C10 DNS Day
2023/11/21(火) 15:30-16:30

ランダムサブドメイン攻撃において事業者として行なった対策と解析について

神田 敦、坪井 祐一、飛岡 良明、畑田 充弘

NTT Communications

スピーカー紹介

NTTコミュニケーションズ

神田 敦　イノベーションセンター

セキュリティ技術研究・開発（攻撃インフラの脅威分析）

坪井 祐一　イノベーションセンター

セキュリティ技術研究・開発（攻撃インフラの脅威分析）

飛岡 良明　クラウド＆ネットワークサービス部

NTT Com エバンジェリスト、SDPFクラウド開発

畑田 充弘　情報セキュリティ部

NTT Com-SIRT、NTTグループ認定セキュリティマスター

本セッションの目的・狙い

今年話題になったランダムサブドメインによる大量アクセスについて、
研究やサービス提供など様々な観点から調査した結果を共有します。

このような事象の知見や特徴を可能な限り共有することが、
「対応方式の確立」「事象発生時の対応迅速化」に貢献し、
インターネット全体の品質向上のために重要であると考えています。

アジェンダ

1. ランダムサブドメイン攻撃とは
2. ハニーポットで観測した大量ランダムサブドメイン
3. クラウドサービスで観測した大量ランダムサブドメインの対策と教訓
4. 大量ランダムサブドメインの特徴とクエリ元の傾向
5. まとめ

アジェンダ

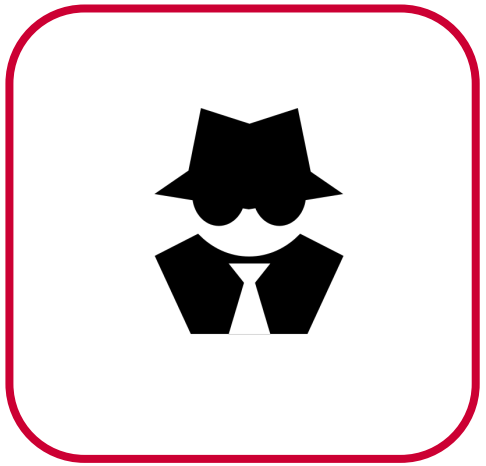
1. ランダムサブドメイン攻撃とは
2. ハニーポットで観測した大量ランダムサブドメイン
3. クラウドサービスで観測した大量ランダムサブドメインの対策と教訓
4. 大量ランダムサブドメインの特徴と攻撃元の傾向
5. まとめ

ランダムサブドメイン攻撃

DNSを使ったDDoS攻撃手法のひとつ

ランダムサブドメイン攻撃

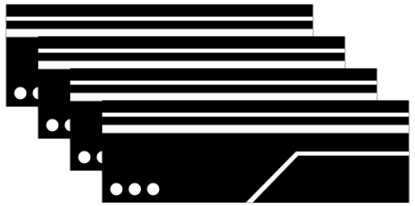
DNSを使ったDDoS攻撃手法のひとつ



悪意をもってDNSクエリを
発生させるアクター
（+ ボットネット）

ランダムサブドメイン攻撃

DNSを使ったDDoS攻撃手法のひとつ

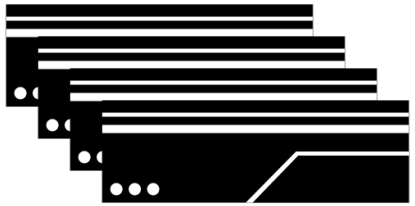


オープンリゾルバなどの
キャッシュDNSサーバ

**不特定のクライアントからの
クエリを受け付ける
キャッシュDNSサーバ**

ランダムサブドメイン攻撃

DNSを使ったDDoS攻撃手法のひとつ



オープンリゾルバなどの
キャッシュDNSサーバ

example.jp
権威DNSサーバ

権威DNSサーバ

ランダムサブドメイン攻撃

DNSを使ったDDoS攻撃手法のひとつ

ポイント① 大量の実在しないサブドメイン
（NXDOMAIN）

実在しないドメイン名であるため、キャッシュが効かない
＝ 権威DNSサーバに問い合わせることになる

※ この特徴から別名「NXDOMAIN攻撃」とも呼ばれる

ランダムサブドメイン攻撃

DNSを使ったDDoS攻撃手法のひとつ

ポイント② メインターゲットは権威サーバ

オープンリゾルバなどの
キャッシュDNSサーバ

大量の問い合わせを発生させて権威DNSサーバに負荷をかけるのが狙い
（と考えられている）

※ ISPのキャッシュDNSサーバが過負荷に陥るケースもある

“ランダム”サブドメイン攻撃？

DNSを使ったDDoS攻撃手法のひとつ

真に“ランダム”な文字列とは限らない

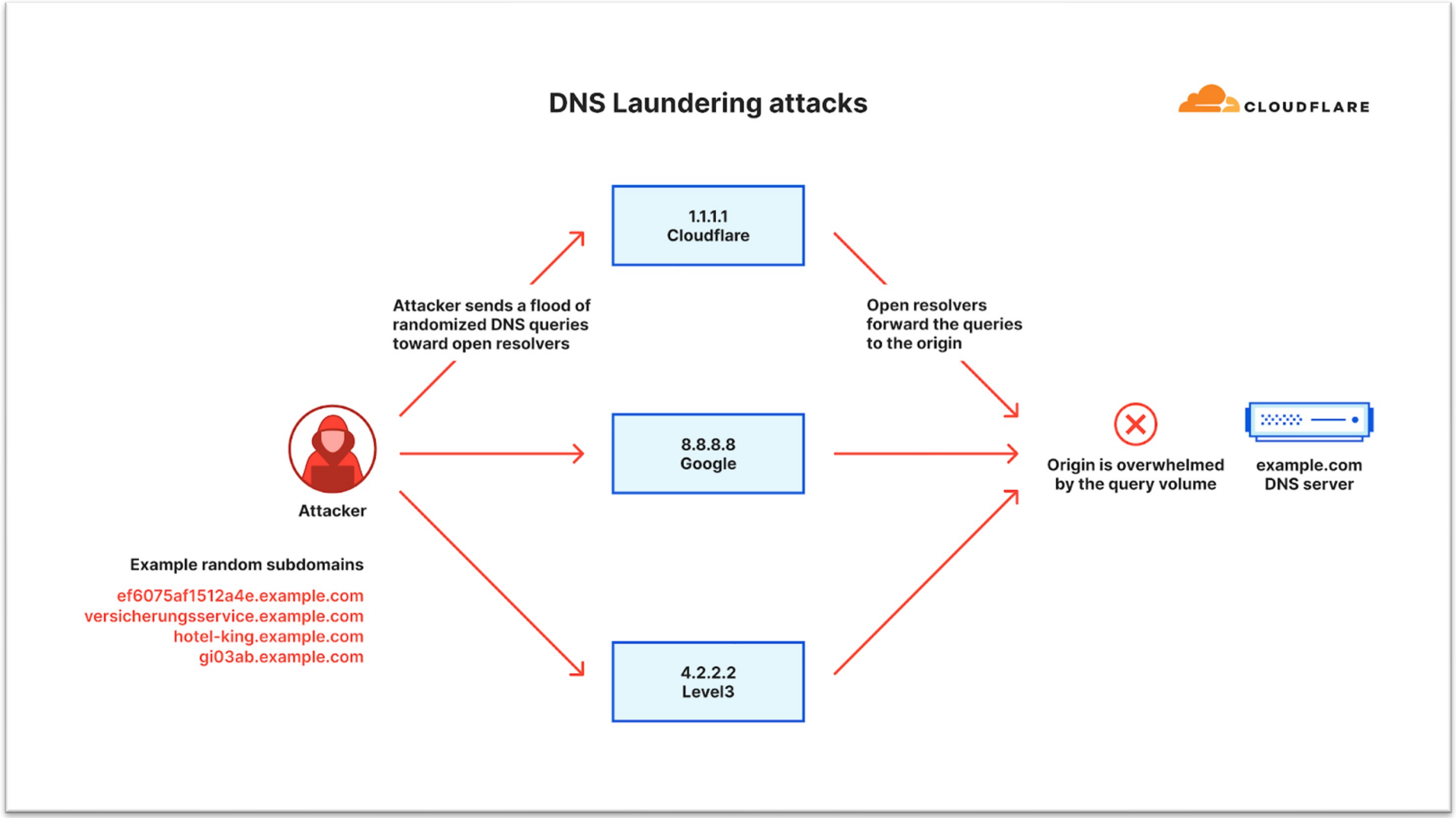
- 単語のつなぎ合わせ、特定prefix/suffix+ランダム文字列、など

最近のランダムサブドメイン攻撃の特徴

パブリックDNSサービスも悪用する

オープンリゾルバなどの
キャッシュDNSサーバ

最近のランダムサブドメイン攻撃の特徴



DDoS threat report for 2023 Q2
https://blog.cloudflare.com/ddos-threat-report-2023-q2/

日本 × ランダムサブドメイン攻撃

2023年3月ごろ～

- 世界各国でランダムサブドメイン攻撃の報告が相次ぐ

- 日本でも大量のランダムサブドメインクエリが原因で
  サービス影響が出たと見られる事例が複数報告されている

- 「誰が」「何のために」大量クエリを発生させたかは不明
  - 攻撃を表明したアクターがいるわけではない
  - 明確に害する意図をもった“攻撃”かどうかも分からない

アジェンダ

1. ランダムサブドメイン攻撃とは
2. ハニーポットで観測した大量ランダムサブドメイン
3. クラウドサービスで観測した大量ランダムサブドメインの対策と教訓
4. 大量ランダムサブドメインの特徴とクエリ元の傾向
5. まとめ

ハニーポット観測のきっかけ

先述の大量ランダムサブドメインクエリが原因と見られる事案の
ニュースやSNSなどの情報をきっかけに、
オープンリゾルバを模したハニーポットを設置し、観測した

オープンリゾルバ ハニーポット

（管理の甘い状態で放置された）
オープンリゾルバの振りをさせる

オープンリゾルバ
ハニーポット

オープンリゾルバ ハニーポット

「どんなサブドメイン」を
クエリしてくるか

「どんな（親）ドメイン」が
狙われるか

**オープンリゾルバ
ハニーポット**

脅威インテリジェンスサービスなどをフル活用して事象の実態を分析

ハニーポット運用上の注意ポイント

攻撃に加担して
権威DNSサーバに
過剰な負荷をかけない

オープンリゾルバ
ハニーポット

example.jp
権威DNSサーバ

送信元詐称されたホスト
など

DNSリフレクション攻撃など
他の攻撃に加担して
他のホストに過剰な負荷をかけない

※DNSリフレクション攻撃：送信元を詐称したクエリを大量発生させ、そのDNS応答により負荷をかけるDDoS攻撃

ハニーポットの設計／構築

脅威アクターの行為への加担を防ぐために以下に配慮

- DDoSへの加担を回避するため、
  ネットブロック毎に1QPS（クエリ／秒）の制限
  （IPv4: /24、IPv6: /48）
- キャッシュDNSから権威DNSへの帯域圧迫を抑止するため、
  DNSSECの署名検証機能オフ／ DNSSECの無効化
- クライアントからキャッシュDNSの帯域圧迫を抑止するため
  ＆DNSリフレクション攻撃を抑止するため、
  バッファサイズを制限

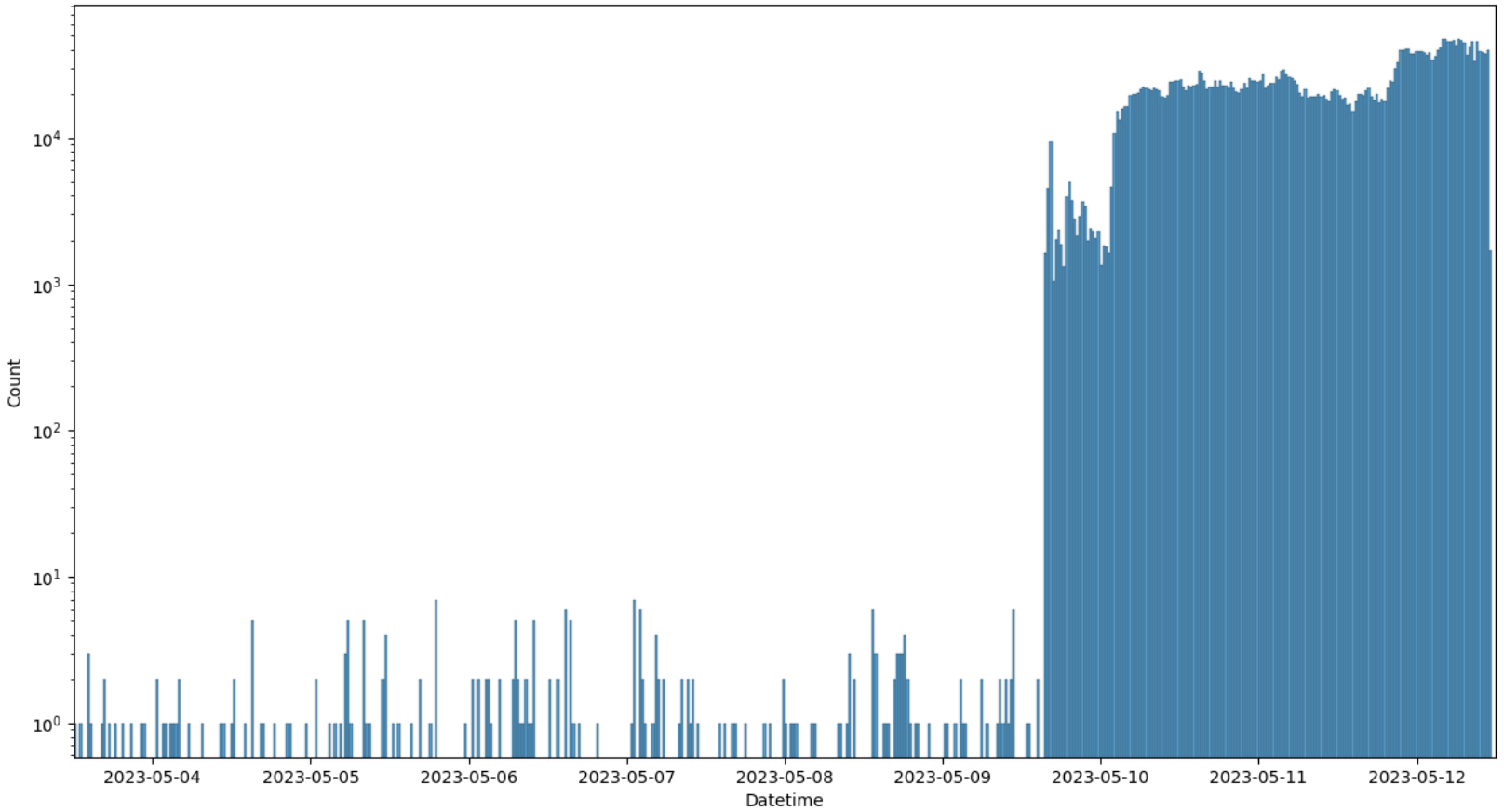
ハニーポットを配置して観測をしてみた

アクターの特徴を捉えるためアプローチを変えて観測

- 1回目：公開されているオープンリゾルバのリストに（途中で）敢えて登録
- 2回目：公開されているオープンリゾルバのリストに登録しない

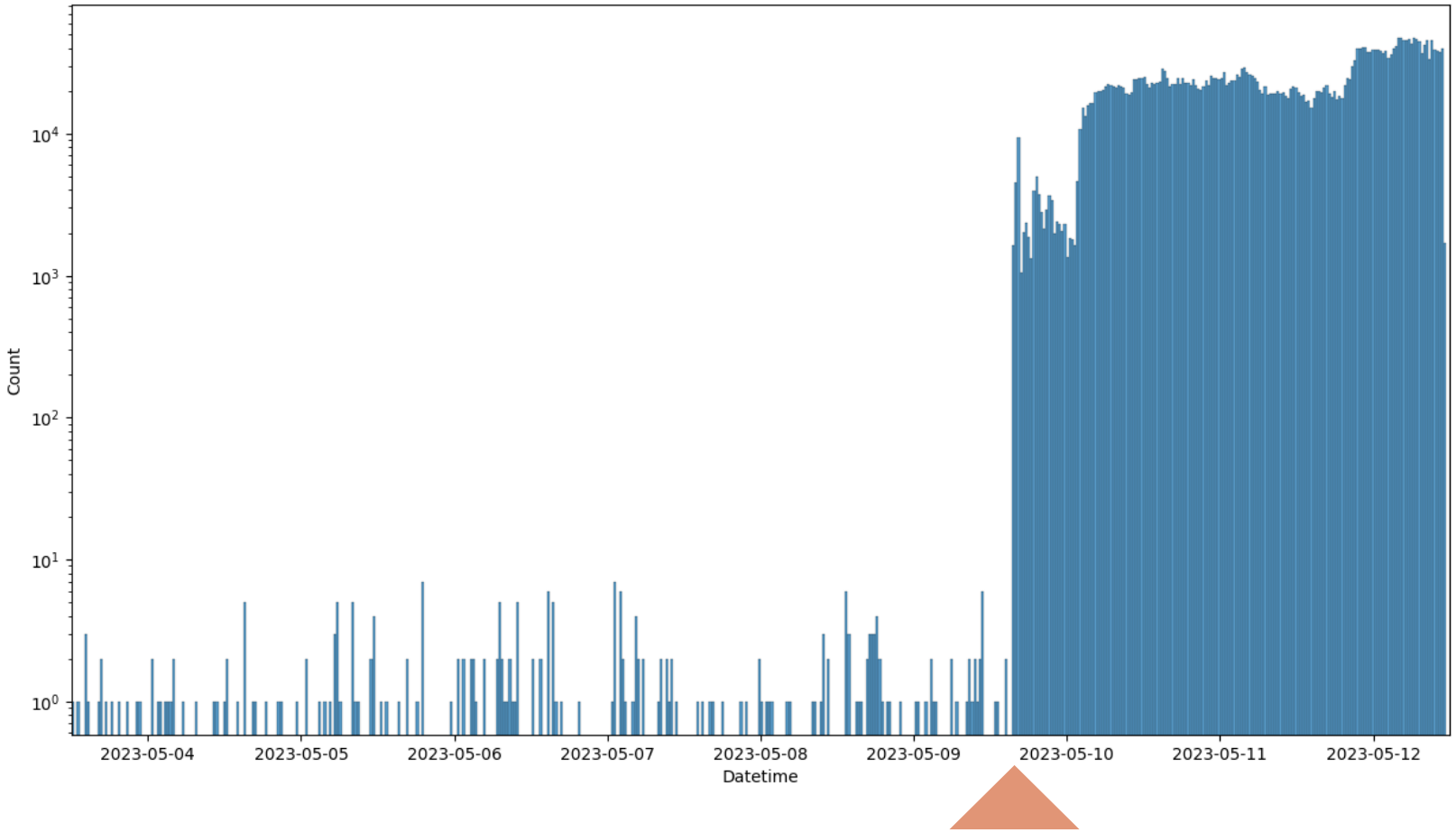
設置期間（１回目）の観測内容

- 5月上旬



設置期間（１回目）の観測内容

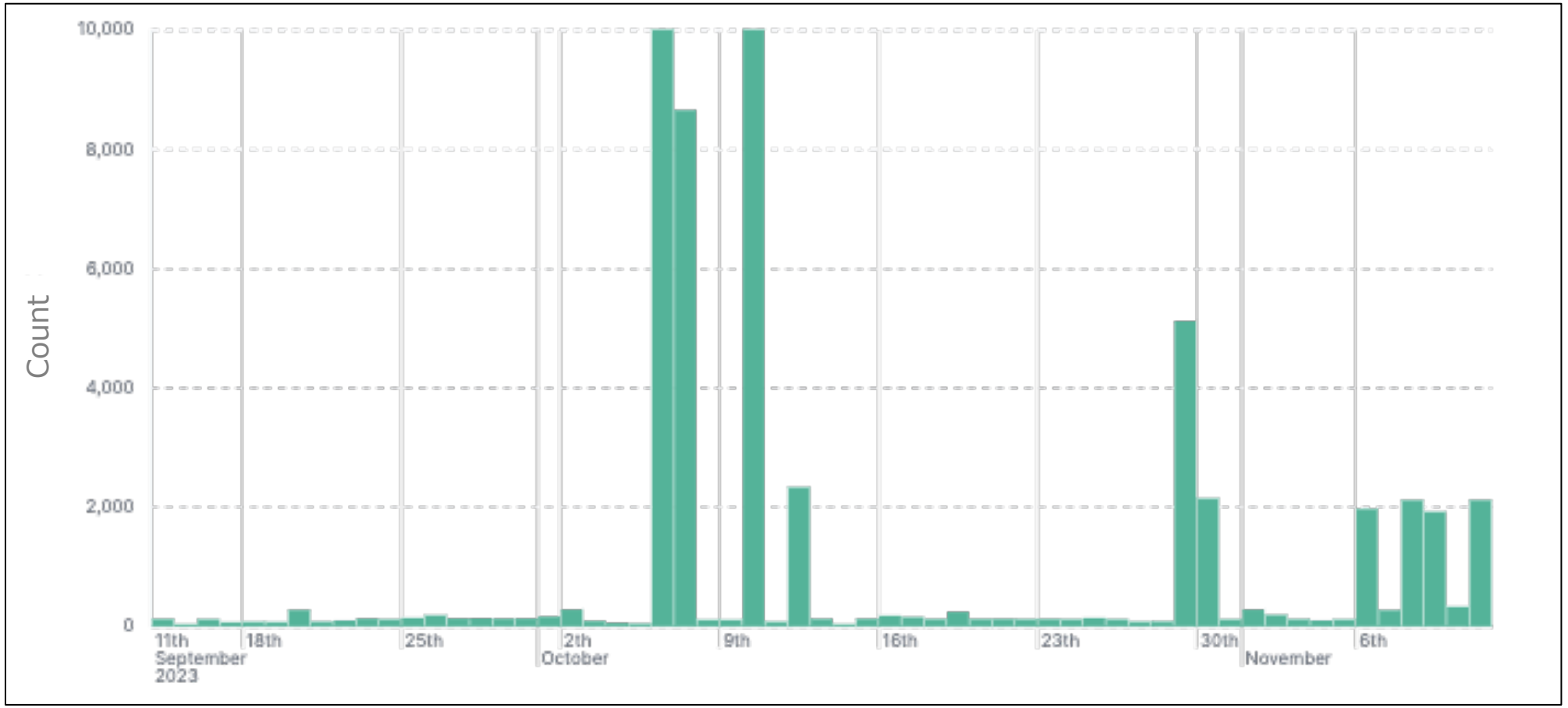
- 5月上旬



オープンリゾルバの公開リストに掲載される

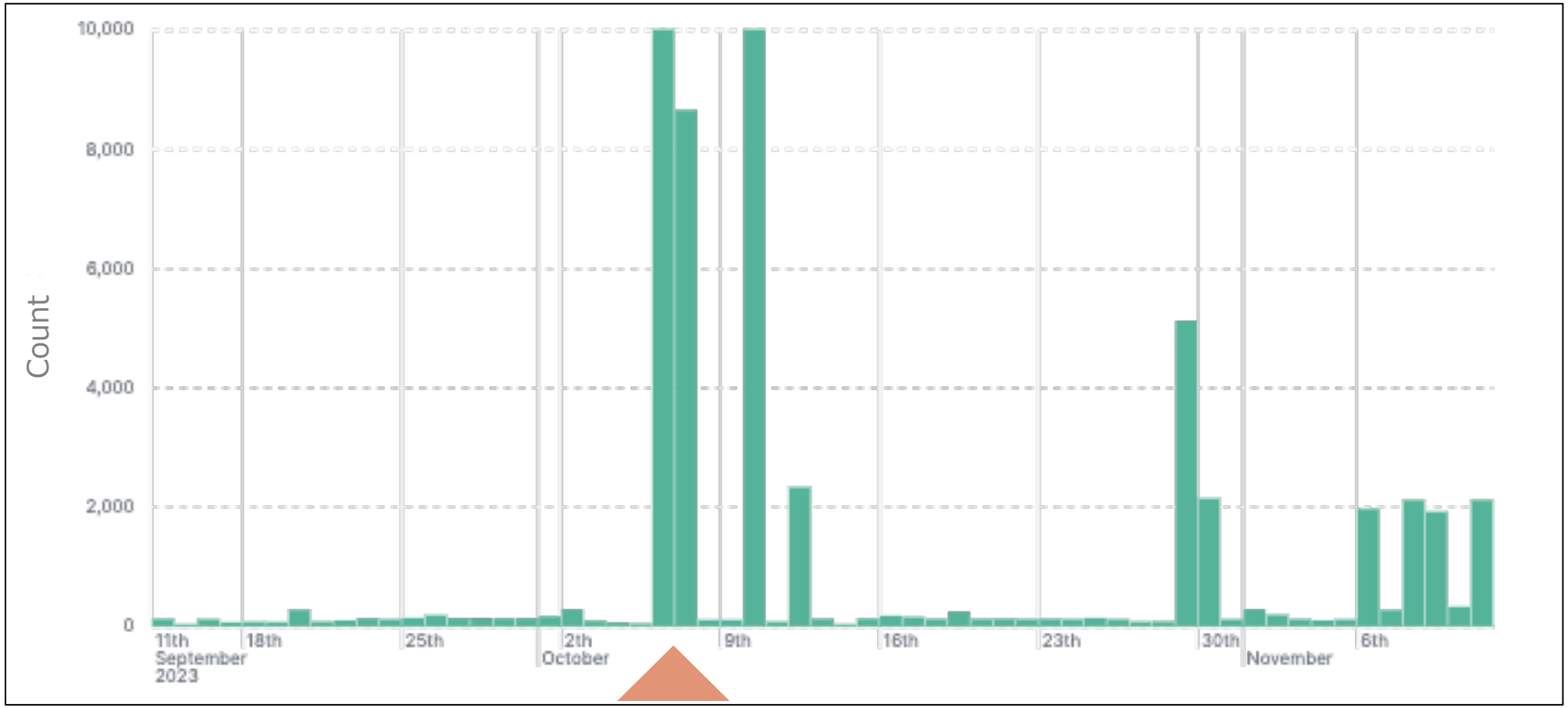
設置期間（２回目）の観測内容

- 9/14～11/13までの2ヶ月間、リクエスト件数107,413件



設置期間（２回目）の観測内容

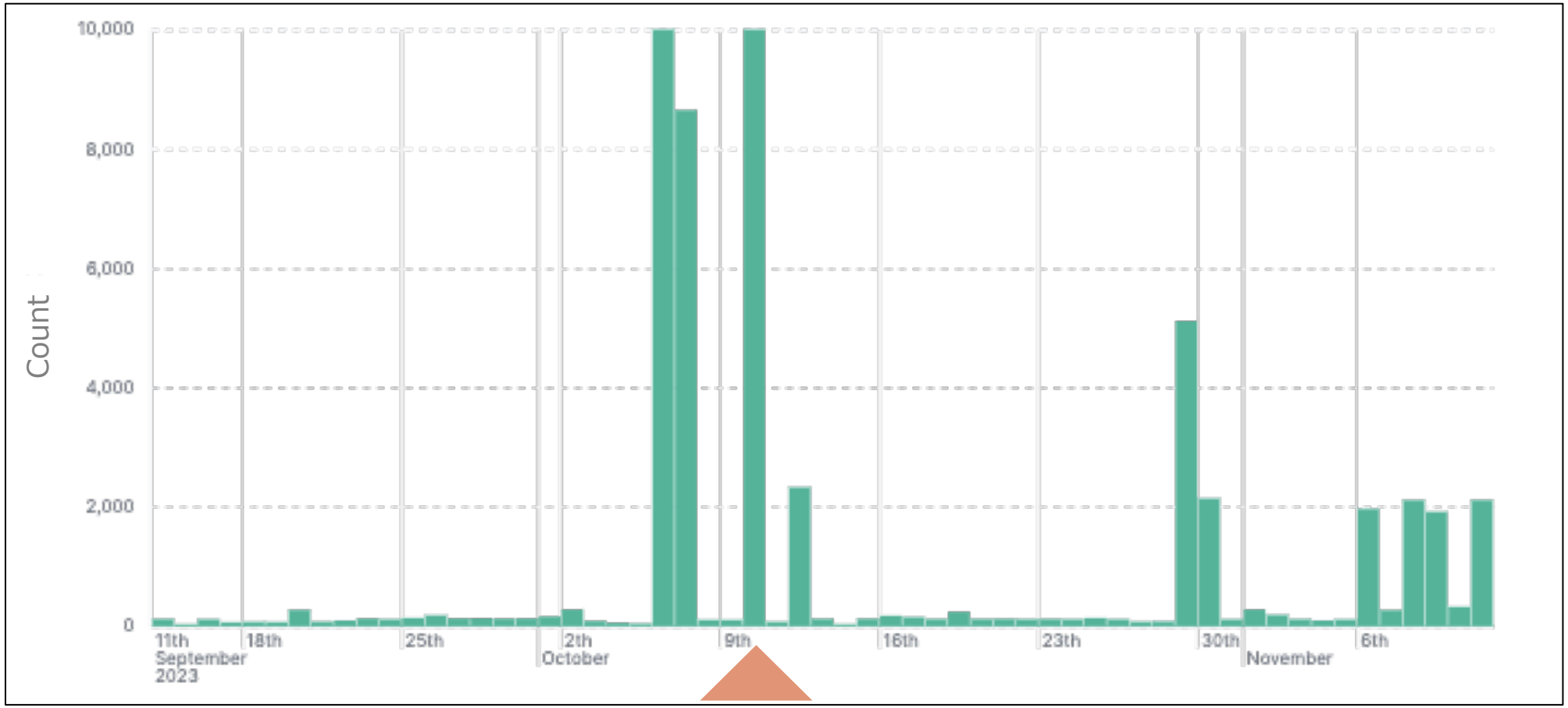
- 9/14～11/13までの2ヶ月間、リクエスト件数107,413件



10/6～7に１つの送信IPから大量のランダムサブドメインリクエスト（67,541件）を観測

設置期間（２回目）の観測内容

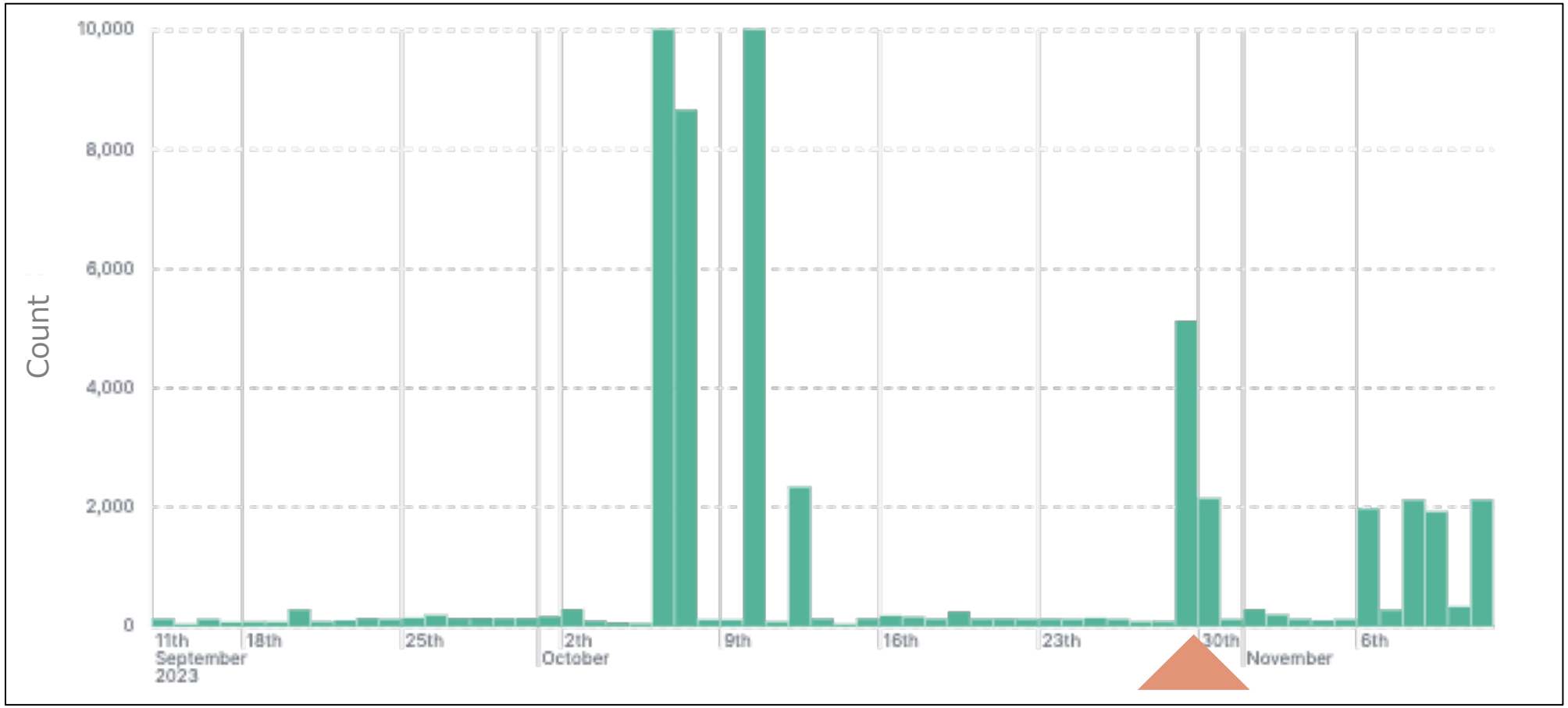
- 9/14～11/13までの2ヶ月間、リクエスト件数107,413件



10/10に１つの送信IPから大量のタイプAnyリクエスト（13,325件）を観測

設置期間（２回目）の観測内容

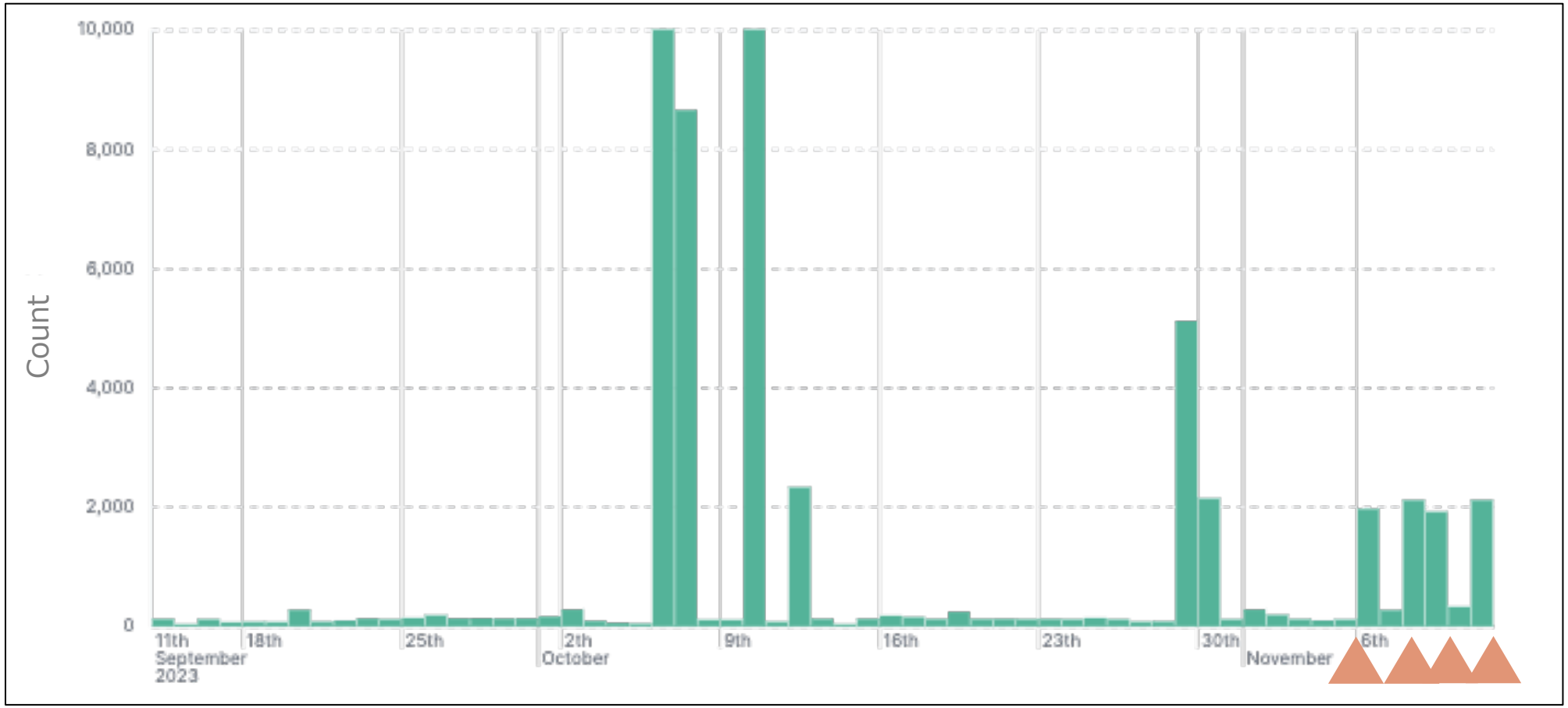
- 9/14～11/13までの2ヶ月間、リクエスト件数107,413件



10/28～30に複数の送信IPからタイプAnyでのリクエスト（7,004件）を観測

設置期間（２回目）の観測内容

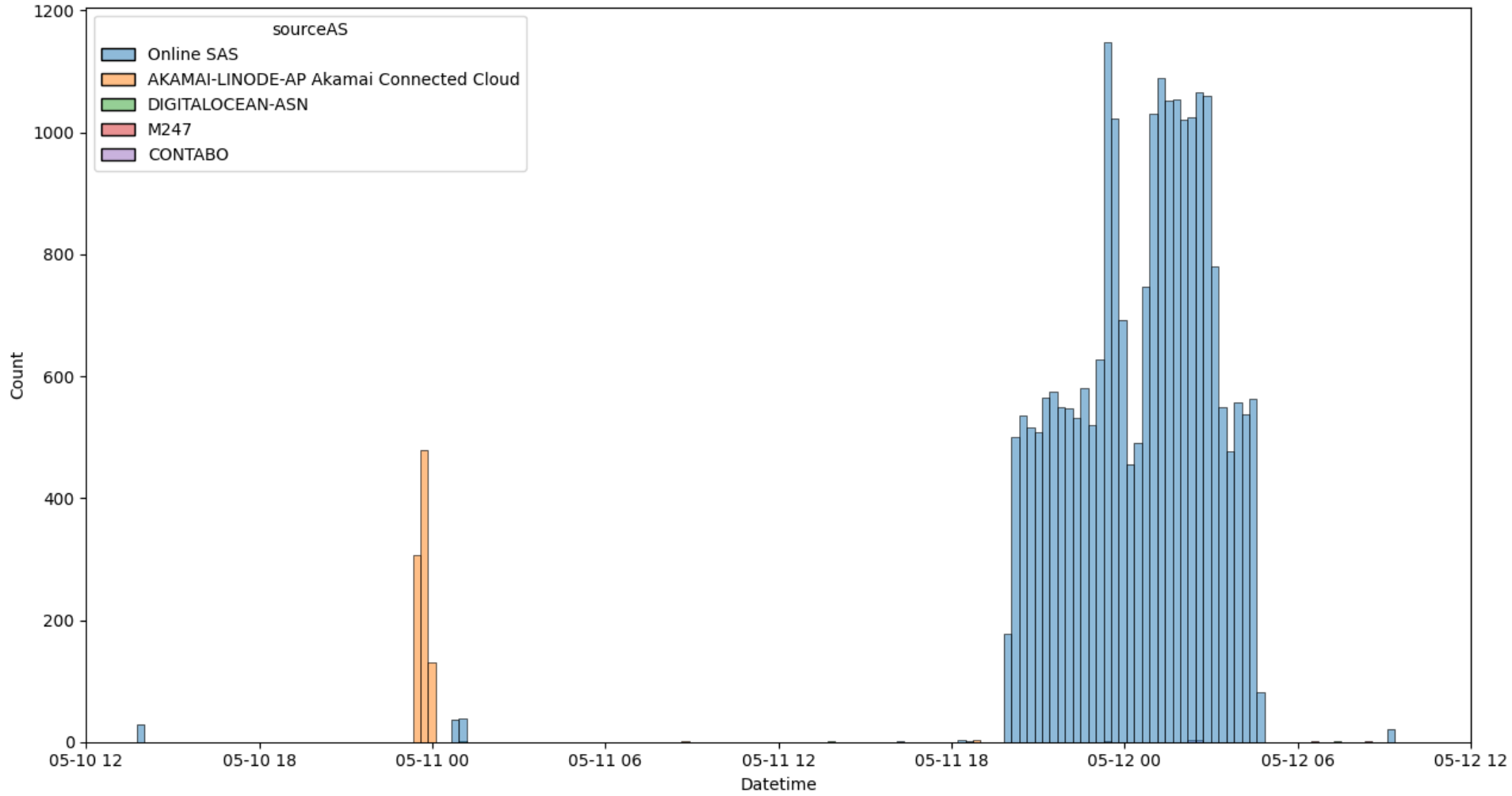
- 9/14～11/13までの2ヶ月間、リクエスト件数107,413件



11/6～11/11 複数日に分けて１回2000件ごとで１つの送信IPからの
ランダムサブドメインリクエスト（合計7,998件）を観測

深堀分析１：
観測期間（1回目）に
大量サブドメインクエリが観測された
親ドメインについての分析

とある親ドメインへの大量サブドメインクエリ①



とある親ドメインについて観測されたクエリ量

とある親ドメインへの大量サブドメインクエリ①

- 観測されたサブドメインの特徴
  - 単語をハイフンで結合
    - 例　`dclb03-dca1`

      `lathena-phx-testngley-docker`

      `coconut-getter-staging`

表：単語の出現回数 Top10

単語	出現回数	単語	出現回数
staging	5200	web	688
cadence	1246	dca1	680
atg	975	dev	668
phx	831	test	596
dca	777	phx2	551

とある親ドメインへの大量サブドメインクエリ①

- 観測されたサブドメインの特徴
  - 単語をハイフンで結合
    - 例　`dclb03-dca1`

      `lathena-phx-testngley-docker`

      `coconut-getter-staging`

バグハンティング？

表：単語の出現回数 Top10

単語	出現回数	単語	出現回数
staging	5200	**web**	688
cadence	1246	dca1	680
atg	975	**dev**	668
phx	831	**test**	596
dca	777	phx2	551

サブドメイン列挙（Subdomain Enumeration）

- バグハンティングの一環などで、
  ドメイン名空間から存在するサブドメイン名を探し出し列挙する行為
  - 意図せず公開されているサービスを糸口に報奨金獲得を狙う
  - 列挙テクニックの一つが
    「ターゲットの特定ドメインに関連する可能性のあるワードや用語を含む
    ワードリストを使用する」

	ランダムサブドメイン攻撃	サブドメイン列挙
外形的な見え方	大量のクエリ	大量のクエリ
目的	DoS	存在するサブドメインの発見
戦略	積極的に外しにいく	積極的に当てにいく

とある親ドメインへの大量サブドメインクエリ①

- 仮説を支持する事実
  - 当該親ドメインはバグバウンティプラットフォームサービス（HackerOne）にて**報奨金の対象**となっている（登録日：2023/3/14）
  - 当該親ドメインは社内利用が主目的と思われる文字列
    （政治的・社会的主張を目的とした攻撃ならもっとメジャーなドメインを狙うはず）
  - OSS公開されている著名なサブドメイン列挙ツールの中には
    以下の機能をもつものが存在する
    - 単語をつなぎ合わせて**サブドメイン候補リストを生成する**機能
    - （処理高速化のために）
      複数のオープンリゾルバを使って分散して名前解決する機能

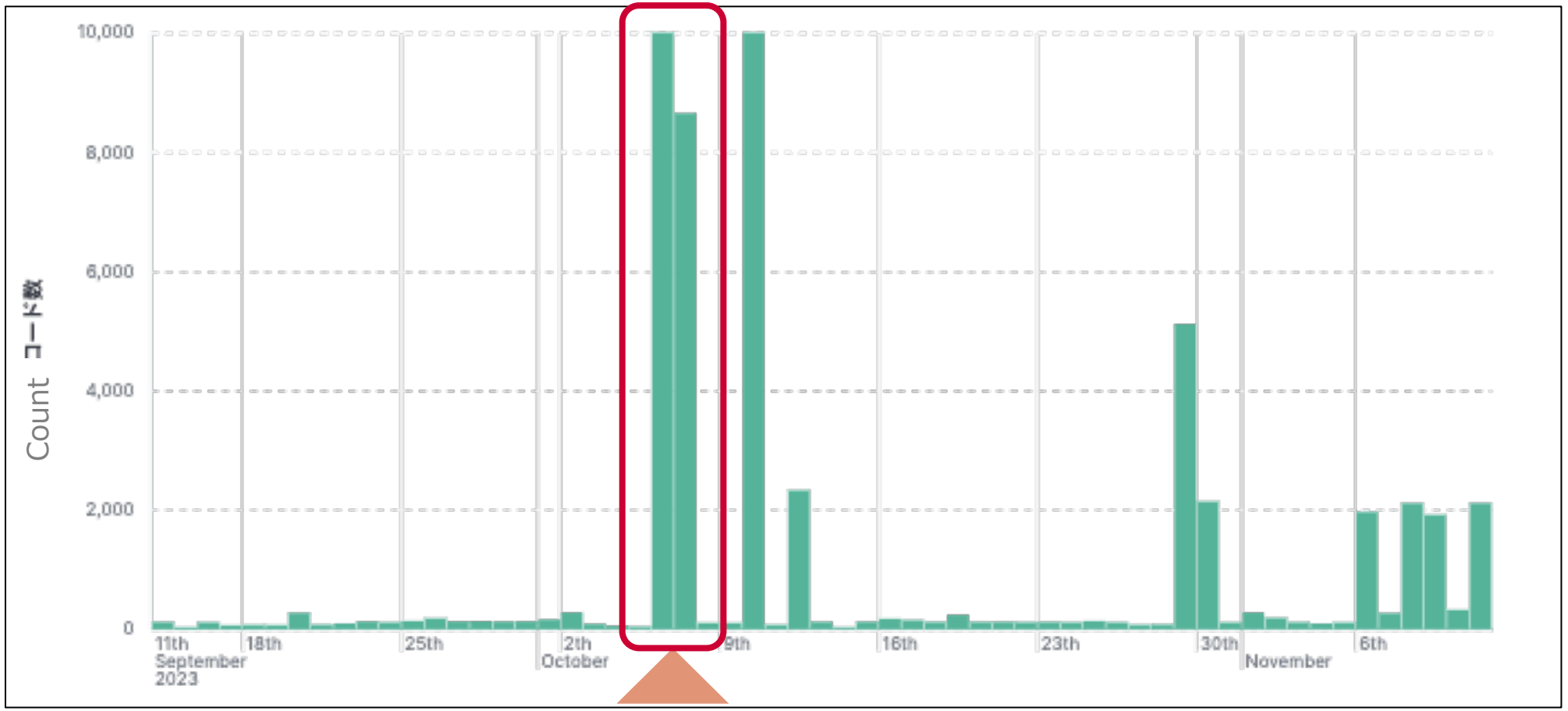
とある親ドメインへの大量サブドメインクエリ①

- 結論
  - 観測されたランダムサブドメイン攻撃（に見えた事象）は、
    バグハンターによるサブドメイン列挙行為の一部だった蓋然性が高い

- 学び
  - 世の中で観測されている大量ランダムサブドメインの中には
    攻撃を意図したものではないクエリが含まれている
  - ランダムサブドメイン攻撃とサブドメイン列挙は紙一重
  - 職業倫理の観点から
    「バグハンティングにおけるオープンリゾルバ利用」は1つの議論ポイント

深堀分析2:
観測期間（2回目）に
大量サブドメインクエリが観測された
親ドメインについての分析

とある親ドメインへの大量サブドメインクエリ②



とある親ドメインについて大量のランダムサブドメインリクエスト（67,541件）を観測（10/6～7）

とある親ドメインへの大量サブドメインクエリ②

- 観測されたクエリの特徴
  - パターンは**www.{3~5文字のランダムな英数字記号の組み合わせ}.mil**
  - 例：
    - 3文字：www.dtl.mil. www.i6l.mil. www.vt9.mil.
    - 5文字：www.9-2lk.mil. www.¥--5l2.mil. www.¥--4qd.mil.

    ※6文字になっているがバックスラッシュを入れて-(ハイフン)をエスケープしてるので基本的には3~5文字ドメインを生成している様子

とある親ドメインへの大量サブドメインクエリ②

- 観測されたクエリの特徴
  - ランダムな英数字記号であり、意味のある単語になっていないことから、深堀分析1のように単語の組み合わせによるサブドメイン列挙で生成されたわけではなさそう
  - 生成された単語を見ると先頭文字だけa-z,1-9の順で残りの文字がランダムの総当たりで生成されているように見える
    - ブルートフォースでドメイン名生成しているように見える

ドメイン名生成にはサブドメイン列挙ツール（ブルートフォース）で生成された文字列を組み合わせているようだ。

とある親ドメインへの大量サブドメインクエリ②

- 観測されたクエリの特徴
  - 全てのクエリのサブドメインが「www.」から始まっている
    - サブドメインをターゲットにしていない可能性
    - Prefixを固定化しておくことでランダムサブドメイン攻撃としての検知を回避しようとしている可能性
    - Webサーバを超原始的なブルートフォースで探索している可能性

とある親ドメインへの大量サブドメインクエリ②

- 観測されたクエリの特徴
  - 全てのクエリが「.mil」で終わっている
    - .milのドメインはアメリカ国防総省とその下部組織が使用するTLDである
    - アメリカ国防総省は、**今では.milドメインの下でバニティドメインも使用している**

    ※バニティドメインとは特定の目的や魅力的で記憶に残りやすいドメイン名のこと。

- 「www.」から始まってブルートフォースでドメイン名を検索していることから、バニティドメインを探しているのではないか

とある親ドメインへの大量サブドメインクエリ②

- 仮説を支持する事実
  - .milのTLDを利用しているバニティドメインには短いドメイン名の物があることを確認
    - navy.mil: アメリカ海軍の公式ウェブサイト
    - afrl.mil: アメリカ空軍の研究所であるAir Force Research Laboratoryのサイト
    - darpa.mil: アメリカ国防総省の先進的な研究プロジェクトを担当するDefense Advanced Research Projects Agencyのサイト
    - nasa.mil: アメリカの宇宙開発機関であるNational Aeronautics and Space Administrationのサイト

とある親ドメインへの大量サブドメインクエリ②

- 結論．．．に至らず（無念）
  - 観測されたランダムサブドメイン攻撃（に見えた事象）は、探索ともとれるし、攻撃ともとれる

まとめ：ハニーポット観測から見えたもの

大量ランダムサブドメインの特徴を捉えるために
ハニーポットを設置し観測、分析を行った

- 得られた学び
  - **公開オープンリゾルバリストへの掲載有無**でクエリの傾向が変わる
  - 個々のケースに着目すると、
    サブドメイン文字列の作り方には違いがある（アクターの癖？）
  - 必ずしも**攻撃（DoS）目的とは限らない**（例：バグハンターによる探索活動）
    - 簡単には判別できないものもある
      （ランダムサブドメイン攻撃とサブドメイン列挙は紙一重）

（何が目的であれ）
大量ランダムサブドメインの脅威は
既に顕在化

事業者として対策は不可避

アジェンダ

1. ランダムサブドメイン攻撃とは
2. ハニーポットで観測した大量ランダムサブドメイン
3. クラウドサービスで観測した大量ランダムサブドメインの対策と教訓
4. 大量ランダムサブドメインの特徴とクエリ元の傾向
5. まとめ

観測された事象

弊社で提供しているエンタープライズ向けクラウドサービスの1サービスである「SDPF DNS」に対して、ランダムサブドメインアクセスと思われる大量アクセスが確認された。

大量アクセス概要:

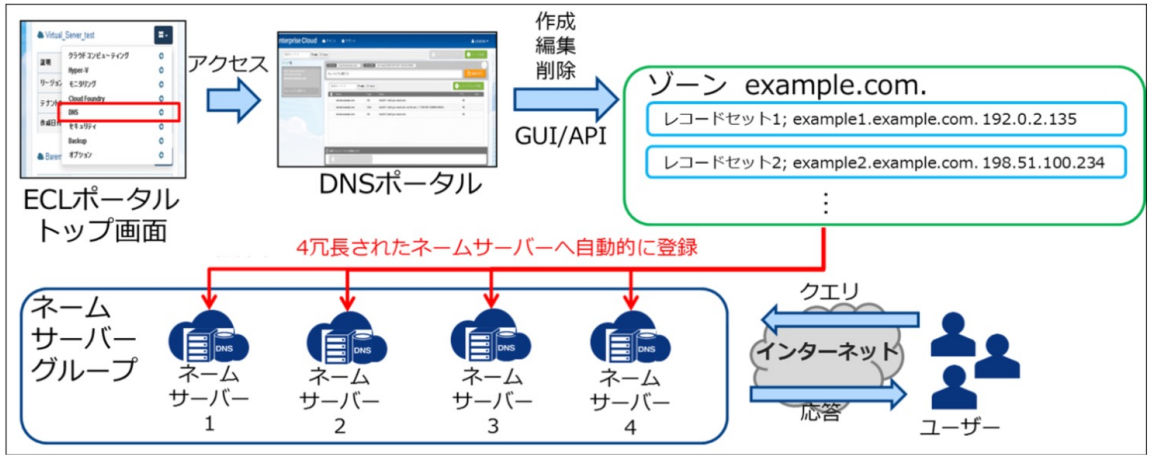
- 通常時の数百倍のリクエスト
- 大量アクセスは数時間継続

SDPF DNSのサービス概要

エンタープライズ向けクラウドサービスである、SDPFクラウドサービスの一部

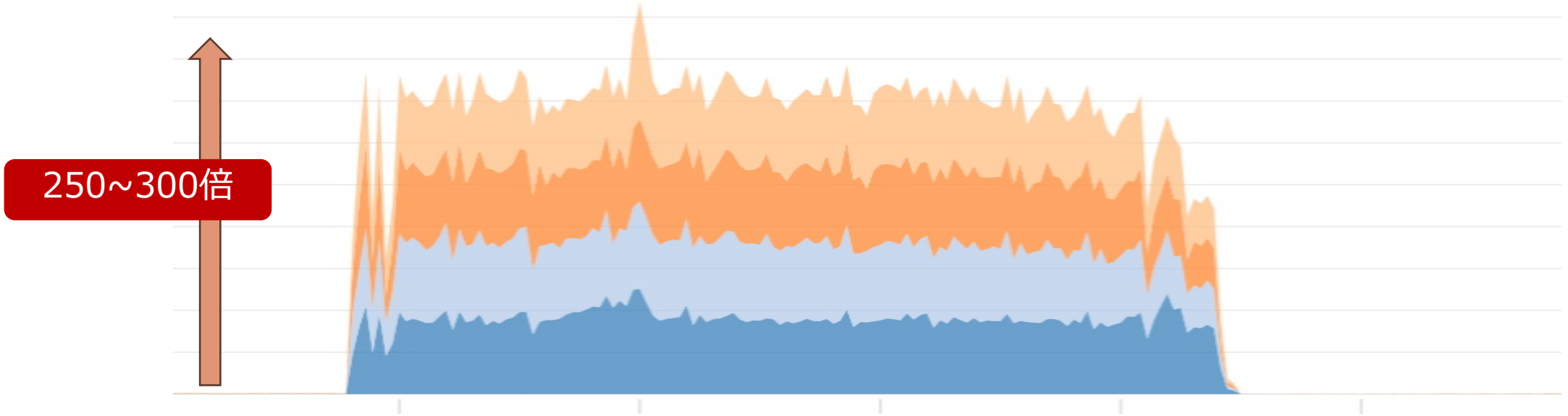
4拠点に冗長化され、Comのデータセンタ(SDPFクラウド上)で運用

権威DNSサーバ機能だけを提供。フルサービスリゾルバ（キャッシュサーバ）機能は提供していない
お客様のゾーン、レコード情報を簡単に管理できるポータルや、OpenStack互換APIを提供



観測された大量アクセスの特徴

- アクセスの量としては通常時250倍程度 (req/sec)
- 正しくNS Recordを引いてのアクセスであるため、4拠点に分散していても、清く正しく均等に大量アクセスが届く
- 送信元のIPアドレスは非常に多岐にわたる



アクセス例

バラバラなIPからのアクセス

ランダムな文字列(辞書?)を追加したアドレスへの名前解決

```
IP a.a.a.a.44826 > x.x.x.x.53: 53962 [1au] A? crodance.example.com. (67)
IP b.b.b.b.64554 > x.x.x.x.53: 6462% [1au] A? csRi-gODDardANCe.example.com. (74)
IP c.c.c.c.54380 > x.x.x.x.53: 47715% [1au] A? cBGSUANcE.example.com. (56)
IP d.d.d.d.44812 > x.x.x.x.53: 23544% [1au] A? cKfC1973-stoCkAnCe.example.com. (76)
IP e.e.e.e.21834 > x.x.x.x.53: 63233 [1au] A? cjendelamyance.example.com. (61)
IP f.f.f.f.46856 > x.x.x.x.53: 3157% [1au] A? CeCcmACancE.example.com. (69)
IP g.g.g.g.56400 > x.x.x.x.53: 38598% [1au] A? cweiLlAnCE.example.com. (68)
IP h.h.h.h.48977 > x.x.x.x.53: 27370 [1au] A? cchiefance.example.com. (69)
IP i.i.i.i.43589 > x.x.x.x.53: 44515% [1au] A? cxyzance.example.com. (66)
IP j.j.j.j.53501 > x.x.x.x.53: 33912 [1au] A? cfrancois04ance.example.com. (62)
IP k.k.k.k.39351 > x.x.x.x.53: 31086% [1au] A? ckillerwhaleance.example.com. (74)
IP l.l.l.l.36051 > x.x.x.x.53: 5947% [1au] A? cldhance.example.com. (55)
IP m.m.m.m.6308 > x.x.x.x.53: 37840 [1au] A? cpharmagossipance.example.com. (64)
IP n.n.n.n.41750 > x.x.x.x.53: 3924 [1au] A? catwance.example.com. (55)
```

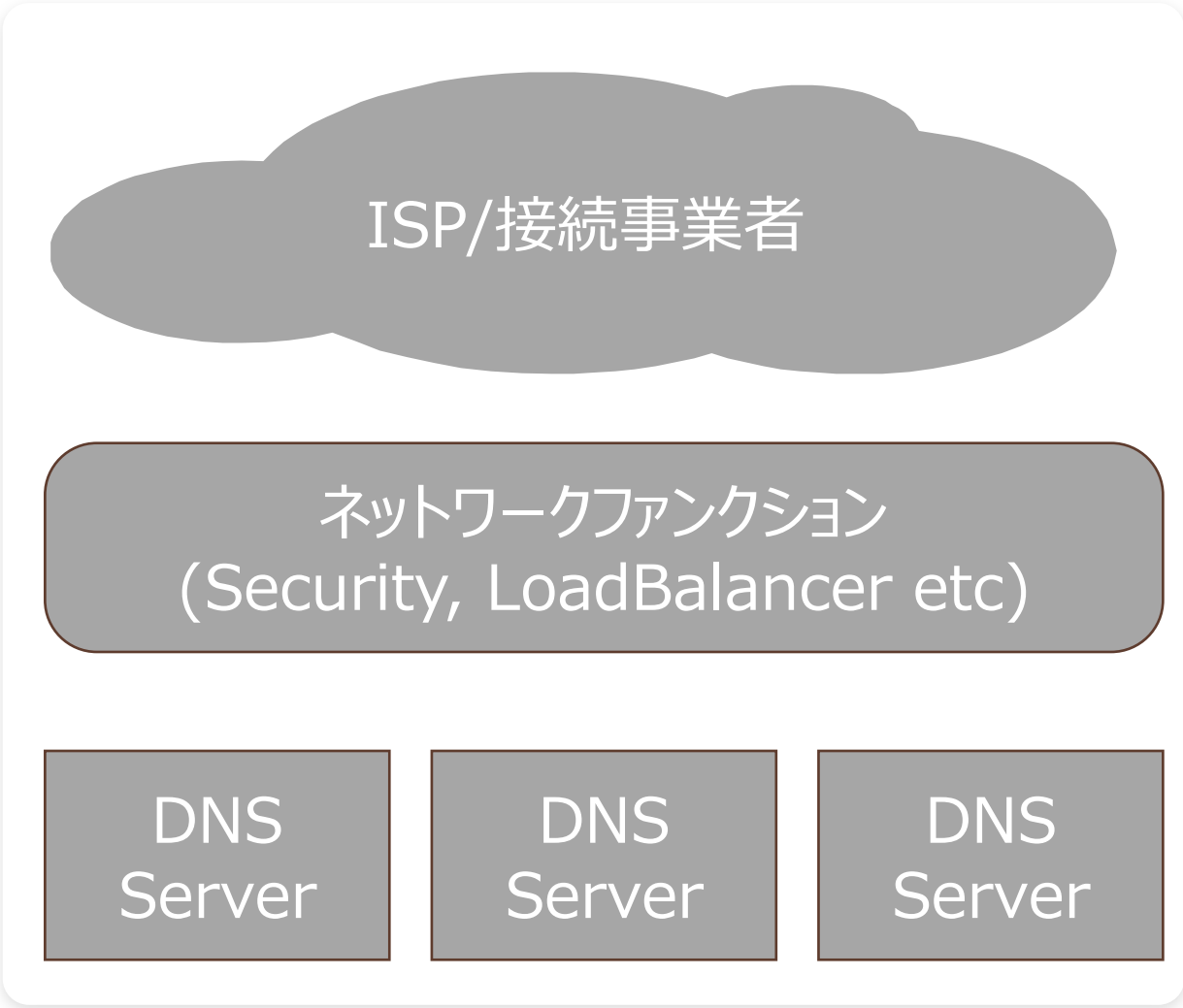
大量アクセスを観察しての気付き

処理に必要な性能

ネットワーク性能(帯域)

ネットワークファンクション

DNSサーバの処理性能



ネットワーク性能

増加したリクエスト量に比例してトラフィック量も増える

- 250倍のリクエストが来るということは、トラフィック量も250倍となる
- 清く正しいDNSクエリが届くため、我々が観測できた範囲では、bpsの総量としては数百Mbpsか1Gbps程度

通常時権威サーバはアクセス数はそれほど多くないが、上記のようなリスクは考慮した帯域設計が必要

- 特に複数のサービスでネットワークを共有している場合は、それらを加味した設計を

DNS サーバの性能

昨今のDNSサーバ(ソフトウェア) はどれも優秀で一定以上の性能が出る

- 正しくマルチコアが使える状況になっていることは確認が必要
- 通常時は権威サーバはアクセスがそれほど多くないが、リスクを考慮した上での試験は実施をしておくべき
  - 通常時の2倍から10倍ではなく、500倍程度は見越しておくことが良さそう

仮想環境でDNSサービスを提供している場合でも、アクセス急上昇時にスケールアウト or スケールアップするための準備をしておく

- 何事も避難訓練、練習をしておかないと急な対応は難しいものです
- スケールアウトは後述の通り少し注意が必要

ネットワークファンクション

現在のサービス、システムでは多くのネットワークファンクションが利用されている

- NAT, ロードバランサ、多くのセキュリティ対策製品
  - DNS Serverを冗長、スケールアウトさせるためのLoadBalancer
  - DNS Serverの自発通信(パッケージ取得や、各種SaaS利用など) は通すが、外部からの通信は制限したいStateful Firewall など
- 大量の送信元から、大量のアクセスが届く際に、ネットワークファンションが作成するセッションなどのState数とStateを作って、削除する処理が結構大変

本件に該当するような大量アクセスを考慮した設計、試験の実施

- リクエスト数のみを増やしたり、セッション数の数は準備するが増減が少ない試験では不十分
- なるべくセッションを維持しない (Stateを捨てる)設計も一つの方法

大量アクセスを観測した経験から

- 権威サーバに対して、通常の数百倍のアクセスが到達する
- 清く正しいDNSリクエストが大量に届くので
  - 拠点分散をしていても全てに均等にアクセスは届く
  - bpsはそれほど多くないが、全体のppsと送信元が非常に多いのが特徴
- 大量アクセスを受けるリスクを考え、各要素で準備が重要
  - ネットワーク、DNSサーバ、ネットワークファンクション

アジェンダ

1. ランダムサブドメイン攻撃とは
2. ハニーポットで観測した大量ランダムサブドメイン
3. クラウドサービスで観測した大量ランダムサブドメインの対策と教訓
4. 大量ランダムサブドメインの特徴とクエリ元の傾向
5. まとめ

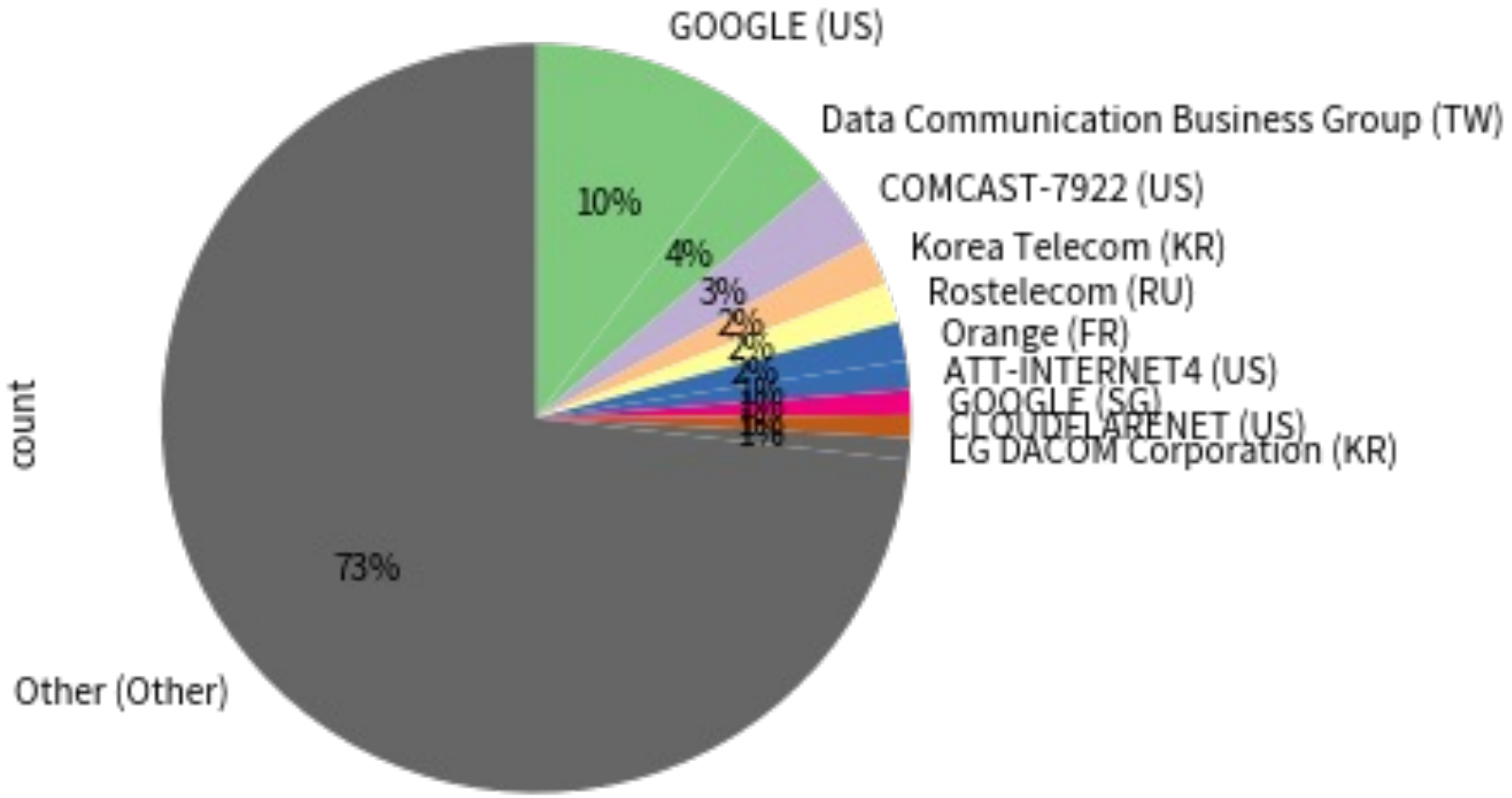
ある2秒間の観測データ

項目	件数
ユニークなクエリ元IPアドレス数	13,031

- クエリ元IPアドレスのうち
  - オープンリゾルバの割合：26%
  - 1回のみクエリのあったクエリ元IPアドレスの割合：40%
    - 最大で4,856回

クエリ元のAS(国)傾向

- パブリックDNSのバックエンドと考えられるIPアドレス多数



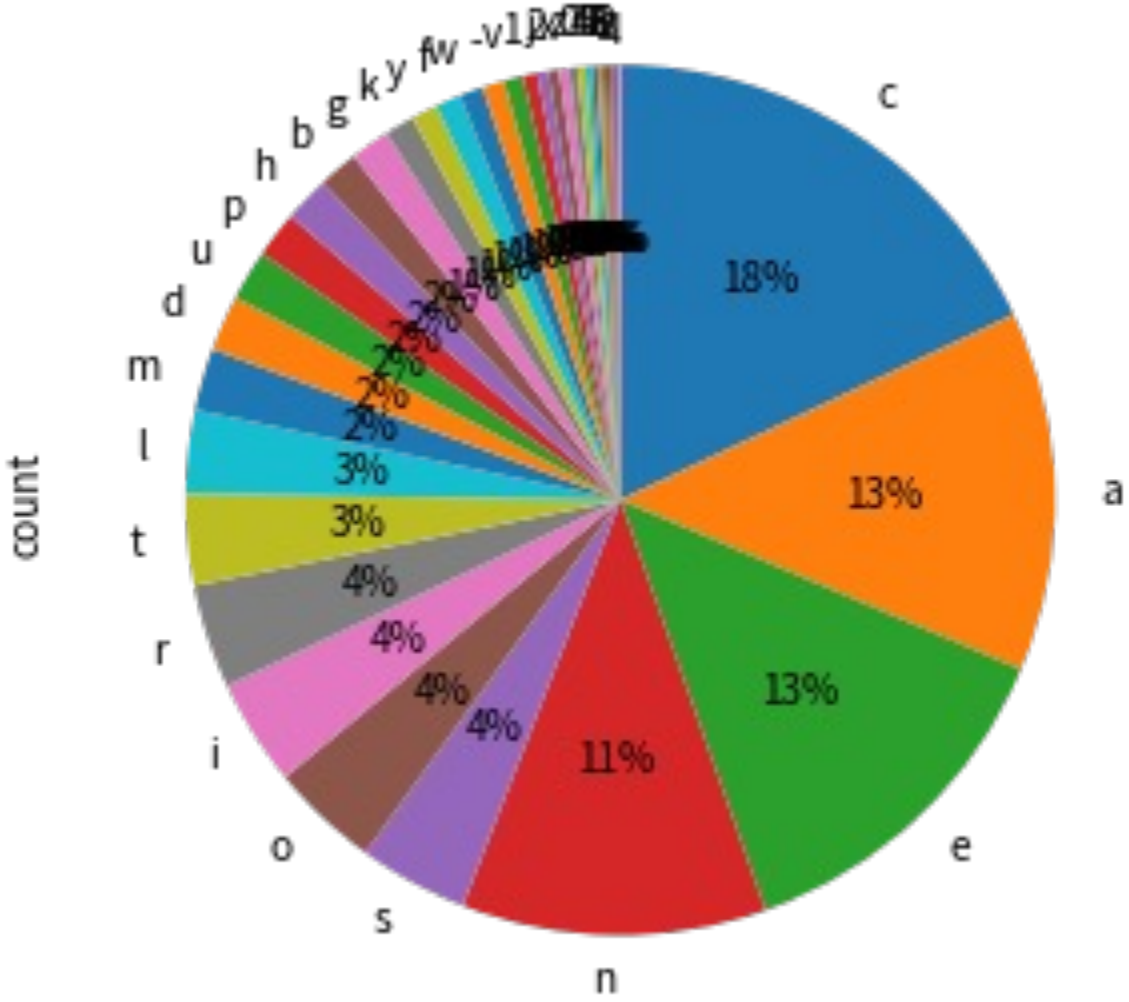
ある2秒間の観測データ

項目	件数
ユニークなサブドメイン数 (大文字小文字区別なし)	20,174

- サブドメインのうち
  - 4文字以上の英単語*を含む割合：76%　　例：c**littles****town**ance
  - 1回のみクエリのあったサブドメインの割合：45%
    - 最大で26回

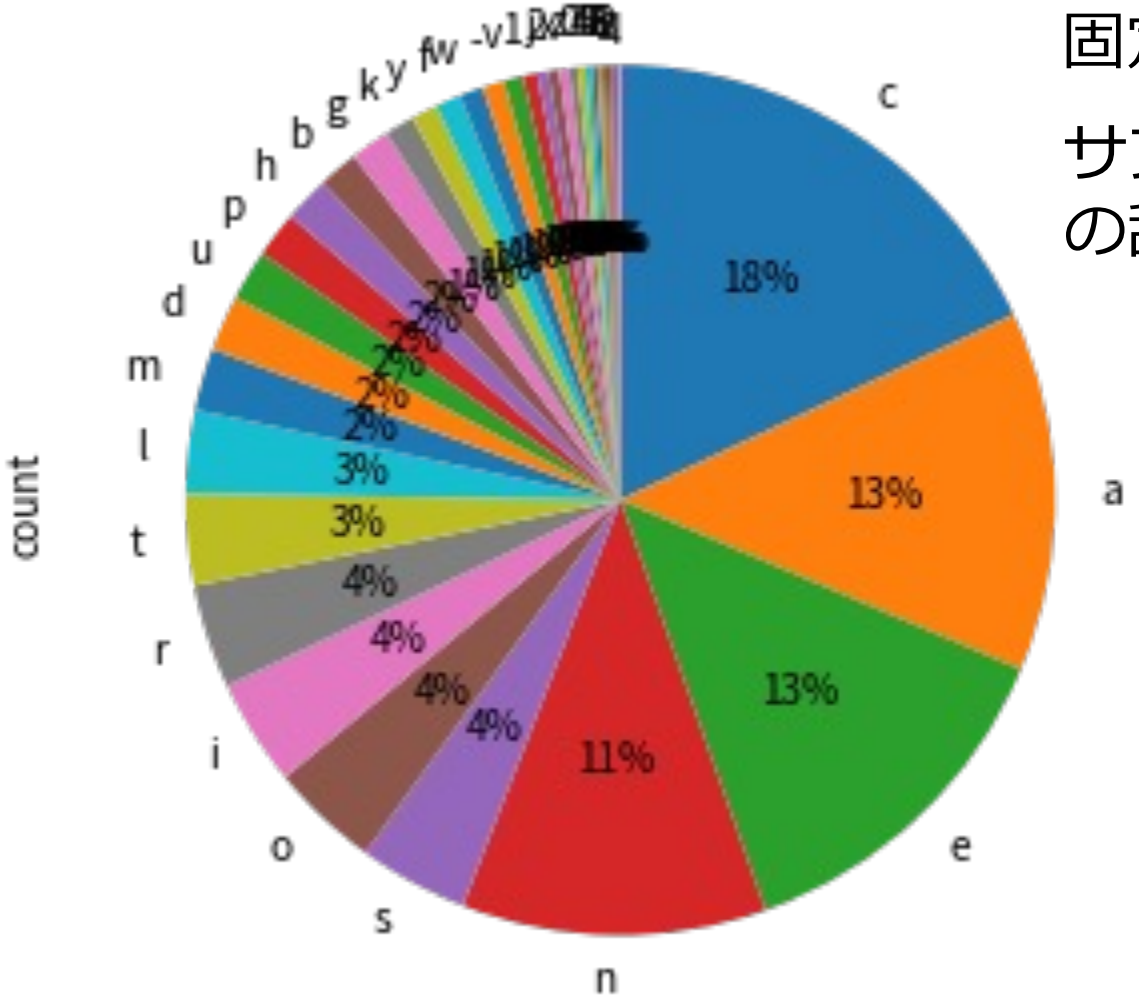
* https://pypi.org/project/english-words/

Q1: 何の割合でしょう？



A1: サブドメインに含まれる文字の出現傾向

- こんなに偏るもの？

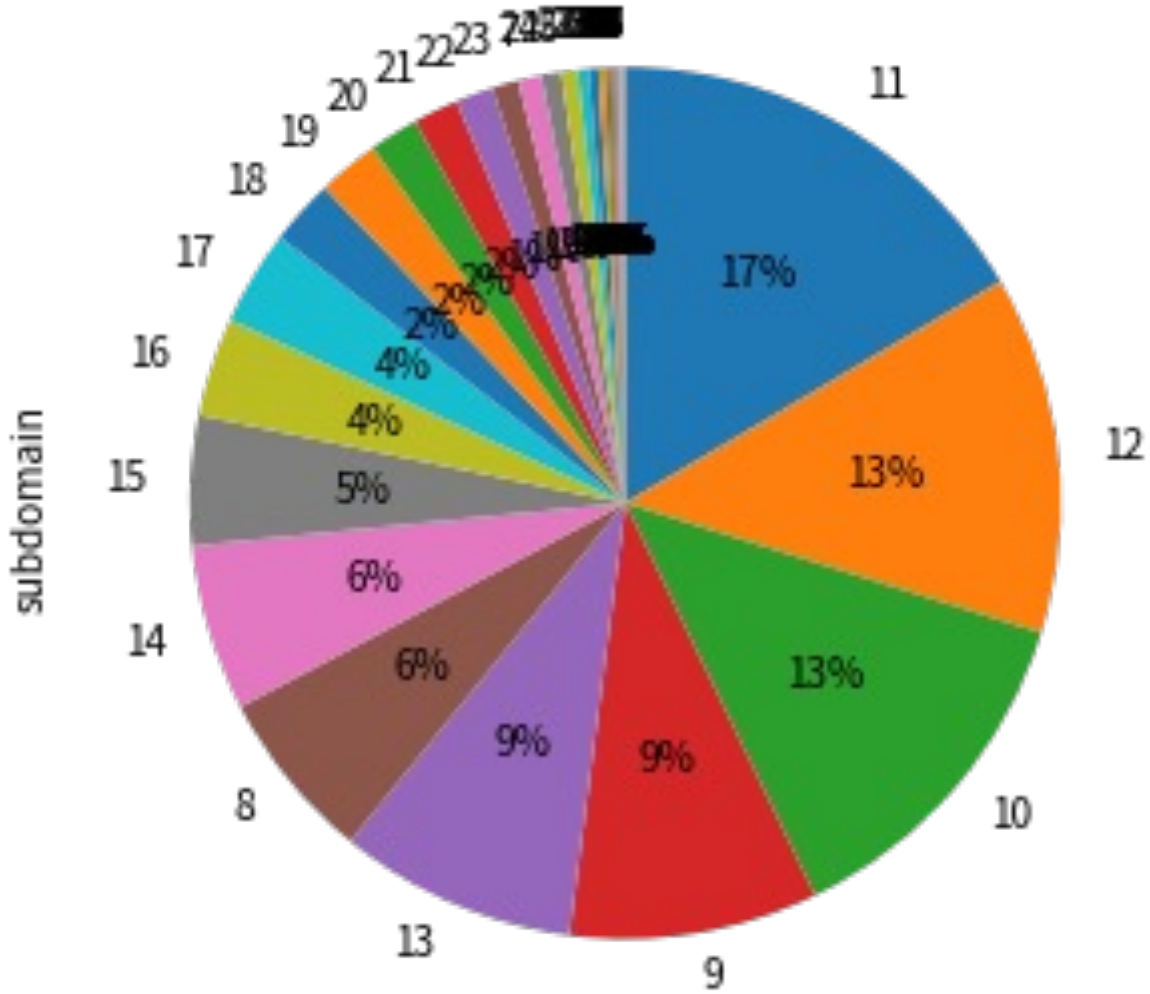


固定サフィックス“ance”

サブドメイン列挙ツールの辞書*を利用

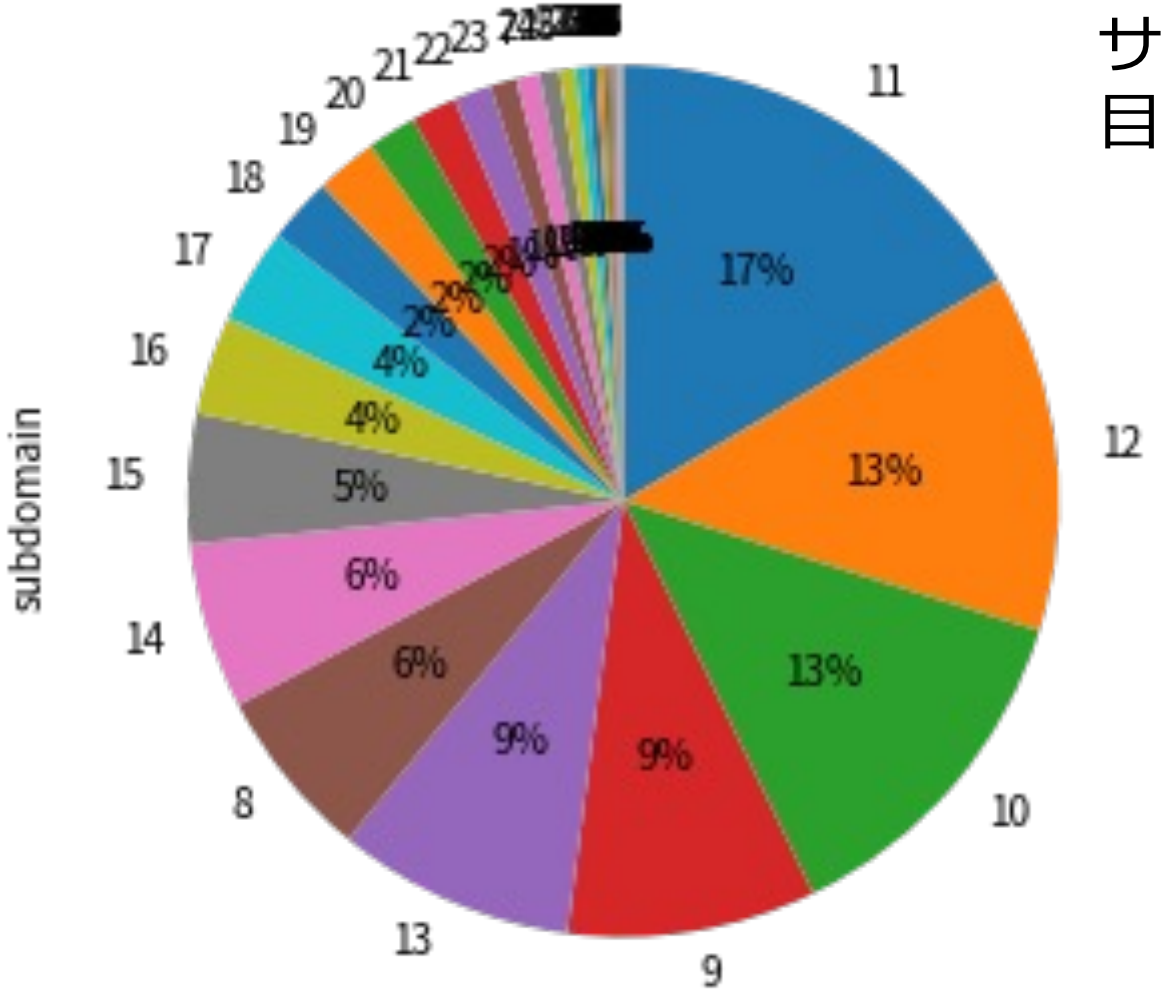
* https://github.com/TheRook/subbrute/blob/master/names.txt

Q2: 何の割合でしょう？



A2: サブドメインの文字数の傾向

- サブドメインとしては長め？



サブドメイン列挙とは
目的が異なる

分析してみてわかったこと

- クエリ元
  - やはりオープンリゾルバは悪用される
  - 偏りはあれどあちこちからクエリが来る
- サブドメイン
  - 真にランダムかというとそうでもない
  - 観測時期や観測環境によっても変わる

アジェンダ

1. ランダムサブドメイン攻撃とは
2. ハニーポットで観測した大量ランダムサブドメイン
3. クラウドサービスで観測した大量ランダムサブドメインの対策と教訓
4. 大量ランダムサブドメインの特徴とクエリ元の傾向
5. まとめ

まとめ

- ランダムサブドメイン攻撃とは、
  大量のランダムサブドメインクエリによるDDoS攻撃
- DDoSが目的とは限らないが、大量クエリの脅威は顕在化
- 権威DNSの運用には通常クエリの数百倍のトラフィック想定
- サブドメインの文字列的特徴から攻撃者の傾向がありそう
  - 早期の情報共有で、効果がある対策も共有できそう