ハニーポットで観測される新規エクスプロイトの分類手法の提案

九鬼 琉[1,a)]　佐々木 貴之[2,b)]　インミンパパ[2,c)]　吉岡 克成[2,3,d)]

概要：近年，年間に報告される脆弱性の件数は増加の一途を辿っており，全てに直ちに対応することは現実的に困難である．そのため脆弱性対応の必要性や優先度を見極めるトリアージが重要であり，その判断基準の一つとして脆弱性の悪用状況を速やかに把握することが重要である．本研究では，ハニーポット等で観測された膨大な通信リクエストから特に深刻度の高い脆弱性を狙う攻撃を抽出し，そのうち既知のルールにマッチしない新規の攻撃について攻撃リクエストの特徴（シグネチャ）をもとにエクスプロイトごとに分類しオペレータに通知することにより，新規悪用状況の迅速な把握を支援する手法を提案する．本手法により，8 ヶ月間の観測期間において 3 件のゼロデイ攻撃を含む 46 件の脆弱性を狙う新規の攻撃を検知した．また，一部の脆弱性については製品開発者への報告を行い，早期の修正および悪用状況の周知に貢献した．本手法を用いることで，脆弱性の新規悪用状況を迅速に把握し，脆弱性対応のトリアージ等に有効活用することができる．さらに，ゼロデイやその疑いがある未知の脆弱性を狙うエクスプロイトに対して分類結果を用いて独自の仮識別子を付与することにより，継続的な攻撃監視を始めとした詳細調査に役立てることができる．

キーワード：ハニーポット，攻撃分析，セキュリティ

Towards the Classification of Newly Exploits Observed by Honeypots

Ryu Kuki[1,a)]　Sasaki Takayuki[2,b)]　Yin Minn Pa Pa[2,c)]　Katsunari Yoshioka[2,3,d)]

Abstract: In recent years, the number of vulnerabilities reported per year has continued to increase, and it is difficult to respond to all of them immediately. Therefore, triage to determine the necessity and priority of vulnerability response is important, so it is essential to quickly detect the exploitation status of vulnerabilities, which is used as one of the criteria for triage. In this study, we propose a method to support the rapid identification of new abuse conditions by extracting attacks targeting vulnerabilities of particularly high severity from the large number of traffic observed by honeypots, etc., and classifying each exploit based on the characteristics (signatures) of the attack requests for new attacks that do not match known rules and notifying the operator. Using this method, we detected 46 new attacks targeting vulnerabilities, including 3 zero-day attacks, in 8 months of observation. And we reported on the exploitation of some vulnerabilities to the developers, and contributed towards the early remediation. This method is useful for quickly detecting new exploits of vulnerabilities and triaging vulnerability. Furthermore, by using the classification results to assign original, temporary identifiers to exploits targeting zero-day or suspected vulnerabilities, it is possible to use them for detailed investigations such as continuous attack monitoring.

Keywords: honeypot, attack analysis, security

[1] 横浜国立大学理工学部
College of Engineering Science, Yokohama National University
[2] 横浜国立大学先端科学高等研究院
Institute of Advanced Sciences, Yokohama National University
[3] 横浜国立大学大学院環境情報研究院
Faculty of Environment and Information Sciences, Yoko-

1. はじめに

近年，報告される脆弱性の数は増加の一途を辿っている．実際に，2023 年に National Vulnerability Database (NVD) に報告された CVE-ID の件数は 28,824 件に上り，2018 年の 16,509 件と比べると 5 年間で約 1.7 倍に増加している [1]．このような状況下において日々報告される脆弱性の全てに対応することは現実的に困難であることから脆弱性対応の必要性や優先度を見極めるトリアージが重要視されており，脆弱性そのものの深刻度や影響範囲だけでなく，その脆弱性を狙った攻撃が既に発生しているかといった脆弱性の悪用状況も重要な判断基準の一つとして考慮されている．

脆弱性の深刻度を定量的に評価するための指標として，共通脆弱性評価システム Common Vulnerability Scoring System (CVSS) [2], [3] や Stakeholder-Specific Vulnerability Categorization (SSVC) [4]，Exploit Prediction Scoring System (EPSS) [5], [6] などが提案されている．また，攻撃者による悪用が確認された既知の脆弱性のリストとして Known Exploited Vulnerabilities Catalog (KEV) が Cybersecurity and Infrastructure Security Agency (CISA) によって提供されており，2024 年 7 月時点で 1,140 件の脆弱性が登録されている [7]．しかし，KEV を始めとする既存の情報源は，実際の悪用状況を十分に網羅できていない，既に悪用が始まっている脆弱性の情報が迅速に反映されていない [8] などの問題が存在している．

本研究では，ハニーポット等で観測された膨大な通信リクエストからこれまでに観測されたことのない新規の攻撃を抽出し攻撃に利用されているエクスプロイトごとに分類することにより，オペレータによる新規悪用状況の迅速な把握を支援する手法を提案する．

提案手法では，ハニーポットで観測された攻撃リクエストの中から既知のルールにマッチしない未知の攻撃を抽出し，攻撃のリクエストパスとペイロードが含まれるパラメータ名の組を攻撃の特徴（シグネチャ）として攻撃に利用されているエクスプロイトごとに分類を行い，新規のクラスタとして分類された場合には Slack などのツールへ即時通知を行う．通知内容には攻撃リクエストの詳細情報や攻撃元ホスト情報，攻撃のタイムスタンプなどの情報が含まれ，通知を受けたオペレータはこの情報をもとに攻撃の対象となっている製品や脆弱性の調査を行う．攻撃の対象が公知の脆弱性である場合には，分類時に使用したシグネチャを用いて CVE-ID や対象製品情報のタグ付けを行うためのルールを作成することにより，悪用状況の把握や継続的な動向監視を行えるようにする．一方で攻撃の対象となっている脆弱性が公知でなく対象製品の特定も困難な場合には，当該クラスタに対して独自の仮識別子を付与してタグ付けルールを作成することで，未知のエクスプロイトに対しても攻撃動向の継続的な追跡を行うことができる．

本手法により，8 ヶ月間の観測期間において 3 件のゼロデイ攻撃を含む 46 件の脆弱性を狙う新規の攻撃を検知し，一部については関係機関等への報告を通じて脆弱性の早期修正及び悪用状況の周知に貢献した．

hama National University
a) kuki-ryu-dr@ynu.jp
b) sasaki-takayuki-yv@ynu.ac.jp
c) yinminn-papa-jp@ynu.ac.jp
d) yoshioka@ynu.ac.jp

2. 関連研究

ハニーポット: ハニーポットとは，脆弱な機器やサービスを模したホストを囮として設置し攻撃者を誘引することによりサイバー攻撃の観測や攻撃手法の収集を行うシステムである．ハニーポットの例として，IoTPOT [9], [10] のように実際の IoT デバイスをハニーポットとして利用するものや，IoT 機器のファームウェアの応答を事前に収集し学習する FirmPot [11]，インターネット上に公開されている機器やサービスの応答を模倣する X-POT [12] など，さまざまな種類のハニーポットが提案されている．

X-POT: X-POT は，インターネット上に公開されている機器やサービスの応答を収集し模倣するハニーポットであり，模倣する対象を拡張することにより多様な攻撃を観測することができる．

我々は X-POT のアーキテクチャを拡張し，ハニーポットで観測した攻撃と及び収集したマルウェア検体のマルウェア検体の動的解析を通じて得られた通信リクエストの双方に対して攻撃の対象製品や脆弱性情報をタグ付けすることにより，統合的な攻撃状況の収集及び分析を行えるようにした [13]．さらに，NVD や Exploit-DB などの公開脆弱性データベースを始めとしたインターネット上の公開脆弱性情報を基にハニーポット等で観測された攻撃の対象製品や脆弱性を自動的に推定し，攻撃ログへのタグ付けを行うためのルールを自動的に生成する手法を提案した [14]．

上述した X-POT の拡張アーキテクチャを用いて，2019 年 7 月から 2024 年 7 月までの約 5 年間に渡り計 21 インスタンスから構成されるハニーポット群の運用及び観測された攻撃の分析を行った．結果，累計で 2 億 6000 万件以上の通信リクエストを観測し，200 種類の脆弱性を狙う攻撃に対してタグ付けのためのルールを作成することができた．

攻撃検知: これまで，ハニーポットなどの攻撃観測網や不正侵入検知システム (IDS)，不正侵入防止システム (IPS)，Web Application Firewall(WAF) などで記録された通信リクエストを分析し攻撃を検知するため，シグネチャ (ルール) ベースや機械学習を用いた様々な攻撃検知のアプローチが取られてきた [15], [16], [17], [18], [19]．これら既存のアプローチの多くは通信リクエストの悪性判定や既知または類似の攻撃のクラスタリングを目的としているが，本研究はこれらのアプローチを通じて発見された未知

の攻撃について攻撃リクエストの特徴をもとに攻撃に利用されているエクスプロイトごとに分類することにより，新規エクスプロイトの悪用を効率的に把握するための手法を提案する．

3. 課題

脆弱性対応のトリアージを行うためには日々更新される脆弱性の悪用状況を迅速に把握する必要がある．CISA によって管理されている Known Exploited Vulnerabilities Catalog (KEV) は悪用が確認されている脆弱性の一覧を提供しているが，KEV は実際の悪用状況を十分に網羅できておらず，また悪用の開始から KEV 掲載までの間にタイムラグが存在する [8] という 2 つの問題を抱えている．

KEV の運用が始まった 2021 年 11 月 3 日以降，我々が運用しているハニーポットにおいて新たに悪用が確認された CVE-ID 採番済の脆弱性 147 件のうち，半数以上を占める 81 件は 2024 年 7 月現在も KEV に掲載されていない．この事実は，KEV が実際の脆弱性の悪用状況を十分に網羅できていないことを示している．

また，KEV に掲載された脆弱性であっても悪用の開始から KEV 掲載までに大幅なタイムラグが発生することがある．具体例として Apache Spark の WebUI における OS コマンドインジェクション脆弱性である CVE-2022-33891 の事例を示す．当該脆弱性は 2022 年 7 月 18 日 NVD に掲載され，そのわずか 2 日後にあたる 2022 年 7 月 20 日には我々が運用するハニーポットにおいて当該脆弱性を悪用した攻撃が観測されていた．一方，当該脆弱性が KEV に追加されたのは 2023 年 3 月 7 日であり，実際に悪用が開始してから KEV に掲載されるまで少なくとも 230 日以上の遅延が生じている．この事実は，KEV による悪用状況の迅速な提供機能が不十分であることを示している．

この一因として，ハニーポット等の攻撃観測網で観測される通信リクエストはその大半をスキャン通信や既知の脆弱性に対する攻撃リクエストが占めており，この膨大な観測ログの中から新規の脆弱性の悪用の発生を速やかに検知する必要があるという課題が存在する．そこで本研究では，ハニーポット等で観測した膨大な通信リクエストのうち特に深刻な脆弱性を狙った未知の攻撃について，攻撃リクエストの特徴（シグネチャ）をもとに攻撃に利用されているエクスプロイトごとに分類を行いその情報を通知することにより，オペレータによる新規の悪用状況の迅速な把握を支援する手法を提案する．

4. 提案手法

提案手法を用いてハニーポット等で観測した膨大な通信リクエストから脆弱性の新規悪用状況を効率的かつ速やかに把握するための攻撃分析のフローを図 1 に示す．以下では，提案手法の各工程におけるシステムの詳細及び運用手法について述べる．

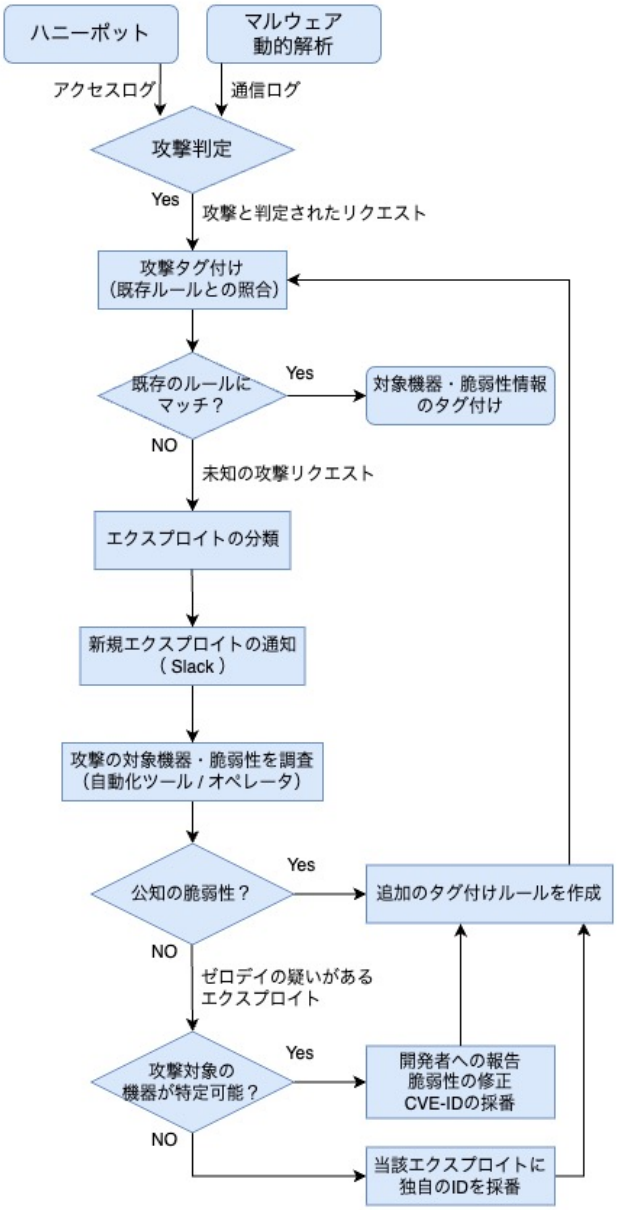

図 1 提案手法を用いた攻撃分析フロー

攻撃判定: ハニーポットにて観測した通信リクエスト及び収集したマルウェア検体の動的解析によって得られた通信リクエストは，その多くがスキャンなどの直接的な攻撃ではない通信で占められており，これら全てについて攻撃情報の分析やタグ付けを行うことは非効率である．そのため，最初にこれらの膨大なイベントの中から明らかに攻撃であると判断できるイベントのみを抽出し，以降の攻撃情報のタグ付けや分析の対象とする．現在は，コマンドインジェクションやリモートコード実行などの脆弱性を用いてマルウェア検体等をダウンロードする際に使用される wget や curl などのコマンドと検体 URL(以下，ペイロード) を含む通信リクエストを攻撃と判断している．この判定基準の拡張や攻撃判定手法の改善については今後の課題である．

攻撃タグ付け: 観測されたイベントのうち明らかに攻撃であると判断された通信リクエストについて，YAML 形式で定義されたタグ付けルールとの照合を行うことにより，攻撃の対象となっている脆弱性や製品に関する情報をイベントログに付与する．タグ付けルールの定義例を図 2 に示す．

```
- condition:
  - /goform/exeCommand
  - cmdinput=
  tag: CVE-2024-30891
  device_type: iot
  iot_type: router
  memo: https://github.com/Lantern-r/IoT-vuln/blob/
      main/Tenda/AC18/formexeCommand.md
```

図 2 タグ付けルールの定義例

condition には，HTTP リクエストのパスやパラメータ名などの特徴的な文字列を AND 条件で記載し，これらの文字列を全て含む通信リクエストに対して tag に記載された文字列を付与する．tag には原則として攻撃の対象となっている脆弱性の識別子 (CVE-ID など) を記載し，攻撃対象の脆弱性が特定できない場合には攻撃対象の製品名を，それも特定できない場合には独自に採番した仮識別子 (後述) を記載し，タグ付けに利用する．悪用状況の詳細な分析等に役立てるため，タグ付けルールには上記の情報に加えて攻撃対象製品の種別に関する情報 (device_type, iot_type) や脆弱性情報の出典 (memo) などの情報も合わせて記載する．既存のルールのいずれにもマッチしないと判定された攻撃イベントが発生した場合には，より詳細な分析を行うために次の手法を用いて攻撃に利用されているエクスプロイトごとに分類を行う．

エクスプロイトの分類: 既存のルールのいずれにもマッチしないと判定されたイベントについて，攻撃リクエストの特徴 (シグネチャ) をもとに攻撃に利用されているエクスプロイトごとに分類を行う．攻撃リクエストの特徴 (シグネチャ) としては，攻撃リクエストのパスとペイロードが含まれているパラメータ名の組を用いる．例えば図 3 の攻撃リクエストが観測された場合，シグネチャは攻撃リクエストのパスである「/goform/exeCommand」と，ペイロードが含まれているパラメータ名である「cmdinput」の組となる．なお，ペイロードが特定のパラメータ内に含まれていないような攻撃リクエストについてはリクエストパスのみをシグネチャとして用いる．このシグネチャを用いて攻撃リクエストをエクスプロイトごとに分類し，新規のエクスプロイトであると判定された場合には Slack などのツールを通じてオペレータに対し即時通知を行う．なおエクスプロイトの分類時に抽出したシグネチャについては，当該エクスプロイトに対応する新たなタグ付けルールを作成する際に condition 項目として流用することができる．

```
POST /goform/exeCommand?cmdinput=[payload] HTTP/1.1
Host: XX.XX.XX.XX:80
Accept-Encoding: identity
Cache-Control: no-cache, no-store, max-age=0
User-Agent: Hello World
```

図 3 CVE-2024-30891 を狙う攻撃リクエストの例

新規エクスプロイトの通知: エクスプロイトの分類結果をもとに新規のエクスプロイトであると判定された場合には，Slack などのツールを通じてオペレータに対して即時通知を行う．通知内容には，攻撃リクエストの情報 (リクエストパス，宛先ポート，攻撃ペイロードなど)，攻撃元ホスト情報，攻撃観測日時 (タイムスタンプ) など，後述する攻撃対象の特定や脆弱性の調査に必要な情報を記載する．

攻撃対象の特定: 通知を受けたオペレータは，通知内容をもとに攻撃の対象となっている製品や脆弱性の調査を行う．具体的には，NVD や Exploit-DB などの公開脆弱性情報を参照して攻撃の対象となっている脆弱性を自動で推定するツール [14] による調査及び人手によるインターネット上の公開情報の調査を行い，攻撃の対象となっている脆弱性や製品の特定を試みる．調査により攻撃の対象となっている脆弱性が特定できた，すなわち攻撃が公知の脆弱性を狙った攻撃であった場合には，攻撃分類時に抽出したシグネチャと調査結果を用いて追加のタグ付けルールを作成し，悪用状況の把握や継続的な動向監視を行えるようにする．

攻撃の対象脆弱性が特定できず攻撃の対象となっている製品またはベンダーのみが特定できた場合には，当該製品に存在するゼロデイまたは開示されていない脆弱性を狙った攻撃である可能性が高いことから，製品開発者や関係機関等に対して悪用状況の共有を行い，脆弱性の修正が行われ CVE-ID が採番された際に改めてタグ付けルールを作成する．

攻撃の対象となっている脆弱性及び製品のいずれも特定できない場合には，当該エクスプロイトに対して独自の仮識別子を付与し前述のシグネチャを用いてタグ付けルールを作成する．これにより，攻撃対象が不明な未知のエクスプロイトに対しても攻撃動向の継続的な追跡や把握を行うことができる．仮識別子は「unknown-YYMMDD[-NN]」の形式で付与され，YYMMDD は攻撃の初観測日時，[-NN] は同日に複数の未知のエクスプロイトの悪用が観測された場合に付与する連番を表す．

5. 実験結果

5.1 実験結果概要

提案手法における攻撃分類及び新規エクスプロイト検知の有効性を評価するため，ハニーポットで観測された通信

リクエストに対して提案手法を適用し，攻撃リクエストの分類及び新規エクスプロイトの検知実験を行った．検知の対象は，2023 年 9 月 1 日から 2024 年 4 月 30 日までの 8 ヶ月間において我々が運用しているハニーポット群において観測された通信リクエストとし，攻撃リクエストの分類及び新規エクスプロイトの検知にあたってはハニーポットの運用を開始した 2019 年 7 月 21 日以降に観測された全通信リクエストを利用した．実験結果の概要を以下に示す．

- 実験期間: 2023-09-01 〜 2024-04-30
- 設置ハニーポット数: 21 インスタンス
- リクエストセッション数: 33,407,088 件
- 攻撃と判定されたセッション数: 241,972 件
- 新規エクスプロイト検知数: 58 種類
  - 新たに悪用が確認された脆弱性件数: 46 種類
  - ゼロデイ脆弱性件数: 3 種類

実験期間中にハニーポットで観測された通信リクエストは合計で 33,407,088 件であり，そのうち明らかに攻撃であると判定されたセッション数は全体の 0.72%にあたる 241,972 件であった．これらのうち既存のタグ付けルールにマッチしない攻撃リクエストについて提案手法を適用しエクスプロイトごとに分類を行った結果，58 種類の新規エクスプロイトを検知することができた．このうちハニーポットでこれまでに観測されたことのない脆弱性を狙った攻撃が 46 種類，ゼロデイ脆弱性を狙った攻撃が 3 種類含まれていた．ゼロデイ脆弱性を狙った攻撃のうち 1 件については攻撃の対象機器を特定することができたため，JPCERT/CC を通じて製品開発者に報告を行い，脆弱性の早期修正に貢献した．この事例については 5.3.1 で詳細を述べる．

5.2 攻撃分類の粒度

提案手法では，既存のルールのいずれにもマッチしないと判定された攻撃リクエストについて，攻撃に利用されているエクスプロイトごとに分類を行う．エクスプロイトの分類には攻撃リクエストの特徴 (シグネチャ) を用いるが，その条件の厳密さによって新規エクスプロイト検知の感度が変化する．以下では，攻撃リクエストの特徴として用いるシグネチャとして以下の 3 種類の粒度を用いて実験期間中に観測された新規攻撃リクエストに対してエクスプロイトの分類を行い，攻撃分類の粒度を変化させたときに新規エクスプロイト検知の感度がどのように変化するかを調査した．

実験に用いた攻撃分類の粒度

(a) リクエストパスの一致
(b) リクエストパス+ペイロードを含むパラメータ名の組の一致
(c) リクエストパス+全パラメータ名の組の一致

表 1 は，実験期間中に観測された新規攻撃リクエストについて (a), (b), (c) の 3 種類の粒度を条件として用いてエクスプロイトの分類を行った結果を示している．表中では各条件によって新規エクスプロイトとして検知されたイベントについて，オペレータが攻撃の対象となっている脆弱性を調査しそのステータスを評価している．具体的には，当該イベントが我々のハニーポットで観測された当該脆弱性 (CVE-ID) を狙った初めての攻撃であった場合は当該脆弱性の開示状況に応じて「ゼロデイ」「未知」「公知」のいずれかとして評価し，既に同一の脆弱性を狙う実装が異なるエクスプロイトによる攻撃が観測されていた場合には「既に観測済」と評価している．

表 1 攻撃分類の粒度ごとの検知件数の推移

分類粒度	#ゼロデイ	#未知	#公知	#既に観測済
(a)	3	4	37	2
(b)	3	5	38	12
(c)	3	5	39	24

分類粒度 (a) の条件では，攻撃のリクエストパスの一致のみを攻撃分類の基準としている．そのため同一のリクエストパスを持つ異なる機器や脆弱性に対する攻撃を区別することができず，新規の脆弱性に対する攻撃を見逃してしまう事例が複数存在していた．具体例として，図 4, 5 に CVE-2020-28188 及び CVE-2021-45836 を狙う攻撃リクエストの例を示す．これらはいずれも TerraMaster TOS に存在するリモートコマンド実行の脆弱性であり，リクエストパス (/tos/index.php) は同じであるものの，それに続くクエリ (explorer/pathList, app/hand_app) およびパラメータ名 (path, name) は異なっており，それぞれに固有の CVE-ID が採番されている．しかし，分類粒度 (a) の条件ではこれらが同一の脆弱性として分類されてしまうことから，本事例と同様に新規や未知の脆弱性に対する攻撃を見逃してしまう可能性がある．

分類粒度 (b) の条件では，粒度 (a) の条件を改善し，リクエストパスに加えてペイロードを含むパラメータ名の 2 項目を組として攻撃の分類の基準としている．これにより，前述の図 4, 5 のような事例においてもリクエストパスとペイロードを含むパラメータ名の組 ([/tos/index.php, path],[/tos/index.php, name]) が完全に一致しない脆弱性であれば両者に対する攻撃を区別することができ，結果として適切な粒度で分類することができる．さらに，図 6 のように一つの脆弱性にペイロードを含めることができるパラメータが複数存在するような事例についても．これらををエクスプロイトの実装ごとに分類することができるため，既存のタグ付けルールでカバーできない新たな実装のエクスプロイトが観測された際にもそれを検知し，ルールのアップデートに活用することができる．

分類粒度 (c) の条件では，攻撃のリクエストパスと全てのパラメータ名の組を基準として攻撃分類を行う．これに

よりエクスプロイトの実装の僅かな差異まで検出する極めて厳密な分類が可能である．しかし，攻撃に直接影響しない任意のパラメータの有無なども分類結果に影響を与えてしまうため，既知のものと実質的に同一のエクスプロイトが誤って新規のエクスプロイトとして分類され多数オペレータに通知されてしまう可能性があり，結果として運用の効率性が低下してしまうことが懸念される．

これらの結果から，提案手法では攻撃の分類を行うシグネチャの粒度を変化させることで新規エクスプロイト検知の感度を調節できることが示された．本研究では新規脆弱性に対する攻撃の見逃しのリスクを軽減しつつオペレータによる運用の効率性を保つために，分類粒度 (b) を採用し観測された攻撃の分析に利用した．

```
GET /tos/index.php?explorer/pathList&path=[payload]
    HTTP/1.1
Connection: close
```

図 4 CVE-2020-28188 を狙う攻撃リクエストの例

```
GET /tos/index.php?app/hand_app&name=[payload] HTTP
    /1.1
Host: XX.XX.XX.XX:8080
User-Agent: python-requests/2.31.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

図 5 CVE-2021-45836 を狙う攻撃リクエストの例

```
POST /boafrm/formNtp HTTP/1.1
Host: XX.XX.XX.XX
User-Agent: Go-http-client/1.1
Content-Length: 281
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

timeZone=3+2&enabled=ON&ntpServerIp1=XX.XX.ntp.org&
    ntpServerId=1&ntpServerIp2=[payload]&submit-url
    =%2Fntp.htm&save_apply=Salvar+%26+Aplicar
```

図 6 CVE-2018-13307 を狙う攻撃リクエストの例

5.3 観測した攻撃の早期検知事例

5.3.1 ゼロデイ攻撃の検知・報告事例

提案手法を用いた攻撃分析を通じてゼロデイ脆弱性を狙った攻撃を早期に検知し，製品開発者に対する報告に繋げることができた事例を示す．

図 7 は，FXC 株式会社が 2014 年に発売したコンセント壁埋込型無線 LAN アクセスポイント AE1021/AE1021PE に存在する OS コマンドインジェクションの脆弱性を狙う攻撃リクエストの観測件数の推移を示している．当該脆弱性を狙う攻撃は 2023 年 10 月 29 日に我々のハニーポットにおいて初めて観測され，提案手法を用いた攻撃分析の結果，新規エクスプロイトであると判定された．さらに，攻撃リクエストの特徴がインターネット上で公開されている既知の脆弱性情報やエクスプロイトコードのいずれとも一致しなかったことから，当該攻撃がゼロデイ脆弱性を狙ったものである可能性が高いと判断し，攻撃対象機器の特定を試みた．観測された攻撃リクエスト及びペイロードに含まれていたマルウェア検体について詳しく調査を行ったところ，機器名とみられる文字列（ae1021pe）が含まれていたことから攻撃対象機器の特定に至り，同月 31 日に JPCERT/CC を通じて製品開発者に対してゼロデイの疑いがある攻撃の観測状況および観測された攻撃リクエスト等の分析結果について報告を行った．その後製品開発者から当該脆弱性の確認及び修正に向けた調査を行う旨の返答があり，2023 年 12 月 6 日には当該脆弱性を修正したファームウェアが公開された [20].

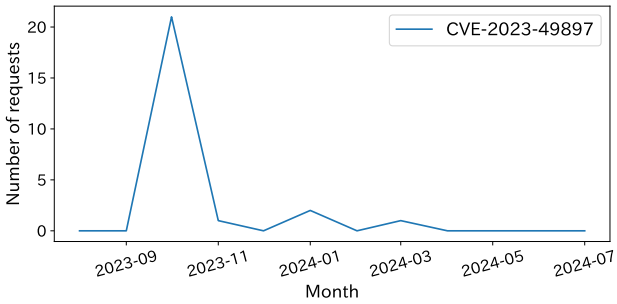

図 7 CVE-2023-49897 を狙う攻撃リクエストの観測件数の推移

当該脆弱性を狙った攻撃リクエストは脆弱性の修正後も数カ月間に渡って散発的に観測されていたものの，その後沈静化し，2024 年 7 月現在においては観測されていない．当該脆弱性は CVE-2023-49897 として採番され，脆弱性の深刻度を評価する共通脆弱性システム CVSSv3.0 の Base Score は 8.0(High) と評価されている [21].

5.3.2 太陽光発電施設の遠隔監視機器を狙う攻撃

2024 年 5 月，日本国内の太陽光発電施設の遠隔監視機器がサイバー攻撃を受け，インターネットバンキングにおける不正送金に悪用されるなどの被害が発生していたことが報じられた [22].

我々のハニーポットは同製品を狙っているとみられる攻撃リクエストを 2022 年頃から観測してきた．図 8 は，株式会社コンテックが販売する太陽光発電の計測・遠隔監視システム SolarView Compact に存在する 3 件の脆弱性 (CVE-2022-29303，CVE-2022-31373，CVE-2023-23333) を狙う攻撃リクエストの観測件数の推移を示している．これらの当該脆弱性を狙う攻撃リクエストは 2022 年 7 月ごろから

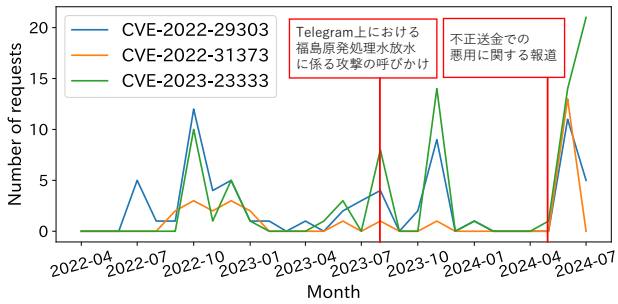

図 8 太陽光発電施設の遠隔監視機器に存在する脆弱性を狙う攻撃リクエストの観測件数の推移

図 9 脆弱性の悪用方法を共有する Telegram 上の投稿

2024 年 7 月現在に至るまで継続的に観測されており，我々はこれまで複数回に渡り，当該機器の悪用状況について関係機関への情報提供を行ってきた．

また，Telegram 等の SNS コミュニティ上において当該機器への攻撃を呼びかける投稿なども確認されており，これらの投稿と攻撃についての関連も疑われる．図 9 は，2023 年 8 月に福島原子力発電所の処理水の海洋放出に反対する攻撃者グループによって Telegram 上に投稿された，当該脆弱性を狙った攻撃を行うための PoC や広域スキャンシステムで当該機器を探索するための検索クエリなどの具体的な攻撃手法を共有するメッセージである．本投稿と同時期に我々のハニーポットにおいても攻撃観測件数が増加しており (図 8)，加えて観測された攻撃リクエストの特徴が Telegram 上で共有された攻撃手法と類似していることが確認できた．このことから，ハニーポット等を利用した直接的な攻撃観測によって得られた情報に加えてインターネット上の公開情報や攻撃者の活動観測 (OSINT/HUMINT) を通じて得られたインテリジェンスを融合することにより，昨今の多様化する脅威に対してより多角的な分析及び効果的な対策に繋げることができると考えられる．本事例の詳細および攻撃観測網と OSINT/HUMINT の融合から得られる知見の活用については論文 [23] で述べる．

6. 考察

6.1 課題

攻撃対象機器の特定: 提案手法を用いて新規エクスプロイトとして検知され，その攻撃リクエストの特徴が公知の脆弱性と一致しない場合にはゼロデイ脆弱性を狙った攻撃である可能性が疑われる．このような未知の脆弱性の悪用については，悪用の対象となっている機器を速やかに特定し製品開発者に対して報告を行うことが重要であるが，攻撃リクエストやペイロードに攻撃対象機器を特定するための手がかりとなる情報が含まれていない場合に攻撃対象機器の特定が困難であるという問題が存在する．実際に提案手法を用いた実験を通じてゼロデイの疑いがある未知の攻撃リクエストが複数検知されているが，そのうち攻撃対象機器を特定し製品開発者への報告にまで至った事例は限られている．そのため，未知のエクスプロイトが観測された際にその攻撃対象機器を特定するための追加の調査手法の検討が必要である．具体的には，製品のマニュアルやファームウェア等の解析を行い攻撃対象機器の特定に繋げるなどの方法が考えられる．

新規悪用状況の共有: KEV を始めとした脆弱性の悪用状況に関する既存の情報源が実際の悪用状況を十分に網羅できていない要因として，ハニーポット等で観測される膨大な通信リクエストの中から新規の脆弱性の悪用状況を特定することが困難であることに加えて，各組織が新規の悪用状況を検知した際にその事実を十分に共有・周知できていないことが挙げられる．そのため，各組織が新規の悪用状況を把握した際に当該脆弱性が既知/未知であるかによらずその悪用状況を速やかに中央機関等に報告すること，また中央機関はそれらの情報を集約し開発者やユーザー，その他の関係者に対して適切な形で情報を提供することで悪用状況の迅速な周知に努めることが重要である．

攻撃判定の改良: 提案手法においては，ハニーポットで観測された膨大な通信リクエストからスキャン通信などを除外し明らかに攻撃であるとみなせるリクエストのみを対象として攻撃分類を行っているが，この攻撃判定の網羅範囲の改良が課題である．現時点では wget や curl などのマルウェアをダウンロードするためのコマンドがリクエストに含まれている場合に攻撃と判定しているが，本判定手法で検知可能な攻撃は OS コマンドインジェクション等のリモートコード実行を狙う攻撃に限られる．より広範な攻撃手法に対する迅速な検知を可能にするためには，様々な種類の脆弱性を狙う攻撃リクエストの特徴をより詳細に分析し，攻撃判定の条件を拡張することが必要である．

6.2 研究倫理

運用中のハニーポットが攻撃者によって悪用されることを防ぐため，ハニーポットから外部 (インターネット) に対

するアウトバウンド通信は遮断している．

また観測した攻撃の分析を通じて得られた情報の取り扱いには十分注意し，特にゼロデイ及びその疑いがある未知の脆弱性の悪用に関する情報については脆弱性の修正及び開示前に当該情報が第三者に漏洩することがないよう秘密保持に努めた．さらに，ゼロデイ脆弱性の疑いがある製品が特定できた場合には JPCERT/CC を通じて速やかに報告を行い，開発者が脆弱性の検証および対策を行うために必要な情報の提供を行った．

7. 結論

本研究では，ハニーポットで観測される膨大な通信リクエストから新規の脆弱性を狙う攻撃を抽出し，攻撃リクエストの特徴（シグネチャ）をもとにエクスプロイトごとに分類することで新規の悪用状況を迅速な把握を支援する手法を提案した．さらに，提案手法を用いて実際のハニーポットの観測ログから 3 件のゼロデイ攻撃を含む 46 件の脆弱性を狙う新規の攻撃を検知し，一部は関係機関等への報告を通じて脆弱性の早期修正および悪用状況の周知に貢献した．今後は，攻撃判定部などの改善や新規悪用状況の監視及び迅速な周知に向けて継続的に取り組んでいく予定である．

謝辞 本研究は，国立研究開発法人情報通信研究機構 (NICT) の委託研究（JPJ012368C05201, JPJ012368C08101）により得られた成果を含む．提案手法により検知されたゼロデイ脆弱性の報告および修正にあたりご対応いただいた製品開発者および JPCERT/CC ほか各関係者の皆様に感謝する．

参考文献

[1] NVD: Statistics Vulnerability Database - CVE, https://nvd.nist.gov/vuln/search.
[2] NVD: Vulnerability Metrics, https://nvd.nist.gov/vuln-metrics/cvss.
[3] 独立行政法人情報処理推進機構：共通脆弱性評価システム CVSS 概説, https://www.ipa.go.jp/security/vuln/scap/cvss.html.
[4] CISA: Stakeholder-Specific Vulnerability Categorization (SSVC), https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc.
[5] Jacobs, J., Romanosky, S., Edwards, B., Adjerid, I. and Roytman, M.: Exploit Prediction Scoring System (EPSS), *Digital Threats*, Vol. 2, No. 3 (2021).
[6] Jacobs, J., Romanosky, S., Suciu, O., Edwards, B. and Sarabi, A.: Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights, *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (2023).
[7] Cybersecurity and Agency, I. S.: Known Exploited Vulnerabilities Catalog, https://www.cisa.gov/known-exploited-vulnerabilities-catalog.
[8] Informa PLC: Exploited Vulnerabilities Can Take Months to Make KEV List, https://www.darkreading.com/vulnerabilities-threats/exploited-vulnerabilities-can-take-months-to-make-kev-list.
[9] Yin Minn Pa Pa, Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T. and Rossow, C.: IoTPOT: Analysing the Rise of IoT Compromises, *9th USENIX Workshop on Offensive Technologies (WOOT 15)* (2015).
[10] Yin Minn Pa Pa, Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T. and Rossow, C.: IoTPOT: A Novel Honeypot for Revealing Current IoT Threats, *Journal of Information Processing*, Vol. 24, No. 3, pp. 522–533 (2016).
[11] Yamamoto, M., Kakei, S. and Saito, S.: FirmPot: A Framework for Intelligent-Interaction Honeypots Using Firmware of IoT Devices, *2021 Ninth International Symposium on Computing and Networking Workshops (CANDARW)*, pp. 405–411 (2021).
[12] Kato, S., Tanabe, R., Yoshioka, K. and Matsumoto, T.: Adaptive Observation of Emerging Cyber Attacks targeting Various IoT Devices, *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)* (2021).
[13] 佐々木貴之, 九鬼琉, 植田岳洋, 鮫嶋海地, Guo Binnan, 市川詩恩, 山口陽平, 岡田晃市郎, 吉岡克成, 松本勉：ハニーポットによる攻撃観測と多角的分析のための統合アーキテクチャの提案，情報処理学会コンピュータセキュリティ研究会 (2022).
[14] 九鬼琉, 植田岳洋, 佐々木貴之, 吉岡克成, 松本勉：ハニーポットで観測されたサイバー攻撃の対象機器及び脆弱性の自動推定手法の提案，情報処理学会コンピュータセキュリティ研究会 (2022).
[15] Guo, Y.: A review of Machine Learning-based zero-day attack detection: Challenges and future directions, *Computer communications*, Vol. 198 (2022).
[16] Baykara, M. and Firat, R. D.: A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems, *International Journal of Computer Networks And Applications (IJCNA), EverScience Publications* (2015).
[17] Patel, R. R. and Thaker, C. S.: Zero-Day Attack Signatures Detection Using Honeypot, *International Conference on Computer Communication and Networks CSI-COMNET-2011* (2012).
[18] Musca, C., Mirica, E. and Deaconescu, R. A.: Detecting and Analyzing Zero-Day Attacks Using Honeypots, *2013 19th International Conference on Control Systems and Computer Science*, pp. 543–548 (2013).
[19] Garcia-Teodoro, P., Diaz-Verdejo, J., Tapiador, J. and Salazar-Hernandez, R.: Automatic generation of HTTP intrusion signatures by selective identification of anomalies, *Computers & Security*, Vol. 55, pp. 159–174 (2015).
[20] FXC 株式会社：AE1021/AE1021PE のファームウェア 2.0.10 公開のお知らせ，https://www.fxc.jp/news/20231206.
[21] JPCERT/CC and IPA: JVNVU#92152057 FXC 製無線 LAN ルータ「AE1021PE」および「AE1021」における OS コマンドインジェクションの脆弱性，https://jvn.jp/vu/JVNVU92152057/.
[22] 産経新聞：太陽光発電にサイバー攻撃 機器８００台を乗っ取り 身元隠し不正送金に悪用 ，https://www.sankei.com/article/20240501-ZSOLVFVJZZL6BLQJR6S6SJ23GM/.
[23] 吉岡克成, 金子翔威, 青山航大, 九鬼琉, Yin Minn Pa Pa, 佐々木貴之, 田辺瑠偉：INSITE: 攻撃観測網と OSINT/HUMINT の融合によるサイバーセキュリティ情報収集・分析・対策機構，情報処理学会コンピュータセキュリティ研究会 (2024).