NML - Network Muscle Learning - Project

サイバー脅威ビッグデータ解析によるリアルタイム攻撃検知と予測

Real-time threat detection and prediction by analyzing cyberthreat big data

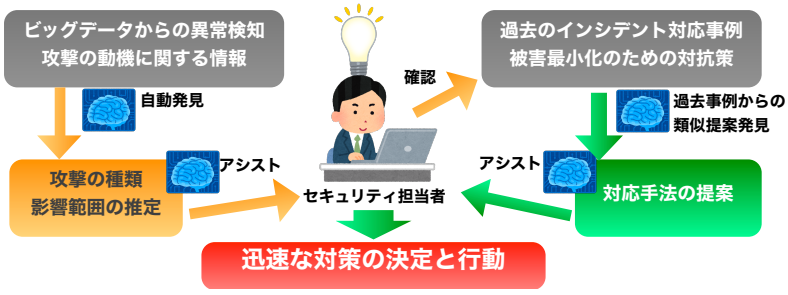
Web: https://nml.ai/
Contact: info@nml.ai

研究代表者 関谷勇司
(東京大学 情報基盤センター)

サイバー脅威の課題

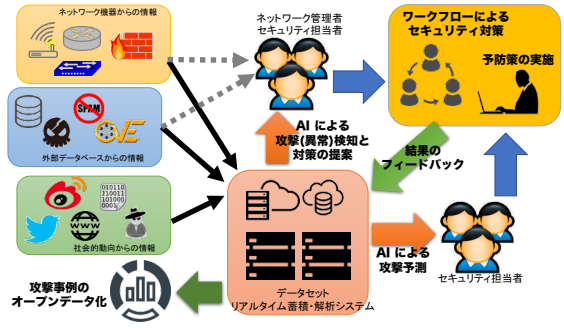
- 毎日大量に発生するインシデント
  - 高度化・組織化する攻撃
  - 日々出現する新しい攻撃手法
- 属人的対応の改善
  - 経験則による調査
  - 対応者の能力に依存した対策立案

AIによるアシストの必要性



本研究の目的

(1) サイバー脅威ビッグデータのストリーミング解析基盤構築
(2) 知識ベースを用いたサイバー脅威予測手法の確立
(3) インシデントレスポンスの自動化基盤とその要素技術
(4) リアルデータによる実証実験
(5) サイバー脅威オープンデータの作成

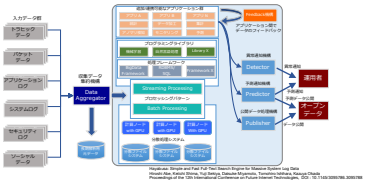


これまでの研究成果

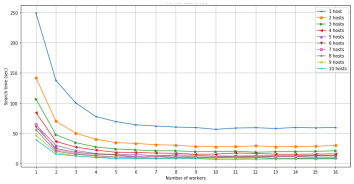
リアルタイム分析基盤Hayabusa

- 時系列データの蓄積を念頭に置いたデータ構造とコアスケールを活用した分散データ蓄積および検索システム
- 10台の分散環境で140億レコードの全文検索を5秒で完了

Hayabusaアーキテクチャ



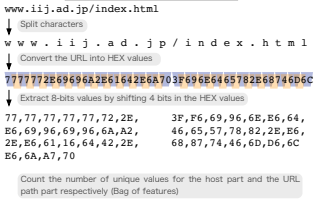
スケールアウト性能評価



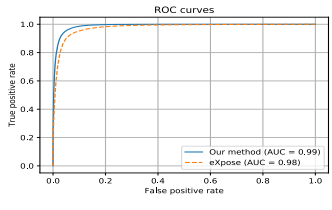
URL文字列のBag of Featuresによる深層学習を用いた詐称サイト判定

- URLをASCII codeのビットパターンとみなしてパターンの出現頻度を計上
- ビットパターンの出現頻度をURLの特徴ベクトルとして学習
- 94%の正確さで詐称サイトと通常サイトを判別

URL特徴ベクトルの計算



詐称サイト判定精度



パケットBag of Featuresによる深層学習を用いた悪性判定

- 深層学習の分野で大きな成果を上げた画像認識の概念を応用
- パケットコンテンツをビット列として深層学習に利用
- ビット列の出現頻度が悪性通信と良性通信で異なる特性を持つと仮定
- CIC-IDS2017データセットに対して高精度な検知結果を獲得
  - 対ブルートフォース：AUC 0.995
  - 対ボットネットトラフィック: AUC 0.996

IPパケット特徴ベクトルの計算

IPパケット中に出現する数字を数え上げる (パケットBag of Featues)

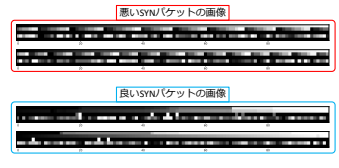
0x0000: 4500 0034 0000 4000 4006 e6e1 c0a8 0004

→ 0x45→1、0x50→1、0x00→11、0x03→1、0x34→1、0x40→2、…

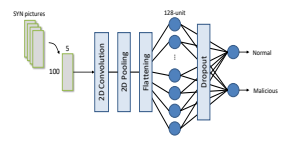
TCP Synストリーム画像と深層学習を用いた悪性判定

- TCP Synパケットの情報を画像化
  - Timestamp、Src/Dst ports、Sequence #、Window size
- ダークネットに到着したTCP Synと通常のネットワークに到着したTCP Synに現れる違いを画像認識技術を使って判定
- ダークネットに到着した接続(悪性接続と仮定)のうち
  - 51%以上の接続を99%以上の確率で悪性接続と判定
  - 86%以上の接続を50%以上の確率で悪性接続と判定

悪いSynと良いSynの画像例



学習に用いたニューラルネット



今後の展望

2017年度の成果
- ビッグデータ解析基盤
- 単一攻撃検知へのAI活用
- インシデントレスポンスフローの調査とモデル化

次年度に向けた基礎研究を完了