

# Network intrusion (ネットワークへの侵入)

## 機能の視点

Attack reference  
Attack type  
Sub-category of attack  
Host information  
Malicious scripts  
Etc

## 通信の視点

Imbalanced number of harmful attacks

これに対応するために、Transformerでtransferを学習する侵入検知システム  
IDS-INT: Intrusion Detection System- Imbalanced Network Traffic

# ネットワーク侵入検出はAIを活用する時代に

これまでのNIDS

Flow-based

パケットの通信ヘッダー情報による  
検出システム

パケットに事前定義したラベルを当  
てはめて分類

新しいNIDS

Packet-level

パケットに含まれる全情報による  
検出システム

パケットの特徴に基づいたタグを生  
成しこのタグを使ってパケットの内  
容と潜在的なリスクを表示

## Embeddingを使用したタグ分類

1. Transformerを用い、各パケットにembeddingを生成。← セマンティック情報を含む
2. ネットワーク専用コーパスを使い、パラグラフレベルで近しいembeddingを特定 ← N-gram word extraction
3. クラスタリングで、パケットを24クラスに分類 ← K-means Cluster Analysis
4. 入力パケットに対し、単純なクラス分類より説明的なラベルを付与できる。



事前に定義されたクラスに属さないパケットに対しても近しいタグを割り当てることができる。

## 専用データセットを使用

CIC-IDS2017 (packetフォーマットはEthernet)

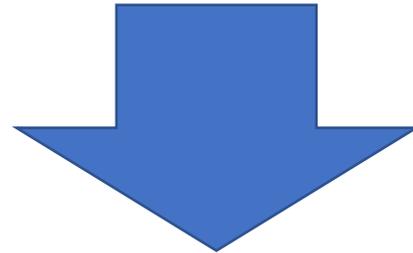
2.27M 通常フロー

557K 攻撃フロー

UNSW-NB15 (packetフォーマットはCooked Linux)

1.96M 通常フロー

99.6K 攻撃フロー



Combined Dataset

専用加工して統合。24クラス分類に整理



# 入力するパケット例

The image shows a Wireshark packet capture analysis. The main pane displays a list of network packets. Packet 2417 is selected, showing it is a TCP segment of a reassembled PDU. The packet details pane is expanded to show the 'TCP payload (1440 bytes)' section, which is further expanded to show the 'Reassembled PDU in frame: 2417' section. The hex stream pane shows the raw data of the payload, with a blue box highlighting a portion of it. A callout box points to this hex stream with the text 'パケット全体をHex streamとして出力を取り出すことが可能' (It is possible to output the entire packet as a hex stream). Another callout box points to the 'TCP payload (1440 bytes)' section with the text '1440バイトのTCP payload' (1440 bytes of TCP payload).

No.	Time	Source	Destination	Protocol	Length	Info
2412	22.036166	2409:10:c300:200:5...	2603:1036:2404:1:1...	TCP	74	50021 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
2413	22.037698	2409:10:c300:200:5...	2603:1036:2404:1:1...	TLSv1	259	Client Hello (SNI=mexus.officeapps.live.com)
2414	22.204669	2603:1036:2404:1:1...	2409:10:c300:200:5...	TCP	1514	443 → 50021 [ACK] Seq=1 Ack=186 Win=525312 Len=1440 [TCP segment of a reassembled PDU]
2415	22.204672	2603:1036:2404:1:1...	2409:10:c300:200:5...	TCP	1514	443 → 50021 [ACK] Seq=1441 Ack=186 Win=525312 Len=1440 [TCP segment of a reassembled PDU]
2416	22.204673	2603:1036:2404:1:1...	2409:10:c300:200:5...	TCP	1514	443 → 50021 [ACK] Seq=2881 Ack=186 Win=525312 Len=1440 [TCP segment of a reassembled PDU]
2417	22.204674	2603:1036:2404:1:1...	2409:10:c300:200:5...	TCP	1514	443 → 50021 [ACK] Seq=4321 Ack=186 Win=525312 Len=1440 [TCP segment of a reassembled PDU]
2418	22.204675	2603:1036:2404:1:1...	2409:10:c300:200:5...	TLSv1	362	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
2419	22.204859	2409:10:c300:200:5...	2603:1036:2404:1:1...	TCP	74	50021 → 443 [ACK] Seq=186 Ack=6049 Win=256064 Len=0
2420	22.205265	2409:10:c300:200:5...	2603:1036:2404:1:1...	TCP	74	[TCP Window Update] 50021 → 443 [ACK] Seq=186 Ack=6049 Win=262144 Len=0
2421	22.224990	2409:10:c300:200:5...	2603:1036:2404:1:1...	TLSv1	181	Client Key Exchange
2422	22.225077	2409:10:c300:200:5...	2603:1036:2404:1:1...	TLSv1	80	Change Cipher Spec
2423	22.225101	2409:10:c300:200:5...	2603:1036:2404:1:1...	TLSv1	119	Encrypted Handshake Message
2424	22.388124	2603:1036:2404:1:1...	2409:10:c300:200:5...	TCP	74	443 → 50021 [ACK] Seq=6049 Ack=344 Win=525056 Len=0
2425	22.389119	2603:1036:2404:1:1...	2409:10:c300:200:5...	TLSv1	125	Change Cipher Spec, Encrypted Handshake Message
2426	22.389275	2409:10:c300:200:5...	2603:1036:2404:1:1...	TCP	74	50021 → 443 [ACK] Seq=344 Ack=6100 Win=262080 Len=0
2427	22.390294	2409:10:c300:200:5...	2603:1036:2404:1:1...	TLSv1	396	Application Data
2428	22.390621	2409:10:c300:200:5...	2603:1036:2404:1:1...	TLSv1	367	Application Data
2429	22.553499	2603:1036:2404:1:1...	2409:10:c300:200:5...	TCP	74	443 → 50021 [ACK] Seq=6100 Ack=959 Win=524544 Len=0
2430	22.746246	192.168.1.11	52.192.46.121	TCP	54	50015 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
2431	22.781409	52.192.46.121	192.168.1.11	TCP	66	[TCP ACKed unseen segment] 443 → 50015 [ACK] Seq=1 Ack=2 Win=0 Len=0 TSval=9292265 TSecr=3825447753
2432	23.074868	2409:10:c300:200:5...	2404:6800:4004:81d...	UDP	195	64697 → 443 Len=133
2433	23.075604	2409:10:c300:200:5...	2404:6800:4004:81d...	UDP	128	64697 → 443 Len=66
2434	23.084214	2404:6800:4004:81d...	2409:10:c300:200:5...	UDP	94	443 → 64697 Len=32
2435	23.086140	2404:6800:4004:81d...	2409:10:c300:200:5...	UDP	88	443 → 64697 Len=26
2436	23.110337	2409:10:c300:200:5...	2404:6800:4004:81d...	UDP	94	64697 → 443 Len=32
2437	23.270345	2404:6800:4004:81d...	2409:10:c300:200:5...	UDP	1136	443 → 64697 Len=1074
2438	23.271016	2409:10:c300:200:5...	2404:6800:4004:81d...	UDP	100	64697 → 443 Len=38
2439	23.271414	2404:6800:4004:81d...	2409:10:c300:200:5...	UDP	198	443 → 64697 Len=136
2440	23.271519	2409:10:c300:200:5...	2404:6800:4004:81d...	UDP	96	64697 → 443 Len=34
2441	23.278952	2404:6800:4004:81d...	2409:10:c300:200:5...	UDP	88	443 → 64697 Len=26

Sequence Number: 4321 (relative sequence number)  
Sequence Number (raw): 3627207891  
[Next Sequence Number: 5761 (relative sequence number)]  
Acknowledgment Number: 186 (relative ack number)  
Acknowledgment number (raw): 4153621513  
0101 .... = Header Length: 20 bytes (5)  
Flags: 0x010 (ACK)  
Window: 2052  
[Calculated window size: 525312]  
[Window size scaling factor: 256]  
Checksum: 0x63c0 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
[Timestamps]  
[SEQ/ACK analysis]  
TCP payload (1440 bytes)  
[Reassembled PDU in frame: 2417]  
TCP segment data (1440 bytes)

```
0000 3c 09 50 10 08 04 63 c0 00 00 b5 c9 c2 c3 8d 17 <P...c...>  
0001 8e 34 27 dc c1 53 93 03 9e bf b7 c3 23 12 ed 12 4...5...>  
0002 96 4c 1f 79 53 75 03 9e cd dd 45 f7 6b 17 df 87 L...yS...E...k...>  
0003 00 31 3d 22 30 94 77 ab ea b4 4f e3 79 87 68 b6 -...0...w...o...y...h...>  
0004 88 59 70 76 f1 5c dc f4 bd b3 70 7f 2f db f9 c6 Y...p...-...p.../...>  
0005 b9 f0 f0 a9 7f f9 72 4c 54 f0 e3 a6 b9 74 cb 59 .....rL...t...Y...>  
0006 22 a0 82 04 f4 30 82 04 10 30 82 04 ec 30 82 02 .....0...-...0...>  
0007 d4 a0 03 02 01 02 02 13 33 00 26 bd bc 5e 18 df .....3...>  
0008 6f d4 c9 63 1b 00 00 00 26 bd bc 30 0d 06 09 2a .....&...0...>  
0009 86 48 86 f7 0d 01 01 0c 05 00 30 5d 31 0b 30 09 H...>  
000a 06 03 55 04 06 13 02 55 53 31 1e 30 1c 06 03 55 U...U...S1...>  
000b 04 0a 13 15 4d 69 63 72 6f 73 6f 66 74 20 43 6f M...r...o...s...o...f...C...>  
000c 72 70 6f 72 61 74 69 6f 6e 31 2e 30 2c 06 03 55 r...p...o...r...a...t...i...o...n...>  
000d 04 03 13 25 4d 69 63 72 6f 73 6f 66 74 20 41 7a M...>  
000e 75 72 65 20 52 53 41 20 54 4c 53 20 49 73 73 75 ure...R...S...A...T...L...S...I...s...s...>  
000f 69 6e 67 20 43 41 20 30 34 30 1e 17 0d 32 34 30 ing...C...A...>  
0010 33 30 35 31 38 33 37 33 31 5a 17 0d 32 34 30 34 3051837312...>  
0011 30 34 31 38 33 37 33 31 5a 30 1f 31 1d 30 1b 06 0418373120...>  
0012 03 55 04 03 13 14 41 7a 75 72 65 52 53 41 30 34 U...>  
0013 20 4f 43 53 50 20 43 65 72 74 30 82 01 22 30 0d O...C...S...P...>  
0014 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 01 .....H...>
```

パケット全体をHex streamとして出力を取り出すことが可能

1440バイトのTCP payload

## タグの出力例

24クラス、上位5クラスを表示

```
{'considered regular expected':  
0.9683609760620078, 'malicious intent':  
0.9615794211373029, 'typical':  
0.9613007669189144, 'standard network':  
0.9597006785861135, 'reference point':  
0.9590239229010236}
```