文書ファイルの内部構造を利用したマルウェア検知手法

古川 菜摘[1,a)]　今泉 貴史[2,b)]

概要：特定の組織の情報を不正に入手することを目的とした標的型攻撃が大きな問題となっている．標的型攻撃に用いられる電子文書型マルウェアの中には，exploit と呼ばれる脆弱性を攻撃するコードを用いるものがある．このマルウェアは受信者が簡単に区別することができないため，システム側で自動的に検知・駆除できることが望ましい．マルウェア検知の手法として，実際にマルウェアを動作させる動的な検知手法もあるが，この方法ではマルウェアの起動条件を満たさない場合に見逃しが発生する．静的な検知手法として，文書ファイルの内部構造に不整合が生じることに着目した手法がある．この手法は高速に検査できるものの，構造的に正しいマルウェアは検知できない．本論文では，文書ファイルの内部構造を利用しながら，さらにファイルのエントロピーに注目することでマルウェアの検知を行う．実行ファイルと文書ファイルでは，エントロピーが異なる．単にファイル全体のエントロピーを計算するだけでなく，文書ファイルの構造に着目することで，実行ファイルが含まれる可能性のある部分を限定して計算することが可能となり，より精度の高い検知が行えると期待できる．

キーワード：標的型攻撃，検知，マルウェア，静的解析

Malware detection method using document file structures

Natsumi Furukawa[1,a)]　Takashi Imaizumi[2,b)]

Abstract: Targeted attacks aimed at obtaining information of a specific organization have become a major problem. Among malicious documents used for targeted attacks, there is one using code that attacks a vulnerability called exploit. Since it is difficult for recipients to notice this malware, it is desirable that the system can automatically detect and remove it. In this paper, we detect malware by paying attention to the file entropy while using the internal structure of the document file. Entropy differs between executable and document files. Not only by calculating the entropy of the whole file, but also focusing on the structure of the document file, it is possible to calculate with limited parts that may contain executable files, and more accurate detection can be performed.

Keywords: Targeted attack, detection, malware, static analysis

1. はじめに

企業を狙った標的型攻撃が大きな問題となっている．情報処理推進機構が 2019 年に発表した情報セキュリティ 10 大脅威では，標的型攻撃が組織編で第 1 位となっている [1]．標的型攻撃の代表的な手口としては，メールに不正プログラムを含むファイルを添付することが挙げられる．メールや添付ファイルの内容は，業務で使われるものに似せてあるため，受信者が標的型攻撃と気づくことは難しい．メールに添付される不正ファイルの種類としては，大きく分けて文書ファイル（Office 文書，PDF など）に似せてアイコンや拡張子を偽装した不正な実行ファイルと，文書ファイルの編集ソフトやビューワ自体の脆弱性を悪用したものがある．特に後者の割合が高く，2012 年の調査によると，検

[1] 千葉大学大学院融合理工学府
Graduate School of Science and Engineering, Chiba University
[2] 千葉大学統合情報センター
Institute of Management and Information Technologies, Chiba University
[a)] Furukawa723@chiba-u．jp
[b)] imaizumi_takashi@faculty．chiba-u．jp

知された不正侵入のうち，約 7 割が文書ファイルの脆弱性を利用したものだった [2]．標的型攻撃に用いられるマルウェアは，既知のマルウェアではなく，新しく作られたものが使われることが多いため，ウイルス対策ソフトのシグネチャマッチングによる検知が難しいという特徴がある．また，文書ファイルの編集ソフトやビューワの脆弱性を利用した文書型マルウェアの場合，正常なファイルとの外見上の差がないため，人の目によって見分けるのは困難である．本論文では，PDF ビューワの脆弱性を利用する不正なプログラムが埋め込まれた PDF ファイルを，内部構造とエントロピーを用いることで静的検知することを目的とする．

2. 関連研究

2.1 エントロピーに着目したもの

文献 [3] では，マルウェアを先頭から 256byte のブロックで処理し，平均エントロピーと最高エントロピーブロック値を用いることにより，パッキングや暗号化されているかを検知している．文献 [4] では，文書型マルウェアには識別可能な高エントロピー部分があると指摘している．文献 [5][6] では，悪意のあるドキュメントには誤った情報とパディングが含まれている可能性があり，エントロピーの値が低くなっていると想定している．文献 [7][8] では，文書型マルウェア内に埋め込まれているシェルコードの位置を特定する際に，ブロックごとに区切ったエントロピーの値と，その前後の差を用いている．文献 [9] では，PDF ファイルのエントロピーや構造的特徴から決定木を作成し，検知を行っている．

2.2 文章の構造に着目したもの

文献 [10][11] では，構造やメタデータから特徴量を抽出し，検知を行っている．文献 [12][13][14] では，文書型マルウェアの構造的特性が，正常なファイルと違いが出ることを利用して検知を行っている．一方，文献 [15] では，良性の PDF ファイルの構造を模倣するマルウェアを開発することにより，構造ベースの検知が破られる可能性があることを指摘している．文献 [16] では既存の PDF パーサによる検知を回避する手法を検討している．

3. 提案手法

本研究では，PDF ファイルの内部構造に基づいて悪性 PDF ファイルのエントロピーを算出することにより，悪性 PDF ファイルの検知が可能であるかを調査した．実験は全て仮想環境上で行った．実験環境を**表 1** に示す．実験に用いた検体は，良性 PDF ファイルと悪性 PDF ファイルの両方を，マルウェアの検体を配布しているサイトである contagio[17] で入手した．本論文では，良性と悪性の両方で，ランダムに 1800 ずつ検体を抽出して実験を行った．

表 1 実験環境

CPU(実機)	1.1 GHz Intel Core m3
メモリ (実機)	8GB
OS(実機)	MacOS Mojave 10．14．4
CPU(仮想環境)	0.9 GHz Intel Core m3
メモリ (仮想環境)	4GB
OS(仮想環境)	Linux version 4.18.5-041805-tsurugi

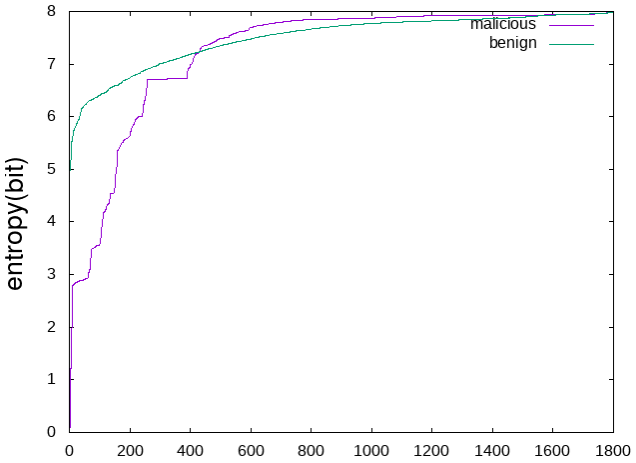

図 1 良性 PDF ファイルならびに悪性 PDF ファイルのエントロピー分布

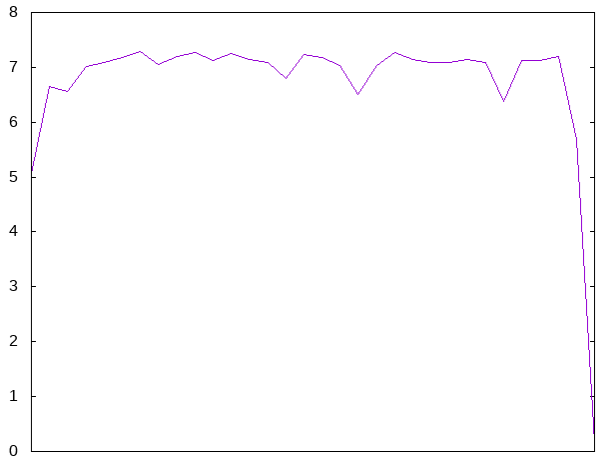

図 2 悪性 PDF1 ファイルのエントロピー分布

実験 1：PDF ファイルのエントロピーの変化の調査

図 1 に示されるように，ファイル全体でエントロピーを計算しても，良性 PDF ファイルと悪性 PDF ファイルの間に大きな差は見られない．そのため，文献 [3] の手法を参考に，ファイルの先頭から 256byte のブロックごとにエントロピーを計算した．良性 PDF ファイルと悪性 PDF ファイルそれぞれのエントロピーの変化を**図 2**，**図 3** に示す． 結果から，ブロック毎にエントロピーを計算することにより，良性 PDF ファイルと悪性 PDF ファイルのエントロピーの変化に差が出ることが示された．

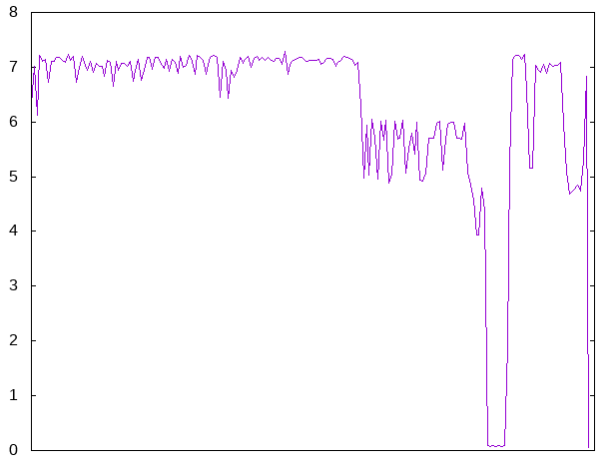

図 3　良性 PDF1 ファイルのエントロピー分布

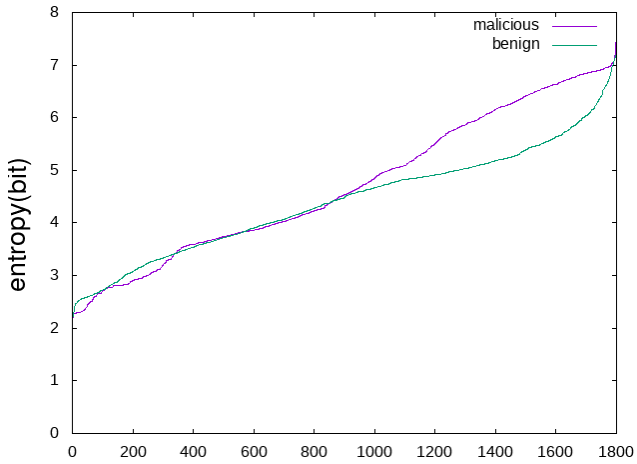

図 4　先頭から 256byte ずつ分割した場合

実験 2：エントロピーの差の最大値算出における，ストリームの考慮の検討

実験 1 の結果から，PDF ファイル内での連続した二つのブロックのエントロピーの差の最大値を求め，良性 PDF ファイルと悪性 PDF ファイルで違いが現れるか比較した．**図 4** に結果を示す．良性 PDF ファイルと悪性 PDF ファイルにおいて大きな違いが存在しなかった理由として，PDF の内部構造の一つであるストリームの存在が考えられる．

PDF ファイルは，複数のオブジェクトと呼ばれる要素から成り立っている．その中の一つであるストリームには，画像などの大きなデータが格納されており，PDF ビューワはこのデータを直接バイトデータとして順に読み込んでいく．ストリームは普通は圧縮されているため，エントロピーを算出する際にストリームとストリーム以外の部分が混在していると，値に影響を及ぼす可能性がある．本論文では，**図 5** のようにストリームとストリーム以外の部分を分割し，ストリーム部分のみを用いる．また，ストリーム全体でエントロピーを計算した場合，実験 1 と同様に，良性と悪性で値の差が出ない可能性が高い．本研究では，ストリームを 256byte ごとに分割し，それぞれの区間でエントロピーを算出した．

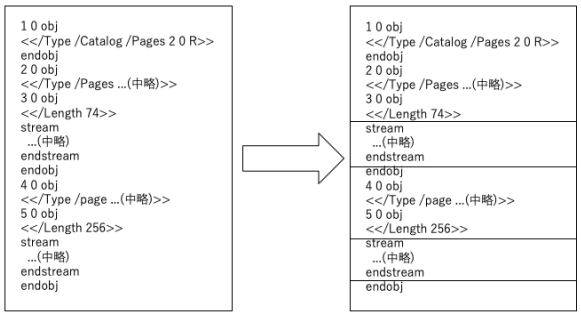

図 5　ストリームとストリーム以外の分割

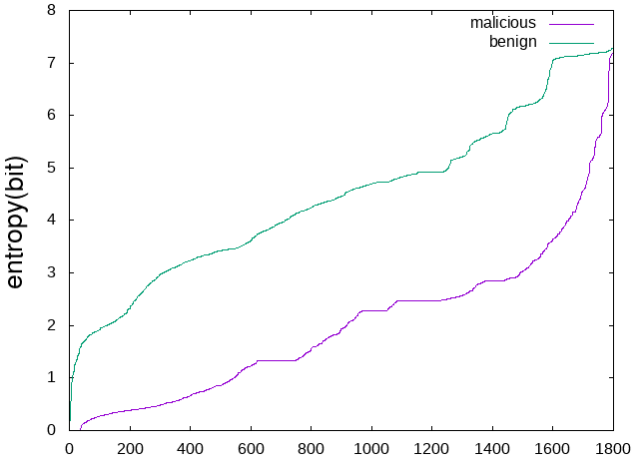

図 6　stream と stream 以外の部分に分割した場合

表 2　検知率

閾値	TPR	FPR
1.0	0.303	0.006
3.0	0.829	0.172
5.0	0.957	0.697
7.0	0.993	0.887

結果を**図 6** に示す．ストリームのみをエントロピーの抽出に用いた場合，エントロピーの差の最大値の分布が良性 PDF ファイルと悪性 PDF ファイルで異なっていることがわかる．

実験 3：検知率の算出

実験 2 の結果から，良性 PDF ファイルと悪性 PDF ファイルの判定を，ストリーム内の連続したブロックのエントロピーの差の最大値で行い，TPR と FPR を求めた．閾値よりもエントロピーの差の最大値が大きい場合に良性とみなす．閾値を 1.0,3.0,5.0,7.0 とした場合の結果を**表 2** に示す．

4. 考察

4.1 エントロピーを算出するブロック幅の検討

本研究では，エントロピーを算出するブロック幅として，関連研究で用いられた 256byte を採用したが，最適なブロック幅に関わる検討を行っていない．ブロック幅を再検討することによって，精度がどう変化するかを検討する必要がある．

4.2 ストリームの圧縮

本論文では，エントロピーを抽出するためにストリームを用いたが，ストリームの圧縮による影響を考慮していない．ストリームの圧縮を解除して計算した場合にどのようになるかを検討する必要がある．

5. おわりに

本研究では，PDF ファイルの構成要素の一つである stream に着目し，ストリーム内部の連続した区間のエントロピーの差の絶対値が良性 PDF ファイルと悪性 PDF ファイルで異なることを利用して，良性 PDF ファイルと悪性 PDF ファイルの分類が行えるかの考察を行った．本研究の手法の特徴として，

- pdf パーサなどの特定のツールに依存しない
- 複雑な構文解析を必要としない
- 実際にファイルを開かないため，端末や外部への影響がない

ことが挙げられる．しかし，検知率を上げるために閾値を上げると誤検知が非常に多くなるという問題があり，実用化に向けては精度を向上させる必要があると考える．今後は，内部構造を詳しく見ることで精度を向上させることが必要と考える．

参考文献

[1] 情報処理推進機構: 情報セキュリティ 10 大脅威 2019，情報処理推進機構（オンライン），入手先 ⟨https://www.ipa.go.jp/files/000072668.pdf⟩（参照 2019-08-21）.

[2] 本宮学：文書ファイルの脆弱性を突いた標的型攻撃に注意 ―― トレンドマイクロが警告，ITmedia（オンライン），入手先 ⟨https://www.itmedia.co.jp/enterprise/articles/1201/27/news019.html⟩（参照 2019-08-21）.

[3] Lyda, R. and Hamrock, J.: Using entropy analysis to find encrypted and packed malware, *IEEE Security & Privacy*, Vol. 5, No. 2, pp. 40–45 (2007).

[4] Li, W.-J., Stolfo, S., Stavrou, A., Androulaki, E. and Keromytis, A. D.: A study of malcode-bearing documents, *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, Springer, pp. 231–250 (2007).

[5] Pareek, H., Eswari, P., Babu, N. S. C. and Bangalore, C.: Entropy and n-gram analysis of malicious PDF documents, *International Journal of Engineering*, Vol. 2, No. 2 (2013).

[6] Dabral, S., Agarwal, A., Mahajan, M. and Kumar, S.: Malicious PDF Files Detection Using Structural and Javascript Based Features, (online), DOI: 10.1007/978-981-10-6544-6_14 (2017).

[7] 岩本一樹，神薗雅紀，津田侑，遠峰隆史，井上大介，中尾康二：電子文書型マルウェアからシェルコードを抽出する方法の提案，No. 13 (2014).

[8] Iwamoto, K. and Wasaki, K.: A Method for Shellcode Extractionfrom Malicious Document Files Using Entropy and Emulation, *International Journal of Engineering and Technology*, Vol. 8, No. 2, p. 101 (2016).

[9] V Nath, H.: Ensemble Learning for Detection of Malicious Content Embedded in PDF Documents (2015).

[10] M, I., S, O. and T, N.: A Study of Malicious PDF Detection Technique, *2016 10th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS)*, pp. 197–203 (online), DOI: 10.1109/CISIS.2016.45 (2016).

[11] Smutz, C. and Stavrou, A.: Malicious PDF detection using metadata and structural features, *Proceedings of the 28th annual computer security applications conference*, ACM, pp. 239–248 (2012).

[12] Šrndic, N. and Laskov, P.: Detection of malicious pdf files based on hierarchical document structure, *Proceedings of the 20th Annual Network & Distributed System Security Symposium*, Citeseer, pp. 1–16 (2013).

[13] 大坪雄平，三村守，田中英彦：悪性文書ファイル検知のためのファイル構造検査の長期有効性，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, pp. 955–962 (2015).

[14] ドゥアンパチャンカンボリスット，今泉貴史：L-005 構成要素の関係性を利用した悪性 PDF ファイルの検知 (L 分野:ネットワーク・セキュリティ, 一般論文)，情報科学技術フォーラム講演論文集，Vol. 14, No. 4, pp. 171–175 (2015).

[15] Maiorca, D., Corona, I. and Giacinto, G.: Looking at the bag is not enough to find the bomb: an evasion of structural methods for malicious pdf files detection, *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*, ACM, pp. 119–130 (2013).

[16] Carmony, C., Hu, X., Yin, H., Bhaskar, A. V. and Zhang, M.: Extract Me If You Can: Abusing PDF Parsers in Malware Detectors., *NDSS* (2016).

[17] Mila: contagio, (online), available from ⟨http://contagiodump.blogspot.com⟩ (accessed 2019-08-22).