サイバーセキュリティレポート

2022.05

NTT セキュリティ・ジャパン株式会社
コンサルティングサービス部　脅威インテリジェンス管理チーム

目次

【当レポートについて】

当レポートでは 2022 年 5 月中に生じた様々な情報セキュリティに関する事件、事象、またそれらを取り巻く環境の変化の中から特に重要と考えられるトピック 3 点を選び、まとめたものである。各トピックの要旨は以下のとおりである。

第 1 章『ウクライナ侵攻とサイバー攻撃の現在』

- ウクライナ侵攻から 100 日以上が経つが、ロシアのサイバー攻撃はウクライナに大きな損害を与えるには至っておらず、米、英、NATO 諸国の政府や民間企業による支援が効果をあげている可能性がある。
- 「アノニマス」が親ロシア系グループに宣戦布告して公式サイトをダウンさせるなど、政府だけでなく民間でも激しい攻防が続いている。
- ロシアのウクライナ侵攻に関連した、日本を狙った活動は今までのところ観察されていないが、ランサムウェアをはじめとした攻撃には引き続き警戒する必要がある。

第 2 章『英国 NCF によるサイバー犯罪者へのサイバー作戦実施が明らかに』

- 2022 年 5 月、英国政府のジェレミー・フレミング GCHQ 長官はセキュリティーシンポジウムでの講演で、英政府でサイバー攻撃活動を担う機関である国家サイバー部隊（NCF）が成果を上げていることを述べた。
- NCF がサイバー犯罪組織のネットワークを弱体化させる作戦を実施してきたと、フレミング長官は明かした。
- 英国政府はこれまで、敵対する国家やテロリスト、犯罪者らの攻撃を抑止するため NCF を設立したと説明してきたが、成果を上げていたことは公にしていなかった。

第 3 章『Telegram』

- Telegram は、ロシア人が 2013 年に開発したプライバシーと表現の自由に力を入れているメッセージングアプリである。IT 法規制を回避するために国境を跨いで拠点を何度も移転している。
- ハッカーは、Telegram の自身のチャネルで盗んだ銀行口座などを販売したり、グループチャットでハッキング方法を議論したりしている。日本では闇バイトの連絡手段としてシークレットチャットの機能が使われている。
- Telegram は 2018 年にロシア政府に禁止されたが、その後もロシア政府の規制と妥協することなく戦い、2020 年に禁止が解除された。現在のウクライナ侵攻においても規制されず、ロシアでは検閲に対する象徴となっている。

1. ウクライナ侵攻とサイバー攻撃の現在

1.1. はじめに

2 月 24 日にロシアが開始したウクライナへの侵攻から、6 月 3 日で 100 日が経過したが、現在でもウクライナ東部を中心に激しい戦闘が続いている。

サイバー空間でも、両国が主導する組織と、それぞれの政府を支持するハッカーグループが攻撃を仕掛けあい、世界中の民間人までを巻き込んだ激しいサイバー戦争が繰り広げられている。本稿では 4 月以降明らかになった状況について紹介する。

1.2. ロシア側の攻撃者の動き

【政府系】

ロシアは世界でもトップレベルのサイバー攻撃能力を有していることから、侵攻当初は多くの専門家が、ロシアからウクライナへの大規模なサイバー攻撃と甚大な被害を予想していた[1]。しかし、開戦後はこれまでのところ、ロシア政府が主導・支援するグループのサイバー攻撃によって、ウクライナで目立った被害は出ておらず、攻撃は上手くいっていないとみられている。

専門家は、米、英、NATO 諸国の政府や民間企業による支援が奏功していると指摘している[2]。特に米国は、2015 年以降、ウクライナに対してサイバーセキュリティ支援を行っており、今回も米サイバー軍やマイクロソフト社がウクライナにエンジニアを送り込み、ウクライナ国内での輸送や、エネルギーインフラのような重要拠点において、防御を行っている。

図 1 米国務省によるプレスリリース
「ウクライナの接続性とサイバーセキュリティに対する米国のサポート」[3]

[1] 出典：時事通信社『ウクライナ侵攻の裏にある「見えない戦争」サイバー工作』
https://www.jiji.com/jc/v8?id=202204ukrrusyt

[2] 出典：Foresight『ロシアから重要インフラを守る米・ウクライナ「サイバーセキュリティ協力」』
https://www.fsight.jp/articles/-/48810

[3] 出典：U.S. Department of State『U.S. Support for Connectivity and Cybersecurity in Ukraine』
https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/

ロシアの攻撃が阻まれた一例として、ウクライナ政府のサイバーインシデント対応チーム「CERT-UA」と協力しているセキュリティ会社「ESET」が 4 月 19 日に公開した事件がある[4]。同社のブログによると、ウクライナのエネルギー企業の高圧変電所に対し、マルウェア「Industroyer2」が仕掛けられ、4 月 8 日 16 時 10 分(UTC)に実行されるよう設定されていた。このマルウェアは 2016 年にウクライナで大規模停電を引き起こした「Industroyer」の新バージョンと推測されており、当時攻撃を行ったロシアの APT グループ「Sandworm」が今回も関与していたと見られる。詳細な経緯は説明されていないが、重大な事態に至る前に発見、修復され、施設は保護された。

【非政府系】

日本を含む西側のメディアでは、ロシアに敵対するハッカーとしてアノニマスの活動が報じられることが多いが、ロシアを支援するハッカーも存在し、現在は「Killnet」と「Legion」というグループが活動している。Killnet の創設者はインタビューで、同グループがウクライナ侵攻を機に、以前行っていた DDoS ボットネットの販売を止め、その後はグループ自身が同様のボットネットを使用し、ウクライナ及び NATO 諸国に立ち向かうロシアの戦いを支援することにしたと語っている。実際に 5 月 11 日には、イタリアの複数の政府系ウェブサイトに対して DDoS 攻撃を実行し、数時間にわたりサイトへのアクセスが不可能となる事態を引き起こした[5]。

その後、新たな標的として、60 年以上の伝統があり視聴者数 2 億 4 千万人にのぼる欧州の歌合戦イベント「ユーロビジョンソングコンテスト」の投票システムへの攻撃を予告し、大きな注目を集めた。このコンテストは欧州では一大イベントであり欧州の市民に与えるインパクトが大きいこと、またウクライナの代表が勝ち進んでいたために攻撃対象とされたと考えられる。しかし、5 月 14 日の投票日までに投票システムはダウンせず、コンテストはウクライナのラップバンド「Kalush Orchestra」の優勝で無事終了した[6]。

翌 15 日、イタリア警察はこれらの親ロシアハッカーグループによる攻撃を阻止したと発表した[7]。その後、Killnet はユーロビジョンを攻撃しなかったと発表し、次回はイタリア警察を標的とした DDoS 攻撃を行うことを宣言した。

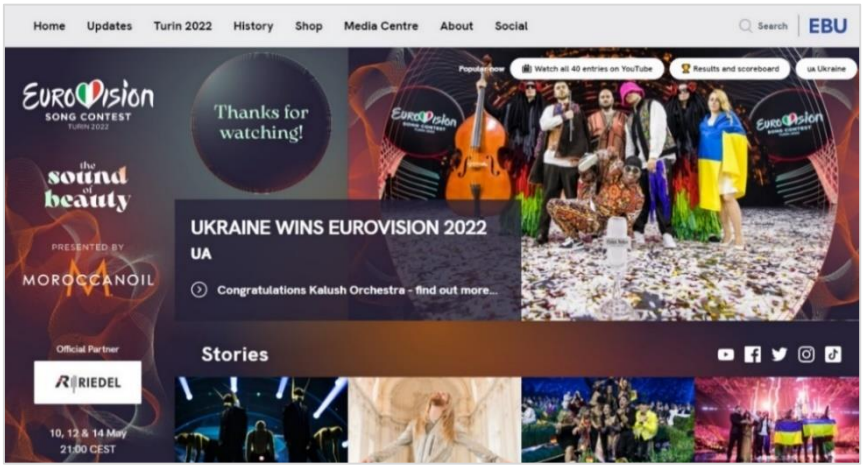


図 2「ユーロビジョンソングコンテスト」Web サイト

[4] 出典：ESET『ウクライナに大規模停電をもたらした「Industroyer」マルウェアの新バージョン「Industroyer2」確認』
https://www.eset.com/jp/blog/welivesecurity/industroyer2-industroyer-reloaded/?utm_source=malware_info&utm_medium=refferal&utm_campaign=industroyer2

[5] 出典：Sysdig『イタリアと NATO に対する Killnet サイバー攻撃について』
https://www.scsk.jp/sp/sysdig/blog/container_security/natokillnet.html

[6] 出典：NBC『Ukraine crowned winner of 2022 Eurovision Song Contest』
https://www.nbcnews.com/pop-culture/pop-culture-news/ukraine-crowned-winner-2022-eurovision-song-contest-rcna28318

[7] 出典：REUTERS『Italy prevents pro-Russian hacker attacks during Eurovision contest』
https://www.reuters.com/world/europe/italian-police-prevents-pro-russian-hacker-attacks-during-eurovision-contest-2022-05-15/

【ランサムウェアグループ】

世界中に深刻な損害を与えているロシア語圏のランサムウェアグループ「Conti」にも大きな動きがあった。5 月 20 日、セキュリティ会社 Advanced Intelligence は、Conti が被害者との交渉用サイトやメッセンジャー、サーバーやプロキシといったインフラを 5 月 19 日までにシャットダウンし、解散したと述べた[8]。Conti が被害企業のデータを公開するために開設したブログ「Conti News」は 19 日以降も更新されているが、以前のようには管理されておらず、「米国は地球の癌」だと批判する反米ヘイトスピーチが投稿されるなど、掲載されるメッセージの質も著しく低くなった。

ただ、Advanced Intelligence によると、この解散はブランド変更を狙った計画的なものである。Conti は 2020 年夏の活動開始以降、複数のランサムウェアの運営を引き継ぎ、活動の幅を広げ、ウクライナ侵攻以前より世界中の法執行機関から追われる立場となっていた。

図 3 ロシア支持を表明する Conti の投稿 8

さらに、ウクライナ侵攻の直後、ブログでロシア政府への支持を表明したことが、Conti ブランドを崩壊させる決定打となった。Conti はロシア人を中心にウクライナやベラルーシをはじめ様々な国のメンバーで構成されている[9]が、この表明により、ロシア人メンバーとウクライナやその他の国のメンバーとの間に内紛が起こり、内部資料やプライベートチャットのログがリークされる事態となった。また、Conti とロシア政府が結びつけられて見られるようになり、Conti の身代金要求に応じると、米国のロシアに対する制裁違反となるため、身代金を支払う企業はほとんどなくなった [8]。さらに、米国務省は、5 月 6 日、Conti の運営者の特定につながる情報に対して最大 1,000 万ドル(およそ 14 億円)という多額の報奨金を提供することを発表した[10]。

Conti の運営者は以前から、「KaraKurt」、「BlackByte」、「BlackBasta」といった別ブランドのランサムウェアグループも運営しているとみられており、Conti ブランドを捨てた後も、そういった別のブランドで活動していくと考えられる。

---

[8] 出典：Advanced Intelligence『DisCONTInued: The End of Conti's Brand Marks New Chapter For Cybercrime Landscape』
https://www.advintel.io/post/discontinued-the-end-of-conti-s-brand-marks-new-chapter-for-cybercrime-landscape

[9] 出典：WIRED『ランサムウェア集団「Conti」の情報流出から見えた、ロシア政府との複雑な関係』
https://wired.jp/article/conti-ransomware-russia/

[10] 出典：U.S. Department of State『Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice』
https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspirators-to-justice

1.3. ウクライナ側のサイバー防衛と攻撃者の動き

【政府系】

ロシアによる侵攻以前、ウクライナには正式なサイバー軍がなかった。侵攻後の 2 月 27 日、ウクライナのデジタル改革担当大臣のミハイロ・フェドロフは、「私たちは IT 軍を組織している。デジタルの才能を持つ者が必要だ」とツイートし[11]、世界中から広く参加者を募集した。

ウクライナ IT 軍はサイバー攻撃に関する Web サイトを設け、ロシアの銀行、通信、電力、医療機関等の重要インフラ組織をターゲットとして挙げ、それらに対して DDoS 攻撃を行うことを推奨している。また、攻撃用のツールも同サイトで提供され、攻撃全体の進捗状況や個別のターゲットの現在の状態も確認できるようになっている。

図 4 IT 軍への参加を呼び掛ける大臣のツイート

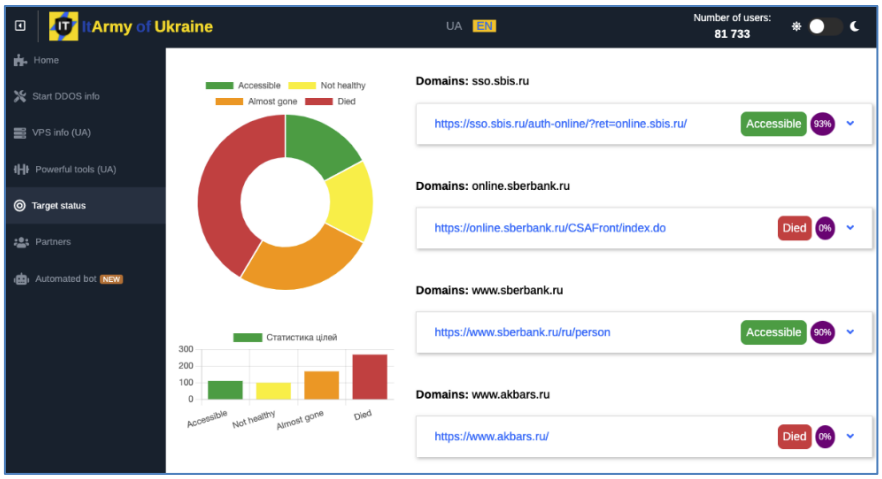


図 5 ウクライナ IT 軍のターゲットステータスページ(ロシアのいくつかのドメインが”Died”になっている)

上述の攻撃には効果があったとみられ、プーチン大統領は 5 月 20 日、ロシアがサイバー攻撃に直面しているとして、防衛力を高めることを国民に約束した[12]。また 5 月 23 日、国連安全保障理事会での技術と安全保障に関するブリーフィングで、ロシアの大使は世界に対して、インターネットを非軍事化することを要求し、西側のサイバー版全体主義化を非難した[13]。

[11] 出典：Twitter『@FedorovMykhailo』
https://twitter.com/FedorovMykhailo/status/1497642156076511233

[12] 出典：REUTERS『Putin promises to bolster Russia's IT security in face of cyber attacks』
https://www.reuters.com/world/europe/putin-warns-cyber-aggression-against-russia-promises-security-shakeup-2022-05-20/

[13] 出典：INSIDER『Russia demands that the world 'demilitarize' the internet and accuses the West of 'cyber-totalitarianism'』
https://www.businessinsider.com/russia-demands-demilitarization-online-information-2022-5

【非政府系】

非政府系でウクライナを支持している組織としてはアノニマスがあげられる。ロシアの対ナチスドイツ戦勝記念日である 5 月 9 日、デジタルテレビ番組表が改ざんされ、すべてのテレビ番組名が「あなた達の手はウクライナ人の血で汚れている」といった反戦を訴えるメッセージに変わった。攻撃の実行者は明らかになっていないが、アノニマスの一人「@YourAnonNews」は、この状況を報告したツイートを引用し、「おはよう、モスクワ」とツイートしている[14]。

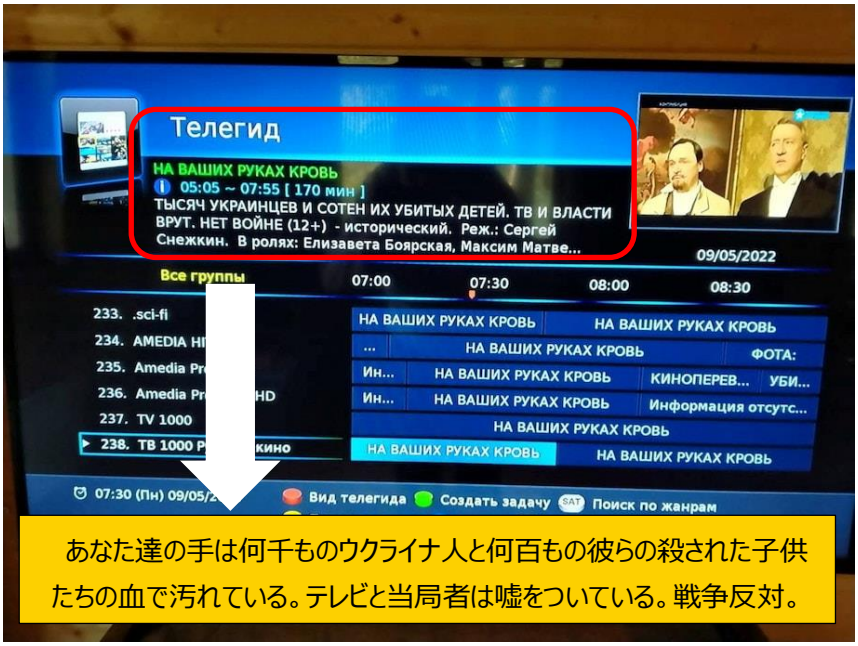


図 6 反戦を訴えるメッセージに書き換えられた番組表[15]
(赤枠以外の箇所にも同様のメッセージが記載されている)

また、アノニマスは前述の親ロシアハッカー集団「Killnet」に対しても対抗措置を取っている。Killnet がイタリア政府機関に対して攻撃することを宣言した後、アノニマスの「@YourAnonOne」は 5 月 22 日午前 1 時 20 分に、「アノニマスは親ロシアのハッカーグループ Killnet とのサイバー戦争に正式に参加する」と宣言した。
そのわずか 1 分後の 1 時 21 分、「安らかに眠れ Killnet」とツイートすることで、Killnet の公式サイトがオフラインになっていることを告げた[16,17]。

[14] 出典：Twitter『@YourAnonNews』
https://twitter.com/YourAnonNews/status/1523578517694341121
[15] 出典：The Washington Post『Russian TV, online platforms hacked with antiwar message on Victory Day』
https://www.washingtonpost.com/world/2022/05/09/russia-tv-hack-victory-day-ukraine-war/
[16] 出典：Twitter『@YourAnonOne』
https://twitter.com/YourAnonOne/status/1528048043647434752
[17] 出典：Infosecurity『Anonymous Declares Cyber-War on Pro-Russian Hacker Gang Killnet』
https://www.infosecurity-magazine.com/news/anonymous-declares-war-on-killnet/

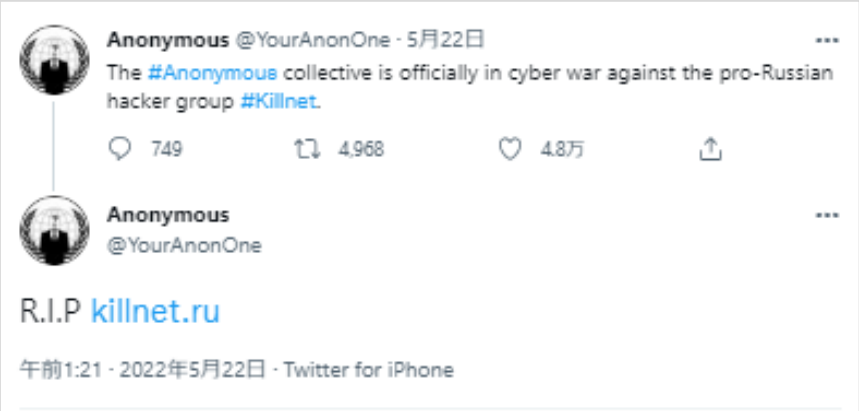


図 7 @YourAnonOne の投稿
宣戦布告と Killnet がオフラインになったことを連続して投稿

1.4. まとめ

サイバー空間ではウクライナ、ロシア共に多方面で攻防を繰り広げているが、米、英、NATO 諸国及び、世界中の政府、民間の協力もあり、現在のところウクライナが有利に立ち回っている印象である。

ロシアのウクライナ侵攻に関連した日本を狙った活動は今までのところ観察されていないが、ランサムウェアをはじめとした攻撃には引き続き警戒する必要がある。

2. 英国 NCF によるサイバー犯罪者へのサイバー作戦実施が明らかに

2.1. 概要

図 8 「CYBER UK 2022」で講演するフレミング GCHQ 長官 [18]

2022 年 5 月、英国で開催されたセキュリティーシンポジウム「CYBER UK 2022」で英国政府通信本部（GCHQ）のジェレミー・フレミング長官が講演した。フレミング長官は、国防省や GCHQ 等の組織によるパートナーシップである国家サイバー部隊（NCF）が、サイバー犯罪に対して積極的に介入し「サイバー犯罪を混乱させる取り組みを巨大な規模で行っている」と明かした[19]。

2.2. 英国のサイバーセキュリティ戦略と NCF

【GCHQ へのサイバーセキュリティ対策組織の集約】[20]

2010 年代に入り、英国政府内には、民間等に対してサイバーセキュリティ対策の支援等の活動を行う組織が林立して縦割り化し、重要インフラでのセキュリティ事故発生に対応しきれない等の問題を抱えていた。2016 年に英国政府は「国家サイバーセキュリティ戦略 2016」を策定して、新設した「NCSC」に集約した。この NCSC を傘下に置いて所管するのが**「GCHQ」**である。GCHQ は古くからある首相直轄の英国の諜報機関で黒子のような存在だったが、サイバーセキュリティを管轄する組織として NCSC 設置以降は表舞台に現れるようになった。GCHQ の諜報機関としての情報やスキル・経験を活用できることが NCSC の強みとされている。

---

[18] 出典：YouTube『CYBERUK ONLINE Plenary 1 : Global response, Global impact: Strategic alignment and collaboration』 https://www.youtube.com/watch?v=7Ywcj8Jdv7w

[19] 出典：GCHQ『Director GCHQ speaks at CyberUK 2022』 https://www.gchq.gov.uk/speech/cyberuk2022

[20] 出典：JETRO『英国のサイバーセキュリティ体制の現状と課題』 https://www.jetro.go.jp/ext_images/_Reports/01/427a23803575001d/20170120.pdf

【NCF 設立】[21] [22] [23] [24]

GCHQ 傘下への集約後、英国は国家サイバーセキュリティ戦略をさらに進め、GCHQ と国防省（MOD）のパートナーシップ組織として**「NCF」**を設置した。テロリスト・犯罪者・敵対国といった安全保障上の脅威によるサイバー攻撃に対抗し抑止するための、サイバー作戦実行を目的としている。

作戦に必要な様々なサイバーセキュリティの専門家を、統一された指揮下に収め、GCHQ のグローバルな情報収集能力と国防省の作戦の専門知識を主とし、それに加えて国防科学技術研究所（Dstl）から科学技術能力、英国秘密情報部（MI6）から秘密作戦遂行能力等を結集させている。

2020 年 11 月に英国政府が NCF の存在を発表した際には、「テロリストが連絡先と通信できないようにするためにスマートフォンを妨害する」「インターネットが深刻な犯罪のプラットフォームとして使用されることを防ぐ」「英国の軍用機が敵の兵器システムの標的にならないよう保護する」[25]といった活動が、目的とする作戦例として発表された。

もともと GCHQ と国防省は、NCF の結成前からサイバー攻撃の共同作戦を実施していた。過去には国防大臣や GCHQ 長官が、中東の ISIS 等のテロ組織に対してプロパガンダネットワークを弱体化させる等の作戦を行ったことを明らかにしている。これらの実績が NCF にも引き継がれていると考えられる。

2.3. フレミング長官の講演

GCHQ のフレミング長官は英国政府によるセキュリティーシンポジウム「CYBER UK 2022」で講演を行い[26]、英国のサイバーセキュリティにおける GCHQ や NCSC の取り組みについて語る中で、NCF を通じたサイバー犯罪組織へのサイバー作戦の一端を明らかにした。

フレミング長官は具体的な作戦の内容には言及しなかったが、犯罪者の不当な利得を防いだり、サイバーツールやマルウェアへのアクセスを拒否したりするために、NCF が国内外の法執行機関と連携して、サイバー犯罪組織のネットワークを弱体化させる作戦を実施してきたことを述べた。作戦の成果について「何十万もの盗まれたクレジットカード情報が、犯罪者にとっては無価値になった」「世界中の無数の犯罪被害者のデータとアカウントは保護されている」と表現している。これにより英国経済は、数千万ポンドに相当する潜在的な詐欺被害を回避できたという。

NCF は存在が明らかにされてからも、実際にサイバー作戦を行っていることは公にされてこなかったため、フレミング長官の発

---

[21] 出典：JST 研究開発戦略センター（CRDS）『英国のサイバー能力を変革し、英国を守る「国家サイバー部隊」（NCF）の設立』 https://crds.jst.go.jp/dw/20201127/2020112725279/

[22] 出典：英国政府『International Policy Review Puts Cyber at the centre of the UK's Security』 https://www.gov.uk/government/news/international-policy-review-puts-cyber-at-the-centre-of-the-uks-security

[23] 出典：英国政府『Permanent location of National Cyber Force campus announced』 https://www.gov.uk/government/news/permanent-location-of-national-cyber-force-campus-announced

[24] 出典：King's College London The Policy Institute『The National Cyber Force that Britain Needs?』 https://www.kcl.ac.uk/policy-institute/research-analysis/national-cyber-force

[25] 出典：NCF『NATIONAL CYBER FORCE EXPLAINER』 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1041113/Force_Explainer_20211213_FINAL__1_.pdf

[26] 出典：GCHQ『Director GCHQ speaks at CyberUK 2022』 https://www.gchq.gov.uk/speech/cyberuk2022

言は、メディアで「英国政府による、法の範囲内の正当なハッキングの例」として取り上げられた[27] [28]。

2.4. まとめ

今回、英国政府がサイバー犯罪者を標的としたサイバー作戦実施の事実を自ら公表したのは画期的な出来事である。国家機関によるサイバー作戦はこれまで、ロシアや中国、北朝鮮等の関与とされる APT が注目されていたが、最近、米英も作戦実施の事実を公表するようになった。6 月 1 日には米サイバー軍司令官も、ウクライナ侵攻のロシアに対し「攻撃的なハッキング作戦」を実施していると、メディアのインタビューに答えている[29]。一方で、英国政府は法の範囲内で実施していると説明しているが、他国に仕掛けた場合のサイバー戦争との境目のあいまいさが英国国内でも懸念[30]されている。

NCF のサイバー作戦の効果についてフレミング長官は「敵にコストを課す」と語っている。日本では現在のところ、NCF のような活動を行っている政府機関は存在しないが、サイバー犯罪やサイバーテロの脅威は増しており、対抗するためにも「コストを課す」ための研究や議論は進めて行くべきではないかと考える。

[27] 出典：Sky News『UK government hackers destroyed hundreds of thousands of stolen credit card details held by criminals』
https://news.sky.com/story/uk-government-hackers-destroyed-hundreds-of-thousands-of-stolen-credit-card-details-held-by-criminals-12609745

[28] 出典：ZDNet『Government hackers made hundreds of thousands of stolen credit cards 'worthless' to crooks』
https://www.zdnet.com/article/government-hackers-made-hundreds-of-thousands-of-stolen-credit-cards-worthless-to-crooks/

[29] 出典：Sky News『US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command』
https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139

[30] 出典：King's College London The Policy Institute『The National Cyber Force that Britain Needs?』
https://www.kcl.ac.uk/policy-institute/research-analysis/national-cyber-force

3. Telegram

3.1. 概要

近年、サイバー犯罪の通信手段として、Telegram が利用される機会が増えている。また、ウクライナ侵攻に伴いロシア語圏の情報源として注目が集まっている。本稿では Telegram の特徴や、犯罪者の間やロシア語圏での利用が広がっている要因について紹介する。

3.2. Telegram とは [31] [32] [33]

図 9 Telegram マーク

Telegram は、2013 年に Telegram Messenger LLP(以下、Telegram 社)を設立したロシア人技術者 2 名（兄弟）により開発されたメッセージングアプリである。同社のスタッフの多くはロシア出身であり、Telegram の月間アクティブユーザー数は 5 億人を超える。ロシア国内の IT に関する法規制のため、2014 年に本社をロシアから移転することを余儀なくされ、ベルリン、ロンドン、シンガポールなど、これまでに多くの都市を転々とした。現在の拠点はドバイであり、現地の法規制が変更された場合は移転するとしている。

Telegram にはユーザー間のメッセージを暗号化するオプションがあり、これを使うと Telegram 社でさえもメッセージのやり取りを見ることは不可能となる。また、分散インフラストラクチャを採用しているため、サーバーに保管されるチャットデータは世界中の複数のデータセンターに分散して保存される。そのため、サーバー上のメッセージ開示には、異なる国からの複数の裁判所命令が必要となる。これにより政府等はプライバシーと表現の自由を侵害できない、と Telegram 社は主張している。

LINE などの他のメッセージアプリでは、トークの履歴を消去してもこれらがサーバーに残るため、復元が可能である。それらに比べ Telegram でのやり取りは、アプリで一度消去するとサーバーからも消去され、メッセージの復元は困難となる。そのため Telegram は、犯罪者が法執行機関の追跡を逃れるための連絡手段として使われることが多い。

Telegram 社は、法執行機関から電話番号やチャット履歴などの情報開示を求められた場合、Telegram のユーザーがテロの容疑者であることを証明する裁判所からの命令を受け取ったときのみ対応すると述べている。ただこれまでに、そのようなケースは一度も起きていない。

---

[31] 出典：Telegram『Telegram Privacy Policy』
https://telegram.org/privacy

[32] 出典：Telegram『Telegram FAQ』
https://telegram.org/faq#q-what-is-telegram-what-do-i-do-here

[33] 出典：Line『捜査機関の対応』
https://linecorp.com/ja/security/article/28

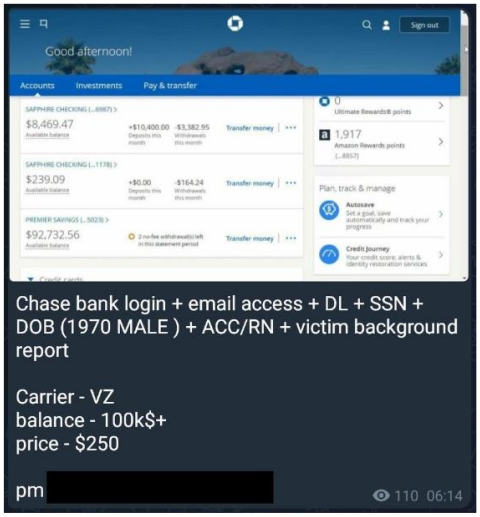
3.3. サイバー犯罪と Telegram

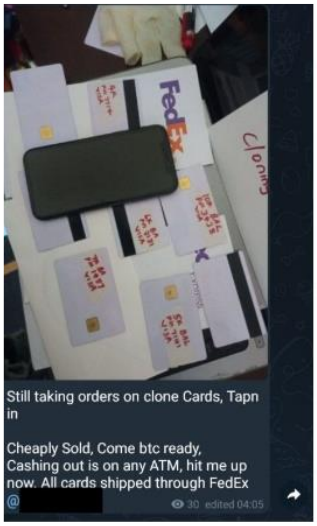
【リークチャネル】[34]

Telegram には、チャネルという不特定多数の人に向けてメッセージを発信する機能がある。ユーザーは自分の電話番号を公開せずに自分が設定したユーザー名で、チャネルを作成できる。Telegram は、上述の通り法執行機関に追跡されにくいことに加え、チャネルを作成すれば、膨大な数のアクティブユーザーの中から多くのチャネル購読者を獲得できるチャンスがある。管理の難しいダークウェブよりも、Telegram のチャネルは簡単に立ち上げられる。

これらに注目したサイバー犯罪者は、Telegram に自身のリークチャネルを作成し、盗んだ銀行口座や、偽の身分証明書、ワクチン証明書、企業から流出した VPN アカウント等を無料で投稿したり、販売したりしている（**図 10**）。Telegram はサイバー犯罪者の間で、ダークウェブの代替手段として広がりを見せている。

サイバー犯罪グループ LAPSUS$は企業からデータを窃取した後、Telegram の自身のチャネルで、当該企業を脅迫し、身代金を支払わない場合は盗んだ情報を流出させると述べた（**図 11**）。





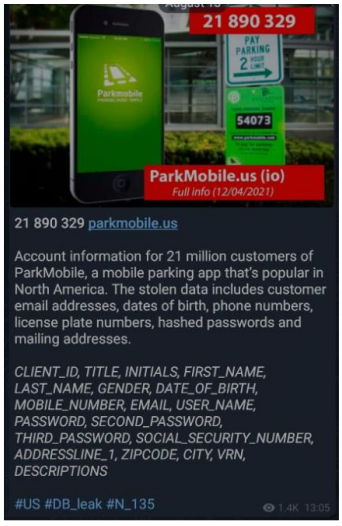


図 10 リークチャネルが暴露したデータ

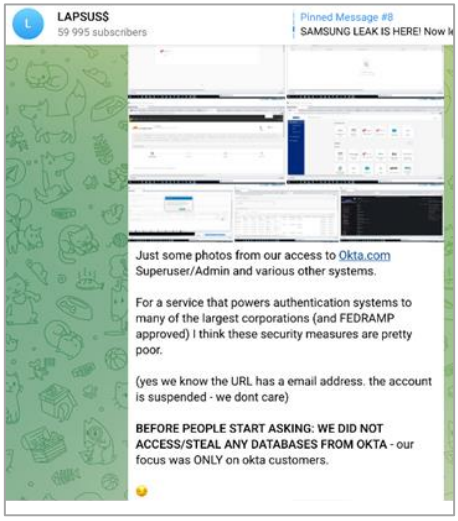


図 11 LAPSUS$の Telegram チャネル

[34] 出典：Security Boulevard『Dark Web Threat Intelligence Part 1: Deep Dive into the Criminal Underground Network on Telegram』
https://securityboulevard.com/2022/01/dark-web-threat-intelligence-part-1-deep-dive-into-the-criminal-underground-network-on-telegram/

【ハッキンググループ】[35]

Telegram のグループ機能は、友人や家族と、また閉じられたチームで物事や情報を共有するときに使う。

ハッカーは、集まった何百人ものメンバーでサイバー犯罪の手口を共有したり、不正に入手した個人情報をどのように悪用するか積極的に議論したりすることに、グループ機能を使っている。**図 12** はハッカーが Telegram のグループで、企業から漏洩したデータを共有し、議論を行っている様子である。

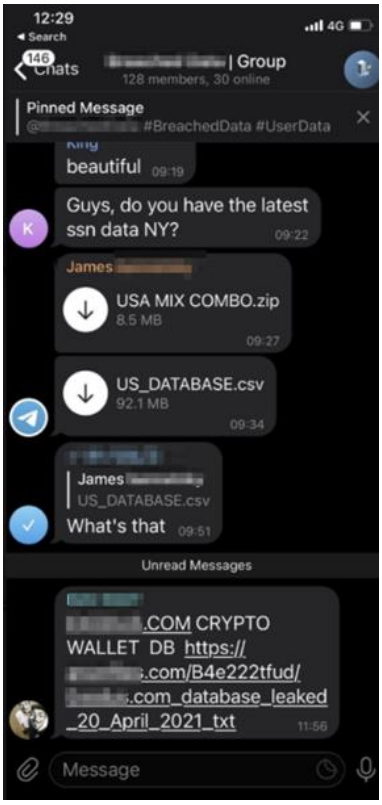


図 12 ハッカーたちのグループチャット

【シークレットチャット】[36]

Telegram には、ユーザー間のメッセージを暗号化して送受信できるシークレットチャットと呼ばれる機能も含まれている。これにより、Telegram のサーバーを経由せず、そのまま端末同士で通信が完結するため、自分と相手の端末上にしかメッセージが残らない。また、自身のメッセージを相手端末から削除できる他、ログアウトやタイマー設定により履歴の自動削除も可能である。

日本では出会い系サイト／アプリのサクラ、オレオレ詐欺に加担する出し子や受け子といった、違法な手段で高額なバイト報酬を受け取るアルバイト（闇バイト）の連絡手段としてもシークレットチャットが用いられている。令和元年以降に警視庁捜査 1 課が摘発した強盗事件 41 件のうち 39 件で Telegram が使用されていた。Telegram でのやりとりの履歴は一度削除されると復元が困難で、物証にならないため、警察当局は、この特質を悪用する犯罪者の摘発に苦労している。

3.4. ロシアと Telegram

2018 年 4 月、Telegram 社が、ロシア政府に暗号化キーを提供するようにとの命令を拒否したため、ロシア通信監督庁は Telegram をロシア国内で使用禁止とした[37]。ロシア政府は 1900 万を超える IP アドレスをブロックするなどして、ロシア国内のユーザーらの Telegram へのアクセスを阻止しようとしたが、ユーザーらは VPN を利用しブロックを回避した[38]。これ以来 Telegram は、ロシア政府のネット検閲に抵抗する象徴となった。2020 年 6 月、ロシア政府は Telegram 社がテロ対策に前向きな姿勢を示したことを理由に、規制を解除した。

---

[35] 出典：vpnMenter『Cybercrime on Telegram: How Hackers Are Using the Messaging App to Share Data Leaks and Hacks』
https://www.vpnmentor.com/blog/cybercrime-on-telegram/

[36] 出典：産経新聞『アプリ「テレグラム」悪用進む　法規制難しく　栃木県警、全国の警察と情報共有で包囲網』
https://www.sankei.com/article/20200902-TRTZXIAFPBJLRPKODZRD6CTJBA/

[37] 出典：REUTERS『Russia starts blocking Telegram messenger』
https://www.reuters.com/article/us-russia-telegram-blocking-idUSKBN1HN13J

[38] 出典：9to5Mac『Russia asks Apple to remove Telegram from App Store after banning the encrypted messaging service』
https://9to5mac.com/2018/04/17/russia-apple-ban-telegram-app-store/

【政治的影響力を強めるチャネル】

2022 年 3 月 21 日、モスクワの裁判所は、ウクライナ侵攻に関連し、米 Meta 社を「過激派組織」と認定。Facebook、Instagram の国内事業を禁止した 。Meta 社のメッセージングアプリ WhatsApp は禁止されなかったが、ロシア国内で同アプリから Telegram への乗り換えが見られた。ロシアでの Telegram のシェアは 68%となり、ロシアで最も人気のあるメッセージングアプリとなった[39]。チャネルはロシア人にとって主要な情報源にもなっており、ロシア当局も自らのチャネルでメッセージを発信し、ロシア政府寄りのチャネルも急拡大している。

独立系ジャーナリストが運営するチャネルである Varlamov News[40]は、ロシア国営テレビ局の社員がニュースの生放送中に「プロパガンダを信じないで」と書かれたポスターを掲げ、「戦争をやめろ」と叫んだ時の動画を無修正で Telegram に投稿し、視聴回数は 120 万回を超えた（**図 13**）。このようにチャネルでは、検閲されていないニュースを自由に発信でき、ロシア政府による規制を免れている。

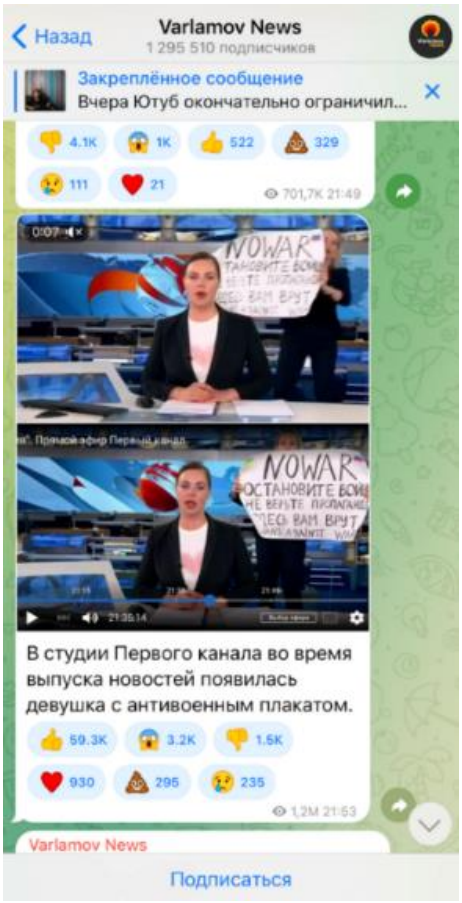


図 13 Varlamov News

3.5. まとめ

Telegram の持つプライバシー保護の強固さは法執行機関による犯罪者の追跡を困難にさせ、さまざまな犯罪の温床となっている。一方で、言論統制下のロシアにおいて Telegram はネット検閲に抵抗する象徴となっている。Telegram を覗くとサイバー犯罪への対処と専制国家の検閲への対抗という二つの命題が矛盾し、国際社会が抱える問題を垣間見ることができる。

以上

[39] 出典：THEWALLSTREETJOURNAL『ロシアで SNS「テレグラム」急成長の理由』
https://jp.wsj.com/articles/telegram-thrives-amid-russias-media-crackdown-11647826301

[40] 出典：Telegram『ValamosNews』
https://t.me/s/varlamov_news

免責事項

本記事の内容は、正確であることに最善を尽くしておりますが、内容を保証するものではなく、本記事の利用に起因して発生したいかなる損害、損失についても補償しませんのでご留意ください。記事内に誤植や内容の誤り、その他ご指摘等、お問い合わせ事項がある場合は、お手数ですが下記までご連絡ください。

お問い合わせ先：NTT セキュリティ・ジャパン株式会社

コンサルティングサービス部　脅威インテリジェンス管理チーム
メールアドレス： WA_Advisorysupport@ntt.com