2ZB-02

ネットワークログと社会情勢を活用したサイバー攻撃の動向調査

前田 龍司† 川端 純弥† 平原 蒼生† 守屋 海斗† 塩崎 雅基†
阿部 祐輔‡ 永田 正樹‡

静岡産業技術専門学校 みらい情報科† 静岡大学 情報基盤センター‡

1. はじめに

昨今，インターネットにアクセスする人の増加に伴い，サイバー攻撃の被害が増加している[1]．また，深刻なサイバー攻撃は往々に発生前の段階として予兆となる深刻ではない通信を発する[2]．その為，各機関に所属するセキュリティ対策チームはネットワーク機器のログを細部まで見て分析し，動向を掴むことで早期対応をしなければならない．しかし，サイバー攻撃の増加・巧妙化に伴いセキュリティ機器から発生するアラートも増加している為，深刻なアラートのみの対処に留まり細部まで把握する事が困難な現状にある[2]． そこで本研究では，市井の社会情勢が組織内ネットワークの UTM 機器の通信内容にどのような変化をもたらすかについて，両者の関係性を分析する．これらの関係性分析を実施するために，サイバー攻撃の動向と関連する社会情勢の情報収集手法及び，ネットワークログデータの分析手法を検討する．

2. 先行研究

サイバー攻撃と社会情勢とするに関連する研究の 1 例に，プレッシャーによるサイバー攻撃兆候検知[3]がある．これは，2010 年に発生したイランの核施設へのサイバー攻撃と攻撃の動機に繋がる外部から与えられるストレスの関係性を立証する試みである．ストレスの増加機会は軍事攻撃活動や脆弱性の公表などの社会情勢に関わる事象も存在しており，社会情勢とサイバー攻撃に関係性が存在する事も示している．当研究では市井の社会情勢ニュースの統計やネットワークログデータといったより粒度の細かい情報の分析は実施されていない．本研究ではこの点に着目し，具体的な社会情勢とサイバー攻撃の関係性を得ることができれば，ログとは別の角度から詳細な攻撃動向の予測を立てることができると考えた．これら背景から本研究は，社会情勢とネットワークログデータの関係性に焦点を当てることにした．

Predicting the frequency of Cyber Attacks by combining Network logs with socio-political landscape
†Maeda Ryuji, Kawabata Junya, Hirahara Sou, Moriya Kaito, Shiozaki Masaki, Shizuoka Professional Training College of I.T.
‡Abe Yusuke, Nagata Masaki, Shizuoka University CII.

3. 社会情勢とネットワークログデータの関係

社会情勢とネットワークログから関係性を考察し，サイバー攻撃判断の為に利用できるデータの提示を行うことを目標とする．ネットワークログデータは，筆者らが所属する教育機関の情報基盤で採用している UTM のログデータを用いる．社会情勢は，Web 上の各種ニュースをスクレイピングにて情報を収集し，テキスト化したデータとする．表 1 は用いたログデータの概要である．UTM ログは多種多様な情報を扱うため，本研究では必要情報のみ抜粋して用いている．表 1 のログデータと社会情勢データを可視化および分析し，両者の関係性を考察する．

表 1 UTM ログデータ概要

ファイル数	8
記録日時	2022/08/28- 2022/09/03 2022/12/02
カラム数	120カラム
データ容量	約50GB (1ファイル)
行数	約9000万行 (1ファイル)
記録日数	1日分 × 8データ

3.1 可視化・分析

ログデータおよび社会情勢の可視化・分析をし，社会情勢と機関内ネットワークの通信それぞれを時系列に揃えて，動向や特徴を調査する．ログデータ解析は，多数出力される UTM ログデータの各カラムの内，特に有用そうな十数カラムを選定し集計・可視化・分析を行う．カラムの抽出及び可視化は pyspark ライブラリを用いて，分析・可視化したい対象を指定した後，matplotlib ライブラリの pyplot モジュールで円グラフによる対象の全体比の可視化と，積み上げ棒グラフによる時系列データの可視化による通信動向の推移調査を行う．社会情勢データは様々なニュースサイトからネットワークログ取得期間周辺のニュースを調べることで，ログ取得期間中の社会情勢を探っていく．具体的手法は，ニュースサイトから WayBackMachine とスクレイピング用のライブラリである BeautifulSoup, Requeats を利用して指定した期間中の全てのニュースの”日付”,”タイトル”, ”カテゴリ”

Copyright ©2024 Information Processing Society of Japan.
All Rights Reserved.

を 1 日単位で出力するプログラムを作成し，それらをワード指定により抽出して集計する．

3.2 関係性の考察

分析して得られた社会情勢およびネットワークログデータから得られた機関内通信の特徴・動向を照らし合わせることで互いの関係性を考察し，活用法を探る．

4. 分析結果

4.1 2つの通信タイプ

UTM ログデータには通常通信の TRAFFIC と危険通信の THREAT の 2 つの通信タイプが存在する．TRAFFIC は表 2 に示す通り end（許可），deny（拒否）の他，ルールに当てはまらない drop が存在する．drop に分類された場合，表 2 赤字で示す通りサイバー攻撃を連想される情報も含まれていることから危険通信の可能性もあるが，通信量が膨大であることから，本研究ではより危険度が高い THREAT 通信の分析を対象とする．

表 2 タイプ TRAFFIC の出力内容

出力	内容
end	許可ルールに伴い正常終了した
deny	拒否ルールに該当する為破棄された
drop	• 無関係な通信なので破棄した • 22,23,80番といったサイバー攻撃に利用されるポートを宛先としている

4.2 THREAT の主な送信元の国と危険通信

THREAT の主な送信元の国は 8/28～9/03 の期間ではイランのログ件数が継続的かつ多量に見られた（図 1(a)）．特に多いのはメールの認証プロトコルへの攻撃等のメールに関係する攻撃であった．また，イランとの密接な関係とされるロシアから脅威レベル medium 以上の通信件数が若干の増加傾向にあった．図 1(b)で示す Failed Authentication Trough Mail Protocol は SMTP-AUTH による認証プロトコルの認証失敗を差し，正規のユーザ以外からのアクセスによるメッセージである．MAIL: User Login Brute Force Attempt は，短期間に大量のユーザ認証及びログイン試行を行った場合のメッセージである．

4.3 社会情勢

表 3 から 8/22～8/28 にウクライナ・イラン情勢が不安定になる事象が複数起きていた．また，8/22 においてウクライナ・ロシアを含むニュースの件数が他の日時と比べて多いという統計結果が出ている．表 3 の事象と図 1 の THREAT 件数の増加には何かしらの関係が推察される．

5. 期待する効果

ネットワークログから不正通信の特徴を把握することで、組織にとって対処すべき攻撃の動向を掴むことができると考える．また，外部情勢と機関内部通信の関係性を把握することで，ニュース等の外部情勢に関連する様々な情報源を判断材料として，ある程度の危険予測が可能にとなる．この結果，セキュリティ対策チームの負担軽減と脅威判定の効率が向上し，セキュリティ向上につながると考えられる．

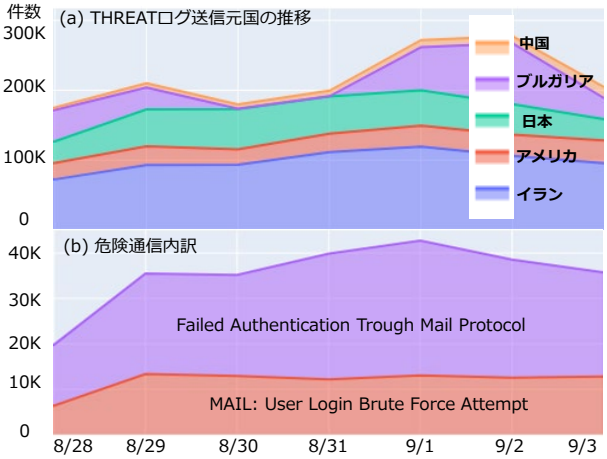

図 1 THREAT ログ送信国と危険通信

表 3 社会情勢事象

日時	事象
8/22	ロシア・ザポリージャ原発に砲撃
8/25	拒否ルールに該当する為破棄された
8/27	イラン、国産ドローンを発表
8/28	イラン・IAEAを非難。核合意は進まず
9/8	ウクライナ、イラン製攻撃ドローンを迎撃

6. おわりに

今回の分析は，1 例としてサイバー攻撃との関係が深いと予想される戦争・内紛などの社会情勢データを対象とし，ネットワークログのとの突き合わせ分析を実施した．現在も研究段階であるが，社会情勢の変化が脅威通信に及ぼす影響が示唆された．今後は本分析を基に，様々な事象に対してネットワークログの挙動変化や動向を分析していく．

参考文献

[1] 令和 4 年版情報通信白書(総務省) https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/ (2024 年 1 月 11 日 参照)

[2] サイバーセキュリティ白書 2023(IPA) https://www.ipa.go.jp/publish/wp-security/2023.html (2024 年 1 月 11 日 参照)

[3] 石井友基, 後藤厚宏: プレッシャーによるサイバー攻撃兆候検知に向けた検討, 情報処理学会第 79 回全国大会講演論文集, 1 号, pp.611-612(2017)

Copyright ©2024 Information Processing Society of Japan.
All Rights Reserved.