



第1日目

情報セキュリティ担当者のためのインシデント対応入門

マルウェア感染対応 フォレンジック基礎編

2014年12月
セクタンラボ勉強会

講座の全体構成

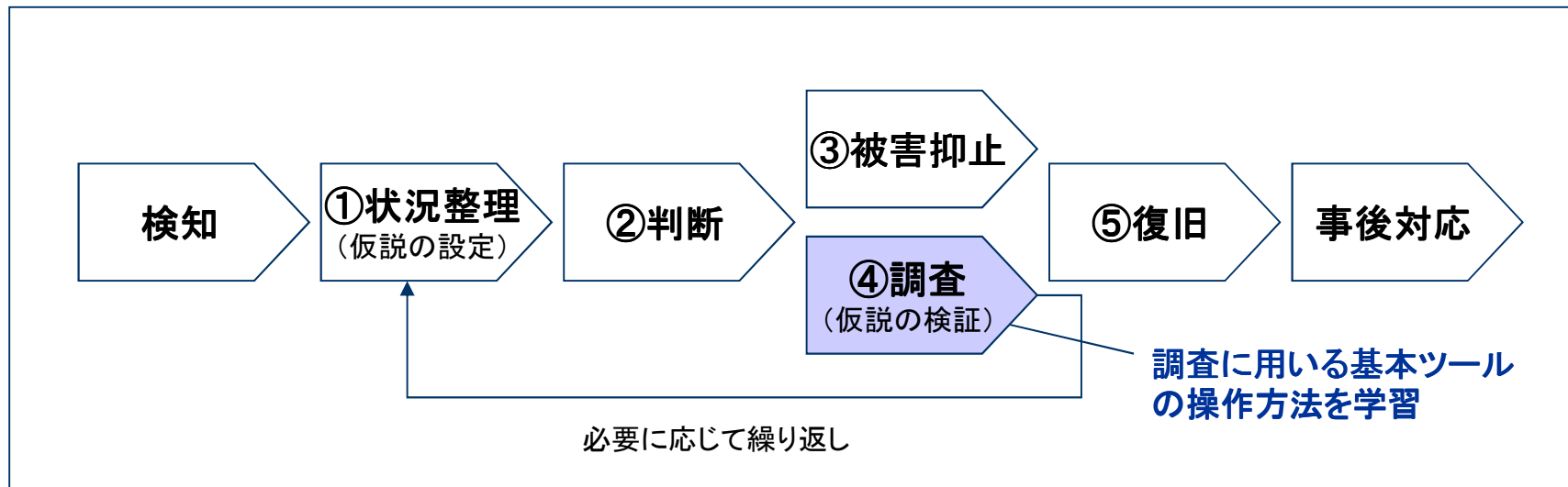
本日

講座名称	主な学習内容
フォレンジック基礎編	<ul style="list-style-type: none">・感染PCの調査に用いる基本ツールの操作方法
WEB型マルウェア編	<ul style="list-style-type: none">・感染源WEBサイトの特定・遮断方法・感染PCに潜伏しているマルウェア検体の取得方法
メール型マルウェア編	<ul style="list-style-type: none">・特定の不審メールの遮断方法・特定の不審メール受信者の把握方法・感染PCに潜伏しているマルウェア検体の取得方法
模擬訓練	<ul style="list-style-type: none">・机上での模擬訓練により、マルウェア感染状況の把握、ならびに被害拡大防止対応の判断と指示を体験

本日の学習内容

- インシデント対応では、状況整理フェーズで事実と推測を整理し、発生している事象とリスクの「仮説」を設定します。
- しかし、対応の初期段階では、情報の不足や輻輳が発生しやすく、仮説には、推測が含まれることが多いため、必要に応じて、フォレンジック技術や、マルウェア解析技術を活用し、仮説の検証を行います。
- 本講座では、マルウェア感染PCの調査に用いる、基本的なフォレンジックツールの操作方法を学習します。

◆ インシデント対応の基本手順



本日の次第

第1章 証拠保全

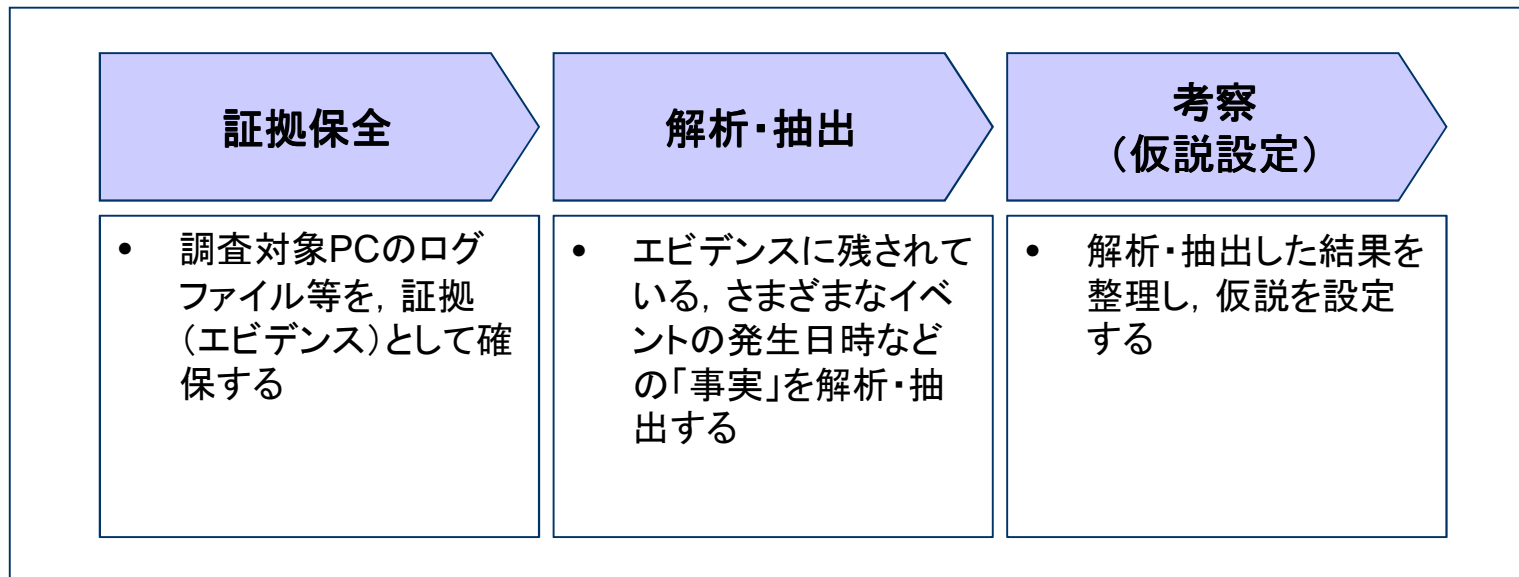
第2章 解析・抽出

第3章 考察

フォレンジックとは

- 情報セキュリティにおける、フォレンジック(Forensics)とは、インシデントが発生したコンピュータの解析を行い、いつ、何が起きたのかを調査する科学捜査手法のことです。
 - デジタル鑑識と表現される場合もあります。
 - 本勉強会では、フォレンジックを、「証拠保全」、「解析・抽出」、「考察(仮説設定)」の一連の対応と定義します。

◆ フォレンジックの基本手順





第1章 証拠保全

証拠保全の概要

- 証拠保全とは、インシデントが発生したコンピュータなどのデータを、証拠(エビデンス)として確保することです。
- 調査結果をもとに、法的対応を行う可能性がある場合、または社内規程に基づき従業員を処罰する可能性がある場合は、法的な証拠性の確保を意識した慎重な対応が必要となります。
 - デジタルデータは改竄が容易であるため、不用意に取り扱くと法的な証拠性を失う可能性があります。(調査対象PCの電源をONにし、OSを起動しただけで、多くの情報が改変される)
- しかし、一般企業の情報セキュリティ担当者として対応にあたる案件では、技術的制約、時間的制約があり、また、マルウェア感染対応の社内報告においては、法的な証拠性を要求されることが少ないため、簡易的な証拠保全を選択することも多いです。

事件現場における「鑑識官」になったつもりで対応しましょう

(参考) 調査対象PCのOS起動による影響

- 調査対象PCの電源をONにし、OS起動をすると、さまざまな情報が変更されます。
 - － 事件現場を土足で踏み荒らし、証拠品に自分の指紋を残すようなもの。

◆ OS起動による影響

影響	問題点
タイムスタンプの更新	● ファイルのタイムスタンプが更新され、時系列の調査に支障が出る可能性がある。
ログファイル等の上書き	● ログファイル、レジストリなどの内容が、OS起動時の情報で上書きされてしまい、解析に支障が出る可能性がある。
未使用領域の上書き	● NTFS, FATなどのファイルシステムでは、通常操作でファイルを削除しても、未使用領域のステータスに変更されるだけで、ディスク上にあるファイルの内容は、直ちには削除されない。 ● しかし、OS起動時のファイル更新処理の際に、未使用領域が上書きされ、削除済みファイルの復元に支障が出る可能性がある。
マルウェアの活動	● 調査対象PCにマルウェアが感染している場合、OS起動により、活動を開始する。マルウェアの種類によっては、ネットワークからの切断を検知すると、自動的に自身を削除し、証拠隠滅を図るものもある。
法的な証拠性の低下	● 調査員による証拠の改変が疑われ、法的な証拠性が低下する可能性がある。

証拠保全すべきエビデンス

- 取得すべきエビデンスは、想定シナリオにより異なります。下表に記載したデータは、ほとんどの事案で必要となるため、可能な限り取得するよう努めます。

◆ 証拠保全すべきエビデンス

分類	ファイル名
マルウェアの検体	<ul style="list-style-type: none"> マルウェア本体（駆除されていない場合）、およびマルウェアが作成したファイルが明確である場合は、対応初期の段階で、検体として取得しておく。
ファイルシステム	<ul style="list-style-type: none"> \$MFT（NTFSのファイルエントリ管理テーブル） [保存場所] 各ドライブのルートディレクトリ(OS標準ツールでは表示・取得不可)
レジストリファイル	<ul style="list-style-type: none"> SYSTEM , SOFTWARE , SAM , SECURITY [保存場所] C:¥WINDOWS¥system32¥config¥ NTUSER.DAT [保存場所 XP] C:¥Documents and Settings¥【ユーザー名】¥ [保存場所 7] C:¥Users¥【ユーザー名】¥
イベントログ	<ul style="list-style-type: none"> SysEvent.evtx , SecEvent.evtx , AppEvent.evtx など [保存場所 XP] C:¥WINDOWS¥system32¥config¥ [保存場所 7] C:¥Windows¥System32¥winevt¥Logs¥
その他の アーチファクト*1	<ul style="list-style-type: none"> Prefetchファイル一式 -C:¥WINDOWS¥Prefetchフォルダ内に格納されている全てのファイルを取得する。

*1 OSやアプリケーションが作成するファイルのこと。レジストリなどの設定ファイルだけでなく、ショートカット(LNKファイル)や、ごみ箱などの特殊フォルダ、システムの復元機能により、自動取得されるバックアップなども含まれる。

証拠保全の方法

- エビデンスを取得する際は、可能な限り、証拠性を損ねない方法で実施します。
- やむを得ず、調査対象PCのOSを起動する必要がある場合は、対応責任者に証拠性が損なわれる可能性を報告し、リスク受容の判断を下したうえで作業を実施します。

◆ 証拠保全の方法


分類	概要
ディスク複製	<ul style="list-style-type: none"> • 調査対象PCから取り出したHDDを、ディスク複製装置を用いて、他のHDDに複製する。(専門家の作業における、標準的な証拠保全方法) • 解析作業は、複製したHDDに対して実施し、原本HDDは厳重に保管する。
ディスクイメージ取得	[方法1] <ul style="list-style-type: none"> • 調査対象PCを、フォレンジック用Live Linux CD等で起動し、HDDのディスクイメージを取得する。解析作業は、ディスクイメージに対して実施する。
	[方法2] <ul style="list-style-type: none"> • 調査対象PCのOS(Windows)を起動し、フォレンジックツールを利用して、HDDのディスクイメージを作成する。
証拠ファイル取得	<ul style="list-style-type: none"> • 調査対象PCのOS(Windows)を起動し、解析に必要なファイルのみ取得する。
調査対象HDDの直接解析	<ul style="list-style-type: none"> • 調査対象PCから取り出したHDDを、書き込み防止装置を介して、フォレンジック用PCに接続し、直接解析する。 • 本手法により、簡易解析を実施した後で、ディスク複製や、証拠ファイル取得などの対応を実施する場合もある。

証拠保全方法のメリット・デメリット

分類	メリット(○)とデメリット(×)
ディスク複製	○原本HDDに改変を加えないため、証拠性を確保しやすい。 ×HDDの複製に時間がかかる。
ディスクイメージ取得	[方法1] Linux Live CD ○原本HDDに改変を加えないため、証拠性を確保しやすい。 ○HDDが取り出せない場合でも対応できる。 ×ディスクイメージ作成に時間がかかる。
	[方法2] Windows起動 ○不慣れな調査員でも容易に作業できる。 ○OSの起動により、ディスク暗号化が自動的に回避される。 ×OS起動により、原本に改変を加えることとなる。 ×OS起動により、感染したマルウェアが活動する。 ×ディスクイメージ作成に時間がかかる。
証拠ファイル取得	○作業効率が高い。 ○OSの起動により、ディスク暗号化が自動的に回避される。 ×OS起動により、原本に改変を加えることとなる。 ×OS起動により、感染したマルウェアが活動する。
調査対象HDDの直接解析	○ディスク複製、ディスクイメージ取得と比較して、速やかに解析作業に着手できる。 ×解析作業時に、原本HDDを物理的に故障させるリスクがある。

ディスク複製の基本手順

- ① 調査対象PCの電源ケーブル(ノートPCはバッテリー)を取り外した上で、PCのケースを開けてHDD(原本HDD)を取り出す。
- ② 取り出した原本HDDを、ディスク複製装置を用いて、フォレンジック用のクリーンなHDD(全セクターをゼロで上書きしたものが望ましい)に複製する。
- ③ 原本HDDは、型番、シリアル番号、容量などを記録した上で、識別用ラベルを付けて厳重に保管する。

利用するツール	説明	参照情報
これdo台 PRO 	<ul style="list-style-type: none">• SATA/IDE (2.5 or 3.5 inch)に対応したディスク複製装置。• 入力と出力を間違えて接続すると、証拠を破壊することになるので要注意。	株式会社センチュリー 製品情報 http://www.century.co.jp/products/series/series-koredo/


ディスク複製のポイント

- メーカー製PC(特にノート型PC)からHDDを取り出す場合は、HDD交換方法を解説したWEBサイトを探し、事前に情報収集します。^{*1}
- HDDは精密機器であるため、静電気や強い衝撃による損傷を与えないよう、静電気防止手袋を着用し、HDDを机に置く際には、気泡緩衝材(通称ぷちぷち)を敷くなどの対策を講じます。
 - ディスク複製中は、HDDが高温になるため、気泡緩衝材は取り外したほうが無難です。
- PCケースを開ける際には、デジタルカメラで配線の接続状態などを随時記録し、現状復帰の際の確認に利用します。
 - 必要に応じて、取り外した配線にラベルを付けて、現状復帰の間違いを防止します。

*1 パソコン初心者講座 HDD交換 パソコン分解サイト <http://www.pc-master.jp/trouble/hdd-bunkai.html>

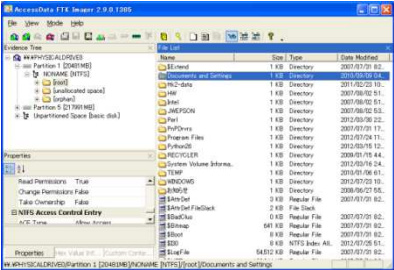
ディスクイメージ取得の基本手順 -Live Linux CD-

- ① 調査対象PCの電源をONにし、BIOS設定画面を表示する。
- ② CDブートの優先順位が、HDDよりも高くなっていることを確認する。
 - HDDのほうが優先順位が高くなっている場合は、BIOS設定を変更する。
- ③ 調査対象PCにForensic用Live Linux CDをセットした後、PCを再起動し、Live Linux CDを起動する。
- ④ 調査対象PCに、データ保管用USB-HDDを接続し、Linuxのツールを利用して、調査対象PCのディスクイメージを、データ保管用USB-HDDに作成する。

利用するツール	説明	参照情報
DEFT Linux 	<ul style="list-style-type: none"> • オープンソースのForensic用Linux Live CD。 • GUI操作のディスクイメージ取得ツール「Guymager」が導入されており、Linuxが苦手な調査員でも比較的容易に利用できる。 • オープンソースの各種フォレンジックツールが導入されており、さまざまな調査に利用できる。 • また、CDにはWindows用の調査ツールも格納されており、Windowsが起動しているPCにCDを接続して利用することもできる。 	DEFT Linux http://www.deflinux.net/ Guymager (ディスクイメージ取得ツール) http://guymager.sourceforge.net/

ディスクイメージ取得の基本手順 -Windows用ツール-

- ① 調査対象PCの電源をONにし、Windowsを起動する。
- ② 調査対象PCに、ディスクイメージ取得ツールを格納した、データ保管用USB-HDDを接続する。
- ③ ディスクイメージ取得ツールを利用して、調査対象PCのディスクイメージを、データ保管用USB-HDDに作成する。

利用するツール	説明	参照情報
<p>FTK Image Lite (Windows)</p> 	<ul style="list-style-type: none"> • Access Data社の簡易フォレンジックツール。(GUIツール) • ディスクイメージ作成機能に加え、ファイル取得機能、ディスクの簡易閲覧機能も有する。 • 本ツールは、USBメモリに格納して利用できる。 	<p>Access Data http://accessdata.com/ FTK Imagerのマニュアル(英語) http://accessdata.com/downloads/current_releases/imager/FTKImager_UserGuide.pdf</p>

FTK Imager Lite

- FTK Imager Liteは、OSを経由せず、解析対象のディスクを直接解析するGUIの簡易フォレンジックツールです。
- OSを経由しないため、ACLやファイルロックの影響を受けずにエビデンスの取得、閲覧を行うことができます。また、メモリイメージの取得もできます。
- 本ツールは、USBメモリにインストールできるため、現地作業で利用しやすいです。
- なお、タイムスタンプはUTC*1表示のため、日本時間に換算するには+9時間します。

The screenshot shows the FTK Imager interface with four red boxes and arrows pointing to specific features:

- Evidence Tree:** A tree view on the left showing the disk structure. A red box highlights it with the text: "Evidence Tree" and "物理ディスクやディスクイメージを、複数登録できる。"
- File List:** A table on the right showing files and directories. A red box highlights it with the text: "File List" and "Evidence Treeで選択したエビデンスに格納されているディレクトリとファイルを表示する。"
- Properties:** A panel at the bottom left showing details for the selected file. A red box highlights it with the text: "Properties" and "選択したオブジェクトの詳細情報が表示される。"
- Preview:** A panel at the bottom right showing a hex dump of the selected file. A red box highlights it with the text: "Preview" and "File Listで選択したオブジェクトの内容をプリビュー表示する。(Hex, またはTextで表示することも可能)"

Name	Size	Type	Date Modified
Users	1	Directory	2012/10/30 ...
Windows	1	Directory	2014/07/23 ...
WORK	1	Directory	2014/07/29 ...
\$AttrDef	3	Regular File	2012/10/22 ...
\$BadClus	0	Regular File	2012/10/22 ...
\$Bitmap	6,797	Regular File	2012/10/22 ...
\$Boot	8	Regular File	2012/10/22 ...
\$I30	8	NTFS Index ...	2014/07/29 ...
\$LogFile	65,536	Regular File	2012/10/22 ...
\$MFT	241,664	Regular File	2012/10/22 ...
\$MFTMirr	4	Regular File	2012/10/22 ...
\$Secure	1	Regular File	2012/10/22 ...
\$TXF_DATA	1	NTFS Logge...	2014/07/29 ...

Name	File Class	File Size	Physical Size	Start Cluster
\$MFT	Regular File	247,463,936	247,463,936	786,432

*1 協定世界時のこと。UTCに+9時間することで日本時間に換算できる。

[実習01] FTK Imager

- 実習用PCで、FTK Imagerの操作方法を確認します。
(実習では通常版FTK Imagerを利用しますが、Lite版も操作方法は同じです)

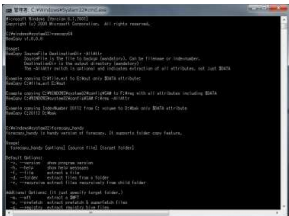
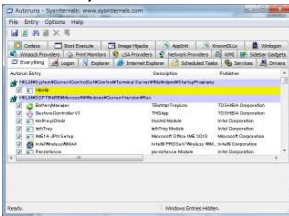
Mission01 イメージファイル内のファイル取得

Mission02 イメージファイル内の削除済ファイル復元

Mission03 PC内蔵HDDのディスクイメージ取得

証拠ファイル取得の基本手順 -Windows用ツール-

- ① 調査対象PCの電源をONにし、Windowsを起動する。
- ② 調査対象PCに、証拠ファイル取得ツールを格納したUSBメモリを接続する。
- ③ 証拠ファイル取得ツールを利用して、調査対象PCのファイルやレジストリ等を、USBメモリにコピーする。

利用するツール	説明	参照情報
FTK Imager Lite	<ul style="list-style-type: none"> • 前述のとおり 	
RawCopy ForeCopy_handy (Windows) 	<ul style="list-style-type: none"> • コマンドライン版の証拠ファイル取得ツール。OSの制限を回避し、任意のファイルをコピーすることができる。 • 事前にバッチファイルを用意しておくことで、迅速に証拠ファイルを取得することができる。 	Mft2csv(Rawcopy) https://code.google.com/p/mft2csv/downloads/list proneer(forecopy_handy) https://code.google.com/p/proneer/downloads/list
Autoruns (Windows) 	<ul style="list-style-type: none"> • 起動時に自動実行するプログラムの一覧を表示する。(GUIツール) • 実行結果をファイルに保存することができる。保存したデータと現在の一覧を比較し、変更点を表示することができる。 	Windows Sysinternals http://technet.microsoft.com/ja-jp/sysinternals/b963902.aspx

[実習02] Autoruns

- 実習用PCで, Autorunsの操作方法を確認します。

Mission01 実習用PCの自動実行プログラムの確認/実行結果の保存

Mission02 実行結果の読み込み



第2章 解析・抽出

解析・抽出の概要

- 証拠保全で取得したエビデンスを解析し、いつ、何が起きたのかを抽出します。
 - ログの種類や利用するツールによって、タイムゾーンの取扱いが異なるため、「日本時間」、「UTC」を取り違えないよう注意が必要です。

◆ 解析対象

分類	主な作業項目	確認できる情報の例
ファイルシステム	<ul style="list-style-type: none"> • ファイル/ディレクトリのタイムスタンプの確認 • 削除済みファイルの復元 	<ul style="list-style-type: none"> • マルウェアの感染日時 • マルウェアに操作されたファイルと操作日時(作成, 更新, 削除 など)
レジストリ	<ul style="list-style-type: none"> • レジストリの設定が変更がされた日時とその内容 	<ul style="list-style-type: none"> • マルウェアの感染有無と感染日時(OS起動時の自動実行の有無) • USBメモリの接続履歴
イベントログ	<ul style="list-style-type: none"> • PCの電源ON/OFFの日時の確認 • ログオン失敗の履歴の確認 	<ul style="list-style-type: none"> • PCの稼働状況 • 不審なログオンの有無
その他 アーチファクト*1	<ul style="list-style-type: none"> • OSやアプリケーションが作成するファイルに記録されるさまざまな痕跡の確認 	<ul style="list-style-type: none"> • インターネットの接続履歴

*1 OSやアプリケーションが作成するファイルのこと。レジストリなどの設定ファイルだけでなく、ショートカット(LNKファイル)や、ごみ箱などの特殊フォルダ、システムの復元機能により、自動取得されるバックアップなども含まれる。

主な解析ツール

- ここでは、解析の基本である、タイムライン解析ツール、レジストリ解析ツール、ならびにWindowsアーチファクト解析ツールを紹介します。

◆ 主な解析ツール

分類	ツールの名称	概要
タイムライン 解析	Log2timeline.pl	Log2timeline https://code.google.com/p/log2timeline/ \$MFT, レジストリ, イベントログなどを解析し, タイムライン, またはbodyファイル形式に出力するスクリプト。
	mactime.pl (The Sleuth Kitに同梱)	The Sleuth Kit http://www.sleuthkit.org/index.php bodyファイル形式を, タイムラインに変換するスクリプト。
レジストリ解析	Registry Viewer	Access Data http://accessdata.com/ 証拠保全したレジストリファイルを解析する。レジストリキーの最終更新時刻の表示, 対応するデータの解析結果の表示機能などを有する。(GUIツール)
Windows アーチファクト解析	Windows File Analyzer <div style="border: 1px solid black; padding: 2px; display: inline-block;">本日は説明を割愛</div>	MiTeC http://www.mitec.cz/index.html Windowsの各種ファイルを解析する。(GUIツール)

タイムライン解析の概要

- タイムライン解析は、エビデンスの各タイムスタンプ(作成, 更新, アクセス, 属性変更)を分解し、時系列に整理した上で、いつ、何が起きたのかを確認する調査手法です。

◆ 一般的なファイル一覧

ファイル名	更新日	作成日	アクセス日
AAA.txt	2012/01/01	2012/01/01	2012/05/01
BBB.xls	2012/03/15	2012/05/22	2012/07/01
CCC.doc	2011/09/04	2011/03/04	2011/09/04
...			

発生した事象を時系列に確認するためには、各タイムスタンプごとにソートをしなが、整理していく必要がある。(データ量が多いと大変)

◆ タイムラインに変換した結果

ファイル名	日時	タイプ
CCC.doc	2011/03/04	..b
CCC.doc	2011/09/04	m.a
AAA.txt	2012/01/01	m.b
BBB.xls	2012/03/15	m..
AAA.txt	2012/05/01	.a.
BBB.xls	2012/05/22	..b
BBB.xls	2012/07/01	.a.
...		

タイムラインは、タイムスタンプが分解され、時系列に整理されているため、「いつ」、何が起きたのか分かりやすい。

「タイプ」は、その日時にファイルに加えられた変更の種類を表している。

タイプの分類

m: 更新日時 (modify)
 a: アクセス日時 (access)
 c: 属性更新日時 (change)
 b: 作成日時 (born)

ファイルのタイムスタンプ

- タイムライン解析の実施にあたっては、ファイルのタイムスタンプが更新される条件を理解する必要があります。

◆ ファイルのタイムスタンプが更新される条件(NTFS)

ファイル操作	ファイルのタイムスタンプ			
	更新日 (Modification Time)	作成日時 (Birth/Born Time)	アクセス日時*1 (Access Time)	属性変更日時 (Change Time)
ファイル作成	○	○	○	○
ファイル内容にアクセス	—	—	—	—
ファイル内容の更新	○	—	—	○
プロパティ変更	—	—	—	○
ファイル名変更	—	—	—	○
ファイル移動 (同一ファイルシステム内)	—	—	—	—
ファイル削除	—	—	—	—
タイムスタンプ変更	(指定日時に変更)	(指定日時に変更)	(指定日時に変更)	○

*1 Windows Vista/Windows Server 2008以降のOSでは、標準設定ではアクセス日時の更新機能が無効化されている。

Log2timeline (1)

- Log2timelineは、\$MFT、レジストリ、イベントログなどを解析し、CSV形式またはbody形式(後述)でタイムラインを出力するPerlスクリプトです。
- \$MFTの解析では、「-d」オプションでNTFSのFilename属性*1のタイムスタンプも表示されるため、マルウェアにより改竄されたタイムスタンプの調査に活用できます。

•書式:

```
Log2timeline.pl -f [エビデンス形式] -o [出力形式] -w [出力ファイル名] -d  
-m [ファイル名の先頭に付加する文字] -z [タイムゾーン] [エビデンスファイル名]
```

[補足1] -f/-o/-z は、「list」オプションをつけることで、対応形式を一覧表示できる

[補足2] -w で指定したファイルが既に存在する場合、末尾に追記される

[補足3] -d オプションを加えると、詳細(Detail)な解析結果が出力されるが、データ量が大きくなる

•使用例1: \$MFTの解析結果をCSV形式で出力

```
C:¥> log2timeline.pl -f mft -o csv -w timeline.txt -d -m C: -z Japan $MFT
```

•使用例2: SYSTEMレジストリの解析結果をCSV形式で出力

```
C:¥> log2timeline.pl -f system -o csv -w timeline.txt -d -z Japan system
```

*1 Explorerでは、NTFSのStandard Information(SI)属性のタイムスタンプを表示している。これは、Windows標準APIで容易に改竄が可能である。NTFSでは、SI属性とセットで、ファイル名などを保持するFile Name(FN)属性も作成される。FN属性のタイムスタンプは、改竄が容易ではないため、調査の参考材料とすることができる。

Log2timeline (2)

- Log2timelineでCSV形式で出力したファイルは、時系列でソートされていないため、Excelなどのツールで別途ソートする必要があります。
- なお、Excel 2010は、約100万行までしか閲覧できない。大きなタイムラインを閲覧する場合は、Log2timelineでbody形式^{*1}(-f mactime)として出力したものを、mactimeでタイムラインに変換し、テキストエディタなどで閲覧します。
(mactimeではソート処理も実施される)
 - Log2timelineの出力は、文字コードがUTF-8のため、Excel 2010でそのまま開くと日本語が文字化けします。ファイルを開く際に、文字コードをUTF-8に指定する必要があります。
(事前に、文字コードをShift-JISに変換しておく方法もあります)

•書式:

```
mactime.pl -b [bodyファイル] -z [タイムゾーン] -d -m
```

[補足1] 解析結果は標準出力に表示されるため、ファイルにリダイレクトする

•使用例1: \$MFTからタイムライン作成

```
C:¥> log2timeline.pl -f mft -o mactime -w body.txt -d -m C: -z Japan $MFT
```

```
C:¥> mactime.pl -b body.txt -z Japan -d -m > timeline.txt
```

*1 body形式は、The Coroner's Toolkit(TCT)という古いフォレンジックツールで利用されていたタイムライン作成用の中間ファイルであり、その後登場したフォレンジックツールでも採用された。bodyファイルをmactimeなどのツールでタイムラインに加工する。

[実習03] Log2timeline

- 実習用PCで、Log2timelineによるタイムライン作成方法を確認します。

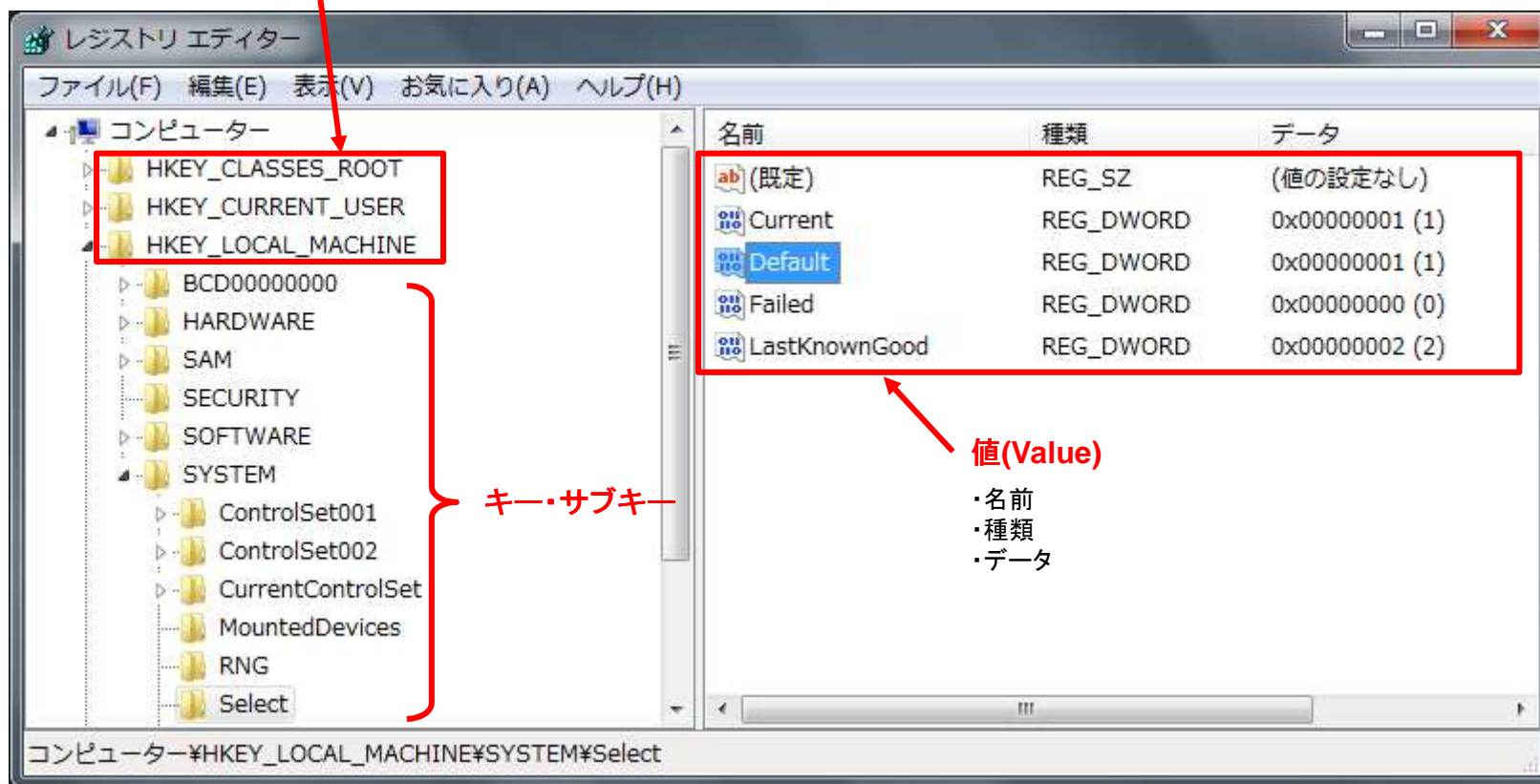
Mission01 タイムライン作成

Mission02 Excelによるタイムライン閲覧

レジストリの概要

- レジストリとは、Windowsのシステム設定およびアプリケーション設定を記録するデータベースです。
- レジストリエディタを起動すると、レジストリの論理構造を確認できます。

レジストリハイブ(最上位キーの名称)



レジストリファイル(1)

- レジストリは、複数のレジストリファイルとして保管されています。
- OS起動時に各ファイルが読み込まれ、レジストリハイブとして構成されます。また、OS終了時・アプリケーション終了時に変更内容がファイルに保存されます。

◆ レジストリハイブとレジストリファイル

レジストリハイブ	レジストリファイルの場所
HKEY_LOCAL_MACHINE¥SAM	C:¥Windows¥System32¥config¥SAM
HKEY_LOCAL_MACHINE¥SECURITY	C:¥Windows¥System32¥config¥SECURITY
HKEY_LOCAL_MACHINE¥SOFTWARE	C:¥Windows¥System32¥config¥SOFTWARE
HKEY_LOCAL_MACHINE¥SYSTEM	C:¥Windows¥system32¥config¥SYSTEM
HKEY_USERS¥ (ユーザーのSID)	C:¥Users¥【ユーザー名】¥NTUSER.DAT

レジストリファイル(2)

- OS標準の「レジストリエディタ」で表示される一部のレジストリハイブは、複数のレジストリファイルなどの情報を組み合わせて自動構成されます。

◆ 複数のレジストリファイル等から自動構成されるレジストリハイブ

レジストリハイブ	説明
HKEY_CLASSES_ROOT	エクスプローラーを使用してファイルを開くときに正しいプログラムを起動するための情報が格納される。
HKEY_CURRENT_CONFIG	システムの起動時にローカル コンピューターにより使用されるハードウェア プロファイルに関する情報が格納される。
HKEY_CURRENT_USER	現在ログオンしているユーザーの構成情報が格納される。

レジストリの調査項目

- レジストリには、ハードウェア情報や利用者操作の痕跡など、さまざまな情報が残されています。
- 調査項目の一例を下表に記載します。

◆ レジストリの調査項目の一例

調査項目	レジストリ	キー/値
OSインストール日時	SOFTWARE	キー: ¥SOFTWARE¥Microsoft¥WindowsNT¥CurrentVersion 値: InstallDate (バイナリ値だが, Registry Viewerでは解析結果が表示される)
USBストレージの接続履歴	SYSTEM	キー: ¥ControlSet001¥Enum¥USBSTOR¥[メーカー, 型番のキー] ¥[シリアル番号のキー] (補足) ControlSetは複数存在する。現在値は, ¥Selectキー配下の値Currentで確認する。 上記キーの更新日時は, 最終接続日(OS起動後, 1回目以降の接続履歴のみ記録。OSが再起動されるまで, 再接続してもキーの更新日時は更新されない。)その他のキーおよびログファイルにもさまざまな接続履歴が記録される。(本日の講義では, 説明を割愛)
プログラムの起動履歴	NTUSER.DAT	キー: ¥Software¥Microsoft¥Windows¥CurrentVersion¥Explorer¥UserAssist¥{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}¥Count 上記キーの配下に, エクスプローラーから起動したプログラム名, 実行日時, 実行回数などが記録されている。

Registry Viewer

- Registry Viewerは、レジストリファイルを解析するGUIのフォレンジックツールです。
- レジストリエディタとは異なり、レジストリキーの更新日時を表示します。また、一部のレジストリキーについては、解析結果が表示されます。

The screenshot shows the AccessData Registry Viewer interface. The left pane displays a tree view of registry keys. The right pane shows a list of registry keys with columns for Name, Type, and Data. The bottom pane shows the properties of the selected key.

レジストリキー
レジストリキーをツリー表示する。

キープロパティ
レジストリキーの更新日時が表示される。また、一部のレジストリキーでは、解析結果も表示される。

Name	Type	Data
HRZR_PGYFRFFVBA	REG_BINARY	BA F8
HRZR_EHACVQY:%pfvqy2%#...	REG_BINARY	01 00
HRZR_EHACVQY:%pfvqy2%#...	REG_BINARY	01 00
HRZR_EHACVQY:%pfvqy2%#...	REG_BINARY	01 00
HRZR_PGYPHNPbhag:pgbe	REG_BINARY	01 00
HRZR_EHACNGU	REG_BINARY	04 00
HRZR_EHACNGU:P:¥JVAQBJF...	REG_BINARY	03 00
HRZR_HVDPHG	REG_BINARY	04 00
HRZR_HVFPHG	REG_BINARY	04 00
HRZR_EHACNGU:::{871P538...	REG_BINARY	04 00
HRZR_EHACNGU:P:¥Cebtenz	REG_BINARY	04 00

値(Value)とデータ
選択したレジストリキー配下の値とデータを表示する。

データ
選択した値のデータを、バイナリおよびASCIIで表示する。

[実習04] Registry Viewer

- 実習用PCで、Registry Viewerによるレジストリファイル閲覧方法を確認します。

Mission01 OSインストール日時の確認

Mission02 USB接続履歴の確認



第3章 考察

考察と報告書の作成

- 解析・抽出により確認した「事実」を整理し、報告書を作成します。
- 報告書には、事実を正確に記載することは当然ですが、それに加え、調査結果をどのように受け止めるべきか、次のどのようなアクションをとるべきか、上司が「判断」をするために必要な考察を記載するよう心がけます。



まとめ

まとめ

- 適切なインシデント対応とするためには、状況を正しく把握することが重要です。
- 正しく状況を把握するためには、事前の準備が必要です。
(特に、システム管理者の皆さんのスキルアップが必要)
- 感染PCなどを調査する際は、鑑識官になったつもりで、証拠性を損ねないように注意します。
- 報告書は、事実だけを記載するのではなく、上司の判断の参考材料となる考察を記載するよう心掛けましょう。

次回以降、想定シナリオの調査方法を学習します