
# ソーシャルメディア・プラットフォームとサイバー犯罪経済

*Into The Web of Profit* の第二章

犯罪学上級講師
Michael McGuire博士
Surrey大学

Sponsored by Bromium

Bromium®

## 序文

**GREGORY WEBB**
CEO of Bromium

我々がMcGuire博士と一緒に仕事を始めたとき、サイバー犯罪が今日の世界に与えている社会的影響に焦点を当てたかったのです。彼の調査結果は驚くべきものでした。オリジナルの”Into the Web of Profit”レポートでは、サイバー犯罪経済は毎年1.5兆ドルの収入を生み出しており、その資金の一部は人身売買やテロなどの伝統的な犯罪に再流用されていることが示されていました。レポートの中で最も興味深い成果の一つは、サイバーを利用した犯罪の新たな形態である「プラットフォーム犯罪」の存在を明らかにしたことです。プラットフォーム犯罪は、UberやAmazonなどが普及させた、データを主要な商品とする破壊的なプラットフォームベースのビジネスモデルを反映しています。その結果は衝撃的であり、今日でも政府、法執行機関、ビジネスの中で議論されています。そのため、さらなる調査が必要だと感じました。

この第二章では、サイバー犯罪や他の形態の犯罪を可能にするための人気のあるソーシャルメディア・プラットフォームの役割を調査しながら、クリア・ウェブを詳しく見ていきます。その結果、この問題はおそらく私たちが考えていた以上に深刻であり、法執行機関や政府だけでなく、個人や企業にも警鐘を鳴らすべきであることがわかりました。

ソーシャルメディアは、しばらく前から、企業のセキュリティにとって厄介な存在となっています。最大で 5 社に 1 社がソーシャルメディアに由来するマルウェアに感染しており、8 社に 1 社がソーシャルメディアに誘導されたサイバー攻撃の結果としてセキュリティ侵害を経験しています。初期の頃は、企業はその使用を禁止しようとしていましたが、ソーシャルメディアは企業にとって、特にマーケティングと人事のための強力なツールとなっており、その使用を防止することは現実的ではありません。

このレポートは、ソーシャルメディアが企業の防御における巨大な盲点であることを示しています。ソーシャルメディアは、巨大なユーザーベースでの迅速な感染を可能にしているだけでなく、自称ハッカーが攻撃に必要なツールやサービスを簡単に入手できるようにしています。率直に言って、心配です。企業システムへのこのバックドア・アクセスは、顧客データとビジネスIPを日常的に危険にさらしています。そして、現時点では、企業も個人もそれに対処するための準備ができていません。

このレポートを読むことで、すべてのビジネスは自問自答すべきでです。ソーシャルメディアを利用した攻撃から自分の組織をどのように守ればいいのか？私の3つの重要なポイントは以下の通りです。

1. ソーシャルメディア・プラットフォームは、ハッカーが企業に侵入するためのトロイの木馬として利用されています。サイバー犯罪者は、簡単なハッキングを利用して世界中の何百万人ものユーザーに、ほんの少しの努力でアクセスすることができます：事実上、ソーシャルメディアはマルウェアの世界的な流通センターです。現在、5人に1人の組織がソーシャルメディアを介して配布されたマルウェアに感染しています。このレポートのために実施された調査では、特定されたマルウェア感染の最大40%が不正広告に関連していることがわかりました。さらに 30% は悪意のあるプラグインやアプリが原因でした。従業員がサイバー犯罪者によって拡散された悪意のあるコンテンツを何気なくクリックすることで、知らず知らずのうちにトロイの木馬のような役割を果たし、ハッカーに高価値値資産へのバックドア・アクセスを与えています。
2. ソーシャルメディアは、クリプトマイニング・マルウェアの普及を可能にしています。この調査で得られたデータによると、クリプトマイニング・コードをホスティングしている世界のウェブサイトのトップ5のうち4つがソーシャルメディア・プラットフォームであることがわかっています。YouTubeの広告をクリックするような無害なことでも、クリプトマイニング・マルウェアがデバイスにインストールされ、デバイスをハイジャックしてクリプトカレントシーを採掘し、消費電力を増加させ、将来的にはクリプトジャッキングペイロードを使用してさらに悪質な目的のために使用する可能性があります。ハッカーの視点から見ると、このことの素晴らしさは、被害者の多くは自分が攻撃を受けたことに気づかないということで、ハッカーは長い間発見されずに済む可能性があることを意味しています。しかし、CPUやGPUへのパフォーマンス負荷の増加は、企業の機器の劣化を加速させ、ITリソースを枯渇させ、コンピューティングパワーに関連したコストの大幅な上昇を引き起こすことになります。

3. ソーシャルメディアは、攻撃を仕掛けようとする者が攻撃に必要なツールや専門知識を手に入れることをさらに容易にしています。レポートでは、ハッキングサービスやハッキングチュートリアル、エクスプロイトやボットネットの採用など、ハッキング活動を支援するために必要なツールが広く利用可能であることがわかりました。ソーシャルプラットフォームとダーク・ウェブの境界が曖昧になりつつあり、ツールやサービスが自由に利用できるようになったり、ダーク・ウェブ上のより広範なショッピング施設への入り口として機能したりしています。

結局のところ、ハッカーは弱点である従業員を知っており、信頼できるコネクションを介して従業員を操作する方法を知っています。サイバー犯罪者は、自分たちが捕まらない可能性が高いことを知っています。これは確率のゲームです。ソーシャルメディアは、マルウェアをクリックしてくれる人を見つける確率をサイバー犯罪者に有利なようにしています。問題の範囲を十分に理解し、封じ込めを含めた高度な機能を配備して自分たちの身を守ることで初めて、状況を変えることができます。今のままでは、ただのカモになってしまいます。

## 内容

Surrey大学犯罪学上級講師、Michael McGuire博士によるエグゼクティブ・サマリー
数字は語る
1.1 ソーシャルメディア・プラットフォームとサイバー犯罪経済
1.2 ソーシャルメディア・プラットフォーム：サイバー犯罪者のターゲットとハッカー天国
1.3 マルウェア配布センターとしてのソーシャルメディア・プラットフォーム
2.1 ソーシャルメディア上での増幅・説得・伝染
3.1 ソーシャルメディアでよくある攻撃方法
3.2 特定のソーシャルプラットフォームにカスタマイズした攻撃
4.1 ソーシャルメディアユーザーとそれを雇用する企業に対する新たな脅威
- デジタル通貨と暗号通貨詐欺
- クリプトジャッキング
- 悪意のあるプロフィールを後押しするために偽の「いいね！」で信頼を買う

5.1 Crimeware-as-a-Service（わかりやすい範囲）
- エクスプロイト
- ボットネット
- ハッキングサービス
- データの売買と販売

5.2 伝統的な犯罪におけるソーシャルメディアの役割
- ミレニアル・マネーミュール募集
- 薬物
- 詐欺
- 暴力とヘイトクライム

6.1 リコメンデーション
6.2 クロージング

## エグゼクティブ・サマリー

**Michael McGuire博士**
Surrey大学
犯罪学上級講師

サイバー犯罪は立ち止まりません。ハッカーは最新のブラウザー、eコマースサイト、モバイルコンピューティングデバイスを悪用する新たな方法を見つけ出し、技術的、社会的なイノベーションから継続的に機会が生まれています。これはソーシャルメディアでも同様です。ソーシャルメディア・プラットフォームの力は、新しい方法でユーザーを結びつけ、交流のための新しい道を切り開く能力に基づいています。個人、企業、政府にとって、ソーシャルメディアは視聴者にリーチし、製品を宣伝し、コミュニティを育成するための新たな経路を促進します。

ソーシャルメディア・プラットフォームはサイバー犯罪者にとっても同様に魅力的です。しかし、ソーシャルメディアで遭遇する犯罪リスクの範囲が拡大していることについては、まだ十分な研究がなされていないのが現状です。本レポートでは、ソーシャルメディア・プラットフォーム上でのマルウェアの共有、またはサービス、ツール、データの売買が、いかにしてサイバー犯罪の機会に貢献し、従来の犯罪を助長しているかを概説しています。また、これがユーザーや組織に与えている影響についてもハイライトし、どのようになっているかを示します。

- ソーシャルメディア・プラットフォームは、サイバー犯罪者にとって、クリア・ウェブ内での収益生成のための魅力的な機会を生み出しています。多くの場合、ダーク・ウェブのような伝統的な不正なチャネルを介して行うことができるのと同じくらい、またはそれ以上のことができます。
- ソーシャルメディアユーザーの膨大なユーザーベースと独自の信頼レベルが、個人、組織、国全体に感染するマルウェアの迅速かつ広範囲な普及を促進しています。
- ソーシャルメディアのユーザー間の相互作用という特性は、「連鎖的エクスプロイト」つまり、感染率を迅速かつシームレスに拡散させ、サイバー犯罪者に非常に効果的な攻撃手法のツールボックスを提供します。
- 攻撃は特定のプラットフォームに合わせて行われており、例えば、LinkedInの「知っていることを確認する」という特徴のようにソーシャルネットワークの特徴を武器にしてユーザーに展開されています。
- 正当なソーシャルメディア・プラットフォームとダーク・ウェブ上の同等のものとの間の線引きが曖昧になってきており、一部のプラットフォームはサイバー犯罪者のツールやサービスを宣伝するためのマーケティング・リソースとして使用されたり、ダーク・ウェブ上のより広範な施設のためのショップ・ウィンドウとして機能したりしています。
- サイバー犯罪者は、マネーロンダリングや薬物の販売を支援するためのミレニアム・マネーラバの募集など、より伝統的な形態のオフライン犯罪のためにソーシャルメディアのプラットフォームを悪用しています。

このレポートは、ソーシャルメディア・プラットフォーム上で行われている犯罪の規模を徹底的に理解し、Web of Profitを破壊するのに必要な洞察を提供することを目的としています。

## 数字は語る

利用可能な証拠から、犯罪におけるソーシャルメディア・プラットフォームの利用には、いくつかの顕著な傾向があることは明らかです。

- この調査では、ソーシャルメディアを利用した犯罪は、世界のサイバー犯罪経済に年間少なくとも**32.5億ドル**の収益を生んでいると計算されています。
- 本レポートのためにICCから入手したデータによると、米国では2015年から2017年の間にソーシャルメディアを利用した犯罪の報告が**300倍**以上に増加し、一方英国の警察のデータでは2013年から2018年の間にソーシャルメディアを利用した犯罪が**4倍**に増加したことが示されています。
- Web of Profit の研究者は、**13億人**以上のソーシャルメディア・ユーザーが過去5年以内にデータを侵害されており、2017年から2018年にかけてのデータの不正取引の**45 ~ 50%**がLinkedInやFacebookなどのソーシャルメディア・プラットフォームの侵害に関連している可能性があると計算しています。
- この調査ではソーシャルメディアのプラットフォームには、eコマース、メディア、カルチャー系のウェブサイトなどの同等のソースと比べて、更新や共有、アドオン、プラグインなどを介してユーザーにマルウェアを配信する方法が最大**20%**も含まれていることがわかりました。
- ソーシャルメディア感染の約**30 ~ 40%**は、感染した広告から来ています。
- ソーシャルメディア感染の少なくとも**20%**は、ソーシャルメディア・プラットフォームのアドオンやプラグインから発生します。
- ソーシャルメディアは、クリプトマイニング・ソフトウェアの重要な経路となっています。最も検索されたウェブサイトの**500件に1件**が、そのようなソフトウェアを扱っていると推定されており、ソーシャルメディアが**トップ5のうち4件**を占めています。
- 本レポートで検査したソーシャルメディア・プラットフォームの約**30 ~ 40%**が、何らかの形でハッキングサービスを提供しているアカウントを持っていました。
- 私たちの調査では、Facebook、Instagram、Twitter、その他いくつかのサイトでボットネットやブーター（DDoSサービス）のレンタルオファーが見つかりました。価格は安定しており、平均的な費用は1ヶ月で約10ドル、ライフタイムレンタルの場合は25ドルでした。
- ソーシャルメディアを活用した詐欺による犯罪収益は2017年から**60%**以上増加しています。
- CIFASの調査中に得られたデータによると、2016年以降、21歳以下のマネーラバを募集するためのソーシャルメディア・プラットフォームの利用が**36%**増加しています。

## 1.1 ソーシャルメディア・プラットフォームとサイバー犯罪経済

入手可能なほとんどの研究では、サイバー犯罪の価値を、そのコスト、つまり企業が侵害やデータ盗難に遭った場合の被害額に基づいて推定しようとしています。より良いアプローチは、サイバー犯罪活動から得られる収益に注目することでしょう。*'Into the Web of Profit'* で強調されているように、犯罪に従事する動機を説明し、犯罪活動を追跡する（そして、おそらく破壊する）のに役立ちます。
ダーク・ウェブ上の犯罪プラットフォームは直接的な収益源ですが、犯罪目的のための合法的なプラット フォームの広範な利用は、さらなる収益源を提供します。これは、本レポートで検討されているソーシャルメディア・プラットフォームについての重要な 疑問を提起しています。彼らはこのサイバー犯罪経済にどの程度の貢献をしているのでしょうか？特に、可能な限り保守的にして、私たちが知っていると思っていることではなく、私たちが知っていることだけに基づくことによって、暫定的ではありますが、根拠のある推定を行うことができます。わずか４つの指標を用いて、以下のような推定値を導き出すことができました[1]。
この調査の一環として算出された数値は、ソーシャルメディア・プラットフォームが少なくとも世界のサイバー犯罪経済に年間**32.5億ドル**の貢献をしていることを示しました。これは以下の分野に基づいています。

> *ダーク・ウェブ上の犯罪プラットフォームは直接的な収益源ですが、犯罪目的のための合法的なプラット フォームの広範な利用は、さらなる収益源を提供する。*

- **違法な医薬品販売（処方箋薬など）- 19億ドル**
- **窃盗データの売上高 - 6億3,000万 ドル**
- **金融詐欺 - 2億9,000万 ドル**
- **クリプトマイニング・マルウェア - 2億5000万 ドル**
- **ロマンス/デート詐欺 - 1億3800万 ドル**

> *情報経済では、データが商品交換の最新の形態となっている。*

しかしながら、これらの「直接」収入源に加えて、サイバー犯罪者は、マルウェアやハッキングサービス、偽ブランドを 含む知的著作権の窃盗、コカイン、MDMA、ヘロインなどの違法薬物販売など、他にも多くの方法で ソーシャルメディアを利用して収益を得ています。これらの活動からの収益は、利用可能なデータが信頼性の高い推論を行うのに十分な堅牢性を持っていないため、上記の推定には含まれていません。しかし、ソーシャルメディアからの犯罪収益の合計レベルはもっと高くなる可能性が高いと考えても良いでしょう。

## 1.2 ソーシャルメディア・プラットフォーム：サイバー犯罪者のターゲットとハッカー天国

情報経済では、データが商品交換の最新の形態となっています。ソーシャルメディア・プラットフォームは、個人データの取得に絶え間なく焦点を当てているため、サイバー犯罪者にとって非常に魅力的なデータバンクとなっています。ユーザーベースの大きさ、交換されたデータの種類、あるいはユーザーの信頼度の高さに関わらず、ソーシャルメディア・プラットフォームは、データを求めるハッカーにとって新たな「人気のある」ターゲットの一つとなっています。

ソーシャルメディアのユーザーとそのデータがサイバー犯罪者に悪用される重要な資源になりつつあるという証拠が増えてきています。実際、この調査では過去5年間に**13億**[2]以上のソーシャルメディア・ユーザーがデータを侵害されており、オンラインで取引されているデータの**45 ~ 50%**は、ソーシャルメディアのデータ侵害によって得られたデータに関連している可能性があることがわかりました。[3]

---

[1] 計算の詳細は、本報告書の Apendix1、方法論の項に記載されています。
[2] 計算の詳細は、本報告書の Apendix1、方法論の項に記載されています。
[3] この発見は、2018年上半期にソーシャルメディアの侵害が総侵害件数の56%以上を占めていたことを示唆している公開データ侵害の世界的なデータベースであるGemaltos Breach Level Index内の指標によって裏付けられています。Cambridge Analytica-Facebookの事件を含む6件のソーシャルメディア侵害が、何億件ものデータが盗まれた原因となっていることは、ソーシャルメディアのデータ盗難の影響がどれほど深刻であるかを示しています。

*調査によると従業員は週に3時間以上もソーシャルメディアサイトを閲覧している。*

ソーシャルメディア・プラットフォームは、ハッカーが選択したターゲットに到達したり調査したりするための簡単なルートを提供しています。FBIのデータによると、2015年から2017年の間にソーシャルメディアが関与する犯罪の報告が300倍に増加していることが示唆されています[4]。この顕著な増加は、被害者がその手の犯罪を報告する可能性が高いことや、法執行機関の分類方法に一因であることは間違いありません。とはいえ、著しい情報が他でも裏付けられており、より地域に密着した警察のデータでも、ソーシャルメディアを利用した犯罪が2013年から2018年の間に**4倍に増加**したと報告されています[5]。

企業にとって憂慮すべきことに、調査によると従業員は週に3時間以上もソーシャルメディアサイトを閲覧しています。同じ調査では、どのように使用すべきかについてのポリシーがあるかどうかに関わらず、最大77%の従業員が職場でソーシャルメディアを使用していると答えています。[6] ビジネス自体がソーシャルメディア・プラットフォームへの依存度の高まりに関係しています。約 73%の企業が仕事の目的で Facebook のアカウントを使用しており、64%が LinkedIn を使用し、56%が Twitter を使用していると推定されています。[7] 5社に1社以上の企業が、ソーシャルメディア・プラットフォームと直接接触した結果、マルウェアに感染しているのは当然のことです。[8]

## 1.3 マルウェア配布センターとしてのソーシャルメディア・プラットフォーム

世界中のソーシャルメディア・ユーザーの数の多さは、ソーシャルメディア・プラットフォームが個人と組織の両方にとって、オンライン上でのマルウェア感染の主要な感染源の一つとなっていることを意味します。問題は拡大の一途をたどっています。ソーシャルメディア・プラットフォームには、eコマース、メディア、文化的指向のウェブサイトなどの同等のソースに比べて、潜在的なマルウェアの配信手段が最大20%も多く含まれています。[9]これは、一般的に画像、動画、広告、プラグインの数が多いためです。Facebook の詐欺のようなプラットフォーム固有の脅威は、企業ネットワークを侵害する第一の方法として評価されており、[10]いくつかの情報源は、8社に1社がソーシャルメディア経由のサイバー攻撃によるセキュリティ侵害を経験していると主張しています。[11]

*8社に1社がソーシャルメディア経由のサイバー攻撃によるセキュリティ侵害を経験している。*

マルウェアの拡散は、ソーシャルメディアの大規模なユーザー基盤だけでなく、疑わしいリンクをクリックしたときにユーザーが感じる信頼感の高さや、「連鎖的エクスプロイト」という構造的な現象によっても促進されています。[12] これによって、ソーシャルネットワーク上での相互作用の性質が、感染の迅速かつシームレスな拡散を促進します。さらに、ソーシャルメディアがユーザーのプロフィールを複数のプラットフォームで共有できるようにする傾向が、問題をより複雑にしているのです。この種の典型的な例としては、Facebookメッセンジャー上のフィッシングリンクを利用して、被害者をYouTubeに似たサイトに誘導するというものがあります。アップデートをダウンロードしたユーザーは、パスワードなどを盗むことができる高度なマルウェアに感染していました。[13]

---

[4] （FBI 2015年-2017年）。2015年には、ソーシャルメディアがサイバー犯罪を助長する媒体またはツールとして使用されていることに関する報告が58件寄せられました。2017年にはその数は19,986件となりました。

[5] このデータでは、Facebookが最も多くの犯罪関与の報告を受けており、次のプラットフォームの約5倍の数の犯罪に関与していることがわかりました。Snapchatは、報告された犯罪の増加率が最も高いプラットフォームの1つであり、次に高いプラットフォームであるInstagramよりも1,000%以上の高さです。（Reynolds 2018年）

[6] Bean（2017年）、Pew（2016年）

[7] Osterman （2016年）

[8] Cimpanu, 2018年

[9] 10,000種類のマルウェア感染タイプとその感染源の分析から外挿したもの

[10] Cisco （2015年）

[11] Hayes （2016年）

[12] Aditya and Enbody （2011年）

[13] Palmer （2018年）

## 2.1 増幅・説得・伝染

連続的エクスプロイトとサイバー犯罪を可能にするその力は、サイバー犯罪者が学習しているソーシャルメディアの3つの重要な特徴と関連付けることができます。

### 1. 増幅

アメリカの成人の3分の2がソーシャルメディアからニュースを得ている世界では[14]、ソーシャル・プラット フォームは、ソーシャル・エンジニアリング戦略を広めるための明白な踏み台となっています。実際、商品であれ、フェイクニュースであれ、政治的なメッセージであれ、ほとんど何でもソーシャルメディアのプラット フォームに載せることで、そのリーチは増幅され、しばしば個人の影響力のネットワークを指数関数的に拡大させま す。

*「サイバー犯罪者はソーシャルメディアの増幅力を利用して、被害者を巻き込む方法を開発することに熟達しています。」*

### 2. 説得

「大きな声で話す」ことは、より多くの耳に届くかもしれませんが、メッセージが伝わることを保証するものではありません。その性質上、ソーシャルメディアは人気が非常に価値のある通貨である領域です。マーケティング担当者は現在、増幅の2つのバージョン、「リーチ」（ページを閲覧したユニークな個人の数）と「インプレッション」（コンテンツが人々に表示された回数の合計）を日常的に区別しています。しかし、ソーシャルメディアキャンペーンは「エンゲージメント」、つまり個人がコンテンツに反応する度合いにも関心を持っています。例えば、「いいね！」をしたり、コメントをしたり、さらにコンテンツを投稿したりすることです。サイバー犯罪者はこれらの教訓を学び、ソーシャルメディアの増幅力を利用して、被害者を巻き込む方法を開発することに熟達しています、つまり、被害者の注意を引きつけ、エクスプロイトをより受けやすくしています。実際、彼らは単なるエンゲージメントを説得に変えることに成功することが多いため、エンゲージメントの分野ではマーケターよりもはるかに優れているように見えます。例えば、被害者が「面白い」アプリを見るようにするだけでなく、そのアプリをフォローしたり、コンテンツをダウンロードしたりするように説得しているということです。

*「成功したランサムウェア攻撃の最大70%は、電子メールやソーシャルメディア・プラットフォームを介したフィッシング攻撃由来でした。」*

ソーシャルメディア・ユーザーは、説得に非常に敏感であるようで、最近の心理学的研究では、Facebookのようなソーシャルメディア・プラットフォームの常習的なユーザーは、頻度の低いユーザーや非ユーザーよりも、フィッシングやスパムベースの感染につながるリンクをクリックする可能性が最大40%高いことが示唆されています。また、常習的なユーザーは、ソーシャルメディアサイトへの訪問頻度の低いユーザーや非ユーザーと比較して、友人ベースの攻撃（「友人」からのメッセージに含まれるリンクをクリックすること）に反応しがちです。[15]

説得は、エンゲージメントよりもサイバー犯罪者にとって明らかに利益です。それは、投票の意図を変更することやマネー・ミュールとして行動することに同意することなど全てのことで、プラットフォームの枠を超えて行動や意見を方向付けることができるからです。

### 3. 伝染

突如として大流行したアイデアやトレンドを論じる際に「バズる」という言葉がよく使われるようになりました。しかし、評価されるべきではありませんが、おそらくその起源はサイバー犯罪にあります。コンピュータ・ウイルスは、コンテンツが与えられた媒体を通じて、非常に急速に、多くの場合は指数関数的に拡散することを示す典型的な例です。現代のプラットフォームに焦点を当てたサイバー犯罪者が、増幅と説得のサイクルのある転換点に達すると、不正な試みからはるかに多くの利益を得ることができることを、マーケティング担当者と同じように認識していることは、驚くに値しません。

詐欺を、遍在するまで増幅することは、サイバー犯罪者にとって聖杯のようなものです。サイバー犯罪者は、収益を生み出す取り組みを強化する上で、ソーシャルメディアの伝染の可能性に気づいています。例えば、2017年に成功したランサムウェア攻撃の最大70%は、電子メールやソーシャルメディア・プラットフォームを介したフィッシング攻撃由来でした。ビジネスにとって憂慮すべきことは、これらのソーシャルメディアを利用したランサムウェア攻撃のほとんどは、企業ネットワークを標的としたものだったということです。[16]

[14] Pew （2017年）
[15] Halevi et al （2013年）、Vishwanath （2015年）
[16] Jay （2018年）

## 3.1 ソーシャルメディアでよくある攻撃方法

最もよく知られているサイバー詐欺の中には、伝染指向の戦略を含むものがあります。昔ながらの419詐欺のようなマスマーケティング詐欺は、スパムの大量配布と共にその一例です。最近では、特定の金融機関への嗜好を示す個人をターゲットにした偽の広告や金融関連のハッシュタグを使用した攻撃にソーシャルメディアが影響を受けやすいことが証明されています。

この研究の一環として特定された、ソーシャルメディアの生態系を悪用して感染を広める一般的な方法やテクニックには以下のものがあります。

**感染した広告** - ソーシャルメディアのマルウェアの**30～40%**は、感染した広告のクリックが原因で発生します。有名な例としては、クリックするとウイルスに感染する、InstagramやFacebookなどに掲載されているRay-BanのサングラスやNikeのシューズの広告が挙げられます。[17]

**プラグインとアプリ** - このレポートでは、ソーシャルメディア感染の少なくとも**30%**は、追加機能を提供すると主張するソーシャルメディアのプラグインから発生していることがわかりました。これらのプラグインには、ゲームや性格テストなどが含まれています。その量はプラットフォームにより大きく異なるります。例えば、Facebook上の感染の少なくとも**60%**はサイトからダウンロードされた悪意のあるサードパーティ製アプリから発生しています。

**友達からのニュース投稿、アップデート、写真** - 友達が何をしているのか、広い世界で何が起こっているのかなどの最新情報を受け取ることは、ソーシャルメディアの魅力の明らかな要素です。サイバー犯罪者は、友人からの投稿や更新がマルウェアを仕込んだり、個人情報にアクセスするために悪用できる可能性をいち早く察知しています。Facebookプラットフォーム上で友人や同僚の写真が広範囲に使用されていることで、もう一つのリスクが生じています。サイバー犯罪者はフォトタグ通知を利用して、ユーザーに添付ファイルを開くように説得し、マルウェアをダウンロードさせています。[18]

**おかしな写真やビデオ** - **犯罪者の説得の別の方法は、しばしばソーシャルメディアの投稿で発見された「おかしな」または面白いビデオへのリンクを利用しています。ソーシャルメディアの感染の約15%はこの方法によるもので、2015年には10万人以上のFacebookユーザーがわずか3日間でこの方法で感染しました。**[19]

**ドライブバイダウンロード** - これは、ユーザーが積極的にファイルを開いたり、コンテンツをインストールしたりしていなくても発生する可能性のあるマルウェアのダウンロードです。ソーシャルメディアの投稿で推奨されているウェブサイトを訪問するような一見無害な行為であっても、ウェブサイトがハイジャックされていて、マルウェアを含む別のアドレスにユーザーをリダイレクトさせる小さなコードが含まれている場合は危険です。ソーシャルメディア・プラットフォームを介してアクセスできるコンテンツが多岐にわたっているため、ユーザーは特にこのような攻撃に対して脆弱です。この調査のためにSANSから得られたデータによると、ドライブバイダウンロード攻撃は、現在ではサイバー犯罪者が組織を攻撃するために使用する方法の1つとなっており、ウェブベースの脆弱性を悪用する攻撃の約48%を占めています。[20]

**フィッシングとスピアフィッシング** - サイバー犯罪者がデータ取得のために偽のソーシャルメディアページを作成する「ソーシャルネットワーク・フィッシング」が増加しています。2018年には、ソーシャルネットワーク・フィッシングの**60%**が偽の**Facebook**サイトを経由して発生し、**20%**がロシアのソーシャルメディア・プラットフォームVKの偽サイトを経由し、約**13%**が偽の**LinkedIn**ページを経由して発生しています。ソーシャルメディア・フィッシングは、2017年には2倍近くに増加したと推定されており[21]、ソーシャルメディアのユーザーを説得して感染したリンクにアクセスさせるハッカーの能力は、タイムラインから取得した投稿やトピックの詳細をパーソナライズして、被害者に接続が本物であると信じ込ませるスピアフィッシングのテクニックによって大いに助けられています。最近の調査ではユーザーを説得してよりパーソナライズされたコンテンツをクリックさせる成功率は30～60%と言われています。[22]

[17] Krustev （2018年）
[8] Pesce et al （2012年）
[19] Ragan （2015年）
[20] SANS （2017年）
[21] Barker （2018年）
[22] Seymour & Tully （2016年）

## 3.2 特定のソーシャルプラットフォームにカスタマイズした攻撃

*"他人とのつながりを確認する偽メールを受け取ったLinkedInユーザーの最大68%がリンクをクリックすることが判明している。*

プラットフォームは、提供するサービスの種類だけでなく、そのデザインや機能性によっても区別することができます。サイバー犯罪者は、悪用する各プラットフォームの特定の機能に合わせて活動をカスタマイズすることに長けています。

- **Facebook**は、2017年のフィッシング攻撃の標的トップ3の1つを構成しており、明らかに犯罪者のリソースとなっていることが証明されています。つまり、個人情報を取得するためのサイロとして、ソーシャルメディアの増幅力をサイバー犯罪者が意識していることを明確に示しています。[23]
- **LinkedIn**は、自分の職業上のネットワークに他の人を追加する機能に基づいています。 これが、 サイバー犯罪者が悪用することを学んだ根本的な特徴です。偽の「あなたが知っていることを確認する」メールは、本物のメールとほとんど区別がつかず、マルウェアがダウンロードされる悪質なサイトにユーザーをリダイレクトすることがわかっています。このようなメールを受け取ったLinkedInユーザーの最大68%がリンクをクリックすることが判明しており、サイバー犯罪者は企業内の重要人物を特定し、ログイン情報の詳細などを取得することが可能になっています。[24] サイバー犯罪者は、LinkedInが1次、2次、3次の3つのレベルで人間関係をランク付けする方法を悪用することも得意としています。一次のコネクションは最も信頼できるものとして認識されているため、フィッシング攻撃やマルウェアの拡散に利用できる魅力的なツールとなっています。LinkedInが直接の社会的な知人ではなく、オンラインネットワーク上に構築された人脈に依存していることは、感染がより急速に広がることを可能にするさらなる要因となっています。[25]
- **WhatsApp**の音声メッセージング、リンクの共有、グループの形成などの能力は、独特な攻撃手法に適しています。例えば、WhatsApp のメッセージには、”WhatsApp Gold”と呼ばれるWhatsApp のプレミアム版へのアップグレードを提供するリンクが貼られていました。[26] この新しいプレミアムサービスでは、インスタントメッセージの削除や、WhatsApp の有名人ユーザーと直接話をする機会など、通常のユーザーにはない様々な機能が提供されます。これをダウンロードすると、会話の盗聴などユーザーの行動を監視するソフトウェアがインストールされていました。[27]
- **YouTube**動画はユーザーにリンクのクリックを提案あるいは要求することがあります。サイバー犯罪者はこの機能を悪用して、人気のあるゲームに関連した攻撃を仕掛けてきました。例えば、Fortniteのプレイヤーには無料のゲーム内通貨が提供されていましたが、提供されたリンクをクリックすると、ユーザーは外部サイトにリダイレクトされ、端末にされるマルウェアをダウンロードされました。[28]
- **Instagram**ユーザーの投稿へのコメントが、肥沃な不正収入源であることが証明されています。あるケースでは、Britney SpearsのInstagramページへのコメントが、サイバー犯罪グループTurlaのコマンド＆コントロールページにリダイレクトされていました。その後バックドア型のマルウェアがインストールされ、ユーザーの情報が収集されました。[29] 別の例では、Instagramの認証情報を盗むアプリが13個もGoogle Playで検出されました。これらのアプリは、フォロワーを管理したり、増やしたりするために設計されたように見えますが、Instagramの認証情報を取得することを目的としていました。認証情報が盗まれると、ハッカーはそれらを利用してアカウントからスパムや広告を送信することができますが、最大150万人のユーザーがアプリをインストールする可能性がありました。[30]

[23] Kaspersky （2018年）
[24] Boodai （2011年）
[25] Tsing （2018年）
[26] Action Fraud （2019年）
[27] Correa （2016年）
[28] https://www.polygon.com/2018/5/4/17307268/fornite-scams-youtube-free-v-bucks
[29] Matthews （2017年）
[30] Leyden （2017年）

## 4.1 ソーシャルメディアユーザーとそれを雇用する企業に対する新たな脅威

*ソーシャルメディア・プラットフォームは、デジタル通貨や暗号通貨詐欺のビジネスにとってますます重要になってきている*

*2017年から2018年にかけてクリプトジャッキングの影響を受けた企業の数が2倍に増加している。*

### デジタル通貨および暗号通貨詐欺

ソーシャルメディア・プラットフォームは、デジタル通貨や暗号通貨詐欺のビジネスにおいてますます重要性を増しています。今回の調査で英国警察から入手したデータによると、2018年6月から7月にかけて、サイバー犯罪者がソーシャルメディア・プラットフォームを利用して、暗号通貨取引やマイニングに関わる詐欺的な投資を宣伝する事件が203件発生していたことが判明しました。被害者は約200万ポンド（250万ドル）の損失を被ったと推定されています。[31] 2018年には、イニシャル・コイン・オファリング（ICO）の少なくとも80%が詐欺であり、[32] ソーシャルメディアはこれらを可能にする上で重要な役割を果たしました。例えば暗号通貨詐欺を推し進める少なくとも15,000のボットが最近Twitterで検知されています。[33]

別の例としては、英国の小売業者Matalanのような信頼できる検証済みのアカウントを乗っ取るというものがあり、アカウントがElon Muskの個人プロフィールに似せて変更されました。その後、偽の”Elon Musk”アカウントからBitcoinの「報酬」を約束して少額のBitcoin寄付を求めるツイートが送信されました。この詐欺は、寄付後に報酬を受け取ったという他の「信頼できるアカウント」からの返信ツイートを含むことで、より信憑性を高めました。言うまでもなく、寄付をした人は見返りに何も受け取っていません。[34]

### クリプトジャッキング

「クリプトジャッキング」や「クリプトマイニング」マルウェアの台頭は、ソーシャルメディアのユーザーや企業にとって高まる懸念です。クリプトマイニングによって収益を生み出すプロセスでは、新しい暗号通貨を生成するためにコンピュータが複雑な計算を実行する必要がありますが、このプロセスには多くのメモリと処理時間が必要です。犯罪者は、タスクを実行するために他のコンピュータをハイジャックし、それによって何も知らない第三者に計算コストを転嫁します。

2017年以降、世界的に不正な暗号通貨マイニングマルウェアの検知数が400 ~ 600%増加しています。[35] 今回の調査で検知された不正な暗号通貨のマルウェアの大部分は、Monero（約75 ~ 80%）とBitcoin（10%）に向けられているようです。[36]

これは、サイバー犯罪者がソーシャルメディアを利用したクリプトマイニング・マルウェアやクリプトジャック攻撃によって、年間2億5千万ドル近くを稼いでいる可能性があることを意味しています。[37]

必然的に、クリプトマイニング・マルウェアは、ソーシャルメディア・プラットフォームとそのユーザーに顕著な影響を与えました。最も検索されたウェブサイトのうち、500中1サイトまでがクリプトジャッキング・ソフトウェアを含んでいると推定されており、[38] そのトップのうち5の4サイト、トップ20のうち11サイトがソーシャルメディアとなっています。[39]

アプリケーション、広告、リンクが主な配信メカニズムとなっていますが、特にFacebookメッセンジャーの利用は、Digmineのような新しい系統の拡散を助けるのに役立っています。クリプトジャッキング・マルウェアは2018年にYouTubeでも発見され、Moneroを「採掘」するために被害者のCPU時間の80%以上を消費していました。[40]

クリプトジャッキング・マルウェアの多くは、Coinhiveというオープンソースのマイニングコードに由来しています。現在、Facebook、Instagram、Pinterest、LinkedInのソーシャルメディア・ユーザーは、このコードに基づくプラグインを含むリンクにさらされています。

---

[31] Godshall （2018年）
[32] Alexandre （2018年）
[33] Francis （2018年）
[34] プラットフォーム上でホストされている広告を取り除けなかった結果、Facebookに対して法的措置が取られ、その後Bitcoinの広告がFacebook上で禁止されました。
[35] CTA （2018年）、 McAfee （2018年）
[36] 方法論を参照。CTA（2018年）の類似の調査結果と比較
[37] See methodology.
[38] Musch et al （2017年）
[39] DN Pedia （2018年）
[40] BBC （2018年）

*ソーシャルメディアのインフルエンサーの最大25%が、偽のフォロワーやその他の誤解を招くような影響力の指標を用いた準犯罪的な操作に関与している可能性がある。*

企業にとって、この種のマルウェアは、パフォーマンスの向上によってITリソースを消耗させ、重要資産の劣化を加速させるため、非常に大きなコストがかかる可能性があります。調査によると、クリプトジャッキングの影響を受ける企業の数は2017年から2018年にかけて倍増しており、VvivaやTeslaなどの大企業でさえ被害に遭っています。[41]

推定収益は、単一のプログラムでは大したものではありません（調査によると、1日5ドル程度）。しかし、増幅と伝染の戦略が機能し、十分な数のクリプトジャッキング・ソフトウェアがソーシャルメディアを通じて被害者のシステムに配信されれば、かなりの収益を生み出すことができます。

## 悪意のあるプロフィールを後押しするために偽の「いいね！」で信頼を買う

人気と影響力がソーシャルメディア・プラットフォームの説得の通貨であるならば、その指標がオンライン経済のお金に変換されるのは時間の問題でした。ソーシャルメディア上での人気を示す重要な指標（Facebookの「いいね！」機能やLinkedInの「つながり」など）が、新しい種類の犯罪あるいは少なくとも半合法的な機会を産み、収益を煽るために利用されています。これにより、アカウントは実際よりもはるかに影響力があるように見えたり、信用できるように見えたりします。


例としては、以下のようなものがあります。

- 現在、インフルエンサーの最大25%が、偽のフォロワーやその他の誤解を招くような影響力の指標を用いた準犯罪的な操作に関与している可能性があります。あるイギリスのファッション・インフルエンサー（1投稿につき1,000ポンドの報酬を得ていた）の例では、活動の96%は架空のものであり、ボットによって仲介されていたことがわかりました。[42]
- 同様に、#sponsoredや#adのようなハッシュタグが使われた1日の投稿を分析したところ、50%以上の偽のエンゲージメントが見つかり、スポンサー付き投稿のコメントの約40%にボットが関与している可能性が高いことがわかりました。[43]
- Ritz-Carltonのような大手ブランドは、偽物であることが判明したインフルエンサー戦略によって、最大で72%の人にリーチした可能性があります。[44]

*ソーシャルメディアの「いいね！」はダークウェブサイトの広い範囲で購入でき、クレジットカード番号よりも高価で取引されている。*

「いいね！」の取引が始まっていますが、これは密かに、そして平然と行われています。このプロジェクトのために行われた調査では、「いいね！」はダークウェブサイトの広い範囲で購入でき、クレジットカード番号よりも高価で取引されていることがわかりました。価格は、Facebookの「いいね！」で10ドルから20ドル、LinkedInの「いいね！」で25ドルからでした。おそらくサイバー犯罪者にとってより便利なのは、LinkedInの偽の「つながり」を購入できることであり、価格は100「つながり」で30ドルからとなっています。オンラインで簡単にアクセスできる”Getsomelikes”や”Ibuyfans.com”のような準合法的なサイトがあり、「いいね！」や「フォロワー」、「つながり」などの様々なパッケージを提供しています。これらは多くの場合、信憑性を追加するために実際のアカウントから来ています。このようなサイトでは、競合割引、顧客サービスとサポート、ビジネスアドバイスや追跡機を提供しています。

このように、サイバー犯罪者を含め、誰でも簡単に影響力を買うことができ、彼らがより信用され、信頼されているように見せることができ、マルウェアの配布や従業員やユーザーを詐欺に利用することがはるかに簡単になります。

---

[41]Redlock （2018年）
[42]Greer （2016年）
[43] Faull （2018年）
[44]Faull （2018年）

## 5.1 Crimeware-as-a-Service（わかりやすい範囲）

サイバー犯罪経済を牽引する合法的なプラットフォームと非合法的なプラットフォームの曖昧さを確認したこの研究の顕著な発見は、ソーシャルメディアのプラットフォーム上で利用可能なクライムウェアや「サービスとしてのサイバー犯罪（Cybercrime as a Service）」と呼ばれるツールやスキルの多さです。いくつかのケースでは、ツールが公然と大胆に提供されていることが判明しました。他のケースでは、プラットフォームは、商品やサービスのための一種のマーケティングの「入口」として機能し、ダーク・ウェブ上のより広範なショッピング機能へのリンクを提供していました。

現在利用可能なサイバー犯罪ツールの数が非常に多いことを考慮し、本調査では、4つの主要なツールや商品、すなわち*エクスプロイト*、*ボットネット*、*ハッキングサービス*、*盗難データ*に焦点を当てて検索、観察、購入の試みを行いました。実施された検索のうち、最大30%でサイバーツールが容易に入手できるという明確な証拠が得られました。サイバー犯罪ツールを利用することで、ハッカーが攻撃を開始するために必要な機器やサービスを簡単に入手できるようになるため、これは組織にとって大きな懸念材料となるでしょう。

*“サイバー犯罪ツールを利用することで、ハッカーが攻撃を開始するために必要な機器やサービスを簡単に入手できるようになる。*

### エクスプロイト

エクスプロイトを発見すること自体は違法ではありません。実際、影響を受ける可能性のあるソフトウェア会社や関連企業から報酬を得られることも多々あります。[45] しかし、犯罪に使用されることを知っていながら販売した場合、共犯者として告発される可能性があります。ここでの法的曖昧さは、合法性と犯罪性の境界線上にあるエクスプロイトの取引のグレーな経済を生んでいます。以下のアカウントを含む、ソーシャルメディアのプラットフォーム上のいくつかのサイトでは、公然とエクスプロイトを販売していることが判明しました。


- **Injector exploit database** - Facebookで簡単にアクセスできるエクスプロイトの取引や学習の機会を提供するアカウントです。このサイトには96,000人以上のフォロワーがいて、Twitterでも宣伝しています。
- **Exploit Packs** - 4,000人以上のフォロワーを持つこのアカウントには、38,000以上のエクスプロイトのフルセットが含まれていることを保証しています。

このようなアカウントは、「専門的なペネトレーションテストの実行と実施」を目的とした製品を提供することで、正当性を伝えているように見えることがよくあります。しかしながら、ログイン詳細を超えてエクスプロイトの詳細を取得するための障壁がないことを考えると、このようなツールは潜在的なハッカーに魅力的な「ハウツーガイド」を提供していることは明らかです。

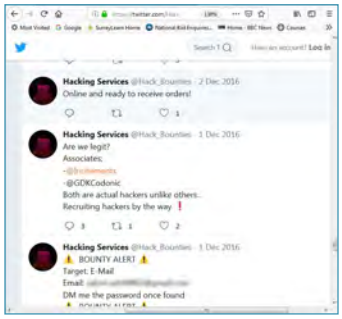
### ボットネット

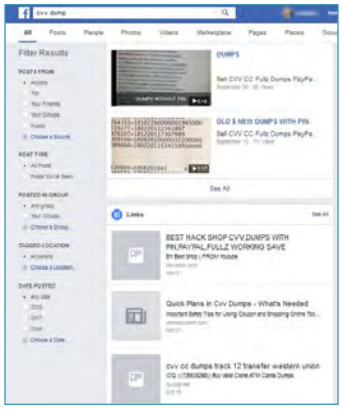
ボットネットのレンタルは、ほとんどのソーシャルメディア・プラットフォームで容易に行えるようになっています。例えば、YouTubeでは、単純なテーマ別検索で200以上の結果が出てきて、ボットネットを購入あるいはレンタルすることができました。

ボットネットやブーター（Booter）のレンタルは、調査のためにサンプリングしたFacebookやInstagram、Twitterなどのサイトでも見られました。価格はかなり安定しており、フルサービスパッケージ（チュートリアル、テクニカルサポート、その他アドオンなどを含む）のボットネットであれば月10ドル前後、無制限のライフタイム・レンタルであれば25ドル前後が平均的なコストとなっていました。サービスの宣伝方法は、各プラットフォームの形式によって様々でした。

---

[45]企業は、脆弱性を発見した研究者やホワイトハットに報酬を支払っていますが、その報酬の額は、そのソフトウェアの欠陥がどれだけ複雑で危険なものであるかによって異なります。そのため、悪意のある分野に焦点を当てるために、このようなエクスプロイト・ハンティングは除外しています。


### ハッキングサービス

調査したソーシャルメディアサイトの約30 ~ 40%が何らかの形のハッキングサービスを提供していました。ほとんどの場合、「倫理的」なハッキングサービスが強調されていましたが、それを明白に確認する方法はありませんでした。調査中に発見された例としては、ウェブサイトをハッキングするためのツール、ハッカーのレンタル、ハッキング・チュートリアルなどがあります。

クレジットカードのハッキングサービスなど、よりあからさまな犯罪行為が行われているアカウントもありました。しかしながら、検索を繰り返すと、これらのアカウントは、自らあるいは法執行機関やソーシャルメディアのプラットフォームが急速に介入したために、急いでに閉鎖しているようにでした。
Twitterでは、ハッキングサービスを利用できるようなアカウントへのアクセスは、少し手間がかかりました。しかし、根気強く続けることで、合法的なものであれ、そうでないものであれ、ハッキングサービスを得ることができるアカウントがいくつか見つかりました。

### データの取引と販売

アカウントの乗っ取りや金銭的な利益を得るために盗まれたデータを取引することは、より明確な犯罪性を伴います。最も顕著なのは、またもや「灰色の経済」バージョンで、クレジットカード番号を販売するために広告を出す際に、盗まれたことを示唆しないというものです。購入者が「盗まれていない」カードの詳細にアクセスできるようにするサービスを見つけることはよくあることです。その際、この種にサイトでは購入者が自分の詳細を開示することなく、カード情報へのアクセスを可能にする代理人としてアクセスすることができます。このような投稿や広告の多くには、次のような免責事項が記載されています

> ***免責事項***：*カードは教育的目的にのみ使用ください。人を騙したり詐欺する目的で使用しないでください。それは法律で罰せられる犯罪で、利用者は単独で責任を負うことになります。*

広告されているカードデータの中には、クリックされるとマルウェアのダウンロードを開始するものもあります。昔からFacebook上のカードダンプやCVV番号を広告する行為が知られており、そのようなアカウントは常にモデレーターによってテイクダウンされていますが、多数のページが、いまだにFacebookやTwitte上で動作しています。また、いくつかのプラットフォームで提供されているカードの「チュートリアル」もあります。

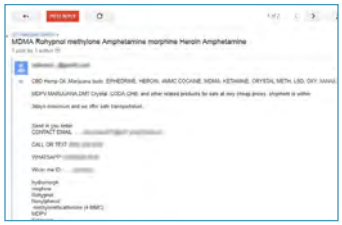
欧米のソーシャルメディアサイトとは対照的に、中国のソーシャルメディアでは、カードデータやその他の個人情報の販売は、はるかにオープンで大胆に行われているようです。最近の調査では、個人データの売買を中心とした中国のサイト”QQ”や”Tieba”では、30以上のユーザーグループが情報を提供していることがわかりました。そのような情報の価格は、10 万件のデータレコードあたり 300 元（43.64 ドル）から、より本物であることが確認されている場合は 2800 元までとなっています。[46]

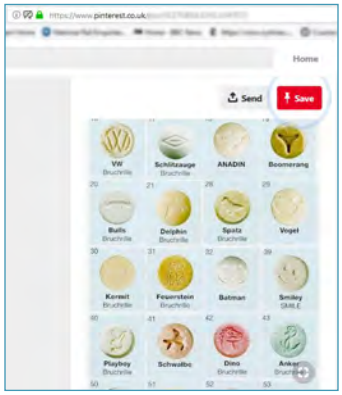
## 5.2 伝統的な犯罪におけるソーシャルメディアの役割

ソーシャルメディアの不正使用はサイバー犯罪に限定されていません。より多くの「伝統的な」犯罪活動が、今ではソーシャルメディア・プラットフォームの開放性とリーチを利用しているようです。おそらく、最も明白でよく知られている例は、薬物取引と流通のためのソーシャルメディア・プラットフォームの使用です。この研究は、他の活動を含む繁栄した犯罪の生態系も発見しました。

**ミレニアル・マネーミュール募集** – ソーシャルメディアは一種のリクルートセンターとしての役割を果たしており、必要としているクライアントと利用可能な労働力を簡単に結びつけています。「短期間で大量のお金を稼ぐ」機会を強調するソーシャルメディア上の投稿、フィード、広告は、この募集プロセスの一部であり、意欲的な応募者には事欠きません。

[46] Reuters （2018年）


*「ソーシャルメディアによって可能になった詐欺による犯罪収益が2017年から60%以上増加している。」*

ソーシャルメディアを介したマネーロンダリングは、通常は犯罪に関与しない個人、特に若いミレニアル世代を引き込んでいます。今回の調査でCIFASが入手したデータによると、英国には21歳未満の個人が所有するマネーミュール口座が8,500件もある可能性があることが示唆されています。14歳の個人のミュールアカウントが発見されました。2016年以降、21歳未満のマネーラバの募集が36%増加しており、増加傾向にあるように見えますが、そのほとんどはソーシャルメディアを介して行われています。[47] このことは、10代の若者がオンライン・マネーミュール取引で最も急速に成長している年齢層である可能性を示唆しています。

**薬物** – オンラインの薬物市場の通常の認識は、ダークウェブサイトやSilk Roadのような専門市場を介して行われている、はっきりとしない秘密の事件ということでしょう。しかし、ソーシャルメディアのプラットフォームのリーチは、もはやそうではないことを意味しています。

ソーシャルメディア・プラットフォームは、処方箋薬を提供する違法オンライン薬局を支援する新たな手段を提供しています。例えば、ある研究[48] では、Facebook上の医薬品関連コンテンツの最大17%に違法オンライン薬局の広告が含まれていることが示唆されています。TwitterやYouTube上の特定の医薬品に関する投稿の4分の1は、お客様の声として提示されています。

このプロジェクトの調査では、このようなプラットフォームで、オープンに堂々に売られている違法薬物の購入が驚くほど簡単であることも判明しました。個々の供給者の利益は、月平均5万ドルにもなります。[49] このような物質が入手できるプラットフォームには、以下のようなものがあります。

- **Twitter** - MDMA、アンフェタミン、コカイン、その他の薬物
- **Instagram** - MDMA、大麻、アヘン
- **Facebook** - 大麻、GHB、コカインをプライベートチャットやグループで販売
- **Google (Gropups)** - ヘロイン、GHB、MDMA、ケタミン
- **Pinterest -** エクスタシー

**詐欺** – トップブランドのソーシャルメディア・アカウントの最大 20%が「詐欺」であると推定されており、[50] 犯罪者はこれらのアカウントを、マルウェアの配布、ユーザー情報や好みに基づいたフィッシングメールの作成などのさらなるサイバー犯罪のために頻繁に利用しています。企業の役員は特に詐欺の標的となり、Facebookなど詐欺が最も蔓延しているソーシャルメディア・プラットフォームでは、心配なほどに高い可視性を持っています。最近の調査によると、オンライン上で存在感を示す役員のうち、61%がFacebookを利用しているのに対し、LinkedInを利用しているのは31%です。[51]

本レポートで調査したソーシャルメディアの投稿の約0.2%は、何らかの金融詐欺が関与しているようでした。[52] より広く外挿してみると、これは様々な種類の詐欺行為がソーシャルメディア全体で年間**2億9000万ドル**以上の収益を生み出していることを示しています。これは、ソーシャルメディアによって可能になった詐欺による犯罪収益が2017年から**60%**以上増加していることを示唆しており、2017年の調査では収益は（最高値で）約1億8000万ドルと推定されています。[53]

[46] Reuters （2018年）
[47] Keyworth （2018年）
[48] Tyrawski & DeAndrea （2015年）
[49] 他の調査（BBC 2017年）では、2 日以内に 3 万ドルの利益を上げることができると自慢しているサプライヤーもあり、同等の数字が出ています。
[50] Gwynn （2016年）
[51] CIFAS （2018年）
[52] この計算の詳細は、方法論のセクションに記載されています。
[53] Zerofox （2017年）

*出会い系詐欺をより信憑性の高いものにするために、Facebookサイトから個人情報や写真が盗まれることもよくある。*

オンライン・デート詐欺もまた、非常に儲かることが証明されている詐欺の一種で、アメリカだけでも2億3,000万ドル以上の被害が報告されていますが、[54] このような犯罪のうち報告されるのは15%以下です。このような詐欺は、小規模でニッチな、あるいは専門的な出会い系プラットフォームで行われることに加えて、犯罪者が主流のソーシャルメディアを標的にすることも多くなってきました。テキサス州のある女性は、犯罪者がFacebookに載せた彼女の信仰に関する情報を利用して彼女と仲良くなり偽の恋愛をしたことで、約200万円を失いました。[55] また、出会い系詐欺をより信憑性の高いものにするために、Facebookサイトから個人情報や写真が盗まれることもよくあります。

**暴力とヘイトクライム** – オンラインの世界は日常の暴力の現実から一歩離れているように見えますが、ソーシャルメディアの遍在性は、それらの犯罪を可能にする役割を果たしていることを意味します。例えば、少年ギャングがソーシャルメディアを利用して勧誘したり、対立するギャングを煽って暴力を振るったりすることが挙げられます。YouTubeやSnapchatなどに投稿された嘲笑いの動画は、攻撃性や喧嘩の増加と関連しており、時には死亡者も出ています。[56]

元空き巣犯の大多数（78%）が、Facebookのようなソーシャルメディア・プラットフォームを利用して、空き巣の標的となりそうな物件を狙っていることを示唆しています。[57] あるケースでは、ニューハンプシャー州の3人の男性がFacebookを使って18軒以上の家に強盗に入ったことを告白しています。[58]

[54] Brenoff （2017年）
[55] Brenoff （2017年）
[56] Marsh （2018年）
[57] Phillips （2016年）
[58] Irshad and Soomro （201年）

## 6.1 リコメンデーション

*組織は階層的なサイバーセキュリティ防御を含むソーシャルメディアに対する強固なサイバーセキュリティー・ポリシーを策定する必要がある。*

### ソーシャルメディア・プラットフォーム

- ソーシャルメディア企業は、プラットフォームを悪用するサイバー犯罪者の活動に対して、より積極的な姿勢で臨む必要があります。ユーザーとそのデータを保護するためには、このような行為を厳しく取り締まる必要があります。これには、サイバー犯罪者によるアカウント乗っ取りを困難にするTwitterの認証済みバッチなどが含まれます。
- また、ソーシャルメディア・プラットフォームがサイバー犯罪の行為から利益を得ていないことを確認するために、より多くのことをしなければなりません。感染した広告はすべて有料であるため、Facebook、Twitter、Instagram、Snapchatなどがユーザーの搾取から利益を得ている可能性があります。代わりに、ソーシャルメディア・プラットフォームは、これらの収益を止めるか、サイバー犯罪や詐欺と戦う慈善団体に寄付することを目指すべきです。
- プロファイルの影響力を弱めるために、ソーシャルメディアのプラットフォームは、偽のフォロワー、「いいね！」やリツイートを取り締まる必要があります。このような偽のフォロワーは、権威のオーラを醸し出し、その結果、ユーザーがリンクをクリックすることが多くなります。

### エンタープライズ

- 企業は、ソーシャルメディアが組織内でどのように使われているかをよりよく理解し、簡単に悪用される企業へのバックドアとして扱う必要があります。これには、どのプラットフォームが組織に最も効果的に利益をもたらすかだけでなく、最大のリスクをもたらすプラットフォームについても明確にすることが含まれます。
- 単純に従業員のソーシャルメディアへのアクセスを禁止するだけでは不十分です。制限を回避する方法は必ず見つかり、セキュリティチームのブラックホールとなってしまいます。
- 組織はソーシャルメディアに対する強固なサイバーセキュリティー・ポリシーを策定する必要があります。階層的なサイバーセキュリティ防御策が含まれ、さらにパスワード・ハイジーン（二要素認証など）、複数プラットフォームで再利用されるパスワード対策の奨励が含まれます。
- また、どの様な防御策もソーシャルメディア・プラットフォームごとに異なる戦術を考慮する必要があります。 一つの対策ですべてをカバーすることはできません。組織は、ソーシャル・エンジニアリングを防止するための強化された手法を検討する必要があります。

### 法執行機関

- 警察や司法機関は、サイバー犯罪に対する基本的対策を、プラットフォーム犯罪、特にソーシャルメディアで行われている活動向けに転換し始めるべきです。
- 情報収集ツールとしてのソーシャルメディアの利用には、その犯罪リスクに対する認識を深める必要があります。
- ソーシャルメディアを利用して行われる犯罪の種類やタイプを検知するための職員向けのトレーニングを強化する必要があります。

## 結論

**GREGORY WEBB**
CEO of Bromium

*アプリケーション隔離はソーシャルメディアを利用した犯罪に対するユニークな防御策を提供。*

このレポートは、ソーシャルメディアはどのような組織にとっても深刻なビジネスリスクであり、攻撃を受け る可能性を大きく広げていることを示しています。現在のセキュリティへのアプローチは、ソーシャルメディアを利用した攻撃が企業への足掛かりとなるのを防ぐために必要な保護を全く提供していません。

組織がこの増大する脅威を理解し、それに対応した防御を行うことは極めて重要です。単にソーシャルメディアのウェブサイトをブロックすればいいという安易な考えは通用しません。LinkedIn、Twitter、YouTube、Facebook、Instagramなどのソーシャルチャネルでのエンゲージメントに失敗した組織は、競争優位性を失い、デジタルネイティブの顧客基盤とのエンゲージメントに失敗することになってしまいます。

では、企業は何ができるのか？

企業は、ソーシャルメディアがサイバー犯罪を助長する役割を十分に理解していないと、企業を乗っ取ろうとするサイバー犯罪者に陥れられてしまう恐れがあります。そのためには、階層的なサイバーセキュリティ防御策とアプリケーション隔離を採用することで、ソーシャルメディアを利用した犯罪のビジネスへの影響を軽減することに注目する必要があります。

アプリケーション隔離は、ハードウェアで強化された仮想マシン内にウェブページや添付ファイルを隔離することで、ソーシャルメディアを利用した犯罪に対するユニークな防御策を提供します。ユーザーが悪意のあるリンクやマルウェアを含む広告をクリックした場合、トラップされ、他のアプリケーションから隔離され、アプリケーションとネットワークを保護します。これにより、マルウェアは無害化され、ハッカーはどこにも行くことができず、盗むものもありません。ユーザーはブラウザーを閉じるだけで、仮想マシンとその中に封じ込められたマルウェアを削除することができます。これにより、従業員は侵害を起こすことを気にすることなく仕事に取り組むことができ、組織への被害を劇的に減らし、高価値の資産を保護することができます。

### BROMIUMについて

Bromiumは、アプリケーション隔離による仮想化ベースのセキュリティを利用して、お客様のブランド、データ、そして人々を保護します。企業の最大の負債であるエンドポイントを最高の防御に変換します。アプリケーション隔離と制御を提供する特許取得済みのハードウェア強化コンテナと、主要な脅威ベクトルと攻撃タイプのすべてを保護する分散型センサーネットワークを組み合わせることで、マルウェア未然に防ぎます。従来のセキュリティ技術とは異なり、Bromiumは自動的に脅威を隔離し、ビヘビア分析を用いて新たな攻撃に対応し、脅威インテリジェンスを瞬時に共有してマルウェアの影響を排除します。Bromiumは、ディフェンスグレードのセキュリティを提供し、Fortune 500や政府機関などの急速に成長している企業を顧客としています。

アプリケーションの隔離と制御がソーシャルメディア上の従業員の保護にどのように役立つか、また、既存の階層化されたサイバーセキュリティ防御をどのように補完することができるかについての詳細は、Bromium（現HP）にお問い合わせください。

## APPENDIX I
### 方法論

このプロジェクトの研究では、サブスクリプションが最も多い10のソーシャルメディア・プラットフォームから得られたデータの量的分析と、ソーシャルメディア・ユーザーとのインタビューや、投稿、コメント、写真などのアップロードの観察から得られた質的データを組み合わせた混合アプローチを利用しました。このオリジナルデータは、2015年 ~ 2018年の間に、主要な学術、ビジネス、法執行、およびその他の関連データソースの包括的な調査から引き出された二次データで補完されています。

今回の調査サンプルとなった10大ソーシャルメディア・プラットフォームは：

- Facebook
- Instagram
- Twitter
- Snapchat
- YouTube
- Reddit
- LinkedIn
- Pinterest
- Tumblr
- WhatsApp

これらに加えて、ロシアと中国のソーシャルメディア・サイトの投稿 を 、VKontakte、Odnoklassniki（ロシア）、WeChat、QQ、Qzone（中国）など、翻訳や翻訳機能があるサイトから選びました。

これらのプラットフォーム全体で、投稿、広告、写真などのアップロードを含む 50 万件以上のデータポイントを選択して、マルウェアの配布、クライムウェアの販売や広告、詐欺、薬物の販売、その他の種類のサイバーを利用した犯罪を検索しました。可能であれば、そのような活動に従事しているソーシャルメディア・ユーザーとの密かな観察とコミュニケーションを確立し調査結果を裏付けました。

**ソーシャルメディアが可能にした犯罪収益の計算についての注意点：**

**違法オンライン薬品販売**

- 全体で年間約4,000億ドル
- Facebookの投稿の約17%が違法なオンライン医薬品販売に関連していることがわかっています。[59]
- 4,000億ドルの17% = 680億ドル。しかし、明らかにこれらの17%の投稿のすべてが実際に収益を生むわけではありません。
- 可能な収益をより正確に把握するために、eコマースサイトの平均コンバージョン率（つまり「リード」の顧客への変換率） = 2.86%を使用することができます。[60]
- 680億ドルの2.86% = 年間**19億ドル**

**金融詐欺**

- 調査した500,000件のうち、0.2%が金融詐欺やその企てに関連していたと思われます。
- ソーシャルメディア・ユーザー数に外挿する - Facebookは、毎日47億件の新しいコンテンツをアップロードしていることを示唆しています。61
- ここでは40億を基準とすると、40億の0.2% = 800万件の不正行為を含む投稿/広告などが含まれていることになります。

[59] Tyrawski & DeAndrea （2015年）
[60] Saleh（2018年）
[61] Zephoria （2018年）

- 詐欺1件あたりの収益1ドルという（非常に低い）数字を使うと、毎日800万ドルが計算でき、1年間で29億ドルが発生すると仮定することができます。
- 信頼できる金融情報ソースからは、3 件の不正行為のうち約 2 件が防止されていることがわかっています。[62] これは、試みられた不正行為の約 30%が成功する可能性があることを示唆しています。不確実性をさらに減らし他の予防策も考慮に入れ、これらのうち実際に収益を上げることができ るのは3件に1件のみであることを考えてみます。つまり、より保守的に見積もっても、詐欺未遂のうち、収益を生み出すことに成功したのは約 10%に過ぎないということです。
- 29億ドルの10% = 年間**2億9,000万ドル**

### デート詐欺

- 米国での被害者の損失額は2億3,000万ドル。[63]
- 約60%の人が、出会い系プラットフォームやアプリの形でソーシャルメディアを使用しているまたは使用したことがあると答えています。[64]
- 2億3,000万ドルの60% = 年間**1億3,800万ドル**

### 盗難データからの収益

- 2018年上半期に45億件の情報が漏洩 = 通年に換算して80億件
- このうち56%はソーシャルメディアからのもの（44億件）です。[65]
- 盗まれたデータの平均的な価値は、クレジットカードのデータが5ドルから、「Fullz情報」（請求先住所、PIN番号、生年月日、社会保障番号、ユーザーの旧姓やオンライン銀行口座の認証情報などの一式）が20 ~ 30ドル。[66]
- 銀行口座データ - 社会保障番号、生年月日、請求先住所、旧姓、電子メールアドレスが含まれる銀行の認証情報は口座の価値の約10%を占めています。 - 例えば、2,000ドルの口座の場合には200ドルです。
- 最小レベルの収益を使用する。 - $5
- ソーシャルメディア・プラットフォームを介して盗まれたデータがすべて販売されているわけではないと仮定します。eコマースサイトと同様のコンバージョン率を使用する。 - 2.86%
- 44億件の2.86% = 125,840,000件（*5ドル） = 629,200,000ドル（切り上げて**6億3,000万ドル**）

### クリプトマイニングからの収益

- クリプトマイニング・ソフトウェアが稼働しているコンピュータは約 5 億台ある。[67]
- インターネットのユーザー数40億人のうち、約75%（約30億人）がソーシャルメディアを利用していることがわかっている。[68]
- これら2つの基本的な統計を考えると、約3億7,500万人のソーシャルメディア・ユーザーが何らかのクリプトジャッキング・ソフトウェアに感染している可能性があると推測できます（5億人の75%）。
- クリプトジャッキングによって生成された収益については、さまざまな推定がありますが、ほとんどは個々の収益が現時点ではあまり高くないことに同意しています。しかしながら、個々の収益が低いことと累積収益が高いことは矛盾しません。実際、上記の数字が相当なものに見えるという事実自体が、個々のサイバー犯罪者が多額の収入を得ていないにもかかわらず（そして、おそらくこれを彼らの活動ポートフォリオの中の1つとしてしか利用しておらず）、多くの個人がこれを試しているということを示唆しているのかもしれません（おそらくランサムウェア攻撃による収入からの切り替えの一環として）。

[62] UK Finance （2018年）
[63] Brenoff （2017年）
[64] Statista （2017年）
[65] Gemalto （2018年）
[66] DarkWeb News （2017年）
[67] Olson （2018)年）https://www.csoonline. com/article/3262987/cyber-attacks-espionage/cryptomining-the-new-lottery-for-cybercriminals.html
[68] Global Digital （2018年）https://wearesocial.com/uk/blog/2018/01/global-digital-report-2018

- 例えば、最近の研究では、ブラウザーベースのマイニングでは非常に低いと示唆されています。この研究では、「平均して、クライトジャッキングのウェブサイトは、1日あたり24,721人の訪問者を集め、およそ3分間滞在させています。したがって、0.17 ~ 89,000コア時間の範囲で、平均1,550コア時間を観測しました。ハッシュレートは80H/sとなり、Coinhiveのペイアウト率では、マイナーは平均して1日あたり約5.80ドルを稼ぐことになり、ウェブベースのクリプトジャッキングでは現在、限られた利益しか得られないという我々の観察を裏付けています。」と結論付けています。[69]
- ただし、この計算はブラウザーベースのクリプトジャッキングのことであることに注意してください。冒頭の統計値は、ソーシャルメディアの活動の結果としてコンピュータに不正にインストールされたクリプトマイニング・ソフトウェアから得られる収益についてです。
- ある試算では、マイニング専用のPCには月当たり**40 ~ 70ドル**[70]（電気代込みで）しかかけられないとされています。
- 繰り返しになりますが、これは個々にはそれほど高くはありませんが、全体としては、月当たり約**150億ドル**、年間**1,800億ドル**の累積収益となります。（つまり、40ドルという低価格の収益見積もりを使用すると、3億7500万台の感染したコンピュータ × 40ドル = 月当たり150億ドルの収益となります）
- しかしながら、これは高すぎると思われます。そこで、別の基準で収益の見積もりを考えてみましょう。
- 別の、より保守的な調査によると、5,000サイトの攻撃でわずか24ドル[71]の利益を得ることができると示唆しています。
- このようなソフトウェアに感染した3億7500万人のソーシャルメディア・ユーザーを使うと、この数字は次のような収益を示唆しています。180万ドル（3億7500万/5,000 = 75,000；75,000 x 24ドル = **180万ドル**）
- この推定値は、**1回**の攻撃に基づいています。原則として、1日の間に複数の攻撃が行われる可能性があります。保守的に、1日に1回の攻撃とすると以下のようになります。月に30回の攻撃があり、その結果月当たり**5,400万ドル**、年間**6億4,800万ドル**の収益になります。
- この収益は、より現実的に見えますが、PCに不正にインストールされたソフトウェアではなく、サイトベースのクリプト攻撃によるものです。
- これをより正確に把握するために、マイニング・マルウェアに攻撃されたユニークユーザーの数を特定する最近のデータを使用することができます。もっともらしい推定は、2018年に80万 ~ 100万人のユニークユーザーが攻撃された[72]ことを示唆しています。
- 上記の統計値を使用して、これらの75%がソーシャルメディアを使っていたと仮定すると、75万人がマイニング・マルウェアに攻撃されたことになります。
- これらの攻撃の50%未満がマイニングソフトウェアのダウンロードに成功したと仮定すると、37万5千人のユニークユーザーがサイバー犯罪者のためにクリプトマイニングの収益を生み出したことになります。
- 上記の最低利益の見積もり（40ドル）を使用します。350,000 x 40ドル = 月当たり**1,400万ドル**または年間1億6,800万ドルの収益
- その結果、もっともらしい収益の範囲は、年間**1億6,800万ドル**から**6億4,800万ドル**の間になります。さらに保守的に考えるならば、**2億5,000万ドル**以下としましょう。

**注意：**マルウェアやハッキングサービスの販売、違法薬物の販売など、ソーシャルメディアを介した犯罪収益の他の形態は、利用可能なデータがないため、この計算には含まれていません。したがって、犯罪収益のレベルは、この推定値よりもはるかに高くなる可能性が高いでしょう。

---

[69] Musch et al （2018年） https://arxiv.org/pdf/1808.09474.pdf

[70] Van Allen （2018年） https://medium.com/finance-republic/heres-how-much-i-make-mining-crypto-with-my-gaming-pc-c692e46d38f# &
https://medium.com/finance-republic/heres-how-i-turned-my-crypto-mining-fail-into-a-wildly-profitable-machine-128f533aa62f

[71] Hern （2018年） https://www.theguardian.com/technology/2018/feb/14/cryptojacking-campaign-24-dollars-hackers-cryptocurrency-salon

[72] Huillet （2018年） https://cointelegraph.com/news/kaspersky-cryptojacking-increasingly-popular-attack-vector-for-botnets

## APPENDIX II
### ソーシャルメディアの情報漏洩

| 年 | プラットフォーム | 損失 | 方法 |
|---|---|---|---|
| 2018 | **Facebook** | 5,000万ユーザー・レコード | 攻撃者がFacebookへのログインを許可するユーザーのセキュリティキーを盗み出したハッキング |
| 2018 | **Reddit** | 大量の非公開 ユーザー名とハッシュ化されたパスワード、電子メールアドレス、およびプライベートメッセージを含むコンテンツ | SMSの傍受 |
| 2018 | **Google +** | 5,200万ユーザー・レコード | 外部のアプリ開発者がデータにアクセスできるようにしたプラットフォームの不具合 |
| 2017 | **WeChat** | 6億6,200万ユーザーのレコードが曝露 | レコードがおそらく中国政府によりアクセスされる |
| 2017 | **VKontakte** | ユーザー名、パスワード、電子メールアドレスを含む1,000万レコード | 古いログイン/パスワードの使用 |
| 2016 | **Myspace** | 4億2,700万ユーザー・レコード | 以前のハッキングで売られたものから発見されたデータ |
| 2016 | **LinkedIn** | 1億1,700万 | 不明 |
| 2016 | **Twitter** | 3,300万 | 感染したブラウザー経由で取得した認証情報 |
| 2014 | **Snapchat** | 100,000 | 不明 |
| 2013 | **Snapchat** | 490万件の電話番号 | 他のユーザーがSnapchatを使っているかどうかを確認するために電話番号を入力する必要がある「友達を探す」機能を利用 |
| **2013年以降ソーシャルメディアを通じて曝露されたユーザー・レコードの合計 - 保守的推論** | | **13億** | |

## APPENDIX III
### ニッチあるいはローカルなソーシャルメディア・プラットフォームと犯罪

今回の調査では、3種類のニッチなプラットフォームを調査しました。その例とユーザーが遭遇したリスクの一部を以下に示します。

| 子育てプラットフォーム | MUMSNET、JUSTMOMMIES、FAMSTER、BABYCENTER その他 |
|---|---|
| **Mumsnet** | フィッシングメールとポップアップ |
| | DDoS攻撃とスワッティング攻撃（一部Twitter経由） |
| **BabyCenter** | フォーラムページからマルウェアにリダイレクトされる<br>モバイルプラットフォームからマルウェアやスパムが拡散 |
| **Justmommies** | マルウェアのリダイレクト |
| **デートプラットフォーム** | **TINDER、MATCH.COM　など** |
| **Ashley Maddison** | 2016年に60ギガバイトのデータがハッキンググループ「インパクトチーム」にハッキングされる |
| **Plenty of Fish** | 2015年にブラウザーがマルウェアをインストールするエクスプロイトにユーザーをリダイレクトした |
| **Fling.com** | 2017年に個人情報、性的嗜好、志向、空想などを含む4,000万レコードが漏洩した。同サイトのデータは、ダーク・ウェブ上で約400ドル（Bitcoinで）で販売されていた。 |
| **フィットネス＆医療プラットフォーム** | **PATIENTSLIKEME、FITMETRIX　など** |
| **PatientsLikeMe** | 2017年に体調に関するデータを共有する60万会員のデータが第三者に盗まれた |
| **MyFitnessPal** | 2017年に1億5,000万ユーザーが（暗号化にもかかわらず）ユーザー名、Eメールアドレス、パスワードにアクセスされた |
| **Singapore Medical Platform** | シンガポール首相のレコードを含む150万件の記録が流出 |

## 参考文献

Alexandre, A. (2018) New Study Says 80 Percent of ICOs Conducted in 2017 Were Scams, Coin Telegraph, 13/07/2018

Barker, S. (2018) Social media phishing on the rise as attackers experiment with tactics, Security Brief, 05/03/2018

Bean, S. 2017 UK workers waste over two hours a day on social media and other distractions, Insight, 24/8/2017

BBC (2016) How innocent photos of children have been exploited on Twitter, 28/11/2016

BBC (2017) Teens found selling drugs on Snapchat and Instagram, 14/07/2017

BBC (2018) YouTube caught out by coin-mining adverts, 29/01/2018

Boodai, M. (2011) LinkedIn Spam Emails Download Malware, Security Intelligence, 02/06/2011 Brenoff, A.

(2017) How A Billion-Dollar Internet Scam Is Breaking Hearts And Bank Accounts, HuffPost, 20/07/2017

CIFAS (2018) Wolves on the Internet

Cimpanu, C (2018) One in Five Companies Gets Malware Infections via Social Media, Softpedia News, 05/04/2016

Cisco (2015) Midyear Security Report

Colleto et al (2016) Pornography Consumption in Social Media. Proceedings of the 10th International AAAI Conference on Web and Social Media. ICWSM 2016, May17-20, Cologne, Germany

Correa, D (2016) It's a trap! WhatsApp Gold 'premium' version lures users to malware, SC Media, 25/05/2016

CTA (2018), The Illicit Cryptocurrency Mining Threat, Cyber Threat Alliance, see: https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-CryptoMining-Whitepaper.pdf

DarkWeb News (2017) The Value of Stolen Data on the Dark Web, see: https://darkwebnews.com/dark-web/value-of-stolen-data-dark-web/

DN Pedia (2018) Top Million Websites & TLDs, see: https://dnpedia.com/tlds/topm.php

Faull, J. (2018) Influencer marketing fraud – how big a problem is it? The Drum 25/6/2018

FBI (2015-2017) Internet Crime Report

Francis, J. (2018) Researchers Find Over 15K Twitter Bots Pushing Cryptocurrency Scams, Bitcoin News, 13/08/18

Fraudwatch International (2018) Saving Face on Social Media, see: https://fraudwatchinternational.com/social-media/saving-face-social-media/

Frenkel, S., Isaac, M. & Conger, K. (2018) On Instagram, 11,696 Examples of How Hate Thrives on Social Media, New York Times, 29/10/2018

Gemalto (2018) Data Breaches Compromised 3.3 Billion Records in First Half of 2018, Press Release, 23/10/2018

Godshall, J. (2018), British Cyber Crime Center Reports $2.5 Million Lost in Cryptocurrency Scams This Summer, Unhashed, 11/08/2018

Greer, S. (2018) Social Chain wage war on fake Instagram influencers, Manchester Evening News 9/10/2018

Griffin, A. (2015) 10 million Twitter accounts could be deleted in porn purge to satisfy advertisers, Independent, 19/05/2015

Halevi, T., Lewis, J. & Memon, N. (2013) Phishing, Personality Traits and Facebook, see: https://arxiv.org/pdf/1301.7643v2.pdf

## 参考文献
つづき

Hayes, N. (2016) Why Social Media Sites Are The New Cyber Weapons Of Choice, Dark Reading, 06/09/2016

Jay, J. (2018) Hackers still exploiting the human factor to carry out ransomware attacks, SC Media, 31/03/2018

Greer, S. (2018) Social Chain wage war on fake Instagram influencers, Manchester Evening News, 09/10/2016

Gwynn (2016) Fifth of top brands' social media accounts are 'fraudulent', Campaign, 01/09/2016

Irshad and Soomro (2018) Identity Theft and Social Media, IJCSNS International Journal of Computer Science and Network Security, 18, 1

Kaspersky (2018) Fake Facebook sites account for 60% of social network phishing in early 2018, 23/05/2018

Keyworth, M. (2018) I was a teenage 'money mule', BBC, 26/05/2018

Krustev, V. (2018) Facebook Nike Shoes Scam of 2018 Shows History Repeats Itself, Security Boulevard, 14/08/2018

KVRR (2017) Three Teams, 500+ Pills, One Snapchat Deception, see: https://www.kvrr.com/2017/03/31/three-teams-500-pills-one-snapchat-deception-leads-to-six-arrests-in-joint-nd-mn-drug-bust/

Leyden, J. (2017) Instagram phishing apps pulled from Google Play, The Register, 09/03/2017

Lo, C. (2018a) Almost 250 people in Hong Kong lose HK$1.9 million in WhatsApp scam, South China Morning Post, 11/04/2018

Lo, C. (2018b) Phone scammers now using WeChat voice messages to snare victims, South China Morning Post, 18/01/2018

McAfee (2018) June 2018 Threats Report

Marsh, S. (2018) Social media related to violence by young people, say experts, The Guardian 02/04/2018

Matthews, L. (2017) Russian Hackers Hid Link To Malware Servers In Britney Spears Instagram Comments, Forbes, 07/06/2017

Muller, K. & Schwarz C. (2018) Fanning the Flames of Hate: Social Media and Hate Crime, Warwick Business School, 19/02/2018

Mumsnet (2014) see: https://www.mumsnet.com/Talk/site_stuff/1957616-What-is-with-the-random-redirect-to-porn

Musch, M. et al (2017) Web-based Cryptojacking in the Wild, Technische Universit ä t Braunschweig Institute for Application Security

Palmer D. (2018) This password-stealing malware uses Facebook Messenger to spread further, ZDNet, 01/05/2018

Pesce et al (2012) Privacy attacks in social media using photo tagging networks: A case study with Facebook, PSOSM' 12 April 17 2012, Lyon, France

Pew (2016) "Social Media and the Workplace", Pew Research Center, June, 2016

Pew (2017) News Use Across Social Media Platforms 2017, Pew Research Center, September, 2017

Phillips, G. (2016) The Dark Side of Social Media, Mud, 31/10/2016

Powell, J. (2018) The Problem With Banning Pornography on Tumblr, New York Times, 06/12/2018

Ragan, S. (2015) Malware uses video and tags to infect 100,000 people on Facebook, CSO, 30/01/2015

Redlock (2018) Lessons from the Cryptojacking Attack at Tesla, 20/02/18

## 参考文献
つづき

Reynolds, J. (2018) Mentions of social media in crime quadruple in four years, Shropshire Star, 22/01/2018

Reuters VoA 2018 China Sees Surge in Personal Information Up for Sale, 23/08/2018

Saleh, K. (2018) The Average Website Conversion Rate by Industry (updated November 2018), Invesp, see: https://www.invespcro.com/blog/the-average-website-conversion-rate-by-industry/ SANS

(2017) Threat landscape survey: Users on the front line, White paper, 2017

Seymour, J. & Tully, P. (2016) Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter, Black Hat Conference

Statista (2017) Share of internet users in the United States who have used online dating sites or apps as of April 2017, by age group, see: https://www.statista.com/statistics/706499/us-adults-online-dating-site-app-by-age/

Tambini, Damian (2018) Social Media Power and Election Legitimacy. In: Tambini, Damian and Moore, Martin, (eds.) Digital dominance: the power of Google, Amazon, Facebook, and Apple. Oxford University Press, New York, NY, pp. 265-293

Thomas (2013) Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse, Usenix Security Symposium

Tsing, W. (2018) Maybe you shouldn't use LinkedIn, Malwarebytes, 05/04/2018

Tyrawski, J. & DeAndrea, D. (2015) Pharmaceutical Companies and Their Drugs on Social Media: A Content Analysis of Drug Information on Popular Social Media Sites, J Med Internet Res. 2015 Jun; 17(6): e130

UK Finance (2018) Banks and card companies prevented £2 in every £3 of attempted unauthorised fraud in 2017, see: https://www.ukfinance.org.uk/finance-industry-stops-1-4-billion-in-attempted-fraud/

Vishwanath, A. (2015) Habitual Facebook Use and its Impact on Getting Deceived on Social Media, Journal of Computer-Mediated Communication, 20, 83 – 98

WMC (2012) Pinterest users finding unwanted porn pinned, 20/9/2012, see: http://www.wmcactionnews5.com/story/19590096/pinterest-users-finding-unwanted-porn-pinned/

Zephoria (2018) The Top 20 Valuable Facebook Statistics, see: https://zephoria.com/top-15-valuable-facebook-statistics/

Zerofox (2017) External social and Digital threats to Financial institutions, whitepaper



Copyright ©2019 Bromium, Inc. All rights reserved. WoP-Social-Platforms-Report-02252019