Yuji Sekiya

Professor, The University of Tokyo
Graduate school of Information Science and Technology
Security Informatics Education and Research Center

Detecting Cyber-Threats and Assisting the Countermeasures using Cyber-Security Big Data

NML Project : (https://nml.ai)

Convergence of HPC and Data Science for Future Extreme Scale Intelligent Applications
Nov, 6th, 2019

BACKGROUND

- We have security incidents.
  - Person(s) responsible for Cybersecurity are busy for incident responses.
  - Academic organizations also had critical incidents in Japan.
- Need more security EXPERTs.
  - But not enough cost and human resource.
  - Can AI help the incident response ?
  - What kinds of information need for making assistance for Cybersecurity ?
- Providing the knowledge of Cybersecurity Analysis and Assisting the Countermeasures.

Our Challenges

- Collecting and Pre-Processing Big Datasets for Cybersecurity
- Finding Attack Behaviors using Machine Learning in Realtime
- Predicting Attack Behaviors using Machine Learning
- Assisting Security Operators to Find the Attacker’s Behavior
- Assisting Security Operators to Decide the First Action

NML Project

- Joint Research Project
  - Network Machine Learning Project
  - Funded by JST CREST

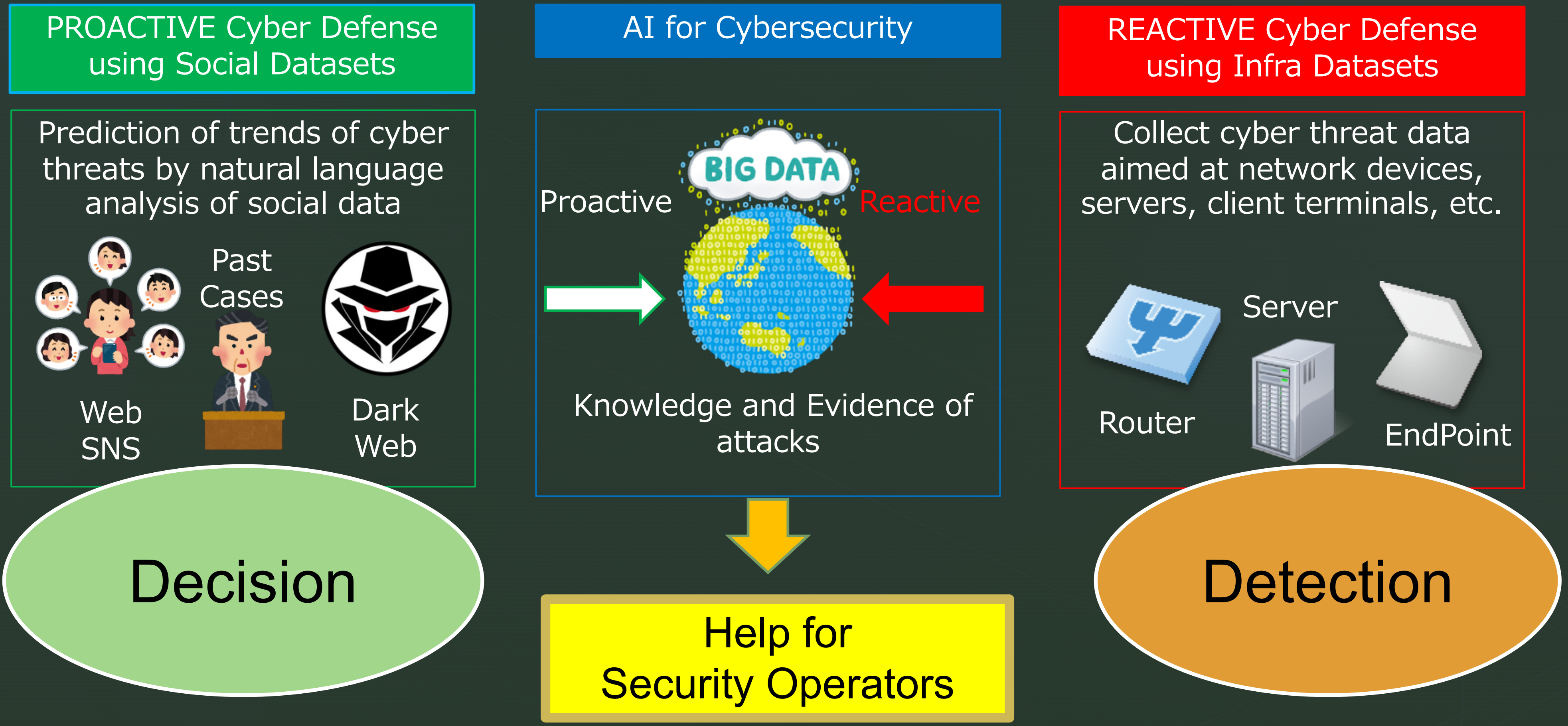
東京大学 THE UNIVERSITY OF TOKYO

東京工業大学 Tokyo Institute of Technology

Nara Institute of Science and Technology NAIST®

IIJ INNOVATION INSTITUTE

Our Approach



PROACTIVE Cyber Defense using Social Datasets

Prediction of trends of cyber threats by natural language analysis of social data

Decision

AI for Cybersecurity

Knowledge and Evidence of attacks

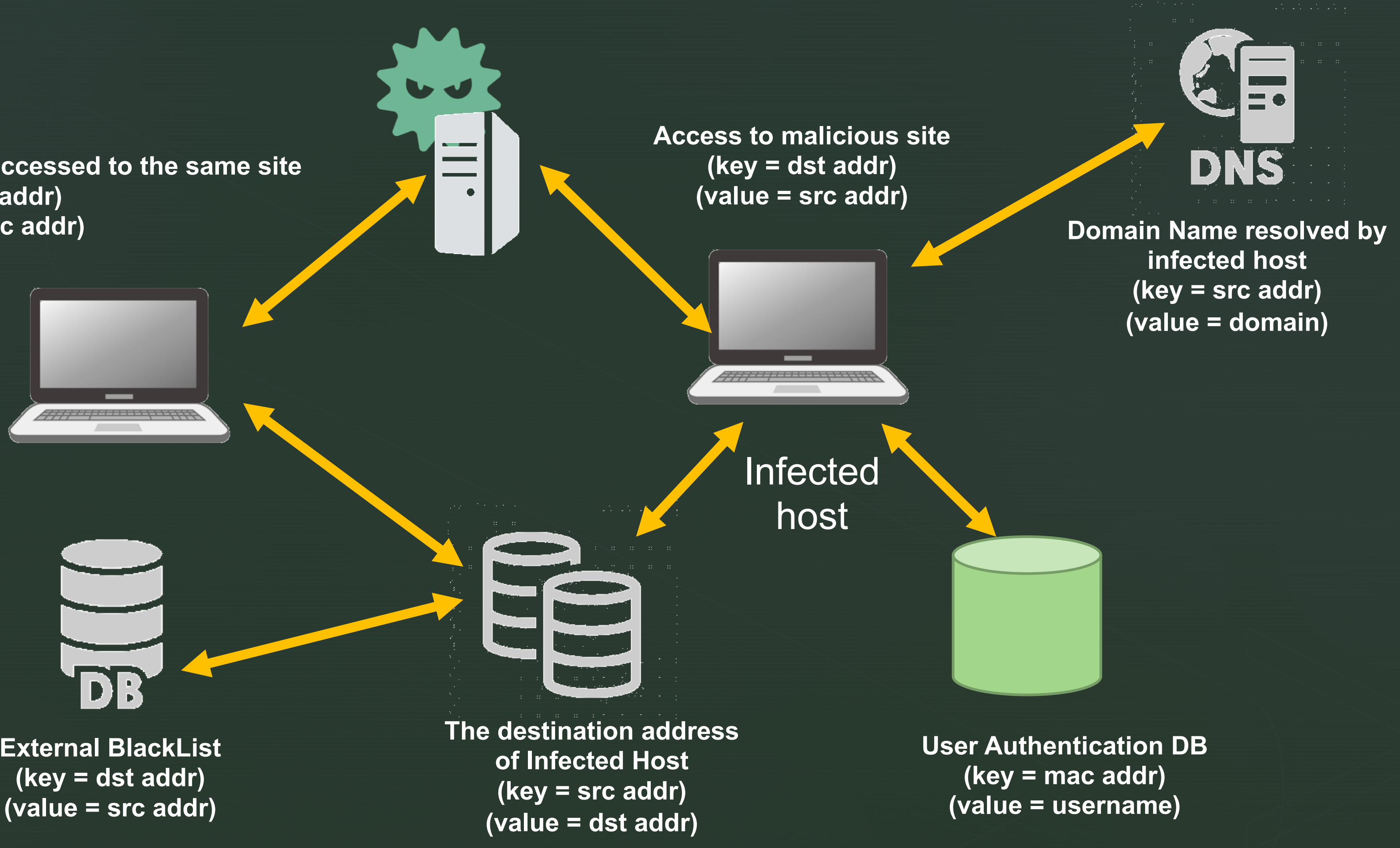
Help for Security Operators

REACTIVE Cyber Defense using Infra Datasets

Collect cyber threat data aimed at network devices, servers, client terminals, etc.

Detection

Reactive Approach – Find the Behaviors



The host accessed to the same site
(key = dst addr)
(value = src addr)

Access to malicious site
(key = dst addr)
(value = src addr)

Domain Name resolved by infected host
(key = src addr)
(value = domain)

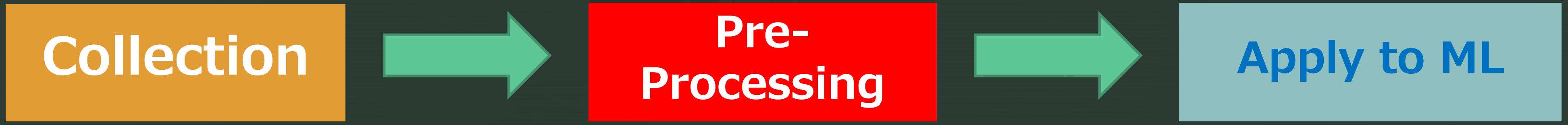
Infected host

External BlackList
(key = dst addr)
(value = src addr)

The destination address of Infected Host
(key = src addr)
(value = dst addr)

User Authentication DB
(key = mac addr)
(value = username)

Collecting and Calculating Feature values of Dataset



Traffic (pcap)
Malware (exe, pdf, ..)
Web site (html)

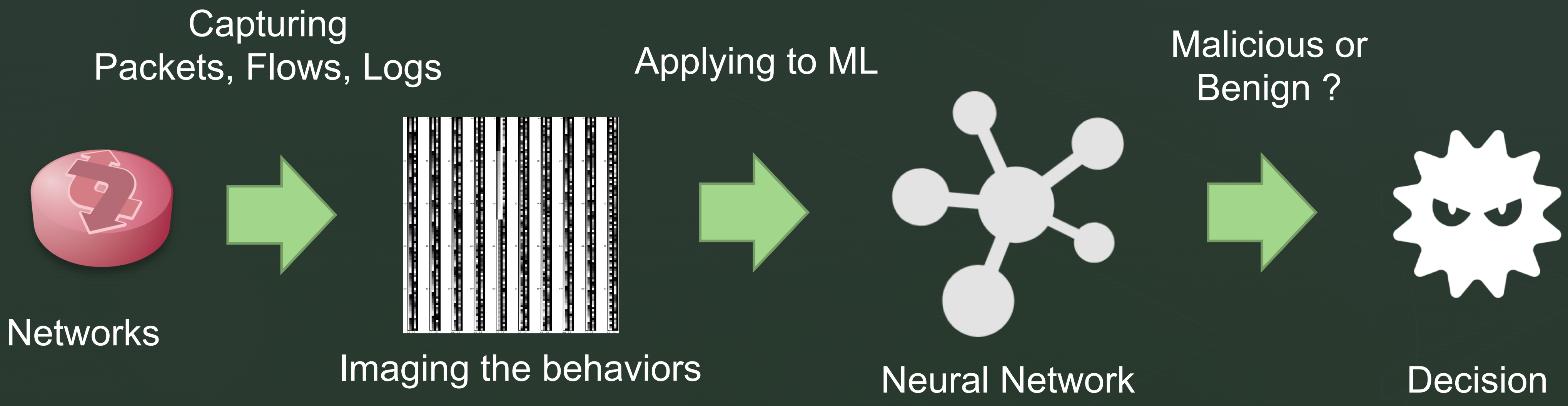
How convert the mixture of datasets to feature values ?

SVM, Bagging, Bosting, Decision Tree, Decision Forest Neural Network, K-means, K-NN, …

- Collection
  - Network dataset tends to be huge amount
  - Over 10k messages per second
  - Need real-time storing and alanysis
- Converting Feature Values
  - Which values are useful ?

Our BASIC Approach : Picturization

- Processing the images of network behaviors
  - Based on Hosts, Services, Entities…
- The Key point is “Picturization”
  - Applying Image Processing Methods to Network Behaviors



Capturing
Packets, Flows, Logs

Applying to ML

Malicious or
Benign ?

Networks

Imaging the behaviors

Neural Network

Decision

Application : SYN packet behaviors

Goal : Detecting Malicious Behaviors of Infected Hosts or Attackers

Advantages

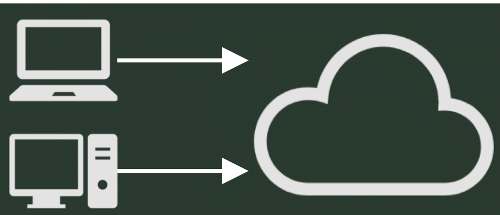
(1) No Need of FULL Capturing – Applicable for High-Speed Networks

(2) Applicable for not only specific infection and attacks

(3) Light-Weight Realtime detection

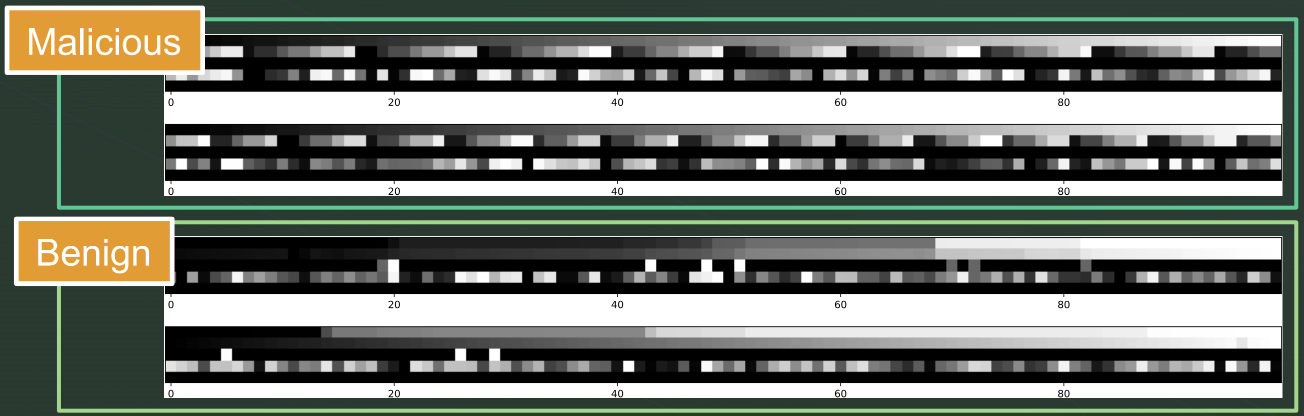
TCP SYN Packets

- SYN is the start point of TCP connections.
- Observing only SYN packets : No need of full capturing
- Detecting the infected hosts inside the network
- Finding the attacker’s behaviors



HOST Behaviors

Picturization of SYN Packets Behavior



Ryo Nakamura, Yuji Sekiya, Daisuke Miyamoto, Kazuya Okada, Tomohiro Ishihara, “Malicious Host Detection by Imaging SYN Packets and A Neural Network”, International Symposium on Networks, Computers and Communications (ISNCC 2018), Rome, Italy, June 2018

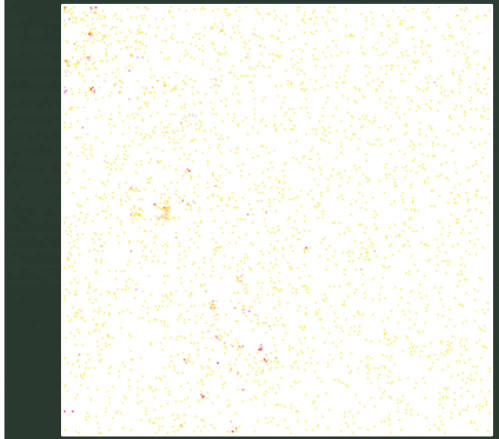
Application : Datagram Behavior

Goal : Detecting Malicious Communication Flows

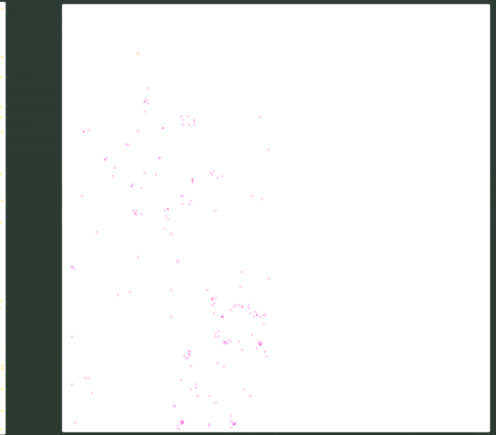
Advantages

(1) No need of detecting applications and protocols
(2) Need full packet capture, but no need of inspection : Just counting
(3) Can be processed on the edge switch

- Converting one flow to one image.
  - Apply images to CNN
- Converting 16bit HEX data to X and Y axis
  - X (256) and Y(256)
- RGB Color : Number of 16bit HEX data
  - Color shows the Density of data (16bit)



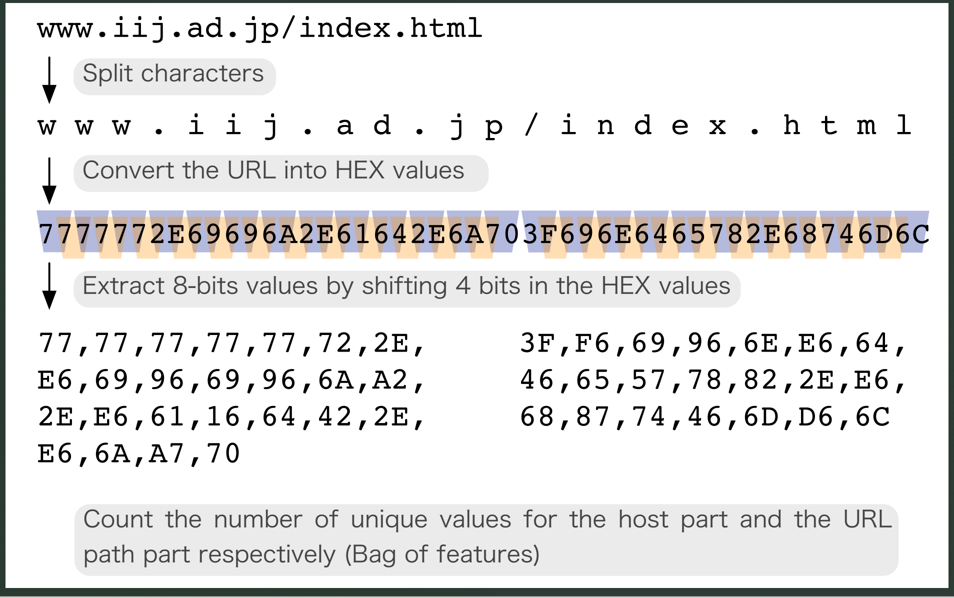
Benign



Malicious

Application : URL Detection

- Detection the URL of Malicious Web Site
  - Using only URL information
- Converting URL into Byte Stream as Bag-of-Bytes
  - Not URL semantics
  - Just a Byte Stream
  - Same as Image Processing
- Applying Byte Patterns against Neural Network



```
www.iij.ad.jp/index.html
```

Split characters

```
w w w . i i j . a d . j p / i n d e x . h t m l
```

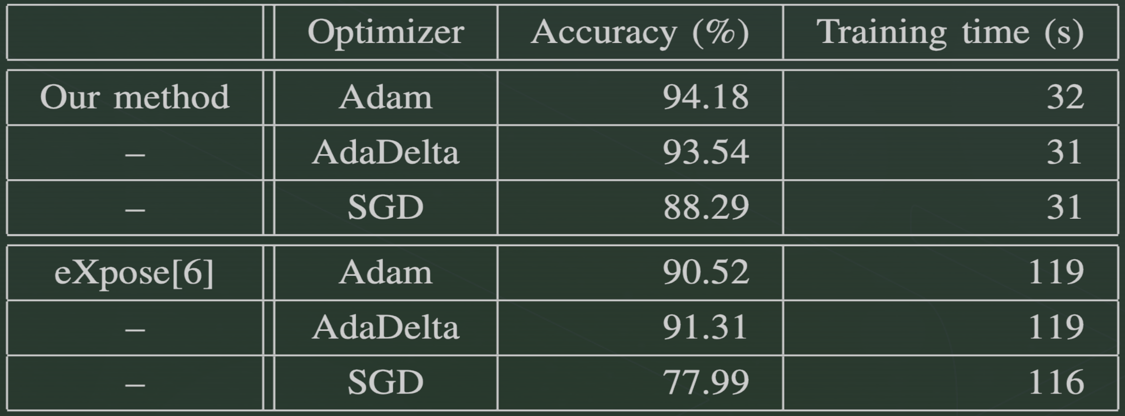
Convert the URL into HEX values

```
7777772E69696A2E61642E6A703F696E6465782E68746D6C
```

Extract 8-bits values by shifting 4 bits in the HEX values

```
77,77,77,77,77,72,2E,     3F,F6,69,96,6E,E6,64,
E6,69,96,69,96,6A,A2,     46,65,57,78,82,2E,E6,
2E,E6,61,16,64,42,2E,     68,87,74,46,6D,D6,6C
E6,6A,A7,70
```

Count the number of unique values for the host part and the URL path part respectively (Bag of features)



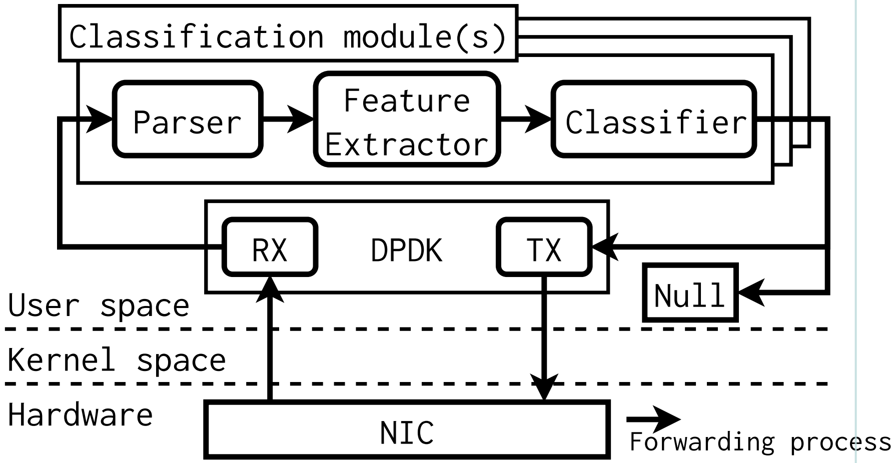
	Optimizer	Accuracy (%)	Training time (s)
Our method	Adam	94.18	32
–	AdaDelta	93.54	31
–	SGD	88.29	31
eXpose[6]	Adam	90.52	119
–	AdaDelta	91.31	119
–	SGD	77.99	116

Keiichi Shima, Daisuke Miyamoto, Hiroshi Abe, Tomohiro Ishihara, Kazuya Okada, Yuji Sekiya, Hirohchika Asai, Yusuke Doi, “Classification of URL bitstreams with Bag of Bytes”, First International Workshop on Network Intelligence (NI2018), 20-22 February 2018

Edge Device

- Switch Type PC with INTEL NICs
  - Apply DPDK Technology for Pre-Processing
- Processing the packets for simple counting and classification
  - Send processed data to server or cloud.

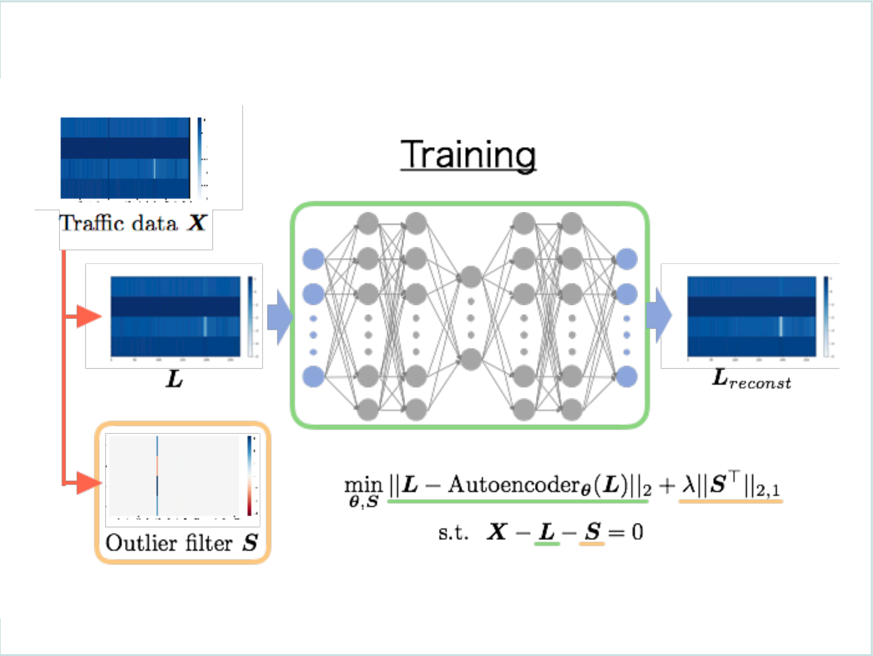
Toki Suga, Kazuya Okada, Hiroshi Esaki, "Toward Real-time Packet Classification for Preventing Malicious Traffic by Machine Learning", 1st International Workshop on Artificial Intelligence and Machine Learning Techniques for Enhanced Network Management (AIMLEM 2019), February 2019.

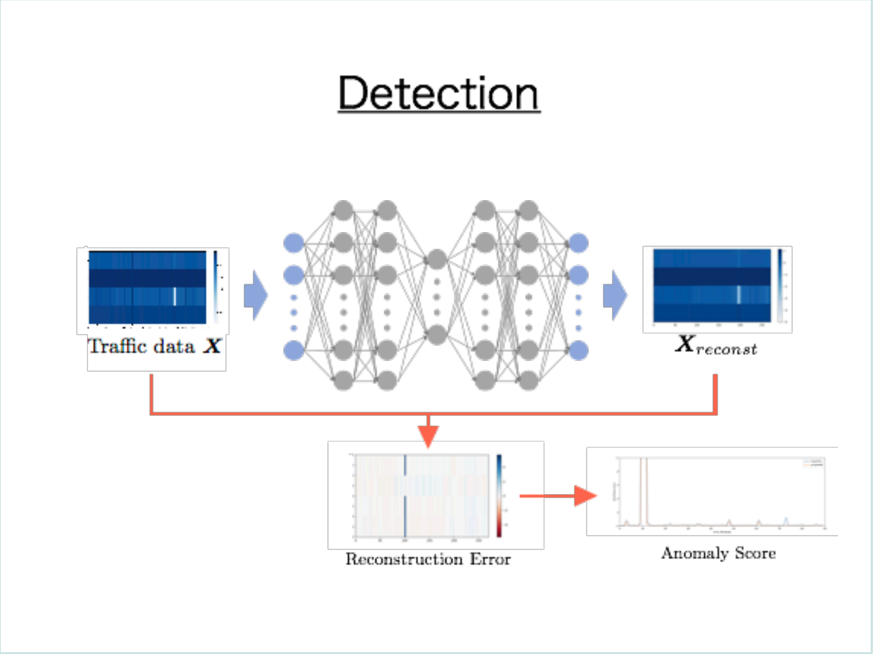


Problem : Not enough Training Datasets

- Datasets from network devices and packets are mixture of malicious and benign communications
  - Need more training datasets labeled
  - No universality of network traffic : depend on the users
- Applying SEMI-Supervised Method
- Trying to apply Robust Auto-Encoder

Gaku Kotani and Yuji Sekiya, "Unsupervised scanning behavior detection based on distribution of network traffic features using robust autoencoders", 1st IEEE International Workshop on Adapting Data Mining for Security (ADMiS) 2018, Singapore, November 2018.


Training
Traffic data $\boldsymbol{X}$
$\boldsymbol{L}$
$\boldsymbol{L}_{reconst}$
Outlier filter $\boldsymbol{S}$
$\min_{\theta,\boldsymbol{S}} ||\boldsymbol{L} - \text{Autoencoder}_{\boldsymbol{\theta}}(\boldsymbol{L})||_2 + \lambda||\boldsymbol{S}^\top||_{2,1}$
s.t. $\boldsymbol{X} - \boldsymbol{L} - \boldsymbol{S} = 0$



Need for Open Datasets

Providing Open Datasets for Cybersecurity Researches

- Traffic Flows
- DNS name resolution logs
- IDS logs

Beware for privacy issues

- Anonymization and removing personal identification

Previous Case : MAWI datasets

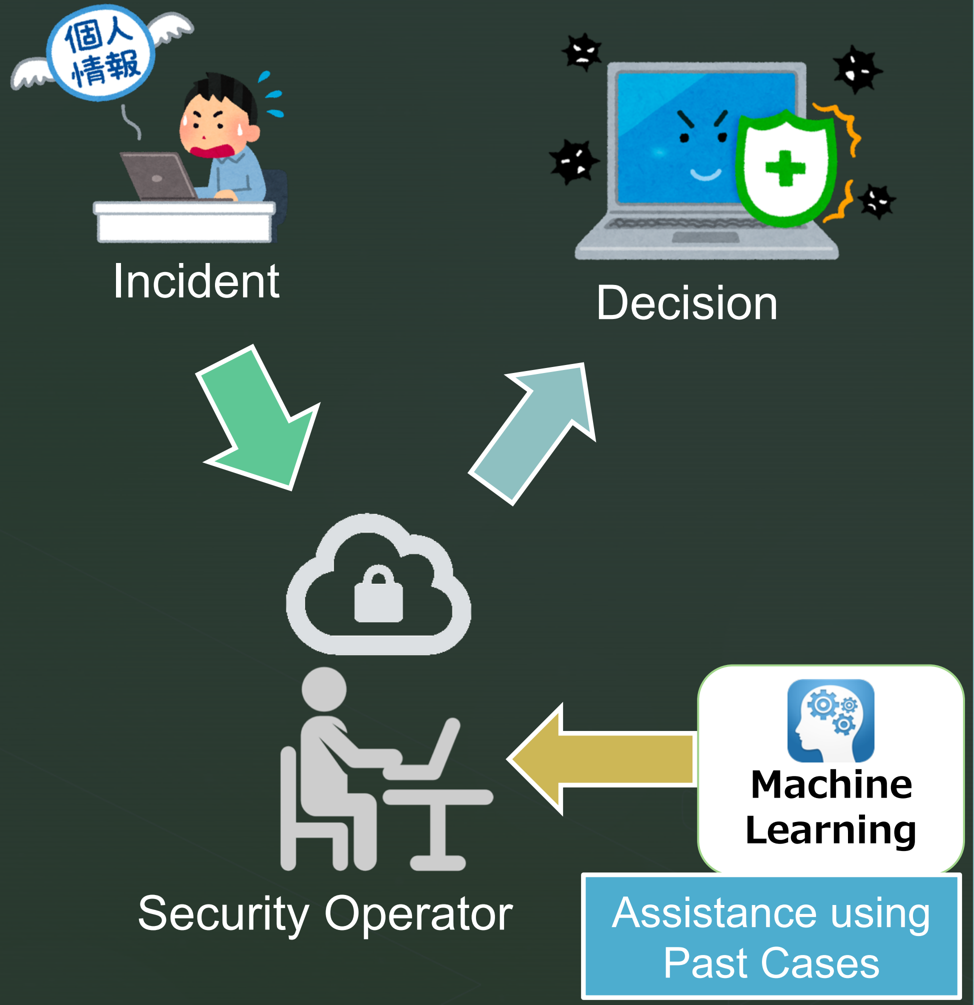
- WIDE Project

Proactive Approach - Decision

- When an incident occurred,
  1. Decide the first action
  2. Find the evidences of the attack
  3. Identify the scope of impact
  4. Decide a fundamental countermeasure

This is Incident Response !!

- It highly depends on the person's skills to perform these workflows
- Applying AI technology
  - Assist to find the traces of the attackers
  - Assist to make a decision of the first action



Incident

Decision

Security Operator

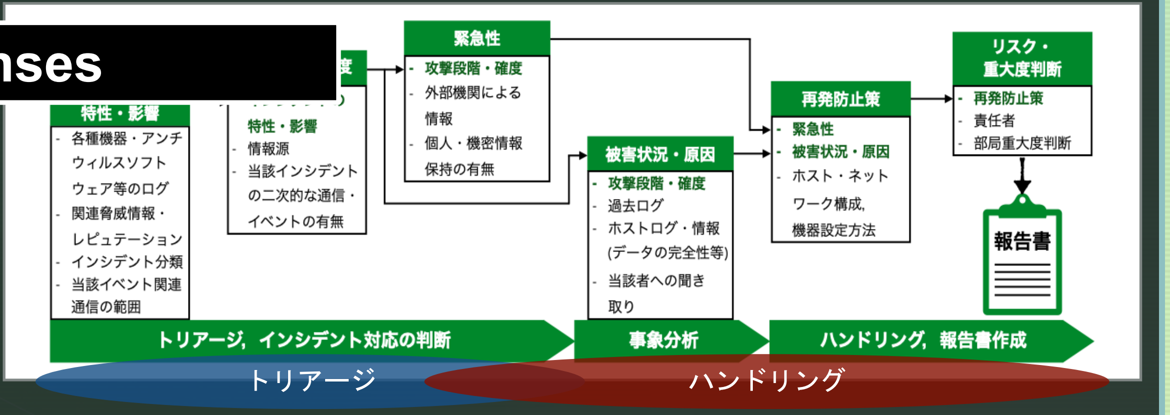
Machine Learning

Assistance using Past Cases

Normalization of Knowledges

Workflow of Incident Responses

- Using Real CERT incident handlings
- Classification of handling steps
- Classification incidents based on NIST and MITRE CAPEC standards



特性・影響
- 各種機器・アンチウィルスソフトウェア等のログ
- 関連脅威情報・レピュテーション
- インシデント分類
- 当該イベント関連通信の範囲

特性・影響
- 情報源
- 当該インシデントの二次的な通信・イベントの有無

緊急性
- 攻撃段階・確度
- 外部機関による情報
- 個人・機密情報保持の有無

被害状況・原因
- 攻撃段階・確度
- 過去ログ
- ホストログ・情報(データの完全性等)
- 当該者への聞き取り

再発防止策
- 緊急性
- 被害状況・原因
- ホスト・ネットワーク構成,機器設定方法

リスク・重大度判断
- 再発防止策
- 責任者
- 部局重大度判断

報告書

トリアージ, インシデント対応の判断

事象分析

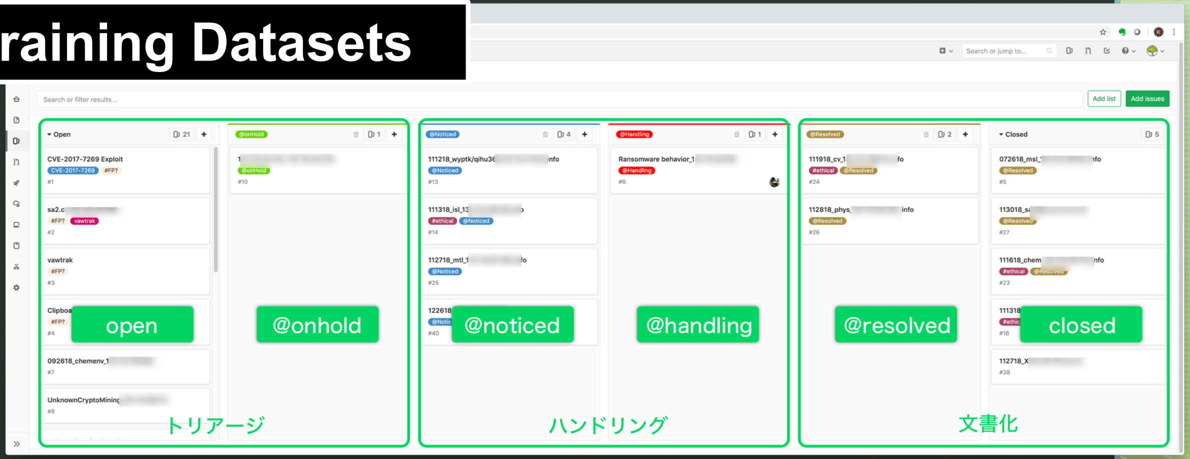
ハンドリング, 報告書作成

トリアージ

ハンドリング

Normalization of Cases and Making Training Datasets

- Making training datasets of incident response assistance
- Applying natural language processing
- Trying LSTM and other algorithms
- Ongoing works..



Open 21
- CVE-2017-7269 Exploit — CVE-2017-7269 #FP? — #1
- sa2.c[redacted] — #FP? vawtrak — #2
- vawtrak — #FP? — #3
- Clipboa[redacted] — #FP? — #4
- 092618_chemenv_1[redacted] — #7
- UnknownCryptoMining[redacted] — #8

@onHold 1
- 1[redacted] — @onHold — #10

@Noticed 4
- 111218_wyptk/qihu3[redacted]info — @Noticed — #13
- 111318_isl_13[redacted]o — #ethical @Noticed — #14
- 112718_mtl_1[redacted]fo — @Noticed — #25
- 122618[redacted] — @Notic — #40

@Handling 1
- Ransomware behavior_1[redacted] — @Handling — #6

@Resolved 2
- 111918_cv_1[redacted]fo — #ethical @Resolved — #24
- 112818_phys_[redacted]info — @Resolved — #26

Closed 5
- 072618_msl_[redacted]nfo — @Resolved — #5
- 113018_s[redacted] — @Resolved — #27
- 111618_chem[redacted]nfo — #ethical @Resolved — #23
- 111318 — #ethic — #16
- 112718_X[redacted] — #38

Classification of Security Documents using LDA

Incident Reports
Web Pages Related to Cybersecurity

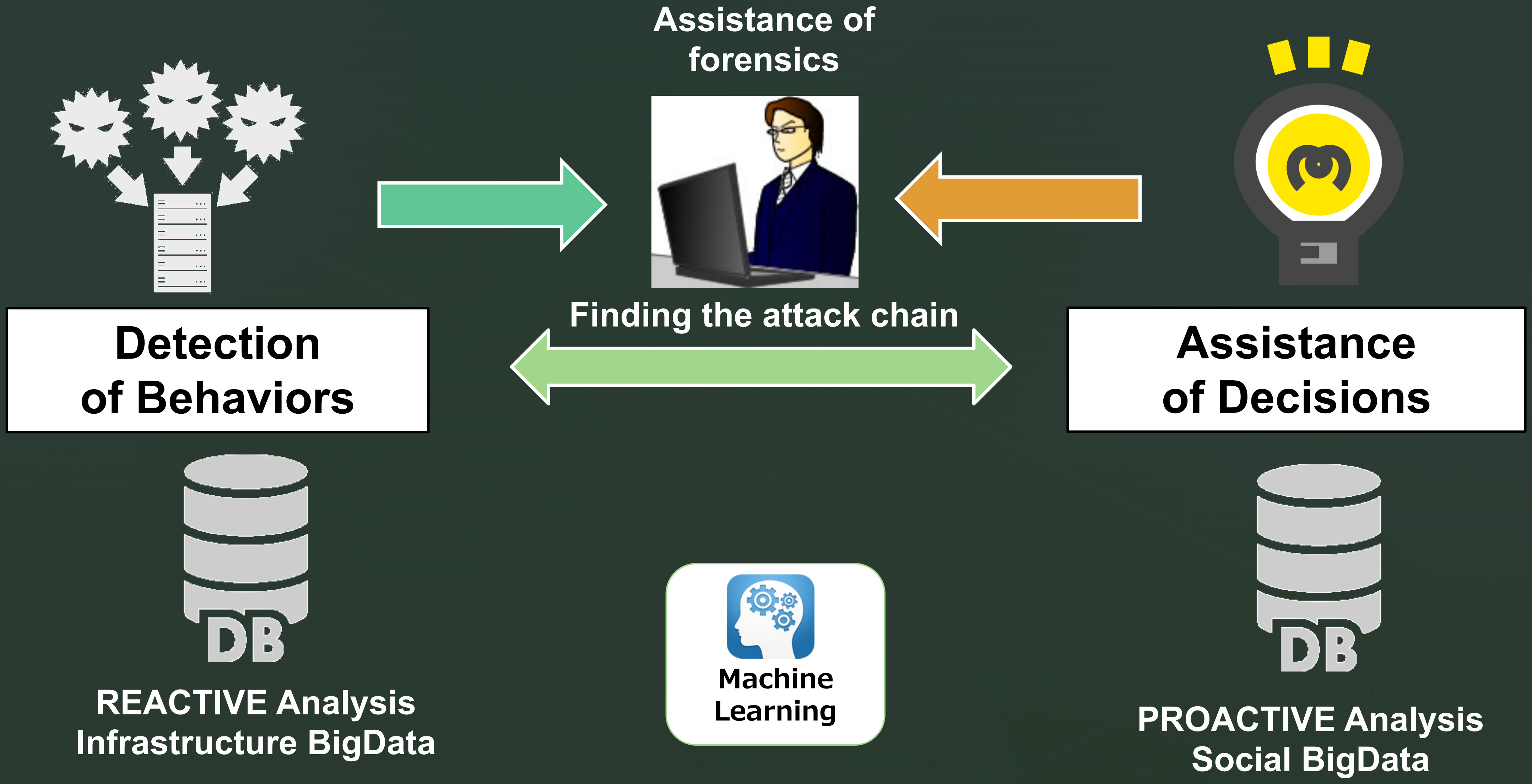
- **Attack Type**
- **Impact Range**
- **Urgency**
- **Countermeasure**

- Applying LDA (latent Dirichlet allocation) Algorithm to Classification of Documents
  - Need detailed categorization for cyber-security ⇒ LDA is not sufficient
  - The cost of making training datasets is large ⇒ Supervised Model is not good

⇒ **Seeded LDA: Try SEMI-Supervised Model**

- Datasets and Analysis
  - Datasets：CERT Report of TITECH + Blogs of Security Vendors
  - Classification：Incident Types and Attack Types
  - Evaluation
    - ❖ Comparison of labeld LDA and seeded LDA
    - ❖ Appropriateness of seeds
    - ❖ Picking up similar attacks and incidents

The Proposed Architecture of Our System



Assistance of forensics

Finding the attack chain

Detection of Behaviors

Assistance of Decisions

REACTIVE Analysis
Infrastructure BigData

Machine Learning

PROACTIVE Analysis
Social BigData

THANK YOU

This work is supported by JST CREST Grant Number JPMJCR1783, Japan.

https://nml.ai/