キャプチャ通信のセキュリティアプライアンスによる事後検査の精度評価

名執 邦彦† 髙橋 佑典†

吉岡 克成† 松本 勉†

†横浜国立大学
240-8501 神奈川県横浜市保土ヶ谷区常盤台 79-7
{natori-kuhnihiko-xs,takahashi-yusuke-pw}@ynu.jp

{yoshioka,tsutomu}@ynu.ac.jp

あらまし 近年，増加するサイバー攻撃から情報システムを守るためにセキュリティアプライアンスが広く導入されている．通常，セキュリティアプライアンスは，機器が設置されたネットワーク内を流れる通信をリアルタイムで検査する．しかし，研究開発時には，過去の通信をアプライアンスに通して，その結果を検証する場合がある．その通信が長期間である場合，キャプチャ時と同じタイミングで再現を行うと事後検査にも長期間必要となる．そこで，再現時にパケット送信間隔をキャプチャ時よりも短くして，検査所要時間を短くする場合に検査結果にどのような影響があるかを検証する．

Accuracy Evaluation of Detection Results of Security Appliance on Examining Reproduced Packets

Kunihiko Natori† Yusuke Takahashi†

Katsunari Yoshioka† Tsutomu Matsumoto†

†Yokohama National University
79-7 Tokiwadai, Hodogaya-ku, Yokohama-shi, Kanagawa, 240-8501 Japan
{ natori-kuhnihiko-xs,takahashi-yusuke-pw }@ynu.jp,

{ yoshioka, tsutomu}@ynu.ac.jp

Abstract. Security appliance has been introduced widely in order to protect information systems from cyber-attacks. Normally, these security appliances examine in real-time communication through the network. However, in R&D, there is a case when the appliance examines reproduced communication captured in the past. If the examined communication is reproduced at the same speed as it is captured, the examination takes just as much time as its capture time. Therefore, in this study, we look at the detection results of the appliance when the packet reproduction is faster than when captured.

1 はじめに

近年，増加するサイバー攻撃から情報システムを守るためにセキュリティアプライアンスが広く導入されている．セキュリティアプライアンスは機器が設置されたネットワーク内を流れる通信をリアルタイムで監視し，不正な通信を発見した場合は通信の遮断や管理者に対して注意を促すアラートを発生させる．しかし，セキュリティ技術の研究開発時には，様々な状況で取得された通信キャプチャを通信再現ツールで再度パケットとして復元し，これをセキュリティアプライアンスに入力することにより事後検査を行う場合がある．特に大量のキャプチャ通信の事後検査を行う場合，キャプチャ時と同じタイミングでパケット送出を行うとキャプチャ時間と同じだけの時間が事後検査に必要となる．

そこで本研究では，過去に収集された通信の再現時に，パケット送信間隔をキャプチャ時よりも短縮し再現速度を上げることで，検査所要時間を短くする場合に検査結果にどのような影響があるかを検証する．具体的には，セキュリティアプライアンスが導入されていない環境でキャプチャされた通信をパケット再送ツールであるTcpreplay[1]を用いて様々な速度で再現し，セキュリティアプライアンスによる攻撃検知結果を比較検証する．また，この評価実験の前提として，Tcpreplay 自体が十分な高速パケット再生能力を有しているかを評価するため，セキュリティアプライアンスを導入しない状況で高速再生を行い，パケットロスの有無を検証した．この結果，Tcpreplay は実験に用いた特定の機器においてキャプチャ時の5倍程度の高速再送をパケット落ちを起こすことなく実行する能力を有していることを確認した．また，セキュリティアプライアンスについては，特に再現対象の通信に多くの攻撃が含まれる場合に，再現通信の通信速度が機器の仕様上のスループットを下回っている場合においても検知漏れを起こすことを確認した．

本稿では，まず第 2 章でパケット再送ツールである Tcpreplay について述べ，これを用いた通信再現手法を説明する．第3章でこの手法の精度について検証実験を行い，第4章で考察を行い，第5章でまとめと今後の課題を述べる．

2 Tcpreplay による通信再現

2.1 Tcpreplay

Tcpreplay は pcap 形式で保存された通信を再送するためのツールである．ファイアーフォールや侵入検知/侵入防御(IDS/IPS)機能やルータ,スイッチといったネットワーク機器の動作検証など様々な用途で使用されている．Tcpreplay は，動作するホストの IP アドレスや Mac アドレスに関係なくパケットを送信する．デフォルト設定におけるパケット送信タイミングは，pcap 内の各パケットのタイムスタンプに基づいている．また再送速度を変更することが可能である．

Tcpreplay による再送を補助するツールとして Tcpprep[2]がある．Tcpprep により，特定の IP アドレスや MAC アドレスをもつパケットに対してタグ付けを行い，タグに基づきパケットを送出するネットワークインターフェースの指定やアドレスの書き換えを行うことができる．

本研究ではこの Tcpreplay および Tcpprep を用いて通信を再現し，検証を行う．

2.2 通信再現

本章では Tcpreplay を用いた通信再現方法について記述する．図1に Tcpreplay を動作させる環境を示す．

1) NIC を二枚搭載しているホストへ Tcpreplay をインストールする．2 つのインターフェースをそれぞれ eth0，eth1 とする．
2) Tcpprep を用いて，再送する pcap 内のどのホストの通信を，どちらのインターフェースから送信するか指定する．例えば，ホスト A とホスト B の間の通信を保存した pcap ファイルを再送する場合,ホスト A が送信元のパケットはすべて eth0 から送信し，ホスト B が送信元のパケットはすべて eth1 から送信

するように指定することで eth0 と eth1 の間で両ホスト間の通信を再現できる．多対多の通信を保存した pcap ファイルから通信を再現する場合も同様に 2 つのインターフェースのどちらからどのパケットを送信するかを指定することで再現を行う

3) 再送対象の pcap ファイルを Tcpreplay により再現する．

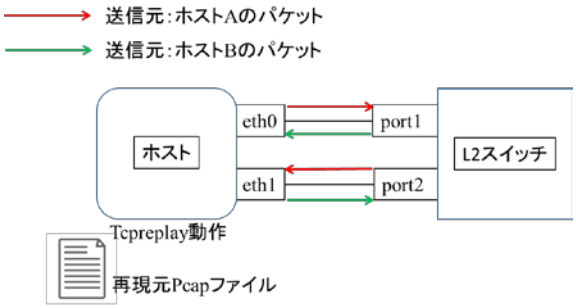

図 1.通信再現環境

3 検証実験

本章では 2 章に記述した通信再現手法の再現性について検証する．まず，Tcpreplay が通信再現を正確に行っているか確認する．次に，再現された通信をセキュリティアプライアンスに通して検査結果の比較を行う．再現対象の通信はマルウェア動的解析により得られた攻撃通信を用いる．表 1 は図 3 に示す各実験機器の情報である．

表 1. 実験機器情報

	ホスト	観測用ホスト
CPU	Intel(R)Pentium (R)CPUG620 2.60GHz	Intel(R) Core(TM) i5-2467M CPU 1.60GHz
メモリ	3.6GB	3.6GB
NIC	Intelcorporation 82574L Gogabit Network Connection	Intelcorporation 82579V Gigabit Network Connection

L2 スイッチは Cisco Catalyst 3750G-24TS-24 を使用．

3.1 再現対象通信の取得

再現対象となる pcap ファイルを収集するために行ったマルウェア動的解析の環境を図 2 に示す．表 2 に示す解析対象の検体についてそれぞれ以下の手順で動的解析を行い，再現対象通信を取得した．

1) 仮想マシン V1 上でマルウェア検体を 5 分間実行する
2) Iptables[3]のパケットフィルタリングを用いて特定の宛先ポート(135, 139, 445/TCP など)への攻撃通信を V2,V3 上で動作するハニーポットへ転送する．ハニーポットとしては Nepenthes v 0.2.0[4]と Dionaea v 0.1.0[5]を用いている．この時に V1 と他のホストの間の通信を Tcpdump[6]によりキャプチャし，再現対象 pcap ファイルとする．

得られた pcap ファイルの情報とホスト V1 からの通信の情報を表 3, 4 に示す．

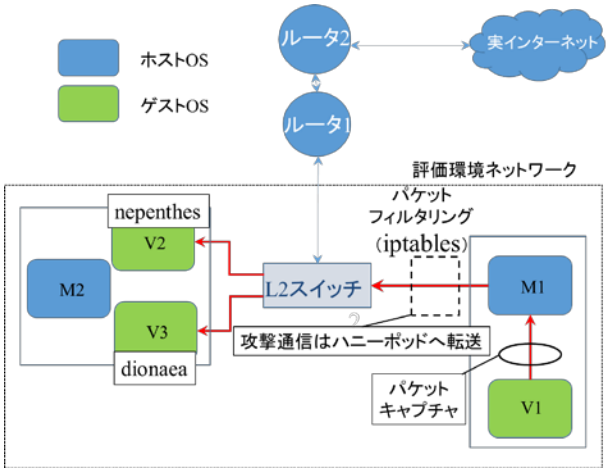

図 2. マルウェア動的解析環境

表 2.動的解析に用いた検体

検体	MD5ハッシュ値	McAfee 検知名
検体1	a12cab51ef99e9830 5668d189d0db147	Generic BackDoor.l
検体2	1e8c768616096e7b0 3ee8c206c07eba3	W32/Sdbot.worm
検体3	d1ee9d2e39e06495a a8b457e3d2d75a4	W32/Blaster.worm.f
検体4	e6d380d44ebb53941 1002dcbb249d43a	Artemis!E6D3 80D44EBB

表 3. 再現対象 pcap ファイル情報

収集検体	パケット数	平均 pps	平均bps	時間 (sec)
検体1	18507	57.6	6430.8	321.3
検体2	30388	94.4	22247.5	322.0
検体3	291	0.9	154.4	321.2
検体4	6659	20.7	1639.9	322.5

表 4.V1 を送信元とするパケット情報

検体	tcpパケット			udpパケット	
	宛先ポート	パケット数	セッション数	宛先ポート	パケット数
検体1	445	14054	63	1900	3
				123	2
				53	2
検体2	135	12978	2597	135	1296
	9191	3903	1301	53	149
				1900	3
				123	2
検体3	135	111	20	1900	3
	4444	43	15	123	2
				53	1
検体4	445	5886	2607	53	17
	44445	72	24	190	3
				123	2
	11000	39	13		

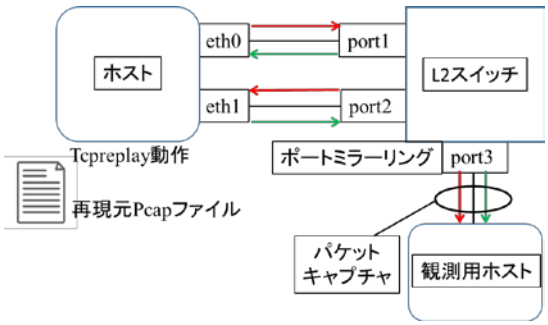

図 3 検証用通信再現環境

3. 2 Tcpreplay の再現精度評価

3.1 節で得られた再現対象通信を図 3 の環境で再現し，Tcpreplay の再現精度評価を行った．Tcpreplay による再現は，1 倍速(デフォルト速度)から 10 倍速までを 5 回ずつ行い，それぞれの場合について，L2 スイッチのポートミラーリング機能により観測用ホストへのパケットの転送を行い，通信再現の様子を観測した．

再現時に観測用ホスト上で得られた pcap ファイル（再現時 pcap ファイル）の分析を行った．図 4 に再現対象 pcap ファイルには含まれるが再現時 pcap ファイルには含まれないパケット，すなわちパケット落ちしたパケット数を示す．パケット落ちの有無は，再送対象 pcap ファイルと再現時 pcap ファイルを比較することで調べた．

実験の結果を図 4 に示す．再現対象 pcap ファイルには存在した IGMP プロトコルの 2 パケットがいずれの倍速再生時にも観測されなかった．これは Tcpreplay が IGMP パケットの再送に対応していないためと考えられる．これ以外のプロトコルのパケットは，5 倍速再生時までは完全に再現されている．

次に再現対象 pcap ファイルと再現時 pcap ファイルを wireshark[7]で読み込み，分析を行い得られる以下の情報を比較する[8][9]．

・Error 数
　プロトコルの仕様に沿っていないパケットやチェックサムエラー等の起きたパケット数
・Warning 数
　シーケンスナンバーの不一致や Window サイズに問題のあるパケット数
・Note 数
　再送，重複 ACK，特異な TTL，アプリケーションエラーの数
・Chat 数
　リクエスト/レスポンスを分類した数

このうち，「Error 数」および「Warning 数」を異常パケット数とし，再現対象 pcap ファイルより得られる値から，再現時 pcap ファイルより得られる値を引いたものを図 5 に示す．

これらの結果から，Tcpreplay による再送は，再現対象 pcap ファイルの内容にも依存するものの，一定の再送速度まではほぼ正確に行われると考えられる．

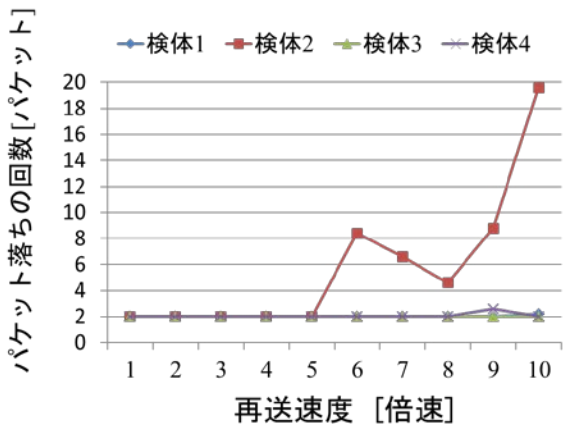

図 4. 各再送速度における平均パケット落ち数

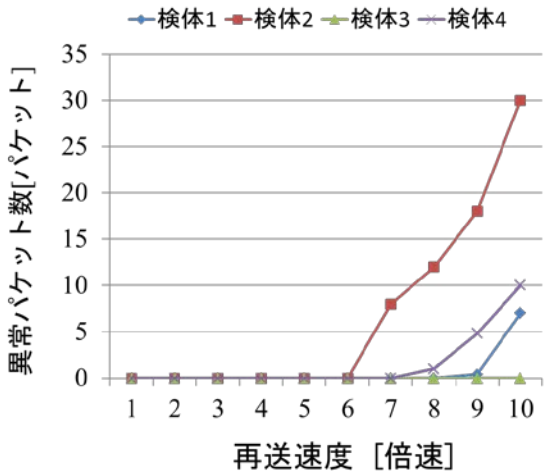

図 5. 各再送速度における平均異常パケット数

3.3 再現通信のセキュリティアプライアンスによる検査

図 1 における L2 スイッチをあるセキュリティアプライアンスに置き換えた環境で，Tcpreplay による通信再現を行い，通信の事後検査を行う．セキュリティアプライアンスは L2 スイッチとして動作するように設定し，ファイアウォール機能は無効にする．また，通信の遮断はせず，攻撃通信の検知だけをするように設定し(IDS 機能による検査のみ行う)，攻撃を検知した際の検知ログの内容および検知ログ数について検証をする．

再現には 3.1 節で得られた 4 検体の動的解析時の通信に加えて，表 5 に示す 2 検体を図 2 と類似した動的解析環境において 1 時間実行した際に得られた通信を用いる．pcap ファイルの情報と検体実行ホストからの通信の情報を表 6, 7 に示す．再送速度は 1 倍速(デフォルト速度)から 10 倍速まで試験した．

表 5. 評価用の動的解析を行った検体

収集検体	MD5 ハッシュ値	McAfee検知名
検体5	cd10050574974a441cc89d1a5a41ba59	ZeroAccess.ib
検体6	3b7eb30a8309d9ec39ce22f07c958f15	W32/Bobax.worm.gen

表 6. 再現対象 pcap ファイル情報

検体	パケット数	平均 pps	平均 bps	時間 (sec)
検体5	6497	1.8	692.2	3599.6
検体6	85728	23.8	3400.3	3599.3

表 7. 検体実行ホストを送信元とする通信内容

検体	tcpパケット			udpパケット	
	宛先ポート	パケット数	セッション数	宛先ポート	パケット数
検体5	16471	161	5	16471	3577
	80	10	2	53	16
				123	5
				1900	3
検体6	25	22679	22677	53	16036
	443	7068	6949	137	2634
	80	6640	699	138	35
	22	149	2	その他	83
	65520	81	1		

表 8 には再現元となる pcap を収集した検体番号と，pcap を再送した際にセキュリティアプライアンスから出力された検知ログを示す．

図 6 に倍速再生時の検知ログ数と通常再生時の検知ログ数との比較を示す．

表 8. セキュリティアプライアンスが出力した検知ログの内容

検体	検知ログの内容
検体1	Windows LSASSへのバッファオーバーフロー(445/tcp)
検体2	Windows Messenger Service へのバッファオーバーフロー(135/udp)
検体3	Windows DCOMバッファオーバーフロー(135/tcp)
検体4	Windows LSASSへのバッファオーバーフロー(445/tcp)
検体5	ZeroAccessボットネット(16471/udp)
検体6	SSLv3 Session IDオーバーフロー(443/https) salityボットネット(80/http) virutボットネット(80/http)

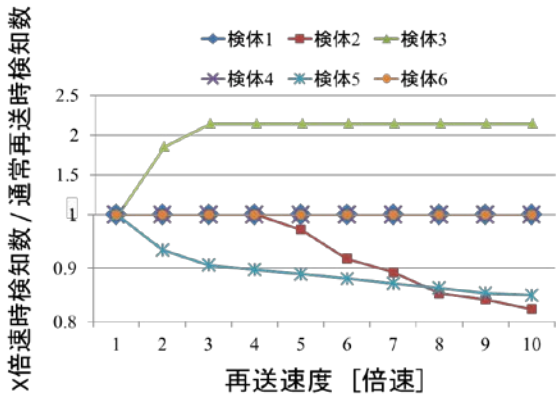

図 6.倍速生成時のセキュリティアプライアンスの検知ログ

4 考察

再送速度を変更しても検知ログ数が変化しない場合，検知ログ数が減少した場合，増加した場合が確認された．検体 1，4，6 については再送速度に関わらず検知ログ数は変化しなかった．以降では，検知ログ数が減少した通信と，増加した通信について，それぞれ考察を行う．

4.1 検知ログ数が減少した通信

検体 2 と検体 5 の動的解析により得られた通信については，再生速度を上げるにつれてアプライアンスによる検知ログ数が減少した．検知数減少の原因としては以下の二つが考えられる

1. Tcpreplay による再送速度変更によるパケット落ちもしくはパケット異常の影響
2. セキュリティアプライアンスの検知漏れ

パケット落ち，パケット異常の影響

図 4 と図 5 より，検体 2 については 5 倍速以降でパケット落ちの数や異常パケット数が増加している．攻撃として検知される通信が落ちてしまう，もしくは攻撃パケットではなく異常パケットとなった場合には検知数減少の要因として考えられる

セキュリティアプライアンスの検知漏れの影響

通信の再送速度を上げたことにより，セキュリティアプライアンスの処理が追いつかず検知漏れが発生した可能性について考察する．図 7 に検体 2 と検体 5 から得られた通信の倍速再生時の情報を示す．図 7 において通信速度[bps]は Tcpreplay が通信の再送終了時に出力した通信全体の平均値である．なお，今回使用したセキュリティアプライアンスの IDS スループットは 135Mbps となっている．

図 7 を見てみると，どの再送速度の場合においても 135Mbps を超えているものはない．しかし，これは再送期間全体における平均の速度である．そこで，wireshark の statistics により，再送期間中，瞬間的にアプライアンスのスループットを超える通信が発生していたか調査した．

135(Megabits/sec) =135000000 (bits/sec)
=135000 (bits/0.001 sec)

であるので，0.001 秒に 135,000bit を超える通信が発生していた場合に，パケットの処理が追いつかないことが考えられる．この値を閾値として，検体 2 の通信を図 3 の環境で，検知数が大きく減り始めた 5 倍速再送を行い，観測用ホストで得られた pcap ファイルについて wireshark で分析した結果の一部を図 8 に示した．

これを見ると閾値を超えている通信を確認で

きる. 3 倍速, 4 倍速においても確認できたが, その数は少なかった. 9 倍速や 10 倍速では閾値を超える通信が多数存在しており, これによるアプライアンスの検知漏れが起きていると考える. しかし, 検体 5 について同様の分析を試みたが閾値を超える通信は観測できないにも関わらず, 検知数が減少していた.

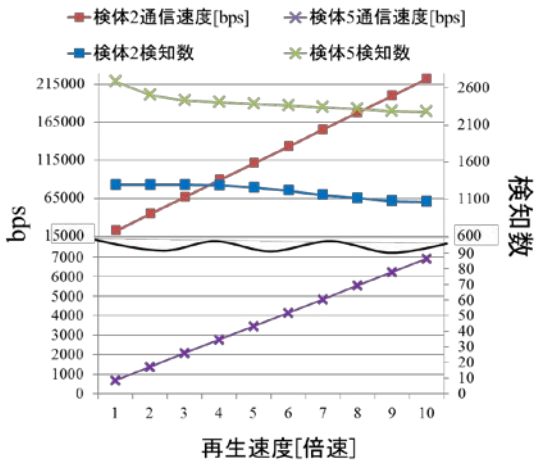

図 7.検体 2 および検体 5 の検知数と通信速度の推移

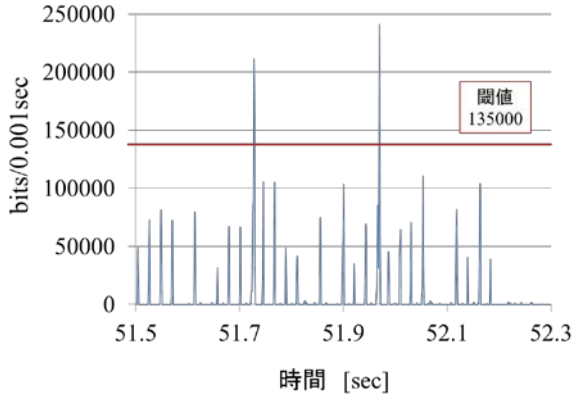

図 8. 検体 2 の通信の倍速再現(5 倍)時における各時刻の通信速度(1 秒単位で集計)

表 9 には検体 2, 検体 5 の再送実験を行った際にセキュリティアプライアンスが出力したトラヒックログ数を示す. 表 9 を見てみると, 検体 5 については再送速度を上げることによってセキュリティアプライアンスから出力されるトラヒックログ数が大きく減少しており, 検査したパケット数が減少していることがわかる.

検体 5 は再現対象 pcap ファイルのパケット数に対する, 1 倍速再送時の検知数の割合が 41.157%と非常に高く, 多くの悪性通信を含んでいるが, このことにより処理の遅延が発生し, 検知漏れが起きている可能性がある.

表 10 に再送実験に用いた 6 個の通信を 1 倍速で再送した際に, セキュリティアプライアンスが出力した検知ログ数の, 再現元 pcap ファイルのパケット数に対する割合を示す.

表 9. 検体 2, 検体 5 の各再送速度において出力されたトラヒックログ数

再送速度	検体2ログ数	検体5ログ数
1倍速	10430	5357
2倍速	10417	4945
3倍速	10416	4861
4倍速	10416	4806
5倍速	10416	4730
6倍速	10410	4652
7倍速	10391	4620
8倍速	10379	4578
9倍速	10372	4532
10倍速	10376	4506

表 10.1 倍速再送時における検知数の再現元パケット数に対する割合

収集検体	検知数/再現元パケット数（%）
検体5	41.157
検体2	4.265
検体3	2.405
検体1	0.967
検体4	0.360
検体6	0.030

4.1 検知数が増加した通信

検体 3 については, 再送速度を上げることによって検知数が増加した. この検体についてセキュリティアプライアンスが出力するトラヒックログを確認すると, 表 11 に示すように再送速度を上げることで IDS 機能以外による破棄パケットの数が減少していることが分かった. 速度変更によってパケットがアプライアンスに到達するタイミングがずれたことにより, 本来 IDS 機能によ

って検査される前に破棄されていた通信が検査対象となり，結果としてより多くの攻撃が検知されたのではないかと考える．これはセキュリティアプライアンスの実装に関わるため詳細は不明であるが，今後，より多くの通信による検証を行うことでこの現象の解析を行いたい．

表 11. 検体 3 通信の各再送速度における検知ログと破棄パケット数

再送速度	検知ログ数	破棄パケット数
1倍速	7	16
2倍速	13	4
3倍速	15	0
4倍速	15	0
5倍速	15	0
6倍速	15	0
7倍速	15	0
8倍速	15	0
9倍速	15	0
10倍速	15	0

5 まとめと今後の課題

通信再現ツールである Tcpreplay を用いて通信の再現を行いセキュリティアプライアンスによる通信の事後検査を行った．その際に送信間隔をキャプチャ時よりも短縮することで検査時間を短縮した場合に，セキュリティアプライアンスのスループット以下の通信速度であっても，検知結果に影響を与える場合があることがわかった．再現する通信に悪性通信が含まれる割合が検知結果に影響している可能性がある．今後は，Tcpreplay 以外の再現ツールの利用や対象のアプライアンスを増やして倍速再生時の検知結果の変化を検証したい．

謝辞　本研究の一部は，総務省情報通信分野における研究開発委託／ 国際連携によるサイバー攻撃の予知技術の研究開発／サイバー攻撃情報とマルウェア実体の突合分析技術／類似判定に関する研究開発により行われた．

参考文献

[1] Tcpreplay pcap editing & replay tools for NIX, http://tcpreplay.synfin.net/
(Last Visit : 2014/08/15)
[2]tcpprep, http://tcpreplay.synfin.net/wiki/tcpprep
(Last Visit : 2014/08/15)
[3] The netfilter.org "iptables" project, http://www.netfilter.org/projects/iptables/
(Last Visit : 2014/08/15)
[4]nepenthes, http://nepenthes.carnivore.it/
(Last Visit : 2014/08/25)
[5]dionaea, http://dionaea.carnivore.it/
(Last Visit : 2014/08/25)
[6]Tcpdump&Libpcap, http://www.tcpdump.org/
(Last Visit : 2014/08/15)
[7]Wireshark, https://www.wireshark.org/
(Last Visit : 2014/08/15)
[8]Wireshark-7.3. Expert Infos, https://www.wireshark.org/docs/wsug_html_chunked/ChAdvExpert.html(Last Visit : 2014/08/15)
[9]Wireshark 分析機能入門, http://pa.hebikuzure.com/Files/Wireshark_4.pdf
(Last Visit : 2014/08/15)