Drive-by-download 攻撃通信の可視化システム

松本浩明 †　　石井啓之 †　　薄羽大樹 ‡　　菊池浩明 ‡

† 東海大学大学院
108-8619 東京都港区高輪 2-3-23
matsumoto@ishiilab.net

†† 明治大学総合数理学部
〒 164-8525 東京都中野区中野 4-21-1
kikn@meiji.ac.jp

あらまし Drive-by-download 攻撃による通信の特徴を抽出するため，HTTP 通信のフローを可視化するシステムを構築した．本システムを用いて攻撃時の通信と正規通信との比較を行う．

Visualization system for Drive-by-download traffic

Hiroaki Matsumoto†　　Hiroshi Ishii†　　Hiroki Usuba‡　　Hiroaki Kikuchi‡

†Graduate School of Information and Telecommunication Engineering, Tokai University,
2-3-23 Takanawa, Minato, Tokyo, 108-8619 Japan
matsumoto@ishiilab.net

‡School of Interdisciplinary Mathematical Sciences, Meiji University
4-21-1 Nakano, Nakano, Tokyo, 164-8525 Japan
kikn@meiji.ac.jp

Abstract To extract features of Drive-by-download trafficattacks, we developconstructed a system for visualizing the flow of HTTP traffic. We show the compared comparison between the attack malicious traffic with and a normal benign traffic using this system.

1　はじめに

Web サイト上にマルウェアを設置しておき，その Web サイトにアクセスしてきた閲覧者に対して自動的にそのマルウェアをダウンロードさせるなどして閲覧者のパソコンに攻撃を行う Drive-by-Download 攻撃（以下，DbD 攻撃）が大きな脅威となっている．2014 年 7 月には，世界最大の男性向けライフスタイルマガジンであり，米国内で 1ヵ月あたりおよそ 1,400 万人もの読者層がいる AskMen の Web サイト上に，ランサムウェアをデスクトップにインストールする DbD 攻撃が発生していた事例などがあった [1]．DbD 攻撃では Adobe や JRE などの各種製品の脆弱性をついた攻撃などが行われている．また，これらの製品に含まれている多数の脆弱性をパッケージングし，様々な環境において DbD 攻撃が行われるようにした Exploit Kit と呼ばれるツールも各種提供されている．DbD 攻撃におけるほとんどの脅威の原因がこの Exploit Kit であるという報告もある [2]．

本研究では，DbD 攻撃が行われる際の通信と正常なサイトを閲覧した際の通信の差異を比較することにより，DbD 攻撃通信を検知することを目的とする．しかしながら，DbD 攻撃の通信と正常なサイトの通信の差は小さく，特徴量を

決定づけるのは非常に難しい．そこで機械学習の適用と，DbD 攻撃による通信を視覚的にするシステムを併用する．

桑原らは，[3] で同一マルウェアにおいては攻撃の際に用いられる脆弱性，リダイレクトなどによって遷移するパスに共通性があるのではという点に着目している．[4] で北野らは，Exploit Kit が使用された攻撃において発生する状態遷移に着目している．[5] で笠間らはは既知の Exploit Kit における特徴の抽出を行いそれに基づく検知を行っている．これらの手法では，アクセスの際に発生した通信から DbD 攻撃の検知を行うことを目的としており，FQDN や IP アドレスに関する特徴についてはその変化の激しさから特徴量の対象とはしていない．これらの研究に対し [6][7] では DbD 攻撃を行うサイトの FQDN や IP アドレスを特徴とする手法について提案をしている．[6] で千葉らは対象となるサイトの IP アドレス，WHOIS 情報，FQDN 文字列について分析を行い，DbD 攻撃の判別を行っている．[7] で田中らはマルウェアが感染後に行う通信で要求されるドメインを基に判別を行っている．マルウェア感染後に要求される通信と既知の悪性ドメインリスト等を組み合わせ悪性サイトの抽出を行っている．

先行研究で挙げられている特徴量では，抽出された特徴量を基にシグネチャの生成などを行い DbD 攻撃の検知を行っている．Exploit Kit の亜種が大量に生成されたり，悪性サイトのライフサイクルが短かったりすることを考えると，これらの手法では既知の攻撃手法に強く未知の攻撃手法には弱くなりやすい．

そこで本研究では，[4][5] におけるアプローチに近い手法を提案する．DbD 攻撃通信において変化が発生しやすい特徴量について着目し，その特徴量についての変化が視覚的に確認できるようなシステムの構築を行うことによって判別の補助を試みる．予備実験において観測された DbD 攻撃における特徴的な通信に着目し，可視化システムを構築することを提案する．

以下 2 章では DbD 攻撃の説明のほか，MWS Datasets の説明を行い，3 章では本研究における可視化システムについての提案手法と使用する技術詳細について述べる．4 章で DbD 攻撃と正常なサイトとの通信の判別のために行った実験とその結果，及び考察について述べ，5 章でまとめとする．

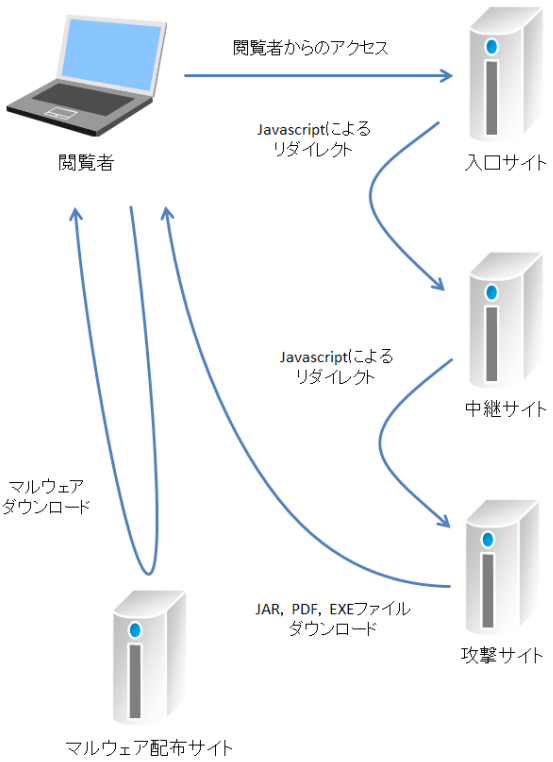

図 1: DbD 攻撃通信の流れ

2 準備

2.1 Drive-by-Download 攻撃

図 1 に一般的な DbD 攻撃の流れを示す．図 1 は，本稿で用いたデータセットの一つである．

DbD 攻撃は大きく分けて，入口サイト，中継サイト，攻撃サイト，マルウェア配布サイトと呼ばれる 4 つのサイトから構成されていていることがほとんどである．

入口サイトでは主に閲覧者に対して，攻撃サイトへの誘導が行われる．攻撃サイトへの誘導方法は様々で，iframe などの HTML タグを利用したものや Javascript などを用いたものなどがある．このような入口サイトは攻撃者が直接用意したサイトだけでなく，正規の Web サイ

トが改ざんされて入口サイトとなっているケースなどもある．

中継サイトでは文字通り入口サイトから攻撃サイトへの中継が行われる．301，302 ステータスコードなどの Redirection や Reflesh などによるリダイレクトが行われ，入口サイトから誘導されてきた閲覧者は攻撃サイトへと誘導される．中継サイトは複数経由されることもあり，リダイレクトが複数回発生することもある．

攻撃サイトでは閲覧者のパソコンに対してマルウェアをダウンロードさせるため，脆弱性を突く攻撃コードがダウンロードされる．閲覧者のパソコンに JAR ファイルや PDF ファイルなどをダウンロードさせることが多い．

マルウェア配布サイトでは脆弱性により実行された攻撃コードをもとにマルウェアのダウンロードが行われ，閲覧者のパソコンにマルウェアがインストールされる．

以上のように入口サイトから誘導が行われ，複数のサイトを経由し，最終的に閲覧者のパソコンの脆弱性をつかれることによりマルウェアのダウンロードが行われてしまうのが DbD 攻撃の一連の流れとなっている．

2.2 D3M Dataset

D3M は MWS Datasets[8] に含まれるデータセットのうちの一つである，秋山らが開発した高対話型クライアントハニーポット [9] を用いて，公開ブラックリストにアクセスし DbD 攻撃通信を検知した際に記録された攻撃通信データ，DbD 攻撃によってダウンロードされた ma マルウェア，ダウンロードされたマルウェアをサンドボックス上で実行した際のマルウェア通信データからなっている．このデータセットにおける攻撃通信データはすべて DbD 攻撃が行われたと検知されたものである．使用したデータセットの概要を表 1 に示す．

このキャプチャデータには，期間ごとに複数の DbD 攻撃通信が含まれているため，データセットに付属する不正 URL リストと一致するパケットを基準とし分割を行った．分割された一連の DbD 攻撃をセッションと呼ぶ．セッション内で，リダイレクトが行われる単位をドライブと呼ぶ．ドライブ ID を識別に用いる．例えば，図 1 は単一のセッションであり，攻撃サイトは第 3 ドライブである．

表 1: D3Mdatasets の概要

データセット	期間	入力 URL 数	HTTP レスポンス数
D3M 2014	2014/4/11	2	91
	2014/4/10	12	226
	2013/8/30	36	43
	2013/4/12	6	11
D3M 2013	2013/2/26	9	67
	2012/10/2	18	98
	2012/8/2	19	85
D3M 2012	2012/3/21	43	570
	2012/3/23	36	375
	2012/3/25	37	332
	2012/3/28	42	479

2.3 決定木

DbD 攻撃通信データと正常サイト閲覧通信データの判別を行うために決定木学習を行った．決定木の生成には Weka[10] を用いた．

DbD 攻撃通信データと正常サイト閲覧通信データから特徴量となりえるデータを推定，抽出を行い入力用データセットとした．決定木生成に使用した学習アルゴリズムは J4.8 である．

3 提案手法

3.1 データセットの解析

決定木学習用のデータセットについて解析を行った結果を述べる．

正常サイトとの通信例として，Alexa[11] の提供している Top サイトから上位 50 件分の通信をキャプチャしたものを用意した．

これらの通信において，特に DbD 攻撃において関連性の高いと思われる種類のファイル別に通信量の分布を図 2，図 3 に示す．また正常サイトについても同様に図 4 に示す．

図 2，図 3 ではそれぞれ正常サイト閲覧時の通信，緑色の Javascript のグラフに加え他の色であらわされている JAR，PDF ファイル，EXE

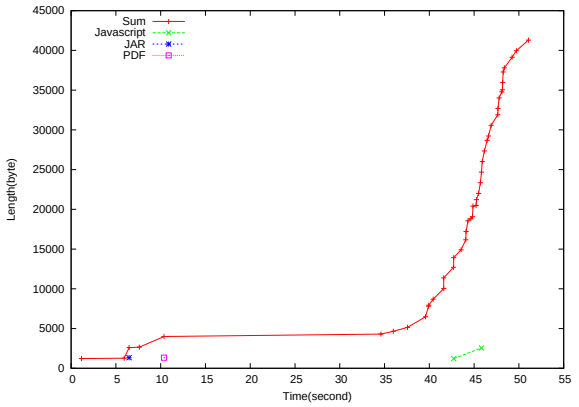

図 2: DbD 攻撃における各種トラフィックの累積分布 (2012 年 3 月 28 日-3)

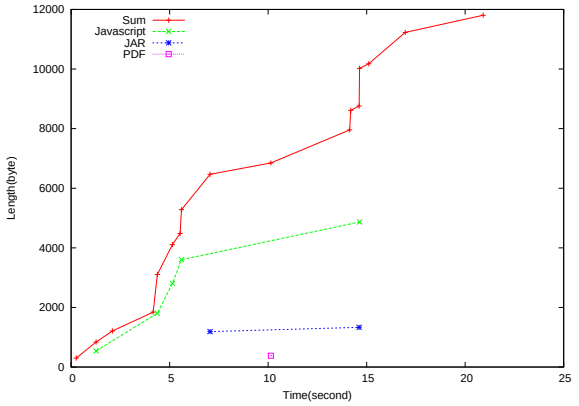

図 3: DbD 攻撃における各種トラフィックの累積分布 (2014 年 4 月 10 日-5)

ファイルのダウンロードが行われている．また，Javascript ファイルのダウンロード終了時刻においても大きく差があることがわかる．図 2，図 3 ではそれぞれ約 45 秒，15 秒程度と長めなのに対し図 4 の正常サイト閲覧時では約 1 秒程度で終了している．

以上，解析の結果から本研究では以下に述べる特徴量を用いる．

1. 攻撃コードダウンロードの特徴量
   DbD 攻撃通信において脆弱性をつくために利用されることが多い Adobe などの製品で使用されるファイルの種類である JAR，PDF，Flash ファイル，また Windows 上で実行される可能性がある EXE ファイル，それぞれのダウンロード長．

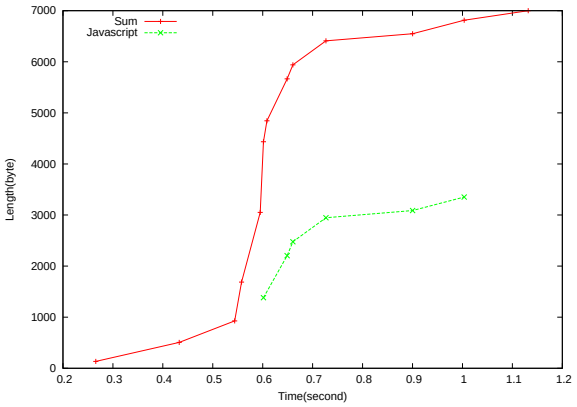

図 4: 正常通信における各種トラフィックの累積分布 (baidu.com)

2. リダイレクトの特徴量
   iframe によるリダイレクト，Redirection の 301，302 によるリダイレクト，それぞれの実行回数．Javascript については，リダイレクト以外の処理も行われる可能性があるためリダイレクトの特徴量としては用いない．またリダイレクトに関連する特徴量としてユニークホスト数を計測する．

3. 難読化処理の特徴量
   unescape 関数を用いた処理が行われているかの有無．

4. その他の特徴量
   Javascript ファイルのダウンロード byte 数，ダウンロードファイルの合計 byte 数，PDF ファイルのダウンロード開始時刻，Javascript ファイルのダウンロード終了時刻．

3.2 本研究におけるアイデア

DbD 攻撃通信は正常サイト閲覧時の通信と違い，マルウェアをダウンロードするために脆弱性を実行させる攻撃コードがダウンロードされるのが一般的である．また，入口サイトから攻撃サイトへの誘導のため iframe や Javascript，HTTP リダイレクトなども用いられている．また Javascript が難読化に用いられることも多い．

本研究では以上の特徴量について DbD 攻撃通信，正常サイト閲覧通信のそれぞれから抽出を行う．DbD 攻撃通信の可視化は，どの特徴量

を注目すればよいかを示し，判別を支援するシステムである．

3.3 可視化システム

DbD 攻撃における複数のホスト間の通信を鳥瞰し，特徴的な通信パターンを探索する補助ツールとして，トラフィック可視化システムを開発した．ダウンロードするコンテンツの種類や量ではなく通信先とその変化が直感的に観測できる様に，クライアントと複数のサーバの通信パケットを実際の通信時刻に応じて再現している．

可視化の対象は，D3M データセットにおける Pcap データの HTTP 通信である．クライアントを東京に位置させ，サーバは Pcap データの IP アドレスから Geo Location サービスを利用して国名を調べ，その間をパケットに見立てたカラーピクセルが飛び交う．一連のドライブされた HTTP 通信の関係が分かるように，パケットごとに次のように色分けをしている．通常の HTTP GET は緑，リダイレクトなどでサーバが変更したときの HTTP Response を赤，それ以外は対応する GET と Response が明示的になるように 20 色の色から選ぶ．赤いパケットの時に，実際のシェルコードやマルウェアがダウンロードされることが多い．

描画を Pcap データ内に記録された相対時刻に比例したタイミングで再現している．D3M の全観測データから，日時と何番目で識別されるセッションをマウス操作で選択して可視化させることができる．

Processing 2.2 を用いて実装している．入力データはセッションに切り出された Pcap データを用いる．

図 5 に本システムで描画中の 2011 年 2 月 16 日の DbD 攻撃の様子を示す．この日，用いられているサーバは世界各国に分散しており，それらからハニーポットとの間にいくつかの赤いパケットが流れており，頻繁なリダイレクトが実施されていることが観測できる．

現実装では，攻撃先がどこに分布して，どのようなタイミングで通信が行われるかは把握できるが，識別の為の特徴を抽出するまでには至っていない．類似のセッションを並べて再生するなど，他のセッションとの比較が容易になるような工夫が必要と考える．

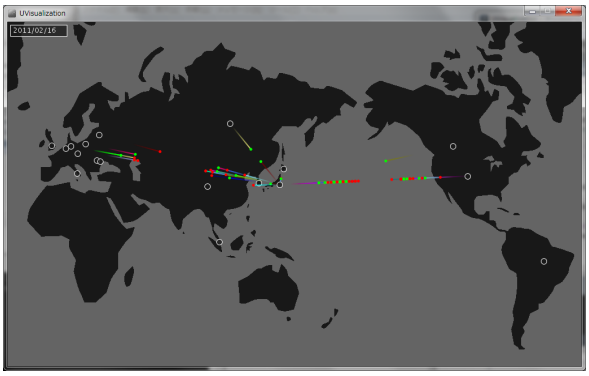

図 5: DbD 攻撃の可視化実行例

表 2: D3M 50 セッション

データセット	セッション数
D3M 2014	14
D3M 2013	29
D3M 2012	7

4 評価実験

4.1 概要

本実験では，Weka に入力するデータセットとして DbD 攻撃通信データと正常サイト閲覧通信データを合計 100 セッション分用意した．

DbD 攻撃通信データとして D3M の各年度から表 2 に示す通り合計 50 セッション分を用意した．DbD 攻撃通信データを判別するための特徴量として抽出したものは 3.1 で述べたとおりである．

それぞれのサイトから抽出した特徴量の一部を表 3 に示す．PDF や Javascript のダウンロードが発生していないセッションもあったため欠損値として “-1” を使用した．またこれら特徴量の統計値を表 4 に示す．それぞれの特徴量について合計，最大，最少，平均を与えている．

表 3: 抽出した特徴量

	Javascript byte	JAR byte	PDF byte	Flash byte	EXE byte	iframe times	301 times	302 times	unescape code	packet Sum	Host Sum	PDF DLstartTime	Javascript DLendTime	D3M
20120328-1	0	1314	1334	0	0	0	0	0	no	3553	1	20.109125	-1	yes
20120328-2	0	111	549	0	0	0	0	0	no	954	1	10.705616	-1	yes
20120328-3	2556	1334	1334	1334	0	1	0	3	no	41300	13	10.373214	45.817264	yes
20120328-4	0	0	0	0	0	0	0	1	no	384	1	-1	-1	yes
20120328-5	0	0	0	0	0	0	0	1	no	488	1	-1	-1	yes
google.com	0	0	0	0	0	0	0	2	no	1756	2	-1	-1	no
facebook.com	0	0	0	0	0	0	1	0	no	648	2	-1	-1	no
youtube.com	0	0	0	0	0	0	2	0	no	1061	2	-1	-1	no
yahoo.com	0	0	0	0	0	0	1	0	no	319	1	-1	-1	no
baidu.com	3352	0	0	0	0	0	0	0	no	7000	5	-1	1.003479	no

表 4: 特徴量の統計値

		Javascript byte	JAR byte	PDF byte	Flash byte	EXE byte	iframe times	301 times	302 times	unescape code	packet Sum	Host Sum	PDF DLstartTime	Javascript DLendTime	D3M
D3M	合計	56957	21946	20862	6427	18445	29	8	66	13	613097	185	314.022981	195.351827	50
	最大	15735	3918	1334	2730	4002	7	6	43	-	153222	49	42.822571	45.817264	-
	最少	0	0	0	0	0	0	0	0	-	54	1	0.135648	1.141391	-
	平均	1139.14	438.92	417.24	128.54	368.9	0.58	0.16	1.32	0.26	12261.94	3.7	14.27377186	19.5351827	-
Alexa	合計	386621	0	0	550	0	82	33	123	11	2549205	536	-	156.889139	0
	最大	86499	0	0	550	0	17	3	27	-	470521	55	-	22.618211	-
	最少	0	0	0	0	0	0	0	0	-	319	1	-	0.596231	-
	平均	7732.42	0	0	11	0	1.64	0.66	2.46	0.22	50984.1	10.72	-	5.603183536	-

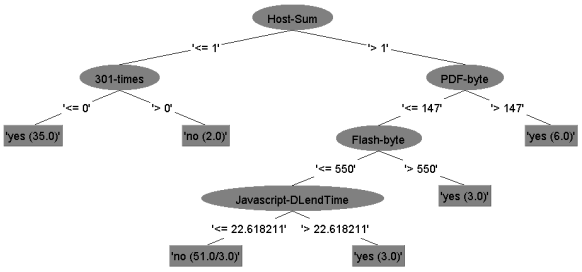

図 6: DbD 攻撃を識別する決定木

4.2 実験結果

用意した 100 件分のデータセットを Weka に入力し，出力された決定木を図 6 に示す．左から 3 つ目の葉の部分において no(51.0/3.0) と表現されているもの，は DbD 攻撃通信でないと判定されたものが 51 セッションあり，そのうち 3 セッションが誤りで，実際は DbD 攻撃通信であるという表現である．

出力された決定木による判別精度を表 5 に示す．

表 5: DbD 攻撃の判別精度

判別結果	DbD 攻撃	正常通信
DbD 攻撃	47	0
正常通信	3	50
計	50	50

4.3 考察

FalseNegative となったのは 3 セッションであり，FN は 3/50=0.06 である．これら誤検知が起こったセッションについて，特徴量を表 6 に示す．表内の Drive 誘導方法において “?” となっているものは，リダイレクト元のページにおいてアクセス先の URL となる記述部分を見つけることができなかったものである．これら 3 件の通信においては，リクエストのみでレスポンスがないパターン．Javascript ファイルのダウンロードのみで通信が終了しているパターン．このことから，この 3 件については通信をキャプチャした段階でパケットの欠損が起こってしまったパターンや，アクセスを行ったものの DbD 攻撃通信にまで至らなかったパターンではないかということが考えられる．入力に用いたその他の D3M データセットについても解析を行ったところ，特徴量として指定したファイルのダウンロードが行われていないパターンが 19 セッション，Javascript ファイルのダウンロードのみというパターンが 5 セッション，合計 24 セッションが実際には DbD 攻撃通信にま

表 6: FN セッション内容

データセット	DriveID	Drive 誘導方法	Response受信相対時刻（Second）	受信data（byte）	Dest IP	FQDN	Path	備考
20121002-2	1	–	0.362763	7190	37.221.xxx.207	strike.xxxxxxx.org	/crime/index.…	
	2-a	?	–	–	74.125.xx.95	ajax.xxxx.com	/ajax/libs/jqu…	No Res
	2-b	?	2.440111	690	37.221.xxx.207	strike.xxxxxxx.org	/crime/js/co…	
20121002-4	1	–	0.38767	3434	176.67.xxx.195	xxxxx.org	/od.php/main…	
	2	javascript	?	?	93.170.xxx.161	df54dgd.xxx.tm	/links/past-p…	No Res
	3	?	7.897855	130	93.170.xxx.161	df54dgd.xxx.tm	/links/past-p…	502
20140410-6	1	–	0.860308	30511	46.30.xxx.164	xxxxxxx.com	/	
	2-a	iframe	2.498957	1605	209.15.xx.134	xxxxx.com	/tets.html	404
	2-b	iframe	3.362999	294	69.43.xxx.167	xxxx.com	/?click=2595…	
	3-b	302 Found	4.918902	8018	50.56.xx.182	ww38.xxxx.com	/?click=2595…	
	4-b-a	script tag	9.605443	632	173.194.xx.114	www.xxxx.com	/adsense/do…	
	4-b-b	?	9.830686	135922	173.194.xx.114	www.xxxx.com	/ads/searc…	Js DL
	4-b-c	script tag	14.404316	5259	54.230.xxx.240	d1vbm0eveofcle.xxxxx.net	/scripts/js…	Js DL
	4-b-d	?	15.056104	170	50.56.xx.182	ww38.xxxx.com	/track.php…	
	4-b-e	script tag	15.129301	25372	54.230.xxx.240	d1vbm0eveofcle.xxxxx.net	/scripts/ti…	Js DL
	4-b-f	?	16.077878	7695	50.56.xx.182	ww38.xxxx.com	/scripts/…	

で至っていない可能性があると思われる．

リダイレクトに関しては，今回の判別結果は推測と大きく異なっていた．抽出した特徴量の 301，302，iframe のうち判別に使用されたのは 301 のみであった．さらにその 301 の判別においても回数が 0 のものを DbD 攻撃通信，1 以上のリダイレクトをしているものを正常と判別している．このパターンを使用した判別結果が 35 セッション，すなわち DbD 通信全体の 70%がリダイレクト用いていない．通常 DbD 攻撃通信では複数サイトを経由することが多いと言われているが，実際はそうでもない．この原因として，用いたデータセットの少なさや偏よりが想定できる．この点については入力するデータ量を増やすことにより，再度有効な特徴量かどうかの考察を行いたい．

PDF，Flash ファイルのバイト数で判断するセッションでは，DbD 攻撃通信でのみ使われることが多いからか誤検知は見られない，また Javascript ファイルのダウンロード終了時刻は判別に有益であった．表 3 にある値から考察すると，正常サイト閲覧時はアクセスしたサイトにおいてほとんどの Javasscript ファイルが初回にダウンロードされてしまうのに対し，DbD 攻撃通信の場合は中継サイトや攻撃サイトにおいて遅延して Javascript ファイルのダウンロードが発生する可能性があるかと思われる．しかしこの特徴量については，通信環境においてずれが発生することが考えられるため，同一環境下でのアクセスを行い，その時刻を記録し再度学習，判別を行うことでより信頼度の高い結果を得ることができると思われる．

D3M データセット同様，AlexaTop サイトそれぞれについて解析を行ったところ，24%のサイトが HTTPS の通信を行っていた．TLS の通信内容は復号ができないので特徴量に用いていない．このため，HTTPS の通信が行われた部分について今回使用した特徴量が含まれる可能性が考えられる．

5 おわりに

本研究では，Web サイトを閲覧する際の通信を可視化し，DbD 攻撃が行われる際の特徴的な通信に着目することにより DbD 攻撃の通信を検知することを試みた．DbD 攻撃が行われる際の特徴については多数の候補があり，その選定は非常に難しいものであるが，そのいくつかに着目し可視化することで，DbD 攻撃通信を判別できることを示した．

今後の改善点としては，入力のために用意したデータセットの少なさが根本的な問題として挙げられる．また正規サイトとしてキャプチャしたデータを解析した結果，大半が HTTPS による通信が行われていた．このため，単純な HTTP のみのフィルタリングによる特徴量抽出では判別精度の信頼が高くなりにくい点も問題といえる．今後は入力データセットそれぞれについてデータ量を増やし，より信頼度の高い

特徴量の選定，システムの構築をしていくことを目標としたい．

参考文献

[1] バラクーダラボ, “セキュリティの現場から from バラクーダラボ (158) AskMen.com、ドライブバイダウンロードでランサムウェアに感染”, 158, マイナビニュース, 2014/8/5 (http://news.mynavi.jp/ column/barracuda/158/, 2014/8/22 参照)

[2] マカフィー, “マカフィー、8 月のサイバー脅威の状況を発表”, マンスリーウィルスレポート, マカフィー株式会社 (http://www.mcafee.com/ japan/security/monthly/PC201308.asp, 2014/8/22 参照)

[3] 桑原, 安藤, 藤原, 菊池, 寺田, “パスシーケンスに基づく Drive-by-Download 攻撃の分類”, マルウェア対策研究人材育成ワークショップ 2010, 3F1

[4] 北野, 大谷, 宮本, “Drive-by-Download 攻撃における通信の定性的特徴とその遷移を捉えた検知方式””, Computer Security Symposium 2013, pp. 595-602, 2013.

[5] 笠間, 神薗, 井上, “Exploit Kit の特徴を用いた悪性 Web サイト検知手法の提案”, Computer Security Symposium 2013, pp. 603-610, 2013.

[6] 千葉, 森, 後藤, “Web サイト探索のための優先巡回順序の選定方法”, Computer Security Symposium 2012, pp. 805-812, 2012.

[7] 田中, 長尾, 森井, “DNS ログからの不正 Web サイト抽出についてー解析手法とその匿名化ー”, Computer Security Symposium 2013, pp. 132-138, 2013.

[8] 秋山, 神薗, 松木, 畑田, “マルウェア対策のための研究用データセット～MWS Datasets 2014～”, 情報処理学会 研究報告コンピュータセキュリティ（CSEC） Vol. 2014-CSEC-66, No. 19, pp. 1-7, 2014.

[9] M. Akiyama, et al., “Design and Implementation of High Interaction Client Honeypot for Drive-by-download Attacks, ” IEICE Trans., Vol.E93-B No.5 pp.1131-1139, 2010.

[10] Machine Learning Group at the University of Waikato, “Data Mining with Open Source Machine Learning Software in Java” (http://www.cs.waikato.ac.nz /ml/weka/downloading.html, 2014/8/22 参照)

[11] Alexa, “Alexa Top 500 Global Sites” (http://www.alexa.com/topsites, 2014/8/22 参照)