原著論文

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可視化機能の開発

中野心太*・早稲田篤志**・村上洋一**・岸本頼紀**
花田真樹**・関口竜也***・折田彰***・布広永示**

要旨：企業のサービス，システムなどの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などが報告されている．そして，無差別な攻撃のみならず，特定の組織や企業に対象を絞っ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から，攻撃者が行った一連の攻撃活動を可視化し，マルウェアの攻撃手順，ファイルの改ざんや攻撃者の目的を解析するログ解析支援ツールを開発している．本論文では，インシデント対応時の痕跡情報抽出作業から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からフィルタ処理，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時系列に可視化するタイムライン型のイベントログ可視化機能について報告する．

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 Visualization Function Using Traces of Unauthorized Access

Shinta NAKANO*, Atsushi WASEDA**, Yoichi MURAKAMI**,
Yorinori KISHIMOTO**, Masaki HANADA**,
Tatsuya SEKIGUCHI***, Akira ORITA*** and Eiji NUNOHIRO**

Abstract: Several damages caused by RAT (remote access tools) have been reported in association with attacks aimed at stealing information regarding corporate services and systems. In addition to indiscriminate attacks, the threat of targeted attacks aimed at specific organizations and companies is increasing. Digital forensics has therefore become increasingly important as a method for identifying the cause of infection and the extent of damage. Hence, in this research, we developed a log analysis support tool for the Windows operating system to visualize the series of activities performed by an attacker by incorporating trace information obtained from the compromised computer system. Furthermore, the proposed log analysis support tool can analyze the malware's attack procedure, file tampering, and the attacker's objective. In this paper, we defined the criteria for extracting trace information while responding to various incidents and accordingly implemented them for the proposed log analysis support tool. Furthermore, we demonstrate a timeline-based event log visualization function that extracts logs having a high probability of illegal operations (such as file tampering and filtering of logs recorded at normal times).

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

* 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
** 東京情報大学　総合情報学部
Faculty of Informatics, Tokyo University of Information Sciences
*** 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

2020年5月22日受付
2020年7月28日受理

1．はじめに

2019年以降，国内でランサムウェアの感染を目的とするばらまき型メールの攻撃件数が増加していることが報告されている[1]．このような攻撃に関連して，Windows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が報告されており[2]，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．

一般的にデジタル・フォレンジックでは，ヒアリングによって得た被害状況から予測される攻撃内容や攻撃範囲に合わせて複数のツールを使用してマルウェアや攻撃者の痕跡を調査する．この際，システムログやMFTなどOS内の各種痕跡データに対応したツールを用いて，断片的な情報を収集する．次に，それらによって集められた情報を時系列ごとに整理し，一連の攻撃活動の概要を示すタイムラインにすることで攻撃の全体像を掴む必要がある．しかし，これらの分析手法で使用されるツールは，特定のログに対する詳細な分析には秀でているが，汎用的に全体像の概要を把握することには適していない．また，攻撃対象端末と同じネットワーク上の別の端末にLAN経由で次々と横方向へと侵入，展開を繰り返すラテラルムーブメントによる攻撃の調査などでは，組織内に存在する複数の端末を横断的に調査する必要があり，個々の端末データから概要を得ることは多大な人的，時間的なリソースが必要となる．

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[3]．本支援ツールでは，膨大なサイズのログから攻撃の詳細な内容を分析する前段階として，一連の攻撃活動の全体概要を視覚的に表現する．その結果，サイバー攻撃の被害における事後調査の初動調査として，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することが可能となる．

本論文では，本研究で定義したログ解析の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のイベントログ可視化機能について報告する．このため，平常時に記録されるログからフィルタ処理，ファイル改ざんなどの不正な操作が行われた可能性の高いログを抽出する実験環境として，組織，企業を模した構成の仮想ネットワークを構築した．次に，実際に行われた攻撃内容を基に定義した攻撃手順書に沿って模擬攻撃を実行した．そして，このログを本支援ツールで解析し，解析結果を時系列に可視化した．これによって，複数の端末に対して横断的な攻撃活動の痕跡が残されているケースにおいても，攻撃の全体像を可視化することが出来た．

以下，２章では関連研究について述べる．３章ではインシデント対応時におけるデジタル・フォレンジックにおいて，手作業でフィルタリングを行う際の判断基準となる知見（以下，know-how）について述べる．４章では本支援ツールの概要とknow-howの実装について述べる．５章ではタイムライン型のイベントログ可視化機能について述べる．６章，７章では本支援ツールの適用例と考察について述べる．８章，９章ではまとめと今後の展望について述べる．

2．関連研究

ラテラルムーブメントが行われた被害環境を調査するためのツールとして，JPCERT/CCが無償で提供しているLogonTracer[4]などが挙げられる．LogonTracerでは，攻撃によって被害を受けた可能性のある範囲を明らかにするために，リモートデスクトップ機能によってアカウントのログオンが行われたホスト間の結合関係をリンクでつなぐことによって表現し，攻撃の影響範囲の可視化を行う．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）[5]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Sysmon Search[6]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．

Sysmonによる証跡の常時収集とElasticsearchへのインデックスを行うことで，複数端末に横断的に存在するログからラテラルムーブメントの痕跡を検索する研究例として，“Lateral movement detection using ELK stack”[7]が挙げられる．当該研究では，PowerShell, Mimikatz，RDPなどを含む23パターンの攻撃を行い各攻撃手法によってSysmonに記録される痕跡を分析している．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，先行研究の多くは，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，これらの研究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，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（Master File Table）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]．

SI属性のタイムスタンプの多くは，FN属性のタイムスタンプと同時刻もしくはそれ以降の時刻である．また，マルウェアが作成，変更を行ったファイルのタイムスタンプを改ざんする際，フォレンジックを困難にする目的で同ディレクトリ内の他のファイルのタイムスタンプと同じ値か近しい値を自身のタイムスタンプに設定することがある．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．

また，前述した公式ドキュメントには記載がないが，開発者用ドキュメント[15]の列挙型データ型から，ログオンタイプが13まであることが確認できる．“Investigating Hard Disks, File and Operating Systems”[16]によると，ログオンタイプ12であるCachedRemoteInteractiveによってキャッシュを使用したリモートログオンのイベントが内部的に記録されていることが報告されている．過去の事例として，ログオンタイプがCachedRemoteInteractiveとして記録された攻撃の事例があったことから，ログオンタイプ12もログオンタイプ10同様に調査対象とした．

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．更に，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

一般的なログ解析ツールでは，異なる痕跡を組み合わせた分析や全体概要を得ることが難しい．また，近年では標的型攻撃などで行われる攻撃には，ウイルス対策ソフトウェアなどによって検知されやすいマルウェアを極力用いずにPowerShellなどのOS標準の機能が利用される傾向にある[17]．そのため，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．例えば，OSのインストール日時より後に作成されたファイルのうち，MFTのFN属性よりもSI属性の方が古いファイルは改ざんが行われた可能性があるため，このファイルに関する他のログファイルを調査し状況を把握する．このように，know-howの多くは１つの痕跡情報と他のログ情報を関連づけることによって抽出が可能となる．すなわち，他のログで現れた怪しい痕跡情報を基準にしたフィルタリングを実現できれば，概要を得るための主要な情報を抽出できる．また，ブルートフォース攻撃のような大量にログオンの失敗が行われるログは単純に抽出しただけでは概要図が肥大化する．そこで，類似情報を時間単位で区切ってグループ化し，情報を圧縮して表示することで，重要なイベントが埋もれないよう視覚的に表現した．

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[18]を用いて証跡を抽出し，ElasticSearch[19]へインデックスを行う．この際，先行研究[3]ではEvtxToElk[20]を利用することで，直接調査対象のログをインデックスしていたが，他の証跡への対応状況，インデックスにかかる時間的コストが高いことからイベントログ，Prefetch，MFTを対象とした証跡のパースライブラリを独自に作成しOSSとして公開し，有志で継続的にメンテナンスを行うことで解決を行った．

図１に，本支援ツールで開発したライブラリ（This Library）とEvtxToElkを用いてElasticsearchへのインデックスをそれぞれ100回実行した平均実行時間を示す．グラフから，先行研究と比較して約98.04％の高速化ができていることが読み取れる．実行時間の計測にはLogonTracerのSampleとして提供されているファイルサイズ約30MBのSecurityイベントログを用いた．実行環境を表１に示す．

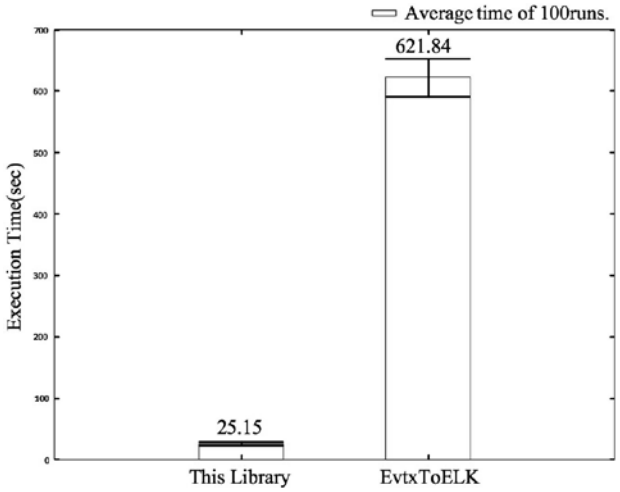

図１　証跡パースライブラリの平均実行時間
Figure 1　Average Execution Time of the Trail Parsing Library

表１　証跡パースライブラリの実行環境
Table 1　Running Environment of the Trail Parsing Library

OS	macOS 10.13.6
Processor	Intel Core i7 3.4GHz
Memory	32GB 1333MHz DDR3
Python	3.7.0（Clang 10.0.0）
Elasticsearch	7.4 – docker official image（Docker: 19.03.08）

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２に示す．図２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が疑われる同じLAN内の調査対象端末である．

ユーザは，各調査対象端末から抽出した証跡をElasticsearchにインデックス後に支援ツールを実行することで，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イベントログ可視化などの機能を通してタイムラインを出力することができる．

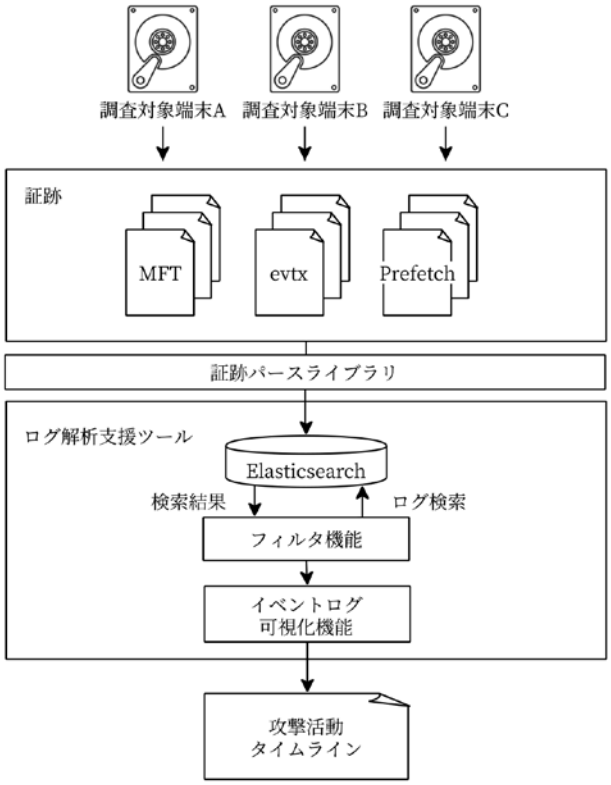

図２　本支援ツールの処理の流れ
Figure 2　Process flow of Log Analysis Support Tool

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２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．

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３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．また，一定期間内に設定された閾値以上のリモートログオン施行，失敗が行われた際に，閾値を下回るまでの期間をブルートフォース攻撃として扱い，ライフライン上に開始，終了のイベントを表示した．図３において，攻撃者は次の操作

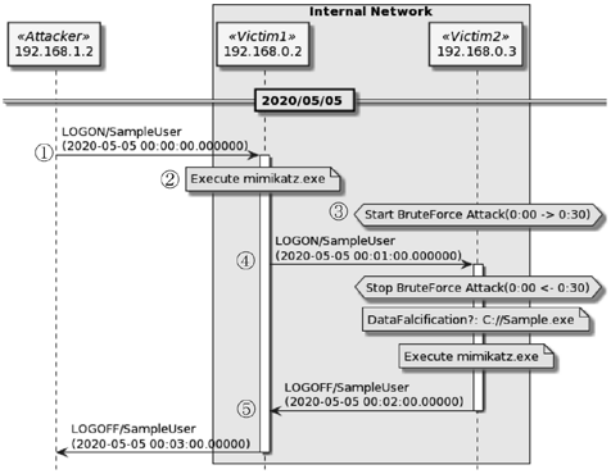

図３　生成する攻撃活動タイムラインのイメージ
Figure 3　Image of the Generated Attack Activity Timeline

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

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[21]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

イベントログ可視化機能の適用例として，次に示す２パターンの実験環境を構築して模擬攻撃を行った．

- 単一端末
- 企業，組織を模したネットワーク構成の複数端末

その結果で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．

模擬攻撃活動にあたって，単一の端末構成（図４上）と複数の端末構成（図４下）の仮想ネットワーク環境を構築し，攻撃者は，予め定められた手順に従って，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リモート操作を行った．

６．１　単一端末における適用例

単一端末の構成における適用例を図５に示す．

図５から，次のような事象が確認できる．

① 被害側端末に対してブルートフォース攻撃が行われた
② 攻撃者が被害側端末にログオン後にmimikatzを使用したことから認証情報の窃取が行われた
③ ファイルのタイムスタンプが改ざんされた

これらの結果から，バックドアのように発見を遅らせるような悪意あるファイルが作成されているで

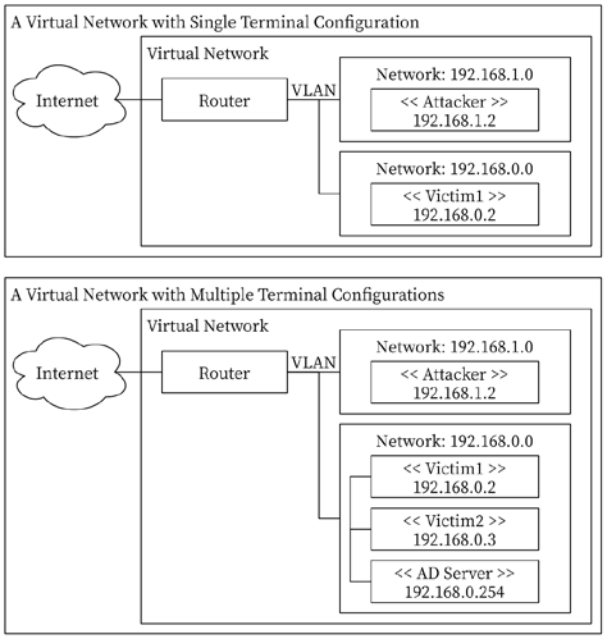

図４　模擬攻撃対象のネットワーク構成
Figure 4　Network Configuration of Simulated Attack Target

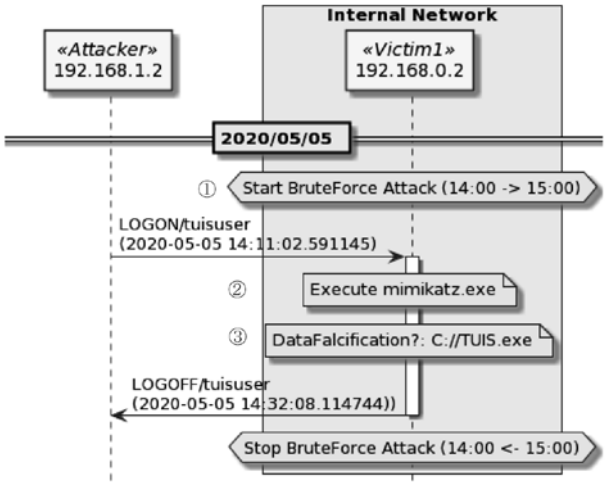

図５　単一端末構成における適用例
Figure 5　Timeline Example of Single Terminal Configuration

あろうということが読み取れる．特定の時間帯にどのユーザがログオンしているかの調査においても，活性区間上に可視化されたイベントから攻撃活動の流れを確認することができる．

６．２　企業，組織を模した構成の複数端末における適用例

複数端末の構成における適用例を図６に示す．図６から，次のような特徴的なイベントが可視化されていることが確認できる．

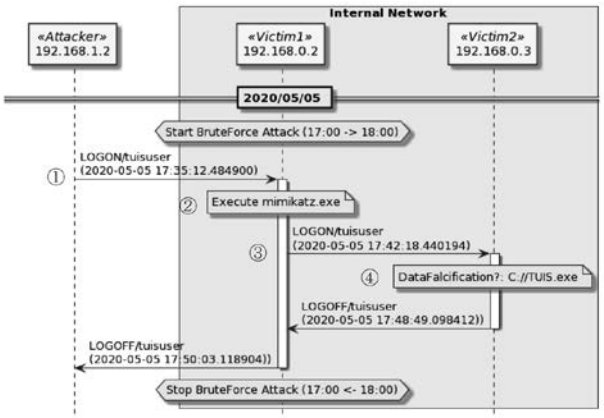

図６　複数端末構成における適用例
Figure 6　Timeline Example of Multiple Terminal Configurations

① ホスト間のリモートログオンの対応関係
② mimikatzの実行，認証情報の窃取
③ 被害端末と同ネットワーク内の他の端末に対して侵入を繰り返すラテラルムーブメント
④ ファイルのタイムスタンプ改ざん

７．考　　察

６．１，６．２の適用例から，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．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，単一の端末構成，複数の端末構成における適用例を示した．また，[20]を本支援ツールのインデックス処理に用いる際の欠点であった，ログのパース速度の改善にあたってライブラリの新規開発を行っており，前処理の高速化についても成功している．

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．

8．まとめ

本論文では，外部から不正に侵入を受けたシステムにおいて得られた証跡から，行われた攻撃活動の概要を把握するための本支援ツールにおけるタイムライン型のイベントログ可視化機能について報告した．

本支援ツールでは，OS標準の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る．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）実装した知見から得られた関連情報を起点として，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らの研究[22]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のみの解析を行っているが，ブラウザキャッシュやレジストリなど，関連する他の証跡についても調査，検討を行い，新規know-howを定義していく．

（4）ログ取得用実験環境において，攻撃目標，シナリオを設定した複数の攻撃者に攻撃を実施させることでログのサンプル数を増やすとともに，攻撃者や手順の違いによるログへの影響分析，攻撃手順とログ，実施目的の関連付けを行うことで，攻撃者の攻撃目的の推測などの行動特性分析を検討する．

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］Trend Micro: 2019年 第1四半期セキュリティラウンドアップ：データを暗号化する標的型攻撃（オンライン），入手先.〈https://resources.trendmicro.com/jp-docdownload-form-m121-web-2019q1-securityroundup.html〉（参照2020-04-08）.

［2］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（オンライン），入手先.〈http://www.npa.go.jp/publications/statistics/cybersecurity/data/R01_kami_cyber_jousei.pdf〉（参照2020-04-08）.

［3］中野心太，早稲田篤志，村上洋一，岸本頼紀，花田真樹，関口竜也，折田彰，布広永示：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．情報処理学会．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.

［4］JPCERT/CC: LogonTracerを用いた不正ログオンの調査（オンライン），入手先.〈https://blogs.jpcert.or.jp/ja/2018/01/logontracer2.html〉（参照2020-04-08）.

［5］Microsoft: Sysmon（online），available from〈https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon〉（accessed 2020-04-08）.

［6］JPCERT/CC: Sysmonログを可視化して端末の不審な挙動を調査～ SysmonSearch ～（オンライン），入手先.〈https://blogs.jpcert.or.jp/ja/2018/09/SysmonSearch.html〉（参照2020-04-08）.

［7］Jain Utkarsh: Lateral movement detection using ELK stack. Published ETD Collection, University of Houston, 2019.

［8］OFFENSIVE security: timestomp（online），available from〈https://www.offensive-security.com/metasploit-unleashed/timestomp/〉（accessed 2020-04-08）.

［9］Andrea Fortuna: MAC（b）times in Windows forensic analysis（online），available from〈https://www.andreafortuna.org/2017/10/06/macb-times-in-windows-forensic-analysis〉（accessed 2020-04-08）.

［10］SANS: Windows 7 MFT Entry Timestamp Properties（online），available from〈https://www.sans.org/blog/windows-7-mft-entry-timestamp-properties/〉（accessed

2020-04-08）.
［11］IIJ: IIJ Technical WEEK2017 Mimikatz実行痕跡の発見手法（オンライン），入手先〈https://www.iij.ad.jp/dev/tech/techweek/pdf/171108_02.pdf〉（参照2020-04-08）.
［12］JPCERT/CC: 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（オンライン），入手先〈https://www.jpcert.or.jp/research/20160628ac-ir_research.pdf〉（参照2020-04-08）.
［13］IIJ-SECT: Event Log Analysis（online），available from〈https://sect.iij.ad.jp/d/2018/05/044132/training_material_sample_for_eventlog_analysis.pdf〉（accessed 2020-04-08）
［14］Microsoft: Threat protection, More Windows 10 security, 4624（S）: An account was successfully logged on（online），available from〈https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624〉（accessed 2020-04-08）.
［15］Microsoft: Windows Dev Center, SECURITY_LOGON_TYPE enumeration（online），available from〈https://docs.microsoft.com/en-us/windows/win32/api/ntsecapi/ne-ntsecapi-security_logon_type〉（accessed 2020-04-08）.
［16］EC-Council, Computer Forensics: Investigating Hard Disks, File and Operating Systems, EC-Council Press（2009）.
［17］Trend Micro: 2020年セキュリティ脅威予測，入手先〈https://resources.trendmicro.com/jp-docdownload-form-m189-web-2020prediction.html〉（参照：2020-04-08）.
［18］log2timeline: log2timeline/plaso（online），available from〈https://github.com/log2timeline/plaso〉（accessed 2020-04-08）.
［19］Elastic: Elasticsearch（online），available from〈https://www.elastic.co/jp/〉（accessed 2020-04-08）.
［20］Dan Gunter & Marc Seitz: EvtxToElk: A Python Module to Load Windows Event Logs into ElasticSearch（online），available from〈https://dragos.com/blog/industry-news/evtxtoelk-a-python-module-to-load-windows-event-logs-into-elasticsearch〉（accessed 2020-04-08）.
［21］Arnaud Roques: PlantUML（online），available from〈https://plantuml.com/〉（accessed 2020-04-08）.
［22］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.