1Z-8

標的型攻撃に対する OpenFlowを用いたマルウェア通信検知・対応手法の提案

中川 直人† 佐々木 良一† 勅使河原 可海†

東京電機大学†

1 はじめに

近年，標的型攻撃の被害が増加して問題となっている．標的型攻撃は，初期侵入，攻撃基盤構築，内部侵入・調査，目的遂行の4フェーズに分類される．企業は，様々な標的型攻撃の対策を施しているが，従来の対策では不十分であり，新しい対策が求められている．そこで昨今，標的型攻撃等の新しいタイプの攻撃対策として出口対策が注目を集めている．

出口対策は，マルウェア感染した場合でも可能な限り情報奪取を防ぐことを目的としており，従来のマルウェア感染等を防ぐための入口対策とは別の視点の対策である．出口対策には，システム稼働前に行っておくべき事前対策として，アクセス制限やトラフィック監視，重要サーバの隔離などがあり，事前対策を行うことでネットワーク内部に侵入されたとしても外部攻撃者との通信を遮断することができる．事前対策に加えて，攻撃された場合はネットワークログを解析して感染ノードを特定，所属LANから隔離，原因の特定等の事後対応が必要になる．現在，事後対応は人手による作業が主流のため，ヒューマンエラーや時間等を含めたコストが増加するという問題がある．また，マルウェア感染ノードの早期発見や隔離に時間がかかり，重要情報の流出を食い止めることができない問題も挙げられる．この問題を解決するために，システムによる感染後の応急措置が必要になる．

本稿では，仮想ネットワーク技術であるOpenFlowを用いてネットワーク監視と制御の一元化を行い，標的型攻撃の検知と対応を自動で行うシステムを提案する．

2 背景

2.1 標的型攻撃における通信の特徴

前章で述べた通り，標的型攻撃は主に4つのフェーズから成っている．可能な限り目的遂行フェーズでの情報流出を阻止する出口対策を考案するために，攻撃基盤構築と内部侵入・調査の2つのフェーズに着目して，標的型攻撃に関する報告書[1][2]をもとにマルウェア通信の特徴を調査した．

調査の結果，主にマルウェア通信はC&Cサーバとのバックドア通信とシステム内感染拡散等の2種類に分類することができた．前者は主に攻撃基盤構築フェーズでの通信であり，後者は内部侵入・調査フェーズの通信である．攻撃基盤構築フェーズでは，マルウェアはまずC&Cサーバとの通信確立を試みる．また，成功後の内部侵入・調査フェーズでは，マルウェアはネットワーク調査や他ノードへの侵入，重要サーバへのアクセス等を試みる．これらマルウェアの挙動を攻撃事象とし，攻撃事象における通信の挙動を通信事象として細分化したものを表1に示す．本稿では，通信事象を検出し，その組み合わせからマルウェア感染の判断を行う．

表1． マルウェアの攻撃事象および通信事象

フェーズ	攻撃事象	通信事象
基盤構築	共通	業務時間外通信
		未使用ポート通信
		未使用プロトコル通信
	C&Cサーバとの通信	ブラックリストのC&Cサーバとの通信
		長時間のKeep-Alive通信
		長時間のSSH通信
		プロキシを経由しない通信
		許可していないリモートアクセス
内部侵入・調査	共通	業務時間外通信
		未使用ポート通信
		未使用プロトコル通信
	内部ネットワーク調査	ポートスキャン
		ファイル共有
	他ノードへの侵入	他ノードへのアクセス
	重要サーバへのアクセス	管理ノードを経由しない通信

2.2 OpenFlowについて

OpenFlowは，レイヤ2スイッチおよびレイヤ3スイッチの機能をカバーする技術として，2008年に登場したネットワーク制御プロトコルである．2014年1月段階でのバージョンは1.3.2であり，現在も標準化が進められている．

OpenFlowは，図1の通りOpenFlowコントローラ(以下，OFC)，OpenFlowスイッチ(以下，OFS)から構成される．従来のスイッチでは同筐体に実装されていたパケットの転送機能を担うデータプレーンと経路制御機能を担うコントロールプレーンを分離して，コントロールプレーンをOpenFlowコントローラとして外出した集中制御型アーキテクチャとなっている．経路制御をパケットヘッダ情報であるMACアドレス，IPアドレス，ポート番号，VLANタグなどをベースにして行う．リアルタイムにネットワーク監視および制御を行うことで，標的型攻撃等におけるマルウェア感染の検知と同時に，ノードの隔離等の応急措置を行うことができる．

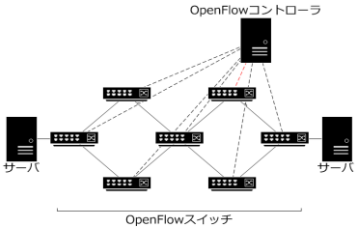

図1． OpenFlowネットワーク

Proposal of the Methods for Detecting and Solving Malware Communication by Using OpenFlow to APT
†Naoto Nakagawa, Ryoichi Sasaki, Yoshimi Teshigawara
†Tokyo Denki University

3　提案方式

3.1 提案システムの概要

本稿では，OpenFlowを用いて標的型攻撃の特徴を持った通信を検出するとともに，動的アクセス制御を行うシステムを提案する．標的型攻撃の特徴を持つ通信はOpenFlowとSnortを連携させて検出を行う．検出後，その脅威度に応じて動的ネットワーク制御による対応を図る．システムの開発環境を表2に示す．

表２．　開発環境

OS	Ubuntu12.04
Trema バージョン	0.4.5
OpenvSwitch バージョン	2.0.90
Snort バージョン	2.9.5.6
MySQL バージョン	5.6.15

提案システムは，主にマルウェアの通信を検出するシステムと検出後に動的対応するシステムの2つで構成されており，どちらもOFC内に実装される．システムの全体図を図2に示す．この構成は，安藤らのシステムを参考にしている[3].

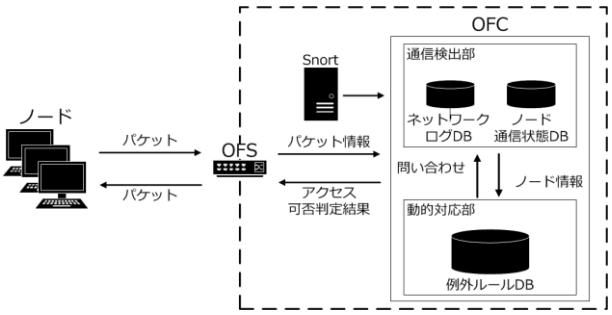

図２．　システム構成図

3.2 OpenFlowコントローラ

提案システムの中核となるOFCは，通信検出部と動的対応部から成っている．

通信検出部システムは，マルウェアの特徴的な通信を検出する．ネットワークログDBにはネットワーク全体のログを蓄積していき，ノード通信状態DBには各ノードの通信事象に重み付けを行い，加算形式で記録していく．重み付けは表3に示す通り，脅威度の低い順に1，2，3とした．

表３．　通信事象の重み付け

フェーズ	攻撃事象	通信事象	重み付け	動的対応
基盤構築	共通	業務時間外通信	1	
		未使用ポート通信	1	
		未使用プロトコル通信	1	
	C&Cサーバとの通信	ブラックリストのC&Cサーバとの通信	3	全アクセスの禁止
		長時間のKeep-Alive通信	1	
		長時間のSSH通信	1	
		プロキシを経由しない通信	2	強制経路設定
		許可していないリモートアクセス	2	
内部侵入・調査	共通	業務時間外通信	1	
		未使用ポート通信	1	
		未使用プロトコル通信	1	
	内部ネットワーク調査	ポートスキャン	2	
		ファイル共有	1	
	他ノードへの侵入	他ノードへのアクセス	2	
	重要サーバへのアクセス	管理ノードを経由しない通信	3	強制経路設定

動的対応部システムは，例外ルールDBとノード通信状態DBに応じた動的対応を行う．通信事象単体検出時の動的対応を表3に，重み付け加算による動的対応を表4に示す．例外ルールDBには許可する通信を記述していく．

表４．　重み付け加算による動的対応

重み付け加算	動的対応
1～2	管理者に通知
3～4	管理者に通知，一時的にネットワークから隔離
5	管理者に警告，ノードの全通信を禁止

3.3 システム動作

提案システムの動作の流れは以下の通りである．

①OFCはOFSからパケットを受信，継続的にネットワークログを蓄積すると同時にマルウェアの特徴を持つ通信を検出，ノード通信状態DBに記録する．

②各ノードの重み付け加算の変更に応じて，例外ルールDBから，許可された通信であるか確認する．

③動的対応を行うために，OFSに対して制御情報を送信する．また，管理者へデータを送信する．

重み付け加算3～4の動的対応によりネットワークから隔離されたノードは，一定時間マルウェア通信が検出されなかった場合に復帰する．重み付け加算5の動的対応により全通信を禁止されたノードは，管理者の許諾により復帰する．

3.4 開発状況

開発前段階において，検体におけるマルウェアの特徴を持つ通信を確認した．現在は，OpenFlowを用いてマルウェアの特徴を持つ通信を検知して重み付けを行うシステムを構築している．現状の動的対応は，アクセス制御のみの実装となっているため，その他の動的対応の実装も進めている．

4　おわりに

調査の結果，標的型攻撃等のサイバー攻撃の被害を防ぐために，早急な感染ノードの特定や隔離が必要なことがわかった．OpenFlowを活用することで，リアルタイムにネットワーク監視および制御ができるため，問題解決に有効であると考えた．そこで本稿では，OpenFlowを用いてマルウェア通信の検出を行い，同時に動的アクセス制御により標的型攻撃の被害を防ぐシステムを提案した．

今後は，現在開発中の提案システムを構築し，実際の標的型攻撃における有効性を評価する予定である．

5　参考文献

[1]　『標的型メール攻撃』対策に向けたシステム設計ガイド, http://www.ipa.go.jp/security/vuln/newattack.html

[2]　Detecting APT Activity with Network Traffic Analysis, http://www.trendmicro.com/us/security-intelligence/research-and-analysis/reports-white-papers/index.html

[3]　安藤玲未他，”踏み台攻撃防止のための通信状態ベースアクセス制御”，コンピュータセキュリティシンポジウム2013 論文集，pp.1018-1025，2013年