THE CHALLENGES OF ASSISTING THREATS DETECTION, ANALYSIS, AND RESPONSE BY DATA-MINING TECHNOLOGY

NETWORK MUSCLE LEARNING (NML) PROJECT

YUJI SEKIYA (THE UNIVERSITY OF TOKYO)

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 ?

CHALLENGES OF THIS RESEARCH

1. Attacks and Anomality Detection using Big Datasets and Machine Learning.
   - Combination with existing IDS/IPS devices
2. Finding the motivation of attackers
   - Social Datasets : Web, SNS, Dark Web
   - Some motivations for attacks such as politics issue, making money, and memorial days.
3. Assistance of Incident / Response
   - Collecting Incident / Response cases
   - Assist non-expert security operators to analysis attacker's behaviors and their decision of incident response.
4. Providing Open Datasets
   - Datasets for future researches

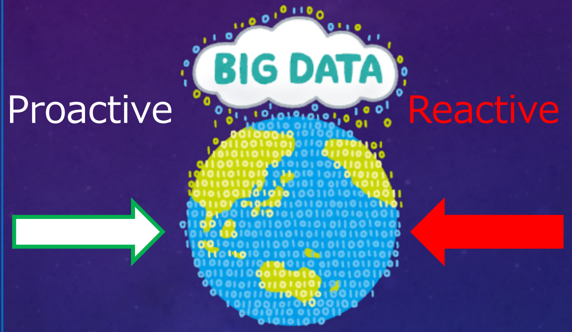
APPROACH

PROACTIVE Cyber Defense using Social Datasets

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

Social Datasets

AI for Cybersecurity

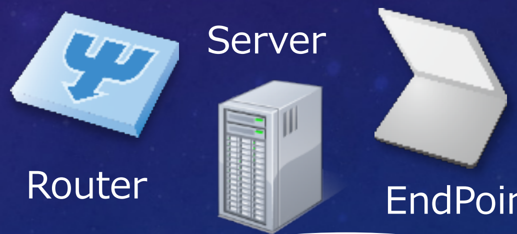


Motivation and Evidence of attacks

Assistance of Analysis and Incident Response For Non-Experts

REACTIVE Cyber Defense using Infra Datasets

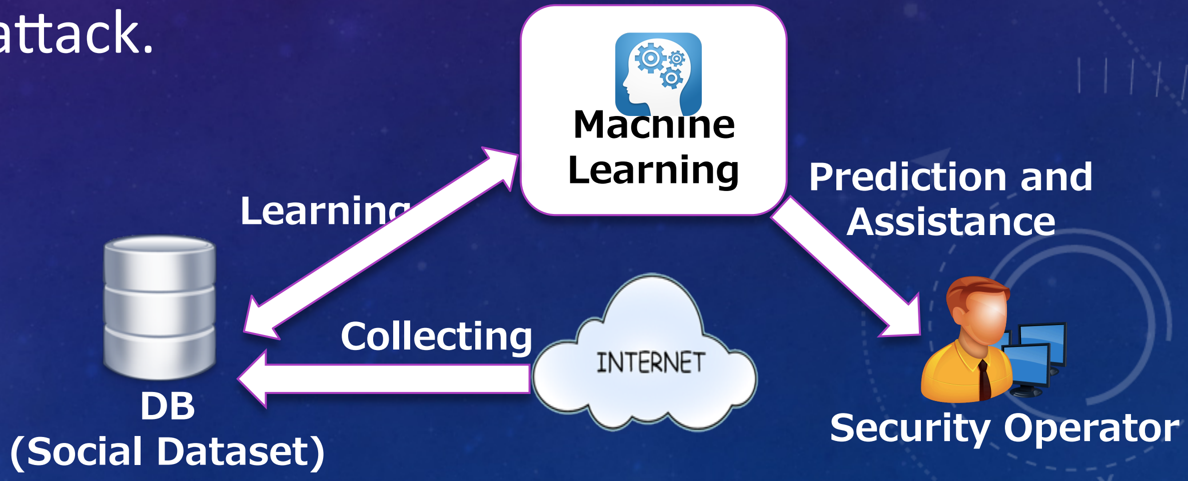
Collect cyber threat data aimed at network devices, servers, client terminals, etc.



Network Infrastructure Datasets

PROACTIVE APPROACH

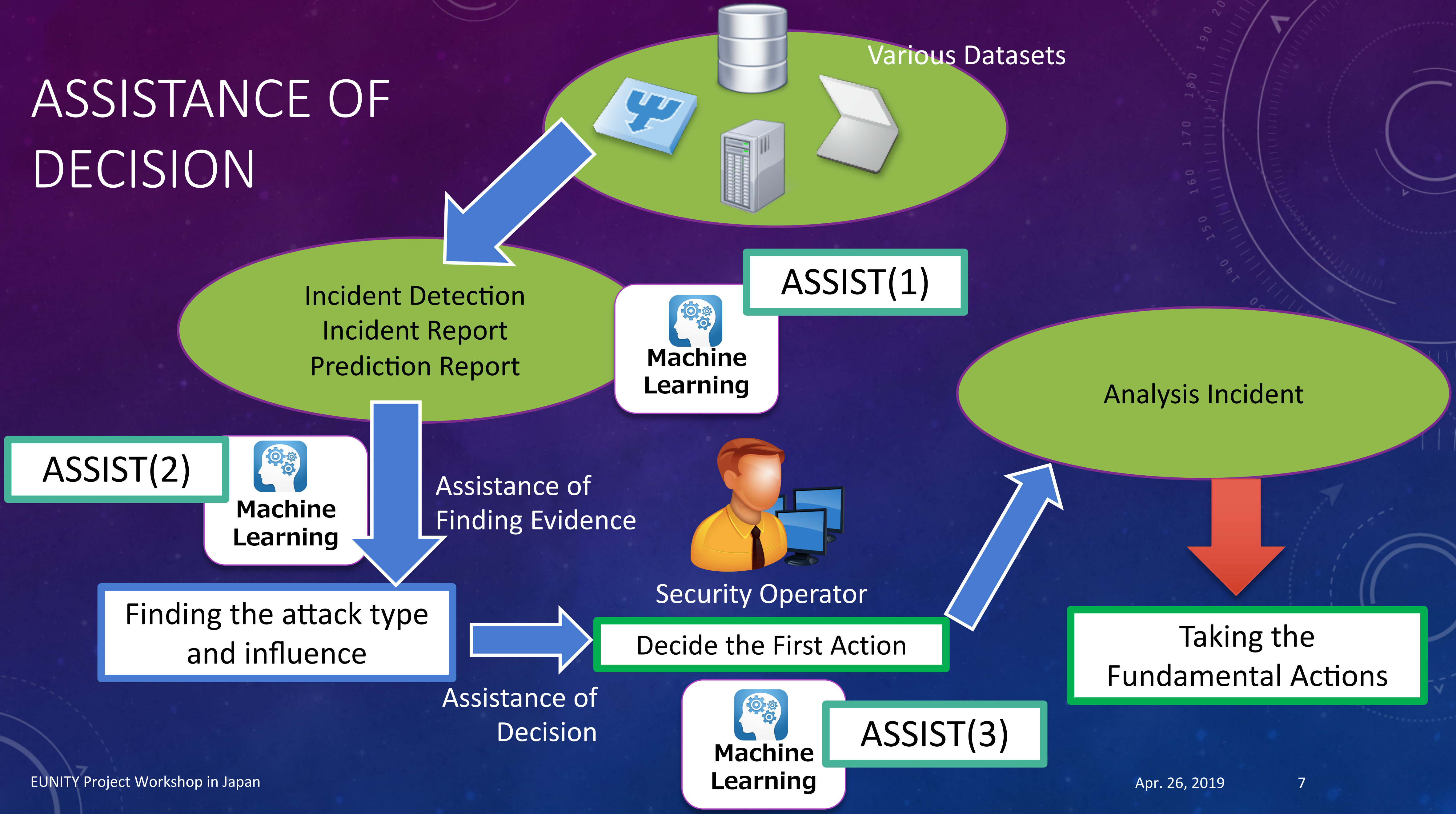
- Picking up social trends published in SNS, Web, etc…
  - Tweets of important users.
  - Articles showing political, social and religious trends.
- There is always "intent" or "motive" in the attack.
  - It is political or financial purpose.
  - Collecting from Dark Web Sites.
- By collecting these information and learn the relationship with cyber attacks, can we predict a trend of cyber threat ?



REACTIVE APPROACH

- When an incident occurred
- Security Operator will …
    1. Decide the first action
    2. Find the evidences of the attack
    3. Identify the scope of impact
    4. Decide a fundamental countermeasure
- It highly depends on the person's skills to perform these workflows
- AI can
    - Assist to find THE BEHAVIOR of ATTACKERS
    - Assist to make a decision of THE FIRST ACTION

ASSISTANCE OF DECISION



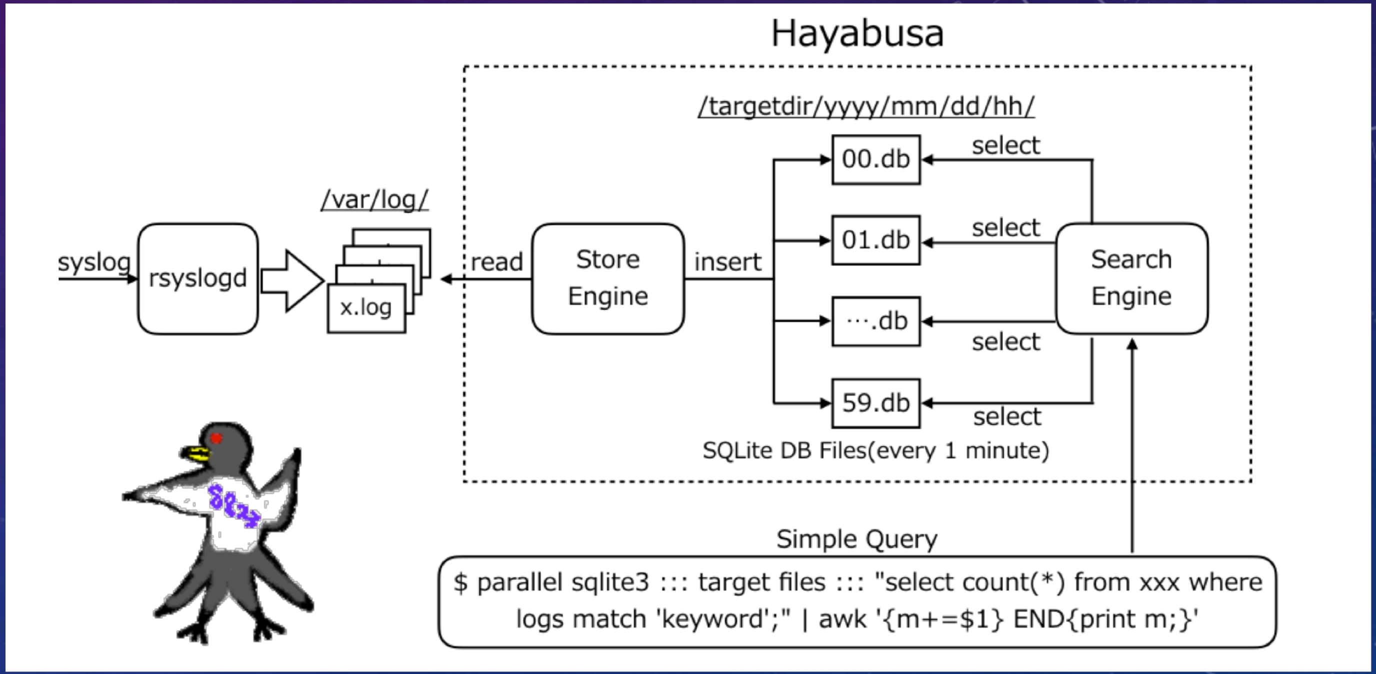
REACTIVE APPROACH : DATASET COLLECTION

DATASET COLLECTION

- To assist a Security Operator in REACTIVE APPROACH
  - Collecting various kinds of data from network infrastructure in real time and store them uniformly
  - Providing high-speed and full-text search by keywords as following.
    - IP address, port number, user name, domain name, etc…
- We evaluated
  - Google Big Query
  - Elastic Search
- We build our own system : HAYABUSA
  - Collecting over 100k messages per second
  - Searching keywords in few seconds from over hundreds of millions messages.

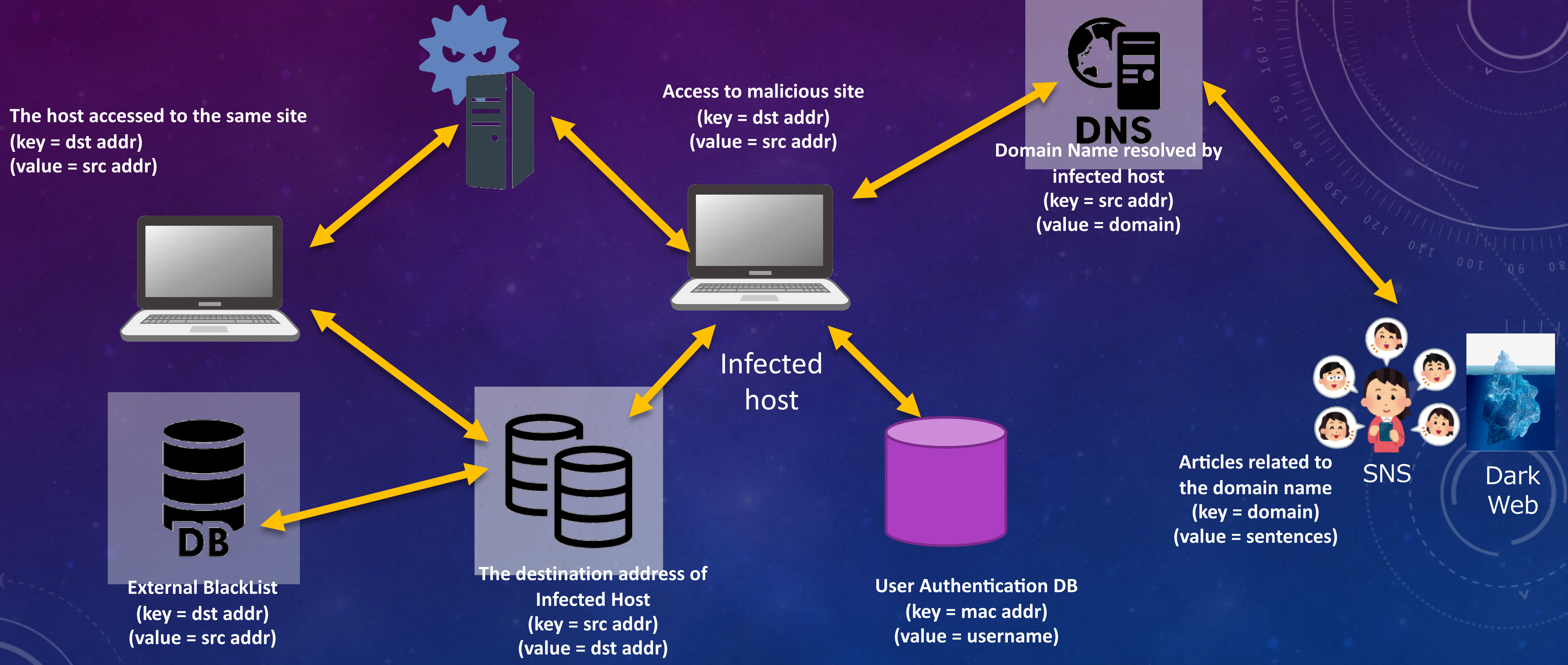
DATASET COLLECTION

- Design and Implementation of Data Collection System
  - Developed by IIJ Team
- HAYABUSA
  - Using all CPU cores for searching
  - Full text indexed search
  - Collecting over 100k lines / sec in real-time

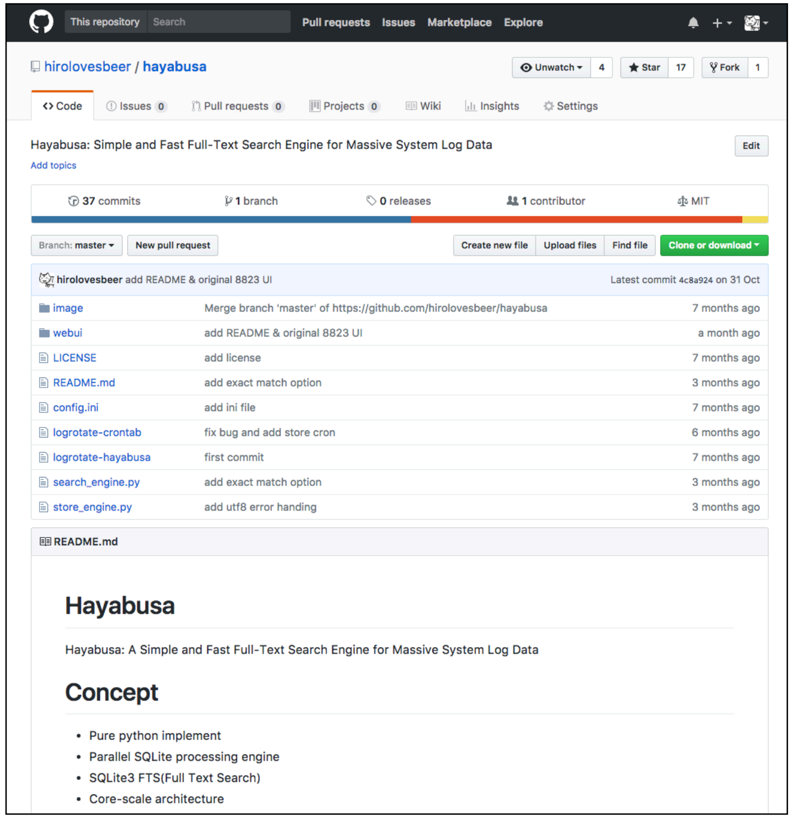


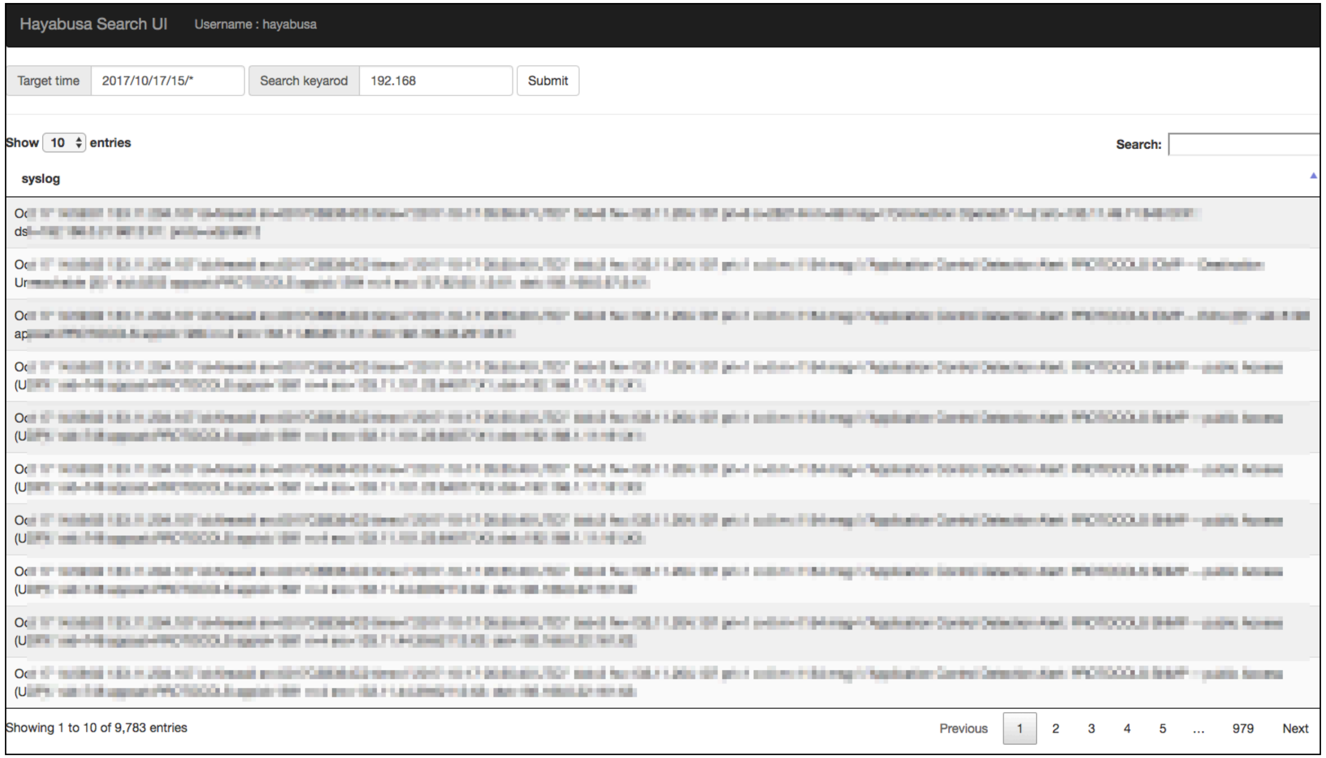
Hiroshi Abe, Keiichi Shima, Yuji Sekiya, Daisuke Miyamoto, Tomohiro Ishihara, and Kazuya Okada, "Hayabusa: Simple and Fast Full-Text Search Engine for Massive System Log Data", Proceedings of the 12th International Conference on Future Internet Technologies, ACM, DOI: 10.1145/3095786.3095788, June 2017

ASSISTANCE OF FINDING ATTACKER’S BEHAVIORS



HAYABUSA : OPEN SOURCE SOFTWARE





13

[redacted]

REACTIVE APPROACH : PICTURIZATION

DEFINING FEATURE VALUES OF DATASET

Collection → **Characteristic** → **Pattern Recognization**

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

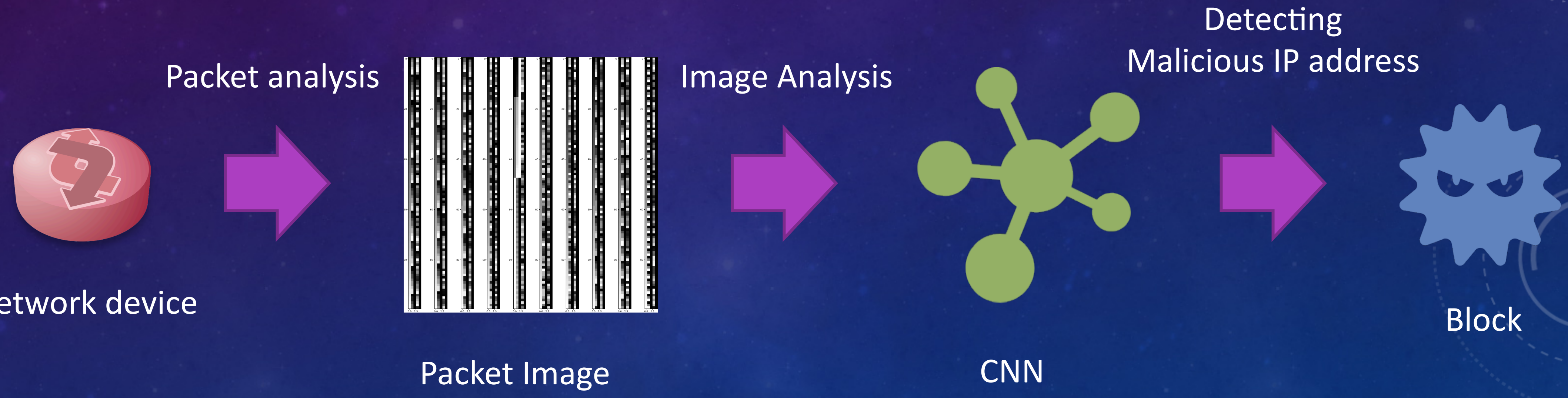
How convert the dataset to feature values ?

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

- Collection
  - Network dataset tends to be large amount
- Converting Feature Value
  - Which values are useful ?
  - Need semantics ?

BASIC IDEA OF PICTURIZATION

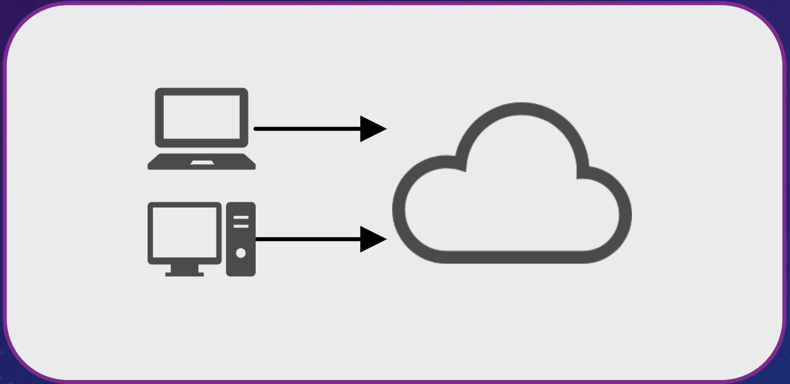
- Detecting malicious IP address using images
- The images are generated following packet arrival interval
- Using Darknet and Honeypot data as learning dataset



ANALYSIS OF HOST BEHAVIOR

TCP SYN Packets

- This method can apply to the analysis of the behavior of hosts.
- Just using SYN packets, it can be analyzed on over 100Gbps links.

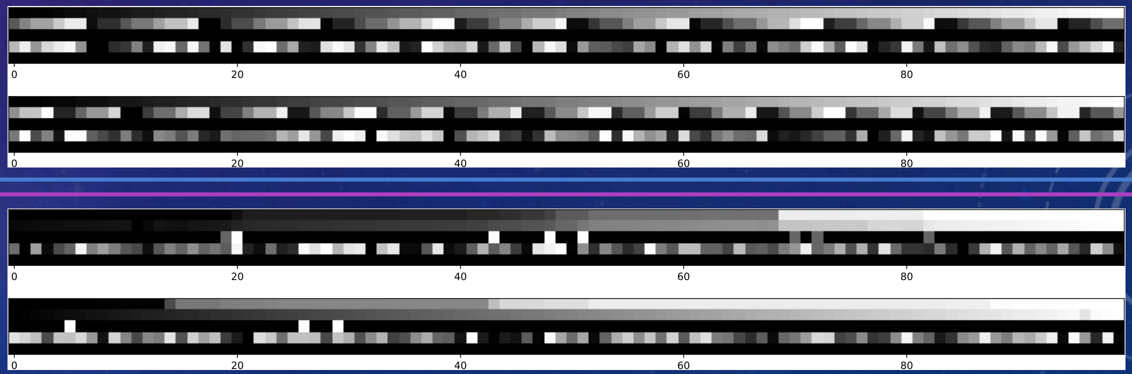


Picturize SYN Packet BEHAVIORS

- Not 5 tuples, just using timestamp, window size, sequence number
- Converting host behaviors to a image and process it using CNN algorithm

BAD

GOOD



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

ANALYSIS OF ACCESSED URL

- Analysis URL literatures as just a BYTE STREAM
- Bag-of-Bytes Processing
- Real-time Detection

	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

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,
E6,69,96,69,96,6A,A2,
2E,E6,61,16,64,42,2E,
E6,6A,A7,70

3F,F6,69,96,6E,E6,64,
46,65,57,78,82,2E,E6,
68,87,74,46,6D,D6,6C

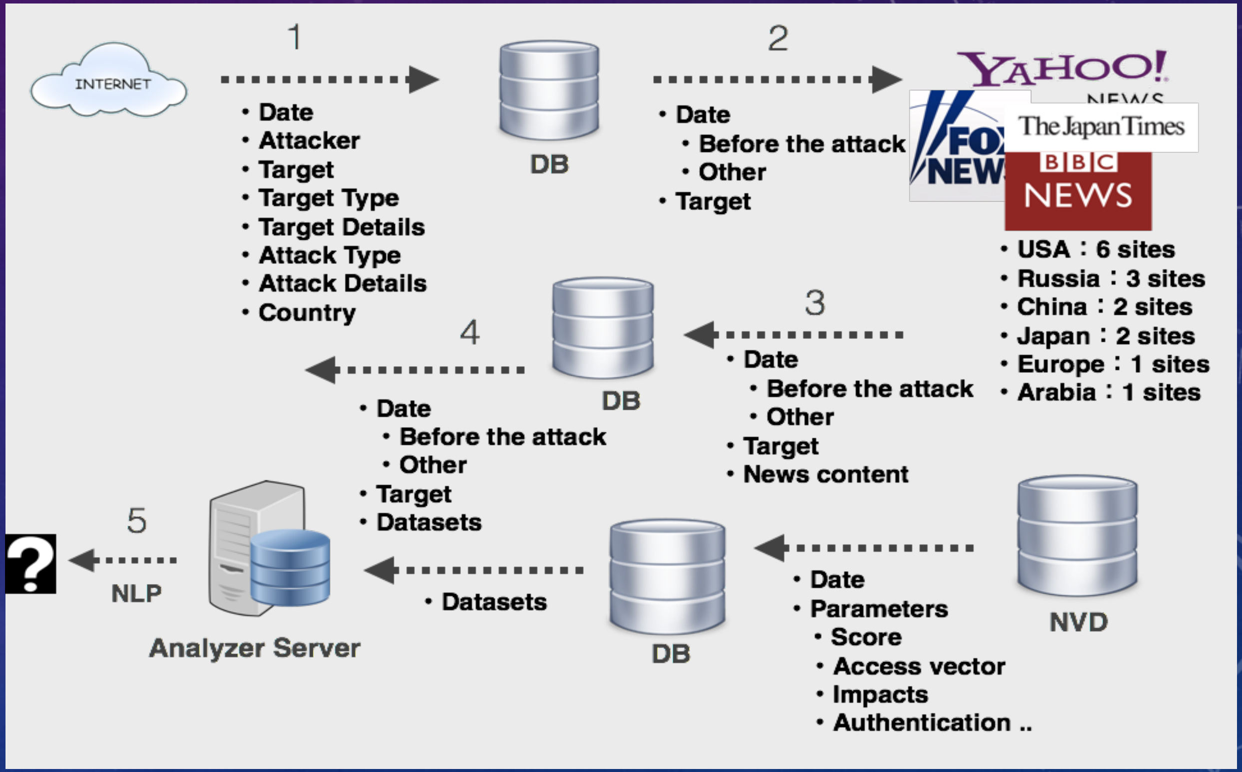
Count the number of unique values for the host part and the URL path part respectively (Bag of features)

[1] 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), DOI : 10.1109/ICIN.2018.8401597, 20-22 February 2018
[2] J. Saxe and K. Berlin, "eXpose: A character-level convolutional neural network with embeddings for detecting maliciou URLs, file paths and registry keys," *CoRR*, vol. abs/1702.08568, February 2017.

PROACTIVE APPROACH : MOTIVATION ANALYSIS

ANALYSIS OF ATTACKER'S MOTIVATION

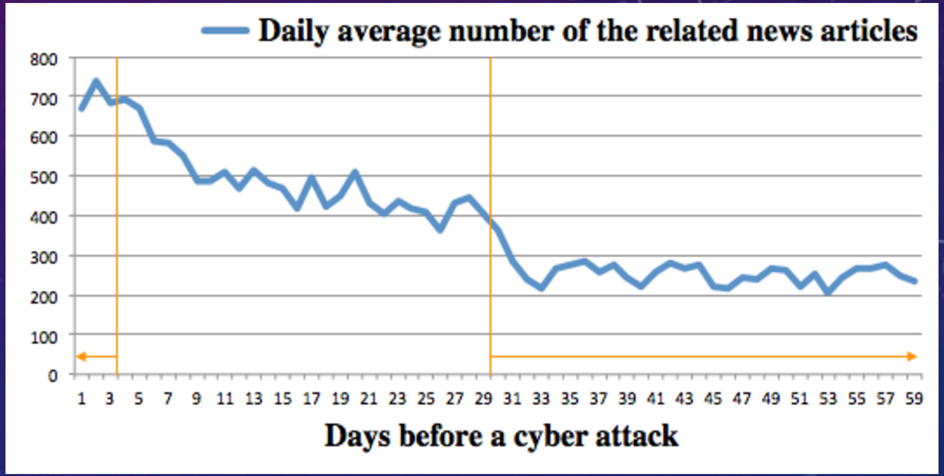
- Social Dataset Collection System
  - SNS
  - Surface Web
  - Dark Web
- Finding the Related Sentence and Keywords of Attacking
  - Making Learning Dataset from the Past Attacks
  - Natural Language Processing
- Prototype Works



Munkhdorj Baaatarsuren, and Yuji Sekiya, "Cyber attack prediction using social data analysis", IOS Press, Journal of High Speed Networks, vol. 23, no. 2, pp. 109-135

PRELIMINARY EVALUATION

- Finding the motivation of Past Real Attacks
- Collecting Past Real Attacks
  - Categorized by Incident Types
  - TA : Targeted Attack, AH : Account Hijacking, DDoS, SQL Injection
- Collecting SNS Datasets, Web Pages
  - Any Signs of Attacks ?
- Making Labeled Datasets



Prediction accuracy of the experiments using SVM

	TA	AH	DDoS	SQLi
Vector A	62.4%	60.7%	70.3%	59.1%
Vector A*	61.0%	56.7%	62.0%	53.4%
Vector B	56.0%	64.0%	62.0%	56.8%

NATURAL LANGUAGE PROCESSING OF INCIDENTS

- Incident Log including Human Interactions of E-mails
- Teacher Datasets
  - E-mails of Incident Response
  - The reason of the Incident and the Countermeasure
- First Step :
  - Assistance using the Similar Incident Response
- Future Goals :
  - More complicated Assistances by Chat Bot
  - Assistances of Forensics by Datasets Analysis

Report of Incident

Event ID:xxxxxxxxxxxxxx
Event Summary: WordPress Login Brute Force Attempt
Occurrence Count: 7

Host and Connection Information
Source IP: 192.0.2.xxx
Source Port: aaaaa
Destination IP: 10.0.0.yyy
Destination Port: 80
Destination IP Geolocation: Somewhere, USA
Connection Directionality: OUTGOING
Protocol: TCP

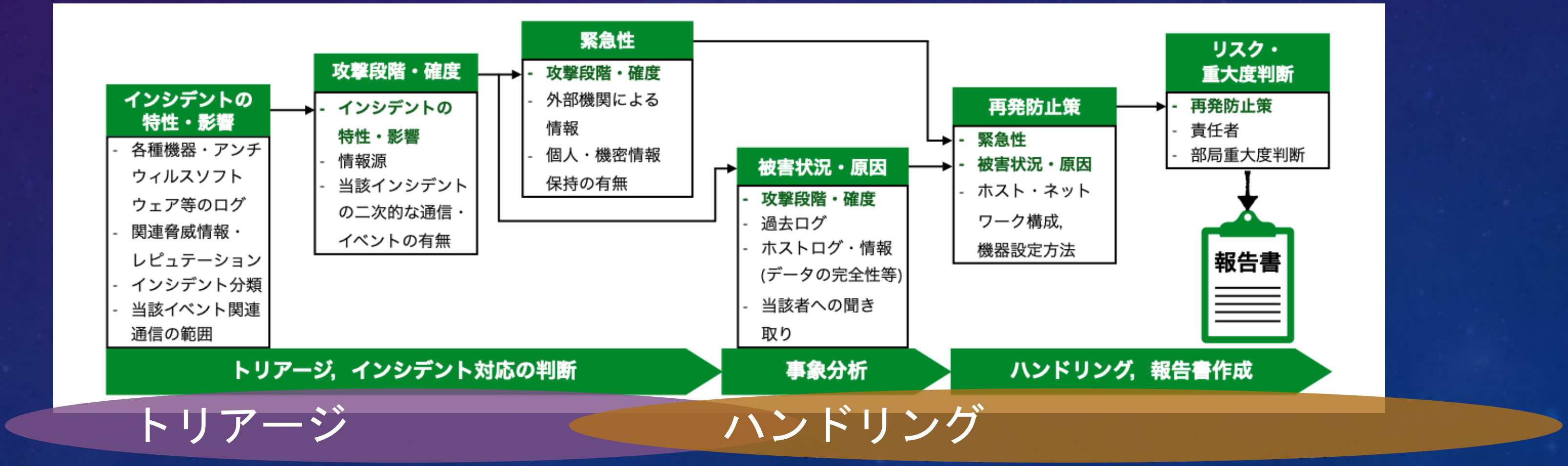
Log Time: 2018-11-xx at 01:10:xx
Action: Not Blocked
CVSS Score: -1
Vendor Classification: THREAT,vulnerability
Vendor Priority: critical
Threat Name: WordPress Login Brute Force Attempt

Event Detail:
Nov xx 01:10:xx ,2018/11/xx 01:10:xx,0000,THREAT,vulnerability,1, 2018/11/xx 192.0.2.xxx, 10.0.0.yyy, 192.0.2.xxx, allow,,,web-browsing,.....,trust,untrust, ...,tcp,alert, "wp-login.php",WordPress Login Brute Force Attempt(40044), educational-institutions,critical,client-to-server,.....

NORMALIZATION OF INCIDENT RESPONSE FLOWS

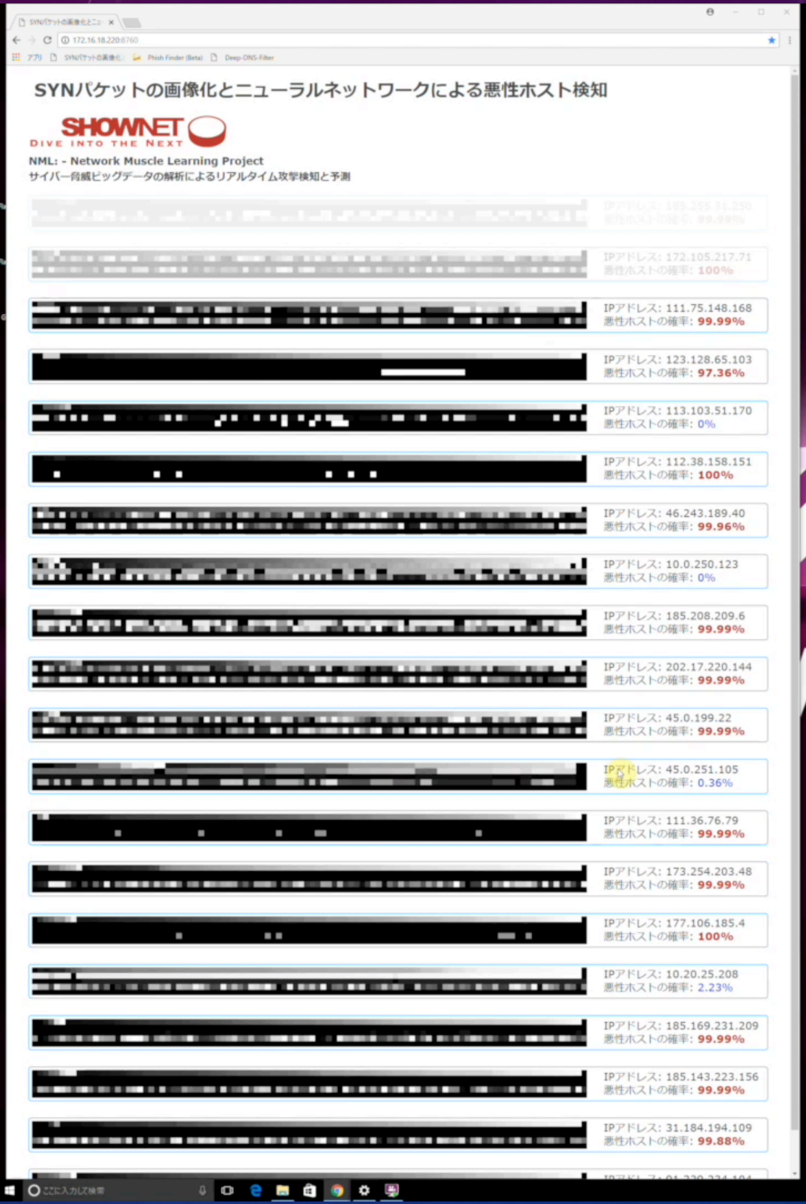
- Making Labeled Datasets of Incident Response Flow
  - Need Normalized and Labeled Datasets for Machine Learning
  - Using Natural Language Processing for Analysis
- Assistance of the FIRST DICISION of Security Operators
  - Helping them for Analysis Datasets and
  - Making a kind of Chat Bot for Assistance

[1] 石井将大, 森健人, 松浦知史, 金勇, 北口善明, 友石正彦 : “東工大CERTにおけるインシデント対応の分析とその自動化に関する考察”, 研究報告 インターネットと運用技術 (IOT), 2018



DEMONSTRATION IN INTEROP TOKYO 2018

- We had a demonstration in IT event, called Interop Tokyo 2018
  - Three days events
  - 140,000 people were join
- We measured the Real-Time Network Traffic in the venue
- Detecting Malicious Behaviors using Machine Learning
  - Attack from outside and inside
  - Accessing malicious sites



SYNパケットの画像化とニューラルネットワークによる悪性ホスト検知
SHOWNET
DIVE INTO THE NEXT
NML: - Network Muscle Learning Project
サイバー脅威ビッグデータの解析によるリアルタイム攻撃検知と予測
IPアドレス: 172.105.217.71
悪性ホストの確率: 100%
IPアドレス: 111.75.148.168
悪性ホストの確率: 99.99%
IPアドレス: 123.128.65.103
悪性ホストの確率: 97.36%
IPアドレス: 113.103.51.170
悪性ホストの確率: 0%
IPアドレス: 112.38.158.151
悪性ホストの確率: 100%
IPアドレス: 46.243.189.40
悪性ホストの確率: 99.96%
IPアドレス: 10.0.250.123
悪性ホストの確率: 0%
IPアドレス: 185.208.209.6
悪性ホストの確率: 99.99%
IPアドレス: 202.17.220.144
悪性ホストの確率: 99.99%
IPアドレス: 45.0.199.22
悪性ホストの確率: 99.99%
IPアドレス: 45.0.251.105
悪性ホストの確率: 0.36%
IPアドレス: 111.36.76.79
悪性ホストの確率: 99.99%
IPアドレス: 173.254.203.48
悪性ホストの確率: 99.99%
IPアドレス: 177.106.185.4
悪性ホストの確率: 100%
IPアドレス: 10.20.25.208
悪性ホストの確率: 2.23%
IPアドレス: 185.169.231.209
悪性ホストの確率: 99.99%
IPアドレス: 185.143.223.156
悪性ホストの確率: 99.99%
IPアドレス: 31.184.194.109
悪性ホストの確率: 99.88%

THANK YOU

THIS WORK WAS SUPPORTED BY JST CREST GRANT NUMBER JPMJCR1783, JAPAN.