

# パソコン内の怪しいマルウェアを見つけ出す方法

山守一徳<sup>†</sup> 松原伸樹<sup>‡</sup>

## A Method to Check Whether Doubtful Malware is Included in Own PC

Kazunori YAMAMORI<sup>†</sup> Nobuki MATSUBARA<sup>‡</sup>

<sup>†</sup>三重大学教育学部

<sup>‡</sup>三重大学総合情報処理センター

### 概要

大学のネットワーク内には、ウイルス感染に気付かずにいる利用者が少なからず存在し、被害が広がってしまう恐れがある。ウイルス駆除ソフトをダウンロードしてインストールできる環境にありながら、最新版をインストールせず無頓着に利用を続ける場合だけでなく、ウイルス駆除ソフトで検出されないウイルスが隠れていたりする。ネットワーク管理者は、ネットワークデータの挙動から怪しい端末を見つけることがあるため、そのために役に立つ手法を述べる。この提案する手法は、ネットワーク管理者だけでなく、Windows を利用する個々人にも役に立つ手法であり、自分のWindows パソコン上に怪しいマルウェアが動いているのではないかと心配になった時に調べて、マルウェアを突き止める方法である。

### キーワード

コンピュータウイルス、ウイルス対策、セキュリティ対策、FireWall、エンドポイントセキュリティ

#### 1. はじめに

ウイルスが自分のパソコンに入り込んでいないかは、ウイルス駆除ソフトでスキャンして調べるのが簡単であるが、検出漏れを起こすことがある。ウイルス駆除ソフトが最新状態になっていない場合には、調べる能力も激減してしまっており、状態を最新にするために、ネットワーク接続を続けて更新作業をしてよいかも不安になる。ウイルス駆除ソフトがインストールすらされ

ていない場合もある。

そこで、ウイルス駆除ソフトを使わずに調べる方法を述べる。

いつどこからウイルスが入り込んだのかを調べたい場合には、できるだけ状態を保全したまま、パソコンの中を調べたいものである。再起動することなく、ツールを取り込んで稼働させることで、怪しいプログラムを見つけ出したい。ここで紹介するツールは、USB メモリ上などに用意しておき、その媒体をパソコンに接続し、その中のプ

プログラムを起動させてパソコン内を調べることができるツールである。

大学のネットワークを監視していると、怪しいデータの流れを見つけることがある。端末の持ち主にウイルスが入り込んでいないかを調べて欲しいと頼んでも、ウイルス駆除ソフトが最新になっていなかったり、利用者自身で突き止められない場合がある。その場合に、ネットワーク管理者が出向いていき調べる時に使うことができるツールを挙げる。

実際に大学の現場で、怪しい動きを見つけ、端末上のウイルスを見つけ出した時の方法についても述べる。

## 2. 使用するツール

以下に解説するツールを列挙する。

- (1)Virus Total
- (2)Autoruns
- (3)Process Hacker
- (4)Process Explorer
- (5)Process Monitor
- (6)WinPrefetchView
- (7>User Assist
- (8)TCP Explorer
- (9)TCPView
- (10)Wireshark
- (11)NetworkUsageView
- (12)HashMyFiles
- (13)HybridAnalysis
- (14)urlQuery
- (15)Cymon

### 2.1 Virus Total

ダウンロードして利用するツールではなく、ファイルを読み込ませてウイルスが含まれているかを判定してくれるサイトである。https://www.virustotal.com/ の英語サイト(図 1 参照)が本家であり、https://www.virustotal.com/ja/ の日本語サイ

トも開設されているが、最新のウイルスのチェックが反映されるのは英語サイトからであろうと推測されるので、英語サイトを利用した方が良い。Choose file ボタンを押して、ファイルを選択し、「Do you want to continue with the upload and get this file scanned?」と聞かれたら OK ボタンを押すと、ファイルがアップロードされていき、調査が開始される。分母が 60 程度の大きな数字で分子が 0 という結果になれば問題はない。分子が 1 になることもある。分子が 2 以上なら危険なファイルである。

注意しないといけないのは、ファイルがアップロードされていくので、重要機密ファイルは、このサイトで調べることをしてはいけない。有償サービスの「VirusTotal Intelligence」ではアップロードされたファイルの情報を入手できるため、セキュリティベンダーなどがマルウェア動向などを研究する目的で、この有償サービスを利用してアップロードされたファイルを取得している。マクニカネットワークスが調べたところ<sup>4)</sup>では、アップロードされたファイルは、サンドボックス上で解析されていたりするが、マルウェア解析以外のシステムで利用されている可能性もあるとされている。

VirusTotal は、URL を指定して、危険なページか調べることができるので、メール

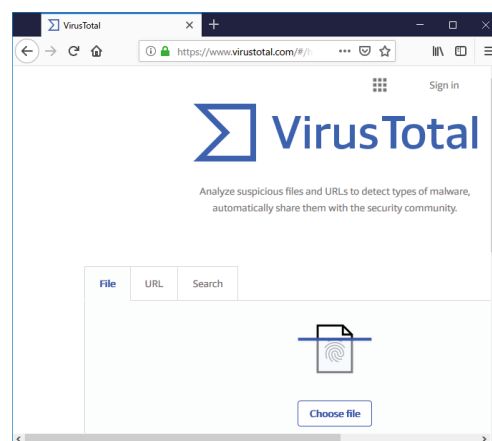


図 1 Virus Total の英語サイト画面

本文等に書かれてくる URL が怪しい時には、この URL 指定の方法でチェックすることができる。また、検索欄にドメイン名や、IP アドレス、ファイルのハッシュ値を入れてメガネの絵のボタンを押すことでも、危険性を調べてもくれる。ファイルの中に機密情報が入っているかもしれないファイルの場合は、ハッシュ値を入れる方法で調べるのが良い。

VirusTotal の弱点は、新しいマルウェアの場合、多くのウィルス対策ソフトで対応できてない場合があるため、判定が正しくできてない恐れがある。そのため、DETAILS のタグの中の History の欄の First Submission の日時を確認した方が良い。これは、VirusTotal に初めて送られてきた日時を示しており、新しい日付の場合、新しいマルウェアである可能性が高くなる。

## 2.2 Autoruns

Windows Sysinternals という Microsoft 自身が Windows のトラブルシューティング用に役に立つ無償ツールをいくつか提供している。Autoruns はそのツール群の中にあるツールの一つであり、<https://technet.microsoft.com/ja-jp/sysinternals> のサイトには、「毎回起動する迷惑ソフトウェアの除去」の方法として紹介されている。

<https://technet.microsoft.com/ja-jp/sysinternals/hh237366> のサイトに使い方

が掲載されており、その中では、Publisher 欄が空欄になっているプログラムを見つけ、「迷惑ソフトウェアかもしれないと思った時には、まずチェックボックスを外して再起動し、自動実行されなくなるかまずは確認してください。」「再起動後に迷惑ソフトウェアが実行されなくなり、かつ Windows そのものも正常に起動した場合、チェックボックスを外したプログラムを削除します。」という手順が書かれている。正常に動いている時に Autoruns を実行し、情報を保存しておく、怪しいと感じた時に比較して迷惑ソフトウェアを見つけることができることも書いてあるが、正常時から Autoruns の実行結果を保存しておくように仕向けるのは、よほど指導しないと実施しないと思われる。

<https://technet.microsoft.com/ja-jp/sysinternals/bb963902> から実行ソフトをダウンロードすることができ、デフォルトでは Autoruns.zip のファイル名で保存される。展開すると、Autoruns フォルダができ、その中に Autoruns.exe と Autorunsc.exe (64bit 版もある) が現れ、autoruns.exe は GUI のツール、autorunsc.exe はコマンドラインのツールであるため、Autoruns.exe の方が使い勝手が良い。Autoruns.exe を起動すると利用の仕方の同意を求められ Agree ボタンを押す。図 2 のように動き出して、Options のメニューの Scan Options を選び、Check VirusTotal.com にチェックを入れて Rescan ボタンを押す。右の方に表示される Virus Totals の欄の分子の数が 0 だと安心、数が多いのは大変危険なプログラムである。1 はよくあり得るので、即アウトとは言えない。さらに、Options のメニューの Scan Options を選び、Verify code signatures にチェックを入れて Rescan ボタンを押す。そして、Publisher の欄に (Verified) と出ていると一応安心で

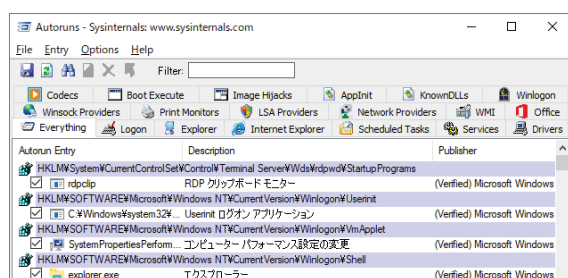


図 2 Autoruns.exe の起動後の画面

ある。(Not verified) と出ている有名会社のソフトもある。

Image Path の欄に、プログラムのファイルの場所を示しており、その場所をエクスプローラで見に行っても見えない場合が多く、その場合は、コマンドプロンプトで `dir /a` フォルダ名 のコマンドを叩くと、隠しファイル状態のファイルも見ることができる。Image Path の欄に、File not found: が現れる行も複数存在する。

起動を止めるために左端のチェックを外すと、「アクセスが拒否されました」と表示され、「Run as Administrator」ボタンが出て、そのボタンを選ぶと「Autoruns にこのコンピューターへの変更を許可しますか?」と聞かれるので、「はい」のボタンを押す。チェックを外し再起動して問題なければ行選択し Entry メニューから delete を選択すると削除される。アクセスが拒否されましたと表示されてチェックを外すことができない行も存在する。

## 2.3 Process Hacker

<https://processhacker.sourceforge.io/> のサイトから processhacker-2.39-setup.exe のインストーラ版と processhacker-2.39-bin.zip のポータブル版をダウンロードすることができるが、USB メモリに保存して解凍しその USB メモリを調べるパソコンに接続して稼働させることを考慮すると、processhacker-2.39-bin.zip のポータブル版をダウンロードする。展開すると、デフォルトでは processhacker-2.39-bin

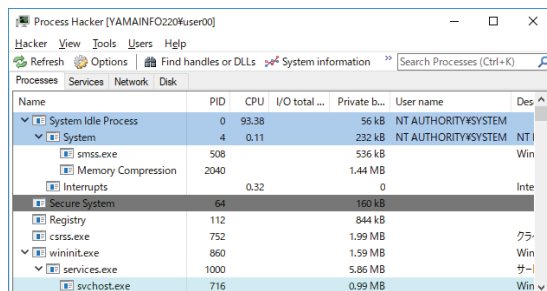


図 3 ProcessHacker の起動後の画面

のフォルダの下に、x64 のフォルダと x86 のフォルダができ、64bitOS の場合、x64 の下の ProcessHacker.exe を起動する。

Processes のタブで、デスクトップやスタートメニューから起動したプログラムは、explorer.exe の配下に表示されるはずである。階層構造で表示してくれる (図 3 参照) ので、どのプログラムから起動されているのかがわかる。Internet Explorer を起動している場合は、iexplore.exe の名前が表示されるが、起動していないにもかかわらず iexplore.exe が存在する場合は、怪しいプロセスであると判断できる。

Name の欄でクリックすると並び順を変えてくれる。Options の中の Reset ボタンを押すと表示の仕方の設定を初期状態に戻してくれる。行を選んで右クリックして、Properties を選べば、詳細が見える。Network のタブで、行を選んで右クリックして、Go to process を選べば、Processes のタブの中の該当プロセスを示してくれる。Network のタブで、行を選んで右クリックして、Tools の中の Whois を選べば、接続先の情報を教えてくれる。

<https://mag.osdn.jp/09/11/12/0840211> のサイトには、使い方が紹介されており、Processes のタブの中の怪しいプロセスを右クリックして Send To を選び、virustotal.com を選びと、VirusTotal のサイトでそのプログラムがマルウェア等でないかをチェックしてくれる。ProcessHacker は起動したタイミングにおいて、動作中であったプログラムが表示されるので、ずっと見る時には、View メニューの中にある Refresh automatically をチェック入った状態にしておく必要がある。

## 2.4 Process Explorer

Process hacker と似たツールで、稼働中のプロセスの一覧を表示する。Microsoft 自身が提供する Windows Sysinternals ツー

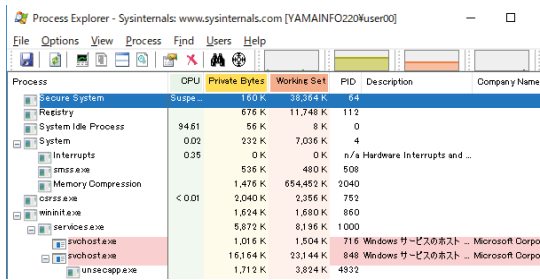


図 4 ProcessExplorer の起動後の画面

の一つである。<https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer> から「Download Process Explorer」と書いてあるリンクをクリックし ProcessExplorer.zip をダウンロードする。展開すると、procexp.exe と procexp64.exe の2つの実行ファイルが現れる。同じサイトの「Run now from Sysinternals Live」と書いてあるリンクをクリックし、procexp.exe をダウンロードし、実行させることもできて、これは、ProcessExplorer.zip を展開して現れたファイルと同じである。

Process hacker と比べると、Process hacker のタグ分けされている中の Processes のタグで見えてくる情報と良く似ている (図 4 参照)。Process hacker の Services、Network、Disk のタグで見えてくる情報がない。Process の一覧表示は両者とも似ていて、Process Explorer では Company Name の欄が一覧表示で見える。Process の行を選んで右クリックして Properties メニューを選ぶという操作は同じで、見えてくる情報が僅かに違う。

## 2.5 Process Monitor

Microsoft 自身が提供する Windows Sysinternals ツールの一つである。<https://docs.microsoft.com/en-us/sysinternals/downloads/procmom> から

「Download Process Monitor」と書いてあるリンクをクリックし ProcessMonitor.zip をダウンロードする。

プロセスの動作を確認できるツールであり、どのファイルに書き込んだか、どのレジストリを読み込んだか、どのような通信をしているかなどの動作をプロセスごとに確認できる。起動直後の画面は、図 5 のようになり見にくいですが、Tools のメニューの中の Process Tree... を選ぶと、ProcessExplorer のようにプロセスのツリー構造が見えてわかりやすくなる。Tools のメニューの中の File Summary... を選ぶと、時間がかかるが、全てのファイルへのアクセス記録が見えてくる。

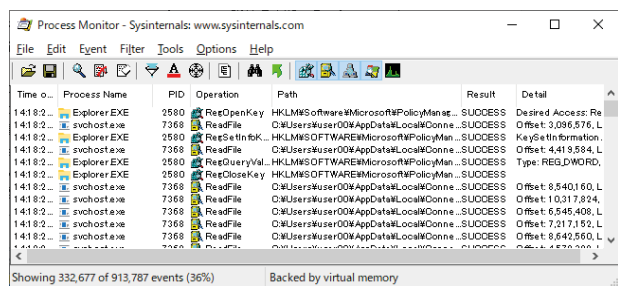


図 5 ProcessMonitor の起動後の画面

## 2.6 WinPrefetchView

[http://www.nirsoft.net/utils/win\\_prefetch\\_view.html](http://www.nirsoft.net/utils/win_prefetch_view.html) から 32bit 用には winprefetchview.zip、64bit 用には winprefetchview-x64.zip をダウンロードする。最新は version1.35 である。展開して、WinPrefetchView.exe を起動すると「こ

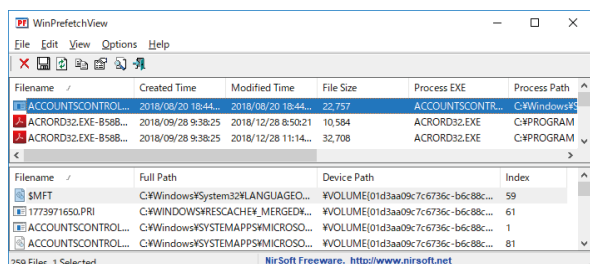


図 6 WinPrefetchView の動作画面



のアプリがデバイスに変更を加えることを許可しますか？」と尋ねられ「はい」を選んだ後に画面（図 6 参照）が表示される。

WindowsOS は、起動を高速化するために Prefetch ファイルを作成しており、起動時に読んでいます。Prefetch ファイルは `c:\Windows\Prefetch` に拡張子 `pf` のファイルとして保存されている。Prefetch ファイルを解析することで、実行したプログラムファイル名、前回実行した日時、今まで何回実行したか、プログラムが読んだファイル名を調べることができる。WinPrefetchView.exe の起動後の画面の半分より上の欄の行を右クリックすると Properties を選ぶことができ、作成日などを見ることができる。

## 2.7 UserAssist

<https://blog.didierstevens.com/programs/userassist/> の中の I posted my program (source code and binaries) here. と書いてある here の位置に UserAssist\_V2\_4\_3.zip があるが、その下に Download: UserAssist\_V2\_6\_0.zip (https) と書いてあるところがあり、そこから UserAssist\_V2\_6\_0.zip をダウンロードする。zip ファイルを展開して、32bitOS の時は、`UserAssist\bin\Release\UserAssist.exe` を実行、64bitOS の時は `UserAssist\bin\x64\Release\UserAssist.exe` を実行する。

このツールは、エクスプローラからアプリケーションを実行した履歴を表示する

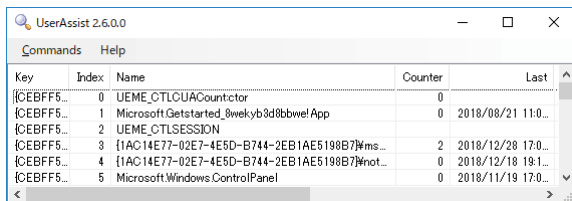


図 7 UserAssist の起動後の画面

（図 7 参照）。Last の欄をクリックして並び順が日付順になるが、日付の値が入っていない行もある。Last の欄は、感染した日時を調べる時に役に立つ。Counter の欄に起動した回数が表示されるが、Counter の値が 0 の行もある。エクスプローラから実行されたアプリケーションだけが表示され、他の方法で実行されたアプリケーションは表示されない。

## 2.8 TCP Explorer

<http://www.umechando.com/software/> から TCPXPLOR.ZIP をダウンロードし、展開して TCPXPLOR フォルダの下の Tcpxplor.exe を起動する。梅村博一氏によって開発されているソフトである。起動すると「この不明な発行元からのアプリがデバイスに変更を加えることを許可しますか？」と尋ねられ「はい」を選んだ後に設定画面が開き、デフォルトのまま OK ボタンを押す。ウィンドウが開いたら、左上の「パケットキャプチャーを開始します」のボタンを押して監視スタートする。

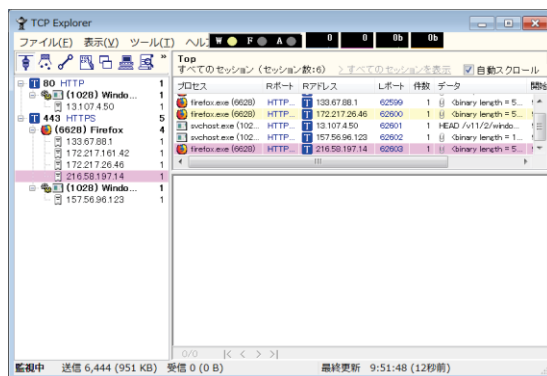


図 8 TCPEXplorer の動作画面

図 8 に TCPEXplorer の動作画面を示す。IP アドレスの箇所を右クリックすると whois で調べることができる。通信をしているプログラムと紐付して表示してくれる。このツールは、パケットキャプチャーをしながら、どのプログラムがその動作を起こ

しているのかまで調べてくれるため、怪しいプログラムを見つけるのに役に立つ。データ欄には、HTTP 通信の通信内容まで見ることができる。右上欄に現れるセッションを左の欄で選択することによって、絞り込むことができる。ずっと見ているとセッション数が上がっていくので、変化のあるプログラムを見つけるのに役に立つ。

## 2.9 TCPView

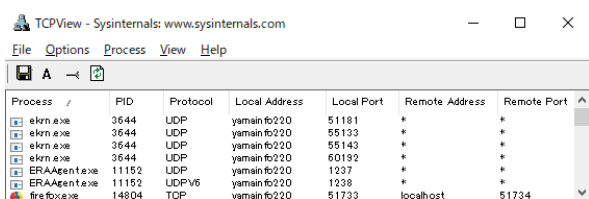


図9 TCPViewの起動後の画面

TCP Explorer と似たツールで、通信中のプロセスごとの、通信先や使用ポート番号の一覧を表示する。https://technet.microsoft.com/ja-jp/sysinternals/tcpview.aspx のサイトから TCPView.zip をダウンロードし、展開すると、TCPView のフォルダの下に Tcpview.exe が存在するので、それを起動する (図9 参照)。

TCP Explorer では、Hyper-V 利用等の計算機環境によって表示されて来ないことが起きていたが、その場合でも Microsoft 自身が提供する Windows Sysinternals のツールの一つであるため TCPView では表示がされてくる。表示行を右クリックして、ProcessProperties... を選択すると、実行ファイルの存在場所も見ることができる。

## 2.10 WireShark

コンピュータ上で流れるネットワークパケットを確認できるツールである。ネットワークにおけるトラブルシューティングや、不審な通信がないかといった解析に利用する。http://www.wireshark.org の中の

Download のボタンを押し、WindowsInstaller の 64bit 版、32bit 版が存在しているが、USB メモリにインストールして使うと便利であるため、WindowsPortableApps(32bit) を選んで USB メモリにダウンロードする。WiresharkPortable\_3.0.3.paf.exe がダウンロードされ、起動すると、インストーラが動き、USB メモリ上にファイル展開されるが、その展開された中の WiresharkPortable.exe を起動しただけでは、ネットワーク上のパケットデータをキャプチャできない。npcap ドライバをパケットキャプチャするマシンの上にインストール

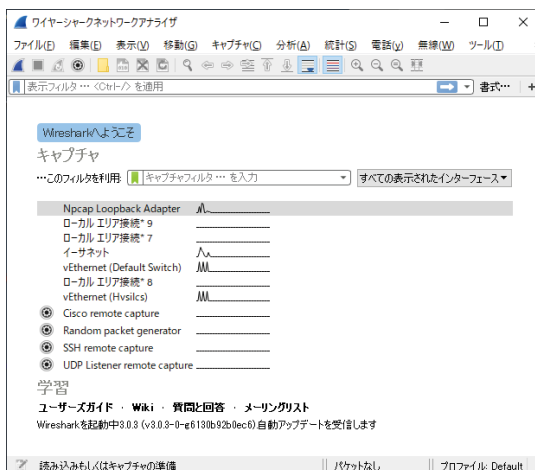


図10 npcap インストール後の Wireshark 起動後画面

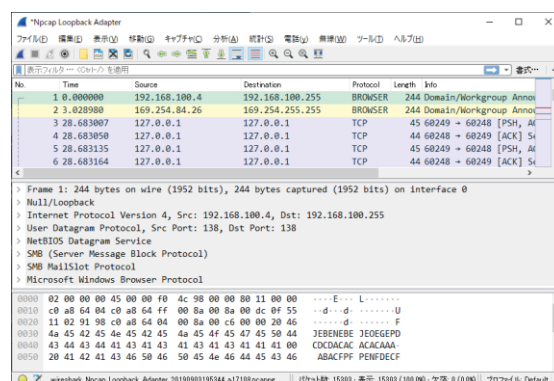


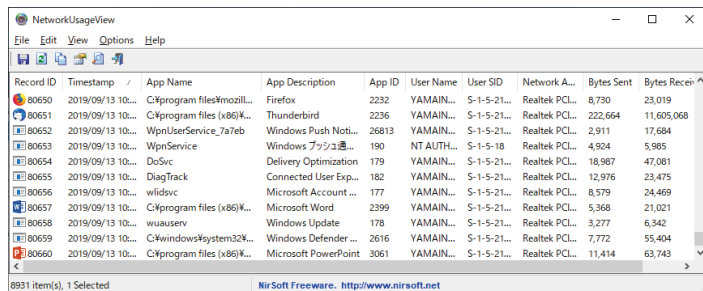
図11 Wireshark のパケットキャプチャ実行中の動作画面

ールする必要がある。npcap をインストールするには、<https://nmap.org/npcap/>の中の Npcap 0.9982 installer for Windows Vista/2008, 7/2008R2, 8/2012, 8.1/2012R2, 10/2016 (x86 and x64)をクリックし、npcap-0.9982.exe をダウンロードしてキャプチャするマシン上で実行するとインストールされる。その後、WiresharkPortable.exe を起動すると、図 10 の画面になる。Npcap Loopback Adapter というインターフェース名が表示されてきて、この状態で、左上の「パケットキャプチャを開始します」ボタンを押すと図 11 の画面になって、パケットデータが見える。TCP Explorer、TCPView はプロセス毎に見えたが、WireShark はプロセス毎でなく時間順に流れていくデータが見える。

## 2.11 NetworkUsageView

アプリケーションごとのネットワーク使用履歴を確認できるツールである。[http://www.nirsoft.net/utills/network\\_usage\\_view.html](http://www.nirsoft.net/utills/network_usage_view.html) から 32bit 版か 64bit 版かを選んで zip ファイルをダウンロードする。ファイル展開して現れる NetworkUsageView.exe ファイルを実行させると、アプリケーションがどのくらいのパケットを送受信したかを確認できる。図 12 に動作画面を示す。

Windows 8 以降の OS では、アプリケー



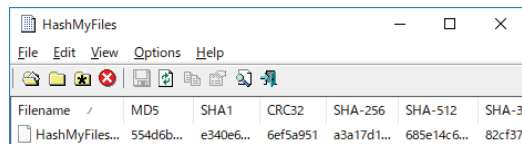
Record ID	Timestamp	App Name	App Description	App ID	User Name	User SID	Network A...	Bytes Sent	Bytes Recei...
80650	2019/09/13 10:...	C:\program files\mozill...	Firefox	2232	YAMAIN...	S-1-5-21-...	Realtek PCL...	8,730	23,019
80651	2019/09/13 10:...	C:\program files (x86)\...	Thunderbird	2236	YAMAIN...	S-1-5-21-...	Realtek PCL...	222,664	11,605,068
80652	2019/09/13 10:...	WpnUserService_7a7eb	Windows Push Noti...	26813	YAMAIN...	S-1-5-21-...	Realtek PCL...	2,911	17,684
80653	2019/09/13 10:...	WpnService	Windows アプデ通知...	190	NT AUTH...	S-1-5-18	Realtek PCL...	4,924	5,985
80654	2019/09/13 10:...	DoSvc	Delivery Optimization	179	YAMAIN...	S-1-5-21-...	Realtek PCL...	18,987	47,081
80655	2019/09/13 10:...	DiagTrack	Connected User Exp...	182	YAMAIN...	S-1-5-21-...	Realtek PCL...	12,976	23,475
80656	2019/09/13 10:...	wlidsvc	Microsoft Account ...	177	YAMAIN...	S-1-5-21-...	Realtek PCL...	8,379	24,469
80657	2019/09/13 10:...	C:\program files (x86)\...	Microsoft Word	2399	YAMAIN...	S-1-5-21-...	Realtek PCL...	5,368	21,021
80658	2019/09/13 10:...	wuauclnt	Windows Update	178	YAMAIN...	S-1-5-21-...	Realtek PCL...	3,277	6,342
80659	2019/09/13 10:...	C:\windows\system32\...	Windows Defender ...	2616	YAMAIN...	S-1-5-21-...	Realtek PCL...	7,772	55,404
80660	2019/09/13 10:...	C:\program files (x86)\...	Microsoft PowerPoint	3061	YAMAIN...	S-1-5-21-...	Realtek PCL...	11,414	63,743

図 12 NetworkUsageView の起動後の画面

ションによるネットワーク利用ログが c:\¥Windows¥System32¥sru¥SRUDB.dat というファイルに記録されている。このファイルからデータを抽出して表示しており、各アプリケーションが 1 時間ごとに何バイトのデータを送受信したかを確認できる。

## 2.12 HashMyFiles

不審なプログラムのハッシュ値を調べるツールであり、[http://www.nirsoft.net/utills/hash\\_my\\_files.html](http://www.nirsoft.net/utills/hash_my_files.html) のサイトからダウンロードして使用する。Download HashMyFiles、Download HashMyFiles for 64-bit systems、Download HashMyFiles - Non-Unicode Version (For Windows 98) の 3 つのリンクがページ中程にあり、hashmyfiles.zip (64bit 用は hashmyfiles-x64.zip、Windows98 用は hashmyfiles98.zip) をダウンロードし、解凍すると HashMyFiles.exe が現れる。



Filename	MD5	SHA1	CRC32	SHA-256	SHA-512	SHA-3
HashMyFiles...	554d6b...	e340e6...	6ef5a951	a3a17d1...	685e14c6...	82cf37

図 13 HashMyFiles の動作画面

起動して、ファイルをドラッグ&ドロップすると、MD5 / SHA1 / CRC32 / SHA-256 / SHA-512 / SHA-384 ハッシュ値が計算されて表示される (図 13 参照)。フォルダをドラッグ&ドロップすると、そのフォルダ内の全ファイルについてそれぞれ計算が行われる。行を選択し、右クリックして Open In VirusTotal Web Site のメニューを選ぶと、VirusTotal を使って危険なファイルかどうかを調べることができる。

ファイルの中に機密情報が



入っているかもしれないファイルの場合は、VirusTotal にファイル自身を入力せず、ファイルのハッシュ値を入力して調べないと機密情報が洩れる恐れがある。そのため、HashMyFiles は、SHA-256 等のファイルのハッシュ値を求めるために使われる。また、ハッシュ値を併記している Web サイトに書かれているハッシュ値と算出したハッシュ値が同じかを調べて、インターネットなどでダウンロードしたファイルが正常かどうか、改竄されていないかを調べるのにも使われる。 <https://blog.halpas.com/archives/6562> <sup>[2]</sup>等にも使い方が書かれている。

## 2.13 Hybrid Analysis

怪しいファイルをアップロードすると、サンドボックス内で実行し、実行結果をレポート表示してくれるサイトである。 <https://www.hybrid-analysis.com/> のページ (図 14 参照) の中ほどに、ファイルをドラッグ&ドロップで落としてアップロードさせる領域がある。 <https://www.falcon-sandbox.com/> <sup>[3]</sup> の表によると、無料で調べてくれるのは、1 か月に 30 個までで、サンドボックスで調べる対応 OS も、

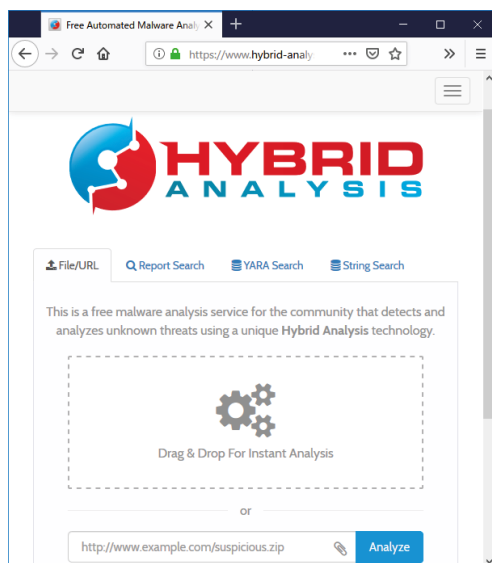


図 14 Hybrid Analysis のサイト画面

Windows7 (32/64) と Ubuntu (64) に限られている。最大アップロードサイズが 100MB までの制限もある。

アップロードすると、「Do not submit my sample to unaffiliated third parties」のチェックボックスが現れ、第 3 者に検査ファイルを送っていいかを選べ、「Allow community members to access sample」のチェックボックスでコミュニティメンバーに送っていいかも選べるようになっている。「I consent to the Terms & Conditions and Data Protection Policy.」にチェックを入れて、「私はロボットではありません」にチェックを入れてから Continue ボタンを押す。その後、Generate Public Report ボタンを押すと調査結果が表示されてくる。

## 2.14 urlQuery

URL を入力して危険なサイトであるかを調べてくれるサイトである。 <https://urlquery.net> のページ (図 15 参照) の上部に URL を入力する欄があり、そこに URL を入力して Go ボタンを押すと、調査を開始し、Processing...が表示される。数分掛かって調べられ、No alerts detected と出れば問題はない。JavaScript で動く部分や外部サーバとの連携も調べられる。

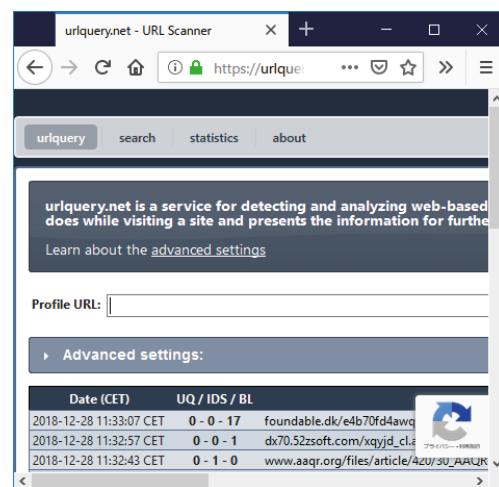


図 15 urlQuery のサイト画面



図 16 Cymon のサイト画面

## 2.15 Cymon

マルウェア、フィッシングサイト、ボットネットの追跡サイトである。https://cymon.io/のページ（図 16 参照）に怪しいホストの IP アドレスかドメイン、またはファイルのハッシュ値を入力し、Search ボタンを押すと、ブラックリストのデータベースの中に登録されていないかを調べることができる。Not Found と表示されれば問題はない。

## 3. ツールの利用方法

USB メモリ内に 2 章で挙げたツールをダウンロードし、圧縮ファイルは展開状態にして保存しておく。パソコンの挙動が怪しいと思った時は、まず TCP Explorer を起動し、通信しているプログラムを見つける。TCP Explorer は、「パケットキャプチャーを開始します」のボタン接続後に表示が見えてくるまでに時間が掛かる。Hyper-V を利用している場合等、動かない場合もある。動かない場合は、TCPView を利用する。怪しいプログラムは、外部と通信しようとする事が多いため、まず外部と通信しているプログラムを探るのが良い。

その後、Process Hacker を起動し、現在稼働中のプログラムを見る。Process Hacker は、多くのプロセスが見えてくるので、View メニューの中の「Hide Signed

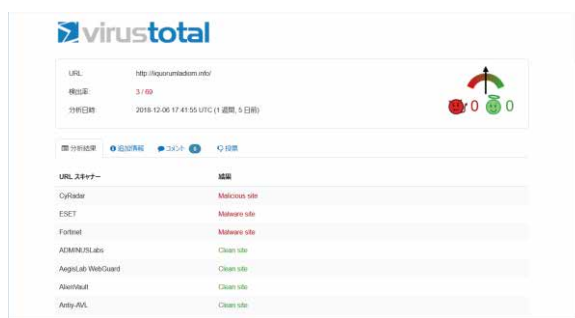


図 17 VirusTotal の確認結果

processes」にチェックを入れたりして、怪しい候補を絞る。怪しいプロセスの行を右クリックし、「Send To」を選び、virustotal.com を選ぶことで、マルウェアであるかのチェックをする。図 17 に表示されてくる画面例を示す。1 個ずつチェックするのが面倒な場合、Process Explorer の Option のメニューの Virus.com のサブメニューの CheckVirusTotal.com を選ぶと一覧で VirusTotal による検査結果が表示されてくる。図 18 にその画面例を示す。

また、Process Explorer では Company Name の欄が一覧表示で見えるので、その欄が空欄であるプロセスは怪しいと注目できる。さらに、Process Explorer の Options のメニューの中の Verify Image Signature にチェックを入れて、Verified Signer の欄を見て、(Verified) と表示されていないプロセスは、マルウェアの可能性が高いと推定できる。このデジタル署名の有無は、署名無しが全てマルウェアであると断定はできないが、多くのマルウェアは署名無しであることが多いため、注目する時のヒントになる。

Process Explorer ではプロセスが色別表示されるが、Options のメニューの Configure Colors... を選ぶと表示される Color Selection 表の中の紫色の Packed Images に該当するプロセスは、怪しいソフトであると推測できる。この Packed Images とは、パッキングと呼ばれ、プログラムが

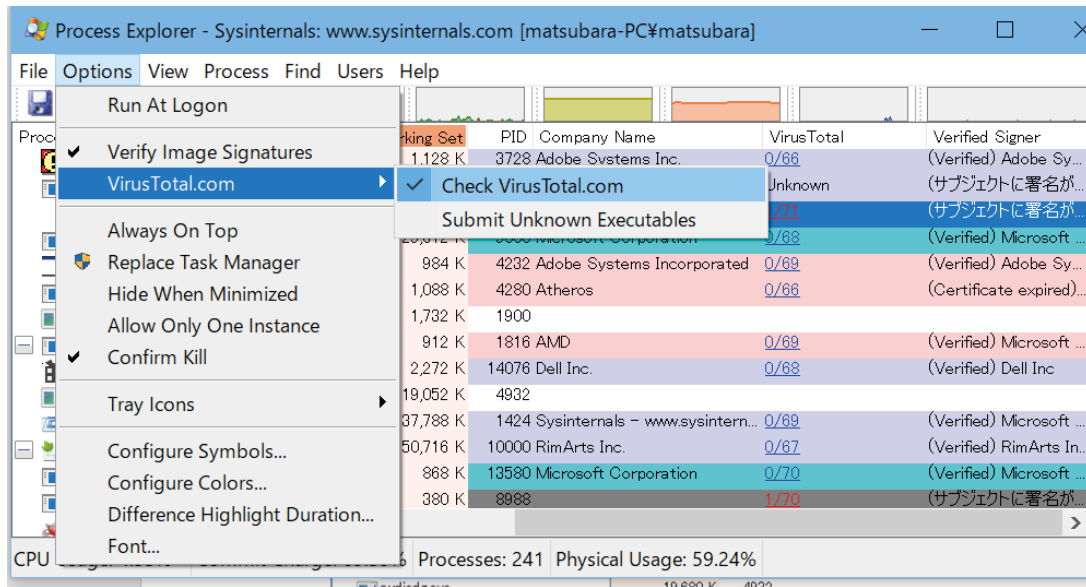


図 18 ProsessExplorer を実行し、VirusTotal にチェックを入れた画面

実行可能状態のまま圧縮・暗号化されていることを示している。正規のソフトウェアでもこのパッキングされているものがあるが、怪しいソフトは検知・解析を困難にするためにプログラムをパッキングすることが多い。

怪しいプロセスが多いと感じる場合は、Autoruns を起動し、右の方に表示される「Virus Total」の欄の数字を調べる。Options のメニューの「Hyde VirusTotal Clean Entries」にチェックを入れて、「Virus Total」の欄の値が 0 の行を表示させないようにする。このようにすることで表示されるプログラムの数がかなり減る。それでも「Virus Total」の欄の値が 1 のプログラムは多く存在しており、その中で 1 より大きいプログラムがあった場合は明らか

かに怪しいプログラムである。

なお、Virus Total の利用には、アップロードされたファイルは、Virus Total のサイトへファイル自身が取得されていることに注意が必要である。

#### 4. 本学での状況

本学では、Firewall のログ等から、危険なデータの動きを検知すると、その PC を突き止めて確認をする。9 割ぐらいの確率で、最新版のウイルス対策ソフトがインストールされてないことが多い。最新版のウイルス対策ソフト(Eset Endpoint Security)をインストールして、全スキャンをかけるとウイルスが検知することが出来る。(図 19 参照)

ウイルス対策ソフトで検知できなかった場合、2 章で紹介したツールを利用して、不審なプロセスを発見する。ここで該当のと思われるプロセスを発見したら、該当プロセスを殺す(図 20 参照)。その後、FireWall ログ等で状況が改善されたことを確認する。

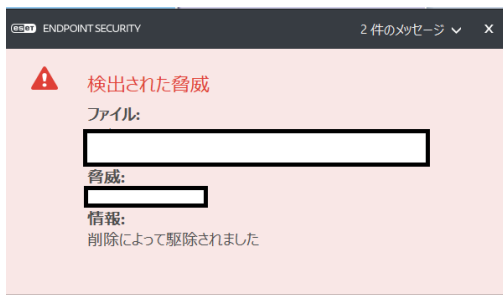


図 19 ESET で検出できた時の画面

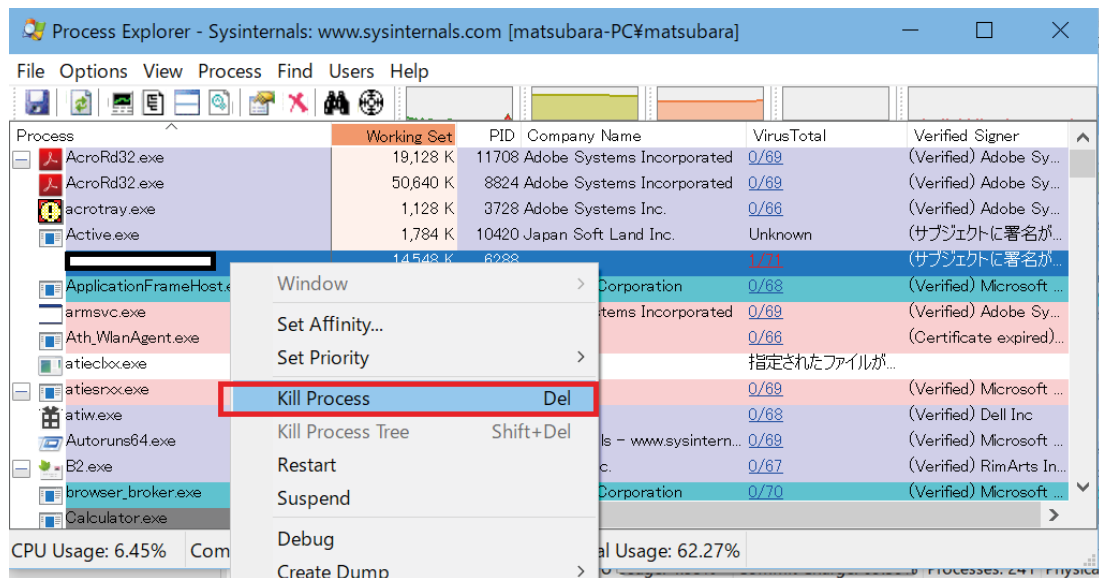


図 20 プロセスを殺す画面

## 5. まとめ

明らかにウイルスが入り込んでいると指摘された場合には、被害最小にするために、ネットワーク接続は切り離したいところである。一方で、入り込んでいるウイルスの特定をしたいし、できれば感染経路、感染日時を特定したいところである。

紹介したツールは、ウイルスのファイルを見つけ出し、感染日時のヒントを与えてくれるツールである。感染経路を特定するには、OutlookAttachView<sup>[4]</sup>や IECashView<sup>[5]</sup>などの別のツールが必要である。

また、ウイルスの入り込んだパソコンの被害状況を解析したり攻撃の痕跡を確認するためには、パソコンをデータ保全する必要があり、そのためのツールが存在する。メモリイメージを保存する DumpIt<sup>[6]</sup>、ハードディスクのストレージイメージとメモリイメージを保存する FTK Imager Lite<sup>[7]</sup>、Prefetch ファイルや NTFS 情報など解析に必要なデータを取得する CDIR Collector<sup>[8]</sup>がそのためのツールである。

## 参考文献

- [1] ウイルスチェックのつもりで情報漏えい？ VirusTotal の使い方に注意, <http://www.itmedia.co.jp/enterprise/articles/1603/14/news104.html> (2019年9月現在)
- [2] 【MD5/SHA1】簡単に使えて高性能なハッシュ計算ソフト「HashMyFiles」, <https://blog.halpas.com/archives/6562> (2019年9月現在)
- [3] Falcon Sandbox Services and Products, <https://www.falcon-sandbox.com/> (2019年9月現在)
- [4] OutlookAttachView v3.26 - View/Extract/Save Outlook Attachments, [https://www.nirsoft.net/utils/outlook\\_attachment.html](https://www.nirsoft.net/utils/outlook_attachment.html) (2019年9月現在)
- [5] IECacheView v1.58 - Internet Explorer Cache Viewer, [http://www.nirsoft.net/utils/ie\\_cache\\_viewer.html](http://www.nirsoft.net/utils/ie_cache_viewer.html) (2019年9月現在)
- [6] DumpIt ダウンロードサイト, <https://my.comae.io/> (2019年9月現在)
- [7] FTK Imager Lite ダウンロードサイト,

<https://accessdata.com/product-downloads/> (2019年9月現在)

[8] CDIR Collector ダウンロードサイト,  
<https://www.cyberdefense.jp/products/cdir.html/> (2019年9月現在)