一般口演 | セキュリティとプライバシー保護
一般口演4
セキュリティとプライバシー保護
2019年11月22日(金) 09:00 ～ 11:00 H会場 (国際会議場 3階中会議室304)

[2-H-1-05] NetFlowデータを活用した院内通信の可視化と自動解析アラート機能検証によるセキュリティ対策評価

○田木 真和[1]、玉木 悠[2]、若田 好史[2]、廣瀬 隼[1]（1. 徳島大学大学院医歯薬学研究部　医療情報学分野, 2. 徳島大学病院　病院情報センター）

キーワード：NetFlow, security, automatic analysis alert

病院情報システムのセキュリティ確保のため，多くの医療機関でセキュリティ対策装置が導入されており，主にシグネチャ型のウイルス検知手法が用いられている．しかし未知のマルウェアの検知は困難であり，その課題対策として， NetFlowデータ等の内部ネットワークのトラフィックデータを解析することで潜在的な脅威を検知する方法が開発されてきているが，医療機関において NetFlowデータを活用した報告は渉猟されない．本研究の目的は，当院内部ネットワーク対策システムの NetFlowデータの解析による，院内通信の可視化と潜在的脅威を機械学習で自動的に検知できるセキュリティアラート機能の有用性を検討することである．
2019年1月に導入した内部ネットワーク対策システムにおいて，病院情報システムネットワーク内の NetFlowデータを収集しトラフィック情報に応じてアラート表示する機能を活用し，3月21日～27日（期間1）と5月21日～27日（期間2）のアラート件数と5月27日の院内通信ログを調査した．
アラート件数は期間1が1220件，期間2が392件だった．院内から院外への通信ログは1時間に1320件抽出され，その通信ログの一部は院外への不適切な通信設定がある端末38台から出力されていた．
アラート機能では，病理や CT画像の閲覧が大容量データダウンロードとして過剰検知されることが期間1で判明したため，画像閲覧を過剰検知しない設定に変更した期間2ではアラート件数が減少した．また，院内通信の可視化により，院外への通信が高頻度で行われていることが明らかとなったが，その通信はファイアウォールで確実に遮断されていた． NetFlowデータの有効活用が病院情報システムにおいてもセキュリティ対策として有用であることが確認できたが，通信可視化の効率的な運用とアラート機能チューニングが今後さらに必要である．

NetFlow データ自動解析機能を活用した院内通信の可視化とアラート（セキュリティ対策としての有用性検証）

田木 真和[*1]、玉木 悠[*2]、若田 好史[*2]、廣瀬 隼[*1]
*1 徳島大学大学院医歯薬学研究部医療情報学分野、*2 徳島大学病院病院情報センター

Visualization of the hospital network flow using the security alert function by automatic analysis of NetFlow data (Evaluation of the usefulness of security system)

Tagi Masato[*1], Tamaki Yu[*2], Wakata Yoshifumi[*2], Hirose Jun[*1]
*1 Department of Medical Informatics, Institute of Biomedical Sciences, Tokushima University Graduate School,
*2 Medical IT Center, Tokushima University Hospital

It is still difficult to detect unknown malware although medical institutes have installed security equipment using signature-type virus detection methods. To detect potential threats, analyzing traffic data such as NetFlow data in the internal network has been developed in recent years. The purpose of this study is to analyze NetFlow data for visualizing the hospital network flow and to evaluate the usefulness the security alert function that automatically analyzing the NetFlow data for detecting potential threats. The number of alerts and the hospital network flow were investigated in two periods from March 21 to 27 (Period 1) and May 22 to 28 (Period 2). The number of alerts was 1220 in period 1 and 392 in period 2. The network flow out of the hospital was detected 1320 per hour on May 28. Thirty-eight devices were improperly connected to a network outside the hospital. After adjusting the settings to avoid over-detection of pathological and CT images as large data downloads, the number of alerts decreased in period 2. By analyzing the NetFlow data, visualization of the hospital network flow it was performed, it was indicated that the data frequently tried to connect outside the hospital. However, these communications were blocked by the firewall, and the security alert function was shown to works reliably for detecting potential threats.

Keywords: NetFlow, security, automatic analysis alert

1. 背景

医療機関では極めて機微な患者情報を大量に扱うため、病院情報システムのセキュリティを確保することは重要な課題である。病院情報システムのネットワーク管理者は様々なセキュリティ装置を導入して、ネットワークを安全に利用できるようにしており、多くの施設では外部からの脅威侵入の対策として、ゲートウェイに設置する不正侵入防止システム（Intrusion Prevention System : IPS）の導入やクライアント端末におけるエンドポイント対策などが実施されている。一方、それらのセキュリティ装置の多くはシグネチャ型の検知手法が用いられており、未知のマルウェアの検知は困難である。また、ネットワークの出入り口に注力した装置が多いため、施設内部への侵入が成功した脅威については把握できない恐れがある。これらの問題点の対策として、施設内部ネットワークのトラフィックデータを可視化し、その内容を解析することで潜在的な脅威を検知する方法が開発されてきている [1,2]。その中にパケットキャプチャによりパケットの中身を解析する手法があり、正常通信との差異を検出することで悪性通信の有無が判定可能か検証されている [3]。ただし、この手法は解析に多くの時間がかかることがボトルネックとなっている [4]。そこで近年、パケットからトラフィック情報に関係しない部分等を除いた NetFlow データを活用し、機械学習を連携し脅威を検知する方法が検討されている [5]。NetFlow データはパケットキャプチャより少ないデータ容量だが、全ての通信の追跡が可能となるため、トラフィックデータ解析に適している。情報処理の分野では、すでにその有用性が報告されているが [5]、我々の渉猟した範囲では、医療機関において NetFlow データを活用したセキュリティ対策の評価報告はない。

2. 目的

NetFlow データ自動解析によるセキュリティアラート機能のセキュリティ対策における有用性を評価することが本研究の目的である。まず、NetFlow データから解析通知されたセキュリティアラートのセキュリティイベント抽出精度について検証し、さらにアラートに関連する NetFlow データを分析して外部への不正通信を調査した。

3. 方法

徳島大学病院では、2019 年 1 月の病院情報システムの更新に合わせて、病院情報システムネットワーク内の NetFlow データを収集しトラフィック情報に応じて自動解析したセキュリティアラートを表示できる内部ネットワーク対策システムを導入した。

3.1 セキュリティアラート機能

NetFlow データは、NetFlow 対応ネットワーク機器で生成され、内部ネットワーク対策システムのサーバに自動的に収集される（図 1）。セキュリティアラート機能は、収集した NetFlow データを自動解析しセキュリティイベントとして潜在的な脅威

を表示できる。

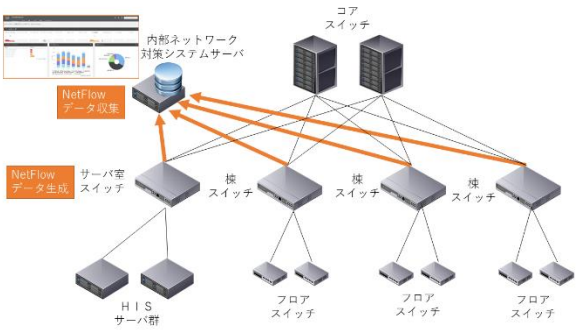

図 1　NetFlow データの生成と収集の仕組み

セキュリティアラート機能画面は、図 2 に示すように上部にアラートカテゴリ別のアラート情報、左中央部にアラート通知が多いホスト情報、中央部に 1 週間のセキュリティイベント数の棒グラフ、右中央部に当日のセキュリティイベント数の円グラフ、左下部に 1 秒あたりのフロー数の折れ線グラフ、右下部に使用されているアプリケーションの種類が表示される。アラートとして判断されるデータ量の閾値は、直近の 7 日間の日ごとの最大値と過去 3 週間の同じ曜日の最大値の平均値からシステムによって自動的に計算され設定される。

図 2　セキュリティアラート機能画面

表 1　アラートカテゴリ

アラート名	検知内容
Concern Index	疑わしいトラフィックを生成
Target Index	疑わしい振る舞いをする トラフィックの標的
Recon	偵察行為
C&C	C&C サーバとの通信
Exploitation	マルウェアの拡散等の攻撃
DDoS Source	DDoS 攻撃の送信元
DDos Target	DDoS 攻撃の標的
Data Hoarding	データの大量ダウンロード、 内部情報漏えい行動
Exfiltration	外部へのデータ漏えい
Policy Violation	ポリシー違反
Anomaly	その他の動作異常

セキュリティアラートは、High Traffic（異常に大量のデータ送受信がある）、ICMP Flood（Ping 等の ICMP パケットを大量に送信することで機能不全に陥れたり、偵察行為を行ったりしている）、Suspect Data Hoarding（他の内部のサーバ機器やクライアント端末からダウンロードするデータ量が閾値を超えている）など、94 種類のセキュリティイベントとして表示され、それらをまとめると 11 種類のアラートカテゴリに分類される（表 1）。

3 月 21 日～27 日（期間 1）と 5 月 22 日～28 日（期間 2）において、セキュリティアラート内容の分析を行った。期間 1 では、内部ネットワーク対策システムの標準設定でアラートを抽出した。期間 2 では、期間 1 で発生したアラートの中で誤検知と判断したアラートが発生しないようにチューニングを行い、その設定を反映した状態でアラートを抽出した。

3.2 NetFlow データによる院内通信の可視化

過去の NetFlow データから IP アドレスや時間帯などを指定することで、ホスト毎の通信状況を表示することができる。この機能を利用し院内通信を可視化することで、不正な通信がないかどうか確認することができる。

5 月 28 日のセキュリティアラートに関連する NetFlow データについて、その院内通信を可視化し、通信状況を確認した。本院のセキュリティポリシーの一つである「保守メンテナンスのためのリモートメンテナンスを行う場合を除き、病院情報システムネットワークでの外部接続の使用は禁止する。」が守られていない通信を不正な通信として、その通信の有無を調査した。

4. 結果

内部ネットワーク対策システムにより、定常的に NetFlow データを自動生成・取得することが可能となった。3 月 26 日午前 8 時から 3 月 27 日午前 7 時までの NetFlow データ数は、経時的に変化し（図 3）、1 時間毎に 2 分間のデータを抽出すると合計 16,109,640 件で、1 日の平均値は 5,594 件/秒であった。

図 3　NetFlow データグラフ

4.1 セキュリティアラートの分析

期間 1 のセキュリティイベント別アラート件数を抽出したグラフを図 4 に示す。アラート件数の総数は 1,220 件となり、High Traffic のイベントが最も多く、通信量が多いことが脅威として通知された。このイベントの詳細を確認すると、その多くは病院情報システムのクライアント端末から病理画像や CT 画像が保管されている統合ストレージシステムへの通信であった。クライアント端末の利用者が日々異なる現場では、画像を閲覧する時と閲覧しない時があり、画像が閲覧される端末

が固定されない。これらの画像は大容量データであり、普段、画像があまり閲覧されない端末で多くの画像が閲覧されると、その通信量は過去の通信量の平均値より多くなる。このことから、アラートとして通知されたと考え、このアラートは過剰検知であると判断した。

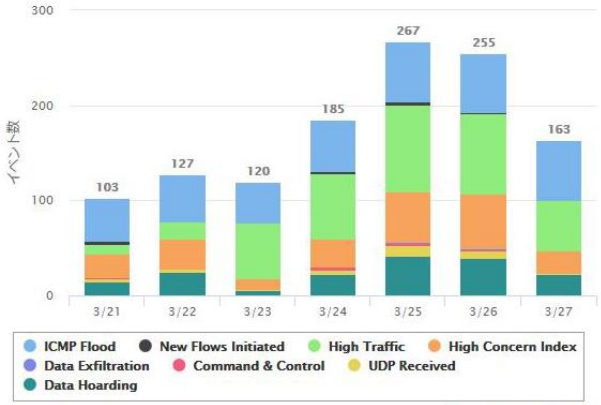

図 4　セキュリティイベント別アラート数（期間 1）

期間 1 の結果より、誤検知と判断されたクライアント端末から統合ストレージシステムへの大容量通信は検知しないようにチューニングを行い、期間 2 においてセキュリティイベント別アラート件数を抽出した。その結果、アラート件数の総数は 392 件と減少した（図 5）。最も多かったのは ICMP Flood のイベントで、ICMP パケット通信が多数あることが偵察行為として通知された。特定のサーバ機器では死活監視ツールが出力するネットワークゲートウェイ機器との間の ICMP パケットが多数あり、それがアラートとして検知されたことから、このアラートも過剰検知であると判断した。

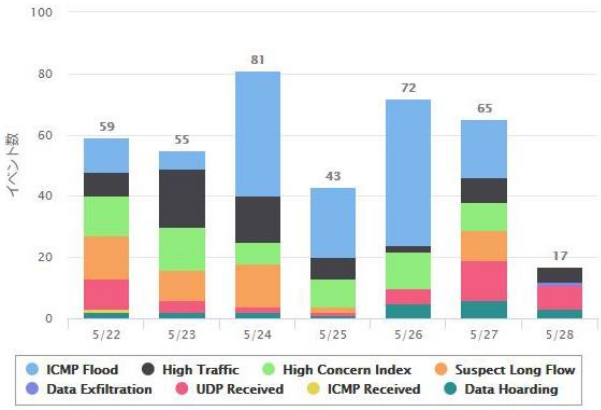

図 5　セキュリティイベント別アラート数（期間 2）

4.2 NetFlow データの分析

外部への不正通信を調査するため、5 月 28 日に発生したセキュリティアラートの中で、Data Exfiltration（外部へのデータ漏えい）に関連する NetFlow データを分析した。その結果、院外へのデータ漏えいはなかったが、院内から院外への通信ログが 1 時間に 1,320 件抽出され、その通信ログの一部は院外の DNS サーバへの通信設定がある端末 38 台から出力された。しかしながら、院外から院内への通信は 0 パケットで（図 6）、院内への通信は遮断されていることが確認された。

図 6　院内通信の可視化

5. 考察

NetFlow データは、パケットキャプチャより少ないデータ容量ではあるが、1 秒間の平均が 5,594 件のデータとなり、そのすべてのデータを確認し分析することは不可能である。しかし、内部ネットワーク対策システムを導入し、セキュリティアラートとして脅威になる可能性のあるイベントを自動抽出できるようになり、そのアラートに関連する NetFlow データから院内通信を可視化することができた。

NetFlow データを自動解析し、セキュリティアラート機能として活用した場合、医療機関では、病理や CT 画像の閲覧が大容量データ通信として検知されたり、サーバ機器の死活監視ツールの ICMP パケットが多数のデータ通信として検知されたりした。しかし、これらは正常通信なので過剰検知と判断した。このことより、アラート通知設定は、病院情報システムクライアント端末と病理画像や CT 画像を保管する統合ストレージシステムの通信をアラートとして通知しないようにしたり、アラートとして判断されるデータ数の閾値を変更したりするなど、さらにチューニングが必要であることがわかった。

また、Data Exfiltration に関連する NetFlow データの分析により、院外への通信が高頻度で行われていることが明らかとなった。セキュリティポリシーで運用のルールを通知しておき、その通りに端末の設定をしたと思っていても実際の通信を確認すると、ポリシー違反の通信が発見されるので、セキュリティを確保するためには院内通信を可視化し定期的に確認する必要がある。今回は幸いにも、その通信はファイアウォールで確実に遮断されおり、既存のセキュリティ対策が有用であることが示された。院外から院内への通信遮断記録は、ファイアウォールからも取得できるが、セキュリティアラートで問題点に気づき、それに関連するデータをすぐに分析できることがこの仕組みの有用な点である。

セキュリティアラートに関連する NetFlow データから院内通信の可視化を行い、セキュリティ対策として活用することができた。医療機関においても NetFlow データ自動解析によるセキュリティアラート機能のセキュリティ対策が有用であることがわかった。今後、新しくネットワークに接続する機器を導入する際に院内通信を可視化し、その機器の通信状態を確認して、安全に機器を導入するために活用できると考えられる。

参考文献

1）高倉弘喜．悪性トラフィック挙動解析による未知のサイバー攻撃検知．日本信頼性学会誌　信頼性 37(3), 126-133, 2015.
2）佐藤信，杉　暁彦，林直樹，磯部義明，佐々木良一．マルウェアによるネットワーク内の挙動を利用した標的型攻撃における感染経路検知ツールの開発と評価．情報処理学会論文誌 58(2),

366-374, 2017.
3) 田中恭之，畑田充弘，稲積孝紀．パケットキャプチャからみた悪性通信に関する特徴の考察.コンピュータセキュリティシンポジウム 2013 論文集 2013(4), 118-124, 2013
4) 水越大貴，棟朝雅晴. Hadoop を用いた遺伝的アルゴリズムによる DDoS 攻撃防止システムの検討．研究報告数理モデル化と問題解決（MPS） 2014-MPS-101(1), 1-6, 2014.
5) 鈴木彦文，浅川圭史，永井一弥，林裕裕平，工藤伊知郎．NetFlow トラフィックデータの取得と解析に関する共同研究．学術情報処理研究 22(1), 3-11, 2018.