4Z-1 データマイニング技術を活用したサイバー攻撃検出法の検討

小池　愛理†　　宮保　憲治†
東京電機大学大学院　情報環境学研究科†

１．はじめに

情報通信技術の目覚ましい発展によりインターネットが普及し，現在では社会基盤の一部として定着している．利便性が向上した一方で，サイバー攻撃と呼ばれる，悪意あるユーザからの通信機器に対するネットワーク攻撃の脅威が増えつつある．特に，マルウェアに代表される,悪意あるソフトウェアによるユーザの被害が深刻化している．

近年ではマルウェア感染経路の多様化が進み，クライアントの WEB アクセスを契機として発生する「Drive by Download 攻撃」が増加する傾向[1]にある．Drive by Download 攻撃の対策[2]としては,悪性 WEB サイト URL をブラックリストとして定義し，フィルタリング操作により攻撃を回避する対策が取られている．しかしながら，WEB サイト数は年々増加すると共に，攻撃者も短期間で当該 URL を変更する対抗策を採る場合が多く発生しているため，ブラックリストには依存しない新たな技術が必要とされている．

本研究では，Drive by Download 攻撃に利用される悪性WEBサイトにおけるHTMLファイルの特徴を用いた,マルウェア配布に関わる危険な WEB ページの判別方法を提案する．

２．Drive by Download 攻撃

2.1 Drive by Download 攻撃の概要

Drive by Download 攻撃は，ユーザの気づかない内に不正な WEB サイトへ誘導し，マルウェアに感染させるための攻撃手法である．Fig.1 に基本的な攻撃フローを示す．

ユーザが，HTML タグや難読化 JavaScript による,不正な誘導コードが埋め込まれた入口サイトに,偶然にアクセスすることにより，異なる WEB サイト（中継サイト）へリダイレクトされる事象が発生する．次にユーザは攻撃者の WEB サイトへ誘導される．ユーザコンピュータの OS やブラウザ,プラグインなどの脆弱性を狙った不正コードによる攻撃を受け,ユーザ端末に強制的にマルウェアがダウンロードされ，感染に至る．

アクセス先の WEB サイトが悪意のある記述を含んでいるか否かは，一見して判別出来る場合は少なく，また，①攻撃は複数の WEB サイトを経由する複雑な構成である場合が多いこと，②複数の脆弱性を組み合わせて利用するタイプの攻撃手法が多いこと,等の状況が,攻撃回避策を困難にさせる要因となっている．

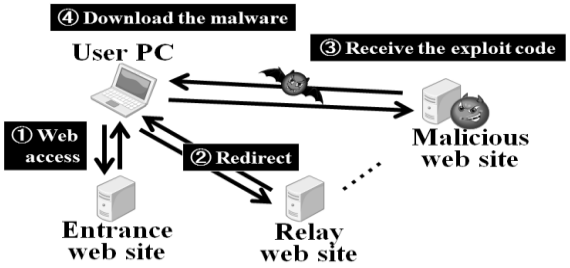

Fig. 1 Flow of Drive by Download attack

2.2 関連研究

攻撃に利用されるWEBサイトに着目し，Exploitコードの特徴（JavaScriptやJava Appletコードの有無),リダイレクトの特徴,攻撃の隠蔽に関する3つのカテゴリ内の特徴を利用し,機械学習による悪性WEBサイトの検出手法が,従来より検討されてきた[3].

３．機械学習による WEB ページ性質の分類手法

以下に,機械学習を用いて WEB ページの性質(悪性/良性)を分類する手法について述べる．

3.1 分類に用いるデータ

悪性 WEB ページのデータは，Drive by Download 攻撃時の一連の通信データを収録した D3M(Drive-by Download Data by Marionette)Dataset[4]から得られた 1165 件の HTML ファイルを利用した．また，比較対象とした良性の WEB ページのデータは，Alexa[5] が提供する正規 WEB サイト閲覧数ランキングの URL リストを基に WEB クローリングを行い，3610 件の HTML ファイルを収集して利用した．

3.2 分類に用いる特徴量

悪意ある WEB サイトの特徴を従来手法[3]に適用し,抽出した特徴量を用いて分類を行った(Table1)．

Table 1. Feature value to be used

Feature value	
1	Number of lines
2	Number of characters
3	Number of spaces
4	Number of <iframe>tags
5	Minimum value of the width attribute
6	Minimum value of the height attribute
7	Number of script tags
8	Number of characters
9	Number of the alphabet
10	Number of digits
11	Number of symbols (<>{}/_¥-!?%...)
12	Maximum value of the argument
13	Ratio of <8> to alphabet
14	Ratio of <8> to digits
15	Ratio of <8> to symbols
16	Ratio of <8> to Maximum value of the argument

Study of the cyber attack detection method by making use of the data mining technology
†Airi Koike and Noriharu Miyaho, Graduate School of Information Environment Technology, Tokyo Denki University

3.3 分類手法

従来手法で使用されている決定木学習法（データマイニングツール Weka[6]の J48 アルゴリズム）を利用し，10 分割交差検定による分類精度を評価した．また，特徴量を比較対象として提案手法の有効性を検証した．

４．分類実験の結果と考察

従来手法と提案手法を用いた WEB ページの性質の分類精度を ROC(Receiver Operating Characteristics: 受信者動作特性)曲線として Fig.2 に示す．

Fig.2 は，学習した分類器が様々なデータの割合に対応可能かどうか，データ件数を変化させ，誤検知率(FP(False Positive)Rate:良性を悪性と誤分類した割合）と検知率（TP(True Positive)Rate:悪性を正しく分類した割合）をプロットした曲線である．適切なサンプル抽出を行い，TP Rate を 0.9 から 1.0 まで変化させた時の FP Rate の値を比較することにより，分類手法の優劣を評価できる．曲線の右下の面積(ROC Area)は分類器の評価値として活用できる．実線で示された提案手法は，従来手法と比べてより左上にシフトした曲線を描き，総合的に判断すると分類性能が優れていることが分かる．この理由は，一般に TP/(FP+TP) 値は，判別結果が悪性であった時に，正しく悪性であったことを判別できる確率に等しいからである．Table2 に，TP Rate と TN(True Negative) Rate(良性を正しく分類した割合）の結果をまとめた．アンチウイルスソフトの誤検知により正規の WEB サイトへのアクセスが遮断される事例が問題視されており，正確に事象を捉え TN Rate の向上を目指す必要がある．提案手法は従来手法と比較して，TN Rate が約 3%向上することが判明し，その有効性が検証できた．従来手法では，主に特定の HTML タグやスクリプト関数，スクリプトの出現数等を特徴量として抽出しているが，これは正規の WEB サイトにおいても多用されている．提案手法において TN Rate が向上した要因としては，スクリプト内で利用される記号や数値の出現頻度・比率などを特徴として利用することにより，不正用途に用いられるスクリプトと正規用途に用いられるスクリプトを，より正確に判別できたとためと考えられる．

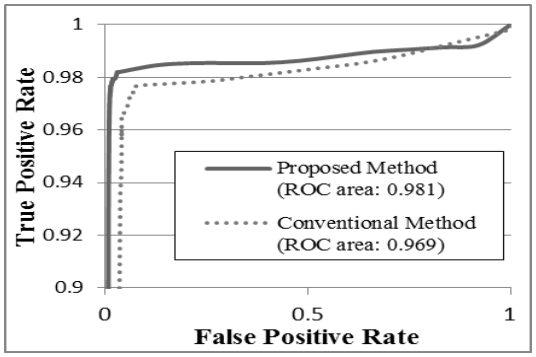

Fig.2 Comparison of the ROC curves obtained by changing the characteristic amount

Table 2. Accuracy of classification by decision tree

	TP Rate	TN Rate
Proposed Method	97.2 %	**98.7 %**
Conventional Method	96.7 %	95.8 %

提案手法において活用した分類処理の過程で，42 の分岐点を持つ決定木が生成された．

この決定木の一部を Fig.3 示す．最上位からスクリプトの出現数，スクリプト内の数値の出現頻度，HTML ファイルの行数，HTML ファイルのスペースやタブの出現数を判断要素とするノードが配置され，これらが本提案手法における分類に効果的な影響を与えた特徴的な要素と考えられる．

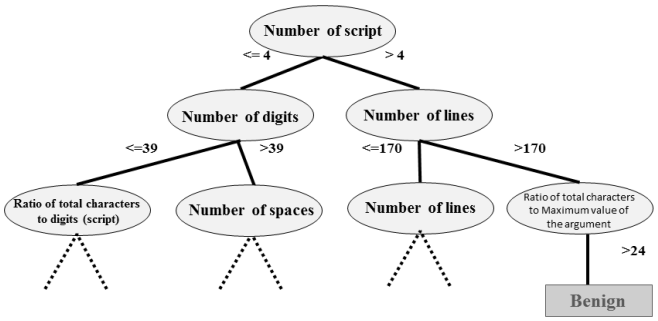

Fig.3. Decision tree for the classification of WEB page

５．まとめ

本稿では，Drive by Download 攻撃に利用される悪性 WEB サイトの HTML ファイルの特徴を用いた，マルウェア配布に関わる危険な WEB ページを検出する方法について提案した．また，機械学習を用いた分類実験により，従来手法と比較して提案手法では，より精度の高い分類が可能であることが判明した．

提案した分類手法では，HTML ファイルの特徴のみに着目したが，今後は，パケットデータ（特に HTTP レスポンスヘッダー情報等）を含め，複数の特徴量を，効果的に組み合わせた手順で，悪性 WEB ページの検出を行う手法について検討を進める予定である．

参考文献

[1] IBM, 2013 年上半期 TokyoSOC 情報分析レポート, http://www-935.ibm.com/services/jp/its/pdf/tokyo_soc_report2013_h1.pdf
[2] 笠間 貴弘, 他 “ドライブ・バイ・ダウンロード攻撃対策フレームワークの提案”, Computer Security Symposium 2011, 2011年
[3] Christian Seifert et al. “Identification of Malicious Web Pages with Static Heuristics”, ATNAC 2008, 2008.
[4] 神薗 雅紀, 他 “マルウェア対策のための研究用データセット～MWS Datasets 2013～”, マルウェア対策研究人材育成ワークショップ 2013 (MWS 2013), 2013 年
[5] Alexa, http://www.alexa.com/ 2014.1.12
[6] Weka 3.7.10,2014.1.12 http://www.cs.waikato.ac.nz/ml/weka/