Copyright© 2013 The Institute of Electronics,
Information and Communication Engineers

SCIS 2013 The 30th Symposium on
Cryptography and Information Security
Kyoto, Japan, Jan. 22- 25, 2013
The Institute of Electronics,
Information and Communication Engineers

名前解決動作の類似性に基づくマルウェア感染ホストの特定
A Method for Detecting Malware Infected Hosts with Similarity of Name Resolution Behavior

牧田 大佑* Yin Minn Pa Pa* 吉岡 克成* 松本 勉*
Daisuke Makita Yin Minn Pa Pa Katsunari Yoshioka Tsutomu Matsumoto

あらまし マルウェアによるスパムメール送信やサービス妨害攻撃等がインターネット上の大きな脅威となっている．マルウェアの多くは，DNS（Domain Name System）を利用してインターネット上の各種サーバへ接続を試みる．そこで，DNS サーバのトラヒックを分析することにより，マルウェア感染ホストやマルウェアが悪用するドメインを特定する手法が検討されている．本稿では，同一の DGA（Domain Generation Algorithm）やドメインリストを用いるマルウェアに感染したホスト群の名前解決動作は互いに類似することを想定し，ホスト間の名前解決動作の類似性のみを手掛かりに，マルウェア感染ホストを特定する手法を提案する．また，キャッシュ DNS サーバの実トラヒックを用いた実証実験により，本提案手法が既存のブラックリストなどの知識に頼らずにマルウェア感染ホスト群を検知できる例を示す．

キーワード Domain Name System, マルウェア感染ホスト検知

1 はじめに

スパムメール送信やサービス妨害攻撃等のサイバー攻撃を行うマルウェアがインターネット上の大きな脅威となっている．このような脅威に対抗するため，インターネット上のマルウェア感染ホストやマルウェアが悪用するドメイン（以下，悪性ドメイン）を特定する研究が進められている．

インターネット上で通信を行うマルウェアの多くは，一般ユーザと同様，DNS（Domain Name System）を用いて接続先のサーバとの通信を試みる．そこで，マルウェアが利用するドメイン名をブラックリストに登録し，DNS トラヒックを監視することでマルウェア感染ホストを特定する手法（ブラックリスト方式）が検討されている．しかし，近年，解析対象のマルウェアが急増していることに加え，攻撃者はブラックリストによる検知の回避を目的として新しいドメイン名を利用する傾向にあるため，ブラックリストによる対応は困難になりつつある．そこで，DNS トラヒックを分析することにより，マルウェア感染ホストや悪性ドメインを特定する手法が検討されている[1, 2, 3, 4, 5].

本稿では，DGA（Domain Generation Algorithm）のように特定のアルゴリズムに従いドメインを内部生成しこれを利用するマルウェアや，ドメインリストを用いて攻撃者の制御サーバに接続するマルウェアは，その名前解決動作に高い類似性をもつことを想定し，キャッシュ DNS サーバで観測される各ホストの名前解決動作の類似性を調べることでマルウェア感染ホストを特定する手法を提案する．提案手法ではユーザのアクティビティにより発生する名前解決の影響を軽減するため，偶然に一致する可能性の高い人気 FQDN（Fully Qualified Domain Name）に関する名前解決を分析対象から排除する．また，正規のプログラムによる名前解決の影響についても，複数ドメインに渡る類似度を厳密に調べることにより軽減する．実運用中のキャッシュ DNS サーバの実トラヒックを用いた実証実験により，本提案手法が既存のブラックリストなどの知識に頼らずにマルウェア感染ホスト群を検知できる例を示す．

本稿の構成は以下の通りである．まず，2 章で関連研究を概説する．3 章で提案手法を述べ，4 章で実証実験について記述する．5 章で考察を述べ，6 章でまとめと今後の課題とする．

2 関連研究

本章では，DNS サーバのトラヒックを分析することにより，マルウェア感染ホストや悪性ドメインを特定する手

* 横浜国立大学, 240-8501 神奈川県横浜市保土ケ谷区常盤台 79-7,
Yokohama National University, 79-7 Tokiwadai, Hodogaya-ku,
Yokohama-shi, Kanagawa, 240-8501 Japan.

法の先行研究を取り上げる.

論文[1, 2, 3]では，DNS サーバに集まるトラヒックを分析することにより，悪性ドメインを判定する手法がそれぞれ提案されている．これらの手法では，数週間から数ヶ月の DNS トラヒックを分析することにより，正規のドメインと悪性ドメインで異なる特徴を抽出し，その特徴量から悪性が未知のドメインを評価する．いずれの手法においても，高い精度で悪性ドメインを検出できることが評価実験によって示されている.

論文[4]では，DNS サーバのトラヒックから，DGA によって生成されたドメイン名を検知する手法が提案されている. DGA とは接続先のドメイン名を生成するアルゴリズムである. DGA で生成されたと推測されるドメイン名の例を表１に示す．マルウェアは，ブラックリストによる検知の回避を目的として，このようなアルゴリズムを使用すると考えられている．論文[4]で提案されている手法では, DGA で生成されたドメインには応答が存在しない（NXDomain 応答が返される）ことが多く，同じ DGA で生成される文字列には類似性があることに着目している.

表 1　DGA で生成されたと推測されるドメイン名の例

（論文[4]の Figure4 より抜粋）

semk1cquvjufayg02orednzdfg.com
invfgg4szr22sbjbmdqm51pdtf.com
0vqbqcuqdv0i1fadodtm5iumye.com
np1r0vnqjr3vbs3c3iqyuwe3vf.com
s3fhkbdu4dmc00ltmxskleeqrf.com
gup1iapsm2xiedyefet21sxete.com
y5rk0hgujfgo0t4sfers2xolte.com
me5oclqrfano4z0mx4qsbpdufc.com

論文[5]では，既知の悪性ドメインリストと DNS トラヒックを用いて，新たな悪性ドメインを検知する手法が提案されている．この手法では，ボットが名前解決を試みるドメインは１つではないという仮説のもと，既知の悪性ドメインと共起するドメインを抽出することで新たな悪性ドメインの検知を試みている．また，提案手法により既知の悪性ドメインリストだけでは検知できないボット感染ユーザを検知できる可能性についても言及されている.

3　提案手法

本章では，キャッシュ DNS サーバのトラヒックにおけるホスト間の名前解決動作の類似性を調べることにより，既存のブラックリストに依存せず, マルウェア感染ホストの特定を行う手法を提案する．まず 3.1 節で，提案手法のアイディアを述べ，3.2 節で提案手法によるマルウェア感染ホスト検知の手順を説明する.

3.1　提案手法のアイディア

提案手法では，DGA のように特定のアルゴリズムに従いドメインを内部生成しこれを利用するマルウェアや, ドメインリストを用いて攻撃者の制御サーバに接続するマルウェアを検知するため, 名前解決動作の類似性が高いホスト群を感染ホストとして検出する．しかしながら，名前解決動作の類似性が高くなる要因はマルウェア感染以外にも考えられる.

たとえば，Web ブラウジングなどのユーザのアクティビティや正規プログラムによる名前解決動作が類似する可能性がある．そのため，提案手法では，入力となるキャッシュ DNS サーバのトラヒックを事前に解析し，多くのクライアントから名前解決される人気 FQDN を選出し，その後の解析対象から除外する．これにより，人気 Web サイトへのアクセスによりホスト間の名前解決動作が類似する影響を軽減する.

また，同一の正規プログラムが動作するホスト間では，当該プログラムが行う名前解決動作が類似することが予想される．そこで，このような正規プログラムが名前解決するドメインの種類数はマルウェアに比べて少ないことを想定し, 多くの種類のドメインについて名前解決を行っており，かつ，類似性が高いホスト群のみを感染ホストとして検出する.

3.2　マルウェア感染ホスト検知手順

提案手法によるマルウェア感染ホスト検知手順は以下の 4 つのステップからなる.

STEP1 データ収集： キャッシュ DNS サーバのログまたは通信トラヒックから, A レコードに関するクエリを送信したホスト(の IP アドレス)と FQDN の組を抽出する.

STEP2 人気 FQDN の除外 : ホスト間の名前解決動作の類似性に影響を与える可能性の高い人気 Web サイトやそれに関連する FQDN に関するクエリを以降の処理から除外する.

STEP3 名前解決動作の類似性に基づくクラスタリング： ホスト間の類似性スコアを以下のように算出し，これに基づきホスト群のクラスタリングを行う.

まず， 3.1 節で述べたとおり，特定の正規プログラムによる名前解決の影響を軽減するため, 少なくとも T_{domain} 種類のドメインについて名前解決を行っているホストのみを検査対象とし，それ以外のホストについては，以降の処理から除外する.

検査対象の各ホストについて，名前解決した FQDN をドメイン毎の集合に分割し, 各ドメインに関する類似度を算出する．FQDN 集合の類似度としては，様々な指標が考えられるが 4 章の実験ではシンプソン係数を用いている. 集合 X, Y の類似度を計算するシンプソン係数は式(1)

で表される.

$$Simpson(X,Y) = \frac{|X \cap Y|}{\min(|X|,|Y|)} \qquad (1)$$

そして, すべてのドメインに関する類似度の和をホスト間の類似性スコアとする．ただし，FQDN 集合の要素数が T_{FQDN} 未満のドメインについては十分な類似度判定ができないことから，類似性スコアとして加算しない.

2 つのホスト A と B の間の類似性スコア算出の例を図 1 に示す. この例では, ホスト A は com, a.com, net, org, biz の 5 種類のドメインに属する FQDN を問い合わせており，ホスト B は com，a.com，net，org，info の 5 種類のドメインの FQDN を問い合わせている. ホスト A とホスト B に共通する 4 つのドメイン com，a.com，net，org が類似度計算の対象となるが, org ドメインの FQDN 集合は要素数が少ないのでスコア算出対象から除外される．よって，この例では 3 つのドメイン com，a.com，net についてそれぞれ類似度を計算し, この和がホスト間の類似性スコアとなる.

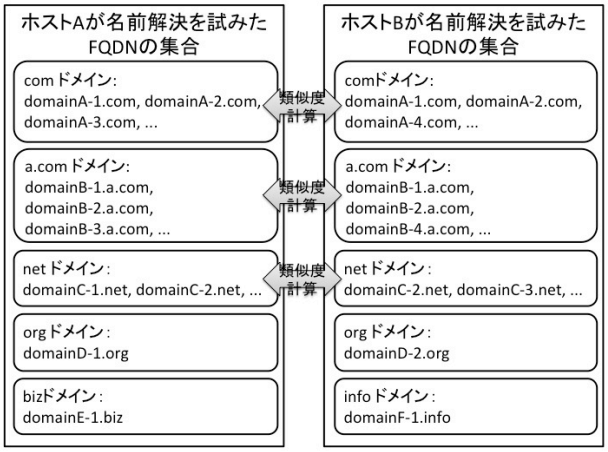

図 1　ホスト間の類似度計算の例

ホストのクラスタリングは類似性スコアに基づき行う. クラスタリングの手法としては, 4 章の実験では階層的クラスタリング[13, 14]を用いている．具体的には，1 個のホストだけを含む N（N はホスト数）個のクラスタがある初期状態から，式(2)の距離関数に基づき，最も距離の近い二つのクラスタを順に併合する．この併合の過程を，全てのクラスタが 1 つに併合されるまで繰り返し，階層構造のクラスタを構築する. この併合が繰り返される過程で，クラスタ間の距離が D 以下ものを名前解決動作が類似するクラスタとして出力する. ただし，クラスタもホスト同様に類似性スコアを計算されるものとし, 類似度計算に利用するクラスタの FQDN 集合は，クラスタ内のホストの三分の二以上のホストが名前解決を試みた FQDN からなるようにした.

4 章の実験で利用したクラスタ C_1，C_2の距離関数（式(2)）を以下に示す.

$$Distance(C_1, C_2) = \frac{1}{1 + \mathrm{C_1とC_2の類似性スコア}} \qquad (2)$$

STEP4 マルウェア感染ホストの特定： STEP3 で出力されたクラスタには, 名前解決動作が類似するホスト群が含まれている．これらのクラスタの中で，多数のドメインについて類似度が高いクラスタをマルウェア感染ホストからなるクラスタとして特定する．4 章の実験では，STEP3 同様に，クラスタ内のホストの三分の二以上のホストが名前解決を試みた FQDN の集合において，T_{inf}以上のドメインの FQDN が存在するものをマルウェア感染ホストと推定した.

4　実証実験

本章ではキャッシュ DNS サーバの実トラヒックを用いた実証実験により提案手法の有効性を検証する．まず 4.1 節で, 実験に使用した DNS トラヒックの概要を説明する. 4.2 節で実験の手順について述べ，4.3 節で提案手法の評価方法を述べる. そして, 4.4 節で実験の結果をまとめる.

4.1　分析対象の DNS トラヒック

本稿では，キャッシュ DNS サーバの実トラヒックを用いて実証実験を行った. 分析した DNS トラヒックの概要を表 2 に示す．なお，本研究では解析段階，送信元等，個々のユーザが特定できる情報は解析していない.

表 2　分析対象の DNS トラヒック

日時	2012 年 6 月の平日 22 時台で 1 時間程度
問い合わせ数	1 億～2 億
ホスト数	100 万～200 万
FQDN 数	300 万～400 万

4.2　実験方法

本節では実証実験の手順を記述する.

STEP1 データ収集： まず，DNS キャッシュサーバのトラヒックから, A レコードの問い合わせに関するクエリの送信元 IP アドレスと FQDN の組を抽出した．抽出した FQDN の中には，不正な形式の FQDN[1]が多数確認されたため，この段階で不正な形式の FQDN を除外した.

1 ここでは，FQDN のトップレベルドメインが存在しない値のもの，及び，FQDN の文字列中に英数，ハイフン，ピリオド以外の文字が含まれているものを不正な形式とみなした.

STEP2 人気 FQDN の除外： 本実験では，次の条件に当てはまる FQDN のクエリを解析対象から除外した．

- Alexa [6]で公開されている人気サイトランキングのうち，上位 10,000 以内のドメインに関する FQDN（ランキングは 2012 年 10 月 31 日付の Global 版を使用）
- STEP1 で収集した FQDN の中から，5,000 以上のユーザに名前解決された FQDN
- トップレベルドメインが分析対象のキャッシュ DNS サーバが設置されている国の ccTLD となっている FQDN

人気 FQDN を除外することにより，解析対象のホストを 4 割まで削減することに成功した．

STEP3 名前解決動作が類似するホストのクラスタリング： 本実験では，$T_{domain} = 3$，$T_{FQDN} = 5$ とし，クラスタ間の距離 D が 0.3 以内のクラスタを，名前解決挙動が類似するクラスタとした．

STEP4 マルウェア感染ホストの特定： STEP3 で出力されたクラスタ（ホスト群）について，各クラスタのホストの三分の二以上が名前解決を試みた FQDN の集合でドメイン数が $T_{inf} \geqq 5$ となるクラスタを出力した．

4.3 評価方法

提案手法の有効性を検証するため，4.2 節で出力されたクラスタがマルウェア感染ホストを含んでいる可能性を次の 3 段階の手順で評価する．

評価方法1.
既存のブラックリストによる評価

評価方法2.
セキュリティベンダのレポートによる評価

評価方法3.
FQDN の表層表現に関する主観的評価

まず，既存のブラックリストを用いた評価(評価方法 1)を行う．検証に利用した 4 種類のブラックリストについて，ブラックリスト名，登録ドメイン数，ブラックリストの取得日を表 3 に示す．なお，ドメインの登録日が記載してある DNS-BH と Malware Domain List（MDL）に関しては, DNS トラヒックの取得日(2012 年 6 月 21 日）以前に登録されていたリストを別に用意し（それぞれ DNS-BH/JUN，MDL/JUN と表記），本提案手法の評価の参考とした．

表 3 検証に使用したブラックリスト

ブラックリスト名	登録ドメイン数	取得日
DNS-BH [7]	9,052	2012 年 11 月 12 日
Malware Domain List (MDL) [8]	43,979	2012 年 11 月 12 日
Exposure [9]	107,179	2012 年 11 月 12 日
Zeus Tracker [10]	844	2012 年 11 月 14 日

これらのブラックリストには，改竄された正規の Web サイトや悪用されている正規のサービス, 悪質な広告サイトと推測されるドメイン名や FQDN が含まれている．そこで，本実験では，各ホストが名前解決を試みた FQDN のうち少なくとも 3 つ以上の FQDN がいずれかのブラックリストで検知されたものをマルウェア感染ホストとみなす. なお, 既に使用されなくなったドメイン名や FQDN がブラックリストから削除されている可能性に関しては考慮していない.

次に，評価方法 1 で感染が確認されなかったクラスタに対して, セキュリティベンダのレポートによる評価を行う．具体的には，クラスタを構成するホスト群が共通して名前解決する FQDN を抽出し, Web 検索エンジンで検索し，マルウェアに関する記述が見つかったものを悪性 FQDN とみなし，この名前解決を試みたホストを感染ホストとする．

最後に，評価方法 1 と評価方法 2 で感染が確認されなかったクラスタに対して, そのクラスタに属するホスト群が共通して名前解決した FQDN に関して著者による主観的評価を行った. 具体的には, 表 1 に記述したような DGA で生成されたと推測される FQDN が多量に存在するかどうかを著者が確認し, マルウェア感染ホストであるかどうかを判断した.

4.4 実験結果

4.2 節の STEP4 で出力された上位 10 個のクラスタに関して 4.3 節の評価方法で検証した結果を表 4 に示す. なお，表 4 の推定マルウェア名は，該当クラスタのホスト群が共通して名前解決を試みた FQDN を Web 検索し，得られた情報から推定した.

表 4　提案手法により検出されたクラスタの検証

クラスタ No.	ホスト数	FQDN の類似性が高いドメイン	ブラックリストで検知されたホスト数							推定マルウェア名	評価
			DNS-BH/JUN	DNS-BH	MDL/JUN	MDL	Exposure	ZeuS Tracker	全体		
1	7	monbe.be. net. netsolhost.com. org. info. tk. co.tv. biz. eu. in. cc. cx.cc. de. com. cn. ru. co.cc. cz.cc. rel7.com. fileave.com. nl.	7	7	7	7	7	6	7	ZeusS/ Zbot? [8, 10]	感染（評価方法 1）
2	256	net. org. info. ws. cc. com. cn. biz.	0	1	1	1	255	1	255	W32.DownadupB (Symantec) [11]	感染（評価方法 1）
3	3	net. ru. info. osa.pl. ce.ms. com. cn. co.cc.	3	3	3	3	3	2	3	ZeuS / Zbot? [8, 10]	感染（評価方法 1）
4	9	net. ru. info. biz. com. org.	0	0	0	0	0	0	0	Unknown	感染（評価方法 3）
5	71	net. org. no-ip.org. com. ath.cx. no-ip.info.	0	0	0	0	49	0	49	Unknown	感染（評価方法 1）
6	25	net. in. info. kz. com.	1	1	0	0	0	0	1	OSX/Flashfake (McAfee) [12]	感染（評価方法 2）
7	3	com. net. biz. org. info.	0	0	1	1	1	0	1	Unknown	感染（評価方法 3）
8	2	info. net. biz. org. com.	0	0	0	0	0	0	0	−	非感染
9	2	info. net. biz. org. com.	0	0	0	0	2	0	2	Unknown	感染（評価方法 1）
10	2	net. org. info. biz. com.	0	0	0	0	0	0	0	−	非感染

4.2 節で出力された上位 10 個のクラスタのうち，クラスタ No. 1，No. 2，No3，No.5，No. 9 については，構成ホスト群の多くがブラックリストに掲載されている FQDN の名前解決を行っており，感染ホスト検出におおむね成功している．クラスタ No. 6 は既存のブラックリストでは，ほとんど検知されなかったが，クラスタ No. 6 に属する全ホストが共通して名前解決を行っている FQDN “tgnqheyqmfogmgt.kz”について Web 検索エンジンを用いて情報収集したところ，明らかにマルウェアによる名前解決であることが確認できた．クラスタ No. 4 と No. 7 については，ブラックリストによる検知も，Web 検索エンジンによる確認においても悪性であると判断できなかったが，主観的評価により我々はこの 2 つのクラスタも DGA を行うマルウェア感染ホストを含むと考えている．クラスタ No.4 と No.7 に属するホストが名前解決した FQDN の一部をそれぞれ表 5，表 6 に示す．クラスタ No. 8 と No. 10 はいずれの段階の評価においてもマルウェア感染に関連する挙動は確認できず，誤検出と考えられる．

表 5　DGA で作られたと推測される FQDN（No.4）

pzevgwfwn60cxj26fwbrlvn60dsh24a57bsa27.net.
pyh44frdxbsp22jui45otd40gypxevjsmyaq.com.
pvfvn30dxg23kxp22fxgvgyerctbsitcrfw.net.
puktpsaxd40dxm19d60jroxe51d10psfzf32e11.info.
pslxayntlvb58m59bygzptf42b18dyhydups.net.
psjxm59p42avdvm69cqf22byj36l68j56f22cuhr.biz.
prn10i55oscvnviuc29ovnrbrhxexcsg63m39.biz.
p62msarbxb28nskul18j16gshrewg23bqp52l18.ru.

表 6　DGA で生成されたと推測される FQDN（No.7）

ytptqonxrtqkiju.org.
ytptqonxrtqkiju.com.
ykorwpevroqhjmp.org.
ykorwpevroqhjmp.net.
yjpuzxnjlmtigonu.info.
yjpuzxnjlmtigonu.biz.
xjvulxrudkfrotm.org.
xjlgveipohlvwh.net.

5　考察

前章の実証実験により, 複数ホスト間の名前解決動作の類似性を調べることによって, マルウェア感染ホストを特定できる例が確認できた. 実証実験において特定したホストの中には，評価用に用意した既存の 4 種類のブラックリストでは検知できないホストも存在しており, 本提案手法によって既知のブラックリストでは発見できないマルウェア感染ホストを特定できる可能性があると考えられる．また，表 4 には含まれていないが，実証実験で検知したホストについて，2012 年 6 月以前のブラックリスト（DNS-BH/JUN, MDL/JUN）では感染が確認されないものの，2012 年 11 月時点のブラックリストでは感染が確認されるようになったものも存在しており, 本提案手法によって既知のブラックリストのみを利用した検知よりも早期に感染ホストを特定できる例といえる．更に，提案手法で検知されたマルウェア感染ホスト群によって共通して名前解決される FQDN はマルウェアに悪用されている可能性が高いと考えられるため，本提案手法は悪性 FQDN のブラックリストの作成にも有用であると考えられる.

なお, 提案手法では名前解決動作の類似性を利用するため, 名前解決が少ないマルウェアは検知することができない．最後に，本実験では，各種パラメータや類似度定義, クラスタリングアルゴリズムの検討は詳細に行なっていない．これらを変更することで，より精度の高い検知を実現できる可能性もあるため, 今後これらの検討を進めていきたいと考えている.

6　まとめと今後の課題

本稿では, 同種のマルウェアに感染したホストが試みる名前解決動作は高い類似性を有するという想定のもと, ホスト間の名前解決動作の類似性を調べることにより, マルウェア感染ホストを特定する手法を提案した．また，キャッシュ DNS サーバに実トラヒックに対して本提案手法を適応することにより，本提案手法が，DGA（Domain Generation Algorithm）などを用いて多数の FQDN の名前解決を試みるマルウェアに感染したホスト群を検知できることを確認した.

今後は, 提案手法で使用した各種パラメータやアルゴリズムの検討, 及び, 提案手法では特定できないマルウェア感染ホストを検知する手法を考案することが課題として挙げられる．また，本提案手法を応用して長期に DNS キャッシュサーバのトラヒックを観測することにより, 大規模なサイバー攻撃の原因となりうるマルウェア感染ホストの動向を把握することも検討している.

謝辞　本研究の一部は, 総務省情報通信分野における研究開発委託／国際連携によるサイバー攻撃の予知技術の研究開発／サイバー攻撃情報とマルウェア実体の突合分析技術／類似判定に関する研究開発により行われた.

参考文献

[1] Leyla Bilge, Engin Kirda, Christopher Kruegel and Marco Balduzzi, “ EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis, ” In Proceedings of NDSS, 2011.
[2] Manos Antonakakis, Roberto Perdisci, David Dagon, Wenke Lee, and Nick Feamster, “Building a Dynamic Reputation System for DNS,” In the Proceedings of 19th USENIX Security Symposium, 2010.
[3] Manos Antonakakis, Roberto Perdisci, Wenke Lee, Nikolaos Vasiloglou and David Dagon, “ Detecting Malware Domains at the Upper DNS Hierarchy,” In the Proceedings of 20th USENIX Security Symposium, 2011.
[4] Manos Antonakakis, Roberto Perdiscit, Yacin Nadji, Nikolaos Vasiloglou, Saeed Abu-Nimeh, Wenke Lee and David Dagon, “From Throw-Away Traffic to Bots: Detecting the Rise of DGA-Based Malware,” In the Proceedings of 21st USENIX Security Symposium, 2012.
[5] 佐藤 一道, 豊野 剛, 石橋 圭介, 三宅 延久, “DNS トラフィックデータを利用したボット感染者検出方法,” 情報処理学会研究報告 2009-IOT-7 No.11, pp.1-6.
[6] Alexa - The Web Information Company, http://www.alexa.com/, last visited 2012/12/07.
[7] DNS-BH - Malware Domain Blocklist, http://www.malwaredomains.com/, last visited 2012/12/07.
[8] MALWARE DOMAIN LIST, http://www.malwaredomainlist.com/, last visited 2012/12/07.
[9] Exposure - Malicious DNS world activity, http://exposure.iseclab.org/, last visited 2012/12/07.
[10] Zeus Tracker, https://zeustracker.abuse.ch/monitor.php, last visited 2012/12/07.
[11] ThreatExpert, http://www.threatexpert.com/report.aspx?md5=6b6ba315c9f8d83bdb08f2d16dddc1ce, last visited 2012/12/07
[12] McAfee Labs Threat Advisory OSX/Flashfake, https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/23000/PD23747/en_US/Threat_Advisory_OSX_Flashfake.pdf, last visited 2012/12/14.
[13] 神嶌 敏弘, "データマイニング分野のクラスタリング手法(1) － クラスタリングを使ってみよう！ －," 人工知能学会誌, 18 巻 1 号, pp.59-65 (2003).
[14] Toby Segaran 著, 當山 仁健, 鴨澤 眞夫 訳,「集合知プログラミング」, オーム社 (2008) .