DNS サーバから見た Telemetry - ネットワーク・インフラとの相乗効果検討

松本 陽一
Senior Solutions Engineer
APJ Carrier Presales

Akamai
Experience the Edge

このプレゼンテーションにおいてなされる記述は作成者個人の見解を示すものであり、アカマイ・テクノロジーズの見解を示すものではありません。提供される情報は作成時点において正確なものであると考えておりますが、当該情報についてなんら表明又は保証を行いません。

今日のテーマ

- Akamai (旧 Nominum) の DNS 関連製品である、DNSi / SPS シリーズにおける telemetry や DNS クエリ・データ収集等、Apache Kafka の活用の紹介
- DNSi CacheServe (キャッシュ DNS) から収集した DNS クエリ・データと telemetry データの Elasticsearch / Logstash / Kibana による可視化の例

  DNS のデータを例に、個々のネットワーク・ノードの監視にとどまらない、各種データの統合処理による活用の可能性が感じられたら...

Akamai DNSi / SPS シリーズ

2017 年 11 月に Akamai が買収した
Nominum に由来する DNS 関連製品群

- CDN のようなサービスではなく、
  ソフトウェア (ライセンス) 販売
- 主にサービス・プロバイダ市場をターゲット

- DNSi CacheServe : キャッシュ DNS (フル・サービス・リゾルバ)
- DNSi AuthServe : 権威 DNS
- SPS ThreatAvert : DNSi CacheServe のポリシー機能と Akamai からのポリシー配信を活用したネットワーク・セキュリティ・オプション
- SPS Secure (Consumer | Business | Public Wi-Fi) : DNSi CacheServe と Nom Proxy (HTTP プロキシ) によるコンテンツ・フィルタリング等のユーザ・セキュリティ
- SPS Reach : 〃 インブラウザ・メッセージング

CacheServe で本来の WEB サーバのアドレスの代わりに Nom Proxy のアドレスを応答し、
Nom Proxy でパスの検査やメッセージの挿入をなどを行う

今日のテーマでないもの

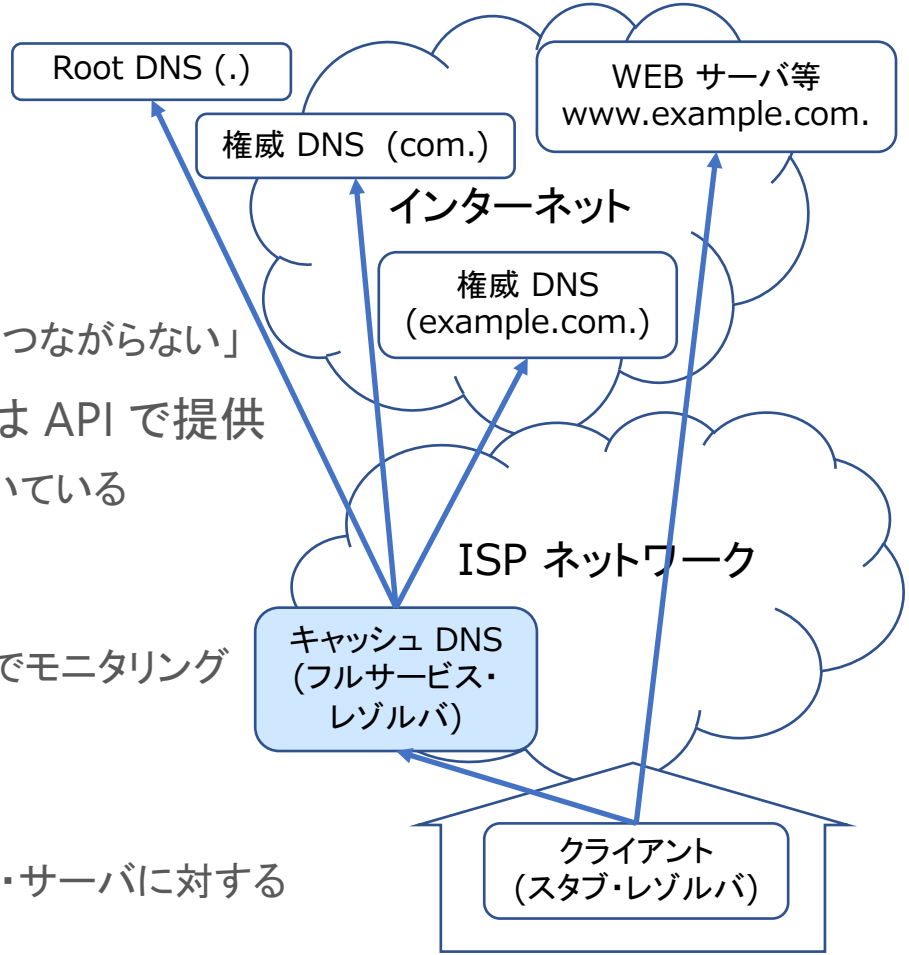
- Akamai の Fast DNS、Global Traffic Management (GTM)、Enterprise Threat Protector (ETP) といった DNS 関連サービスや DNS によるマッピング
- Akamai Intelligent Platform における telemetry や Kafka の利用
- Akamai のメッセージング・ソリューション (IoT Edge Connect)

Akamai DNSi CacheServe

キャッシュ DNS (フルサービス・レゾルバ)

インターネット・サービスの重要な要素
キャッシュ DNS の障害 → 加入者「インターネットにつながらない」

- 設定、統計情報の取得、イベント通知などは API で提供
  - config や show 的な CLI コマンドも API をたたいている
  - SNMP エージェントも API をたたいている
  - API はユーザにも解放
    例) 統計情報を定期的に APIで 取得して Cacti でモニタリング
- DNS クエリ・ログを外部のサーバに送信
  - クエリだけでなくレスポンスの情報も保存
  - クライアントからのクエリだけでなく、権威ネーム・サーバに対する再帰検索クエリの情報も保存



Akamai DNSi / SPS における telemetry、その他の Kafka 利用

従来コンポーネント間で直接独自のプロトコルで行われていた通信を Kafka　経由に

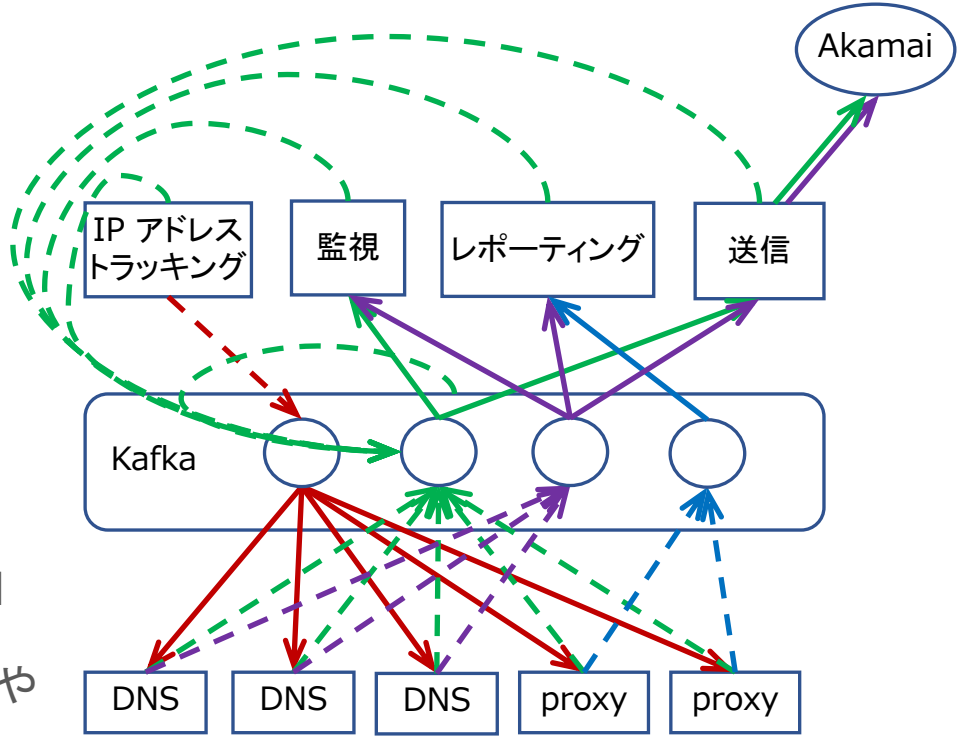
- DNS クエリ・ログ、Proxy HTTP トランザクション・ログ
  - ネットワーク内で監視 (Network View) やレポーティングに使用
  - Akamai で脅威分析に使用
  - JSON形式に変換し外部にエクスポートするオプション (Big Data Connector) を提供
- 統計情報、イベント情報 (telemetry)
  - CacheServe の他、主要な関連コンポーネントが対応
  - ネットワーク内での監視 (Network View) で使用
  - Akamai で受け取り、リモート監視、ライセンス管理等で使用 (オプション)
  - JSON 形式なので、他のシステムでも容易に処理可能
- IP アドレスのトラッキング
  - 加入者ごとに異なるポリシーを適用するために、IP Tracker Agent は RADIUS や DHCP 等から IP アドレスの情報を取得し、動的に CacheServe や Nom Proxy に設定

Akamai DNSi / SPS における telemetry、その他の Kafka 利用

- 同じデータを複数の目的で使用
- スケーラビリティ
- 拠点毎のデータ収集
- 冗長性
- 事後的なデータ処理
- 出す側の都合、見る側の都合

独自の Kafka / Zookeeper パッケージを配布

- topic 設定スクリプト、dump / load ツール等
- CacheServe と同じスタイルの CLI や telemetry



telemetry メッセージの種類

3時間に1回
- server.information

定期的(デフォルト5秒)
- server.usage
- server.statistics
- monitoring.statistics
- auth-monitoring.statistics
- telemetry.statistics
- layer.status (layer毎)
- resolver.statistics (resolver毎)
- ratelimiter.statistics (ratelimiter毎)

イベント
- action.changed
- address-list.changed
- address-node.changed
- auth-monitoring.changed

  :
- policy.hit
- ratelimiter.abate
- ratelimiter.changed
- ratelimiter.onset

  :
- resolver.id-spoofing-suspected

  :

telemetry メッセージの例


```
{
    "creator": "cacheserve",
    "type": "resolver.statistics",
    "current-time": 1533030300.000466,
    "server-start-time": 1532511236.824244,
    "node-id": "7ca8bcb8-903b-51e7-8446-99a80c617081",
    "host-name": "s222",
    "key": "world",
    "content": {
        "name": "world",
        "reset-time": 1532511240.098832,
        "cache-memory-in-use": 16916137,
        "lookups": 230001,
        "recursive-lookups": 142989,
        "proactive-lookups": 4045,
        "ignored-referral-lookups": 27049,
        "cache-misses": 146134,
        "id-spoofing-defense-queries": 1,
        "dnssec-validations-success": 8610,
        "dnssec-validations-insecure": 1,
        "dnssec-validations-failure": 2,
        "requests-sent": 236302,
        "tcp-requests-sent": 6,
        "rate-limited-requests": 6,
        "queries": 83294,
        "dropped-recursions": 0,
        "interrupted-recursions": 0,
        "queued-prefetches": 0,
        "interrupted-before-recursion": 0,
        "interrupted-recursion-waits": 0,
        "prefetch-extensions": 16,
        "active-recursions": 0,
        "responses-by-rcode": {
            "noerror": 78339,
            "formerr": 0,
            "servfail": 491,
            "nxdomain": 4464,
            "notimp": 0,
            "refused": 0,
            "yxdomain": 0,
            "yxrrset": 0,
            "nxrrset": 0,
        : (中略)
        },
        "queries-by-type": {
            "TYPE0": 0,
            "A": 75188,
            "NS": 26,
            "MD": 0,
        : (後略)
```

DNS メッセージ (base) の例

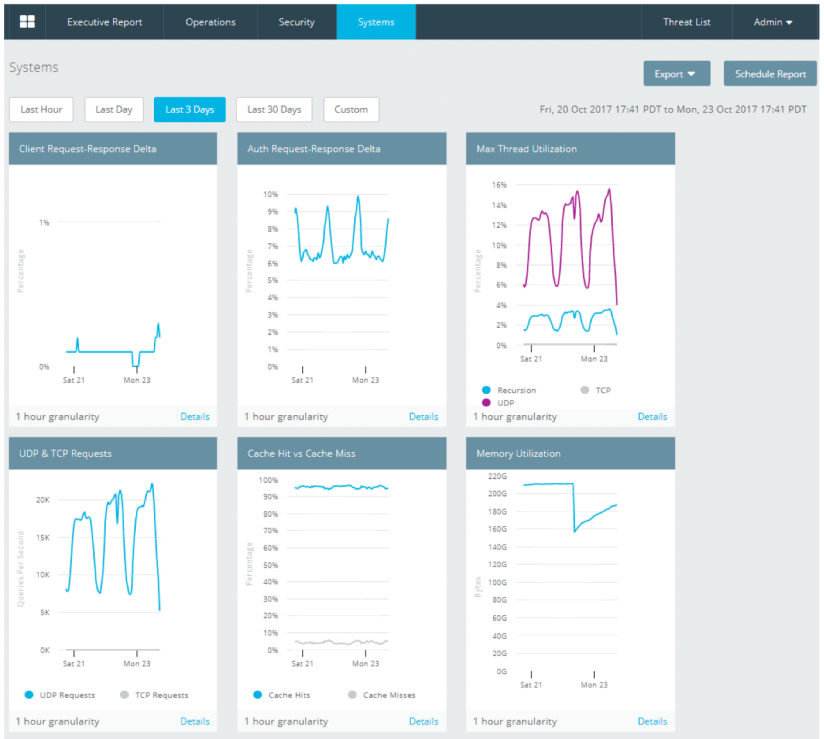

```
{
  "start-time": 1536717640436809,
  "flags": [
    "rd"
  ],
  "client-port": 35853,
  "address-family": 4,
  "dns-message": {
    "id": 16062,
    "rcode": "nxdomain",
    "opcode": "query",
    "flags": [
      "qr",
      "rd",
      "ra"
    ],
    "question": [
      {
        "name": "foo.akamai.com.",
        "rdclass": "IN",
        "rdtype": "A"
      }
    ],
    "answer": [],
    "authority": [
      {
        "name": "akamai.com.",
        "rdclass": "IN",
        "rdtype": "SOA",
        "ttl": 60,
        "rdata": "ns1-2.akam.net.
hostmaster.akamai.com. 2018091112 7200 3600 1209600
300"
      }
    ],
    "additional": []
  },
  "client-address": "192.168.1.1",
  "server-address": "192.168.101.101",
  "view": "world",
  "zone": "akamai.com.",
  "resolver": "pm-resolver",
  "request-length": 32,
  "response-length": 93,
  "core-domain": "akamai.com.",
  "_meta": {
    "timestamp": 1536717641,
    "engine-type": "cacheserve",
    "engine-version": "7.2.4.0",
    "node-id": "7ca8bcb8-903b-51e7-8446-99a80c617081"
  }
}
```

Network View での統計情報の可視化 (Systems Report)

telemetry に基づく CacheServe 全体の統計情報を可視化

- メモリ使用量
- スレッド・タイプ毎のCPU使用率
- キャッシュ・ヒット率
- プロトコル(UDP/TCP)別のリクエスト数

等..



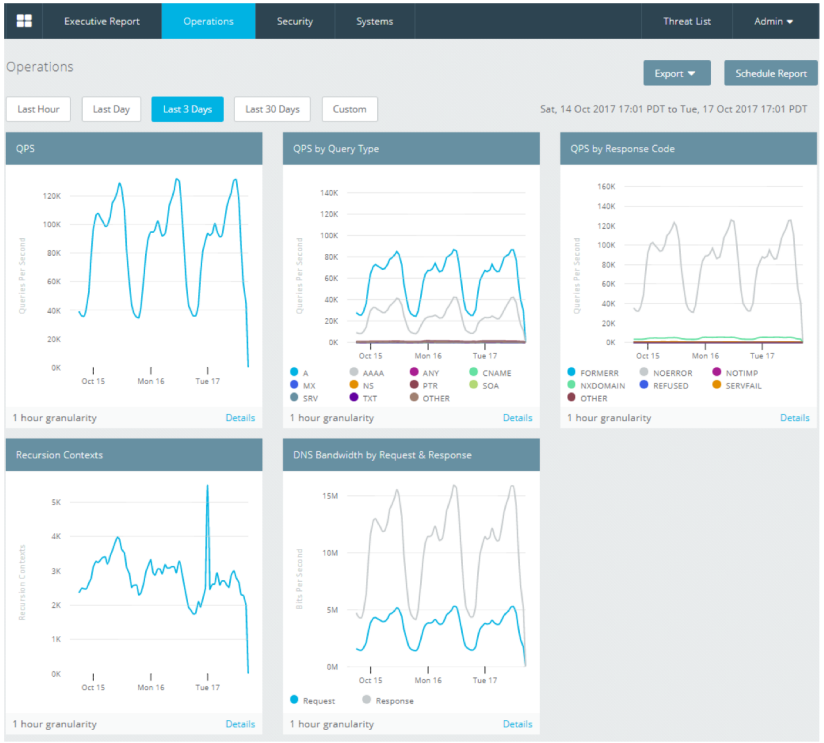
Network View での統計情報の可視化 (Operations Report)

telemetry に基づく DNS 関連の統計情報を可視化。

- QPS
- クエリタイプ別(A、AAAA、PTR等)　QPS
- レスポンス・コード別(NOERROR、NXDOMAIN、SERVFAIL 等) QPS
- Recursion Contexts (クライアントからのクエリがキャッシュにヒットせず名前解決処理中のもの)

等..

ドリルダウンによりクエリ・ログに基づいたQPS上位クライアントIPアドレスやQPS上位ドメイン名等

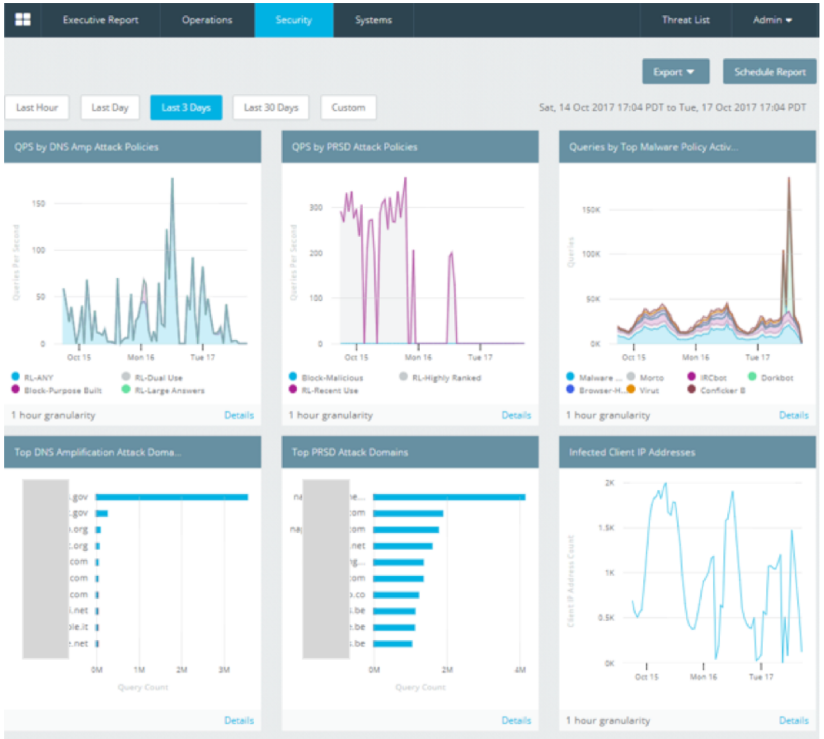


Network View での統計情報の可視化 (Security Report)

telemetry / クエリ・ログに基づくセキュリティ関連の詳細レポート

主に ThreatAvert によるリストベースの処理

- マルウェア C&C
- DNS アンプ
- ランダム・サブドメイン
- DNS トンネリング



telemetry / クエリ・ロギングを外部で利用するメリット

既存の Network View / Threat Avert のレポートとは異なる切り口でのカスタム・レポート

- ハードウェアやOSなどシステム全体との統合モニタ
- 他のセキュリティ監視との統合モニタ
- グラフ表示されない統計情報のグラフ化

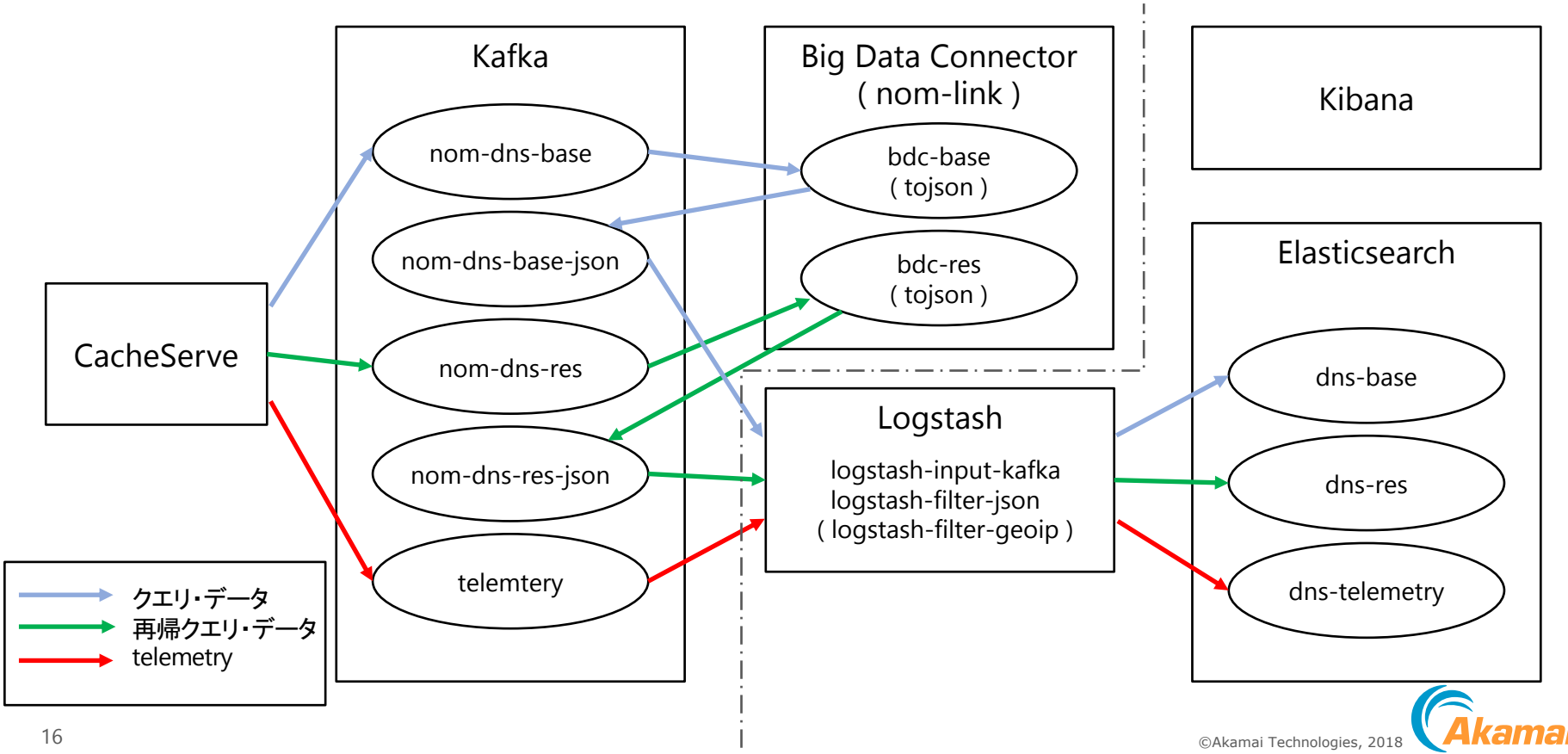
データをトリガとしたリアルタイム処理(感染者にメールで自動通知)

他の装置の telemetry 等と統合して関連性を分析し、役立てられるのでは？

- 障害予兆解析
- トラブル・シューティング
- セキュリティ・インシデント解析
- 解約予兆解析
- マーケティング

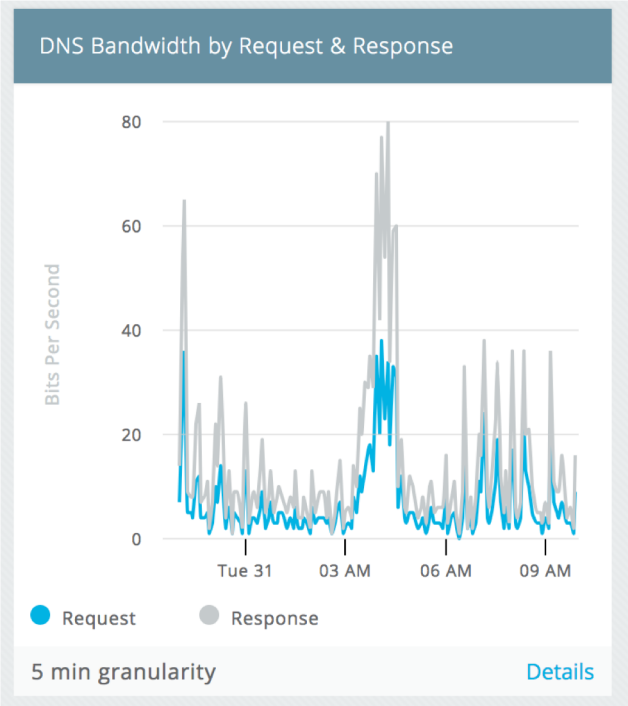
(通信事業者によるクエリ・ログ等の解析に関しては、通信の秘密を侵害しないことが前提)

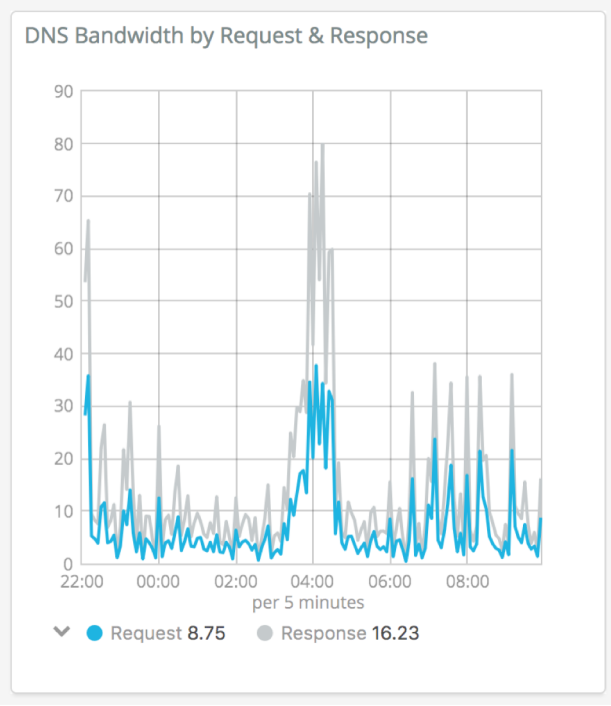
Logstash による Elasticsearch へのデータ取り込みの例



(1) Network View と同じグラフを Kibana で描いてみる

例) DNS Bandwidth by Request & Response





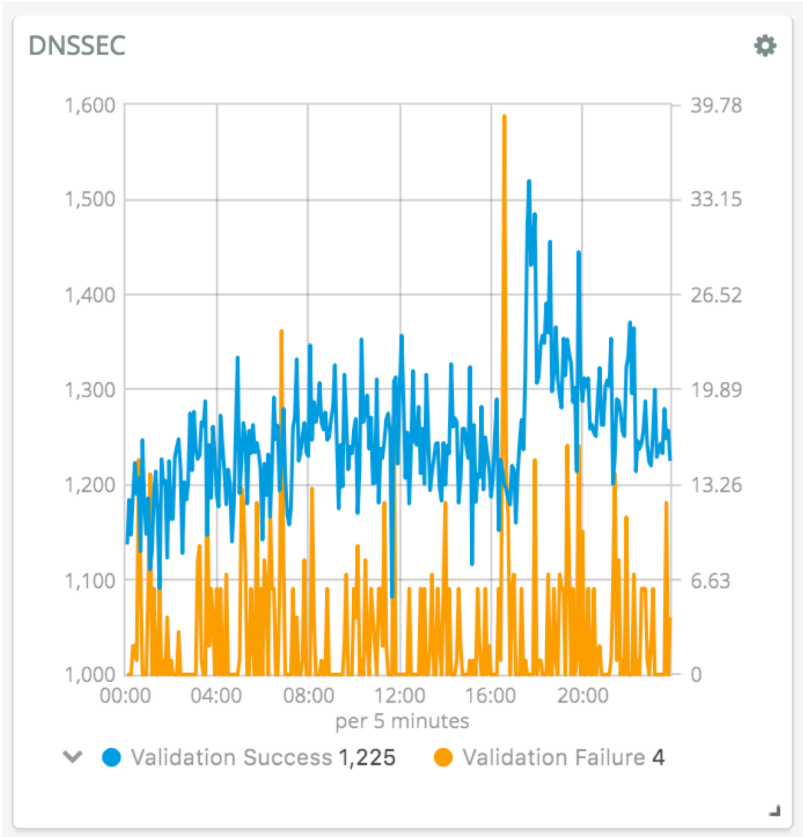
(2) Network View にないグラフを描いてみる

例) DNSSEC Validation
DNSSEC で署名を行う組織の増加傾向を把握

その他)

- proactive-queries
  (prefetch)
- id-spoofing-defense-queries
  (cache poisoning の疑い)
- malformed-request-dropped
- malformed-response-dropped

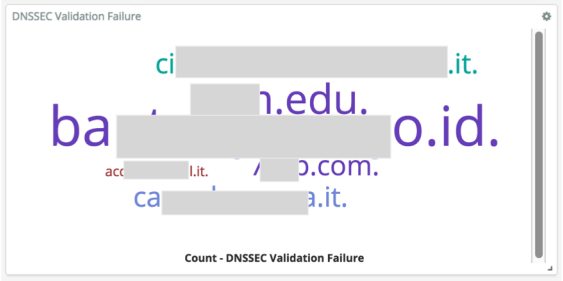
など
クエリ・ログでの詳細の解析へつなげる

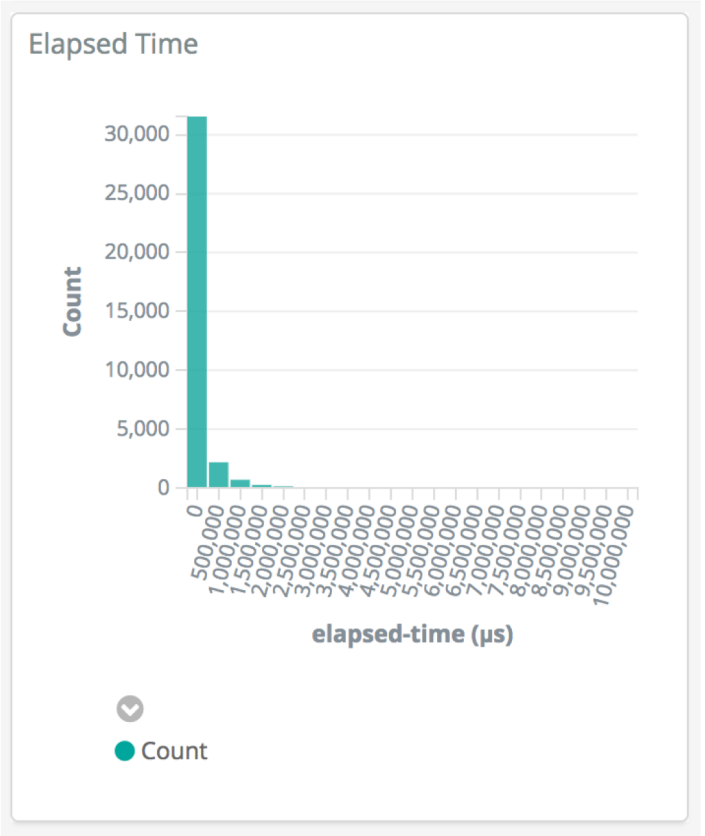


(3) クエリ･データからの視覚化

統計情報として提供されないものの統計化
(キャッシュにヒットせず)解決にかかった時間 →

DNSSEC Validationに失敗したドメイン
ポピュラーなドメインがオペレーション･ミスにより失敗すると顧客からの問い合わせが多発する恐れ





Prefetch Extension が起動したドメイン - 権威ネームサーバが DoS などで障害の可能性

(4) GeoIP との組み合わせ

- 権威ネームサーバへのクエリのタイムアウトが平常時よりも多く発生していればネットワークの障害の可能性？

- 位置情報のみならず、他装置のtelemetry等、他のデータ・ソースとの複合処理により、障害検知等に役立てられないか

まとめ

- Kafka を利用した telemetry を含めたデータ収集は大変有効
- telemetry は、リモート監視という観点でも有用だが、ローカル監視でも柔軟な応用を可能に
- Akamai では DNS クエリ・データを脅威分析に活用しています
  ユーザにおいても多様な分析に活用いただけるのではないかと考えています