[ポスター発表] 研究報告

IDS・SDN連携型ファイアウォールシステムにおける遮断動作の高速化

桂 祐成[1] 児玉 伊太郎[1] Pranpariya Sakarin[2] 山井 成良[1,a)] 君山 博之[3] Vasaka Visoottiviseth[2]

Quick Blocking Operation of Firewall System Cooperating with IDS and SDN

1. はじめに

近年，インターネットの普及に伴いサイバー攻撃が社会問題となっており，その攻撃からICTリソースを守るためのファイアウォールシステムは必要不可欠となっている．ファイアウォールシステムの構成法としてIDS（Intrusion Detection System）とSDN（Software Defined Network）システムとを併用する方法（以下，IDS・SDN連携型ファイアウォールシステムと呼ぶ）が提案されている[1]．このIDS・SDN連携型ファイアウォールシステムは，一般的な一体型のファイアウォールシステムと異なり，攻撃を検知するIDSとパケットの廃棄や経路を変更するSDNシステムとを分離して構成することにより，廃棄対象とする攻撃や回線速度，攻撃パケットの処理方法（廃棄，リルート）など，要求に応じて柔軟にシステムを構成できるメリットがある．

このIDS・SDN連携型ファイアウォールシステムに対してSDNとして広く利用されているOpenFlowシステムを適用する場合，OpenFlowコントローラを介してHTTPベースのREST（Representational State Transfer）メッセージを使ってIDSから制御する方法が一般的である．しかし，RESTを使用する場合，開発が容易である反面TCPのコネクション確立がオーバヘッドとなるため，検出からSDNへ反映させるまで時間がかかるという問題があり，我々は，この処理時間を短縮する方式の検討を行っている．

本報告では，多くのIDSが備えているsyslog，SNMP trapから特殊なAlertメッセージを生成し，それをSDNへ入力することによってSDNを制御する方式を提案する．さらに，提案方式によりREST APIを経由するよりも短縮できることを確認した評価実験結果についても報告する．

1 東京農工大学 Tokyo University of Agriculture and Technology
2 Mahidol University, Thailand
3 大同大学 Daido University
a) nyamai@cc.tuat.ac.jp

2. 提案方式

我々が提案するIDS・SDN連携型ファイアウォールシステムの概要を以下に示す．

(1) 外部から送られてくるパケットのミラーリングを行いIDSに転送する．
(2) IDSは，受信したパケットを処理対象と判定した場合，IDSが出力する標準のAlertメッセージ(syslog，SNMP trap等)をSDNスイッチに送信する．
(3) SDNスイッチは受信したAlertメッセージをPacket-Inなどの方法でSDNコントローラに転送する．
(4) SDNコントローラは受信したAlertメッセージを解析し，制御対象となるトラフィックを特定する．
(5) SDNコントローラはSDNスイッチに対して 制御対象となるトラフィックの遮断やハニーポットなどに転送するための設定を行う．

3. 実装

提案手法の実現性を確認するため，下記のプロトタイプ実装を行った．実装したプロトタイプシステムの構成を**図1**に示す．

攻撃検知を行うIDSとしてSnortを採用し，IDSがシグネチャと一致する通信を検知した際にSDNコントローラへAlertメッセージを送信する方法として，(1)rsyslogによりIDSが出力するsyslogをAlertメッセージとして送信する方式および比較のため(2)ログ監視ツールであるSwatchを用い，Alertメッセージを生成送信するプログラムを起動し，Alertメッセージを送信する方式の2方式を実装した．なお，(2)のAlertメッセージを生成送信するプログラムはソケットAPIを用いて我々が実装したものである．

IDSによって検知された攻撃パケットを処理させるSDNシステムとして，OpenFlowソフトウェアスイッチとOpenFlowコントローラを採用した．具体的には，OpenFlowソ

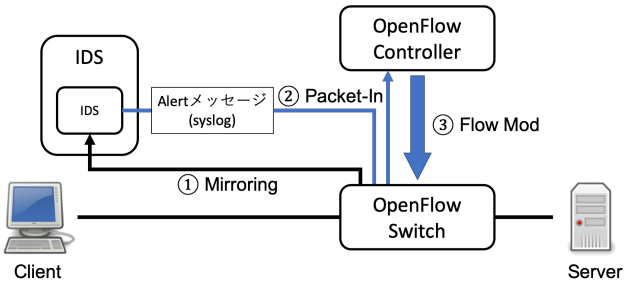

図 1　実装したプロトタイプシステムの構成図

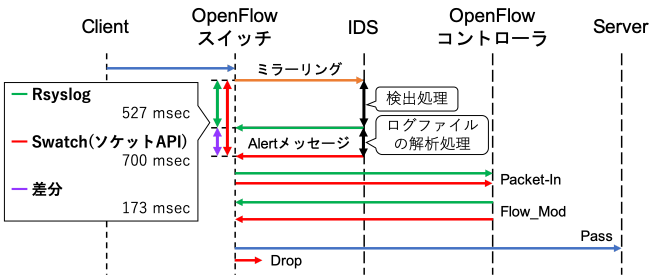

図 2　提案手法における Alert 検出までのオーバーヘッド

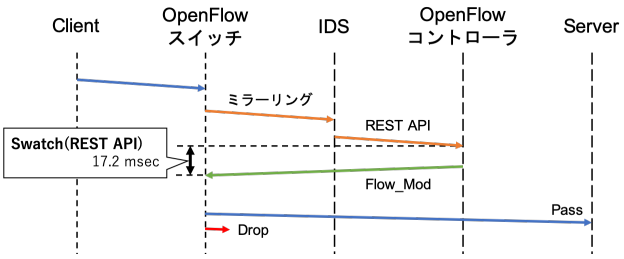

図 3　既存手法での遮断設定フローと設定時間

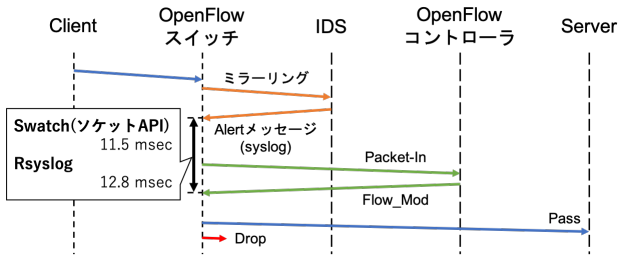

図 4　提案手法での遮断設定フローと設定時間

フトウェアスイッチとして Open vSwitch を，OpenFlow コントローラとして Ryu を採用している．そして，IDS から送信された Alert メッセージを OpenFlow コントローラに Packet-In させるためのフローテーブルを作成するとともに，受信した Alert メッセージを解析してパケットの廃棄設定を行うフローエントリーをフローテーブルに追加するプログラムを OpenFlow コントローラ上に実装した．

4. 評価

提案手法の効果を実証するため，Raspberry Pi を使って前述したプロトタイプを動作させ評価実験を行なった．まず最初に，Alert メッセージが生成されるまでの処理時間を評価するために，rsyslog を用いた場合と Swatch を用いた場合の処理時間の評価を行った．この評価では，**図 2** に示すように，OpenFlow スイッチで攻撃パケットがミラーリングされてから，IDS にパケットが受信されて Alert メッセージが送信され，OpenFlow スイッチに戻ってくるまでの時間を計測し，評価を行った．この評価実験の結果，rsyslog を用いた場合，Swatch を使用した場合に比べて 173msec 処理時間が短くなることが確認できた．

次に，IDS の攻撃検知を契機に生成された Alert メッセージが，OpenFlow スイッチに受信されてから，フローエントリーが追加されるまでの時間を処理時間として計測した．既存手法との比較のために Swatch により Alert メッセージを生成するプログラムを動かす代わりに，REST メッセージを生成するプログラムを動かし，REST API により Ryu を介してフローエントリーを追加する方式も実装し，フローエントリーが追加されるまでの時間もあわせて実測した．**図 3** に REST API を用いた方法の処理シーケンスと処理時間測定箇所を示し，**図 4** に提案手法の処理シーケンスと処理時間測定箇所を示す．図 3 と図 4 の結果から，Swatch とソケット API を用いて Alert メッセージを送信し，フローエントリの追加処理を行った場合，既存の手法である REST API を用いてフローエントリの追加処理を行うよりも 5.7msec の処理時間の短縮が可能であり，また rsyslog を用いて Alert メッセージを送信した場合は，4.4msec の短縮が可能であることが確認できた．

5. まとめ

本報告では，IDS・SDN 連携型ファイアウォールシステムにおいて IDS が検出したアラートに基づき不審な通信の遮断処理を高速に行うため，REST メッセージを使わずに，ログ監視ツールや rsyslog など IDS が標準的に備えている仕組みを利用して，Alert メッセージを生成し，Packet In により，SDN コントローラにアラートを通知する方法を提案した．今後，文献 [2] のようなリアルタイム性の高いファイアウォールシステムへ提案手法を導入し，その有効性を検証していく予定である．

参考文献

[1] Paul Zanna, Benjamin O'Neill, Pj Radcliffe, Sepehr Hosseini and MD. Salman Ul Hoque: "Adaptive Threat Management Through the Integration of IDS Into Software Defined Networks", *Proceedings of 2014 International Conference and Workshop on the Network of the Future (NOF2014)*, pp.13–17, December 2014.

[2] 桂祐成，君山博之，堤智昭，米崎直樹，丸山充: "ソフトウェアスイッチを使ったリアルタイム総当たり攻撃検出遮断システムの提案"，電子情報通信学会技術研究報告，NS2018-272, pp.461–464，2019 年 3 月．