情報処理学会論文誌 Vol.56 No.9 1706–1715 (Sep. 2015)

推薦論文

マルウェア調査のためのSDNによるネットワーク切替え手法

来間 一郎[1,a)] 甲斐 賢[1] 木城 武康[2] 磯部 義明[1]

受付日 2014年12月5日, 採録日 2015年6月5日

概要：マルウェア感染への対処には，感染ホストをLANから隔離することと，マルウェア活動による被害状況を調査することが必要となる．しかし，隔離されたことを検知し挙動を変化させるマルウェアに対しては，隔離と被害状況の調査を両立させるのが難しいという問題がある．本稿では，マルウェア通信タイミングの予測と，SDN（Software Defined Networking）技術を活用したタイミング調整可能な切替えからなる，マルウェアに検知されずに感染ホストを隔離するネットワーク切替え手法を提案した．さらに，マルウェアの通信ログを用いてタイミング予測の精度評価を行い，偽陽性・偽陰性確率の観点から提案手法の有効性を明らかにした．

キーワード：マルウェア，隔離，SDN

Method for Network Switching with SDN to Support Investigation of Malware

Ichiro Kurima[1,a)] Satoshi Kai[1] Takeyasu Kishiro[2] Yoshiaki Isobe[1]

Received: December 5, 2014, Accepted: June 5, 2015

Abstract: On security incident response, isolation of malware infected host and investigation of the damage situation of malware activity are needed. However, it is difficult to carry out them at the same time, when the malware has function to detect change of network state and change activity. In this paper, we propose the method to isolate malware infected host avoiding being detected by malware with prediction of malware's activity and safe network switching using SDN (Software Defined Networking). We evaluated false-positive rate and false-negative rate of our prediction method with communication log of malware and found it useful in proposed situation.

Keywords: malware, isolation, SDN

1. はじめに

1.1 インシデント対処とマルウェアの動向

近年，標的型攻撃に代表されるサイバー攻撃の高度化・組織化が進んでいる．これらの攻撃では標的ごとにカスタマイズされたマルウェアが利用されるため，従来のウイルス対策ソフトによる感染防止には限界がある．そのため，マルウェアの侵入を前提とした，マルウェアによるインシデントに対処する重要性が増している．

一般的なインシデントへの対処で必要とされる対応作業には以下のステップがある [1]．

1. インシデントの封じ込め
2. インシデントの詳細調査

マルウェアによるインシデントでは，対応作業1は，マルウェア感染が疑われるホスト（被疑ホスト）をLANから切り離すことにあたる．マルウェアがLAN上の他のホストやインターネットに対して，攻撃や感染拡大を目的とした悪意ある通信を行うことを防ぐことが主な目的である．

対応作業2は，マルウェア検体やその挙動（ファイルア

[1] 株式会社日立製作所
Hitachi Ltd., Yokohama, Kanagawa 244–0817, Japan
[2] 株式会社日立システムズ
Hitachi Systems, Ltd., Shinagawa, Tokyo 141–8672, Japan
[a)] ichiro.kurima.ep@hitachi.com

本論文の内容は2014年7月のCSEC66研究発表会にて報告され，同研究会主査により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

クセス，レジストリアクセス，通信等）の情報収集に相当する．この目的は，マルウェアの駆除，マルウェア活動による影響の特定，法的措置に備えた証拠保全等である．通常，この作業はセキュリティ専門家で構成されたインシデントレスポンスチーム（IRT: Incident Response Team）により行われる．

一方で，近年のマルウェアには，置かれた環境によって挙動を変更し活動を隠蔽することで，これらの IRT の作業を阻害するものがある．マルウェア検体の複数環境での挙動を比較する実験では，Lindorfer ら [2] によると 1,686 検体中 431 検体で，Kirat ら [3] によると 110,005 検体中 5,835 検体で挙動の変化が見られた．このような，環境要因により挙動を変更するマルウェアは，環境変化を検知する情報により，ホスト情報検知型と，ネットワーク情報検知型の 2 つに分けられる．

1) ホスト情報検知型マルウェア

“Jerry.c” は，自身が活動している環境が仮想環境上か否かを判別するコードである [4]．このコードは，マルウェアの動的解析環境として多用される VMware [*1] 製品に特有のチャネルを検出する．同様に，仮想環境特有のプロセス，ファイル等の確認，特定の応答の監視 [5] による環境検知方法がある．Chen らの調査では，調査対象の 40%以上のマルウェアでこのような機能が確認された [6]．

また，2012 年から 2013 年にかけて発見された “UpClicker” や “BaneChant” は，自身が活動する環境が動的解析用の環境か否かを判別するマルウェアである．ユーザからの入力の有無に注目し，ユーザの通常利用時に見られる入力操作がない場合は動的解析にかけられていると判定して活動を制限する [7]．

2010 年に発見された “Win32.DelfInj.” [8]，2013 年に発見された “Nap” や “Hastani” [9] は，活動時間の調整により動的解析を回避するマルウェアである．起動してから活動を開始するまでの時間や活動可能な日程を設定しておくことで，動的解析中に活動することを避け，長期にわたって潜伏した後に活動する．

“Citadel” は，自身が動作するホスト環境の相違を判別するマルウェアである．このマルウェアは，初期感染時にその環境特有の情報を自身のコードに書き込む．後に検体として回収され動的解析にかけられた場合は，現在の環境情報と初期感染時の環境情報とを比較して環境の相違を判定し，活動を停止する [10]．

2) ネットワーク情報検知型マルウェア

シーケンシャルマルウェア [11] 等は，攻撃者が用意したサーバに接続し，攻撃者からの指示を受信したり，新たなマルウェアをダウンロードしたりすることで，攻撃を進めていく．たとえば，CCC DATAset 2009 [12] の，SHA1 ハッシュ値の先頭 4 桁が 393F，7190 の検体は，インターネットとの通信を完全に遮断した場合よりも，一部の通信を許可した場合の方が実行されるコード量が多い [13]．この種のマルウェアは，インターネットから隔離された検査環境上では攻撃に必要な通信が阻害され，一部の機能が実行されない．より能動的な例としては，インターネットへの接続可否を確認し，接続不能であれば隔離された環境に置かれていると判定して活動を停止するマルウェアも確認されている [14]．

また，LAN 内の他のホストに対する通信を定期的に試み，応答を監視することで隔離状況を検知するマルウェアの存在も示唆されている．マルウェアによっては，証拠隠滅だけでなく，感染ホストのデータ全体を破壊する場合もある [15]．

これらのマルウェアに対しては，マルウェア感染が疑われるホストを LAN から切り離し，被疑ホストや抽出した検体を詳細に調査する，という従来のインシデント対処の手順では対応できない．

1.2 本稿の目的

本稿では，インシデント対処において，環境により挙動を変えるマルウェアに検知されずに被疑ホストを LAN から切り離し，詳細調査可能な状態に置く手法の提案を目的とする．

2. 従来技術とその課題

1) ホスト情報検知型マルウェアへの対抗手法

Chubachi は，マルウェアが感染したホストと別のホスト上で実行されていることを検知した場合に挙動を変更し，動的解析できなくなるという問題に注目した．これに対処するため，プロセスマイグレーション手法および API プロキシを提案・実装した [16]．プロセスマイグレーション手法は，活動中のプロセスを別のホスト上に移行可能にする手法である．この手法では，CPU エミュレータを用いたプロセス用サンドボックスを構築することで，不審な挙動を見せたプロセスを一時停止し，周辺データとともに解析環境のサンドボックス上に移行できる．また，API プロキシは，前述サンドボックス上のプロセスが呼び出す API を監視し，環境情報を取得する API の呼び出しに対しては，移行前のホストの環境情報を返す．これにより，プロセスに環境の変化を検知されることなく，解析環境に移行できる．

Chubachi の手法では，マルウェアに感染する可能性があるホストにあらかじめプロセス用サンドボックスが組み込まれ，稼働している必要がある．また，解析環境に移行した後，ホスト情報の変化に関しては API プロキシを介することでマルウェアに検知させないが，LAN からの切り離し等の，ネットワーク情報の変化に関しては考慮されていない．

[*1] VMware は，VMware, Inc. の登録商標です．

2) ネットワーク情報検知型マルウェアへの対抗手法

Kreibich らは，マルウェア検体の動的解析時に，マルウェアの活動を観測するために必要な通信を許可し，同時に外部に被害を与える悪性通信を遮断するため，マルウェアが活動するホストとインターネット環境の間に配置する専用プロキシサーバを提案した [17]．この専用プロキシサーバは，パケットの遮断，書き換え，リダイレクト，帯域制限等により，安全確保と動的解析を両立させる．

Kreibich らの手法は，マルウェア感染ホストからマルウェア検体を回収した後，検体を動的解析環境に投入することを想定している．このため，ホスト情報の変化を検知するマルウェアに対しては有効ではない．また，被疑ホストを LAN から切り離し，これらの動的解析環境に接続することで同一のホストをそのまま解析に使うとしても，接続変更の過程でのネットワーク接続状態の変化については考慮されないため，マルウェアによる検知から逃れられない．

つまり従来技術ではホストあるいはネットワークのいずれか一方で検知されるリスクが残っていた．そのため本研究では，ホスト・ネットワークの両面においてマルウェアに変化を検知されることなく，被疑ホストを LAN から切り離し，詳細調査可能な環境に置くことを課題と設定する．

3. 提案手法

3.1 SDN（Software Defined Networking）の適用

SDN とは，ネットワークの構成や機能等をソフトウェアにより制御する技術である．近年の情報システムの潮流として，計算機リソースの仮想化があげられる．普及が進むクラウドを中心に，サーバ，ストレージ，ネットワーク等のリソースを物理的な制約から分離して論理的に管理・利用する仮想化技術の需要が高まっている．特に，サーバ，ストレージの仮想化技術の進歩と比較して遅れていたネットワークの仮想化技術が，SDN により近年，急速に進展した．このため，SDN は今後データセンタをはじめとして多くの情報システムを支える基盤として組み込まれていくと期待されており，多くのユースケースで利用可能になると予想される．

OpenFlow[*2] とは，SDN を制御する代表的なプロトコルの 1 つである．OpenFlow ver1.3.2 には，以下のような特徴がある [18]．

(1) パケットの送受信を実行するスイッチと，スイッチを管理し送受信の規則を制御するコントローラを分離したアーキテクチャを採用している．あらかじめ設定された規則に従いスイッチ単独で動作することも，パケットを受信するたびにコントローラに処理方法を問合せすることも可能である．

(2) レイヤ 1 からレイヤ 4 までの情報について，パケットの識別に利用でき，また操作対象とすることが可能である．物理ポート番号，MAC アドレス，VLAN ID，IP アドレス，TCP/UDP ポート番号等でパケットを識別し，ヘッダ情報を書き換えて指定した物理ポートから出力させることができる．

以上のように，ネットワークの動的制御，詳細なルールの適用が可能であり，アドレスを偽装するマルウェアに対してもスイッチ側の物理ポートの制御で対応可能といった特徴から，マルウェアに検知されることなく通信経路を変更することに適している．

以上より，本稿では SDN の活用を前提として検討を進める．

3.2 解決方針

本稿では，被疑ホストの特定は，IDS やプロキシサーバの不審通信検知等により行われるものとし，被疑ホストの特定以降の対応業務について検討する．被疑ホストを LAN から切り離すことで問題が生じる状況として，以下の 2 点がある．

A) マルウェアが通信していないときに切り離しを実行した場合，マルウェアが再度通信を開始したときに，応答がないことから環境変化を検知し，挙動を変更・隠蔽する．

B) マルウェアが通信しているときに切り離しを実行した場合，通信が中断されることで環境変化を検知し，挙動を変更・隠蔽する．

A) に対しては，被疑ホストの通信に対して応答を返す擬似環境を用意し，被疑ホストからの通信が擬似環境に到達するよう，ネットワーク切替えを行うことで解決する（**図 1** (a)）．

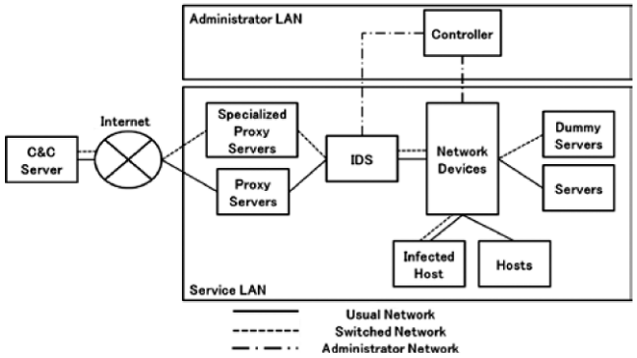
被疑ホストから LAN 内サーバへの通信については，同様のサービスを稼働させたダミーサーバを設置し，被疑ホストからの通信がダミーサーバに到達・応答するようパケットヘッダを更新し，転送する．

被疑ホストからインターネット上のサーバ，特に攻撃者が用意した C&C（Command and Control）サーバへの通信については，前述の従来技術のような，安全を確保しながらマルウェア検体を動的解析可能にする専用プロキシサーバ等を経由するように，パケットヘッダを更新し，転送する．

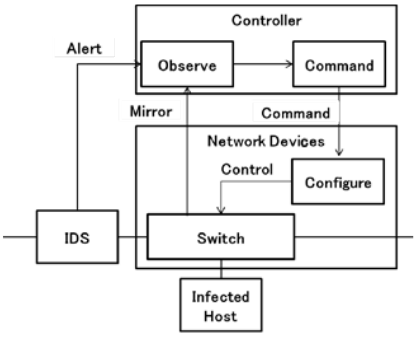
B) に対しては，コントローラが被疑ホストの通信状態を観測し，通信していないタイミングで A) のネットワーク切替えを行うことで解決する．

ただし，さらに考慮すべき要素として，ネットワーク切替えに要する時間（タイムラグ）がある．通信遅延や設定更新処理等により，通信状態の観測からネットワーク切替えの完了までにはタイムラグが発生する．本稿では，仮想

[*2] OpenFlow は，Open Networking Foundation の登録商標です．



a) System Configuration Diagram



b) Functional Block Diagram

図 1 マルウェア通信への応答を維持するネットワーク切替えシステム構成

Fig. 1 System architecture for network switching maintaining response to the malware.

マシン上のソフトウェアスイッチの処理時間等を測定し，タイムラグを最大 1 [s] と想定した．このタイムラグのため，被疑ホストが通信していないタイミングでネットワーク切替えを行ったとしても，切替えのタイムラグ中にマルウェアが通信を開始すると，マルウェアの通信を異常中断させてしまう．この通信の異常中断を検知し，挙動を変更するマルウェアに対処できなくなる．

これに対し，本稿では，以下の 2 つの手法を提案する．

手法 1. 通信タイミング予測手法：統計的手法により被疑ホストの通信開始タイミングを予測し，通信開始タイミングを避けてネットワークを切り替える．

手法 2. タイミング調整可能な切替え手法：被疑ホストが送受信するパケットが，コントローラを経由する状態を経ることで，ネットワーク切替えタイミングを被疑ホストの通信状態の変化に基づいて調整可能にする．

これらの手法には，それぞれ以下の問題点がある．

1. 被疑ホストの通信開始タイミングを完全に予測することは難しく，マルウェアの通信を中断する可能性が残る．
2. コントローラを経由する通信は管理系 LAN を介するため，スループットが低下し，大量のトラフィックを処理することができない．

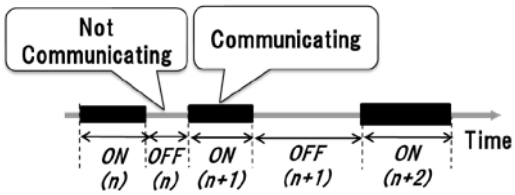


図 2 通信状態の時間変化

Fig. 2 Translation of connection state.

本稿では，これら 2 つの手法を組み合わせることで，互いの問題点を補う．すなわち，手法 2 により，手法 1 による予測が外れた場合でも安全なネットワーク切替えを可能にする．一方で，手法 1 により，手法 2 の問題点となる，管理系 LAN のトラフィック量を低減する．

以下では，手法 1 の詳細を 3.3 節で，手法 2 の詳細を 3.4 節で説明する．

3.3 通信タイミング予測手法（手法 1）

本節では，通信タイミング予測手法（手法 1）の詳細を説明する．手法 1 は，ネットワーク切替え時に通信を中断させないために，被疑ホストの通信タイミングを予測し，通信開始可能性が低いタイミングを選んでネットワークを切り替える手法である．

3.3.1 タイミング予測原理

手法 1 では，ネットワーク上から観測できる情報を機械学習に適用し，被疑ホストの通信タイミングを予測する．特徴量としては，通信ログから得られる過去の通信・非通信の継続時間のパターンを利用した．

図 2 は，TCP 通信の様子を表している．TCP コネクションが張られている状態（ON: Communicating）の継続時間を通信時間，それ以外の状態（OFF: Not Communicating）の継続時間を非通信時間と定義する．

あるホストから特定のサーバへの通信状態（TCP コネクションの状態）の時間変化は，図 2 のように ON と OFF の繰返しパターンで表現できる（n 回目に出現した ON/OFF を ON/OFF(n) と表記）．

これらの通信パターンの学習用データについては，マルウェアの動的解析で得られたパケットログや過去の被疑ホストのパケットログを利用する．また，予測対象の通信データについては，被疑ホストのパケットログをネットワーク機器からミラーリング等で採取する．マルウェアによる通信とその他の通信は区別することが困難なため，被疑ホストからのすべてのパケットを処理対象とする．

手法 1 では，最新の非通信時間を予測するため，直前の通信時間・非通信時間を特徴量として回帰モデルを作成する．非通信時間の「長さ」を予測対象とするため，正規分布が適当と考え，この現象を表す回帰モデルとして，複数の正規分布の重ね合わせを利用した（式 (1)）．

以上をふまえ，手法 1 では，ある時点の非通信時間と，

図 3 特徴量ベクトルリスト（左：2 次元，右：4 次元）
Fig. 3 Feature vectors (dimension: 2 (left), 4 (right)).

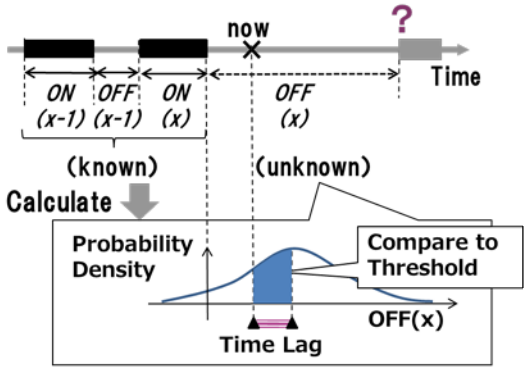


図 4 ネットワーク切替え可否判定
Fig. 4 Decision of route modification timing.

直前の通信時間・非通信時間との関係を定式化するため，学習用データを利用して，これらの組合せを特徴量ベクトルとしてリスト化する．これをもとに回帰モデルを作成する．**図 3** は，ある時点の非通信時間（OFF(n)）と，その直前の 1 つの状態（ON(n)）または 3 つの状態（ON(n)，OFF($n-1$)，ON($n-1$)）を 1 つのベクトルとして作成した，2 次元と 4 次元のリストの例である．

$$p(x) = \sum_i \frac{w_i}{(\sqrt{2\pi})^m \sqrt{|S_i|}} \exp\left(-\frac{1}{2}(x-u_i)^T S_i^{-1}(x-u_i)\right) \quad (1)$$

x：特徴量ベクトル
w_i：i 番目の正規分布の重み
S_i：i 番目の正規分布の共分散行列
u_i：i 番目の正規分布の平均値ベクトル
m：特徴量ベクトルの次元数

通信タイミング予測は，前述の回帰モデルを用いて行う．最新の非通信時間を推定するため，被疑ホスト・サーバの最新の通信ログから特徴量（最新の非通信時間のみ未知）を算出し，前述の算出済み回帰モデルに適用して，最新の非通信時間（OFF(x)）についての確率密度関数を得る．この関数を，タイムラグ（前述のとおり今回は 1 [s] に設定）に相当する区間で積分した値が，最新の非通信時間がその区間で終了する確率となる．この確率からネットワーク切替えの可否を判定するため，事前に切替え可否閾値を設定しておき，算出した確率が切替え可否閾値より小さければ，切替え可能と判定する．**図 4** は，4 次元の特徴量を利用した場合の概念図である．

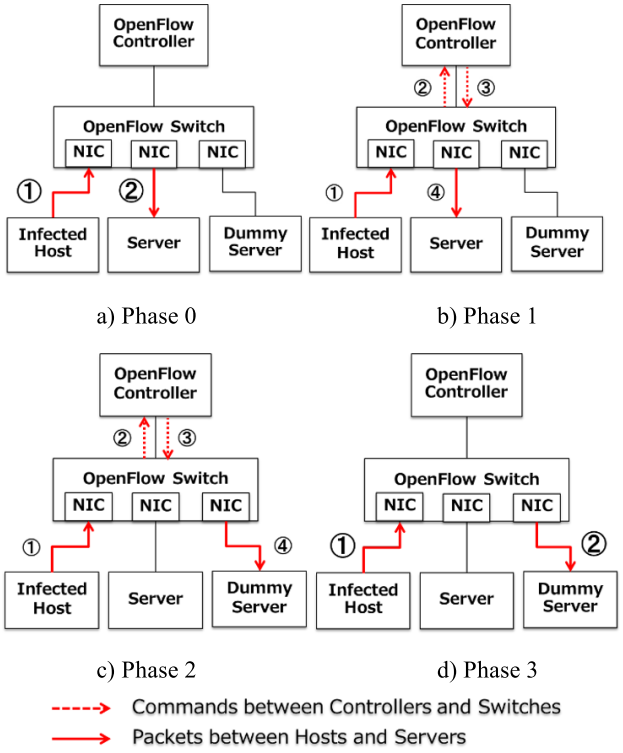


図 5 調整可能なネットワーク切替えの各段階におけるパケットの移動経路
Fig. 5 Routes of packets on each phase.

3.4 調整可能なネットワーク切替え手法（手法 2）

手法 2 は，OpenFlow 仕様を前提とし，ネットワーク切替えタイムラグと被疑ホストの通信開始のタイミングが重なった場合に，被疑ホストの通信を異常中断させないための手法である．そのために，被疑ホストが送受信するパケットが OpenFlow コントローラを経由する状態を一時的に作る．手法 2 では，ネットワークの状態は**図 5** に示す 4 つの段階を経る．以下では，被疑ホスト，サーバ，ダミーサーバ，OpenFlow スイッチ各 1 台からなる最も単純なシステム構成を例に，被疑ホストからサーバへの通信をダミーサーバへ経路変更する処理を説明する．

(a) 段階 0（通常時の設定）

通常のネットワーク構成に従い，スイッチはホスト・サーバ間で通信できるようパケットを転送する（図 5 (a)）．

(b) 段階 1（インシデント対応時の過渡設定）

コントローラは被疑ホストの非通信中に，スイッチを，特定のホストからサーバへのパケットを受信した場合（図 5 (b)①）に，コントローラに処理を問い合わせる（図 5 (b)②）よう設定する．段階 0 から段階 1 に遷移する間に被疑ホストが通信を開始した場合，コントローラは，この問合せに対してパケットをサーバへ転送するよう，スイッチに指示し（図 5 (b)③），スイッチは指示に従ってパケットを転送する（図 5 (b)④）．被疑ホストからのパケットに関する問合せをコントローラが受信する間は，段階 1 を維持する．

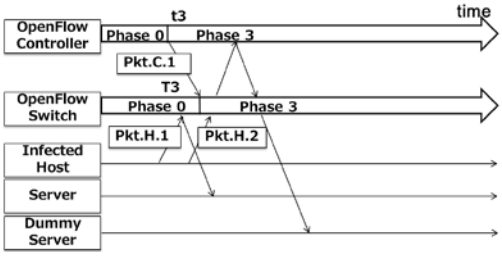


図 6 通常のネットワーク切替え
Fig. 6 Normal method.

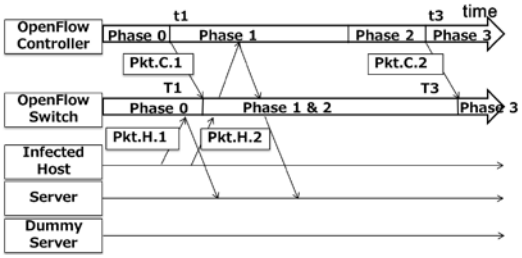


図 7 調整可能なネットワーク切替え（延期時）
Fig. 7 Adjustable method (postponed).

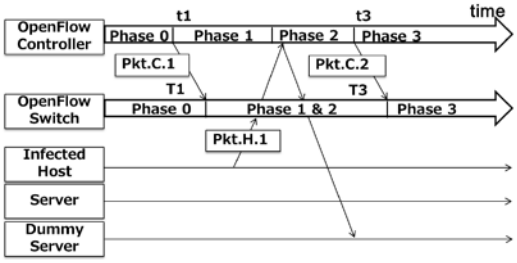


図 8 調整可能なネットワーク切替え（非延期時）
Fig. 8 Adjustable method (not postponed).

(c) 段階 2（インシデント対応時の過渡設定）

スイッチの設定は段階 1 と同様で，被疑ホストからサーバへのパケットを受信した場合（図 5 (c)①），コントローラに処理を問い合わせる（図 5 (c)②）よう設定される．段階 1 から段階 2 に遷移する間に被疑ホストが通信を開始した場合，コントローラは，被疑ホストからのパケットをダミーサーバへ転送するようスイッチに指示し（図 5 (c)③），スイッチは指示に従ってパケットを転送する（図 5 (c)④）．その際，イーサネットヘッダ内の，サーバの MAC アドレスをダミーサーバの MAC アドレスに書き換えるように指示する．被疑ホストからのパケットに関する問合せをコントローラが受信する間は，段階 2 を継続する．

(d) 段階 3（インシデント対応時の設定）

コントローラは，スイッチを被疑ホストからサーバへのパケットをダミーサーバへ転送し，その際，イーサネットヘッダ内のサーバの MAC アドレスをダミーサーバの MAC アドレスに書き換えるよう設定する．

手法 2 では，スイッチからコントローラへのパケット転送と，コントローラからスイッチへの経路変更指示が同じ経路（スイッチとコントローラをつなぐ経路）上を通るため，被疑ホストの通信と経路変更指示が入れ違いになることがない．そのため，被疑ホストが通信しているタイミングでの経路変更を確実に回避できる．以下では，ネットワーク切替え途中に被疑ホストの通信が発生した場合を想定し，段階の移行とパケットの動きを時系列で説明する．

手法 2 を使わない，OpenFlow を用いたネットワーク切替えは，段階 1，2 を介さずに段階 0 から 3 へ移行することにあたる（**図 6**）．この場合，コントローラが通信ログを参照し，被疑ホストの通信状態を把握して切替え可能と判定し，スイッチに設定変更指示パケット Pkt.C.1 を送信して（時刻 t3）それがスイッチに反映される（時刻 T3）までには時間がかかる．そのため，その間に被疑ホストが送信したパケット Pkt.H.1 はサーバに送信される．一方，設定反映後のスイッチに届いたパケット Pkt.H.2 はダミーサーバに送信される．

これに対し，手法 2 では，段階 1，2 により，設定が反映されるまでの通信の有無を確認する余裕を作ることができる．**図 7** で，コントローラが設定変更指示パケット Pkt.C.1 を出した後，被疑ホストからの通信が開始されていないか確認できるまで待機し，パケット Pkt.H.1 がサーバに送られていた場合，コントローラは段階 1 を維持し，後のパケット Pkt.H.2 もサーバへ転送させる．通信終了が確認できた後，ネットワーク切替えを続行する，**図 8** は，段階 1 の待機中に被疑ホストが通信を開始しない場合であり，コントローラは段階 2，3 に移行して，後のパケットはダミーサーバに送信される．

4. 評価

4.1 評価目的

本章では，提案した 2 手法のうち，通信タイミング予測手法（手法 1）を評価する．調整可能なネットワーク切替え手法（手法 2）は，システムの機能として実装するものであるため，本稿では定量評価を行わなかった．

提案した 2 手法を併用した環境では，手法 1 が失敗し，ネットワーク切替え中に被疑ホストからの通信が発生した場合に，手法 2 が機能する．このとき，スイッチに到達した被疑ホストからのパケットは，スイッチからコントローラへ転送される．この通信は管理系 LAN を圧迫するため，ネットワーク管理のための通信の阻害，コントローラの応答遅延につながる．

本稿では以下の環境を想定した．管理系 LAN の帯域のうち手法 2 に割り当てられる帯域を 50 Mbps，同時にネットワーク切替えを行うホストを最大 100 台，各ホストの通信量を平均 5 Mbps とした．想定される最大の通信量に対し，利用可能な帯域が 10%であるため，手法 1 の失敗率は 10%以下である必要がある．

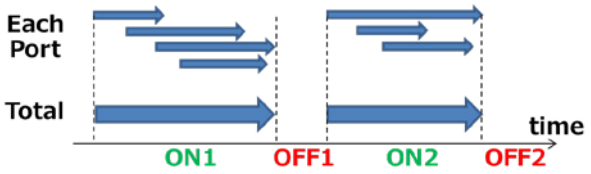


図 9 トータル通信パターンの算出
Fig. 9 General communication pattern.

4.2 通信タイミング予測精度評価

マルウェアの通信ログとしては，MWS（マルウェア対策研究人材育成ワークショップ）2014 [19] で提供されている研究用データセットを使用した．MWS は，サイバークリーンセンタのハニーポットで収集しているボットの観測データや，研究者コミュニティから提供されたデータの提供を通し，マルウェアに関する専門知識を備えた人材の育成を目指すワークショップである．本稿で使用したのは，データセットのうち，想定する状況に近い通信ログが得られると考えられる D3M DATAset [20] である．D3M DATAset に含まれる pcap ファイルは，悪性 URL を巡回した際に得られるドライブバイダウンロード攻撃の通信を記録したものであり，本稿で想定する，マルウェアが外部と通信する状況のサンプルとして適している．本実験では，データセットの通信ログのうち，1 日分（約 41,000 パケット）を学習データ，別の 1 日分（約 55,000 パケット）をテストデータとして使用した．

4.2.1 手順 1：通信パターンの算出

1. 学習用およびテスト用の pcap ファイルをパースし，TCP/IP パケットのうち，TCP フラグが SYN，RST，FIN のものを抽出する．
2. TCP ポート番号ごとに，SYN パケットを通信開始，RST または FIN パケットを通信終了と見なして，通信状態（通信中（ON）/非通信中（OFF））の変化時刻を算出する．
3. TCP ポート番号ごとの通信状態をマージして，トータルの通信状態を算出する（**図 9**）．1 つでも通信中のポートがあれば，トータルでも通信中と見なす．

4.2.2 手順 2：回帰モデルの算出

1. 3.3 節で説明した通信タイミング予測手法に従う．学習用データから，適当な次元の特徴量ベクトルリストを作成する．
2. 特徴量から回帰モデルを算出する．算出には EM アルゴリズムを使用した [21]．

4.2.3 手順 3：精度評価

テスト用データに対して前項で算出した回帰モデルにより，通信開始タイミングの予測精度を評価した．評価指標は以下の 2 つとした．

A) 偽陽性（False Positive）確率
B) 偽陰性（False Negative）確率

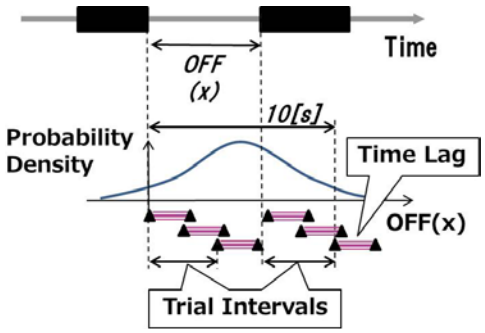


図 10 偽陽性確率算出
Fig. 10 Calculation of false-positive rate.

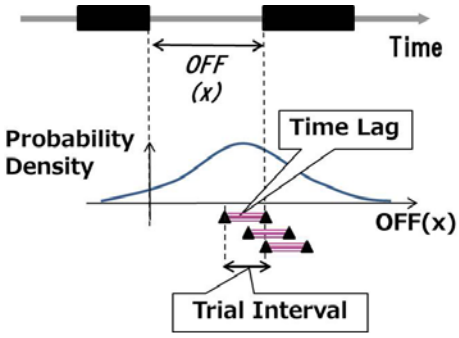


図 11 偽陰性確率算出
Fig. 11 Calculation of false-negative rate.

A) 偽陽性（False Positive）確率

被疑ホストの通信が発生しないにもかかわらず，通信発生を予測してしまい，ネットワークの切替え機会を逃す確率を偽陽性確率とする．

偽陽性確率の算出方法は以下のとおりである．まず，回帰モデルから得た OFF(x) の確率密度関数に対し，偽陽性判定の対象とする区間を設定する．本評価では，この区間を 0〜10 [s] とした．次に，上記区間の中で，切替えを実行してもタイムラグ中に次の通信が発生しない範囲を試行区間とする（**図 10** Trial Intervals）．さらに，この試行区間内で，積分区間をずらしながら切替え可否判定を複数回行う．すなわち，タイムラグに相当する区間で確率密度関数を積分し（図 4 参照），切替え可否閾値と比較する．この結果，切替え不可と判定された場合は偽陽性とし，全試行回数に対する偽陽性出現回数の割合を偽陽性確率とする．

B) 偽陰性（False Negative）確率

被疑ホストの通信が発生する場合に，発生を予測できず，ネットワークの切替えを実行してしまう確率を偽陰性確率とする．

偽陰性確率の算出方法も同様に，回帰モデルから得た OFF(x) の確率密度関数に対し，切替えのタイムラグが次の通信開始と重なる範囲，つまり切替えを実行した場合タイムラグの期間に通信が発生する範囲を試行区間として（**図 11** Trial Interval），この試行区間内で，積分区間をずらしながら切替え可否判定を複数回行う．その中で切替え

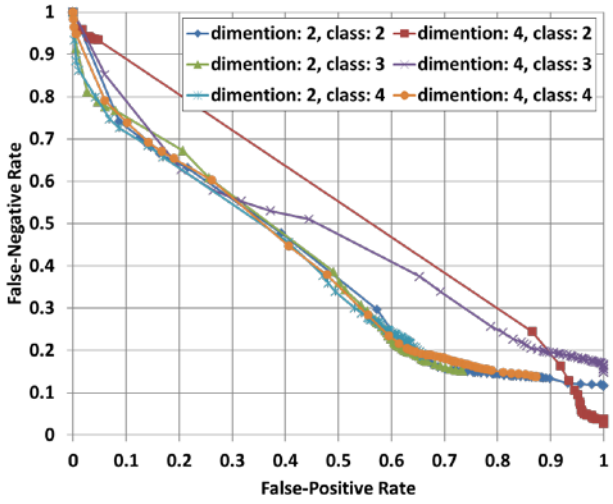


図 12 偽陽性・偽陰性確率の変化
Fig. 12 Change of FPR and FNR.

可能と判定された場合は偽陰性とし，全試行回数に対する偽陰性出現回数の割合を偽陰性確率とする．

4.1 節で述べた前提条件から，本稿では，偽陰性確率 10%以下を目標値とした．

4.3 評価結果

実験にあたり，パラメータを変化させて偽陽性・偽陰性確率を計測した．変化させたパラメータとその範囲は，回帰モデルに利用する特徴量ベクトルの次元数（2，4），正規分布の重ね合わせ数（2，3，4），切替え可否閾値（1×10^{-1}～1×10^{-18}）である．各パラメータに対し 5 回ずつ計測を行い平均値を算出した．結果を**図 12** に示す．横軸は偽陽性確率，縦軸は偽陰性確率とした．左下ほど偽陰性・偽陽性確率ともに低く，理想的な状態といえる．また，各線は，次元数およびクラス数を固定し，閾値を変化させてプロットした点をつないだものである．

5. 考察

図 12 によると，次元数 4，重ね合わせ数 2 の場合に，目標である偽陰性確率 10%以下を達成できることが明らかとなった．この場合，偽陰性確率 10%以下となる切替え可否閾値の範囲では，偽陽性確率は 95%を超える．このため，切替え可能な時間のうち 95%で正しく切替え可能と判定できず，偽陽性の誤判定が多すぎて切替えタイミングを逃し続けてしまう可能性がある．これは切替え実行までに時間を要することを意味しており，マルウェアの活動によるリスクを考慮して，許容できる範囲に収まるか評価する必要がある．

一方で，偽陽性確率を一定値以下に抑えながら偽陰性確率を 0%にすることは困難であった．このため，確実にマルウェアに検知されずにネットワーク切替えを実行するには，手法 2 が必要となるといえる．

6. おわりに

本稿では，マルウェア感染が疑われる被疑ホストを発見してから，被疑ホストを調査可能な状態に置くまでの過程において，ホスト・ネットワークの両面から，マルウェアの環境変化検知を防ぐことを目的とし，

- 通信タイミング予測手法（手法 1）
- 調整可能なネットワーク切替え手法（手法 2）

からなるネットワーク切替え手法を提案した．

さらに，手法 1 をマルウェアの通信ログに適用し，予測精度を評価した．その結果，次元数 4，重ね合わせ数 2 の条件下で，偽陰性確率 10%以下，偽陽性確率 95%以上という結果を得て，想定する環境下で，方式 2 と組み合わせることで機能する見通しを得た．

今後の課題は以下のとおりである．

- 本稿では，通信タイミング予測のための回帰モデルに正規分布を利用したが，その妥当性については検証が必要である．
- 本評価では，通信タイミング予測手法（手法 1）に対し，限られたデータセットに対する実験のみを行った．手法 1 の汎用性を評価するためには，より多くの種類のデータで評価する必要がある．
- 本評価では，データセットに基づき通信タイミング予測手法（手法 1）を評価しているが，実際の有効性は不明であるため，実マルウェアを用いて挙動の変化を観測し，評価する必要がある．
- 偽陽性判定によりネットワーク切替え実行までにかかる時間を評価し，この時間内のマルウェアの活動によるリスクが許容できるか検討する必要がある．

参考文献

[1] Cichonski, P., Millar, T., Grance, T. and Scarfone, K.: Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology (online), Special Publication 800-61, p.35, available from ⟨http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf⟩ (2008).

[2] Lindorfer, M., Kolbitsch, C. and Milani, P.: Detecting Environment-Sensitive Malware, *Proc. International Conference on Recent Advances in Intrusion Detection* (*RAID 2011*), pp.338–357 (2011).

[3] Kirat, D., Vigna, G. and Kruegel, C.: BareCloud: Bare-metal Analysis-based Evasive Malware Detection, *Proc. USENIX Conference on Security Symposium*, pp.287–301 (2014).

[4] Carpenter, M., Liston, T. and Skoudis, E.: Hiding Virtualization from Attackers and Malware, *IEEE Security and Privacy*, pp.62–65 (2007).

[5] Rutkowska, J.: Red Pill... Or How To Detect VMM Using (Almost) One CPU Instruction, Internet Archive (online), available from ⟨https://web.archive.org/web/20070108160054/http://invisiblethings.org/papers/redpill.html⟩ (accessed 2014-11-28).

[6] Chen, X., Andersen, J., Mao, Z., Bailey, M. and Nazario, J.: Towards an understanding of anti-virtualization and anti-debugging behavior in modern malware, *IEEE International Conference on Dependable Systems and Networks With FTCS and DCC* (*DSN 2008*), pp.177–186 (2008).
[7] Islam, A.: 2013: Attack Trends for the Year Ahead, RSA Conference Asia Pacific 2013 (online), available from ⟨https://www.rsaconference.com/writable/presentations/file_upload/spo-w01a_final_2.pdf⟩ (accessed 2014-11-28).
[8] Kolbitsch, C., Kirda, E. and Kruegel, C.: The power of procrastination: Detection and mitigation of executionstalling malicious code, *Proc. ACM Conference on Computer and Communications Security* (*CCS '11*). pp.285–296 (2011).
[9] FFRI, Inc.：Citadel の解析から得られた近年のマルウェア傾向，情報セキュリティ EXPO2014 春 (2014).
[10] Kolbitsch, C.: Analyzing Environment-Aware Malware, Lastline Labs (online), available from ⟨http://labs.lastline.com/analyzing-environment-aware-malware-a-look-at-zeus-trojan-variant-called-citadel-evading-traditional-sandboxes⟩ (accessed 2014-11-28).
[11] 独立行政法人情報処理推進機構セキュリティセンター：近年の標的型攻撃に関する調査研究（オンライン），入手先 ⟨https://www.ipa.go.jp/files/000013943.pdf⟩（参照 2014-11-28）.
[12] 畑田充弘，仲津留勇，寺田真敏，篠田陽一：マルウェア対策のための研究用データセットとワークショップを通じた研究成果の共有，マルウェア対策研究人材育成ワークショップ 2009 (2009).
[13] 青木一史，川古谷裕平，岩村　誠，伊藤光恭：半透性仮想インターネットによるマルウェアの動的解析，情報処理学会コンピュータセキュリティシンポジウム論文集 (2009).
[14] 菅原継顕：長期潜伏，自らを削除—サンドボックスを回避する未知のマルウェア，ZDNet Japan（オンライン），入手先 ⟨http://japan.zdnet.com/security/sp_networksec/35047336/⟩（参照 2014-11-28）.
[15] Mell, P., Kent, K. and Nusbaum, J.: Guide to Malware Incident Prevention and Handling, Recommendations of the National Institute of Standards and Technology (online), Special Publication 800-83, p.65 (2005).
[16] Chubachi, Y.: Freeze Drying for Capturing Environment-Sensitive Malware Alive, *Black Hat Europe 2014* (2014).
[17] Kreibich, C., Weaver, N., Kanich, C., Cui, W. and Paxson, V: GQ: Practical Containment for Measuring Modern Malware Systems, *Proc. ACM SIGCOMM Conference on Internet Measurement*, pp.397–412 (2011).
[18] Open Networking Foundation: OpenFlow Switch Specification Version 1.3.2. (online), available from ⟨https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.3.2.pdf⟩ (accessed 2014-11-28).
[19] 秋山満昭，神薗雅紀，松木隆宏，畑田充弘：マルウェア対策のための研究用データセット～MWS Datasets 2014，情報処理学会研究報告コンピュータセキュリティ（CSEC），Vol.2014-CSEC-66, No.19, pp.1–7 (2014).
[20] Akiyama, M., Aoki, K., Kawakoya, Y., Iwamura, M. and Itoh, M.: Design and Implementation of High Interaction Client Honeypot for Drive-by-download Attacks, *IEICE Trans. Communications*, Vol.E93-B, No.5, pp.1131–1139 (2010).
[21] Bishop, C.: *Pattern Recognition and Machine Learning*, pp.435–439, Springer (2006).

推薦文

端末に感染したと推察されるマルウエアの調査フェーズにおいて，マルウエアをネットワーク的に隔離する方式を提案している．特に，SDN の特徴を巧みに利用し，ネットワークを動的に切り替えることによって，検査精度とスループットの両立を達成している点を評価し，推薦論文として推薦したい．

（コンピュータセキュリティ研究会主査　西垣正勝）

来間 一郎　（正会員）

2011 年東京大学工学部卒業．2013 年同大学大学院情報理工学系研究科修了．同年株式会社日立製作所横浜研究所に入社．現在，日立製作所研究開発グループシステムイノベーションセンタに勤務．情報セキュリティの研究開発に従事．

甲斐 賢　（正会員）

1996 年京都大学理学部卒業．1998 年同大学大学院理学研究科修了．同年株式会社日立製作所システム開発研究所に入社．現在，日立製作所研究開発グループシステムイノベーションセンタに勤務．情報セキュリティの研究開発に従事．2012 年京都大学大学院情報学研究科博士課程修了．日本セキュリティ・マネジメント学会会員，CISSP．

木城 武康

株式会社日立システムズネットワークセキュリティサービス事業部セキュリティ ICT サービス本部サイバーセキュリティソリューション部部長兼 CSIRT センタセンタ長．JNSA セキュリティ市場調査 WG リーダ，BCI 日本支部 IT 継続 WG メンバ，CISSP，BCM-RM リスクマネージャ，CCSA，CCSE．

磯部 義明

1993 年豊橋技術科学大学大学院知識情報工学専攻修士課程修了．同年株式会社日立製作所に入社．システム開発研究所に配属．以来，医用画像処理，医用情報システム，指紋画像処理，生体認証システム，情報セキュリティの研究開発に従事．現在，同社研究開発グループシステムイノベーションセンタセキュリティ研究部主任研究員．電子情報通信学会会員．