Computer Security Symposium 2017
23 - 25 October 2017

状態変化型リアクティブセンサーを用いた攻撃ロジック観測手法の提案

小堀 佳和子† 稲村 勝樹†

概要： 全ての攻撃に対して考えうる最大限のセキュリティ対策を実装することは，コストの問題があるため現実的ではない．そのためサイバーセキュリティ対策はリスク分析に基づいて効率よく実施されるのが望ましいとされる．攻撃者が攻撃を行う際，サイバーキルチェーンに代表されるようなロジックを元に行動していると言われている．そこで，攻撃者のロジックを知ることで攻撃への対策を事前に行い，リスク分析にも役立たせる手法を検討する．本研究ではロジックの一部を知るために，パッシブセンサーからリアクティブセンサーへ状態を変化させる観測手法を考察し，実際に観測を行った結果，攻撃者のロジックの一部を把握できた可能性があるので報告を行う．

キーワード：パケット解析，インターネットノイズ，ネットワーク監視

Proposal of the Observation Method for Cyber Attack Logics using Status Modification Type Reactive Sensors

Kanako Kobori† Masaki Inamura†

Abstract: Implementation of all conceivable security measures for all attacks is not realistic because of the cost problem. Therefore, cyber security measures should be implemented efficiently based on risk analysis. According to reports attackers probably use a logic, e.g. cyber kill chain on cyber-attack operations. Therefore, we consider the method, which takes measures against attacks and are utilized for risk analysis, by knowing the attacker's logics. In this research, in order to know a part of the logics, we considered an observation method to change the state from a passive sensor to a reactive sensor. And a result of actual observation, Possibility of perceiving a part of the attacker's logics are shown.

Keywords: Packets Analysis, Internet Noise, Network Observation

1. はじめに

近年，インターネット技術の普及に伴いパーソナルコンピュータや携帯端末など，自動車や各種センサー等がインターネットに接続されるようになった．このようにあらゆる装置がインターネットに接続される状況を IoT (Internet of Things)と呼ぶことがある．あらゆるものが接続されることにより便利なサービスが開発されるメリットがあるとされる．一方で，サイバーセキュリティの観点では対策をしなければならない箇所が増えることになり，実際に IoT をターゲットとした攻撃が確認されている [6]．今後は，インターネットに接続されるあらゆる装置に対してセキュリティ対策が必要である．

実際のセキュリティ対策では，全ての攻撃に対して考えうる最大限のセキュリティ対策をしたシステムを実装することは，コストの問題があるため現実的ではない．そのため，サイバーセキュリティ対策はリスク分析に基づいて効率よく実施することが望ましいとされる[19]．リスク分析は，過去のセキュリティインシデント等の分析結果を通じて得た知見に依存している．

一方，標的型と呼ばれるサイバー攻撃は攻撃目標に特化していると言われており，攻撃目標によって用いるマルウェア等が異なる可能性がある．

攻撃者が攻撃を行う際は，サイバーキルチェーン[1]に代表されるようなロジックを元に行動していると言われている．つまり，サイバー攻撃はある考え方に基づいて攻撃の方法を設計している可能性がある．攻撃者の攻撃に関するロジック(以下ロジック)を知ることで，あらかじめ攻撃への対策をとることが期待でき，さらにリスク分析にも役立つことが期待できる．

攻撃を観測する手法としてパッシブセンサーやリアクティブセンサーなどが知られている．どちらか一つのセンサーのみでは，特定のロジックしか知ることができず，ロジックの全体像を把握することは難しい．

そこで，本研究ではそのロジックの一部を知るために，観測期間の中でパッシブセンサーからリアクティブセンサーへ状態を変化させる観測手法を考察し，実際に観測を行った結果，攻撃者のロジックの一部を把握できた可能性があるので報告を行う．

本論文の構成は，第 2 章で関連研究について述べ，第 3 章で本研究のアプローチ方法と実装内容を述べる．次に第

†東京電機大学理工学部情報システムデザイン学系
Division of Information Systems and Design, School of Science and Engineering, Tokyo Denki University

4 章で実験結果について記述し，第 5 章で分析結果の考察を行う．そして，第 6 章で本論文のまとめを行う．

2. 関連研究

2.1 既存研究

インターネット上の攻撃を観測する手法として，以下の 3 つに分類できる．

2.1.1 パッシブセンサーでの観測

パッシブセンサーでの観測には，情報通信研究機（NICT）が研究している NICTER (Network Incident analysis Center for Tactical Emergency Response) でのダークネット観測を始め，様々な研究が行われている[9]．ダークネット観測は，定点観測とも呼ばれており長期的な運用を行うことでインターネット上の攻撃活動の傾向を把握することが可能であるとされている．NICTER プロジェクト[2][8]では，インターネット上で発生するイベントを定常的に収集することで，インシデントの自動検出を可能としている．

2.1.2 リアクティブセンサーでの観測

リアクティブセンサーとは，発信元に対して応答を返す手法のことである．芦野らの研究では，リアクティブセンサーを用いて意図が不明なインターネットノイズの通信を観測することで，相手の能力を推定できる場合があると示している[3].

また，サービスを偽装するハニーポットもリアクティブセンサーの一つである[4]．マルウェア感染や攻撃が行われる前にあらかじめハニーポットを設置しておくことで，攻撃やマルウェアの振る舞いを分析することができる．

2.1.3 アクティブセンサーでの観測

アクティブセンサーの観測で代表的なものとして，クライアント型ハニーポットが挙げられる[13]．クライアント型ハニーポットは，対象のウェブサイトに対してアクセスを行い攻撃が発生するか確かめることで，そのサイトが悪性なものであるか検知・分析する技術のことである[11].

また、Antonio Nappa らが行なっているサイバープローブと呼ばれる能動的観測では，マルウェアや悪性サーバーの探索可能性を示している[12][14].

2.2 課題

攻撃者が攻撃を行う際は，図 1 のようなロジックを元に行動していると推定される．しかし，既存の研究方法では，センサーの状態を途中で変更することができない．これはセンサーの状態が固定されているため，攻撃者の状態が変化した場合追跡できないことを意味する．その結果，変更した後の情報が欠けているため全体像を把握することができないという課題が生じる．

本研究は，攻撃者のロジックを知ることが目的であるため，センサーの状態が変更できないと観測対象の全体像を把握することが困難である．

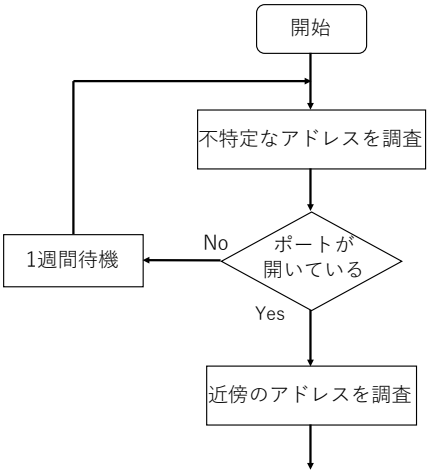

図 1 攻撃時に攻撃者が使用するとされるロジックの例

2.3 研究領域

インターネット上の通信観測から，攻撃者のロジックを捕捉するためには，状態変化型のセンサーを用いてパケットを観測しその挙動を分析する必要がある．

しかし，着信したパケットを定常的に観測するダークネット観測では，パケットに対して応答を返すことができないため，通信相手のロジックを知ることはできない．また，ハニーポットはパケットに対して応答を返すことはできるが，特定のセンサーを模した振る舞いしかできない．加えて観測で用いるセンサーによって応答内容が決まってしまうため，センサーの応答内容を変更することができない．芦野らの論文では発信元からの通信に着目することで，リスク分析の制度が向上すると述べている[15]．しかし，具体的な挙動を捉えることは難しいとされている．

そこで本研究では，この課題を解決するためにパッシブとリアクティブの 2 種類のセンサーを用いて応答内容を変化させ，インターネット上の通信を観測する．そして，その前後で攻撃者の応答内容に変化が生じるか観測を行う．また，3 章で攻撃者のロジックを捕捉するための実装を行なったのでその手法を述べる．

3. 分析アプローチ

3.1 通信の観測

本研究におけるインターネット通信の観測方法を以下に述べる（図 2）.

(1)未使用のグローバル IP アドレスを用いてインターネットの通信観測を行う.

(2)一定期間経過後，一部 IP アドレス(以下アドレス CD とする)の 80 番ポートを解放する.

(通信に対して SYN + ACK の応答を返す設定にする.)

(3)通信の観測を行う.

(4)未解放のIPアドレス(以下アドレスABとする)とポートを解放したIPアドレス(アドレスCD)で発信源に変化が生じるか分析を行う.

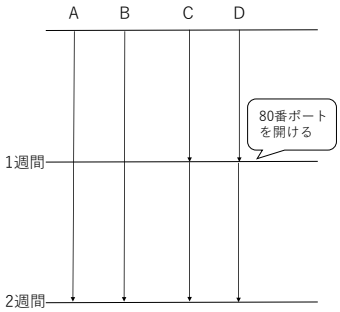

図2 本研究での通信観測手法

本研究において80番ポートを開放する理由は以下の2つである.

(1) パケット観測を実験開始前に行ったところ80番ポートに対してのアクセスが多くみられた.

(2) 未検知のマルウェアは80番ポートを使用して感染する割合が高いと言われている[16] .

松木らの研究ではマルウェアの感染は80番ポートを使用して行われる割合が高いとされており,マルウェアの挙動を知ることで,攻撃ロジックの全体像を把握することが期待される.

3.2 センサーの実装

本節では2.2節で述べた課題を解決すべく,センサーの実装を行なった(図3).詳細なアプローチ内容は以下の通りである.

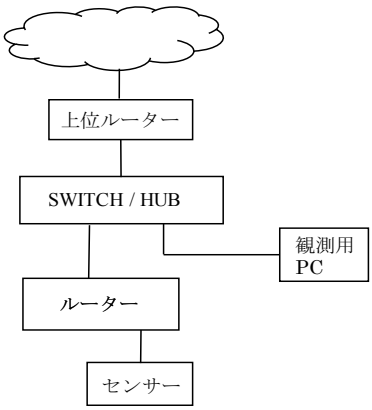

図3 センサーの実装内容

(1) CentOSをインストールしたパソコンとUbuntuをインストールしたパソコンを用意する.

(2) Ubuntuパソコンを観測用PCとし,CentOSがインストールされたパソコンは応答を返すセンサー(詳細を表1に示す)として利用する.

(3) 観測用PCが通信を行わないよう設定する.

(4) 観測用PCでtcpdumpを実行し通信の観測を行う.

(6) 観測用マシンに着信したパケットをpcapファイルに出力する.

(7) ルーターのファイアウォール設定を用いて,特定のアドレスのみ80番ポートを通過するよう設定する.

(8) 一定期間を経過したところで,センサーをパッシブからリアクティブに変更し,特定のアドレスへSYNパケットが着信した場合はセンサー側でSYN+ACKを返すよう設定する(課題(1)への対応).

表1 センサーの詳細

OS	CentOS 7
メモリ	3.6 GB
プロセッサ	Intel Core i5

4. 実験

4.1 センサーを用いて観測した通信観測パケットのデータセット

本論文で使用するデータセットは,観測用PCで観測したパケットをpcapファイルにまとめたものである.このデータセットの詳細を表2に示す.なお8月9日から8月12日の4日間はセンサーが停止していたため,観測データに含めないものとする.

表2 観測データ

観測期間	2017年7月25日から2017年8月21日
容量	約1.01GB
パケット数	約9467000

4.2 分析結果

7月25日から観測を始め,8月3日の13:15頃にセンサーをパッシブからリアクティブに変更した.そして,アドレスCDにSYNパケットが着信した場合は,SYN + ACKを返すような設定に変更した.

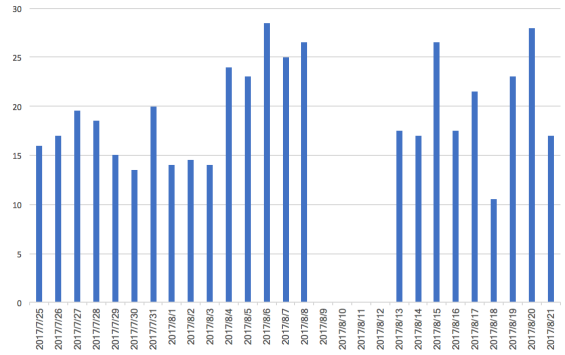

図4 アドレスCDにアクセスしたアドレス数の平均

図 4，はアドレス CD に着信した平均アクセスアドレス数のグラフである．8 月 4 日から 8 日までの 5 日間はパッシブだったときのアドレス数よりも多くなっているが，8 月 13 日以降は数にばらつきがあることが判明した．

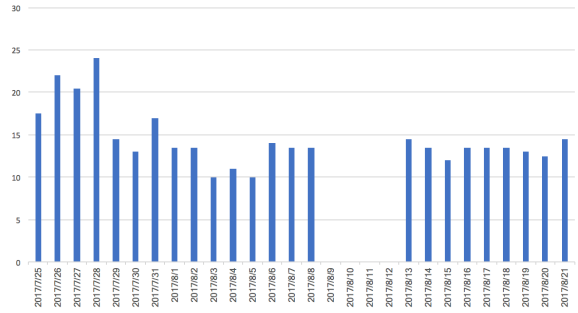

図 5 アドレス AB にアクセスしたアドレス数の平均

図 5 は，アドレス AB に着信した平均アクセスアドレス数のグラフである．7 月 29 日以降アドレス数に大きな変化がないことが判明した．

これらのことから，観測するセンサーを変更してもアクセスアドレス数に大きな変動がないことが判明した．

観測したデータを時間ごとでグラフ化したところ（図 7, 図 8），本研究で使用しているグローバル IP アドレスに対して 3 分間で集中的に SYN パケットを送信するというアドレスを 3 つ発見した（以下，この 3 つのアドレスをアドレス ABC とする）．この通信はセンサーをリアクティブに変更してから観測されたもので，パッシブセンサーの時には，このアドレス ABC からのパケットは観測されなかった．

[redacted]	1030	4998	6912
[redacted]	10001	19999	6924
[redacted]	10002	19998	6932
[redacted]	80	80	7003
[redacted]	10001	19997	7018
[redacted]	40331	59391	7097

図 6 ソースアドレスごとのポート最小値・最大値とアクセス数

ソースポートには，発信元の環境や実装が反映される場合があるため[20]，ソースポートに着目することで，通信相手の情報を発見できることが期待される．その結果，アドレス ABC がソースポートの最小値と最大値において類似していることも判明した(図 6). 図 6 の黄色い箇所がアドレス ABC である．

5. 考察

本章では 4.2 節で記述した分析結果をもとに考察を述べる．

5.1 攻撃ロジックの推定

本研究では，センサーの状態をパッシブからリアクティブに変更したことで，攻撃元のロジックを一部推定することができた．

センサーの挙動が同じ状態では，相手の挙動にも変化が起きず同じ応答しか返ってこないため，攻撃者側の新しいロジックを知ることができない．そこで，観測側の挙動を変更することで攻撃者側も新たなロジックで応答してくるのではないかと考え，観測途中でセンサーの状態をパッシブからリアクティブに変更した．

その結果，3 分という短い期間で集中的にパケットを送信するアドレス ABC を発見することができた．このアドレス ABC に着目すると，ソースポートの最小値と最大値が類似していることから，同じシステムを使用して通信を行なっているのではないかと推測される．このことを踏まえ考察を行うと，この通信は何らかの方法で同じシステムをインストールした人が動かしている，または同一人物がアクセスしている可能性が高いと推定される．あるいは，組織的に攻撃しているグループからの通信という可能性も考えられる．

5.2 情報伝達の仕組みの推定

4.2 節で述べたように 80 番ポートの開放後に大量のパケットが着信している．このようなことが起こっている場合，それ以前にも多数のセンサーから複数のグローバル IP アドレスに対して調査が行われていると推定される[17][18]. そして，そのうち 1 つのセンサーが SYN + ACK を受けとったことで攻撃者が 80 番ポートの解放を検知し，アドレス CD の近くにあるアドレスに対して一斉にパケットを送信したという可能性が高い．

また，ポート解放の情報が，調査を行なった攻撃者から伝搬したことでアクセスが来た可能性も考えられる．

5.3 その他の注目すべき通信

実験結果には掲載しなかったが，観測データの中に UDP/53 番ポートの DNS サーバーに対して GET リクエストを送信しているパケットが複数あることを発見した．DNS サーバーへの攻撃には，DNS サーバーの脆弱性をつく DNS エクスプロイト，キャッシュサーバーに偽の情報を送信する DNS キャッシュポイズニングなどの攻撃がある．今回観測された観測データには，サーバーに対しての大量のパケットは着信していなかったので DNS キャッシュポイズニング攻撃の可能性は低い．しかし，サーバーの脆弱性を狙った攻撃という可能性も考えられる．

本研究では SYN パケットに対して SYN + ACK を返す機能しかなかったため，通信相手が求める応答を返すことができず，ロジックの全体像を把握することができなかった．これらのことから，攻撃者が持っているロジックに合った応答を返すことで，攻撃ロジックの新たな一面を知ること

ができるのではないかと推定される．

5.4 本研究の課題

本研究では，80 番ポートしか開けておらず，センサーも SYN + ACK の応答を返すのみの簡単な実装であった．ただ SYN + ACK を返すのではなく，応答する内容を複数設定し，相手の通信内容に合わせて応答内容を変えることで，攻撃者のロジックについて詳しく知ることができるのではないかと考える．また，今回の研究は観測期間が約 4 週間と短かったことや応答内容が SYN + ACK のみだったため，当初予定していたような攻撃ロジックの全体像を把握することができなかった．攻撃者にサーバーと思わせるシステムが動作していなかったことも原因ではないかと考えられる．

5.5 今後の課題

今後の研究では，80 番以外のポート開放や SYN + ACK の応答に偽のサーバー情報を加えるなど，様々な応答を返していくことを検討する．また，より詳細なロジックを知るためにも，長期的なネットワークの通信観測を行なっていくことを検討する．

6. まとめ

本研究では，通信の観測から攻撃者のロジックを見つけるべく調査を行なった．観測状態をパッシブセンサーから SYN パケットに SYN + ACK 応答を返すリアクティブセンサーに変更し，通信の観測を行った結果，ロジックの一部を把握することができた．

今後は攻撃者の状態が変化した場合にも対応できるようなセンサーを構築し，可能な限り多くのロジックを見つけることができるよう，提案手法を改良する予定である．

参考文献

[1] “Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform”, http://lockheedmartin.com/content/dam/lockheed/data/corporate/documents/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.PDF, (参照 2017-08-09).

[2] “NICT NEWS”. http://www.nict.go.jp/publication/NICT-News/0607/research/, (参照 2017-08-09).

[3] 芦野佑樹, 島成佳:インターネットノイズに対する偽装応答機能の実装と観測に基づいた意図が不明なリクエストに関する考察, SCIS2015, 2015.

[4] “ハニーポット|マルウェア情報局”. https://eset-info.canon-its.jp/malware_info/term/detail/00085.html, (参照 2017-08-009).

[5] 沖野浩二, 片山昌樹, 占部優希:80/TCP ポートへの攻撃の時間的変化, CSS2015, 2015.

[6] 中山颯, 鉄穎, 楊笛, 田宮和樹, 吉岡克成, 松本勉:IoT 機器への Telnet を用いたサイバー攻撃の分析, CSS2016 ,2016.

[7] “TUBAME(インターネット定点観測システム)”, http://www.jpcert.or.jp/tsubame/, (最終閲覧日:2017/08/16).

[8] D. Inoue, M. Eto, K. Yoshioka, S. Baba, K. Suzuki, J. Nakazato, K. Ohtaka, K. Nakao, “nicter : An incident analysis system toward binding network monitoring with malware analysis,” WOMBAT Workshop on Information Security Threats Data Collection and Sharing(WISTDCS2008), pp.58-66, 2008.

[9] “警察庁セキュリティーポータルサイト@police-インターネット定点観測” , https://www.npa.go.jp/cyberpolice/detect/observation.html, (参照 2017-08-23).

[10] “セキュリティインシデントの積極的な検知:ハニーポットの利活用” , https://www.ipa.go.jp/files/000025088.pdf, (参照 2017-08-23).

[11] 吉岡克成 , インミンパパ , 鈴木将吾 , 渡邉直紀, 中山颯, 志村俊也, 徐浩源 ,四方順司 ,松本勉 , 中尾康二, 針生剛男, 岩村誠, 八木毅, 秋山満昭, 寺田真敏, 島成佳, 渡部正文, 角丸貴洋, 川北将, 山田正弘, 井上大介:能動的観測と受動的観測の融合によるサイバーセキュリティ情報の収集と分析, CSS2015, 2015.

[12] A Nappa, Z Xu, MZ Rafique, J Caballero, G Gu, "Cyberprobe: Towards internet-scale active detection of malicious servers," NDSS2014, 2014.

[13] M. Akiyama, et al. “Searching structural neighborhood of malicious URLs to improve blacklisting,” Proc. IEEE/IPSJ SAINT 2011.

[14] “CyberProbe_final.pdf”, http://security.di.unimi.it/sicurezza1314/slides/CyberProbe_final.pdf , (参照 2017-08-24).

[15] 芦野佑樹, 山根匡人, 矢野由紀子, 島成佳:長期間に渡るインターネットノイズの観測に基づいたサイバー攻撃の初期活動と推定される通信の発信源を分類する手法の提案, IPSJ-SPT, vol. 2017-SPT-24, No.6, pp.1-8, 2017.

[16] 松木隆宏:時系列分析による連鎖感染の可視化と_検体種別の推測, MWS2008, pp.37-42, 2008.

[17] “不正侵入の手口と対策（1）:攻撃者側から見た侵入前の事前調査（下見）(1/2) -@IT” , http;//www.atmarkit.co.jp/ait/spv/0210/11/news001.html, (参照 2017-08-26).

[18] “攻撃者側からみた侵入前の事前調査（下見）(2/2) -@IT”, http://www.atmarkit.co.jp/ait/articles/0210/11/news001_2.html, (参照 2017-08-26).

[19] 佐々木良一，石井真之，日高悠，矢島敬士，吉浦裕，村山優子，“多重リスクコミュニケータの開発構想と試適用”，情報処理学会論文誌，Vol.46，No.8，pp. 2120-2128, 2005.

[20] “lcamtuf.coredump.cx/p0f3/README”, http://lcamtuf.coredump.cx/p0f3/README, (参照 2017-8-27).

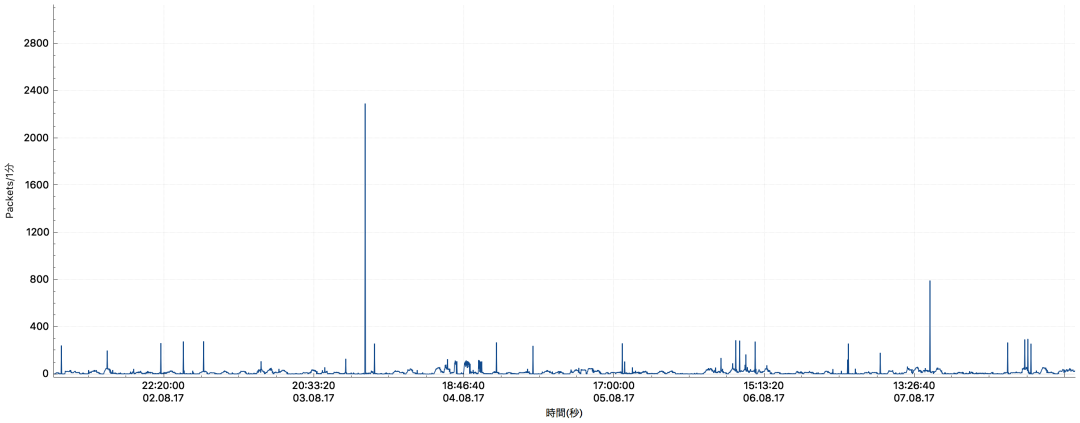

図 7　80 番ポートに着信した SYN パケットの数（前半）

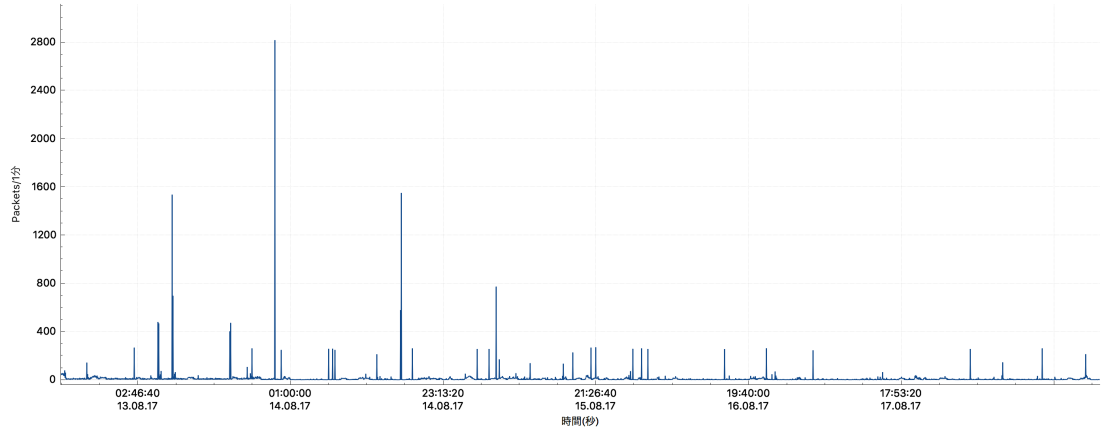

図 8　80 番ポートに着信した SYN パケットの数（後半）