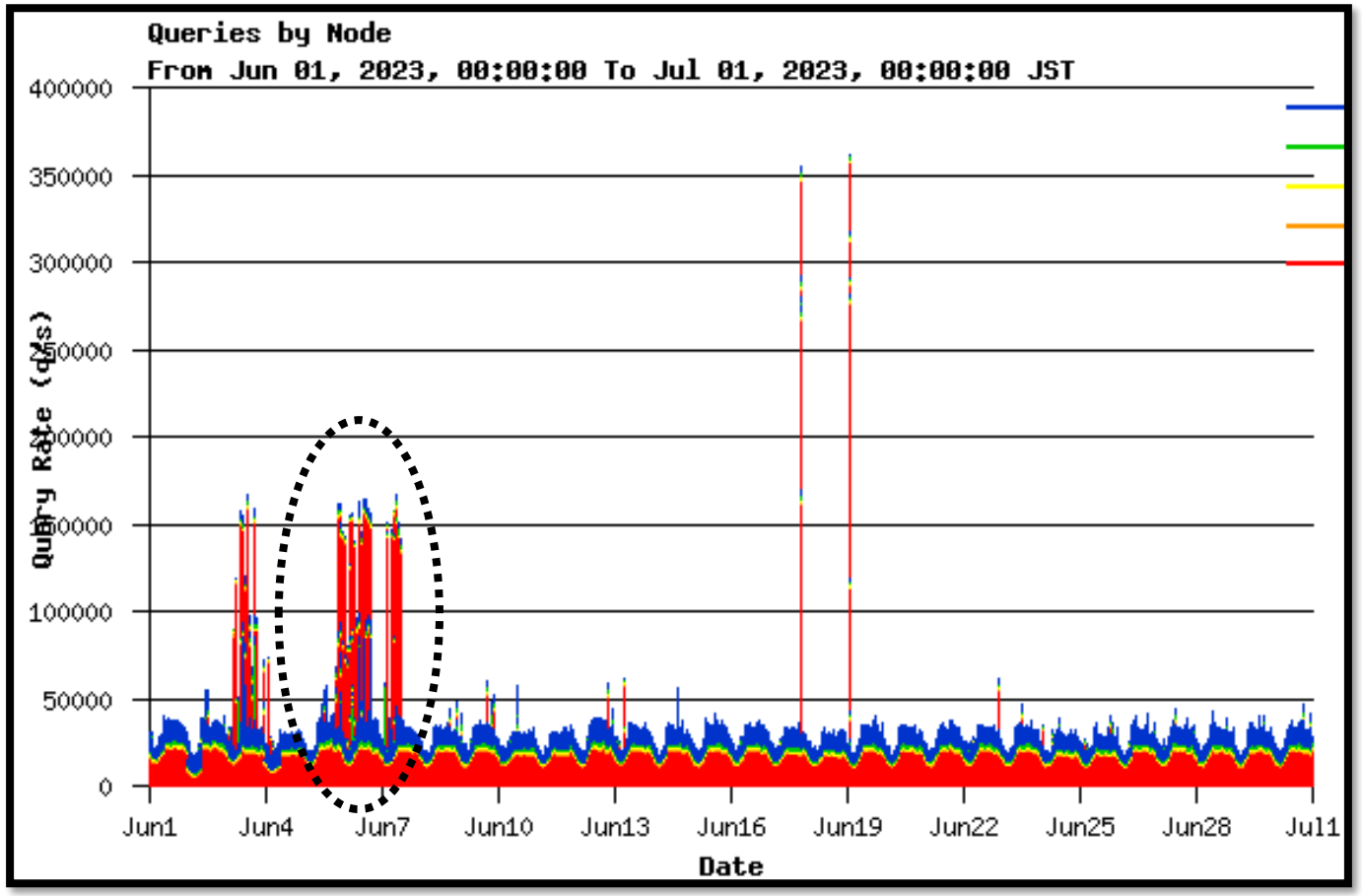
- バーストクエリ: 攻撃を目的とした突発的な大量のDNSクエリ

2023年の傾向 - 最大クエリ数



2023年の傾向 - 攻撃の分析（DSC）

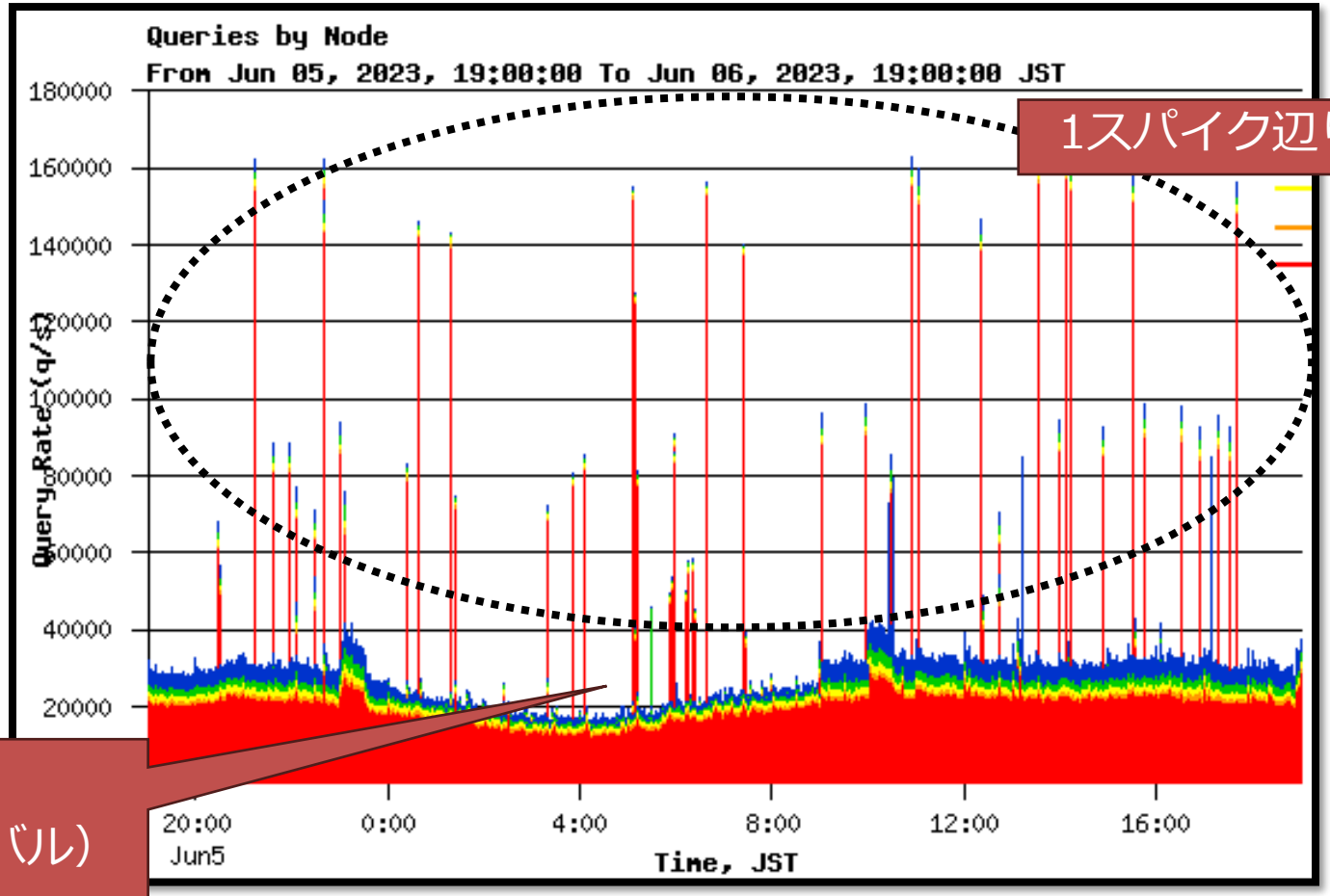
サービス全体（2023年6月）



6/5 19:00 ～ 6/6 19:00

2023年の傾向 - 攻撃の分析（DSC）

サービス全体から特定日時に絞り込み (6/5 19:00 - 6/6 19:00)

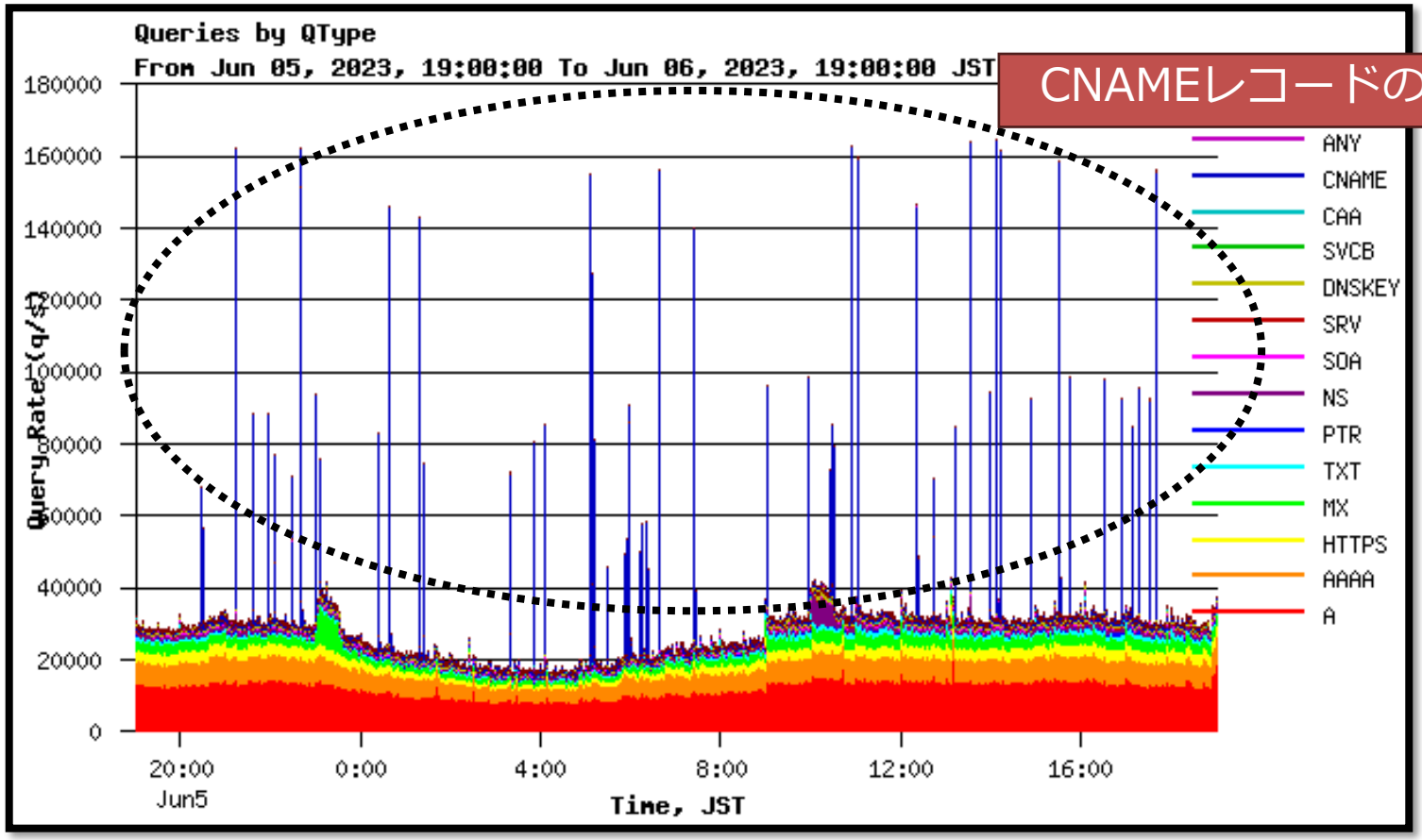


1スパイク辺りの攻撃時間は1分程度

断続的なクエリ
（1～2分間のインターバル）

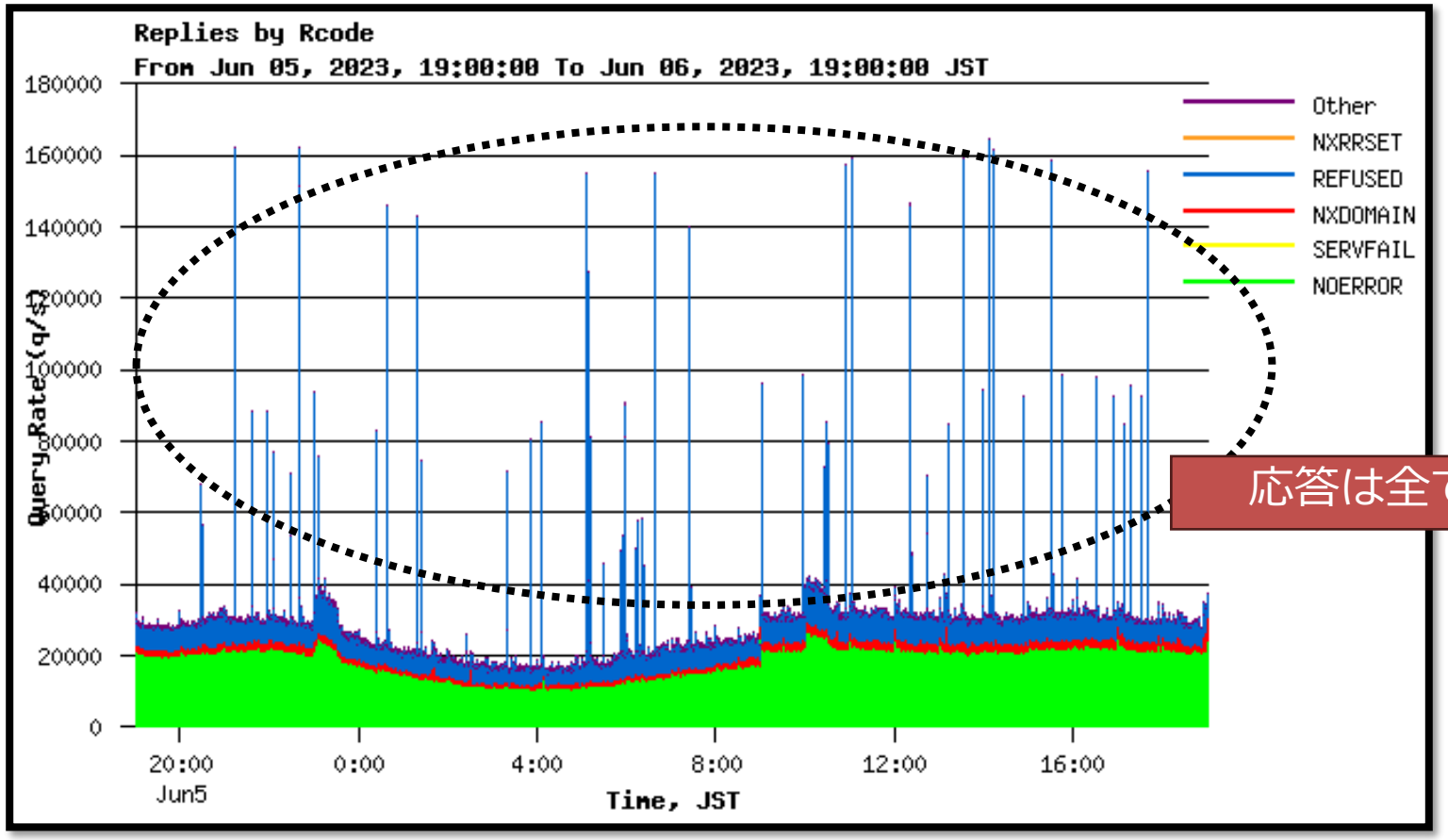
2023年の傾向 - 攻撃の分析（DSC）

問い合わせRRタイプ別 (6/5 19:00 - 6/6 19:00)



2023年の傾向 - 攻撃の分析（DSC）

応答コード別 (6/5 19:00 - 6/6 19:00)



2023年の傾向 - 送信元アドレスの分析(tcpdump)

送信元アドレスの分析について

- DSCは統計情報のみ保存するため、DNSクエリは保存されない
- そこでtcpdumpを用いてパケットデータを収集
  - tcpdump -nn -w $file -G 60 -W 1 -i any 'dst port 53'
  - 1分毎にファイルへ保存し、ファイルサイズが小さいものを破棄するスクリプトをCronで実行
  - ディスク容量の消費や、CPUの負荷が高いので常用は禁物
  - ポートミラーリング等で本番環境と分ける
- 2023/08/20に収集したものから送信元アドレスを分析

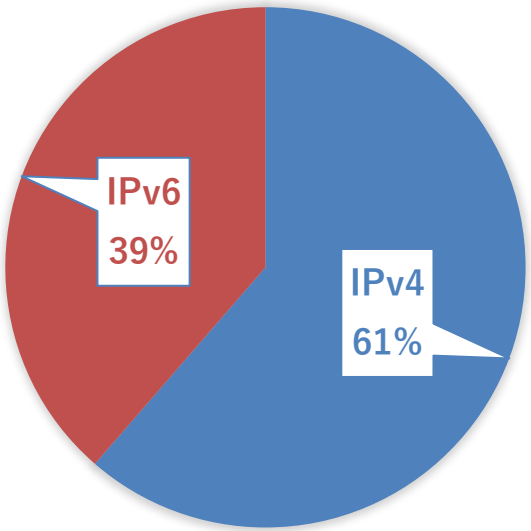
2023年の傾向 - 送信元アドレスの分析(tcpdump)

■条件

日時：2023/08/20 03:45頃
ドメイン名： {random}.example.tokyo (ランダムサブドメイン)
RRタイプ：CNAME
RCODE：REFUSED

■結果

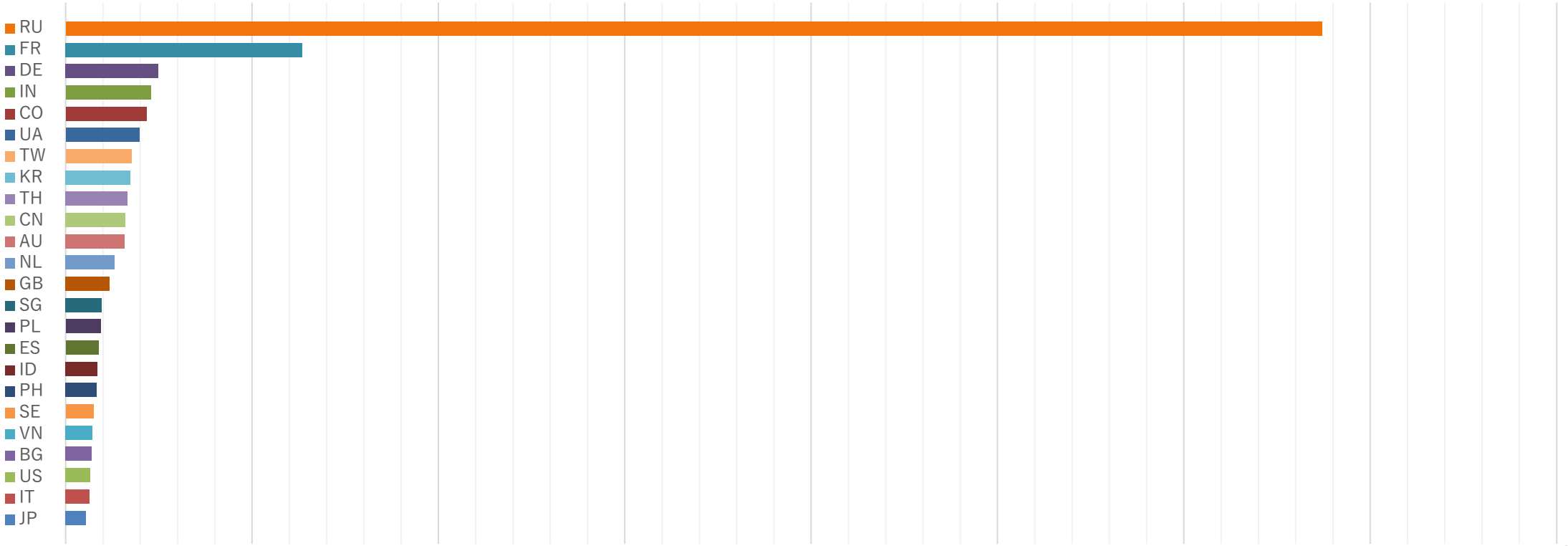
クエリ数：28万/QPS (1アドレスあたり12/QPS程度)
アドレス数： 23,797
内訳
IPv4アドレス: 14,605 (61%)
IPv6アドレス: 9,192 (39%)



2023年の傾向 - 送信元アドレスの分析(tcpdump)

■国別（簡易版）

- 送信元アドレスをWHOISで検索しCountryを集計
- 簡易的なプログラムのためCountryを検出出来ないものは集計から除外
- 日本を1として相対的に多いものを抽出



2023年の傾向 - 送信元アドレスの分析(tcpdump)

日本からのクエリ

- ISP、企業系、ホスティングサービスなど
  業態を問わず複数のアドレスからのクエリを確認
- 送信元アドレスを逆引きしたところ、一部のホスト名は
  ISPやホスティングサービスなど事業者が提供する
  フルサービスリゾルバ（キャッシュDNS）の可能性が高い

クエリの送信経路として考えられるパターン

- スタブリゾルバ（BOT感染している等）
- フルサービスリゾルバを経由（NW内にBOTが存在）
- オープンリゾルバ
- 隠れオープンリゾルバ

ランダムサブドメイン攻撃の特徴と傾向

Lame Delegation（ゾーンファイルが存在しない権威DNSサーバ）
- 共用DNSサービスに多く見られる

キャッシュされていないであろうCNAMEレコードの問い合わせ
- 通常のクライアントはCNAMEレコードを指定して問い合わせない

多数のクライアントからの同時名前解決
- 一定の時間送信するのではなく、送信タイミングを揃えている

DNSに対する効率的なDDoS攻撃を目的としている？

一方で非効率な面も多い
- 攻撃対象のドメイン名が非常に多く、攻撃の時間や間隔を含め規則性が見当たらない
- 真の攻撃対象を隠すためのカモフラージュ？
- 攻撃意図は他に存在する？

すべての人にインターネット

GMO