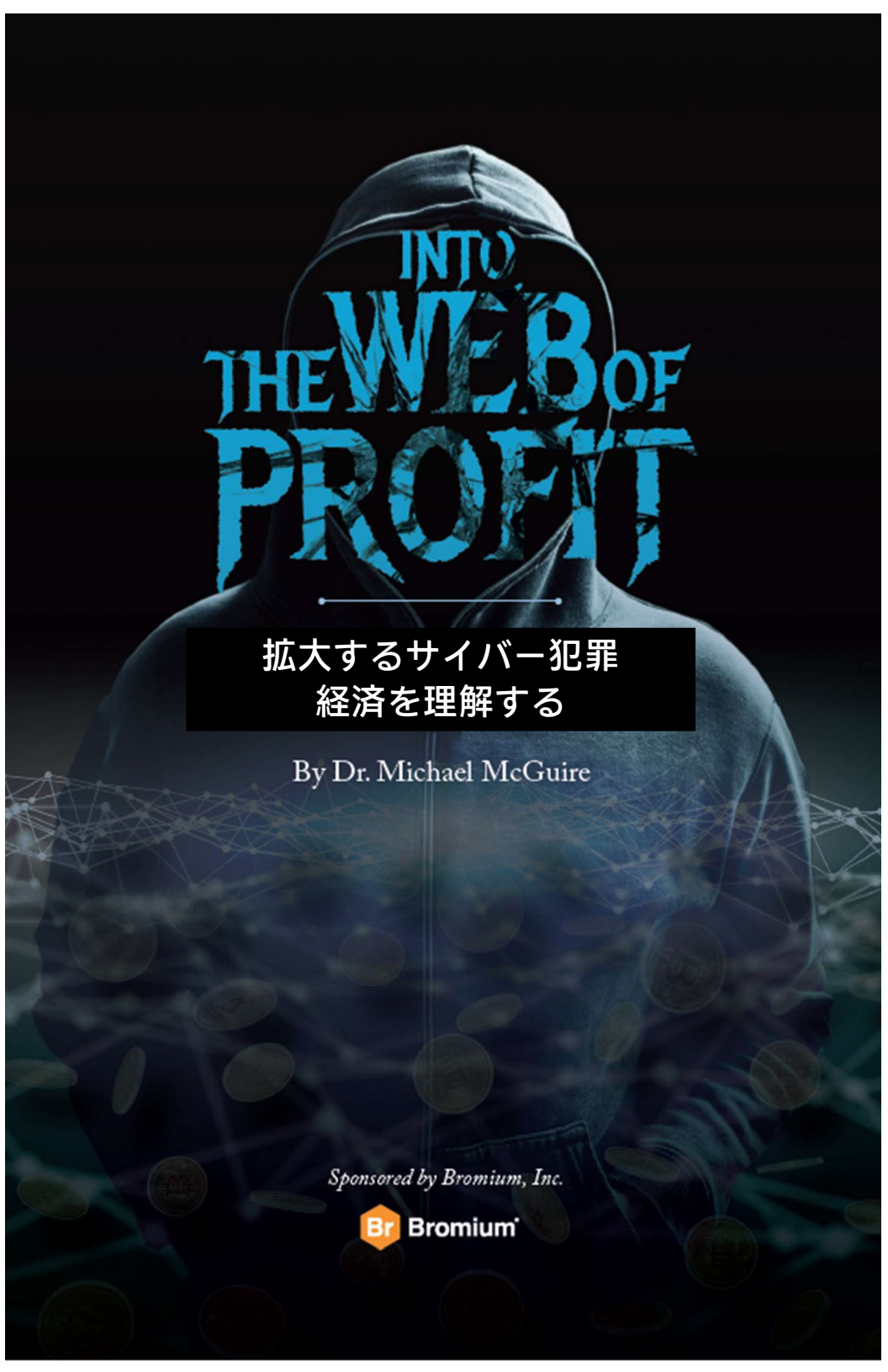

INTO
THE WEB OF
PROFIT
拡大するサイバー犯罪
経済を理解する
By Dr. Michael McGuire
Sponsored by Bromium, Inc.
Br Bromium

The Web of Profit（利益の網）の中へ

サイバー犯罪、犯罪者、お金についての詳細な研究。

Mike McGuire博士によって研究され、書かれています。
2018年4月

Bromium, Inc.によりファンドされたプロジェクト

謝辞

本報告書のために実施した調査の際に相談に乗っていただいたU.S.とヨーロッパの刑事司法機関、金融機関、学識経験者の方々に感謝の意を表します。

特に、貴重なデータを提供してくださったCity of London PoliceのU.K. National Fraud Intelligence Bureauの皆様、また、有益な提案やサポートをしてくださったThe National Crime Agency、The Metropolitan Police、Home Office Cybercrime Research Unitの皆様に感謝いたします。

内容

図一覧

序文

Gregory Webb
CEO, Bromium

私たちがこの研究に投資したのは、それが重要だと考えたからです。McGuire博士の研究結果は、サイバー犯罪の収益がどのようにして生み出され、ロンダリングされ、犯罪経済に再投資されているかを説明しています。サイバー犯罪を支えているシステムをよりよく理解することで、それを破壊する方法をよりよく理解することができると考えています。

本質的には、ハッカーの生活をより困難にしたいと考えています。

サイバー犯罪者は常にサイバーセキュリティ業界の一歩先を行っています。データは取引や販売が可能な貴重な商品であり、サイバー犯罪は他の形態の犯罪と比較して比較的リスクが低く、有利なビジネスとなっています。
サイバー犯罪者が有罪判決を受けることはめったにありません。そして今では、誰もがパッケージ化されたマルウェアを購入し、ハッカーをオンデマンドで雇うことができるようになり、これまで以上に簡単になりました。

この報告書の中で、McGuire博士は「プラットフォーム犯罪」の出現を指摘しています。

新しいデジタルビジネスと同じような形で サイバー攻撃を行いやすくなっています彼らはプロセスを自動化しているので 今後はより頻繁に攻撃を受けることになるでしょう

"潮目を止めるのに失敗した結果、社会が苦しんでいる。"

犯罪者と合法的な世界の間の壁が曖昧になってきています。私たちは単に「パーカーを着たハッカー」を扱っているのではなく、麻薬取引からテロまで、世界規模の犯罪活動を可能にし、資金を提供し、支援する経済の生態系に取り組んでいます。潮目を止めるのに失敗した結果、社会が苦しんでいるのです。

報告書によると、サイバー犯罪者はテクノロジーの革新者であると同時に、アーリーアダプターでもあります。法執行機関だけで新しいシステムを追跡し、破壊することができると考えるのは非現実的です。私たちは共通の目標を持つコミュニティであるため、協力し合い、これまでとは異なることにも意欲的に取り組む必要があります。私たちは、この犯罪生態系を支えるコアシステムを破壊する社会的・道徳的義務を共有しています。

私たちの最も貴重な資源であるデータをハッカーが収集することをより困難にする必要があります。サイバーセキュリティ業界は、検知から保護までのセキュリティの限界を理解し、問題を切り分けるためのより良い方

法を見つける必要があります。私たちは、組織の中で最も脆弱で攻撃しやすい経路に焦点を当てることで、全く異なる方法でサイバー防御に取り組む必要があります。犯罪者は、私たちがどこに脆弱性を抱えているかを知っていますが、その多くは人間がキーボードに指をかける場所です。人間の行動を変えることは困難であり、コストがかかることも知っています。

その代わりに、検知ではなく保護に焦点を当てることで、サイバー犯罪を大きく破壊することができます。

研究はサイバー犯罪を理解する上で極めて重要であり、いつか The Web of Profit（利益の網）に終止符が打たれる日が来るかもしれません。それまでの間、私たちは仲間と協力して、インターネットと、それに依存してコミュニケーション、コラボレーション、ビジネスを行う組織を保護し続けます。

さあ、協力して The Web of Profit を破壊しましょう。

序文

Michael McGuire博士
Surrey大学 上級講師

サイバー犯罪に対する認識はかつてないほど高まっていますが、サイバー犯罪が犯罪行為を統合したものとしてどのように機能しているのかについての理解はまだ十分とは言えません。脅威の範囲や規模に対する理解ははるかに進んでいるものの、サイバー犯罪がどのように機能するか、またそれを推進・支援する要因についての理解は依然として限られています。

これまでは、サイバー犯罪のメカニズム、つまりどのように発生するのかという点に主に注目が集まっていました。そのため、マルウェアの種類やセキュリティホール、特定のタイプの攻撃の防止など、技術的な要因が最も頻繁に議論されています。最近では、「ヒューマン・ファクター」、つまりヒューマン・エラーや判断力の低さがサイバー犯罪者のシステム侵害の成功に貢献している可能性があることが、原因要因としてより深刻に扱われるようになってきました。

しかし、まだあまり発展していないのは、犯罪者、被害者、警察やセキュリティの専門家、企業、国家、金融機関、サービスやサポートの仕組みが互いに、そして様々なインフラ（データサイロ、決済システム、Webそのものなど）と相互に結びつき、複合的な全体を生み出すシステムとしてのサイバー犯罪の理解です。

このシステムはダイナミックに進化しており、その主要な推進要因の一つは収益の創出であり、最終的には利益です。収益生成とその流れを理解することは、サイバー犯罪に関する知識を高めるための新たな方法を提供するだけでなく、収益構造とその流れをよりよく理解することで、サイバー犯罪を制御するための新しい選択肢を開発することができます。

The Web of Profitプロジェクトは、収益と利益の流れというレンズを通してサイバー犯罪のダイナミクスを見ようとした最初の大規模な研究の一つです。収益と利益に関連する要因をよりよく理解することに焦点を当てることで、新しい種類の知識ベースに貢献することを目的としています。

したがって、以下の研究の議論は、収益がどのように発生し現在最も儲かる収益はどのようなものか、収益がどのように移動あるいはロンダリングされているのか、収益がどこで他の資産や活動に使用あるいは変換されているのか、という3つの重要な要素によって構成されています。

序章

新興の犯罪経済：サイバースペースと The Web of Profit

金銭的な動機は、サイバー犯罪の形態と広がりの両方において、最も重要な唯一のドライバーとなっています。セキュアなコンピューターに侵入するという知的な「スリル」といった以前の動機よりも、お金はサイバー犯罪者に強力な影響力を及ぼします。しかし、「ビジネスとしてのサイバー犯罪」という（しばしば乱用される）比喩は、もはやその複雑さを捉えるには適切ではありません。より適切な比喩は、ビジネスではなく経済であり、文字通りの”The Web of Profit（利益の網）”として機能する　-　経済行為者、経済関係、およびその他の要因が複雑に関係し、今ではかつてない規模で犯罪収益を生み出し、サポートし、維持することができるようになっている構造体です。

The Web of Profitは、合法な相手を食い物にするだけではなく、従来からの世界の収益創出や利益を支え、強化していくものです。その結果、両者の間の相互接続性と相互依存性が高まっています。今や企業や国家はそこからお金を稼ぎ、そこからデータと競争優位性を得て、それを活用し、戦略や世界進出、社会統制のためのツールとして活用しています。

"サイバー犯罪経済は現代の資本主義の鏡像になっている。"

同様に、あるいはそれほど重要でないにしても、サイバー犯罪経済は現代の資本主義の鏡像のようなものになっており、AmazonやUberのような破壊的なビジネスモデルを再現しています。合法的な情報経済の一種の「怪物的な替え玉」として、データが王様であるThe Web of Profitは、富が生成される方法を食い物にしているだけではなく、正当な経済を再現し、場合によっては、それを上回っています。これは、現在の富を創造しているプラットフォーム・モデルを見れば明らかです。

The Web of Profitを支える複雑なサイバー犯罪経済は、（少なくとも）次のように構成されています。

- 収入を得るための様々な方法や仕組み、多くの場合は産業規模での収入を得ることができます。
- デジタルに特化した通貨と通貨交換ツール。
- 生産者、供給者、サービス提供者、消費者など、さまざまな専門の経済行為者。
- 違法取引のためのキーとなる材料や価値の対象としてのデータの抽出と交換（この取引は現在では様々な次元で行われており、もはや盗まれたクレジットカードやデビットカードからデータを売買するだけではなく、ホテルのポイントやFacebookの「いいね！」、アカウントのログイン情報、さらにはソフトドリンクの処方

や政府が開発したハッキングツールなど、価値を持つ新しいデータ形式も含まれています）。

- ロシアのトロール工場であれ、ルーマニアのハッカービル詐欺 寸であれ、西アフリカのマス・マーケティング詐欺センターであれ、収益を生み出す特化した生産地帯や中心地があります。
- 専門的なツールの供給、技術サポート、スキルと専門知識の提供。
- 専門性の向上とキャリア構造の開発 - これには、トレーニング、履歴書、個人的な推薦、推薦状などが含まれます。
- 専用のマーケットプレイスは、麻薬、銃器、盗まれたデータや営業秘密などの明らかに違法な商品だけでなく、合法的な経済内での取引を反映した、偽物の商品、偽のサービス、偽の真正性や身元、さらには偽のニュースなどのドッペルゲンガー商品のためのものでもあります。
- グローバルな流通メカニズム。
- 自主規制と代替的な法の支配。
- 本レポートでは、The Web of Profitを解剖し、サイバー犯罪経済の全体像を構成する3つの中核的な機能を具体的に掘り下げています。
- サイバー犯罪の収益がどのようにして生み出されているか。
- サイバー犯罪の収益がどのようにロンダリングされ、どのように変換されているか。

- サイバー犯罪の収益が最終的にどのように処分され、再投資されるか。

サイバー犯罪の収益は1.5兆ドルに達する

サイバー犯罪は比較的新しい犯罪経済ですが、すでに毎年*少なくとも*1.5兆ドルの収入を生み出しています。これは、収益を生み出すサイバー犯罪の中でも特に注目度が高く、もうかる5つの種類のデータのみに基づいた保守的な見積もりです。

犯罪	年間収益
違法、違法なオンライン市場	8,600億ドル
営業秘密、知的財産の盗難	5,000億ドル
データ取引***。	1,600億ドル
クライムウェア、CaaS（サービスとしてのサイバー犯罪）の提供	16億ドル
ランサムウェア	10億
*合計は概算 **クレジットカードやデビットカードの情報、銀行のログイン情報、ロイヤルティ制度など、盗まれたデータを取引することで得られる収益。 ***データを暗号化して支払いを要求することに基づく恐喝から得られる収益。	

表1：サイバー犯罪の年間売上高の推定値

違法なオンライン市場は、現在ではサイバー犯罪の収益源として最も儲かる形態となっており、総収益の50%以上を占め、営業秘密やその他の知的財産の窃盗はサイバー犯罪の収益の約35%を占めています。盗まれた

データを商取引の対象として利用することは、サイバー犯罪経済の活気ある部分であり、総収入の約11%を占めています。リスクの低い活動として、現在では窃盗そのものよりも魅力的なものになっているかもしれません。

サイバー犯罪者個人にとっては、CaaS（Cybercrime-as-a-Service）とランサムウェアは、高収益の収益源となり得ますが、（現時点では）収益を生み出す単一のカテゴリーとしては割合が低く、それぞれ総収益の1%未満です。これらの推定値については、いくつかの条件の考慮が推奨されています。第一に、今回の推定では犯罪ウェア/CaaSの3つのカテゴリーのみを考慮したため、実際の数字はもっと高くなる可能性があります。第二に、ランサムウェアはクライムウェア/CaaSのカテゴリーに含まれる可能性があります。なぜなら、ランサムウェアのツールはクライムウェアのプラットフォームで購入したり、レンタルしたりできることが多いからです。

現在のところその知名度が高いことから、本研究ではランサムウェアを別のカテゴリーとして扱っていますが、検知・予防システムが洗練されていく中で、それに伴う収益は今が最高潮に達しているのかもしれません。確かに、ランサムウェアが最も収益性の高いサイバー犯罪の一つであるという主張は、個々の攻撃の場合には通用するかもしれませんが、全体の収益は他のカテゴリーに比べて低いままです。

"サイバー犯罪の収益が 合法的な企業の収益を上回ることが多いという証拠がある。"

収益、つまりサイバー犯罪に関与することで得られるものは、サイバー犯罪が引き起こすコストや損失などのこれまでの財務指標に比べて、この犯罪を理解するための新たな、あまり検証されていない方法を提供します。サイバー犯罪からの収益なのか、従来の（純粋に物理的なものやコンピューターを利用しない）犯罪からの収益なのかを確かめるのは難しいことですが、本レポートのために一次情報源と二次情報源の両方から収集した証拠によると、犯罪カテゴリーのさまざまな種類の中で、詐欺はサイバー犯罪の方がより収益性が高い明白な例です。このカテゴリーに属する個々のサイバー犯罪者の収益は、従来の犯罪の世界のそれを上回るだけでなく、サイバー犯罪に関与して収益を得ることができる者の数もはるかに多くなっています。このように、伝統的な犯罪からの総収益は全体的にはまだ高いと思われますが、偽造のようにサイバーと伝統的な手法の相互依存性が高まっているものを考えれば、これがいつまで続くかは決して明らかではありません。

サイバー犯罪の収益は、特に中小企業では正規の企業の収益を上回ることが多いという証拠があります。実際、サイバー犯罪の収益は、10億ドル以上の利益を生み出す大規模な「多国籍」事業から、3万ドルから5万ドル

の利益が一般的な小規模事業まで、さまざまなレベルで発生しています。

ポスト-犯罪とプラットフォーム犯罪

複雑で多層的なサイバー犯罪経済の出現は、犯罪の本質そのものの根本的な変化を示唆し始めています。このような状況の中で、犯罪を糧とし、犯罪をサポートする低投資、高利回り、低リスクの事業であるサービスやプラットフォームに比べれば、あからさまな犯罪行為は、犯罪の生態系の中心的な特徴では無くなっています。

その結果が犯罪プラットフォーム・モデルへのシフトとなり「プラットフォーム資本主義」として特徴づけられてきた現代のグローバル経済のシフトを反映しています。この言葉は、Uber、Google、Facebook、YouTube、Instagram、LinkedInなどのような企業が、プラットフォームを他者に提供し、そのデータを収集するだけで大きな収益を得ることができるようになったことを説明しています。

"その結果、犯罪のプラットフォーム・モデルへとシフトし、現代のグローバル経済の変化を反映している。"

サイバー犯罪用語では、プラットフォーム・モデルは2つの形態で収益を生み出します。

- 合法的なプラットフォームの悪用
- 新しいタイプの不正プラットフォームの創出

ポスト-犯罪の世界が出現してきています。これは、殺人のような重大な犯罪が存在しなくなったり、被害者にとってトラウマになることが少なくなったりするということではありません。むしろ、少ない犯罪への関与や、あるいは二次的な形での間接的に利益と言った犯罪性の多様性が、収益を生み出すという点でより魅力的なものになるということです。

サイバー犯罪化が進む世界では、合法的な経済と非合法的な経済の両方が共存しています。情報犯罪のツールや文化が、情報社会のツールや文化と曖昧になり、交換可能になり、またその逆もまた然りです。

収益の移動

他の犯罪行為と同様に、サイバー犯罪による利益の増大は、資金洗浄や処分の方法の複雑さの増加を引き起こしています。世界中で流通している推定1.6 ~ 2兆ドルの洗浄されたお金のうち、約10%以上がサイバー犯罪からの収益に起因しており、合計2,000億ドルにもなります。

その証拠に、サイバー犯罪者は、合法的な銀行システムの不正利用、マネーミュール、シェルカンパニー、電信送金などの伝統的なロンダリング方法を導入することにますます習熟してきていることが示唆されています。

これらを補完するものとして（時には併用して）、PayPalのようなオンライン決済システム、Bitcoinのような暗号通貨、あるいはオンラインゲーム用通貨など、革新的でよりデジタルに焦点を当てた資金洗浄の方法があ

ります。

しかし、資金洗浄目的での暗号通貨の使用は、実際の使用よりも評判の方が急速に高まっています。最も正確な推定では、現在洗浄されている資金のうち、Bitcoinやその他の暗号通貨が使用されているのは約4%に過ぎないと言われています。

"サイバー犯罪が多発する世界の中で、合法的な経済と違法な経済が一体となっている。"

暗号通貨は、しかしながら新しいサイバー犯罪経済の主要な要素を構成しており、将来的に収益が合法経済と非合法経済を介してどのように流通する可能性が高いかに大きな意味を持っています。この文脈では、Bitcoinは、新しい、そして継続的に出現している様々な暗号通貨を利用した、はるかに発展したロンダリングの世界への入り口に過ぎません。

暗号通貨を使った取引は、一般的に言われているほど匿名性は高くありません。それらを支えるブロックチェーンシステムは、透明な公的記録を生成します。また、活動をさらに曖昧にするためにミキサーシステムを使用した場合でも、他のデータ（ウェブクッキーなど）が流出して痕跡を残すため、暗号通貨の取引の最大60%が個人と結びつく可能性があるという証拠も出てきています。

暗号通貨資産の押収を含む一連の成功した捜査は、暗号通貨取引を追跡する法執行機関のスキルと能力の成長を実証しています。

サイバー犯罪資金の処分

有罪判決を受けた、または現在サイバー犯罪活動に従事している個人サンプルのインタビューと観察データを利用して、以下のことが明らかになりました。

- サンプリングされたサイバー犯罪者の15%は、収益の大部分を、おむつの購入、請求書の支払いなど、当面のニーズをカバーするために費やしています。
- サンプリングされたサイバー犯罪者の20%は、麻薬の購入や売春婦への支払いなど、収益を無秩序または快楽主義的な支出に集中させていました。
- サンプリングされたサイバー犯罪者の15%は、ステータスを獲得するために、あるいはパートナーや他の犯罪者に好印象を与えるために、高価な宝石を購入するなど、より計算された支出に収益を向けていました。
- サンプリングされたサイバー犯罪者の30%は、収益の一部を地所などの資産に変えていました。
- サンプリングされたサイバー犯罪者の20%は、その収益の少なくとも一部を、さらなる犯罪活動への再投資に使用していました。例えば、機器やクライムウェアの購入、さらには違法薬物の生産、人身売買、テロリズムに収益を回していました。

"サイバー犯罪者が求める報酬は従来の犯罪者とあまり変わらない。"

これらの結果は、犯罪者による収益の利用方法に興味深い構造的連続性があることを示しており、サイバー犯罪者が求める報酬は従来の犯罪者とあまり変わっていないことを示唆しています。

例えば、この調査では、高級車や宝石などの高級品に利益を使っている傾向が続いていることが明らかになっています。また、従来の犯罪者と同様に、サイバー犯罪者も収益を不動産や土地などの長期的な資産や、ワインや美術品などの代替的資産に転用しようとしているという証拠もありました。

しかしながら、サイバー犯罪経済は、資産を現金化するための新たな選択肢を提示しています。例えば、暗号資産やその他のデジタル決済ツールで直接購入可能な商品などです。

重要なことは、収益がさらなるサイバー犯罪に投資されているという証拠もあったことです。これは、機器やツールの購入という比較的低レベルのものから、さらなる犯罪への高額な長期投資という形の可能性もあります。

さらに気になるのは、サイバー犯罪の収益が、人身売買やテロなどのより深刻な犯罪に資金を提供しようとする人々の注目を集めるほど大きなものになっているという証拠です。

同時に、サイバー犯罪者がデジタル収益を使用する時、現金化プロセスを実現する方法を発見することのプレッシャーが高まっていることは、法執行機関やサイバーセキュリティの専門家にサイバー犯罪を阻止し、破壊するための新たな選択肢を提示している可能性があります。

メトリクス：一覧

数字で読み解くThe Web of Profit

　このレポートのハイライトをご覧になりたいですか？簡単にご覧いただけるようにしました。このセクションでは、情報を簡単に発見できるように、サマリー、ビジュアル、一目でわかるスニペットを提供しています。

犯罪	年間収益*
不正、違法なオンライン市場	8,600億ドル
営業秘密、知的財産の盗難	5,000億ドル
データ取引**	1,600億ドル
クライムウェア/CaaS (サービスとしてのサイバー犯罪)	16億ドル
ランサムウェア***	10億ドル
サイバー犯罪の発生件数	**1兆5,000億ドル**

*合計は概算。
**クレジットカードやデビットカードの情報、銀行のログイン情報、ロイヤルティ制度などの盗難データを取引することで得られる収益。
***データを暗号化して支払いを要求することに基づく恐喝から得られる収益。

FBIは、2016年のランサムウェアの支払いだけでも約10億ドルに達すると推定しています。以下は選択されたランサムウェア製品からの収益です。

ランサムウェア	時期	推定利益
CryptoLocker	2013	~300万ドル
Clyptowal	2014-16	~1,800万 ~ 3億2,000万ドル
Locky		750万ドル ~ 1億5,000万ドル
Cerber		690万ドル
WannaCry	2016	$55,000-$140,000
Petya/NetPetya		$10,000

サイバー犯罪の収益は大きい場合も小さい場合もある

- 年間10億ドル以上の利益を誇る大規模な多国籍企業。
- 年間30,000 ~ 50,000ドルの利益を上げる小規模事業。

個人情報の販売で稼ぐ

- わずか50枚のクレジットカードやデビットカードの個人情報を販売することで、25万ドル ~ 100万ドルの収益を得ることができます。
- コンテンツ窃盗サイトは、広告収入だけでも2億2,700万ドル近くを稼いでおり、全体の収入は年間約440万ドルとなっています。

"社会保障情報、生年月日、住所を取得するための費用は 3 ドル。"

より大きな努力は、より大きな報酬をもたらす

- 2016年に撤去される前は、Kickass Torrentsのプラットフォームは5,400万ドル以上の価値があり、広告収入だけで推定年間収入は1,250万ドル ~ 2,230万ドルでした。
- 個人の犯罪者が映画やテレビなどの豊富なコンテンツへのアクセスを提供するストリーミング機器を販売し、年間最大37万ポンド（521,000ドル）を稼いでいます。
- ダーク・ウェブ上の多くの店では、3ドル ~ 100ドルでWindowsコンピューターにアクセスできるRemote Desktop Protocolパスワードやその他のアクセス認証情報が数千件販売されているのが発見されています。

プラットフォーム資本主義は合法に見える

サイバー犯罪者は、犯罪を行うではなく売ることにプラットフォーム資本主義のアプローチを取っています。これらのサイトは、カスタマーレビュー、技術サポート、説明、評価、成功率の情報も提供しています。いくつかの例としては、以下のようなものがあります。

- ゼロデイのAdobeのエクスプロイトは3万ドルです。

- ゼロデイのiOSのエクスプロイトは最大25万ドルです。
- マルウェアのエクスプロイト・キットは、1つのエクスプロイトにつき200 ~ 600ドルです。
- Blackholeエクスプロイト・キットは1ヶ月のリース料が700ドルか1年間で1,500ドルです。
- カスタム・スパイウェアは200ドルです。
- SMSなりすましの1ヶ月間の費用は20ドルです。
- 小規模のハッキングのためのレンタルハッカーは、200ドル程度のコストです。

サイバー犯罪者の稼ぎ

- 個人のハッカーは1つまたは複数の仕事で3万ドル前後の収入を得ることができますが、複数のカードデータフォーラムを提供するプラットフォーム管理者は、最大200万ドルを稼ぎます。
- サイバー犯罪による個人の収益は、現在、平均して、ほとんどの従来の犯罪よりも10 ~ 15%高くなっています。
- 高収入サイバー犯罪者は月に16万6,000ドル以上稼ぎます。
- 中収入サイバー犯罪者は月に75,000ドル以上稼ぎます。
- 低収入サイバー犯罪者は月に3,500ドル以上稼ぎます。

資金洗浄の方法

- 流通している推定1.6～2兆ドルの洗浄資金のうち10% - 合計2,000億ドルがサイバー犯罪に起因していると考えられています。
- The Web of Profitの調査の一環として質問されたサイバー犯罪者のサンプルの少なくとも30%は、サイバー収益を物理的に送金したり、航空会社の宅配便で送金したりして外国の銀行に預金したことがあると答えています。

"マネーミュール（不正資金の運び屋）活動の95%は サイバー犯罪の活動とリンクしている。"

- デジタル決済システムがロンダリングツールとして使用されたのは、本調査でサンプリングしたケースのうち少なくとも20%で、少なくとも10%のケースではPayPalが何らかの役割を果たしていました。
- Bitcoinの取引の25%はミキサーにかけられています。
- ランサムウェアの利益の95%は、暗号通貨取引プラットフォームBTC-eで現金化またはロンダリングされました。その後BTC-eは国際法執行機関の介入を受けて取引を停止しました。

お金の保存、貯め方

- 11%は銀行や住宅金融組合に入っています。

- 8%はその他の金融資産となっています。
- 1%は車の形になっています。
- 不動産取引の1～2%は、犯罪行為によって直接資金調達されています。 - これは、毎年約15万～30万件の不動産に相当し、約37億ドル～74億ドルの価値があります。
- 調査対象となったサイバー犯罪者の30%が、収益を現金化しようとしていると報告しています。

"犯罪資産の69%は何らかの不動産の形で保管されている。"

サイバー犯罪者のお金の使い方

- 暗号通貨取引の60%が個人と結びつけることができるにもかかわらず、洗浄されたお金の4%、およそ年間800億ドルが暗号通貨に保管されています。

割合	買ったもの
15%	目先の必要性をカバーするためにお金を利用。
20%	無秩序な支出や快楽主義的な支出に走った。
15%	女友達や他の犯罪者などを感動させるためにステータスアイテムに費やす。
30%	お金を不動産などの資産に変換。
20%	さらなる犯罪行為への再投資に使われた部分もある。

EUだけでも組織犯罪グループの約35%が違法薬物の生産や取引に直接関与しており、ダーク・ウェブの活動の57%が薬物の取引に関連しています。

英国生まれのアルカイダ信者、Younis Tsouliはグループに技術支援を提供し、37,000件のクレジットカードとデビットカードのデータを収集し、その後テロ活動に再投資された350万ドルの収益を得ることに成功しました。

第1章： The Web of Profit（利益の網）

犯罪行為は、時代を経ても変わっていません。私たちの個人的な安全と財産が脅かされる標準的な方法 - これに暴行や強盗を含むかどうかは議論がありますが - があり 、これらは最古の社会以来、実質的にはあまり変わっていません。

多くの人は、コンピューター関連の犯罪、つまり現在受け入れられているサイバー犯罪の出現が、このような状況を一変させたと考えていました。マルウェアやDDoS攻撃を使ってコンピューターやコンピュータ・ネットワークを不安定化させることは、弓鋸（hacksaw）を使ってターゲットに侵入するのとは全く異なる種類の犯罪*手法*であることは確かです。しかし、一般的にサイバー犯罪は、コンピュータ・ネットワークを利用して増強、強化されたとはいえ、身近な犯罪の実行を伴うのが普通です。

サイバー犯罪経済とプラットフォーム犯罪の出現

この研究から浮かび上がってきた発見の一つには、犯罪性の本質に大きな再検討をもたらす可能性のある指標の兆しが含まれています。The Web of Profit では、犯罪は割に合わないという古い格言を再評価する必要があるかもしれません。もちろん、犯罪から報酬を*得ること*が多いことは誰もが知っていることですが、犯罪とその報酬の関係を根本的に再調整する動きが始まったようです。The Web of Profit では多くの場合、増加する犯罪を取り巻くさまざまな支援インフラに比べて、犯罪の直接的な行為はその報酬が*低いように*見えます。

"この現象で特に興味深いのは、現代の世界経済の変化を反映しているように見えることだ。"

デジタル技術は現在、ある種のポスト-犯罪の現実の中心にあり、最も顕著な犯罪発生の傾向は犯罪の原材料、すなわち特定の犯罪行為とは関係なく、そのような行為がどのようにして採掘され、交換され、そこから二次的な価値が抽出されるかということにはるかに関係しています。

この現象で特に魅力的なのは、この現象が現代のグローバル経済の中での変化を反映しているように見えることです。これは、プラットフォームが現在、社会の中で最も強力な文化的・経済的勢力の一つになっているという観察に焦点を当てています。つまり、Facebook、Google、Amazon、YouTubeのような会社、あるいは

LinkedIn、Twitter、Uber、WhatsApp、Airbnb、Instagram、Twitter、Pinterestのような第二の波、第二層のプラットフォームのことです。

プラットフォームの主な貢献は、これまでつながっていなかった人たちをつなぎ、個人が（表向きは）自分たちの利益になるような方法で情報を共有できるようにすることです。例えば、UberやAirbnbでは、タクシーや休日のレンタルサービスを提供したいドライバーや家の所有者と仲介者を介さずに直接つながることができます。同様に、Facebookは古い友人や新しい友人とつながることを可能にし、YouTubeは面白い猫の動画を共有することを可能にし、LinkedInは見込みのある従業員と雇用者がつながることを可能にしています。プラットフォーム自体はこのプロセスでは何も生み出していませんが、ユーザーは情報経済の中で最も貴重な商品であるデータをプラットフォームに提供しています。

今日データは、新しい製品や新しい目的のために、探し出し、抽出し、販売し、流行らせることができる原材料です。数百万のFacebookユーザーの記録が違法に取得され、2016年の米国大統領選挙の結果に影響を与えるために英国のデータ会社ケンブリッジ・アナリティカによって使用されていたことが最近明らかになった（Lewis & Hilder、2018年）ことは、プラットフォームによって取得されたデータが、現在では更なる犯罪目的のために利用されるということが、ますます当たり前な方法になっていることを示す印象的な例です。

また、急成長しているサイバー犯罪経済の中には、

プラットフォームに非常に近い構造が出現していることも明らかになってきています。このシステムでは、犯罪の直接的な行為は付随的なものとなり、犯罪の成果を共有し、その周辺の資源やサービスを収益源として活用するという重要なビジネスの副次的な役割になっています。

プラットフォーム犯罪の形が現れ始めている中で、サイバー経済犯罪の2つの方法が顕在化し始めているようです。

- 既存のプラットフォームを犯罪のスポンサーとして利用する。
- サイバー犯罪に特化したプラットフォームを開発する。

既存のプラットフォームを武器にする

私たちの代表的で最も尊敬されるオンライン・プラットフォームの多くが、（ほとんどの場合、知らず知らずのうちにとはいえ）犯罪を可能にしたり支援したりしていることは驚くべきことであり、サイバー犯罪の研究が著しく不足している分野であることを示しています。The Web of Profitプロジェクトのためのデータ収集とフィールド調査で、少なくとも4つの実際に起こっている手段が示唆されています。

- **データ窃盗とハッキングの対象**

  データがプラットフォームの重要な原材料であることを考えると、彼らが取得したデータがサイバー犯罪者の注目を集めていることも不思議ではありませ

ん。2013年から2016年にかけて発生したYahoo！のプラットフォーム侵害は、これまでに記録された最大規模とされており、最大30億人のユーザーに影響を与えた可能性があります（Perlroth、 2016年）。しかし、それだけではなく他にもたくさんあります。

2013年Facebookは1年近くにわたって検知されなかった侵害を受けて、最大600万人のユーザーの登録情報を危険に曝していたことを認めました（Shih、2013年）。2014年にSnapchatはハッカーによって400万人以上のユーザー名と電話番号をダウンロードされました（BBC、2014年）。2017年写真共有プラットフォーム We Heart It は、800万人以上のユーザーの個人データの侵害を認めました（Perez、 2017年）。

- **マルウェアの配布**

  大規模なユーザー基盤を持つプラットフォームは、多面的で多様な目的を持つマルウェアを配布するための肥沃な土壌を提供しています。

  2018年初頭、サイバー犯罪者が Google の DoubleClick ネットワークを悪用してクリプトジャッキング攻撃　-マルウェアが被害者のコンピューター上でビットコインマイニングソフトウェア Coinhive を実行するというもの - を行っていたことが明らかになりました（Matthews、 2018年）。
  他にも、2013年に Instagram プラットフォーム向けのマルウェアが、ブランドの製品評価を（有料で）後

押しするために、人為的に「いいね！」を作成していたことが判明しました（Vincent、 2013年）。

サイバー犯罪者は、 LinkedIn のプラットフォームを悪用して、役員やベンダーとして（非常に説得力のある）偽のアカウントを作成し、メンバーを騙して個人情報を提供させるという全く異なるアプローチもとっています（Krehel、 2016年）。

これらを手にして、フィッシング・キャンペーンを開始し、標的となる企業のシステムにマルウェアをダウンロードさせることができます。さらに、CEOや幹部の詳細情報を不正に入手することができます。この種のマルウェアにより、サイバー犯罪グループ Carbanak は100以上の金融機関から10億ドル以上を窃盗することができました（ロイター、2015年）。

- **違法な調達と販売**

  この調査の過程で、不正または違法な製品を流通または販売するためのプラットフォームがどれだけ頻繁に使用されているかが明らかになりました。現在、Amazon や eBay を通じてどれだけの偽造品や違法品が販売されているかは不明ですが、ほとんどの法執行機関は、その量は相当なものであると推測しています。

  もっとよく知られているのは、これらのプラットフォームが輸入関税や付加価値税を逃れるために利用されていることです。潜入調査の結果、英国だけでもこの方法で年間10億ポンドの損失を出しているこ

とが判明し、さらに売り手は自社の商品価格が著しく下落していることに気付き、多くが廃業を余儀なくされています。（Bowers、 2016年）。

他にも、Twitter、Instagram、Facebookなどのプラットフォームが、 “ihavedrugs”（ドラッグあります）のような明らかに露骨なアカウント名で投稿する麻薬ディーラーによって広範囲に利用されていることが最近明らかになっています（Ward & Mainment、2017年）。連絡を取り合い、写真を共有し、Wickr のような暗号化されたメッセージング・プラットフォームを介して交渉が行われます。

- **ロンダリング**

  収入の移動はサイバー犯罪者にとって長年の懸念事項であるため、これを平然と行うことができる商用プラットフォームの利用は、予測可能ではないにしても、目を見張るような発展を遂げています。ロシアのハッカーフォーラムへの投稿では、合法的またはハッキングされたAirbnbアカウントを使って、協力しているAirbnbホストへの予約や支払いを行うスキームが示されています。
  その利益の一部は、実際には誰もその施設に宿泊せずに送金されロンダリングされます（Cox、2017年）。

  フランスでは、Airbnbがキャッシュレスでのレンタルを認めているプリペイド式の Payoneer カードが、Airbnbの物件を使った資金洗浄に使われているとして、政府から苦情が寄せられています。同社は現在、圧力に屈し、フランス国内での支払いには利用できな

くなりました（Vidalon、 2017年）。Airbnb が Payoneer カードを他の場所でどうしているかは不明です。ニューヨーク当局は、この問題に非常に関心を持つようになり、Airbnb に書面で、ロンダリングのリソースとして使用される可能性のあるサイト上の違法なリスティングを削除するよう警告しました。

この種の詐欺のより手の込んだバージョンでは、2016年のTrump大統領選挙キャンペーンの元選対本部長であるPaul Manafortに対する起訴状の一つが次のようなお金に関係していることが明らかになりました。彼はマンハッタンの280万ドルのアパートを購入するのに使われた資金をロンダリングし、それを使ってAirbnbで賃貸することでさらに収入を得ていました。（Berson、 2017年）。

もう一つの選択肢はUberのようなプラットフォームを利用して、アカウントを介して資金洗浄を行うことです。ある詐欺では、偽のIDで2つのアカウントを作成します。その後ライドシェア（実際には乗っていません）が支払われ、盗まれたカードのような不正な収入源から別の種類の金融商品にお金が移動します（Teicher、 2018年）。

- **一般的な犯罪の可能化**

  例えば、犯罪者を被害者と接触させたり、コミュニケーションや共謀を可能にしたり、ジハードの勧誘やプロパガンダを可能にしたりなど、より一般的な方法でプラットフォームがどのように犯罪を助長しているのかについては、まだ誰も詳細な分析を行っ

ていません。このような方法で部分的または実質的に可能になっている犯罪の量を考えれば、その量は相当なものでしょう。しかし、もっと調査しない限り、現代のプラットフォームが提供する犯罪可能化の真のレベルは未知の要素のままでしょう。

サイバー犯罪特化型プラットフォーム

第二のプラットフォーム犯罪、すなわちサイバー犯罪に直結したプラットフォームが収益を上げるために使用されている例はまだ比較的新しい現象です。トレンドの詳細な研究はまだ行われていないません。しかし、今のところこのテーマについては、少なくとも3つの重要なバリエーションがあることが示唆されています。

- **データ取引プラットフォーム**

  おそらくここで最も自明なのは、盗まれたデータを取引するためのプラットフォームとして開発された多くのオープン・ウェブやダーク・ウェブ・サイトです。これらのサイトがどれだけ稼働しているかの数字はなく、この種の研究は、これらのサイトの出入りの速さを考えると、完成したとたんに古いものになってしまう可能性が高いでしょう。

  購入できるデータの種類は非常に広範囲にわたっています。盗まれたクレジットカードやデビットカードの詳細など、決まり切ったデータ素材の他に、様々な国の社会保障情報、生年月日、居住地の住所

などを取得することが可能で、その他の関連情報も、多くの場合、1件あたり3ドル以下で取得することができます。信用情報も購入可能で、スコアが高い（したがって、詐欺に役立つ）情報は、プレミアムレートで販売されています。

- **サービスとしてのサイバー犯罪（CaaS）プラットフォーム**

  新興のプラットフォーム犯罪モデルの第二の例として、クライムウェアまたはサービスとしてのサイバー犯罪サイトがあります。このようなサイトで利用できるデータ素材やサービスの範囲は圧倒的です。

  バンキング型トロイの木馬のような特定のツールの他に、標的型DDoS攻撃（分単位、時間単位、日単位など）、ボットネット・インフラ、既知のエクスプロイト（侵入を可能にするシステムのセキュリティホール）、特定のハッキングをオンコールで実行できるハッカー、すぐに利用可能な複製あるいは新しいフィッシングサイト、暗号化サービス、など他にもたくさんあります。レンタル可能な犯罪者向けコールセンター（Johnson、 2017年）のような真偽の怪しい話もありますが、驚くほど幅広い用途があります。

  フィッシング・メール・キャンペーンでは、被害者を騙して（銀行のサポートや税金の問い合わせなど）電話番号に電話をかけさせ、そこから個人情報を盗み出します。CaaSサイトでは、犯罪事業者がサイトに参加するために参加料のようなものを請求するこ

とがよくあります。サイトのオーナーは、取引が発生するためのプラットフォームを提供する以外に何もしなくても、ただ座っているだけで収益を上げることができます。一部のサイトでは、最大10万ドルの料金が請求されていると主張する関係者もいます（McKeon、 2017年）が、このようなプラットフォームが大きな収益を生み出す可能性があることは明らかです。

- **BitTorrent とダウンロード・プラットフォーム**

  これらのサイトは、映画、音楽、ソフトウェアなどの著作権で保護された作品を中心としたトレントサイト機能を提供しホスティングすることで知られています。Pirate Bayなどのプラットフォームは、法執行機関とコンテンツ制作会社自身によって、何回も閉鎖の試みのターゲットとされています。しかしながら、Pirate Bayはすべての試みを回避し、いまだに続いています。同様の Rarbg.to 、 YTS.ag や Torrentz2.eu など、多くの収益性の高いプラットフォームが今でも運用中です。

  これまであまり評価されてこなかったのは、収益モデルがどのように機能しているかということです。プラットフォーム犯罪の典型的な例として、海賊版素材の共有ではなく、広告や広告スペースの販売が利益を上げているということがあります。例えば、2016年に閉鎖される前の KickassTorrents プラットフォームは1,250万ドル ~ 2,230万ドルの年間広告収入が推定され5400万ドル以上の価値がありました。

（Fossbytes、2017年）。Pirate Bay のような大規模なサイトでは、600万ドルを超える年間利益を生み出しますが、比較的小規模な事業者であっても、年間約10万ドルの価値のディスプレイ広告を販売していると推定されます。

これらは、現在存在する最も明白でよく知られた共有型サイバー犯罪経済サイトのほんの一例に過ぎません。正当な経済圏とサイバー犯罪経済圏の両方でプラットフォーム・モデルが成功していることを考えると、犯罪のイノベーションがまだ予測できない方法でこのモデルを拡大し、さらに発展させるということは驚くには当たらないでしょう。明らかなのは、データを提供したり、データを入手するためにあくせくと働く多くの個人よりも、これらのサイトを管理したり運営したりしている人たちの方が、どれだけ利益を得ているかということです。

最近の例では、ランサムウェアの運営とホスティングを行った個人が、利益の3分の2を自分のために取ったという例があります（Szoldra、 2016年）。同様に、個人のハッカーは、1つまたは複数の仕事で3万ドルしか稼げないと推定されていますが（Brown、 2016年）、学術的な研究で、複数のカードデータのフォーラムを提供することで、自分で自由にできるのが50枚の盗まれたカード情報であっても、管理者は場合によっては200万ドルまで稼ぐことができることが示唆されています（Holt et al、2016年）。

第2章：サイバー犯罪による収益

サイバー犯罪に関与する主な動機として、収益の創出が明らかな役割を果たしているにもかかわらず、その詳細についてはほとんど注目されていないのは驚くべきことです。その理由の一つとして、昔から使われているサイバー犯罪のメトリクス、すなわち犯罪のコストと損失の見積もりに注目が集まっていることが考えられます。

"サイバー犯罪の世界的な収益の推定：年間1.5兆ドル以上。"

コストを決定しようとする試みは、研究者や政策立案者の間でも何かと話題になっており、（下の表が示すように）以前の推定値を更新しようとする試みが続いています。例えばDetica (2011年)は英国の場合年間30億ポンドを提案しています。

しかしながら、コスト指標の使用を巡っては、多くの混乱が生じており、すこし泥沼化しています。例えば、サイバー犯罪のコストは、サイバー犯罪による損失と常

に同じものなのでしょうか？大きな混乱を招いているのは、コストの推定値を得る際に、それが不確かなものであっても*収益の*推定値も得られるという仮定です。例えば、Norton (2011年) は、サイバー犯罪の世界的な*コストと*、マリファナ、ヘロイン、コカインの取引から得られる*利益との*間の等式を作成しました。このような主張は、多くの場合真の収益ではなく、記録された損失に依存しています。

サイバー犯罪の推定年間コスト	出典
世界で：2019年までに6兆ドル	Cybersecurity Ventures、 2017年
世界で：7,990億ドル ~ 22.5兆ドル	Dreyer et al、 2018年
世界で：4,000億ドル以上	CSIS、 2014年

表2：サイバー犯罪コストの見積もり

サイバー犯罪による損失は、サイバー犯罪者が犯罪をした結果として得られる収入や利益そのものではないことは明らかです。例えば、損失には取り締まりやセキュリティのコスト、またはダメージの修復などがその要素に含まれます。簡単に言えば、サイバー犯罪者が追加のサイバーセキュリティのコストを*使う*ことはできません。

"サイバー犯罪の収益の50%以上がオンライン市場で発生している"

もちろん、サイバー犯罪の収益を見積もる際には、

必然的に多くの注意点があります。現在議論中の最も明白な難しさは、サイバー犯罪に何を*含めるか*です。ここでの決定は、推定総額に大きな影響を与える可能性があります。例えば、偽造品を例に考えてみましょう。このような商品の取引は、サイバー犯罪の中でも最も高い収益源の一つとなってる（下記参照）ので、もし模倣品を含めるべきではないと判断された場合、模倣品を除外することで、サイバー犯罪の収益の評価が大きく変わることになります。

この問題は、サイバー犯罪の性質、特に*サイバーを利用した*犯罪（コンピューターやマルウェアの配布に依存しない犯罪）がどこまでサイバー犯罪としてカウントされるのかということについての、この分野におけるより広範な議論を反映したものです。犯罪を行う前にコーヒーを一杯飲むなどの間接的な行為が、より直接的で明白なツールの使用と同様の方法で犯行を可能にするのか？本レポートでは、**サイバー犯罪の収益とは、コンピューターが明らかに直接的な役割を果たしている犯罪から発生する収益を指します。**

信頼できる収益の推定値を得るために同様に重要な第二の問題は、信頼できるあるいは十分に包括的なデータを得ることの問題に関連しています。犯罪者は、どのようにして、どのような方法で収益を得ているのか、その詳細を簡単には教えてくれません。同様に、法執行機関、民間企業、セキュリティの専門家は、機密業務に影響を与える可能性のある情報を明らかにすることには常に慎重です。

"サイバー犯罪の収益の3分の1は営業秘密やその他の知的財産などの抽象的商品の盗難にリンクしている。"

もちろん、これはサイバー犯罪の調査全般に関わる問題であり、裁判所や警察の記録など、表向きには透明性の高い情報源が含まれている場合でも同様です。例えば、このような記録は収益については何も教えてくれませんし、資産が差し押さえられていたとしても、それらがどのように使われていたのかが明確になっていることはほとんどありません。

しかし、データが乏しいからといって、暫定的な収益についての結論を出すことができ*ないわけではありません*。社会調査では複数の情報源をまたいで三角測量を行い、データの中の不明瞭なパターンを絞り込み焦点を合わせることで、サンプル数が少なくても一般的な推論を正当化することができます。

"今日サイバー犯罪は利益が大きく、比較的入手が容易な活動のポートフォリオを提供している。"

この調査では、収益を生み出す5つのサイバー犯罪活動を利用して推定値を算出しました。様々な一次および二次ソースから指標を抽出することで、選択したサイバ

ー犯罪活動の各分野の収益指標を作成し、それらを合計して、サイバー犯罪者が現在世界で生み出している収益の初期推定値を算出しました。

本報告書では、選定された5つの分野とその推定収入は以下となります。[1]

犯罪	年間収益
不正、違法なオンライン市場	8,600億ドル
営業秘密、知的財産の窃盗	5,000億ドル
データ取引*	1,600億ドル
クライムウェア/CaaS	16億ドル
ランサムウェア**	10億ドル
**クレジットカードやデビットカードの情報、銀行のログイン情報、ロイヤルティ制度などの盗難データを取引することで得られる収益。 ***データを暗号化して支払いを要求することに基づく恐喝から得られる収益。	

表3：サイバー犯罪の年間収益の推定値

[1] これらの見積りの詳細は、本レポートの方法論のセクションに記載されています。

これらの推計は、多くの人が疑っていたことを裏付けるものです。サイバー犯罪は、武装強盗、窃盗、路上犯罪などの従来の収益を生む犯罪活動に比べて、現在では利益が大きく、比較的容易に得られる活動のポートフォリオを提供していることが確認されました。

選択されたカテゴリーには若干の作為性があります。例えば、前述のようにランサムウェアはクライムウェアの一種として含まれている可能性があります。しかし、ランサムウェアは短期間で非常に注目度が上がり収益を生み出すことが証明されていることを考え、これを別個に扱うことにしました。今後のこの種の作業では、収益のカテゴリーとそれに関連する推定値が洗練され、さらに発展することが期待されています。

どのような見積もりでもそうですが、それを導き出すには科学と同様に芸術の要素がありますが、これは*非常に保守的な*見積もりであることを明確にしておくことが重要です - 実質的な数字はかなり高くなる可能性があります。
その理由はいくつかあります。

- **収益は見えないまま**

  この数字は、上記のサイバー犯罪の5つのカテゴリーのみから導き出されたものです。他の多くの収益を生み出す分野は目に見えないか、数字の面で不完全に捉えられています。例えば、マスコミュニケーションを利用した詐欺（419事件や恋愛詐欺など）は含まれていませんが、上記の推定値を押し上げるでしょう。

このような詐欺は英国では2015年に約36億ポンド（49億ドル）、米国では約250億ドル（ICE、2010年）、オーストラリアでは約9,400万豪ドル（7,400万ドル）を稼ぎ出しており（Whitty、2015年）、合計で290億ドルを超えると推定されています。しかし、このための信頼できるグローバルなデータを得ることが困難であることと、これにより上記の1.5兆ドルの推定値が大幅に変わらないために、本レポートではこのカテゴリーを省略しています。

- **推定値が不足している可能性が高い**

  記載されているカテゴリーの中でも、関連する推定値は、おそらく実際に発生している金額を過大に示すのではなく、むしろ過小に示しています。例えば、クライムウェアのカテゴリーでは、収益は3種類の活動についてのみカウントされています。DDoS およびボットネットのレンタル、トロイの木馬関連マルウェアの販売、ハッカーのレンタル価格です。同様に、不正・違法オンライン市場の販売による収益は、違法薬物、不正あるいは違法医薬品、偽造品の3種類の商品の販売のみに基づいています。他にも、特定された収益カテゴリーのそれぞれの中で検討される可能性のある収益発生の例は数多くありますが、証拠が乏しかったり、一貫性がなかったりしたため、これらは省略されました。

- **保守的な見積もりでコストを見積もる**

  ほとんどの場合、範囲推定が可能であった場合には、収益範囲の中の低い、より保守的な値が選択されました。これは、犯罪企業の*コスト*を会計処理する一つの方法を提供します。これはやや恣意的なアプローチですが、サイバー犯罪に関与するコストを見積もる他の試みは信頼できないないため（Anderson et al、2012年）、他よりは良い方法と言えるでしょう。いずれにしても、コストを見積もらなければ、導きだされるのは（利益ではなく）収益の推定値だけです。何らかの利益の値がなければ、サイバー犯罪者によるロンダリングや支出を推定することはできません。一般的に、本レポートでは利益ではなく収益という用語を使用していますが、これは単純化と一貫性のためであると同時に、収益の方が具体的な利益よりも一般的に見積もりやすいためでもあります。

これらの条件を考慮すると、今後サイバー犯罪の収益を調査する研究者が、ここで提案されているよりも高い合計値に到達する可能性は非常に高いでしょう。しかし、合理的に確信できるものだけを使った方が良いという根拠に基づけば、これらの合計は少なくともそのような研究の出発点を形成することができるでしょう。

サイバー犯罪収益と従来の犯罪収益の比較

サイバー犯罪は、しばしば現在では従来の犯罪よりも重要であると主張されます。この主張の最も一般的な

根拠は、すべてのカテゴリーにおける爆発的な成長と前年比での増加という認識です。それぞれの収益を比較することで、その相対的な重要性を評価しようとする試みは、これまであまり一般的ではありませんでした。

従来の犯罪の収益についての理解は、サイバー犯罪の場合よりも進んでいます。利用可能なデー タソースが増えるだけでなく、従来の犯罪からの利益や損失を測定するためのたくさんの経験もあります。このような理由から、まず従来の犯罪からの収益についての知見を確かめることから始めるのが有益でしょう。

"サイバー犯罪は従来の犯罪よりも重要であると主張されることが多い。"

英国内務省が実施した英国の組織犯罪からの利益に関する先行研究（Dubourg & Prichard、 2008年）は、サイバー犯罪の収益レベルを比較評価するための一つの前例を提供しています。この比較には麻薬販売や麻薬取引によって生み出される利益のレベルと、他の最も高い収益を生み出すカテゴリーである詐欺の重要性が明確に表れています。

分野	年間利益
薬物	53億ポンド
物品税詐欺	29億ポンド
詐欺	19億ポンド
物品税対象外知的財産権の窃盗	8億4000万ポンド
人身売買	2億7500万ポンド
人の密輸	2億5000万ポンド

表 4：2008 年の英国の組織犯罪収益

より最近の世界的な研究（GFI、 2017年）では、より具体的に国境を越えた犯罪に注目し、犯罪から得られる年間利益の推定値の範囲を以下のように提示しました（次の表参照）。

これを見て解るのは第一に、従来型犯罪のこの指標の累積収益総額（1.6 ~ 2.2 兆ドル）は、推定値の上限でしかサイバー犯罪を上回っていない（1.5 兆ドルに対して 2.2 兆ドル）という点です。サイバー犯罪が比較的新しい犯罪現象であり、手法も比較的新しく進化していることを考えると、この比較は、従来の犯罪と同様にサイバー犯罪を真剣に扱うためのより直接的で具体的な理由を提供しています。

従来の犯罪	年間利益
偽造	9,230億ドル-1.13兆ドル
薬物取引	4,260億 ~ 6,520億ドル
人身取引	1,500億ドル
違法伐採	5,200億 ~ 1,570億ドル
違法採掘	120億 ~ 480億ドル
IUU（違法）漁業	155億ドル ~ 164億ドル
違法な野生動物取引	50 ~ 230億ドル
原油の窃盗	52億ドル ~ 119億ドル
違法な銃器取引	17 ~ 35億ドル
臓器売買取引	8億4000万ドル ~ 17億ドル
文化財の取引	12億ドル ~ 16億ドル
合計	**1.6 ~ 2.2兆ドル**

表5：国際犯罪による世界の利益の推定値

また、この報告書が示唆するように、従来の犯罪の多くのカテゴリーが、現在ではサイバー犯罪とどこまで相互に依存しているのかということも忘れてはいけません。例えば、麻薬密売による4,260億ドル ~ 6,520億ドル、偽造による9,230億ドル ~ 1兆1,300億ドルの利益を、デジタル技術がどこまで助けているのでしょうか。これらの従来からの活動の多くがデジタルに依存した要素を持っているのであれば、上記のような従来からの犯罪活動の多くは、ある意味ですでにサイバー化されており、サイバー犯罪からの収入にカウントされる可能性が高いと考えられます。

サイバー犯罪による個人収益

犯罪からの利益の推定値は、従来からのものであれそうでないものであれ、非常に大まかなレベルしか考慮していない傾向があります。言い換えれば、そのような収益が犯罪者の間でどのように*分配され*ているのか、あるいは犯罪企業に関与する個人にどのような収益が発生するのかについては、あまり教えてくれません。

"現在サイバー犯罪からの個人収益は多くの従来の犯罪から得られる収益より平均で10～15%も高い。"

分配はおそらく不平等であるため、一部の犯罪者は他の犯罪者よりも利用可能な多くの収入を得ることになり、これは犯罪者の資金の使い方に明らかに影響を与えます。例えば、組織犯罪グループ（OCG）のリーダーは、再投資や更なる犯罪活動をサポートするために資金を流用する必要性をより意識しているでしょう。

対照的に、一兵卒には制約があまりありません。そのため、おそらく彼らは衝動的な支出や派手な支出をするでしょう。犯罪収益の分配における不平等、または一般的に個々の犯罪者が獲得した収益についての研究は限られています。そのため、1980年代に実施された実証研究の非常に少数のものに大きく依存しています。その結果、個々の犯罪者による現在の収益の可能性についての我々の理解は、事実より少し遅れています。

ある研究（Freeman and Holzer、1986年）では、1979

~1980年に実施されたNBER Survey of Inner City Black Youth（NBER調査）から得られた、ボストン、シカゴ、フィラデルフィアのマイノリティの若者2,358人のサンプルを使用しています。このデータを用いて、Viscusi（1986年）は、犯罪による収益が年間約1,504ドルであると推定しています。これは同じサンプル内の合法的収益が約2,800ドルであることを考えると、比較的高い値です。個人に絞り込んでも、従来の犯罪の中の高額な収益を生み出す活動と、サイバー犯罪者の収益を生み出す活動に明らかな関連性があることは重要です。例えば、Viscusiの研究によると、個人の犯罪者の場合、薬物取引が窃盗よりも約3分の1多くの収入を得ていることが示されています。

このパターンは、2つの独立した調査で収集された（自己申告による）違法収益に関するデータを比較したNguyenとLoughranの研究（2017年）のような、犯罪者の収益に関する最近の研究でも見られます。彼らの研究は、プロジェクトのコスト、費用、その他の要因（異常な外れ値）により収益を絞り込むことに成功しています。彼らの調査結果は、この分野の過去の研究を引き続き反映しており、ある程度確信をもって収益が高くサイバー犯罪者にとって継続的に魅力があるものを特定することができること示しています。

"個々のサイバー犯罪者の利益を評価することは、データの不足を考えるとさらに複雑です。"

Nguyen と Loughranの研究によると、路上での麻薬の売買は平均週収900ドルであることがわかりました。収益は、強盗、強盗、小切手の偽造など、他の伝統的従来からの低レベルの犯罪行為と同等ですが、これらの活動は通常、薬物取引よりも複雑で高いリスクです。

これらの収益レベルは、BouichardとWilkins（2008年）の研究でも裏付けられており、（ほとんどが組織化された）犯罪者の年収の中央値は約46,000ドル、つまり週に約884ドルで、NguyenとLoughranの数字に非常に近いことが分かります。

個々のサイバー犯罪者の利益を評価することは、データが乏しく、信頼できる収益の平均値を出すのに十分な大規模サンプルを集めることの困難さを考えるとさらに複雑です。それでも、有罪判決を受けたサイバー犯罪者や活動中のサイバー犯罪者が特定のケースで得た利益についてわかっていることに基づいて、いくつかの限定的な推論を行うことができます。例えば、最近逮捕された6人の大規模事業者のサンプルでは、150万ドル～250万ドルの間のBitcoinその他の没収が行われています。これが彼らの事業からの年間収益に近似していると仮定すると、中間値に基づき1月あたり約16万6000ドルと計算されます。

これは従来の犯罪とほぼ同じですが、サイバー犯罪によってそのような収益を得ることができる個人が以前よりもはるかに多くなっているという重要な注意事項があります。中所得者層では、我々のサンプルのサイバー犯罪者は、（この期間に単独あるいは複数の事業から）平均して年間5万ドル～10万ドルを稼いでおり、中間値は約7万5,000ドルでした。低所得者は、1回の活動で報告された最低の収益に基づいて計算され、Nguyen と Loughranによる調査の（例えば、路上の犯罪者が捕まったり、それ以上の活動から手を引いたりしたために）1-2回の活動の所得と比較されました。

これにより、従来の犯罪者とサイバー犯罪者の収益を比較すると、次のようになります。

犯罪者のランク（月当たり所得）	従来からの犯罪者	サイバー犯罪者
高所得	$130,000+	$166,000+
中所得	$40,000+	$75,000+
低所得	$1,800+	$3,500+

表6：従来型とサイバー犯罪者の年収比較

これらの数字は大規模なサンプルを欠き明らかに投機的な側面を持っていますが、他の利用可能な証拠と合わせると、特定の示唆に富むパターンが現れているように見えます。

- 一般的に著名な従来の犯罪者、特に以下に詳述するような組織的犯罪グループのリーダーの稼ぎは、いまだに非常に高収入のサイバー犯罪者を上回る傾向

があります。

- しかしながら、サイバー犯罪者の収入は、あまり目立たない高-中所得の範囲では、従来の犯罪者の収入を上回ることが少なくありません。例えば、Holtら（2016年）が行った儲かるハイエンド事業に関する調査では、わずか50枚のカードの個人情報の販売で約25万ドル~100万ドルの潜在的な収益を生み出す可能性があることが示唆されています。対照的に、多くのオンライン・ドラッグ・ディーラーの活動は、ある種の中所得層を示しています。このプロジェクトで得られたデータによると、オンラインでのマリファナやコカインの販売は、年間60,000ポンド~80,000ポンドの純利益を得ることができ（112,000ドル以上）、ステロイドの売上高は100,000ポンド（約140,000ドル）の純利益を得ることができることが示唆されています。
- 低レベルの所得層が、前述のような比較的慎ましい単発的な活動を行っていると解釈できるならば、サイバー犯罪活動は単発的な街頭犯罪活動よりも、はるかに少ない作業量と（通常は）はるかに少ないリスクで、より良い収益を上げているように見えます。

"ハッカーや他の最前線サイバー犯罪者はしばしば重労働をしていますが、その恩恵ははるかに少ないという証拠がある。"

プラットフォーム犯罪モデルの発展の兆しとして、ハッカーやその他の第一線のサイバー犯罪者は、ハード

ワークを行うことが多いですが、その利益はデータを販売するプラットフォームを運営する者よりもはるかに少ないという証拠がいくつかあります。ある研究（Szoldra、2016参照）では、組織化されたロシアのランサムウェアグループを調査し、300ドルずつ受け取った30回の身代金に基づいて、その大部分の約7,500ドルがグループのリーダーに支払われていたことを確認しています。

前に示したように、非常に目を見張るようなレベルの収益は、このセクションの推定値から除外されています。例えば、メキシコの麻薬密売人Joaquín Loera (El Chapo)のような従来からの犯罪者 - 2010年の*フォーブス*によると世界で937番目の富豪に挙げられていた人物（個人資産が10億ドル以上）。あるいは、ヤクザのゴッドファーザー石井進は、融資、銀行取引、不動産詐欺で15億ドル以上稼いでいます。Amado Carrillo Fuentesはコカイン販売で約250億ドルを稼いでいます。サイバー犯罪で稼いだ非常に華々しい稼ぎ手についてはあまり知られていませんが、Silk RoadのRoss Ulbrichtは10億ドルの個人的な財産を蓄積したと言われています。

第3章：サイバー犯罪者の主な収益源

今や利益がサイバー犯罪とそのインフラを動かすものを理解するための鍵となるのであれば、サイバー犯罪者にとっての主要な収益源について、より洗練された認識を持つことが不可欠です。私たちは、特定の種類の収益源についてある程度の知識を持っていますが、これは断片的であり、より多くの情報に基づいた介入や壊滅を可能にする戦略的な利点を提供できるような統合された全体像には欠けている傾向があります。

このセクションでは、サイバー犯罪者がその活動から利益を得るための目立った手段のいくつかを検討し、彼らが生み出すことができる相対的な収益を評価します。しかし、以下に述べることはあくまでも選択であることを明確にしておくことが重要です。The Web of Profitは、この研究で発見できたものよりもはるかに複雑で儲かる可能性が高いでしょう。

違法オンライン市場の収益

インターネットがもたらす多くのパラダイムシフトの影響の中で、サイバー犯罪の最も有望な機会の1つはeコマースの発展とオンライン市場を介した商品の売買に由来します。2017年だけでもeコマースの売上高は23.2%増加し、小売売上高全体の10分の1を占めています。これらの売上高の総額は、2016年に比べて5.8%増の22兆7,370億ドルに迫る勢いです（Chaffey、 2017年）。ヨーロッパでは現在、個人の68%が定期的にオンラインショッピングをしていると答えています（Eurostat、2017年）。

"不正なオンライン市場は世界で最低でも年間8,600億ドルの収益を上げている。"

正規のeコマースサイトと並行する不正マーケットプレイスの成長は、The Web of Profit に多大な貢献をしており、最も有効な正規経済を反映する指標の一つとなっています。その結果、現在ではサイバー犯罪の総収入の50%以上を占める、最も重要な収益源となっています。

犯罪の利益を生み出すためのオンライン小売の使用には、少なくとも2つの種類があります。

- オークション詐欺や偽の広告など、合法的なオンライン市場の悪用によって発生する収益。
- オンライン市場で違法または不正な商品を販売することで得られる収益。

オンラインでショッピングやビジネスを行う最近の傾向は、搾取のための多くの機会を提供しています。これには存在しないもの、あるいは広告よりもはるかに劣った品質のアイテムを広告することが含まれています。また、お金や個人情報を得るための偽のウェブサイトも含みます。

これには基本的に2つの方法があります。オリジナルの本物のサイトをコピーしたり複製したりする方法と、ゼロからサイトを作成する方法です。ユーザーはDNSスプーフィングなどのテクニックを使って偽サイトに誘導されますが、複製サイトはしばしばChromeやSafariなどのブラウザによってブロックされます。一方JavaScriptを使ってブラウザのポップアップをブロックすることができるという証拠があります（Bengineer、2015年）。

中国や日本では、さまざまなサイズや価格で、さまざまな支払い方法で何百もの商品が販売されていることを宣伝している偽のeコマースサイトの例が数多く発見されています（Isaza、 2015年）。他にも、偽物を販売することで収益を上げているものがあります。2015年以降、イギリスの警察だけでも、BurberryやAbercrombie & Fitchなどの偽高級品を販売するサイトを1,000以上閉鎖しています（BBC、2015年）。

他のサイトでは、存在しないあるいはすでに入居している賃貸物件や、配達されないあるいは存在しないチケットや休暇やレジャー関連の商品を販売しているものもあります。比較的価値の低いものを販売しているサイトでも、十分な回数を重ねることで利益を得ることができます。

チケット詐欺による（購入者の）平均的な損失は英国では約80ポンドですが（Button and Cross、 2017）、2014年に英国で逮捕された9人は、Arctic Monkeys、Arcade Fire、Beyoncé、Reading Music Festivalなどのコンサートのチケットを偽って販売し、約850人から騙し取っていたことが判明しました。この表向きには地味な活動は、犯人が拘留されるまでに最大116,000ポンドを稼いでいました（Southport Local、 2014年）。

合法的なマーケットプレイスでの犯罪的搾取は、比較的簡単で低コストで実施することができますが、この種の収益源から得られる利益を計算するのは容易ではありません。大手オンライン小売業者は、利益が相当なものになる可能性があることはわかっていても、詐欺的な買い手や売り手が関与している取引の数については、あまり積極的ではありません。例えば、Amazonの返品ポリシーを操作して、元の商品が到着する前に交換品を受け取り、120万ドルの利益を上げたカップルがいました（Steiner、2017年）。しかしながら、偽造品の取引を専門としているサイトは、信頼できる情報源によると8,000億ドルを超える莫大な収益を生み出している可能性があることも知られています。

"オンラインで売られているあらゆる種類の違法品の中で 最も注目を集めているのはおそらく薬物市場でしょう。"

ダーク・ウェブ上の違法・不正商取引の世界を調査するのは、通常のインターネットよりもナビゲーション

が簡単ではないだけでなく、多くのサイトが時間のかかる口コミや評価状況や信頼に基づいてしかアクセスを許可していないため、非常に困難です。

オンラインで販売されているあらゆる種類の違法商品の中で、最も注目を集めているのはおそらく薬物市場でしょう。最近の調査で、*The Economist*が、違法薬物、合法医薬品、銃器を販売する3つのオンライン市場内で発生している収益を調べました（Economist、 2016年）。それによると、2013年12月 ~ 2015年7月までの間に約2,700万ドルの売り上げがあり、マリファナとMDMAの売り上げが全体の約50％を占めており、薬物市場が最も収益性の高い市場であることがわかりました。

法執行機関によって取り壊される前に、最大のダーク・ウェブ市場の1つであったAlphaBayは、25万のそれぞれのエントリが、すべての薬物リストの68％を売っていました。その30％はクラスAの薬物に関係していました（IOCTA、2017年）。これらの推定値は、他のエビデンスソースで見られる他の収益と比較すると、非常に保守的に見えます。例えば、オンライン薬物市場Silk Roadの撤⼱を受けて、検察官は約8,000万ドルの手数料を稼いでいた管理者 Ross Ulbrichtにより運営されていた2.5年間で12億ドル以上を稼いでいたと主張しています。Ulbrichtはこれを否定し、これらの金額のほとんどは運営と成長のために使われたと主張しています。2013年までに、FBIはUlbrichtと関連があると主張するBitcoin口座の3,450万ドル（Greenberg、 2013年）と、FBIが手の届かなかった流通中の2,200万ドルを差し押さえました。

しかし、最近の研究（Kruithof et al、 2016年）では、

オンライン薬物市場は、世界の薬物市場全体としての規模、米国だけで年間1000億ドルに比べると全然大きくないことが確認されているようです。この研究では、このようなサイトが年間約1億8000万ドルを積み上げていると推定されています。 近年、オンラインの販売数量が3倍に増加していることを考えると、それほど長くはないかもしれませんが、同等の収益を達成するまでには、いくつかの道のりがあることを示しています。

対照的に、違法な処方薬のオンライン販売は、犯罪収益のかなりの部分を占めており、その総額は約4,000億ドルにのぼります。

知財と営業秘密の盗難

アイディアの盗用による収益の創出（Wall、2016年）は、他の多くのサイバー犯罪と同様に、何も新しいものではありません。古代ギリシャでさえも、彫刻家は他の人が自分の作品を自分のものと主張するのを防ぐために、作品に商標を付けることを余儀なくされていました。しかし、技術の進歩は、ここでの利益の機会に大きな影響を与えました。例えば、英国のアンネ著作権法（1710 年）は、複﨟権をめぐる最初の法制化の枠組みを作ったもので、 印刷という新しい技術とそれが促進した海賊版の書籍やパンフレットの急激な普及に対応したものでした。300年後、デジタル技術は、誰かのアイディアを他人の収益源に変えることを可能にするための最新のツールを提供し、他の誰かの仕事から利益を得ようとする犯罪者のための全く新しい収入源を生み出しました。

"知的財産権と営業秘密の窃盗は世界で最低でも年間5,000億ドルの収益がある。"

最初の波は、映画、音楽、コンテンツのダウンロードに関連した知的著作権に集中していました。これは、アーティストの権利にダメージを与える可能性について、道徳的なパニックの波を生み出しました。主にクリエイティブ産業が自分たちの製品の独占を維持したいと考えていることに起因しています。また、数人の象徴的な違反者に対する厳罰的な公開処罰から、iTunesのようなサイトを通じて提供されている所有者のコンテンツの固定化に至るまで、かなり迅速な対応を生み出しました。

様々な方法で今も手ごろな収益源となっています。例えば、音楽の違法コピーだけでも年間約125億ドルの価値があると推定されています（Siwek、 2007年）。しかし、サイバー犯罪者は盗まれたコンテンツを収益化するためのより巧妙な方法を進化させており、現在では特にプラットフォームを利用して、はるかに堅牢な収入源を生み出しています。典型的には、次のようなものがあります。

- 違法コンテンツを取得できるサイトでの広告販売。
- そのようなサイトのサブスクリプション販売。
- 海賊版ソフトウェアのような商品のコピーの販売、あるいはそのようなサイトへのマルウェアの仕込み。

IPを利用して収益を生み出す創造的な方法は、コンテ

ンツ窃盗サイトが2014年に広告収入だけで2億2700万ドルを稼ぎ出したという事実に示されています（DCA、2014年）。広告のみで利益を得ているサイトは、平均して年間約440万ドルの収益を上げており、最もトラフィックの多いBitTorrentやP2Pポータルサイトでは年間600万ドルを超えています。調査した小規模なサイトでも、広告収入で年間10万ドル以上の収益を上げています。

プラットフォーム犯罪モデルは、直接的な窃盗行為が仲介的な販売方法によって徐々に補強されていることにも見ることができます。例えば、違法にコピーされたコンテンツを手に入れるために時間を費やすのではなく、現在では、映画やテレビなどの豊富なコンテンツへのアクセスを提供するストリーミングデバイスを販売することで、年間最大37万ポンド（521,000ドル）を稼いでいる犯罪者もいます（Sulleyman、 2017年）。

"グローバル企業の20%がサイバースパイ活動をビジネスにとって最も深刻な脅威と評価している。"

米国だけでも著作権侵害からの収益は約3,000億ドルと推定されてる（IPC, 2013）ので、世界的にはもっと高い数字になるでしょう。しかし、上記で示唆した知的財産権侵害による収益の実質的な部分は、企業の知的財産、企業の営業秘密、企業データ（例えば、事業計画、新製品開発など）の盗用と販売によるものです。加害者の多くが政府やその他の企業であり、その利益が金銭的なものよりも抽象的なものであることが多いことを考えると、

ここで明確な収益の合計を確定するのは多くの困難がありますが、控えめな仮定であっても、この取引は年間約2,000億ドルの価値があると考えられます（議論はAppendixを参照）。最近の調査（Trend Micro、2017年）では、グローバル企業の20%がサイバースパイ活動をビジネスにとって最も深刻な脅威と評価していることが示唆していることに驚きはありません。米国の組織の約20%がサイバースパイ関連の攻撃を受けたことがあります。

"営業や財務上の秘密を売るために、企業のスタッフは、Kick Ass MarketplaceやStock Insidersなどの地下サイトを使用しているようです。"

彼らが懸念しているのにはそれなりの理由があります。最近の調査データによると、データ漏洩の平均コストは約500万ドルと推定されており、記録1件あたり13ドルから217ドルの範囲にあります（Ponemon、 2015年）。他の課題はより技術的なものです。例えば、4年前のリモート・アクセス型トロイの木馬H-Wormをベースにした Copperfieldのような新しいサイバースパイツールが利用可能になりました。このマルウェアツールは、データ盗難や偵察のために設計された可能性が高いようですが、重要インフラへの攻撃にも関与しています。

この問題のもう一つの解釈は、組織化されたグループが、標的とする企業のシステムにデータを盗むことができるマルウェアをインストールするために使用する戦術が常に進化しているということです。例えば、ロシア

のサイバースパイ組織 Turla ギャングは最近、Adobe Flash のインストーラに関連する正当なIPアドレスを使用してマルウェアを偽装していることが判明しています（Apps & Finkle、 2014年）。その多くの犠牲者の中には米国国務省も含まれています。

他にも、2017年にMicrosoftのリモート・デスクトップ・プロトコル（RDP）を使ってWindowsコンピューターへのアクセスを得るためのリモート・アクセス認証情報が販売されているという証拠が浮上しています。これは、企業のデータを盗むために仮想デスクトップにアクセスし、犯罪者がシステムを遠隔で管理することを可能にします。このトリックは、成功するためにマルウェアを必要としないという点で特に効果的で、一度侵入すれば、サイバー犯罪者は、通常は被害者の知らないところで、ほとんど何でも好きなものにアクセスすることができます。

ダーク・ウェブ上の様々なアンダーグラウンドストアがRDPパスワードやその他のアクセス情報を現在3 ~ 100ドルで販売しているということが発見されています。一度購入すると、何千台ものWindowsコンピューターのデータが窃盗の対象となります。例えば、 Ultimate Anonymity Services や xDedic のようなダーク・ウェブのサイトは、米国、中国、ブラジル、インドのWindows XPやWindows 10コンピューターへのアクセスを可能にする数千のRDP認証情報を提供していることが判明しています（Palmer、 2017年）。

営業秘密の取引は、取引に関与するインサイダーの数が増加していることによっても著しく促進されていま

す。会社の従業員は、取引や財務上の秘密を販売するために、 Kick Ass Marketplace や Stock Insiders などの地下サイトを利用しているようです。Kick Ass Marketplace（これは、似たような名前のトレントサイトとは異なるようです。明確ではありませんが。）は、エキスパートが監視してデータを正確なものから悪いものまで評価し、株式の選択や投資に関するアドバイスまで提供しています。このサイトの既知のメンバーには投資会社が含まれており、彼らはこのサイトを利用して競争上の優位性を得ようとしているようです（Darknetmarkets、 2017年）。

これとは対照的に、 Stock Insiders のサイトは、より露骨に犯罪的であるように見え、銀行員に盗難されたクレジットカード情報を提供するように誘惑していることさえ判明しています。また、このサイトは、盗まれたカードの所有者になりすます個人を募集して運営しているとも言われています。店頭でカードが機能するかのテストが行われます。また、これらの操作を支援するための店舗の従業員が勧誘されていたという証拠も発見されています。

製薬会社のように価値の高い知的財産を持つ企業は、特にこの種の企業窃盗の被害を受けており、現在では法執行機関と密接に協力してEnigmaのようなサイトに潜入しようとしています。このオープン・ウェブ・マーケットプレイスは、企業情報の売り手と買い手候補者をマッチングさせることに純粋に重点を置いていましたが、捜査官の侵入を疑い現在は運営を停止しています（Krebs、 2016年）。

銀行員がこのようなサイトを利用して、インサイダー取引やその他の不正行為によって市場での優位性を得ようとしたり、企業が機密情報を盗み出したりしようとすることは、The Web of Profitが合法的な経済とサイバー犯罪の経済を曖昧にしていることの顕著な例です。このようなサイトが生み出す利益は、プラットフォーム犯罪モデルの魅力をさらに物語っています。Kick Ass Marketplace のサイトだけでも、このような活動から毎月3万ドル以上を稼いでいると推定され、約200BitcoinのBitcoinウォレットを保有しています（Darknetmarkets、2017年）。一般的なプラットフォームと同じように、サイトの所有者は、この情報を共有できる出会いの場を提供することで、他の人に犯罪行為をさせて、簡単にお金を稼ぐことができます。

データ取引からの収益

サイバー犯罪のビジネスモデルの中で、はるかに確立された収益源は、個人のデータを獲得または傍受し、不正に利用する技術です。これは、個人情報の盗難の言い換えというわけではなく、転換可能な価値を持つデータのほぼすべての形態に関与するものです。

私たちのお金の電子版への移行、すなわち、交換メカニズムとしてのデビットカードやクレジットカード取引の使用やオンラインバンキングの出現は、犯罪機会に関する全く新しい空間を提供しています。データタイプと他のデータタイプの取得と取引は、データが今や主要な商品となっている、The Web of Profitと合法的な経済と

の間の最も明確な一致点を表しています。

"データ取引は世界で最低でも年間1,600億ドルの収益を上げている。"

この機会はサイバー犯罪者によって巧妙に悪用されており、主に2つの収益源を生み出しています。

- 個人情報などのデータを不正に利用して得る収益（カードや銀行の不正利用）。
- データの売買で得る収益。

カードや銀行の不正行為から得られる数字は、データ盗難からの収益を測定するためのより信頼性の高い情報源の一つとなっています。これらの数字は、銀行やカード当局によって包括的に記録されているだけでなく、当然のことですが損失が収益として読み取れます（カードでの犯罪支出が直接損失に変換されるため）。多くの情報源がデータの悪用をダブルカウントしているため、多少の注意が必要です。例えば、英国金融詐欺行為の年次報告書のような情報源では、eコマースによる損失の数字の中に、リモートで使用されたカードデータによる損失の数字が含まれています。しかし、米国と欧州の損失総額を合算することで、不正使用されたカードからの収益を合理的に正確に見積もることは可能です。

2015年に記録されたカード詐欺による損失は約220億ドル（Nilson、 2016年）に達しましたが、ヨーロッパで2016年にFICOが提供したかなり正確な損失推定額は約18億ドルでした。損失の中で最も多いのは英国で、約6

億ポンド（FICO、2016年）となっています。丸めると、実際に盗まれたカードが使われたことによるサイバー犯罪の収益だけで240億～250億ドルになることを示唆しています。

しかしながら、盗難されたカードの利用は、データから生じる収益の一部にすぎません。データの*取引*も考慮に入れる必要があり、実際の利用をはるかに上回る収益を提供している可能性があります。データや他の多くの商品を売買できる多数の大規模なプラットフォームの存在は、現在では十分に確立されており、価格設定が透明であるため、他の種類のサイバー犯罪の収益を評価するよりも、ここで得られる収益を評価する方が、一見したところ簡単です。

AlphaBay や The RealDeal のような大型プラットフォームはここ数年で撤去されていますが、これらを代替するために参入したサイトが多数あります。これらのサイトの多くは、Facebook や Twitter のページへのリンクでプラットフォーム犯罪モデルの目印を示し、データ取引サイトへのアクセスを希望する人のための情報やガイダンスを提供する DeepDotWeb のようなニュースや情報サイトでサポートされています。

Holt et al（2016年）がこのようなサイト(カーディング・フォーラムとも呼ばれます)で行った研究では、盗まれたカードを取引した個人やグループが、たった50枚のカードから25万ドルから100万ドルの収益が得られたことがわかりました。

ここでの収益の他の指標は、サイバー犯罪のアマゾ

ンのような役割を果たしたデータ取引サイトInfraudの最近の閉鎖の例で見ることができます。このサイトは、盗まれた生年月日、住所、パスワード、社会保障番号、支払いカードの詳細、その他の個人を特定する情報を、印象的なポートフォリオで売買していました。このサイトの価値は、閉鎖された時には約5億ドルと推定されていました。

しかし、収益に関する情報が比較的透明であるにもかかわらず、どの様な方法でも妥当な合計を計算することは容易ではありません。明らかな問題の一つは、価格設定の変動性です。これには需要と供給の問題が大きく関わっており、希少なデータは容易に入手可能な例よりもはるかに高い価格が設定されます。例えば、2013年に発生したTargetチェーンの大規模な侵害では、カード記録1枚あたり15～20ドルだった価格が、あっという間に0.75ドルにまで下落したと推定されています。もちろん、このようなサイトを介して実際にどれだけのデータが売られているという点についての確実性の欠如もあります。

しかし、2016年には約40億件の異なる種類のデータ記録が盗まれたことがわかっています（RBS、2016年）。その後、サイト間で取引される3種類のデータ（クレジットカードやデビットカードのデータ、銀行や決済システムのデータ、Netflixやアプリのアカウントへのログインデータ）だけを取り出し、さまざまなサイト間でこれらのデータの価格を平均化することで、データ取引によって現在発生している年間収益は約1,600億ドルと推定することができました。サイト間で取引される他のデータ（例えば、ポイント、クレジット履歴、医療記録、社会

保障の詳細など）も見積もって含めることができれば、この合計額はおそらくもっと高くなるでしょう。

クライムウェアとCaaSからの収益

新興のサイバー犯罪経済と収益を生み出すためのプラットフォーム・アプローチの中核にあるのは、サイバー犯罪の委託をサポートするサービスの範囲の拡大です。この収益生成の形態は、最も収益性の高いものではありません。しかし新しい収益源であり、成長の急速な速度を考えると、これから大きく伸びる可能性があります。

"クライムウェアとCaaS（サービスとしてのサイバー犯罪）は最低でも世界で16億ドルの年間売上高がある。"

サイバー犯罪のためのツールやサービスの販売を中心とした収入源の発展は、深刻なサイバー犯罪が特定の犯罪を実行すること自体に依存するのではなく、犯罪を実行するのではなく売るというプラットフォーム資本主義のアプローチに依存するようになったことを物語っています。

本質的にはクライムウェアの収益源はサービス産業で、サイバー攻撃のためのツールを提供することに端を発していますが、現在ではサイバー犯罪に必要なものが買ったり雇ったりして何でも揃う、ある種の出来合い品の倉庫施設へと進化しています。したがって、この方法

で利益を上げる犯罪者は技術に精通したハッカーの伝統的なロマンティックなイメージではなく、技術サポートや顧客フィードバックのようなアドオンを提供する小売業者やサービスプロバイダーとの共通点が多い傾向にあります。

ここでどのような種類の収益が得られるかを推定することは複雑な計算を伴います。この種の素材が販売されているサイトにアクセスできれば、確かに証拠はあります。しかし、いくつかの要因が確定的な収益に到達するのを非常に難しくしています。

- アクセスできるこの種のサイトが非常に多いこと。
- 価格が急速に変化すること。
- クライムウェアの種類による価格が違うこと。

例えば、2012年にこの調査のために調査したサイトでは、Adobeのゼロデイのエクスプロイトは何であれ5,000 ~ 30,000ドルの費用でしたが、iOS用の同様のツールは最大で25 万ドルでした（Ablon et al、 2014 年）。同様に、2006年にはマルウェア・エクスプロイト・キットは20ドル程度で入手できましたが、現在では最低でも200ドル程度になっています。

どのような小売企業でもそうであるように、一部の␣品は他の␣品よりも消費者に人気があります。例えば、最も成功したエクスプロイト・キットの1つであるBlackholeは（最盛期には）1ヶ月のリースが700ドルで販売され、1年間のライセンスは1,500ドルでした（Krebs、2013）。

多くのクライムウェアサイトのショッピングリスト

の特徴は、マルウェアやエクスプロイトの価格設定のオプションが提供されていることが多いことです。ロシアのウェブサイトの例では、1エクスプロイトあたり200ドルから600ドルの間で製品を提供していました。Operaシステムのエクスプロイトは、役に立つ説明、レーティング、そしてもちろんコストを提供しています。

**"約200ドルでカスタム・スパイウェア
わずか20ドルで1ヶ月のレンタル
SMSなりすましが入手できる。"**

もっと経済的なオプションもたくさんあります。例えば、ダーク・ウェブ上の主要なクライムウェア・プロバイダー5社の様々なサービスの価格を比較した研究（Barth、 2016年）では、カスタム・スパイウェアを約200ドルで作成でき、月20ドルでSMSなりすましを1ヶ月間レンタルすることができます。また、ツールだけでなく特定のスキルをレンタルことも可能でした。Checkatrade のようなサイトで電気技師や配管工を雇うのと同じように、Rent a Hackerのようなサイトがハッキングサービスを提供しており、小さなハッキングの平均コストは約200ドルです。

DDoS やボットネットのレンタル、マルウェアの購入やレンタル、ハッキングサービスのレンタルの 3 種類のサービスだけに焦点を当て、これらのサービスが提供されている 5 つのプラットフォームの平均コストを調べたところ、その推定年間収益が約 16 億ドルであることがわかりました。このようなサイトでは、通常より多くの

サービスが提供されていることを考えると、これは実際に稼いでいる金額よりも大幅に低い可能性が高いでしょう。この調査では、クラウドベースのDDoS攻撃、Gmailへのアクセス、TripAdvisorのようなサイトでの評価の操作、小論文の成績変更、記録の削除（免許証のポイントや犯罪歴など）、Amazonや他の商品のレビューの強化など、多くの事例が見つかりました。

ランサムウェアからの収益

支払いや身代金を支払わない限り、暗号化マルウェアをシステムに送り込む（または送ると脅す）ことは、比較的新しい犯罪現象として認識されており、現在のレベルにまで増え始めたのは、約6年前（2012年頃）からです。もちろん、脅迫や恐喝によって収益を得ることは、古くからある犯罪行為であり、サイバー犯罪の前例もあります。

例えば、Graboskyの報告によると、1993年 ~ 1995年にかけて、システムがクラッシュしたことを話すことで4,200万ポンドが機関から恐喝されたとのことです（Grabosky et al、 2002年）。しかし、今につながるランサムウェアの起源は、デバイスやシステムに危険があるという簡単な脅しを送ってくるソフトウェアであるスケアーウェアの使用がより広く注目され始めた2008年頃から始まっています。

"ランサムウェアは世界で最低でも年間10億ドルの収益を上げている"

しかしながら、収益の創出という点では、ランサムウェアのこれらの先例はあまり成功していませんでした。サイバー犯罪者がランサムウェアのモデルを洗練させるにつれて、収益の急増は劇的なものとなりました。例えば、2014年に登場したランサムウェア Cryptowall は、1,800万ドルから3億2,000万ドルの利益を生み出したと推定されています。その成功により、2014年 ~ 2016年の間に100以上の亜種が出現し、ランサムウェアが現在最も収益性の高いサイバー犯罪を代表するものであるという印象を与える一助となりました。

NYUとUC San Diegoの研究者による最近の調査（Googleとの提携）では、ランサムウェアの被害者が過ヂ2年間で約2,500万ドルの身代金を支払っていたことが報告されています（UCSD、2017年）。これは月平均で100万ドル以上に達していました。

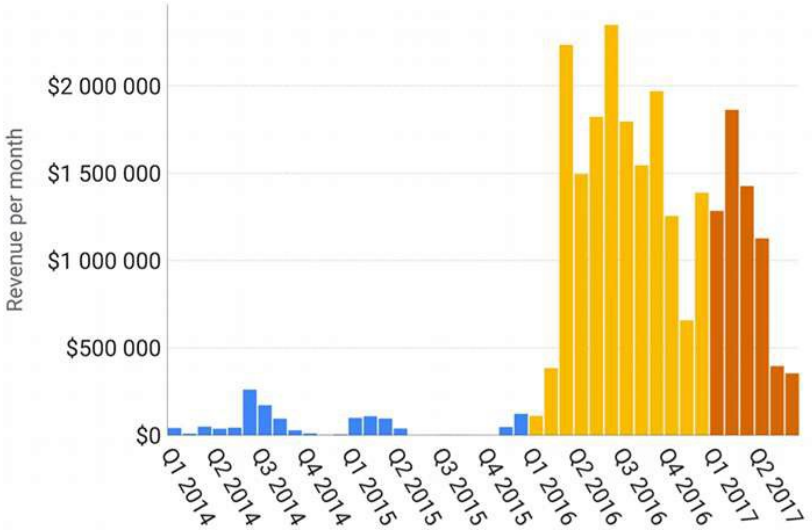


図 1：ランサムウェアの月次支払い額 2014 ~ 2017年
出典：Google、UC San Diegoなど

ランサムウェア	期間	推定利益
CryptoLocker	2013	~300万ドル
Cryptowall	2014-16	~1,800万 ~ 3億2,000万ドル
Locky		780万ドル ~ 1億5000万ドル
Cerber		690万ドル
WannaCry	2016	$55,000-$140,000
Petya/NotPetya		$10,000

表7：ランサムウェア🚄品からの収益

"収益生成を目的としたランサムウェアと破壊を目的としたランサムウェアは違う。"

ランサムウェアによる収益のより高い推定値は、2016年のランサムウェアの支払いだけで約10億ドルに達することを示唆したFBIが作成した数字で見つけることができます（NBC、 2017年）。このような対照的な見積もりはサイバー犯罪の調査では典型的なものですが、結論から言うと、2500万ドルであろうと10億ドルであろうと、ランサムウェアは現在、サイバー犯罪者にとって成長を続ける収入源を提供しているということです。

しかし、上記の収益の内訳が示すように、「最も収益性の高いサイバー犯罪」ではありません。ランサムウェア攻撃の犠牲になることがどんなにダメージを与えストレスになるにしても、不正なオンライン市場のような高収益を生み出すものと比較すると、ここでの利益はかなり小さいものになります。

また、ランサムウェアの主な機能が常に収益であることも明らかではありません。例えば、WannaCryやPetya/NotPetyaのような注目度の高いランサムウェアを調査した研究者は、要求された身代金の収益化があまり効果的に行われていないことを発見しています。つまり、収益を得るために設計されたランサムウェアと破壊を目的として設計されたランサムウェア（おそらくは国家権力の意向によるもの）は違うということです。

ケーススタディと事例

大宇IP盗難

2009年、韓国企業の大宇はセダンの新型車に関連する6,000以上のコンピューターファイルが従業員によってロシアの自動車メーカーTagAZに渡されていたことを発見しました。（米商工会議所、2015年）。同車の開発には約2億4,500万ドルの費用がかかっていました。彼らが提出した差止命令は、Tag AZが営業秘密を使用したり開示したりすることを防ぐことに成功しました。

大学へのFruiflyスパイウェア攻撃

2017年、"Fruitfly"と呼ばれるMacコンピューターを標的としたスパイウェアが米国の様々な生物医学施設、特に大学内で検知されました。このマルウェアはウェブカメラへのアクセスやスクリーンキャプチャを可能にし、異常な発信トラフィックが検知され初めて発見されました。誰が、どこで、どのような目的で行ったかは不明ですが、生物医学データの価値が高いことから、動機があるのは明らかです。

ThyssenKruppへのハッキング

2016年、ドイツの鉄鋼メーカー ThyssenKruppは、おそらく中国のサイバースパイグループWinntiによってハッキングされていたことを発見しました。同社のプラントエンジニアリング部門から技術的な営業秘密が大量に盗まれましたが、その額は発表していません。この攻撃は、サイバー犯罪者にとって魅力的な価値の高いIPを保有しているドイツ企業が被る一般的なパターンでした。ドイツの業界団体Bitkomの最近の調査によると、ドイツ企業の半数以上が過去2年間にスパイやデータ盗難の被害に遭っており、その被害額は年間550億ユーロを上ることが示唆されています。

ノルウェーのダークウェブハウスの知財秘密

2017年後半、ディープウェブサイトがノルウェーの多くの企業に属する営業秘密を取引していたことが判明しました。例えば、Statoil社は、風力発電プロジェクトに関連するデータが盗まれ、その後ダーク・ウェブで販売されていたことが判明しました。

サウジ政府へのスピアフィッシング攻撃

2017年に、サウジアラビアの12の政府機関が、スパイ活動を目的としたスピアフィッシング攻撃の犠牲になっていたことが発覚しました。この攻撃は、コンピューターにマルウェアを送り込みデータを探し盗み出すことを目的としていました。また、ここ数年はサウジアラビアの企業、特にエネルギー部門が、サイバースパイ集団 Greenbug やハッキング集団 Shamoon のような悪意あるアクターからのスパイ攻撃の犠牲になり、2012年には石油会社Saudi Aramcoが35,000台のコンピューターを破壊されました。

第4章 ：ダーティマネーのロンダリング

サイバー犯罪からの収益を推定することは、お金の行方を追う上での課題の一つに過ぎません。収益がどのようにして、隠されたり洗浄されたりしてその価値を維持する形に変換されているのかを理解しない限り、その痕跡をたどることは不可能です。次の支出のセクションで示唆されているように、いくつかの収益はかなり迅速に処分されているように見えます。しかしながらその多くはそうではないため、後日支出するために隠す方法を見つけるためには、継続的な工夫が必要です。

"現在の最善の予測では、サイバー犯罪の収益は、世界のマネーロンダリング総額の（最小で）約4% ~ 10%を占めているとされている。これは、2,000億ドルのサイバー犯罪の収益に相当する。

現在流通しているロンダリングされたお金の量を計算するための様々な試みが行われてきました。例えば、

1998 年に国際通貨基金は、世界の国内総生産の 2-5%までの金額が洗浄されていることを示唆し、その時点での価値は 5,900 億ドルから 1.5 兆ドルの間でした。

国連（UNODC、 2011年）が発表したより最近の推計によれば、世界の GDP 総額の約 2 ~ 5%（最大 2 兆ドル）が不正またはロンダリングされた形で流通している可能性があることが示唆されています。しかし、ロンダリングに対する認識と規制により、銀行や金融機関が異常に多額の預金を報告する役割を補い始めたことで、（理論的には）犯罪者が金融システムを利用して利益を現金化することが難しくなってきています。しかし、汚れたお金をきれいに洗い流すことは、どのような犯罪企業にとっても長年の問題なので、様々な方法が試行錯誤され、サイバー犯罪者が望んでこれを悪用しようとしても驚くことではありません。さらに、デジタル経済によって提示された新しい手法も出現し始めています。

従来のロンダリング

サイバー犯罪者が利用してきた、従来からのロンダリング方法には以下のようなものがあります。

- **銀行システムの不正利用**

  合法的な銀行システムを使ってお金を隠すことができるということは、「悪いお金」をすぐに良いものにすることができるので明らかに魅力的です。これは、銀行や金融機関内で何らかの形での共謀が必要になります。そして、これは珍しいことではありま

すが、報酬はそのような機関の内部者を誘惑して援助をもらうのに十分に大きいでしょう。

2017年3月、HSBC、Lloyds、Barclays、Couttsを含む英国の銀行は、“The Global Laundromat” と呼ばれる巨大なロシアのマネーロンダリング活動への関与の可能性があるとして、調査を受けていることが判明しました（Harding et al、 2017年）。200億 ~ 800億ポンドが2010年 ~ 2014年の間にロシアから流出しましたが、なぜこれらの銀行がモスクワからのおよそ2,000件の7億8000万ポンドを超える疑わしい取引を報告しなかったのかという疑問が生じました。

銀行や銀行員が協力すれば簡単に資金洗浄ができることを考えれば、サイバー犯罪者がすぐにこれに目をつけたことは驚くに値しません。2017年、英国国家犯罪対策庁は、Barclaysに勤務する不正な銀行員を含む5人の男たちのグループによって、1,600万ポンド以上がサイバー犯罪者のためにロンダリングされていたことを発見しました。このグループは、東欧のサイバー犯罪者に資金を送り返す前に、約400の銀行口座を開設し、盗んだ資金をフィルタリングするために使用していました（Sky、 2017年）。同様に、銀行員がダークサイトを利用して情報を流したり、詐欺に勧誘されたりしたという証拠から、この種の活動は見かけ以上に広まっている可能性があることが示唆されています。

- **シェル法人や架空ビジネスの利用**

  シェルや架空ビジネスは、汚れたお金をきれいなも

のに変えるために使われることがあります。資金を保護する手段としてのこれらの事業体の最近の成長は顕著です。1980年代半ばには、英領ヴァージン諸島で登録されていたこのような企業は5,000件に達してませんでした、1990年代半ばには12万件を超えています。ケイマン諸島には 1960 年代初頭にはそのような企業はありませんでしたが、1995 年には 23,500 社に達しています（Richards、 1998年）。

ここでの傾向は十分に明らかであり、現金に余裕のあるサイバー犯罪者は、他の犯罪者と同様に収益を隠すためにこのオプションを利用したいと考えていると推測されます。Hubbs (2014年)は、サイバー犯罪者は現在、この詐欺の最も頻繁な利用者の一人であると報告していますが、確固たる証拠はまだ乏しいままです。しかしながら、東京のBitcoin取引所Mt Goxから50億ドル以上のビットコインが盗まれたことに関連した最近の1つの事件は、この考えを裏付けるように見えます。英国の登録企業であるAlways Efficient LLPは、大規模なサイバーロンダリングの結果として閉鎖されたライバルのBitcoin取引所BTC-eのシェル会社として活動していたようです（White、 2018年）。

シェル会社の利用を規制するために、新しい規則では、PSC（重要なコントロールを持つ人物）を常にリストアップしなければならないことになっています。一方、Always Efficient の最新の PSC は、モスクワのナイトクラブの DJ で、事業に関する知識を一切否定しています。この事実とAlways Efficient の住所がマネー

ロンダリングの疑いがある他の企業と共有されていることから、同社の正当性と、Mt Gox から取得した収益を隠す役割を果たしその後 BTC-e を使ってマネーロンダリングを行っていたのではないかという点に対する疑惑が浮上しています。

- **金融その他の資産への投資**

  資産に投資してお金を隠すことは、非常に成功してきたロンダリングの形態です。目的は、多額の現金を目立たないが同じ価値のあるものに変えることです。これは、金融資産あるいは希少美術品やワインなどの場合もあれば、不動産や土地、あるいはエネルギーや石油産業への投資の場合もあります。

  研究者たちはサイバー犯罪者が現在、金融市場を投資に利用し新たな収益を得るために市場を利用する前に、M&Aに関する機密データを盗み出して、積極的に金融市場を利用しようとしている証拠をディスカッションフォーラムで発見しています（Kuchler、2014年）。この調査のために行われたフィールドワークの中で、恋愛詐欺を専門とするカリブ海地域のサイバー犯罪者が、ジャマイカの不動産に多額の投資を行っており、それがジャマイカの GDP に影響を与えていることが明らかになりました。

- **ギャンブルとカジノ**

  カジノを利用したマネーロンダリングは、古くから好まれてきました。例えば、ギャンブルのチップを購入し、それを売却したり他の物に変換したりする

ことは比較的簡単なことです。最近のあるスキームでは、ある資金洗浄者が市内の様々なブックメーカーでリスクの低い賭けを繰り返し、その結果損失率は7%になりました。その後、賞金の小切手をその中にたまたま犯罪者もいる 10 人の異なる第三者とその家族の名前で 14 の銀行口座に振り出しました（Reuter、 2005年）。

無免許オンラインギャンブルサイトの成長は、サイバー犯罪者の資金をロンダリングするための全く新しい分野の機会を提供しています。オンラインギャンブル業界は2016年には約390億ドルの価値があり（Cosgrave、2014年）、無免許サイトの数は非常に多い（2011年でさえ25,000以上）ということは法執行機関がそれらを介して資金がどのようにロンダリングされる可能性があるかを追跡することはほぼ不可能であることを意味しています。2018年初頭、英国ギャンブル委員会の調査によりマネーロンダリング規制に重大な問題があること、特に疑わしい活動に関する適切な情報を提出しなかったことが明らかになったため、最大5つのオンラインカジノが英国で運営するライセンスを失う可能性があることが明らかになりました（Davies, 2018）。

- **電信送金**

  Western Unionのような昔ながらの電信送金サービスを利用して、お金を管轄区域間で簡単に移動させることができます。サイバー犯罪者は、盗まれたデータやCaaSの支払い、デジタル通貨の購入などにこれら

の仕組みを利用することに熟練しています。ナイジェリアでの調査（Panda、 2010年）では、定期的にWestern UnionやMoneyGramを使って資金を送金していたことが報告されており、ある個人は以下の理由から前者を好んでいたと報告しています。「…Western Unionの代理人自身がゲームに参加しているので、偽の身分証明書を使ってお金を請求することができ、彼らは自分たちのために5%を徴収するだけです」と報告しています。

2017年、Western Unionは米国司法省から5億8600万ドルの支払いを命じられ、詐欺罪を示談しました。Western Unionには、2004年から2015年の間に55万件以上の不正送金に関する苦情が寄せられており、そのほとんどが、宝くじ詐欺、オンライン恋愛と出会い系詐欺、419詐欺、振り込め詐欺などのサイバー犯罪に関連し、その他の違法行為の複数の事例がありました。これらの詐欺の一部として6億3,200万ドル以上が送金されました。

司法省はまた、不法移民が密輸業者に支払うために中国に数百ドルから数百万ドルを送金するなど、人身売買や密輸にWestern Unionが広範囲に利用されていたことも明らかにしました。Western Unionは、違法な仕組取引が行われていることを認識していたようで、Western Unionの所有者または従業員の少なくとも29人の有罪判決が記録されています（Pananini,2001年）。アルバニアやナイジェリアのような既知のサイバー犯罪センターから、世界中への大規模な送金が行わ

れているという信頼できる証拠が見つかっています。

- **マネーミュールとキャッシュドロップ**

  もう一つの非常に確立されたロンダリングの方法は、個人を利用して犯罪収益を物理的に運んだり受け取ったりする、いわゆるミュール（ラバ）です。この方法で送金される資金の規模の大きさから、これを防止するための政府や警察の取り組みが数多く行われています。例えば、ユーロポールのEC3、サイバー犯罪対策合同タスクフォース、欧州司法機構、欧州銀行連盟の一連の協調行動は「欧州マネーミュール・アクション」イニシアチブを支援してきた。その第2弾として2016年に実施された活動では、欧州全域で178人の個人が逮捕され、580人の異なるマネーミュールが特定されました。これらの容疑者は、2,300万ユーロの損失をもたらした犯罪行為と関連していました（ユーロポール、2016年）。

  このシステムは取引を行うためや、得た収益を洗浄するためにサイバー犯罪者によって広範囲に利用されているというかなり信頼性の高い証拠が出てきています。この研究で驚くべき発見があったのは、サイバー犯罪グループが現金を物理的に輸送している割合でした。有罪判決を受けたサイバー犯罪者（n=100）とのインタビューのサンプルの少なくとも30%で、サイバー収益を物理的に運ぶか、航空会社の宅配便で送って外国の銀行に預けていたと報告されています。また、上述した欧州マネーミュール・アクションは、マネーミュールの95%がサイバ

ー犯罪活動と直接リンクしていることを発見しています。

ミュールは、彼らが依頼された役割を自覚しているか、無意識のうちに騙されているか、どちらにしても、汚いお金を合法的にすることができる非常に効果的な方法です。ミュールの利用は、多くの場合身分証明書を提示する必要がなく、実際に支店に現れる必要もない、オンライン口座の開設が可能な国外司法権の緩いルールによって非常に簡単になっています。

サイバー犯罪活動の異なる分野間の柔軟性の表れとして、ミュールが収益生成のために利用されることもあります。サイバー犯罪者が使用するミュールを用いた新しい資金洗浄の中で、最も一般的かつ効果的な方法は、いわゆる「転売詐欺」を経由するものです。この詐欺は、犯罪者が（通常は盗まれたカードや個人データを使って）高額の商品を購入することで行われます。そして、個人（意識しているかどうかは別として）が小包を受け取るように勧誘され、それがサイバー犯罪者に転送されます。彼らが小包を受け取ると、その🔪品は闇市場で現金で売られます。研究者が追跡したある事業（Hao et al、 2015年）では、このスキームが運用されていた9ヶ月間だけで約6,000個の小包が出荷されました。これは年間730万ドルの収益をもたらし、18億ドル近くの転売詐欺全体の収益に貢献しました（同上）。

サイバーロンダリング

サイバー犯罪者が従来のロンダリング方法を使用しているという証拠は、The Web of Profitのニーズがいかに簡単に既存の経済に適応できるかを示唆しており、さらに合法的な経済圏とサイバー犯罪経済圏の間の相互依存性が高まっていることを示しています。

しかしながら、これらの方法は現在ではロンダリングのための新しい選択肢の一つに過ぎません。デジタル決済、デジタル通貨、モバイル決済、その他の新しい交換手段への移行は、以下で検討するようなサイバー収益を移動させたり消滅させたりするための新たなツールボックスを提供しています。

PayPalのような決済システムの利用

サイバー犯罪経済の重要で増大する特徴として、電子マネーとデジタル決済システムの開発が挙げられます。これらのシステムは「キャッシュレス」取引を可能にし、相対的に匿名性を保ったまま使用することができ、多くの場合、伝統的な銀行の管理外で使用することができます。

"PayPalやその他のデジタル決済システムは、この調査のためにサンプリングされたケースの少なくとも20%でロンダリングツールとして使用されていた。"

PayPalは、おそらくこれらの中で最もよく知られているもので、特にフィッシングのようなサイバー犯罪のためだけでなく、彼らの手数料収益を洗浄するためにも使われているという十分な証拠があります。

右名ではありますが、PayPalはこのようなツールの犯罪的使用に向けた非常に大きなシフトの一部に過ぎません。今では、例えば、Skrill、Dwoll、Venmo、Xoom、Popmoney、Square Cash、またサイバー犯罪者による（誤）使用の機会を提供するケニアのM-Pesaのようなモバイル決済システムなど、他にも多くのデジタル決済システムや電子キャッシュの形態があります。

"電子決済システムを使ったロンダリング方法は、例えば盗用された銀行口座情報や他の形態のIDなど様々な他の方法と組み合わせて使用される傾向があります。"

銀行を探す必要がなく、携帯電話をバーチャルウォレットとして使うことの魅力は、特に銀行システムが未発達な国では明らかです。M-Pesaは特に成功し急速に成長しており、現在では1,500万人以上の加入者が毎月約10億ドルを送金するために利用しています（GSMA、2017年）。これだけの量のデジタルマネーが流通しており、ほとんどが従来の銀行システムの外にあるため、米国財務省が最近、M-Pesaのようなモバイル決済システムがロンダリングの大きな成長分野の一つになる可能性が高いと警告したことは驚くに値しません。

現在、ケニアだけでも月に最大3,000件のサイバー犯

罪が報告されており、M-Pesaへのハッキング未遂が繰り返されています（Benyawa、 2016年）。今後数年のうちに接続デバイスは500億台に達する可能性が高く、バングラデシュのbKashやラテンアメリカのYellow Pepperなどの新しいモバイル決済システムは、特にサイバー犯罪の拠点として認識されている地域で、非常に人気の高い銀行業務の形態となるでしょう。

デジタル決済システムは、オンライン取引と組み合わせた場合、または他のロンダリング方法やリソースの一部となる場合に、最も効果的に使用されているように見えます。ここで非常に一般的なテクニックは、ロンダリングを容易にすることができる購入を行うためにeBayのようなサイトを使用することです。これらの取引は、その後より少ない疑惑でPayPalシステムを通過することができ、受け取ったお金は簡単に消えてしまいます。

"サイバー犯罪者による収益洗浄のためのデジタル決済システムの利用が拡大していることは権限や管轄外での莫大な収益源を生むことで従来の金融システムの自律性と権威の低下を助長している。"

しかしながら、従来の銀行口座、物理的現金、そして最近ではBitcoinのような暗号通貨も、デジタルリソースのポートフォリオの一部として使用されることが多くなっています。これらは、資金の痕跡を隠し、法執行機関や金融規制当局を混乱させることを助長しています。

"デジタル決済システムでは資金洗浄の限度を逃れるためにマイクロ・ロンダリング技術を利用し、小額の支払いが複数回行われることが多い。"

The Web of Profitプロジェクトのための専門家とサイバー犯罪者のインタビューとオンラインフォーラムによるデータ収集は、違法な活動や取引の少なくとも10%で、PayPalはロンダリング収益における役割の一部を担っていることが示されました。PayPalには年間2,500ユーロの受領制限があるにもかかわらず、関与する金額が時には約250,000ポンドに達することがありました。しかし、サンプルのより大きな数（約35%）は、上記のように詳細が知られてはいないデジタル決済システムを使用していました。実際の数字は、おそらく確かなデータが示唆するものよりもはるかに大きいでしょう。

ケーススタディと事例

ペイパル返金詐欺

最近の詐欺では、サイバー犯罪者がPayPalの会員同士がお金をリクエストできる機能を悪用しました。この機能を使う際に、会員はメッセージを入力できるエリアを含むフォームに入力を行います。サイバー犯罪者はこの機能を利用して、彼らのPayPalアカウントから狙った被害者のアカウントに100ドルを不正に送った結果の返金を要求しました。彼らの主張の信憑性は、PayPalに送信されたインシデントレポートと一緒に、詐欺取引の詳細を記載した文書にリンクしているように見えるgoo.glのURLを含めることで高められました。被害者がこのURLをクリックしたとき、彼ら

は偽装されたJPEGファイルを使用してコンピューターに悪意のあるスクリプトを送り込むウェブサイトに誘導されました。このファイルを開いた人は誰もが、自分のコンピューターがマルウェアに感染していることに気付きました。

ペイパルアカウントの乗っ取り

最近の別の事例では、PayPalがサイバー犯罪者の目的を達成するための非常に一般的かつ簡単な方法、つまりアカウント乗っ取りのためのツールとして利用できることが示されています。最近の犯罪プラットフォーム*InFraud*の撤廃において、1,300以上の侵害されたPayPalアカウントIDが販売のために提供されていたことが判明しています。

PayPalアカウントの販売

PayPalアカウントの販売を提供するダーク・ウェブ・サイトの例は数多くあります。この調査のためにハッキングフォーラムで実施されたスキャンでは、100個のPayPalアカウントが平均で約100ドルあるいは0.4Bitcoinで手に入ることがわかりました。

イスラエルでPayPalが悪用される

イスラエルのハッキングサービスグループ VdOs は、2年間で60万ドル以上の収益を上げてましたが、Coinbase経由のBitcoin決済に切り替える前は、PayPalを使って収益を集め資金洗浄を行っていたことが判明しました。

ペイパルと薬のオンライン販売

資金洗浄のためのPayPalの最も悪名高い最近の使用の一つは、Silk Roadマーケットプレイスの閉鎖の前に存在していた数多くのオンライン薬物市場への関与です。これらの中にはマリファナからケタミンまですべてを販売したTFM（ファーマーズマーケット）がありました。ここではPayPal経由の支払いだけでなく、PayPal経由でロンダリングされたPecunix支払い（I-Goldのようなデジタル通貨）も受け入れていました（Power、 2013年）。

PayPalによるマイクロ・ロンダリング

2013年、Silk Road経由でメタンフェタミンを販売していたJason Hagenは、PayPalを使った大規模なマネーロンダリングにも関与していたことが判明しました。Hagenは60万ドル以上の支払いを受け取りましたが、そのほとんどにBitcoinを使用しており、複数のPayPalアカウントを使って 干回させ銀行口座を不正に開設し、Western Unionの送金で利益を分配していました。

複数のPayPalアカウント、または少額の複数の預金を利用するHagenの方法は、すでに正規の銀行により開発されたテクニックとして、広く使われています。例えば、不適切な管理により、組織化された麻薬ギャングとイランのような不正な国によって銀行を介した数十億ドルの資金洗浄を許してしまったHSBCの巨大ロンダリングスキャンダルにおいて、内部告発者からの証言は、PayPalが現金を洗浄するために銀行の従業員によってどのように利用されたのか示しました。このプロセスは、15セントという小額の複数回の送金から始まり、時には60日という長い期間に渡って行われました。一度確立されると、数万、数十万ドルがこれらの複数のPayPalアカウントを介して洗浄されました。

「マイクロ・ロンダリング」とも呼ばれるこの手法の多くの例が、国連により調査されました（Richet、 2013年）。「これは、PayPalアカウントに紐づいた仮想クレジットカードや詐欺口座のような手段が、大量のお金を何千回もの電子取引による少額で移動することができるということを示しました。」

PayPalと米国の不正選挙

欺瞞的な目的のためにPayPalが悪用されている最も深刻なケースの1つは、2016年の米国大統領選挙に影響を与えるためのロシアの試みに対するRobert Mueller調査として浮上しました。13人のロシア人の起訴に続いて、本物の米国の社会保障番号が盗まれ、ロシア人らがPayPalアカウントを開くためにそれを利用し、Facebookやソーシャルメディアのアカウントを開くためにその偽のIDを提供したことが浮上しています。

PayPalとテロリズム

極端な例はテロリスト資金の洗浄のためのPayPalの悪用です。最近の例では、米国に拠点を置くISISの工作員、Mohamed Elshinawyが関与していました。Elshinawyは忠誠を誓った後、PayPalを通じて組織から約9,000ドルを受け取りました。この資金は、eBayでの偽のコンピュータ・プリンタの販売を使って隠蔽されました。

魅力を失ったPayPal

PayPalは現在、デジタルマネーロンダリングの世界への入り口に過ぎず、洗練されたサイバー犯罪者がデジタル決済システムのはるかに広い範囲を探っていることを示す多くの兆候があります。このプロジェクトでダークサイトを観察して得られた会話データは、サイバー犯罪者の間で、他のデジタル決済システムの方が安全で生産性の高い選択肢であることが明確に認識されていることを示しています。これには次のようなコメントが含まれていました。

– 「私は一月半以内にPayPalを使うのをやめるつもりだ。ccnowはより良い選択肢で、彼らはeBay/PayPalと情報を共有しない。ccnow経由でPayPal決済を受け付けるので、それも素晴らしい。」
– 「金を買ってeBayで売るのは簡単だ。」
– 「騙されないようにしたいならプリペイドが良い選択肢だがVenmoに行って 反対取引をすることもできる。」
– 「私はもうPayPalを使用ない。連邦政府は本気だ。」

勢いを増す匿名取引

資金洗浄のための代替的デジタル決済システムへのシフトの明確な例として、コスタリカに拠点を置くデジタル通貨サービスLiberty Reserveの最近の事例を挙げることができます。匿名の取引を可能にする機能は、世界中で60億ドル以上の資金洗浄を可能にしました。これらの取引の多くは、あからさまに犯罪的なものでした。Liberty Reserveを使って送金する際には、顧客は名前、住所、生年月日を提供するだけで、身元を確認するための他の手

段は一切必要ありませんでした。これにより、架空のIDを使って多数の口座が開設され、時にはRussian Hackersのような名前で開設されることもありました。調査員はまた、「コカインのため」のような目的で口座を開設することもできました。

資金洗浄のための暗号通貨の使用

Bitcoinやその他の暗号通貨の成長は、合法経済と非合法経済の両方に貢献するものとして、広く認識され観察され始めています。現在、総数1,500万以上のBitcoinが流通しており、これまでに1億5,000万件以上のBitcoin取引が記録されています（1日に最大25万件の取引）。Bitcoinは成長を続ける暗号通貨市場の中心にあります。大手Bitcoinウォレット・プロバイダーの1つであるBlockchainは、1,200万以上のウォレットを管理しており、これは2014年から12倍に増加しています（Carlisle、 2017年）。しかし、これだけの取引量があっても、現金での取引がまだ大半を占めており、Bitcoinとその他の暗号通貨はその非常に初期段階の現象に留まっています。

"サイバー犯罪者のBitcoinから Moneroのような知名度が低く 追跡性の低いシステムへの移行の兆候が出てきている。"

現時点では、暗号通貨が本当にマネーロンダリングにとってどれほど重要なものなのかについては、意見が分かれています。英国国家犯罪捜査局はその規模について懐疑的な姿勢を崩していません。そして、ユーロポールは「現金はマネーロンダリングの中核であることに変

わりはない」と同意しています（SOCTA、 2017年）。Bitcoinやその他の暗号通貨がマネーロンダリングの未来を表していると確信している人もいます（Khan、 2016年）。

本調査と他の情報源から、犯罪者の日の目を浴びるBitcoinの勢いが、他の種類の暗号通貨の人気により衰退している可能性があることが明らかになりました。多くのサイバー犯罪者がBitcoinを避け始めた理由の一つは、ブロックチェーンの透明性と、Bitcoinのウォレットを介して資金がどのように送金されたかを検知するツールの増加に関係しています。

"イスラムのハワラ 制度のような直接送金制度は、ピアツーピアの交換形態で、通常の管理外で運用されているため 特別な洗浄機会を提供している。"

これを回避するためにミキサーやタンブラー（ブロックチェーンを不明瞭にするソフトウェア）を使用すると、その効果を相殺することが可能で、Bitcoinの取引の25%がミキサーを利用しているという最近の研究もあります（Robinson & Fanusie、 2017年）。

しかしながら、オランダ当局による最近の決定では、ミキサーを使用している人を誰でも告発することになっており、その使用を隠蔽しようとすると、いくつかの深刻な課題を突きつけられる可能性があります。Bitcoinの価値の変動や、中国や韓国のような管轄区域での潜在的

な取引禁止などの他の要因も、その魅力を低下させています。その影響で、Moneroのような新しい暗号通貨へと注目が移っていると考えられます。Moneroはブロックチェーン上で受信者のアドレスの暗号化を提供するだけでなく、実際の送信者を隠すために偽のアドレスを生成することや取引金額を隠すことができます。

ケーススタディと事例

Bitcoin ATMが簡単なアクセスを提供

Bitcoinがマネーロンダリングに使われる最も一般的で地味な方法がBitcoin専用のATMを利用する方法です。今これは伝統的な犯罪活動のための有用なツールになりつつあります。この調査中に収集され、その後メディアで確認された証拠から、英国ロンドンの街角やその他の目立たない場所に設置されたBitcoin ATMが、麻薬の売人や売春婦によって、現金で得た利益を追跡しにくいデジタル形式に変えるために使用されていることが示唆されました。

このパターンは、世界中で再現されているようです。2017年に米国ユタ州で行われた警察の介入では、麻薬ギャングが利益のかなりの部分を洗浄するためにBitcoinを使用していたことが判明しました。この活動は法執行機関によって壊滅させられ、彼らのBitcoin資産は押収されました。

Silk Roadの有罪判決

オンライン市場、麻薬販売、Bitcoinロンダリングの関連性を示す最大かつ有名な事例として、Silk RoadのRoss Ulbrichtの有罪判決があります。米国警察によると、Ulbrichtからオンライン薬物市場で儲けた莫大な利益をロンダリングするために使われていた2,800万ドル以上のBitcoinを押収したとのことです。皮肉なことに米警察はその後、ロンダリングされた5万Bitcoin（2018年4月には3億ドル以上の価値がありました）をオークションにかけました。

2017年、Ulbrichtの起訴に関与したシークレットサービスのエージェントであるShaun Bridgesは、彼の口座に 千回させた80万ドル以上のBitcoinを洗浄しようとしたことを受けて、自ら6年の刑を言い渡されました。

Bitcoinを使ったアルゼンチン国家の詐欺

2014年の事件には、バルセロナでクレジットカードや公共交通機関のチケットを偽造する装置を使っていたことが発覚し逮捕されたアルゼンチン国籍の男が関与していました。彼はまた、Bitcoinと引き換えにユーロを売るという詐欺も行っていました。購入者はコインを受け取ることはありませんでしたが、犯人はこのスキームにより100万ユーロ以上の資金を調達し、その資金をBitcoinにロンダリングしました。

オランダ人がロンダリングで逮捕される

2016年には、Bitcoinを闇市場で販売することで、麻薬取引の収益から2,000万ユーロの資金洗浄を試みたオランダ人10人が逮捕されました。彼らの活動は、銀行口座に変換されたBitcoinをATMで現金化したことで初めて明らかになりました。

Sheepオンラインドラッグ市場

2015年3月、オンラインドラッグ市場 Sheep を運営していた28歳のチェコ国籍のTomáš Jiříkovskýが4,000万ドルのBitcoinをロンダリングしました。Bitcoin取引所Bitstampに登録されているJiříkovskýの口座から、彼のガールフレンドの口座に送金が行われていました。

WannaCryがBitcoinとMoneroを利用

2017年9月、サイバー犯罪者がBitcoinを隠しやすい他の暗号通貨に変換していることを示唆する傾向が現れました。イタリアのセキュリティ会社Neutrinoは、ランサムウェアWannaCryで集められた合計5 Bitcoinから51.93 Bitcoinまでの収益が、BitcoinからMoneroに変換され始めている様子を追跡することができました。

ロンダリングに利用されるE-GoldとWebMoney

2013年にニューヨークで、E-GoldとWebMoneyの仮想通貨取引所Western Express International, Incの社長がマネーロンダリングの罪を認めました。米シークレットサービスの捜査官は、ハッカーがE-GoldとWebMoneyに交換するために盗んだクレジットカード情報が、Western Expressを使ってドルに換金されているところを突き止めました。WebMoneyが1500万ドル以上、E-Goldが2000万ドル以上換金されていました。

2008年、デジタル通貨E-Goldの管理者が、E-Gold Ltd.の3人の主要な取締役とオーナーと共に、マネーロンダリングと違法な送金ビジネスを行っていた罪で有罪判決を受けました。E-Goldの口座開設に必要なのは、有効なEメールアドレスだけでした。口座所有者は、場所に関係なく、ある口座から別の口座にE-Goldを簡単に送金するだけで、匿名のオンライン取引を行うことができました。この裁判の証拠から、E-Goldはサイバー犯罪者にとって、盗まれた金融情報や児童ポルノを購入するための好ましい方法になっていることが示唆されました。

コロンビアの麻薬密輸業者がBitcoinを使用

他でも、資金洗浄装置としての役割を超えて、Bitcoinが犯罪のイネーブラーとして、より重要な役割に使われているという証拠が出てきています。例えば最近の米国の諜報機関は、コロンビアの麻薬密輸にBitcoinが使用されていることを示唆し、人身売買業者がオンラインでの営業にBitcoinを受け入れている例を確認しています。米上院司法委員会での証言の中で、国土安全保障省の移民・税関執行局のエージェントは、薬物密輸者や知的財産侵害者だけでなく児童密輸者や搾取者が、犯罪取引にBitcoinを利用していると指摘しています。

暗号通貨は、いくつかの理由からロンダリングに適しているように見えます。第一に、暗号通貨はデジタルであるため、サイバー犯罪の収益を取得したり、移転したりすることが容易にできます。第二に、当初は匿名で

の取引を可能にすると考えられていました。しかし、前述したように、Bitcoinやその他の暗号通貨の背後にあるブロックチェーン技術は、すべての取引が透明であることを意味します。このため、ランサムウェアWannaCryやPetyaファミリーの後に、Bitcoinの身代金の支払いが指定されたウォレットに出入りするのを追跡するための、下記のような多数の追跡アプリが設定されました。

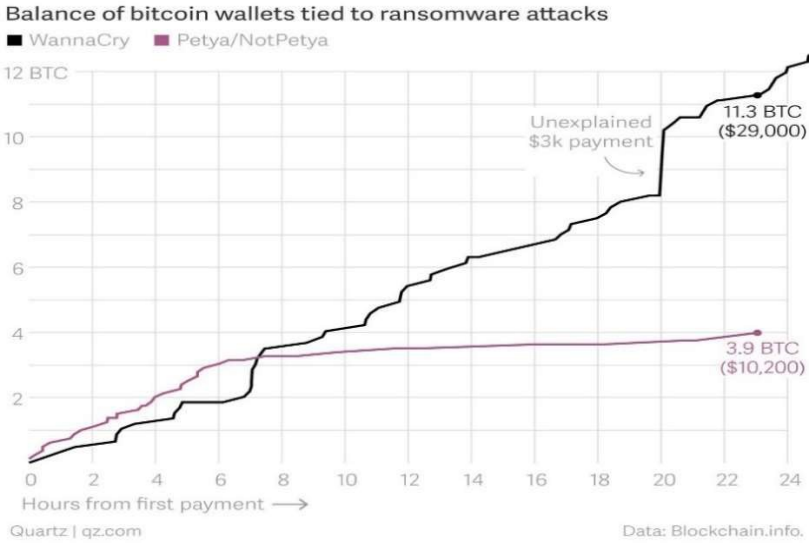


図 2：ランサムウェア攻撃と結びついたBitcoinウォレット

タンブラーやミキサーサービス、例えばCoinJoinやCoinSwapのような（ユーザーがBitcoinの支払いをミックスして識別を困難にすることで）支払元を隠蔽するために使用されているサービスでさえも、必ずしもそれを隠蔽することに成功するとは限りません。先に議論したオランダが作ったような法的規制の可能性はさておき、これらの犯罪への使用には他にも技術的な欠点があります。プリンストン大学の研究者たちは、ウェブのインタラクション中に必然的に流出する情報が、（たとえばウェブトラッカーやクッキーを介して）Bitcoin取引の60％以上で個人とユニークにつながる可能性があることを発見しました（Goldfeder et al、 2017年）。

"暗号通貨を通じた資金洗浄は従来の方法で洗浄された現金の量と比較して、比較的少ないままである。"

MoneroやZcashのような代替暗号通貨は、匿名性をより考慮して設計されており、サイバー犯罪者はBitcoinではなく、これらを使用することにますます興味を持っているようです。例えば、2017年にはランサムウェアのパッケージKirkは、支払いメカニズムとしてMoneroを初めて使用しました（IOCTA、2017年）。しかし、これらにも法執行機関が支払いを追跡する方法が残っていますが、現時点ではまだ秘密裏に行われています。

暗号通貨を通じた資金洗浄は、従来の方法で洗浄された現金の量と比較して比較的少ないままです。例えばユーロポールの推計によると、暗号通貨を介したマネー

ロンダリングは、現在欧州でロンダリングされた総量の4%に過ぎないとされています（Silva、 2018年）。しかし終わりではなく始まりにいることは間違いありません。サイバー犯罪を取り巻く複雑な経済構造が発展しているということは、暗号通貨がThe Web of Profitにおける犯罪能力を低下させるのではなく、むしろ強化する可能性が高いことを意味しています。また、暗号通貨の不正利用が今後も拡大していくことを意味しています。これは、資金の換金や送金を可能にするための暗号通貨の役割についての多くの話が出始めていることからも明らかです。

例えば2016年、オランダの警察は、現金自動支払機から引き出す直前に、銀行に大金を入金した10人を逮捕しました。これはBitcoinの販売からのものだったようです（Guardian、 2016年）。他では、2017年にBitcoinロンダリングに関連した最も注目度の高い逮捕者の1人は、ギリシャのAlexander Vinnickでした（Popper、 2017年）。

Vinnickは、暗号通貨取引所BTC-eを利用してサイバー犯罪者やその他の犯罪行為に関与する個人のために約40億ドルのBitcoinをロンダリングした罪で起訴されています（本人は否認している）。しかし、CocaineCowboys、ISIS、dzkillerhackerなどの偽名を使ったBTC-eの顧客は、新規口座開設時に身分証明書の提出を求められなかったため、容易にオンライン犯罪で採取したBitcoinのロンダリングができました。ランサムウェアの利益の95%がBTC-eで現金化されていると推定されており、サイバー犯罪者のロンダリング活動としては最大級のものとなっています（Fox-Brewster, 2017）。

"ゲームを通じた資金洗浄の規模は拡大していると疑われているが、データは最小限でまだ十分に理解されていない。"

コンピュータゲームの中に隠された通貨を使って、他の現金に簡単に変換でき、国境を越えた送金をほとんど監視されずに可能にするというアイディアは、非常に魅力的なものです。これまでのところ証拠は限られているかあるいは裏付けが乏しいため、実際にどの程度実現されているのかは不明です。これは米国の金融規制機関であるFinCENが、ロンダリングの目的でゲーム内の通貨交換に関与する個人や企業が送金者とみなされ、それに応じて起訴される可能性があることを明確にするガイドラインを発行したことを妨げるものではありません。

"ゲームを介したロンダリングはアプリ内、ゲーム内購入の増加により大幅に拡大している。"

ゲーム内購入の増加により、ロンダリングの可能性がさらに高まり、現在では単純な通貨や金のようなアイテムの不正使用にとどまらないものとなっています。現在のところ、このような購入を行うゲーマーの数はかなり少なく、最近の調査によるとゲーム内収益の半分を占めているのはわずか0.15%のプレイヤーであることが示唆されています(Takahasi、 2014年)。しかし、この独占

性が犯罪的な魅力を高める可能性もあります。

"中国や韓国などの極東諸国はゲーム内通貨ロンダリングのホットスポットだ。"

ゲーム会社の間では、カードの盗難や資金洗浄に関与するサイバー犯罪者が、詐欺を行うウェブサイトを作っている可能性があるというリスクに対する認識が高まっています。Kingdoms of CamelotやStar Wars: Uprisingなどのゲームを開発しているKabam社は先日、同社のゲームHobbitで使用されているゲーム通貨Mithrilがサードパーティのウェブサイトで悪用される可能性があることについて警告を発しました。

> *「Kabamと提携していない第三者の詐欺サイトから、様々なKabamゲームのために安いMithrilを販売していると主張する活動が急増しています。これらのサイトを利用すると、お客様のゲームや支払い情報が危険にさらされる可能性があります。これらのウェブサイトでは、盗まれたクレジットカード情報を使用して、お客様が受け取るであろうMithrilの購入を行っています。これは、あなたの将来的な詐欺行為につながる可能性があります」*（Szabo 2016）。

ケーススタディと事例

韓国のゴールドファーミング

2008年、韓国警察は中国の「ゴールドファーミング」グループ（高額ゲームアイテムの収集）を支援していたマネーロンダリング集団のメンバーを逮捕しました。彼らは、韓国のオンラインゲームで集めた3,800万ドル以上を中国に送金しようとしていました。

MinecraftのようなMMORPGがロンダリングに使われる

2013年に行われたオンラインゲームロンダリングに関する調査（Richet、 2013年）では、ゲーム通貨を用いてマネーロンダリングを行う方法についての情報を提供している様々なサイトが見つかりました。特に共通していたのは、MinecraftのようなMMORPG（多人数参加型オンラインロールプレイングゲーム）の役割で、プレイヤーは異なる管轄区域を越えて交流し、国際的な管理に制限がある状態で通貨を交換することができます。データは、これを行う方法について自由にアドバイスが提供されている多くのフォーラムから収集されました。例えば、あるレポートでは、可能な限り多くのゲーム内資産を購入し、闇市場を作ってそれを売却して現金に交換することを提案しています。また、より確立されたゲーミングゴールド市場を提案するものもありました。そこでは手数料がかかりますが、換金は非常に信頼できるものです。

ダークウェブゲームフォーラムはロンダリングを魅惑

3つのダークウェブゲームフォーラムで行われた観察では、資金を見えなくする選択肢として、Clash of ClansやWorld of Warcraftなどのゲームが挙げられていました。MmoGahのような新しいサイトは、ゲーミングゴールドやゲーム通貨を実際の現金に簡単に換金する方法を提供していますが、規制の関係上、ダーク・ウェブ上の隠密サイトの方が望ましいと指摘されています。

中国にあるこれらのテクニックの一種では、収益を使ってゲーミングクレジットを購入し、それを現金に換金することができました。

第5章：犯罪収益の処分

警察や政府にとって、もちろん研究者にとっても、犯罪者がその利益をどのように使っているのかを見極めることは、サイバー犯罪を理解する上で最も困難な知識の一つです。ここでの重要な問題は、従来の犯罪における収益の処分を見るにしても、サイバー犯罪における収益を見るにしても、どこからデータを入手し、入手したデータをどのように*解釈するかということ*です。また、サイバー犯罪で有罪判決を受けた犯罪者やサイバー犯罪に関与した犯罪者など、そのような情報が得られる数少ない情報源には信頼性の問題があることは明らかです。犯罪者は、様々な理由で信頼できる情報を提供したくない、あるいは提供できないことがあります。

- 自分たちの犯罪に関わっている人たちが、まだ利益を使っている可能性があります。
- 情報を公開すべきだと脅迫を受けた可能性があります。

- 釈放された後に、利益を消費あるいは再度利用したいと考えている可能性があります。
- 一般的な反感 - 彼らは単に嘘をつきたい、法執行機関や他の捜査機関を困らせたいと思っている可能性があります。

その他のデータソース、例えば米国の資産没収プログラムや英国の犯罪収益法（POCA）に基づく没収に関する裁判所の記録は、必ずしも容易にアクセスできるとは限りません。また、資産が押収された場合にサイバー犯罪がどのような関与をしているかが必ずしも明確ではないため、このようなデータは誤解を招く可能性もあります。

ここで定めた世界全体で1.5兆ドルという収益レベルについて、本調査でインタビューした有罪判決を受けた者や現役サイバー犯罪者のサンプルで発見された支出パターンを再現すると、次のようになります：

- サイバー犯罪の収益のうち最大3,000億ドルは、新しいサイバー犯罪や既存のサイバー犯罪、あるいはテロや人身売買のようなより深刻な犯罪のための資金として犯罪活動に再投資されています。
- サイバー犯罪の収益のうち最大4500億ドルが、サイバー犯罪者によって金融資産、地所、その他の資産に投資されています。このことは、合法的な経済に、ますます大きな影響を与えていることを示しています。
- サイバー犯罪の収益のうち、最大で7,500億ドル（全

体の約50%）が、サイバー犯罪者によってステータスを求める、快楽主義的、あるいは世俗的な購買に費やされています。このような支出の多さと、そのカジュアルな特性のため、法執行機関やその他の規制機関には、介入や破壊のための大きな選択肢が与えられています。

ただし、インタビューしたサンプルに基づいて、これらの合計値に外挿する際には多少の注意が必要です。インタビューを受けたサイバー犯罪者が関与した犯罪の種類にサンプルの偏りがある可能性を考えると、他の種類の犯罪に関与しているサイバー犯罪者が全く同じように収益を使うと自動的に仮定することはできません。そのような仮定を明確にするためには、より多くのデータが必要です。しかしながら、予備的な観察だとしても、サイバー犯罪の収益がサイバー犯罪の活動に与える影響について、重要な結論を導き出すことができることは明らかです。このようなデータをより多く取得することで、より精度の高い推論が可能になることが期待されます。

このような限界があるにもかかわらず、研究者は、従来の犯罪者が現金を使う方法のいくつかを解明することができました。例えば、最近の英国内務省の調査（Dubourg & Prichard、 2008年）では、犯罪資産の保管方法を見ることで、そのパターンの一面を把握しようとしました。すべての資産のうち：

- 69%が地所の形
- 11%が銀行口座か建物
- その他金融資産が8%

- 1%は車の形

この発見は、年間の不動産取引の約1～2%が犯罪的利益によって直接資金調達されていという、犯罪が合法的な経済に与える影響についての興味深い推測を示します。例えば、英国では、これを税と歳入データ（HMRCから）にリンクすることによって、これが毎年約15万～30万件の不動産、つまり約30億～74億ポンドの価値がある犯罪者による大規模な投資に等しいことがわかります。

Kruisbergenら（2014年）の研究では、組織化された犯罪者による処分を見るために、より強固な方法論が開発されました。この研究でも、類似したパターンが見られました。研究では、（疑いのある）組織的犯罪者から押収された約 1,196 件の資産のデータセットを使用しました。容疑者は、麻薬取引や生産、人身売買、違法武器取引、詐欺やマネーロンダリングなどの犯罪に様々な形で関与していました。ここでも、不動産や企業への出資などの投資に資金を使おうとする姿勢が見られました。しかし、調査によると、容疑者はその収益を利用して、高価な車やボート、宝石などのアイテムを手に入れたり、休暇やパートナーにお金を使ったりして、現実的で目立った消費に使っていることも指摘されています。

このパターンは、先に議論したロシアのGlobal Laundromat（Harding et al、 2017年）から得られたデータでも再現されています。このスキームの収益処分の分析は、明らかに類似した贅沢品の支出傾向を示しています。例えば、ロンダリングされた大量の資金は、ダイヤモンド、クリスタルのシャンデリア、高価な毛皮などの

アイテムを購入するために使用されました。また、犯罪収益は、犯人の息子のイギリスのサマセットにある名門Millfield Schoolの寄宿費にも使われました。

サイバー犯罪収益の処分

従来の犯罪者の収益支出パターンの分析が困難であることを考えると、サイバー犯罪者がその収益をどのように使うのかについての証拠がさらに乏しいのは当然です。そのためこの種の数少ない研究の一つであるこのプロジェクトは、サイバー犯罪の証拠の広がりの中の限られた情報源から結論を導き出さなければなりませんでした。

最初のデータは、有罪判決を受けたサイバー犯罪者や現役のサイバー犯罪者とのインタビューのサンプル（n=100）と、多数のダーク・ウェブやオープン・ウェブのソースでの観察から得られたものです。その結果は、専門家のインタビュー、学術研究、裁判所や警察の文書、パブリックドメインで入手可能なものとフィルタリングし比較しました。

このようにして導き出された結論は暫定的なものであり、今後の研究者による更なるデータ収集と精緻化を待つものです。しかし、これらの結論は少なくともサイバー犯罪者が収益を処分する方法のいくつかについて、現時点でできる最善の推測の一つを示しています。

割合	何を買ったか
15%	目先のニーズをカバーするためのお金の利用
20%	無秩序な支出または快楽主義的な支出にフォーカス
15%	女友達や他の犯罪者などを感動させるためのステータスアイテムへの支出
30%	お金を不動産などの資産に変換
20%	さらなる犯罪行為への再投資に使われた部分

収集したデータから、サイバー犯罪者が支出を向けている可能性が高いのは、大きく分けて5つの分野であると考えられます。

以下のように分類されます：

- **目先のニーズへの支出**

  主に快適または充分なライフスタイルを維持することに関連した支出。これには、請求書の支払い、車の維持、食品やその他の必要なアイテムの購入などが含まれます。

- **無秩序な支出または快楽主義的な支出**

  衝動的または快楽の充足を求める不必要なアイテムを含む支出。これは、ドラッグ、売春、または贅沢、スポーツカーや宝石類のような高価なアイテムの購入が含まれます。

- **意図的な支出**

  これはある程度の高級品または贅沢な支出を伴う可

能性があるという点で、前のカテゴリーと一致しています。しかしここでは、犯罪者仲間の間であれパートナーや家族の間であれ、ステータスを獲得することが主たる動機になっています。

- **投資支出**

  これには、取得した収益を維持または成長させることを目的とした支出が含まれます。例えば、不動産、金融商品、または芸術品のような価値を保持する他のアイテムなどです。

- **犯罪への再投資**

  犯罪防止という観点から見ると、これは明らかに重要な支出カテゴリーの一つです。なぜなら、法執行機関は、将来のサイバー犯罪活動を破壊したり防止したりするための努力を指示するかもしれないからです。しかし、再投資というのは専門用語なので、この分類に該当する支出は多岐にわたりますし、この用語に含むべきどうかの理由づけも明らかではありません。例えば、盗まれたクレジットカード番号を保存するためにUSBメモリを購入することと、クレジットカード番号を取得する攻撃を行う一連のコンピューター サーバーを購入することが同等のことと言えるでしょうか？

  本研究では、さらなる犯罪の発生に大きく貢献する可能性のある項目への支出を含んだ、広く包括的な意味で再投資という言葉を使っています。したがって、DDoS攻撃の際に集中力を高めるためにコーヒー

を一杯買ってもカウントされません。しかしながら、どんなに小さなものであっても、IT機器への支出はカウントされます。

上記のカテゴリーは相互に排他的なものではないので、表示されているパーセンテージの和は合計を形成しないことに注意してください。言い換えれば、ほとんどの犯罪者はカテゴリー間を行き来することになります。例えば、明らかにすべてのサイバー犯罪者は、基本的ニーズに少なくともある程度の収益を使い、ほとんどの犯罪者は犯罪への取り組みに対して少なくとも何らかの褒賞で自分自身を満足させるでしょう。

"取引は...簡単でありさらに重要なのは、金融規制当局からほとんど見えないところで行うことができるということだ。"

この調査のためにサンプリングしたケースのうち、少なくとも30% (n=35) では、サイバー犯罪者は収益の一部を現金に換えようとしていると報告しています。このような場合、お金が次にどこに行くのか、何に使われるのかを特定することは、通常ほとんど不可能です。従来の犯罪と同様に、物理的なお金はしばしばブラックホールのようなものを作り、そこに収益が消えてしまうことがあります。研究者や法執行機関にとってより重要なのは、キャッシュアウト・ポイント - 洗浄された収益が物理的またはその他の資産に変換される収益フローのノードを特定することです。

キャッシュアウトの壁は、従来の犯罪者にとっての問題と同様に、サイバー犯罪者にとっても依然として大きな問題となっています。お金を動かす方法がどれほど独創的であったとしても、それだけでは最終的な報酬は得られません。サイバー犯罪によって得られた収益はある時点で、最終製品あるいは少なくとも価値のある資産に変換する必要があります。キャッシュアウトの問題は、暗号資産の形で保有されている収益に対して特に強く影響を与えます、なぜなら、現金に変えようとする動きは、金融機関や法執行機関によってすぐに指摘される可能性があるからです。

仮想通貨から現物資産へのキャッシュアウトをよりスムーズに行う方法の一つとして、通貨を*直接*資産に変換する方法があります。この傾向は、現在では様々なツールを使って瞬時に換金できることによって進んでいます。おそらく最も簡単なのは、高級志向の様々な資産や商品を暗号通貨の形で購入することができる様々なウェブサイトです。

例えば、パリのペントハウスや南国の島々など、世界中の高級な土地や不動産を提供している下記のウェブサイト（図3参照）を見てみましょう。サイト上での取引は容易で、さらに重要なことは、金融規制当局から主に見えないところで行うことができることです。

現在、不動産の支払いの約25%が、今後数年以内に暗号通貨の形で行われると予測されています（Machalinksi、 2017年）。この見通しは一部の金融アナリストを懸念させています。彼らは犯罪起源のものが多

い暗号通貨の、より迅速でより隠れた不動産取引が可能になるため、世界の不動産市場が混乱する可能性を恐れています。

図 3： http://bitcoin-realestate.com

しかしながら、暗号通貨の直接の現物資産への変換は、地所に限定されていません。現在では、このような通貨を高価値の商品に直接処分するための、多くのオンラインマーケットプレイスが存在します。例えば、いくつかのサイト（図 4 を参照）では、時計や宝飾品への変換を提供していますし、Bitcoinを使って車を直接購入できるサイトもあります（図 5 を参照）。

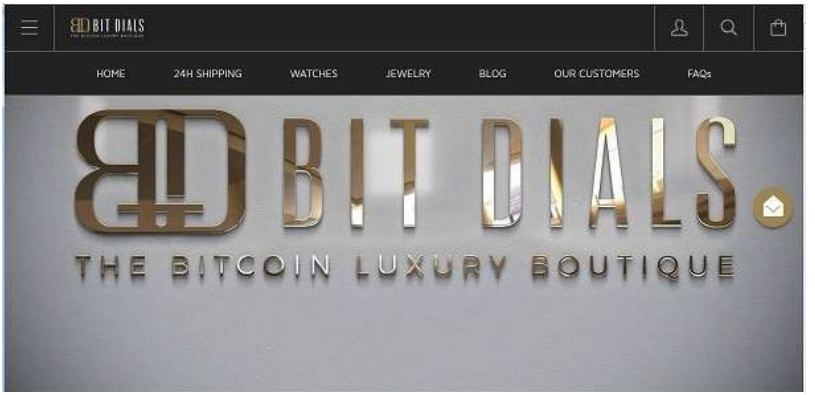


図 4： https://www.bitdials.eu/

図 5：https://www.bitdials.eu/

他には、暗号通貨をベースにしたサイバー犯罪の収益を、金の延べ棒や美術品のような資産に変換するという選択肢もあります（図 6 を参照）。また、Expedia や Dell のような伝統的な事業者から、ホテルの宿泊施設やコンピューターなどの商品を購入する機会も増えています。

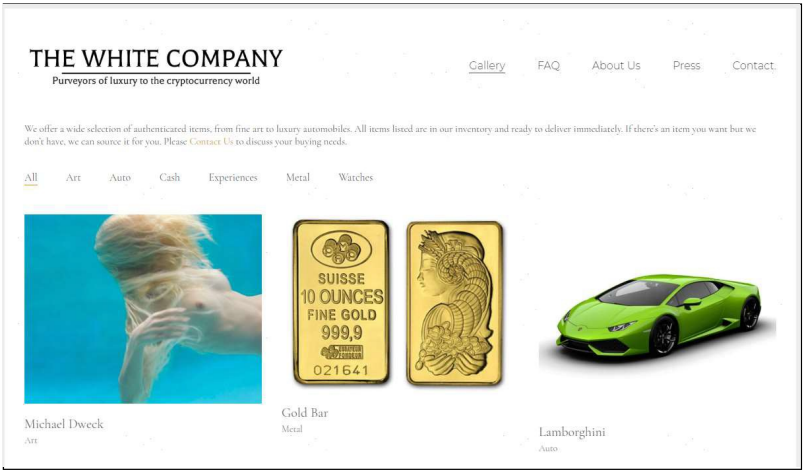


図 6：http://thewcomp.com

サイバー犯罪の収益を高級品に費やすというパターンは、犯罪者個人の消費レベルにデータを掘り下げてみても同様です。一方で、もちろん収益がここで論じたような方法で処分されるということを断定するのは困難ですが、容疑者へのインタビューデータからパブリックドメインでの事例報告まで、できるだけ多くの情報源を横断して三角測量を行うことで、予備的な洞察を構築することが可能になります。

もう一つのすぐにアクセス可能で合理的に信頼でき

る情報源は、サイバー犯罪者が盗んだクレジットカードデータを使用したことで影響を受けた支出パターンに関するものです。不正検知の会社Forterによるこの分野の非常に大規模な最近の調査では、盗難されたクレジットカードを使用した300万件以上の取引を調査しました（Anand、 2015年）。これによると、Rolexの時計や高級ホテルでの休暇などの高級品や、MacBook Airのようなハイステータスな電子機器品を好む傾向が明確に示されていました。このパターンは、米国の全米小売調査（Fahmy、2010年）で得られたデータや、本調査で得られたサンプルデータでも同様で、インターネットや路面店で転売可能な人気ブランドの「爆買い」の準備ができていることがわかりました。

同時に、盗まれたカードデータを使って、ピザのようなありふれた食品を購入しようとしている人もいました。これは、本プロジェクトの現地調査でも裏付けられています。インタビューに応じたサイバー犯罪者の多くは、より個人的で自発的なレベルで活動しており、長期的な投資を慎重に検討するよりも、目先の欲求やニーズを満たすことを目的とした衝動的な購入パターンを示す傾向がありました。贅沢なテイクアウト食品に加えて、犯罪者が感動させたい人のための売春婦、コカインや派手な贈り物に支出している証拠もありました。

Forter調査、2015年	全米小売業協会、2010年	本調査サンプル
高級な商品		
Rolex時計	Braunの歯ブラシ	スポーツカー
ルイヴィトンのハンドバッグ	Claritin	高級なスパでの週末
ダイヤモンドの婚約指輪	CoverGirlの化粧品	香水
電子・デジタル機器		
MacBook Air	X-Box	タブレット端末
スマートウォッチ	Duracellの電池	スマートフォン
デバイスケース	iPod	メモリーカード
Best Buyのギフトカード	ギフトカード	ゲーム通貨
iTunesクーポン		
食と遊び		
ピザ	KitchenAidのミキサー	売春婦
Red Bull	Enfamilのベビーミルク	コカインなどの薬物
高級ホテルの予約	ランジェリー	贈り物

表8：犯罪者の衝動買い

ケーススタディと事例

悪い奴らは戦略的

インタビューデータによると、収益が主に使われている方法と、犯罪に関わるプロフェッショナリズムのレベルとの間には強い相関関係があることが示唆されました。不必要なリスクが取られたり、オペレーションが散発的であったり、「一回限り」であったりする場合、支出は当面の必要性や純粋な快楽主義のために使われる傾向がありました。例えば、働いていた中小企業で顧客カードの詳細を盗むという一回限りのインサイダー詐欺に従事したある個人は、一連の借金を返済するためだけにそれを行っていたと述べています。

対照的に、オークション詐欺に従事するより組織的なグループは、例えば高価なワインや骨董品などの、価値があり警察の目を引きそうにない投資の形で収益を偽装する方法について話し合っていました。

快楽主義は健在

快楽主義的な大きな支出パターンの一例を、フェンタニルを販売するオンラインの薬物スーパーマーケットを運営していたとして2017年に有罪判決を受けたイギリスのヨーク出身の2人の習慣に見ることができます。このスキームを首謀した個人は、27万5,000ポンドから150万ポンドの間に相当するBitcoinの支払いを受け取っていましたが、警察は彼が金を多少購入していた以外は、収入の大部分をドラッグ、高価な時計、週に約2,000ポンドの売春婦に費やしていたことを発見しました。

贅沢な生活を送る

同様のより直接的なパターンは、Zeusボットネットの亜種を使用して、約127の米国の銀行から資金を盗んだ個人のケースにも見られます。警察に利益の使い道を尋ねられたとき、彼は主に例えば5つ星ホテルに泊まるような旅行と贅沢な生活に費やしたと答えました。

ラスベガスで派手に生きる

ウェールズのオンライン薬物ディーラーは、ウェブサイトで250万ポンド（350万ドル）以上を稼ぎ、その収益を贅沢なライフスタイルの資金に充てていました。警察は、彼が得た利益を1回6,000ドル以上でポルシェやランボルギーニをレンタルし、カジノで4万ドル以上のギャンブルをするラスベガスへの5週間の休暇など、贅沢な体験に費やしていたことを発見しました（Wales Online、2015年）。

スーツケースの現金を持つアフリカのサイバー犯罪者

2017年銀行詐欺に手を染め、モバイル決済システムM-Pesaにハッキングを試みたアフリカのサイバー犯罪者が、非常に贅沢なライフスタイルを送っていることが発覚しました。ドル紙幣でいっぱいのスーツケースに囲まれているだけでなく、デザイナーズスーツを着てポーズを取り、高価な時計を身に着けている姿も撮影されています。

チェコの犯罪者が投資に注力

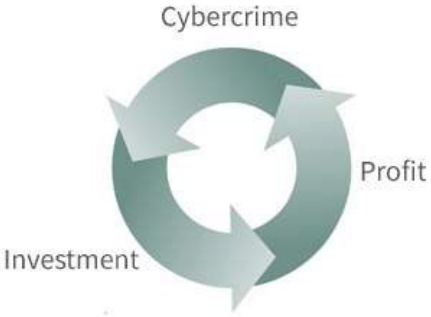
より直接的な投資指向の支出の例を、前述のチェコのサイバー犯罪者Tomas Jiříkovskýの支出習慣に見ることができます。彼は、オンライン薬物マーケットSheepからの利益を地所に大きく投資していました。

収益向上に使われたギフトカード

この調査で見られたもう一つのパターンは、利益が犯罪に投資されというものでした。以前に報告されていないフロリダ州の米国連邦政府の例では、盗まれたクレジットカードのデータから得た利益が、Walmartや他の小売業者の45,000枚のギフトカードを購入するために使用されました。これらはその後、ギフトカード交換サイトRaise.comでの販売を通じて、さらなる収益を得るために使用されました。それぞれ2ドルから2,000ドルのギフトカードがRaise.comから合計900万ドルの新たな収益を生み出しました。

犯罪への再投資

現在のところ私たちの知識との間に大きな隔たりがあるのは、サイバー犯罪からの収益がどの程度さらなる犯罪活動に再投資されているのかという点です。もし、発生している収益が、本レポートで確認されている規模に近いものであれば、犯罪を大幅に強化する可能性があるため、立法者は警戒を始めています。（SOCTA、2017年）。これらの予備的な兆候が正しいとすれば、サイバー犯罪が現在どのように犯罪を誘発しているのか、つまりサイバー犯罪がどこまで（サイバーの世界であれ、それ以外の世界であれ）さらなる犯罪を支援し、資金を提供し、あるいは可能にしているのかを理解するためのさらなる研究は、明らかに緊急の優先事項であると言えるでしょう。



様々な犯罪への投資の中で、最も明白にサイバー犯罪への再投資がされています。効果的に研究が行われれば、収益を特定の犯罪に結びつけるサイバー犯罪のループを検知することができます。このループがサイバー犯

罪経済を推進する様々なエンジンを提供しているので、法の執行者や政策立案者にとって大きな意義があることは明らかです。

このようなサイクルが、既に整ってはいないとしても、はっきりと始まっているという証拠があります。例えば、これまでに発見された大規模なサイバー犯罪組織の多くは、通常収益の少なくとも一部を、さらなるクライムウェアの購入、ウェブサイトの維持、ミュールへの支払い、その他の犯罪要件など、組織の拡大と発展に充てているように見えます。サイバー犯罪の魅力の一つは、スタートアップ・コストの低さであるとされていることを考えると、より洗練されたインフラにより犯罪の範囲を維持したり拡大したりするために、大規模な投資を必要としないことは明らかです。

上述のForterの研究（表8参照）では、盗まれたクレジットカードのデータは、単なる無秩序あるいは快楽主義的な支出には使用されていないという証拠がありました。この調査で収益はホスティングサービス、リモートホスティング、ロゴやウェブサイトのデザインなど、ビジネス関連の活動への投資にも使われていました。検索エンジン最適化やFacebook広告のクーポンなどのプロモーションにも支出が記録されていました。

同様に（それ以上ではないにせよ）深刻なのは、サイバー犯罪の収益が他の種類の犯罪を支援することに向けられていることです。証拠はまだ限られていますが、このようなことが起きていることを示唆する十分な指標があるように思えます。薬物生産と薬物密売は、この傾

向の明白で直接的な例をいくつか示しています。ユーロポールによる最近の調査（2017年）では、EU内の組織犯罪グループの約35%が違法薬物の生産や密売に直接関与しており、薬物市場がすでに組織犯罪とどれだけ絡み合っているかが示されています。

"サイバー犯罪で収益を得ているグループが積極的に麻薬を生産しているという証拠さえある。"

薬物は、EUで最も収益性の高い犯罪市場で、最低でも年間約240億ユーロの収益を上げています。我々はダーク・ウェブの活動の最大57%が今では薬物の取引に関連付けられていることを知っているので、取引の継続に必要なのが新しい在庫の購入だけであれば、オンライン薬物市場からの莫大な利益の少なくとも一部が事業に再投資されることは十分に明白であると思われます。この種のサイバー犯罪ツールは、2005年以降620種類以上の新しい合成麻薬によって、新しい向精神薬の蔓延を大幅に進めています（Europol、 2017年）。この種の物質の多くは、中国やインドで製造され、オンライン市場で購入された後、大量にヨーロッパに出荷されています。

サイバー犯罪で収益を得たグループが薬物の積極的な生産に関与しているという証拠さえあります。例えば、先に取り上げたオランダのマネーロンダリングギャングの逮捕（Guardian、2016年）でも、彼らがエクスタシーを作るために所持していた成分が発見されており、サイバー犯罪活動と組織犯罪活動との間には具体的なつなが

りがあることが浮き彫りになっています。

サイバー犯罪から他の犯罪活動への収益の流れの存在を立証するのは難しいですが、このようなことが起きていると考えるには十分な理由があります。例えば、売春（特に新しいオンライン形態の売春）からの収益と人身売買の問題との間には、巧妙な関係があることがわかっています。ポン引きはクライアントとワーカーから収益を集めるためのツールとしてインターネットを利用し、経済的に弱い人々がいるターゲット地域から人身売買被害者（とコスト）の管理にも利用しています。

米国への人身売買の資金源にBitcoinが使われていることは、先に見たように、米国司法省がすでに認識していることです。このプロジェクトのために米国で収集されたデータはこれを裏付けるもので、メキシコやカリブ海諸国から米国南部への人身売買ルートは、その原因となっているギャングのオンライン活動、例えばギャンブルから資金を得ていることが多いことを示唆しています。

オンライン市場で入手可能なアイテムを簡単に精査するだけでも、サイバー犯罪活動が他の種類の犯罪活動といかに密接に関連しているかがわかります。例えば、このような最大規模の市場の1つであるAlphaBayの撤去では、25万件以上の違法薬物のリストに加えて、有害化学物質、銃器、偽造品、マルウェア、そして10万件以上の盗難・不正な身分証明書やアクセスデバイスのリストがあることが明らかになりました（Europol、 2017年）。

"イスラムのテロリズムは、すでにハワラ送金メカニズムという形で、独自の既㆓資金調達・洗浄サービスを利用している。"

おそらく、サイバー犯罪の収益をさらなる犯罪に再投資するという最も深刻な事例の一つは、情報技術の悪用とテロリズムの促進との間にますます強い関係があることにあるのではないでしょうか。イスラムのテロリズムは、すでにハワラ送金メカニズムという形で、独自の既㆓資金調達・洗浄サービスを利用しています。

この非公式な金融ネットワークは技術的なインフラを必要とせず、ナイジェリア北部、イエメン、アフリカの角など、既知のテロリストの活動拠点で使用されていることが分かっています。しかし、テロリストは、よりデジタルに焦点を当てたロンダリング手法を利用することにも同様に長けています。例えば、2016年には、ガザ地区に位置するオンラインのジハード主義メディアユニット Ibn Taymiyyah Media Center が、Bitcoinで寄付を募ることで、ソーシャルメディアを使った資金調達を試みました。また、インドネシアのISIS㆑下の過激派が Bitcoin や PayPal を使ってシリアの個人と取引を行っているという証拠も出てきています（Maxey、 2017年）。また、Bitcoin は、ISIS が発見を逃れるために人員や資源をシリアに移動させるための資金源として利用していたことも判明しています（Irwin and Milad、 2016年）。

"テロのための収益を得るためにサイバー犯罪が行われたケースさえもあった。"

現金洗浄のためのサイバー犯罪インフラもまた、テロリストの活動をより直接的に支援しています。例えば、悪名高い過激派のソーシャルメディア・サイトであるal-Fallujahフォーラムの投稿者は、サイバー犯罪活動からの安定した資金調達の流れがあることを示唆し、電子決済サービスを監視している可能性のある当局から逃れる方法についてアドバイスを提供しています（Jacobsen、2009年）。

テロリストのプロパガンダのためのソーシャルメディアの悪用もまた、財政的支援を得るための有用な方法であることが証明されています。最盛期には、ISISは1日に約4万件のツイートを発信しており、テロリストグループと関連があるとされる1,000件以上のアカウントが、現在Twitterよって停止されています（Telegraph、 2014年）。

テロリズムのための収益を得るためにサイバー犯罪が行われたケースさえもありました。この種のデータの多くは必然的に秘密裏に行われており、一般の人が調べることはできませんが、少なくともいくつかの事例がわかっています。例えば、イギリス生まれのアルカイダ信者であるYounis Tsouli（オンラインでの別名”Irhabi007”で知られる）は、動画のアップロードに関してテログループに技術的な支援を提供しました。Tsouliはすぐに、自分の技術がサイバー犯罪にも利用でき、それがテロ組

織の新たな資金源となることに気付きました。

Tsouli は共犯者の Tariq al-Daour とともに、Cardplanet などのオンラインフォーラムでの取引を通じて、盗まれたクレジットカード番号を取得し始めました。Tsouli は逮捕されるまでに、37,000以上の個別のカードデータファイルを集めることに成功し、350万ドル以上の収益を得るために使用しました（Jacobsen、 2009年）。Tsouli はまた、The Web of Profit が提供するリソースを十分に利用して、absoluteepoker.com や paradisepoker.com などのギャンブルサイトを通じて資金洗浄を行いました。

第6章 ：結果と提言

サイバー犯罪が生み出す収益と、その収益がどのように移動し処分されるかというレンズを通して、サイバー犯罪問題を再検討すると、サイバー犯罪の規模と複雑さが明らかになりました。

特に、重要なポイントは以下の通りです。

- サイバー犯罪はビジネスのようなものだという古いアイディアは、その内部の複雑さをよりよく捉えた新しい比喩、すなわちサイバー犯罪は独自の経済を持っているに置き換える必要があります。 “Web of Profit（利益の網）”は文字通り正当な経済の鏡像となっているだけではなく、正当な経済を食い物にし、かつそれを包含しています。
- 長期的な解決策としては、サイバー犯罪の*システミック*な側面、特にサイバー犯罪を支えている経済の側面に対する感度を高める必要があります。サイバー犯罪は、複数のアクターや相互依存関係からなる動的に進化する分野なので、より全体的にアプローチする必要があり、その中には特定の侵害やセキュリティ事故と直ちに関連性があるとは限らないもの

もあります。

- 現在では、経済的な理由がサイバー犯罪の主要な動機の一つとなっています。システムに対するサイバー攻撃を、被害やデータ取得ではなく、経済的利益の観点から再定義することで、新しい種類の解決策を生み出すことができるかもしれません。例えば、闇市場でどのようなデータに価値があるとされているのか、どこにリソースを向けるべきなのかについての理解を促すことができるかもしれません。
- サイバー犯罪は現在、比較的簡単で低いスタートアップ・コストで収益を得る方法を提供しています。また、その収益は武装強盗のような従来の犯罪から得られる収益をはるかに上回ることがよくあります。多くの場合、その収益は合法的なビジネスから得られる収益よりも大きくなります。
- 特定の種類のサイバー犯罪とその犯行方法に焦点を当てることは、ある点までであれば有効でしょう。サイバー犯罪経済のダイナミックで相互に関連した全体的な概観がなければ、問題の理解は部分的または不完全なものになる可能性が高いでしょう。
- 次に、サイバー経済と合法的経済の間の密接な相互関係が考慮されない限り、伝統的な犯罪あるいはサイバー犯罪のモデルに固執してしまうことで、より効果的な対応を創造する方法が妨げられてしまう危険性があります。
- これらすべてに不可欠なのは、合法であるか違法であるかに関わらず、プラットフォームがどのように

してサイバー犯罪者の行動を可能にし、支援しているのかをよりよく理解する必要があるということです。この調査で明らかになった最も顕著なプラットフォーム犯罪へのシフトの例として、不正または違法なオンライン市場の爆発的な拡大が挙げられます。これらの市場は現在、サイバー犯罪者に開かれた最大の収益生成源を構成しています。サイバーセキュリティの専門家は、これらの活動に広く潜入し、弱体化させ、ブロックするためのツールを見つけるために、はるかに積極的である必要があるでしょう。

- 営業秘密の盗難は、現在ではサイバー犯罪の中でも重要な収益源となっています。これは内部と外部の双方で発生する問題ですが、現在ではインサイダーの脅威や悪意のアクターといった従来の概念を超えるものになっています。この問題を管理するためには、従業員の疎外感を増大させそれによって問題を悪化させるだけの単純な監査や監視ではなく、より繊細なポリシーやソフトウェア・ソリューションが必要になるでしょう。
- サイバー犯罪の収益が指数関数的に増加していることで、さらなる犯罪を支援しサポートするための資源が蓄積されています。これらの中には、サイバー犯罪そのものを超えて、人身売買やテロなどのより深刻な犯罪に拡大しているものもあります。犯罪に再投資されようとしているサイバー犯罪の収益を食い止めるための技術的なアプローチや取り締まりのアプローチを見つけることが不可欠です。

- 国家や企業その他の合法的なアクターが、現在サイバー犯罪経済の中で、収益の生成、ロンダリング、収益の処置に重要な役割を果たしているという現実は、適切に認識されなければなりません。The Web of Profitでは、安全な避難場所はほとんどありません。これは警察やサイバーセキュリティの専門家がほとんどコントロールできない問題のように見えるかもしれませんが、信頼を測定するためのより良いツールや積極的に脅威を破壊し対処するための準備を整えることは、この問題をより良く管理するための選択肢の一つです。

サイバー犯罪問題に取り組む上でフロントエンドの役割を担う人々 - 最も明らかなのはサイバーセキュリティや法執行の分野の人々 - にとっては、この研究が提起した概念的な問題に追加して、より喫緊で実践的な意味合いがあります。その中でも特に顕著なものは以下になります。

法執行機関への提言

警察は、サイバー犯罪を犯罪取締りや犯罪防止の観点のみで扱うマインドセットから脱却し、サイバー犯罪経済の急速な変化に対応できる機動的なアプローチへと移行する必要があります。警察の情報収集や警察の介入は、サイバー犯罪の経済構造とそれが加害者の動機や方法にどのように寄与しているかに、より直接的に焦点を当てる必要があります。例えば、容疑者や有罪判決を受けたサイバー犯罪者がどのようにして収益を得ていたの

か、またその収益を使って何をしたのかをより明確に報告することは、有用な警察や裁判所の記録になります。

従来の犯罪取締りのための市場削減アプローチは、サイバー犯罪が依存しているハイパーコネクテッドな市場に合わせて調整し、経済的利益を破壊したり減少させたりするための新たな方法を開発する必要があります。特に、データに基づいているかどうかに関わらず、サイバー犯罪経済を通じた収益の*流れ*を中心に、より多くの情報収集を行う必要があります。この鍵となるのは、主要な収益ポイントを特定するためのより洗練された分析ツールの獲得と、エージェントベースのモデリングのような新しい技術の使用で、これによって収益生成のリアルタイムシミュレーションとこれを破壊することが可能になります。

予測ソフトウェアと自動化されたインテリジェンスの使用はこの目標に貢献する可能性が高いでしょう。このようなツールは、犯罪者が従来のキャッシュアウトプロセスをデジタル使用により行う新たな方法、つまり洗浄された収益を使用したり、使用可能な形の価値に変換したりすることをターゲットにすることにも役立つかもしれません。

取り締まりの技術を超えて、サイバーに特化した取り締まりと金融のスキルを備えた専門家チームが多数必要とされています。このようなチームは、暗号通貨、デジタル決済システム、およびサイバー犯罪経済のその他の要素の犯罪利用に関する専門知識を迅速に身に着ける必要があります。また、マルウェアやその他の亜種の発

生源を特定するために、マルウェアを解析し、キルチェーン分析を行うためのツールも必要となるでしょう。

また、警察機関は、プラットフォーム・プロバイダーとより緊密に連携して、その悪用をターゲットにし、プラットフォームが可能にしている犯罪機会を減らすための支援を行う必要があります。

サイバーセキュリティ専門家への提言

サイバーセキュリティ業界は、サイバー犯罪に対する単純な銃撃戦や対応策を超えて、サイバー犯罪経済全体にどのように対応していくかということに明確に焦点を当てていく必要があるでしょう。

サイバーセキュリティの専門家の間で、金融機関や警察とより密接に連携して、戦略的なノードと介入が最も利益をもたらすことができるThe Web of Profitの弱点を特定する必要があることを認識する必要があります。

その一環として、データとデータ保護はプライバシーをはるかに超えるものであることを認識しなければなりません。合法経済とサイバー犯罪経済の両方で富を生み出すための重要な原材料の一つとして、データは従来の通貨と同じように扱われ、交換の制限やマネーサプライの適切な規制など、より具体的な安全策で保護される必要があります。

サイバー犯罪者がどのようにデジタル技術を使って収益を隠し、資金洗浄しているかを明らかにするためには、新しい種類のソフトウェア・ツールが必要とされています。その一例として、インターネットから隔離され

た安全な場所を作ることができる仮想化ツールがあり、不正な収益を生み出す活動を 干回して無力化することができます。もう一つの例として、ネット上の価値のあるアイテム、特に個人データを正確に追跡し特定することができる、より洗練されたスキャンツールがあります。

しかし、最終的には、サイバー犯罪のサプライチェーンを破壊するために、業界は*予防*とデータ保護の確保にもっと力を入れるべきです。

学会や研究者への提言

サイバー犯罪研究者は、本調査で特定されたサイバー犯罪の収益生成の3つの主要な段階について、より良いデータを至急収集する必要があります。また、本報告書で提供されているベースラインの収益推定値を洗練させ理解を深めることで、サイバー犯罪の収益をより包括的に把握することも必要です。

ここでのデータを強化する重要な方法は、収益を生み出すサイバー犯罪のカテゴリーの範囲を広げることや各カテゴリーに変数を取り入れることです。例えば、医療記録など、より多くの種類のデータがやり取りされている分野の収益推定値を取得することで、データを強化することができます。

収益データの強化は経済的動機がより顕著に因果関係を説明するような、サイバー犯罪に関する新しい理論モデルの開発に結びつける必要があるでしょう。

Apendix：方法論

本レポートの調査は、以下の3つの要因を追跡しモデル化することを目的としています。

1. サイバー犯罪の収益の典型的な起源、量、種類。
2. これらの収益の経路と法の執行から隠す方法。
3. 収益の目的と利用。

調査は、2つの主要な測定ツールを組み合わせた混合アプローチを利用して実施されました。

- 有罪判決を受けた、または現在活動中のサイバー犯罪者のサンプル（n=100）から得られたインタビューおよび観察データ。ここで収集されたデータは、以下のように分解されます。
  - 2017年6月 ~ 2017年11月の間に実施された既決サイバー犯罪者へのインタビュー（n=25）。
  - 2017年10月 ~ 2018年1月の間に、現在サイバー犯罪関連の活動に関与している個人へのオンラインインタビュー（n=25）。

- 2017年8月 ~ 2017年12月の間に収集された、クリア/オープン・ウェブまたはダーク・ウェブのフォーラムの会話ログデータと観測（n=50）。

- 警察、金融、サイバーセキュリティ、学術の各分野から集められた50人以上の専門家とのインタビューとコンサルテーション。回答者は、直接または個人的な接触と機縁法（snowball sampling）を組み合わせて選ばれました。
- インタビュー資料と観察は、半構造化されたアプローチを利用し、5つの主要な調査ラインを中心とした質問と観察基準を利用しました。
  - *サイバー犯罪の種類* - 前述のいずれかの分野に従事している個人に特に注意を払いました。
  - *典型的な収益* - 犯罪から得られる収益（ある場合）。
  - *方法* - どのように収益を獲得したか。
  - *移動* - 収益はロンダリングされたか、された場合はどのようにロンダリングされたか。
  - *処分* – 収益はどのように使われたか。

これらの一次データソースは、査読付き学術研究、インテリジェンス報告書、セキュリティおよび金融データベース、メディアの報告書、およびダーク・ウェブの資料やフォーラムやチャットルームなどの他の指標となるソースを含む広範な二次資料によって補完されています。

収益計算上の注意事項

サイバー犯罪の収益やコストを見積もろうとする試みは、ほとんどの場合、大きなデータのギャップに直面するか、あるいはより正確で精度の高い見積もりに取って代わられることになります。これは、このような試みに対する健全な懐疑心を抱く理由になりますが、推定値を導き出すことが完全に不可能であるということではありません。また、見積もりが無意味であるということでもありません。サイバー犯罪のあらゆる側面に関わってしまうことの欠点や欠陥は、この分野を研究している人なら誰もが知っていることですが、現時点で可能なベンチマークを設定することは確かに有用です。欠点を最小限に抑えることができれば、そのようなベンチマークは、この分野での思考を発展させ、洗練させようとする将来の研究者に有用な出発点を提供することができます。少なくとも、対話を始めるという利点があります。

このような精神に基づき、サイバー犯罪経済の現状を説明する収益を推定しようという本研究の試みが開始されました。慎重にならざるを得ず、収益カテゴリーの数を多くではなく少なめにしたり、見積もり範囲のポイントを高くするのではなく低くしたりすることで、サイバー犯罪は儲かる犯罪であるという仮定が、サイバー犯罪経済の中で実際に起きていることに基づいているかどうかを理解することを目的としました。最終的に導き出された驚くほど高いその数字は、この犯罪の人を引き付ける力とそれにどう取り組むかについて、もっと真剣に

考える必要があることを示唆しています。サイバー犯罪からの総収益の数字は、ある程度までの正確さでしかありませんが、それが意図的に保守的なものであるという事実は、その不正確さが少なくとも過大評価ではなく過小評価でしかないことを意味しています。

サイバー犯罪から得られる世界の年間収益を保守的に見積もった結果、約1.5兆ドルという数字が導き出されました。この数字は、収益を生み出すサイバー犯罪の5つの主要なカテゴリーから得られる収益を合計して導き出されたものです。

犯罪	年間収益*
不正、違法なオンライン市場	8,600億ドル
営業秘密、知的財産の盗難	5,000億ドル
データ取引**	1,600億ドル
クライムウェア/CaaS (サービスとしてのサイバー犯罪)	16億ドル
ランサムウェア***	10億ドル

表 9：サイバー犯罪の年間売上高の推定値

違法オンライン市場の収益 – 8,600億ドル

これは、証拠がはっきりしている3つのタイプの不正なオンライン市場からの収益を合計して導き出されたものです。

- *違法なオンライン薬物販売* - ~年間1億8,000万ドル（cf. Kruithof et al、 2016年）。おそらく、Silk Road か

ら2年間で10億ドルの利益を上げたことが知られていることを考えると、非常に低い推定値。この理由から、上限の推定値が採用されました。

- *違法な医薬品の売上高* - ~ 年間4,310億ドル（Scott、2016年）。この調査により、違法なオンライン薬局では、偽造、規格外の配合、汚染、ごまかし、有効成分の置換がある商品を定常的に販売していたことがわかりました。
- *オンラインで販売されている偽造品* - ~ 年間4,600億ドル。偽造品の世界貿易額は、以下の通りと推定されています。17.9兆ドル（OECD、2016年）このうち最大4,600億ドルがオンラインで取引されています（Klara、2017年）。

合計 = 1.071兆ドル+

偽造品や医薬品の収入源は、いずれもオンラインで販売されているものがほとんどであることが示唆されていますが、正確な数量は不明です。

見積もりのために、上記の合計の20%はオンラインで販売されていない商品が含まれているか、またはそのようなオペレーションを立ち上げるためのコストで失われていると想定されています。オンラインマーケットプレイスを構築する場合、コストは最小限に抑えられますが、ここでのすべての見積もりと同様に、範囲の下限を使うことを決定しました。オフライン販売やコストで失

われた20%を考えると、オンライン販売では**8,600億ドル**という数字が導き出されました。

営業秘密、知的財産の盗難-5,000億ドル

この数字は2つのソースから導き出されたものです。

- *営業秘密や企業のIPの盗難* - ~年間2,000億ドル程度。最近の推定では、世界経済に対する経済スパイ活動のコストは年間4,450億ドル以上 - または世界の所得のほぼ1%に相当します（Center for Strategic and International Studies、 2014年）。ここでの加害者の性質（多くの場合、国家や他の大きなアクター）は、そのような利益/収益を決定することが困難であることを意味します。しかし、資産の価値は、それを取得するためのコストと移動での損失の結果として50%で減少すると仮定しても、利益はまだ約2,000億ドル残っています。
- *海賊版音楽 / 映画* - ~年間 3,000 億ドル（IPC、2013年）。この数字は米国のものですが、世界的にはもっと高い数字になる可能性があります。

合計 = 5,000億ドル

データ取引 - 1,600億ドル

これは、不完全なデータソース、異なるデータソース間の多くの価格の不整合性、価格の変動性を考えると、最も困難な計算の一つでした。ここでは、あらゆる種類

の収益を評価しようとすると、どんなにもっともらしい方法でも不可能なので、相殺し収益の最小の見積もりをすることに到達しました - 4つの活動が選択されました。

1. 盗難カードデータの損失（カードの使用価値）。
2. 盗まれたカードの取引。
3. 銀行や決済システムのデータでの取引。
4. ウェブサイト等へのログインデータの売買。

2016年には最大40億件のデータ記録が盗まれたことがわかっています（RBS、 2016年）が、この数字は2017年までほぼ20億から40億の間で推移しています。しかし、ここでのデータの回転率、つまり、盗まれた記録のうち、実際にオンライン市場に出回っている記録の数はわかりません。しかし、2012年から盗まれた10億件以上のヤフーの記録の場合、そのほとんどが最終的に何らかの形で販売されたようです。この典型的なデータ侵害に基づいて、盗まれたデータ件数の大部分が最終的に販売されるというのは、合理的な仮定であるように思われます。しかし、不正な取引に利用できる盗まれた件数の75%程度という、より控えめな回転率を想定すると、年間約30億件の盗まれたデータ・レコードが取引されているというベースラインの数字を推測することができます。

この30億という数字を、調査した20以上のサイトで販売されていたデータと相関させると、異なる種類のデータ販売の以下のような内訳が浮かび上がってきます。

- *盗まれたカードデータ*-発見されたものの約50%（す

なわち、約15億件が販売）。

- *銀行または決済システムのログインデータ* - 発見されたものの約20%（すなわち、約6億件が販売）。
- *Netflix、その他アプリのログイン認証情報* - 発見されたものの約30%（約9億件が販売）。

そして、様々な研究（例えばMcAfee、 2015年）から得られた価格と、サンプリングされた5つのダーク・ウェブ・サイトで見つかった価格を使用して、これらの収益を計算することが可能です。利用可能な中間点価格を使用すると、次のようになります。

- **クレジットカードデータ**の価値は1枚あたり約10ドル（2016年 ~ 2017年の1件あたりの平均販売額）。調査によると10ドルで15億件なので、合計**150億ドル**となります。
- **銀行や決済システムのデータ**はそれぞれ約190ドル（2016年 ~ 2017年の1件あたりの平均販売額）。調査によると190ドルで6億件なので、合計**1,140億ドル**となります。
- **ログイン認証情報**は、1件あたり約0.55ドル（2016年 ~ 2017年の1件あたりの平均販売額）。調査によると、0.55ドルで9億件なので**4億9500万ドル**となります。
- **盗まれたカードの使用**は、2016年 ~ 2017年の間に**300億ドル**の損失（収益）があると推定されています。

合計 = 1,600億ドル

より高い価格を適用した場合や、ポイントや医療記録、社会保障番号、信用格付けなどの他の種類の記録が含まれている場合は、実際にはこれよりもはるかに収益が高くなる可能性が高いでしょう。

クライムウェア (CaaS) - 16億ドル以上

データ取引の収益を計算するのと同様の困難さは、クライムウェアやサービスとしてのサイバー犯罪プラットフォームで利用可能な多種多様な商品やサービスから得られる収益を理解しようとする研究者も直面しています。同様の最小限アプローチを用いて、収益を生み出す活動を3つのタイプに限定して推定値を算出しました。DDoS/ボットネットのレンタル、マルウェアの購入またはレンタル、基本的なハッキングサービスのレンタルです。価格設定に関する証拠は、2017年7月から2018年1月の間にアクセスした5つのオンライン・ダーク・ウェブ・フォーラムのサンプルから得られたものと利用可能な公開研究データと組み合わせています。

- *DDoS攻撃/ボットネットのレンタル* - ~年間1,300万ドル。この見積もりは、2つの要因に基づいています。

    1) DDoS/ボットネットのレンタルには、攻撃の時間やその強さにもよりますが、1日あたり平均200ドル程度のコストがかかることが判明しました。一部の情報源（例：Ablon et al、 2014年）によると、DDoS のレンタルには 1,000 ドルもの費用がかかる

ものもあります。

2) これらのコストは、年間平均650万件のDDoS攻撃が行われているという現在の推定値と相関させることができます（Khalimonenko & Kupreev、 2017年）。ただし、同じボットネットが複数回展開される可能性があることや、もちろん、すべてのDDoS攻撃にレンタルしたボットネットが関与しているわけではないことを考慮しなければいけません。そこで、レンタルしたDDoS/ボットネットが関与しているのは攻撃の1%だけだと仮定すると、合計1,300万ドルの収益が得られます（つまり、65,000回の攻撃 × レンタルされた場合の1回あたり200ドル）。

- マル*ウェアの購入* - ~ 年間1,100万ドル。この見積もりは、マルウェアを2種類だけ購入することの合計値に基づいています。

  1) *エクスプロイト* -コストは調査したデータソースやサンプリングしたサイトによって大きく異なります。現在は廃止された RealDeal のサイトでは、より需要の高いエクスプロイト、特にAppleのシステムに関わるものの価格は非常に高く、Apple Cloudのエクスプロイトで約17,000ドル、iOSのエクスプロイトでは最大25万ドルとなっていました。最近の調査（Ablon et al、 2017年）では、Blackhole のエクスプロイト・キットが1,500ドル前後で販売されていることがわかりました。この

調査のためにサンプリングしたサイトでの調査結果に裏付けられた他のデータ（例：Secureworks、2016年）によると、エクスプロイトは100ドル以下のような低価格で手に入れることができます。この低い100ドルという数字を使い、2016年に推定された800万件のエクスプロイト・キット攻撃のわずか1％（Escueta、2017年）と相関させると、エクスプロイトの販売による**800万ドル**の収益を導き出すことができました（すなわち、8万件 × 100ドル）。

2) *リモート・アクセス型トロイの木馬（RAT）* - この種のマルウェアは、調査したサイトやさまざまな公表されたソースから、わずか10ドルで入手することができました。2016年の1億2700万件のマルウェアサンプルのうち23%がトロイの木馬が関与していたことがわかっています（AV-Test、 2017年）が、これは約2,921万件になります。再度、購入したRATが1％だけに関与していたと仮定すると、切り上げて、約**300万ドル**（すなわち、292,100件 × 10ドル）となります。

- *ハッカーのレンタルサービス* - ~ **年間16億ドル。**この見積もりは2つの要因に基づいています**。**

1) 上記の他の犯罪サービスのコストと同様に、ハッキングサービスをレンタルする際の価格は非常に幅がありました。ある情報源（Weissman、 2015年）では、ウェブサイトを攻撃する場合の価格を

2,000ドルとしていますが、別の情報源では、データをハッキングして盗むために人を雇うと350ドル程度の低価格になることがわかっています（Secureworks、 2016年）。メールアカウントのハッキングなどの小規模な仕事の費用は、調査したソースとサンプルしたサイトによると、平均で約200ドルでした。

2) 2017年には40億人のソーシャルメディアユーザーがおり、Google は年間約20%のソーシャルメディア・アカウントがハッキングされていると推定しています。これは、約8,000万件のハッキングになります。ソーシャルメディアのハッキングとハッカーのレンタルの双方が上記のCaaS指標よりも普及しているように見えることを考えると、少し甘く見てこれらのハッキングの10%（とはいえ非常に保守的な）については、ハッキングサービスが関与していたと仮定することができるでしょう。これにより、16億ドルのハッキング収益が得られることになります（すなわち800万件 × $200)。驚くほど高いとはいえ、ハッカーの雇用はソーシャルメディアのアカウントだけではなく、はるかに幅広いターゲットを対象としていることを考えると、これは過小評価ではないかと思われます。

合計 = 16億ドル

これらよりも多くのサービスがCaaSサイトで広告されていることに注意してください。例えば、DDoS クラウド攻撃、フィッシングメールサイトやキャンペーン、Gmail へのアクセス、ホテルや航空会社などのポイント付与、小論文の成績変更、記録の削除（運転免許証のポイントや犯罪歴など）、Amazon のレビューなどが挙げられます。これらの収益が含まれていないことを考えると、クライムウェアからの収益はここで示されている合計よりもはるかに高い可能性が高いと思われます。

サイバーロンダリング - 最大2,000億ドル

少なくとも2つの情報源がこの数字を三角測量しています。第一に、ユーロポールは、暗号通貨が現在ヨーロッパだけでロンダリングされた資金の約4%を占めていると推定しています。UNODCの2兆ドルのグローバル・ロンダリングの総額と関係づけると、ロンダリングされたサイバー犯罪の収入の基準値は少なくとも800億ドルになることを意味します。しかし、サイバー犯罪の収益を洗浄する方法は、もちろん暗号通貨の利用以外にもたくさんあります。

例えば、20億ドルもの資金洗浄に成功したミュールと再発送の事業があります。このような事業が世界で30件あるだけで、ミュール・ロンダリングで約600億ドルの資金洗浄が行われていることになります。正規の銀行やオンラインギャンブルなど、サイバー犯罪者が関与していることが知られている他の種類のロンダリングを考

慮すると、少なくともさらに600億ドルを含む可能性があります。これにより、サイバーロンダリングの収益は最大2,000億ドルに達します。（すなわち、600億ドル + 800億ドル + 600億ドル = 2000億ドル）。

合計 = 最大2000億ドル

参考文献

Ablon, L., Libicki, M.C. and Golay, A.A. (2014). *Markets for Cybercrime Tools and Stolen Data*. RAND.

Anand, P. (2015). *'18 most popular things fraudsters buy with your credit card'* [online]. Market Watch. Available at: https://www.marketwatch.com/story/18-most-popular-things-fraudsters-buy-with-your-credit-card-2015-11-24

Anderson R., Barton, C., Böhme, R., Clayton, R., van Eeten, M.J.G., Levi, M., Moore, T. and Savage, S. (2012). *Measuring the Cost of Cybercrime*. Paper presented at the Weis 202 Workshop on the Economics of Information Security Berlin, Germany, 25-26th June 2012.

Apps, P. and Finkle, J. (2014). *Suspected Russian Spyware Turla Targets Europe, United States* [online]. Reuters. Available at: https://www.reuters.com/article/us-russia-cyberespionage-insight/suspected-russian-spyware-turla-targets-europe-united-states-idUSBREA260YI20140307

AV-Test (2017). *Security Report 2016/7* [online]. Accessed at: https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2016-2017.pdf

Barth, B. (2016). *Snack attack: A crimeware-as-a-service menu for wannabe hackers* [online]. SC Media. Accessed at: https://www.scmagazine.com/snack-attack-a-crimeware- as-a-service-menu-for-wannabe-hackers/article/527865/

BBC (2014). *Snapchat hack affects 4.6 million users* [online]. BBC News. Accessed at: http://www.bbc.co.uk/news/technology-25572661

BBC (2015). *Fake luxury goods online sites closed by police* [online]. BBC News. Accessed at: http://www.bbc.co.uk/news/technology-31454822

Beaming (2017). *Cyberthreat Report 2017:Attacks on UK businesses increase to 231,028 each* [online]. Beaming. Accessed at: https://www.beaming.co.uk/cyber-reports/cyber-attacks- uk-businesses-increase-231028-2017/

Bengineer (2015). *How to Steal Form Data from Your Fake Website* [online]. Null Byte. Accessed at: https://null-byte.wonderhowto.com/how-to/steal-form-data-from-your-fake-website-0164112/

Benyawa, L. (2016). *Agency says 3000 cyber-crime cases reported in Kenya monthly* [online]. Standard Digital. Accessed at: https://www.standardmedia.co.ke/business/article/2000 204352/agency-says-3000-cyber-crime-cases-reported-in- kenya-monthly

Berson, S (2017). *Manafort rented out illegal AirBnb, indictment says. So did his daughter, lawsuit claimed* [online]. Miami Herald. Accessed at: http://www.miamiherald.com/news/nation-world/national/article181676271.html

Bowers, S. (2016) *MPs poised to investigate VAT fraud on Amazon and eBay* [online]. The Guardian. Accessed at: https://www.theguardian.com/business/2016/dec/21/mps-vat-fraud-amazon-ebay-public-accounts-committee

Bouchard, M. and Wilkins, C. (2010). *Illegal Markets and the Economics of Organised Crime*. Routledge.

Brown, J. (2016). *The average hacker makes less than $30,000 a year* [online]. The Week. Accessed at: http://theweek.com/articles/604630/average-hacker-makes-less-than-30000-year

Button, M. and Cross, C. (2017). *Cyber Frauds, Scams and Their Victims*. London: Taylor And Francis.

Carlisle, D. (2017). *Virtual Currencies and Financial Crime: Challenges and Opportunities*. RUSI.

CCFS (2016). *Annual Fraud Indicator*. Centre for Counter Fraud Studies, University of Portsmouth.

Chaffey, D. (2017). *Forecast growth in percentage of online retail / Ecommerce sales* [online]. Smart Insights. Accessed at: https://www.smartinsights.com/digital-marketing- strategy/online-retail-sales-growth/

Cosgrave, J. (2014). *Online gambling: The new home for money launderers?* [online]. CNBC. Accessed at: https://www.cnbc.com/2014/04/25/online-gambling-the-new-home-for-money-launderers.html

Cox, J. (2017). *Inside Airbnb's Russian Money-Laundering Problem* [online]. The Daily Beast. Accessed at: https://www.thedailybeast.com/inside-airbnbs-russian-money-laundering-problem

CSIS (2014). *Estimating the Global Cost of Cybercrime*. Centre for Strategic and International Studies/McAfee

Cybersecurity Ventures 2017 *Annual Cybercrime Report.*

Davies, R. (2018). *Five UK online casinos may lose licence over money-laundering fears* [online]. The Guardian. Accessed at: https://www.theguardian.com/society/2018/jan/05/five-of-uk-online-casinos-may-lose-licence-over-money-laundering-fears

DCA (2014). *Good Money Gone Bad: Digital Thieves and the Hijacking of the Online Ad Business.* Digital Citizens Alliance

Detica (2011). *The Cost of Cybercrime*. Detica and UK Cabinet Office.

Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., Welburn, W. and Winkelman, Z. (2018). *Estimating the Global Cost of Cyber Risk*. RAND.

Dubourg, R. and Prichard, A. (2008). *Organised crime: revenues, economic and social costs, and criminal assets available for seizure*. UK Home Office.

Economist (2016). *Buying drugs online: shedding light on the dark web* [online]. The Economist. Accessed at: https://www.economist.com/news/international/217021 76-drug-trade-moving-street-online-cryptomarkets- forced-compete

Escueta, G. (2017). *Tracking the Decline of Top Exploit Kits* [online]. Trendlabs Security Intelligence Blog. Accessed at: https://blog.trendmicro.com/trendlabs-security-intelligence/tracking-decline-top-exploit-kits/

Eurostat (2017). *E-commerce statistics for individuals.* Data extracted from 2017 Survey on ICT usage in households and by individuals.

Europol (2016). *178 arrests in successful hit against money muling* [online]. Europol press release. Accessed at: https://www.europol.europa.eu/newsroom/news/178-arrests-in-successful-hit-against-money-muling

Europol (2017). *How Illegal Drugs Sustain Organised Crime in Europe* [online]. Europol Business Fundamentals Report. Accessed at: https://www.europol.europa.eu/publications-documents/how-illegal-drugs-sustain-organised-crime-in- eu

Fahmy, D. (2010). *Credit Card Crooks Like to Shop at Best Buy, Target, Amazon* [online]. ABC News. Accessed at: http://abcnews.go.com/Business/credit-card-theft-crooks-shop-best-buy-target/story?id=9931006

Fossbytes (2017). *How Much Money Torrent Sites Like The Pirate Bay And KickassTorrents Make?* [online]. Fossbytes. Accessed at: https://fossbytes.com/how-much-money-torrent-site-make-pirate-bay-kickass/

Fox-Brewster, T. (2017). *Google Warns Ransomware Boom Scored Crooks $2 Million A Month* [online]. Forbes. Accessed at: https://www.forbes.com/sites/thomasbrewster/2017/07/25/google-ransomware-multi-million-dollar-business-with-locky-and-cerber/#51fd09266caf

Freeman, R. and Holzer, H. (1986). *The Black Youth Employment Crisi*s. University of Chicago Press.

GFI (2017). *Transnational Crime and the Developing World*. Global Financial Integrity.

Goldfeder, S., Kalodner, H., Reisman, D. and Narayanan, A. (2017). *When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies* [online]. Cornell University. Accessed at: https://arxiv.org/abs/1708.04748

Grabosky, P., Smith, R.G. and Dempsey, G. (2002). *Electronic Theft: UnlawfulAcquisition in Cyberspace*. Cambridge: Cambridge University Press.

Greenberg, A. (2013). *FBI Says It's Seized $28.5 Million In Bitcoins From Ross Ulbricht* [online]. Forbes. Accessed at: https://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/#76df4feb2765

GSMA (2017). *State of the Industry Report on Mobile Money* [online]. Accessed at: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/03/GSMA_State-of-the-Industry-Report-on-Mobile-Money_2016.pdf

Guardian (2016). *Ten arrested in Netherlands over bitcoin money-laundering allegations* [online]. The Guardian. Accessed at: https://www.theguardian.com/technology/2016/jan/20/bitcoin-netherlands-arrests-cars-cash-ecstasy

Hao, S., Borgolte, K., Nikiforakis, N., Stringhini, G., Egele, M., Eubanks, M., Krebs, B. and Vigna, G. (2015) *Drops for Stuff, An Analysis of Reshipping Mule Scams*. ACM Conference on Computer and Communications Security.

Harding, L., Hopkins, N. and Barr, C. (2017). *British banks handled vast sums of laundered Russian money* [online]. The Guardian. Accessed at: https://www.theguardian.com/world/2017/mar/20/briti sh-banks-handled-vast-sums-of-laundered-russian-money

Holt, T., Smirnova, O. and Chua.Y. (2016). *Exploring and Estimating the Revenues and Profits of Participants in Stolen Data Markets*. Deviant Behavior.

Hubbs, R. (2014). *Shell games: Investigating shell companies and understanding their roles in international fraud.* Fraud Magazine, July/August.

ICE (2010). *Mass marketing Fraud, A Threat Assessment*. International Mass Marketing Fraud Working Group, US Immigration and Customs Enforcement.

IOCTA (2017). *Internet Organised Crime Threat Assessment 2017*. Europol.

IPC (2013). *Report on the Theft of American Intellectual Property.*

Irwin, A. and Milad, G. (2016). *The use of crypto-currencies in funding violent jihad.* Journal of Money Laundering Control, 19 4, pp.407-425.

Isaza, A. (2015). Fake Japanese E-Commerce Sites Used for E-commerce [online]. ISBuzz News. Accessed at: https://www.informationsecuritybuzz.com/articles/fake-japanese-e-commerce-sites-used-for-stealing-credit-card-information/

Jacobsen, M. (2009) *Terrorist Financing on the Internet*. CTC Sentinel, June, 2,6.

John (2017). *Corporate Bankers Stealing Own Company Data to Sell on Darknet* [online]. Darknetmarkets.co. Accessed at: https://darknetmarkets.co/corporate-bankers-stealing-own-company-data-to-sell-on-darknet/

Johnson, L. (2017). *Crime-as-a-Service Could Be the Next Big Threat to Your Business* [online]. Entrepreneur. Accessed at: https://www.entrepreneur.com/article/298727

Khalimonenko, A. and Kupreev, O. (2017). *DDos Attacks in Q1 2017* [online]. Securelist. Accessed at: https://securelist.com/ddos-attacks-in-q1-2017/78285/

Khan, I. (2016). *The virtual future of money laundering*. Fraud Magazine, June.

Klara, R. (2017). *Counterfeit Goods Are a $460 Billion Industry, and Most Are Bought and Sold Online*. Adweek. Accessed at: http://www.adweek.com/brand-marketing/counterfeit-goods-are-a-460-billion-industry-and-most-are-bought-and-sold-online/

Krebs, B. (2013). *Crimeware Author Funds Exploit Buying Spree* [online]. Krebs on Security. Accessed at: https://krebsonsecurity.com/2013/01/crimeware-author-funds-exploit-buying-spree/

Krehel, O. (2016). *The rise of LinkedIn fraud* [online]. CSO Online. Accessed at: https://www.csoonline.com/article/3036072/social-networking/the-rise-of-linkedin-fraud.html

Kruisbergen, E., Kleemans, E. and Kouwenberg, R. (2014). *Profitability, Power, or Proximity? Organised Crime Offenders Investing Their Money in Legal Economy.* Eur J Crim Policy Res 21:237–256.

Kruithof, K., Dujso, E. Décary-Hetu, D. and Aldridge, J. (2016). *Internet-facilitated drugs trade.* RAND.

Kuchler, H. (2014). *Cyber criminals eye financial markets for a better return on investment* [online]. Financial Times. Accessed at:

https://www.ft.com/content/2a11ee92-3cbc-11e4-871d-00144feabdc0

Lewis, P. and Hilder, P. (2018). *Leaked: Cambridge Analytica's Blueprint for Trump Victory* [online]. The Guardian. Accessed at: https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory

Maxey, L. (2017). *Terror Finance in the Age of Bitcoin* [online]. The Cipher Brief. Accessed at: https://www.thecipherbrief.com/article/tech/terror-finance-age-bitcoin

Machalinksi, A. (2017). *Bitcoin and the Blockchain Are Disruptors in Global Real Estate* [online]. Mansion Global. Accessed at: https://www.mansionglobal.com/articles/77889-bitcoin- and-the-blockchain-are-disruptors-in-global-real-estate

Matthews, L. (2018). *Hackers Abuse Google Ad Network To Spread Malware That Mines Cryptocurrency* [online]. Forbes. Accessed at: https://www.forbes.com/sites/leemathews/2018/01/26/hackers-abuse-google-ad-network-to-spread-malware-that-mines-cryptocurrency/#3e933e987866

McAfee (2015). *The Hidden Data Economy.*

McKeon, A. (2017). *A Look Into the Thriving Dark Web Criminal Market* [online]. Recorded Future. Accessed at: https://www.recordedfuture.com/podcast-episode-30/

NBC (2017). *Ransomware: Now a Billion Dollar a Year Crime and Growing* [online]. NBC News. Accessed at: https://www.nbcnews.com/tech/security/ransomware- now-billion-dollar-year-crime-growing-n704646

NCA (2016). *Cybercrime Assessment 2016*. UK National Crime Agency.

Nguyen, H. and Loughran, T. (2017). *On The Reliability And Validity Of Self-Reported Illegal Earnings: Implications For The Study Of Criminal Achievement*. Criminology, 5, 3, pp. 575–602.

Nilson (2016). *Card Fraud Losses Reach $21.84 Billion*. Nilson Report, Issue 1096.

Norton (2011). *Annual Cybercrime Report.*

OECD (2016). *Trade in Counterfeit and Pirated Goods.*

Paganini, P. (2017). *Western Union agreed to pay $586 Million to settle fraud charges* [online]. Security Affairs. Accessed at: http://securityaffairs.co/wordpress/55573/breaking-news/western-union-settlement.html

Palmer, D. (2017) *Dark web vendors are selling remote access to corporate PCs for as little as $3* [online]. ZDnet. Accessed at: https://www.zdnet.com/article/dark-web-vendors-are-selling-remote-access-to-corporate-pcs-for-as-little-as-3/

Panda (2010). *Western Union Entwined with Cybercrime?* [online]. Panda Security Mediacenter. Accessed at: https://www.pandasecurity.com/mediacenter/malware/western-union-entwined-with-cybercrime/

Perez, S. (2017). *We Heart It says a Data Breach affected over 8 million Accounts* [online]. TechCrunch. Accessed at: https://techcrunch.com/2017/10/16/we-heart-it-says-a-data-breach-affected-over-8-million-accounts-included-emails-and-passwords/

Perlroth, N. (2017). *All 3 billion Yahoo Accounts Were Affected by 2013 Attack* [online]. The New York Times. Accessed at: https://www.nytimes.com/2017/10/03/technology/yah oo-hack-3-billion-users.html

Ponemon (2015). *Annual Cost of Data Breach Study: Global Analysis*. Ponemon Institute.

Popper, N. (2017). *Bitcoin Exchange Was a Nexus of Crime, Indictment Says* [online]. New York Times. Accessed at: https://www.nytimes.com/2017/07/27/business/dealbo ok/bitcoin-exchange-was-a-nexus-of-crime-indictment-says.html

Power, M. (2013). *Drugs 2.0.* New York: St Martins Press.

RBS (2016). *Databreach QuickView Report*. Risk Based Security.

Reuter, P. (2005). *Chasing Dirty Money: the Fight Against Money Laundering*. Peterson Institute.

Reuters (2015). *Cybercrime ring steals up to $1 billion from banks: Kaspersky* [online]. Reuters. Accessed at: https://uk.reuters.com/article/uk-cybersecurity-banks/cybercrime-ring-steals-up-to-1-billion-from-banks-kaspersky-idUKKBN0LJ02L20150215

Richet, J.L. (2013). *Laundering Money Online: a review of cybercriminals' methods*. United Nations Office on Drugs and Crime (UNODC), Tools and Resources for Anti- Corruption Knowledge.

Richards, J.R. (1998) *Transnational Criminal Organizations, Cybercrime, and Money Laundering*. CRC Press.

Robinson, T. and Fanusie, Y. (2017). *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services*. Center on Sanctions and Illicit Finance.

Scott, G. (2016). *The Very Real Risks Behind the $400 Billion Illegal Online Pharmacy Industry* [online]. Medscape. Accessed at: https://www.medscape.com/viewarticle/873704

Secureworks (2016). *Underground Hacker Marketplace Report.*

Shih, G. (2013). *Facebook admits year-long data breach exposed 6 million users* [online]. Reuters. Accessed at: https://uk.reuters.com/article/net-us-facebook-security/facebook-admits-year-long-data-breach-exposed- 6-million-users-idUSBRE95K18Y20130621

Silva, S. (2018) *Criminals hide 'billions' in crypto-cash – Europol* [online]. BBC Accessed at: http://www.bbc.com/news/technology-43025787

Siwek, S. (2007). *The True Cost of Sound Recording Piracy to the U.S. Economy*. Institute for Policy Innovation Report.

Sky (2017). *Banker helped gang launder £16m for cybercriminals* [online]. Sky News. Accessed at: https://news.sky.com/story/banker-helped-gang-launder-16m-for-cybercriminals-11044498

Srnicek, N. (2016) *Platform Capitalism*. London: Wiley.

SOCTA 2017 *Serious and Organised Crime Threat Assessment 2017*, Europol

Southport Local (2014). *Nine arrested in ticket fraud investigation.* Southport Local, 15th May 2014.

Steiner, I. (2017) *Rethinking Returns in Wake of $1.2 million Amazon Fraud*. EcommerceBytes Blog. Accessed at: https://www.ecommercebytes.com/C/blog/blog.pl?/pl/2017/10/1506992808.html

Sulleyman, A. (2017). *Kodi Box Seller Who made £370,000 Given Suspended Prison Sentence* [online]. The Independent. Accessed at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/kodi-box-maiz-limited-daniel-david-brown-llansamlet-suspended-prison-sentence-made-370000-profit-a7821601.html

Szabo, A. (2016) *From the Mob to Mario: How Money Laundering Lives on Through Video Games*, Panopticon. Accessed at: https://www.panopticonlabs.com/from-the-mob-to-mario-how-money-laundering-lives-on-through-video-games/

Szoldra, P. (2016). *Hackers are making $7,500 per month by holding people's data hostage* [online]. Business Insider. Accessed at: http://uk.businessinsider.com/flashpoint-report- ransomware-2016-6?r=US&IR=T

Takahashi, D. 2014 *Only 0.15 percent of mobile gamers account for 50 percent of all in game purchases* [online]. Venturebeat. Accessed at: https://venturebeat.com/2014/02/26/only- 0-15-of-mobile-gamers-account-for-50-percent-of-all-in-game-revenue-exclusive/

Teicher, R. (2018). *How Uber Ghost Rides are Linked to Money Laundering* [online]. The Next Web. Accessed at: https://thenextweb.com/contributors/2018/03/18/uber-ghost-rides-linked-online-money-laundering/

Telegraph (2014). *How terrorists are using social media* [online]. The Telegraph. Accessed at: https://www.telegraph.co.uk/news/worldnews/islamic-state/11207681/How-terrorists-are-using-social-media.html

Trend Micro (2016). *The Cybercriminal Roots of Selling Online Gaming Currency*.

Trend Micro (2017). *Threats to Global Business Survey*.

Trustwave (2015). *Global Security Report*.

UCSD (2017). *UC San Diego and NYU estimate 25 million in ransomware payout*. UC San Diego Press release, July 2017.

UNODC (2011). *Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organised Crimes*. United Nations Office on Drugs and Crime Report, October 2011.

Vidalon, D. (2017). *Airbnb drops controversial payment card in France* [online]. Reuters. Accessed at: https://uk.reuters.com/article/us-airbnb-card/airbnb-drops-controversial-payment-card-in-france-idUKKBN1E616B

Vincent, J. (2013). *Instagram Virus Shows that 'Online Likes' are Worth More than Stolen Credit Cards* [online]. The Independent. Accessed at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/instagram-virus-shows-that-online-likes-are-worth-more-than-stolen-credit-cards-8774997.html

Viscusi, W. (1986). *The Risks and Rewards of Criminal Activity: A Comprehensive Test of Criminal Deterrence*. Journal of Labor Economics, 4 3, 317-40.

Wales Online (2015). *Dealer lived the high life on profits from selling illegal drugs and legal highs online* [online]. Wales Online. Accessed at: https://www.walesonline.co.uk/news/wales-news/dealer-lived-high-life-profits-9385858

Wall, D. (2016). *The theft of ideas as a cybercrime: downloading and changes in the business model of creative arts.* In McGuire, M. and Holt, T. (eds) *The Handbook of Technology Crime & Justice*. Routledge.

Ward, V. and Maidment, J. (2017). *Dealers 'using social media sites to sell drugs to teenagers* [online]. The Telegraph. Accessed at: https://www.telegraph.co.uk/news/2017/12/31/dealers-using-social-media-sites-sell-drugs-teenagers/

Weissman, C. (2017). *9 things you can hire a hacker to do and how much it will (generally) cost* [online]. Business Insider: http://uk.businessinsider.com/9-things-you-can-hire-a-hacker-to-do-and-how-much-it-will-generally-cost-2015-5

Whitty, M. T. (2015). *Mass-marketing fraud: A growing concern*. IEEE Security & Privacy, 13(4).

White, G. (2018). *UK company linked to laundered Bitcoin billions* [online]. The BBC. Accessed at: http://www.bbc.co.uk/news/technology-43291026

バイオグラフィー：Michael McGuire博士

Surrey大学 上級講師

Michael McGuire博士は、イギリスのSurrey大学で犯罪学の上級講師を務めています。サイバー犯罪、テクノロジー、司法制度の研究で国際的な注目を集めており、これらの分野で広く出版をしています。

彼の最初の著書である*Hypercrime: The New Geometry of Harm*（Glasshouse、2008年）は、ハイパーコネクテッドネスという概念でサイバー犯罪を初めて定義したもので、2008年にBritish Society of Criminologyの次点図書賞を受賞しています。

彼の近著*Technology, Crime & Justice: The Question Concerning Technomia*と*Handbook of Technology, Crime and Justice*（Routledge、2012年、2016年）では、司法制度における技術の意味合いを包括的に概観しています。

これらの研究は、組織犯罪がインターネットにどのように移行してきたかを初めて研究した *Organised Crime in the Digital Age*（2012年）や、英国内務省の *Cybercrime, A Review of the Evidence*（2014年）など、サイバー犯罪に関する応用研究を補完するものです。現在は、英国工学・物理科学研究会議が資金提供した*ACCEPTプロジェクト（Addressing Cybersecurity and Cybercrime via a co-Evolutionary Approach to reducing human-related risks）*の主席研究員を務めています。このプロジェクトの目的は、サイバーセキュリティにおける人的要因をモデル化するための共進化ベースの方法論を開発することです。

研究スポンサー：Bromium, Inc.

私たちの使命は、デジタルコミュニケーションを利用して、自由なアイディアの交換からグローバルな商取引の可能性、情報や教育の民主化まで、社会の発展に貢献したいと願う人々にセキュリティを提供することです。サイバー犯罪者がオンラインの安全性を脅かそうと活動していますが、当社は優れた技術革新によってサイバー犯罪者の活動を阻止することに全力を尽くしています。

"セキュリティを真剣に考えているならBromiumと話すべきだ。"

当社の創業者であるIan PlattとSimon Crosbyは、もともとXenSourceを設立し、Xenハイパーバイザーをベースにエンタープライズクラスの仮想化製品を構築していました。XenSourceは2007年にCitrixに買収されました。彼らはしばらくCitrixに在籍した後、エンドポイントセキュリティに革命を起こすアイディアを思いつきました。

その結果、エンドポイントの所有権を本質的に保護

するBromium Secure Platformは、今日の検知-保護ソリューションが必要とする最初の感染者を無くします。すでにいくつかの政府が、世界中の従業員を保護するためにBromiumを導入しています。

アプリケーションの隔離と制御

多くの技術者にとって、アプリケーション隔離は、サイバーセキュリティとエンドポイント保護に関して、新しい用語かもしれません。この用語は、国家安全保障局（NSA）によって広まっています。アプリケーション隔離が、高度な、ゼロデイ、国家レベルのマルウェアを最終的に阻止するための方法であることが詳細に説明されています。

"「マルウェアを止める唯一の方法は、マルウェアを止めないことだ」とよく言われてきました。それこそが、アプリケーション隔離です。"

根本的に検知を利用してマルウェアを止めることには欠陥があります。悪意のあるコードを書く人は一歩先を行く傾向があるため、常にキャッチアップが必要になります。一般論として、マルウェアを書く人は一度だけ正しく書けばいいのに対し、マルウェアを停止させるソフトウェアを書く人は毎回正しく書く必要があります。このことは最近のマルウェアWannaCryとPetyaのエクスプロイトで公に明らかになりました。ほとんどの主要な検知ベンダーは、これまでに見たことがないようなもので

あったため、このエクスプロイトに対して脆弱性を持っていました。彼らはそれを止めるための方法を素早く開発していましたが、もしあなたが不運にもゼロデイにこのエクスプロイトを受けてしまったらどうでしょうか？

本当の問題はマルウェアを止める方法としての検知です。Fred Cohenは、著名なコンピューター科学者で、「コンピュータウイルス」という言葉の発明者でもあります。彼は、「すべての可能性のあるウイルスを完全に検知できるアルゴリズムは存在しない」ため、検知は劣っていると考えていました。

「マルウェアを止める唯一の方法はマルウェアを止めないことだ」とよく言われてきました。

それこそが、アプリケーション隔離です。

信頼されていないタスクを保護する

アプリケーション隔離では、ユーザーがマルウェアの侵入ポイントとなり得る信頼できないタスクを実行すると、そのタスクをユーザーにシームレスに実行させるための隔離された環境が作成されます。マルウェアがそのタスクの一部に含まれている場合、保護されたホスト・オペレーティング・システムにアクセスすることなく、隔離された環境で最後まで動かすことができます。これは、マルウェアは完全に動いていると信じているにもかかわらず、使い捨ての環境にしかダメージを与えないという古典的な「ハニーポット」シナリオです。

"マルウェアは仮想マシンから逃がれることができない。"

Bromium がまさにそれです。Bromium の隔離は、信頼されていないユーザータスクを、ユーザーから透過的なハードウェア隔離された仮想マシンで実行します。ユーザーがブラウザでタブを開いたり、信頼されていないOfficeやPDFドキュメントを開いたり、信頼されていない実行ファイルを実行したりするたびに、ブロミウムの隔離は、ユーザーのためにタスクを実行するシームレスなハードウェア隔離された仮想マシンを作成します。マルウェアがそのタスクの一部である場合、その仮想マシンにのみ存在し、保護されたホスト・オペレーティング・システムを安全に保ちます。

ハードウェアで隔離された仮想マシンがユーザーに代わって信頼されないタスクを実行している間、Bromiumの隔離はイントロスペクションを使い、外部から仮想マシンを覗き込んでいます。つまり、仮想マシンを監視し、「異常な」活動を探しているのです。マルウェアのペイロード全体を含むこのすべての脅威インテリジェンスは、その後収集されSOCチームの分析のためにBromium Controllerに送られます。フォレンジックの詳細がSOCチームの分析のために準備されますが、攻撃がユーザーのホストコンピュータに触れることはありません。

"我々は検知する前に保護するアプローチを取る。"

以下のウォークスルーでは、Bromiumがどのようにアプリケーション隔離を利用して、信頼できないドキュメントからユーザーを保護しているかをご覧いただけます。

続いて、ハードウェアで隔離された仮想マシンを外部から監視するためにイントロスペクションを使用する方法をご覧ください。最後に、なぜ検知が失敗するのか、そしてなぜアプリケーション隔離が機能するのかを示す方法としてVirusTotalを使います。

まず、内部にマルウェアが隠されているMicrosoft Wordドキュメントを起動します。Bromium Live Viewというユーティリティを使用すると、私のエンドポイント上で稼働しているすべてのハードウェアで隔離された仮想マシンを見ることができます。マルウェアが入ったWordドキュメントは「Micro-VM 0123」の中で実行されています。しかしながら、ユーザーの視点から見ると、ドキュメントが他のWordドキュメントと同じように実行されているように見えます。

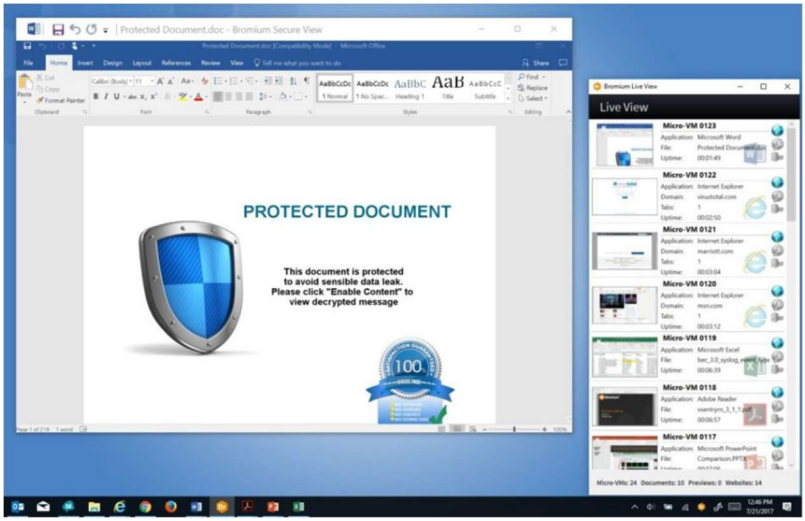


図 7：WordドキュメントのBromiumライブビュー

ハードウェアで隔離された仮想マシンでドキュメントが開かれると、マルウェアはペイロードの実行を開始

します。Bromiumのイントロスペクションは、異常なイベントが発生していることを検知し、ドキュメントにマルウェアが含まれていることを知らせるアラートをユーザーとSOCチームに送信します。しかしながら、マルウェアはハードウェアで隔離された仮想マシン内でしか動くことができません。

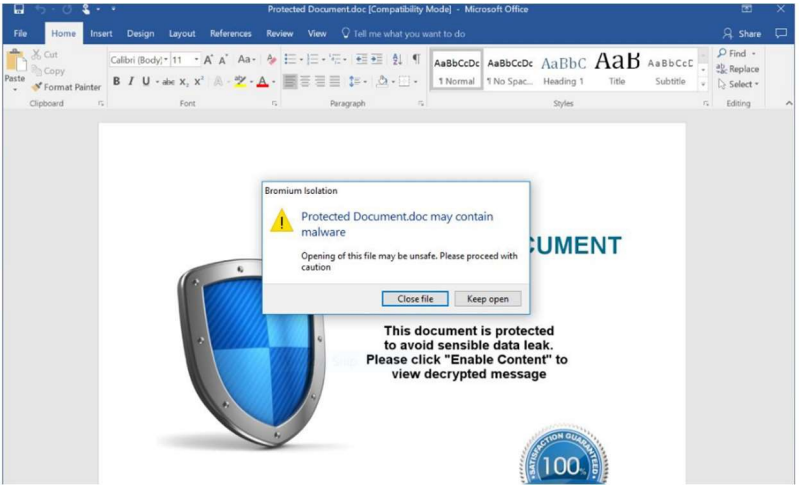


図 8：Bromiumのマルウェアに関する警告

イントロスペクションが仮想マシン上で実行されている間、すべてのフォレンジック情報の詳細がBromium Controllerサーバーに送られています。

Bromium Controllerは高精度のアラートを提供

この時点でSOCチームは、マルウェアが何をしたかのキルチェーン全体を調べることができます。マルウェアを完全に実行させているため、イントロスペクションは、ペイロード全体とマルウェアが何をしたかをステップ-バ

イ-ステップを見ることができるユニークな立場にあります。ほとんどのマルウェアで、最初のステップは「ドロップ＆実行」です。このマルウェアのSHA256ハッシュを調べることで、VirusTotal.comのような公開サイトを検索して、この特定のマルウェアについて業界が何を知っているかを判断することができます。

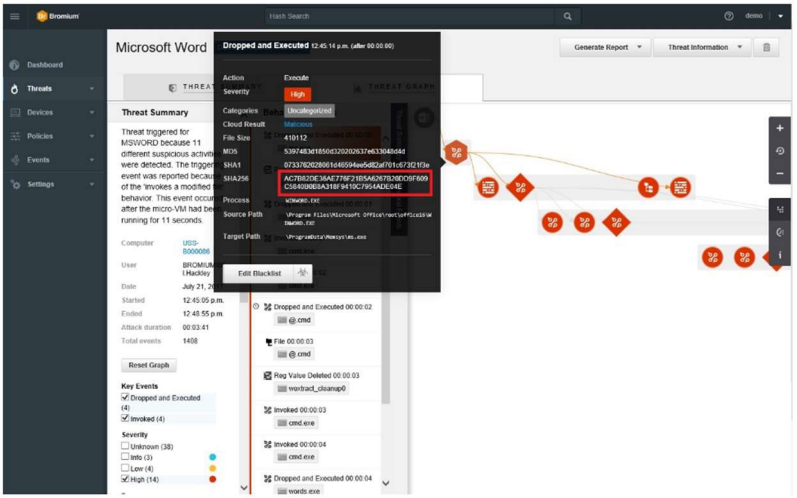


図 9：Bromium Controllerが提供するキルチェーン情報

VirusTotal.comでのマルウェア表示

SHA256をVirusTotal.comの検索エンジンに入力すると、このマルウェアの詳細が表示されます。最初に気づくことは、これが書かれている時点でこのマルウェアのペイロードはすでに1年以上も前のものであるということです。さらに興味深いのは、これが書かれている時点で、VirusTotal.comに報告している57社のベンダーのうち、このファイルが悪意のあるものであることを示しているのは31社だけだということです。もしVirusTotal.comがどの

ようにレポートするかをよく知らないようであれば、”Result” が赤字のベンダーはファイルが悪意のあるものであることを表しています。

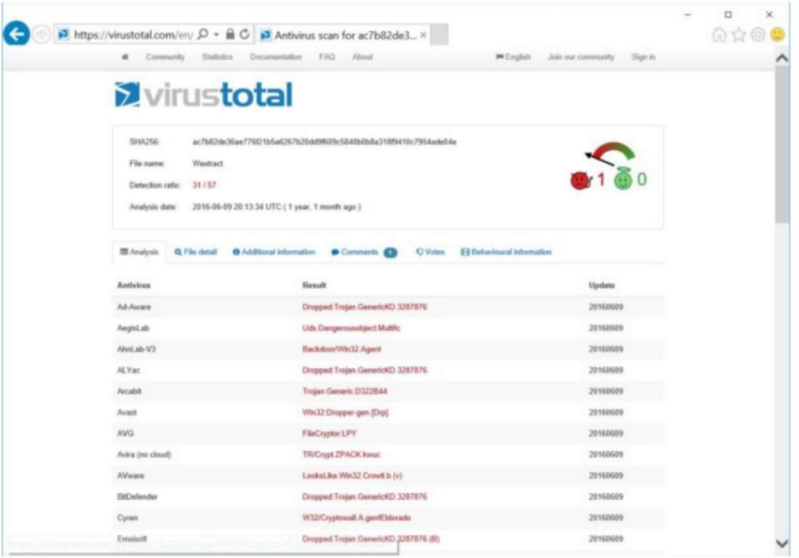


図 10：赤色のファイルはマルウェアが悪意のあるものとして認識されていることを意味する

しかしながら、下にスクロールしてみると緑のチェックマークの ”Result” がついているベンダーは、このファイルを悪意のあるものとして認識していません。つまり緑のチェックマークがついているベンダーを利用しても、この古いマルウェアからは守られないということです。

VirusTotal.comのリストにあるベンダーのほとんどは検知に頼っていますが、なぜ検知に欠陥があるのかは明らかです。それは、そのベンダーがシグネチャファイルを更新することができるかどうかにかかっているからです。必ずしもシグネチャに基づいていない「Next-Gen」

のAVであっても欠点があります。注意深く作られたマルウェアは、「Next-Gen」であっても、どのようなタイプの検知でも常に一歩先を行くことになります。

仮想化のターゲットとなる典型的な脅威ベクトル

- **メールの添付ファイルの保護。**

  従業員は、仕事をするために電子メールの添付ファイルを開かなければなりません。サイバー犯罪者はこのことを知っており、ユーザーを騙して悪意のある添付ファイルを開かせる巧妙な方法を考案し、多層防御を 干回させています。仮想化ベースのセキュリティは、安心してクリックできる唯一のソリューションです。

  マルウェアを封じ込め。安全な使い捨てマイクロVMでOutlookとWebメールの添付ファイルを瞬時に隔離します。

  ホストを保護。マルウェアは隔離から逃れることができず、オンラインの場合もオフラインの場合もユーザーを保護します。

  心配する必要無し。検知の必要がないため、これまでに知られていなかった脅威も完全に隔離され封じ込められます。

- **フィッシング攻撃の封じ込め。**

  フィッシング攻撃は常に進化しており、様々な形をとっています。従業員が仕事をするためにリンクをクリックする必要があるため、ソーシャルエンジニアリングによりフィッシングリンクの特定が困難になるため、フィッシングは特に効果的です。

仮想化ベースのセキュリティは、悪意のあるリンクであっても安全に共有リンクを開くことができる唯一のソリューションです。

マルウェアを隔離。各ブラウザタブは悪意のあるコードを封じ込め、ホストにアクセスできないように、独自の安全なマイクロVMで動作します。

ハッカーの裏をかく。Bromiumのフィッシングプロテクションは、従来の検知技術を回避するための典型的攻撃戦術である、良性のドキュメントに埋め込まれた悪意のあるリンクに対しても機能します。

自信を持ってクリック。外部リンクや共有URLのクリックを気にせずに仕事をしましょう。制限的なITセキュリティポリシーは必要ありません。

- **ウェブダウンロードの保護。**

  悪質なダウンロードが効果的なのは、サイトが非常に多く、一時的で、分類を避けるために内容が頻繁に変化するためです。仮想化ベースのセキュリティは、ドキュメントや実行ファイルを安全にダウンロードしてアクセスできる唯一のソリューションです。

  安全に開く。すべてのドキュメントと実行ファイルのダウンロードは、隔離されたマイクロVM内で自動的かつ瞬時に開かれます。

  継続的に保護。すべてのファイルは、どのようなネットワーク上でも、さらには切断された場合でさえも安全にダウンロードしてアクセスすることができます。

生産性の向上。ダウンロードしたファイルへのユーザーのアクセスを制限したり、ワークフローを阻害したりするような制限的なITセキュリティポリシーの必要はありません。

- **保護されていないネットワークへの安全なアクセス。**

  現代の従業員は、安全ではないパブリックネットワークを使用してネットにアクセスすることもたびたびあります。リモートユーザーにVPNへの接続を要求しても、セキュリティ上の課題は解決しません。なぜならVPNは高度なマルウェアに対する保護を提供しておらず、しかもユーザーは厳格なセキュリティガイドラインに従わないことも多くあります。仮想化ベースのセキュリティは、保護されていないネットワークを使用する際に従業員のアクセスを保護する唯一のソリューションです。

  あらゆるコンテンツを開く。あらゆる種類のファイル、リンク、ブラウザウィンドウ、画像、zipアーカイブ、リッチメディアコンテンツは、安全なマイクロVM内で自動的に隔離されます。

  パフォーマンスの維持。リモートレンダリングではなく、ネイティブアプリケーションがマイクロVM内で実行されるので、使い慣れたユーザーエクスペリエンス、スピード、パフォーマンスを提供します。

  従業員の生産性向上。ユーザーに遅く、制限があり、手間がかかる階層型ネットワークセキュリティの利用を強いる必要はありません。どのようなネットワ

ークでも、侵害のリスクなくユーザーを保護します。

- **未分類のサイトへの安全なアクセス。**

  現在では多くのウェブサイトが暗号化されていますが、マルウェアは暗号や多層防御を回避して侵入する方法を見つけ出しています。また分類によるフィルタリングも、分類が不正確、不完全、時代遅れであるために役に立たないことが多くあります。
  仮想化ベースのセキュリティは、ユーザーをマルウェアから確実に保護し、制限なく閲覧できるようにする唯一の方法です。

  あらゆるウェブサイトのコンテンツにアクセス。
  Bromiumは、あらゆるものが悪意のあるものである可能性を想定しており、各ファイル、タブ、ドキュメントを独自の安全なコンテナで開きます。

  任意のURLを参照。従業員は分類されていないウェブサイトへの訪問を、禁止されることなく続けることができ、アプリケーション隔離により保護されます。

  ITの負担を軽減。分類のための面倒な手動によるサイトの例外処理レビューをなくし、セキュリティ管理者を解放します。

- **防衛グレードのセキュリティ - 完全な保護に対応。**

  Bromiumアプリケーション隔離は、他のエンドポイントセキュリティソリューションが失敗した場合の最後の防御ラインです。最も脆弱な経路である電子メールの添付ファイル、実行ファイル、電子メールの

リンク、およびブラウザのダウンロードを保護します。仮想化ベースのセキュリティは、国家レベルの攻撃やゼロデイ攻撃を阻止する唯一のソリューションです。

マルウェアを封じ込め。自動的かつ瞬時に、タスクとコンテンツを安全で使い捨てのマイクロVMに隔離します。

ホストを保護。マルウェアは隔離から逃れることができず、オンラインとオフラインの双方のユーザーを保護します。

心配不要。検知の必要がないため、これまでに知られていなかった脅威も完全に隔離され封じ込められます。

もしこれがあなたの興味をそそるものであれば、Bromium（現HP）に連絡してください。今が、NSA（国家安全保障局）のアドバイスを信じて、アプリケーション隔離を真剣に検討する時かもしれません。