# 標的型攻撃で用いられたマルウエアの特徴と攻撃の影響範囲の関係に関する考察

船越 絢香† 中村 祐† 竹田 春樹†

†一般社団法人 JPCERT コーディネーションセンター
101-0054 東京都千代田区神田錦町 3-17 廣瀬ビル 11 階
aa-info@jpcert.or.jp

**あらまし** 昨今、複数の組織より標的型攻撃によるマルウエア感染とそれにともなう情報漏えいが報告されている。標的型攻撃においては、標的に合わせてカスタマイズされたマルウエアや汎用的なツールが使用される事が知られている。そのため、既知のマルウエアや個別のツールといった目に見える脅威にのみ対応しても、適切に対処したとは言えない。本稿では、実際の標的型攻撃の調査事例をもとに、使用されたマルウエアやツールの使い分けや機能の分析を行い、単体の検体といった限られた情報から、攻撃による影響範囲を推察する方法について提案する。

# A study on malware characteristics and its effects observed in targeted attacks

Ayaka Funakoshi† Yu Nakamura† Haruki Takeda†

†Japan Computer Emergency Response Team Coordination Center
Hirose Bldg.11F, 3-17 Kanda-nishikicho Chiyoda-ku, Tokyo 101-0054, Japan
aa-info@jpcert.or.jp

**Abstract** Lately, various organizations have reported about targeted attacks resulting in malware infection and information leakage. It is widely known that targeted attacks use customized malware for each target and generic tools. Thus, dealing with visible threats, such as known malware and individual tools is not enough to completely address the threat. This article analyzes different usage and functions of malware and exploit tools based on actual targeted attack cases, and suggests a method to infer attack effects through limited information such as individual samples.

## 1. はじめに

昨今、標的型攻撃によるマルウエア感染とそれにともなう情報漏えいが、政府機関や企業等の複数の組織から報告されている[1]。

標的型攻撃の攻撃者（以下、攻撃者という）は、標的とした組織(以下、被害組織という)内の機密情報や知的財産といった情報（以下、重要情報という）の窃取や改ざん、破壊を目的に、長期間にわたって被害組織に対し執拗に攻撃を試みることが分かっている。攻撃者は、目的

を達成するために複数のマルウエアおよびツールを使い分けることが知られている[2]。攻撃者は一連の攻撃を通して、複数のマルウエアを使用するにも関わらず、攻撃を受けた、もしくは攻撃を受けている疑いがあるとわかった時点の初動対応では、検体の痕跡は一部しか発見できないことが多く、被害範囲を把握することが困難であることが多い。また、これらのマルウエアやツールは標的組織に合わせてカスタマイズが施されており、マルウエア自体も段階的にアップデートが繰り返されるため、シグネチャマッチングによる検知が難しい。そのため端末から発見された検体を調査･駆除するのみでは攻撃の全体像が把握できず、被害範囲の想定を誤る可能性がある。また、駆除されず潜伏していたマルウエアから攻撃が再開され、さらに被害が拡大することも考えられる。そのため、限られた情報から、攻撃の全体像や被害範囲を想定し、体系的な調査･対処を行うことが重要である。

本稿では、特定の検体群が使用される標的型攻撃の事例の分析を行い、攻撃の流れをステップに分け、各ステップにおいてマルウエアやツールが使い分けられていることを示し、使用された検体の分類について述べる。その結果を用いて、一部の痕跡としての検体の情報から、攻撃による影響を推察する方法を提案する。

## 2. 背景

### 2.1. 標的型攻撃の流れ

標的型攻撃への対応を検討する際に、事前調査から目的の遂行まで複数の攻撃ステップに分けて整理する考え方がある[3]。標的型攻撃では、マルウエアの通信先の用意や配布サーバの構築、被害組織の関連情報の収集といった準備を整えた後、偽装メールや正規サイト等の改ざんによるマルウエア配布サーバへの誘導等を通して、被害組織の端末にマルウエアを感染させ、ネットワーク内に侵入する。被害組織への侵入後は、被害組織のシステムを横断的に侵害していき、重要情報が存在するシステムに到達するとともに、被害組織のネットワーク内に最初の侵入経路と違ったバックアップとして用意した入口(以下、裏口という)を設置し、侵害したシステムや端末に継続してアクセスできるようにする。そして、攻撃者は重要情報の窃取や改ざん、破壊等の目的を達成することがわかっている。

### 2.2. 初動対応の難しさ

標的型攻撃にあった被害組織のうち半数以上は被害の認知までに数ヶ月から数年を要しており、被害組織の多くは外部組織からの連絡によって被害を知ることが報告されている[4]。外部組織からの連絡を契機に初動対応を開始した場合には、連絡を受けた内容をもとに攻撃者のインフラと通信している端末を特定する調査を行う。攻撃の最初に使用されるマルウエアの挙動は、被害組織が攻撃を受けていることに最も気づきやすい機会である。しかし、攻撃者は被害組織に侵入後、すみやかに次のステップに移行し、裏口を設けるマルウエアを送り込み、被害組織内の侵害した複数のシステムや端末を起点(以下、攻撃拠点という)とする攻撃を行うことがわかっている[3]。裏口を設けるために使用されるマルウエアは、通信頻度が限定されていたり、直接外部との通信を行わない等、発見されにくい工夫がなされている。これらのことから、標的型攻撃に対する初動対応は、非常に重要であるにも関わらず、攻撃の全体像を把握し的確な対処を行うことは困難である。

## 3. 標的型攻撃事例の分析

本稿では、いくつかの標的型攻撃の事例をもとに、攻撃の各ステップで使用されるマルウエアやツールの分類手法とその結果について述べる。その結果を用いて、発見された検体と被害組織における攻撃の進行度との関連について考察する。

### 3.1. 各ステップにおけるマルウエアやツールの使い分け

標的型攻撃のプロセスに対する考え方としては、Cyber Kill Chain[5]がよく知られている。Cyber Kill Chain では、攻撃が 7 つのステップに分解されているが、本稿では、攻撃者が目的の達成に至るまでのステップを、(1)準備、(2)侵入、(3)横断的侵害、(4)目的の遂行の 4 ステップに分け、それぞれのステップで行われる攻撃内容と使用されるマルウエアやツールを調査した。

(1) 準備

攻撃者は、被害組織の関連情報の収集や新しいドメインの取得、正規サーバのハッキング等を行い攻撃基盤の構築および被害組織に侵入するためのマルウエアの生成等を行い、攻撃手法や侵入経路の構築を行う。

(2) 侵入

マルウエアを添付した偽装メールや正規サイトの改ざん等によるマルウエアの配布サーバへの誘導、または脆弱性を悪用した攻撃により、被害組織の端末をマルウエアに感染させ、被害組織のネットワークに侵入する。この際には主にボットと呼ばれるマルウエアが使用される。

(3) 横断的侵害

被害組織内での攻撃拠点の構築のため、さらに自由度の高い遠隔操作を行うためのRAT(Remote Administration Tool)や、ネットワーク内のシステムや端末を把握するためのスキャンツールやパスワード情報取得ツール等の複数のマルウエアやツールに加え、正規ツールやOSの標準コマンド等が使用される。また、侵入で使われたマルウエアとは別のボットが裏口として送り込まれる。横断的侵害を行う際には、実際に攻撃を行う端末と外部から遠隔操作される端末は別であることが多く、これらは被害組織のネットワーク内で相互に通信を行うマルウエアが使用される。

(4) 目的の遂行

横断的侵害の結果、重要情報が保管されているシステムや端末に到達すると、攻撃拠点を用いて、重要情報の窃取等を行い、正規のデータ圧縮ツールでデータを圧縮または暗号化して攻撃者のインフラに送信する等の活動が行われる。

### 3.2. 検体の種別による攻撃の進行度の想定

被害組織の端末から発見される検体と横断的侵害の範囲の相関について、事例をもとに分析を行った。攻撃者の目的は重要情報の収奪や破壊等の活動であると思われることから、ドメインコントローラやファイルサーバ等の重要なシステムの侵害の可能性が高いと判断できた場合に、被害規模が大きいとした。例として、ドメインコントローラやファイルサーバに想定しないアカウントでのログイン（攻撃者による不正ログイン）が確認された場合等である。一方、重要サーバへの侵害の痕跡が発見されず、初期感染端末からの横展開の可能性も低い状況であると考えられた場合に、被害規模が小さいと判断した。

(1) 被害規模の小さい事例

被害規模が小さいと思われる事例では、組織への侵入のために使用されるボットが発見される他には、横断的侵害のための調査目的の検体が確認された。検体が発見されるのも攻撃の入り口となった端末のみである等、限定的であった。これらの事例では、侵入～横断的侵害の半ばまでが行われたものの、攻撃者の目的達成までは至っていないケースであると推察される。このような状況の組織では、攻撃への対処に約1～数ヶ月の期間を要した。

(2) 被害規模の大きい事例

被害規模が大きいと思われる事例では、侵入に使用されるボットに加えて、横断的侵害のための検体が複数種類発見された。さらに、初期感染端末以外のクライアントや重要サーバから裏口となるマルウエアが発見された。これらの事例では、侵入～目的の遂行までの一連の流れが行われ、攻撃者が目的を達成したケースであると思われる。このような状況が確認された組織では、攻撃への対処に1年以上かかる場合もあり、また、対処が十分でなく、裏口から攻撃が再開された事例も確認している。

このような事例から、横断的侵害に使われる検体が複数種類確認された場合、裏口となるマルウエアが発見された場合、初期感染端末以外の端末や重要サーバから検体が見つかった場合に、より攻撃が進行していることが推察された。

## 4. 特定の攻撃に着目した検証

本稿では、昨今、標的型攻撃において使用されるマルウエアである Emdivi[6]の亜種に着目し、Emdivi が用いられた一連の攻撃について、各ステップで使用される検体の種類･機能を調査した。

### 4.1. ステップ毎に使い分けられる検体の分類

Emdivi の亜種が用いられた一連の攻撃では、複数の端末から発見された検体が以下の7種類に分類できることがわかった。表 1 に検体の分類を示す。

検体 1 は、メールでの感染時に主に発端となる検体であり、文書ファイル等に偽装されているものが多く見られる。検体 1 は、実行すると、無害の表示用文書を表示する裏で、検体 2 の作成、実行が行われる。検体 3 は、例として mimikatz[7], timestomp 等のツールの他、Active Directory Application Mode (ADAM)に含まれる csvde コマンド等の正規ツールが使用されているのを確認している。検体 4 は、DLL ファイルもしくは data ファイルで、他の実行ファイルに読み込まれることで起動され、ダウンロードした設定情報に従って他の検体をダウンロードする検体で、裏口として使用されるケースを確認している。検体 5 は検体 2 に構造的に類似したボットであるが、検体 2 とは異なる体系の検体と思われ、ボットとしての機能も検体 2 より豊富である。検体 6 はリモートシェル検体であり、相互に通信可能なクライアントおよびサーバの役割を持つ検体が存在する。検体 1～6 に分類できない検体について、検体 7 に分類した。

### 4.2. 攻撃のステップと検体の関係

Emdivi が用いられた攻撃の実際の事例を 3.2と同様に被害規模の小さい事例、大きい事例に分け、4.1で分類した検体の存在有無と攻撃の進行度の関係を調査した。

(1) 被害規模が小さい事例における各検体の存在有無

被害組織のシステムからは、検体1, 2に加え、検体3が高い割合で発見された。

| 分類 | 概要 | ファイル形式 | 使用されるステップ |
|---|---|---|---|
| 検体 1 | 偽装されたメールに添付されたマルウエア | EXE | 侵入 |
| 検体 2 | 検体 1 を実行すると作成される、検体内に t17.**の文字列を持つボット | EXE | |
| 検体 3 | ツール類 (パスワードダンプツールや脆弱性を悪用するツール) | EXE 等 | 横断的侵害 |
| 検体 4 | 他の検体をダウンロードするダウンローダ | DLL, data | |
| 検体 5 | 検体内に t19.**, t20.**の文字列を持つボット | EXE | |
| 検体 6 | リモートシェルツール | EXE, DLL | |
| 検体 7 | その他 | | - |

表 1 被害組織の端末から発見される検体の分類

一方、検体4, 5, 6 は見つからないか、いずれか1種類程度が発見されることがあった。

(2) 被害規模が大きい事例における各検体の存在有無

検体1, 2に加え、検体3, 4, 5, 6の全てが高い割合で発見された。これらの事例では、重要サーバ上に検体3, 4や検体6のサーバ側が設置されている場合もあり、攻撃拠点の構築が達成されていることが想定された。

これらの事例において、それぞれの検体の発見された端末とその作成日時から、一例として、攻撃の進行度を図に表した(図 1, 図 2)。

### 4.3. BOS 2015 データセットを用いた検証

MWS DATAset 2015[8]の BOS 2015 のうち、Virus Total での検知結果に"EMDIVI"の文字列が含まれる d18, d19, d37 について、表 1 で分類された検体が含まれるかを調査した。なお、d18, d19 については、Pcap データが取得されていない時間帯が存在するため、システム全体の影響について考察できていない点がある。

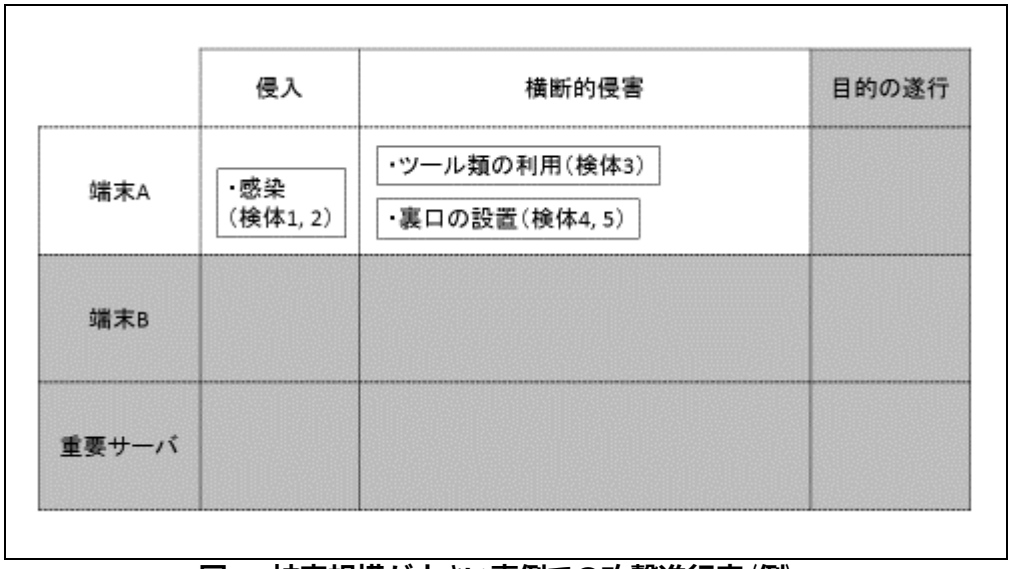


図 1 被害規模が小さい事例での攻撃進行度(例)

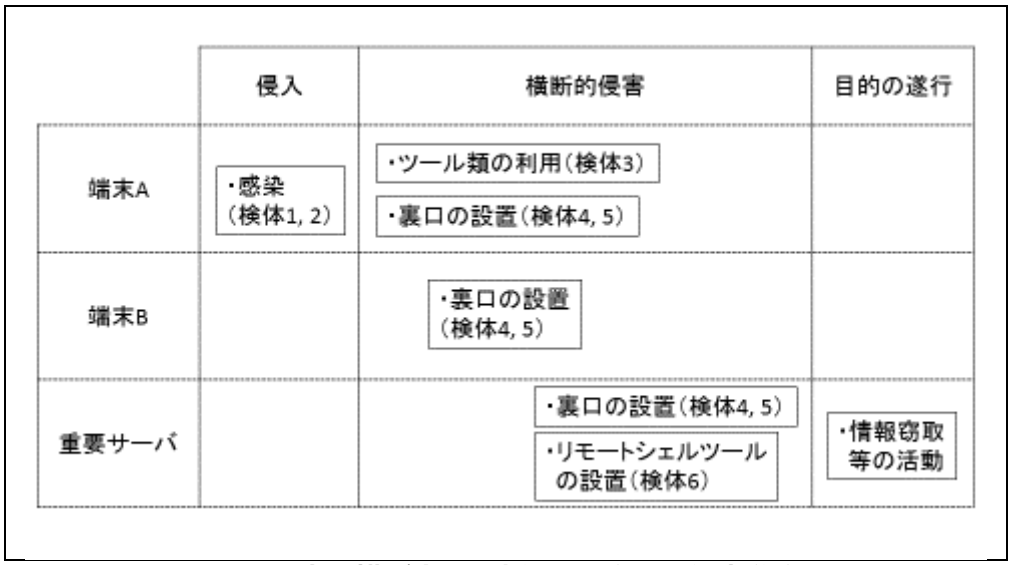


図 2 被害規模が大きい事例での攻撃進行度(例)

| 実行日時 | 実行ログ |
|---|---|
| 2014/10/16 21:03:13 | C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥csvde.exe |
| 2014/10/16 21:03:12 | C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥csvde.exe –f C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥1016.csv -u |
| 2014/10/9 15:15:21 | cmd /cC:¥Users¥tada¥AppData¥Local¥Temp¥uc.exe 127.0.0.1 ""tasklist /v"" |

**表 2 イベントログから抽出されたファイルの実行ログ** (d18)

| 検体の分類 | ファイルパス |
|---|---|
| **検体** 1 | C:¥Users¥administrator¥Desktop¥**医療費通知のお知らせ**.exe |
| **検体** 2 | C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥leassaq.exe |
| **検体** 3 | C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥csvde.exe (*1) |
| **検体** 4 | |
| **検体** 5 | |
| **検体** 6 | C:¥Users¥tada¥AppData¥Local¥Temp¥uc.exe (*2) |
| **検体** 7 | |

**表 3 検体の分類** (d18)

(1) d18

d18 **のイベントログから、ファイル実行を行っていると思われるものを抽出したところ、表** 2 **のエントリが得られた。表**2 **から、少なくとも**2 **つの検体が攻撃者により送り込まれていることが想定される。**d18 **と感染時期が近い事例で使われた検体名や使用時の引数との比較により、**csvde.exe(*1)**は** Active Directory **のアカウント情報をエクスポートするコマンド、**uc.exe(*2) **は、リモートシェルのクライアント側検体であると思われ、これらはそれぞれ検体** 3 **および検体** 6 **に分類される。以上から、少なくとも** d18 **の初期感染端末に存在する可能性がある検体を表** 3 **のように分類した。**

**以上から、**d18 **の環境においては、少なくとも横断的侵害のための調査が行われていることがわかった。ただし、他の端末やサーバに検体** 4**～**7 **に属する検体が存在する可能性があり、攻撃のステップはより進行している可能性がある。**

(2) d19

d19 **のイベントログについて** d18 **と同様の調**

| 実行日時 | 実行ログ |
|---|---|
| 2014/10/14 11:29:56 | C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥CallMail.EXE /stext C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥1.tmp |

**表 4 イベントログから抽出されたファイルの実行ログ** (d19)

| 検体の分類 | ファイルパス |
|---|---|
| **検体** 1 | C:¥Users¥administrator¥Desktop¥**医療費通知のお知らせ**.exe |
| **検体** 2 | C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥leassaq.exe |
| **検体** 3 | C:¥Users¥ADMINI~1¥AppData¥Local¥Temp¥CallMail.EXE (*3) |
| **検体** 4 | |
| **検体** 5 | |
| **検体** 6 | |
| **検体** 7 | |

**表 5 検体の分類** (d19)

査を行い、表 4 のファイル実行結果のエントリと表 5 の検体分類結果を得た。CallMail.EXE(*3)は端末内に保存されているメールアカウント情報を出力するツールであると思われる。

d19 の環境においても、少なくとも、組織のシステムの調査が行われていることが推察された。

(3) d37

d37 のイベントログについて、d18 と同様の調査を行ったところ、ファイルの実行ログは確認できなかった。また、d37 の Pcap データに含まれる HTTP 通信で送受信されたファイルを全て抽出し、EXE, DLL 形式、あるいは内部に EXE, DLL ファイルを含む ZIP, RAR, LZH ファイルが含まれているかを調査した。なお、検体が通信を開始する前から通信が発生していた以下のドメインに関しては、正規ドメインとして解析対象外とした。

| |
|---|
| deepdiscovery37-p.activeupdate.trendmicro.co.jp |
| tms-rcv01.trendmicro.co.jp |
| jdc2-tmsp01-rt.trendmicro.co.jp |
| licenseupdate.trendmicro.com |
| dl.javafx.com |
| ddi37-jp.url.trendmicro.com |

表 6 解析対象外とした正規ドメイン

d37 の 2015 年 1 月 23 日～27 日の Pcap データについて分析を行ったところ、条件に該当するファイルはなかった。以上から、d37 は、侵入までが行われており、被害規模は小さいと考えられる。

## 5. 検証結果と考察

Emdivi が用いられた標的型攻撃の実事例および BOS 2015 を用いて、標的型攻撃の各ステップのうち、侵入・横断的侵害で使用されるマルウエアやツールの分類と使い分けについての調査を行い、被害組織のシステムから発見される検体から被害規模を推測する方法を提案した。横断的侵害で用いられる検体は、主に調査目的の検体（検体 3）と侵害に使われる検体（検体 4, 5, 6）に分けられることがわかった。侵害に使われる検体がより多く発見された場合に、被害組織における影響が大きくなる傾向があった。また、初期感染端末から横断的侵害が行われたと思われる端末やサーバに検体が存在した場合にも、被害が大きくなる可能性があることがわかった。被害組織のシステムで、以上の条件が満たされている場合、被害の規模について更なる調査が必要であると考えられる。

今回の調査では、重要サーバの侵害を重要情報の窃取や破壊に繋がる比較的大きな被害と定義して考察したが、重要情報が個々の端末に保存されている場合等は、横断的侵害を行わなくても攻撃者が目的を達成できる可能性がある。その結果、システムから発見される検体数が少なくなる等、本稿の推定と異なることも考えられる。また攻撃者が、不要になったツール類等を削除する事例も確認しており、ファイルシステム上からは一部検体が確認できない場合もある。実際、BOS 2015 の d18 および d19 では、一部の検体を削除する挙動をイベントログから確認している。このような事例では、ファイルシステム上での確認のみでなく、端末のフォ

| 検体の分類 | ファイルパス |
|---|---|
| 検体 1 | C:¥Users¥hcg01504.HITACHI¥Desktop¥2015.01.19.102850.exe |
| 検体 2 | C:¥Users¥HCG015~1.HIT¥AppData¥Local¥Tempvmmat.exe |
| 検体 3 | |
| 検体 4 | |
| 検体 5 | |
| 検体 6 | |
| 検体 7 | |

表 7 検体の分類（d37）

レンジック等を実施する必要がある。

## 6. まとめ

本稿では、標的型攻撃の実事例を元に、一連の攻撃をステップに分け、各ステップで用いられるマルウエアやツールの特徴および使い分けを示した。さらに、その結果を元に、端末内から発見された検体から、被害規模を想定する方法を提案した。

昨今、サイバー攻撃に対して、マルウエアの通信先やハッシュ値といった情報を共有する取り組みが行われるようになってきている。一方で、標的型攻撃では、巧妙な攻撃手法が用いられ、個々の組織の弱点を悪用して攻撃が継続される。また、準備段階で標的組織の特性やシステムが入念に調査された上で攻撃が開始されるため、攻撃手法自体に重要情報が含まれる場合がある。したがって、各組織のシステム内部での攻撃者の活動といった情報の共有が進みにくい状況にあり、本稿で提案したような手法を様々な攻撃に対して提供して行くことは容易ではない。

本稿で示したように、実事例を元にして攻撃者の組織侵入後の活動を整理することで、個々の事例についての詳細を示すことなく、対策考案に寄与する情報が提示できるようになる。そのためには、信頼できる組織間での連携による密度の高い情報共有が欠かせない[9]。

標的型攻撃では今後もより複雑な手法が用いられることが予想される。情報共有への理解を得るためにも、引き続き実事例を元にした分析を行うとともに、それらの分析結果を安全に共有する方法についても検討していく。

## 7. 参考文献


[1] 独立行政法人情報処理推進機構. サイバーレスキュー隊(J-CRAT)の活動報告 ～2014 年度および J-CRAT 発足1年(2014/7～2015/6)～. https://www.ipa.go.jp/files/000047193.pdf

[2] 株式会社ラック. Cyber GRID View vol.1 日本における標的型サイバー攻撃の事故実態調査レポート. http://www.lac.co.jp/security/report/pdf/20141216_cgview_vol1_d001t.pdf

[3] 独立行政法人情報処理推進機構. 標的型攻撃／新しいタイプの攻撃の実態と対策. https://www.ipa.go.jp/files/000024542.pdf

[4] Verizon. 2014 年度データ漏洩/侵害調査報告書. http://www.verizonenterprise.com/resources/reports/rp_Verizon-DBIR-2014_ja_xg.pdf

[5] Cyber Kill Chain. http://cyber.lockheedmartin.com/cyber-kill-chain-lockheed-martin-poster

[6] Backdoor.Emdivi. http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2014-101715-1341-99

[7] mimikatz. https://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2012-042615-3731-99&tabid=2

[8] 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～. 情報処理学会 研究報告コンピュータセキュリティ(CSEC). Vol. 2015-CSEC-70, No. 6, pp. 1 - 8, 2015

[9] 澤田昭浩, 竹田春樹. 水飲み場型攻撃などの最近の標的型攻撃の動向と対策. Vol.28, No2, 日本セキュリティ・マネジメント学会, 2014