不正アクセスの痕跡情報を用いたタイムライン型イベントログ解析支援ツールの開発

中野 心太[1,*] 早稲田 篤志[2] 村上 洋一[2] 岸本 頼紀[2]
花田 真樹[2] 関口 竜也[3] 折田 彰[3] 布広 永示[2]

概要：企業・組織のサービス，システムから情報を窃取することを目的とする攻撃に関連して，RAT（遠隔操作ツール）による攻撃被害事例が多数報告されている．近年ではこのような特定の対象に限定して攻撃を行う標的型攻撃の脅威が増加傾向にあり，感染原因や被害範囲を特定する手法としてデジタル・フォレンジックの重要性が高まっている．本研究では，Windows を対象として，不正に侵入を受けたシステム上の痕跡情報を用いて，攻撃者が行った一連の攻撃活動を可視化し，攻撃手順及びファイルの改ざんなどの特徴的なイベントを検出するログ解析支援ツールを開発した．本論文では，インシデント対応時の痕跡情報抽出作業で用いる抽出の判断基準を定義し，ログ解析支援ツールに実装した内容について述べる．次に，平常時に記録されるログのフィルタ処理，ファイル改ざん等の不正な操作が行われた可能性の高いログを抽出して可視化するタイムライン型のイベントログ解析支援ツールとその適用例について報告する．

キーワード：マルウェア，イベントログ，デジタル・フォレンジック，タイムライン，ラテラルムーブメント

Development of Timeline-Based Event Log Analysis Support Tool Using Traces of Unauthorized Access

Shinta Nakano[1,*] Atsushi Waseda[2] Yoichi Murakami[2] Yorinori Kishimoto[2]
Masaki Hanada[2] Tatsuya Sekiguchi[3] Akira Orita[3] Eiji Nunohiro[2]

Abstract: Many damages caused by RAT have been reported in relation to the attacks aimed at stealing information of corporate services and systems. In recent years, the threat from such targeted attacks has been increasing, and digital forensics has become more important as a method to identify the cause of infection and the damage scales. In this research, we have developed the Windows log analysis tool to visualize a timeline of attack activities and detect characteristic events, such as attack procedures and file falsification, by using the evidences that have been illegally intruded. In this paper, we report how to define the criterion for extraction in incident responses, and how to implement the log analysis tool. Furthermore, we report a timeline-based event log visualization function which filters logs recorded in normal times and extracts or visualizes logs with high probability of illegal operations such as falsification, showing its application examples.

Keywords: Malware, Event Log, Digital Forensics, Timeline, Lateral Movement

1. はじめに

近年，標的型攻撃の脅威は激化しており，情報処理推進機構が公開する情報セキュリティ 10 大驚異[1] において，組織における情報セキュリティの脅威では 2016 年から 5 年連続で 1 位にランクインしている[2]．Microsoft Windows[a] が提供している SMB や WMI などの標準機能や管理機能を用いて同じネットワーク内の他の端末にコマンドを送る，RAT（遠隔操作ツール）を用いてシステムへの侵入後にランサムウェアを実行するなどの被害事例なども報告されており[3]，無差別な攻撃による脅威のみならず，特定の組織，企業に対象を絞り，情報窃取を目的とした攻撃を行う標的型攻撃の脅威が増加傾向にある．このような背景から，これらの感染原因，被害範囲特定の手法としてデジタル・フォレンジックの重要性が高まっている．本研究では，Windows を対象とし，攻撃の被害調査に際して，各端末から抽出したログから一連の攻撃活動における全体像の概要を可視化するためのログ解析支援ツール（以下，本支援ツール）を開発している[4]. 本支援ツールの目的は，サイバー攻撃の被害におけるインシデント対応時の初動調査として断片的な情報を組み合わせるのではなく，攻撃活動の全体像から攻撃内容の詳細を深く掘り下げて分析を可能にすることである．そのため，インシデントのログから攻撃の詳細な内容を分析する前段階として，一連の攻撃活

1 東京情報大学大学院 総合情報学研究科
Graduate School of Informatics, Tokyo University of Information Sciences
2 東京情報大学 総合情報学部
Faculty of Informatics, Tokyo University of Information Sciences
3 株式会社日立システムズ サイバーセキュリティリサーチセンタ
Hitachi Systems, Ltd. Cyber Security Research Center

* g19004sn @edu.tuis.ac.jp

a) Microsoft，Microsoft Windows は，米国 Microsoft Corporation の米国およびその他の国における登録商標です．

動の全体概要を視覚的に表現する．

本論文では，本研究で定義したインシデント対応時のログ解析に用いる判断基準とそれらの実装方法，本支援ツールの主要な機能である攻撃活動を時系列に可視化するタイムライン型イベントログ可視化機能について説明する．次に，実際に行われた攻撃内容を基に 5 パターンの攻撃シナリオを作成し，そのシナリオに沿って模擬攻撃を実行した．そして，これらの模擬攻撃を通して得られたイベントログを本支援ツールで解析し，それらの解析結果を時系列に沿って可視化した．これによって，それぞれ異なる操作を行った各シナリオにおける特徴的なイベントの流れの可視化をすることが出来た．

2. 関連研究

ラテラルムーブメントが行われた端末のログから被害範囲を調査するためのツールとして，JPCERT/CC が提供している LogonTracer[5]などが挙げられる，このツールを使用することによって，感染が行われた端末が判明している場合に，その端末とリンクのつながっている端末を洗い出して調査することが可能となる．それによって不正なログオン時に使用されたアカウントの特定や感染の拡大が行われた端末など，ラテラルムーブメントが行われた痕跡を見つけることに繋がる．しかし，このツールは影響範囲の特定のみに特化しており，単体ではログオンが行われたホストの情報を時系列で整理することができないため，感染の原因となった端末の特定のために通信が行われた順序のようなラテラルムーブメント特有の情報を確認することができない. また, Microsoft が提供する Sysmon(System Monitor)[6]という Windows アクティビティの記録拡張ツールを用いることで, OS 標準では記録されないサービス，ネットワークコネクション，ファイル変更時間などの詳細なログを記録することが可能となる．これらのログを JPCERT/CC が提供する SysmonSearch[7]にインデックスすることで, 端末上で行われた不審な挙動やプロセスから関連するファイルやレジストリ情報を追跡することが可能である．しかし，これらの手法では環境に Sysmon を予めインストールしておく，常時ログを記録しておく必要があるなど，事前の準備が必要であり，このような対策を事前に行っていない組織，企業においては OS 標準で記録されるログから情報を収集する必要がある．加えて，これらの手法では特定のプロセスに関連するレジストリの洗い出しなど詳細な調査が出来る反面，調査したログの全体の流れをまとめるような機能はなく，本研究の目的である初期調査において断片的な情報を収集した後に整理する必要があるという課題の解決ができない．

このように，既存ツールの多くは，それぞれのログに対する分析が主であり，攻撃活動の全体像を得るためには被害ケースに合わせた複数のツールを使用する必要があることがわかる．また，これらのツールではログの検索などに焦点を向けており，各イベントの概要を掴むように情報の圧縮を行うことについても課題であると言える．

本研究では，これらの問題を解決するために，イベントログを解析するための 6 つの know-how を定義して本支援ツールに実装し，ログ解析の精度改善を進めている．その結果，タイムスタンプが改ざんされたレコードの検出，調査対象端末間で行われたリモートログオンの記録などの攻撃活動における特徴的なイベントの検出が可能となった．

3. know-how の概要と実装方法

イベントログを解析する判断基準として，人手によるデジタル・フォレンジックを行う際の知見を整理し，次の 6 つの know-how を定義した．

① タイムスタンプの SI，FN 属性の活用
② 時間単位別 MFT レコード数の活用
③ ディレクトリ別のタイムスタンプ外れ値の検知
④ Prefetch の動作特性の活用
⑤ Security イベントログのリモートログオン記録の活用
⑥ Microsoft-Windows-TerminalServices-LocalSessionManager¥Operational イベントログのリモートログオン記録の活用

3.1 タイムスタンプの SI，FN 属性の活用

3.1.1 概要

ファイルシステムの MFT(Master File Table)に記録されているタイムスタンプ情報のうち，SI(Standard Information)属性の値については，ユーザレベルのプロセスで変更が可能であり，それを悪用した timestomp[8]などの痕跡削除ツールも存在する．それと対象的に，FN(File Name)属性の値はシステムカーネルによってのみ変更が可能であり，変更，改ざんすることは非常に困難である[9]．これらの特性に着目し，FN 属性のタイムスタンプよりも SI 属性のタイムスタンプが古くなっているレコードはタイムスタンプの改ざんが行われた可能性が高いと推測する．

3.1.2 実装方法

MFT から抽出した全レコードから，ファイルが新規作成された時間を示す項目である CreateTime の SI 属性，FN 属性の 2 種類の情報を比較し，FN 属性よりも SI 属性が古いものを抽出した．

3.2 時間単位別 MFT レコード数の活用

3.2.1 概要

MFT 内のレコードは，ファイルの書き込み，変更などの動作によって記録される[10]．プログラムのインストール

などによって大量のファイル作成が行われるため，MFT レコードを時間単位別件数で集計することで平常時よりも多くのレコードが記録されていることが確認できる．この特性に着目し，レコードが大量に作成された時間帯付近のレコードからインストールされたプログラムを特定する．

3.2.2 実装方法

MFT 内のレコードを任意の単位時間でグルーピングし，各グループのレコード件数のカウントを行い，任意の閾値以上のものを抽出した．

3.3 ディレクトリ別のタイムスタンプ外れ値の検知

3.3.1 概要

プログラムがインストールされたディレクトリ配下に存在するファイル群のタイムスタンプは，それらの多くがインストールされた日時を記録している．この特性に着目し，同一ディレクトリ配下において，他のファイルと著しくタイムスタンプが異なるファイルに関連するレコードを特定する．

3.3.2 実装方法

3.2 で示した時間単位別 MFT レコード数の活用を用いてフィルタしたレコードの FilePath の情報を用いて，各レコードと同一のディレクトリに存在するファイルのグルーピングを行い，各グループ内で最も FN 属性の CreationTime が新しいレコードを抽出した．

3.4 Prefetch の動作特性の活用

3.4.1 概要

Windows 系 OS においてパスワードの窃取，認証情報の取得を行う際に用いられる Mimikatz は，平常時には記録されない特徴的なイベントログが記録されることが報告されている[11]．Mimikatz には，PowerShell からファイルレスで実行が可能なもの，exe 形式のものなど複数の実行形式が存在し，それぞれ残される痕跡が異なる．また窃取する情報によっても残される痕跡が異なり，パスワードハッシュを窃取する場合，イベントログには反映されず，Prefetch にのみ記録されることが報告されている[12]．この特性に着目し，悪性ソフトウェアが動作したか否かを特定する．

3.4.2 実装方法

プログラムの実行形跡（最終実行日時）が Prefetch に記録されるため，Mimikatz に関するログの有無で動作したか否かの判断を行った．

3.5 Security イベントログのリモートログオン記録の活用

3.5.1 概要

Windows 系 OS においてログオンの際に，Security イベントログにログオン情報が記録される．IIJ の資料 [13]では，端末のユーザがクライアントから離れている間に，攻撃者が RDP を使用してログオン，もしくはサーバへの侵入を試みることがあると報告されており，これらのリモートログオンに関連する情報をデジタル・フォレンジックにおける重要な情報としてピックアップしている．公式ドキュメントによれば，記録される情報のログオンタイプを確認することで，ログオンの際にネットワークを経由したのか，対話型ログオンが行われたのかなどを判別することができる[14]．特に，ログオンタイプが 10 のものは Windows 標準のリモートデスクトップ機能を用いてログオンが行われたものであり，Mimikatz などで窃取した認証情報をもとにリモートデスクトップでラテラルムーブメントを行う際に残される痕跡の特定に用いる．

3.5.2 実装方法

Security イベントログにイベント ID: 4624 が残されている場合はログオンの成功，イベント ID: 4625 ではログオンの失敗として検出する，また，ログオンが成功しているイベントのうち，ログオンの種別を示すログオンタイプが 10，もしくは 12 として記録されているレコードについて，Windows 標準のリモートデスクトップ機能を用いてログオンしたものとして抽出した．また，この know-how からログオンの失敗イベントが一定期間内に任意の閾値以上の回数出現する場合にブルートフォース攻撃として検出した．

3.6 Microsoft-Windows-TerminalServices-LocalSessionManager¥Operational イベントログのリモートログオン記録の活用

3.6.1 概要

3.5 で述べた Security イベントログと同様に，Microsoft-Windows-TerminalServices-LocalSessionManager¥Operational イベントログにもログオン関連のイベントが記録される．詳しい仕様は公開されていないが，どちらか片方のみにログオン関連イベントが記録されている場合などがあるため，個別に調査を行う必要がある．

3.6.2 実装方法

Microsoft-Windows-TerminalServices-LocalSessionManager¥Operational イベントログは，リモートデスクトップセッションに関連するイベントログを記録しており，イベント ID21 はログオン成功，23 はログオフ成功，24 は切断，25 は再ログオンが行われたことを示している．

これらの詳細なリモートログオンの挙動を確認することによって，ログオン成功イベントの記録後に複数の異なる IP から RDP の認証が行われるような，平常時に発生することのない順序，回数のイベントが記録されることの検知が可能となる．

4. 本支援ツールの概要と know-how の実装

本支援ツールは，調査対象端末から得られた証跡から主要な情報を抽出し，攻撃の概要と全体像を把握することを目的とする．攻撃の概要と全体像を把握する手法として，人手によってログ解析を行う際の know-how に着目する．実際に何らかの操作が行われた可能性のあるログを抽出するためには，複数の痕跡情報を組み合わせて比較検討する必要がある．本支援ツールでは，3 章で示した 6 つの know-how を機能化して実装した．本支援ツールはログ解析を行う前段階として，事前に調査対象端末のハードディスク及び仮想イメージファイルから log2timeline/plaso[15]を用いて証跡を抽出し，Elasticsearch[16]へインデックスを行う．

本支援ツールの処理の概要を次に示す．

① Elasticsearch にインデックスされた各種証跡に対して know-how に基づいて構築されたクエリ，及びその後処理を用いて平常時に記録されるログのフィルタリングを行う．
② フィルタされたログはイベント種別ごとに整形が行われ，タイムライン出力機能によって Json，PlantUml，Excel などの形式に変換後，出力が行われる．

本支援ツールの処理の流れを図 1 に示す．図 1 において，調査対象 A～C はラテラルムーブメントによる被害の影響が疑われる同じ LAN 内の調査対象端末である．本支援ツールでは，各調査対象端末から抽出した証跡を Elasticsearch にインデックスした後に，平常時のログをフィルタ処理，特徴的なイベントを抽出する処理，及び全体像の把握を行うためのログ可視化処理などの機能を通してタイムラインを出力する．

次に，know-how の実装について記述する．3 章で示した 6 つの know-how は，図 1 のフィルタ機能に実装し，それらの処理をイベントログ可視化機能から必要に応じて呼び出すことによって攻撃活動の大まかな把握が可能となる．これらの know-how を本支援ツールの機能として実装することで，大容量のログファイルからマルウェアによって行われたと推測される痕跡を抽出することが可能となり，マルウェアの検知，リモートログオンの記録，ソフトウェアのインストールなどの主要なイベントを時系列にマッピングすることが出来る．この結果，一連の攻撃活動の概要をタイムライン上に表現することが可能となる．

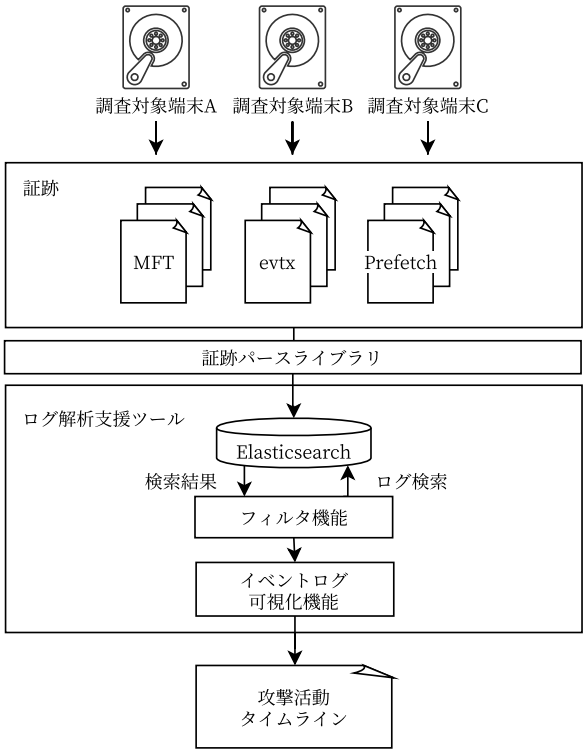

図 1　本支援ツールの処理の流れ

Figure 1　Process flow of Log Analysis Support Tool.

5. イベントログ可視化機能

本支援ツールのイベントログ可視化機能では，3 章で示した know-how，もしくはそれらを複数組み合わせた形に沿ったクエリを定義し，Elasticsearch にインデックスされている証跡をフィルタリングした．また，必要に応じてログの集計，ログ同士の紐付けなどの後処理を行うことで複数ログにまたがるイベントを検出した．具体的には，次のような処理を行っている．

① 3.1～3.3 で示した know-how を組み合わせ，MFT から CreationTime の SI 属性が FN 属性よりも新しくなっているレコードをタイムスタンプが改ざんされた可能性があるものとして抽出する．
② ①で抽出したレコードの内，MFT の時間単位別件数が多くなっているレコードを抽出する．
③ ②で抽出したレコードと正規プログラムのインストール日時が一致しないレコードを抽出する．
④ ③で抽出したレコードのタイムスタンプと同一ディレクトリ内の他のレコードのタイムスタンプを比較して，最も乖離しているレコードをタイムスタンプ改ざんの可能性が高いレコードとして抽出する．

可視化時における視認性確保のための情報圧の縮手法として，図 2 に示すような UML のシーケンス図をベースとして，各ライフラインと調査対象端末を対応させ，ライフ

ライン間をつなぐメッセージとイベントのアクティベートによってログオン関係の可視化を行った．図 2 において，攻撃者は次の操作を行っている．

① 被害側端末（victim1）に対してリモートログオン
② victim1 上で Mimikatz を実行，認証情報の窃取
③ 被害側端末（victim2）に対してブルートフォース攻撃
④ victim2 にログオン，タイムスタンプの改ざん
⑤ 認証情報の窃取後，victim1，2 から接続断

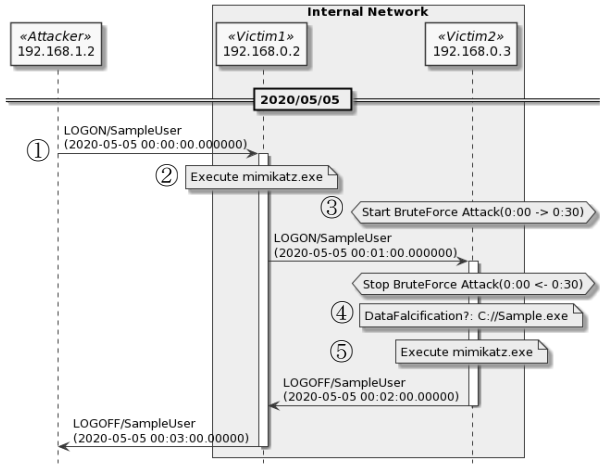

図 2　生成する攻撃活動タイムラインのイメージ
Figure 2　Image of the Generated Attack Activity Timeline.

また，これらの可視化を行うために抽出したログから，対応するイベントの概要をライブラリに対応する形式に整形し，PlantUML[17]を可視化ライブラリとして用いてタイムラインの生成を行った．

6. 適用例

本支援ツールの適用例として，図 3 に示す実験環境を構築し，5 パターンの攻撃シナリオに沿った模擬攻撃を行った．

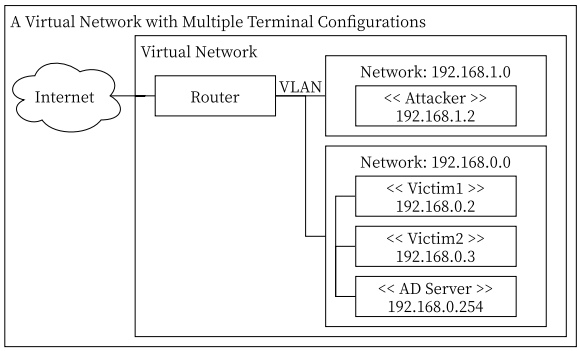

図 3　模擬攻撃対象のネットワーク構成
Figure 3　Network Configuration of Simulated Attack Target.

模擬攻撃の実行にあたって，Active Directory によるアカウント管理下にある複数の端末構成の仮想ネットワーク環境を構築した．攻撃者は，予め定められた攻撃シナリオの手順に従って，構築した仮想ネットワーク環境内の攻撃対象端末に対して遠隔操作及び攻撃活動を行った．その結果から得られた調査対象端末のログを収集し，本支援ツールのイベントログ可視化機能により，攻撃活動に関するイベントログのタイムラインを生成する．

6.1 攻撃シナリオ

模擬攻撃の実施では，5 パターンの攻撃シナリオ a～e と 7 つの特徴的な攻撃を定義し，5 つの攻撃シナリオのイベントを可視化した結果から，各シナリオの攻撃内容を評価した．

【攻撃シナリオ】

a　認証情報の使い回しや，事前に侵入を行ったアカウントよりも上位の権限を持つアカウントの権限を奪取することを目的とした攻撃であり，ラテラルムーブメントを行いながら Mimikatz を用いて複数台の認証情報を窃取する．

b　マルウェアはアンチフォレンジックの為にファイルのタイムスタンプを変更することが知られており[18]，それらの痕跡情報削除を目的としたシナリオである．本シナリオでは OS 標準の機能である Powershell を用いたタイムスタンプの改ざんを行う．

c　単純なパスワードが設定されたアカウントに対する不正ログオン，権限の奪取を目的とする攻撃である．本シナリオではブルートフォース攻撃を含む操作を行う．

d　国内標的型攻撃レポート[19]によると，アンチウイルスソフトウェアによるシグネチャ検知の回避や解析困難化を狙って不正ファイルの分割圧縮を行うことがあるため，そのようなケースを想定した攻撃である．

e　リモートログオン先の端末でマルウェアの実行を行う．残される痕跡はマルウェアによって差異があるため，本シナリオでは模擬的に作成したソフトウェアをマルウェアの代用として扱った．

【特徴的な攻撃】

- ブルートフォース攻撃
- タイムスタンプ改ざん
- Mimikatz による認証情報窃取
- ラテラルムーブメント
- 分割圧縮ファイルの作成
- 分割圧縮ファイルの削除
- マルウェアの実行

攻撃シナリオ a～e の攻撃内容を表 1 に示す．

表 1　攻撃シナリオ a～e の攻撃内容

Table 1　Attack activities of attack scenario a～e.

	ブルートフォース攻撃	タイムスタンプ改ざん	認証情報窃取	ラテラルムーブメント	ファイル作成	ファイル削除	マルウェア実行
a	N	N	Y	Y	N	N	N
b	N	Y	N	Y	N	N	N
c	Y	Y	Y	Y	N	N	N
d	Y	Y	Y	Y	Y	Y	N
e	Y	Y	Y	Y	N	N	Y

Y：該当する攻撃を実行する，N：該当する攻撃を実行しない

6.1.1 シナリオ a

シナリオ a のタイムラインを図 4 に示す.

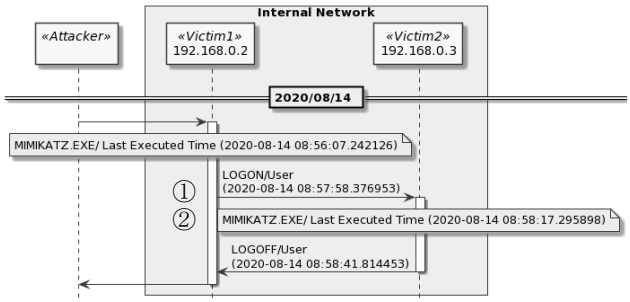

図 4　シナリオ a のタイムライン

Figure 4　Timeline of Scenario a.

図 4 から，次のような事象が確認できる.

① ラテラルムーブメントの挙動
② Mimikatz による認証情報の窃取

6.1.2 シナリオ b

シナリオ b のタイムラインを図 5 に示す.

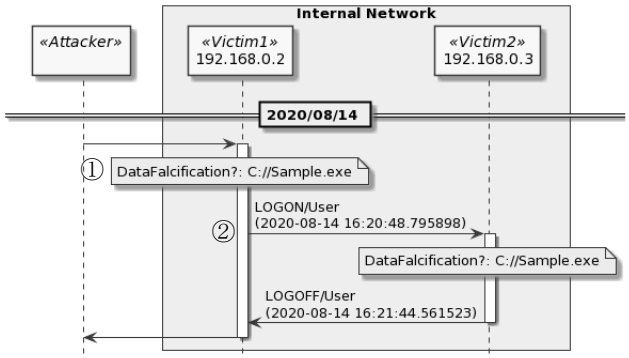

図 5　シナリオ b のタイムライン

Figure 5　Timeline of Scenario b.

図 5 から，次のような事象が確認できる.

① タイムスタンプの改ざん
② ラテラルムーブメントの挙動

6.1.3 シナリオ c

シナリオ c のタイムラインを図 6 に示す.

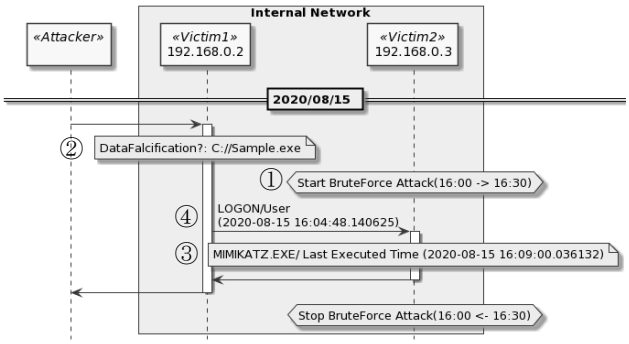

図 6　シナリオ c のタイムライン

Figure 6　Timeline of Scenario c.

図 6 から，次のような事象が確認できる.

① ブルートフォース攻撃
② タイムスタンプの改ざん
③ Mimikatz による認証情報の窃取
④ ラテラルムーブメントの挙動

6.1.4 シナリオ d

シナリオ d のタイムラインを図 7 に示す.

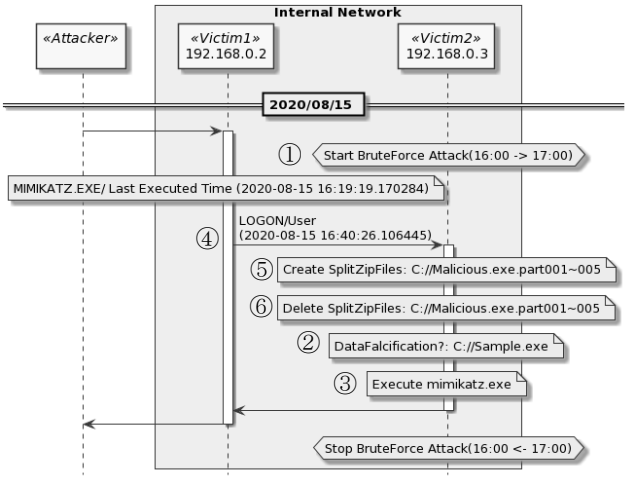

図 7　シナリオ d のタイムライン

Figure 7　Timeline of Scenario d.

図 7 から，次のような事象が確認できる.

① ブルートフォース攻撃
② タイムスタンプの改ざん

③　Mimikatz による認証情報の窃取
④　ラテラルムーブメントの挙動
⑤　分割圧縮ファイルの作成
⑥　分割圧縮ファイルの削除

6.1.5 シナリオ e

シナリオ e のタイムラインを図 8 に示す.

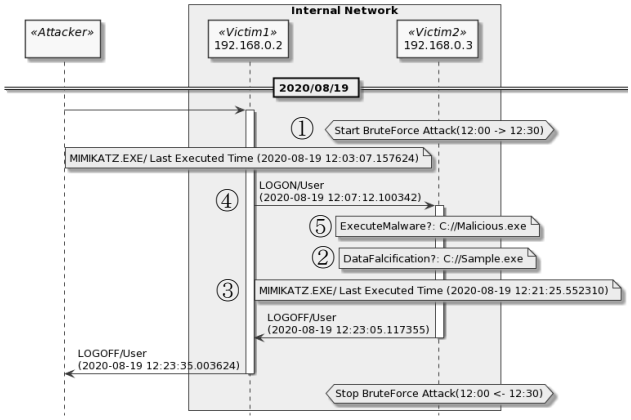

図 8　シナリオ e のタイムライン
Figure 8　Timeline of Scenario e.

図 8 から，次のような事象が確認できる.

①　ブルートフォース攻撃
②　タイムスタンプの改ざん
③　Mimikatz による認証情報の窃取
④　ラテラルムーブメントの挙動
⑤　マルウェアの実行

7. 考察

本研究では，メモリダンプやネットワークのパケットキャプチャのような，ライブフォレンジックで用いられる情報を用いずに，攻撃活動が行われた事後の端末から得られる証跡からタイムラインの俯瞰図を生成する可視化機能について，それぞれ異なる操作を行った 5 パターンの攻撃シナリオに沿った模擬攻撃活動について適用例を示した．これらの適用例によって，シナリオごとに行った攻撃内容と本支援ツールの可視化機能の出力である攻撃タイムラインの内容が一致していることが確認できる．このように，人手による解析の際に用いる知見をシステムに実装することで，これまでの人手によるデジタル・フォレンジックで行う作業の短縮を行うことが可能となり，人的，時間的なコストの削減ができるようになったと考える．また，関連研究で述べた複数の分析ツールを使い分け断片的な情報を収集して俯瞰図にまとめる作業の短縮，情報の圧縮表現など課題の解決を果たすことができたと考える.

8. まとめ

本論文では，外部から不正にアクセスされた端末の痕跡情報を用いて，行われた攻撃活動の概要を把握するためのログ解析支援ツールの実装と適用例について報告した.

本支援ツールでは，OS 標準のログ機能のみで記録された膨大な証跡から，人手による解析の際に用いる知見を基に攻撃活動に関連する特徴的なイベントを抽出しタイムライン型の俯瞰図として出力することで，攻撃活動の概要を把握することができた．これにより，これまでの初動調査に必要な，断片的な情報から大まかに証跡のチェックを行う範囲を狭めていきタイムラインに整理する過程を省略し，攻撃活動の概要から必要に応じた詳細な調査が可能となる.

9. 今後の展望

サイバー攻撃に対するログ解析精度の向上のため，本支援ツールに対して次のような機能追加・改良を進める.

(1) 本支援ツールによって得られた情報を起点として，それらに関連する情報から攻撃者の狙いや攻撃パターンとログの関連性について分析する.
(2) K.K.Sindhu ら[20]の研究では，データの損失や改ざん，ログオンの試行などのイベントを基に，ファイルシステム及びネットワーク上の証跡から，頻出攻撃パターンといくつかのルールを設定して攻撃の動機を推定するシステムの提案が行われている．それらの攻撃者の動機と証跡に記録されるイベントの関連付けについて解析し，攻撃パターンを分類する.
(3) 現時点では，MFT，イベントログ，Prefetch のみを証跡として用いているが，ブラウザキャッシュやレジストリなど，他の証跡についても調査，検討を行い，新規 Know-How を定義する.
(4) 本研究では，シナリオごとに異なる操作を行いログへの分析を行ったが，情報窃取，破壊，ランサムウェアなどによる金銭の要求など攻撃者の目的をベースにした実験について検討する.

謝辞　本研究を進め論文を執筆するにあたり，貴重なご意見と資料を提供して頂いた株式会社日立システムズサイバーセキュリティリサーチセンタのエンジニアの皆様，システム開発や機能評価などにご協力いただいた東京情報大学布広ゼミの学生の方々に深謝いたします.

参考文献

[1] “情報処理推進機構 情報セキュリティ 10 大脅威 2020”. https://www.ipa.go.jp/security/vuln/10threats2020.html, (参照 2020-08-18).

[2] “株式会社 FFRI 改めて確認する標的型攻撃の脅威とは”. https://www.ffri.jp/blog/2020/03/2020-03-12-What-are-the-threats-of-targeted-attacks.htm, (参照 2020-08-18).

[3] “警視庁 令和元年度上半期におけるサイバー空間をめぐる脅威の情勢等について”. http://www.npa.go.jp/publications/statistics/cybersecurity/data/R01_kami_cyber_jousei.pdf, (参照 2020-04-08).

[4] 中野心太, 他 7 名. 外部から不正侵入されたシステムのログ解析支援ツールの開発. コンピュータセキュリティシンポジウム 2019 論文集, 2019, 194-199.

[5] "LogonTracer を用いた不正ログオンの調査". https://blogs.jpcert.or.jp/ja/2018/01/logontracer2.html, (参照 2020-04-08).

[6] "Sysmon". https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon, (参照 2020-04-08).

[7] "Sysmon ログを可視化して端末の不審な挙動を調査 ~SysmonSearch~". https://blogs.jpcert.or.jp/ja/2018/09/SysmonSearch.html, (参照 2020-04-08).

[8] "timestomp". https://www.offensive-security.com/metasploit-unleashed/timestomp, (参照 2020-04-08).

[9] "MAC(b) times in Windows forensic analysis". https://www.andreafortuna.org/2017/10/06/macb-times-in-windows-forensic-analysis, (参照 2020-04-08).

[10] "Windows 7 MFT Entry Timestamp Properties". https://www.sans.org/blog/windows-7-mft-entry-timestamp-properties, (参照 2020-04-08).

[11] "IIJ Technical WEEK2017 Mimikatz 実行痕跡の発見手法". https://www.iij.ad.jp/dev/tech/techweek/pdf/171108_02.pdf, (参照 2020-04-08).

[12] "インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書". https://www.jpcert.or.jp/research/20160628ac-ir_research.pdf, (参照 2020-04-08).

[13] "Event Log Analysis". https://sect.iij.ad.jp/d/2018/05/044132/training_material_sample_for_eventlog_analysis.pdf, (参照 2020-04-08).

[14] "4624(S) An account was successfully logged on". https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624, (参照 2020-04-08).

[15] "log2timeline/plaso". https://github.com/log2timeline/plaso, (参照 2020-04-08).

[16] "Elasticsearch", https://www.elastic.co, (参照 2020-04-08).

[17] "PlantUML". https://plantuml.com, (参照 2020-04-08).

[18] “IIJ セキュリティ動向 2010(2) デジタルフォレンジックに関する取り組み”. https://www.iij.ad.jp/dev/tech/techweek/pdf/techweek_20101119_2-1_t-haruyama.pdf, (参照 2020-08-18).

[19] “国内標的型攻撃分析レポート 2019 年版”. https://resources.trendmicro.com/jp-docdownload-form-m139-sem-report-2019-2.html, (参照 2020-08-18).

[20] K.K.Sindhu, and B.B. Meshram. Digital Forensics and Cyber Crime Datamining, Scientific Research. Journal of Information Security, Vol.3, No.3, 2019, 196-201.