# インシデント対応時のファイル証跡収集を強化するネットワークフォレンジック方式の改良

乾 真季[1] 海野 由紀[1] 及川 孝徳[1] 金谷 延幸[1,2] 津田 侑[2] 遠峰 隆史[2] 井上 大介[2] 鳥居 悟[1]

**概要**：標的型攻撃をはじめとするサイバー攻撃において攻撃者は標的の組織に侵入した後，マルウェアを送り込み，リモート管理操作を実行することにより攻撃拡大を行う．攻撃による被害を最小限に抑えるには，攻撃者が悪用したファイルを特定し，調査することにより，攻撃の全容を明らかにすることが重要である．著者らは 2019 年に通信データを解析し，攻撃者が実行したリモート管理操作とリモートファイル書き込みをひも付けることにより，攻撃の進行度に応じた攻撃関連ファイルのリアルタイムでの収集を実現するネットワークフォレンジック方式を提案した．本稿では，攻撃関連ファイル収集精度を向上させるための，リモート管理操作とリモート書き込みされたファイルのひも付けの改良手法を提案する．本改良手法は，これまで照合が困難であった Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) プロトコルに対応するものであり，これにより，悪用されやすい更新系リモート管理操作にもファイル証跡の特定範囲を拡げるものである．提案した改良手法を実装したプログラムを用いて MWS Datasets 2019 の攻撃観測データや Microsoft の Advanced Threat Analytics Attack Simulation Playbook のシナリオを再現した模擬攻撃データを解析し，ファイル収集精度が向上したことを示した．

# Improvement of Network Forensic Method to Enhance File Evidence Collection for Incident Response

Maki Inui[1] Yuki Unno[1] Takanori Oikawa[1] Nobuyuki Kanaya[1,2] Yu Tsuda[2] Takashi Tomine[2] Daisuke Inoue[2] Satoru Torii[1]

## 1. はじめに

近年では標的型攻撃をはじめとするサイバー攻撃により組織内にマルウェアを送り込まれ，組織内の諜報活動が行われた結果，機密情報を窃取されてしまうことが後を絶たない．攻撃者は，標的の組織内のネットワークの端末に RAT (Remote Access Trojan/Remote Administration Tool) と呼ばれるマルウェアを送り込み，感染させることで組織内に侵入する．そして，感染端末をリモート操作し，組織のネットワークや周囲の端末に関する情報を収集しながら機密情報の探索を行う．さらに感染端末から周囲の端末に攻撃し，攻撃基盤を拡大する (図 1)．攻撃対策をどれほど施しても，攻撃者の組織内への侵入を完全に防ぐことは不可能である．従って攻撃を受けたことが発覚した場合には如何に被害を最小限に抑えるかが重要であり，迅速な攻撃への対処 (インシデント対応) が必要不可欠である．[1]

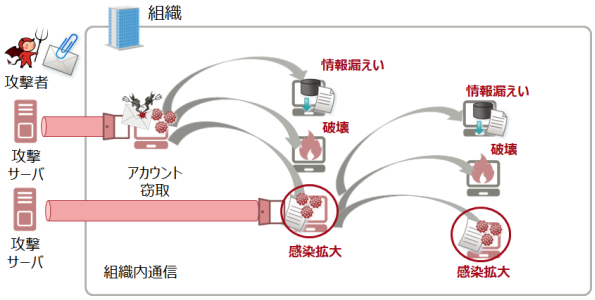


図 1 標的型攻撃の例

攻撃に対処するには攻撃者の攻撃範囲及び攻撃手段を特

[1] 株式会社富士通研究所
FUJITSU LABORATORIES LTD.
[2] 国立研究開発法人情報通信研究機構
National Institute of Information and Communications Technology

定しなければならない. 本稿では前者に必要な調査を攻撃全貌調査, 後者に必要な調査は攻撃全容調査と呼ぶ. 特に攻撃基盤拡大のフェーズでは, 攻撃者は感染端末の周囲の端末へマルウェアを送り込み, その後リモート管理操作を用いてマルウェアを実行させることで感染端末を増加させるため, 攻撃全貌調査では攻撃者が悪用した端末や被害端末の特定を, 攻撃全容調査では被害端末から攻撃者が悪用したファイルについての属性情報やファイル本体そのものを収集し, マルウェアやスクリプトを分析し, マルウェアの種類や外部への通信先の特定を行う必要がある [2].

従来では攻撃全貌調査及び攻撃全容調査にはデジタルフォレンジックが用いられてきた [3]. デジタルフォレンジックにはハードディスクを解析して調査するコンピュータフォレンジックと, ネットワークを流れるパケットを解析して調査を行うネットワークフォレンジックがある. しかし, コンピュータフォレンジックでは被害を受けたと推測される端末全てに対して, 端末のハードディスクなどを入手し, 解析を行わなければならないため, 調査に時間がかかってしまう. 一方, ネットワークフォレンジックは調査対象である攻撃を受けた組織内の通信データがあらかじめ全て保存されている必要があり, 保存には非常に膨大なストレージ容量を要する. また, どちらの手法においても膨大な解析対象データから攻撃関連データの特定, 抽出・分析を行うことは, 攻撃手法やシステム, ネットワーク, セキュリティに関する高度な知識が必要不可欠であるため専門家ではないと難しく, また非常に時間がかかる作業になる. 迅速に攻撃の対処に移るには , 調査は属人性を排除し, 短時間で終えられることが望ましい. 2018 年に海野らは攻撃者が組織内の攻撃拡大にリモート管理操作を悪用することに着目し, 攻撃全貌調査を効率化するための, 攻撃の被害範囲を特定する高速なネットワークフォレンジック手法を提案した [4][5]. 攻撃者が実行したリモート操作と悪用したアカウントを解析して攻撃被害範囲を特定しており, デジタルフォレンジックに比べ, 非常に短時間で, かつ専門家でなくても解析可能な手法である. そして我々は攻撃全容調査を効率化すべく, 2019 年に組織内の通信データからリアルタイムで, ファイル情報をコントロールしつつ収集する新しいネットワークフォレンジック方式を提案した [6]. 攻撃全容調査では攻撃者が感染拡大に悪用するファイルを調査することが必要である. この方式はこれらのファイルを収集することを目的としており, ファイルの書き込み前後で実行されるタスク登録などの更新系リモート管理操作をはじめとする攻撃に悪用される操作と書き込まれたファイルをひも付けることにより実現する. Server Message Block (SMB) プロトコルのセッションで通信データを分割し, 同一セッションのリモート管理操作とリモートで書き込まれたファイルをひも付けて, セッションを単位として危険度を算出し, 危険度に準じたファイル情報の収集を行う. 収集した情報はファイル証跡と呼ぶ. しかし, リモート管理操作には SMB プロトコルと, さらに Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) プロトコルを用いるものがあり, リモート管理操作が SMB プロトコルを用いる場合は操作とファイル書き込みが同じセッションになり, DCE/RPC プロトコルを用いる場合は別セッションになってしまうことがある. 悪用される傾向が強い更新系リモート管理操作の多くが DCE/RPC プロトコルを用いるため, 従来提案手法ではファイルを収集できない場合が存在してしまうという課題があった. そこで今回 DCE/RPC プロトコルが用いられ, 新たに別セッションを開始して実行されるリモート管理操作に対応し, ファイル証跡収集精度を向上させる改良手法を提案する. 同一操作元, 操作先においてリモート管理操作, リモートファイル書き込み操作が実行されており, かつ実行時間が近接している複数のセッションをひも付け対象とすることで, DCE/RPC プロトコルが用られ別セッションで実行されるリモート管理操作が実行された場合でも想定したファイル証跡を取得することが可能となる. 本改良により, 従来提案よりも注意すべき危険なリモート管理操作をトリガーとして, 攻撃関連ファイルを収集することが可能となり, 攻撃全容調査に必要な情報の収集精度の向上を可能としている. 評価実験の結果より, 収集精度が従来方式の約 3.3 倍に改善していることが示せた. また, 実ネットワークで 6 か月間ファイル書き込みを伴う更新系リモート管理操作を観測し, 実行された操作のおよそ 98%が別セッションで実行されていることを明らかにした. 本改良により, リモートによる実行が行われたファイルのファイルハッシュやファイル本体を用いて悪性ファイルかどうかの判断が即座にできる. さらには, 悪性ファイルであった場合には実行先の端末をネットワークから隔離し, 該当のファイルを消去の指示を行うことで, 迅速な攻撃への対処とシステム復旧が実現できる.

本稿では, 第 2 節で従来の解析手法とその課題を, 第 3 節で提案手法の改良について述べる. 第 4 節では改良手法を, 攻撃者が悪用すると知られているリモート管理操作, 実際の攻撃観測データや攻撃模擬データの解析に適用した結果について述べ, 第 5 節で考察について述べる. 第 6 節で関連研究を, 第 7 節ではまとめと今後の課題について述べる.

## 2. 従来手法

サイバー攻撃を受けた場合には, 攻撃による被害を最小限にするために攻撃手法などを調査する攻撃全容調査を行う. 攻撃手法は年々巧妙になっており, システム内のログや残存する痕跡が攻撃者により隠滅され, 少ないことも多い. そのため, デジタルフォレンジックを用いた調査は重要である. デジタルフォレンジックにはハードディスクなどを調査するコンピュータフォレンジックと, あらかじめ保存

しておいた調査対象の通信を調査するネットワークフォレンジックがある.

### 2.1 コンピュータフォレンジック

コンピュータフォレンジックは, コンピュータシステムやハードディスクなどの記憶媒体を調査し, 攻撃に関する情報の修復や攻撃の事象の再構成を行うものである. コンピュータフォレンジックでは攻撃による被害を受けた恐れのある端末を特定し, そのすべての端末に対して 端末やハードディスクを回収し, 解析を行うため非常に時間を要し, 解析中に攻撃が進行してしまう恐れがある. 他にもディスクイメージやメモリイメージを作成し, 解析する手法もある.

### 2.2 ネットワークフォレンジック

ネットワークフォレンジックは, ネットワークを流れる通信データのパケットを解析し, 各端末の通信経路や通信内容の再構成を行うものである. ネットワークフォレンジックを行うには, 調査対象の通信データを予め全て保存しておく必要があるため, 保存に要する記憶媒体の容量が膨大なものとなる. 内閣サイバーセキュリティセンター (NISC) の推奨に従って [7], 仮に 1 日の通信データ量が 4 テラバイトである組織の全ての通信データを 1 年間以上保管する場合, 1.4 ペタバイト以上の容量が必要である. また, 通信データを解析する際には, 膨大な通信データの中の解析すべき範囲の特定には時間を要する上に, 様々なネットワークプロトコルや攻撃手法についての専門知識が必要不可欠である.

### 2.3 攻撃進行度に応じた情報を蓄積するネットワークフォレンジック方式

本ネットワークフォレンジック方式は, 通信データを流れるファイルについて蓄積条件を設け, 収集する情報を変動させることにより, データの保存に要する容量を押さえながら, リアルタイムで攻撃全容調査に必要なファイル証跡を収集する方式である [6]. 本方式ではリアルタイムで通信データを解析し, 実行された Windows のリモート管理操作と書き込まれたファイルとをひも付け, セッション毎に危険度という指標を決定し, 危険度に応じて収集するファイル証跡を決定する (図 2).

#### 2.3.1 危険度について

危険度とは実行されたリモート管理操作が攻撃だと仮定した場合の脅威の大きさを表す指標である. 専門家の知見を基に, 攻撃者が組織に侵入した後, 攻撃基盤構築するために組織内の端末やネットワーク環境についての諜報活動を行っているのか, または端末間での侵害拡大を行っているのかを実行されたリモート管理操作から推測し, 危険度を決定する.

#### 2.3.2 収集ファイル証跡

本方式では, ファイル名, ファイルタイプやタイムスタンプをはじめとするメタデータとファイルハッシュ, ファイル本体を収集している. メタデータ, 特にファイルタイプは, 攻撃者によってファイルの拡張子を偽造され, 拡張子だけでは実行ファイルか否かを判断できない場合に役立つ. また, ファイルハッシュは, VirusTotal[8] などを利用することにより, マルウェアかどうかの判断を行う際に有益である. マルウェアであった場合には, どのマルウェアなのかを特定することも可能である. ファイル本体は静的解析や動的解析を行うことができる.

危険度が高ければ高いほど, ファイル証跡は多く収集し, 保管しておくべきだと考えられる. 危険度が低い段階であれば必要最低限, つまりメタデータだけを収集すればよい. 本手法では危険度毎に収集するファイル証跡を設定する.

#### 2.3.3 収集ファイル証跡のコントロールについて

標的型攻撃では, 攻撃者による遠隔操作によって, 感染端末から周囲の端末への感染拡大が起こることが過去の事例から判明している. その際に実行されるリモート管理操作は SMB プロトコルなどの通信プロトコルが使用されている. ネットワークを流れる通信データを解析し, 通信フローを再構築することで, プロセス間通信の要求パケットの特徴から操作元の端末で実行されたリモート管理操作や書き込まれたファイルを復元する.

SMB によるリモート管理操作の実行時には操作元, 操作先の端末間でネゴシエーションを行い, その後セッションセットアップが行われ, セッションが確立し, リモート管理操作やファイルの書き込み, 読み込みが実行される. その後, ログオフされる, あるいはセッションタイムアウト時間が経過したときセッションが終了される. 本手法ではパケットを解析し, 得たセッション情報を基にセッションインデックスを決定する. 実行されたリモート管理操作のリクエストパケットを解析し, セッションインデックスとリモート管理操作を特定し, 危険度を取得する. ファイルの書き込みについても同様に, WRITE のリクエストパケットを解析し, セッションインデックスを取得する. また, ファイルの書き込みに関するパケットからファイルサイズを取得し, パケットを連結することによりファイルを復元し, 取得する. そしてセッションセットアップリクエストパケットを観測してから, タイムアウト時間が経過するまでに実行されたリモート管理操作とファイルのセッションインデックスと突き合わせ, 一致するものをひも付ける. セッションの中で実行されたリモート管理操作の危険度のうち, 最も高い危険度をセッションの危険度とし, 危険度に応じたファイル証跡を通信データから取得したファイルのバイナリや本体を解析することにより収集する.

#### 2.3.4 課題

SMB プロトコルを用いるリモート管理操作とファイル

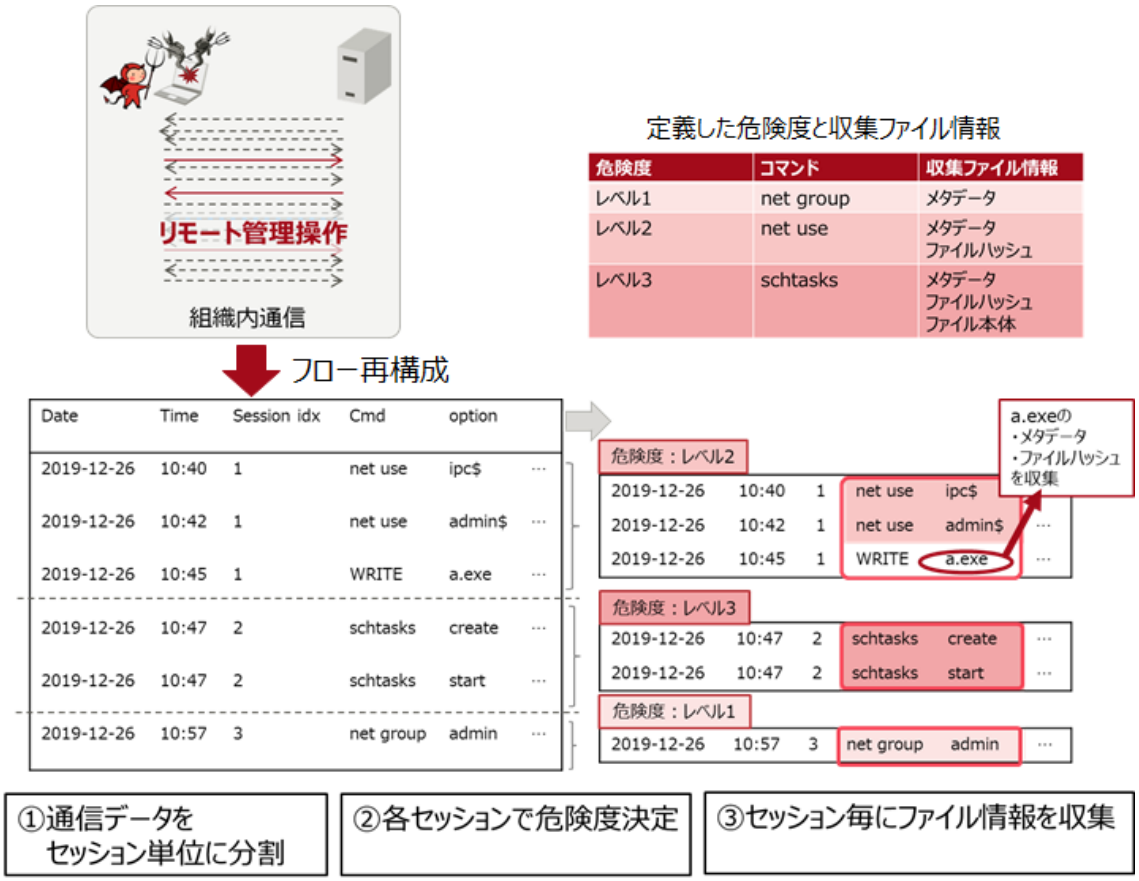


**図 2** 従来提案方式概要

の書き込みを連続して行った場合, ファイルの書き込みと同じセッションで操作が実行されることが観測されている. リモート管理操作の中にはさらに DCE/RPC プロトコルを呼び出すものも存在しており, リモート管理操作の実行が SMB プロトコルのみを用いる操作と別セッションになってしまうことがある. DCE/RPC プロトコルにより別セッションになってしまった操作のリクエストパケットを解析して得たセッションインデックスと SMB プロトコルによる操作のリクエストパケットを解析して得たセッションインデックスは異なるため, 実行されたリモート管理操作と, ファイルをひも付けることができない場合がある. さらにシステムの更新を可能とするリモート管理操作は危険度が高いと判断されるものであるが, これらは DCE/RPC プロトコルが用いられ SMB による操作と別セッションで実行されるものが多い. 実際にある業務ネットワークでは, 2019 年 10 月から 2020 年 3 月までの 6 か月間で, ファイル書き込みを伴う更新系操作の実行は 1245 件起こったが, そのうち 1213 件はファイル書き込みと別セッションであった. このため, 想定した危険度でファイル証跡の収集が不可能な場合がある.

## 3. 提案する改良手法

SMB プロトコルを利用するリモート管理操作, DCE/RPC プロトコルを利用して SMB プロトコルの操作と同じセッションで実行されるリモート管理操作に加えて, DCE/RPC プロトコルにより別セッションで実行されるリモート管理操作とファイルをひも付ける方式へと改良する (図 3).

### 3.1 別セッションで実行されるリモート管理操作とファイルのひも付け

DCE/RPC プロトコルを用いる SMB プロトコルと別セッションで実行されるリモート管理操作に対応するために, リクエストパケットを解析する際にセッションインデックスに加えて, 操作元, 操作先の IP アドレスの組を取得し, セッションインデックスによるひも付けと, 新たに IP アドレスの組によるひも付けを導入する. 単純に IP アドレスの組を用いて, リモート管理操作とファイルをひも付けてしまうと, ひも付け対象が広がり, 必要以上のファイル証跡を収集することになり, 調査対象のファイル証跡が増加することにより攻撃全容調査が非効率になる恐れがある. また, ファイル証跡保存に必要なストレージ容量の増加も招いてしまう. セッションインデックスによるひも付けで定まる危険度と IP アドレスによるひも付けで定まる危険度とを比較し, 高い危険度を採用することにより, ひも付け対象を絞ることで注意すべきファイルに関するファイ

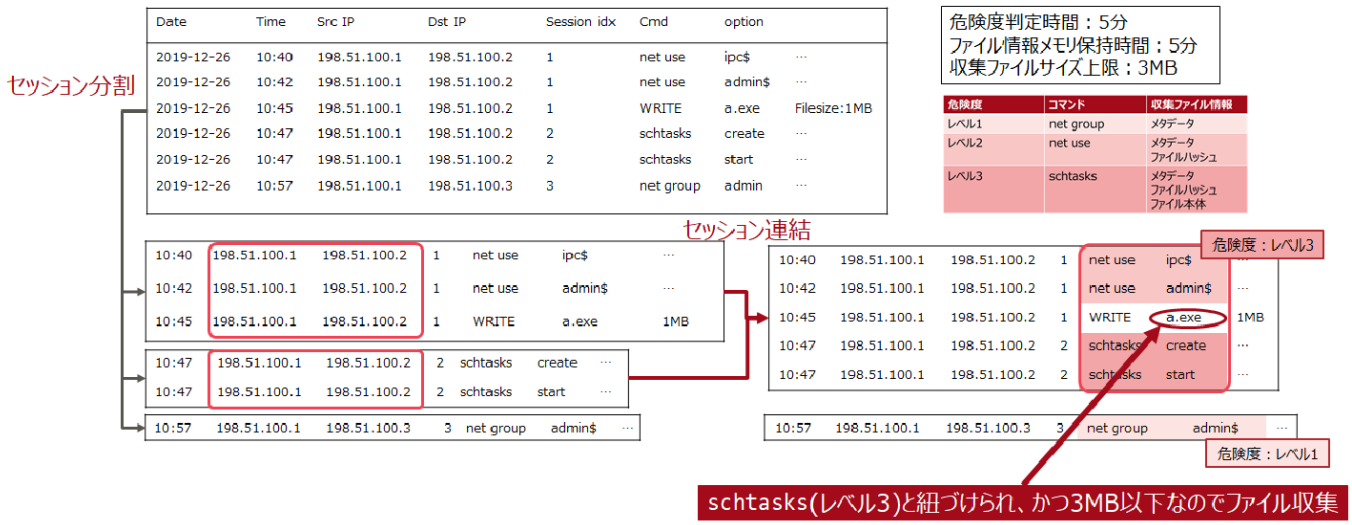


**図 3** 改良手法概要

ル証跡の収集をコントロールする.

さらに, リモート管理操作の実行を起点として一定時間危険度を保持し続ける危険度情報保持時間と, ファイルの書き込みを起点としてファイルをメモリに保持し続けるファイル保持時間を設ける. この 2 種類の保持時間を組み合わせることで, 書き込まれたファイルとファイルの書き込みの前後に実行されたリモート管理操作とのひも付けを実現する. 攻撃ではファイルの書き込みを行ってからリモート管理操作で実行を登録する操作が行われると予想されるが, その場合でも操作とファイルのひも付けが対応可能である.

通信データ内の, 実行されたリモート管理管理操作のリクエストパケットを解析し, 実行されたリモート管理操作を特定し, さらにセッションインデックスと操作元, 操作先の IP アドレスの組と危険度を取得し, それぞれ保持する. ファイルの書き込みについても同様に, WRITE のリクエストパケットを解析し, セッションインデックスと操作元, 操作先の IP アドレスの組を取得し, ファイルを復元し保持する. 最初のリモート管理操作の実行を起点としてその後危険度情報保持時間内に実行された, セッションインデックス, あるいは IP アドレスが一致するリモート管理操作の危険度とファイルとのひも付けを行う. 危険度情報保持時間内により危険度が高い操作が実行されれば危険度を上書きし, その後危険度情報保持時間の間危険度を保持する. ファイルについては, 書き込まれた際にセッションインデックス, IP アドレスを突き合わせて, リモート管理操作により定まる危険度とひも付けファイル保持時間の間保持する. ファイル保持時間が経過した際に再度, セッションインデックス, IP アドレスを突き合わせ, ひも付けにより得られる危険度がその時点で保持されている危険度よりも高い場合は危険度を更新し, それに応じたファイル証跡を保持したファイルのバイナリの解析やハッシュを求めるなどして収集する.

### 3.2 メモリアクセス効率化と収集ファイルのフィルタリング

実行されたリモート管理操作とファイルをひも付ける処理が頻繁に起こると, 改良方式を実装し, 実行した際に負荷がかかってしまう. 最悪の場合, 通信データのパケットを落としてしまい, 正確な危険度の判定やファイルの復元に失敗する恐れがある. それを回避するために, ひも付け処理に間隔を設けることとする. 例えば, 10000 パケット観測毎にひも付け処理を行う.

また, 今回危険度判定を行う対象のリモート管理操作は Windows 標準のものであり, 実際にサーバの運用管理者が業務で行う操作が多い. 攻撃者は攻撃の発覚を避けるために, 使用するファイルのファイルサイズは通常業務で使用するファイルに比べて小さい傾向がある. そこで, ファイル本体の収集をファイルサイズでフィルタリングすることで, より攻撃で利用された可能性が高いファイルを炙りだし, 通常業務で使用されるファイルを除外することで, 収集ファイル全体における調査対象ファイルの割合の向上を可能とする.

## 4. 評価実験

提案手法を実装したプログラムを用いて,

- 攻撃者が悪用する Windows のリモート管理操作と, ファイルの書き込みを行った際の通信データの解析 (実験 1)
- マルウェア対策のための研究用データセット MWS Datasets 2019[9] に含まれる動的活動観測 BOS (Behavior Observable System) の研究用データセット [10], 以下 BOS Dataset の実攻撃の観測データの解析と, Microsoft Advanced Threat Analytics Simulation Play-

表 1　攻撃者が悪用する Windows リモート管理操作

| コマンド | 攻撃フェーズ [14] |
|---|---|
| netview | Discovery |
| net use | Defense Evasion<br>Discovery<br>Lateral Movement |
| net user | Discovery<br>Persistence |
| net group | Discovery |
| at | Lateral Movement<br>Execution |
| reg | Credential Access<br>Defense Evasion<br>Discovery |
| netsh advfirewall | Command and Control<br>Defense Evasion<br>Persistence<br>Discovery |
| sc | Discovery<br>Persistence<br>Impact<br>Privilege Escalation |
| schtasks | Lateral Movement<br>Execution |
| csvde | Lateral Movement |

book [11](以下 MS ATA Playbook) 内のシナリオを基にした模擬攻撃の解析 (実験 2)

を行い, 提案手法が攻撃者が悪用したファイルについて, どれほどファイル証跡を収集可能かを評価した.

### 4.1　実験 1

実験 1 では, 提案手法が攻撃に悪用するリモート管理操作が実行された場合にファイル証跡の収集可能かどうかを検証する.

攻撃者が悪用する Windows のリモート管理操作には net view, net use や at, sc コマンドがあるということが, 2015 年, 2016 年に JPCERT により報告されている [12][13]. また, MITRE 社が発表している ATT&CK[14] というナレッジベースのフレームワークでは, 攻撃者が感染拡大を行う Lateral Movement において schtasks が悪用されるということが述べられている. これら攻撃者が悪用するリモート管理操をまとめたものが表 1 である. 表 1 での攻撃フェーズは MITRE ATT&CK に基づいたものである.

本実験では実験環境の 2 台の端末間で, 共有フォルダをマウントした後, 表 1 のコマンドを実行し, ファイルを書き込むという一連の操作を実行した通信データを採取し, 解析した. ファイル書き込みとリモート管理操作実行のセッションが同じか否かは, DCE/RPC 上で呼び出されるサービスの種類や利用される SMB プロトコルのバージョン, つまり実行コマンドや操作元, 操作先端末の OS のバージョンの組み合わせによって変化する. そのため今回, Windows10 同士, Windows10 と Windows7 間, Windows7 同士の環境で通信データを 28 個の通信データを採取した. 解析において危険度は, 危険度 3 に表 1 にある操作を設定した. また, 収集するファイル証跡は危険度 3 でファイル本体, ファイルハッシュ, ファイルタイプである. 危険度と収集ファイル証跡の設定は表 2 の通りである.

表 2　実験 1 での危険度と収集ファイル証跡の設定

| 危険度 | コマンド | 収集ファイル証跡 |
|---|---|---|
| 危険度 3 | net view, net use<br>net user, net group<br>at, reg<br>netsh advfirewall, sc<br>schtasks, csvde | メタデータ<br>ファイルハッシュ<br>ファイル本体 |

通信データの解析結果は表 3 の通りである.

表 3 より, 本提案手法によりファイルの書き込みと別セッションになるリモート管理操作を実行した場合でも, ファイルと操作をひも付けて危険度を算出し, ファイル証跡を収集できていることが分かる.

### 4.2　実験 2

実験 2 では, BOS Dataset 内のケース g15 と, MS ATA Playbook 内のシナリオを再現した模擬攻撃データを解析し, 提案手法がファイル証跡を収集できているかを評価する. BOS dataset は電子メールと遠隔操作ツールとを組み合わせた組織内ネットワークへの侵害活動を想定した標的型攻撃の動的活動を観測したデータである [10] . 2018 年の研究用データセットでは, 情報通信研究機構のサイバー攻撃誘因基盤上で収集された攻撃観測データも組み込まれている [15] . MS ATA Playbook は Microsoft 社の Advande Threat Analytics チームが作成した, 現実世界の高度な攻撃シナリオのシミュレーション手順を含むプレイブックである [11] .

ケース g15 では, 攻撃者は, net group コマンドにより Active Directory サーバのグループ情報を取得し, その翌々日同サーバの netlogon フォルダに接続し, ファイル ago.exe を書き込んだ直後に, at コマンドを用いて ago.exe を指定した時刻に実行するジョブ登録していた. [5][10]

MS ATA Playbook を基にして下記の 4 通りの攻撃シナリオを模擬環境で再現した [11][16].

**DCSync**　任意のユーザ, あるいは任意の有効期限が設定された認証チケットである Golden Ticket を偽ドメインコントローラにより作成し, Pass the Ticket を行う.

**Skeleton Key**　ドメインコントローラ上の lsass.exe にパッチを適用し, 認証パスワードの改竄を行う.

**DCShadow**　偽ドメインコントローラにより Active Directory のアカウント情報を改竄し, 権限昇格を行う.

**PowerShell**　PowerShell スクリプトを用いて, Pass the

**表 3** 実験環境で取得した通信データの解析結果

| 実行したコマンド | ファイル書き込みセッションとの関係 | 想定取得ファイル証跡 | 改良手法 | 従来方式 [6] |
|---|---|---|---|---|
| net view | 同一セッションで実行 | メタデータ<br>ファイルハッシュ<br>ファイル本体 | 取得 | 取得可 |
| net use | 同一セッションで実行 | メタデータ<br>ファイルハッシュ<br>ファイル本体 | 取得 | 取得可 |
| net user | 異なるセッションで実行 | メタデータ<br>ファイルハッシュ<br>ファイル本体 | 取得 | 取得不可 |
| net group | 異なるセッションで実行 | メタデータ<br>ファイルハッシュ<br>ファイル本体 | 取得 | 取得不可 |
| at | 異なるセッションで実行 | メタデータ<br>ファイルハッシュ<br>ファイル本体 | 取得 | 取得不可 |
| reg | 同一セッションで実行 | メタデータ<br>ファイルハッシュ<br>ファイル本体 | 取得 | 取得可 |
| netsh advfirewall | 異なるセッションで実行 | メタデータ<br>ファイルハッシュ<br>ファイル本体 | 取得 | 取得不可 |
| sc | 異なるセッションで実行 | メタデータ<br>ファイルハッシュ<br>ファイル本体 | 取得 | 取得不可 |
| schtasks | 異なるセッションで実行 | メタデータ<br>ファイルハッシュ<br>ファイル本体 | 取得 | 取得不可 |
| csvde | 異なるセッションで実行 | メタデータ<br>ファイルハッシュ<br>ファイル本体 | 取得 | 取得不可 |

Ticket を行う.

これらはいずれも, 攻撃者がリモート操作を行う端末から mimikatz[17] を標的端末にリモートコピーを行い, 直後に PsExec.exe で mimikatz をリモート実行しているという操作を含んでいる. PsExec.exe でのリモート実行は内部では sc コマンドと同一の DCE/RPC プロトコルを利用して, 標的端末での mimikatz の実行をタスク登録している. さらに MS ATA Playbook のシナリオを基に, mimikatz の PowerShell スクリプトである Invoke-Mimikatz.ps1[18] という PowerShell を標的端末に送り込み, PSSession を用いて Invoke-Mimikatz.ps1 をリモート実行し, Pass the Hash 攻撃を行う攻撃シナリオを実行したものも実験環境で再現した. 以下では PowerShell と表記する.

解析において危険度の定義は実運用で用いることを想定し, 危険度 3 に at, sc コマンドを, 危険度 2 に net use を, 危険度 1 には net view, net group とした. また, 収集するファイル証跡は危険度 3 でファイル本体, ファイルハッシュ, ファイルタイプを, 危険度 2 ではファイルハッシュ, ファイルタイプを, 危険度 1 ではファイルタイプである. 危険度と収集ファイル証跡の設定は表 4 の通りである. 危険度保持時間とファイル保持時間に関しても実運用を想定しパケットを落とさずに, 長い間関連する操作とファイルをひも付けられるよう, ともに 5 分と設定した.

**表 4** 実験 2 での危険度と収集ファイル証跡の設定

| 危険度 | コマンド | 収集ファイル証跡 |
|---|---|---|
| 危険度 3 | at, sc | メタデータ<br>ファイルハッシュ<br>ファイル本体 |
| 危険度 2 | net use | メタデータ<br>ファイルハッシュ |
| 危険度 1 | net view | メタデータ |

攻撃データ, 攻撃模擬データを解析した結果は表 5 の通りである.

表 5 より, 本提案手法は攻撃者がリモートで標的端末に書き込んだ ago.exe, mimkatz については十分にファイル証跡を取得できていることが分かる. PSEXESVC.exe ファイルは PsExec.exe を実行した際にリモート操作先にコピーされるファイルであるが, このファイルに関してはファイ

ルタイプのみ取得できていた．Invoke-Mimikatz.ps1 についてはファイル名のみの取得であった．

## 5. 考察

実験 1 の結果から, ファイルの書き込みと別セッションで実行されるリモート管理操作の場合でも想定したファイル証跡を収集可能であり, 改良手法は従来方式と比較し, 収集精度が約 3.3 倍に改良できていることが分かる．

実験 2 に使用した MS ATA Playbook を PowerShell を用いるよう改変した模擬攻撃では, PowerShell が本提案手法のファイル証跡収集対象ではなかったため, ファイルタイプが取得できず, ファイル名のみの取得となり, 想定する情報を取得することができなかった．また, MS ATA Playbook で PsExec.exe を実行した際にリモート先に転送される PSEXESVC.exe がファイル本体, ファイルハッシュの取得ができていないのは, 通信データ内の PSEXESVC.exe の書き込みに関するパケットからファイルサイズを得られなかったため, パケット連結を行うことができなかったことが原因である．

攻撃者が意図して標的端末に書き込み, リモート実行を行った各ファイルについては, DCE/RPC プロトコルが用いられ別セッションで実行されるリモート管理操作が行われていたとしても, 書き込まれたファイルと実行された操作をひも付け, 十分なファイル証跡を収集可能であることが検証できた．MS ATA Playbook を基にした模擬攻撃データを解析して収集した mimikatz のファイルハッシュは VirusTotal に登録されている mimikatz のハッシュと一致したので, 正確に抽出できていることが分かる．また, 今回実ネットワークでの運用を想定し危険度保持時間とファイル保持時間を 5 分としたが, 実験した通信データに対しては想定したファイル証跡を取得できた．実運用に比べ, 実験環境で採取した通信データは単位時間当たりの通信量が圧倒的に少なく, 危険度とファイルのひも付け処理の負荷が軽いと考えられる．今回解析したデータに対しては 5 分以上としても設定されたファイル証跡を収集可能であり, 実運用する際には適用環境の通信データ流量を考慮して設定することが重要だと推定される．

## 6. 関連研究

Li らはリアルタイムでネットワークを流れる通信データを解析し, Hypertext Transfer Protocol (HTTP) を悪用する攻撃を検知し, 攻撃サンプルとメタデータを抽出するネットワークフォレンジック手法を 2016 年に提案している [19]. Li らは通信データから HTTP のパケットを取り出し, Length などでフィルタリングすることにより怪しいパケットを抽出し, アンチウィルスソフトで検査している．

また, Marchetti らは, 通信データを解析し, サイバー攻撃によってデータ流出した恐れのある組織内端末を特定している [20]．この際, 組織内の端末が外部への, 通信回数, 通信先, アップロードしたデータサイズを特徴量とし, 各端末に対して suspiciousness score を付与している．

我々が提案したネットワークフォレンジック手法の改良は, リアルタイムに通信データを解析し, 実行されたリモート管理操作を基に危険度を定め, リモート管理操作と関連の強いファイルについての証跡を危険度に応じて収集する手法である．

## 7. まとめ

本稿では攻撃者がファイルを標的端末に書き込み, DCE/RPC プロトコルを用いるリモート管理操作を実行した場合でも, 書き込まれたファイルと実行されたリモート管理操作をひも付け, ファイル証跡を収集するネットワークフォレンジック方式の改良を提案した．DCE/RPC プロトコルは, リモート管理操作と書き込みファイルとが異なるセッションとなるため, ファイル証跡の収集が困難であった．本改良方式は, 実行時間と IP アドレスに着目した照合を行うことで, これらの照合を実現するものであり, さらに, リモート管理操作の危険度に応じて収集内容を制御することで, 調査に必要な情報収集の精度向上を実現するものである．これらにより, 攻撃者が悪用したファイルの特定する範囲を拡大でき, 迅速な攻撃への対処とシステム復旧が実現できると考える．また, 提案手法を実装したプログラムを用いて, BOS Dataset の攻撃観測データや MS ATA Playbook のシナリオを再現した攻撃データを解析することで, 攻撃者が利用したファイルについてのファイル証跡を収集可能であることを示した．

今後はファイル証跡収集対象のファイルの拡充や, 実際の業務ネットワークにおいて改良手法の有益性の評価や危険度保持時間とファイル保持時間の適切な設定値についての検討を行う．

### 参考文献


[1] Trend Micro, “Lateral Movement: How do threat actors move deeper into your network?, ” 2013

[2] Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone, “Computer Security Incident Handling Guide,”National Institute of Standards and Technology, Special Publication 800-61 Revision 2, August 2008

[3] Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang, “Guide to Integrating Forensic Techniques into Incident Response,” National Institute of Standards and Technology, Special Publication 800-86, August 2006

[4] 海野 由紀, 森永 正信, 及川 孝徳, 古川 和快, 金谷 延幸, 津田 侑, 遠峰 隆史, 井上 大介, 鳥居 悟, 伊豆 哲也, 武仲 正彦, “標的型攻撃の被害範囲を迅速に分析するネットワークフォレンジック手法の提案,” 暗号と情報セキュリティシンポジウム (SCIS), 2018

[5] 海野 由紀, 森永 正信, 及川 孝徳, 古川 和快, 金谷 延幸, 津田 侑, 遠峰 隆史, 井上 大介, 鳥居 悟, 伊豆 哲也, “標的型攻撃の被害範囲を迅速に分析するネットワークフォレン

表 5　攻撃データの解析結果

| データ名 | リモート書き込みファイル | 危険度判定操作 | 使用プロトコル | 取得ファイル証跡 |
|---|---|---|---|---|
| g15 | ago.exe | at | DCE/RPC | メタデータ<br>ファイルハッシュ<br>ファイル本体 |
| DCSync | mimidrv.sys | sc | DCE/RPC | メタデータ<br>ファイルハッシュ<br>ファイル本体 |
| | mimilib.dll | sc | DCE/RPC | メタデータ<br>ファイルハッシュ<br>ファイル本体 |
| | mimikatz.exe | sc | DCE/RPC | メタデータ<br>ファイルハッシュ<br>ファイル本体 |
| | PSECESVC.exe | sc | DCE/RPC | メタデータ |
| Skeleton Key | mimidrv.sys | sc | DCE/RPC | メタデータ<br>ファイルハッシュ<br>ファイル本体 |
| | mimilib.dll | sc | DCE/RPC | メタデータ<br>ファイルハッシュ<br>ファイル本体 |
| | mimikatz.exe | sc | DCE/RPC | メタデータ<br>ファイルハッシュ<br>ファイル本体 |
| | PSECESVC.exe | sc | DCE/RPC | メタデータ |
| DCShadow | mimidrv.sys | sc | DCE/RPC | メタデータ<br>ファイルハッシュ<br>ファイル本体 |
| | mimilib.dll | sc | DCE/RPC | メタデータ<br>ファイルハッシュ<br>ファイル本体 |
| | mimikatz.exe | sc | DCE/RPC | メタデータ<br>ファイルハッシュ<br>ファイル本体 |
| | PSECESVC.exe | sc | DCE/RPC | メタデータ |
| PowerShell | Invoke-Minikaz.ps1 | net use | SMB | - |


ジック手法の改良," コンピュータセキュリティシンポジウム (CSS), 2018

[6] 乾 真季, 海野 由紀, 及川 孝徳, 古川 和快, 金谷 延幸, 津田 侑, 井上 大介, 伊豆 哲也, "インシデント対応において攻撃進行度に応じた情報を蓄積するネットワークフォレンジック方式の提案," 暗号と情報セキュリティシンポジウム (SCIS), 2019

[7] 内閣官房情報セキュリティセンター, "平成 23 年度 政府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書," 2012 年 3 月

[8] Google Inc.,VirusTotal, https://www.virustotal.com/

[9] 荒木粧子, 他, "マルウェア対策のための研究用データセット〜MWS Datasets 2019〜," 情報処理学会, Vol.2019-CSEC-86, No.8, 2019 年 7 月.

[10] 寺田真敏, 佐藤隆行, 青木 翔, 亀川 慧, 清水 努, 津田 侑, "研究用データセット「動的活動観測 2018」," コンピュータセキュリティシンポジウム (CSS), 2018

[11] Andrew Harris, "Advanced Threat Analytics Attack Simulation Playbook," 2017

[12] 朝長 秀誠, "攻撃者が悪用する Windows コマンド (2015-12-02)," 入手先 ⟨https://blogs.jpcert.or.jp/ja/2015/12/wincommand.html⟩ (参照 2020-04-15)

[13] 朝長 秀誠, "攻撃者の行動によって残る痕跡を調査 (2016-06-28)," 入手先 ⟨https://blogs.jpcert.or.jp/ja/2016/06/ir_research.html⟩ (参照 2020-04-15)

[14] MITRE, "MITRE ATT&CK," available from ⟨https://attack.mitre.org/⟩ (accessed April 14, 2020)

[15] 津田侑，遠峰隆史，金谷延幸，牧田大佑，丑丸逸人，神宮真人，高野祐輝，安田真悟，三浦良介，太田悟史，宮地利幸，神薗雅紀，衛藤将史，井上大介，中尾康二, "サイバー攻撃誘引基盤 STARDUST," コンピュータセキュリティシンポジウム (CSS)，2017

[16] "DCShadow They told me I could be anything I wanted ... So I became a domain controller, " available from ⟨https://www.dcshadow.com/⟩ (accessed May 8, 2020)

[17] Benjamin DELPY, "mimikatz," available from ⟨https://github.com/gentilkiwi/mimikatz⟩ (accessed April 22, 2020)

[18] Matt Graeber, "Invoke-Mimikatz.ps1," available from

⟨https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Invoke-Mimikatz.ps1⟩ (accessed April 22, 2020)
[19] Li, Z., Pan, H., Liu, W. et al., "A network attack forensic platform against HTTP evasive behavior," J Supercomput, 73, 3053–3064 (2017)
[20] Marchetti, M., Pierazzi, F., Colajanni, C. et al., "Analysis of high volumes of network traffic for Advanced Persistent Threat detection," Computer Networks, Volume 109, 127-141, November 2016