ダークウェブに関する現状

中沢 潔
JETRO/IPA New York

1　サマリー

我々が普段利用しているインターネット上の公開情報（パブリックウェブページ）は全体のわずか 4%にすぎないと言われており、大部分の情報はアクセスが制限され見えないことから、こうしたインターネットの階層構造は氷山に例えられることが多く、目的のサイトにアクセスすることが困難な「ディープウェブ」や「ダークウェブ」は深海に沈む氷山の最深部に位置付けられている。特に「ダークウェブ」は、インターネット上における言論の自由とプライバシー保護を実現するために開発された匿名通信ツールのリリースと共に生まれたが、同ツールの特性を悪用した違法サイト（闇市場）の出現・拡大と共に発展を遂げてきたといえる。

近年、大規模な闇市場サイトの摘発・閉鎖がニュースメディアで度々取り上げられ、犯罪に悪用されるイメージが先行しているダークウェブであるが、ある調査によれば、合法的なコンテンツがサイトの半分以上を占めており、違法コンテンツの中ではドラッグ等の違法薬剤取引に関するサイトが半分以上であるが、大量破壊兵器の取引やテロ行為、人身売買といった過激行為に関するサイトの存在は非常に稀である。合法的コンテンツの例として、以下が挙げられる。

〇ニュースメディア／匿名情報投稿サイト（BBC 等）
〇SNS（Facebook 等）
〇電子メール
〇インテリジェンス情報の収集（CIA 等）
〇ダークウェブ上にあるサイト検索
〇科学論文の無料共有

世界各国がダークウェブ上のサイバー犯罪対策を強化しているが、別の調査によれば、ダークウェブを利用する理由として最も多かったのは「匿名でいられるから」であり、特に中東地域やアフリカ地域、BRICS 地域のユーザーは、「自国でアクセスできないウェブコンテンツを閲覧できるため」や「政府のネット検閲を回避するため」及び「オンラインプライバシーの保護」を主な理由として挙げる一方、北米ユーザーは、「インターネット企業からプライバシーを保護するため」や「外国の政府からプライバシーを保護するため」といった理由を主に挙げており、今後、検閲の回避やプライバシーの保護の機運が高まれば、ダークウェブの利用が進む可能性が考えられる。

ニューヨーク市立大学工科校で准教授を務める中村正人氏は次のように述べている。「コンピューターの世界においては、並列計算機やベクトル計算機の戦いの後、クラウドコンピューティングや GPU による汎用計算を経て、現在世界の目は量子コンピューティングに向かっている。同様に、ウェブの世界においても、ウェブの表層の 4%だけでなく、ダークウェブを含め残りの 96%とそれに関連するテクノロジーが急速に独占・寡占されることが起こり得る。」

2　独自の発展を遂げるダークウェブの由来と仕組み

（1）　「ダークウェブ」とは何か

欧米を中心に、闇市場での違法な取引やサイバー犯罪の温床として近年度々メディアで取り上げられ、「ダークウェブ（dark web）」に世間の注目が集まっている。ダークウェブとは、Google 等の通常の検索エンジンでは見つけられず、Tor や I2P といったユーザー情報を簡単に追跡できないようにするための専用ツール（特定のソフトウェア、設定、認証）を閲覧に要するウェブサイトを指す[1]。インターネット上のウェブページは、①Google、Bing、Yahoo を含む標準ウェブ検索エンジンで検索・アクセス可能なページ（サーフェス（又はパブリック）ウェブ）と、②それができないページ（ディープウェブ）に大別され、ダークウェブのページは②の一部に分類されるが、アクセスには専用のツール（ウェブブラウザ）が必要であり、ユーザーの高い匿名性が保証されている点で、ディープウェブとは区別される[2]。我々が普段利用しているインターネット上の公開情報（パブリックウェブページ）は全体のわずか 4%にすぎないと言われており、大部分の情報はアクセスが制限され見えないことから、こうしたインターネットの階層構造は氷山に例えられることが多く、目的のサイトにアクセスすることが困難なダークウェブは深海に沈む氷山の最深部に位置付けられている（図表 1 参照）[3]。

図表 1：インターネット上のウェブページの階層構造（上）と各ウェブ階層の特徴比較（下）

出典：Hacker Noon

[1] https://www.upguard.com/blog/dark-web
[2] https://www.icuinvestigations.com/post/2017/11/01/the-surface-web-deep-web-and-dark-web-explained
[3] https://hackernoon.com/wtf-is-dark-web-358569fde822

	サーフェス／パブリックウェブ（Surface／Public Web）	ディープウェブ（Deep Web）	ダークウェブ（Dark Web）
インターネット上に占めるウェブコンテンツの推定割合	4%	90%	6%
アクセス条件	特になし（誰でもアクセス可能）	アクセスに認証が必要	匿名性の高い通信を担保する専用のツール（ブラウザ）が必要
ウェブページの特徴	Google 等の通常の検索エンジンによって、キーワード、ウェブアドレス、コンテンツ等を基にインデックス化されており、これらの検索エンジンを用いて検索・アクセスできる	・通常の検索エンジンでインデックス化されていないため、検索結果に表示されない ・Facebook 等の SNS サイトや Dropbox 等のファイル共有サービスサイト、購読形式の有料ニュースサイト、個人の医療データ、企業の組織内ネットワークのページなど、データ保護目的及び有料サービスであることなどを理由にパスワード保護（暗号化）されており、アクセス権限を有する特定のユーザーのみがアクセスできる。ウェブページはサーフェス（パブリックウェブ）のブラウザ／アプリケーションを用いて閲覧できる	・ディープウェブと同様、通常の検索エンジンでインデックス化されておらず、Tor や I2P に代表される通信匿名化ツールを経由することで閲覧が可能となる。ダークウェブの汎用性については、その匿名性の高さから、言論の自由が制限されている国における人々の自由な情報発信・通信を支援する有効な手段の一つとなっている一方、近年はドラッグや武器、サイバー攻撃、個人情報、児童ポルノ等の違法商品を取引するための闇市場サイトの存在が大きく問題視されるようになっている ・ドメイン名には一般的な「.com」や「.org」ではなく、「.onion」や「.i2p」等が用いられる

出典：各種資料を基に作成

（2） ダークウェブの誕生・発展の経緯

ダークウェブは、インターネット上における言論の自由とプライバシー保護を実現するために開発された匿名通信ツールのリリースと共に生まれたが、同ツールの特性を悪用した違法サイト（闇市場）の出現・拡大と共に発展を遂げてきたといえる（図表 2 参照）[4]。2000 年代はじめに「Freenet」、「Tor」、「I2P」の 3 つの主要ツールが相次いで一般にリリースされた（各ツールの概要については図表 3 参照）が、特に 2002 年 9 月にオープンソースソフトウェアとして公開された「Tor」は、2010 年末から 2012 年にかけてチュニジアやエジプトなどで起きた民主化運動「アラブの春（Arab Spring）」と、2013 年のスノーデン事件[5]において情報発信者を保護するための有効なツールとして注目を集め、現在最も普及している匿名通信ツールである[6]。Tor は、米政府を含む多数のスポンサーから資金援助を受け[7]、現在も機能改善に向けた開発が続けられている[8]（Tor の匿名通信の仕組みについては次項で後述）。

[4] https://www.technadu.com/dark-web-history/52017/

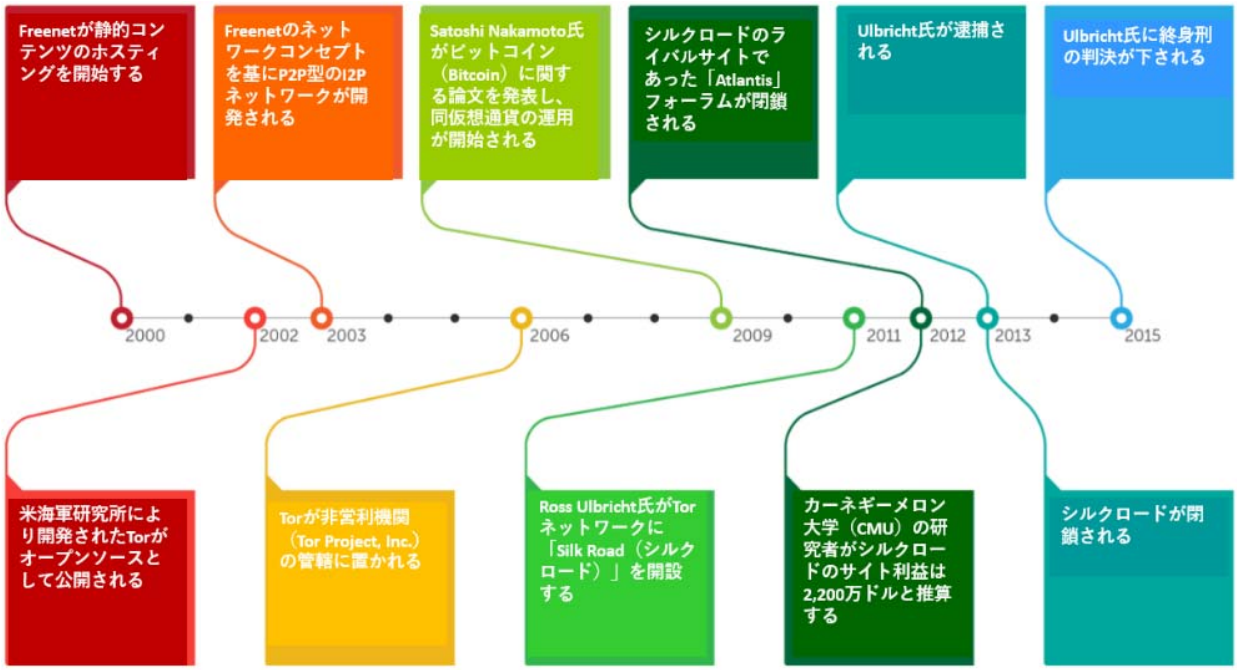
[5] 米国家安全保障局（NSA）の元局員 Edward Snowden（エドワード・スノーデン）氏が、NSA によるテロ対策としての大規模な国民監視（通話、SMS、メール等の情報収集）活動を暴露した事件。スノーデン氏はインターネット上でプライバシーを保護するための手段として Tor の活用を推奨し、同匿名通信ツールに対する世間の関心を高めるきっかけを作った。

[6] Tor のユーザー数はおよそ 200 万人と推定されている。https://metrics.torproject.org/userstats-relay-country.html?start=2019-10-01&end=2020-01-13&country=all&events=off

[7] Tor は 2015 年まで、その資金源の 80～90%を米政府に依存していたが、米連邦捜査局（FBI）が Tor ユーザーの身元を特定するために 100 万ドルをカーネギーメロン大学（CMU）の研究者に提供していた疑惑が公になり大きな議論を呼んだことをきっかけに、資金源の多様化に注力しており、2017 年にはスウェーデン政府や Mozilla 社、その他世界の多数の団体・個人から多額の資金を調達、米政府からの資金源は調達資金総額（413 億ドル）のおよそ 50%程度にまで減少している。https://techcrunch.com/2019/01/11/tor-lessens-reliance-us-grants/、https://www.torproject.org/about/sponsors/

[8] https://www.torproject.org/about/history/

図表 2:ダークウェブに関連した主な出来事



出典:Trend Micro

図表 3:ダークウェブに用いられる 3 つの主要匿名通信ツールの概要

	Freenet[9]	Tor[10] （The Onion Router）	I2P[11] （Invisible Internet Project）
公開時期	2000 年	2002 年	2003 年
開発目的	検閲耐性の高い通信システムを実現し、インターネット上における言論の自由を守る	当初は米スパイがインターネット上で発信元の痕跡を隠し通信を匿名化できるようにすることであったが、2004 年に電子フロンティア財団（Electronic Frontier Foundation）が資金提供と組織運営を担って以降、インターネット上のプライバシー保護及び言論の自由を実現する強固なツールとなることに重点を置いている	検閲耐性の高い通信システムを実現し、ユーザーのプライバシーとセキュリティ保護に最も配慮した通信システムを実現する
概要	アイルランドのコンピューターサイエンティスト、Ian Clarke 氏が 1999 年に発表した論文「分散型情報保存・検索システム（A Distributed Decentralised Information Storage and Retrieval System）」を基に開発された P2P 分散型匿名通信ネットワークシステム。Freenet	1990 年代半ばに米海軍研究所（U.S. Naval Research Laboratory）により開発された「オニオン・ルーティング（onion routing）」と呼ばれる通信経路を匿名化する暗号化通信技術を基盤とする。米国防高等研究計画局（DARPA）による資金援助を受けて開発が進められ、2002 年、同分散型ネットワークは多様な利益と信頼に基づ	Tor と類似した技術原理を用いて世界中に散らばる匿名開発者グループにより開発が進められている匿名通信ネットワーク。IP アドレス、送受信者情報、送信内容を全て匿名化することが可能であり、I2P ネットワーク上での匿名通信の実現をより重視した設計となっている。サーフェスウェブへの匿名

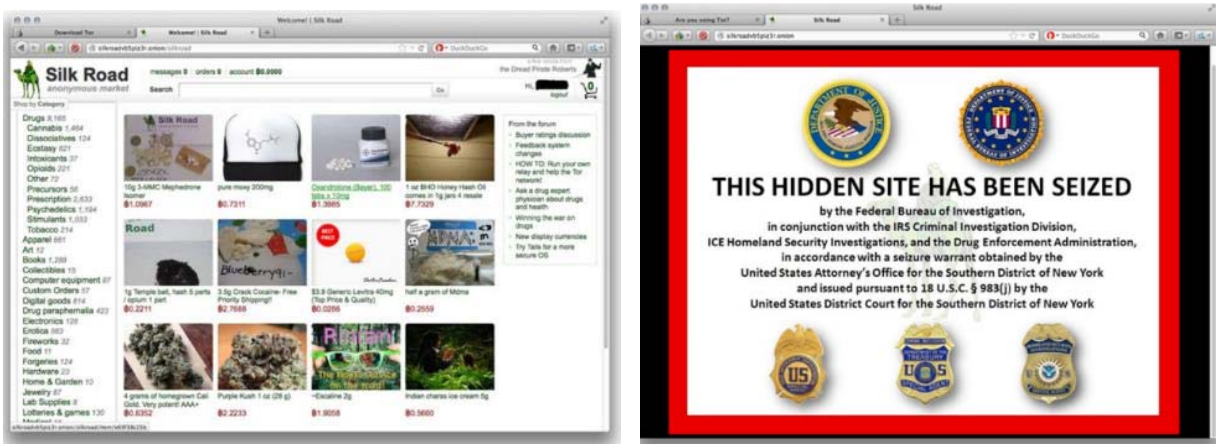
[9] https://freenetproject.org/author/freenet-project-inc.html
[10] https://www.torproject.org/
[11] https://geti2p.net/en/

	の活用は同通信ネットワーク上の情報保存と検索に限定されており、サーフェスウェブへの匿名アクセス機能はない。同ツールはこれまでに 200 万回以上ダウンロードされ、中国や中東諸国など、厳格なネット検閲体制を敷く国でのファイル共有や情報交換ツールとして用いられている	く媒体により運営される必要性があるとの認識に基づき、オープンソースとしてコードが公開され、2006 年に非営利機関（Tor Project, Inc.）となる。2008 年以降は Firefox ベースの Tor ウェブブラウザの開発も開始され、Tor ネットワーク内のウェブサイト（onion サイト）へのアクセスよりも、サーフェスウェブへの匿名アクセスを実現するツールとしての有用性が高まっている	アクセスも不可能ではないが、その機能は限定的である

出典：各種資料を基に作成

インターネット上における自由な情報発信やアクセス、プライバシー保護を目的に開発された匿名通信ツールの意図とは対照的に、「ダークウェブ」の存在が広く知られるきっかけを作ったのは、米連邦捜査局（FBI）が 2013 年に摘発し閉鎖に追い込んだ onion サイト上の大規模な闇市場「シルクロード（Silk Road）」である。2011 年に開設された同サイトで取引されていた違法商品・サービスの 70%はドラッグで、偽造運転免許証、盗難クレジットカード情報、児童ポルノなどが売買されていたほか、殺人依頼・受託の仲介までも行われており、FBI によると、2013 年 10 月にサンフランシスコで逮捕され 2015 年に終身刑の判決が下された同サイトの創設・運営者である Ross Ulbricht 氏は、サイトが閉鎖されるまでのわずか 2 年半の間に、同サイトを通じておよそ 12 億ドルの売上と 8,000 万ドルを仲介手数料として得ていたという。同サイトでは、決済手段として、匿名性の高い取引が可能な暗号資産のビットコインが用いられており、同資産の最初のユースケース事例としても話題を集めた[12]。

図表 4：違法 onion サイト「シルクロード（Silk Road）」の閉鎖前（左）と後（右）のメインページ



出典：Trend Micro

シルクロードの閉鎖後も違法ドラッグの販売を中心とする闇サイトが次々と出現し、身元の特定が困難な Tor が犯罪者により悪用されるケースは増え続けており、米国家安全保障局（National Security Agency：NSA）は、Tor を「非常に安全な低レイテンシの匿名化システムの頂点に立つツール（The king of high-secure, low-latency anonymity）」であり、同局の諜報活動の脅威とみなしている[13]。

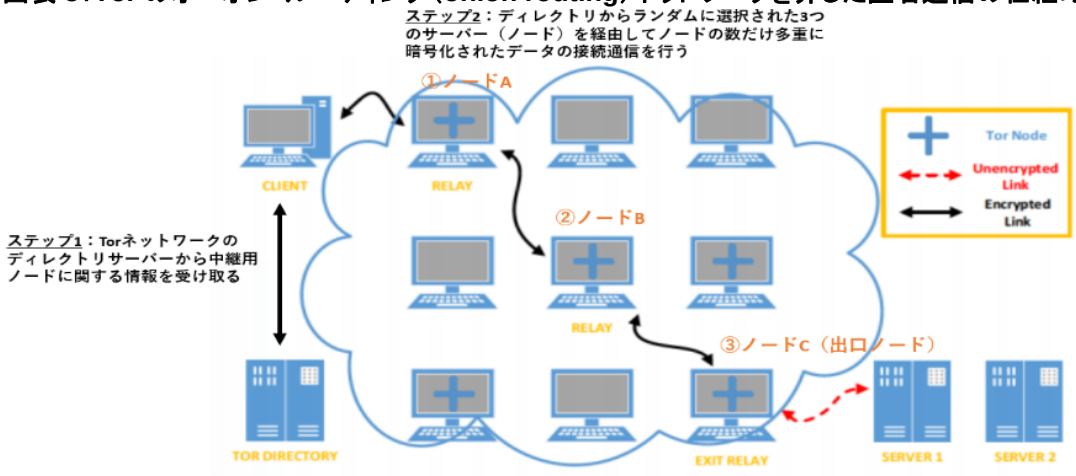
[12] https://www.hackersdenabi.net/deep-web-and-dark-web/、https://documents.trendmicro.com/assets/wp/wp-deepweb-and-cybercrime.pdf?_ga=2.44092964.1209765379.1578568892-1861512088.1578568892
[13] https://www.infoworld.com/article/2612232/report--nsa-has-little-success-cracking-tor.html

（3） 匿名通信を実現する「Tor」の仕組み

通常、インターネットに接続してウェブサイトへのアクセス等を行う場合、接続先（目的地）のサーバーに直接アクセス要求が出されアクセス元のユーザー情報（IP アドレス）が残る。これに対し、Tor の匿名通信では、世界中のボランティアが提供・運営するサーバー[14]から構成される P2P ベースの分散ネットワークを介してユーザーのトラフィックを最終目的地のサーバーに到達する前に複数のサーバー（ノード）をランダムに経由させ、接続経路を暗号化することでアクセス元の IP アドレス情報を秘匿し、送信者を追跡・特定しにくい仕組みを確立している[15]。

具体的には、図表 5 に示すように、Tor による通信を開始すると、まず Tor ネットワークのディレクトリサーバーと通信し、利用できる中継用ノードに関する情報を受け取り、ランダムに 3 つの中継ノードが選択される[16]。その後、中継ノードを介して行われる通信では、各ノード間の接続は暗号化されており、各ノードで宛先と送信データを取り出す復号処理を行って最後の中継用ノードである出口ノード（exit node）までデータが送信され、出口ノードでユーザーが送信した元の通信データを目的地のウェブサイトに送信する。目的地のウェブサイトのサーバーからみると、アクセス元は出口ノードの IP アドレスとなり、他の中継ノードの情報にはアクセスできないため、ユーザー情報は秘匿される。Tor ネットワークのこの仕組みは、ノードの数に応じでデータを多重に暗号化し、玉ねぎの皮をむくように、ノードを通過するごとに一つずつ復号化してデータを取り出すことから、「オニオン・ルーティング（onion routing）」と呼ばれる[17]。なお、Tor による通信は、出口ノードと最終的な目的地のウェブサイトのノードとの間は暗号化されていないため、HTTPS 通信などエンド・ツー・エンドで通信内容全体を暗号化する手法が用いられていない限り、通信内容を読み取られたり改ざんされたりする可能性がある。Tor は、通信内容ではなく、あくまで情報送信者の情報（IP アドレス）を秘匿することに重点を置いた技術である点に留意する必要がある[18]。

図表 5：Tor のオニオン・ルーティング（onion routing）ネットワークを介した匿名通信の仕組み



①ノードA：宛先情報と暗号化されたデータを取り出し、次のノードに暗号化データを中継する（送信元の情報としてユーザーのIPアドレスはみえるが元の通信データはみえない）
②ノードB：宛先情報、暗号化されたデータを取り出し、次のノードに暗号化データを中継する（元の通信要求データはみえず、送信元の情報はノードAのIPアドレスとなる）
③ノードC（出口ノード）：元の通信データを取り出し、最終的な宛先のウェブサーバーに当該データを送信する（ユーザーが送信した元の通信内容が露呈するが、送信元の情報はノードBのIPアドレスとなる）

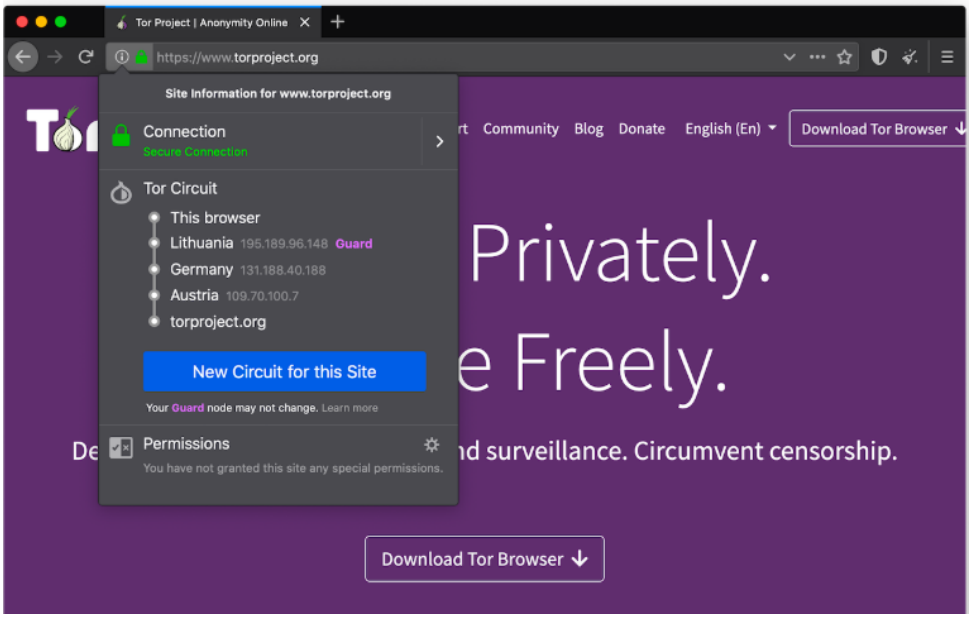
⇒目的地のウェブサイトのサーバーからみると、アクセス元は出口ノードのIPアドレスとなり、他の中継ノードの情報にはアクセスできないため、ユーザー情報は秘匿される

[14] 同サーバーは世界中に 6,000 以上存在する。https://metrics.torproject.org/networksize.html
[15] https://2019.www.torproject.org/about/overview.html.en
[16] 選択された中継ノードを介した接続経路は約 10 分ごとに変更される。
[17] https://blokt.com/guides/what-is-i2p-vs-tor-browser
[18] https://ccdcoe.org/uploads/2018/10/TOR_Anonymity_Network.pdf

出典：CCDCOE 等の情報を基に作成

Tor Project は、複雑な設定を必要とせず、誰もが容易に Tor ネットワークに接続できるようにするため、この機能を組み込んだ Firefox ベースのウェブブラウザ（Tor Browser）をインストールパッケージとして配布している[19]。現在同ブラウザは 32 言語に対応しているほか、2019 年 5 月には Android 向け Tor ブラウザも公式にリリースされている[20]。

図表 6：デスクトップ版 Tor ブラウザを用いてウェブサイトにアクセスした際の接続経路の表示例[21]



出典：Tor Project

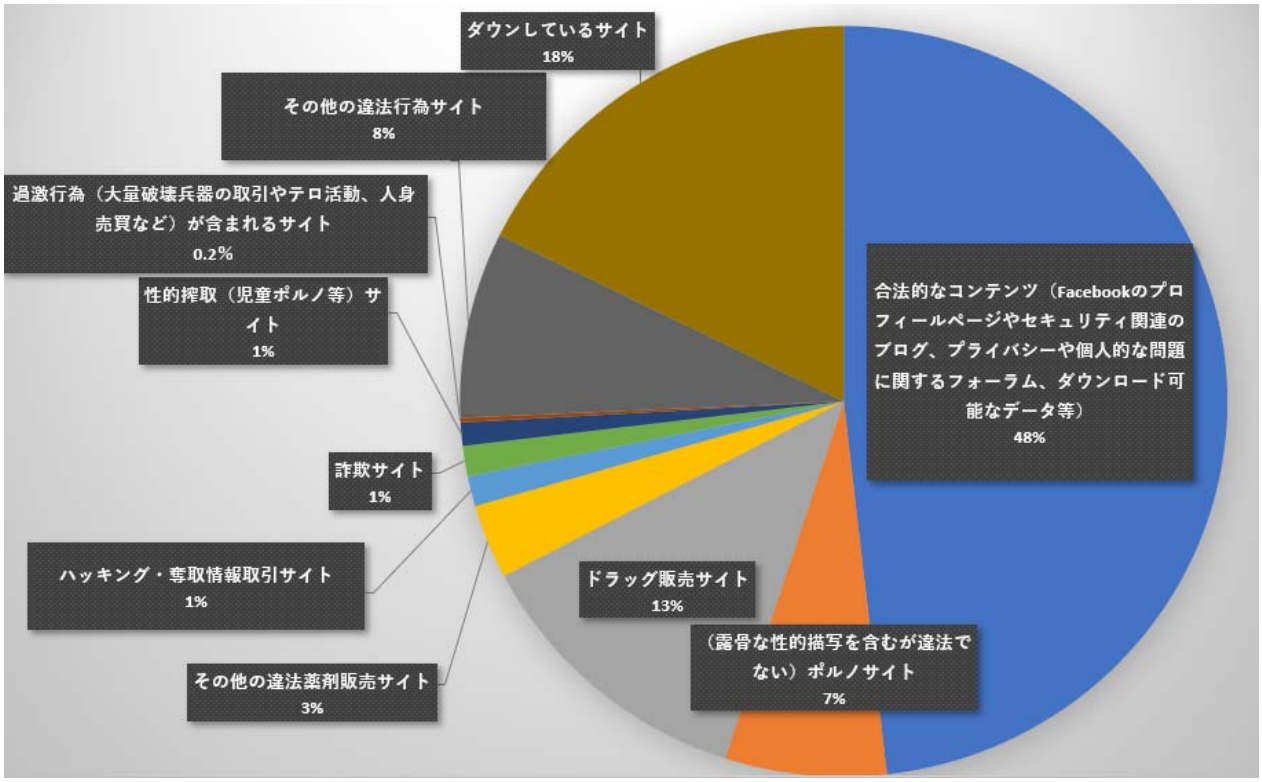
3　ダークウェブで提供されているサービスと利用規制に関する最新動向

（1）　ダークウェブで提供されている主なサービス

Tor の通信ネットワーク上に存在する onion サイト数は、現在 6 万 5,000 以上に上る[22]。近年、大規模な闇市場サイトの摘発・閉鎖がニュースメディアで度々取り上げられ、犯罪に悪用されるイメージが先行しているダークウェブであるが、米情報セキュリティ企業 Terbium Labs 社が実施した onion サイトのコンテンツに関する調査[23]によると、Facebook のプロフィールページやセキュリティ関連のブログ、プライバシーや個人的な問題に関するフォーラムのほか、（露骨な性的描写を含むが違法でない）ポルノサイトなど、合法的なコンテンツがこれらのサイトの半分以上（約 55%）を占めていたことが明らかになっている（図表 7 参照）[24]。

[19] https://www.torproject.org/download/
[20] https://www.zdnet.com/article/first-official-version-of-tor-browser-for-android-released-on-the-play-store/
[21] https://blog.torproject.org/new-release-tor-browser-90
[22] https://metrics.torproject.org/hidserv-dir-onions-seen.html
[23] これは、Terbium Labs 社が自社で開発した自動ビッグデータクローラー（crawler）を用いて、とある一日の間に収集した onion サイトのうち、400 のサイトをランダムに選択して調査を行ったもの。調査対象となった onion サイトのサンプルの大きさや闇サイトの流動性の高さから、同調査結果が必ずしも onion サイトの全貌を示すものではない点に留意する必要がある。
[24] https://btcmanager.com/whats-really-out-there-on-the-dark-net-terbium-labs-provides-some-answers/?q=/whats-really-out-there-on-the-dark-net-terbium-labs-provides-some-answers/&

図表 7：onion サイトに占める違法・合法コンテンツの割合



出典：Terbium Labs 社の調査結果データを基に作成

また同調査は、ダークウェブ（onion サイト）の違法コンテンツの中では、ドラッグとその他の違法薬剤取引に関するサイトがそれぞれ 45%、12%を占め、非常に多くなっている一方、大方のイメージに反し、大量破壊兵器の取引やテロ行為、人身売買といった過激行為に関するサイトの存在は非常に稀であることも明らかにしている[25]。

a. サイバー犯罪のエコシステムが構築されているダークウェブ

上述のように、ドラッグや武器、偽文書（偽造パスポート／免許証／札）、クレジットカードデータ等の個人情報、児童ポルノなど、様々な違法取引が横行していることで悪名高いダークウェブの闇市場であるが、2016 年に英国の脅威インテリジェンスソリューション企業 Intelliagg 社が発表したダークウェブのコンテンツに関する調査では、企業の漏洩データやクレジットカード情報を含む個人の金融資産に係るデータ、サイバー犯罪に用いられるツール・サービスを扱うサイトが onion サイト全体の 43%を占めていたことが判明しており[26]、サイバーセキュリティ業界では、世界でサイバー攻撃が増加し続ける[27]一因とみられている。

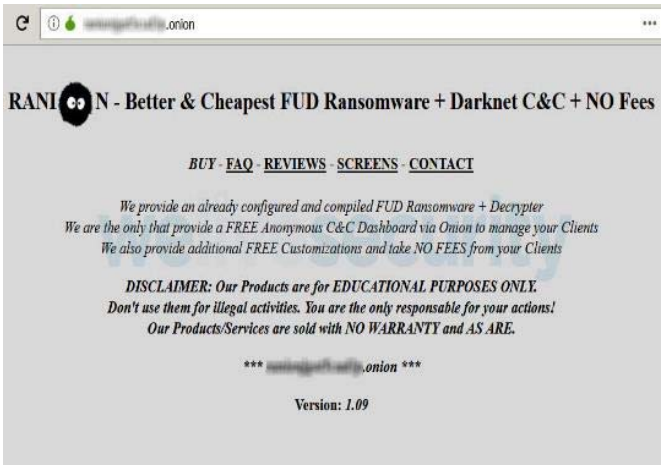
サイバー犯罪者は、サイバー犯罪に必要な商品又はインフラをダークウェブ上の闇市場で販売しており、こうした「サービスとしてのサイバー犯罪（cybercrime as a service）」ツールの例として、以下が挙げられる[28]。

- *サービスとしてのランサムウェア（ransomware as a service）*

[25] https://www.helpnetsecurity.com/2016/11/03/dark-web-legal/
[26] https://securityaffairs.co/wordpress/46202/deep-web/dark-web-mapping.html
[27] 米サイバーセキュリティ調査会社 Cybersecurity Ventures 社による最新のサイバー犯罪レポート（The 2020 Official Annual Cybercrime Report）によると、世界のサイバー犯罪による被害額は、2015 年の 3 兆ドルから、2021 年までに 6 兆ドル以上に達すると予想されている。https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/
[28] https://www.welivesecurity.com/2019/01/31/cybercrime-black-markets-dark-web-services-and-prices/

ダークウェブ上では、幅広いランサムウェアパッケージが販売されており、アップデートや技術サポート、C&C サーバー[29]へのアクセス等のサービスを支払いプランに応じて受けられる。「Ranion」は、こうしたランサムウェアパッケージの一例であり、月又は年単位でのサブスクリプション形式で 120～900 ドルで提供されており、ランサムウェアの実行ファイルに複数の機能を追加したプレミアムプラン（年間 1,900ドル）も用意されている。その他の販売モデルでは、マルウェアと C&C サーバーを無償提供し、攻撃により得られた報酬の一部を支払うモデルも存在する。

図表 8：ダークウェブ上で提供されているランサムウェア「Ranion」（上）とサブスクリプション形式の販売モデル（下）



-= PACKAGES COMPARISON =-

	Package #3	Package #2	Package #1	Package #ELITE
Subscription	1 Month	6 Months	12 Months	12 Months
Darknet C&C Dashboard	Yes	Yes	Yes	Yes
Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer	Yes	Yes	Yes	Yes
Offline Encryption	No	Yes	Yes	Yes
Support	No	Yes	Yes	Yes
Real-Time Client Manager	No	Yes	Yes	Yes
Dropper	No	Buy	Yes	Yes
Clone	No	Buy	Buy	Yes
FUD+Obfuscator	Buy	Buy	Buy	Yes
Unkillable Process	No	Buy	Buy	Yes
FUD Stub #	1	1	2	12
Price	120 USD	490 USD	900 USD	1900 USD

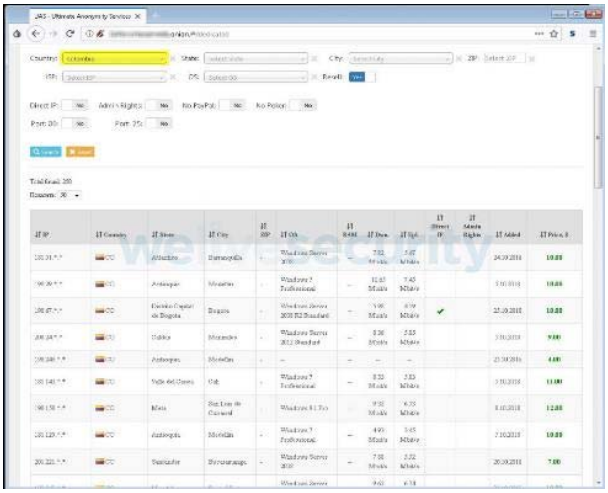
出典：WeLiveSecurity

- *サーバーへのアクセス情報*

[29] Command and Control Server の略で、サイバー攻撃において、マルウェアに感染したコンピューター群であるボットネットに命令を出したり制御したりする役割を担うサーバーを指す。

ダークウェブ上では、RDP（remote desktop protocol）を介して世界の様々な場所に設置されているサーバーにアクセスするためのログイン情報を販売する多様なサービスが提供されている。料金は各サーバーにつき 8～15ドルで、国や OS、ユーザーが利用した支払い手段ごとに検索可能であり、同アクセス情報を取得後、サイバー犯罪者はランサムウェアの実行のほか、バンキング型トロイの木馬やスパイウェア等の気づかれにくいマルウェアをサーバーにインストールするために用いる可能性がある。

図表 9：RDP を介したコロンビアのサーバーへのアクセス情報を販売するサイト

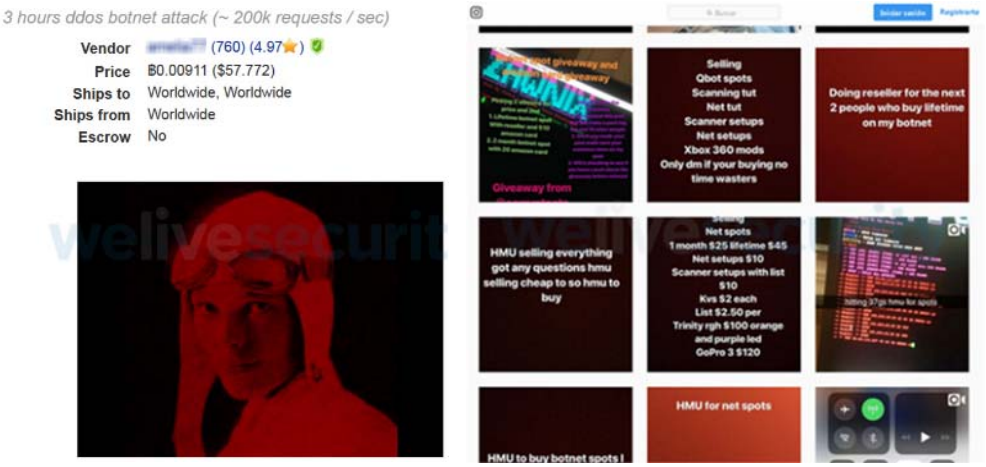


出典：WeLiveSecurity

- *インフラの貸与*

サイバー犯罪者の中には、ボットネット（マルウェアに感染したコンピューターネットワーク）を構築し、スパムメールの送信や DDoS（Distributed Denial of Service）攻撃の実行のためのコンピューター機能をダークネット上で貸し出す例もみられる。DDoS 攻撃の場合、料金は、攻撃の継続時間（1～24 時間）と、攻撃の間にボットネットが生成できるトラフィック量によって異なる。また、若年層のサイバー犯罪者を中心としたグループが、「Fortnite」のようなオンラインゲームで使用されるサーバーを攻撃することを主な目的として、独自に構築した（小型）ボットネットを貸し出すために SNS で積極的に売り込みを行う動きもみられる。

図表 10：3 時間約 60 ドルで DDoS 攻撃のインフラを貸与するサイバー犯罪者の例（左）と Instagram を用いてボットネット貸与の売り込みを行う匿名ユーザーの例（右）



出典：WeLiveSecurity

フィッシング攻撃などに成功したサイバー犯罪者は、盗んだアカウントを自ら利用することはなく、ダークウェブ上で他の犯罪者に転売する。ダークウェブには犯罪者が高い利益を上げ、安全にデータを取引するための仕組みが構築されており、オランダのネットワークセキュリティ会社 VPNOverview 社によると、ダークウェブでは、銀行のカード情報や PayPal、Amazon ギフトカード、モバイル決済サービス「Cash App」など、様々な個人の流出金融アカウント情報が取引されている[30]ほか、個人のソーシャルメディアのアカウント情報（販売額は 12.99 ドル～）や（氏名、住所、信用情報、電話番号を含む）個人情報（40～200 ドル）、銀行口座情報（50～200 ドル）なども多数販売されており、オンラインアカウントからの個人情報の流出リスクは高まっている。また闇サイトでは、スマートフォン向けビデオメッセージアプリ「Dubsmash」のデータベースから流出した 1,550 万人分のユーザーの電子メール及びパスワード情報が闇サイトで 4,500 万ドルの値で販売されるなど、企業のデータベースへのハッキングに伴う顧客情報の流出被害がますます深刻化している実態も明らかになっている[31]。

図表 11：闇サイトで取引されているハッキング被害に遭った主な企業のデータベース情報へのアクセス料金

DATABASE	PRICE	Category	RECORDS
ShareThis	$3,800	Web Plugin	1,900,000
500px	$2,800	Photography	206,000
Houzz	$4,500	Lifestyle	3,400,000
MyFitnessPal	$3,800	Lifestyle	50,000,000
MyHeritage	$3,200	Lifestyle	65,700,000
Dubsmash	$4,500	Entertainment App	15,500,000
YouNow	$3,200	Entertainment App	40,000,000
Armor Games	$900	Entertainment	7,800,000
Wanelo	$3,800	ecommerce	2,900,000

出典：VPNOverview

2017 年に発生した米信用情報サービス大手 Equifax 社の大規模な顧客の個人情報流出事件[32]を受けて企業の IT セキュリティ管理を見直す動きが高まる中、米グローバル情報企業の Experian 社は、流出した個人情報対策として闇サイトで取引される個人情報を検知し被害を最小限に抑制するためのダークウェブモニタリングサービス[33]をアメリカでいち早く開始している。その後、Norton 社[34]をはじめとする大手セキュリティ企業が相次いで同様のサービスを立ち上げ、メディアの注目を集めている。しかし、これらのサービスについては、ダークウェブ上のあらゆるサイトをスキャンすることは実質的に不可能であることや、流出情報が検知されてもその販売取引や不正利用を未然に防ぐことは非常に困難であることに留意する必要があり、専門家の中には、組織内のあらゆるデータを暗号化したり従業員に対するリスク教育を強化したりするなどの対策を講じる方がより有効とみる声もある[35]。

[30] こうしたアカウント情報は、一般的に、アカウント残高のおよそ 10%の金額で取引されている。
[31] https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/
[32] ハッキングにより、1 億 4,700 万人分の顧客の社会保障番号等の機密個人情報が流出した事件で、Equifax 社は 2019 年 7 月、最大 7 億ドル（この内 4 億 2,500 万ドルはデータ流出被害に遭った消費者への補償に充てられる）を支払うことで連邦取引委員会（FTC）と和解している。https://www.cbsnews.com/news/equifax-lawuit-settlement-how-to-claim-your-share-of-700-million-ftc-penalty-for-equifax-data-breach/
[33] https://www.experian.com/consumer-products/free-dark-web-email-scan.html
[34] https://us.norton.com/feature/dark-web-monitoring
[35] https://www.kaspersky.com/blog/secure-futures-magazine/dark-web-monitoring/29084/

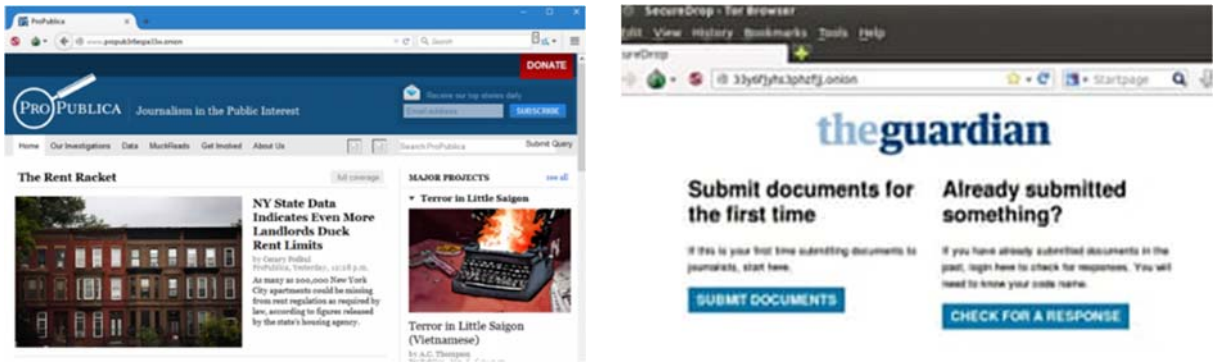
b. Tor ネットワークにおける合法サイトの例

犯罪者が違法商品を取引する闇市場やサイバー犯罪の巣窟としての危険なイメージが強くなりつつあるダークウェブであるが、匿名通信ツールの本来の開発の意図に沿って、圧政下の国でネット検閲により言論の自由を奪われた人々の匿名かつ安全な通信や、インテリジェンス情報（秘匿情報）の通信を実現するために提供されているサイトを含め、ダークウェブ上には合法的なサイトも多数存在する[36]。.onion ドメインで提供されているこうした合法的なサービスには、主に以下が挙げられる。

- *ニュースメディア／匿名情報投稿サイト*

Tor ネットワークには、米独立系非営利報道機関の Propublica が 2016 年 1 月、厳しいネット検閲体制を敷く中国などの国からの読者の情報アクセスの自由と安全を守るため、大手ニュースメディアとして初めて公式サイト（propub3r6espa33w.onion）を立ち上げており[37]、その後 2017 年 10 月には米紙 The New York Times も公式サイト（https://www.nytimes3xbfgragh.onion）を開設[38]、2019 年 10 月には英公共放送局 BBC もミラーサイト（bbcnewsv2vjtpsuy.onion）を開設[39]するなど、独立した信頼できるニュースの配信を提唱する大手報道機関が同様の動きを見せている。また、これらのニュースメディアを含む世界の 50 以上の報道機関は、オープンソースの匿名情報投稿システム「SecureDrop[40]」を活用し、内部告発者から機密情報・文書を安全にやり取りするための匿名情報投稿サイトを Tor ネットワーク上に有している[41]。

図表 12：ProPublica の onion サイト（左）と英紙 The Guardian の「SecureDrop」を介した情報投稿サイト（右）



出典：PCWorld[42]、The Guardian[43]

- *SNS*

ダークウェブ上の SNS サイトでは、Facebook 社が 2014 年 10 月以降、Tor ユーザーが Facebook のデータセンターと直接通信し、より安全に Facebook ページ（https://facebookcorewwwi.onion）にアクセス[44]できるようにしている。これは、通信規制により Facebook へのアクセスがブロックされている中国などのユーザーに新たなアクセス手段を提供するもので、運用開始からおよそ 2 年が経過した 2016 年 4 月時点で、Tor を用いて Facebook ページにアクセスしているユーザー数は月間 100 万人を超えている[45]。

---

[36] https://www.technadu.com/legal-dark-web-activities/52348/
[37] https://www.propublica.org/podcast/why-propublica-joined-the-dark-web
[38] https://open.nytimes.com/https-open-nytimes-com-the-new-york-times-as-a-tor-onion-service-e0d0b67b7482
[39] https://www.bbc.com/news/technology-50150981
[40] https://securedrop.org/overview/
[41] 米コンピュータープログラマーAaron Swartz 氏らにより開発され、2013 年の Swartz 氏の死後、非営利団体 Freedom of the Press Foundation が同ツールの開発プロジェクトの運営を担っている。
[42] https://www.pcworld.com/article/3020215/propublica-joins-the-dark-web-with-onion-version-of-news-site.html
[43] https://www.theguardian.com/technology/2014/jun/05/guardian-launches-securedrop-whistleblowers-documents
[44] 実装にあたり、Facebook 社は HTTPS（新たな暗号レイヤ）を追加している。
[45] https://www.zdnet.com/article/one-million-people-are-accessing-facebook-each-month-in-secret/

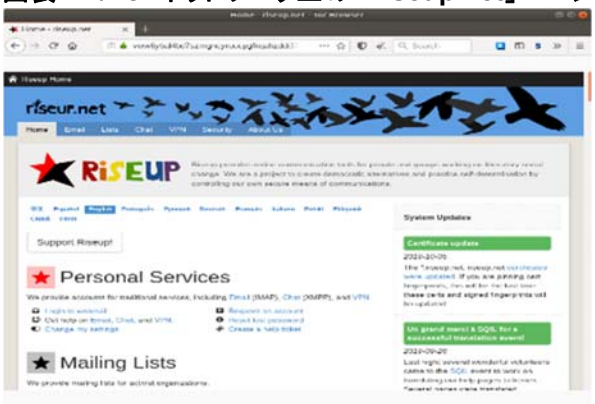
図表 13：Tor ネットワーク上の Facebook ページ

出典：ZDNet

- *電子メール*

Tor ネットワーク上には、ジャーナリスト、社会運動家、反体制活動家、内部告発者、政府関係者たちが匿名で安全にメッセージのやり取りができるようにいかなるサード・パーティも介在しない、ProtonMail（protonirockerxow.onion）、Torbox（torbox3uiot6wchz.onion）、Bitmessag（bitmailendavkbec.onion）、Mail2Tor（mail2tor2zyjdctd.onion）などのセキュリティ面で定評のある電子メールサービスを提供するプロバイダーが複数存在する[46]。これらのプロバイダーの中でも、1999 年にシアトルで開催された第 3 回世界貿易機関（WTO）閣僚会議に対する大規模なプロテスト後に、社会運動家を対象としてサービスの提供が開始されたオンラインコミュニケーションツール「Riseup.net」はユーザーの IP アドレスを記録として残さずあらゆるデータを暗号化して保存する安全な電子メール／チャット／ファイル交換ツールとして知られ、onion サービス（vww6ybal4bd7szmgncyruucpgfkqahzddi37ktceo3ah7ngmcopnpyyd.onion）の提供も行っており、これまで 600 万人以上のユーザーに活用されている[47]。

図表 14：Tor ネットワーク上の「Riseup.net」ページ



出典：ExpressVPN

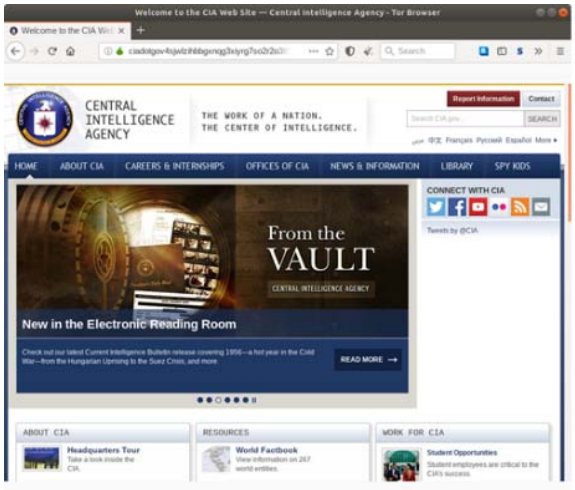
- *インテリジェンス情報の収集*

米中央情報局（Central Intelligence Agency：CIA）は 2019 年 5 月、Tor ネットワーク上に同組織の公式ウェブサイト（ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion）を開設した[48]。CIA の

[46] https://freedomhacker.net/list-of-secure-dark-web-email-providers-in-2016-4946/
[47] https://blog.torproject.org/tor-heart-riseupnet、https://www.expressvpn.com/blog/best-onion-sites-on-dark-web/
[48] https://www.cia.gov/news-information/featured-story-archive/2019-featured-story-archive/latest-layer-an-onion-site.html

onion サイトで提供されるコンテンツは、CIA に情報提供を行う方法などの解説を含むサーフェスウェブ上の CIA の公式ウェブサイトと全く同じ内容である。CIA の広報担当ディレクターBrittany Bramell 氏は、onion サイト立ち上げの理由について、「我々の世界的任務の達成には様々な個人が場所を問わず安全に情報にアクセスできるようにすることが必要である」と述べ、匿名筋からの情報収集活動を拡大することが主な狙いであるとしている[49]。.

図表 15: CIA の公式 onion サイト

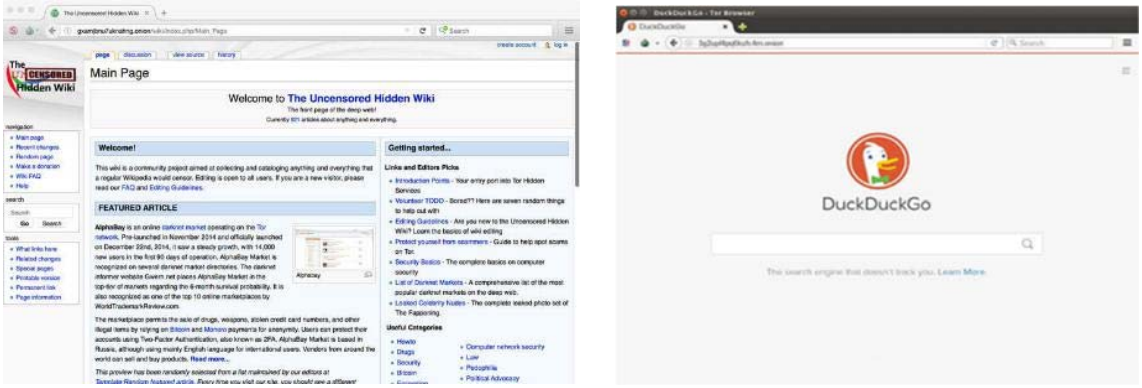


出典：ExpressVPN

- *ダークウェブ上にあるサイト検索*

ダークウェブでは、通常のウェブサイトのようにインデックス化されておらず、長く複雑な URL が用いられており、特定のウェブサイトを見つけ閲覧することは容易でない。そのため、ユーザーの間では、Tor ネットワーク上におけるウェブサイト検索ツールとして、ウィキペディア（Wikipedia）によく似たサイト設計で、ダークネットで閲覧できる onion サイトのあらゆるリンク情報がカテゴリ別にリスト[50]されている「Hidden Wiki（http://zqktlwi4fecvo6ri.onion）」や、プライバシー保護の観点からユーザーの個人情報収集及びウェブ閲覧履歴を追跡しない検索エンジン「DuckDuckGo（https://3g2upl4pq6kufc4m.onion/）」等が用いられている[51]。

図表 16:「Hidden Wiki」及び「DuckDuckGo」の onion サイトページ



出典：Wondershare

[49] https://www.wired.com/story/cia-sets-up-shop-on-tor/
[50] リンク切れの情報や詐欺サイト、違法サイト情報も多数含まれている。
[51] https://drfone.wondershare.com/dark-web/tor-search-engine.html

- *科学論文の無料共有*

「Sci-Hub」は、科学論文誌の購読費用の高さに不満を抱いたカザフスタンの研究者 Alexandra Elbakya 氏が、あらゆる科学論文を誰もが無料でダウンロードできるようにするため 2011 年に開設された世界最大規模の海賊版科学論文サイトで、現在 7,800 万本以上の論文が公開されている[52]。同サイトは、人間社会で知識の拡散を妨げる全ての障壁を取り除くことをミッションとして同活動を支えるユーザーコミュニティの献金を基に運営され、科学コミュニティの賞賛を得る一方、同サイトは 2015 年と 2017 年、アメリカの学術出版社により著作権侵害で訴えられ、サイトの閉鎖と賠償金支払いを命じられている[53]。Sci-Hub は同判決を受け、サーフェスウェブ上のサイトは新たなドメイン名を取得することで運営を継続しており、米地方裁判所は 2018 年 4 月、Sci-Hub が現在及び将来的に取得している（する）全てのドメインの利用を差し止める命令を下したが、アメリカ国外のドメイン登録業者の中には同判決に従っていないケースもあるほか、ドメインの取得を管理する機関が存在しない Tor ネットワーク上の Sci-Hub サイトは当面は継続運営される見込みである[54]。

図表 17：Tor ネットワーク上の「Sci-Hub」ページ

出典：ExpressVPN

（2） ダークウェブの利用規制に関する主な動き

a. ダークウェブにおける闇市場の取り締まりを巡る状況

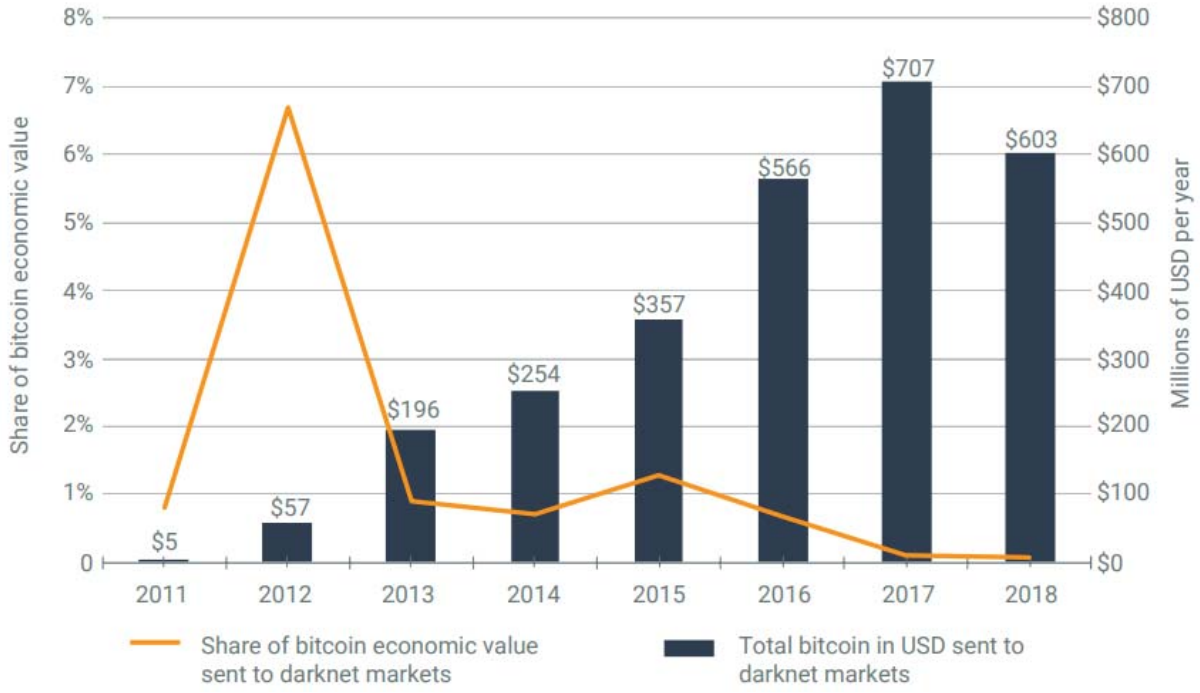
法執行機関は、国境を超えたサーフェスウェブ上のサイバー犯罪への対応においても既に多数の課題を抱えているが、ダークウェブでは、①監視・検閲から逃れるために暗号機能が用いられていること、②世界中にある複数のサーバーをランダムに経由するネットワーク設計となっており犯罪者の特定が困難なこと、③闇市場サイトは URL を定期的に変え情報収集が容易でないこと、の 3 つの点が違法サイトの取り締まり捜査をさらに難しくしている[55]。これまでに欧米の法執行機関が特定した闇サイトの数は 100 以上に上っており、2013 年 10 月のシルクロード閉鎖を皮切りに、FBI 及び欧米の捜査当局は、「シルクロード 2.0」、「AlphaBay」、「Hansa」を含む複数の大規模な闇市場の摘発・閉鎖にも成功している[56]。

[52] https://www.sciencemag.org/news/2016/04/frustrated-science-student-behind-sci-hub
[53] http://www.sciencemag.org/news/2017/11/court-demands-search-engines-and-internet-service-providers-block-sci-hub
[54] https://torrentfreak.com/publisher-gets-carte-blanche-to-seize-new-sci-hub-domains-180410/
[55] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/qna-deep-web-anonymity-and-law-enforcement
[56] 捜査当局が摘発・閉鎖したサイトも含まれる。
http://www.emcdda.europa.eu/system/files/publications/12078/20192630_TD0319332ENN_PDF.pdf

これまで、アメリカ及び欧州諸国の法執行機関によるダークウェブにおける違法な取引活動を取り締まる努力が精力的に進められており、捜査当局のテクノロジーを駆使したダークウェブの犯罪取り締まりに関する捜査技術は着実に進化しているとみる声もある[57]。しかし、暗号資産の不正な取引活動を監視するソリューションを手がける米 Chainalysis 社によると、ダークウェブにおける闇市場へのビットコイン流入額は 2013 年以降も増加傾向にあり、2017 年には 7 億ドルを超える過去最大の取引額を記録する（図表 18 参照）など、闇市場は拡大傾向にあるという[58]。

ダークウェブにおける闇市場へのビットコイン流入額は 2018 年に 6 億ドル程度に減少しているが、これには、米司法省（Department of Justice）と欧州刑事警察機構（Europol）が協力し、2017 年 7 月にダークウェブ上の 2 つの大規模な闇市場サイトである AlphaBay 及び Hansa を閉鎖に追い込んだ[59]ことが影響している。しかし、闇市場の活動は両サイトの閉鎖直後こそ 60%の落ち込みを示したが、2018 年に入ってから徐々に回復し、同年末には 1 日当たり 200 万ドルの取引額を記録するまでに戻っている（2018 年当初と比較すると 2 倍の取引高を記録）。Chainalysis 社は、この背景には、AlphaBay や Hansa で行われていた取引の多くが、ロシア語の闇市場サイト大手「Hydra」など別のサイトに移行したことが影響しているとし、法執行機関による闇市場サイトの取り締まり活動は、大規模な闇市場サイトを摘発・閉鎖しても後継の闇市場サイトが次々と出現・成長し、取引が別のサイトに単に移行していくだけの「モグラ叩きゲームのような状態」と表現している。

図表 18：ダークウェブにおける闇市場へのビットコイン流入額の推移



出典：Chainalysis

[57] https://matthiasgruber.ch/the-dark-net-an-unknown-terrain/
[58] https://blog.chainalysis.com/2019-cryptocrime-review
[59] 最大の闇市場サイト AlphaBay だけで、20 万人以上の顧客を有し、違法薬物を含む 10 万以上の違法商品の取引が行われ、サイト閉鎖直前には 10 億ドル以上の売上を上げていたとみられている。https://www.cnet.com/news/alphabay-hansa-shutdown-closed-dark-web-market-silk-road/

b. ダークウェブの利用規制動向

仮想プライベートネットワーク（VPN）や Tor は、ユーザーのプライバシー及び匿名性を保護する強力なツールである。しかし、ロシア、中国、ベラルーシ、イラン、イラク、オマーン、アラブ首長国連邦（UAE）、トルコ、ベネズエラなど、世界的にもインターネット規制が厳しい国の中には、VPN（及び Tor）の利用をブロックする技術を導入したり、こうしたツールの利用を禁止する法律を制定したり、その利用規制を強化している[60]。中でも、中国及びロシア政府は、VPN や Tor などの匿名ネットワークの利用を近年厳しく制限しており、中国では 2017 年 1 月、政府が閲覧を認めていないウェブサイトやサービスへのアクセスをブロックしている政府の承認を受けた VPN 以外の全ての VPN 接続サービスの利用を禁止する規制通達を行っている。また、ロシア連邦議会も同年 7 月、ネット検閲を回避できるソフトウェアを提供するサイトなど、政府がアクセスを禁止しているウェブサイトをブロックしていない VPN や Tor などの匿名ネットワークサービスの利用を禁止する新法案を全会一致で可決している[61]。

図表 19：VPN（及び Tor）の利用をブロックする技術を導入している又は利用を禁止する法律を制定している世界の国々

※国内での VPN の利用に政府が反対の立場をとるその他の国には、北朝鮮、エジプト、ベトナム、バーレーン、トルクメニスタン、ミャンマー、シリア、リビアが挙げられる。

出典：ProtonVPN

ダークウェブに関するあらゆる規制は、サーフェスウェブ、ディープウェブを含むインターネット全体に適用されるため、ダークウェブのみを個別に切り離して規制することは不可能である。アメリカでは、ダークウェブ対策を考える上で、匿名性を担保することでユーザーのプライバシーや言論の自由を保護しながら、オンライン上における犯罪行為をいかに防止するかが大きな課題となっている。ジョージ・W・ブッシュ米元大統領の下で国土安全保障長官を務め、米リスク管理／サイバーセキュリティコンサルティング会社 Chertoff Group 社の共同創設者である Michael Chertoff 氏は、法執行機関による最も効果的かつ合理的なダークウェブ対策は、無作為にあらゆる匿名ユーザーの身元を特定しようとするのではなく、2015 年に摘発された

[60] https://protonvpn.com/blog/are-vpns-illegal/
[61] https://www.theregister.co.uk/2017/07/11/russia_china_vpns_tor_browser/

児童ポルノサイト「Playpen」の例[62]のように、ダークウェブ上で違法行為を犯しているユーザーのみを対象としてその身元を割り出すことが将来的な犯罪の抑止につながると指摘する[63]。

欧米諸国では、主要法執行機関が相互に協力し、ダークウェブ上の違法サイトの摘発及び取り締まりを強化しているが、こうした取組みと同時に、闇市場の拡大を助長している暗号資産取引に対する規制の厳格化を世界的に求める動きが高まっている。2018 年 3 月にアルゼンチンで開かれた 20 か国財務大臣・中央銀行総裁会議（G20）では、暗号資産規制について初めて議論され、暗号資産を用いたマネーロンダリング（資金洗浄）やテロ資金対策が大きな焦点となり、これらの問題に対する国際基準を策定している金融活動作業部会（Financial Action Task Force：FATF）に暗号資産に適用される基準の見直しを求めることで合意した[64]。この要請を受けて FATF は 2019 年 6 月、暗号資産の取引所などに対し、送金者の名前、口座番号、所在地や受取手の名前と口座番号といった情報を収集・共有するよう求める内容の新ガイドライン（Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers）を発表した[65]。同ガイドラインの発表後に大阪で開催された G20 首脳会合（G20 Summit）では、同ガイドラインを支持し従う内容の公式声明が出されたが、業界では、世界的に同ガイドラインを遵守するには莫大なコストとこれまでにない国際連携が必要になるとし、懸念を示す声も上がっている[66]。

4　今後の展望と日本への示唆

コンピューターセキュリティウェブサイト Precisesecurity.com が最近実施したダークウェブを用いて匿名でオンライン活動を行っている世界のユーザーに関する調査によると、ダークウェブを日常的に（毎日又は毎週）利用しているユーザーの割合は北米地域で最も多く、特に毎日ダークウェブを利用するユーザーの割合は全体の 26%に上ることが明らかになっている（図表 20 参照）。

図表 20：世界のダークウェブユーザーのダークウェブへのアクセス頻度（地域別）

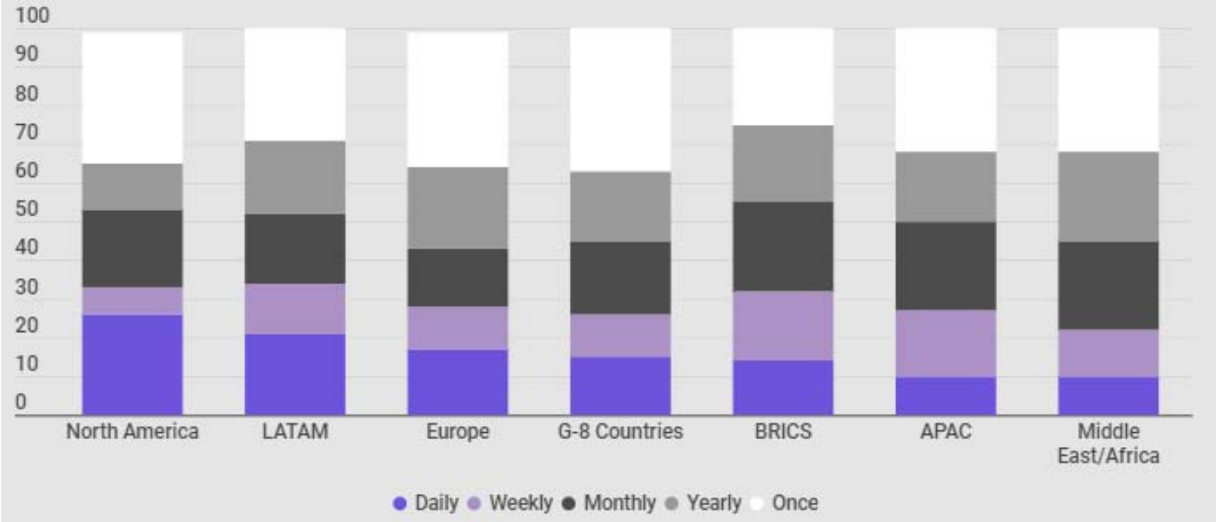
[62] FBI は 2015 年 2 月、Tor ネットワーク上の大規模な（サイト開設後 1 年で 21 万 5,000 アカウント登録され、週間ユニークビジターは 1 万 1,000 人に上っていた）児童ポルノサイト「Playpen」を摘発した。しかし FBI はこれを公表せず、押収したサーバーに同サイトにアクセスしようとするユーザーの IP アドレスを特定するためのハッキングツールを仕掛けた上でサイトを 12 日間にわたり継続運用、同期間にサイトにアクセスした約 1,000 人の身元を特定することに成功している。

[63] https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1298643

[64] https://cointelegraph.com/news/g20-and-cryptocurrencies-baby-steps-towards-regulatory-recommendations https://cointelegraph.com/news/g-20-summit-results-crypto-is-important-for-global-economy-needs-to-be-regulated-and-taxed

[65] https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

[66] https://www.theblockcrypto.com/linked/29632/g20-officially-supports-fatfs-crypto-guidelines-that-require-exchanges-to-share-customer-data



出典：Precisesecurity.com

アジア太平洋（APAC）地域におけるダークウェブの利用率は欧米その他の地域と比較すると低いが、ダークウェブ上の犯罪者による潜在的な脅威やリスクも低いというわけではない。日本においては、2018 年はじめに暗号資産交換業者のコインチェック社から流出した 580 億円分の暗号資産「NEM」がダークウェブ上で売買されていた[67]ことや、2019 年 5 月にも国内のインターネット関連企業から流出した顧客の個人情報がダークウェブ上の闇サイトで取引されていた事件[68]、同年 7 月に京都のアニメ制作会社（京都アニメーション社）で起きた放火殺人事件において、公式サイトへの殺害予告や脅迫の書き込みに Tor が用いられていた[69]ことなど、ダークウェブの匿名性を悪用した犯罪ニュースが目を引くようになっている。2020 年夏の東京五輪を前に、サイバーテロなどの犯罪に危機感を抱く企業ニーズが増え、複数のインターネットセキュリティ企業がダークウェブ調査サービスの提供を開始[70]したり、警察庁も 2018 年 1 月よりダークウェブの実態調査に着手[71]したりするなど、ダークウェブ上のサイバー犯罪対策を強化しているが、その取組みは米英と比べるとまだまだ遅れているとみる声もある[72]。デジタル化の進展により、今後サイバー空間と現実世界の境界がますます曖昧になり、ダークウェブの悪用リスクも高まることが見込まれる中、こうしたリスクに備えるための対策・体制づくりが求められる。

他方で、Tor 及びダークウェブを利用する理由として最も多かったのは「匿名でいられるから」であり、特に中東地域やアフリカ地域、BRICS（ブラジル、ロシア、インド、中国、南アフリカ共和国）地域のユーザーは、「自国でアクセスできないウェブコンテンツを閲覧できるため」や「政府のネット検閲を回避するため」及び「オンラインプライバシーの保護」を主な理由として挙げる一方、北米ユーザーは、「インターネット企業からプライバシーを保護するため」や「外国の政府からプライバシーを保護するため」といった理由を主に挙げており[73]、検閲の回避やプライバシーの保護の高まりがダークウェブの利用が進む可能性が考えられる。

ニューヨーク市立大学工科校で准教授を務める中村正人氏は次のように述べている。「コンピューターの世界においては、並列計算機やベクトル計算機の戦いの後、クラウドコンピューティングや GPU による汎用計算を経て、現在世界の目は量子コンピューティングに向かっている。同様に、ウェブの世界においても、ウェ

[67] https://www.yomiuri.co.jp/fukayomi/20180308-OYT8T50016/
[68] https://www.sankeibiz.jp/compliance/news/190515/cpd1905150650001-n1.htm
[69] https://www.sankei.com/affairs/news/190727/afr1907270023-n1.html
[70] https://www.itmedia.co.jp/business/articles/1805/02/news083.html
[71] https://www.nikkei.com/article/DGXMZO26246310Y8A120C1000000/
[72] https://www.siemple.co.jp/darkweb-monitoring/news/131/
[73] https://www.precisesecurity.com/articles/more-than-30-of-north-americans-used-dark-web-regularly-in-2019/

ブの表層の 4%だけでなく、ダークウェブを含め残りの 96%とそれに関連するテクノロジーが急速に独占・寡占されることが起こり得る。」

※ 本レポートは、その内容に関する有用性、正確性、知的財産権の不侵害等の一切について、執筆者及び執筆者が所属する組織が如何なる保証をするものでもありません。また、本レポートの読者が、本レポート内の情報の利用によって損害を被った場合も、執筆者及び執筆者が所属する組織が如何なる責任を負うものでもありません。