ダークウェブからの収集情報を利用したマーケットサイト間の販売トレンドの分析とライフサイクル推定

古本 啓祐[†1,*] 海崎 光宏[†1] 藤田 彬[†1]
永田 貴彦[†2] 高橋 健志[†1] 井上 大介[†1]

概要：ダークウェブではサービス利用者の秘匿性を確保しやすいため，違法ドラッグの取引など様々な犯罪のプラットフォームになっている．サイバー攻撃に関しても同様に，マルウェアやエクスプロイトキットなどがマーケットサイトで販売されており，攻撃手法などもフォーラムサイトにおいて議論されている．我々はダークウェブ上のサイトをクローリングする際の技術的な問題を解決し，実装したクローラを用いて大規模なデータ収集を行った．そして，大規模なデータセットを利用して，マーケットサイトの収集情報に着目した場合のミクロな視点での販売トレンドと，フォーラムサイトの収集情報に着目した場合のマクロな視点でのサイトのライフタイムについて分析を行った．その結果，マーケットサイト間のトレンドの違いや，各マーケットサイトのライフサイクルに関する新たな考察が得られた．

キーワード：ダークウェブ，脅威インテリジェンス

Analysis of Sales Trends and Life Cycle Estimation Among Market Sites Using Information Collected from Dark Web

Keisuke Furumoto[†1,*] Mitsuhiro Umizaki[†1] Akira Fujita[†1]
Takahiko Nagata[†2] Takeshi Takahashi[†1] Daisuke Inoue[†1]

Abstract: Dark Web has become a platform for various crimes, such as illegal drug trafficking, because it is easy to ensure the confidentiality of service users. Cyber-attacks are also being conducted in the same way, with malware and exploit kits being sold on market sites, and attack methods being discussed on forum sites. We have solved the technical problem of crawling sites on the Dark Web, and have conducted large-scale data collection using a crawler that we implemented. Using the large dataset, we analyzed sales trends from a micro perspective by focusing on information collected from market sites. And we analyzed lifetime of the sites from a macro perspective by focusing on information collected from forum sites. As a result, we obtained new insights into the differences in trends among market sites and the life cycle of each market site.

Keywords: Dark Web, Threat Intelligence

1. はじめに

Tor[1][2]を利用したダークウェブ上のサイトへのアクセスはユーザの秘匿性を確保しやすく，違法ドラッグの取引など様々な犯罪のプラットフォームとなっている．サイバー攻撃に関しても同様に，マルウェアやエクスプロイトキット，不正入手した認証情報などがマーケットサイトで販売されており[3][4]，エクスプロイトキットの使用方法や攻撃キャンペーンの情報などがフォーラムサイトにおいて議論されている[5][6]．このように，ダークウェブ上の情報をクローリングすることで，表層ウェブ側のセキュリティレポートや脆弱性情報データベースなどの情報源のみからでは得られないサイバー攻撃に関する情報（以下，「脅威インテリジェンス」と表記する）を得ることが可能である．しかし，ダークウェブ上のサイトをクローリングする場合，表層ウェブ側のサイトをクローリングする場合とは異なる課題が存在する．例えば，ダークウェブ上のマーケットサイトの多くにはサイトごとに異なる画像認証方式が採用されており，サイトによっては 2 段階の画像認証をログイン時に必須としているケースもある．また，著名なサイトであっても，摘発などの理由で突然閉鎖されるケースも多く[7][8][9]，収集先リストの更新が必要である．さらにダークウェブ上の情報をクローリングする場合，違法コンテンツのダウンロードを確実に回避することも重要である．ここで，ダークウェブ上のサイトからクローリングしたデータセットも公開されているが[10][11]，文献[10]のデータセットは機械学習用に違法サイトのラベリングが付与されたベクトルデータであり脅威インテリジェンス自体は含まれて

†1 国立研究開発法人 情報通信研究機構
National Institute of Information and Communications Technology
†2 GMO サイバーセキュリティ by イエラエ株式会社
GMO Cybersecurity by Ierae, Inc.
* k.furumoto@nict.go.jp

いない．文献[11]のデータセットには，2013 年から 2015 年にかけて収集した HTML ファイルや画像ファイルが含まれている．文献[11]のデータセットを用いた既存研究は多いが，このデータセットには近年のデータは含まれてなく，ダークウェブ上の動向は急速に変化するため，ダークウェブ上の最新の脅威インテリジェンスを収集することが重要である．

本稿では，ダークウェブ上のサイトをクローリングする際の技術的な課題を解決するクローラを実装し，実装したクローラを運用することでダークウェブ上の情報を収集した．本稿では，マルウェアやエクスプロイトキットなどの販売が行われている可能性の高いマーケットサイト（以下，「ダークマーケット」と表記する）と，攻撃手法や攻撃キャンペーンなどに関する投稿が行われている可能性の高いフォーラムサイト（以下，「ダークフォーラム」と表記する）に着目し，収集対象とした．クローリングの結果，脅威インテリジェンスを含む大規模なデータセットを構築し，そのデータセットを利用してダークマーケットのライフサイクルに関する実態調査・分析を行った．ダークマーケットの調査に関する先行研究は多く存在するが，ダークマーケットは閉鎖されることが多く，過去に遡ってダークマーケットのサイト群の全体像を把握することは困難である．ダークマーケット用に実装したクローラを運用する場合も，3 章で説明する課題から長期間の運用は難しく，頻繁に閉鎖するサイト群を網羅的にクローリングし続けることは困難である．そこで，本稿ではダークフォーラム上のダークマーケットに関するカテゴリの投稿に着目した．ダークフォーラムはダークマーケットと比較して閉鎖されるケースは少なく，ダークフォーラム上の過去の投稿を利用することで，すでに閉鎖されたマーケットサイトに関する情報も得ることが可能である．本稿ではまず，実装したクローラで収集した大規模なデータセットを利用して，マーケットサイトの収集情報に着目した場合のミクロな視点での販売トレンドの分析を行った．次に，フォーラムサイトの収集情報に着目した場合のマクロな視点でのサイトのライフタイムについて分析を行った．その結果，マーケットサイト間のトレンドの違いや，各マーケットサイトのライフサイクルに関する新たな考察が得られた．

2. ダークウェブ

ダークウェブ上のサイトにアクセスするためには，匿名性の高い Tor[1][2]のプロトコルに対応したブラウザが必要であり，この匿名性の高さを利用して違法な商品の売買や犯罪に関わる情報交換を行うサイトが数多く存在する．ダークウェブ上には様々な種類のサイトが存在するが，本稿ではサイバーセキュリティ領域の脅威インテリジェンスが含まれている可能性の高いダークマーケットとダークフォーラムを収集・解析対象とする．ダークマーケットとダークフォーラムについては，それぞれ 2.1 節，2.2 節で詳しく説明する．

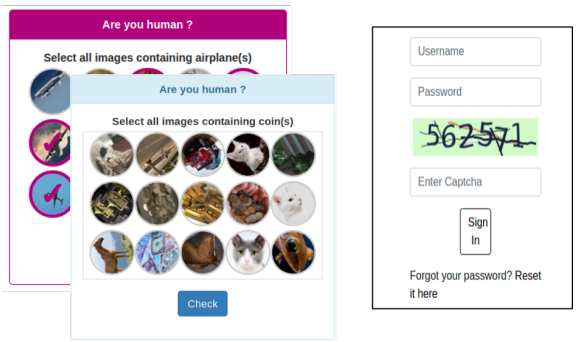

図 1　ダークマーケットのログイン時における画像認証・CAPTCHA の例

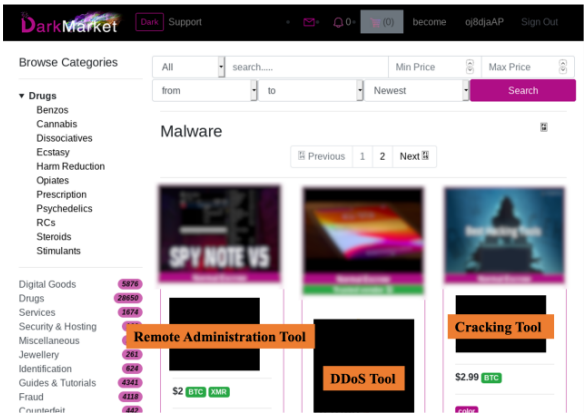

図 2　ダークマーケットの例
（DarkMarket における Malware のカテゴリ）

ダークウェブを含むアンダーグラウンドなサイト群を対象とした研究は複数存在する．文献[12]では，ダークウェブ上で収集したデータから脅威インテリジェンスを抽出するための機械学習手法を提案しているが，クローラの実装や実データを用いた提案手法の評価は今後の課題となっている．文献[13]では，onion ドメインのサイトを利用している約 500 名を対象に利用目的などを調査した結果，onion ドメインのサイトの利用者の多くは匿名性の確保を目的としていることを示している．文献[14]では，表層ウェブ上のフォーラムサイトの情報を収集し，攻撃者側が使用する監視ツールのインテリジェンスを抽出することで，監視による被害防止に貢献可能であることを示している．文献[15]では、アーカイブとして公開されているダークウェブのデータセット[11]を利用して，ダークフォーラムのサイト上で使用されているサイバーセキュリティ領域のスラングを抽出する手法を提案している．文献[16]では，画像のクローリング時に児童ポルノなどの違法コンテンツのダウンロードを回避するために，画像から抽出した特徴量のみを収集する手法を提案している．

アンダーグラウンドなサイト群を対象とした研究におい

て，ダークウェブ上のサイトのデータを実際にクローリングしている研究は多くなく，特にダークフォーラムのデータを実際にクローリングしている研究は少ない．この理由として，ダークウェブ上のサイトをクローリングする際には技術的・法的に考慮すべき点が多く，特にダークフォーラムのクローリングはクローラの実装ならびに運用負担が大きいことが挙げられる．また，収集対象のサイト群が閉鎖されるケースも多く，クローリング期間によって生存しているサイト群も変わってくる．そのため，サイト群が生存している期間にクローリングを行うことは，研究用のデータセットを蓄積していく観点でも重要であると考えられる．

2.1 ダークマーケット

ダークマーケットは，複数の売り手と買い手を結びつけるプラットフォームである．ダークマーケットは，商品を閲覧するのみであってもログインを必要とするサイトが多く，ログイン時に画像認証や CAPTCHA を必要とするサイトも少なくない．図 1 にダークマーケットのログイン時における画像認証・CAPTCHA の例を示す．ダークマーケットの商品の多くは，ドラッグやマルウェアなどの違法性のある商品である．ダークマーケットにおいて商品に付与されるカテゴリはサイト側が用意しているケースが多く，例えばデジタルグッズのカテゴリにはマルウェアやエクスプロイトキットのサブカテゴリが用意されているケースが多い. 図 2 はダークマーケットのサイトである DarkMarket における商品の例であり，Malware のカテゴリに属する商品ページの例である．図中の商品画像はぼかしており，商品のタイトルや出品者に関する項目は黒塗りをしている．

2.2 ダークフォーラム

ダークフォーラムは，投稿されたスレッドのトピックに対する各ユーザーのコメントで構成されるプラットフォームである．ダークフォーラムに投稿されるトピックの多くは, ドラッグの取引などの違法取引に関するものであるが, マルウェアやエクスプロイトキットの使い方に関する情報交換や違法に取得した認証情報の受け渡しなど，そのカテゴリは多岐に渡る．言語は英語のサイトが多いものの，スペイン語やロシア語のダークフォーラムも存在する．多くのサイトでは, スレッドタイトル, 投稿者の ID, コメント, 投稿日時, レピュテーションなどの情報が公開されている．また，ダークマーケットとは異なり，ダークフォーラムではログイン時に画像認証や CAPTCHA を必要としないサイトが多い．図 3 はダークフォーラムのサイトである Dread におけるスレッドの例であり，EmpireMarket（ダークマーケット）のカテゴリに属するスレッドである．図中の投稿者に関する項目は黒塗りをしている．

3. ダークウェブ上のクローリング時の課題

ダークウェブ上のサイトをクローリングする場合，表層

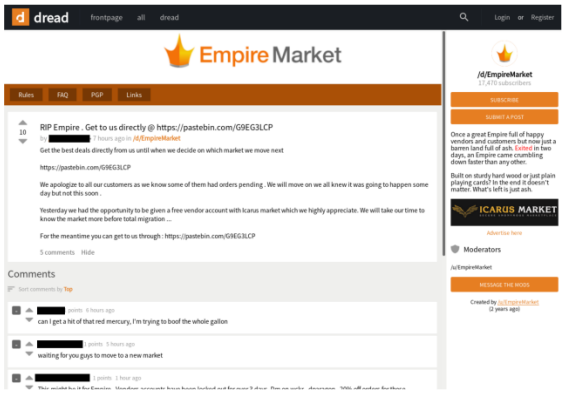

図 3　ダークフォーラムの例
（Dread における Empire Market のカテゴリ）

ウェブのサイトをクローリングする場合とは異なる課題が存在する．

- 収集先サイトの頻繁な閉鎖

ダークウェブ上のサイトは捜査機関の摘発や DDoS 攻撃などの利用により，サイトの閉鎖や移転が行われるケースが非常に多い．特にダークマーケットにおける閉鎖の頻度は高く，人気のあるダークマーケットであっても 2 年以上存続するケースは少ない．例えば，EmpireMarket は 2020 年の 8 月ごろに閉鎖され，サイトは再開しない可能性が高い[17]．本稿で実装したクローラは, 収集先サイトの URL リストを定期的に更新している．収集先サイトの onion ドメインは，ダークウェブ上のサイト情報をまとめている表層ウェブ上のサイト[18]-[20]を参照している. ただし, ダークウェブのサイト群の実態把握は難しく，これらのサイトの情報は最新ではないケースも多い．

- サイト側のクローリング対策

ダークウェブ上の多くのサイトは，クローリング対策として，画像認証や CAPTCHA をログイン時に必須としているケースが多い．前述のように，特にダークマーケットでは多くのサイトで必須となっており，特定の画像を選択させる認証と画像内の文字を入力させる CAPTCHA を用いた認証の 2 種類が多い．ダークマーケットの中には，2 段階の画像認証を必要とするサイトや，商品ページを一定数遷移するごとに認証を必要とするサイトも存在する. そのため, クローリング時には，ログインや認証に対する対策が必要である．本稿で実装したクローラは，ログイン時や認証時にのみ手動で操作を行う半自動の仕様となっている．

- Tor の通信速度

Tor の通信時には 3 重の暗号化・復号化を必要とし，世界中に設置されたサーバをランダムに経由するため，通信速度は遅い傾向にある．そのため，ダークマーケットやダークフォーラムのサイト全体をクローリングする際には，多

表 1　ダークマーケットにおける収集対象カテゴリとメタ情報

Category	Security, Hacking, Botnets, Malware, Exploit Kits, Security Software, Carding, Fake Documents, Hosting, Operational Management, SOCKS, Social Engeneering, VPN, Anonymity, Cryptocurrency, Crackers, Leaks, Crypters
Meta-Information	Item ID, File Path, Page Title, Product Title, Price, Left Quentity, Sold Quentity, Category, Feedback, Description, Product Type, Meta Tags, Vendor

表 2　ダークマーケットからの収集結果

Name	Language	Lifetime[(a)]	Number of Goods	Number of Sales Vendors	Categories
ASAP Market[(b)]	English	March 2020 to now	2,884	40	7
DarkMarket	English	June 2019 to now	5,085	131	17
DarkFox	English	April 2020 to now	1,689	55	18

[(a)] Last confirmed month: January 2021
[(b)] Old name: ASEAN Market

くの実行時間を要する．本稿では，収集対象のサイトにおいて，サイバーセキュリティ領域の脅威インテリジェンス関連のカテゴリのみを収集対象としている．

- 違法ダウンロードの回避

ダークウェブ上には，児童ポルノなどの違法コンテンツが存在するため，クローリング時には違法コンテンツのダウンロード自体を確実に回避することが重要である．本稿では違法コンテンツのダウンロードを確実に回避するために，画像ファイルや動画ファイル，実行ファイルは収集対象外とし，ダークマーケットの商品に付随する情報やダークフォーラムの投稿コメントなどのメタ情報のみを収集対象としている．

4. ダークマーケットの収集情報の分析

4.1 ダークマーケットの収集結果とミクロな視点での価格帯・出品者の分析

3 章で述べたダークウェブ上のクローリング時の課題を考慮して実装したクローラを利用して，ダークマーケットの情報を収集した．収集対象は脅威インテリジェンス関連のカテゴリの商品のメタ情報に限定して収集を行った．収集対象のカテゴリとメタ情報を表 1 に示す．表 1 におけるカテゴリ名の中にはサイト独自の表現も含まれるため，同じ意味を持つ別の単語に置き換えている例も含まれている．今回，ダークマーケットのサイトである ASAP Market, DarkMarket, DarkFox の 3 サイトを対象に収集を行った．3 サイトとも英語圏のダークマーケットであり，2020 年 10 月から 2021 年 1 月にかけて収集作業を実施し，参照可能であった商品のメタ情報を収集した．表 2 は ASAP Market, DarkMarket, DarkFox の 3 サイトに関する記述言語やライフタイム，収集した商品数や出品者数，収集対象のカテゴリ数を記載している．

ASAP Market, DarkMarket, DarkFox の 3 サイトの脅威インテリジェンス関連の商品の価格帯の分布を図 4 に示す．3 サイトとも脅威インテリジェンス関連の商品の価格帯の分布は異なっており，ASAP Market は特定の価格帯の商品

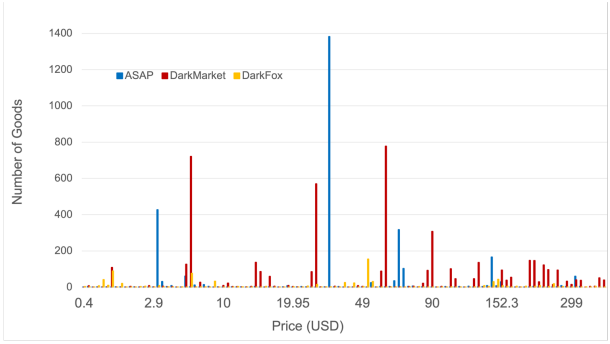

図 4　ダークマーケットの 3 サイトにおけるサイバーセキュリティ関連の商品の価格帯の分布

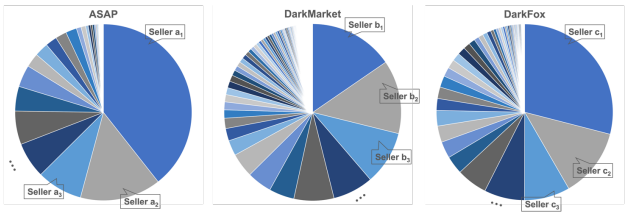

図 5　ダークマーケットの 3 サイトにおける各出品者による出品数の割合

が多く，DarkMarket は高価格帯まで広く分布しており，DarkFox は低価格帯の商品が多い．この理由としては，ダークマーケットごとに主力商品の価格帯のトレンドがあることに加えて，特定の少数の出品者の影響に拠るものであると考えられる．この根拠として，ASAP Market, DarkMarket, DarkFox の 3 サイトにおける脅威インテリジェンス関連の商品の出品数に応じた出品者の分布を図 5 に示す．図 5 から，3 サイトとも少数の出品者が大きな割合を占めており，3 サイトとも約 75%の脅威インテリジェンス関連の商品が 10 人以下の出品者によって出品されている．また，上位の出品者の ID のうち，複数のダークマーケットで利用されている ID もあり，例えばある ID-X の出品者は ASAP Market では出品数 1 位，DarkMarket の出品数は 7 位であった．さらに，DarkFox の出品数 1 位のユーザ ID-Y は前述の ID-X

表 3　ダークフォーラムにおける収集対象カテゴリとメタ情報

Category	Market, Security, Hacking, Botnets, Malware, Exploit Kits, Security Software, Carding, Fake Documents, Hosting, Operational Management, SOCKS, Social Engeneering, VPN, Privacy, Anonymity, Cryptocurrency, Crackers, Leaks, Crypters
Meta-Information	Thread ID, File Path, Category, Number of Comment, Thread Title, Post Date, Body(Comment) , Number of Vote, Author(Name, Number of Post, Number of Thread, Number of Reaction , Awards/Class, Age, Location, Website)

表 4　ダークフォーラムからの収集結果

Name	Language	Lifetime[(a)]	Number of Threads / Comments	Number of Contributors[(b)]	Categories
Dread	English	February 2018 to now	189,260 / 1,022,857	62,203	469

[(a)] Last confirmed month: March 2021
[(b)] Total number of thread creators and commenters

と酷似しており，同一ユーザである可能性が考えられる．ただし，図 4 の価格帯がサイトごとに異なる結果から分かるように，少数のユーザが複数のダークマーケットの出品数の上位を占めている場合でも，サイトごとに主力商品の価格帯のトレンドがあると考えられる．以上の結果から，各ダークマーケットの脅威インテリジェンスの商品数は多いものの，一部の少数の出品者により占められている傾向が確認された．さらに，この少数の出品者は脅威インテリジェンス関連の商品を多く制作している可能性もあるものの，ダークマーケット上の商品は著作権の観点での拘束力はないため，電子媒体である脅威インテリジェンスの商品の多くは少数の出品者により転売されている可能性も考えられる．

4.2　ダークマーケットの収集情報に対するマクロな視点での分析時の課題

前節ではダークマーケットの収集情報に対して，3 サイト間に限定したミクロな視点での分析を行った．その結果，少数の出品者が脅威インテリジェンス関連の商品の多くを出品している傾向が確認されたが，対象のサイト数を増やしてよりマクロな視点での分析を行う際には以下の課題がある．

- ダークマーケットのサイトは頻繁に閉鎖されるため，収集作業時点で生存しているサイトのみが対象であり，過去に生存したサイトに遡ることができない
- 3 章で述べた Tor の通信速度やログイン時の画像認証に対する手動操作により，ダークマーケットのサイト群全体をクローリングする際は運用負担が大きい

以上の課題から，ダークマーケットに関する既存研究はアーカイブのデータセット[11]を使うケースや，収集作業時点で生存しているダークマーケットを数サイト選別し独自に収集したケースが多い．前者はデータセットの収集日が古いという課題があり，後者はそれぞれの研究者が収集作業する時点での生存サイトが異なるためデータセットに含まれるサイトが異なる，という課題がある．よって，過去数年間に渡るダークマーケットのサイト群に対するマクロな視点でのサイト閉鎖・開設などの傾向を把握するためには，ダークマーケットのサイト群をクローリングする方法はコストが非常に大きい．そこで，ダークフォーラムの収集情報を利用することで，ダークマーケットのサイト群のライフサイクルを推定するアプローチについて次章で述べる．

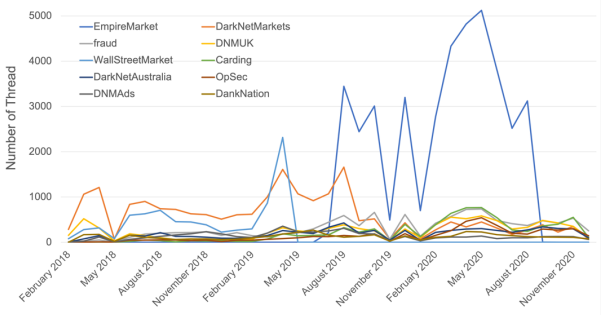

図 6　ダークフォーラム（Dread）の収集情報における累積スレッド数の上位 10 カテゴリの時系列推移

5. ダークフォーラムの収集情報を利用したダークマーケットのライフサイクル推定

本章では，ダークフォーラムの収集情報を利用することで，ダークマーケットのサイト群のライフサイクルを推定するアプローチとその結果について報告する．まず，5.1 節ではダークフォーラムの全カテゴリの収集情報を利用した場合の分析結果について述べる．次に 5.2 節では，ダークフォーラムの収集情報のうち，ダークマーケット関連のカテゴリの収集情報に限定した場合の分析結果とライフサイクルの推定結果について述べる．

5.1　ダークフォーラムの収集結果と収集対象の全カテゴリに関する分析

3 章で述べたダークウェブ上のクローリング時の課題を考慮して実装したクローラを利用して，ダークフォーラムの情報を収集した．ダークフォーラムのサイトにはドラッグなど多くのカテゴリが存在するが，IT 分野やマーケットサイトに関するカテゴリ，サイバーセキュリティ分野の脅

表 5　ダークフォーラムからの収集結果（ダークマーケット関連のカテゴリのみ）

Name	Language	Lifetime[(a)]	Number of Threads / Comments	Number of Contributors[(b)]	Categories
Dread	English	February 2018 to now	93,684 / 590,966	21,492	85

[(a)] Last confirmed month: March 2021
[(b)] Total number of thread creators and commenters

威インテリジェンスのカテゴリに限定して収集を行った．収集対象のカテゴリとメタ情報を表 3 に示す．表 3 におけるカテゴリ名の中にはサイト独自の表現も含まれるため，同じ意味を持つ別の単語に置き換えている例も含まれている．今回，ダークフォーラムのサイトである Dread を対象に収集を行った．Dread は英語で記述されたダークフォーラムであり，2020 年 10 月から 2021 年 2 月にかけて収集作業を実施し，参照可能であった 2018 年 2 月以降の情報を収集した．表 4 は Dread に関する記述言語やライフタイム，収集したスレッド数やコメント数，投稿者の総数や収集対象のカテゴリ数を記載している．2018 年 1 月の Dread の情報は参照できなかったが，これは Dread の開設時期に起因するものであると考えられる．図 6 は収集期間中の累計スレッド数が最も多かった 10 カテゴリの時系列推移を示している．図 6 の 10 カテゴリのうち 4 カテゴリは特定のダークマーケットに関するカテゴリであり，これはダークウェブにアクセスするユーザの多くはダークマーケットの利用を目的としており，ダークマーケットに関する投稿への関心が高いためだと考えられる．特に，EmpireMarket のような著名なマーケットが摘発・閉鎖される情報が流れた際には（2020 年 5 月 5 月ごろ），顕著にスレッド数が増加している．EmpireMarket は 2020 年 8 月 20 日ごろに閉鎖されたと報道されており[17][21]，閉鎖後はスレッド数が顕著に減少している．我々は，Dread における EmpireMarket のカテゴリの収集情報を定性的に分析し，表層ウェブ側のレポートや記事で報告されているように捜査機関による摘発がサイト閉鎖の要因ではなく，競合相手等による DDoS 攻撃がサイト閉鎖の原因と考えられる点について報告を行った[22]．さらに，ダークマーケットに対する DDoS 攻撃の犯行声明の事例も報告されており[23]，このようにダークマーケットの閉鎖の原因は捜査機関による摘発に起因するもののみではなく，ダークウェブにアクセスするユーザも多くの情報を保持しているものと考えられる．ここで，Dread におけるダークマーケット関連のカテゴリのスレッドの増減は実際のサイト閉鎖といったサイトの動きを反映していると仮定し，ダークマーケット関連のカテゴリに対象を絞った場合の検証を行った．

5.2　ダークフォーラムの収集情報を利用したダークマーケットのライフサイクル推定

本節では Dread におけるダークマーケット関連のカテゴリに対象を限定した場合の分析結果とライフサイクルの推定結果について述べる．まず，表 4 の Dread の収集結果に

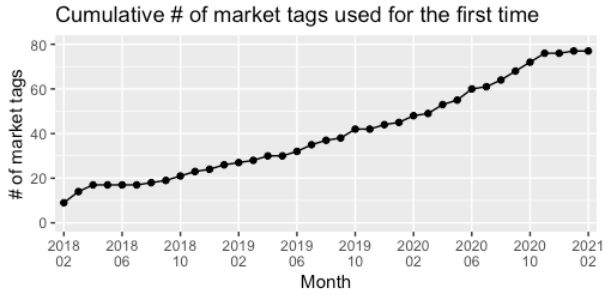

図 7　ダークフォーラム（Dread）の収集情報から推定したダークマーケットの生成ペース

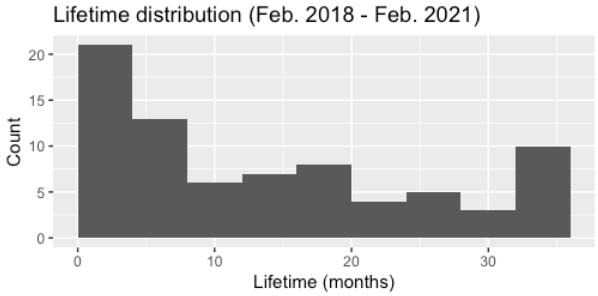

図 8　ダークフォーラム（Dread）の収集情報から推定したダークマーケットのライフタイム

おいて，ダークマーケット関連のカテゴリに絞った場合の収集結果を表 5 に示す．ダークマーケット関連のカテゴリ数は収集対象の 469 のうちの 85 となっているものの，スレッド数やコメント数は全カテゴリの収集結果のうち約半分を占めている．この点から，ダークマーケット関連のカテゴリでは議論が活発に行われていると考えられる．

図 7 はダークマーケット関連のカテゴリの Dread の収集情報において，初めて立てられたカテゴリのスレッド数を集計・累積したものである．例えば，毎月 5 つの新たなダークマーケット関連のカテゴリのスレッドが Dread に立てられた場合，累積数は毎月 5 サイトずつ増加していくことになる．図 7 のグラフから，Dread のサイト開設当時の 2018 年 2 月ごろは増加傾向が大きいが，それ以降は 2020 年末にかけて一定のペースで累積数は増加し，2021 年に入ってからは増加傾向が緩くなっている．以上の点から，Dread のユーザが関心を寄せてスレッドを立てるダークマーケットは，一定のペースで累積数が増えているが，これは新たなダークマーケットが開設しただけではなく，同数程度のダークマーケットが閉鎖したと考えられる．新たなダークマ

ーケットが開設されたタイミングと，Dread に当該ダークマーケットのカテゴリのスレッドが最初に立てられたタイミングは一致していない可能性はあるものの，図 7 からダークマーケット全体での閉鎖・開設のペースは一定であると推測される．

図 8 はダークマーケット関連のカテゴリの Dread の収集情報において，各ダークマーケット関連のカテゴリのスレッドが初めて立てられた月と最後に立てられた月の差（ライフタイム）を示したものである．最も割合が多いカテゴリは 5 ヶ月以下のライフタイムであり，一方で 30 ヶ月以上のライフタイムのカテゴリも存在する．ここで，図 9 はダークマーケット関連のカテゴリのスレッドが各月あたり少なくとも 1 つ以上存在した月を赤で示したものである．図 9 から，スレッドが長期間継続して立てられているダークマーケットのカテゴリがある一方で，スレッドが特定の期間しか立てられていないダークマーケットのカテゴリも存在する．以上の結果から，図 7 で示したダークマーケット全体での閉鎖･開設のペースが一定であることと同じく，図 9 からもダークマーケットの話題は特定のサイトに限定されるものではなく，定期的に新たなダークマーケットのカテゴリが追加されていることがわかる．一方，図 8 で示したように各カテゴリのライフタイムはサイトごとに異なり，閉鎖された後であってもスレッドが立てられるダークマーケットと閉鎖された以後はスレッドが立てられることが皆無となるケースが確認された．

図 10 は，ダークマーケット関連のカテゴリの Dread の収集情報において，24 ヶ月以上のライフタイムに該当する 19 カテゴリに着目して，年毎のスレッドの増減の季節性を調査したものである．図 10 の結果から毎年定期的に繰り返されるスレッドの増減はなく，サイトの閉鎖などのタイミングで大きく増減していることが確認された．ここで，Dread の収集情報において，表層ウェブ側のレポートなどで閉鎖時期が確認されたダークマーケットのカテゴリのスレッド数の推移を図 11 に示す. 表層ウェブ側のレポートで取り上げられるのは，話題性のある著名なマーケットに限られるため，実際には多くのダークマーケットが閉鎖されていると考えられるものの，表層ウェブ側のレポートなどで取り上げられる例は少ない．図 11 は以下の 4 つのマーケットのスレッド数の推移を示しており，これらの 4 サイトの閉鎖に関しては表層ウェブ側のレポートなどから閉鎖時期を確認可能である．4 つのマーケットの閉鎖時期は，図 11 のスレッド数の推移で大きく増減している時期と一致している. この傾向はこれらのマーケットのみではなく，表層ウェブ側のレポートなどで正確な閉鎖時期は特定できないものの，スレッド数の推移から閉鎖時期を推定できるダークマーケットのカテゴリも存在する．これらの表層ウェブ側のレポートなどでは閉鎖時期を正確に特定できないダークマーケットに関して，ダークフォーラムのスレッド

図 9　ダークフォーラム（Dread）の収集情報における
ダークマーケットに関するスレッドの生存期間

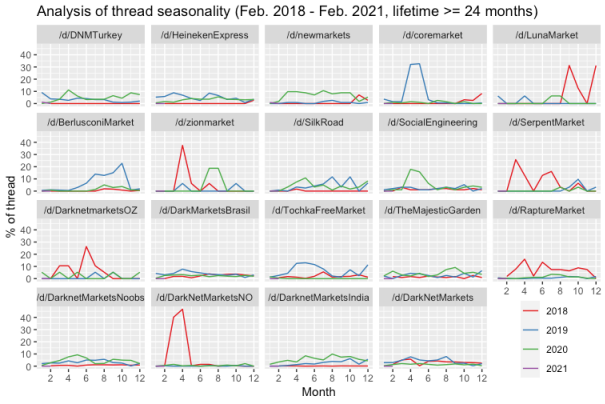

図 10　ダークフォーラム（Dread）の収集情報における
ダークマーケットに関するスレッドの季節性

数の推移から閉鎖を検証・予測する手法は今後の課題とする．

- DreamMarket：2019 年 4 月 30 日[24]
- EmpireMarket：2020 年 8 月 20 日[17][21][25]
- WallStreetMarket：2019 年 5 月 3 日[9]
- DarkMarket：2021 年 1 月 12 日[26]

6. おわりに

本稿ではまず，実装したクローラで収集した大規模なデータセットを利用して，マーケットサイトの収集情報に着目した場合のミクロな視点での販売トレンドの分析を行っ

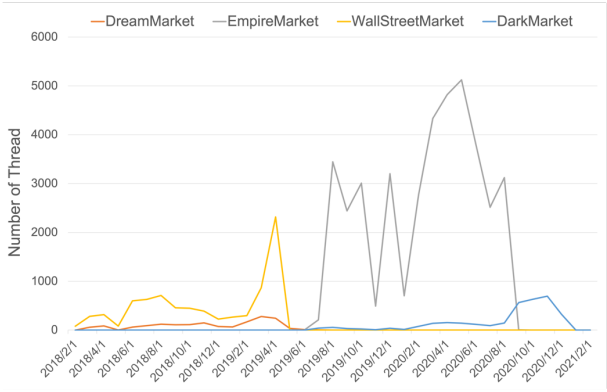

図 11　ダークフォーラム（Dread）の収集情報における閉鎖されたダークマーケットのスレッド数推移

た．次に，フォーラムサイトの収集情報に着目した場合のマクロな視点でのサイトのライフタイムについて分析を行った. その結果, マーケットサイト間のトレンドの違いや, 各マーケットサイトのライフサイクルに関する新たな考察が得られた．

謝辞　本研究は総務省の「電波資源拡大のための研究開発(JPJ000254)」における委託研究「電波の有効利用のための IoT マルウェア無害化／無機能化技術等に関する研究開発」によって実施した成果を含みます．

参考文献

[1] “Tor project: Anonymity online.” [Online]. Available: https://www.torproject.org/

[2] D.McCoy, K.Bauer, D.Grunwald, T.Kohno, and D.Sicker, “Shining Light in Dark Places: Understanding the Tor Network,” in International Symposium on Privacy Enhancing Technologies Symposium, vol.5134, 2008, pp. 63–76.

[3] “Halloware Ransomware on Sale on the Dark Web for Only $40” [Online]. Available: https://www.bleepingcomputer.com/news/security/halloware-ransomware-on-sale-on-the-dark-web-for-only-40/

[4] “Scammer Uses Fake Tor Browser to Lure Victims to Supposed Dark Web Marketplace” [Online]. Available: https://www.bleepingcomputer.com/news/security/scammer-uses-fake-tor-browser-to-lure-victims-to-supposed-dark-web-marketplace/

[5] “Hackers' private chats leaked in stolen WeLeakData database” [Online]. Available: https://www.bleepingcomputer.com/news/security/hackers-private-chats-leaked-in-stolen-weleakdata-database/

[6] “Hacker Leaks 900 Enterprise VPN Server Passwords on Dark Web” [Online]. Available: https://healthitsecurity.com/news/hacker-leaks-900-enterprise-vpn-server-passwords-on-dark-web

[7] “Operation Onymous | Europol” [Online]. Available: https://www.europol.europa.eu/activities-services/europol-in-action/operations/operation-onymous

[8] “Buying Drugs Online Remains Easy, 2 Years After FBI Killed Silk Road | US News” [Online]. Available: https://www.usnews.com/news/articles/2015/10/02/buying-drugs-online-remains-easy-2-years-after-fbi-killed-silk-road

[9] “Double blow to dark web marketplaces | Europol” [Online]. Available: https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces

[10] “DDIR: An Open Source Dataset for Darkweb Researc” [Online]. Available: https://github.com/nenaiko-dareda/DDIR

[11] “Darknet Market Archives (2013-2015)” [Online]. Available: https://www.gwern.net/DNM-archives

[12] E.Nunes, A.Diab, A.Gunn, E.Marin, V.Mishra, V.Paliath, J.Robertson, J. Shakarian, A. Thart, and P. Shakarian, “Darknet and deepnet mining for proactive cybersecurity threat intelligence,” in IEEE Conference on Intelligence and Security Informatics, 2016, pp.7–12.

[13] P.Winter, A.Edmundson, L.M.Roberts, A.Dutkowska-Z ̇uk, M.Chetty, and N.Feamster, “How do tor users interact with onion services?” in In Proceedings of the 27th USENIX Security Symposium, 2018, pp. 411–428.

[14] E. Tseng, R. Bellini, N. McDonald, M. Danos, R. Greenstadt, D. McCoy, N. Dell, and T. Ristenpart, “The tools and tactics used in intimate partner surveillance: An analysis of online infidelity forums,” in In Proceedings of the 29th USENIX Security Symposium, 2020, pp. 1893—-1909.

[15] K. Yuan, H. Lu, X. Liao, and X. Wang, “Reading thieves’ cant: Automatically identifying and understanding dark jargons from cybercrime marketplaces,” in 27th USENIX Security Symposium, Aug. 2018, pp.1027–1041.

[16] E.Bursztein, T.Bright, M.DeLaune, D.M.Eliff, N.Hsu, L.Olson, J.Shehan, M.Thakur, and K.Thomas, “Rethinking the detection of child sexualabuse imagery on the internet,” in In USENIX Enigma, 2019.

[17] “Dark web market Empire down for days from DDoS attack” [Online]. Available: https://www.bleepingcomputer.com/news/cryptocurrency/dark-web-market-empire-down-for-days-from-ddos-attack/

[18] “Deep Onion Web” [Online]. Available: https://www.deeponionweb.com/

[19] “Dark Market List 2020.” [Online]. Available: https://www.thedarkweblinks.com/dark-web-links/

[20] “DeepWebSitesLinks.” [Online]. Available: https://www.deepwebsiteslinks.com/darknet-markets-links/

[21] “Dark web drug haven Empire Market has mysteriously disappeared - The Verge” [Online]. Available: https://www.theverge.com/2020/8/26/21403362/empire-market-dark-web-drug-marketplace-police-shutdown-silk-road-alphabay

[22] Keisuke Furumoto, Mitsuhiro Umizaki, Akira Fujita, Takahiko Nagata, Takeshi Takahashi, Daisuke Inoue, "Extracting Threat Intelligence Related IoT Botnet From Latest Dark Web Data Collection (Short Paper)," The 14th IEEE International Conferences on Internet of Things (iThings-2021), Online, Dec.6-8, 2021.

[23] “The Top Dark Web Trends in 2021 - Webz” [Online]. Available: https://webz.io/blog/dark-web/the-top-dark-web-trends-in-2021/

[24] “Top dark web marketplace will shut down next month | ZDNET” [Online]. Available: https://www.zdnet.com/article/top-dark-web-marketplace-will-shut-down-next-month/

[25] “What Now After the Empire Market Shutdown ?” [Online]. Available: https://flare.systems/learn/resources/infographic-winners-losers-of-empire-market-shutdown/

[26] “DarkMarket: world's largest illegal dark web marketplace taken down | Europol” [Online]. Available: https://www.europol.europa.eu/media-press/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down