Computer Security Symposium 2020
26 - 29 October 2020

セキュリティオペレーションの効率化に向けたSOCアナリストの共通行動抽出

鐘本 楊[1,a)]　芝原 俊樹[1]　秋山 満昭[1]

概要：Security Operation Center (SOC) では複数のアナリストがセキュリティ機器のアラートを分析し，脅威がある場合に通知あるいは暫定対処を行う．アラートを受けて通知すべき脅威かどうかの判断はSOCアナリスト個人に委ねられ，個々のスキルに依存する部分が大きく，どのような判断基準かは共通になっていない．そのため，SOCアナリスト個々が試行錯誤して判定を行うため手順が増大し稼働がかかったり，判定の品質が一定でなかったりすることが課題である．本研究ではこの暗黙知となっているアラートに対する脅威の判断手順・判断基準を明確にし，形式知にすることで，SOCアナリストがより迅速に判断できるよう支援することでSOC業務の効率化を試みる．より具体的にはSOCアナリストの調査・分析の際に行った行動を記録し，共通する行動を明確化する．参加者実験によりアラート種類に応じて共通する検索や情報を参照するといった行動を抽出することができ，今まで暗黙だったアラート調査の手順が明確になった．

キーワード：セキュリティオペレーションセンタ, アラート，行動分析，自動化

Extracting Common Behavior of SOC Analysts for Efficient Security Operation

Yo Kanemoto[1,a)]　Toshiki Shibahara[1]　Mitsuaki Akiyama[1]

Abstract: In a Security Operation Center (SOC), multiple analysts analyze alerts triggered by security devices to determine if they are threats. Once a threat is identified, analysts notify it to a customer or respond to it. This analysis and determination is not stylized and depend on experience and skills of SOC analysts. Specifically, SOC analysts make decisions through trial and error. As a result, the analysis requires a lot of time and the quality of the decision is not constant. Therefore, we propose a method for clarifying the decision-making procedure and criteria of SOC analyst by extracting implicit knowledge from behavior of SOC analysts. We record the actions taken by SOC analysts in their analysis, and extract the common actions. The experimental result shows our method clarified the procedure for alert analysis, which was previously implicit.

Keywords: Security Operation Center, Alert, Behavior Analysis, Automation

1. はじめに

Security Operation Center (SOC) では自社または顧客のネットワークを監視し，サイバー攻撃による被害が発生した際に，攻撃対象となったシステムの管理組織や顧客への通知を行う．SOCではアナリストがセキュリティ機器から発せられるアラートを監視し，攻撃による被害や影響があるか否かを判断する．セキュリティ機器は攻撃を検知した際に，検知・遮断することが可能である．しかし，インターネットを通じて日々新たなサービスが活用できるようになっており，サイバー攻撃もそれに合わせて新しい方法が考案されていることや，既存の検知手法を回避する

[1] NTT セキュアプラットフォーム研究所
NTT Secure Platform Laboratories
[a)] yo.kanemoto.zx@hco.ntt.co.jp

ための方法が取り入れられるため，最新の攻撃をセキュリティ機器単体で完全に検知することは困難である．SOC アナリストはセキュリティ機器だけでは攻撃の脅威判定が難しい場合に，それを明確にする役割を果たしている．例えば，セキュリティ機器が誤検知した場合に，様々な脅威情報を参照して攻撃が無害で影響がないことを確認する．よって，脅威判定の正確性や迅速性は SOC アナリストのスキルに依存している．SOC では経験の浅い SOC アナリストに対しては訓練を実施したり判断手順を設けたりすることで，スキルや正確性の向上に努めている．しかし，脅威は非常に多様であり，さらに日々高度化しているため，すべての脅威の判断基準を作成し網羅し続けることは困難である．判定手順が SOC アナリスト間で明確に共有されていない脅威では，SOC アナリスト個々が試行錯誤して判定を行うための手順が増大し稼働がかかったり，判定根拠が不十分のまま解析を終了し SOC の品質が低下することが予想される．

本研究ではアラートに対する脅威の判断手順と判断基準を明確化し，経験の浅い SOC アナリストの解析支援に活用したり，定型的な解析を半自動化し稼働を難しい解析に集中させたりすることで SOC における業務の効率化や品質の向上を目指す．本研究では SOC アナリストの調査における行動を収集し，共通する行動を抽出する分析手法を提案する．実験により，提案する手法により，複数の実験参加者から共通する行動を抽出することに成功した．また，得られた共通行動が判断手順を作成することに寄与することを示す．しかし，判断基準をいかにして求めるかは今後の課題である．本研究の貢献は以下の通りである．

- 暗黙知だった SOC のアラート調査業務を可視化し，形式知化するための共通行動を抽出する手法を提案した．
- 参加者実験を行い，同種類のアラートの調査においては共通する行動が存在することを確認し，SOC アナリストの行動から半自動的な判断手順の作成に寄与した．

2. 研究背景

2.1 Security Operation Center

サイバー攻撃の高度化により，IT システムの維持管理を担う IT システム管理者だけでセキュリティインシデントに対処することが困難になり，サイバー攻撃の被害に専門的に対処する組織である Security Operation Center (SOC) が普及した [1]．SOC では自社または顧客のネットワークを監視し，サイバー攻撃による被害が発生した際に，適切な対処や管理組織への通知を行う．SOC ではアナリストが様々なセキュリティ機器から発せられるアラートを保管した Security Information and Event Management (SIEM) を監視し，攻撃による被害や影響があるか否かを判断する．被害を受けた可能性が高い場合は，攻撃対象となった機器の管理組織や顧客に通知を行う．アラートの監視は 24 時間 365 日行う必要があるため，複数の SOC アナリストが輪番で常時監視を行っている．さらに，Managed Security Service (MSS) のように SOC 機能をサービスとして提供する事業者では多くの顧客のネットワークを監視するため，より多くの SOC アナリストが交代で勤務にあたっている．

1 章で説明した通り，セキュリティ機器単体で最新の攻撃を完全に検知することは困難である．つまり，セキュリティ機器の検知結果には少数だが，攻撃を検知しない検知漏れや正常な通信を攻撃として検知してしまう誤検知が発生する．セキュリティ機器は検知漏れを少なくするように設計されているため，SOC アナリストは誤検知を取り除き，機器では完全でない部分を補う役割を担っている．つまり，SOC アナリストはセキュリティ機器だけでは攻撃の脅威判定が難しい場合に，それを明確にする役割を果たしている．ここでいう脅威判定とは攻撃があった際にその攻撃によって被害や影響をもたらすものかどうかを判定することを指す．

SOC ではアンチウイルスを始め，Endpoint Detection and Response (EDR) や Web Application Firewall (WAF) など 様々な種類のセキュリティ機器を扱うため，アラートの種類も様々であり，SOC アナリストの脅威判定の調査内容も多岐にわたる．例えば，外部から攻撃を受けているホストに対する脆弱性調査，マルウェア感染が疑われるホストに対する通信先情報と各種脅威情報を照らし合わせる Open Source INTelligence (OSINT) 調査などを実施する．著者らによる SOC アナリストに対するヒアリングにより．様々ある SOC 業務の中で OSINT 調査が最も頻繁に行われていることがわかった．

2.2 課題

脅威判定における判定基準は個々の SOC アナリストのスキルに依存している．経験の浅い SOC アナリストに対しては訓練を実施したり判断基準を設けたりすることで，スキルや正確性の向上に努めている．しかし，脅威は非常に多様であり，さらに日々高度化しているため，すべての脅威の判断基準を作成し網羅し続けることは困難である．SOC アナリストは個々の知識や経験をもとに，通信ペイロードの解析，OSINT や脅威情報の参照，過去事例の検索など，自身の経験から確立した手順をもとに調査を行い，脅威判定を行うことが多い．OSINT 調査では特に，インターネット上に散らばった情報を調査するため，自由度が高く，経験やスキルを要する．よって，脅威判定手順が SOC アナリスト間で明確に共有されていない場合，SOC アナリスト個々が試行錯誤して判定を行うための手順が増大し稼働がかかることが予想される．

この課題は，SOC における課題を調査した複数の研究でも指摘されており，著者らがヒアリングを行った SOC

だけでなく，多くの SOC が抱える課題である．Zhong らの研究 [2] では，SOC の課題としてアラートが大量にあり SOC アナリストの人数が限られる中，大量のアラートを対処するには SOC アナリストの作業を自動化することが必要と述べている．Kokulu らの研究 [3] では，SOC アナリストと SOC マネージャが認識する SOC の課題をインタビュー調査によって明らかにした．SOC マネージャの間でもっとも多く上がった課題が分析・対処の速度を上げるための自動化であった．一方で SOC アナリストは，既存の検知手法の精度に関する懸念や，新しい攻撃への対処を自動化することが難しいことを指摘した．Sundaramurthy らの研究 [4] では，SOC アナリストが実施する分析作業は高度かつ複雑ゆえに暗黙知に基づくことが多いと指摘し，組織に入り込んで SOC アナリストを観察することで彼らの行動のモデル化を試みた．

SOC アナリストの支援のため，システム操作の自動化や SOC 業務の自動化に関してはすでに実用化されている製品も存在する．例えばシステム操作については Robotic Process Automation (RPA) 製品が現れ，人間が定義した操作を繰り返し実行することが可能である [5]．またセキュリティオペレーションに特化したものとして Security Orchestration and Automated Response (SOAR) 製品が存在する．SIEM は様々なセキュリティ機器のアラートを管理製品はセキュリティ製品のアラートに対応して予め定義したプレイブックと呼ばれる条件と対策を自動的に施すものである．どちらも人間の操作を削減して業務の効率化を目指すものであるが，プレイブックを記述するためには，本研究で形式知化を目指す判断手順が事前に定義されている必要がある．

3. 共通行動抽出

アラートに対する脅威判定を行うための OSINT 調査は SOC アナリストの主要業務の一つである．脅威判定手順が SOC アナリスト間で明確に共有されていない場合，SOC アナリスト個々が試行錯誤して判定を行うための手順が増大し稼働がかかることが予想される．本研究では SOC アナリストの OSINT 調査において今まで暗黙知だった SOC アナリストの脅威判定を形式知にとして抽出することを試みる．

まず，本研究が目指す形式知について定義する．一般的な形式知の定義は文書や手順書などによって言葉や図，数式で示された知識の状態を指している [6]．一方，暗黙知とはスキルやノウハウのように言葉にできていない段階の知識の状態を指す．また，Zhong ら研究によれば SOC アナリストの行動は Action-Observation-Hypothesis (AOH) モデルとして解釈できる [2, 7]．AOH モデルとは人間の行動を実行，観察，仮説の 3 つ処理手順が循環していると考え，フローチャートのように表現する方法である．例えば，OSINT 調査において，ある通信先が悪性かどうかを判断する場合，まず脅威情報を利用してその通信先を検索し (Action)，通信先のレピュテーション結果を確認する (Observation)，その結果によって悪性か否かを判断する (Hypothesis) という一連の行動はこのように AOH モデルで表現される．本研究では AOH モデルで表現される一連の明示的な処理手順を求めたい形式知として定義する．Zhong らの研究でも述べられるように AOH モデルを作成するには繰り返し行動し，継続的に観察し，仮説となる条件を求める必要がある．

図 1 に本研究の処理概要を示す．提案手法は大きく行動収集と行動分析の 2 つの処理から構成される．行動収集では様々なセキュリティ機器のアラートを保管する SIEM から SOC アナリストがアラートを受け取り，調査する際の行動をログとして記録する．行動分析では収集した行動ログから複数の SOC アナリスト間で共通する行動を抽出する．

3.1 行動収集

OSINT 調査では脅威情報を掲載する Web サイトを頻繁に活用することから本研究では収集した行動から SOC アナリストに共通の行動を抽出することを考慮して，同種類のアラートに対する複数の SOC アナリストの行動を収集する．取得する行動の粒度は処理手順として再現できることを鑑み，人間が認識できる最小の粒度で行動をログとして記録する．ログ取得は SOC アナリストの端末で行われるため，例えば，マウスカーソルの座標変化のような過度な粒度で行動を取得してしまうと端末の負荷を増大させる恐れがある．本研究で述べる行動とは一例の操作の系列として考える．操作とはクリックやキー入力のようなこれ以上分解できない行動の最小の単位として定義する．表 1 に本研究で取得する操作とその内容を示す．例えば，ある通信先が悪性かどうかを判断する場合を想定する．SOC アナリストはまず脅威情報の Web サイトにアクセスする (page)．次に通信先の文字列を選択 (select) してコピーペースト (copy, paste) あるいは直接，脅威情報の Web ページに入力する (input)．次に検索ボタンをクリック (click) して，検索結果を閲覧する (scroll)．さらにタブを切り替えて (tab) 別の脅威情報を参照する．このように，表 1 にて定義した操作を取得することで十分 OSINT 調査の操作を網羅できる．

行動収集機能の実装ではブラウザ拡張を利用した方法を採用した．Web プロキシを利用した情報取得方法も存在するが，SSL 通信の問題やタブの注目やクリックなど収集できない操作があり要件を満たさないため採用しなかった．ブラウザ拡張を利用する方法の懸念点としてはブラウザ間の差異に対するサポートである．現状では適用可能なブラ

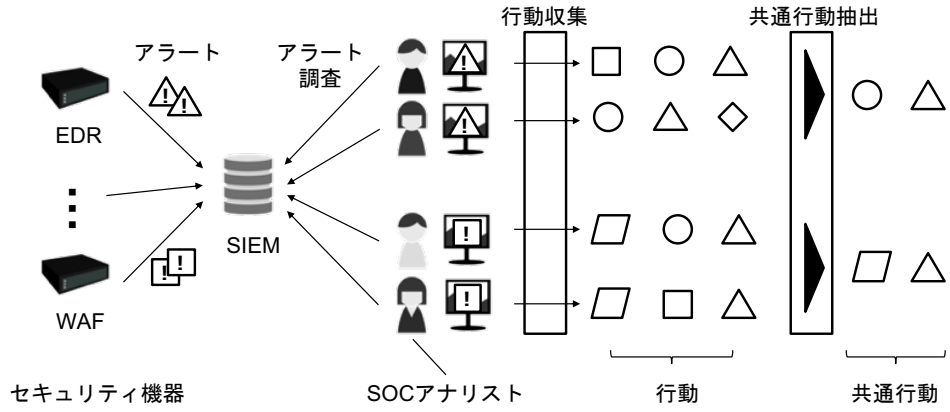

図 1: 本研究の処理概要
Fig. 1 Overview of our research.

表 1: 収集する操作の一覧
Table 1 A list of actions we collect.

操作	内容
ページアクセス (page)	時刻，Web ページの URL
タブの注目 (tab)	時刻，注目しているタブの Web ページの URL
クリック (click)	時刻，Web ページの URL，対象 HTML 要素，クリック時のボタン
文字列選択 (select)	時刻，Web ページの URL，選択文字列
文字列のコピー・カット・ペースト (copy, cut, paste)	時刻，Web ページの URL，対象文字列
文字列入力 (input)	時刻，Web ページの URL，入力文字列
スクロール (scroll)	時刻，Web ページの URL，対象 HTML 要素，スクロール割合 (25%, 50%, 75%)

ウザは限られるが，Mozlilla 社の WebExtension API[*1]のように互換性ある開発が行われている背景もあり，将来的には多くのブラウザで適用可能になると考えられる．

3.2 行動分析

同じアラートに対する異なる SOC アナリストの行動から共通する行動を抽出する．本研究で述べる共通とは操作における完全な一致という意味ではなく，同様な操作として位置付ける．同様な行動をしていても，時刻や環境によってはログとして記録される内容が異なる場合がある．例えば同じクリックをしても時刻や環境によってアクセス先の Web ページの URL パラメタが変化することがある．しかし，この差異は人間では認識しない差異であり，この差異は抽象化して扱うべきである．そこで本研究では取得

[*1] https://developer.mozilla.org/ja/docs/Mozilla/Add-ons/WebExtensions/Porting_from_Google_Chrome

表 2: 操作に対する抽象化処理
Table 2 Normalization process for each action content.

対象操作の内容	抽象化処理
時刻	消去
Web ページの URL	URL を URL パスに置換
HTML 要素	HTML タグで囲まれる内容を消去
選択文字列	ハッシュ値や IP アドレスなど形式が存在する場合はそれを表す符号に置換

した操作記録を抽象化し識別子となる ID を付与する．この手法はログ分析やデータマイニング等でよく用いられる手法である [8]．各操作の内容に対する具体的な抽象化処理は表 2 に示す．操作を ID 化した後，操作 ID の SOC アナリスト間の出現頻度を求め，ある閾値以上の出現頻度で現れる操作を共通操作として扱う．例えば，ある Web ページ https://example.com/sample.js?param=value にアクセスした際の操作は (ID_1, page, example.com, sample.js) のように ID が割り当てられた状態で扱われる．

4. 行動分析実験

サイバーセキュリティ業務経験や SOC 業務経験がある複数の参加者に対して著者らが用意したシナリオで OSINT 調査を行ってもらい，調査時の行動を収集した．収集した行動に対してその共通点の分析を行った．

4.1 参加者募集

実験に際して，サイバーセキュリティの知識があり，サイバーセキュリティの業務経験を有する著者らの勤務先の同僚を参加者として募集した．参加者全てが SOC における業務経験を有する訳ではないが，サイバーセキュリティ業務の従事年数は長いため，OSINT 調査を適切に遂行可能なスキルを持っており，被験者としては適切である．参加者に SOC における OSINT 調査に関する実験であるこ

表 3: 参加者情報
Table 3 Participants in our research study.

参加者番号	職種	業務経験	SOC 業務経験
P1	研究	7 年	なし
P2	開発	15 年	なし
P3	開発	3 年	なし
P4	研究	2 年	なし
P5	研究	8 年	3 年
P6	研究	7 年	なし

と，著者らが用意したアラート発生の 3 つのシナリオに対して脅威判定を行ってもらいたいことを説明し理解を確認した．また Web ブラウザにブラウジング行動を収集するツールをインストールすることおよび本実験に収集された行動ログを利用することに関して，参加者から同意を得た．表 3 に各参加者の情報を示す．

4.2 調査シナリオの設計

SOC における OSINT 調査を想定して，表 4 に示す 3 つの調査シナリオを作成した．シナリオの作成にあたっては参加者と異なる SOC アナリストから得た業務で頻出する OSINT 調査の事例を参考にした．アラート情報に示すファイル名や通信先情報は実際のマルウェアに利用されていたものである．シナリオ 1 および 2 は PC 端末などのクライアント側の脅威を想定したものであり，シナリオ 3 はサーバ側の脅威を想定したものである．参加者はこの 3 つのシナリオの提示文およびアラート情報が与えられ，調査を開始する．各シナリオにおいて調査が終了した時点で脅威あるいはで脅威でないの判定のみを行う．

4.3 実験結果と考察

全ての参加者が全てのシナリオで正しく脅威判定を行っていた．そのため，収集したすべての行動を対象として分析を行った．

4.3.1 共通操作

各シナリオについて取得した行動ログに対して 3.2 節にて述べた分析を行い，抽出できた共通操作を表 5 に示す．頻度とは対象の操作が参加者間で発生する確率である．頻度が 1.00 の場合は参加者全員が行った操作であり，頻度が 0.50 の場合は参加者の半分が行った操作であることを示している．実験では頻度が 0.50 以上の操作を共通する操作として扱うこととした．シナリオ 1 では参加者は項番 1-1 から 1-4 の操作より検索エンジンである Google 検索を活用して対象ファイル名に関する情報を検索し，その結果を閲覧していることを示している．項番 1-5，1-6，1-8，1-9 および 1-11 の操作は検索結果が示すブログや脅威情報の内容を閲覧していることを表している．著者らによる確認の結果，これらのブログや脅威情報は検索結果の上位数件以内に含まれている．つまり，アラート情報に含まれるファイル名を検索エンジンで検索し，上位数件の結果を確認し，マルウェアに関する記述があったため，マルウェア感染が発生していると結論づけていることが推測できる．

シナリオ 2 では参加者は項番 2-1，2-2，2-4 の操作よりシナリオ 1 と同様に Google 検索で対象 IP アドレスに関する情報を検索したり，脅威情報共有サイトである VirusTotal (VT) で対象 IP アドレスに関する情報を検索していることがわかる．特に項番 2-2，2-4 の操作のアクセス URL パスが VT の検索機能 (/gui/search) あることから，参加者の半数以上が Google 検索の結果に頼っている訳ではなく，VT を活用して IP アドレスの悪性判定を行う知見があることを表している．VT に掲載されている悪性判定結果からマルウェア感染が発生し，対象 IP アドレスに対する C2 通信が開始していると結論づけていることが推測できる．

シナリオ 3 ではシナリオ 1，2 と同様に Google 検索で攻撃コードに含まれるキーワードの検索を行い，攻撃コードに関する情報を収集している．項番 3-5 でアクセスした Web ページに攻撃コードと CVE 番号に関する情報が記載されていたため，項番 3-5，3-6 の操作により攻撃コードが対象とする脆弱性情報を参照した．脆弱性情報からこの攻撃が Cisco 社の製品を狙うの脆弱性に対するものであると判明し，通常の Web サーバには影響しない攻撃であるから無害と結論づけていることが推測できる．

以上，3 つのシナリオを通じて共通している動作は検索エンジンでキーワードとなるような単語を検索し，上位の検索結果を確認することが共有的な操作であることがわかった．シナリオ 1 では Google 検索でファイル名を検索後，上位の検索結果を確認し，マルウェアに関する記述があることからマルウェア感染と判断したことが推測できる．シナリオ 2 では Google 検索でアラート情報にある IP アドレスを検索し，脅威情報である VT の情報を参照し，VT の判定結果からマルウェア感染と判断したことが推測できる．シナリオ 3 では Google 検索で攻撃コードに含まれるキーワードを検索し，攻撃に関する脆弱性情報である CVE 番号を入手したことから CVE 番号で攻撃が対象とする製品を把握し，シナリオで想定するサーバ環境と一致しないことから無害であり，脅威でないと判断したと推測できる．

シナリオ内では行動は共通するものの，シナリオ間では最初に検索エンジンで検索を行うこと以外に共通的な部分がないことから，共通的な行動はアラートの内容に応じて脅威判定の行動がそれぞれ異なることがわかった．本研究で求めた共通行動からアラートの種類ごとに有用な OSINT 情報を把握したり，必要な調査の観点を整理することができたりするため，この点も SOC 業務の効率化に貢献するものである．

本研究の目的である形式知を作成する上では共通行動だ

表 4: 調査シナリオの一覧
Table 4 A list of analysis scenarios.

番号	脅威箇所	提示文	アラート情報	想定する脅威判定	脅威判定の理由
S1	C[1]	PC 端末でアラート情報に示すファイル名がアンチウイルスに検知された．誤検知なのか，あるいはマルウェア感染が疑われ，脅威となるかを判断してほしい．	tiagac3.png	脅威	対象のファイル名はマルウェアに感染した後にダウンローダを通じて取得されるものであるため．
S2	C[1]	PC 端末でアラート情報に示す通信先が Web アクセスを監視する IDS によって検知された．誤検知なのか，それともマルウェア感染が疑われ，脅威となるかを判断してほしい．	37.221.*.* 45.153.*.*	脅威	2 つの IP アドレスは一貫してマルウェアの C2 通信に利用されるものであるため．
S3	S[2]	WAF でアラート情報に示すリクエストが検知された．この WAF が対象としている Web サーバでは WordPress が運用されている．誤検知なのか，あるいは被害が発生して脅威となるかを判断する．	`GET /+CSCOT+/translation-table ?type=mst&textdomain= /%2bCSCOE%2b/portal_inc.lua &defaultlanguage &lang=../ status: 200 response_size: 1423`	脅威でない	この攻撃は Cisco 製品で発見された脆弱性を狙ったものであり，対象の Web サーバのアーキテクチャと異なるため，攻撃が成立することがないため．

[1] クライアント側
[2] サーバ側

けでなく，判定の根拠に至った脅威基準を条件として表す必要があるが，今回の実験ではその根拠となる部分を見出すことはできていないため，この部分は今後の課題である．

4.3.2 参加者間の Web アクセス傾向

次に参加者ごとに異なる行動を分析するために，参加者間の Web アクセス傾向を分析した．表 6 にその結果を示す．シナリオを通して参加者間で Web サイトへのアクセス頻度が高い順に並んでいる．前節の分析結果からわかるように表の上位には Google 検索や VT は多くの参加者から利用されていることがわかる．一方，表の下位には特定の参加者しかアクセスしない Web サイトが並ぶ．著者らが確認した結果，表の下位に位置する Web サイトは検索結果としても下位に存在する傾向であった．つまり，検索上位の結果では断定せずに，より多くの情報を見た上で脅威判定しようとする個性が現れている．特にシナリオ 3 では参加者 P2 および P5 は他の参加者は行わなかった Web サイトへのアクセスが顕著に現れている．P2 は Cisco 製品の公式の情報を参照したり (tools.cisco.com へのアクセス)，P5 はそれだけでなく，攻撃者によって PoC コード[*2]を悪用された場合にサーバ側がどのようなレスポンスを返すかを確認していると推測する (gblogs.cisco.com，exploit-db.com へのアクセス)．P2 や P5 は業務経験の長さや SOC 経験を有することから，より確実な根拠から調査を行おうとする行動が他の参加者との差異を生んだと考える．このように，熟練した SOC アナリストからその知見を明確にし共有する効果にも本研究は貢献できると考える．

[*2] 脆弱性が攻撃可能であることを検証するコード

5. 関連研究

本研究では SOC の効率化に対する研究は IDS などを始めとるセキュリティ機器のアラートの質を向上する方法 [9] と SOC アナリストの調査，分析を支援する方法の 2 つの観点に分けて考える．IDS の検知精度向上の研究は古くから行われている．Sommer らは IDS に利用される攻撃の特徴となる部分をパターン化したシグネチャに情報量を付加して誤検知を減らす手法を提案している [10]．その後，アラート間の相関や，アラートと脆弱性の情報や OS レベルの情報など異なる種類の情報と関連性に着目した誤検知低減手法が提案された．Kruegel らの手法では事前にネットワークに対して脆弱性スキャンを行い，その際に発覚した製品のバージョンに脆弱性が存在すれば，その製品に攻撃が仕掛けられれば，アラートの緊急度をより高く設定するものである [11]．これにより，SOC アナリストは喫緊のアラートに対してより迅速に調査に取り掛かることができることが効果である．鐘本らの手法ではサーバに対する攻撃に含まれる攻撃コードを抽出し，エミュレーションを行うことで攻撃成功時の痕跡を取り出し，痕跡が通信内容に含まれる否かで攻撃の成否を判定することを提案している [12]．攻撃が成功している可能性が高いアラートの対処優先度を高くし，攻撃が失敗しているアラートの対処優先

表 5: 各シナリオにおける共通操作
Table 5 Common operations observed for each scenario.

	項番	頻度	Web サイト	操作	URL パス	補足情報
S1	1-1	1.00	www.google.com	page	/search	
	1-2	0.83		scroll	/search	検索語例: “tiagac3.png”, “Adhijuac3.png”, “IcedID”
	1-3	0.67		tab	/search	
	1-4	0.50		click	/search	クリック対象: <h3 class=“LC20lb DKV0Md” >
	1-5	1.00	isc.sans.edu	page	/forums/diary/*	
	1-6	0.83		scroll	/forums/diary/*	
	1-7	0.67		tab	/forums/diary/*	
	1-8	0.67	any.run	page	/report/*/*	
	1-9	0.67		scroll	/report/*/*	
	1-10	0.50		tab	/report/*/*	
	1-11	0.67	malware-traffic[1]	page	/2020/05/19/index.html	
	1-12	0.50		tab	/2020/05/19/index.html	
S2	2-1	1.00	www.google.com	page	/search	検索語例: “37.221.*.*”, “45.153.*.*”, “ポートスキャン”, “悪性 IP アドレス”
	2-2	0.67	www.virustotal.com	page	/gui/search/45.153.*.*	
	2-3	0.67		page	/ip-address/45.153.*.*/detection	
	2-4	0.50		page	/search/37.221.*.*	
	2-5	0.50		page	/ip-address/37.221.*.*	
	2-6	0.50		page	/ip-address/37.221.*.*/detection	
	2-7	0.50		page	/ip-address/37.221.*.*/details	
	2-8	0.50		page	/ip-address/37.221.*.*/relations	
	2-9	0.50		page	/ip-address/45.153.*.*/details	
	2-10	0.50		page	/ip-address/45.153.*.*/relations	
S3	3-1	1.00	www.google.com	page	/search	検索語例: 攻撃コード, “portal_inc.lua”, “CVE-2020-3452 wordpress”
	3-2	0.83		click	/search	クリック対象: <input ... aria-label=“検索” ... >
	3-3	0.50		tab	/search	
	3-4	0.50		scroll	/search	
	3-5	0.67	nvd.nist.gov	page	/vuln/detail/CVE-2020-3452	
	3-6	0.50		click	/vuln/detail/CVE-2020-3452	クリック対象: <p data-testid=“vuln-description” >
	3-7	0.50	jp.tenable.com	page	/blog/*	

[1] www.malware-traffic-analysis.net

度を下げることでより効率的なアラートの対処を提案している．芝原らの手法では教師あり学習を用いてセキュリティ侵害につながるアラートとそうでないアラートを区別することでアラートの対処優先度を変える手法を提案している [13]．これらの手法ではセキュリティ機器のアラート品質を向上することに寄与するが，課題で述べた様に検知結果が確実であるという訳ではない．また，対処できる攻撃の種類が限られているなど，SOC アナリストが確認する必要性は残っている．

一方で SOC アナリストを支援する手法も研究が進んできている．Zhong らの手法では SOC アナリストに独自ツールを利用させ，取得できた行動ログから SOC アナリストの業務支援を行おうとしている [2]．Zhong らの手法では独自のツールを作成し，SOC アナリストに操作させることで SOC アナリストの行動を取得する．しかし，SOC アナリストは独自ツールで操作を行わなければならないという制約があり，多くある SOC 業務の中で適用できる用途が限定的である．

6. おわりに

本研究では暗黙知だった SOC アナリストの脅威判定手順を形式知として明確化することを目的として，SOC アナリストの行動を記録し，そこから共通な部分を取り出すことで脅威判定手順を明確化した．実験の結果，様々なシナリオからアナリスト間で共通する行動を抽出でき，得られた共通行動が判断手順を作成することに寄与することがわかった．今後の課題はシステム的に抽出した共通行動から脅威判定の根拠となる部分を求めることである．

謝辞 本研究にあたり SOC に関する知見を頂いた NTT セキュリティ・ジャパン株式会社の羽田大樹氏，森下知哉氏，野岡弘幸氏に感謝いたします．また参加者実験に快くご協力いただいた同僚の皆様に感謝いたします．

表 6: 各シナリオにおける Web サイトへのアクセス
Table 6 Status of web site accessed for each scenario.

	シナリオ 1						シナリオ 2						シナリオ 3					
参加者	P1	P2	P3	P4	P5	P6	P1	P2	P3	P4	P5	P6	P1	P2	P3	P4	P5	P6
www.google.com	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
www.virustotal.com					x	x	x		x	x	x	x						
any.run	x		x		x	x		x		x		x						
isc.sans.edu	x	x	x	x	x	x												
malware-traffic[1]	x			x	x	x					x							
nvd.nist.gov													x	x			x	x
jp.tenable.com														x		x		x
ipinfo.io							x	x										
cve.mitre.org															x	x		
github.com															x			x
twitter.com													x					x
blogs.juniper.net	x																	
www.cylance.com		x																
web-designer.cman.jp												x						
www.cman.jp												x						
project.iw3.org								x										
www.abuseipdb.com										x								
www.security-next.com														x				
tools.cisco.com														x				
securityaffairs.co														x				
www.idaten.ne.jp																	x	
www.cisco.com																	x	
www.exploit-db.com																	x	
www.secpod.com																	x	
gblogs.cisco.com																	x	
www.tagindex.com															x			
blog.rapid7.com																		x
packetstormsecurity.com													x					

[1] www.malware-traffic-analysis.net

参考文献

[1] 早川敦史, 阿部慎司, 武井滋紀, 河島君知, 田中朗, ももいやすなり, 彦坂孝広. セキュリティ対応組織 (SOC / CSIRT) の教科書. 日本セキュリティオペレーション事業者協議会 (ISOG-J), 2018.

[2] Chen Zhong, John Yen, Peng Liu, and Robert F Erbacher. Learning From Experts' Experience : Toward Automated Cyber Security Data Triage. *IEEE Systems Journal*, Vol. 13, pp. 603–614, 2019.

[3] Faris Bugra Kokulu, Tiffany Bao, and Adam Doupé. Matched and Mismatched SOCs : A Qualitative Study on Security Operations Center Issues. In *ACM CCS*, pp. 1955–1970, 2019.

[4] Sathya Chandran Sundaramurthy, John McHugh, Xinming Ou, Michael Wesch, Alexandru G. Bardas, and S. Raj Rajagopalan. Turning Contradictions into Innovations or: How We Learned to Stop Whining and Improve Security Operations. In *SOUPS*, pp. 237–251, 2016.

[5] Wil M P Van Der Aalst, Martin Bichler, and Armin Heinzl. Robotic Process Automation. *Business & Information Systems Engineering*, Vol. 60, No. 4, pp. 269–272, 2018.

[6] Ikujiro Nonaka and Ryoko Toyama. *The Knowledge-creating Theory Revisited: Knowledge Creation as a Synthesizing Process*. Palgrave Macmillan UK, 2015.

[7] Chen Zhong, Deepak Samuel, John Yen, Peng Liu, Robert Erbacher, Steve Hutchinson, Renee Etoty, Hasan Cam, and William Glodek. RankAOH : Context-driven Similarity-based Retrieval of Experiences in Cyber Analysis. In *IEEE CogSIMA*, pp. 230–236, 2014.

[8] Tatsuaki KIMURA, Akio WATANABE, Tsuyoshi TOYONO, and Keisuke ISHIBASHI. Proactive Failure Detection Learning Generation Patterns of Large-scale Network Logs. *IEICE Transactions on Communications*, 2018.

[9] Neminath Hubballi and Vinoth Suryanarayanan. False Alarm Minimization Techniques in Signature-based Intrusion Detection Systems: A Survey. *Computer Communications*, Vol. 49, pp. 1–17, 2014.

[10] Robin Sommer and Vern Paxson. Enhancing Byte-level Network Intrusion Detection Signatures with Context. In *ACM CCS*, pp. 262–271, 2003.

[11] Christopher Kruegel and William Robertson. Alert Verification: Determining the Success of Intrusion Attempts. In *DIMVA*, 2004.

[12] 鐘本楊, 青木一史, 三好潤, 嶋田創, 高倉弘喜. 攻撃コードのエミュレーションに基づく Web アプリケーションに対する攻撃の成否判定手法. 情報処理学会論文誌, Vol. 60, pp. 945–955, 2019.

[13] 芝原俊樹, 小寺博和, 千葉大紀, 秋山満昭, 波戸邦夫, Ola Söderström, Daniel Dalek, 村田正幸. 潜在的な重要アラートの推定によるインシデント特定の効率化. コンピュータセキュリティシンポジウム論文集, pp. 1092–1099, 2019.