マルウェア感染対応基礎編

ウイルス検知アラートとタイムライン解析から感染経緯を読み解く方法

平成30年9月8日

仙台CTF推進プロジェクト

目次

講師自己紹介

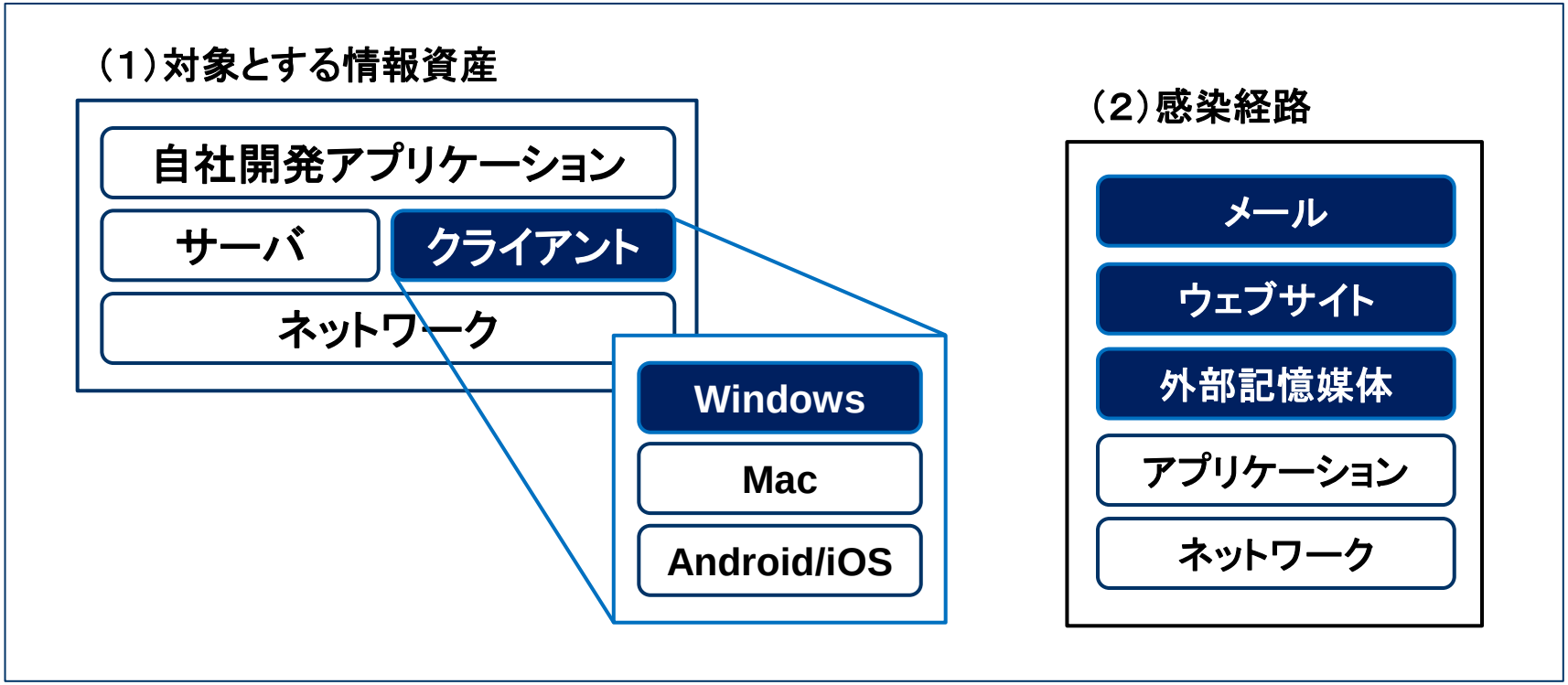
名前	五十嵐　良一（いがらし　よしかず）
職業	会社員
趣味	・フォレンジック技術の検証 ・マルウェアの解析

情報セキュリティ担当者のための実験室 セクタンラボ 管理人
http://sectanlab.sakura.ne.jp/

本講座の対象範囲

- 本講座では、自組織のパソコンに導入しているウイルス対策ソフトから「検知アラート」が通知された場合の調査・対応手法について、学習します。

◆本講座の対象範囲



本講座の学習目標とねらい

学習目標

① ウイルス対策ソフトの検知アラートを読み解き、マルウェアの感染経路※1と感染の可能性を推測できる。

※1　USBメモリ、ウェブサイト、メールなど

② タイムライン解析による、マルウェア感染経緯の調査手法を理解する。

ねらい

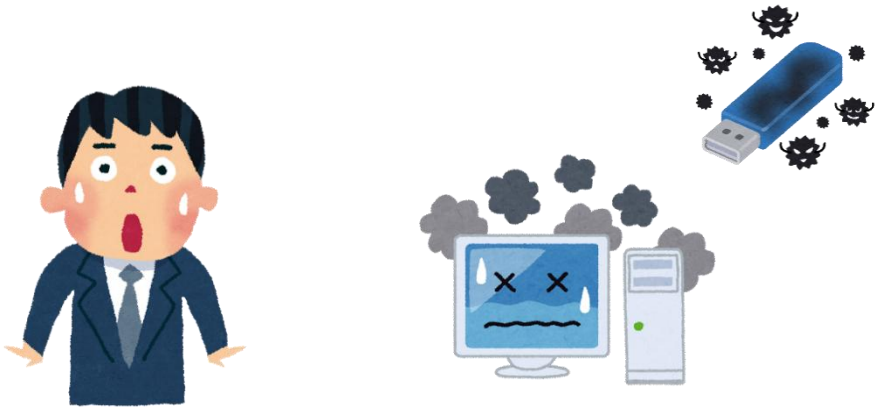
ツールを活用したインシデント対応を体験

↓

面白そう・使ってみようかな、勉強してみようかな

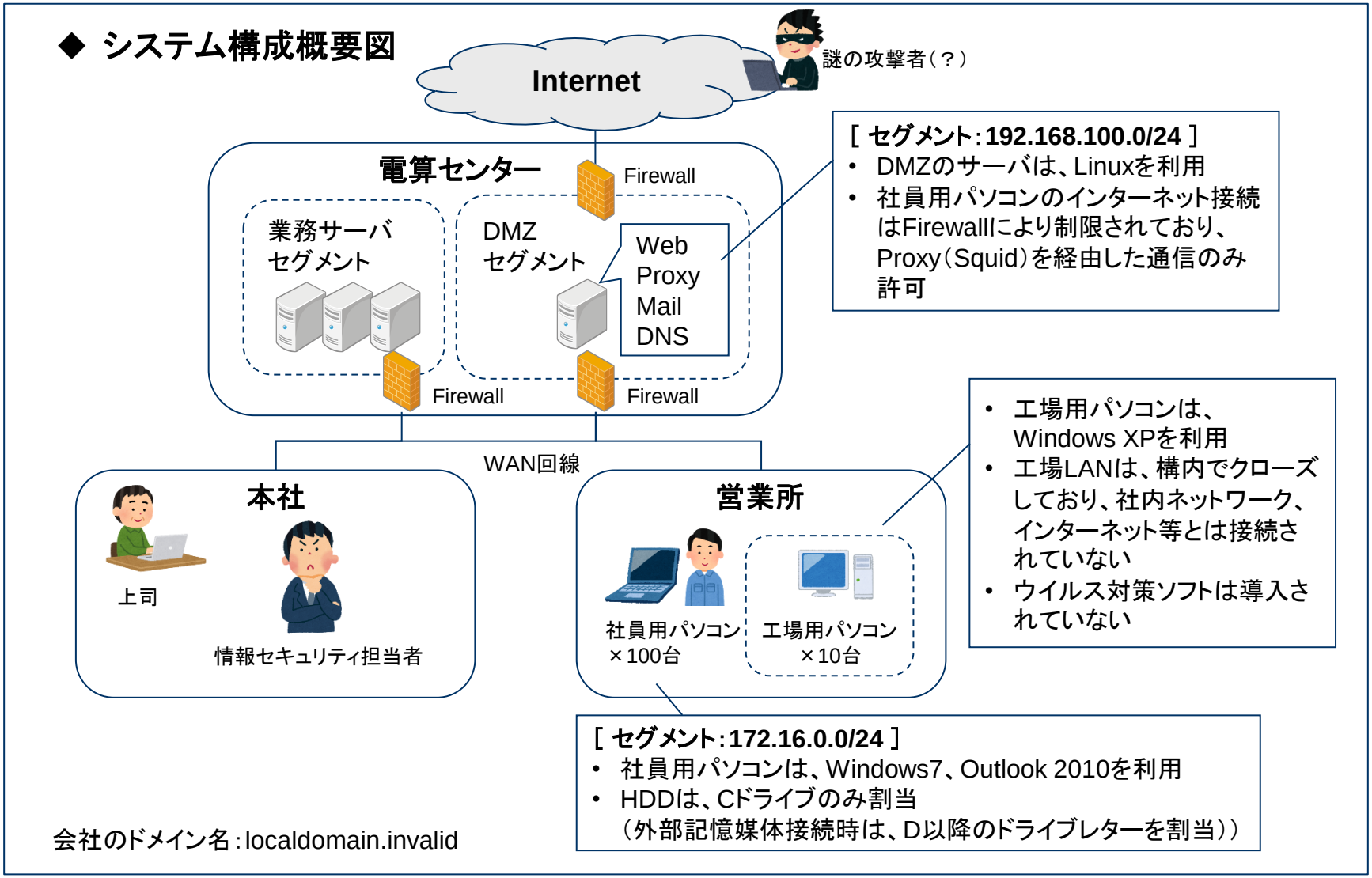
舞台設定

- あなたは、架空の企業「株式会社仙台シーテーエフ」に入社したばかりの新米情報セキュリティ担当者です。
- 先輩と2人で業務を進めていましたが、先輩が怪我で入院してしまったため、社内の情報セキュリティに関するさまざまな問題に一人で対処することになりました。



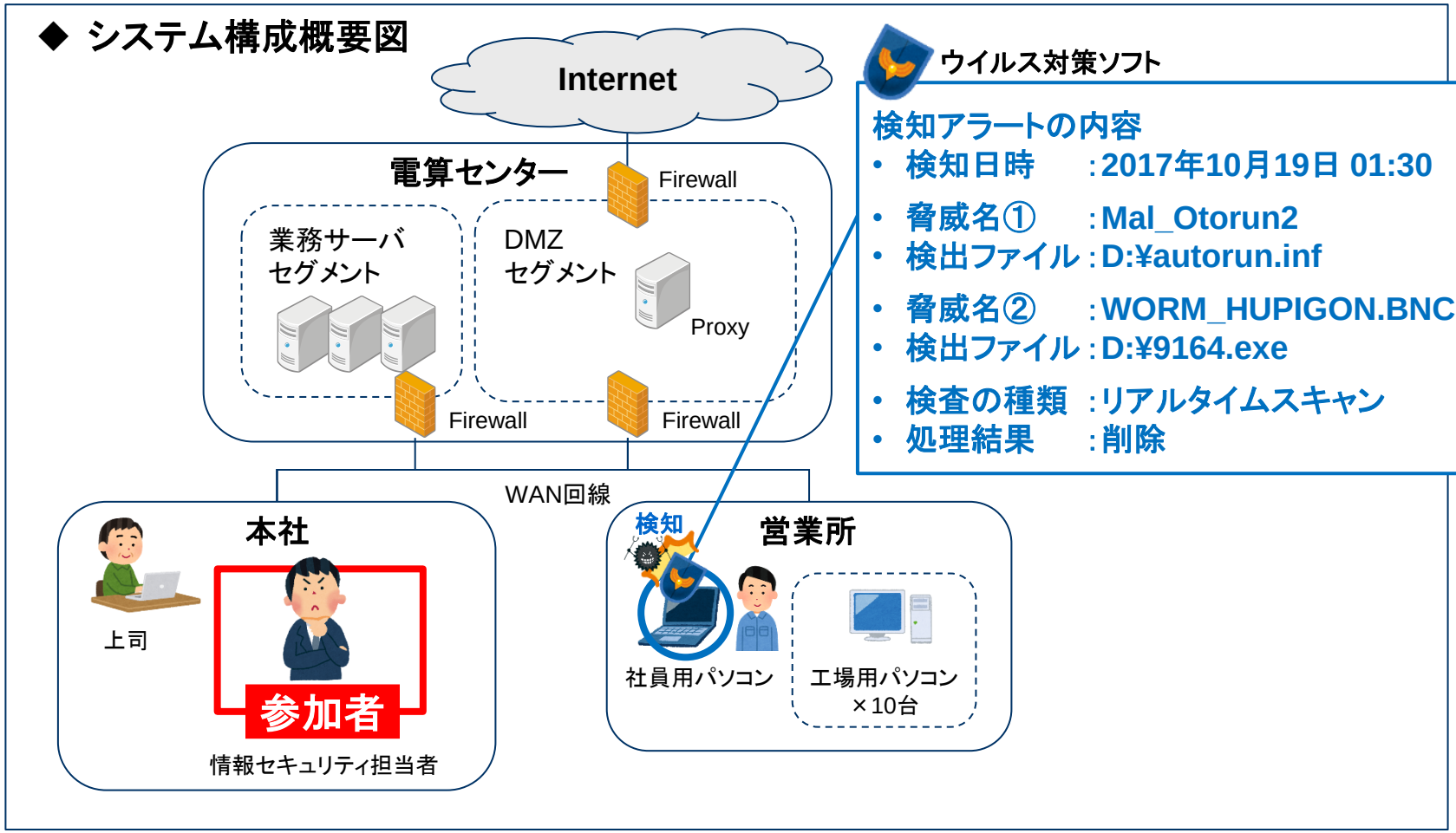
「株式会社仙台シーテーエフ」のシステム構成

◆ システム構成概要図



本日のインシデント

- ある日、社員用パソコンのウイルス対策ソフトから、検知アラートが通知されました。
- さて、どうしますか？



本講座の進行に関するお願い事項

- 本講座は盛りだくさんの内容となっていることから、時間の都合上、要点を絞って説明します。説明を割愛したスライドについては、後日、各自で資料をご参照ください。

- また、実習時間も短めとなっており、時間内に全ての実習が終わらないこともあるかと思いますが、実習終了時間になったら講義を再開させていただきます。

- 講義資料、実習資料ともに、皆様が持ち帰り復習できるよう準備しておりますので、ご理解・ご協力くださいますようお願いいたします。

第1章. ウイルス対策ソフトの検知アラート

この章では、一般的なウイルス対策ソフトの動作原理と、ウイルス検知アラートに記載される各項目について学習します。

一般的なウイルス対策ソフトの動作

- **一般的なウイルス対策ソフトは、既知のマルウェアの特徴を定義したデータベース（パターンファイル）に基づき、検査対象ファイルの内容を検査します。**
- **ファイルを検査するタイミングは、以下の2種類に分類されます。**

① リアルタイムスキャン
- システムの動作を常時監視し、ファイルにアクセス（作成、参照、削除）したタイミングで、検査を実施

② オンデマンドスキャン
- 利用者の手動または指定したタイミングで、指定したドライブ・フォルダ内の全ファイルの検査を実施

◆ 検知アラートの例

項目	内容の例	補足
検知日時	2017年10月19日01:30	
脅威名	Mal_Otorun2	ウイルス対策ソフトのメーカーごとに命名しているマルウェアの名称
検出ファイル名	D:¥autorun.inf	
検査の種類	リアルタイムスキャン	
処理結果	隔離	隔離　：検知したファイルを暗号化したうえで「隔離フォルダ」に移動 削除　：検知したファイルを削除 駆除　：検知したファイルの中のマルウェア部分のみ削除 放置　：検知したファイルを放置（アクセスはブロック） **例：マクロウイルスに感染したエクセルファイルから、マクロのみ削除**
検出コンピュータ名	PC0010	

ウィルス検知アラートからの状況推測

- マルウェア感染時・感染後に「どのようなファイルアクセスが発生するのか」を理解していれば、検出したファイル名とパス（フォルダ）から、状況を推測することができます。（詳細は、第2章で学習）

◆ マルウェア感染時・感染後のファイルアクセスのイメージ

時刻	ファイルアクセス
10:02:10	通常のファイルアクセス 例：メールソフトがメールを受信し、メールボックスファイルに書き込み
10:15:12	マルウェア感染前に発生するファイルアクセス 例：利用者が、不審メールに添付されたZIPファイルを閲覧した際に、ZIPファイルに格納されていたファイルが展開され、一時フォルダに書き込み
10:15:15	マルウェア感染 例：利用者が、ZIPファイルに格納されていたダウンローダー（拡張子.JS）をダブルクリックしたことで、マルウェア本体がダウンロード・実行されて感染
10:15:20	マルウェア感染後に発生するファイルアクセス 例：感染したマルウェアが、自身を別のフォルダーにコピーし、OS起動時に自動起動できるようレジストリを改変

検出したファイル名とパス（フォルダ）から、「感染前」と「感染後」のどちらのタイミングで検知したのか推測

リアルタイムスキャン

- リアルタイムスキャンは、基本的に「現在進行形の事象」を検知します。
- 検知されたタイミング、検出したファイルのパスなどから状況を推測します。

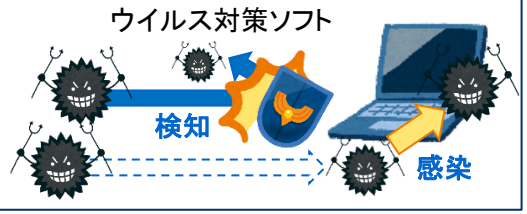
◆リアルタイムスキャンによる検知のパターン例

（1）マルウェアが侵入した瞬間に検知（感染する前に防御成功）

不審メールの添付ファイルを開封した際に、メールソフトが一時フォルダに作成した添付ファイルのコピーなどを検知し、感染する前に防御できた。

（2）マルウェアが侵入した瞬間に検知（ただし他のマルウェアに感染）

悪意のあるウェブサイト閲覧時に、ブラウザが一時フォルダにダウンロードした複数のマルウェアのうち、一部のマルウェアを検知したものの、他のマルウェアには感染した。



（3）パターンファイル更新により、すでに感染していたマルウェアを検知

すでにマルウェアに感染していたが、パターンファイルを更新したことにより、マルウェアへのファイルアクセス時※1に検知した。

（※1）パソコンのログイン直後など、マルウェアが起動する際のファイルアクセスで検知されることがある。

オンデマンドスキャン

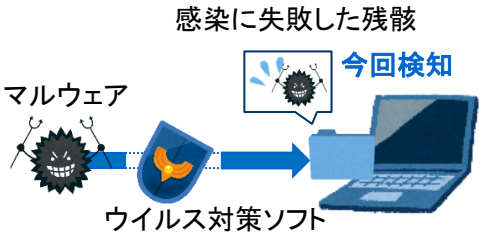
- オンデマンドスキャンで検知されたということは、過去のどこかの時点で、「ウイルス対策ソフトで検知できないマルウェアが侵入していた」ということであり、検知したパソコン、および他のパソコンが感染した可能性を考える必要があります。
- 検出したファイルのパスなどから状況を推測します。

◆オンデマンドスキャンによる検知のパターン例

（1）感染に失敗したマルウェアの残骸を検知

悪意のあるウェブサイト閲覧時に、ブラウザが脆弱性攻撃コードを含むファイルを一時フォルダにダウンロードしたものの、セキュリティパッチ適用済みなどの理由により脆弱性攻撃が失敗した。

オンデマンドスキャンにより、一時フォルダに残されていた残骸を検知した。（他のパソコンでは感染が成功した可能性もある）



（2）感染しているマルウェアの一部を検知

マルウェア感染時に利用される「ダウンローダー」など、マルウェアの一部を検知したが、感染しているマルウェア本体は検知されずに活動を続けている。

（他のパソコンも感染している可能性がある）

第2章. マルウェア感染時の挙動

検出したファイルのパスから状況を判断するためには、マルウェア感染時・感染後に「どのようなファイルアクセスが発生するのか」を理解する必要があります。
この章では、USBメモリ、ウェブ、メールなど、感染経路ごとに、感染時の挙動について学習します。

（補足）本講座では、「悪意のあるコード」（ダウンローダーを除く）が実行されることを「感染」と定義しています。

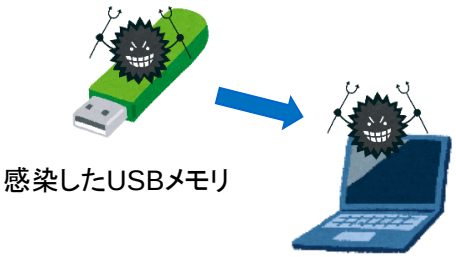
マルウェアとは

- マルウェアとは、コンピューターウイルス、ワーム、ランサムウェアなど「悪意のあるソフトウェア」（Malicious Software）の総称です。
- 感染に至る経路はさまざまですが、本講座では、「USBメモリ」、「ウェブサイト」、「メール」からの感染について説明します。

◆本講座で説明するマルウェアの感染経路

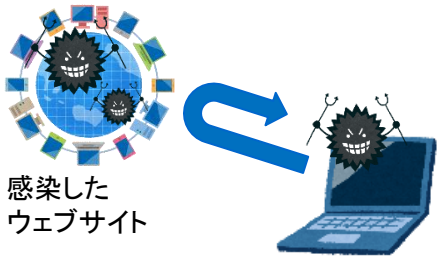
USBメモリからの感染

感染したUSBメモリを接続されたパソコンが感染



ウェブサイトからの感染

感染したウェブサイトにアクセスしたパソコンが感染



メールからの感染

不審メールの添付ファイルを開封したパソコンが感染

1.USBメモリからの感染時の挙動

2.ウェブサイトからの感染時の挙動

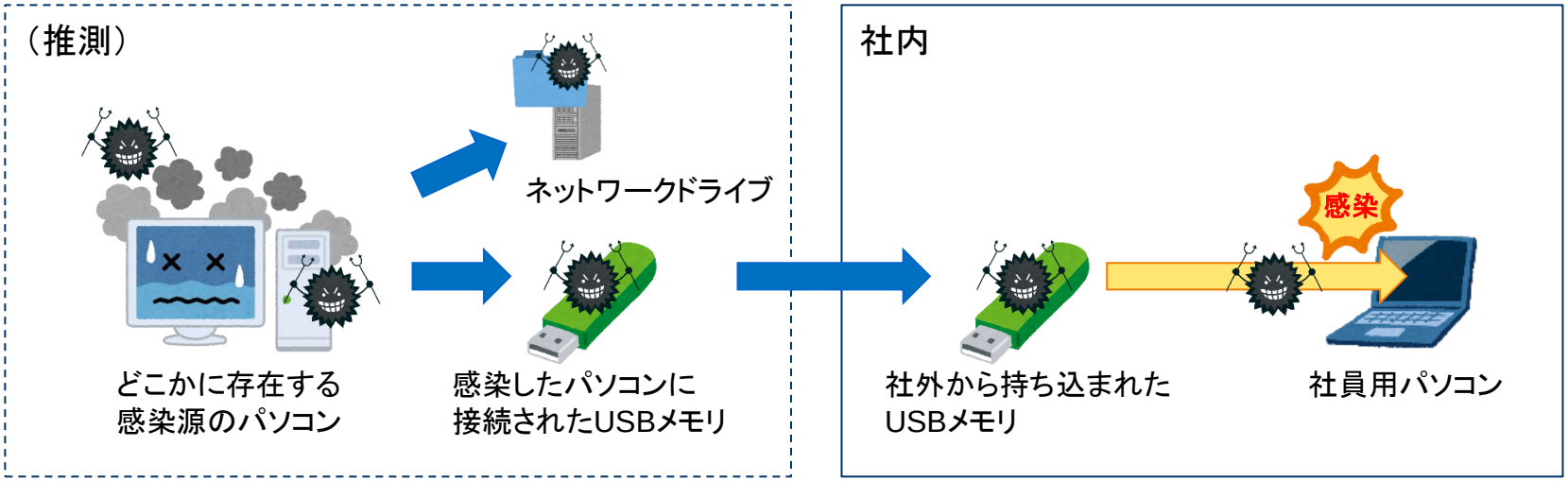
3.メールからの感染時の挙動

4.感染後の挙動（感染永続化）

感染経路の概要

- USB感染型マルウェアに感染したパソコンは、接続されたUSBメモリやネットワークドライブなどへの感染を試みます。
- 感染したUSBメモリが、セキュリティ対策が不十分なパソコンに接続されることで感染が拡大していきます。

◆感染経路の概要



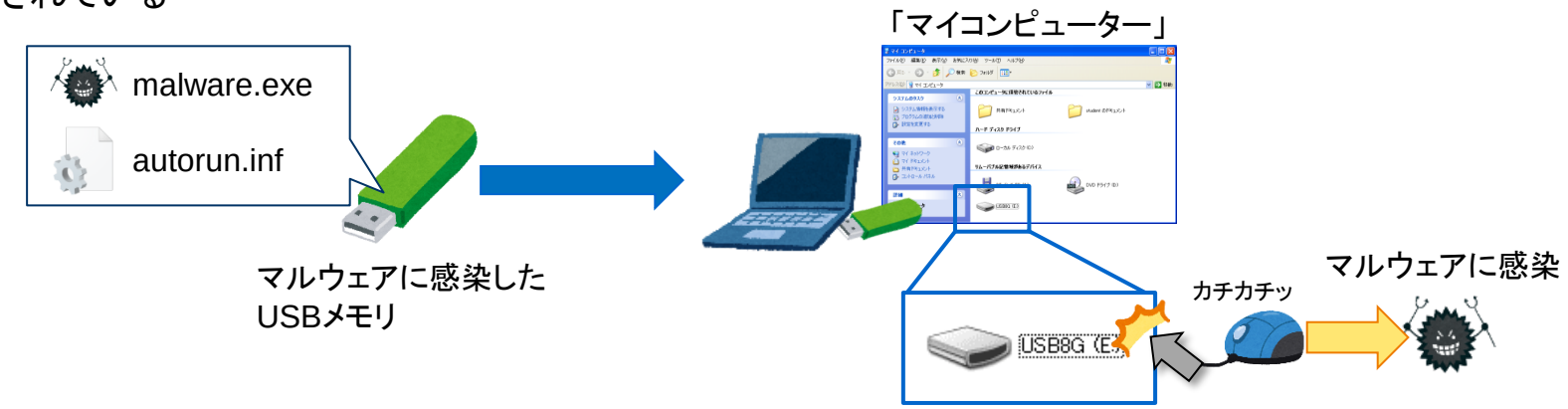
主な感染手法（1）自動実行機能（Autorun機能）

- **Windows Vista以前の古いパソコンは、USBメモリの自動実行機能（Autorun機能）により、感染したUSBメモリを利用しただけでマルウェアに感染します。**
  - Winows7以降は、USBメモリの自動実行機能が無効化されているため、感染する危険性は低くなっています。

◆自動実行機能の概要

①USBメモリにマルウェア本体と自動実行機能の設定ファイル「autorun.inf」が格納されている

②感染したUSBメモリをパソコンに接続し、エクスプローラーで**USBメモリのドライブアイコンをダブルクリックすると感染**



（補足）トレンドマイクロによると、2008年に発生したマルウェア「Downad」（別名Conficker」は、2017年度になっても蔓延しており、古いOSを利用していた場合、いまでも感染する危険性がある。
トレンドマイクロセキュリティブログ：　https://blog.trendmicro.co.jp/archives/16614

主な感染手法（2）ショートカットファイルの脆弱性

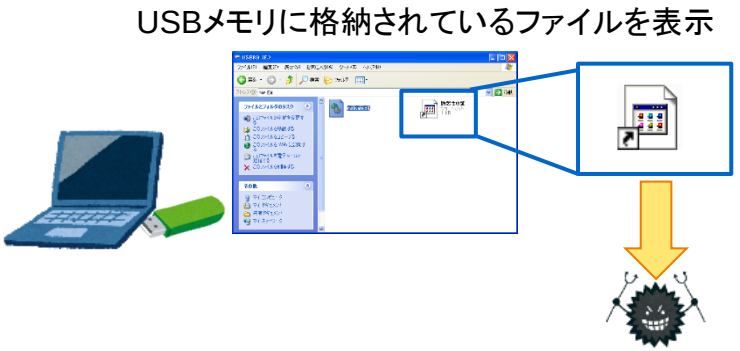
- 脆弱性※1が改修されていないパソコンは、感染したUSBメモリに格納されている
  ショートカットファイル（拡張子.LNK）を表示しただけで、マルウェアに感染します。

◆ショートカットファイルの脆弱性の概要

①USBメモリにマルウェア本体（DLL）と、細工したショートカットファイルが格納されている

マルウェアに感染した
USBメモリ

②感染したUSBメモリに格納されているショートカットファイルをエクスプローラーで表示すると感染



マルウェアに感染

（※1）MS10-046（2010年に発表）、またはCVE-2017-8464（2017年に発表）の脆弱性
なお、MS10-046は、イランの核燃料施設へのゼロデイ攻撃に利用された脆弱性

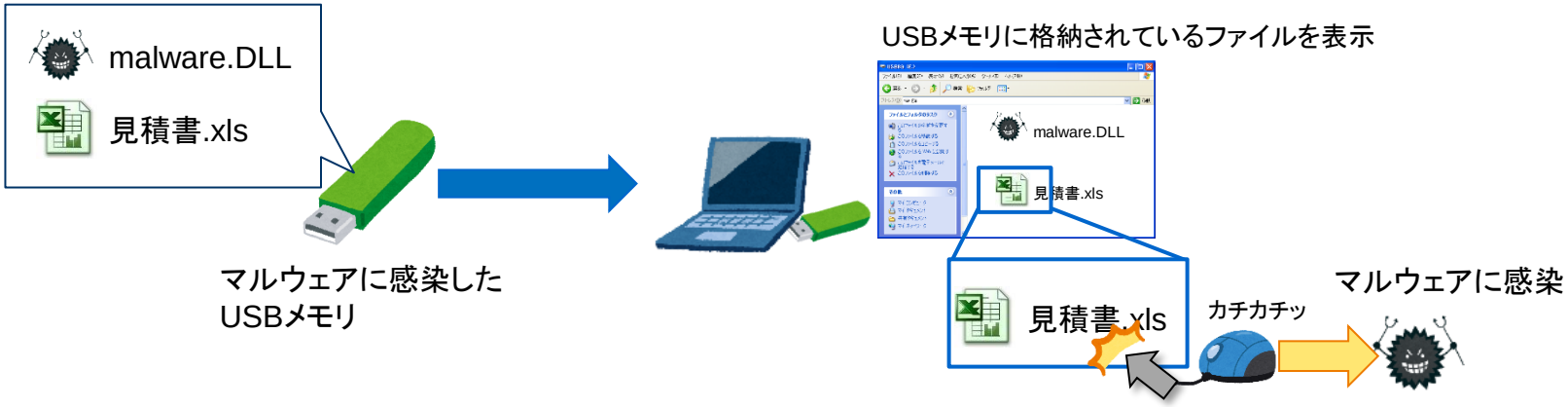
主な感染手法（3）DLL読み込みの脆弱性

- DLLの読み込みの脆弱性があるソフトウェアがインストールされているパソコンは、感染したUSBメモリに格納されているファイル（脆弱性があるアプリケーションに関連付けされたファイル）を開いただけで、マルウェアに感染します。

◆DLL読み込みの脆弱性の概要

①USBメモリにマルウェア本体（DLL）と、
脆弱性があるアプリケーションに関連付けされたファイル（例：エクセル文書）が格納されている

②USBメモリに格納されている、
「アプリケーションに関連付けされたファイル」
をダブルクリックすると感染



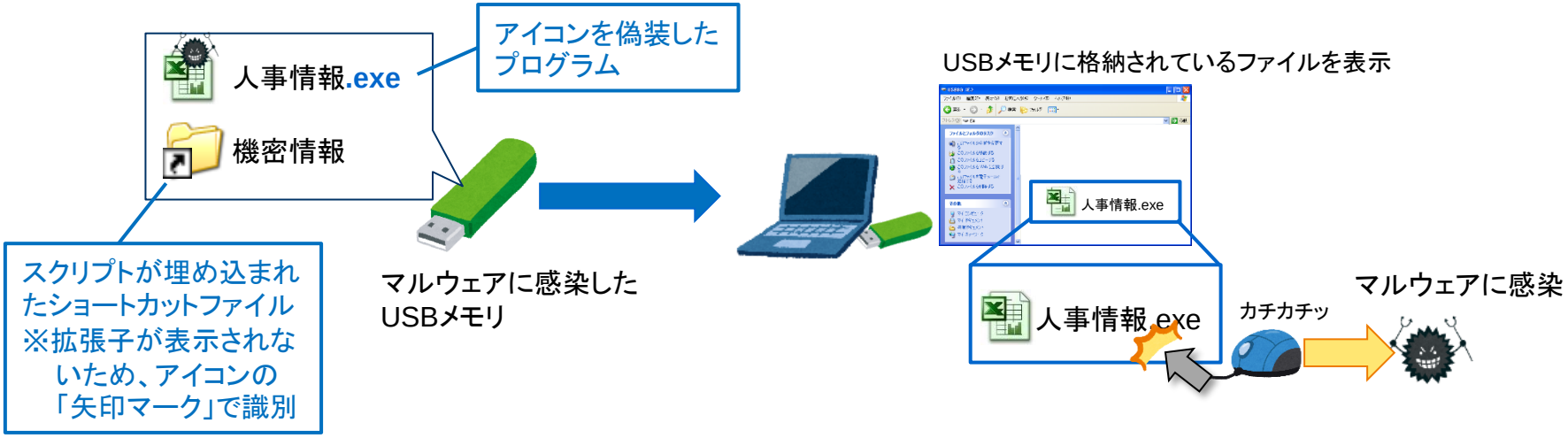
主な感染手法(4)利用者の心理的な脆弱性

- 利用者の勘違いや不注意などにより、感染したUSBメモリに格納したマルウェアをダブルクリックさせることで感染します。

◆利用者の心理的な脆弱性

①USBメモリに、利用者が興味を引きそうな名前のマルウェア本体を格納します。また、無害なファイルを装うためにアイコンも偽装します。

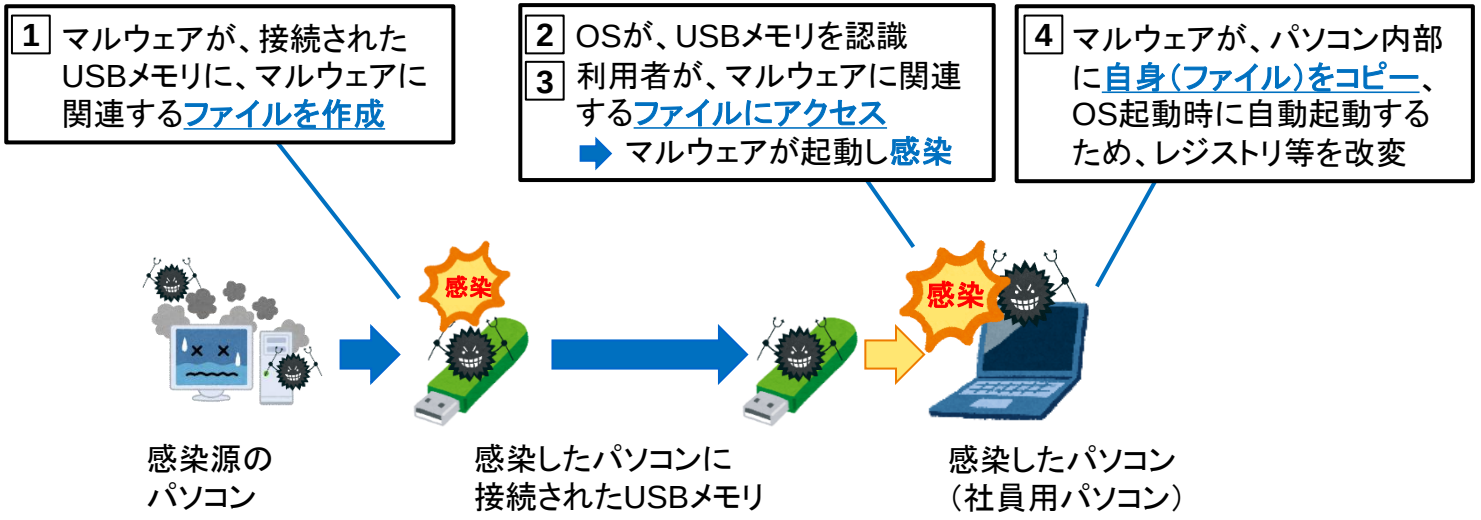
②USBメモリに格納されているマルウェアをダブルクリックすると感染



感染時の挙動と痕跡の概要

- 感染時の挙動と、調査に役立つ痕跡が残る個所を下図に示します。
- マルウェアによる「ファイルアクセスが発生するタイミング」を理解することで、ウイルス検知アラートから状況を推測することができます。

◆感染時の挙動と痕跡の概要



ウイルス検知アラートの特徴

- 検出ファイルのパスが、USBメモリなどに割り当てられるドライブ、またはネットワークドライブとなります。

◆ ウイルス検知アラートの例

項目	内容の例
検知日時	2017年10月19日01:30
脅威名	Mal_Otorun2
検出ファイル名	D:¥autorun.inf
検査の種類	リアルタイムスキャン
処理結果	隔離
検出コンピュータ名	PC0010

- 脅威名をインターネットで検索すると、USBメモリ感染型マルウェアであることが判明する。

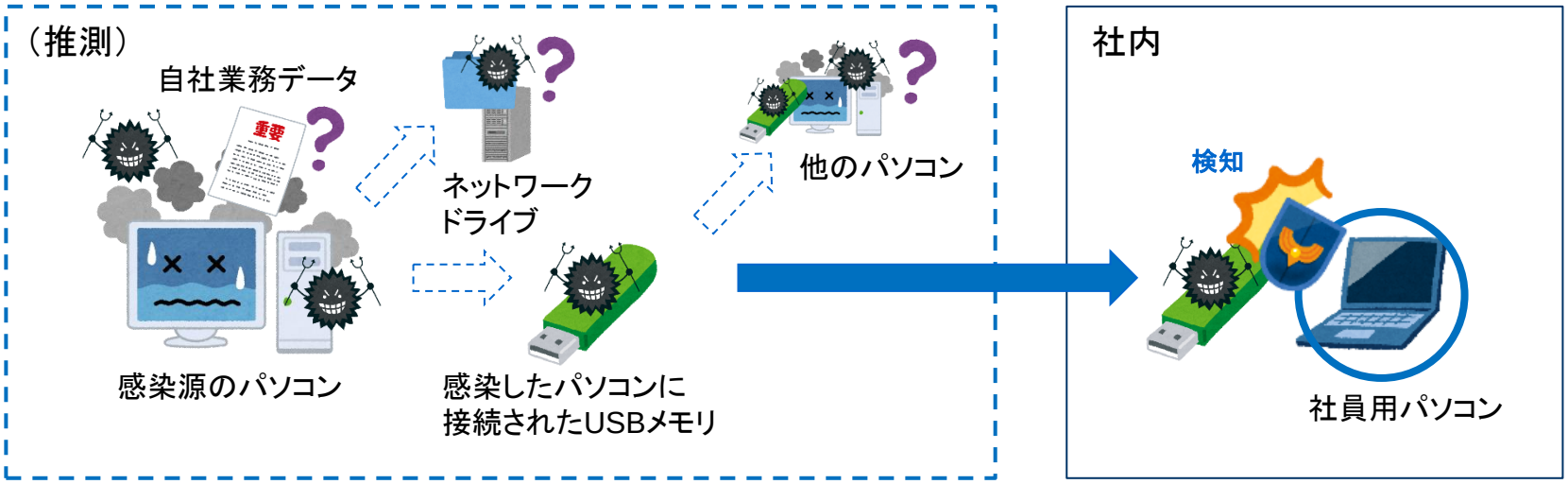
- USBメモリなどに割り当てられるドライブに格納されている「autorun.inf」を検知していることから、USBメモリ感染型マルウェアと推測できる。

（※1）社員用パソコンのHDDは、Cドライブのみ割り当てられており、外部記憶媒体はDドライブ以降になるという前提

ウイルス検知アラートからの状況推測

- **検知したパソコンは、感染前に防御できた可能性があると推測できます。**
- **しかし、感染USBメモリが、セキュリティ対策が不十分な他のパソコンに接続されていた場合、感染が拡大している可能性があります。**
  - ➡ 感染USBメモリの利用を禁止し、証拠保全するとともに、接続したパソコンを洗い出します。
- **また、どこかに存在する「感染源のパソコン」から業務データが流出したり、感染が拡大したりしている可能性があります。**
  - ➡ 感染USBメモリがどこから持ち込まれたのか確認します。

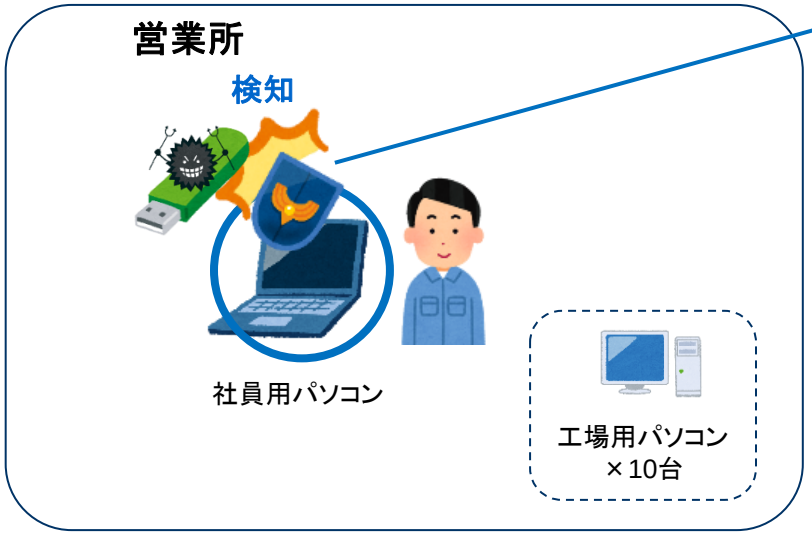
◆状況推測



いきなり体験！フォレンジック調査（USB感染型マルウェア編）

- 「株式会社仙台シーテーエフ」におけるフォレンジック調査の体験を通じて、USB感染型マルウェアの痕跡を確認してみましょう。

◆ウイルス検知アラートの内容



ウイルス対策ソフト

検知アラートの内容
- 検知日時　：2017年10月19日 01:30
- 脅威名①　：Mal_Otorun2
- 検出ファイル：D:¥autorun.inf
- 脅威名②　：WORM_HUPIGON.BNC
- 検出ファイル：D:¥9164.exe
- 検査の種類　：リアルタイムスキャン
- 処理結果　：削除

「体験」していただくことが目的ですので、
気楽な気持ちで、調査の雰囲気をお楽しみください。

ウイルス検知アラートからの状況推測（1）

- まずは、ウイルス検知アラートから状況を推測します。

◆状況推測

ウイルス対策ソフト

検知アラートの内容
- 検知日時　　：2017年10月19日 01:30
- 脅威名①　　：Mal_Otorun2
- 検出ファイル：D:¥autorun.inf
- 脅威名②　　：WORM_HUPIGON.BNC
- 検出ファイル：D:¥9164.exe
- 検査の種類　：リアルタイムスキャン
- 処理結果　　：削除

USB感染型マルウェア（自動実行機能を悪用するタイプ）かもしれない。

（※1）社員用パソコンのHDDは、Cドライブのみ割り当てられており、外部記憶媒体はDドライブ以降になるという前提

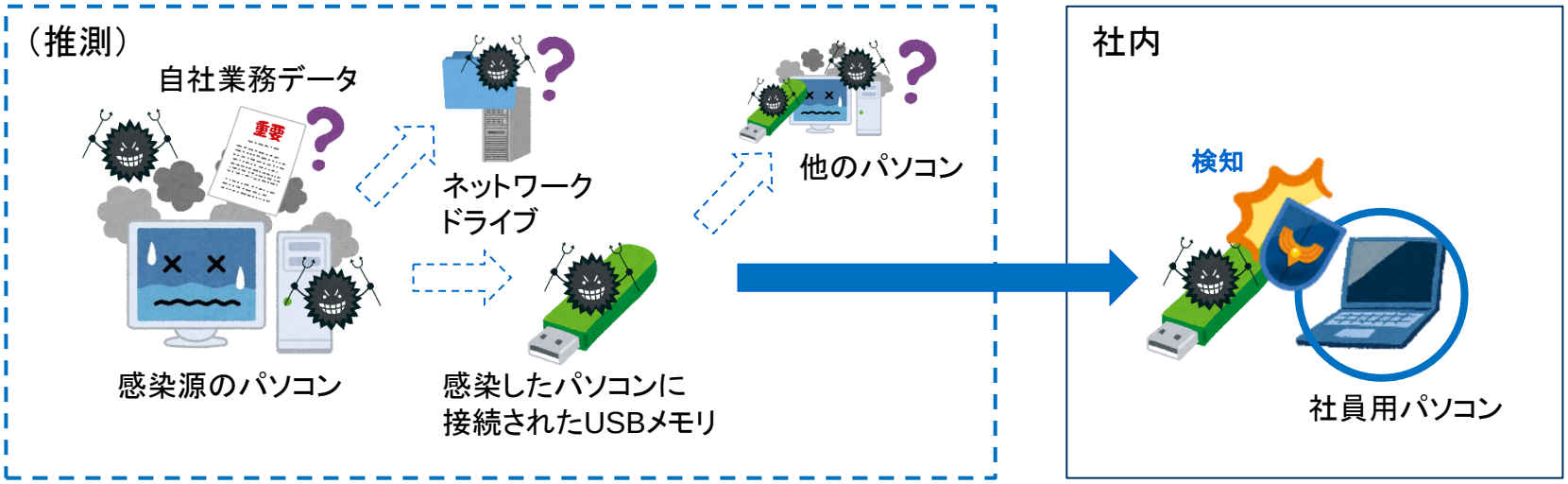
USBメモリが接続された瞬間に検知しており、社員用パソコンが感染している可能性は低いと思われる。

体験中

ウイルス検知アラートからの状況推測（2）

- **ウイルス検知アラートが発生した背景と潜在しているリスクを推測します。**
  - ① 感染USBメモリは、どこから持ち込まれたのか
    - 自社のどこかにあるパソコンが感染源の可能性はないか
    - 委託先等社外のパソコンが感染源の場合、そのパソコンに自社の業務情報は格納されていないか
  - ② 感染USBメモリを他のパソコンに接続していないか
    - 社内の他のパソコンに感染を拡大させていないか
    - 社外の取引先に感染を拡大させるなど、自社が加害者になっていないか

◆状況推測



体験中

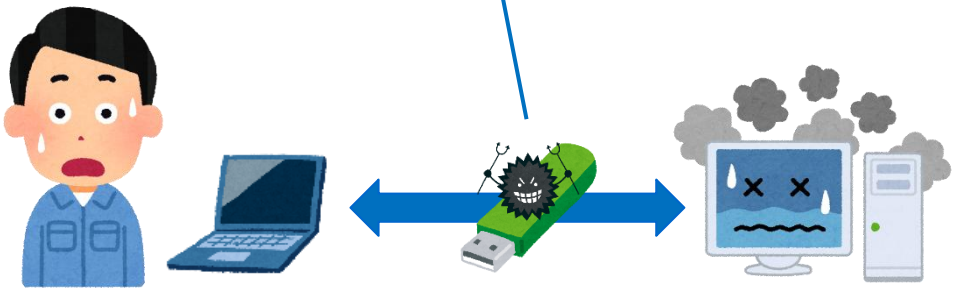
現地の状況確認

- ウイルス検知アラートが発生した職場の管理職に電話連絡するなど、現地の状況を確認します。

◆現地の状況確認の結果

現地からの回答
- 検知された外部記憶媒体は、工場用パソコンとのデータ授受専用の社給USBメモリである。
- 他のパソコンには接続していない。
- なお、工場用パソコンで利用しているUSBメモリは社給USBメモリ1個だけであり、その他のUSBメモリは接続したことがない。

→ 工場用パソコンが感染している可能性がある。



社員用パソコン　工場用パソコン

フォレンジック調査開始

- **工場用パソコンの感染が疑われることから、フォレンジック調査を行うこととしました。**
- **まずは、感染USBメモリを調査してみます。**

［調査対象］

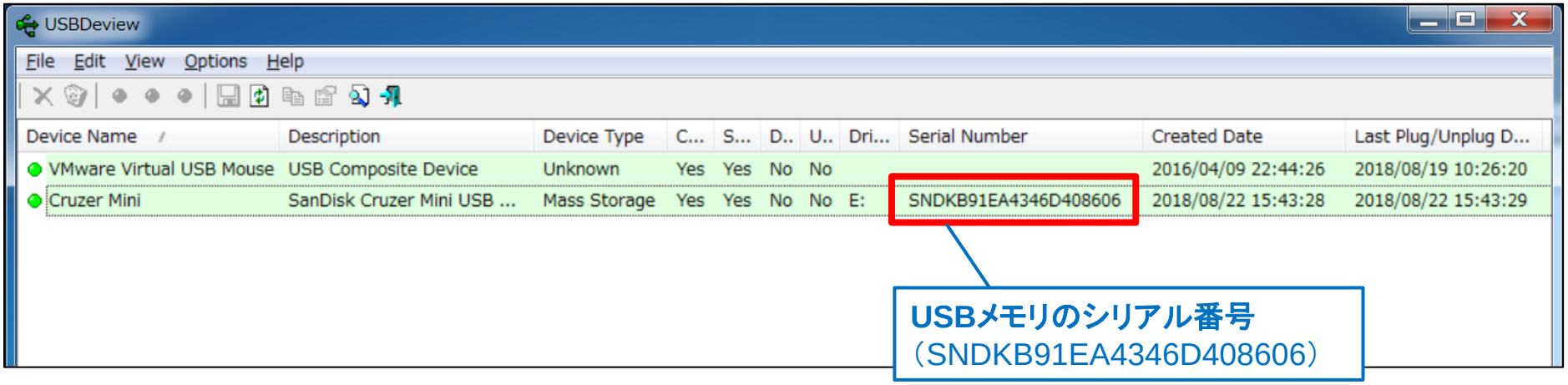
- 感染USBメモリ （FAT32形式でフォーマット）
- 工場用パソコン （Windows XP）

「体験」していただくことが目的ですので、
気楽な気持ちで、調査の雰囲気をお楽しみください。

感染USBメモリのシリアル番号の確認

- **感染USBメモリをフォレンジック用パソコンに接続し、調査用ツールでUSBメモリの「シリアル番号」を確認します。**
  - パソコンにUSBメモリを接続すると、レジストリ等にシリアル番号や接続した日時が記録されます。本手順で確認したシリアル番号は、感染USBメモリの接続履歴の調査に活用します。

◆調査用ツールによるUSBメモリの「シリアル番号」の確認の例（USBDeview）



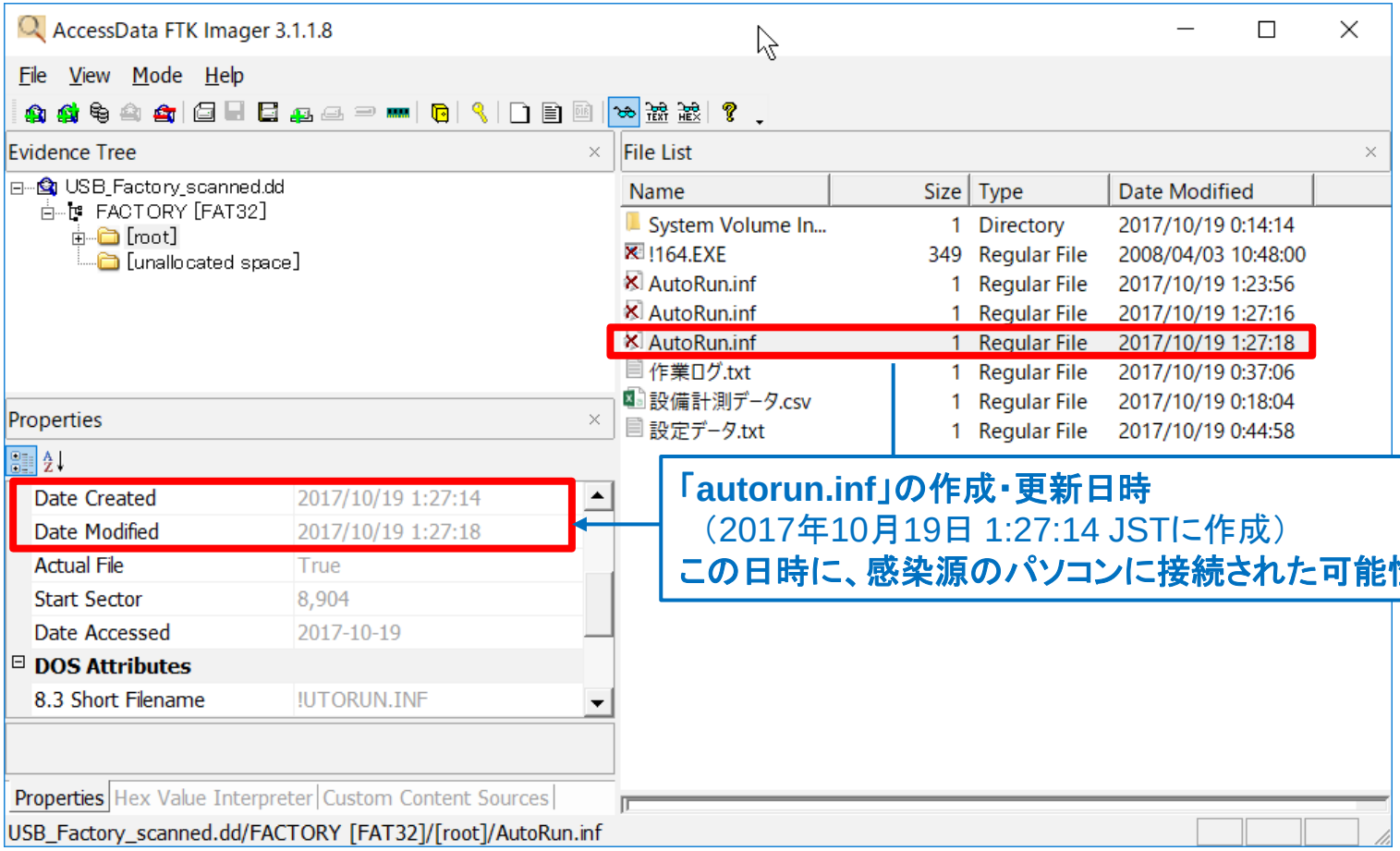
NirSoft USBDeview
https://www.nirsoft.net/utils/usb_devices_view.html

（注意）シリアル番号の2文字目が「&」になっている場合、シリアル番号を保有していない機器に対してOSがランダムに付けた番号である。パソコンごとに異なる値となるため、シリアル番号と誤認しないこと。
Forensic Wiki USB History Viewing http://www.forensicswiki.org/wiki/USB_History_Viewing

感染USBメモリに格納されているファイルの確認

- マルウェア関連ファイルの「作成日時」などのタイムスタンプから、感染USBメモリが感染源パソコンに接続された日時を推測できる場合があるため、念のため確認します。

◆フォレンジックツールによる感染USBメモリの確認結果（FTK Imager Lite）



Access Data FTK Imager Lite https://accessdata.com/product-download

（参考）タイムスタンプに関する補足

- **USBメモリに書き込んだファイルのタイムスタンプを改ざんするマルウェアも存在します。**
- **タイムスタンプが改ざんされた場合、感染USBメモリだけを調査しても、感染日時を特定することは困難となります。**
  - 利用者がUSBメモリに書き込んだデータファイルなどのタイムスタンプから、ある程度推測できる場合もあります。

［参考］FATのタイムスタンプ確認時の留意事項

•FATのタイムスタンプの分解能（記録精度）
- •作成日時：10ms単位、 最終更新日時：2秒単位、 最終アクセス日：1日単位

（注意）Windows Vista/Windows Server 2008以降のOSでは、標準設定ではNTFSの最終アクセス日時は更新しない仕様に変更された。しかし、FATの最終アクセス日時は従来どおり更新される。

•タイムゾーン
- •FATのファイルシステム内部では、タイムスタンプはローカルタイム（日本時間）で記録される。
  フォレンジックツールにより、タイムスタンプの取り扱いが異なるため事前に確認すること。

•タイムスタンプの改ざん
- •FATの仕様上、タイムスタンプを改ざんされると、改ざん前のタイムスタンプの確認は困難である。
- •特殊ファイル「.」（カレントディレクトリ）、および「..」のタイムスタンプは、改ざんされる可能性が低いため、必要に応じてフォレンジックツールでこれらのタイムスタンプを確認する。

工場用パソコンの調査

- 続いて、工場用パソコンを調査します。

［調査対象］

- 感染USBメモリ （FAT32形式でフォーマット）
- 工場用パソコン （Windows XP）

「体験」していただくことが目的ですので、
気楽な気持ちで、調査の雰囲気をお楽しみください。

パソコンの感染有無の確認

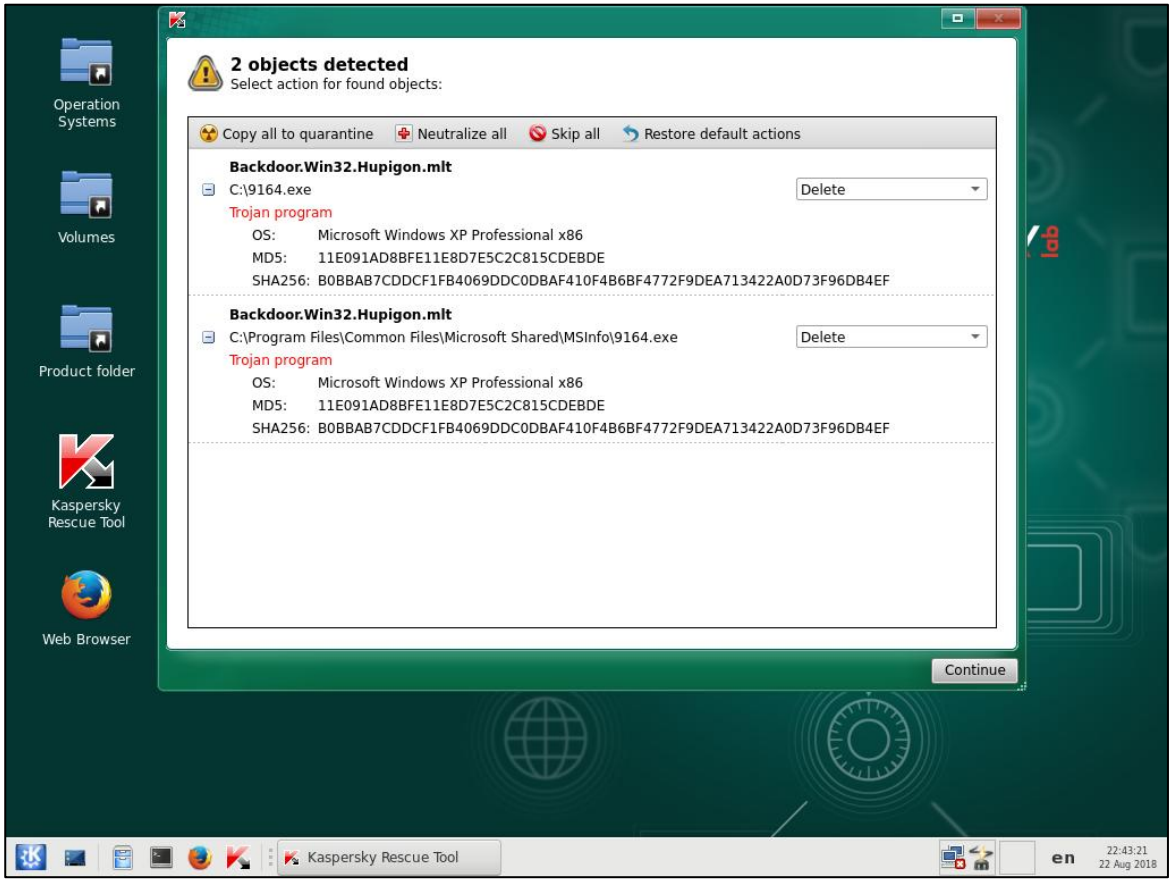
- フォレンジック調査を実施する前に、パソコンがUSB感染型マルウェアに感染しているか確認します。

◆感染有無の確認方法

分類	確認方法
ウイルスチェックツール	①　CD/USBメモリ等から起動できるオフライン型ウイルスチェックツールを準備する。 ②　感染している可能性があるパソコンをオフライン型ウイルスチェックツールで検査する。 ［注意］ウイルス判定されたファイルは、削除すると調査に支障が出るため「放置」（スキップ）すること。
簡易調査（上級者）	①　感染している可能性があるパソコンに、フォーマット済みUSBメモリを接続する。 パソコンがUSB感染型マルウェアに感染している場合、USBメモリにマルウェア関連ファイル（autorun.inf等）が書き込まれる。 ②　セキュリティ対策が実施された調査用パソコンにUSBメモリを接続し、不審なファイルが作成されていないか確認する。 ［注意］感染拡大の危険性があるため、感染している可能性があるパソコンに接続したUSBメモリは、調査用パソコン以外に接続しないこと。再利用する場合は、フォーマットすること。

ウイルスチェックツールの実行結果

◆ ウイルスチェックツールの実行結果の例（Kaspersky Rescue Tool）



Kaspersky Rescue Tool　https://support.kaspersky.co.jp/viruses/utility#kasperskyrescuedisk

CD/USBメモリからLinuxを起動するタイプの無料ウイルスチェックツール。なお、本ツールを起動すると、Cドライブ直下にログ等を保存するためのフォルダが作成されるため、厳格な証拠保全が必要とされる調査では利用しないこと。

工場用パソコンが感染していることを確認

接続されたUSBメモリのシリアル番号の確認（USBSTOR）

- 続いて、工場用パソコンに接続されたUSBメモリを確認します。
- レジストリ「SYSTEM」の「USBSTOR」キー配下に、過去に接続されたUSBメモリの製造元・型番のキー、およびシリアル番号のキーが記録されます。
- 各シリアル番号のキーには、OSがUSBメモリを一意に識別するために自動生成する「ParentIdPrefix」というランダムな値が記録されます。
  - ParentIdPrefixは、GUID（後述）とUSBメモリのシリアル番号を紐づけるために利用します。

◆調査対象のレジストリ
レジストリ：C:¥Windows¥system32¥config¥SYSTEM
キー　　：¥ControlSet001¥Enum¥USBSTOR¥[ベンダーID,プロダクトID]
　　¥[USBメモリのシリアル番号]

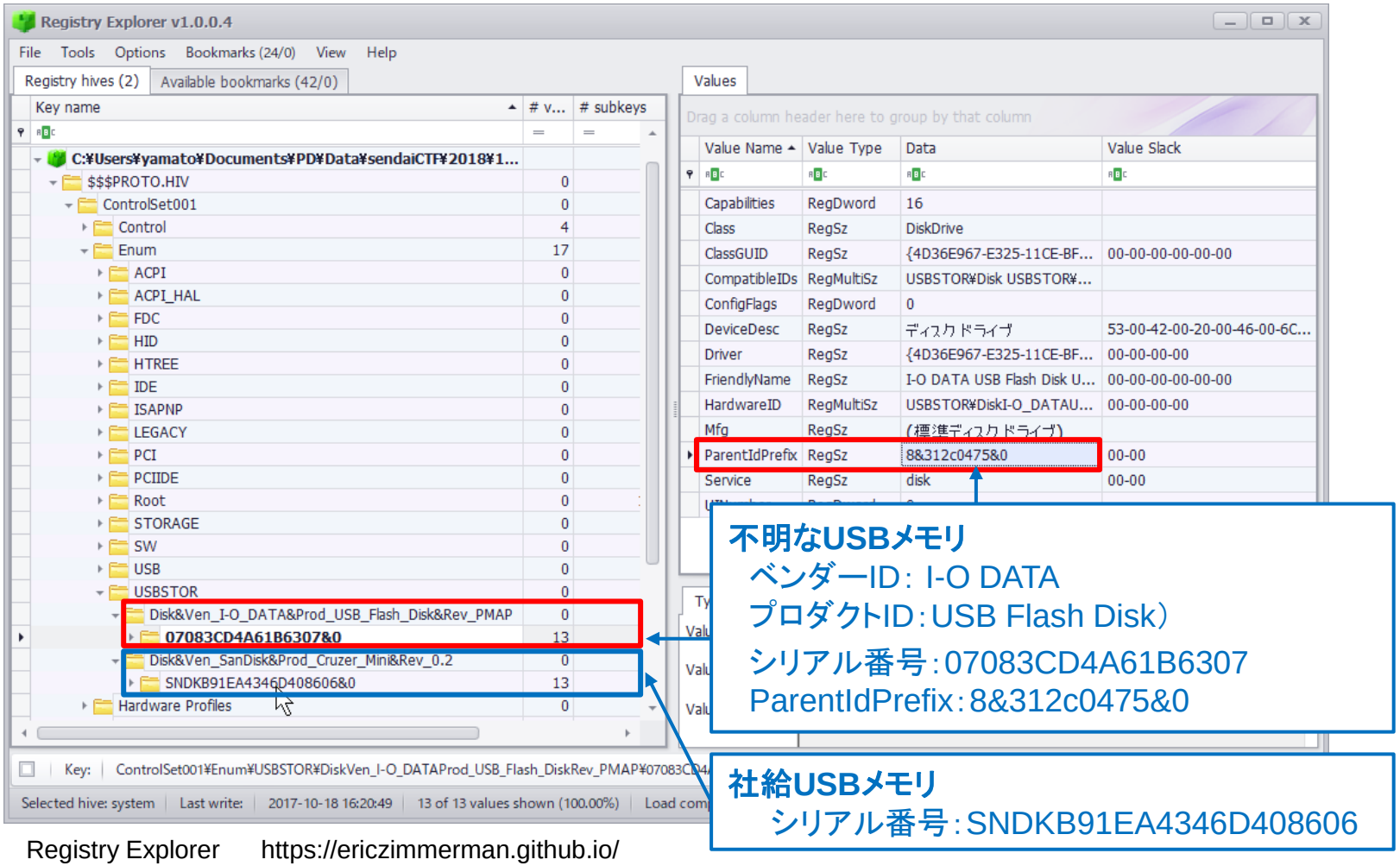
（注意）「ControlSet001」の数字（1）の部分は、「¥Select」キー配下の値「Current」の数字に読み替えること。

◆調査内容
① 過去に接続されたUSBメモリの製品名、シリアル番号を確認する。
② 各シリアル番号キーに記録されているParentIdPrefixのデータを確認する。

[ParentIdPrefixのデータの例]
¥??¥STORAGE#RemovableMedia#7&23a29435&0&RM#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
└ ParentIdPrefix

レジストリ「SYSTEM」-「USBSTOR」の確認結果

◆ 調査用ツールによるレジストリ確認結果の例（Registry Explorer）



Registry Explorer　https://ericzimmerman.github.io/

社給USBメモリの他に、不明なUSBメモリが接続されていることを確認

USBメモリのGUIDの確認（MountedDevices）

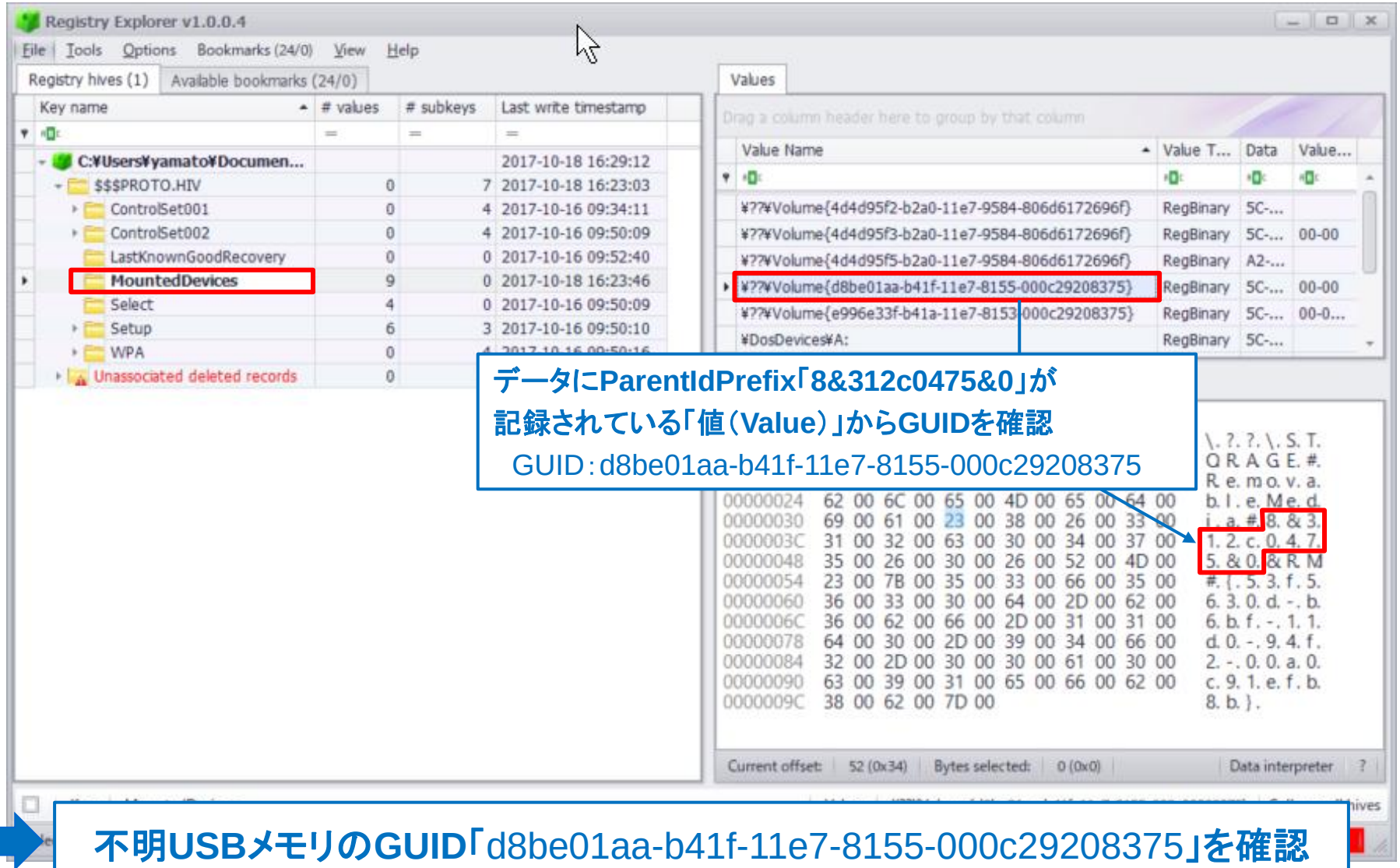
- **レジストリ「SYSTEM」の「MountedDevices」キーに、OSがUSBメモリを一意に識別するために自動生成する「GUID」というランダムな値が記録されます。**
- **また、GUIDのデータに、ParentIdPrefixが記録されます。**
  - ここで前述したParentIdPrefixとGUIDを紐づけします。
  - この後、GUIDごとに記録される「自動実行機能の痕跡」を確認します。

◆調査対象のレジストリ
レジストリ：SYSTEM
キー　　：¥MountedDevices
値　　：¥¥??¥Volume{*USBメモリのGUID*}

［GUIDの例］
¥??¥Volume{**d8be01aa-b41f-11e7-8155-000c29208375**}
└ GUID

◆調査内容
① GUIDの「値」（Value）のデータに含まれているParentIdPrefixを確認する。

レジストリ「SYSTEM」-「MountedDevices」の確認結果



データにParentIdPrefix「8&312c0475&0」が
記録されている「値（Value）」からGUIDを確認
GUID：d8be01aa-b41f-11e7-8155-000c29208375

不明USBメモリのGUID「d8be01aa-b41f-11e7-8155-000c29208375」を確認

自動実行機能の痕跡の確認（MointPoints2）

- レジストリ「NTUSER.DAT」の「MountPoint2」キー配下に、USBメモリのGUIDごとに自動実行機能の設定ファイル（autorun.inf）を認識した痕跡が記録されます。
- 不明なUSBメモリに自動実行機能の痕跡があるか確認します。

◆調査対象のレジストリ

レジストリ：C:¥Documents and Settings¥ユーザー名¥NTUSER.DAT

キー　　：¥Software¥Microsoft¥Windows¥CurrentVersion¥Explorer¥MountPoints2¥{*USBメモリのGUID*}

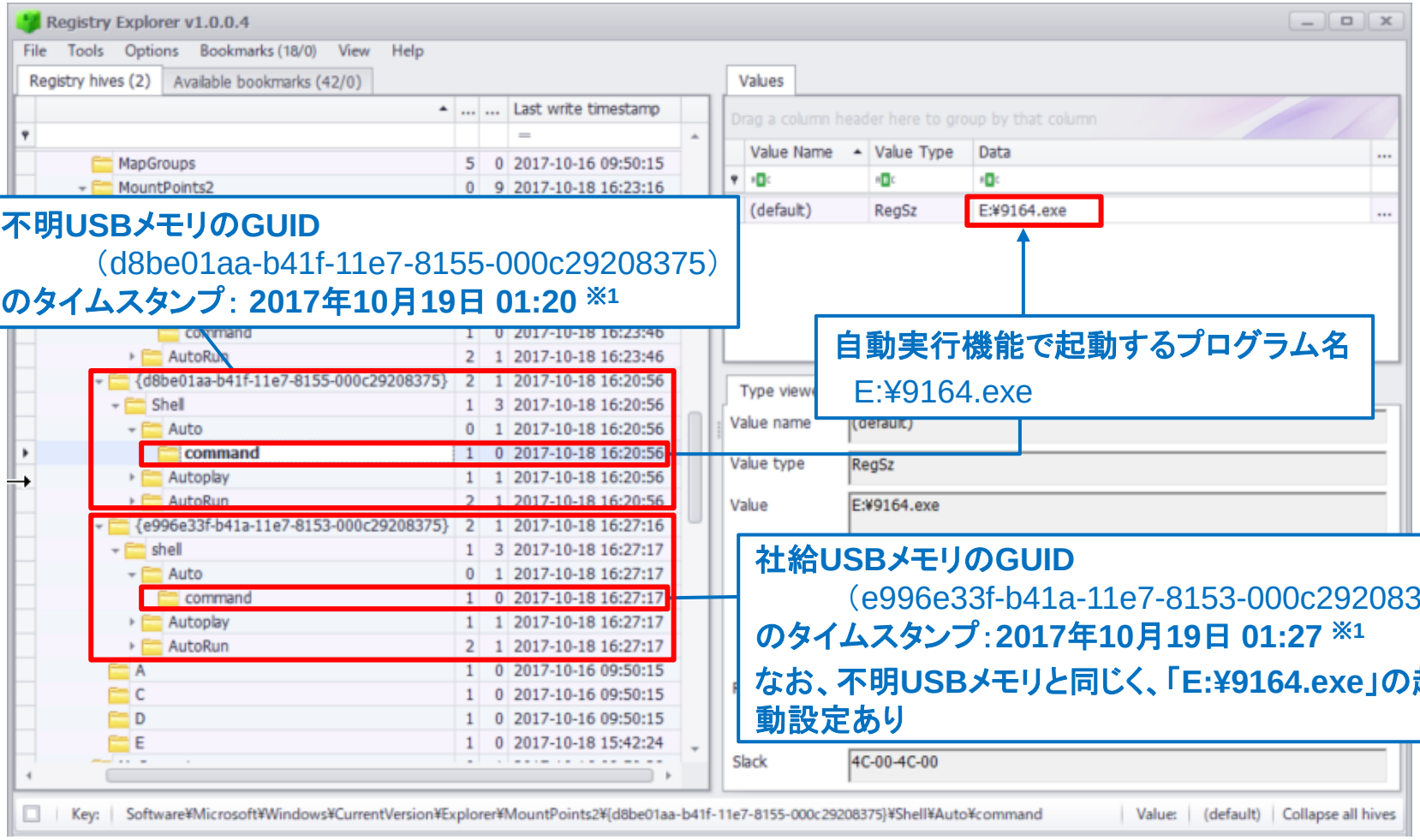
◆調査内容

① USBメモリのGUIDのキーのサブキーを確認し、自動実行機能の設定（プログラム名等）が存在するGUIDを確認する。

② GUIDキーのタイムスタンプ（＝USBメモリの最終接続日時）を確認する。

（注意）「autorun.inf」が格納されたUSBメモリが接続されただけで、レジストリに自動実行の設定内容が記録されるため、マルウェアが実行されたとは限らない。
また、USBメモリから「autorun.inf」を削除した後，USBメモリを再接続すると，レジストリから自動実行設定の痕跡が削除される。

レジストリ「NTUSER.DAT」-「MountPoints2」の確認結果



（※1）Registry Explorerは、タイムスタンプをUTC（協定世界時）で表示するため、日本時間に換算するには+9時間する。

社給USBメモリおよび不明なUSBメモリに、同じ自動実行設定があることを確認

USBメモリの初回接続日時の確認（setupapi.log）

- **「setupapi.log」に、USBメモリの初回接続日時が記録されます。**
- **不明なUSBメモリ（シリアル番号：07083CD4A61B6307）が、工場用パソコンに初めて接続された日時を確認します。**

◆調査対象のファイル

Windows XP　：C:¥Windows¥setupapi.log
Windows 7以降　：C:¥Windows¥Inf¥setupapi.dev.log

◆調査内容

USBメモリのハードウェアチップに記録されている以下の情報がログファイルに記録されます。

- 製造元の識別番号（ベンダーID）
- 製品の識別番号（プロダクトID）
- 個体識別番号（シリアル番号）

（注意）USBメモリのハードウェアチップに記録されている情報です。データの記憶領域には記録されません。
（USBメモリのディスクイメージには記録されていません。）

「setupapi.log」の確認結果

ログが記録された日時（不明なUSBメモリの初回接続日時）

[**2017/10/19 01:17:26** 668.3 Driver Install]
#-019 ハードウェア ID を検索しています: usb¥vid_04bb&pid_1004&rev_0100,usb¥vid_04bb&pid_1004
#-018 互換性のある ID を検索しています:
usb¥class_08&subclass_06&prot_50,usb¥class_08&subclass_06,usb¥class_08
#-198 コマンドラインは処理されました。: C:¥WINDOWS¥system32¥services.exe
#I022 C:¥WINDOWS¥inf¥usbstor.inf で "USB¥Class_08&SubClass_06&Prot_50" が見つかりました; デバイス: "USB 大容量記憶装置デバイス"; ドライバ: "USB 大容量記憶装置デバイス"; プロバイダ: "Microsoft"; Mfg: "互換性のある USB 大容量記憶装置デバイス"; セクション名: "USBSTOR_BULK"
#I023 実際のインストール セクション: [USBSTOR_BULK.NT] ランク: 0x00002000. ドライバ有効開始日: 07/01/2001.
#-166 デバイス インストール関数: DIF_SELECTBESTCOMPATDRV。
#I063 選択されたドライバは "c:¥windows¥inf¥usbstor.inf" のセクション [USBSTOR_BULK] からインストールされます。
#I320 デバイス [redacted] C465-11CF-8056-444553540000}。
#I060 選択した[redacted]
#I058 最も互換性[redacted]
#-166 デバイス インストール関数: DIF_INSTALLDEVICEFILES。
#I124 USB¥ **VID_04BB** & **PID_1004** ¥ **07083CD4A61B6307** のコピーのみのインストールを実行しています。
#-166 デバイス インストール関数: DIF_REGISTER_COINSTALLERS。
#I056 共同インストーラは登録されました。
#-166 デバイス インストール関数: DIF_INSTALLINTERFACES。
#-011 "c:¥windows¥inf¥usbstor.inf" からセクション [USBSTOR_BULK.NT.Interfaces] をインストールしています。
#I054 インターフェイスはインストールされました。
#-166 デバイス インストール関数: DIF_INSTALLDEVICE。
#I123 USB¥VID_04BB&PID_1004¥07083CD4A61B6307 の完全インストールを実行しています。
#I121 USB¥VID_04BB&PID_1004¥07083CD4A61B6307 のデバイス インストールは正しく終了しました。

ベンダーID（コード番号）

プロダクトID（コード番号）

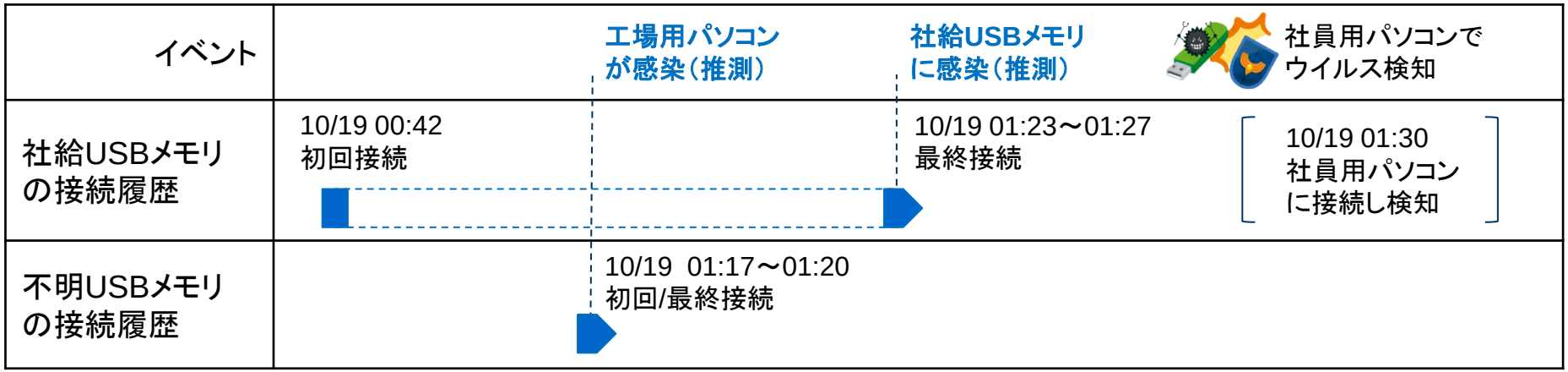
シリアル番号

ここまでの調査結果の整理

- 工場用パソコンに接続されたUSBメモリの痕跡、および自動実行機能の痕跡を踏まえると、不明なUSBメモリからマルウェアに感染した可能性も考えられますが、まだ断定はできません。

◆これまでの調査結果の整理

名称	シリアル番号	Parent Id Prefix	GUID	自動実行設定	接続日時	
					初回	最終
社給USBメモリ	SNDKB91EA4346D408606	8&62f9b79&0	e996e33f-b41a-11e7-8153-000c29208375	E:¥9164.exe	2017/10/19 00:42:17	2017/10/19 01:27:16
不明USBメモリ	07083CD4A61B6307	8&312c0475&0	d8be01aa-b41f-11e7-8155-000c29208375	E:¥9164.exe	2017/10/19 01:17:26	2017/10/19 01:20:56



体験中

プログラム実行履歴の確認（Prefetch）

- プログラムを実行した痕跡は、Prefetchファイル（拡張子.pf）として記録されます。
- 不明なUSBメモリに感染していたマルウェア「9164.exe」が起動した痕跡があるか確認します。

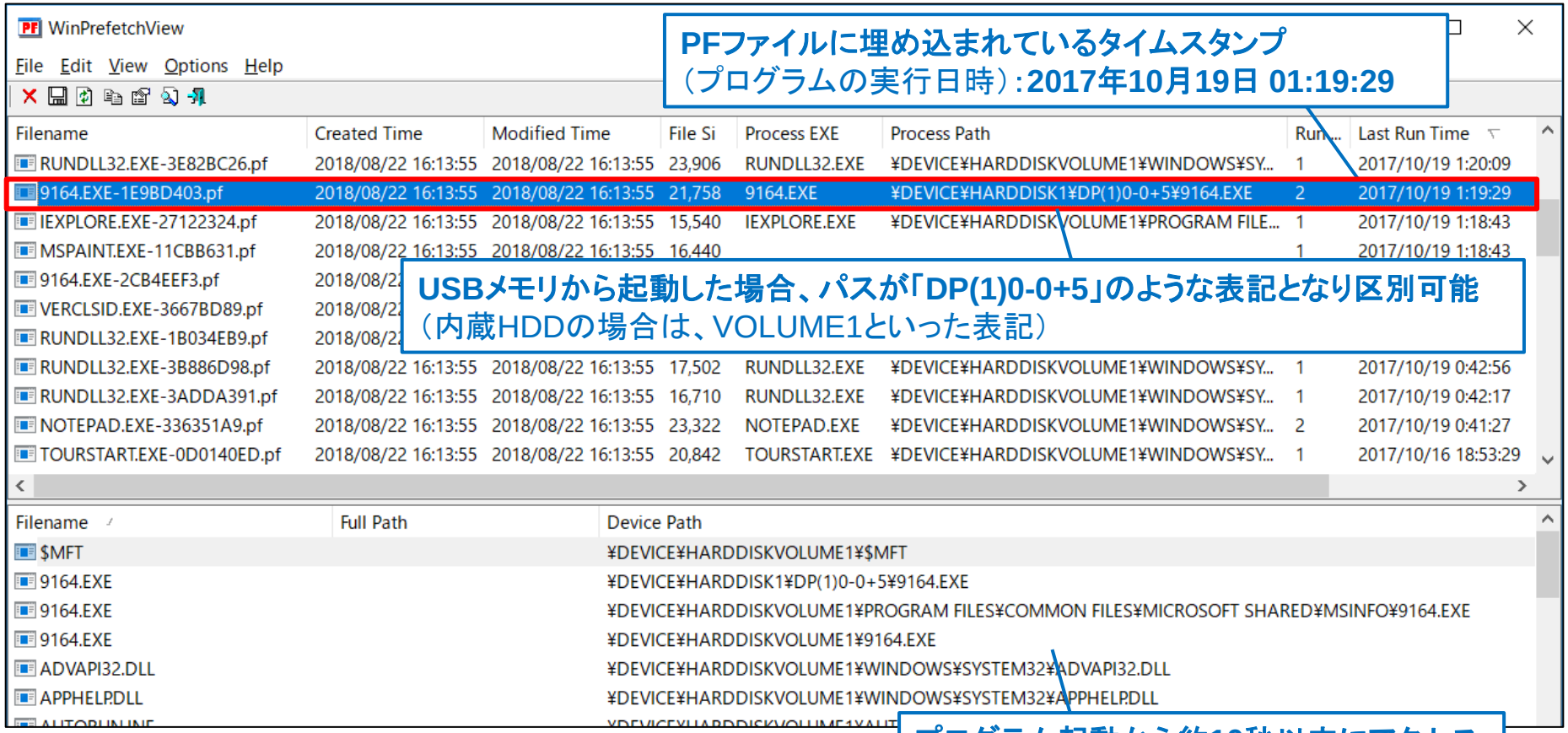
◆調査個所
フォルダ ： C:¥Windows¥Prefetch
ファイル ： *プログラム名-フルパスのハッシュ値*.pf
（例：ABC.EXE-2A07A1F9.pf）

◆調査内容
① マルウェアのPrefetchファイルのタイムスタンプを確認する。
（Prefetchファイルは、プログラム起動の約10秒後に作成される）
② フォレンジックツールでPrefetchファイルに記録されているデータを確認する。

（補足） Windows XPでは、Prefetchファイル（PFファイル）は、最大128個まで保持される。
同じプログラム名で、異なるファイルパスのハッシュが存在する場合、異なるフォルダから実行されたということ。
なお、PFファイルのデータには、最終起動日時、起動回数、起動直後に読み込まれたファイル等が記録されており、
WinPrefetchView等の調査ツールを利用することで解析できる。

「Prefetch」の確認結果

◆ 調査用ツールによるPrefetch確認結果の例（WinPrefetchView）



Filename	Created Time	Modified Time	File Si	Process EXE	Process Path	Run...	Last Run Time
RUNDLL32.EXE-3E82BC26.pf	2018/08/22 16:13:55	2018/08/22 16:13:55	23,906	RUNDLL32.EXE	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SY...	1	2017/10/19 1:20:09
9164.EXE-1E9BD403.pf	2018/08/22 16:13:55	2018/08/22 16:13:55	21,758	9164.EXE	¥DEVICE¥HARDDISK1¥DP(1)0-0+5¥9164.EXE	2	2017/10/19 1:19:29
IEXPLORE.EXE-27122324.pf	2018/08/22 16:13:55	2018/08/22 16:13:55	15,540	IEXPLORE.EXE	¥DEVICE¥HARDDISKVOLUME1¥PROGRAM FILE...	1	2017/10/19 1:18:43
MSPAINT.EXE-11CBB631.pf	2018/08/22 16:13:55	2018/08/22 16:13:55	16,440			1	2017/10/19 1:18:43
9164.EXE-2CB4EEF3.pf	2018/08/2						
VERCLSID.EXE-3667BD89.pf	2018/08/2						
RUNDLL32.EXE-1B034EB9.pf	2018/08/2						
RUNDLL32.EXE-3B886D98.pf	2018/08/22 16:13:55	2018/08/22 16:13:55	17,502	RUNDLL32.EXE	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SY...	1	2017/10/19 0:42:56
RUNDLL32.EXE-3ADDA391.pf	2018/08/22 16:13:55	2018/08/22 16:13:55	16,710	RUNDLL32.EXE	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SY...	1	2017/10/19 0:42:17
NOTEPAD.EXE-336351A9.pf	2018/08/22 16:13:55	2018/08/22 16:13:55	23,322	NOTEPAD.EXE	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SY...	2	2017/10/19 0:41:27
TOURSTART.EXE-0D0140ED.pf	2018/08/22 16:13:55	2018/08/22 16:13:55	20,842	TOURSTART.EXE	¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SY...	1	2017/10/16 18:53:29

Filename	Full Path	Device Path
$MFT		¥DEVICE¥HARDDISKVOLUME1¥$MFT
9164.EXE		¥DEVICE¥HARDDISK1¥DP(1)0-0+5¥9164.EXE
9164.EXE		¥DEVICE¥HARDDISKVOLUME1¥PROGRAM FILES¥COMMON FILES¥MICROSOFT SHARED¥MSINFO¥9164.EXE
9164.EXE		¥DEVICE¥HARDDISKVOLUME1¥9164.EXE
ADVAPI32.DLL		¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥ADVAPI32.DLL
APPHELP.DLL		¥DEVICE¥HARDDISKVOLUME1¥WINDOWS¥SYSTEM32¥APPHELP.DLL

NirSoft WinPrefetchView
https://www.nirsoft.net/utils/win_prefetch_view.html

不明なUSBメモリが接続された直後に、マルウェアが起動したことを確認

体験終了

ここまでの調査結果

- **工場用パソコンの作業履歴を確認したところ、「不明なUSBメモリ」は、パソコンの保守を委託している会社が持ち込んだものであることが確認できました。**
- **委託先のパソコンがマルウェアに感染している可能性があるため、委託先と連携し、調査を進めることとしました。**
  - 本事案のエビデンスは、実習用仮想マシンの「/var/samba/public/bonus/」に保存してありますので、お時間のある時に、調査に挑戦してみてください。

「体験」はここで終了です。
ご愛読いただき、ありがとうございました。

1.USBメモリからの感染時の挙動

2.ウェブサイトからの感染時の挙動

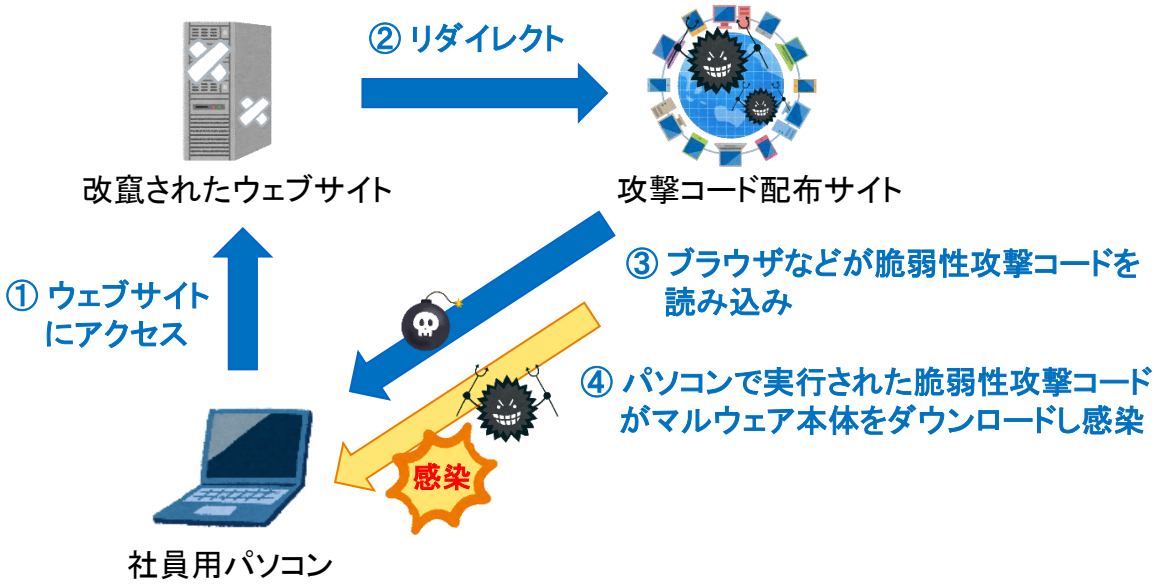
3.メールからの感染時の挙動

4.感染後の挙動（感染永続化）

感染経路の概要

- **脆弱性があるパソコンは、ウェブサイトを閲覧しただけで感染する可能性があります。**
  ① 攻撃者は、第三者のウェブサイトに不正アクセスし、「攻撃コード配布サイト」に自動転送するようコンテンツを改ざんします。
  ② 改ざんされたウェブサイトにアクセスしたパソコンは、攻撃コード配布サイトにリダイレクトされます。
  ③ 攻撃コード配布サイトは、脆弱性攻撃コードが起動するように細工したコンテンツをブラウザなどに読み込ませます。
  ④ 起動に成功した脆弱性攻撃コードは、マルウェア本体をダウンロードし感染します。

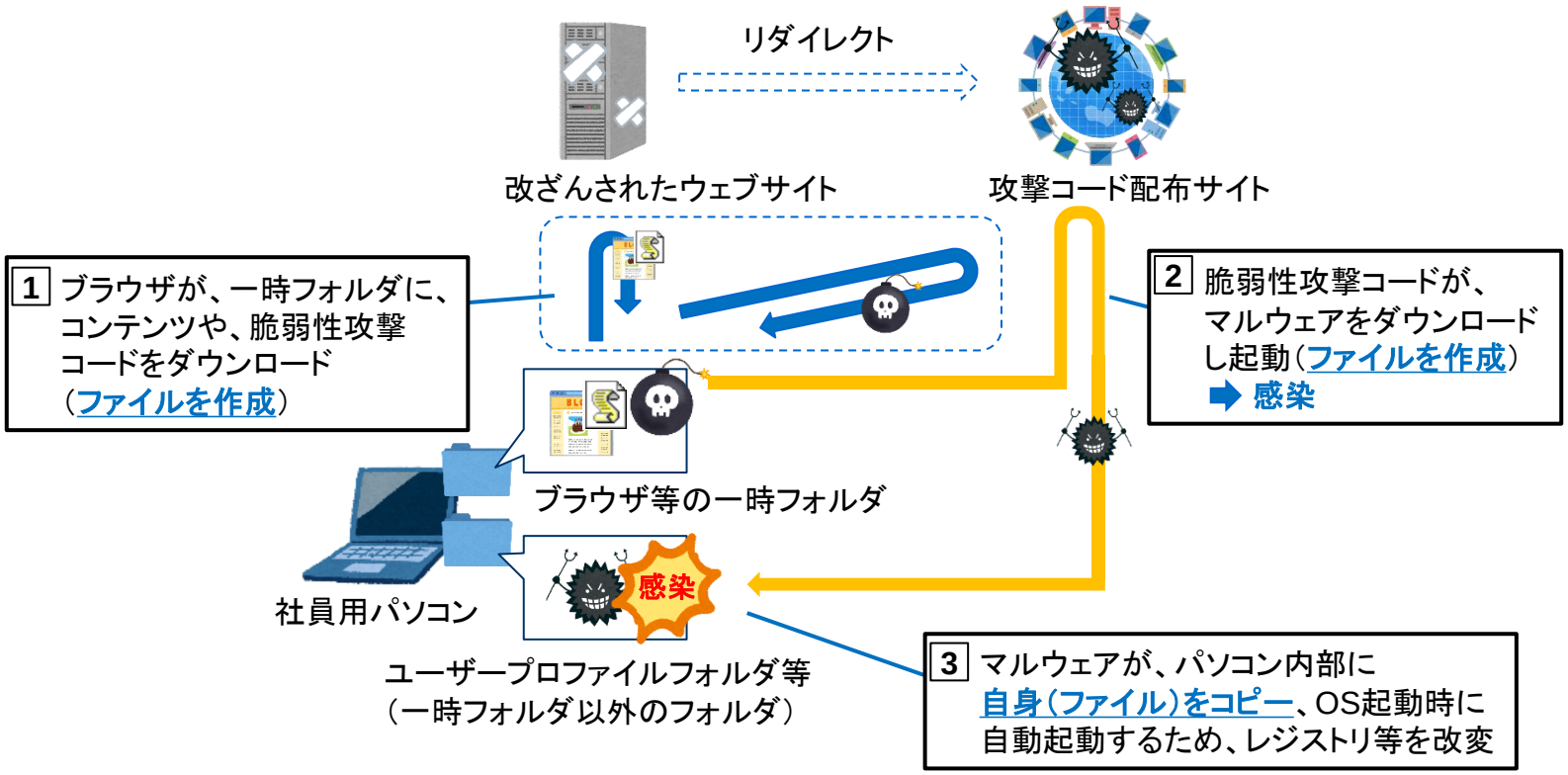
◆感染経路の概要



感染時の挙動と痕跡の概要

- 感染時の挙動と、調査に役立つ痕跡が残る個所を下図に示します。
- マルウェアによる「ファイルアクセスが発生するタイミング」を理解することで、ウイルス検知アラートから状況を推測することができます。

◆感染時の挙動と痕跡の概要



ウイルス検知アラートの特徴

- 検出ファイルのパスが、「ブラウザ関連の一時フォルダ」となります。

◆ ウイルス検知アラートの例

項目	内容の例
検知日時	2018年9月8日13:30
脅威名	SWF_AXPERGLE.VZ
検出ファイル名	C:¥Users¥User10¥AppData¥Local¥Microsoft¥Windows **¥Temporary Internet Files**¥Low¥Content.IE5¥43MHHANH¥**QirRgZ[1].swf**
検査の種類	リアルタイムスキャン
処理結果	隔離
検出コンピュータ名	PC0010

Internet Explorerの一時フォルダにダウンロードされたファイル（Adobe Flash形式、拡張子.swf）を検知していることから、ウェブサイトからダウンロードされた脆弱性攻撃コードの検知と推測できる。

ブラウザ関連の一時フォルダ

- **ブラウザは、ウェブサイトのコンテンツを一時フォルダにダウンロードしてから、メモリに読み込みします。**
  - 2回目以降のウェブアクセスでは、一時フォルダのファイル（キャッシュ）にアクセスします。

◆ ブラウザ関連の一時フォルダの例

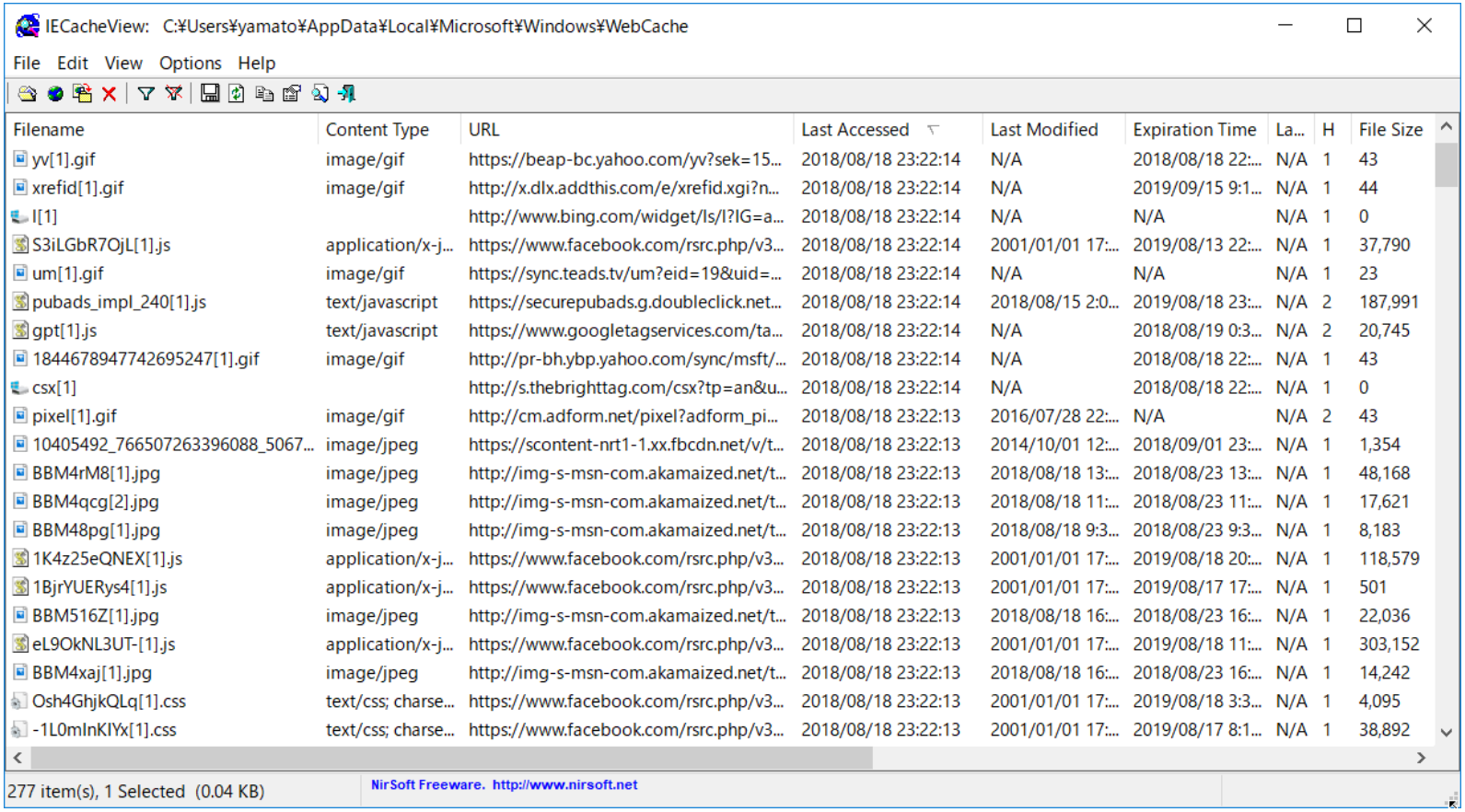
ソフトウェア		フォルダ
Internet Explorer	IE 8-11（Windows7）	C:¥Users¥*【ユーザー名】*¥AppData¥Local¥Microsoft¥Windows¥Temporary Internet Files¥Content.IE5※1
	IE 11（Windows8 以降）	C:¥Users¥*【ユーザー名】*¥AppData¥Local¥Microsoft¥Windows¥INetCache※2
Firefox 32.0以降		C:¥Users¥*【ユーザー名】*¥AppData¥Local¥Mozilla¥Firefox¥Profiles¥*【プロファイル名】*.default¥cache2
Chrome		C:¥Users¥*【ユーザー名】*¥AppData¥Local¥Google¥Chrome¥User Data¥Default¥Cache
Java Applet		C:¥Users¥*【ユーザー名】*¥AppData¥LocalLow¥Sun¥Java¥Deployment¥cache¥6.0¥

（※1）保護モード/UACが有効の場合は、［前略］¥Temporary Internet Files¥Low¥Content.IE5
（※2）後述する調査用ツールで解析する場合は、C:¥Users¥【ユーザー名】¥AppData¥Local¥Microsoft¥Windows¥WebCache¥ を指定

（参考）ブラウザのキャッシュ解析ツール

- 調査用ツール※1で一時フォルダを解析すると、キャッシュのダウンロード元URL、アクセス日時などを確認することができます。

◆ ブラウザのキャッシュ解析ツールの例（IECacheView）



Filename	Content Type	URL	Last Accessed	Last Modified	Expiration Time	La...	H	File Size
yv[1].gif	image/gif	https://beap-bc.yahoo.com/yv?sek=15...	2018/08/18 23:22:14	N/A	2018/08/18 22:...	N/A	1	43
xrefid[1].gif	image/gif	http://x.dlx.addthis.com/e/xrefid.xgi?n...	2018/08/18 23:22:14	N/A	2019/09/15 9:1...	N/A	1	44
I[1]		http://www.bing.com/widget/ls/I?IG=a...	2018/08/18 23:22:14	N/A	N/A	N/A	1	0
S3iLGbR7OjL[1].js	application/x-j...	https://www.facebook.com/rsrc.php/v3...	2018/08/18 23:22:14	2001/01/01 17:...	2019/08/13 22:...	N/A	1	37,790
um[1].gif	image/gif	https://sync.teads.tv/um?eid=19&uid=...	2018/08/18 23:22:14	N/A	N/A	N/A	1	23
pubads_impl_240[1].js	text/javascript	https://securepubads.g.doubleclick.net...	2018/08/18 23:22:14	2018/08/15 2:0...	2019/08/18 23:...	N/A	2	187,991
gpt[1].js	text/javascript	https://www.googletagservices.com/ta...	2018/08/18 23:22:14	N/A	2018/08/19 0:3...	N/A	2	20,745
184467894774269524 7[1].gif	image/gif	http://pr-bh.ybp.yahoo.com/sync/msft/...	2018/08/18 23:22:14	N/A	2018/08/18 22:...	N/A	1	43
csx[1]		http://s.thebrighttag.com/csx?tp=an&u...	2018/08/18 23:22:14	N/A	2018/08/18 22:...	N/A	1	0
pixel[1].gif	image/gif	http://cm.adform.net/pixel?adform_pi...	2018/08/18 23:22:13	2016/07/28 22:...	N/A	N/A	2	43
10405492_766507263396088_5067...	image/jpeg	https://scontent-nrt1-1.xx.fbcdn.net/v/t...	2018/08/18 23:22:13	2014/10/01 12:...	2018/09/01 23:...	N/A	1	1,354
BBM4rM8[1].jpg	image/jpeg	http://img-s-msn-com.akamaized.net/t...	2018/08/18 23:22:13	2018/08/18 13:...	2018/08/23 13:...	N/A	1	48,168
BBM4qcg[2].jpg	image/jpeg	http://img-s-msn-com.akamaized.net/t...	2018/08/18 23:22:13	2018/08/18 11:...	2018/08/23 11:...	N/A	1	17,621
BBM48pg[1].jpg	image/jpeg	http://img-s-msn-com.akamaized.net/t...	2018/08/18 23:22:13	2018/08/18 9:3...	2018/08/23 9:3...	N/A	1	8,183
1K4z25eQNEX[1].js	application/x-j...	https://www.facebook.com/rsrc.php/v3...	2018/08/18 23:22:13	2001/01/01 17:...	2019/08/18 20:...	N/A	1	118,579
1BjrYUERys4[1].js	application/x-j...	https://www.facebook.com/rsrc.php/v3...	2018/08/18 23:22:13	2001/01/01 17:...	2019/08/17 17:...	N/A	1	501
BBM516Z[1].jpg	image/jpeg	http://img-s-msn-com.akamaized.net/t...	2018/08/18 23:22:13	2018/08/18 16:...	2018/08/23 16:...	N/A	1	22,036
eL9OkNL3UT-[1].js	application/x-j...	https://www.facebook.com/rsrc.php/v3...	2018/08/18 23:22:13	2001/01/01 17:...	2019/08/18 11:...	N/A	1	303,152
BBM4xaj[1].jpg	image/jpeg	http://img-s-msn-com.akamaized.net/t...	2018/08/18 23:22:13	2018/08/18 16:...	2018/08/23 16:...	N/A	1	14,242
Osh4GhjkQLq[1].css	text/css; charse...	https://www.facebook.com/rsrc.php/v3...	2018/08/18 23:22:13	2001/01/01 17:...	2019/08/18 3:3...	N/A	1	4,095
-1L0mInKIYx[1].css	text/css; charse...	https://www.facebook.com/rsrc.php/v3...	2018/08/18 23:22:13	2001/01/01 17:...	2019/08/17 8:1...	N/A	1	38,892

（※1）NirSoft IECacheView（IE用）、MozillaCacheView（Firefox用）、 ChromeCacheView（Chrome用）
https://www.nirsoft.net/web_browser_tools.html

ウイルス検知アラートからの状況推測（1）

- **ブラウザ関連の一時フォルダから「リアルタイムスキャン」で検知した場合、ファイル名やパスなどから攻撃の進行状況（下図①～③）を判断し、感染の可能性を推測します。**

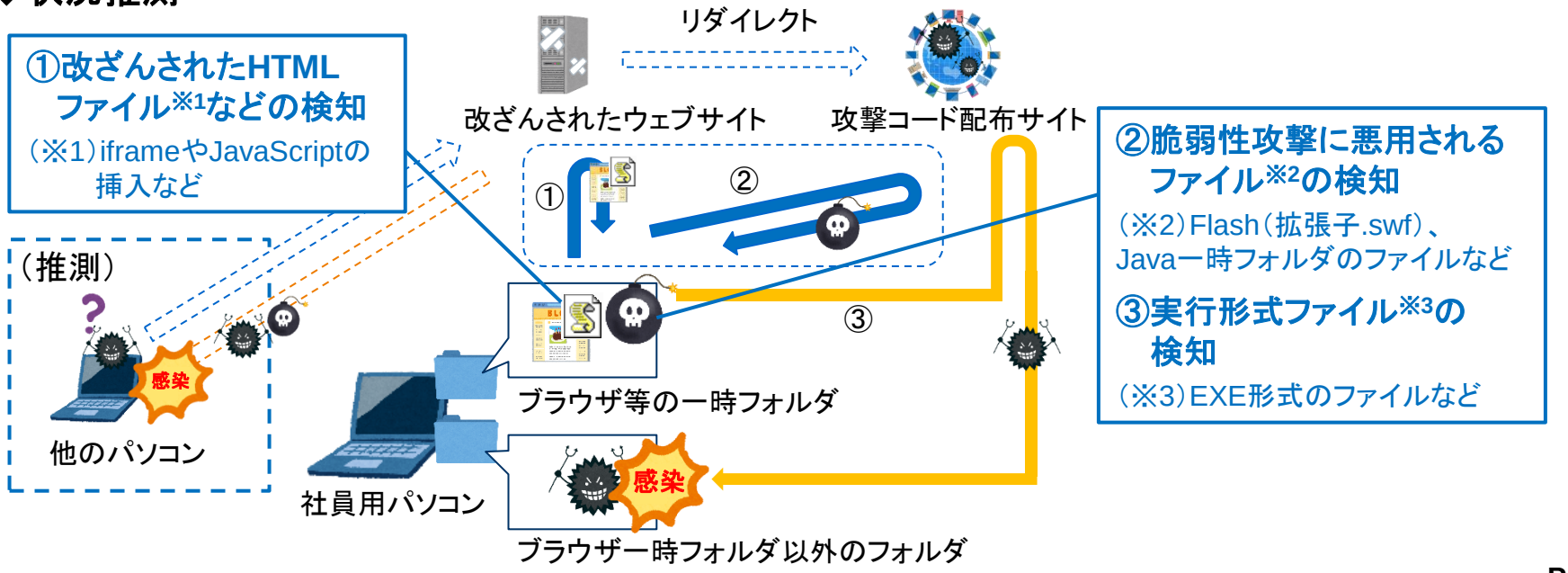
  ①～②　：感染前に防御できた可能性があると推測できます。

  ③　　：利用者がダウンロードしたファイルにマルウェアが混入していた可能性、または脆弱性攻撃が成功し、マルウェアがダウンロードされた可能性があります。

  ➡ 状況を確認し、脆弱性攻撃が疑われる場合、「ダウンロードされた複数のマルウェアの一部」のみを検知できた可能性もあるため、パソコンを隔離したうえで調査します。

  また、プロキシログなどから特定した不審URLを遮断したうえでアクセス状況を調査します。

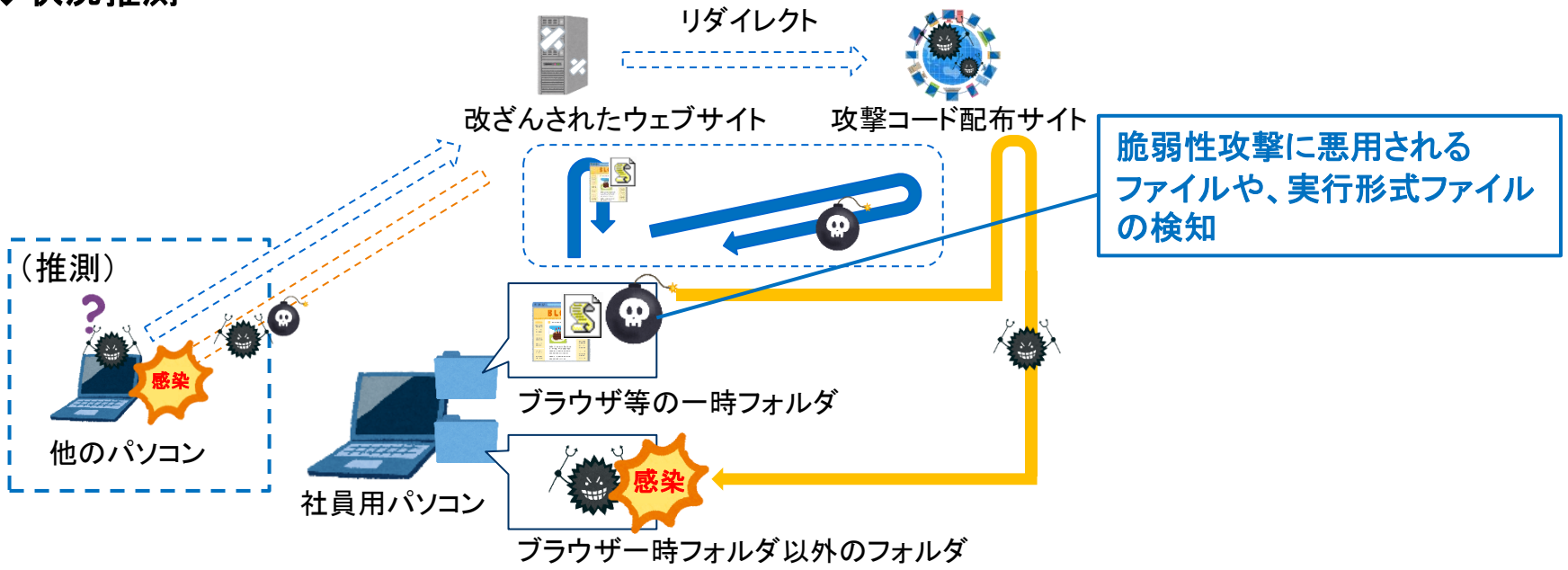
◆状況推測



ウイルス検知アラートからの状況推測（2）

- **ブラウザ関連の一時フォルダから「オンデマンドスキャン」で検知した場合、ウイルス対策ソフトで検知できなかった「過去のある時点」で感染した可能性があります。**
  - ➡ パソコンが感染している可能性があるため、パソコンを隔離したうえで調査します。
    また、調査により特定した不審URLを遮断したうえで、アクセス状況を調査します。

◆状況推測



（参考）ブラウザの閲覧履歴

- **ブラウザの閲覧履歴は、下表のファイルに記録されています。**
  - ブラウザをプライベートモードで起動した場合や、ブラウザの終了時に閲覧履歴を削除する設定にしている場合は、履歴が保存されません。

◆ ブラウザの閲覧履歴ファイル

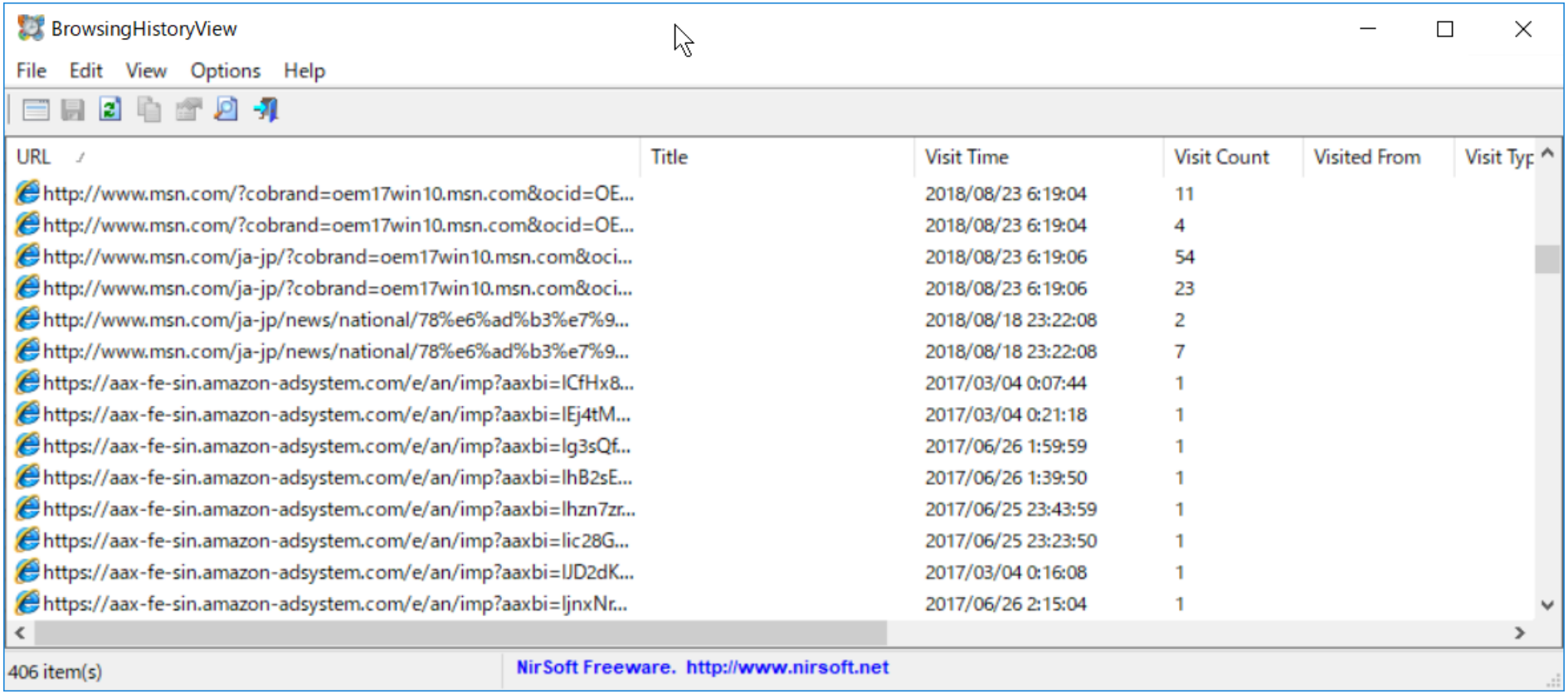
ソフトウェア		フォルダ
Internet Explorer	IE 8-9	［全体履歴］※1 C:¥Users¥*【ユーザー名】*¥AppData¥Local¥Microsoft¥Windows¥History¥History.IE5¥index.dat
		［週・日単位の履歴］※1 C:¥Users¥*【ユーザー名】*¥AppData¥Local¥Microsoft¥Windows¥History¥History.IE5¥MSHist01*【yyyymmddyyyymmdd】*[*2]¥index.dat
	IE 10-11	C:¥Users¥*【ユーザー名】*¥AppData¥Local¥Microsoft¥Windows¥WebCache¥WebCacheV01.dat
Firefox		C:¥Users¥*【ユーザー名】*¥AppData¥Roaming¥Mozilla¥Firefox¥Profiles¥*【プロファイル名】*.default¥places.sqlite
Chrome		C:¥Users¥*【ユーザー名】*¥AppData¥Local¥Google¥Chrome¥User Data¥Default¥History

（※1）保護モード/UACが有効の場合は，[前略] ¥History.IE5¥Low フォルダ配下となる。

（参考）ブラウザの閲覧履歴ファイルの解析ツール

- ブラウザの閲覧履歴は、調査用ツール※1を利用すると、アクセスしたURLと日時を確認することができます。

◆ ブラウザ閲覧履歴の解析ツールの例（Browsing History View）

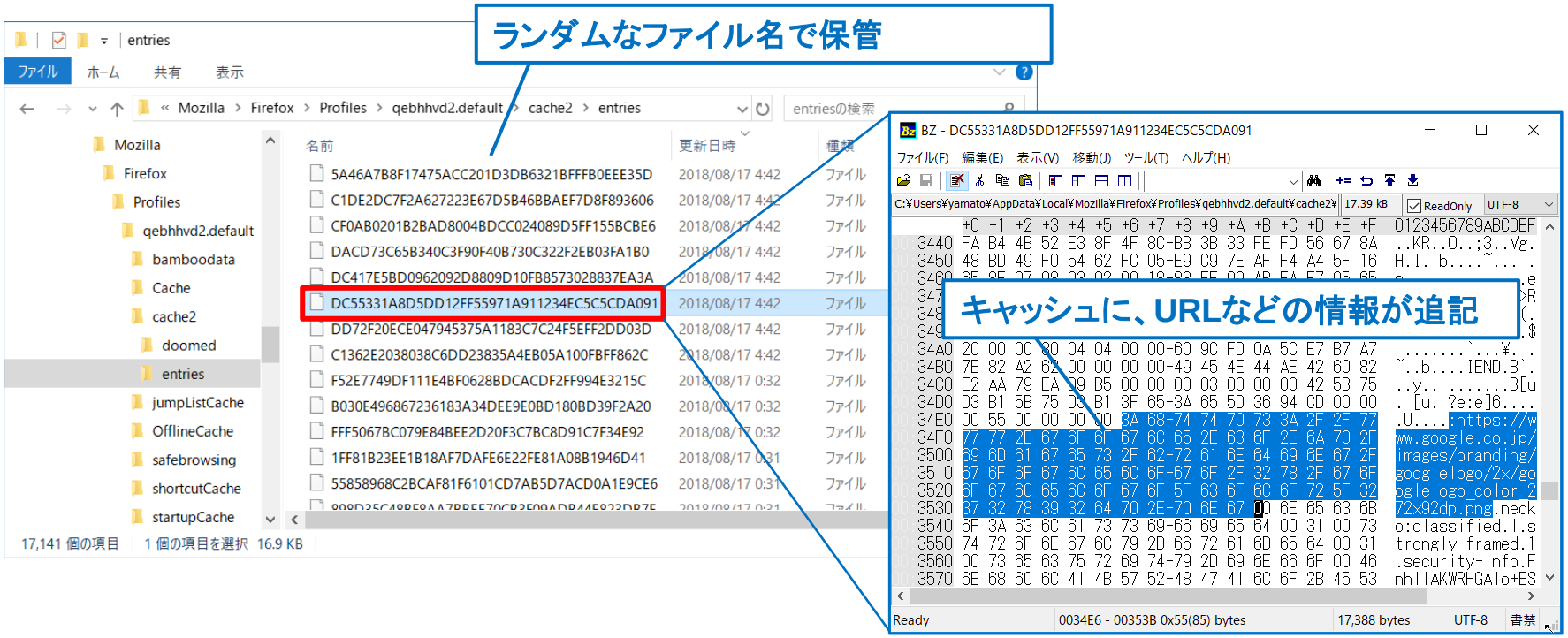


（※1）NirSoft BrowsingHistoryView https://www.nirsoft.net/utils/browsing_history_view.html

（参考）Firefoxのキャッシュ

- **Firefoxの一時フォルダのキャッシュは、ランダムなファイル名で保管されます。**
  - もとのファイル名を確認する場合は、フォレンジックツール※1を利用します。
- **また、各キャッシュに、ダウンロード元のURLなどの情報が追記されます。**

◆ **Firefoxの一時フォルダ**



（※1）ツールの例　NirSoft MozillaCacheView
https://www.nirsoft.net/utils/mozilla_cache_viewer.html

（参考）Java Appletのキャッシュ

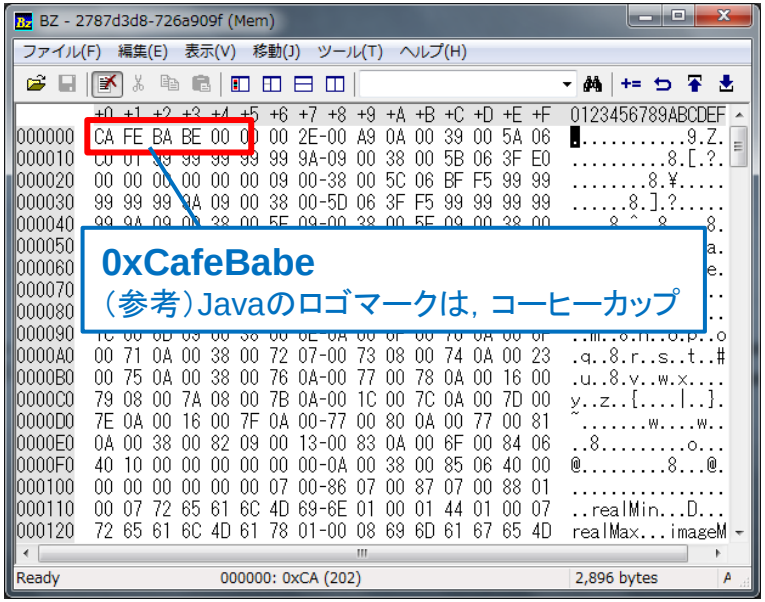
- **Java Appletの一時フォルダには、以下の2種類のファイルがキャッシュとして保管されます。**

  ［キャッシュの一例］（ファイル名はランダムな英数字）

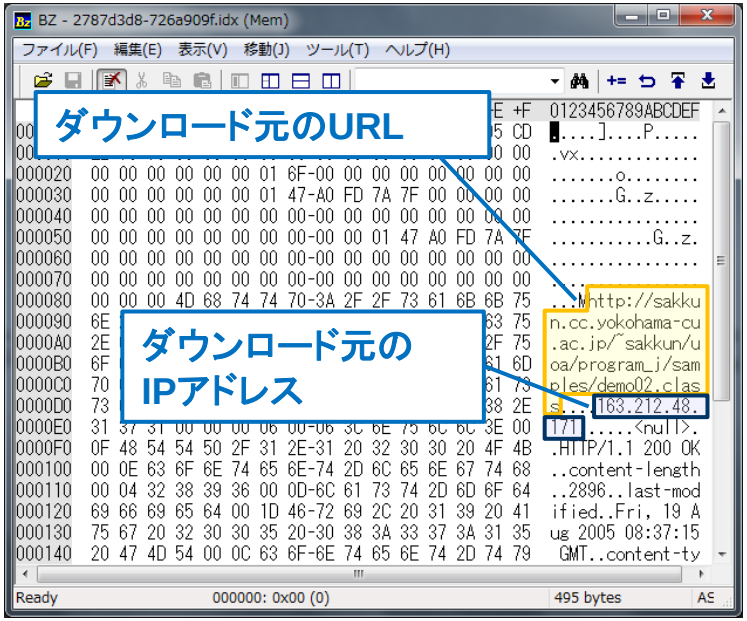
  ① 2787d3d8-726a909f
  - Java Classファイル（ファイルシグネチャ0xCA FE BA BE）
  - またはJARファイル（ファイルシグネチャ 0x50 4B=“PK” ）

  ② 2787d3d8-726a909f.idx
  - Java Classファイルのダウンロード元のURL、IPアドレスなどの情報が記録されます。

◆Java Classファイル



◆Java idxファイル



1.USBメモリからの感染時の挙動

2.ウェブサイトからの感染時の挙動

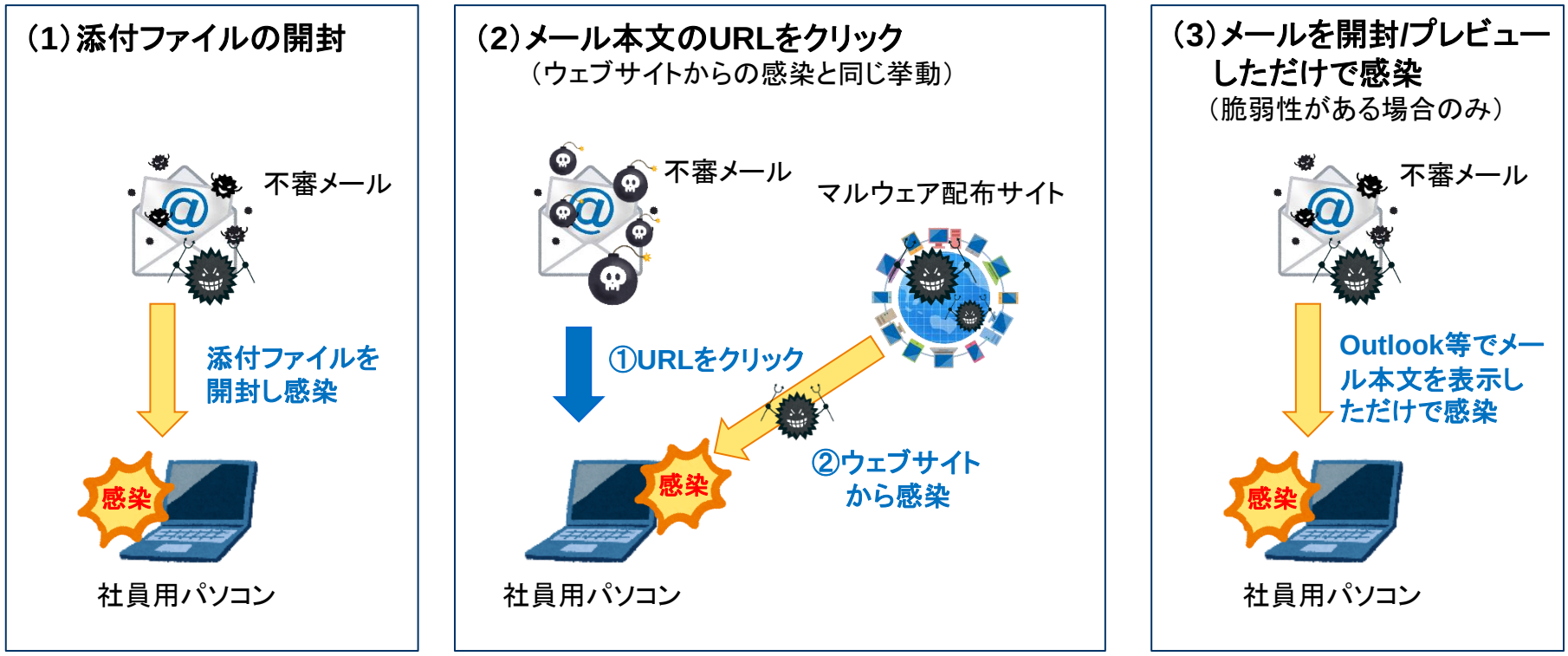
3.メールからの感染時の挙動

4.感染後の挙動（感染永続化）

感染経路の概要

- 利用者が、不審メールの添付ファイルを開封したり、メール本文に記載されたURLをクリックしたりすることでマルウェアに感染します。
- また、Outlookなどのメールソフトの脆弱性がある場合は、メール本文を表示しただけで感染することもあります。

◆感染経路の概要

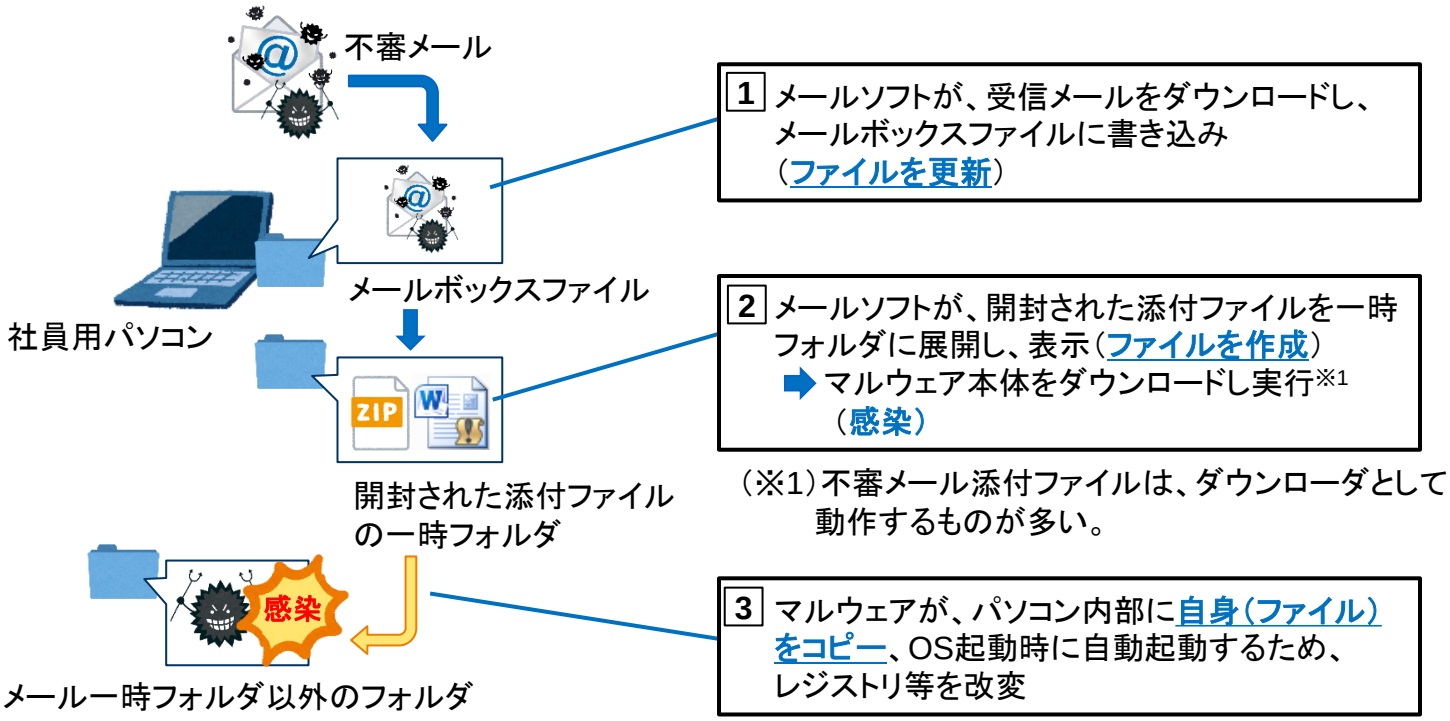


感染時の挙動と痕跡の概要

- 感染時の挙動と、調査に役立つ痕跡が残る個所を下図に示します。
- マルウェアによる「ファイルアクセスが発生するタイミング」を理解することで、ウイルス検知アラートから状況を推測することができます。

◆感染時の挙動と痕跡の概要

（メール本文のURLをクリックした場合は、ウェブサイトからの感染と同じ挙動）



ウイルス検知アラートの特徴

- 検出ファイルのパスが、「メール関連の一時フォルダ」となります。

◆ ウイルス検知アラートの例

項目	内容の例
検知日時	2018年9月8日13:30
脅威名	JS_POWLOAD.ELDSAUJQ
検出ファイル名	C:¥Users¥User10¥AppData¥Local¥Microsoft¥Windows¥Temporary Internet Files¥**Content.Outlook**¥BNTENH3O¥**請求書.zip**
検査の種類	リアルタイムスキャン
処理結果	隔離
検出コンピュータ名	PC0010

Outlookの添付ファイル一時フォルダのファイルを検知していることから、不審メール添付ファイルを開封したものと推測できる。

メール関連の一時フォルダ

- **メールボックスファイルと、メール添付ファイル開封時の一時フォルダを例示します。**

◆ メール関連の一時フォルダ

<table>
<tr><th colspan="2">ソフトウェア</th><th>メールボックスファイル</th><th>メール添付ファイル一時フォルダ</th></tr>
<tr><td rowspan="2">Microsoft Outlook</td><td>Windows7</td><td rowspan="2">C:¥Users¥【ユーザー名】¥Documents¥Outlook ファイル¥
　または
C:¥Users¥【ユーザー名】¥AppData¥Local¥Microsoft¥Outlook¥
　POPの場合　　:【メールアドレス】.pst
　IMAP等の場合　:【メールアドレス】.ost</td><td>C:¥Users¥【ユーザー名】¥AppData¥Local¥Microsoft¥Windows¥Temporary Internet Files¥Content.Outlook¥</td></tr>
<tr><td>Windows8以降</td><td>C:¥Users¥【ユーザー名】¥AppData¥Local¥Microsoft¥Windows¥INetCache¥Content.Outlook¥</td></tr>
<tr><td colspan="2">Thunderbird</td><td>C:¥Users¥【ユーザー名】¥AppData¥Roaming¥Thunderbird¥Profiles¥【プロファイル名】.default¥
　POP　　:Mail¥【メールサーバ名】¥
　IMAP等　:ImapMail¥【メールサーバ名】¥
上記フォルダにあるメールフォルダ名のMBOX形式ファイル（拡張子なし）に記録</td><td>C:¥Users¥【ユーザー名】¥AppData¥Local¥Temp¥</td></tr>
<tr><td colspan="2">ZIPファイル
（Explorerで開いた場合）</td><td colspan="2">• メールに添付されたZIPに格納されているファイル一覧を表示すると、上記の一時フォルダにZIPファイルが作成される。
• 続いてZIPに格納されているファイルをダブルクリックして開くと、ZIPファイルが以下のフォルダに展開（解凍）されたうえで、ファイルの内容が表示される。
C:¥Users¥【ユーザー名】¥AppData¥Local¥Temp¥Temp【半角数字1桁】_【ファイル名】.zip¥</td></tr>
</table>

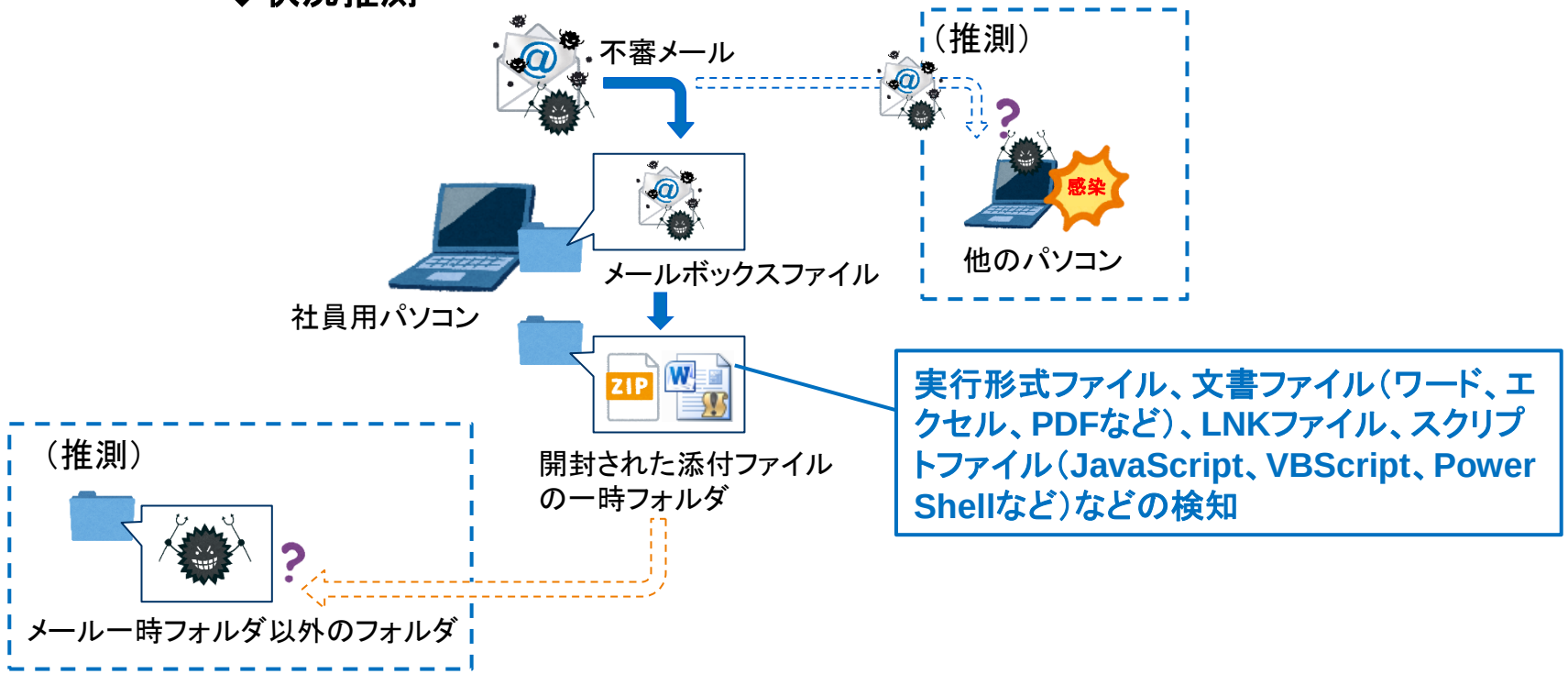
ウイルス検知アラートからの状況推測

- **メール関連の一時フォルダから「リアルタイムスキャン」で検知した場合、不審メール添付ファイルの開封時に防御できた（感染していない）可能性があります。**

  ➡ パソコンの操作状況を確認し、感染の可能性を判断します。

  不審メール添付ファイルの通信先を特定し、プロキシサーバなどで遮断します。
  また、プロキシログなどを調査し、他のパソコンから開封による通信が発生していないか確認します。（パターンファイル対応前に、不審メールを開封したパソコンがいないかを確認）

◆状況推測

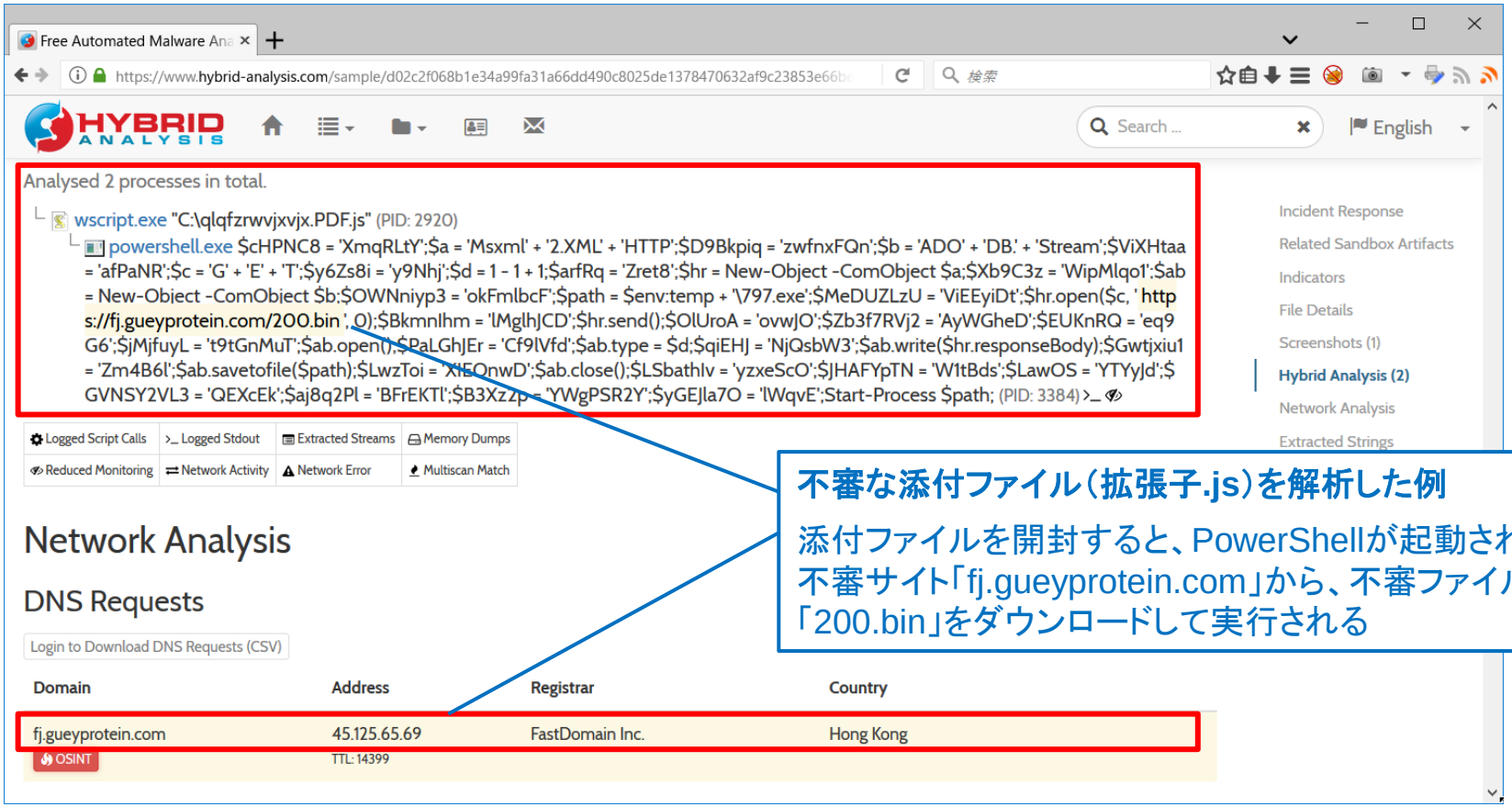


（参考）マルウェア検体の解析サービス

- クラウドの解析サービスを利用すると、不審メール添付ファイルの通信先を簡単に特定することができます。

◆ **Hybrid-Analysis**

https://www.hybrid-analysis.com/



不審な添付ファイル（拡張子.js）を解析した例

添付ファイルを開封すると、PowerShellが起動され、不審サイト「fj.gueyprotein.com」から、不審ファイル「200.bin」をダウンロードして実行される

1.USBメモリからの感染時の挙動

2.ウェブサイトからの感染時の挙動

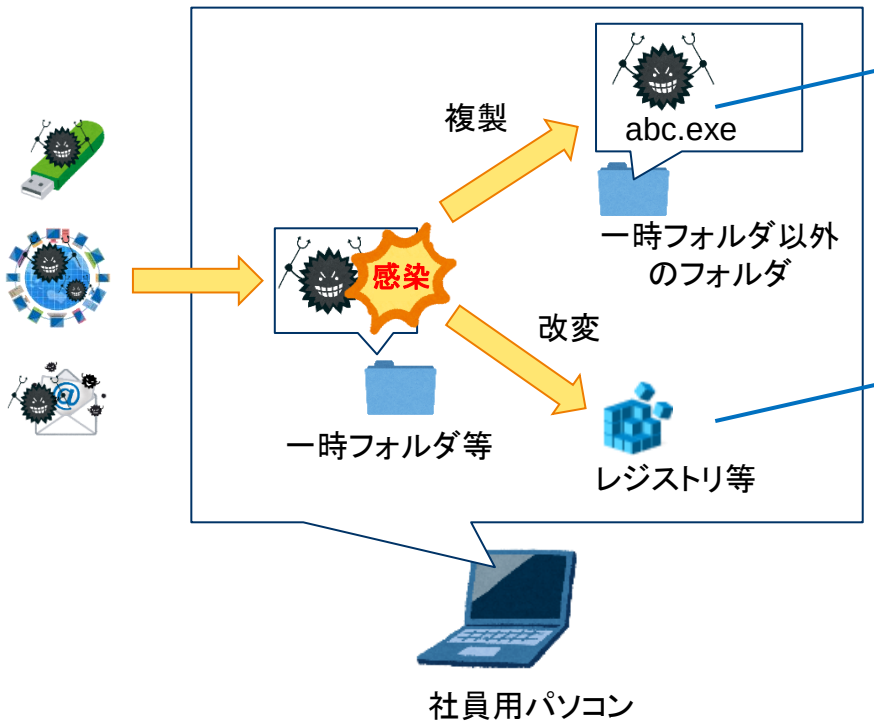
3.メールからの感染時の挙動

4.感染後の挙動（感染永続化）

感染後の挙動（感染永続化）の概要

- **感染したマルウェアの挙動はさまざまですが、ほとんどのマルウェアは、OSが再起動されても活動を継続できるよう、システムを改変します。**
  - 本講座では、このような挙動を「感染の永続化」と呼びます。

◆感染永続化の概要



1 何らかの手段により感染（起動）したマルウェアは、自身をシステムフォルダなどに複製※1（ファイルを作成）

（※1）一時フォルダのファイルは、名前のとおり、一時的に利用されるものであり、何らかのタイミングで消去される可能性があるため

2 OS起動の都度、マルウェアが起動するようレジストリの自動起動設定などを改変

ウイルス検知アラートの特徴

- **検出ファイルのパスが、システムフォルダなど「一時フォルダ以外のフォルダ」の場合、感染している可能性があります。**

◆ **ウイルス検知アラートの例**

項目	内容の例
検知日時	2018年9月8日9:00
脅威名	TSPY_URSNIF.TIBAIDD
検出ファイル名	**C:¥Users¥*【ユーザー名】*¥AppData¥Roaming¥Microsoft¥Api-spex** ¥BWCorpol.exe
検査の種類	リアルタイムスキャン
処理結果	隔離
検出コンピュータ名	PC0010

USBメモリ、ウェブサイトの一時フォルダ、メール添付ファイルなどの一時フォルダに該当しない。

どうしてこのフォルダにマルウェアのファイルが作成されたのか分からない場合は、感染を疑う。

マルウェアが複製されるフォルダ

- **一般的なマルウェアは、システムフォルダ、ユーザープロファイルフォルダなど、「一時フォルダ以外のフォルダ」に複製を作成します。**

◆ **マルウェアが複製されるフォルダの例**

分類	フォルダ
システムフォルダ	C:¥Windows¥System32¥ などのフォルダ
ユーザープロファイルフォルダ	C:¥Users¥*【ユーザー名】*¥ 配下のフォルダ ［一例］ • C:¥Users¥*【ユーザー名】*¥ • C:¥Users¥*【ユーザー名】*¥AppData¥Roaming¥ • C:¥Users¥*【ユーザー名】*¥AppData¥Roaming¥Microsoft¥Api-spex¥ （正規プログラムに成りすますため、既存フォルダを利用することもある）

自動起動設定の改変

- また、OSの起動時にマルウェアが起動するよう、レジストリなどを改変します。

◆ 自動起動設定の例

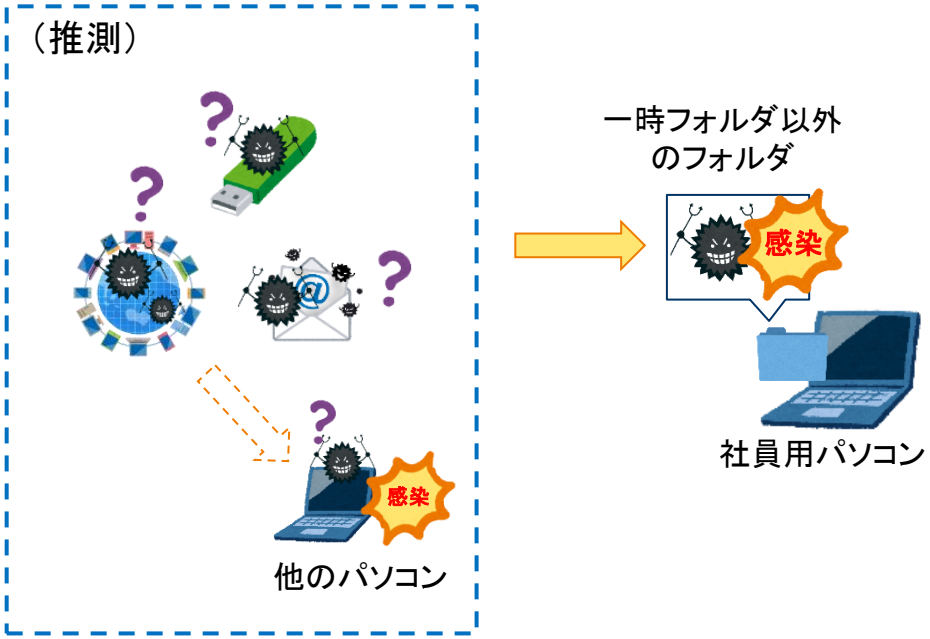
分類	フォルダ
レジストリ	レジストリ NTUSER.DAT ¥Software¥Microsoft¥Windows¥CurrentVersion¥Run ¥Software¥Microsoft¥Windows¥CurrentVersion¥RunOnece レジストリ SOFTWARE ¥Microsoft¥Windows¥CurrentVersion¥Run ¥Microsoft¥Windows¥CurrentVersion¥RunOnece レジストリ SYSTEM ¥CurrentControlSet¥Services
タスク	C:¥Windows¥System32¥Tasks

ウイルス検知アラートからの状況推測

- オンデマンドスキャンや、OS起動直後のリアルタイムスキャンなどにより、感染していたマルウェアを検知した場合、ウイルス検知アラートの情報だけで感染経路を推測することは困難です。

  ➡ 感染経路や影響範囲を特定するため、タイムライン解析などの調査を行います。

◆状況推測



第3章. タイムライン解析の基礎

この章では、感染パソコンにおいて、「いつ」、「何が起きたのか」を時系列で調査する「タイムライン解析」というフォレンジック調査手法について学習します。

状況把握に役立つ技術「フォレンジック」

- 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。
- サイバー攻撃の状況は目に見えづらいですが、フォレンジック技術を活用することで、「状況を正しく把握」できるようになります。

◆ フォレンジックのイメージ

解析対象（エビデンス）

証拠保全・解析

解析結果（タイムライン解析）

いつ	何が
○月○日 12:30:50	PC-Aが改ざんされたウェブサイト「http://○○.com」にアクセス
12:30:55	リダイレクトにより、PC-Aが不審サイト「http://□□.ru」にアクセス
12:31:10	Adobe Reader への脆弱性攻撃により、PC-Aで不審プログラム「a.exe」が起動
12:31:12	PC-Aが「a.exe」が「http://△△.cn」との通信を開始
12:32:30	PC-Aから社内サーバに感染が拡大
12:35:00	IDSが、PC-Aの不審通信を検知

タイムライン解析の概要（1）

- タイムライン解析は、各タイムスタンプを時系列に整理した「タイムライン」を作成し、「いつ」、「何が起きたのか」を推測する調査手法です。

◆ タイムライン解析の例

［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	2017/01/01	2017/01/01	2017/05/01
BBB.xls	2017/03/15	2017/05/22	2017/07/01
CCC.doc	2016/09/04	2016/03/04	2016/09/04
・・・			

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ら、整理していく必要があり、調査に時間がかかる。

［タイムラインに変換した結果］

日時	タイプ※1	ファイル名
2016/03/04	btime	CCC.doc
2016/09/04	mtime	CCC.doc
2016/09/04	atime	CCC.doc
2017/01/01	btime	AAA.txt
2017/01/01	mtime	AAA.txt
2017/03/15	btime	BBB.xls
		・・・

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」を把握しやすい。
「タイプ」※1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。

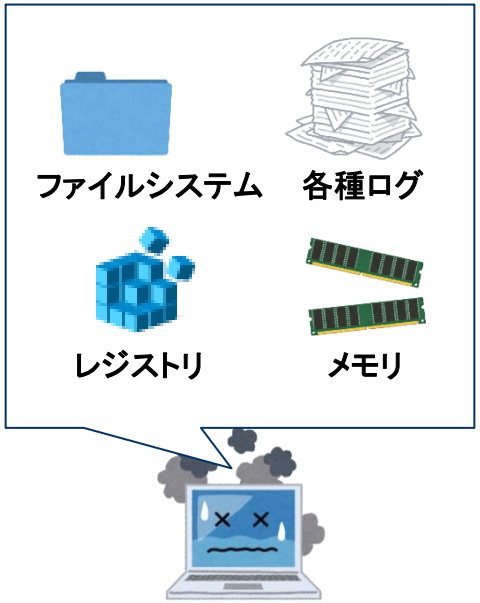
※1　btime(crtime)：作成日時、mtime：更新日時、atime：アクセス日時、ctime：属性変更日時

タイムライン解析の概要（2）

- ファイル・フォルダ、レジストリ、各種ログなど、タイムスタンプを持つさまざまな情報をタイムラインに展開することで、インシデントの経緯を把握しやすくなります。

◆ タイムライン解析のイメージ
（≒ フォレンジックのイメージ）

解析対象（エビデンス）



解析結果（タイムライン解析）

日時	タイムスタンプの種類	推測
○月○日 12:30:50	レジストリに記録された、ブラウザの起動日時	ブラウザを起動した
12:30:55	ブラウザのキャッシュファイルの作成日時	ブラウザでウェブサイトを閲覧した
12:31:10	レジストリに記録された、Adobe Readerの起動日時	ウェブサイトに埋め込まれたPDFファイルにアクセスした
12:31:12	メモリに記録された、不審プロセスの起動日時	**PDFの脆弱性攻撃により感染？？？**

タイムライン解析の基本手順

- タイムライン解析は、「証拠保全」、「解析・抽出」、「考察」の順番に進めます。

◆ タイムライン解析の基本手順

証拠保全	解析・抽出	考察（仮説設定）
調査対象のパソコンから、解析対象とするデータを、証拠（エビデンス）として確保する。	エビデンスに残されている、さまざまなイベントのタイムスタンプを時系列に整理した「タイムライン」を作成する。	タイムラインを解析し、「いつ」、「何が起きたのか」を推測し、仮設を設定する。 必要に応じて、仮設の検証に必要な追加調査を行う。

簡易証拠保全

- フォレンジック調査を実施する際は、まず最初に、解析対象とするデータ（エビデンス）の証拠保全を実施します。
- 本講座では、調査対象パソコンで証拠保全用ツールを起動し、エビデンスを抽出する「簡易証拠保全」による調査手法を学習します。
  - 法的対応が必要となる本格的なフォレンジック調査では、原則として、調査対象パソコンのディスクイメージを作成し、ハードディスク全体を証拠保全します。

◆簡易証拠保全のイメージ

簡易証拠保全の対象データ

- 簡易証拠保全で取得すべきデータを下表に記載します。

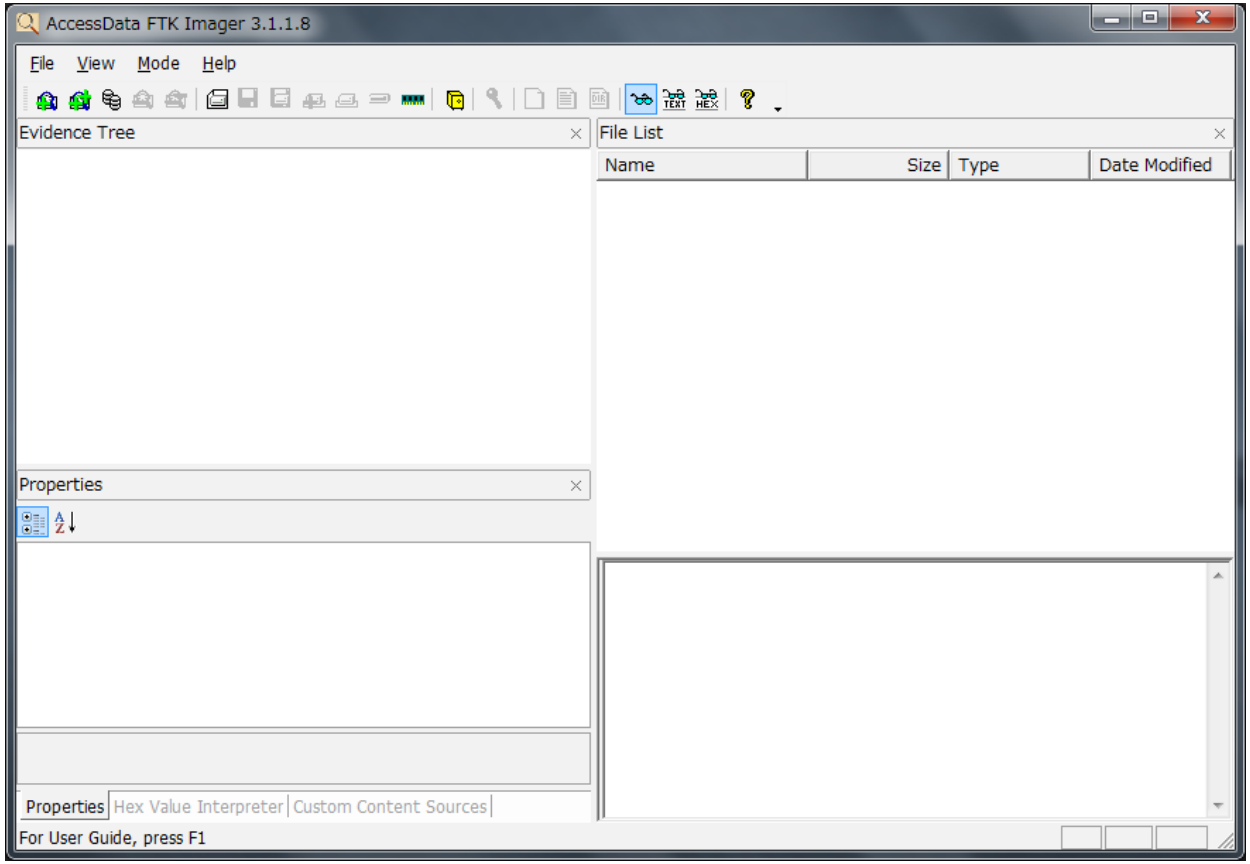
◆ 簡易証拠保全の対象データ

分類	ファイル名
マルウェアの検体	•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判明している場合は、検体として取得しておく。
ファイルシステム	•$MFT※1 ［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されない）
レジストリファイル	•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	•各種イベントログファイル ［保存場所 XP］C:¥WINDOWS¥system32¥config¥ （拡張子.evt） ［保存場所 7］C:¥Windows¥System32¥winevt¥Logs¥ （拡張子.evtx）
その他のアーティファクト※2	•Prefetchファイル C:¥WINDOWS¥Prefetchフォルダ内に格納されている全てのファイル（拡張子.pf） •ブラウザ、メールの一時フォルダなど

（※1）NTFSのファイルエントリ管理テーブル。全てのファイル・ディレクトリのタイムスタンプなどの情報が記録されている。
（※2）OSやアプリケーションが作成するファイルのこと。

「FTK Imager Lite」による簡易証拠保全（1）

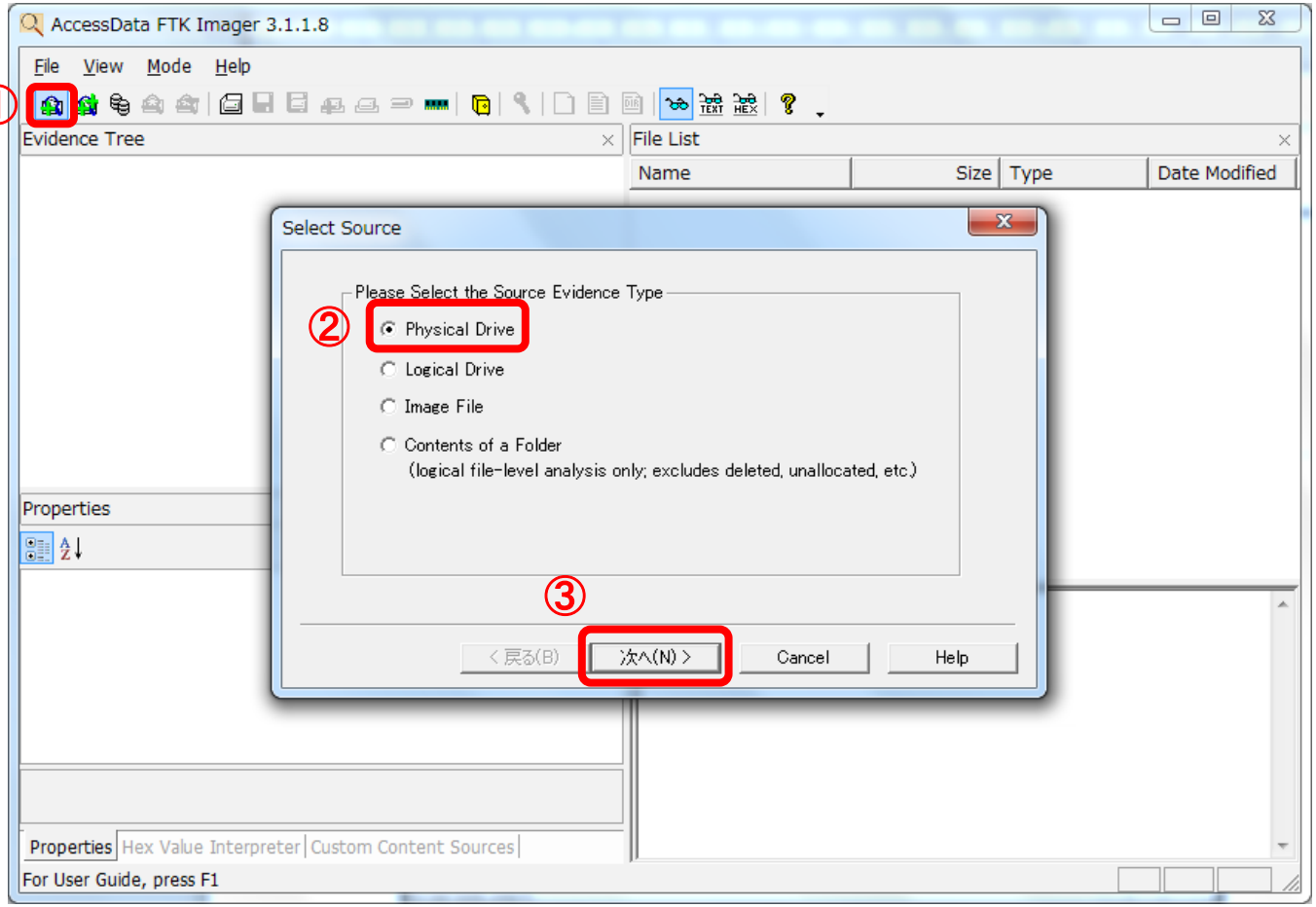
- 証拠保全用ツール「FTK Imager Lite」による簡易証拠保全の手順を説明します。
- 証拠保全用ツールを格納した調査用USBメモリ等を感染パソコンに接続し、ツールを起動します。（起動には管理者権限が必要）



Access Data FTK Imager Lite
https://accessdata.com/product-download

「FTK Imager Lite」による簡易証拠保全（2）

- ツールバーから「Add Evidence Item」をクリックします。
- 「Select Source」ダイアログで「Physical Drive」を選択した状態で、「次へ」をクリックします。

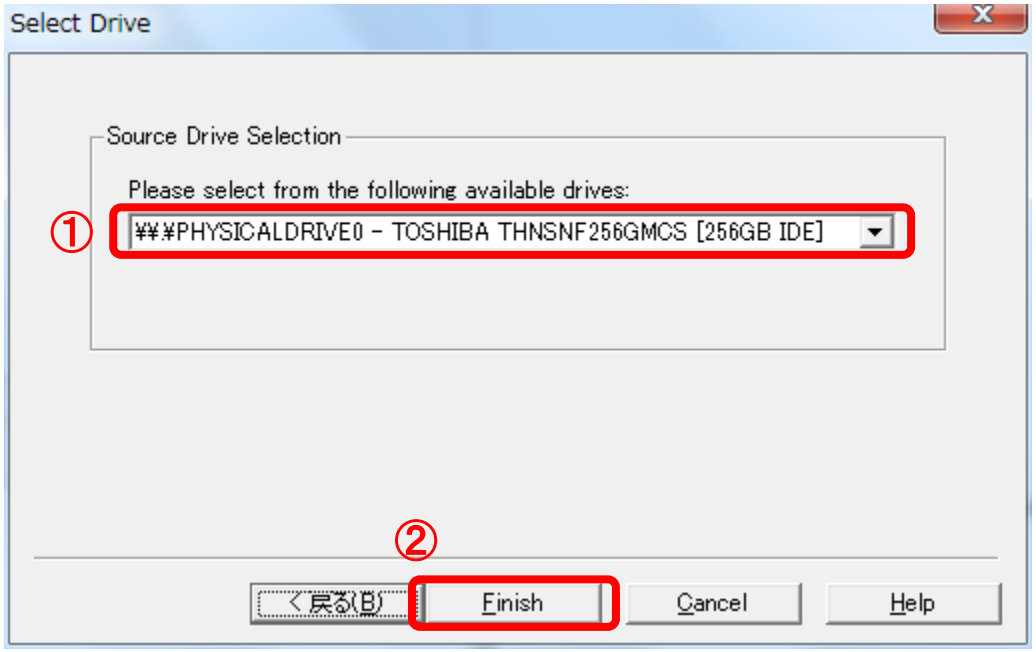


（補足）「Select Source」ダイアログ

選択肢	説明
Physical Drive	• 物理的なディスクを選択します。 • 未割当領域、削除済領域も含めて、ディスクの全領域を調査できます。
Logical Drive	• 論理ドライブ（例：Cドライブ）を選択します。 • 選択したパーティションのみ調査できます。
Image File	• イメージファイルを選択します。
Contents of a Folder	• 特定のフォルダを選択します。 • 未割当領域、削除済領域などは調査できません。

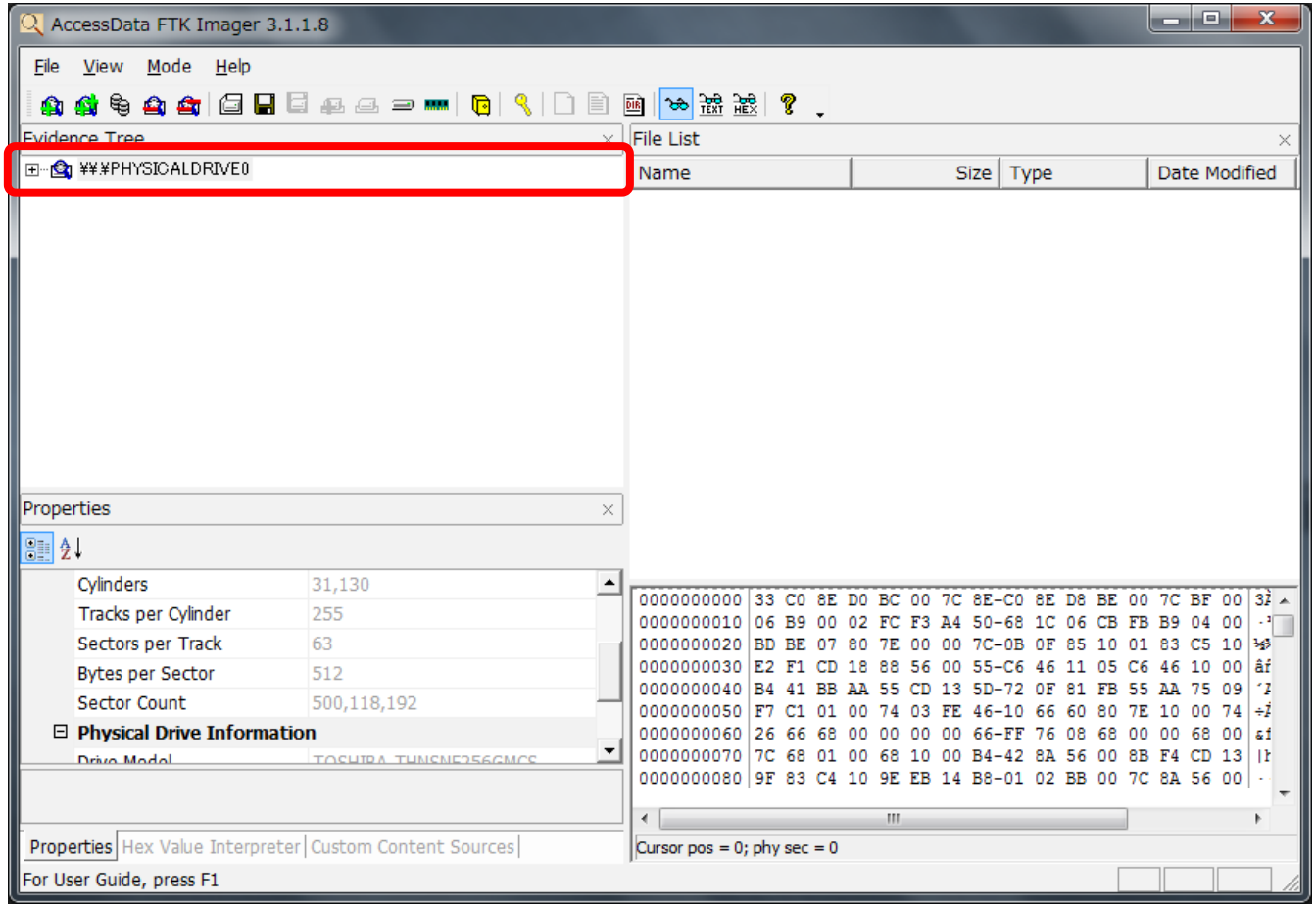
「FTK Imager Lite」による簡易証拠保全（3）

- 「Select Drive」ダイアログで、調査対象ディスクを選択し「Finish」をクリックします。
  - ドロップダウンリストには、パソコンに接続されている全てのストレージが表示されます。（USBメモリも表示されます）
  - メーカー名、型番、容量などを参考に、調査したいディスクを選択します。



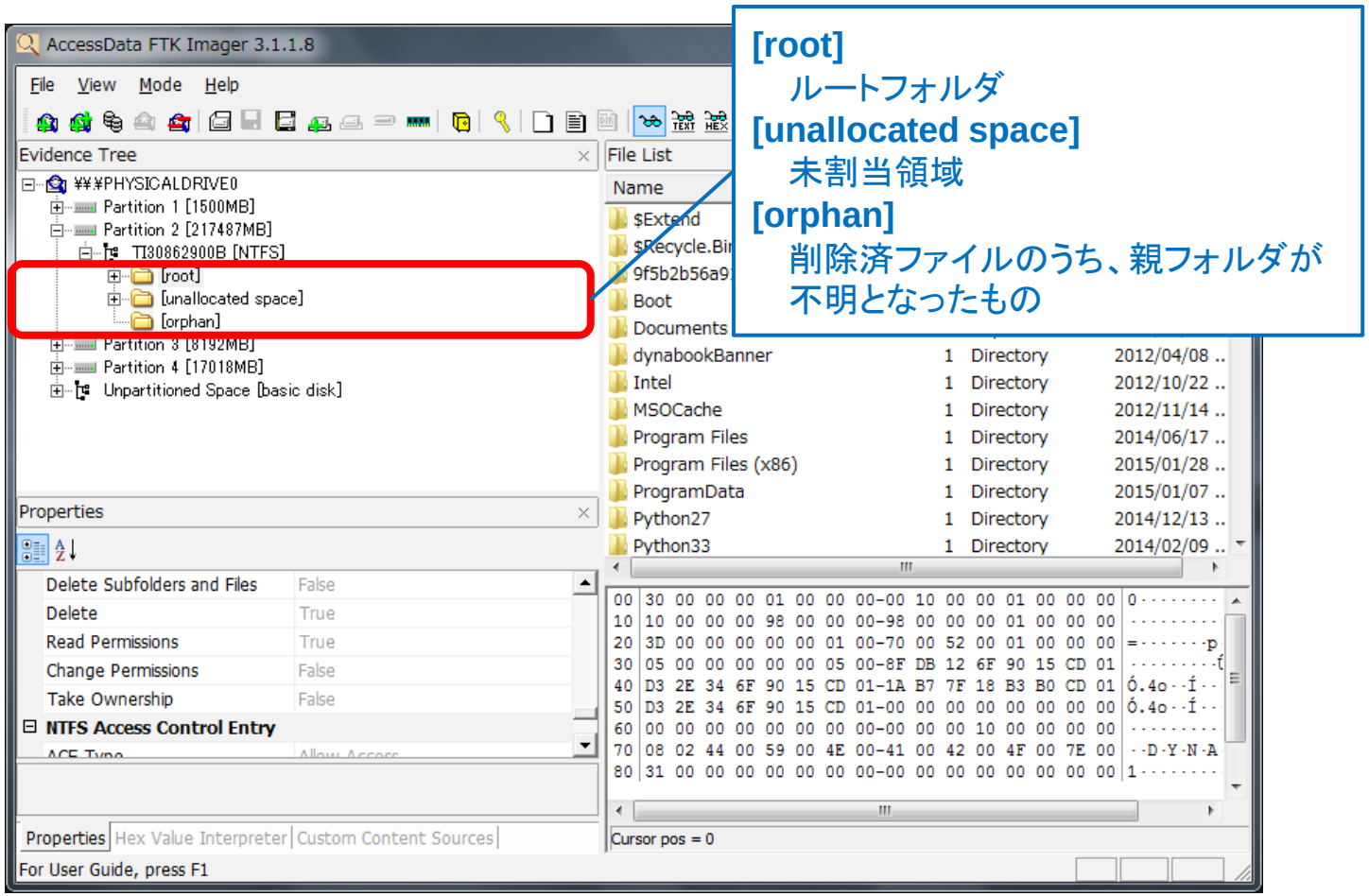
「FTK Imager Lite」による簡易証拠保全（4）

- 「Evidence Tree」に、ディスクが追加されました。
- 同様の操作で、複数のディスクやディスクイメージをエビデンスツリーに追加できます。



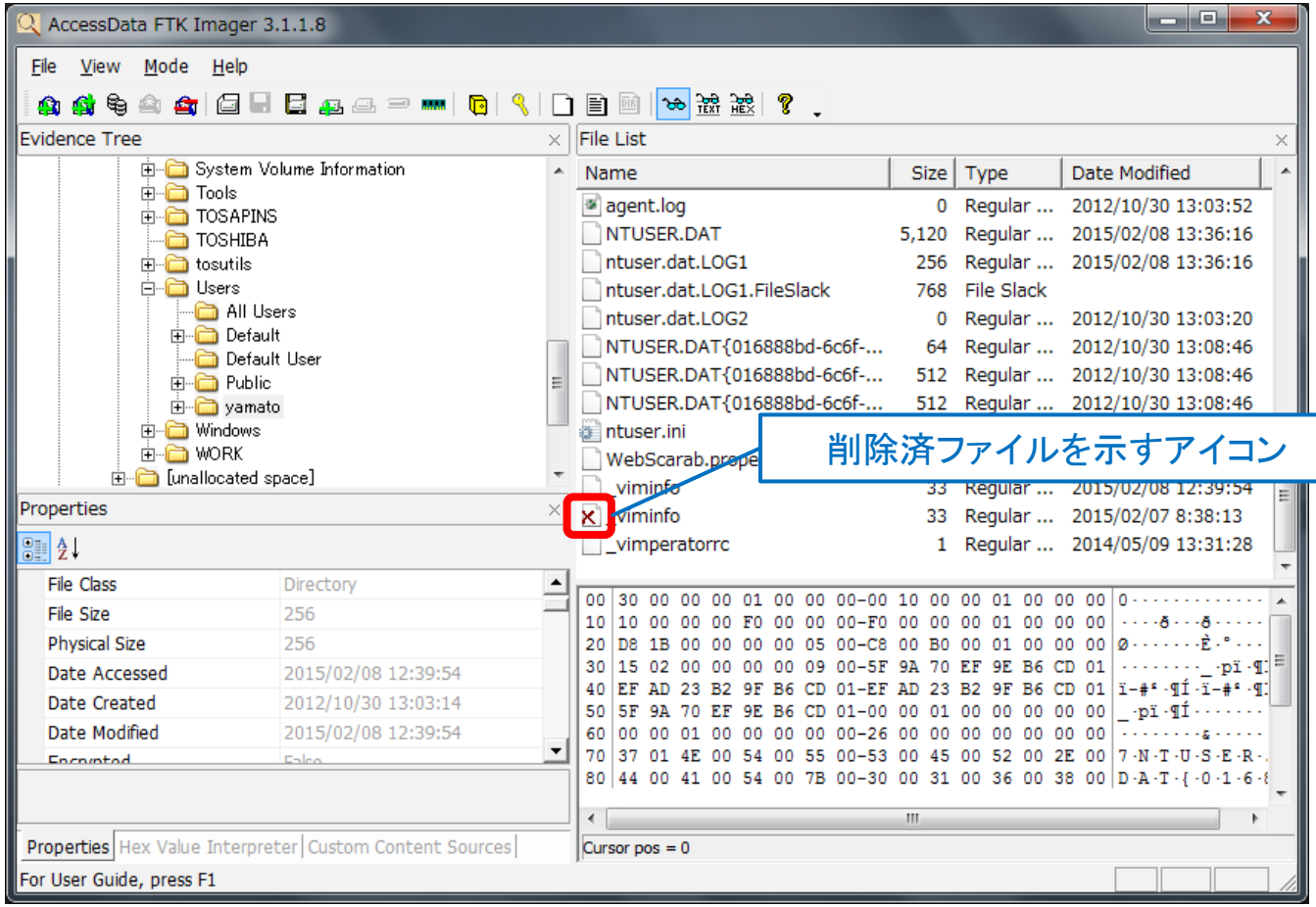
「FTK Imager Lite」による簡易証拠保全（5）

- 「Evidence Tree」のディスクを展開していくと、各パーティションに格納されているフォルダなどが表示されます。



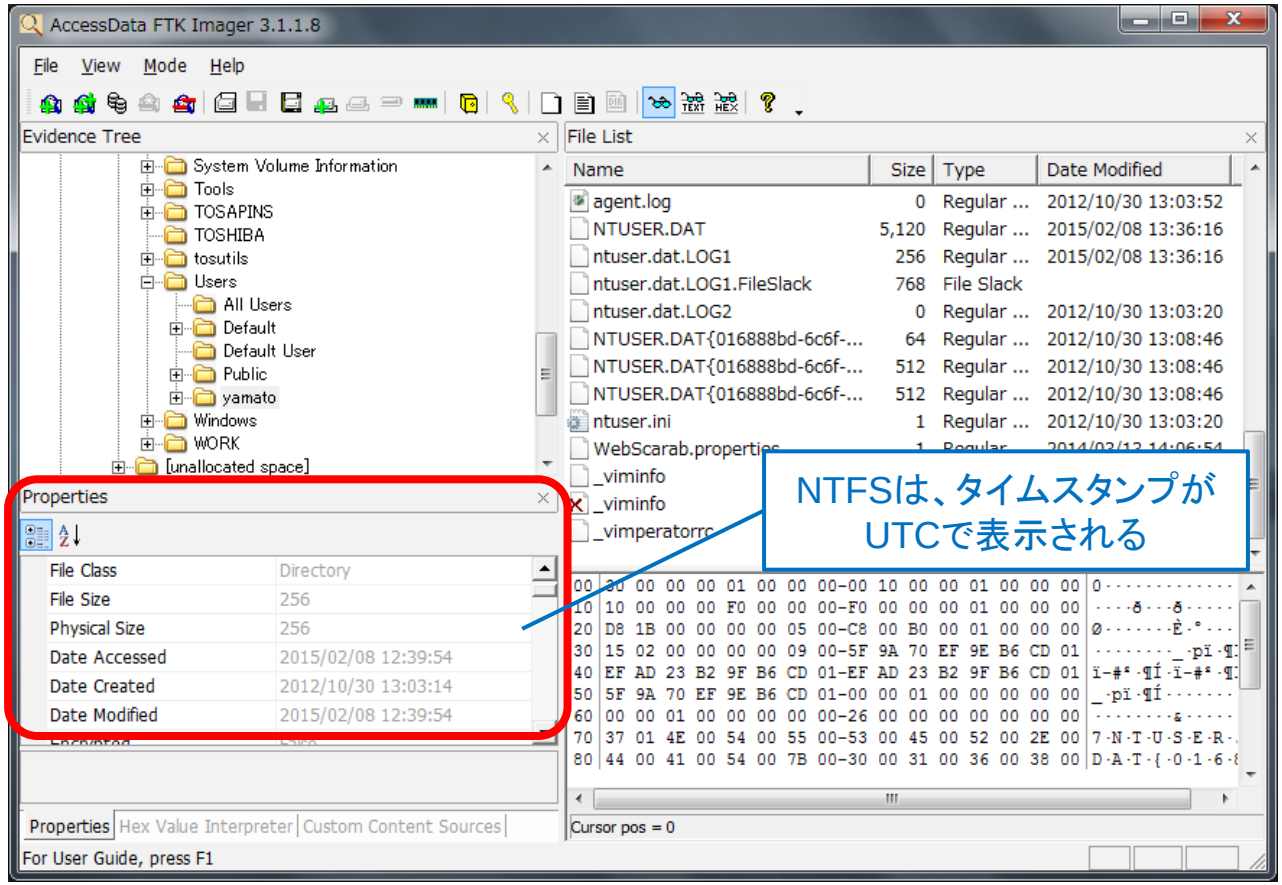
「FTK Imager Lite」による簡易証拠保全（6）

- 「FTK Imager Lite」は、OSを介さずにファイルシステムを直接解析するため，Windowsのアクセス権などの影響を受けずに、全てのフォルダ・ファイルにアクセスできます。また、削除済フォルダ・ファイルも表示できます。



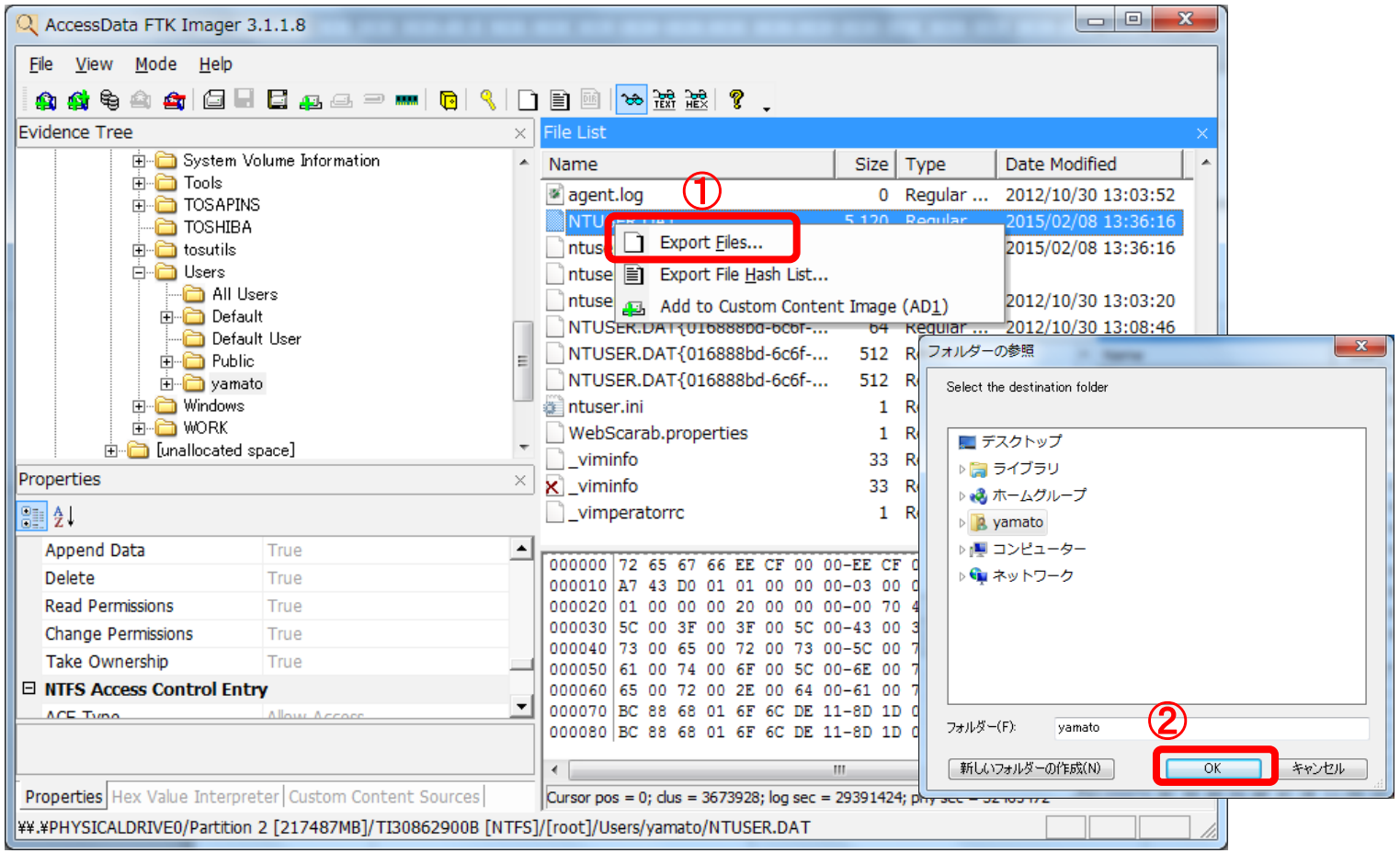
「FTK Imager Lite」による簡易証拠保全（7）

- プロパティペインには、選択したファイルのタイムスタンプなどの詳細情報が表示されます。なお、NTFSのタイムスタンプは，UTC（協定世界時）で表示されます。日本時間に換算するには、+9時間する必要があります。
  - FATのタイムスタンプは日本時間で表示されるため、注意が必要です。



「FTK Imager Lite」による簡易証拠保全（8）

- **次の操作により、任意のフォルダ・ファイルを抽出して保存することができます。**
  - ① 取得したいフォルダ・ファイルを右クリックし，「Export Files…」をクリック
  - ② 保存するフォルダを指定して「OK」をクリック



タイムライン解析ツール

- 本講座では、下表のツールを利用してタイムライン解析を行います。

◆ タイムライン解析ツール

利用目的	ツール	解析対象	説明
ファイルシステムのタイムライン作成	**MFTECmd**	$MFT	$MFTから、ファイル、ディレクトリのタイムスタンプを抽出し、「body」形式の中間ファイルを作成する。 https://github.com/EricZimmerman/MFTECmd/releases
	mactime	bodyファイル	「body」ファイルから、時系列に整理したタイムライン（テキストファイル）を作成する。 （補足）plasoで「body」からタイムラインを作成することも可能だが、日本語が文字化けする。 https://www.sleuthkit.org/
各種アーティファクトのタイムライン作成	**Plaso** （Log2timeline）	bodyファイル、レジストリなど	さまざまなエビデンスから、イベントのタイムスタンプを抽出し、タイムライン（テキストファイル）を作成する。 https://github.com/log2timeline/plaso
タイムラインの閲覧	**Timeline Explorer**	タイムライン形式テキストファイル	タイムライン形式テキストファイルを高速に表示・検索する。 https://ericzimmerman.github.io/

ファイルシステムのタイムライン作成（1）

- **「$MFT」から、ファイル・フォルダのタイムラインを作成します。**

手順

① 「$MFT」を「mftecmd」コマンドで前処理し、「body」形式の中間ファイルを作成する。
② 「mactime」コマンドにより、「body」ファイルを整形し、タイムラインを作成する。

コマンド書式

① mftecmd -f *【$MFTのファイル名】* --body *【bodyの出力先フォルダ名】*※1 --bdl *【ドライブ名】*※2
（※1）指定したフォルダに、ファイル名「YYYYMMDDhhmmss_MFTECmd_Output.body」で出力される。
（※2）ドライブレターとして表示したい任意の文字列を指定する。（例：C）

② mactime -b *【bodyファイル名】* -z Japan -m -d > *【タイムラインの出力ファイル名】*
（①で出力したファイル）

ファイルシステムのタイムライン作成(2)

◆実行例 ① mftecmd

```
caine@caine:$ mftecmd -f MFT --body . --bdl C
caine@caine:/var/samba/public/Lab02$ mftecmd -f MFT --body . --bd
0014:err:xrandr:xrandr12_get_current_mode Unknown mode, returning
MFTECmd vers

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

Command line: -f MFT --body . --bdl C

0038:err:winsock:WSAIoctl -> SIO_ADDRESS_LIST_CHANGE request failed with status 0x2733
0038:err:winsock:WSAIoctl -> SIO_ADDRESS_LIST_CHANGE request failed with status 0x2733

Processed 'MFT' in 8.6680 seconds

Bodyfile output will be saved to '.¥20180826050356_MFTECmd_Output.body'
003b:err:winsock:WSAIoctl -> SIO_ADDRESS_LIST_CHANGE request failed with status 0x2733
003b:err:winsock:WSAIoctl -> SIO_ADDRESS_LIST_CHANGE request failed with status 0x2733
003d:err:winediag:SECUR32_initNTLMS                                              uth >= 3.0.25
is in your path. Usually, you can f

caine@caine:$
```

タイムラインに表示するドライブレターとして「C:」を指定

$MFTのファイル名「MFT」を指定

出力先フォルダとして、カレントディレクトリを意味する「.」(ドット)を指定

ファイル名「20180826050356_MFTECmd_Output.body」でbodyファイルが出力された。

ファイルシステムのタイムライン作成（2）

◆実行例 ② mactime

```
caine@caine:$ mactime -b 20180826050356_MFTECmd_Output.body -z Japan -m -d > timeline_mft.txt
caine@caine:$
```

手順①で作成したbodyファイル名

ファイル名「timeline_mft.txt」でタイムラインを出力

◆タイムライン「timeline_mft.txt」の内容例（抜粋）

```
Date,Size,Type,Mode,UID,GID,Meta,File Name
Fri 02 21 2003 04:42:22,348160,m..b,r/rrwxrwxrwx,0,0,18808-128-3,"c:/Windows/System32/msvcr71.dll"
Tue 03 18 2003 21:12:12,1047552,m...,b,r/rrwxrwxrwx,0,0,18807-128-3,"c:/Windows/System32/mfc71u.dll"
Tue                                                                                              dll"
Mon                                                                                              with ID 0x0000AD05-
    00000002/x86_microsoft-windows-s..svc-admin.resources_31bf3856ad364e35_6.1.7601.17514_zh-hk_6f445dbca8eb0dca/mail.chm
    (deleted)"
Mon 06 08 2009 09:34:42,326373,m...,r/rrwxrwxrwx,0,0,125927-48-5,"c:/PathUnknown/Directory with ID 0x0000AD05-
    00000002/x86_microsoft-windows-s..svc-admin.resources_31bf3856ad364e35_6.1.7601.17514_zh-hk_6f445dbca8eb0dca/mail.chm
    ($FILE_NAME) (deleted)"
```

時刻情報

タイムスタンプの種類※1

ファイル・フォルダ名※2

（※1）ファイル・フォルダには、更新日時、作成日時など、複数のタイムスタンプが記録されている。タイムラインでは、同じ時刻のタイムスタンプを一行で表現している。
m:更新日時、a:アクセス日時、c:属性変更日時、b:作成日時

（※2）削除済みファイルは(deleted)が付記される。また、NTFSの「Filename属性」のタイムスタンプは「$FILE_NAME」が付記される。

各種アーティファクトのタイムライン作成（1）

- **レジストリ、Prefetch、ブラウザ閲覧履歴など、各種アーティファクトに記録されているイベントのタイムラインを作成します。**

手順

① 解析対象のファイルを「log2timeline」コマンドで前処理し、「plaso storage」と呼ばれる中間ファイルを生成する。

② 「psort」コマンドにより、「plaso storage」からタイムラインを作成する。

コマンド書式

① log2timeline.py *【出力ファイル名】【解析対象ファイルを格納したフォルダ名】*※1
（plaso storage）

② psort.py -z *【タイムゾーン】* -o *【出力形式】* -w *【出力ファイル名】【plaso storage】*
（①で出力したファイル）

（※1）レジストリなど、解析対象のアーティファクトを格納したフォルダを指定する。log2timelineは、サブフォルダも再帰的に処理する。

各種アーティファクトのタイムライン作成(2)

◆実行例 ① log2timeline

```
caine@caine:$ log2timeline.py db.plaso Users/
plaso - log2timeline version 20171020

Source path : /
Source type : d

Tasks:          Queued  Processing      To merge        Abandoned       Total
                0       0               0               0               536

Identifier      PID     Status          Memory          Sources         Events          File
Main            28332   completed       346.3 MiB       536 (4)         3955 (504)
Worker_00       28342   idle            264.2 MiB       194 (4)         2705 (51)
OS:/var/samba/public/Lab02/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet
Files/Virtualized/C/Users/user01/AppData/Roaming/Microsoft/Windows/PrivacIE/Low
Worker_01       28346   idle            263.4 MiB       341 (0)         1250 (323)
OS:/var/samba/public/Lab02/Users/user01/AppData/Local/Microsoft/Windows/History/History.IE5/index.dat

[2018-08-26 06:10:39,243 [INFO] (MainProcess) PID:28332 <zeromq_queue> Queue main_task_queue responder exiting.
Processing completed.

caine@caine:$
```

「db.plaso」というファイル名で plaso storageを出力

「Users」フォルダに格納されている各種アーティファクトを解析対象として指定

各種アーティファクトのタイムライン作成(3)

◆実行例 ② psort

```
caine@caine:$ psort.py -z Japan -o l2tcsv -w timeline_plaso.txt db.plaso

plaso - psort version 20171020

Storage file            : db.plaso

Identifier              PID     Status          Memory          Events (filtered)       Tags (filtered)         Reports (filtered)
Main                    28431   exporting       195.5 MiB       3949 (1941)     0 (0)                   0 (0)

Processing completed.

********************************** Export results **********************************
        Events processed : 3955
     Events MACB grouped : 2485
Duplicate events removed : 107
          Events filtered : 0
（以下略）
```

「timeline_plaso.txt」という
ファイル名でタイムラインを出力

手順①で作成した
plaso storageのファイル名

◆タイムライン「timeline_plaso.txt」の内容例(抜粋)

```
date,time,timezone,MACB,source,sourcetype,type,user,host,short,desc,version,filename,inode,notes,format,extra
09/23/2002,19:32:41,Japan,M...,WEBHIST,MSIE Cache File URL record,Content Modification Time,-,-,Location:
    https://www.scollabo.com/banban/lectur/sample/niagara_01.html Cache...,Location:
    collabo.com/banb                                                                    ile: 1PG2JDV9¥niagara_01[1].htm
    ize: 1414 HTTP H                                                                    eout=5  max=100 - Content-Type:
    text/html - Content-Length: 1414 - - 0,User01 - [Recovered
    Entry],2,OS:/var/sam                                                    ppData/Local/Microsoft/Windows/Temporary Internet
    Files/Low/Content.IE                                                    irectory_index: 2; cache_directory_name: 1PG2JDV9; cached_filename:
    niagara_01[1].htm; recovered: True; sha256_hash: 4f1a72bda0b2612404f41565c78a76f0d30c6923ebfdac8ecbd00936824b89ed
```

時刻情報

イベントの種類(以降、イベント内容などの説明)

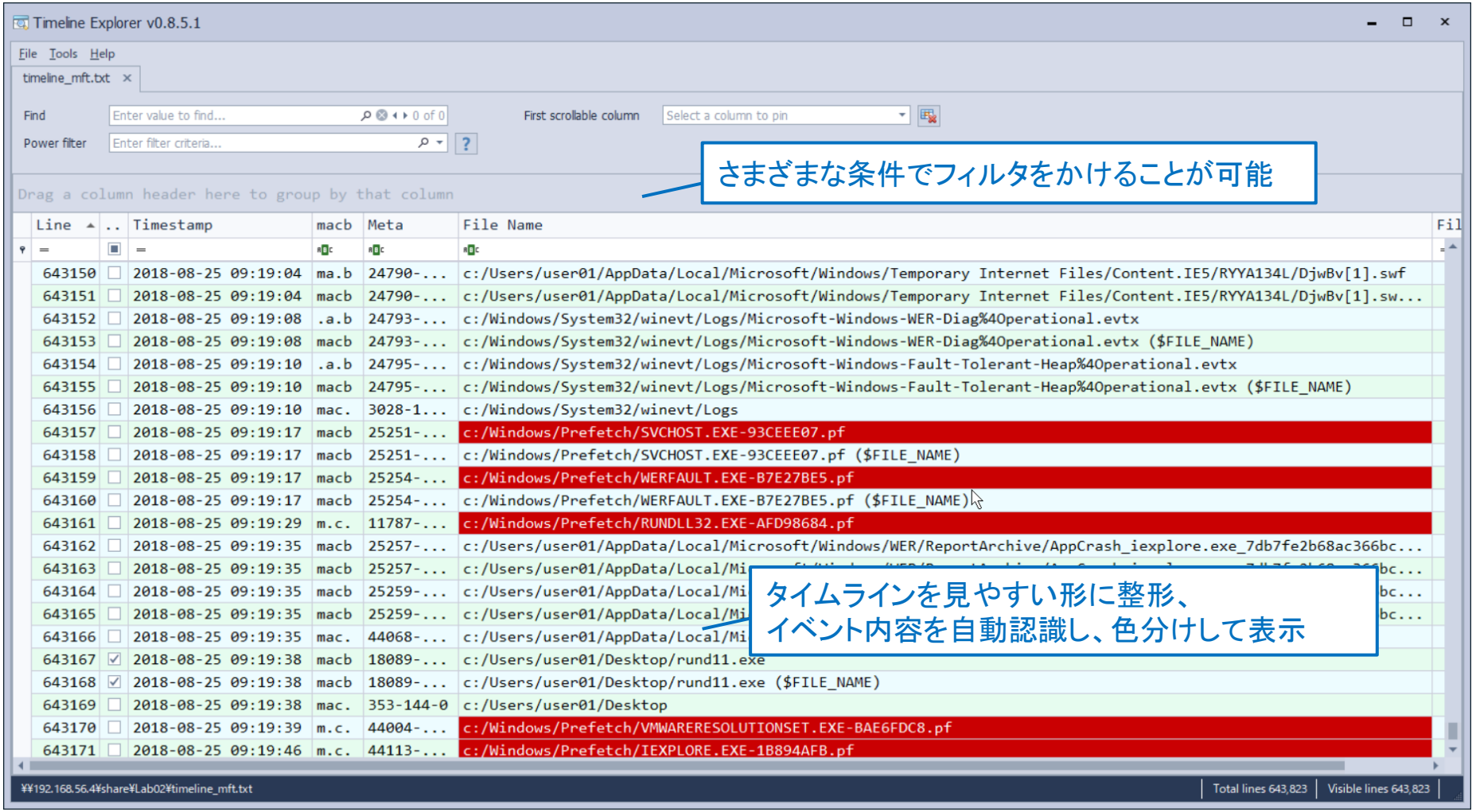
タイムスタンプの種類※1

(※1)M:更新日時、A:アクセス日時、C:属性変更日時、B:作成日時

タイムラインの閲覧

- 作成したタイムラインは、テキストエディタや「Timeline Explorer」などで閲覧します。

◆ Timeline Explorerによるタイムライン表示の例



Line	..	Timestamp	macb	Meta	File Name
643150		2018-08-25 09:19:04	ma.b	24790-...	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/RYYA134L/DjwBv[1].swf
643151		2018-08-25 09:19:04	macb	24790-...	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/RYYA134L/DjwBv[1].sw...
643152		2018-08-25 09:19:08	.a.b	24793-...	c:/Windows/System32/winevt/Logs/Microsoft-Windows-WER-Diag%4Operational.evtx
643153		2018-08-25 09:19:08	macb	24793-...	c:/Windows/System32/winevt/Logs/Microsoft-Windows-WER-Diag%4Operational.evtx ($FILE_NAME)
643154		2018-08-25 09:19:10	.a.b	24795-...	c:/Windows/System32/winevt/Logs/Microsoft-Windows-Fault-Tolerant-Heap%4Operational.evtx
643155		2018-08-25 09:19:10	macb	24795-...	c:/Windows/System32/winevt/Logs/Microsoft-Windows-Fault-Tolerant-Heap%4Operational.evtx ($FILE_NAME)
643156		2018-08-25 09:19:10	mac.	3028-1...	c:/Windows/System32/winevt/Logs
643157		2018-08-25 09:19:17	macb	25251-...	c:/Windows/Prefetch/SVCHOST.EXE-93CEEE07.pf
643158		2018-08-25 09:19:17	macb	25251-...	c:/Windows/Prefetch/SVCHOST.EXE-93CEEE07.pf ($FILE_NAME)
643159		2018-08-25 09:19:17	macb	25254-...	c:/Windows/Prefetch/WERFAULT.EXE-B7E27BE5.pf
643160		2018-08-25 09:19:17	macb	25254-...	c:/Windows/Prefetch/WERFAULT.EXE-B7E27BE5.pf ($FILE_NAME)
643161		2018-08-25 09:19:29	m.c.	11787-...	c:/Windows/Prefetch/RUNDLL32.EXE-AFD98684.pf
643162		2018-08-25 09:19:35	macb	25257-...	c:/Users/user01/AppData/Local/Microsoft/Windows/WER/ReportArchive/AppCrash_iexplore.exe_7db7fe2b68ac366bc...
643163		2018-08-25 09:19:35	macb	25257-...	c:/Users/user01/AppData/Local/Mi...
643164		2018-08-25 09:19:35	macb	25259-...	c:/Users/user01/AppData/Local/Mi...
643165		2018-08-25 09:19:35	macb	25259-...	c:/Users/user01/AppData/Local/Mi...
643166		2018-08-25 09:19:35	mac.	44068-...	c:/Users/user01/AppData/Local/Mi...
643167	☑	2018-08-25 09:19:38	macb	18089-...	c:/Users/user01/Desktop/rund11.exe
643168	☑	2018-08-25 09:19:38	macb	18089-...	c:/Users/user01/Desktop/rund11.exe ($FILE_NAME)
643169		2018-08-25 09:19:38	mac.	353-144-0	c:/Users/user01/Desktop
643170		2018-08-25 09:19:39	m.c.	44004-...	c:/Windows/Prefetch/VMWARERESOLUTIONSET.EXE-BAE6FDC8.pf
643171		2018-08-25 09:19:46	m.c.	44113-...	c:/Windows/Prefetch/IEXPLORE.EXE-1B894AFB.pf

タイムライン解析と考察

- **マルウェア感染時の挙動や痕跡などを推測しながらタイムラインを検索・閲覧し、感染原因を推測します。**

◆ **タイムライン解析のポイント（一例）**

① 把握できているウイルス関連ファイル名で検索し、前後の状況を確認する。
（ウイルス検知されたファイル名など）

✓不審なプロセス起動の痕跡はないか。
（Prefetchファイルの作成など）

✓他に不審なファイルはないか。
（ウイルス関連ファイルと類似したファイル名、マルウェアが作成したフォルダ内のファイルなど）

✓ブラウザやメールを利用していた痕跡はないか。
（ブラウザやメールの一時フォルダへのファイル作成など）

② 不審な事象が発生した時刻で検索し、前後の状況を確認する。
（画面に不審なメッセージが表示された時刻など）

※確認ポイントは①と同じ。

NTFS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、エビデンスのタイムスタンプの意味（更新条件）を理解する必要があります。
- ここでは一例として、Windowsが利用するファイルシステム「NTFS」における、ファイルのタイムスタンプの更新条件を説明します。

◆ NTFSのファイルのタイムスタンプの更新条件

操作	ファイルのタイムスタンプ			
	更新日時 (Modification Time)	作成日時 (Birth/Born Time)	アクセス日時※1 (Access Time)	属性変更日時※2 (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	–	–	–	○
ファイルコピー	–	○	○	○
ファイル移動（同一ボリューム内）	–	–	–	–
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の標準設定では、アクセス日時の更新が無効化されています。
（※2） NTFSの属性情報（メタデータ）のタイムスタンプです。エクスプローラーでは表示されません。

タイムライン解析の例（1）ウェブサイトからの感染 - 事案の概要

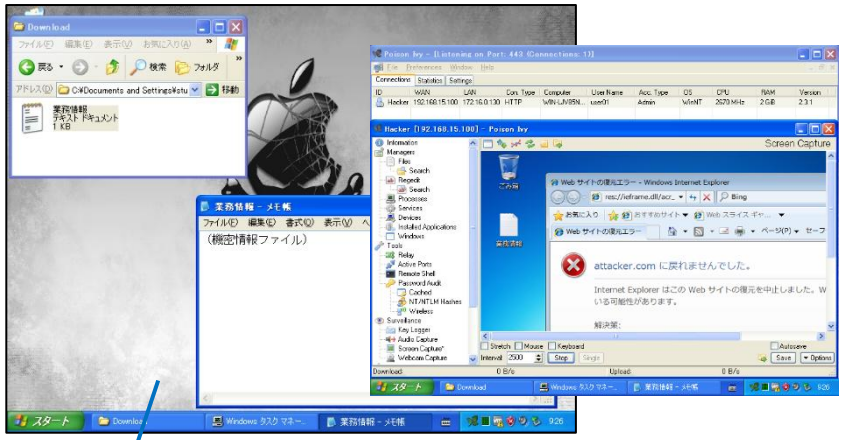
［事案の概要］2018年8月25日（土）

① 社員がウェブサイト閲覧中に、攻撃サイト「exploit.attacker.com」にアクセスした。（9:19頃）
② Adobe Flashの脆弱性（CVE-2015-5122）を悪用するSWFファイルが、「http://www.attacker.com/a.exe」から遠隔操作型マルウェアをダウンロードし、デスクトップに「rund11.exe」として保存のうえ実行（感染）した。（9:19頃）
③ 攻撃者は、遠隔操作型マルウェアにより、感染パソコンのデスクトップに保存されていた「業務情報.txt」の窃取、スクリーンキャプチャ取得などを行った。（9:19～9:26頃）

①、②感染時の社員用パソコンの画面

脆弱性攻撃により、ブラウザが異常終了したが、その他、目に見える形での異常はない。

③攻撃者による遠隔操作の画面



攻撃者の画面には、社員用パソコンの画面が転送され遠隔操作可能となっている。

タイムライン解析の例（1）ウェブサイトからの感染 - 解析例1

［検知・認知したキッカケ］

オンデマンドスキャンにより、デスクトップに作成された不審ファイル「rund11.exe」を検知

［タイムライン解析による考察］

$MFTのタイムラインを確認した結果、不審ファイルの作成・実行の直前に、ブラウザー時ファイルへのアクセスが発生していることから、ウェブサイトから感染した可能性がある。

感染直前にアクセスしたFlashファイル（拡張子.swf）など、脆弱性攻撃コードの可能性があるファイルを「Virus Total」※1などで解析する。

ウェブサイトー時フォルダへのアクセス

Timestamp	macb	.	File Name
2018-08-25 09:19:03	ma.b	.	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/RYYA134L/exploit_attacker_com[...
2018-08-25 09:19:03	macb	.	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/RYYA134L/exploit_attacker_com[...
2018-08-25 09:19:04	ma.b	.	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/MA7LM1CU/smTHSU[1].htm
2018-08-25 09:19:04	macb	.	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/MA7LM1CU/smTHSU[1].htm ($FILE_...
2018-08-25 09:19:04	ma.b	.	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/RYYA134L/DjwBv[1].swf
2018-08-25 09:19:04	macb	.	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5/RYYA134L/DjwBv[1].swf ($FILE_N...
2018-08-25 09:19:08	.a.b	.	c:/Windows/System32/winevt/Logs/Microsoft-Windows-WER-Diag%4Operational.evtx
2018-08-25 09:19:08	macb	.	c:/Windows/System32/winevt/Logs/Microsoft-Windows-WER-Dia
2018-08-25 09:19:10	.a.b	.	c:/Windows/System32/winevt/Logs/Microsoft-Windows-Fault-T
2018-08-25 09:19:10	macb	.	c:/Windows/System32/winevt/Logs/Microsoft-Windows-Fault-Tolerant-Heap%4Operational.evtx ($FILE_NAME)
2018-08-25 09:19:10	mac.	.	c:/Windows/System32/winevt/Logs
2018-08-25 09:19:38	macb	.	c:/Users/user01/Desktop/rund11.exe
2018-08-25 09:19:38	macb	.	c:/Users/user01/Desktop/rund11.exe ($FILE_NAME)
2018-08-25 09:19:48	.a.b	.	c:/Windows/Prefetch/RUND11.EXE-D1A948B1.pf
2018-08-25 09:19:48	macb	.	c:/Windows/Prefetch/RUND11.EXE-D1A948B1.pf ($FILE_NAME)
2018-08-25 09:20:12	m.c.	.	c:/Windows/Prefetch/RUND11.EXE-D1A948B1.pf

Flashコンテンツ（.swf）の表示

検知したファイル「rund11.exe」の作成、起動

（※1）ファイルやウェブサイトのウイルスチェックを行う無料ウェブサービス
https://www.virustotal.com/ja/

タイムライン解析の例（1）ウェブサイトからの感染 - 解析例2

［タイムライン解析による考察］

- Virus TotalでFlashファイル「DjwBv.swf」のウイルスチェックを実施したところ、脆弱性攻撃コードと判定された。（自社のウイルス対策ソフトでは検知できないものであった。）
- ブラウザ関連のアーティファクトのタイムライン（Log2timelineで作成）を確認したところ、不審サイト「http://exploit.attacker.com/smTHSU/」からダウンロードされていることを確認した。
- 今後、プロキシログなどを調査し、他のパソコンが不審サイトにアクセスしていないか調査する必要がある。

Timestamp	Sour...	Sourc...	macb	.	Long Description
2018-08-25 09:19:03	MSIE...	WEBHIST	.a..	0	Location: http://exploit.attacker.com/ Number of hits: 1 Cached file: RYYA134L\exploit_attacker_com[1].htm
2018-08-25 09:19:03	MSIE...	WEBHIST	.a..	0	Location: :2018082520180826: user01@http://exploit.attacker.com Number of hits: 1 Cached file size: 0
2018-08-25 09:19:03	MSIE...	WEBHIST	.a..	0	Location: :2018082520180826: user01@:Host: exploit.attacker.com Number of hits: 1 Cached file size: 0
2018-08-25 09:19:03	MS				ts: 2 Cached file size: 0
2018-08-25 09:19:04	MS				nber of hits: 1 Cached file size: 0
2018-08-25 09:19:04	MS				nber of hits: 1 Cached file size: 0
2018-08-25 09:19:04	MS				ts: 2 Cached file size: 0
2018-08-25 09:19:04	MSIE...	WEBHIST	....	0	Location: http://exploit.attacker.com/ Number of hits: 1 Cached file: RYYA134L\exploit_attacker_com[1].htm
2018-08-25 09:19:06	MSIE...	WEBHIST	....	0	Location: https://s.yimg.jp/images/top/searchbox/s_i-140325.gif Number of hits: 2 Cached file: MA7LM1CU\s_
2018-08-25 09:19:06	MSIE...	WEBHIST	....	0	Location: http://exploit.attacker.com/smTHSU/ Number of hits: 3 Cached file: MA7LM1CU\smTHSU[1].htm Cached
2018-08-25 09:19:06	MSIE...	WEBHIST	....	0	Location: http://exploit.attacker.com/smTHSU/DjwBv.swf Number of hits: 3 Cached file: RYYA134L\DjwBv[1].sw
2018-08-25 09:19:12	MSIE...	WEBHIST	....	0	Location: https://s.yimg.jp/images/top/searchbox/s_mp-140325.gif Number of hits: 2 Cached file: RYYA134L\s
2018-08-25 09:19:38	MSIE...	WEBHIST	.a..	0	Location: :2018082520180826: user01@http://exploit.attacker.com/smTHSU Number of hits: 1 Cached file size:
2018-08-25 09:19:38	MSIE...	WEBHIST	.a..	0	Location: Visited: user01@http://exploit.attacker.com/favicon.ico Number of hits: 3 Cached file size: 0
2018-08-25 09:19:40	MSIE...	WEBHIST	....	0	Location: :2018082520180826: user01@http://exploit.attacker.com/smTHSU Number of hits: 1 Cached file size:
2018-08-25 09:19:40	MSIE...	WEBHIST	....	0	Location: Visited: user01@http://exploit.attacker.com/favicon.ico Number of hits: 3 Cached file size: 0
2018-08-25 09:20:08	MSIE...	WEBHIST	....	0	Location: https://s.yimg.jp/images/top/sp/cgrade/iconVideo_150713.gif Number of hits: 2 Cached file: KGV7F
2018-08-25 09:20:08	MSIE...	WEBHIST	.a..	0	Location: http://exploit.attacker.com/smTHSU/ Number of hits: 3 Cached file: MA7LM1CU\smTHSU[1].htm Cached
2018-08-25 09:20:09	MSIE...	WEBHIST	.a..	0	Location: http://exploit.attacker.com/smTHSU/DjwBv.swf Number of hits: 3 Cached file: RYYA134L\DjwBv[1].sw
2018-08-25 09:20:11	MSIE...	WEBHIST	.a..	0	Location: Visited: user01@http://exploit.attacker.com/smTHSU Number of hits: 9 Cached file size: 0

「http://exploit.attacker.com/smTHSU/」から、「DjwBv.swf」をダウンロード

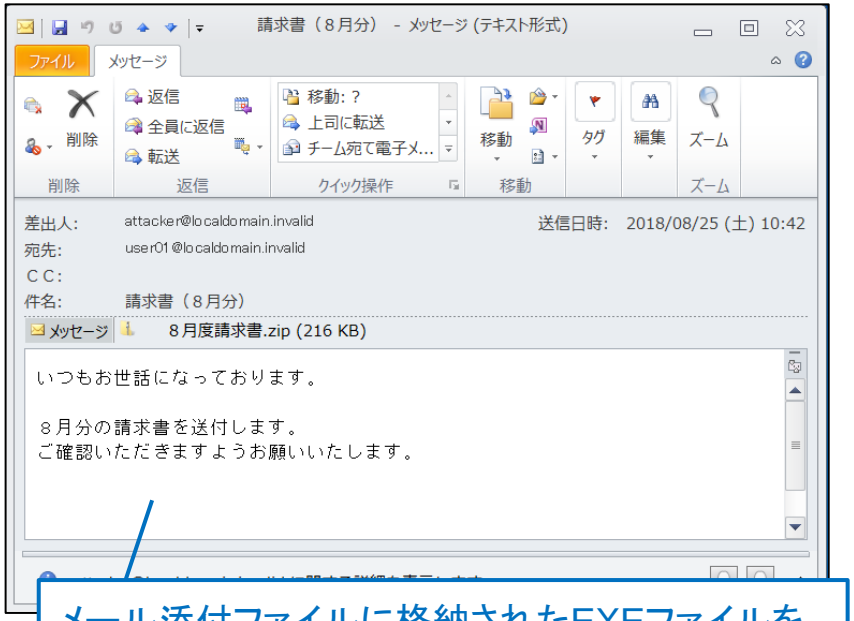
タイムライン解析の例(2)メールからの感染 - 事案の概要

[事案の概要] 2018年8月25日(土)

① 社員がOutlookで不審メールを受信し、添付ファイル「請求書.zip」に格納されていた「請求書.exe」を開封(実行)し、ランサムウェアに感染した。(10:47頃)

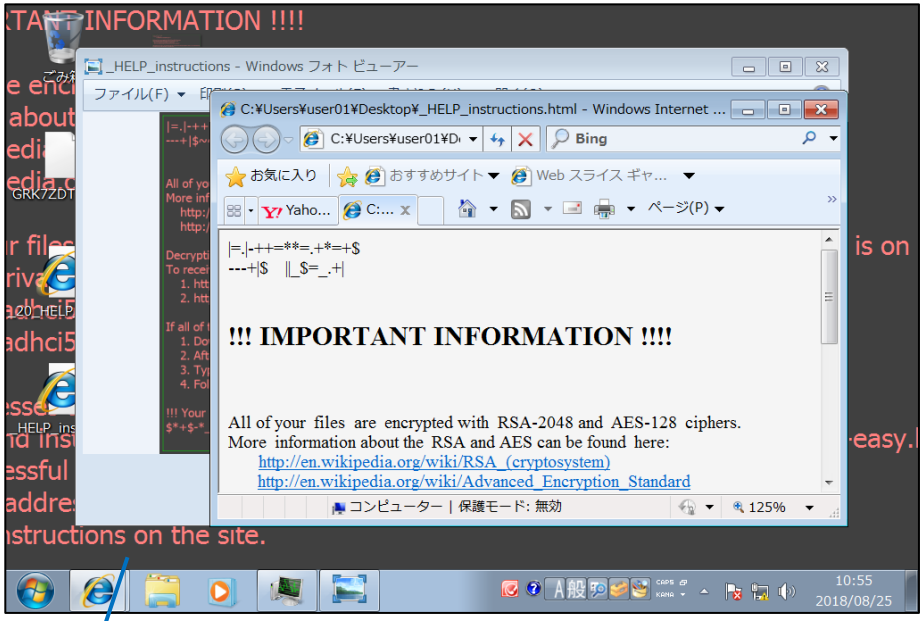
② ランサムウェアは、社員用パソコンのデータを暗号化するとともに、ファイル名を「ランダムな英数字.zepto」に変更し、画面に脅迫メッセージを表示した。(10:55頃)

①不審メールの画面



メール添付ファイルに格納されたEXEファイルを実行する際に、セキュリティの警告が表示されたが、社員は気にせずに「実行」をクリックした。

②ランサムウェアが表示した脅迫メッセージ



ランサムウェアは、暗号化処理が完了してから、脅迫メッセージを表示した。
(異常に気が付いた時には手遅れの状態)

タイムライン解析の例(2)メールからの感染 - 解析例

[検知・認知したキッカケ]

10:55頃、利用者からの通報。画面に不審なメッセージが表示され、業務データが壊れたとのこと。

[タイムライン解析による考察]

- 異常が発生する8分前に、メール添付ファイルの一時フォルダから「請求書.exe」を実行していることから、不審メールの添付ファイルを開封し感染し、ランサムウェアに感染した可能性がある。

Outlookのメール添付ファイル一時フォルダに、不審ZIPファイル作成
（メール添付ファイルの開封）

Timestamp	macb	.	File Name
2018-08-25 10:43:37	mac.	.	c:/Users/user01/AppData/Roaming/Microsoft/Windows/Recent/業務情報.lnk ($FILE_NAME)
2018-08-25 10:43:58	m.c.	.	c:/Users/user01/Desktop/GRK7ZDTT-KSKH-HAKS-001A-2B85AE577D71.zepto ($FILE_NAME)
2018-08-25 10:46:00	...b	.	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.Outlook/9VCWF8J5/ 8月度請求書.zip
2018-08-25 10:46:00	...b	.	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.Outlook/9VCWF8J5/ 8月度請求書.zi
2018-08-25 10:46:31	mac.	.	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.Outlook/9VCWF8J5/ 8月度請求書.zip
2018-08-25 10:46:31	mac.	.	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.Outlook/9VCWF8J5/ 8月度請求書.zi
2018-08-25 10:46:31	macb	.	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.Outlook/9VCWF8J5/ 8月度請求書.zi
2018-08-25 10:46:31	macb	.	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.Outlook/9VCWF8J5/ 8月度請求書 (2
2018-08-25 10:46:31	macb	.	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.Outlook/9VCWF8J5/ 8月度請求書 (2
2018-08-25 10:46:31	macb	.	c:/Users/user01/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.Outlook/9VCWF8J5/ 8月度請求書 (2
2018-08-25 10:47:30	...b	.	c:/Users/user01/AppData/Local/Temp/Temp1_ 8月度請求書.zip
2018-08-25 10:47:30	macb	.	c:/Users/user01/AppData/Local/Temp/Temp1_ 8月度請求書.zip ($FILE_NAME)
2018-08-25 10:47:47	.a.b	.	c:/Windows/Prefetch/8月度請求書.EXE-6FD29AC9.pf
2018-08-25 10:47:47	macb	.	c:/Windows/Prefetch/8月度請求書.EXE-6FD29AC9.pf ($FILE_NAME)
2018-08-25 10:48:07	m.c.	.	c:/Windows/Prefetch/8月度請求書.EXE-6FD29AC9.pf
2018-08-25 10:53:54	m.c.	.	c:/Users/user01/Documents/Outlook ファイル/GRK7ZDTT-KSKH-HAKS-AAB5-69F82BCC914A.zepto ($FILE_NAME)
2018-08-25 10:55:41	macb	.	c:/Users/user01/Desktop/GRK7ZDTT-KSKH-HAKS-001A-2B85AE577D71.zepto
2018-08-25 10:55:41	macb	.	c:/Users/user01/
2018-08-25 10:55:43	mac.	.	c:/Users/user01/

ZIP一時フォルダに展開された不審プログラム「請求書.exe」の実行

タイムライン解析の留意事項

- タイムラインは、イベントを時系列に記録した「ログ」ではありません。
- 調査時点で残されているタイムスタンプを時系列に整理したものであるため、ファイルの名前変更・削除、タイムスタンプの上書きなどにより、感染経緯の痕跡が確認できない可能性もあるという前提で取り扱う必要があります。

➡ インシデント対応を迅速・確実に行うためには、パソコンの操作履歴を記録するソフトウェアを導入することが望ましい。

実　習　タイムライン解析

- 別紙1.「実習資料」を参照し、タイムライン解析ツールの操作方法を確認しましょう

実習時間
20分間

第4章. サイバー防御演習

「サイバー防御演習」により、ウイルス検知アラート発生時の対応を体験します。

サイバー防御演習の説明

- 別紙2.「サイバー防御演習 説明資料」で説明します。

まとめ

まとめ

ウイルス対策ソフトの「リアルタイムスキャン」は、現在進行形の事象を検知、「オンデマンドスキャン」は過去の事象を検知する。

マルウェア感染時の挙動や痕跡を理解することで、ウイルス検知アラートから感染経路と感染の可能性を推測できる。

ウイルス検知アラートから感染経路などを推測できない場合は、タイムライン解析によりイベントを時系列に整理してみる。

タイムライン解析では感染経緯を特定できない場合もあるため、パソコンの操作履歴記録ソフトを導入することが望ましい。