[ポスター発表] 研究報告

ネットワークセキュリティ機器の評価に関する考察

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

Practical considerations for evaluating network security devices

1. はじめに

多くの企業・組織においてセキュリティ対策が求められており，これは喫緊の課題となっている．しかしながら，セキュリティ製品は種類，機能共に数多く存在するが，それらの評価基準は明確ではない．そのため，セキュリティ担当者は何を指標としてこれらの機器の導入を決定すれば良いか，判断が難しい．そこで本稿では，様々なネットワークセキュリティ機器の評価機を試験運用し，実際の運用トラヒックを適用してそれらの機器がどの様な出力を出すのかについて検証を行った。

2. 評価機の分類と考察

大学では私企業とは異なり学生の私物の持ち込み PC を認めている，もしくは必携を義務付けている場合が多く，様々な種類のデバイスがキャンパスネットワークに接続される．このため学生が自宅で感染した持ち込み PC を学内で接続することで不審通信として検知される事が多く発生する．したがって，前提条件として，

(1) 大学内はすでに何らかのマルウェアに感染している端末が多数存在する
(2) (1) の理由により入口対策は効果が薄い
(3) C&C 通信や情報漏洩対策といった出口対策が重要

となる．以下ではこれらを考慮した上で，ネットワークセキュリティ機器の大まかな分類とそれらの評価軸について述べる．次世代ファイアーウォールについては過去に [1] で述べているが，それら以外にも様々な種類のセキュリティ機器が存在するため，それらについて分類・分析および結果の考察について以下で述べていく．

2.1 振る舞い検知装置

図 1 に 2014 年 11 月〜2017 年 4 月頃までの評価環境を示す．評価開始当初は予算的な問題もあり，既存のネットワーク機器で実施可能なミラートラヒックによる機器の評価を行った．図 1 に示す様にファイアーウォール通過後の

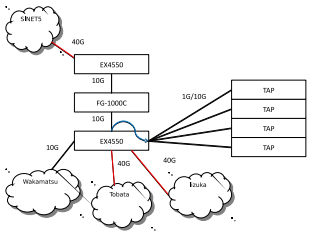

図 1 2014 年頃の評価環境

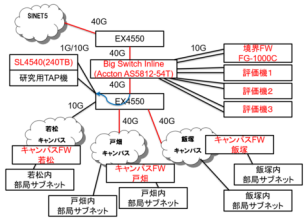

図 2 2018 年頃の評価環境

ミラーされたトラヒックを各評価機は検査する．以下に振る舞い検知系機器で必要と思われる項目について述べる．

- 検知後に担当部局へ連絡，対応を依頼するため，どのようなマルウェアに感染しているのか？どのような通信が発生していたのか？といったエビデンス情報が取得できるかどうか？
- 各メーカの対応状況を調査するために，マルウェアの検体を取得できるかどうか？
- C&C 通信の検出精度がどの程度正確か？

2014 年 11 月から 2015 年 11 月頃にかけて振る舞い検知と呼ばれる機器について評価を行った．最初に評価した FireEye 社の NX については 1 ヶ月の評価期間で C&C 通信が検知 53 件検出され実際にインシデントレスポンス対応を行った案件も発生した．また FireEye EX では悪意のある添付ファイルが 1 ヶ月で 400 件以上観測された．これも以降の境界ファイアーウォールによるアンチウィルス実施の契機となった．FireEye 以外に Lastline, Fortisandbox, Deep Discovery Inspector と評価を行った．各メーカ毎に検知ロジックの違いから出力の傾向に違いが見られた．

[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

2.2 次世代ファイアーウォール

以下に次世代ファイアーウォールにおける評価軸について述べる．

(1) IPS
外部からサーバの脆弱性に対する攻撃や brute force 攻撃の検出や内部から外部への攻撃トラヒックの検出
(2) アンチウィルス、脅威防御
外部から侵入してくるメールに添付するウィルスの除去、HTTP 通信における drive by download の検出，外部から学内へのウィルスの注入などの検出や除去
(3) Web filter
訪問サイトの分類や脅威の判定
(4) Application control
利用されているアプリケーションの分類や流量の表示
(5) C&C サーバへの通信検出
学内から学外への Botnet への通信や C&C サーバへの通信の検出
(6) マルウェア検体のダウンロード可否
AV/TP や Sandbox 機能を用いたマルウェア検体の取得が可能かどうか？
(7) Sandbox の動作
振る舞い検知機能が装備されているかどうか？
(8) 仮想ドメインの有無
(9) ダッシュボードの動作
ダッシュボードがスムーズに動作するかどうか？
(10) TAP, one arm, sniffer モードの可否
TAP モードと透過モードで機能に差異があるか？

2016 年 5 月頃〜2018 年 10 月頃にかけて次世代ファイアーウォール機器について評価を行った．Fortinet 社の FG-1000C，PaloAlto 社の PA-5060，CheckPoint 社の CP-15600，Juniper 社の SRX-1500，Sophs 社の XG-750 および SonicWall 社の SM-9200 である．この評価中にミラートラヒックでは十分な機能評価が出来ない機器が確認できた．各メーカ毎に仮想ドメインの有無であったり，アンチウィルス機能および web filtering のカテゴリ分類に明確な違いが見られた．一方で，アプリケーション制御については，あまり明確な違いは見られなかった．

2.3 インライン環境での評価

2017 年 4 月から 2018 年 7 月までのインライン環境による評価について述べる．図 2 にその頃のネットワーク構成図を示す．次世代ファイアーウォール機器で機能評価が出来なかった機器に対応するために，SDN スイッチ Big Monitoring Fabric[2] の導入した．大学の境界領域に SDN スイッチを導入することで，実環境を運用しながら，設定変更によりインライン環境に評価機を導入することが可能となった．この環境を用いて，Trendmicro 社の Tipping Point，Watchguard 社の M5600，Sophos 社の XG-750 rev2 などを評価した．また引き続きミラートラヒックを用いて McAfee 社の NSP9100，DarkTrace，damballa，PFU 社の iNetSec MP 2040，Vectra 社の X24，Cisco 社の FirePower 4120，Umbrella なども評価した．IPS 専用機である Tipping Point や NSP9100 はパケット毎に処理を行うため，次世代ファイアーウォールと異なりアンチウィルス等の機能は持っていない．しかしながら専用機であるため IPS に特化したハードウェアのためスループットは十分であると感じた．この頃から damballa や Umbrella といった DNS 通信に対する高度なセキュリティ機器が登場し，機械学習を用いた分析による検知ロジックがセキュリティ機器に入り始めた．iNetSec MP 2040 はフローの振る舞いを分析し各端末の状態を学習する事で異常検知を行う装置である．同様な装置として darktrace や vectra 社の X シリーズが挙げられる．

インライン環境での評価では，運用中のネットワークにインラインで装置を導入するため，機器の設定不備や機能不足により全学ネットワークを停止させる障害も発生した．この問題を解決するために，我々は過去に蓄積したパケットデータを再現するプログラムを作成し，ネットワークセキュリティ機器を独立した環境で評価することが可能な評価システムを構築した [3]．この評価環境を用いた評価では，PaloAlto 社の PA3250，CheckPoint 社の CP-238000，Juniper 社の SRX-1500，Fortinet 社の FG-500E，SonicWall 社の SM-9600，F5 社の BigIP-i5800，Cisco 社の Stealth Watch などの評価を行った．またこれとは別に akamai 社の DNS セキュリティを評価した．評価環境を用いた評価では，同一トラヒックを何度でも適用できる利点を生かして設定変更やチューニングを施すといった運用中では出来ない機器の調整が可能となった．

3. おわりに

本稿では，様々なネットワークセキュリティ機器の評価機を試験運用し，実際の運用トラヒックを適用してそれらの機器がどの様な出力を出すのかについて検証を行った。今後はエンドポイントやクラウド対策など，未実施のカテゴリもあるため引き続き評価を進めていく予定である．

謝辞 本研究開発は総務省 SCOPE(受付番号 192210001) の委託を受けたものです．

参考文献

[1] 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)
[2] Big Monitoring Fabric, 入手先 ⟨http://www.bigswitch.com/sdn-products/sdn-products/big-monitoring-fabric/overview⟩
[3] 中村 豊, 佐藤 彰洋, 福田 豊, 和田 数字郎: ネットワークセキュリティ機器の評価環境構築, インターネットと運用技術シンポジウム 2018 論文集, 2018, 70-76 (2018-11-29)