ドメイン情報の分析による Drive by Download 攻撃の対策の提案

木村匡[1]　　佐々木良一[1]

概要： 近年，不正アクセス手法の 1 つである Drive by Download 攻撃によるマルウェア感染の被害が深刻になっている．この攻撃は複数の悪性 Web サイトの連携によって行われる．現在の対策手法の 1 つには悪性 Web サイトをブラックリストに登録し，掲載された悪性 Web サイトへのアクセスを遮断する手法がある．しかし，攻撃者は次々に悪性 Web サイトを設置しており，即座にブラックリストに追加することは不可能である．よって新たに設置された悪性 Web サイトへの対策が困難となる．そこで，我々は Web サイトのドメインから得られるレコードの個数などの情報に着目した．DNS のドメイン情報を収集・分析し，それによって得られた特徴を基に機械学習での Web サイトのドメインの分類実験を行った．その結果，92.75%のドメインを正しく分類できた．よって本稿ではその報告を行う．

Proposal of Countermeasure against Drive by Download Attack by Analyzing Domain Information

TADASHI KIMURA[1]　　RYOICHI SASAKI[1]

はじめに

近年,Drive by Download（以下，DbD）攻撃によるマルウェア感染被害が増加している．DbD 攻撃とは，複数の悪性 Web サイトの連携によって引き起こされる不正アクセスの手法である[1]．DbD 攻撃によるマルウェア感染は，入り口サイト，中継サイト，攻撃サイト，マルウェア配布サイトの 4 種類の悪性 Web サイトによって一般的に引き起こされる．DbD 攻撃の流れを図 1 に示す．

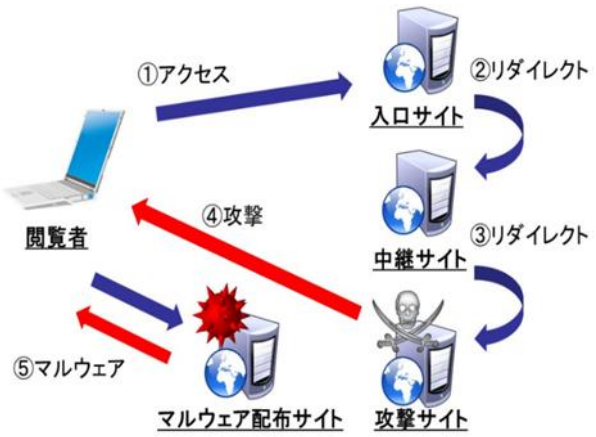

図 1．DbD 攻撃の流れ

入り口サイトとは攻撃者が改竄を行った正規 Web サイトや攻撃者が設置した悪性 Web サイトである．閲覧者が入り口サイトにアクセスをすると，JavaScript や iframe タグにより中継サイトにリダイレクトが行われる．DbD 攻撃にはコードに難読化の処理が施された JavaScript（以下，難読化 JavaScript）が利用される．難読化は攻撃コードのセキュリティソフトによる検知の回避や，攻撃コードの解析の妨害などの目的で行われる．中継サイトにリダイレクトされた後は，攻撃サイトへとリダイレクトが行われる．攻撃サイトではプログラムの脆弱性を狙った攻撃が行われる．攻撃が成功した場合，コンピュータの制御が奪われ，マルウェア配布サイトよりマルウェアが強制的にダウンロード，インストールされてしまう．

現在のDbD攻撃の代表的な対策方法にブラックリスト方式がある．ブラックリストに掲載されたURLへのアクセスを遮断することにより, DbD攻撃に対応している. しかし，攻撃者はブラックリストに掲載されたWebサイトを削除しており，次々にDbD攻撃に関わる悪性Webサイトを設置している．設置されたWebサイトを即座にブラックリストに追加することは難しいので，それらの悪性Webサイトの対策に遅れてしまう．

そこで，我々はDomain Name System（以下，DNS）のドメイン情報に着目した．ブラックリストに掲載された悪性Webサイトの中で，DbD攻撃に関わるWebサイトのドメイン（以下，DbDドメイン）と正規Webサイトのドメイン（以下，良性ドメイン）を分析した．その結果,ドメイン情報の個数や値に差異があることが確認された．

本研究では，それらのドメイン情報をパラメータとした機械学習でのドメインの分類を行う手法の提案を行う．いくつかのドメイン情報を組み合わせて実験を行い，最適な組み合わせを導出する．

この手法によってDbDドメインと分類されたドメインを含むURLへのアクセスを遮断することによって，ブラックリストに掲載されていないDbD攻撃サイトへの対応が可能となると考えられる．

1 東京電機大学

2. 関連研究

岡安ら[2]は，ドメイン情報を用いたドメインの分類により，ボットネット[3]のC&Cサーバの特定手法を提案している．ボットネットの対策として，ボットネット全体を3つに分割して攻撃者を段階的に特定していくシステムの構想がある．ボットPC群からC&Cサーバへのトレースバックにおいて，ドメインを分類することにより攻撃者の特定の一助を担っている．C&Cサーバのドメインからドメイン情報を取得し，数量化理論Ⅱ類[4]およびサポートベクターマシン（以下，SVM）[5]によってドメインをボットネットに関連のあるドメインとボットネットに関係の無いドメインに分類している．

同様にドメイン情報を利用した悪性Webサイトの対策手法には，Ma[6]らの研究がある．こちらはフィッシングサイトやスパムに関連するサイトを対象にしている．URLの文字列やDNSのレコード，WHOIS情報などの特徴を用い，95%以上のURLを正しく分類している．

また，難読化JavaScriptの検知に着目したDbD攻撃の対策が多くの研究者によって盛んに行われている．Jodavi[7]らはJavaScriptのコード内に隠蔽された特定の関数の出現頻度やeval関数の入れ子の深さの最大値などを特徴とした検知を行っている．蘇[8]らはシャノンのエントロピーやK-Lダイバージェンスなどの情報理論的指標を用いた難読化JavaScriptの対策を行っている．同研究では提案手法の処理速度を計算しており，大規模なデータセットの分析においても高速で処理が可能であることが示されている．Jayasinghe[9]らはJavaScriptエンジンにより得られたOpcodeのログを利用している．Opcodeのキーワードを N-gramにより特徴ベクトル化を行い，機械学習によるDbD攻撃の予測を行っている．

3. 提案方式と実験内容

本研究ではドメイン情報をパラメータとしたSVMでのドメインの分類実験を行った．SVMの実験にはPythonの機械学習ライブラリであるscikit-learn[10]を使用した．

実験の順序として，まず事前調査としてDbDドメインと良性ドメインをDNSサーバに問い合わせる事によってドメイン情報を取得した．次に取得したドメイン情報のレコードの個数や値を特徴量設定値に変換した．そして事前調査を行ったドメイン情報の全ての組み合わせでSVMによるドメインの分類実験を行い，それぞれの分類精度を比較した．

3.1 実験用ドメイン

実験に用いたドメインはDbDドメイン，良性ドメイン共に200件である．DbDドメインはD3M(Drive by Download Marionette)Dataset2015[11]に含まれるURLからドメインを抽出して利用した．D3MDataset2015とはMWS-マルウェア対策研究人材育成ワークショップ[12]より提供されたDbD攻撃の通信記録である．良性ドメインはサイトの規模によってドメイン情報に偏りが発生する恐れがあると考え，大規模ドメイン，中規模ドメイン，小規模のドメインの3規模に分けて調査した．大規模ドメインは世界のアクセスランキングを掲載している”The top 500 sites on the web”[13]から取得した．中規模ドメインはFortune[14]の世界の大企業ランキングから取得した．小規模ドメインも同じくFortuneの中・小規模企業のランキングから取得した．それぞれの実験用ドメインの件数を以下の表１に示す．

表１．実験用ドメインの件数

ドメイン	件数（件）
DbDドメイン	200
大規模ドメイン	100
中規模ドメイン	70
小規模ドメイン	30

3.2 ドメイン情報

事前調査を行ったドメイン情報を以下の表２に示す．

表２．調査ドメイン情報

番号	ドメイン情報	調査用ライブラリコマンド
1	TTL	Resolv
2	Minimum	Resolv
3	Retry	Resolv
4	Expire	Resolv
5	Refresh	Resolv
6	MXレコード	Resolv
7	NSレコード	Resolv
8	TXTレコード	Resolv
9	Preference	Resolv
10	Strings	Resolv
11	Aレコード	DNS-Client
12	国情報	DNS-Client
13	登録期間	WHOISコマンド

ドメイン情報の説明として，番号1から番号5はSOAレコードに記述してある情報であり，それぞれの値を調査した．番号6から番号8および番号11はドメインのDNSレコードでありそれぞれの個数を調査した．なお，番号9のPreferenceはMXレコードの優先度であり，番号10のStringsはTXTレコードの文字列の個数である．番号12の国情報はドメインの割当国を示す．番号13の登録期間はドメインの登録日から有効期限日までの日数である．

調査方法は，番号1から番号10はRubyのResolvライブラリ[15]，番号11および番号12は.NETのDNS-Clientライブラリ[16]，番号13はWHOISコマンドを利用して調査した．事前調査の結果，NSレコード，登録期間において特に差異が大きかったことが確認された．

NSレコードはドメインのゾーン情報を管理するDNSサーバを定義するものである．NSレコードを調査した結果，良性ドメインでは3個以上返答のあった割合が約80%となったのに対して，DbDドメインでは20%未満となった．この理由としては，攻撃者が次々に攻撃サイトの設置を行うために，NSレコードの設定をしていないものと考えられる．NSレコードの事前調査の結果を図２に示す．

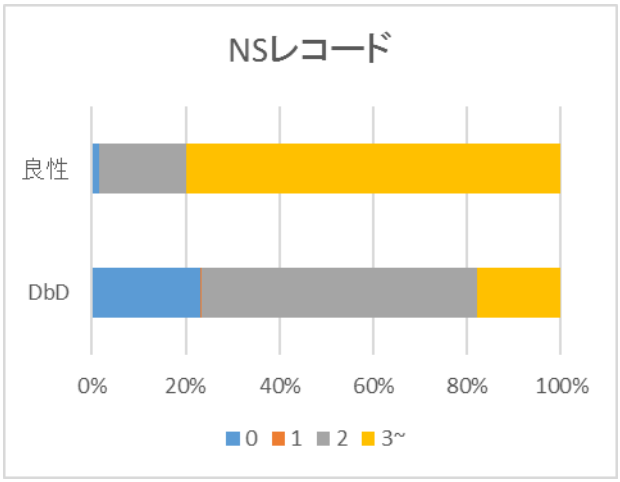

図２．NS レコード

次に，登録期間の事前調査の結果を図３に示す．良性ドメインはDbDドメインに比べて登録期間が長い傾向にあることがわかった．この理由としては，攻撃者が次々にDbD攻撃に関わるWebサイトを出現させていることから，登録期間が短いものと考えられる．

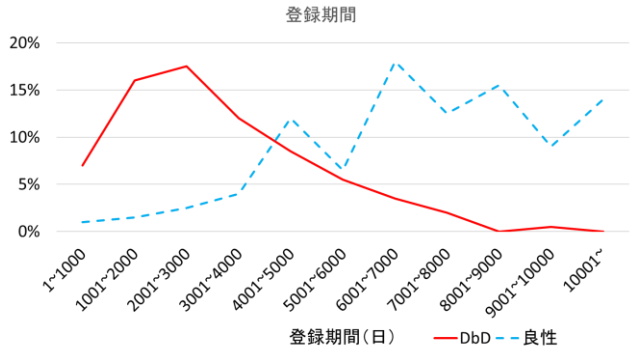

図３．登録期間

3.3 特徴量設定値

実験を行う前に，ドメイン情報を特徴量設定値に変換するスケーリングを行う．スケーリングを行うことで大きい値の範囲を取るドメイン情報による情報落ちを発生させずに分類を行う事ができる．特徴量設定値とは，ドメイン情報のとりうる範囲をあらかじめ設定した値である．それぞれのドメイン情報に1~3，または1~4の特徴量設定値を設定した．この値は，事前調査の結果から，DbDドメインと良性ドメインを最適に分類できるように設定した．例えば，登録期間の場合，登録期間が4000日以下，6000日以上を境目にDbDドメインと良性ドメインの割合の差が変化している．そのため，特徴量設定値はその日数を境界値とした．

ドメインそれぞれのドメイン情報の特徴量設定値を以下の表３に示す．表中のnilはドメイン情報の取得が出来なかったことを示す．

表３．ドメイン情報の特徴量設定値

TTL	特徴量設定値
nil,0 - 1000	1
1001 – 10000	2
10001 -	3

Minimum	特徴量設定値
nil,0 - 1000	1
1001 - 10000	2
10001 -	3

Retry	特徴量設定値
1 – 1000	1
1001 - 3000	2
3001 -	3

Expire	特徴量設定値
0 - 500000	1
500001 - 3500000	2
3500001 -	3

Refresh	特徴量設定値
1 – 1000	1
1001 – 10799	2
10800 – 86399	3
86400, nil	4

MX レコード	特徴量設定値
0 - 1	1
2	2
3	3

NS レコード	特徴量設定値
0	1
1 – 2	2
3 -	3

TXT レコード	特徴量設定値
0	1
1	2
2 -	3

Preference	特徴量設定値
0 – 1	1
2	2
3 -	3

Strings	特徴量設定値
0	1
1	2
2 -	3

Aレコード	特徴量設定値
nil, 0	1
1	2
2 -	3

国情報	特徴量設定値
nil	1
アジア・北米	2
その他地域	3

登録期間	特徴量設定値
nil, 1- 4000	1
4001 – 6000	2
6001 -	3

3.4 SVM

SVMは機械学習に用いる教師ありの学習モデルの1つであり，分類や回帰に適用できる．1963年にVladimir N. Vapnik, Alexey Ya. Chervonenkisが線形SVMを発表し，1992年に

Bernhard E. Boser，Isabelle M. Guyon，Vladimir N. Vapnik が非線形へと拡張した．

SVM の特徴の 1 つ目に線形写像がある．データを変換することによって，線形分類可能にしている．2 つ目にマージン最大化がある．マージンとは識別面と各群に属する個体までの距離の最小値のことである．識別面と距離が最小になる個体をそれぞれサポートベクターと呼ぶ．識別面とサポートベクターとのマージンを最大化することにように学習を行うことで，高い識別性能を得ている．SVM による分類の概要図を以下の図 4 に示す．

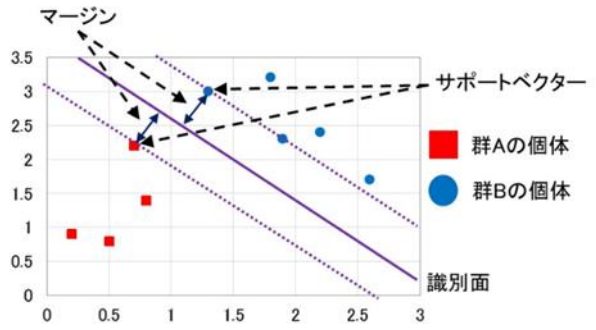

図 4．SVM による分類の概要図

3.5 交差検証法

標本データが少ない場合には，評価データと学習データの選び方によっては，分類精度に誤差が生じる可能性がある．そこで，交差検証法[17]を用いて実験を行い，分類精度の妥当性の検証を行った．

以下の図 5 は交差検証法の概要図である．今回は10分割の交差検証法で実験を行った．まず実験に用いる標本データを10個に分割し，その中の1個を評価データ，残りの9個を学習データとして実験を行う．そのようにして10個に分割された標本データそれぞれを評価データとして10回実験を行う．それらの検知率の平均値を実験の推定検知率とした．今回はDbDドメイン，良性ドメイン共に200件であるので標本データは合計400件となる．10分割した場合は評価データが40件，学習データが360件となる．検知率の算出方法については4.1節で述べる．

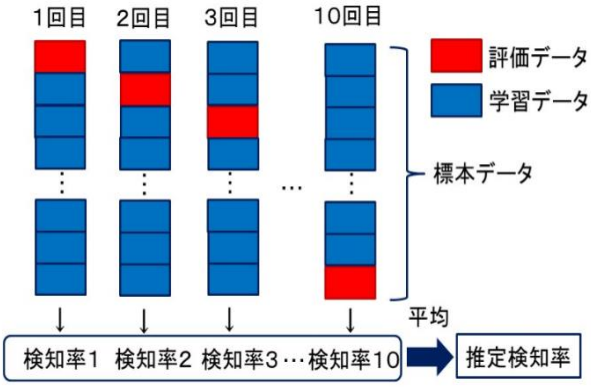

図 5．交差検証法の概要図

4. 評価方法

4.1 検知率

本実験による検知率はドメインが正確に判定された数を基に算出し，提案手法の評価を行う．検知判定の組み合わせを表 4 に示す．DbDドメインがDbDドメインと判定された場合はTruePositive（以下，TP），良性ドメインと判定された場合はFalseNegative（以下，FN）とする．同様に，良性ドメインがDbDドメインと判定された場合はFalsePositive（以下，FP），良性ドメインと判定された場合はTrueNegative（以下，TN）とする．

表 4．検知判定の組み合わせ

	DbDドメインと判定	良性ドメインと判定
DbDドメイン	TP	FN
良性ドメイン	FP	TN

検知率は式(1)から求められる．また，この実験における統計モデルの複雑さとデータとの適合度のバランスを赤池情報量規準[18]によって評価した．

$$\frac{\text{TP の数} + \text{TN の数}}{\text{総ドメイン数}} \quad \cdots \quad \text{式(1)}$$

4.2 赤池情報量規準

赤池情報量規準(以下，AIC)は，統計数理研究所元所長の赤池弘次が1973年に発表した統計モデルの良さを評価するための指標である．実験においてパラメータ数が多いほど検知率が高くなる傾向があるが，ノイズなどの影響を受け，信頼性が低下してしまう恐れがある．そこで，実験結果ごとにAICを算出し比較を行うことで最適パラメータ数を導出することができる．算出されたAICが最小のAICである時のパラメータ数が，多くの場合で最適なパラメータ数である．AICは式(2)によって求められる．ここで，Lは最大尤度であり，正検知数と検知率によって導出される．kは実験に使用するパラメータ数を示す．

$$AIC = -2 \ln L + 2k \quad \cdots \quad \text{式(2)}$$

4.3 F 値

F値はシステムの出力した判定結果などの正確性と網羅性を総合的に評価することに用いる指標である．F値は，式(3)によって算出される．ここで，適合率（以下，Precision）は正確性に関する指標である．実験によってDbDドメインと判定されたドメインの内，実際にDbDドメインであったドメインの割合を示す．Precisionは式(4)によって算出される．また，再現率（以下，Recall）は網羅性に関する指標である．実験用のDbDドメインの内，DbDドメインと判定された割合を示す．Recallは式(5)によって算出される．

$$\text{F 値} = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}} \quad \cdots \quad \text{式(3)}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \quad \cdots \quad \text{式(4)}$$

$$\text{Recall} = \frac{TP}{TP + FN} \quad \cdots \quad 式(5)$$

5. 実験結果

5.1 各パラメータ数での実験結果

各パラメータ数での最高検知率，AICを算出した表５を以下に示す．

表５．各パラメータ数での最高検知率，AIC

パラメータ数	最高検知率 (%)	AIC
2	87.50	97.47
3	91.00	74.66
4	92.75	63.84
5	92.75	65.84
6	93.00	65.99
7	93.25	66.13
8	93.25	68.13
9	93.25	70.14
10	93.25	72.14
11	92.25	81.53
12	92.00	85.37
13	92.50	83.69

今回の実験結果，パラメータ数 7~10 での 93.25%が最も高い検知率となった．しかし，AIC を算出し比較したところパラメータ数 4 での 63.84 が最小 AIC となった. 最小 AIC を算出する k が最適パラメータ数となるので，最適パラメータ数は 4 となる．

5.2 最適パラメータ

パラメータ数4において検知率92.75%を算出した最適パラメータのドメイン情報の組み合わせを以下の表６に示す．

表６．最適パラメータ

ドメイン情報			
Minimum	登録期間	Strings	Expire

5.3 ドメインごとの分類精度

最適パラメータの実験結果を分析した結果，標本データのドメインごとの分類精度は以下の表７のようになった．

表７．ドメインごとの分類精度

ドメイン	標本データ数(件)	正検知数（件）	誤検知数(件)	検知率 (%)
DbDドメイン	200	185	15	92.50
大規模ドメイン	100	91	9	91.00
中規模ドメイン	70	66	4	94.29
小規模ドメイン	30	29	1	96.67

5.4 最適パラメータの F 値，Precision，Recall

最適パラメータのF値，Precision，Recallを以下の表８に示す．今回の実験ではPrecision，Recallの間に大きな差は見られず，DbDドメイン，良性ドメイン共に偏りなく検知出来ていることがわかった．

表８．最適パラメータでのF値，Precision，Recall

F値	Precision	Recall
0.9273	0.9296	0.9250

6. 考察

今回の実験の結果，最適パラメータの検知率は92.75%となった．本研究の提案手法は関連研究[7][8][9]の手法と比較して検知率の点では劣っている．しかし，処理速度に注目すると, JavaScriptは1つのWebサイトにつき複数存在する場合もある．そのため，あるWebサイトに存在する全てのJavaScriptに対して検知を行った場合，処理に時間がかかってしまうことが考えられる．一方，ドメインは1つのWebサイトにつきただ1つに決まるので, 処理速度の点で本研究の提案手法が優れている場合があると考えられる．

実験は13種類のドメイン情報を用いて行ったが，更に最適パラメータの候補となる特徴を用いて，提案手法の改善を行い，検知率を向上させる必要がある．

今回の実験による最適パラメータはMinimum，登録期間, Strings，Expireとなったが，事前調査において差異が顕著であったNSレコードが含まれなかった．これは，SVMによって分類をする上でNSレコードより登録期間の方が分類に大きな影響を与えており，NSレコードが最適パラメータに含まれなかったと考えられる．また，登録期間は2~13のパラメータ数で最も高い検知率を算出したドメイン情報の組み合わせに必ず含まれていた．このことから，登録期間が今回使用したドメイン情報の中で最も分類に影響を与えていることがわかった．

最適パラメータのドメインごとの分類精度に注目すると，標本データの数に差があるものの，良性ドメインの規模が小さくなるほど検知率が高くなる傾向があることが確認された．これは，DbDドメインと小規模ドメインのドメイン情報が異なる傾向にあることが考えられる．また，最適パラメータのPresicion，Recallに差はあまり見られないことから，DbDドメインと良性ドメインが偏りなく分類できていることがわかった．今回の実験で使用した良性ドメインは3規模の組み合わせで構成したが, 検知率に多少の差があることから，ドメインの規模によって最適パラメータが異なる可能性があると考えられる．そこで，良性ドメインの規模ごとに最適パラメータを導出することを検討している．

ドメイン情報はドメインによって年々変化する場合があり，経年変化によって検知率が低下するおそれがある．また，経年変化に伴い最適パラメータも変化する可能性がある．そこで，DbDドメインのドメイン情報に変化が見られるかの調査を行うことが必要であると考えられる．また，D3M2015のDbDドメインだけでなく，他のブラックリストからDbDドメインを取得して実験を行う．可能な限り最新のブラックリストを利用して実験を行い，最適パラメータを導出することがDbD攻撃を対策する上で重要であると考

えられる．

7. おわりに

本研究では，DbDドメインと良性ドメインの分類に13種類のドメイン情報を用いた．13種類のドメイン情報の全ての組み合わせで分類精度を比較し，検知率と分類に有効なドメイン情報を導出した．その結果，AICによりMinimum，登録期間，Strings，Expireの4種類のドメイン情報が分類の最適パラメータであることがわかった．今後は，検知率を92.75%より向上させるために，更に分類に有効な特徴を利用することを検討している．

一方で，ドメインによるフィルタリングはDbD攻撃に無関係なコンテンツも巻き込んでしまう恐れがある．そこで，DbD攻撃に利用されることの多い難読化JavaScriptの検知と提案手法の組み合わせを検討している．具体的にはドメイン情報を利用した分類を始めに行い，DbDドメインと判定されたドメインを含むWebサイトに対して難読化JavaScriptが含まれるかの判定を行う．この2段階の検知手法によってDbD攻撃サイトと判定されたサイトをフィルタリングすることで，誤検知を減少できるのではないかと考えた．

本研究の提案手法については，プロキシサーバを用いたフィルタシステムの実装を検討している．既存の DbD・良性ドメインのリストから最適な分類モデルを作成する．リクエストのあった URL からドメインを抽出し，機械学習での分類を行い，DbD ドメインと判定された場合，アクセスを遮断する．今後はこのようなシステムを構築し，それらの性能を評価することを検討している．

参考文献

[1] ドライブバイダウンロード：危険にさらされる Web, http://www.viruslistjp.com/analysis/?pubid=204792056 (参照 2015-12-10)

[2] 岡安翔太，佐々木良一：ボットネットの C&C サーバ特定手法における数量化理論と機械学習での評価と提案，マルチメディア，分散，協調とモバイル DICOMO2015 シンポジウム（DICOMO2015），pp911-917(2015)

[3] ボットネットとは, http://www.sophia-it.com/content/%E3%83%9C%E3%83%83%E3%83%88%E3%83%8D%E3%83%83%E3%83%88(参照 2015-12-10)

[4] 林知己夫：数量化－理論と方法，朝倉書店(1993)

[5] History of Support Vector Machines, http://www.svms.org/history.html(参照 2015-12-20)

[6] Justin Ma, Lawrence K.Saul, Stefan Savage, and Geoffrey M.Voelker : Beyond Blacklists:Learning to Detect Malicious Web Sites from Suspicious URLs, Proceeding of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining(KDD '09), pp.1245-1254 (2009)

[7] Merhan Jodavi, Mahdi Abadi, and Elham Pah : DbDHunter:An Ensemble-based Anomaly Detection Approach to Detect Drive-by Download Attacks, 2015 5th International Conference on Compoter and Knowledge Engineering(ICKKE), pp.273-278(2015)

[8] 蘇佳偉，吉岡克成，四方順次，松本勉：情報理論的指標と異常検知に基づく難読化 JavaScript 検知手法の提案, コンピュータセキュリティシンポジウム 2015 論文集，Vol.2015，No.3, pp226-233(2015)

[9] Gaya K.Jayasinghe, J.Shane Culpepper,and Peter Betrok : Efficient and effective realtime prediction of drive-by download attacks, Journal of Network and Computer Applications 38, pp.135-149(2014)

[10] scikit – learn:machine-learning in Python, http://scikit-learn.org/stable/index.html(参照 2016-01-17)

[11] 神薗 雅紀，秋山満昭，笠間貴弘，村上純一，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 Dataset2015～，情報処理学会 研究報告 コンピュータセキュリティ(CSEC) Vol.2015-CSEC-70，No6(2015)

[12] マルウェア対策研究人材育成ワークショップ, http://www.iwsec.org/mws/2015/(参照 2016-02-08)

[13] Alexa:The top sites on the web, http://www.alexa.com/topsites (参照 2016-02-15)

[14] Fortune:Fortune500-Daily&Breaking Business News, http://fortune.com/(参照 2016-02-15)

[15] Library Resolv:Ruby 2.1.0, http://docs.ruby-lang.org/ja/2.1.0/library/resolv.html(参照 2015-12-18)

[16] DNS Client Library for .NET, http://simpledns.com/dns-client-lib.aspx(参照 2015-12-18)

[17] Kohavi, Ron: A study of cross-validation and bootstrap for accuracy estimation and model selection, Proceedings of the Fourteenth International Joint Conference on Artificial Intelligence 2, pp.1137-1143.(1995)

[18] 赤池弘次，甘利俊一，北川源一郎，樺島祥介，下平英俊：赤池情報量規準 AIC，共立出版(2007)