jh171006-NWJ

関谷勇司 (東京大学)

Proactive and Reactive Cyber Security

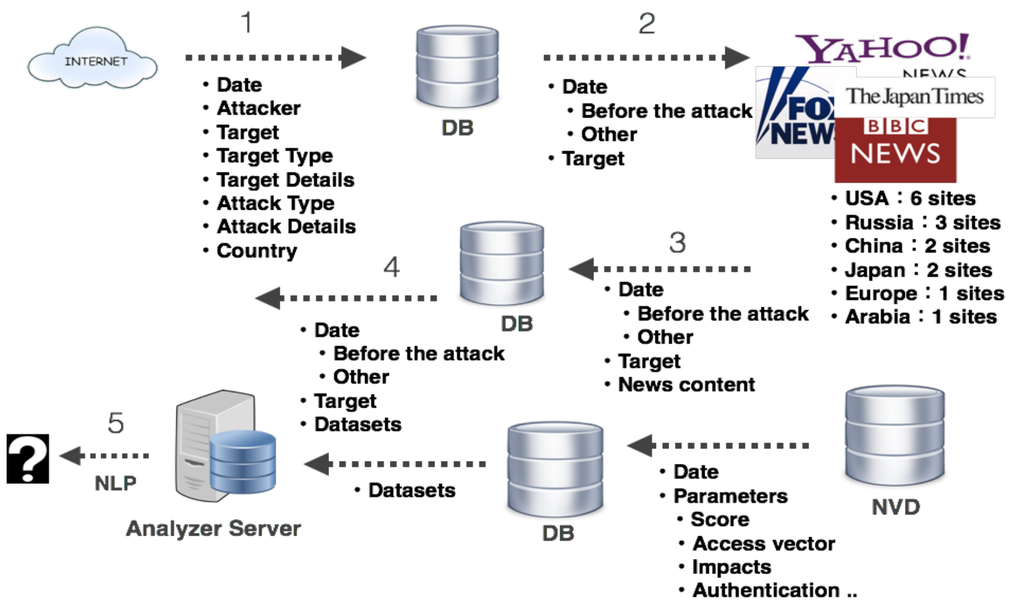
研究目的

1. サイバー攻撃の予兆となる社会データを収集 ➡ Proactive
2. サイバー脅威を観測し、ビッグデータを形成 ➡ Reactive
3. 異種ビッグデータから攻撃の全体像の解明 ➡ Cyber Security

Proactive解析

ニュース記事やTwitterなどの社会的データを
深層学習を用いて解析し攻撃を予測する

[研究のポイント]
1. Motivation / 特定のターゲットに対するサイバー攻撃の確率
2. Opportunity / 発生し得る攻撃種類
3. Timing / 攻撃発生タイミング



Prototype implementation of analysis to predict attacks using SNS data

※ *M. Baaatarsuren and Y. Sekiya, "Cyber attack prediction using social data analysis", Journal of High Speed Networks, vol. 23, no. 2, pp. 109-135, 2017, DOI: 10.3233/JHS-170560*

Reactive解析

ネットワーク、サーバ、エンドポイント等にて
観測されるサイバー脅威を垂直統合型で解析

[研究のポイント]
1. ネットワークデータの解析アルゴリズムへの適用方法
2. 属人的な知識や経験に頼らない攻撃発見
3. 異常検知と対策の提示

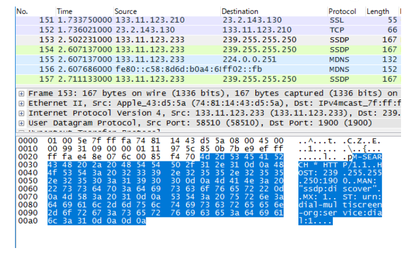
CNN is widely used for Image Recognition

1. Resize to fixed size (for classification)
2. Extract color for each pixel
3. Generate m-by-3 matrix

(0, 0, col) (0, 1, col), … , (0, *w*, col)
(1, 0, col) (1, 1, col), … , (1, *w*, col)
…
(*h*, 0, col), (*h*, 1, col), …, (*h*, *w*, col)

, where *h* is height, *w* is width
an m-by-3 matrix
(width, height, color)

How can we use it for Packet Recognition

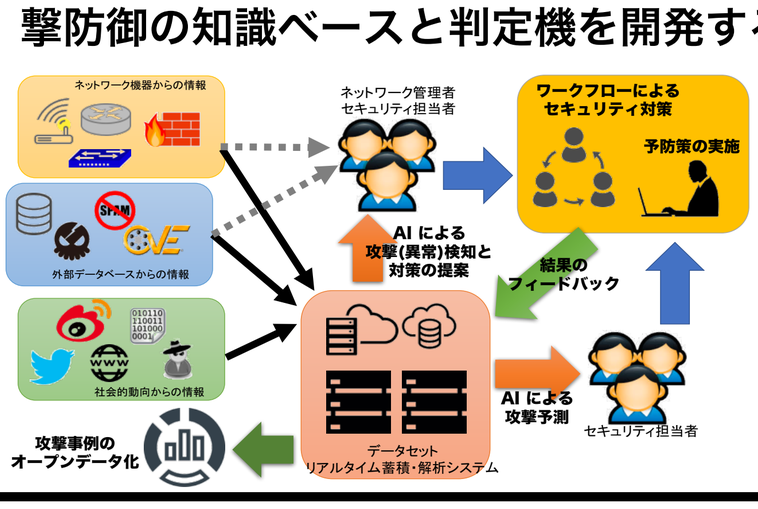


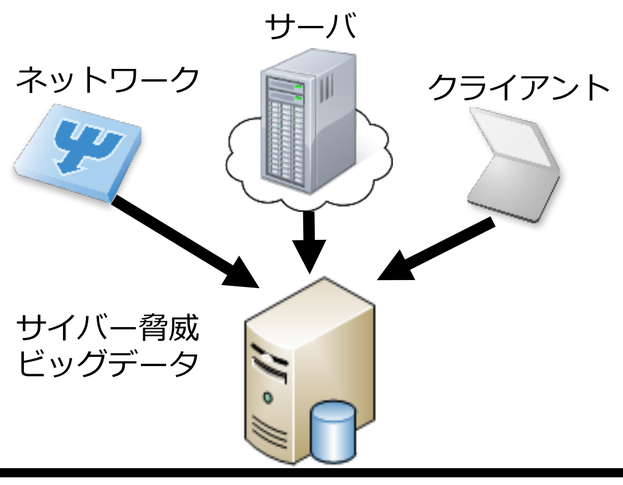
1. Resize … how … !?
2. Extract … what … !?
   Source ip, port number
   Destination ip, port number
   and sequence of TCP flow ?
3. Generate … possible !?

CNN for network analysis

Cyber Security の高度化

- 東京大学と奈良先端科学技術大学院大学が持つ社会データから、サイバー攻撃の予兆を示す特徴データを抽出し実際に観測されるサイバー脅威と紐付けて解析する
- サイバー脅威への対策あたっては UNITEC の持つ知見を導入し、異なった大学においても共通に利用できる攻撃防御の知識ベースと判定機を開発する





JHPCN（東京大学・その他の資源「リアルタイム専有型データ解析ノード」）により、データをフレキシブルに更新しながら、ストリーミング解析を行う。

関谷勇司（東京大学）
Hossein Sarrafzadeh (UNITEC)
Paul Pang (UNITEC)
荒牧 英治 (NAIST)
宮本 大輔 (NAIST)