Computer Security Symposium 2016
11 - 13 October 2016

攻撃種別に着目した悪性文書ファイルの特徴に関する考察

大坪 雄平[1,3]　窪 優司[1]　三村 守[2,3]　田中 英彦[3]

概要：悪性文書ファイルは，標的型攻撃やドライブバイダウンロード（DBD）攻撃など，様々なサイバー攻撃に使用されている．悪性文書ファイルを閲覧すると，閲覧ソフトの脆弱性が攻撃され，マルウェア本体のプログラムに感染する．この本体が悪性文書ファイルに埋め込まれているか否かで，悪性文書ファイルの種別を dropper と downloader に分けることができる．我々の調査の結果，標的型攻撃で使われた悪性文書ファイルのほとんどは dropper であり，DBD 攻撃の場合は downloader であることが分かった．本論文では，その理由について，攻撃の成功率を高めるために行った攻撃者の行動という観点で考察を行う．

キーワード：悪性文書ファイル，標的型攻撃，ドライブバイダウンロード攻撃

Classifying Malicious Documents based on the Nature of Cyber-Attack

Yuhei Otsubo[1,3]　Yuji Kubo[1]　Mamoru Mimura[2,3]　Hidehiko Tanaka[3]

Abstract: Malicious documents are abused in various cyber attacks including targeted e-mail attacks and Drive-By-Download(DBD) attacks. Opening a malicious document results in the infection with the malicious executables in the document through the vulnerabilities in the document viewer. Whether or not this malicious executables are embedded in the document determines the kind of the malicious document to be the dropper or downloader. Our research shows that most malicious documents are the droppers in targeted e-mail attacks and are the downloaders in DBD attacks. This paper focuses on the reasons from the viewpoint of the attackers' actions to make the attacks more successful.

Keywords: malicious document, targeted attacks, drive by download attacks

1. はじめに

文書ファイル形式のマルウェアである悪性文書ファイルは，標的型攻撃やドライブバイダウンロード（DBD）攻撃など，様々なサイバー攻撃に使用されている．例えば，2014 年の標的型攻撃に使用されたマルウェアのうち約 6 割が文書ファイル形式である [1] など，悪性文書ファイルの脅威は無視できないものとなっている．

一方，攻撃者にとって，悪性文書ファイルは目的を達成するための手段である．目的を効率的に達成するための最適の手段として，攻撃者は悪性文書ファイルを選択しており，攻撃種別ごとに悪性文書ファイルの傾向が異なっていると考えられる．

攻撃者のとる戦略に関する研究としては，Nelms らの研究 [2] がある．Nelms らは，悪意のある不要なソフトウェアをダウンロードさせるためにユーザを誘い込む Web ベースのソーシャルエンジニアリング（SE）攻撃を分析し，悪意ある Web サイトにユーザを誘い込むための戦略や，さらに誘い込んだユーザに不要なソフトウェアをインストールさせるための戦略を体系化している．

本論文では，悪性文書ファイルを用いた代表的なサイバー攻撃として，標的型メール攻撃と DBD 攻撃を取り上げ，悪性文書ファイルの特徴を比較し，その違いの 1 つを明らかにする．さらに，その違いについて，攻撃の成功率を高めるためにとった攻撃者の行動という観点から考察を

[1] 警察庁
National Police Agency
[2] 海上自衛隊幹部学校
JMSDF Command and Staff College
[3] 情報セキュリティ大学院大学
Institute of information security

表 1　データセットの概要
Table 1　A summary of the datasets.

		tar (09–15)	D3M (10–15)	mal (con)	mal (VT)
RTF	rtf	158	–	–	69
CFB	doc	76	–	–	61
	xls	66	–	–	9
	ppt	–	–	–	2
	jtd(c)	45	–	–	–
PDF	pdf	179	309	11,101	86
OOXML	ppsx	3	–	–	–
Total		529	309	11,101	227

行う．

以下，第 2 章では，本論文で取り扱う 4 種類のデータセットの概要を説明する．第 3 章では，データセットの悪性文書ファイルを閲覧した際に実行されるマルウェア本体の格納場所を調査する．第 4 章では，悪性文書を閲覧した際に開かれるマルウェア本体やダミー表示用の文書ファイルの格納場所で悪性文書ファイルを 6 種類に分類し，各悪性文書ファイルについて，攻撃者の意図どおりに動作するかという観点で分析を行う．第 5 章では，前章の分析結果を踏まえ，攻撃者にとってメリットがあるかという観点で，攻撃種別ごとに悪性文書ファイルの再評価を行う．第 6 章では，攻撃種別ごとの最適な悪性文書ファイルについて考察し，最後に第 7 章でまとめる．

2. データセット

本論文で使用するデータセットの概要を**表 1** に示す．表の左側の欄は，ファイル形式および拡張子を示している．データセットには，4 種類のファイル形式が含まれ，それぞれ，RTF（Rich Text : rtf 拡張子）[3]，CFB（Compound File Binary : doc，xls，ppt，jtd 拡張子など）[4] および PDF（Portable Document Format : pdf 拡張子）[5]，OOXML（Office Open XML ; docx，xlsx，pptx 拡張子など）となっている．

2.1 tar(09–15)

このデータセットは，2009 年から 2015 年までの間に日本の複数の組織に送付された標的型メールから採取した悪性文書ファイルである．特定の脆弱性の種類，検知名，RAT の種類等について，同一のものが多数含まれるといった検体の偏りが生じるのを防ぐため，検体の採取期間に標的型攻撃に用いられたメールとして提供を受けたもの全てから添付ファイルを取り出し，拡張子が文書ファイルのものを機械的に選定した．ただし，拡張子と実際の中身が一致していないものがあり，それらについては実際の中身に基づいて分類した．その上で同一ハッシュ値を持つものは取り除いた．

表 2　データセットの分類
Table 2　analysis sheet of the datasets.

	tar (09–15)	D3M (10–15)	mal (con)	mal (VT)
Dropper	519	0	137	51
Downloader	10	309	10,964	176
Total	529	309	11,101	227

2.2 D3M(10-15)

このデータセットは，MWS データセット [6] で提供される D3M データセットであり，主に DBD 攻撃を対象として収集されたものである．

2.3 mal(con)

このデータセットは，マルウェアダンプサイト contagio で研究用に公開された文書ファイルである [7]．その大部分は，標的型攻撃によらないものである．一部ファイルが破損していたため，ヘッダから文書ファイルとして認識できないものは除外している．

2.4 mal(VT)

このデータセットは，VirusTotal[8] において，2013 年から 2014 年の間に登録され，CVE 番号がタグ付けされたファイルのうち拡張子が rtf,doc,xls,ppt および pdf であるものという条件で検索し，検索結果から機械的に選定したものである．

3. マルウェア本体の格納場所の調査

文書ファイルそのものは，閲覧ソフトを介して文書を表示することを想定しており，文書ファイル単独で動作することはできない．そのため，悪性文書ファイルは，閲覧ソフトを介して，端末にマルウェア本体のプログラム（exe や dll）を実行させる．このマルウェア本体が，文書ファイルに含まれるか否かで，悪性文書ファイルの種類を dropper と downloader に定義する．

我々は，各データセットの悪性文書ファイルを分析し，dropper と downloader に分類した．**表 2** は，各データセットを分析した結果を示している．

3.1 標的型メール攻撃に使用された悪性文書ファイル

分析の結果，tar(09–15) の 98.1 %は dropper であり，標的型メール攻撃に使用された悪性文書ファイルのほとんどは，dropper であることが分かった．

典型的な dropper の構造および動作を**図 1** に示す．悪性文書ファイルを開くと，閲覧ソフトの脆弱性を攻撃する exploit と呼ばれる部分が動作し，shellcode（侵入した端末を制御できるようにするためのコード）が実行される．shellcode は文書ファイルに埋め込まれたマルウェア本体の

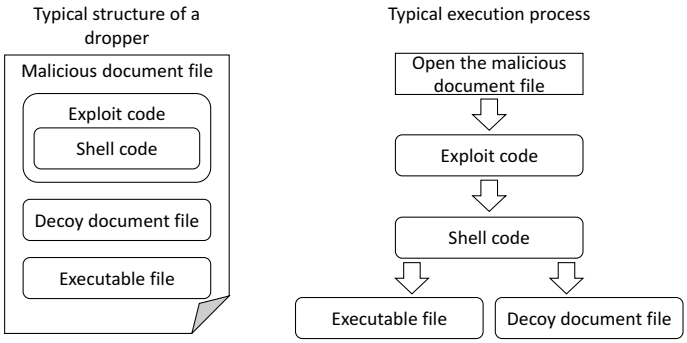

図 1　dropper の構造および動作
Fig. 1　Structure and execution process of a dropper.

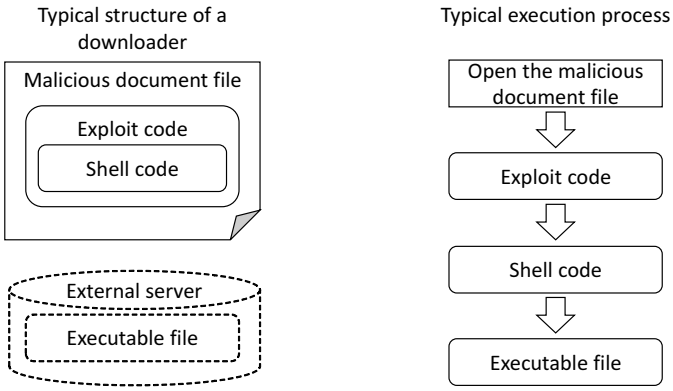

図 2　downloader の構造および動作
Fig. 2　Structure and execution process of a downloader.

プログラム（exe や dll）やダミー表示用の文書ファイルを取り出す．ダミー表示用の文書ファイルを表示するとともに，バックグラウンドで，マルウェア本体のプログラムを実行する．これによって悪性文書ファイルを閲覧した端末はマルウェアに感染する．

3.2　DBD 攻撃に使用された悪性文書ファイル

分析の結果，D3M(10–15) の 100 %が downloader であり，mal(con) の 98.8 %が downloader であった．従って，DBD 攻撃に使用された悪性文書ファイルのほとんどが downloader であることが分かった．

典型的な downloader の構造および動作を図 **2** に示す．悪性文書ファイルを開くと，dropper と同様に exploit が動作し，shellcode が実行される．shellcode は，攻撃者が用意した外部のサーバからマルウェア本体のプログラムをダウンロードし，そのプログラムをバックグラウンドで実行する．これにより，悪性文書ファイルを閲覧した端末はマルウェアに感染する．

4.　悪性文書ファイルの分類と特徴

悪性文書ファイルは，ダミー表示をするか否か，表示をする場合は，ダミー表示用の文書ファイルを自身から取り出すか否かの 3 種類に分類できる．したがって，マルウェア本体の格納場所の 2 種類と組み合わせると，悪性文書ファイルは 6 種類に分類できる．各悪性文書ファイルについて，攻撃者の意図どおりに動作するかという観点で分析した結果を表 **3** に示す．表の各欄の意味について以下に示す．

表 3　悪性文書ファイルの分類と特徴
Table 3　Chracteristics of malicious documents.

		Online		Offline		Shell	
Exe	Dec.	Inf.	Dec.	Inf.	Dec.	code	Target
Down	None	OK	–	NG	–	Small	Wide
	Down	OK	Slow	NG	NG	Small	Wide
	Drop	OK	Fast	NG	Fast	Big	Wide
Drop	None	OK	–	OK	–	Small	Narrow
	Down	OK	Slow	OK	NG	Big	Narrow
	Drop	OK	Fast	OK	Fast	Small	Narrow

4.1　Exe

マルウェア本体を外部のサーバからダウンロードするものを “Down”，自身から取り出すものを “Drop” とした．

4.2　Decoy(Dec.)

ダミー表示をしないものを “None”，ダミー表示をするもののうちダミー表示用の文書ファイルを外部のサーバからダウンロードするものを “Down”，自身から取り出すものを “Drop” とした．

4.3　Online / Offline

悪性文書ファイルの侵入経路として，Web，メール，USB 等様々なものが想定され，悪性文書ファイルを閲覧する際の端末の環境は，攻撃手法によっては，攻撃者が制御することが難しい場合がある．そこで，端末の環境として，端末が外部のネットワークにつながっているか否かで，“Online” と “Offline” に分け，それぞれの状況で，攻撃者の意図どおりに悪性文書ファイルが動作することが可能か否かを分析した．

4.3.1　Infection(Inf.)

マルウェア本体が攻撃者の意図どおり実行されるものを “OK”，実行されないものを “NG” とした．

4.3.2　Decoy(Dec.)

悪性文書ファイルの中からダミー表示用の文書ファイルを取り出す場合，既にメモリ上に展開されたデータをファイルに保存したり，端末上に保存された悪性文書ファイルから必要な部分を切り出すだけである．そのため，悪性文書ファイルを開いてからダミー表示用の文書ファイルが表示されるまでの時間は，通常の文書ファイルを表示する場合の時間と大差がない．

一方，外部のサーバからダミー表示用の文書ファイルを作成する場合，表示にかかる時間は，受信者のネットワー

ク環境に依存する．さらに，悪性文書ファイルを開く環境がオンラインである保証もないため，ダミー表示用の文書ファイルのダウンロードに失敗する可能性もある．

ダミー表示する機能がないものを “–”，ダミー表示に失敗してしまうものを “NG”，ダミー表示に成功するもののうち悪性文書ファイルを開いてからダミー表示されるまでの時間で “Fast” と “Slow” に分類した．

4.4 Shellcode

Shellcode は，使用する脆弱性によりサイズを制限されることが多い．言い換えると，shellcode のサイズが小さければ，攻撃者が攻撃に使用することができる脆弱性の種類が増えることになる．そのため，shellcode は，コードサイズを小さくするための様々な工夫が施されている．ダミー表示用の文書ファイルを作成する手法とマルウェア本体の実行ファイルを作成する手法に着目し，両手法を同一のものにすることで，共通で使えるコードを増やし，shellcode のサイズを小さくすることができるものを “Small” とした．また，ダミー表示をしないものも “Small” にした．それ以外を “Big” とした．

4.5 Target

攻撃対象の範囲．downloader は，感染端末の環境に合わせて柔軟に，ダウンロードするマルウェア本体を変更することができることから “Wide” に分類した．dropper は，感染端末の環境に合わせてマルウェア本体を変更することが困難であることから，“Narrow” とした．

5. 悪性文書ファイルの評価

本章では，各攻撃で使用される悪性文書ファイルについて，何故表 2 のような特徴を持つことになるのか，表 3 を基準に，攻撃種別ごとに攻撃者にとってのメリットという観点で再評価を行う．

5.1 標的型メール攻撃

標的型メール攻撃は，特定の個人や組織を対象にした攻撃であり，攻撃対象が興味を引くようにメールの件名や本文を調整することで，添付されたマルウェアを感染させる．マルウェアの多くは，端末の遠隔操作を目的とした RAT と呼ばれるものである．攻撃者は，RAT を使用することで，攻撃対象の保有する情報を窃取したりする．

表 3 を基準に，標的型メール攻撃に使用される悪性文書ファイルについて，攻撃の成功率を高めるものを “+1”，攻撃に気づかれる確率を上げるものを “-1”，どちらでもないものを “0” として評価を行った．評価の結果を**表 4** に示す．

各項目ごとの評価基準について以下に示す．

表 4 標的型メール攻撃で使用される悪性文書ファイルの評価
Table 4 Evaluation (1) of malicious documents used in targeted email attacks.

		Online		Offline		Shell	
Exe	Dec.	Inf.	Dec.	Inf.	Dec.	code	Target
Down	None	+1	-1	0	-1	+1	0
	Down	+1	-1	0	-1	+1	0
	Drop	+1	0	0	0	0	0
Drop	None	+1	-1	+1	-1	+1	0
	Down	+1	-1	+1	-1	0	0
	Drop	+1	0	+1	0	+1	0

5.1.1 Infection(Inf.)

マルウェア本体の実行に成功（OK）のものを “+1” とした．また，3.1 で述べたとおり，マルウェア本体の実行はダミー表示のバックグラウンドで処理されている．マルウェア本体の実行という処理は被害者が意識をしているものではないことから，その処理に失敗したとしても，被害者が攻撃に気づくことには繋がらない．したがって，マルウェア本体の事項に失敗（NG）のものは “0” とした．

5.1.2 Decoy(Dec.)

この攻撃の初期段階であるマルウェアへの感染には，添付ファイルを開くという受信者の操作が必須である．受信者は，添付ファイルがメールの本文や件名に関連した内容が表示されることを期待して，悪性文書ファイルを開く．悪性文書ファイルを開いた際に，何も表示しなかったり，閲覧ソフトの動作が停止したりする動作は，受信者の期待を裏切る動作である．そのような動作があった場合，受信者がメールを不審に感じ，攻撃に気付く可能性が高くなる．マルウェアへの感染という攻撃者の初期の目的を達成できたとしても，短い時間で受信者が感染に気付いてしまうため，情報窃取という攻撃者の最終目的が達成できなくなってしまう．そのため，標的型メール攻撃に使用される悪性文書ファイルを開くと，ダミー表示用の文書ファイルが表示されるものを “+1”，表示されないものを “-1” とした．

5.1.3 Shellcode

Shellcode を小さくすることで，攻撃することのできる脆弱性の種類が増えたり，shellcode 内に実装できる検知回避技術の種類が増えることから，シェルコードのサイズが小さくなるものを “+1” と評価した．

5.1.4 Target

攻撃対象を広く取れることは，一般的に考えるとメリットである．しかしながら，標的型攻撃は，攻撃対象を絞っているため，攻撃の成功率に対し，この項目が大きく貢献することはないと考えられる．したがって，すべて “0” とした．

5.2 DBD 攻撃

DBD 攻撃とは，主に Web ブラウザを介して，閲覧者に

表 5　DBD 攻撃で使用される悪性文書ファイルの評価
Table 5　Evaluation (2) of malicious documents used in DBD attacks.

		Online		Offline		Shell	
Exe	Dec.	Inf.	Dec.	Inf.	Dec.	code	Target
	None	+1	0	–	–	+1	+1
Down	Down	+1	-1	–	–	+1	+1
	Drop	+1	-1	–	–	0	+1
	None	+1	0	–	–	+1	0
Drop	Down	+1	-1	–	–	0	0
	Drop	+1	-1	–	–	+1	0

気づかれずにマルウェアに感染させる攻撃である．マルウェア感染までの流れを以下に示す．攻撃者は，Web サイトを改ざんする．Web サイトは様々なコンテンツの組み合わせで構成されている．ある 1 つの url のページを指定すると，Web ブラウザはそのページに関連する様々な関連するコンテンツをダウンロードする．攻撃者は，Web サイトを改ざんする際に，この関連するコンテンツとして悪性文書ファイルを追加する．閲覧者が改ざんされた Web サイトを表示しようとすると，Web ブラウザは，正規のコンテンツの表示と並行して，バックグラウンドで悪性文書ファイルをダウンロードして表示をしようとする．これにより，改ざんされた Web サイトを表示した端末はマルウェアに感染する．

表 3 を基準に，DBD 攻撃に使用される悪性文書ファイルについて，攻撃の成功率を高めるものを “+1”，攻撃に気づかれる確率を上げるものを “-1”，どちらでもないものを “0” として評価を行った．DBD 攻撃には攻撃対象を限定しないバラマキ型の攻撃と，攻撃対象を限定した水飲み場型の攻撃の 2 種類がある．水飲み場型の事例がバラマキ型と比較して少ないため，ここではバラマキ型を想定して評価を行う．評価の結果を**表 5** に示す．

各項目ごとの評価基準について以下に示す．

5.2.1　Offline

DBD 攻撃は，攻撃の起点が Web サイトの閲覧であり，被害者の端末がネットワークに繋がっていることが前提となっている．したがって，被害者の端末がネットワークに繋がっていない場合については評価を行わない．

5.2.2　Infection(Inf.)

マルウェア本体の実行に成功（OK）のものを “+1” とした．また，マルウェアの実行はバックグラウンドで処理されており，マルウェアの実行に失敗したとしても，被害者が攻撃に気づくことには繋がらないことから “0” とした．

5.2.3　Decoy(Dec.)

DBD 攻撃の初期段階である，マルウェアへの感染の起因となった被害者の行動は，改ざんされた Web サイトの表示である．被害者は正規の Web サイトのコンテンツを期待して改ざんされた Web サイトを表示する．Web ブラウザは，改ざんされた Web サイトに関連するコンテンツとして悪性文書ファイルを表示する．しかしながら，この悪性文書ファイルの表示に関する処理は，閲覧者の行動と直接結びついたものではない．閲覧者は，この悪性文書ファイルの存在自体意識していない．したがって，標的型メール攻撃の場合と異なり，ダミー表示は必要ない．逆に，ダミー表示をすると，閲覧者が文書ファイルを開いていることを意識するため，閲覧者が攻撃に気づく可能性が高くなってしまう．そのため，ダミー表示用の文書ファイルが表示されるものを “-1”，表示されないものを “+1” とした．

表 6　マルウェア感染の成功回数の期待値
Table 6　The number of success attacks.

		s				
k	n	1 %	25 %	50 %	75 %	99 %
1 %	99	0.99	24.75	49.50	74.25	98.01
25 %	3	0.03	0.75	1.50	2.25	2.97
50 %	1	0.01	0.25	0.50	0.75	0.99
75 %	0.3	0.00	0.08	0.17	0.25	0.33
99 %	0.01	0.00	0.00	0.01	0.01	0.01

5.2.4　Shellcode

Shellcode を小さくすることで，攻撃することのできる脆弱性の種類が増えたり，shellcode 内に実装できる検知回避技術の種類が増えることから，シェルコードのサイズが小さくなるものを “+1” と評価した．

5.2.5　Target

DBD 攻撃の多くは攻撃対象を限定しない，いわゆるバラマキ型の攻撃である．したがって，攻撃対象を広く取れることは，感染端末の増加につながり，攻撃の成功率を高めるものである．したがって，攻撃対象を広げるもの（Wide）を “+1” とし，それ以外を “0” とした．

6.　各攻撃に最適な悪性文書ファイル

1 回の攻撃で被害者が攻撃に気づく確率を k とすると，攻撃に気づかれるまでに，攻撃者が攻撃できる回数の期待値 n は以下の数式で示せる．

$$n = \frac{1}{k} - 1 \tag{1}$$

また，1 回の攻撃での攻撃の成功確率を s とすると，攻撃に気づかれるまでに，マルウェア感染に成功する回数の期待値 N は以下の数式で示せる．

$$N = s \times n = s \times (\frac{1}{k} - 1) \tag{2}$$

攻撃に気づかれる確率（n）とマルウェア感染の成功確率（s）から，マルウェア感染に成功する回数の期待値（N）を求めた結果を**表 6** に示す．

マルウェアの感染という攻撃の初期段階の目的を達成するためには，マルウェア感染に成功する回数は 1 回で十分である．したがって，攻撃対象が限定されている場合，マ

ルウェア感染に成功する確率を上げるよりも，いかに攻撃に気づかれないかが重要になってくる．一方，攻撃対象を特に限定しない場合，いかに攻撃範囲を広げるかが重要になってくる．

この結果を踏まえ，各攻撃ごとに最適な悪性文書ファイルについて考察を行う．

6.1 標的型メール攻撃

標的型メール攻撃の場合，攻撃対象は特定の組織または個人である．攻撃対象が限定されているため，攻撃に気づかれる確率を下げることが重要になる．したがって，表 4 で “-1” と評価されている悪性文書ファイルは攻撃に適していない．その上で，よりマルウェア感染の確率が高くなるものを選択した場合，マルウェア本体およびダミー表示用の文書ファイルを悪性文書ファイルの中から取り出すタイプの悪性文書ファイルになるものと推測される．

6.2 DBD 攻撃

DBD 攻撃の場合，その多くが攻撃対象を限定しない，いわゆるバラマキ型攻撃である．この場合，以下に攻撃範囲を広げるかが重要になってくるため，表 5 の “Target” で “+1” と評価されていることが重要である．また，ダミー表示をするコストをかけた上で得られる効果は，攻撃に気づかれやすくなるというデメリットであるため，ダミー表示をすることは通常考えられない．したがって，DBD 攻撃で使用される悪性文書ファイルは，ダミー表示を行わない downloader になるものと推測される．

7. おわりに

本論文では，攻撃種別ごとに悪性文書ファイルの特徴に顕著な差があることを明らかにした．この差が生じる理由を推測するため，攻撃の成功率を高めるという攻撃者の視点にたった考察を行った．各攻撃には攻撃者の目的があり，その目的を達成するために最適な悪性文書ファイルの種類を攻撃者が選択した結果，悪性文書ファイルの特徴に偏りが出ていることが推測される．

今後は，攻撃種別の種類を拡大しマルウェアのファイル形式を文書ファイルに限定せずに調査を行うことで，マルウェアの特徴に差がでるのか明らかにしていきたい．

参考文献

[1] Micro, T.: Targeted Attack Campaigns and Trends: 2014 Annual Report, `http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-targeted-attack-trends-annual-2014-report.pdf` (2015).

[2] Nelms, T., Perdisci, R., Antonakakis, M. and Ahamad, M.: Towards Measuring and Mitigating Social Engineering Software Download Attacks, *25th USENIX Security Symposium (USENIX Security 16)*, Austin, TX, USENIX Association, pp. 773–789 (online), available from ⟨https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/nelms⟩ (2016).

[3] Microsoft: Rich Text Format (RTF) Specification, version 1.9.1., `https://www.microsoft.com/en-us/download/details.aspx?id=10725`.

[4] Microsoft: [MS-CFB]: Compound File Binary File Format, `https://msdn.microsoft.com/ja-jp/library/dd942138.aspx`.

[5] ISO: ISO32000–1:2008 Document management – Portable document format – Part 1 : PDF1.7., `http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51502`.

[6] 神薗雅紀，秋山満昭，笠間貴弘，村上純一，畑田充弘，寺田真敏：マルウェア対策のための研究用データセット～MWS Datasets 2015～，技術報告 6，プライスウォーターハウスクーパース株式会社, 日本電信電話株式会社，NTT セキュアプラットフォーム研究所, 国立研究開発法人情報通信研究機構, 株式会社 FFRI, エヌ・ティ・ティ・コミュニケーションズ株式会社, 株式会社日立製作所 (2015).

[7] contagio: 16,800 clean and 11,960 malicious files for signature testing and research, `contagiodump.blogspot.jp/2013/03/16800-clean-and-11960-malicious-files.html` (2013).

[8] VirusTotal: VirusTotal, `https://www.virustotal.com/`.