Vol.2019-CSEC-87 No.13
2019/12/4

サイバー攻撃解析共有プラットフォームを用いた悪性サイトの継続的観測

藤井 翔太[†1] 佐藤 隆行[†1] 青木 翔[†1] 津田 侑[†2]
岡野 友輔[†3] 川口 信隆[†1] 重本 倫宏[†1] 寺田 真敏[†1]

概要：年々サイバー攻撃に用いられるマルウェアが高度化・増加しており，重大な脅威となっている．特に標的型攻撃に用いられるようなマルウェアは，遠隔操作のための通信確立や窃取した情報の送信等，攻撃者のサーバと通信する事で目的を達成するものが多い．即ち，マルウェアの接続先をいち早く特定し，当該接続先への通信を遮断することが攻撃を抑制において有効な手段であると言える．また，攻撃のタイミング等に伴って生死を繰り返す攻撃サーバの存在も知られており，継続的な観測によって攻撃の予兆を捉えることも重要である．さらに，集団防御の観点から，観測結果を組織間で共有・活用することが重要となっている．そこで我々は，サイバー攻撃解析共有プラットフォーム（PF）の研究開発を進めている．同 PF は，サイバー攻撃の観測や分析を実施すると共に，その結果を他組織と共有するものである．本稿では，不審接続先をマルウェアから抽出し，継続的に観測すると共にその結果を共有するまでのシステムに関して設計と実装を述べる．また，実際に 660 件の不審接続先を観測し，攻撃者のアトリビューションの可能性やブラックリストの棚卸しといった同 PF の活用可能性を確認した．

キーワード：悪性サイト，定点観測，マルウェア解析，STIX/TAXII

Continuous Observation of Suspicious Hosts with Cyberattack Analysis and Sharing Platform

SHOTA FUJII[†1] TAKAYUKI SATO[†1] SHO AOKI[†1] YU TSUDA[†2]
YUSUKE OKANO[†3] TOMOHIRO SHIGEMOTO[†1]
NOBUTAKA KAWAGUCHI[†1] MASATO TERADA[†1]

Abstract: Cybersecurity threats have been increasing and sophisticaed year by year. Especially, in APT attacks, malicious hosts play an important role, e.g., commander of remote control or receiver of theft information. Thus, identifying remote hosts of malwares and blocking communication with them are effective for suppressing damage of cyberattacks. Moreover, some malicious hosts become activate only during the attacks that occur periodically, and keep inactive for the rest of time for evading detection. Therefore, continuous observation is important for detecting such hosts. Furthermore, sharing observed data is also important from the viewpoint of collective defense. For these backgrounds, we have been developing a cyberattack analysis and sharing platform (PF). The PF aims to automate observation and analysis for cyberattacks and sharing the result with stakes holders. This paper focuses on the functions for extracting suspicious IP addresses and URLs from malwares, observing them continuously, and sharing the extracted and observed results with other organizations. This paper describes a design and implementation of systems structure of the PF. This paper also shows an observation result by prototype of the PF.

Keywords: malicious host, fixed point observation, malware analysis, STIX/TAXII

1. はじめに

年々サイバー攻撃に用いられるマルウェアが高度化・増加しており，重大な脅威となっている．このような状況からマルウェアを解析していち早く対策に繋げることや攻撃の予兆を捕らえ，攻撃者に先んじて対策を打つことがより重要となってきている．ここで，特に標的型攻撃に用いられるマルウェアは, C2 サーバ等の攻撃者が有するサーバとの通信を実施することにより，攻撃を達成する．例えば，遠隔操作を目的とした Remote Access Trojan（以降，RAT）が攻撃者とセッションを確立するための通信や窃取した情報の攻撃者のサーバへのアップロード等が挙げられる．よって，マルウェアの接続先をいち早く特定し，当該接続先への通信を遮断することが攻撃を抑制するにあたって有効な手段であると言える．他方で，特定した接続先を自組織のみでブラックリストへ追加するような活用形態の場合，当該接続先情報の入手には，当該検体を検出できる機構や動的解析機構が各組織に必要となる．また，各組織におけ

†1 株式会社日立製作所
Hitachi, Ltd.
†2 国立研究開発法人 情報通信研究機構
National Institute of Information and Communications Technology
†3 株式会社ＦＦＲＩ
FFRI, Inc.

る接続先情報の入手タイミングも組織毎に攻撃者がマルウェア検体を送ってきた後等の検体を入手した時点に限定されてしまう．これに対し，当該接続先情報を他組織に展開した場合，他組織としては各種機構を有していない場合でも当該情報を入手でき，かつマルウェア検体を攻撃者に送り込まれるよりも前のタイミングで対策を打てる場合もある．攻撃者も組織化が進んでいることから，このように防御側としても独立に分析を実施するだけでなく，解析結果等を共有し，協力して脅威に対抗することが重要となりつつある．さらに，単純に接続先をブラックリストに登録していくだけでは，同リストが不必要に肥大化してしまう恐れがある．攻撃者のサーバは使い捨てにされる場合もあることが知られていることから，例えば当該接続先が稼動していないのであればブラックリストからは一旦削除するといった，継続的なブラックリスト管理を行うに資する情報が存在することが望ましい．

以上のような状況から，マルウェア検体を解析し，解析結果，特にマルウェア検体が接続を試みる不審接続先の情報を他組織と共有すると共に，当該接続先に関して継続的な観測を行い，接続先の稼働状況等，当該接続先への対応可否等を判断するに資する情報を取得および共有するシステムが求められている．

上記のような状況を受け，我々はサイバー攻撃解析共有プラットフォーム（以降，サイバー攻撃解析共有 PF）を研究開発している．同 PF は，マルウェア検体の動的解析結果を基に，当該検体の接続先を機械可読なフォーマットで出力し，他組織と共有する．これにより，受け取り側の組織は，当該接続先のブラックリストへの迅速かつ自動的な登録とそれに伴う被害抑制が可能になる．加えて，当該情報を他組織と共有することにより,集団防御を可能とする．また，当該接続先に対する継続的な観測および観測結果の共有を行うことにより，接続先の稼働状況等，ブラックリストからの削除等の判断に資する情報を提供できる．さらに，当該接続先への継続的な観測の結果を活用することにより，以下のような効果も期待できる．例えば，マルウェア検体に紐付く C2 サーバの活性化を契機に当該検体の解析を開始することにより,挙動抽出の成功性を向上させる．また，攻撃者のサーバをはじめとしたインフラの変化を攻撃開始の予兆として捕らえることにより，攻撃開始に先んじた対策の実施を図る．

本稿では，上記 PF の全体像を示すと共に，マルウェア検体の接続先の抽出と継続的な観測を行い，その結果を共有するまでの流れを具体化する．また，左記の具体に基づいてプロトタイプを実装し，実際にシステムを稼動させた結果を報告する．なお，本観測結果は，MWS データセット [1] の一部として共有している．

2. 研究背景

2.1 不審接続先へのアクセス防止

近年の，特に標的型攻撃に用いられるマルウェアは，C2 サーバ等の攻撃者が有するサーバとの通信を実施する．例えば, 遠隔操作を目的とした RAT が攻撃者とセッションを確立するための通信や窃取した情報の攻撃者のサーバへのアップロード等が挙げられる．実際に，公開ブラックリストのうち，多くがマルウェア由来のものであるという調査結果もある [2]. よって, マルウェアの接続先をいち早く特定し，当該接続先への通信を遮断することが攻撃を抑制するにあたって有効な手段であると言える．

2.2 継続的観測

悪性サイトへの接続を遮断することは，前述の通り被害抑制に有効である一方で，悪性サイトには様々な異なる特徴があることが確認されており，単一的に遮断出来るものではない．例えば，悪性サイトは短期間で廃棄されるものが多い [3] 一方で，一部に関しては長期間生存することや一度ダウンした後に復活するものがあるといった，相反する特性が知られている [3, 4]. また, 一度利用したインフラを別の用途に再利用する事例も観測されている [5, 6]．さらに，特定の時間帯にのみ有効化される C2 サーバの存在 [7] や、名前解決すると、普段はループバックアドレスやプライベートアドレスが返るが，特定期間のみ攻撃に用いると思われる IP アドレスと紐づけられるドメインの存在も確認されている [8]. 即ち, 通信を遮断するためのブラックリストは，不審接続先が攻撃毎に使い捨てのものが多いことから肥大化しがちな一方で，不正接続先が再利用される可能性もあるために，時間経過等でブラックリストから除外する事が困難である．

こうした特性から，悪性サイトに関しては，継続的に観測を行い，その状況に応じて遮断するか否かを判断することが望ましいと言える．

2.3 情報共有

複雑・巧妙化し続けるサイバー攻撃に対し，被害を最小化するためには，多層防御のひとつの手段として集団防御のための連携，特に，複数組織間においてサイバー攻撃に関する情報を速やかに共有する仕組みを構築し，迅速な対策を講じることが重要となってきている [9]．こうした状況の中，情報共有の共通フォーマットや情報共有のプラットフォーム等が整いつつある [10-14]. 一方で，現状共有されている情報の多くは，専門家が分析した情報であることから，その内容が高度である反面，速報性にやや欠ける点がある．年々被害の拡大速度が大きくなり即時的な対処を要求されることから，高度かつ速報性のある情報を用いた即時的な自動対処が必要となる．

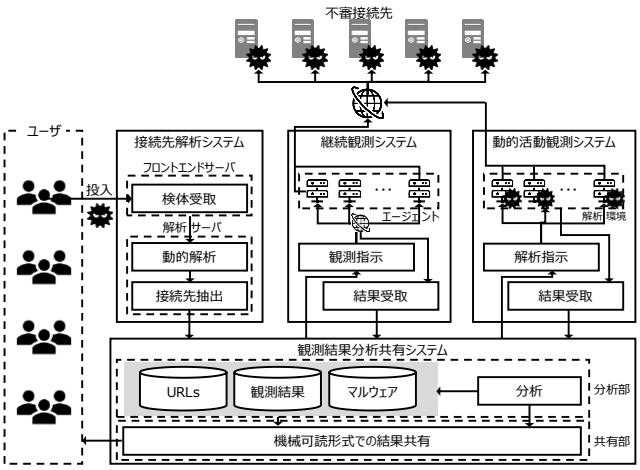

図 1 サイバー攻撃解析共有プラットフォームの全体像

3. サイバー攻撃解析共有プラットフォーム

3.1 目的と要件

本章では，我々が研究開発を進めているサイバー攻撃解析共有 PF の設計を述べる．同 PF は，2 章の研究背景で述べたマルウェアの接続先を特定することによる攻撃の抑制，悪性サイトの継続観測による対処判断支援，および即時的な情報共有による集団防御・自動対処を目的としている．同目的を達成するための要件と要望は，以下の通りである．

（要件1） マルウェアより接続先を抽出できること

先に述べたように，マルウェアが接続を試みる不審な接続先への通信を遮断することが攻撃の抑制に有効である．これを達成するための要件として，マルウェアから不審な接続先を抽出することが挙げられる．

（要件2） 不審な接続先を継続的に観測できること

生死等の状況が変わりうる不審接続先に対して，その稼働状況等を把握するためには，継続的な観測が必要である．

（要件3） 観測結果を機械可読な形で共有できること

集団防御実現のために，観測した結果を共有できることが要件として挙げられる．この際，自動的な機械処理を可能とするために，機械可読な形で共有することが望ましい．

（要望1） 不審接続先の変化に連動して当該接続先に関連するマルウェア検体を動的解析できること

先述のように，近年のマルウェアは C2 サーバと連携して動作することが多く，C2 サーバの中には攻撃するときのみ稼動するものもある．このため，マルウェアの挙動を誘発するには，C2 サーバの稼働時に解析を実施する必要がある．そこで，マルウェアに紐づく接続先の活性化を契機に動的解析を開始することにより，挙動抽出の成功性向上を図る機能があることが望ましい．

（要望）に関しては，サイバー攻撃共有解析 PF を実現する上で必須の要件ではないものの，目的の 1 つであるマルウェアの接続先特定に寄与することから挙げている．

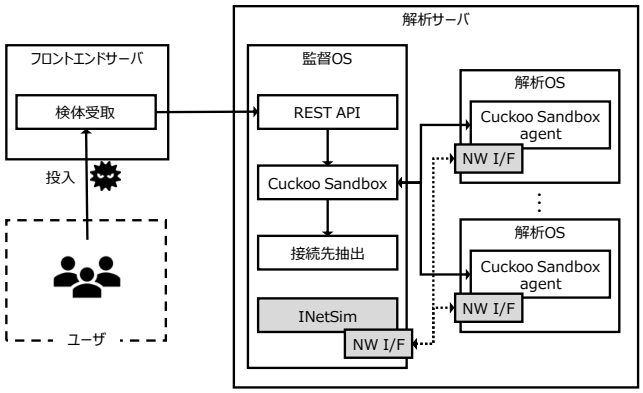

図 2 接続先解析システムの全体像

3.2 全体像

3.1 節の要件を満たす PF を検討した．同 PF の全体像を図 1 に示す．図 1 に示すとおり，本 PF は大きく以下の 4 システムからなる．

(1) 接続先解析システム

マルウェアを動的解析することにより，マルウェアが接続を試みる不審接続先を抽出する．これにより，（要件 1）を満足する．

(2) 継続観測システム

(1)で抽出した不審接続先を継続的に観測する．これにより，（要件 2）を満足する．

(3) 動的活動観測システム

(2)の観測における不審接続先の応答変化等を契機に，当該接続先にアクセスを試みるマルウェアに関して再度動的解析を実施する．これにより，（要望 1）を満足する．

(4) 観測結果分析共有システム

(1)～(3)のシステムを用いて解析・観測した結果を収集し，分析を行う．また，収集した情報を機械可読な形に整形し，共有する．これにより，（要件 3）を満足する．

上記のシステム群により，要件と要望を満足するサイバー攻撃解析共有 PF を実現する．また，本稿では，同 PF 実現に際しての第一段階として，要件に係る 3 システム（接続先解析システム，継続観測システム，および観測結果分析共有システム）について実現方式を述べる．

4. 実現方式

4.1 接続先解析システム

接続先解析システムは，マルウェア検体を動的解析し，その接続先を抽出するものである．本システムは，大きく利用者から検体を受け取るフロントエンドサーバと実際に動的解析を実施する解析サーバの 2 つからなる（図 2）．

フロントエンドサーバは，利用者からマルウェア検体を受け取り，同検体の解析リクエストを解析サーバに送付すると共に，解析結果を利用者に表示する．解析リクエストの送付には，後述の解析サーバが持つ REST API を用いる．

解析サーバは，フロントエンドサーバから解析リクエストを受けてマルウェアを動的解析すると共に，解析結果から当該検体の接続先一覧を抽出する．本サーバは，動的解析エンジンとしては Cuckoo Sandbox [15] を利用し，解析リクエストには，Cuckoo Sandbox の持つ REST API を利用する．また，解析時に，実際のインターネットに対して接続を行った場合，他の組織等に攻撃を試行してしまう可能性もある．これを抑制するために，インターネットを模倣する INetSim [16] を用いることにより，クローズドな環境で解析を実施する．なお，解析用端末としては，仮想マシン上に Windows 7 を構築し，Cuckoo Sandbox のエージェントを導入して利用する．同仮想マシンは，INetSim とのみ通信し，外部への通信を行わないことにより，外部への攻撃試行を防止する．

4.2 継続観測システム

継続観測システムは，不審接続先に対して継続的な観測を行い，その結果を記録するものである．本システムは，観測対象の接続先情報を定期的に受領し，当該接続先を観測エージェントによって観測する．なお，観測エージェントは，アクセス元の国に依って応答を変化させる攻撃サーバを想定し，複数国に設置する．また，観測としては以下の 3 つを行う．

- HTTP GET の送付
- PING の送付
- robots.txt の存在確認

各接続先へ HTTP GET を行うことにより，各接続先のステータスコードおよびコンテンツを取得する．この際，User-Agent やポート番号等を設定し，攻撃者の想定するリクエストに可能な限り近づけるようにする．なお，接続先解析システムでは接続先毎にこれらの値を保存しており，継続観測システムでの自動的な設定が可能である．加えて，PING の送付や robots.txt の存在確認を行い，攻撃者が持つサーバの稼動状態やその構成を確認する．

観測に際しては，正規サーバへの誤観測を抑制するために，robots.txt をまず確認し，クロールを禁止されたページであれば HTTP GET の送付は実施しない．その後，観測エージェントを用いて観測した結果を観測結果分析共有システムに送信する．

なお，今回は，観測間隔は固定で 4 時間とし，観測エージェントは 5 カ国に 2 台ずつ合計 10 台を設置した．

4.3 観測結果分析共有システム

4.3.1 分析部

観測結果分析共有システムは，各システムで解析・観測した結果を分析・共有するシステムであり，分析部と共有部の 2 つに大別できる．分析部では，先に述べたシステム群で解析・観測したデータを保管すると共に，分析も実施する．また，今回は分析部に相当する機能として可視化機能を実装した（図 3）．各接続先に対して，青線が HTTP GET

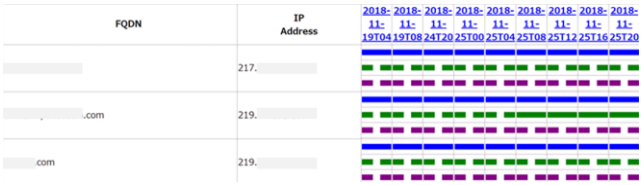

図 3 可視化機能の画面

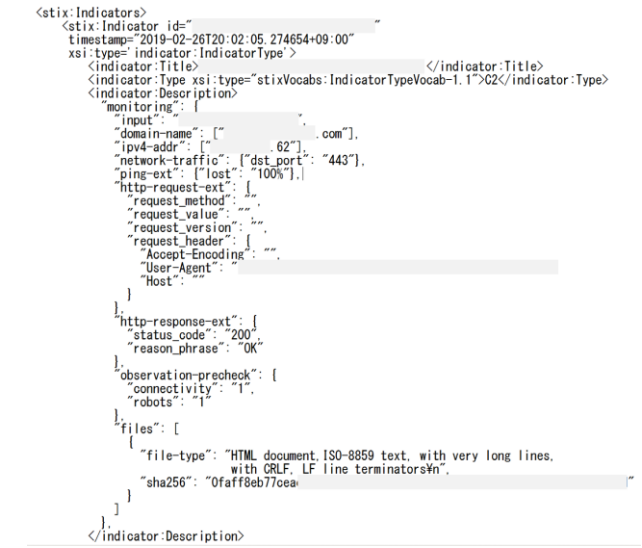

図 4 共有する STIX の例（一部抜粋）

への応答有無，緑線が PING の反応有無，および紫線が robots.txt の存在有無を意味している．また，実線が HTTP 応答，PING 反応，および robots.txt が存在したこと，破線が存在しなかったことを意味しており，これにより接続先の状態や接続先間の状態の関係等を視覚的に確認できるようにした．

4.3.2 共有部

共有部では，各システムで解析・観測した結果や分析部で分析した結果を共通フォーマットで共有する．今回共通フォーマットとして STIX 1.x [17]，共有に用いるプロトコルとして TAXII 1.x [18] を選択した．この際，TAXII サーバとしては，Soltra [19] を用いた．

また，共有部を用いて共有する STIX の例を図 4 に示す．図 4 に示した例は，継続観測システムの観測結果を STIX 1.x の形式に載せたものである．この際，自由記述が可能な Description フィールドに観測結果を JSON 形式で記載している．monitoring キー以下の input に URL，domain-name に FQDN，ipv4-addr に当該ドメインの A レコードという形で接続先の情報を記載している．また，dst_port にポート番号，User-Agent に観測時の User-Agent 等，観測時の設定項目についても記載している．さらに，他のフィールド内にステータスコード，HTTP GET の結果得られたコンテンツのファイルタイプや SHA256 ハッシュ値，PING 応答の有無，および robots.txt の有無等を観測結果として記載している．

このようにして，脅威情報交換の共通フォーマットを活用しつつ，PF を構成する各システムにおける解析・観測結果の即時的な共有を図る．

表 1 観測期間中のステータスコードの割合

ステータスコード	観測数	割合（%）
応答なし	2,409,786	87.8126371
404	199,305	7.2626771
200	109,019	3.9726540
403	15,668	0.5709421
301	9,941	0.3622502
500	367	0.0133735
302	103	0.0037533
408	26	0.0009474
503	20	0.0007288
502	1	0.0000364
合計	2,744,236	100.0000000

表 2 観測期間中のステータスコードの遷移

遷移前	遷移後	回数
200	502	1
301	503	15
302	404	2
404	408	1
408	404	1
502	200	1
503	301	15

5. 観測と分析

5.1 要旨

今回の実験では，4 章で述べた 3 システムのプロトタイプを実装し，2018 年 12 月から 2019 年 2 月の期間運用した．この中でマルウェアからの不審接続先の抽出，不審接続先の継続的な観測, および観測結果の ICT-ISAC の TAXII サーバを介した組織間での共有が可能となり, 3.2 節の要件を満足していることを確認した．また，観測・共有したデータについて，実施した観測の項目ごとに分析するとともに，下記 2 点の観点から活用可能性を検証した．

- ブラックリストの管理
- 攻撃者のアトリビューション

なお，今回の実証実験では，我々が独自に入手した検体（主に RAT）から接続先解析システムを用いて抽出した接続先と AlienVault OTX から選出した IOC の合計 660 件を観測対象とした．AlienVault OTX の IOC に関しては，記述欄を参照し, マルウェア名や APT グループ名が含まれているものを中心に選出している．さらに, Alexa が公開しているアクセス数 Top100 万サイトに含まれるものは，過検知の可能性があるため除外している．

次の節において，上記の手順で抽出した 660 件に対する当該期間中の観測結果と上述の活用可能性について述べる．

5.2 観測結果

5.2.1 ステータスコード

観測対象に HTTP GET を実施した際のステータスコードの割合を表 1 に示す．約 87.8%で応答がなく，次点が 404（Not Found）の約 7.2%であり，合計約 95%の期間非稼動状態であった．これは，悪性サイトの多くが短命であるという文献 [20] における観測と同様の結果であった．また，観測対象のうち 551 件（約 83.4%）は一度も応答がなく，観測開始時点で既に廃棄されていた，あるいは生存期間が極めて短いものであった等の可能性が考えられる．このことから，攻撃者の挙動を観測するという観点からは，いち早く不審な URL を発見し観測を行うのが望ましいと言える．また，ブラックリストによる通信遮断の観点からは，一度ブラックリストに登録されたものでも，その多くが破棄されるため，不要なサイトをリストから削除し，リストの肥大化を抑制するのが望ましいことが言える．

次に，観測期間中に見られたステータスコードの遷移について，遷移前のステータスコード，遷移後のステータスコード，および観測された回数を表 2 に示す．

503（Service Unavailable）から 301（Moved Permanently）に遷移した例では，3 サイトが同時期に 503→301→503 に遷移しており, かつ 301 の期間中は同等のコンテンツ（web シェルのパスワードフォーム）が配置されていた．このことから，何らかの攻撃であった可能性があるが断定には至らなかった．404（Not Found）から 302（Found）に遷移した例では，休止状態のサイトを一時的に攻撃のリダイレクトに活用したのではないかと推察されるが，今回の実装ではリダイレクト先まで追っていないため，断定するに至らなかった．このように，断定には至らなかったものの，幾つか不審な遷移が観測された．特に前者の例は，同等の遷移が同時期に生じていることから，同じ攻撃によるものである可能性があり，遷移情報を用いることによる攻撃者のアトリビューションの可能性があると言える．

以上のように，応答を用いたブラックリスト管理可能性や遷移情報を用いたアトリビューション可能性が確認できた．今後は，リダイレクト先の追跡等の機能拡充等をした上で鮮度の高い接続先も含めて観測を継続する予定である．

5.2.2 コンテンツ

ここでは，観測対象に HTTP GET を実施した際に，返却されたコンテンツについて述べる．まず，コンテンツのハッシュ値を比較したところ，同等のコンテンツが複数の接続先で観測された（表 3）. その多くは, 空のファイル（#11），Web サーバ・CMS のデフォルトトップページ（#2，#12，#13 等），Apache 等に用意された Not Found を示すページ（#3，#5，#6 等）等，既に利用されていないものを示すコンテンツだった．また，#7 は，あるレンタルサーバの Not Found を示すページであり，過去に特定のキャンペーンで用いられた URL 群が紐付いていた．これらは既に攻撃に利用されていないページであり，ブラックリストから削除するか否かの判断材料になると推察される．

また, #4 は, 図 5 に示すようなシンクホール化された旨を記載したページであり，これもブラックリストから削除するか否かの判断材料になりうる情報であると言える．

表 3 複数の接続先に紐付いたコンテンツ

#	コンテンツの SHA256 ハッシュ（先頭 32 字）	紐付いた接続先数
1	132fcc07495b5d5a1d921e8a11d9a593*	2
2	370be45f65276b3b8de42a29adfb1220*	3
3	46f105d18a3321e7b3422513c1e68d82*	2
4	56e6968a127729565d6170d784e60bb5*	7
5	70c65bd0e084398a87baa298c1fafa52*	4
6	7da7df6b2ae25a2b32a494dacea2c51b*	3
7	aa64e22b9d64df3b91b0d61f263f5ba4*	2
8	b42e9ce5a8a3df69af95b1f516139db7*	2
9	c9f593b156a25a319c453cea92f94d94*	4
10	e36ebeffa3a0b9340b8f6a938617062f*	2
11	e3b0c44298fc1c149afbf4c8996fb924*	9
12	e6134491cb1cd3e211b94d20b48482ca*	2
13	2c3adc6b6fb69d3a4e7b75b64e913dc9*	3
14	38ffd4972ae513a0c79a8be4573403ed*	2
15	5b80b1566219a6c3321b14127ebae23f*	2
16	9278d16ed2fdcd5dc651615b0b8adc6b*	2
17	9ec2f0698f1c3497de39a192dd1c3f3e*	2
18	9f89814b48fc3249bf67a8a6e4439d97*	3
19	c5b7c193086290b978c98965e661f3b5*	2
20	dc1d54dab6ec8c00f70137927504e4f2*	3
21	6de80ca19e2cfba24c73fd498c3cbf0e*	3

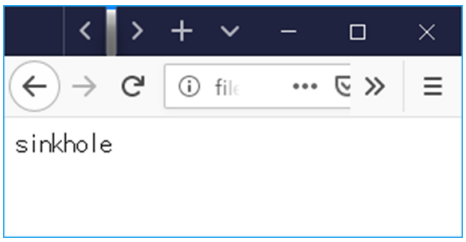

図 5 シンクホール済ページの例

さらに，#19 は，ある組織のページを模したつくりになっており，同コンテンツに紐付く 2 つの接続先は，過去に同等のマルウェアを配布していたと報告のあるものであった．このことから両接続先は，同じ攻撃者や攻撃グループが活用している可能性があり，コンテンツを用いることによる攻撃者のアトリビューションの可能性があると言える．

上記のように，コンテンツを利用したブラックリストの管理や攻撃者のアトリビューション等，幾つかのセキュリティオペレーションへの活用可能性が確認できた．

5.2.3 その他

PING 応答については，幾つかの接続先において，一定期間のみ応答があり，それ以外の期間は応答なしという事象が確認されている．これらは，攻撃の準備に際して，攻撃者のインフラが変動した結果と推察される．本事象を攻撃の予兆と捉えることによるセキュリティオペレーションへの活用を検討していく．

また，前述のように複数の国にエージェントを設置したものの，今回は国毎に応答を変える接続先は観測できなかった．同様に，robots.txt 由来の変動も見られなかった．この要因のひとつとして，観測数やエージェントを設置した国の数が多くないことが挙げられる．今回は，本節の情報がブラックリスト管理やアトリビューションに寄与することは確認できなかったものの，今後も観測数を拡大した上で，引き続き同観点での分析を行う．

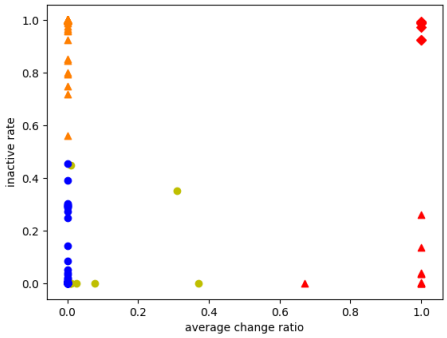

図 6 非稼働期間の割合とのコンテンツの平均変化率

6. 議論

6.1 活用先

ここでは，サイバー攻撃解析共有 PF における接続先の抽出結果や観測結果の活用先について検討する．

接続先解析システムで抽出した不審接続先を機械可読な形で共有することにより，ブラックリスト拡充やその自動化が期待できる．加えて，継続観測システムでの定期的な観測結果も共有することにより，各不審接続先の状態（稼動状態，休止状態，シンクホール等）に基づいたブラックリストの更新の判断を支援できると期待できる．また，先に述べたように，不審接続先の変化に応じて関連するマルウェア検体を解析することにより，解析網羅性の向上につながる可能性もある．なお，今回観測したデータは，先述の通り MWS データセットの一部として提供している．

6.2 サイトの分類

提案 PF は，前述の通り観測対象サイトの稼働状態やコンテンツの変化に着目してブラックリストの更新支援等を図る．他方で，稼働状態や変化をすべて人手で確認することは現実的ではない．そこで，本節では，稼働状態と変化に着目したサイトの分類可能性を検討する．検討にあたり，サイト毎の非稼働率とコンテンツの平均変化率を図 6 にプロットした．なお，それぞれの値は下記の（式 1）と（式 2）で導出した．ここで，変化率は HTTP GET への応答に対して fuzzey hash の一種である ssdeep を用いてハッシュ値を算出し，変化前後の差分を取ることで change ratio として導出した．

$$y = \frac{inactive\ \ period}{active\ \ period + inactive\ \ period} \quad \text{(式 1)}$$

$$x = \begin{cases} 0\ \ (the\ \ number\ \ of\ \ change = 0) \\ \dfrac{change\ \ ratio}{the\ \ number\ \ of\ \ change}\ \ (otherwise) \end{cases} \quad \text{(式 2)}$$

図から大きく 5 カテゴリに分類可能なことが読み取れる．

1. 最左下：非稼働率=0，平均変化率=0（丸，青）

観測期間中常に稼働しており，かつコンテンツの変化も無いものがここにあてはまる．具体的にはホスティングサーバのデフォルトページやシンクホールが含まれていた．また，今回は観測対象外だが多くの良性サイトも本カテゴリに含まれると推察される．

2. 左下：非稼働率=0，平均変化率<0.5（丸，黄）
観測期間中常に稼働しており，かつ少し変化しているものがここに当てはまる．例えば，時刻を含むページにおいて時刻のみ変化したようなものが観測された．
3. 左上：非稼働率<0.5，平均変化率<0.5（三角，橙）
ここには，観測期間中一度も稼働していないものときわめて生存期間が短くかつコンテンツが 1 種類のみで変化率を算出できなかったものが含まれる．このうち，後者はサイトが非稼働状態から稼働状態に変化したものであり，攻撃の兆候である可能性がある．
4. 右下：非稼働率<0.5，平均変化率>=0.5（三角，赤）
稼働率が高く，その中で変化がありかつ変化率が大きい者が含まれる．具体的には，普段はホスティング会社の domain reserved（コンテンツが置かれていない状態）のページや良性サイトを模したページで，一定期間それ以外のコンテンツが置かれていたものであった．
5. 右上：非稼働率>=0.5，平均変化率>=0.5（菱形，赤）
本カテゴリには，短期間各種 Web サーバ（IIS，nginx 等）のデフォルトページが出現した後，別のコンテンツに置き換わったものが含まれていた．これらは，攻撃者が疎通確認を行った後に本命のコンテンツを設置した現象が観測されたものと推察される．

上記より，非稼働期間の割合とコンテンツの変化率に着目することでサイトを 5 カテゴリに分類できることが確認できた．本文類の活用について今後も検討を続けていく．

6.3 観測における設定項目

今回は，選定した 660 の接続先に対し，エージェント環境の計算機性能等も考慮して 4 時間毎に観測を実施した．ここで，最も早いものは 1 時間程度でその性質を変えるという報告 [3] もあり，観測間隔については検討の余地がある．一方で，今回は，時間経過によって状態変化が発生する接続先数が多くなかった．この要因は，鮮度の低い検体から発せられた比較的安定状態にある接続先を観測しており，かつ接続先の個数も多くはなかったためと考えられる．

また，攻撃者のグルーピングを行うに際しては，より多くの対象を観測し，観測対象のカバレッジを確保することが重要であるが，今回観測した 660 件ではカバレッジが十分とは言えない．

上記課題を解決するため，エージェントの性能拡充も含めた観測間隔短縮の検討が必要であると考えられる．加えて，観測対象の大規模化や鮮度の確保が望ましいと言える．

6.4 クローキング

攻撃者がリサーチャによる悪性サイトの解析を妨害する手法のひとつに，攻撃対象にのみ悪意のあるサイトを表示し，リサーチャを含むそれ以外の訪問者には無害なサイトを表示するクローキングがある．具体的な手法のひとつに，ターゲットとしている特定の国に対してのみ悪意のあるコンテンツを返却するという手法がある．継続観測システムは，前述の通り複数の国に観測エージェントを配置しているため，本手法に対しては耐性を有していると言える．ただし，他の手法としてリサーチャの有する IP アドレスをブラックリスト化し，当該アドレスからの通信には無害なサイトを表示するというものがある [21]．この手法のように，継続観測システムのエージェント群がブラックリストに加えられた場合，観測に失敗する可能性がある．また，標的型攻撃においては，マルウェアに感染した端末の IP アドレスに対してのみ悪意のあるコンテンツを返す手法の存在も示唆されている [22]．現状のサイバー攻撃解析共有 PF はマルウェアに感染する端末（接続先解析システム）と継続観測を行う端末（継続観測システム）の IP アドレスは異なるため，同手法によっても，観測を妨害されうる．

前者に対しては観測エージェントの IP アドレスの定期的な変更，後者に対しては接続先解析システムをフォワードプロキシとした感染端末と観測端末の IP アドレスの統一が有効であると考えられる．耐クローキング性を向上する機能として，これらについても今後検討していく．

6.5 研究倫理

今回の観測では，インターネットに公開されているホストに対して，HTTP GET や PING のような通常利用の中で発生しうる通信を行っており，悪意を持った通信は実施していない．また，前述したように，Alexa ランクの高いサイトをホワイトリストとして活用することにより，可能な限り良性のサイトへのスキャンを避けていると共に，各ホストに対して一定間隔をあけて通信を行うことにより，過剰な負荷を避けている．さらに，スキャン前に robots.txt を確認し，クローラを拒否する記載があった場合は，スキャンを行っていない．

7. 関連研究

サイバー攻撃解析共有 PF について，本稿で述べた内容に関連するものとして，以下に示す技術・研究がある．

まず，接続先解析システムのように，マルウェアから不審接続先を抽出する手法としては，マルウェアの動的解析がある．動的解析システムとしては，前述の Cuckoo Sandbox に加え，Ether [23]，CWSandbox [24]，および TTAnalyzer [25] 等がある．今回は，Cuckoo Sandbox を利用したが，これらのシステムを含む他の解析システムを利用することや組み合わせることも可能である．

また，不審接続先について継続的な観測を行い，その特性を報告する研究も幾つか存在する．文献 [3] では，約 43,000 件のマルウェアダウンロードサイトを 1.5 年にわた

って観測し，何度も生死を繰り返すような特性が見られたこと等が報告されている．同等の特徴は，文献 [4] においても報告されている．また，文献 [5] では，一度攻撃に利用したボットネットを別の攻撃キャンペーンで再利用するというようなインフラの再利用があることが報告されている．こうした報告の存在は，不審サイトの特徴を捉えるには，継続的な観測が重要であることを示唆している．一方で，各研究ではそれぞれで観測を行うシステムを構築しており，かつ観測対象の収集を人手で行う等，観測に至るまでに多くの前準備を行っている．本項で述べた PF は，接続先解析システムとの連携により，観測対象の収集を支援すると共に，観測結果を共有することにより，組織毎でのシステム構築等を不要にしつつ，分析を実施するに資する情報を自動で提供するものである．

情報共有基盤についても，前述のように整いつつある．Facebook ThreatExchange [10]，Defense Industrial Base Cybersecurity Information Sharing Program [11]，および Automated Indicator Sharing [12] は，それぞれの加入組織間で信頼性の高い情報を共有する枠組みである．これらの枠組みとは対照的に，AlienVault OTX [13] や IOC Bucket [14] のように，IOC を共有するパブリックな枠組みもある．ただし，これらは先述したように，専門家が分析した情報であることから，速報性にやや欠ける点がある．本稿で述べた内容は，解析，観測，および共有までを自動で行うことにより，速報性の高い情報を提供し，上記の枠組みの不足部分を補完するものである．

8. おわりに

本稿では，マルウェアから不審な接続先を抽出し，継続的に観測すると共に，観測結果を機械可読な形で共有することにより，攻撃の抑制や集団防御を可能とするサイバー攻撃解析共有 PF について述べた．また，同 PF のうち，不審接続先をマルウェアから抽出し，継続的に観測すると共にその結果を共有するまでのシステムに関して，設計と実装を述べた．また，同システムのプロトタイプを実装し，660 件の不審接続先を約 3 ヶ月間観測した結果，攻撃者のアトリビューションの可能性やブラックリストの管理といった同 PF の活用可能性が確認できた．

本稿では，PF の構成要素である 3 システムについて述べたが，今後も継続的に機能拡張を行っていく．また，今回の観測は，小規模なデータを用いたものに留まっているため，今後は，より大規模なデータセットを用いて観測を実施する予定である．

謝辞

本研究は，国立研究開法人情報通信研究機構事業「サイバー攻撃に関する解析作業」で実施したものである．本研究を進めるにあたって有益な助言と協力を頂いた関係各位に深く感謝申し上げる．

参考文献

[1] 荒木粧子，笠間貴弘，押場博光，千葉大紀，畑田充弘，寺田真敏：マルウェア対策のための研究用データセット～MWS Datasets 2019～，情報処理学会研究報告，Vol. 2019-CSEC-86, No. 8，pp. 1－8 (2019).
[2] Zhao, B., Z., H., Ikram, M., Asghar, H., Kaafar, M., A., Chaabane, A., and Thilakarathna, K.: A decade of mal-activity reporting: a retrospective analysis of internet malicious activity blacklists, in Proceedings of the 14th ACM Asia Computer Communication and Security (ASIA CCS '19), pp. 1－13 (2019).
[3] Tanaka, Y., Akiyama, M., and Goto, A.: Analysis of malware download sites by focusing on time series variation of malware, Journal of Computational Science, Vol. 22, pp. 301－313 (2017).
[4] 須藤年章：悪性サイトドメインの長期観測結果に基づくブラックリスト利用の有効性に関する一考察，コンピュータセキュリティシンポジウム 2013 論文集（CSS 2013），pp. 376－381 (2013).
[5] Chang, W., Mohaisen, A., Wang, A., and Chen, S.: Measuring Botnets in the Wild: Some New Trends, in Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (ASIA CCS '15), pp. 645－650 (2015).
[6] Unit 42: New Python-Based Payload MechaFlounder Used by Chafer, available from <https://unit42.paloaltonetworks.com/new-python-based-payload-mechaflounder-used-by-chafer/> (2019-06-27 accessed).
[7] ZDNet：カスペルスキー，日本を狙うサイバー攻撃を報告--米国政府の対応にも見解，入手先 <https://japan.zdnet.com/article/35111882/>（2019-07-24 アクセス）.
[8] 神薗雅紀，遠峰隆史，津田 侑，衛藤将史，星澤裕二，井上大介，吉岡克成，松本 勉：ループバックアドレスが返答されるドメインの定点観測によるマルウェアの活動予測，電子情報通信学会技術研究報告，Vol. 114，No. 489，pp. 376－381 (2015).
[9] ICT-ISAC：サイバー攻撃の防御に向けた情報共有基盤に関する実証事業について，入手先 <https://www.ict-isac.jp/news/news20180629.html> (2019-06-27 アクセス).
[10] Facebook: Facebook ThreatExchange Overview, available from <https://developers.facebook.com/programs/threatexchange/> (2019-06-27 accessed).
[11] DoD: Defense Industrial Base Cybersecurity Information Sharing Program, available from <https://dibnet.dod.mil/portal/intranet/> (2019-06-27 accessed).
[12] CISA: Automated Indicator Sharing (AIS), available from <https://www.us-cert.gov/ais> (2019-06-27 accessed).
[13] AlienVault: Open Threat Intelligence, available from <https://otx.alienvault.com/> (2019-06-27 accessed).
[14] IOC Bucket, available from <https://www.iocbucket.com/> (2019-06-27 accessed).
[15] Cuckoo Sandbox - Automated Malware Analysis, available from <https://cuckoosandbox.org/> (2019-06-27 accessed).
[16] INetSim: Internet Services Simulation Suite, available from <https://www.inetsim.org/> (2019-07-31 accessed).
[17] MITRE: Structured Threat Information eXpression (STIX™) 1.x Archive Website, available from <https://stixproject.github.io/> (2019-07-31 accessed).
[18] MITRE: Trusted Automated eXchange of Indicator Information (TAXII™) 1.x Archive Website, available from <https://taxiiproject.github.io/> (2019-07-31 accessed).
[19] Soltra, available from <https://www.soltra.com/en/> (2019-06-27 accessed).
[20] Akiyama, M., Yagi, T., Yada, T., Mori, T., and Kadobayashi, Y.: Analyzing the ecosystem of malicious URL redirection through longitudinal observation from honeypots, Journal of Computational Science, Vol. 69, pp. 155－173 (2017).
[21] Zeeuwen, K., Ripeanu, M., and Beznosov, K.: Improving Malicious URL Re-evaluation Scheduling Through an Empirical Study of Malware Download Centers, Proceedings of the 2011 Joint WICOW/AIRWeb Workshop on Web Quality (WebQuality '11), pp. 42－49 (2011).
[22] Mansoori, M., Welch, I., Choo, K., K., R., Maxion, R., A., and Hashemi, S., E.: Real-world IP and network tracking measurement study of malicious websites with HAZOP, International Journal of Computers and Applications, Vol. 39, pp. 106－121 (2017).
[23] Dinaburg, A., Royal, P., Sharif, M., and Lee, W.: Ether: Malware analysis via hardware virtualization extensions, in Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS '08), pp. 51–62 (2008).
[24] Willems, C., Holz, T., and Freiling, F.: Toward automated dynamic malware analysis using CWSandbox, Security Privacy, IEEE, Vol. 5, No. 2, pp. 32–39 (2007).
[25] Bayer, U., Kruegel, C., and Kirda E.: TTAnalyze: A tool for analyzing malware, in Proceedings of the 15th European Institute for Computer Antivirus Research Annual Conference (EICAR), (2006).