L-005

Cyber Threat Intelligence を活用したログ分析システムの提案
Proposal of the Intelligence Driven Cyber Threat Analysis System

片山貴大‡ 川口信隆‡ 杉本暁彦‡ 重本倫宏‡
Katayama Takahiro Kawaguchi Nobutaka Sugimoto Akihiro Shigemoto Tomohiro

1. はじめに

サイバー攻撃の巧妙化に対し，標的型攻撃の 42%が見逃されているとの調査結果[1]が存在する. 当該問題に対して，CTI(Cyber Threat Intelligence)活用による最新脅威への追従が重要となっている. しかし，多くの CTI は自然言語で記述されており，検知へ活用するには適した形式への変換や活用方法の検討など専門家や時間が必要となる. そこで本稿では，CTI による機械的なログ分析システムを提案する. 本システムは，固有表現抽出により CTI から IOC を抽出し，IOC 同士の関係性グラフを構築することで，相関分析を機械的に実現する. 本稿では，提案システムの設計と実装を述べるとともに，CTI として 29 件の公開記事を用いた分析実験を実施し，CTI を駆動とするログ分析自動化の実現性を示す.

2. Introduction

近年，様々なデバイスやセンサーがインターネットを介して繋がる IoT 世界が本格的に到来し，物理世界とサイバー空間とが融合しつつある.その一方で，様々なシステムがインターネットに繋がっていることからサイバー攻撃の対象が拡大している. このようなサイバー攻撃に対抗するため，一般的な組織の IT システムにはアンチウイルス製品などの対策機器が導入されているが，すべての攻撃に対応できず，侵害に気が付かないことも多い.Domain tools 社の報告では，標的型攻撃の 42%が検知できずに見逃されているとの調査結果が示されている[1]. このように脅威の見逃しが表面化してきており，脅威に対応しきれていないことが問題となっている.従来のセキュリティ監視では，セキュリティ機器が検知してから対応を実施する受動的な対応が一般的であったが，上記問題のため，Threat Hunting などの能動的に侵害を検知することが重要となってきた. しかし，そのような能動的な対応を実施可能な人材は，高度な知見を有した専門家に限定されており，セキュリティ業界の専門家不足も重なり深刻な問題となっている.

3. インシデント対応

なぜ標的型攻撃に代表される高度な攻撃からの侵害を検知することが困難であるか. これは複数の要因が考えられるが，攻撃者も検知製品を活用して，自身の攻撃が検知されうるものなのか確認してから攻撃を仕掛けるなどの攻撃者の対策が高度化してきていることが大きい. そのためにセキュリティ製品は，最新の侵害情報を製品に反映させることで既知となった侵害情報への対応を実施している. しかし，そのような侵害情報は，常に更新され続けているかつ当該製品に対して発生した侵害のみ反映されるため，単一製品の侵害情報では限界がある. また，製品への反映にも時間がかかる場合があり，対応しきれていない. そこで近年重要視されてきているのが，検知機器に依存しない能動的なインシデント対応である[2]. 検知機器は侵害を検知できずとも，その端末の挙動情報をログとして大量に保有している. 当該ログから分析官が自身のノウハウを活用して侵害の痕跡を発見することで，見逃されていた脅威への対応を実現する.本稿では，SOC や CSIRT などのセキュリティ監視組織で従来実施されてきたインシデント対応をリアクティブ型インシデントレスポンスとし，分析官が能動的に実施する分析をプロアクティブ型インシデントレスポンスとした. Table.1 ではそれぞれの利点・欠点を示している.

従来型のセキュリティ監視サービスであるリアクティブ型インシデント対応では，アラートや問い合わせがなければ対応できないため検知見逃しが問題となっていた. それに対してプロアクティブ型インシデント対応では，分析官が能動的に監視対象のログなどを分析することで侵害の痕跡を発見し，対処を実施する. Table.1 に示す通り，種類ごとに利点・欠点が存在しており背反するものではなく併用することが望ましい.

リアクティブ型インシデントレスポンスとは，従来型のセキュリティ監視で実施されてきたインシデント対応である. 本対応は，セキュリティ機器の(1)アラート駆動や(2)顧客からの問い合わせなどを起因として運用員が対処を実施する. このような対応は，運用員に専門的な知見を必要としない一方で，侵害の検知が検知精度などに依存しているため依存先の機器や人物が見逃していた場合，システムへの侵害が継続してしまい重大な被害を及ぼしかねない.

プロアクティブ型インシデントレスポンスとは，分析官が能動的に監視対象のログなどを分析することで侵害の痕跡を発見し，対処を実施する.主に 2 つの分析方法が存在しており，(1)インテリジェンス駆動分析と(2)Threat Hunting などが存在する. 本研究では，プロアクティブ型インシデント対応の中でもインテリジェンス駆動分析を対象とした手法について検討を進めている.

Table 1 Incident Response Type

	Advanced Threat	Basic Threat coverage	Running Cost
Reactive IR	×	○	○
Proactive IR	◎	△	×

3.1 CTI (Cyber Threat Intelligence)

インテリジェンス駆動分析の分野において重要となるのが CTI である.CTI とはサイバー攻撃に関連するインテリジェンスのことを指す. CTI の定義は，厳密には存在しないが，

†株式会社日立製作所 Hitachi Ltd.

例えばガートナー社は「脅威・危険に対する主体者の対応の決定を支援する，既存または今後発生しうる資産への脅威に関する文脈，メカニズム，指標，含意および実行可能な助言を含むエビデンスベースの知識」としている[2]. この定義は，広範な意味を含んでおり，セキュリティ関係者であっても立場によっては必要となる情報が異なるため注意が必要である. ログ分析の運用現場では，主に Table.2 に示す#2,3 の情報として IoC(Indicator of Compromised)を活用した分析を実施する. しかし，ログ分析を組織的に実施している場合，実情としてマネジメント層が注目する#1 の情報を起因とした分析が必要となる場合も存在する.

Table 2 Cyber Threat Intelligence Type [3]

Intelligence Type	User	Cycle	Purpose
Strategic	Business Manager	Long Term	Business Risk
Operational	Manager	Middle Term	Risk Assessment System Design
Tactical	Analyst	Short Term	Threat Hunting IncidentResponse

3.2 脅威情報の分類

IoC とは，セキュリティが侵害された場合に残る痕跡を示す情報のことを指す. 攻撃者が対象のシステムを侵害した場合，特有の IoC を痕跡として残すことが多く，このような情報を共有することで自システムへの攻撃が発生する前から防御することが可能となる. IoC の種類は，様々であり，Sqrrl 社の研究員が提唱する Pain of Pyramid などのフレームが存在している[4]. 当該フレームは，IoC の差し替えの困難性を表現しており，例えば攻撃者は Hash や IP アドレスなどは対策が実施されても即座に別のものを活用することができるが，TTPs(攻撃手口)や攻撃に活用する Tools などは別の手段を講じることが困難であることを示している.

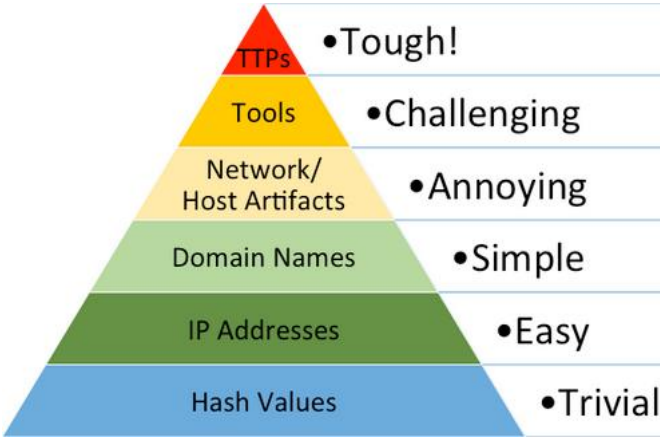

Figure 1 Pain of Pyramid [4]

3.3 インテリジェンス駆動分析の課題

Figure.2 では，CTI と IoC の関係性およびインテリジェンス駆動検知の技術課題を示している.前節で示した通り，CTI は様々な情報が存在しているが，ログ分析に活用できる情報は IoC などの一部にとどまる. しかし，従来はセキュリティ運用において，SOC や CSIRT などの現場が中心となり CTI を活用してきたが，昨今は経産省が「経営者向けのサイバーセキュリティガイドライン」[5]を発行するなど，セキュリティ運用のステークホルダーとして経営層も含まれる. そのため，運用現場に経営層などの技術よりではない意見も取り入れていくことが必要となってきている. 具体的には，ビジネス記事にサイバー攻撃に関連する情報が記載されていた場合，経営層が自組織に関連するか否かを運用現場に確認する. しかし，ビジネス記事にはログ分析に有用な情報が含まれていることは少ないため，経営層の意見を反映させることに多くの手間がかかる. Figure.2 では，この経営層と現場の間に発生するギャップを整理した. Figure.2 に示す通り，ビジネス記事の情報を基にログ分析まで実現するためには 4 つの課題が存在している.

(1). 課題 1:ビジネス記事と技術情報の乖離 (GAP 1)
ビジネス記事には，サイバー攻撃に関する概要は含まれているが IoC などの具体的な技術情報が含まれていない. そのため，技術情報に乖離があるためビジネス記事駆動の分析が困難となっている.

(2). 課題 2:記事同士の乖離 (GAP 2)
技術的な記事には，IoC などの具体的な情報が含まれている.しかし，技術的な情報を発信する媒体は統一されておらず，同じ内容を別々に発信していることも多い. その場合，情報が重複していることが記事を確認した後でなければ判断できないため，情報の整理が手間となっている. また，同一脅威について，ベンダー別に異なる分析情報も発信していることがあるが，別々の画面を見なければ当該脅威に関する広範な情報が手に入らない. 従来はこのような作業を人手で実施してきたため，すべての記事を確認しきることが困難であった.

(3). 課題 3:IoC 同士の乖離 (GAP 3)
脅威に関する技術記事(インテリジェンス)を駆動として，単純に分析を実施した場合，当該記事に含まれる IoC のみを分析対象とするため，本来関連するはずの IoC を用いた分析を実施しないことが多い.具体的には，とある記事から特定脅威に関する危険な URL 情報を取得した場合，その URL 情報のみを脅威が発生した期間だけ確認する. ここで別のブラックリスト情報から当該 URL と類似する情報が取得できていたとしても，起因となった記事のみを参照してブラックリストからの URL はその特定脅威が発生したと思われる期間の分析を実施せずに，単純にブロックリストに追加するだけで，痕跡を後から分析することを実施しないで見逃してしまうことが考えられる.

(4). 課題 4:IoC のログ分析への活用 (GAP4)
技術記事などの CTI から得られる情報は様々な種類が存在している.しかし，基本的なインテリジェンス駆動におけるログ分析では，IP アドレスや URL などの単純マッチングで分析可能な IoC を活用するのみであり，それ以外の CTI による分析手段は確立されているとは言い難い. 単純マッチング以外の分析手段は，分析官のノウハウとして明文化されておらず，同じ IoC を得たとしても分析官によって結果が異なる. 特に Figure.1 でしめした Pain of Pyramid の上位として存在する IoC ほど分析手段が確立

されておらず，ログ分析に活用することは高度な分析知見を有していなければ困難となる．

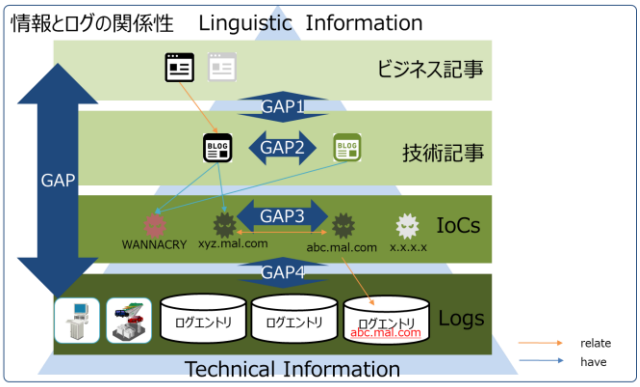

Figure 2 CTI Chain

3.4 関連研究

CTI を活用したログ分析の研究においていくつかの関連研究が存在する．まず，国際的な取り組みとして CTI 共有のため STIX(Structured Threat Information eXpression)による情報共有フレームの活用が推進されている．これは，国際的な標準化組織である OASIS(Organization for the Advancement of Structured Information Standards)および MITRE 社が推進する脅威情報共有の標準仕様である．サイバー攻撃への対応策を検討する上で，攻撃の情報を把握することは非常に有効である.その為，STIX ではサイバー攻撃に関する情報を標準的なフォーマットに共有することを目的として策定された[6].

伊藤らの研究では，ダイヤモンドモデルに基づく脅威のモデル化並びに分析システムの提案をしている．当該研究は，収集した脅威情報をダイヤモンドモデル化して一元管理することで検索の利便性を高めることを目的としているが，モデルの登録は手動で実施されている.[8]

藤井らの研究では，自然言語で記述された CTI を STIX 等の構造化フォーマットへの変換を図る技術の研究開発を実施している[7]．当該研究は，SOC 等でサイバーインテリジェンスの活用を効率化することを目的としている．当該技術は，情報収集機能，固有表現認識機能，関係性抽出機能などの複数機能から構成されている．

本研究では，上記研究の固有表現認識を活用して非構造記事からログ分析に活用可能な情報を抽出し，インテリジェンス駆動分析を実現する．

4. 提案方式

インテリジェンス駆動検知を実現するシステムを示す.まず，3.3 節で示した諸課題に対する要件を示し，要件を満たすシステムの全体像を示す． その次にシステムを構成する要素技術を説明する

4.1 機能要件

(1)． 要件 1：関係性の高い記事を紐づける

本要件は 3.3 節で示した GAP1(ビジネス記事と技術情報の乖離)に対する要件である．関係性の高い記事同士を紐づけることで，ビジネス記事を駆動として技術記事に含まれる IoC を参照することを可能ととし，記事駆動の分析を実現する．

(2)． 要件 2：記事単位ではなく事柄単位で集約

本要件は 3.3 節で示した GAP2(記事同士の乖離)に対する要件である．記事単位ではなく，収集した情報を特定脅威などの事柄単位で集約することで，当該脅威に関する IoC を網羅的に確認することが容易となる．これにより，従来人手で確認してきたインテリジェンスの確認コストが削減されるとともに，記事駆動での分析範囲が記事単体に収まらずに特定脅威全体に対する分析が可能となる．

(3)． 要件 3：類似する IoC を紐づける

本要件は 3.3 節で示した GAP3 (IoC 同士の乖離)に対する要件である.類似する IoC 同士を紐づけることで，記事内の IoC では一致することがなく関係性がないと判断されていたが，本来関係する IoC も分析範囲に含めることが可能となる．類似の具体例を説明する.例えば，特定脅威 A に関連する URL (a)と特定脅威 B に関連する URL (b)がまったく別々の記事から得られた場合，通常は脅威 A と URL (b)を関係ないものとして扱う．しかし，URL (a)と URL (b)がサブドメイン同士で類似性がある場合は，IoC 同士としての関係性が高い．このような場合に，脅威 A に関連する IoC として URL (b)も含めることで分析範囲を拡張できる．これは例えば，ブラックリストなどの特定脅威と紐づけが困難な情報との紐づけも可能とする．

(4)． 要件 4：IoC 種別とログ種別の組み合わせで分析方法を確立する

本要件は 3.3 節で示した GAP4(IoC のログ分析への活用)に対する要件である．課題 4 で示した通り，単純マッチングなどの分析方法は確立されているが，それ以外の分析方法は分析官のノウハウなどに依存しており，確立されていない．本要件を達成することで記事駆動分析において，分析精度の向上が見込める．

4.2 システム全体像

4.1 節で示した要件を満たすインテリジェンス駆動検知システムを提案する．本システムは，事前に登録した情報サイトに新規記事が投稿されることを起因として，途中で分析官の確認を挟むが，当該記事が分析官が監視するシステムに関係しているか機械的に判定することを可能とする．Figure.3 に示す通り，情報収集部と分析部から構成されており，さらに分析部は①脅威ナレッジ技術および②危険度判定技術から構成されている．以下に本システムの動作について示す．

(1). 登録した Web サイトに新規記事が投稿されると，RSS(Rich Site Summary)により RSS リーダーへ通知される．
(2). 通知を受けた RSS リーダーは,提案システムへ新規投稿について通知する．
(3). クローラ(Crawler)は，通知された記事に対して HTTP リクエストを送信し本文情報を取得する．
(4). 言語処理部(NLP Engine)は，取得した本文情報を解析して IoC 属性を抽出する．

(5). IoC 関連性判定部(IoC relation)は，抽出した IoC から関係性を判断して脅威ナレッジグラフを生成する. 脅威ナレッジグラフの例を Figure.4 に示す.
(6). 類似 IoC 判定部(Similar IoC)は，IoC 同士の類似性を判定して脅威ナレッジフラフへ追加する.
(7). ナレッジ可視画面(Knowledge WebUI)は，(6)までに生成された脅威ナレッジおよび脅威関連情報を WebUI 上で表示する.
(8). 突合分析クエリ生成部(Create SIEM Query)は，投稿された新規記事に関連する IoC 情報を脅威ナレッジから抽出し，SIEM で分析可能な形式に変換する.この時分析方法はルール DB から引用する.
(9). 分析手段表示部は(Output SIEM Query)は，分析官へ(8)で生成したクエリを表示する.
(10). 分析官は，(9)で取得したクエリを自身が利用可能な SIEM システムに入力し結果を受け取る.
(11). 分析官は，(10)で取得した結果を分析結果部(Input SIEM Result)に入力する.
(12). 突合スコア算出部(Scoring)は，(8)のルール別に登録されたスコアに基づき算出する.
(13). 相関分析部(Correlation)は，(11)および(12)の結果を集約し，(5)および(6)で今までに生成された脅威ナレッジとの相関性を比較する. 最終的に，監視対象のシステムに発生している可能性のある脅威を確度情報とともに結果として出力する.

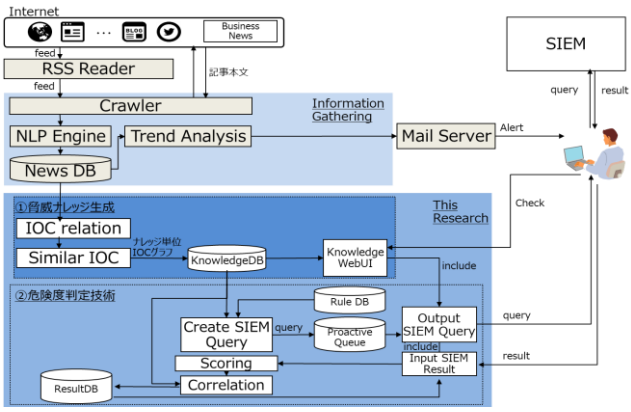

Figure 2 Proposed System

4.3 脅威ナレッジ生成

脅威ナレッジ生成技術は Figure.4 の左部のように収集してきた情報を記事単位ではなく，事柄単位に集約する. 収集した情報は，データソースが別々であるため同一の事柄を説明していても記述形式が統一されていない. しかし，文字情報として扱うことで，当該情報を自然言語処理(NLP)により IoC 情報およびその属性に変換することで，共通する IoC 同士で集約することを可能とした. 本技術は，Figure.3 に示す通り，(a)IoC 関係性判定部と(b)類似 IoC 判定部および(c)可視画面から構成されている. (a)は要件 1 および 2 に対応しており，(b)は要件 3 に対応している.また，(c)可視画面は 4.1 節で示した要件に該当しないが，ログ分析の運用現場との議論により脅威ナレッジ技術を単体で活用する需要が高いとの意見があったため採用した. この言語処理部は，関連研究として示した藤井らの研究と協力している.

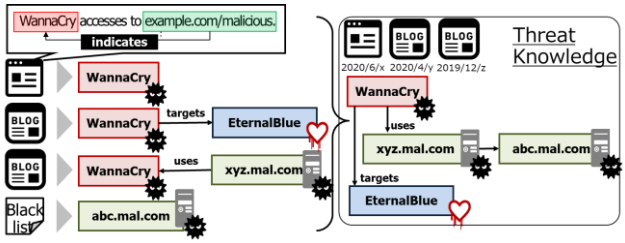

Figure 3 Threat Knowledge Technology

Figure. 5 Knowledge Web UI

4.4 危険度判定

危険度判定技術は，脅威ナレッジをログ分析に活用する技術である. セキュリティのインテリジェンスは分析に活用できるとされているが，その活用手段は分析官のノウハウに依存しがちである. そのため，本技術では，Figure.6 が左部で示す収集インテリジェンスの属性と右部が示す分析対象であるログ種別の組み合わせごとに分析方法を登録した DB を用意する. これにより，利用者は分析したい記事ならびにログを入力するだけで，あらかじめ登録されたルールに従って機械的に IoC を用いた分析が可能となる. 本報では，このような分析を突合分析とした. なお，SIEM システムとの連動がシステム的に困難であったため，本研究で開発したプロトシステムでは，Figure.3 に示す通り分析実行までを機械化しておらず，SIEM システム向けの分析クエリを出力する形式としている.

また，突合分析だけではログ内の IoC 痕跡の有無にとどまり，その結果が侵害に値するのかの判断が困難である.そのため，本技術では，突合分析結果を端末単位ならびに IoC 属性別に集約し，監視対象がどのログと関連性が高いのかを判定する機能も採用した. 当該機能を相関分析とした. これにより，監視対象システム内のどの端末が侵害されている可能性が高いのかをその侵害が確認された濃度でスコアリングし，さらに監視対象システム内でどのような脅威が広まっているのかを出力可能としている. 本機能は関連する記事数に基づいてスコアを算出する形式を採用している.

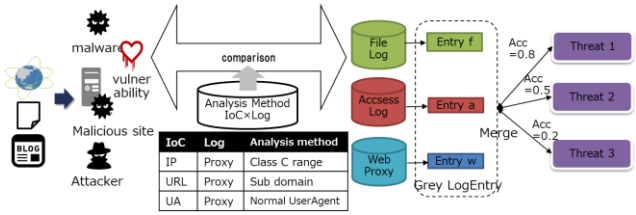

Figure 6 Log Assessment Technology

5. 実験

本章では，4 章で示したシステムが実現可能であるのか評価する．下記内容での評価実験を実施した．なお，本研究では実験に必要なログが調達できず，インテリジェンスからのクエリ生成にとどまっており，クエリを用いたログ分析の有効性評価は実施できていない．

5.1 実験

目的：一般的なニュース記事を起点としたログ分析クエリの出力の実現性を検証
評価概要： 公開情報をすべて検証することは困難なため，注目度の高いニュース記事に基づいた分析が可能か検証
対象記事：ニュースサイト[9]において指定期間にトップトピックスとして表示された記事であり，かつサイバー攻撃に関連する記事 (29 件)を対象．なお，同一事象を扱った記事は重複として一記事を除いて対象外とした．
期間：2020/08/20 – 2021/2/28

- 情報流出系：9 記事
- 大規模攻撃系：7 記事
- 不正アクセス系：5 記事
- 不審メール系：5 記事
- 危険サイト系：3 記事

5.2 結果および考察

```
db.runCommand({
    aggregate: "database_name",
    pipeline: [
        { $match : {$or: [{ "logtype": "AntiVirus" },
            { "logtype": "FireWall" } ]}},
        { $match : {$or: [{ "ip4": "80.158.3[.]161" },
            { "ip4": "80.158.51[.]209" },
            { "MD5": “2b7d83998b3a015c172fd684bbe356fbea1423d5” } ]}},
        { $group: { _id: "$srcip", count: { $sum : 1 } } },
        { $sort : { count : -1} },
        { $limit : 100}
    ],
    cursor: { }
})
```

Figure 7 Output Query

29 のニュース記事を本プロトシステムに入力した結果，55.2%である 16 の記事から分析可能なクエリを生成できた．クエリを生成することができなかった 13 記事を確認したところ，記事本文に分析に有益な情報及び他の IoC に紐づく情報が存在していない記事であることが確認できた．例えば，特定組織に関する情報流出を開設する記事であり，企業名や流出件数のみが記載され，公開情報からの分析が論理的に不可能な記事であった．これら 13 記事全てが，同様の理由によりそもそも分析の起点とすることが不可能であると確認できた．従って，人手であっても 29 記事中の 16 記事のみが分析の起点とすることが可能となり，本システムで 16 記事が機械的に分析クエリを生成できたことは，目標とした 100%の分析クエリ生成を達成したと評価した．なお，

本システムにより出力される分析クエリ例を Figure.7 に示す．本クエリをログが保管された SIEM などの分析基盤へ入力することで分析結果を取得できる．この分析結果をスコアリング機構に投入することで当該ニュースが監視対象のシステムに影響があるのか判断することが可能となる．しかし，本稿では前述した通りログを用いた実験を実施していない．

今後，研究に協力いただいている組織からログ提供を予定しているため，ログ分析ならびにスコアリング機能の実現性検証および性能評価を改めて侵害実施する予定である．

6. 結び

6.1 今後の課題

本評価実験では，分析クエリの生成を対象に実現性を評価した．しかし，分析クエリによりログ分析した侵害性の結果については評価できていない．そのため,スコアリングによる監視対象への影響都が評価できていない．今後，ログを活用した実験を実施する予定である．

また，当初の想定では当該技術をログが補完されている SIEM などと連動させることで新規記事投稿から危険度判定までの一連の流れをすべて機械的に処理することを検討していた．しかし，人間の判断が介在しないことおよび権限を与える点の影響からシステムを切り分けて構築した．これらの問題を改善することで一連の流れを機械化することを目指す．

6.2 まとめ

本研究では，脅威情報に基づく能動的なインシデント対応を実現するインテリジェンス駆動検知の課題検討，インテリジェンス駆動検知システム提案・実装，ならびにシステムの評価を実施した．提案システムでは，脅威ナレッジ生成機能および危険度判定技術によるインテリジェンスからログ分析までの一連の流れの機械化の手順を示した．実験では，一般的なニュースサイトから 29 の記事を収集し，そのうちの 16 記事から分析クエリを生成できることを示した．しかし，機能の検証に必要となるログの不足により実証が不十分な点が課題がとして残る．

謝辞

本研究は，関連研究として挙げさせていただいた藤井らの研究を活用する形で研究を推進されたものです.この場を借りて深くお礼申し上げます．

参考文献

[1] DomainTools, “2019 Threat Hunting Report”, < https://www.domaintools.com/content/2019-Threat-Hunting-Report.pdf> (2019).
[2] ガートナー社, “Threat Intelligence :What is it, and How Can it Protect ou from Today’s Adcanced Cyber-Attacks?”, < https://www.gartner.com/imagesrv/media-products/pdf/webroot/issue1_webroot.pdf >, (2014).
[3] 鎌田敬介，他,”サイバーセキュリティマネジメント入門”, KINZAI バリュー文庫(2017)
[4] David J Bianco, “The Pyramid of Pain”, < http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html/> (2013).
[5] 経済産業省,”サイバーセキュリティ経営ガイドライン Ver2.0” (2017)
[6] 藤井翔太, 川口信隆, “Cyber Threat Intelligence の構造化による分析支援手法の提案”, DPS, Vol.47 (2021).
[7] 伊藤大貴, 姓 名 2, “スレットインテリジェンスのためのダイアモンドモデルに基づく脅威 情報分析システム”, 電子情報通信学会論文誌,Vol J101-D, No.10 (2018).

[8] STIX， https://www.ipa.go.jp/security/vuln/STIX.html ， 姓 名, 姓 名, 姓 名, “文献のタイトル”, 論文誌名, Vol.n, No.n (2008).
[9] Yahoo! Japan News, https://news.yahoo.co.jp