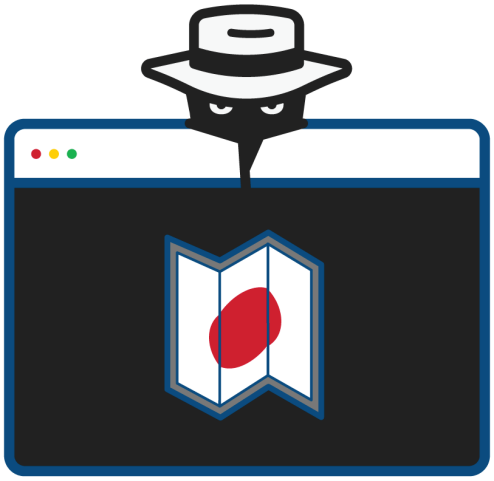
Recorded Future

サイバースレット分析

日本語圏アンダーグラウンドコミュニティの過去と現状

トモキ・タナカ
Recorded Future



CTA-2018-1214

スコープノート：レコーデッド・フューチャーは日本語圏のアンダーグラウンドフォーラムに関して幅広い知識を持つ日本人セキュリティ研究者との協力のもと、当社が前回行った中国とロシアのハッキングコミュニティ調査の続編として日本語圏のハッキングコミュニティの能力、文化、組織構造を調査しました。研究者が使用したリソースにはフォーラムへの直接アクセスやアクターとの直接的関与から得られたものも含まれています。

本レポートは、日本における業界や会社固有の脅威への監視強化を目的として日本語圏の犯罪地下組織を理解したい企業組織や、日本のネット犯罪活動の調査に関わる機関に興味深いものとなるでしょう。

エグゼクティブサマリー

アンダーグラウンドのハッカーコミュニティは通常、国内で技術を学んだ人がプロジェクトに協力する手段として、また、無害のものから非合法のものまで商売上の取引をする手段として様々な形態をとってきました。したがって世界でも有数の技術先進国である日本に独自のアンダーグラウンドコミュニティがあっても驚くにはあたりません。日本のアンダーグラウンドは主に協調的な複数の匿名フォーラムで形成され、外国と日本のフォーラムメンバーの間には中国で我々が見てきたものよりも積極的な相互交流がありました。

主要判断

- 日本のアンダーグラウンドコミュニティは中国語、英語、ロシア語圏と比較して未成熟である。しかし、日本人ハッカーと外国人ハッカーの間の交流が増えていることから、日本のハッカーは将来増加し高度化する可能性が高い。
- 日本のアンダーグラウンドコンテンツは違法薬物の販売が大半を占める。英語圏のアンダーグラウンドコミュニティとは異なり、違法コンテンツに特化した闇市場は存在せず、ほとんどの販売スレッドは汎用のフォーラムや電子掲示板システム（BBS）に作成されている。違法薬物の販売は、販売スレッドに書き込まれたアクターのメールアドレスに連絡して直接落ち合うことにより行われる。
- 英語、ロシア語その他の言語のコミュニティとは異なり、オンライン決済手段としてのBitcoinの採用は遅い。代わりにAmazonやiTunesのギフトカードのようなプリペイド式ギフトカードが決済に使用されている。
- 日本語コミュニティの一部は英語圏フォーラムのサブスレッド内部に形成されている。さらに、日本のハッカーは自己作成したツールではなく、他のハッキングコミュニティで採用された外部ツールを使用することが多い。

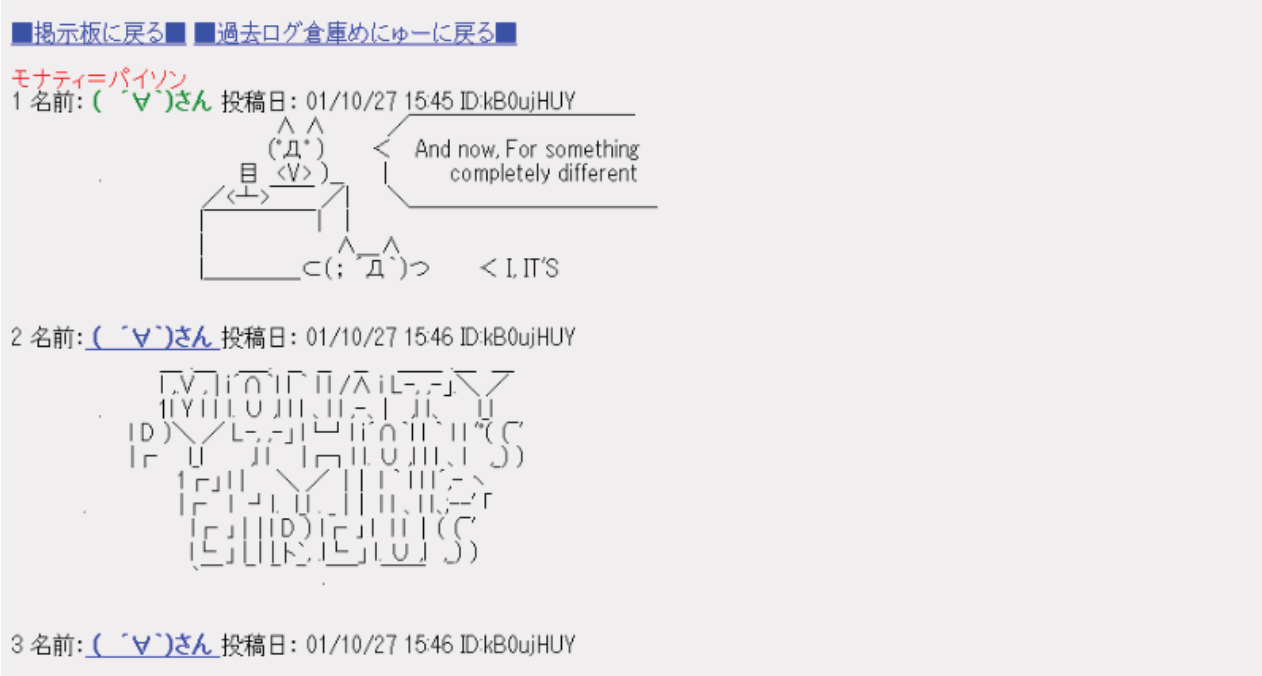
背景

インターネット上のアンダーグラウンドコミュニティは数多くの言語で普及し、様々なフォーラム内に存在します。こうしたフォーラムには、インターネット上で簡単に検索可能なウェブサイト上にホストされているフォーラムもあればモバイルチャットグループさらにはインターネット接続を匿名化するTorの秘匿サービスやその他のオーバーレイネットワークにホストされるウェブサイトに組み込まれているものもあります。違法コンテンツの宣伝や議論を行うサイトはTorの秘匿性の恩恵を受けています。このような様々なウェブサイトは電子掲示板システム（BBS）をはじめとして、この秘匿性を活用した違法なアダルトコンテンツ、ハッキング、マルウェアに加え薬物や銃器、偽造身分証明書の取引を専門に行っています。このような市場は、薬物、銃器、ハッキングで盗まれた偽造身分証明書のような非合法の商品をBitcoinやMoneroなど秘匿性の高い仮想通貨で安全に取引が行えるプラットフォームとなっています。

上記に挙げたもののほとんどは英語、中国語、ロシア語コミュニティーの例であり、日本語圏のアンダーグラウンドコミュニティは汎用電子掲示板システム形式（書き込みにより会員間で情報交換を行う掲示板群やフォーラム群）が多くを占めています。BBSの一部はTorのウェブサイトではあるものの、その多くはクリアウェブ上のサイトであり、汎用インターネットブラウザで簡単にアクセスすることができます。

日本のアンダーグラウンドコミュニティの歴史

日本のアンダーグラウンドコミュニティの歴史は1990年代後半に遡ります。1996年にBBSフォーラム「あやしいわーるど」が作成されました。複数の掲示板群で形成され、日本最大規模でした。パソコン通信の時代から現在のインターネットフォーラムへの過渡期に作られたあやしいわーるどは、当時のネチズンには画期的でした。このサイトは複数の投稿やコメントができるシンプルな掲示板や別建てのページで同様のウェブサイトを宣伝する「リンク集」で構成されていました。この形式はたちまち複数のグループのテンプレートとなり、同じ文化や同じサイトデザインを持つに至りました。2010年代に入っても新規ウェブサイトが立ち上げられましたが、高機能のソーシャルメディアサイトが出現すると掲示板への書き込みも減っていきました。



掲示板のフォーマット例。
出典：モナーフォントの掲示板

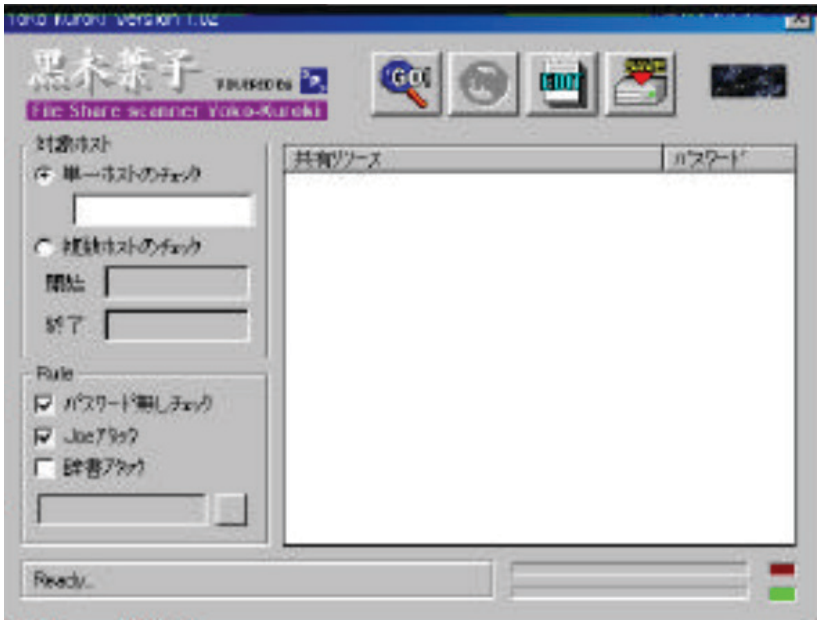
1999年5月には「ハッキングから今晩のおかずまで」というキャッチフレーズと共に、幅広いトピックで話題が投稿される匿名BBS、２ちゃんねるが登場しました。2017年に2ちゃんねるは5ちゃんねるに名称変更しましたが現在も日本で一番大きな掲示板であり、アメリカのフォーラム4chanの先駆けとしてインスピレーションを与えました。

90年代は日本のインターネットの黎明期に当たり、アクセスするユーザも限られていたことから日本のインターネットにアクセスするユーザはアンダーグラウンドコミュニティの一員でした。上記に挙げたインターネットコミュニティは独自の文化を形成したため、各分野に特化した掲示板によりコミュニティ内では様々なカテゴリの議論が行われていました。

当時のハッカー文化はまたハッキングやアングラサイトに関する書籍の出版にも導き、1998年3月に出版された「コンピュータ悪のマニュアル」は　10万部以上を売り上げました。同年7月には「ハッカージャパン」が創刊、セキュリティ関連の定期刊行物の中では最も長い歴史を誇っていましたが2013年11月に休刊となりました。

しかしインターネットは世間から隔絶して動作するわけではありません。1999年には不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）が日本政府によって公布されました。インターネットが一般に普及しソーシャルメディアの利用が増え始めるとアンダーグラウンドコミュニティは鳴りを潜めていきました。

不正アクセス禁止法施行前の日本のアンダーグラウンドコミュニティでは、様々な違法な商品やサービスが気軽にやり取りされていました。海賊版製品、主に海賊版ソフト（warez）やファイル共有ソフト、さらに海賊版のゲームのROMやチートに関する情報が交わされていました。これはおそらく90年代後期から2000年代初めにかけて日本の著作権規制がゆるやかであったせいでしょう。 電話ハッキング技術のようなハッキングツールやマルウェア、その他のクラッキングツールも、さらにソフトウェアのリバースエンジニアリングツールもごくわずかに共有されていました。このころ日本のフォーラムで共有されていたツールの多くは日本人が独自に開発したものでした。例えば、不正アクセス禁止法施行前の2000年1月にリリースされたパスワード解析ツール黒木葉子は、日本のクリエイターが日本向けに開発したものでした。



黒木葉子のインタフェース。
出店： 麗澤大学

違法薬物、銃器や爆発物、非合法組織（オウム真理教のような）、報道におけるタブー、未解決事件に関する情報もBBSで広く共有されていました。このような情報は日常から逸脱したものが多くを占め、怖いもの見たさでコンテンツを探す閲覧者の興味を引くものでした。このような情報サイトは2000年初めには人気を博し、危険な情報を専門に扱う「激裏情報」というフォーラムまで生まれました。しかし、このようなゴシップあるいはタブロイド関連のサイトの多くは以後閉鎖または一般のフォーラムへと進化していきました。

C現在の激裏情報のホームページ
出典: *https://gekiura.com/*

現在の状況

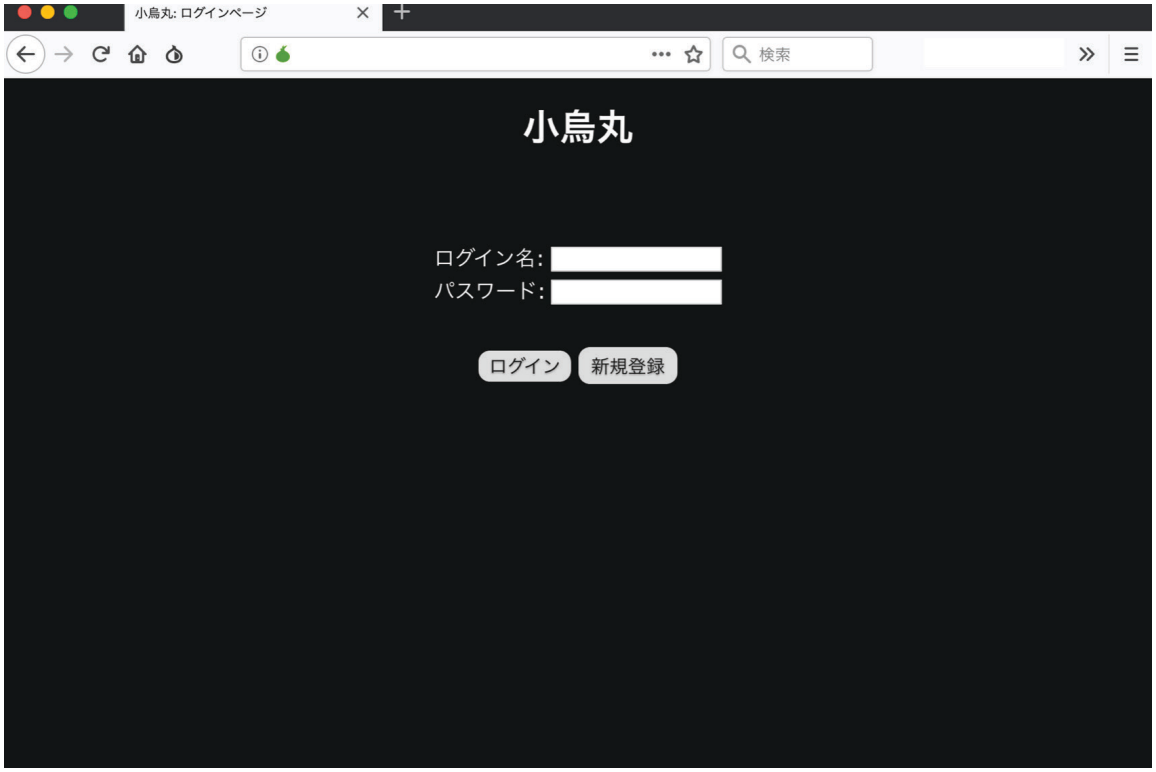
中国語圏のフォーラムと同様、日本のフォーラムはwarezを複数の市場にコンパートメント化することなく、ハッキングや他の話題の議論も発生する汎用フォーラム上で宣伝しています。日本のアンダーグラウンドのやり取りのほとんどは今日の日本語圏最大のアンダーグラウンドコミュニティ「Onionちゃんねる」で行われています。このBBSは、以前に作成された2チャンネルフォーラムにインスパイアされて2004年に開設されました。Onionちゃんねるは公的には「Tor板」、「エロいの」、「アングラ板」の３つの掲示板に分割されているものの、そのすべてには様々なサブフォーラムがあり、違法薬物、ハッキング、違法なアダルトコンテンツまで含まれています。すべての掲示板にはファイルアップロード機能が付いており、違法なアダルトコンテンツ、検閲ではじかれた情報や盗み出されたと思われるファイルがアップロードされています。これらの掲示板は、1990〜2000年代のアンダーグラウンドコミュニティの文化が今も健在で、今日のコミュニティにも強い影響を及ぼしていることを示しています。

OnionちゃんねるのTor板

日本語圏のアンダーグラウンドコミュニティは、英語圏のコミュニティがアカウント登録を必要とするフォーラム形式であるのに反し、従来のBBSスタイルで構築されているため、アカウント登録無しの匿名の投稿が可能です。このサイト構造ゆえに、スパム投稿や荒らしを排除しにくいため、サイト全体の動作も重くなります。さらに、その匿名性からこれらのサイトでのアクターの追跡は考えられないほど難しくなります。例えば、2013年8月に5ちゃんねるBBSの有料サービスであった「5ちゃんねるビューア」の会員情報がOnionちゃんねるのアングラ板に大量流出しました。この事件のメディア報道でOnionちゃんねるは一躍有名となりました。

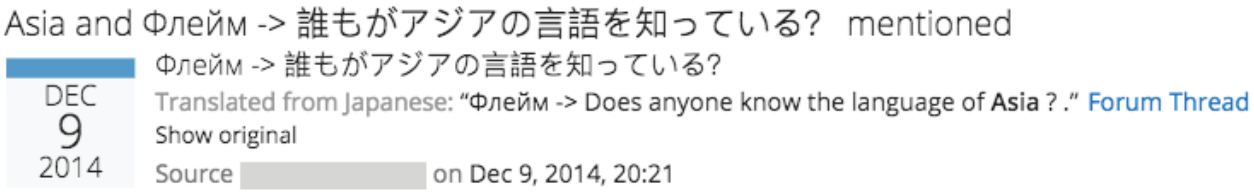
多くの投稿は匿名ではあるもののOnionちゃんねるのようなBBSサイトには、投稿する際に固定ハンドルネームを入力できる機能が付いています。これを使うには、ユーザは「トリップコード」システムで登録することを求められます。この機能は5ちゃんねるから踏襲されました。ユーザがユーザ名とパスワードを入力すると、BBSはパスワードをハッシュしてトリップコードと呼ばれる任意の文字列を計算します。このトリップコードはその後そのユーザからのすべての投稿にユーザ名の隣に「固定ハンドル名◆トリップコード」のように表示されます。パスワードが誤ってパブリックドメインに流出すると、他の人であってもそのアカウントでログインしてなりすますことが可能になります。トリップコードはログインの度に同じものが使われるからです。

他の著名な日本のアンダーグラウンドフォーラムには、小烏丸 やすでに閉鎖された恒心教サイバー部もあります。小烏丸はもともとOnionちゃんねるから派生し、会員専用の情報共有サークルとして日本のハッカーが利用するようになりました。小烏丸のサークル内投稿のほとんどはハッキング関連で、オンライン秘匿性を維持し、「torrcで最適な設定の仕方」や「Whonixで匿名性を高くする方法」、「Kali Linuxでハッキングをする方法」などの情報が飛び交っています。恒心教サイバー部のページでは、主にハッキング、カーディング、秘匿性に関する議論が行われていました。



小鳥丸のログインページ

中国語圏とは異なり、日本語圏のコミュニティは日本のフォーラムにのみ依存してるわけではありません。日本語圏コミュニティが英語圏のコミュニティ内部のサブセクションで形成されている例もあります。日本のハッカーはまた、防弾ホスティングのように国内のフォーラムではすぐにはアクセスできない情報を得るためには、ロシア語圏や英語圏のフォーラムのほうがアクセスしやすいことから日本語以外の掲示板にもアカウント登録します。外国のコミュニティも、たまに日本語の掲示板に押し寄せてはオンラインウェアを宣伝しています。日本語コミュニティにはまた、たどたどしい日本語で書かれた外国の掲示板の宣伝の形跡もあります。



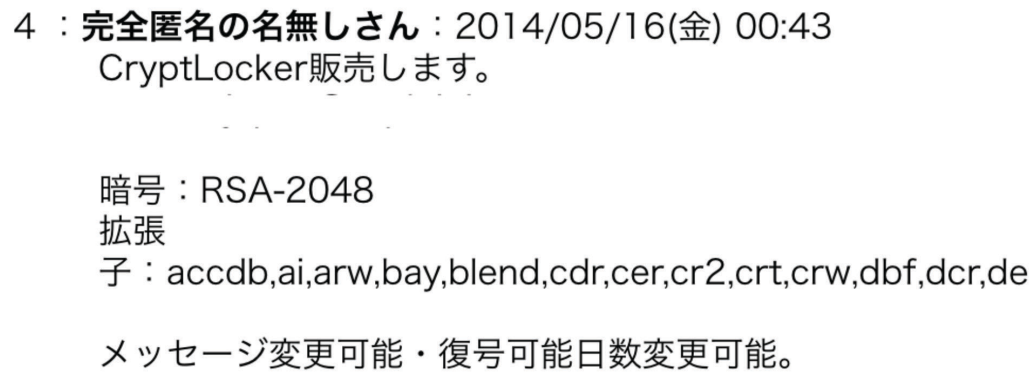
アジアの言語を話す人がいるかどうかを尋ねるダークなウェブコミュニティの中の日本フォーラムのポスト。

日本と外国のフォーラム間の連携が進むにつれ、日本のアンダーグラウンドコミュニティ内で望ましいとされてきた連絡手段にも変化が現れ始めました。つい数年前までは、Yahoo!メールや使い捨てメールアドレスで行うのが主流でしたが、英語圏コミュニティで広く普及しているProtonMailやTutanotaなどのメールサービスが人気を集め始めました。Telegram、Signal Private Messenger、Wickr、Jabberのようなプライバシー保護に特化したメッセンジャーサービスの使用も普及し始めています

日本語アンダーグラウンドフォーラムのコンテンツ

マルウェアとデータ

マルウェア開発は、マルウェア開発関連の投稿数が少ないことから日本語圏コミュニティでは一般に追及される対象となっていませんが、海外の犯罪コミュニティから購入または流出されたマルウェアが活発に販売されています。外国のアクターが作成したランサムウェアを日本の犯罪者が取り入れて日本のホストを標的に流暢な日本語で脅迫状を書くといった例があります。


4 ：**完全匿名の名無しさん**：2014/05/16(金) 00:43
CryptLocker販売します。

暗号：RSA-2048
拡張
子：accdb,ai,arw,bay,blend,cdr,cer,cr2,crt,crw,dbf,dcr,de

メッセージ変更可能・復号可能日数変更可能。

CryptoLockerの亜種を宣伝するBBSの投稿

データに関して言えば日本のハッカーはえり好みしません。国内外のデータが日本のアンダーグラウンドフォーラムで販売されていますが、多くの場合、日本のハッカーが盗んだものかどうかもはっきりしていません。例えば、2017年5月には韓国のデータの日本向けの宣伝が小鳥丸で見つかっていますが、日本以外のフォーラムでハッカーにより盗まれたものと思われます。

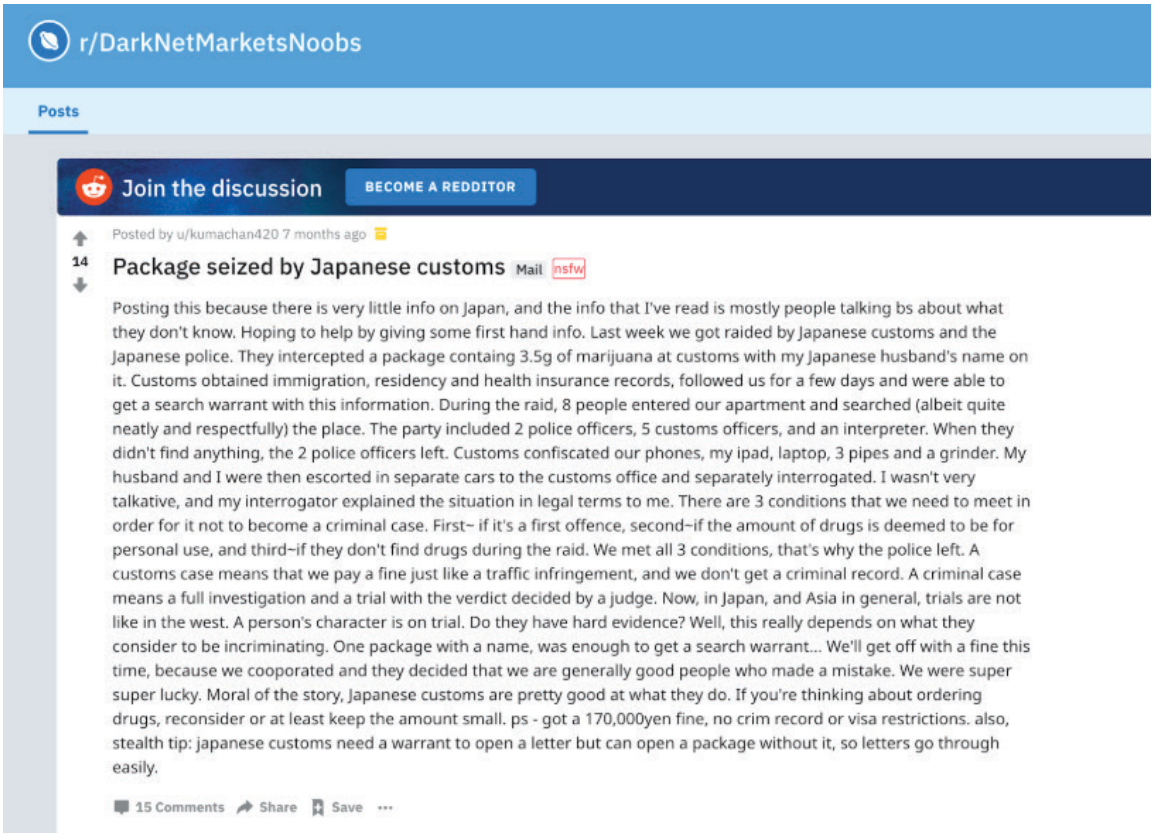
小烏丸上で韓国のデータダンプを売り込む日本向けの宣伝

薬物、武器、違法アダルトコンテンツ

日本のアンダーグラウンドでは多種多様な薬物が販売され、薬物が投稿の大部分を占めます。英語圏では、大麻のことを時には「weed」、コカインのことを「coke」と呼びます。同様に、日本語フォーラムの会員は大麻を「野菜」、コカインを「チャリ」、覚せい剤を「氷」と呼んでいます。他にも、武器や違法なアダルトコンテンツもたまに宣伝されています。拳銃「チャカ」も時折、日本語フォーラムのフォーラム広告に見られます。掲示板にはすべてファイルアップロード機能がついていてデフォルトで匿名となっているため、売人はこの機能を利用して罰せられる恐れなく違法なコンテンツを広く共有することができます。

日本の違法薬物の販売においては、「手押し」という直接取引の形が主流です。売人はまず「大阪、野菜、1g 5000円から」といった宣伝コメントをBBS上に書き込み、買い手のメール連絡を待ちます。そして特定の場所で落ち合い、取引を行います。

直接会って取引を行えば、証拠を残さないで済みます。郵便は日本国内では薬物取引に推奨されていません。売人が偽造薬物を送る傾向があることと、国内外の郵便物が配達前に検査されるためです。これもあって、日本のアンダーグラウンドコミュニティの薬物は外国から発注を受けません。日本の税関は通常薬物押収に長けており、薬物が郵送された場合に売人や買い手の家にまで直接訪問することもあります。また、英語圏のアンダーグラウンドコミュニティのユーザの中では、日本に違法薬物を送ってはならないとの了解があり、複数の薬物関連の英語フォーラムで日本の税関の優秀さを議論していました。



日本の税関を理由に薬物ユーザに日本に送ってはならないと警告するRedditの書き込み

防弾ホスティングサービスとVPN

通常日本政府の検閲対象となるコンテンツをホストするウェブサイトの開設には、停止要求を受けにくいサーバが必要となるため、防弾ホスティングサービスが利用されます。ここ最近、防弾ホスティングサービスを提供する国際的プロバイダの宣伝が日本語フォーラム内で浸透しつつあります。一昔前までは、000WebHostやXREAといったサービスが日本国内で利用されていましたが、今では、Novogara　LTD、BlazingFast、AbeloHostといった海外のサービスが日本のハッカーによって普通に使われています。こういったサービスに関する情報は、日本のハッカーが海外とのハッカー繋がりで入手しています。

日本国内でのVPNの使用も同様の進化をしており、筑波大学が無料提供するVPN Gateと呼ばれるVPNサービスには多くのユーザがいました。TorとVPN Gateで秘匿性を維持する方法を説明した英語と日本語の文書が数々のフォーラムで広く出回っていました。しかし、日本の警察がVPN Gateのログをアーカイブしていることが周知した為に、ExpressVPNやProtonVPNなどの海外VPNを宣伝する書き込みが次第に増えていきました。

決済方法

英語圏やその他のハッカーコミュニティとは異なり、日本のハッカーの間ではオンライン決済へのBitcoinの採用はあまり進んでいません。薬物購入には現金取引が主流ですが、日本語フォーラムのオンライン決済ではAmazonやiTunesのギフトカードのようなプリペイド式カードが通常利用されています。これはネチズンが日本国内で匿名性を確保するのに便利である一方、仮想通貨を換金するには取引所にアカウントを作成し、身分証明書を提示する必要があるためです。プリペイドギフトカードはまたオンラインでの利用が驚くほど容易で、唯一カードの裏面に記載されたコードさえ入力すればギフトカードを使用できます。この為、プリペイドカードが欲しいといった書き込みが日本の掲示板に散見されます。

展望

日本のアンダーグラウンドコミュニティは主に1990年代初めからの先駆者の文化を踏襲しています。しかし、日本と外国のハッカーの相互交流が増えていることから、日本のハッカーの数が増え、高度化していく可能性もあります。英語圏のコミュニティフォーラム内で数多くの日本のサブセクションが拡大を続けており、日本のハッカーが外国ハッカーとの繋がりを深めていることから、日本のハッカーは、これまでマルウェアやVPNアクセスを取得するためにそうしてきたように、日本にはない情報やオンライン商品を取得するために外国のウェブサイトを模索し続けるでしょう。海外のフォーラムのフォーマットを踏襲する掲示板が台頭する可能性もあれば、これらがOnionちゃねんるよりも影響力をもった大きなフォーラムへと拡大する可能性もあります。