Vol.2020-DPS-182 No.39
Vol.2020-CSEC-88 No.39
2020/3/13

攻撃シナリオに基づく感染範囲推定方式の提案

内藤久詞[1]　西川弘毅[1]　河内清人[1]

概要：特定の組織を対象とした，高度なサイバー攻撃である APT（Advanced Persistent Threat）の多発により，情報セキュリティインシデントの発生を完全に防ぐことは困難な状況である．したがって，サイバー攻撃の入口対策だけでなく，サイバー攻撃による侵入を検知した場合は，すみやかにサイバー攻撃の侵入を受けている経路である感染経路を特定し，対処を的確に行なうことで被害の拡大を防ぐ必要がある．しかし，限られた時間内で感染経路の可能性がある範囲である感染範囲を推定するには，高度なスキルが要求される．また，コマンドラインツールなどの，OS に標準でインストールされた正規ツールが悪用された場合，攻撃者の活動と，正規ユーザの活動の痕跡を区別することが困難になる．そこで本稿では，攻撃者の活動を予め定義した攻撃シナリオに基づき，感染範囲を推定する方式を提案する．

キーワード：インシデントレスポンス，攻撃シナリオ，アタックツリー，フォレンジック

Proposal of Affected Range Estimation Method Based on Attack Scenarios

HISASHI NAITO[†1]　HIROKI NISHIKAWA[†1]
KIYOTO KAWAUCHI[†1]

Abstract: Due to the frequent occurrence of Advanced Persistent Threats (APTs), which are sophisticated cyber attacks targeting specific organizations, it is difficult to completely prevent the occurrence of information security incidents. Therefore, if an intrusion by cyber attacks is detected, it is necessary to take appropriate measures to prevent the spread of damage by promptly specifying the routes of infection, which have been compromised by cyber attacks, as well as entrance measures against cyber attacks. However, advanced skills are required to exhaustively estimate an affected range, which is the range of possible routes of infection, within a limited time. In addition, if the legitimate tools installed on an operating system by default, such as command line tools, are abused, it becomes difficult to distinguish the traces of the attacker's activity and the authorized user's activity. In this paper, we propose a method to estimate the affected range based on the attack scenarios in which the attacker's activity is predefined.

Keywords: Incident Response, Attack Scenarios, Attack Tree, Forensic

1. はじめに

企業や重要インフラに対するサイバー攻撃は依然として深刻な状況が続いている[1]．特定の組織を対象とし，長期にわたり攻撃活動が行なわれる標的型攻撃（Advanced Persistent Threat: APT）では，攻撃者は，事前に組織におけるセキュリティ対策状況を把握し，監視を回避するような攻撃を行なうため，侵入に気づかないことが多い[2]．また，ゼロデイ攻撃と呼ばれる，修正プログラムが提供される前の，すなわち未知の脆弱性を悪用して侵入を行なう攻撃に加え，端末に攻撃用のプログラムをインストールせずに，OS に備わっている標準機能を利用してメモリ上で実行されるファイルレス攻撃などの高度な攻撃手法が用いられることが多く，完全に侵入を防ぐことは難しい[3]．

このような状況を背景とし，今後は攻撃に対する入口対策だけではなく，万が一侵入されても被害を軽微なものに留めることが重要となってきている．例えば，内閣サイバーセキュリティセンター（NISC）は，重要インフラにおけるサイバー攻撃に対処するために，セキュリティ監視だけでなく，専門知識を持つ組織を含めたインシデントの対処体制の構築を指針として挙げている[1]．

米国国立標準技術研究所（NIST）が作成したセキュリティ標準である SP 800-61[4]によると，インシデント対応では，攻撃が検知されたら，まず被害拡大を最小限に抑えるために，感染した端末の判別や隔離などの封じ込め作業を行なう．そのためには，実際に攻撃活動が行なわれていたかどうかを判断するために，感染の可能性のある端末のログやディスクから攻撃の痕跡を探し，すみやかに感染範囲を洗い出す作業が必要である．このような作業は，どのような手順で何を調べれば良いか，といった調査方針が必要であり，サイバー攻撃に関する専門的な知識が要求される．しかし，これらのスキルを備えた，高度なセキュリティ人材は限られていることから[5]，今後，隔離が必要な感染箇

1 三菱電機株式会社　情報技術総合研究所
Mitsubishi Electric Corporation, Information Technology R&D Center.

Vol.2020-DPS-182 No.39
Vol.2020-CSEC-88 No.39
2020/3/13

所を推定して提示する技術の需要が高まると推察される．

そこで本稿では，攻撃者の最終目標とそれを実現するまでに攻撃者が行なう一連の攻撃活動（攻撃シナリオ）に基づいて，攻撃の痕跡情報を調査するとともに，正規ツールが悪用された場合に，攻撃者とユーザのツールの利用頻度から，攻撃の有無を判断することで，インシデント発生時の感染範囲を推定する方式を提案する．

本稿の構成を以下に示す．2 章でインシデント対応における本稿のスコープを示す．3 章では，関連技術や現状の課題について概説する．4 章では，今回提案する方式について述べる．5 章では，提案方式に関する考察を述べ，最後に 6 章でまとめる．

2. インシデント対応における本稿のスコープ

本章では，インシデント対応の流れについて，NIST が発行する二つの文献[4][6]を基に概要を説明した後に，本稿でのスコープを示す．

SP 800-61[4]では，インシデントの発生を想定した準備から，今後の改善活動までの一連のライフサイクルが五つのフェーズによって示されており，各フェーズで実施すべき内容や手順を説明している（表 1）．

表 1　SP 800-61 の五つのフェーズ

フェーズ	説明
準備	インシデントの発生予防や，発生時に向けた体制作りの実施．
検知 分析	インシデントの発生を検知し，兆候の分析や，優先度付けを実施．
封じ 込め	感染箇所を特定し，被害拡大を防止するために，隔離や停止などの止血対応を実施．
根絶	インシデントの原因や被害状況を詳細に分析し，根本原因の修復を実施．
復旧	修復後のシステムを再開し，正常に動作していることの確認を実施．
教訓	各フェーズで実施した内容を評価し，今後の改善案の検討を実施．

一方，サイバーセキュリティフレームワーク（CSF）[6]では，重要インフラのシステムをサイバー攻撃から守るためのセキュリティ対策を，五つのコア機能として定義している（表 2）．

二つの文献から，インシデントの発生前や，システムの復旧が完了した後のフェーズを除くと，インシデント対応には大きく分けて，(1)攻撃を検知する，(2)攻撃を封じ込める，(3)根本原因を修復する，の三つのフェーズがあることが分かる．それぞれのフェーズで行なわれる活動の例として，以下の内容が挙げられる．

表 2　CSF の五つの機能

機能	説明
特定	守るべき資産や脅威の特定，対策するための体制の決定などの実施．
防御	脆弱性情報の収集と分析，攻撃を防ぐためのセキュリティ対策の実施．
検知	マルウェア，ネットワークなどの攻撃を検知するための対策の実施．
対応	攻撃が発生した場合の影響分析，攻撃の拡大を防ぐための封じ込め，低減などの実施．
回復	攻撃の受けたシステムの回復の実施．

(1) 攻撃を検知する

IDS（Intrusion Detection System）や SIEM（Security Information and Event Management）などのセキュリティ監視装置を用いて，例えば，メールに添付されたマルウェアの実行による端末の侵害や，その端末からの C2 通信を検知する．

(2) 攻撃を封じ込める

攻撃者の行動を緩和して，短期間攻撃者を足止めするとともに，長期的対応を実施するための応急処置を行なう．例えば，悪性の URL やドメイン名を含むリソースへアクセスしている端末を，ネットワークから隔離したり，攻撃者が悪用していると思われるユーザアカウントを，一時的にロックしたりする．

(3) 根本原因を修復する

封じ込めのような一時的な措置ではなく，攻撃者を締め出し，脅威を完全に排除するための長期的な対策を行なう．例えば，攻撃者がインストールしたマルウェアの削除や，ソフトウェアのパッチを適用する．また，再発を防ぐため，各種ログや履歴情報などから，インシデントの発生を裏付ける痕跡を特定し，全容を明らかにする．

本稿では，これまで数多くの研究や製品開発がなされている(1)と比べ，有効な対策技術がまだ少ないとされる(2)を対象とし，封じ込めに必要な感染範囲の特定を行うための方式を提案する．なお，(2)が適切に実施できることで，被害の拡大を抑え，(3)の円滑な実施にも繋げることができる．

3. 関連技術

インシデント対応を支援する技術として，ネットワークを複数のサブネットワークに分割し，アクセス制御により不審な通信を遮断する，ネットワーク分離設計の手法がある[7]．本手法により，感染端末を効率的に隔離し，マルウェアの感染拡大や情報漏洩を抑制することができるが，導入前にネットワーク設計と大規模な構築作業が必要であり，システムの変更に対する柔軟性の課題も残されている．

また近年では，脅威情報の収集，インシデント管理機能，

Vol.2020-DPS-182 No.39
Vol.2020-CSEC-88 No.39
2020/3/13

感染箇所の隔離など，インシデント発生時の初動対応に至るまでの業務プロセスを自動化する SOAR（Security Orchestration and Automation Response）ツールが登場してきている[8][9]．SOAR による自動化を実現するためには，インシデント対応フローや，条件式，判定ルールなどを，人手によって予め記述しておく必要があり，また運用に合わせたカスタマイズを行なわないと，効果的に活用できないため，導入の敷居が高いことが課題となっている[10]．

さらに，最近の攻撃事例では，侵入後に OS に標準搭載されるツールなどの正規ツールが悪用されることが多い[11]．したがって，端末に残された痕跡が，正規ユーザの活動によるものと混在した場合，同じ動作として記録されるため，どちらの活動によるものか判断が必要になり，感染の切り分けを困難にさせる原因となる．

4. 提案方式

本稿では，以上のような背景を踏まえ，セキュリティ分析で用いられることが多いアタックツリー（Attack Tree: AT）を用いて，インシデント発生後の初動対応を目的とした，感染範囲特定を行なう方式を提案する．

アタックツリーを用いたセキュリティ分析手法では，攻撃者の最終目標（以下，アタックゴール）と，目標を達成するための攻撃手段（以下，アタックメソッド）を，論理ゲートを用いて木構造で表現した，アタックツリーと呼ばれるグラフを作成することで，対象システムのセキュリティ分析を行なう．アタックツリーは，分析対象システムで想定される脅威や，脅威を顕在化させる攻撃の発生条件を分析し，攻撃の経路を洗い出すために作成されるが，その際に専門知識と高い作業コストが要求される．

そこで著者らは，分析対象システムに関する情報を入力として，攻撃手順を系統的に抽出する，ルールベース推論型のアタックツリー自動生成技術を開発した[12]．本技術では，システム構成や脆弱性情報などのファクト（事実）と，攻撃の発生条件を定義したルールを入力として，アタックツリーを生成することで，システムに潜在する脅威に対して，攻撃の経路を洗い出すことが可能である（図 1）．本技術をベースにし，対象システムで想定される攻撃シナリオを表現したアタックツリーに沿って攻撃の痕跡調査を行なうことで，初動対応に必要な感染範囲を推定することができると考える．また，事前に自動でアタックツリーを生成しておくことで，人手による調査手順の作成を簡略化することができ，もし対象システムの構成が変わっても，アタックツリーを作り直すことで対応が可能である．

4.1 システム概要

提案方式のシステム構成例を図 2 に示す．図 2 において，感染範囲推定サーバが提案方式を実装したサーバであり，対象システムの調査を行なうために組織内に配置される．また，感染範囲推定サーバは，「攻撃経路推定機能」，

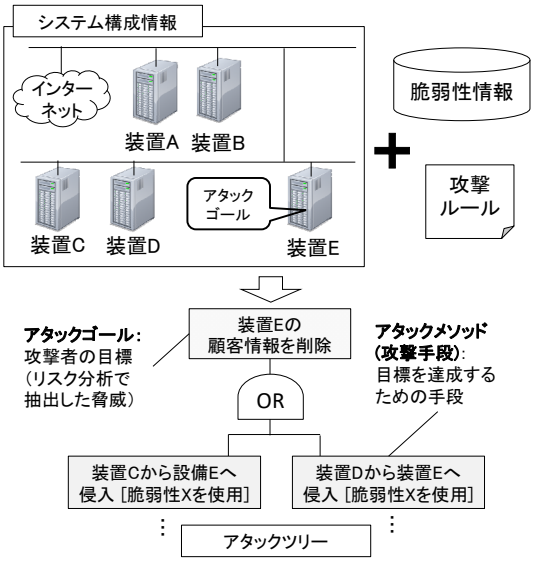

図 1　アタックツリーの生成イメージ

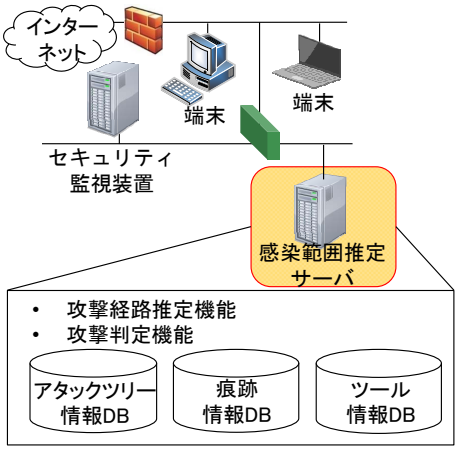

図 2　提案方式のシステム構成例

「攻撃判定機能」の二つの機能と，「アタックツリー情報データベース」，「痕跡情報データベース」，「ツール情報データベース」の三つのデータベースを有する．

4.2 各機能の説明

4.2.1 攻撃経路推定機能

本機能では，アタックツリーで表現された攻撃シナリオに沿って攻撃経路を推定する．

事前準備

まず事前準備として，アタックツリー自動生成技術[12]を用いて対象システムに対応したアタックツリーを生成し，アタックツリー情報データベースに格納しておく．アタックツリーには，攻撃の対象となる端末，アタックメソッド，及びノード間の接続関係が定義され，親ノードの攻撃が行なわれるための前提条件を，分岐条件 AND または OR で表現される．アタックツリー情報データベースに格納される情報の例を表 3 に，表 3 に基づいて表現されるアタックツリーを図 3 に示す．なお，攻撃シナリオは，論理ゲー

表 3　アタックツリー情報データベースの例

ノード ID	端末 ID	分岐条件	親ノード ID	アタックメソッド	攻撃 ID
1	D	-	-	顧客情報を削除	-
2	D	OR	1	“OSの脆弱性X”を用いて侵入	A00001
3.1	B	-	2	“OSの脆弱性Y”を用いて侵入	A00002
3.2	C	-	2	“ソフトウェアOの脆弱性Z”を用いて侵入	A00003
4	A	AND	[3.1, 3.2]	“マルウェアP”の実行による感染	A00004
5.1	A	-	4	端末情報を収集	[A50020, A50022]
5.2	A	-	4	C&Cサーバとの通信	…
6	A	-	[5.1, 5.2]	メールに添付された“マルウェアQ”の実行による感染	…
…	…	…	…	…	…

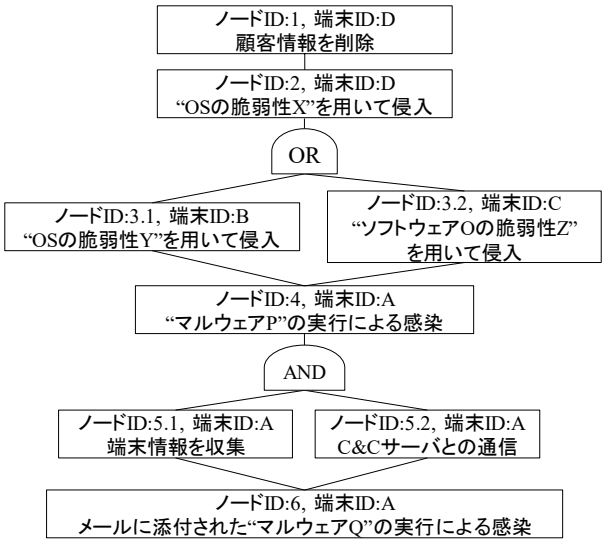

図 3　表 3 で表現されるアタックツリーの例

トで繋がれていない一つ一つの攻撃経路のことであり，表 3 の例では，ノード ID を用いて記載すると，攻撃シナリオは以下の二つが挙げられる．

- ID:6→ID:5.1 かつ ID:5.2→ID:4→ID:3.1→ID:2→ID:1
- ID:6→ID:5.1 かつ ID:5.2→ID:4→ID:3.2→ID:2→ID:1

また，侵害を受けたシステムを特定するために，脅威が存在したことを示す攻撃の痕跡情報を，表 4 に示す例のように，事前に痕跡情報データベースに格納しておき，アタックツリーの各ノードと関連付けておく（表 3 と表 4 では，攻撃 ID を使用）．痕跡情報の例として IOC（Indicator of Compromise: IOC）と呼ばれる，マルウェアのファイル名やハッシュ値，悪性の URL やドメイン名，永続化用 Windows レジストリなどの情報がある．IOC の代表的な記述形式として，ネットワークベースの IOC として Snort ル

表 4　痕跡情報データベースの例

攻撃ID	痕跡情報
A00002	Filepath:¥Windows¥System32¥...
A00003	ProgramName:O Version: 1.0.1 to 1.1.0
A00004	Filemame:malwareP.exe RegKey:¥Software¥Microsoft¥Windows¥CurrentVersion¥Run
…	…

ール[13]が，ホストベースの IOC として OpenIOC[14]や Yara[15]がある．他には，偵察や，内部ネットワークへのマルウェアの侵入拡大の活動であるラテラルムーブメントの段階の攻撃活動を示す痕跡情報がある．これらは，悪用された正規ツールの痕跡であることが多い[11]．その場合の調査方法に関しては 4.2.2 項に示す．

攻撃経路の推定処理

アタックツリー情報データベースの情報を基に，攻撃経路を推定する処理のフローの例を図 4 に示す．以下に，図 4 のフローの各処理について説明する．

① セキュリティ監視装置のアラートをトリガーに，攻撃経路の推定を開始する．
② アラートの内容に対応するアタックツリーを検索する．ある場合は②へ，ない場合は⑧の処理へ進む．
③ アタックツリーのノードの中から，痕跡調査の起点とするノードを選択する．

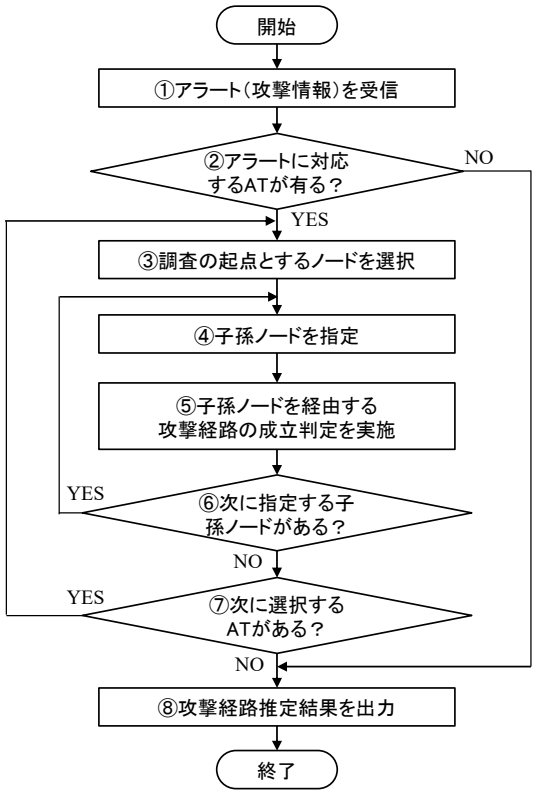

図 4　攻撃経路の推定処理のフロー

Vol.2020-DPS-182 No.39
Vol.2020-CSEC-88 No.39
2020/3/13

④ ③で選択したノードの子孫ノードのうち，一つの子孫ノードを指定する．指定できる子孫ノードが複数ある場合は，例えばノード ID の順に指定する．処理⑥から戻った場合は，攻撃経路の成立判定をしていない子孫ノードを一つ指定する．

⑤ ④で指定されたノードを経由する攻撃経路が成立するか判定するため，ノードに示されるアタックメソッドが行なわれたかどうかを，4.2.2 項に示す「攻撃判定機能」を用いて判定する．指定したノードが，攻撃の可能性がないと判断された場合は，以降の全ての子孫ノードを経由する攻撃経路が成立しないと判定する．そうでなければ，指定したノードを経由する攻撃経路が成立すると判断する．

⑥ ⑤の処理を実施していない子孫ノードがある場合は④へ戻り，そうでない場合は⑦の処理へ進む．

⑦ ②の処理で選択したアタックツリー以外に，アラートに対応するアタックツリーがある場合は③へ，そうでない場合は⑧の処理へ進む．

⑧ 攻撃経路の推定結果を出力する．

4.2.2 攻撃判定機能

本機能では，アタックツリーの各ノードのアタックメソッドによって，端末が攻撃を受けたかどうかを判定する．APT における攻撃のフェーズを定義した，サイバーキルチェーン[16]において，キルチェーンの後段のフェーズでは，感染を決定付ける IOC が被害端末に残る場合が多いため，IOC の有無によって攻撃の判定が可能である．しかし，前段のフェーズは，偵察や侵入拡大を目的として正規ツールが悪用されることが多く，また後段のフェーズでも，発見されないように正規ツールを使って攻撃する場合もある[3]．この場合，IOC だけでなく，悪用された正規ツールを手掛かりに感染の有無を判断する必要がある．

そこで，本機能では IOC の調査による攻撃判定に加え，攻撃者と攻撃者とユーザの正規ツールの利用頻度から，攻撃の有無を判定する．

事前準備

まず公開情報などを用いて，攻撃者が侵入後の情報収集やラテラルムーブメント，さらには最終目標の達成を目的として使用される可能性がある正規ツールと，それらが過去にサイバー攻撃で用いられた頻度に関する情報を定義しておく．それらのツールに対し，対象のシステムや組織内における業務時のログを用いて，正規ユーザの利用頻度やその時間帯などの情報を収集する．他にも，例えば対象が制御システムの運用環境の場合，保守作業計画の中で許可されるツールと実施時間に関する情報があれば，それを用いることもできる．これらの情報をツール情報データベースに格納しておく．利用頻度の格納例を表 5 に示す．データベースの情報は定期的に更新することで，最新の攻撃者の手法や，組織の利用環境に対応する必要がある．

表 5 ツール情報データベースの例

攻撃ID	ツール名	攻撃者の利用頻度	正規ユーザの利用頻度	操作履歴の記録
A50020	tasklist	高	低	しない
A50021	net use	高	低	しない
A50022	route	低	低	する
A50023	telnet	高	高	する
・・・	・・・	・・・	・・・	・・・

次に，攻撃者とユーザの利用頻度に統計上の有意差がないツールを特定し，両者の活動の区別を行なうために，それらのツールに対して正規ユーザがツールを操作したこと操作履歴として記録するようにする（表 5 の例では，route と telnet が該当とする．ただし，リソースの制約がない場合は全ての操作履歴を記録してもよい）．これらのツールの操作履歴を記録する方法としては，例えば，攻撃者によってマルウェアなどのソフトウェアによる改ざんが難しい，ハードウェアベースの入力操作記録装置を用いたり，ツールを使用する際に確認ダイアログが表示され，GUI（Graphic User Interface）上でのユーザによる操作許可を求めたりする方法が挙げられる．

攻撃の判定処理

ツール情報データベースの情報を基に，悪用されたツールを推定する処理のフローを図 5 に示す．以下に，図 5 のフローの各処理について説明する．

① システムの動作記録（Windows イベントログやファイル操作ログなど）と，ツール情報データベースを参照して，インシデントが発生する前の一定期間（数時間～数日）に操作されたツールを推定する．

② 推定したツールが，操作履歴の記録対象でない場合は③へ，記録対象である場合は④の処理へ進む．

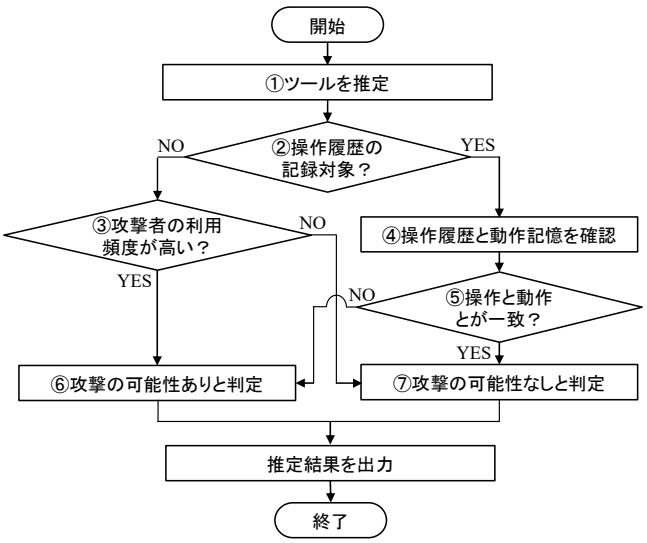

図 5 悪用されたツールの推定処理のフロー

③ ツールが操作履歴の記録対象でない場合は，ユーザと攻撃者の利用頻度に有意差があるため，ツール情報データベースを確認して，それぞれの利用頻度を確認する．攻撃者の利用頻度が高い場合は⑥へ，ユーザの利用頻度が高い場合は⑦の処理へ進む．

④ ツールが操作履歴の記録対象である場合は，ユーザと攻撃者の利用頻度に有意差がないため，ツールの操作履歴と動作記録を確認する．

⑤ 操作履歴と動作記録が一致する場合は，ユーザの意思によってツールが使用されたと判断して⑦へ，そうでない場合は⑥の処理へ進む．

⑥ ツールが攻撃者によって悪用されたものと判定する．

⑦ ツールがユーザによって使用されたものと判断する．

正規ツールを悪用した攻撃以外の攻撃に関しては，痕跡情報データベースに格納された痕跡情報を用いて，一致する痕跡が残されているかを調査することによって，攻撃の判定を行なう．

5. 考察

本章では，4 章で示した提案方式について考察する．

5.1 攻撃経路推定機能について

アタックツリーの攻撃シナリオに沿って痕跡調査を進めることで，調査対象の範囲を可能性の高い箇所に絞ることができるため，攻撃を封じ込め，被害を最小限に抑えるために隔離が必要な端末の候補を優先して特定することができる．

一方で，現在のアタックツリー自動生成技術[12]で作成されるアタックツリーは，セキュリティ分析を主目的としている．そのため生成されるアタックツリーは，キルチェーンの前段のフェーズである，偵察や侵入拡大のアタックメソッドが表現できていない．また攻撃シナリオも，アタックゴールを達成するための最短経路で表現されており，不要なステップは省略するようにしている．しかし，実際の攻撃者はこれらの攻撃活動も行なうため，インシデント対応の調査手順として妥当な攻撃シナリオになるように，ツールを改良していく必要がある．

5.2 攻撃判定機能について

本提案方式のように，システムの動作記録だけでなく，サイバー攻撃の攻撃者に気づかれない方法で，別途ユーザの操作履歴を記録し，比較することで，正規ツールの悪用によってウイルス対策ソフトやIOCの調査などの従来手法では特定が困難な場合においても，攻撃を推定することができる．本方式は，攻撃を検知するフェーズに比べると少なからず時間の余裕があり，より広範囲で多くのログが確認できる状態である，攻撃の発生後の攻撃を封じ込めるフェーズでの使用を想定しているが，PowerShell を中心とする悪用可能性の高い対象に絞るなど，リアルタイム監視が可能なリソース消費に抑えることで，攻撃検知でも使用可能な方式であると考えられる．

一方で，攻撃シナリオに沿って感染範囲を推定するためには，攻撃シナリオを構成するアタックメソッドに対し，事前に攻撃を判定するための痕跡情報を定義しておかなければならない．そこで，STIX[17]や TAXII[18]と呼ばれるサイバー攻撃に関する情報を記述・交換する国際標準規格を用いたサイバー攻撃共有基盤[19]などを活用して，痕跡情報を収集する仕組みや，もしくは模擬環境でサイバー攻撃を再現して，痕跡情報を生成する技術を開発し，人手による作業の自動化を進める必要があると考えられる．

6. まとめ

本稿では，アタックツリーで表現された攻撃シナリオに基づいて攻撃の痕跡情報を調査し，正規ツールが悪用された場合に，攻撃者とユーザのツールの利用頻度から，攻撃の有無を判断することで，インシデント発生時の感染範囲を推定する方式を提案した．

今後は，本提案方式を検証するために，まずは小規模で具体的なシステムを対象とし，インシデントが発生した際に最優先で対応が必要な範囲を絞り，使用するシステムやソフトウェアなどの情報を限定した上で，提案方式の詳細検討を行なう．次に，システムに求められる要件や制約条件を考慮した上で，プロトタイプの実装を通して評価を行なう．

参考文献

[1] 内閣サイバーセキュリティセンター：サイバーセキュリティ 2019，入手先〈https://www.nisc.go.jp/active/kihon/pdf/cs2019.pdf〉（参照 2020-02-03）．

[2] JPCERT/CC：高度サイバー攻撃（APT）への備えと対応ガイド，入手先〈https://www.jpcert.or.jp/research/20160331-APTguide.pdf〉（参照 2020-02-03）．

[3] IPA：長期期感染の実態と攻撃証跡の分析，入手先〈https://www.ipa.go.jp/files/000062281.pdf〉（参照 2020-02-03）．

[4] Cichonski, P., Millar, T., et al.: Computer Security Incident Handling Guide, NIST Special Publication 800-61 Revision 2 (2012).

[5] 総務省：我が国のサイバーセキュリティ人材の現状について，入手先〈https://www.soumu.go.jp/main_content/000591470.pdf〉（参照 2020-02-03）．

[6] National Institute of Standards and Technology (NIST): Framework for Improving. Critical Infrastructure Cybersecurity Version 1.1 (2018).

[7] 長谷川皓一，山口由紀子，嶋田創ほか：標的型攻撃に対するインシデント対応支援システム，情報処理学会論文誌，Vol.57，No.3，pp.836-848 (2016).

[8] Ayehu: IT Automation & Orchestration Platform，入手先〈https://ayehu.com/platform/〉（参照 2020-02-03）．

[9] Splunk: Splunk Software | Phantom， 入手先〈https://www.splunk.com/en_us/software/splunk-security-orchestration-and-automation.html〉（参照 2020-02-03）．

Vol.2020-DPS-182 No.39
Vol.2020-CSEC-88 No.39
2020/3/13

[10] NRI セキュア：SOAR 導入・運用支援 / サービス・製品 / 情報セキュリティの NRI セキュア，入手先〈https://www.nri-secure.co.jp/service/consulting/soar〉（参照 2020-02-03）.
[11] 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(第 2 版), 入手先〈https://www.jpcert.or.jp/research/20171109ac-ir_research2.pdf〉（参照 2020-02-03）.
[12] 島邉遼佑，浅井健志，河内清人：ルールベース推論型アタックツリー自動生成ツールにおける効率的な生成方式の提案，SCIS2019 (2019).
[13] Snort: Snort - Network Intrusion Detection & Prevention System, 入手先〈https://www.snort.org/〉（参照 2020-02-03）.
[14] Mandiant: GitHub - mandiant/OpenIOC_1.1，入手先〈https://github.com/mandiant/OpenIOC_1.1〉（参照 2020-02-03）.
[15] Alvarez, V.M.: YARA - The pattern matching swiss knife for malware researchers，入手先〈http://virustotal.github.io/yara/〉（参照 2020-02-03）.
[16] Hutchins, E.M., Cloppert, M.J. and Amin, R.M.: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, 6th International Conference on Information Warfare and Security, pp.113-125 (2011).
[17] IPA：脅威情報構造化記述形式 STIX 概説，入手先〈https://www.ipa.go.jp/security/vuln/STIX.html〉（参照 2020-02-03）.
[18] IPA：検知指標情報自動交換手順 TAXII 概説，入手先〈https://www.ipa.go.jp/security/vuln/TAXII.html〉（参照 2020-02-03）.
[19] ICT-ISAC：ICT-ISAC サイバー攻撃の防御に向けた情報共有基盤の概要，入手先〈https://www.ict-isac.jp/news/ict-isac_tip_ov.pdf〉（参照 2020-02-03）.