ネットワークセキュリティ機器の評価環境構築

中村 豊[1,a)]　佐藤 彰洋[1,b)]　福田 豊[1,c)]　和田 数字郎[2,d)]

概要：
これまでのネットワークセキュリティ機器の評価は，実際の環境からミラートラヒックを取得して機能を評価する，もしくはエミュレータを用いて評価するのどちらかであった．実際の環境での評価の場合は，同時期に複数の機器を評価することが難しいため，公平な視点での評価が難しい，という問題点がある．また，エミュレータを用いた評価では公平な基準で評価することはできるが，実際の環境と異なるため，運用に入った際に挙動が異なるという問題点が考えられる．この様な問題点を解決するために本論文では，過去に蓄積したパケットキャプチャを再現することで，同一の条件で複数のネットワークセキュリティ機器を評価できる環境を構築した．さらに複数のメーカのセキュリティ機器をパケット再現装置に適用しメーカ毎の違いを確認した．

キーワード：ネットワークセキュリティ，評価環境，pcap replay tool，次世代ファイアーウォール

Construction of evaluation environment for network security products

Yutaka Nakamura[1,a)]　Akihiro Satoh[1,b)]　Yutaka Fukuda[1,c)]　Sujiro Wada[2,d)]

Abstract: To evaluate the network security products so far, we perform either evaluation of the function by obtaining mirror traffic from the actual environment, or evaluation using the emulator. In the case of evaluation in an actual environment, it is difficult to evaluate multiple devices at the same time, and therefore it is difficult to evaluate fair them. In the evaluation using the emulator, there is a problem it is different from the actual environment. In order to solve such a problem, in this paper we propose to replay the packet capture stored in the past, thereby constructing an environment that can evaluate multiple network security products under the same conditions. Furthermore, we applied security products of multiple manufacturers to packet replay device and confirmed the difference between manufacturers.

Keywords: Network Security, Evaluation Environment, pcap replay rool, Next Generation Firewall

1. はじめに

情報セキュリティ対策の高まりにより，セキュリティ機器の選定，導入は重要な課題の 1 つとなっている．しかしながら，セキュリティ製品の評価では客観的な基準の設定が難しく，ガートナー [1] や NSSLABS[2] の様な第三者機関の評価に依存している．この様な第三者機関の評価結果を得るためには多くの費用が必要であることが問題となっている．また，自社でネットワークセキュリティ機器の評価を行う場合
(1) 実際の環境からミラートラヒックを取得して評価する
(2) エミュレータを用いて評価する
のいずれかである．実際の環境でのミラーポートでの評価の場合は，同時期に複数の機器を評価することが難しいた

[1] 九州工業大学 情報科学センター / 情報基盤運用室
Kyushu Institute of Technology, Information Science Center / Information Infrastructure Office
1-1 Sensui-cho, Tobata-ku, Kitakyushu, 804–8550, JAPAN
[2] 九州工業大学 飯塚キャンパス技術部 / 情報基盤運用室
Kyushu Institute of Technology, Iizuka Campus Technical Support Office / Information Infrastructure Office
680-4 Kawazu, Iizuka-shi, Fukuoka, 820-8502, JAPAN
[a)] yutaka-n@isc.kyutech.ac.jp
[b)] satoh@isc.kyutech.ac.jp
[c)] fukuda@isc.kyutech.ac.jp
[d)] swada@isc.kyutech.ac.jp

め，公平な視点での評価が難しい，という問題点がある．またネットワークセキュリティ機器が全ての要素を有効にできないという問題もある．エミュレータを用いた評価では公平な基準で評価することはできるが，実際の環境と異なるため，運用に入った際に挙動が異なるという問題点が考えられる．また，エミュレータ自体が非常に高価であるという事も問題である．

この様な問題点を解決するために本論文では，過去に蓄積したパケットキャプチャを再現することで，同一の条件で複数のネットワークセキュリティ機器を評価できる環境を構築する．九州工業大学では [3][4] で述べている様に，これまで様々なネットワークセキュリティ機器の評価を行ってきた．また [4] では，情報セキュリティ対策の一環としてキャンパスネットワークの境界においてパケットのフルキャプチャを行うネットワークフォレンジックシステムを構築している．本研究では，このネットワークフォレンジックシステムに蓄積されている過去 2 週間分のキャプチャデータをトラヒック再現装置へコピーし実際の運用環境に影響を与えない形でネットワークセキュリティ機器の評価を行える環境を構築した．

さらに [4] で述べた SDN スイッチに評価用機器を接続することで Web UI の操作のみで評価機器の切り替えを実施した．構築した評価環境の有効性を評価するために複数のメーカのセキュリティ機器を本提案環境に適用し実際のトラヒックをセキュリティ機器へ適用し，それらの出力するログの違いについて機器毎の違いが確認できた．

2. 関連研究

本章では，既存のネットワークセキュリティ機器の評価方法について，問題点を述べる．

2.1 パケット再生ツール

蓄積された pcap データを再現するツールとして，tcpreplay[5] がある．tcpreplay はタイムスタンプに基づき正確に pcap を再現することができるツールである．tcpreplay では dual interface mode が存在し，インタフェース 1 へ出力する pcap およびインタフェース 2 へ出力する pcap を準備することで，仮想的な WAN 側および LAN 側の実現が可能である．しかしながら，再現の正確性を高めるために，事前に pcap ファイルをメモリへプリロードする必要があるため，大容量の pcap データを連続的に正確に再現することは困難である．また，メモリへプリロードしない再生を行なった場合，tcpreplay が出力するログがエラーを出力するため，再生が正しく実施されているかどうか，確認することができない．

2.2 エミュレータ

ネットワークセキュリティにおける負荷ツールは商用製品が供給されている．例えば Spirent 社は Avalanche[6] と呼ばれるアプリケーション/セキュリティ負荷ツールを提供している．Avalanche では様々なセキュリティ試験を実施することが可能であるが非常に高価なため，セキュリティ機器を導入するために購入して事前に試験することは非常に困難である．また，大容量の pcap ファイルの連続的な再生も困難である．

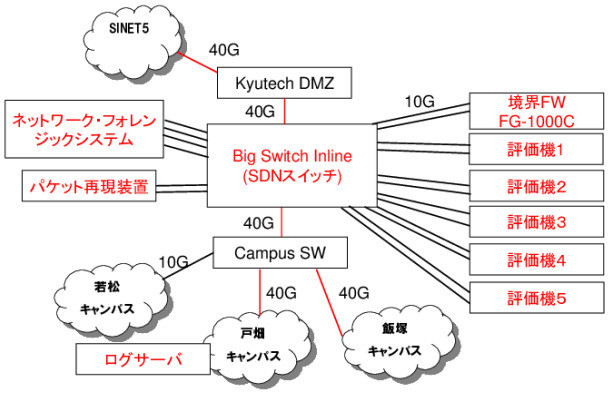

図 1 システム概要図

2.3 ミラーポートを用いた評価手法

スイッチからミラーポートを設定して，ネットワークセキュリティ機器に対してトラヒックを入力することでネットワークセキュリティ機器を評価する手法は一般的である．しなしながら，一部のネットワークセキュリティ機器では，インライン環境で有効な機能と，ミラーポートでの有効な機能で差異がある．例えば Fortinet 社の Fortigate シリーズではミラーポートでの環境ではアンチスパム機能は有効にならない．また，SonicWall 社の SuperMassive シリーズでは [7] に示されるように，TAP モードではほとんどの機能が有効にならない．したがって，インライン環境において全ての機能を有効にしてネットワークセキュリティ機器を評価する必要がある．

3. 提案システム

本節では，2 節で述べた既存研究の問題点を解決するために，インライン環境において過去に蓄積したパケットを再生するためのツールを用いた，ネットワークセキュリティ機器の評価環境の構築について述べる．

3.1 システム概要

図 1 にシステム概要図を示す．図 1 で赤色で示した部分が本システムの構成要素である．構成要素としては，Kyutech DMZ，SDN スイッチ，境界 FW，Campus SW，ネットワークフォレンジックシステム，パケット再現装置，

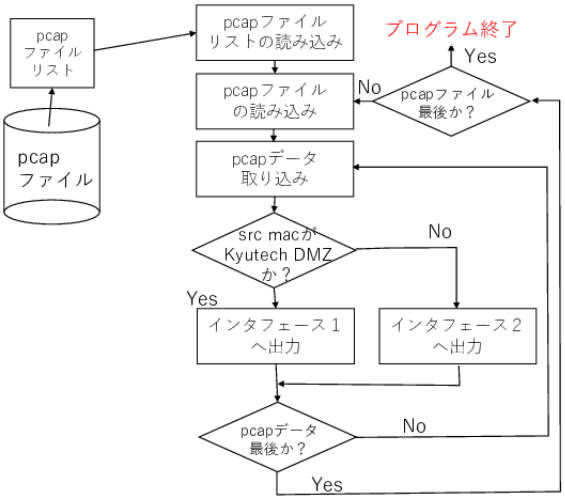

図 2　パケット再現ソフトウェアフローチャート

ログサーバ，評価機 1 ～ 5 がある．以下の節でそれぞれの構成要素について詳細を述べる．

3.2　キャンパスネットワーク機器

図 1 における，Kyutech DMZ および Campus SW はジュニパーネットワークス社の EX4550-32T である．Kyutech DMZ は SINET5 への接続のためのレイヤー 3 スイッチであり，Campus SW は戸畑キャンパス，飯塚キャンパス，若松キャンパスへ接続するための L2/L3 スイッチである．ネットワークフォレンジックシステムに蓄積される pcap データはこれらのスイッチの mac アドレスが保存される．したがって，学外から到着したパケットは src mac アドレスが Kyutech DMZ として保存され，学内から学外へ向かうパケットは dst mac アドレスが Kyutech DMZ として保存される．

境界 FW はフォーティネット社の FG-1000C である．境界 FW では Web Filtering，アプリケーション制御，アンチウイルス，情報漏洩対策等の様々なポリシーが設定されている．SDN スイッチによって，境界 FW を通過したパケットをネットワークフォレンジックシステムにミラーしている．したがって，外部からの攻撃は境界 FW でブロックされ，外部への異常な通信も境界 FW でブロックされるため，蓄積される pcap データには学内から学外へのブロックされる前のパケットが保存される．

3.3　パケット再現装置

パケット再現装置は PC サーバとパケット再現ソフトウェアより構成される．パケット再現ソフトウェアは C 言語によりプログラムを作成した．PC サーバは 10Gbase-SR インタフェースを 2 個備えたもので，これらのインタフェースが評価機から見て仮想的な WAN 側および仮想的な LAN 側のインタフェースとなる．

図 2 に再現ソフトウェアのフローチャートを示す．再現ソフトウェアはハードディスクに保存されている pcap ファイルをリスト化した pcap ファイルリストを読み込む．pcap ファイルリストを読み込んだ後に，リストに記述されている pcap ファイルを読み込み，pcap データを取り込む．pcap データを取り込むと，イーサフレーム以下のパケットデータを取得できるので，イーサフレーム内の src mac アドレスフィールドを確認する．src mac アドレスが Kyutech DMZ スイッチと同一のものであれば，学外から届いたパケットであるため，仮想的な WAN 側インタフェースであるインタフェース 1 へパケットを出力する．そうでない場合は学内から届いたパケットであるため，仮想的な LAN 側であるインタフェース 2 へパケットを出力する．

3.4　ネットワーク・フォレンジックシステム

ネットワーク・フォレンジックシステムは HP 社 ProLiant SL4540 Gen8 サーバが導入されている．OS として CentOS7 が稼働し，tcpdump コマンドにより大学の出入り口のすべてのパケットをペイロードも含めて保存している．ストレージとして 4 TB ニアライン SAS が 60 台導入されており，物理容量は 240TB となっている．これを RAID6 構成とし，100TB のパーティション 2 つに分割している．それぞれのパーティションで奇数日，偶数日と振り分けを行い，ディスク障害対策としている．ネットワークインタフェースは 10Gbase-T インタフェースを 2 口準備し，キャンパス間スイッチからのポートミラーでトラヒックをキャプチャしている．また，実験用インタフェースとして 10Gbase-SR インタフェースを 2 口準備し，パケットキャプチャしたデータを実験用インタフェースへ出力する環境も構築した．ネットワーク・フォレンジックシステムを用いる事で九州工業大学ではおおよそ 3 ヶ月間のトラヒックを保存することが可能となっている．3 ヶ月以内であれば，遡って通信履歴を追跡することが可能となっているため，ネットワーク・フォレンジックの重要な設備となっている．

3.5　SDN スイッチ

2017 年 3 月に導入した，SDN スイッチ Big Monitoring Fabric[8] により，これまではミラートラヒックによる評価しかできなかったものが，インライン環境で評価することが可能となり，評価機の導入，撤去が容易になった．このシステムを用いる事で，実験完了後にセキュリティ機器に問題ない事が確認できれば，直ちに運用環境へ切り替えを行う事ができる．

3.6　ログサーバ

ログサーバは HP 社製 DL360 Gen7 4 CPU core 8

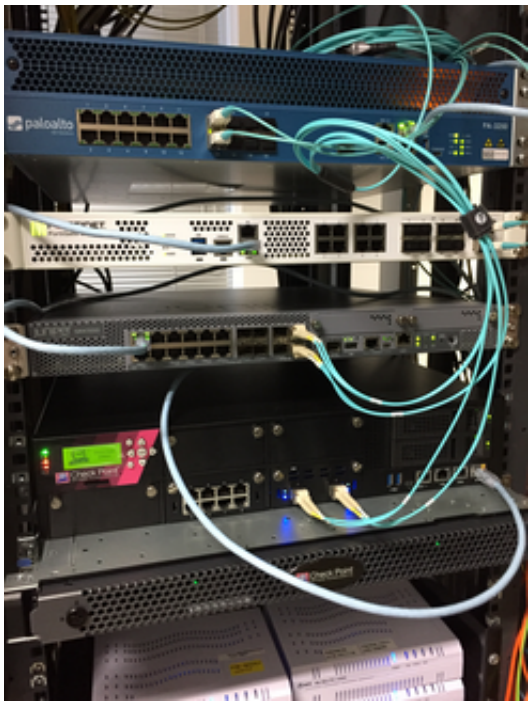

図 3　評価機

threads, 60GB メモリ，物理容量 24 GB (3TB HDD 8 台) を用い，OS には CentOS 7.5 を選択した．評価機 1 ～ 5 から出力されるログを受信するために，標準の rsyslogd を用い，機器の IP アドレス毎に分類する設定とした．

3.7　評価用ファイアーウォール装置

図 1 に示されている評価機 1～5 は，今回実験を進めるにあたって，我々がメーカに依頼し評価用の検証機の貸し出しを受けたものである．具体的には，PaloAlto Networks 社 PA-3250，チェック・ポイント・ソフトウェア ・テクノロジーズ社 CP-23800，フォーティネット社 FG-500E，ジュニパーネットワークス社 SRX-1500，ソニックウォール社 SM-9600 をそれぞれ借り受けて，パケット再現装置が出力するパケットを通過させる実験を行った．図 3 に実際の評価機の外観図を示す．一番上が PA-3250，上から 2 番目が FG-500E，三番目が SRX-1500，一番下が CP-23800 である．CP-23800 はセンサーおよびマネージャが別々の筐体となっている．これとは別ラックに SM-9600 がマウントされている．

4.　実験

図 4 に実験構成図を示す．学外から学内向けのパケットはパケット再現装置の仮想的な WAN 側インタフェースから出力され評価機 1 ～ 5 を順に通過して，パケット再現装置の仮想的な LAN 側インタフェースへ到着する．逆に学内から学外向けのパケットは仮想的な LAN 側インタフェースから出力されて評価機 5 ～ 1 の順で通過してパケット再現装置の仮想的な WAN 側へ到着する．

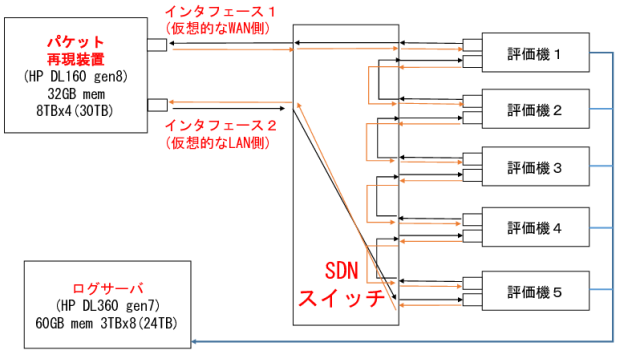

図 4　実験構成図

パケット再現装置には，ネットワークフォレンジックシステムから 15 日分 (2018 年 4 月 16 日から 4 月 30 日まで) の pcap データを事前にコピーして保存しておいた．pcap ファイルの総容量は約 23TB である．これは，ネットワークフォレンジックシステムから直接実験環境へパケットを送信することによる，ライブデータ保存への悪影響を防止するためである．しかしながら，平日 1 日分の pcap データ約 2TB のコピーには約 12 時間程度の時間を必要とするためコピー中にデータ欠損が発生している可能性は考えられる．したがって，ネットワークフォレンジックシステムの管理用インタフェースやパケット再現装置の管理用インタフェース増速を検討する必要がある．

パケット再現装置に事前に pcap データを保存しておく事で，実験失敗時に何度でも繰り返し評価機をテストする事が可能となっている．これは通常のセキュリティ装置の評価環境では持ち得ない特徴の 1 つである．1 回の実験で 23TB の pcap データをパケット再現装置が出力し，実行するためには約 36 時間が必要であった．

各評価機は管理用インタフェースを備えているため，パケット通過時のログ処理を管理用インタフェースを用いて行い，ログサーバへ syslog として出力する．パケット再現装置では約 1～2Gbps のスループットを出力することができるため，高負荷時の評価機の挙動を確認することができる．

実験後に明らかとなった事であるが，パケット再現装置では送信するパケットの TCP のセッションステートを確認していないため，ファイアーウォールのポリシーにおける TCP ステートを再現するシステムでは正しく動作しないことがわかった．したがって，実際の実験では，評価機 5 台を同時にテストするのではなく，1 台ずつのテストの実施となった．

全ての評価機において出力するログ項目および検知機能を公平に評価するために，評価機のパラメータのチューニングを行った．表 1 に各機器の設定したプロファイル一覧を示す．各ベンダ毎に有効化すると負荷が高くなる機能が

表 1　各機器の設定プロファイル一覧

機種	設定したセキュリティプロファイル
PA-3250 PAN-OS 8.1.2	アンチウィルス
	アンチスパイウェア
	脆弱性防御
	URL フィルタリング
	ファイルブロッキング
	WildFire 分析
	SSL 復号化
CP-23800 R80.10	アンチウィルス
	Anti-bot
	Threat Emulation (sandbox)
	アプリケーション制御
	URL Filtering
	IPS
FG-500E FortiOS 5.6.5	Web Filtering (flow mode)
	アンチウィルス (flow mode)
	SSL inspection
	アプリケーション制御
	DNS Filtering
	IPS
SRX-1500 JUNOS 15.1X49-D140.2	IPS
	Web Filtering
	アプリケーション識別
	アンチウィルス (未実験)
	アンチスパム (未実験)
SM-9600 SonicOS 6.5.1.1-42n.jpn	CFS(コンテンツフィルタリング)
	ゲートウェイアンチウィルス
	IPS
	Capture ATP (sandbox)
	アンチウパイウェア
	地域 IP フィルタ (ログのみ)
	ボットネットフィルタ (ログのみ)

あるが，ここではセキュリティ検知の公平性を評価することに注視したため，機器毎の負荷については考慮していない．以降の節で各セキュリティ設定項目について述べる．

4.1 PA-3250

パロアルトネットワークス社の PA-3250 は PAN OS 8.1.2 を用いて表 1 に示すプロファイルを設定し，全てをモニタとして syslog へ出力するように設定して実験を行った．ログ出力はセッションクローズ時に syslog サーバへ転送とした．PAN OS ではアプリケーション識別は標準で設定されているため，ここではプロファイルとしては存在しない．

4.2 CP-23800

チェック・ポイント・ソフトウェア・テクノロジーズ社の CP-23800 は R80.10 を用いて表 1 に示すプロファイルを設定し，全てをモニタとして syslog へ出力するように設定して実験を行った．ログ出力はある程度のセッションをまとめて出力する形式であったため，他メーカと比較してログ量は少なくなっている．また，高負荷時のインタフェースへのパケットキューイングに問題が生じていたため，複数コアを用いてパケットキューイング処理を行う様に設定変更を行った．

4.3 FG-500E

フォーティネット社の FG-500E は FortiOS 5.6.5 を用いて表 1 に示すプロファイルを設定し，全てをモニタとして syslog へ出力するように設定して実験を行った．FortiOS 5.6.5 では Web Filtering および Anti Virus は proxy mode のデフォルトでのプロファイルは proxy mode である．proxy mode で実験した際のログを確認した時に，Web Filtering ログが出力されていなかったため，Web Filtering および Anti Virus を proxy mode から flow mode へ変更して実験を行った．syslog への出力タイミングは設定で変更できないため，セッション開始時，終了時にログが出力される．

4.4 SRX-1500

ジュニパーネットワークス社の SRX-1500 は JUNOS 15.1X49-D140.2 を用いて表 1 に示すプロファイルを設定し，全てをモニタとして syslog へ出力するように設定して実験を行った．実験当初はアンチスパムおよびアンチウィルスのプロファイルも設定していたが，高負荷時に機能が停止してしまったため，これらのプロファイルは外して実験することとなった．SRX-1500 の設定を確認したところ，セキュリティイベントではないセッションログも保存される設定となっていたこと，および，セッション開始時・終了時にログ出力されるため非常に大量のログ件数として出力された．

4.5 SM-9600

ソニックウォール社の SM-9600 は SonicOS Enhanced 6.5.1.1-42n.jpn を用いて表 1 に示すプロファイルを設定し，全てをモニタとして syslog へ出力するように設定して実験を行った．SM-9600 もログ出力タイミングの設定ができないため，ログ開始時およびログ終了時にログが出力される．同一の pcap データを用いた実験において，外部脅威情報が変更された場合，ログ出力に影響が出ることが確認できた．

5. 結果および考察

本節では構築した実験システムにおけるキャプチャデータの妥当性の検証，及び各セキュリティ機器の評価結果を示す．

```
/data/20180416/tcpdump_20180416_000001.pcap
filename:/data/20180416/tcpdump_20180416_000001.pcap
start time:1535707053.465209
Interface ens1f0: 81289564 sent
Interface ens1f1: 68048364 sent
end time:1535707058.015516
exec time:4.550307
```

図 5　パケット再現ソフトウェアの出力例

5.1　パケット再現ソフトウェアの結果と考察

図 5 にパケット再現ソフトウェアの出力例を示す．pcap ファイルのパスおよび実行開始時刻，実行終了時刻，実行時間，各インタフェースの出力パケット数を出力している．実行開始時刻および実行終了時刻を保存することで，syslog ファイルに保存されているタイムスタンプから再生した pcap ファイルを調べることが可能となっている．

5.1.1　ネットワーク・フォレンジックシステムにおけるパケットロス問題

tcpdump を用いて，pcap ファイル内の TCP ペイロードが正しく取り出せるかどうか調べたところ，一部欠損していることが確認できた．2018 年 1 月 23 日 13 時 02 分から 2 分間の pcap データを調査したところ，9.6GB のデータ内でセッション数が 39914，正常と識別できるセッション数が 36373 であった．これらから，3541 セッションにおいてデータの欠損が確認できている．約 8.8%のセッションにおいてデータ欠損が発生していると思われる．これはネットワーク・フォレンジックシステムの構成上の問題である．ワイヤーレートでのパケットストアよりもディスク容量を重視した構成となっているため，書き込みが追いつかず欠損が生じていると思われる．この問題を回避するためにはディスク I/O をより高速なインターフェースに変更する必要があるが，これは今後の課題である．

5.1.2　ポートミラーおよびキャプチャ手法によるパケット到着順の変化の問題

wireshark[9] に付属している reordercap を用いて，pcap ファイル内のタイムスタンプが正しい順序で保存されているかどうか調べたところ，約 9GB の pcap ファイルにおいて約 42000 パケットが順不同であった．正確なセキュリティ機器評価のテストを行うための pcap を考えると，境界 FW の WAN 側インタフェースおよび LAN 側インタフェースにおいて入力パケットのミラーを取得してパケットを保存するべきである．しかしながらネットワーク・フォレンジックシステムではフォレンジックを実施することに主眼を置いているため，境界 FW のポリシー制御を通過した後のミラーパケットを保存している．よって本実験システムではネットワークセキュリティ機器が TCP ストリームを再構成するシステムの場合は，我々が提案する環境では正しく動作しないことが確認できた．この問題を解決するためには，TCP ストリームを考慮したパケット送信タイミング制御を行う必要があるが今後の課題とする．また，本提案環境においてセキュリティ機器をテストする場合，flow mode におけるプロファイルの統一が必要であることがわかった．

5.2　セキュリティ機器の結果と考察

表 2 に各メーカの実験結果を示す．以下の節に各メーカの結果および考察について述べる．

5.2.1　PA-3250

PA-3250 はマルウェアサイト判定数が 14366 件であった．これは脅威ログ (URL Filtering) より malware と判断されたものおよびトラヒックログにより検出されたものが含まれている．パロアルトネットワークス 社の URL 格付けサイト [10] により Web Filtering の格付けは確認することができる．また，C&C 通信の検知数は 5799 件であった．

5.2.2　CP-23800

CP-23800 はマルウェア判定数が 284 件であるが，これは，Anti Malware 207 件, Anti Virus 56 件, Threat Emulation 21 件で判定されたものが出力されている．チェックポイント 社の格付け判定サイト [13] は，URL Filtering で格付けを判定しているため，システム全体での脅威情報を得ることはできない．また，R80.10 ではログ集約化が行われているため，他メーカと比較してログ総量および件数が 2 番目に少なくなっている．実験後のデータ集計で明らかとなった事であるが，CP-23800 の実験時ではチューニングが十分ではなく，機器内でパケットロスが発生していた可能性が高い．したがって，機能試験のための再実験が必要であると思われる．

5.2.3　FG-500E

FG-500E はマルウェアサイト判定数が 77918 件で今回評価した機器の中で最も多かった．この件数には Web Filtering の格付けによって Malicious Web Site と判定されたものがカウントされており，フォーティネット社の格付け判定サイト [11] で手動により確認することができる．フォーティネット社の格付けは，経験的に Malicious Web Site からクリーンサイトへの格付け変更の実施が他のセキュリティベンダよりも遅いため，このような結果になったのではないかと考えられる．

5.2.4　SRX-1500

SRX-1500 はマルウェアサイト判定数が 7261 件であり，これは Web Filtering の格付けによって Malicious Web Site と判定されたものがカウントされている．ジュニパーネットワークス 社の格付け判定サイト [12] で手動により確認することもできる．ログ件数が約 21 億件と 5 メーカの中で一番多くなっているが，これはセッション開始時，セッション終了時およびセキュリティイベントではないログも

表 2　各セキュリティ機器の結果まとめ

機種	実験期間	ログ総量	ログ件数	マルウェアサイト判定数
PA-3250	7/19 0900 - 7/20 2300	約 277GB	約 6 億 6624 万件	14366 件
CP-23800	7/26 1600 - 7/28 0400	約 13GB	約 1535 万件	284 件
FG-500E	8/15 0700 - 8/16 1900	約 211GB	約 3 億 5323 万件	77918 件
SRX-1500	8/20 0900 - 8/21 1900	約 589GB	約 21 億 2541 件	7261 件
SM-9600	(1)9/9 1700 - 9/11 0700	約 61GB	約 1 億 6186 万件	3455 件
	(2)7/30 0900 - 7/31 2100	約 44GB	約 1 億 1946 万件	1847 件
	(3)6/18 1600 - 6/20 0500	約 237GB	約 7 億 6145 万件	1910 件

出力されているためであると考えられる．検出のチューニングで減らすことが可能であると考えられる．

5.2.5 SM-9600

SM-9600 は実験を 3 回実施している．実験 (2) および (3) では，以前の OS である 6.2 系を用いて実験を実施した．表 2 からも分かるように，同一 OS であっても，実験の実施時期の違いによって，外部の脅威情報が変化するためログの出力傾向に変化が見られる．マルウェアサイト判定数が実験 (3) の 1910 から (2) の 1847 件と減少している．OS のアップグレードによって，(2) と比較してログ総量，ログ件数ともに若干増加している．また，マルウェア判定サイト数が 3455 件となっており，約 1.5 倍増加している．これらより OS のバージョンを変化させることによって，セキュリティ検知機能の変化が見られることが明らかとなった．

6. まとめ

これまでのネットワークセキュリティ機器の評価は，実際の環境からミラートラヒックを取得して機能を評価する，もしくはエミュレータを用いて評価するのどちらかであった．我々は，このどちらでもない実際に大学で保存しているパケットキャプチャデータを用いて，それを再現するソフトウェアを作成することで，実環境に影響を与えない公平なネットワークセキュリティ機器の評価環境を構築した．また様々なメーカの評価機を借り受けて評価することで，それらの違いを確認することができた．今後の課題として，ネットワークフォレンジックシステムにおけるパケットロスの削減および，パケット再現手法のさらなる検討が挙げられる．

謝辞　本研究を推進するにあたり評価用機器を提供して頂いたパロアルトネットワークス社様，フォーティネット社様，チェック・ポイント・ソフトウェア・テクノロジーズ社様，ジュニパーネットワークス社様，ソニックウォール社様に心より感謝致します．

参考文献

[1] Magic Quadrant for Enterprise Network Firewalls https://www.gartner.com/doc/reprints?id=1-45UW8EQ&ct=170711&st=sb
[2] NSS LABS https://www.nsslabs.com/
[3] 中村 豊, 佐藤 彰洋: 次世代ファイアーウォール機器の評価検証について, インターネットと運用技術シンポジウム 2016 論文集,2016,106-106 (2016-12-01)
[4] 中村 豊, 佐藤 彰洋, 福田 豊, 和田 数字郎: 九州工業大学における情報セキュリティ対策の取り組みについて, インターネットと運用技術シンポジウム 2017 論文集,2017,42-49 (2017-11-30)
[5] TCP Replay: pcap editing & replay tools for *NIX http://tcpreplay.synfin.net/
[6] Avalanche - Testing the security of app aware devices and networks - Spirent https://www.spirent.com/Products/Avalanche
[7] How to Configure Wire / Tap mode in SonicOS — SonicWall https://support.sonicwall.com/kb/sw8962
[8] Big Monitoring Fabric, http://www.bigswitch.com/sdn-products/sdn-products/big-monitoring-fabric/overview
[9] Wireshark Go Deep. https://www.wireshark.org/
[10] Palo Alto Networks URL filtering - Test A Site, https://urlfiltering.paloaltonetworks.com/query/
[11] FortiGuard Labs, https://fortiguard.com/learnmore#wf
[12] Juniper Test-a-Site Results, http://mtas.surfcontrol.com/mtas/Juniper-Results.php
[13] URL Categorization — Check Point Software Technologies, https://www.checkpoint.com/urlcat/main.htm
[14] SonicWALL Content-Filter Service, http://cfssupport.sonicwall.com/Support/servlet/CFSSupportServlet/viewRating