TRILOGY
In collaboration with customer

JANOG37 Meeting in Nagoya Day3

DNS-OARC 2015 注目トピック

2016年1月22日

松浦洋一
株式会社テリロジー

DNS-OARC

目次

- 自己紹介
- どうしてこのセッションを企画したのか？
- セッションオーバービュー
- こんなセッションありました（注目セッションオーバービュー）
  - 暗号化・セキュリティ関連（さわりだけだよ）
    - An Overview of DNS Privacy Mechanisms
    - Using TLS for DNS privacy in practice
    - Next Steps in DANE Adoption
  - ベンチマーク関連ベンチマーク、パフォーマンス関連セッション（タイトルだけご紹介。説明は致しませんm(_ _)m
- DNSトラフィックをビッグデータとしてとらえる
  - DNS big data analytics
  - Managing DDoS Attacks
- ディスカッション

自己紹介

- 自己紹介
  - 名前
    - 松浦　洋一　（まつうら　よういち）
  - 所属
    - 株式会社テリロジー
    - ビジネスイノベーション部　momentumビジネス開発G
  - 担当
    - 自社開発パケットキャプチャ製品 「momentum」のプロダクトマネジメント、マーケティングを担当 。現在、パケット情報をDNSセキュリティに利用するプロジェクトを推進中。

どうしてこのセッションを企画したのか？

- DNSトラフィックのモニタリング、DNSセキュリティに注目しています！
- 大量のパケットから情報を抽出する＝ビッグデータ分析だとすると、どうやって分析するか情報がほしい
- 分析結果の利用についても、参考になるセッションがありそう！
- Privacyについても無視できない状況。。。

- 可視化なくして打つ手なし、という考え方について皆さんの意見を聞いてみたい（止めちゃえばいい？）
- Privacyの重要性が注目される＝解析できなくなる？？でも攻撃はやってくるんですよね。

こんなセッションありました
（注目セッションオーバービュー）

セッションオーバービュー

- NANOG & DNS-OARC（Montrealにて開催）に、弊社メンバー（US在住）が参加しました。
- この参加報告をもとに、DNSにまつわる面白そうなトピックについて、弊社なりの解釈を入れつつ解説を試みます。
- 弊社の好みが反映された選定となっていますので、一般的に面白いかどうかについては保証いたしかねます＾＾；
- 本資料中では、DNS-OARCで開催された各セッションの資料を抜粋で利用させていただいています。資料に関する各種権利については、保有者の主張に従います。
- 情報の正確さには正確さを保つよう努めていますが、“又聞き”による説明になりますので、最終的な情報の確認については必要に応じて各自でお願いいたします。

- 参考URL（DNS-OARCサイト）
  プログラム・資料ダウンロード
  https://indico.dns-oarc.net/event/24/timetable/#20151003.detailed
  公開ビデオ
  https://plus.google.com/+DnsoarcNetPlus/videos

NANOGとDNS-OARC

- NANOG65
  - 2015年10月5日～7日
  - ネットワークオペレータやコンテンツプロバイダ、約1000名が参加
  - DataCenter、Security、NetDevOps、IPv6など広くカバー
  - DNSに関しては半日に渡りDNS-OARCとセッションを共有
- DNS-ORAC
  - 2015年10月3日～5日
  - DNSに特化したコミュニティ。今回は約130名が参加。
  - DNS Privacy、DANE、EDNA、DNSSEC、DNS over TCP、DNS over QUIC、攻撃対策・解析など

DNS Privacy Overview

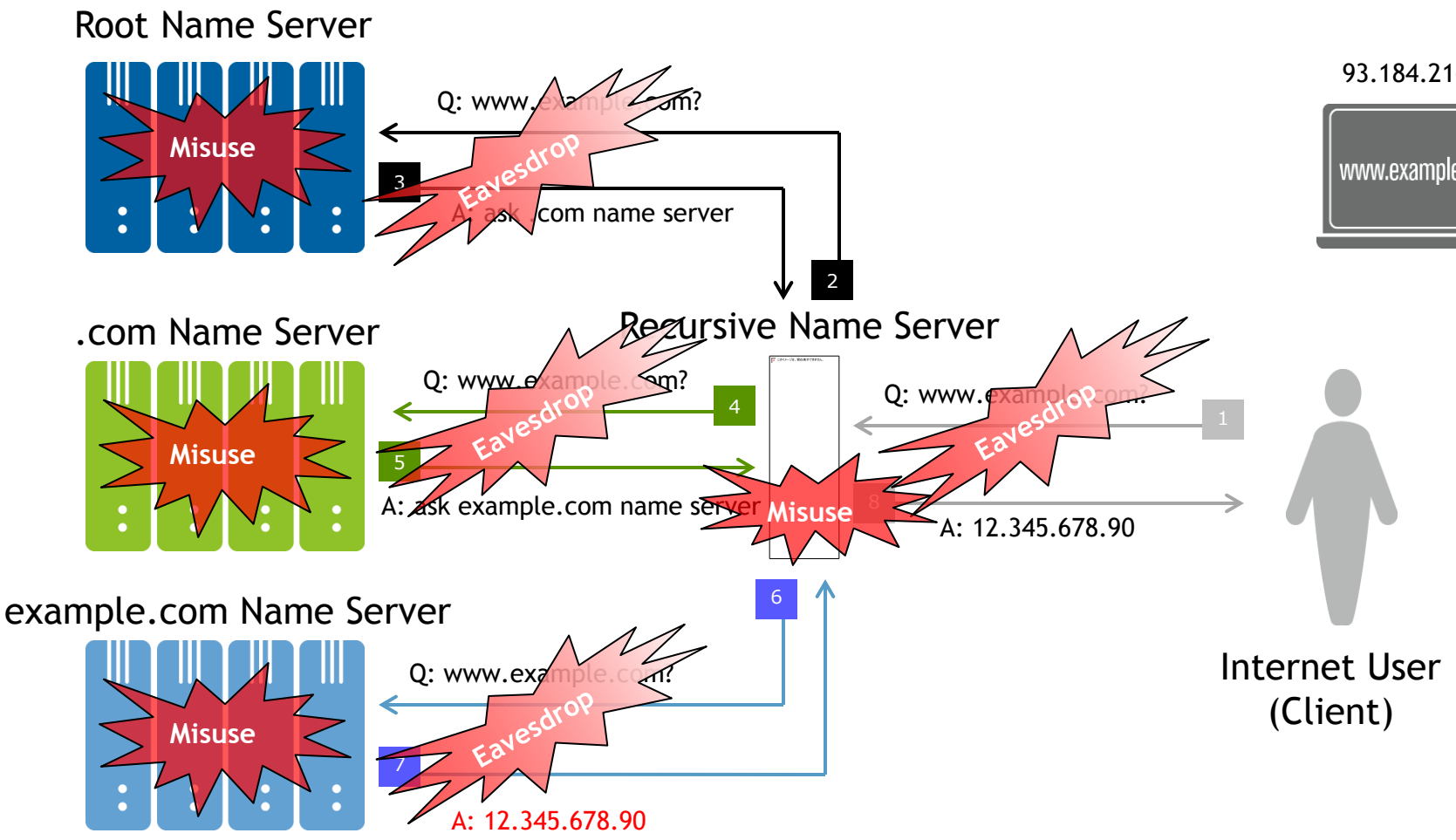
こちらの動画は https://www.youtube.com/watch?v=aoQx3UJ8qnE から
（5:50あたりから）

- Presenter : Allison Mankin & Shumon Huque, Verisign Lab

- DNSのセキュリティとプライバシー情報の扱いに関するセッション
- プライバシー関連RFC
  - DNSSEC(RFC 4033)、NSEC3、RFC 7258、RFC 7624、RFC 7626(DPRIVE@IETF)
- DNS Privacy Risk(どの部分が危険にさらされているか？)
- Riskの低減
- その他のRisk
- DNS以外のプロトコルで懸念されるRisk

- 【参考】IETFの活動報告
  - http://jprs.jp/related-info/event/2015/1207IETF.html

Summary of DNS system risks



https://indico.dns-oarc.net/event/24/session/6/contribution/24/material/slides/0.pptx から引用

こんなことも取り上げられた

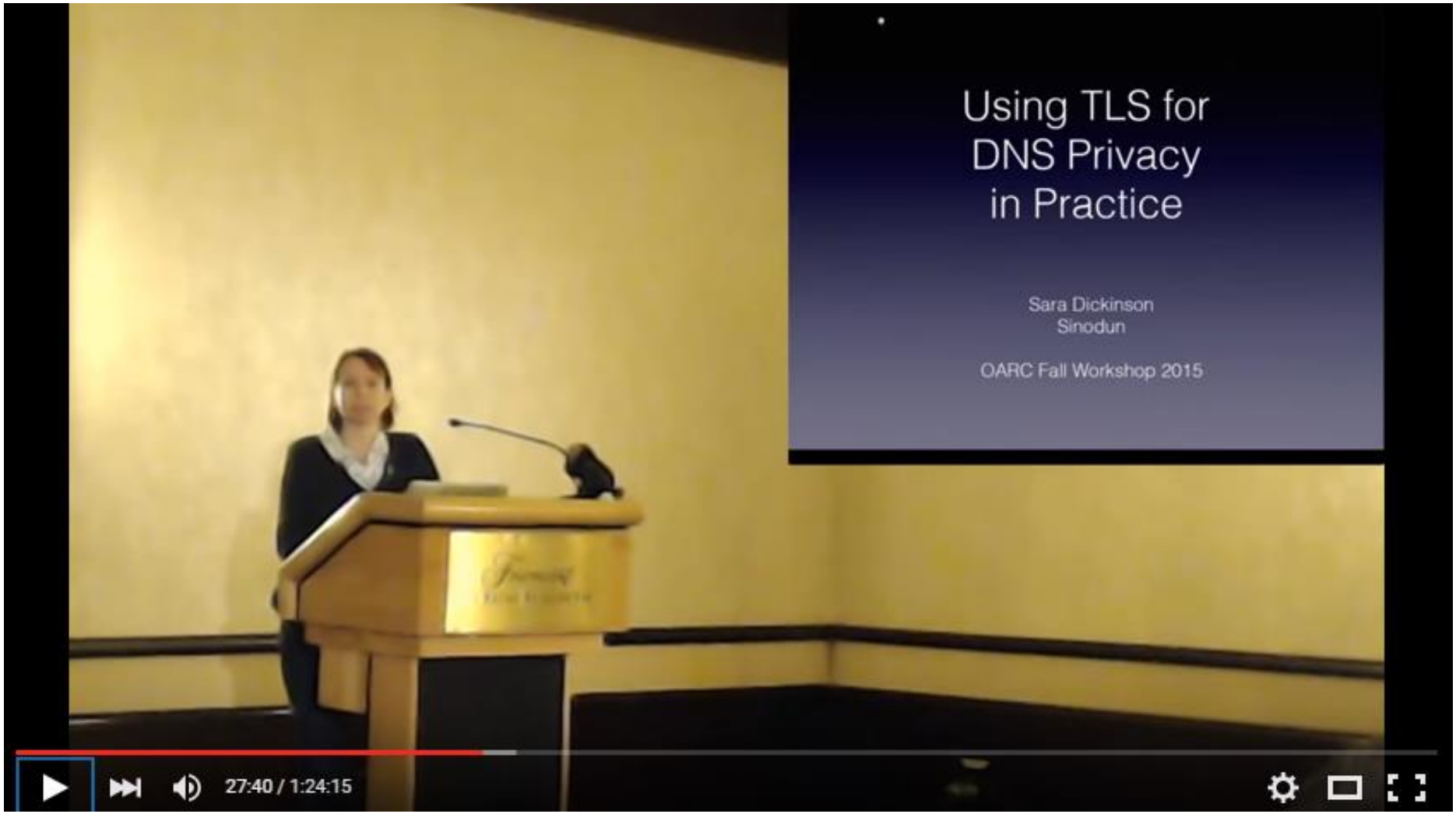
- リスク緩和の方法
  - Data Handling (ポリシー)
  - Query Confidentiality（暗号化）
  - Qname Minimization（問い合わせ内容の簡素化）

- Additional Risks and Mitigations
  - Enumeration *1
  - Size-based side channel（暗号化された情報を推測する攻撃）

*1 NSEC5 について⇒ https://www.youtube.com/watch?v=t4tro7BP6CA

- Domain Name Leakage in Other Protocols
  - TLS server name extension（TLS通信に含まれるドメイン名は平文）
  - DHCP FQDN option （DHCPでも同様のリスク）

Using TLS for DNS privacy in practice



こちらの動画は https://www.youtube.com/watch?v=aoQx3UJ8qnE から
（27:35あたりから）

- Presenter : Sara Dickinson, Sinodun
- TLSを利用する場合気になるのは
  - DNSとしてのパフォーマンスが十分か
  - DNSサーバがTCPコネクションを扱うための負荷に耐えうるか
- パフォーマンスを上げるには
  - クライアントからのリクエストの並列処理（Pipelining）
  - RecursiveとAuthの間の処理の並列化（OOOR）
  - コネクションの開始と再利用の高速化（RFC7413,RFC5077）
  - その他（サーバコネクション管理/keepalive、カーネルチューニング）
- 実装
  - Unbound DNSSEC-Trigger
  - LDNS と NSD TLS patches
  - getdns
- TLS BCP（RFC7525）
  - TLS v1.2（v1.1、V1.0やSSLは使わない）
- TLS v1.3

T-DNS: Connection-Oriented DNS to Improve Privacy and Security (extended)

tionally to authoritative servers. Expectations about DNS suggest connections will balloon client latency and overwhelm server with state, but our evaluation shows costs are modest: end-to-end latency from *TLS to the recursive resolver is only about 9% slower* when UDP is used to the authoritative server, and 22% slower with TCP to the authoritative. With diverse traces we show that frequent connection reuse is possible (60–95% for stub and recursive resolvers, although half that for authoritative servers), and after connection establishment, we show TCP and TLS latency is equivalent to UDP. With conservative timeouts (20 s at au-

http://www.isi.edu/publications/trpublic/files/tr-693.pdf から引用

Current status

Software	digit	LDNS	getdns		Unbound		NSD	BIND
mode	client	client (drill)	stub	recursive*	server	client	server	server/ client
TLS								
TFO								
Conn reuse								
Pipelining								
OOOP								

Dark Green: Latest stable release supports this
Light Green: Patch available
Yellow: Patch in progress, or requires building a patched dependancy
Grey: Not applicable or not planned

* getdns uses libunbound in recursive mode

https://indico.dns-oarc.net/event/24/session/6/contribution/25/material/slides/0.pdf から引用

Next Steps in DANE Adoption

こちらの動画は https://www.youtube.com/watch?v=aoQx3UJ8qnE から
（57:40あたりから）

- Presenter: Shumon Huque, Verisign Labs
- DANEの前提条件⇒DNSSEC
  - TLDの85%程度が署名完了（2015年9月時点）、逆引きやRIRレベルに委譲されているゾーンも署名されている
  - TLD以下の状況はすこぶる悪い（.NL、.BR、.GOVは例外）
  - TLSAゾーンの数は増えているが署名されているものはまだ少ない
  - 使い方はDANE-EEがほとんど
- DANEの新しい動き
  - OPENPGPKEY、SMIMEAのサポート
  - DANE for SIP
  - Client証明書
  - DANE/DNSSEC Chain Extension for TLS
  - Payment Association (PMTA)
- 今後の課題
  - 他のアプリケーション
  - DANEのソフトウェア面でのサポート
  - などなど

Source	#Zones	#Signed	%Signed	#TLSA zones	%TLSA of signed
COM	118m	524k	0.44%	4100	0.78%
NET	15m	94k	0.63%	1432	1.52%
Alexa 100k	~100k	1039	1.04%	44	4.23%

#TLSA zones: #signed zones that have deployed at least 1 TLSA record.
%TLSA of signed: What percentage of the signed zones are they.

Source	#TLSA records	#TLSA RRsets
COM	6,340	5,516
NET	2,583	2,279
Alexa 100k	120	118

Comparing COM+NET with previous study:

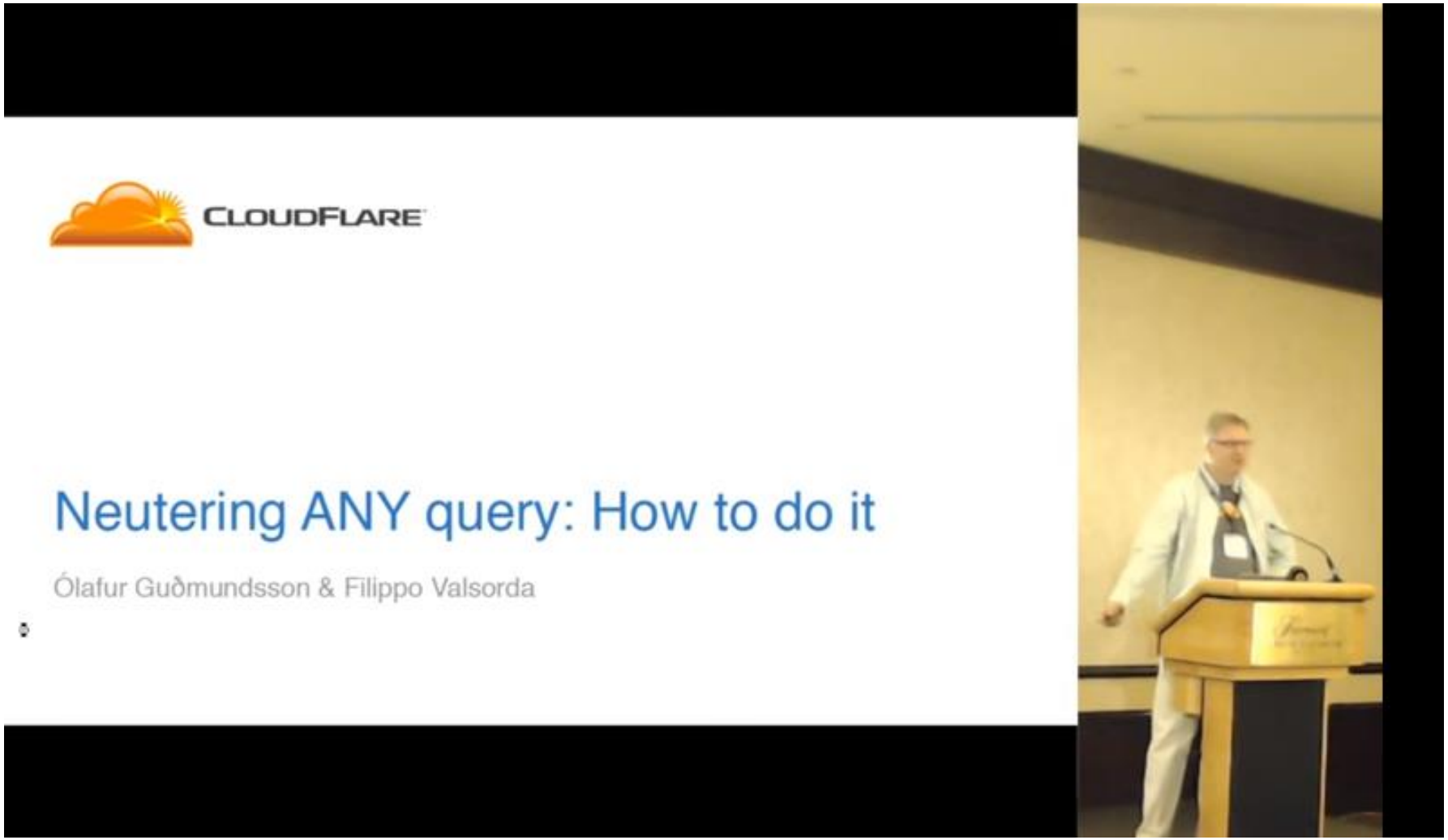
7795 TLSA names vs 1533
5532 zones vs 565

https://indico.dns-oarc.net/event/24/session/6/contribution/23/material/slides/0.pdf より引用

ベンチマーク、パフォーマンス関連セッション

- DNSのパフォーマンスに関するセッションも多く行われていました
  - Benchmarking of authoritative DNS servers and DNSSEC impact assessment
    - CZ.NICが開発しているKNOT DNS authoritative DNS serverのベンチマーク結果の報告
  - Impact of unknown EDNS options on the DNS
    - ISCで実施された、不明なEDNSオプションが使用された場合のEDNS failure mode の検証内容と結果の報告
  - Benchmarking and profiling DNS systems with modern Linux tools
    - netsniff-ng toolkit や自家製ツールの利用法と、これらを使ったベンチマークの結果を報告
  - Impact of DNS over TCP - a resolver point of view
    - TCPを利用したリカーシブサーバの効果を測定してみる

Neutering ANY query: How to do it



こちらの動画は https://www.youtube.com/watch?v=Gt9VUPDoZk0 から
（1:01:20あたりから）

from “Neutering ANY query: How to do it” by Ólafur Gudmundsson & Filippo Valsorda, CouldFlare

TERILOGY
In collaboration with customer

DNSトラフィックを
ビッグデータとしてとらえる

- ビッグデータ処理システムとしてのENTRADA

DNS Big Data Analytics

こちらの動画は https://www.youtube.com/watch?v=LLDGbnxOmwc から
（28:15あたりから）

- Presenter: Maarten Wullink, SIDN

- 目次
  - ENTRADAとは
  - ENTRADAで利用している技術
  - ENTRADAアーキテクチャ
  - Privacyフレームワーク
  - ワークフロー
  - パフォーマンス
  - 利用用途
  - サンプルアプリケーション

- 各ページの図表などは
https://indico.dns-oarc.net/event/24/session/9/contribution/18/material/slides/1.pptx
から引用しています

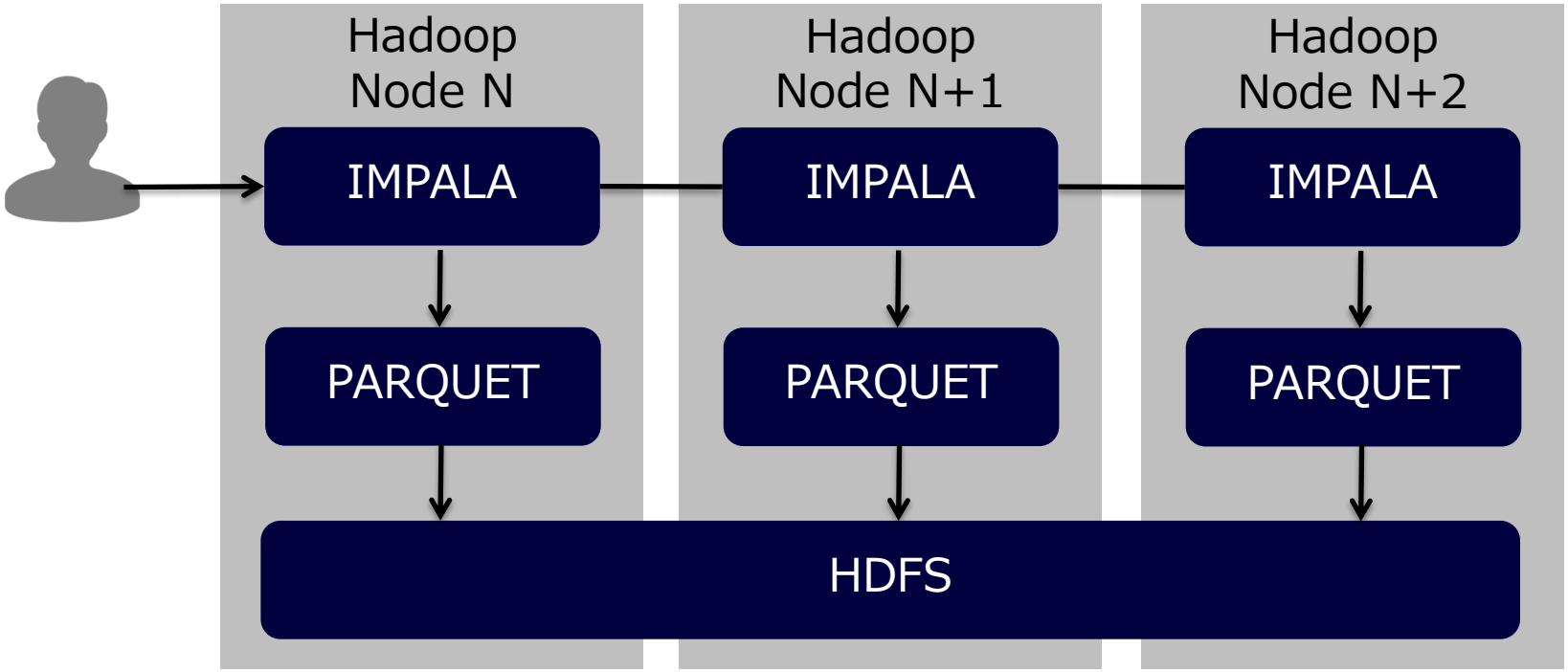
ENTRADAとは

- オランダのSIDNが開発したDNS情報解析のためのシステム
- SIDNは
  - 560万のドメインネームを管理する、世界第7位のTLDを管理
  - .nl domain において245万の DNSSECレコードを扱っており、これは世界で最も大きなDNSSECゾーン保持数である
- ENTRADA=
  - ENhanced Top-Level Domain Resilience through Advanced Data Analysis
- SIDNは大量のクエリを取り扱っている
  - 3.1 million distinct resolvers
  - 1.3 billion query's daily
  - 300 GB of PCAP data daily
- ENTRADA開発の理由
  - データをもとにしたセキュリティ強化を実現するための、ビッグデータに対応したツールがなかった
  - PCAPそのものを使わず、処理しやすいフォーマットに変換することで、ハイパフォーマンスでニアリアルタイム処理が可能なものを目指した

ENTRADAで利用している技術

- 要件
  - SQL support
  - Scalability
  - High performance
  - Capacity for >1 year of DNS data
  - Extensibility
  - Stability
  - Don’t spend too much money!
- SQL on Hadoop
  - HDFS
  - Impala
  - Parquet(パーケイ)

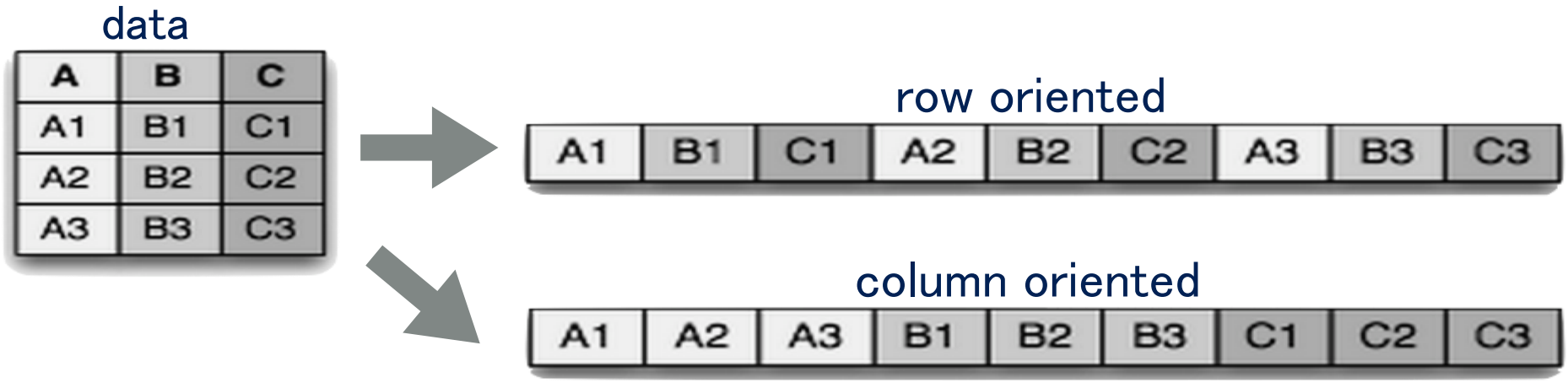
SQL on Hadoop



- parquetはカラムナ型DBであり、本システムのデータに非常によくマッチしパフォーマンスに貢献している
- Hadoop HDFS分散ファイルシステムは fault tolerance、 redundancy、scalabilityに貢献している
- ImpalaはSQLの大量並列処理エンジンであり、システムのパフォーマンスとSQL互換に貢献している
- クエリーはすべてのノードに配信され、各impalaは自身のノードにあるデータに対してのみ処理を実行。これにより無駄なネットワークIOが減る。

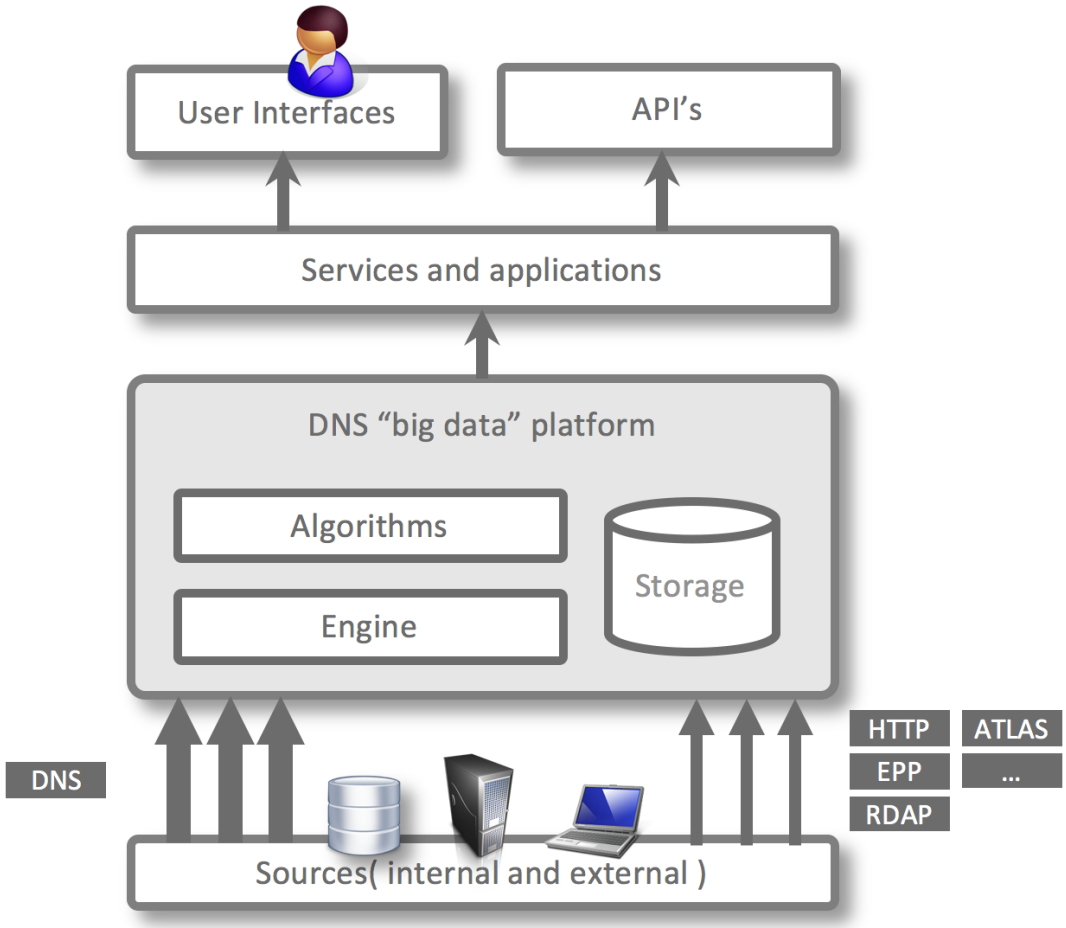
ENTRADAはPCAPを直接使わない

- PCAPデータの読み込みは時間がかかる処理
- 分析システムはPCAPそのものを読み込むことができない
- カラムナ（カラムオリエンテッド）は、集計・分析に向いている
- データ圧縮効率も高い（同じようなデータが連続するので）
- ImpalaでparquetのデータフォーマットをしてできるImpalaでparquetのデータフォーマットをしてできる



ENTRADAアーキテクチャ

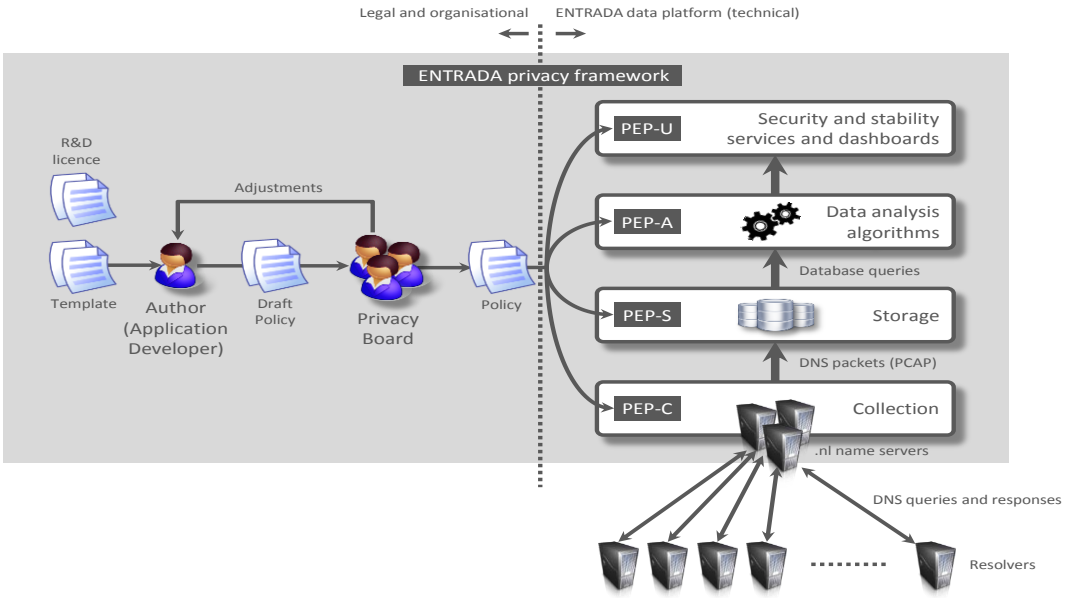
- 現在はDNSデータとICMPデータのみ対象
- ENTRADAのメインコンポーネント
  - Applications and services
  - Platform
  - Data sources
  - Privacy framework



Privacyフレームワーク

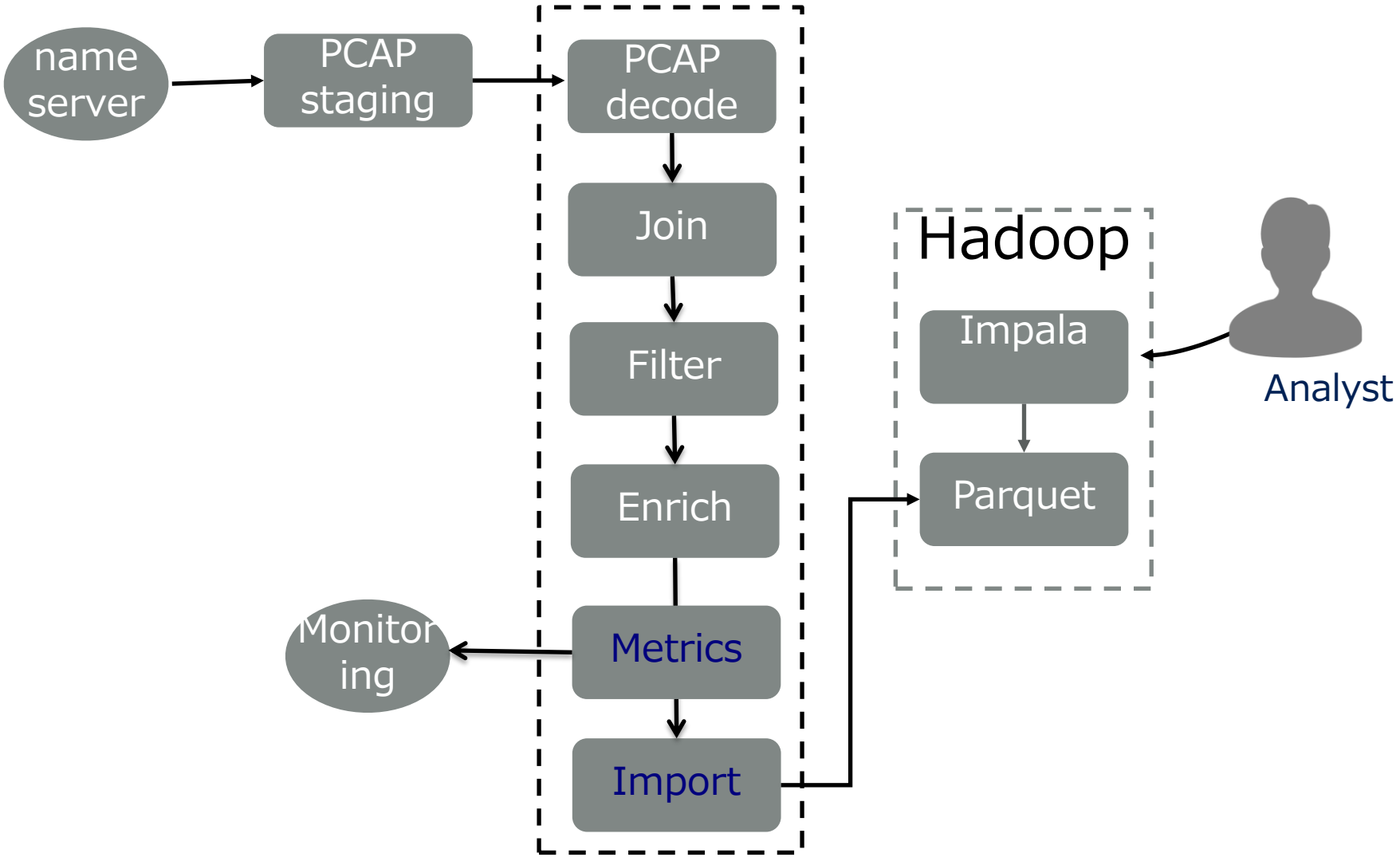
- Dutch Data Protection Ack（オランダ語の略称はWBP） による規制
  - 個人情報の定義(*)
    - ‘any piece of information regarding an identified or identifiable natural person’ and the processing of personal data as ‘any action or sequence of actions involving personal data, including but not restricted to the collection, recording, sorting, […] deletion or destruction of such data’

* https://www.sidnlabs.nl/SIDN_Labs_Privacyraamwerk_Position_Paper_V1.4_ENG.pdf



レイヤごとにPEP（policy enforcement point) を設置し、Privacyデータをフィルタできる仕組みを実装

ワークフロー

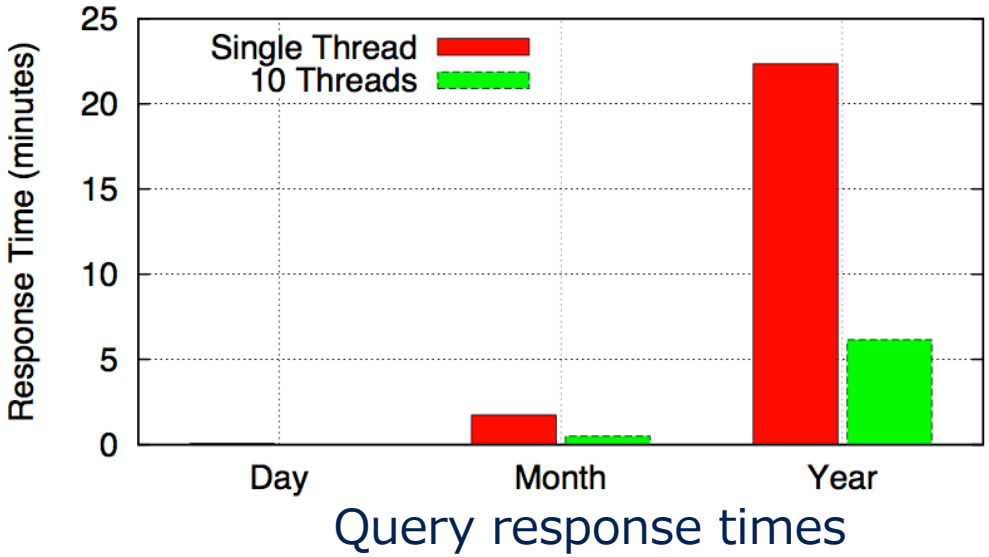


Query data available for analysis within 10 minutes

パフォーマンス

Example query, count # ipv4 queries per day.

```
select concat_ws('-
',day,month,year), count(1)
from dns.queries
where ipv=4
group by concat_ws('-
',day,month,year)
```



Query response times

1 Year of data is 2.2TB Parquet ~ 52TB of PCAP

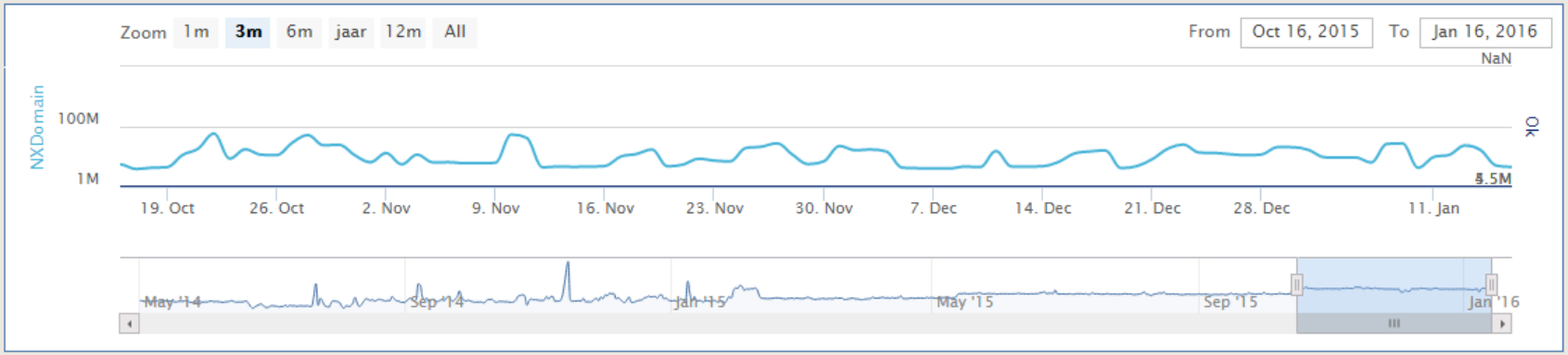
利用用途

- DNSトラフィックパターンの可視化 (フィッシングサイトに対するトラフィックパターンなど)
- ボットネットの影響を検出
- フィッシングのリアルタイム検出
- Statistics (stats.sidnlabs.nl：次の2ページで紹介)
- Scientific research (collaboration with Dutch Universities)
- Operational support for DNS operators

statsグラフ（ http://stats.sidnlabs.nl/#dns）

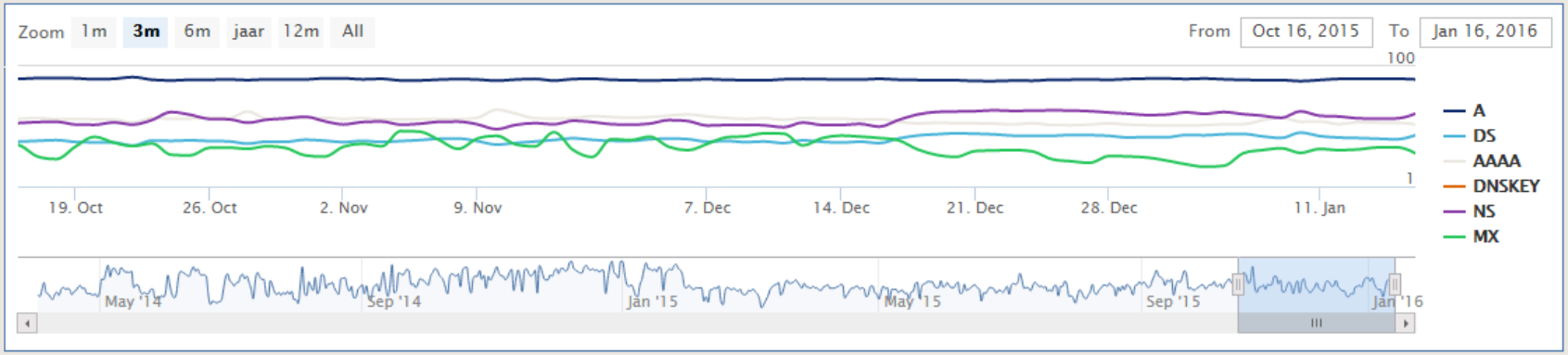
Unique domain names

How many unique domain names are queried each day? This chart shows how many unique **existing** domain names are queried each day (response code "Ok"). Also displayed is the number of **non existing** unique domain names (response code "NXDomain"). The queries for non existing domain names show a much more unpredictable pattern.



Query type

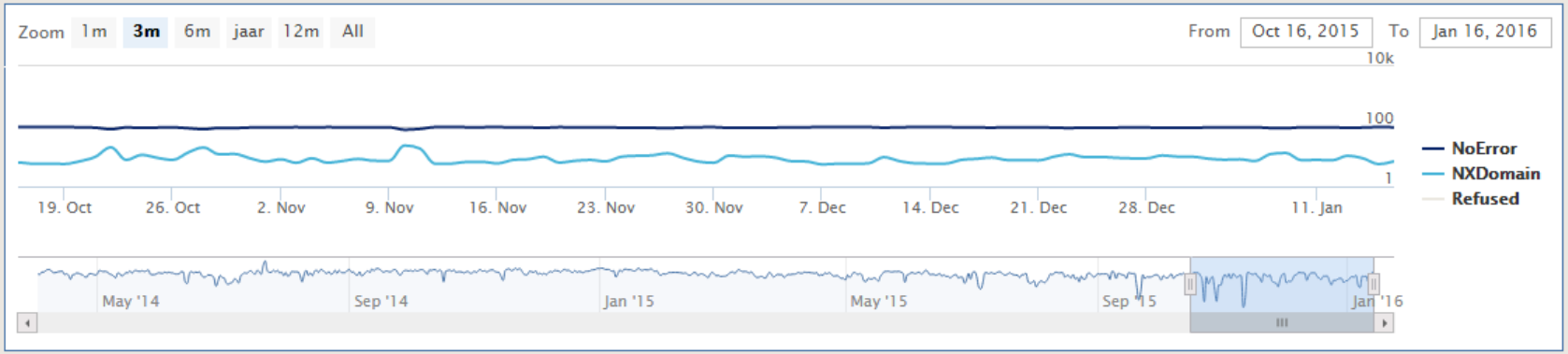
Each DNS query contains information about the type of response required from the server, this is called the query type. If we look at a query for a version 4 IP address, the query type will be "A" and for locating the mail server for a domain name the query type "MX" is used. This chart show how often the most common query types are requested. More information about DNS resource record types.



statsグラフ（ http://stats.sidnlabs.nl/#dns）

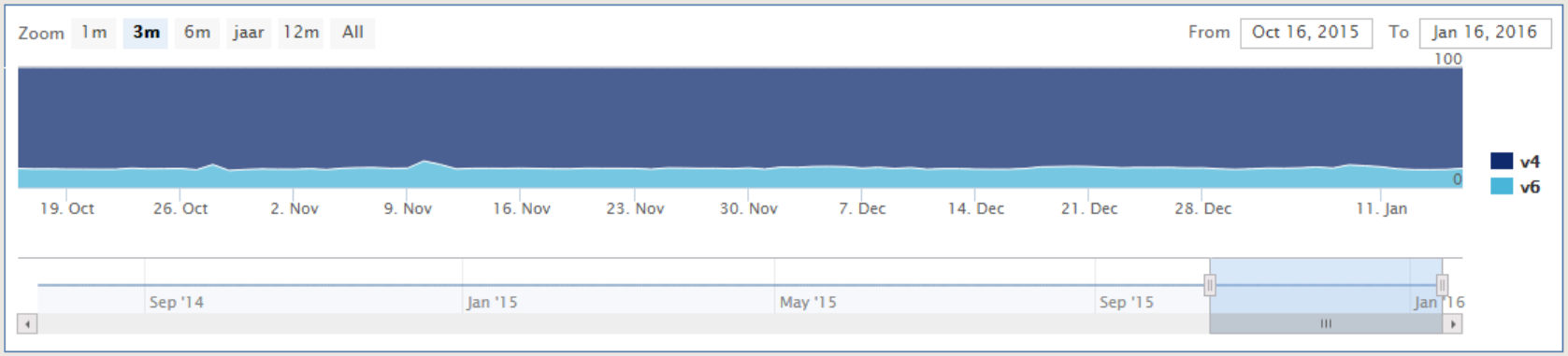
Response code

The response for a DNS query contains a response code which indicates if the query was successfully processed (response code "Ok").
Other response codes include "NXDomain" for non existing domain names and "Refused" for queries which are not accepted by the server.
There are more DNS response codes but they are only used in a small percentage of all queries.

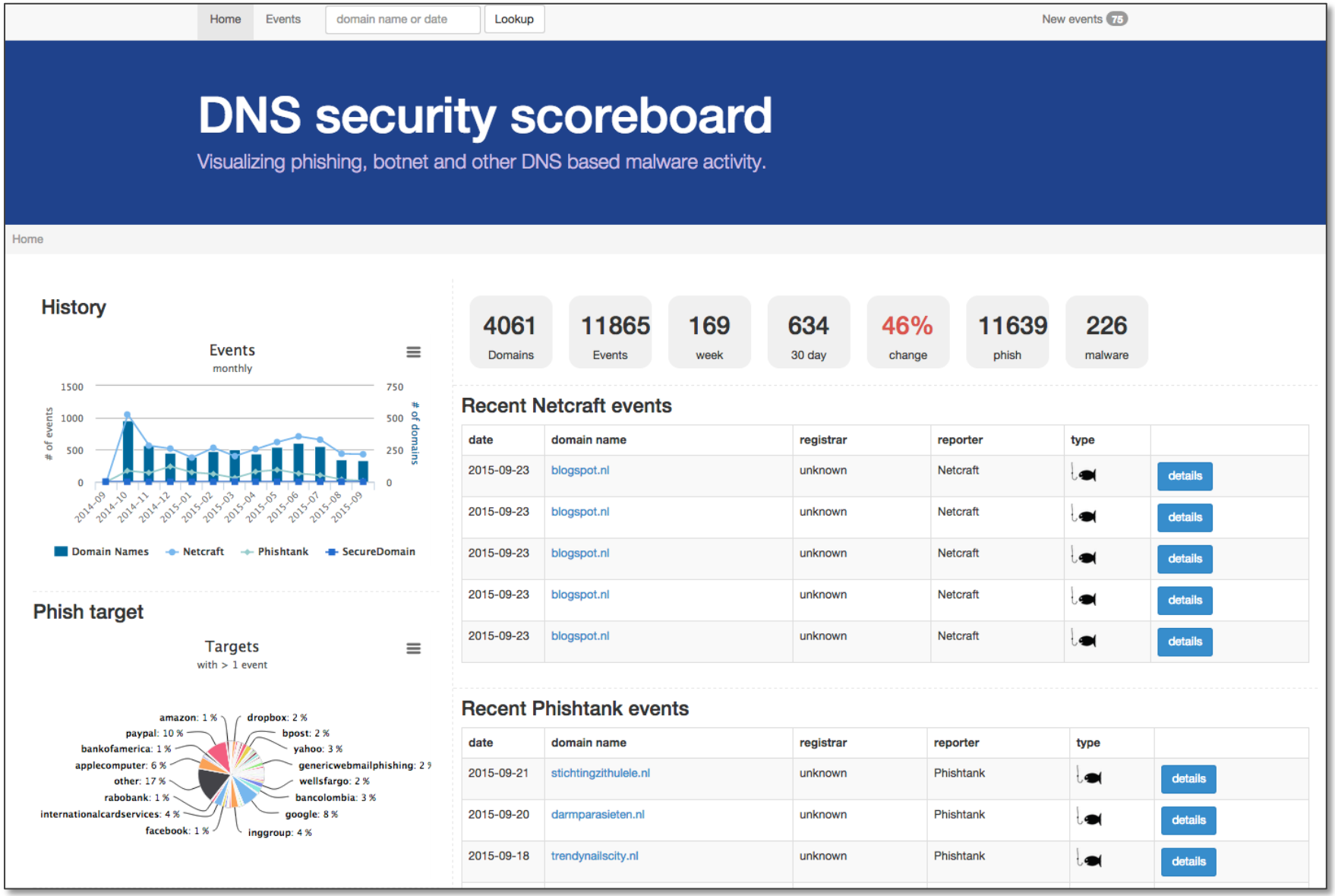


Queries by resolver IP version

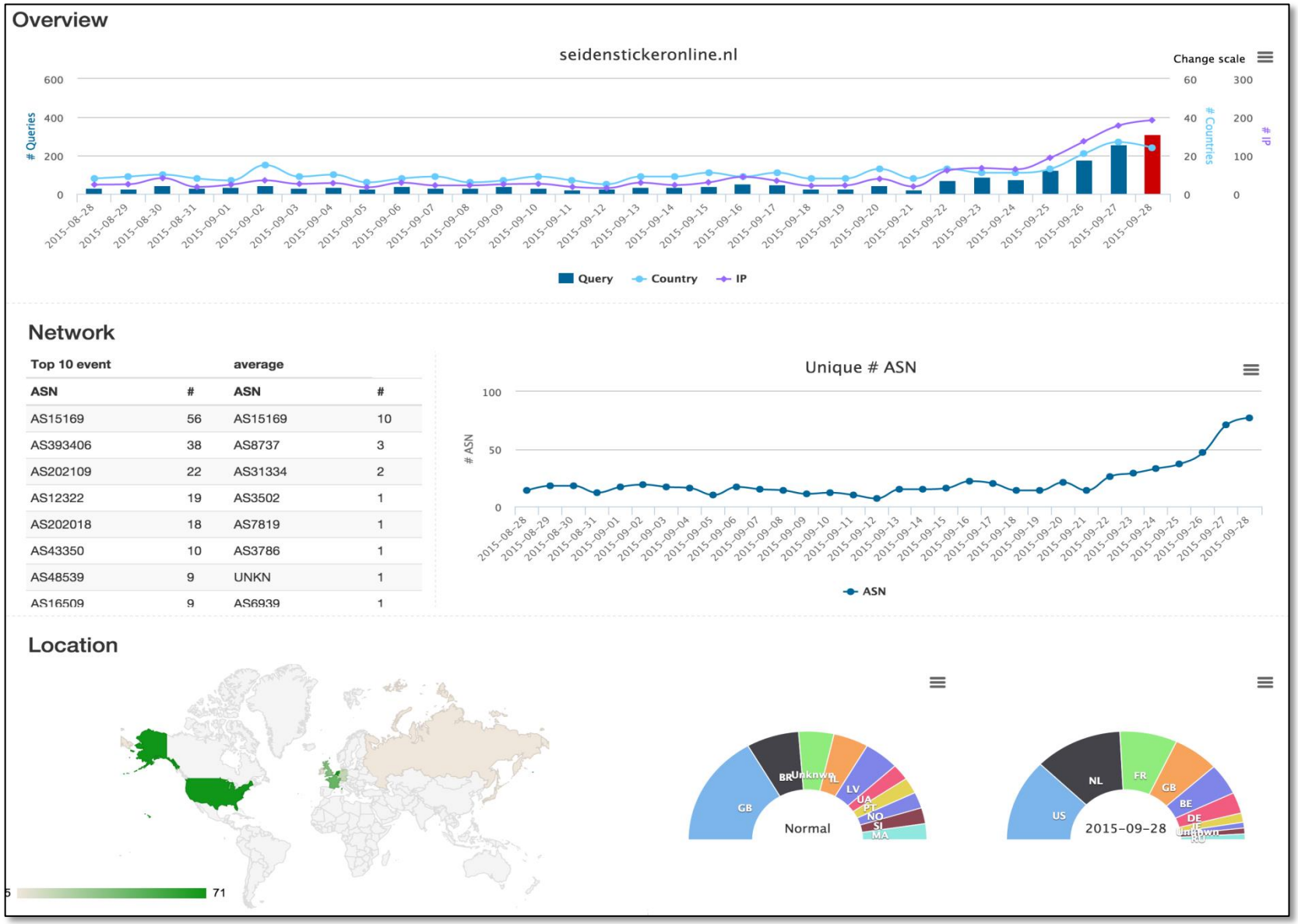
Because the world is running out of IP version 4 addresses, a new IP version 6 has been developed some time ago. The IP version 6 adoption is still quite low.
This chart shows the percentage of queries sent by resolvers using an IP version 6 address.



サンプルアプリケーション



サンプルアプリケーション



Managing DDoS Attacks

こちらの動画は https://www.youtube.com/watch?v=Gt9VUPDoZk0 から
（6:40あたりから）

- Presenter: Brian Somers, OpenDNS

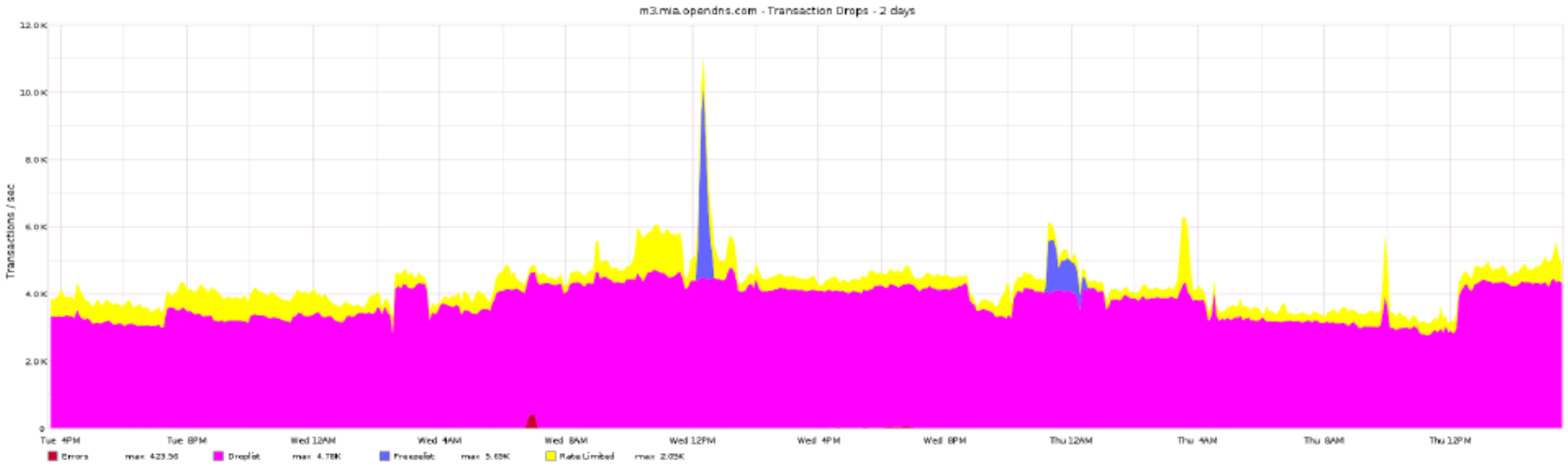
- 目次
  - 攻撃の分類
  - 攻撃への対処としてのRate Limiting
  - ランダムドメイン攻撃のグローバル検知
  - Domain Dropリスト
  - Domain Freezeリスト
  - グラフ
  - AuthoritativeのRTTを利用する（SERVFAILにしないために）
  - 攻撃を可視化してみる
  - これからの改善
- おまけ：DNS Veiwer by テリロジー

各ページの図表などは
https://indico.dns-oarc.net/event/24/session/8/contribution/13/material/slides/2.pdf
から引用しています。

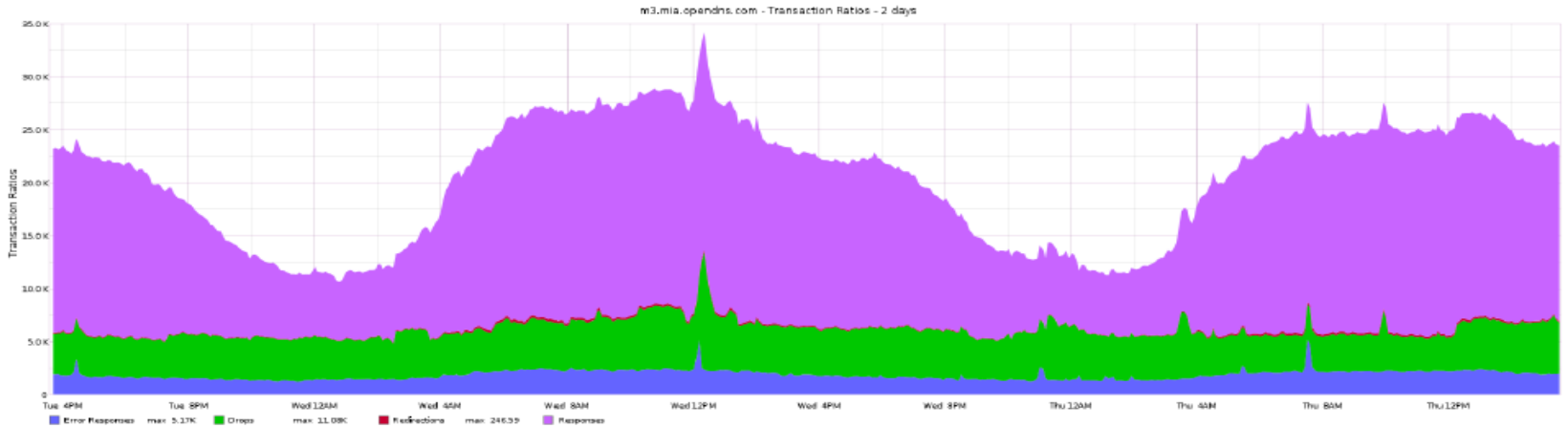
- 攻撃の分類
  - 偶発的攻撃
  - Amp攻撃
  - NXDOMAIN攻撃（＝ランダムドメイン攻撃＝水責め）
- 攻撃への対処としてのRate Limiting
  - 偶発的攻撃や、簡単なAmp＝SrcIPがみな同じ
    - IPアドレスベースの制限をかけられる
  - IPアドレス詐称のケースでは別の判別が必要となる
    - client categorization
    - query type
    - domain categorization
    - response size
    - client customer status
- ランダムドメイン攻撃のグローバル検知
  - OpenDNSではユーザのQueryステータスを集めて統計処理
    - 10秒で500以上のユニークなクエリーがあればそれは「怪しい」
    - クエリーの95%以上がNegativeレスポンスになり、かつSERVFAILが30%あるとそれは「怪しい」
    - 長すぎるドメイン名は「怪しい」

- Domain Dropリスト
  - リストに含まれるドメイン名は無条件にドロップ
  - グローバルアタックと認識されたドメインのうち、過去2週間の毎時平均クエリが100を超えないものはDropリスト入り。
  - この情報はリゾルバに配信され、数秒単位にアップデートされる。
- Domain Freezeリスト
  - グローバルアタックと認識されたドメインのうち、過去2週間の毎時平均クエリが100以上500,000までのものはDrop Freezeリスト入り。
  - このリストはOpenDNSのキャッシュサーバでは、10GBのメモリ上に配置された専用のエリア上に記憶される。
  - リストに入れられたドメインのライフタイムは1日。（これはTTLではない）。
  - このリストにあるドメインに対するクエリが問い合わせられた場合は、Freeze listから除外される（＝正しいクエリとみなされる）。
  - 問い合わせられなかったものはライフタイム（1日）が経過した後はドロップの対象となる。
  - これは極力FalsePositiveを減らすというポリシーで設計されていると思われる

- ドロップ状況（Drop＝マジェンダ、Rate Limit＝黄、Freeze＝青）



- 全体の中での割合（通常＝紫、Dropped＝緑、青＝NXDOMAIN）

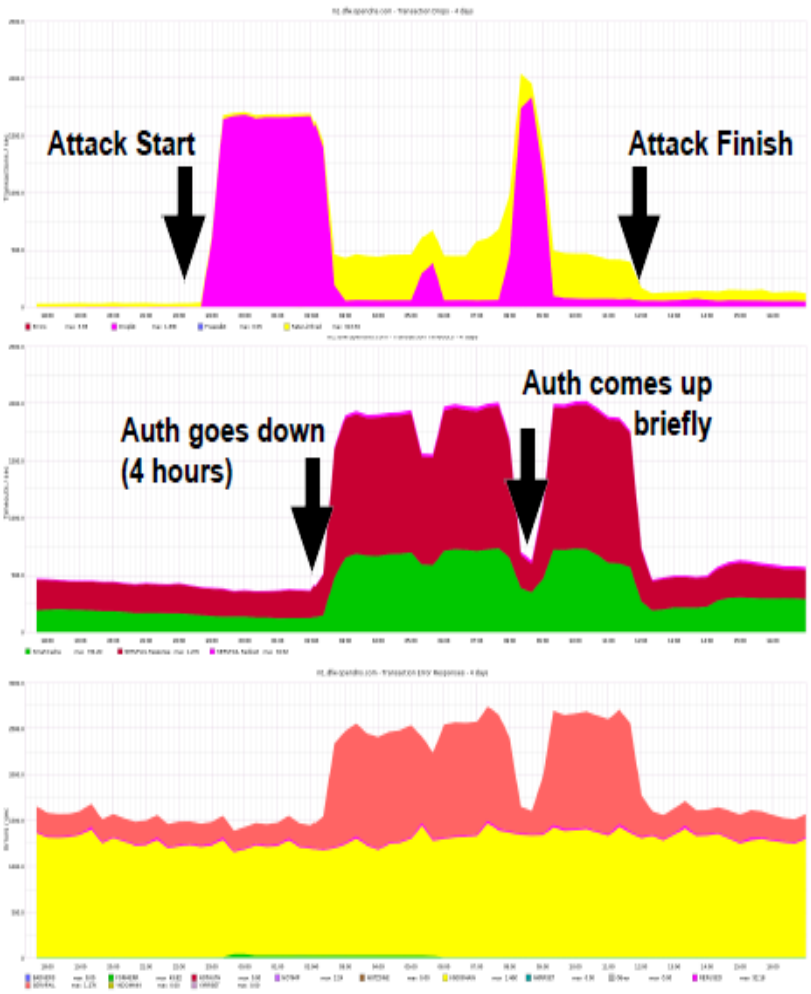


  - 1日当たり950億クエリーのうち150億クエリーをドロップしている

- AuthoritativeのRTTを利用する（SERVFAILにしないために）
  - ResolverからAuthへのクエリーが攻撃になってしまってはいけない。
  - Authからのレスポンスが長くなって結果的にクライアントへのレスポンスが悪くなることは避けたい。
    - AuthへのアクセスはRTTが良いものを選ぶ。なぜならRTTが悪いものは、攻撃されているか、距離的に遠いか、メンテナンス中かである可能性が高いため。
    - ある程度以上のRTTを示したDNSサーバはダウンしているかもしれないとみなす（閾値はタイムアウト40秒、またはすぐにSERVFAILになるもの）
    - リゾルバがRTTを覚えておいて、次回はもっともRTTが短いサーバにする（RTTのレベルによってカテゴリわけして、使用するAUTHサーバを使い分ける）

	ns0	ns1	ns2
4			RTT=4+
2			
1			
0.6	RTT=0.41		
0.35		RTT=0.12	

攻撃を可視化してみる（2015年6月）



- 紫はDrop。黄はRate Limiting。
- ランダム攻撃が増えるとdropリストに該当するクエリーが増加。

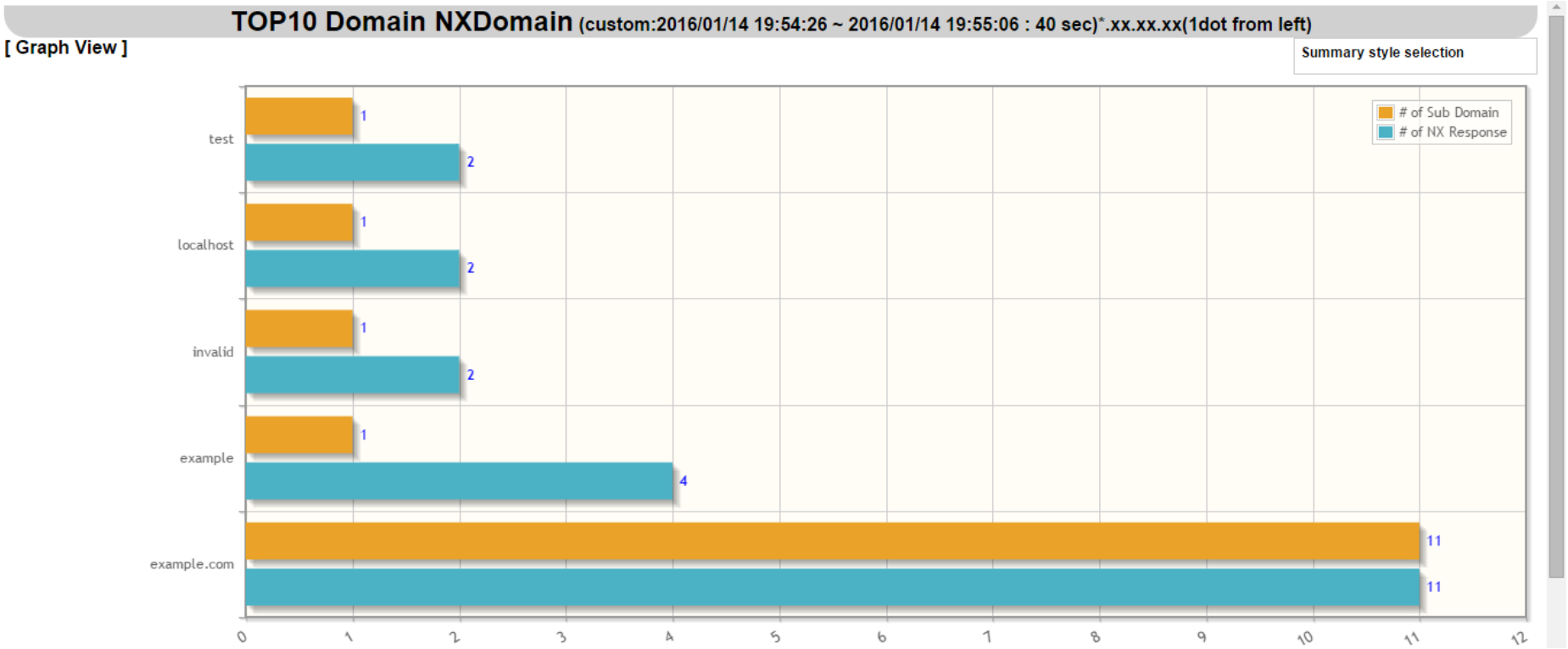
- 赤はSERVFAIL。黄緑はSmartCache。
- 攻撃開始4時間後に攻撃者は攻撃対象を変更したらしく、SERVFAILが急増。このタイミングでRate limitがかかり始めた。
- SERVFAILでAuthが返答しない場合はSmartCacheでサポート。

- サーモンはSERVFAIL、黄はNXDOMAINその他のネガティブレスポンス。
- SERVFAIL以外のネガティブレスポンスはこの時は一定量を保っていた。

これからの改善

- NXDOMAINのカウント方法
  - Z.mydomain.com stored as level1-nxdomain-count
  - Y.Z.mydomain.com stored as level2-nxdomain-count
  - X.Y.Z.mydomain.com stored as level3-nxdomain-count
  - **.X.Y.Z.mydomain.com stored as level3+-nxdomain-count
  - Ratelimit based on per-zone *-nxdomain-count
- White Listラベル（例）
  - {www,mail,ns}0?[0-9]?
  - これはいいけど
    ⇒ www01.target-domain.com is whitelisted
  - これはダメ
    ⇒ www01.ac84lsdlies.target-domain.com is not whitelisted

DNS Viewer by テリロジー



- DNS Viewer ではNXDOMAINになったクエリを任意のレベルで集計
- その集計においてユニークなFQDNがいくつあったかを集計
- この2つの値が近ければ近いほど、水責めである可能性が高いと判断

ご清聴まことにありがとうございました。

- 可視化なくして打つ手なし、という考え方について
  皆さんの意見を聞いてみたい（止めちゃえばいい？）
- Privacyの重要性が注目される＝解析できなくなる？？
  でも攻撃はやってくるんですよね。

展示会場に出展しています。ぜひお立ち寄りください。