Computer Security Symposium 2018
22 - 25 October 2018

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改良

海野 由紀[1]　森永 正信[1]　及川 孝徳[1]　古川 和快[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]　伊豆 哲也[1]

概要：標的型攻撃において攻撃者が組織内ネットワークに侵入した場合には，IT システムの停止や情報漏洩を阻止して損失を最小限に抑えることが最も重要である．そのためには早い段階で攻撃活動を検出し被害の範囲を特定して，攻撃が広がる前に適切な対処を実施する必要がある．著者らは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．本稿では，被害範囲の特定精度を向上させるためのアカウントとリモート操作コマンドの自動ひも付け方式の改良手法を提案する．また，提案手法を実装したプログラムを用いて，MWS Datasets 2018 の攻撃分析を行った結果について述べる．

キーワード：セキュリティ，ネットワーク，インシデントレスポンス，フォレンジック，攻撃分析，動的活動観測，攻撃誘引基盤，STARDUST

Improvement of Network Forensic Method for Promptly Analyzing the Extent of Damage after Targeted Attacks

Yuki Unno[1]　Masanobu Morinaga[1]　Takanori Oikawa[1]　Kazuyoshi Furukawa[1]
Nobuyuki Kanaya[1,2]　Yu Tsuda[2]　Takashi Tomine[2]　Daisuke Inoue[2]　Satoru Torii[1]
Tetsuya Izu[1]

Abstract: When an attacker of a targeted attack broke into the internal network, it is important to obstruct the stop of the ICT system and the leak of information and suppress the loss to the minimum. For that purpose it is necessary to detect the attack activity at an early stage and execute an appropriate action for that before the attack extends.The authors have proposed a high-speed network forensics method for the analysis of the remote operation that the attacker executed and the misused account to specify the extent of damage. In this paper the authors propose improvement method which automatically correlating accounts with operations to improve accuracy of specifying the extent of damage. This paper describes the result of analyzing MWS Datasets 2018 by using the program implemented the proposed method.

Keywords: Security, Network, Incident Response, Forensic, Attack Analysis, Behavior Observable System, Infrastructure for Luring Cyber Adversaries, STARDUST

1. はじめに

標的型攻撃では，攻撃者は組織内ネットワークの端末を RAT（Remote Access Trojan/Remote Administration Tool）と呼ばれるマルウェアに感染させた後，RAT を遠隔操作して感染を拡大させたり，ネットワークや周囲にある端末の情報を収集して機密情報を探す．最悪の場合，IT システムが停止したり，機密情報や個人情報が外部に流出するなどして，標的となった組織やその組織の取引先に多

[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

大な損害を発生させてしまう．

攻撃者は標的のネットワーク環境を事前に調査して，標的が使っているアンチウイルスソフトウェアなどに検知されないようにマルウェアをカスタマイズしたり，標的の心理的な隙や行動のミスに付け込むソーシャルエンジニアリングと呼ばれる方法を使う．攻撃の手口は巧妙であるためマルウェア感染を完全に防ぐことは難しい．セキュリティインシデントを予防することは不可能な状況であるため，近年インシデントが発生したときのレスポンス能力の向上求められている．

アメリカ国立標準技術研究所（NIST：National Institution of Standards and Technology）はセキュリティインシデントに効果的かつ効率的に対応するための実用的な手引きとして，セキュリティ標準 NIST SP800-61 Computer Security Incident Handling Guide を作成した．このガイドでは，攻撃を検知した後に分析を行い，その後マルウェアの活動を封じ込め，攻撃者の諜報活動を根絶して IT システムを復旧するというインシデントレスポンスのライフサイクル（**図 1**）が示されている [1]．このライフサイクルに従って，できる限り早期に攻撃を検知し短時間で攻撃の分析を行って，被害が拡大する前に包括的に適切な対処を実施すれば，標的型攻撃により甚大な損失を被ることを防止できるようになる．

インシデントライフサイクルの検知フェーズに該当する技術に，組織内ネットワークにおける RAT による諜報活動を早期に検知する技術 [3][4] がある．この技術では，組織内通信を解析して攻撃者のサーバと RAT に感染した端末との間の遠隔操作通信と，RAT 感染端末から別の端末に侵入する内部の攻撃通信とを，それぞれの特徴から通信を抽出して関連付けを行う方法で RAT による諜報活動を検知している．インシデントを検知した後には，被害を範囲を特定して諜報活動を封じ込め・根絶させるのがよいが，攻撃によって被害がどの範囲まで及んだのかを前述の検知技術から得られる情報のみから特定するのは通常情報が不十分であるため困難である．

被害の詳細を分析する専用の技術にデジタルフォレンジックが存在する．デジタルフォレンジックの実施においては，高度な知識を持ったサイバーセキュリティの専門家が必要であること，複数の端末が攻撃を受けた場合，被害の分析に長い時間を要することが大きな課題となっている．著者らはこの課題を解決するために「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」を提案している [2]. この手法では，諜報活動の中で攻撃者が実行するリモート操作や悪用したアカウントに着目して，攻撃の証跡を収集している．また，収集した証跡から攻撃の進行状況を分析して被害の範囲を特定している．この手法による被害の特定する時間が大幅に短縮できることを評価している．

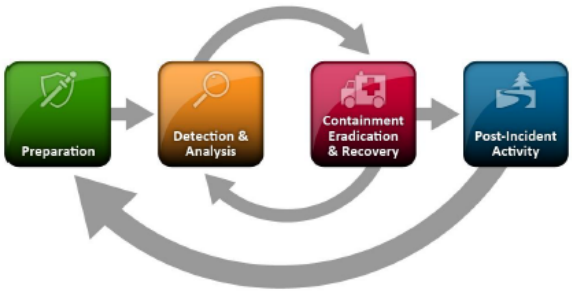

図 1 インシデントレスポンスのライフサイクル
Fig. 1 Incident Response Life Cycle

しかしながら，現在，攻撃者の諜報活動の中で使われているリモート操作コマンドの種類によって，被害範囲の特定の精度が低下する場合があることが分かっている．そこで，現手法に含まれるアカウントとリモート操作コマンドの自動ひも付けの方式を改良した．本改良により，被害範囲の特定精度を向上できる．それにより，被害を受けた全ての端末をネットワークから遮断したり，悪用された全てのアカウントを停止する，あるいはパスワードを変更するなどして，迅速かつ適確に諜報活動の封じ込めと根絶を行って，IT システムを復旧することを実現する．

本稿では，第 2 節で既存の分析手法と課題を，第 3 節で提案手法の改良について述べる．第 4 節では提案手法を MWS Datasets 2018 に含まれる動的活動観測 BOS(Behavior Observable System)，以下 BOS Dataset の攻撃分析に適用した結果を述べ，第 5 節で考察した後，第 6 節でまとめと今後の課題について述べる．

2. 既存の分析手法

攻撃と被害の分析に用いられる手法に攻撃者がネットワーク機器や端末に残した攻撃活動の痕跡を解析する手段であるデジタルフォレンジックと呼ばれる手法がある．

2.1 従来のデジタルフォレンジックによる分析

組織内ネットワークの諜報活動をデジタルフォレンジックで分析する方法の一例を述べる．

2.1.1 アカウントの不正利用の分析

オペレーティングシステム（OS）は不正利用を防ぐために認証機構や監査ログ出力の機構を備えている．攻撃者が OS 標準のコマンドを実行する際や，攻撃者が送り込んだマルウェアを実行する際は，アカウント名，パスワード，チケットなどの認証情報を要求される．認証手続きの結果は監査ログに出力される．インシデントが発生した際は，攻撃者による正規アカウントの悪用の状況を調査するために，Active Directory などの認証サーバの監査用イベントログ [5][6][7][8] や Windows 端末の監査用イベントログに残る認証の成功・失敗，特権の利用などの監査ログを分析する．

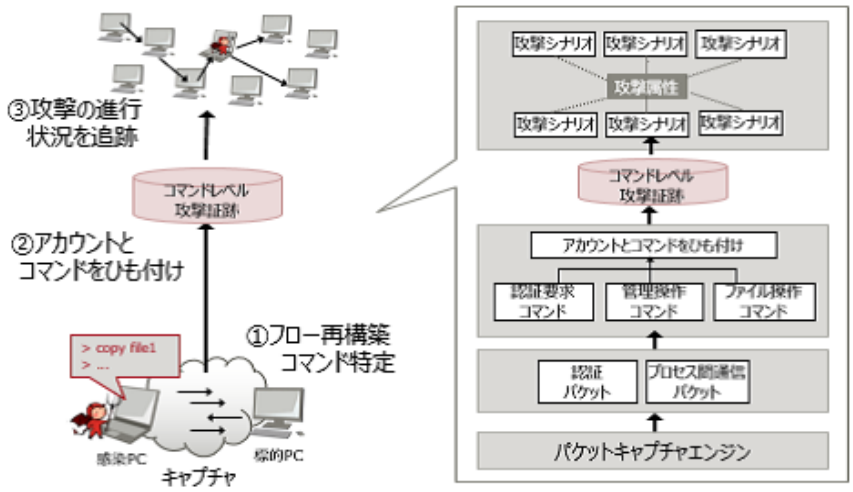

図 2　提案手法の概要

Fig. 2　An Overview of Proposed Method

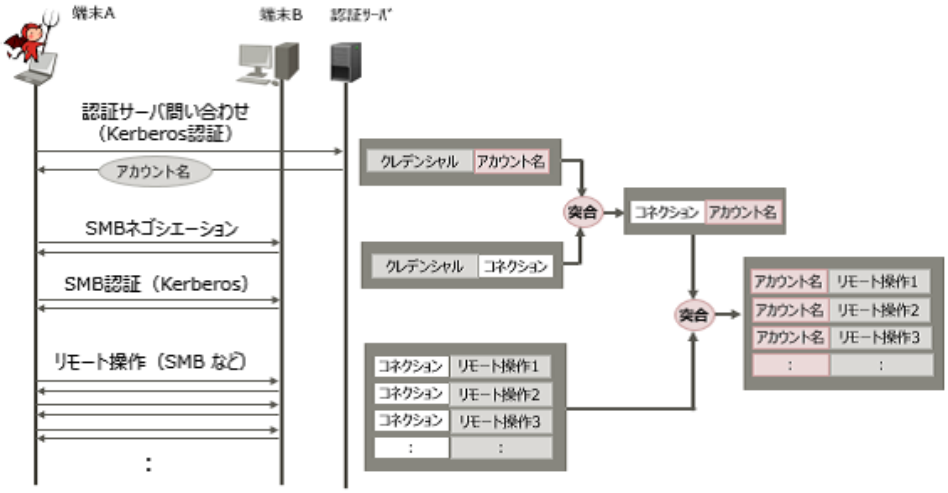

図 3　アカウントとリモート操作コマンドのひも付け-SMB

Fig. 3　Automatically correlating accounts with operations - SMB

2.1.2　攻撃手順と被害の範囲の分析

2.1.1 で述べた個々のログの調査では，断片的な情報しか把握できないため，攻撃の有無や詳細な調査が必要かどうかの判断はできても，攻撃の全貌を把握することは難しい．不足した情報を補うためにハードディスクのコピーを取りそのファイルシステムを解析して，ファイルの復元や電子メール，Web 閲覧，デバイス接続の履歴などを採取する（コンピュータフォレンジック）．その他，組織内ネットワークを流れる通信データを収集してマルウェアの通信や攻撃者が送信したファイルを解析する（ネットワークフォレンジック）．

2.2　従来のデジタルフォレンジックにおける課題

2.1 で示した分析を実施するには，セキュリティに関する高度な知識と技術を保持する人材が必要不可欠である．また，コンピュータフォレンジックでは，攻撃を受けた可能性がある端末の台数分，専門性の高いツールを使うなどして解析を繰り返し行うため，攻撃の全貌を把握するまでに数週間から数か月の時間がかかる場合がある．また，ネットワークフォレンジックでは，組織内ネットワークを流れる通信データの全てを保存するため大量の記憶媒体が必要となる．内閣サイバーセキュリティセンター（NISC）の推奨に従って [9]，仮に全ての通信データを 1 年以上保存する場合，数ペタバイトから数十ペタバイトのデータ蓄積量となる場合がある．また，膨大な通信データの中から解析すべきデータの範囲を特定するのは時間がかかる．その上，分析には様々なネットワークプロトコルの仕様に関する知識が必要であり，通信データから誰が何をしたのかという操作のレベルに読み解くことは困難である．

2.3 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による分析

本ネットワークフォレンジック手法は，2.1.1 と 2.1.2 で述べたデジタルフォレンジックを効率化する手法である．リアルタイムに通信データを解析しフローを再構築して，コマンドレベルで Windows のリモート操作を特定する方式，アカウントとリモート操作コマンドを自動的にひも付けする方式，および攻撃の特徴を示す属性値で攻撃シナリオを抽出・連結して, 攻撃の進行状況を追跡する方式で構成される（図 **2**）.

2.3.1 コマンドレベルのリアルタイム証跡収集

標的型攻撃では，RAT による遠隔操作によって感染した端末から周囲の端末に対してリモート操作コマンドが実行されることが過去の攻撃事例から分かっている．リモート操作コマンドの内部では SMB(Server Message Block）などのプロセス間通信プロトコルが使われる．そこで，ネットワーク中を流れる通信データをキャプチャし通信フローを再構築して，プロセス間通信の要求パケットの特徴から端末で実行されたリモート操作コマンドの種類を特定する．また，応答パケットを解析しリモート操作コマンドの実行結果（成功・失敗）の情報を取得して，リモート操作コマンドの情報と実行結果を併せ証跡ログとして蓄積する．膨大な通信データをコマンドのレベルに要約して記録することにより，従来のネットワークフォレンジック手法に比べて，証跡ログのサイズの縮小化が可能である．

2.3.2 アカウントとリモート操作コマンドの自動ひも付け

リモート操作コマンドの実行時，操作元端末は操作先端末に認証される必要がある．例えば，SMB によるリモート操作の場合は，最初に操作元端末と操作先端末との間でネゴシエーションを行い認証プロトコルを決める．ネゴシエーションが完了した後は，操作元端末は SMB のセッション・セットップに移る．セッション・セットアップでは，操作元端末はクレデンシャル情報を操作先端末に送信して接続要求を送信する．操作先端末に認証された後はセッションが確立され，操作要求を送信することができるようになる．

図 3 は認証サーバに Active Directory を採用した環境において，端末 A と端末 B の SMB ネゴシエーションによって認証プロコトルが Kerberos に決められた場合に，提案手法がどのようにアカウントとリモート操作コマンドをひも付けしているかを示したものである．まず，Active Directory のアカウントでログインする際の認証パケットを解析してクレデンシャルとアカウント名の情報を取得する．次に SMB 認証に該当するセッション・セットアップのパケットを解析して，クレデンシャルとコネクションの情報を取得する．それらをクレデンシャルで突合してコネクションとアカウント名の情報を得る．SMB のリモート操作のパケットを解析してコネクションとリモート操作の情報を得る．この情報と先の突合結果をコネクションで突合し，アカウントとリモート操作コマンドをひも付ける．インシデント対応者は，このひも付け結果から攻撃者に悪用されたアカウントを特定して，該当アカウントの停止，あるいはパスワード変更などの対処を迅速に行うことができる．また悪用されたアカウントの権限のレベルを把握することで，被害の範囲を適切に把握できる．

2.3.3 攻撃進行状況の追跡

証跡ログを入力として，諜報活動に特徴的なリモート操作コマンドの動作定義を基に，業務による正常なリモート操作と攻撃の可能性の高いリモート操作とを識別する．また，攻撃に悪用されたアカウント名や操作の不審度など攻撃の特徴を表す属性値によってフィルタリングしながら攻撃シナリオを抽出する．次に攻撃シナリオを操作の方向で連結して攻撃進行状況を追跡する．これにより被害範囲が把握でき，マルウェアの活動の封じ込めと諜報活動の根絶のための対処検討を早期に開始することができる．

2.4 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課題

諜報活動では，SMB ベースのリモート操作コマンドの他に，WMI（Windows Management Instrumentation ），WinRM（Windows Remote Management）,Windows PowerShell が使われるケースがあることが報告されている [7]. これらは Windows に標準で含まれており，わざわざインストールする必要がない．また，正当な理由で管理者が利用することもあり，使用を禁止することがほとんどない．攻撃者がこれらを利用しても目立たない．SMB ベースのリモート操作コマンド同様に攻撃者に悪用されている．WMI や WinRM，Windows PowerShell のリモート操作は SMB ベースではないため，アカウントとリモート操作コマンドのひも付けを自動的に行わないため，被害範囲の特定が不十分になる場合がある．

3. 提案手法の改良

SMB ベースのリモート操作コマンドに追加して，WMI，WinRM，Windows PowerShell によるリモート操作とアカウントを自動ひも付けする方式を追加する．

3.1 WMI の場合のアカウントとリモート操作コマンドの自動ひも付け

WMI は DMTF（Distributed Management Task Force）の定めた WBEM（Web-Based Enterprise Management）と CIM（Common Information Model）を Microsoft が実装したものであり，DCOM を利用している．WMI に対応するために DCOM を解析してリモート操作とアカウントを自動ひも付けする．**図 4** は認証サーバに Active Directory を採用した環境において，端末 A と端末 B の間の認証プ

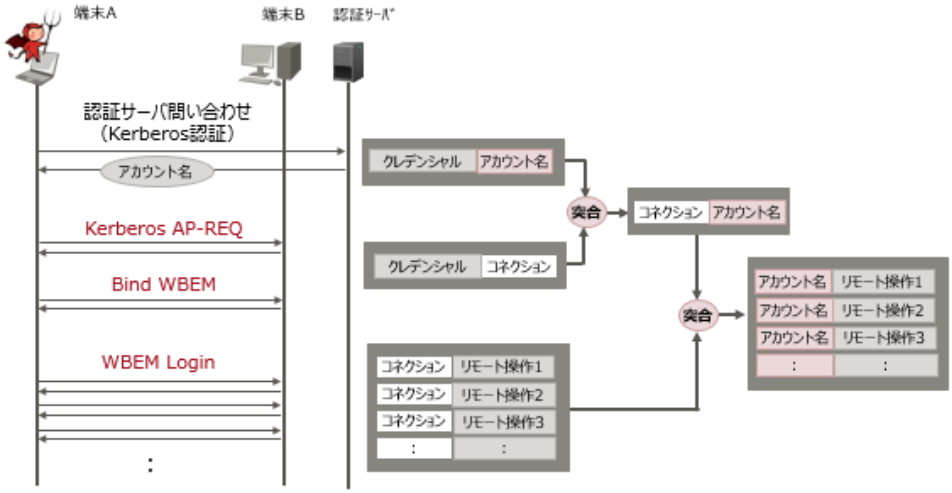

図 4　アカウントとリモート操作コマンドのひも付け - WM

Fig. 4　Automatically correlating accounts with operations - WMI

I

ロコトルが Kerberos に決められた場合に，どのようにアカウントと WMI によるリモート操作をひも付けしているかを示したものである．まず，Active Directory のアカウントでログインする際の認証パケットを解析してクレデンシャルとアカウント名の情報を取得する．次に Kerberos の AP_REQ に該当するパケットを解析して，クレデンシャルとコネクションの情報を取得する．それらをクレデンシャルで突合してコネクションとアカウント名の情報を得る．次に WBEM へのパケットを解析してコネクションとリモート操作の情報を得る．この情報と先の突合結果をコネクションで突合し，アカウントとリモート操作コマンドをひも付ける．

3.2　WinRM, PowerShell におけるアカウントとリモート操作コマンドの自動ひも付け

WinRM はリモート管理用の WS-Management（Web Services for Management）プロトコルを実装している．WS-Management はリモートのソフトウェアとハードウェアの管理に使用される標準の Web サービスプロトコルである．PowerShell でリモート操作を行う際には WinRM が利用される．WinRM，PowerShell に対応するため，WS-Management を解析してリモート操作とアカウントをひも付けする．**図 5** は認証サーバに Active Directory を採用した環境において，端末 A と端末 B の間の認証プロコトルが Kerberos に決められた場合に，どのようにアカウントと WinRM，PowerShell によるリモート操作をひも付けしているかを示したものである．まず，Active Directory のアカウントでログインする際の認証パケットを解析してクレデンシャルとアカウント名の情報を取得する．次に端末 B への HTTP の Authorization：Kerberos に該当するパケットを解析して，Base64 でデコードした後クレデンシャルとコネクションの情報を取得する．それらをクレデンシャルで突合してコネクションとアカウント名の情報を得る．次に端末 B への Post メッセージのパケットを解析してコネクションとリモート操作の情報を得る．この情報と先の突合結果をコネクションで突合し，アカウントとリモート操作コマンドをひも付ける．

4.　評価実験

提案手法を実装したプログラムを用いて，マルウェア対策のための研究用データセット MWS Datasets 2018 に含まれる BOS Dataset の攻撃分析を行う評価実験を行った．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 BOS Dataset には攻撃誘引基盤 STARDUST[11][12][13] で収集された攻撃の観測データが組み込まれている．

評価実験では通信データ（pcap ファイル）が提供されている かつ 進行度 6 以上の 7 つのケース f03，g01，g05，g07，g09，g12，g15 を対象にした．進行度 6 とは C2 サーバと攻撃通信が成立したが攻撃活動/操作が観測できたなかったものをさしており，ケース g01，g05，g07，g12 の 4 つがこれに該当する．これらのケースを攻撃分析結果は進行度 6 と合致した．進行度 7 は C2 サーバと攻撃通信が成立 かつ 攻撃活動/操作が観測できたものであり，ケース f03 と g09 の 2 つが進行度 7 に該当する．これらのケースを攻撃分析した結果についても進行度 7 と合致した．またケース f03 については net view コマンド，net group コマンドなど文献 [10] に記載されている観測事象とも合致した．進行度 8 は C2 サーバと攻撃通信が成立 かつ 攻撃活動/操作が継続的に観測できたものであり，ケース g15 がこれに該当する．本ケースを分析して自動作成した攻撃シ

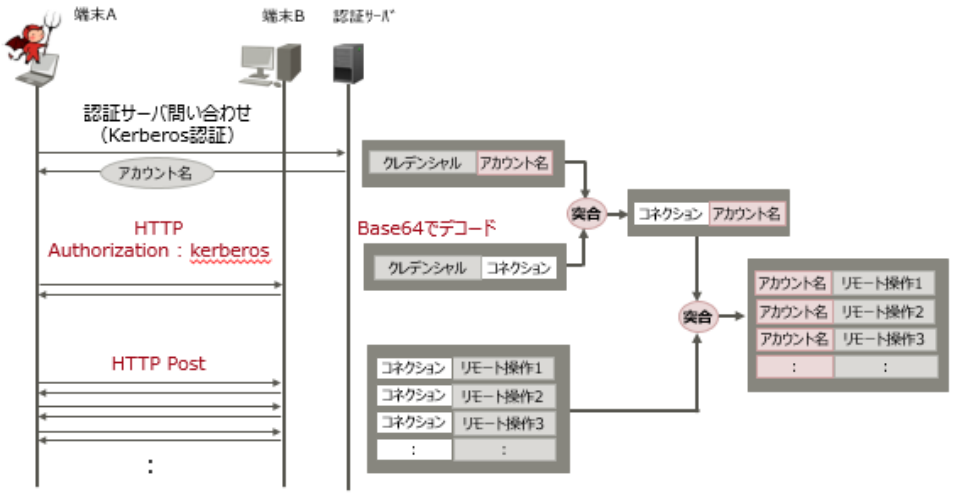

図 5 アカウントとリモート操作コマンドのひも付け - WinRM, PowerShell
Fig. 5 Automatically correlating accounts with operations - WinRM, PowerShell

ナリオの詳細を**表 1**，**表 2**，**表 3**，**表 4** に示す．ケース g15 の攻撃活動/操作は 201*年*月 23 日～25 日までの間，継続的に観測できており進行度 8 と合致している．攻撃者は net group コマンドを実行して，Active Directory サーバ (***.***.8.8) のグループ情報の取得に成功している．また，Active Directory サーバの netlogon フォルダに接続した後，ファイル ago.exe を書込み，at コマンドを使って指定した時刻に ago.exe を実行するジョブを 4 件登録していた．ago.exe のリライトや実行時間を変更しながらジョブを繰り返し登録している様から攻撃者の試行錯誤が垣間見えるが，攻撃者自身は ago.exe とジョブを削除していなかった．ファイルサーバ (***.***.8.10) に対しては総務部など 8 つの共有フォルダへの接続に成功している．ファイルサーバの管理共有 admin$への接続も繰り返し試みたが権限の高いアカウントを利用していなかったため全て失敗していた．その他，Active Directory サーバ，ファイルサーバ，周囲の端末に対しては Wannacry と同様に SMB trans2 の Session Setup のリクエストを送信していたがこれらも全て失敗していた．

5. 考察

評価実験で利用した 6 つのケースの攻撃観測データには，WMI, WinRM，PowerShell によるリモート操作が含まれていなかったため，DCOM ベース，WS-Management ベースのリモート操作とアカウントをひも付けした証跡を収集することはできなかった．しかし，ケース g15 の攻撃分析においては，攻撃者が行った SMB ベースのリモート操作とアカウントとをひも付けしてコマンドレベルの証跡を収集し，短時間で攻撃シナリオを作成できることを検証できた．作成した攻撃シナリオからは攻撃者特有のコマンドの使い方など有益な情報が得られた．

6. まとめ

本稿では攻撃者が行ったリモート操作と悪用したアカウントに着目して攻撃証跡を収集し，収集した証跡から攻撃の進行状況を分析して被害範囲を特定するネットワークフォレンジック手法の改良を提案した．また，提案手法を実装したプログラムを使い BOS Dataset を分析して，攻撃シナリオの抽出と攻撃進行状況を追跡できることを示した．

今後は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 および 証跡ログのサイズの縮小度，攻撃進行状況の追跡速度の評価を行う．

参考文献

[1] Paul Cichonski, Thomas Millar, Tim Grance, Karen Scarfone,“Computer Security Incident Handling Guide,” National Institute of Standards and Technology, Special Publication 800-61 Revision2, August 2012
[2] 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
[3] 山田 正弘, 森永 正信, 海野 由紀, 鳥居 悟, 武仲 正彦,“組織内ネットワークにおける標的型攻撃の諜報活動検知方式,” 情報処理学会研究報告, Vol.2013-CSEC-62 No.53，2013
[4] 山田 正弘, 森永 正信, 海野 由紀, 鳥居 悟, 武仲 正彦,“組織内ネットワークにおける標的型攻撃の諜報活動検知方式,” 暗号と情報セキュリティシンポジウム (SCIS)，2014
[5] 満永拓邦,“ログを活用した高度サイバー攻撃の早期発見と分析,” 2015
[6] 一般社団法人 JPCERT コーディネーションセンター,“高度サイバー攻撃への対処におけるログの活用と分析方法 1.1 版,” 2016 年 10 月 19 日
[7] 一般社団法人 JPCERT コーディネーションセンター,“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,” 2017 年 11 月 9 日
[8] Laura A. Robinson, Khurram Chaudhary, Roger Grimes, and Eric Leonard,“Best Practices for Securing Active Di-

表 1　BOS Dataset g15（STARDUST） 攻撃シナリオ 1
Table 1　BOS Dataset g15（STARDUST） Attack Scenario 1

日時 (UTC)	操作元	操作先	ユーザ	操作内容	結果
201*/*/23 09:48:14	***.***.16.110	***.***.8.8	tmaeda	net group /domain	成功
201*/*/23 09:48:14	***.***.16.110	***.***.8.8	tmaeda	net group 'Domain computers' /domain	成功
201*/*/23 09:48:14	***.***.16.110	***.***.8.8	tmaeda	net group /domain	成功
201*/*/23 09:48:14	***.***.16.110	***.***.8.8	tmaeda	net group 'Domain computers' /domain	成功
201*/*/24 03:46:01	***.***.16.110	***.***.8.8	NULL	SESSION_SETUP	失敗
201*/*/24 03:47:54	***.***.16.110	***.***.8.8	NULL	SESSION_SETUP	失敗
201*/*/24 09:33:03	***.***.16.110	***.***.8.8	NULL	SESSION_SETUP	失敗
201*/*/25 00:45:49	***.***.16.110	***.***.8.8	Administrator	net view ￥￥127.0.0.1	成功
201*/*/25 00:45:51	***.***.16.110	***.***.8.8	Administrator	net use device ￥￥127.0.0.1￥netlogon	成功
201*/*/25 00:45:54	***.***.16.110	***.***.8.8	Administrator	net view ￥￥127.0.0.1	成功
201*/*/25 00:45:56	***.***.16.110	***.***.8.8	Administrator	net use device ￥￥127.0.0.1￥netlogon	成功
201*/*/25 00:46:29	***.***.16.110	***.***.8.8	Administrator	net view ￥￥127.0.0.1	成功
201*/*/25 00:46:31	***.***.16.110	***.***.8.8	Administrator	net use device ￥￥127.0.0.1￥netlogon	成功
201*/*/25 00:46:51	***.***.16.110	***.***.8.8	Administrator	WRITE ago.exe FileSize:57344	成功
201*/*/25 00:46:55	***.***.16.110	***.***.8.8	Administrator	READ ago.exe FileSize:57344	成功
201*/*/25 00:47:02	***.***.16.110	***.***.8.8	Administrator	net use device ￥￥127.0.0.1￥netlogon	成功
201*/*/25 00:48:33	***.***.16.110	***.***.8.8	Administrator	at ￥￥127.0.0.1 jobTime=35280000 daysOfMonth=0x00000000 daysOfWeek=0x00 command=netlogon￥ago.exe jobid:1	成功
201*/*/25 00:48:46	***.***.16.110	***.***.8.8	Administrator	at ￥￥127.0.0.1	成功
201*/*/25 00:51:11	***.***.16.110	***.***.8.8	Administrator	net view ￥￥127.0.0.1	成功
201*/*/25 00:51:13	***.***.16.110	***.***.8.8	Administrator	net use device ￥￥127.0.0.1￥sysvol	成功
201*/*/25 00:51:16	***.***.16.110	***.***.8.8	Administrator	net view ￥￥127.0.0.1	成功
201*/*/25 00:52:09	***.***.16.110	***.***.8.8	Administrator	at ￥￥127.0.0.1	失敗
201*/*/25 00:52:19	***.***.16.110	***.***.8.8	Administrator	at ￥￥127.0.0.1 jobTime=35280000 daysOfMonth=0x00000000 daysOfWeek=0x00 command=c:￥netlogon￥ago.exe jobid:2	成功
201*/*/25 00:52:29	***.***.16.110	***.***.8.8	Administrator	at ￥￥127.0.0.1 jobTime=35520000 daysOfMonth=0x00000000 daysOfWeek=0x00 command=netlogon￥ago.exe jobid:3	成功
201*/*/25 00:52:34	***.***.16.110	***.***.8.8	Administrator	at ￥￥127.0.0.1	成功
201*/*/25 00:53:33	***.***.16.110	***.***.8.8	Administrator	net use device ￥￥127.0.0.1￥sysvol	成功
201*/*/25 00:54:42	***.***.16.110	***.***.8.8	Administrator	net view ￥￥127.0.0.1	成功
201*/*/25 00:55:09	***.***.16.110	***.***.8.8	Administrator	net use device ￥￥127.0.0.1￥netlogon	成功
201*/*/25 00:55:11	***.***.16.110	***.***.8.8	Administrator	READ ago.exe FileSize:57344	成功
201*/*/25 00:55:13	***.***.16.110	***.***.8.8	Administrator	net view ￥￥127.0.0.1	成功
201*/*/25 00:55:15	***.***.16.110	***.***.8.8	Administrator	net use device ￥￥127.0.0.1￥sysvol	成功
201*/*/25 00:55:22	***.***.16.110	***.***.8.8	Administrator	WRITE ago.exe FileSize:57344	成功
201*/*/25 00:55:25	***.***.16.110	***.***.8.8	Administrator	READ ago.exe FileSize:57344	成功
201*/*/25 00:56:08	***.***.16.110	***.***.8.8	Administrator	at ￥￥127.0.0.1 jobTime=35700000 daysOfMonth=0x00000000 daysOfWeek=0x00 command=netlogon￥ago.exe jobid:4	成功
201*/*/25 00:56:12	***.***.16.110	***.***.8.8	Administrator	at ￥￥127.0.0.1	成功
201*/*/25 00:56:13	***.***.16.110	***.***.8.8	Administrator	READ ago.exe FileSize:57344	成功
201*/*/25 01:15:11	***.***.16.110	***.***.8.8	Administrator	READ ago.exe FileSize:57344	成功

表 2　BOS Dataset g15（STARDUST） 攻撃シナリオ 2
Table 2　BOS Dataset g15（STARDUST） Attack Scenario 2

日時 (UTC)	操作元	操作先	ユーザ	操作内容	結果
201*/*/24 09:53:16	***.***.16.110	***.***.8.10	NULL	SESSION_SETUP	失敗
201*/*/24 03:59:56	***.***.16.110	***.***.8.10	admins	net use device ￥￥127.0.0.1￥admin$	失敗× 5
201*/*/24 03:59:57	***.***.16.110	***.***.8.10	admins	net use device ￥￥127.0.0.1￥admin$	失敗× 7
201*/*/24 04:01:58	***.***.16.110	***.***.8.10	admins	net use device ￥￥127.0.0.1￥admin$	失敗× 6
201*/*/25 04:01:19	***.***.16.110	***.***.8.10	admins	net view ￥￥127.0.0.1	成功
201*/*/25 04:01:28	***.***.16.110	***.***.8.10	admins	net view ￥￥127.0.0.1￥総務部	成功
201*/*/25 04:01:31	***.***.16.110	***.***.8.10	admins	net view ￥￥127.0.0.1￥人事部	成功
201*/*/25 04:01:34	***.***.16.110	***.***.8.10	admins	net view ￥￥127.0.0.1￥営業部	成功
201*/*/25 04:01:37	***.***.16.110	***.***.8.10	admins	net view ￥￥127.0.0.1￥経理部	成功
201*/*/25 04:01:40	***.***.16.110	***.***.8.10	admins	net view ￥￥127.0.0.1￥第一事業部	成功
201*/*/25 04:05:45	***.***.16.110	***.***.8.10	admins	net view ￥￥127.0.0.1	成功
201*/*/25 04:05:52	***.***.16.110	***.***.8.10	admins	net view ￥￥127.0.0.1￥情報システム部	成功
201*/*/24 04:16:50	***.***.16.110	***.***.8.10	NULL	SESSION_SETUP	失敗× 3
201*/*/25 09:02:50	***.***.16.110	***.***.8.10	admins	net view ￥￥127.0.0.1	成功
201*/*/25 09:02:52	***.***.16.110	***.***.8.10	admins	net view ￥￥127.0.0.1	成功
201*/*/25 09:02:59	***.***.16.110	***.***.8.10	admins	net view ￥￥127.0.0.1￥経理部	成功
201*/*/25 09:03:03	***.***.16.110	***.***.8.10	admins	net view ￥￥127.0.0.1￥情報システム部	成功
201*/*/25 09:10:05	***.***.16.110	***.***.8.10	admins	net view ￥￥127.0.0.1￥第三事業部	成功
201*/*/25 09:10:13	***.***.16.110	***.***.8.10	admins	net view ￥￥127.0.0.1￥営業部	成功
201*/*/25 09:10:20	***.***.16.110	***.***.8.10	admins	net view ￥￥127.0.0.1￥人事部	成功
201*/*/25 09:44:13	***.***.16.110	***.***.8.10	admins	net view ￥￥127.0.0.1￥経理部	成功
201*/*/25 09:44:18	***.***.16.110	***.***.8.10	admins	net view ￥￥127.0.0.1￥開発部	成功
201*/*/25 09:53:16	***.***.16.110	***.***.8.10	NULL	SESSION_SETUP	失敗× 6

表 3　BOS Dataset g15（STARDUST） 攻撃シナリオ 3
Table 3　BOS Dataset g15（STARDUST） Attack Scenario 3

日時 (UTC)	操作元	操作先	ユーザ	操作内容	結果
201*/*/23 09:46:55	***.***.16.110	***.***.8.111	NULL	net view	成功
201*/*/23 10:06:11	***.***.16.110	***.***.8.111	NULL	net view /domain	成功

表 4　BOS Dataset g15（STARDUST） 攻撃シナリオ 4
Table 4　BOS Dataset g15（STARDUST） Attack Scenario 4

日時 (UTC)	操作元	操作先	ユーザ	操作内容	結果
201*/*/24 09:26:20	***.***.16.110	***.***.8.202	NULL	SESSION_SETUP	失敗
201*/*/24 09:28:41	***.***.16.110	***.***.8.202	NULL	SESSION_SETUP	失敗

rectory,” 2017
[9] 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,” 平成 24 年 3 月
[10] 寺田 真敏, 佐藤 隆行, 青木 翔, 亀川 慧, 清水 努, 萩原 健太,“研究用データセット「動的活動観測 2017」,” コンピュータセキュリティシンポジウム (CSS), p.525-529，2017
[11] 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), p.472-479, 2017
[12] 金谷 延幸, 津田 侑, 遠峰 隆史, 安田 真悟, 井上 大介,“環境特徴情報による模擬環境自動構築効率化手法の提案と実装,” 暗号と情報セキュリティシンポジウム (SCIS), 2018
[13] 金谷 延幸, 津田 侑, 遠峰 隆史, 高野 祐輝, 井上 大介,“サイバー攻撃に対する能動的観測による収集データのモデル化と正規化手法,” コンピュータセキュリティシンポジウム (CSS), 2018