Web サイトへのマルウェア感染攻撃に用いられるボットネットの分析

八木 毅 †　　針生 剛男 †　　大崎 博之 ‡　　村田 正幸 §

†NTT セキュアプラットフォーム研究所
〒 180-8585　東京都武蔵野市緑町 3-9-11
{yagi.takeshi,hariu.takeo}@lab.ntt.co.jp

‡ 関西学院大学理工学部情報科学科
〒 669-1337　兵庫県三田市学園 2 丁目 1 番地
ohsaki@kwansei.ac.jp

§ 大阪大学大学院情報科学研究科
〒 565-0871 大阪府吹田市山田丘 1-5
murata@ist.osaka-u.ac.jp

あらまし　本稿では，Web サイトへのマルウェア感染攻撃において，Web サイトにダウンロードさせるマルウェアを攻撃者が配置するボットネットを調査した結果を報告する．本調査では，マルウェアが配置されたボットであるマルウェアダウンロードサイトの長期観測結果に基づいて，ボットネットの活動を分析した．さらに，マルウェアダウンロードサイトをブラックリスト化して攻撃を防御する際に，本調査結果に基づいてマルウェアダウンロードサイトの監視周期を制御する手法を示し，評価結果を報告する．

Analysis of Botnets Using Malware Infection Attacks on Websites

Takeshi Yagi†　　Takeo Hariu†　　Hiroyuki Ohsaki‡　　Masayuki Murata§

†NTT Secure Platform Laboratories, NTT Corporation
Midori-cho, Musashino-shi, Tokyo 180-8585, JAPAN
yagi.takeshihariu.takeo@lab.ntt.co.jp

‡Department of Informatics, School of Science and Technology, Kwansei Gakuin University
2-1 GAkuen, Sanda, Hyogo 669-1337, JAPAN
ohsaki@kwansei.ac.jp

‡Graduate School of Information Science and Technology, Osaka University
1-5 Yamadaoka, Suita 565-09871, JAPAN
murata@ist.osaka-u.ac.jp

Abstract　This paper reports our results of investigations about botnets which are used by attackers to host malware for malware infection attacks on websites. In the investigations, activities of botnets were analyzed by long-term monitoring of bots, on which malware had been located. These bots are called malware download sites. To detect the malware infection attacks by blacklisting the malware download sites, this paper indicates and evaluates a method to controls the monitoring interval of each malware download sites based on our results of botnets investigations.

1 はじめに

現在，Web 経由のサービスが広く普及しており，様々な Web サービスが多種多様な Web アプリケーションによって提供されている．しかし，多くの Web アプリケーションには脆弱性が存在し，Web サイトへの攻撃に悪用されている [1]．特に，攻撃された Web サイトが攻撃者によって自由に操作されて新しい攻撃の攻撃元としても使用されるという点で，マルウェア感染が攻撃の根源といえる [2]．近年では，Web サービス基盤という意味で，サービスプロバイダがセキュリティを確保することが要求されている．

2 章でも詳しく述べるように，サービスプロバイダが Web サイト群をマルウェア感染から保護する手法として，攻撃者がマルウェア感染のために設置したマルウェアダウンロードサイト (MDS)URL をブラックリスト化する手法 [5] が検討されている．この手法では，脆弱な Web アプリケーションを搭載した Web サーバ型ハニーポット [3, 4] で攻撃を収集して MDS の URL を特定し，当該 URL への通信をフィルタすることで，Web サイトをマルウェア感染から保護する．

一方，ブラックリストによる攻撃防御を回避する目的で，MDS 上のマルウェアは攻撃者によって一定期間後に別のサイトに移動され，新たな MDS が構築される．また，MDS 構築にはボットとして不正操作されている Web サイトが使用される場合が多い．ブラックリスト化された URL は，ドメインや IP アドレス単位で集約されてフィルタされる場合や，本来は正しいファイルが配置される場合が考えられる．このため，マルウェアが削除された元 MDS はブラックリストから直ちに除外する必要がある．従来，サービスプロバイダは，ユーザ申告があったサイトや，一定期間攻撃に使用されない MDS をブラックリストから除外する [10]．しかし，サービスプロバイダ視点からみると，マルウェア削除から URL 除外までの間，当該 URL へのアクセスが攻撃と誤検知される事象（ここでは False Positive（FP）と呼ぶ）が発生する．誤検知を防止するためには，MDS 上のマルウェアを確認するプローブを定期的に送信する必要がある．しかし，プローブが攻撃者に感知された場合，攻撃者は

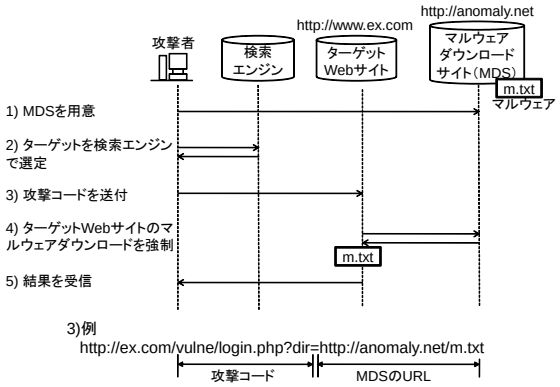

図 1: 攻撃手順

マルウェアを別サイトに移動して新たな MDS を構築し，攻撃を継続する．この際，サービスプロバイダ視点からみると，MDS をブラックリストに掲載する事象（ここでは True Positive（TP）と呼ぶ）が，FP や，MDS がブラックリストに掲載されない事象（ここでは False Negative（FN）と呼ぶ）に変化する．

そこで本稿では，MDS として使用されるボットを長期観測した結果を分析する．具体的には，Web サーバ型ハニーポットで発見した MDS を継続的に観測し，攻撃者の行動の特性を分析する．さらに，分析結果を攻撃防御に応用する手法を提示する．具体的には，攻撃者とサービスプロバイダの行動をモデル化し，MDS のブラックリスト掲載に関する状態遷移モデルを解析する．これにより，単純な観測では解明困難な MDS の潜在変化を明らかにし，FP を抑制しつつ TP を改善可能なプローブ送信周期を決定する．

2 Web サイトへの攻撃と防御手法

2.1 Web サイトへのマルウェア感染攻撃

Web サイトへの典型的なマルウェア感染攻撃 [7] では，以下の手順をとる（図 1）．

1. 攻撃者は，マルウェアを配置した MDS を用意する．
2. 攻撃者は，検索エンジン等を利用して，脆弱な Web アプリケーションを搭載した Web サイトをターゲットとして選定する．

3. 攻撃者は，ターゲット Web サイトに対して，MDS からマルウェアをダウンロードするよう，脆弱な Web アプリケーションを利用する攻撃コードを HTTP リクエストメッセージに記述して送信する．

4. ターゲット Web サイトは，MDS からマルウェアをダウンロードして実行する．

5. ターゲット Web サイトは攻撃者に HTTP レスポンスメッセージを送信する．

2.2 マルウェア感染攻撃に対する防御手法

この攻撃への対策には，サーバでの対策とネットワーク上での対策がある．前者にはアンチウィルスソフトの適用が挙げられるが，Web サイトに使用されるマルウェアは悪意判定が困難で検知率は低い [8]．一方，ネットワーク上で Web サイト群への攻撃を効率的に防御する手法として，Web サイトから MDS へのアクセスをフィルタする手法 [5] がある．この手法では，Web サイトへの攻撃を収集するおとりシステムである Web サーバ型ハニーポットの通信内容から MDS の URL を特定し，ブラックリストとして Firewall 等に入力することで，Web サイトから MDS へのアクセスをフィルタする．MDS の URL は公開ブラックリスト [9] にも掲載されており，ログ検査にも使用される．

3 MDS の長期実態調査

3.1 MDS の挙動とブラックリストの精度

MDS 上のマルウェアは攻撃者や Web サイト管理者により削除される．ここで，MDS を管理する際に発生する 4 つの事象を説明する．MDS ではないサイトがブラックリストに掲載されない事象（ここでは True Negative（TN）と呼ぶ）において，当該サイトにマルウェアが配置されると FN が発生する．FN 発生時に，当該 MDS が発見されてブラックリストに掲載されると TP が発生する．TP 発生時に，当該 MDS 上のマルウェアが削除された場合，当該サイトへのアクセスが攻撃と誤検知される FP が発生する．

このように，MDS の挙動とブラックリストの攻撃検知精度には依存関係があるため，MDS の挙動に基づく対策を講じる必要がある．

3.2 実態調査の概要

MDS として使用されるボットの挙動を調査するための実態調査を実施した．本調査では，Web サーバ型ハニーポット 34 台を *.com*，*.net*，*.org*，*.jp*，*.ru*，*.cn*，*.us*，*.br* など，幅広いドメイン空間に配置した．さらに，1 日に 1 回各 MDS にプローブを送信し，MDS 上のマルウェア配置期間を観測した．本調査は 2012 年 4 月 20 日から 2013 年 2 月 28 日まで実施し，攻撃を 372,100 件，MDS を 574 サイト確認した．本調査では，マルウェアが配置された MDS を活動中の MDS と呼び，マルウェアが削除された MDS を休止中の MDS と呼ぶ．なお，約 24.1% の MDS はプローブを送信した翌日にはマルウェアが削除されていた．このため，攻撃者がプローブを感知した可能性が高い．一方，他の MDS においても，Web クライアントのマルウェア感染の原因となる悪性サイトでプローブ監視が実施されているという報告があるため，頻度は低いがプローブ監視は実施されていると考えられる．

3.3 実態調査結果

図 2 に，休止中の MDS のうち活動を再開した MDS の割合を示す．表 1 には，同期間中に発見した MDS の活動休止回数と活動休止期間の統計情報を示す．さらに，発見した MDS 数と活動している MDS 数の時系列を図 3 に，MDS の平均活動期間の時系列を図 4 に示す．

図 2 に示すように，平均で約 14% の元 MDS 上にマルウェアが再配置された．また，同一のマルウェアが再配置される確率は約 7% であった．なお，最大で 28% の元 MDS 上にマルウェアが再配置される月も確認できた．MDS の活動休止回数の平均値は，表 1 に示すように，約 2.6 回であった．この際，活動休止期間が 1 日である MDS が存在する一方，最大で 292 日活動を休止した MDS も存在した．本調査では，図 3

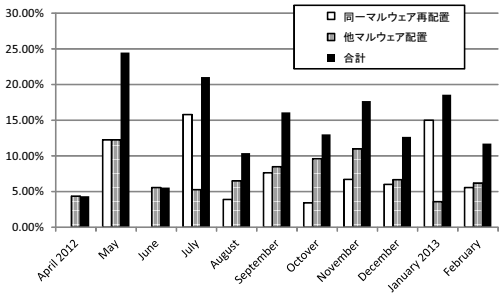

図 2: 活動を休止した MDS の再使用率

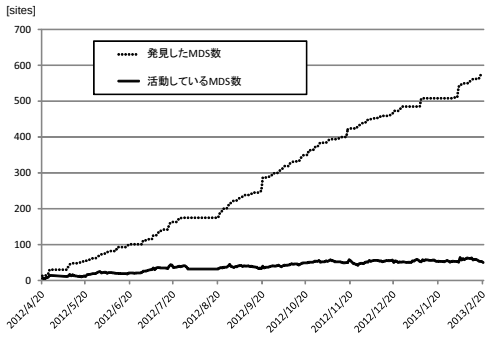

図 3: 発見した MDS 数と活動中の MDS 数

表 1: MDS の活動休止期間

	Min.	Ave.	Max.
マルウェア削除回数	1	2.66	20
活動休止期間 [日]	1	39.91	292

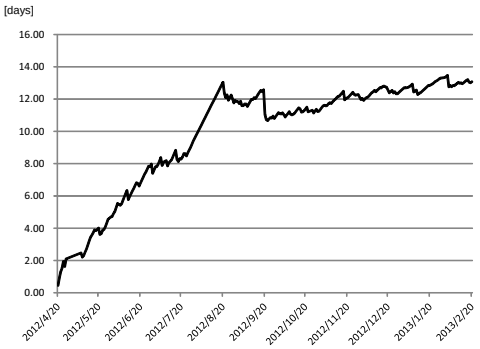

図 4: MDS の平均活動期間

に示すように，定常的に MDS を発見できており，活動している MDS の平均活動期間は，図 4 に示すように，ほぼ一定値となり，最終観測日の段階で 13.08 日となっていた．

以上から，MDS として使用されるボットに対し，攻撃者は定期的にマルウェアの削除と再配置を実施していると考えられる．

4 攻撃防御への応用

4.1 最適なプローブ送信周期の解析

MDS の挙動分析に基づく対策の一例として，MDS に対する最適なプローブ送信周期を決定する．なお，通常，攻撃者は攻撃を送信する際にもボットを使用するが，本解析では MDS として使用されるもののみをボットと表記する．

4.1.1 解析モデル

本解析モデルは，図 5 に示すように，単一の攻撃者 A，サービスプロバイダに相当する単一の被攻撃者 V，N 台のボット B_1,B_2, ...,B_N によって構成される．なお，事象はポアソン過程に従って発生すると仮定する．

1. A は，一定の攻撃レート α で，V に対して攻撃を実施すると仮定する．
2. A は，攻撃に使用している B_i を一定のレートで停止する．ここでは，A がレート η で B_i を停止すると仮定する．また，A は，使用していない B_i を用いた攻撃を一定のレートで開始する．ここでは，A がレート ζ で B_i を用いた攻撃を開始すると仮定する．
3. V は，一定の検知レート β で，ブラックリスト未登録の B_i を使用した攻撃を検知し，B_i をブラックリストに登録すると仮定する．

A の使用ボットを $\boldsymbol{b} = (B_i)\ (1 \leq i \leq N)$ と表記する．B_i が使用されている時は $B_i = 1$，未使用時は $B_i = 0$ とする．V のブラックリストを $\boldsymbol{l} = (l_i)(1 \leq i \leq N)$ と表記する．B_i がブラックリストに掲載済みの時は $l_i = 1$，未掲載時は $l_i = 0$ とする．V のプローブ送信レートを γ と表記する．V は，$l_i = 1$，すなわち，B_i をブラックリストに掲載済みの時，B_i にレート γ でプローブを送信する．このとき，A は，

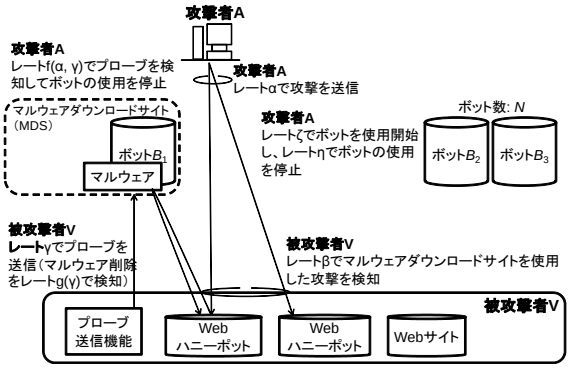

図 5: 解析モデル

$B_i = 1$，すなわち，攻撃に使用している B_i が受信パケットを監視し，プローブを感知した際に B_i の使用を停止する．B_i は，攻撃パケットとプローブを受信するため，攻撃が多い場合，プローブ感知確率は低下する．このため，A によるプローブ感知レートを $f(\alpha,\gamma)$ と表記する．V の攻撃停止ボット検知レートを $g(\gamma)$ と表記する．V が，$l_i = 1$，すなわち，ブラックリスト掲載済みの B_i に対してレート γ でプローブを送信した時に，$B_i = 0$，すなわち，B_i を A が未使用だった場合，レート $g(\gamma)$ で B_i による攻撃が停止していることを検知する．

4.1.2 状態遷移レートの導出

システムの状態は$\boldsymbol{b}$，$\boldsymbol{l}$によって表現できる．ある状態 $(\boldsymbol{b},\boldsymbol{l})$ から状態 $(\boldsymbol{b'},\boldsymbol{l'})$ への状態遷移レートを $\lambda_{(\boldsymbol{b},\boldsymbol{l})(\boldsymbol{b'},\boldsymbol{l'})}$ と表記する．まず，状態 $(\boldsymbol{b},\boldsymbol{l})$ から状態 $(\boldsymbol{b'},\boldsymbol{l})(\boldsymbol{b} \neq \boldsymbol{b'})$ への状態遷移レート，つまり，A が攻撃に使用するボットを追加削除する場合のレートを考える．A はレート ζ で攻撃に使用するボットを追加するため，

$$\lambda_{(\boldsymbol{b},\boldsymbol{l})(\boldsymbol{b'},\boldsymbol{l})} = \zeta \quad (|\boldsymbol{b}| = \sum B_i = \sum B'_i - 1) \quad (1)$$

となる．また，A はレート η で攻撃に使用しているボットを停止するため，

$$\lambda_{(\boldsymbol{b},\boldsymbol{l})(\boldsymbol{b'},\boldsymbol{l})} = \eta \quad (|\boldsymbol{b}| = \sum B_i = \sum B'_i + 1) \quad (2)$$

となる．ただし，$B_i = l_i = 1$，すなわち，攻撃に使用しているボットがブラックリストに掲載されている時のみ，A は，プローブを感知した際にもボットの使用を停止するため，

$$\lambda_{(\boldsymbol{b},\boldsymbol{l})(\boldsymbol{b'},\boldsymbol{l})} = \eta + f(\alpha,\gamma) \quad (|\boldsymbol{b}| = \sum B_i = \sum B'_i + 1, B_i = l_i = 1) \quad (3)$$

となる．次に，状態 $(\boldsymbol{b},\boldsymbol{l})$ から状態 $(\boldsymbol{b},\boldsymbol{l'})$ $(\boldsymbol{l} \neq \boldsymbol{l'})$ への状態遷移レート，つまり，V がブラックリストを更新する場合のレートを考える．本解析における仮定より，単位時間において，たかだか単一の B_i に対するブラックリスト変更しか発生しないことに注意する．まず，V がボット B_i をブラックリストから削除する場合，すべてのボットは等価であり，V が B_i からの攻撃停止を検知するレートが $g(\gamma)$ であることから，

$$\lambda_{(\boldsymbol{b},\boldsymbol{l})(\boldsymbol{b},\boldsymbol{l'})} = g(\gamma) \quad (\boldsymbol{l} \neq \boldsymbol{l'}, l_i = 1, l'_i = B_i = 0) \quad (4)$$

となる．逆に，V が B_i をブラックリストに掲載する場合，すべてのボットは等価であり，また，V が B_i からの攻撃を検知するレートが β であることから，

$$\lambda_{(\boldsymbol{b},\boldsymbol{l})(\boldsymbol{b},\boldsymbol{l'})} = \beta \quad (\boldsymbol{l} \neq \boldsymbol{l'}, l_i = 0, l'_i = B_i = 1) \quad (5)$$

となる．最後に，遷移が発生しないレートは，

$$\lambda_{(\boldsymbol{b},\boldsymbol{l})(\boldsymbol{b},\boldsymbol{l})} = \mathrm{e}^{-(\sum \lambda_{(\boldsymbol{b},\boldsymbol{l})(\boldsymbol{b'},\boldsymbol{l})} + \sum \lambda_{(\boldsymbol{b},\boldsymbol{l})(\boldsymbol{b},\boldsymbol{l'})})} \quad (\boldsymbol{b} \neq \boldsymbol{b'}, \boldsymbol{l} \neq \boldsymbol{l'}) \quad (6)$$

となる．それ以外の状態遷移レートはすべて 0 となることに注意されたい．

B_1 が攻撃に使用される際に B_1 と B_2 に着目した状態遷移図の一部を図 6 に示す．B_1 が攻撃に使用されていない時，式 (1) に従ってレート ζ で，B_1 の使用が開始される．B_1 が攻撃に使用されているがブラックリストに未掲載の時，式 (5) に従ってレート β で，V が B_1 を使用した攻撃を検知して B_1 をブラックリストに掲載するか，式 (2) に従ってレート η で，B_1 の使用が停止される．ただし，B_1 の使用が停止される状態遷移は，B_1 が攻撃に使用されていてブラックリストに掲載されている時は，式 (3) に従って

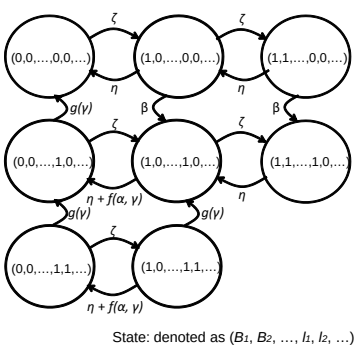

図 6: 状態遷移例

レート $\eta + f(\alpha, \gamma)$ で発生する．B_1 が攻撃に使用されていないがブラックリストに掲載されている時，式 (4) に従ってレート $g(\gamma)$ で，B_1 がブラックリストから削除される．

4.1.3 数値例と評価指標の導出

本解析モデルのマルコフ連鎖を用いて各状態の定常分布確率を算出することで，γ に対する TPR(TP Rate)，TNR(TN Rate)，FPR(FP Rate) および FNR(FN Rate) を算出できる．なお，攻撃に使用されるボット数は，図 3 に示すように一定数となることが推測されるため，本解析では 1 とした．このとき，攻撃に使用されている B_i の停止と，新たに選択された $B_j (i \neq j)$ を用いた攻撃の開始が同時に発生するため，

$$\zeta = \eta \quad (|\boldsymbol{b}| = \sum B_i = \sum B_j = 1) \tag{7}$$

となる．また，前述の通り，プローブ感知レートは，攻撃数の増加に対して低下するため，

$$f(\alpha, \gamma) = \frac{\gamma}{\alpha} \tag{8}$$

とする．なお，攻撃停止ボット検知レートは，被攻撃者がプローブの応答を確認することから，

$$g(\gamma) = \gamma \tag{9}$$

とする．

本解析では，ボット間で遷移レートに差異が発生しないため，B_i がブラックリストに掲載されている際に B_i が MDS である確率を示す PPV(Positive Predictive Value) と，B_i が MDS ではない際にブラックリストから除外されている確率を示す NPV(Negative Predictive Value) を，以下の式で定義して評価値として検討できる．ここで，全状態の集合を S とし，状態 $(\boldsymbol{b}, \boldsymbol{l})$ の定常分布確率を $P(\boldsymbol{b}, \boldsymbol{l})$ と規定する．

$$\begin{aligned} PPV &= \frac{\sum TPR}{\sum TPR + \sum FPR} \qquad (10) \\ \sum TPR &= \textstyle\sum_{\{(\boldsymbol{b},\boldsymbol{l}) \in S | B_i = l_i = 1\}} P(\boldsymbol{b}, \boldsymbol{l}) \\ \sum FPR &= \textstyle\sum_{\{(\boldsymbol{b},\boldsymbol{l}) \in S | B_i = 0 \cap l_i = 1\}} P(\boldsymbol{b}, \boldsymbol{l}) \end{aligned}$$

$$\begin{aligned} NPV &= \frac{\sum TNR}{\sum TNR + \sum FNR} \qquad (11) \\ \sum TNR &= \textstyle\sum_{\{(\boldsymbol{b},\boldsymbol{l}) \in S | B_i = l_i = 0\}} P(\boldsymbol{b}, \boldsymbol{l}) \\ \sum FNR &= \textstyle\sum_{\{(\boldsymbol{b},\boldsymbol{l}) \in S | B_i = 1 \cap l_i = 0\}} P(\boldsymbol{b}, \boldsymbol{l}) \end{aligned}$$

さらに，全ボットで発生している事象が TP または TN となる状態の定常分布確率の総和 O_p も評価値として検討できる．

$$O_p = \textstyle\sum_{\{(\boldsymbol{b},\boldsymbol{l}) \in S | B_i = l_i\}} P(\boldsymbol{b}, \boldsymbol{l}) \tag{12}$$

各評価値を最大化する γ を算出するためには，ボット数 N や，同一の MDS が使用された攻撃数 α の監視に加え，η と β を推定する必要がある．次節では，η と β の推定方法を説明する．

4.2 実態調査に基づくパラメータ推定

3 章に記述した実態調査において収集したデータを用いて，η と β を推定する．なお，本調査では同一 MDS を使用した攻撃を最短で 1 秒間隔で確認したため，本稿における解析の単位時間を分オーダとした．

MDS の活動期間は指数分布に従う傾向がある [6]．3 章に記述したとおり，平均活動期間は 13.08 日であったことから，分単位に MDS 上のマルウェアが別のサイトに再配置されるレートは次式で算出できる．

$$\eta = 1 - \mathrm{e}^{-\frac{1}{13.08 \times 24 \times 60}} = 0.53 \times 10^{-4} \tag{13}$$

本調査では，1 台の Web サーバ型ハニーポットにおいて同一の MDS を用いた攻撃を平均 22

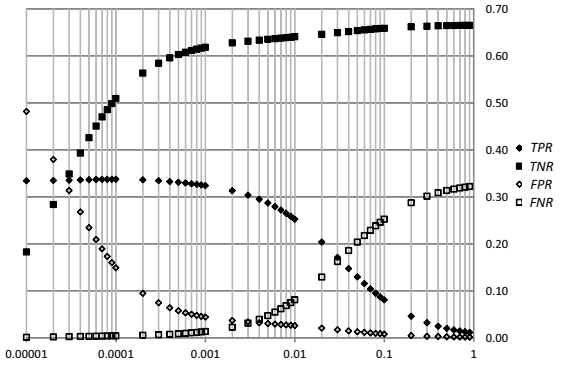

図 7: TPR, TNR, FPR, FNR と γ $(N = 3)$

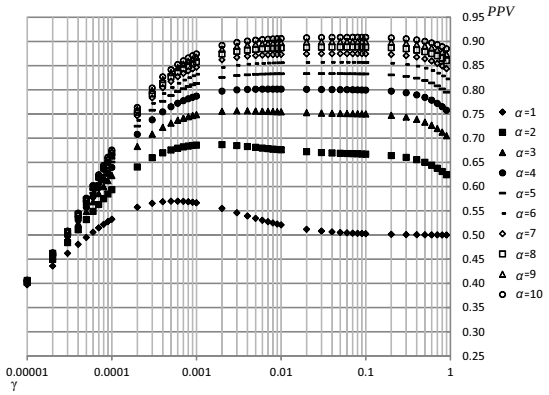

図 8: 各 α における PPV と γ $(N = 3)$

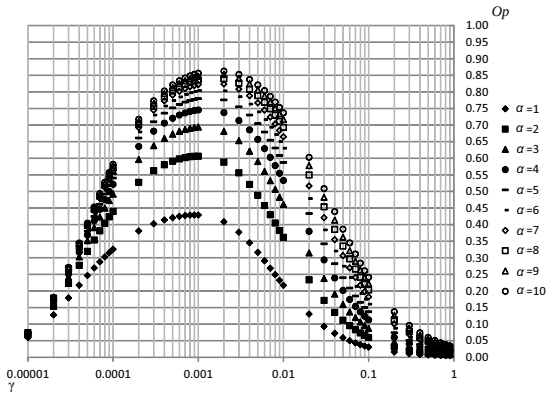

図 9: 各 α における O_p と γ $(N = 3)$

日間隔で受信する現象を確認した．攻撃の到着間隔がポアソン過程に従うと仮定し，Web サーバ型ハニーポット台数を x とし，各 Web サーバ型ハニーポットの攻撃検知レートを y とすると，β は次式で算出できる．

$$\beta = \sum_{i=1}^{x} y_i \quad = \quad x(1 - \mathrm{e}^{-\frac{1}{22\times 24\times 60}}) \quad (14)$$

ここで，Web サーバ型ハニーポット数を，既存の攻撃調査で用意されていた 100 台 [4] と仮定すると，$\beta = 0.32 \times 10^{-2}$ となる．

なお，これらの推定手法は一例である．例えば，複数の Web サーバ型ハニーポットのログを用いた cross validation check から β を推定しても，解析を適用することができる．

4.3 解析結果

推定した η と β を用いて，α が変動した際に最適となる γ を解析した．なお，今回の実態調査では，1 分間に最大 10 回の攻撃を観測したため，α を 1 から 10 まで変化させた際の γ の最適値を算出した．さらに，ボット数が評価値に与える影響を調査するために，ボット数を増加させた際の評価値も算出した．各評価値は，本解析モデルにおいて，任意に選択された B_i が MDS として使用され全ボットがブラックリストに未掲載の状態を初期状態とし，各状態が定常分布に到達するまで遷移を繰り返して各状態の定常分布確率を特定することで算出した．図 7 は，ボット数 $N = 3$，$\alpha = 10$ において γ を変化させた際の TPR, TNR, FPR, FNR を示している．図 8 は，ボット数 $N = 3$ の際に，各 α において γ を変化させた際の PPV を示している．図 9 は，ボット数 $N = 3$ の際に，各 α において γ を変化させた際の O_p を示している．

図 7 に示すように，γ の増加に対して TNR は急速に増加して収束する一方で FNR は徐々に増加し，かつ，常に $TNR > FNR$ となる．NPV に着目すると，γ は最小値が望ましいが，その場合，FPR が多発する．したがって，本解析において NPV は評価値として適切ではない．

図 8 に示すように，PPV に関しては，各 α に対して異なる最適な γ が存在する．例えば，$\alpha = 1$ の場合における最適値は $\gamma = 0.05 \times 10^{-2}$（約 1.38 日）となっている．一方，$\alpha = 2$ における最適値は $\gamma = 0.01 \times 10^{-1}$ となっている．また，O_p に関しては，図 9 に示すように，PPV とは異なるが最適な γ を保有していた．

次に，本解析モデルにおいて，ボット数を 10 まで増加させた際の PPV と O_p を算出し，ボット数の増加に対する最適な γ を解析した．本解析の結果，最適な γ は多少変化するが，グラフとしては図 8 や図 9 とほぼ同じとなった．

以上から，同一のマルウェアが配置されたボット数 N や攻撃レート α を監視しつつ，本解析を実施することで，FP を抑制しつつ，TP を最大化する γ を決定できると考えられる．

5 関連研究

マルウェアの感染過程を解析する手法として，worm が IP アドレスに基づいて次の攻撃先を選定する挙動を解析することで worm の拡散過程を解明する手法 [11] が検討されている．また，マルウェア感染を引き起こすサイトを解析する手法としては，Web クライアントへの Drive-by-download 攻撃で使用される悪性サイトを解析する手法が数多く検討されている．これらの手法で解析対象としている攻撃は，本稿で解析対象としている Web アプリケーションの脆弱性を悪用する攻撃とは大きく異なる．このため，提案手法を含め，各々の手法に適応領域が存在すると考えられる．

6 おわりに

本稿では，Web サイトへ感染させるためのマルウェアが配置されたボットである MDS の実態調査結果を報告した．さらに，調査結果を活用し，攻撃者とサービスプロバイダの行動をモデル化して MDS のブラックリスト掲載に関する状態遷移モデルを解析し，その結果から，MDS の活動を監視する周期を決定した．これにより，誤検知を抑制しつつ攻撃検知率を高めるブラックリストの更新を実現できるため，Web サイトをマルウェア感染から高精度に保護可能な，安心安全な Web サイト環境を構築できる．

今後の課題としては，実システムへの適用のためのパラメータ推定のリアルタイム化や，ボット数拡大に伴う計算負荷の増加に対応するための近似アルゴリズムの検討が挙げられる．

参考文献

[1] D. Canali and D. Balzarotti, "Behind the Scenes of Online Attacks: an Analysis of Exploitation Behaviors on the Web," The 2013 Network and Distributed System Security Symposium (NDSS), Feb, 2013.

[2] Z. Zhao, G. Ahn and H. Hu, "Examining Social Dynamics for Contering Botnet Attacks," IEEE Global Communication Conference (GLOBECOM), 2011

[3] The Honeynet Project, "Web Applicaton Honeypot," `http://www.honeynet.org/gsoc/project8`

[4] J. P. John, F. Yu, Y. Xie, A. Krishnamurthy and M. Abadi, "Heat-seeking honeypots," World Wide Web (WWW), 2011.

[5] T.Yagi, N.Tanimoto, T.Hariu and M.Itoh, "Design of Provider-Provisioned Website Protection Scheme against Malware Distribution," IEICE Transactions on Communications, B93-B, No.5, pp 1122-1130, May, 2010.

[6] T.Yagi, N.Tanimoto, T.Hariu and M.Itoh, "Life-cycle monitoring scheme of malware download sites for websites," IEEE International Conference on Service-Oriented Computing and Applications (SOCA), Dec, 2010.

[7] H.F.G.Robledo, "Type of hosts on a Remote File Inclusion (RFI) Botnet," Electronics, Robotics and Automotive Mechanics Conference (CERMA), 2008.

[8] T.Yagi, N.Tanimoto, T.Hariu and M.Itoh, "Investigation and analysis of malware on websites," IEEE International Conference on Web System Evolution (WSE) 2010, Sep, 2010.

[9] www.malwaredomainlist.com, "Malware domain list," `http://malwaredomainlist.com/`

[10] Y.C. Hu, A. Perrig and D.B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," IEEE Conference on Computer Communications (INFOCOM), 2003.

[11] S. Staniford, V. Paxson and N. Weaver, "How to 0wn the Internet in Your Spare Time," USENIX Security Symposium, 2002.