

マルウェア対策研究人材育成ワークショップ 2012

IPS への実装を想定した マルウェアの通信検知方法の一検討

2012年11月1日

株式会社MCセキュリティ

大西 祥生 常松 直樹

はじめに

- マルウェアによる被害は後を絶たない
- ウイルス対策 + a の対策が増えている
- 不正な通信を検出/防御する必要性
 - CCC Dataset 2012が発生させる不正な通信を防御する

目次

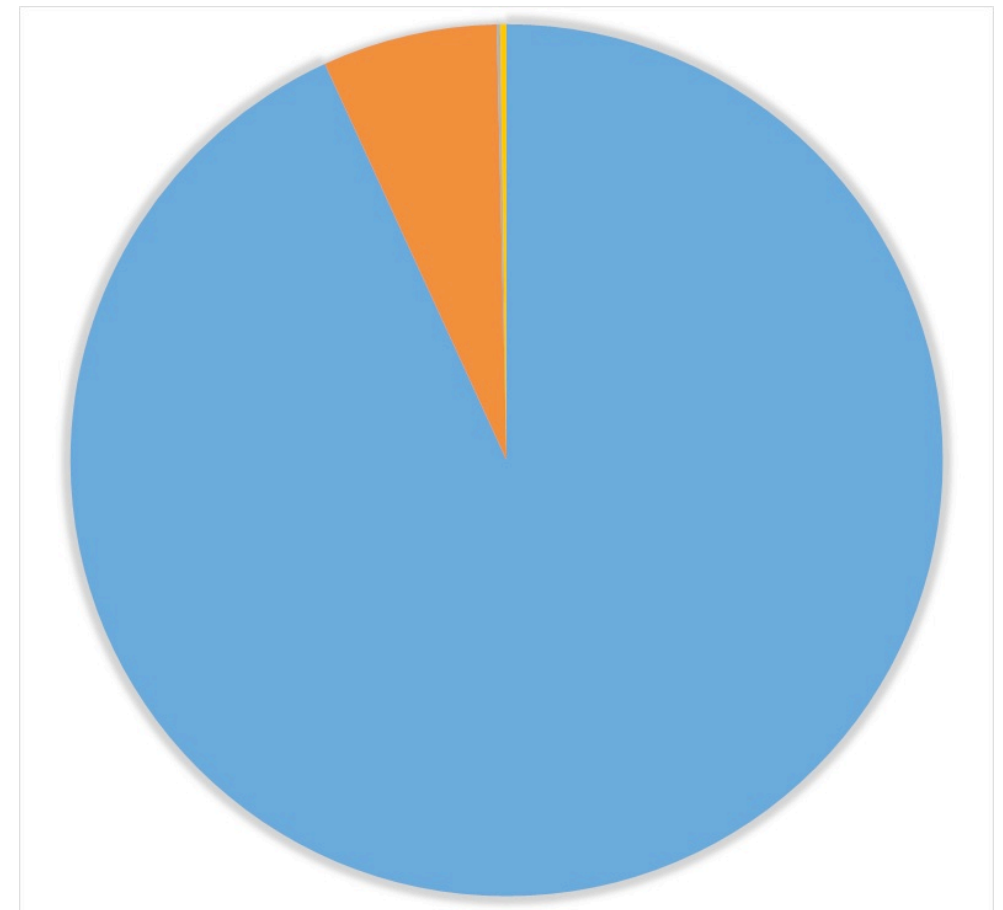
- 検体について (CCC DATASET 2012)
- 検体の動作
- IPSによる防御方法の検討
- まとめ

検体について

- CCC DATASet 2012 の分類

提供されたウイルス対策ソフトによる分類

種類	個数
■ Worm Allaple	9817
■ Worm Downad	683
■ PE Virut	13
■ その他	25
計	10538



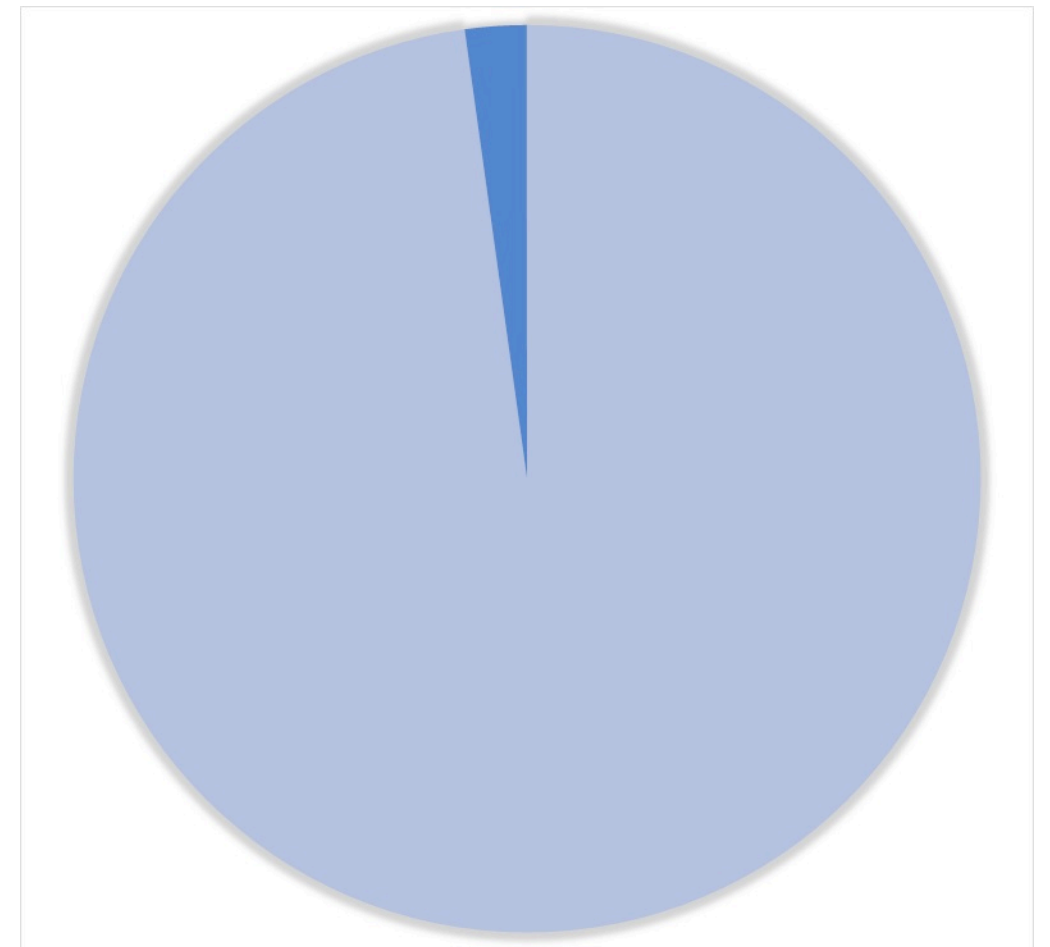
多く 検体が提供されたWorm Allapleについて検証を行う

検体について

- Worm Allaple 亜種の分類

ウイルス対策ソフトの分類を元に、亜種に分類した

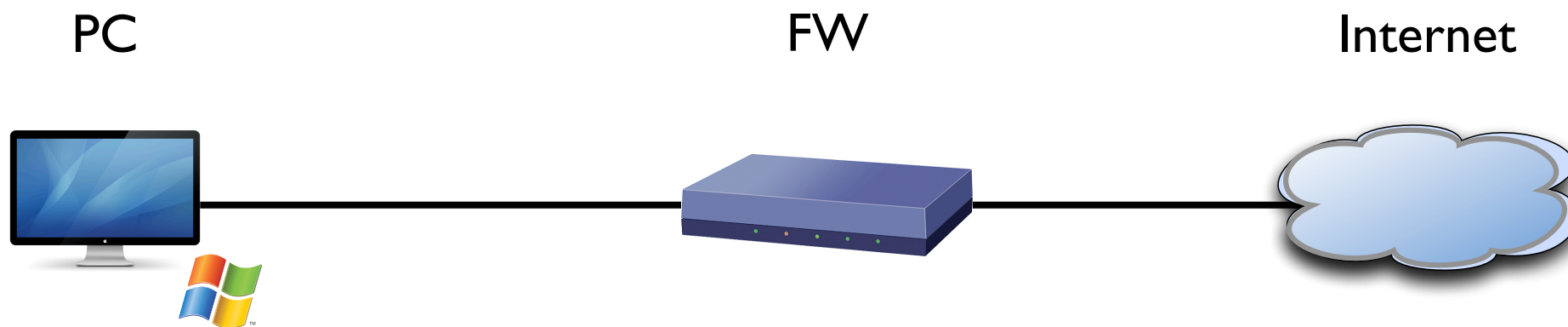
種類		数量
Worm Allaple		9817
	Allaple.IK	9601
	Allaple.PF	214
	他の亜種	2



動作環境の検討

- 検体を動作させる環境

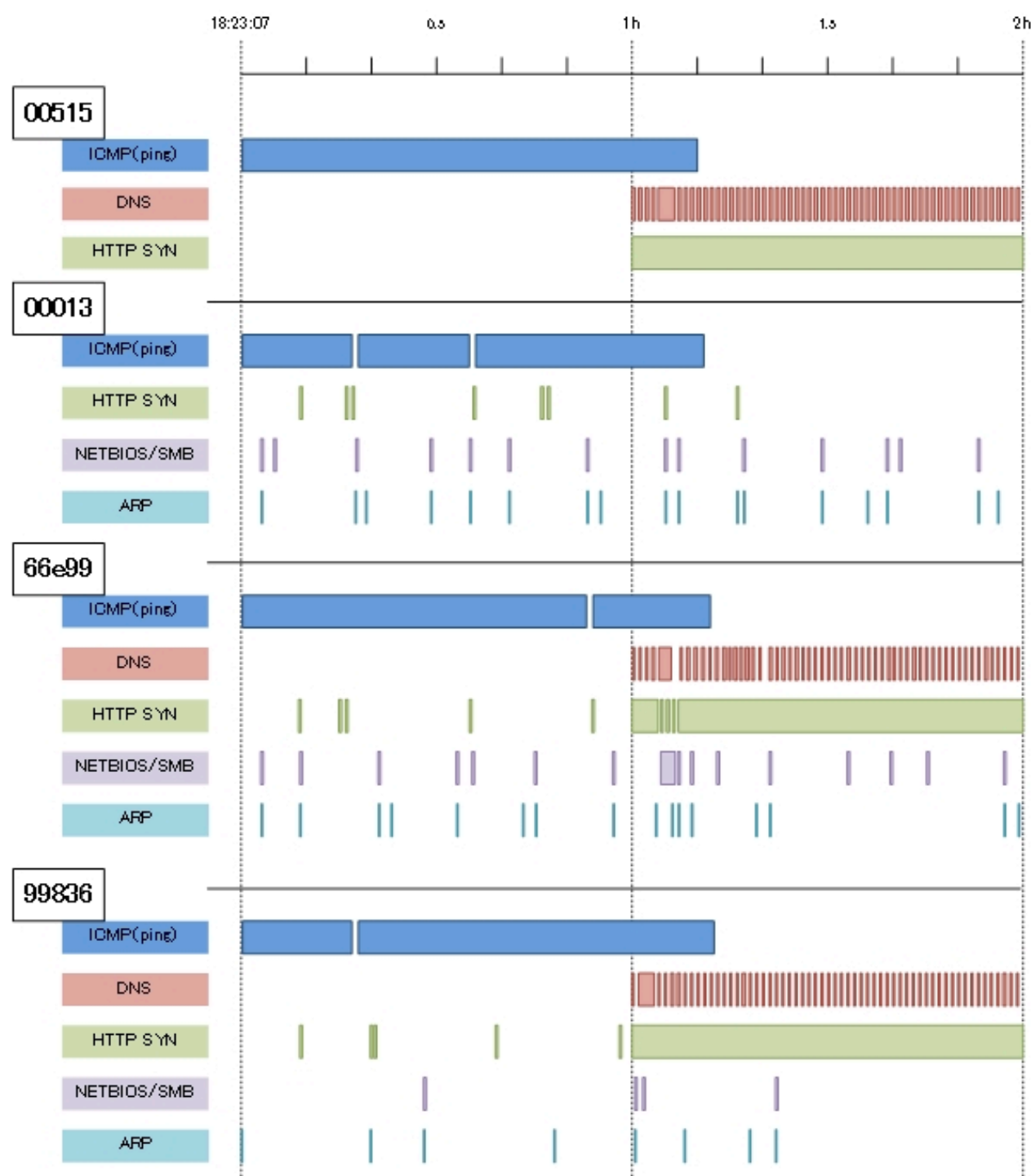
FWにて検体PCが外部に接続できない設定とする



PCを Allappleに感染させて挙動を確認

検体の動作 (Allapple)

- 2時間周期の動作シーケンス

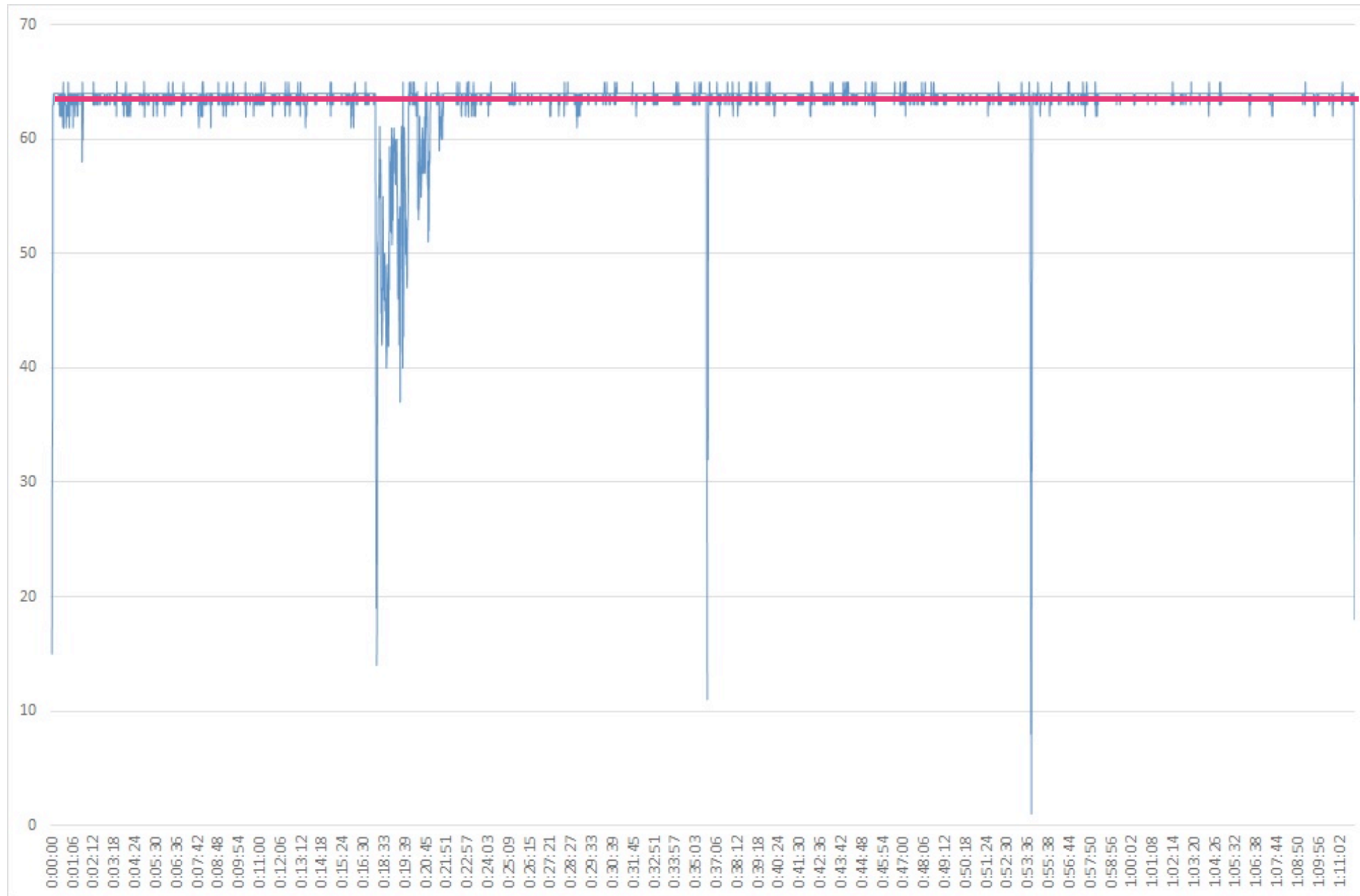


特徴

1. ping requestを送る
0:00 ~ 1:12
2. 名前解決 -> HTTP
1:00 ~ 1:59
3. SMB共有への接続
0:00 ~ 3:59

検体の動作 (Allapple)

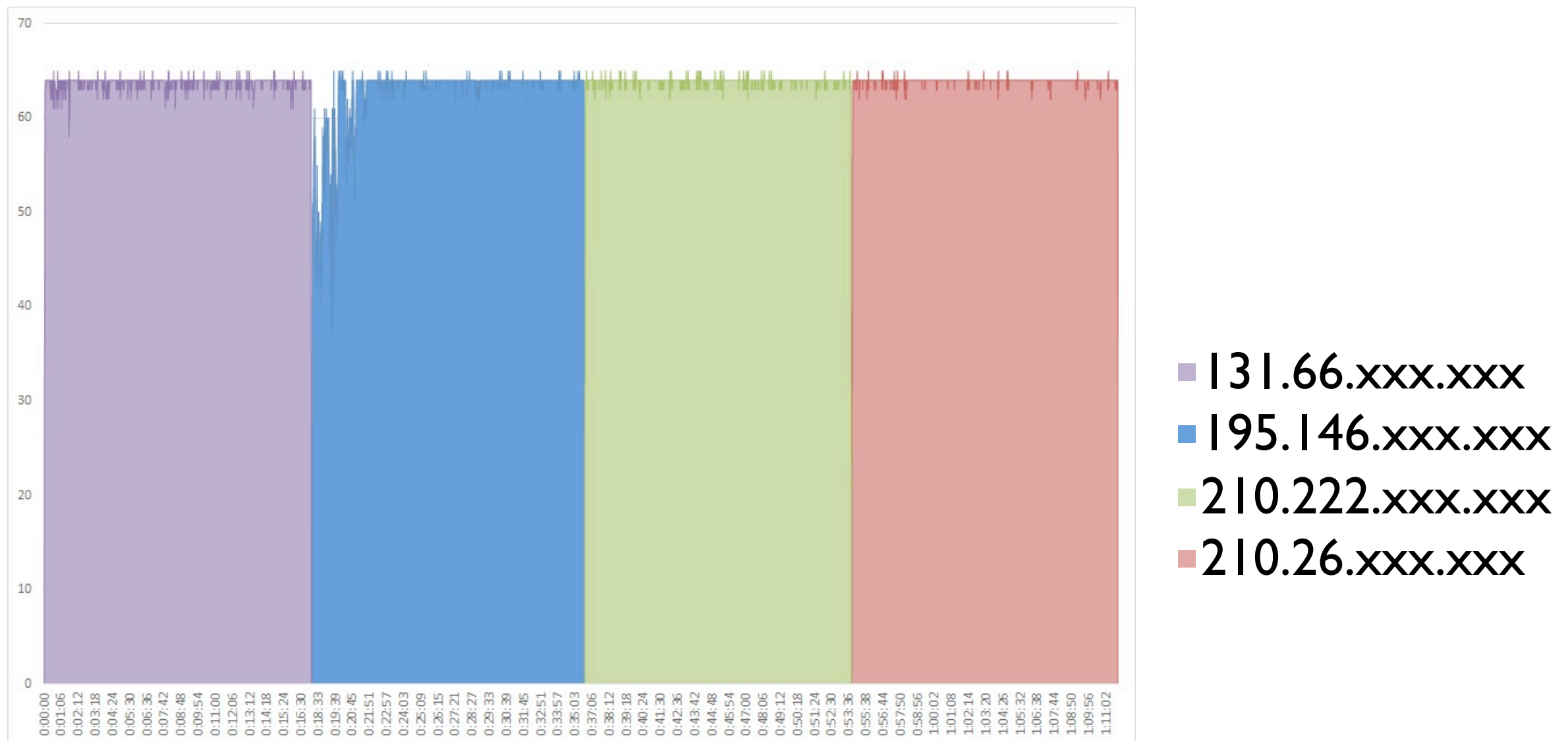
- ping requestの詳細



64回/sec

検体の動作 (Allapple)

- 第2オクテットにより分類した場合



- 18分おきに接続先が切り替わっている
- 切り替えのタイミングで回数が減少する場合がある

検体の動作 (Allapple)

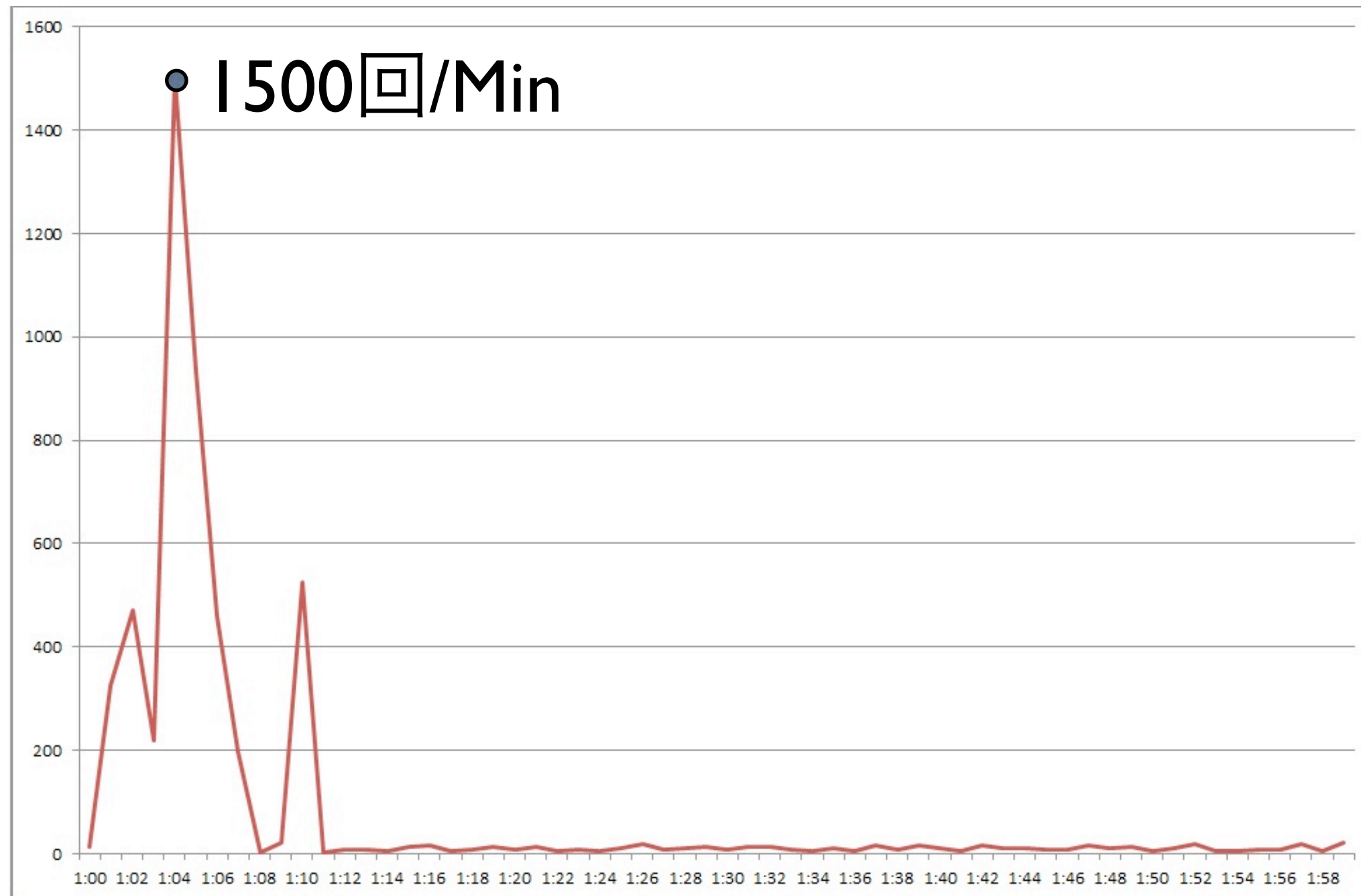
- ping通信先IPアドレスの国別の分類



通信先は特定の国に固定されていない
= 国別フィルタリングでは防御出来ない

検体の動作 (Allapple)

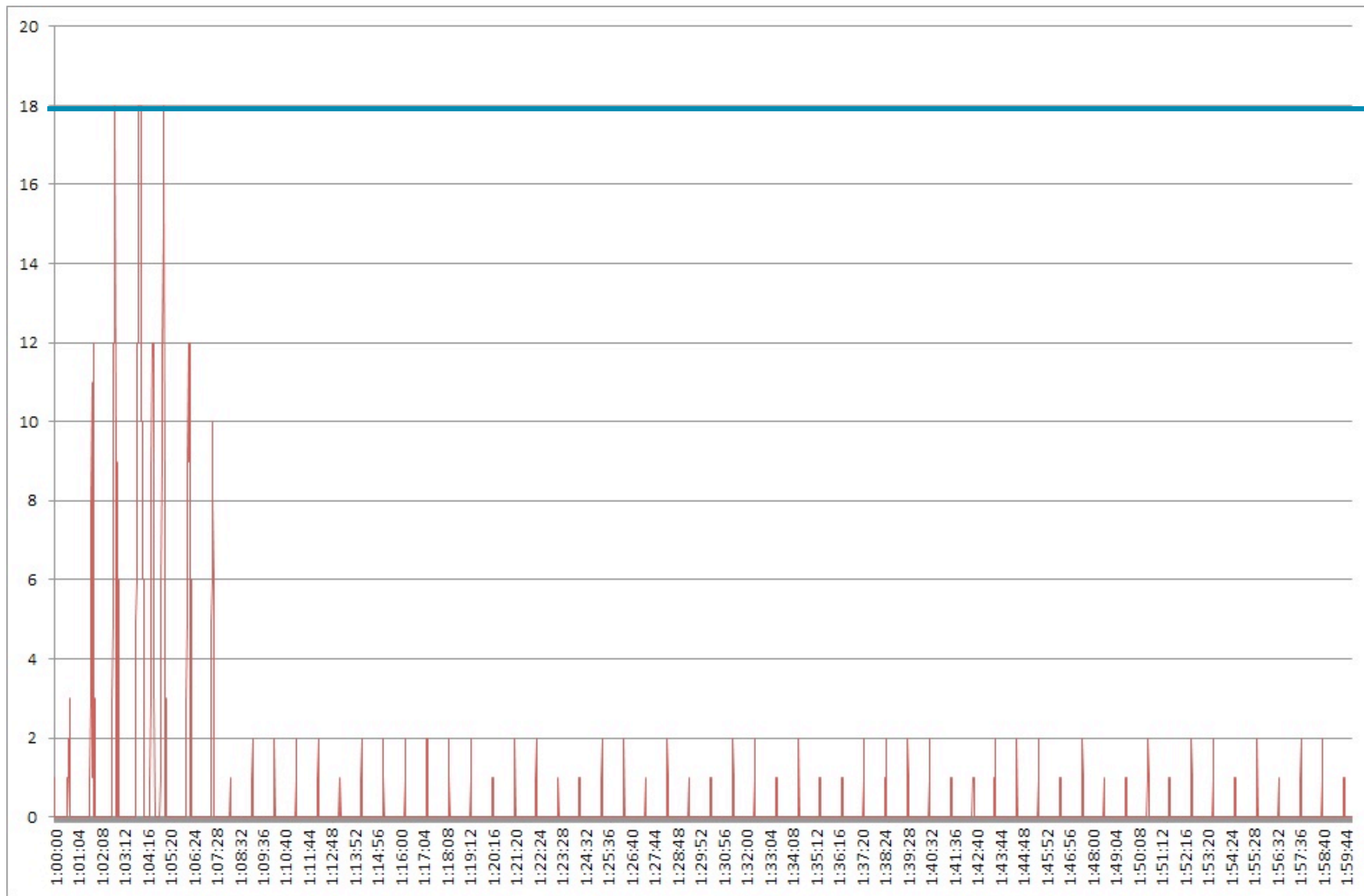
- DNSによる名前解決パケットの推移 (1分間隔)



固定のドメイン名問い合わせしている(エストニア)

検体の動作 (Allapple)

- DNSによる名前解決パケットの推移 (1秒間隔)



18回/Sec

検体の動作 (Allapple)

- Worm Allappleの動作まとめ
 - 2時間で1サイクル
 - 外部のIPアドレスに対してping requestを送る
 - 特定のURLに対してDNS名前解決を図る
 - 解決したIPアドレスへSYNを送る

ping & DNS に対してDoS攻撃的挙動が見られる

IPSによる防御手法の検討

- トラフィックシェーピングによる負荷低減
- 送信元ごとのトラフィック解析
- pingとDNSを防御する条件のしきい値の決定
 - 各OSが送信する間隔の調査

防御手法の検討

- 送信元ごとのトラフィック解析
 - 今回のケースは、送信元と宛先の関係が1 : N
 - 送信元ごとに、解析値の蓄積

防御手法の検討 (ping編)

- OSによるping送信間隔

Windows/Mac/Linux 1回/秒 ※1

- マルウェアによるping送信間隔

検体ハッシュ	最大送信間隔
7daac	53ms
00515	33ms
a6b66	55ms
00013	68ms
66e99	93ms
82c67	93ms
38787	70ms
99836	50ms
a5df5	90ms

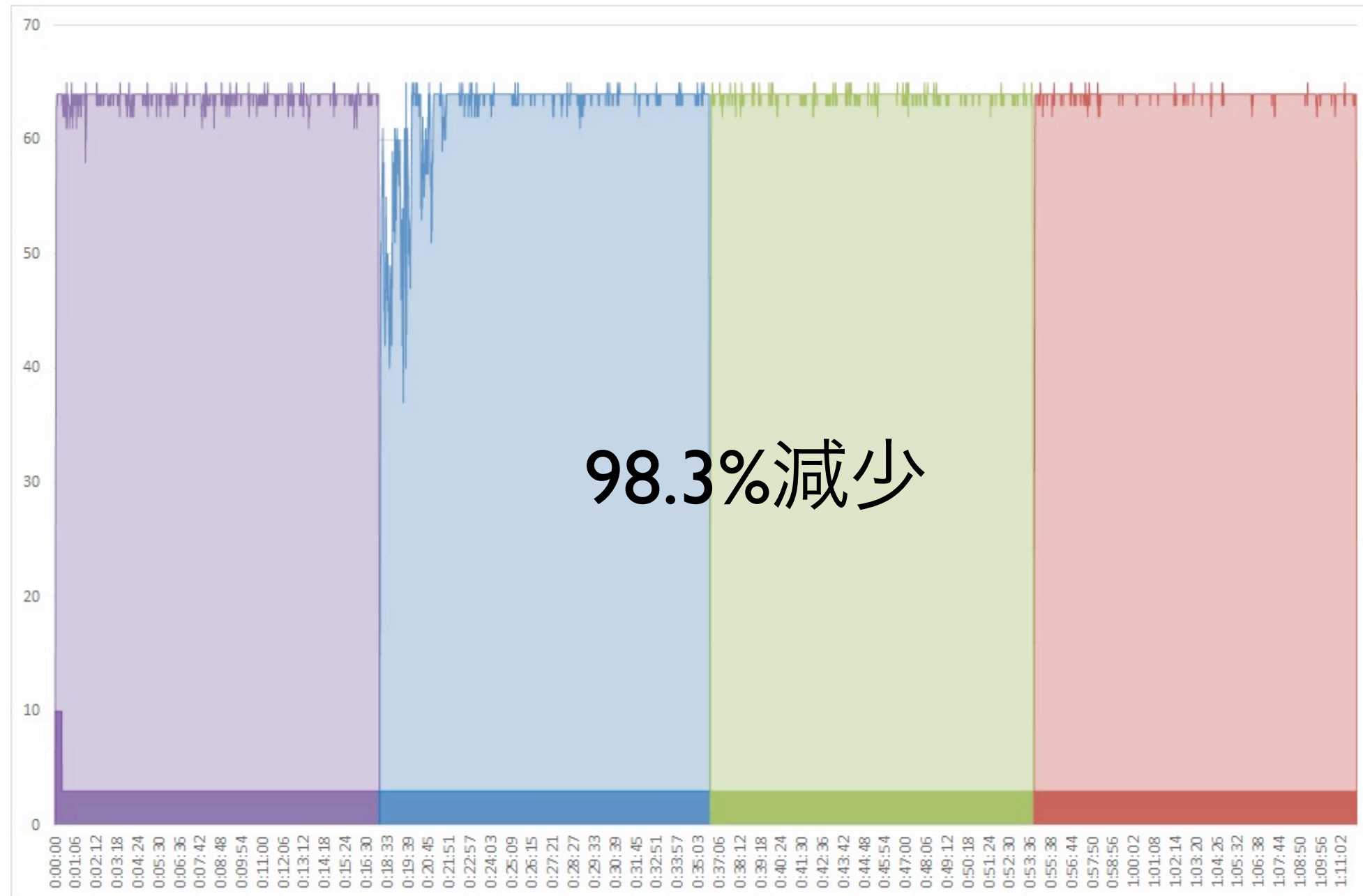
最大送信間隔 93ms = 10.75回/秒

10回/秒 以上のping送信を

ブロックする

防御結果 (ping編)

- 防御結果



防御手法の検討 (DNS編)

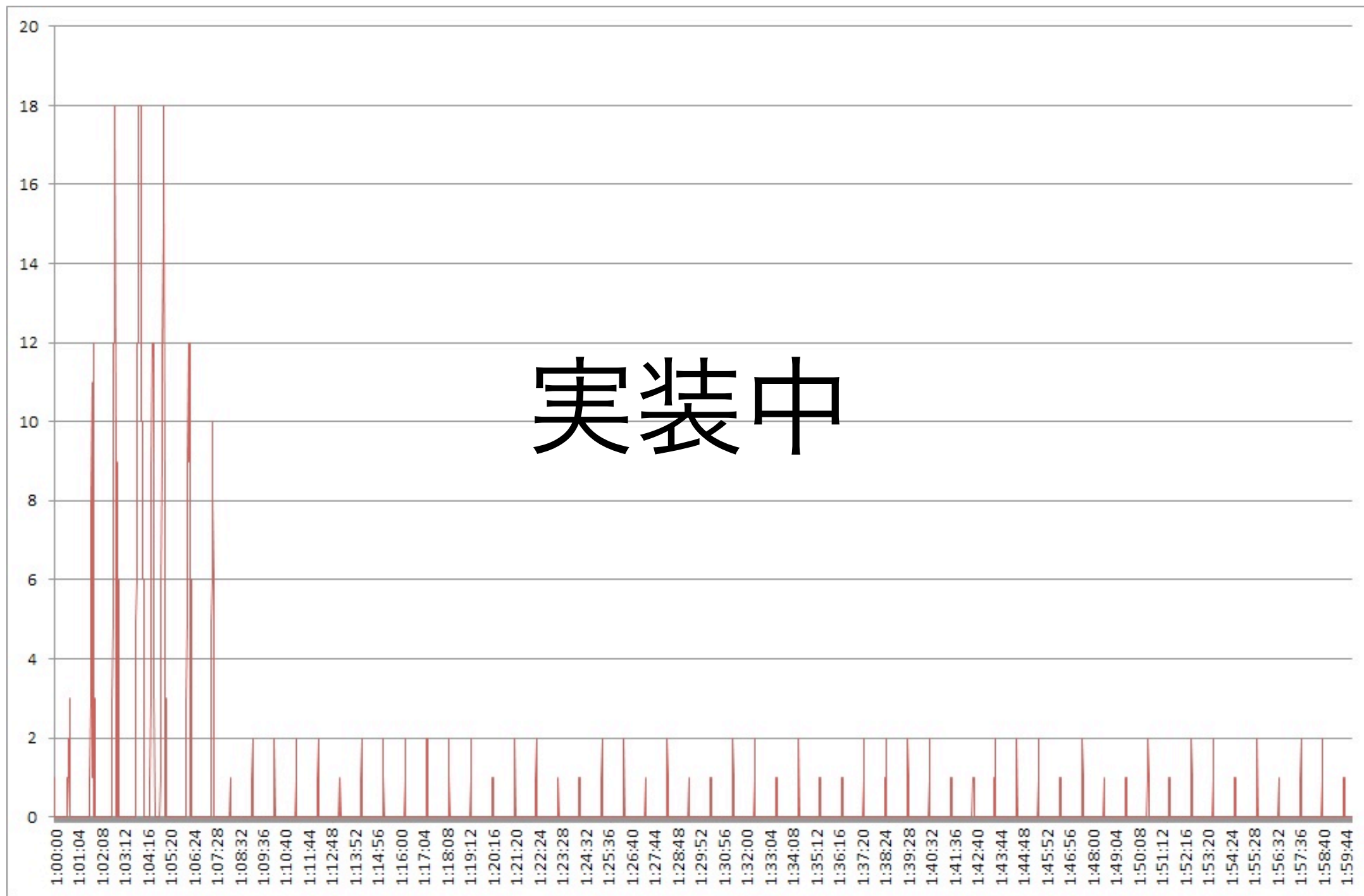
- OSによるDNS名前解決要求リクエスト
 - 応答が無い、または遅延している場合は、1秒後に再度リクエストを送信する(Windows)

秒	優先	代替
0	●	
1		●
2	●	
3		
4	●	●
5		
6		
7		
8	●	●

- 応答があった場合、TTL時間分だけキャッシュを利用する
今回の検体のTTLは、300秒 (5分)

検体の動作 (Allapple)

- DNSによる名前解決パケットの推移 (1秒間隔)



まとめ

- Allappleの動作

秒間に大量のping/DNSリクエストを発生させる

→ トラフィックシェーピング

- 課題

しきい値の調整 & 自動化

同様の動作をする検体調査