IDSによる
不正トラフィックの検出

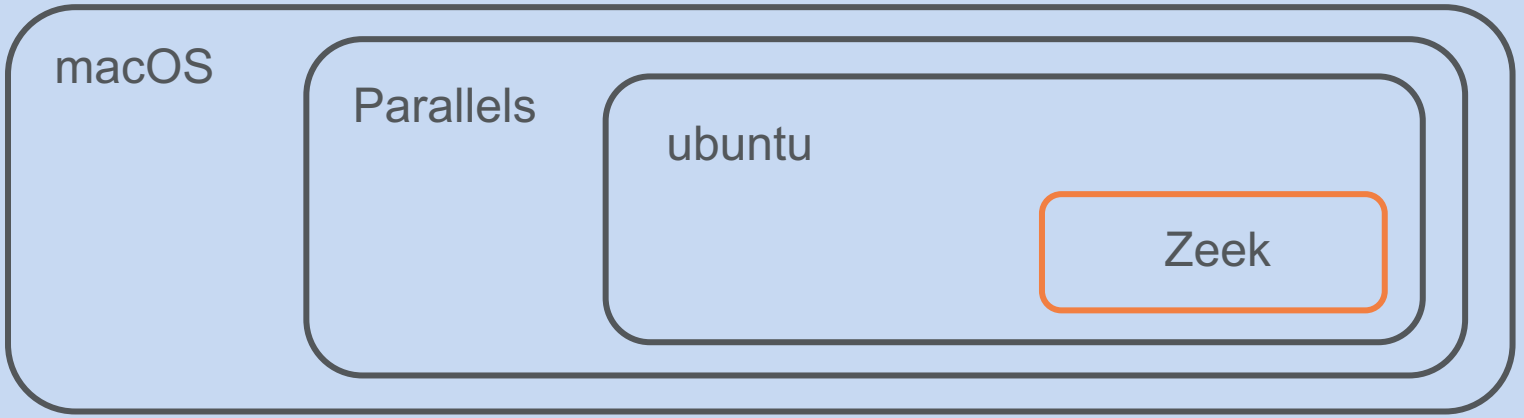
情報理工学部セキュリティ・ネットワークコース
3回生
菅原　颯真

目次

- 実行環境
- IDSとは
- Zeekとは
- 自分の目標
- 結果
- マルウェアトラフィックの分析
- まとめ

実行環境

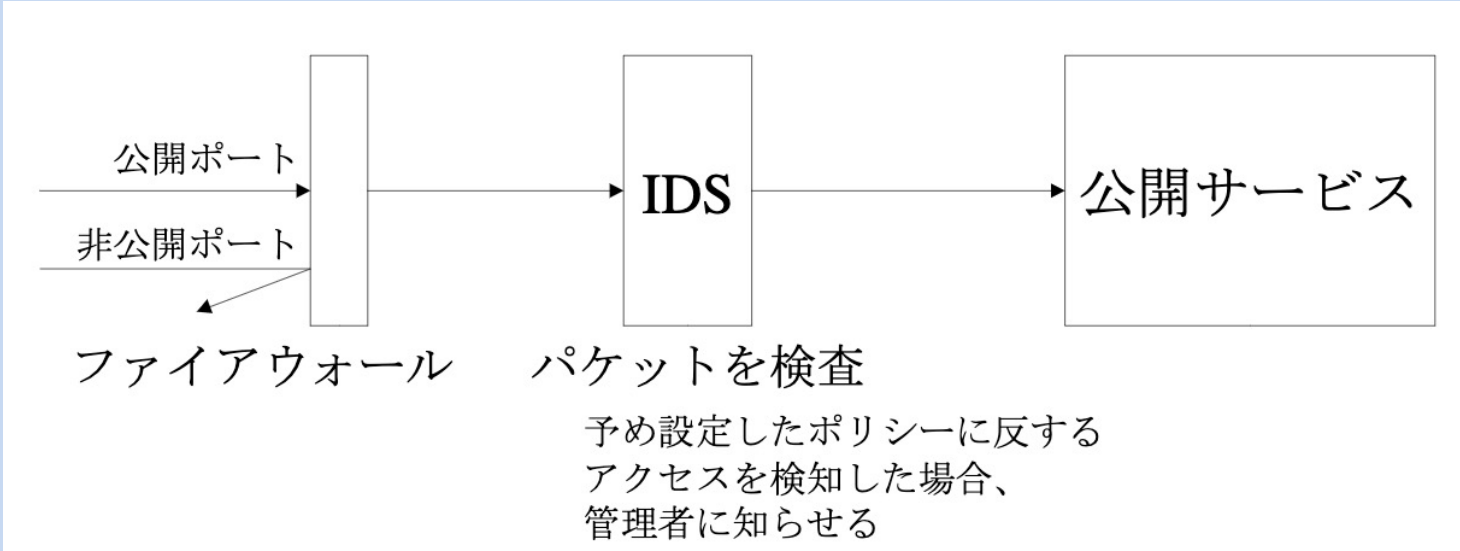
- ホストOS：macOS BigSur 11.4 (64bit)
- ゲストOS：ubuntu 18.04 (64bit)
- OS仮想化ソフトウェア： Parallels Desktop 16 for Mac
- ネットワーク分析フレームワーク：Zeek (v4.0.1)



実行環境の概要

IDSとは

- IDSは侵入検出システムのことで、ファイアウォールで防ぐことのできない不正プログラムの侵入や行為を発見する仕組み
- ホスト型とネットワーク型に分けられる



ネットワーク型IDSの例

IDSとは

- 通常作業との比較により異常を検出する「anomaly 型」と、予め用意した不正行為パターンへのマッチングを行う「signature 型」に分けることもできる
- anomoaly 型IDSは誤検知の可能性，signature 型IDSは未知の攻撃に弱いためIDSの検知は100%信用できない
- ホスト型IDSとして「Tripwire」，ネットワーク型IDSとして「Snort」・「Zeek」が有名

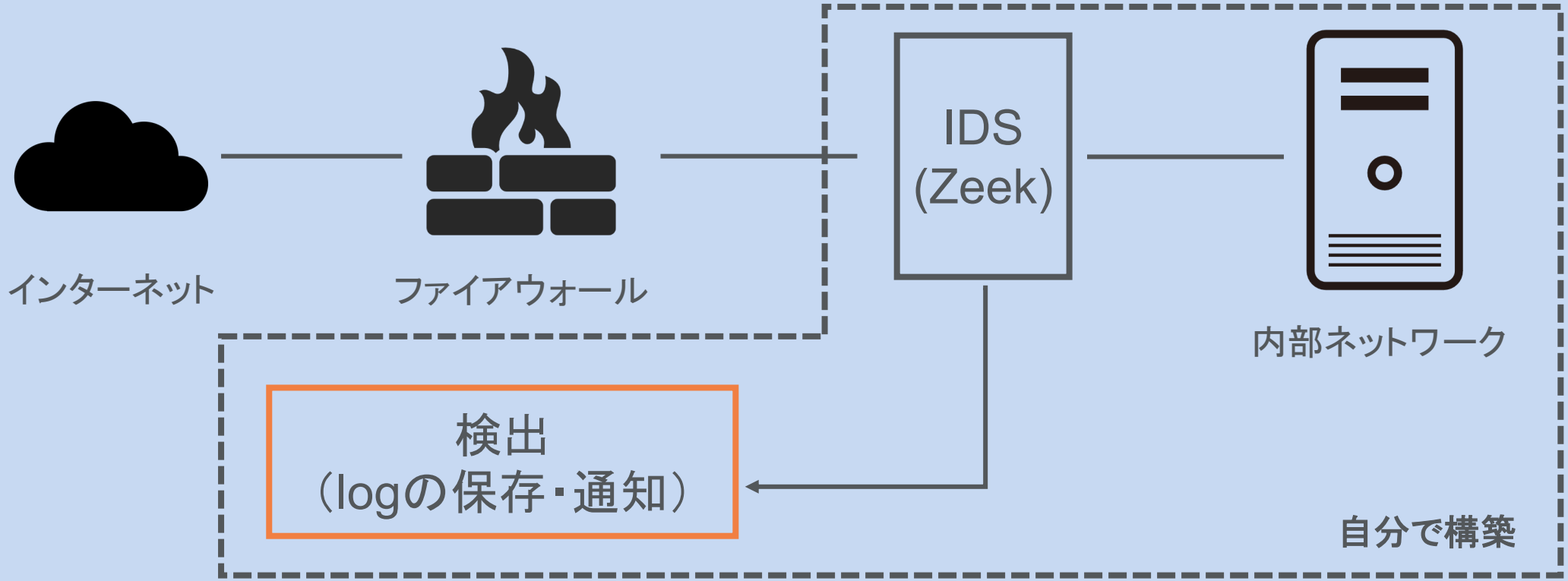
Zeekとは

- ネットワーク型・signature 型IDSのオープンソースソフトウェア
- ネットワークの監視を目的として使用しているユーザが多いが、元はネットワークトラフィックの分析を目的としたソフトウェア
- ネットワークの監視以外にも以下のことをlogとして保存・分析できる
  - URL
  - HTTPセッション
  - DNSの要求と応答
  - SSL証明書

  etc…

自分の目標

- デフォルト・自作シグネチャを用いて不正トラフィックを検出したい
- （内容によって管理者への通知を行いたい）



結果

だめでした

すいません、、

結果

【出来たこと】
- Zeekの構築（自分のPC上）
- トラフィックをlogとして保存
- logの解析
- シグネチャの書き方の理解

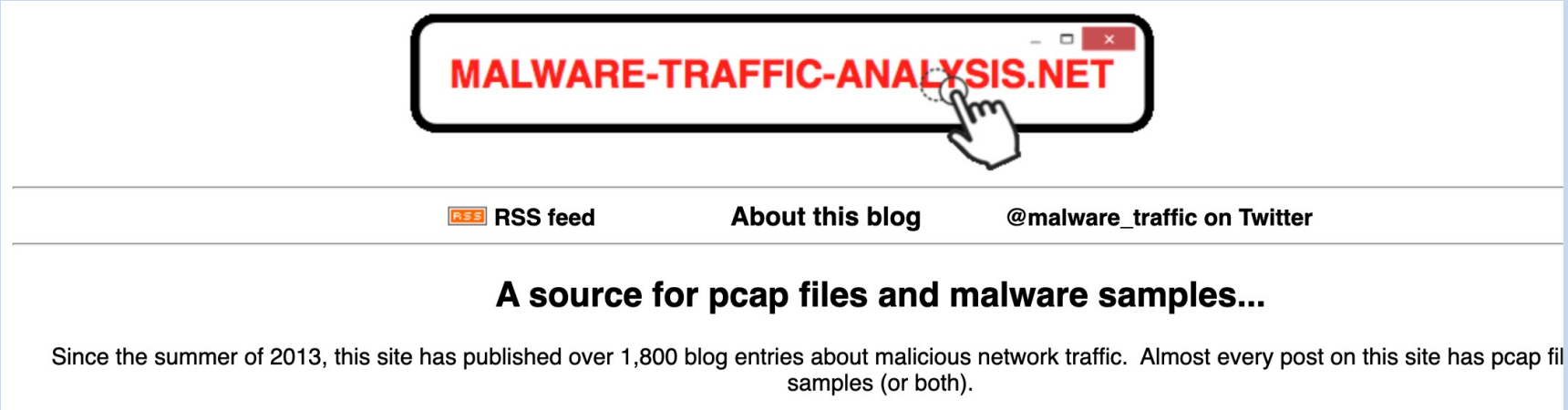
【出来なかったこと】
- シグネチャの設定
- 内部ネットワークの構築
- 不正トラフィックを流す
- 管理者への警告

テーマ変更

不正トラフィックがZeekを通ったと仮定してlogを分析する
（マルウェア感染の原因を究明する状況を擬似的に作る）

マルウェアトラフィックの分析

- 実際にマルウェアとの通信をキャプチャした有害な pcap ファイルを公開しているサイトを利用
- 今回は2020年の Lokibot の pcap ファイルを解析
  （Lokibot はトロイの木馬型のマルウェア）



https://www.malware-traffic-analysis.net/

マルウェアトラフィックの解析

1. Zeekをオフラインモードで実行
2. 指定の pcap ファイルをロード（今回は Likibot の pcap ファイル）
3. pcap ファイルから得たトラフィックのlogを解析
4. どのようにしてマルウェアに感染したのかを調べる

logの種類	概要	logの種類	概要
conn.log	TCP / UDP / ICMP接続	packet_filter.log	適用されたパケットフィルタの一覧
dns.log	DNSアクティビティ	pe.log	Portable Executable（後述）
files.log	ファイルの分析結果	ssl.log	SSL/TLSハンドシェイク情報
http.log	HTTPリクエストと応答	x509.log	X509証明書情報

logの種類

マルウェアトラフィックの解析

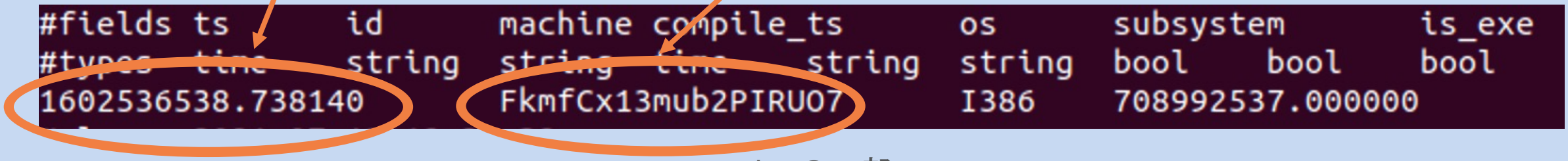
- Portable Executable（PE）とは、

→Windowsの32ビット（64ビット）の実行可能なファイル形式（EXE）のこと

- pe.log を見てみる

ID
（トラフィックごとにIDが割り当てられていてすべてのlog共通）

タイムスタンプ



pe.logの一部

マルウェアトラフィックの解析

- 先程のIDのトラフィックの log をすべて調査

```
parallels@parallels-Parallels-Virtual-Platform:/tmp/zeek$ grep FkmfCx13mub
2PIRUO7 *.log
files.log:1602536538.735918     FkmfCx13mub2PIRUO7      45.14.112.133   10
.10.12.101      C9TyHyfALN2KFpnw        HTTP    0       PE      applicatio
n/x-dosexec     -       1.240462        -       F       629760  629760  00
F       -       -       -       -       -       -
http.log:1602536538.593756      C9TyHyfALN2KFpnw        10.10.12.101    49
979     45.14.112.133   80      1       GET     millsmiltinon.com       /o
jHYhkfkmuofwuendkfptktnbujgmfkgtdeitobregvdgetyhsk/Xehmigm.exe  -       1.
1       Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident
/7.0; .NET4.0C; .NET4.0E)       -       0       629760  200     OK      --
(empty) -       -       -       -       -       -       FkmfCx13mub2PIRUO7
-       application/x-dosexec
pe.log:1602536538.738140        FkmfCx13mub2PIRUO7      I386    708992537.
000000  Windows 95 or NT 4.0    WINDOWS_GUI     T       F       F       FF
T       T       F       F       F       .text,.itext,.data,.bss,.idata,.tl
s,.rdata,.reloc,.rsrc
```

怪しい

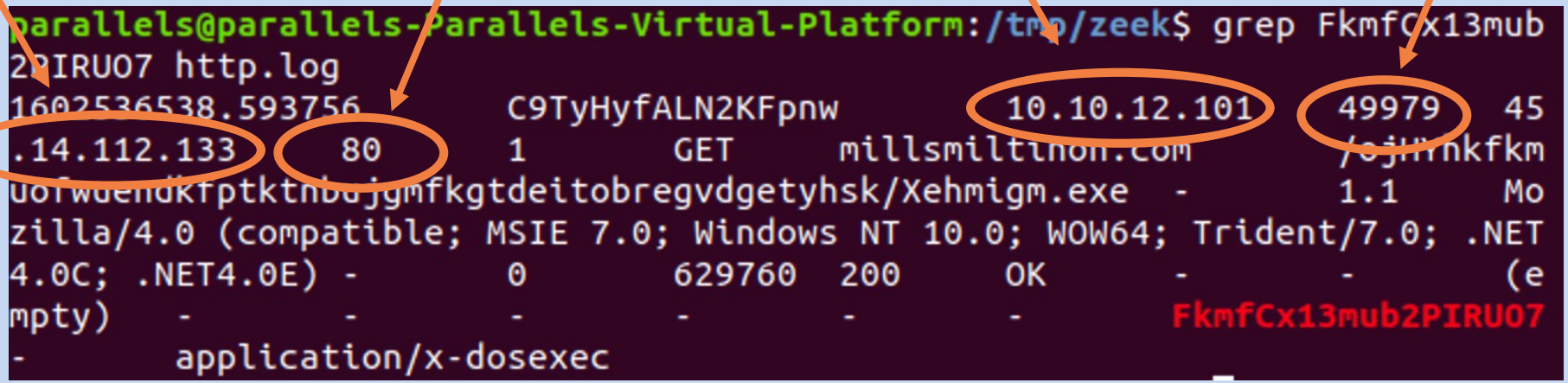
先程のIDをすべてのlog ファイルから検索

マルウェアトラフィックの解析

- http.log について詳しく見てみる

→マルウェアの感染経路の特定に成功

宛先IPアドレス　宛先ポート　送信元IPアドレス　送信元ポート



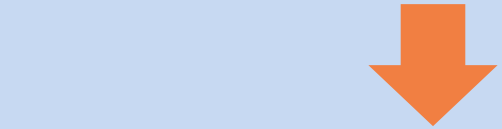
先程のIDのhttp.logに記録された情報のみ表示

マルウェアトラフィックの解析

- マルウェアの感染経路の特定に成功

→先程のIPアドレスからの通信をシャットアウトすることで対策可能

→（先程の情報をもとにシグネチャの設定をすることで対策可能）



擬似的に不正トラフィックを調査してマルウェアの感染経路の特定を行うことができた.

また，その他のlogの分析を行うことができた.

まとめ

- もともとやろうとしていたことはできなかったが，IDSに対しての理解が深まった
- どのようにトラフィックを log をして保存して分析するのかを理解したことでネットワークの知識が増えた
- 擬似的にトラフィックの解析，および不正トラフィックの調査を行うことができ，実際の感染調査の大変さを理解することができた（数十トラフィックの解析でもかなり大変だった）
- 今後はもともとの目標である，Zeekによるデフォルト・自作シグネチャを用いた不正トラフィックを検出・警告に挑戦したい