Vol.2019-MPS-122 No.17
2019/3/1

USB セキュリティに関するリスク推定に関する考察

西山魁人[†1]　鈴木海斗[†1]　田中雅浩[†1]　村田雄一朗[†1]　松田健[†1]　園田道夫[†2]

概要：データのやり取りや機器の接続時に，PC やマイコン，IoT 製品の USB ポートを利用する機会は多くのユーザーにとって少なからず存在するものと考えられる．USB セキュリティに関する情報は組織における研修やメディアなどを通じて共有されるようになりつつあるものの，身近にある USB 製品が安全なものであるかどうか検査する方法に関する従来研究は存在するが，未だ浸透しているとは言えないのが実情である．本稿では，USB ポートに接続された USB 機器のバイナリデータを解析することで有害なデータを含む USB を検知する手法について考察を行う．

キーワード：USB，セキュリティ，検知

Consideration on Risk Estimation for USB Security

KAITO NISHIYAMA[†1]　KAITO SUZUKI[†1]　MASAHIRO TANAKA[†1]
YUICHIRO MURATA[†1]　TAKESHI MATSUDA[†1]　MICHIO SONODA[†2]

Abstract: It may be said that there are many opportunities to use PCs, microcomputers, USB ports of IoT products when exchanging data and connecting equipment. A lot of information on USB security are shared through organizational training and media. In addition, there exist conventional studies on how to check whether USB products are safe. However, many pepoples do not have software or devices that can check the safety of USB. This paper considers a method to detect USB including malicious data by analyzing binary data of USB device connected to USB port.

Keywords: USB, Security, Detection

1. はじめに

USB の利用場面は，日常の PC 操作やデータ移行の他，IoT 製品へのデバイスの接続や車の USB ポートなど，様々なものを想定することができる．USB メモリや USB 関連製品を利用する際のセキュリティ的なリスクとしては，USB メモリからのマルウェア感染や Bad USB などが挙げられる．USB メモリにマルウェアが含まれているかどうかアンチウィルスソフトで検査することは可能ではあるものの，USB 製品を USB ポートに挿入した時点で，使用している PC やデバイスにおけるマルウェア感染などのセキュリティの状態を把握することは困難である．従来研究として，[1]や[2]などが存在するが，新たな情報を簡易に学習しながら USB の危険度をチェックするソフトウェアやデバイスは末端のユーザーの身の回りにないのが実情である．

本研究では，USB メモリに含まれる有害な情報をチェックするための特徴の一部を紹介し，実際の USB メモリを用いてその有用性や可能性について検討した結果を報告する．

2. 関連研究

関連研究について簡単にまとめる．文献[1]では，USB メモリの操作ログを視覚化した情報を管理者に提供し，ユーザーにフィードバックを返すことを実現する方法を提案している．文献[2]では，USB デバイスの構成情報を検査して悪性 USB デバイスを検知・遮断する USB ハブを提案している．本研究は，USB メモリが持つ有害な情報やデータをダンプファイルに含まれるアスキー文字列を解析することで，有害な情報やデータを含む USB メモリ（以下，有害な情報を含む USB という）を検知する手法について検討する．

3. USB メモリデータの特徴

USB メモリには，メモリに含まれているファイルの情報の他にも，その USB メモリを製造した会社の情報など多くの情報が含まれている．このようなデータを総合的に活用して USB メモリの危険度を評価することで，USB メモリを利用するリスクを低減させることができると考えられる．本研究では，USB メモリのバイナリ情報に含まれる一部の情報を用いることで，有害な情報を含む USB メモリを検知する一手法を提案する．図 1 のように，USB メモリのダンプファイルを解析すると，様々な文字列が含まれていることが確認できる．

本研究では，このような文字列の中から最も簡単なアスキー文字列のみに着目することで，有害な情報を含む USB メモリを検知する方法について検討する．

†1 長崎県立大学情報セキュリティ学科
†2 国立研究開発法人情報通信研究機構

図 1　ダンプファイルの例
Figure 1　Example of dump file.

図 1 は有害な情報を含む USB メモリのダンプファイルの一部である.データに含まれる 16 進数のデータも有用な情報であると考えらえるが，本研究では，ダンプファイルに含まれるアスキー文字列に着目する.

ダンプファイルに含まれるアスキー文字列の特徴として，@（アットマーク）を先頭とした文字列が存在することを確認できる．図 2 に図 1 の USB メモリのダンプファイルに含まれる@から始まるアスキー文字列の一部を示す.

図 2　ダンプファイルに含まれるアスキー文字列の一部
Figure 2　Part of the ASCII character string included in dump file.

一方，図 3 は未使用の USB メモリのダンプファイルの情報である.

図 3　未使用 USB のダンプファイルに含まれるアスキー文字列の一部
Figure 3　Part of ASCII character string included in unused USB dump file

図 2，3 を比較すると，有害な情報を含む USB メモリのダンプファイルに含まれるアスキー文字列の特徴として

@大文字のアルファベット文字列
@アルファベットや特殊記号からなる文字列

という形式のものが多く見られることがわかる.
したがって，本研究では，このような特徴を用いて，有害な情報を持つ USB メモリを検知できるかどうか簡単に調査した.

4.　検知実験と結果

図 2 の USB メモリとは異なる有害な情報を含む USB メモリと通常の USB メモリをそれぞれ 1 つずつ用意し，それらのダンプファイルを解析することで，前章で紹介した有害な情報を含む USB メモリの特徴が有効であるかどうか調べる.

特徴ベクトルの生成:
有害な情報を含むかどうかを検知するためにダンプファイルに含まれる@から始まる文字列の，@以降の 4~5 個の文字列をランダムに 200 個抽出して 200 次元ベクトルを生成する.
参考までに，有害な情報を含む USB から生成されるベクトルには,
|$HH　　VWAUAVAWH1$`H　　d$hE3
のような文字列が含まれ，正常な USB から生成されるベクトルには,
USBSy　　Z-d　　USBCz　　USBSz　　USBC{
のような文字列が含まれる.

学習データ:
有害な情報を含むUSBから生成したベクトルの個数をM個，正常な USB から生成したベクトルの個数を N 個として，以下のデータセットを学習データとして用意した.

learning data 1 : (M, N) = (7, 7)
learning data 2 : (M, N) = (14, 14)
learning data 3 : (M, N) = (88, 14)

テストデータ:
学習データを Microsoft の Azure に用意されている SVM で学習し，以下のテストデータで検知実験を行った．学習データを生成したUSBとは異なるUSBを用いて生成している.
test data 1 : (M, N) = (2, 1), learning data 1 で学習
test data 2 : (M, N) = (2, 4), learning data 2 で学習
test data 3 : (M, N) = (17, 3), learning data 3 で学習

検知実験結果:
test data 1：どちらも 100%検知
test data 2：有害 100%，正常 75%検知
test data 3：有害 100%，正常 0%検知　（つまり，全て有

害と検知）

learning data 2，3 のデータセットの配分と test data 2，3 の結果から，SVM で学習を効率良くするためには，正常 USB の特徴の学習がたくさん必要である可能性が考えられる．

5. 考察と今後の課題

本研究では，有害な情報を含む USB メモリのダンプファイルが持つ１つの特徴について紹介した．
なお，このような特徴は正常な USB メモリにも含まれるパターンも想定する必要があるため，今後はたくさんのデータ収集を実施しながら，有害な情報を含む USB メモリを検知する数理モデルの構築について検討し，有害な情報の特徴を自動的に学習しながら USB メモリの危険度をチェックするデバイスの開発を進めていくことが今後の課題である．

謝辞 本研究は，FAVVO 長崎のクラウドファンディングによる助成を受けて実施しております．
ご支援を頂いた方々に深謝致します．

参考文献

[1] 小崎 真寛,芝口 誠仁,中山 祐輝,岡田 謙一
“USB メモリを介したファイル移動の監視とそのログ視覚化“.
情報処理学会 グループウェアとネットワークサービス（GN）2010-GN-75(4), pp.1-8 (2010),(参照 2019-01-30).
[2] 竹久 達也，岩村 誠，丑丸 逸人，井上 大介
“悪性 USB デバイスに対する検査機能付き USB ハブの提案,
電子情報通信学会技術研究報告 = IEICE technical report : 信学技報 114(489), pp.61-66 (2015), (参照 2019-01-30).