情報処理学会論文誌 Vol.58 No.1 249–257 (Jan. 2017)

ボットネットのC&Cサーバ特定手法における フィルタシステムの提案と評価

岡安 翔太[1] 佐々木 良一[1,a)]

受付日 2016年3月29日, 採録日 2016年10月4日

概要：マルウェアに感染した複数の PC 群から構成されるボットネットによる被害は年々増加しており，大きな問題となっている．この問題を解決するために，著者らは数量化理論 2 類を用いて C&C サーバを検出する手法を先に提案した．この手法では，ブラックリストに登録されていない C&C サーバを検出することができる．しかし，この手法は時間経過とともに検知率が低下していくことが継続研究から予測された．そこで，本論文では，まずある時点のデータに基づき作成した C&C サーバの検出のための判別モデルがどの程度の期間有効であるか，時間経過による検知率の低下にどのように対応するかの検討を行いモデルの頻繁な変更が必要であることを示す．次に，従来手法の数量化理論 2 類と Support Vector Machine（SVM）での C&C サーバの検出精度の比較を行った結果，その精度はほぼ同等であることを示す．最後に，SVM を支援するプログラムはいろいろな機能を持ち，自由度が高いことから，SVM を用いる方式を利用した C&C サーバフィルタシステムの開発を行い，有効性の検証を行った結果，実用可能である見通しを得たことを報告する．

キーワード：ボットネット，C&C サーバ，DNS，数量化理論，SVM

Proposal and Evaluation of Filter System for Detection Method of C&C Server Used in a Botnet

Shota Okayasu[1] Ryoichi Sasaki[1,a)]

Received: March 29, 2016, Accepted: October 4, 2016

Abstract: In recent years, the damage caused by botnets has increased and become a big problem. To solve this problem, we proposed a method to detect unjust C&C servers by using Hayashi's quantification theory class II. This method is able to detect unjust C&C servers, even if they are not included in a blacklist. However, it was predicted that the detection rate for this method decreases with passing time. Therefore, in this paper, we clarify the useful period of the discriminative model created using the data at the starting point, as well as a reduction tendency of detection rate depending on the passing time. Next, we compare the detection accuracy of C&C server obtained from the conventional quantification theory class II and the newly used Support Vector Machine (SVM). The result of the experiment made appear that detection accuracy of two methods is almost same. Last of all we report the confirmed usefulness of the C&C server filter system developed using the proposed SVM method of which program has many and free functions.

Keywords: Botnet, C&C server, DNS, Hayashi's quantification methods, SVM

1. はじめに

1.1 研究の背景

近年ボットネットによる被害が増加しており問題となっている．ボットネットとは悪意を持った攻撃者の命令に基

[1] 東京電機大学
Tokyo Denki University, Adachi, Tokyo 120–8511, Japan
[a)] sasaki@im.dendai.ac.jp

づき動作するプログラムに感染したPC（以下，ボットPC）および攻撃者の命令を送信する指令サーバ（以下，C&Cサーバ）からなるネットワークであり，なかには数万規模のPCなどからなるボットネットもあるといわれている [1]．攻撃者がC&Cサーバに命令を送ることで，ボットネットに接続されたボットPCはフィッシング目的などのSPAMメールの大量送信や，特定サイトへのDDoS（Distributed Denial of Service）などに利用され，非常に大きな脅威となりうる [2]．これらのボットPCを用いた攻撃は，攻撃元の特定手法としてIPトレースバックなどを用いることで，攻撃元を偽装した場合でも，攻撃者を特定することができる．しかし，ボットPCの特定ができたとしても，そのPCの対策が不十分であれば再度マルウェアに感染してC&Cサーバに操られる可能性がある．したがってC&Cサーバへの対策がなされていない限り，ほかのPCもマルウェアに感染して操られる可能性もあるため，ボットPCの特定だけでは根本的な解決とはならない．

このような問題に対して本研究室では，ネットワーク管理者が情報共有を行い，ボットPCだけではなく，C&Cサーバや攻撃者の特定を目的とする，多段追跡システムの研究を行ってきた [3]．本論文は，そのうち第2段においてC&Cサーバ・ダウンローダを特定する方式に関するものである．

著者らが先に開発した方式はC&Cサーバと正常サーバのDNS情報に基づき林が考案した数量化理論2類 [4] を用いることで識別モデルを構築し，C&Cサーバかどうかを推定するものであり，ブラックリストに登録されていないC&Cサーバであっても検出できるという特長がある．この基本方式についてはすでに論文として報告してきた [3]．しかし，この方式をC&Cサーバフィルタシステムに組み込み実際に使おうとすると，時間経過にともない有効性が低くなる可能性が危惧された．

1.2 本研究の概要

このような問題点に関し，本論文は以下の研究結果を報告するものである．

(1) ある時点のデータに基づき作成した数量化理論2類の識別モデルがどの程度の期間有効か，時間の経過にともないどのように改良していく必要があるかの検討を行った．このような検討は従来行われてこなかったものである．その結果，時間の経過とともに識別モデルを変化させる必要を明らかにした．

(2) 従来用いてきた数量化理論2類を支援するプログラムは，いろいろな制約があり識別モデルを容易に変更できず，C&Cサーバフィルタシステムの機能を最新のものにするのが困難である．そこで機械学習技術の1つであるSupport Vector Machine（SVM）に着目し，数量化理論2類を用いた場合とC&Cサーバの検知の有効性の比較を行った．SVMを支援するプログラムは交差検定法など種々の機能が用意されており，自由度があるため，SVMを支援するプログラムを用いた方がC&Cサーバフィルタシステムの機能を最新のものにしやすいからである．

(3) 比較の結果，SVMを用いる方式は数量化理論2類を用いる方式に劣らないことを明らかにした．

(4) そこでSVMを用いる方式を用い，最新のドメインデータから識別モデルを自動生成する機能を持つC&Cサーバフィルタシステムの開発を行い，有効性の検証を行った結果，実用可能である見通しを得た．

2. 関連研究

2.1 類似研究

ボットネットにおける，C&Cサーバの特定を目的とした研究は，次の2つに分類される．

(1) C&Cサーバとの制御通信に着目した特定手法

C&Cサーバと感染PC間で行われる通信に着目し，制御通信のペイロードに含まれる文字列などの特徴を分析する手法 [5], [6], [7] がある．この通信内容からC&Cサーバの特定が可能である．

これら手法は，トランスポート層のポート番号や独自プロトコルといった仕様変更にともない，対応できなくなる従来の検出手法と異なり，宛先IPアドレスや発信元IPアドレスなどヘッダ情報を除いたデータ部分を検証するため，十分な検証により高い検出精度を出す．しかし，年々移り変わる攻撃手法によるトラフィックの複雑化，多様化の観点からゼロデイ攻撃などの未検証検体への対応に不十分な点がある．

(2) C&Cサーバのドメイン情報に着目した特定手法

感染PCに潜伏するボットウイルスは，DNSサーバに対してC&Cサーバの名前解決を行うことが確認されている．C&Cサーバのドメイン情報に着目し，設定されているドメイン情報や外部リポジトリから取得した情報を併用し，データマイニング手法を用いて検証を行う手法 [8], [9], [10] がある．これらの手法はある時点で観測したデータを用いたものであり，検知率は95%以上と精度が高いものとなっている．しかし，ドメイン情報が変化していった場合の検知率の変化までは言及しておらず，時間経過にともなうドメイン情報の変化などには対応しきれていない．

2.2 先行研究の概要

本論文の基となり，著者らが先に開発した基本方式は2.1節の(2)と同様にC&Cサーバのドメインに着目した特定手法である [3]．本手法は，C&Cサーバに関連するDNSサーバから，ドメイン情報や各レジストリ組織が管理している情報を取り出して用いる．C&Cサーバに関するブラックリストに記載されたドメインと，正規サーバのドメ

インの DNS 情報を利用し，数量化理論 2 類を用いることで識別モデルを作り，対象となるサーバが C&C サーバかどうかの特定を行う．

数量化理論は，元統計数理学研究所所長の林知己夫教授らにより開発されたデータ分析手法である [4]．このうち，数量化理論 2 類ではダミー変数の導入による質的データの数量化を行うことで，判別分析に相当する処理を可能にする．

たとえば，分析対象データの集合に 1 群と 2 群が混在するとき数量化理論 2 類を用いて 1 群と 2 群に判別するケースを考える．初めに，1 群と 2 群，それぞれを特徴付ける各特徴量をカテゴリ化したものをパラメータとして設定した判別式と 1 群と 2 群に判別するための基準となる境界値の 2 種を設定する．この判別式に集合の各要素を入力し出力される判別値を，先に求めた境界値と比較する．この際に，判別値が境界値より高い値ならば 1 群，低い値ならば 2 群と判別を行う．また，使用した集合外の要素についても同様に境界値を比較することで，1 群・2 群どちらに属する可能性が高いかを推定することが可能である．数量化理論 2 類では判別式，判別境界値を求めることで未知のデータを分類する．

3. C&C サーバ特定手法の評価

本章では，数量化理論 2 類を用いた継続的な調査結果と，数量化理論 2 類と SVM の検知精度の比較結果を主に報告する．それらの結果を説明するうえで必要となる数量化理論 2 類や SVM で用いる特徴量とカテゴリ化や，検出精度検出方式，SVM 方式の概要についてもあわせて記述している．

3.1 特徴量とカテゴリ化

数量化理論 2 類や SVM で用いる特徴量の候補を**表 1** に示す．三原らの方式 [3] を基本に追加したものである．これらの特徴量の情報は C&C サーバに関連する DNS サーバから取得する．No.1〜8 は対象 DNS サーバに dig コマンドを使用することで取得する．No.9 は各レジストリ組織が管理している WHOIS サービスを用いて取得する．

表 1 特徴量候補一覧
Table 1 Candidate list of parameters.

No.	特徴量
1	逆引き
2	TTL
3	minimum
4	A レコード
5	MX レコード
6	NS レコード
7	CNAME レコード
8	TXT レコード
9	登録期間

各項目の説明として，No.1 は，DNS サーバに対して IP アドレスからドメイン名の問合せの結果を調査する．No.2, 3 は，DNS サーバから取得したドメインの設定情報が記載されている SOA レコードから，設定値を調査する．No.4〜8 は DNS で定義されるドメインについての情報であり，各項目の個数や有無を調査する．No.9 は，各レジストリ組織が管理している，ドメインの登録情報から，ドメインの登録日時と利用期限の調査を行い，その差を登録期間とする．本論文では以上 9 つの DNS ドメインの要素を特徴量とし，C&C サーバの検出に用いる．

数量化理論 2 類では特徴量をカテゴリに分類することが必要である．ここでは**表 2** に示すように「有り」や「無し」などの特徴量の定性的特性に着目して分類するのが基本であるが，特徴量の値が連続量として表現される場合には適当に区分してカテゴリ化することになる．区分の方法に絶対的に正しいものはなく C&C サーバと通常のサーバの違いが出やすいかどうかなどを検討しながらカテゴリ化することになる．今回のカテゴリ化は文献 [3] の 4 章および表 7 に記載されたものを基本とし，新しく導入した特徴量については類似の方法でカテゴリ化を行っている．

3.2 識別モデルの C&C サーバの検出精度判定方式

提案手法では B ドメインと N ドメインの複合データを用いて C&C サーバ特定のための識別モデルを作成する．

表 2 項目のカテゴリ化
Table 2 Categorization of items.

逆引き	値
返答なし	1
不正	2
一致	3

Aレコード	値
1 〜 2	1
3 〜	2
N/A	3

TTL	値
1-1000	1
1001-10000	2
10001-	3

NSレコード	値
有り	1
無し	2

CNAMEレコード	値
有り	1
無し	2

minimum	値
1-1000	1
1001-10000	2
10001-	3

TXTレコード	値
有り	1
無し	2

MXレコード	値
有り	1
無し	2

登録期間 （日）	値
1-2500	1
2501-5000	2
5001-	3
N/A	4

表 3 検知判定組合せ
Table 3 Categories of decision results.

	検知結果が真	検知結果が偽
N ドメイン	True Positive	False Negative
B ドメイン	False Positive	True Negative

表 4 利用データセット
Table 4 Used data sets.

年度	データセット	B ドメイン
2009	CCC Datasets 2009	19 件
2010	CCC Datasets 2010	30 件
2011	CCC Datasets 2011	42 件
2013	PRACTICE Datasets 2013	18 件
2014	DNS-BH	105 件

その際に，複合データの一部を学習データとして識別モデルの作成に用いる．複合データの残りを評価データとして識別モデルの性能評価に用いる．

本論文における C&C サーバの検出精度判定方式を**表 3** に示す．識別結果に対する評価指標として，N ドメインが正しく N ドメインと判別されることを True Positive，その割合を True Positive Rate（TPR）とする．B ドメインを正しく B ドメインと判別されることを True Negative，その割合を True Negative Rate（TNR）とする．検知率は式 (1) から求められる．本論文では TPR，TNR，検知率を用いて識別モデルの評価を行う．

$$\frac{\text{True Positives の数} + \text{True Negatives の数}}{\text{総ドメイン数}} \quad (1)$$

3.3 数量化理論 2 類を用いた継続的な調査

数量化理論 2 類を用いた C&C サーバ特定手法は 2009 年に三原ら [3] によって確立された．その後，2011 年から中村 [12] が，2013 年以降は本論文の著者の 1 人である岡安 [13] によって継続的な調査が行われている．このような継続調査は従来行われてこなかったものであるが，その結果，本手法では時間経過にともない識別モデルの C&C サーバ分類精度が減少する傾向があることが判明している．これは C&C サーバの特徴が時間経過によって変動していることが原因である．そのため，我々は一定期間ごとに最新のデータを用いた識別モデルの作成，評価を行ってきた．利用したデータの概要を**表 4** に示す．2009〜2011，2013 年度で利用した CCC DATAset [14] や PRACTICE Dataset [15] はマルウェア対策研究育成ワークショップ [16] から提供されたハニーポットの通信記録である．そのデータセット内から C&C サーバと関連のある B ドメインを取得し利用した．しかし，2014 年度データにはデータセットの提供が行われなかったため，DNS-BH [17] からボット PC が接続する C&C サーバのドメインリストを用いる．このリストから 2014 年度に追加されたドメインを新たに発見されたものと見なし，2014 年度の B ドメインと定義した．なお，B ドメインは PC が接続する C&C サーバのドメインであり，ボットネット自身のドメインではない．N ドメインには安全性が高いドメインが最適であるため，世界のアクセスランキングトップ 500 を掲載している “The top 500 sites on the web” [18] を利用した．人気サイトはサイト規模が大きい傾向にあるため特徴量に偏りが生じると考え，“IR サイトランキング” [19] と “FORTUNE” [20] から中小規模企業のドメインも利用した．

表 5 継続的調査による識別モデルの評価
Table 5 Evaluation of identification model using continuous survey.

識別モデル	検知率 (%)				
	2009	2010	2011	2013	2014
2009	96.5	85.0	76.5	-	-
2011	-	-	95.2	42.5	-
2013	-	-	-	80.3	80.8
2014	-	-	-	-	96.7

時間経過による識別モデルの性能評価結果を**表 5** に示す．識別モデルの作成，評価には株式会社エスミ社のソフトウェア Excel 数量化理論 Ver3.0 [21] を使用した．併用して，識別モデルの作成には 4.4 節で示す AIC を用いることで最適な特徴量の数と組合せを導いている．表 5 の 2009 年度で作成した識別モデルは 2009 年度では検知率 96.5%と非常に高い値であった．しかし，2010 年度のデータで 2009 年度識別モデルを評価したところ検知率は 85.0%，2011 年度では 76.5%と年を追うごとに検知率が低下している．2009 年度識別モデルでは 2010，2011 年度に対応することができなかったといえる．

そのため，2011 年度で新たに 2011 年度データを用いた識別モデルの作成を行った．識別モデル作成の際に，NS レコード，CNAME レコードの 2 つを特徴量候補として追加し，特徴量の定量化の値の調整なども加えて行った．その結果，検知率 95.2%となり改善に成功した．2014 年度では識別モデル作成の際に TXT レコードを特徴量の候補に追加した．その結果，2014 年度識別モデルは検知率 96.7%と高い値となった．

以上のことから C&C サーバの特徴量の変動に対応するには最新のデータを利用した識別モデルが有効であるといえる．また，B ドメインの解析を通して新たな特徴量を識別モデル作成の候補として利用することで一定の成果が得られた．

3.4 数量化理論 2 類と SVM の分類精度比較実験

3.4.1 SVM を用いる方式

SVM は機械学習に用いられる教師あり学習モデルであ

表 6 複合データ件数
Table 6 Number of data for learning and evaluation.

	学習データ	評価データ
B ドメイン	30 件	75 件
N ドメイン	30 件	75 件

表 7 交差検定法実験環境
Table 7 Experimental environment for cross validation.

データ数（表 6 の件数）	210 件
学習用データ	80%
評価用データ	20%
試行回数	5 回

表 8 識別モデル比較実験結果
Table 8 Experimental results of identification models.

	TPR	TNR	検知率
数量化理論 2 類	94.7%	98.7%	96.7%
SVM 交差検定法	96.6%	94.8%	95.7%

る．主に識別や回帰分析に適用できる．SVM は，データを高い次元の特徴空間にマップすることで動作するため，データを線状に分けることができない場合であっても，データポイントをカテゴリ別に分けることができる．カテゴリ間の区切りが検出された後，区切りを超平面として描画することができる方法でデータが変換される．これにより，新しいデータの特性を利用して，新しいレコードが属するグループを予測できる [11]．

3.4.2 実験概要

本実験では従来用いていた数量化理論 2 類が SVM で代用できるか否か，分類精度の妥当性検証を行う．

利用するデータセットは表 4 のデータセットの DNS-BH で，2014 年度の B ドメイン 105 件を利用する．このデータに 2014 年度の N ドメイン 105 件を合わせて 2014 年度複合データとする．実験手順は複合データから**表 6** で示す件数でデータの分割を行い，学習データで識別モデルを作成し，評価データで識別モデルの分類精度を評価する．

また，識別モデルの分類精度の妥当性を求めるために交差検定法を用いて SVM の識別モデルの検証を行った．交差検定法での実験環境を**表 7** に示す．今回交差検定法に用いたライブラリは scikit-learn [22] である．なお，数量化理論 2 類には交差検定法を行うための有効なシステムがなく，行っていない．

3.4.3 実験結果

識別モデルの評価結果を**表 8** に示す．求められる TPR，TNR は組織や利用する形態によって異なる．本論文では後述するフィルタシステムに適用することが最終的な目的であるため，識別率 90%以上を目標値と設定することにする．結果，数量化理論 2 類と SVM では TPR，TNR がともに 90%を超える値となった．C&C サーバの検出のために，従来用いていた数量化理論 2 類を SVM で代用可能な数値であるといえる．

なお，SVM は数量化理論 2 類の処理プログラムと比較して多様なライブラリが存在するため拡張性の多いデータマイニング手法となっている．著者らは数量化理論 2 類での検証を長期的に行ってきたが，SVM での識別モデルでも十分な分類精度があると判断し，今後は SVM をメインとした検証を行っていくこととする．後述するフィルタシステムにも多様なライブラリや利用するプロキシサーバへの実装言語の相性から，提案システムでは SVM を採用する．

3.5 最適な特徴量の選定

本論文で 2014 年度識別モデルの作成に 9 個の特徴量を候補にあげている．しかし，すべての特徴量を用いれば良い識別モデルができるというわけではない．データを統計的に説明する数式では，用いる項目数を増やせば，測定データとの適合度が高くなる．しかし，ノイズの影響が大きくなり，信頼性を低下させる可能性も孕んでいる．そこで最適な特徴量の数と組合せを調べるために赤池情報量基準（以下，AIC）[23] を用いる．AIC は元統計数理研究所所長の赤池弘次によって考案された，統計モデルの良さを評価するための指標である．AIC を用いることで，モデルの複雑さとデータとの適合度のバランスをとることが可能となる．AIC は式 (2) によって求められる最小 AIC 時の項目数を選択することで，多くの場合，最適なモデルを選択できる．2014 年度識別モデルの場合は 9 個の特徴量という項目から過学習が少なく，最も説明力が高くなる項目数とその組合せを選ぶことが可能となる．

$$\mathrm{AIC} = -2\mathrm{In}L + 2k \tag{2}$$

L は最大尤度，k は自由パラメータである．今回の場合，k が各要素数に相当し，L が各パラメータ数での判別結果と，正答との乖離の最小 2 乗和に相当する．

本論文では 2009～2014 年まで継続的に提案方式の調査を行っており，2014 年度には SVM での検証も行った．これらの識別モデルを作成する際には AIC を用いることで，最適なモデルの選定を行った．年度ごとに作成した識別モデルの項目数と，選定された特徴量を**表 9** に示す．○がついているものが選定された特徴量であり，斜線の欄は該当年度には存在しなかった項目である．2010，2012 年では識別モデルの設定に必要なデータが取得できなかったため，行っていない．年度によって有効な特徴量は若干異なるが，登録期間は通年，特徴量として用いられており，C&C サーバの分類に大きな影響を及ぼしていると考えられる．

3.6 識別モデルの生成に影響の大きな特徴量

特徴量の中で「TXT レコード」と「登録期間」が，B ド

メインとNドメインの違いが特に顕著であった．この特徴の違いがAICにおける最適な特徴量の選定に大きな影響を及ぼしている．次項でこの2つの特徴量の傾向調査結果を示す．調査対象は2014年度データであり，Bドメイン105件，Nドメイン500件での調査を行った．

3.6.1 TXTレコード

TXTレコードは，DNSで定義される情報の一種で，ドメイン外部のソースにテキスト情報を提供する役割を持つ．ドメインの所有者の確認やメールのセキュリティ対策の実装などに用いられる．TXTレコードの有無をBドメイン，Nドメインに分けて調査した．その結果を**表10**に示す．Bドメインは TXTレコードを設定しない場合がほとんどである．Nドメインは，7割以上がTXTレコードを設定している．このような大きな違いはドメインの識別に大きな影響を及ぼすといえる．

3.6.2 登録期間

Bドメインと Nドメインの登録期間を調査した結果を**図1**に示す．Bドメインは Nドメインと比べて登録期間が短い傾向にある．さらに管理情報の取得ができずに登録期間が不明のBドメインも多数存在する．また，継続研究の結果，Bドメインの特徴として登録期間が長くなるとそのドメインを破棄する傾向があることが判明している．登録期間の長い C&Cサーバを破棄して，新たな C&Cサーバを構築するため，Bドメインが短い登録期間に集中すると考えられる．対して，Nドメインの登録期間は長い傾向にある．Nドメインは正規サイトであるという性質上，長期運用を目的としているからである．

表9 各識別モデルで選定されているパラメータ
Table 9 Selected parameters for each identification model.

	数量化理論2類						SVM
	2009	2010	2011	2012	2013	2014	2014
逆引き	○		○		○		
TTL						○	
minimum	○		○			○	○
Aレコード			○		○		
MXレコード							○
NSレコード						○	
CNAMEレコード					○		○
TXTレコード						○	○
登録期間	○		○		○	○	○
特徴量個数	3		4		4	5	5

表10 TXTレコードの分類
Table 10 Categorization from viewpoint of TXT record.

	Bドメイン（件）	Nドメイン（件）
有り	3	393
無し	102	107

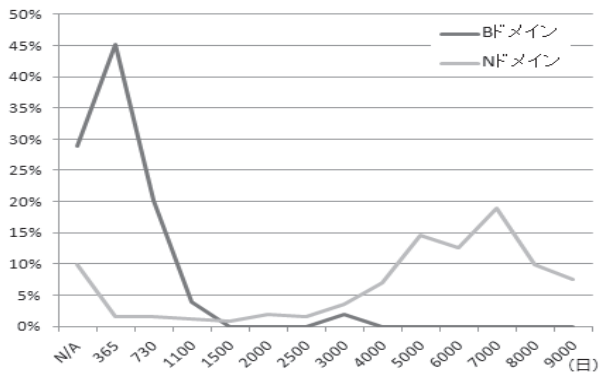

図1 登録期間の分類割合
Fig. 1 Distribution of registration period.

4. フィルタシステムの開発と評価

4.1 システム概要

4.1.1 フィルタシステム

提案する C&Cサーバ特定手法では，作成した識別モデルを用いることで，ブラックリストには存在しない未知の C&Cサーバを特定できる．そこで3章で作成したSVMの識別モデルを用いたフィルタシステムの開発を行った．本システムは識別モデルをプロキシサーバに用いることで要求のあったURLに対し，ドメインの判定を行い処理することで，良性通信か悪性通信かどうか判断し，処理をするフィルタシステムである．

システムの構成を**図2**に示す．プロキシサーバはリスト判定部と SVM判定部で構成されている．ここで本システムを構成する各要素に関して以下に示す．

- ブラックリスト
  インターネット上から取得したBドメインのリスト
- ホワイトリスト
  Nドメインのリスト
- SVM_BL
  Bドメインと判定されたドメインリスト
  次回アクセスを早めるキャッシュとして用いる
- SVM_WL
  Nドメインと判定されたドメインリスト

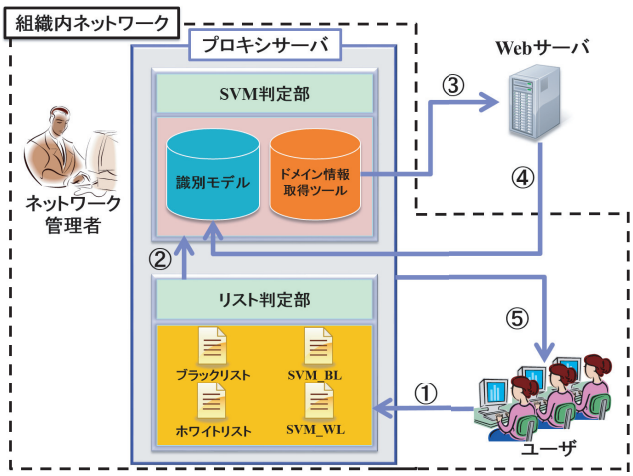

図2 フィルタシステム構成図
Fig. 2 Overview of the proposed filtering system.

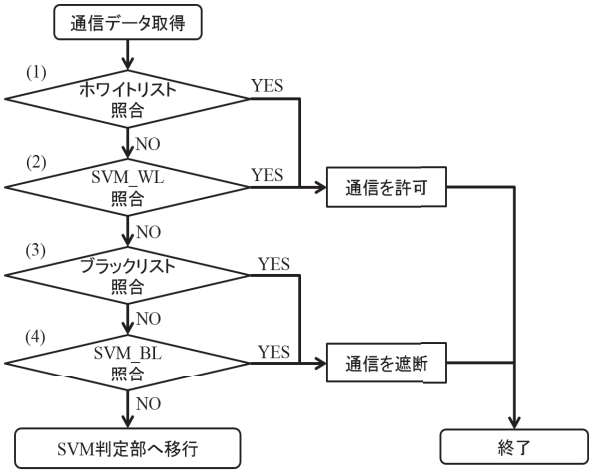

図 3 リスト判定部アルゴリズム
Fig. 3 Flow showing algorithms for selection list.

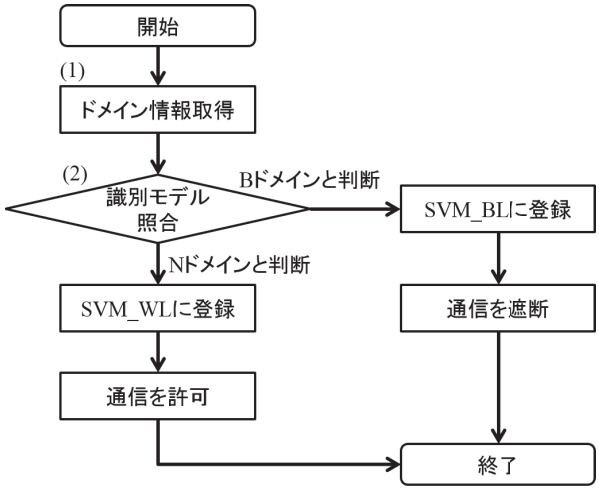

図 4 SVM 判定部アルゴリズム
Fig. 4 Flow showing algorithms for selection SVM.

次回アクセスを早めるキャッシュとして用いる

- ドメイン情報取得ツール
  URL リクエスト先の DNS サーバの特徴量取得ツール
- 識別モデル
  C&C サーバ特定のために SVM で作成した識別モデル

本システムはユーザから URL リクエストを受け（図 2-①）リスト判定部で下記の処理を行う（**図 3**）．通信が許可された時点で要求 URL の通信結果をユーザに返す（図 2-⑤）．

(1) 要求された URL がホワイトリストに記録されているか確認する．リストにあればその通信を許可し，なければ (2) に移行する．
(2) 要求された URL が SVM_WL に記録されているか確認する．リストにあればその通信を許可し，なければ (3) に移行する．
(3) 要求された URL がブラックリストに記録されているか確認する．リストにあればその通信を遮断し，なければ (4) に移行する．
(4) 要求された URL が SVM_BL に記録されているか確認する．リストにあればその通信を遮断し，なければ SVM 判定部に処理を移行する（図 2-②）．

リスト判定部で検出できなかった URL は SVM 判定部に処理が移行し，下記の処理を行う（**図 4**）．

(1) 要求された URL について 3.2 節で述べた 9 項目の特徴量の取得，定量化を行う（図 2-③）．
(2) SVM で作成した識別モデルを用いて B ドメインであるか N ドメインであるかを判定する（図 2-④）．B ドメインの場合，SVM_BL に要求 URL のドメインを記録し通信を遮断する．N ドメインの場合，SVM_WL に要求 URL のドメインを記録し通信を許可する．

4.1.2 識別モデル自動生成システム

4.2 節の C&C サーバ特定手法の継続的な調査結果から，最新のデータを用いることで C&C サーバの特徴量の変化に対応できるといえる．そこで最新データから最適な識別

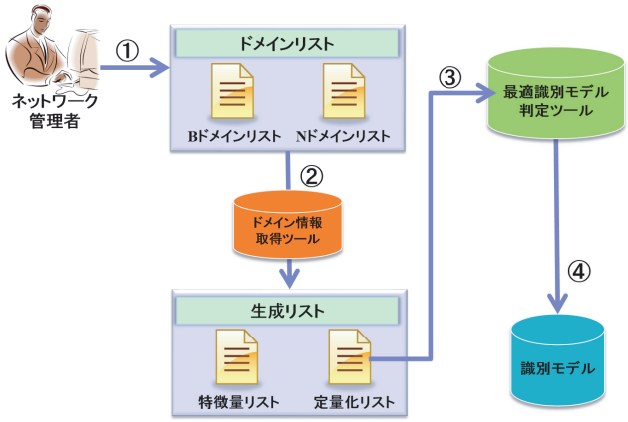

図 5 識別モデル自動生成システム構成図
Fig. 5 System structure for automatic generation of identification model.

モデルを自動生成するシステムを開発した．このシステムを用いることでフィルタシステムの識別モデルを最新データの識別モデルに更新することが可能であり，時間経過にともなう検知率の低下の対策として有効である．この有効性は 4 章での検証結果からいえる．

システムの構成を**図 5** に示す．ここで本システムを構成する各要素に関して以下に述べる．

- B ドメインリスト
  インターネット上から取得した B ドメインのリスト
- N ドメインリスト
  インターネット上から取得した N ドメインのリスト
- 特徴量リスト
  ドメインリストから生成された特徴量リスト
- 定量化リスト
  取得した特徴量を定量化したリスト
- 最適識別モデル判定ツール
  交差検定法，AIC を用いた検証，および識別モデルの生成を行う．

本システムはネットワーク管理者が用意する最新のドメインリスト（図 5-①）を使用する．B ドメインと N ドメインの 2 つのリストに対してドメイン情報取得ツールを適用することで特徴量を取得し，特徴量リストを生成する．同時に特徴量を定量化した定量化リストも生成する（図 5-②）．生成された定量化リストを最適識別モデル判定ツールに適用させる（図 5-③）．モデルの判定には SVM を用いており，交差検定法，AIC での検証をとおして最適な識別モデルを生成する（図 5-④）．この識別モデルをフィルタシステムに適用することで C&C サーバの特徴量の変化に動的な対応が可能である．また，B ドメインは時間経過によって応答がなくなる傾向にある．そのため，特徴量リストに記録することで今後のデータ解析などに利用することを可能とした．

4.2 システムの実装

システムの実装にはオープンソースソフトウェアとして公開されている Squid [24] を用いる．Squid は HTTP などの通信を中継するプロキシサーバソフトである．Squid はリストマッチング機能が備わっており，提案フィルタシステムのリスト判定部で用いている．また，機能の一部に “url_rewrite_program” というオプションが存在する．このオプションではユーザの用意したプログラムから，要求のあった URL の受け渡しや，書き換えが可能である．このオプションを用いて SVM 判定部の処理を行う．プロキシサーバには Squid 3.3.8 を用い，Python 3.4.3 で実装を行った．

これらのシステムの適用実験を行うことにより必要な機能を持つことが確認できた．次節では性能実験の結果を記述する．

4.3 性能評価実験

4.3.1 フィルタシステム

フィルタシステムを適応した場合に懸念されるのがアクセス速度の問題である．C&C サーバとの通信規制を実現できたとしても，アクセス速度が遅すぎる場合，ユーザ負担度が大きくなってしまう．そこで，フィルタシステムを適用しない場合とした場合の 2 通りで Web ページが表示されるまでアクセス速度の比較を行った．検証に用いる Web サイトは “squid-cache.org”（squid 公式サイト）と “Yahoo! JAPAN” とし，10 回のアクセス時間の平均をアクセス速度とする．Web ブラウザは Mozilla Firefox を用い，計測にはアドオンの Firebug を使用した．キャシュや履歴は残さない環境で実験を行った．計測時の回線速度と動作環境を**表 11** に，計測の結果を**表 12** に示す．回線速度の測定には BNR スピードテストを用いた．

“squid-cache.org” ではシステムを未適用の場合 1.40 秒，システム適用した場合 1.85 秒で，その差は 0.45 秒であった．“Yahoo! JAPAN” では未適用の場合 2.84 秒，システム適用した場合 3.76 秒で，その差は 0.91 秒であった．

表 11 実験環境
Table 11 Experimental environment.

回線速度	下り	21.68Mbps
	上り	71.42Mbps
動作環境	メモリ	5199MB
	プロセッサ数	2 CPU

表 12 アクセス速度測定結果
Table 12 Measured results of access speed.

	システム未適用時	システム適用時
squid-cache.org	1.40s	1.85s
Yahoo! JAPAN	2.84s	3.76s

両サイトの違いは URL のリクエスト数に依存しており，“Yahoo! JAPAN” の URL リクエストは 76 件，“squid-cache.org” の URL リクエストは 9 件である．URL リクエスト数に比例し，システムの呼び出し回数が増加することがアクセス速度に影響を与えている．両サイトともにシステム適応時のアクセス速度は未適応時に比べて約 1.3 倍となった．本システムは大型なポータルサイトでは，通常サイトよりもアクセス速度が長くなる傾向があるが，十分に運用可能な負荷レベルであると思われる．

4.3.2 識別モデル自動生成システム

2015 年度に取得したデータを最新データとして，識別モデル自動生成システムに適用した．ドメインデータには B ドメイン 150 件，N ドメイン 150 件を用いた．

識別モデル自動生成システムは，要求機能を実現することができた．そして識別モデルの生成には 20 分程度を要するが実用上問題ないことを確認した．

5. おわりに

本論文では C&C サーバ特定手法を用いて C&C サーバの継続的な調査を行った．時間経過による C&C サーバの特徴の変化に対し，最新データでの適用や特徴量の候補の追加・修正により高い検知率を得ることができた．従来用いていた数量化理論 2 類と SVM での検知率には大きな違いはなく，どちらも C&C サーバの特定に有効であった．

C&C サーバの特定手法を基にプロキシサーバを用いたフィルタシステムの開発と評価を行った．フィルタシステムの C&C サーバ判定部分には SVM を用いた．理由としては，SVM には多様なライブラリが存在し，交差検定法やシステムの自動化への適用が可能という点で優位性が見られたためである．本システムには最新のドメインデータから識別モデルを自動生成する機能がある．この識別モデルを適用することで，C&C サーバの時間経過による特徴

量の変化に動的な対応を可能とした．検証により，本フィルタシステムは大型ポータルサイトのようなページ内の要素数に比例し負荷が大きくなるが，十分に運用可能な範囲の負荷であった．

今後の課題として以下が考えられる．

(1) 識別モデル自動生成システムがどの程度 C&C サーバの特徴量の変動に有効であるかの調査．
(2) フィルタシステムの利用規模に応じたシステム設計やアクセス負荷における影響の検証．

参考文献

[1] 警視庁：情報セキュリティ広場，入手先 ⟨http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku409.htm⟩.
[2] サイバークリーンセンター，入手先 ⟨https://www.ccc.go.jp/bot/⟩.
[3] 三原　元, 佐々木良一：数量化理論と CCCDATAsets2009 を利用したボットネットの C&C サーバ特定手法の提案と評価，情報処理学会論文誌，Vol.51, No.9, pp.1579–1590 (2010).
[4] 林知己夫：数量化—理論と方法，朝倉書店 (1993).
[5] Jang, D.I., Kim, M., Jung, H.C. and Noh, B.N.: Analysis of HTTP2P Botnet: Case Study Waledac, *2009 IEEE 9th Malaysia International Conference on Communications* (*Micc*), pp.409–412 (2009).
[6] Lu, W., Tavallaee, M. and Ghorbani, A.A.: Automatic Discovery of Botnet Communities on Large-Scale Communication Networks, *Proc. 4th International Symposium on Information, Computer, and Communications Security, ASIACCS'09* (2009).
[7] Nelms, T., Perdisci, R. and Ahamad, M.: ExecScent: Mining for new C&C domains in live networks with adaptive control protocol templates, *Proc. 22nd USENIX Conference on Security* (*SEC'13*), pp.589–604 (2013).
[8] Tsai, M.H., Chang, K.C., Lin, C.C., Mao, C.H., Lee, H.M. and IEEE: C&C Tracer: Botnet Command and Control Behavior Tracing, *IEEE International Conference on Systems, Man and Cybernetics* (*SMC*), pp.1859–1864 (2011).
[9] Antonakakis, M., Perdisci, R., Lee, W., Vasiloglou, N. and Dagon, D.: Detecting Malware Domains at the Upper DNS Hierarchy, *20th USENIX Security Symposium*, San Francisco (Aug. 2011).
[10] 津田　航：複数の DNS トラフィック特徴量を用いた多様なボットネットに与するドメイン検知システムの実装と評価 (2015)，入手先 ⟨http://library.naist.jp/dspace/handle/10061/9994⟩.
[11] IBM Knowledge Center, available from ⟨http://www-01.ibm.com/support/knowledgecenter/SS3RA7_15.0.0/com.ibm.spss.modeler.help/svm_howwork.htm?lang=en⟩.
[12] 中村暢宏，佐々木良一：累積データを用いたボットネットの C&C サーバ特定手法の評価，コンピュータ・セキュリティシンポジウム 2011 論文集，No.3, pp.456–461 (2011).
[13] 岡安翔太，佐々木良一：ボットネットの C&C サーバ特定手法の経年変化データを用いた評価，第 76 回全国情報処理学会論文集 (2014).
[14] 畑田充弘ほか：マルウェア対策のための研究用データセット—MWS 2011 Datasets，MWS2011 (2011).
[15] 大村　優，畑田充弘：PRACTICE Dataset，MWS2013 (2013)，入手先 ⟨http://www.iwsec.org/mws/2013/about.html⟩.
[16] マルウェア対策研究人材育成ワークショップ，入手先 ⟨http://www.iwsec.org/mws/2014/⟩.
[17] DNS-BH – Malware Domain Blocklist, available from ⟨http://www.malwaredomains.com/⟩.
[18] The top 500 sites on the web, available from ⟨http://www.alexa.com/topsites/global⟩.
[19] Gome, available from ⟨http://www.gomez.co.jp/⟩.
[20] FORTUNE, available from ⟨http://archive.fortune.com/⟩.
[21] 株式会社エスミ，入手先 ⟨http://www.esumi.co.jp/⟩.
[22] scikit-learn, available from ⟨http://scikit-learn.org/stable/⟩.
[23] 赤池弘次，甘利俊一，北川源四郎，樺島祥介，下平英俊：赤池情報量基準 AIC (2007).
[24] Squid, available from ⟨http://www.squid-cache.org/⟩.

岡安 翔太 （正会員）

平成 22 年 4 月東京電機大学未来科学部情報メディア学科入学．卒業研究でネットワーク・セキュリティに関する研究を実施．平成 26 年 3 月同大学卒業．同年 4 月東京電機大学大学院入学．平成 28 年 3 月同大学院修了．同年 4 月東日本電信電話株式会社入社．

佐々木 良一 （正会員）

昭和 46 年 3 月東京大学卒業．同年 4 月日立製作所入社．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．平成 13 年 4 月より東京電機大学教授，工学博士（東京大学）．平成 14 年情報処理学会論文賞受賞．平成 19 年総務大臣表彰等．著書に，『IT リスクの考え方』(岩波新書, 2008 年) 等．日本セキュリティ・マネジメント学会前会長，内閣官房サイバーセキュリティ補佐官．本会フェロー．