pipeline

DNSログによる
ネットワーク異常の検出

Pipeline株式会社

情報セキュリティ製品を導入する時に発生する懸念

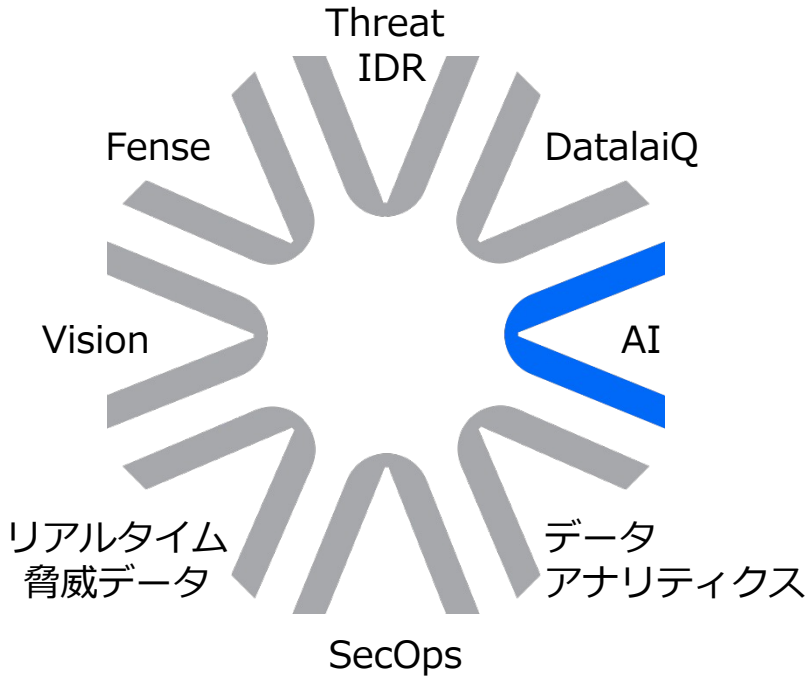
お客さまが懸念されること	PIPELINEがお手伝いできること
24時間365日システムを監視する人的リソースがない	サイバーセキュリティ専門家と弊社製品がお客様の代わりに常時監視し、お客様のシステムを守ります
既存システムが稼働していて、追加の機器購入は既存システムの設定変更などを行いたくない	弊社のセキュリティ製品は新しいサーバや端末の購入は不要です。既存システムに影響を与えることなくインストール、併存が可能です
セキュリティログなどを取得しても、見方がよくわからない	弊社製品のレポートはシステムご担当者以外の方が見ても、状況を把握しやすいデザインとなっています
どんなに対策しても新しいやり方で、次から次へとネットワーク攻撃やセキュリティ事故がおこるのでは	世界中のセキュリティデータを常時モニタリングし最新情報を入手します。お客様には常に安心してお使いいただける環境を提供します

製品・ソリューションの特徴

区分	商品名	特徴
製品	PhishR	• フィッシングを遮断し、ユーザーが安全な判断 • 行動的メールセキュリティプラットフォーム
	Fense	• エンドポイントに特化したクラウド型セキュリティ • プライバシーの監視及び保護
	Threat IDR	• DNSセキュリティゲートウエイ • スレット・アナリティクス・プラットフォーム
	DatalaiQ	• オペレーションインテリジェンスプラットフォーム • ログの効果的な相関分析
ソリューション	リアルタイム脅威データ	• セキュリティデータの提供
	Vision	• 脅威インテリジェンスのデータサービス • ユーザー別管理カスタマイズに特化したツール
サービス	データ アナリティクス	• ログによる検知・応答サービス • AI、ディープラーニング、機械学習
	SecOps	• DevSecOps & SecOps Service

パイプラインの目標

PIPELINEでしかできないサービスとソリューションで様々なお客様のニーズにお応えしていきます。



大学　医療　金融

企業　ISP MSP TEL　製造

インテリジェンス

自動化

マシーンラーニング

AI

DNSログによるネットワーク異常の検出 - 研究チーム紹介

佐藤 聡(サトウ アキラ)
筑波大学
所属
システム情報系
職名
准教授

https://trios.tsukuba.ac.jp/ja/researcher/0000000943

A.S.M. Shamim Reza
CTO
Pipeline Pte. Ltd.

Shaoyu Yang
東京工業大学
博士号候補生
Pipeline株式会社

Md. Towfiqur Rahman
ダッカ大学
ソフトウエアエンジニア
Pipeline Pte. Ltd.

DNSログによるネットワーク異常の検出

ネットワークは複雑なシステムである

- ネットワークトラフィックには異常が多く含まれる

装置障害

通信エラー

悪意がある行為

大量のトラフィックから異常を検出するのは難しい

- 機械学習を用いて人力検出のコストを削減

DNSのセキュリティへの配慮[1]

- 2018年の**DNS攻撃**の平均コストは71万5千ドル
- 77%の組織が**DNS攻撃**を受けた

[1] A New Era Of Network Attack, 2018 EfficientIP Global DNS Threat Report, EfficientIP, retrieved 2019-05-14.

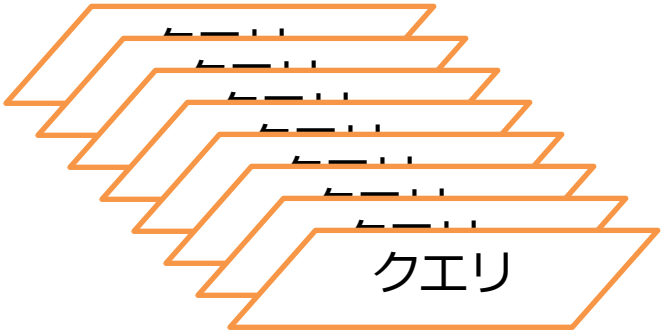
DNSログによるネットワーク異常の検出

低コストでDNSログの保存と監視が可能

- BIND 9 ネームサーバーのログ取得
  - ロギング記録例

```
01-May-2019 00:27:48.084 queries: info: client @0x7f82bc11d4e0 10.80.0.1#53995
(google.com): query: google.com IN A +E(0) (10.80.1.88)
```

クエリログを監視するにより、異常を検知することが可能

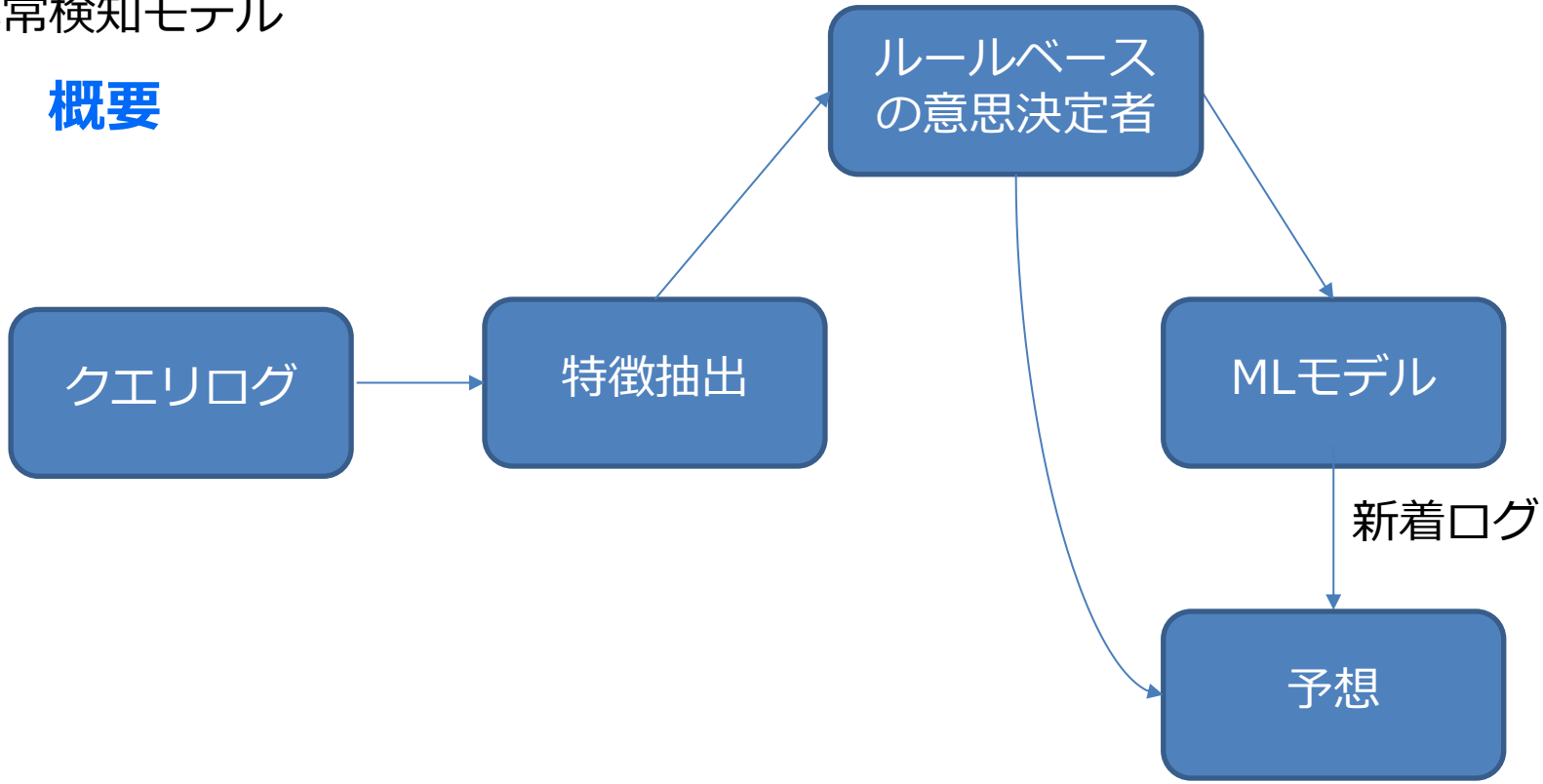


アノマリー

DNSログによるネットワーク異常の検出

異常検知モデル

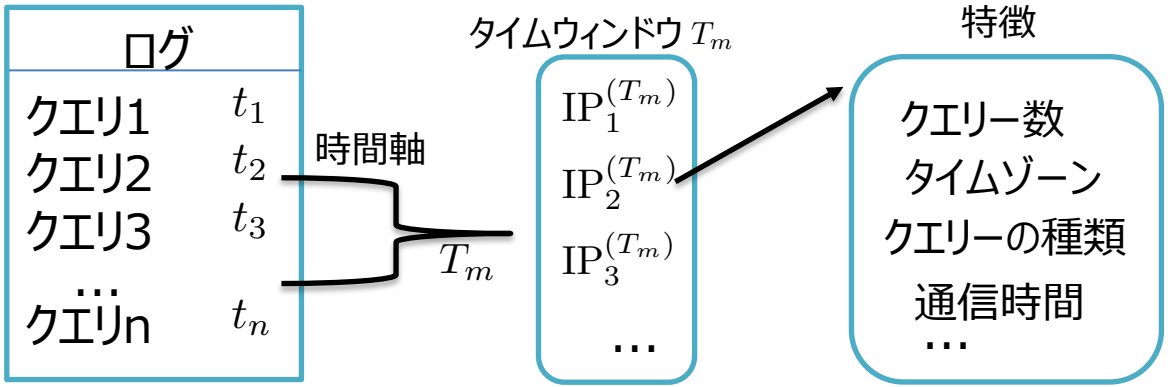
概要



DNSクエリログからの特徴抽出

クエリーのタイムウィンドウ

- DNSクエリログの時系列解析

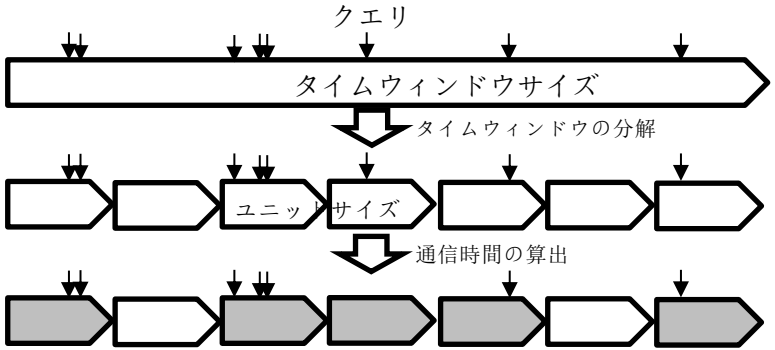


DNSログによるネットワーク異常の検出

特徴

- **総クエリ数**
  - 時間内にIPで行われた総クエリ数
- **レコード種別の比率**
  - a, aaaa, txt …
- **昼と夜**
  - クエリーのタイムゾーン
- **平日または休日**
  - 勤務実態を反映した日付情報

- **通信時間の割合**[2]

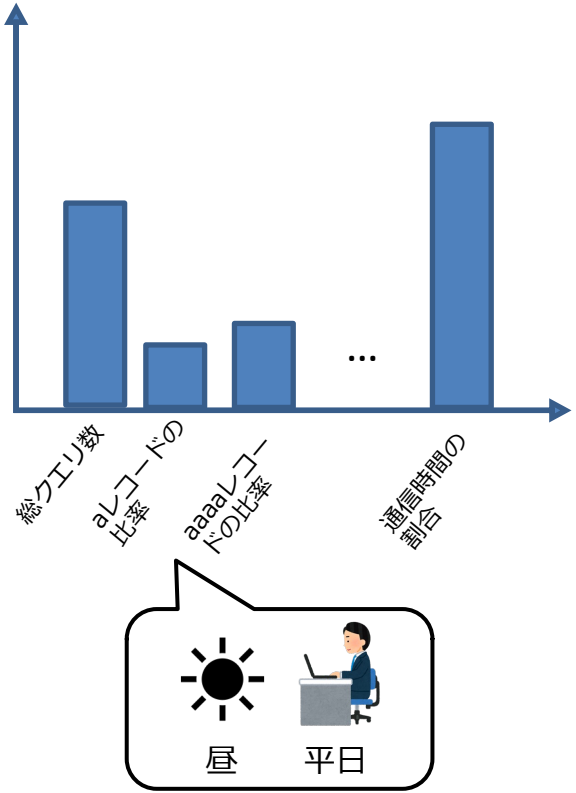


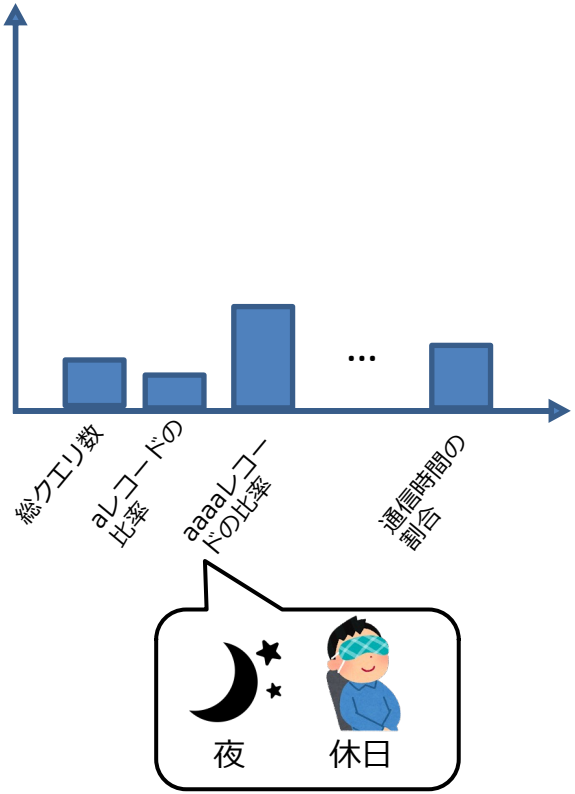
[2] 渡部耕大+、DNSクエリの分析によるサーバと非サーバの識別、ipsj sig iot 2017

DNSログによるネットワーク異常の検出

特徴から不審なIPを検出

- 時間帯や日付などの状況によりクエリ行動が変容する

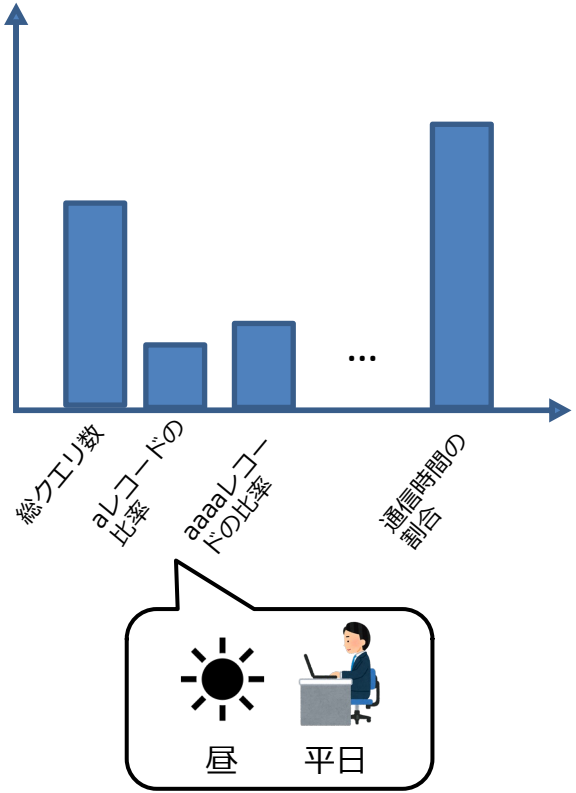


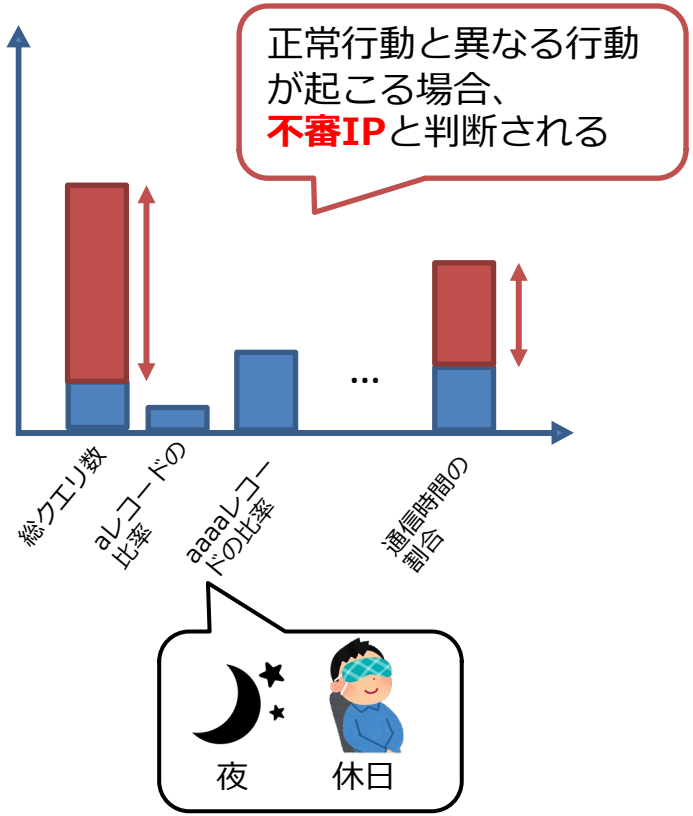


DNSログによるネットワーク異常の検出

特徴から不審なIPを検出

- 時間帯や日付などの状況によりクエリ行動が変容する

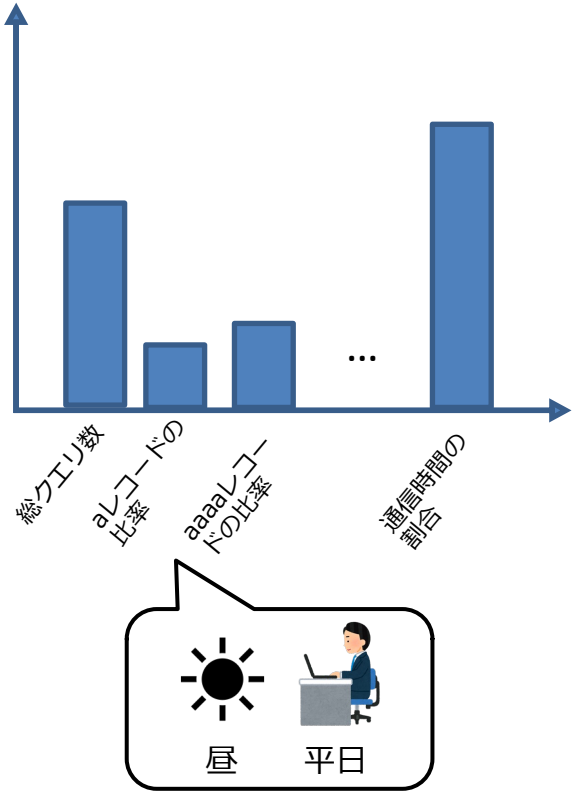


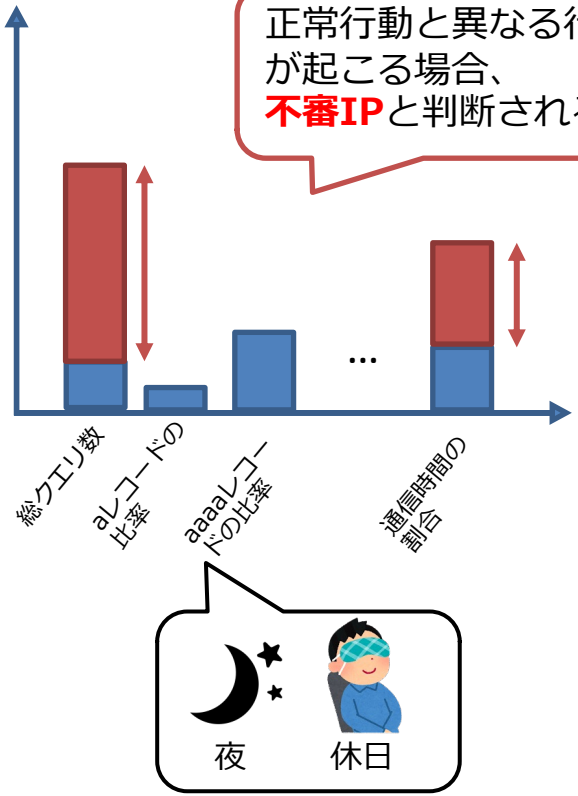


DNSログによるネットワーク異常の検出

特徴から不審なIPを検出

- 時間帯や日付などの状況によりクエリ行動が変容する





正常行動と異なる行動が起こる場合、
不審IPと判断される

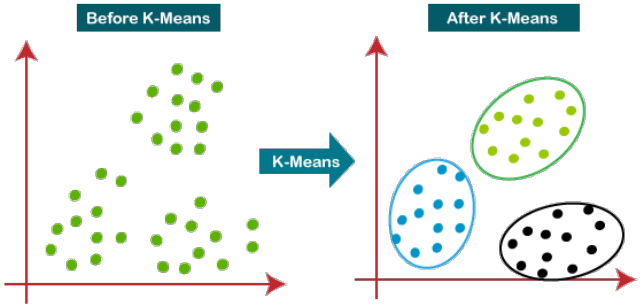
機械学習で実現する！

DNSログによるネットワーク異常の検出

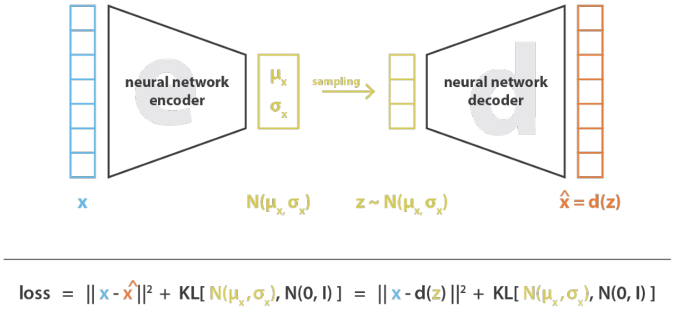
異常検知モデル

異常値検出アプローチ

- **K-means（ケイメーンズ**



- **オートエンコーダ**
  - 入力
    抽出された特徴量
  - 出力
    再構築された機能
  - Anomaly IPは再構成誤差が大きくなる



テスト結果

Pipeline株式会社

DNSデータ (国内とある組織） から取得したデータ

- 2021/02/01～2022/02/08まで
  - 平日・土日を含む192時間
  - 総クエリ数 18,589,831件
- 内部IPに着目
  - ネットワークやIPセグメントのデバイスによるクエリ

DNSログによるネットワーク異常の検出

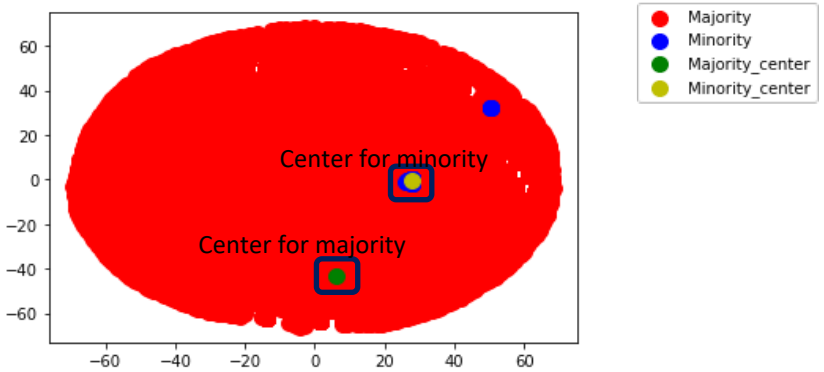
結果

K-meansクラスタリング

- 多数派IP数
  - 86,145
- 少数派IP数
  - 70
- 両グループのIP数
  - **7 不審なIP!**

オートエンコーダ

- 多数派IP数
  - 86,022
- 少数派のIP数
  - 193
- 両グループのIP数
  - **24 不審なIP!**



T-SNEプロット

不審なIPの例

行動変容

通常の動作

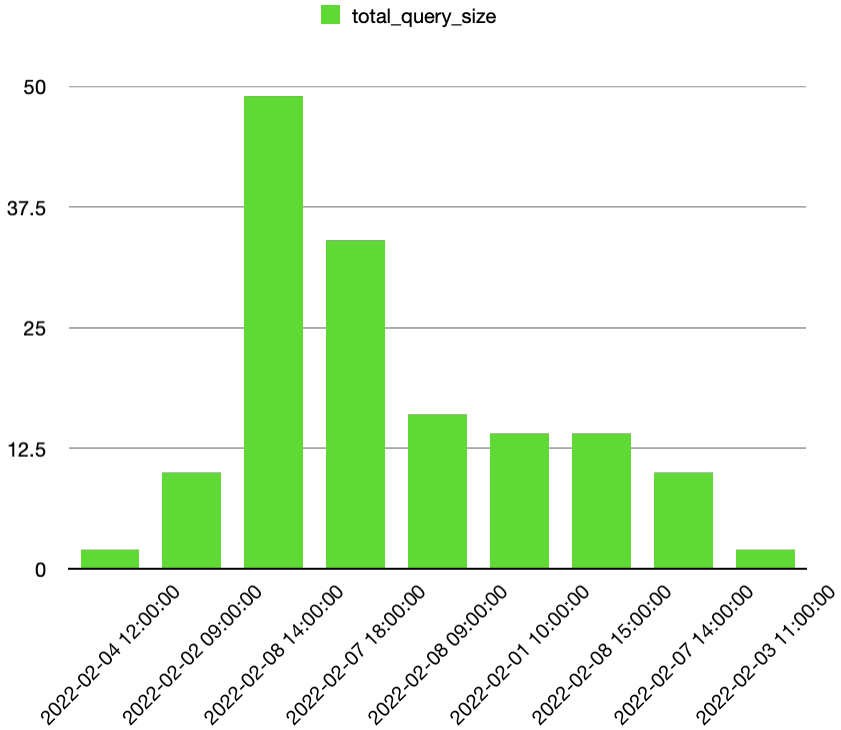
ウィンドウ／タイム	IP Address	合計クエリーサイズ	平日	週末	日中	夜間
2022-02-02 09:00:00	xxx.xx.7.27	10	1	0	1	0
2022-02-04 12:00:00	xxx.xx.7.27	2	1	0	1	0
2022-02-01 10:00:00	xxx.xx.7.27	14	1	0	1	0
2022-02-03 11:00:00	xxx.xx.7.27	2	1	0	1	0

異常行動

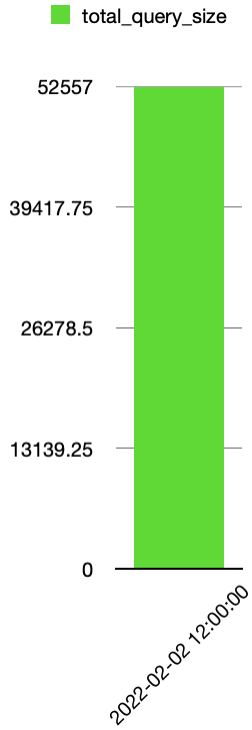
ウィンドウ／タイム	IP Address	合計クエリーサイズ	平日	週末	日中	夜間
2022-02-02 12:00:00	xxx.xx.7.27	52557	1	0	1	0

DNSログによるネットワーク異常の検出

不審なIPの例



通常の動作



異常行動

DNSログによるネットワーク異常の検出

pipeline

ルールベースの意思決定者

DNSクエリの異常の経験則

- キャッシュヒット率の低下
- クエリーの比率が一定期間ごとに増減すること。
- **クエリに大文字と小文字が混在している (DGA)**
- Null クエリ要求が多い
- TXTクエリが多い
- **サブドメインが63文字以上 (DNS Tunneling)**
- base64 でエンコードされた文字列を含むクエリ
- IPやドメインのレピュテーションデータに基づく検知

不審なクエリの大量発生

DGAドメインのようにランダムな文字で表示される

特定のドメインに対して変なサブドメインクエリが生成される。

MTyUE20352x325kdafj….
これ何？

結論

概要

- DNSクエリを利用したネットワーク異常検知
- クエリの特徴量から異常を検出する機械学習モデル
  - K-means（ケイメーンズ
  - オートエンコーダ
- 実際のDNSクエリを用いた実験により、異常な振る舞いをする不審なIPを検出できることが判明

今後の課題

- モデル性能を評価するための人工的な悪意あるデータの追加
- アプリケーションをリアルタイムに検出

DatalaiQ（データレイク）

〃 お客様のデータを最大限に引き出し、
「重大な意思決定」をお手伝いする
オペレーションインテリジェンスサポートツールです。 〃

DatalaiQの使用方法：検索結果画面

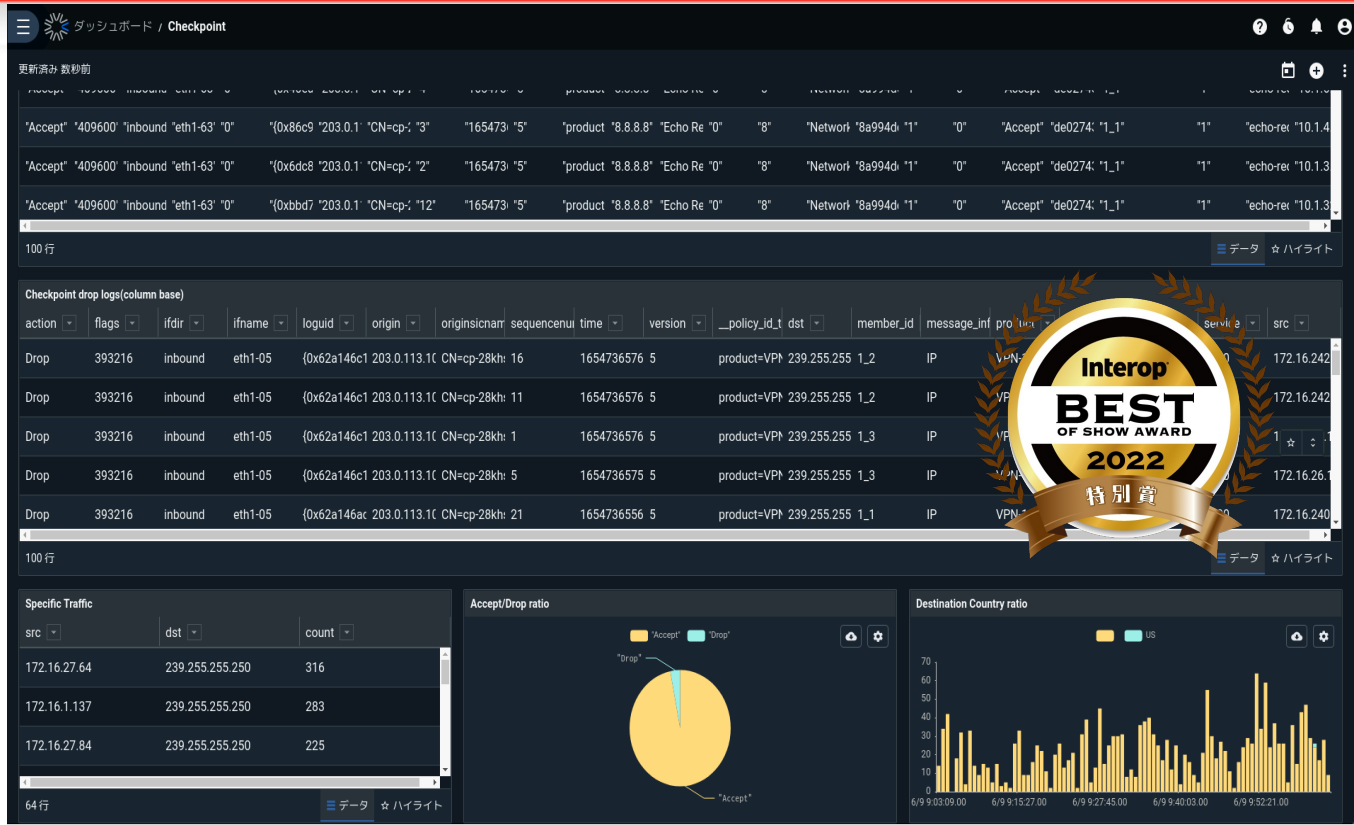
```
tag=dns_query regex "[a-z0-9A-Z-:.@#() ]query: (?P<domain>[a-zA-Z0-9-].[a-zA-Z0-9.]+) IN (?P<record>[A-Z]+) [a-zA-Z0-9+.()-:]+" | count by domain | chart co
unt by domain limit 100
```

統計

①エンドポイントやサーバーなどのログを集める

②ログをインデクスして保存

③検索した結果をダッシュボードで表示



使用方法：豊富なデータキット

カスタマイズ可能なダッシュボードは、ユーザーが設定したものと、キットに組み込まれたものがあります。

管理のしやすさ

独自のアクショナブルを作るリソースとその他

多種多様なデータの融合を可能にするクエリ

インジェススターからのバイナリデータのストリーミング エンリッチメントモジュールユーザー定義の静的データ

強力なクエリで迅速な回答

お客様の声

“セキュリティが大幅に向上
簡単で導入しやすい製品、手が届かなかった部分に手が届いた
製品導入後にインシデントが起きていない。
１日１０００件の脅威通信を自動的に遮断している”

大学共同利用機関法人自然科学研究機構岡崎情報ネットワーク管理室
大野人侍氏
澤　昌孝氏（技術職員主任）

自然科学研究機構（NINS＝National Institutes of National Sciences）は岡崎にある研究所の基礎科学研究所、生理学研究所、分子化学研究所の3研究所とその事務を統括する岡崎総合事務センターから成る組織になっている。自然科学研究機構は研究所の基礎研究を行っている。このなかで、「岡崎情報ネットワーク管理室」は旧岡崎国立共同研究機構の3研究機関と事務組織の共通ネットワーク部分、および対外ネットワークの運用管理を担当している。同機構ではセキュリティを向上させるソリューションとしてThreatIDR（スレットIDR）の「DNSFirewall」、ログ解析ツール、総合ログ管理、相関分析プラットフォーム「DatalaiQ」を採用した。

DatalaiQ - どんなデータでも、データの欠損なく取り込むことができる

データアグリゲーション

データの取り込み、利用者、保持に制限はありません。あなたのデータに障害はありません

全データタイプ

データを生の状態で取り込み、すぐに全体を検索することができます。

パワフルなクエリ

堅牢で豊かなクエリシンタックスにより、環境の隅々まで探索し、データを深く掘り下げることができます。単純解析、相関解析が可能

キット

素早くスケールアップするために必要なものがすべて揃っています。ダッシュボード、クエリ、リソース、プレイブック。必要なツールがすべて揃っています。

DNS Summer Days
13GBまで無料！