ダークウェブサイトとTorネットワークに対する正しい認識

東京理科大学　創域理工学部　情報計算科学科　教授　明石（あかし）　重男（しげお）

1．サイバーセキュリティの教育方法について

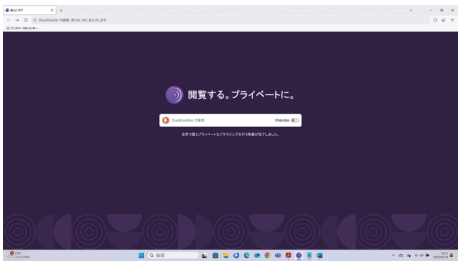
インターネットを基盤とする情報化社会は、功罪両方の側面を持っています。良い面としては、色々な意味で私達を助けてくれて、生活を楽にしてくれる優秀なアシスタントですが、悪い面としては、知らないうちに、私達に危害を加える道具となる場合があります。

Tor は、そもそも米国海軍が作成したネットワークで、無実の政治犯等が、逃亡を続けながら情報発信をするための道具として開発されたネットワークでした。「情報発信源元が特定されない」という、ある意味で特殊な機能を持つこのネットワークは、残念なことに、違法薬物や軍事兵器等の販売に使用される環境となっていることは事実です。私達は、インターネットの「功」としての側面を使用する以上、「罪」としての側面にも向かい合う必要があります。そのためには、どのような点が危険なのか、という現実を知っておく必要が無ければ、正しい防御方法を取得することは不可能であると思われます。そこで本稿では、Tor ブラウザに焦点を当てて、あまり議論されることの無い「Tor ネットワーク」が危険とみなされる理由を明確にします。

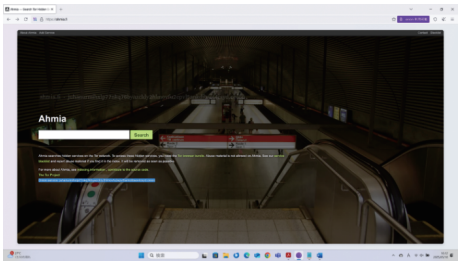
2．ダークウェブサイトへのアクセス

私たちが普段 Yahoo や Google を使って表示される検索結果は、「表層ウェブ」と言われており、全ウェブサイトの中で、わずか 1%しか存在しないと推定されています。逆に検索結果に表示されない 99%のサイトは「深層ウェブ」と言われており、具体例として、学術論文や会員制のサイトが存在します。検索エンジンは「クローラー」というプログラムでネット上を巡回して検索結果を表示していきますが、深層ウェブは、そのセクションに特殊なタグを追加しているため、クローラーによる巡回を回避しています。この深層ウェブの領域の一部に存在するのがダークウェブであり、URL に「.onion」という拡張子がつけられています。更に、「何層にもわたる情報の暗号化」による高い匿名性を維持した「オニオンルーティング」と呼ばれる通信が、国によるインターネット検閲を回避することを可能にしており、政治的迫害を受ける人達の継続的情報発信を実現しています。

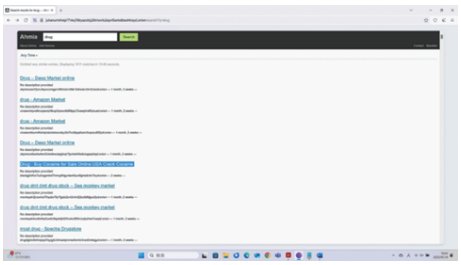
【図１】は、Tor ブラウザ起動時の初期画面を表示しています。通常、Tor ブラウザは、検索エンジンとして DuckDuckGo を使用しますが、近年注目を集めて、裏サイト取り締まりの際に、検索上位サイトを調査するという利用法が確立されたために、あまり上位に違法サイトが登ってこないです。当然ですが、裏サイト管理者も、このような状況を把握しているため、今回は、ahmia という検索エンジンを用いることにします。通常は、https::/ahmia.fi/ で繋がるのですが、直接リンクが存在するので、以下のリンク：http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion で検索をかけると、【図２】のような画面が表示されます。上記直接リンクは、ダークウェブサイトのみ有効な URL であり、通常のブラウザではアクセス不可能です。その理由は、Tor ネットワークの名前解決に不可欠な「.onion」という拡張子が含まれているためです。次節では、違法薬物販売サイトへのアクセスを行います。



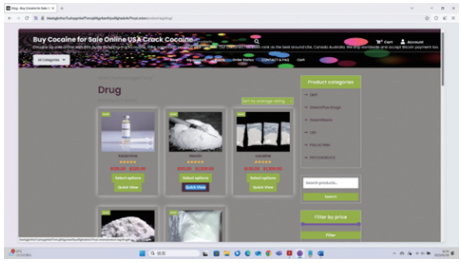
【図１】Tor ブラウザ起動時初期画面



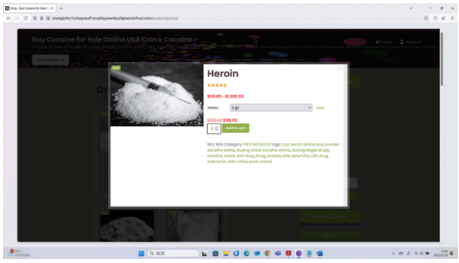
【図２】検索エンジン Ahmia 起動時初期画面



【図３】検索エンジン Ahmia による drug 検索リスト



【図4】検索上位薬物販売サイトの初期コンテンツ



【図5】drug 販売サイトで薬物を選択した画面

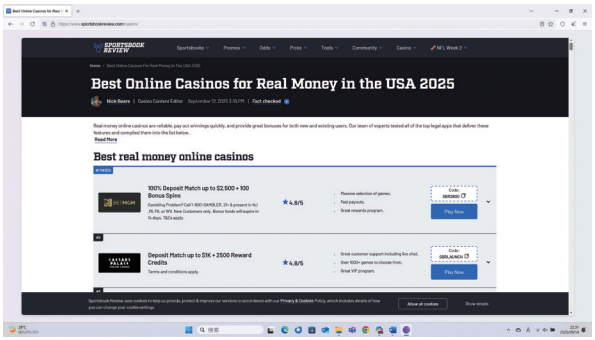
【図6】ダークウェブへの Edge によるアクセス結果

3．ダークウェブ drug 販売サイトへのアクセス

続いて、前節の【図2】の画面で、drug というキーワードを入力してみます。すると、【図3】のような画面が得られます。これは、検索上位に位置する drug 販売サイトリストです。そこで、青色でマーカー表示した「クラック・コカイン」と書かれているリンクをクリックしてみますと、【図4】のような特定の drug 販売サイトへと移動します。更に、選択したサイトで、「どの drug を購入するか」という問いかけに対して、「ヘロイン」を選択した状況を表示したものが、【図5】に相当します。ここから先をクリックすると、個人情報入力を求める支払い画面に進みます。例えば、自宅でこのような作業を行う場合、契約している ISP を経由するため、「たとえ購入しなくても、」ISP に個人情報を残すことになるため、警察は、この時点で使用した IP アドレスに基づいて、違法薬物購入者の特定を実施することになります。

なお、商品購入情報を入力する以下の画面の URL：http://blackgjlz4hzr7uzlvpgmbef7nmujdl4gy4ae4hjus5lghadz4e7hryd.onion/product-tag/drug/ を Microsoft Edge ブラウザや Google Chrome ブラウザ等で閲覧を試みても、上記、サーバサイトに到達できません。Edge の場合、【図6】の画面が表示されます。更に、【図6】の画面に表示されているリンクをクリックしても、drug 販売サイトとは無関係の検索結果が表示されます。この事実は、Edge や Chrome が、深層ウェブに属するダークウェブへのアクセスを許可していないことの証明となっています。

別項目として、最近話題の online casino を提供する海外のウェブサイトの検索結果を【図7】に示します。



【図7】海外運営される online casino 検索上位サイト

4．残されたいくつかの疑問

本節では、「論理的に考えてみると、理由が分からない」という質問に対する回答を与えたいと思います。

質問１：何故、Tor がダークウェブサイトにアクセス可能なのに、Microsoft Edge や Google Chrome では、アクセス不可能なのですか？

回答１：違法薬物をネット販売するサイトは、当然身元（＝販売ウェブサイトに供給された IP アドレス）を秘匿することを望んでいます。そのために Tor ネットワークを利用します。このため、ウェブサイトの拡張子である「.onion」を使用することが義務付けられます。しかし、この .onion というドメインは、通常の世界で行われる名前解決作業、（例えば、.ac.jp というドメインを日本の研究機関と解釈すること、）が不可能であり、Tor ネットワークのみで解釈可能なためです。

質問２．Tor ネットワーク内への誘導はどのようにして行われるのですか？

回答：Tor ブラウザで用いる検索エンジンが、DuckDuckGo であれ、Ahmir であれ、ダークウェブサイトのみならず表層ウェブサイトも検索表示しています。しかし、ダークウェブサイトについては、先に述べたような複雑な文字の羅列形式で、URL が表示されています。これは、サーバ管理者の身元秘匿のために必要です。しかし、身元秘匿を目的とした複雑な URL 全てに共通するのは、必ず、.onion というドメインが含まれている点です。 DuckDuckGo および Ahmir は、このドメインを見つけると、「Tor ネットワーク内部に存在する特有の」DNS サーバに、複雑な URL の名前解決を依頼します。この作業は、通常私達が用いている名前解決用の DNS サーバでは実行不可能です。一方、閲覧者からの依頼を受けた Tor ネットワーク内部の DNS サーバは、複雑な URL の解釈が可能なため、閲覧者の違法サイトへの誘導を実現することが可能です。